LAB 20: Using `hping3` for Security Auditing and Testing of Network Devices

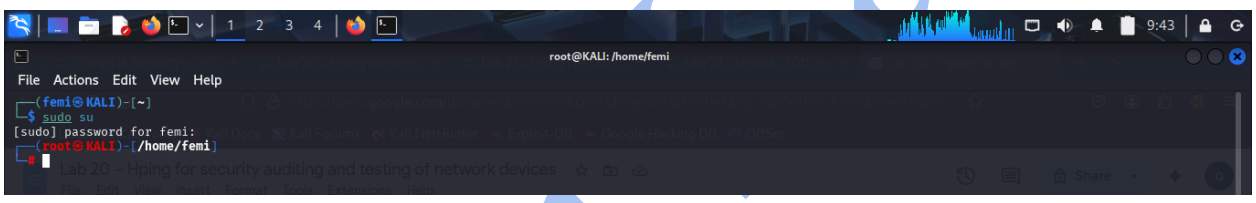
💻 OS Used: Kali Linux

📦 Tool: `hping3`

🌐 Target: `scanme.nmap.org` (legal target for practice)

🔰 Getting Started: Switch to Root

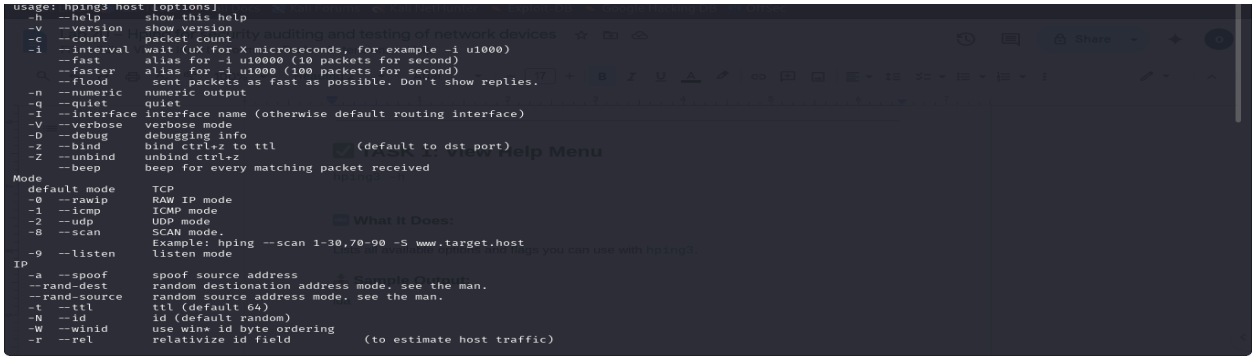
```
sudo su -
```



🔤 This command switches you to the **root user** (administrator). `hping3` needs root access to send raw packets.

✅ TASK 1: View Help Menu

```
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.
                  Example: hping --scan 1-30,70-90 -S www.target.host
  -9  --listen    listen mode
IP
  -a  --spoof     spoof source address
  --rand-dest     random destination address mode. see the man.
  --rand-source   random source address mode. see the man.
  -t  --ttl       ttl (default 64)
  -N  --id        id (default random)
  -W  --winid     use win* id byte ordering
  -r  --rel       relativize id field          (to estimate host traffic)
```

🔤 What It Does:

Lists all available options and flags you can use with `hping3`.

📥 Sample Output:

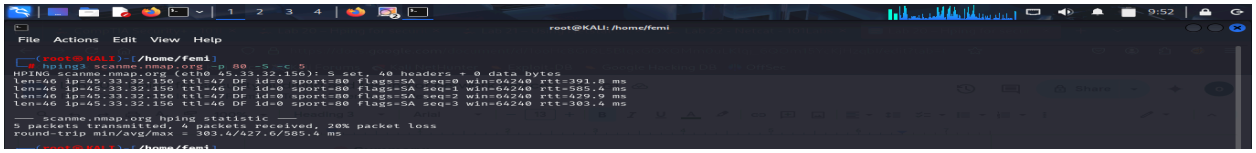
```
usage: hping3 host [options]
 -8 --scan [port+]        scan mode
 -S --syn                 set SYN flag
 -A --ack                 set ACK flag
 -F --fin                 set FIN flag
 -p --destport [port]     destination port
 -s --baseport [port]     source port
 -c --count [num]         send only num packets
...
```

🧠 Summary:

Think of this as a cheat sheet for using the tool. Always run this when learning a new command.

