Network Analysis with Hping3

Author: Ayesha Nadeem | Ethical Hacker

Lab Objective: The primary objective of this lab is to develop proficiency in using Hping3 for advanced network packet crafting and analysis. Participants will learn to perform stealth reconnaissance, including SYN and FIN scans, and execute custom packet manipulation for firewall testing and protocol analysis. This hands-on exercise is designed to simulate authorized security assessments to evaluate network perimeter defenses and diagnose complex network issues.

Date: August 20th, 2025

Table of Contents

1.0. Executive Summary

This document outlines a practical exercise conducted to evaluate the functionality and application of hping3, a advanced network packet crafting and analysis tool. The exercise involved executing a series of fundamental commands to demonstrate its capabilities in network reconnaissance, diagnostics, and protocol manipulation. The results confirm hping3's efficacy in conducting stealth scans, path analysis, and TCP flag manipulation, validating its critical role in security auditing and network engineering.

2.0. Introduction to Hping3

2.1. Definition

Hping3 is a sophisticated command-line utility used for crafting, sending, and analyzing custom TCP/IP packets. It extends beyond the capabilities of standard ICMP-based ping tools by supporting a variety of protocols including TCP, UDP, ICMP, and RAW-IP, providing granular control over packet headers and payloads.

2.2. Core Purpose and Applications

Hping3 is designed for advanced network diagnostics and security assessment. Its primary applications include:

- **Firewall Testing:** Evaluating rule sets by simulating traffic with specific packet flags.
- **Stealth Port Scanning:** Conducting reconnaissance using low-noise techniques like SYN scans.
- **Packet Crafting:** Constructing custom packets for deep protocol analysis and testing.
- **Path Discovery:** Performing traceroute operations using TCP or UDP to bypass ICMP restrictions.
- **Operating System Fingerprinting:** Inferring a host's OS based on its TCP/IP stack response.
- **Load Testing:** Simulating Denial-of-Service (DoS) conditions to assess system resilience.

3.0. Lab Objective

The primary objective of this lab was to utilize hping3 to perform a stealth TCP SYN scan on a target host to identify open ports, simulating the initial reconnaissance phase of a penetration test.

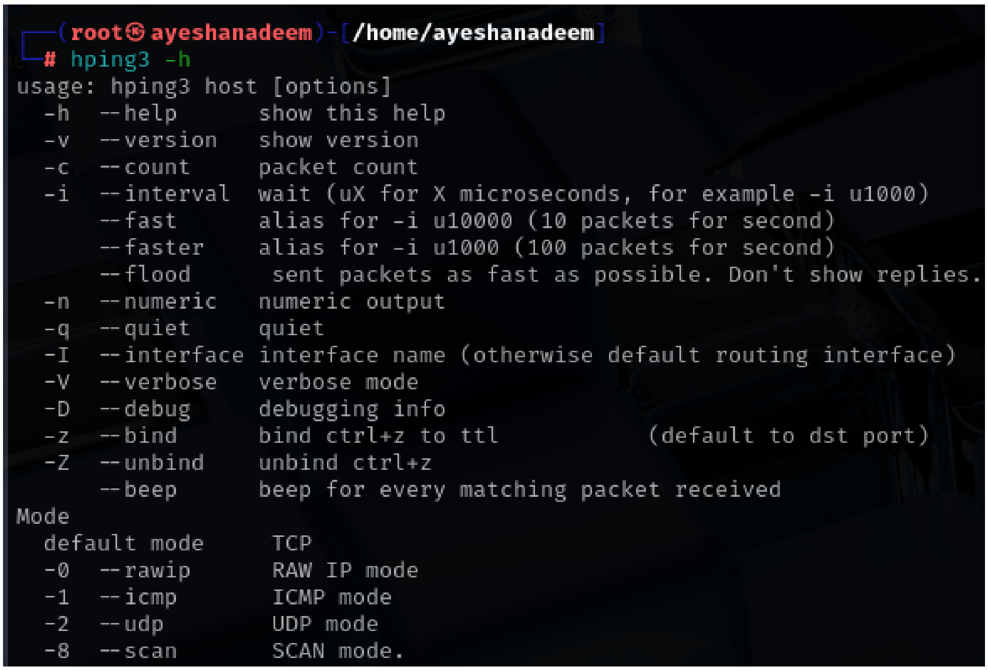
3.1. Lab Requirements

- **Platform:** Kali Linux (or any Linux distribution with hping3 installed).
- **Target:** A designated host (virtual machine or localhost).
- **Permissions:** Root privileges necessary for raw socket manipulation.

4.0. Initial Lab Setup & Verifications

4.1. Help Menu

Command 1 hping3 -h

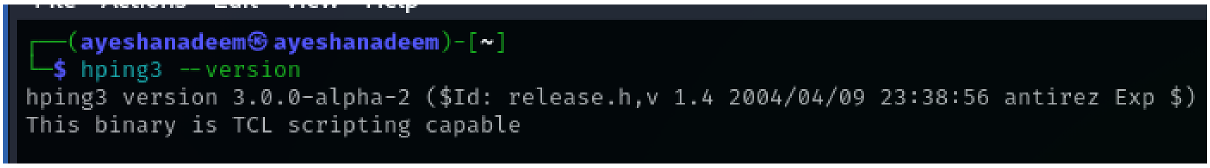


```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
  -8  --scan       SCAN mode.
```

Shows the detail of switched (option) you can use in your commands.

