Task ‘Scanning Activities Unit 3

Scanning Activities Analysis Unit_3

Scanning Activities

Introduction

This scanning activity will be assessing the Zero Bank website’s security posture and gathering critical network information. By utilizing tools such as Traceroute, Dig, and NSLookup, the goal will look to identify key data points including network hop counts, delays, nameservers, mail exchange (MX) records, and hosting information. This analysis is crucial for performing a Vulnerability Audit and Assessment as part of Unit 6 of this course. Below, the key findings from the scans will be detailed, followed by a reflection on the process and challenges faced during the exercise.

Scanning Results

How many hops from your machine to your assigned website?

Using the Traceroute tool, we determined the number of hops from the local machine to the assigned website. The average number of hops was 30, indicating that the website resides on a server located relatively far from the origin. Traceroute tracks the route of packets from source to destination, and the number of hops reflects the number of intermediary routers or devices the packets pass through before reaching the website.

(Mazzola, et al. 2022)

Which step causes the biggest delay in the route? What is the average duration of that delay?

During the traceroute, hop 5 (ewr-sa1-i.XX.XXX.XXX.XX – XX.XX.XX.66) had the highest delay at 110.845ms, with Hop 4 showing the second highest at 110.471 ms. Average latencies were ~110.3ms for Hops 4–5, while Hops 1–3 ranged from ~2.8 to 8.3ms. The significant jump from Hop 3 ~7.3ms to Hop 4 ~110ms indicates traffic entering the ISP’s higher-latency backbone or long-distance transit router. High delays at these intermediary hops can affect response times, though some routers may prioritize ICMP probes lower than application traffic.

(Mazzola, et al. 2022; Orzach, and Khuanna, 2022)

Figure 1: Traceroute Zero Bank

What are the main nameservers for the website?

The NSLookup tool did not provide provided details about the website's nameservers as I use my own internal DNS server. I needed to override the response using a

specified DNS record type called NS (Name Server), I used the parent domain name instead of the subdomain (webappsecurity.com):

