Assignment Report 3

|  |
| --- |
|  |

*Author:* Ruth Dirnfeld

*Department and Organization:* Linnaeus University

*Investigation Number.* 003

*Report Date:* 2019-05-07



[Executive Summary 3](#_Toc9862723)

[Methodology 4](#_Toc9862724)

[Report Findings 4](#_Toc9862725)

[● Chef 4](#_Toc9862726)

[● Gardener 5](#_Toc9862727)

[● Jeeves 5](#_Toc9862728)

[● Rich 6](#_Toc9862729)

[● Ubuntu 7](#_Toc9862730)

[● auth.log 7](#_Toc9862731)

[● Keyword search 7](#_Toc9862732)

[● Deleted files recovery 7](#_Toc9862733)

[Conclusion 8](#_Toc9862734)

[Prevention 9](#_Toc9862735)

[Exhibits/Appendices 9](#_Toc9862736)

[Users files and .bash\_history of commands 9](#_Toc9862737)

[● Chef 9](#_Toc9862738)

[● Gardener 10](#_Toc9862739)

[● Jeeves 10](#_Toc9862740)

[● Rich 11](#_Toc9862741)

[● Ubuntu 12](#_Toc9862742)

[Activity log - auth.log file 13](#_Toc9862743)

[● Keyword search 14](#_Toc9862744)

[● Deleted files recovery 15](#_Toc9862745)

[● Decrypted solutions 18](#_Toc9862746)

## Executive Summary

A British butler handed over the biggest diamond-encrusted hard drive anyone has ever seen. Now, it's a fundamental truth that money attracts crooks like Martians attract germs, so he said that his employer's computer had recently been broken into. What *was* surprising was the M.O. -- the crooks deleted the boss' files to show they were serious, and then they encrypted his Swiss bank account access codes and held the decryption keys ransom for 1 megabucks.

The boss needs the access codes to do business, but he doesn't want to cave in, either. At this point, he doesn't care about his computer, and he doesn't particularly care how they got in. He's just hoping that there is a way to decrypt the codes so he doesn't have to pay those lowlifes.

The purpose of the examination is to find the decryption keys. This has the highest priority. Secondly, the examination will be performed to try and find out who is responsible for deleting the files and encryption of the bank account access codes. Furthermore, the examiner's professional recommendation as to what needs to be done to avoid this situation in the future can be viewed at the end of this report.

The following account files are on the machine: 'chef', 'gardener', 'jeeves', 'rich', and ‘ubuntu’.

The examined image file shows the following major findings:

1. Under the user “rich” files, the “swiss\_keys” directory contains the encrypted eight swisskeys with the “.gpg” extension, to which the decryption keys need to be found.

2. Under the user “rich” files, two of the eight decryption keys were found:

key4: 11hibiscus2hibiscus23 within “.extrtmtc” directory

key5: 19rose42blossom35 within “.mozilla/cache/a234Z8x0

3. By performing a key word search with the autopsy software the keys 1, 2, and 3 were found as follows:

key1: 23philo7dendron88

key2: 41jade6tree29p

key2: 41jade6tree29~~~

key3: 29azalea8flower00

4. Three decryption keys were found under the name “1001” when recovering deleted files. The keys found here are:

key6: 13tulip34root28

key7: 17jonquil23scent14

key8: 26daisy99daisy99

5. When using the decryption keys on the .gpg swisskeys the solutions are as follows:

1. me\_and\_you\_and\_you\_and\_me-so\_happy\_2gether

2. everybody\_dance\_now\_hey\_now

3. what\_would\_you\_do\_if\_sang\_out\_of\_tune

4. im\_pickin\_up\_good\_vibrations

5. its\_the\_little\_old\_lady\_from\_pasadena

6. raindrops\_keep\_fallin\_on\_my\_head

7. twist\_again\_like-we\_did\_last\_summer

8. goodness\_gracious\_great\_balls\_of\_fire

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 and autopsy. This allowed the examiner to browse through the different directories and files within a User Interface and view different files and time stamps more easily.

