**ST. FRANCIS INSTITUTE OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SECURITY LAB**

**Experiment – 9: Simulate DOS attack using Hping and Wireshark.**

**Aim:** To simulate DOS attack using Hping3 and observe with Wireshark.

**Objective:** After performing the experiment, the students will be able to analyze the DOS attack and its effect on the network using Hping3 and Wireshark.

**Lab objective mapped:** L502.6: Students should be able to Apply network security basics, analyze different attacks on networks, and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** Kali Linux OR Unix/Linux, Hping3, Wireshark

**Pre-Experiment Theory:**

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means during the attack period, regular traffic on the website will be either slowed down or completely interrupted.

A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency site instead.

**Implementation:**

1. Install Hping3 and Wireshark on the Ubuntu machine. Alternatively, you can use a kali Linux machine.
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- flood option). Use the following commands in the ‘Terminal’ window,
   1. hping3 –h

Observe all the options hping3 offers. Take a screenshot (SS).

* 1. Simultaneously open Wireshark. Start sniffing the appropriate network. Then use the following command in the ‘Terminal’ window.

sudo hping3 *(suitable IP Address)*

Observe the DoS attack using Wireshark. Take the SS of the terminal and Wireshark window. Terminate hping3 using ‘ctrl c’ and stop sniffing through Wireshark.

Use the following commands one by one and observe the DoS attacks using Wireshark. For each command take SS of the terminal and Wireshark window.

* 1. sudo hping3 *(suitable IP Address)* -1
  2. sudo hping3 *(suitable IP Address)* -1 --fast
  3. sudo hping3 *(suitable IP Address)* -1 --faster
  4. sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com or *(suitable IP Address)*

**Observations & Output:**

1. Attach all the screenshots (SS) in sequence.
2. Under each hoping command SS, explain the command with all the options used with it.
3. Under each Wireshark window, SS write your own observations.

**Post Experimental Exercise:** *(to be handwritten on journal sheets)*

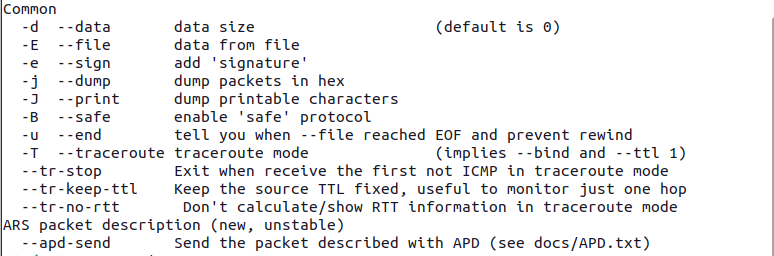
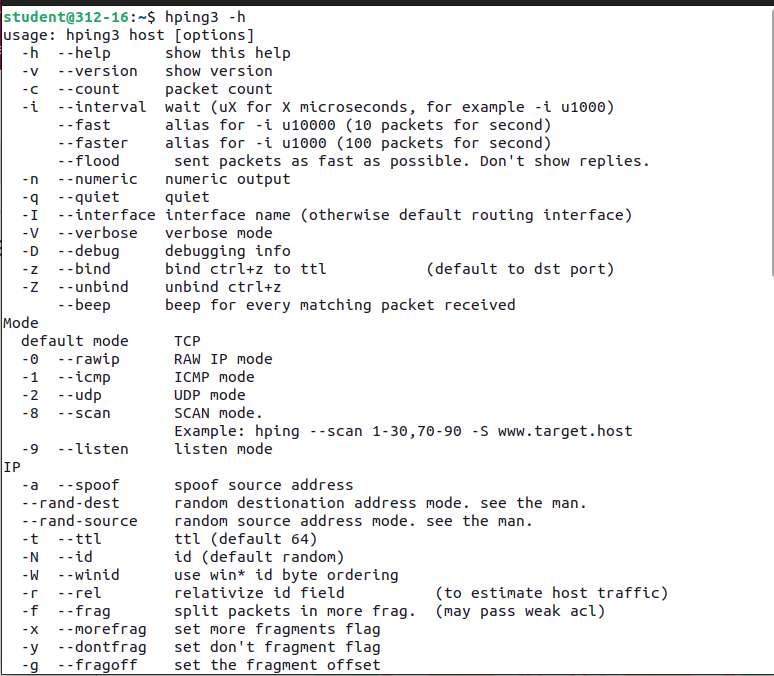
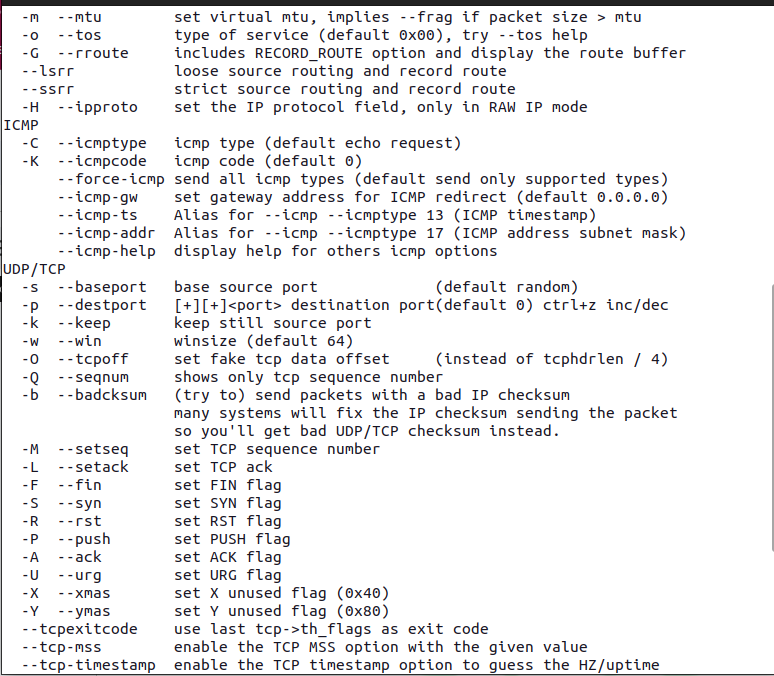
1. Briefly explain the DDOS Attack.
2. Discuss the Buffer overflow attack in detail.