✅ TASK 2: SYN Scan on Port 80

```
hping3 scanme.nmap.org -p 80 -S -c 5
```



```
┌──(root㉿KALI)-[/home/femi]
└─# hping3 scanme.nmap.org -p 80 -S -c 5
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=391.8 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=585.4 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=429.9 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt=303.4 ms

--- scanme.nmap.org hping statistic ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 303.4/427.6/585.4 ms
```

🔤 What Each Flag Means:

Flag	Meaning
`-p 80`	Target port 80 (used for HTTP traffic)
`-S`	Send a SYN packet
`-c 5`	Send the packet 5 times

📥 Sample Output:

```
HPING scanme.nmap.org (2600:3c01::f03c:91ff:fe18:bb2f): S set, 40
headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=53 DF id=0 sport=80 flags=SA seq=0
win=29200 rtt=89.2 ms
len=46 ip=45.33.32.156 ttl=53 DF id=0 sport=80 flags=SA seq=1
win=29200 rtt=88.7 ms
...
```

🧠 Interpreting the Output:

- `flags=SA` → Port is **open** (SYN-ACK received)
- `flags=RA` → Port is **closed** (RST-ACK received)

Flag	Meaning
`SA`	SYN-ACK (port is open)
`RA`	RST-ACK (port is closed)

✅ TASK 3: Sweep Scan Multiple Ports

`hping3 scanme.nmap.org -8 1-1024 -S`

```
┌──(root㉿KALI)-[/home/femi]
└─# hping3 scanme.nmap.org -8 1-1024 -S
Scanning scanme.nmap.org (45.33.32.156), port 1-1024
1024 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   25 smtp       : .S..A ...  58     0 65535    46
   22 ssh        : .S..A ...  47     0 64240    46
   80 http       : .S..A ...  47     0 64240    46
All replies received. Done.
Not responding ports:
```

🔤 What Each Flag Means:

Flag	Meaning
`-8 1-1024`	Scan ports 1 through 1024
`-S`	Use SYN flag

🧠 Output Explanation:

Only **open** ports are shown. It tells you which **services** might be running:

Port	Service (Likely)	Status
22	SSH	Open
80	HTTP	Open

✅ TASK 4: Scan All Ports One-by-One

`hping3 -S scanme.nmap.org -p ++1`

```
┌──(root㉿KALT)-[/home/femi]
└─# hping3 -S scanme.nmap.org -p ++1
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=1 flags=RA seq=0 win=0 rtt=504.9 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=2 flags=RA seq=1 win=0 rtt=716.3 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=4 flags=RA seq=3 win=0 rtt=421.4 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=5 flags=RA seq=4 win=0 rtt=516.0 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=6 flags=RA seq=5 win=0 rtt=383.7 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=7 flags=RA seq=6 win=0 rtt=386.4 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=8 flags=RA seq=7 win=0 rtt=286.5 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=9 flags=RA seq=8 win=0 rtt=339.1 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=10 flags=RA seq=9 win=0 rtt=450.0 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=11 flags=RA seq=10 win=0 rtt=352.7 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=12 flags=RA seq=11 win=0 rtt=446.1 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=14 flags=RA seq=13 win=0 rtt=500.4 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=15 flags=RA seq=14 win=0 rtt=492.9 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=16 flags=RA seq=15 win=0 rtt=325.7 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=17 flags=RA seq=16 win=0 rtt=348.3 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=18 flags=RA seq=17 win=0 rtt=788.4 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=19 flags=RA seq=18 win=0 rtt=324.2 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=20 flags=RA seq=19 win=0 rtt=351.8 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=22 flags=SA seq=21 win=64240 rtt=425.9 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=24 flags=RA seq=23 win=0 rtt=598.0 ms
len=46 ip=45.33.32.156 ttl=58 DF id=0 sport=25 flags=SA seq=24 win=65535 rtt=103.8 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=26 flags=RA seq=25 win=0 rtt=477.3 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=27 flags=RA seq=26 win=0 rtt=385.2 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=28 flags=RA seq=27 win=0 rtt=498.3 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=29 flags=RA seq=28 win=0 rtt=430.8 ms
len=46 ip=45.33.32.156 ttl=47 DF id=0 sport=30 flags=RA seq=29 win=0 rtt=438.2 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=32 flags=RA seq=31 win=0 rtt=788.2 ms
len=46 ip=45.33.32.156 ttl=46 DF id=0 sport=33 flags=RA seq=32 win=0 rtt=396.0 ms
```

