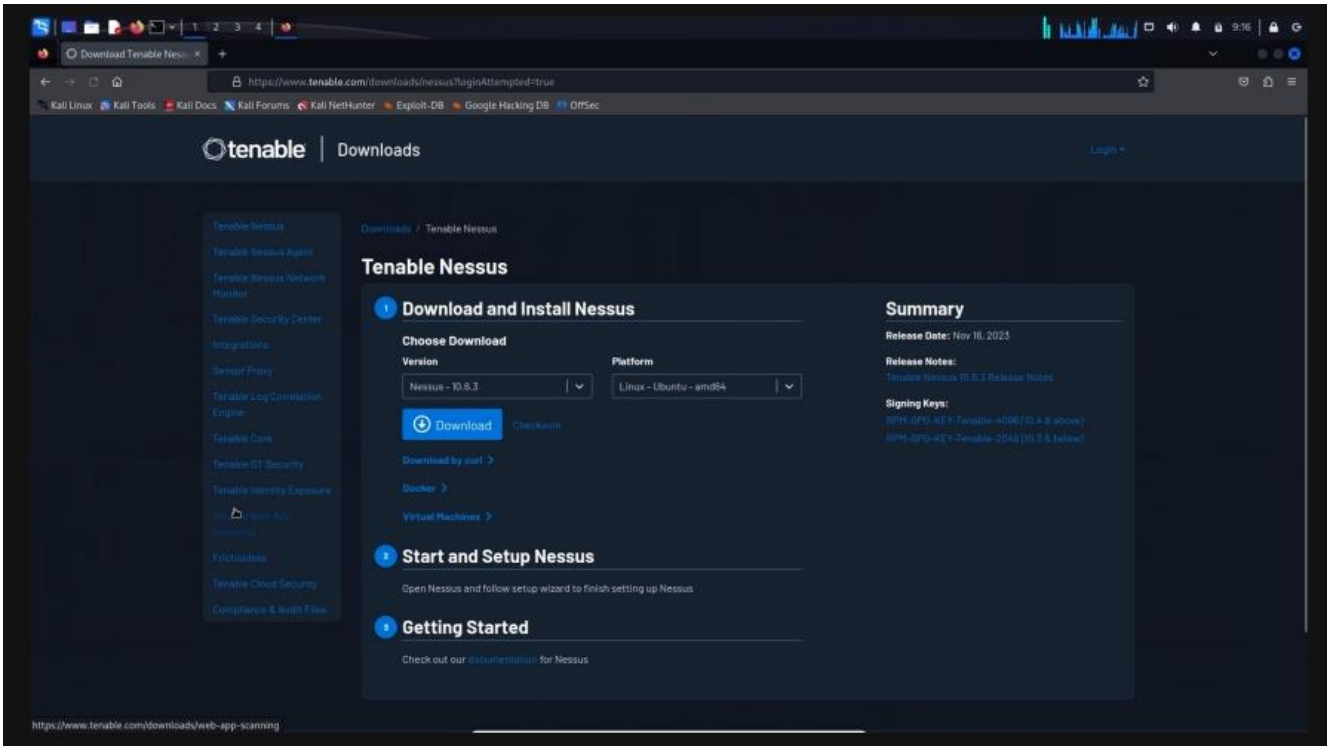
CFSS Internship Documentation

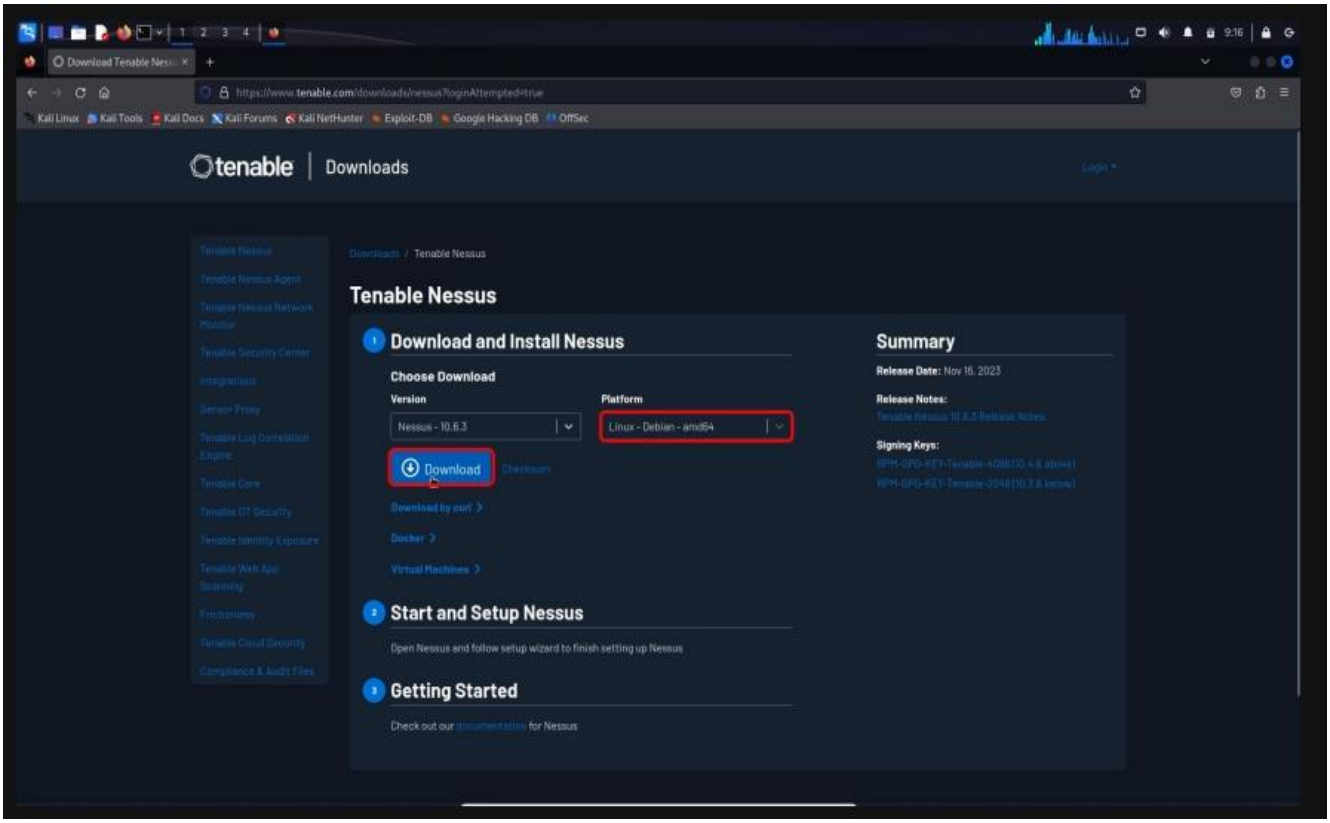
Jagadeesh Kannedari
honeyjagadeesh2@gmail.com

Nessus Installation Guide

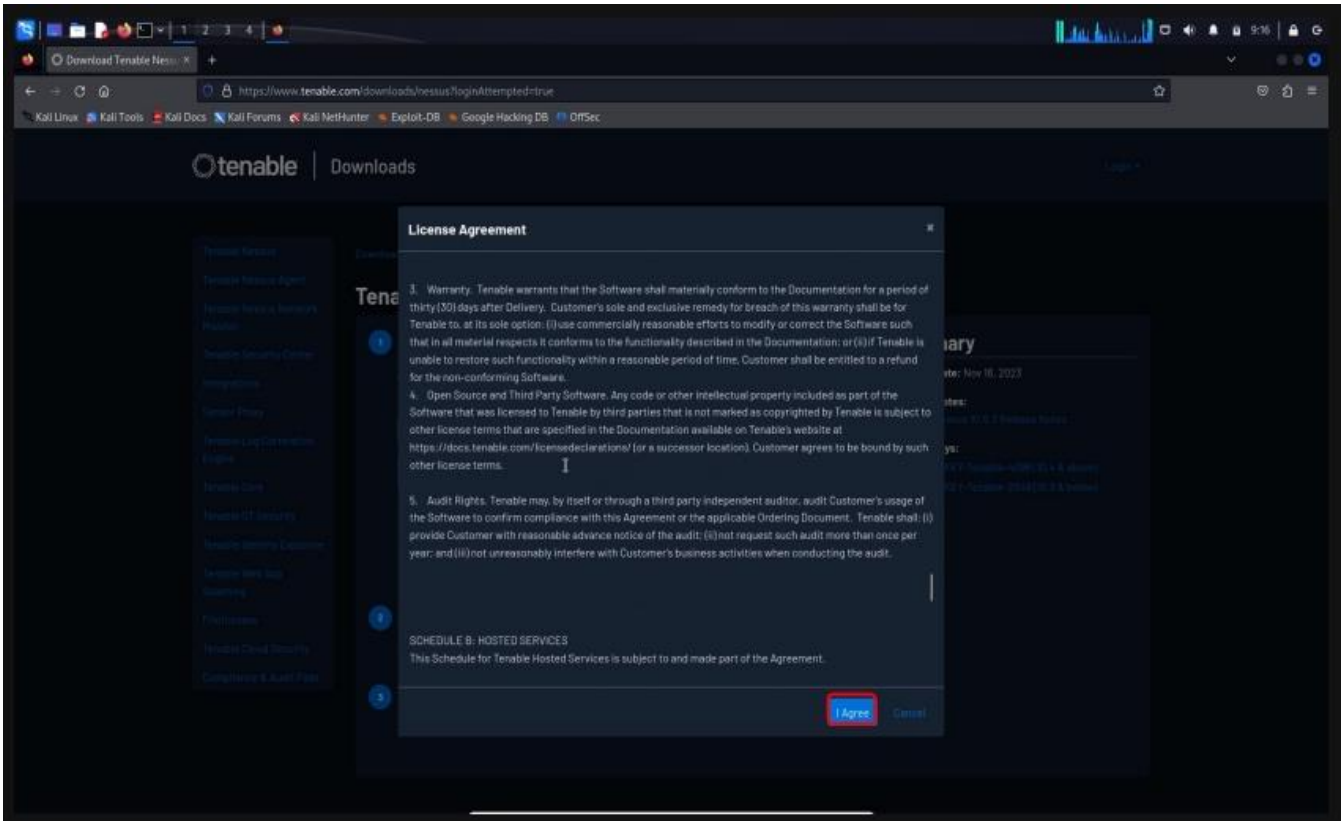
1. Go to website: https://www.tenable.com/downloads/nessus?loginAttempted=true



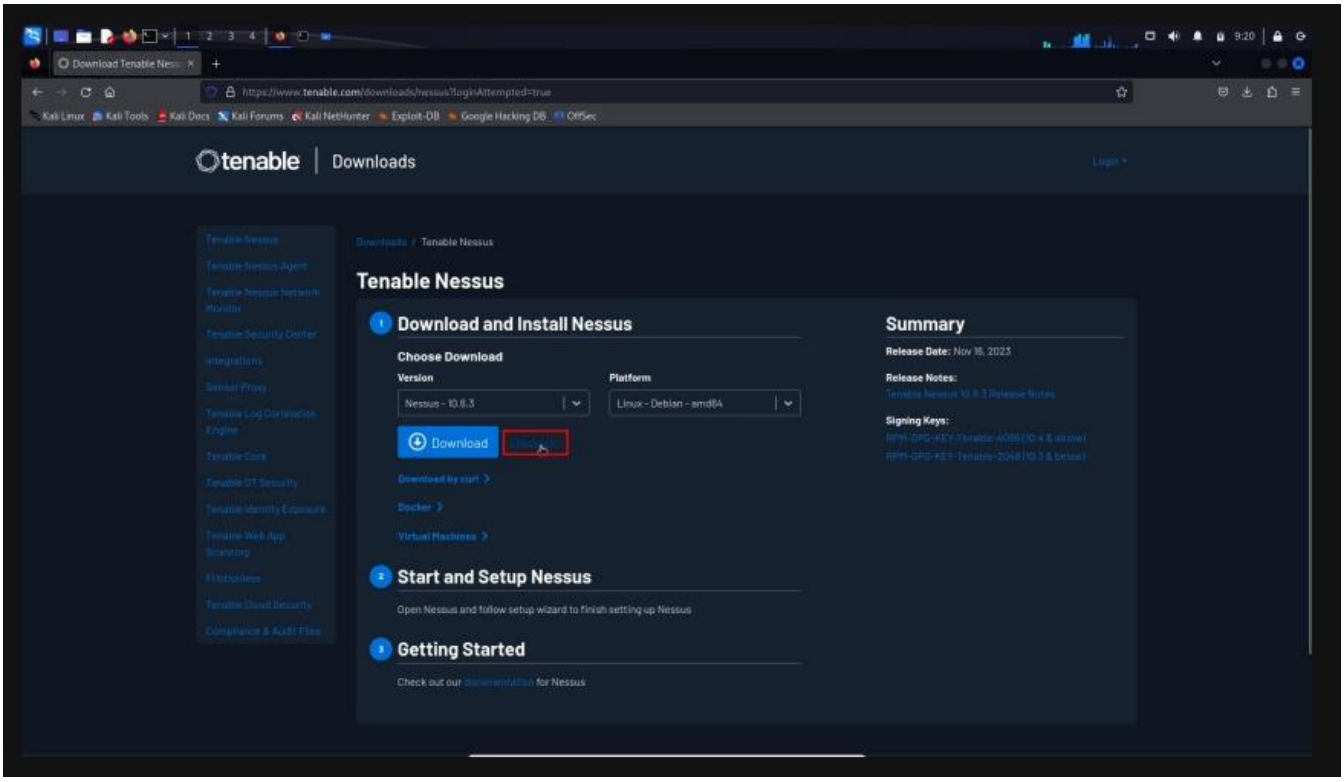
2. From Platform search for Linux - Debian – amd64 and download the file



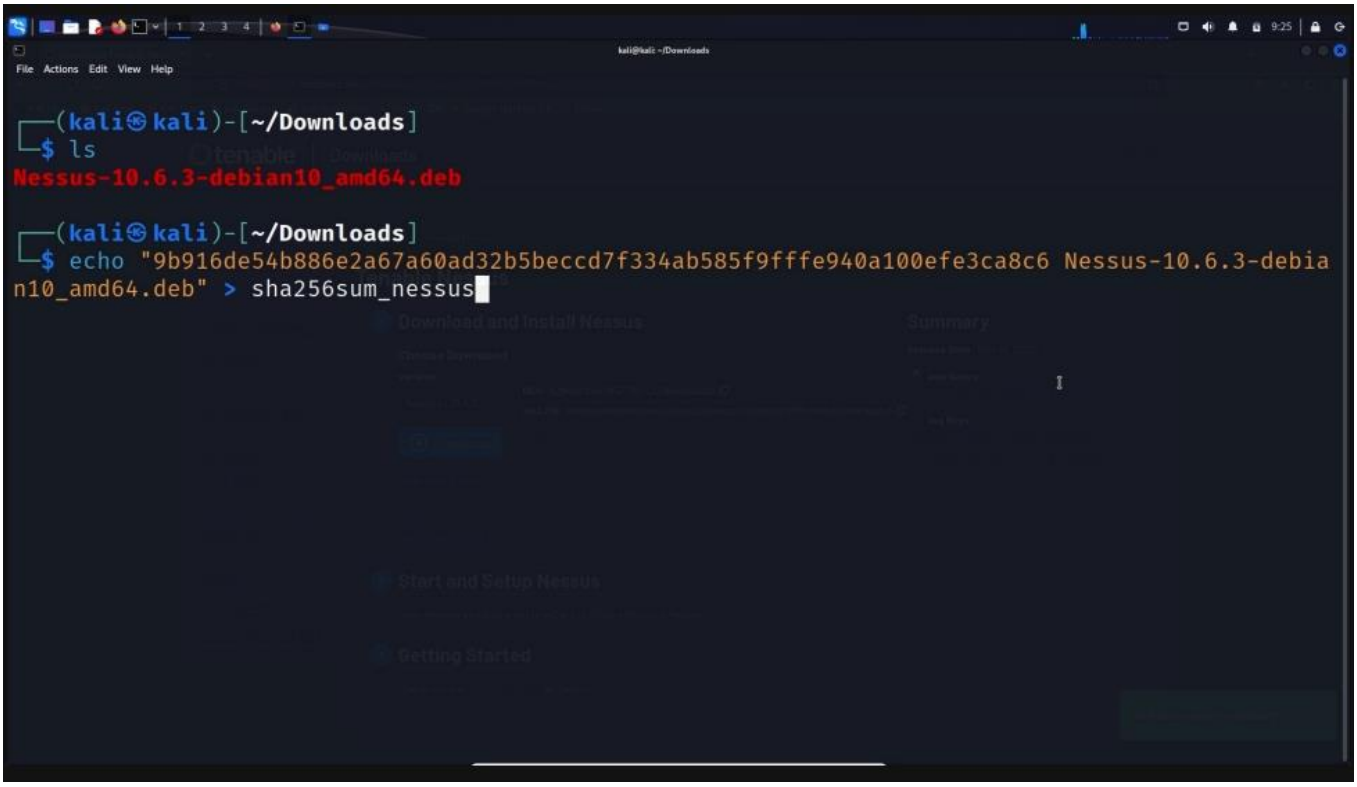
3. Agree to the License Agreement



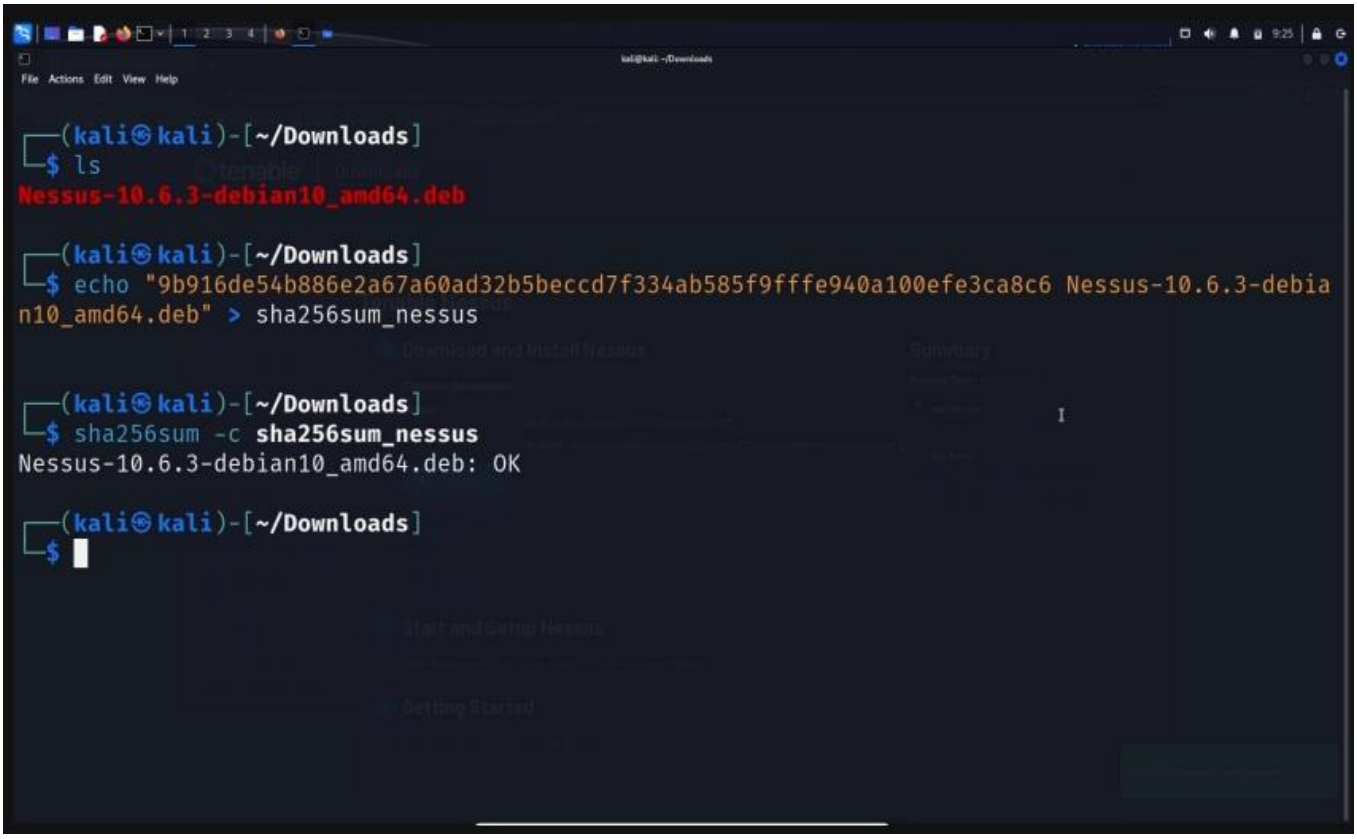
4. Click on Checksum right next to the download button and copy the SHA256 checksum



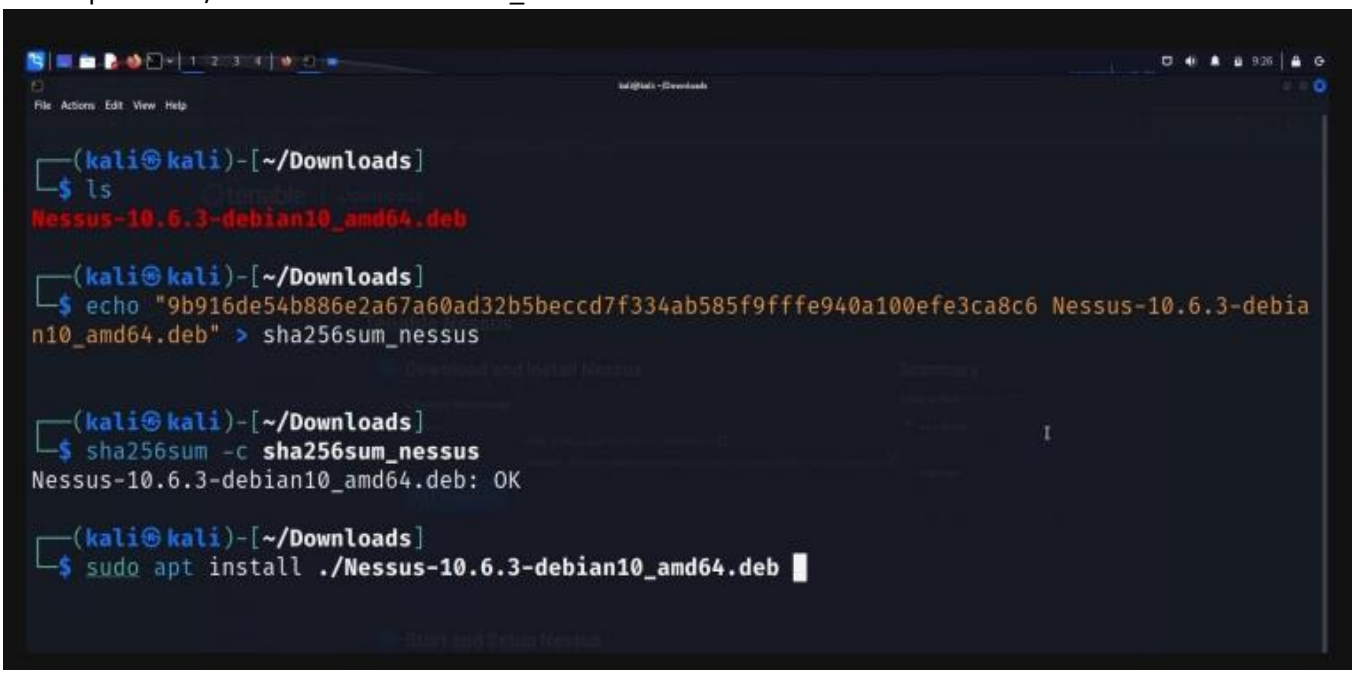
5. Open the ~/Downloads directory in the terminal and enter the following command (change the checksum and the Nessus version to the correct values):
   echo "9b916de54b886e2a67a60ad32b5beccd7f334ab585f9fffe940a100efe3ca8c6 Nessus-10.6.3-debian10_amd64.deb" > sha256sum_nessus



