Network Penetration Testing Methodology-Internal

6 Hr 44 Min Remaining

Instructions Resources Help  100%

Exercise 2: Scanning and Scripting with hping3

Scenario

To begin the lab, a proficient tester may use any tool depending on his or her personal preference. The objective of this lab is to help students use the hping3 tool.

In this lab, you will:

* Start the hping3 tool
* Conduct a query with hping3
* Check hping3 capabilities
* Execute a simple script within the hping3 command environment
* Capture packets with hping3
* Conduct a hping3 scan
* Review the data from the scan
* Send files using ICMP

**Lab Duration**: **10** Minutes

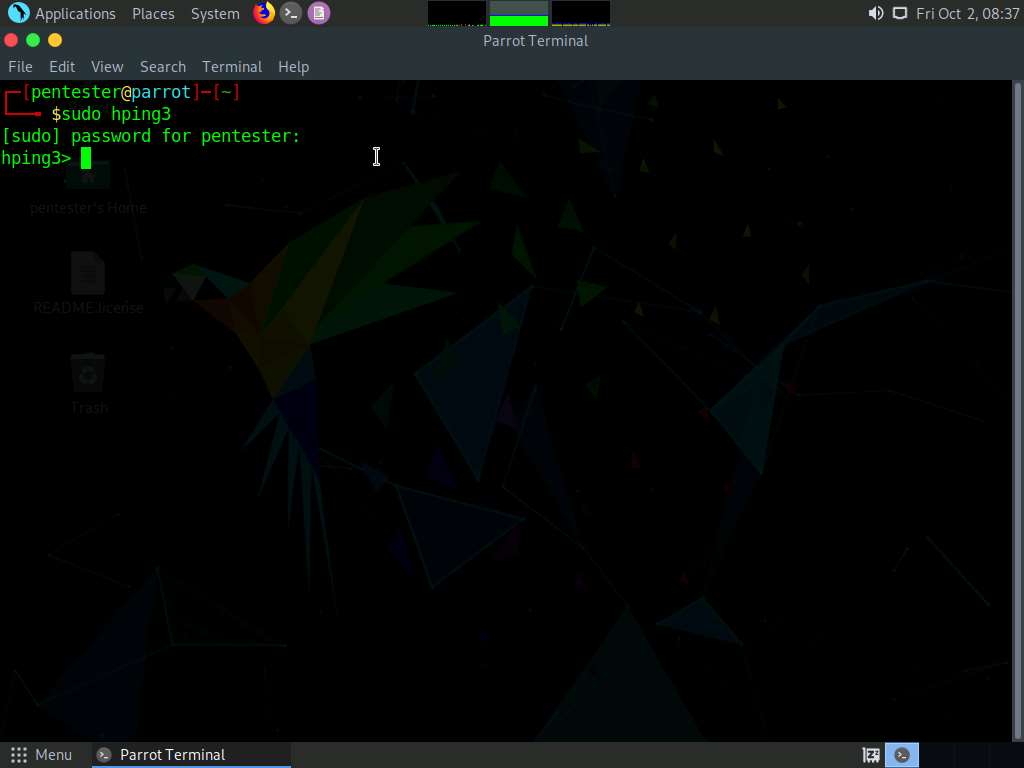
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



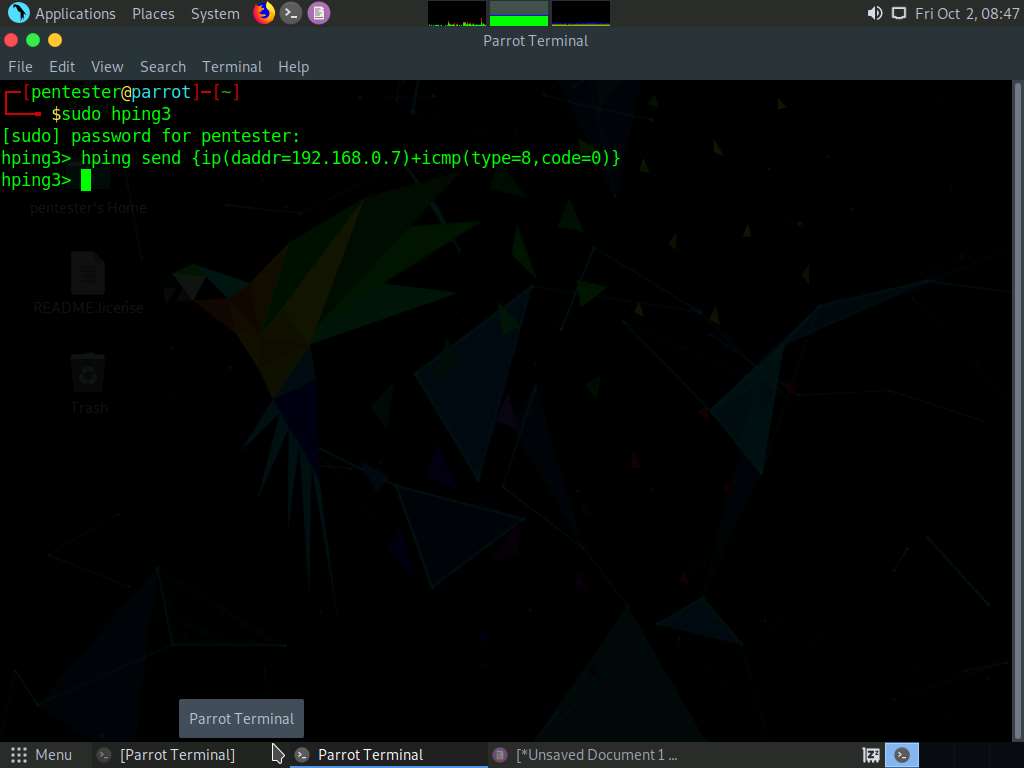
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



