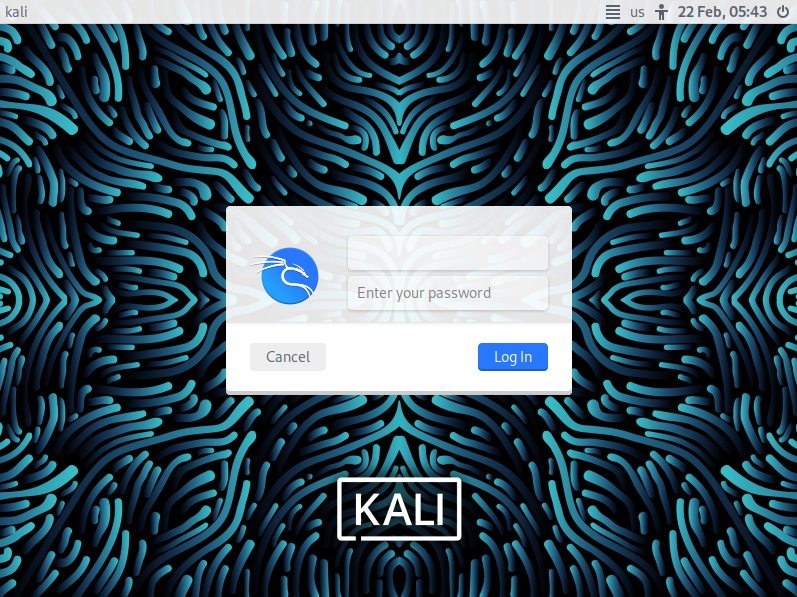
**3. Lab Task - 1**

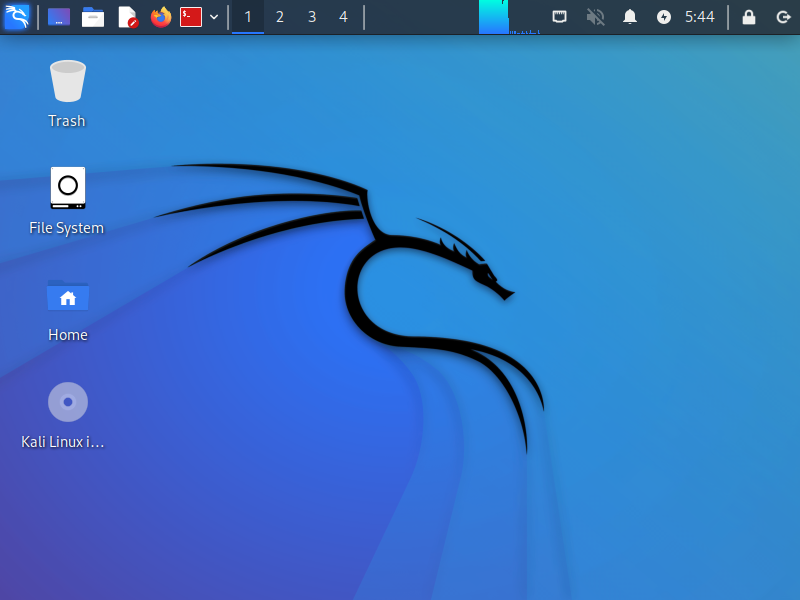
**Part I: Starting Virtual Machines**

We need to use two VMs for this lab: The Kali Linux and the Metasploitable2-Linux.

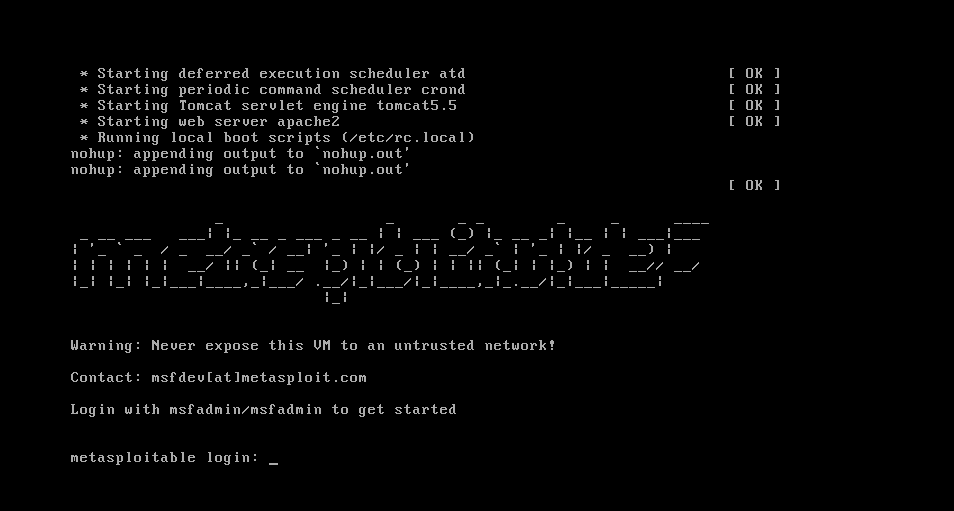
**Step 1:** Start up the Kali Linux.



**Step 2:** Login the Kali Linux with username and password. Below is the screen snapshot after login.

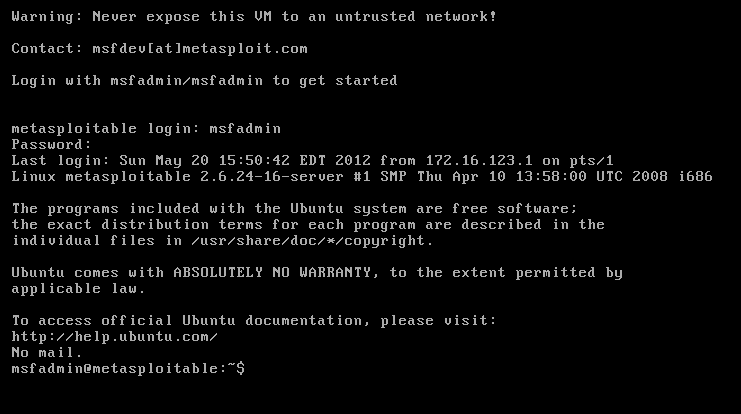


**Step 3:** Then, you select **Metasploitble2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.



**Step 4:** Log into the virtual machine with username, **msfadmin**, and password **msfadmin**.

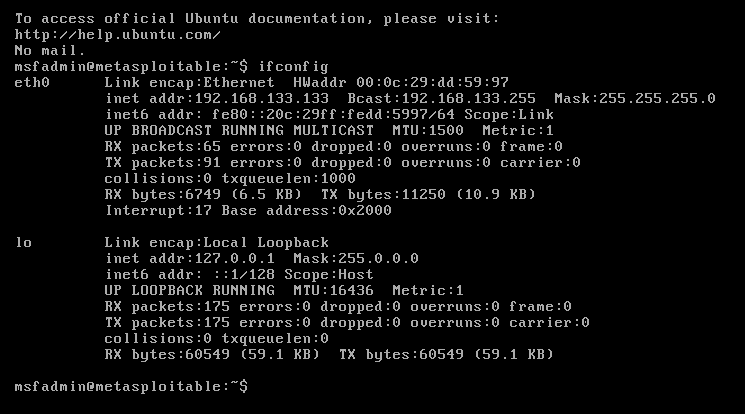
**Step 5:** After you log into the VM, you will see the screen below.



