CYBR371

LAB 3

Olivia Fletcher
300534281
fletcholiv

Denial of Service Attacks

Question A1 [0.5 marks]

What are the meaning of -s and -c parameters and what are the differences between two of the two commands?

- ‘-s’ stdin reads commands from standard input
- In this lab it use it to -s to set the SYN tcp flag on

- ‘-c’ reads commands from the command_string instead of from the standard input
- In the lab using the -c command directly giving the number of packets we attempt to ping with e.g ping <ubuntu ip> -c 10 (ping 10 packets to the ubuntu terminal)

Question A2 [0.5 marks]

Why aren’t new operating systems susceptible of Ping of Death attack? (250 words)

- In a Ping of Death attack, another subset of DDoS attack, the attacker sends large-scale packets to the victims system than the maximum packet size the connection can handle thus directly causing the device to significantly slow down or crash.
- The Ping of Death attack originally surfaced in the 1950’s and (most) devices since 1998 have been generally protected against it except for a recent attack emerging in 2013 (& 2020) where there was an exploit found on Windows XP and Windows server 2013. Many websites have tools in place to stop this type of attack by blocking ICMP ping messages.
- Since these cases adjustments have been made to the OS and server softwares such as;
    - Use of a larger memory buffer to avoid buffer overflow.
    - The router and firewall level have tools in place that filter malicious packets out of the network;
    - As the packets from PoD attacks are sent in fragments the system on the router/firewall level scans the fragments to check that the fragments do not exceed the maximum size for received packets (65 bytes).
    - The IP header of each IP fragment is checked that the requirements are met as such; “Fragment Offset + Total length <= 65.535 Bytes” otherwise the packet is rejected.

- New Operating systems are good are detecting if the packets are larger than the system can handle using the above method but there are still ways this attack can happen on modern OS’s and here are a few extra ways we can protect ourselves:
    - Ensuring system and applications are all up to date
    - Block all segmented pings from accessing your network/system
    - Allow access for large data bits **after** packets received to avoid crashing
    - Use an overflow buffer to allow for larger memory packets to be received

Question A3 [0.5 marks]

How can you make the Ping of Death packets effective against a target (these days)? (250 words)

- To this day the Ping of Death attack is still a cause of concern as some legacy devices (outdated systems or devices such as medical devices or workplace systems) are vulnerable due to being outdated and use unsupported interfaces that are continuing to be relied on for use. These devices that have yet to be patched can cause significant damage to a network if attacked
- A more recent flaw in 2020 has been noted in the Windows component TCPIP.sys which is a kernel driver which could reach the core of any Windows OS if exploited
- A more recent development of the Ping of Death attack is using an ICMP (Internet Control Message Protocol) flood attack. All computers use an ICMP echo-reply message system (ping). Ping commands are limited to a maximum size of 65,535 bytes, an attacker manipulates this system and does an ICMP flood attack by;
    - Attacker sends out pings from source machine to a victim's target system and waits for an ICMP echo reply
    - Once a connection between the source and target is intact the attacker then overloads the connection with packets
- Most computers are safe against basic PoD and ICMP flood attacks but there is still risk for those who rely on outdated devices

Question B1 [0.5 marks]

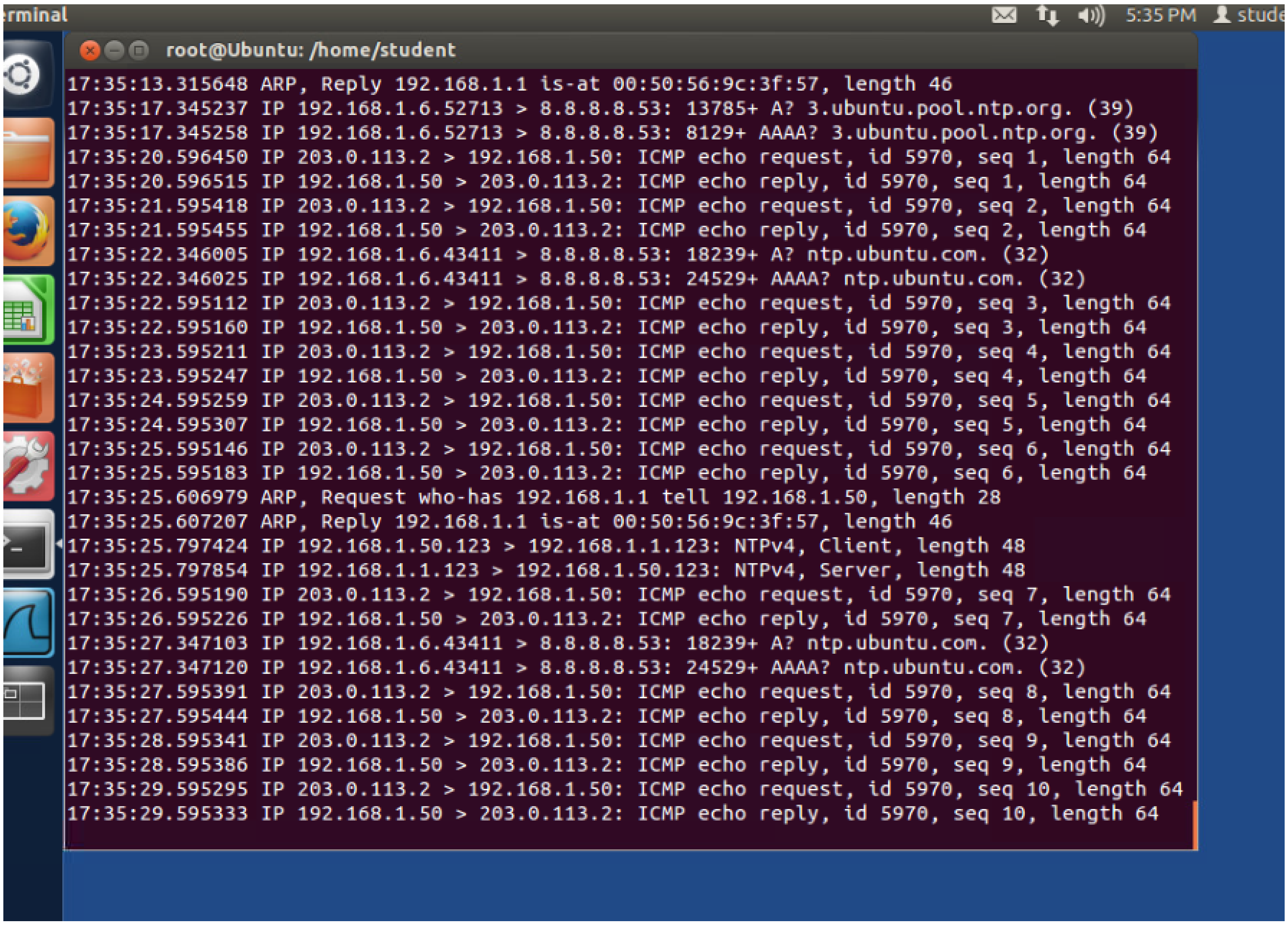
Briefly explain the countermeasures to stop and defend against a smurf attack? (250 words)

