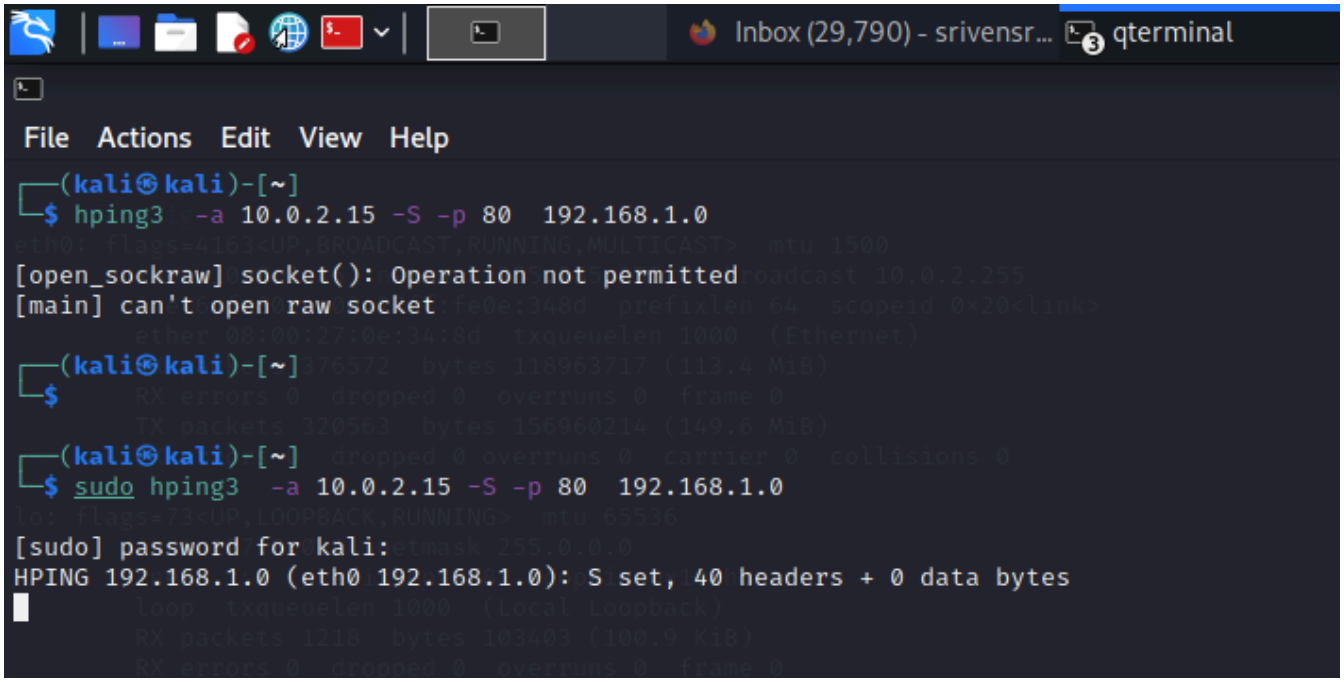
IP Spoofing Attack on GreenValley University

Tools and Steps Involved:

1. **Scanning the Network**:
    - **Tool:** Nmap
    - **Purpose:** Identify live hosts and open ports within the university's network to find potential targets.
    - **Command:** `nmap -sP 192.168.1.0/24`
    - `Nmap -p 1-65535 192.168.1.0`

