SANDFLY
SECURITY

Command Line Forensics For Linux

Craig H. Rowland
chc2017@sandflysecurity.com
www.sandflysecurity.com

Introduction

What you will learn:

Checking Linux systems for suspicious activity using basic tools.

What you will not learn:

Finding North Korean zero day exploits.

1000:1 Rule

Defenders need to know thousands of ways for a system to get compromised. Attackers need to be right just once.

Attackers need to know about thousands of ways to cover their tracks. Defenders need to spot something wrong just once.

Simple First

“Common problems are surprisingly common.”

- Don’t worry about Advanced Persistent Threats (APT)

- Worry about Commonly Run Attacks Preferred (CRAP)

- If you can’t spot common problems, why worry about sophisticated attacks?

What About Zero Day Attacks?

- Zero day attacks are rare and expensive
- Common attacks work and have total deniability
- Advanced attacks are particular about how and where they work
- 1000:1 Rule: They still need to hide once in!

Basic Concepts

Computers are not spontaneous

Focus first on what got your attention

Basic Concepts

Look for suspicious directories

Look for suspicious files

Look for suspicious processes

Basic Linux Commands

ls
lsattr
cat
strings
last
lastb

lastlog
utmpdump
ps
file
rpm
debsums

Suspicious Directories

SANDFLY SECURITY

Targeted Directories

/tmp, /var/tmp

/dev

/dev/shm

/bin

/sbin

/usr/bin

/usr/sbin

/lib, /lib64, /lib32

/usr/lib, /usr/lib64, /usr/lib32

/etc

/var

/var/log

/var/spool/cron

Web server directories

Privileged/system user directories

Suspicious Directories

- Tries to look like a system directory
- Hidden directory in system areas
- Weird permissions, attributes, or creation dates
- Doesn’t match what a duplicate virtual OS image shows
- Contains suspicious files and data

Suspicious Directories

```
root@ubuntu16-dirty:~# ls -al /bin
total 17120
drwxr-xr-x  2 root root    4096 Jul 25 21:45
drwxr-xr-x  2 root root    4096 Sep  7 09:52  .
drwxr-xr-x 10 root root   12288 Sep  7 09:52 .
drwxr-xr-x  2 root root    4096 Mar 25  2017 .
drwxr-xr-x  2 root root    4096 Mar 25  2017 . .
drwxr-xr-x 24 root root    4096 Oct 11 04:01 ..
drwxr-xr-x  2 root root    4096 Jun  4 01:56 ..
drwxr-xr-x  2 root root    4096 Jun  4 02:25 ...
drwxr-xr-x  2 root root    4096 Jun  7 00:46 ..%
-rwxr-xr-x  1 root root 1037528 May 16 12:49 bash
-rwxr-xr-x  1 root root  520992 Jun 15 23:46 btrfs
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-calc-size
lrwxrwxrwx  1 root root       5 Jun 15 23:46 btrfsck -> btrfs
-rwxr-xr-x  1 root root  278376 Jun 15 23:46 btrfs-convert
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-debug-tree
```

Suspicious Directories

```
root@ubuntu16-dirty:~# ls -al /bin
total 17120
drwxr-xr-x  2 root root    4096 Jul 25 21:45
drwxr-xr-x  2 root root    4096 Sep  7 09:52  .
drwxr-xr-x 10 root root   12288 Sep  7 09:52 .
drwxr-xr-x  2 root root    4096 Mar 25  2017 .
drwxr-xr-x  2 root root    4096 Mar 25  2017 . .
drwxr-xr-x 24 root root    4096 Oct 11 04:01 ..
drwxr-xr-x  2 root root    4096 Jun  4 01:56 ..
drwxr-xr-x  2 root root    4096 Jun  4 02:25 ...
drwxr-xr-x  2 root root    4096 Jun  7 00:46 ..%
-rwxr-xr-x  1 root root 1037528 May 16 12:49 bash
-rwxr-xr-x  1 root root  520992 Jun 15 23:46 btrfs
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-calc-size
lrwxrwxrwx  1 root root       5 Jun 15 23:46 btrfsck -> btrfs
-rwxr-xr-x  1 root root  278376 Jun 15 23:46 btrfs-convert
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-debug-tree
```

What is this?