## 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 PT: Pacific Time since the file “timezone” in the “etc” folder shows that it is set to the timezone in the US/Pacific. The analysis was performed on all users since it was found that the users don’t have countless files.

The users 'chef', 'gardener', 'jeeves', and ‘ubuntu’ have a bash history, where all bash histories are attached in the Exhibits/Appendix section:

### Chef

Chef’s account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:51 and 07:28:04 PT explained as follows:

1. “recipes” directory contains the file “bread” which was modified 2007-09-10 07:27:21 PT. This file contains the text “best bread recipe:”

2. “.bash\_history” file

During the analysis of the file .bash\_history the examiner has found that it was modified on 2007-09-10 07:28:04 PT with the commands attached in the Appendix section and explained as:

First, the chef created the recipes directory and then he used the echo command to display line of text/string that is passed as an argument.

The other three files are .bashrc .bash\_logout and .bash\_profile

### Gardener

Gardener’s account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:38 and 07:27:55 PT explained as follows:

1. “.gnupg” directory contains the files: “gpg.conf” “pubring.gpg” “secring.gpg”

2. “.bash\_history” file

During the analysis of the file .bash\_history the examiner has found that it was modified on 2007-09-10 07:28:04 PT with the commands attached in the Appendix section and explained as:

**Explanation:**

First, he views the current opened processes and also processes for all users. Then he uses the gpg command which is used to secure most sensitive files on Linux systems.

“.gnupg” directory: GnuPG (also known as GPG) is a program that encrypts and signs files. This directory contains a lot of private information, so it's accessible only to the owner.

The other three files are .bashrc .bash\_logout and .bash\_profile

### Jeeves

Jeeves’ account shows 1 directory and 4 files and all files show a modified stamp on the 2007-09-10 between 05:05:17 and 07:38:43 PT explained as follows:

1. “housekeepers” directory is an empty directory.

2. “.bash\_history” file

During the analysis of the file .bash\_history the examiner has found that it was modified on 2007-09-10 07:38:43 PT with the commands attached in the Appendix section and explained as:

**Explanation:**

First, with the command “w” he views a quick summary of every user logged into a computer, what each user is currently doing, and what load all the activity is imposing on the computer itself. He uses the “watch” command to repeatedly display the results on the standard output. Then he asks the system to start a new login session for the “rich” user and views his .bash\_history file, and logs in as root user.

The other three files are .bashrc .bash\_logout and .bash\_profile

### Rich

Rich’s account shows 6 directory and54 files and all files show a modified stamp on the 2007-09-10 between 01:58:05 and 07:32:14 PT explained as follows:

1. “.extrtmtc” directory contains the following:

“key4” file

The “key4” file contains the entry: 4 11hibiscus2hibiscus23

2. “.gnupg” directory contains the following files: “gpg.conf” “pubring.gpg” “random\_seed”

3. “.mozilla” directory contains the following:

“cache” directory, which contains a file with the name “a234Z8x0” which has the following entry: 5 19rose42blossom35

4. “swiss\_keys” directory contains 8 files:

“swisskey1.gpg” “swisskey2.gpg” “swisskey3.gpg” “swisskey4.gpg” “swisskey5.gpg” “swisskey6.gpg” “swisskey7.gpg” “swisskey8.gpg”

5. “.games” and “.thunderbird” directories are empty directories

The other five files are .bashrc .bash\_logout .bash\_profile .lesshst and .viminfo

**Explanation:**

Point numbers 1 and 3 contain two of the eight decryption keys, namely key number four and key number five. The keys are as follows:

* 11hibiscus2hibiscus23
* 19rose42blossom35

The “swiss\_keys” directory contains the encrypted eight swisskeys, to which the decryption keys need to be found.

