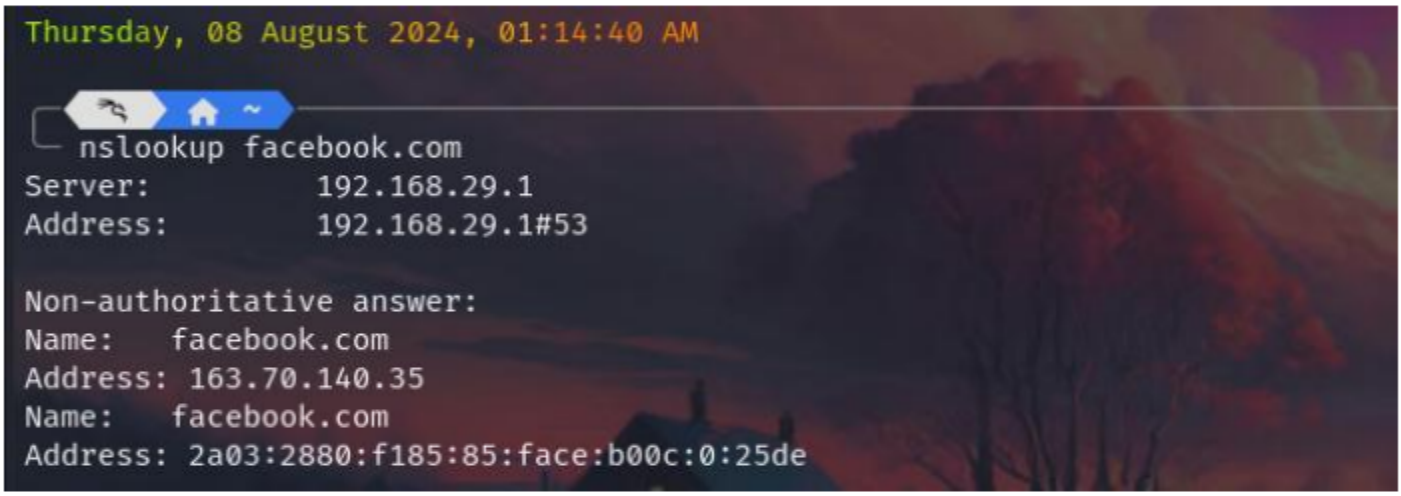
Cybersecurity Observation

Experiment - 1

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

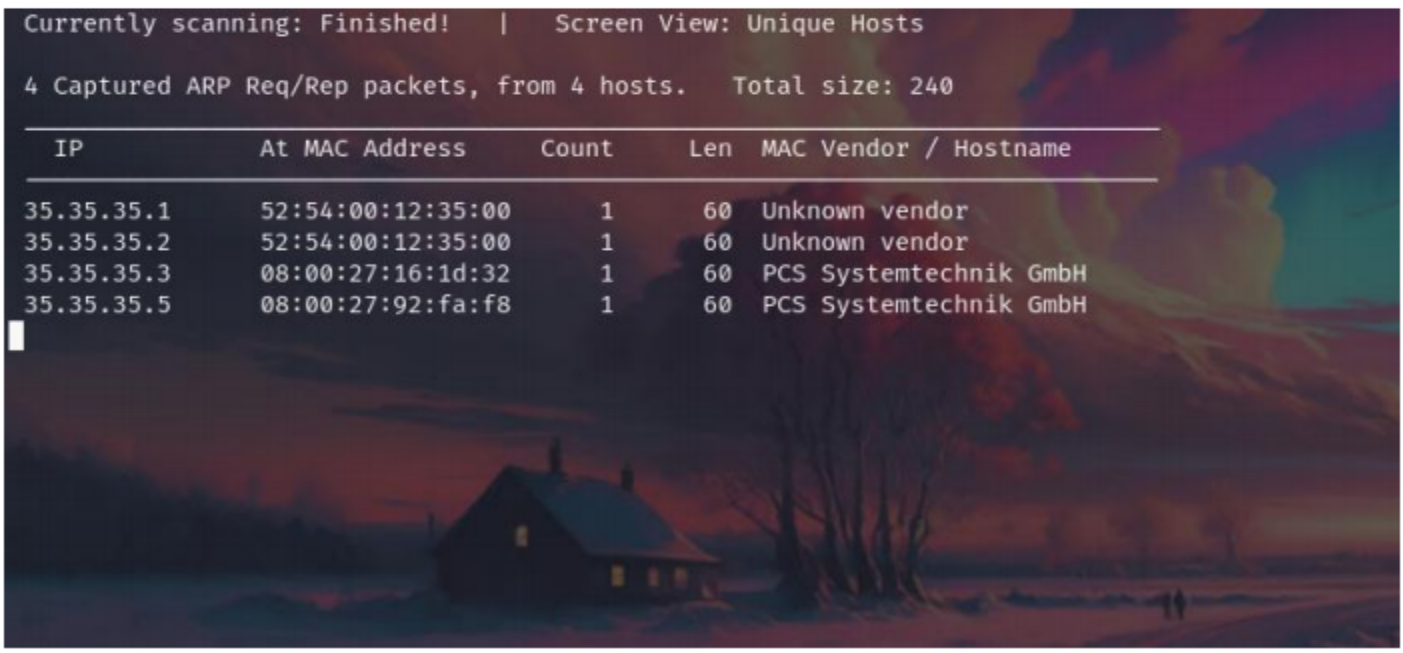
1) Nslookup

```
nslookup DOMAIN_NAME
```