**Part II: Finding the IP Address of the Attacking Target**

**Step 1:** Go to the Metasploitable2-Linux VM, and execute the following command

*$ ifconfig*

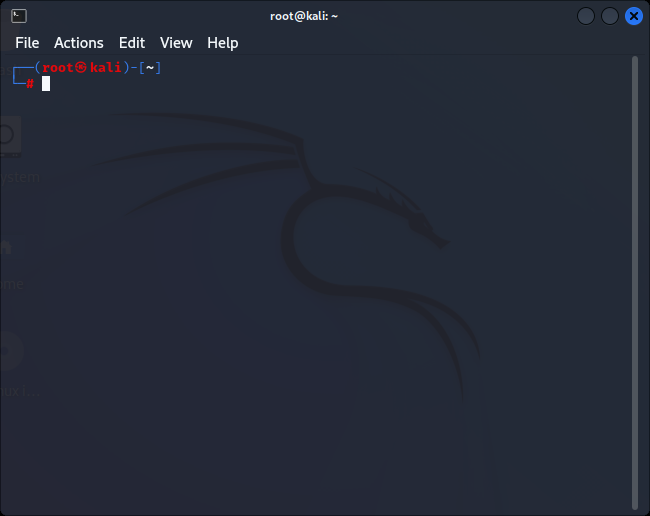


**Step 2:** From the screenshot above, we can see that the IP address of the network interface, eth0, is **192.168.133.133** This is the IP address for the target that you will use later in this lab

**Part III: Scanning the Target Using nmap**

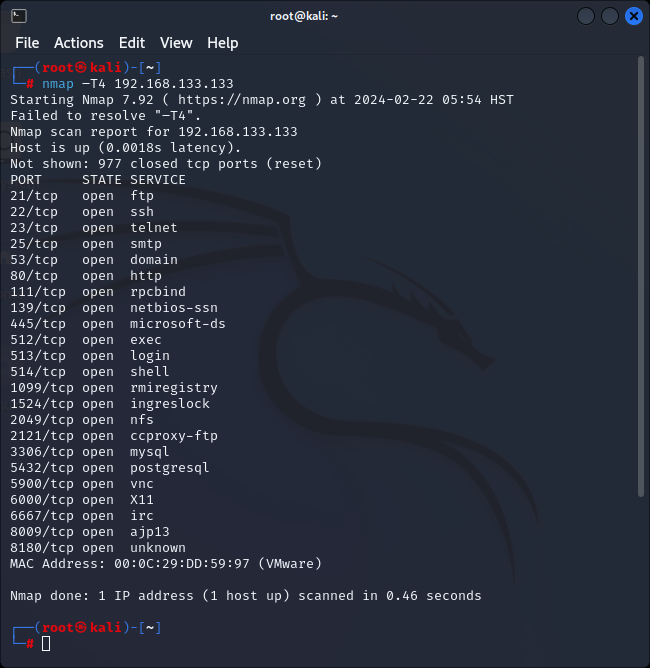
**nmap** ("Network Mapper") is an open-source tool for network exploration and security auditing. Though it was designed to rapidly scan large networks, we use it for scanning the target host in this lab.

**Step 1:** Go to the Kali Linux and open up a terminal by clicking the icon.



**Step 2:** Since nmap has been installed on the Kali Linux, we can just launch the scanning in the terminal by typing the following command:

*$ nmap –T4* **192.168.133.133**

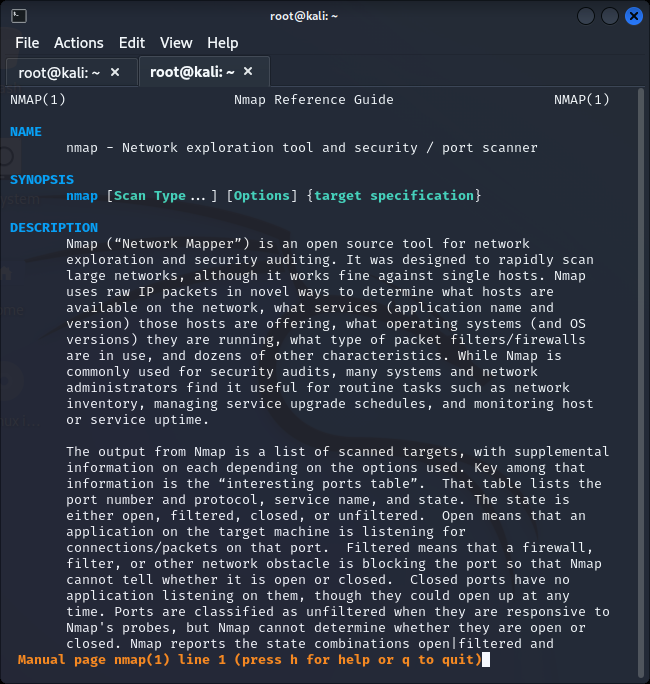


The screenshot above shows a quick scan of the target machine using **nmap**. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

**nmap** provides many useful functions that we can use. You can find more information from the man page of **nmap** from this link: <http://linux.die.net/man/1/nmap>

Or execute the following command in a terminal:

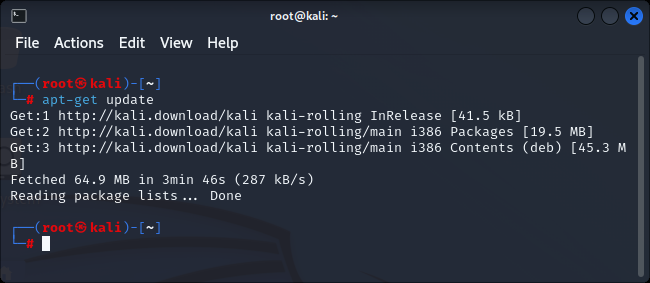
*$ man nmap*



**Part III: Vulnerability Scanning Using OpenVAS**

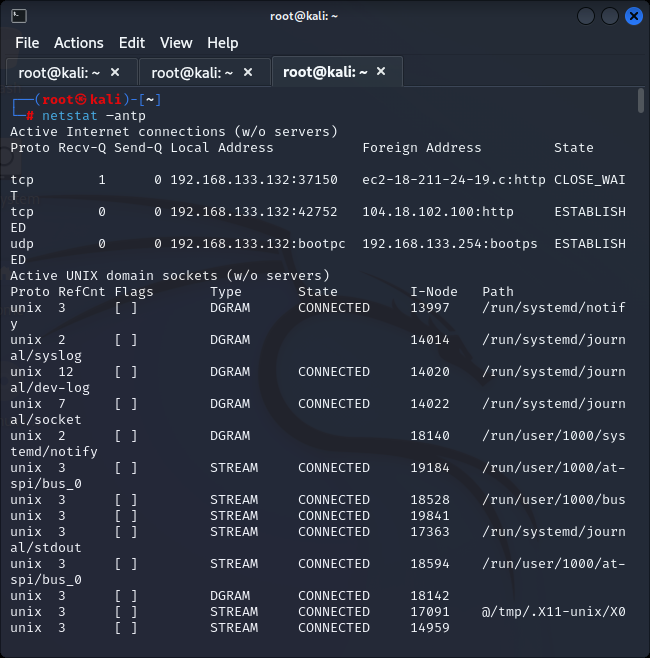
If you want to setup OpenVAS in your own machine, you can follow the steps below.