**Conclusion:**

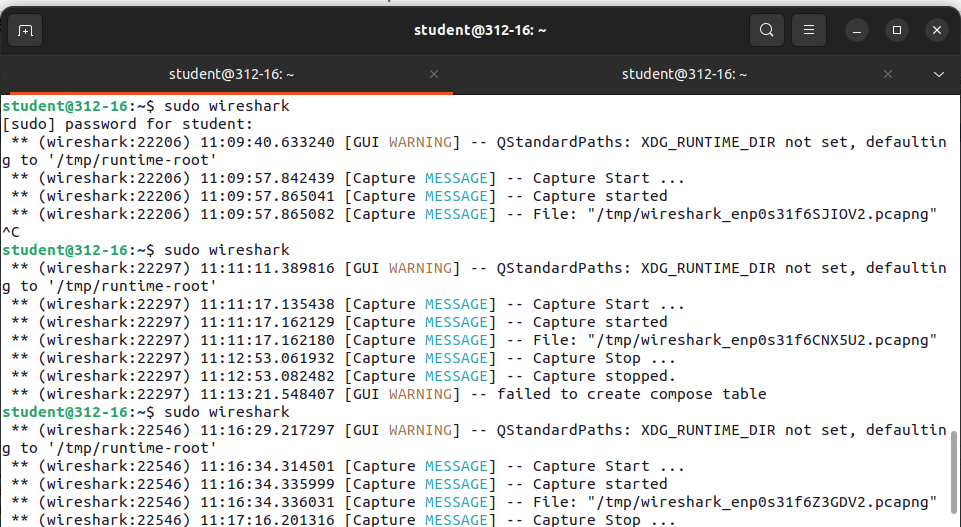
In this experiment DoS attack is simulated using Hping3 and resource exhaustion was monitored using Wireshark. We conclude that DOS is a simple attack technique to deny accessibility to services. It consists of overloading the target with oversized packets, or a big quantity of them. However it does not compromise the information or privacy of the target. It is not a penetrative attack and only aims to prevent access to the target.

**References:**

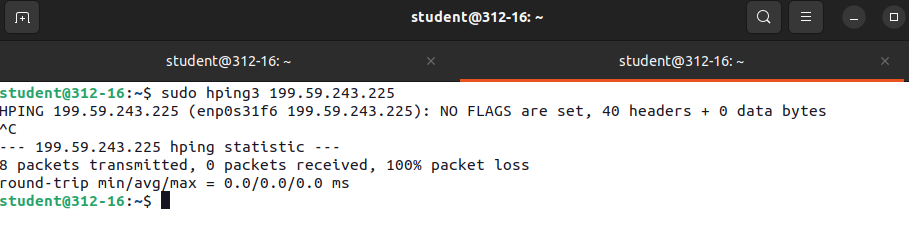
1. “Denial-of-service Attack – DoS using hping3 with spoofed IP in Kali Linux”, <https://www.blackmoreops.com/2015/04/21/denial-of-service-attack-dos-using-hping3-with-spoofed-ip-in-kali-linux/>
2. “Lecture 45: Denial of Service Attack”, <https://youtu.be/2VmQ3Zb4I2I>
3. “DOS Flood With hping3”, <https://linuxhint.com/hping3/>
4. “15+ hping3 command examples in Linux [Cheat Sheet]”, <https://www.golinuxcloud.com/hping3-command-in-linux/>
5. <http://www.vulnweb.com/>
6. [www.hping3testsite.com](http://www.hping3testsite.com)



