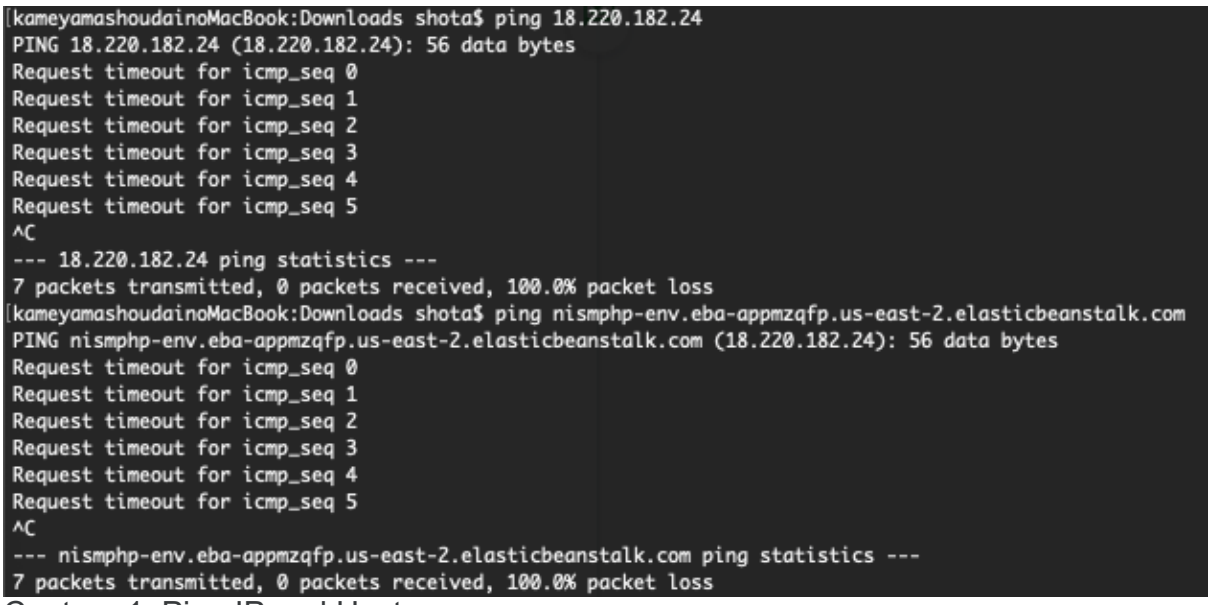
Like adversaries start collecting information to identify the target in the reconnaissance phase of the Cyber-Kill chain model(Liu et al., 2020), penetration testing activities often start gathering relevant information using available tools in the market or commands to scan the target website. As indicated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

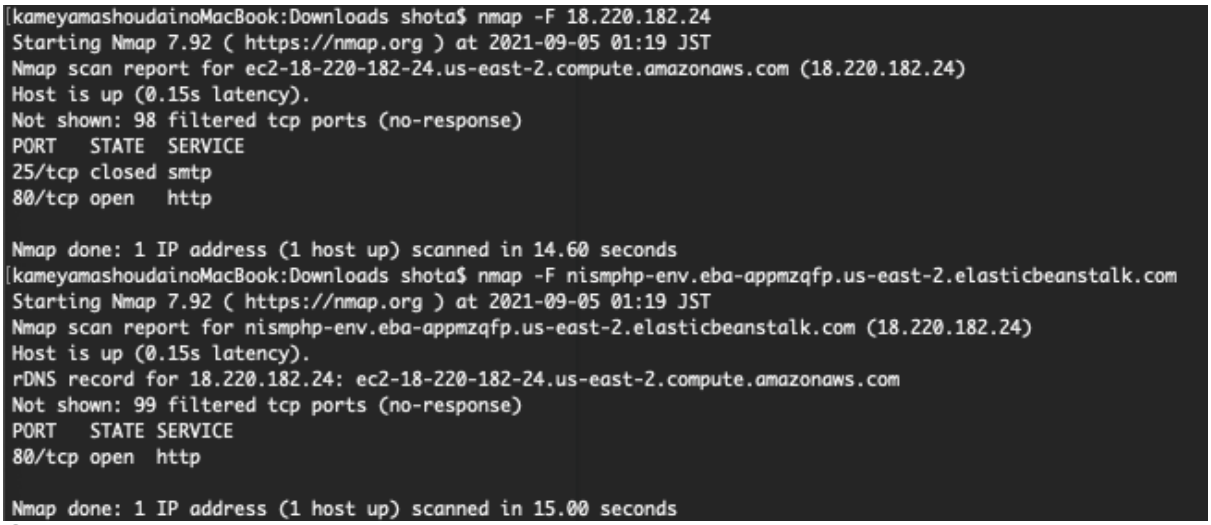
- **Ping** checks if the remote host is responding using ICMP protocols (Fasthosts, N.D.);
- **Traceroute** traces the path to the destination, which displays the area of a problem if there is any;
- **NSlookup** shows information about the domain, including MX records and domain nameservers;
- **Dig** 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.