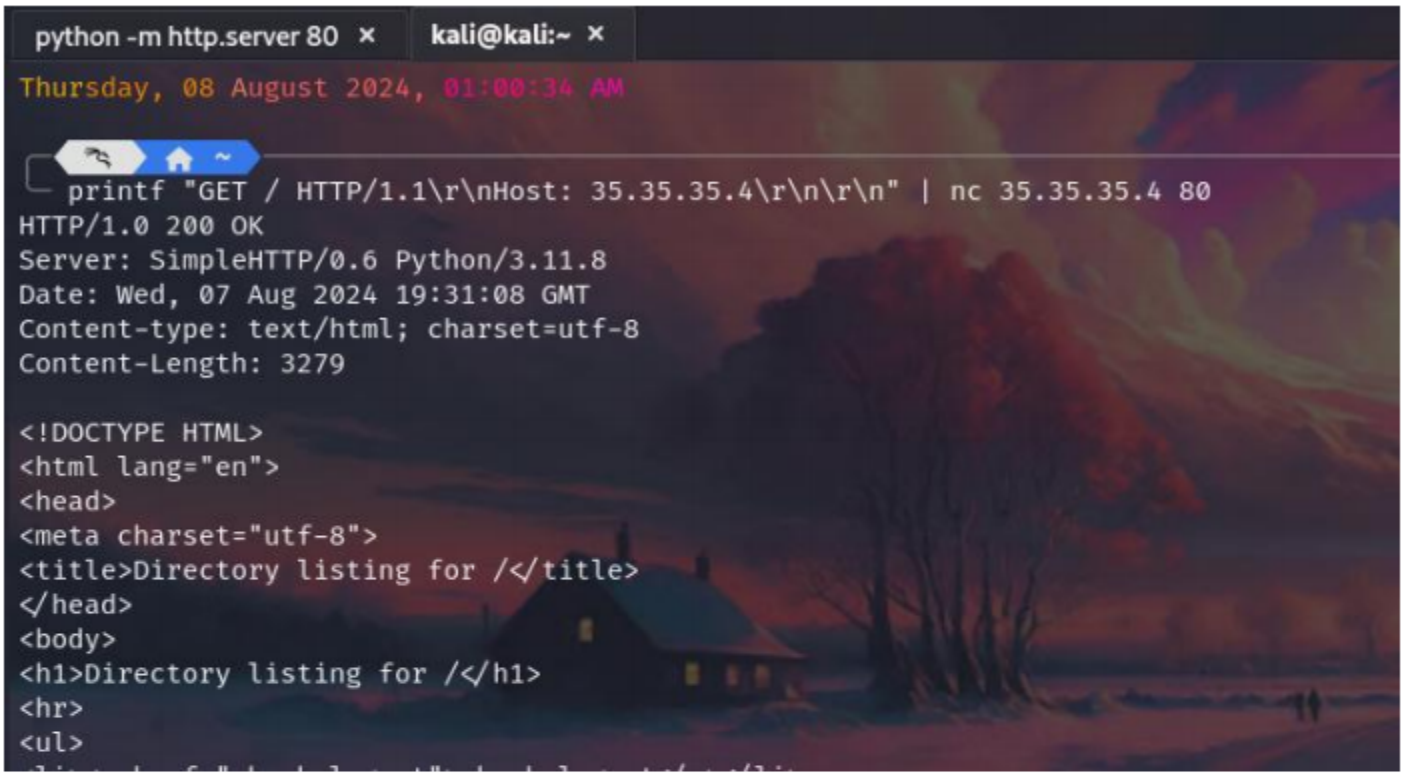
2) Netdiscover

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



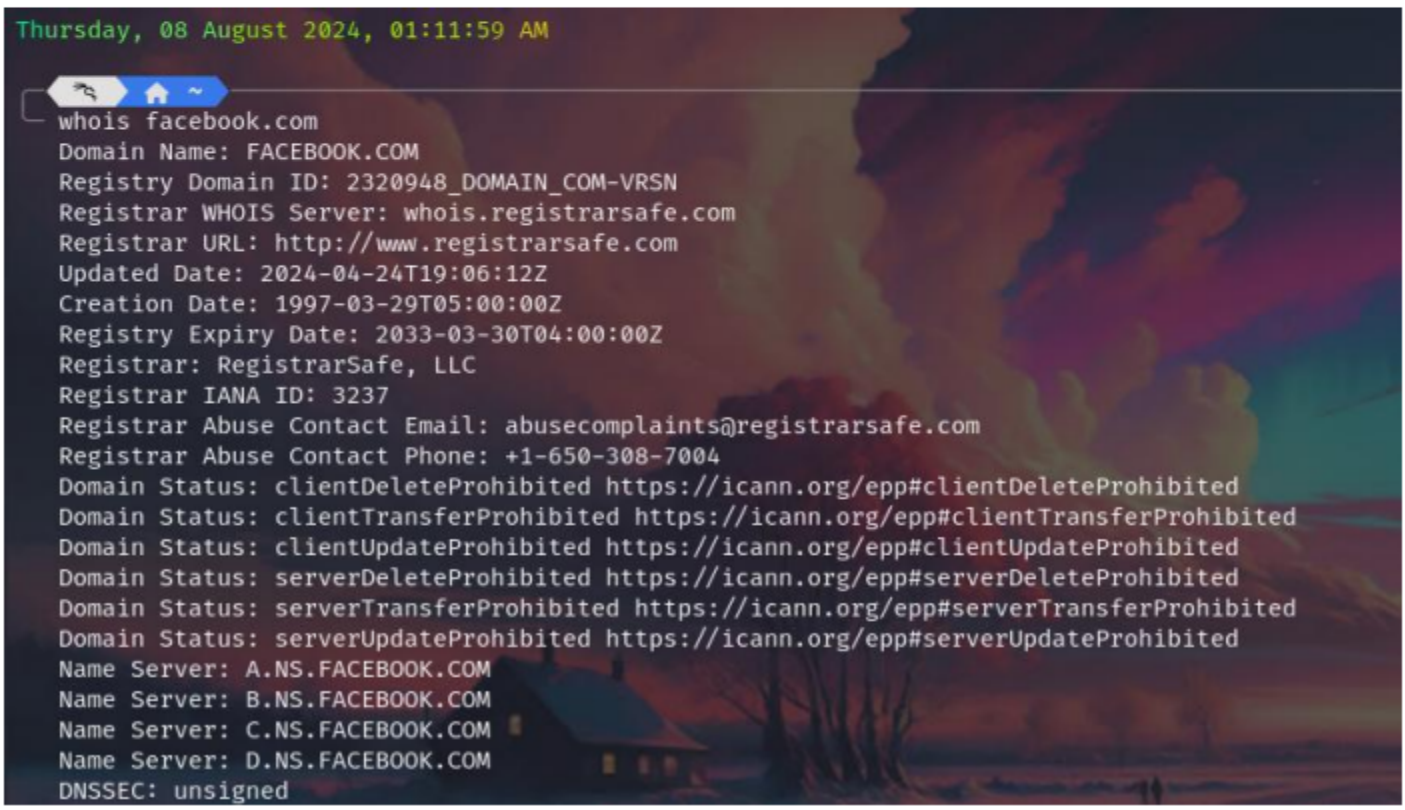
3) Netcat

```
nc TARGET_IP TARGET_PORT
```



