Module 11: Session Hijacking

Scenario

A session hijacking attack refers to the exploitation of a session token-generation mechanism or token security controls that enables an attacker to establish an unauthorized connection with a target server. The attacker guesses or steals a valid session ID (which identifies authenticated users) and uses it to establish a session with the server.

As an ethical hacker or penetration tester, you should understand different session hijacking concepts, how attackers perform application- and network-level session hijacking, and the various tools used to launch this kind of attack. You should also be able to implement security measures at both the application and network levels to protect your network from session hijacking. Application-level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. Network-level hijacking is prevented by packet encryption, which can be achieved with protocols such as IPsec, SSL, and SSH.

Objective

The objective of the lab is to perform session hijacking and other tasks that include, but are not limited to:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Overview of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker:

- **Active session hijacking**: An attacker finds an active session and takes it over
- **Passive session hijacking**: An attacker hijacks a session, and, instead of taking over, monitors and records all the traffic in that session

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

1. Perform session hijacking
    - Hijack a session using Caido
    - Intercept HTTP traffic using Hetty

2. Detect session hijacking
    - Detect session hijacking using Wireshark

Lab 1: Perform Session Hijacking

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

As a professional ethical hacker or penetration tester, you must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Lab Objectives

- Hijack a session using Caido
- Intercept HTTP traffic using Hetty

Overview of Session Hijacking

Session hijacking can be divided into three broad phases:

- **Tracking the Connection**: The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict

- **Desynchronizing the Connection**: A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)

- **Injecting the Attacker's Packet**: Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or

actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Task 1: Hijack a Session using Caido

Caido assists security professionals and enthusiasts in efficiently auditing web applications. It offers exploration tools, including sitemap, history, and intercept features, which aid in identifying vulnerabilities and analyzing requests in real-time. Users can modify incoming requests using Forward and Tamper tools, enhancing testing customization and system security comprehension. Automation is facilitated through the Automate tool, allowing for faster vulnerability discovery by testing requests against large wordlists. Caido's intuitive UI simplifies security testing for both novices and experts with clear navigation and user-friendly controls.

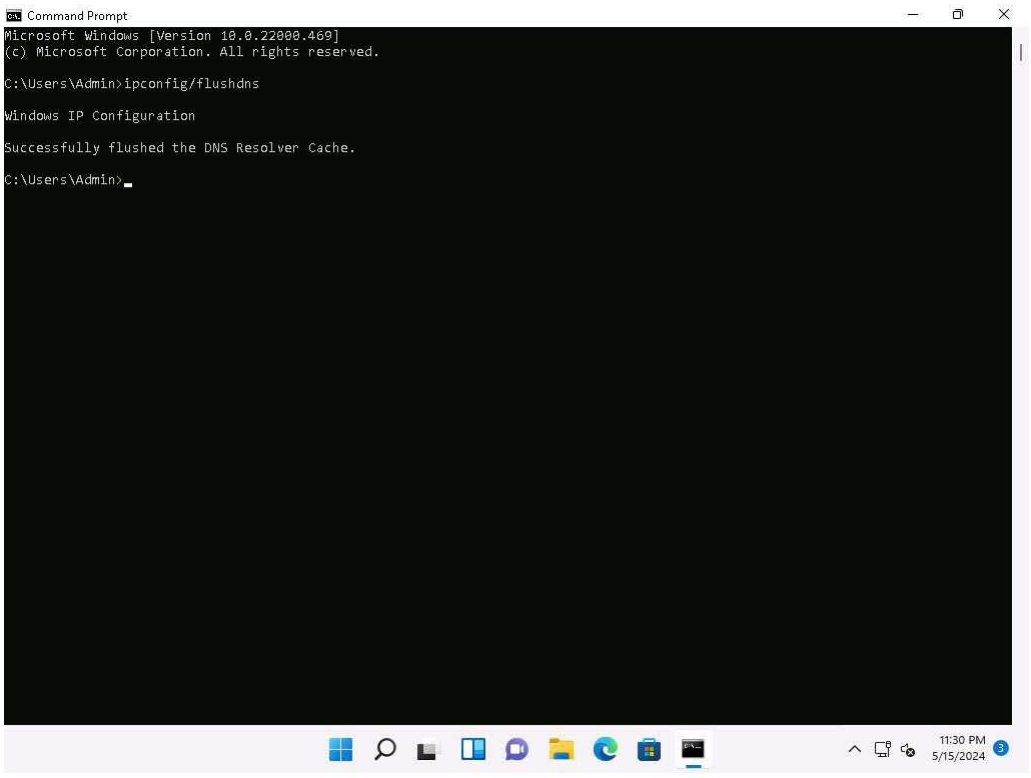
Here, we will use Caido to perform session hijacking on the target machine.

