

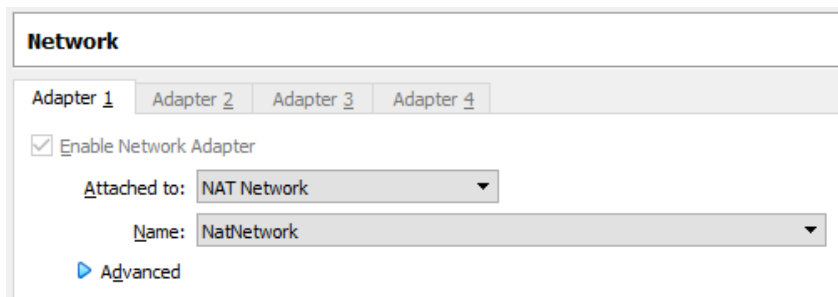
Lab - Spoof Fake TCP/IP Packets Using Hping3

Overview

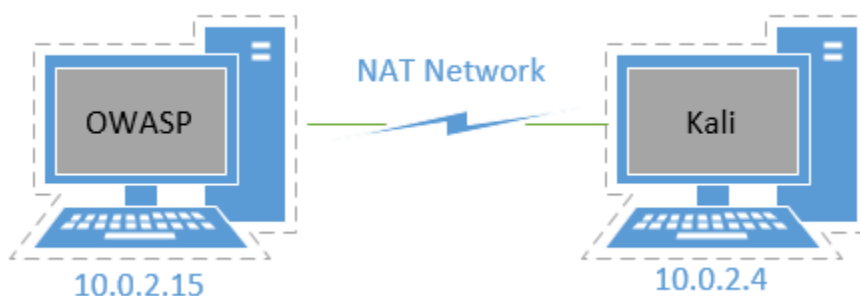
Hping3 is a terminal application for Linux that will allow us to analyze and assemble TCP/IP packets quickly. Unlike a conventional ping used to send ICMP packets, hping3 allows the sending of TCP, UDP, and RAW-IP packets. Along with the analysis of packets, this application can also be used for other security purposes, such as testing a firewall's effectiveness through different protocols, detecting suspicious or modified packets, and even protecting against attacks.

Lab Configuration

- One virtual install of Kali Linux
- One virtual install of OWASP Broken Web Application VM
- Ensure both VirtualBox network adapters are set to NAT network.



Lab Diagram



These are my IP addresses. Yours may differ!

The OWASP VM will show you its current IP address once you log on to the terminal. Username and password are provided at the terminal window.

For your Kali, open a terminal and use the `ifconfig` command to find the IP address assigned to your `eth0` adapter.

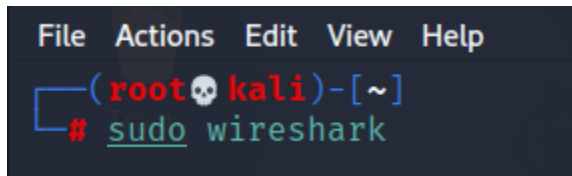
Begin the Lab!

In this lab, you will learn how to send spoofed HTTP traffic to a target system using hping3.

From your Kali desktop, launch a terminal window. If you are not logged on as root, you must prefix each CLI command with sudo.

Launch Wireshark

At the terminal prompt, type **sudo wireshark** press enter.



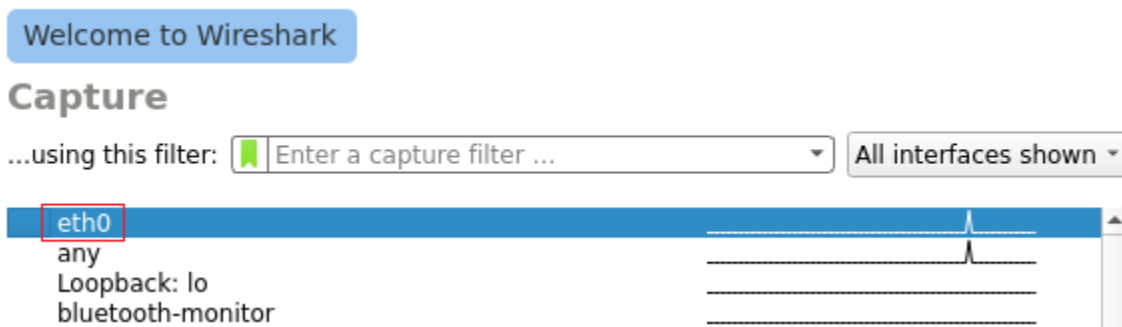
```
File Actions Edit View Help
(root🐼kali)-[~]
# sudo wireshark
```

