Labtainer: iptables2

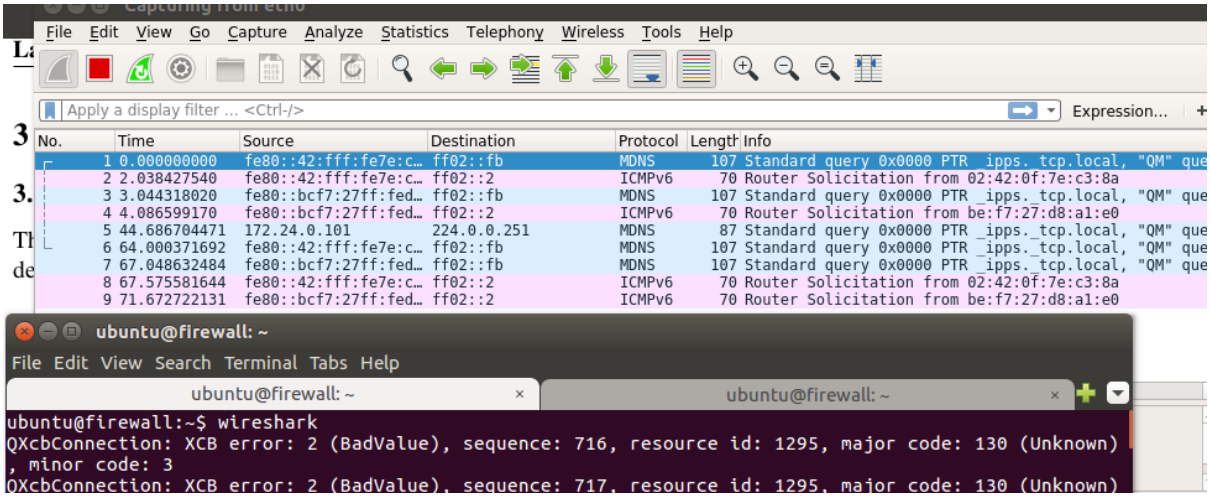
Ecole des Mines Saint Etienne

Malshani RANCHA GODAGE

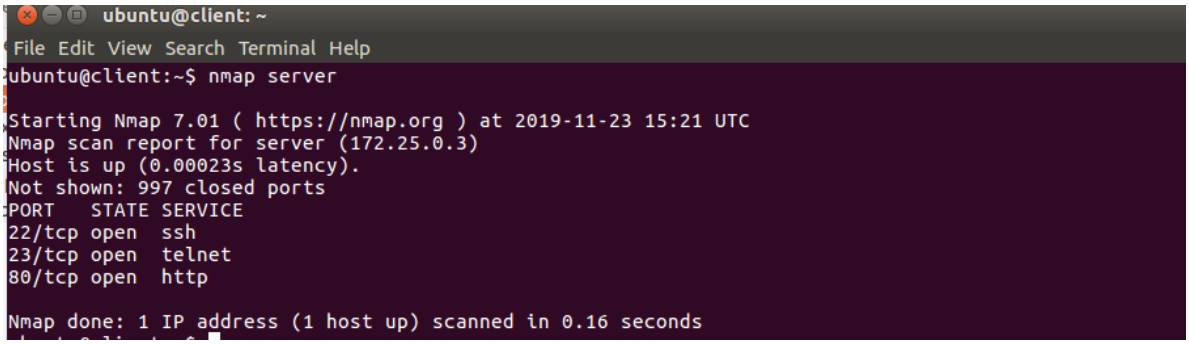
11/23/2019

3.1. Explore

Run **wireshark** command in firewall terminal to run wireshark to check the network traffic. It is free and open source tool to analyze packets going through the networks.