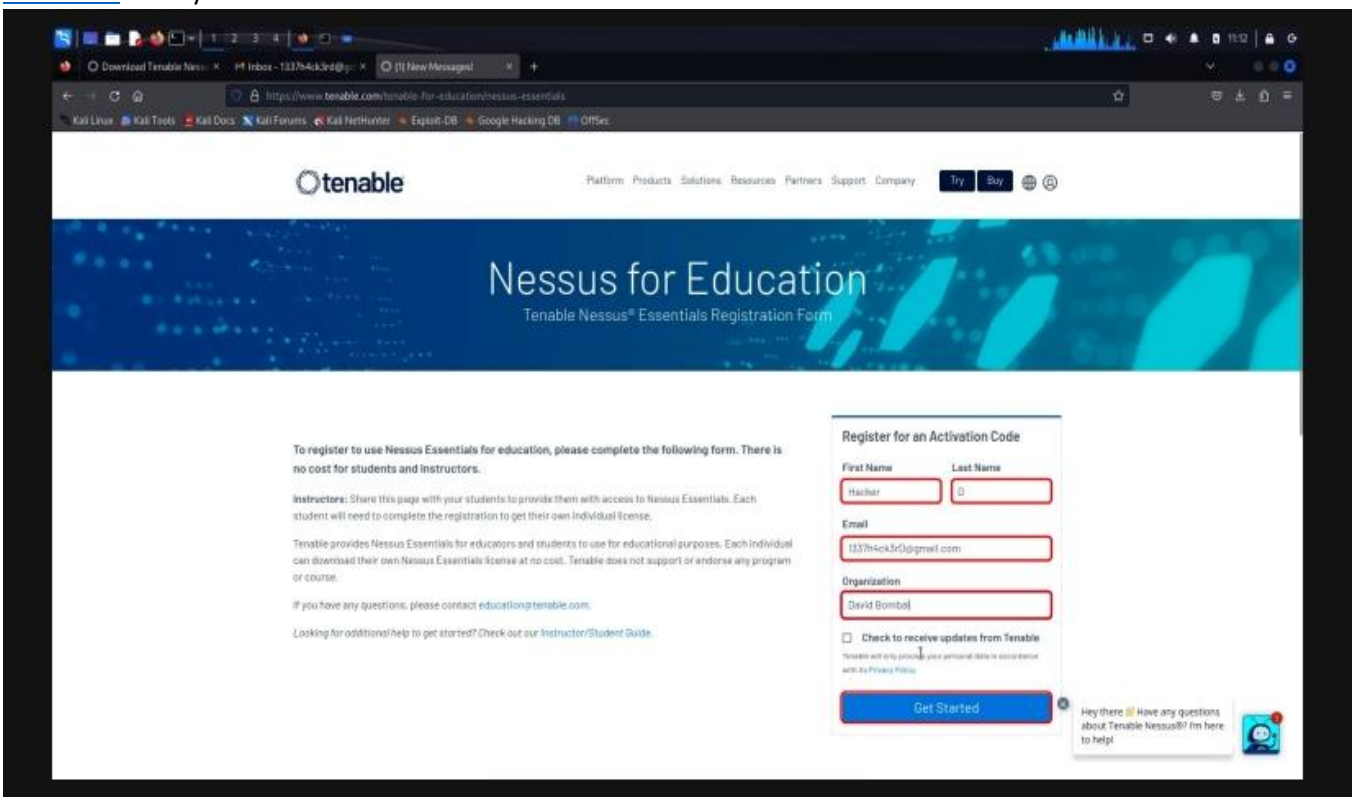
6. Run the command sha256sum –c sha256sum_nessus



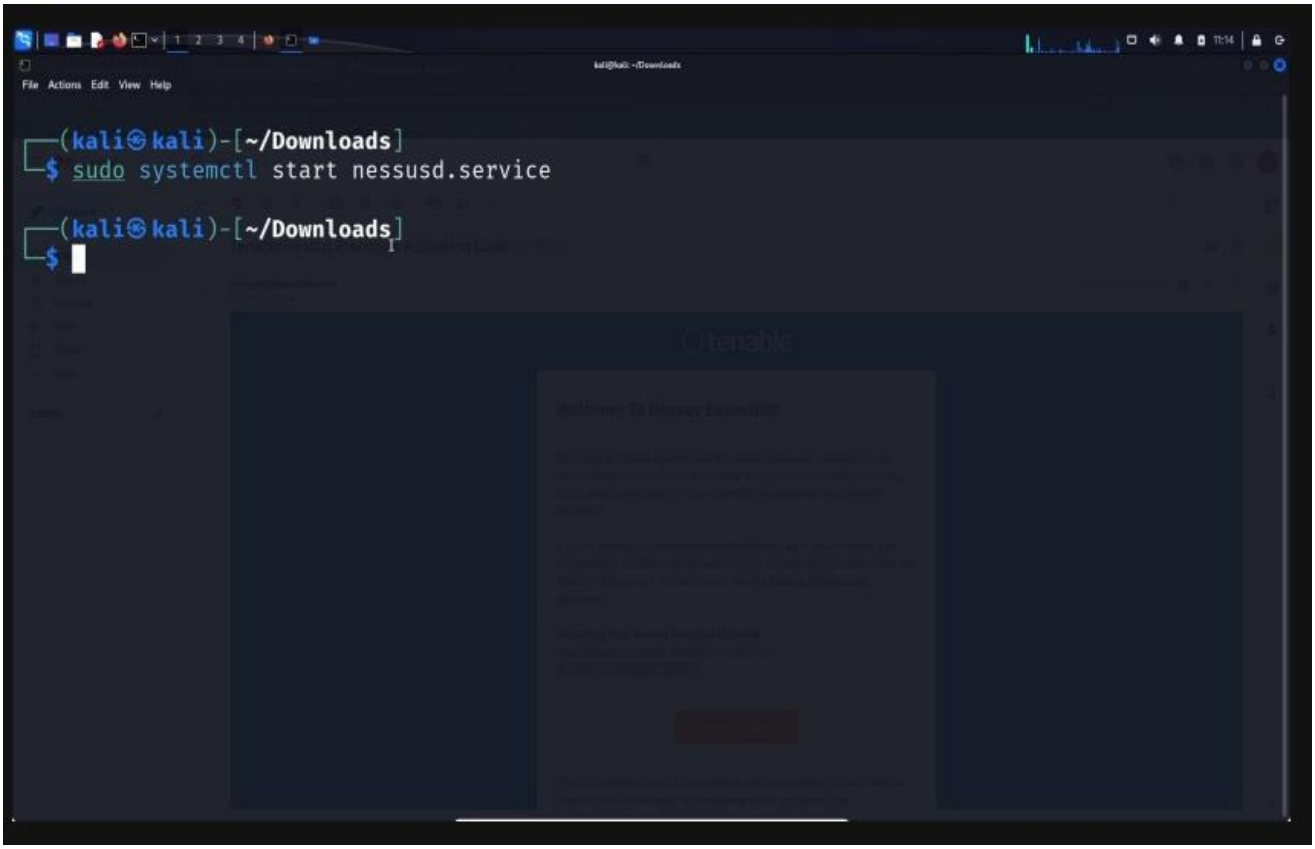
7. Install Nessus by running the command: (change the Nessus version to the correct value):
   sudo apt install ./ Nessus-10.6.3-debian10_amd64.deb This will install Nessus



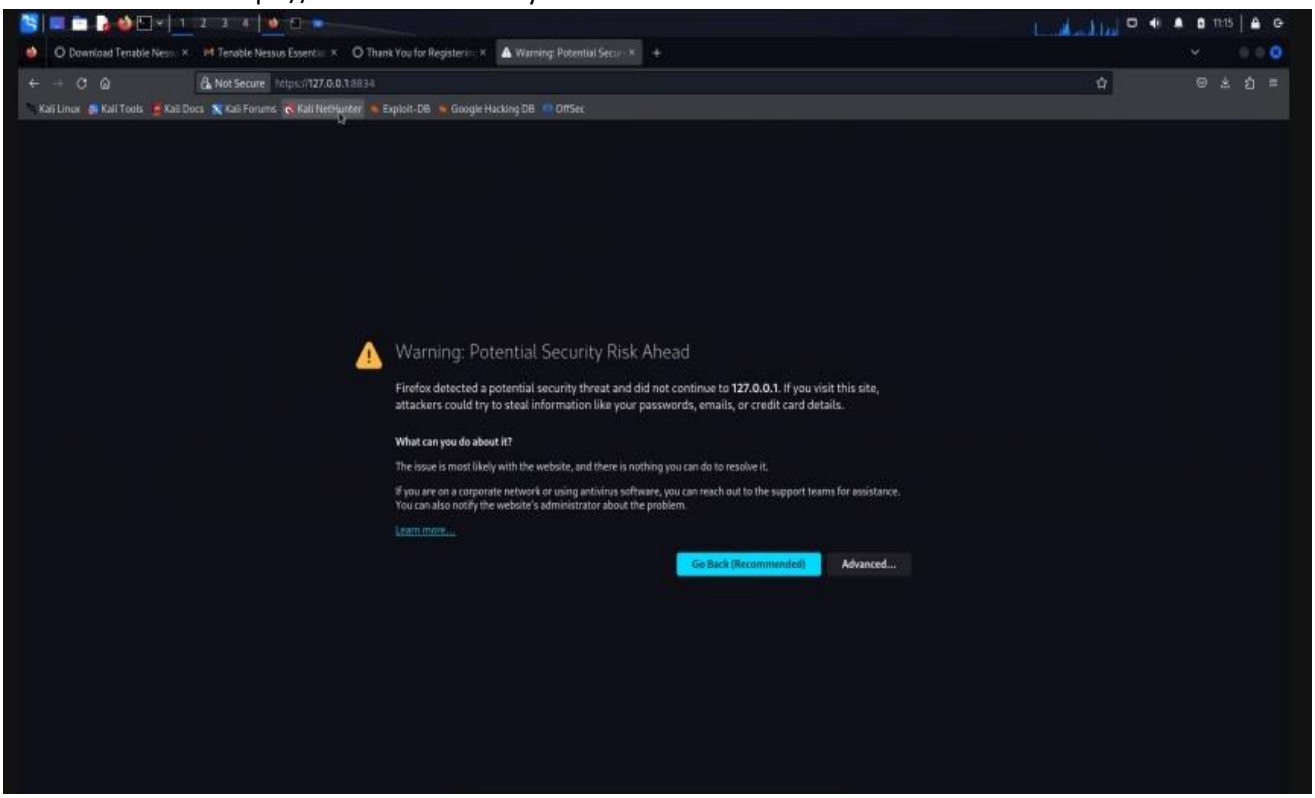
8. You will now need to go to the following website: https://www.tenable.com/tenable-for education/nessus-essentials fill in your details and click Get Started.



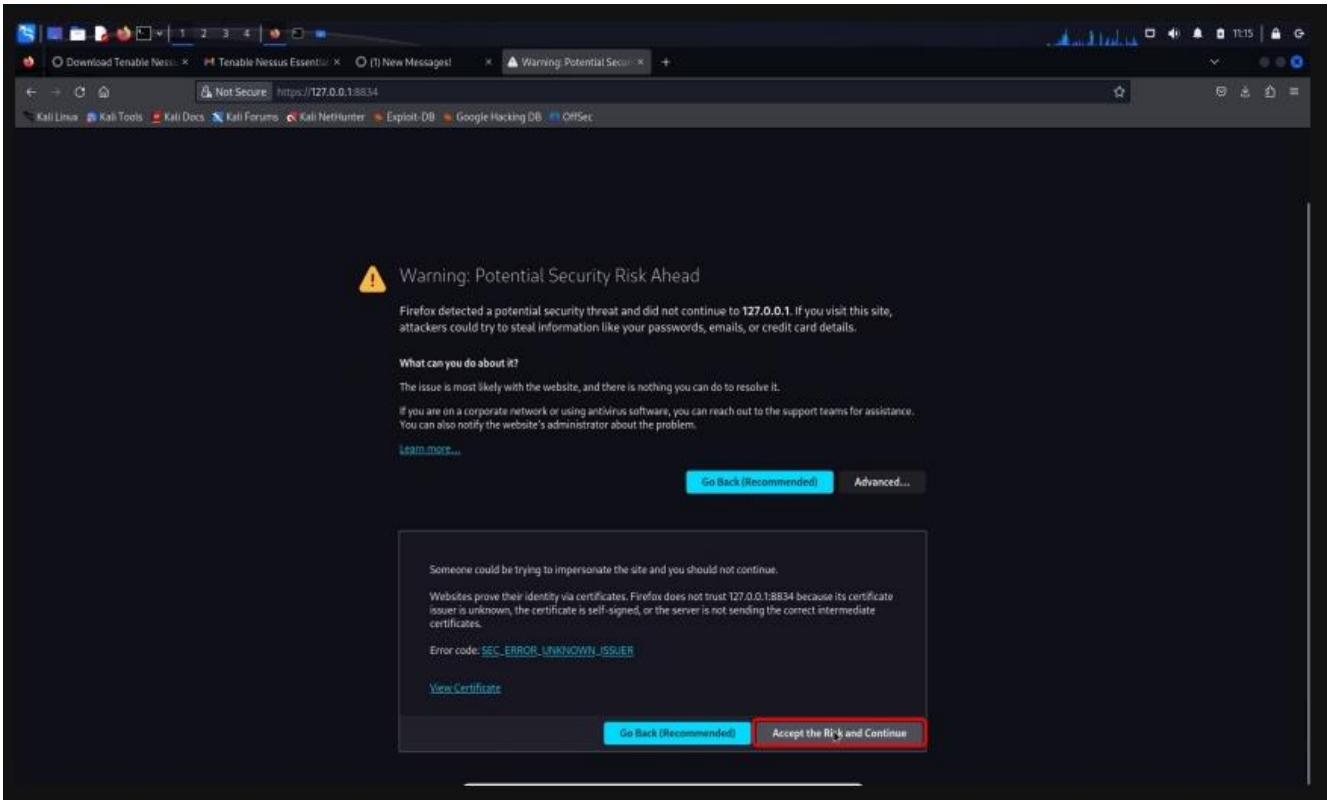
9. Open the terminal and run the command sudo systemctl start nessusd.service



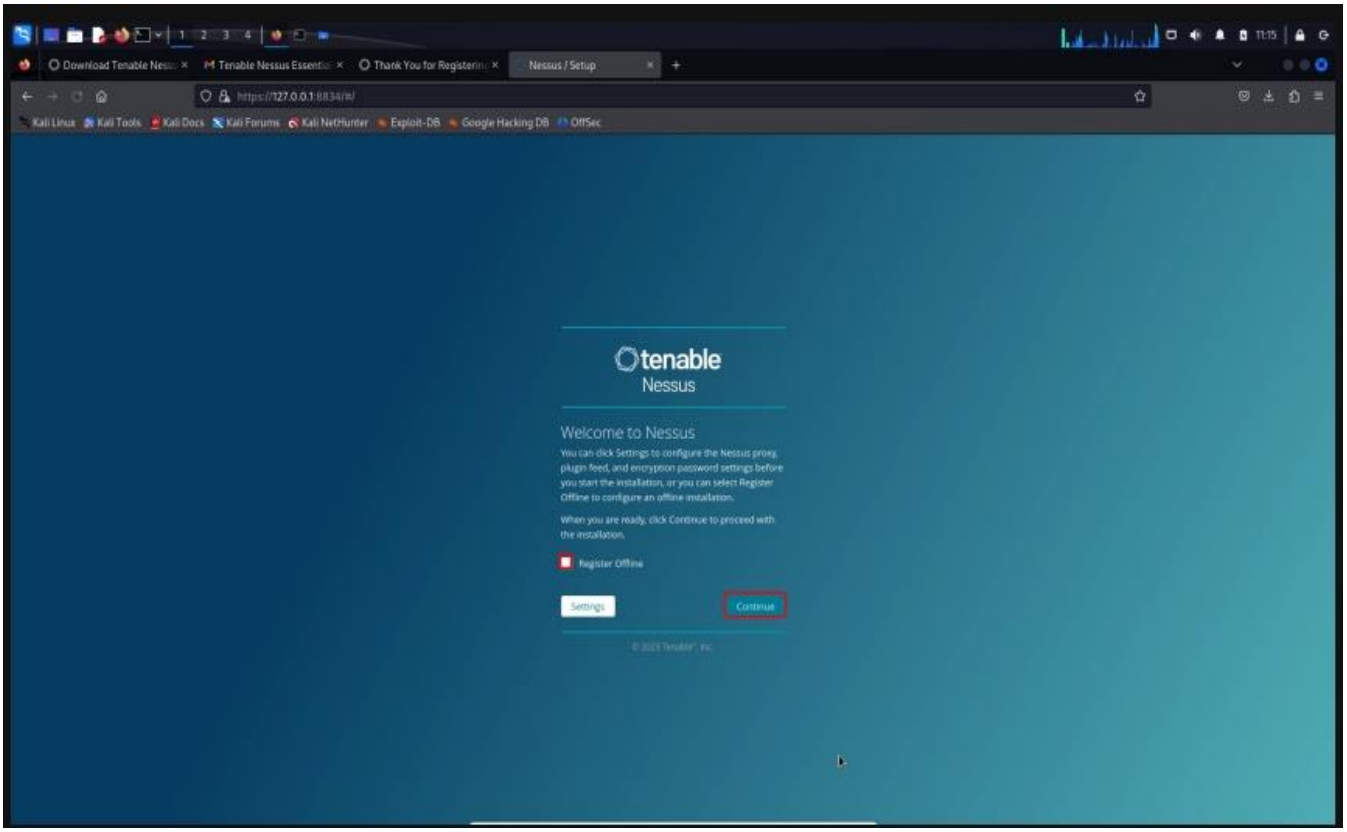
10. Enter the address https://127.0.0.1:8834 in your browser.



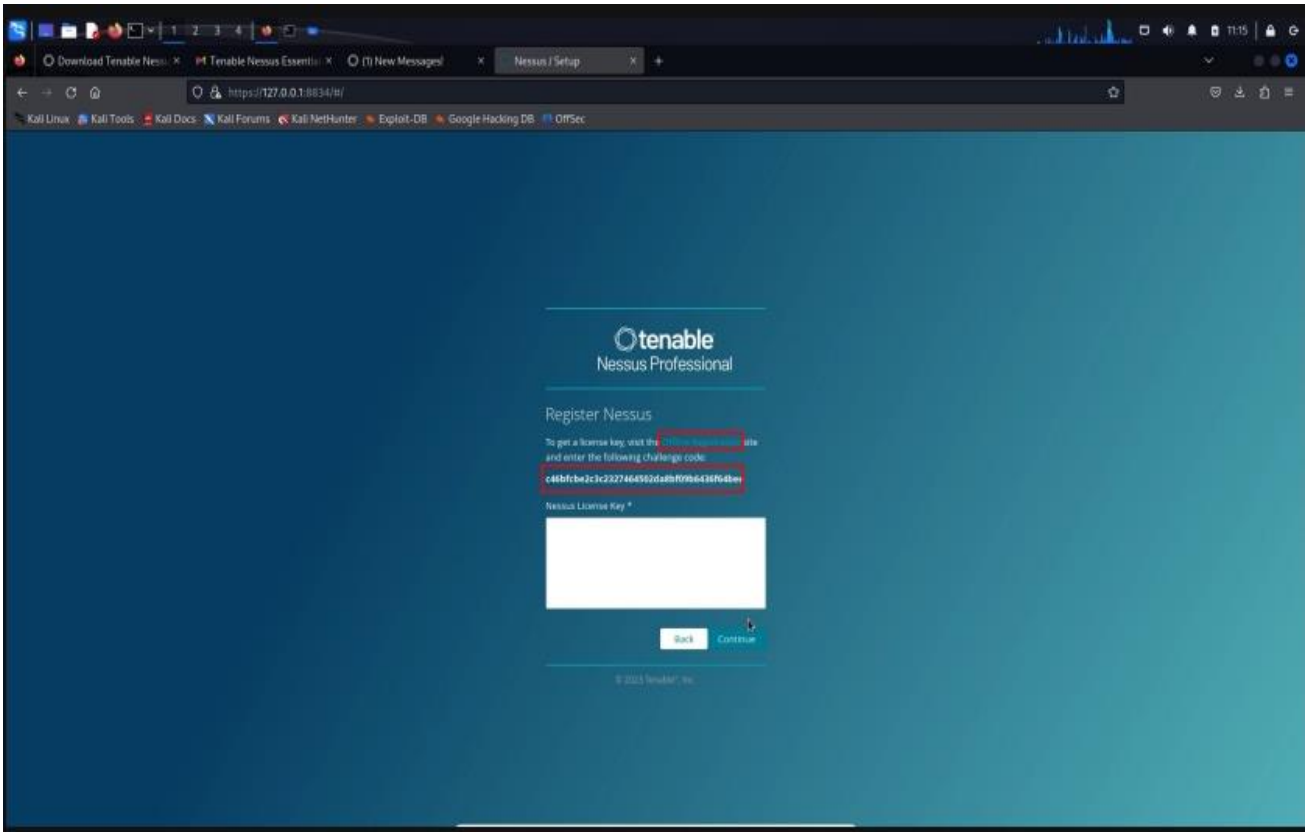
11. Click on Advanced. Click on Accept Risk and Continue.



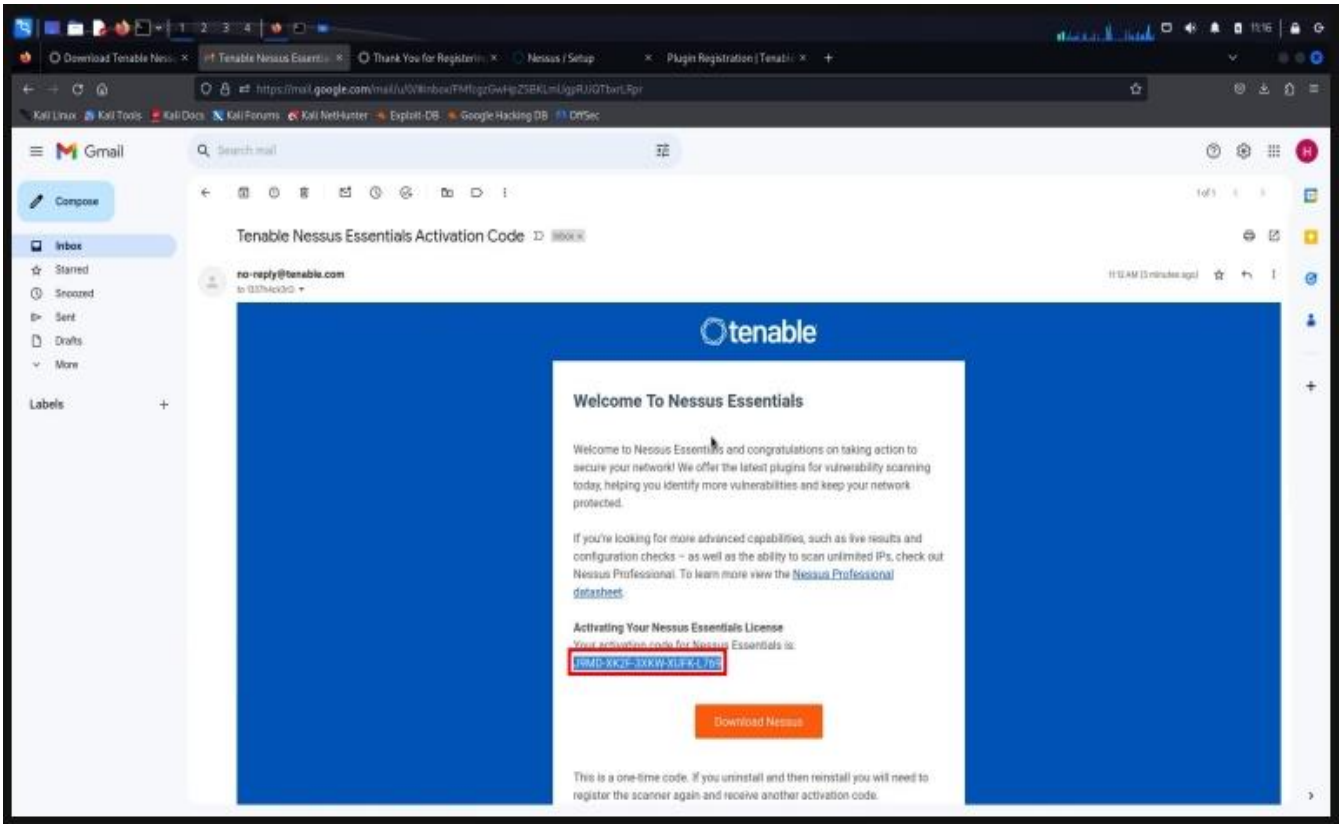
12. Select Register Offline and click Continue.



