Hping3 Spoof IP Address

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

The **hping3** command in Kali Linux is a network tool used for sending custom ICMP, UDP, and TCP packets. It's often employed for network testing and troubleshooting.

There are potential security risks associated with MAC address spoofing, such as bypassing MAC address filtering or impersonating other devices on the network.

It is important to obtain proper authorization before attempting any form of network manipulation or spoofing.

NOTE: Don't do this lab on any network than one that you own or have permission to use.

Update Kali

1. Open **Terminal**. (Look in the topbar.) Run the following commands. These commands will update Kali.
2. **sudo apt update** (This command gets the lists of updates and upgrades. If you receive an error on this step, restart Kali.)
3. **sudo apt upgrade** (This command installs the updates and upgrades. There should be a bunch of different updates.)

4. There may be some screens of information, press Enter until the upgrade process continues and completes. Restart Kali at the end of the update process. Kali may take longer than usual to start, be patient.

Getting Started

1. Start your Windows and Kali Linux virtual machines.
2. Logon to the Windows virtual machine.
3. Click **Start**, type in **Windows Firewall**. Click **Windows Firewall**. Click **Turn Windows Firewall on or off**. Turn the Windows Firewall off for both networks. Click **OK**.
4. Right Click **Start** → Click **Command Prompt** → Type in **ipconfig**. Press the **Enter key**. Note the IP address.
5. **Insert a screenshot.**

Click or tap here to enter text.

Normal IP Packets

Our first step is to send some normal IP packets to ensure we have connectivity between our virtual machines. We will capture these packets to see what normal IP packets look like. The source and destination IP addresses will have unique MAC addresses.

1. Logon to Kali Linux
2. At the Terminal prompt, type:
   sudo hping3 –1 WindowsIPAddress
   (Substitute the IP address you discovered earlier for WindowsIPAddress.)
   Press the **Enter key**.

You should see successful replies from the other virtual machine. If not, check the Windows firewall and ip address to make sure they are set properly.

3. **Paste a screenshot of the Terminal window with successful pings.**

Click or tap here to enter text.

4. Type **CTRL C** to stop hping3.
5. Go to the Kali menu in the upper left corner. Type **Wireshark** → Click Wireshark to start the program.

6. Click the **Capture** menu → Click **Options** → Click **eth0** → Click **Start**.

7. Click the Terminal icon on the top bar. This will create a new terminal session.

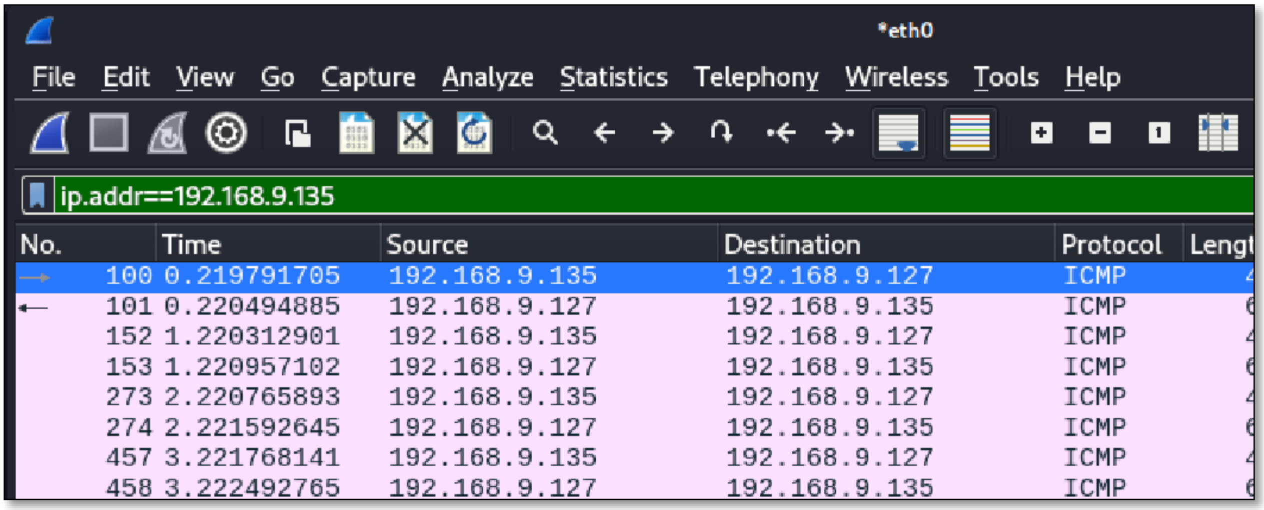
8. Type
   sudo hping3 –1 WindowsIPAddress
   (Substitute the IP address you discovered earlier for WindowsIPAddress.)
   Press the **Enter** key.

9. Click **Wireshark**. Click the **Stop** button.

Let's setup a filter to see only the traffic between the two machines.