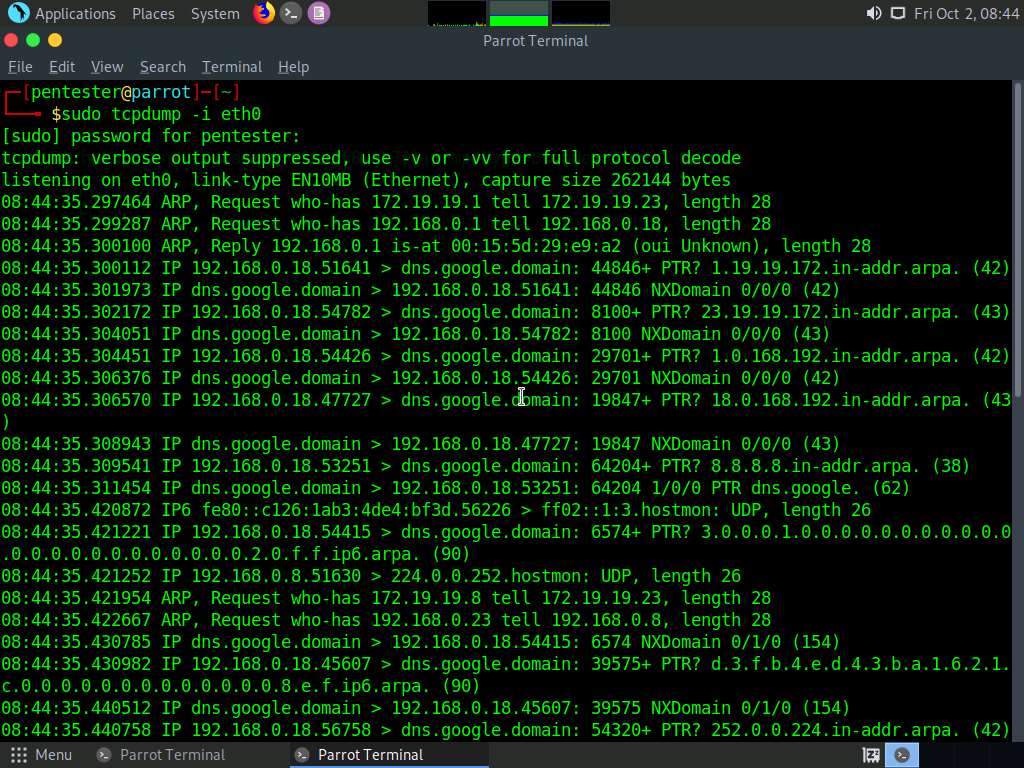
1. In a terminal window, type sudo hping3 and press Enter. This will show the tool options.
2. Hping3 is a powerful tool. It is a TCL scripting engine contained within a shell. For the first attempt, practice with a few commands.
3. To begin the lab, launch **hping3** by issuing the command **sudo hping3** in a command line terminal. If you are asked you enter a password, type **toor** and press **Enter**.

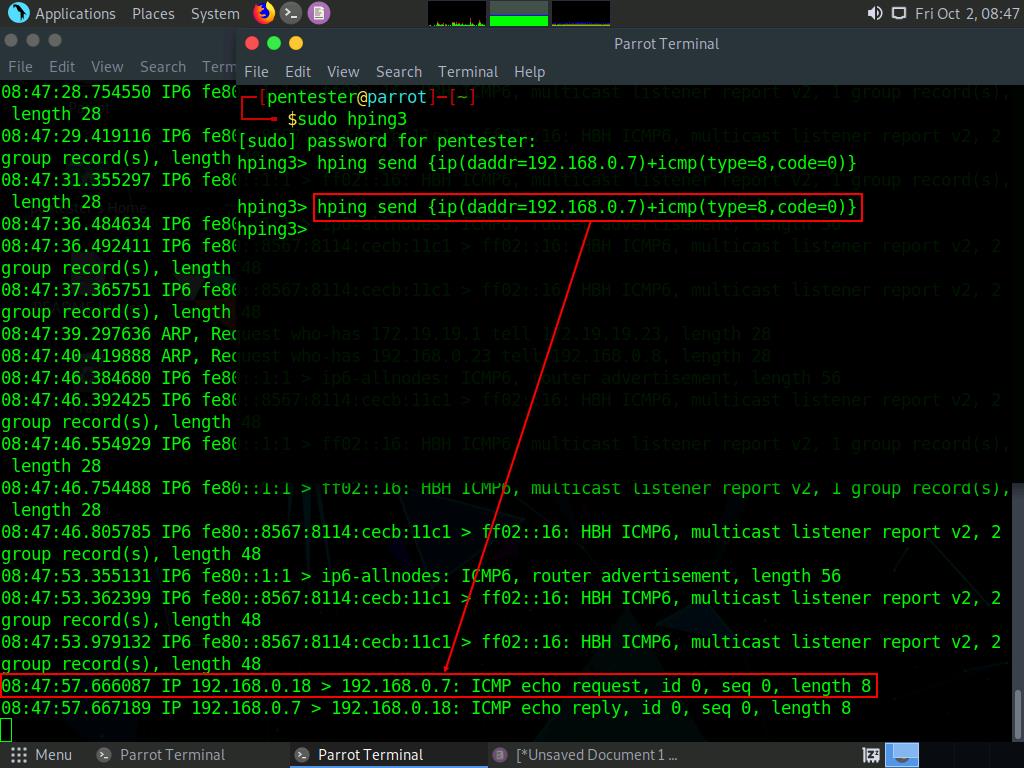


1. The first command will send a simple Internet Control Message Protocol (ICMP) echo request to a target. Select one of the available targets you have discovered and enter the following command, replacing the IP address with that of the machine you are targeting. In this lab, we are targetting **192.168.0.7**. So, type **hping send {ip(daddr=192.168.0.7)+icmp(type=8,code=0)}**. Press **Enter**. This command will send an ICMP type 8 code 0 echo request to a target, as shown in the screenshot.