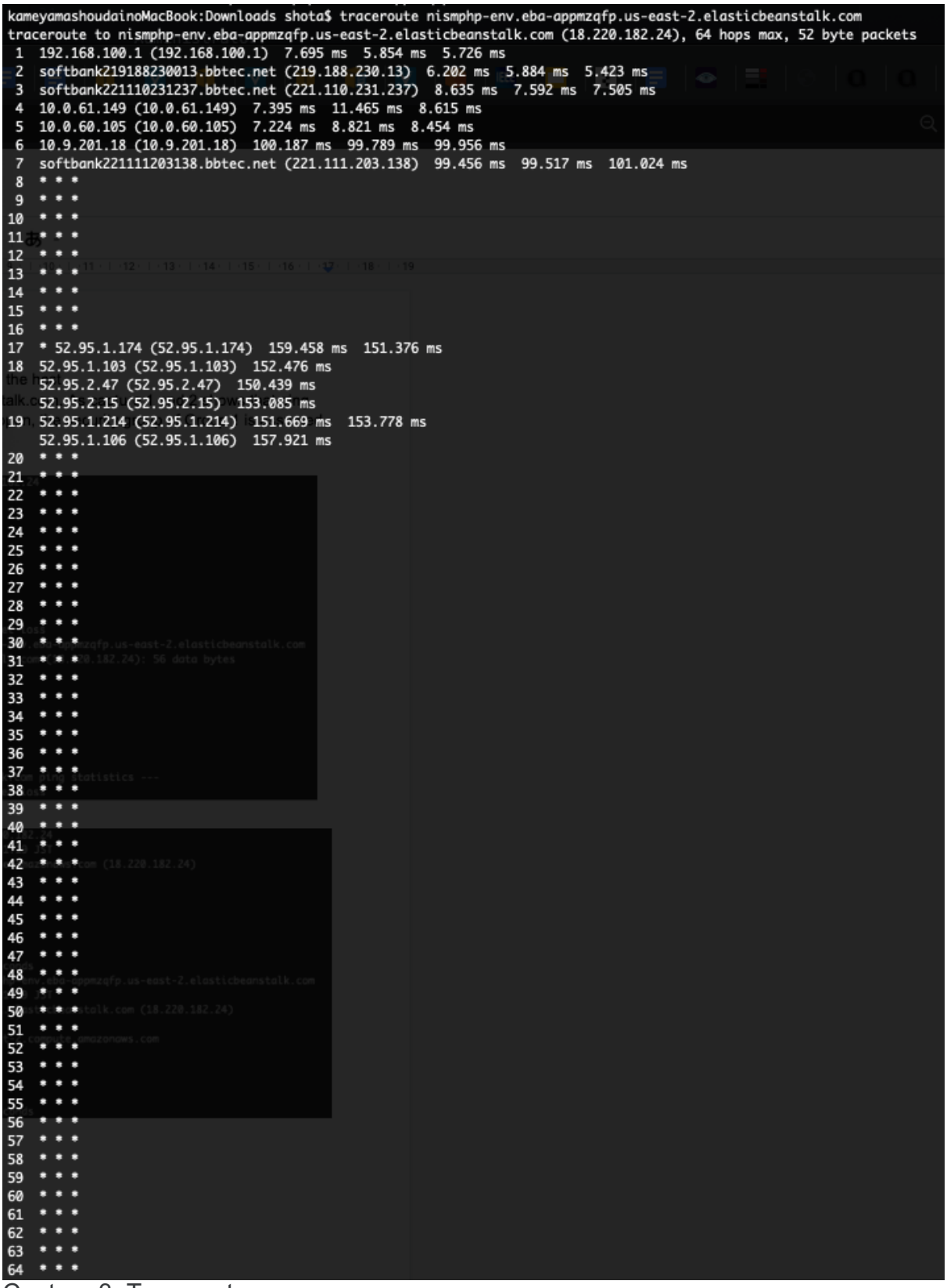


Capture 1: Ping IP and Host



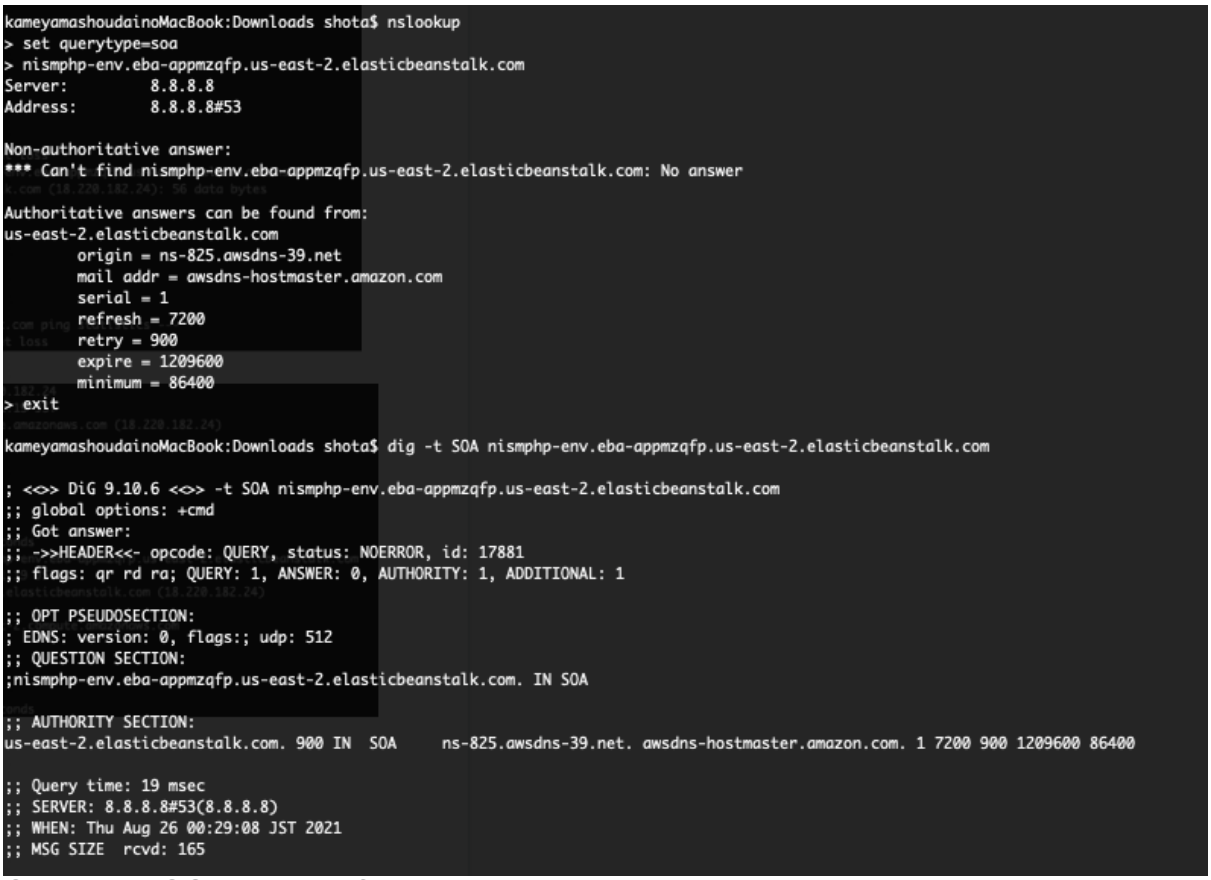
