CSCI-2201
Lab 2

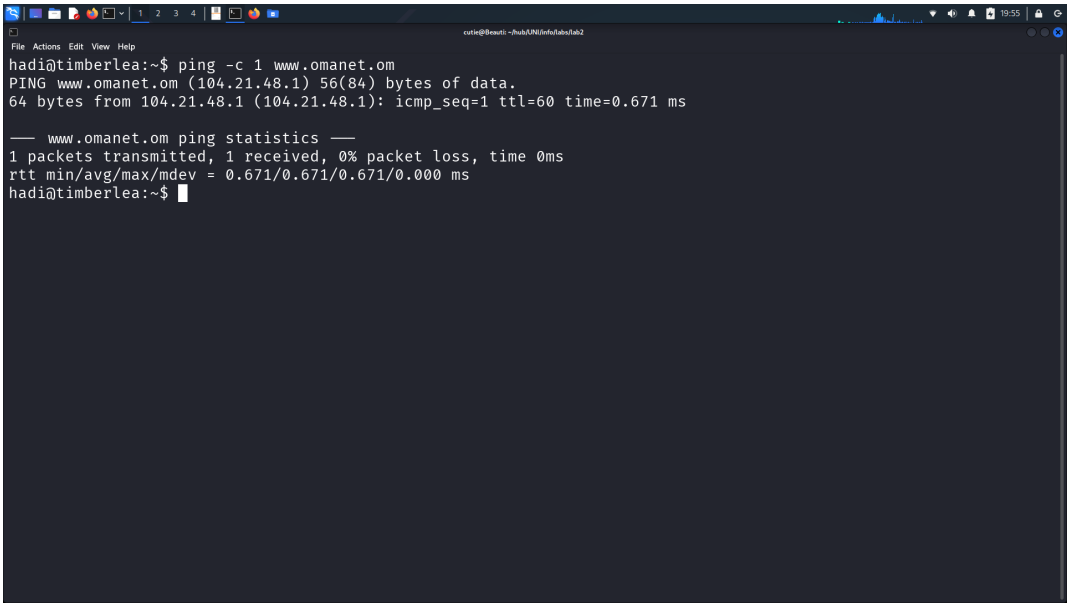
Anas Alhadi

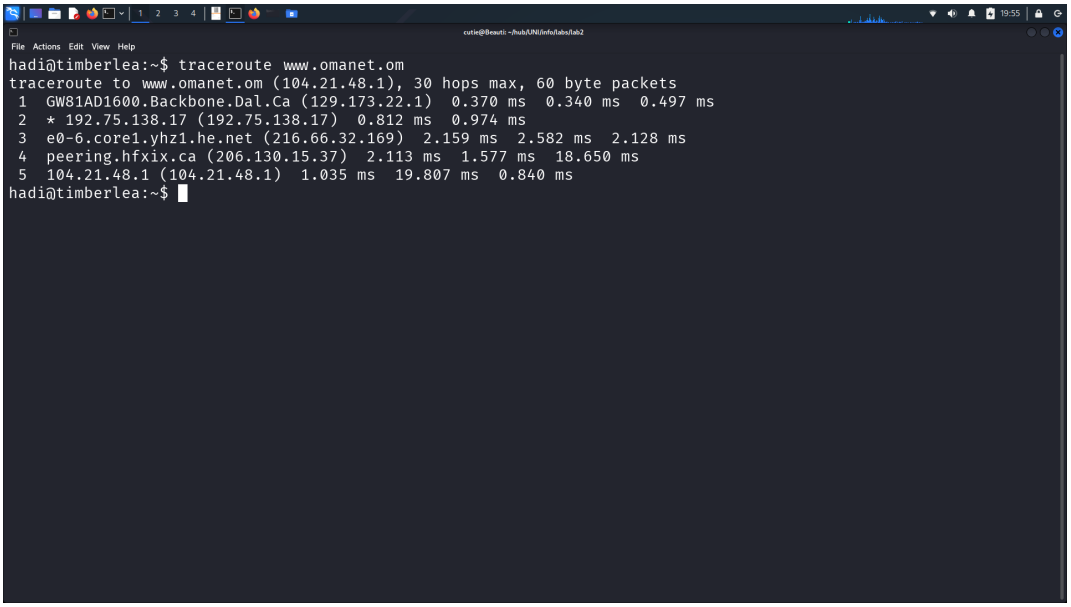
B00895875

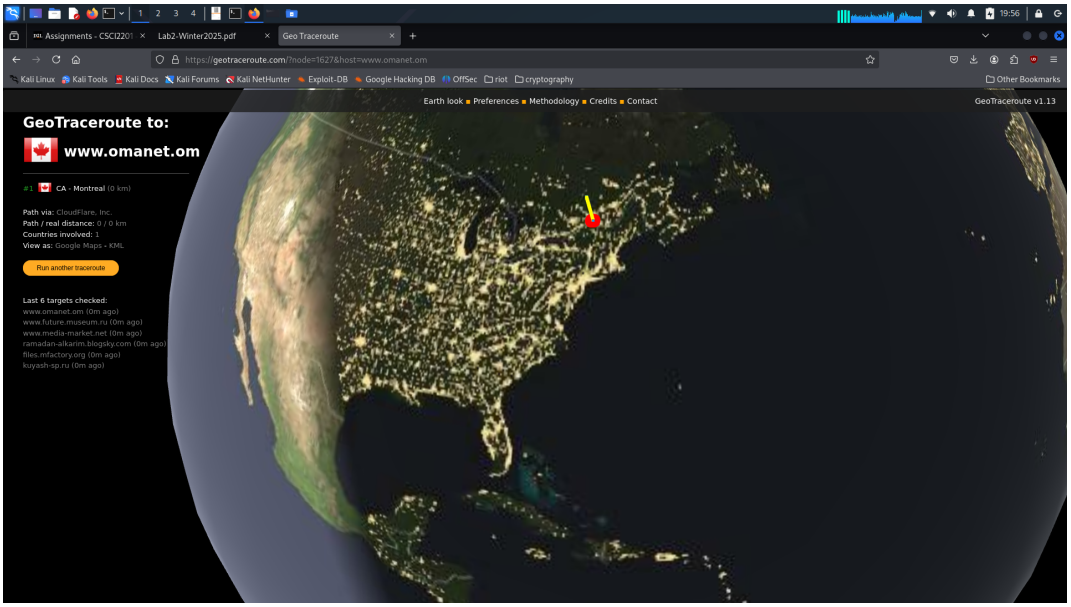
January 31, 2025

Contents

1 Exercise 1


File Actions Edit View Help
hadi@timberlea:~$ ping -c 1 www.omanet.om
PING www.omanet.om (104.21.48.1) 56(84) bytes of data.
64 bytes from 104.21.48.1 (104.21.48.1): icmp_seq=1 ttl=60 time=0.671 ms
--- www.omanet.om ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.671/0.671/0.671/0.000 ms
hadi@timberlea:~$


File Actions Edit View Help
hadi@timberlea:~$ traceroute www.omanet.om
traceroute to www.omanet.om (104.21.48.1), 30 hops max, 60 byte packets
1 GW81AD1600.Backbone.Dal.Ca (129.173.22.1) 0.370 ms 0.340 ms 0.497 ms
2 * 192.75.138.17 (192.75.138.17) 0.812 ms 0.974 ms
3 e0-6.core1.yhz1.he.net (216.66.32.169) 2.159 ms 2.582 ms 2.128 ms
4 peering.hfxix.ca (206.130.15.37) 2.113 ms 1.577 ms 18.650 ms
5 104.21.48.1 (104.21.48.1) 1.035 ms 19.807 ms 0.840 ms
hadi@timberlea:~$