*root@kali:~# apt-get update*

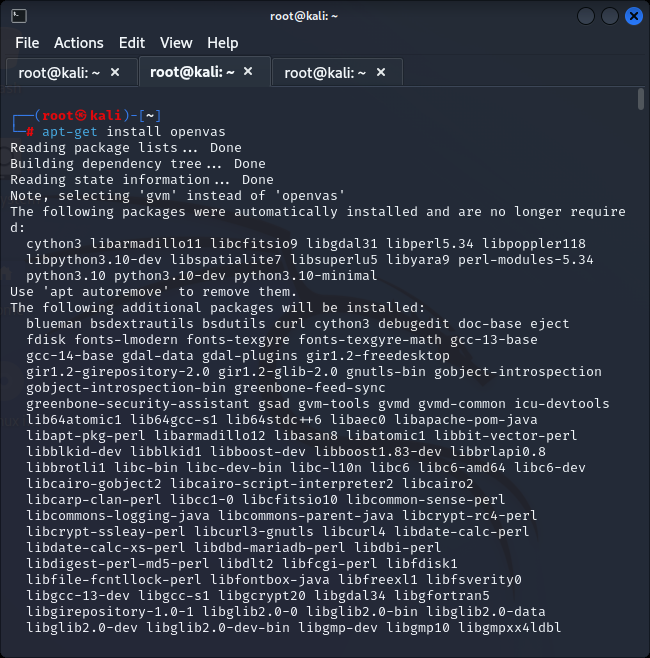


**Step 1:** run the following command to check if the OpenVAS manager, scanner, and GSAD services are listening:

*root@kali:~# netstat –antp*

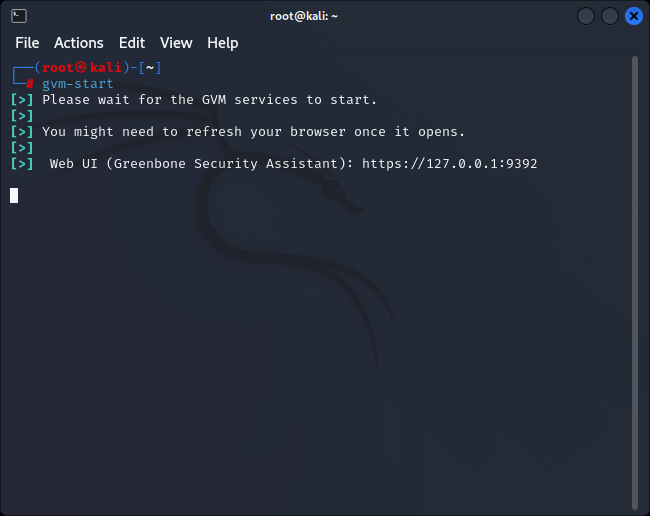


*root@kali:~# apt-get install openvas*



**Step 2:** start the services by executing the following command

*root@kali:~# openvas-start* (OR***gvm-start***if you use Kali 2020 version*)*

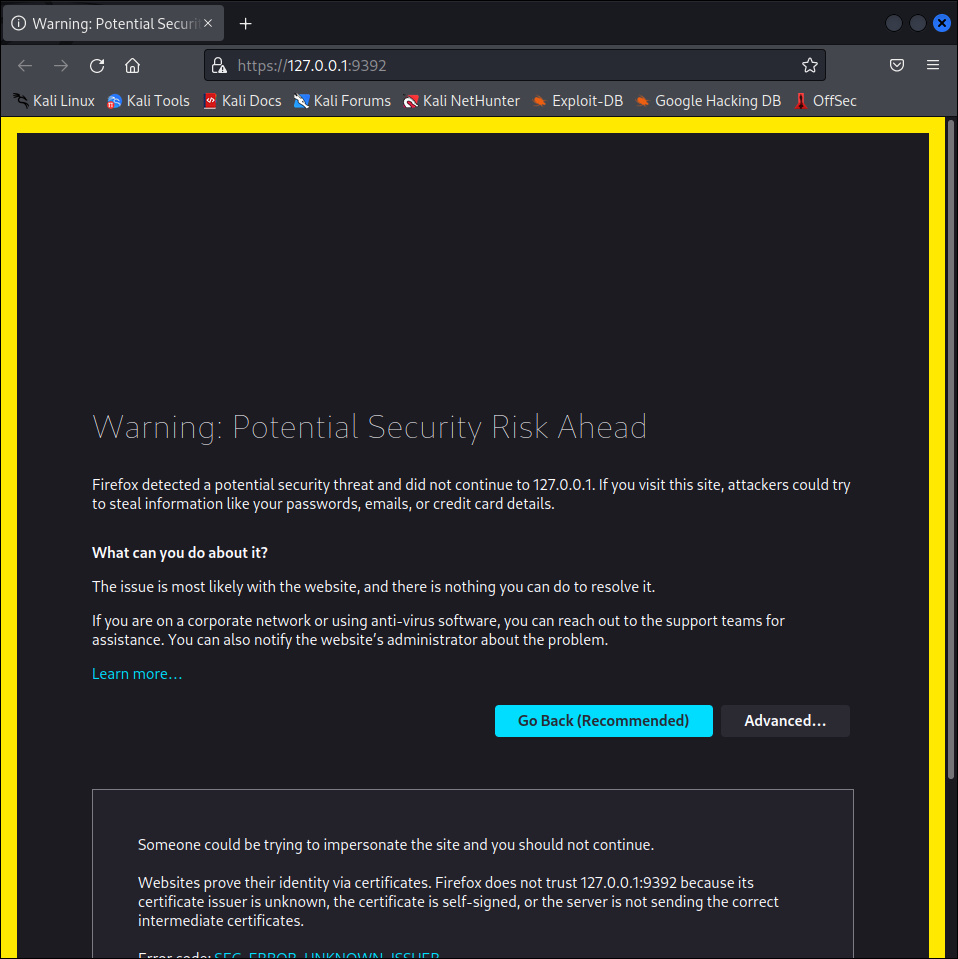


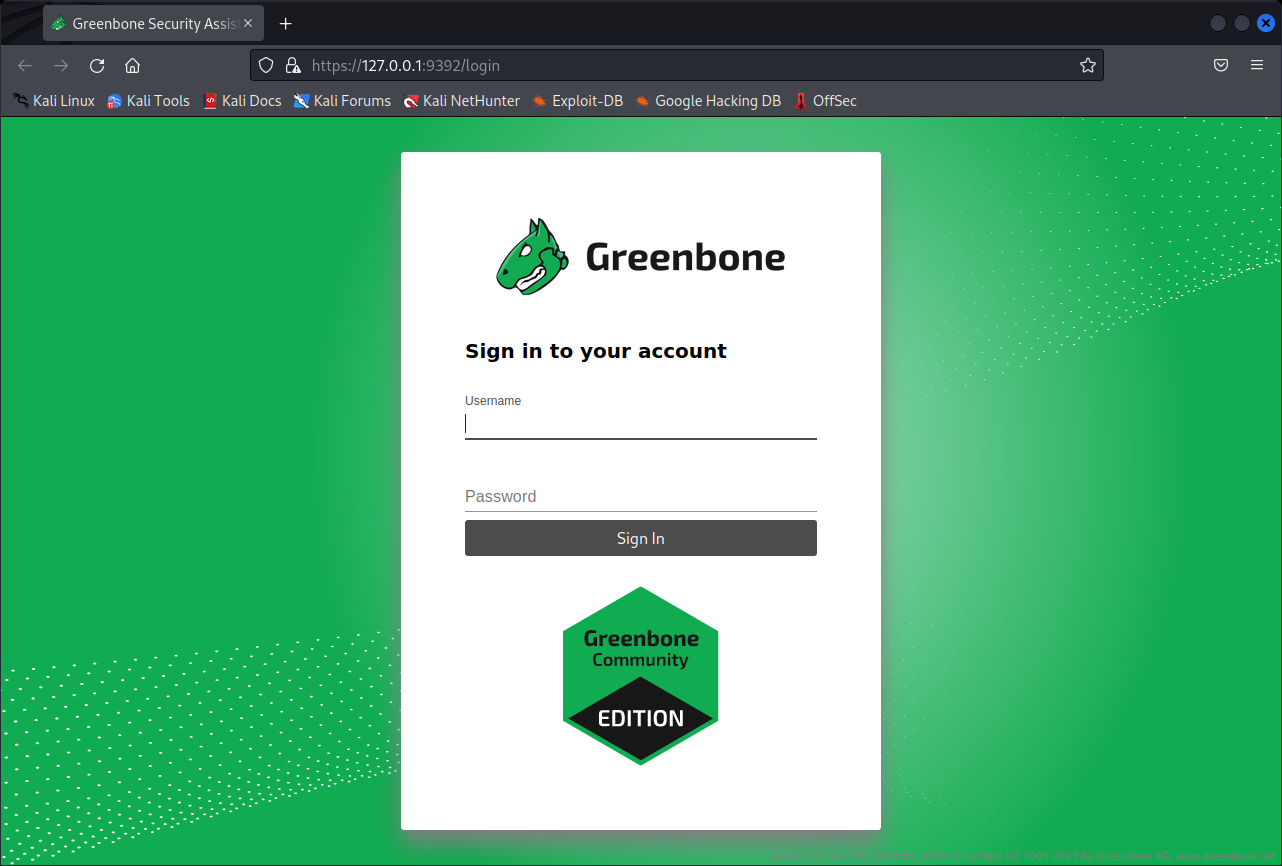
**Part IV: Connecting to the OpenVAS Web Interface**