Wireshark launches. To start the packet capture, you must first select the appropriate network interface. Notice that eth0 is selected by default. There are two methods to start the packet capturing process:

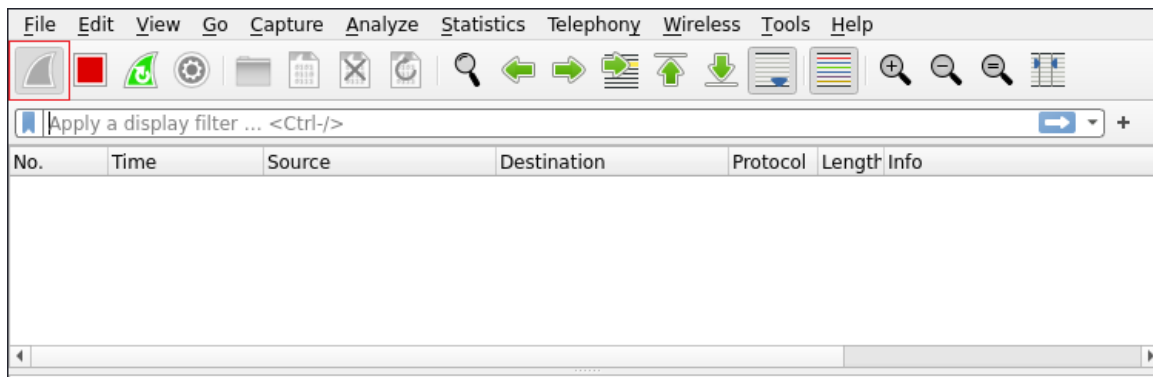
- Double-click on the network adapter name
- Click the first blue button in the icon bar below the menu.



Double-click the eth0 network adapter.



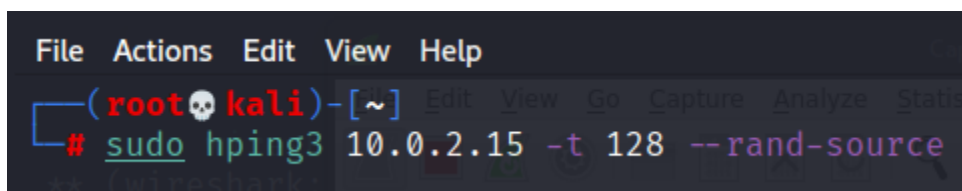
Notice the start button is greyed out. Letting you know the packet capture has started.



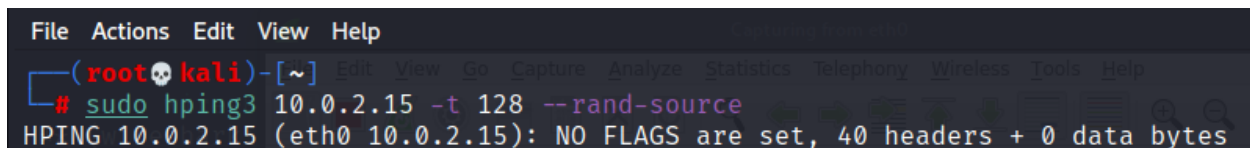
Let the packet capture run.

