Assignment Report 1

Author: Ruth Dirnfeld

Department and Organization: Linnaeus University
Investigation Number. 001
Report Date: 2019-04-09

Executive Summary

Bob, a professor of Computer Science, got an email from the Network Operations Center (NOC) at the University saying that his lab's server was infected with a worm -- the NOC determined this because of a huge spike in Internet traffic which occurred at 4 in the morning. Bob immediately shut it down and brought it in to be imaged, and doesn't think it was infected, but the University wants independent confirmation before they will put it back online. Bob mentioned the following account files are on the machine: 'bob', 'eric', 'kevin', 'peter' and 'takeda'.

The purpose of the examination is to find out whether the server was compromised or not. If it was compromised the questions are how / what happened and what needs to happen before the system is put back into service.

The examined image file shows the following major findings:
Each of the users' directories 'bob', 'eric', 'kevin' and 'takeda' 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 2010-01-04 around 18:00 CET. When viewing at the history of commands of the individual users, worth mention are the following:
1. Bob - shut down the system on the 2010-01-04 around 18:00 CET
2. Eric - made multiple logins and logouts of the system on the 2010-01-04, which might seem suspicious.
3. Takeda - extracted an eggdrop .tar file which is an IRC bot - described in detail in the Report Findings section.
4. Kevin - used a command to synchronize music at the 4th hour of the day, in other words, at 4 in the morning - every day. This causes a huge spike in Internet traffic.

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 autopsy. 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 shortly before Bob's shutdown. The findings will be shown in CET, but in the auth.log file, the time of modifications and access is with -9h offset. Explanation example: One file was modified on 2010-01-04 18:00:25 CET or visible in auth.log file modified on 2010-01-04 9:00:25 because of the -9h offset. The following are the different users:

- ### Bob

  Bob's account shows 5 files, where only 1 was modified on 2010-01-04 18:00:25 CET. The file which shows the stated activity is: .bash_history. The other four files are .bash_logout .bashrc .profile .sudo_as_admin_successful
  During the analysis of the file .bash_history the examiner has found that it was modified on 2010-01-04 18:00:25 CET with the command:
  sudo shutdown -h now
  Bob noted in his statement that "He immediately shut it down and brought it in to be imaged". The command on the 2010-01-04 18:00:25 CET confirms Bob's statement, since this command shuts down all processes, turns off the CPUs and returns the control to a ROM monitor of the mainboard needing the user to press the power button to get a power supply.

- ### Eric

  Eric's account shows 4 files, where only 1 was modified on 2010-01-04 17:57:47 CET. The file which shows the stated activity is: .bash_history. The other three files are .bash_logout .bashrc .profile During the analysis of the file .bash_history the examiner has found that it was modified on 2010-01-04 17:57:47 CET with the following two commands alternately:
  mutt
  logout
  Eric was logging in and out at within a 2-minute window starting at 17:56:06 CET and ending at 17:57:47 CET alternately. The examiner has found no further evidence of why this was done, but logging in and out does not cause a huge spike in Internet traffic.

- ### Kevin

  Kevin's account shows 4 files and 3 directories, where 2 directories and 1 file were modified on 2010-01-04. Modified were in total 3, explained as follows:

  1. ".ssh" directory contains files:
  id_rsa
  id_rsa.pub

Both of these files were modified on 2010-01-04 17:56:08 CET. These files are key-based logins which allow a more secure way of connecting between different machines than password-based authentication. The date of modification means therefore that they were created at that time.

2. “links” directory contains:
Multiple .mp3 files
Multiple .gif files - which are shown as deleted
One README file - which is shown as deleted
All these files were modified 2010-01-04 between 17:56:10 CET and 17:58:15 CET. The examiner has found that all these files were created during a very short 2 minutes window, which might cause traffic.