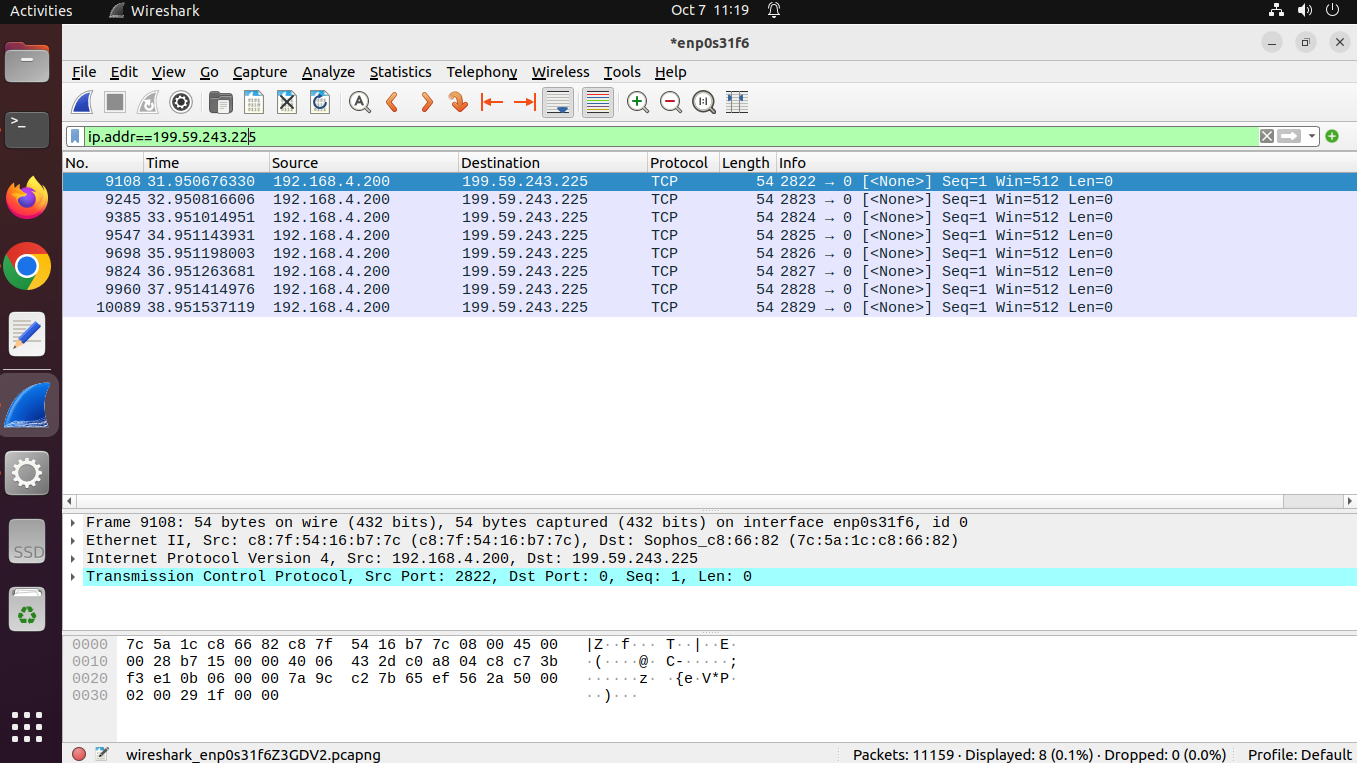
~The snippets are the -h option is the hping3 command which is a help option, displaying the meaning and the use of all the options that can be used for various purposes.