- A smurf attack, being an attack which exploits IP and ICMP vulnerabilities, renders the target's network inoperable. Prevention has to be done on two different levels, one being that your network itself must avoid being attacked and also your network must avoid being used to launch an attack due to the intermediary of the attack being that the source-spoofed IP packet has left a given network.
- To avoid being used to launch an attack you;
    - Should disable IP-directed broadcasting on the router
    - Can also apply an outbound filter to the perimeter router
    - Configure hosts and routers to not respond to ICMP echo requests
- Countermeasures anyone can do to stop and defend themselves against a smurf attack;
    - Have networking tools in place to sniff out any odd packet data like volume, size and signatures
    - Use an active up-to-date antivirus, antimalware and configured network firewalls
    - Expand on bandwidth usage to avoid traffic spikes
    - Spread your servers across multiple data centers and use a good system to balance the traffic distribution between centers
    - Using a cloud-based DNS provider where it is designed with DDoS in mind

Question B2 [0.5 marks]

How much did the smurf attack slow down the network? Compare the average ping response time before and during the smurf.

- Before attack;
- Ubuntu system picks up the ping requests from Kali, network traffic speeds of incoming/outgoing is of usual speeds



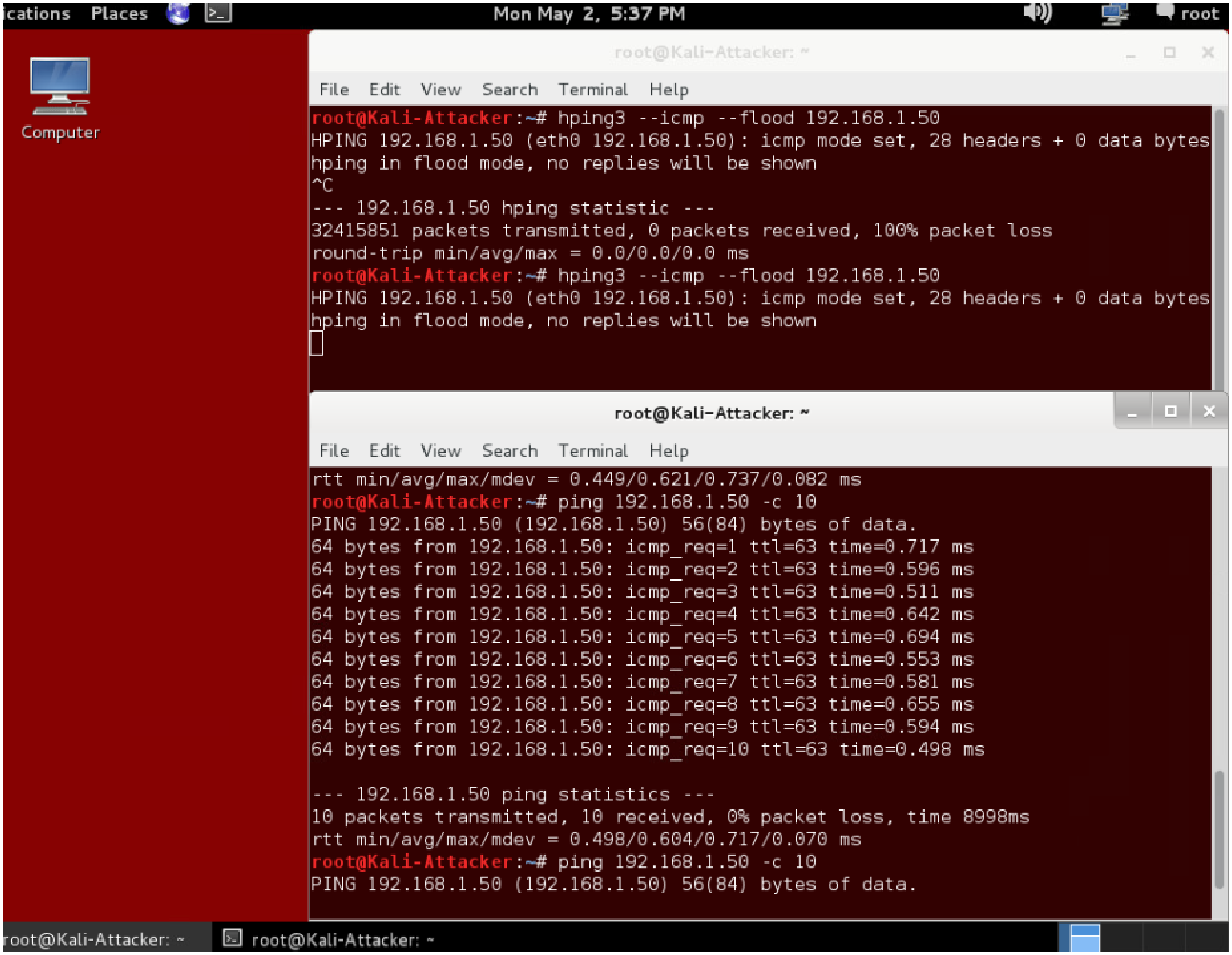
- Takes only 0.717ms for a successful ping from the Kali system to the Ubuntu system