1. If the ICMP echo request is not visible, verify it by opening a new terminal window; type **sudo tcpdump –i eth0** and press **Enter**. If you are asked you enter a password, type **toor** and press **Enter**. This will capture the network traffic. Run the command again and watch the output of the tcpdump command.

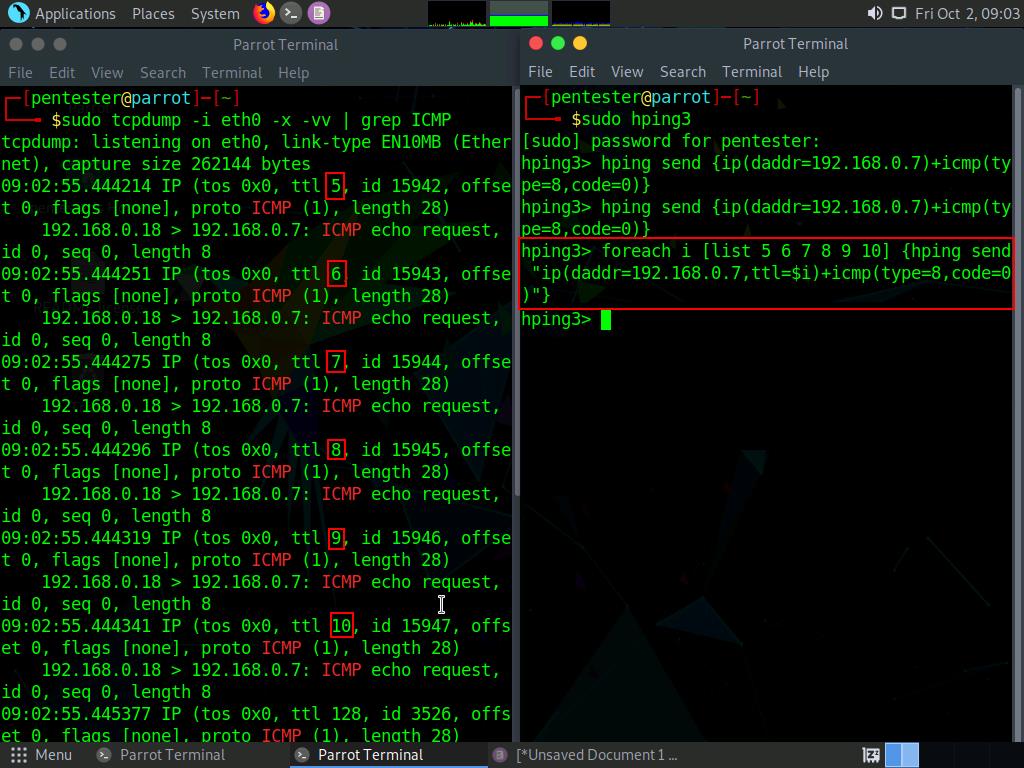




1. Start a query using the scripting capability of the TCL language. The basic syntax is easy to use. In the hping3 terminal window, type the following command (all on one line) and press **Enter**:

**foreach i [list 5 6 7 8 9 10] {hping send "ip(daddr=192.168.0.7,ttl=$i)+icmp(type=8,code=0)"}**

This command will set the time-to-live (TTL) at 5, and then increment it by 1 when it sends an ICMP echo request. The output will take time to appear; you may run tcpdump and capture it by entering **sudo tcpdump –i eth0 –x –vv | grep ICMP**, as shown in the screenshot.



1. Next, identify the capability of hping3 to receive packets. Enter a simple loop to receive packets. In the hping3 terminal window, enter the following command:

**while 1 {**

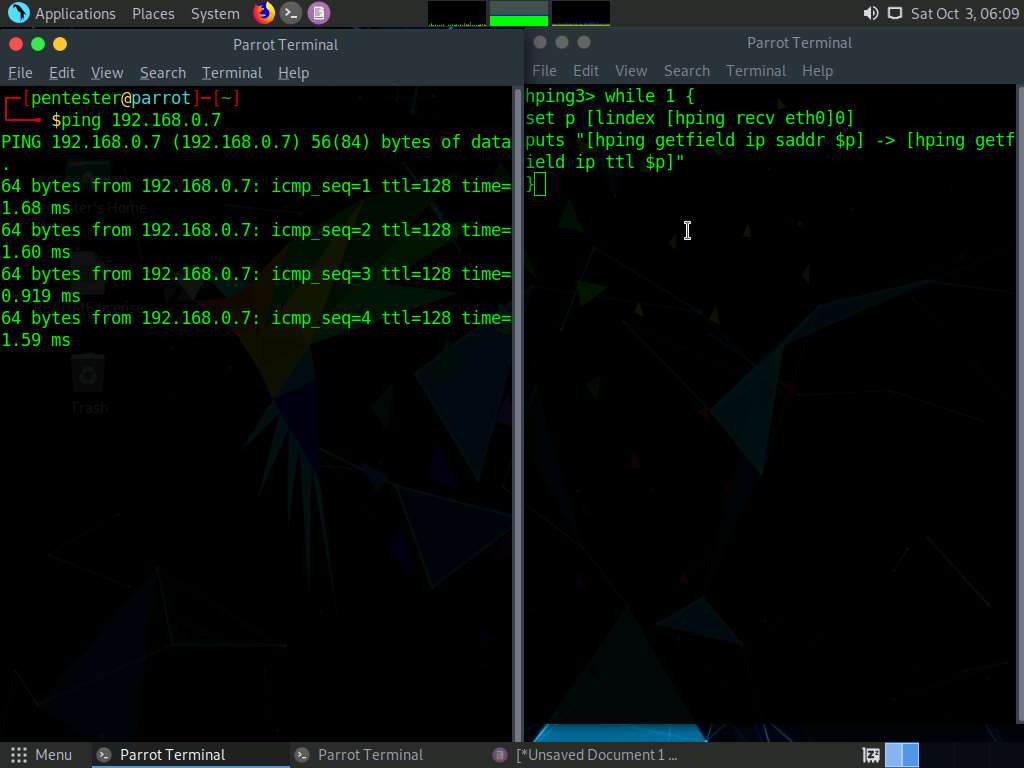
**set p [lindex [hping recv eth0] 0]**

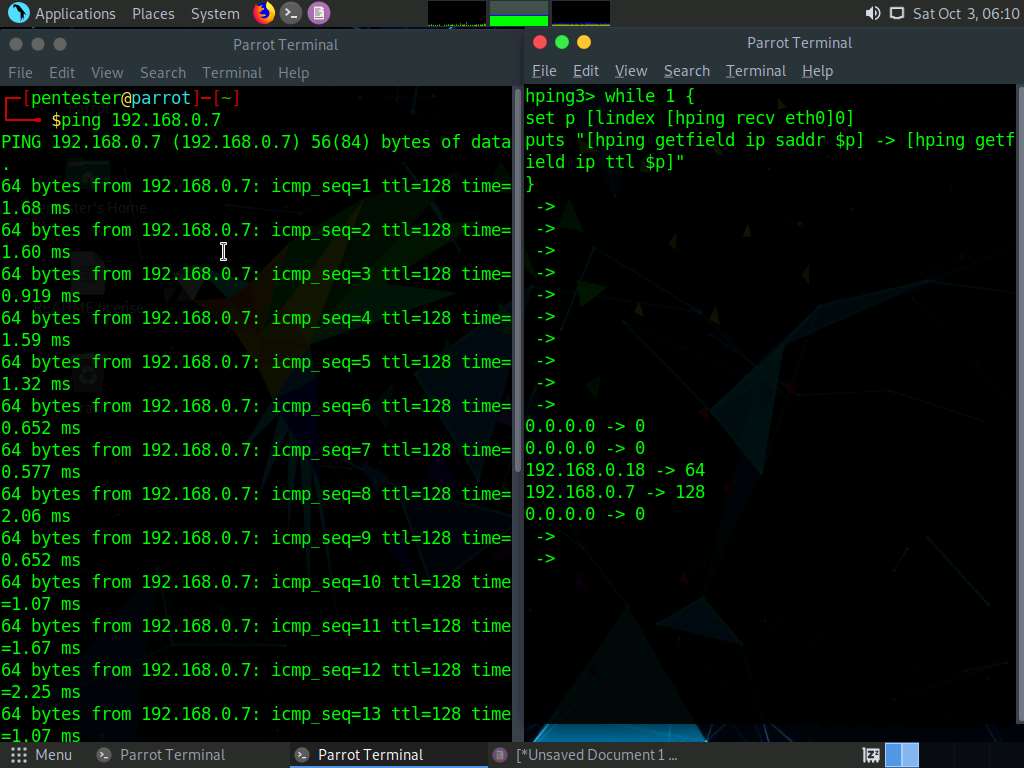
**puts "[hping getfield ip saddr $p] -> [hping getfield ip ttl $p]"**

**}**

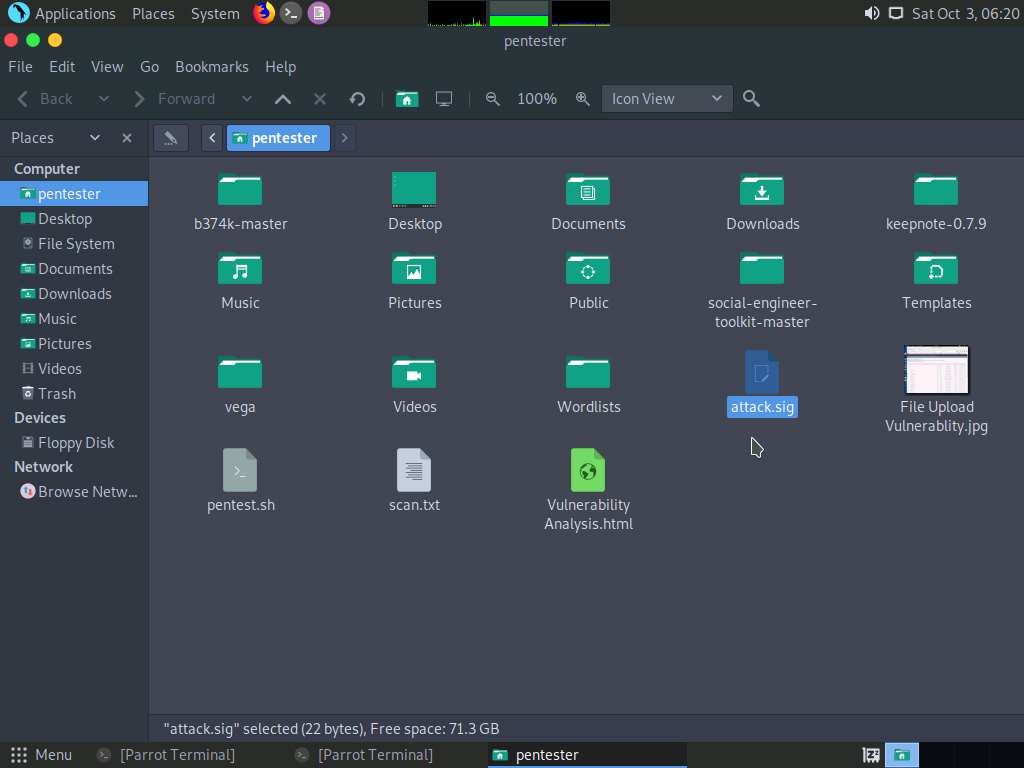
1. The command shown above will help loop and receive packets until you press **Ctrl+C** to stop the loop.