4.2. Verfiy version

Command: hping3 --version



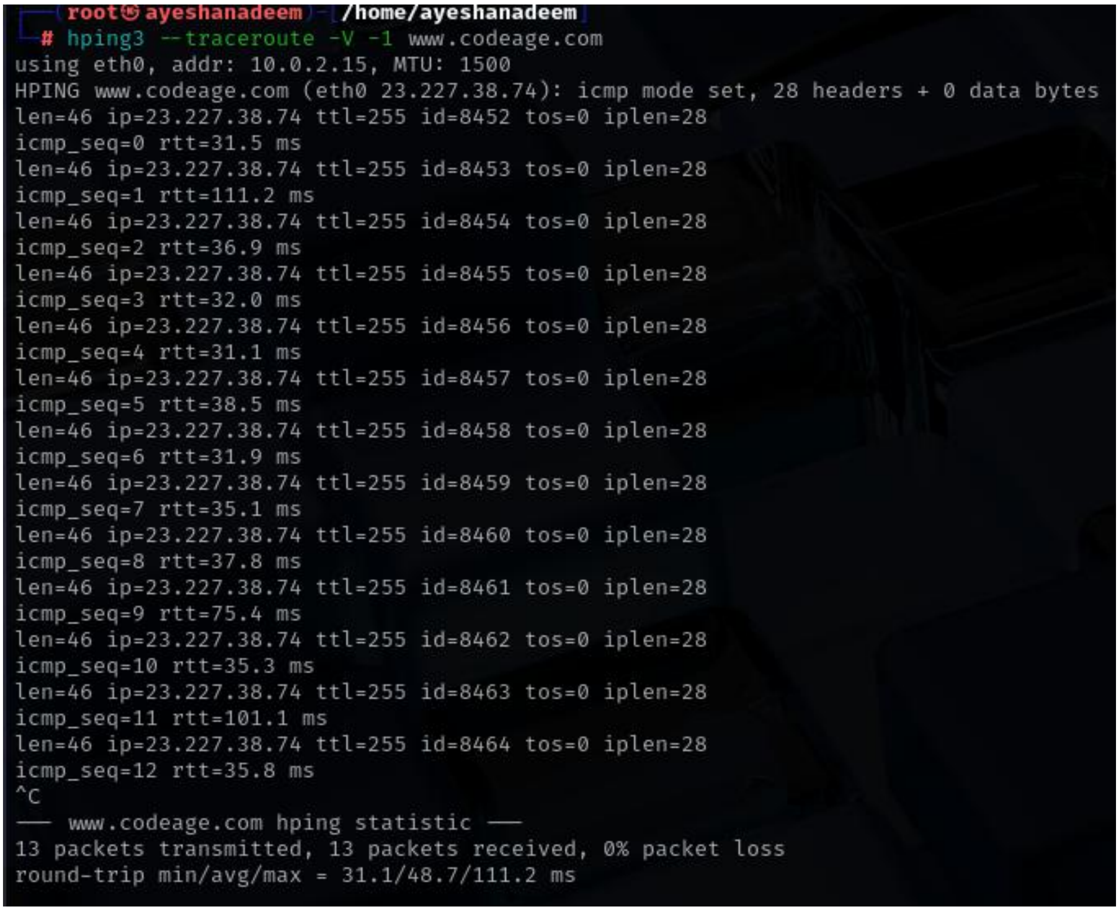
```
┌──(ayeshanadeem㉿ayeshanadeem)-[~]
└─$ hping3 --version
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
```

So yes it shows I have latest version.

5.0. Methodology: Practical Commands

5.1. ICMP Traceroute

Command 2: hping3 --traceroute -V -1 www.codeage.com



```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 --traceroute -V -1 www.codeage.com
using eth0, addr: 10.0.2.15, MTU: 1500
HPING www.codeage.com (eth0 23.227.38.74): icmp mode set, 28 headers + 0 data bytes
len=46 ip=23.227.38.74 ttl=255 id=8452 tos=0 iplen=28
icmp_seq=0 rtt=31.5 ms
len=46 ip=23.227.38.74 ttl=255 id=8453 tos=0 iplen=28
icmp_seq=1 rtt=111.2 ms
len=46 ip=23.227.38.74 ttl=255 id=8454 tos=0 iplen=28
icmp_seq=2 rtt=36.9 ms
len=46 ip=23.227.38.74 ttl=255 id=8455 tos=0 iplen=28
icmp_seq=3 rtt=32.0 ms
len=46 ip=23.227.38.74 ttl=255 id=8456 tos=0 iplen=28
icmp_seq=4 rtt=31.1 ms
len=46 ip=23.227.38.74 ttl=255 id=8457 tos=0 iplen=28
icmp_seq=5 rtt=38.5 ms
len=46 ip=23.227.38.74 ttl=255 id=8458 tos=0 iplen=28
icmp_seq=6 rtt=31.9 ms
len=46 ip=23.227.38.74 ttl=255 id=8459 tos=0 iplen=28
icmp_seq=7 rtt=35.1 ms
len=46 ip=23.227.38.74 ttl=255 id=8460 tos=0 iplen=28
icmp_seq=8 rtt=37.8 ms
len=46 ip=23.227.38.74 ttl=255 id=8461 tos=0 iplen=28
icmp_seq=9 rtt=75.4 ms
len=46 ip=23.227.38.74 ttl=255 id=8462 tos=0 iplen=28
icmp_seq=10 rtt=35.3 ms
len=46 ip=23.227.38.74 ttl=255 id=8463 tos=0 iplen=28
icmp_seq=11 rtt=101.1 ms
len=46 ip=23.227.38.74 ttl=255 id=8464 tos=0 iplen=28
icmp_seq=12 rtt=35.8 ms
^C
--- www.codeage.com hping statistic ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 31.1/48.7/111.2 ms
```