3. “.bash_history” file was modified 2010-01-04 17:56:13 CET. 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 by Kevin, which are visible in the “.bash_hisotry” file. Kevin entered several commands, where the examiner explains the flow of the commands as follows:

Kevin created a music directory and viewed a quick summary of every user that logged into the computer. He printed the user information to the console output and after that opened the music directory. After that, Kevin looked at what files are within the music directory and used the command “crontab -l” →
The crontab (short for "cron table") is a list of commands that are scheduled to run at regular time intervals on the computer system. The crontab command opens the crontab for editing and allows to add, remove, or modify scheduled tasks. Furthermore, Kevin used the commands: “echo "0 4 * * * rsync -aq --del --rsh="ssh" -e "ssh -l kevin" "kevin.dynip.com:My_Music/" "~/music"" | crontab -” → which is a command to synchronize music at the 4th hour of the day, in other words, at 4 a.m. Afterward, Kevin viewed which processes were currently running on the computer, generated his ssh keys, and created the links directory. Kevin used the command “find ../music -exec ln -s {} \;” → which searches for a directory tree of a file system and creates a hard link between files. A hard link creates an exact copy of a file → which explains why the .mp3 files are in the links directory and why it was modified on the 2010-01-04 even though the synchronization at 4 a.m. was scheduled for the music directory. Kevin later used commands to remove all .gif files and also the README file from the links directory and logs out of the system.

The other three files which show no activity are .bash_logout .bashrc .profile

- Peter

  No activity

- Takeda

  Takeda's account shows 5 files, and 1 directory, where 2 files and 1 directory were modified on 2010-01-04. The files which show the stated activity are: .bash_history and eggdrop1.6.19. And the directory eggdrop. Modified were in total 3, explained as follows:

  1. "eggdrop" directory → modified on 2010-01-04 17:58:14 CET, which means that it was extracted at the specified time. Eggdrop is the most advanced IRC robot available. An IRC bot is a set of scripts or an independent program that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. An IRC bot differs from a regular client in that instead of providing interactive access to IRC for a human user, it performs automated functions.

  2. "eggdrop1.6.19" file was deleted at 2010-01-04 18:00:25 CET.

  3. ".bash_history" file was modified 2010-01-04
  During the analysis of the file .bash_history the examiner has found that it was modified on 2010-01-04 17:58:15 CET. 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 by Takeda, which are visible in the ".bash_hisotry" file. Takeda entered several commands, where the examiner explains the flow of the commands as follows:

  First, Takeda views the current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes. Furthermore, Takeda also prints the name, version and other specifications about the operating system, and displays information about all network interfaces currently in operation. With the command "tar xzf eggdrop1.6.19+ctcpfix.tar.gz" Takeda extracts / uncompresses the tar file to the eggdrop1.6.19 folder and enters the specified folder. Meaning of the commands "./configure" "make" and "make install" → The configure script is responsible for getting ready to build the software on a specific system and makes sure all of the dependencies for the rest of the build and install process are available. "make" is used to build the software. This runs a series of tasks defined in a Makefile to build the finished program from its source code. Now that the software is built and ready to run, the files can be copied to their final destinations. The make install command will copy the built program, and its libraries and documentation, to the correct locations. The command "find

eggdrop1.6.19 -delete” removes / deletes the eggdrop1.6.19 and after that Takeda logs out.

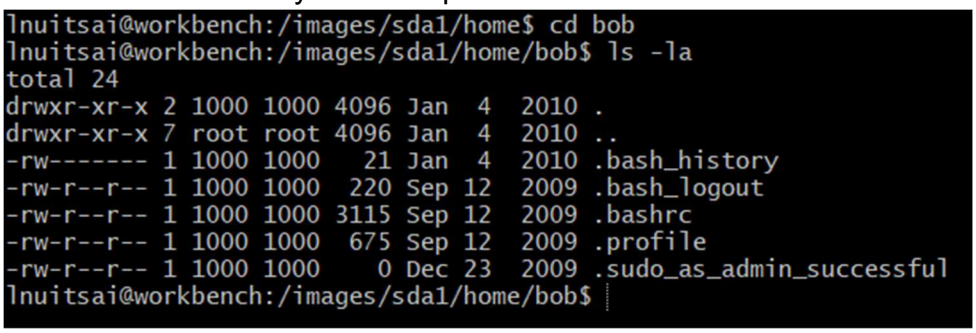
Conclusion

After running the “chkrootkit” - which is a common security scanner - the output indicated that the system is not infected. Furthermore, after examining all the users' history of commands, the conclusion is that the system is not infected and the huge spike in Internet traffic which occurred at 4 in the morning was caused by Kevin's command to synchronize music at the 4th hour of the day, in other words, at 4 a.m.

