Initial Post:

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

The first tool used was Traceroute (Appendix 2.1 and 2.2) which saw discrepancies in results. In appendix 1, we see a significant increase at hop 6 with 12 hops to the target to cause the most considerable delay, 181ms. This could have been caused by the change to the country initially in Hong Kong to the U.S. internet service provider Cogent Communications (Cogent Communications, 2021). Numerous attempts were considered of traceroute to improve the validity of results. In appendix 2.2, we can see several timeouts and 15 hops to the target address; This could be due to packets blocked to a firewall or the time running out to be answered.

TCP port findings were discovered by using the Nmap online tool (Nmap Online, N.D.). The scan was very fast, taking 22.8 seconds, and we see open ports on 21, 80, 110, 143, 443 closed on ports 22 and 445 and filtered on port 25. We judge that ports 21 (FTP), 80 (HTTP), and 22 (SSH) can be eliminated as IANA reserves them as standardised ports for their function (Internet Assigned Numbers Authority, N.D.). Port 110 (POP3) is reserved for mail clients to retrieve internet mail. Port 143 (IMAP) is used to manage e-mail on a server which is usually a non-encrypted port, unlike Port 993, which would be more secure for IMAP. Port 443 is the secured HTTPS where traffic is bonded with encryption that passes through. End users will get a warning if they access a non-HTTPS webpage (SSL2Buy, N.D.). The open ports are listening and able to respond whilst 445 is closed, which is currently in use, and 25 is filtered, which means it is unwilling to respond to requests. Port 25 is the default for STMP; however, the filtering may improve security from the risk of spam or malware. Port 445

is closed, which helps prevent file and printer sharing in the application layer network protocol. Due to its vulnerability to attack, it should be kept closed.

Further findings deliver the name servers A2hosting (appendix 4) and MX record using nslookup and dig. Using Whois, we conclude that the registered contact (appendix 5) is based in the United States; however, the results were limited in detail. Further discrepancies were found by searching the I.P. locations as A2 Hosting could be linked to the Netherlands and the United States.

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).

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].

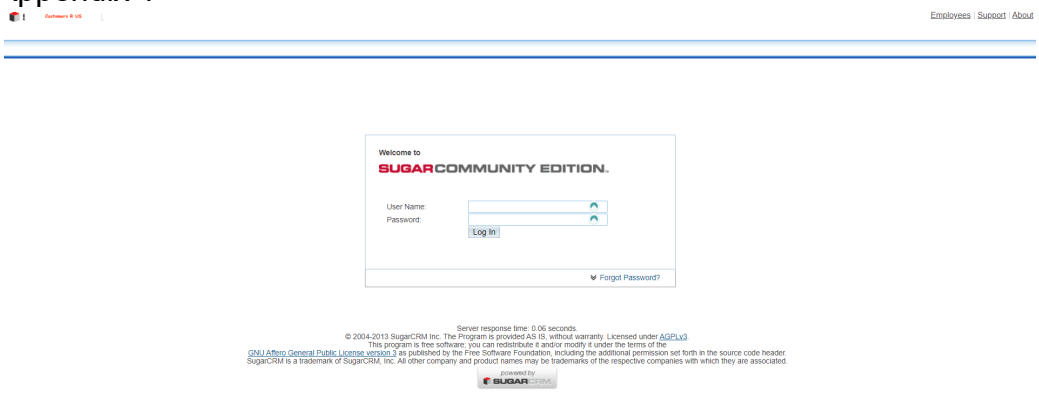
Nmap Online. (N.D.). Scan. Available: https://nmap.online/ [Accessed 5 December 2021].

Ssl2buy. (N.D.). Port 80 (HTTP) vs. Port 443 (HTTPS). Available: https://www.ssl2buy.com/wiki/port-80-http-vs-port-443-https [Accessed 5 December 2021].

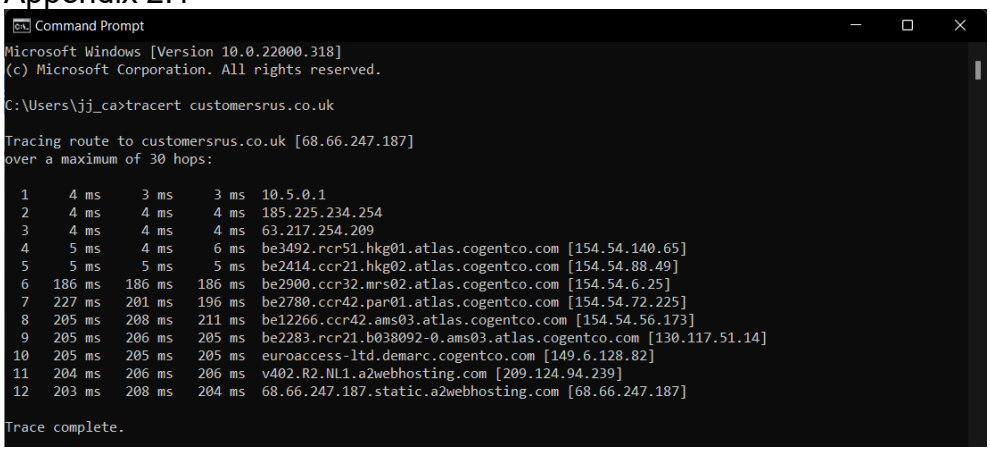
Varonis. (2021). What is a Port Scanner and How Does it Work? Available: https://www.varonis.com/blog/port-scanning-techniques/ [Accessed 5 December 2021].

Appendices:

Appendix 1

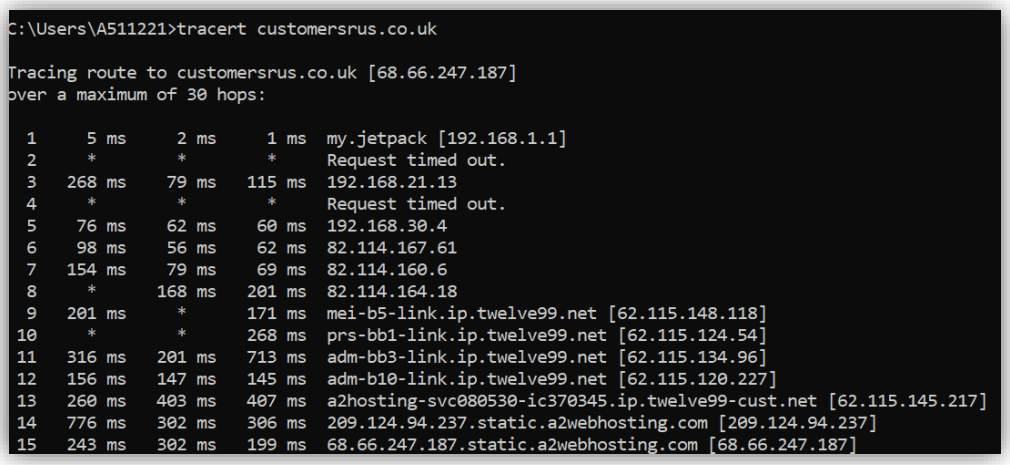


Appendix 2.1



```
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.
```

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 4

Name servers:

ns1.a2hosting.com

ns2.a2hosting.com

ns3.a2hosting.com

ns4.a2hosting.com

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 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