INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab2

Group number:	35	Name	IST Number
Student 1:		Rodrigo Leal Saraiva Ganância	103809
Student 2:		Pedro Miguel de Melo Ribeiro	102663
Student 3:		Diogo José Almeida Rodrigues	102848

1 Acquired artifacts

Name	Type	SHA-256 Value
andromeda.png	png	fcdd6ce7ae9a8f02c2ba3b2693d49848606b1ca5d332a076fe63013fcaa55ab2
best-intro.wav	wav	c3ea6b775dd7eaecebeef00e5523483d182602118ff6de0eb3d6a41b8f43c42f
cartwheel.tiff	tiff	f6861a315acb49b9c8ac18e9d6e92ed366e78f43bd2850d0f2a8f30f695aad45
lactea.jpg	jpg	326f3601ab7ad66fff2c43b3c5d4465d820dbf7381be65ab20c6adac2d1c10bb
nmap	elf	33da582bf8705b3a6818fa25d1f61ee339d46f58b8aedfdd951e1d4a915d582d
tagus.png	png	0b916d4d246372e07b1a6901585b632d8426a07b611fa4b1058341ef2a59f7b2
myzip.zip	zip	255a40424332be5b70c01c6301e05de6049b54ef2c7d2fb8551f0358866f5649
irssi_log.txt	txt	b19ce5156507851d206f7559ed67cb308d2b8b774f096296fcfee754cb98df82
bash_history.txt	txt	9a656b05678b07ac0f4aa7a0fd167ea528bd395893290e09244fbe0888103a44
Inbox.html	html	09e4094cf0f1bb51b120e5f9d24bf780a0b7876af8ea8fad033bf21afae1a009
syslog.txt	txt	21bd644a2359c064bbaae327e178930a9e83771916ab8f22cdf94ba4d4551baa

2 Report of all findings

We began by analyzing the "johnny" disk using the mmls command, which provided a detailed view of the partition layout. From this, we identified Johnny's Linux partition at position 005 with an offset of 4096. To examine the file system, we used the **fls -o 4096 command**, which pointed us to the inode for the home directory. After retrieving this inode, we ran the fls command again to list the files within the home directory, eventually locating the inode for the "johnnymusk" directory. We then proceeded to explore the contents of this folder.

Inside the home directory, we discovered a series of familiar files, such as background.png and tagus.png. However, these files were clean and did not contain any hidden data or embedded files. Additionally, we discovered a document containing a Master's thesis on Ariane 6's telemetry software, suggesting that Johnny had been actively researching this topic, which could be relevant to future investigation.

Bash History

By looking at the .bash_history file, which contains the history of the commands used by Johnny, we can see:

- He used the command irssi, a terminal based chat client, multiple times.
- There is evidence of him getting the hacked credentials from the downloads and hiding it with a doubleEncodingAndHidingInsideElf.py program, sending it to the sigma account and deleting it with the srm command.
- There is also evidence of him opening the discovered artifacts from the first investigation, hiding them using some python scripts he got from a eliteHackingTools-main.zip then sending them to the sigma account and deleting them with the srm command.

We can conclude that Johnny deliberately concealed and later deleted crucial evidence and artifacts relevant to this investigation.

IRSSI chat logs

Following what we discovered earlier, particularly the use of the irssi command, we wanted to see if we could get access to some message exchanges that could give us some lead. For this we decided to run the command **fls -o -Fr -o 4096 johnnyDisk | grep "irssi"** which gave us some logs. One of them with the name #basement was particularly relevant. Inside it we found a conversation between Johnny and someone called RootKitty where:

- RootKitty admits he stole the credentials from Técnico and sends them to Johnny Musk. They talk about hiding them from the authorities with a script they made together.
- Johnny Musk says that he received a strange email telling him to go get a USB pen from a hidden spot in Técnico. Apparently the pen contained all the documents we found alongside the credentials like the API to the MKUltra, the bank statement and the blueprint for ARIANE6. John mentions that he will organize a protest to try to prevent the usage of the mind control technology and both agree in hiding the information using some tactics they learned from CTF's.

The chat logs reveal that the individual known as RootKitty was responsible for stealing the passwords from the IST users. Additionally, they indicate that Johnny was not involved in the use of MKUltra; instead, he obtained the documents from someone else connected to the mind control scheme.

Syslog file

Through the analysis of the syslog file, we confirmed that Johnny had indeed plugged-in a USB drive. We used the command **fls -o 4096 -Fr johnnyDisk.img | grep syslog**, which revealed the file's inode as 274243. By running **icat -o 4096 johnnyDisk.img 274243 | grep usb**, we found a reference to the insertion of the device, identified by the serial number 9AD32EC0.