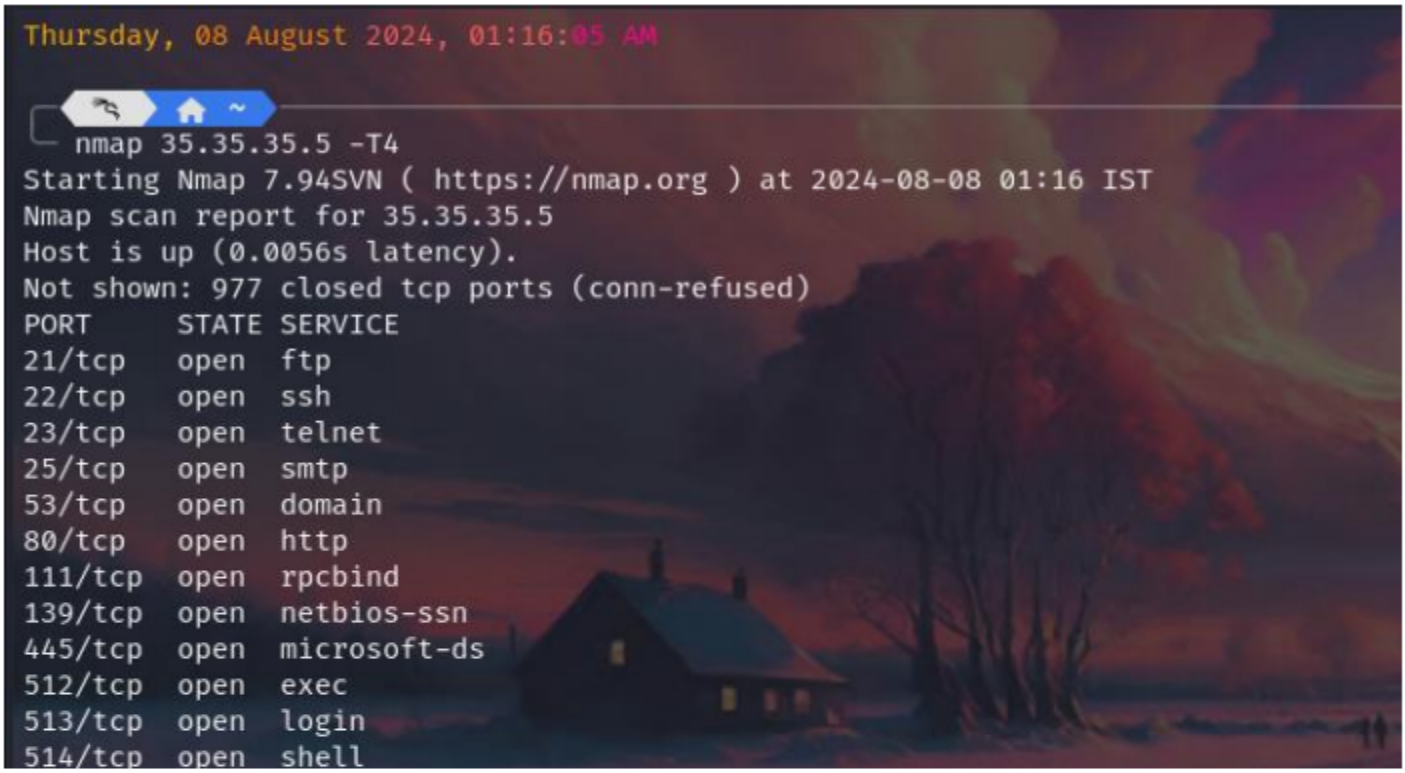
4) Whois

```
whois DOMAIN_NAME
```



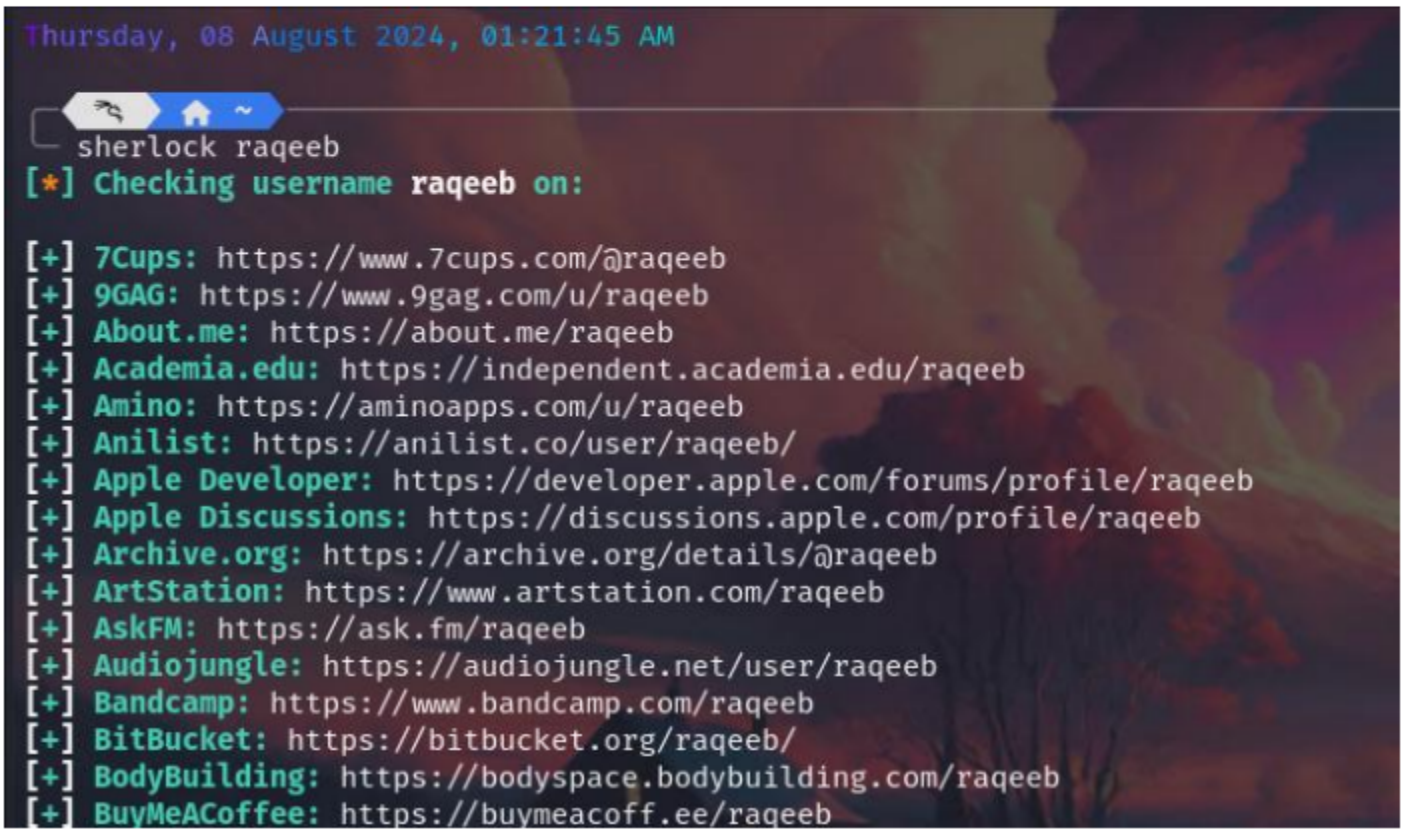
5) Nmap

```
nmap TARGET_IP -T4
```