**Step 1:** Go to the Kali Linux, and open the browser, Iceweasel, by clicking the icon 

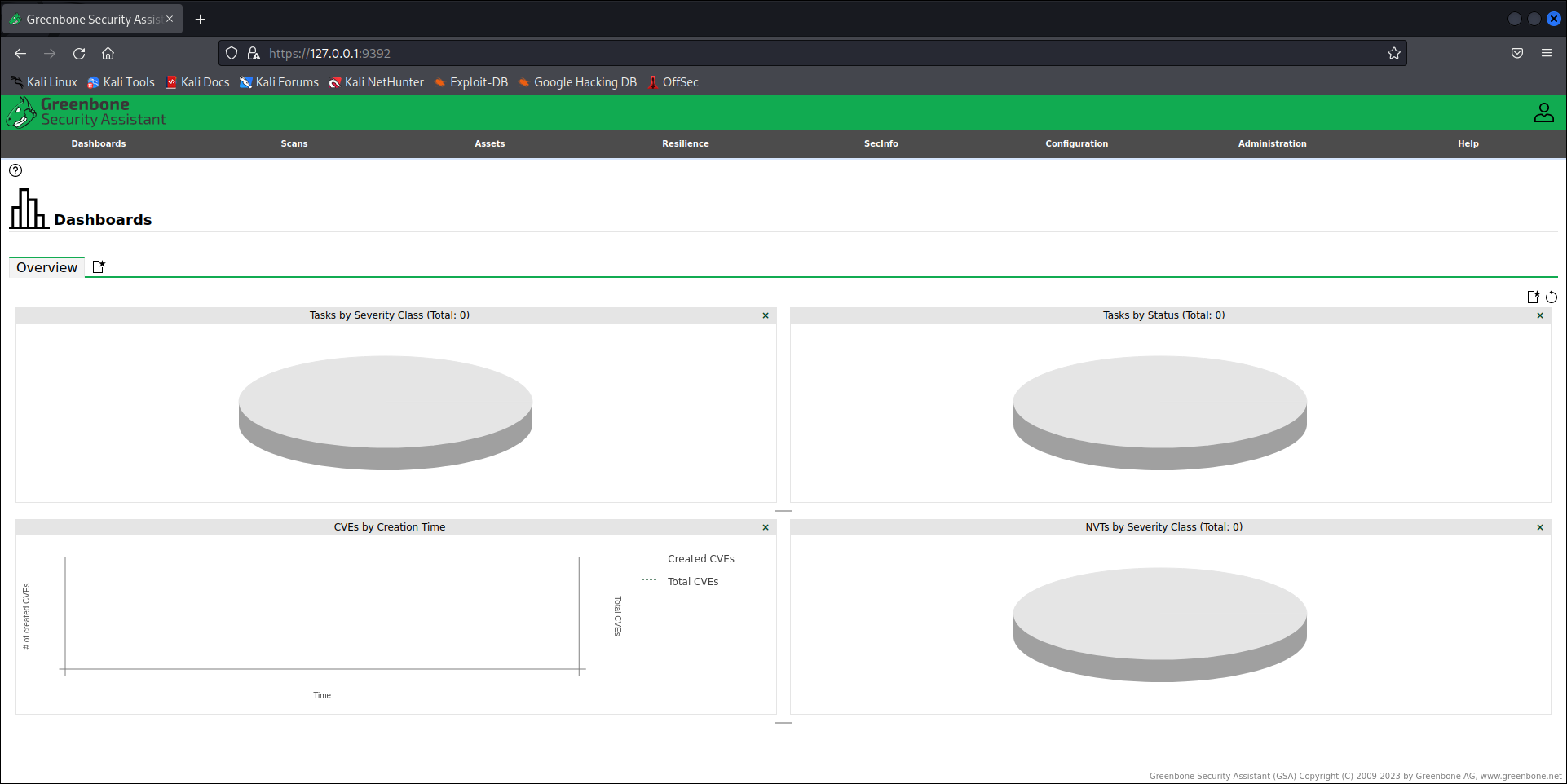
Iceweasel distribution transitioned back to using the official Firefox branding

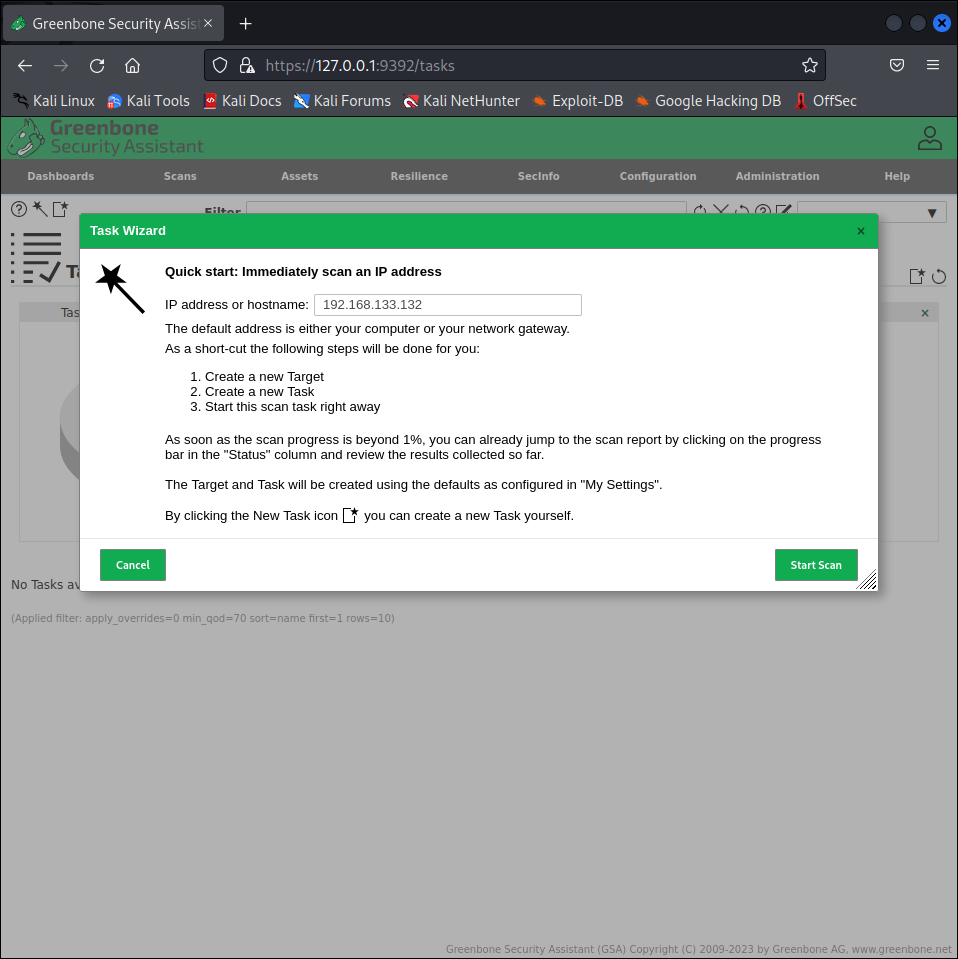
**Step 2:** Then, go to https://127.0.0.1:9392 and accept the self-signed SSL certificate.

