Assignment - 2

Footprinting and Reconnaissance

Introduction:

The processes of footprinting and reconnaissance are critical initial steps in assessing and understanding an organization's digital infrastructure. These proactive measures involve gathering information about a target system or network with the intention of identifying potential vulnerabilities and entry points for unauthorized access. This document aims to provide an overview of footprinting and reconnaissance, their methodologies, tools, and the importance of ethical considerations in conducting these activities.

Footprinting:

Footprinting is the initial phase of the information gathering process, where an attacker seeks to uncover details about a target's network, infrastructure, and online presence. The primary objective is to gather as much information as possible without directly interacting with the target system.

Methodologies:

1. Passive Footprinting: This involves collecting information through publicly available sources such as search engines, social media platforms, company websites, and public records. Passive footprinting aims to gather data without alerting the target organization.

2. Active Footprinting: In contrast to passive techniques, active footprinting involves directly interacting with the target system to gather information. This may include techniques such as port scanning, network sniffing, and reconnaissance using tools like Nmap, Wireshark, and Shodan.

Tools

Whois Lookup: Retrieves domain registration information.

Nslookup: Queries DNS servers for DNS information.

Google Dorks: Uses advanced search techniques to locate specific types of information on Google.

Social Engineering: Exploits human behavior to gather information through techniques such as phishing and pretexting.

Reconnaissance:

Definition

Reconnaissance, often referred to as recon, is the process of actively scanning and probing a target system or network to gather detailed information about its architecture, services, and potential vulnerabilities. Unlike footprinting, reconnaissance involves more direct interaction with the target, potentially leading to detection.

Methodologies

1. Network Scanning: Involves scanning the target network to identify active hosts, open ports, and services running on those ports. Tools like Nmap and Nessus are commonly used for network scanning.

2. Vulnerability Scanning: Once the network is mapped, vulnerability scanning tools such as OpenVAS and Nexpose are used to identify known vulnerabilities in the target's software and configuration.

3. Packet Sniffing: Involves capturing and analyzing network traffic to gather information such as usernames, passwords, and other sensitive data.

Tools

- Nmap: A powerful open-source network scanning tool.

- Wireshark: A widely used packet sniffing tool for network analysis.

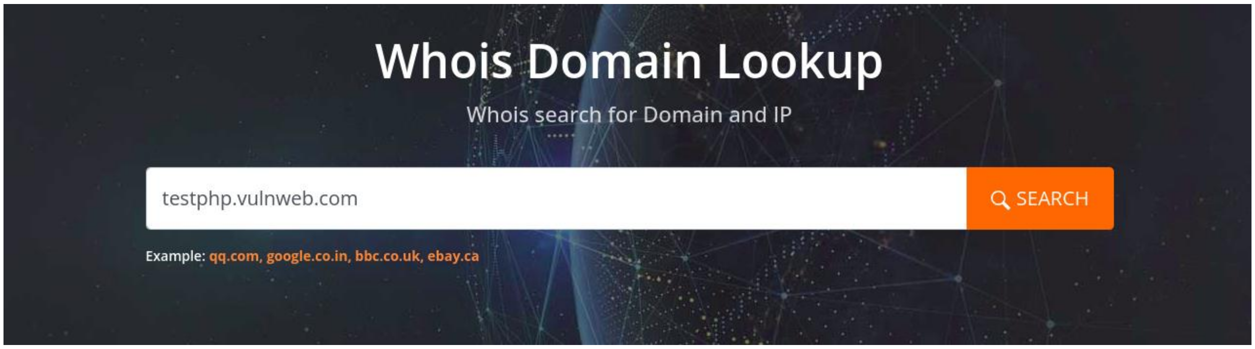
- Shodan: A search engine for internet-connected devices, including servers, routers, and IoT devices.