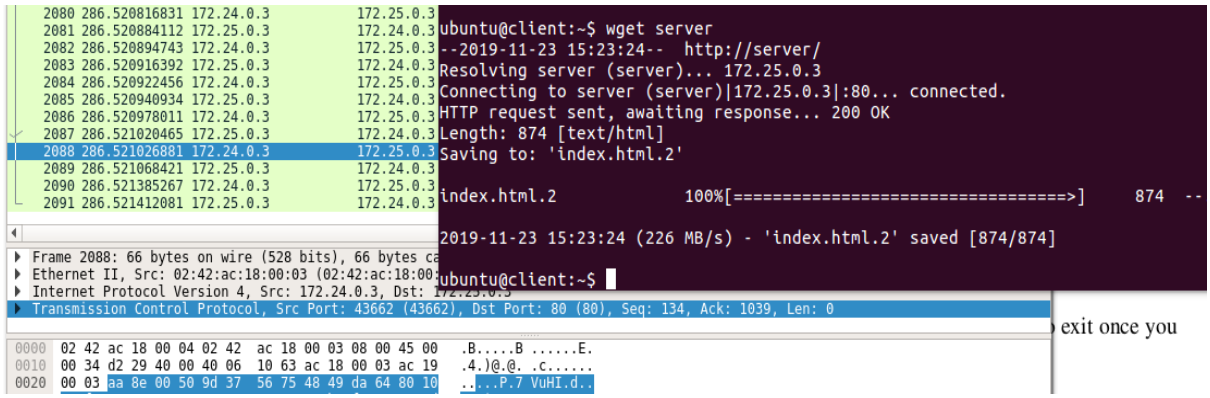


Check the ports of server in client terminal using **nmap server** command. I found three ports such as 22, 23 and 80 with respect to ssh, tenet and http services.

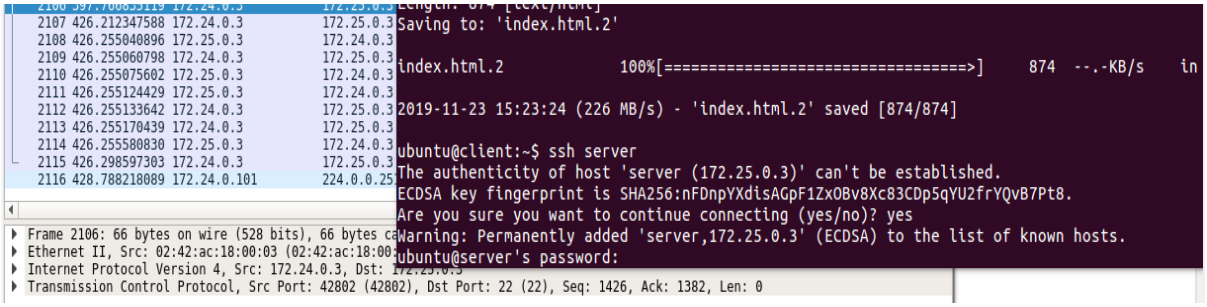


Then I tried to connect to server from client terminal using ssh, telnet and http services.

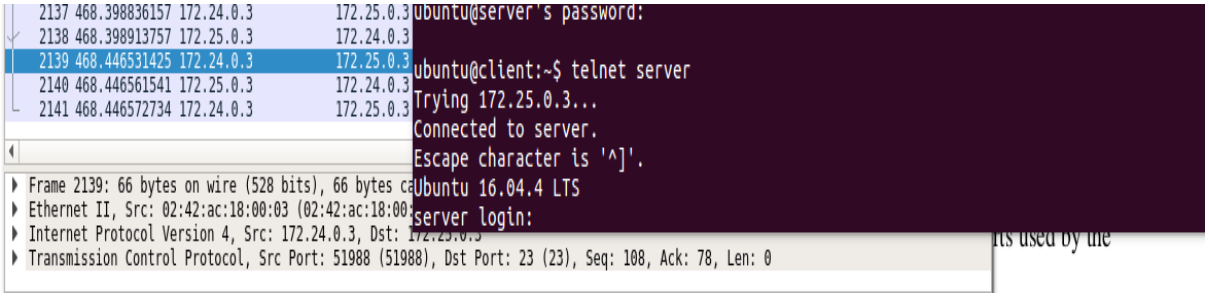
Connect using http by typing the command **wget server.** I saw the data packets on the wireshark interface.



I connected using ssh, by typing **ssh server.** I saw the data packets on wireshark.



Connect using telnet by typing the command **telnet server**. I saw the data packets on wireshark.

