**Footprinting and Reconnaissance**

**By,**

**PILLA VENKATA RAMANA**

**DIET**

FOOTPRINTING:

Footprinting is the process of collecting and gathering information about a target system or network to identify potential vulnerabilities and weaknesses. It is an essential phase in the reconnaissance stage of cybersecurity. Footprinting can be categorized into two main types: passive and active.

Sure, here are simplified steps for the footprinting and reconnaissance phases:

1. Passive Footprinting:

- Identify the Target: Determine the scope of your target, including domain names, IP ranges, and associated entities.

- DNS Information: Collect information from public DNS records, including domain registration details and subdomains.

2. Active Footprinting:

- Network Scanning: Use tools to discover live hosts, open ports, and services on the target network.

- Enumeration: Gather specific information about identified hosts, such as user accounts, shares, and system details.

3. Passive Reconnaissance:

- Social Media Analysis: Collect information about employees, their roles, and potential security weaknesses from publicly available social media profiles.

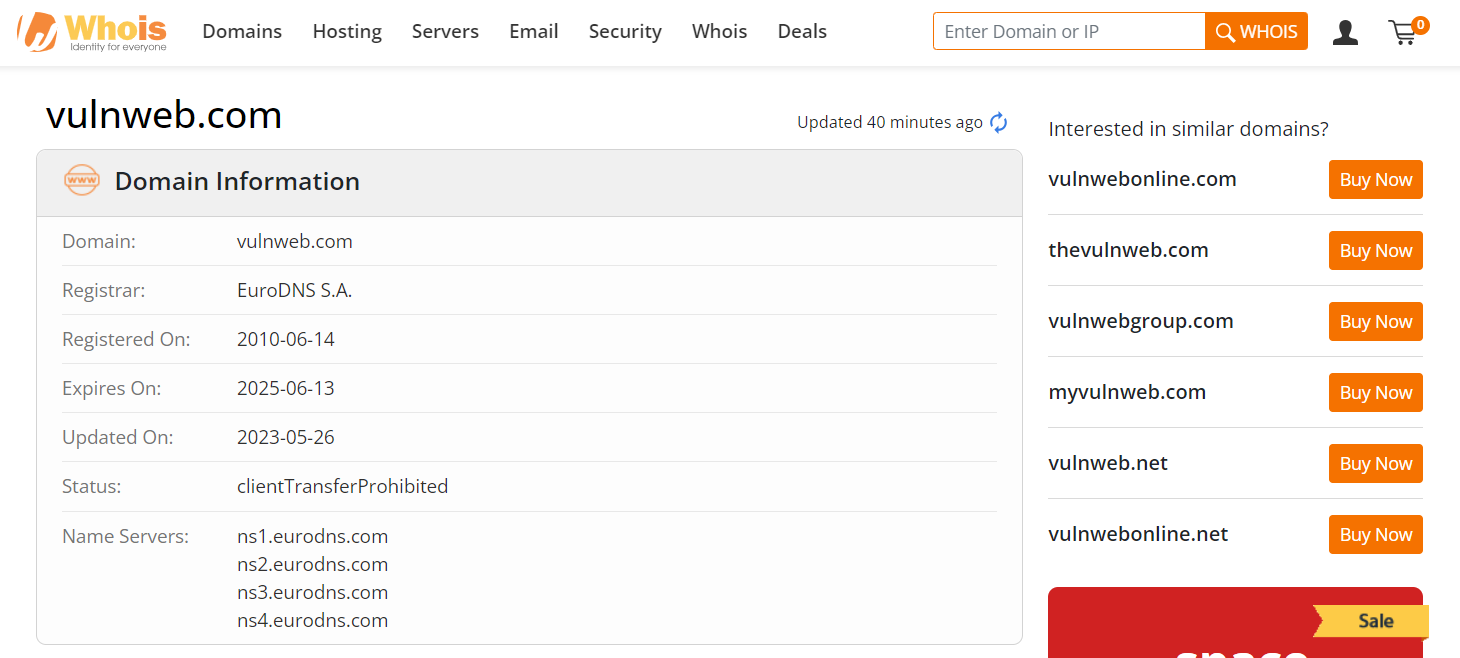
- Job Postings and Company Websites: Analyse job descriptions, organizational structures, and technology used.

4. Active Reconnaissance:

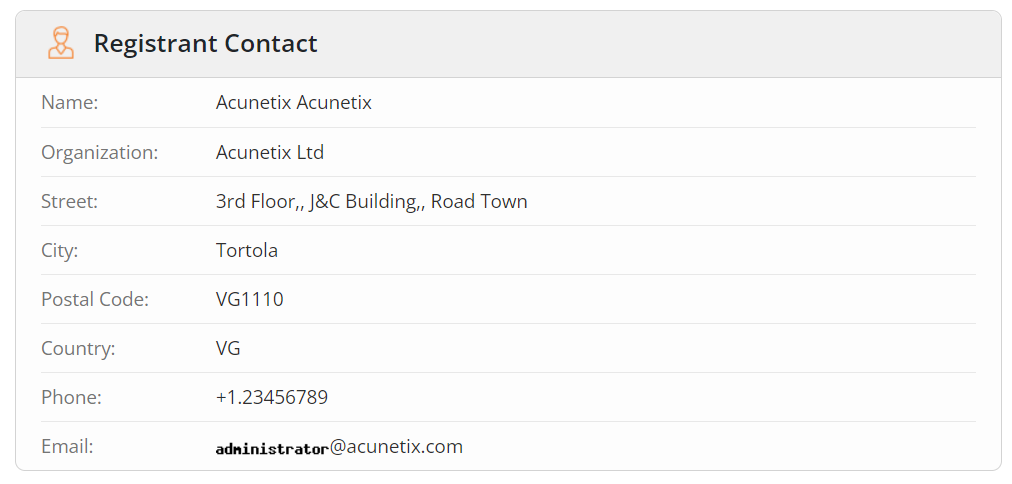
- Scanning and Enumeration: Perform more in-depth scanning and enumeration to gather detailed information about systems, services, and potential vulnerabilities.

