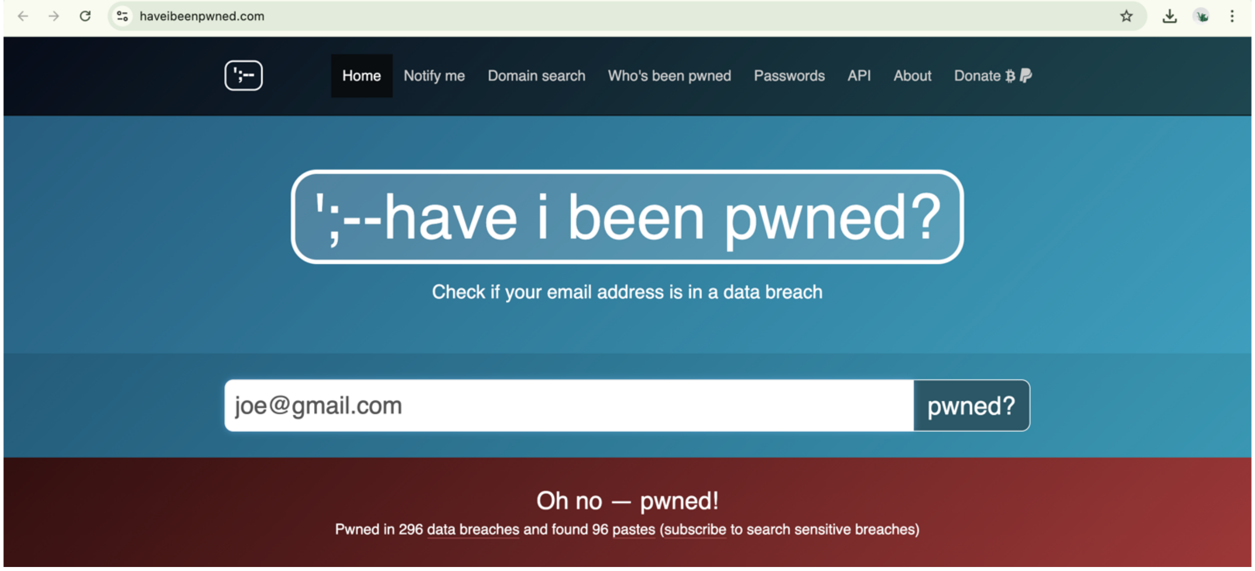
Berk Emre Mert
bmert24@student.oulu.fi

Task 1: Have I been Pwned

Task 1 A) Looking for leaks

For the email of joe@gmail.com:



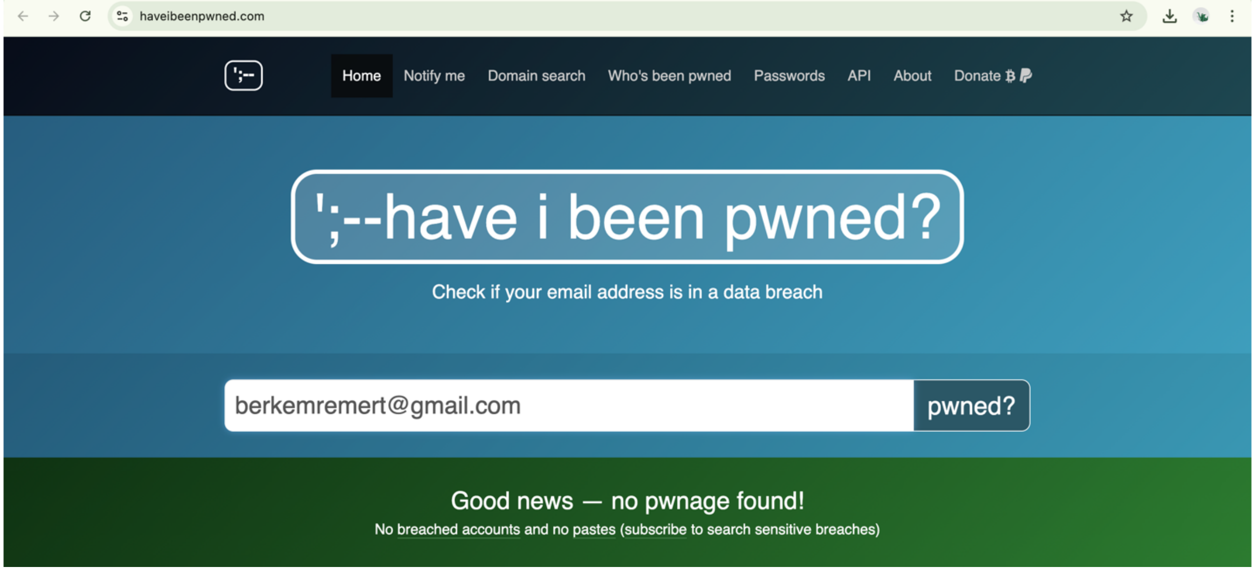
Check if your email address is in a data breach

joe@gmail.com

Oh no — pwned!