root@Kali-Attacker: ~

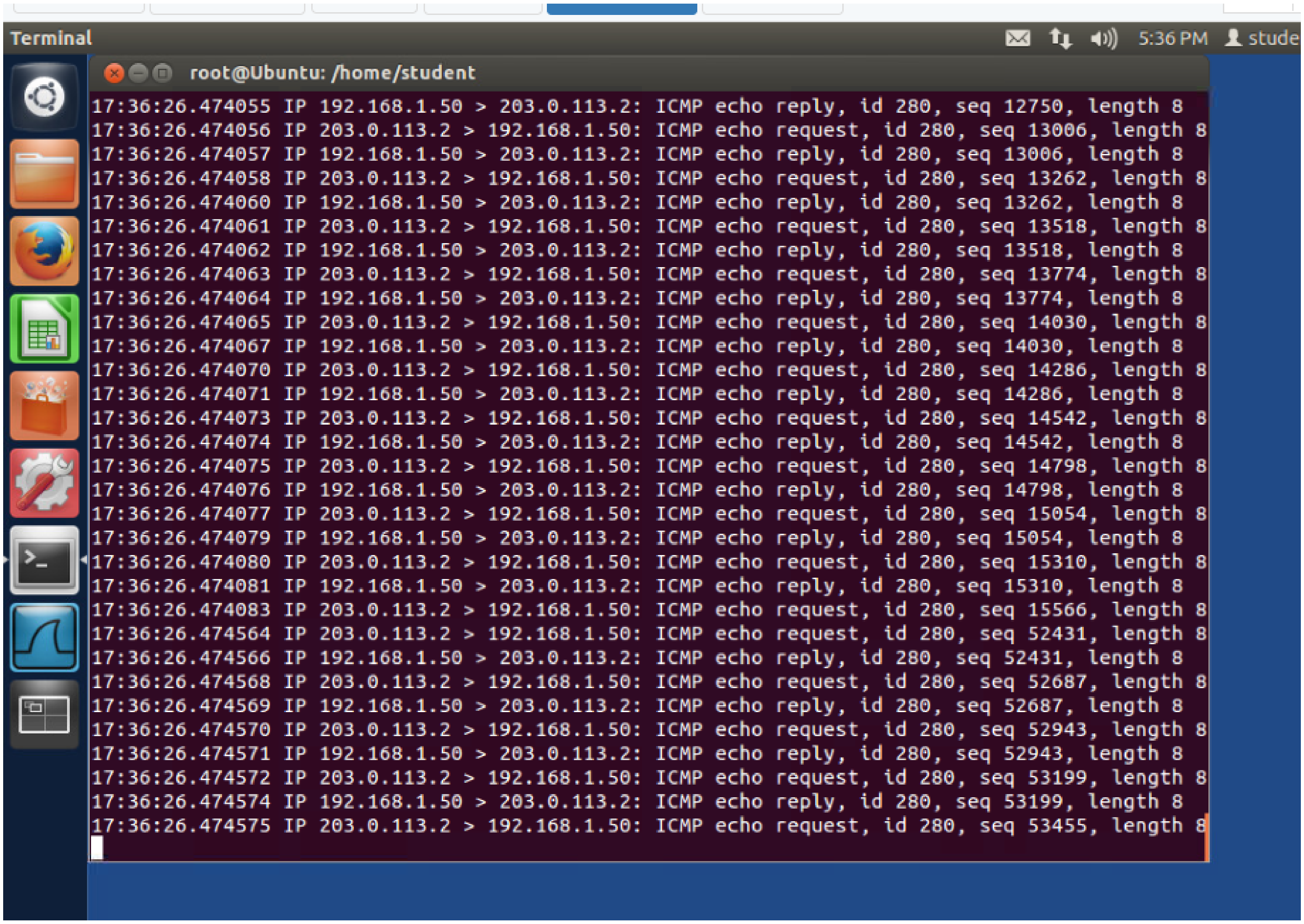
File Edit View Search Terminal Help

```
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_req=1 ttl=63 time=0.737 ms
64 bytes from 192.168.1.50: icmp_req=2 ttl=63 time=0.563 ms
64 bytes from 192.168.1.50: icmp_req=3 ttl=63 time=0.659 ms
64 bytes from 192.168.1.50: icmp_req=4 ttl=63 time=0.700 ms
64 bytes from 192.168.1.50: icmp_req=5 ttl=63 time=0.606 ms
64 bytes from 192.168.1.50: icmp_req=6 ttl=63 time=0.672 ms
64 bytes from 192.168.1.50: icmp_req=7 ttl=63 time=0.648 ms
64 bytes from 192.168.1.50: icmp_req=8 ttl=63 time=0.609 ms
64 bytes from 192.168.1.50: icmp_req=9 ttl=63 time=0.449 ms
64 bytes from 192.168.1.50: icmp_req=10 ttl=63 time=0.573 ms

--- 192.168.1.50 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8998ms
rtt min/avg/max/mdev = 0.449/0.621/0.737/0.082 ms
root@Kali-Attacker:~# ping 192.168.1.50 -c 10
PING 192.168.1.50 (192.168.1.50) 56(84) bytes of data.
64 bytes from 192.168.1.50: icmp_req=1 ttl=63 time=0.717 ms
64 bytes from 192.168.1.50: icmp_req=2 ttl=63 time=0.596 ms
64 bytes from 192.168.1.50: icmp_req=3 ttl=63 time=0.511 ms
64 bytes from 192.168.1.50: icmp_req=4 ttl=63 time=0.642 ms
64 bytes from 192.168.1.50: icmp_req=5 ttl=63 time=0.694 ms
64 bytes from 192.168.1.50: icmp_req=6 ttl=63 time=0.553 ms
64 bytes from 192.168.1.50: icmp_req=7 ttl=63 time=0.581 ms
64 bytes from 192.168.1.50: icmp_req=8 ttl=63 time=0.655 ms
64 bytes from 192.168.1.50: icmp_req=9 ttl=63 time=0.594 ms
64 bytes from 192.168.1.50: icmp_req=10 ttl=63 time=0.498 ms

--- 192.168.1.50 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8998ms
rtt min/avg/max/mdev = 0.498/0.604/0.717/0.070 ms
root@Kali-Attacker:~#
```