Before starting this task, we need to configure the proxy settings in the victim's machine, which in this task will be the Windows Server 2019 machine.

1. Click Windows 11 to switch to the **Windows 11** machine. Login using **Admin**/**Pa$$w0rd**.

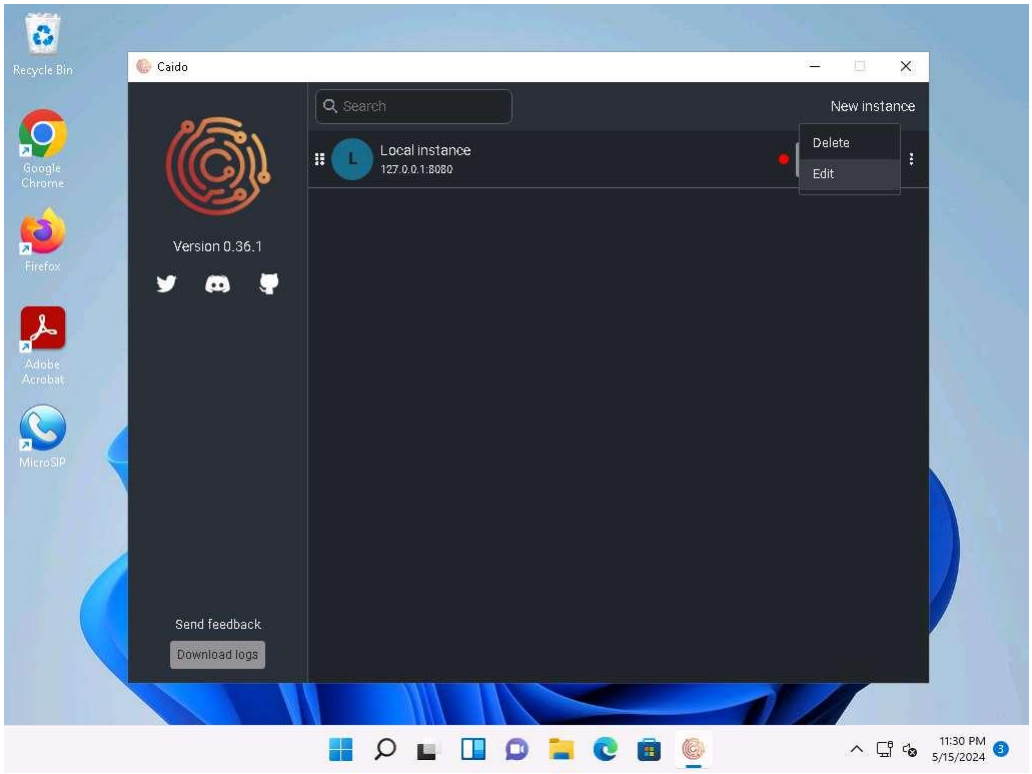
2. Click windows **Search** icon on the **Desktop**, search for **cmd** and launch **Command Prompt** from search bar.