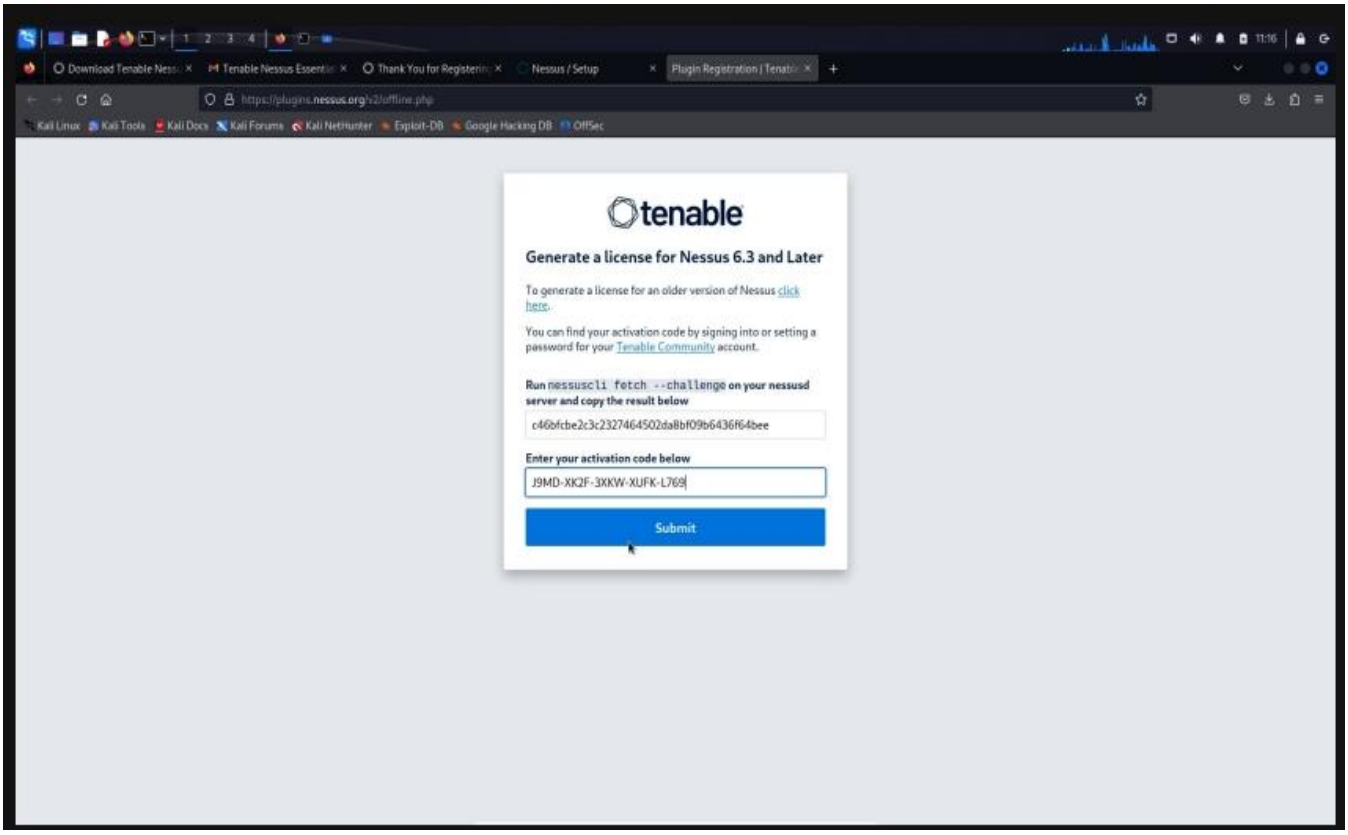
13. Copy the challenge code and select Offline Registration



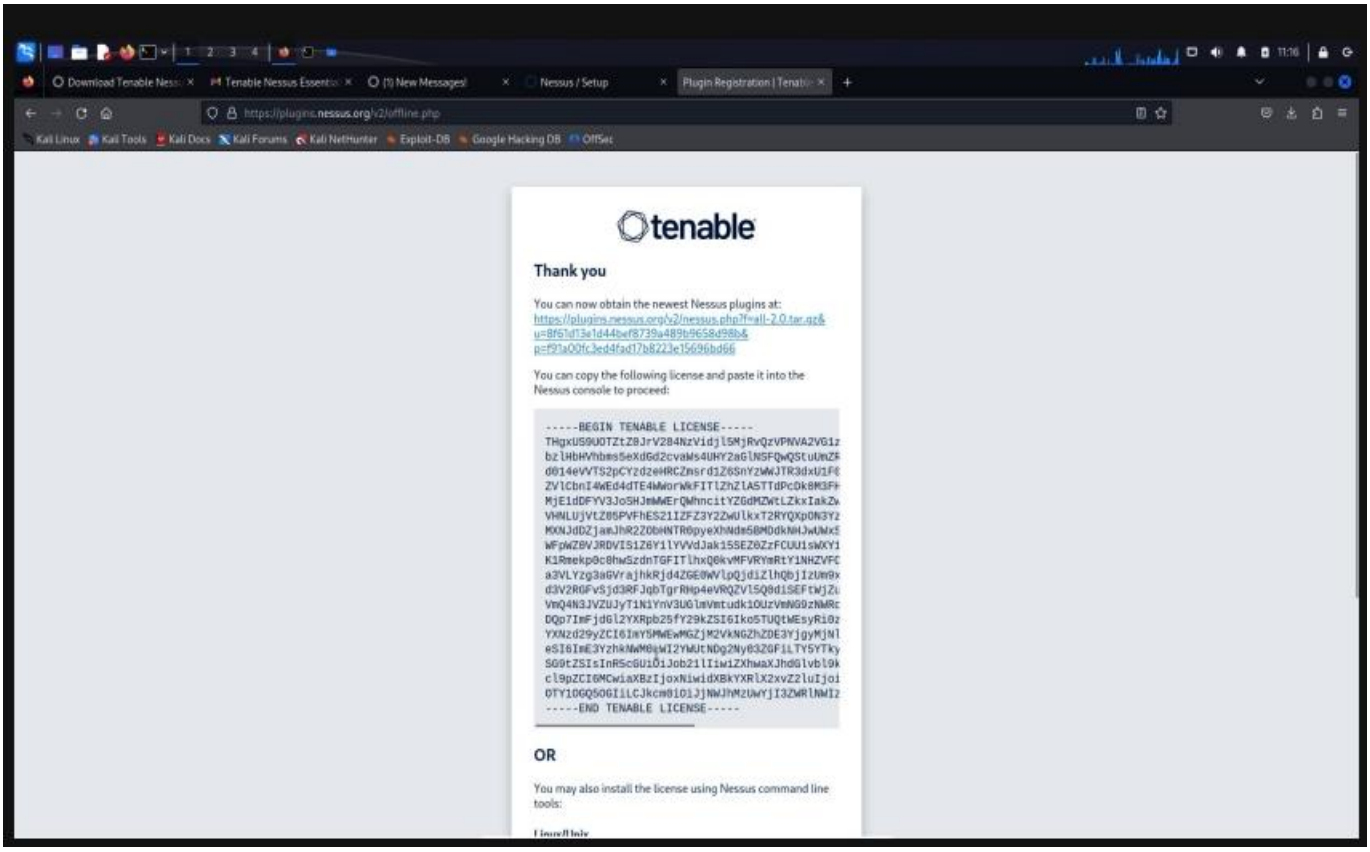
14. Copy your code to Activate Your Nessus Essentials License



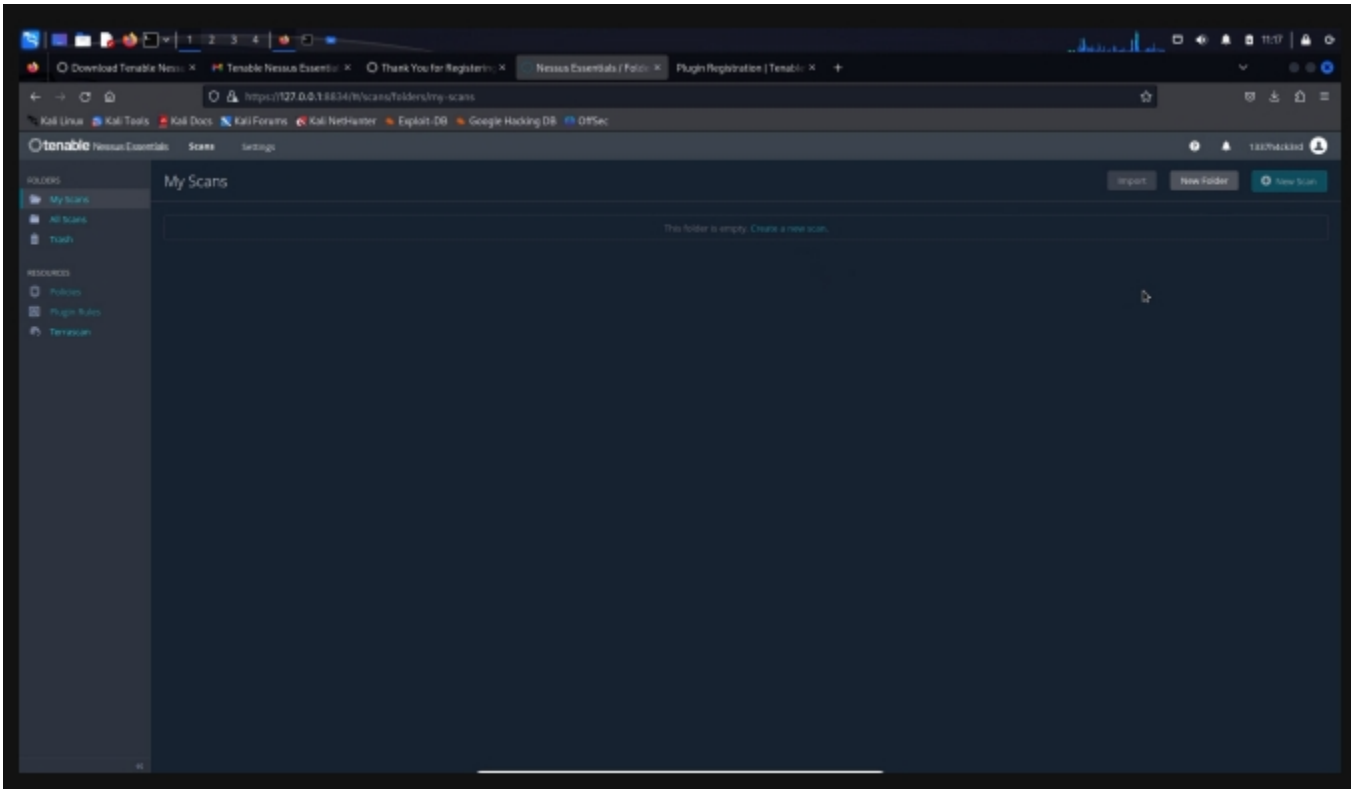
15. Copy the license code



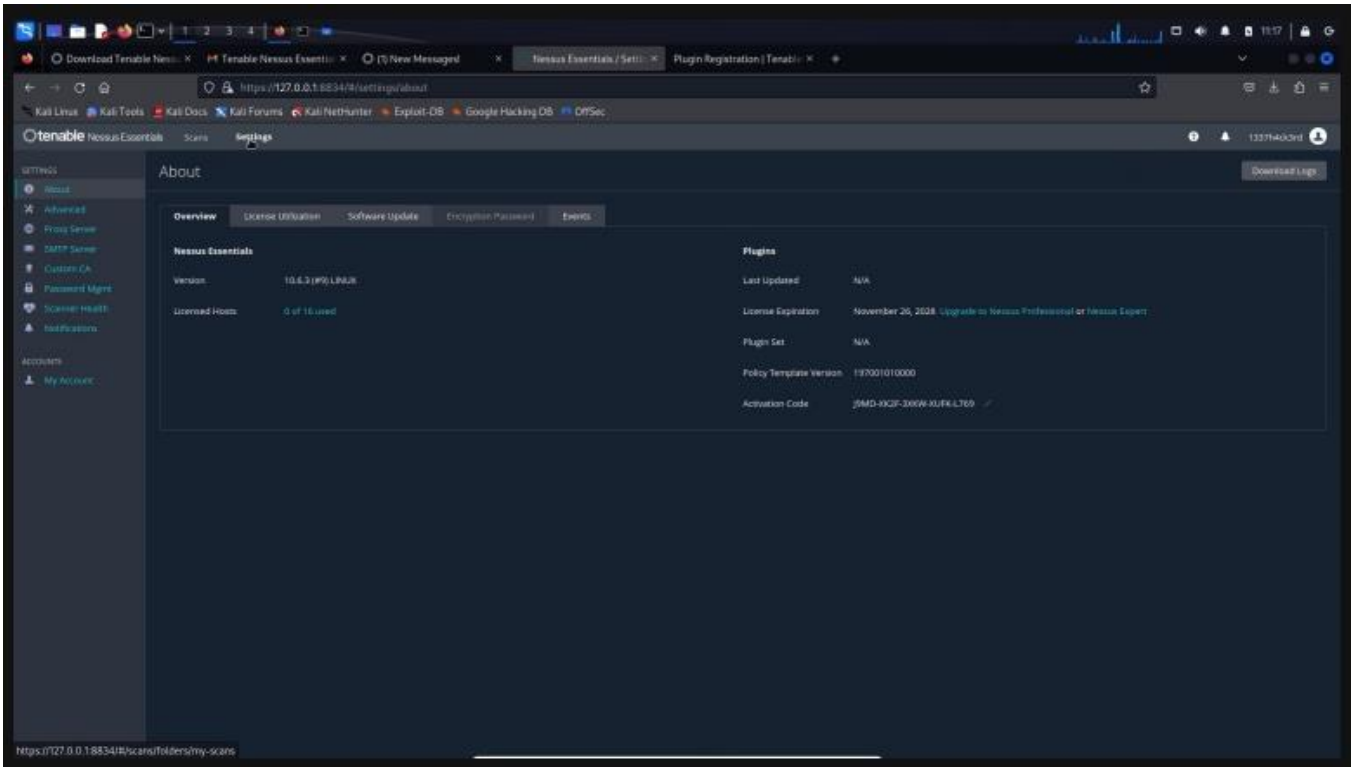
16. Paste it under Nessus License Key, and click continue



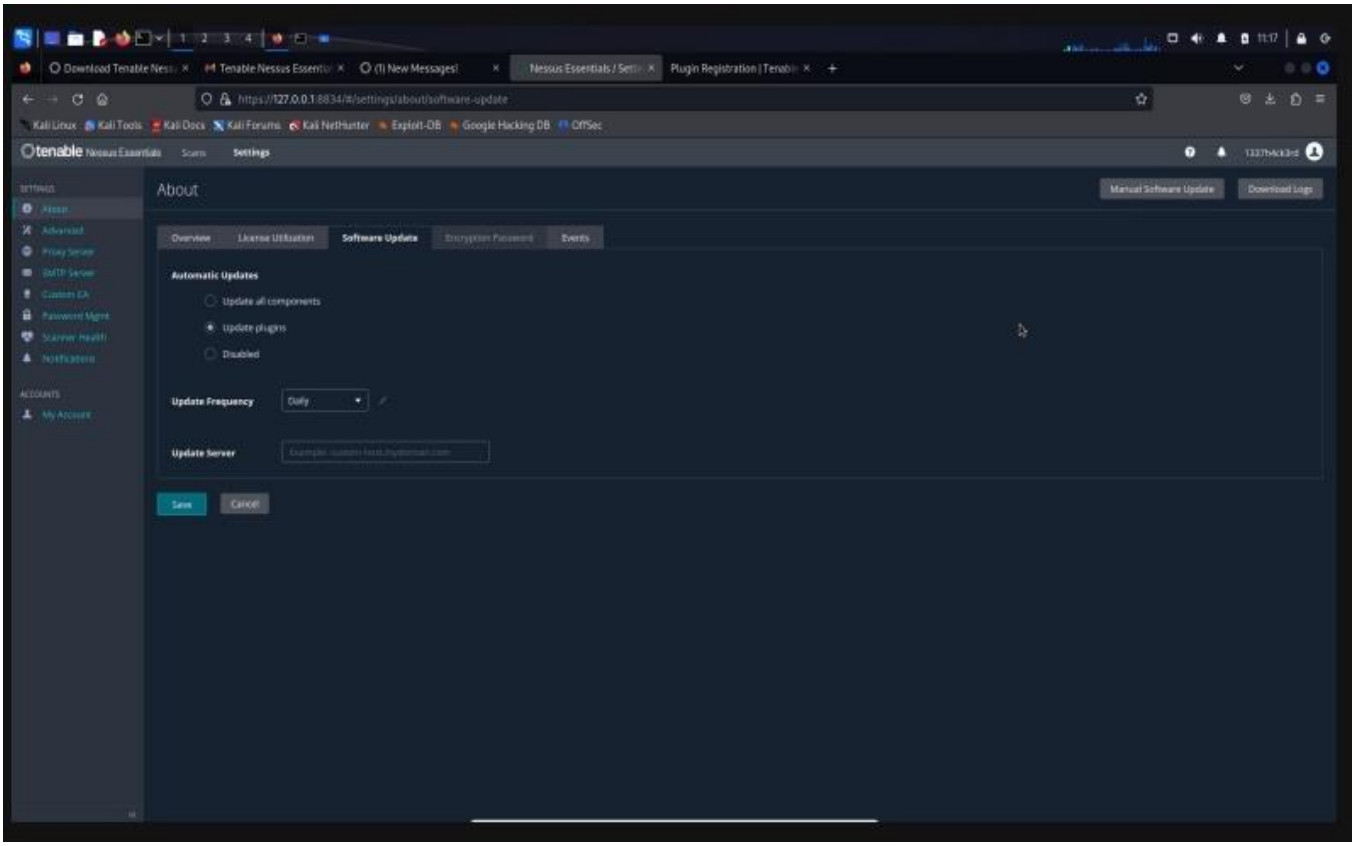
17. Nessus has started



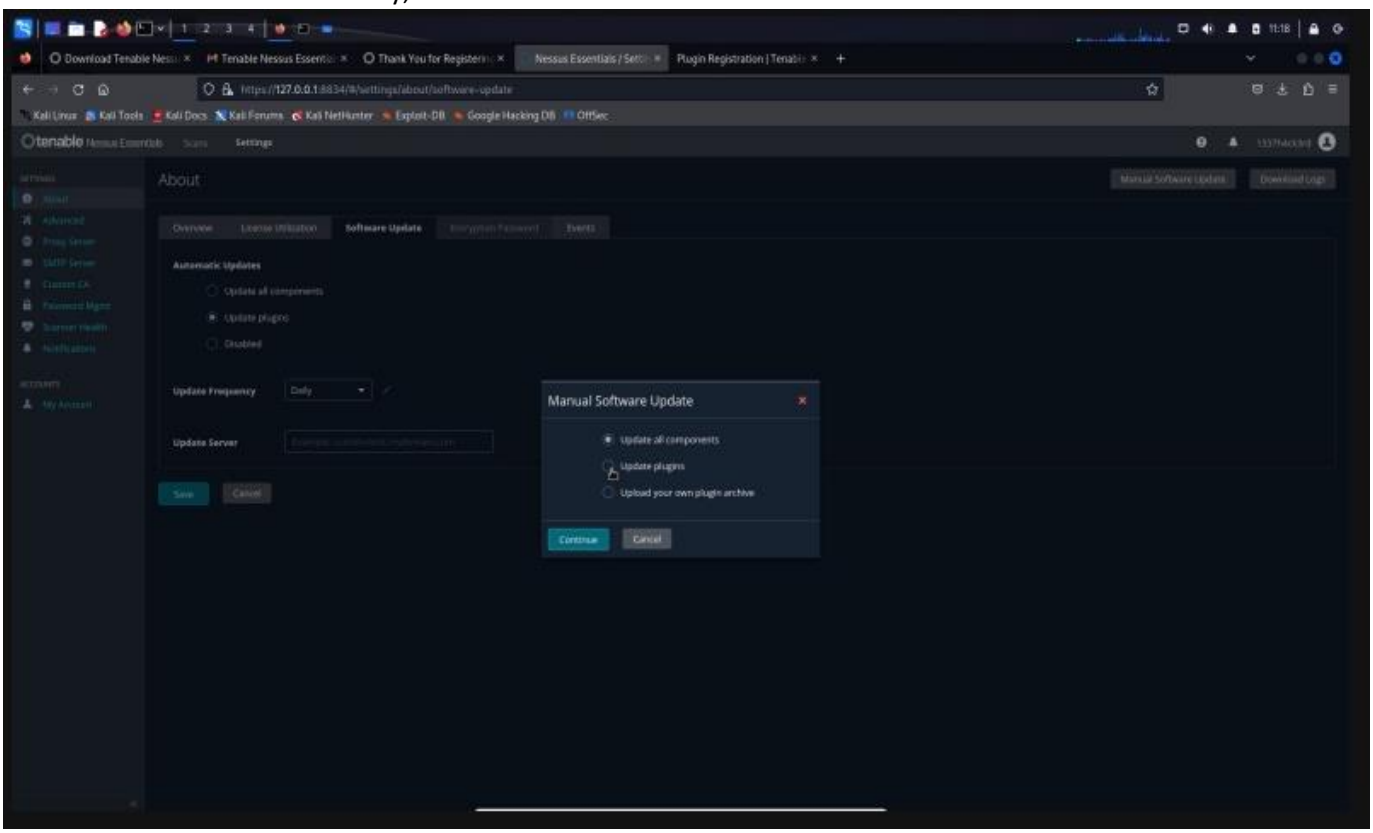
18. Go to settings



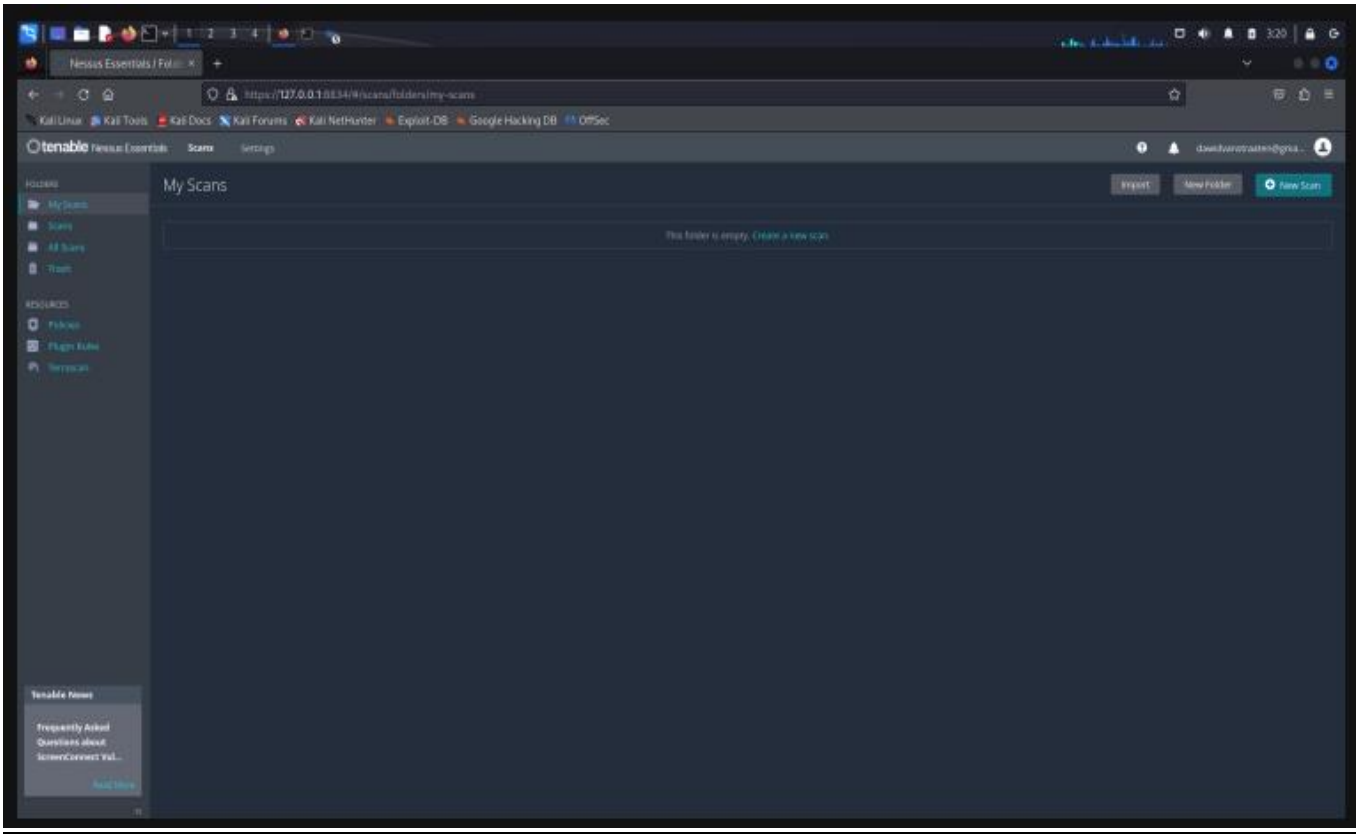
19. Select Software Update



20. Paste it under Nessus License Key, and click continue



21. We can create a scan by Clicking on Create a new scan or the New Scan button



Q 1 : Performing a Vulnerability scan on the Metasploitable Machine.

