### **8: Networking Fundamentals Homework**

**Phase 1: *"I'd like to Teach the World to Ping***

**Summery:**

167.172.144.11/32 IP address accepts connection whiles these others are not allowing connection: 15.199.95.91/28, 15.199.94.91/28,11.199.158.91/28 and 11.199.141.91/28

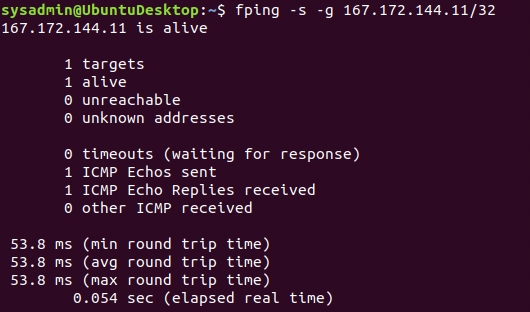
This is the command us : fping -s -g 167.172.144.11/32

The fping -s -g used on 167.172.144.11/32 shows: it’s only one target device and it's alive, 0 unreachable and no unknown address because it is only one device. 0 timeouts, one ICMP sent and one received, 53.8 milliseconds.

The IP address that is alive is a vulnerability as the company wants all ports to be closed.

ICMP is a Network Layer (layer 3) protocol but ICMP messages are encapsulated in IP packets so most people would say that it’s a layer 4 protocol like UDP or TCP. But it is considered to be a layer 3 protocol.

Mitigation is to restrict the ip address that is alive.



**Phase 2: *"Some Syn for Nothin`"***

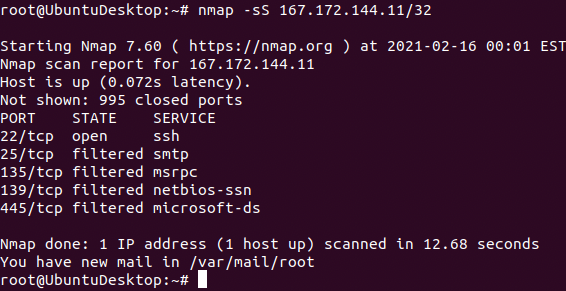
Summery:

The command use is nmap -sS 167.172.144.11/11

Port 22 SSH is opened which i think is associated to the hacker

Port 22 needs to be closed or filtered,the company needs to strengthen their password to force users to be changing their passwords.

SYNC SCAN is transport layer protocol (layer 4) as it is used to detect ports status.



**Phase 3: *"I Feel a DNS Change Comin' On"***

Summery:

Command use - ssh jimi@167.172.144.11 -p22, whoami,ls, cat, ctrl D, nslookup

Nslookup:167.172.144.11

My findings show that there is a DNS spoofing as the rollingstone IP address resolves to a different one, which means the hacker has changed the host file to his own address.

By mitigating this we need to close port 22, change the host file to the appropriate destination or the DNS server can be filtered.

SSH and nslookup are in Application layer (layer 7)

sysadmLn@LmntuDesktop: 
Edit View Search Terminal Help 
g a.) make changes to the master f tie tn /etc/cloud/templates/hosts.tmpl 
g b.) change or remove the value of tn 
letc/cloud/cloud.cfg or cloud-config from user-data 
e. 1.1 GTscavengerHunt.IocaIdomatn GTscavengerHunt 
127. 
127.e.e.1 localhost 
98.137.246.8 rolltngstone.com 
000000001 lowing lines are desirable for IPv6 capable hosts 
tp6-IocaIhost tp6-Ioopback 
feee::e tp6-IocaInet 
tp6-mcastpreftx 
ip6-aIInodes 
tp6-aIIrouters 
ip6-aIIhosts 
connection to 167.172.144.11 closed. 
nslookup 98.137.246.g 
sysadmtn@ubuntuoesktop: 
unknown.yahoo.com. 
name 
Authoritative answers can 
be found from: 
1 

**Phase 4: *"ShARP Dressed Man"***

In this finding I found the hacker notes in the host file that leads to a link that downloads the pcap file that shows the hacker message and duplicate IP

The hacker also changed the mac address that causes IP duplication

To mitigate this, we need to close or filter the port 22 and there should be strong authentication for all remote users and to be monitored with network monitoring tools.

Application layer (layer 7)