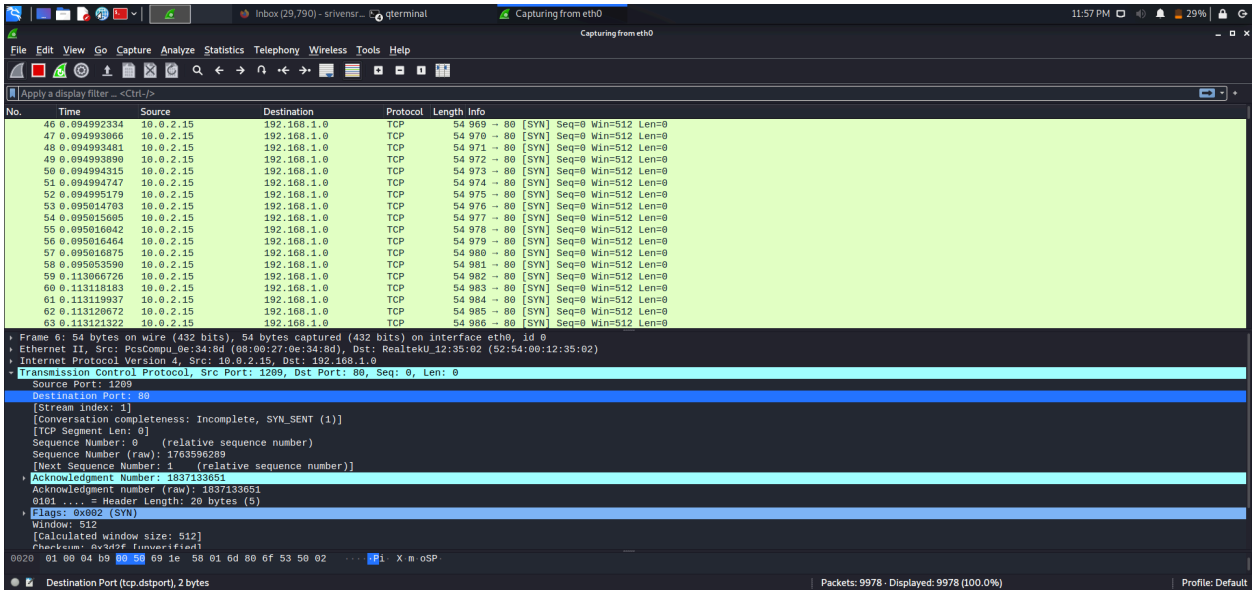


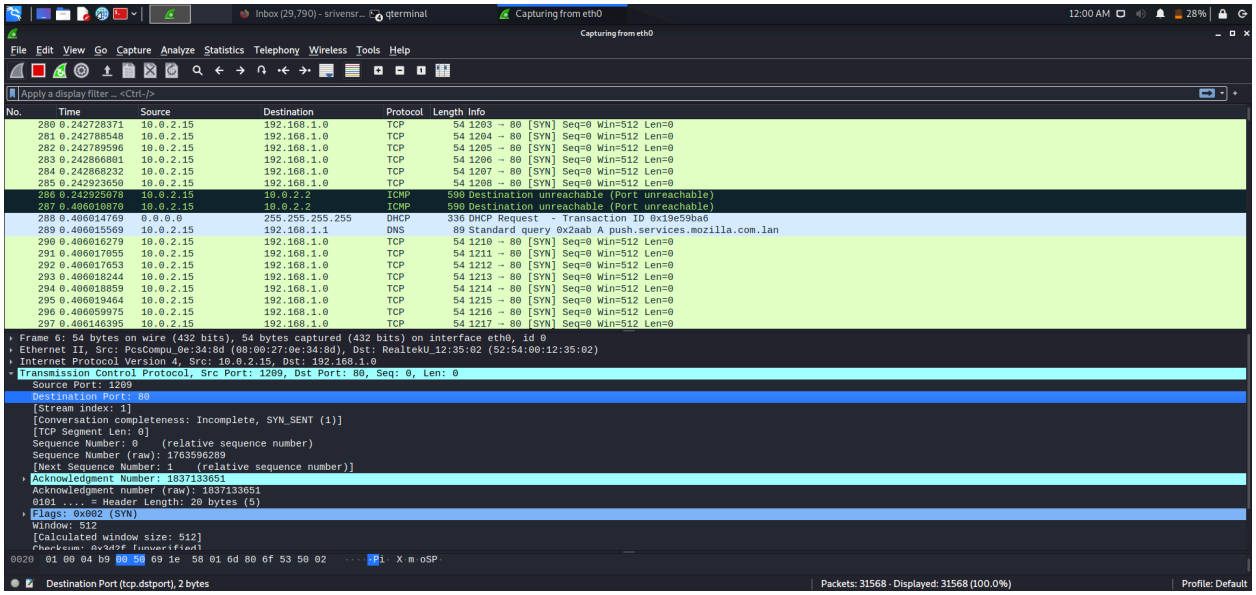
Crafting Spoofed Packets:

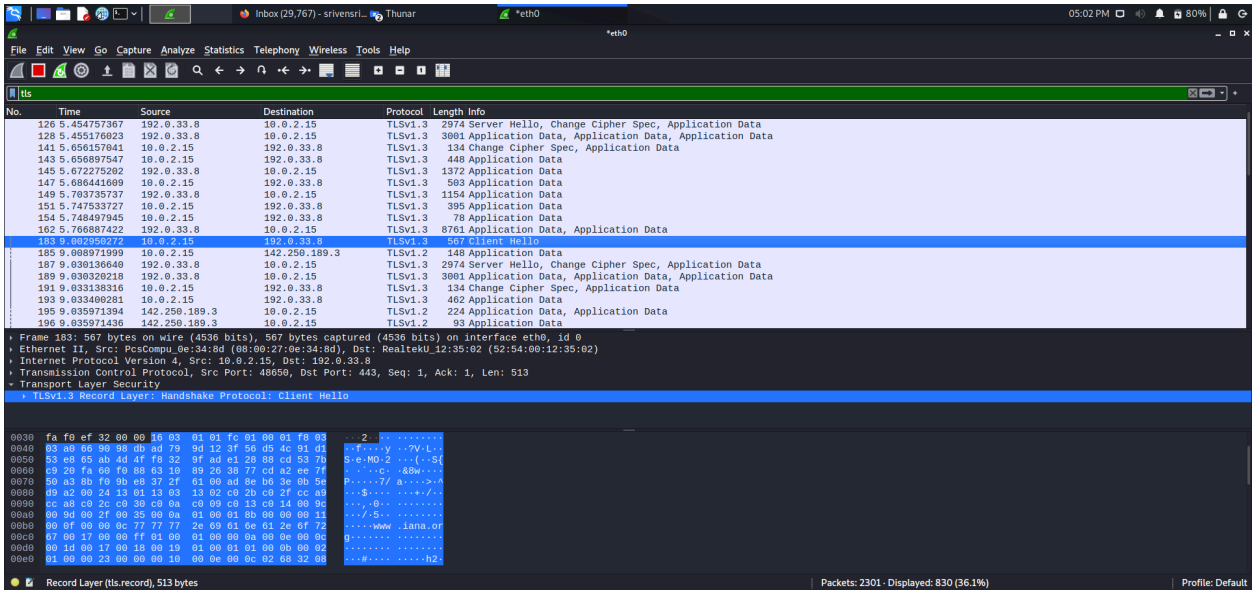
- **Tool:** hping3
- **Purpose:** Generate and send spoofed packets to simulate the attack by using the IP address of the university's servers.

Traffic Monitoring and Logging:

- **Tool:** Wireshark
- **Purpose:** Monitor and capture network traffic to observe the flow of spoofed packets and identify abnormalities.
- **Action:** Capture network traffic on the target system and look for unusual patterns.