Suspicious Directories

```
root@ubuntu16-dirty:~# ls -lap /bin
total 17120
drwxr-xr-x  2  root root    4096 Jul 25 21:45  /
drwxr-xr-x  2  root root    4096 Sep  7 09:52  ./
drwxr-xr-x 10 root root   12288 Sep  7 09:52 ./
drwxr-xr-x  2  root root    4096 Mar 25  2017 . /
drwxr-xr-x 24 root root    4096 Oct 11 04:01 ../
drwxr-xr-x  2  root root    4096 Jun  4 01:56 .. /
drwxr-xr-x  2  root root    4096 Jun  4 02:25 .../
drwxr-xr-x  2  root root    4096 Jun  7 00:46 ..%/
-rwxr-xr-x  1 root root 1037528 May 16 12:49 bash
-rwxr-xr-x  1 root root  520992 Jun 15 23:46 btrfs
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-calc-size
-rwxr-xr-x  1 root root  278376 Jun 15 23:46 btrfs-convert
-rwxr-xr-x  1 root root  249464 Jun 15 23:46 btrfs-debug-tree
-rwxr-xr-x  1 root root  245368 Jun 15 23:46 btrfs-find-root
-rwxr-xr-x  1 root root  270136 Jun 15 23:46 btrfs-image
```

“space”

“space” dot

dot “space”

dot dot “space”

Trying to look legit

Special characters

www.sandflysecurity.com

SANDFLY SECURITY

Suspicious Directories

```
root@ubuntu16-dirty:/bin# lsattr -a /bin
----------I--e-- /bin/.
------------e-- /bin/..
------------e-- /bin/..
----i--------e-- /bin/...
------------e-- /bin/kmod
------------e-- /bin/ping6
------------e-- /bin/cpio
------------e-- /bin/true
------------e-- /bin/ space_before_daemon
------------e-- /bin/tailf
------------e-- /bin/systemd-tmpfiles
------------e-- /bin/mknod
------------e-- /bin/setfacl
------------e-- /bin/ss
----i--------e-- /bin/.foobar
```

Immutable flags are a worm/backdoor persistence tactic.

Suspicious name and immutable.

Hidden in binary directory and immutable.

www.sandflysecurity.com

SANDFLY SECURITY

Suspicious Files

Suspicious Files

- Tampered or missing audit logs
- Files that are not the type they claim to be or are out of place
- Binaries that are modified or in strange locations

Suspicious Files
Audit Log Tampering

High value and frequently targeted files:

/var/log/wtmp - All valid past logins
/var/log/lastlog - Last login for each user
/var/log/btmp - All bad logins
/var/run/utmp - All current logins
/var/log/* - Various logs

Suspicious Files
Zero Byte Logs

```
root@ubuntu16-dirty:~# ls -al /var/log
total 104
drwxrwxr-x  8 root   syslog   4096 Oct 24 06:25 .
drwxr-xr-x 17 root   root     4096 Jul 25 23:18 ..
-rw-r-----  1 syslog adm         0 Oct 25 00:55 auth.log
-rw-r-----  1 syslog adm         0 Oct 25 00:55 auth.log.1
-rw-r-----  1 syslog adm         0 Oct 25 00:55 auth.log.2.gz
-rw-rw----  1 root   utmp        0 Oct 25 00:55 btmp
-rw-------  1 root   utmp        0 Oct 25 00:55 btmp.1
...
-rw-r— —  1 syslog adm        0 Oct 25 00:55 kern.log
-rw-r-----  1 syslog adm         0 Oct 25 00:55 kern.log.1
-rw-r-----  1 syslog adm         0 Oct 25 00:55 kern.log.2.gz
-rw-r--r--  1 root   root   292292 Oct 24 21:09 lastlog
-rw-r-----  1 syslog adm         0 Oct 25 00:55 syslog
-rw-r-----  1 syslog adm         0 Oct 25 00:55 syslog.1
-rw-r-----  1 syslog adm         0 Oct 25 00:55 syslog.2.gz
...
```

Zero byte audit logs?

No bad logins?

No kernel messages?

Log rotate compressed a zero byte file?

Date/time all identical?

Suspicious Files
Temp Files Left Behind

root@ubuntu16-dirty:~# **ls -al /tmp**
total 44

drwxrwxrwt 8 root root 12288 Sep 5 00:12 .
drwxr-xr-x 23 root root 4096 Sep 5 00:03 ..
drwxrwxrwt 2 root root 4096 Sep 5 00:03 .font-unix
drwxrwxrwt 2 root root 4096 Sep 5 00:03 .ICE-unix
drwxrwxrwt 2 root root 4096 Sep 5 00:03 .Test-unix
-rw-r--r-- 1 root root 2304 Sep 5 00:12 utmp.bak
drwxrwxrwt 2 root root 4096 Sep 5 00:03 .X11-unix
drwxrwxrwt 2 root root 4096 Sep 5 00:03 .XIM-unix

File left by poorly written or crashed log cleaner.