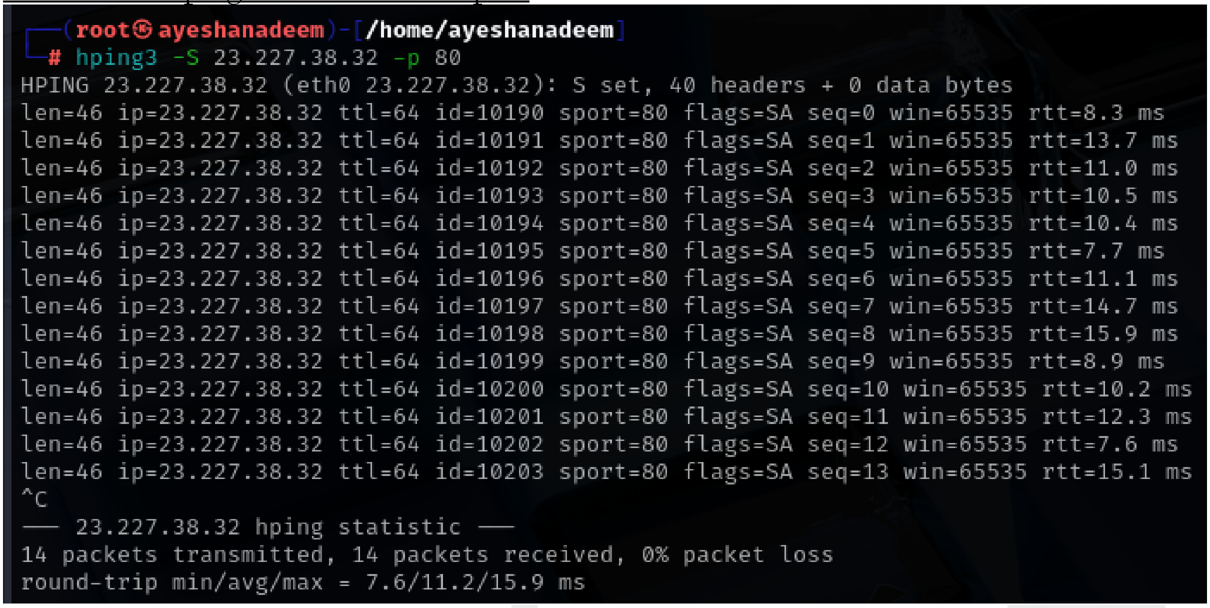
Purpose: To perform a verbose (-V) traceroute to the target domain (www.codeage.com) using ICMP mode (-1) instead of the standard TCP.

Output Analysis: The command successfully mapped the path to the target, displaying each hop's response time (RTT). The output shows 13 packets were transmitted and received with 0% packet loss and an average RTT of 48.7 ms, indicating a stable connection.

Note: For packet flow analysis turn on wore shark as well.