Pwned in 296 data breaches and found 96 pastes (subscribe to search sensitive breaches)

For my personal email berkemremert@gmail.com:



Check if your email address is in a data breach

berkemremert@gmail.com

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

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.

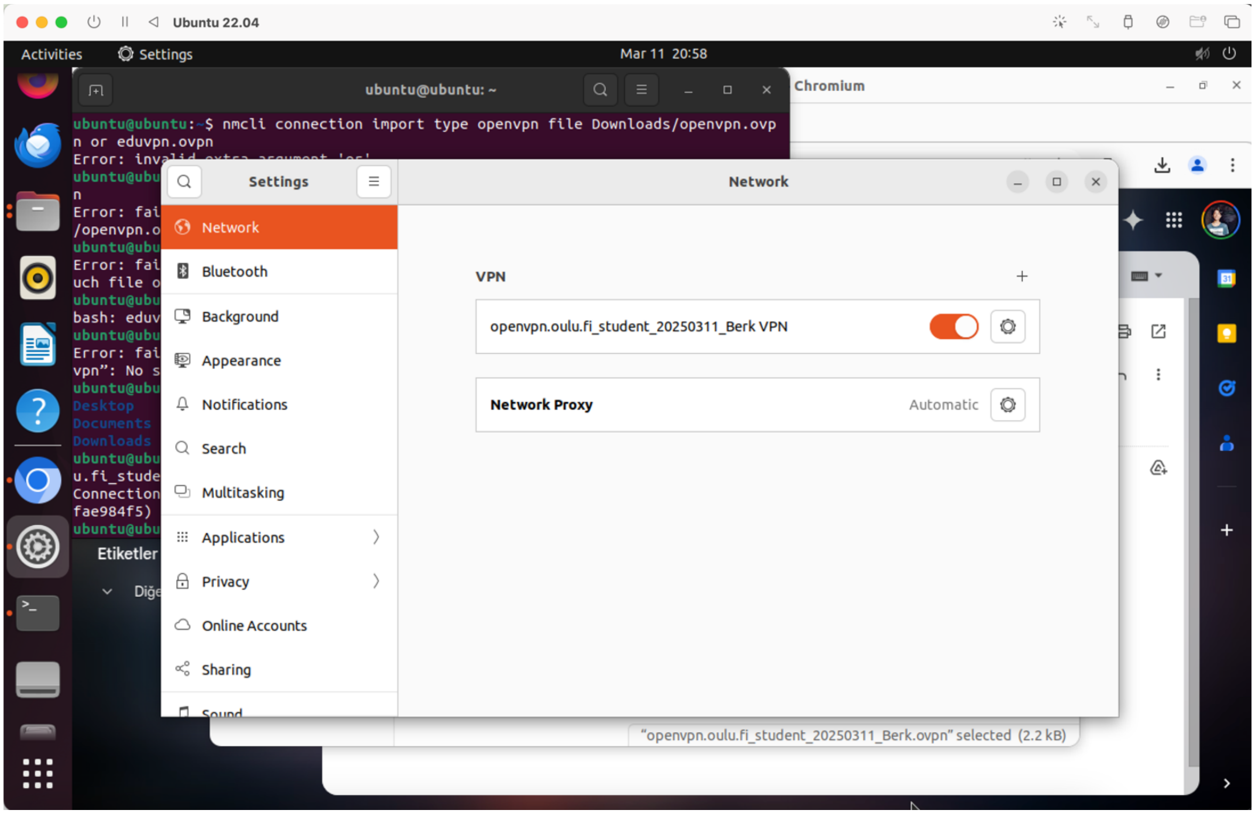
The best idea might be to let only verified users check their own leaked data while hiding the most dangerous information. This way, people can protect themselves, but private details won't be easy to abuse.