**Information gathering in WHOIS**

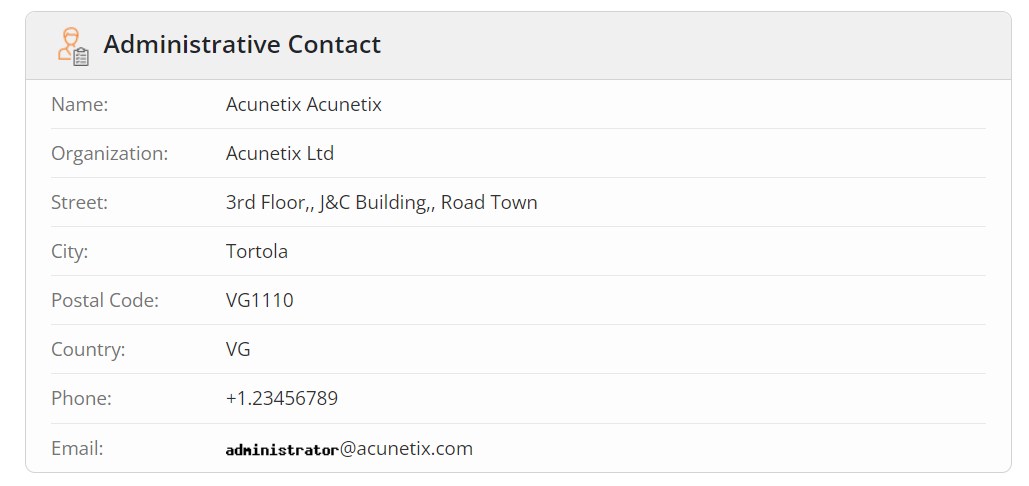
Domain Information



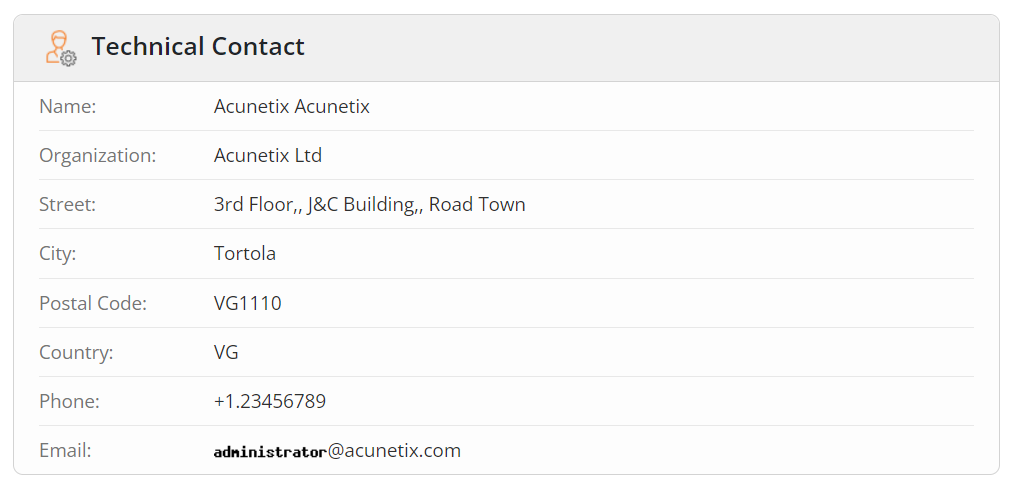
Registrant Contact



Administrative Contact



Technical Contact



**Raw Whois Data**

Domain Name: vulnweb.com

Registry Domain ID: D16000066-COM

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: http://www.eurodns.com

Updated Date: 2023-05-26T10:04:20Z

Creation Date: 2010-06-14T00:00:00Z

Registrar Registration Expiration Date: 2025-06-13T00:00:00Z

Registrar: Eurodns S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: email@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Registry Registrant ID:

Registrant Name: Acunetix Acunetix

Registrant Organization: Acunetix Ltd

Registrant Street: 3rd Floor,, J&C Building,, Road Town

Registrant City: Tortola

Registrant State/Province:

Registrant Postal Code: VG1110

Registrant Country: VG

Registrant Phone: +1.23456789

Registrant Fax:

Registrant Email: email@acunetix.com

Registry Admin ID:

Admin Name: Acunetix Acunetix

Admin Organization: Acunetix Ltd

Admin Street: 3rd Floor,, J&C Building,, Road Town

Admin City: Tortola

Admin State/Province:

Admin Postal Code: VG1110

Admin Country: VG

Admin Phone: +1.23456789

Admin Fax:

Admin Email: email@acunetix.com

Registry Tech ID:

Tech Name: Acunetix Acunetix

Tech Organization: Acunetix Ltd

Tech Street: 3rd Floor,, J&C Building,, Road Town

Tech City: Tortola

Tech State/Province:

Tech Postal Code: VG1110

Tech Country: VG

Tech Phone: +1.23456789

Tech Fax:

Tech Email: email@acunetix.com

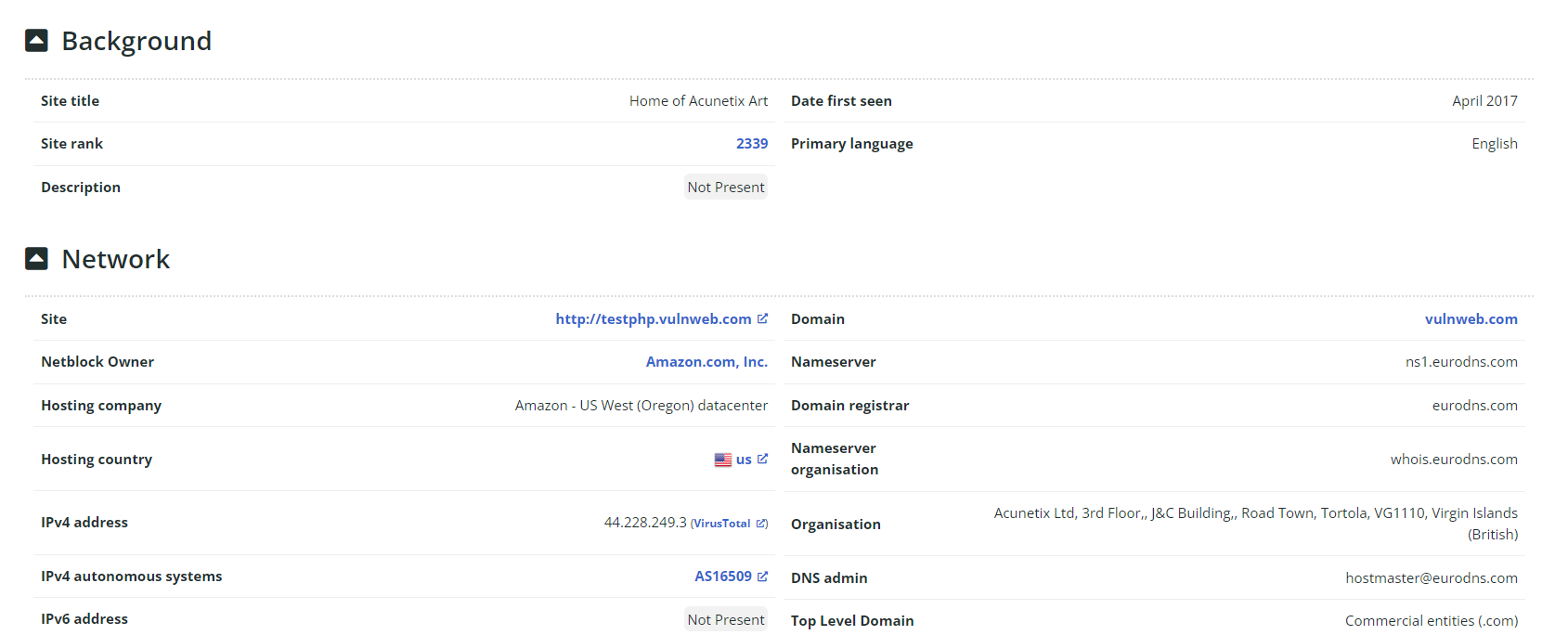
Name Server: ns1.eurodns.com

