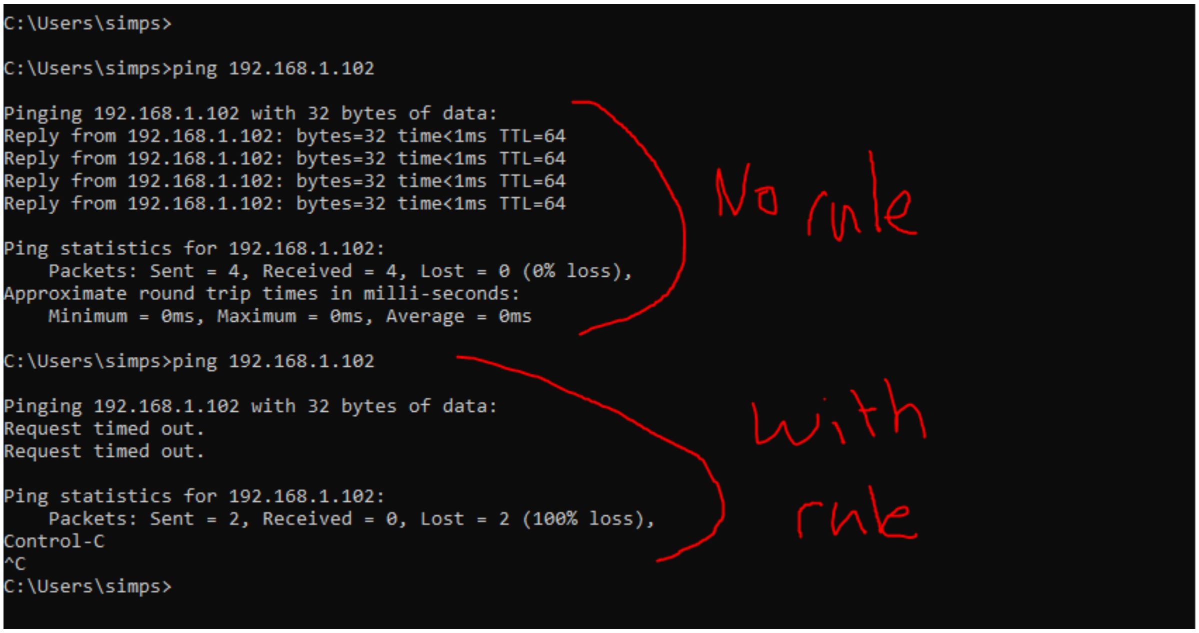
Lab - Linux Firewall

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

Task 1

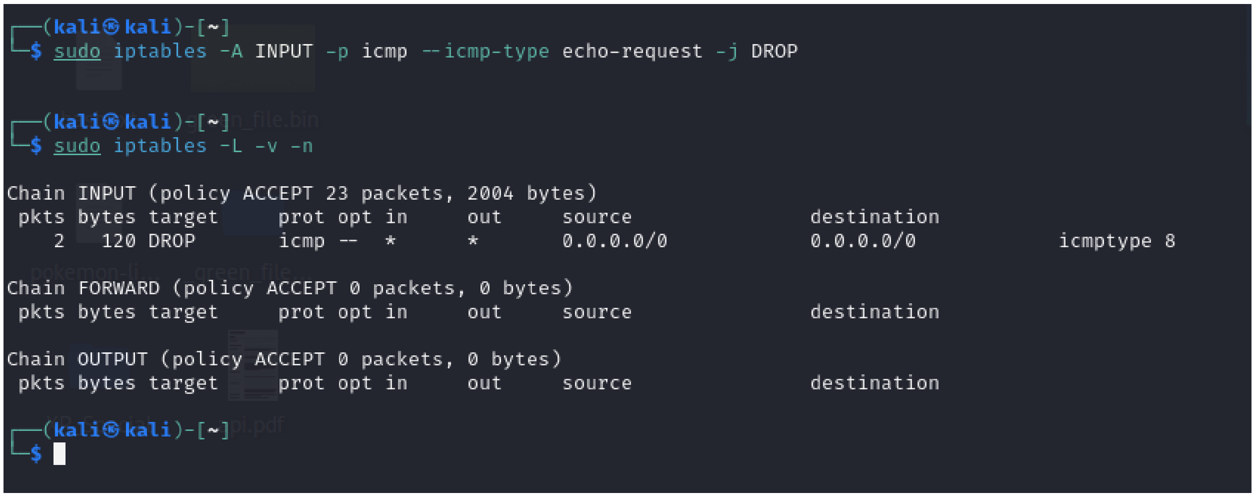
a) On Kali, create a rule that blocks ping requests to the Kali machine.
b) Go to the host machine and ping the Kali. Take a screenshot of the output on the host machine.
c) On Kali, display the rule you created. Take a screenshot of the output.

b.



```
C:\Users\simps>

C:\Users\simps>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.102: bytes=32 time<1ms TTL=64
Reply from 192.168.1.102: bytes=32 time<1ms TTL=64
Reply from 192.168.1.102: bytes=32 time<1ms TTL=64
Reply from 192.168.1.102: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\simps>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.1.102:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\simps>
```

C.