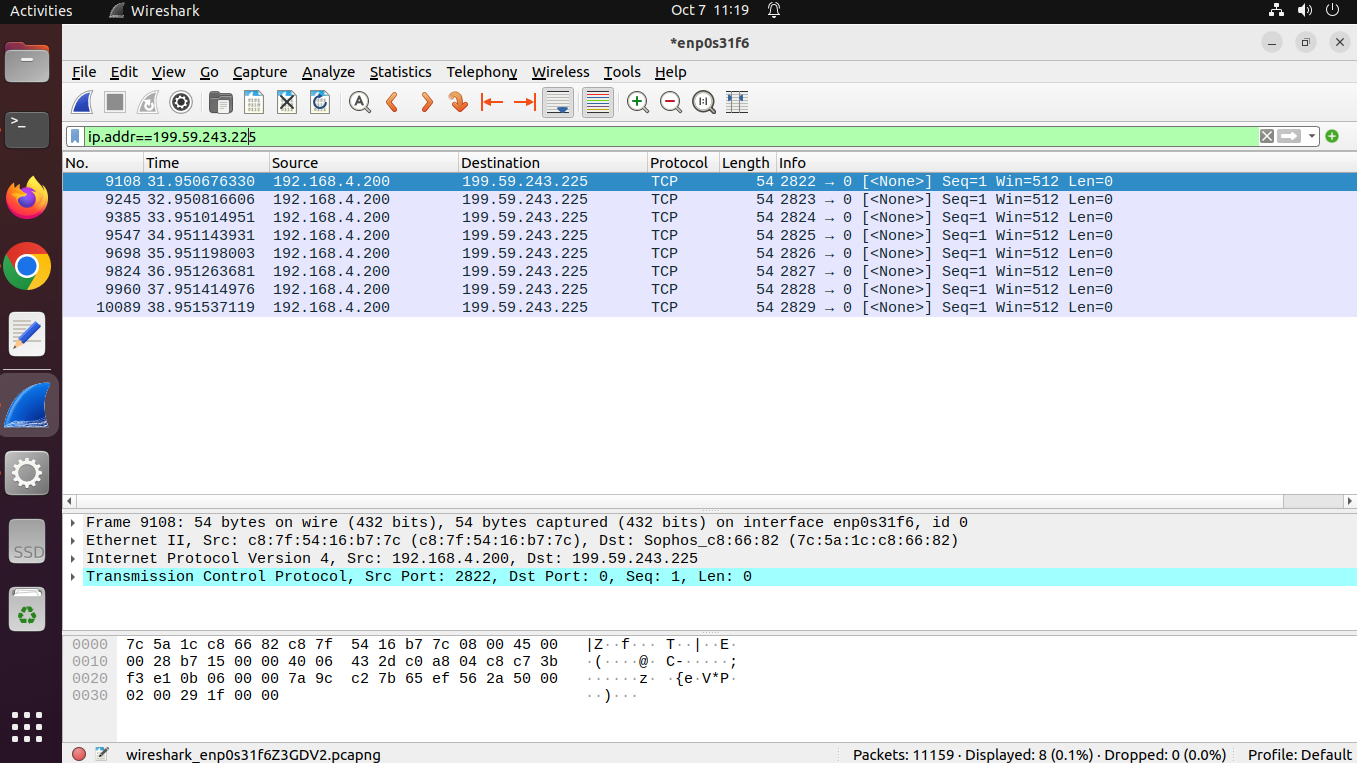


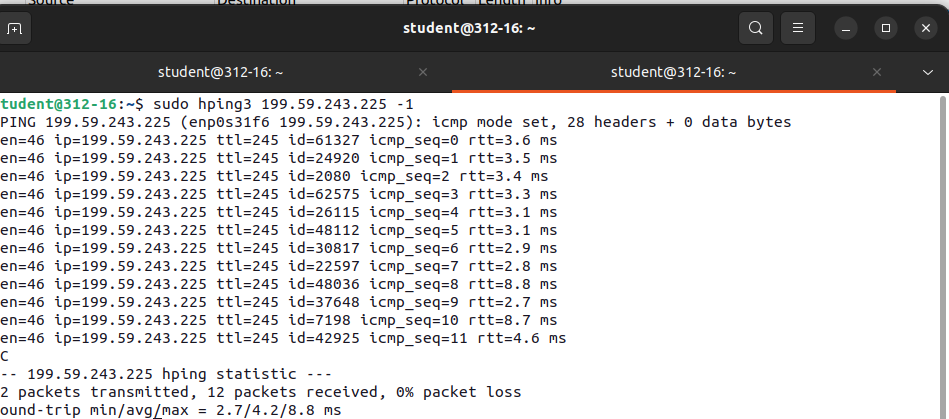
~We have started sniffing in Wireshark by putting the sudo wireshark command from the terminal.



