

## Module 8 Challenge Instructions: Rocking your Network

You are hired by RockStar Corporation as a network security analyst.

- RockStar Corp recently built a new office in Hollywood, California. You are tasked with completing a **network vulnerability assessment** of the office.
- You will complete several steps to analyze the Hollywood network and then provide RockStar Corp a summary of your findings.
- RockStar Corp is also concerned that a malicious hacker may have infiltrated its Hollywood office. You will need to determine whether there is anything suspicious in your findings.

### Files Required

RockStar Corp has provided you with:

- A list of its network assets: [RockStar Corp Server List](#).
- The following instructions to scan its network.

### Instructions

**Follow the instructions to work through the four phases of the network assessment. As you work, take note of:**

- The steps and commands used to complete the tasks
- Any network vulnerabilities discovered
- Any findings associated with a hacker
- Recommended mitigation strategy
- The OSI layer(s) your findings involve

You will use your notes to answer the questions in this quiz.

**IMPORTANT:** Please review your answers carefully before submitting to ensure that they are free of spelling and spacing errors. Incorrect spelling or incorrect spacing syntax will be marked as incorrect answers.

### Topics Covered in This Assignment

- Subnetting
- CIDR
- IP addresses
- ping
- OSI model and its layers
- Protocols
- Ports
- Wireshark

- PCAP analysis
- DNS
- HTTP
- ARP
- SYN scan
- TCP
- nslookup
- Network vulnerability assessments
- Network vulnerability mitigation

### Network Vulnerability Assessment Instructions

Use your Web Lab virtual machine for this assignment.

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

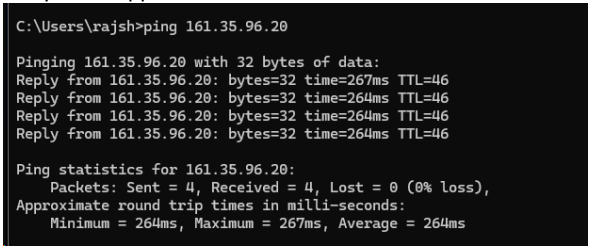
You have been provided a list of network assets belonging to RockStar Corp. Ping the network assets for only the Hollywood office.

- **Important:** You will need to run this one activity from your local machine, and NOT the web lab.
- Determine the IPs for the Hollywood office and run ping against the IP ranges in order to determine which IP(s) are accepting connections.
- RockStar Corp doesn't want any of its servers, even if they are up, to indicate that they are accepting connections.
  - Use ping <IP Address> and ignore any results that say, "Request timed out."
  - If any of the IP addresses send back a reply, press Ctrl+C to stop sending requests.
  - **Hint:** Try to ping a few IPs individually from your local desktop (outside of the web lab), such as:
    - 15.199.95.91
    - 15.199.94.91
    - 161.35.96.20

Take note of the relevant information for Phase 1, including the ping command(s) used, a summary of the results (including which IPs accept connections and which do not), and which OSI layer(s) your findings involve.

Summary of results: RockStar Corp server lists:

IP ADDRESS	LOCATION + SERVER TYPE	Response
12.205.151.91	New York Database Server	Request timed out.
15.199.151.91	New York Web Server 1	Request timed out.
15.199.158.91	New York Web Server 2	Request timed out.

15.199.141.91	New York Web Server 3	Request timed out.
15.199.131.91	New York Application Server 1	Request timed out.
15.199.121.91	New York Application Server 2	Request timed out.
15.199.111.91	Chicago Database Server	Request timed out.
15.199.100.91	Chicago Web Server 1	Request timed out.
15.199.99.91	Chicago Web Server 2	Request timed out.
15.199.98.91	Chicago Web Server 3	Request timed out.
15.199.97.91	Chicago Application Server 1	Request timed out.
15.199.96.91	Chicago Application Server 2	Request timed out.
15.199.95.91	Hollywood Database Server	Request timed out.
15.199.94.91	Hollywood Web Server 1	Request timed out.
203.0.113.32	Hollywood Web Server 2	Request timed out.
161.35.96.20	Hollywood Application Server 1 	Reply received; connection established.
192.0.2.0	Hollywood Application Server 2	Request timed out.
192.0.2.16	Miami Database Server	Request timed out.
198.51.100.0	Miami Web Server 1	Request timed out.
198.51.100.16	Miami Web Server 2	Request timed out.
198.51.100.32	Miami Web Server 3	Request timed out.
203.0.113.0	Miami Application Server	Request timed out.
203.0.113.16	Miami Database Server	Request timed out.

