A Report on
<ICMP Smurf Attack>

1505095 - Jamalia Sultana Jisha
Section: B
Group: 07

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
(BUET)
Dhaka 1000

Contents

1 Smurf attack

According to Wikipedia, the Smurf Attack is "a way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages". In this technique, the attacker forges ICMP echo request packets with the IP address of the victim as the source address and broadcasts the request on the network, making the computers in the network to send replies to the ICMP echo requests. Of course, in multi-access broadcast network, the number of replies could be overwhelming as hundreds of computer may listen to the broadcast.

2 ICMP and ICMP echo

The ICMP "is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached". Typically, the ICMP packets are generated or sent in case the IP datagrams errors or diagnostic and routing purposes, and the echo request is "an ICMP message whose data is expected to be received back in an echo reply ("ping") containing the exact data received in the request message."

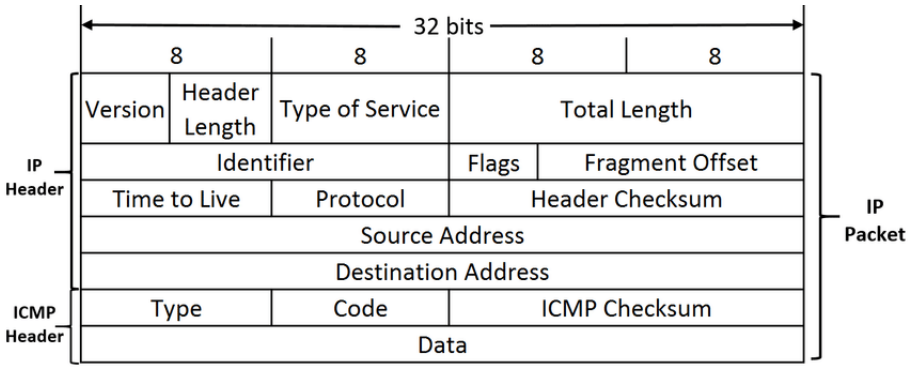


Figure 2: ICMP header

3 Frame details and modifications in header

For ICMP Smurf attack, attacker does not need to modify IP and ICMP header. Attacker only need to set the victim's IP address in the "source address" field of the IP header.

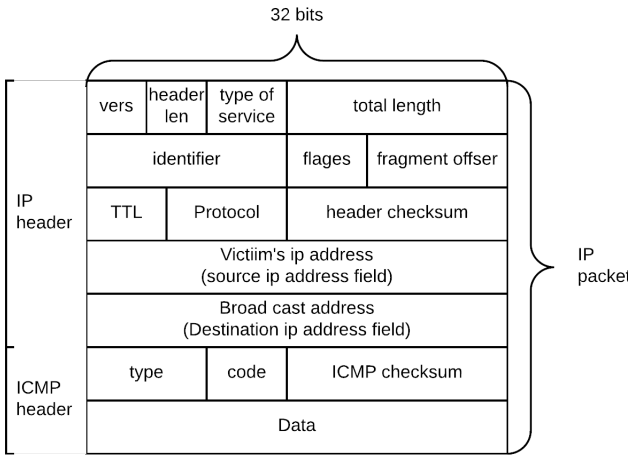


Figure 3: ICMP Smurf attack

4 Steps of ICMP Smurf Attack

- Target IP address is to be identified by the attacker pc (Linux Ubuntu 18.04) through nmap.
- Intermediary site (a broadcast address) is to be identified by attacker which helps in amplifying attack.
- Large amount of traffic/packets (ICMP request) will be sent by attacker to the broadcast address at particular intermediary sites.
- These intermediaries will provide broadcast to all hosts which are there in a subnet(255.255.255.0).
- Hosts will reply to network and will send the ICMP request to the target pc IP address. The target pc IP address will then reply with ICMP reply packets to all the ICMP request packets. Thus, the denial in service attack (ICMP Smurf Attack) is completed.