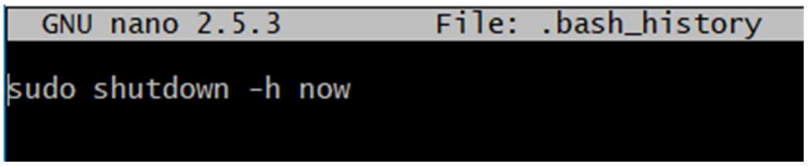
Exhibits/Appendices

Users files and .bash_history of commands

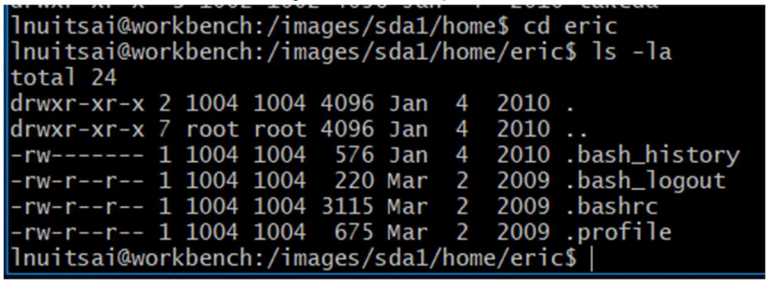
Bob’s files with activity timestamps:



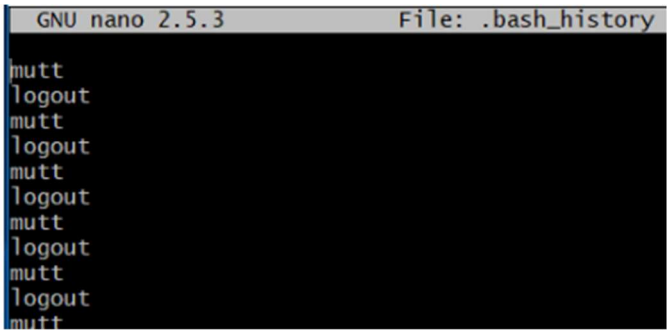
Bob’s .bash_history with executed commands:



Eric’s files with activity timestamps:



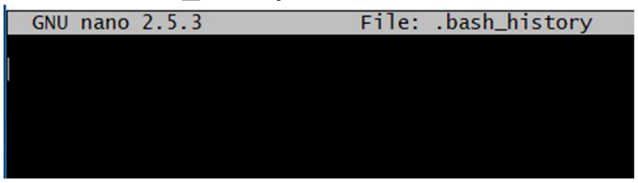
Eric’s .bash_history with executed commands:



Peter's files with activity timestamps:

```
lnuitsai@workbench:/images/sda1/home$ cd peter
lnuitsai@workbench:/images/sda1/home/peter$ ls -la
total 20
drwxr-xr-x 2 1001 1001 4096 Jan  4  2010 .
drwxr-xr-x 7 root root 4096 Jan  4  2010 ..
-rw-r--r-- 1 1001 1001  220 Mar  2  2009 .bash_logout
-rw-r--r-- 1 1001 1001 3115 Mar  2  2009 .bashrc
-rw-r--r-- 1 1001 1001  675 Mar  2  2009 .profile
lnuitsai@workbench:/images/sda1/home/peter$
```

Peter's .bash_history with executed commands:



Kevin's files with activity timestamps:

```
lnuitsai@workbench:/images/sda1/home$ cd kevin
lnuitsai@workbench:/images/sda1/home/kevin$ ls -la
total 36
drwxr-xr-x 5 1003 1003 4096 Jan  4  2010 .
drwxr-xr-x 7 root root 4096 Jan  4  2010 ..
-rw------- 1 1003 1003  337 Jan  4  2010 .bash_history
-rw-r--r-- 1 1003 1003  220 Mar  2  2009 .bash_logout
-rw-r--r-- 1 1003 1003 3115 Mar  2  2009 .bashrc
drwxr-xr-x 2 1003 1003 4096 Jan  4  2010 links
drwxr-xr-x 2 1003 1003 4096 Jan  1  2010 music
-rw-r--r-- 1 1003 1003  675 Mar  2  2009 .profile
drwx------ 2 1003 1003 4096 Jan  4  2010 .ssh
lnuitsai@workbench:/images/sda1/home/kevin$
```

Kevin's .bash_history with executed commands:

```
 GNU nano 2.5.3                File: .bash_history

mkdir music
logout
w
id
ls -al
cd music
ls
cd ..
crontab -l
echo "0 4 * * * rsync -aq --del --rsh="ssh" -e "ssh -l kevin" "kevin.dynip.com:$
crontab -l
ps x
ssh-keygen
cat .ssh/id_rsa.pub
logout
mkdir links
cd links
find ../music -exec ln -s {} \;
ls
logout
cd links
ls -l
rm *.gif
ls -l
rm README
logout
```

Takeda's files with activity timestamps:

```
lnuitsai@workbench:/images/sda1/home$ cd takeda
lnuitsai@workbench:/images/sda1/home/takeda$ ls -la
total 1036
drwxr-xr-x  3 1002 1002    4096 Jan  4  2010 .
drwxr-xr-x  7 root root    4096 Jan  4  2010 ..
-rw-------  1 1002 1002     199 Jan  4  2010 .bash_history
-rw-r--r--  1 1002 1002     220 Mar  2  2009 .bash_logout
-rw-r--r--  1 1002 1002    3115 Mar  2  2009 .bashrc
drwxr-xr-x 10 1002 1002    4096 Jan  4  2010 eggdrop
-rw-r--r--  1 1002 1002 1024745 Jan  1  2010 eggdrop1.6.19+ctcpfix.tar.gz
-rw-r--r--  1 1002 1002     675 Mar  2  2009 .profile
lnuitsai@workbench:/images/sda1/home/takeda$
```

Takeda's .bash_history with executed commands:

```
 GNU nano 2.5.3                File: .bash_history

uptime
uname -a
fgrep takeda /etc/passwd
ifconfig
irssi
logout
tar xzf eggdrop1.6.19+ctcpfix.tar.gz
cd eggdrop1.6.19
./configure
make config
make
make install
cd ..
find eggdrop1.6.19 -delete
logout
```

