

**SANDFLY**  
**SECURITY**

AGENTLESS THREAT HUNTING

# Command Line Compromise Detection for Linux

Craig H. Rowland

@CraigHRowland

@SandflySecurity

[www.sandflysecurity.com](http://www.sandflysecurity.com)

# Introduction

**echo “Don’t Panic.”**

# Simple First

**“Common problems are surprisingly common.”**

- Don't worry about Advanced Persistent Threats (APT)
- Worry about Commonly Run Attacks Preferred (CRAP)
- Spotting common problems allows you to find advanced attackers.

# 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.

# The Big Five

Processes

Directories

Files

Users

Logs

# Suspicious Processes

# Suspicious Processes

- Named to look legit or very odd.
- Network activity you don't recognize.
- High CPU/RAM.
- Deleted binary still running.
- Combination of the above.

# Suspicious Processes

## Unusual Ports

### TCP port 22222

```
root@ubuntu18-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	10580/cron
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	10580/cron

Raw socket

ICMP Protocol

PID

“cron”



# Suspicious Processes


## Investigating a PID

```
root@ubuntu-18-dirty:/# ls -alR /proc/*/cwd 2> /dev/null | grep tmp  
lrwxrwxrwx 1 root      root      0 Nov 14 02:07 /proc/10580/cwd -> /tmp
```

PID of  
interest



Running  
from /tmp



```
root@ubuntu-18-dirty:/tmp# ls -alR /proc/*/exe 2> /dev/null | grep deleted  
lrwxrwxrwx 1 root      root      0 Nov 13 07:39 /proc/10580/exe -> /usr/bin/perl (deleted)
```

Binary deleted but still running?



# Suspicious Processes

## Investigating a PID

root@ubuntu-18-dirty:~# **ls -al /proc/10580/cwd**  
lrwxrwxrwx 1 root root 0 Nov 14 02:07 /proc/10580/cwd -> /tmp

root@ubuntu-18-dirty:/tmp# **cat /proc/10580/comm**  
/usr/sbin/cron

root@ubuntu-18-dirty:/tmp# **cat /proc/10580/cmdline**  
/usr/sbin/cron

root@ubuntu-18-dirty:/tmp# **ls -al /proc/10580/exe**  
lrwxrwxrwx 1 root root 0 Nov 13 07:39 /proc/10580/exe -> '/usr/bin/perl (deleted)'

PID of interest

Running  
from /tmp

Says it's cron.

Really, I'm cron!

You're not cron.

# Suspicious Directories

# Suspicious Directories

- Used to hide malicious binaries.
- Used to hide stolen data.
- Used to holding staging data for further incursion.
- Used to hold persistence mechanisms.

# Suspicious Directories Commonly Targeted

/tmp, /var/tmp

/lib\*, /usr/lib\*

/dev

/etc

/dev/shm

/var/log

/bin

/var/spool

/sbin

public\_html

/usr/bin

Privileged home directories

/usr/sbin

Standard home directories

# Suspicious Directories

## Weird Names

```
root@ubuntu18-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
```

# Suspicious Directories

## Weird Names

```
root@ubuntu18-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
```



What is this?

# Suspicious Directories

## Weird Names

```
root@ubuntu18-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-siz
```

“space”

“space” dot

dot “space”

dot dot “space”

Trying to look  
legit

Special  
characters



# Suspicious Directories

## Hidden Directories

```
root@ubuntu-18:/# find / -type d -name ".*"
```

```
/root/.local
```

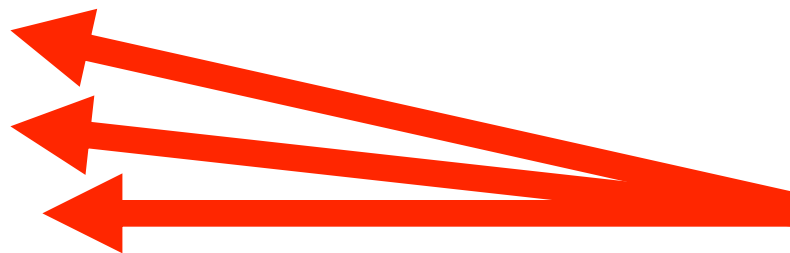
```
/root/.ssh
```

```
/lib/modules/4.15.0-34-generic/vdso/.build-id
```

```
/bin/. .
```

```
/dev/.bLKb
```

```
/dev/shm/. .
```



**All suspicious!**

# Suspicious Files

# Suspicious Files

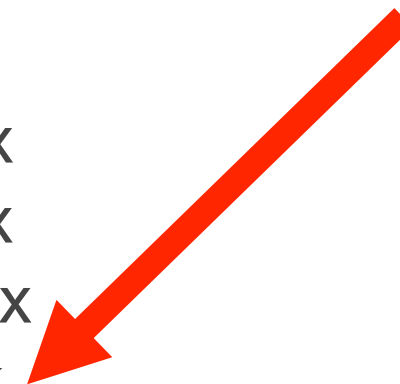
- Exploit traces left behind from attack.
- Files that are not what they claim to be or are out of place.
- Binaries that are modified or in strange locations.

# Suspicious Files

## Exploit Traces Left Behind

