Penetration Testing

Information Gathering

Table of Content

1. Information Gathering

1.1 Introduce Penetration Testing Lifecycle

1.2 Passive Information Gathering

1.3 Active Information Gathering

2. Vulnerability Scanning

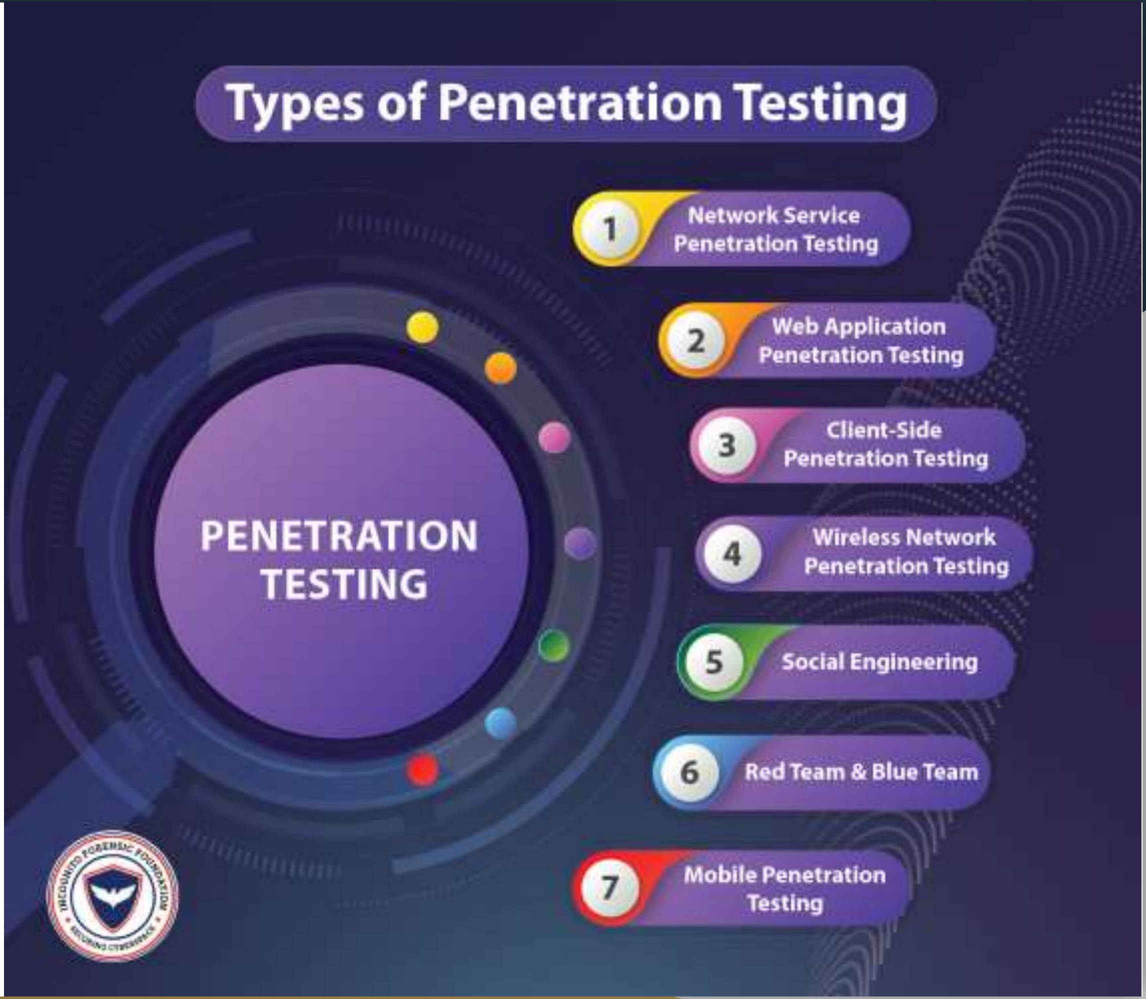
2.1 Vulnerability Scanning Theory

2.2 Vulnerability Scanning with Nmap

3. Osint technique and Use case

PENETRATION
TESTING

- Web Application Pentest
- Mobile Application Pentest
- Code Audit
- Red Team

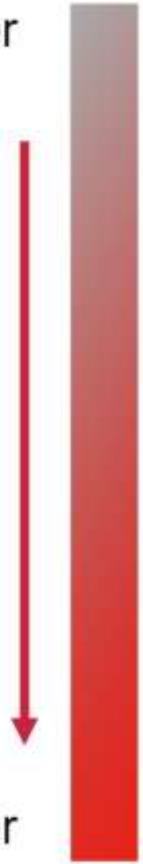


Types of Penetration Testing

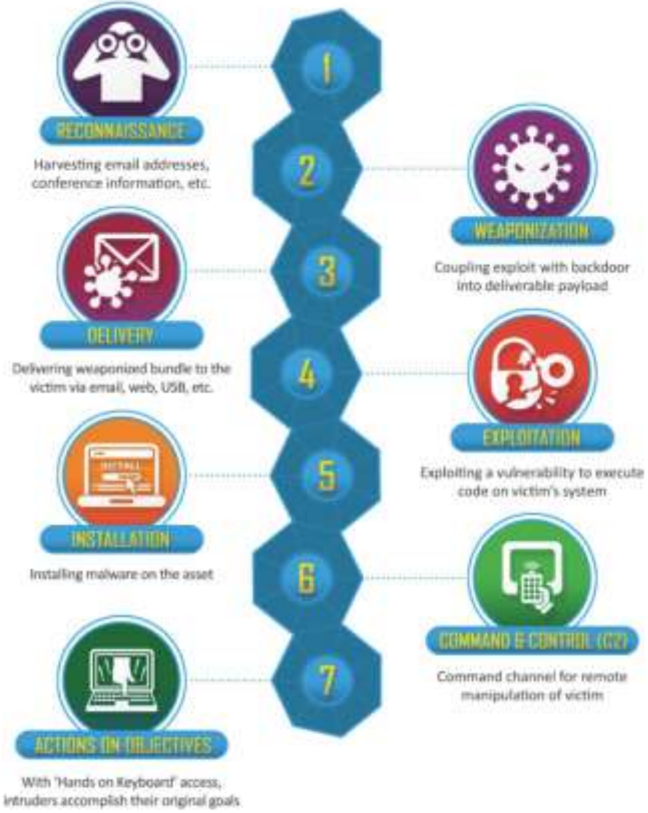
PENETRATION TESTING

1. Network Service Penetration Testing
2. Web Application Penetration Testing
3. Client-Side Penetration Testing
4. Wireless Network Penetration Testing
5. Social Engineering
6. Red Team & Blue Team
7. Mobile Penetration Testing