5.2. TCP SYN Scan on Port 80

Command 3:hping3 -S 23.227.38.32 -p 80



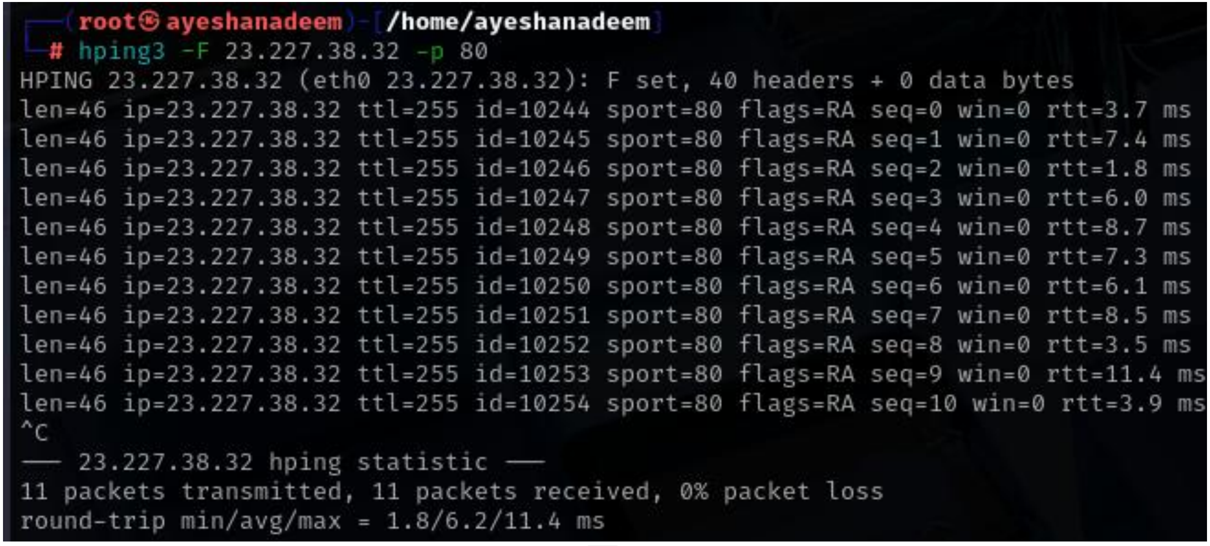
```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -S 23.227.38.32 -p 80
HPING 23.227.38.32 (eth0 23.227.38.32): S set, 40 headers + 0 data bytes
len=46 ip=23.227.38.32 ttl=64 id=10190 sport=80 flags=SA seq=0 win=65535 rtt=8.3 ms
len=46 ip=23.227.38.32 ttl=64 id=10191 sport=80 flags=SA seq=1 win=65535 rtt=13.7 ms
len=46 ip=23.227.38.32 ttl=64 id=10192 sport=80 flags=SA seq=2 win=65535 rtt=11.0 ms
len=46 ip=23.227.38.32 ttl=64 id=10193 sport=80 flags=SA seq=3 win=65535 rtt=10.5 ms
len=46 ip=23.227.38.32 ttl=64 id=10194 sport=80 flags=SA seq=4 win=65535 rtt=10.4 ms
len=46 ip=23.227.38.32 ttl=64 id=10195 sport=80 flags=SA seq=5 win=65535 rtt=7.7 ms
len=46 ip=23.227.38.32 ttl=64 id=10196 sport=80 flags=SA seq=6 win=65535 rtt=11.1 ms
len=46 ip=23.227.38.32 ttl=64 id=10197 sport=80 flags=SA seq=7 win=65535 rtt=14.7 ms
len=46 ip=23.227.38.32 ttl=64 id=10198 sport=80 flags=SA seq=8 win=65535 rtt=15.9 ms
len=46 ip=23.227.38.32 ttl=64 id=10199 sport=80 flags=SA seq=9 win=65535 rtt=8.9 ms
len=46 ip=23.227.38.32 ttl=64 id=10200 sport=80 flags=SA seq=10 win=65535 rtt=10.2 ms
len=46 ip=23.227.38.32 ttl=64 id=10201 sport=80 flags=SA seq=11 win=65535 rtt=12.3 ms
len=46 ip=23.227.38.32 ttl=64 id=10202 sport=80 flags=SA seq=12 win=65535 rtt=7.6 ms
len=46 ip=23.227.38.32 ttl=64 id=10203 sport=80 flags=SA seq=13 win=65535 rtt=15.1 ms
^C
--- 23.227.38.32 hping statistic ---
14 packets transmitted, 14 packets received, 0% packet loss
round-trip min/avg/max = 7.6/11.2/15.9 ms
```

Purpose: To perform a TCP SYN scan (-S) against port 80 on the target host (23.227.38.32).

Output Analysis: The target responded with packets bearing the SA (SYN-ACK) flags, which is the expected response to a SYN packet, confirming that port 80 is open and listening. 14 packets were exchanged with 0% loss. Also verify it form Wireshark.

