
UNIVERSITY OF ESSEX

PRACTICAL ACTIVITY - SCANNING EXERCISE

NETWORK AND INFORMATION SECURITY MANAGEMENT NOVEMBER 2021 A

GROUP 3



[CUSTOMERSRUS.CO.UK] TRACERT

```
Command Prompt
Microsoft Windows [Version 10.0.22000.318]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jj_ca>tracert customersrus.co.uk

Tracing route to customersrus.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1    4 ms    3 ms    3 ms  10.5.0.1
  2    4 ms    4 ms    4 ms  185.225.234.254
  3    4 ms    4 ms    4 ms  63.217.254.209
  4    5 ms    4 ms    6 ms  be3492.rcr51.hkg01.atlas.cogentco.com [154.54.140.65]
  5    5 ms    5 ms    5 ms  be2414.ccr21.hkg02.atlas.cogentco.com [154.54.88.49]
  6   186 ms   186 ms   186 ms  be2900.ccr32.mrs02.atlas.cogentco.com [154.54.6.25]
  7   227 ms   201 ms   196 ms  be2780.ccr42.par01.atlas.cogentco.com [154.54.72.225]
  8   205 ms   208 ms   211 ms  be12266.ccr42.ams03.atlas.cogentco.com [154.54.56.173]
  9   205 ms   206 ms   205 ms  be2283.rcr21.b038092-0.ams03.atlas.cogentco.com [130.117.51.14]
 10   205 ms   205 ms   205 ms  euroaccess-ltd.demarc.cogentco.com [149.6.128.82]
 11   204 ms   206 ms   206 ms  v402.R2.NL1.a2webhosting.com [209.124.94.239]
 12   203 ms   208 ms   204 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Trace complete.
```

```
C:\Users\A511221>tracert customersrus.co.uk

Tracing route to customersrus.co.uk [68.66.247.187]
over a maximum of 30 hops:

  1    5 ms    2 ms    1 ms  my.jetpack [192.168.1.1]
  2    *      *      *      Request timed out.
  3   268 ms   79 ms   115 ms  192.168.21.13
  4    *      *      *      Request timed out.
  5    76 ms   62 ms   60 ms  192.168.30.4
  6    98 ms   56 ms   62 ms  82.114.167.61
  7   154 ms   79 ms   69 ms  82.114.160.6
  8    *     168 ms  201 ms  82.114.164.18
  9   201 ms   *     171 ms  mei-b5-link.ip.twelve99.net [62.115.148.118]
 10    *      *     268 ms  prs-bb1-link.ip.twelve99.net [62.115.124.54]
 11   316 ms  201 ms  713 ms  adm-bb3-link.ip.twelve99.net [62.115.134.96]
 12   156 ms  147 ms  145 ms  adm-b10-link.ip.twelve99.net [62.115.120.227]
 13   260 ms  403 ms  407 ms  a2hosting-svc080530-ic370345.ip.twelve99-cust.net [62.115.145.217]
 14   776 ms  302 ms  306 ms  209.124.94.237.static.a2webhosting.com [209.124.94.237]
 15   243 ms  302 ms  199 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]
```

Findings in tracert:

After the local ISP, other country hop in atlas.cogentco.com domain (ISP: Cogentco) caused the biggest delay, the average duration is 121.41ms.

[CUSTOMERSRUS.CO.UK] NAMESERVERS AND REGISTERED CONTACT

- A2 Hosting web hosting nameservers (nslookup)

Name servers:
ns1.a2hosting.com
ns2.a2hosting.com
ns3.a2hosting.com
ns4.a2hosting.com

```
C:\Users\A511221>nslookup -type=ns customersrus.co.uk
Server: my.jetpack
Address: 192.168.1.1

Non-authoritative answer:
customersrus.co.uk    nameserver = ns3.a2hosting.com
customersrus.co.uk    nameserver = ns4.a2hosting.com
customersrus.co.uk    nameserver = ns2.a2hosting.com
customersrus.co.uk    nameserver = ns1.a2hosting.com
```