## Phase 2: *"Some SYN for Nothing"*

Using your findings from Phase 1, determine which ports are open.

- Run a SYN scan against the IP(s) accepting connections. Follow the instructions in the following **SYN Scan Instructions** section.
- Using the results of the SYN scan, determine which ports are accepting connections.

Fill out the relevant information for Phase 2 in your submission file.

### SYN Scan Instructions

## What is Nmap?

- **Nmap** is a free networking scanning tool available for Linux distributions.
- Security professionals use Nmap to determine what devices are running on a network and to find open ports to determine potential security vulnerabilities.
- Nmap has many capabilities and commands that can be run. Refer to this [Nmap cheat sheet](#) for reference.

For this activity, we will specifically focus on Nmap's ability to run a SYN scan.

- You already know that a SYN scan is an automated method to check for the states of ports on a network. Nmap is simply a tool that can automate this task.

To run a SYN scan:

- Open the terminal within your Linux machine.
- Use the following command to run a SYN scan:
  - `nmap -sS <IP Address>`
  - For example, if you want to run a SYN scan against the server IP 74.207.244.221, run `nmap -sS 74.207.244.221` and press Enter.
  - This will scan the most common 1000 ports.
- After this runs for several minutes, it should return a result similar to the following that depicts the state of the ports on that server:
- Starting Nmap 7.70 (<https://nmap.org>) at 2019-08-14 11:51 EDT
- Nmap scan report for li86-221.members.linode.com (74.207.244.221)
- Host is up (1.4s latency).
- Not shown: 988 closed ports
- PORT STATE SERVICE
- 22/tcp open ssh
- 25/tcp filtered smtp
- 110/tcp open pop3
- 113/tcp filtered ident
- 135/tcp filtered msrpc
- 139/tcp filtered netbios-ssn
- 143/tcp open imap
- 445/tcp filtered microsoft-ds
- 465/tcp open smtps
- 587/tcp open submission
- 993/tcp open imaps
- 995/tcp open pop3s

The results show the port number, TCP, or UDP, the state of the port, and the service or protocol for the ports that are either open or filtered (i.e., stopped by a firewall).

Closed ports are not shown, as indicated on the line Not shown: 988 closed ports.

For this exercise, document in your submission file which ports are open on the RockStar Corp server and which OSI layer SYN scans run on.

```

Host is up (0.21s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|  2048 65:20:61:5f:12:21:31:df:03:d9:b8:41:0c:6e:7c:6e (RSA)
|  256 ea:62:fe:2f:f1:7c:49:3c:74:33:db:c0:ad:aa:5a:42 (ECDSA)
|_  256 2e:ec:14:91:52:35:b3:d1:ce:88:89:34:37:a7:92:59 (ED25519)
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
593/tcp   filtered http-rpc-epmap
646/tcp   filtered ldap
4444/tcp  filtered krb524
Aggressive OS guesses: Linux 3.16 - 4.6 (95%), Linux 3.10 - 4.11 (94%), Linux 3.13 or 4.2 (94%), Linux 4.2 (94%), Linux 4.4 (94%), HP
P2000 G3 NAS device (93%), Linux 3.13 (93%), Linux 3.2 - 4.9 (93%), Linux 3.18 (93%), Linux 3.16 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 117.238 days (since Sat 201Dec 23 03:35:10 2023)
Network Distance: 21 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

TRACEROUTE (using port 1720/tcp)
HOP RTT      ADDRESS
1  7.00 ms  192.168.1.1
2  9.00 ms  10.61-134-203.dynamic.dsl.pth.iprimus.net.au (203.134.61.10)
3  9.00 ms  58.61-134-203.dynamic.dsl.pth.iprimus.net.au (203.134.61.58)
4  10.00 ms be102-99.bdr02.per05.wa.vocus.network (114.31.207.208)
5  ... 6
7  200.00 ms be803.lsr01.dody.nsw.vocus.network (103.1.76.146)
8  ...
9  201.00 ms be202.bdr03.sjc01.ca.us.vocus.network (114.31.199.43)
10 203.00 ms e0-1.core3.sjc1.he.net (64.71.184.45)
11 211.00 ms port-channel5.core4.sjc2.he.net (184.105.65.114)
12 ... 13
14 264.00 ms port-channel5.core1.nyc6.he.net (184.104.198.154)
15 ... 20
21 265.00 ms 161.35.96.20