Suspicious Files
Null Erased Current Logins

```
root@ubuntu16-dirty:~# utmpdump < /var/run/utmp
Utmp dump of /dev/stdin
[2] [00000] [~~  ] [reboot  ] [~          ] [4.4.0-93-generic    ] [0.0.0.0        ] [Tue Sep 05 00:03:17 2017 UTC]
[1] [00053] [~~  ] [runlevel] [~          ] [4.4.0-93-generic    ] [0.0.0.0        ] [Tue Sep 05 00:03:22 2017 UTC]
[6] [01391] [tyS0] [LOGIN   ] [ttyS0      ] [                    ] [0.0.0.0        ] [Tue Sep 05 00:03:23 2017 UTC]
[6] [01388] [tty1] [LOGIN   ] [tty1       ] [                    ] [0.0.0.0        ] [Tue Sep 05 00:03:23 2017 UTC]
[7] [01488] [ts/0] [root    ] [pts/0      ] [120.136.1.1         ] [120.136.1.1    ] [Tue Sep 05 00:03:57 2017 UTC]
[0] [00000] [    ] [        ] [           ] [                    ] [0.0.0.0        ] [                            ]
```

Type 0 (null)

Entries are empty.

No date.

Someone overwrote this entry with nulls.

Suspicious Files
Null Erased Bad Logins

```
root@ubuntu16-dirty:~# utmpdump < /var/log/btmp
Utmp dump of /dev/stdin
[6] [23367] [    ] [cbm     ] [ssh:notty   ] [13.78.176.165      ] [13.78.176.165  ] [Mon Sep 11 20:52:56 2017 UTC]
[6] [23367] [    ] [cbm     ] [ssh:notty   ] [13.78.176.165      ] [13.78.176.165  ] [Mon Sep 11 20:52:58 2017 UTC]
[6] [23515] [    ] [cbm     ] [ssh:notty   ] [13.78.176.165      ] [13.78.176.165  ] [Mon Sep 11 20:55:30 2017 UTC]
[6] [23515] [    ] [cbm     ] [ssh:notty   ] [13.78.176.165      ] [13.78.176.165  ] [Mon Sep 11 20:55:33 2017 UTC]
[0] [00000] [    ] [        ] [            ] [                   ] [0.0.0.0        ] [                        ]
[0] [00000] [    ] [        ] [            ] [                   ] [0.0.0.0        ] [                        ]
[0] [00000] [    ] [        ] [            ] [                   ] [0.0.0.0        ] [                        ]
```

Type 0 (null) **Entries are empty.** **No date.**

utmpdump works on wtmp, utmp, and btmp

SANDFLY SECURITY

Suspicious Files
Null Erased Bad Logins

```
root@ubuntu16-dirty:~# lastb
cbm      ssh:notty    13.78.176.165    Mon Sep 11 20:58 - 20:58  (00:00)
cbm      ssh:notty    13.78.176.165    Mon Sep 11 20:58 - 20:58  (00:00)
cbm      ssh:notty    13.78.176.165    Mon Sep 11 20:52 - 20:52  (00:00)
cbm      ssh:notty    13.78.176.165    Mon Sep 11 20:52 - 20:52  (00:00)
Thu Jan  1 00:00 - 00:00  (00:00)
Thu Jan  1 00:00 - 00:00  (00:00)
```

These two entries are nulled.

Overwritten after intruder logged in.

Suspicious Files Erased Audit Logs

Deleting these files disables login auditing on Linux:

/var/log/wtmp
/var/log/lastlog
/var/log/btmp
/var/run/utmp

Suspicious Files
File not what it is named

root@ubuntu16-dirty:~/html# **file** *
upload.html: HTML document, ASCII text
download.html: HTML document, ASCII text
disk.html: HTML document, ASCII text
index.html: HTML document, ASCII text
erase.html: HTML document, ASCII text

…

update.html: ELF 64-bit LSB executable, …,

This is not a html file.

Suspicious Files
System files modified

[root@centos-6-2 ~]# **rpm -Va | grep ^..5.**
SM5....T. c /etc/ssh/sshd_config
S.5....T. c /etc/ssh/ssh_config
S.5....T. c /root/.bashrc

Manually inspect these.

root@ubuntu16-dirty:/bin# **debsums -c**
/usr/sbin/nologin

Very strange!