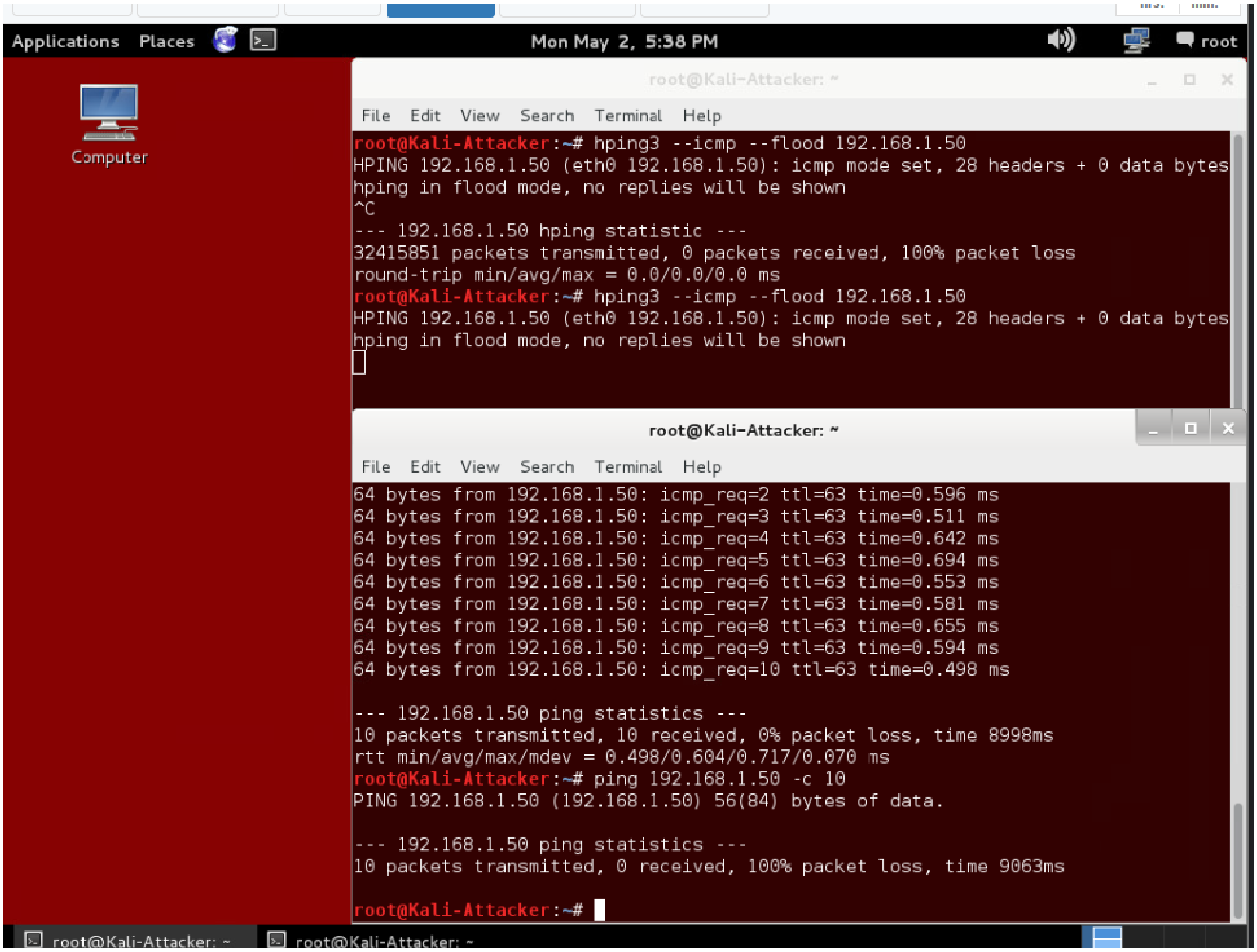
- During attack;
- Kali (in a separate terminal) attempts to ping the Ubuntu system but is taking significantly longer than the previous requests before launching the attack.