About testphp.vulnweb.com

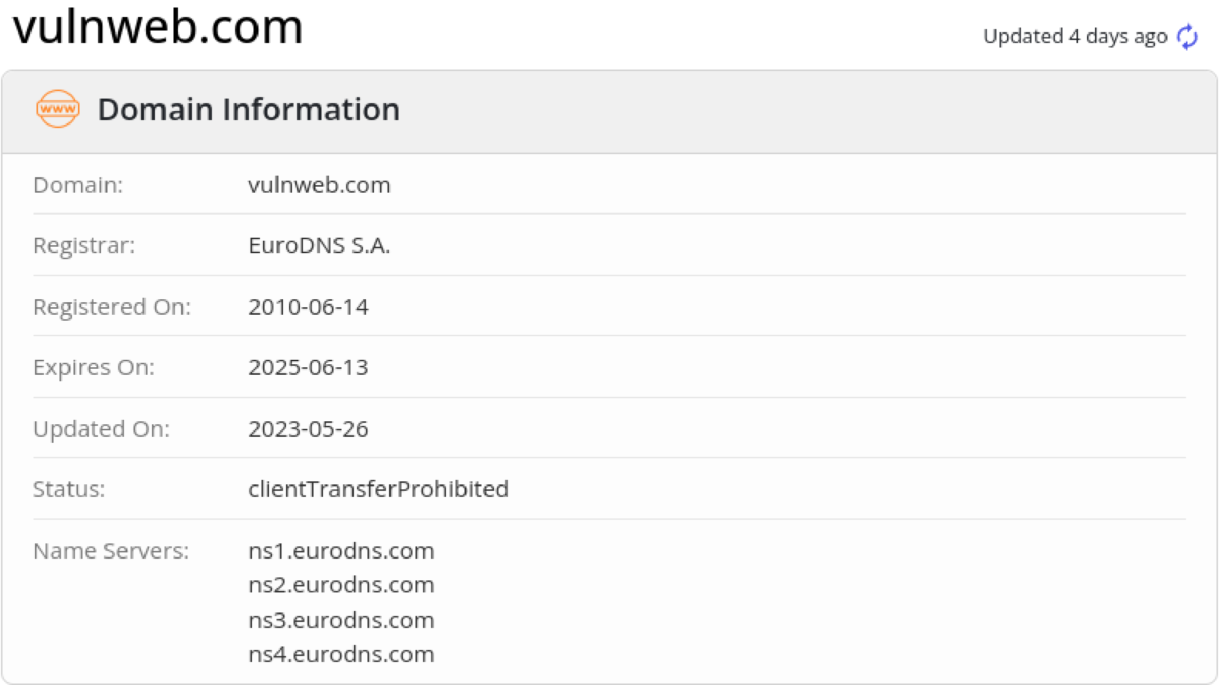
http://testphp.vulnweb.com/ is a purposely vulnerable web application designed for educational and testing purposes. It serves as a platform for cybersecurity professionals, students, and enthusiasts to practice and enhance their skills in identifying, exploiting, and mitigating web application vulnerabilities.

Screenshots of Passive Footprinting:

1. Whois Lookup:


Whois Domain Lookup
Whois search for Domain and IP
SEARCH
Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

testphp.vulnweb.com



vulnweb.com

Updated 4 days ago

Domain Information

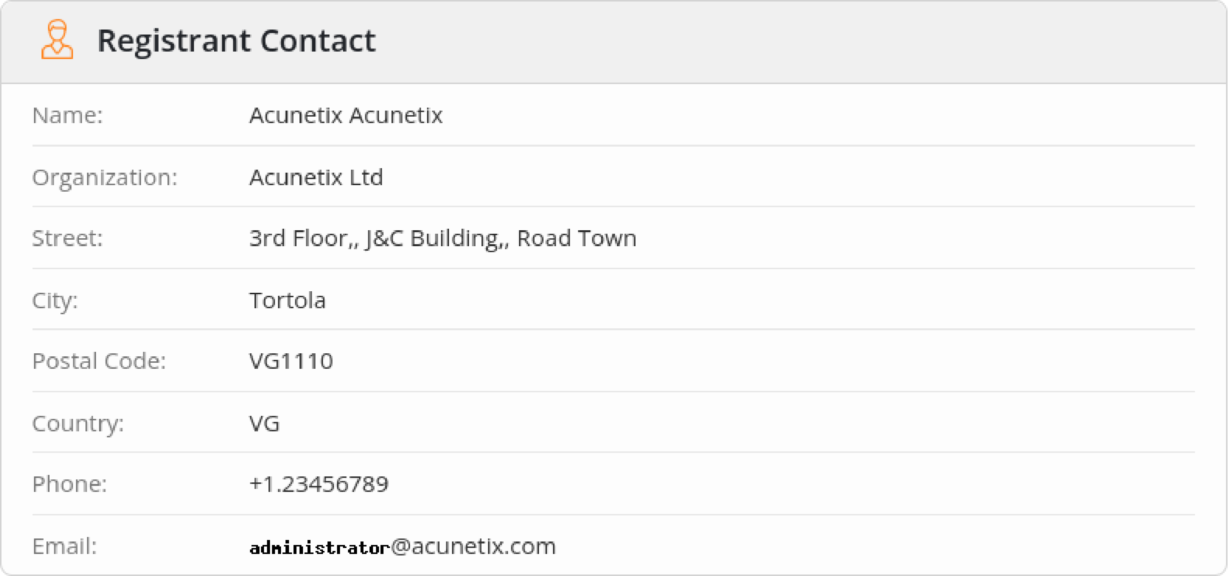
Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2025-06-13
Updated On:	2023-05-26
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