5.3. TCP FIN Scan on Port 80

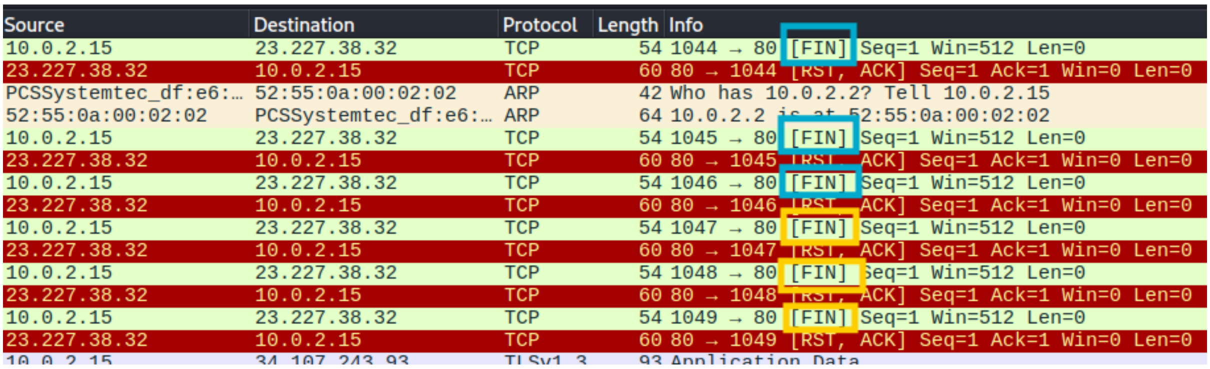
Command4: hping3 -F 23.227.38.32 -p 80



```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -F 23.227.38.32 -p 80
HPING 23.227.38.32 (eth0 23.227.38.32): F set, 40 headers + 0 data bytes
len=46 ip=23.227.38.32 ttl=255 id=10244 sport=80 flags=RA seq=0 win=0 rtt=3.7 ms
len=46 ip=23.227.38.32 ttl=255 id=10245 sport=80 flags=RA seq=1 win=0 rtt=7.4 ms
len=46 ip=23.227.38.32 ttl=255 id=10246 sport=80 flags=RA seq=2 win=0 rtt=1.8 ms
len=46 ip=23.227.38.32 ttl=255 id=10247 sport=80 flags=RA seq=3 win=0 rtt=6.0 ms
len=46 ip=23.227.38.32 ttl=255 id=10248 sport=80 flags=RA seq=4 win=0 rtt=8.7 ms
len=46 ip=23.227.38.32 ttl=255 id=10249 sport=80 flags=RA seq=5 win=0 rtt=7.3 ms
len=46 ip=23.227.38.32 ttl=255 id=10250 sport=80 flags=RA seq=6 win=0 rtt=6.1 ms
len=46 ip=23.227.38.32 ttl=255 id=10251 sport=80 flags=RA seq=7 win=0 rtt=8.5 ms
len=46 ip=23.227.38.32 ttl=255 id=10252 sport=80 flags=RA seq=8 win=0 rtt=3.5 ms
len=46 ip=23.227.38.32 ttl=255 id=10253 sport=80 flags=RA seq=9 win=0 rtt=11.4 ms
len=46 ip=23.227.38.32 ttl=255 id=10254 sport=80 flags=RA seq=10 win=0 rtt=3.9 ms
^C
--- 23.227.38.32 hping statistic ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max = 1.8/6.2/11.4 ms
```

Purpose: To send packets with the FIN flag (-F) set to port 80. This technique is often used for stealth scanning, as some firewalls may not log packets that do not request a connection initiation.

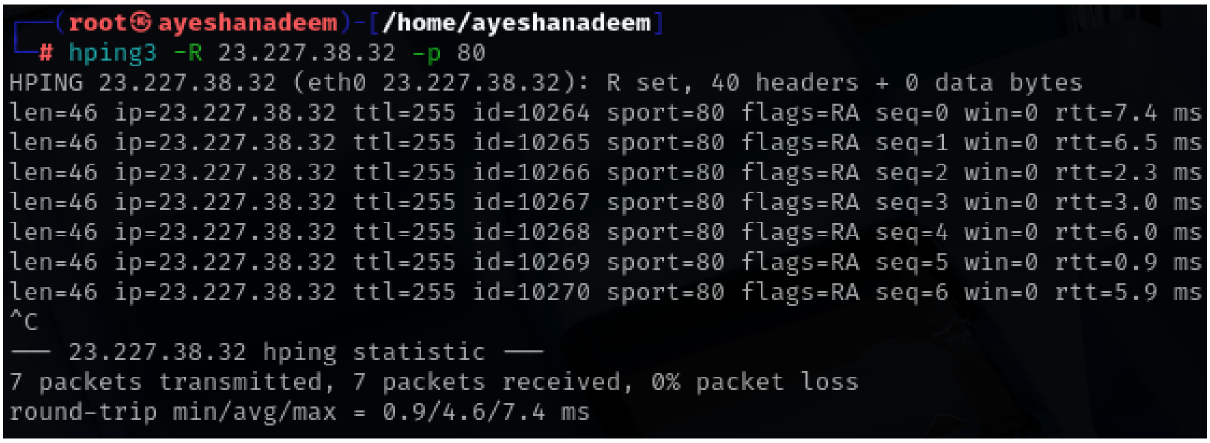
Output Analysis: The target responded with RA (RST-ACK) flags. This is a common response from closed ports or systems that comply with RFC 793 to unexpected FIN packets. You can also verify it on wireshark,



```
Source                  Destination             Protocol  Length Info
10.0.2.15               23.227.38.32            TCP           54 1044 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1044 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
PCSSystemtec_df:e6:…    52:55:0a:00:02:02       ARP           42 Who has 10.0.2.2? Tell 10.0.2.15
52:55:0a:00:02:02       PCSSystemtec_df:e6:…    ARP           64 10.0.2.2 is at 52:55:0a:00:02:02
10.0.2.15               23.227.38.32            TCP           54 1045 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1045 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 1046 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 1047 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1047 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 1048 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 1049 → 80 [FIN] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 1049 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               34.107.243.93           TLSv1.3       93 Application Data
```

