

Cybersecurity Observation

Experiment - 1

Q) Perform reconnaissance to find all the relevant information on selected website using 10 network information gathering tools.

1) Nslookup

```
nslookup DOMAIN_NAME
```

```
Thursday, 08 August 2024, 01:14:40 AM

nslookup facebook.com
Server:      192.168.29.1
Address:     192.168.29.1#53

Non-authoritative answer:
Name:  facebook.com
Address: 163.70.140.35
Name:  facebook.com
Address: 2a03:2880:f185:85:face:b00c:0:25de
```

2) Netdiscover

```
sudo netdiscover -r IP/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
```

```
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
35.35.35.1	52:54:00:12:35:00		1	60	Unknown vendor
35.35.35.2	52:54:00:12:35:00		1	60	Unknown vendor
35.35.35.3	08:00:27:16:1d:32		1	60	PCS Systemtechnik GmbH
35.35.35.5	08:00:27:92:fa:f8		1	60	PCS Systemtechnik GmbH

3) Netcat

```
nc TARGET_IP TARGET_PORT
```

```
python -m http.server 80  x  kali@kali:~ x
Thursday, 08 August 2024, 01:00:34 AM

printf "GET / HTTP/1.1\r\nHost: 35.35.35.4\r\n\r\n" | nc 35.35.35.4 80
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.11.8
Date: Wed, 07 Aug 2024 19:31:08 GMT
Content-type: text/html; charset=utf-8
Content-Length: 3279

<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
```

4) Whois

```
whois DOMAIN_NAME
```

```
Thursday, 08 August 2024, 01:11:59 AM

whois facebook.com
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2024-04-24T19:06:12Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2033-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
Name Server: C.NS.FACEBOOK.COM
Name Server: D.NS.FACEBOOK.COM
DNSSEC: unsigned
```

5) Nmap

```
nmap TARGET_IP -T4
```

Thursday, 08 August 2024, 01:16:05 AM

```
nmap 35.35.35.5 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 01:16 IST
Nmap scan report for 35.35.35.5
Host is up (0.0056s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
```

6) Sherlock

```
sherlock USERNAME
```

Thursday, 08 August 2024, 01:21:45 AM

```
sherlock rafeeb
[*] Checking username rafeeb on:
[+] 7Cups: https://www.7cups.com/@rafeeb
[+] 9GAG: https://www.9gag.com/u/rafeeb
[+] About.me: https://about.me/rafeeb
[+] Academia.edu: https://independent.academia.edu/rafeeb
[+] Amino: https://aminoapps.com/u/rafeeb
[+] Anilist: https://anilist.co/user/rafeeb/
[+] Apple Developer: https://developer.apple.com/forums/profile/rafeeb
[+] Apple Discussions: https://discussions.apple.com/profile/rafeeb
[+] Archive.org: https://archive.org/details/@rafeeb
[+] ArtStation: https://www.artstation.com/rafeeb
[+] AskFM: https://ask.fm/rafeeb
[+] Audiojungle: https://audiojungle.net/user/rafeeb
[+] Bandcamp: https://www.bandcamp.com/rafeeb
[+] BitBucket: https://bitbucket.org/rafeeb/
[+] BodyBuilding: https://bodyspace.bodybuilding.com/rafeeb
[+] BuyMeACoffee: https://buymeacoff.ee/rafeeb
```

7) WhatWeb

```
whatweb -v TARGET_IP
```

```
Thursday, 08 August 2024, 01:06:56 AM

whatweb 35.35.35.5 -v
WhatWeb report for http://35.35.35.5
Status : 200 OK
Title : Metasploitable2 - Linux
IP : 35.35.35.5
Country : UNITED STATES, US

Summary : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], PHP[5.2.4-ub
.10]

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.