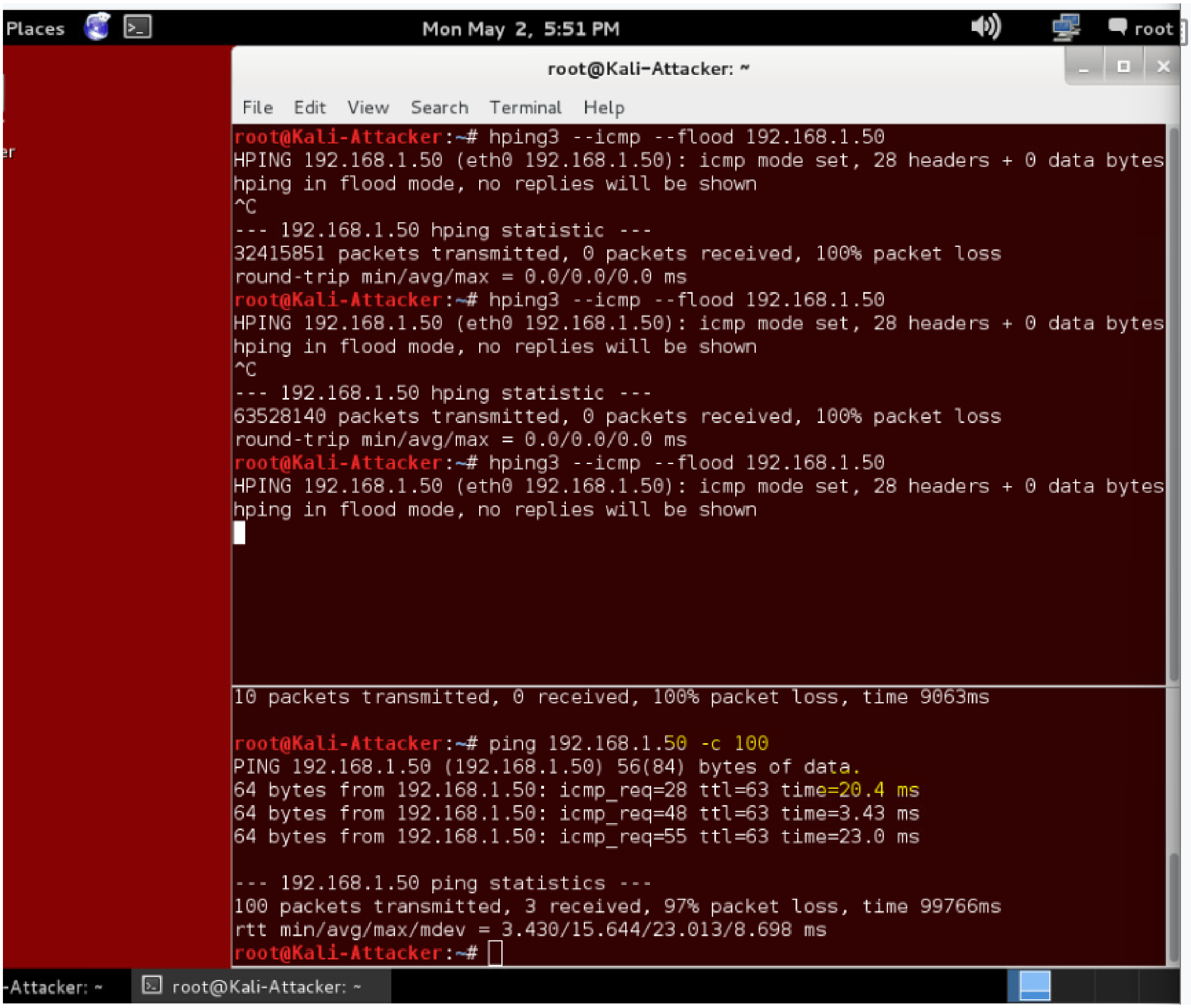
- The Ubuntu terminal had traffic coming in an a significant rate compared to before the attack



- After attack;
- Failed to ping Ubuntu system as the attack rendered the network unable to be pinged
- 100% packet loss, reached the packet limit (10 in this case)