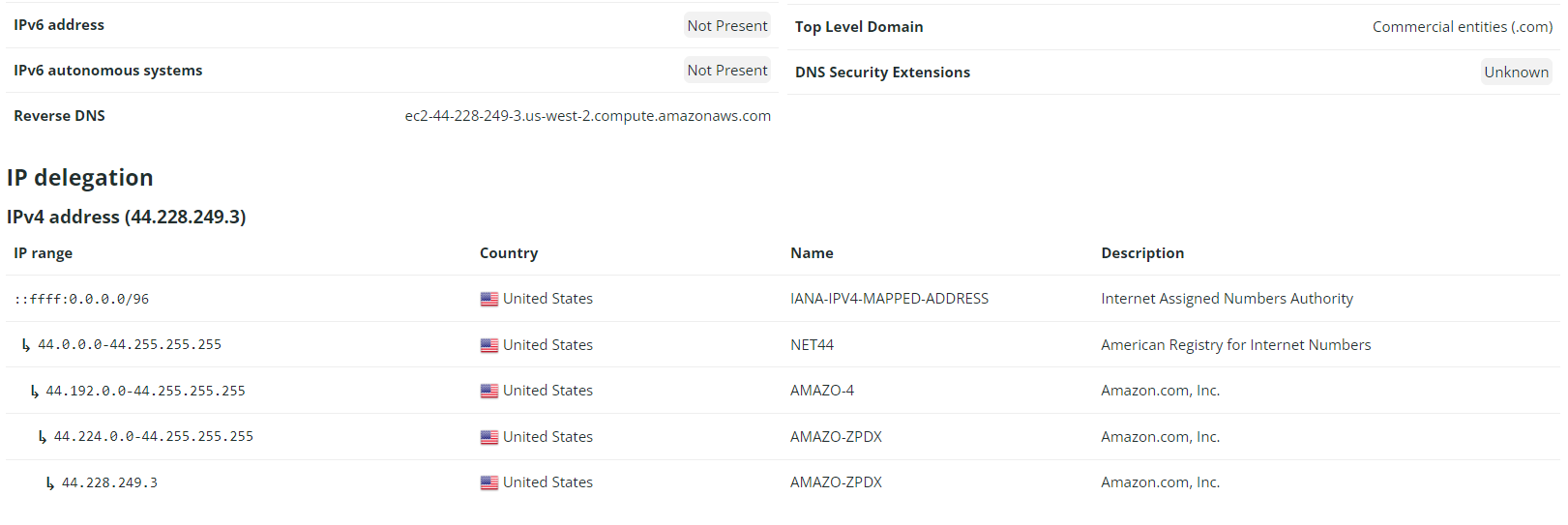
Name Server: ns2.eurodns.com

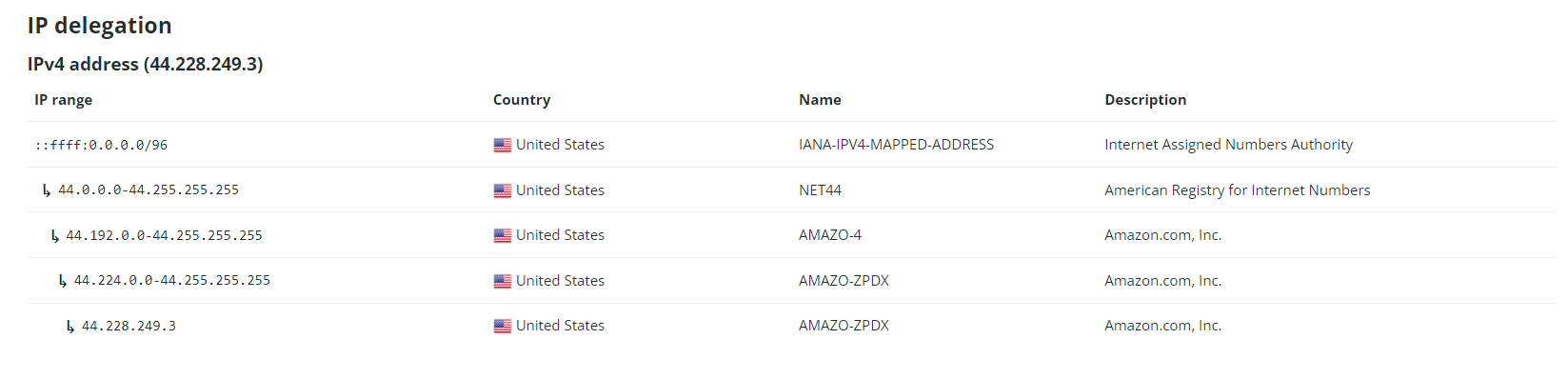
Name Server: ns3.eurodns.com