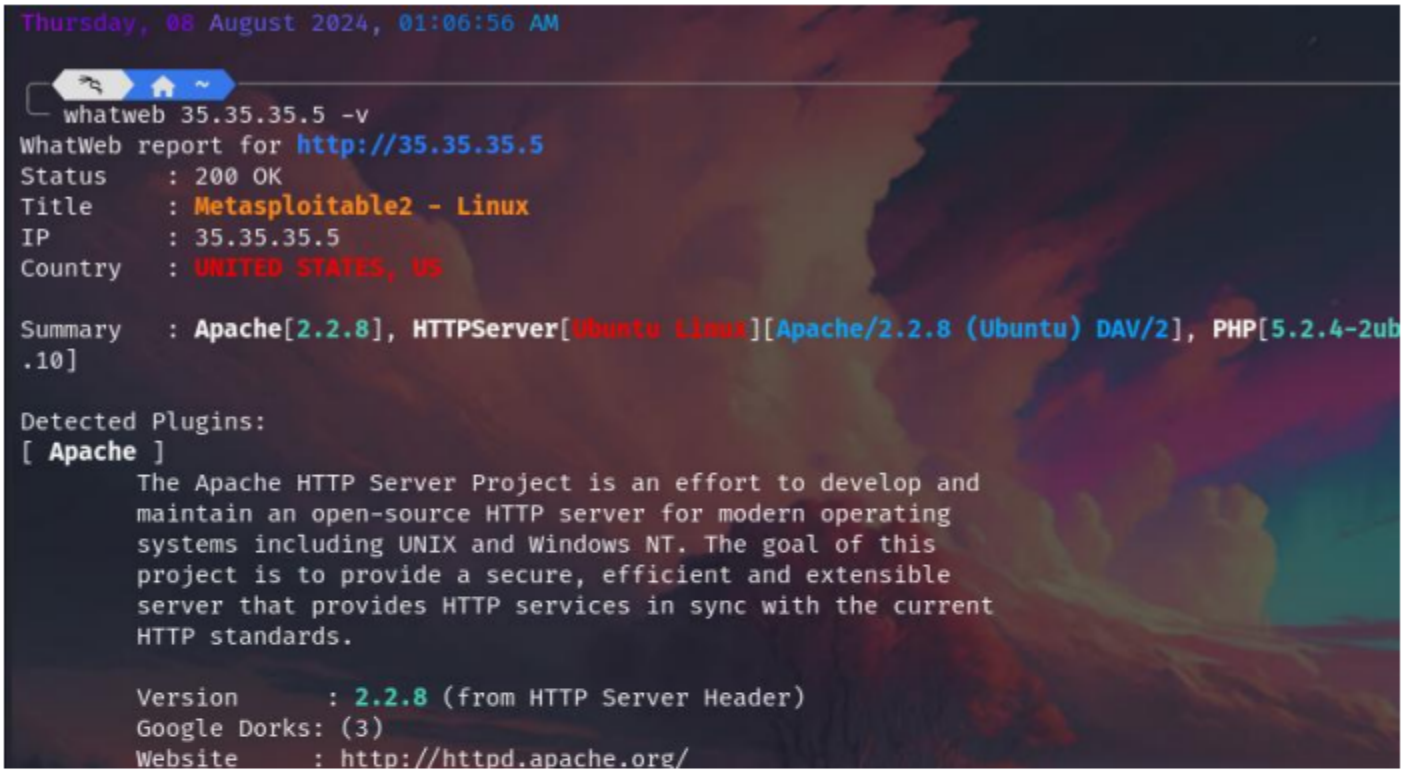
6) Sherlock

```
sherlock USERNAME
```



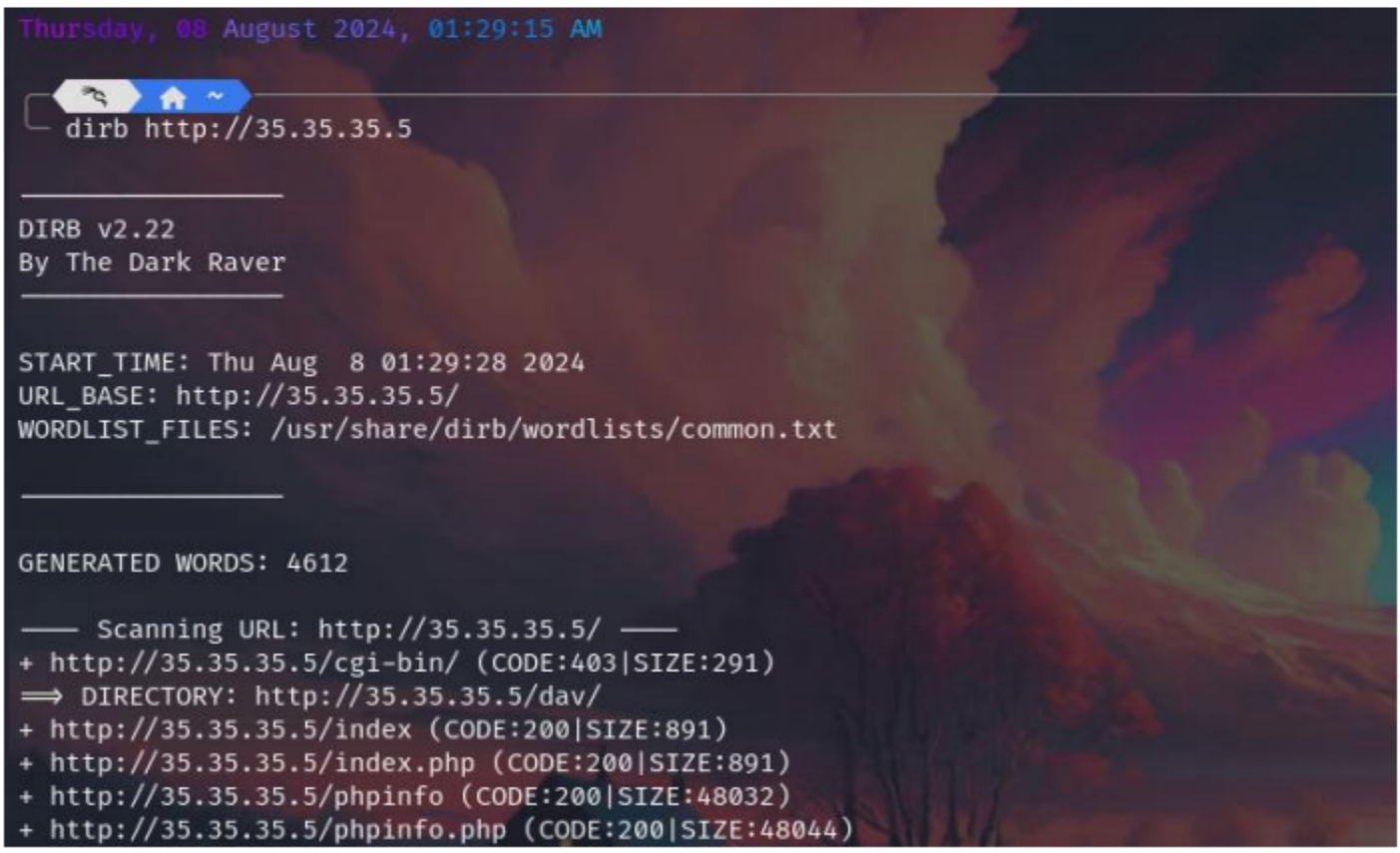
7) WhatWeb

`whatweb -v TARGET_IP`



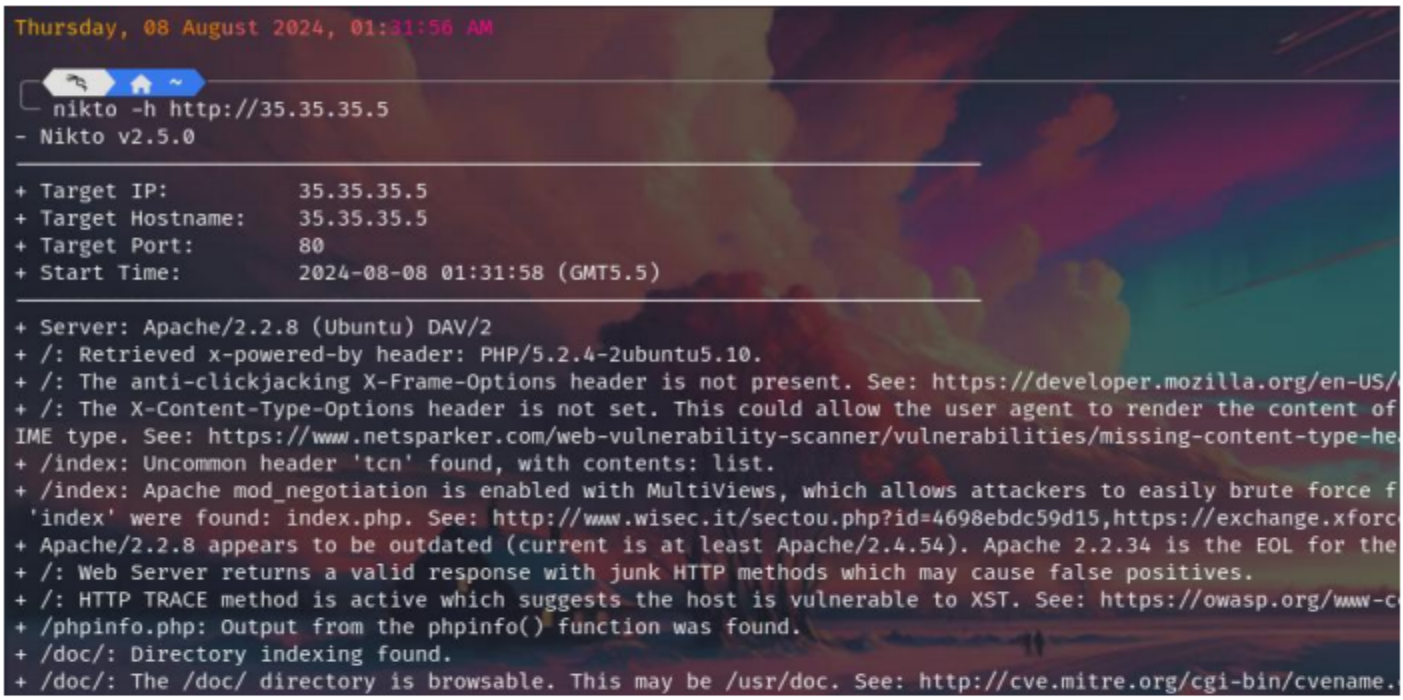
