Summary Post

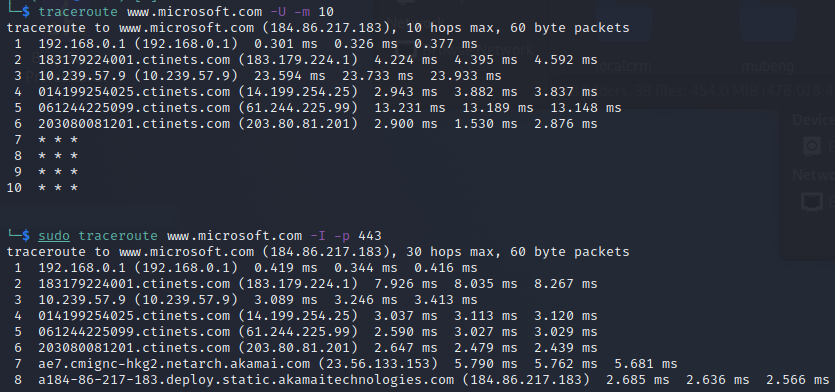
By using standard network tools and numerous internet applications to examine the allocated website https://customersrus.co.uk. It was possible to gain valuable information about the website along with ideas for analytics.

The tracert command in Windows determines the route with Internet Control Message Protocol (ICMP) by sending echo packets to the destination (Microsoft, N.D.). On the other hand, besides the default User Datagram Protocol (UDP), the traceroute command in Linux provided options to use ICMP or Transmission Control Protocol (TCP) with a specific destination port in the trace. That could provide some hidden route other than the default trace result (Appendix).

Similarly, firewalls or security devices block the ICMP completely, disallow the echo requests or block UDP packets in various ports range as security concerns (Palo Alto Networks, 2019). The exploitability of ICMP echo requests is high like the Ping of Death (POD), one of the denial-of-service (DoS) attacks. POD attack transmitting maliciously large packets by either TCP, UDP or Internetwork Packet Exchange (IPX) to the target server that could occur a buffer overflow to crash or freeze the server (Cloudflare, N.D.). Nevertheless, time to live (TTL) or ICMP redirect might be impacted when the firewall blocked all the ICMP, filtering the attacker ICMP packets would be a better option. One of the ways is to deny ICMP fragments by ACL (Cisco Press, 2004). Or else, using the newer technology, Imunify360 Webshield, web application firewall (WAF) with machine-learning rulesets (Imunify360, N.D.), that used in the allocated website to mitigate the distributed denial-of-service (DDoS) attack with reference to peer response (Austin, 2021).

The nslookup command provided different results due to the deficiencies of behaviour (Paul & Cricket, 2001), agreeing that it is technically deprecated regarding the peer response (Austin, 2021). Dig is the preferred alternative tool to query information from various DNS records used in the initial post.

In conclusion, with the new technology, malicious traffic could be more easily identified and filtered out accurately as well as produce precise information for DNS records. Using multiple techniques to obtain information or weaknesses of the target website, whereas various remedies might be discovered to avoid or mitigate.



References:

Cisco Press. (Jun 18, 2004) General Design Considerations for Secure Networks. *Security*. Available from: https://www.ciscopress.com/articles/article.asp?p=174313&seqNum=4 [Accessed 19 December 2021].

Cloudflare. (N.D.). Ping of death DDoS attack. *Common DDoS Attacks*. Available from: https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/ [Accessed 19 December 2021].

Imunify360. (N.D.) Imunify360: Security Solution with Linux Malware Scanner for Servers. *Product*. Available from: https://www.imunify360.com/ [Accessed 19 December 2021].

Microsoft. (N.D.) How to Use TRACERT to Troubleshoot TCP/IP Problems in Windows. *Windows Server 2019.* Available from: https://support.microsoft.com/en-us/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e [Accessed 19 December 2021].

Palo Alto Networks. (Jul 2, 2019) How to Block Traceroute through the Firewall. *Knowledgebase*. Available from: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMUCA0 [Accessed 19 December 2021].

Paul, A. & Cricket, L. (2001) *DNS and BIND 4th Edition*. O'Reilly & Associates. Available from: https://docstore.mik.ua/orelly/networking\_2ndEd/dns/ch12\_01.htm [Accessed 19 December 2021].