Version : 2.2.8 (from HTTP Server Header)
Google Dorks: (3)
Website : http://httpd.apache.org/
```

8) Dirb

```
dirb http://IP
```

```
Thursday, 08 August 2024, 01:29:15 AM

dirb http://35.35.35.5

DIRB v2.22
By The Dark Raver

START_TIME: Thu Aug  8 01:29:28 2024
URL_BASE: http://35.35.35.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

____ Scanning URL: http://35.35.35.5/ ____
+ http://35.35.35.5/cgi-bin/ (CODE:403|SIZE:291)
⇒ DIRECTORY: http://35.35.35.5/dav/
+ http://35.35.35.5/index (CODE:200|SIZE:891)
+ http://35.35.35.5/index.php (CODE:200|SIZE:891)
+ http://35.35.35.5/phpinfo (CODE:200|SIZE:48032)
+ http://35.35.35.5/phpinfo.php (CODE:200|SIZE:48044)
```

9) Nikto

```
nikto -h http://IP
```

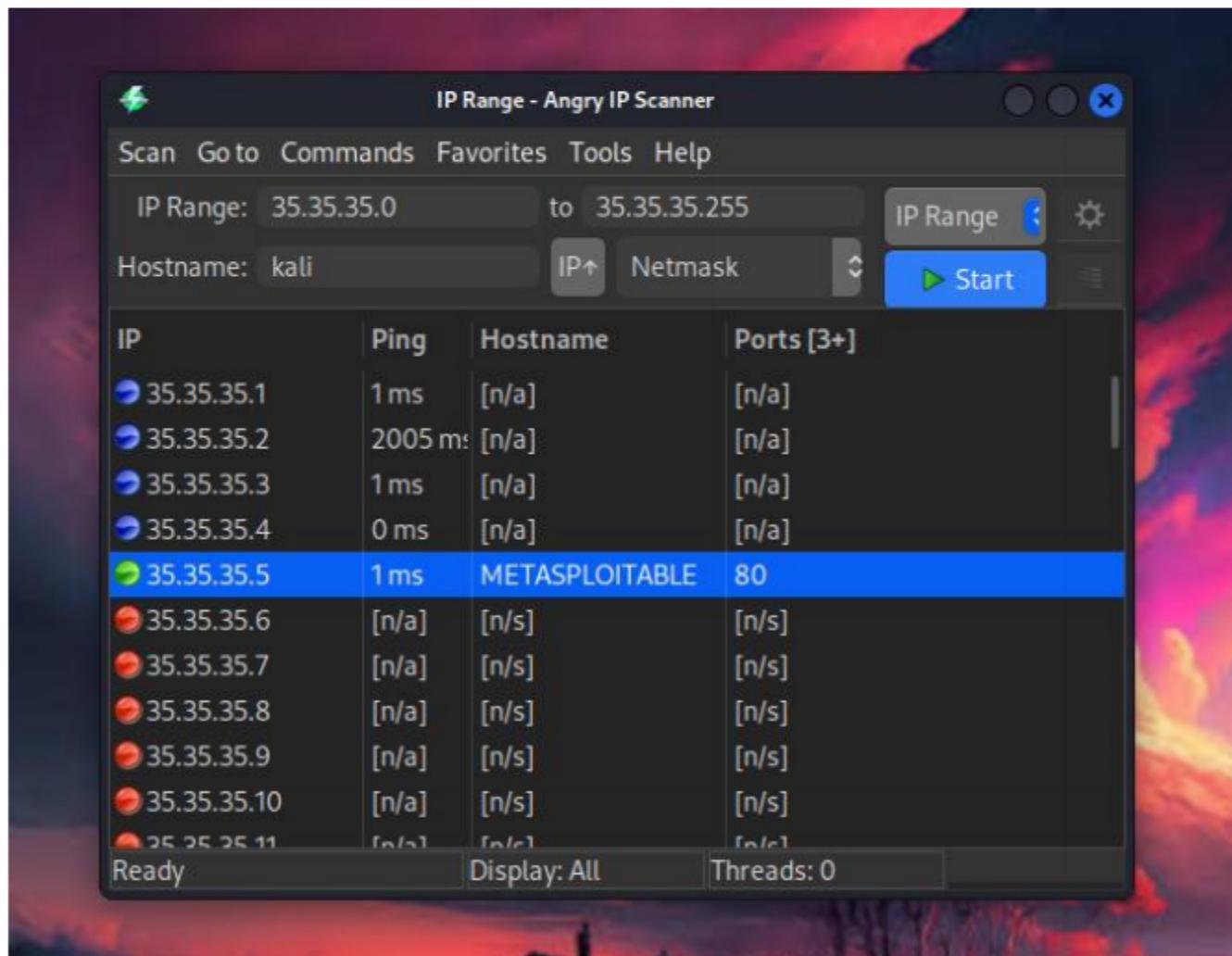
```
Thursday, 08 August 2024, 01:31:56 AM

