University of Essex | Online

Unit 3 – Practical and Team Activity

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: Practical and Team Activity (Unit 3)

Date: Sunday 29th August 2021

Activity Brief:

Perform a basic scan using standard tools such as ping, traceroute, dig and nslookup. Use these basic tools to compile a list that details the following information:

- How many hops from your machine to your assigned website?
- Which step causes the biggest delay in the route? What is the average duration of that delay?
- What are the main nameservers for the website?
- Who is the registered contact?
- What is the MX record for the website?
- Where is the website hosted?

Discuss the results of your scans and answer the following questions.

- Did you have any issues or challenges with the scans?
- How did you overcome them?
- How will they affect your final report?

Basic Scan Outcomes:

Preface:

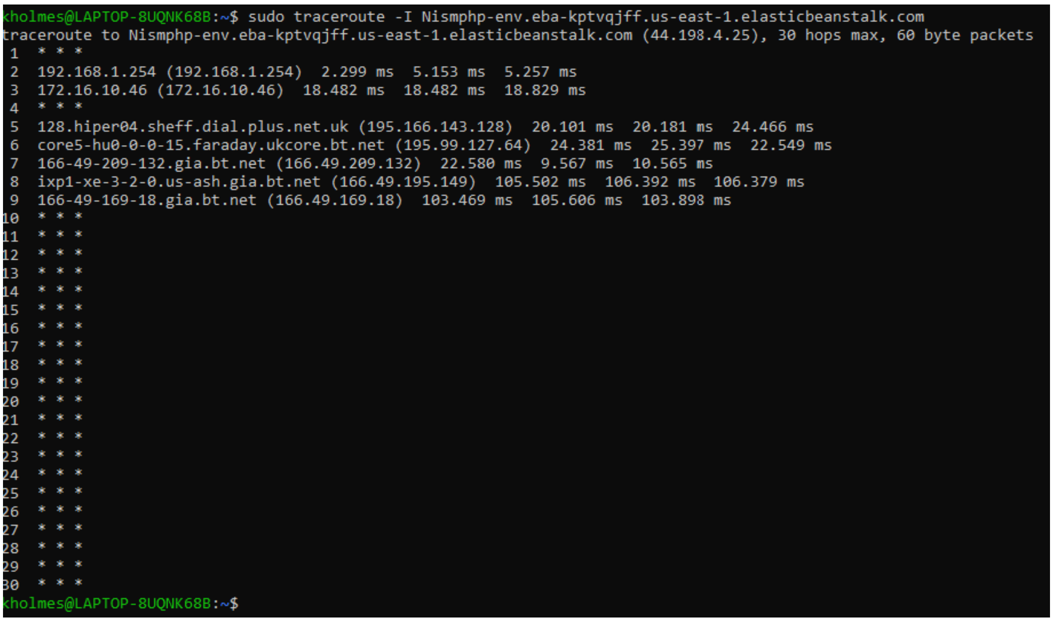
As the domain provided is a subdomain for the elasticbeanstalk.com domain, this value has been substituted when performing high-level MX and whois lookups. Google Public DNS (8.8.8.8) has been used for all DIG queries below.

Number of hops:

Command:

traceroute -I Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com

Result:



```
kholmes@LAPTOP-8UQNK68B:~$ sudo traceroute -I Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com
traceroute to Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com (44.198.4.25), 30 hops max, 60 byte packets
 1  * * *
 2  192.168.1.254 (192.168.1.254)  2.299 ms  5.153 ms  5.257 ms
 3  172.16.10.46 (172.16.10.46)  18.482 ms  18.482 ms  18.829 ms
 4  * * *
 5  128.hiper04.sheff.dial.plus.net.uk (195.166.143.128)  20.101 ms  20.181 ms  24.466 ms
 6  core5-hu0-0-0-15.faraday.ukcore.bt.net (195.99.127.64)  24.381 ms  25.397 ms  22.549 ms
 7  166-49-209-132.gia.bt.net (166.49.209.132)  22.580 ms  9.567 ms  10.565 ms
 8  ixp1-xe-3-2-0.us-ash.gia.bt.net (166.49.195.149)  105.502 ms  106.392 ms  106.379 ms
 9  166-49-169-18.gia.bt.net (166.49.169.18)  103.469 ms  105.606 ms  103.898 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
kholmes@LAPTOP-8UQNK68B:~$
```

A series of ‘hops’ did not respond to the tracert query.