### Ubuntu

Ubuntu’s account shows 6 files and all files show a modified stamp on the 2007-09-10 between 01:13:06 and 18:38:48 PT explained as follows:

During the analysis of the file .bash\_history the examiner has found that it was modified on 2007-09-10 02:05:48 PT with the commands attached in the Appendix section and explained as:

**Explanation:**

First, the “sources.list” file in the “etc/apt” directory is viewed and, afterward, an intelligent upgrade is performed. Then, the command “sudo shutdown -r now” means that the system is shutdown right away, and with the “-r” it also reboots itself.

The other five files are .bashrc .bash\_logout .bash\_profile .sudo\_as\_admin\_successful and .viminfo

### auth.log

All activity is local - coming from local IP addresses, such as: 10.10.10.100 Also shows which user was logged in at what time.

### Keyword search

The examiner used autopsy for a keyword search to look for some of the decryption keys. By entering the words “key” and one of the numbers between 1 and 8. This key word was entered in the combination with or without a space, example as follows: “key1” or “key 1” was entered when searching for the first key. With this search, the following keys were found:

key1: 23philo7dendron88

key2: 41jade6tree29p

key2: 41jade6tree29~~~

key3: 29azalea8flower00

Screenshots of the individual files can be viewed in the Apeendix section.

### Deleted files recovery

After analyzing all users, the auth.log file, and various directories and files, the examiner found 2846 deleted files. Five of these files were under the directory “1001” and the rest under the “root”. By looking at the easier choice → the five files contained three keys (key6, key7, key8) and one bash history.

key6: 13tulip34root28

key7: 17jonquil23scent14

key8: 26daisy99daisy99

.bash\_history analysis:

First, the directories “.mozilla” “.thudnerbird” and ‘.games” are created. Then he downloads the key encrypter and changes access with the command chmod which is used to change the access permissions of file system objects (files and directories). Then all eight swiss keys are encrypted symmetrically, meaning that the same key is used to both encrypt and decrypt a file. To encrypt a file with minimal effort, a command like this is used. After every symmetric encryption, each file is shredded, meaning that the “shred” command is used every time to securely remove the original file.

## Conclusion

As stated already in the Executive Summary section, it is clear that the hard drive was compromised. The task was to find at least 6 out of totally 8 decryption keys since the hacker used symmetric encryption. The examiner has found the following 8 keys and got the following solutions when using the keys:

* Key1 : 23philo7dendron88

→ me\_and\_you\_and\_you\_and\_me-so\_happy\_2gether

* Key 2: 41jade6tree29p

→ everybody\_dance\_now\_hey\_now

* Key 3: 29azalea8flower00

→ what\_would\_you\_do\_if\_sang\_out\_of\_tune

* Key 4: 11hibiscus2hibiscus23

→ im\_pickin\_up\_good\_vibrations

* Key 5: 19rose42blossom35

→ its\_the\_little\_old\_lady\_from\_pasadena

* Key 6: 13tulip34root28

→ raindrops\_keep\_fallin\_on\_my\_head

* Key 7: 17jonquil23scent14

→ twist\_again\_like-we\_did\_last\_summer

* Key 8: 26daisy99daisy99

→ goodness\_gracious\_great\_balls\_of\_fire

No clear evidence was found on who encrypted the swisskeys, but from the Report findings one might assume that the Gardener and Jeeves both had very interesting commands in their .bash\_hisotry. Jeeves started the session as root and rich, where later rich encrypted all swisskeys and as for the Gardener, his interesting commands include using the gpg command and having the setting files for gnupg. But as already mentioned, no clear evidence was found on who encrypted the swisskeys.

## Prevention

Some recommendations on how to prevent a similar situation in the future and how to protect a computer against file-encryption:

* Install preventive software which would block external access to the computer.
* Do not open attachments in emails from unknown senders as these emails might be ransomware that encrypts one's files.
* Keep the operating system, anti-virus software, and other applications always up-to-date. This improves existing features as well as adds new ones.
* Back up files to an external hard drive or to the cloud. In case the files are encrypted, you have less to worry since the files are all backed up.
* Have a strong password - In general, a strong password contains at least 12 characters and includes numbers, symbols, capital letters, and lower-case letters.