Enter the commands exactly as shown above to keep the codes valid. To scroll through the packets view, open a new terminal window and ping a target by typing **ping 192.168.0.7**, as shown in the screenshot.

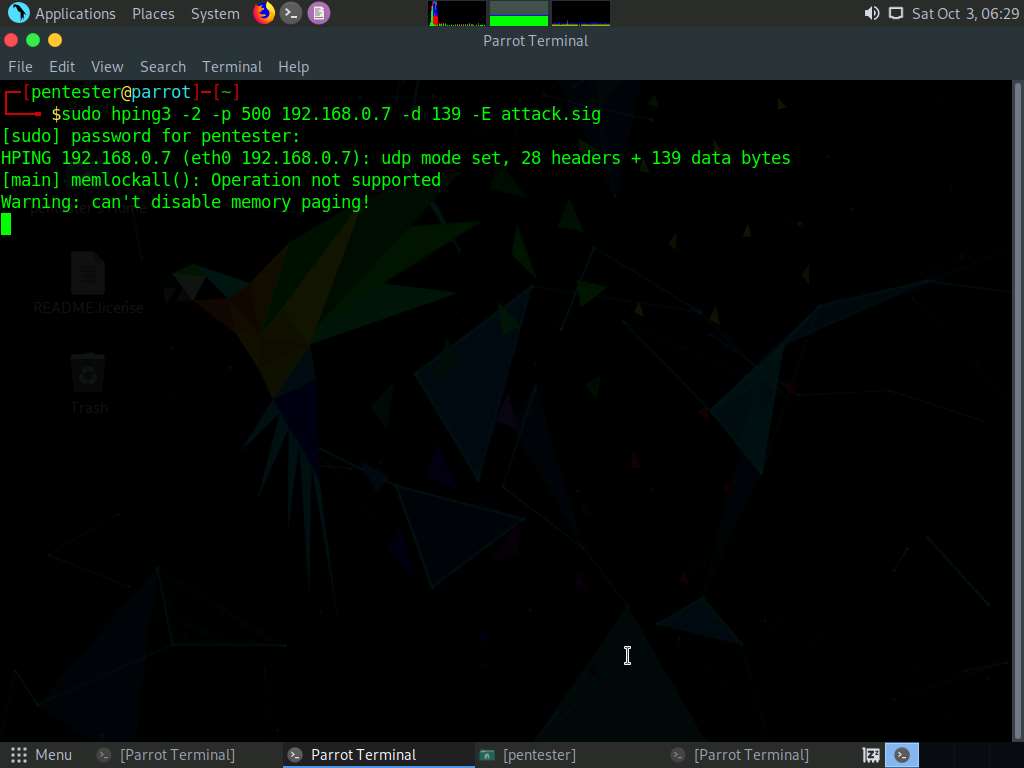




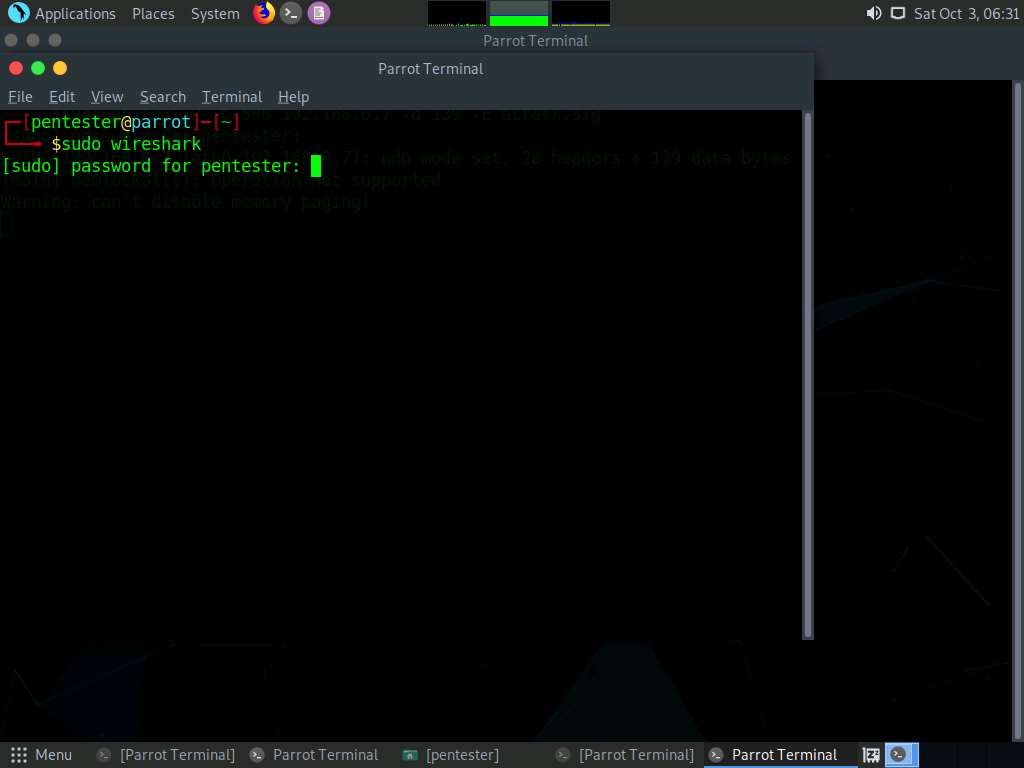
1. Using your chosen text editor, type “**You are under attack!**” and save the file as **attack.sig** in **Home folder**.