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

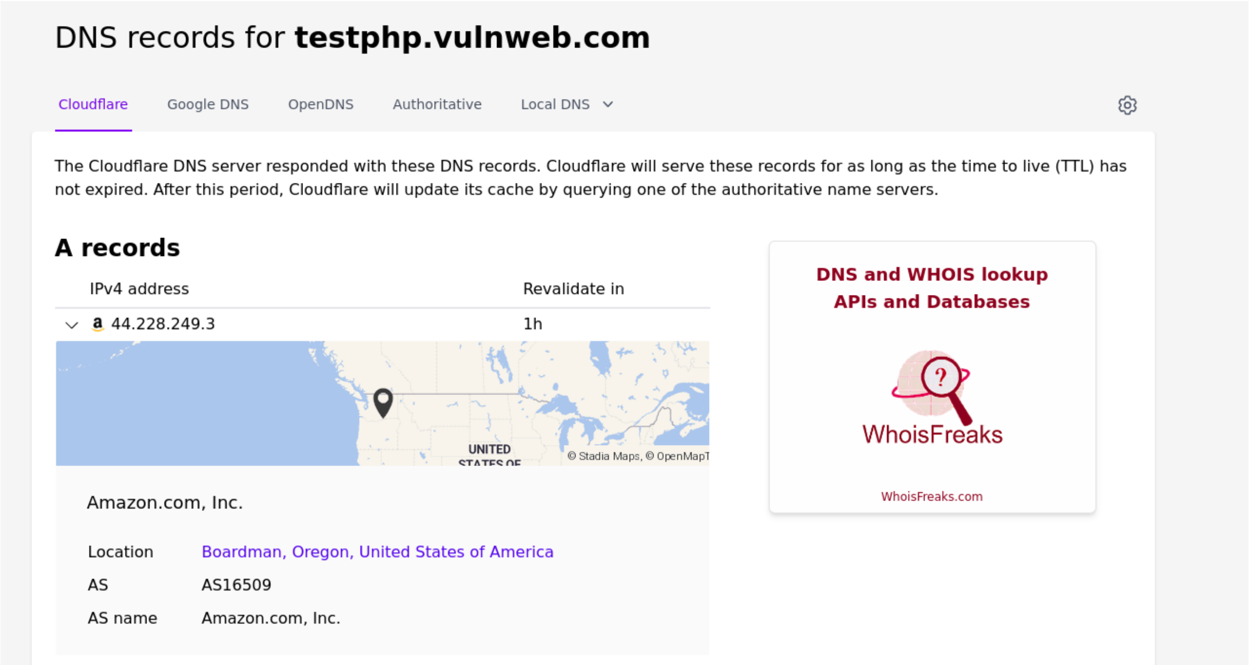
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com



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

2.Nslookup:



DNS records for **testphp.vulnweb.com**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

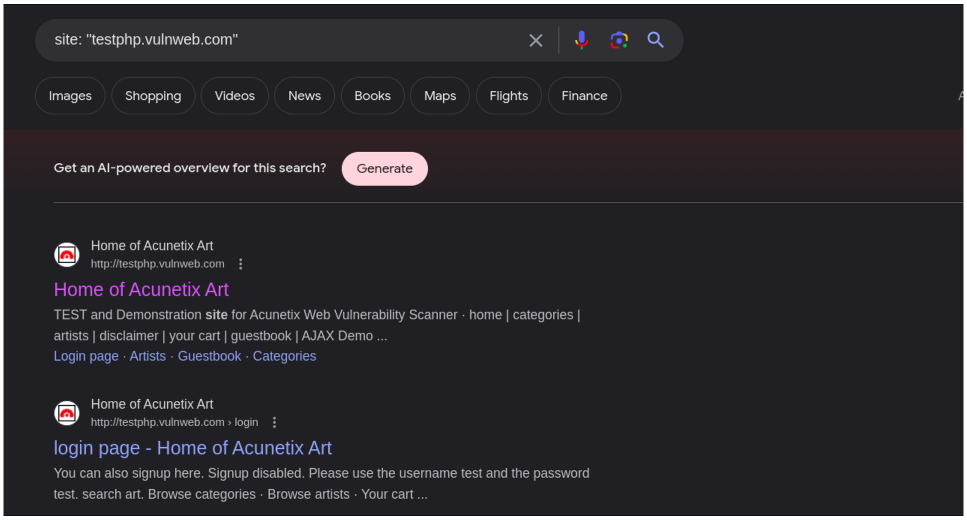
A records

IPv4 address	Revalidate in
a 44.228.249.3	1h

Amazon.com, Inc.

Location	Boardman, Oregon, United States of America
AS	AS16509
AS name	Amazon.com, Inc.

3.Google Dorks:



site: "testphp.vulnweb.com"

Get an AI-powered overview for this search?

Home of Acunetix Art
http://testphp.vulnweb.com

Home of Acunetix Art

TEST and Demonstration **site** for Acunetix Web Vulnerability Scanner · home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo ...