Open a second terminal, and at the prompt, type the following:

```
sudo hping3 10.0.2.15 -t 128 --rand-source
```

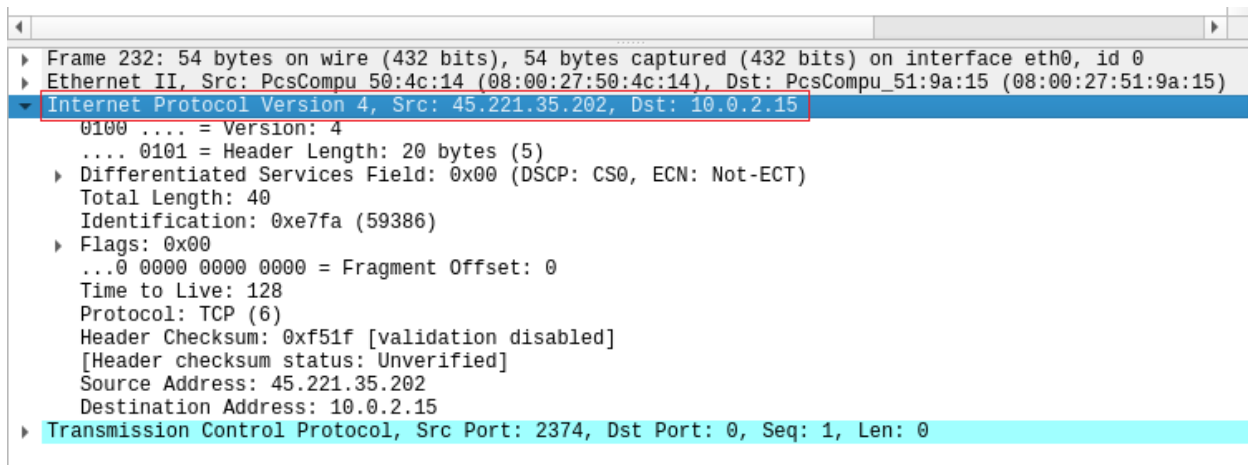


Traffic is now being sent to the target.

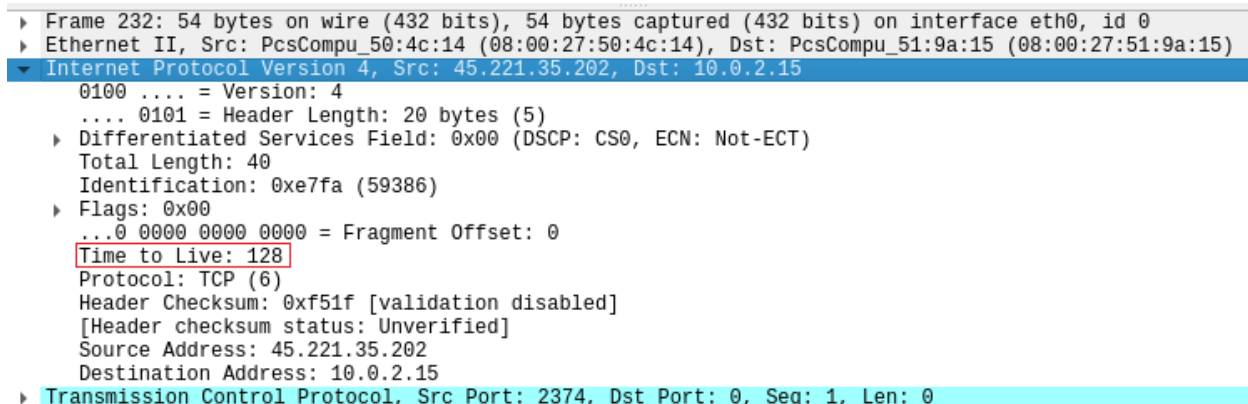


Switch over to Wireshark and stop the packet capture. Notice the IP addresses in the Source column. They are different IP addresses, but the target system in the Destination column is still the same, which is 10.0.2.15. Select any one of the spoofed IP addresses.

In the middle pane, expand Internet Protocol Version 4.

