TEAM B

Kikelomo Obayemi, Suresh Melvin Sigera, Japhet Ndhlovu

Practical Activity - Scanning Exercise

Using the website of your opposite team (assigned in Week 1), carry out the following exercises reporting on the questions listed below.

TEAM A's Website: http://nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com/

IP address: 3.95.35.126

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?**

From Kike's Machine (Lagos)

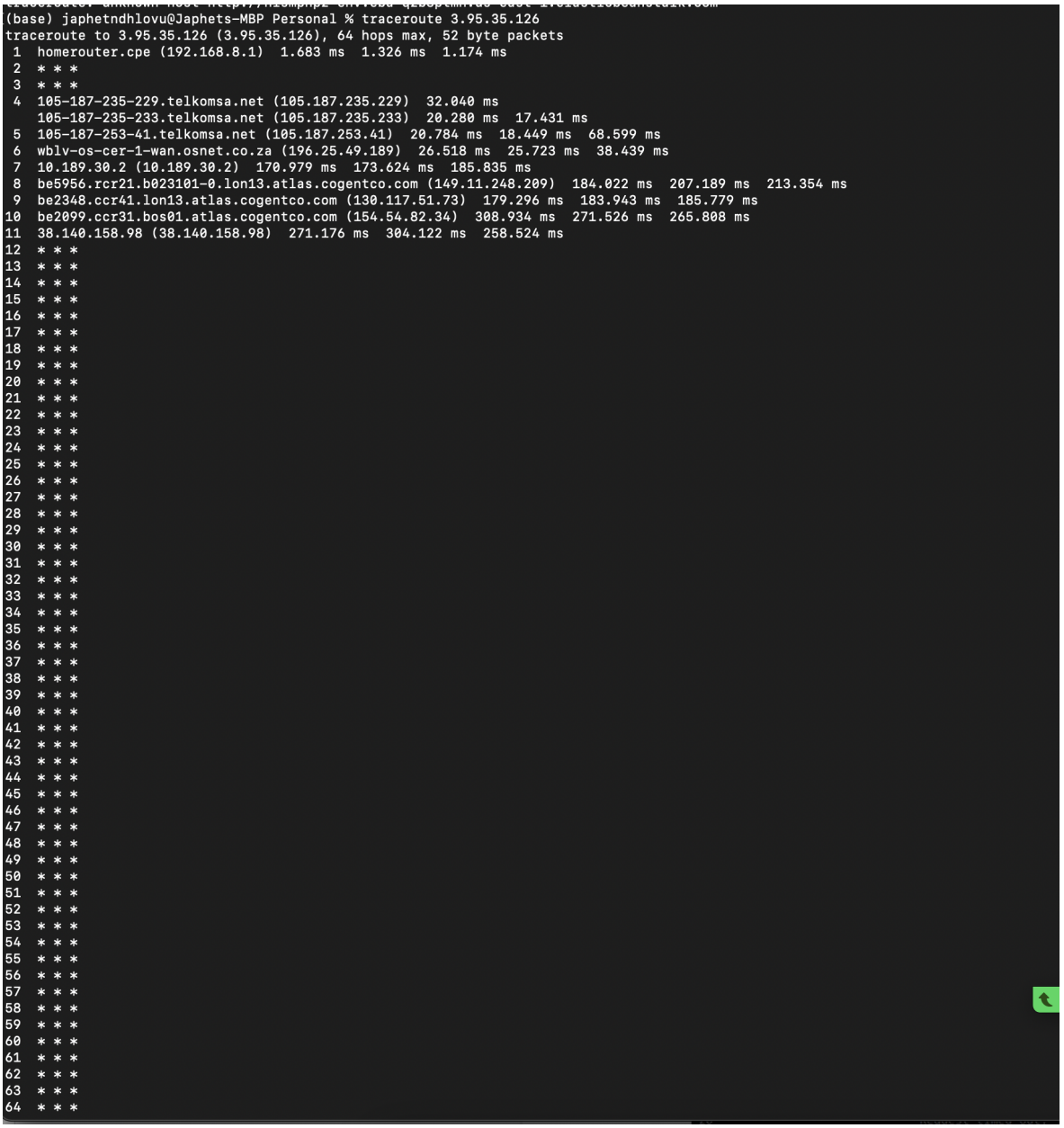
```
C:\Users\KIKE>tracert www.nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com

Tracing route to www.nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com [3.95.35.126]
over a maximum of 30 hops:

  1     2 ms     5 ms     2 ms  www.huaweimobilewifi.com [192.168.8.1]
  2     *        *        *     Request timed out.
  3    30 ms    18 ms    28 ms  10.238.6.131
  4   418 ms   297 ms   237 ms  10.238.98.27
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    45 ms    38 ms    28 ms  41.203.85.247
  8    51 ms    28 ms    19 ms  89.221.43.165
  9   479 ms   401 ms   243 ms  89.221.43.164
 10   440 ms   511 ms   477 ms  195.22.195.35
 11   201 ms   195 ms   199 ms  195.22.206.61
 12     *        *        *     Request timed out.
 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     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

From Japhet's Machine (Cape Town)



Findings: Destination not reached. Series of timeouts after 11 hops.

- **Which step causes the biggest delay in the route? What is the average duration of that delay?**

From Kike's Machine

Hop 9 causes the biggest delay

9 479 ms 401 ms 243 ms 89.221.43.164

```
C:\Users\KIKE>ping 89.221.43.164

Pinging 89.221.43.164 with 32 bytes of data:
Reply from 89.221.43.164: bytes=32 time=225ms TTL=56
Reply from 89.221.43.164: bytes=32 time=1121ms TTL=56
Reply from 89.221.43.164: bytes=32 time=266ms TTL=56
Reply from 89.221.43.164: bytes=32 time=476ms TTL=56