🔤 What ++1 Means:

Start at port 1 and **increment by 1** after each scan.

📥 Sample Output:

ini

CopyEdit

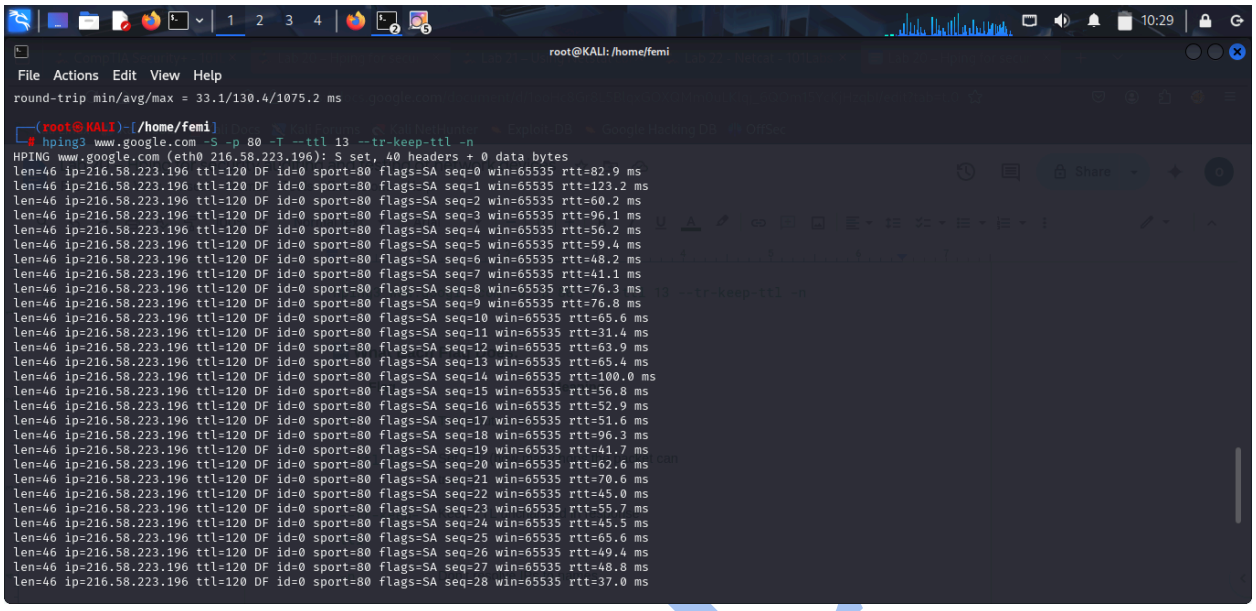
```
len=46 ip=139.162.196.104 flags=SA port=21
len=46 ip=139.162.196.104 flags=SA port=22
len=46 ip=139.162.196.104 flags=SA port=80
```

🧠 Useful When:

You want a **full scan** of all 65535 ports.