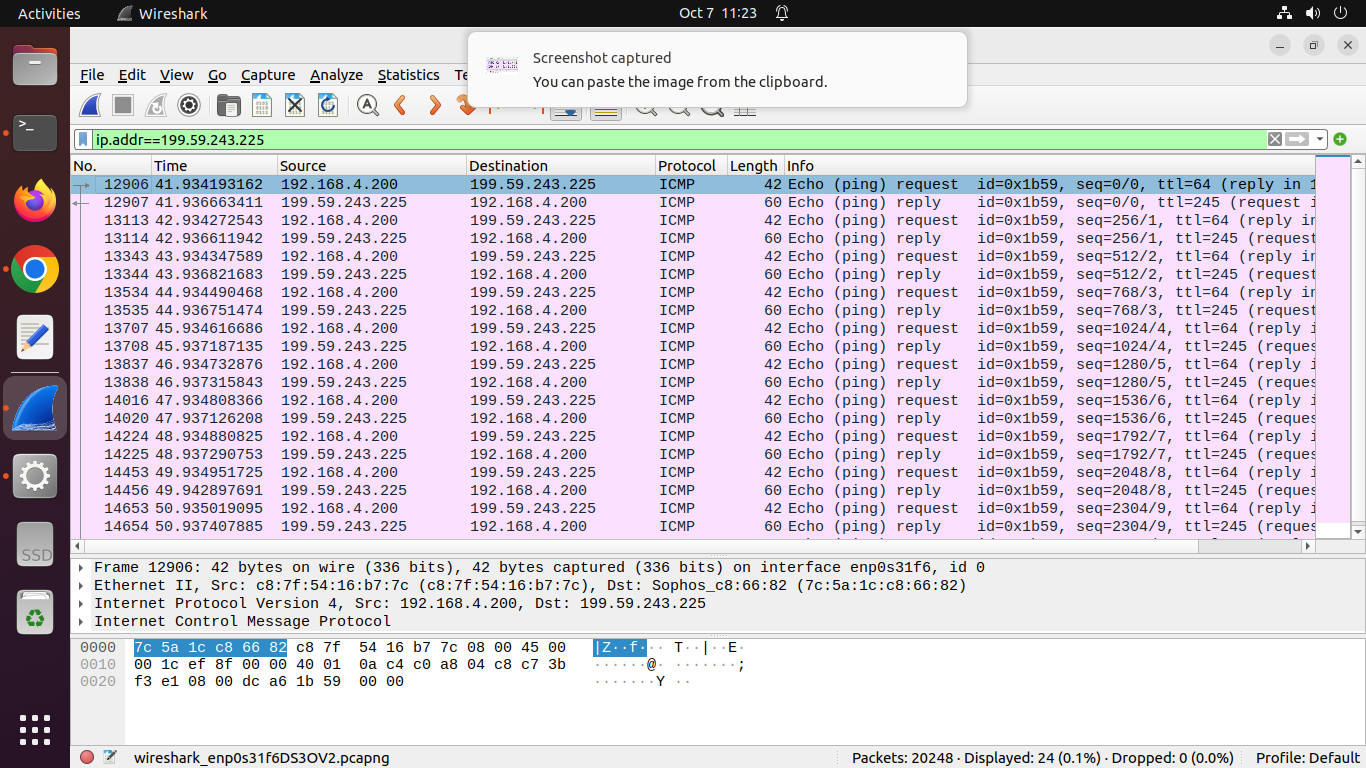
~The above command is used to send packets to IP address 199.59.243.225 through hping3 which is a command-line network tool that can send custom TCP/IP packets. On breaking the running command we observed that 8 packets were sent and 0 packets were received hence there is 100% packet loss, due to trying to flood the receiving IP address.



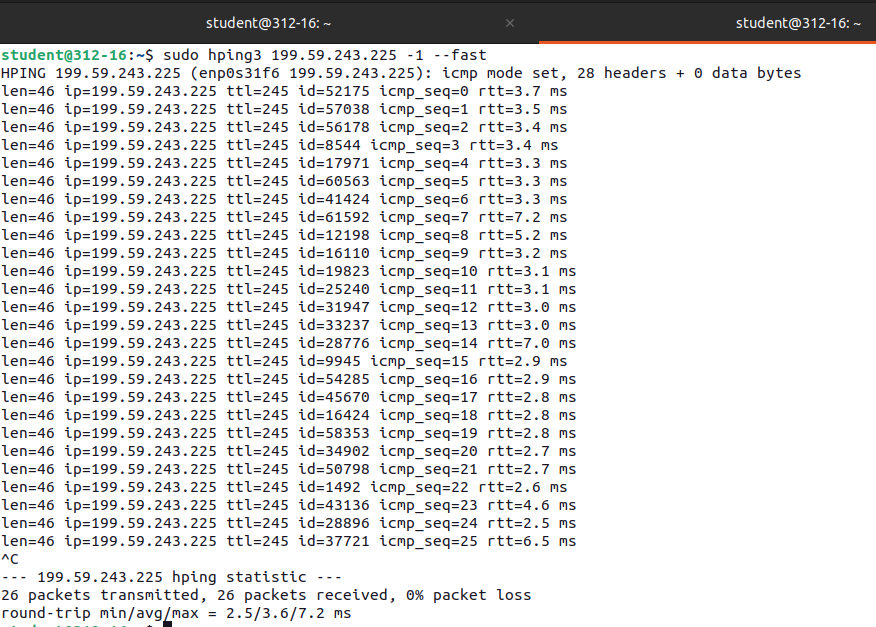
~The 8 TCP packets that were sent by the hping3 command were viewed on pausing the sniffing and searching for IP address 199.59.243.225. The destination, source which is the IP address of my pc, and the protocol used i.e. TCP is seen in the above snippet.



