**Name Mohsin Nawaz**

**Rhombix Technologies**

**CYBER SECURITY INTERNSHIP TASKS**

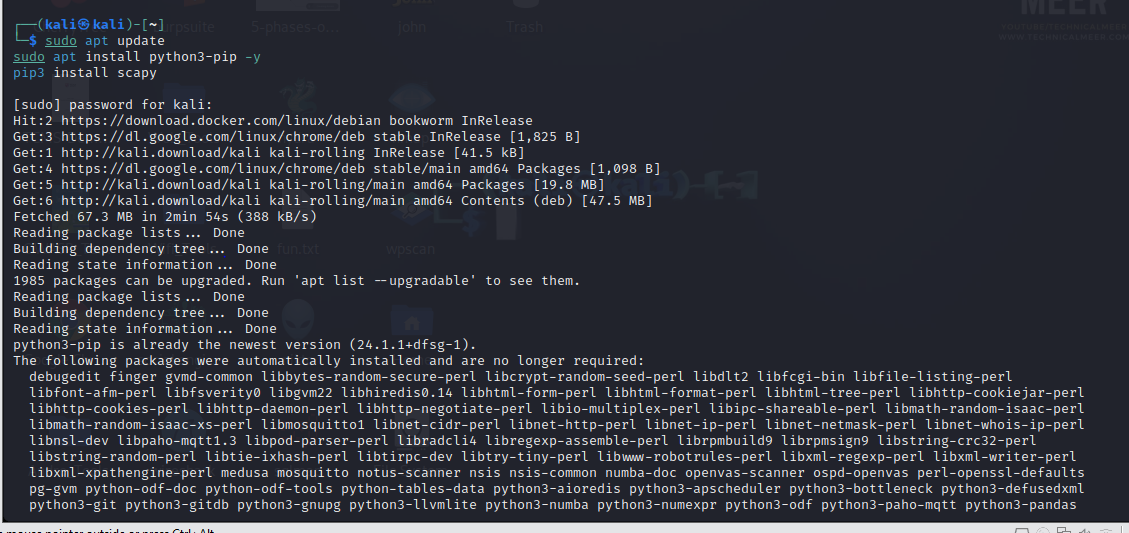
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 1:**

**Network Packet Sniffer:** Create a packet sniffer using Python and libraries like Scapy to capture and analyze network traffic. This project will help you understand network protocols and data analysis

**Answer**

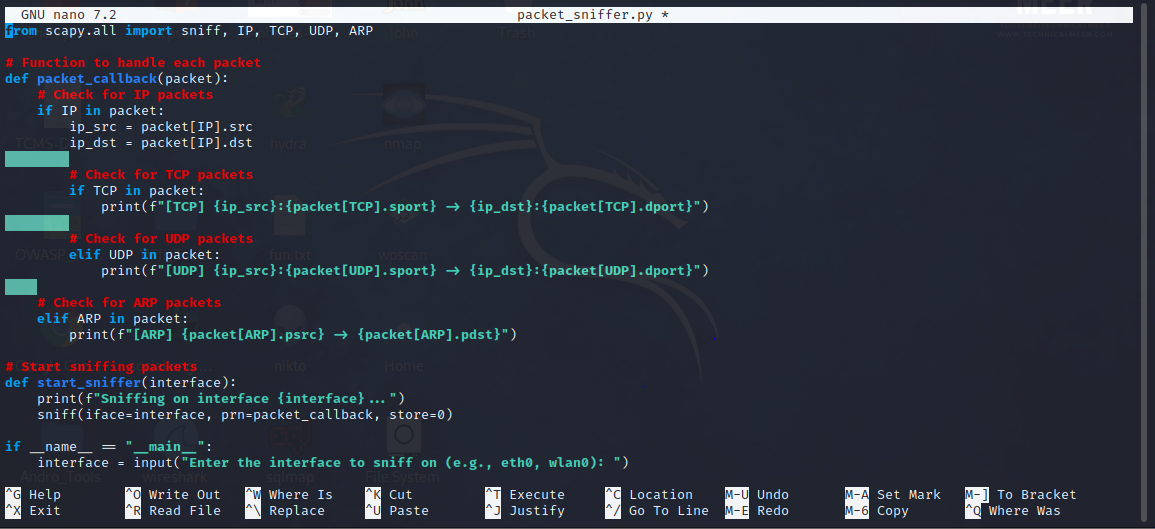
Installing the required libraries of scapy



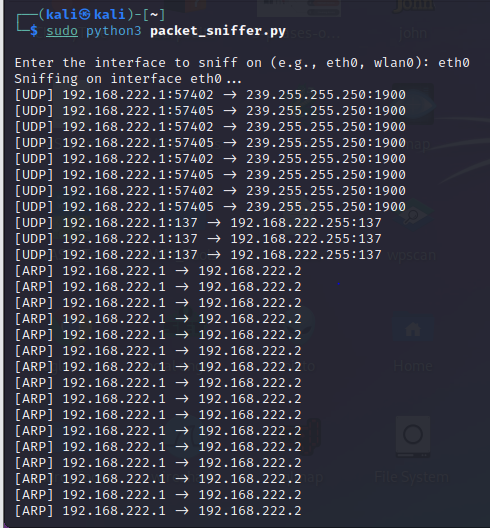
Creating python file named packet\_sniffer.py



Edit the file for coding



Now execute the file : enter the network interface you want to sniff on. Common interfaces include eth0 for wired Ethernet and wlan0 for wireless.