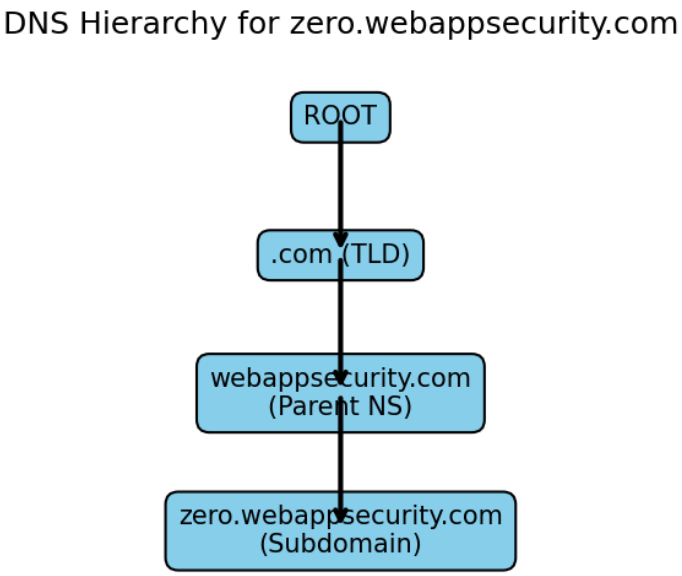

Figure 2: DNS Domain Structure

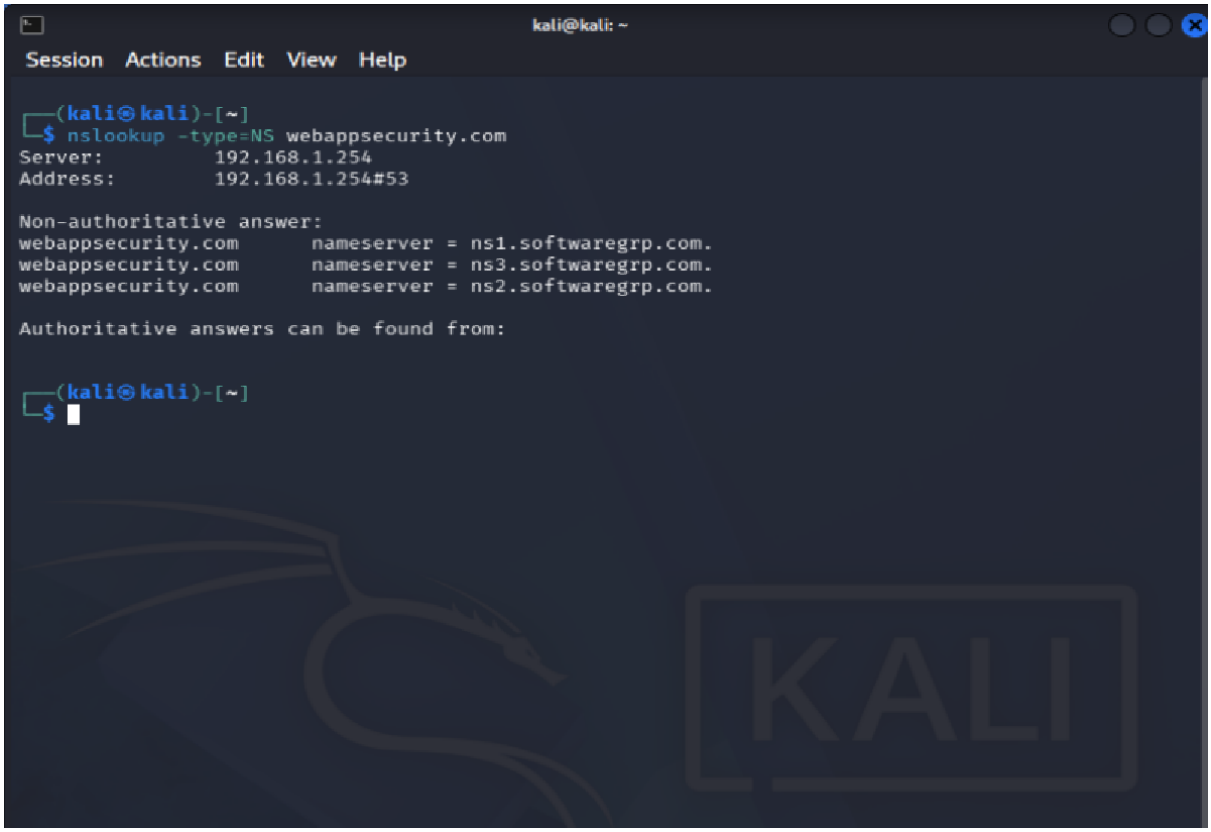

Figure 3: Name Server Query

The primary nameservers for the website were identified as:

- webappsecurity.com nameserver = ns1.softwaregrp.com.
- webappsecurity.com nameserver = ns3.softwaregrp.com.
- webappsecurity.com nameserver = ns2.softwaregrp.com.

These servers are responsible for translating the domain name into an IP address, which is essential for locating the website on the internet. The choice of nameservers indicates that the website is using a multiple dedicated DNS, or Nameservers servers for domain resolution, which is common for ensuring high availability, redundancy and performance.

(Mazzola, et al. 2022)

Who is the registered contact:

By querying the WHOIS database, the registered contact information for the domain was obtained. The registrant is listed as:

- Domain Name: WEBAPPSECURITY.COM
- Registrar WHOIS Server: whois.safenames.net
- Registrant Name: **Data protected, not disclosed**
- Registrant Email: 28n97h7n3frn@idp.email
- Registry Admin ID: Not Available from Registry
- Admin Name: International Domain Administrator
- Admin Organization: Safe names Ltd

- "For more information on Whois status codes, please visit **https://icann.org**/epp"

This information is crucial for identifying the entity responsible for the website, which can be important in case of any security-related incidents, such as data breaches or domain mismanagement. The registration is using the so-called “Private registration” hence; the output Registrant Name: **Data protected, not disclosed.**