Pentester



Red Teamer



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

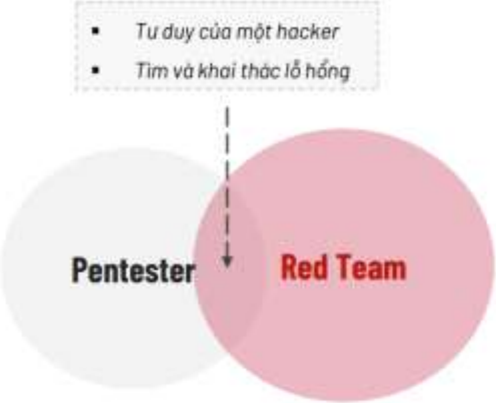
Exploit để xác định mức độ nguy hiểm
Tìm nhiều lỗi nhất có thể

Blackbox / Graybox / Whitebox
Tốc chiến, pentest nhanh, tìm hết lỗi

Một dự án kéo dài trong vài tuần

Khai thác và tái hiện một lỗ hổng cụ thể
Thường chỉ trong phạm vi của:

- Một ứng dụng
- Một hệ thống



- *Tư duy của một hacker*
- *Tìm và khai thác lỗ hổng*

Red Team là một level nâng cấp của Pentester

Đóng vai kẻ thù (adversary) để tấn công
Test khả năng Detection & Response

Blackbox hoàn toàn!
Chậm, chắc, tránh 'rút dây động rừng'

Một dự án có thể kéo dài từ vài tuần cho đến **03+ tháng**

Xâu chuỗi lỗi để đánh úp toàn bộ system
Phạm vi bao quát:

- Con người, máy tính, server...
- Tiền bạc, dữ liệu, uy tín...

The Penetration Testing Lifecycle

- Defining the Scope
- Information Gathering/Reconnaissance
- Vulnerability Detection
- Initial Foothold
- Privilege Escalation
- Lateral Movement
- Reporting/Analysis
- Lessons Learned/Remediation

Information Gathering/Reconnaissance

- Retrieve details about the target organization's infrastructure, assets, and personnel.
- Passive & Active
- Building our knowledge of the target's attack surface

WHY
WHEN
HOW

WHAT
WHERE

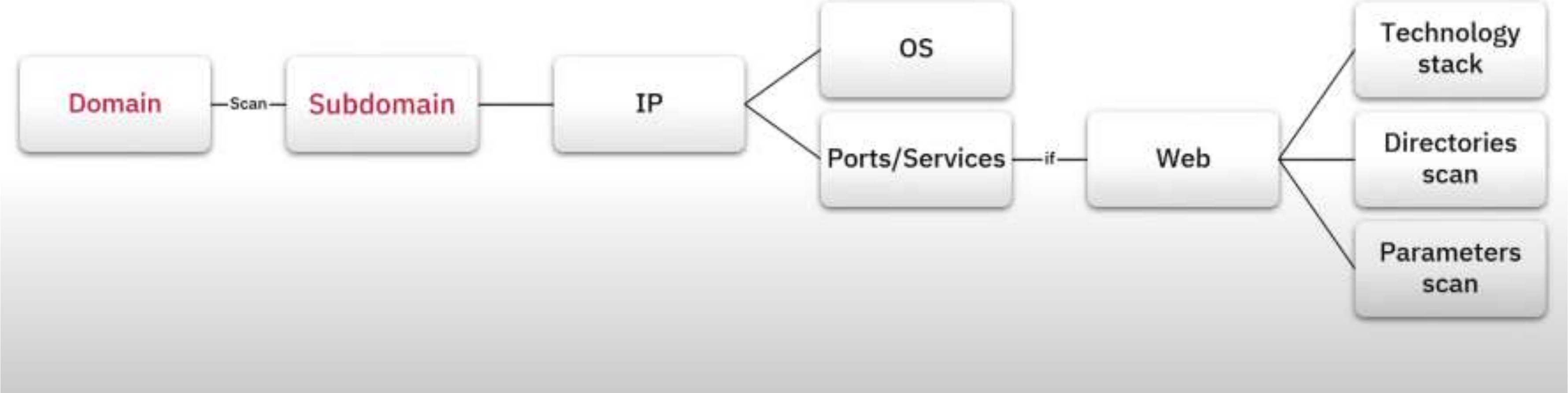
WHAT???

- Language code, server protocol
- Function, API
- Library, Third-party
- OS, IP range, Port, Service
- Subdomain
- Email
- Credentials
- Source code
- …

WHERE

- OSINT
- Search engine
- HTTP Response Header
- Network packet
- …

Recon flow

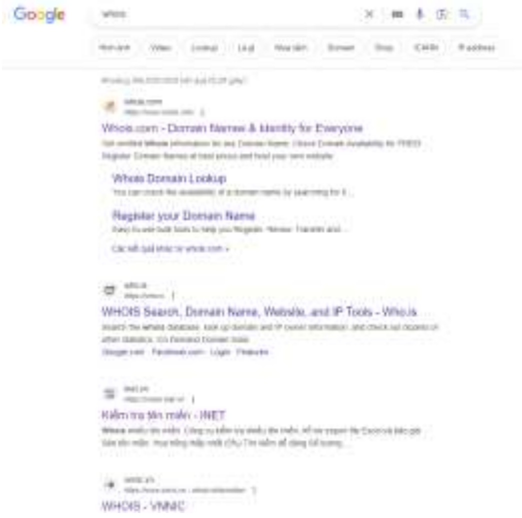

Domain
Scan
Subdomain
IP
OS
Ports/Services
if
Web
Technology stack
Directories scan
Parameters scan

Passive Information Gathering

Passive Information Gathering, also known as **Open-source Intelligence** (OSINT), is the process of collecting openly-available information about a target, generally without any direct interaction with that target.