```
root@ubuntu-18-dirty:~# ls -al /tmp
total 44
rwxrwxrwt  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
```

Left by poorly  
written or  
crashed  
log cleaner.



# Suspicious Files


## Immutable Files

```
root@ubuntu-18-dirty:/tmp# lsattr / -R 2> /dev/null | grep "\----i"
```

```
----i-----e--- /tmp/.t
```

```
----i-----e--- /bin/pss
```

Suspicious name  
and immutable in  
/tmp.



Binaries are not normally  
set immutable.

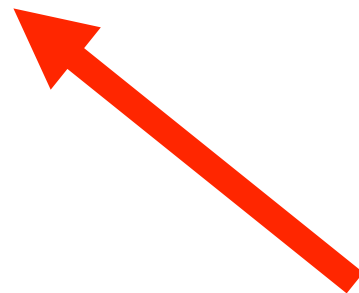


# Suspicious Files

## File Masquerading

```
root@ubuntu-18-dirty:~/public_html# file * -p
```

```
1.jpg:    ELF 32-bit LSB executable, ARM, ...statically linked, stripped  
2.jpg:    ELF 32-bit LSB executable, ARM, ...statically linked, stripped  
3.jpg:    ELF 32-bit MSB executable, MIPS, ...statically linked, stripped  
4.jpg:    ELF 32-bit LSB executable, MIPS, ...statically linked, stripped  
index.html: data  
logo.jpg: PHP script, ASCII text  
logo.png: PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
```

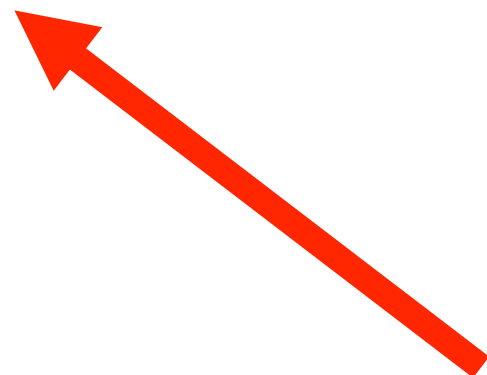


JPGs are ELF executables.  
HTML is unknown data.  
Another JPG is PHP.

# Suspicious Files

## Hidden Binaries

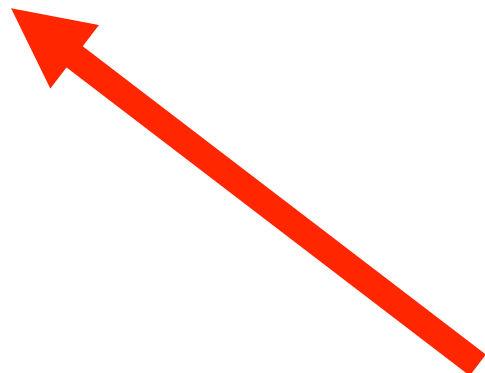
```
root@ubuntu-18-dirty:/tmp# find / -name ".*" -exec file -p '{}' \; | grep ELF  
/var/tmp/.ICE-unix/.db: ELF 64-bit ... stripped
```



Hidden binary in /tmp directory. Why?

# Suspicious Files Named Pipes

```
root@ubuntu-18:/# find / -type p  
/run/dmeventd-client  
/run/dmeventd-server  
...  
/tmp/f
```



One character and in a /tmp directory?



# 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
```

Why was this replaced?



# Suspicious Users


# Suspicious Users

## History File Weirdness

Should www user have  
a history file?

Creation  
Date

Anti-forensics



```
root@ubuntu-18:/# ls -alR | grep .*history
lrwxrwxrwx 1 www www 9 Nov 13 00:23 .bash_history -> /dev/null
-rw----- 1 root root 53083 Nov 12 23:49 .bash_history
```

# Suspicious Users

## SSH Keys

```
root@ubuntu-18-dirty:/tmp# find / -name authorized_keys
/root/.ssh/authorized_keys
/bin/.ssh/authorized_keys
/home/jscott/.ssh/authorized_keys
/home/www/.ssh/authorized_keys
```

User bin with  
SSH key?

Do you recognize all users  
that should have  
SSH credentials?

# Suspicious Users

## Scheduler Persistence

```
root@ubuntu-18:/tmp# crontab -l  
* * * * * /tmp/.d >/dev/null 2>&1
```

Weird name.

Cron script in tmp?

# Suspicious Logs

# Suspicious Logs

## 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 Logs

## 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 bttmp
```

```
-rw----- 1 root utmp 0 Oct 25 00:55 bttmp.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?



