

Labtainer: iptables2

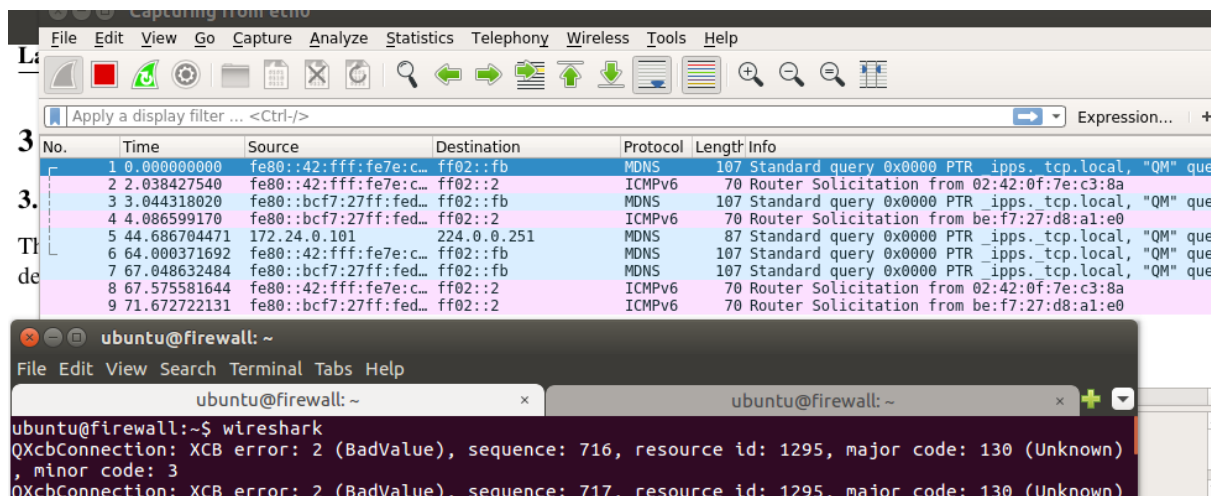
Ecole des Mines Saint Etienne

Malshani RANCHA GODAGE

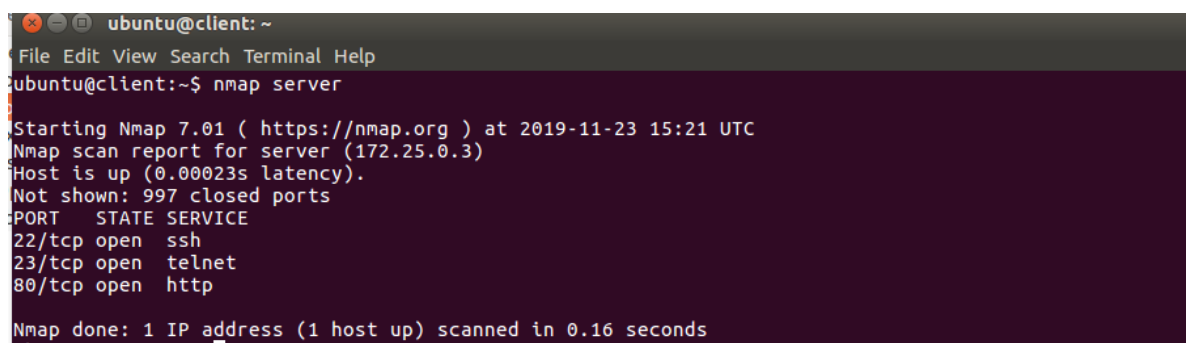
11/23/2019

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.

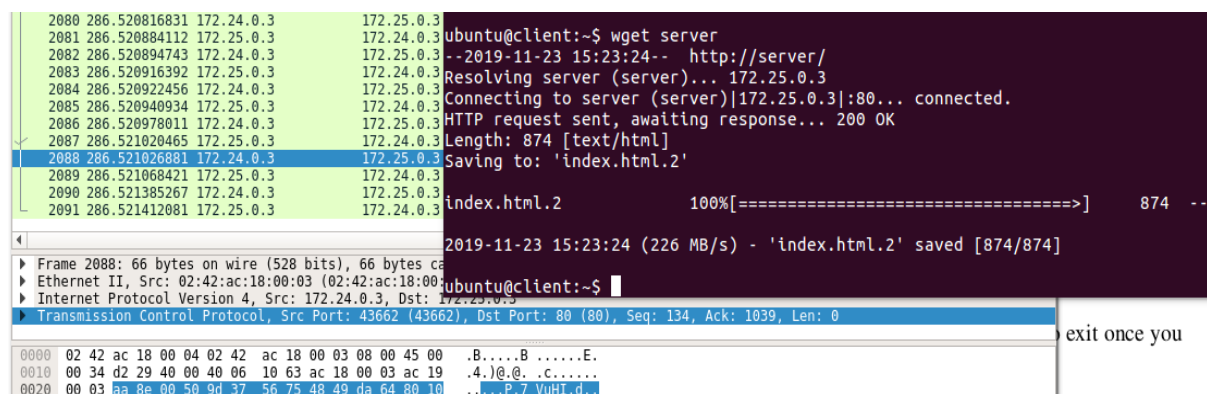


Check the ports of server in client terminal using **nmap server** command. I found three ports such as 22, 23 and 80 with respect to ssh, telnet and http services.