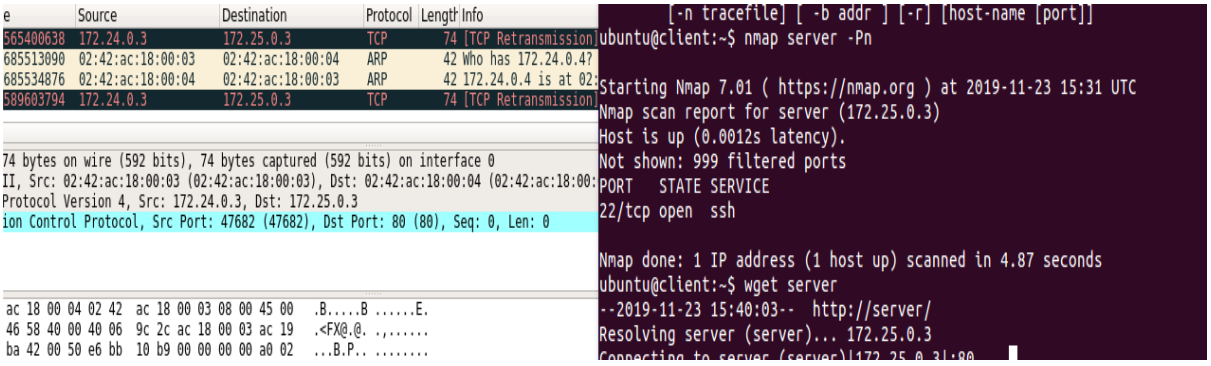


Three services are working with mentioned three ports. Because they are open in the iptable of firewall.

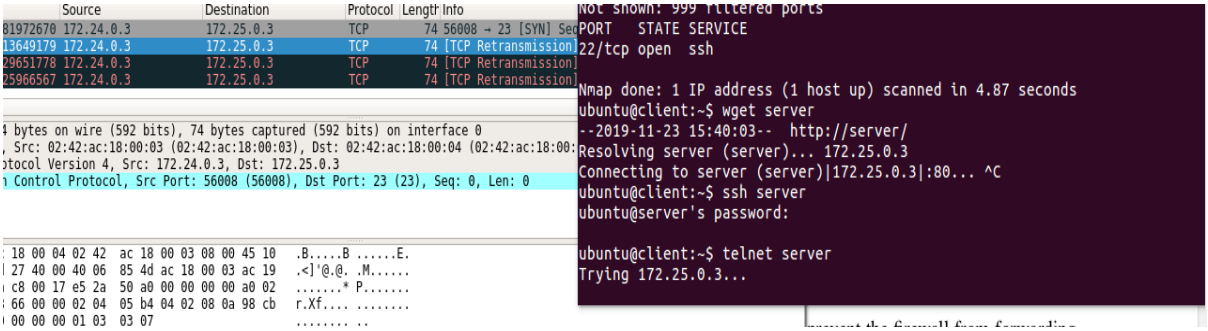
3.2. Limit traffic

Now I run the programme **example_fw.sh** with administrative authorization. Then I tried to run above three commands to connect to the server from the client, but only ssh is working. Both telnet and http are not working.

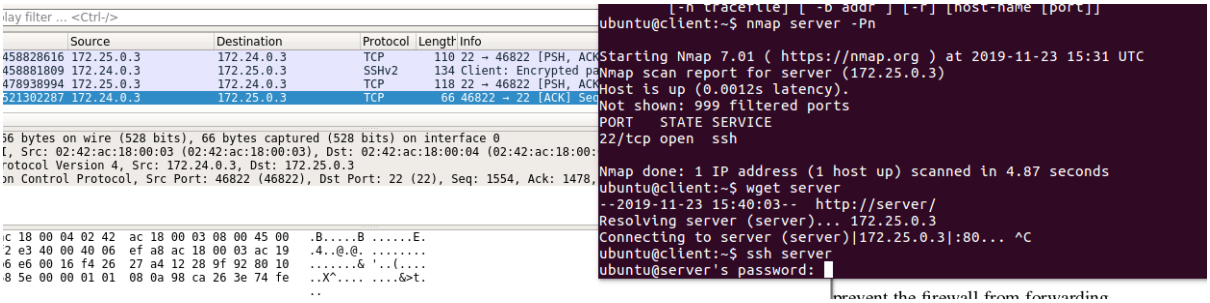
Try http, gave me packets of re-transmissions.