Activity log - auth.log file

Latest activity performed on 2010-01-04 by the different users:

```
  GNU nano 2.5.3                    File: auth.log

Jan  4 08:55:46 server sshd[2208]: pam_unix(sshd:session): session closed for user bob
Jan  4 08:55:47 server sshd[2375]: Accepted password for kevin from 192.168.56.1 port 42660 ssh2
Jan  4 08:55:47 server sshd[2375]: pam_unix(sshd:session): session opened for user kevin by (uid=0)
Jan  4 08:56:03 server sshd[2375]: pam_unix(sshd:session): session closed for user kevin
Jan  4 08:56:04 server sshd[2392]: Accepted password for takeda from 192.168.56.1 port 42661 ssh2
Jan  4 08:56:04 server sshd[2392]: pam_unix(sshd:session): session opened for user takeda by (uid=0)
Jan  4 08:56:05 server sshd[2392]: pam_unix(sshd:session): session closed for user takeda
Jan  4 08:56:06 server sshd[2409]: Accepted password for kevin from 192.168.56.1 port 42662 ssh2
Jan  4 08:56:06 server sshd[2409]: pam_unix(sshd:session): session opened for user kevin by (uid=0)
Jan  4 08:56:06 server sshd[2411]: Accepted password for takeda from 192.168.56.1 port 42663 ssh2
Jan  4 08:56:06 server sshd[2411]: pam_unix(sshd:session): session opened for user takeda by (uid=0)
Jan  4 08:56:06 server sshd[2412]: Accepted password for eric from 192.168.56.1 port 42664 ssh2
Jan  4 08:56:06 server sshd[2412]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:08 server sshd[2411]: pam_unix(sshd:session): session closed for user takeda
Jan  4 08:56:08 server sshd[2412]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:08 server sshd[2409]: pam_unix(sshd:session): session closed for user kevin
Jan  4 08:56:09 server sshd[2531]: Accepted password for takeda from 192.168.56.1 port 42665 ssh2
Jan  4 08:56:09 server sshd[2531]: pam_unix(sshd:session): session opened for user takeda by (uid=0)
Jan  4 08:56:09 server sshd[2533]: Accepted password for eric from 192.168.56.1 port 42666 ssh2
Jan  4 08:56:09 server sshd[2533]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:09 server sshd[2552]: Accepted password for kevin from 192.168.56.1 port 42667 ssh2
Jan  4 08:56:09 server sshd[2552]: pam_unix(sshd:session): session opened for user kevin by (uid=0)
Jan  4 08:56:10 server sshd[2533]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:11 server sshd[2552]: pam_unix(sshd:session): session closed for user kevin
Jan  4 08:56:11 server sshd[2804]: Accepted password for eric from 192.168.56.1 port 42668 ssh2
Jan  4 08:56:11 server sshd[2804]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:12 server sshd[2804]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:12 server sshd[2905]: Accepted password for kevin from 192.168.56.1 port 42669 ssh2
Jan  4 08:56:12 server sshd[2905]: pam_unix(sshd:session): session opened for user kevin by (uid=0)
Jan  4 08:56:13 server sshd[2905]: pam_unix(sshd:session): session closed for user kevin
Jan  4 08:56:13 server sshd[3003]: Accepted password for eric from 192.168.56.1 port 42670 ssh2
Jan  4 08:56:13 server sshd[3003]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:14 server sshd[3003]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:15 server sshd[3217]: Accepted password for eric from 192.168.56.1 port 42671 ssh2
Jan  4 08:56:15 server sshd[3217]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:16 server sshd[3217]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:17 server sshd[3456]: Accepted password for eric from 192.168.56.1 port 42672 ssh2
Jan  4 08:56:17 server sshd[3456]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:18 server sshd[3456]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:19 server sshd[3675]: Accepted password for eric from 192.168.56.1 port 42673 ssh2
Jan  4 08:56:19 server sshd[3675]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:20 server sshd[3675]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:21 server sshd[3871]: Accepted password for eric from 192.168.56.1 port 42674 ssh2
Jan  4 08:56:21 server sshd[3871]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:22 server sshd[3871]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:23 server sshd[4093]: Accepted password for eric from 192.168.56.1 port 42675 ssh2
Jan  4 08:56:23 server sshd[4093]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:23 server sshd[4093]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:25 server sshd[4296]: Accepted password for eric from 192.168.56.1 port 42676 ssh2
Jan  4 08:56:25 server sshd[4296]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:25 server sshd[4296]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:26 server sshd[4525]: Accepted password for eric from 192.168.56.1 port 42677 ssh2
```

```
Jan  4 08:56:26 server sshd[4525]: Accepted password for eric from 192.168.56.1 port 42677 ssh2
Jan  4 08:56:27 server sshd[4525]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:27 server sshd[4525]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:28 server sshd[4750]: Accepted password for eric from 192.168.56.1 port 42678 ssh2