```

```

NSE: Script Post-scanning.
Initiating NSE at 09:17
Completed NSE at 09:17, 0.00s elapsed
Initiating NSE at 09:17
Completed NSE at 09:17, 0.00s elapsed
Initiating NSE at 09:17
Completed NSE at 09:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.91 seconds
Raw packets sent: 1111 (50.576KB) | Rcvd: 1071 (45.096KB)

Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-18 11:27 W. Australia Standard Time
Nmap scan report for 161.35.96.20
Host is up (0.31s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
593/tcp   filtered http-rpc-epmap
646/tcp   filtered ldap
4444/tcp  filtered krb524

Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds

```

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

Using your findings from Phase 2, determine whether you can access the server(s) that accept connections.

- RockStar Corp typically uses the same default username and password for most of its servers, so try this first:
  - Username: jimi
  - Password: hendrix
- Try to figure out which port or service is used for remote system administration. Then, using these credentials, attempt to log in to the IP(s) that responded to pings in **Phase 1**.

RockStar Corp recently reported that it is unable to access rollingstone.com in the Hollywood office. Sometimes when they try to access the website, a different, unusual website comes up.

- While logged into the RockStar server from the previous step, determine whether something was modified on this system that affects viewing rollingstone.com in the browser. When you successfully find the configuration file, record the entry that is set to rollingstone.com.
- Terminate your SSH session to the rollingstone.com server, and use nslookup to determine the real domain of the IP address that you found in the previous step.

**Note :** nslookup is a command-line utility that can work in Windows or Linux systems. It is designed to query Domain Name System records. You can use PowerShell or MacOS/Linux terminal to run nslookup.

- To run nslookup, enter the following on the command line:

nslookup <IP Address> to find the domain associated to an IP address

OR

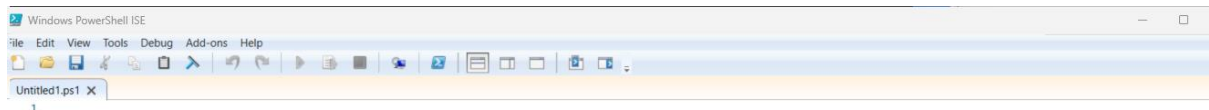
nslookup <domain name> to find the IP address associated to a domain

- You'll know you've found the right domain if it begins with unknown.

Add your findings to your submission file.

```
C:\Users\rajsh>nslookup rollingstone.com
Server:    UnKnown
Address:   fe80::1

Non-authoritative answer:
Name:      rollingstone.com
Address:   192.0.66.114
```



```
PS C:\Users\rajsh> nslookup 161.35.96.20
nslookup : *** Unknown can't find 161.35.96.20: Non-existent domain
At line:1 char:1
+ nslookup 161.35.96.20
+ ~~~~~
+ CategoryInfo          : NotSpecified: (*** Unknown can...existent domain:String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

Server:    UnKnown
Address:   fe80::1

PS C:\Users\rajsh>
```

A screenshot of an OpenSSH SSH client window titled "Select OpenSSH SSH client". The window shows a terminal session using the GNU nano 2.7.4 editor to edit the /etc/hosts file. The terminal output is as follows:

```
GNU nano 2.7.4 File: 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.tpl
# 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 gtc1ass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtc1ass-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
```

Phase 4: "ShARP Dressed Man"

Within the RockStar server that you SSH'd into and in the same directory as the configuration file from Phase 3, the hacker left a note about where they stored some packet captures.

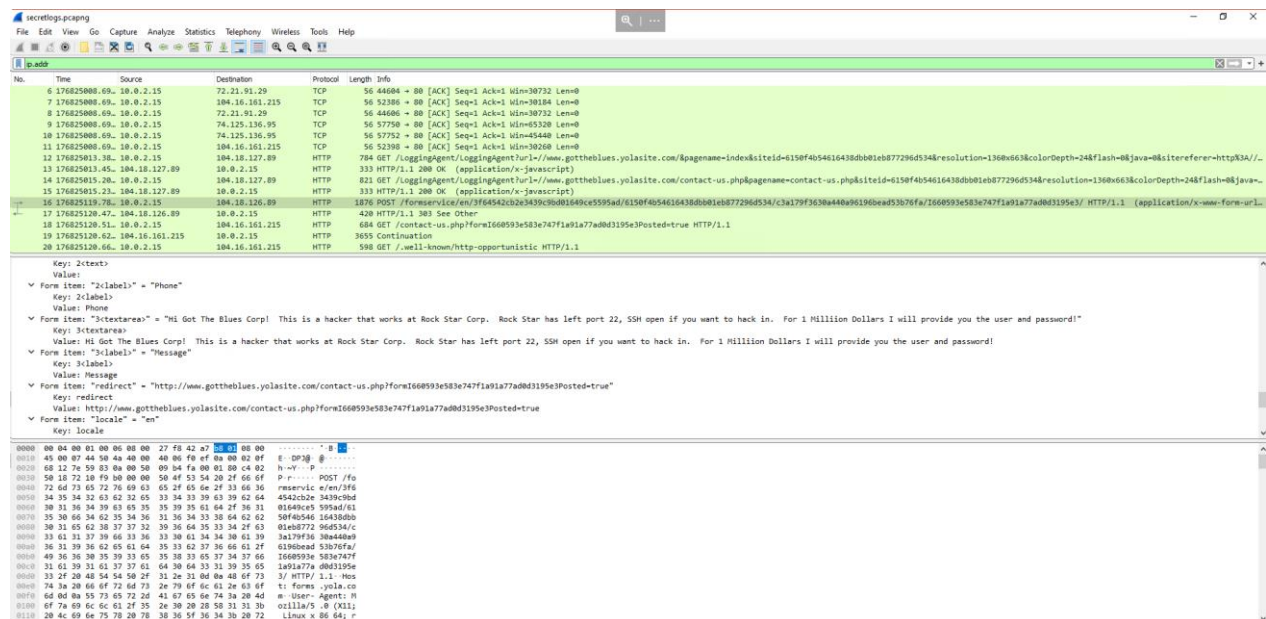
- View the file to find out where to recover the packet captures.

```
drwxr-xr-x 2 root root 4096 May 15 2019 opt
lrwxrwxrwx 1 root root 21 Sep 8 2019 os-release -> ../usr/lib/os-release
-rw-r--r-- 1 root root 115 Aug 15 2019 packetcaptureinfo.txt
-rw-r--r-- 1 root root 12288 Aug 15 2019 .packetcaptureinfo.txt.swp
-rw-r--r-- 1 root root 552 May 27 2017 pam.conf
drwxr-xr-x 2 root root 4096 Sep 17 2019 pam.d
-rw-r--r-- 1 640 root 1610 May 5 2022 passwd
```

- These packets were captured from the activity in the Hollywood office.

```
My Captured Packets are Here:
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71e1TkH3eF/view?usp=sharing
```

- Use Wireshark to analyze this PCAP file and determine whether there was any suspicious activity that could be attributed to a hacker.
- Record and identify your findings (e.g., OSI layers, protocols, IP addresses, and MAC addresses).



**Hint:** Focus on the ARP and HTTP protocols. Recall the different types of HTTP request methods and be sure to thoroughly examine the contents of these packets.

