

Like adversaries start collecting information to identify the target in the reconnaissance phase of the Cyber-Kill chain model(Liu et al., 2020), penetration testing activities often start gathering relevant information using available tools in the market or commands to scan the target website. As indicated in the Unit 3 instructions, hereafter is the list of commands used in this post:

- **Ping** checks if the remote host is responding using ICMP protocols (Fasthosts, N.D.);
- **Traceroute** traces the path to the destination, which displays the area of a problem if there is any;
- **NSlookup** shows information about the domain, including MX records and domain nameservers;
- **Dig** works the same as NSlookup but for Linux-based operating systems;
- **Whois** checks the validity of the domain and provides DNS information; and
- **Nmap** checks if any ports are open.

Those tools provided us with solid insights on the server, including how many hops passed, nameserver details, contacts, MX records, and hosting location.

Group 2 built an e-health website with the IP 18.220.182.24 and the host nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com. As capture 1 and 2 shows that ping does not reach them and nmap tells only 80/tcp is open, the security group of Group 2 is assumed to allow only the HTTP port opened.

```
[kameyamashoudainoMacBook:Downloads shota$ ping 18.220.182.24
PING 18.220.182.24 (18.220.182.24): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
^C
--- 18.220.182.24 ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
[kameyamashoudainoMacBook:Downloads shota$ ping nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com
PING nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com (18.220.182.24): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
^C
--- nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
```

Capture 1: Ping IP and Host

```

[kameyamashoudainoMacBook:Downloads shota$ nmap -F 18.220.182.24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-05 01:19 JST
Nmap scan report for ec2-18-220-182-24.us-east-2.compute.amazonaws.com (18.220.182.24)
Host is up (0.15s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    closed smtp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
[kameyamashoudainoMacBook:Downloads shota$ nmap -F nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-05 01:19 JST
Nmap scan report for nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com (18.220.182.24)
Host is up (0.15s latency).
rDNS record for 18.220.182.24: ec2-18-220-182-24.us-east-2.compute.amazonaws.com
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 15.00 seconds

```

## Capture 2: Nmap IP and Host

As capture 3 shows below, traceroute has 64 hops with the most significant delay, 155.417 ms on average, at step 17.

```

kameyamashoudainoMacBook:Downloads shota$ traceroute nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
traceroute to nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com (18.220.182.24), 64 hops max, 52 byte packets
 1 192.168.100.1 (192.168.100.1) 7.695 ms 5.854 ms 5.726 ms
 2 softbank219188230013.bbtec.net (219.188.230.13) 6.202 ms 5.884 ms 5.423 ms
 3 softbank221110231237.bbtec.net (221.110.231.237) 8.635 ms 7.592 ms 7.505 ms
 4 10.0.61.149 (10.0.61.149) 7.395 ms 11.465 ms 8.615 ms
 5 10.0.60.105 (10.0.60.105) 7.224 ms 8.821 ms 8.454 ms
 6 10.9.201.18 (10.9.201.18) 100.187 ms 99.789 ms 99.956 ms
 7 softbank221111203138.bbtec.net (221.111.203.138) 99.456 ms 99.517 ms 101.024 ms
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * 52.95.1.174 (52.95.1.174) 159.458 ms 151.376 ms
18 52.95.1.103 (52.95.1.103) 152.476 ms
19 52.95.2.47 (52.95.2.47) 150.439 ms
20 52.95.2.15 (52.95.2.15) 153.085 ms
21 52.95.1.214 (52.95.1.214) 151.669 ms 153.778 ms
22 52.95.1.106 (52.95.1.106) 157.921 ms
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
31 18.220.182.24: 56 data bytes
32 * * *
33 * * *
34 * * *
35 * * *
36 * * *
37 * * *
38 * * *
39 * * *
40 * * *
41 * * *
42 * * *
43 * * *
44 * * *
45 * * *
46 * * *
47 * * *
48 nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
49 18.220.182.24
50 nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com (18.220.182.24)
51 * * *
52 * * *
53 * * *
54 * * *
55 * * *
56 * * *
57 * * *
58 * * *
59 * * *
60 * * *
61 * * *
62 * * *
63 * * *
64 * * *

```

Capture 3: Traceroute

Capture 4 shows the main nameservers, ns-825.awsdns-39.net, for the website.  
 Capture 5 shows that there is no MX record for the server.

```

kameyamashoudainoMacBook:Downloads shota$ nslookup
> set querytype=soa
> nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
*** Can't find nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com: No answer
; com (18.220.182.24): 56 data bytes

Authoritative answers can be found from:
us-east-2.elasticbeanstalk.com
      origin = ns-825.awsdns-39.net
      mail addr = awsdns-hostmaster.amazon.com
      serial = 1
      refresh = 7200
      retry = 900
      expire = 1209600
      minimum = 86400
> exit

kameyamashoudainoMacBook:Downloads shota$ dig -t SOA nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com

; <> DiG 9.10.6 <> -t SOA nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 17881
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com. IN SOA

;; AUTHORITY SECTION:
us-east-2.elasticbeanstalk.com. 900 IN SOA      ns-825.awsdns-39.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Aug 26 00:29:08 JST 2021
;; MSG SIZE rcvd: 165

