

FIREWALL TESTING WITH



A COMPREHENSIVE GUIDE



Understanding Hping3

Hping3 is a command-line packet generator and analyzer for the TCP/IP protocol. Unlike traditional ping utilities, Hping3 supports TCP, UDP, and ICMP, allowing testers to craft customized packets for detailed firewall and intrusion detection testing.

Features of Hping3

- ✓ Packet crafting for TCP, UDP, ICMP, and raw IP protocols
- ✓ Ability to modify source/destination IP addresses and ports
- ✓ Stateful and stateless firewall testing
- ✓ Traceroute functionality with customizable flags
- ✓ Port scanning and packet fragmentation
- ✓ TCP/IP fingerprinting
- ✓ Test firewall rules and IDS/IPS behavior
- ✓ Conduct DoS testing in a controlled environment

Step-by-Step Guide to Firewall Testing with Hping3

Installation

Hping3 is available for Linux and Windows (via Cygwin). Install it using:

```
sudo apt update && sudo apt install hping3  
sudo yum install hping3
```

```
(root@kali)-[/home/kali]  
# sudo apt update && sudo apt install hping3  
Get:1 http://free.nchc.org.tw/kali kali-rolling InRelease [41.5 kB]  
Get:2 http://free.nchc.org.tw/kali kali-rolling/main amd64 Packages [20.4 MB]  
Get:3 http://free.nchc.org.tw/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]  
Get:4 http://free.nchc.org.tw/kali kali-rolling/contrib amd64 Packages [112 kB]  
Get:5 http://free.nchc.org.tw/kali kali-rolling/contrib amd64 Contents (deb) [261 kB]  
Get:6 http://free.nchc.org.tw/kali kali-rolling/non-free amd64 Packages [194 kB]  
Get:7 http://free.nchc.org.tw/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]  
Get:8 http://free.nchc.org.tw/kali kali-rolling/non-free-firmware amd64 Packages [10.5 kB]  
Fetched 71.1 MB in 24s (3,026 kB/s)  
1178 packages can be upgraded. Run 'apt list --upgradable' to see them.  
hping3 is already the newest version (3.a2.ds2-11~kali1).  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1178
```

For Windows, use Cygwin or a Linux VM.

Firewall Testing Techniques with Hping3

The target is **elm.sa**.

1. Basic Ping Scan

Most firewalls block standard ICMP requests. Use Hping3 to check if a host is responding:

```
hping3 -1 elm.sa -c 4
```

```
(root@kali)-[/home/kali]
# hping3 -1 elm.sa -c 4
HPING elm.sa (eth0 185.131.97.25): icmp mode set, 28 headers + 0 data bytes

— elm.sa hping statistic —
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **-1:** Uses ICMP (ping mode)
- ✓ **-c:** count

Result:

If no response is received, the firewall is likely blocking ICMP echo requests

2. TCP SYN Scan

SYN scans help identify open ports while avoiding detection by some logging mechanisms.

```
hping3 -S elm.sa -p 80 -c 3
```

```
(root@kali)-[/home/kali]
# hping3 -S elm.sa -p 80 -c 3
HPING elm.sa (eth0 185.131.97.25): S set, 40 headers + 0 data bytes
len=46 ip=185.131.97.25 ttl=128 id=49650 sport=80 flags=RA seq=0 win=64240 rtt=0.0 ms
len=46 ip=185.131.97.25 ttl=128 id=49651 sport=80 flags=RA seq=0 win=64240 rtt=0.0 ms
len=46 ip=185.131.97.25 ttl=128 id=49652 sport=80 flags=RA seq=0 win=64240 rtt=0.0 ms

— elm.sa hping statistic —
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **-S:** Sends SYN (connection request) packets
- ✓ **-p 80:** Targets port 80 (HTTP)

Result:

- ✓ If a **SYN-ACK** is received, the port is open.
- ✓ If a **RST-ACK** is received, the port is closed.
- ✓ No response might indicate packet filtering.

3. Stealth Scan (FIN Scan)

To check if the firewall blocks FIN packets:

```
hping3 -F -p 80 elm.sa
```

```
(root@kali)-[/home/kali]
# hping3 -F -p 80 elm.sa
HPING elm.sa (eth0 185.38.109.109): F set, 40 headers + 0 data bytes
^C
— elm.sa hping statistic —
112 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **-F:** Sends FIN (finish) packets

Result:

- ✓ Firewalls may ignore FIN packets, but if a RST-ACK is received, the port is closed.

4. ACK Scan for Firewall Rule Detection

To test firewall rule sets:

```
hping3 -A -p 80 elm.sa
```

```
(root@kali)-[/home/kali]
# hping3 -A -p 80 elm.sa
HPING elm.sa (eth0 185.131.97.25): A set, 40 headers + 0 data bytes
len=46 ip=185.131.97.25 ttl=128 id=49072 sport=80 flags=R seq=0 win=32767 rtt=7.7 ms
len=46 ip=185.131.97.25 ttl=128 id=49073 sport=80 flags=R seq=1 win=32767 rtt=3.7 ms
len=46 ip=185.131.97.25 ttl=128 id=49074 sport=80 flags=R seq=2 win=32767 rtt=1.8 ms
len=46 ip=185.131.97.25 ttl=128 id=49075 sport=80 flags=R seq=3 win=32767 rtt=4.4 ms
^C
— elm.sa hping statistic —
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.8/4.4/7.7 ms
```

Parameters:

✓ **-A:** Sends ACK packets

Result:

- ✓ If no response is received, the firewall will filter packets.
- ✓ If a **RST** response is received, the port is unfiltered but closed.

5. UDP Scan

Since UDP is connectionless, firewalls often block or restrict UDP traffic. Test with:

```
hping3 --udp -p 53 elm.sa
```

```
(root@kali)-[/home/kali]
# hping3 --udp -p 80 elm.sa
HPING elm.sa (eth0 185.131.97.25): udp mode set, 28 headers + 0 data bytes
^C
— elm.sa hping statistic —
286 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **--udp:** Uses UDP packets
- ✓ **-p 53:** Targets port 53 (DNS)

Result:

- ✓ If no response is received, the firewall will block UDP.
- ✓ If an ICMP "port unreachable" is returned, the port is closed.

6. Testing Stateful vs. Stateless Firewalls

A stateful firewall tracks connection states, while a stateless firewall filters based on predefined rules. To determine firewall behavior:

```
hping3 -S elm.sa -p 80 --fast
```

```
(root@kali)-[/home/kali]
# hping3 -S elm.sa -p 80 --fast
HPING elm.sa (eth0 185.131.97.25): S set, 40 headers + 0 data bytes
len=46 ip=185.131.97.25 ttl=128 id=49078 sport=80 flags=RA seq=0 win=64240 rtt=21068.4 ms
len=46 ip=185.131.97.25 ttl=128 id=49079 sport=80 flags=RA seq=1 win=64240 rtt=21043.1 ms
len=46 ip=185.131.97.25 ttl=128 id=49080 sport=80 flags=RA seq=2 win=64240 rtt=21058.7 ms
len=46 ip=185.131.97.25 ttl=128 id=49081 sport=80 flags=RA seq=3 win=64240 rtt=21056.7 ms
len=46 ip=185.131.97.25 ttl=128 id=49082 sport=80 flags=RA seq=4 win=64240 rtt=21040.3 ms
len=46 ip=185.131.97.25 ttl=128 id=49083 sport=80 flags=RA seq=5 win=64240 rtt=21051.8 ms
```

Parameters:

- ✓ **--fast:** Sends packets faster for quicker testing

Result:

- ✓ If responses differ when sent in sequence, the firewall is stateful.
- ✓ Consistent responses: Firewall is stateless

7. Fragmented Packet Attack Simulation

Firewalls should reassemble fragmented packets, but some misconfigurations allow evasion:

```
hping3 -S elm.sa -p 80 -f
```

```
(root@kali)-[/home/kali]
# hping3 -S elm.sa -p 80 -f
HPING elm.sa (eth0 185.131.97.25): S set, 40 headers + 0 data bytes
len=46 ip=185.131.97.25 ttl=128 id=49573 sport=80 flags=RA seq=0 win=64240 rtt=21035.4 ms
len=46 ip=185.131.97.25 ttl=128 id=49574 sport=80 flags=RA seq=1 win=64240 rtt=21058.7 ms
len=46 ip=185.131.97.25 ttl=128 id=49575 sport=80 flags=RA seq=2 win=64240 rtt=21045.8 ms
len=46 ip=185.131.97.25 ttl=128 id=49576 sport=80 flags=RA seq=3 win=64240 rtt=21045.1 ms
len=46 ip=185.131.97.25 ttl=128 id=49577 sport=80 flags=RA seq=4 win=64240 rtt=21055.9 ms
len=46 ip=185.131.97.25 ttl=128 id=49578 sport=80 flags=RA seq=5 win=64240 rtt=21058.4 ms
len=46 ip=185.131.97.25 ttl=128 id=49579 sport=80 flags=RA seq=6 win=64240 rtt=21029.6 ms
```

Parameters:

- ✓ **-f:** Sends fragmented packets

Result:

- ✓ If fragmented packets bypass filtering, the firewall may be misconfigured.