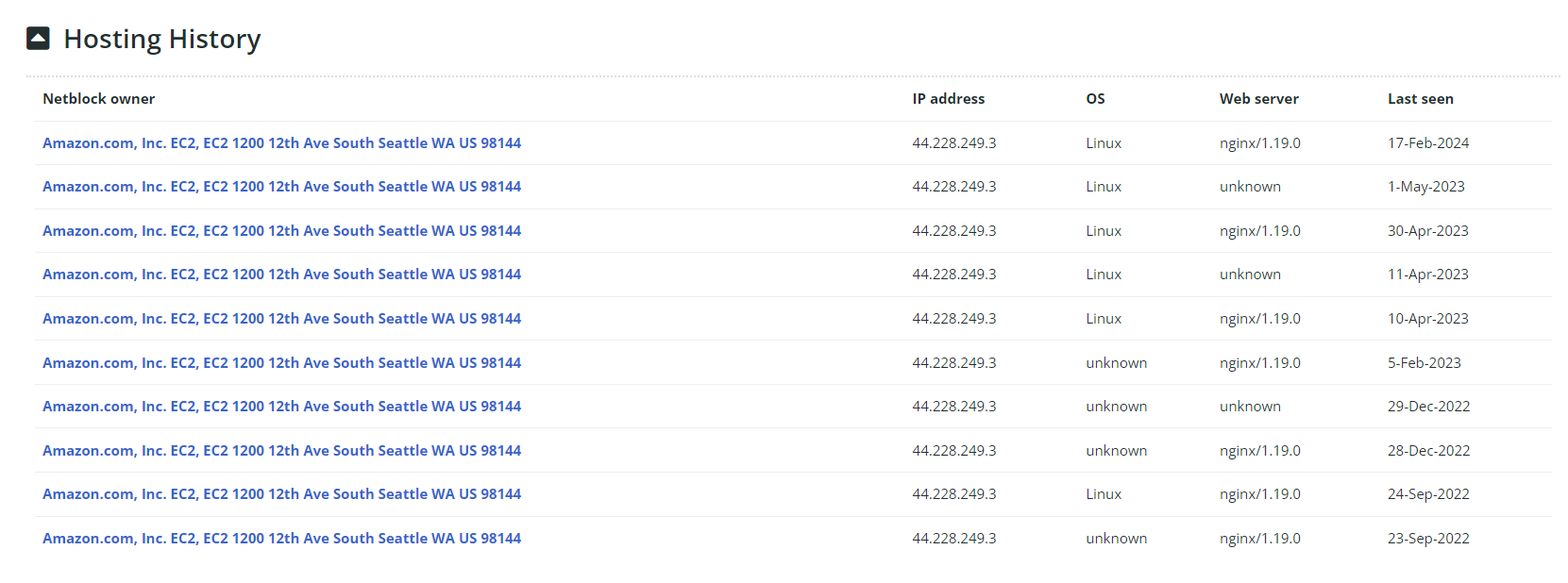
Name Server: ns4.eurodns.com

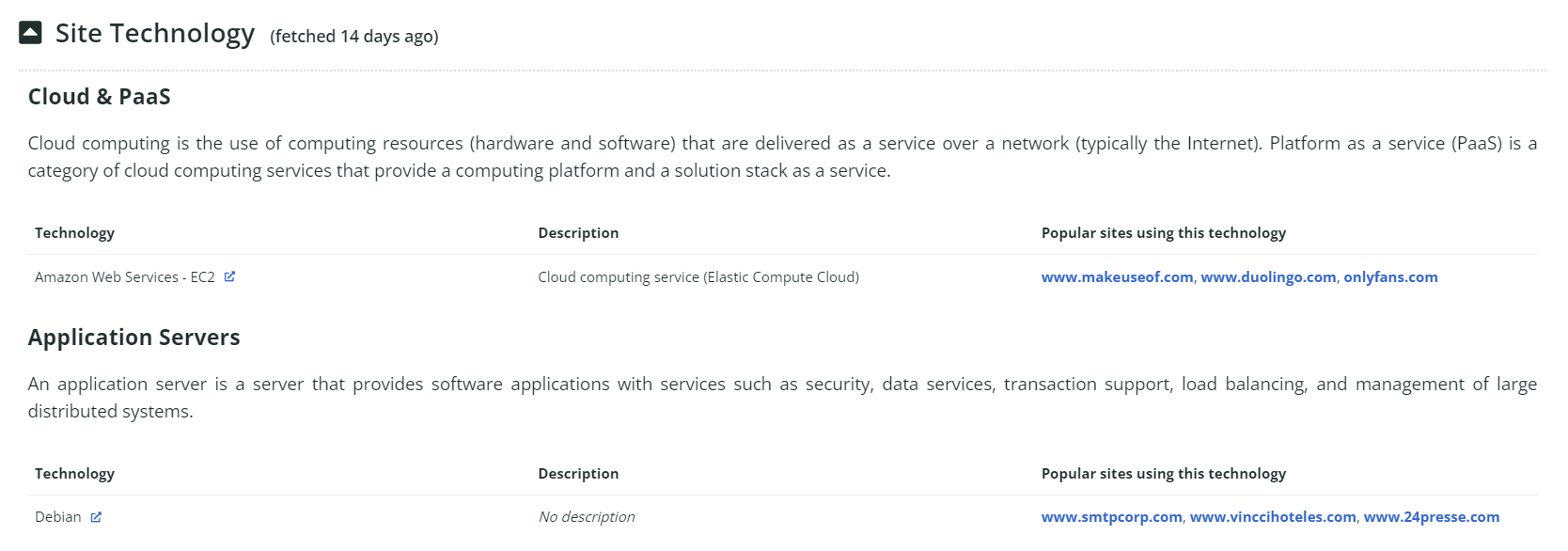
