Berk Emre Mert

[bmert24@student.oulu.fi](mailto:bmert24@student.oulu.fi)

**Task 1: Have I been Pwned**

**Task 1 A) Looking for leaks**

For the email of joe@gmail.com:

A screenshot of a computer

AI-generated content may be incorrect.

For my personal email berkemremert@gmail.com:

A screenshot of a computer

AI-generated content may be incorrect.

**Task 1 B) Breach data content**

Some websites let people pay to see hacked data. Three examples are DeHashed, Snusbase, and IntelX. These sites share leaked emails, passwords, and other private info. Some people use them to check their own security, but hackers can also misuse them.

The big question is: Should everyone be able to search for leaked data, or should we try to remove it? If people can see exactly what was leaked, they can protect themselves. But at the same time, bad people could use this information for scams. Removing it sounds like a good idea, but once data is on the internet, it’s almost impossible to erase.

Companies often don’t tell the full truth about data leaks. If breach data was more open, companies might take security more seriously. But if everything was public, people could be put in danger.

The best idea might be to let only verified users check their own leaked data while hiding the most dangerous information. This way, people can protect themselves, but private details won’t be easy to abuse.

**Task 2: Hardcoded Passwords**

**Valid Password**: Vulture3H

**Valid Activation Key**: The binary accepts activation keys that, when converted from hexadecimal to decimal and summed, equal 0x539 (1337 in decimal). So 539 in hexadecimal is a valid key

