Collaborative Learning Discussion 2

We (Group2) have performed several scanning processes on the Amazon Web Services (AWS) server provided by the opposite team (Group3). We have tried many of the standard tools used for network scanning to understand the network topology. The results returned by each tool are explained below.

First, we used **NSLOOKUP** to find the server's IP from the URL provided.

```
                                              kali@kali: ~
File  Actions  Edit  View  Help
  ┌──(kali㊉kali)-[~]
  └─$ nslookup nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
Server:          192.168.109.2
Address:         192.168.109.2#53

Non-authoritative answer:
Name:    nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
Address: 35.175.70.228


  ┌──(kali㊉kali)-[~]
  └─$
```

WHOIS was used to find out the ownership of the IP address. This tool allows users to query the details for an IP that is registered to the American Registry for Internet Numbers (ARIN, n.d.).

```
  ┌──(kali㊉kali)-[~]
  └─$ whois 35.175.70.228

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       35.152.0.0 - 35.183.255.255
CIDR:           35.152.0.0/13, 35.160.0.0/12, 35.176.0.0/13
NetName:        AT-88-Z
NetHandle:      NET-35-152-0-0-1
Parent:         NET35 (NET-35-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2016-08-09
Updated:        2016-08-09
Ref:            https://rdap.arin.net/registry/ip/35.152.0.0


OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2020-03-31
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will be unable to identify the correct owner of the
IP address at that point in time.
Ref:            https://rdap.arin.net/registry/entity/AT-88-Z


OrgRoutingHandle: ADR29-ARIN
```

Traceroute works by sending Internet Control Message Protocol (ICMP) packets to the destination system. The ICMP packets provide information about whether every router involved in the transfer gets these packets (Fortinet, n.d.). For the test exercise, first, we checked if the destination system responds to ICMP packets.

```
  ┌──(kali㊉kali)-[~]
  └─$ sudo nmap -T4 -sO  nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 17:03 EDT
Nmap scan report for nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com (35.175.70.228)
Host is up (0.0040s latency).
rDNS record for 35.175.70.228: ec2-35-175-70-228.compute-1.amazonaws.com
Not shown: 254 open|filtered protocols
PROTOCOL STATE SERVICE
1        open  icmp   ⟸
6        open  tcp

Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
```

Then we used **tracert** to evaluate the details about the hops traversed while reaching the destination server. It took 20 Hops to reach the server. Intermediate hops responded with

Request Timed Out, which suggests that ICMP packets are disabled between those hops. The last hop confirms that the trace-route requests were responded to by the destination server.

```
C:\Users\chawlav>tracert   35.175.70.228

Tracing route to ec2-35-175-70-228.compute-1.amazonaws.com [35.175.70.228]
over a maximum of 30 hops:

  1     4 ms     4 ms     4 ms  192.168.0.1
  2    16 ms    13 ms    16 ms  10.53.39.157
  3    17 ms    17 ms    16 ms  winn-core-2a-xe-121-0.network.virginmedia.net [62.253.123.158]
  4     *        *        *     Request timed out.
  5    36 ms    27 ms    24 ms  m686-mp2.cvx1-b.lis.dial.ntli.net [62.254.42.174]
  6     *        *        *     Request timed out.
  7    94 ms    93 ms    93 ms  us-nyc01b-rd2-ae-9-0.aorta.net [84.116.140.170]
  8   120 ms   103 ms   105 ms  us-was03a-ri1-ae-10-0.aorta.net [84.116.130.174]
  9   100 ms   102 ms   110 ms  99.82.183.148
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   103 ms   101 ms   103 ms  52.93.28.206
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20   106 ms   108 ms   108 ms  ec2-35-175-70-228.compute-1.amazonaws.com [35.175.70.228]

Trace complete.
```