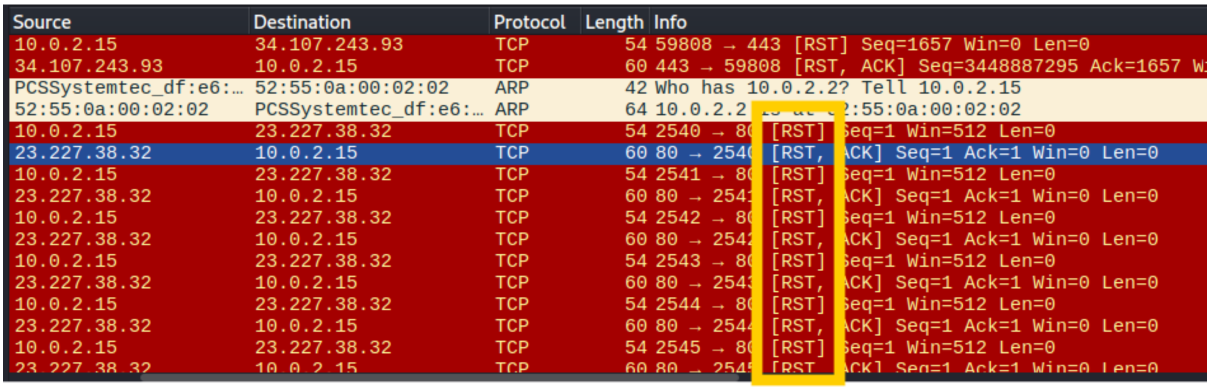
5.4. Other Possible Scans:

Command 5 : hping3 -R 23.227.38.32 -p 80



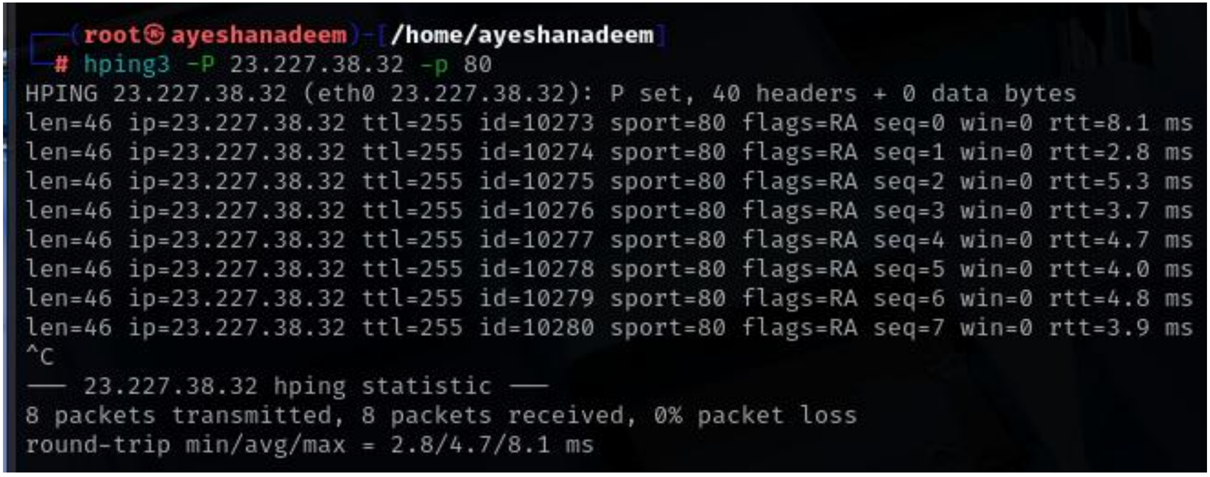
```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -R 23.227.38.32 -p 80
HPING 23.227.38.32 (eth0 23.227.38.32): R set, 40 headers + 0 data bytes
len=46 ip=23.227.38.32 ttl=255 id=10264 sport=80 flags=RA seq=0 win=0 rtt=7.4 ms
len=46 ip=23.227.38.32 ttl=255 id=10265 sport=80 flags=RA seq=1 win=0 rtt=6.5 ms
len=46 ip=23.227.38.32 ttl=255 id=10266 sport=80 flags=RA seq=2 win=0 rtt=2.3 ms
len=46 ip=23.227.38.32 ttl=255 id=10267 sport=80 flags=RA seq=3 win=0 rtt=3.0 ms
len=46 ip=23.227.38.32 ttl=255 id=10268 sport=80 flags=RA seq=4 win=0 rtt=6.0 ms
len=46 ip=23.227.38.32 ttl=255 id=10269 sport=80 flags=RA seq=5 win=0 rtt=0.9 ms
len=46 ip=23.227.38.32 ttl=255 id=10270 sport=80 flags=RA seq=6 win=0 rtt=5.9 ms
^C
--- 23.227.38.32 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 0.9/4.6/7.4 ms
```

