As I am part of group 3 where we decided to the works individual and share the results together <https://customersrus.co.uk>

Issues discovered :

1. Lack or no SSL certificate provided, this makes the site vulnerable to man in the middle attack and packet sniffing on the network.

( IP address for the domain found ( 68.66.247.187 ) and MX records ( mail.customersrus.co.uk)

1. ( Active scan ) NMAP Scans – list of ports are discovered some may not be required and leading to vulnerabilities thus the client ( customersRus needs to evaluate and close them ) recommendation is to keep minimal number of ports opened.

* Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-26 18:55 Arab Standard Time

There are 20075 closed port – 45150 TCP port – Server is used in US –

|\_http-server-header: imunify360-webshield/1.18

110/tcp open pop3 Dovecot pop3d

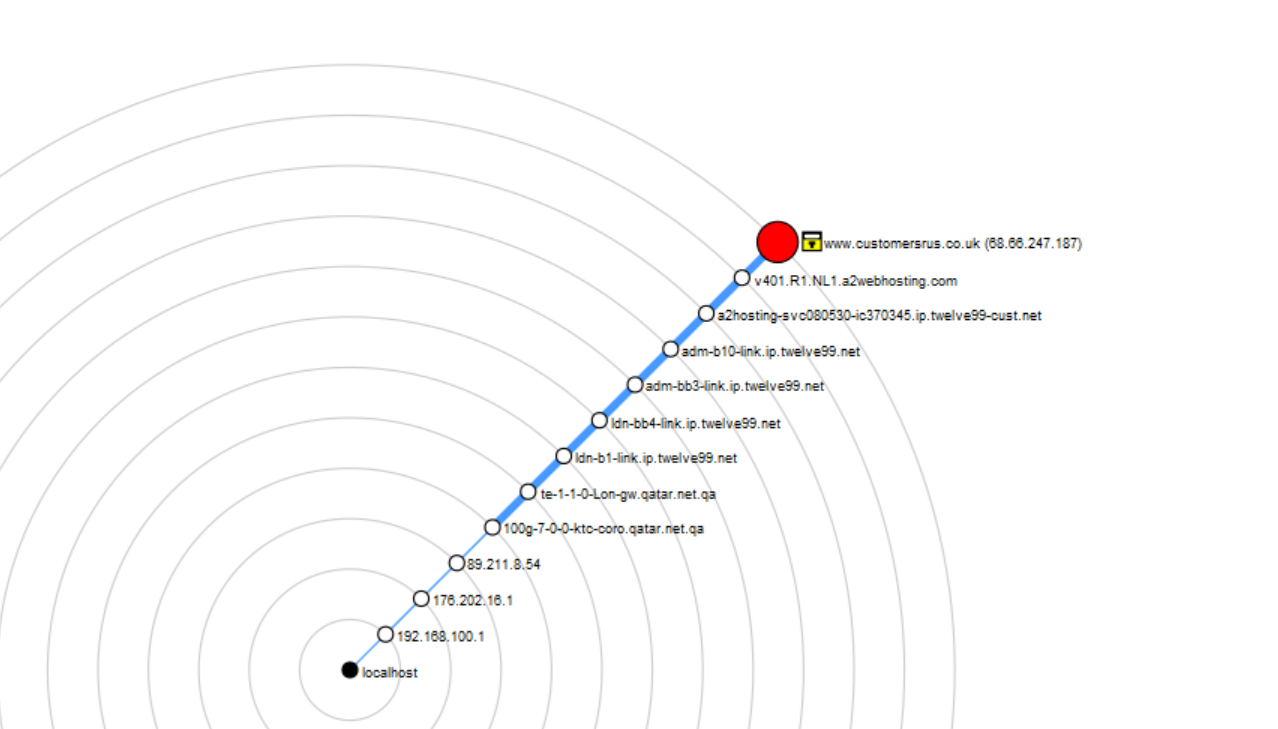
143/tcp open imap Dovecot imapd

|\_imap-capabilities: AUTH=PLAIN have post-login OK SASL-IR capabilities LOGIN-REFERRALS listed more IMAP4rev1 ENABLE STARTTLS IDLE AUTH=LOGINA0001 Pre-login LITERAL+ ID NAMESPACE

443/tcp open ssl/http Apache httpd (W3 Total Cache/0.9.4.6.4)

* also Site doesn't have a title (application/octet-stream).
* | Issuer: commonName=cPanel, Inc. Certification Authority/organizationName=cPanel, Inc./stateOrProvinceName=TX/countryName=US
* \_smtp-commands: Couldn't establish connection on port 465
* \_smtp-commands: Couldn't establish connection on port 587

NMAP hop scan :



Ip location for the website customersrus.co.uk SITE: [IP Location Finder - IP Lookup With Detailed Geolocation Data | KeyCDN Tools](https://tools.keycdn.com/geo?host=68.66.247.187)

