Title: DNS and IP Discovery Report
Student Name: Nandana Padmasenan
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 traffic
    These 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.

Conclusion

This task introduced me to practical DNS and IP discovery techniques. It strengthened 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.

This exercise has enhanced my ability to perform basic reconnaissance safely and responsibly — a critical skill in cybersecurity.

✅ 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.