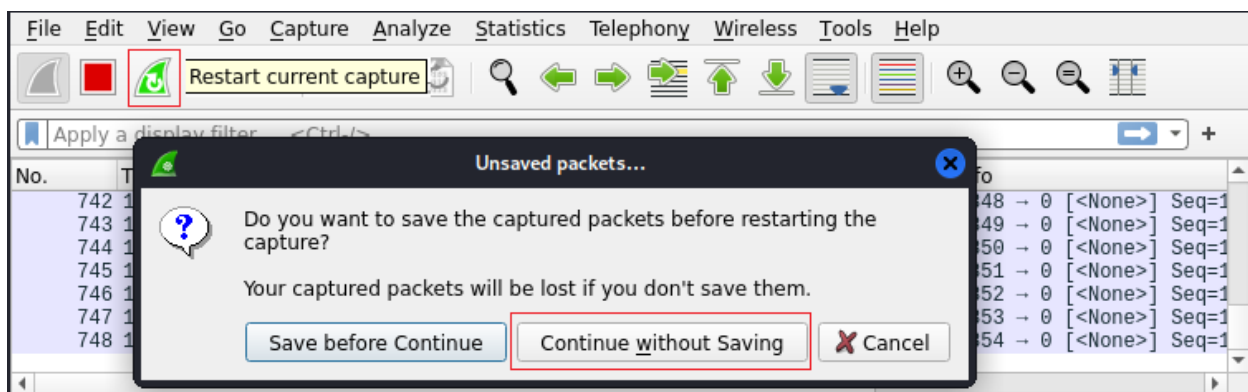


Find Time to Live. Notice that it has the value 128, which you had specified in your command.



Notice that the Source Address is randomly generated in the same section using the **--rand-source** command, but the target IP remains unchanged.

Switch back to the Wireshark window and start a new scan. When prompted, click Continue without Saving.



We can also send the spoofed traffic to a particular port. Let's send our spoofed traffic using port 80. To do this, type the following command:

```
sudo hping3 10.0.2.15 -t 128 -p 80 --rand-source
```

```
File Actions Edit View Help
(rootkali)-[~]
# sudo hping3 10.0.2.15 -t 128 -p 80 --rand-source
```

```
(rootkali)-[~]
# sudo hping3 10.0.2.15 -t 128 -p 80 --rand-source
HPING 10.0.2.15 (eth0 10.0.2.15): NO FLAGS are set, 40 headers + 0 data bytes
```

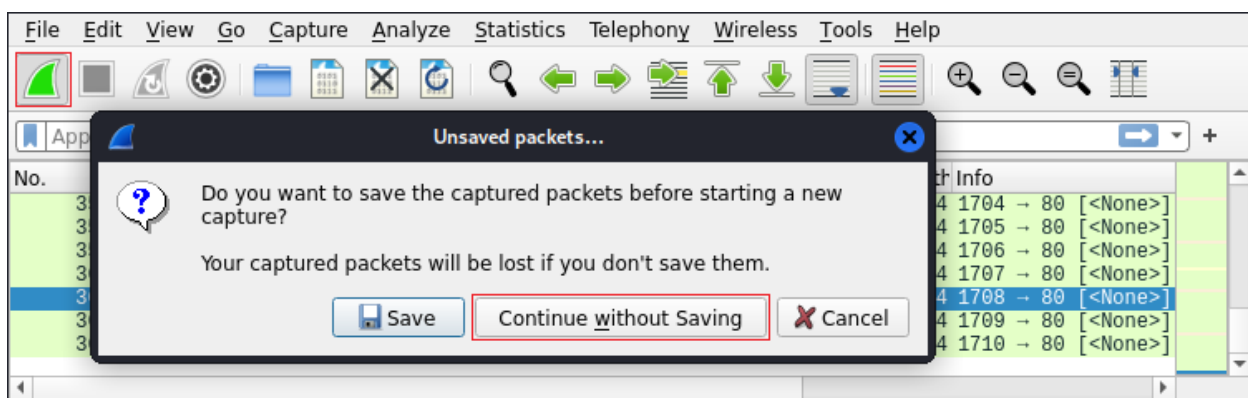
Traffic is now being sent to the target system using the specified port.