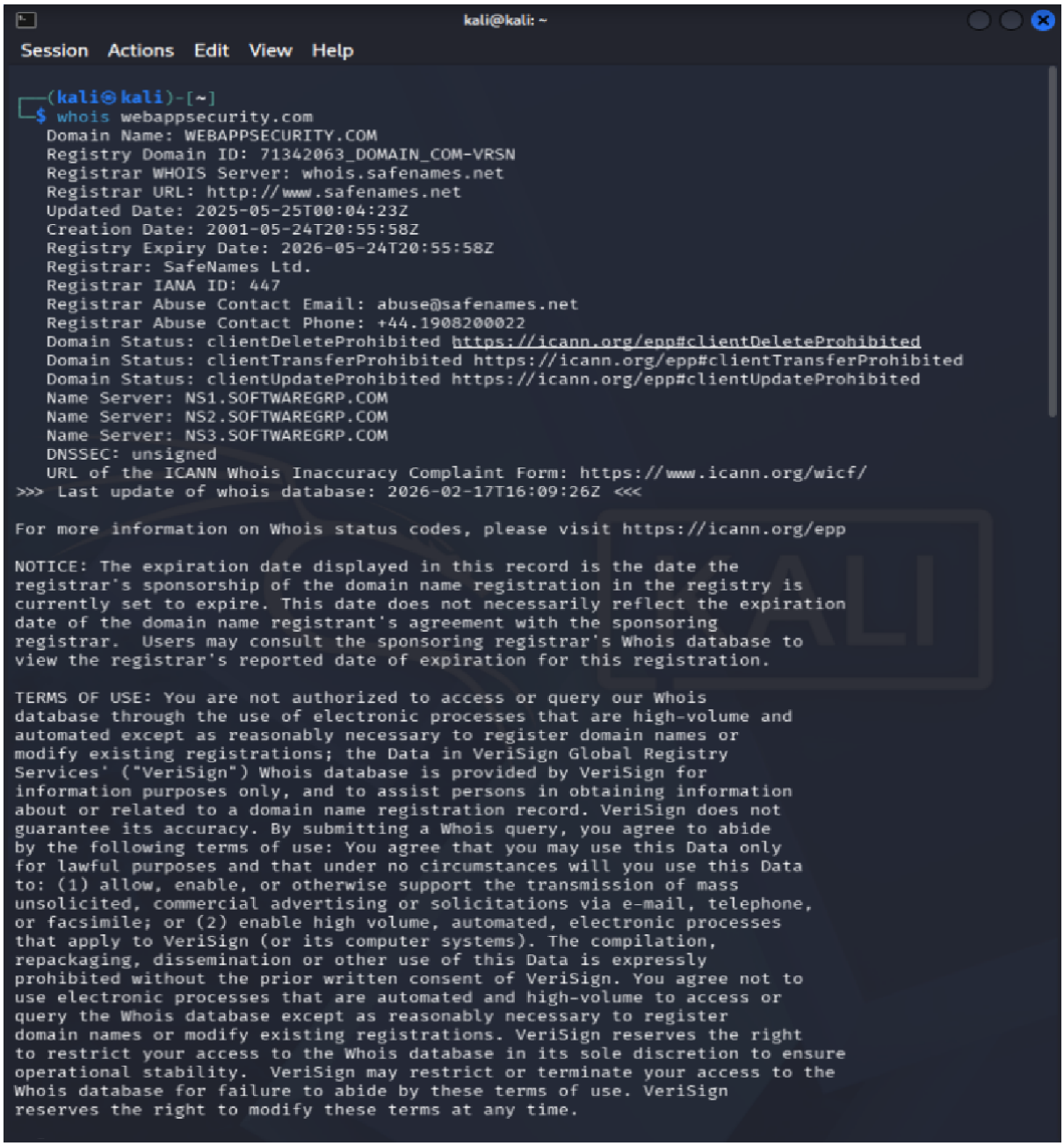

Figure 4: WHOIS Information

What is the MX record for the website?

The MX (Mail Exchange) record for the “zero.webappsecurity.com” was executed using the Dig command. The website does not seem to use an external email service, or have any MX records set-up and running, at lease from this limited assessment standpoint. Therefore, the following dig output MX record:

Output indicating this dig results:

- ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

  Explanation: This indicates that the website’s email traffic is not being managed or configured. Email servers can often be a target for attackers, so it's important to ensure that appropriate measures, such as spam filtering and encryption, are in place, what might not be required in this case.

