**Linux Malware Seek & Destroy**

**Bandwidth monitoring**

Networx

* Free and all OS

Bandwidth monitoring is a good way to see if internet usage is being used in a way that it shouldn’t

Netstat, Wireshark (TCP dump)

**Linux**

Most Linux threats are on servers and not on workstations

Sysdig

Tool for capturing and filtering events and then applying scripts to the events discovered

* Linux, MacOS, Windows
* Combines the functionality of
  + SE trace
  + TCP dump
  + Lsof
  + LUA scripts
  + Etc.

**Downloading sysdig**

Apt-get -y curl

Curl -s [https://s3.amazonaws.com/download .draios.com/DRAIOS-GPG-KEY.public](https://s3.amazonaws.com/download%20.draios.com/DRAIOS-GPG-KEY.public) | apt-key add -OK

* Adding the public key for the sysdig developers

Curl -s -o /etc/apt/sources.list.d/draios.list <http://download.draios.com/stable/deb/draios.list>

* Download and add the draios list to our sources so app-get can get it

Apt-get update

Apt-get -y install linux-headers-$(uname -r)

* Installing linux headers

Apt-get -y install sysdig

Filtering using sysdig

Inspecting a suspicious process

Systdig proc.name=ssh

* This command will filter and show you the info on the ssh server
* Local ip
* Source port
* Remote addr
* Remote port

Can also run scripts to look for top processors in the network for usage and bandwidth

* Sysdig -c topprocs\_net
* Sysdig -c topprocs\_cpu
  + Will show cpu usage instead

To see what directories the user ‘root’ has been accessing

* Sysdig -p”%evt.arg.path” “evt.type+chdir and user.name=root”

To check if there is any activity in a specific directory

* Sysdig fd.name contains /home/Nathan/passwords
* Will show cmd prompt and data processed
* Can be specific and check who has opened the file
* Sysdig evt.type=open and fd.name contains /home/Nathan/passwords
  + Will show specifically who opened it with an open cmd like nano, wont show other cmds like cat

Capture all system events to a file

* Sysdig -qw dumpfile.scap
* Sysdig -r dumpfile.scap
  + Will query file
* Sysdig -r dumpfile.scap -c topprocs\_cpu
  + Will show you the top CPU processes in the file at the time of capturing

Long-term capture

* Compress data as capturing it
* Sysdig -s 4096 -z -w dumpfile.scap.gz

**Csysdig (GUI)**

Easier to use as it uses other tools by default

Csysdig -d 5000

* Changes the update time to 5 seconds from the standard 2 seconds if you don’t need all that data

Sysdig -qw dumpfile.scap

* To create trace

Cysdig -r dumpfile.scap

* Pulls up the trace file in the GUI

The connections tab is good for finding command & control or remote access

Lists all network connections active in the sampling interval

* Will also show cmds used to generate that connection

Spy users

* Lists all cmds that are run interactively i.e., that has a shell as a parent process

DebSums

* Checks the md5sums of the system files against the hashes in the respective repos to check for any changes (Integrity)

Unhide

* Detects hidden processes
* Detects open TCP and UDP ports that are otherwise unseen in netstat

**Netstat**

Any connection that you don’t understand must be traced back to its source and analysed

Netstat -aon | more

* A = All
* O = Time
* N = Numbers – to see numbers instead of resolved ports and ips
* T = TCP
* U = UDP
* P = Process ID
* L = Listening
* C = Continuous (refresh)

Will show local and remote addr with source and dst port

Also, whether its listening or established

To just see listening processes

* Netstat -atp |grep LISTEN
* Netstat -luptn

**Lsof**

List open files

Lsof -P -i

* I = list ip sockets
* P = don’t resolve port names
* N = don’t resolve ip addr

Lsof -p -I |grep EST/LIST

* Shows established or listening connections

**Rkhunter**

Checks for presence of rootkits and others

Signature searching tool

Chkrootkit

* In Debian repo

Linux Malware Detect

Tiger

ClamAV

**Persistence**

Malware remains running after reboot by remaining in a persistent task like services, drivers, tasks, kernels, crontab etc.

Ls -la /var/lib/dpkg/status

Ls -la /var/log/dpkg.log

* Both of these directories contain information on downloaded packages so these can be used to analyse for packages that shouldn’t be downloaded

Tail -20 /var/log/dpkg.log

* To look at latest entries

Creating a new service is a common way for malware to create persistence

INIT is the first process started during boot

INIT uses systemd now

* Systemctl status ‘service’
* Sytsemctl status ‘Tor’
  + Shows the Tor service is running
* INIT file will show variables as to why Tor is running
  + Nano /etc/init.d/tor

Systemctl can help show you persistence in systemd