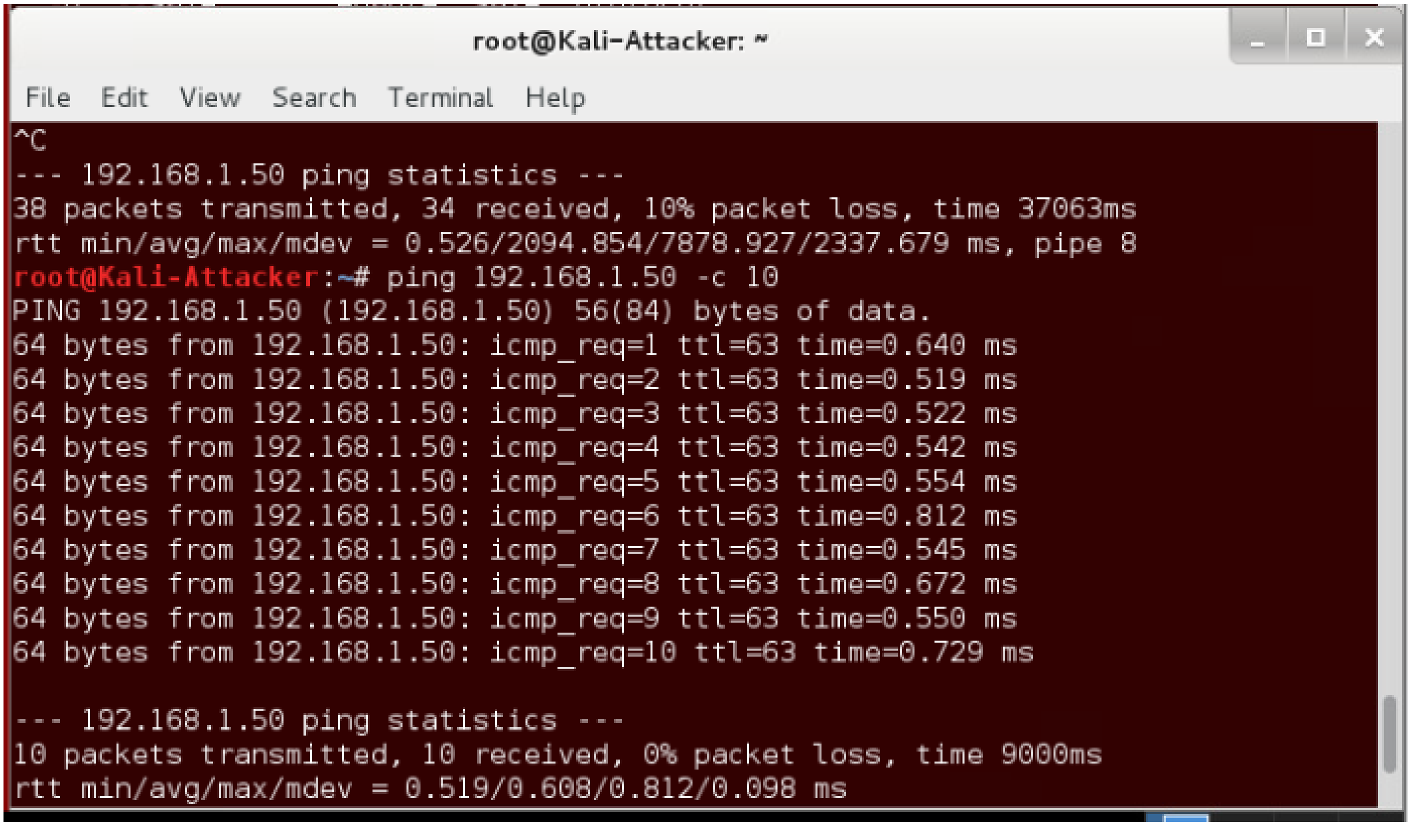
- Another test;
- Did this again but using - 100 packets
- First ping request goes through at 20.4ms which is significantly longer time than the 0.717 it took to ping the ubuntu system before Kali attacking



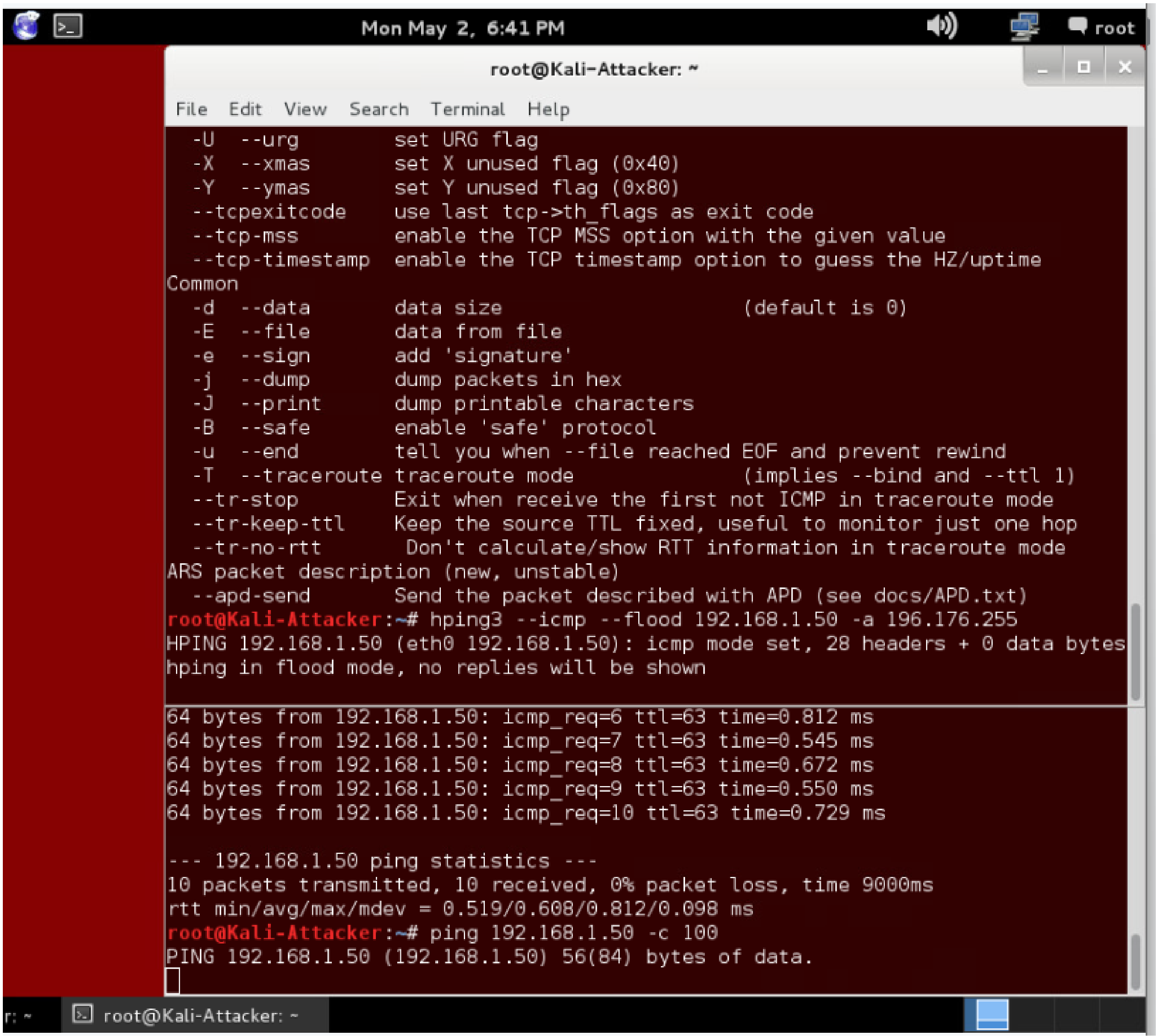
Question B3 [0.5 marks]

