IP Spoofing Attack

Step 1: Setting Up the Environment

- **Tools Needed:**
  - `hping3`: For crafting and sending packets.
  - Kali Linux (as my attacker machine) ip:192.168.100.5
  - Ubuntu machine (as my target system)with IP :192.168.100.4
  - Wireshark: For packet analysis.
- **Objective:** Craft and send spoofed packets from the attacker machine (Kali) to the victim machine (Ubuntu) to simulate the IP spoofing attack.

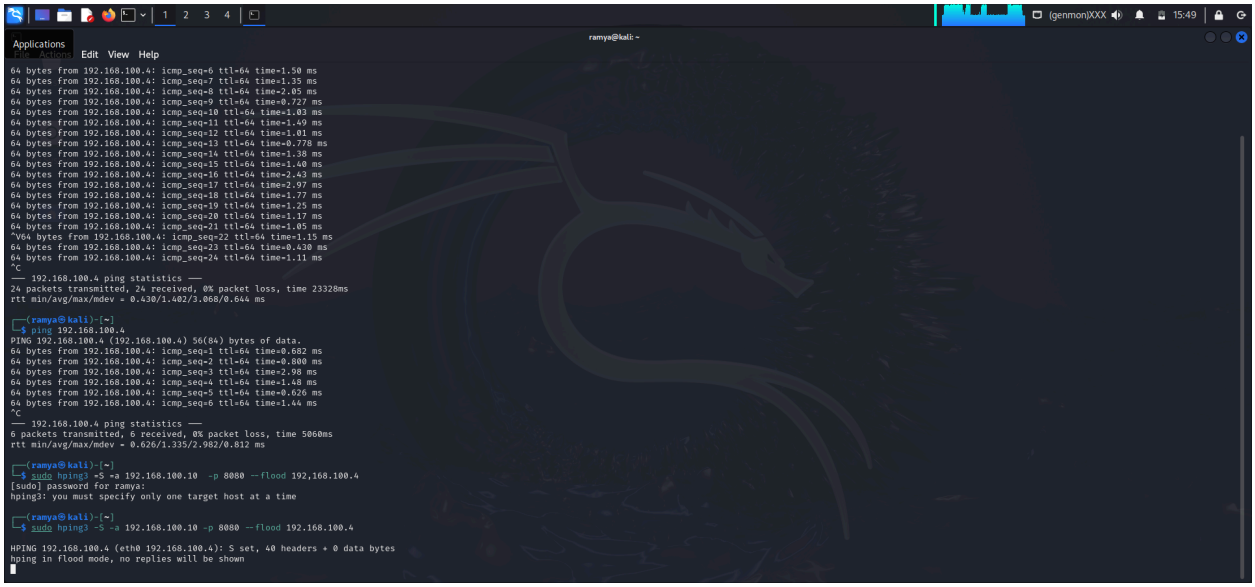
Step 2: Crafting Spoofed Packets Using `hping3`

- **Spoofed Source IP**: The attacker's goal is to send packets to the victim (Ubuntu), with a falsified source ip

command to send TCP packets with a spoofed IP:

hping3 -S -a 192.168.100.10 -p 8080 192.168.100.4

- `-S`: Sends SYN packets (common in DoS attacks).
- `-a [spoofed-ip]`: Specifies the spoofed source IP address.
- `-p 80`: Specifies the destination port (e.g., HTTP).



Step 3: Flooding the Target System with Spoofed Packets

- **Flood Attack**: The attacker sends a large volume of packets to overwhelm the victim system, appearing to come from legitimate sources (spoofed IP addresses).

Example command to flood the target with SYN packets:

Hping3 –flood -S -a 192.168.100.10 -p 8080 192.168.100.4

- `--flood`: Continuously sends packets at a high rate.