Minimize the terminal window and restore the Wireshark window. Stop the packet capture. Select any packet, and in the middle windowpane, expand Transmission Control Protocol.

Notice that the Destination Port mentions 80, which you had specified in the command.

```
Transmission Control Protocol, Src Port: 1708, Dst Port: 80, Seq: 1, Len: 0
Source Port: 1708
Destination Port: 80
[Stream index: 325]
[Conversation completeness: Incomplete (0)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1798496126
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1157359377
```

Start a new packet capture without saving the existing one.



Switch back to the terminal window that had executed the previous command and close the terminal.

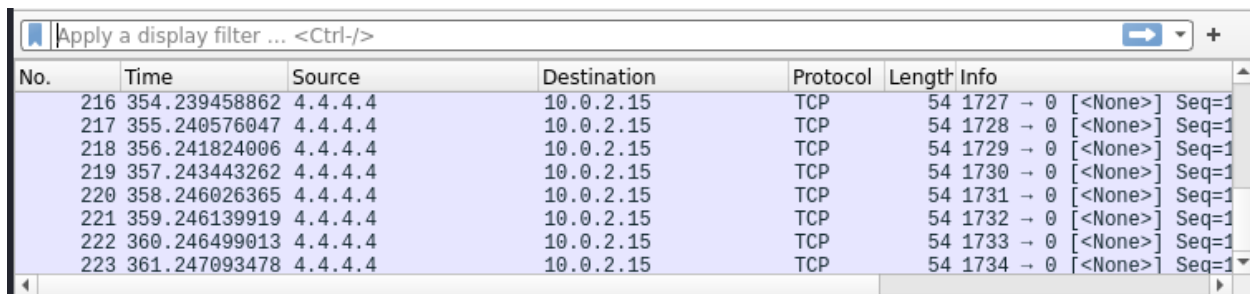
Open a new terminal.

We can also spoof a specific IP address. Let's use the spoofed IP address of 4.4.4.4 and send the traffic to the target system.

Use the following command.

```
sudo hping3 10.0.2.15 -t 128 -a 4.4.4.4
```

Switch to the Wireshark window. Notice that the traffic is now originated from 4.4.4.4 and sent to 10.0.2.15.

A screenshot of the Wireshark network protocol analyzer interface. The top bar shows a display filter: "Apply a display filter ... <Ctrl-/>". Below this is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets shown are all TCP connections from source IP 4.4.4.4 to destination IP 10.0.2.15. The sequence numbers for the SYN packets range from 1727 to 1734. The "Info" column shows details like "Seq=1" and "[<None>]".

No.	Time	Source	Destination	Protocol	Length	Info
216	354.239458862	4.4.4.4	10.0.2.15	TCP	54	1727 → 0 [<None>] Seq=1
217	355.240576047	4.4.4.4	10.0.2.15	TCP	54	1728 → 0 [<None>] Seq=1
218	356.241824006	4.4.4.4	10.0.2.15	TCP	54	1729 → 0 [<None>] Seq=1
219	357.243443262	4.4.4.4	10.0.2.15	TCP	54	1730 → 0 [<None>] Seq=1
220	358.246026365	4.4.4.4	10.0.2.15	TCP	54	1731 → 0 [<None>] Seq=1
221	359.246139919	4.4.4.4	10.0.2.15	TCP	54	1732 → 0 [<None>] Seq=1
222	360.246499013	4.4.4.4	10.0.2.15	TCP	54	1733 → 0 [<None>] Seq=1
223	361.247093478	4.4.4.4	10.0.2.15	TCP	54	1734 → 0 [<None>] Seq=1

Summary

In the short lab, you learned how to spoof your source IP address using hping3. You may see the following scenario on your certification exam where you need to spoof your source IP address. Which of the following tools could you use? The answer is hping3.

End of the lab!