

Linux Compromise Assessment Command Cheat Sheet

The Big Five

Processes • Directories • Files • Users • Logs

Haste makes waste:

```
echo "Don't Panic."
```

Processes

Large amounts of CPU/RAM:

```
top
```

Process tree:

```
ps -auxwf
```

Open network ports or raw sockets:

```
netstat -nalp
```

```
netstat -plant
```

```
ss -a -e -i
```

```
lsof [many options]
```

Deleted binaries still running:

```
ls -alR /proc/* /exe 2> /dev/null |
```

```
grep deleted
```

Process command name/cmdline:

```
strings /proc/<PID>/comm
```

```
strings /proc/<PID>/cmdline
```

Real process path:

```
ls -al /proc/<PID>/exe
```

Process environment:

```
strings /proc/<PID>/environ
```

Process working directory:

```
ls -alR /proc/* /cwd
```

Process running from tmp, dev dirs:

```
ls -alR /proc/* /cwd 2> /dev/null | grep tmp
```

```
ls -alR /proc/* /cwd 2> /dev/null | grep dev
```

Directories

Commonly targeted directories:

```
/tmp, /var/tmp, /dev/shm, /var/run,
```

```
/var/spool, user home directories
```

List and delimit spaces, etc. in names:

```
ls -lap
```

List all hidden directories:

```
find / -type d -name ".*"
```

Files

Immutable files and directories:

```
lsattr / -R 2> /dev/null | grep "\----i"
```

Find SUID/SGID files:

```
find / -type f \( -perm -04000 -o -perm -02000 \) -exec ls
```

```
-lg {} \;
```

Files/dirs with no user/group name:

```
find / \( -nouser -o -nogroup \) -exec ls -lg
```

```
{}
```

List all file types in current dir:

```
file * -p
```

Find executables anywhere, /tmp, etc.:

```
find / -type f -exec file -p {} \; |
```

```
grep ELF
```

```
find /tmp -type f -exec file -p {} \; |
```

```
grep ELF
```

Find files modified/created within last day:

```
find / -mtime -1
```

Persistence areas:

```
/etc/rc.local, /etc/initd, /etc/rc*.d, /etc/modules, /etc/
```

```
cron*, /var/spool/cron/*
```

Package commands to find changed files:

```
rpm -Va | grep ^..5.
```

```
debsums -c
```

Users

Find all ssh authorized_keys files:

```
find / -name authorized_keys
```

History files for users:

```
find / -name *.history
```

History files linked to /dev/null:

```
ls -alR / 2> /dev/null | grep *.history |
```

```
grep null
```

Look for UID 0/GID 0:

```
grep ":0:" /etc/passwd
```

Check sudoers file:

```
cat /etc/sudoers and /etc/group
```

Check scheduled tasks:

```
crontab -l
```

```
atq
```

```
systemctl list-timers --all
```

Logs

Check for zero size logs:

```
ls -al /var/log/*
```

Dump audit logs:

```
utmpdump /var/log/wtmp
```

```
utmpdump /var/run/utmp
```

```
utmpdump /var/log/btmp
```

```
last
```

```
lastb
```

Find logs with binary in them:

```
grep [[:cntrl:]] /var/log/*.log
```

www.sandflysecurity.com

@SandflySecurity

