FOOTPRINTING AND RECONNAISSANCE

KRISHNA SATHVIKA GANNI
4TH YEAR,B.TECH
RCEE

FOOTPRINTING:

- ➔ Footprinting, also known as fingerprinting, is a methodology used by penetration testers, cybersecurity professionals, and even threat actors to gather information about a target organization to identify potential vulnerabilities.
- ➔ Footprinting is the first step in penetration testing. It is one of the best methods of finding vulnerabilities.
- ➔ The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners.
- ➔ This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.
- ➔ There are two types of Footprinting that can be used: active Footprinting and passive Footprinting.

RECONNAISSANCE:

- ➔ Reconnaissance, often referred to as 'cyber reconnaissance' or 'cyber intelligence gathering', is the process of collecting information about potential targets, vulnerabilities, and attack vectors.
- ➔ Reconnaissance refers to a set of processes and techniques, such as footprinting and scanning and enumeration, that are used to gather and covertly discover as much information as possible about a target system.
- ➔ Reconnaissance is an essential step in locating and stealing confidential

information. In a proper recon, attackers would have access to detailed information.

- ➔ In this way, reconnaissance, in information security, is used for penetration testing. To gain information without actively engaging with the network, an attacker uses recon to interact with the network's open ports, running services, etc.
- ➔ The information it provides can help gain access to networks beyond the internet.

STEPS:

Step 1: Access the Target Website Open a web browser (Chrome, Firefox, Safari, etc.).

- ➔ In the address bar, paste the URL: http://testphp.vulnweb.com/ and press Enter.

Step 2: Footprinting and Reconnaissance

- ➔ **WHOIS Lookup:** Use tools like WHOIS to gather information about the domain registration, including the owner's contact details and registration date.
- ➔ **Google Dorking:** Utilize specific search queries on Google to find sensitive information, files, or vulnerabilities associated with the target website.
- ➔ **Website Analysis Tools:** Employ tools like BuiltWith or Wappalyzer to identify technologies, frameworks, and plugins used on the website.
- ➔ **Social Engineering:** Gather information through social media platforms or other online sources to learn about the organization, its employees, and potential vulnerabilities.

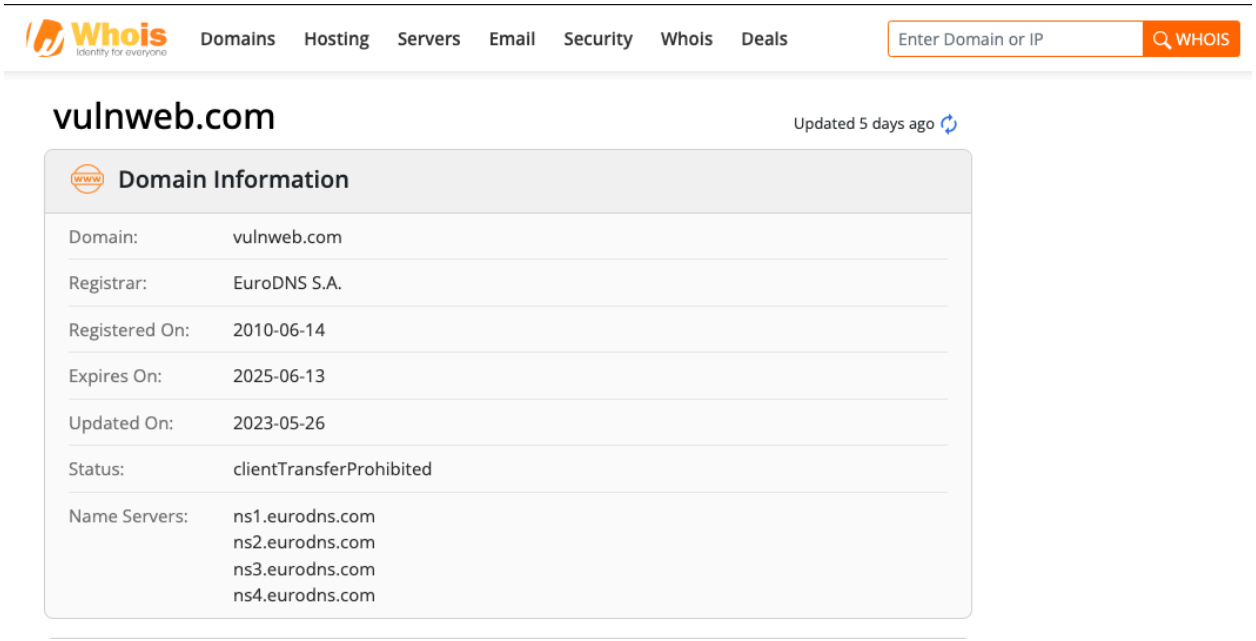
Step 3: Network Scanning with Nmap Install Nmap if you haven't already (you can download it from https://nmap.org/).

