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
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?

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/archives0
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
```