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.



```
ubuntu@ubuntu:~$ nmcli connection import type openvpn file Downloads/openvpn.ovp
n or eduvpn.ovpn
Error: invalid extra argument 'or'.
ubuntu@ubu
n
Error: fai
/openvpn.o
ubuntu@ubu
Error: fai
uch file o
ubuntu@ubu
bash: eduv
ubuntu@ubu
Error: fai
vpn": No s
ubuntu@ubu
Desktop
Documents
Downloads
ubuntu@ubu
u.fi_stude
Connection
fae984f5)
ubuntu@ubu
```

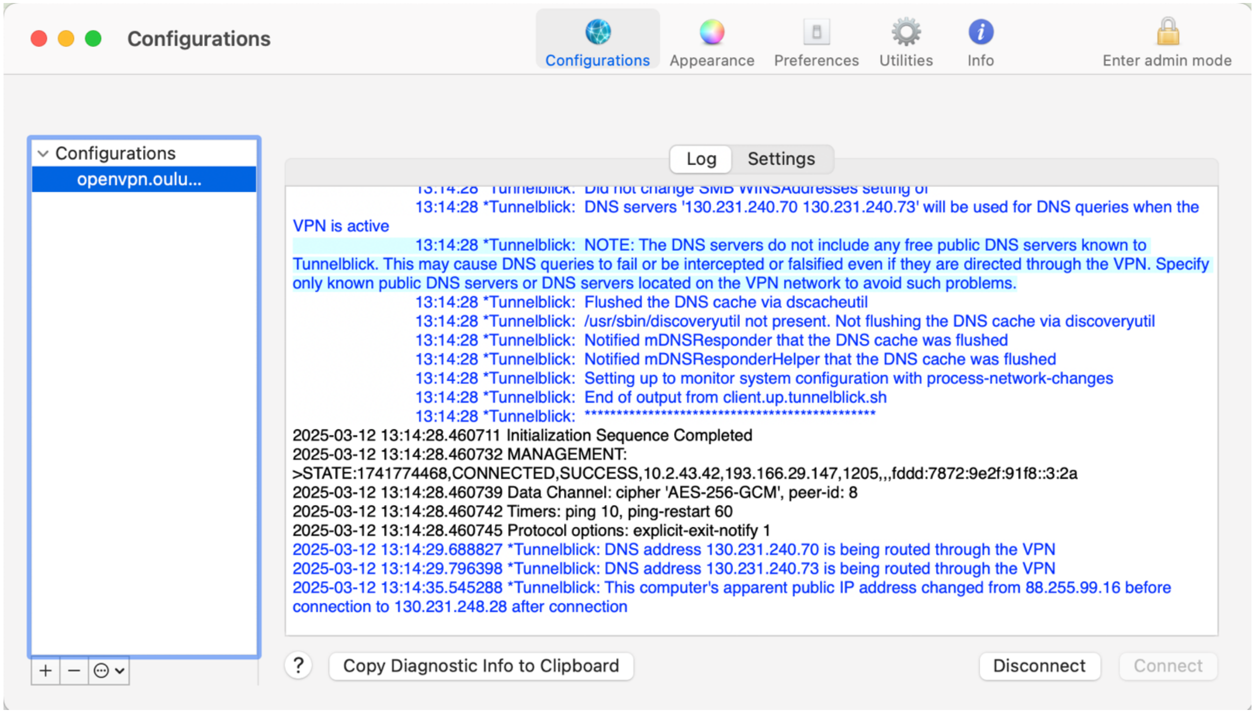
VPN

openvpn.oulu.fi_student_20250311_Berk VPN

Network Proxy Automatic

"openvpn.oulu.fi_student_20250311_Berk.ovpn" selected (2.2 kB)

