DNS Investigation Assignment: Finding Real IP Addresses

Student: Jonathan Carrasco
Reg-no:2462089

Objective

This assignment demonstrates DNS resolution and network reconnaissance using nmap and digtools to analyze zero.webappsecurity.com, a legitimate security testing platformby MicroFocusFortify.

Methodology & Tools

- Nmap (-sL): List scan for IP resolution without port scanning
- Dig: Comprehensive DNS record analysis and query functionality
- Target: zero.webappsecurity.com (authorized educational platform)

Technical Implementation & Results

Primary Commands Executed:

bash

```
$ nmap -sL zero.webappsecurity.com
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$ dig
zero.webappsecurity.com
zero.webappsecurity.com. 300 IN A 54.82.22.214
```

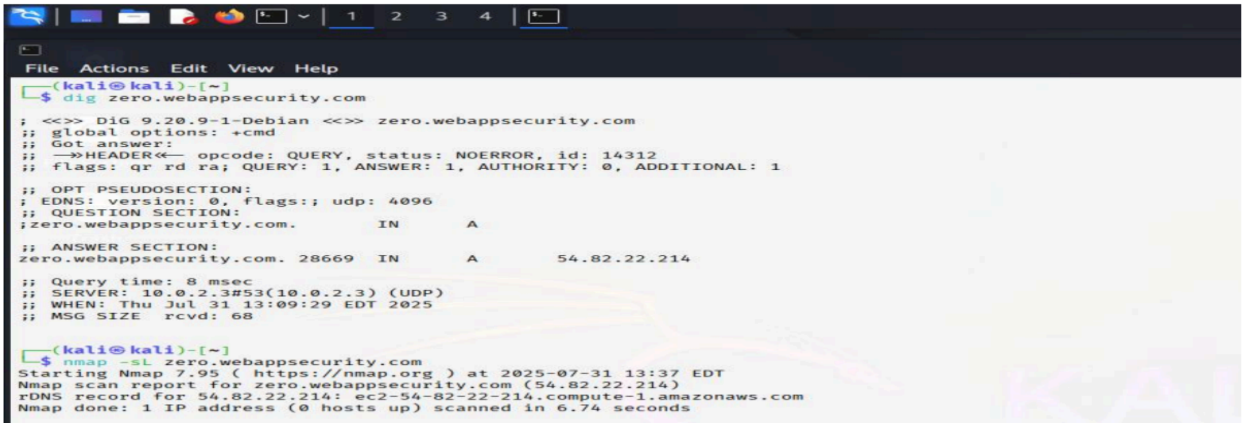
Key Findings:

Primary IP	54.82.22.214	Single A record configuration
Reverse DNS	ec2-54-82-22-214.compute-1.amazonaws.com	AWS EC2 infrastructure

Reconnaissance Value:

Asset discovery and infrastructure mapping
Hosting provider identification

Screenshot:



```
┌──(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: 14312
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zero.webappsecurity.com.        IN      A

;; ANSWER SECTION:
zero.webappsecurity.com. 28669   IN      A       54.82.22.214

;; Query time: 8 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Thu Jul 31 13:09:29 EDT 2025
;; MSG SIZE  rcvd: 68


┌──(kali㉿kali)-[~]
└─$ nmap -sL zero.webappsecurity.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:37 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 6.74 seconds
```

DNS Resolution Flowchart:

[User Types URL in Browser]

↓

[Browser Checks Cache]

↓ **(not found)**

[Ask Local DNS Resolver]

↓

[Local Resolver Checks Its Cache]

↓ **(not found)**

[Ask Root DNS Server]

↓

[Root Server → .com TLD Server]

↓

[TLD Server → Authoritative DNS Server]

↓

[Authoritative Server Responds with IP]

↓

[Local Resolver Caches & Sends IP]

↓

[Browser Connects to IP Address]