LD_PRELOAD ROOTKITS

Hal Pomeranz

WHO IS HAL POMERANZ?

Started as a Unix Sys Admin in the 1980s

Independent consultant since 1997

Digital forensics, incident response, expert witness

Have done some interesting Linux/Unix investigations

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

https://archive.org/details/HalLinuxForensics

ROOTKIT SYMPTOMS

Hidden processes –

"Our CPU is pegged, but we don't see any responsible processes"

Stealthed network activity –

"Firewall is reporting network activity, ***`netstat`*** *says nothing is going on"*

TYPES OF LINUX ROOTKITS

Loadable kernel module (LKM) –

- Malicious kernel module loaded
- Hooks system call interface in kernel

LD_PRELOAD –

- Malicious shared library installed
- Forced into memory space of new processes
- Hooks legitimate library calls in userland

CUT TO THE CHASE

```
# cat /etc/ld.so.preload
cat: /etc/ld.so.preload: No such file or directory
# df -h /etc
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/LabVM-root     28G   17G  9.8G  63% /
# debugfs -R 'cat /etc/ld.so.preload' /dev/mapper/LabVM-root
debugfs 1.46.2 (28-Feb-2021)
/usr/lib/x86_64-linux-gnu/libutilr.so
```

OTHER INVESTIGATIVE IDEAS

Look for strange library paths in **`/proc/<pid>/maps`**

Compare **`ldd`** output to **`/proc/<pid>/maps`**

Look for recently added libraries

USEFUL VOLATILITY PLUGINS

linux.elfs.Elfs – shows all executable/shared lib paths

- Look for non-standard path names
- Stack results and look for suspicious shared libs

Drill into suspicious processes with PsAux, Lsof, Sockstat, etc

UNPACK ATTACKER SESSIONS

See suspicious shells in PsTree output?

Check out command history with Bash plugin!

THANK YOU!

Any final questions?

Thanks for listening!

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

https://archive.org/details/HalLinuxForensics

Linux Forensics Live Online!
September 12-15

Linux Command Line
at WWHF Deadwood