Whois Enumeration

Whois is a TCP service, tool, and type of database that can provide information about a domain name, such as the name **server** and **registrar**.



whois

Whois.com - Domain Names & Identity for Everyone

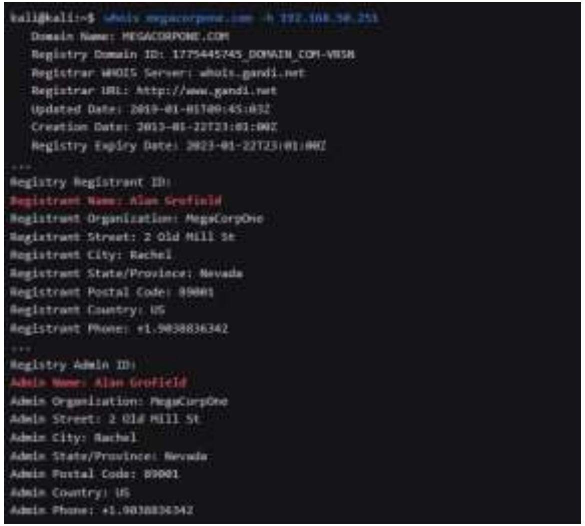
Whois Domain Lookup

Register your Domain Name

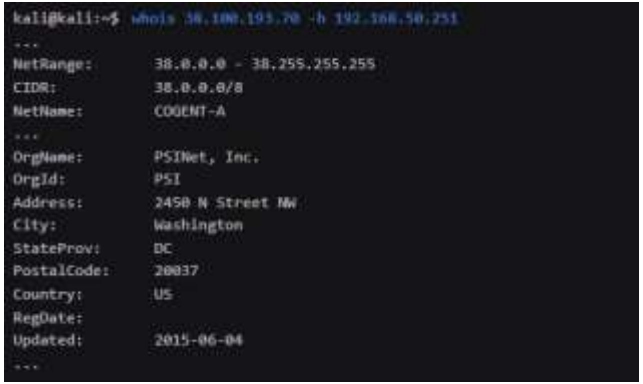
WHOIS Search, Domain Name, Website, and IP Tools - Who.is

Kiểm tra tên miền - INET

WHOIS - VNNIC

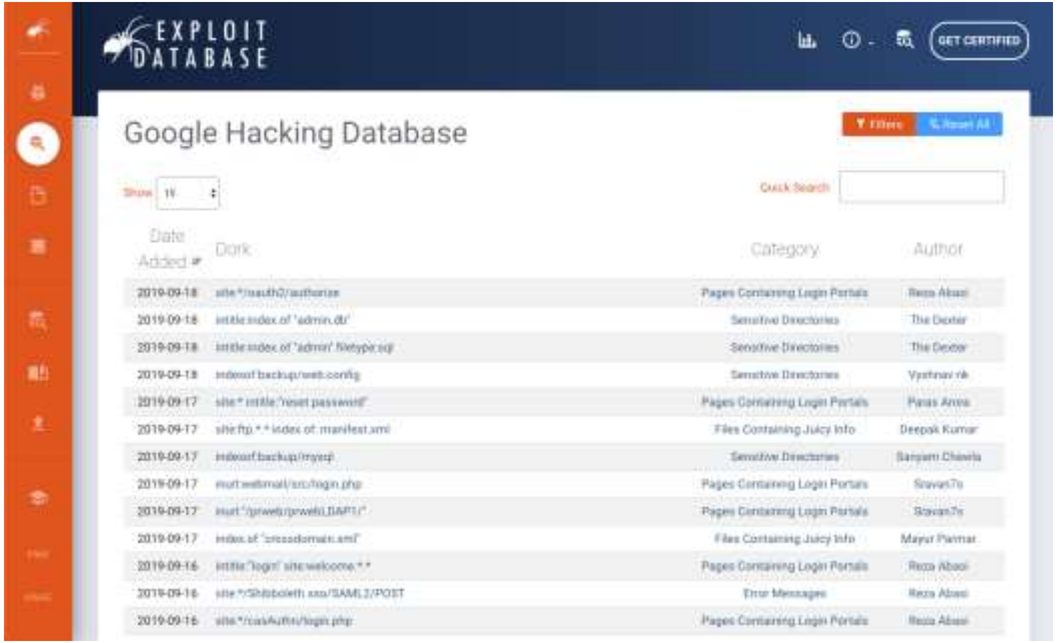


```
kali@kali:~$ whois megacorpone.com -h 192.168.50.251
   Domain Name: MEGACORPONE.COM
   Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gandi.net
   Registrar URL: http://www.gandi.net
   Updated Date: 2019-01-01T09:45:03Z
   Creation Date: 2013-01-22T23:01:00Z
   Registry Expiry Date: 2023-01-22T23:01:00Z
...
Registry Registrant ID:
Registrant Name: Alan Grofield
Registrant Organization: MegaCorpOne
Registrant Street: 2 Old Mill St
Registrant City: Rachel
Registrant State/Province: Nevada
Registrant Postal Code: 89001
Registrant Country: US
Registrant Phone: +1.9038836342
...
Registry Admin ID:
Admin Name: Alan Grofield
Admin Organization: MegaCorpOne
Admin Street: 2 Old Mill St
Admin City: Rachel
Admin State/Province: Nevada
Admin Postal Code: 89001
Admin Country: US
Admin Phone: +1.9038836342
```



```
kali@kali:~$ whois 38.100.193.70 -h 192.168.50.251
...
NetRange:       38.0.0.0 - 38.255.255.255
CIDR:           38.0.0.0/8
NetName:        COGENT-A
...
OrgName:        PSINet, Inc.
OrgId:          PSI
Address:        2450 N Street NW
City:           Washington
StateProv:      DC
PostalCode:     20037
Country:        US
RegDate:
Updated:        2015-06-04
...
```

