ETHICAL HACKING
LAB SERIES

Lab 17: Packet Crafting with Hping

Material in this Lab Aligns to the Following Certification Domains/Objectives
SANS GPEN Objective
5: Exploitation Fundamentals

Document Version: 2016-03-09

Contents

Introduction

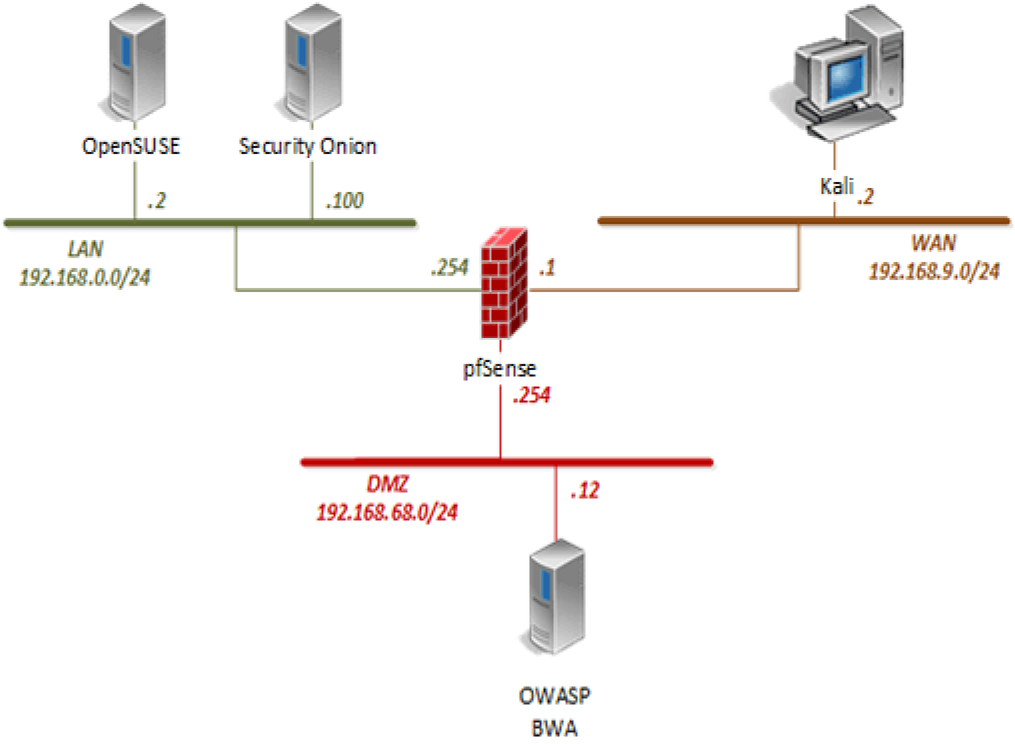
Hping is a TCP/IP packet assembler and analyzer. In this lab, we will use hping to create packets as well as perform different network functions with the packets.

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



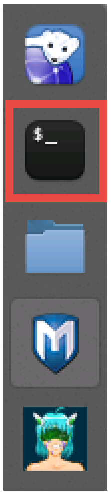
Lab Settings

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	root	toor
pfSense	192.168.0.254	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	n/a	ndg	password123

1 Using Hping as an ICMP Utility

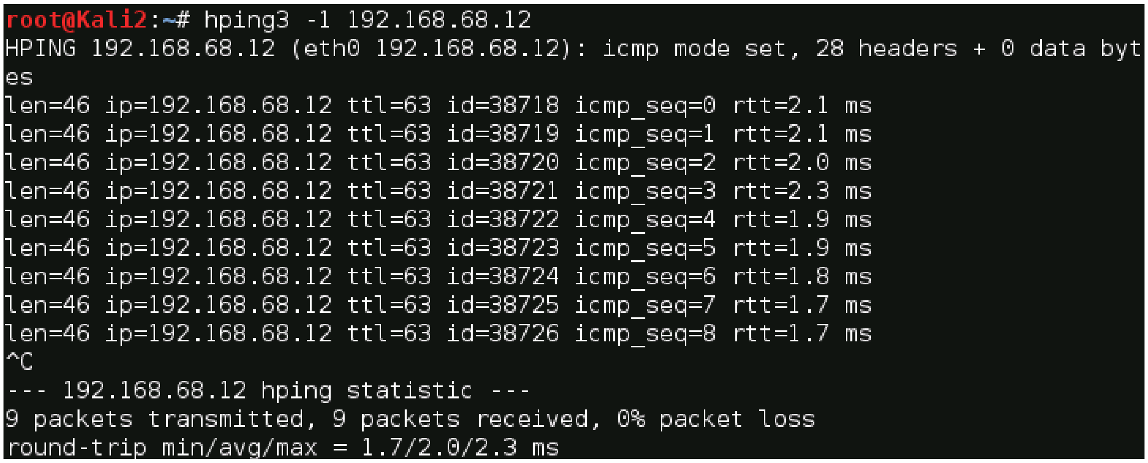
1. Navigate to the *topology* page and click on the **Kali** VM icon.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.