DNSSEC: unsigned





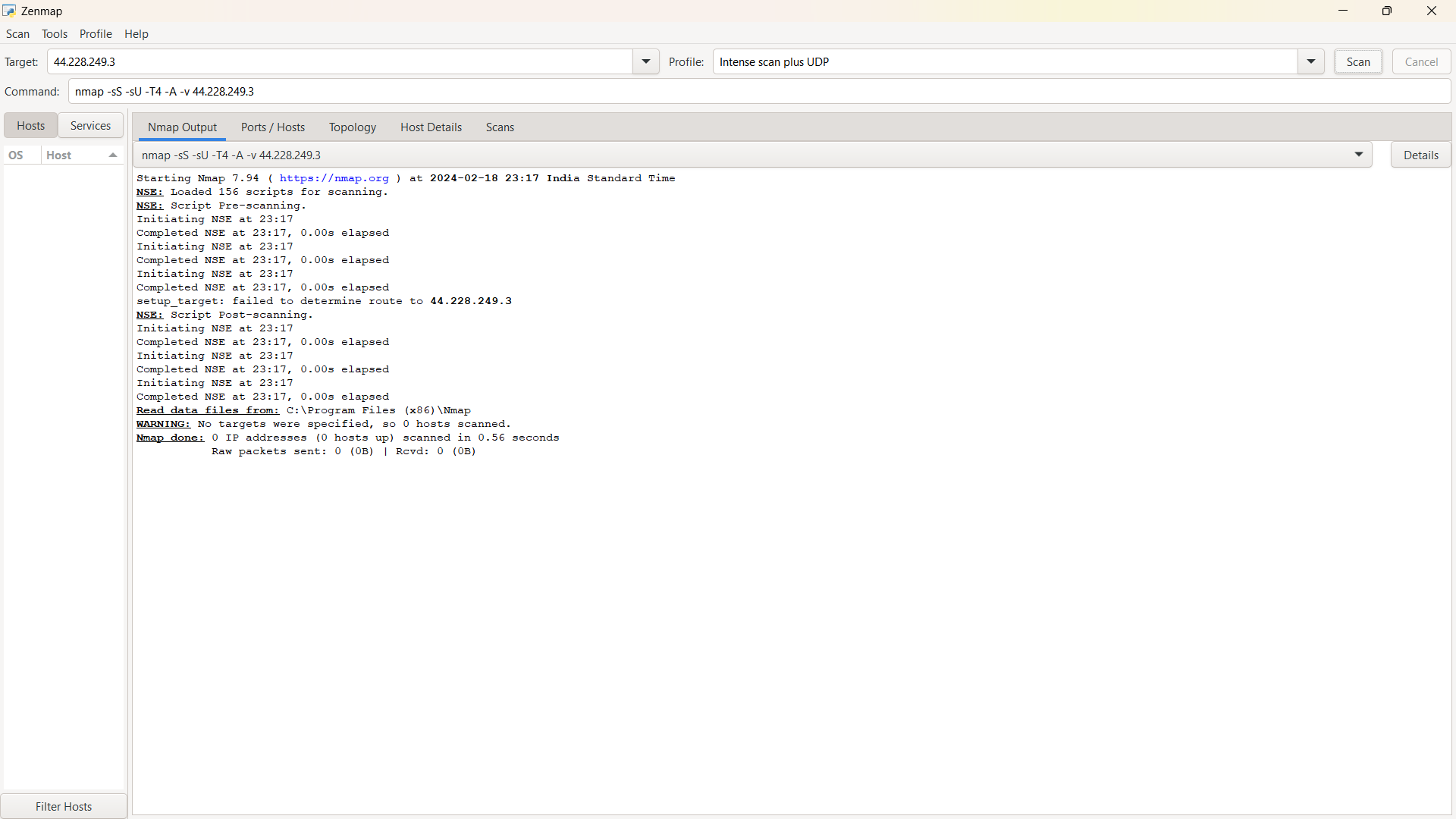


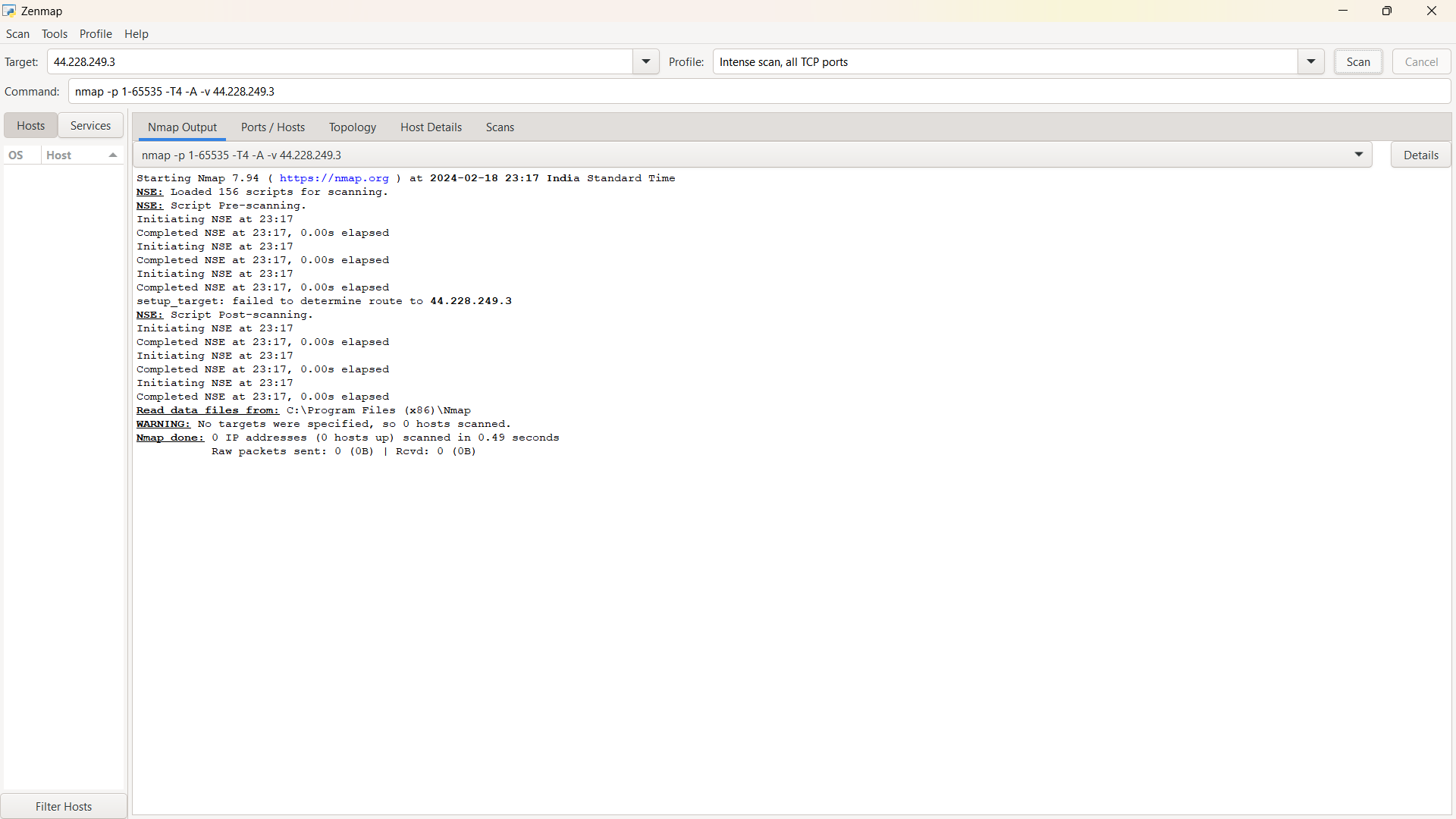