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



```
                    13:14:28 *Tunnelblick:  Did not change SMB WINSAddresses setting of
                    13:14:28 *Tunnelblick:  DNS servers '130.231.240.70 130.231.240.73' will be used for DNS queries when the
VPN is active
                    13:14:28 *Tunnelblick:  NOTE: The DNS servers do not include any free public DNS servers known to
Tunnelblick. This may cause DNS queries to fail or be intercepted or falsified even if they are directed through the VPN. Specify
only known public DNS servers or DNS servers located on the VPN network to avoid such problems.
                    13:14:28 *Tunnelblick:  Flushed the DNS cache via dscacheutil
                    13:14:28 *Tunnelblick:  /usr/sbin/discoveryutil not present. Not flushing the DNS cache via discoveryutil
                    13:14:28 *Tunnelblick:  Notified mDNSResponder that the DNS cache was flushed
                    13:14:28 *Tunnelblick:  Notified mDNSResponderHelper that the DNS cache was flushed
                    13:14:28 *Tunnelblick:  Setting up to monitor system configuration with process-network-changes
                    13:14:28 *Tunnelblick:  End of output from client.up.tunnelblick.sh
                    13:14:28 *Tunnelblick:  ************************************************
2025-03-12 13:14:28.460711 Initialization Sequence Completed
2025-03-12 13:14:28.460732 MANAGEMENT:
>STATE:1741774468,CONNECTED,SUCCESS,10.2.43.42,193.166.29.147,1205,,,fddd:7872:9e2f:91f8::3:2a
2025-03-12 13:14:28.460739 Data Channel: cipher 'AES-256-GCM', peer-id: 8
2025-03-12 13:14:28.460742 Timers: ping 10, ping-restart 60
2025-03-12 13:14:28.460745 Protocol options: explicit-exit-notify 1
2025-03-12 13:14:29.688827 *Tunnelblick: DNS address 130.231.240.70 is being routed through the VPN
2025-03-12 13:14:29.796398 *Tunnelblick: DNS address 130.231.240.73 is being routed through the VPN
2025-03-12 13:14:35.545288 *Tunnelblick: This computer's apparent public IP address changed from 88.255.99.16 before
connection to 130.231.248.28 after connection
```

Then I have downloaded Sherlock by using brew.

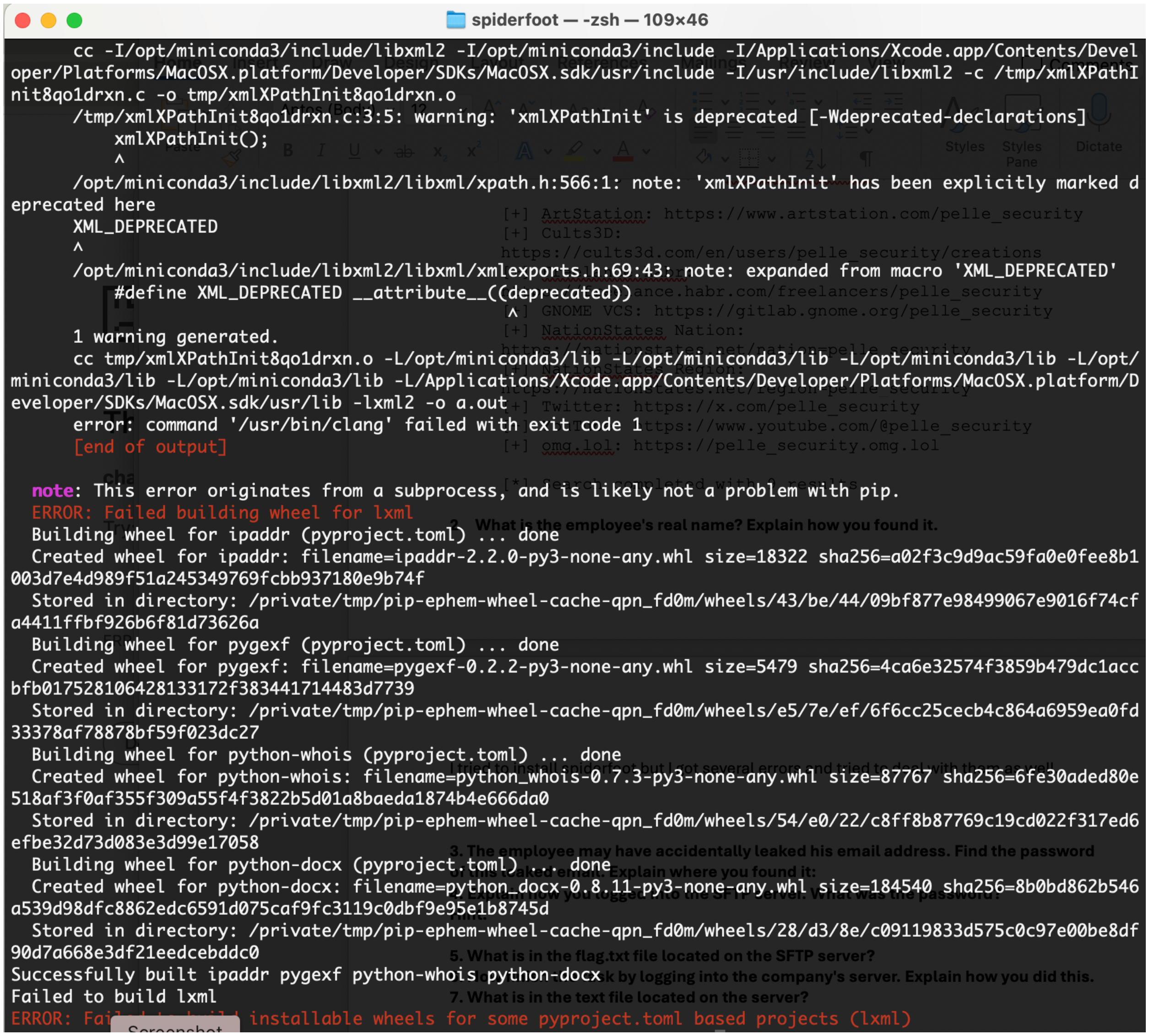
1. **What is the alias of the new employee and where is he from? Explain where you found this information**