8) Dirb

`dirb http://IP`

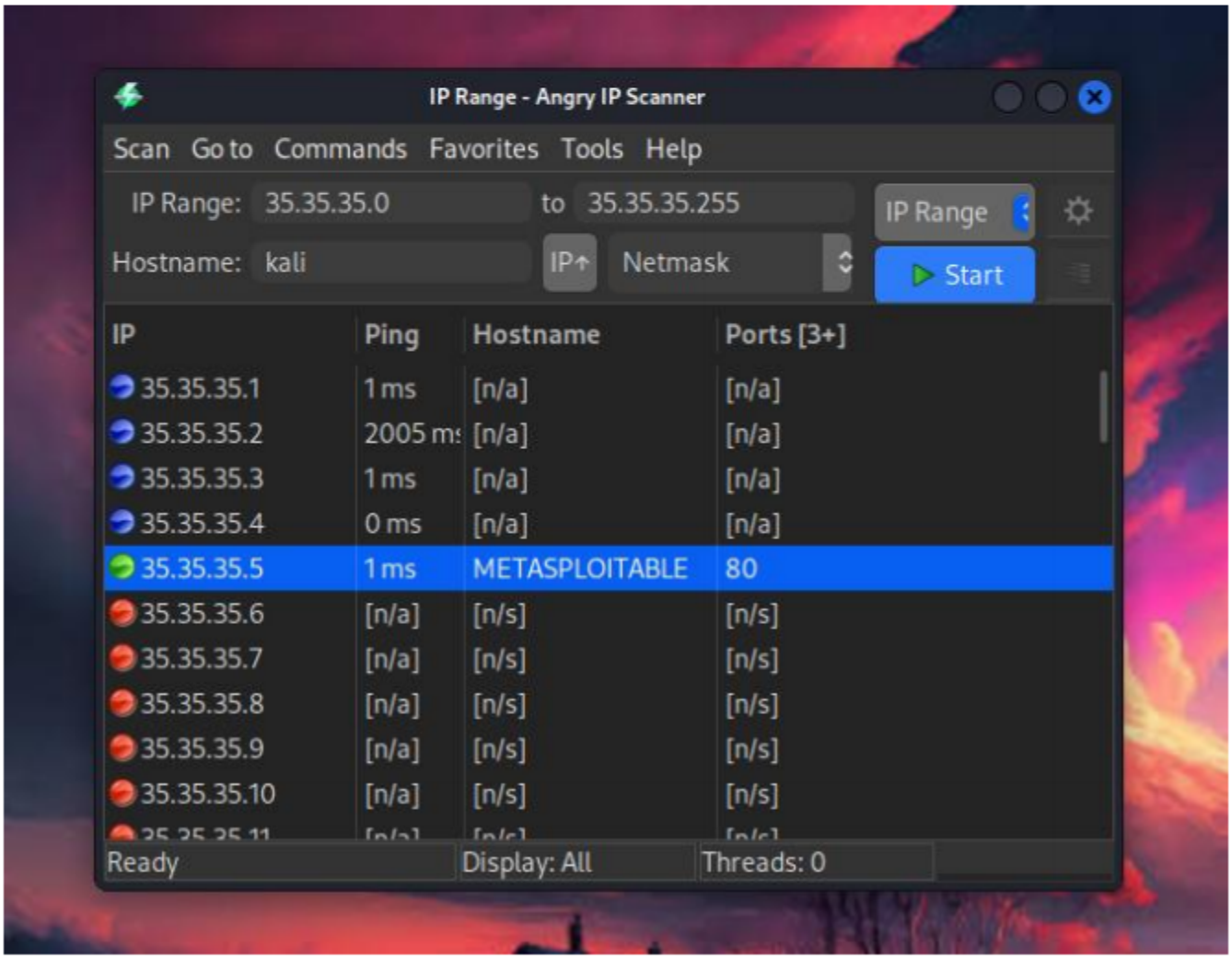


9) Nikto

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