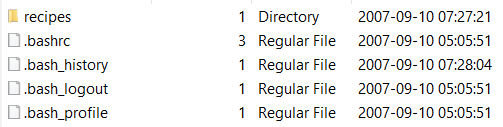
## 

## Exhibits/Appendices

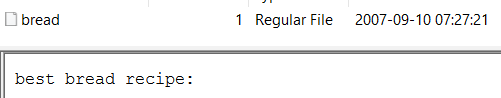
### Users files and .bash\_history of commands

#### Chef

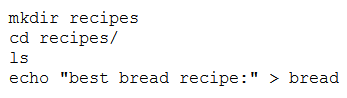
**Chef’s files:**

****

**Chef’s files inside “recipes” directory:**

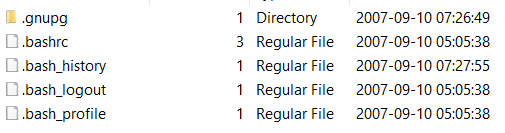
****

**Chef’s .bash\_history:**

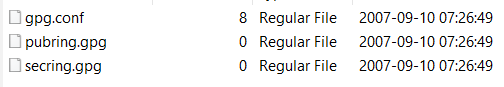
****

#### Gardener

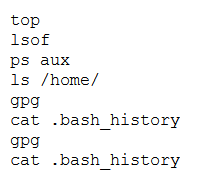
**Gardener’s files:**

****

**Gardener’s files inside .gnupg directory:**

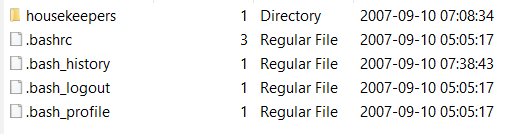
****

**Gardener’s .bash\_history:**

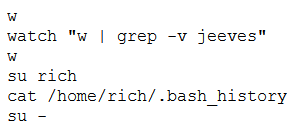
****

#### Jeeves

**Jeeves’ files:**

****

**Jeeves’ .bash\_history:**

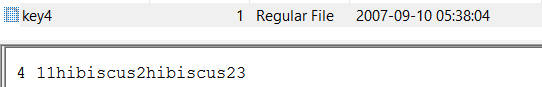


#### Rich

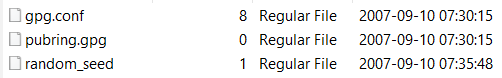
**Rich’s files:**



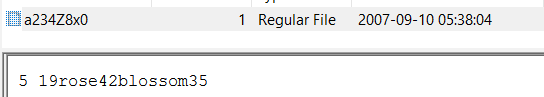
**Rich’s files inside “extrtmtc” directory:**

****

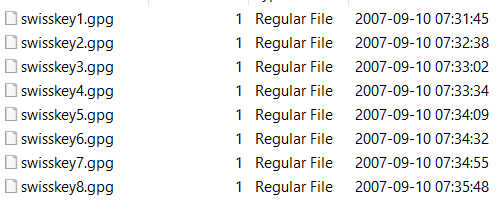
**Rich’s files inside “gnupg” directory:**