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 packet are transmitted, press **CTRL+C** to stop *hping* from running.

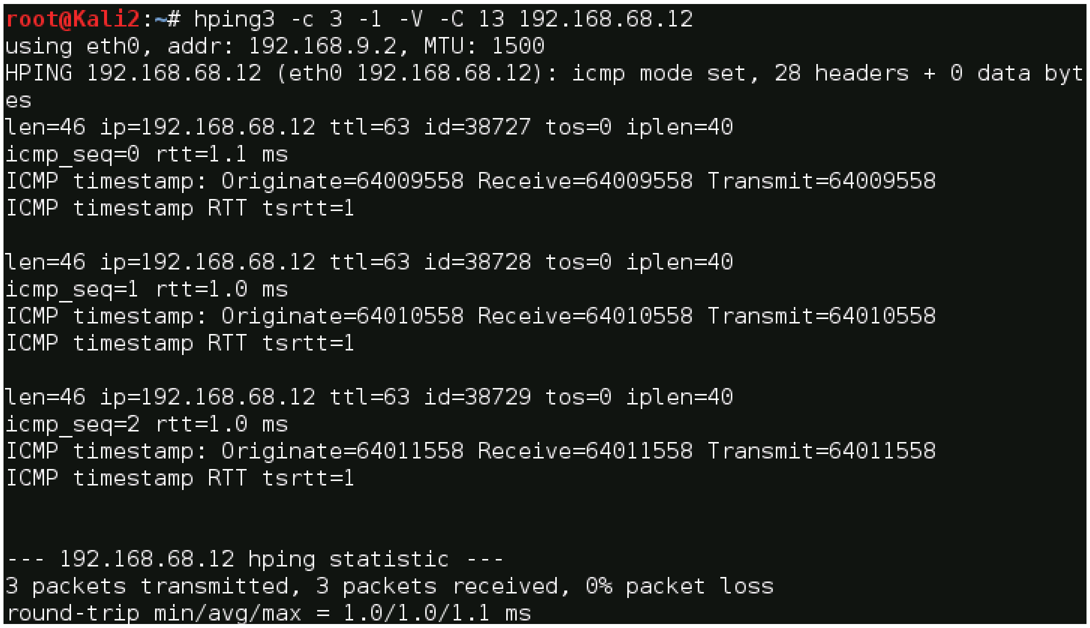


```
root@Kali2:~# hping3 -1 192.168.68.12
HPING 192.168.68.12 (eth0 192.168.68.12): icmp mode set, 28 headers + 0 data byt
es
len=46 ip=192.168.68.12 ttl=63 id=38718 icmp_seq=0 rtt=2.1 ms
len=46 ip=192.168.68.12 ttl=63 id=38719 icmp_seq=1 rtt=2.1 ms
len=46 ip=192.168.68.12 ttl=63 id=38720 icmp_seq=2 rtt=2.0 ms
len=46 ip=192.168.68.12 ttl=63 id=38721 icmp_seq=3 rtt=2.3 ms
len=46 ip=192.168.68.12 ttl=63 id=38722 icmp_seq=4 rtt=1.9 ms
len=46 ip=192.168.68.12 ttl=63 id=38723 icmp_seq=5 rtt=1.9 ms
len=46 ip=192.168.68.12 ttl=63 id=38724 icmp_seq=6 rtt=1.8 ms
len=46 ip=192.168.68.12 ttl=63 id=38725 icmp_seq=7 rtt=1.7 ms
len=46 ip=192.168.68.12 ttl=63 id=38726 icmp_seq=8 rtt=1.7 ms
^C
--- 192.168.68.12 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 1.7/2.0/2.3 ms
```