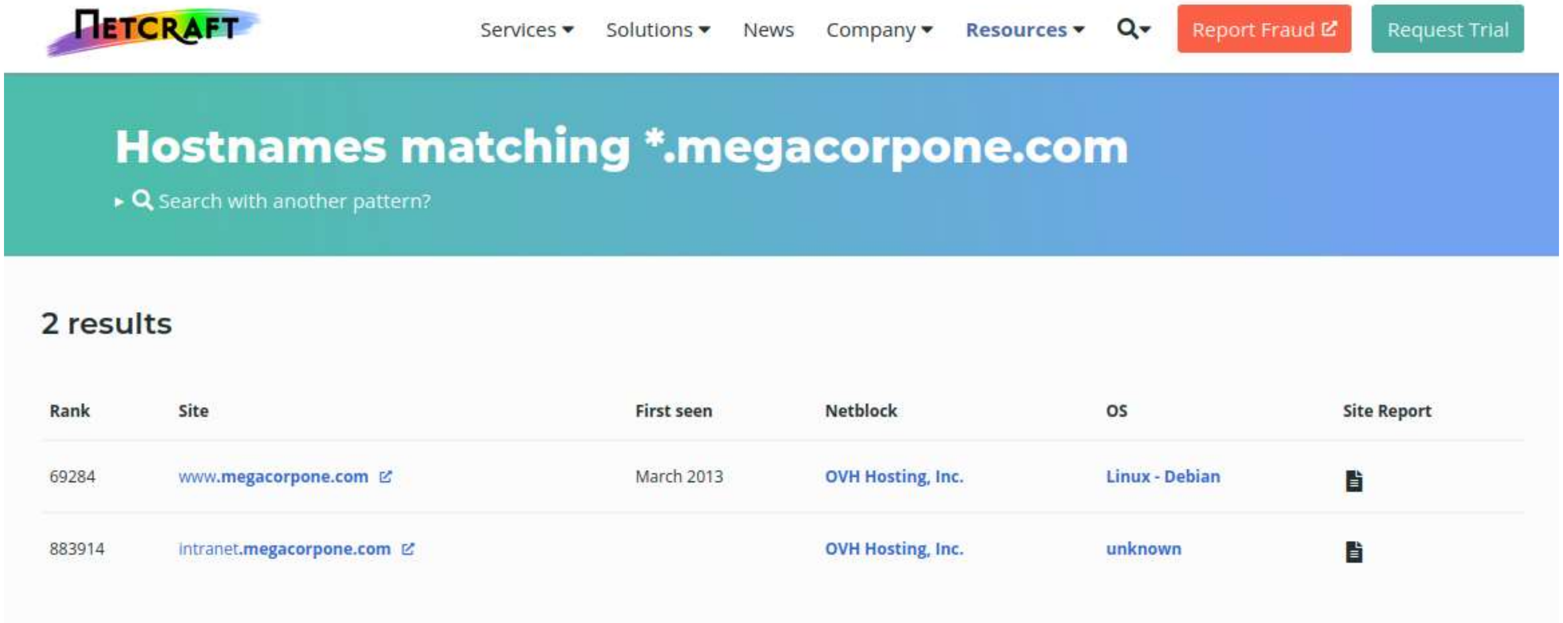
Google Hacking



Google Hacking Database

Date Added	Dork	Category	Author
2019-09-18	site:*/oauth2/authorize	Pages Containing Login Portals	Reza Abasi
2019-09-18	intitle:index.of "admin.db"	Sensitive Directories	The Dexter
2019-09-18	intitle:index.of "admin" filetype:sql	Sensitive Directories	The Dexter
2019-09-18	indexof:backup/web.config	Sensitive Directories	Vyshnav nk
2019-09-17	site:* intitle:"reset password"	Pages Containing Login Portals	Paras Arora
2019-09-17	site:ftp.*.* index of: manifest.xml	Files Containing Juicy Info	Deepak Kumar
2019-09-17	indexof:backup/mysql	Sensitive Directories	Sanyam Chawla
2019-09-17	inurl:webmail/src/login.php	Pages Containing Login Portals	Sravan7s
2019-09-17	inurl:"/prweb/prwebLDAP1/"	Pages Containing Login Portals	Sravan7s
2019-09-17	index.of "crossdomain.xml"	Files Containing Juicy Info	Mayur Parmar
2019-09-16	intitle:"login" site:welcome.*.*	Pages Containing Login Portals	Reza Abasi
2019-09-16	site:*/Shibboleth.sso/SAML2/POST	Error Messages	Reza Abasi
2019-09-16	site:*/casAuth/login.php	Pages Containing Login Portals	Reza Abasi

Netcraft



Hostnames matching *.megacorpone.com

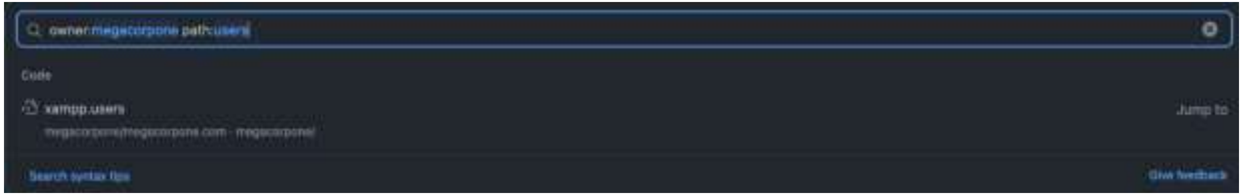
▸ Search with another pattern?

2 results

Rank	Site	First seen	Netblock	OS	Site Report
69284	www.megacorpone.com	March 2013	OVH Hosting, Inc.	Linux - Debian	🗎
883914	intranet.megacorpone.com		OVH Hosting, Inc.	unknown	🗎