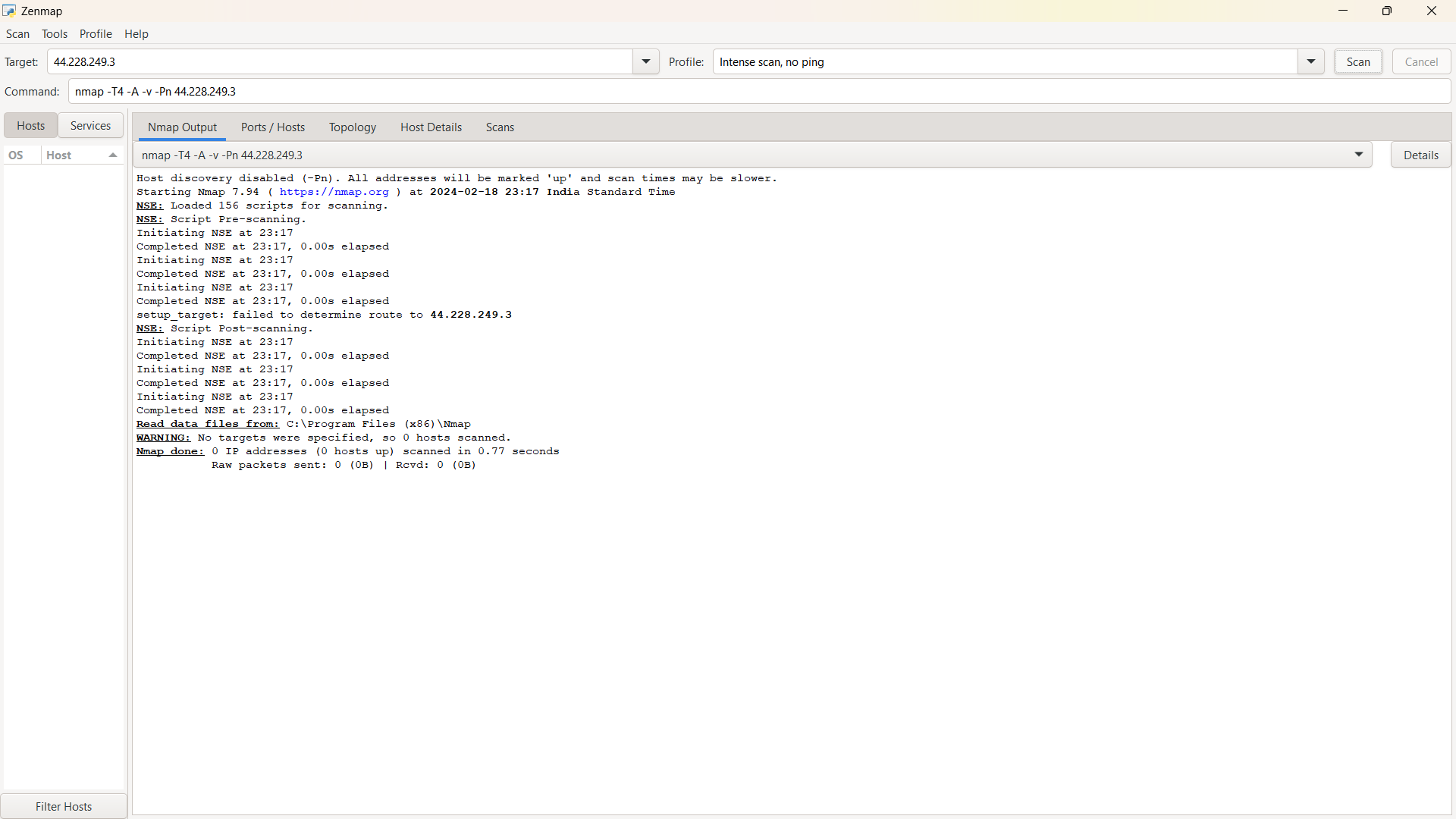


**Using Nmap Tool**

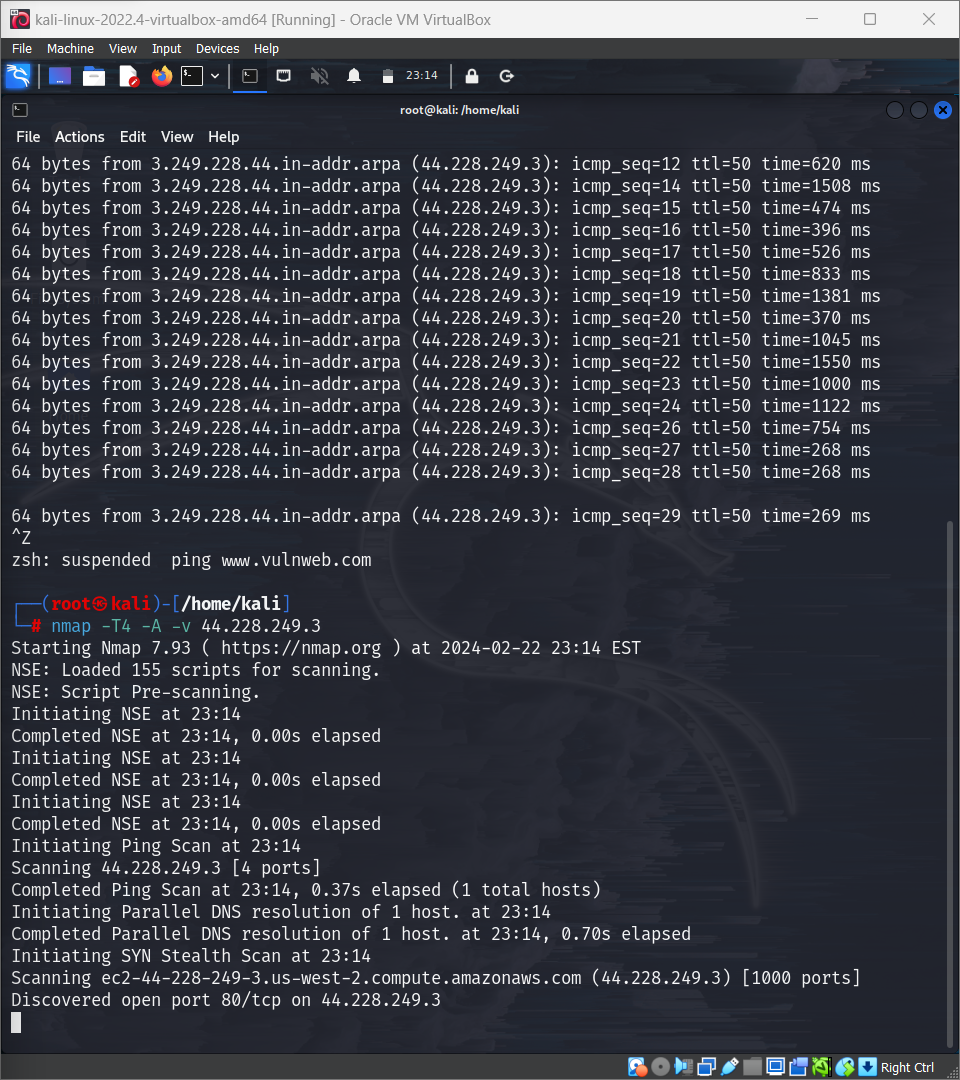
Intense Scan