****

**Rich’s files inside “mozilla” inside “cache” directory:**

****

**Rich’s files inside “swiss\_keys” directory:**

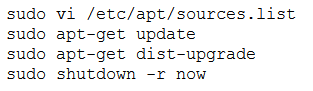
****

#### Ubuntu

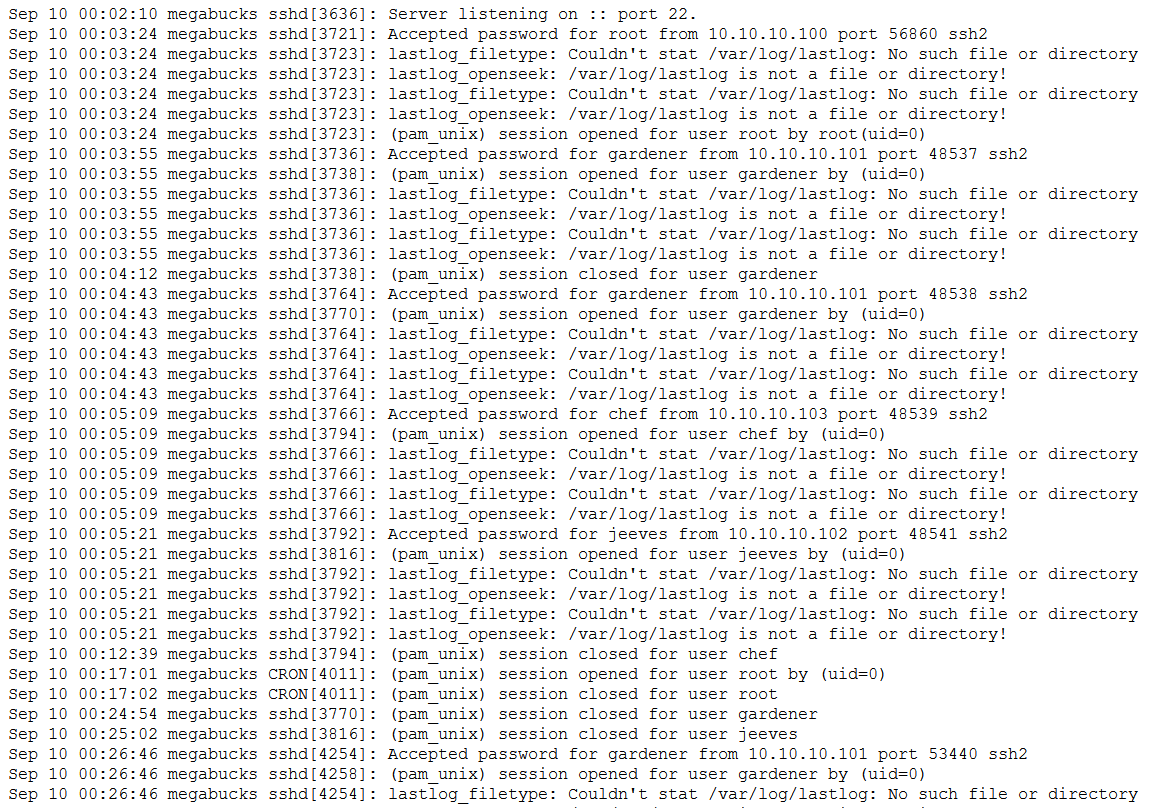
**Ubuntu’s files:**

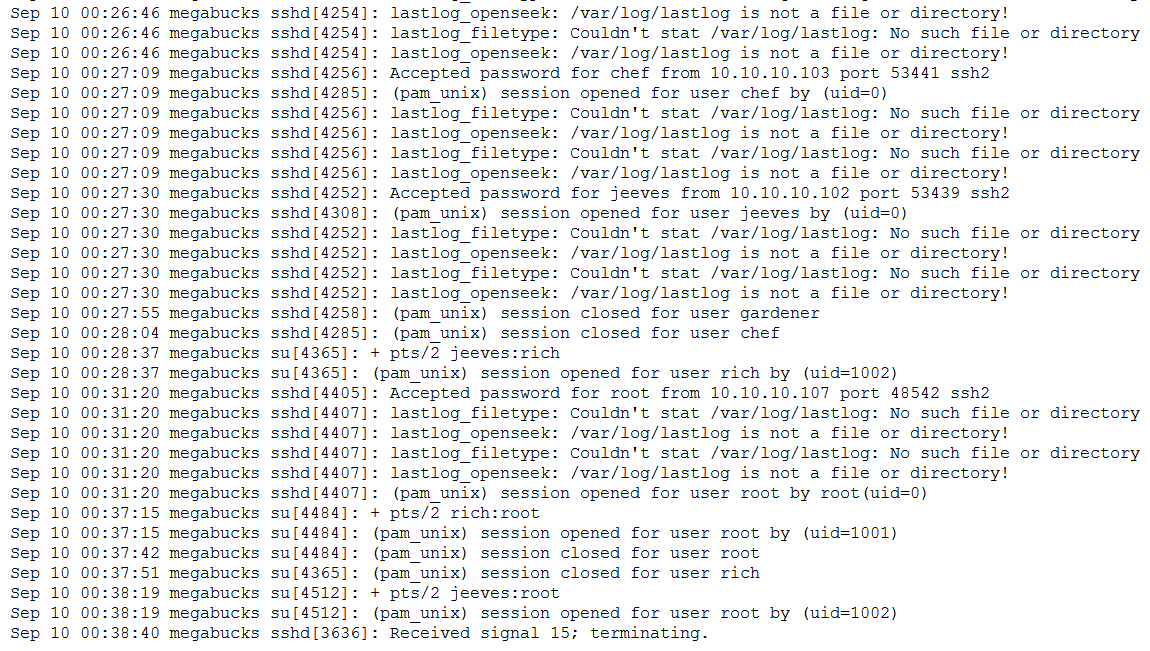
****

**Ubuntu’s .bash\_history:**



### Activity log - auth.log file





### Keyword search

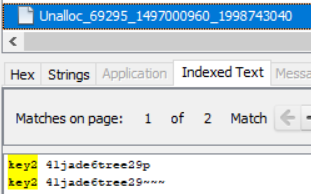
How to search:



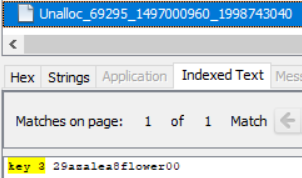