[nikto -h http://35.35.35.5]
- Nikto v2.5.0

+ Target IP:      35.35.35.5
+ Target Hostname: 35.35.35.5
+ Target Port:    80
+ Start Time:    2024-08-08 01:31:58 (GMT5.5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
IME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-he
+ /index: Uncommon header 'tcm' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force f
'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xfor
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-c
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.
```

10) Angry IP Scanner



Experiment - 2

Q) Gather information using social networking and google dorks.

i) `site:*.gov.in`

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** site:*.gov.in - Google Search
- Address Bar:** https://www.google.com/search
- Toolbar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB
- Search Bar:** site:*.gov.in
- Google Logo:** The classic Google logo is visible on the left.
- Search Options:** All, Shopping, Images, Videos, News, Maps, Web, More, Tools.
- Google promotion:** Try Google Search Console
www.google.com/webmasters/
Do you own *.gov.in? Get indexing and ranking data from Google.
- Search Results:**
 - School Education, Haryana**
https://schooleducationharyana.gov.in
 - Department of secondary education, Government of Haryana ...**
Directorate of Secondary Education · Latest News · About the Department · Children · Other Links · Online Applications · Shiksha Saarthi Magazine, SHIKSHA ...
 - Dot.gov.in**
https://dot.gov.in
 - Department of Telecommunication | https://dot.gov.in/node**
Website of Department of telecommunication | https://dot.gov.in/node.

ii) `intitle:"index of" password`

Google search results for "intitle:"index of" password":

- Purdue University - http://ftp.cerias.purdue.edu/pub/doc/passwords
- Index of /pub/doc/passwords