Open-Source Code

- Github, GitLab, SourceForge, …
- Some open-source tools: Gitrob, Gitleaks, …

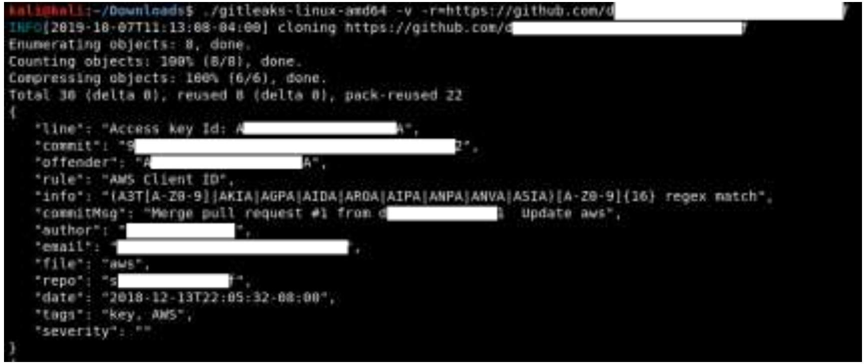


owner:megacorpone path:users

Code

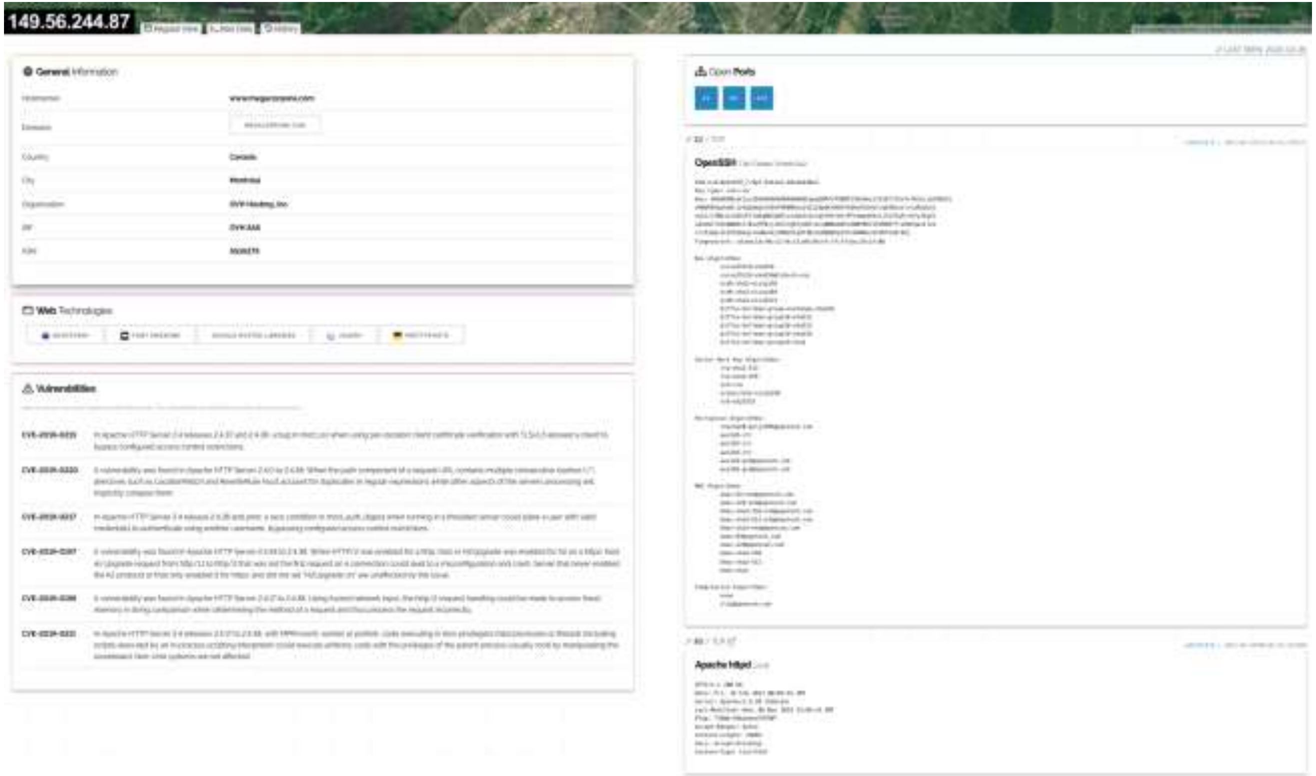
xampp.users

megacorpone/megacorpone.com · megacorpone/



```
kali@kali:~/Downloads$ ./gitleaks-linux-amd64 -v -r=https://github.com/d[redacted]/
INFO[2019-10-07T11:13:08-04:00] cloning https://github.com/d[redacted]/
Enumerating objects: 8, done.
Counting objects: 100% (8/8), done.
Compressing objects: 100% (6/6), done.
Total 30 (delta 0), reused 8 (delta 0), pack-reused 22
{
    "line": "Access key Id: A[redacted]A",
    "commit": "9[redacted]2",
    "offender": "A[redacted]A",
    "rule": "AWS Client ID",
    "info": "(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16} regex match",
    "commitMsg": "Merge pull request #1 from d[redacted]1  Update aws",
    "author": "[redacted]",
    "email": "[redacted]",
    "file": "aws",
    "repo": "s[redacted]f",
    "date": "2018-12-13T22:05:32-08:00",
    "tags": "key, AWS",
    "severity": ""
}
```

Shodan



149.56.244.87

General Information

Hostnames	[illegible]
Domains	[illegible]
Country	Canada
City	Montreal
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	[illegible]

Web Technologies

Vulnerabilities

[illegible]	In Apache HTTP Server 2.4 releases [illegible]
[illegible]	A vulnerability was found in Apache HTTP Server [illegible]
[illegible]	In Apache HTTP Server 2.4 release [illegible]
[illegible]	A vulnerability was found in Apache HTTP Server [illegible]
[illegible]	A vulnerability was found in Apache HTTP Server [illegible]
[illegible]	In Apache HTTP Server 2.4 releases [illegible]

Open Ports

OpenSSH

Apache httpd

Active Information Gathering

Active information gathering is the process of collecting more information about the target network by directly interacting with the target.