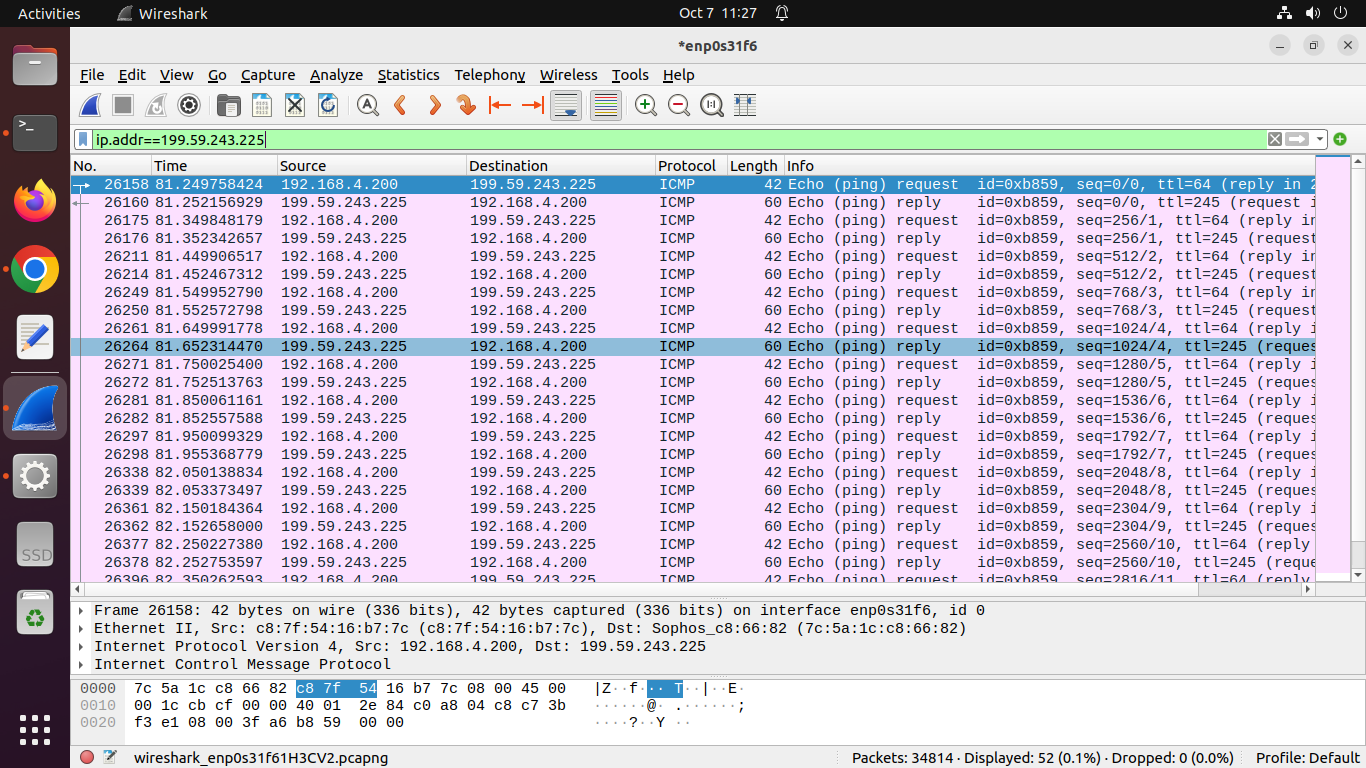
~In the adjacent command, -1 is added in the options section of the command which means sending ICMP protocol-based packets to the receiver to flood. In the above snippet on breaking the command,2 packets were sent and 12 packets were received and thus there is 0% packet loss is seen in the statistics section. The attack is being done on IP address 199.59.243.225.



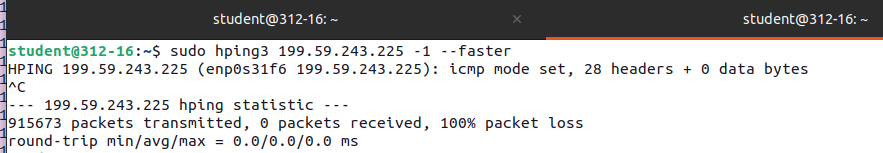
~On pausing the packet capture in the Wireshark, and searching for the DOS attack-related evidence, the IP address 199.59.243.225 has been flooded with ICMP type of protocol-based packets. The snippet shows the request and reply type of packet exchange between IP addresses 192.168.4.200 & 199.59.243.225. The DOS attack specifically includes ICMP type of protocol-based packets as -1 is sent in the command of hping3.