Write an hping3 command to launch a smurf attack against the Ubuntu machine and randomly spoof the source IP addresses

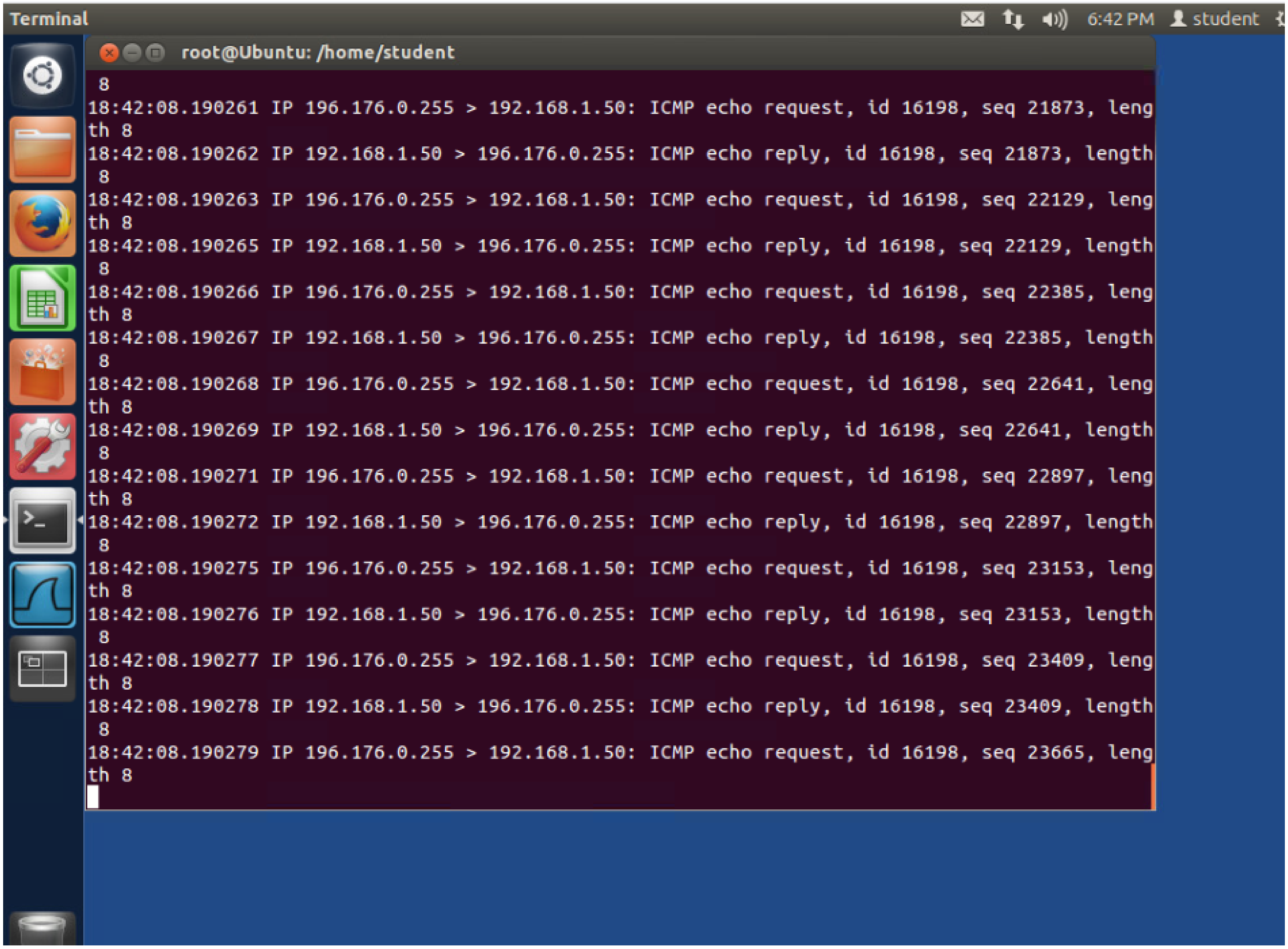
- Before the attack we get the following ping times;