Thunderbird mail (Inbox.html)

We attempted to locate the previous email by running the command **fls -o -Fr -o 4096 johnnyDisk | grep "thunderbird"**. Upon reviewing the files, we found an "Inbox Mail" file containing all received emails. The email contents were encoded in base64, so we used the CyberChef tool (https://gchq.github.io/CyberChef/) to decode them. Among the emails was one from an anonymous sender, which Johnny Musk had mentioned to RootKitty, urging him to retrieve the USB drive. The anonymous sender, using the alias "somebodysupercool," stated that he had left the USB near Johnny's house on Av. Rovisco Pais 1, containing documents related to the MKUltra and Ariane-6 projects.

Stt Directory

Within the "stt" directory, we found a collection of Python programs and scripts that Johnny uses for security team activities, such as Capture the Flag (CTF) events. In addition to these, we also identified scripts that were used to conceal the artifacts discovered in our initial investigation:

- converter.py: This program reads a file, converts its content to binary, and then replaces 0's with spaces and 1's with dots.
- createChunks.py: This script splits a file into multiple chunks.

(These scripts were used to hide logs from the MKUltra API within the user comment section of galaxy images. The process involved first splitting the logs into three chunks, then converting the data to binary, with 0's replaced by spaces and 1's by dots)

- doubleEncodingAndHidingInsideElf.py: This script takes the hacked credentials file and converts it to hexadecimal, and then encodes it in base64. It then opens an ELF file named nmap_og (which we also found in the same folder), reads the first 64 bytes, and writes them into a new file. Finally, it appends the base64-encoded content to the new file.

(This script was used to hide the stolen credentials that we found inside the nmap file during our first investigation.)

- hide_pdf.py: hides a pdf file after the EOF of a .wav file

(It was used to hide the pdf containing the bank account details inside the game_of_thrones intro audio)

- lsb.pyc: This script hides a document inside an image using Least Significant Bit (LSB) steganography. The method is based on a specified number of significant bytes and can embed the data in various directions, such as diagonally downward or horizontally.

(It was used to hide the blueprint inside the tagus.png in the diagonal and to hide the report inside the wallpaper.png)

Backup analysis

Inside the backups folder we can identify three files: backup.sh, obfuscator and pass_gen.sh.

The obfuscator file was a binary compiled python file and to obtain the source script we had to decompile it by running the command **uncompyle6 obfuscator.pyc**. The backup.sh file was a script that generated a new disk backup based on a timestamp. We found that some of the backups made were stored in the backupDisk inside the home directory. The backup.sh executed another script, pass_gen.sh, that ran the obfuscator to generate a new password for the zip. This obfuscator script received an argument and used it alongside a seed to generate a hash and use it as password. Each run generated a new seed for the next run and stored it in a file called seed.txt in the tmp folder, which initially, for the first run, had an unknown password in it. We could see from the backup script that the arguments that were being passed to the obfuscator were the timestamps that were also in the title of the backup zips.

This means that to crack the first backup zip file we have to find the missing keyword that was initially in the seed.txt and run the script with the argument equal to the timestamp present in his name a certain number of times until we reach the password for it. After cracking the first one we have to switch the argument to the timestamp of the second one and run the script until we crack it, and so on…

We needed to find this initial keyword and so we focused our attention to a file called Passwords.kdbx located in the home directory. We tried analyzing it through **keepassxc-cli open passwords.kdbx**, but it was locked behind another password. After continuing exploring the folders inside the johnnyDisk we reached the tmp directory through running **fls -o 4096 johnnyDisk.img -o 1310722.** We stumbled across some log files that were alongside the previous seed.txt file. We analyzed the contents of the first one (K5rb9cnL0Is.log) by running the command

icat -o 4066 johnnyDisk.img 1310805. It registered a series of keypresses and, in the middle, we found strange sequences like [k][e][e][p][a][s][s] and [i][l][l][o][v][e][m][y][d][a][d][t][h][e][g][o][a][t]. These strange patterns stood out among the others which led us to believe that maybe one of them was the password to unlock the passwords database. We started trying to use them in the password query and “ilovemydadthegoat” successfully unlocked the Passwords database. We then reached the password we needed in the “Backups” entry, which was “TheBiteOf87”.