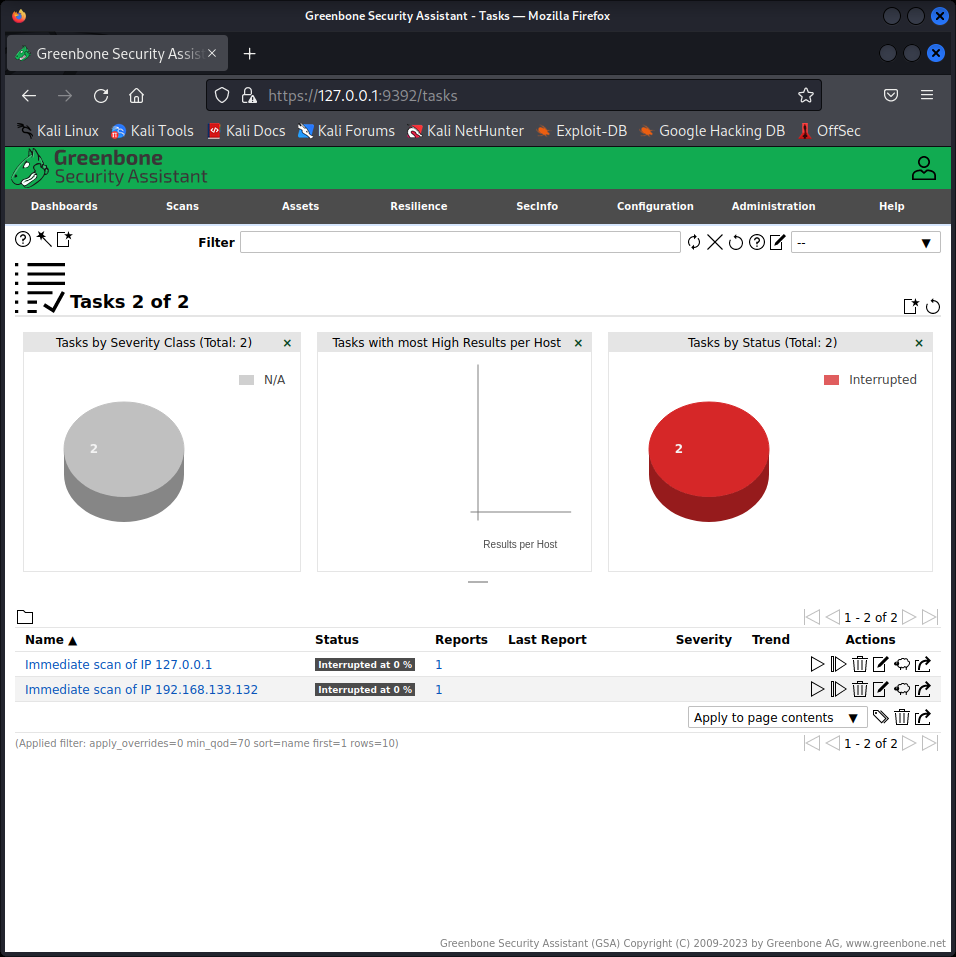


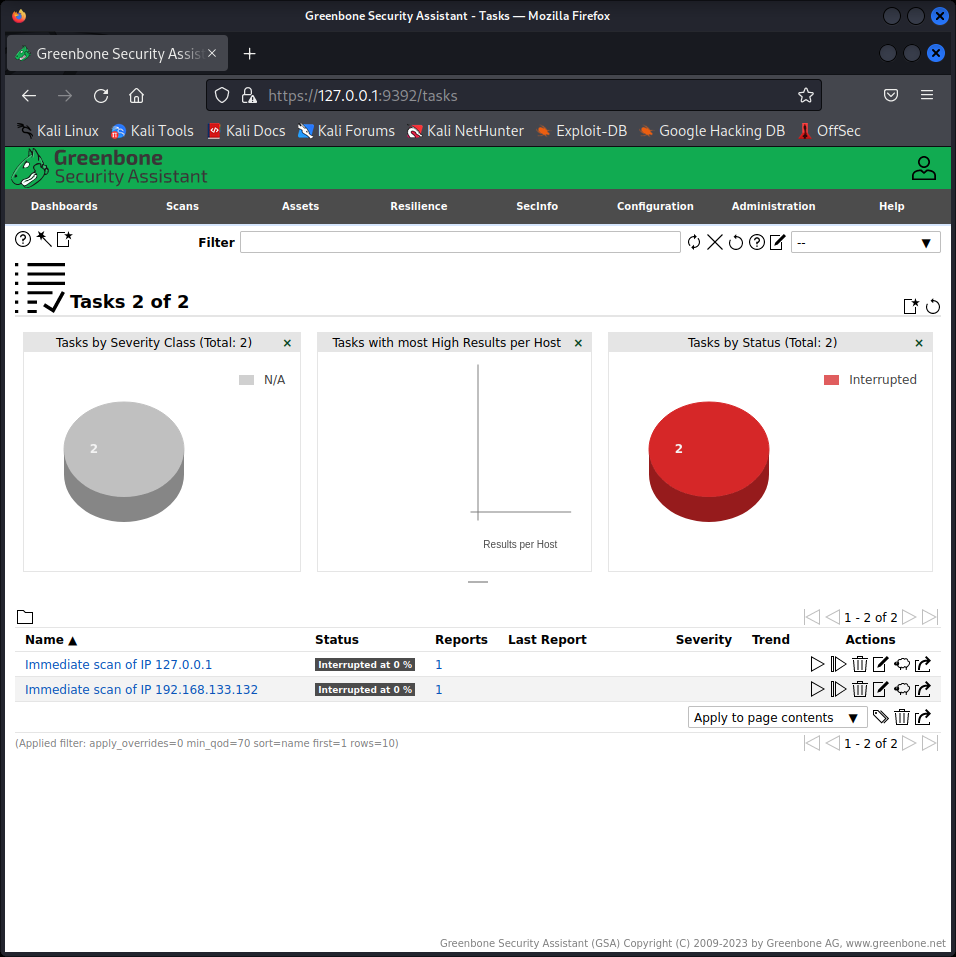


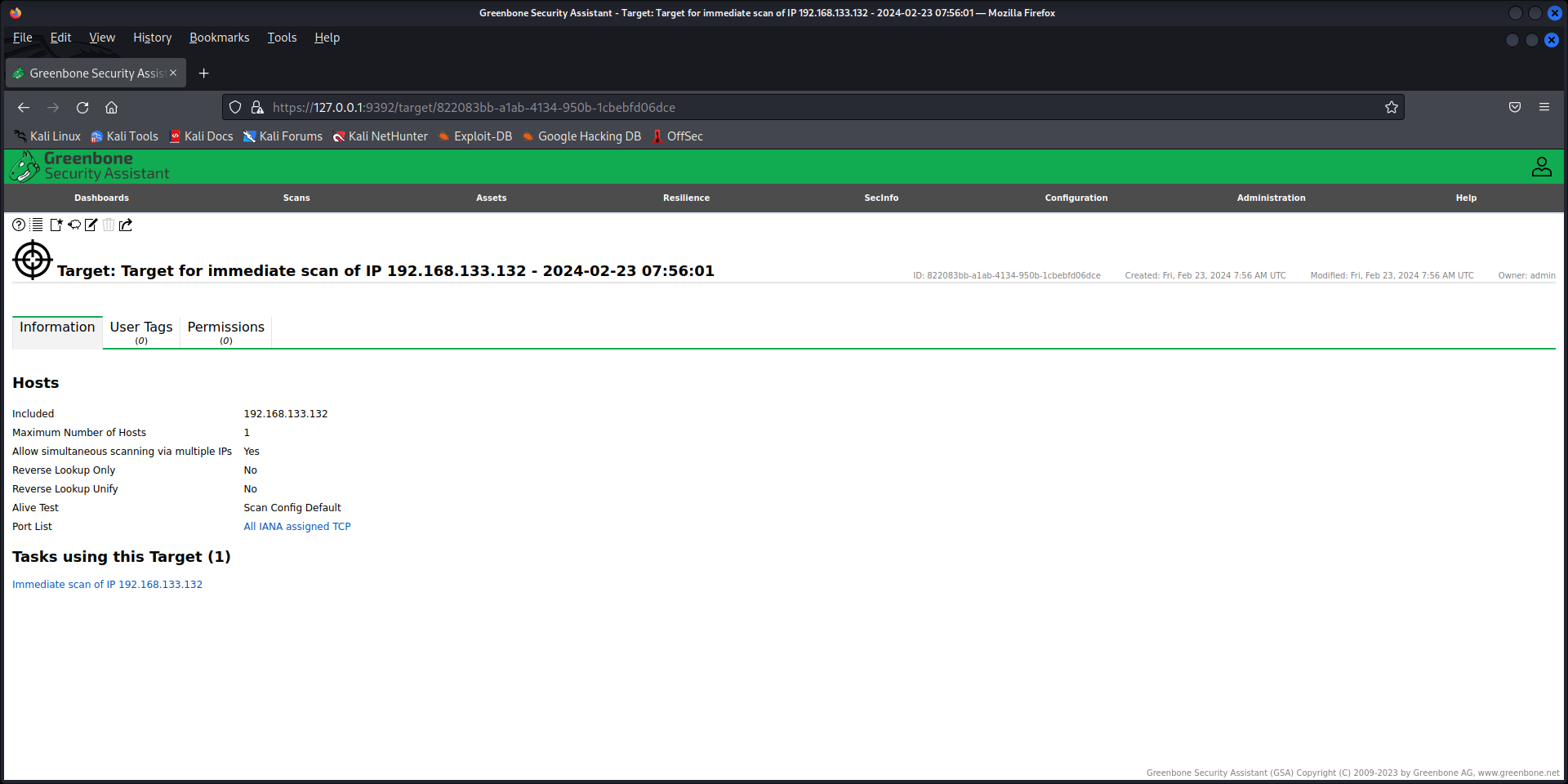
The screenshot on next page is the homepage of OpenVAS. Type the IP address of the target in the “Quick start” box, and press “Start Scan”. It will do the following for you:

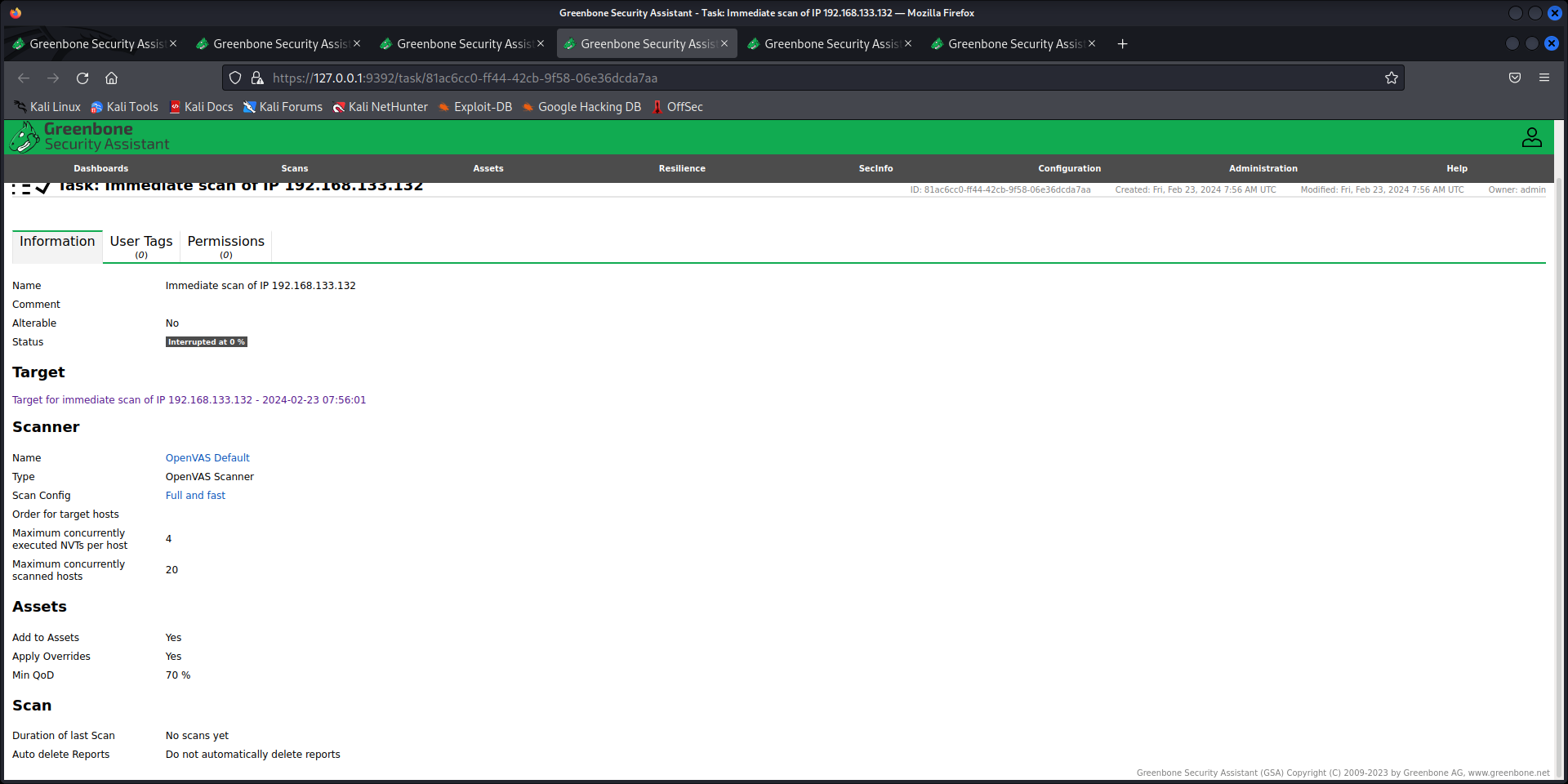




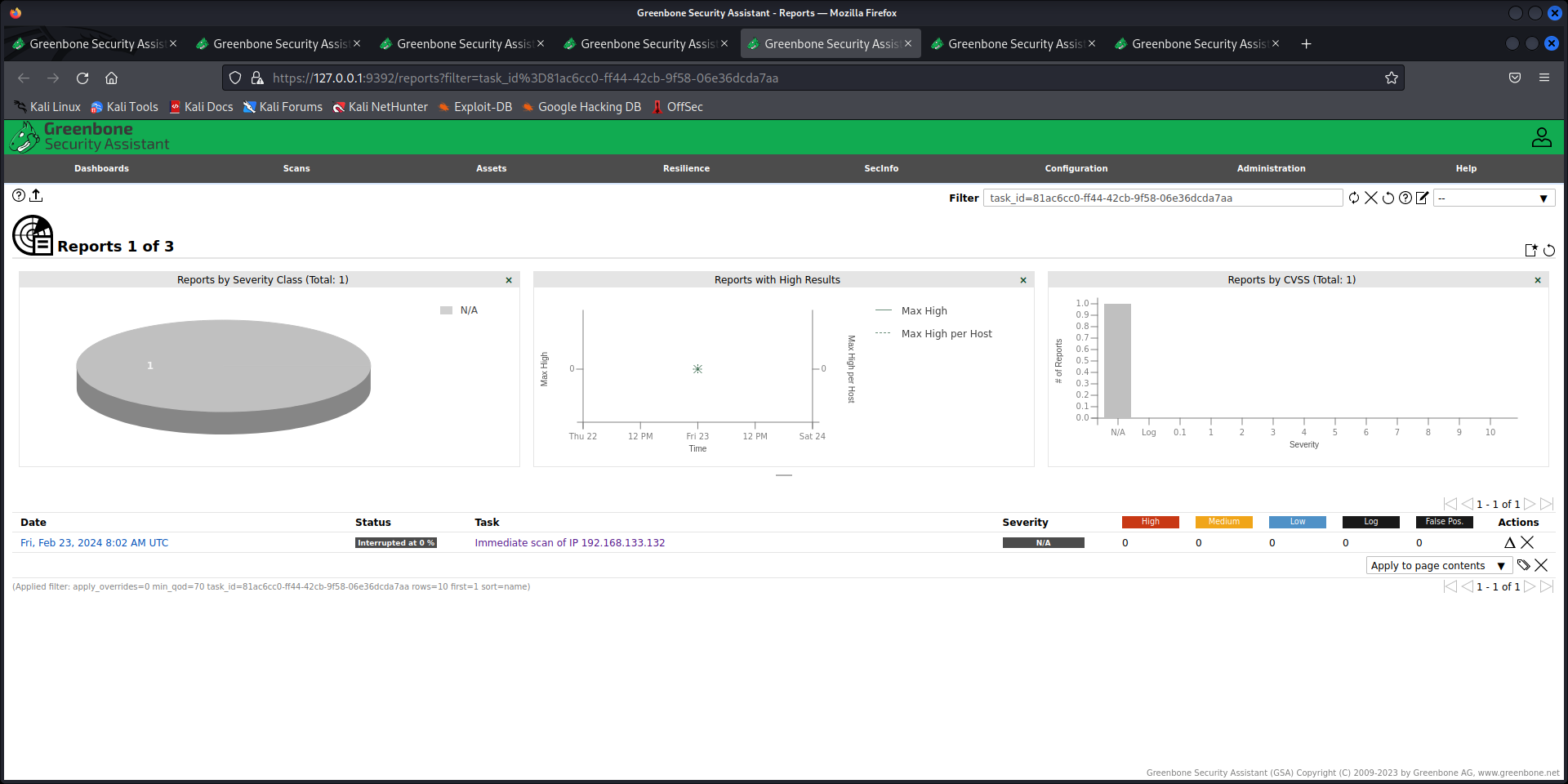








**Step 4:** After finishing the scanning, you can look at the reports as shown in the screenshot below.



**4. Lab Task – 2: Anonymous Web Browsing**

1. Open a web browser.

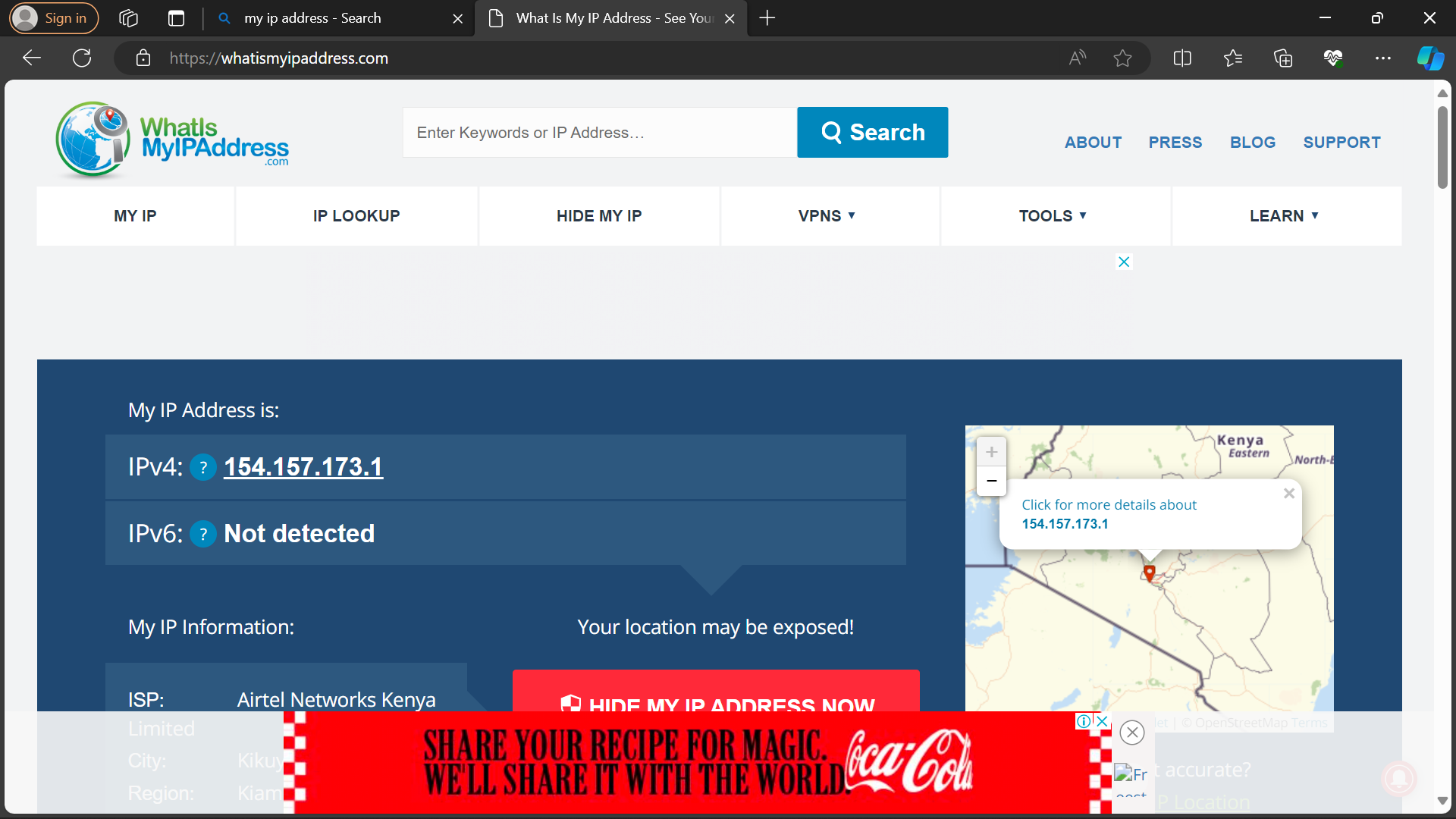
2. Go to www.google.com/.