As the script runs, it will display information about captured packets:

* **TCP Packets**: Shows source and destination IP addresses and ports.
* **UDP Packets**: Similar to TCP but for UDP protocol.
* **ARP Packets**: Displays ARP requests and replies on the network.

**Task2:**

**Phishing awareness training :**

**Create a presentation or online training module about phishing attacks. Educate other about recognizing and avoiding phishing emails , websites , and social engineering attacks.**

**Answer:**

Creating a phishing awareness training module can be an effective way to help people recognize and avoid phishing attacks. Here’s a structured outline for a presentation or online module, including key points, tips, and interactive ideas to keep the audience engaged.

### ****Title Slide: Phishing Awareness Training****

**Subtitle:** How to Recognize and Avoid Phishing Attacks

### ****Slide 1: Introduction to Phishing****

* **What is Phishing?**
  + Phishing is a type of cyberattack where attackers attempt to deceive individuals into providing sensitive information or installing malware by posing as a trusted source.
* **Purpose of Phishing**
  + Obtain usernames, passwords, credit card numbers, or install malware for unauthorized access.
* **Types of Phishing Attacks**
  + Email Phishing
  + Spear Phishing (targeted)
  + Smishing (SMS phishing)
  + Vishing (Voice phishing)
  + Pharming (redirecting to fake websites)

### ****Slide 2: Recognizing Phishing Emails****

* **Red Flags in Emails**
  + **Suspicious Sender**: Check the sender's email address. Attackers often use emails that look like legitimate ones (e.g., amaz0n.com instead of amazon.com).
  + **Generic Greetings**: Phishing emails often use generic greetings like "Dear Customer" instead of your name.
  + **Urgency and Threats**: Messages with urgent action (e.g., “Your account will be locked”) create panic and reduce critical thinking.
  + **Spelling and Grammar Mistakes**: Many phishing emails have noticeable typos.
  + **Suspicious Links and Attachments**: Hover over links to verify URL; phishing links may look similar but often contain misspellings or extra characters.

**Interactive Idea:** Show screenshots of real and fake emails and ask participants to identify the red flags.

### ****Slide 3: Recognizing Phishing Websites****

* **URL Red Flags**
  + Look for misspellings, unusual characters, and extra domains (e.g., www.yourbank-secure.com
  + Ensure the website uses HTTPS.
* **Check for Visual Cues**
  + Look for secure indicators, like a lock icon in the browser.
  + Be cautious of pop-ups asking for sensitive information.
* **Avoid Clicking Links**
  + Instead of clicking a link in an email, type the website address directly into the browser or use saved bookmarks.

### ****Slide 4: Social Engineering Tactics****

* **Impersonation Scams**
  + Attackers might impersonate coworkers, family, or IT support to gain trust.
* **Baiting**
  + Entices the target to take action (e.g., "Free gift" or "You’ve won!").
* **Pretexting**
  + Attackers create a fake scenario to trick the victim into providing sensitive information.

**Interactive Idea:** Provide scenarios and ask participants to identify how attackers may be trying to manipulate them.

### ****Slide 5: Tips to Avoid Phishing Attacks****

* **Be Skeptical**
  + Be cautious of unexpected messages from unknown senders, especially those asking for sensitive information.
* **Verify the Source**
  + When in doubt, contact the source directly using official contact information.
* **Avoid Public Wi-Fi**
  + Use a VPN or avoid logging in to sensitive accounts on public networks.
* **Keep Software Updated**
  + Updates often include security patches to prevent attacks.
* **Enable Multi-Factor Authentication (MFA)**
  + Adds an extra layer of security, even if credentials are stolen.

### ****Slide 6: Responding to a Phishing Attack****

* **Report It**
  + Use internal company reporting tools or report phishing emails to email providers.
* **Don’t Click Links or Download Attachments**
  + If you suspect an email is phishing, avoid any interaction with links or files.
* **Check for Unauthorized Activity**
  + Regularly monitor your accounts for unusual activity.
* **Disconnect and Seek IT Help**
  + If you suspect malware has been installed, disconnect from the internet and contact IT immediately.

**Interactive Idea:** Role-play scenarios where participants must decide how to respond to a suspected phishing attempt.

### ****Slide 7: Quiz and Review****

**Questions:**

1. Identify whether an email is phishing based on provided examples.
2. Choose the safest response to a suspicious email.
3. Recognize red flags in different email and website examples.

**Review Key Points:**

* Understanding different types of phishing.
* Recognizing red flags in emails and websites.
* Strategies to protect against phishing.

### ****Slide 8: Resources for Further Learning****

* **Trusted Websites**
  + Anti-Phishing Working Group (APWG)
  + National Cyber Security Alliance (NCSA)
* **Guides and Tools**
  + Links to browser extensions or apps that help with phishing detection
  + Company-specific resources or policies on phishing and cybersecurity

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*