ETHICAL HACKING V2
LAB SERIES

Lab 04: Reconnaissance with hping

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	3: Scanning and Enumeration
EC-Council CEH v10 Domain Modules	3: Scanning Networks 4: Enumeration
CompTIA Pentest+ Objectives	2.1 Given a scenario, conduct information gathering using appropriate techniques 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	2: Getting to Know Your Targets 3: Network Scanning and Enumeration 7: Network-Based Attacks

Contents

Introduction

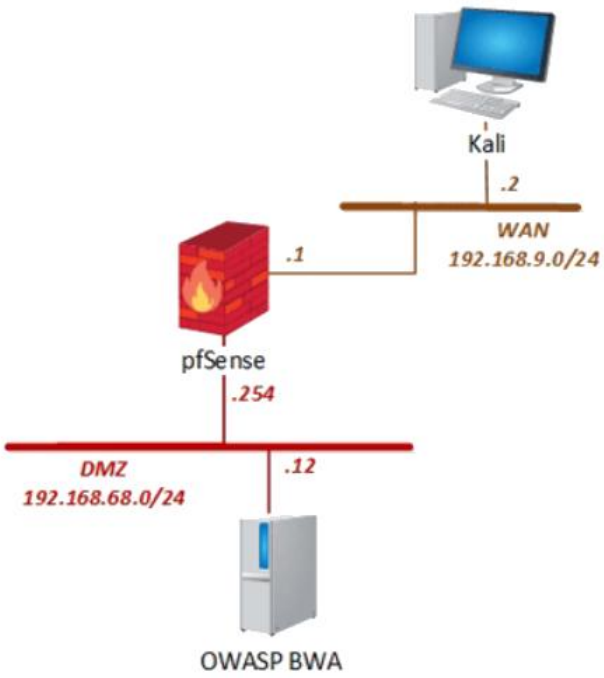
Hping is a TCP/IP packet assembler and analyzer. In this lab, we will use *hping* to create packets as well as perform different network functions with the packets.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Using Hping as an ICMP Utility
2. Using Hping for Port Scanning

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

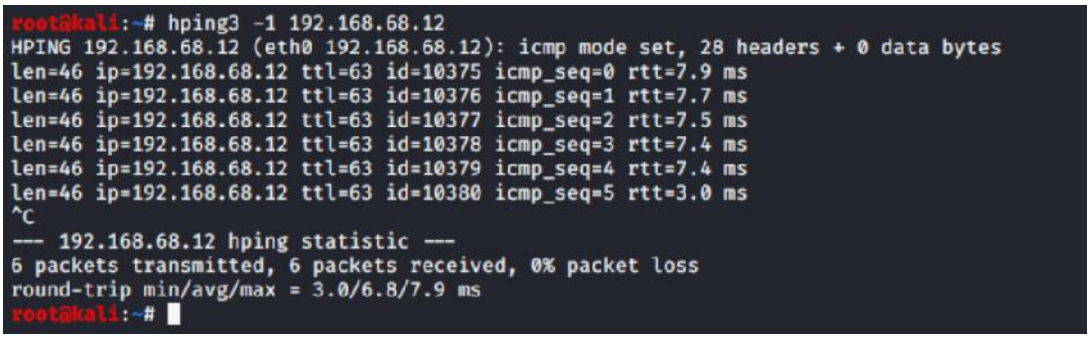
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa

1 Using hping as an ICMP Utility

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter **root** as the *username*. Press **Tab**.
4. Enter **toor** as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. With *hping*, a packet can be crafted with a specific protocol. Type the command below using *ICMP* as the protocol followed by pressing the **Enter** key.

```
hping3 -1 192.168.68.12
```

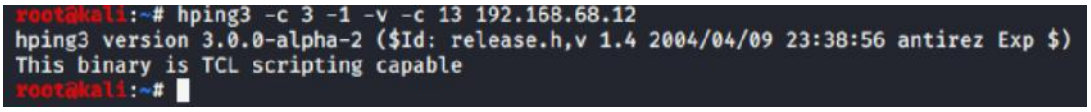
7. After about 6 packets are transmitted, press **CTRL+C** to stop *hping* from running.