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.

```

2107 426.212347588 172.24.0.3 172.25.0.3 Saving to: 'index.html.2'
2108 426.255040896 172.25.0.3 172.24.0.3
2109 426.255060798 172.24.0.3 172.25.0.3 index.html.2 100%[=====] 874 --KB/s in
2110 426.255075602 172.25.0.3 172.24.0.3
2111 426.255124429 172.25.0.3 172.24.0.3
2112 426.255133642 172.24.0.3 172.25.0.3 2019-11-23 15:23:24 (226 MB/s) - 'index.html.2' saved [874/874]
2113 426.255170439 172.24.0.3 172.25.0.3
2114 426.255580830 172.25.0.3 172.24.0.3 ubuntu@client:~$ ssh server
2115 426.298597303 172.24.0.3 172.25.0.3 The authenticity of host 'server (172.25.0.3)' can't be established.
2116 428.788218089 172.24.0.101 224.0.0.255 ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1Zx0Bv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server,172.25.0.3' (ECDSA) to the list of known hosts.
ubuntu@server's password:

```

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

```

2137 468.398836157 172.24.0.3 172.25.0.3 ubuntu@server's password:
2138 468.398913757 172.25.0.3 172.24.0.3
2139 468.446531425 172.24.0.3 172.25.0.3 ubuntu@client:~$ telnet server
2140 468.446561541 172.25.0.3 172.24.0.3 Trying 172.25.0.3...
2141 468.446572734 172.24.0.3 172.25.0.3 Connected to server.
Escape character is '^]'.
ubuntu 16.04.4 LTS
server login:

```

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.

e	Source	Destination	Protocol	Length	Info
565400638	172.24.0.3	172.25.0.3	TCP	74	[TCP Retransmission]
685513090	02:42:ac:18:00:03	02:42:ac:18:00:04	ARP	42	Who has 172.24.0.4?
685534876	02:42:ac:18:00:04	02:42:ac:18:00:03	ARP	42	172.24.0.4 is at 02:42:ac:18:00:03
589603794	172.24.0.3	172.25.0.3	TCP	74	[TCP Retransmission]

```

74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
II, Src: 02:42:ac:18:00:03 (02:42:ac:18:00:03), Dst: 02:42:ac:18:00:04 (02:42:ac:18:00:04)
Protocol Version 4, Src: 172.24.0.3, Dst: 172.25.0.3
Transmission Control Protocol, Src Port: 47682 (47682), Dst Port: 80 (80), Seq: 0, Len: 0

ac 18 00 04 02 42 ac 18 00 03 08 00 45 00 .B....B.....E.
46 58 40 00 40 06 9c 2c ac 18 00 03 ac 19 .<FX@.@.....
ba 42 00 50 e6 bb 10 b9 00 00 00 00 a0 02 ...B.P.....

[-n tracefile] [-b addr] [-r] [host-name [port]]
ubuntu@client:~$ nmap server -Pn
Starting Nmap 7.01 ( https://nmap.org ) at 2019-11-23 15:31 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.0012s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
ubuntu@client:~$ wget server
--2019-11-23 15:40:03-- http://server/
Resolving server (server)... 172.25.0.3
Connecting to server (server)|172.25.0.3|:80

```

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 to 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.

4

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.

```
ubuntu@firewall:~$ tail -f /var/log/iptables.log
Nov 23 15:43:13 firewall IPTABLES DROPPED IN=eth0 OUT=eth1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.24.0.3 DST=172.25.0.3 LEN=60
TOS=10 PREC=0x00 TTL=63 ID=23848 DF PROTO=TCP SPT=56008 DPT=23 SEQ=3844755616 ACK=0 WINDOW=29200 SYN URG=0 MARK=0
Nov 23 15:43:17 firewall IPTABLES DROPPED IN=eth0 OUT=eth1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.24.0.3 DST=172.25.0.3 LEN=60
TOS=10 PREC=0x00 TTL=63 ID=23849 DF PROTO=TCP SPT=56008 DPT=23 SEQ=3844755616 ACK=0 WINDOW=29200 SYN URG=0 MARK=0
Nov 23 15:43:41 firewall IPTABLES DROPPED IN=eth0 OUT=eth1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.24.0.3 DST=172.25.0.3 LEN=60
TOS=10 PREC=0x00 TTL=63 ID=23851 DF PROTO=TCP SPT=56008 DPT=23 SEQ=3844755616 ACK=0 WINDOW=29200 SYN URG=0 MARK=0
Nov 23 15:44:13 firewall IPTABLES DROPPED IN=eth0 OUT=eth1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.24.0.3 DST=172.25.0.3 LEN=60
TOS=10 PREC=0x00 TTL=63 ID=23852 DF PROTO=TCP SPT=56008 DPT=23 SEQ=3844755616 ACK=0 WINDOW=29200 SYN URG=0 MARK=0
Nov 23 16:28:32 firewall IPTABLES DROPPED IN=eth0 OUT=eth1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.24.0.3 DST=172.25.0.3 LEN=60
```

3.3. Open a new service port

I ran the wizbang program with an argument, while checking the wireshark. Then I noticed the port 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.

```
ubuntu@client:~$ ./wizbang 477
Sending instruction 477
bye
ubuntu@client:~$
```

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.

```
ubuntu@client:~$ sudo nmap server

Starting Nmap 7.01 ( https://nmap.org ) at 2019-11-23 17:37 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.00013s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
ubuntu@client:~$ nmap -p 100-20000 server

Starting Nmap 7.01 ( https://nmap.org ) at 2019-11-23 17:38 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.0023s latency).
Not shown: 19900 filtered ports
PORT      STATE SERVICE
10039/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 44.58 seconds
ubuntu@client:~$
```