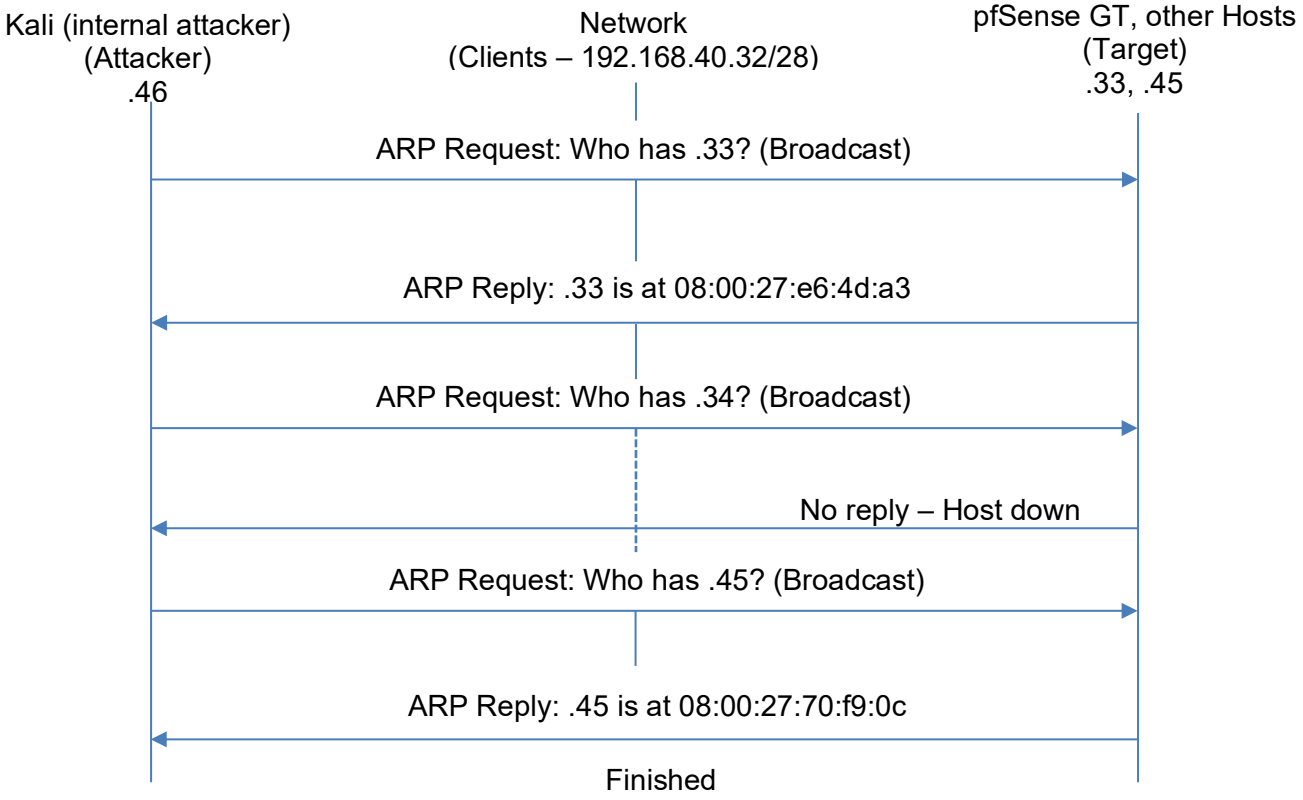
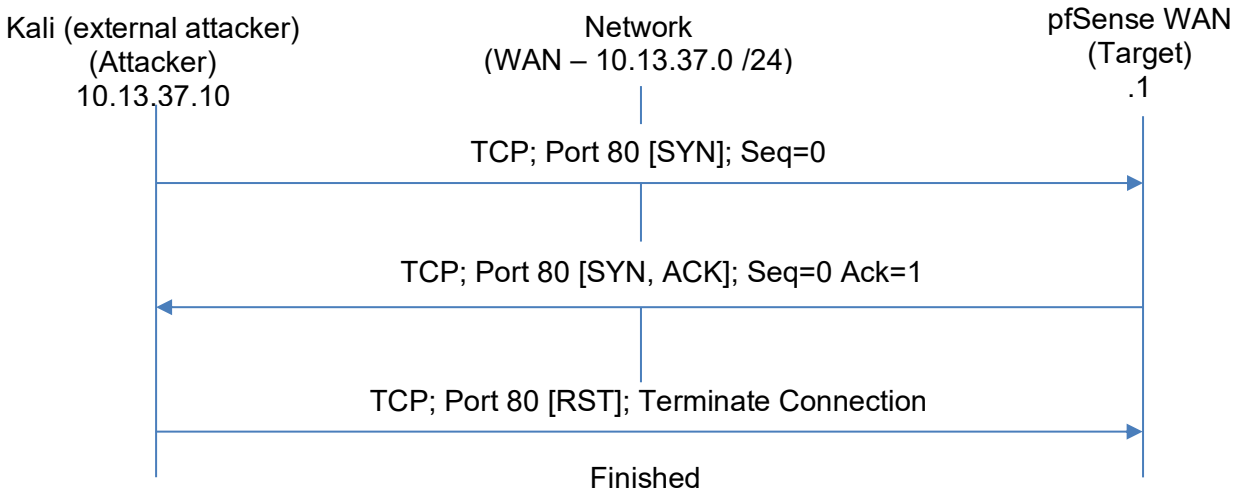
Attack Flowdiagrams