   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
   ```

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

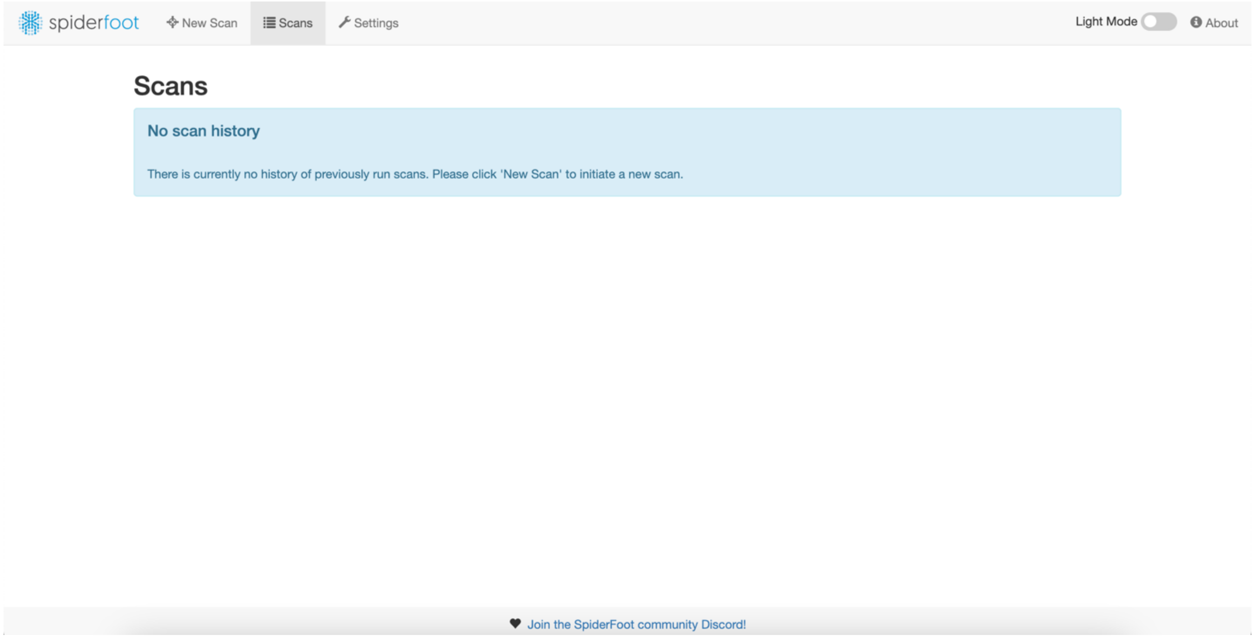
I tried to install spiderfoot but I got several errors and tried to deal with them as well.



```
      cc -I/opt/miniconda3/include/libxml2 -I/opt/miniconda3/include -I/Applications/Xcode.app/Contents/Devel
oper/Platforms/MacOSX.platform/Developer/SDKs/MacOSX.sdk/usr/include -I/usr/include/libxml2 -c /tmp/xmlXPathI
nit8qo1drxn.c -o tmp/xmlXPathInit8qo1drxn.o
      /tmp/xmlXPathInit8qo1drxn.c:3:5: warning: 'xmlXPathInit' is deprecated [-Wdeprecated-declarations]
          xmlXPathInit();
          ^
      /opt/miniconda3/include/libxml2/libxml/xpath.h:566:1: note: 'xmlXPathInit' has been explicitly marked d
eprecated here
      XML_DEPRECATED
      ^
      /opt/miniconda3/include/libxml2/libxml/xmlexports.h:69:43: note: expanded from macro 'XML_DEPRECATED'
          #define XML_DEPRECATED __attribute__((deprecated))
                                                    ^
      1 warning generated.
      cc tmp/xmlXPathInit8qo1drxn.o -L/opt/miniconda3/lib -L/opt/miniconda3/lib -L/opt/miniconda3/lib -L/opt/
miniconda3/lib -L/opt/miniconda3/lib -L/Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/D
eveloper/SDKs/MacOSX.sdk/usr/lib -lxml2 -o a.out
      error: command '/usr/bin/clang' failed with exit code 1
      [end of output]