Process

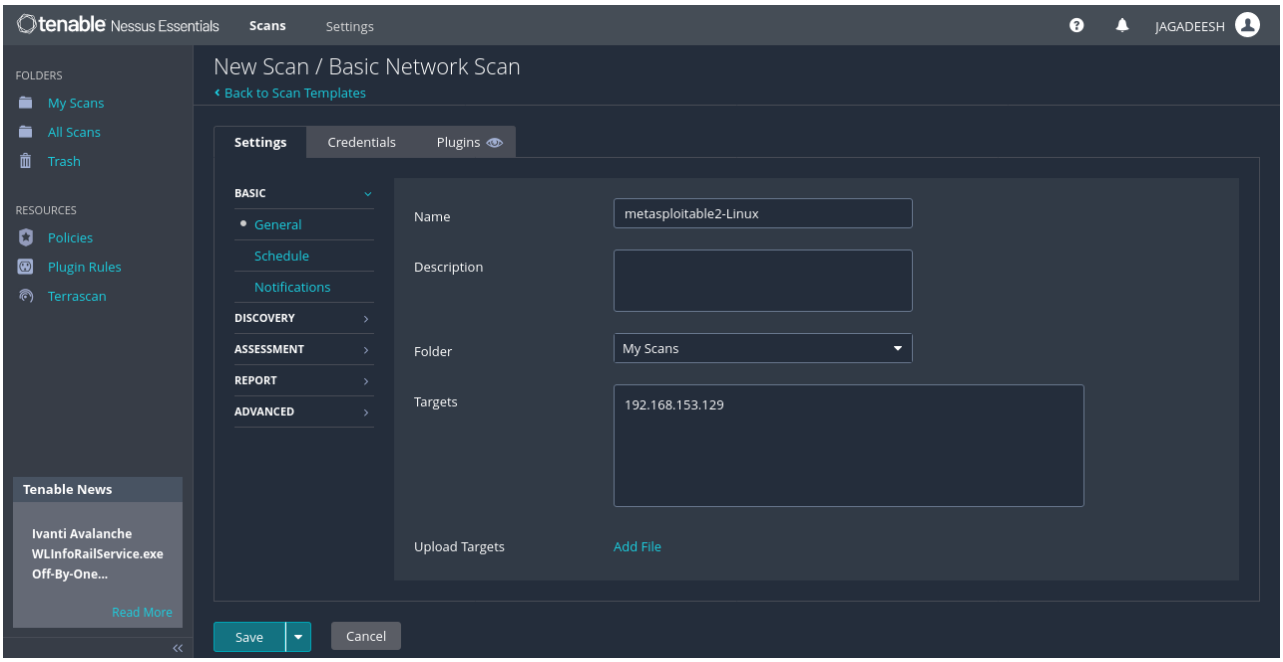
Note : We need to be in the same network during the Scanning process