10. In the filter bar: **ip.addr==WindowsIPAddress**

Example from my network. Notice the normal ping packets going back and aforth.



ip.addr==192.168.9.135

	No.	Time	Source	Destination	Protocol	Lengt
→	100	0.219791705	192.168.9.135	192.168.9.127	ICMP	4
←	101	0.220494885	192.168.9.127	192.168.9.135	ICMP	6
	152	1.220312901	192.168.9.135	192.168.9.127	ICMP	4
	153	1.220957102	192.168.9.127	192.168.9.135	ICMP	6
	273	2.220765893	192.168.9.135	192.168.9.127	ICMP	4
	274	2.221592645	192.168.9.127	192.168.9.135	ICMP	6
	457	3.221768141	192.168.9.135	192.168.9.127	ICMP	4
	458	3.222492765	192.168.9.127	192.168.9.135	ICMP	6

11. Paste a screenshot of Wireshark.

Click or tap here to enter text.

12. Click back to your Terminal session. Press CTRL C to break the hping3 command if it is still running.

Spoofed IP Packets

We will make the Windows computer think the packets we are sending are from itself. We will spoof our IP address.

1. In Wireshark → Click **Start** to start capturing packets.

2. Type **sudo hping3 -S WindowsIPAddress -a WindowsIPAddress** (Substitute the IP address you discovered earlier for WindowsIPAddress.)

   a) **-a** spoof our Kali IP address using the target Windows MAC address

3. Press the **Enter key**..

4. **Insert a screenshot.**

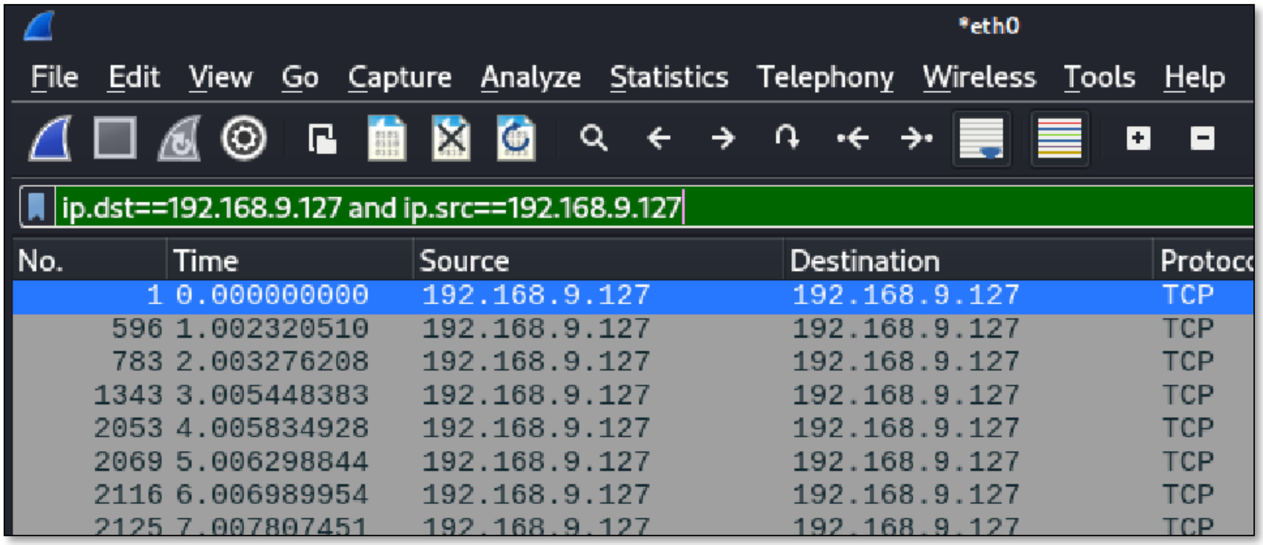
Click or tap here to enter text.

5. Hping3 will show the source and destination IP address are the same, but you won't see packets being sent.

6. Click **Wireshark**. Click the **Stop** button.

13. Apply filter: **ip.dst==WindowsIPAddress and ip.src==WindowsIPAddress**

Example from my network. Notice that the source and destination are the same.



ip.dst==192.168.9.127 and ip.src==192.168.9.127

No.	Time	Source	Destination	Protoco
1	0.000000000	192.168.9.127	192.168.9.127	TCP
596	1.002320510	192.168.9.127	192.168.9.127	TCP
783	2.003276208	192.168.9.127	192.168.9.127	TCP
1343	3.005448383	192.168.9.127	192.168.9.127	TCP
2053	4.005834928	192.168.9.127	192.168.9.127	TCP
2069	5.006298844	192.168.9.127	192.168.9.127	TCP
2116	6.006989954	192.168.9.127	192.168.9.127	TCP
2125	7.007807451	192.168.9.127	192.168.9.127	TCP

You should see a capture where the source and destination packets have the same IP address. Notice that the MAC addresses are still different. Remember, you could also spoof your MAC address to be exactly the same as the Windows computer.

You have successfully spoofed your IP address. The Windows computer has no way of knowing that the ping from the Kali Linux didn't come from itself. The only way it would know is to look at the MAC addresses, which can also be spoofed. By looking at the traffic on the network, you have no way of knowing where the packet actually came from.

5. **Paste a screenshot of WireShark showing the identical IP addresses in the source and destination.**

Click or tap here to enter text.

Assignment Submission

Attach this document to the assignment in Blackboard.