3. Run **ipconfig/flushdns** command to reset dns cache and close the Command Prompt.

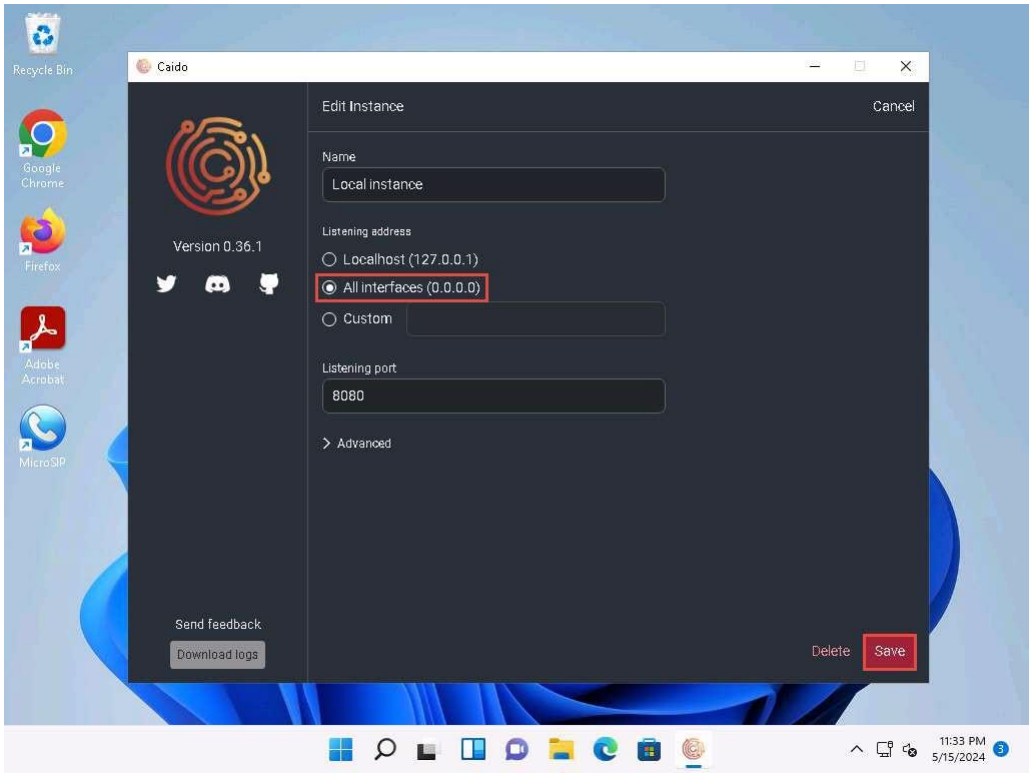


4. Click windows **Search** icon on the **Desktop**, search for **Caido** and launch **Caido** from search bar.

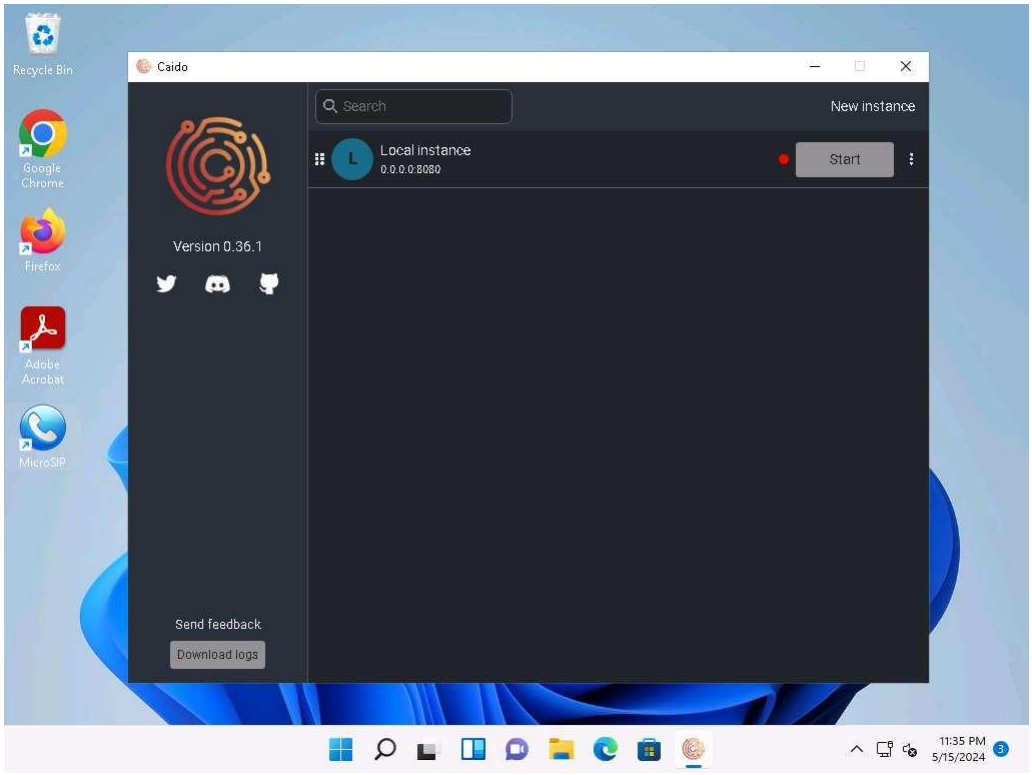
5. **Caido** application window appears, click on **menu** besides Start button and select **Edit**.



