Zihaad Khan

Initial Post

A scanning task was performed on an assigned website called "https://loadedwithstuff.co.uk" from South Africa - Johannesburg with basic scanning tools such as traceroute, mtr, dig, nslookup, whois, nmap and telnet. Various results were obtained and analysed as indicated in the screenshots attached.

tcptraceroute on port 80 was used on an Apple MacBook computer which yielded 13 hops to the destination, this was confirmed by executing an mtr (mytraceroute) which indicated 30% packet loss from hop 2 to hop 3. It was observed that the largest delay was from South Africa to London, with a round trip time (RTT) for a packet increasing from 6.9ms to 179.3ms (hop 7) respectively. The average delay for hop 7 was 179.2ms. This delay is expected as the connectivity average latency is around 140ms if SEACOM cables are used as a transport medium between the two countries (SEACOM, 2021). Name servers translate domain names into IP addresses or vice versa (A2 Hosting, 2021). The name servers (NS) identified were ns1.a2hosting.com, ns2.a2hosting.com, ns3.a2hosting.com and ns4.a2hosting.com; obtained by utilising the dig command. The online whois tool was used to obtain the registered contact details (various contacts at a2hosting.com) as indicated in the screenshots attached. The mail record (mail.loadedwithstuff.co.uk) was identified using nslookup. The website was found to be hosted by A2HOSTING in Amsterdam, Netherlands using the hosting checker online tool (Hosting Checker, 2021).

In addition, nmap was used to determine open ports, with the tools mentioned above it is relatively easy for attackers to fingerprint servers and launch attacks on the protocols identified (McNab, 2017). For example, knowing that port 80 is currently open – one can execute the telnet command and issue a HEAD / HTTP/1.0 request – this reveals that the server is running Apache while nmap reveals a PostgreSQL database installed. No issues were observed in obtaining the above-mentioned results.

List of References

A2 Hosting (2021) Nameservers: What Are They And How Do They Work? Available from: https://www.a2hosting.com/blog/what-are-nameservers/ [Accessed 01 December 2021].

Hosting Checker (2021) Hosting Checker Tool. Available from: https://hostingchecker.com [Accessed 01 December 2021].

McNab, C. (2017) Network Security Assessment: Know Your Network. 3rd ed. O'Reilly Media

SEACOM (2021) PoP Latency Matrix. Available from: https://latency.seacom.com [Accessed 01 December 2021].

Thank you, Zihaad, for the informative post. The dig command was utilised to identify the name servers, a valuable tool for finding the information quickly. The Domain Information Grouper (dig) allows you to specify all aspects of the query you wish to pursue. Dig cleverly specifies arguments in any order and usually defines the type of record rather than the domain name you want to look up (O'Reilly & Associates, 2002). Therefore dig is helpful due to greater options and configuration changes for query information rather than the basic nslookup queries. Dig offers options to send queries to specified ports (-p port) instead of port 53, which is usually default and also send TCP based queries (+vc) (Parziale, 2006). Limitations of this tool can stem from queries that do not hold information about the client who initiated the query. Therefore threat actors tend to prefer this as the server-side will only see the IP address where the query came from, and attackers could manipulate this. Although the nslookup is a powerful tool, it supported the findings of the mail record in your investigation. It translated the domain names into IP addresses which is helpful for non-technical operators. In accompaniment to the dig command, they compliment network debugging.

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.