Nmap is an open-source tool used to scan available hosts on the network, the services they offer, the OS on which they are operating and the firewall that they are currently using (NMAP, n.d.). As seen below, the tests performed on the provided AWS server show that the only ports found open were the ones we expected for, i.e., ports 80 (HTTP) and 22 (SSH). Unfortunately, the Apache server version couldn't be revealed, perhaps because of some security measures.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -A -T5 35.175.70.228
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 16:32 EDT
Nmap scan report for ec2-35-175-70-228.compute-1.amazonaws.com (35.175.70.228)
Host is up (0.14s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 8a:1c:38:8b:0e:2e:dd:29:a9:77:19:eb:2f:12:59:5d (RSA)
|   256 a5:c2:c7:4f:f5:9c:4c:1f:ec:f9:18:38:dc:04:38:94 (ECDSA)
|_  256 ab:0d:f6:d7:56:e5:ad:f9:89:cd:69:eb:00:56:d3:95 (ED25519)
80/tcp open  http    Apache
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.20 seconds
```

```
┌──(kali⊗kali)-[~/Desktop]
└─$ nmap -sV -sC 35.175.70.228

Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 16:33 EDT
Nmap scan report for ec2-35-175-70-228.compute-1.amazonaws.com (35.175.70.228)
Host is up (0.14s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.10 seconds

┌──(kali⊗kali)-[~/Desktop]
└─$ |
```

As TCP protocol works on 3-way handshake; the handshake is initiated by the client using TCP SYN. We generated TCP SYN for each port (1 - 65535) towards the destination server using **NPING** *"nping -tcp-connect nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com -p1-65535 -c 1"*, and found out that out of all the attempts only 3 ports responded. An interesting note worth mentioning is the fact that the port 443 (HTTPS) was spotted only by using TCP SYN scan and not nmap tool.

22 - SSH (Connection Established)

```
┌──(kali⊗kali)-[~]
└─$ nping -tcp-connect nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com -p22 -c 3

Starting Nping 0.7.91 ( https://nmap.org/nping ) at 2021-06-07 16:53 EDT
SENT (0.0356s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22)
RCVD (0.1450s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22) completed
SENT (1.0476s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22)
RCVD (1.1671s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22) completed
SENT (2.0522s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22)
RCVD (2.1737s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:22 (35.175.70.228:22) completed

Max rtt: 121.524ms | Min rtt: 115.348ms | Avg rtt: 118.788ms
TCP connection attempts: 3 | Successful connections: 3 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.17 seconds
```

80 - HTTP (Connection Established)

```
┌──(kali⊗kali)-[~]
└─$ nping -tcp-connect nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com -p80 -c 3

Starting Nping 0.7.91 ( https://nmap.org/nping ) at 2021-06-07 16:53 EDT
SENT (0.0292s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80)
RCVD (0.1498s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80) completed
SENT (1.0342s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80)
RCVD (1.1491s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80) completed
SENT (2.0381s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80)
RCVD (2.1450s) Handshake with nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:80 (35.175.70.228:80) completed

Max rtt: 120.576ms | Min rtt: 106.838ms | Avg rtt: 113.984ms
TCP connection attempts: 3 | Successful connections: 3 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 2.15 seconds
```

443 - HTTPS (responded with RST)

```
┌──(kali㉿kali)-[~]
└─$ nping -tcp-connect nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com -p443 -c 3

Starting Nping 0.7.91 ( https://nmap.org/nping ) at 2021-06-07 16:53 EDT
SENT (0.0301s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:443 (35.175.70.228:443)
SENT (1.0329s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:443 (35.175.70.228:443)
SENT (2.0369s) Starting TCP Handshake > nismphp-env.eba-wj5kp8st.us-east-1.elasticbeanstalk.com:443 (35.175.70.228:443)
RCVD (2.6117s) Possible TCP RST received from 35.175.70.228:443 ⟶ Connection refused

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
TCP connection attempts: 3 | Successful connections: 0 | Failed: 3 (100.00%)
Nping done: 1 IP address pinged in 3.04 seconds
```

References:
NMAP (n.d.). Nmap. Available at: https://nmap.org/ [Accessed 7 June 2021].

Fortinet (n.d.). What is Traceroute and How Does It Work?. Available at: https://www.fortinet.com/resources/cyberglossary/traceroutes [Accessed 7 June 2021].

ARIN (n.d.). Using Whois. Available at: https://www.arin.net/resources/registry/whois/ [Accessed 7 June 2021].