Ping statistics for 89.221.43.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 225ms, Maximum = 1121ms, Average = 522ms
```

Average duration is 522ms

From Japhet's Machine

```
traceroute to 3.95.35.126 (3.95.35.126), 64 hops max, 52 byte packets
 1  homerouter.cpe (192.168.8.1)  1.683 ms  1.326 ms  1.174 ms
 2  * * *
 3  * * *
 4  105-187-235-229.telkomsa.net (105.187.235.229)  32.040 ms
    105-187-235-233.telkomsa.net (105.187.235.233)  20.280 ms  17.431 ms
 5  105-187-253-41.telkomsa.net (105.187.253.41)  20.784 ms  18.449 ms  68.599 ms
 6  wblv-os-cer-1-wan.osnet.co.za (196.25.49.189)  26.518 ms  25.723 ms  38.439 ms
 7  10.189.30.2 (10.189.30.2)  170.979 ms  173.624 ms  185.835 ms
 8  be5956.rcr21.b023101-0.lon13.atlas.cogentco.com (149.11.248.209)  184.022 ms  207.189 ms  213.354 ms
 9  be2348.ccr41.lon13.atlas.cogentco.com (130.117.51.73)  179.296 ms  183.943 ms  185.779 ms
10  be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34)  308.934 ms  271.526 ms  265.808 ms
11  38.140.158.98 (38.140.158.98)  271.176 ms  304.122 ms  258.524 ms
12  * * *
13  * * *
```

The biggest delay in the route is at hop 10
be2099.ccr31.bos01.atlas.cogentco.com (154.54.82.34) 308.934 ms 271.526 ms 265.808 ms

```
^C
--- 154.54.82.34 ping statistics ---
96 packets transmitted, 96 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 239.064/275.591/519.495/60.700 ms
```

Avg duration is 275.591ms

- **What are the main nameservers for the website?**

  nslookup doesn't show much information for the url

```
C:\Users\KIKE>nslookup www.nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com
Server:  www.huaweimobilewifi.com
Address:  fe80::c62b:44ff:fe96:a8f2

Non-authoritative answer:
Name:    www.nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com
Address:  3.95.35.126


C:\Users\KIKE>nslookup 3.95.35.126
Server:  www.huaweimobilewifi.com
Address:  fe80::c62b:44ff:fe96:a8f2

Name:    ec2-3-95-35-126.compute-1.amazonaws.com
Address:  3.95.35.126
```

From whois.com (elasticbeanstalk.com)

Name Server: ns-846.awsdns-41.net
Name Server: ns-1235.awsdns-26.org
Name Server: ns-1537.awsdns-00.co.uk
Name Server: ns-416.awsdns-52.com

- **Who is the registered contact?**

  Registrant Name: Hostmaster, Amazon Legal Dept.
  Registrant Organization: Amazon Technologies, Inc.

whois command executed on Mac shows no match for domain (see screenshot below)

```
(base) japhetndhlovu@Japhets-MBP ~ % whois nismphp2-env.eba-q2b3ptmn.us-east-1.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 "NISMPHP2-ENV.EBA-Q2B3PTMN.US-EAST-1.ELASTICBEANSTALK.COM".
>>> Last update of whois database: 2021-08-29T13:19:39Z <<<
```

Details from whois website

Domain Name: elasticbeanstalk.com
Registry Domain ID: 1633430775_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T19:19:56+0000
Creation Date: 2011-01-04T23:11:58+0000
Registrar Registration Expiration Date: 2024-01-04T08:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited
(https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited
(https://www.icann.org/epp#serverDeleteProhibited)
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:
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:
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:
Nns-1537.awsdns-00.co.uk
Name Server: ns-416.awsdame Server: ns-846.awsdns-41.net
Name Server: ns-1235.awsdns-26.org
Name Server: ns-52.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

- **What is the MX record for the website?**
  From the screenshot below, no MX records found

```
C:\Users\KIKE>nslookup
Default Server:  www.huaweimobilewifi.com
Address:  fe80::c62b:44ff:fe96:a8f2

> set type=mx
> www.nismphp2-env.eba-q2b3ptmn.us-east-1.elasticbeanstalk.com
Server:  www.huaweimobilewifi.com
Address:  fe80::c62b:44ff:fe96:a8f2

us-east-1.elasticbeanstalk.com
        primary name server = ns-59.awsdns-07.com
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
>
```

- **Where is the website hosted?**

United States - Virginia - Ashburn - Amazon Technologies Inc. (Whois, 2021)

Team activity

Discuss the results of your scans and answer the following questions with your teammates before Seminar 2.

- Did you have any issues or challenges with the scans?

  Yes.

  1. We could not reach the destination of the url when the traceroute command was executed. ICMP (Internet Control Message Protocol) is used to transmit packets to the destination and if series of time outs are gotten, it could sometimes mean that ICMP traffic is filtered off by a firewall at the destination (Saegren, 2017)
  2. We could not get some information such as nameservers, registered contact, for the url because it contains subdomains.
  3. No MX records found

- How did you overcome them?

  To get some missing information, we used the whois website and the main domain which is **elasticbeanstalk.com**

- How will they affect your final report?

  Some of the information provided is not specific to the url provided but rather for **elasticbeanstalk.com**

References

a2hosting (n.d) How to troubleshoot network connectivity using ping and traceroute. Available from: https://www.a2hosting.com/kb/getting-started-guide/internet-and-networking/troubleshooting-network-connectivity-with-ping-and-traceroute [accessed 25 August 2021]

Seagren, E. (2011). *Secure your network for free*. Elsevier.

Whois (2021) Whois Record for elasticbeanstalk.com. Available from:https://whois.domaintools.com/elasticbeanstalk.com [Accessed 29 August 2021]