5 Testing environment

The testing environment consists of:

- 1 64 bit Linux Ubuntu 18.04 machine(HP Pavilion Notebook)
- 1 64 bit Linux Ubuntu 16.04 machine(Oracle VirtualBox virtual NIC)
- 1 32 bit Linux SeedUbuntu (Oracle VirtualBox virtual NIC)
- 1 android(Samsung Electronics)
- the devices in the network are connected using a router for wifi (tp link - 4 ports for ethernet).

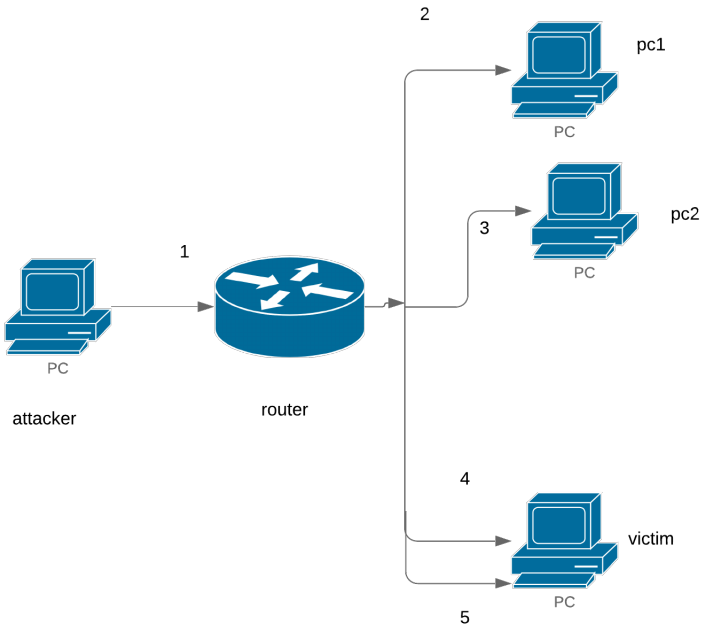


Figure 4: Testing environment topology

6 Images of Devices with their configuration

- Linux Ubuntu 18.04 Hp Pavilion Notebook (attacker) ip address: 192.168.0.175, netmask: 255.255.255.0, broadcast: 192.1680.0.255 and mac address: 10:f0:05:42:51:cb The network map for the environment from the attacker pc :

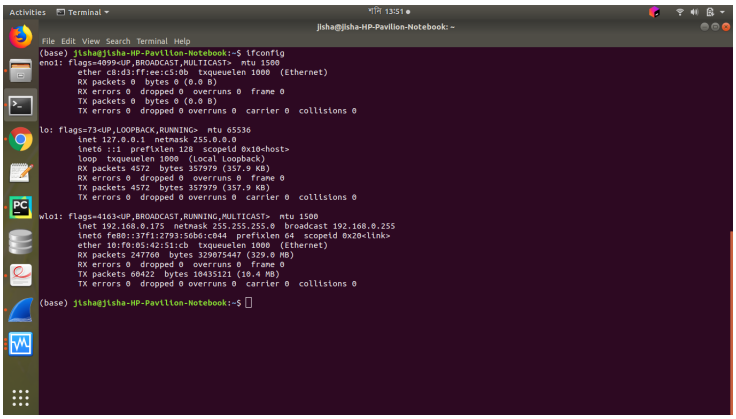


Figure 5: Attacker machine

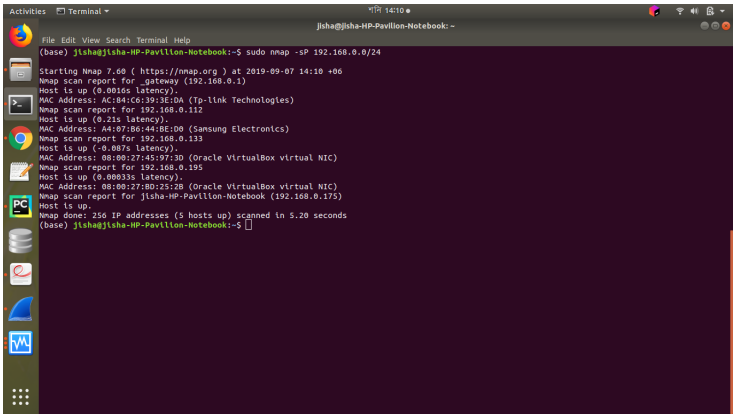


Figure 6: Nmap for Attacker machine

- Linux SeedUbuntu (Oracle VirtualBox virtual NIC) : target device ip address: 192.168.0.133, netmask: 155.255.255.0, broadcast: 192.168.0.255