**Instructions to Create Other Activation Keys**: 53A (5 + 3 + 10 = 18 in decimal) is valid.

**Super Secret Password**: The hash value 4dc9332c corresponds to the plaintext password password123

**Hash Function Used**: The hash function used for the super secret password is SHA-1

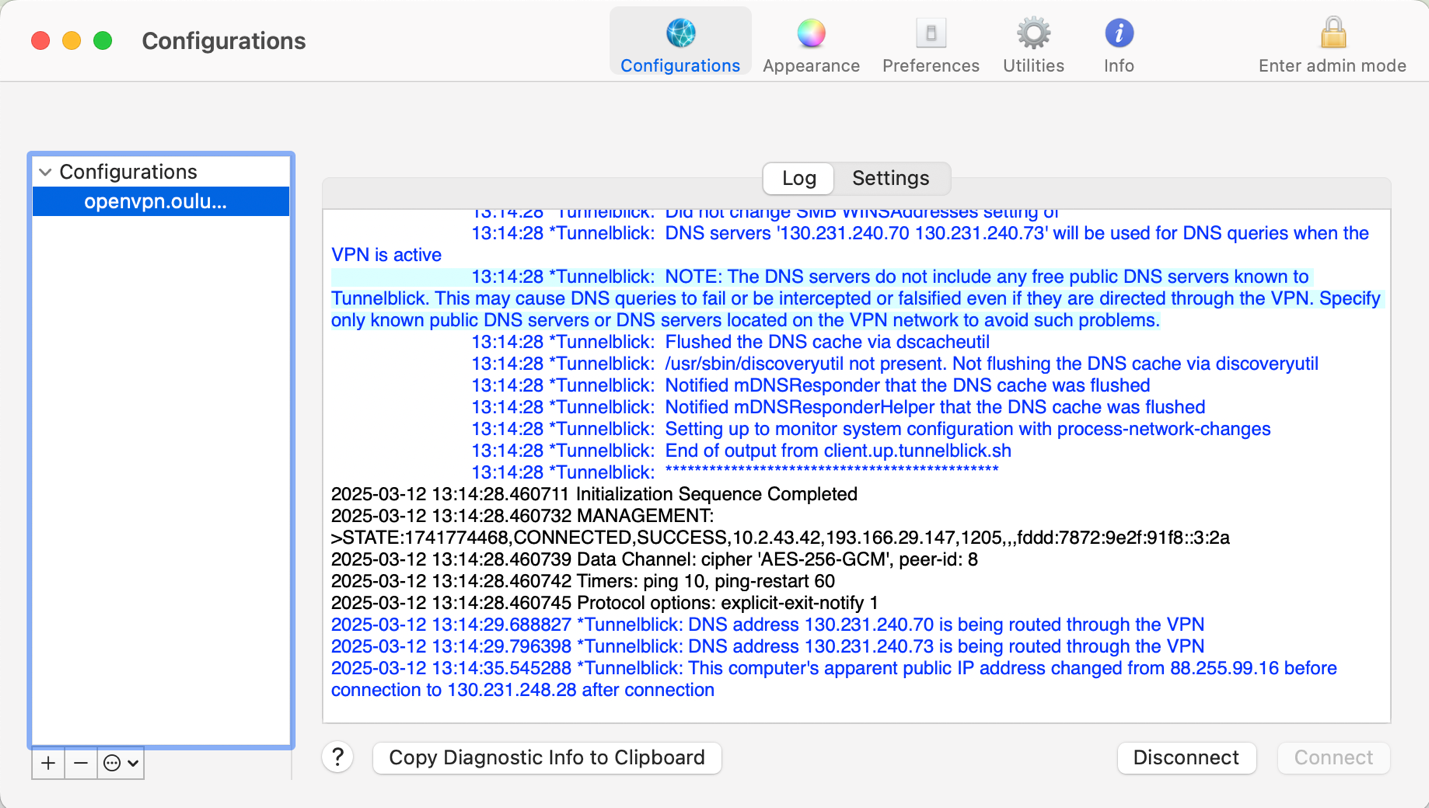
**Task 3: OSINT exploitation**

Firstly, I have successfully set the openVPN up to my Ubuntu virtual machine.

A screenshot of a computer

AI-generated content may be incorrect.

It didn’t work properly so I downloaded the VPN to my Mac.



Then I have downloaded Sherlock by using brew.

1. **What is the alias of the new employee and where is he from? Explain where you found this information**

I used sherlock command to find social media alias:

(base) berkemremert@Berk-MacBook-Air PS3 % sherlock pellesecurity

[\*] Checking username pellesecurity on:

[+] ArtStation: https://www.artstation.com/pellesecurity

[+] Cults3D: https://cults3d.com/en/users/pellesecurity/creations

[+] Freelance.habr: https://freelance.habr.com/freelancers/pellesecurity