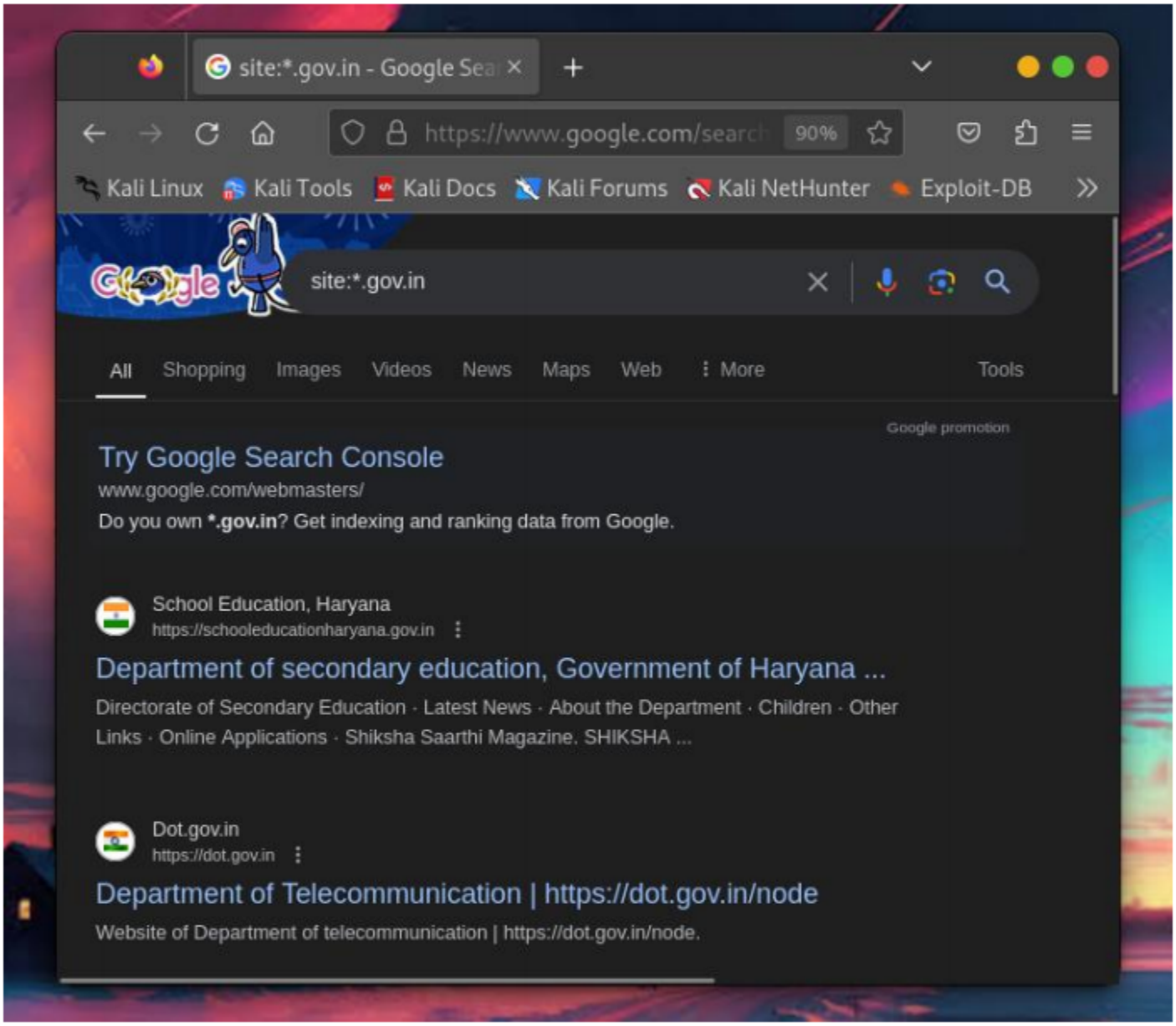
10) Angry IP Scanner



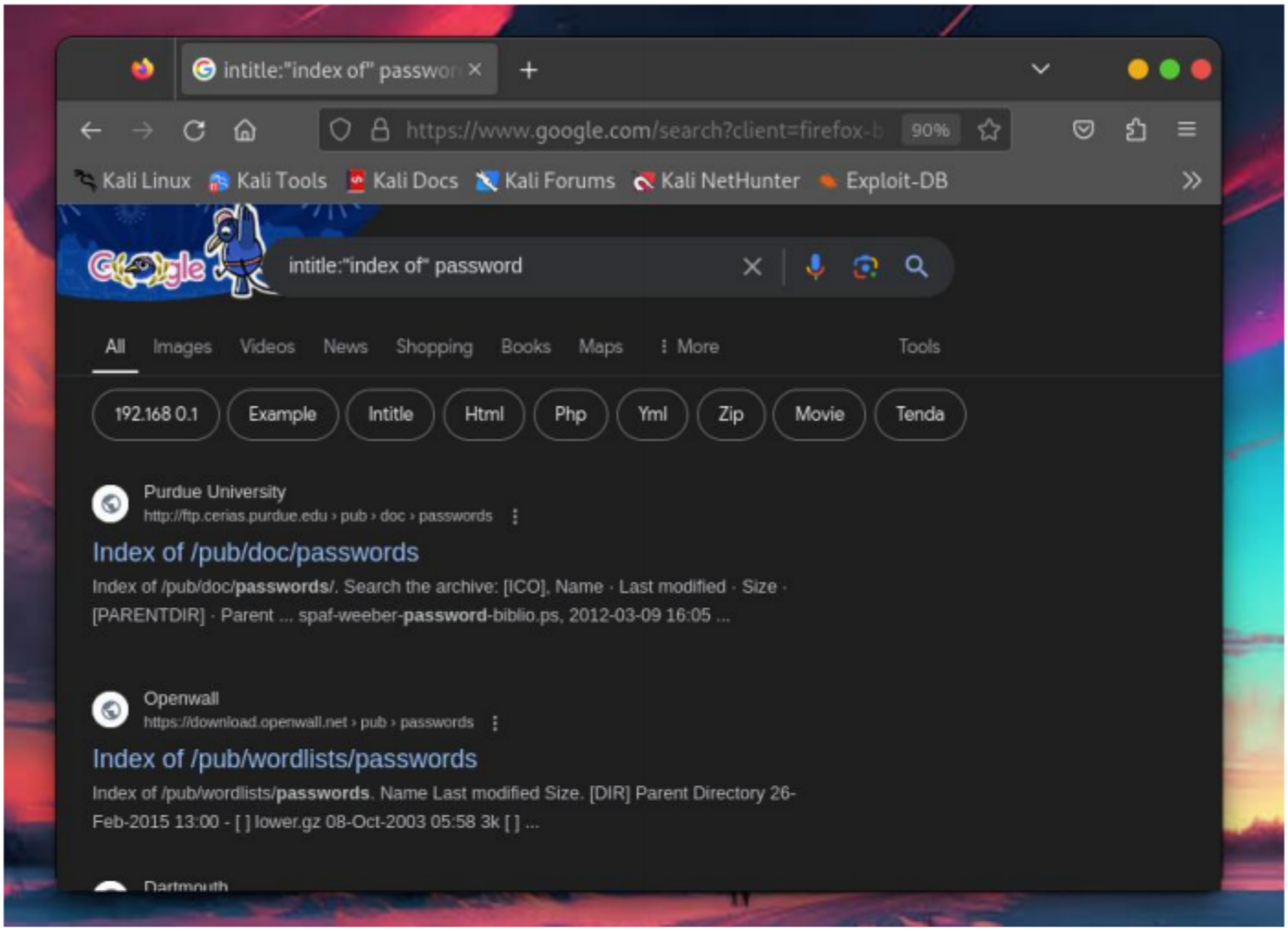
Experiment - 2

Q) Gather information using social networking and google dorks.