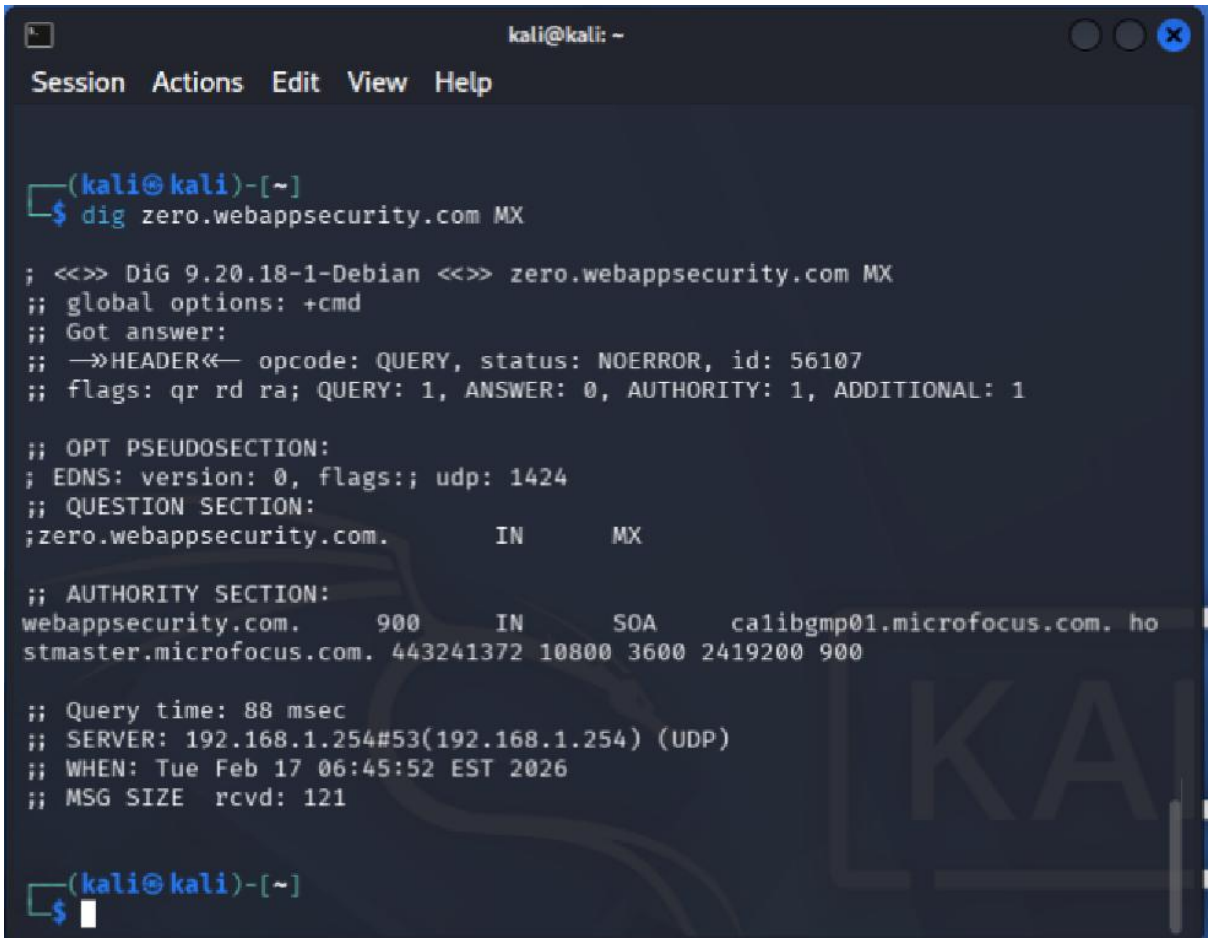

Figure 5: DIG Information

Where is the website hosted?

The hosting provider for the website was identified through a combination of DNS and IP address lookup. The hosting location is in the UK and appears to be managed by a provider specializing in cloud services called “SafeNames Ltd”. Hosting location is significant as it may impact legal jurisdiction for data privacy and security.

Reflection

Did you have any issues or challenges with the scans?

The primary challenge during this scanning activity was understanding the network path and reading the results of time in Traceroute, as the output text is not very clear to interpret, which required further investigation to confirm whether the results were displaying high, low and average, eventually, this was solvable.

(Geeksforgeeks.org, 2025)

How did you overcome them?

To address these challenges, I focused on gathering data from the scans. In cases where intermediate times stamps were unclear, I cross-referenced some guidelines and commands to ensure I was correct with my assumptions.

(Geeksforgeeks.org, 2025)

How will they affect your final report?

The findings from these scans will support the upcoming Vulnerability Audit and Assessment report in Unit 6. This will provide valuable insights into the website's network architecture, hosting information, and possible details about network performance and DNS configuration. Understanding the delay and routing patterns will also help in assessing the overall performance and robustness of the website.

Conclusion

This scanning activity provided valuable insights into the website's network configuration, including hop count, latency, hosting details and more. The identification of key infrastructure components such as the absence of nameservers and MX records enhances the understanding that not every website is configured the same

and helps learning about optimizing security posture of websites. Addressing the challenges encountered in the process and learning form results derived from tools that will be useful for the upcoming practices, vulnerability audit and executive summary.

References

- Geeksforgeeks.org, (2025) Linux Network Commands Cheat Sheet. Web. Available at: https://www.geeksforgeeks.org/linux-unix/linux-network-commands-cheat-sheet/ [Accessed 17 February 2026]
- Orzach, Y. and Khuanna, D. (2022) Network Protocols for Security Professionals. Birmingham: Packt Publishing.
- Mazzola, F. et al. (2022) ‘On the Latency Impact of Remote Peering’, in Oliver Hohlfeld et al. (eds) *Passive and Active Measurement.* [Online]. Switzerland: Springer International Publishing AG. pp. 367–392. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_springer_books_10_1007_978_3_030_98785_5_16 [Accessed 17 February 2026]