**Report: Performing and Analyzing a Networking Attack with Source and Traffic Tracing**

**Objective**:  
The primary objective of this project is to simulate and analyze a networking attack, trace its source, monitor traffic patterns, and propose effective countermeasures to mitigate its impact.

**Scope**:  
This report will focus on:

* Simulating a network attack (e.g., Denial of Service attack)
* Monitoring and analyzing network traffic using tools like **Wireshark**, **tcpdump**, or **NetFlow**.
* Tracing the source of the attack.
* Capturing relevant screenshots and providing detailed analysis.

**1. Tools Used:**

* **Kali Linux**: For launching the attack and analysis.
* **Wireshark**: Network traffic analysis and packet capturing.
* **tcpdump**: Command-line packet analyzer.
* **Nmap**: For network scanning and identifying vulnerabilities.
* **IP Geolocation Tools**: For tracing the attack source.

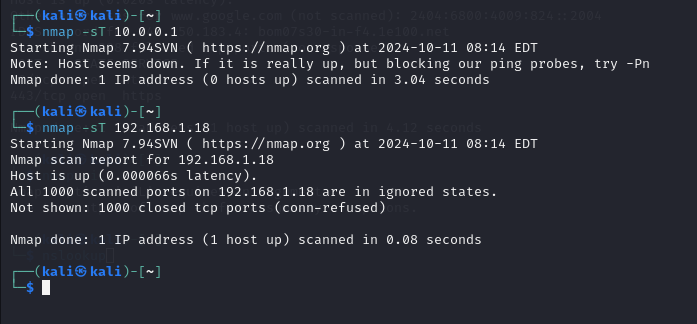
**2. Performing the Attack:**

We will simulate a **Denial of Service (DoS)** attack using Kali Linux's toolkit.

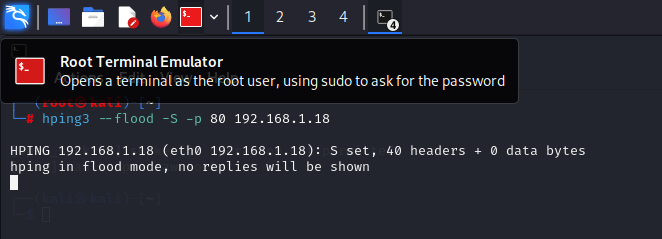
**Step-by-step process:**

1. **Network Scanning (Nmap)**:
   * Use Nmap to identify open ports and vulnerabilities in the target network.

**Screenshot**:



1. **Launch the DoS Attack**:
   * We will use **hping3** to simulate the flood of traffic to the target machine:

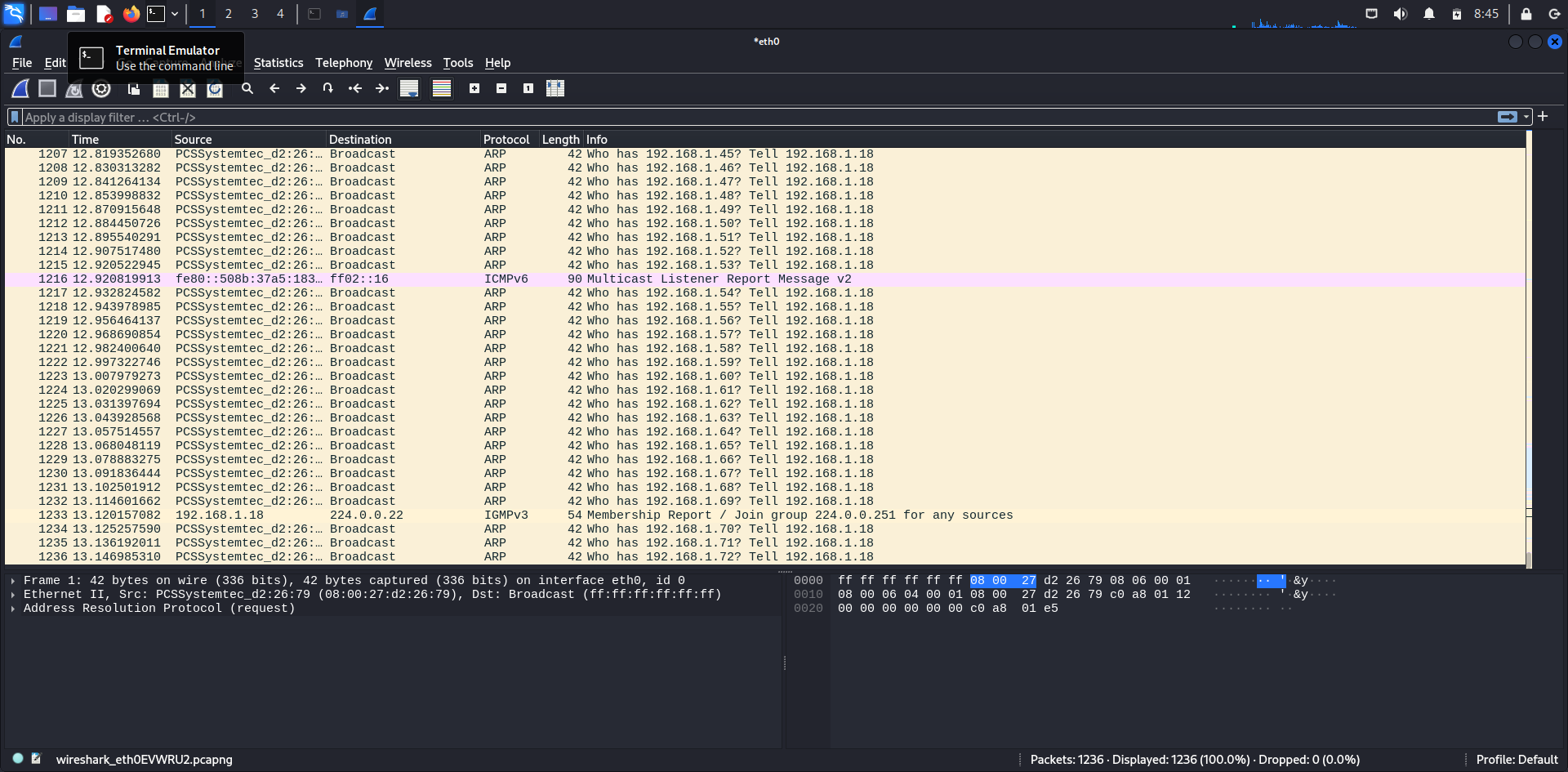
**Screenshot**: 