I

Step with the largest delay:

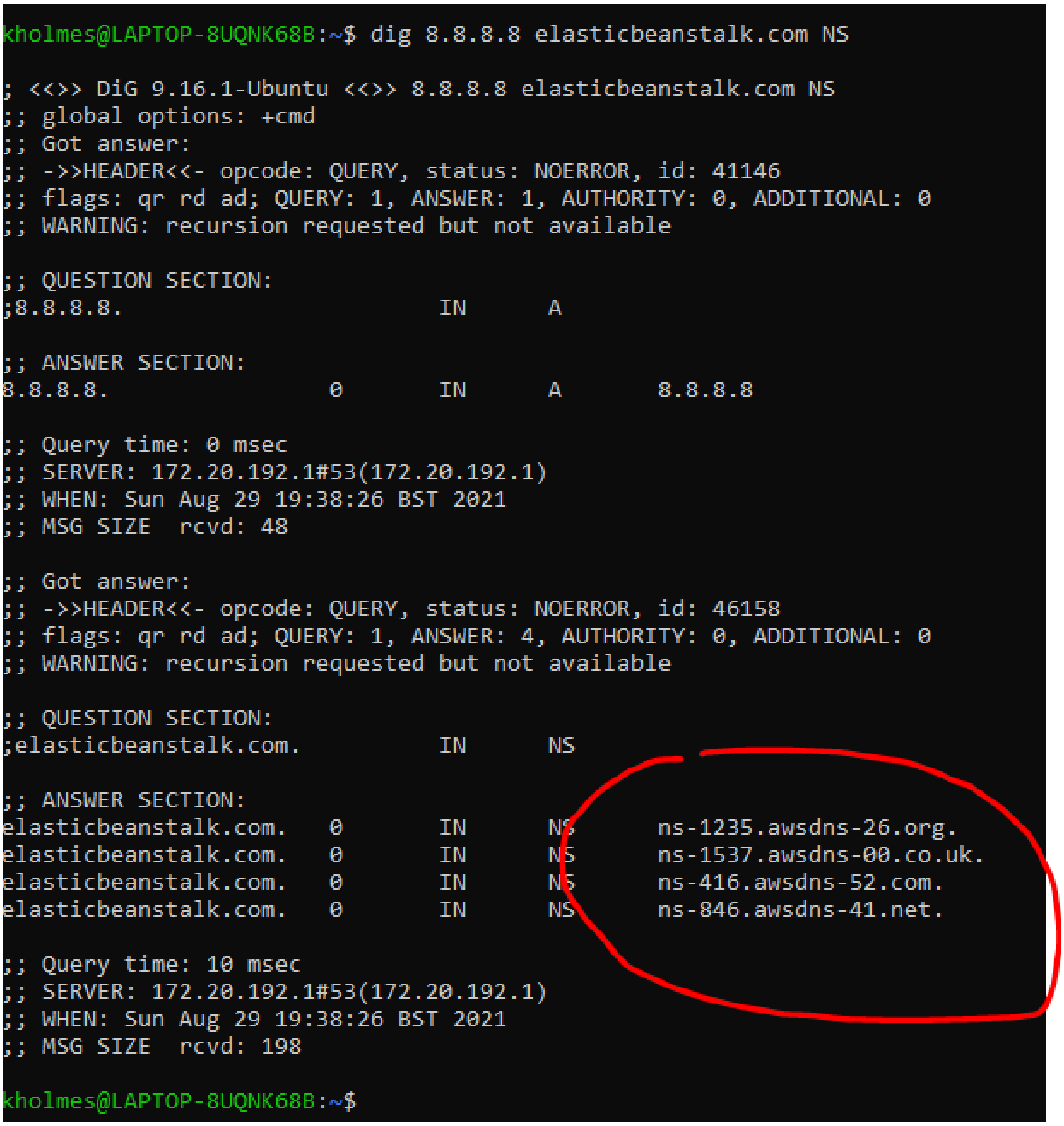
On average, steps 8 and 9 took the longest, with 106.091ms (average of the 3 results) and 105.324ms, respectively. A series of servers did not respond to the tracert query during the execution window.