Suspicious Processes

SANDFLY SECURITY

Suspicious Processes

- Processes named to look legit
- Open ports you don’t recognize
- Outbound connections you don’t recognize
- Deleted processes
- Deleted processes with open network ports

Suspicious Processes

port 22222

```
root@ubuntu16-dirty:/lib# netstat -nalp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address     Foreign Address         State       PID
tcp        0      0 0.0.0.0:22222     0.0.0.0:*               LISTEN      22251/apache
tcp        0      0 0.0.0.0:22        0.0.0.0:*               LISTEN      1293/sshd
tcp        0    332 192.168.1.122     120.136.1.1:56639       ESTABLISHED 11022/2
tcp6       0      0 :::22             :::*                    LISTEN      1293/sshd
udp        0      0 0.0.0.0:555       0.0.0.0:*                           32481/t
raw        0      0 0.0.0.0:1         0.0.0.0:*               7           22251/apache
```

Raw socket

ICMP Protocol

“apache”

Suspicious Processes

```
root@ubuntu16-dirty:/lib# ps -auxwf
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0     0 ?        S    Sep20   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    Sep20   0:24  \_ [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   Sep20   0:00  \_ [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    Sep20   0:43  \_ [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    Sep20   0:00  \_ [rcu_bh]
...
root       667  0.0  0.0 102968   352 ?        Ss   Sep20   0:00 /sbin/lvmetad -f
root       700  0.0  0.5  42592  2796 ?        Ss   Sep20   0:07 /lib/systemd/systemd-udevd
root     22251 0.0  0.1   9184   688 ?        S    Sep20   0:00 /dev/apache
```

High PID

Running out of /dev

Suspicious Processes

```
root@ubuntu16-dirty:~# ls -al /proc/22251
total 0
dr-xr-xr-x   9 root root 0 Sep 23 23:50 .
dr-xr-xr-x 127 root root 0 Sep 20 01:06 ..
dr-xr-xr-x   2 root root 0 Oct 25 02:01 attr
-rw-r--r--   1 root root 0 Oct 25 02:01 autogroup
-r--------   1 root root 0 Oct 25 02:01 auxv
-r--r--r--   1 root root 0 Oct 25 02:01 cgroup
...
lrwxrwxrwx   1 root root 0 Oct 25 04:11 exe -> /dev/apache (deleted)
dr-x------   2 root root 0 Oct 25 04:15 fd
dr-x------   2 root root 0 Oct 25 01:59 fdinfo
-rw-r--r--   1 root root 0 Oct 25 02:01 gid_map
```

PID from previous.

Deleted from disk, but still running.

SANDFLY SECURITY

Suspicious Processes

```
root@ubuntu16-dirty:~# strings /dev/suspicious_binary
/lib64/ld-linux-x86-64.so.2
libc.so.6
socket
execl
htons
perror
daemon
listen
bind
dup2
atoi
accept
GLIBC_2.4
bind() failed
/bin/sh
```

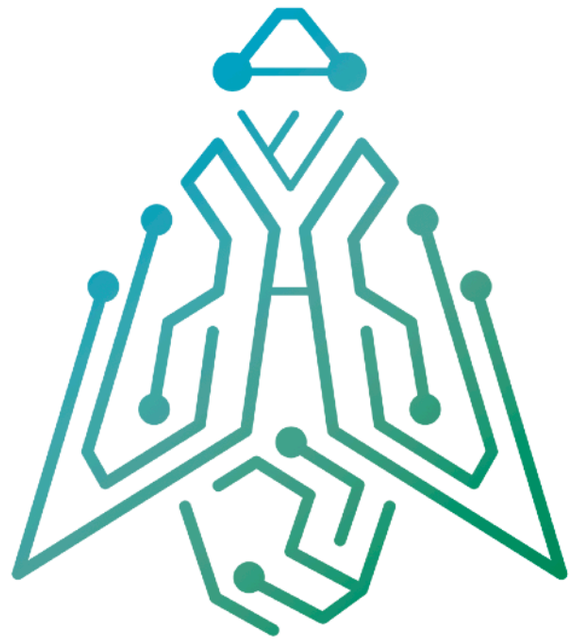
Do NOT run strace on suspicious binaries!

listen(), bind(), accept()
Holy Trinity of bindshells

Not good!

Conclusions

- Focus on simple first
- Remember the 1000:1 rule works in your advantage once a host is compromised
- Look for suspicious directories, files, and processes
- Simple tools and careful attention can find many problems



SANDFLY SECURITY

www.sandflysecurity.com