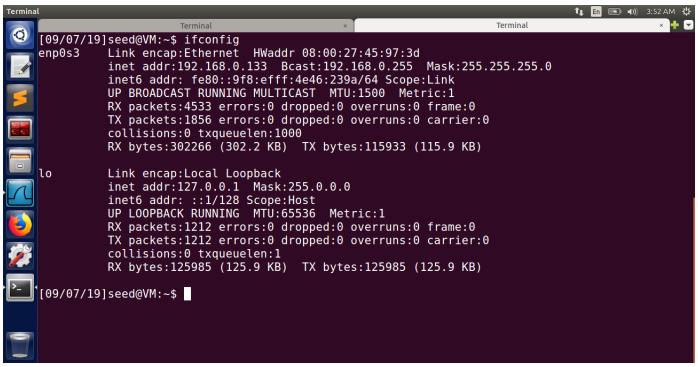


Figure 7: Target machine

- Linux Ubuntu 16.04 (Oracle VirtualBox virtual NIC) : one of intermediate normal pc ip address: 192.168.0.195, netmask: 155.255.255.0, broadcast: 192.168.0.255

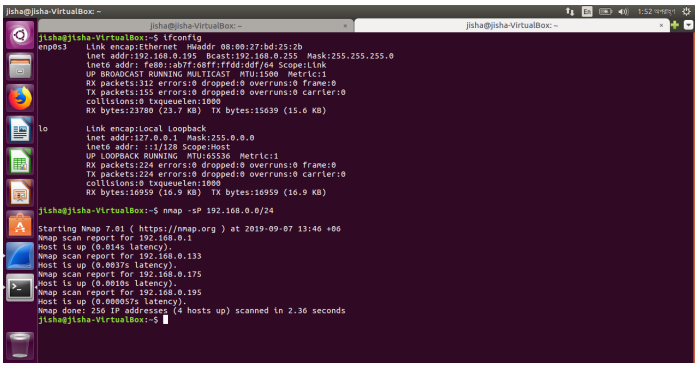


Figure 8: Intermediate normal machine

- Android(Samsung Electronics) : ip address: 192.168.0.112, netmask: 155.255.255.0, broadcast: 192.168.0.255

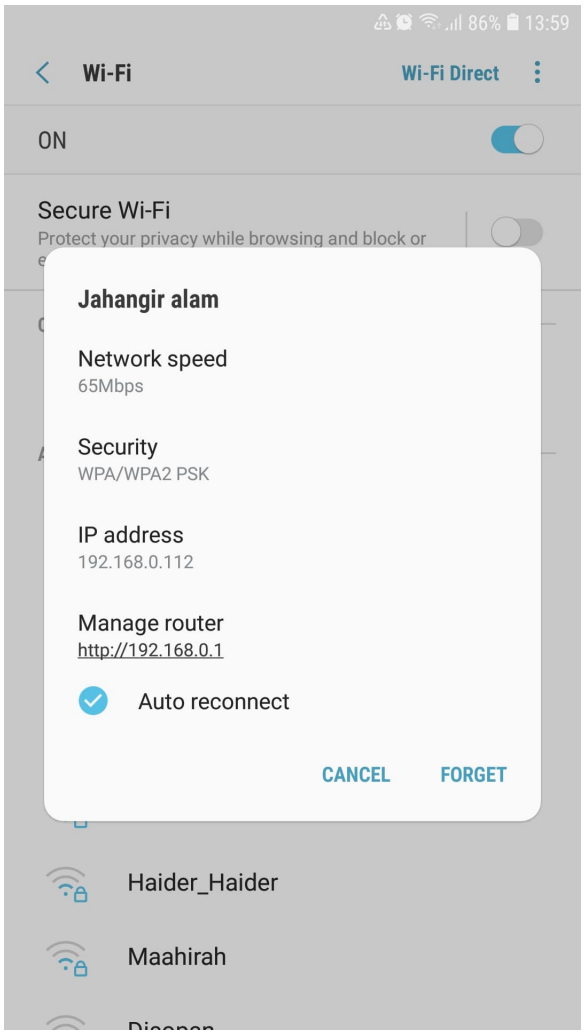


Figure 9: Intermediate normal machine

The network map for the environment from the target machine is same as the attacker machine as the attack is happening under the same network environment.