Capture 2: Nmap IP and Host

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

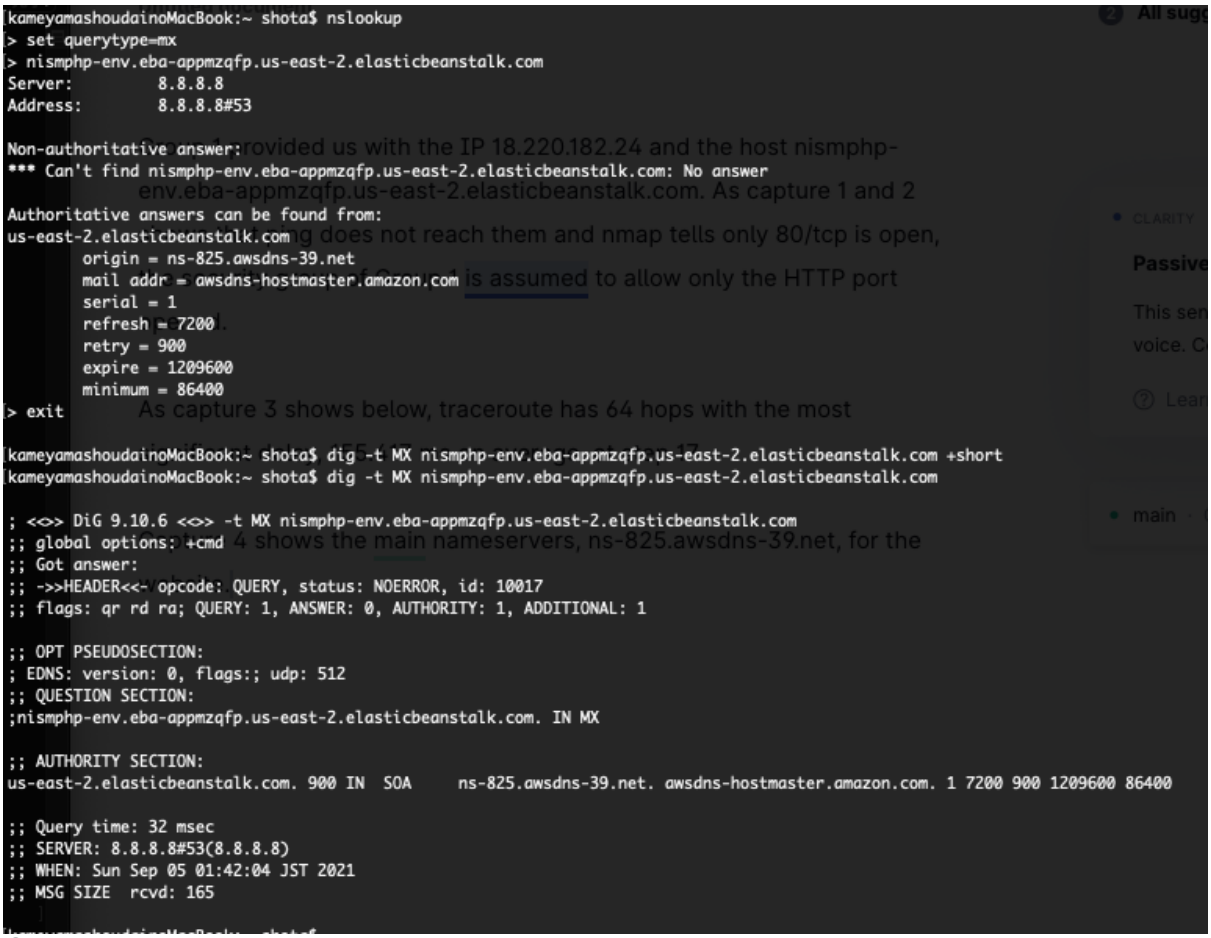


Capture 3: Traceroute

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.