Jan  4 08:56:28 server sshd[4750]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:29 server sshd[4750]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:30 server sshd[4975]: Accepted password for eric from 192.168.56.1 port 42679 ssh2
Jan  4 08:56:30 server sshd[4975]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:31 server sshd[4975]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:32 server sshd[5205]: Accepted password for eric from 192.168.56.1 port 42680 ssh2
Jan  4 08:56:32 server sshd[5205]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:33 server sshd[5205]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:34 server sshd[5417]: Accepted password for eric from 192.168.56.1 port 42681 ssh2
Jan  4 08:56:34 server sshd[5417]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:35 server sshd[5417]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:36 server sshd[5599]: Accepted password for eric from 192.168.56.1 port 42682 ssh2
Jan  4 08:56:36 server sshd[5599]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:37 server sshd[5599]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:38 server sshd[5815]: Accepted password for eric from 192.168.56.1 port 42683 ssh2
Jan  4 08:56:38 server sshd[5815]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:39 server sshd[5815]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:40 server sshd[6040]: Accepted password for eric from 192.168.56.1 port 42684 ssh2
Jan  4 08:56:40 server sshd[6040]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:41 server sshd[6040]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:42 server sshd[6263]: Accepted password for eric from 192.168.56.1 port 42685 ssh2
Jan  4 08:56:42 server sshd[6263]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:43 server sshd[6263]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:44 server sshd[6486]: Accepted password for eric from 192.168.56.1 port 42686 ssh2
```

```
Jan  4 08:56:43 server sshd[6263]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:44 server sshd[6486]: Accepted password for eric from 192.168.56.1 port 42686 ssh2
Jan  4 08:56:44 server sshd[6486]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:45 server sshd[6486]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:46 server sshd[6703]: Accepted password for eric from 192.168.56.1 port 42687 ssh2
Jan  4 08:56:46 server sshd[6703]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:46 server sshd[6703]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:48 server sshd[6888]: Accepted password for eric from 192.168.56.1 port 42688 ssh2
Jan  4 08:56:48 server sshd[6888]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:49 server sshd[6888]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:50 server sshd[7129]: Accepted password for eric from 192.168.56.1 port 42689 ssh2
Jan  4 08:56:50 server sshd[7129]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:51 server sshd[7129]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:52 server sshd[7364]: Accepted password for eric from 192.168.56.1 port 42690 ssh2
Jan  4 08:56:52 server sshd[7364]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:53 server sshd[7364]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:54 server sshd[7639]: Accepted password for eric from 192.168.56.1 port 42691 ssh2
Jan  4 08:56:54 server sshd[7639]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:55 server sshd[7639]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:56 server sshd[7957]: Accepted password for eric from 192.168.56.1 port 42692 ssh2
Jan  4 08:56:56 server sshd[7957]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:57 server sshd[7957]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:56:58 server sshd[8282]: Accepted password for eric from 192.168.56.1 port 42693 ssh2
Jan  4 08:56:58 server sshd[8282]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:56:59 server sshd[8282]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:01 server sshd[8487]: Accepted password for eric from 192.168.56.1 port 42694 ssh2
Jan  4 08:57:01 server sshd[8487]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:02 server sshd[8487]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:03 server sshd[8678]: Accepted password for eric from 192.168.56.1 port 42695 ssh2
```

```
Jan  4 08:57:03 server sshd[8678]: Accepted password for eric from 192.168.56.1 port 42695 ssh2
Jan  4 08:57:03 server sshd[8678]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:04 server sshd[8678]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:05 server sshd[8882]: Accepted password for eric from 192.168.56.1 port 42696 ssh2
Jan  4 08:57:05 server sshd[8882]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:06 server sshd[8882]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:07 server sshd[9087]: Accepted password for eric from 192.168.56.1 port 42697 ssh2
Jan  4 08:57:07 server sshd[9087]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:08 server sshd[9087]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:09 server sshd[9373]: Accepted password for eric from 192.168.56.1 port 42698 ssh2