```

Capture 4: SOA record of the server using nslookup and dig.

```

kameyamashoudainoMacBook:~ shota$ nslookup
> set querytype=mx
> nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer: provided us with the IP 18.220.182.24 and the host nismphp-
*** Can't find nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com: No answer
env.eba-appmqfp.us-east-2.elasticbeanstalk.com. As capture 1 and 2
Authoritative answers can be found from:
us-east-2.elasticbeanstalk.com. 900 IN SOA      ns-825.awsdns-39.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
  origin = ns-825.awsdns-39.net
  mail addr = awsdns-hostmaster.amazon.com
  serial = 1
  refresh = 7200
  retry = 900
  expire = 1209600
  minimum = 86400
> exit

kameyamashoudainoMacBook:~ shota$ dig -t MX nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com +short
kameyamashoudainoMacBook:~ shota$ dig -t MX nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com

;; <>> DiG 9.10.6 <>> -t MX nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10017
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nismphp-env.eba-appmqfp.us-east-2.elasticbeanstalk.com. IN MX

;; AUTHORITY SECTION:
us-east-2.elasticbeanstalk.com. 900 IN SOA      ns-825.awsdns-39.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Sep 05 01:42:04 JST 2021
;; MSG SIZE rcvd: 165

```

Capture 5: MX record using nslookup and dig

Contact for the host domain is VeriSign Global Registry Services, see Capture 6, and the host location is Seattle, WA US, see Capture 7.

```

kameyamashoudainoMacBook:~ shota$ whois nismphp-env.eba-appmzqfp.us-east-2.elasticbeanstalk.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.verisign-grs.com

domain:      COM

organisation: VeriSign Global Registry Services
address:     12061 Bluemont Way
address:     Reston Virginia 20190
address:     United States

contact:     administrative
name:        Registry Customer Service
organisation: VeriSign Global Registry Services
address:     12061 Bluemont Way
address:     Reston Virginia 20190
address:     United States
phone:       +1 703 925-6999
fax-no:      +1 703 948 3978
e-mail:      info@verisign-grs.com

contact:     technical
name:        Registry Customer Service
organisation: VeriSign Global Registry Services
address:     12061 Bluemont Way
address:     Reston Virginia 20190
address:     United States
phone:       +1 703 925-6999
fax-no:      +1 703 948 3978
e-mail:      info@verisign-grs.com

nserver:     A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:     B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:     C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:     D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:     E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:     F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:     G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:     H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:     I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:     J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:     K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:     L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:     M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:    30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766

whois:       whois.verisign-grs.com

status:      ACTIVE
remarks:     Registration information: http://www.verisigninc.com

created:     1985-01-01
changed:     2017-10-05
source:      IANA

# whois.verisign-grs.com

No match for domain "NISMPHP-ENV.EBA-APPMZQFP.US-EAST-2.ELASTICBEANSTALK.COM".
>>> Last update of whois database: 2021-09-04T16:48:52Z <<<

```

Capture 6: whois host domain.

```

kameyamashoudainoMacBook:~ shota$ whois 18.220.182.24
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:          whois.arin.net

inetnum:        18.0.0.0 - 18.255.255.255
organisation:    Administered by ARIN
status:          LEGACY

whois:          whois.arin.net

changed:         1994-01
source:          IANA

# whois.arin.net

NetRange:       18.32.0.0 - 18.255.255.255
CIDR:           18.64.0.0/10, 18.32.0.0/11, 18.128.0.0/9
NetName:        AT-88-Z
NetHandle:      NET-18-32-0-0-1
Parent:         NET18 (NET-18-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        2019-10-07
Updated:        2021-02-10
Ref:            https://rdap.arin.net/registry/ip/18.32.0.0

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:        2021-07-28
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

OrgTechHandle:  ANO24-ARIN
OrgTechName:    Amazon EC2 Network Operations
OrgTechPhone:   +1-206-266-4064
OrgTechEmail:   amzn-noc-contact@amazon.com
OrgTechRef:     https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgAbuseHandle:  AEA8-ARIN
OrgAbuseName:    Amazon EC2 Abuse
OrgAbusePhone:   +1-206-266-4064
OrgAbuseEmail:   abuse@amazonaws.com
OrgAbuseRef:     https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName:   AWS RPKI Management POC
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-rpki-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgNOCHandle:    AAN01-ARIN
OrgNOCHandle:    Amazon AWS Network Operations
OrgNOCHandle:    +1-206-266-4064
OrgNOCHandle:    amzn-noc-contact@amazon.com
OrgNOCHandle:    https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:   IP Routing
OrgRoutingPhone:  +1-206-266-4064
OrgRoutingEmail:  aws-routing-poc@amazon.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/IPROU3-ARIN

```

Capture 7 whois IP.

Based on the information above, as Group 2 effectively reduced the attack surface by limiting the open port to 80, the security testing should focus on Web Application testing with a simple network scanning. There are several tools under consideration, including Dynamic application security testing (DAST). DAST tools test pre-defined attack scenarios and examining the web application response to malicious requests (Rangnau et al., 2020).