**3. Network Traffic Analysis:**

After the attack, we use **Wireshark** and **tcpdump** to capture and analyze network traffic.

**Wireshark Analysis:**

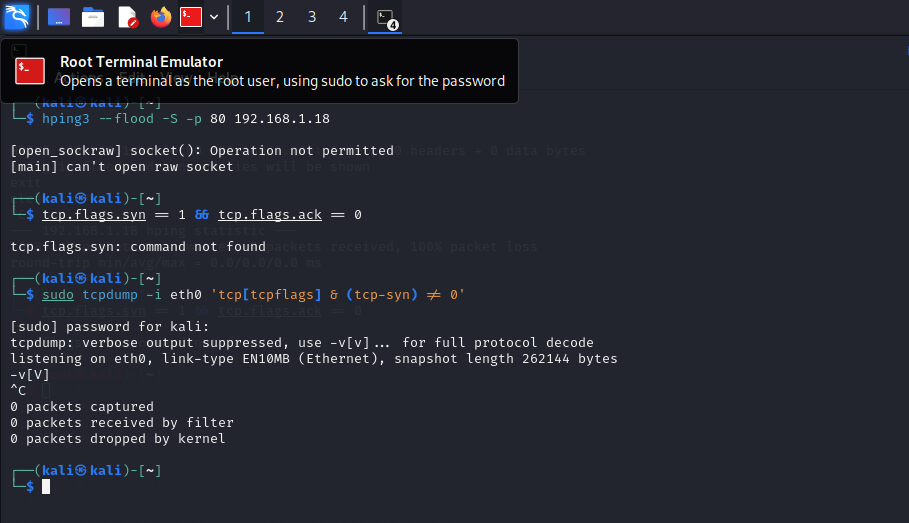
* We set up **Wireshark** to monitor all incoming and outgoing packets from the target machine.
* Filter for **SYN packets** to identify the flood attack:

**Screenshot**:  
Wireshark packet capture highlighting SYN flood attack.

**tcpdump Analysis:**

Using **tcpdump**, we monitor traffic directly from the terminal for further analysis.

**Screenshot**:

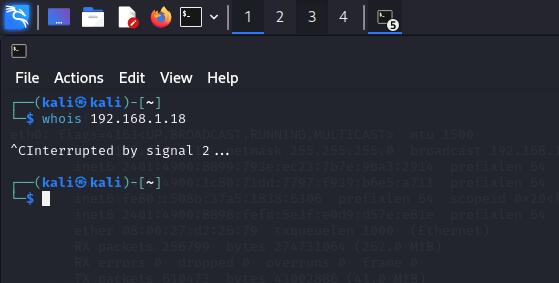
  
tcpdump output showing a high volume of incoming SYN packets.

**4. Tracing the Attack Source:**

After identifying the attack, we trace the source using **Wireshark** and **IP Geolocation Tools**.

1. **Wireshark Analysis**:
   * Use Wireshark to analyze IP addresses generating large amounts of SYN requests.
   * Isolate suspicious IP addresses and trace them using geolocation tools.
2. **IP Geolocation**:
   * Use tools like **iplocation.net** or **whois** to trace the attacker's source.

**Screenshot**:

  
Output of **whois** or IP geolocation tool tracing the attacker's source.

**5. Countermeasures:**

1. **Firewall Configuration**:
   * Configure the firewall to block malicious traffic patterns such as SYN floods.
2. **Rate Limiting**:
   * Implement rate-limiting on network interfaces to prevent flooding.
3. **Intrusion Detection System (IDS)**:
   * Use IDS like **Snort** or **Suricata** to detect and alert on abnormal traffic behavior.
4. **Connection Timeouts**:
   * Reduce connection timeout intervals to drop unacknowledged SYN packets faster.

**6. Conclusion:**

In this project, we successfully simulated a Denial of Service attack, analyzed the resulting network traffic, and traced the source of the attack. The tools and techniques used demonstrated how a DoS attack could overwhelm a target, and effective mitigation strategies were proposed to protect against such attacks in real-world scenarios.

**Screenshots Summary**:

* Nmap scan of the network.
* Launch of a DoS attack using hping3.
* Wireshark and tcpdump analysis.
* Attack source traced using IP geolocation tools.

By understanding these attacks and countermeasures, organizations can improve their defensive capabilities and reduce their vulnerability to network-based attacks.