✅ TASK 5: Find Load-Balancing IPs with TTL

`hping3 www.google.com -S -p 80 -T --ttl 13 --tr-keep-ttl -n`



🔤 What Each Flag Does:

Flag	Meaning
`-T`	Traceroute mode
`--ttl 13`	Set TTL (how many hops the packet can travel)
`--tr-keep-ttl`	Keep TTL unchanged in response
`-n`	Don't resolve IPs to names

🧠 Purpose:

You see **multiple IPs** handling traffic → means **load balancing** (common in big services like Google).

✅ TASK 6: ICMP Traceroute

`hping3 google.com -1 --traceroute -n`

```
┌──(femi㉿KALI)-[~]
└─$ sudo hping3 google.com -1 --traceroute -n
[sudo] password for femi:
HPING google.com (eth0 142.250.200.110): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.1.1
hop=1 hoprtt=7.6 ms
hop=2 TTL 0 during transit from ip=10.157.15.254
hop=2 hoprtt=185.5 ms
hop=3 TTL 0 during transit from ip=172.24.246.82
hop=3 hoprtt=35.2 ms
hop=4 TTL 0 during transit from ip=172.24.246.181
hop=4 hoprtt=27.6 ms
hop=5 TTL 0 during transit from ip=172.24.246.193
hop=5 hoprtt=22.9 ms
hop=6 TTL 0 during transit from ip=192.168.239.202
hop=6 hoprtt=21.4 ms
hop=7 TTL 0 during transit from ip=142.250.170.170
hop=7 hoprtt=57.7 ms
hop=8 TTL 0 during transit from ip=142.250.209.225
hop=8 hoprtt=25.4 ms
hop=9 TTL 0 during transit from ip=192.178.240.16
hop=9 hoprtt=32.6 ms
hop=10 TTL 0 during transit from ip=216.239.47.221
hop=10 hoprtt=193.7 ms
hop=11 TTL 0 during transit from ip=216.239.35.181
hop=11 hoprtt=97.6 ms
hop=12 TTL 0 during transit from ip=142.251.76.111
hop=12 hoprtt=225.3 ms
hop=13 TTL 0 during transit from ip=209.85.247.245
hop=13 hoprtt=110.1 ms
len=46 ip=142.250.200.110 ttl=114 id=0 icmp_seq=13 rtt=158.7 ms
len=46 ip=142.250.200.110 ttl=114 id=0 icmp_seq=14 rtt=105.2 ms
```

🔤 What It Does:

Traceroute using ICMP (like regular ping).

Flag	Meaning
`-1`	Use ICMP mode
`--traceroute`	Enable traceroute
`-n`	Show raw IPs only

📥 Sample Output:

```
hop=1 ip=192.168.1.1
hop=2 ip=10.0.0.1
hop=3 ip=104.244.42.1
...
```

🧠 Purpose:

Shows the **network path** from your machine to the target.

✅ TASK 7: TCP-Based Traceroute

`hping3 google.com -n -S -s 8080 -p 80 --traceroute`

```
┌──(femi㉿KALI)-[~]
└─$ sudo hping3 google.com -n -S -s 8080 -p 80 --traceroute
HPING google.com (eth0 142.250.200.110): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.1.1
hop=1 hoprtt=8.3 ms
hop=2 TTL 0 during transit from ip=10.157.15.254
hop=2 hoprtt=194.9 ms
hop=3 TTL 0 during transit from ip=172.24.246.82
hop=3 hoprtt=197.3 ms
hop=4 TTL 0 during transit from ip=172.24.246.181
hop=4 hoprtt=41.6 ms
hop=5 TTL 0 during transit from ip=172.24.246.193
hop=5 hoprtt=41.3 ms
hop=6 TTL 0 during transit from ip=192.168.239.202
hop=6 hoprtt=74.0 ms
hop=7 TTL 0 during transit from ip=142.250.170.170
hop=7 hoprtt=46.9 ms
hop=8 TTL 0 during transit from ip=142.250.209.221
hop=8 hoprtt=69.4 ms
hop=9 TTL 0 during transit from ip=192.178.240.60
hop=9 hoprtt=52.6 ms
hop=10 TTL 0 during transit from ip=192.178.82.19
hop=10 hoprtt=128.7 ms
hop=11 TTL 0 during transit from ip=142.250.59.27
hop=11 hoprtt=300.1 ms
hop=12 TTL 0 during transit from ip=108.170.248.158
hop=12 hoprtt=210.3 ms
hop=13 TTL 0 during transit from ip=142.250.59.27
hop=13 hoprtt=510.6 ms
len=46 ip=142.250.200.110 ttl=114 DF id=0 sport=80 flags=SA seq=14 win=65535 rtt=419.9 ms
DUP! len=46 ip=142.250.200.110 ttl=114 DF id=0 sport=80 flags=SA seq=14 win=65535 rtt=728.1 ms
hop=14 TTL 0 during transit from ip=209.85.247.245
hop=14 hoprtt=262.2 ms
```