Jan  4 08:57:09 server sshd[9373]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:10 server sshd[9373]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:12 server sshd[9605]: Accepted password for eric from 192.168.56.1 port 42699 ssh2
Jan  4 08:57:12 server sshd[9605]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:13 server sshd[9605]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:14 server sshd[9778]: Accepted password for eric from 192.168.56.1 port 42700 ssh2
Jan  4 08:57:14 server sshd[9778]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:15 server sshd[9778]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:16 server sshd[10043]: Accepted password for eric from 192.168.56.1 port 42701 ssh2
Jan  4 08:57:16 server sshd[10043]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:17 server sshd[10043]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:18 server sshd[10141]: Accepted password for eric from 192.168.56.1 port 42702 ssh2
Jan  4 08:57:18 server sshd[10141]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:20 server sshd[10141]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:21 server sshd[10183]: Accepted password for eric from 192.168.56.1 port 42703 ssh2
Jan  4 08:57:21 server sshd[10183]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:22 server sshd[10183]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:23 server sshd[10225]: Accepted password for eric from 192.168.56.1 port 42704 ssh2
```

```
Jan  4 08:57:23 server sshd[10225]: Accepted password for eric from 192.168.56.1 port 42704 ssh2
Jan  4 08:57:23 server sshd[10225]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:24 server sshd[10225]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:25 server sshd[10264]: Accepted password for eric from 192.168.56.1 port 42705 ssh2
Jan  4 08:57:25 server sshd[10264]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:26 server sshd[10264]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:28 server sshd[10309]: Accepted password for eric from 192.168.56.1 port 42706 ssh2
Jan  4 08:57:28 server sshd[10309]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:29 server sshd[10309]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:30 server sshd[10357]: Accepted password for eric from 192.168.56.1 port 42707 ssh2
Jan  4 08:57:30 server sshd[10357]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:31 server sshd[10357]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:32 server sshd[10402]: Accepted password for eric from 192.168.56.1 port 42708 ssh2
Jan  4 08:57:32 server sshd[10402]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:33 server sshd[10402]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:34 server sshd[10450]: Accepted password for eric from 192.168.56.1 port 42709 ssh2
Jan  4 08:57:34 server sshd[10450]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:36 server sshd[10450]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:37 server sshd[10492]: Accepted password for eric from 192.168.56.1 port 42710 ssh2
Jan  4 08:57:37 server sshd[10492]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:38 server sshd[10492]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:39 server sshd[10534]: Accepted password for eric from 192.168.56.1 port 42711 ssh2
Jan  4 08:57:39 server sshd[10534]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:40 server sshd[10534]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:41 server sshd[10581]: Accepted password for eric from 192.168.56.1 port 42712 ssh2
Jan  4 08:57:41 server sshd[10581]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:43 server sshd[10581]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:44 server sshd[10655]: Accepted password for eric from 192.168.56.1 port 47410 ssh2
```

```
Jan  4 08:57:44 server sshd[10655]: Accepted password for eric from 192.168.56.1 port 47410 ssh2
Jan  4 08:57:44 server sshd[10655]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:45 server sshd[10655]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:57:46 server sshd[10717]: Accepted password for eric from 192.168.56.1 port 47411 ssh2
Jan  4 08:57:46 server sshd[10717]: pam_unix(sshd:session): session opened for user eric by (uid=0)
Jan  4 08:57:47 server sshd[10717]: pam_unix(sshd:session): session closed for user eric
Jan  4 08:58:15 server sshd[2531]: pam_unix(sshd:session): session closed for user takeda
Jan  4 09:00:01 server CRON[11303]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan  4 09:00:01 server CRON[11305]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan  4 09:00:01 server CRON[11303]: pam_unix(cron:session): session closed for user root
Jan  4 09:00:03 server CRON[11305]: pam_unix(cron:session): session closed for user root
Jan  4 09:00:19 server login[2207]: pam_unix(login:session): session opened for user bob by LOGIN(uid$
Jan  4 09:00:25 server sudo:      bob : TTY=tty1 ; PWD=/home/bob ; USER=root ; COMMAND=/sbin/shutdown$
```