Notice several *ICMP* messages (default is *ICMP Type 0* echo) received a reply. If the target didn't reply, other *ICMP* requests can be used.

8. Try a different *ICMP* type using a timestamp *ICMP Type 13*. Enter the command below, limiting the number of packets sent to 3 and get feedback using the verbose option.

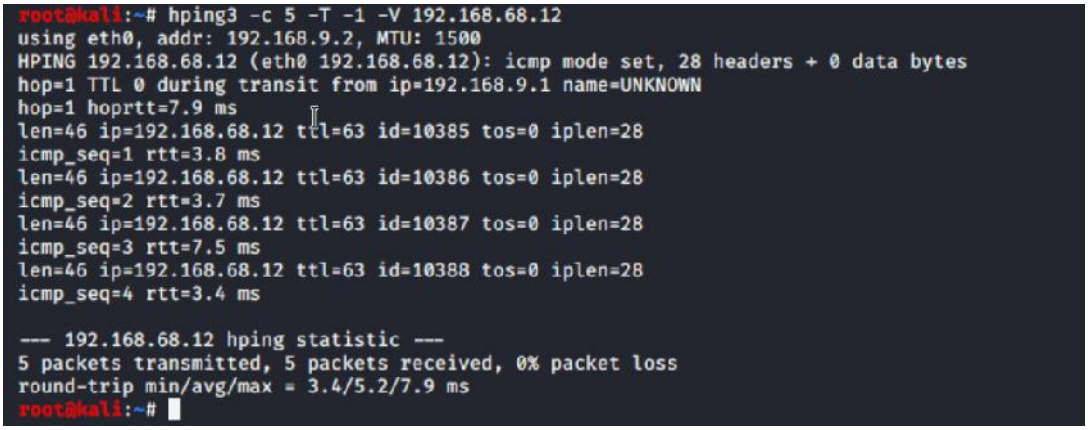
```
hping3 –c 3 -1 –V –C 13 192.168.68.12
```



Notice the retrieval of a timestamp, confirming the target is there.

9. Enter the command below to perform *traceroute* functions using *ICMP*.

```
hping3 –c 5 –T -1 -V 192.168.68.12
```



2 Using hping for Port Scanning

1. Within the *Terminal* window, click **File** and select **New Window** to launch a new one.
2. Enter the command below in the new *terminal* to start capturing packets.

```
tcpdump –i eth0
```

```
root@Kali2:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Let *tcpdump* run in the background uninterrupted.

3. *Hping* can craft packets sending various *TCP* flags set to test the ports being scanned. Send a packet with *SYN* set from a source port of 5151, which is arbitrarily chosen, to port 80 of the *OWASP* VM. Return to the other **Terminal** window and enter the command below to run a simple test.

```
hping3 –S –c 1 –s 5151 –p 80 –V 192.168.68.12
```

```
root@Kali2:~# hping3 -S -c 1 -s 5151 -p 80 -V 192.168.68.12
using eth0, addr: 192.168.9.2, MTU: 1500
HPING 192.168.68.12 (eth0 192.168.68.12): S set, 40 headers + 0 data bytes
len=46 ip=192.168.68.12 ttl=63 DF id=0 tos=0 iplen=44
sport=80 flags=SA seq=0 win=5840 rtt=1.3 ms
seq=3955549859 ack=136383868 sum=72b6 urp=0


--- 192.168.68.12 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.3/1.3/1.3 ms
```

4. Change focus to the **terminal** running *tcpdump* and notice a *SYN* [S] flag was sent with a received *Reset* [R] flag.

