

4th September 2017 OSCP - Linux Privilege Escalation

Information Gathering

+ Get OS information

```
cat /etc/issue
cat /etc/*-release
cat /proc/version
uname -a
rpm -q kernel
dmesg | grep Linux
ls /boot | grep vmlinuz-
lsb_release -a
```

+ Check sudoers

```
sudo -l
cat /etc/sudoers
```

+ Check password files

Check for misconfigurations - i.e. Is shadow readable? Is passwd writeable?

```
cat /etc/passwd
cat /etc/shadow
ls -l /etc/passwd
ls -l /etc/shadow
```

+ Learn your environment

Search for misconfigured PATH variables. Do they prioritize searching for executable files from a non-secure (i.e. world-writeable) path?

```
cat /etc/profile
cat /etc/bashrc
cat ~/.bash_profile
cat ~/.bashrc
cat ~/.bash_logout
cat ~/.bash_history
env
set
```

+ Check history files

You might find plaintext passwords in there

```
cat ~/.*_history
```

+ Check cronjobs

Search for jobs using programs that run with root privileges and are potentially write-accessible by low-privileged users

```
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 processes running as root for vulnerabilities

```
ps aux | grep root
ps -ef | grep root
```

+ Search files for plaintext credentials

```
grep -ir user *
grep -ir pass *
```

+ Find writable configuration files

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

+ Run privesc scripts

```
LinEnum - https://www.rebootuser.com/?p=1758
linuxprivchecker.py - http://www.securitysift.com/download/linuxprivchecker.py
unix-privesc-check - https://github.com/pentestmonkey/unix-privesc-check
```


Escaping jail shells

```
python -c 'import pty;pty.spawn("/bin/bash")'
echo os.system('/bin/bash')
/bin/sh -i
```


Resources

<https://www.kernel-exploits.com/> [<https://www.kernel-exploits.com/>]
<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
[<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>]

Posted 4th September 2017 by WarLord

 0 Add a comment

Enter your comment...

 **Comment as:**

☐ Notify me