DNS Enumeration

- Some of the most common types of DNS records include: NS, A, AAA, MX, PTR, CNAME, TXT, …
- DNSrecon, DNSenum

Port Scanning with Nmap

- -sS: SYN scanning && -sT: Full connect scan
- -sC: Nmap default scripts
- -sU: UDP scan
- -sn: network sweeping scan
- -p: scan with specific port (-p- all port)
- - -top-ports: the top 20 TCP ports
- -sV: Service identification
- -O: OS fingerprinting
- Output mode: -oX, -oN, -oG, -oA

```
sudo nmap -sC -sV -p- <host> -oA <file>
```

SMB Enumeration

```
sudo nmap -v -p 139,445 -oG smb.txt 192.168.50.1-254
sudo nbtscan -r 192.168.50.0/24
sudo nmap -v -p 139,445 --script smb-os-discovery 192.168.50.152
```

Tools

- **Amass**: Collect domain, subdomain
- **Subfinder**: find subdomain
- **Wappalyzer**: Technology stack
- **Gobuster, Dirbuster**: Directories scan
- **Ffuf**, **Wfuzz**: Directories scan
- **enum4linux, smbclient**: Enumeration SMB

Vulnerability Scanning

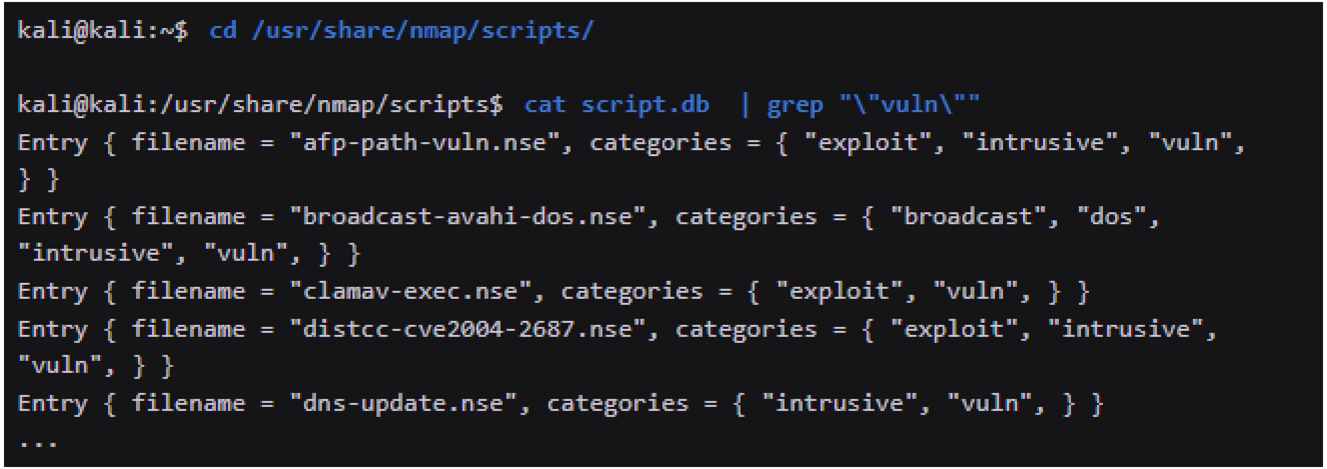
Acunetix
Burp Suite
GFI Software
FRONTLINE VM
nessus Professional
nexpose
OpenVAS
Open Vulnerability Assessment Scanner
tenable
Qualys.
CARSON & SAINT

Vulnerability Scanners Theory

How Vulnerability Scanners Work

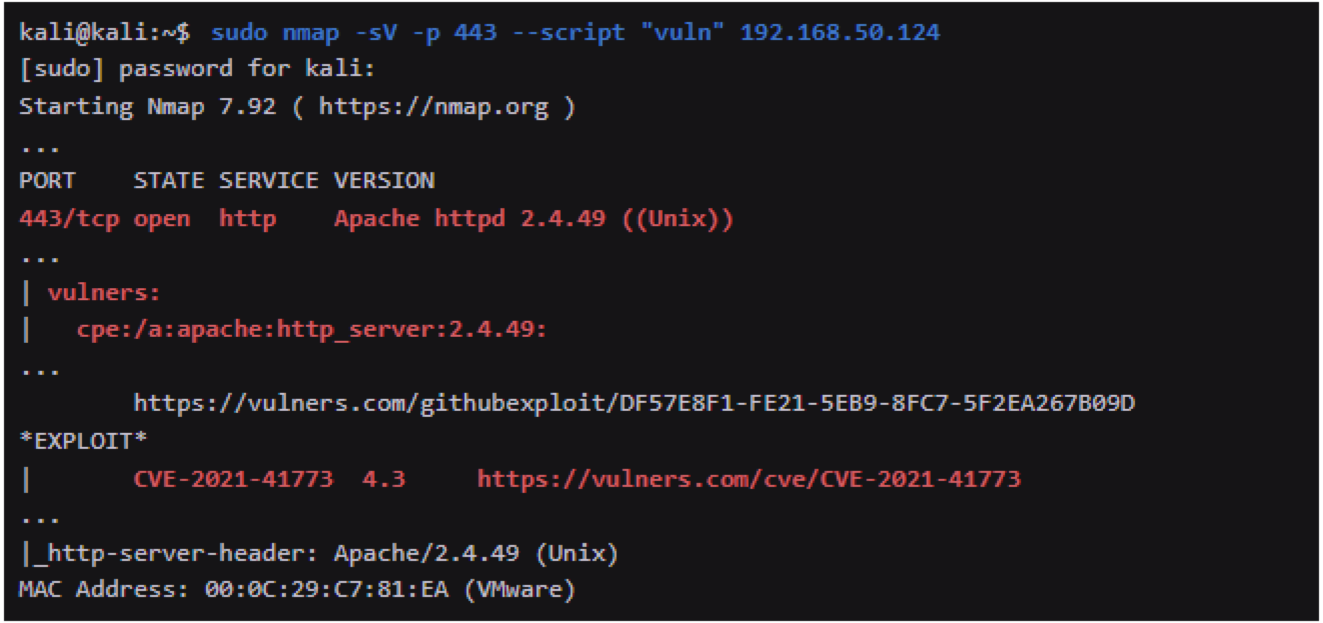
1. Host discovery
2. Port scanning
3. Operating system, service, and version detection
4. Matching the results to a vulnerability database

