R.V. COLLEGE OF ENGINEERING
OBSERVATION / DATA SHEET

Date 06/04/21 Name Durgesh kumar

Dept./Lab MCA Class B Expt./No. 07

Title

* Build a firewall to Restrict Network access using firewall or Build a firewall with SNAT or DNAT

Step 1 :- sudo apt-get update ↵ (VM1, VM2, VM3)

Step 2 : sudo apt-get install nmap ↵ (VM1, VM2, VM3)

Step 3 : set host only adaptor

step 4 : check ipaddress of three VM.

VM1$ ifconfig ↵
192.168.0.11

VM2$ ifconfig ↵
192.168.0.12

VM3$ ifconfig ↵
192.168.0.14

Step 5 : go to VM1 :-

$ nmap -sn 192.168.0.11/24

O/P : Starting Nmap 7.01
Nmap scan report for 192.168.0.10

$ sudo iptables -L -n --line

O/P :- chain INPUT policy (ACCEPT)
num target prot opt source destination
chain FORWARD policy (ACCEPT)
num target prot opt source destination
chain OUTPUT policy (ACCEPT)
num target prot opt source destination

Signature of
Teacher incharge

Step 6 :- go to VM2

$ ping 192.168.0.11 (VM1 ipaddress)

o/p: ping 192.168.0.11
64 bytes from 192.168.0.11 : icmp_seq=1 ttl=64 time=0.0.19 ms

Step 7 : go to VM3

$ ping 192.168.0.11 (VM1 ipaddress)

o/p: ping 192.168.0.11 56(84) byte of data
64 bytes from 192.168.0.11 : icmp-seq=1 ttl=64 time=0.019ms
64 bytes from 192.168.0.11 : icmp-seq=2 ttl=64 time=0.01

Step 8 : go to VM1

* Drop transmit packets to VM2 and VM3

$ sudo iptables -P INPUT DROP

* Accept packets of VM2 and VM3

$ sudo iptables -P INPUT ACCEPT

* Now I will stop transmit packet with ipaddress of VM2

$ sudo iptables -I INPUT -S 192.168.0.12 -j DROP
(VM2 ipaddress)

* I will start transmit packet with ipaddress of VM2

$ sudo iptable -I INPUT -S 192.168.0.12 -j ACCEPT

Step 9 :- go to VM3

* Now I will transmit packets using mac address

$ ifconfig

ether addr: 08:00:27:da:22:98

Step 10 :- go to VM1 :-

* I will drop transmit packets

$ sudo iptable -I INPUT -m mac --mac-source
08:00:27:da:22:98 -j DROP

* Now I will start transmit packets :-

$ sudo iptables -I INPUT -m mac --mac-source
08:00:27:da:22:98 -j ACCEPT