- ➔ Execute Nmap commands to scan the target website for open ports, services, and operating systems.
- ➔ Example command: nmap -A testphp.vulnweb.com

Step 4: Documentation

- ➔ Record all the information gathered during footprinting, reconnaissance, and Nmap scanning processes.
- ➔ Create a detailed report containing: Summary of findings Information about the target website (domain registration details, technologies used) Results of Nmap scans (open ports, services, OS detection) Observations and potential vulnerabilities Recommendations for mitigating identified risks

INFORMATION GATHERING IN WHOIS



Registrant Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com

Administrative Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com

Technical Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com

Raw Whois Data

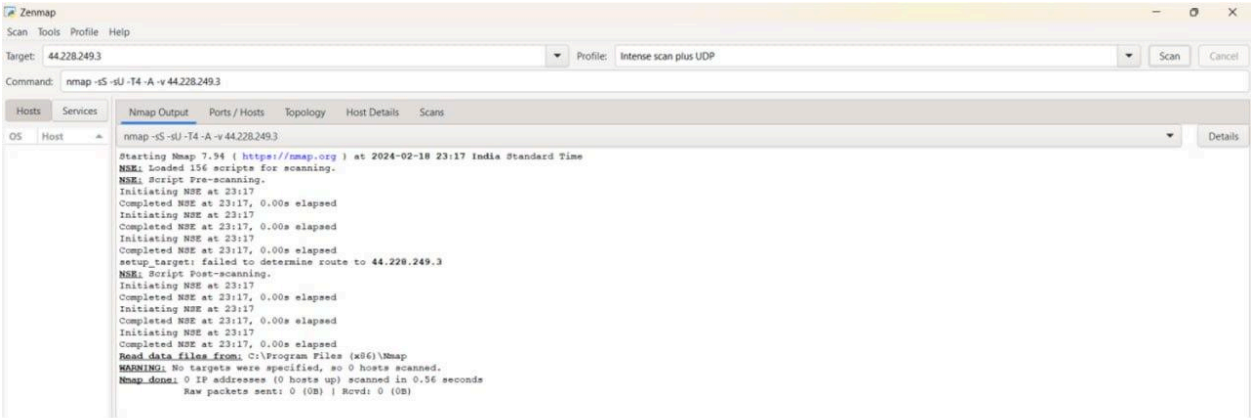
```
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@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
```

