Project BootCon SocialPhish

Jaden Lassiter

Technical Background

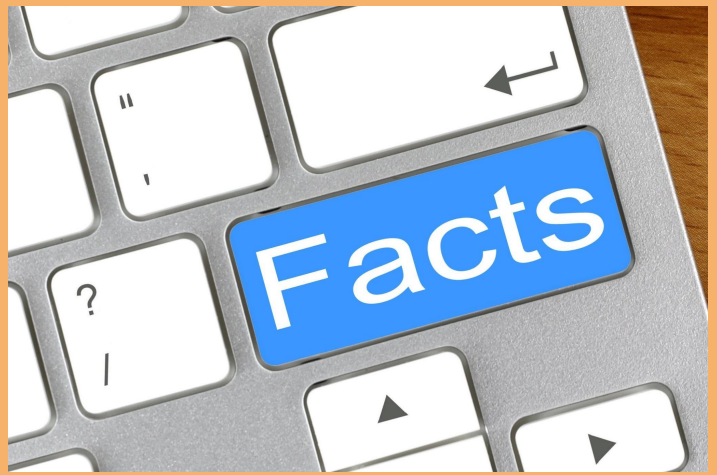
- We choose Socialphish for our final presentation project because phishing is a prevalent and damaging cyber threat. Understanding how tools like Socialphish operate is crucial for improving cybersecurity defenses. This topic will help highlight the importance of security awareness and prevention.
- Socialphish is more user-friendly Social Engineering Toolkit.

<u>Here are some common digital environments where tools like social phishing can be implemented:</u>

- Instagram
- Google
- Snapchat
- Yahoo
- Github
- Netflix,
- Linkedin,
- Microsoft,
- ETC..

Fun Facts

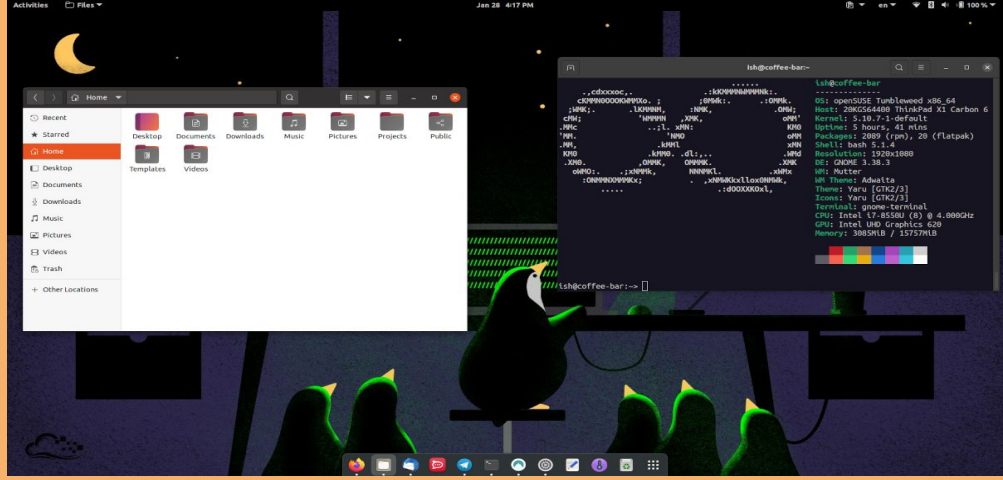
1) 95% of attacks on business networks are the result of successful spear phishing.
2) 41% of employees failed to notice a phishing message because they were tired.
3) The cost of phishing attacks has almost quadrupled over the past seven years.
4) 1 in 3 employees are likely to click the links in phishing emails.
5) Data breaches of over 33 million records are expected to occur by 2023 with a ransomware or phishing attack occurring every 11 seconds.



Demonstration Preview

- Start up your Ubuntu or Kali Linux computer. Go to the desktop. The task at hand is to establish a directory named Socialphish. You must install the tool in this directory.
- You are currently on the desktop. The task at hand is to establish a directory named Socialphish.
- You're currently in the Socialphish directory. You must clone the tool from GitHub in order to get it from this directory.
- The Socialphish directory contains the downloaded tool.
- As soon as you go through the contents of the tool, you'll notice that SocialPhish has created a new directory. To see the contents of the tool, you must relocate to this directory.
- Use a command to view the contents of the directory as a list.
- The tool now needs permission, which you may grant by a command.

Demonstration

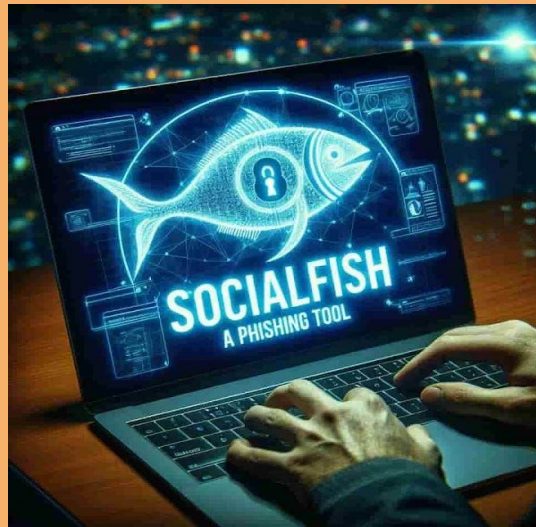


Command Syntax in Virtual Machine step by step:

1) Cd Desktop/
2) Mkdir Socialphish
3) Cd Socialphish/
4) Sudo apt install git (this is essential to make sure the script is downloaded appropriately for malicious use)
5) Git clone https://github.com/pvantas/socialphish.git

Demonstration Summary

- From the demonstration, we were able to gain the victim login credentials to use and exploit their account via the fake login page created by our Socialphish tool.
- This is a common offensive security tactic done by hackers on many technical levels. Bating the victim to click on a malicious link and watch them “successfully” login to their “account”.



Mitigation

Solutions for Risk Mitigation of SocialPhish include, but not limited to:

1) **Awareness and Training**
   - Employee Training
   - Awareness Campaigns
2) **Incident Response Plans**
   - Response teams
3) **Email Filtering**
   - Block malicious emails before they can reach the intended victim

Resources

https://www.geeksforgeeks.org/socialphish-phishing-tool-in-kali-linux/

https://phishgrid.com/blog/facts-about-phishing/

https://github.com/pvantas/socialphish.git