Cybersecurity

Networking Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in. For each phase, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

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

1. Command(s) used to run `ping` against the IP ranges:

```
% ping -c 5 161.35.96.20
PING 161.35.96.20 (161.35.96.20): 56 data bytes
64 bytes from 161.35.96.20: icmp_seq=0 ttl=55 time=68.882 ms
64 bytes from 161.35.96.20: icmp_seq=1 ttl=55 time=69.740 ms
64 bytes from 161.35.96.20: icmp_seq=2 ttl=55 time=66.915 ms
64 bytes from 161.35.96.20: icmp_seq=3 ttl=55 time=69.667 ms
64 bytes from 161.35.96.20: icmp_seq=4 ttl=55 time=66.324 ms
--- 161.35.96.20 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 66.324/68.306/69.740/1.422 ms
```

2. Summarize the results of the `ping` command(s):

```
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 66.324/68.306/69.740/1.422 ms All packets that were transmitted were all received, not one lost.
```

3. List of IPs responding to echo requests:

```
fping -s -g  161.35.96.20/32
161.35.96.20 is unreachable
```

```
       1 targets
       0 alive
       1 unreachable
       0 unknown addresses

       1 timeouts (waiting for response)
       4 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received

 0.00 ms (min round trip time)
 0.00 ms (avg round trip time)
 0.00 ms (max round trip time)
        4.078 sec (elapsed real time)

Its unreachable and not alive
```

4. Explain which OSI layer(s) your findings involve:

```
Network layer
```

5. Mitigation recommendations (if needed):

```
To make sure that any ip address aren’t reachable and not responding to
pings because they can be susceptible to attacks such as dns hick jack and
ddos attacks. So have the any open ports close.
```

Phase 2: *“Some SYN for Nothin’”*

1. Which ports are open on the RockStar Corp server?

```
22/tcp   open     ssh
```

2. Which OSI layer do SYN scans run on?

    a. OSI layer:

```
Transport layer 4
```

b. Explain how you determined which layer:

Because the transports layer is responsible for transmitting data through transmission protocol TCP and UDP like clicking on an image or streaming a video or movie ex.youtube/hulu

3. Mitigation suggestions (if needed):

Close and secure the open 22/tcp in order to prevent and not give people the opportunity to ssh in the system.

Phase 3: *“I Feel a DNS Change Comin’ On”*

1. Summarize your findings about why access to rollingstone.com is not working as expected from the RockStar Corp Hollywood office:

The open port 22/tcp allowed a hacker to hack in and change the IP address

2. Command used to query Domain Name System records:

```
MacBook-Pro ~ %  nslookup 98.137.246.8
Server:          192.168.0.1
Address: 192.168.0.1#53
Non-authoritative answer:
8.246.137.98.in-addr.arpa name = unknown.yahoo.com.
Authoritative answers can be found from:
```

3. Domain name findings:

http://unknown.yahoo.com

4. Explain what OSI layer DNS runs on:

Layer 7 application

5. Mitigation suggestions (if needed):

```
Close and secure port 22/tcp to prevent hackers entering and altering IP
addresses. Utilize a DNS filter and revert the ip address to the suitable
address and set it to be unreachable.
```

Phase 4: *“ShARP Dressed Man”*

1. Name of file containing packets:

```
/etc/packetcaptureinfo.txt
 wget packetcaptureinfo.txt
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing

$ pwd
/
$ ls
bin   etc          initrd.img.old  lost+found  opt   run   sys  var
boot  home         lib              media       proc  sbin  tmp  vmlinuz
dev   initrd.img  lib64             mnt         root  srv   usr  vmlinuz.old
$ cd etc
$ ls
adduser.conf             gss               modules-load.d          rmt
alternatives             host.conf         motd                    rpc
apache2                  hostname  mtab                    rsyslog.conf
apparmor         hosts             mysql                   rsyslog.d
apparmor.d               hosts.allow       nanorc                  screenrc
apt                      hosts.deny        network         securetty
bash.bashrc              init              NetworkManager          security
bash_completion          init.d            networks                selinux
bash_completion.d        initramfs-tools  newt                     services
bindresvport.blacklist   inputrc           nscd.conf               shadow
binfmt.d         insserv.conf.d    nsswitch.conf           shadow-
ca-certificates          iproute2  ntp.conf                shadow_class
ca-certificates.conf     issue             opt                     shells
calendar         issue.net         os-release              skel
cloud                    joe               packetcaptureinfo.txt    ssh
cron.d                   kernel            pam.conf                ssl
cron.daily               ldap              pam.d                   staff-group-for-usr-local
cron.hourly              ld.so.cache       passwd                  subgid
cron.monthly             ld.so.conf        passwd-         subgid-
crontab                  ld.so.conf.d      perl                    subuid
cron.weekly              libaudit.conf     php                     subuid-
dbus-1                   locale.alias      profile         sudoers
debconf.conf             locale.gen        profile.d               sudoers.d
debian_version           localtime         protocols               sysctl.conf
default                  logcheck  python                  sysctl.d
deluser.conf             login.defs        python2.7               systemd
dhcp                     logrotate.conf    python3         terminfo
dpkg                     logrotate.d       python3.5               timezone
environment              machine-id        rc0.d                   tmpfiles.d
euca2ools                magic             rc1.d                   ucf.conf
fstab                    magic.mime        rc2.d                   udev
gai.conf         mailcap           rc3.d                   ufw
```

```
group                   mailcap.order     rc4.d                 update-motd.d
group-                  mime.types        rc5.d                 vim
grub.d                  mke2fs.conf       rc6.d                 wgetrc
gshadow                 modprobe.d        rcS.d                 X11
gshadow-         modules           resolv.conf             xdg
$ wget pa
--2023-10-01 22:44:49--  http://pa/
Resolving pa (pa)... failed: No address associated with hostname.
wget: unable to resolve host address ‘pa’
$ wget packetcaptureinfo.txt
--2023-10-01 22:44:59--  http://packetcaptureinfo.txt/
Resolving packetcaptureinfo.txt (packetcaptureinfo.txt)... failed: Name or service not known.
wget: unable to resolve host address ‘packetcaptureinfo.txt’
$ cat packetcaptureinfo.txt
My Captured Packets are Here:
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
```

2. ARP findings identifying the hacker’s MAC address:

```
 (00:0c:29:1d:b3:b1)
```

3. HTTP findings, including the message from the hacker:

```
http.request.method =="POST"
Packet number 16
16    2019-08-15 07:01:46.121459902 10.0.2.15   104.18.126.89     1876  HTTP

Under the HTML tab there's a message of him saying he's a hacker and his
name and email says hacker.

↓HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "0<text>" = "Mr Hacker"
Form item: "1<text>" = "Hacker@rockstarcorp.com"
Form item: "3<textarea>" = "Hi Got The Blues Corp!  This is a hacker that
works at Rock Star Corp.  Rock Star has left port 22, SSH open if you want
to hack in.  For 1 Milliion Dollars I will provide you the user and
password!"
```

4. Explain the OSI layers for HTTP and ARP.
    a. Layer used for HTTP:

```
Layer 7 Application
```

    b. Layer used for ARP:

```
Layer 2 Data Link
```

5. Mitigation suggestions (if needed):

```
Use stronger passwords and have 2 authentications.
Enforce password reset or change every month.
Make sure port 22 is close and secure.
```