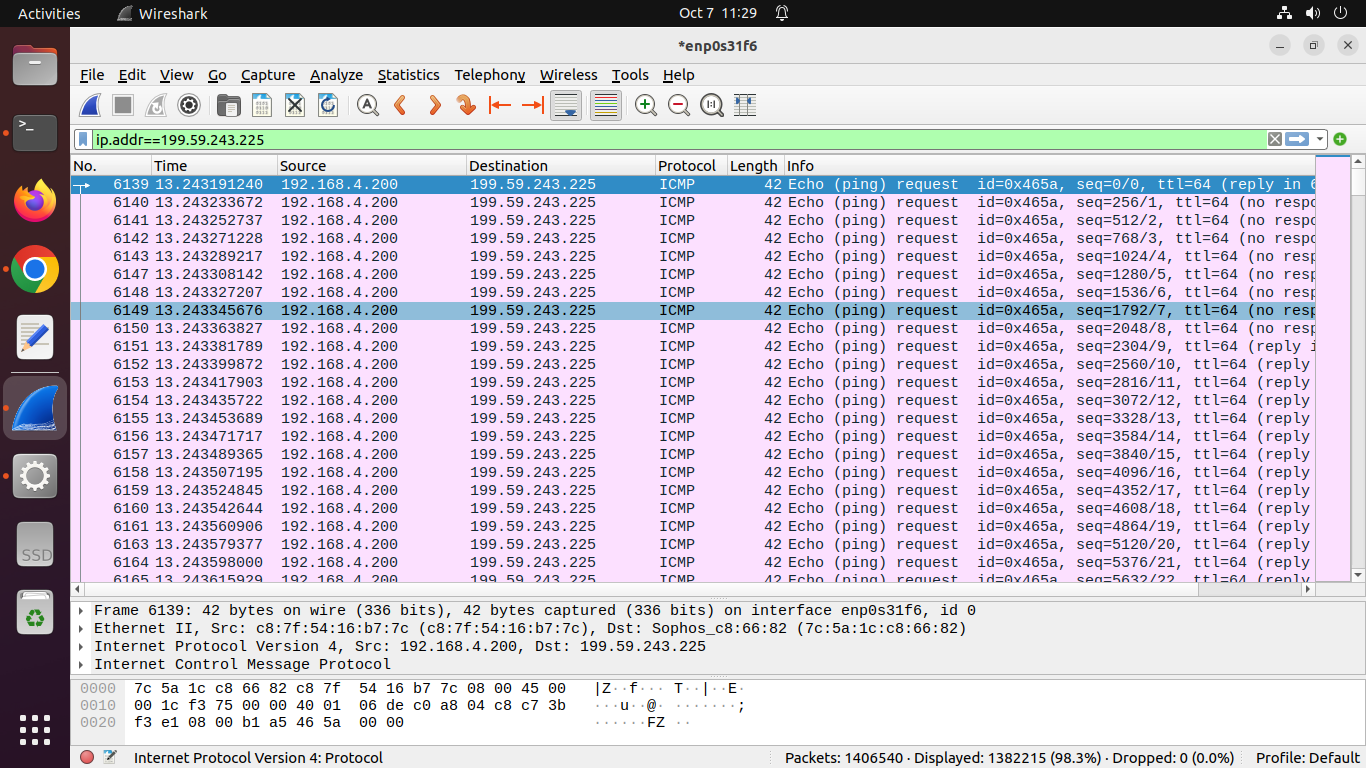
~In this command, -1 is used with - -fast, which the command is telling to flood the IP address 199.59.243.225 with ICMP-type protocol-based packets(as -1 is mentioned) at the rate of 10 packets per second(as - - fast is mentioned).On breaking the command after 2-3 minutes the statistics show 26 packets as transmitted,26 packets as received, and thus 0% of packet loss.



~On pausing the packet capture in the Wireshark, and searching for the DOS attack-related pieces of evidence, The IP address 199.59.243.225 has been flooded with ICMP type of protocol-based packets. The snippet shows the request and reply type of packet exchange between IP addresses 192.168.4.200 & 199.59.243.225. The DOS attack specifically includes ICMP-type protocol-based packets, as -1 is sent in the command of hping3. More packets are seen to be captured in this command than the earlier command as - - fast is used.



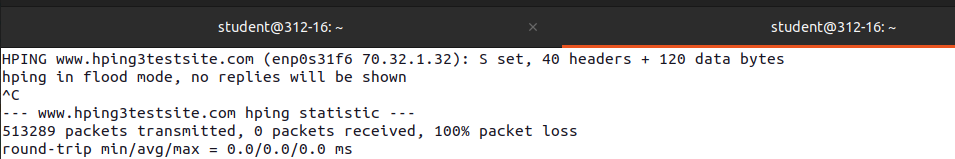
~The command attached here contains -1 which tells the hping3 to flood the IP address 199.59.243.225 with ICMP type of protocol-based packets.The - - faster part of the command tells to flood the network at the rate of 100 packets per second.On breaking the command after 2-3 minutes the statistics is showing that 915673 packets has been transmitted and 0 packets has been received thus making a 100% packet loss.



~On pausing the packet capture in the Wireshark, and searching for the DOS attack-related pieces of evidence, The IP address 199.59.243.225 has been flooded with ICMP type of protocol-based packets. The snippet shows the only request type of packets from IP address 199.59.243.225 saying 100%packet loss which we also saw in the statistics of the command. The DOS attack specifically includes ICMP-type protocol-based packets, as -1 is sent in the command of hping3.More packets are seen to captured in this command than the earlier command as

- - faster is used.