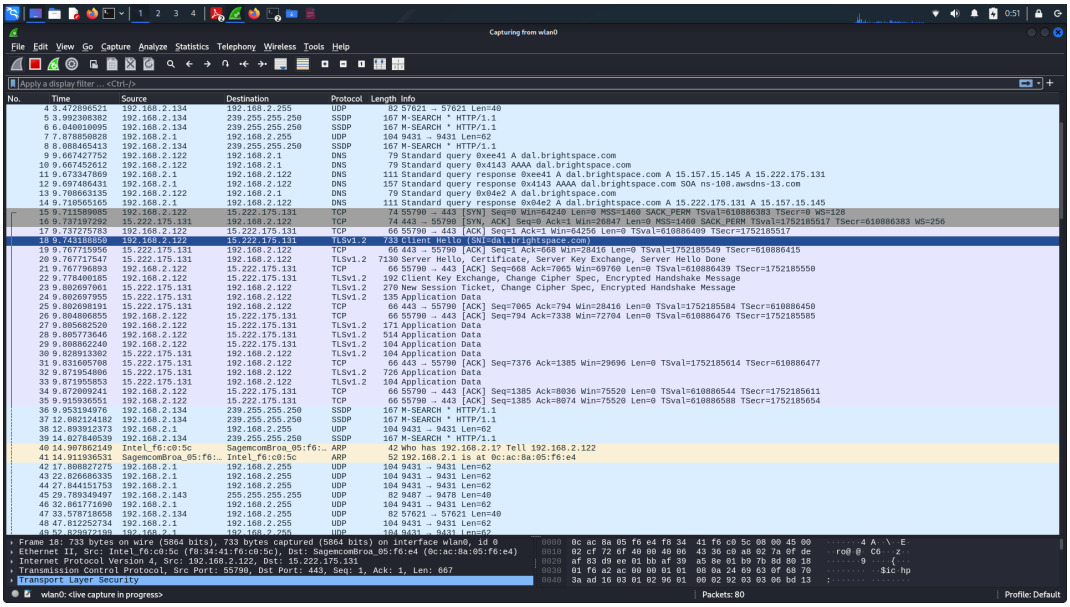
Q1) What was the first hop when tracing from timberlea, and where is the server located?

A) Dal's backbone network. The server is probably in the Goldberg or somewhere on compus.

Q2) Why/why not allow pings and traceroute.

A) ICMP echo requests (which are used by ping and traceroute) can be used to troubleshoot our servers (to check if they are up). On the otherhand, servers can get "flooded" with echo requests (A possible vector of DDoS attacks). I think servers should be allowed to respong to echo requests but also have a rate limit set up to stop processing such requests once we hit a specific threshold.

2 Exercise 2



Q1) Are there any packets

A) Yes, I had firefox open in the background and also refreshed the brighspace webpage.