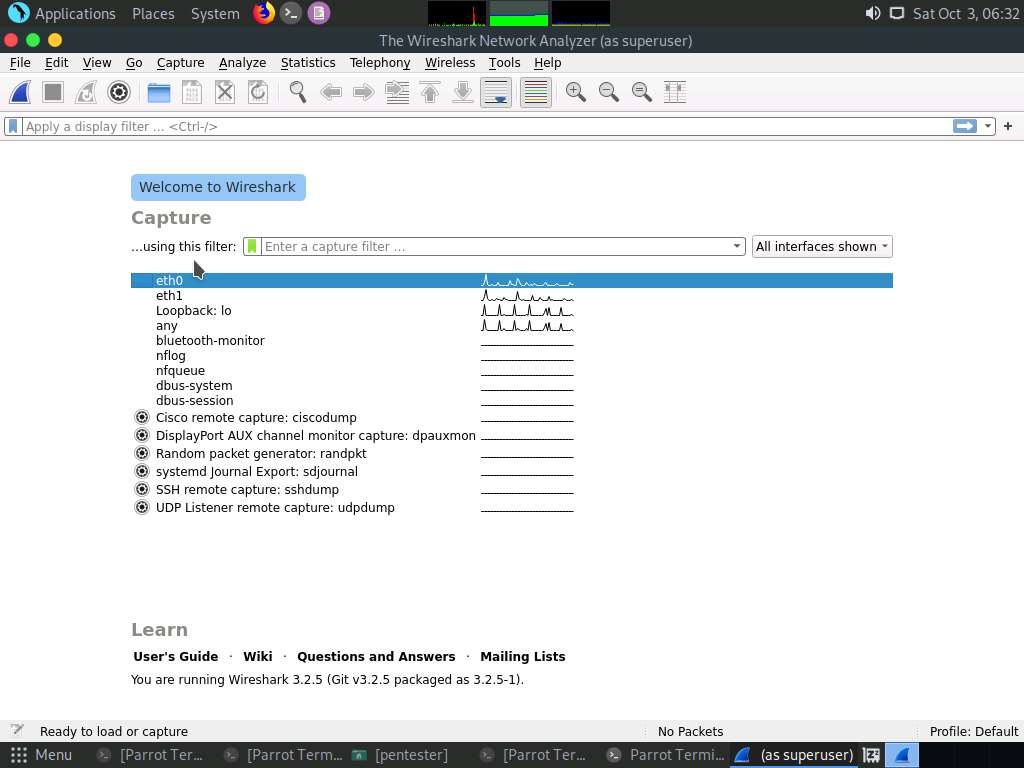
1. The hping3 tool allows users to send messages. Accordingly, send the message as a string. Open a new terminal window, type **sudo hping3 -2 -p 500 192.168.0.7 -d 139 -E attack.sig**, and press **Enter**. Type **toor** in the password field and press **Enter**. This will send the packet to port 139 from port 500.



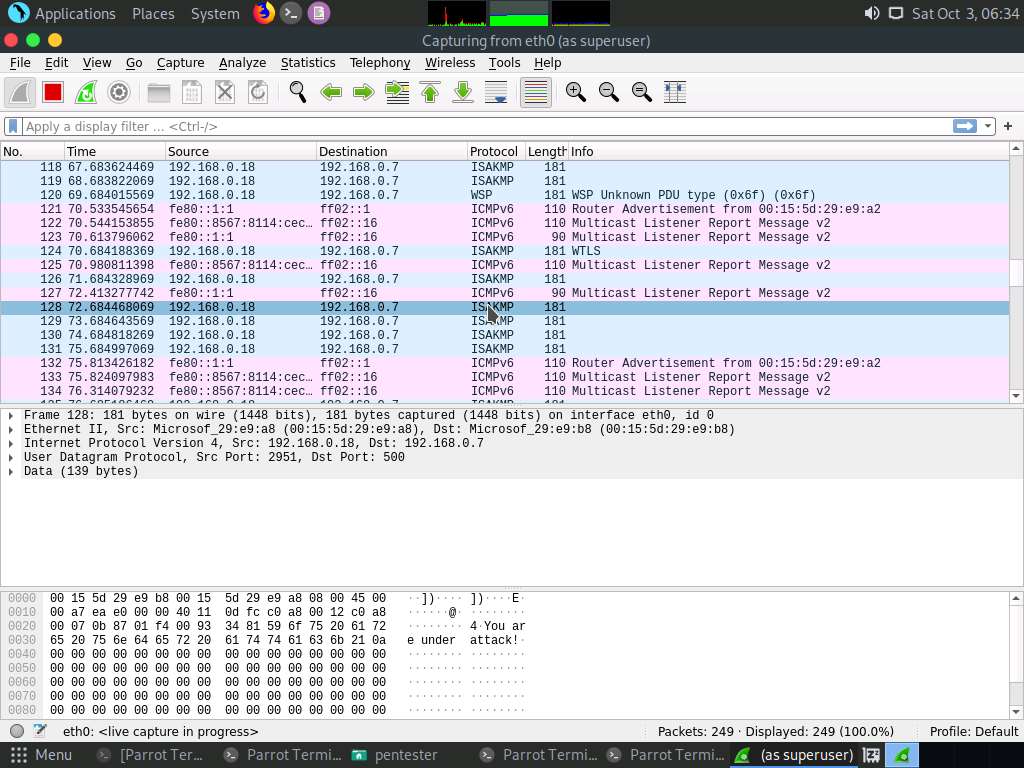
1. Use Wireshark to view the packet information. In a new terminal window, type **sudo wireshark** press **Enter**. If you are asked to enter the password, enter **toor**.