Step 1 – Add the Metasploitable Machine into your Machine and Login with the given Credentials. Then find the IP address of the Metasploitable machine using the command “ip addr”

```
          Interrupt:17 Base address:0x2000

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:214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:79221 (77.3 KB)  TX bytes:79221 (77.3 KB)

msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:b7:ca:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.153.129/24 brd 192.168.153.255 scope global eth0
    inet6 fe80::20c:29ff:feb7:ca47/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:b7:ca:51 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

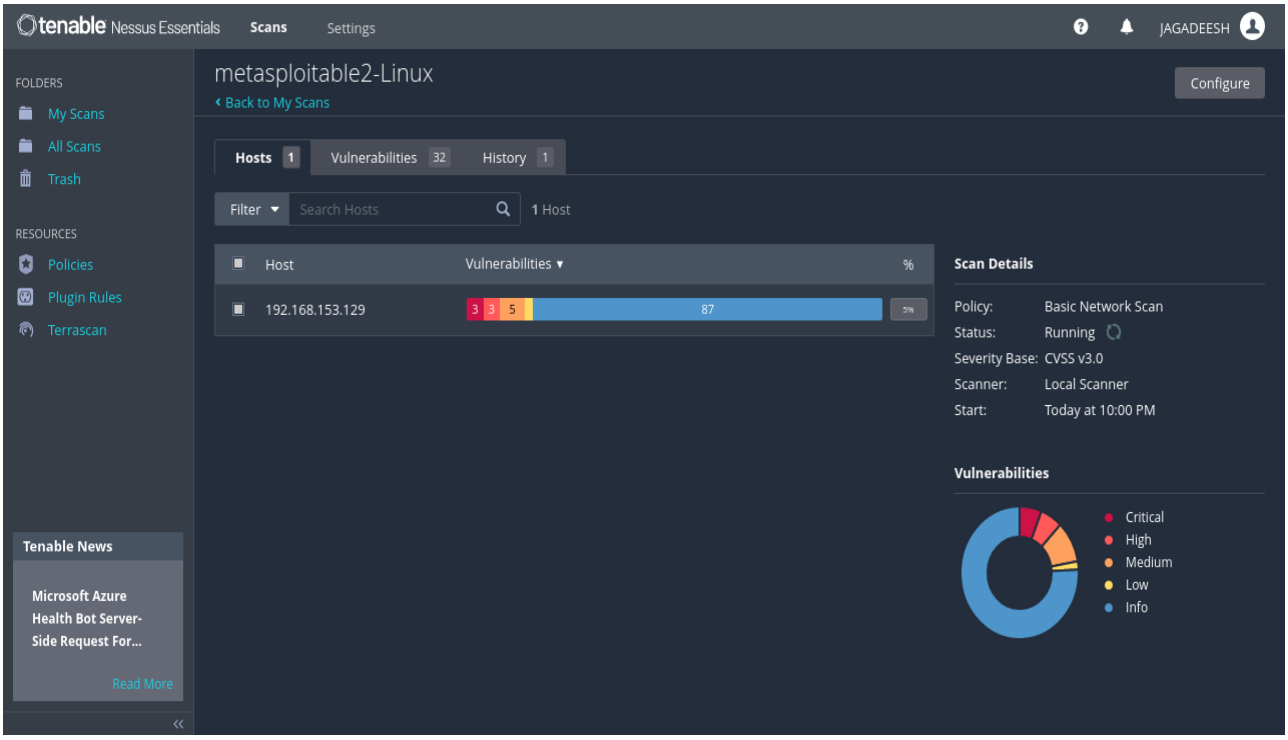
Here our IP address is 192.168.153.129

Step 2 – Create a New scan and give a Name and Target 192.168.153.129 in the Nessus

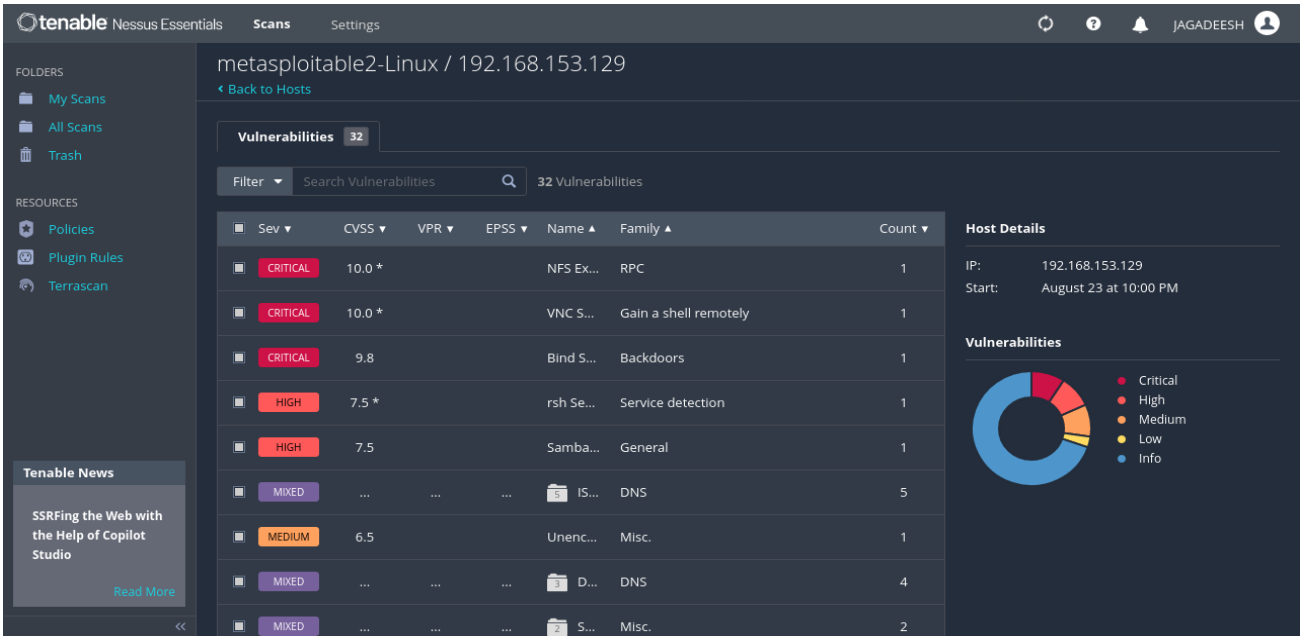


Then click save.

Step 3 – Then start the scanning. It takes some time



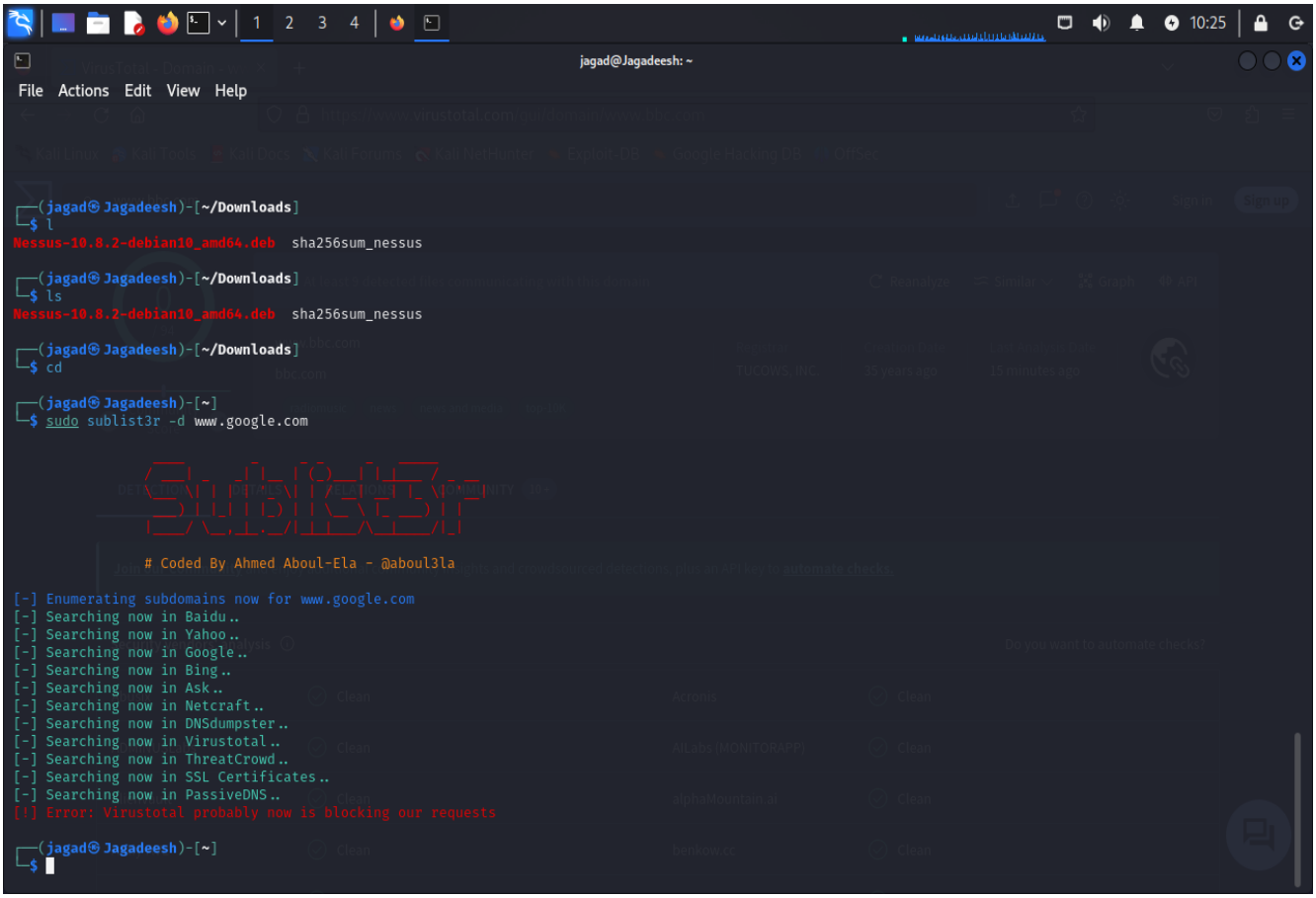
Step 4 – To get a Detailed scanning report click on the Numbers on the Vulnerabilities columns



Q 2 : Utilize the Tools like sublist3r and Maltego along with the search engine netcraft to discover the subdomains of the target bbc.com

Using sublist3r:
Step 1 – Open the terminal and install sublist3r using the command “sudo apt install sublist3r”.

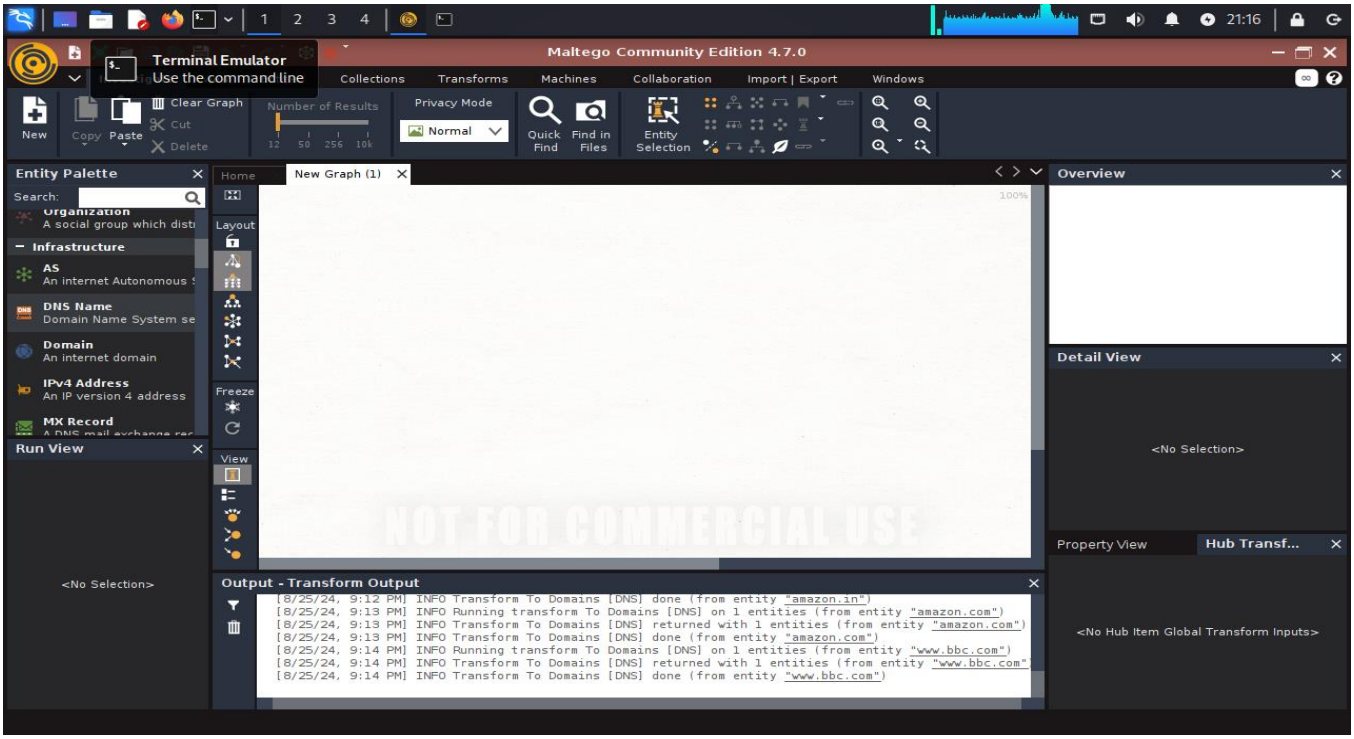
Step2 – Then type the command “sublist3r bbc.com” as a root user to get the list of subdomains of bbc.com



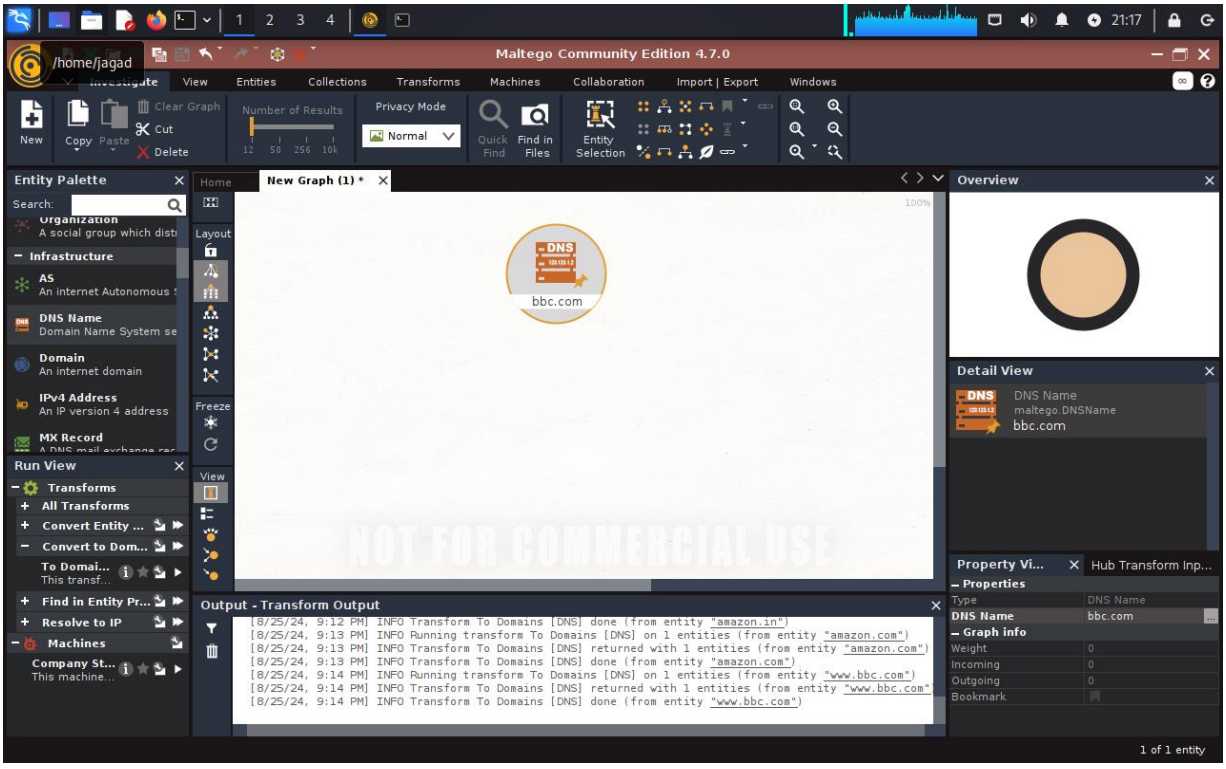
Using Maltego

Step1 – Install the software Maltego and register into it to get the access to use it

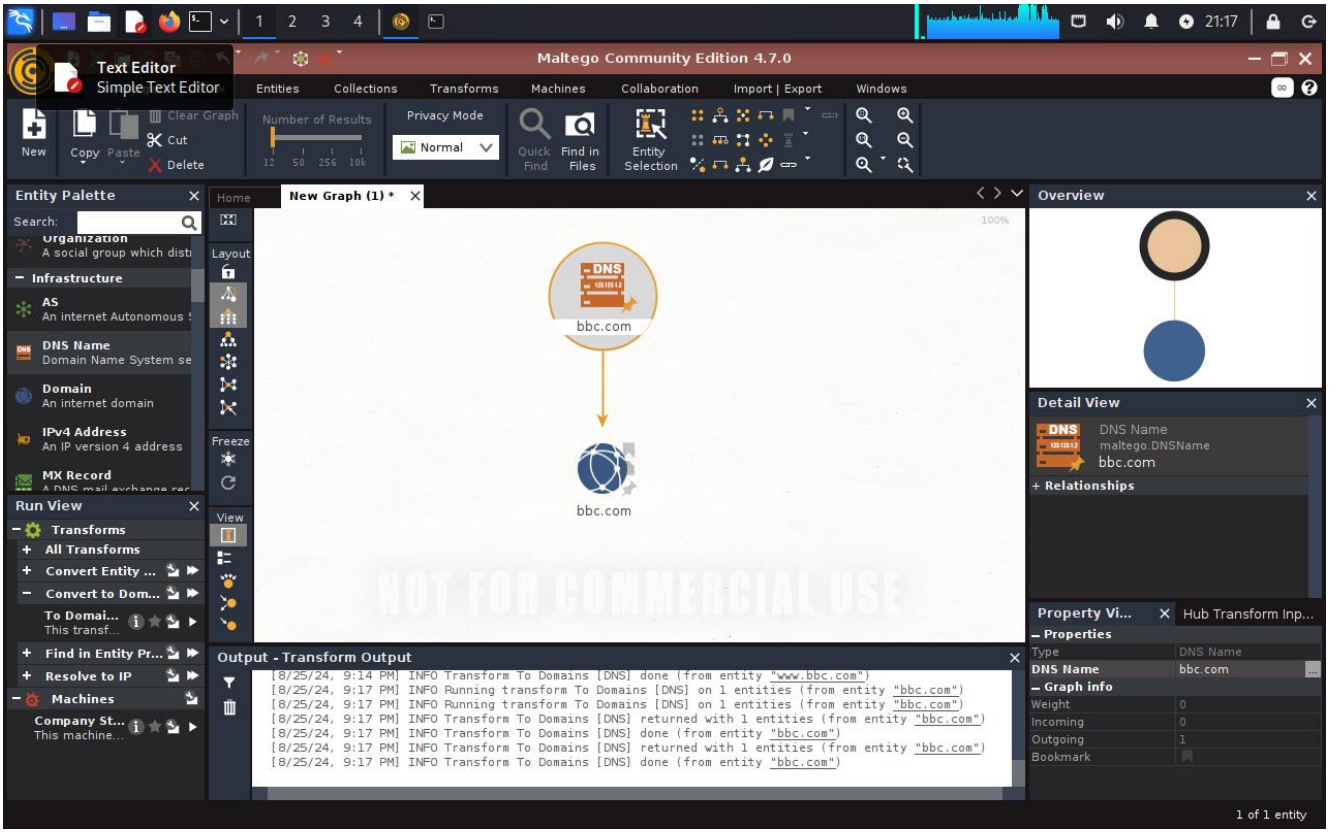
Step2 – After Register and login create a new file by clicking on the + icon on the top left.



Step3 – from the left side drag the icon DNS Name into plane, and then change the name as bbc.com by typing at the bottom right place DNS Name .

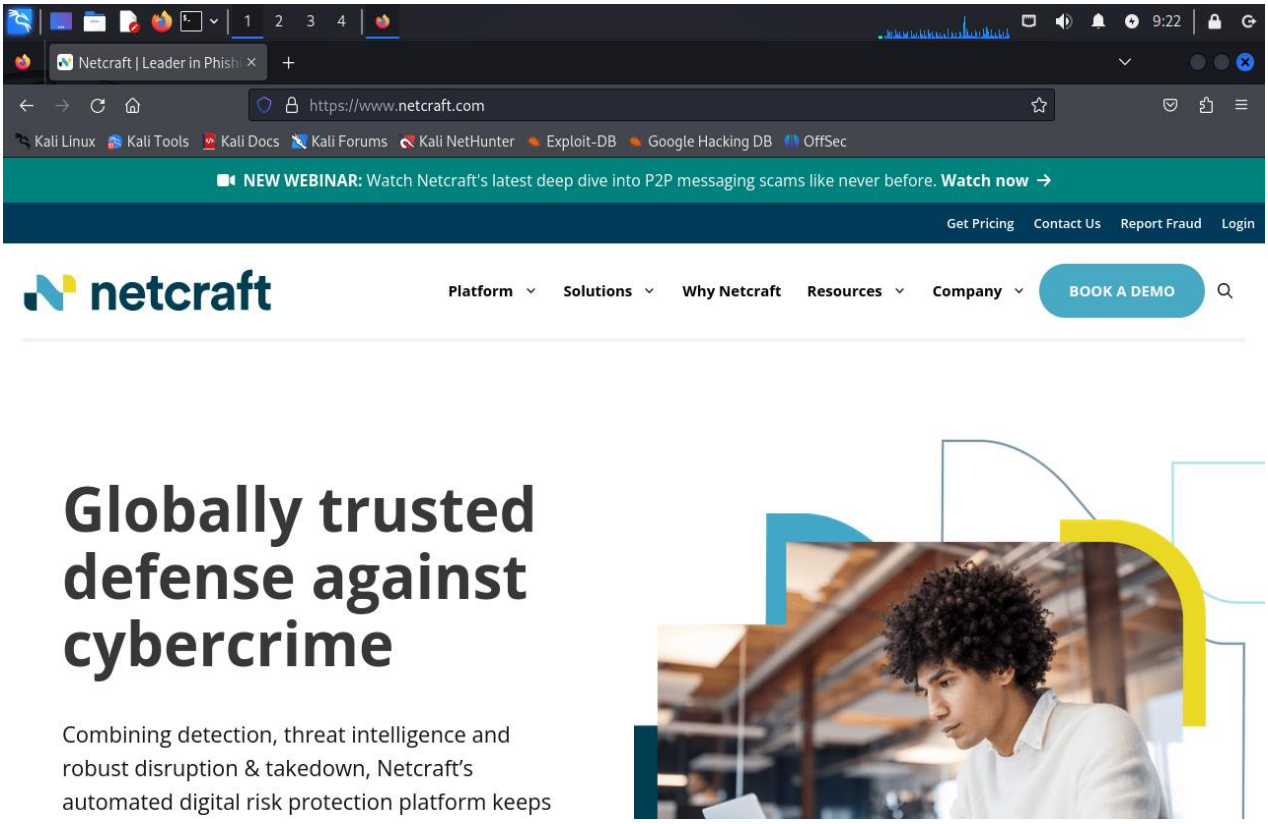


Step4 – Then click option convert to DNS Addresses from same DNS to get the SubDomains of bbc.com

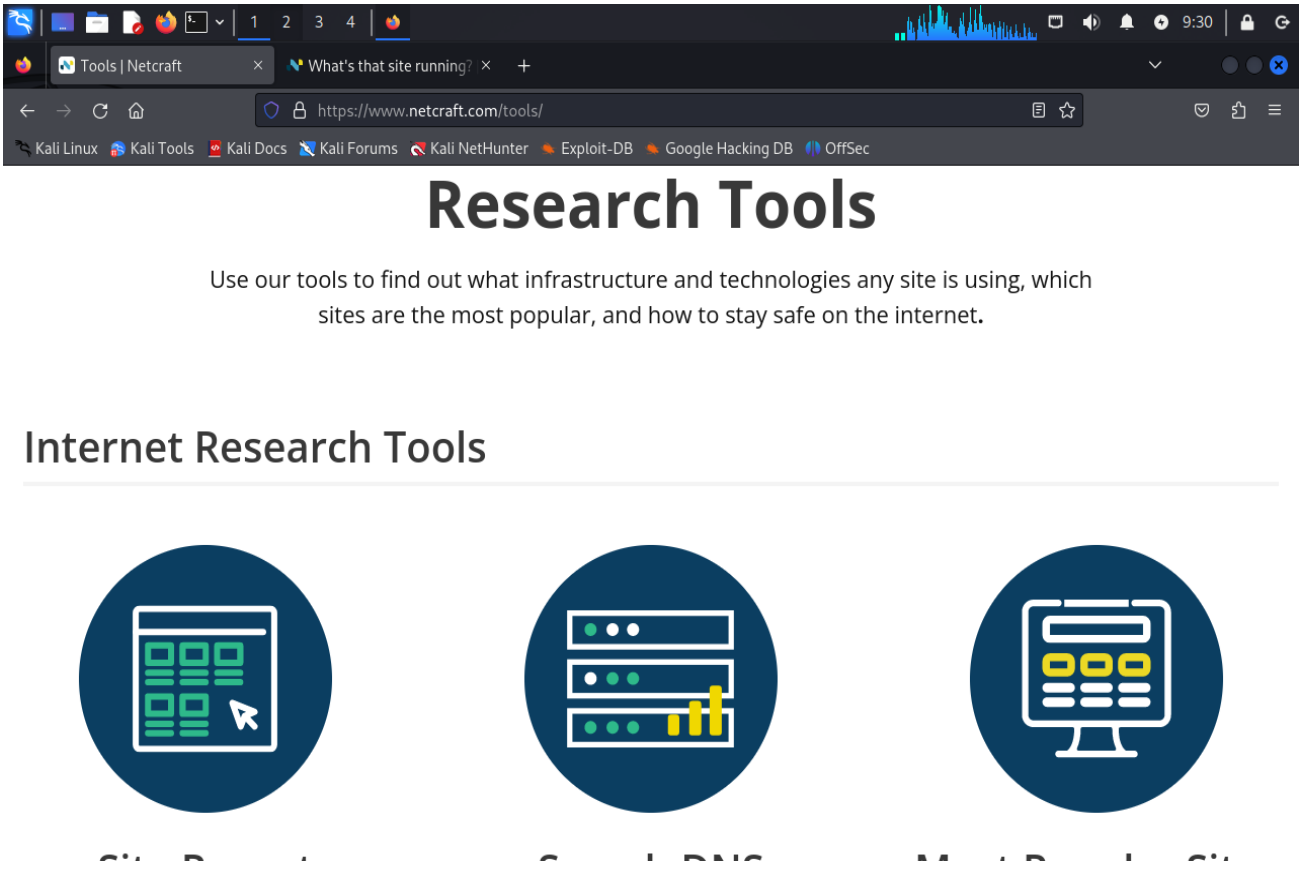


Using Netcraft

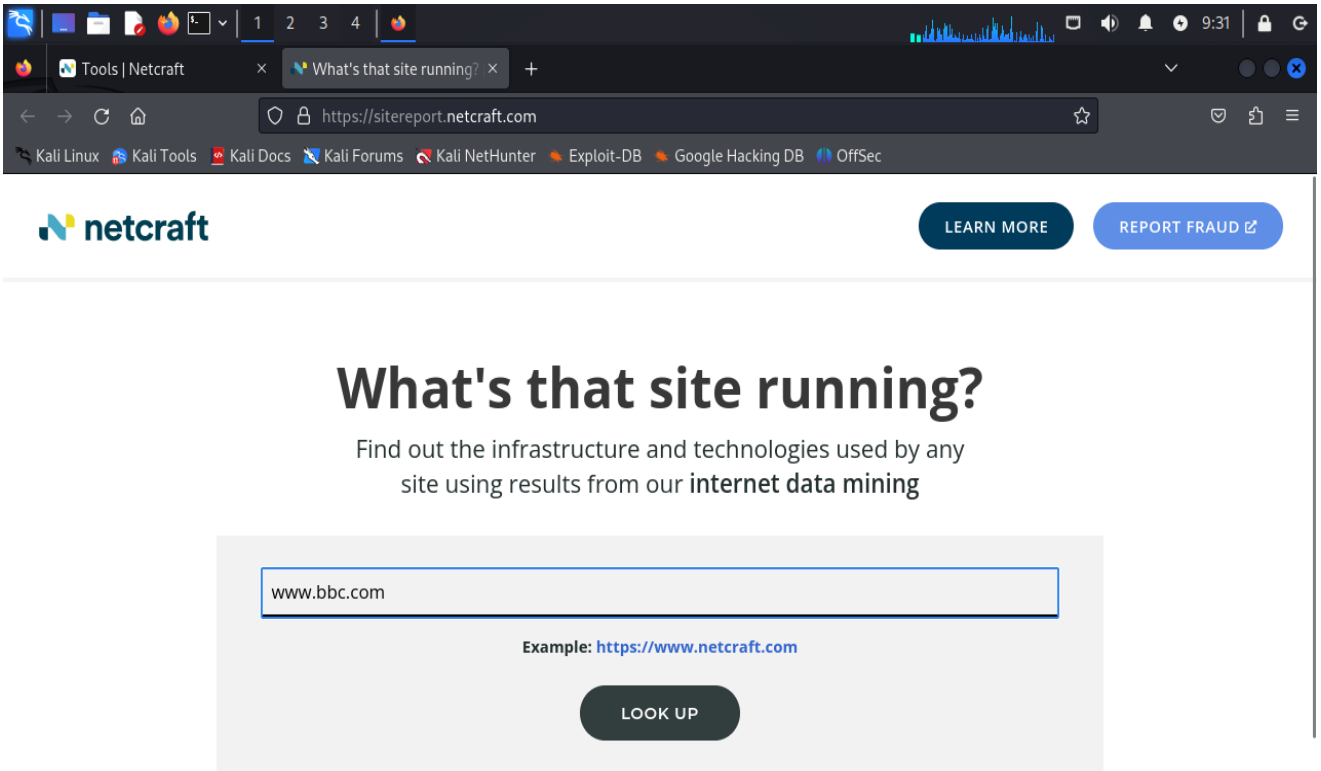
Step1 – Open a new window on browser and type http://www.netcraft.com.



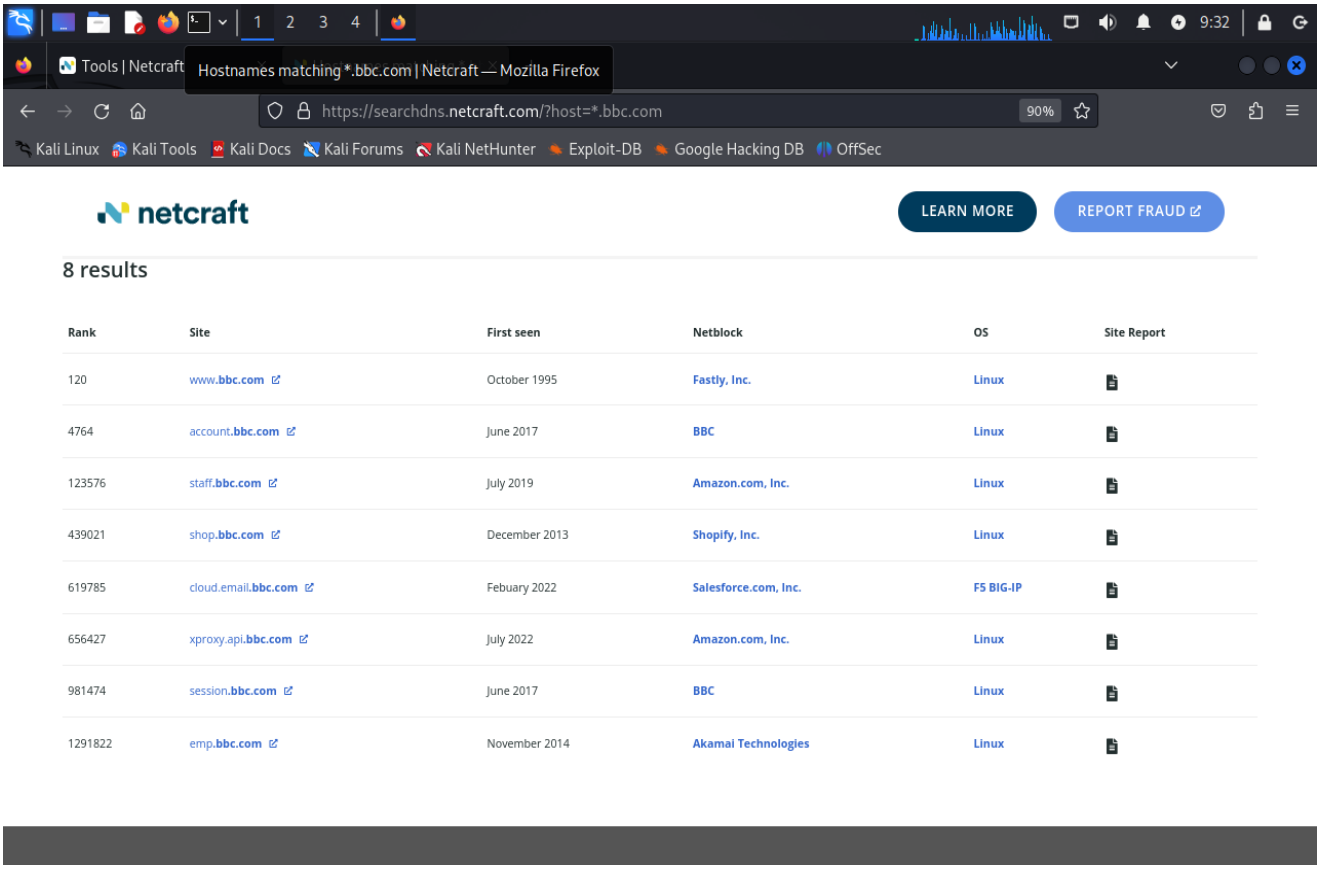
Step2 – in the website open the Internet Resaerch Tool option. And then click on the Search DNS option.



Step3 - In the search bar of the site enter the domain name bbc.com.



Step4 – Scroll down to bottom to get the all Subdoamins of bbc.com.



Rank	Site	First seen	Netblock	OS	Site Report
120	www.bbc.com	October 1995	Fastly, Inc.	Linux	
4764	account.bbc.com	June 2017	BBC	Linux	
123576	staff.bbc.com	July 2019	Amazon.com, Inc.	Linux	
439021	shop.bbc.com	December 2013	Shopify, Inc.	Linux	
619785	cloud.email.bbc.com	Febuary 2022	Salesforce.com, Inc.	F5 BIG-IP	
656427	xproxy.api.bbc.com	July 2022	Amazon.com, Inc.	Linux	
981474	session.bbc.com	June 2017	BBC	Linux	
1291822	emp.bbc.com	November 2014	Akamai Technologies	Linux	

Q 3 : Explain about way back Machine. And describe the process of retrieving sensitive data. And provide a Screen Shot of that how bbc.com appeared in 2010.

Process

Wayback Machine –

The Wayback Machine is a digital archive created by the Internet Archive, a nonprofit organization dedicated to preserving the web. It allows users to view and access archived versions of web pages across time. This tool is invaluable for seeing how websites have changed, retrieving lost information, and researching historical web content.

How the Wayback Machine Works

1. Crawling : The Internet Archive's automated systems regularly crawl the web to capture snapshots of web pages. These crawls are scheduled at various intervals, and the archive captures the content of pages as they appear at specific times.

2. Archiving : When a web page is crawled, its content (text, images, and sometimes scripts) is stored in a database. The archive retains the date and time of each snapshot, allowing users to view how a page looked at different points in history.

3. Accessing : Users can access archived web pages through the Wayback Machine's search interface. By entering a URL, users can browse the history of that page, choosing different dates to see how the content has evolved.

Retrieving Sensitive Data

It's important to clarify that the Wayback Machine is designed to archive public web content, and accessing sensitive or private data through it is both unethical and often illegal. Here's how sensitive data might be mishandled if not properly secured:

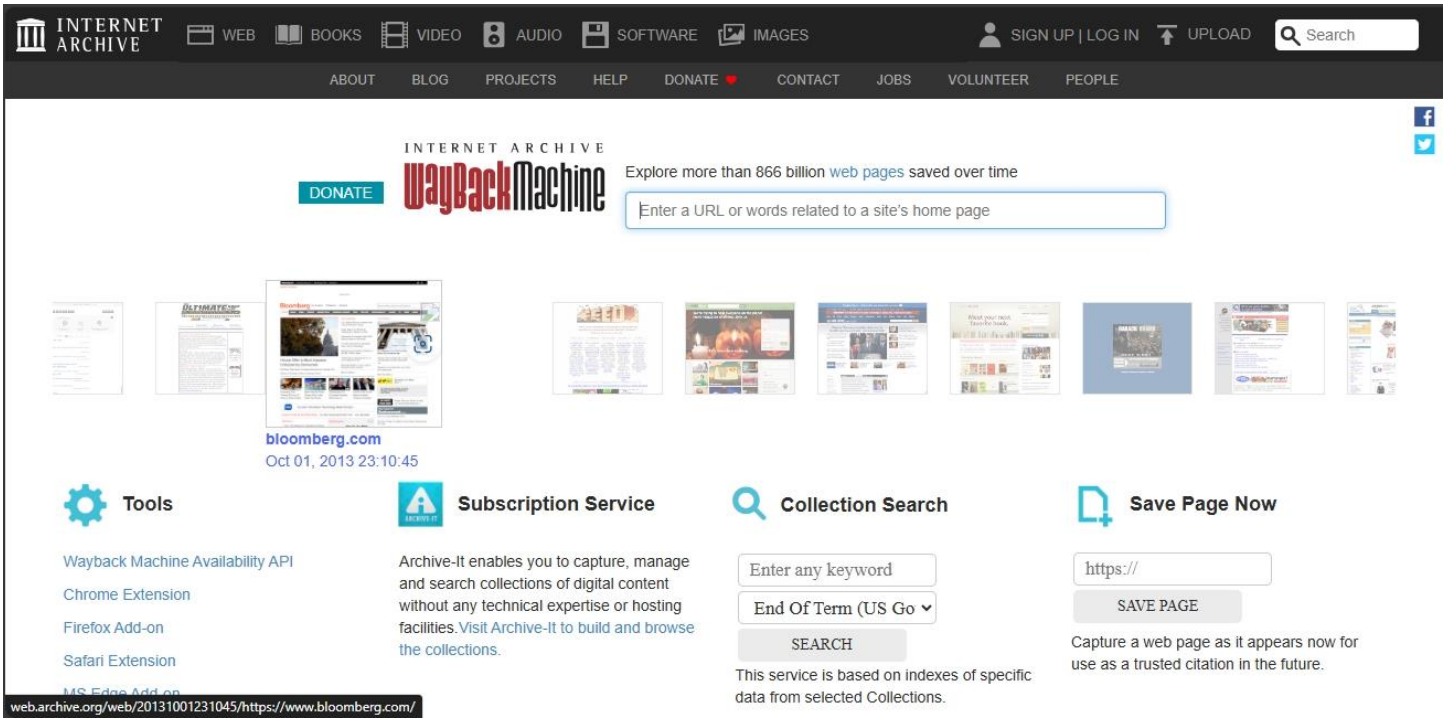
1. Unintentional Exposure : Websites might inadvertently expose sensitive information (e.g., personal data or private documents) if they were publicly accessible at the time of the crawl. However, this is typically not the intended purpose of the archive.

2. Ethical Considerations : It's crucial to respect privacy and ethical guidelines when dealing with sensitive information. The Wayback Machine should not be used to access or retrieve data that should remain private.

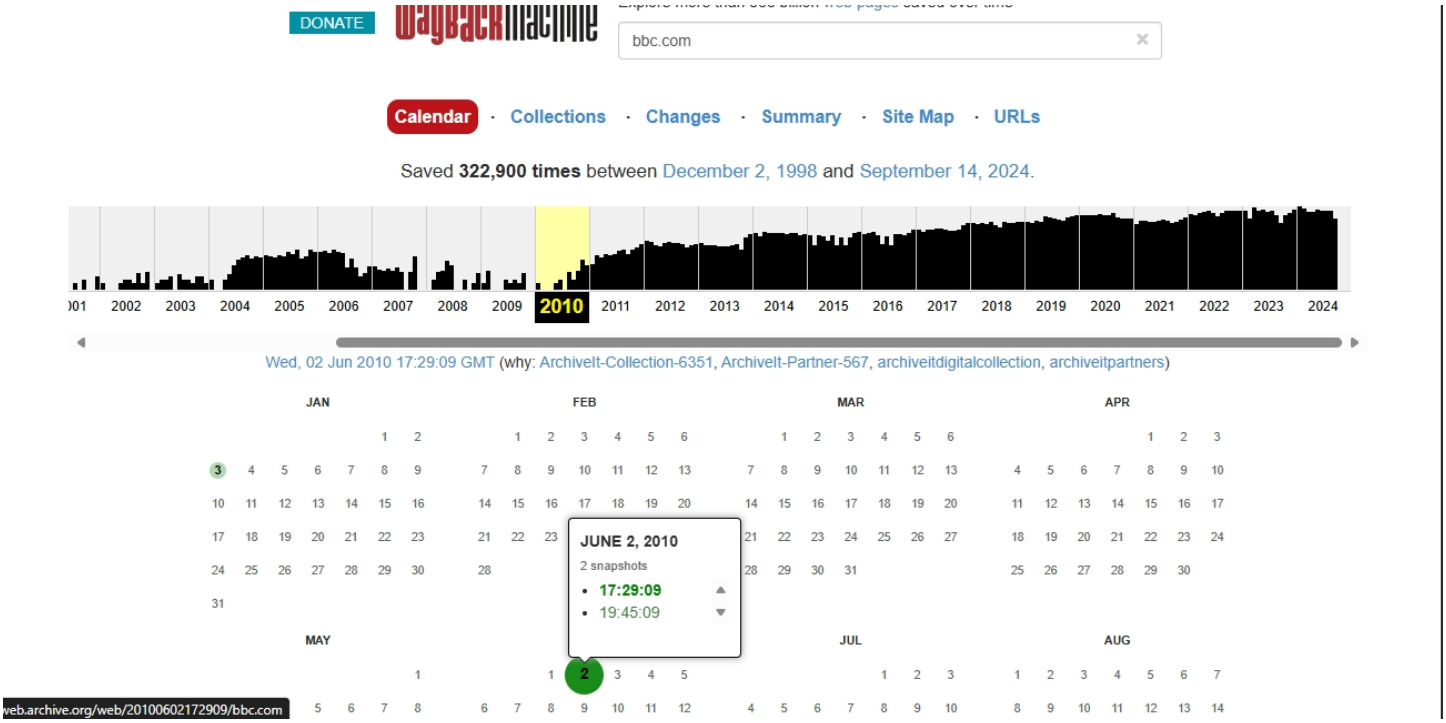
3. Security : For sensitive or private data, ensure that you are following all legal and ethical standards. If you are involved in web development or data management, make sure that private data is not exposed unintentionally in public archives.

In summary, while the Wayback Machine is a powerful tool for historical web research, it should be used responsibly and ethically. Sensitive data should be properly secured and not exposed to unauthorized access.

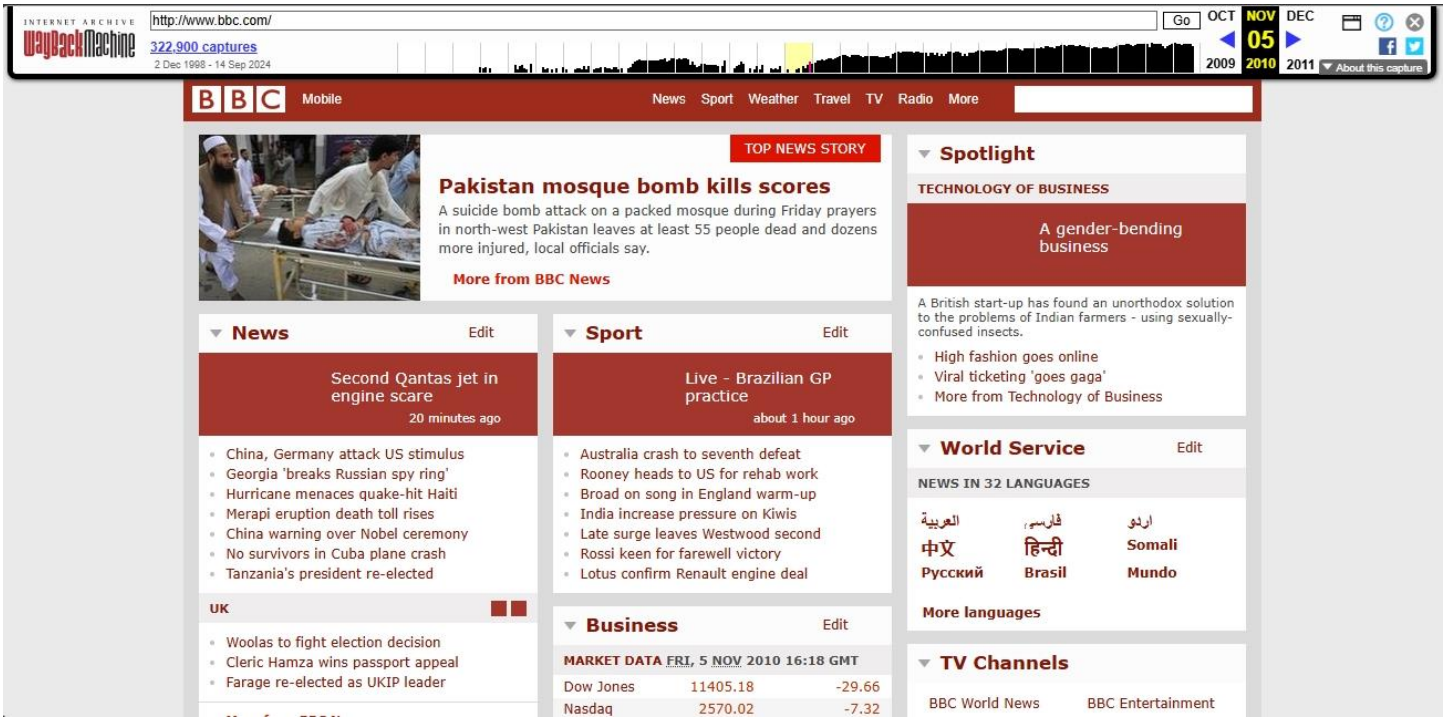
Step 1 – Open the web browser and type the address http://www.wayback.archive.org/



Step 2 – In the website search bar search for the domain bbc.com. A get a row containing Years serially. Then select 2010 year. It gives a calendar of dates. Then select any available date



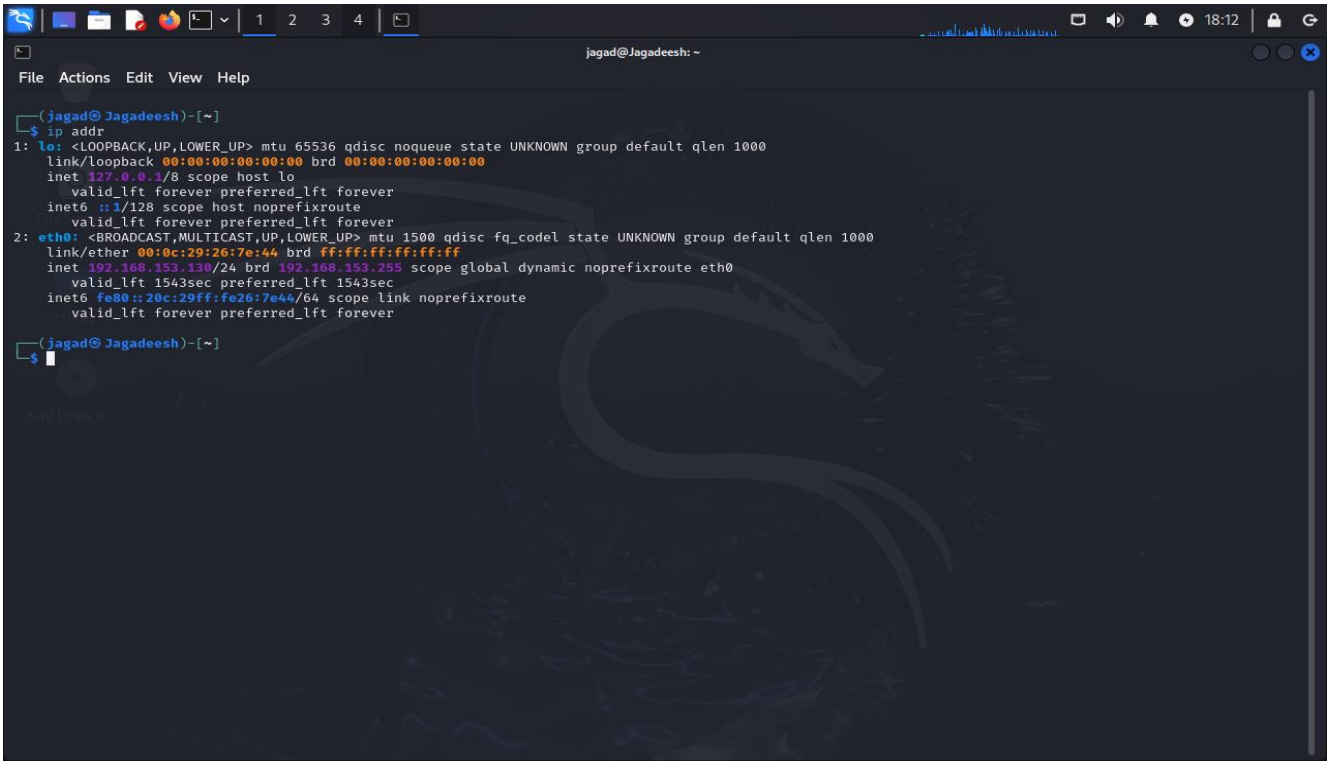
Step 3 – then finally we get a Web interface of bbc.com of the 2010 timeline



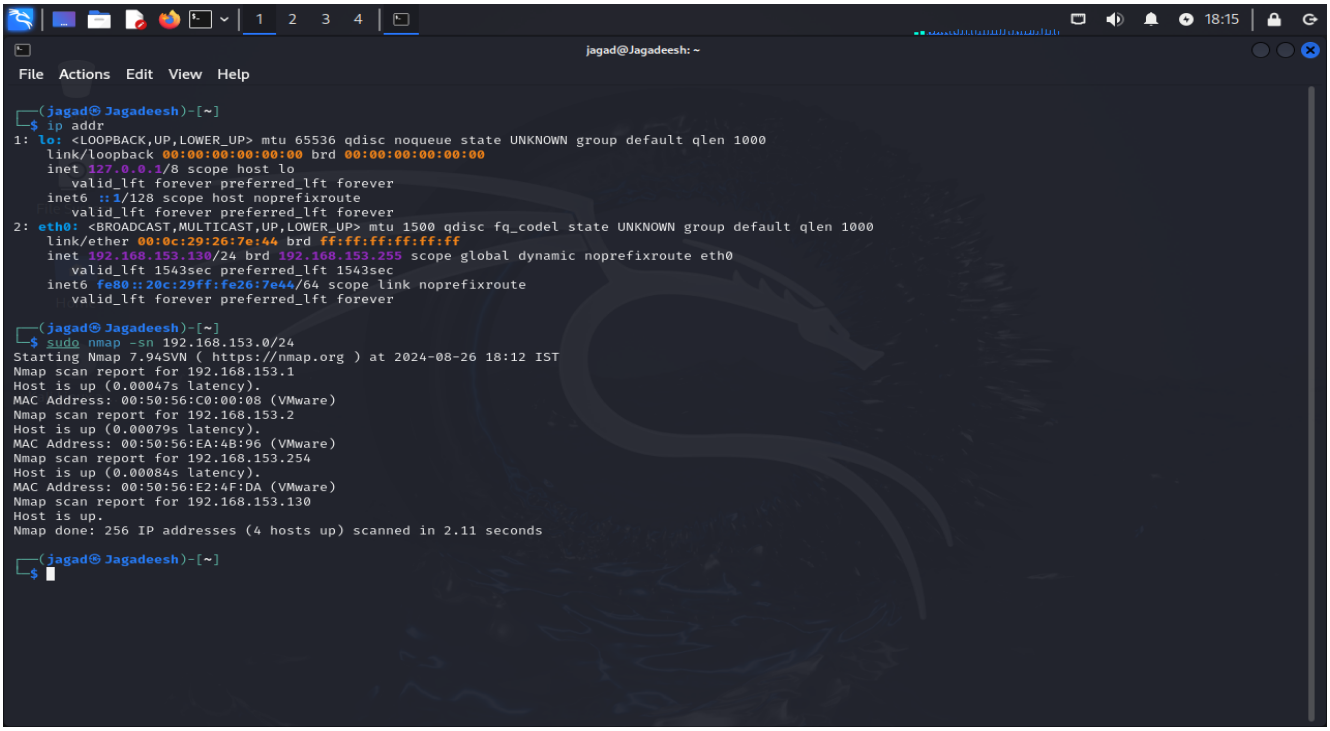
Q 5 – Utilize the NMAP (Network Mapper) tool to find the all connected devices after establishing a connection between the LAN via Wi-Fi.

Process

Step 1 – First we need to connect to a Network via Wi-Fi using their credentials, here our IP address is 192.168.153.130.



Step 2 – enter the command “nmap -sn 192.168.153.0/24”. Here replace the IP with your IP. And -sn means scan all Network.



Q 5 – Performing a privilege escalation on Metasploitable Machine.

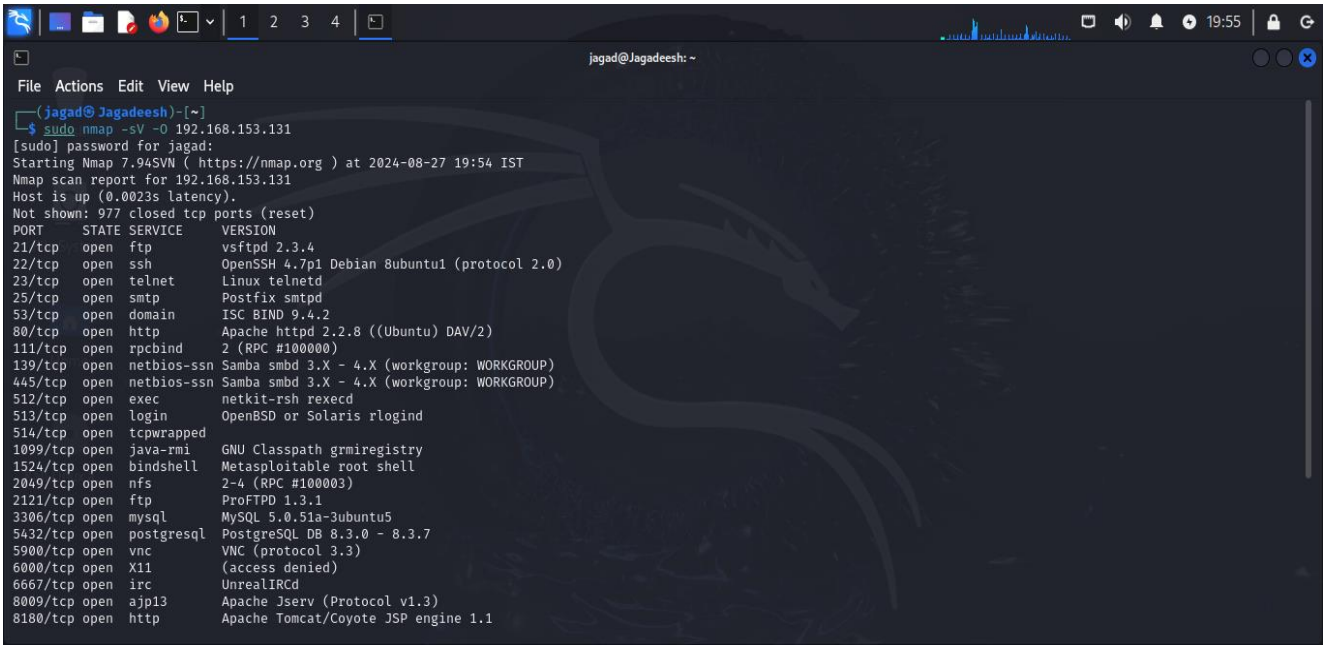
Process

Note :- to Perform Privilege escalation The Linux VM, and Metasploitable Machine are both required to be in the same Network

Step 1 – Open VM and start Metasploitable Machine, Login into it using the given credentials. and find the IP Address using the command “ip addr”.

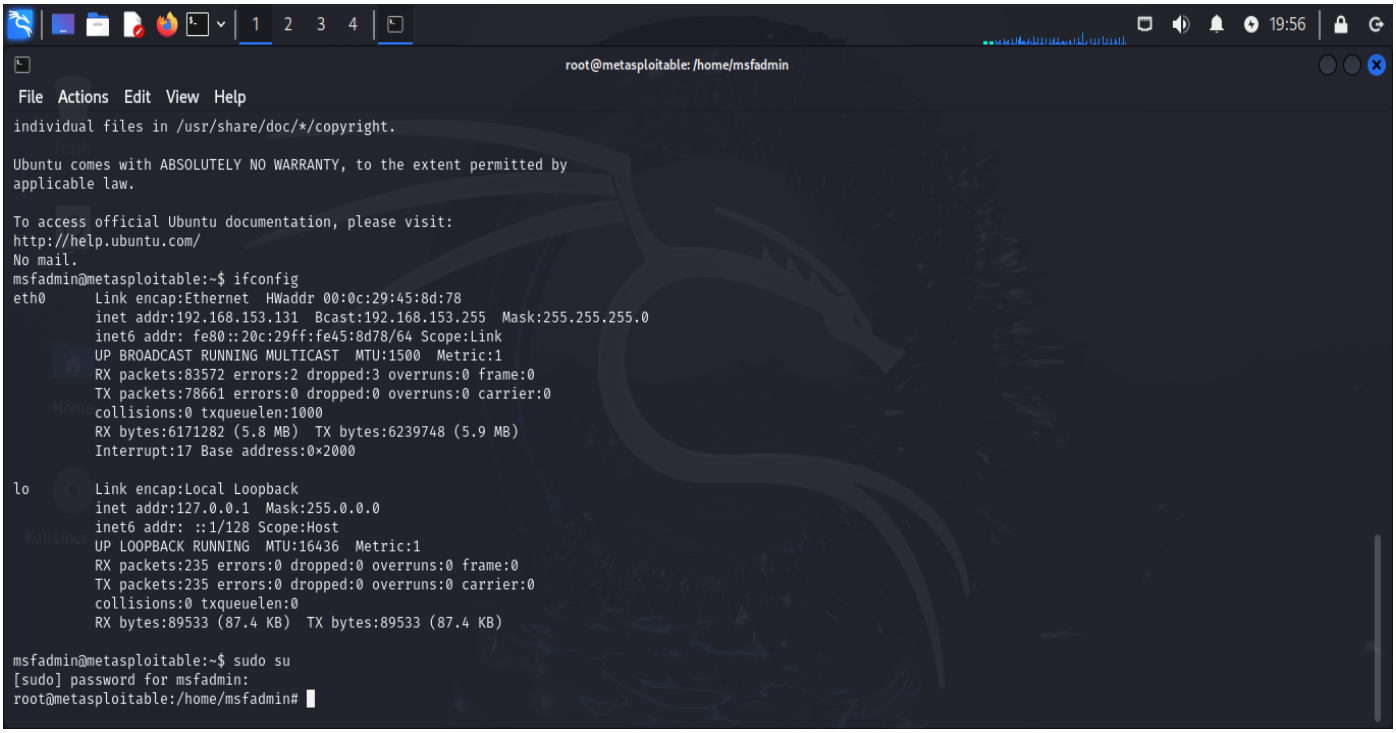
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:45:8d:78
          inet addr:192.168.153.131  Bcast:192.168.153.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe45:8d78/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:82126 errors:2 dropped:3 overruns:0 frame:0
          TX packets:77337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6076845 (5.7 MB)  TX bytes:6113844 (5.8 MB)
          Interrupt:17 Base address:0x2000

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:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85445 (83.4 KB)  TX bytes:85445 (83.4 KB)

msfadmin@metasploitable:~$ _
```