  note: This error originates from a subprocess, and is likely not a problem with pip.
  ERROR: Failed building wheel for lxml
  Building wheel for ipaddr (pyproject.toml) ... done
  Created wheel for ipaddr: filename=ipaddr-2.2.0-py3-none-any.whl size=18322 sha256=a02f3c9d9ac59fa0e0fee8b1
003d7e4d989f51a245349769fcbb937180e9b74f
  Stored in directory: /private/tmp/pip-ephem-wheel-cache-qpn_fd0m/wheels/43/be/44/09bf877e98499067e9016f74cf
a4411ffbf926b6f81d73626a
  Building wheel for pygexf (pyproject.toml) ... done
  Created wheel for pygexf: filename=pygexf-0.2.2-py3-none-any.whl size=5479 sha256=4ca6e32574f3859b479dc1acc
bfb0175281064281331 72f383441714483d7739
  Stored in directory: /private/tmp/pip-ephem-wheel-cache-qpn_fd0m/wheels/e5/7e/ef/6f6cc25cecb4c864a6959ea0fd
33378af78878bf59f023dc27
  Building wheel for python-whois (pyproject.toml) ... done
  Created wheel for python-whois: filename=python_whois-0.7.3-py3-none-any.whl size=87767 sha256=6fe30aded80e
518af3f0af355f309a55f4f3822b5d01a8baeda1874b4e666da0
  Stored in directory: /private/tmp/pip-ephem-wheel-cache-qpn_fd0m/wheels/54/e0/22/c8ff8b87769c19cd022f317ed6
efbe32d73d083e3d99e17058
  Building wheel for python-docx (pyproject.toml) ... done
  Created wheel for python-docx: filename=python_docx-0.8.11-py3-none-any.whl size=184540 sha256=8b0bd862b546
a539d98dfc8862edc6591d075caf9fc3119c0dbf9e95e1b8745d
  Stored in directory: /private/tmp/pip-ephem-wheel-cache-qpn_fd0m/wheels/28/d3/8e/c09119833d575c0c97e00be8df
90d7a668e3df21eedcebddc0
Successfully built ipaddr pygexf python-whois python-docx
Failed to build lxml
ERROR: Failed to build installable wheels for some pyproject.toml based projects (lxml)
```

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.



Scans

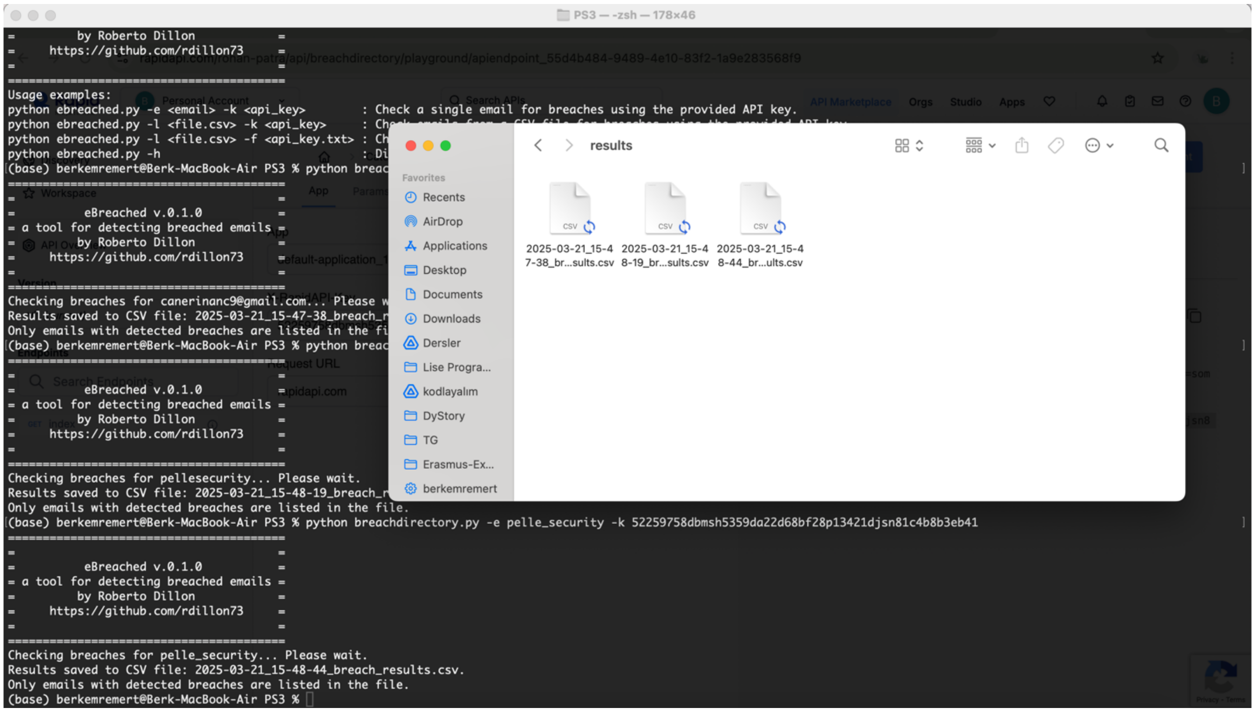
No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

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.

3. 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.

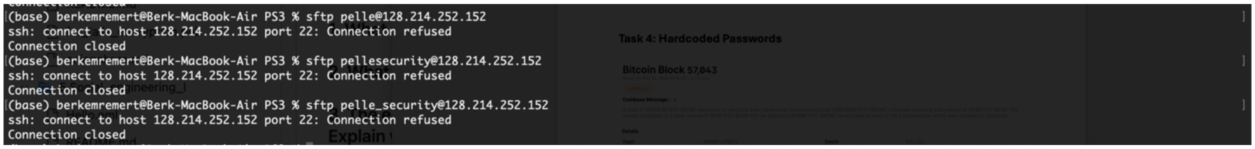