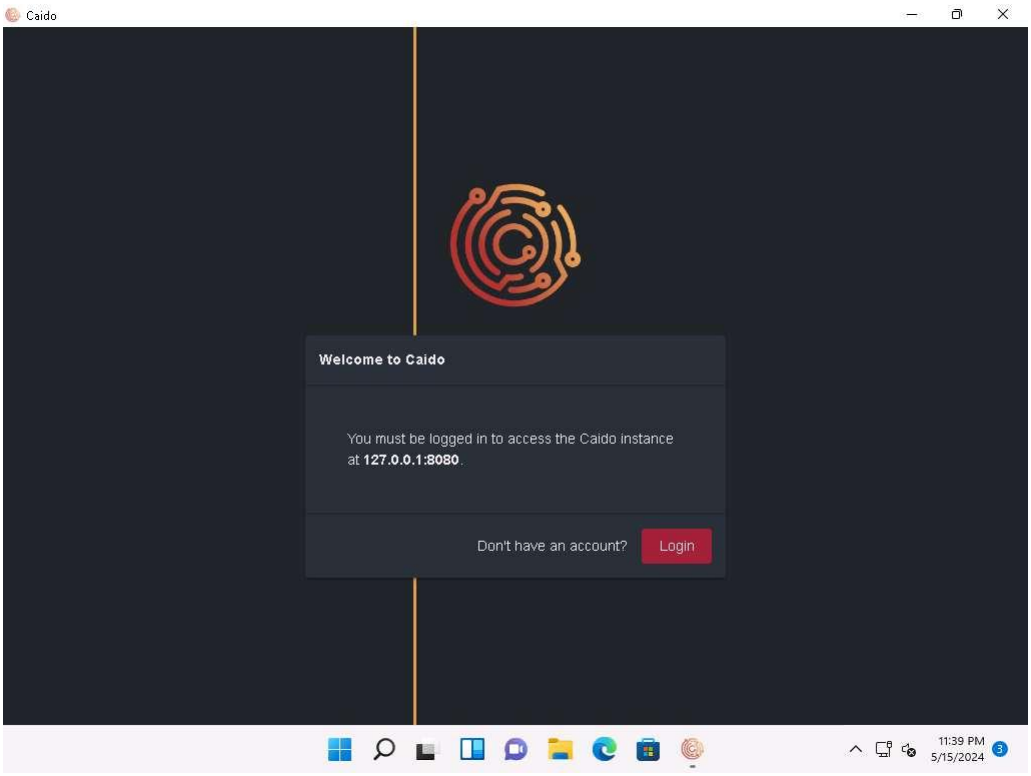
6. In **Edit Instance** window, click on the radio button besides **All interfaces (0.0.0.0)** to listen on all the available network interfaces and click on **Save**.