Step2 – Then open kali VM, and perform a Network scan using NMAP tool to find the detailed network report for Metasploitable Machine IP address.



Step3 – Here we have so many ports open. Now we perform a Privilege escalation method on using telnet port number 23 using the command “telnet 192.168.153.131 23”

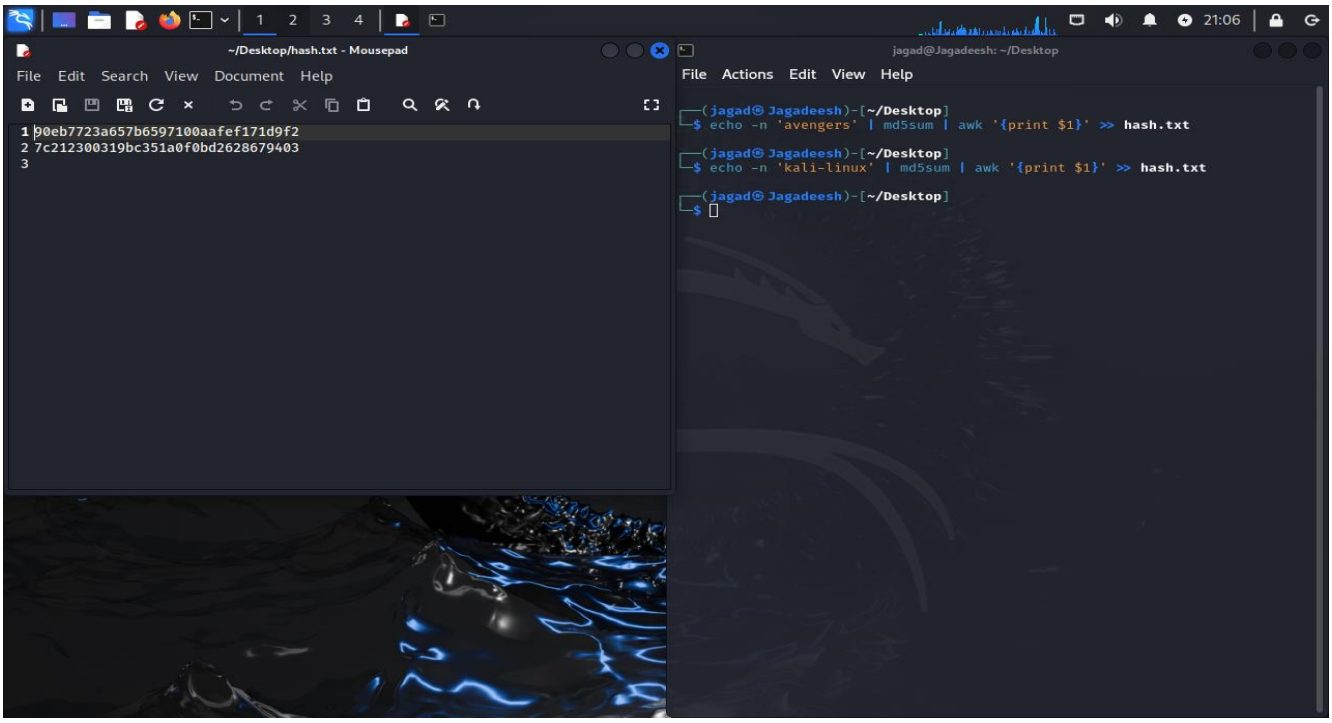
Step 4 – Then we can easily escalated the Metasploitable Machine using telnet port 23.The login into it using the credsentials. So, we can use it as a Root user also



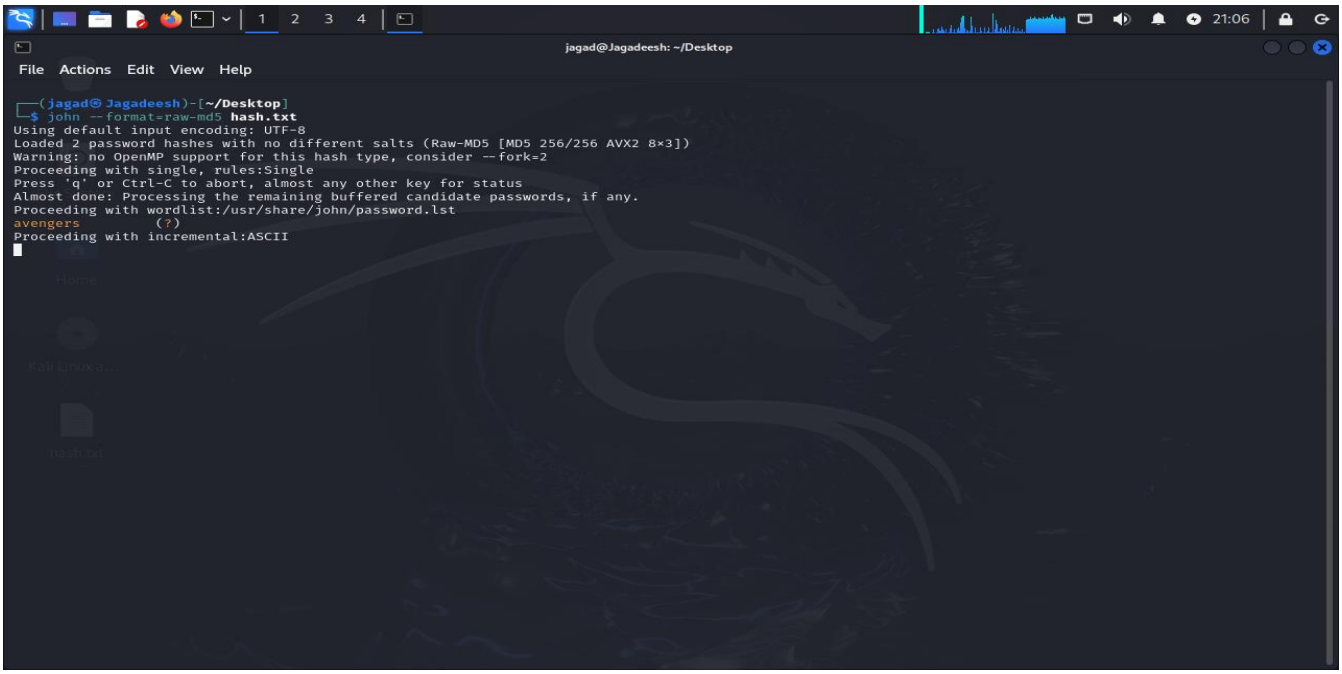
Q 6 : Employing the Password Cracking tool John the Ripper to Illustrate how the password will be compromise.