```
=        by Roberto Dillon             =
=    https://github.com/rdillon73      =
=                                      =
========================================
Usage examples:
python ebreached.py -e <email> -k <api_key>        : Check a single email for breaches using the provided API key.
python ebreached.py -l <file.csv> -k <api_key>     : Check emails from a CSV file for breaches using the provided API key.
python ebreached.py -l <file.csv> -f <api_key.txt> : Ch
python ebreached.py -h                             : Di
(base) berkemremert@Berk-MacBook-Air PS3 % python breac
========================================
=                                      =
=         eBreached v.0.1.0            =
= a tool for detecting breached emails =
=        by Roberto Dillon             =
=    https://github.com/rdillon73      =
=                                      =
========================================
Checking breaches for canerinanc9@gmail.com... Please w
Results saved to CSV file: 2025-03-21_15-47-38_breach_r
Only emails with detected breaches are listed in the fi
(base) berkemremert@Berk-MacBook-Air PS3 % python breac
========================================
=                                      =
=         eBreached v.0.1.0            =
= a tool for detecting breached emails =
=        by Roberto Dillon             =
=    https://github.com/rdillon73      =
=                                      =
========================================
Checking breaches for pellesecurity... Please wait.
Results saved to CSV file: 2025-03-21_15-48-19_breach_r
Only emails with detected breaches are listed in the file.
(base) berkemremert@Berk-MacBook-Air PS3 % python breachdirectory.py -e pelle_security -k 52259758dbmsh5359da22d68bf28p13421djsn81c4b8b3eb41
========================================
=                                      =
=         eBreached v.0.1.0            =
= a tool for detecting breached emails =
=        by Roberto Dillon             =
=    https://github.com/rdillon73      =
=                                      =
========================================
Checking breaches for pelle_security... Please wait.
Results saved to CSV file: 2025-03-21_15-48-44_breach_results.csv.
Only emails with detected breaches are listed in the file.
(base) berkemremert@Berk-MacBook-Air PS3 %
```

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)