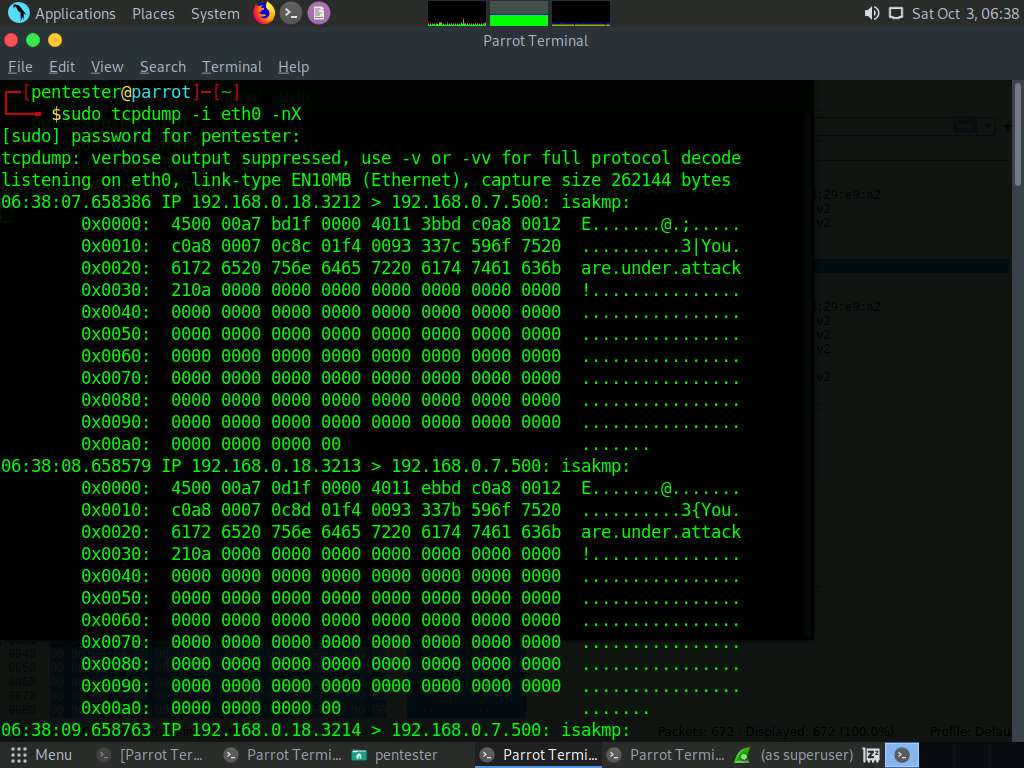
1. **Wireshark** GUI appears, select **eth0** interface.



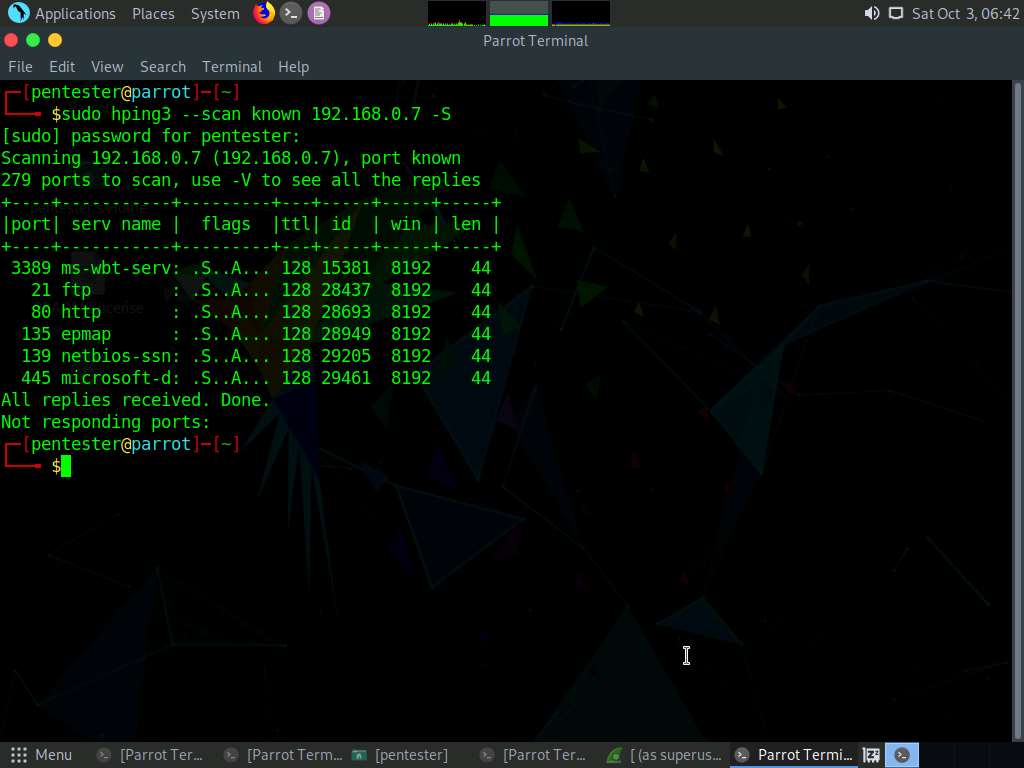
1. The window shows the Internet Security Association and Key Management Protocol (ISAKMP) traffic, as you are using User Datagram Protocol (UDP) port 500. The lower window also shows that the message you specified is carried within the packet.