Nameservers:

Command:

dig 8.8.8.8 elasticbeanstalk.com NS

Result:



```
kholmes@LAPTOP-8UQNK68B:~$ dig 8.8.8.8 elasticbeanstalk.com NS

; <<>> DiG 9.16.1-Ubuntu <<>> 8.8.8.8 elasticbeanstalk.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41146
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; ANSWER SECTION:
8.8.8.8.                0       IN      A       8.8.8.8

;; Query time: 0 msec
;; SERVER: 172.20.192.1#53(172.20.192.1)
;; WHEN: Sun Aug 29 19:38:26 BST 2021
;; MSG SIZE  rcvd: 48

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46158
;; flags: qr rd ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;elasticbeanstalk.com.          IN      NS

;; ANSWER SECTION:
elasticbeanstalk.com.   0       IN      NS      ns-1235.awsdns-26.org.
elasticbeanstalk.com.   0       IN      NS      ns-1537.awsdns-00.co.uk.
elasticbeanstalk.com.   0       IN      NS      ns-416.awsdns-52.com.
elasticbeanstalk.com.   0       IN      NS      ns-846.awsdns-41.net.

;; Query time: 10 msec
;; SERVER: 172.20.192.1#53(172.20.192.1)
;; WHEN: Sun Aug 29 19:38:26 BST 2021
;; MSG SIZE  rcvd: 198

kholmes@LAPTOP-8UQNK68B:~$
```

