

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)

Task ‘Scanning Activities Unit 3

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)

Task ‘Scanning Activities Unit 3

```
kali@kali: ~
Session Actions Edit View Help
└(kali㉿kali)-[~]
└$ traceroute zero.webappsecurity.com
traceroute to zero.webappsecurity.com (54.82.22.214), 30 hops max, 60 byte pa
ckets
 1 [REDACTED] data omitted for security reasons [REDACTED].com (192.168.[REDACTED]) 8.405 ms 8.245 ms 8.178
ms
 2 [REDACTED] ([REDACTED]) 2.368 ms 2.858 ms 3.244 ms
 3 [REDACTED] data omitted for security reasons [REDACTED] (192.168.103) 6.770 ms 8.474 ms 6.550
ms
 4 ewr-sa1-i[REDACTED] [REDACTED].66) 109.978 ms 110.471 ms 110.
363 ms
 5 ewr-sa1-i[REDACTED] ([REDACTED].66) 110.845 ms 110.197 ms 110.
114 ms
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

└(kali㉿kali)-[~]
└$
```

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

Task ‘Scanning Activities Unit 3

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

DNS Hierarchy for zero.webappsecurity.com

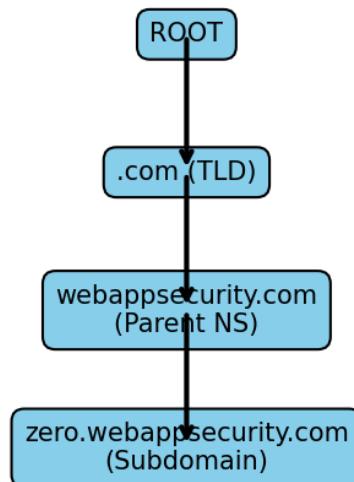


Figure 2: DNS Domain Structure

```
kali㉿kali: ~
Session Actions Edit View Help
└─$ nslookup -type=NS webappsecurity.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
webappsecurity.com      nameserver = ns1.softwaregrp.com.
webappsecurity.com      nameserver = ns3.softwaregrp.com.
webappsecurity.com      nameserver = ns2.softwaregrp.com.

Authoritative answers can be found from:

└─$
```

The screenshot shows a terminal window on a Kali Linux system. The user has run the command `nslookup -type=NS webappsecurity.com`. The output indicates that the server at 192.168.1.254 (the local host) is being queried. The non-authoritative answer shows three name servers: ns1.softwaregrp.com, ns3.softwaregrp.com, and ns2.softwaregrp.com. The terminal prompt `└─$` is visible at the bottom.

Task ‘Scanning Activities Unit 3

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:

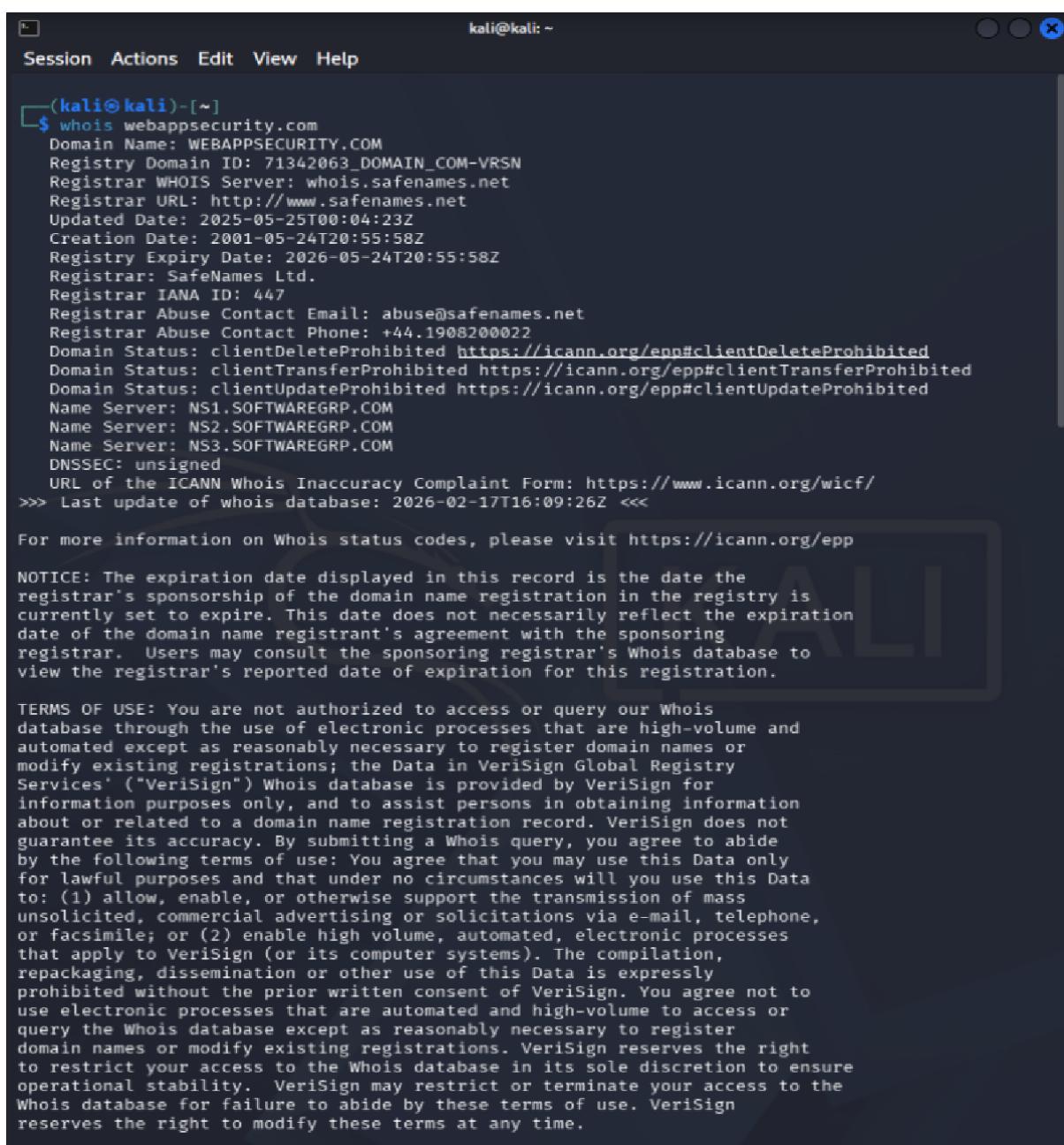
By querying the WHOIS database, the registered contact information for the domain was obtained. The registrant is listed as:

- 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

Task ‘Scanning Activities Unit 3

- "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.**



```
(kali㉿kali)-[~]
$ whois webappsecurity.com
Domain Name: WEBAPPSECURITY.COM
Registry Domain ID: 71342063_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.safenames.net
Registrar URL: http://www.safenames.net
Updated Date: 2025-05-25T00:04:23Z
Creation Date: 2001-05-24T20:55:58Z
Registry Expiry Date: 2026-05-24T20:55:58Z
Registrar: SafeNames Ltd.
Registrar IANA ID: 447
Registrar Abuse Contact Email: abuse@safenames.net
Registrar Abuse Contact Phone: +44.1908200022
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.SOFTWAREGRP.COM
Name Server: NS2.SOFTWAREGRP.COM
Name Server: NS3.SOFTWAREGRP.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2026-02-17T16:09:26Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```

Task ‘Scanning Activities Unit 3

Figure 4: WHOIS Information

What is the MX record for the website?

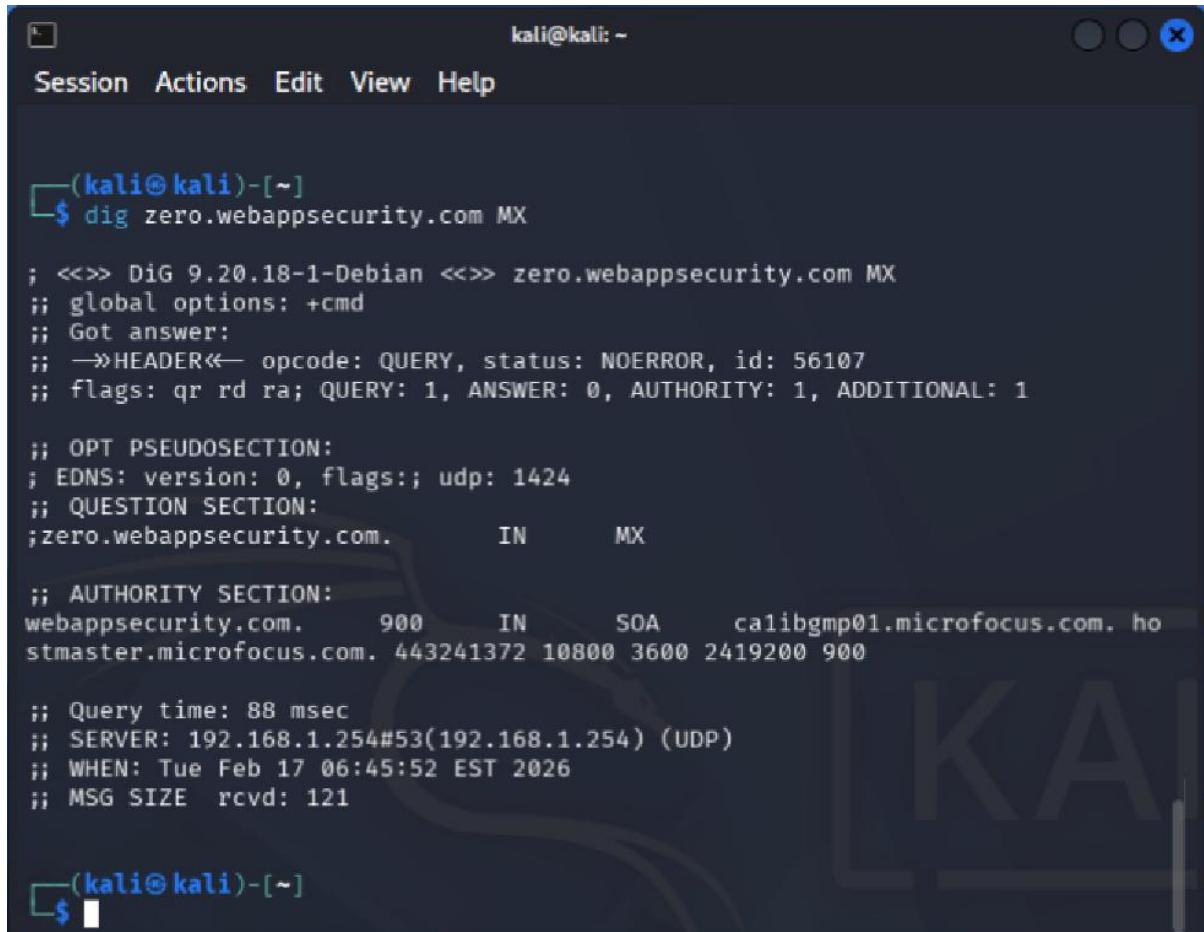
The MX (Mail Exchange) record for the “zero.webappsecurity.com” was executed using the Dig command. The website does not seem to use an external email service, or have any MX records set-up and running, at least from this limited assessment standpoint. Therefore, the following dig output MX record:

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.

Task ‘Scanning Activities Unit 3



The screenshot shows a terminal window titled "kali@kali: ~". The user has run the command "dig zero.webappsecurity.com MX". The output of the command is displayed, showing the DNS query results for the MX record of the domain "zero.webappsecurity.com". The output includes details about the query (version 9.20.18-1-Debian, UDP port 1424), the question section (zero.webappsecurity.com IN MX), the authority section (soa records for webappsecurity.com and stmaster.microfocus.com), and the query time (88 msec). The server is 192.168.1.254 and the query occurred on Tuesday, February 17, 2026.

```
(kali㉿kali)-[~]
$ dig zero.webappsecurity.com MX

; <>> DiG 9.20.18-1-Debian <>> zero.webappsecurity.com MX
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 56107
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;zero.webappsecurity.com.      IN      MX

;; AUTHORITY SECTION:
webappsecurity.com.    900     IN      SOA      calibgmp01.microfocus.com. ho
stmaster.microfocus.com. 443241372 10800 3600 2419200 900

;; Query time: 88 msec
;; SERVER: 192.168.1.254#53(192.168.1.254) (UDP)
;; WHEN: Tue Feb 17 06:45:52 EST 2026
;; MSG SIZE  rcvd: 121

(kali㉿kali)-[~]
$
```

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?

Task ‘Scanning Activities Unit 3

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

Task ‘Scanning Activities Unit 3

and helps learning about optimizing security posture of websites. Addressing the challenges encountered in the process and learning from 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]