8. Spoofed Source IP Testing

To test if the firewall relies on simple source-based filtering:

```
hping3 -S elm.sa -a <fake_IP> -p 80
```

```
(root@kali)-[/home/kali]
# hping3 -S elm.sa -a 8.8.8.8 -p 80
HPING elm.sa (eth0 185.131.97.25): S set, 40 headers + 0 data bytes
^C
— elm.sa hping statistic —
72 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **-a <fake_IP>:** Spoofs the source IP address

Result:

- ✓ If a response is received, the firewall allows spoofed traffic.

9. Testing IDS/IPS Behavior

Intrusion Detection and Prevention Systems (IDS/IPS) analyze traffic patterns and detect anomalies. Use Hping3 to evaluate their effectiveness:

```
hping3 -S elm.sa -p 80 --rand-source --flood
```

```
(root@kali)-[/home/kali]
# hping3 -S elm.sa -p 80 --rand-source --flood
HPING elm.sa (eth0 185.131.97.25): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— elm.sa hping statistic —
11064064 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **--rand-source:** Sends packets from random source IPs
- ✓ **--flood:** Sends packets continuously (DoS attack simulation)

Result:

- ✓ If alerts are generated, the IDS/IPS will function properly.
- ✓ If not, it may require tuning.

10. Conducting DoS Testing in a Controlled Environment

Simulating Denial-of-Service (DoS) attacks help assess how well firewalls mitigate excessive traffic. Controlled DoS tests can be performed using:

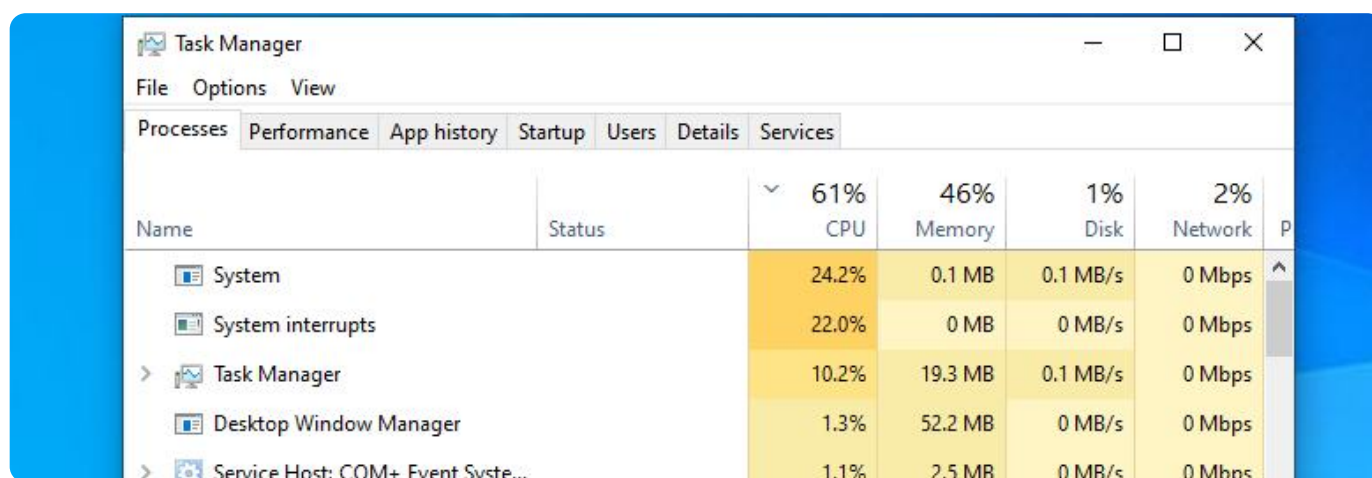
```
hping3 --flood --rand-source -S 192.168.201.129 -p 443
```

```
(root@kali)-[/home/kali]
# hping3 --flood --rand-source -S 192.168.201.129 -p 80
HPING 192.168.201.129 (eth0 192.168.201.129): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.201.129 hping statistic —
4141487 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Parameters:

- ✓ **--flood:** Generates a high packet rate
- ✓ **--rand-source:** Randomizes source IPs
- ✓ **-p 443:** Targets port 443 (HTTPS)

Use this command cautiously and only in a lab environment with permission. Here, performing DOS attack on 192.168.xxx.xxx in controlled environment from kali machine.



The victim system is getting sluggish here.

Analyzing Firewall Responses

Interpreting responses from Hping3 scans helps in determining firewall behavior:

Response	Interpretation
No response	Packet dropped (Firewall or host not responding)
RST-ACK	Port closed but reachable
SYN-ACK	Port open
ICMP "port unreachable"	UDP port closed
Fragmentation allowed	Possible firewall misconfiguration

Conclusion

Hping3 is an essential tool for Ethical Hackers and Penetration Testers to assess firewall security. By using various scanning techniques, security professionals can identify vulnerabilities and improve firewall configurations.

By mastering Hping3, you can enhance your ability to detect and remediate security gaps, making networks more resilient against potential threats.

CEH v13 AI Certification Training with InfosecTrain

[InfosecTrain's CEH v13 AI Certification Training](#) provides hands-on learning of Hping3, a powerful packet crafting and firewall testing tool used in ethical hacking. With expert-led training, real-world labs, and AI-driven security insights, learners gain practical experience in assessing network defenses and detecting vulnerabilities. The training ensures cybersecurity professionals master Hping3 for ethical hacking, intrusion detection, and network security assessments effectively.

KEEP LEARNING WITH



Contact us

✉ sales@infosectrain.com

🌐 www.infosectrain.com

Follow us on