> 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
```

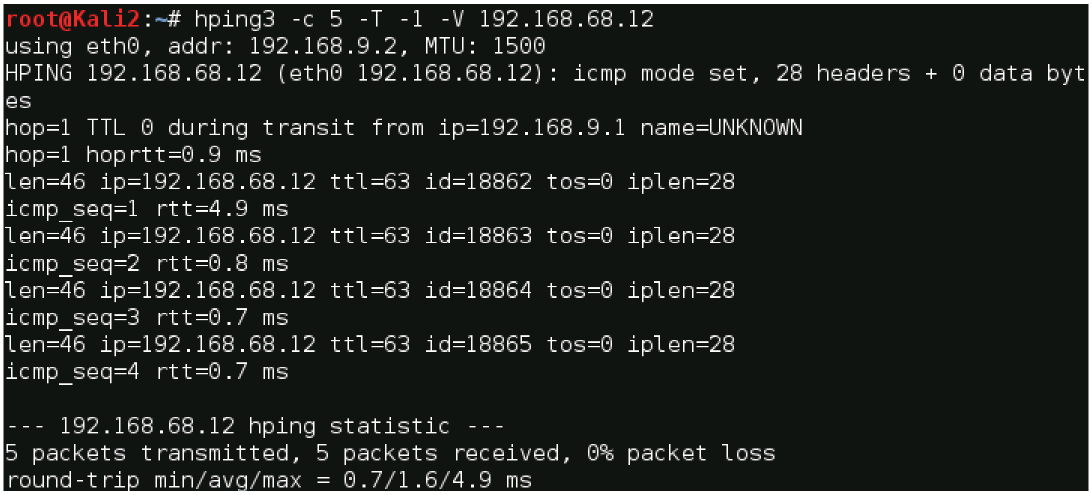


```
root@Kali2:~# hping3 -c 3 -1 -V -C 13 192.168.68.12
using eth0, addr: 192.168.9.2, MTU: 1500
HPING 192.168.68.12 (eth0 192.168.68.12): icmp mode set, 28 headers + 0 data byt
es
len=46 ip=192.168.68.12 ttl=63 id=38727 tos=0 iplen=40
icmp_seq=0 rtt=1.1 ms
ICMP timestamp: Originate=64009558 Receive=64009558 Transmit=64009558
ICMP timestamp RTT tsrtt=1

len=46 ip=192.168.68.12 ttl=63 id=38728 tos=0 iplen=40
icmp_seq=1 rtt=1.0 ms
ICMP timestamp: Originate=64010558 Receive=64010558 Transmit=64010558
ICMP timestamp RTT tsrtt=1

len=46 ip=192.168.68.12 ttl=63 id=38729 tos=0 iplen=40
icmp_seq=2 rtt=1.0 ms
ICMP timestamp: Originate=64011558 Receive=64011558 Transmit=64011558
ICMP timestamp RTT tsrtt=1


--- 192.168.68.12 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.0/1.1 ms
```

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
```

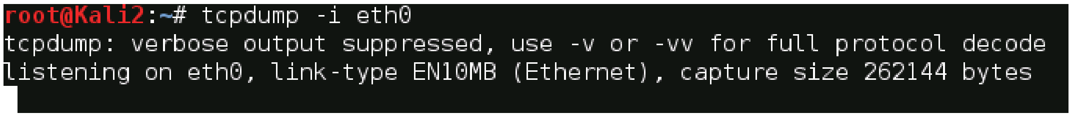


```
root@Kali2:~# hping3 -c 5 -T -1 -V 192.168.68.12
using eth0, addr: 192.168.9.2, MTU: 1500
HPING 192.168.68.12 (eth0 192.168.68.12): icmp mode set, 28 headers + 0 data byt
es
hop=1 TTL 0 during transit from ip=192.168.9.1 name=UNKNOWN
hop=1 hoprtt=0.9 ms
len=46 ip=192.168.68.12 ttl=63 id=18862 tos=0 iplen=28
icmp_seq=1 rtt=4.9 ms
len=46 ip=192.168.68.12 ttl=63 id=18863 tos=0 iplen=28
icmp_seq=2 rtt=0.8 ms
len=46 ip=192.168.68.12 ttl=63 id=18864 tos=0 iplen=28
icmp_seq=3 rtt=0.7 ms
len=46 ip=192.168.68.12 ttl=63 id=18865 tos=0 iplen=28
icmp_seq=4 rtt=0.7 ms

--- 192.168.68.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.6/4.9 ms
```

