## Lab 16: Hping for Security Auditing and Testing of Network Devices

**Scenario**

CyberSecure Labs, a trusted cybersecurity consulting firm, has been contracted by NetWave Enterprises, a regional Internet Service Provider (ISP), to perform a security audit of its core network infrastructure. The assessment focuses on testing the resilience of routers and firewalls against common network-based attacks that could potentially disrupt service availability or expose sensitive configuration data. During the preliminary review, concerns are raised regarding the organization’s exposure to Denial-of-Service (DoS) attempts and packet manipulation attacks. Since the ISP relies heavily on continuous uptime and secure communication for its subscribers, any network disruption could severely impact both business operations and customer trust. To address these risks, the consulting team decides to employ Hping, a powerful command-line tool used for crafting custom TCP/IP packets, to test how the devices respond to different types of network probes, floods, and port scans under controlled conditions.

**Solution**

As a certified cybersecurity practitioner, your task is to utilize Hping to simulate various packet-based attacks and auditing techniques on the target network devices. Begin by using Hping to perform TCP and UDP port scanning to identify open services and validate firewall filtering rules. Next, simulate a SYN flood attack to evaluate the device’s capacity to handle high volumes of half-open connections without crashing or becoming unresponsive. Additionally, use Hping to send malformed packets to test how effectively the devices handle unexpected or irregular traffic patterns. Throughout the simulation, monitor the responses of routers and firewalls to assess whether security controls such as Intrusion Prevention Systems (IPS), rate limiting, and packet filtering are functioning as intended. Upon identifying weaknesses, recommend hardening measures such as enabling rate-limiting policies, configuring Access Control Lists (ACLs) to restrict unauthorized traffic, and applying firmware updates to address known vulnerabilities. This exercise demonstrates how Hping can be leveraged for both offensive testing and defensive validation, ensuring that critical network devices remain resilient against real-world threats while maintaining reliable service availability.

**Note:** In this lab, we used the **192.168.2.108** IP address as the target machine. Do not use this IP address when performing this lab; use your IP address.

|  |
| --- |
| 1. Hping3 comes pre-loaded in ParrotOS. Use the **hping3 –A Target\_IP\_Address-p 80 -c 5** command to ping the target.  **-A flag** specifies the ACK flag    The **ACK probe packet** is sent to the target. An **RST Response** from the target means the port is closed, and no response means the port is filtered.  2. Use the **hping3 -8 0-100 -S Target\_IP\_Address-V** command to ping the target.  **-8 flag** specifies the scan mode  **0-100** is the range of ports to be scanned  **-S flag** specifies the SYN scan  **-V flag** specifies the verbose mode    It shows the ports and services running on them.  3. Use the **hping3 -F -P -U Target\_IP\_Address-p 80 -c 5** command to send five packets to port 80 of the target with the FIN, PUSH, and URG flags set on packets.  **-F flag** sets the FIN flag  **-P flag** sets the PUSH flag  **-U flag** sets the URG flag  **-p flag** specifies the port number  **-c flag** specifies the packet count    If the port is open, you will receive the response. You will get an RST response if the port is closed. The port is open in this case because the packets transmitted and received are the same.  4. Use the **hping3 --scan 0-100 -S Target\_IP\_Address-V** command to scan the target for a hundred ports with the verbose mode.  **-S flag** sets the SYN flag  **-V flag** enables the verbose mode  **--scan flag** specifies the port range from 0 to 100    If the port is open, you will receive a **SYN+ACK** response in the TCP Stealth scan.  5. Use the **hping3 -1 Target\_IP\_Address-c 5 -p 80** command to ping port 80 of the target with a packet count of five.  **-1 flag** specifies the ICMP ping scan  **-c flag** specifies the packet count  **-p flag** specifies the port number |