7 Screensort of code and executive terminal of IDE

For ICMP Smurf Attack, the code is written in python using scapy library. IPheader and ICMPheader have been created in the code. On CreateICMPRequest() function 56 bytes of data has been written to check if wireshark is catching the packets that are sent from attacker or not. Some Screen shots for the code is given below:

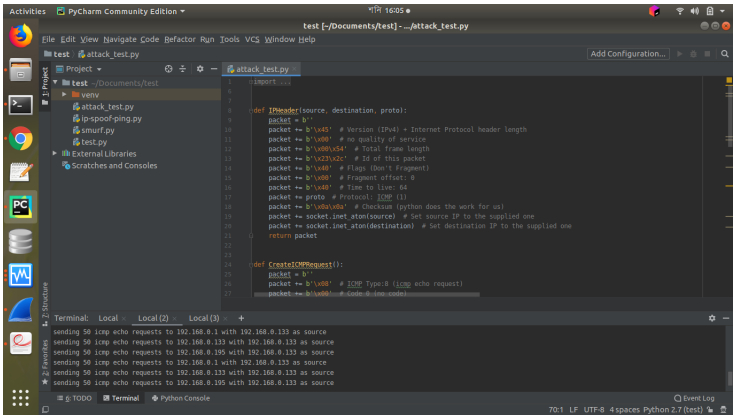


Figure 10: IPheader function

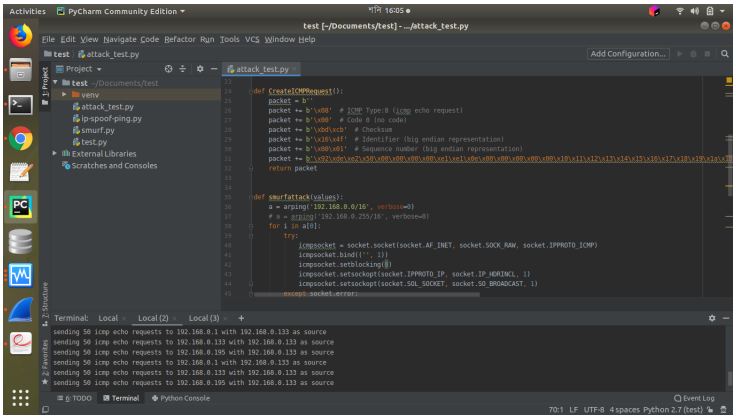


Figure 11: CreateICMPRequest function

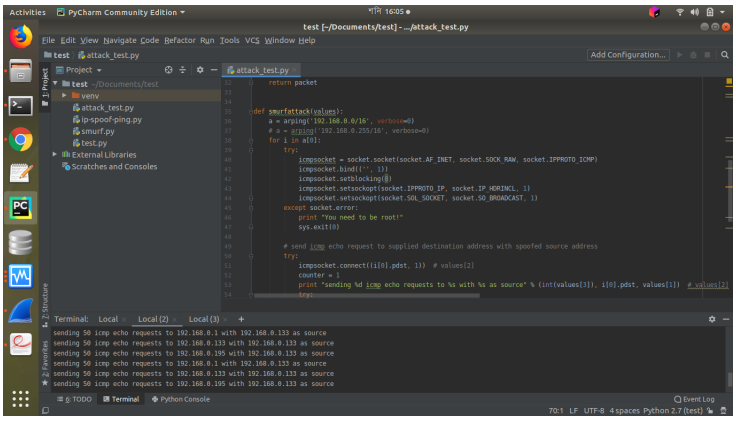


Figure 12: Smurf attack function

After executing the code, we can see ICMP requests are sent from targent pc's ip address as source to the broadcast address as destination. Some Screen shots for the execution terminal is given below:

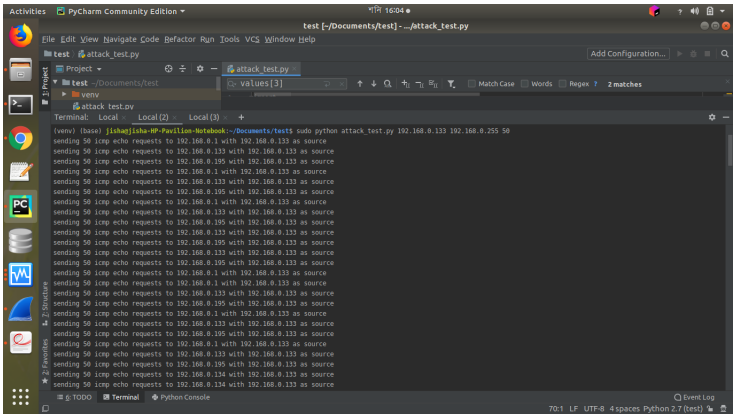
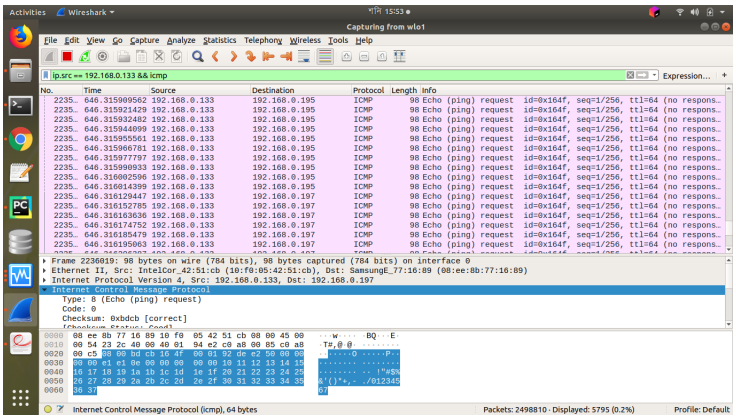
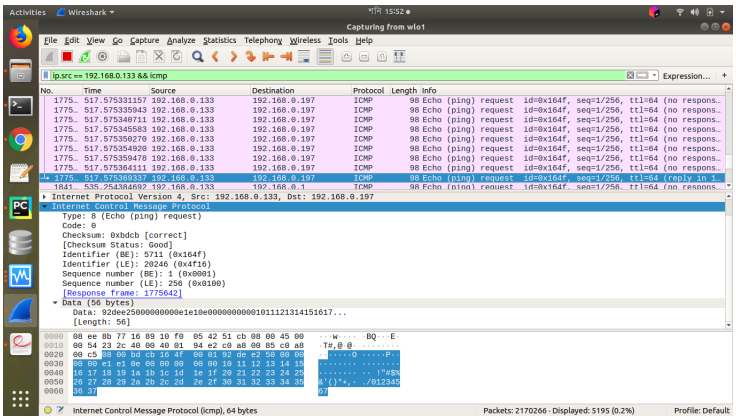


Figure 13: IDE terminal

8 Result of the test

To determine the result and how the packets are traversing, wireshark is runned in attacker, target and intermediate devices.
Wireshark for attacker pc:
For the attacker pc in the wireshark window we can see that the target pc IP adress is sending a lot of ICMP request packets to the boardcast IP address (192.168.0.255). To check if the ICMP requests are the ones we have sent we can check the data byte and its content in the wireshark. We can see that the data content sent as ICMP request matches with the data content in the wireshark below. If we filter the icmp packets according to the target IP address source or destination, we can see a data traffic (packets coming from a lot of IP addresses because of being broadcast) is being created in the network for the target pc.