Key1:



Key2:

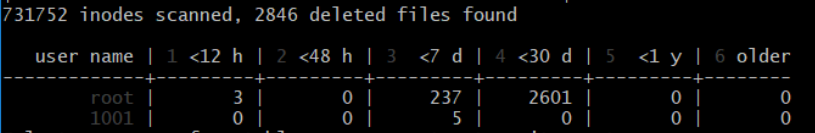


Key3:



### Deleted files recovery

2846 deleted files, where “1001” contains 5 and “root” contains the rest:



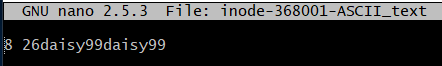
Key number 6:



Key number 7:

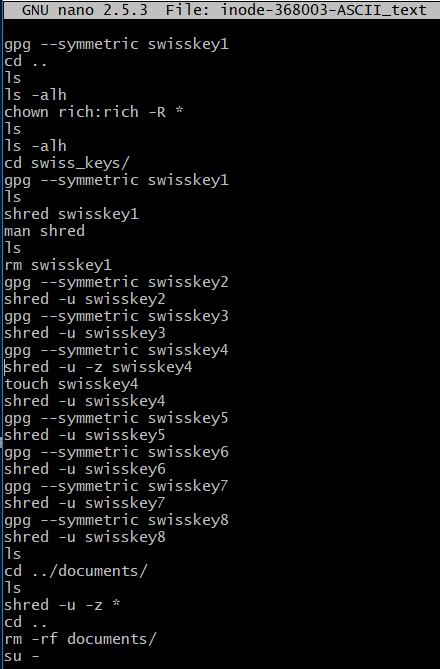


Key number 8:



Recovered .bash\_history:





Symmetric encryption/decryption and deleting (“shred”) existing swisskeys

### Decrypted solutions