[+] GNOME VCS: https://gitlab.gnome.org/pellesecurity

[+] GitHub: https://www.github.com/pellesecurity

[+] NationStates Nation: https://nationstates.net/nation=pellesecurity

[+] NationStates Region: https://nationstates.net/region=pellesecurity

[+] TorrentGalaxy: https://torrentgalaxy.to/profile/pellesecurity

[+] Twitter: https://x.com/pellesecurity

[+] YouTube: https://www.youtube.com/@pellesecurity

[\*] Search completed with 10 results

(base) berkemremert@Berk-MacBook-Air PS3 % sherlock pelle\_security

[\*] Checking username pelle\_security on:

[+] ArtStation: https://www.artstation.com/pelle\_security

[+] Cults3D: https://cults3d.com/en/users/pelle\_security/creations

[+] Freelance.habr: https://freelance.habr.com/freelancers/pelle\_security

[+] GNOME VCS: https://gitlab.gnome.org/pelle\_security

[+] NationStates Nation: https://nationstates.net/nation=pelle\_security

[+] NationStates Region: https://nationstates.net/region=pelle\_security

[+] Twitter: https://x.com/pelle\_security

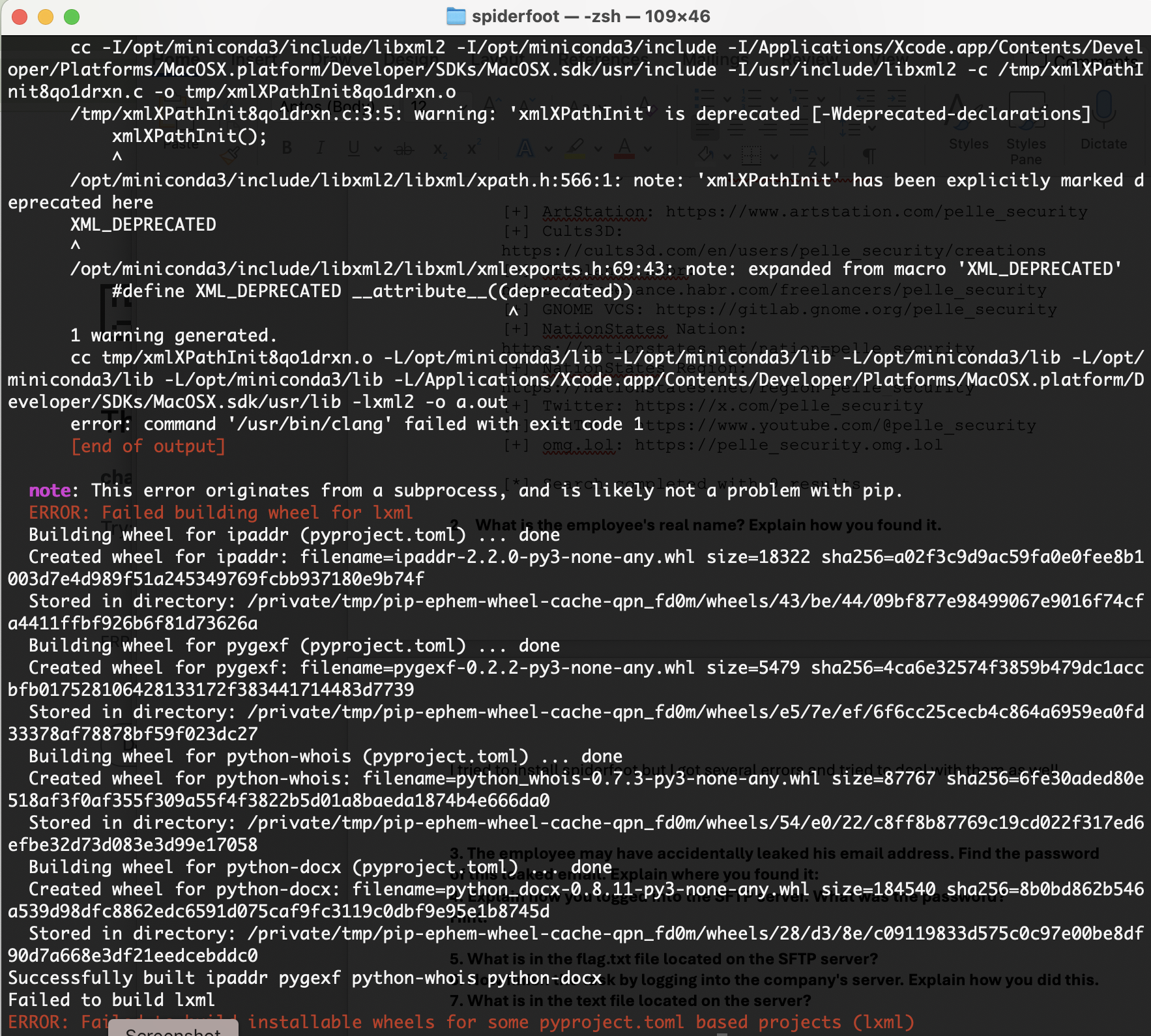
[+] YouTube: https://www.youtube.com/@pelle\_security