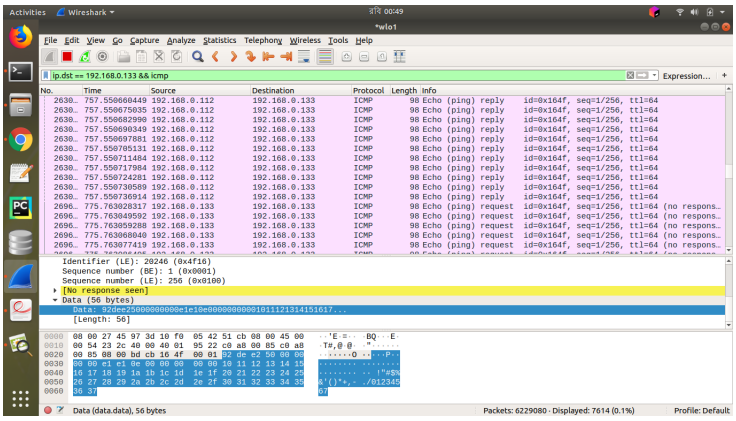
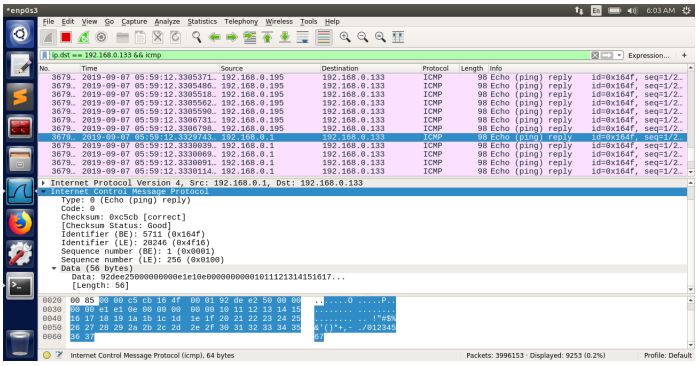


Figure 14: Attacker wireshark window

Wireshark for targeted pc:
For the targeted pc in the wireshark window we can see that a lot of ICMP reply is coming from many different IP addresses of the network creating a traffic for the target pc IP address. ICMP reply data contents 56 bytes of data that matches with the ICMP request we created in the python code.



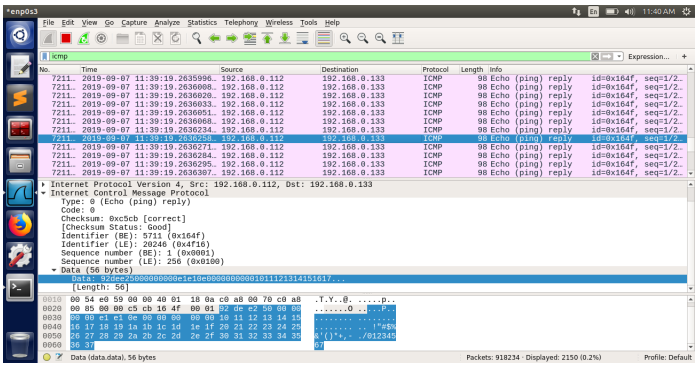


Figure 15: Target wireshark window

Wireshark for Intermediate pc:
For the intermediate normal pc in the wireshark window we can see that the IP address of the pc is getting ICMP request packets from the targeted IP address (192.168.0.133) and in return sending ICMP reply packets to the source IP address (192.168.0.133).

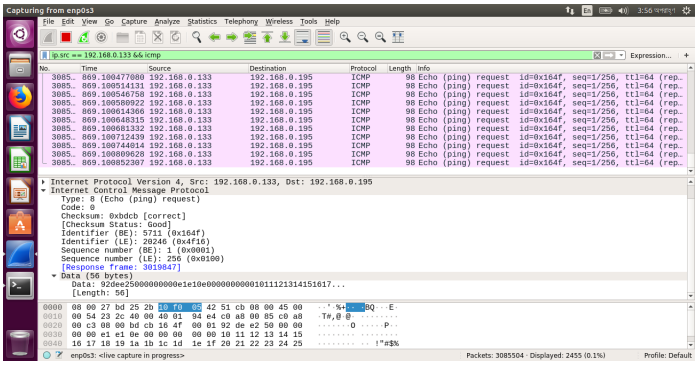


Figure 16: Intermediate pc wireshark window

When the code was running and sending packets in the network, a ping packet had been sent from a normal pc to the targeted pc to see the availability of the target pc. For testing, ping request was two times with the time difference being three minutes.