Verify on Wireshark



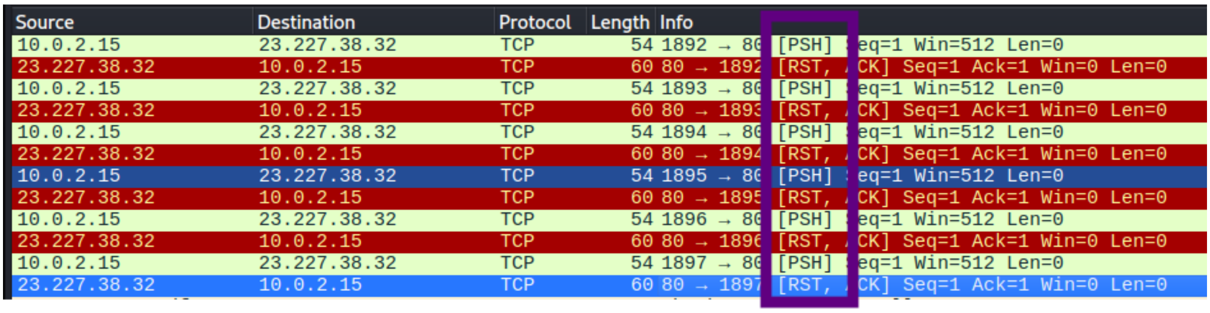
```
Source                  Destination             Protocol  Length Info
10.0.2.15               34.107.243.93           TCP           54 59808 → 443 [RST] Seq=1657 Win=0 Len=0
34.107.243.93           10.0.2.15               TCP           60 443 → 59808 [RST, ACK] Seq=3448887295 Ack=1657 Wi
PCSSystemtec_df:e6:…    52:55:0a:00:02:02       ARP           42 Who has 10.0.2.2? Tell 10.0.2.15
52:55:0a:00:02:02       PCSSystemtec_df:e6:…    ARP           64 10.0.2.2 is at 52:55:0a:00:02:02
10.0.2.15               23.227.38.32            TCP           54 2540 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 2541 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2541 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 2542 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 2543 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2543 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 2544 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15               23.227.38.32            TCP           54 2545 → 80 [RST] Seq=1 Win=512 Len=0
23.227.38.32            10.0.2.15               TCP           60 80 → 2545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Command 6: hping3 -P 23.227.38.32 -p 80



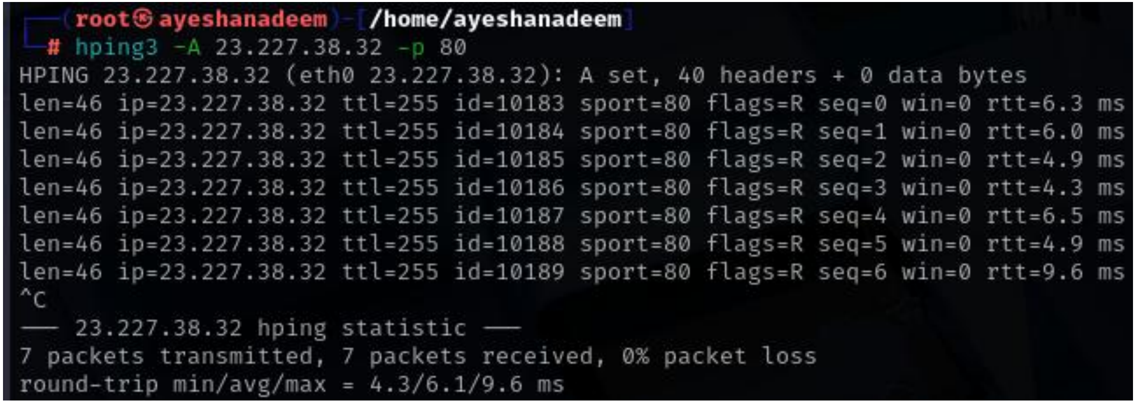
```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -P 23.227.38.32 -p 80
HPING 23.227.38.32 (eth0 23.227.38.32): P set, 40 headers + 0 data bytes
len=46 ip=23.227.38.32 ttl=255 id=10273 sport=80 flags=RA seq=0 win=0 rtt=8.1 ms
len=46 ip=23.227.38.32 ttl=255 id=10274 sport=80 flags=RA seq=1 win=0 rtt=2.8 ms
len=46 ip=23.227.38.32 ttl=255 id=10275 sport=80 flags=RA seq=2 win=0 rtt=5.3 ms
len=46 ip=23.227.38.32 ttl=255 id=10276 sport=80 flags=RA seq=3 win=0 rtt=3.7 ms
len=46 ip=23.227.38.32 ttl=255 id=10277 sport=80 flags=RA seq=4 win=0 rtt=4.7 ms
len=46 ip=23.227.38.32 ttl=255 id=10278 sport=80 flags=RA seq=5 win=0 rtt=4.0 ms
len=46 ip=23.227.38.32 ttl=255 id=10279 sport=80 flags=RA seq=6 win=0 rtt=4.8 ms
len=46 ip=23.227.38.32 ttl=255 id=10280 sport=80 flags=RA seq=7 win=0 rtt=3.9 ms
^C
--- 23.227.38.32 hping statistic ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 2.8/4.7/8.1 ms
```

Verify on Wireshark



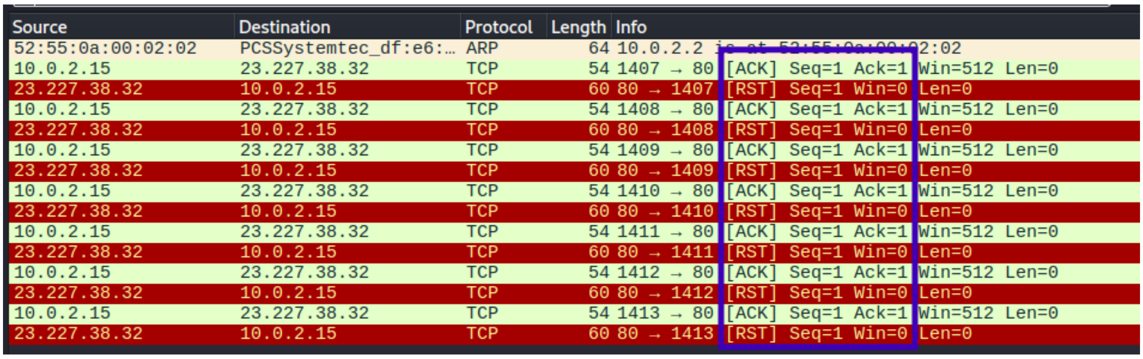
Source	Destination	Protocol	Length	Info
10.0.2.15	23.227.38.32	TCP	54	1892 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1892 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1893 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1893 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1894 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1895 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1896 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1896 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1897 → 80 [PSH] Seq=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1897 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Command 7: hping3 -A 23.227.38.32 -p 80