Vulnerability Scanning with Nmap



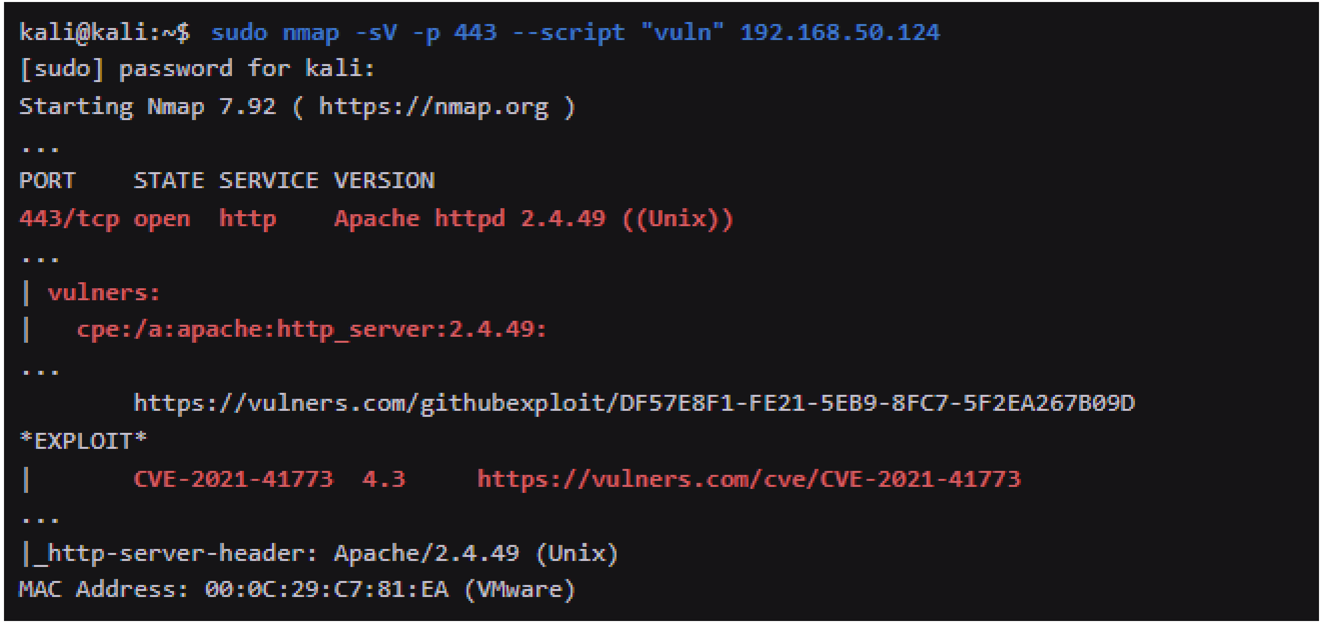
```
kali@kali:~$ cd /usr/share/nmap/scripts/

kali@kali:/usr/share/nmap/scripts$ cat script.db  | grep "\"vuln\""
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln",
} }
Entry { filename = "broadcast-avahi-dos.nse", categories = { "broadcast", "dos",
"intrusive", "vuln", } }
Entry { filename = "clamav-exec.nse", categories = { "exploit", "vuln", } }
Entry { filename = "distcc-cve2004-2687.nse", categories = { "exploit", "intrusive",
"vuln", } }
Entry { filename = "dns-update.nse", categories = { "intrusive", "vuln", } }
...
```

Vulnerability Scanning with Nmap



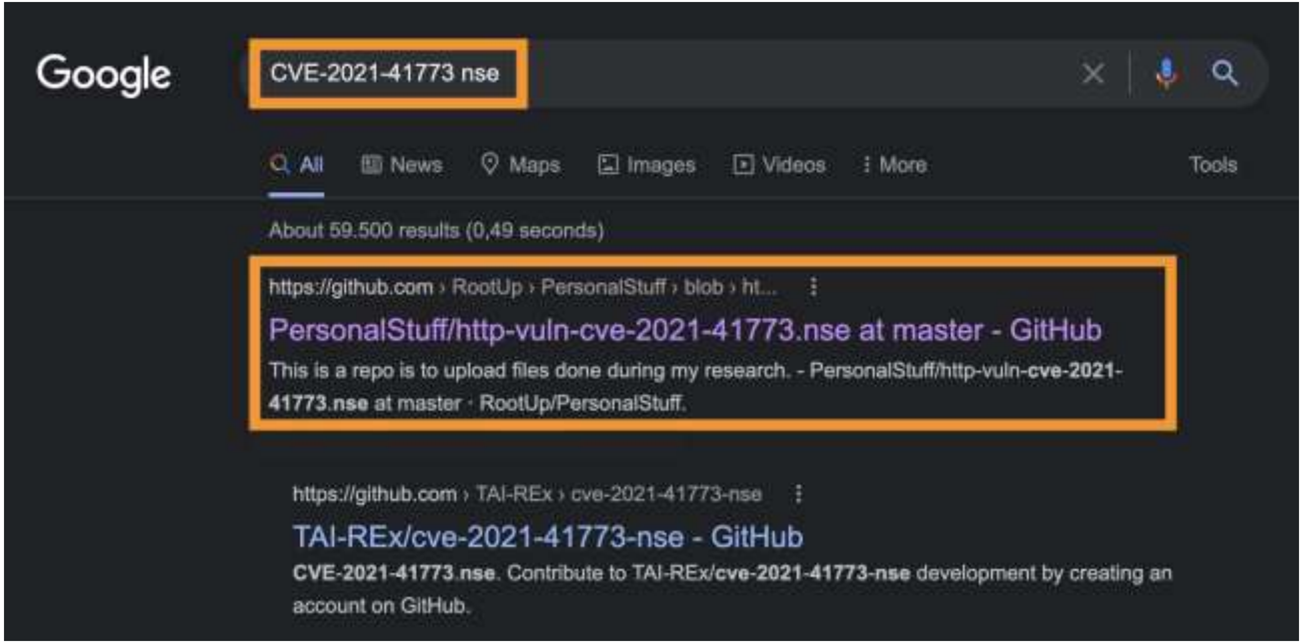
```
kali@kali:~$ sudo nmap -sV -p 443 --script "vuln" 192.168.50.124
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org )
...
PORT    STATE SERVICE VERSION
443/tcp open  http    Apache httpd 2.4.49 ((Unix))
...
| vulners:
|   cpe:/a:apache:http_server:2.4.49:
...
        https://vulners.com/githubexploit/DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D
*EXPLOIT*
|       CVE-2021-41773  4.3     https://vulners.com/cve/CVE-2021-41773
...
|_http-server-header: Apache/2.4.49 (Unix)
MAC Address: 00:0C:29:C7:81:EA (VMware)
```

Vulnerability Scanning with Nmap



```
kali@kali:~$ sudo nmap -sV -p 443 --script "vuln" 192.168.50.124
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org )
...
PORT    STATE SERVICE VERSION
443/tcp open  http    Apache httpd 2.4.49 ((Unix))
...
| vulners:
|   cpe:/a:apache:http_server:2.4.49:
...
        https://vulners.com/githubexploit/DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D
*EXPLOIT*
|       CVE-2021-41773  4.3     https://vulners.com/cve/CVE-2021-41773
...
|_http-server-header: Apache/2.4.49 (Unix)
MAC Address: 00:0C:29:C7:81:EA (VMware)
```

Vulnerability Scanning with Nmap



CVE-2021-41773 nse

About 59.500 results (0,49 seconds)

https://github.com › RootUp › PersonalStuff › blob › ht...