Process

Step 1 – To use John the Ripper tool first we need some Password Hashes to crack. To create hashes use the command “echo -n “avengers” | md5sum | awk ‘print $1’ >> hash.txt” .It creates the Hash for the word ‘avengers’ and place it into a text file names ‘hash.txt’ then saves it.



Step 2 – To crack the password John uses the words list named ‘Rockyou’ in the library. Use the command “john -format-raw-md5 hash.txt” to get the cracked password



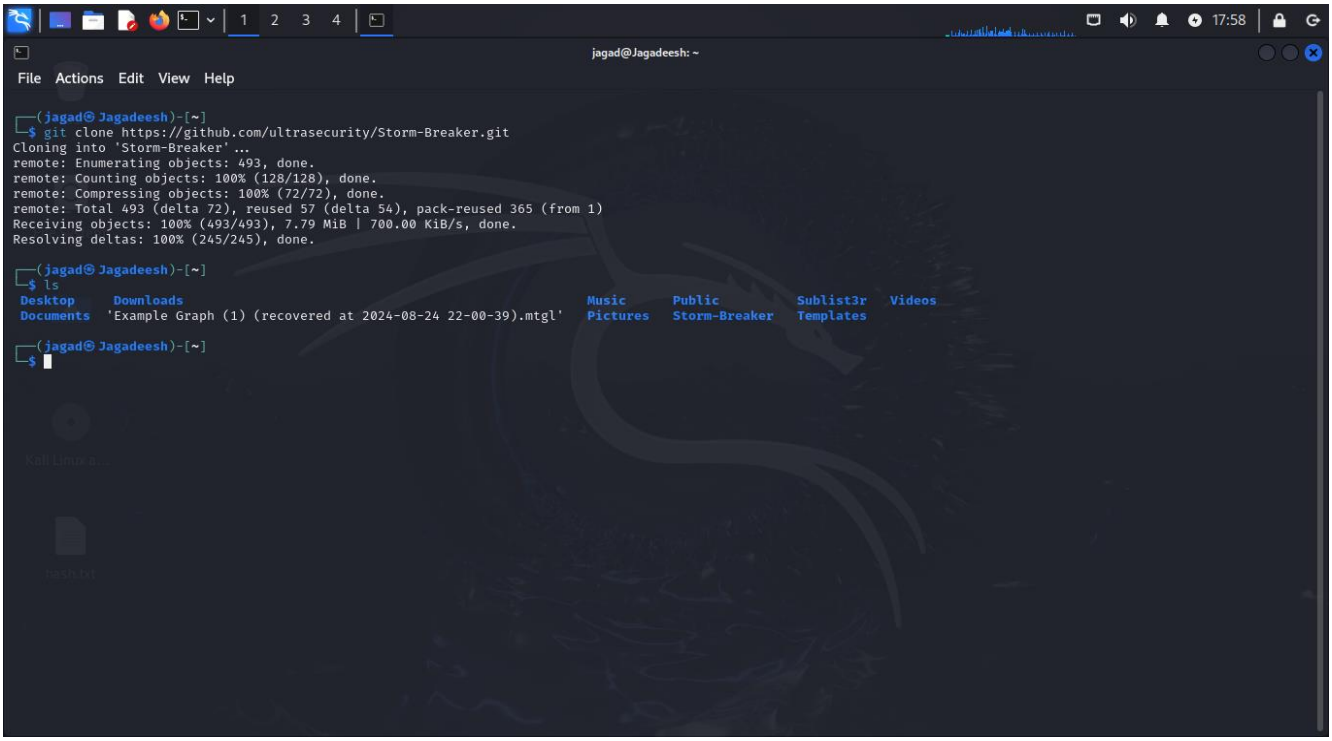
Q 7 : Conduct a stimulated phishing attack in a Wide Area Network environment using suitable Tool to demonstrate potential risk specially focuses on the accessing of Web Camera's.

Process

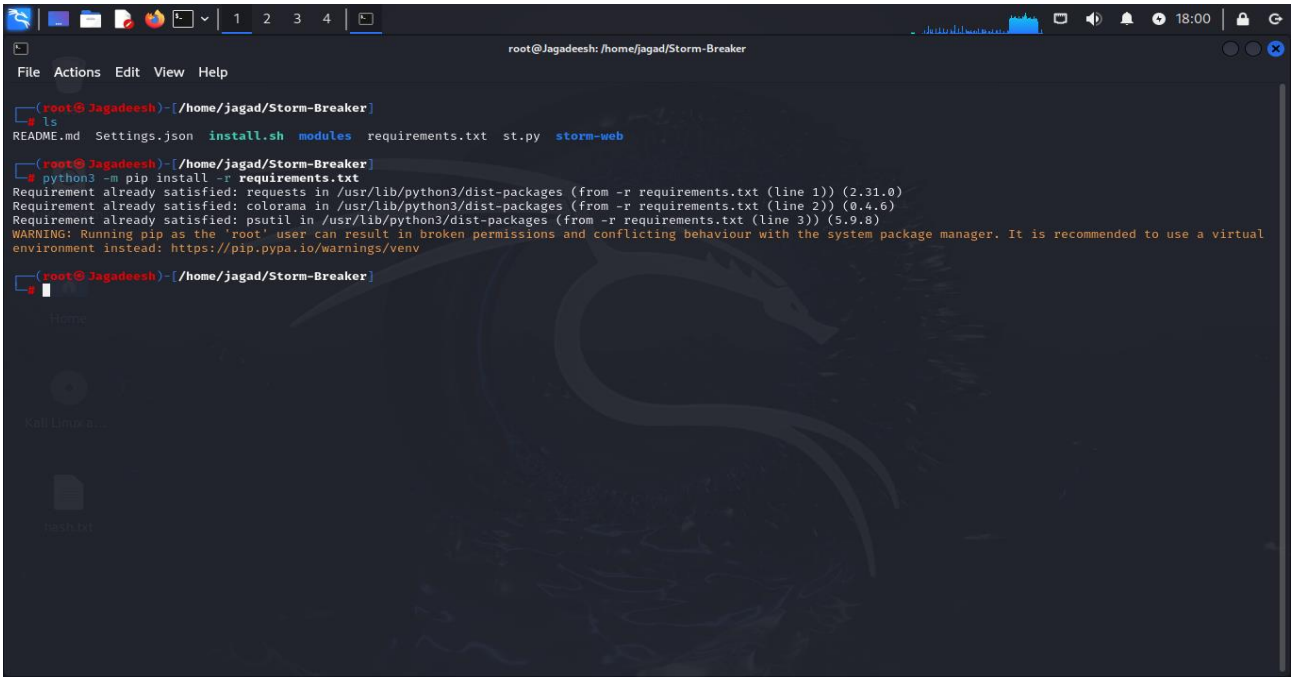
For this task I'm going to use a Tool Named Storm-Breaker.

Step1 – Install the Tool Storm-Breaker by using the command

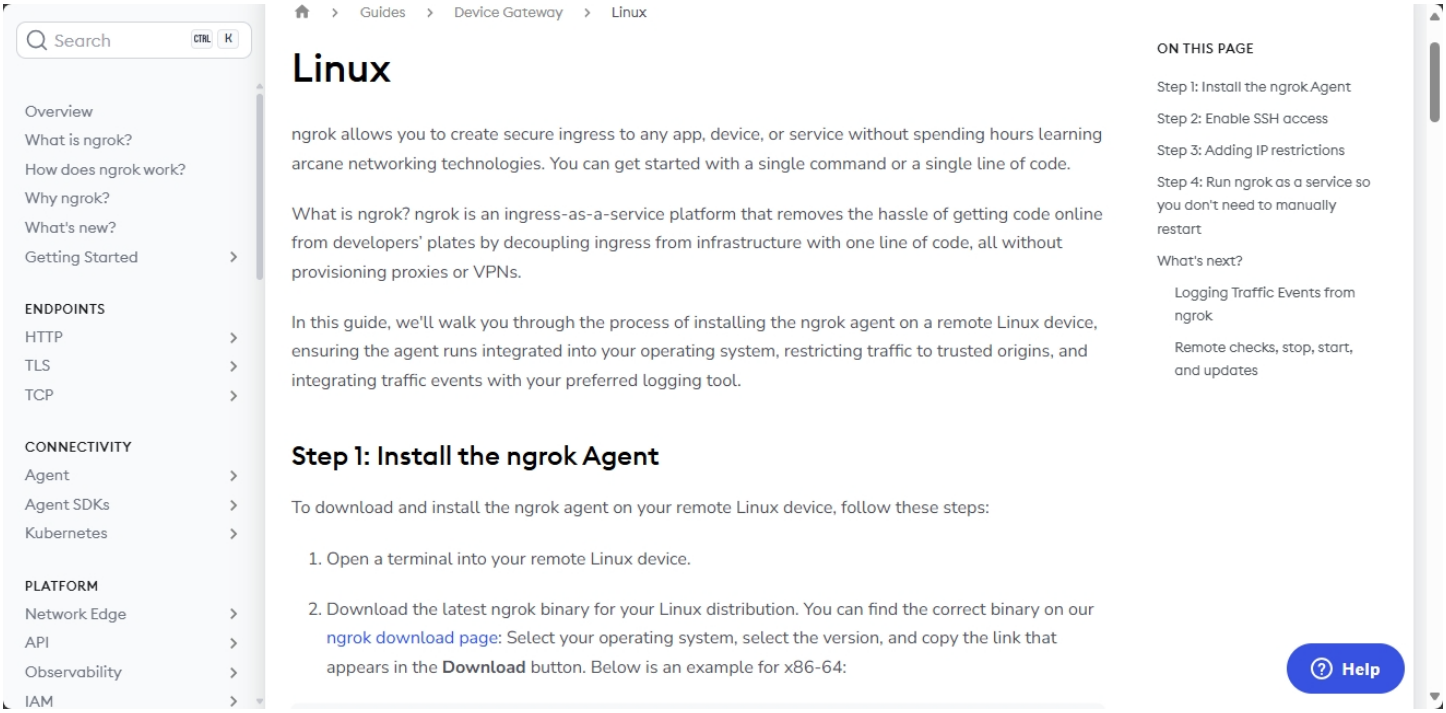
"git clone https://github.com/ultrasecurity/Storm-Breaker.git"



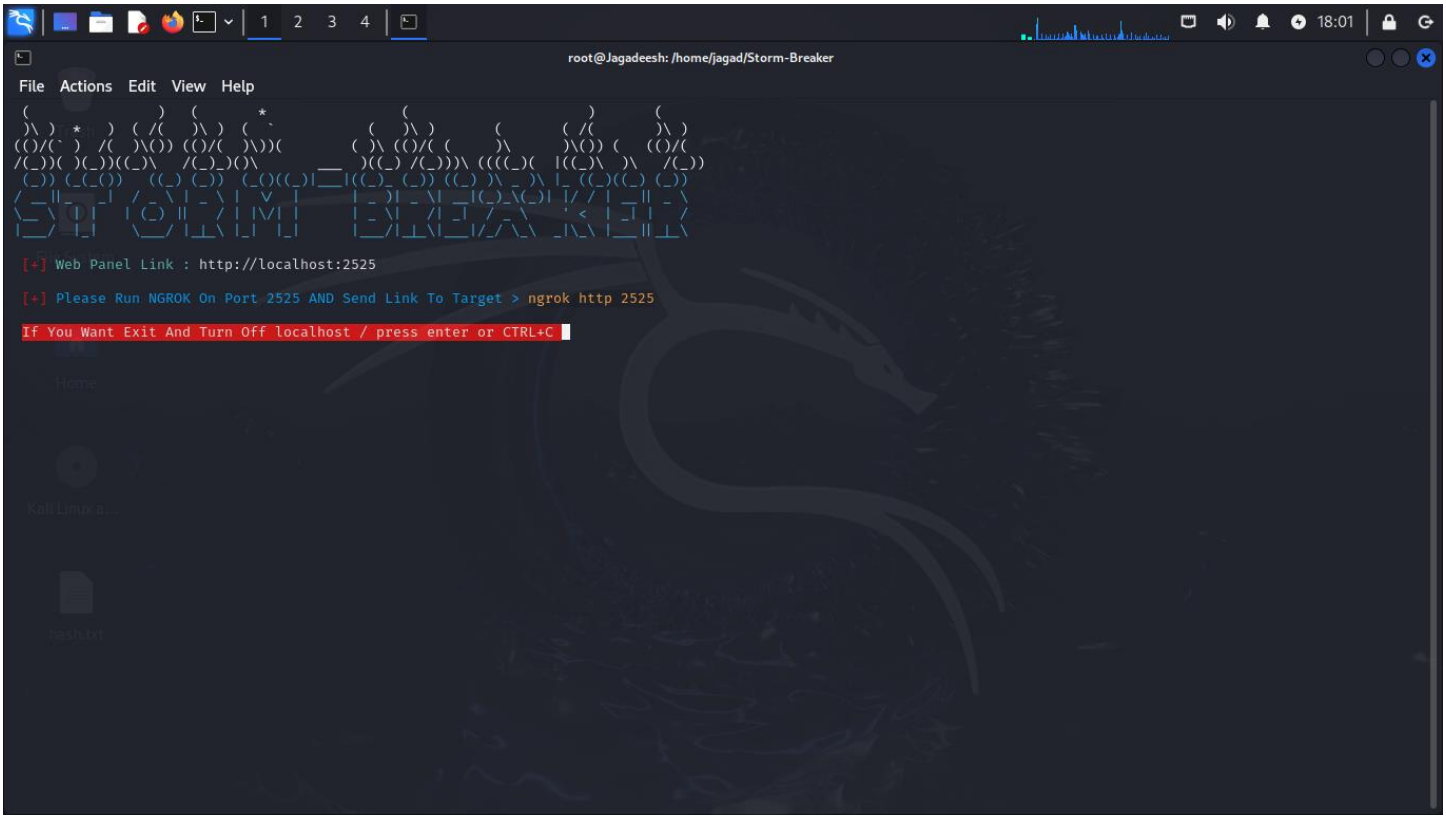
Step2 – After that change the directory to Storm-Breaker and install all Python Dependencies using the command “python3 -m pip install requirements.txt”



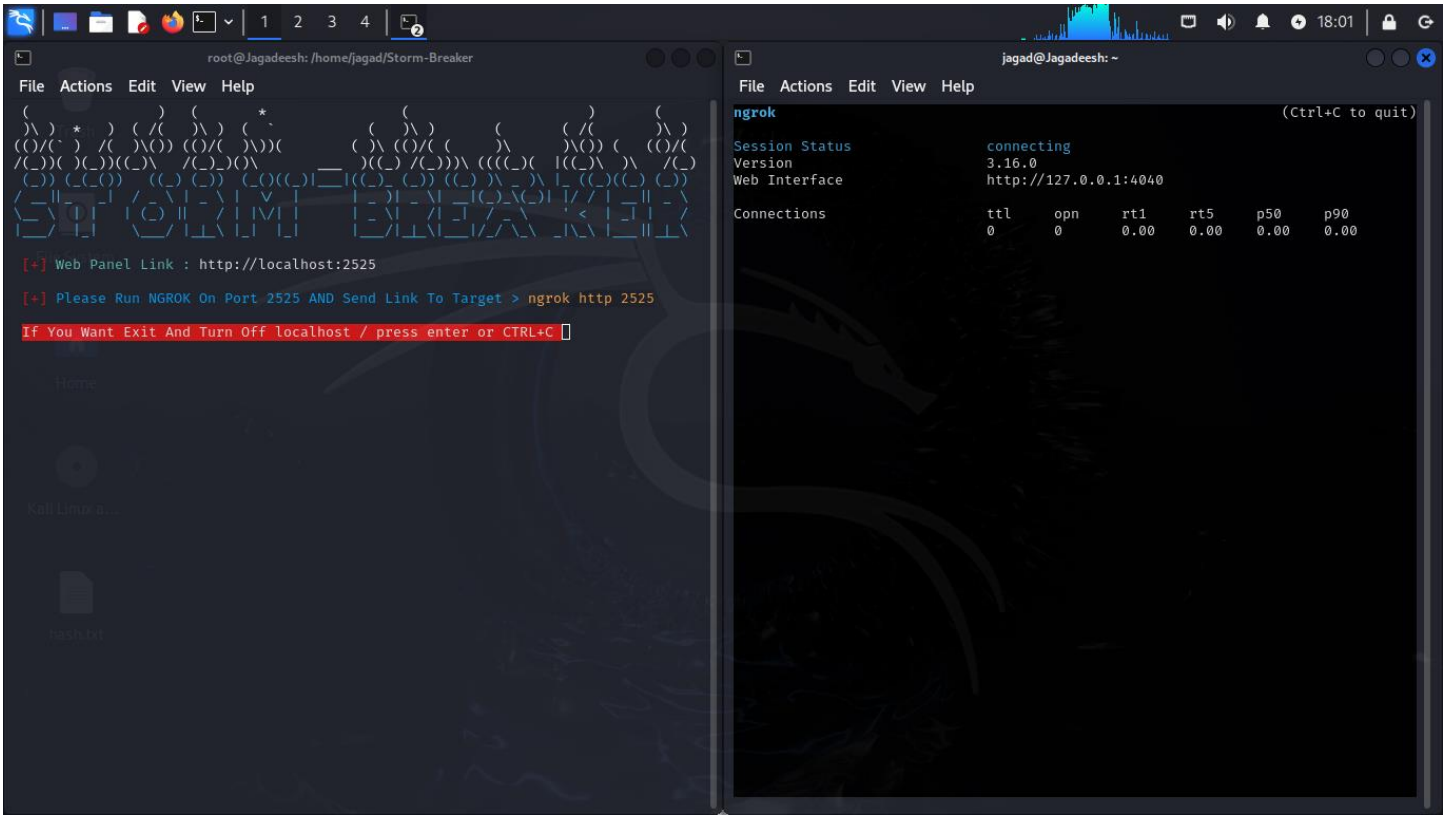
Step3 – Open a new tab in a web browser and search for www.ngrok.com, and signup and follow the steps to install ngrok on Lilnux.



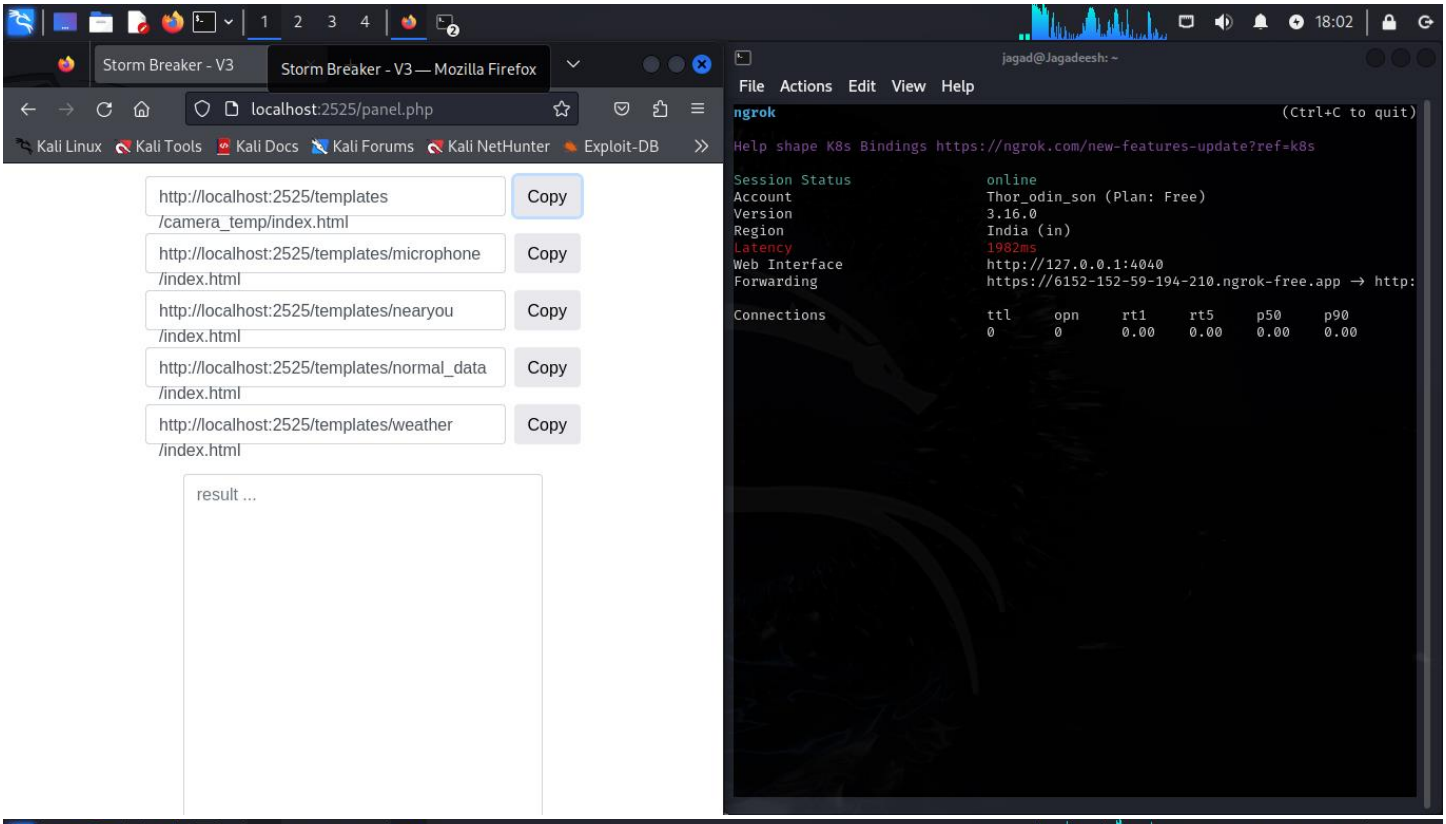
Step4 – After that open the Terminal and execute the Storm-Breaker script using the command “python3 st.py”

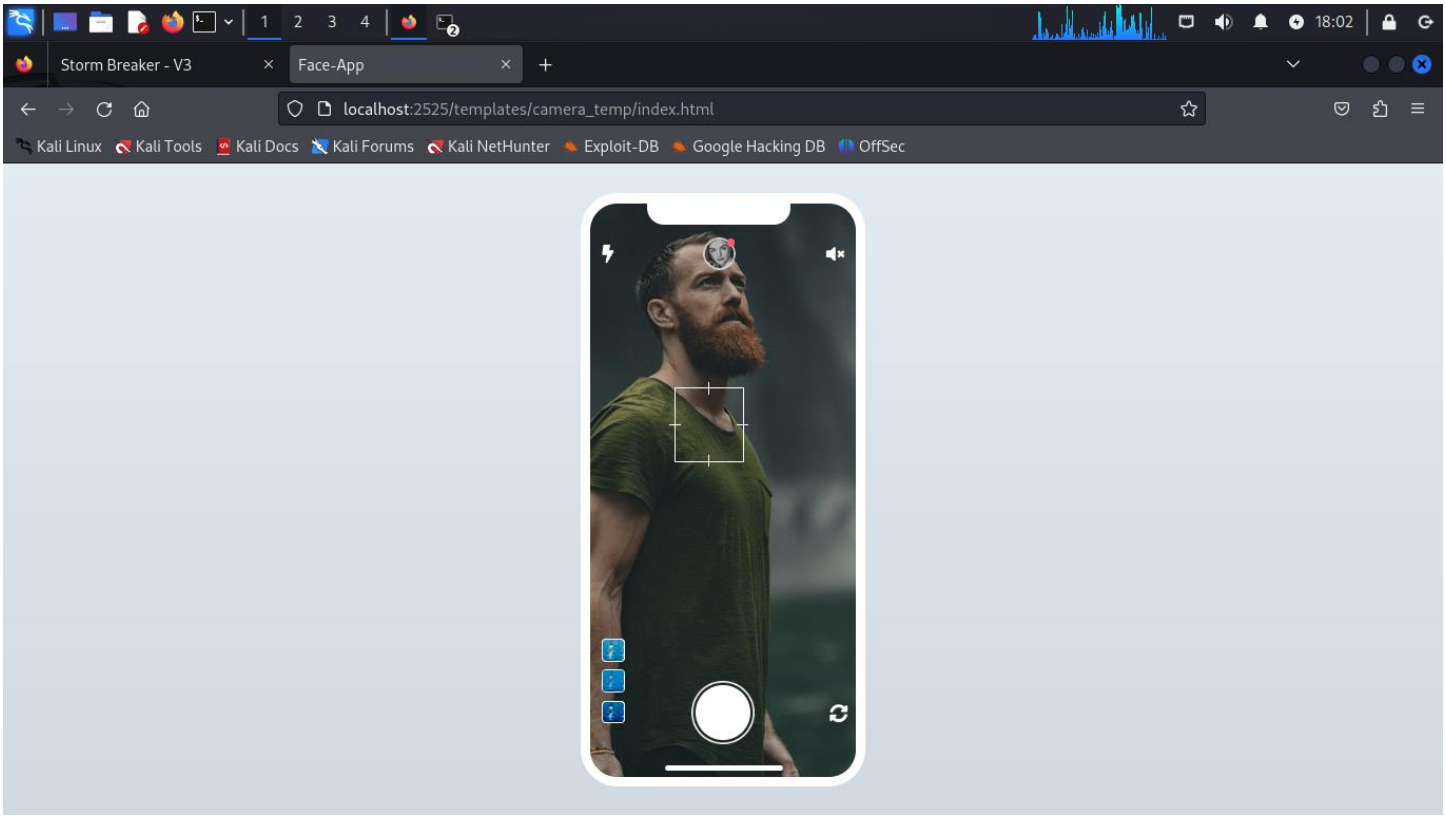


Step5 – Then we get a local host link copy that and paste it in your web browser, and it asks you to login use “admin” as both user name and password. open a new terminal and type the command “ngrok http 2525” then press enter.



