Lab - Linux Firewall

Jackson Hallahan

- This is an individual assignment and worth 5 points.
- The due is tonight.
- Submit the outcome file. Follow the naming convention.

Task 1

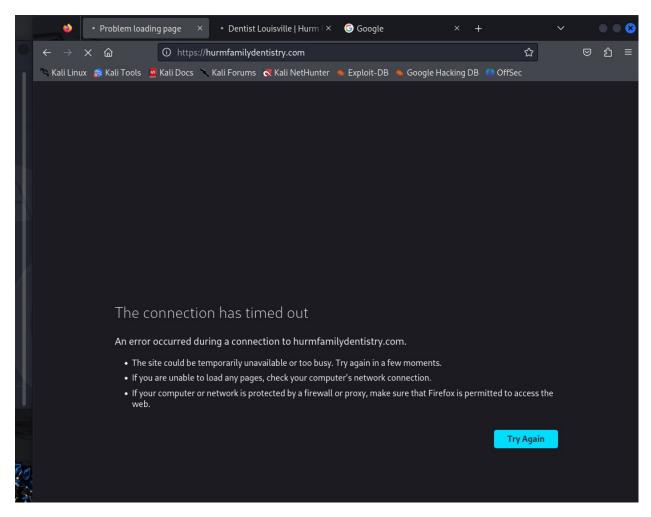
- a) On Kali, create a rule that blocks ping requests to the Kali machine.
- b) Go to the host machine and ping the Kali. Take a screenshot of the output on the host machine.
- c) On Kali, display the rule you created. Take a screenshot of the output.

```
C:\Users\jacks>ping 192.168.189.128
Pinging 192.168.189.128 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.189.128:
        Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\jacks>
```

```
[/home/kali]
   sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 2549 packets, 1797K bytes)
 pkts bytes target
                  prot opt in out source
                                                                 destination
   4 240 DROP
                                             0.0.0.0/0
                      icmp --
                                                                 0.0.0.0/0
                                                                                      icmptype 8
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
                                                                 destination
pkts bytes target
                    prot opt in
                                             source
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
                                                                 destination
pkts bytes target
                                     out
                                            source
                    prot opt in
           li)-[/home/kali]
```

Task 2

- a) On Kali, launch Firefox and visit <u>hurmfamilydentistry.com</u>. Make sure the website is displayed properly.
- b) Create a rule that blocks access to this site. On a separate tab of the browser, visit the site again and show in a screenshot that the site now is not accessible.
- c) Display the rule you created. Take a screenshot of the output. (Hint: watch the 2nd video in Tutorial 1).



```
<u>sudo</u> iptables -A INPUT -s hurmfamilydentistry.com -j DROP
__(kali⊛kali)-[~]

$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 22 packets, 1152 bytes)
pkts bytes target
                        prot opt in
                                                                        destination
                                         out
                                                  source
          0 DROP
                                                  160.153.0.154
                                                                        0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target
                        prot opt in
                                                  source
                                                                        destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
                                                                        destination
 pkts bytes target
                        prot opt in
                                         out
                                                  source
```