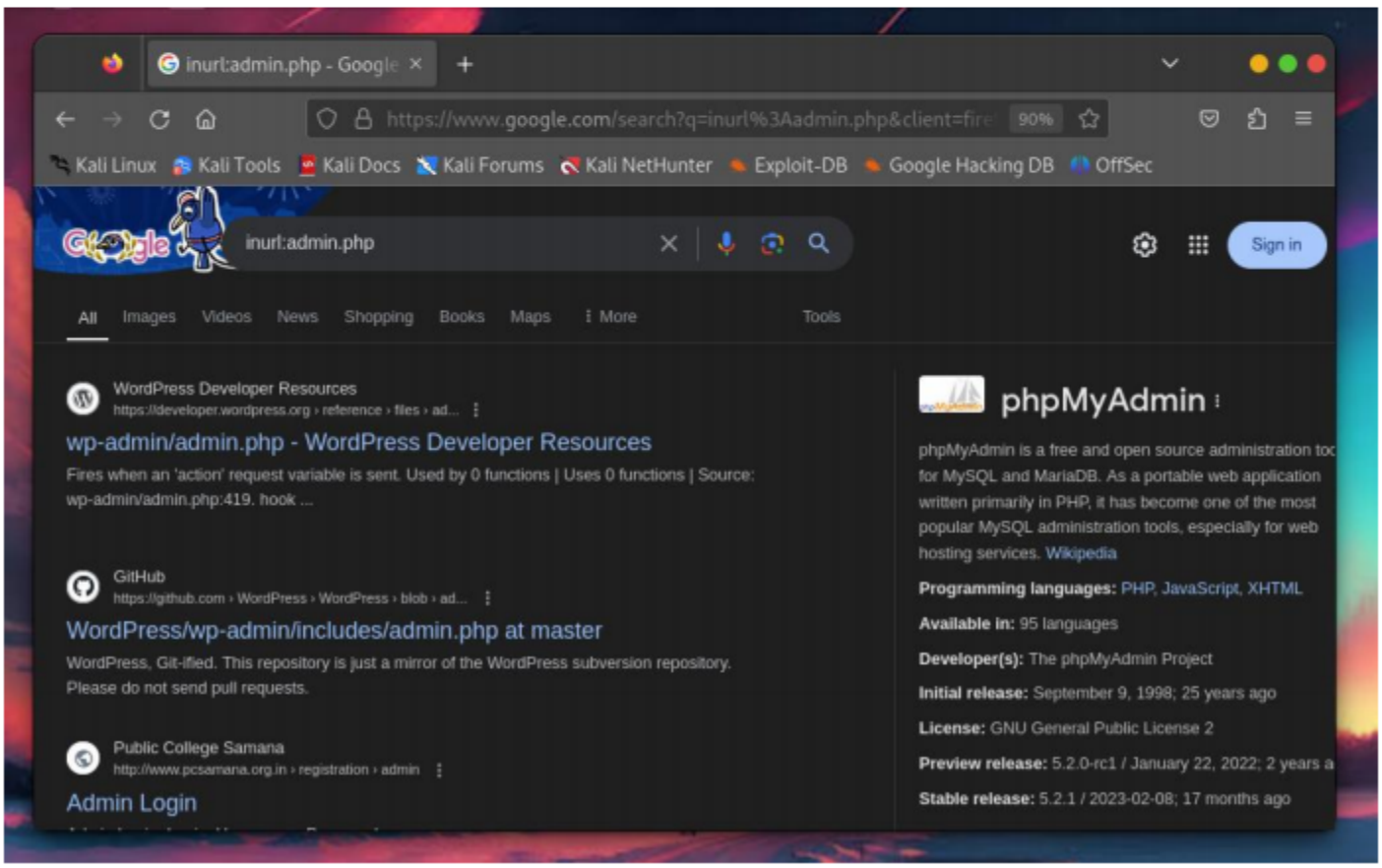
i) `site:*.gov.in`



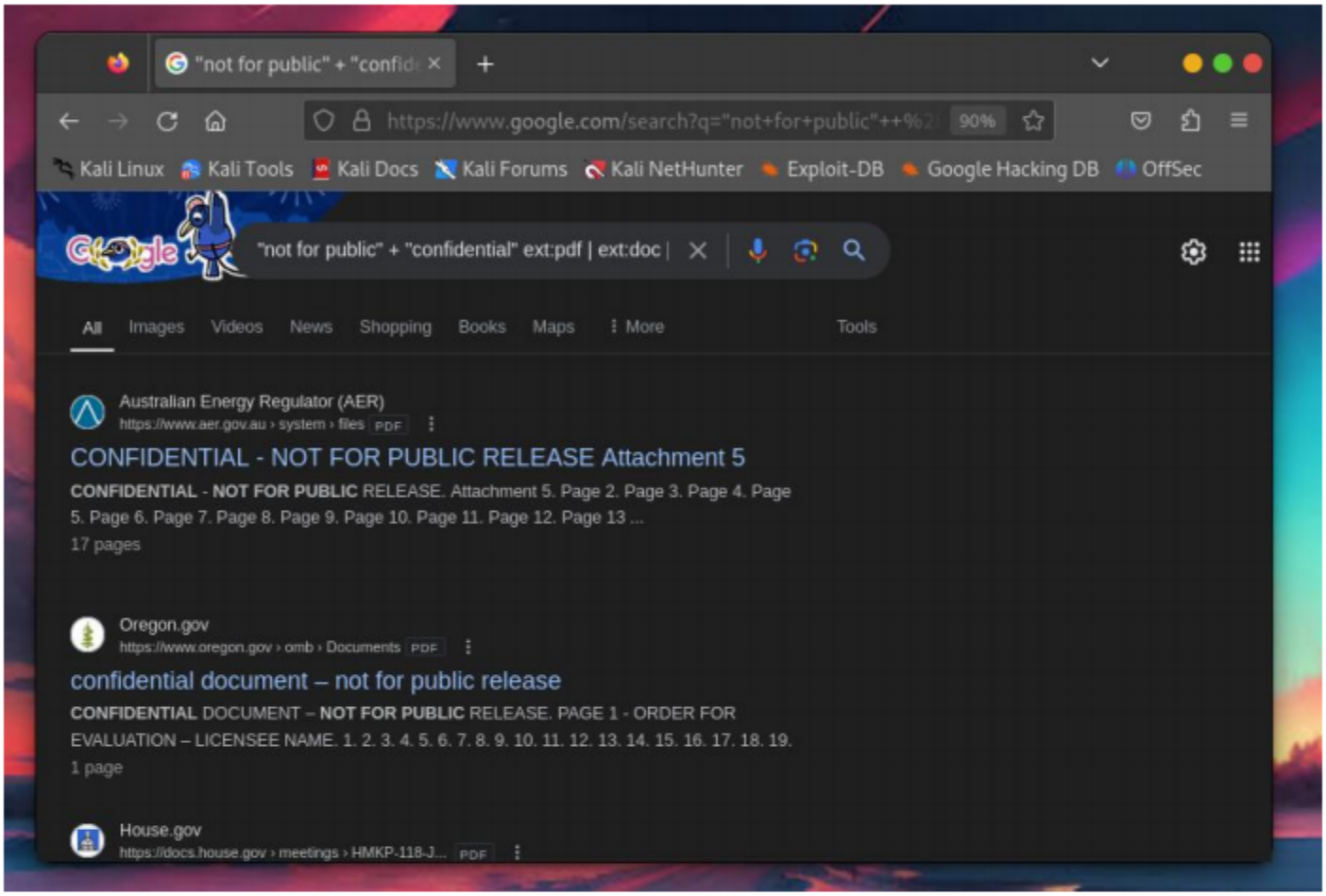
ii) `intitle:"index of" password`



iii) `inurl:admin.php`



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



Experiment - 3

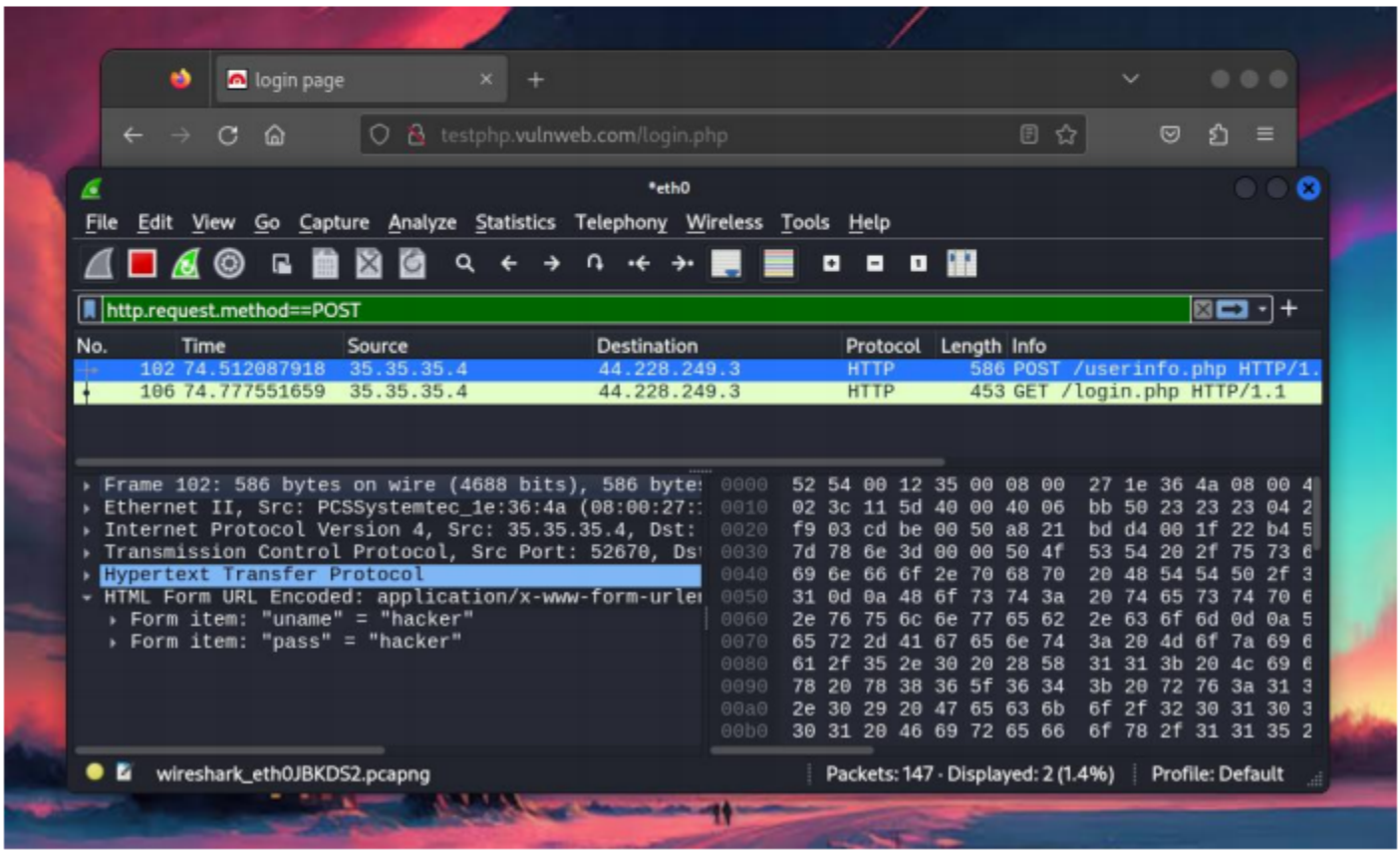
Q) Session hijacking, find credentials in real-time website using wireshark login page.