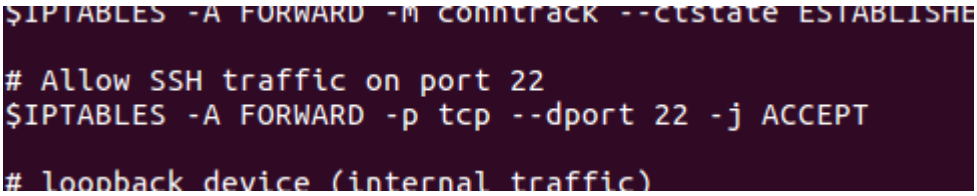
Try telnet, gave me retransmission.



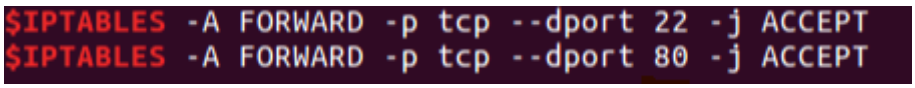
Try ssh, its connecting and I see the packets of connection.



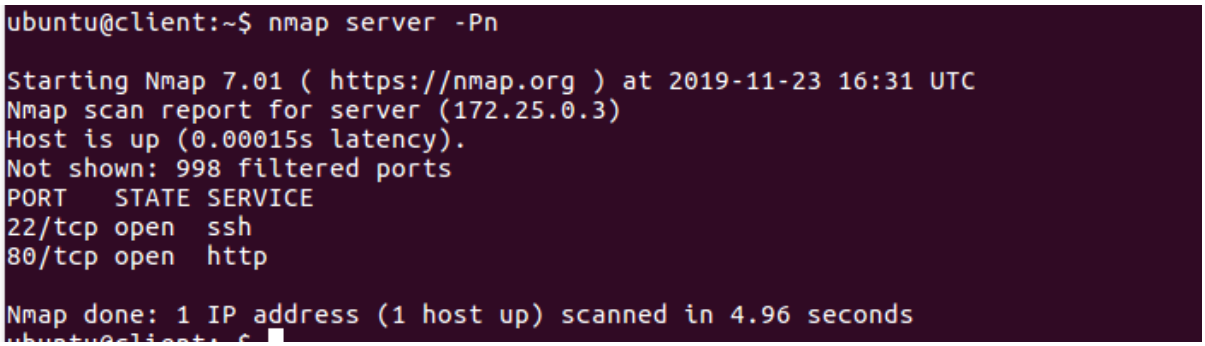
Then I checked my iptable by typing **nmap server –Pn** command. It only showed me port 22 ssh service. Then I checked the content of example_fw.sh and I found a rule only for port 22. Only port 22 is accepted as following image.



I want to accept HTTP as well as SHS. So I updated example_fw.sh file by adding a forwarding rule for accept port 80.



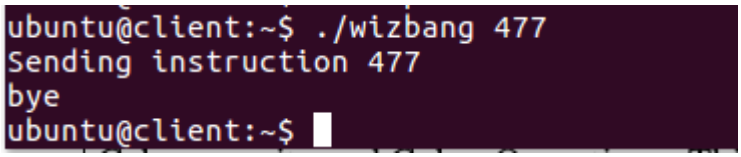
Then I tried to connect from client to the server using HTTP by typing **wget server**, I successfully saw the data packets in wireshark. Then I confirmed my configuration by checking iptable.



I don’t have telnet in my iptable, once I try to connect using telnet my data packets are not forwarding by the firewall. I can check these dropping packets in the iptables log file. I read the last entries of my log file and confirmed dropped packets by port 23.

3.3. Open a new service port

I ran the wizbang program with an argument, while checking the wireshark. Then I noticed the prot number is 10039. Then I registered this new port in my iptable by updating the example_fw.sh programme on the firewall. After I run it, I ran the wizbang program and it connected successfully.



Then I checked my iptable but it did not give me port I registered. My port was between 100 and 20000, so I ran the command **nmap –p 100-20000 server** to check new port. It was successfully showed and confirmed the configuration.