```
┌──(root㉿ayeshanadeem)-[/home/ayeshanadeem]
└─# hping3 -A 23.227.38.32 -p 80
HPING 23.227.38.32 (eth0 23.227.38.32): A set, 40 headers + 0 data bytes
len=46 ip=23.227.38.32 ttl=255 id=10183 sport=80 flags=R seq=0 win=0 rtt=6.3 ms
len=46 ip=23.227.38.32 ttl=255 id=10184 sport=80 flags=R seq=1 win=0 rtt=6.0 ms
len=46 ip=23.227.38.32 ttl=255 id=10185 sport=80 flags=R seq=2 win=0 rtt=4.9 ms
len=46 ip=23.227.38.32 ttl=255 id=10186 sport=80 flags=R seq=3 win=0 rtt=4.3 ms
len=46 ip=23.227.38.32 ttl=255 id=10187 sport=80 flags=R seq=4 win=0 rtt=6.5 ms
len=46 ip=23.227.38.32 ttl=255 id=10188 sport=80 flags=R seq=5 win=0 rtt=4.9 ms
len=46 ip=23.227.38.32 ttl=255 id=10189 sport=80 flags=R seq=6 win=0 rtt=9.6 ms
^C
--- 23.227.38.32 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 4.3/6.1/9.6 ms
```

Verify on wireshark



Source	Destination	Protocol	Length	Info
52:55:0a:00:02:02	PCSSystemtec_df:e6:…	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
10.0.2.15	23.227.38.32	TCP	54	1407 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1407 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1408 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1408 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1409 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1409 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1410 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1410 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1411 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1411 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1412 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1412 [RST] Seq=1 Win=0 Len=0
10.0.2.15	23.227.38.32	TCP	54	1413 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=0
23.227.38.32	10.0.2.15	TCP	60	80 → 1413 [RST] Seq=1 Win=0 Len=0

Here is list of all flags you can try
-L –setack set TCP ack
-F –fin set FIN flag
-S –syn set SYN flag
-R –rst set RST flag
-P –push set PUSH flag
-A –ack set ACK flag
-U –urg set URG flag
-X –xmas set X unused flag (0x40)
-Y –ymas set Y unused flag (0x80)

6.0 Analysis of Findings

The practical execution of hping3 commands yielded significant insights into network behavior and security postures. The successful SYN-SCAN exchange (SYN followed by SYN-ACK) on port **80** definitively identified it as **open** and accepting connections. Conversely, the FIN scan elicited RST-ACK responses, which, according to RFC 793, is the expected behavior for a **closed port** on a compliant system, though this can also be used for stealthy identification of filtering devices. The successful ICMP traceroute to an external domain confirmed that outbound ICMP traffic was not filtered by the local network gateway, providing a baseline for understanding network egress rules. The varied responses to non-standard flag combinations like XMAS and YMAS packets provide a fingerprint of the target's TCP/IP stack, which can be critical for OS identification and understanding how a system handles malformed or unexpected traffic.

6.1. Industrial and Real-World Applications

Hping3 is a versatile tool employed across various IT domains:

Field	Application
Penetration Testing & Red Teaming	Stealth reconnaissance, firewall evasion, spoofed traffic simulation, and banner grabbing.
Security Auditing	Validation of IDS/IPS rulesets and analysis of packet filtering configurations.
Network Engineering	Path MTU discovery, network latency and jitter measurement, and TCP/IP stack auditing.
Academia & Research	Teaching TCP/IP protocol behavior, packet analysis, and advanced network manipulation.

Its ability to use TCP/UDP for diagnostics makes it particularly valuable in environments where ICMP echo requests are blocked.

7.0 Conclusion

The exercise successfully demonstrated the powerful capabilities of `hping3` as a network analysis and security tool. The ability to craft packets with precision allows security professionals and network administrators to gain deep insights into network behavior, security postures, and protocol implementations. Mastery of such tools is essential for effective network defense and vulnerability assessment.

Reference:

Hping3: Full tutorial from noob to pro

Hping3 Cheat Sheet by myke670 - Download free from Cheatography - Cheatography.com: Cheat Sheets For Every Occasion