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v -n

Chain INPUT (policy ACCEPT 23 packets, 2004 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   120 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

┌──(kali㉿kali)-[~]
└─$ 
```

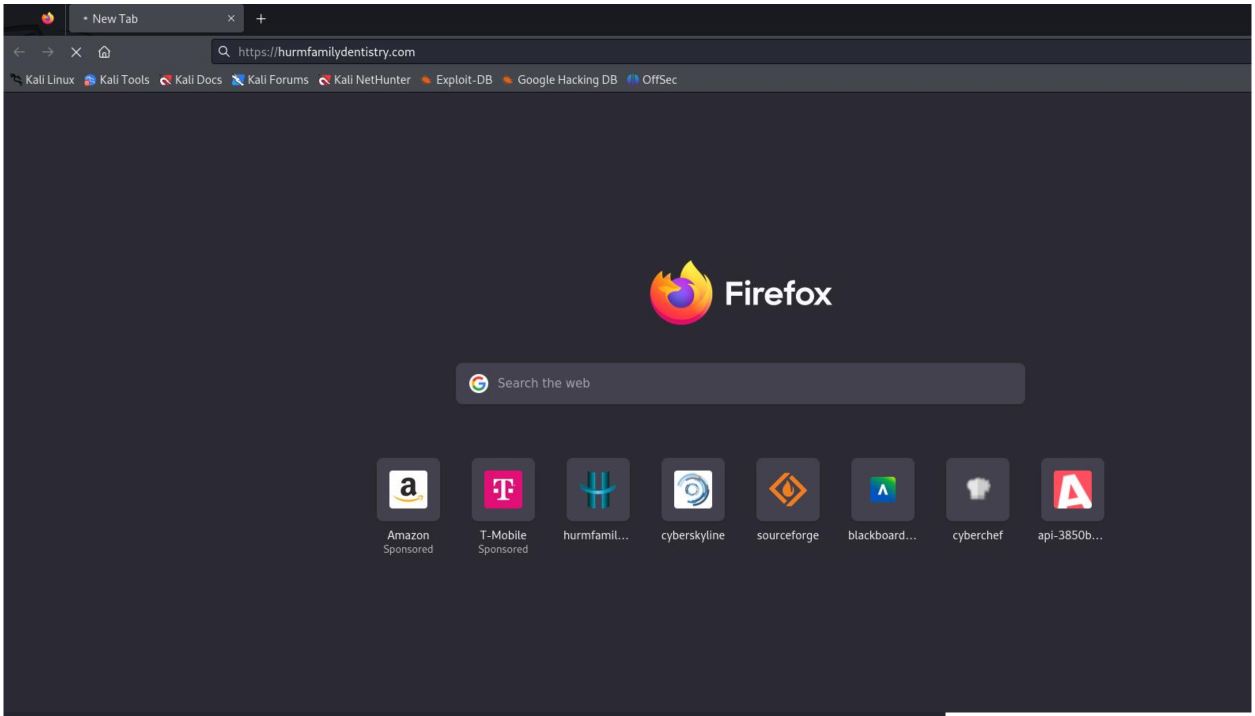
Task 2

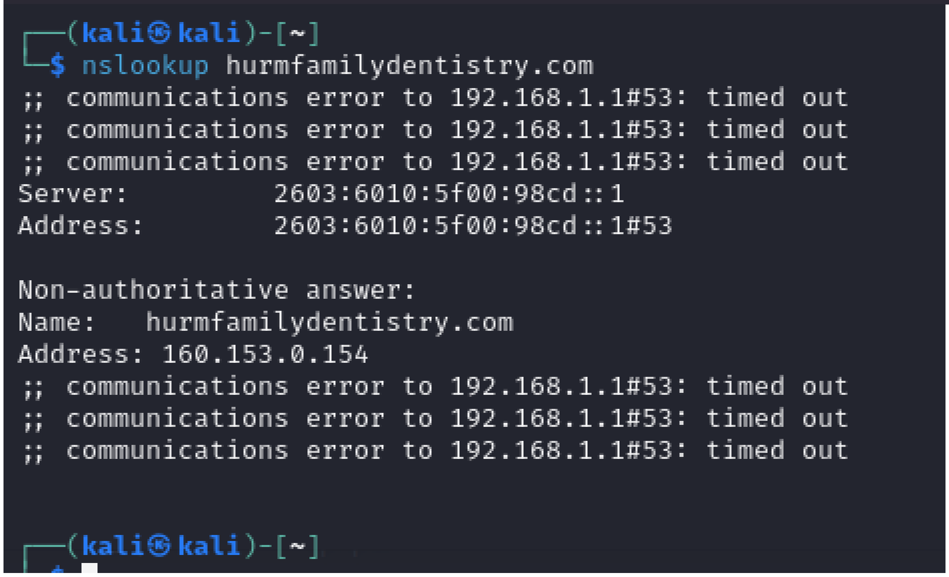
a) On Kali, launch Firefox and visit hurmfamilydentistry.com. Make sure the website is displayed properly.

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).

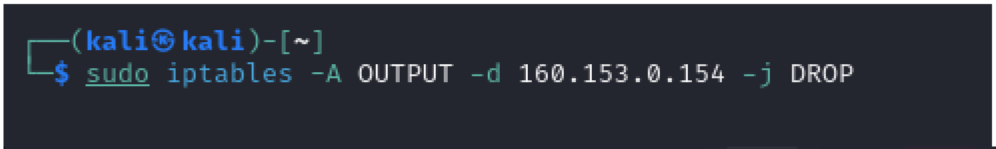
b.



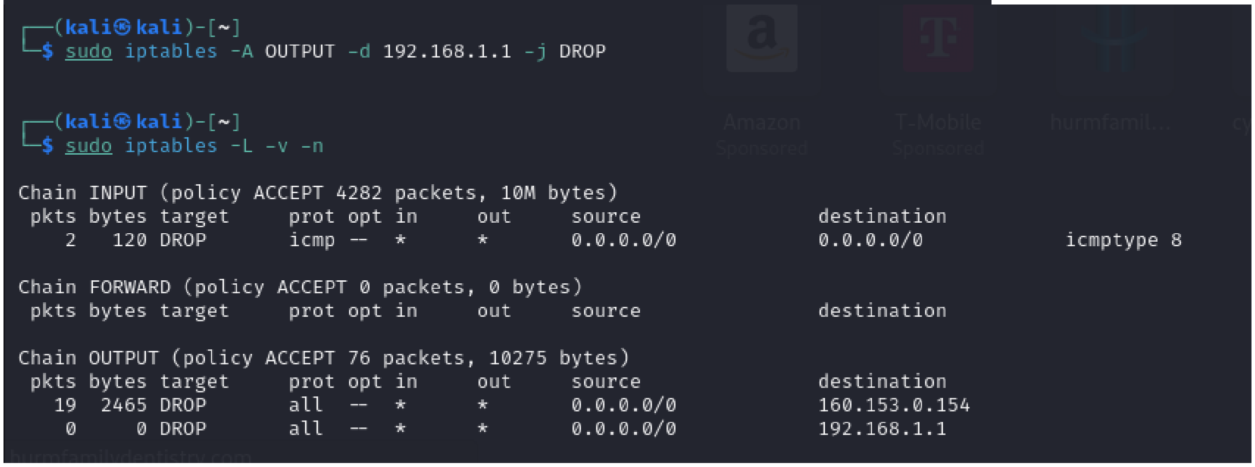


```
┌──(kali㉿kali)-[~]
└─$ nslookup hurmfamilydentistry.com
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
Server:         2603:6010:5f00:98cd::1
Address:        2603:6010:5f00:98cd::1#53

Non-authoritative answer:
Name:   hurmfamilydentistry.com
Address: 160.153.0.154
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out
;; communications error to 192.168.1.1#53: timed out


┌──(kali㉿kali)-[~]
```

c.



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -d 160.153.0.154 -j DROP
```



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -d 192.168.1.1 -j DROP

┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v -n

Chain INPUT (policy ACCEPT 4282 packets, 10M bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   120 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 76 packets, 10275 bytes)
 pkts bytes target     prot opt in     out     source               destination
   19  2465 DROP       all  --  *      *       0.0.0.0/0            160.153.0.154
    0     0 DROP       all  --  *      *       0.0.0.0/0            192.168.1.1
```