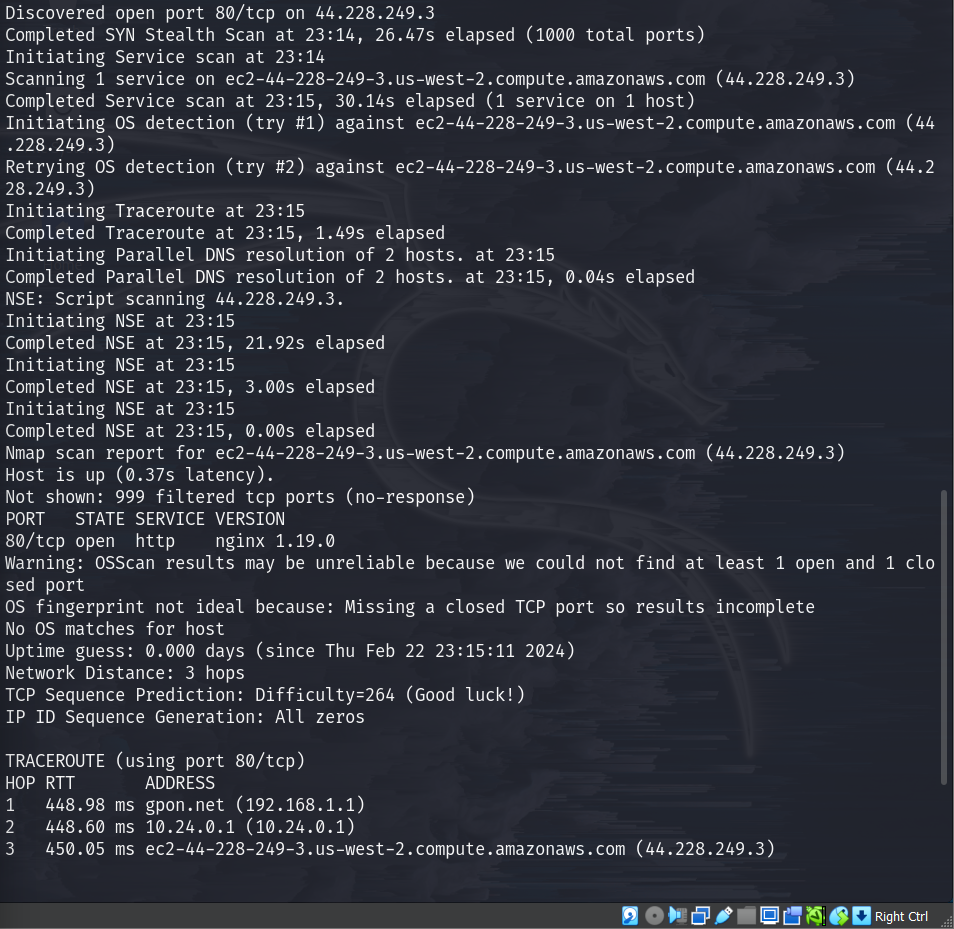
****

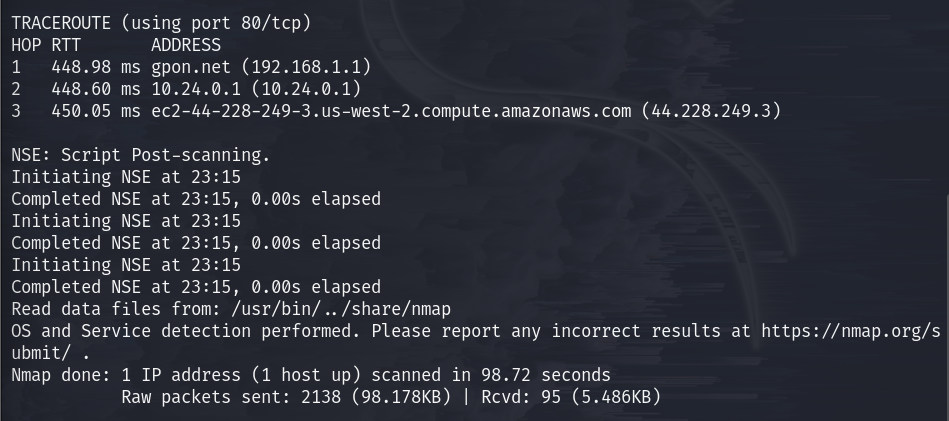
****

****

**In Kali linux Nmap**

****

****

****