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

Sudo apt install fping
fping 15.199.95.91
15.199.95.91 is unreachable
fping 15.199.94.91
15.199.94.91 is unreachable
fping 11.199.158.91
11.199.158.91 is unreachable
fping 167.172.144.11
167.172.144.11 is alive #Hollywood Application Servers
fping 11.99.141.91
11.99.141.91 is unreachable

OSI Layer | Network Layer

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

sudo nmap -sS 167.172.144.11

Starting Nmap 7.60 (https://nmap.org) at 2020-12-26 22:34 EST
Nmap scan report for 167.172.144.11
Host is up (0.0050s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
22/tcp open ssh

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds

OSI Layer | Transport Layer

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

ping rollingstone.com

PING rollingstone.com (151.101.192.69) 56(84) bytes of data.
64 bytes from 151.101.192.69 (151.101.192.69): icmp_seq=1 ttl=55 time=13.6 ms

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ **nslookup rollingstone.com**
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: rollingstone.com
Address: 151.101.64.69
Name: rollingstone.com
Address: 151.101.128.69
Name: rollingstone.com
Address: 151.101.192.69
Name: rollingstone.com
Address: 151.101.0.69

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ **nslookup 151.101.192.69**
** server can't find 69.192.101.151.in-addr.arpa: NXDOMAIN

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ **nslookup 151.101.128.69**
** server can't find 69.128.101.151.in-addr.arpa: NXDOMAIN

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ **nslookup 151.101.64.69**
** server can't find 69.64.101.151.in-addr.arpa: NXDOMAIN

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ **nslookup 151.101.0.69**
** server can't find 69.0.101.151.in-addr.arpa: NXDOMAIN

ssh jimi@167.172.144.11

yes

Hendrix

cat /etc/hosts

Your system has configured 'manage_etc_hosts' as True.
As a result, if you wish for changes to this file to persist
then you will need to either
a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
b.) change or remove the value of 'manage_etc_hosts' in
/etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com

ooooooooollowing lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

exit
nslookup 98.137.246.8
8.246.137.98.in-addr.arpa name =
media-router-fp72.prod.media.vip.gq1.yahoo.com.

Authoritative answers can be found from:

OSI Layer | Application Layer

Phase 4: *"ShARP Dressed Man"*

ssh jimi@167.172.144.11
yes
Hendrix

$ ls /bin |grep .txt
$ ls /etc |grep .txt
packetcaptureinfo.txt
$ cat /etc/packetcaptureinfo.txt
Captured Packets are here:
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing

#I downloaded the secretlog.pcapng file and opened with Wireshark.

Target/Hacker's MAC address: 00:0c:29:1d:b3:b1
Target/Hacker was on POST /formservice
104.18.126.89 was IP address

sysadmin@UbuntuDesktop:~/Documents/08-Networking_Fundamentals$ fping 104.18.126.89
104.18.126.89 is alive

-vulnerabilities discovered
sudo nmap -sS 104.18.126.89
PORT STATE SERVICE
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
8443/tcp open https-alt

OSI Layer | Data Link