🔤 Explanation:

Flag	Meaning
`-s 8080`	Use source port 8080
`-p 80`	Target port 80
`--traceroute`	Use traceroute
`-S`	SYN flag
`-n`	No DNS lookup

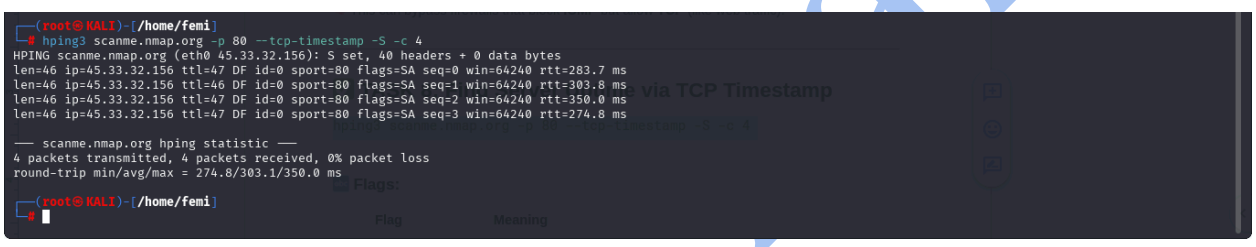
📥 Sample Output:

```
hop=1 ip=192.168.1.1
hop=2 ip=203.0.113.1
hop=3 ip=45.33.32.156
```

🧠 This can bypass firewalls that block **ICMP** but allow **TCP** (like web traffic).

✅ TASK 8: Find Server Uptime via TCP Timestamp

```
hping3 scanme.nmap.org -p 80 --tcp-timestamp -S -c 4
```



🔤 Flags:

Flag	Meaning
`--tcp-timestamp`	Ask for TCP timestamp
`-c 4`	Send 4 packets
`-S`	SYN flag

📥 Sample Output:

```
tcp_tsval=123456789 tsecr=0
tcp_tsval=123456890 tsecr=0
tcp_tsval=123456991 tsecr=0
...
```

🧠 Higher `tcp_tsval` = longer uptime. If the numbers are small, the system may have **recently rebooted**.

⚠️ May not work in **virtual machines** with **NAT networking**.

🚨 TASK 9: SYN Flood Attack (for educational testing only)

`hping3 scanme.nmap.org -S --flood -p 80`

```
┌──(root㉿KALI)-[/home/femi]
└─# hping3 scanme.nmap.org -S --flood -p 80
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

🔤 Explanation:

Flag	Meaning
`--flood`	Send SYN packets as fast as possible
`-p 80`	Target port 80
`-S`	SYN flag

`(no output — runs silently)`

🧠 This is used to **overwhelm** the server and simulate a **Denial of Service (DoS)** attack.

⚠️ DO NOT run this against unauthorized systems. It's illegal and harmful.

✅ Recap Table:

Common Flags in `hping3`

Flag	Description
`-S`	Set SYN flag
`-A`	Set ACK flag
`-1`	ICMP mode (ping)
`-8`	Scan mode (multi-port)
`-p`	Destination port
`-s`	Source port
`-c`	Number of packets
`--flood`	Rapid flood mode
`--ttl`	Set packet lifetime (Time To Live)
`--tcp-timestamp`	Get server uptime info
`--traceroute`	Traceroute mode

THE END