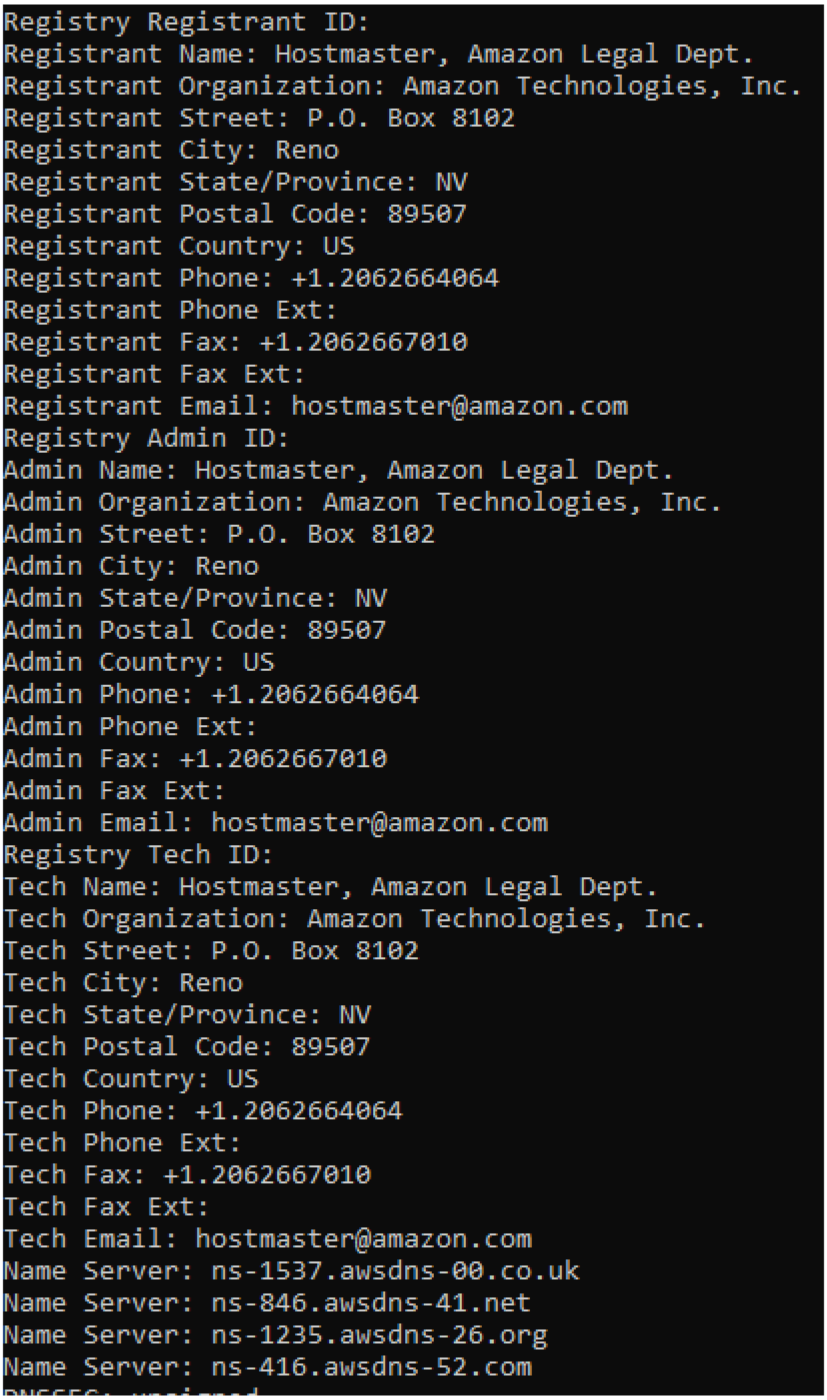
Registered contact:

Command:

```
whois elasticbeanstalk.com
```

Result:

The full outcome of the whois result can be found within the private Gist.



```
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89507
Admin Country: US
Admin Phone: +1.2062664064
Admin Phone Ext:
Admin Fax: +1.2062667010
Admin Fax Ext:
Admin Email: hostmaster@amazon.com
Registry Tech ID:
Tech Name: Hostmaster, Amazon Legal Dept.
Tech Organization: Amazon Technologies, Inc.
Tech Street: P.O. Box 8102
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89507
Tech Country: US
Tech Phone: +1.2062664064
Tech Phone Ext:
Tech Fax: +1.2062667010
Tech Fax Ext:
Tech Email: hostmaster@amazon.com
Name Server: ns-1537.awsdns-00.co.uk
Name Server: ns-846.awsdns-41.net
Name Server: ns-1235.awsdns-26.org
Name Server: ns-416.awsdns-52.com
DNSSEC: unsigned
```