3. Search for “my IP address.”

4. Press Enter.

5. Click on the first result.

6. Take a screenshot showing your IP address.



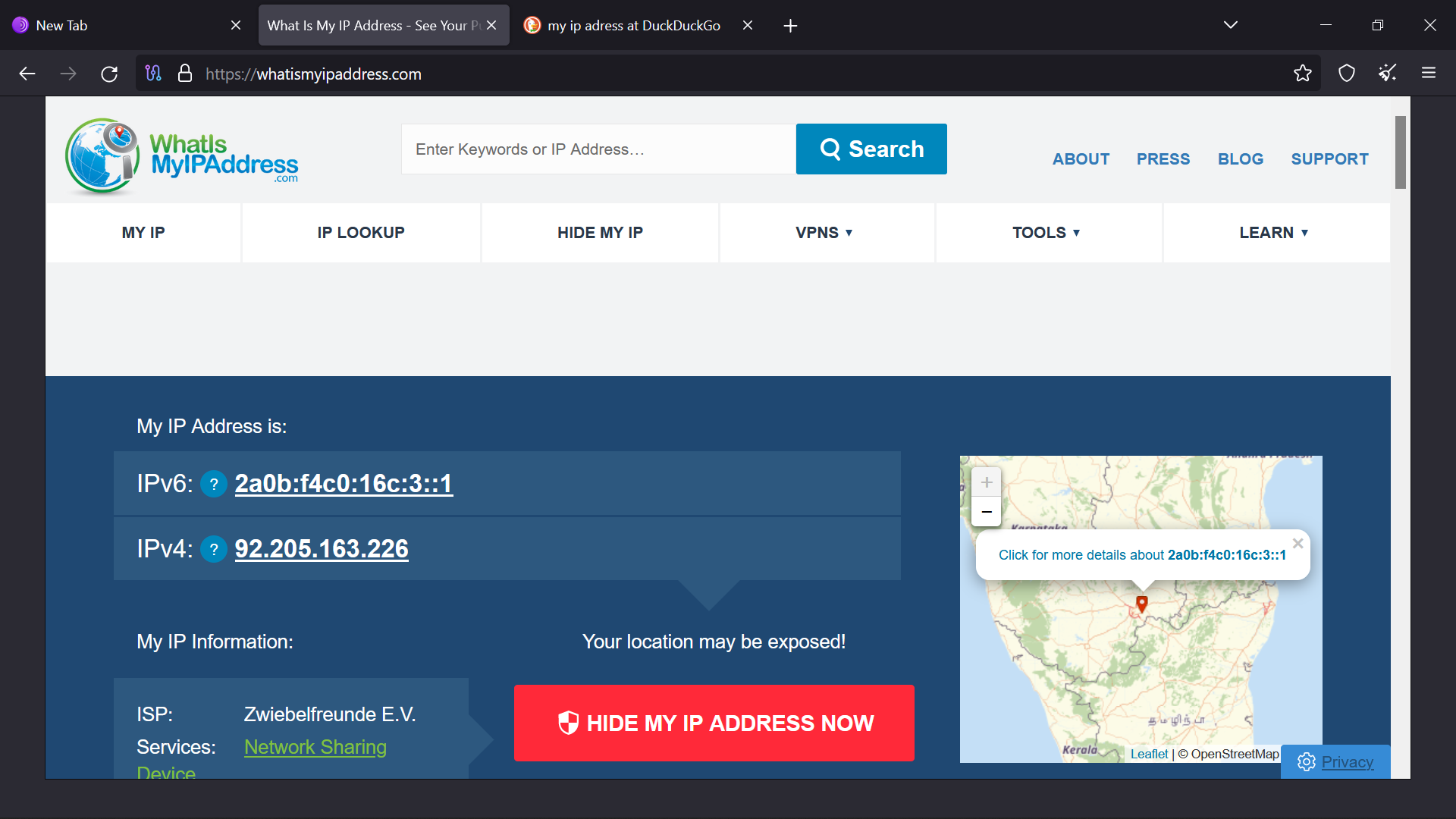
13. Complete the installation process and start the Tor Browser. (If the Tor browser doesn’t automatically start, you can search for “Tor Browser” in the Windows Search menu.)

