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:

```
fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0

fping -c 3 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
```

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

```
fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
161.35.96.20 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
203.0.113.32 is unreachable
192.0.2.0 is unreachable

fping -c 3 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
161.35.96.20 : [0], 84 bytes, 75.5 ms (75.5 avg, 0% loss)
161.35.96.20 : [1], 84 bytes, 33.2 ms (54.4 avg, 0% loss)
161.35.96.20 : [2], 84 bytes, 36.1 ms (48.3 avg, 0% loss)

15.199.95.91 : xmt/rcv/%loss = 3/0/100%
15.199.94.91 : xmt/rcv/%loss = 3/0/100%
203.0.113.32 : xmt/rcv/%loss = 3/0/100%
```

```
161.35.96.20 : xmt/rcv/%loss = 3/3/0%, min/avg/max = 33.2/48.3/75.5
192.0.2.0    : xmt/rcv/%loss = 3/0/100%
```

3. List of IPs responding to echo requests:

```
The IP which responded to the echo request is 161.35.96.20
```

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

```
The findings involves Layer 3 - Network of the OSI Layer Model
```

5. Mitigation recommendations (if needed):

```
1) Installing Firewall: Firewall will filter and block ICMP related
   traffic which serves no real purpose in terms of network operation.
2) Rate limitation: To prevent the DoS attack, limiting the rate of
   implementation which will avoid causing ICMP flood attack.
3) Regular Updates: It is extremely important to keep the operating
   servers and network devices to stay up to date and in known of any
   security vulnerabilities.
4) Disabling ping echo responses: This can be implemented to all the
   servers which are not required to be pingable from external parties
   and their networks.
5) Network Monitoring Software: Installing these software will monitor
   and alert the security analyst of any unusual patterns.

Reference:
https://purplesec.us/prevent-ping-attacks/
```

Phase 2: *“Some SYN for Nothin’”*

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

```
Port 22
```

2. Which OSI layer do SYN scans run on?

a. OSI layer:

```
Layer 4 - Transport
```

b. Explain how you determined which layer:

```
The SYN runs a scan at Layer 4 using TCP (Transmission Control Protocol).
SYN sends TCP SYN packets to a network to know if and which of the ports are
open and is ready to establish a connection. TCP is a transport layer
protocol.
```

3. Mitigation suggestions (if needed):

1) **Intrusion Detection and Prevention System (IDPS):** This will monitor the network traffic. Will read and analyze any suspicious behavior pattern in order to prevent SYN scan attacks.
2) **Firewall:** The firewalls will block the SYN packets and incoming traffic from any and all suspicious unknown sources.
3) **TTL (Time to Live) value reduction:** The reduction in the TTL value for all the incoming packets will limit the packet from traveling multiple hops, which will prevent the attackers from executing a SYN scan successfully.
4) **Software updates:** By updating the software along with other operating systems to keep it up to date will assist in finding vulnerabilities within the system which may potentially exploit it to a SYN scan attack.
5) **Secured SSH file:** Making sure the employees of the company have no access to the SSH files and are unable to share the password. If for any reason an employee is required to access the file, they have to pass the two step authentication.

Reference:

https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/

https://www.techtarget.com/searchsecurity/definition/SYN-flooding

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 contents of the /etc/hosts file screenshot indicate that the IP address
"98.137.246.8" associated with rollingstone.com is incorrectly mapped to a
different domain name, leading to the redirection of Hollywood office users
to an unknown.yahoo.com page when attempting to access rollingstone.com.
```

```
$ cat 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 gtclass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtclass-1578758377314-s-1vcpu-1gb-nyc1-01
127.0.0.1 localhost
98.137.246.8 rollingstone.com

# The following 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
```

2. Command used to query Domain Name System records:

```
nslookup 98.137.246.8
```

3. Domain name findings:

```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa     name = unknown.yahoo.com.
```

4. Explain what OSI layer DNS runs on:

```
Layer 7 - Application
```

5. Mitigation suggestions (if needed):

1) **Monitor DNS traffic:** Monitoring DNS traffic regularly will assist in identifying better any suspicious behavior and tio mitigate any attacks.Additionall, it will also detect any performance flaws.
2) **Implement DNSSEC:** DNSSEC stands for DNS Security Extensions which establish a security layer using digital signature to authenticate DNS data and secure it against attacks like DNS spoofing.
3) **Firewall:** Firewall serves multiple purposes in securing a network from various attacks amongst one of those is DNS attack. Firewall will block suspicious incoming traffic from unknown IP which seems off.
4) **Secured admin access:** It is extremely important that no one other than the trusted admin person has access to the company's DNS. Also, to enable multi-factor authentication for everyone who needs to access the DNS records.
5) **Disable DNS recursion:** An enabled DNS recursion on your server will allow recursive queries to be made for other domains which are outside of the master zones location on the similar server's name. This feature permits third-party hosts to query the name servers at will.

Reference:
https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/
https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

```
packetcaptureinfo.txt
```

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

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

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

Hacker's Mac address - 00:0c:29:1d:b3:b1
Hacker began sending ARP request using IP - 192.168.47.171

GET: The hacker requested the MAC information for 192.168.47.1 and then for 192.168.47.200 and in then spoofed his own IP to be 192.168.47.200 as we can see an alert in the frame 5 indicating that the IP 192.168.47.200 is also in use by Mac address - 00:0c:29:1d:b3:b1 which will redirect the traffic to the hacker.

POST: Upon successful TCP connection with the servers, the hacker started the GET request by loading the following two URLs in sequence:
"//www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x663&colorDepth=24&flash=0&java=0&sitereferer=http%3A//www.gottheblues.yolasite.com/&visi"

"url=//www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x663&colorDepth=24&flash=0&java=0&sitereferer=http%3A//www.gottheb"

The hacker then POST the web application form from the following URL:
"http://forms.yola.com/formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195e3/"

IP use for POST request - 10.0.2.15
MAC address - 08:00:27:f8:42:a7

Which displayed the below message:

"Mr Hacker"
"Name"
"Hacker@rockstarcorp.com"
"Email"
"Phone"
"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!"
"Message"

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

Layer 7 - Application layer, it establishes a communication between the user and application.HTTP is used to make requests to a web browser using hypertext which will then process those requests to the web server.

b. Layer used for ARP:

Layer 2 - Data Link Layer,which transfers data across physical networks. ARP is used to link a network address such as IP address to a physical address, one of which is MAC address.

5. Mitigation suggestions (if needed):

HTTP

1) **Multi-factor authentication:** Establishing a high level of authentication will prevent the web resources from having unauthorized access.
2) **HTTPS implementation:** HTTPS will allow the client and the web server an encrypted and secured communications.
3) **Web application Firewall:**This will protect the network from malicious traffic by filtering and blocking it.
4) **Monitoring Server logs and web traffic:** This will alert of any potential security breach or unusual pattern.

ARP

1) **Installing IDS/IPS:** Intrusion Detection and Prevention System will filter the spoofing attacks and successfully block them as well.
2) **Regular Updates:** It is extremely important to keep the operating servers and network devices to stay up to date and in known of any security vulnerabilities.
3) **Network Isolation:** Isolating network systems containing sensitive information from all the less secured networks allowing extremely limited access with multi-factor authentication.

Reference:

https://www.siakabaro.com/10-tips-to-mihttps://www.siakabaro.com/10-tips-to-mitigate-http-flood-attacks/tigate-http-flood-attacks/
https://www.varonis.com/blog/arp-poisoning