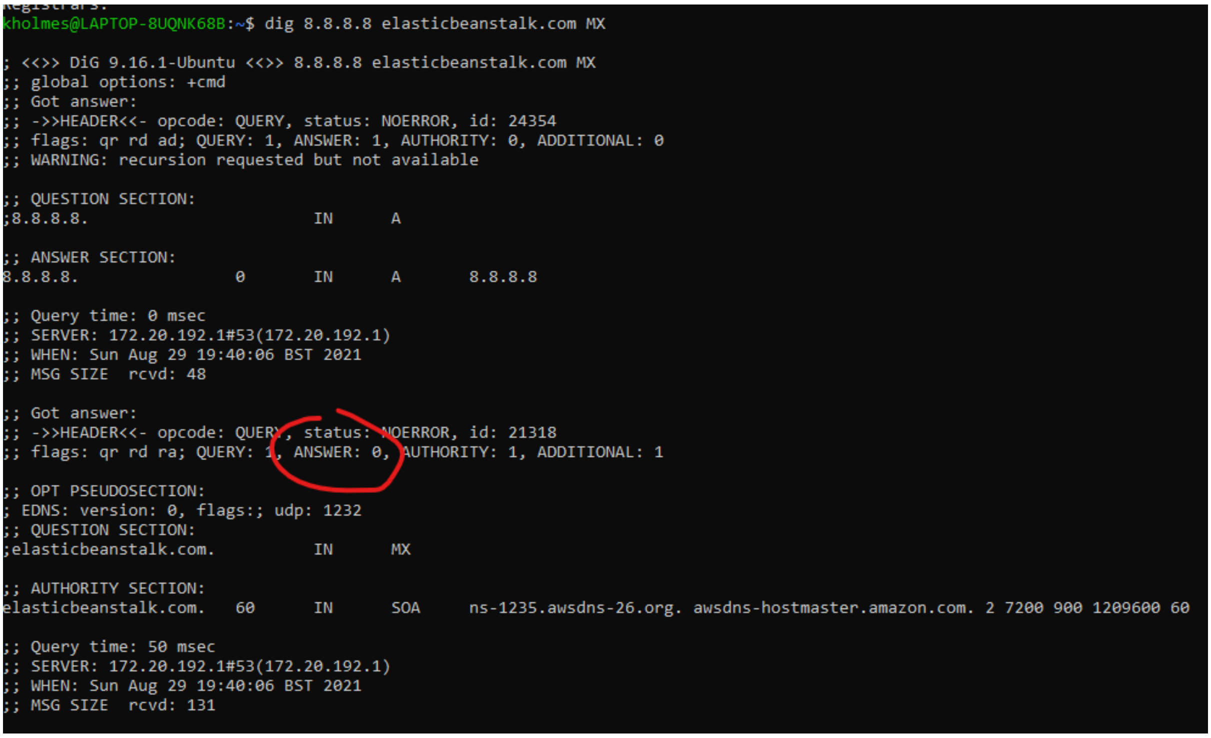
MX record:

Command:

dig 8.8.8.8 elasticbeanstalk.com MX

Result:

No MX records were found for this domain.



```
Registrars:
kholmes@LAPTOP-8UQNK68B:~$ dig 8.8.8.8 elasticbeanstalk.com MX

; <<>> DiG 9.16.1-Ubuntu <<>> 8.8.8.8 elasticbeanstalk.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24354
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; ANSWER SECTION:
8.8.8.8.                0       IN      A       8.8.8.8

;; Query time: 0 msec
;; SERVER: 172.20.192.1#53(172.20.192.1)
;; WHEN: Sun Aug 29 19:40:06 BST 2021
;; MSG SIZE  rcvd: 48

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21318
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;elasticbeanstalk.com.          IN      MX

;; AUTHORITY SECTION:
elasticbeanstalk.com.   60      IN      SOA     ns-1235.awsdns-26.org. awsdns-hostmaster.amazon.com. 2 7200 900 1209600 60

;; Query time: 50 msec
;; SERVER: 172.20.192.1#53(172.20.192.1)
;; WHEN: Sun Aug 29 19:40:06 BST 2021
;; MSG SIZE  rcvd: 131
```