Login page · Artists · Guestbook · Categories

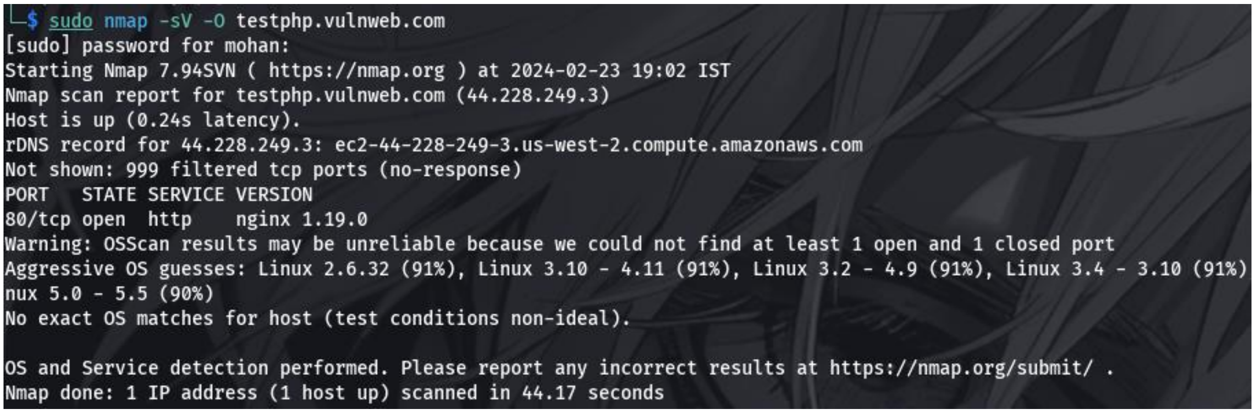
Home of Acunetix Art
http://testphp.vulnweb.com › login

login page - Home of Acunetix Art

You can also signup here. Signup disabled. Please use the username test and the password test. search art. Browse categories · Browse artists · Your cart ...

Screenshots of Active Footprinting:

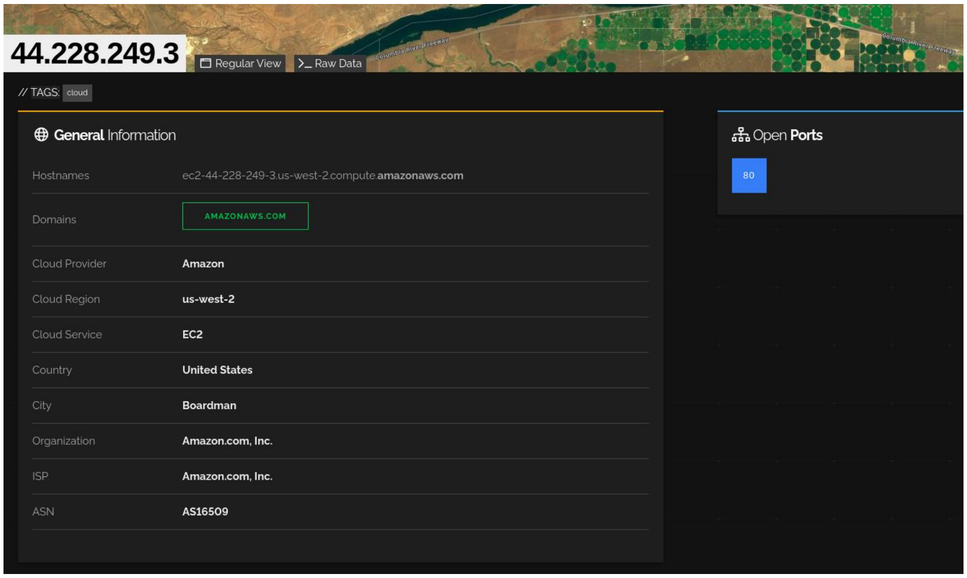
1. Nmap:



```
└─$ sudo nmap -sV -O testphp.vulnweb.com
[sudo] password for mohan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 19:02 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.24s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
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 closed port
Aggressive OS guesses: Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%)
nux 5.0 - 5.5 (90%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.17 seconds
```

2. Shodan:



44.228.249.3

// TAGS: cloud

General Information

Hostnames	ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Domains	AMAZONAWS.COM
Cloud Provider	Amazon
Cloud Region	us-west-2
Cloud Service	EC2
Country	United States
City	Boardman
Organization	Amazon.com, Inc.
ISP	Amazon.com, Inc.
ASN	AS16509

Open Ports

80

Conclusion

Footprinting and reconnaissance are indispensable steps in the cybersecurity lifecycle, providing valuable insights into an organization's digital footprint and potential vulnerabilities. By understanding the methodologies, tools, and ethical considerations involved, cybersecurity professionals can conduct these activities effectively and responsibly, ultimately enhancing the overall security posture of the target organization.