Now, we had the missing keyword that we needed to start cracking the zip files… We modified the initial obfuscate script so it reads the seed from a new file, where we put the “TheBiteOf87” password, and added a couple lines in the end so that, after generating the password, it tries to unzip the file we specify it to (obsfucator_uncompiled_modified.py). We started running this with the timestamp for the first backup (the one with the lowest inode) in the backup disk. In the 71th run it managed to extract the contents inside the zip, so we ran it with the timestamp for the second one. It extracted the second one immediately after, and the other ones followed.

The 6th backup, which was unlocked in the 76 run, contained the artifacts that were present in sigma and through which we extracted the artifacts in the first investigation: andromeda.png, best-intro.wav, cartwheel.tiff, lactea.jpg, myzip.zip, nmap and tagus.png. After a checksum analysis we concluded that these were, in fact, the originally discovered files in João Musk’s account.

Search history

Ultimately, by booting a virtual machine using the JohnnyDisk image, we gained easy access to Johnny's privileged Google and YouTube search history. This provided crucial details, including the date when he downloaded the hacked credentials and the hacking tools, along with searches directly related to the artifacts uncovered in the initial investigation. Specifically, these searches focused on mind control technology, the restaurants linked to the MKUltra issue and how to securely and permanently delete files. This allowed us to better understand and follow John’s course of actions from the moment he got the artifacts to the time he deleted them from his personal computer.

3 Analysis of relevant findings

3.1 Did you find any traces of the hidden artifacts and/or the files originally discovered in João Musk's sigma account on his computers?

We successfully recovered all the originally discovered documents from the backup ZIP files inside the backupDisk. By verifying their checksums, we have confirmed that these files are identical to the ones we initially investigated in João Musk's Sigma account. Although the SHA-256 checksum of myzip.zip differs from the original, extracting its contents with the password that we found previously resulted in the same files. This allowed us to locate the API documentation and the DECO report, which is similar to what we discovered earlier.

3.2 If so, can you trace the origin of these files and how they were processed over time? Construct a timeline of relevant events.

The credentials were sent to Johnny by RootKitty via WeTransfer, while the other artifacts were obtained from a USB drive given to him by an unknown individual. Johnny then concealed these files using tools from a collection of scripts he downloaded from PirateMajima's GitHub repository. He subsequently copied the resulting files to the Sigma cluster and securely deleted all of the traces using secure delete, which permanently removes the files from the system. The timeline of these events is detailed in the attached Excel file, outlining the sequence of commands Johnny executed to conceal the artifacts.

3.3 Did you uncover any evidence of anti-forensic activities?

During our analysis of the .bash_history and the irssi log file, we identified several anti-forensic activities. Notably, the use of the srm command, which was employed to permanently erase artifacts from the computer after they had been concealed, such as the students' credentials. The chat exchanges between John Musk and RootKitty also contain messages that show that they are actively trying to hide from the authorities the passwords that Rootkitty stole and the artifacts he got from the unknown pen drive.

What new discoveries can you report that might clarify the plot or identify other relevant actors?

After discovering crucial information from Johnny's chats and emails, we identified two additional key individuals and gained a deeper understanding of the case. The chat logs revealed that Johnny's friend, known as RootKitty, was also involved, along with an anonymous figure who sent Johnny an email offering him the USB drive.

In the chat logs, RootKitty admitted to stealing the credentials, making him the primary suspect in the theft. We also confirmed that Johnny Musk had indeed encoded and hidden the credentials, as well as the MKUltra and Ariane-6 files.

While Johnny was initially suspected of involvement in the MKUltra and the Ariane-6 ISTSat-1 satellite scheme, a comment about an email he received suggests that he was unaware of where these artifacts really come from. The email, sent by an anonymous figure, seemed to warn Johnny about the situation. This new information not only confirms the possibility that MKUltra is indeed embedded in ISTSat-1, but also points to some larger plan outside the scope of these students.

Following these discoveries, Johnny is allegedly not involved in the use of MKUltra or in the theft of the credentials, though he was aware of both incidents and helped concealing these secrets. These discoveries also suggest that the theft of the credentials is at the moment unrelated to the MKUltra case.

We found out that the tagus protest against the ISTSat-1 satellite was organized by John, who, driven by his concern over the use of mind control technology, shifted his focus towards raising public awareness about the dangers posed by the ISTSat-1 satellite.

The next step should focus on investigating RootKitty to uncover his motives for stealing the credentials, while also working to identify the anonymous individual connected to the Ariane-6 project and MKUltra. It should be taken into consideration what intentions this anonymous figure had for warning Johnny. Additionally, the investigation should explore whether Virgolino Gonçalves is involved in the acquisition of MKUltra and if he plays a role in the case overall. The USB pen that Johnny received should also be retrieved for further analysis.