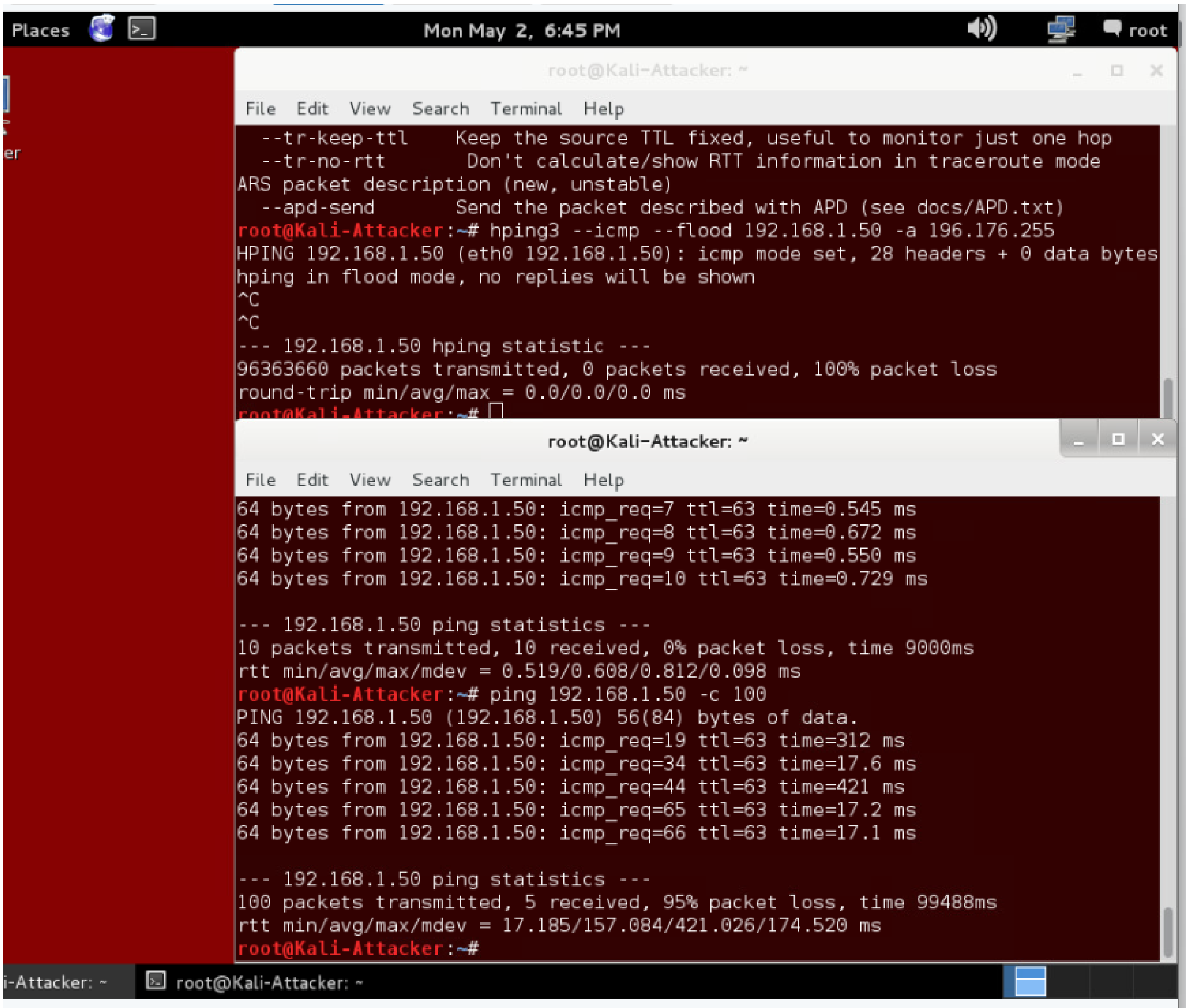
- To launch the attack I used the following command;
- hping3 –icmp –flood 192.168.1.50 -a 196.168.176.255
- The -a flag in this command line allows for spoofing the IP



- Below is the ubuntu terminal during the attack using the 196.168.176.255 spoofed IP



- Below is showing the attempted pings during the Kali attack and the times being significantly higher than before the attack
- Before attack first ping: 0.640ms
- During attack first ping: 312ms



Question C1 [1 marks]

Briefly explain the countermeasures to stop and defend against a SYN-flood attack? (250 words)

- Three processes (three way handshake) must take place for a TCP protocol to be successful between a client and server connection, this processors are initiated when the client sends a SYN message to the server, the server then receives the message and responds with a SYN-ACK message back to the client, then the client confirms the connection with the ACK message. The SYN flood happens when the three-way process (handshake) above is manipulated so the attacker can then rapidly initiate a connection to the server without confirming the connection (last process of the handshake) with the ACK. The server then expends an excess of resources waiting for the opened connections thus resulting in the system becoming unresponsive to, other, legitimate traffic.
- Countermeasures in place to avoid a SYN-flood attack are;
  - Ensure firewall softwares, OS, and antiviruses are up to date
  - Installing an IPS to sniff out unusual packet data like traffic patterns, volume, size and signatures
  - Configure the firewall for SYN flood protection and SYN attack thresholds
  - Use tools that allow for easier access to view all network traffic to ensure simpler constant analysis across the entire network
  - Similar to smurf attack, expand on bandwidth usage to avoid traffic spikes and manage larger scale attacks