Summary Post:

Group 3 members were assigned www.customersrus.co.uk (appendix 1) to scan to systematically analyse security breaches and issues.

Traceroute was used (Appendix 2.1 and 2.2), viewing discrepancies in results. There was a significant increase at hop 6 with 12 hops to the target to cause the most considerable delay, 181ms. This could be a change in location to the U.S. ISP (Cogent Communications, 2021). Numerous attempts were considered to improve the validity. We noted several timeouts and 15 hops to the target address in 2.2; This could be due to packets blocked to a firewall or unanswered timeout.

TCP port findings were discovered using the Nmap online tool (Nmap Online, N.D.). The scan was fast, taking 22.8 seconds with ports open, closed and filtered. Khan (2021) highlighted that Port 21 was open for File Transfer Protocol which can be insecure and vulnerable to attack. Many companies are switching from FTP to SFTP (Khan, 2021), using Transport Layer Security which defines a standard for encryption between two systems (Parziale, 2006).

Chan (2021) highlighted that due to an increase in applications, there are more than 13000 registered official ports with three-port types (system, user and dynamic/private) assigned (Internet Assigned Numbers Authority, N.D.). To avoid well-known ports being used, ports can be customised (Chan, 2021) or by using Network Address Port Translation for port number redirection to the internal service (Parziale, 2006).

Further findings deliver the name servers A2hosting (appendix 4) and MX record using nslookup, dig and Whois. The dig tool has greater flexibility than nslookup as it will provide name servers, IP addresses, and mail servers. The ease of this method means it can be conducted all in one command quickly. Dig offered options to send queries to specified ports and particular TCP based queries (O'Reilly & Associates, 2002).

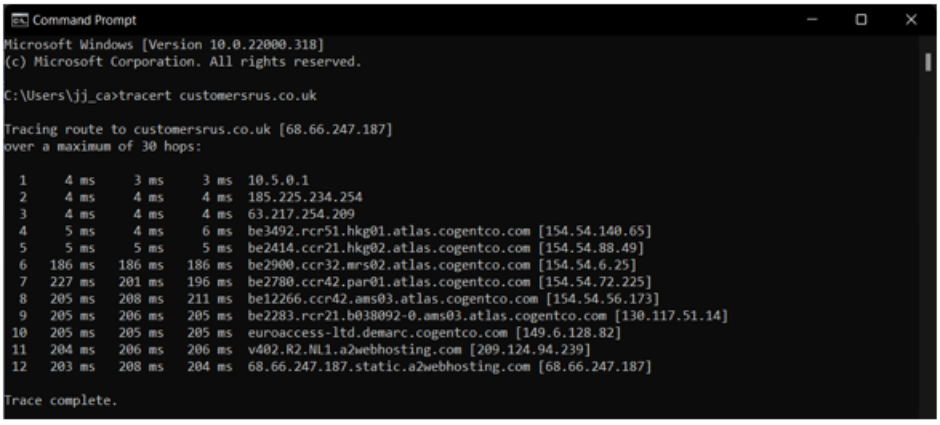
The registered contact (appendix 5) is based in the United States; however, discrepancies could also be linked to the Netherlands. Chan (2021) identified that A2hosting supports domains without Secure Sockets Layers and non-encrypted ports for email service. A solution would be to use iRedMail to disable plaintext authentication and force users to use secure port numbers (iRedMail, N.D.).

To find more conclusive results, more scans using different tools would be needed to improve the validity and reliability of the findings. It is essential to be aware of port scanning by potential attackers, so using an intrusion detection system may help detect scans, especially from Stealth, TCP Half Open or Ping scan techniques (Varonis, 2021).

Appendices:

Appendix 1

Appendix 2.1



Appendix 2.2

```
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]
```

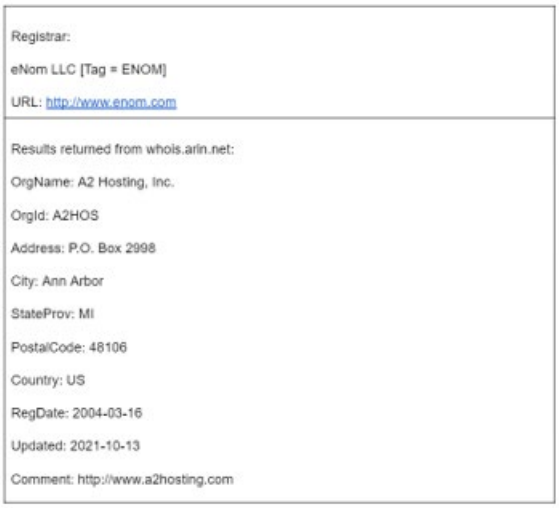
Appendix 3

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-26 19:37 EST
Nmap scan report for www.customersrus.co.uk (68.66.247.187)
Host is up (0.077s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com

PORT    STATE    SERVICE      VERSION
21/tcp  open     ftp          Pure-FTPd
22/tcp  closed   ssh
25/tcp  filtered smtp
80/tcp  open     http         Apache httpd (W3 Total Cache/0.9.4.6.4)
110/tcp open     pop3         Dovecot pop3d
143/tcp open     imap         Dovecot imapd
443/tcp open     ssl/http     Apache httpd (W3 Total Cache/0.9.4.6.4)
445/tcp closed   microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.86 seconds
```

Appendix 5



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

Appendix 4

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

Appendix 6

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

Chan, Y. (2021). Peer Response NISM Collaborative Learning Discussion 2. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289168 [Accessed 16 December 2021].

Cogent Communications. (2021). Network Map. Available: https://www.cogentco.com/en/network/network-map [Accessed 5 December 2021].

Internet Assigned Numbers Authority. (N.D.). IANA. Available: https://www.iana.org/ [Accessed 5 December 2021].

Iredmail. (N.D.). Allow insecure POP3/IMAP/SMTP connections. Available: https://docs.iredmail.org/allow.insecure.pop3.imap.smtp.connections.html [Accessed 16 December 2021].

Khan, Z. (2021). Peer Response NISM Collaborative Learning Discussion 2. Available: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=289168 [Accessed 16 December 2021].

Nmap Online. (N.D.). Scan. Available: https://nmap.online/ [Accessed 5 December 2021].
O'Reilly & Associates. (2002). DNS and BIND. Available: https://docstore.mik.ua/orelly/networking_2ndEd/dns/ch12_09.htm [Accessed 13 December 2021].
Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N.,. (2006). *TCP/IP Tutorial And Technical Overview.* . 8th ed. New York, IBM.
Varonis. (2021). What is a Port Scanner and How Does it Work? Available: https://www.varonis.com/blog/port-scanning-techniques/ [Accessed 5 December 2021].