IP Tables

ASN FERNANDO

18000509

1.

a. iptables –F

- flushes all chains if none is specified

b. iptables -P INPUT ACCEPT

- define the default policy for input chains and the policy is to accept

c. iptables -A INPUT -i eth1 -s 10.0.0.0/8 -m limit --limit 5/m -- limit-burst 7 -j LOG --log-prefix "IP_SPOOF A: "

- append the input chain for the specified rule to the ethernet 1 network interface, the rule is to log traffic from 10.0.0.0/8 source network which the maximum number of packets within the time frame is 5 per minute and maximum number of initial packets to match before the limit is equals to 7, Log entries will be stored with the prefix "IP SPOOF A:".

d. iptables -A INPUT -p TCP --syn -m limit --limit \ 5/second -j ACCEPT

- append a input chain which is to accept TCP packets with a maximum packet rate of 5 per second. The initial request is set to SYN.

e. iptables -A INPUT -p udp -m time --timestart 02:00 \ --timestop 03:00 -j DROP

- This rule will bring up a invalid message as '\' after the 02:00 is unnecessary the correct rule is **iptables -A INPUT -p udp -m time --timestart 02:00 --timestop 03:00 -j DROP** which is to append a input chain that drops udp packets coming from 02.00 to 03.00

f.

I. /sbin/iptables -N port-scanning

- Create a new chain called port-scanning.

II. /sbin/iptables -A port-scanning -p tcp \ --tcpflags SYN,ACK,FIN,RST RST -m limit \ --limit 1/s -- limit-burst 2 -j RETURN

- This rule will bring up a invalid command because of the 2 forward-slahes the correct command is **/sbin/iptables -A port-scanning -p tcp --tcpflags SYN,ACK,FIN,RST RST -m limit --limit 1/s -- limit-**

burst 2 -j RETURN which is to append tcp protocol flags which are SYN,ACK,FIN,RST and the RST limit should be 1 per second and RST limit equal to 2 return it.

III. /sbin/iptables -A port-scanning -j DROP

- Drop all rules of port-scanning chain

g.

I. /sbin/iptables -A INPUT -p tcp --dport ssh \ -m conntrack --ctstate NEW -m recent –set

- Got invalid command don’t know how to fix it

II. /sbin/iptables -A INPUT -p tcp --dport ssh \ -m conntrack --ctstate NEW -m recent --update \ --seconds 60 --hitcount 10 -j DROP

- Got invalid command don’t know how to fix it.

h. iptables -A FORWARD -p tcp -m multiport --dport \ http,https -o eth0 -i eth1 -m time --timestart 21:30 \ --timestop 22:30 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT

- Append a rule to forward chain that accepts http and https request from Ethernet 1 to Ethernet 0 form 21.30 to 22.30 on weekdays

i. iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP

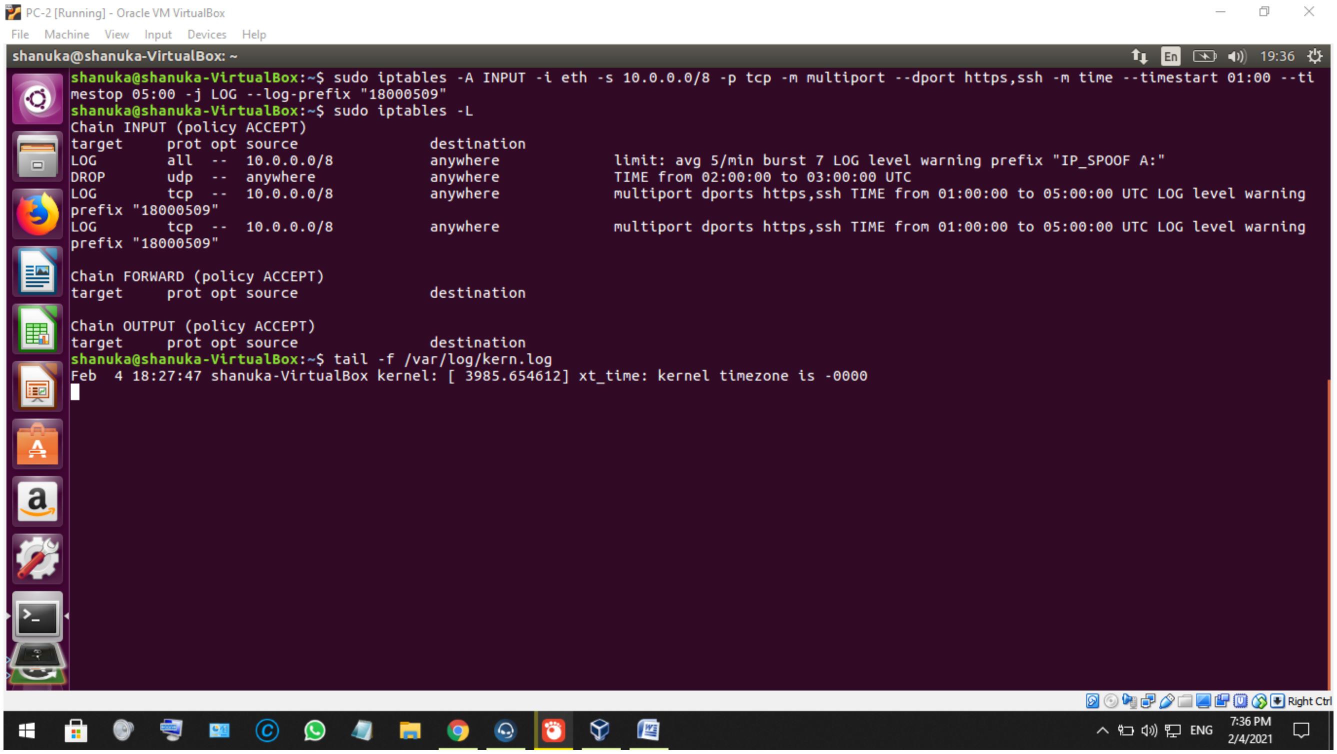
- Append a input chain that drops all the TCP packets

2.

a.

Write an iptables rule to log traffic that are coming from a particular network to the host implementing iptables from 1.00 a.m. to 5.00 a.m. to access https and ssh services. The log entry shall have your index number as a prefix.

The rule command is : iptables –A INPUT –i eth 10.0.0.0/8 –p tcp –m multiport –dport https,ssh –m time –timestart 01:00 –timestop 05:00 –j LOG --l og-prefix “18000509”



PC-2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shanuka@shanuka-VirtualBox: ~
En
19:36
Right Ctrl
ENG
7:36 PM
2/4/2021

```
shanuka@shanuka-VirtualBox:~$ sudo iptables -A INPUT -i eth -s 10.0.0.0/8 -p tcp -m multiport --dport https,ssh -m time --timestart 01:00 --ti
mestop 05:00 -j LOG --log-prefix "18000509"
shanuka@shanuka-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LOG        all  --  10.0.0.0/8           anywhere             limit: avg 5/min burst 7 LOG level warning prefix "IP_SPOOF A:"
DROP       udp  --  anywhere             anywhere             TIME from 02:00:00 to 03:00:00 UTC
LOG        tcp  --  10.0.0.0/8           anywhere             multiport dports https,ssh TIME from 01:00:00 to 05:00:00 UTC LOG level warning
prefix "18000509"
LOG        tcp  --  10.0.0.0/8           anywhere             multiport dports https,ssh TIME from 01:00:00 to 05:00:00 UTC LOG level warning
prefix "18000509"

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
shanuka@shanuka-VirtualBox:~$ tail -f /var/log/kern.log
Feb  4 18:27:47 shanuka-VirtualBox kernel: [ 3985.654612] xt_time: kernel timezone is -0000
```