Lamar Roulhac

Firewall Configuration and Network Traffic Analysis

Background

Firewalls play a critical role in securing networks by monitoring and controlling incoming and outgoing network traffic based on the rules set by the admin. In Linux UFW provides an interface for managing firewall rules. We also use Wireshark to analyze the network before and after rule enforcement.

Objectives

- Create firewall rules to block access to websites.

- Observe and analyze both allowed and blocked network traffic using Wireshark.

Procedures

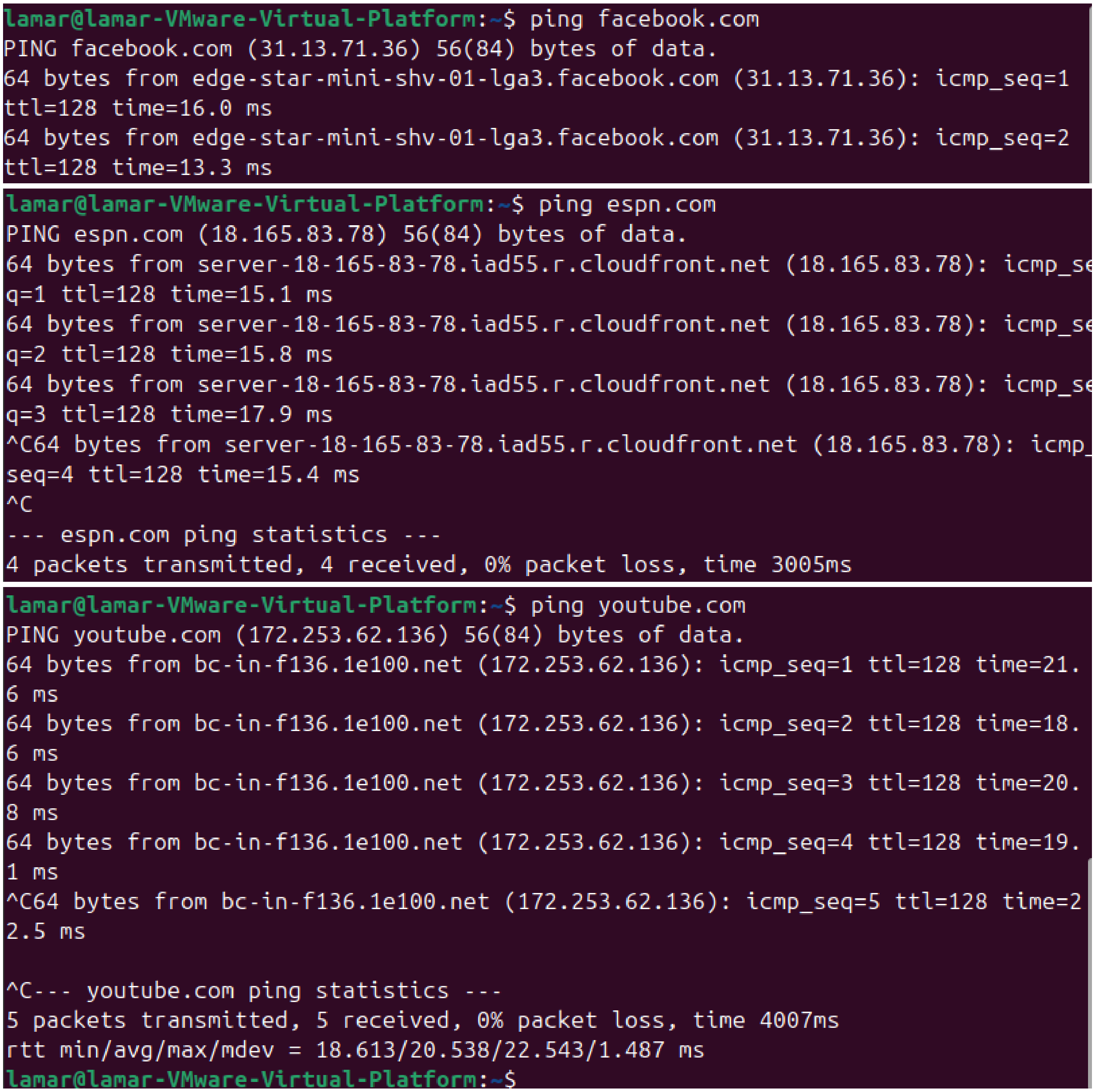
Booted up the Linux VM. I then chose 3 websites to block IP's from