Inbox (29,790) - srivensr... qterminal Capturing from eth0 11:57 PM 29%
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
46 0.094992334 10.0.2.15 192.168.1.0 TCP 54 969 → 80 [SYN] Seq=0 Win=512 Len=0
47 0.094993066 10.0.2.15 192.168.1.0 TCP 54 970 → 80 [SYN] Seq=0 Win=512 Len=0
48 0.094993481 10.0.2.15 192.168.1.0 TCP 54 971 → 80 [SYN] Seq=0 Win=512 Len=0
49 0.094993890 10.0.2.15 192.168.1.0 TCP 54 972 → 80 [SYN] Seq=0 Win=512 Len=0
50 0.094994315 10.0.2.15 192.168.1.0 TCP 54 973 → 80 [SYN] Seq=0 Win=512 Len=0
51 0.094994747 10.0.2.15 192.168.1.0 TCP 54 974 → 80 [SYN] Seq=0 Win=512 Len=0
52 0.094995179 10.0.2.15 192.168.1.0 TCP 54 975 → 80 [SYN] Seq=0 Win=512 Len=0
53 0.095014703 10.0.2.15 192.168.1.0 TCP 54 976 → 80 [SYN] Seq=0 Win=512 Len=0
54 0.095015605 10.0.2.15 192.168.1.0 TCP 54 977 → 80 [SYN] Seq=0 Win=512 Len=0
55 0.095016042 10.0.2.15 192.168.1.0 TCP 54 978 → 80 [SYN] Seq=0 Win=512 Len=0
56 0.095016464 10.0.2.15 192.168.1.0 TCP 54 979 → 80 [SYN] Seq=0 Win=512 Len=0
57 0.095016875 10.0.2.15 192.168.1.0 TCP 54 980 → 80 [SYN] Seq=0 Win=512 Len=0
58 0.095053590 10.0.2.15 192.168.1.0 TCP 54 981 → 80 [SYN] Seq=0 Win=512 Len=0
59 0.113066726 10.0.2.15 192.168.1.0 TCP 54 982 → 80 [SYN] Seq=0 Win=512 Len=0
60 0.113118183 10.0.2.15 192.168.1.0 TCP 54 983 → 80 [SYN] Seq=0 Win=512 Len=0
61 0.113119937 10.0.2.15 192.168.1.0 TCP 54 984 → 80 [SYN] Seq=0 Win=512 Len=0
62 0.113120672 10.0.2.15 192.168.1.0 TCP 54 985 → 80 [SYN] Seq=0 Win=512 Len=0
63 0.113121322 10.0.2.15 192.168.1.0 TCP 54 986 → 80 [SYN] Seq=0 Win=512 Len=0
Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.0
Transmission Control Protocol, Src Port: 1209, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1209
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1763596289
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1837133651
Acknowledgment number (raw): 1837133651
0101 .... = Header Length: 20 bytes (5)
Flags: 0x002 (SYN)
Window: 512
[Calculated window size: 512]
0020 01 00 04 b9 00 50 69 1e 58 01 6d 80 6f 53 50 02 ·····Pi· X·m·oSP·
Destination Port (tcp.dstport), 2 bytes
Packets: 9978 · Displayed: 9978 (100.0%)
Profile: Default