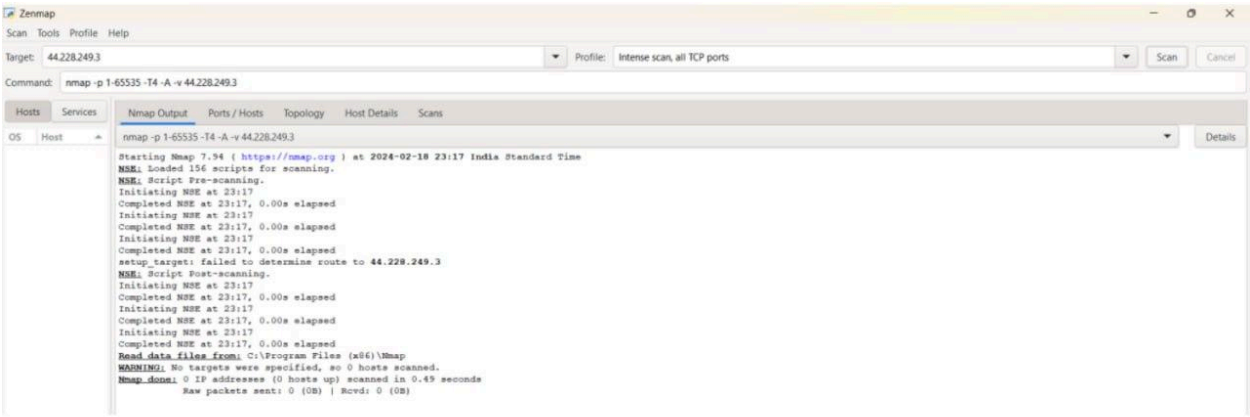
```
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@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: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-02-19T03:09:02Z <<<

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

Please email the listed admin email address if you wish to raise a legal issue.

The Data in EuroDNS WHOIS database is provided for information purposes only.
The fact that EuroDNS display such information does not provide any guarantee
expressed or implied on the purpose for which the database may be used, its
accuracy or usefulness. By submitting a WHOIS query, you agree that you will
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 (spam); or
(2) enable high volume, automated, electronic processes that apply to EuroDNS
(or its systems). EuroDNS reserves the right to modify these terms at any time.
```

```
By submitting this query, you agree to abide by the above policy.
```

NMAP


Zenmap
Scan Tools Profile Help
Target: 44.228.249.3
Profile: Intense scan plus UDP
Scan
Cancel
Command: nmap -sS -sU -T4 -A -v 44.228.249.3
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -sS -sU -T4 -A -v 44.228.249.3
Details
Starting Nmap 7.94 (https://nmap.org) at 2024-02-18 23:17 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
setup_target: failed to determine route to 44.228.249.3
NSE: Script Post-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.56 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)


Zenmap
Scan Tools Profile Help
Target: 44.228.249.3
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 44.228.249.3
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -p 1-65535 -T4 -A -v 44.228.249.3
Details
Starting Nmap 7.94 (https://nmap.org) at 2024-02-18 23:17 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
setup_target: failed to determine route to 44.228.249.3
NSE: Script Post-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.49 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)


Zenmap
Scan Tools Profile Help
Target: 44.228.249.3
Profile: Intense scan, no ping
Scan
Cancel
Command: nmap -T4 -A -v -Pn 44.228.249.3
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
nmap -T4 -A -v -Pn 44.228.249.3
Details
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94 (https://nmap.org) at 2024-02-18 23:17 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
setup_target: failed to determine route to 44.228.249.3
NSE: Script Post-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.77 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -T4 -A -v 44.228.249.3
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-22 23:14 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Initiating Ping Scan at 23:14
Scanning 44.228.249.3 [4 ports]
Completed Ping Scan at 23:14, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:14
Completed Parallel DNS resolution of 1 host. at 23:14, 0.70s elapsed
Initiating SYN Stealth Scan at 23:14
Scanning ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3) [1000 ports]
Discovered open port 80/tcp on 44.228.249.3
```

```
Discovered open port 80/tcp on 44.228.249.3
Completed SYN Stealth Scan at 23:14, 26.47s elapsed (1000 total ports)
Initiating Service scan at 23:14
Scanning 1 service on ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Completed Service scan at 23:15, 30.14s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44
.228.249.3)
Retrying OS detection (try #2) against ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.2
28.249.3)
Initiating Traceroute at 23:15
Completed Traceroute at 23:15, 1.49s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 23:15
Completed Parallel DNS resolution of 2 hosts. at 23:15, 0.04s elapsed
NSE: Script scanning 44.228.249.3.
Initiating NSE at 23:15
Completed NSE at 23:15, 21.92s elapsed
Initiating NSE at 23:15
Completed NSE at 23:15, 3.00s elapsed
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.37s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.000 days (since Thu Feb 22 23:15:11 2024)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   448.98 ms gpon.net (192.168.1.1)
2   448.60 ms 10.24.0.1 (10.24.0.1)
3   450.05 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

Right Ctrl

```
TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   448.98 ms gpon.net (192.168.1.1)
2   448.60 ms 10.24.0.1 (10.24.0.1)
3   450.05 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

NSE: Script Post-scanning.
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.72 seconds
           Raw packets sent: 2138 (98.178KB) | Rcvd: 95 (5.486KB)
```