- Index of /pub/doc/passwords/. Search the archive: [ICO], Name · Last modified · Size · [PARENTDIR] · Parent ... spaf-weeber-password-biblio.ps, 2012-03-09 16:05 ...
- Openwall - https://download.openwall.net/pub/passwords
- Index of /pub/wordlists/passwords
- Index of /pub/wordlists/passwords, Name Last modified Size. [DIR] Parent Directory 26-Feb-2015 13:00 - [] lower.gz 08-Oct-2003 05:58 3k [] ...

iii) inurl:admin.php

Google search results for "inurl:admin.php":

- WordPress Developer Resources - https://developer.wordpress.org/reference/files/admin/
- wp-admin/admin.php - WordPress Developer Resources
- Fires when an 'action' request variable is sent. Used by 0 functions | Uses 0 functions | Source: wp-admin/admin.php:419. hook ...
- GitHub - https://github.com/WordPress/WordPress/blob/ad...
- WordPress/wp-admin/includes/admin.php at master
- WordPress, Git-ified. This repository is just a mirror of the WordPress subversion repository.
- Please do not send pull requests.
- Public College Samana - http://www.picsamana.org.in/registration/admin
- Admin Login
- phpMyAdmin**
- phpMyAdmin is a free and open source administration tool for MySQL and MariaDB. As a portable web application written primarily in PHP, it has become one of the most popular MySQL administration tools, especially for web hosting services. Wikipedia
- Programming languages:** PHP, JavaScript, XHTML
- Available in:** 95 languages
- Developer(s):** The phpMyAdmin Project
- Initial release:** September 9, 1998; 25 years ago
- License:** GNU General Public License 2
- Preview release:** 5.2.0-rc1 / January 22, 2022; 2 years ago
- Stable release:** 5.2.1 / 2023-02-08; 17 months ago

iv) "not for public" + "confidential" ext:pdf | ext:doc | ext:xml

