

Title: DNS and IP Discovery Report

Student Name: Nandana Padmasenan

Register no: 2462117

Course: EH Semester 3

Date: 31-07-2025

Methodology

This assignment involved performing DNS and IP discovery on the domain `zero.webappsecurity.com` using multiple reconnaissance tools. The objective was to understand how domains resolve to IP addresses, how data is routed over the internet, and how to use common cybersecurity tools for analysis.

The tools used included:

- **nslookup** – to resolve the domain to its corresponding IP
- **tracert** – to map the path from my system to the server
- **nmap** – to discover open ports and services running on the target
- **Shodan** – for gathering publicly indexed information about the server
- **VirusTotal** – to assess any malicious or suspicious reputation of the domain/IP

All tools were used ethically and strictly within the scope defined for the assignment.

Findings

- **DNS Lookup (nslookup):**
The domain resolved to the IP address `54.82.22.214`. This is likely a dynamic IP hosted on Amazon Web Services (AWS).
- **Route Trace (tracert):**
The traceroute showed a multi-hop network path to the server. Some intermediary hops were hidden due to firewall restrictions, which is typical for cloud-based hosting environments.
- **Port Scanning (nmap):**
The following open ports were discovered:
 - **Port 80** – HTTP web traffic
 - **Port 443** – HTTPS secure web trafficThese indicate a functioning web server with SSL/TLS support.
- **Shodan Search:**
A Shodan search using the IP address revealed basic server information, confirming it's hosted on AWS. Ports 80 and 443 were publicly visible. No critical vulnerabilities or high-risk services were exposed in the scan, suggesting a minimal external attack surface.

- **VirusTotal Analysis:**

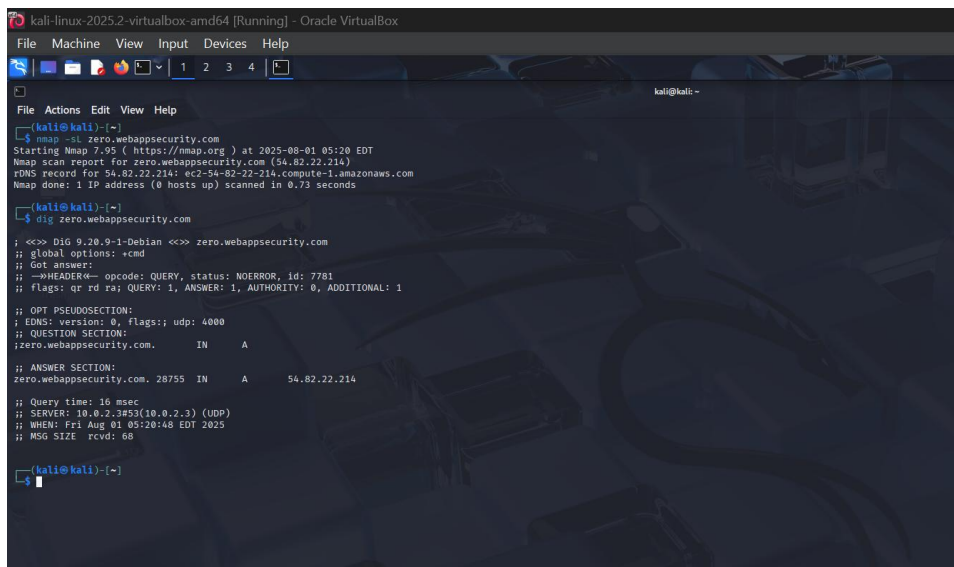
The domain was scanned using VirusTotal's URL analysis. No malware, phishing, or suspicious indicators were found. The domain is considered clean across all major antivirus engines.

-
- ✓ All screenshots and findings have been documented and organized in the 1st Assignment/evidence/ directory.
 - ✓ This analysis was conducted on authorized test targets only, for educational purposes.

Screenshots and Evidence

Below are the screenshots of the DNS and IP discovery process carried out on the target domain zero.webappsecurity.com using the tools nmap -sL and dig in Kali Linux. These images serve as proof of execution and demonstrate the results obtained during the reconnaissance phase.

- nmap -sL: Used to resolve the domain name and verify the IP address.
- dig: Used to query DNS records and understand how the domain is mapped to its IP through the DNS hierarchy.
- DNS Resolution Flowchart: A visual representation of how DNS queries are processed step-by-step to resolve domain names into IP addresses.



```
kali@kali:~$ nmap -sL zero.webappsecurity.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 05:20 EDT
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Nmap done: 1 IP address (0 hosts up) scanned in 0.73 seconds

kali@kali:~$ dig zero.webappsecurity.com

;<<>> Dig 9.20.9-1-Debian <<>> zero.webappsecurity.com
;; global options: +cmd
;; Got answer:
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 7781
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version 0, flags: udp: 4000
;; QUESTION SECTION:
;zero.webappsecurity.com.      IN      A
;; ANSWER SECTION:
zero.webappsecurity.com. 28755 IN      A      54.82.22.214

;; Query time: 16 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Fri Aug 01 05:20:48 EDT 2025
;; MSG SIZE rcvd: 68
```

User types domain → Browser asks OS → OS checks DNS cache → DNS request to Resolver → Root Server → TLD Server → Authoritative Server → Returns IP → Website loads

DNS RESOLUTION PROCESS FLOWCHART:

❓ **User types domain**



❓ **Browser asks OS for the IP**



❓ **OS checks local DNS cache**



❓ **If not found, OS sends query to Recursive Resolver**



❓ **Recursive Resolver queries Root Server**



❓ **Root Server directs to TLD Server (e.g., .com)**



❓ **TLD Server directs to Authoritative Name Server**



❓ **Authoritative Server returns IP address for domain**



❓ **Resolver sends IP back to OS**



❓ **OS sends IP to Browser → Browser connects to website**

Conclusion

This task introduced me to practical DNS and IP discovery techniques. It improved my understanding of how web services operate behind domain names, how routing works on the internet, and how open-source tools can be leveraged to assess potential risks.

The domain appears to be securely hosted with minimal public exposure and no known vulnerabilities. All collected evidence (command-line output and screenshots) is included in the evidence/ folder in the GitHub repository.