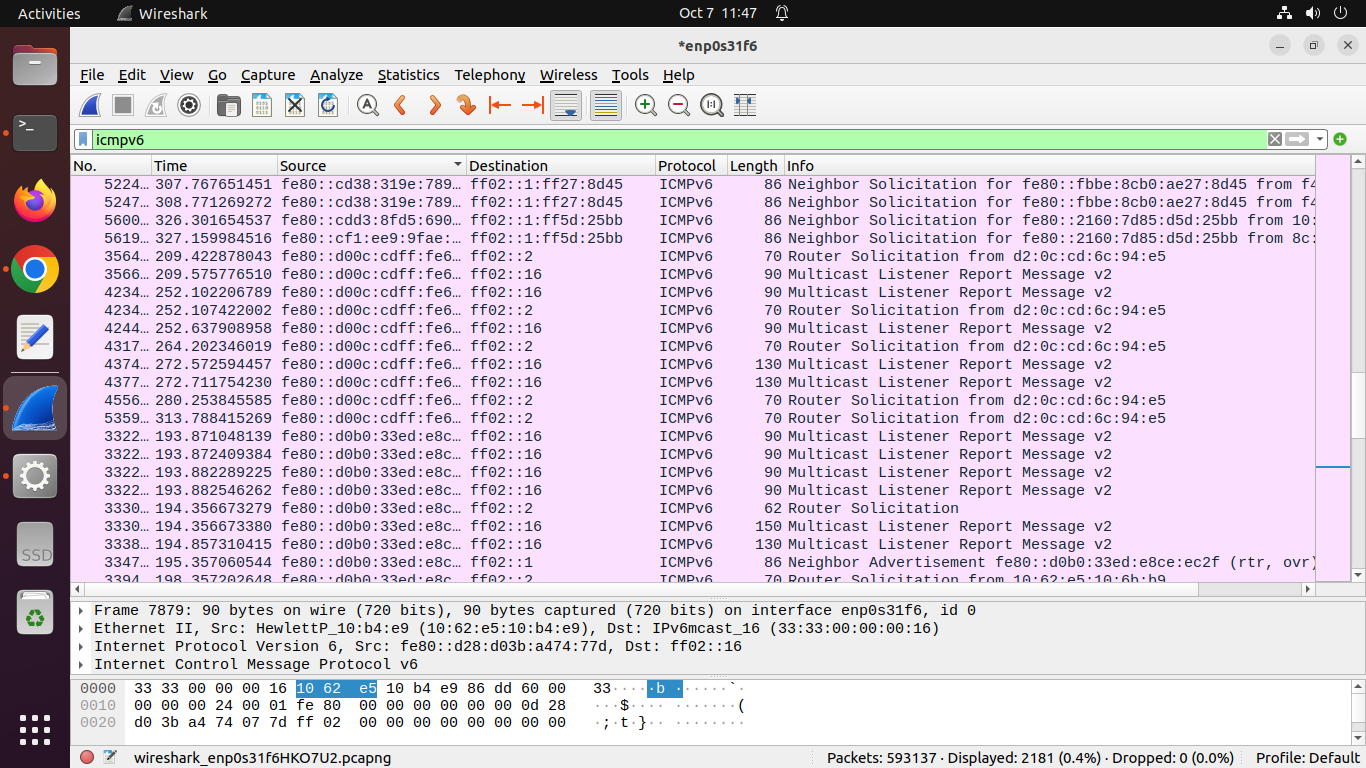
~sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com



The command contains -c 10000 option which tells hping to flood the the site hping3testsite.com with a packet count of 10,000. -d 120 tells the hpinng to maintain the size of packet payload to 120. -s is telling hping3 to perform DOS attack with TCP SYN type of packets. -s 64 is telling the hping3 to maintain the TCP window size to 64. -p 21 is for targeting the port number 21 which is commonly used by FTP servers. - - flood is telling the hping3 to send packets as quickly as possible, without waiting for responses, thereby flooding the target.

- -rand-source is for spoofing the IP address randomly for each packet thereby making it harder for the target system to filter or block the attack based on the source IP. and the very last part of the command is the taget domain for DOS attack ,here in this case it is [www.hping3testsite.com](http://www.hping3testsite.com).

On breaking this command after 2-3 minutes ,the statistics obtained says 513289 packets has been transmitted with 0 packets received thereby resulting in a 100% packet loss.



~On pausing the packet capture in the Wireshark, and searching for the DOS attack-related pieces of evidence, The IP address 199.59.243.225 has been flooded with ICMPv6 type of protocol-based packets. The snippet shows the flood attack on the website [www.hping3testsite.com](http://www.hping3testsite.com) thereby server down at the mentioned website . The DOS attack specifically includes ICMPv6 -type protocol-based packets, as -s is sent in the command of hping3.More packets are seen to captured in this command than the earlier command as - - flood is used.