Step6 – then the local host browser shows 5 another links, copy the first link then paste it to the target system. Then That Web can be accessed.





Q 8 : Develop an incident response plan to address the situation discussed before. The plan should outline the steps to take in case of this security incident.

Process

Creating an incident response plan for a suspected data breach involves several critical steps to manage the situation effectively. Here's a structured approach tailored to your scenario:

Incident Response Plan for Suspected Data Breach

1. Identification

1. Confirm the Breach:

- Validate the unusual activity by examining network logs, access records, and alerts.

- Determine the extent of unauthorized access and identify the compromised systems or data.

2. Assess the Impact:

- Identify which customer data (e.g., personal information, payment details) has been accessed or exfiltrated.

- Evaluate the potential impact on customers and the business.

2. Containment

1. Short-Term Containment:

- Immediately isolate the affected systems to prevent further unauthorized access.

- Change all relevant passwords and disable any compromised accounts.

2. Long-Term Containment:

- Review and update firewall rules and network segmentation to prevent further access.

- Implement additional monitoring to detect any further malicious activity.

3. Eradication

1. Identify and Remove Threats:

- Analyze the attack vector used by the unauthorized user and remove any malware or backdoors.

- Patch any vulnerabilities that were exploited to gain access.

2. Strengthen Security Measures:

- Update security configurations, apply software patches, and review access controls.

- Conduct a thorough security audit to ensure all weaknesses are addressed.

4. Recovery

1. Restore Systems:

- Restore affected systems from clean backups and verify their integrity before bringing them back online.

- Ensure that no remnants of the attack remain.

2. Monitor Systems:

- Continuously monitor the systems for any signs of recurring issues or unauthorized activity.

- Keep a close watch on network traffic and access logs for anomalies.

5. Communication

1. Internal Communication:

- Inform key stakeholders, including management and relevant departments, about the breach and response actions.

- Keep communication channels open for updates and coordination.

2. External Communication:

- Notify affected customers about the breach, providing details on what information was compromised and how they can protect themselves.

- Comply with legal and regulatory requirements for breach notifications, including reporting to authorities if necessary.

3. Media and Public Relations:

- Prepare a statement for the media, if applicable, to control the narrative and maintain public trust.

- Ensure consistent messaging across all communication channels.

6. Post-Incident Review

1. Conduct a Forensic Analysis:

- Perform a detailed forensic investigation to understand the breach's origin, scope, and methods.

- Document findings and lessons learned.

2. Review and Update Policies:

- Evaluate the effectiveness of the incident response and update the incident response plan based on findings.

- Revise security policies, procedures, and training programs to prevent future incidents.

3. Training and Awareness:

- Conduct refresher training for employees on security best practices and incident reporting.

- Enhance awareness programs to address new threats and reinforce security protocols.

7. Documentation

1. Incident Report:

- Compile a comprehensive report detailing the incident, response actions, and outcomes.

- Include timelines, decisions made, and any evidence collected during the response.

2. Action Plan:

- Develop an action plan for ongoing improvements to security infrastructure and incident response processes.

8. Compliance and Legal Considerations

1. Regulatory Compliance:

- Ensure all actions and notifications comply with relevant data protection regulations (e.g., GDPR, CCPA).

2. Legal Consultation:

- Consult with legal counsel to address any potential legal implications and liabilities.

By following these steps, you can effectively manage the response to a suspected data breach and minimize its impact on the company and its customers.

Q 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.

Process

In the context of wireless networking, WEP, WPA, WPA2, and WPA3 are security protocols designed to safeguard wireless networks by encrypting data sent over them. Each of these protocols represents an evolutionary step in improving wireless security standards, with significant advancements in encryption strength, vulnerability mitigation, and user-friendliness. Below is an in-depth explanation of each protocol and a recommendation for the most secure option.

1. WEP (Wired Equivalent Privacy)

- Introduction : WEP was introduced in 1997 as part of the original 802.11 wireless standard. Its aim was to provide a wireless network with security comparable to a wired LAN.

- Encryption : WEP uses the RC4 stream cipher for encryption, with either a 64-bit or 128-bit encryption key. This encryption standard was once considered sufficient but is now regarded as highly insecure.

- Vulnerabilities : WEP has serious flaws, primarily due to the weak initialization vector (IV) used in encryption. The IV is small and can be reused frequently, making it vulnerable to IV collision attacks. Tools such as Aircrack-ng can crack WEP keys in minutes, even by a novice attacker.

- Status : WEP was officially deprecated in 2004 due to its weaknesses, and its use is highly discouraged in modern networks.

2. WPA (Wi-Fi Protected Access)

- Introduction : In response to WEP's vulnerabilities, WPA was introduced in 2003 as a temporary security improvement, pending the development of a more secure protocol.

- Encryption : WPA uses TKIP (Temporal Key Integrity Protocol) , which still relies on the RC4 stream cipher but introduces enhancements to avoid WEP's key reuse issue. TKIP dynamically generates a new key for every data packet, making replay attacks more difficult.

- Vulnerabilities : While WPA improved upon WEP, TKIP itself was a transitional solution. WPA has been found vulnerable to certain attacks, such as TKIP replay attacks and key reinstallation attacks (KRACK) .

- Status : WPA is also considered outdated, but it is still more secure than WEP. However, WPA was quickly replaced by WPA2 due to its shortcomings.

3. WPA2 (Wi-Fi Protected Access 2)

- Introduction : Released in 2004, WPA2 became the mandatory security standard for all Wi-Fi devices certified by the Wi-Fi Alliance. It is based on the 802.11i standard.

- Encryption : WPA2 uses a much stronger encryption protocol, the Advanced Encryption Standard (AES) , which is virtually uncrackable through brute force methods. WPA2 can operate in two modes:

  - WPA2-Personal (PSK) : Uses a pre-shared key, typically for home networks.

  - WPA2-Enterprise : Uses a centralized authentication server (RADIUS) for larger corporate networks.

- Vulnerabilities : While WPA2 is significantly more secure than WPA, it is not without vulnerabilities. KRACK attacks exposed vulnerabilities in the WPA2 protocol in 2017, showing that attackers could potentially decrypt data or inject malware by exploiting flaws in key management.

- Status : Despite the KRACK vulnerability (which can be patched with updates), WPA2 remains widely used and offers a high level of security when configured correctly (e.g., with a strong password and the latest firmware).

4. WPA3 (Wi-Fi Protected Access 3)

- Introduction : WPA3, launched in 2018, is the latest security protocol designed to address the limitations of WPA2 and provide enhanced protection, especially for newer devices and high-security environments.

- Encryption : WPA3 improves upon WPA2 in several ways:

  - SAE (Simultaneous Authentication of Equals) replaces the PSK method for key exchange in WPA3-Personal. SAE uses a key exchange protocol that is resistant to offline dictionary attacks, making it far more difficult for attackers to guess the Wi-Fi password.

- Forward Secrecy : Even if an attacker were to obtain the encryption key for one session, they cannot use it to decrypt previous communications, as each session is encrypted with a unique key.

- Vulnerabilities : WPA3 is not without criticism. Early vulnerabilities, such as Dragonblood attacks , were identified, but these have since been addressed with firmware patches.

- Additional Features :

- 192-bit security in WPA3-Enterprise mode for enhanced encryption strength.

- Individualized Data Encryption (IDE) for public networks, ensuring that even on open Wi-Fi networks, data between the device and the router is encrypted.

- Status : WPA3 is the most secure protocol available today, offering significant improvements in both personal and enterprise environments. It is now required for Wi-Fi 6 certification.

Comparison Summary

Protocol	Encryption Method	Vulnerabilities	Status
WEP	RC4 (64-bit/128-bit)	Weak IVs, easily cracked	Deprecated
WPA	TKIP with RC4	TKIP replay attacks, KRACK	Outdated
WPA2	AES	KRACK (patched)	Widely used
WPA3	SAE, AES	Early vulnerabilities (patched)	Most secure

Recommendation: WPA3

WPA3 is the recommended and most secure wireless encryption protocol. The reasons are:

1. Resistance to Dictionary Attacks : WPA3's use of SAE ensures that offline dictionary attacks (where attackers try to guess the password) are nearly impossible, as each login attempt requires interaction with the network.

2. Improved Encryption : WPA3-Enterprise mode supports 192-bit encryption, making it suitable for even highly sensitive environments. Forward secrecy further enhances the security by ensuring past data cannot be decrypted even if the current key is compromised.

3. Public Wi-Fi Security : With Individualized Data Encryption (IDE) , WPA3 encrypts data on open networks, providing enhanced protection in places like cafes and airports, where open networks are common.

4. Continuous Updates and Patches : Although WPA3 had early vulnerabilities (e.g., Dragonblood), these have been addressed through firmware updates, and it remains the best option for protecting modern wireless networks.

In summary , while WPA2 is still highly secure and widely used, WPA3 is the ideal choice for new devices and networks, offering the most advanced encryption and protection against modern attack vectors.

Q 10 : Provide a insight into the methods for accessing a CCTV camera without authorization. Kindly describe the process. And Elucidate the challenges and difficulties you encounters in attempting to gain unauthorized access.

Process

Note : Accessing the CCTV cameras without permission is Illegal.

Step1 : Download and Install tool named “arp-scan” to scan all the devices in a Network. Then type the command “sudo arp-scan --interface wlan0 -l”. change the interface by where you connect to the Network.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --interface wlan0 -l
[sudo] password for kali:
Interface: wlan0, type: EN10MB, MAC: 00:11:7f:20:f4:87, IPv4: 10.0.0.9
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.0.1                                NETGEAR
10.0.0.3                                Apple, Inc.
10.0.0.4                                Smart Innovation LLC
10.0.0.12                               Q-SEE Zhejiang Dahua Technology Co., Ltd.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.042 seconds (125.37 hosts/sec). 4 respond
ed
```

Here the 3rd one Q-SEE is the target CCTV Camera.

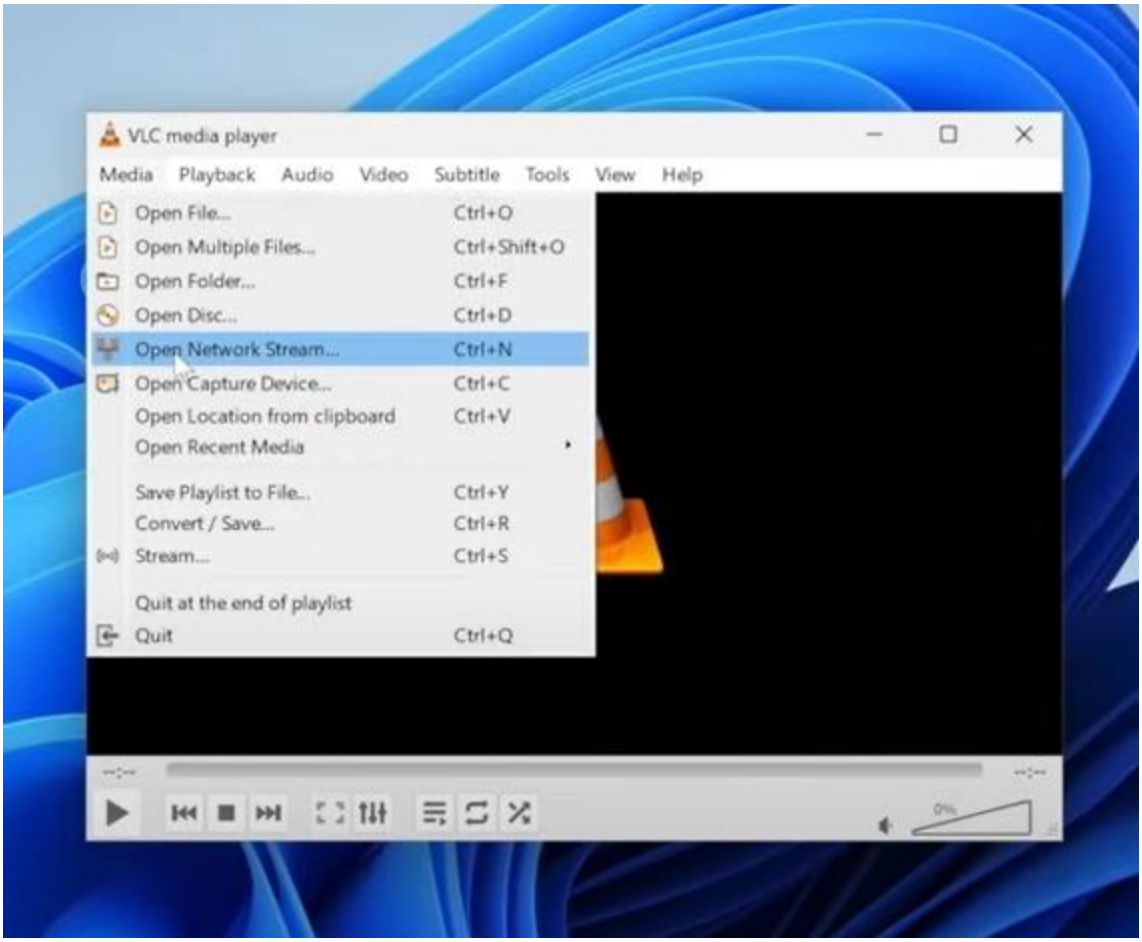
Step2 : start an NMAP scan on the target IP using the command “nmap 10.0.0.12”

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.0.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 23:10 EDT
Nmap scan report for 10.0.0.12
Host is up (0.012s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
85/tcp    open  mit-ml-dev
554/tcp   open  rtsp
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

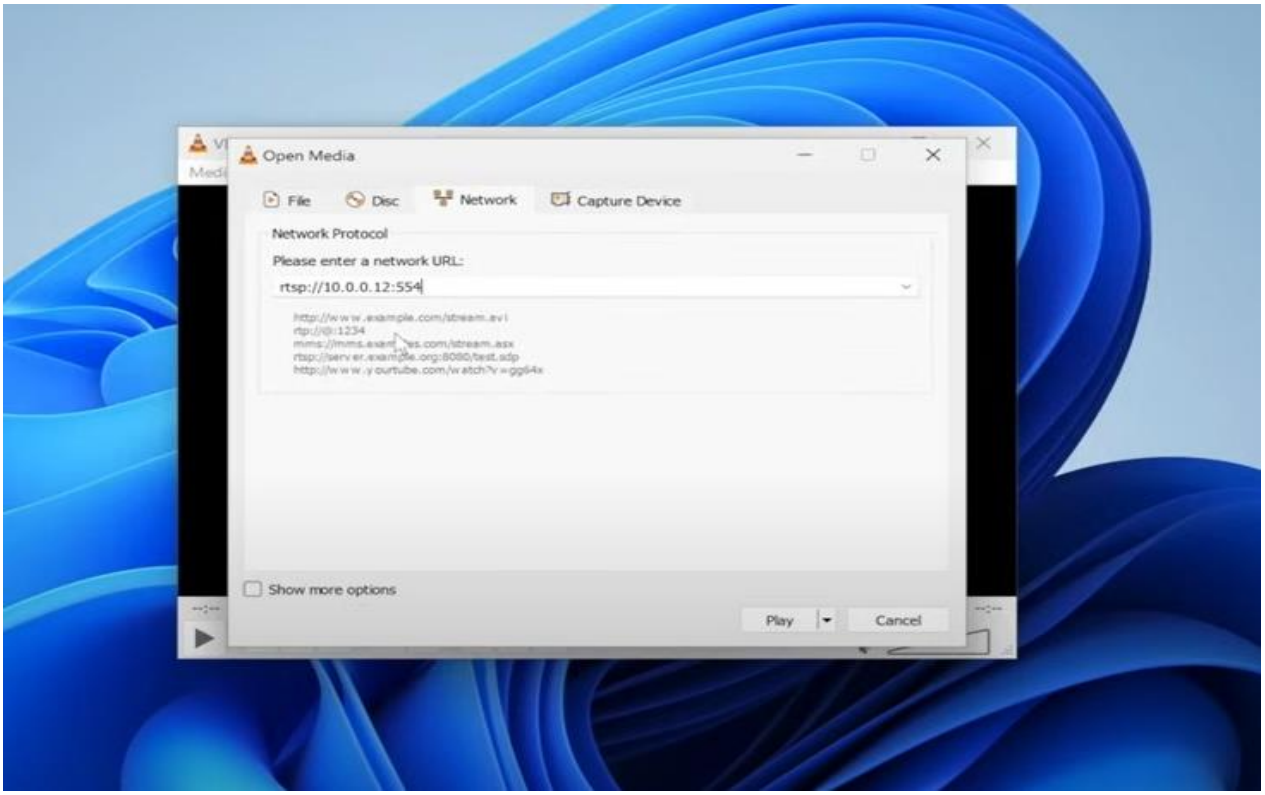
Step3 : Now we are going to use port 554 called as RTSP (Real Time Streaming Protocol).

Download VLC media player on your device using the command “sudo apt install vlc”.

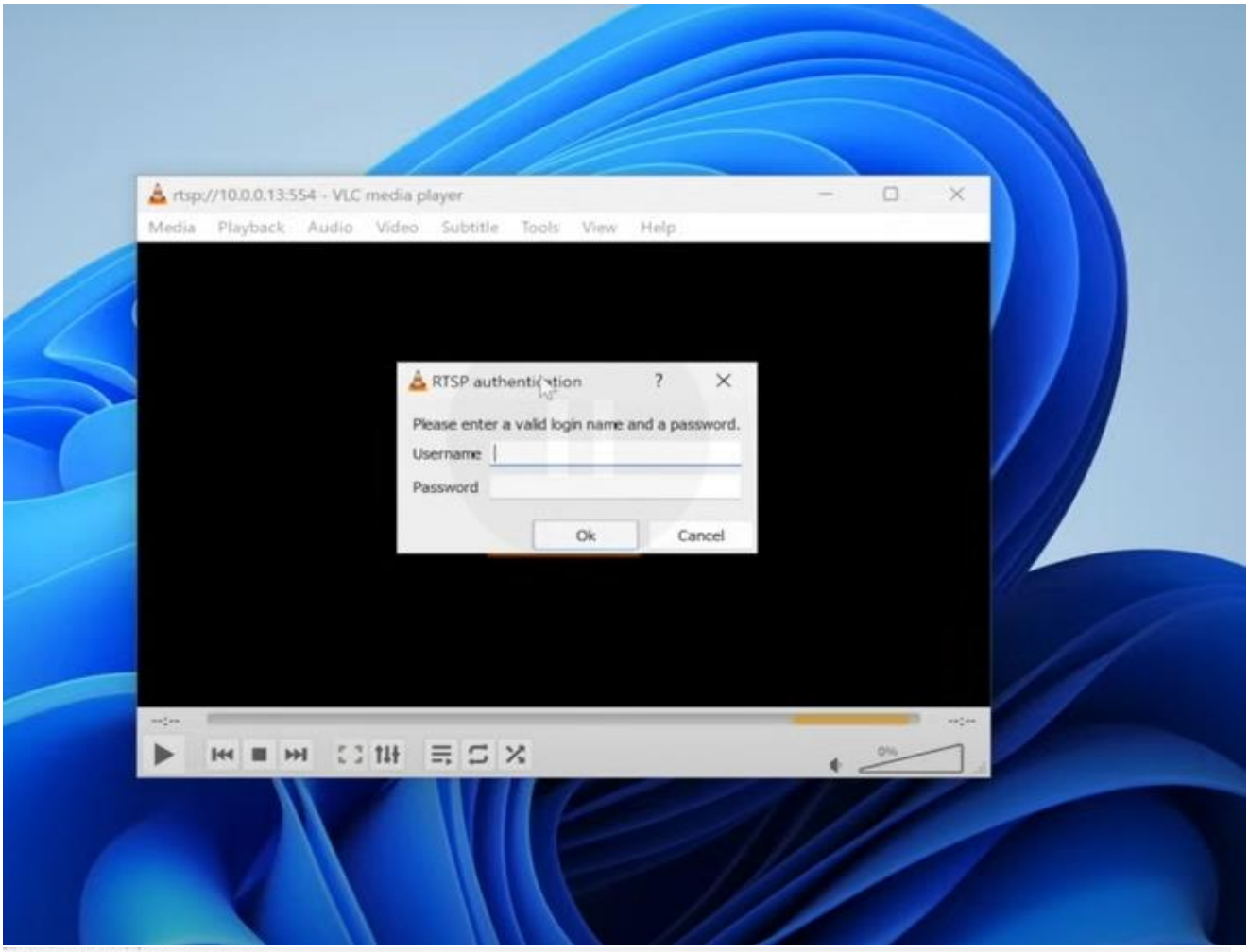
Step4 : Then Open the VLC player and go to the Network Streaming.



Step5 : Then Enter the address “rtsp://10.0.0.12:554/” then press enter



Step6: Enter the default Credentials “admin” for bothe the user and password .then press enter.



Honeyjagadeesh2@gmail.com