```
(base) berkemremert@Berk-MacBook-Air PS3 % sftp pelle@128.214.252.152
ssh: connect to host 128.214.252.152 port 22: Connection refused
Connection closed
(base) berkemremert@Berk-MacBook-Air PS3 % sftp pellesecurity@128.214.252.152
ssh: connect to host 128.214.252.152 port 22: Connection refused
Connection closed
(base) berkemremert@Berk-MacBook-Air PS3 % sftp pelle_security@128.214.252.152
ssh: connect to host 128.214.252.152 port 22: Connection refused
Connection closed
```

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

Couldn't do this task.

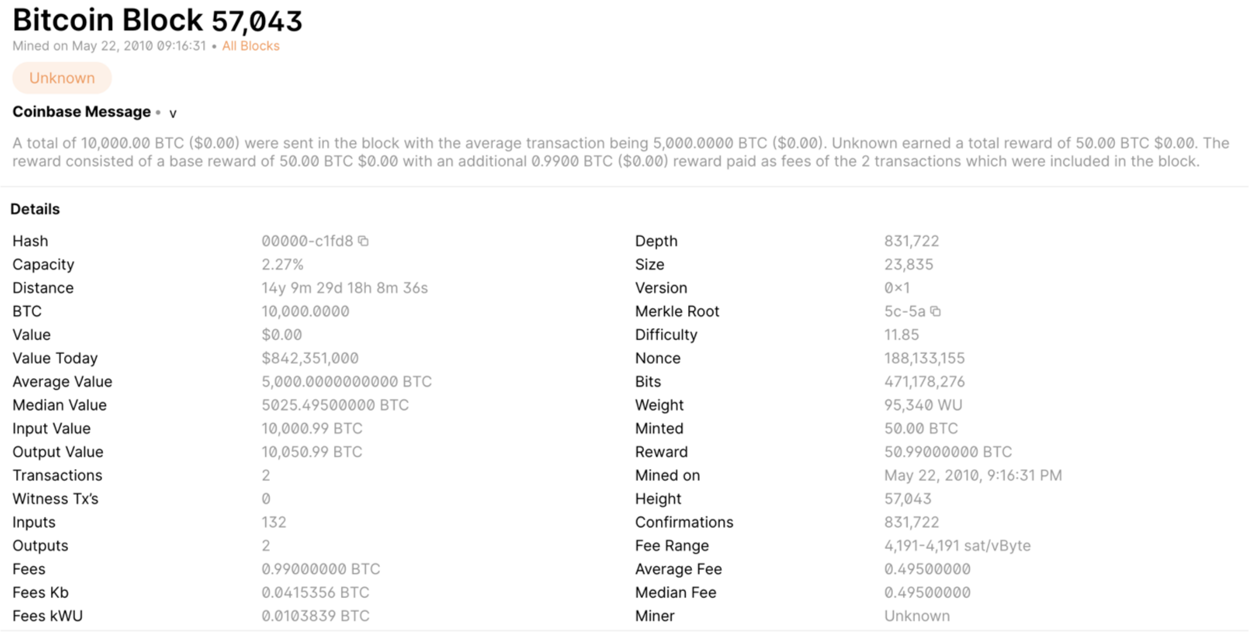
5. Now finish the task by logging into the company's server. Explain how you did this.

Couldn't do this task.

6. What is in the text file located on the server?

Couldn't do this task.

Task 4: Hardcoded Passwords



Bitcoin Block 57,043

Mined on May 22, 2010 09:16:31 • All Blocks

Unknown

Coinbase Message • v

A total of 10,000.00 BTC ($0.00) were sent in the block with the average transaction being 5,000.0000 BTC ($0.00). Unknown earned a total reward of 50.00 BTC $0.00. The reward consisted of a base reward of 50.00 BTC $0.00 with an additional 0.9900 BTC ($0.00) reward paid as fees of the 2 transactions which were included in the block.

Details

Hash	00000-c1fd8	Depth	831,722
Capacity	2.27%	Size	23,835
Distance	14y 9m 29d 18h 8m 36s	Version	0×1
BTC	10,000.0000	Merkle Root	5c-5a
Value	$0.00	Difficulty	11.85
Value Today	$842,351,000	Nonce	188,133,155
Average Value	5,000.0000000000 BTC	Bits	471,178,276
Median Value	5025.49500000 BTC	Weight	95,340 WU
Input Value	10,000.99 BTC	Minted	50.00 BTC
Output Value	10,050.99 BTC	Reward	50.99000000 BTC
Transactions	2	Mined on	May 22, 2010, 9:16:31 PM
Witness Tx's	0	Height	57,043
Inputs	132	Confirmations	831,722
Outputs	2	Fee Range	4,191-4,191 sat/vByte
Fees	0.99000000 BTC	Average Fee	0.49500000
Fees Kb	0.0415356 BTC	Median Fee	0.49500000
Fees kWU	0.0103839 BTC	Miner	Unknown

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.**