- for the first test of sending ping request, 24 request packets were sent and got 21 reply packets with the total loss of 12%. For the test, total time took 23433 ms.
- for the second test of sending ping request, 58 request packets were sent and got 55 reply packets with the total loss of 5%. For the test, total time took 58133 ms.

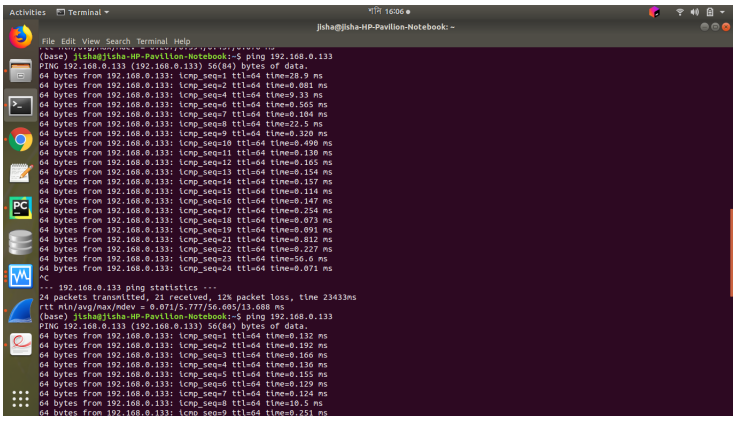


Figure 17: First ping test

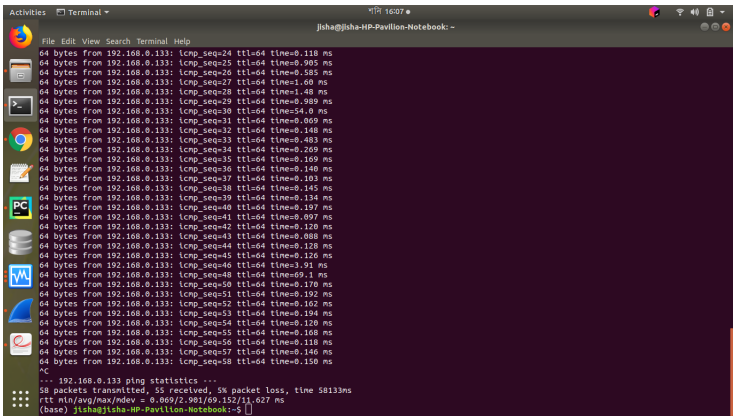


Figure 18: Second ping test

9 Prevention of ICMP Smurf Attack

According to Wikipedia, the prevention of Smurf attacks is two-folds:

- Configure individual hosts and routers not to respond to ping requests or broadcasts.
- Configure routers not to forward packets directed to broadcast addresses. Until 1999, standards required routers to forward such packets by default, but in that year, the standard was changed to require the default to be not to forward.

In addition to these two simple solutions, Craig A. Huegen's article on prevention of Smurf attack is highly revered. Also during the course of the experiment, it was found that broadcasted ICMP Echo request is discarded by default

in all the Windows(7, 10), Linux(Ubuntu 16.04, Ubuntu 18.04, SeedUbuntu) and Cisco machines. The feature to reply to such broadcasts can be enabled in Linux machines but however Microsoft doesn't allow enabling this feature on their operating systems. This can be seen as a security benefit because this keeps the Windows machines from participating in a Smurf Attack by sending ICMP Echo responses; however it still doesn't keep them or any network that allows inbound ICMP packets safe from being attacked.

10 Conclusion

The test for the ICMP Smurf Attack can be considered successful in a sense that after sending a lot of ICMP request with the source id address of the target pc ip address, the target pc denied the ping request service (in the ping test) from a normal pc. We can also see from the target device's wireshark the huge amount of ICMP request and reply packets going to and from the target pc. Though the rate of service (ping request) denial is small, with proper size of network (as in the real world) the rate of service denial for this attack will be big. The advantages of modern devices that all most all the devices are configured to ignore broadcast to prevent from happening this kind of attack.