- MX record (nslookup)

customersrus.co.uk. 5 IN MX 0 mail.customersrus.co.uk.

```
C:\Users\A511221>nslookup -q=MX customersrus.co.uk
Server: my.jetpack
Address: 192.168.1.1

Non-authoritative answer:
customersrus.co.uk    MX preference = 0, mail exchanger = mail.customersrus.co.uk
```

Based the IP ping result, showed that the mail server hosting
in A2 Hosting

Ping mail.customersrus.co.uk [68.66.247.187]

- Registered contact (whois)

Registrar:

eNom LLC [Tag = ENOM]

URL: <http://www.enom.com>

Results returned from whois.arin.net:

OrgName: A2 Hosting, Inc.

OrgId: A2HOS

Address: P.O. Box 2998

City: Ann Arbor

StateProv: MI

PostalCode: 48106

Country: US

RegDate: 2004-03-16

Updated: 2021-10-13

Comment: <http://www.a2hosting.com>

Ref: <https://rdap.arin.net/registry/entity/A2HOS>

Contact Information

Registrant:

Handle: A2HOS

Name: A2 Hosting, Inc.

Whois Server: whois.arin.net

Kind: org

Mailing Address: P.O. Box 2998, Ann Arbor, MI, 48106, United States

Technical:

Handle: FITEJ4-ARIN

Name: Joe Fite

Email: jfite@a2hosting.com

Status: validated

Whois Server: whois.arin.net

Phone: +1-734-222-4678

Kind: individual

Mailing Address: P.O. Box 2998, Ann Arbor, MI, 48106, United States

Technical, NOC:

Handle: NETW08213-ARIN

Name: Network Operations

Organization: Network Operations

Email: noc@a2hosting.com

Status: validated

Whois Server: whois.arin.net

Phone: +1-734-222-4678

Kind: org

[CUSTOMERSRUS.CO.UK] WEBSITE HOSTED

- A2 Hosting, Inc.
 - United States of America (Ann Arbor)
 - Netherlands (Amsterdam)
- Ref: <https://www.iplocation.net/ip-lookup>

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2021-11-1)

IP Address	Country	Region	City
68.66.247.187	United States of America 	Michigan	Ann Arbor
ISP	Organization	Latitude	Longitude
A2 Hosting Inc.	Not Available	42.2288	-83.7359

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
68.66.247.187	Netherlands 	North Holland	Amsterdam
ISP	Organization	Latitude	Longitude
A2 Hosting, Inc.	A2 Hosting, Inc. (a2hosting.com)	52.3740	4.8897

TEAM ACTIVITY

- A2 Hosting, Inc. provided solutions to prevent attack and abuse:
 - Google reCAPTCHA - bot detection
 - Affect: Testing the website with lower level
 - Temporarily banned IP addresses
 - Affect: Unable to send too much request and require to change IP address if blocked
 - SSL
 - Affect: Packet or traffic capture may not able to get information
- References:
 - <https://www.a2hosting.com/kb/security/temporarily-banned-ip-addresses>
 - <https://www.a2hosting.com/kb/security>

DISCUSS THE RESULTS

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

There were discrepancies between results produced from the traceroute such as number of hops to the target website and the delay on the route and average delay.

Two IP location (United States – Netherlands/Amsterdam)

Limited information on the domain registration and the registered contact

DISCUSS THE RESULTS

How did you overcome them?

Using online tools such as ICANN LOOKUP <https://lookup.icann.org/lookup> (to find registered contact) and WHOIS <https://who.is/whois/customersrus.co.uk> (to find registrar and Name servers) and <https://www.findip-address.com/> (to find Hosting name and location)

How will they affect your final report?

Depending on one scan tool would be not enough to get the complete information about the target, which will be needed to conduct a proper website vulnerability assessment.