3 Exercise 3

Figure 1: Full capture

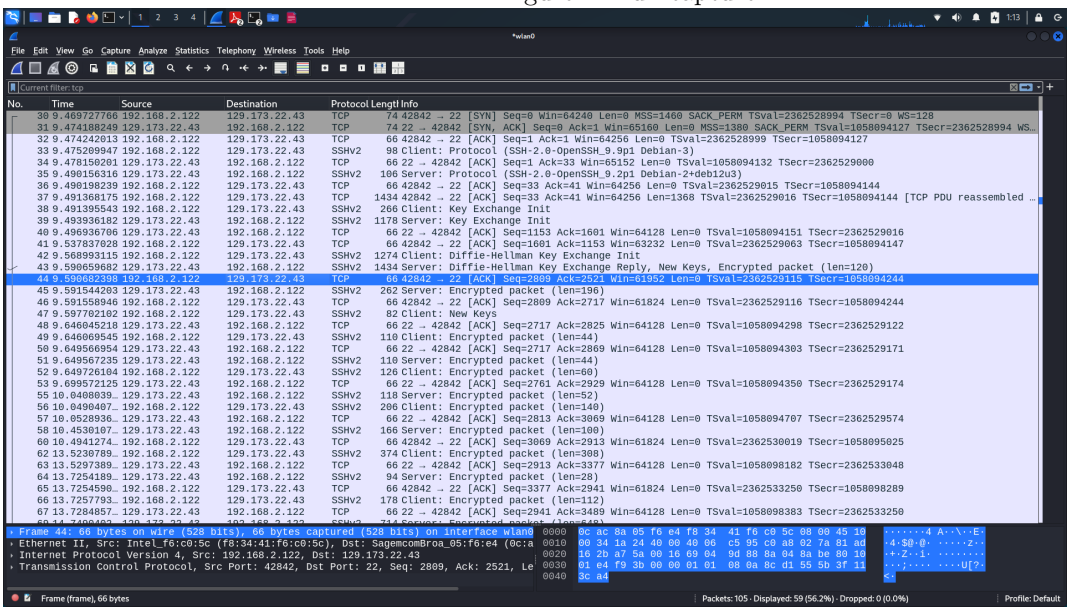
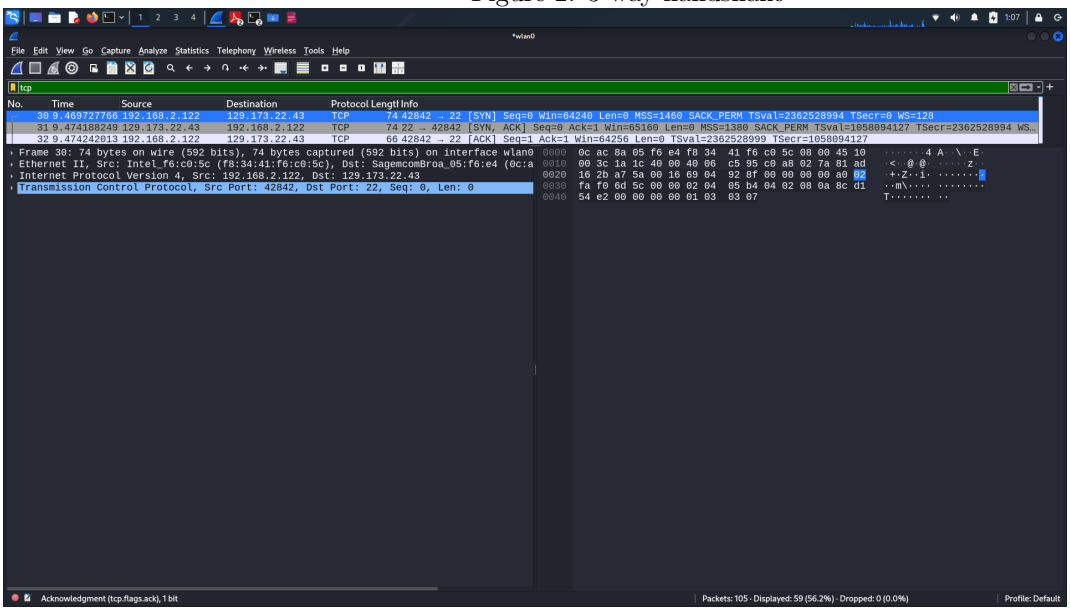


Figure 2: 3-way handshake



Q1) What is timberlea.cs.dal 's IP address

A) 129.173.22.43

Q2) What was the port number used

A) port 22, this is the standard port used for ssh.

4 Exercise 4

- **Client IP:** 192.168.4.17
- **Server IP:** 184.72.58.135
- **TLS handshake steps:**
  1. Client Hello message, where it client initialtes the handshake
  2. Server Hello message, server responds with the cipher suit in our case it uses Diffie Helman key exchange with RSA as the authentication protocol and encrypted with AES-128
  3. Server sends is Digital Certificate
  4. Server Key exchange, server sends it's diffie helman parameters
  5. Client Key exchange, client sends it's diffie helman parameters
  6. Change Spec message, server sends a message indicating that future messages switch to use the key result from diffie helman.
- **Application Data:** There is no human readable data as it is now all encrypted after the TLS handshake.

Figure 3: Application Data