```
13:07:14.202107 IP 192.168.9.2.pcrd > 192.168.68.12.http: Flags [S], seq 1363838
67, win 512, length 0
13:07:14.202769 IP 192.168.68.12.http > 192.168.9.2.pcrd: Flags [S.], seq 395554
9859, ack 136383868, win 5840, options [mss 1460], length 0
13:07:14.202787 IP 192.168.9.2.pcrd > 192.168.68.12.http: Flags [R], seq 1363838
68, win 0, length 0
```


5. Change focus to the other **terminal** window and try the same scan against the firewall by entering the command below.

```
hping3 –S –c 1 –s 5151 –p 80 –V 192.168.9.1
```

```
root@Kali2:~# hping3 -S -c 1 -s 5151 -p 80 -V 192.168.9.1
using eth0, addr: 192.168.9.2, MTU: 1500
HPING 192.168.9.1 (eth0 192.168.9.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.9.1 ttl=64 DF id=49883 tos=0 iplen=44
sport=80 flags=SA seq=0 win=65228 rtt=0.5 ms
seq=484500508 ack=1138264907 sum=6621 urp=0


--- 192.168.9.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.5 ms
```

6. Change focus to the **terminal** running *tcpdump* and notice a *SYN* [S] flag was sent with a received *Reset* [R] flag.

```
12:54:21.210898 IP 192.168.9.2.pcrd > 192.168.9.1.http: Flags [S], seq 113826490
6, win 512, length 0
12:54:21.211195 IP 192.168.9.1.http > 192.168.9.2.pcrd: Flags [S.], seq 48450050
8, ack 1138264907, win 65228, options [mss 1460], length 0
12:54:21.211216 IP 192.168.9.2.pcrd > 192.168.9.1.http: Flags [R], seq 113826490
7, win 0, length 0
```

7. Change focus to the other **terminal** and enter the command below to try a different port, *SSH* port 22, against the firewall.

```
hping3 –S –c 1 –s 5151 –p 22 –V 192.168.9.1
```

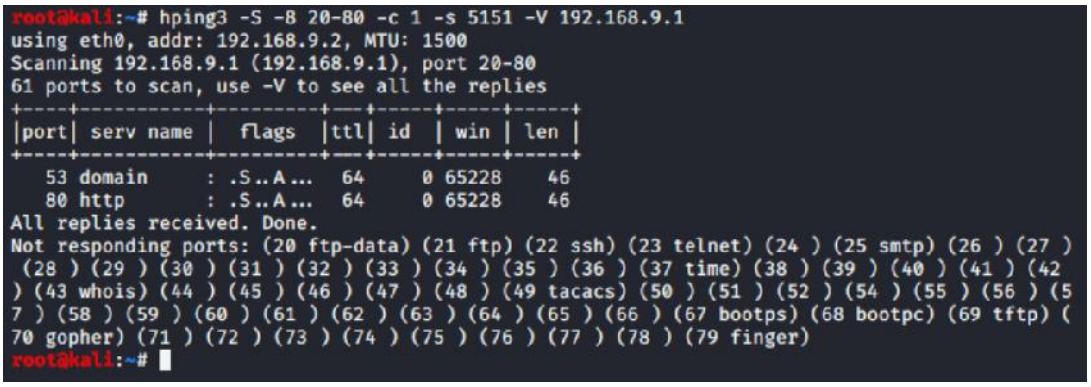
```
root@Kali2:~# hping3 -S -c 1 -s 5151 -p 22 -V 192.168.9.1
using eth0, addr: 192.168.9.2, MTU: 1500
HPING 192.168.9.1 (eth0 192.168.9.1): S set, 40 headers + 0 data bytes

--- 192.168.9.1 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Notice 100% packet loss due to port 22 being closed on the firewall.

8. Initiate a port scan against the firewall, defining a range. Enter the command below.

```
hping3 –S -8 20-80 –c 1 –s 5151 –V 192.168.9.1
```



Based on the results, the firewall has ports 53 and 80 open.

9. You may now end your reservation.

