



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:

```
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91
15.199.95.91 is unreachable
sysadmin@UbuntuDesktop:~$ fping 15.199.94.91
15.199.94.91 is unreachable
sysadmin@UbuntuDesktop:~$ fping 203.0.113.32
203.0.113.32 is unreachable
sysadmin@UbuntuDesktop:~$ fping 161.35.96.20
161.35.96.20 is alive
sysadmin@UbuntuDesktop:~$ fping 192.0.2.0
192.0.2.0 is unreachable
```

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

Used `fping` against all IPs for the Hollywood office and it returned only one as alive.

3. List of IPs responding to echo requests:

161.35.96.20

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

Networking layer

5. Mitigation recommendations (if needed):

Block connections to 161.35.96.20

Phase 2: “Some SYN for Nothin’”

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

```
sysadmin@UbuntuDesktop:~$ sudo nmap 161.35.96.20 -sS
[sudo] password for sysadmin:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-11 16:10 EDT
Nmap scan report for 161.35.96.20
Host is up (0.0057s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 6.06 seconds
```

2. Which OSI layer do SYN scans run on?

a. OSI layer:

Transport layer

b. Explain how you determined which layer:

Anything dealing with ports will be on the Transport layer.

3. Mitigation suggestions (if needed):

Suggest to use a filter or close port 22.

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:

I ssh’d into the RockStar server with the given credentials. Then, I previewed the /etc/host file to find the IP address associated with rollingstone.com. Then, I ran an nslookup on IP 98.137.246.8 and can conclude that RockStar server was redirected to yahoo.com.

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.

Authoritative answers can be found from:
```

4. Explain what OSI layer DNS runs on:

Application layer

5. Mitigation suggestions (if needed):

They need unique usernames and passwords for each server. Also, the host file should only be accessible to those with clearance.

Phase 4: “ShARP Dressed Man”

1. Name of file containing packets:

Inside /etc, there was a file called packetcaptureinfo.txt that contained the link to download the packet capture called secretlogs.pcapng.

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

arp						
Interface		Channel				
No.	Time	Source	Destination	Protocol	Length	Info
1	2014-01-06 17:56:26.340873	VMware_id:b3:b1	Broadcast	ARP	42	Who has 192.168.47.1? Tell 192.168.47.171
2	2014-01-06 17:56:26.340955	VMware_c0:00:08	VMware_id:b3:b1	ARP	60	192.168.47.1 is at 00:50:56:c0:00:08
3	2014-01-06 17:56:26.348782	VMware_id:b3:b1	Broadcast	ARP	42	Who has 192.168.47.200? Tell 192.168.47.171
4	2014-01-06 17:56:26.348860	VMware_0f:71:a3	VMware_id:b3:b1	ARP	60	192.168.47.200 is at 00:0c:29:0f:71:a3
5	2014-01-06 17:56:36.933972	VMware_id:b3:b1	VMware_fd:2f:16	ARP	42	192.168.47.200 is at 00:0c:29:1d:b3:b1

Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
Ethernet II, Src: VMware_id:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)
Address Resolution Protocol (reply)
Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)
Frame showing earlier use of IP address: 4
[Seconds since earlier frame seen: 10]

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

http						
Interface		Channel				
No.	Time	Source	Destination	Protocol	Length	Info
12	2019-08-15 08:59:59.725040880	10.0.2.15	104.18.127.89	HTTP	784	GET /loggingAgent/loggingAgent?url=/www.gottheblues.yolasite.com/&page=...
13	2019-08-15 08:59:59.799030923	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
14	2019-08-15 09:00:01.541084996	10.0.2.15	104.18.127.89	HTTP	821	GET /loggingAgent/loggingAgent?url=/www.gottheblues.yolasite.com/contact...
15	2019-08-15 09:00:01.578797396	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
16	2019-08-15 09:01:46.121459902	10.0.2.15	104.18.126.89	HTTP	1876	POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb6...
17	2019-08-15 09:01:46.812715977	104.18.126.89	10.0.2.15	HTTP	420	HTTP/1.1 303 See Other
18	2019-08-15 09:01:46.852028949	10.0.2.15	104.16.161.215	HTTP	684	GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP...
19	2019-08-15 09:01:46.964813536	104.16.161.215	10.0.2.15	HTTP	3655	Continuation
20	2019-08-15 09:01:47.007470665	10.0.2.15	104.16.161.215	HTTP	598	GET /.well-known/http-opportunistic HTTP/1.1

Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 104.18.126.89 (104.18.126.89)
Transmission Control Protocol, Src Port: 33546 (33546), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1820
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "0<text>" = "Mr Hacker"
Form item: "0<label>" = "Name"
Form item: "1<text>" = "Hacker@rockstarcorp.com"
Form item: "1<label>" = "Email"
Form item: "2<text>" = ""
Form item: "2<label>" = "Phone"
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. ..."
Form item: "3<label>" = "Message"
Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
Form item: "locale" = "en"
Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"
Form item: "form_name" = ""
Form item: "site_name" = "GottheBlues"
Form item: "wl_site" = "0"
Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX705wpny6VYZ_YSkG==:3gjpzPaByJLfcA2oue1FsQG6ZzGkhh31_G12mb5PGk=" "
Form item: "g-recaptcha-response" = "03A0LTBLQA9oZg2Lh3adsE0c70rYkMw1hwPof8XgnYIsZh8cz5TtLw18uDM2uV0ls6duzyYq2MTzsvHYzKda77dqzNUwpa6F5Tu6b9875yKU1wZHpFOQmV8070Tc...

4. Explain the OSI layers for HTTP and ARP.

a. Layer used for HTTP:

Application layer

b. Layer used for ARP:

DataLink layer

5. Mitigation suggestions (if needed):

They can start an investigation on the hacker's MAC Address.