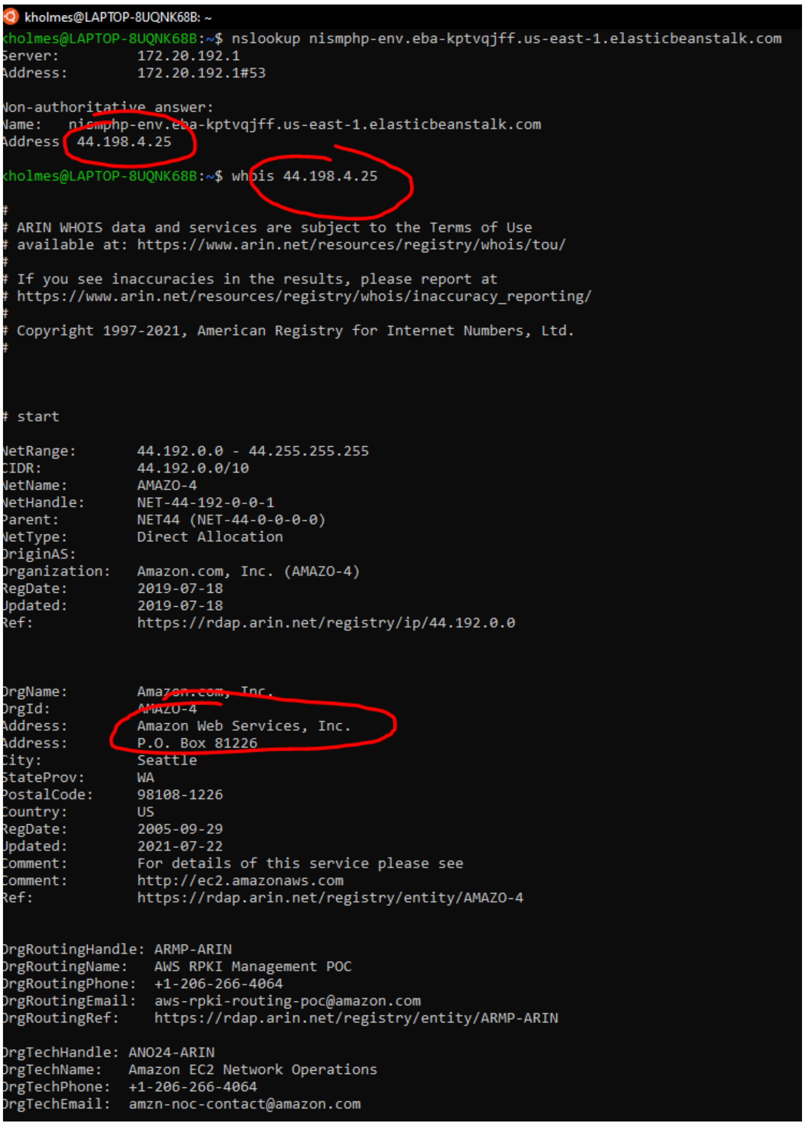
Website hosted:

Commands:

nslookup Nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com

whois {resulting IP from above query}

Results:



```
kholmes@LAPTOP-8UQNK68B: ~
kholmes@LAPTOP-8UQNK68B:~$ nslookup nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com
Server:         172.20.192.1
Address:        172.20.192.1#53

Non-authoritative answer:
Name:   nismphp-env.eba-kptvqjff.us-east-1.elasticbeanstalk.com
Address: 44.198.4.25

kholmes@LAPTOP-8UQNK68B:~$ whois 44.198.4.25

#
# 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.
#



# start

NetRange:       44.192.0.0 - 44.255.255.255
CIDR:           44.192.0.0/10
NetName:        AMAZO-4
NetHandle:      NET-44-192-0-0-1
Parent:         NET44 (NET-44-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon.com, Inc. (AMAZO-4)
RegDate:        2019-07-18
Updated:        2019-07-18
Ref:            https://rdap.arin.net/registry/ip/44.192.0.0


OrgName:        Amazon.com, Inc.
OrgId:          AMAZO-4
Address:        Amazon Web Services, Inc.
Address:        P.O. Box 81226
City:           Seattle
StateProv:      WA
PostalCode:     98108-1226
Country:        US
RegDate:        2005-09-29
Updated:        2021-07-22
Comment:        For details of this service please see
Comment:        http://ec2.amazonaws.com
Ref:            https://rdap.arin.net/registry/entity/AMAZO-4


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

OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
```

The website is hosted on 44.198.4.25, allocated to Amazon Web Services (Within the RIPE administration region).

Team Discussion (Questions):

TBC