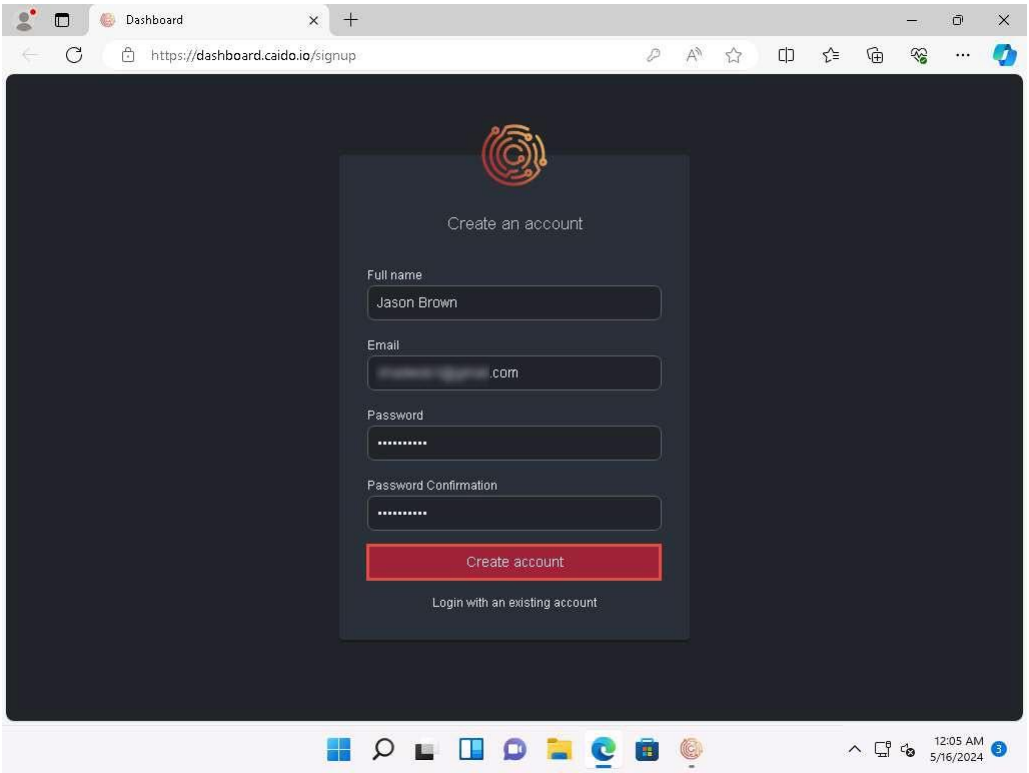
7. Click on **Start** button to start the local instance.



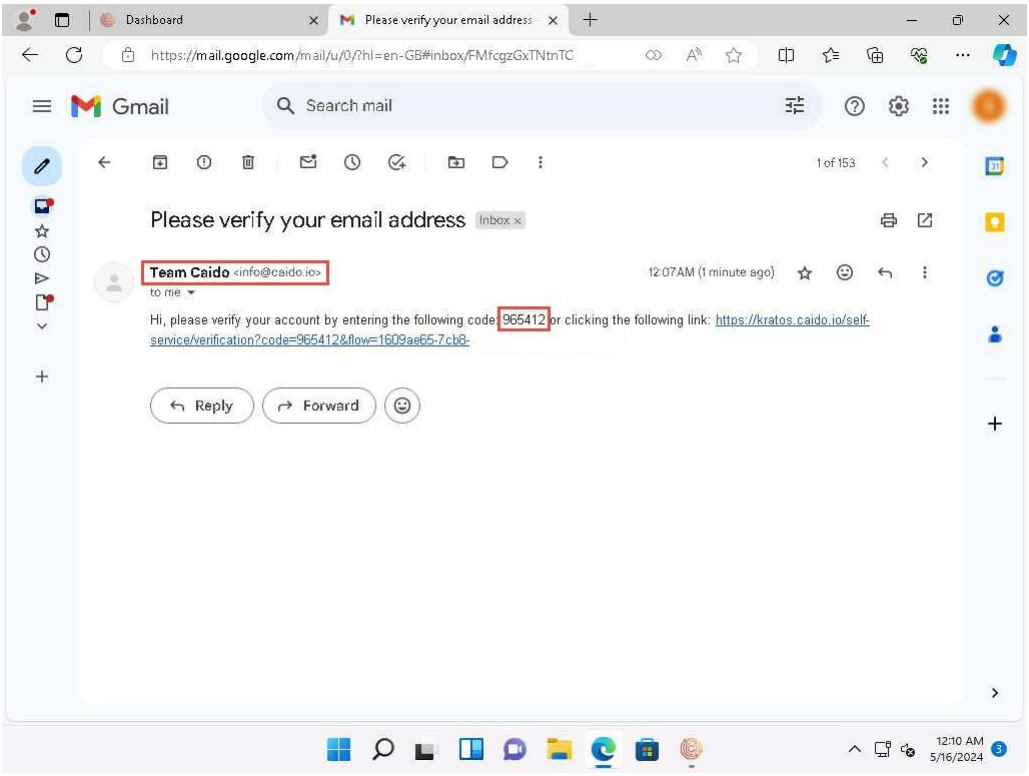
8. **Welcome to Caido** pop-up appears, click on **Login** if you have an account already. If not, select **Don't have an account?**, you will be redirected to Dashboard.