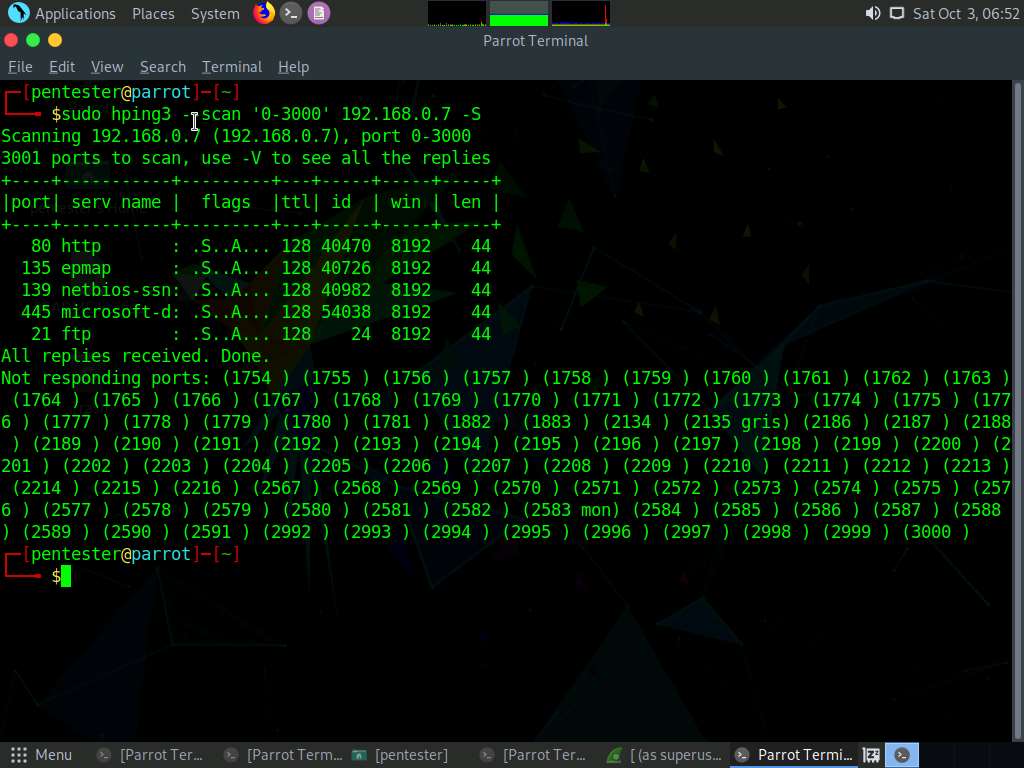
1. The message in the packet can also be displayed using tcpdump: Type **sudo tcpdump –i eth0 –nX** in the terminal window. If you are asked to enter the password, enter **toor**.



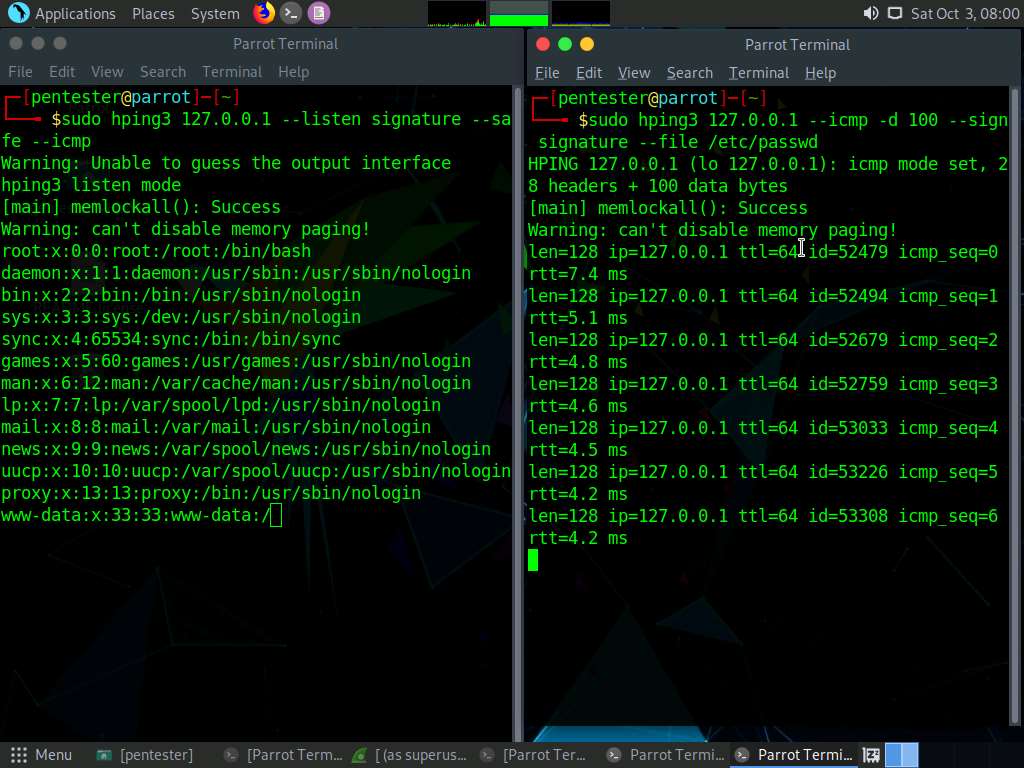
1. Scan a target using hping3. Open a new terminal window and enter **sudo hping3 --scan known 192.168.0.7 -S**. This command displays the list of open ports/services running on the target.



1. Hping3 is a powerful scanning tool that, in the previous example, only showed the known option for the ports listed in /etc/services. Next, specify a range to scan. In the terminal window, enter **sudo hping3 --scan ‘0-3000’ 192.168.0.7 –S**, as shown in the screenshot.



1. Finally, send files using the ICMP. Open two terminal windows and position them side-by-side.
2. In the first terminal window, enter **sudo hping3 127.0.0.1 --listen signature --safe –icmp**. Enter **toor** as password if asked.
3. Create an ICMP packet to send as a file to the listening hping3 window. This could be accomplished across the machines by simply changing the IP addresses. For the purposes of this exercise, a loopback address will be used instead.
4. In the second terminal window, type **sudo hping3 127.0.0.1 --icmp -d 100 --sign signature --file /etc/passwd**. Enter **toor** as password if asked.
5. The file contents begin to appear in the first terminal as shown in the following screenshot:



1. The file has been transmitted successfully. Note that this could be any ASCII file and the process can be used for a number of different actions. This concludes the lab exercise.