14. Within the web browser, go to www.Google.com.

15. Search for "my IP address."

16. Click on the first result. (If you get a warning about an "Untrusted" connection, just click on I Understand the Risks, Add Exception, and Confirm Security Exception.)

17. Take a screenshot showing the new IP address. (This is someone else's IP address.)

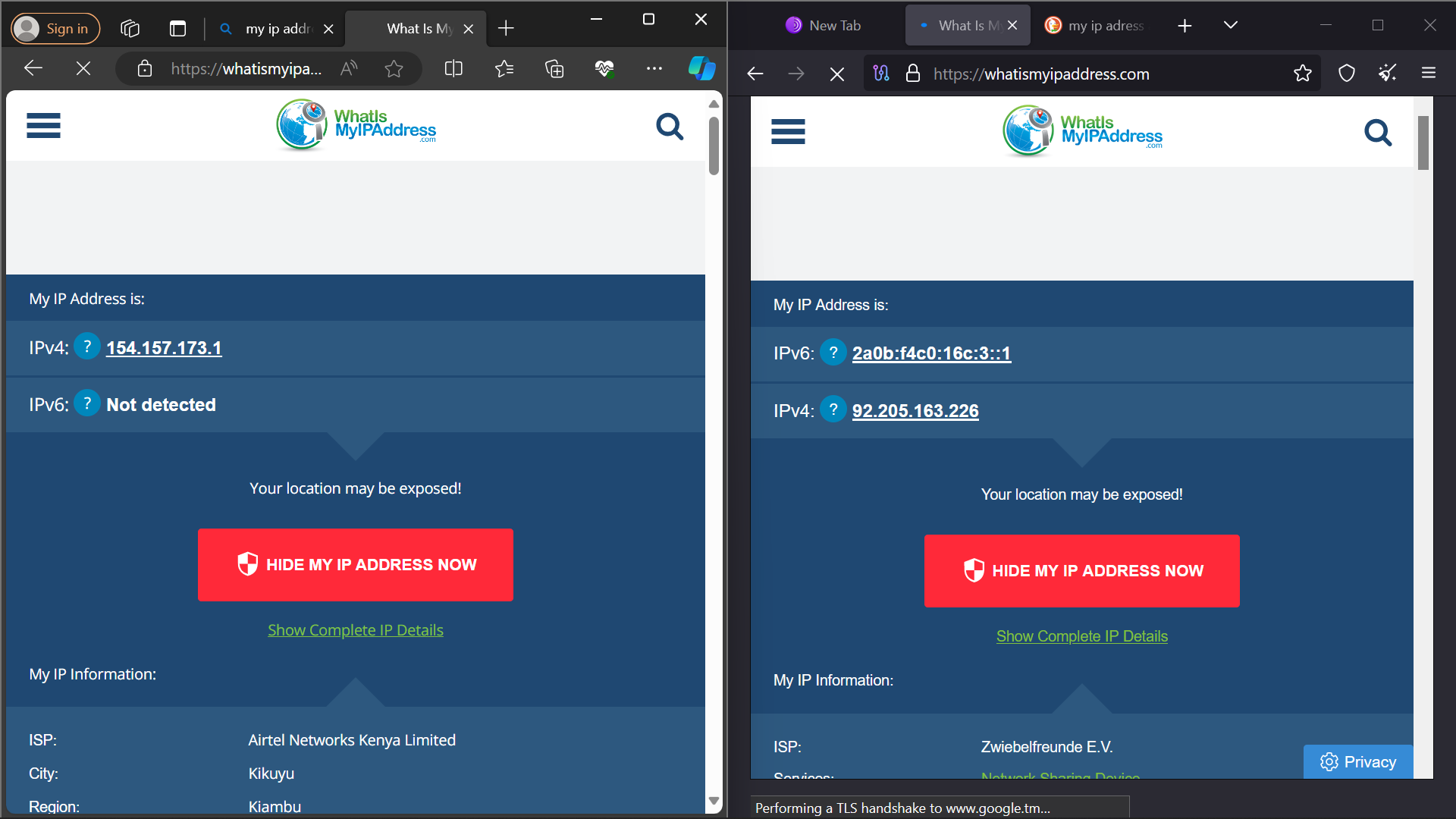


18. Start Microsoft Edge. (Arrange the windows so that the Tor browser and Microsoft Edge are both visible on your desktop.)

26. Search for "my IP address."

27. Click on the first result.

28. Take a screenshot of your desktop (Ctrl-PrintScreen) showing the IP address results in both web browsers. (Use the results from the same website. Each browser should show a different IP address.)



**5. Lab Task – 3: THOUGHT QUESTIONS**

1. **Wireless Network Channels:**
   * Wireless network channels refer to specific radio frequency bands designated for wireless communication. In Wi-Fi networks, these channels are used to transmit data wirelessly between devices. The 2.4 GHz and 5 GHz frequency bands are commonly used, and each band is divided into multiple channels.
   * Whether one channel is better than another depends on factors like interference, congestion, and local regulations. In crowded areas, choosing a less congested channel can improve performance. Also, the 5 GHz band generally offers more channels and is less crowded than the 2.4 GHz band.
2. **WEP Cryptographic Weakness:**
   * WEP (Wired Equivalent Privacy) is considered cryptographically weak due to its use of a static and short encryption key. The key length in WEP is only 40 or 104 bits, making it vulnerable to brute-force attacks.
   * Additionally, WEP reuses initialization vectors (IVs), which further weakens its security. As a result, WEP has been largely deprecated and is not considered secure for protecting wireless networks.
3. **Difference Between WPA and WPA2:**
   * WPA (Wi-Fi Protected Access) and WPA2 are both wireless security protocols.
   * WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption, while WPA2 uses the more secure Advanced Encryption Standard (AES).
   * WPA2 is considered more secure than WPA due to the use of AES and other improvements. WPA3, a newer standard, provides even stronger security features.
4. **Different Network Speeds (11 Mbps vs. 54 Mbps):**
   * Different network speeds are often related to the Wi-Fi standards supported by the devices and routers. For example, 802.11b supports up to 11 Mbps, while 802.11a/g can support up to 54 Mbps.
   * The adoption of newer standards, such as 802.11n and 802.11ac, allows for higher speeds (e.g., 300 Mbps, 600 Mbps, or even higher) depending on the equipment.
5. **Using a Tor Network:**
   * Tor (The Onion Router) provides anonymity by routing internet traffic through a series of volunteer-operated servers (nodes) to conceal the user's location and usage from network surveillance or traffic analysis.
   * Users may want to use Tor for privacy reasons, to bypass censorship, or to access websites on the dark web.
6. **Role of Relay Servers in Tor:**
   * Relay servers in a Tor network pass on user traffic, helping to anonymize it by encrypting and routing it through multiple nodes. Relay servers can operate as entry, middle, or exit nodes in the network.
7. **How Tor Networks Provide Anonymity:**
   * Tor networks provide anonymity by encrypting and routing traffic through multiple nodes, making it difficult to trace the origin and destination of the data. The use of layered encryption and random paths adds an extra layer of security.
8. **Importance of HTTPS in Tor Networks:**
   * While Tor provides anonymity for the user, it only anonymizes the traffic within the Tor network. Using an HTTPS connection ensures end-to-end encryption, securing the data between the user and the destination website. It protects against potential threats like man-in-the-middle attacks even within the Tor network.