PersonalStuff/http-vuln-cve-2021-41773.nse at master - GitHub

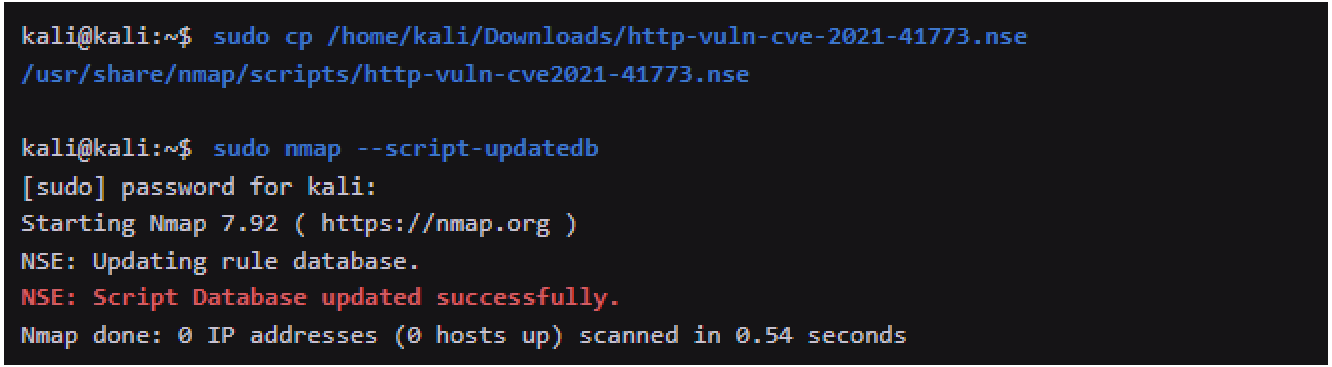
This is a repo is to upload files done during my research. - PersonalStuff/http-vuln-**cve-2021-41773.nse** at master · RootUp/PersonalStuff.

https://github.com › TAI-REx › cve-2021-41773-nse

TAI-REx/cve-2021-41773-nse - GitHub

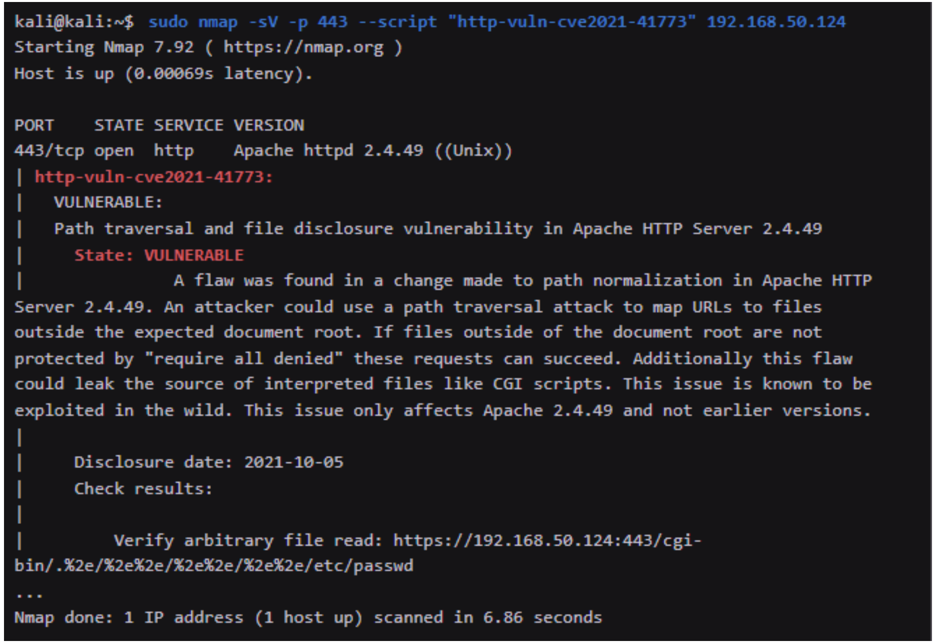
CVE-2021-41773.nse. Contribute to TAI-REx/**cve-2021-41773-nse** development by creating an account on GitHub.

Vulnerability Scanning with Nmap



```
kali@kali:~$ sudo cp /home/kali/Downloads/http-vuln-cve-2021-41773.nse
/usr/share/nmap/scripts/http-vuln-cve2021-41773.nse

kali@kali:~$ sudo nmap --script-updatedb
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org )
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.54 seconds
```

Vulnerability Scanning with Nmap



```
kali@kali:~$ sudo nmap -sV -p 443 --script "http-vuln-cve2021-41773" 192.168.50.124
Starting Nmap 7.92 ( https://nmap.org )
Host is up (0.00069s latency).

PORT    STATE SERVICE VERSION
443/tcp open  http    Apache httpd 2.4.49 ((Unix))
| http-vuln-cve2021-41773:
|   VULNERABLE:
|   Path traversal and file disclosure vulnerability in Apache HTTP Server 2.4.49
|     State: VULNERABLE
|               A flaw was found in a change made to path normalization in Apache HTTP
Server 2.4.49. An attacker could use a path traversal attack to map URLs to files
outside the expected document root. If files outside of the document root are not
protected by "require all denied" these requests can succeed. Additionally this flaw
could leak the source of interpreted files like CGI scripts. This issue is known to be
exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions.
|
|     Disclosure date: 2021-10-05
|     Check results:
|
|         Verify arbitrary file read: https://192.168.50.124:443/cgi-
bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
...
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

Source

https://tryhackme.com/room/furthernmap

https://github.com/wddadk/Offensive-OSINT-Tools