youtube.com

facebook.com

espn.com

I then opened terminal to ping each of the websites to confirm connectivity and get their Ip addresses to block as seen in **Figure 1**.



```
lamar@lamar-VMware-Virtual-Platform:~$ ping facebook.com
PING facebook.com (31.13.71.36) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-lga3.facebook.com (31.13.71.36): icmp_seq=1
ttl=128 time=16.0 ms
64 bytes from edge-star-mini-shv-01-lga3.facebook.com (31.13.71.36): icmp_seq=2
ttl=128 time=13.3 ms
```

```
lamar@lamar-VMware-Virtual-Platform:~$ ping espn.com
PING espn.com (18.165.83.78) 56(84) bytes of data.
64 bytes from server-18-165-83-78.iad55.r.cloudfront.net (18.165.83.78): icmp_se
q=1 ttl=128 time=15.1 ms
64 bytes from server-18-165-83-78.iad55.r.cloudfront.net (18.165.83.78): icmp_se
q=2 ttl=128 time=15.8 ms
64 bytes from server-18-165-83-78.iad55.r.cloudfront.net (18.165.83.78): icmp_se
q=3 ttl=128 time=17.9 ms
^C64 bytes from server-18-165-83-78.iad55.r.cloudfront.net (18.165.83.78): icmp_
seq=4 ttl=128 time=15.4 ms
^C
--- espn.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
```

```
lamar@lamar-VMware-Virtual-Platform:~$ ping youtube.com
PING youtube.com (172.253.62.136) 56(84) bytes of data.
64 bytes from bc-in-f136.1e100.net (172.253.62.136): icmp_seq=1 ttl=128 time=21.
6 ms
64 bytes from bc-in-f136.1e100.net (172.253.62.136): icmp_seq=2 ttl=128 time=18.
6 ms
64 bytes from bc-in-f136.1e100.net (172.253.62.136): icmp_seq=3 ttl=128 time=20.
8 ms
64 bytes from bc-in-f136.1e100.net (172.253.62.136): icmp_seq=4 ttl=128 time=19.
1 ms
^C64 bytes from bc-in-f136.1e100.net (172.253.62.136): icmp_seq=5 ttl=128 time=2
2.5 ms

^C--- youtube.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 18.613/20.538/22.543/1.487 ms
lamar@lamar-VMware-Virtual-Platform:~$
```

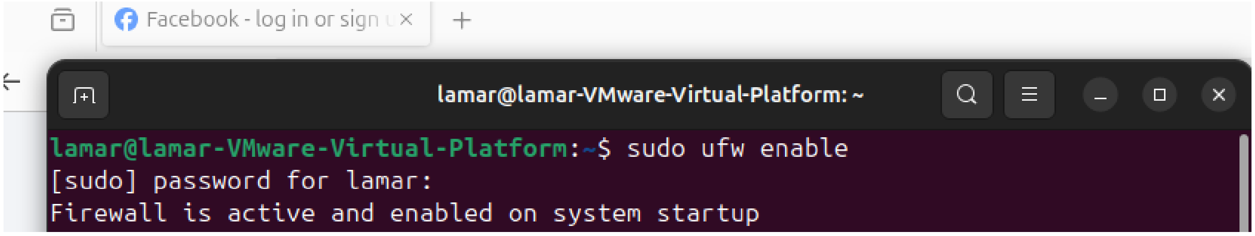
Figure 1: Pinging the Websites and Getting the IP

Then once I got the information i enabled UFW and blocked the website IPs. The command used to enable the UFW was: `sudo ufw enable` **(Figure 2).** Once the UFW was enabled as seen in **Figure 3** I was able to block the IPs with the command: `sudo ufw deny out to (the websites IP).` The websites i chose Ip were:

Youtube.com: 172.253.62.136

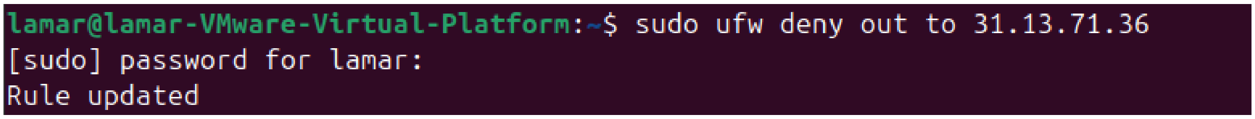
Espn.com: 18.165.83.78

Facebook.com: 31.13.71.36


Facebook - log in or sign u
lamar@lamar-VMware-Virtual-Platform: ~

```
lamar@lamar-VMware-Virtual-Platform:~$ sudo ufw enable
[sudo] password for lamar:
Firewall is active and enabled on system startup
```

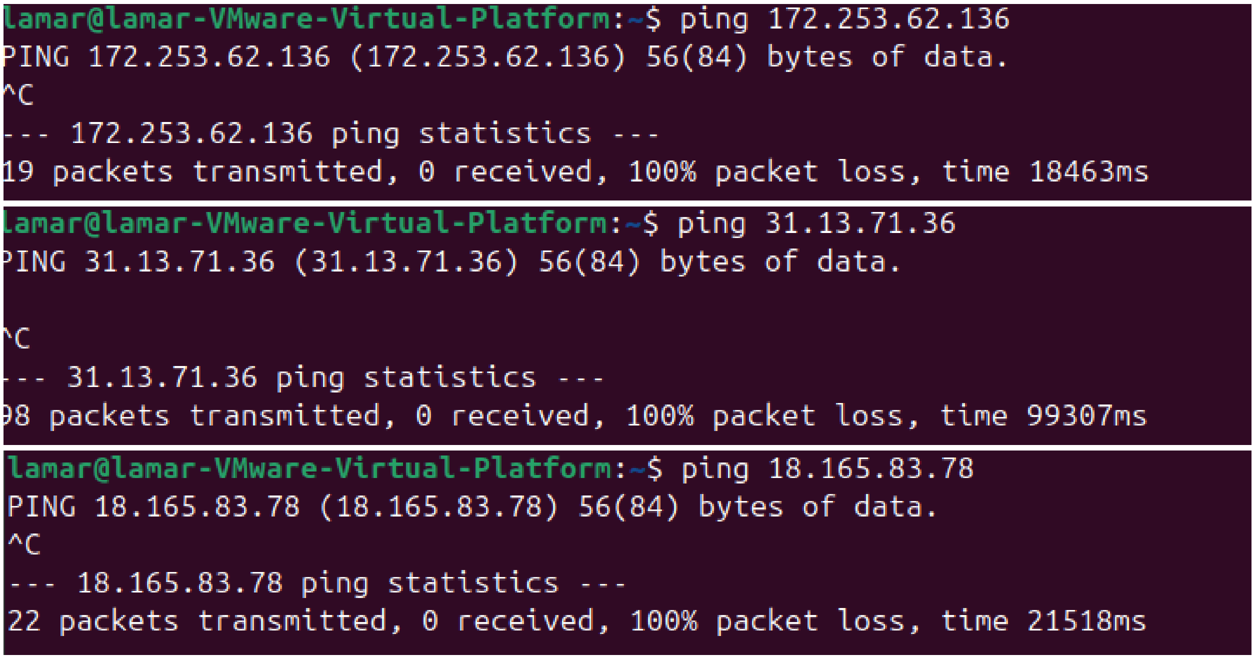
Figure 2: Enabling UFW



```
lamar@lamar-VMware-Virtual-Platform:~$ sudo ufw deny out to 31.13.71.36
[sudo] password for lamar:
Rule updated
```