Can be monitored this attack very effectively by running a http server in ubuntu

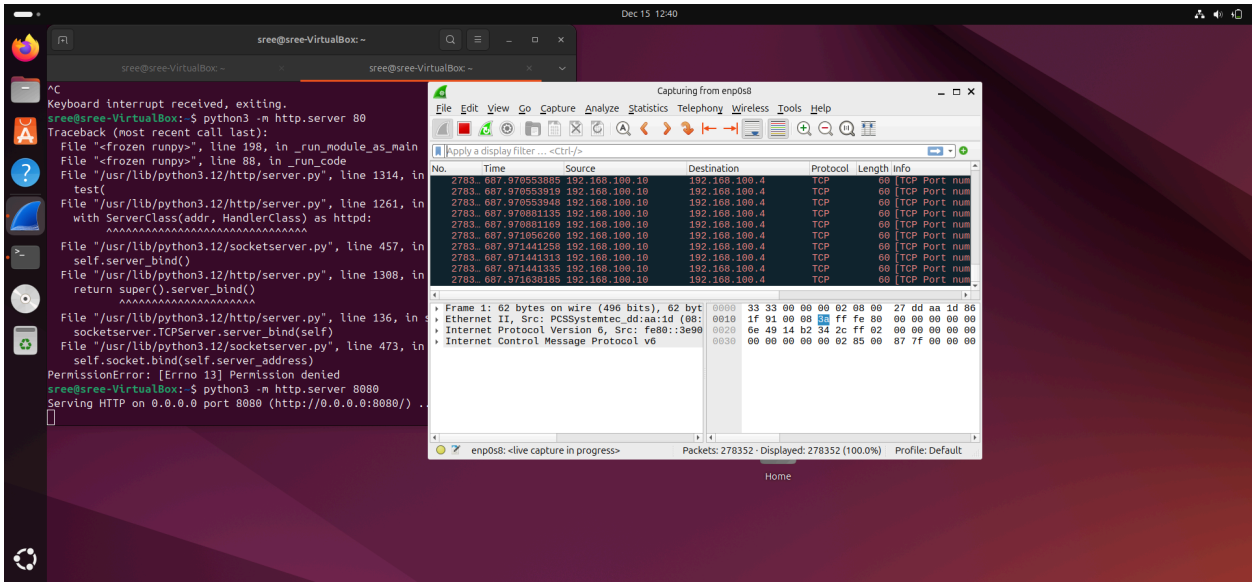
Sudo python3 -m http.server 8080

Step 4: Monitoring the Attack Using Wireshark

- **Wireshark**: Capture the traffic on the victim machine to analyze the incoming spoofed packets.
    - Apply filters to focus on incoming SYN packets:tcp.port == 8080 or
    - `tcp.flags.syn == 1`.
    - Look for anomalous patterns such as source IP addresses that should not be in the traffic.

Step 5: Identifying the Attack

- **Traffic Analysis**: The victim's system will receive packets with source IP addresses that it expects to be internal, but these packets are not genuine. The packet flooding will cause service disruptions.



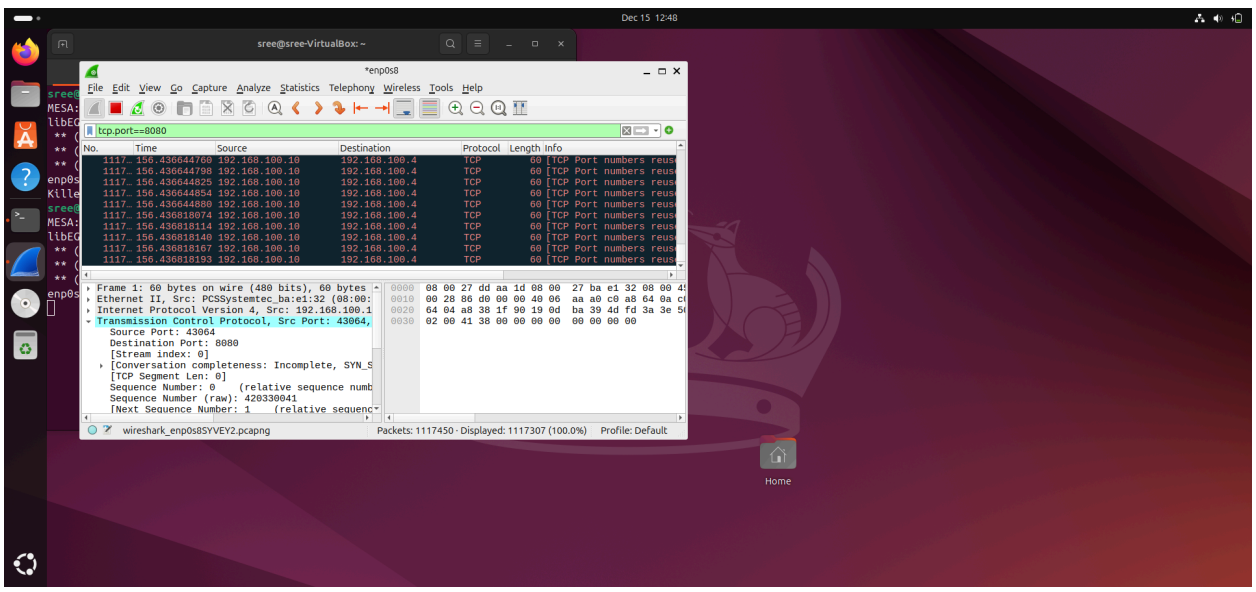


Diagram to Illustrate the Process:

```
+--------------------+          +--------------------+

|  Attacker (Kali)  |          |  Target HTTP Server  |

|  (Uses hping3)    | --->     |  (Ubuntu with HTTP   |
```

```
|   - Sends spoofed    |             |   server running)    |
|    SYN packets      |             |   (Port 8080)        |
+---------------------+             +---------------------+
       |                            |
       |                            |
       |  Floods SYN packets to         |
       |  target server, appearing      |
       |  from a spoofed IP address      |
       |                            |
+---------------------+             +---------------------+
|  Wireshark Capture  | <--- Captures |   Server Disruption  |
|  - Analyzes spoofed  |   and logs    |   - Server may       |
|    traffic           |   flooding    |     experience slow  |
|    (TCP/SYN)         |   or denial   |     response or crash|
+---------------------+             +---------------------+
       |
       |    Defensive Measures:
       |    - Use `iptables` to block
       |      spoofed traffic
+---------------------+
|   Mitigation (iptables)|
|   - Blocks spoofed IP |
|   - Filters traffic   |
+---------------------+
```