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

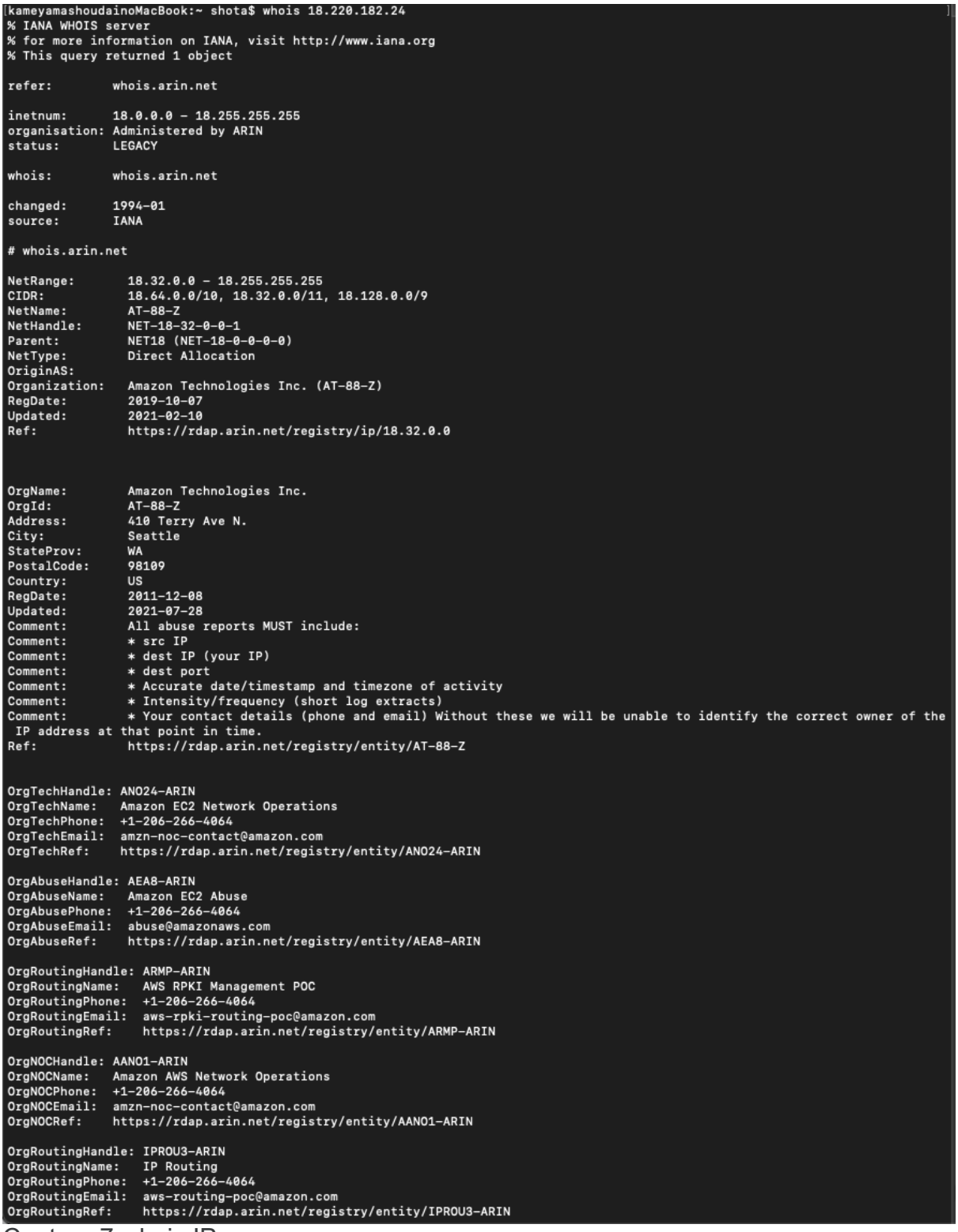


Capture 5: MX record using nslookup and dig

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.



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).