Attack #1: Reconnaissance – ARP Sweep



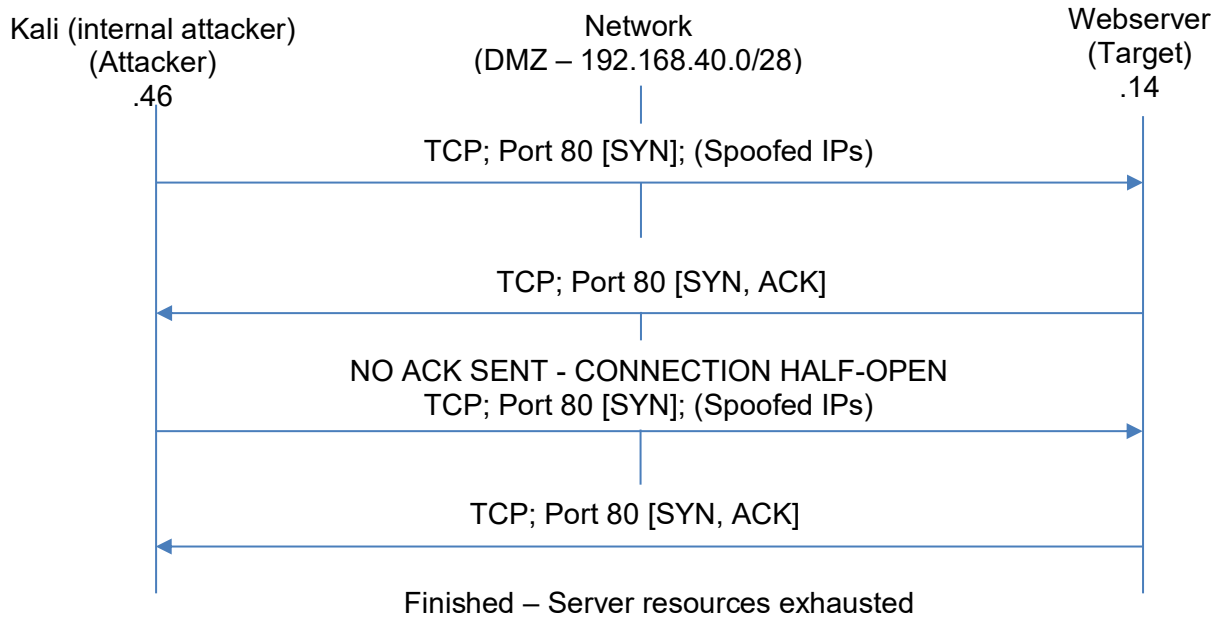
Explanation: The attacker (.46) sends sequential ARP Broadcast requests to the network. The active hosts (pfSense Gateway at .33 and Kali SNM at .45) respond with their MAC address, allowing the attacker to map the network.