2 Using Hping for Port Scanning

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

```
tcpdump -i eth0
```

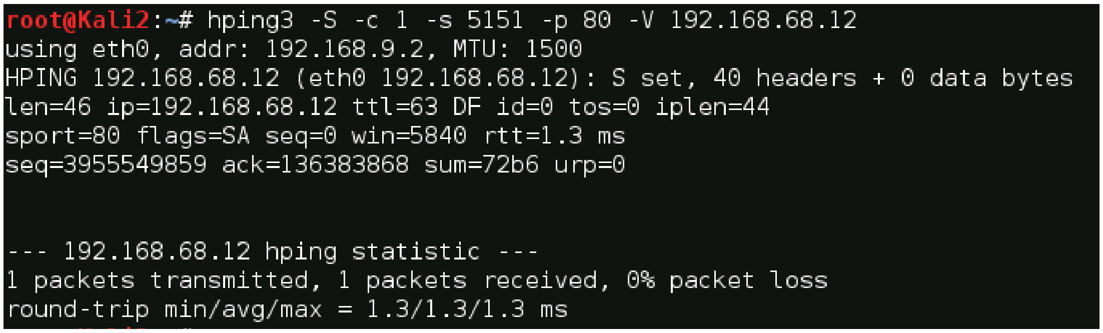


```
root@Kali2:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

> Let *tcpdump* run in the background uninterrupted.

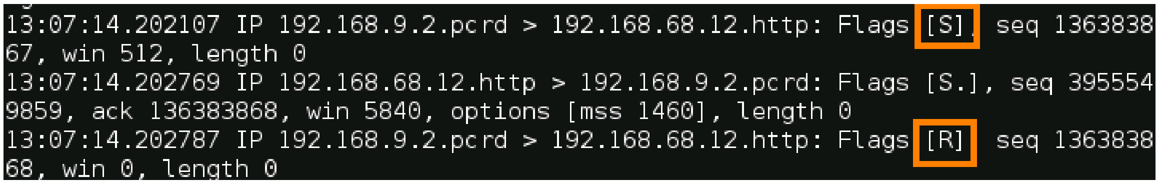
3. *Hping* can craft packets sending various *TCP* flags set to test the ports being scanned. Send a packet with *SYN* set from a source port of 5151, which is arbitrarily chosen, to port 80 of the *OWASP* VM. Return to other **Terminal** window and enter the command below to run a simple test.

```
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
```

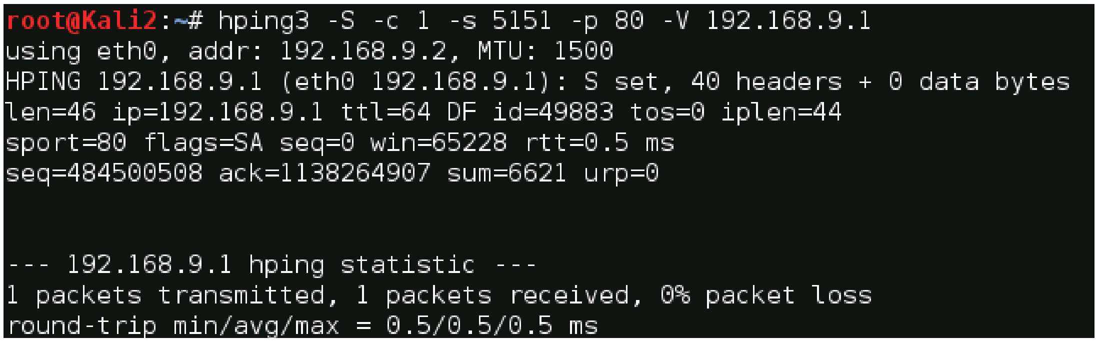
4. Change focus to the **terminal** running *tcpdump* and notice a *SYN* [S] flag was sent with a received *Reset* [R] flag.



```
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
```

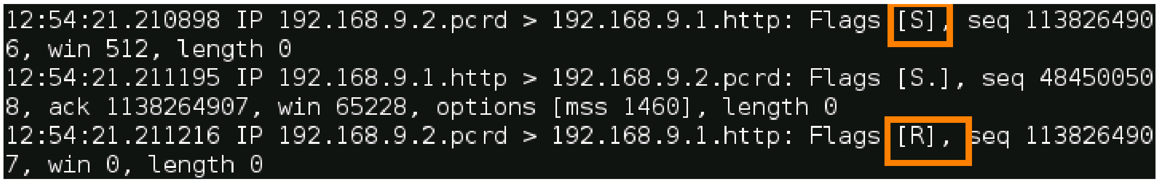
5. Change focus to the other **terminal** window and try the same scan against the firewall by entering the command below.

```
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
```

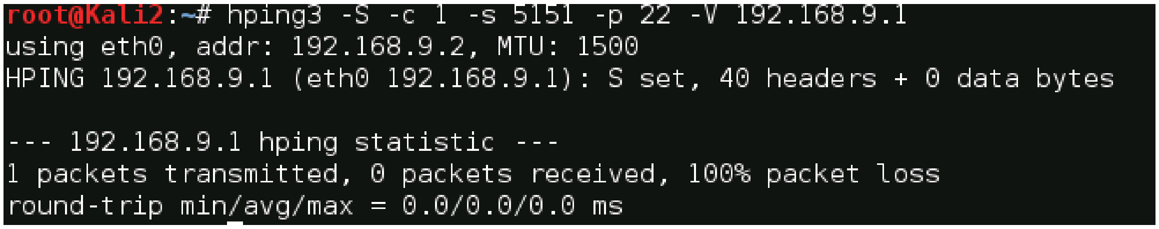
6. Change focus to the **terminal** running *tcpdump* and notice a *SYN* [S] flag was sent with a received *Reset* [R] flag.



```
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. Close the **Kali** PC viewer.