[+] omg.lol: https://pelle\_security.omg.lol

[\*] Search completed with 9 results

1. **What is the employee's real name? Explain how you found it.**

I tried to install spiderfoot but I got several errors and tried to deal with them as well.



I realised that the problem was because I was doing the processes in the virtual environment and lxml wasn’t properly building wheel up for some reason. So I deactivated the environment and tried to install requirements for one more time.

I finally realised that the problem is because spiderfoot was using an old version of lxml so I created an issue about it on Github as well.

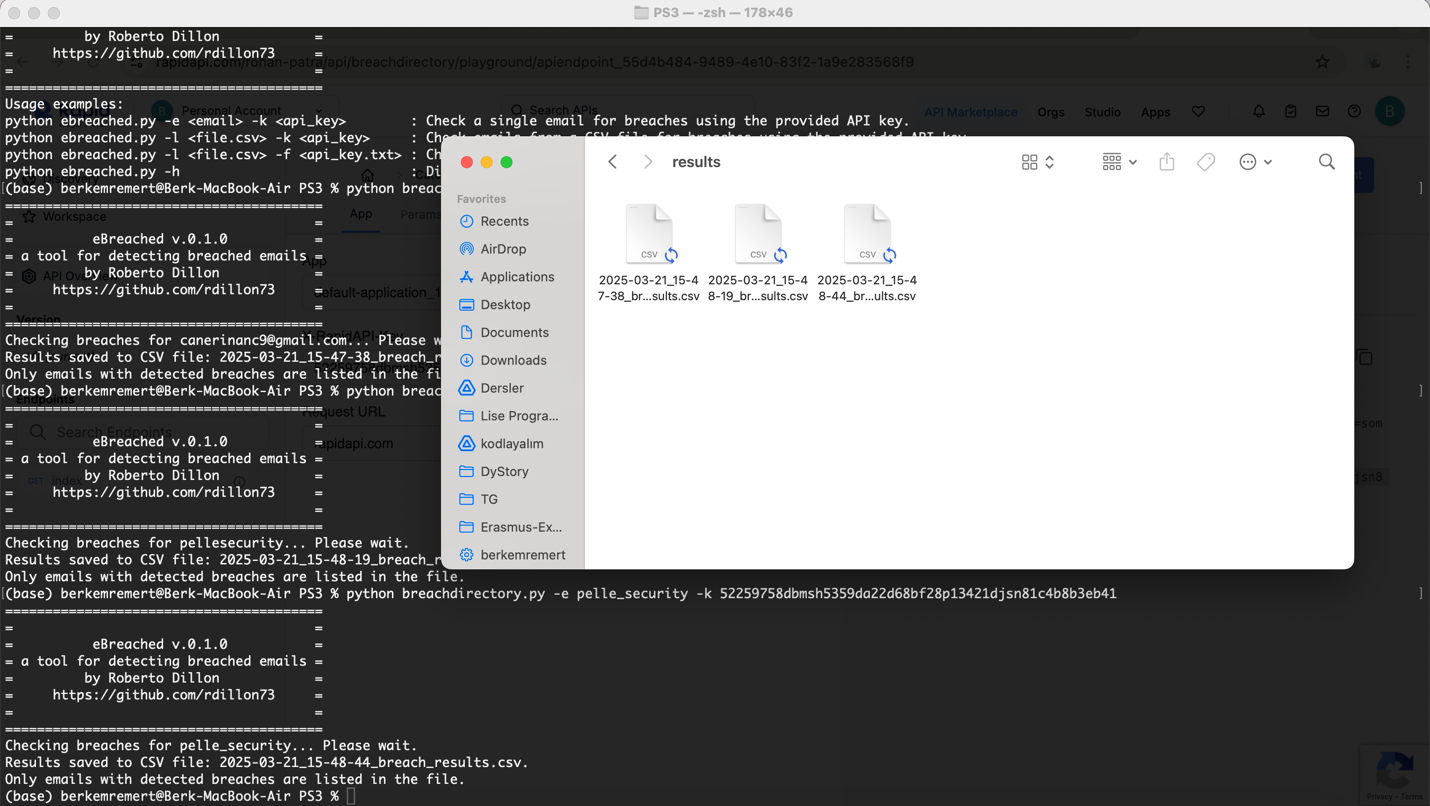
A screenshot of a computer

AI-generated content may be incorrect.

I scanned the name pelle in … and I found that the real name of the employee is Jose Luis Simonetti in the part of similar domains WHOIS.

1. **The employee may have accidentally leaked his email address. Find the password of this leaked email. Explain where you found it:**

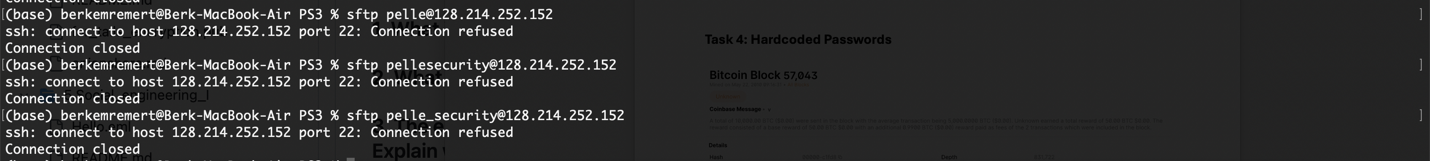
I tried to search pelle\_security or pellesecurity on BreachDirectory but I couldn’t find anything. Result files didn’t include anything.



I got help from the following github page as well: <https://github.com/rdillon73/eBreached>

**4. Explain how you logged into the SFTP server. What was the password?**

I couldn’t find the email unfortunately ☹ but I tried several mail addresses to check. Still I couldn’t log in. (I had my VPN open for Oulu)



1. **What is in the flag.txt file located on the SFTP server?**

Couldn’t do this task.

1. **Now finish the task by logging into the company's server. Explain how you did this.**

Couldn’t do this task.

1. **What is in the text file located on the server?**

Couldn’t do this task.

**Task 4: Hardcoded Passwords**

A screenshot of a computer

AI-generated content may be incorrect.

**Transaction**

Date and Time of the transaction: 5/22/2010, 21:16:31

Hash of the transaction: a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

Address of sender: 1XPTgDRhN8RFnzniWCddobD9iKZatrvH4

Address of receiver: 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ

Transaction fee amount in bitcoin: 99.0M Sats, $83,392.75, in Bitcoin: 0.99 BTC

**Receiver Address**

Who was the owner of this address?

**Laszlo Hanyecz**

Use Google to figure out the real name of the user**: I found him. He bought two pizzas with that money.**

**The receiver: Jeremy Sturdivant**

The owner instantly divided and forwarded the 10,000 to (how many?) **2** other addresses

Addresses that received the 10,000 bitcoin and the corresponding sums to each address

To: 1MLh2UVHgonJY4ZtsakoXtkcXDJ2EPU6RY

5777.00000000 BTC

-> $484,097,406

To: 13TETb2WMr58mexBaNq1jmXV1J7Abk2tE2

4223.00000000 BTC

-> $353,876,293

**Block**

Hash of the block 57043: 00000000152340ca42227603908689183edc47355204e7aca59383b0aaac1fd8

Amount of transactions in the block: 10,000.00 BTC

Block reward amount: 50.00 BTC

**Miner**

Address of the miner for block 57043: **1yXfRNBg9E2URDEcrdZx5R1ZPxTcUJGTH**

Has this address spent the block reward they received?: **S/he didn’t spend it, still has 50.99017620 BTC on his/her account.**