Attack #2: Reconnaissance – TCP SYN Scan



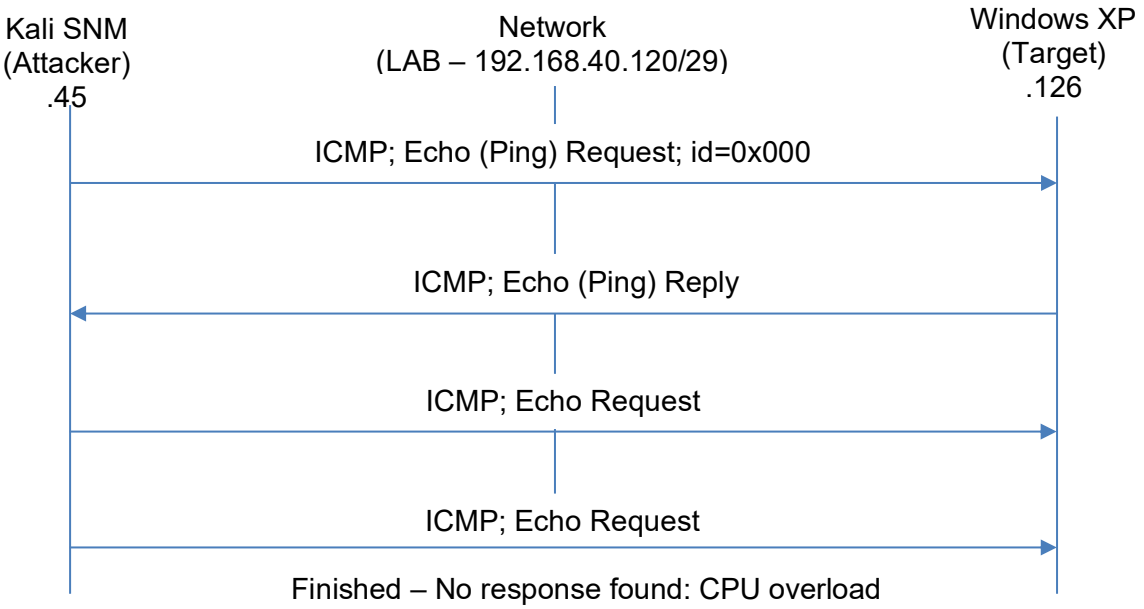
Explanation: The attacker (.10) initiates a handshake with a SYN packet. The target (.1) replies with SYN-ACK, proving the port is open. Instead of completing the connection with an ACK, the attacker sends a RST packet to close it immediately, avoiding a full log entry on the web server application

Attack #3: Denial of Service – TCP SYN Flood



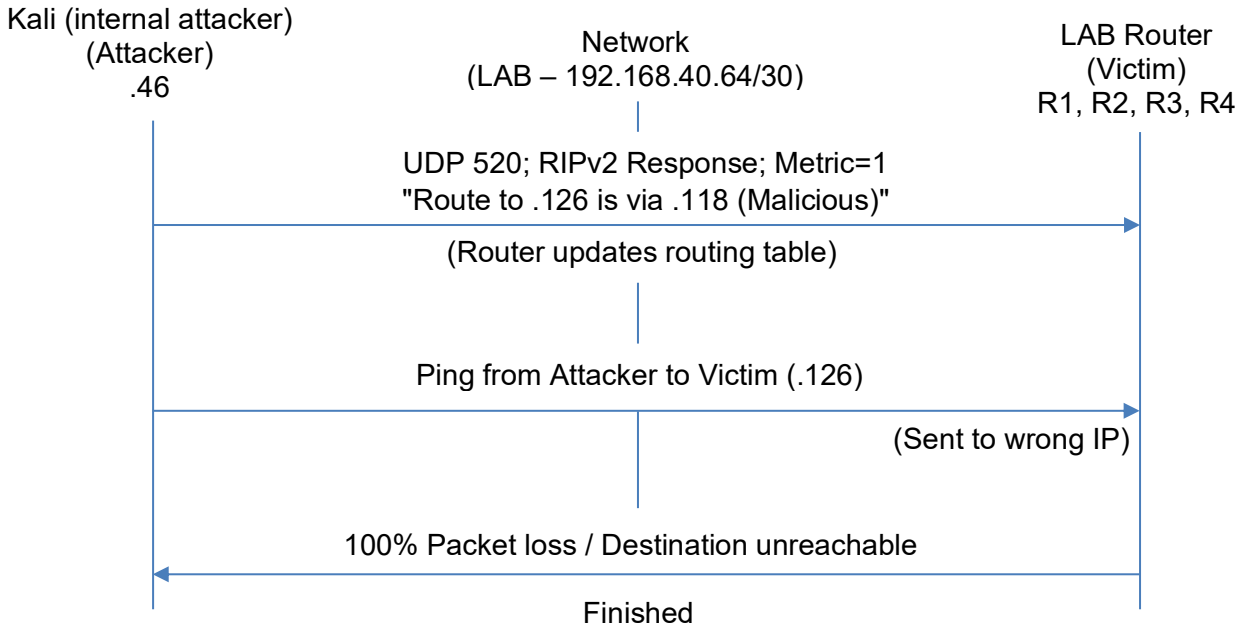
Explanation: The attacker sends a high volume of SYN packets to the target (.14). The server replies with SYN-ACK and waits for a final ACK that never comes. This creates "half-open" connections that fill up the state table, making the server unavailable to actual users.

Attack #4: Denial of Service – ICMP Flood



Explanation: The attacker (.45) sends thousands of ICMP Echo Requests in a short burst. The victim (.126) initially tries to reply, but eventually, the traffic volume overwhelms its processing power, leading to packet loss and unresponsiveness (Wireshark: "no response found").

Attack #5: RIP Attack (Routing)



Explanation: The attacker (.46) exploits the lack of authentication in RIPv2 to send a fake routing update packet. This packet tells the routers that there is a "better" route to the victim (.126) via a different hop (.118). The routers accept this false information, breaking the connectivity to the victim (confirmed by 100% packet loss).