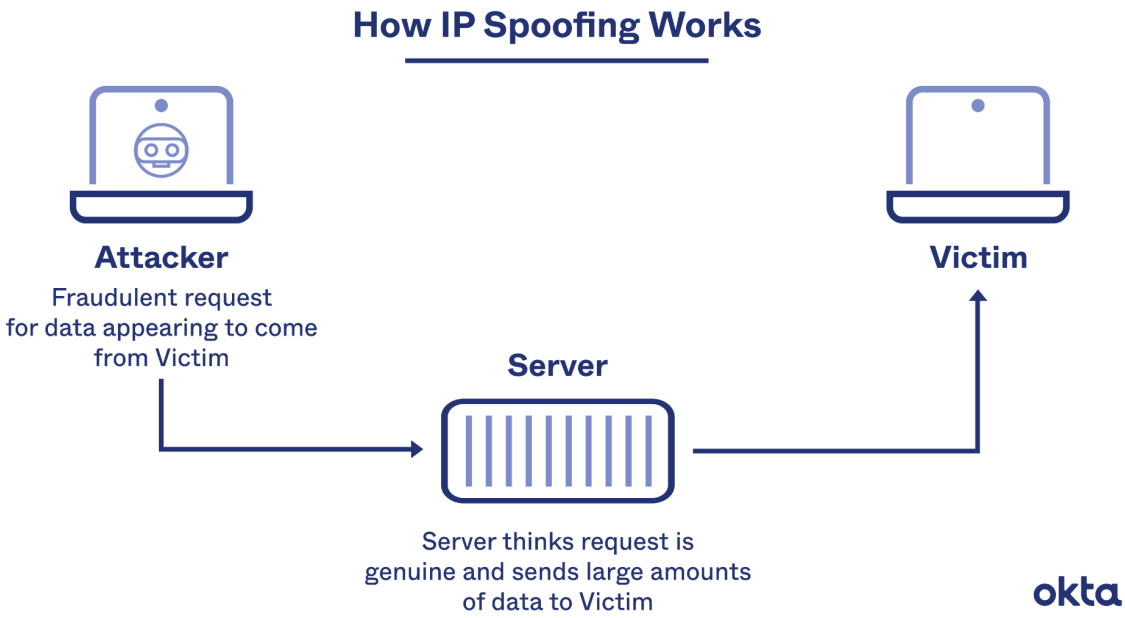

Inbox (29,790) - srivensr... qterminal Capturing from eth0 12:00 AM 28%
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
280 0.242728371 10.0.2.15 192.168.1.0 TCP 54 1203 → 80 [SYN] Seq=0 Win=512 Len=0
281 0.242788548 10.0.2.15 192.168.1.0 TCP 54 1204 → 80 [SYN] Seq=0 Win=512 Len=0
282 0.242789596 10.0.2.15 192.168.1.0 TCP 54 1205 → 80 [SYN] Seq=0 Win=512 Len=0
283 0.242866801 10.0.2.15 192.168.1.0 TCP 54 1206 → 80 [SYN] Seq=0 Win=512 Len=0
284 0.242868232 10.0.2.15 192.168.1.0 TCP 54 1207 → 80 [SYN] Seq=0 Win=512 Len=0
285 0.242923650 10.0.2.15 192.168.1.0 TCP 54 1208 → 80 [SYN] Seq=0 Win=512 Len=0
286 0.242925078 10.0.2.15 10.0.2.2 ICMP 590 Destination unreachable (Port unreachable)
287 0.406010870 10.0.2.15 10.0.2.2 ICMP 590 Destination unreachable (Port unreachable)
288 0.406014769 0.0.0.0 255.255.255.255 DHCP 336 DHCP Request - Transaction ID 0x19e59ba6
289 0.406015569 10.0.2.15 192.168.1.1 DNS 89 Standard query 0x2aab A push.services.mozilla.com.lan
290 0.406016279 10.0.2.15 192.168.1.0 TCP 54 1210 → 80 [SYN] Seq=0 Win=512 Len=0
291 0.406017055 10.0.2.15 192.168.1.0 TCP 54 1211 → 80 [SYN] Seq=0 Win=512 Len=0
292 0.406017653 10.0.2.15 192.168.1.0 TCP 54 1212 → 80 [SYN] Seq=0 Win=512 Len=0
293 0.406018244 10.0.2.15 192.168.1.0 TCP 54 1213 → 80 [SYN] Seq=0 Win=512 Len=0
294 0.406018859 10.0.2.15 192.168.1.0 TCP 54 1214 → 80 [SYN] Seq=0 Win=512 Len=0
295 0.406019464 10.0.2.15 192.168.1.0 TCP 54 1215 → 80 [SYN] Seq=0 Win=512 Len=0
296 0.406059975 10.0.2.15 192.168.1.0 TCP 54 1216 → 80 [SYN] Seq=0 Win=512 Len=0
297 0.406146395 10.0.2.15 192.168.1.0 TCP 54 1217 → 80 [SYN] Seq=0 Win=512 Len=0
Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.1.0
Transmission Control Protocol, Src Port: 1209, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1209
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1763596289
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1837133651
Acknowledgment number (raw): 1837133651
0101 .... = Header Length: 20 bytes (5)
Flags: 0x002 (SYN)
Window: 512
[Calculated window size: 512]
0020 01 00 04 b9 00 50 69 1e 58 01 6d 80 6f 53 50 02 ·····Pi· X·m·oSP·
Destination Port (tcp.dstport), 2 bytes
Packets: 31568 · Displayed: 31568 (100.0%)
Profile: Default



When monitoring for IP spoofing in Wireshark, focus on the following

ARP Requests/Replies: Examine ARP traffic for mismatched IP and MAC addresses. If you see ARP replies that don't match the legitimate MAC address of an IP, this could indicate IP spoofing.

1. **Abnormal Traffic Patterns**: In the images above we see that there is high volumes of traffic from a single IP address or a pattern of SYN requests without corresponding SYN-ACK responses. This could indicate a SYN flood attack using spoofed IP addresses.
2. **Duplicate IP Addresses**: We see that there are packets with duplicate IP addresses coming from different MAC addresses. This is a clear sign of IP spoofing.
3. **DNS Response Traffic**: We monitored DNS traffic for responses from unexpected IP addresses. Spoofed DNS responses can be a part of a DNS spoofing attack. And also saw that there was activity related to DHCP requests.



How IP spoofing works and explaining the diagram above

IP spoofing, also known as internet protocol spoofing, entails impersonation. By manipulating the address data in the IP header, a hacker can deceive a system into thinking it is coming from a reliable source.

Devastating attacks, such as man-in-the-middle and denial of service (DOS), are carried out by people using IP spoofing. However, there are other acceptable applications for this technique, particularly if you're about to launch a new website.

The hacker impersonates like a client to the server and the server sends large amounts of requests that the client is requesting. This is how MITM and DOS attacks happen.