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

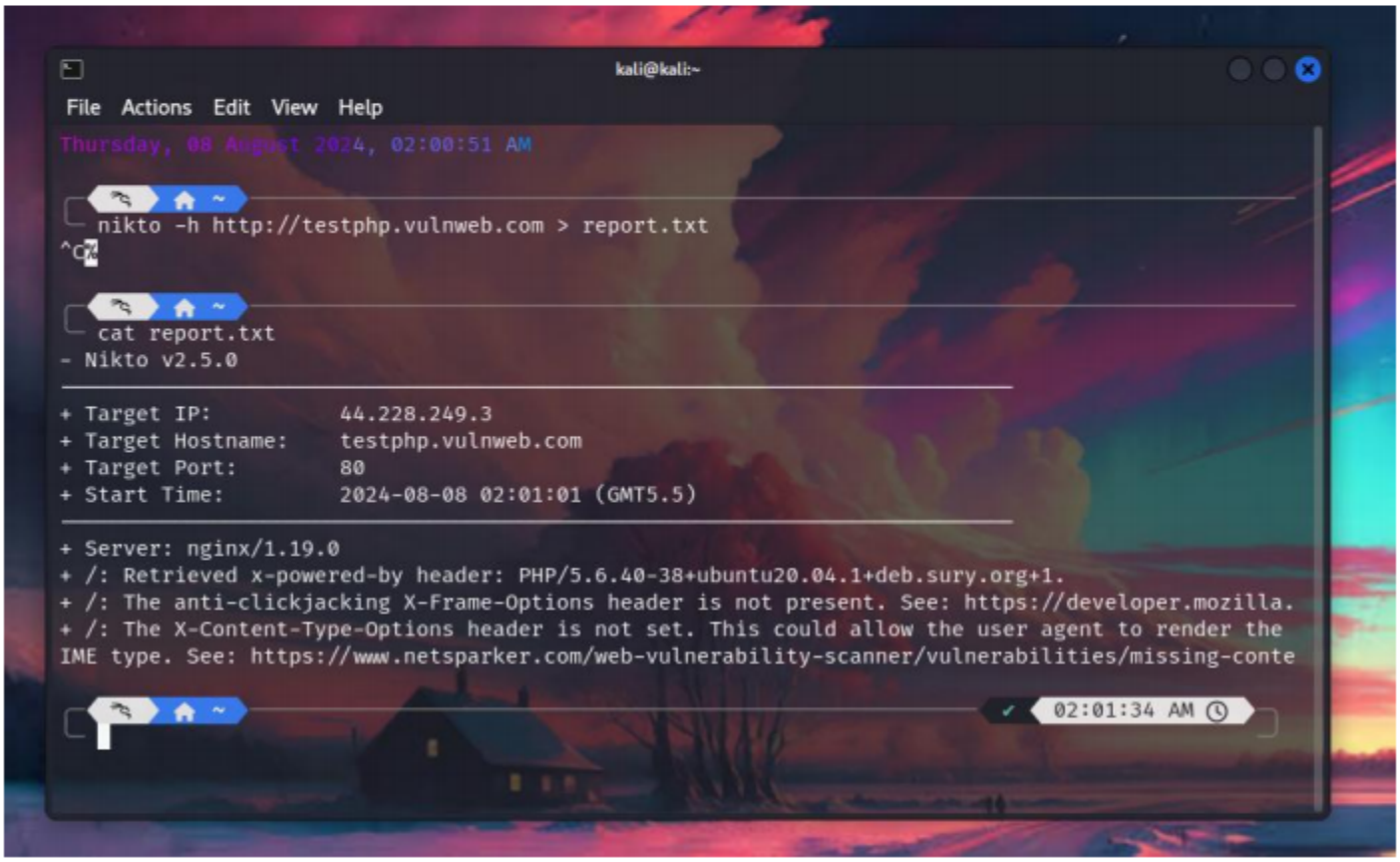
Q) Use nikto tool to find all the vulnerabilities with its levels and generate report for an organization

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
```



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!