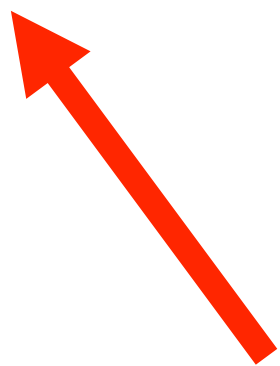
# Suspicious Logs

## Null Erased Logins

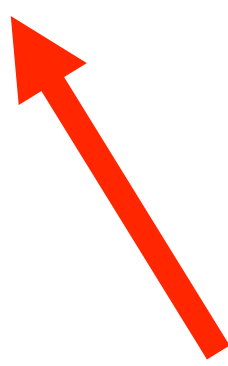
```
root@ubuntu16-dirty:~# utmpdump /var/run/utmp
```

```
Utmp dump of /dev/stdin
```

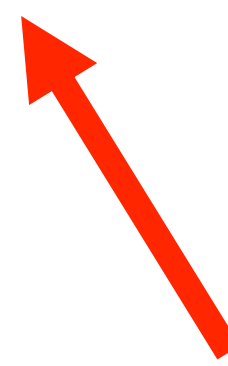
```
[2] [00000] [~~ ] [reboot ] [~      ] [4.4.0-93-generic ] [0.0.0.0      ] [Tue Sep 05 00:03:17 2017 UTC]
[1] [00053] [~~ ] [runlevel] [~      ] [4.4.0-93-generic ] [0.0.0.0      ] [Tue Sep 05 00:03:22 2017 UTC]
[6] [01391] [tyS0] [LOGIN  ] [ttyS0    ] [      ] [0.0.0.0      ] [Tue Sep 05 00:03:23 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 Logs

## 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    ] [  ] [  ]
[0] [00000] [  ] [  ] [  ] [  ] [0.0.0.0    ] [  ] [  ]
```



Type 0 (null)



Entries are empty.



No date.

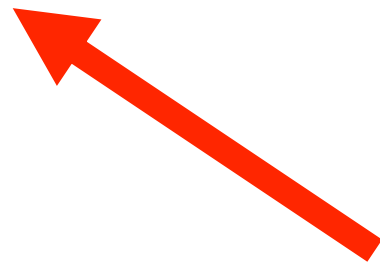
utmpdump works on wtmp, utmp, and btmp

# Suspicious Logs

## 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.

# Conclusions

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

# Linux Compromise Detection 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:

```
cat /proc/<PID>/comm
```

```
cat /proc/<PID>/cmdline
```

Real process path:

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

Process environment:

```
cat /proc/<PID>/environ
```

Process working directory:

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

```
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

Show all 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, /dev, etc.:

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

Find all named pipes:

```
find / -type p
```

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
```

Find history files for all uses:

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

History files linked to /dev/null:

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

List UID 0/GID 0 users:

```
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
```

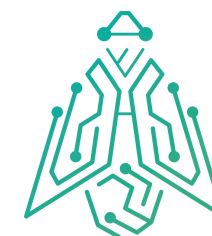
```
utmpdump /var/log/btmp
```

```
last
```

```
lastb
```

Logs with binary in them:

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



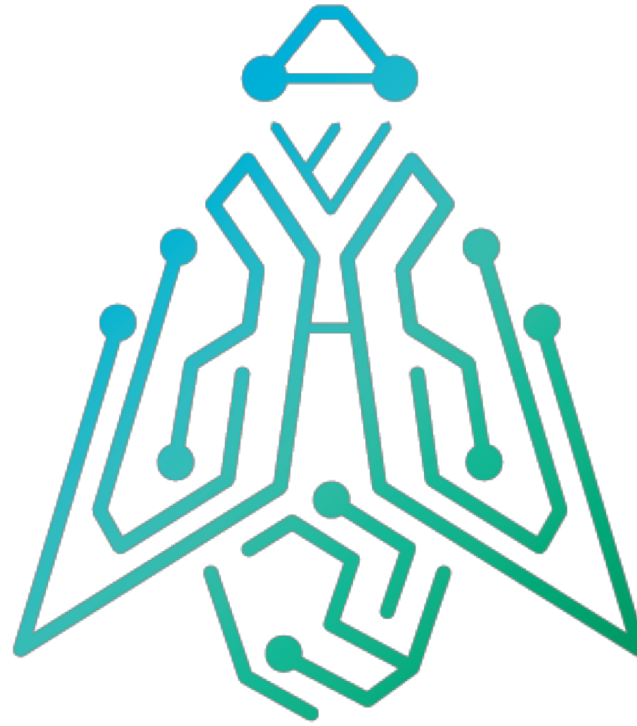
**SANDFLY**  
**SECURITY**

[www.sandflysecurity.com](http://www.sandflysecurity.com)  
@SandflySecurity

# Links

## **PDF Linux Compromise Detection Cheat Sheet**

[www.sandflysecurity.com/blog/compromised-linux-cheat-sheet/](http://www.sandflysecurity.com/blog/compromised-linux-cheat-sheet/)



# SANDFLY SECURITY

AGENTLESS THREAT HUNTING

[www.sandflysecurity.com](http://www.sandflysecurity.com)