The screenshot shows a Firefox browser window with a dark theme. The address bar contains the query: "not for public" + "confidential" ext:pdf | ext:doc | ext:xml". The search results page from Google is displayed, with the first result being from the Australian Energy Regulator (AER). The result title is "CONFIDENTIAL - NOT FOR PUBLIC RELEASE Attachment 5". Below the title, it says "CONFIDENTIAL - NOT FOR PUBLIC RELEASE. Attachment 5. Page 2. Page 3. Page 4. Page 5. Page 6. Page 7. Page 8. Page 9. Page 10. Page 11. Page 12. Page 13 ... 17 pages". The second result is from Oregon.gov, titled "confidential document – not for public release", with the text "CONFIDENTIAL DOCUMENT – NOT FOR PUBLIC RELEASE. PAGE 1 - ORDER FOR EVALUATION – LICENSEE NAME. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 1 page". The third result is from House.gov, with the title partially visible as "House.gov https://docs.house.gov > meetings > HMKP-118-J... PDF".

Experiment - 3

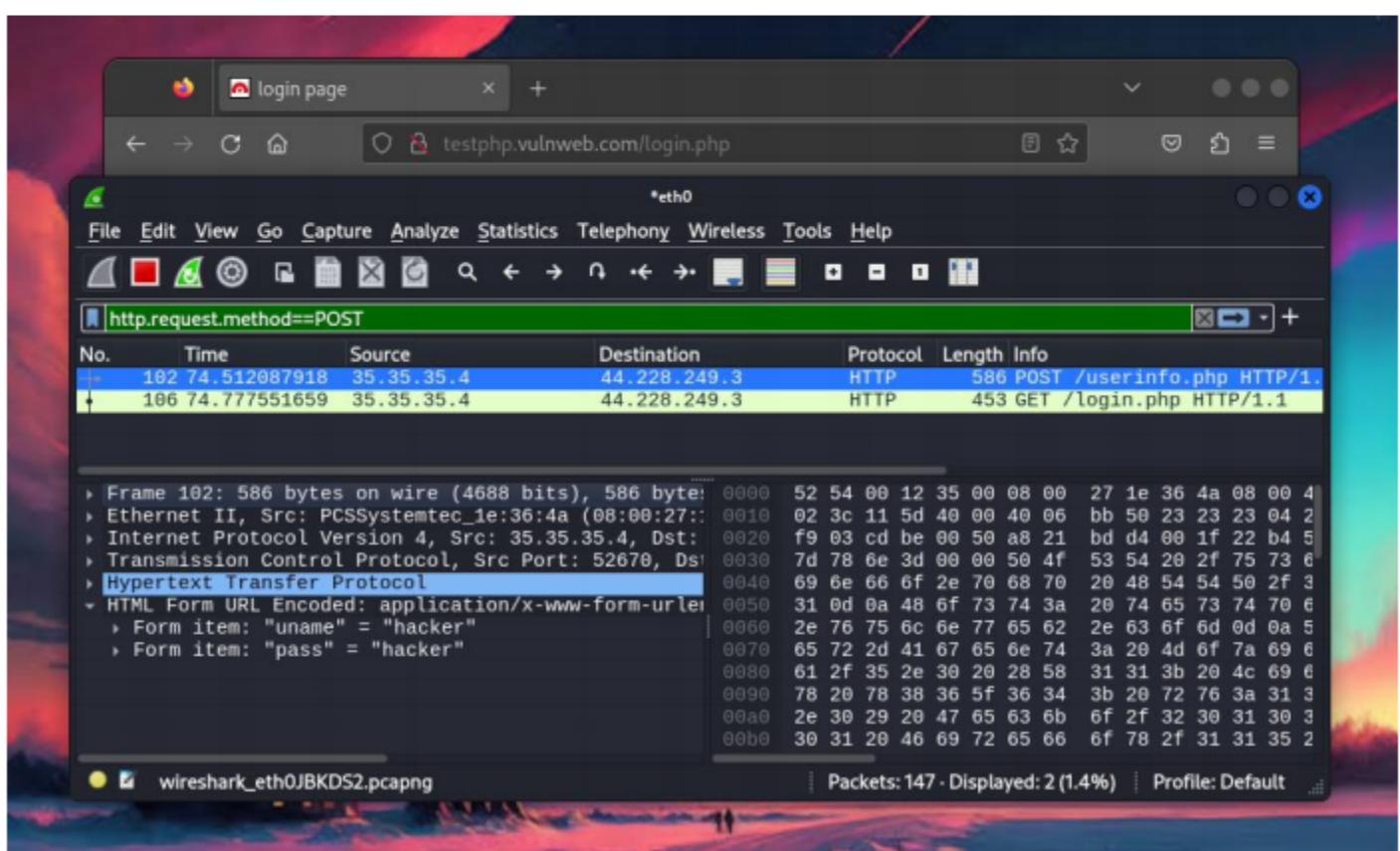
Q) Session hijacking, find credentials in real-time website using wireshark login page.

Wireshark

Wireshark is a widely used network protocol analyzer that enables users to capture and interactively browse the traffic running on a computer network.

Steps:

1. Visit the Target link in firefox
2. Start wireshark, listen on eth0 interface
3. Perform login in the target website
4. Apply the following filter in wireshark
5. http.request.method==POST



Experiment - 4

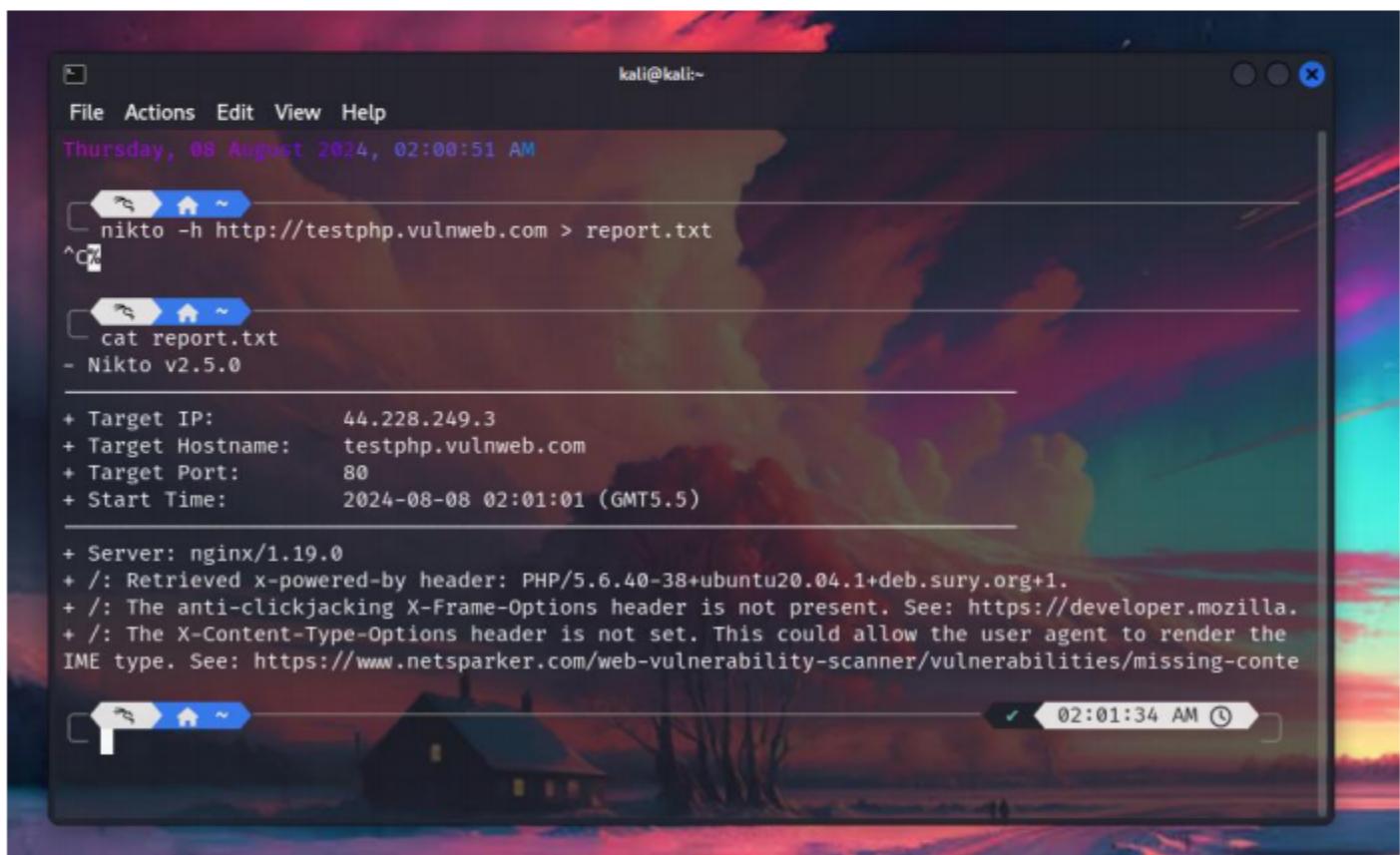
Q) Use nikto tool to find all the vulnerabilities with its levels and generate report for an organization

Nikto

Nikto is an open-source web server scanner that performs comprehensive tests against web servers for multiple items, including over 6,700 potentially dangerous files and programs, checks for outdated versions of over 1,250 servers, and version-specific problems on over 270 servers. It is widely used for web server security assessments.

Command:

```
nikto -h IP > ~/report.txt  
cat ~/report.txt
```



A screenshot of a terminal window titled "kali@kali:~". The window shows the command "nikto -h http://testphp.vulnweb.com > report.txt" being run, followed by a control-C (^C) interrupt. Below this, the command "cat report.txt" is run, and the output of the Nikto scan is displayed. The output includes the target information (IP: 44.228.249.3, Hostname: testphp.vulnweb.com, Port: 80, Start Time: 2024-08-08 02:01:01 (GMT5.5)) and several findings, such as the Server header (nginx/1.19.0), missing X-Frame-Options and X-Content-Type-Options headers, and a note about the anti-clickjacking header. The terminal has a dark theme with a colorful background image of a landscape.

```
nikto -h http://testphp.vulnweb.com > report.txt
^C
cat report.txt
- Nikto v2.5.0

+ Target IP:        44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port:      80
+ Start Time:       2024-08-08 02:01:01 (GMT5.5)

+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the IME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-x-content-type-options-header/
```

Experiment - 5

Q) Perform Kali Linux Login Bypass in VM

Steps:

1. Start Kali Linux Virtual Machine.
2. Press **E** on boot loader time.
3. Scroll down and edit kernel parameter of Linux.

```
rw init=/bin/bash
```

4. Press **CTRL + X** to save.
5. Enter the below command in the newly opened root prompt.

```
passwd kali
```

6. Enter the new password and press Enter two times.

```
exec /sbin/init
```

Password has been changed!