Figure 3: Blocking IP's

After I blocked their Ip's I attempted to ping them to confirm they have been successfully blocked. As seen in **Figure 4** they are not getting any response back in the ping from the blocked Ip which confirms that the UFW rules are working successfully.



```
lamar@lamar-VMware-Virtual-Platform:~$ ping 172.253.62.136
PING 172.253.62.136 (172.253.62.136) 56(84) bytes of data.
^C
--- 172.253.62.136 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18463ms
```

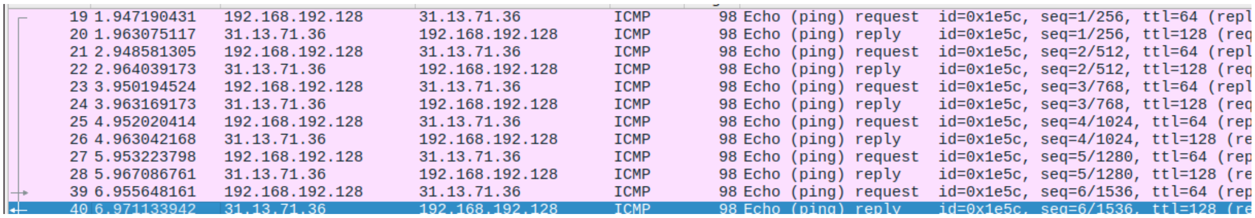
```
lamar@lamar-VMware-Virtual-Platform:~$ ping 31.13.71.36
PING 31.13.71.36 (31.13.71.36) 56(84) bytes of data.

^C
--- 31.13.71.36 ping statistics ---
98 packets transmitted, 0 received, 100% packet loss, time 99307ms
```

```
lamar@lamar-VMware-Virtual-Platform:~$ ping 18.165.83.78
PING 18.165.83.78 (18.165.83.78) 56(84) bytes of data.
^C
--- 18.165.83.78 ping statistics ---
22 packets transmitted, 0 received, 100% packet loss, time 21518ms
```

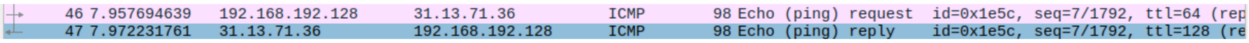
Figure 4: No Response from Pings

I then went into Wireshark and compared the network traffic of the blocked to the unblocked ping commands. As seen in **Figure 5** when the Ip is not blocked the traffic shows multiple reply and request pings in the capture versus in **Figure 6** when the Ip is blocked there is no reply other than the cancel of the ping telling us that 0 packets were received as seen in the terminal screen.



```
19 1.947190431   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=1/256, ttl=64 (repl
20 1.963075117   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=1/256, ttl=128 (req
21 2.948581305   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=2/512, ttl=64 (repl
22 2.964039173   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=2/512, ttl=128 (req
23 3.950194524   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=3/768, ttl=64 (repl
24 3.963169173   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=3/768, ttl=128 (req
25 4.952020414   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=4/1024, ttl=64 (rep
26 4.963042168   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=4/1024, ttl=128 (re
27 5.953223798   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=5/1280, ttl=64 (rep
28 5.967086761   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=5/1280, ttl=128 (re
39 6.955648161   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=6/1536, ttl=64 (rep
40 6.971133942   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=6/1536, ttl=128 (re
```

Figure 5: Unblocked IP Ping



```
46 7.957694639   192.168.192.128   31.13.71.36       ICMP      98 Echo (ping) request  id=0x1e5c, seq=7/1792, ttl=64 (rep
47 7.972231761   31.13.71.36       192.168.192.128   ICMP      98 Echo (ping) reply    id=0x1e5c, seq=7/1792, ttl=128 (re
```

Figure 6: Blocked Ip Ping

Conclusion & Results

Before blocking the Ip's all three target websites were able to be accessed, and after blocking the Ip's the UFW did not allow the Ip to get accessed by the computer and Wireshark showed the lack of replies from the blocked sites.

Blocking IPs is an effective waying to harden your network, but malicious people can change their IP address to bypass it. For you to block a website you'll need to block all their IPs to block all their servers.