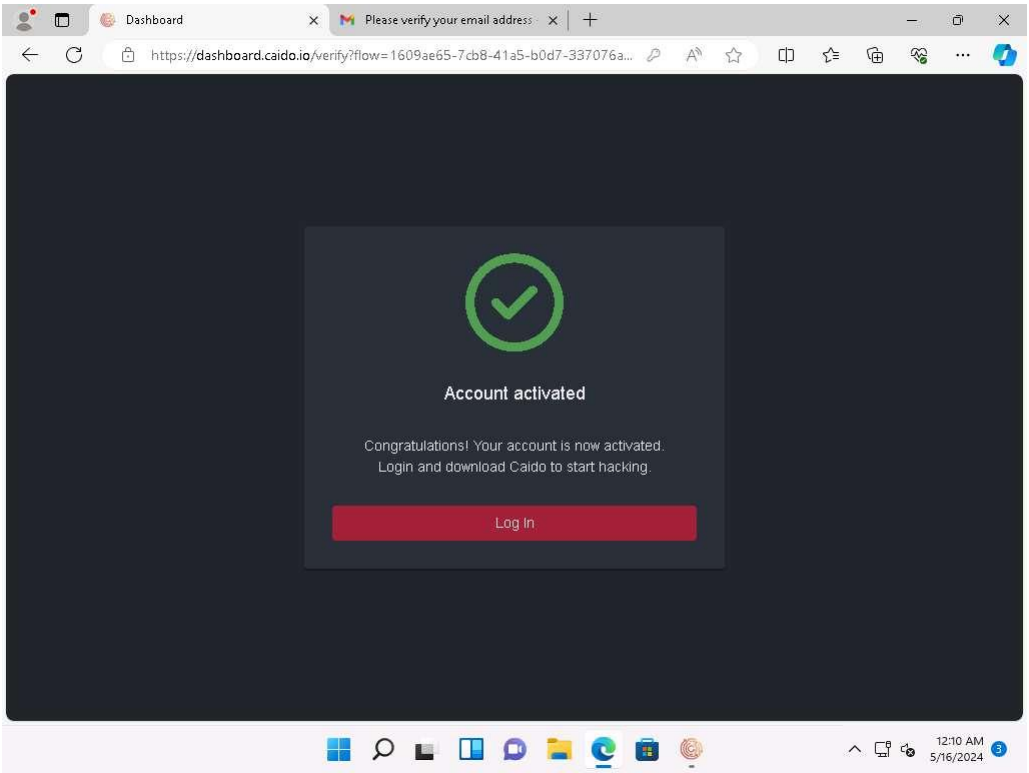
9. **Create an account** window appears, here fill in the details and click on **Create account**.



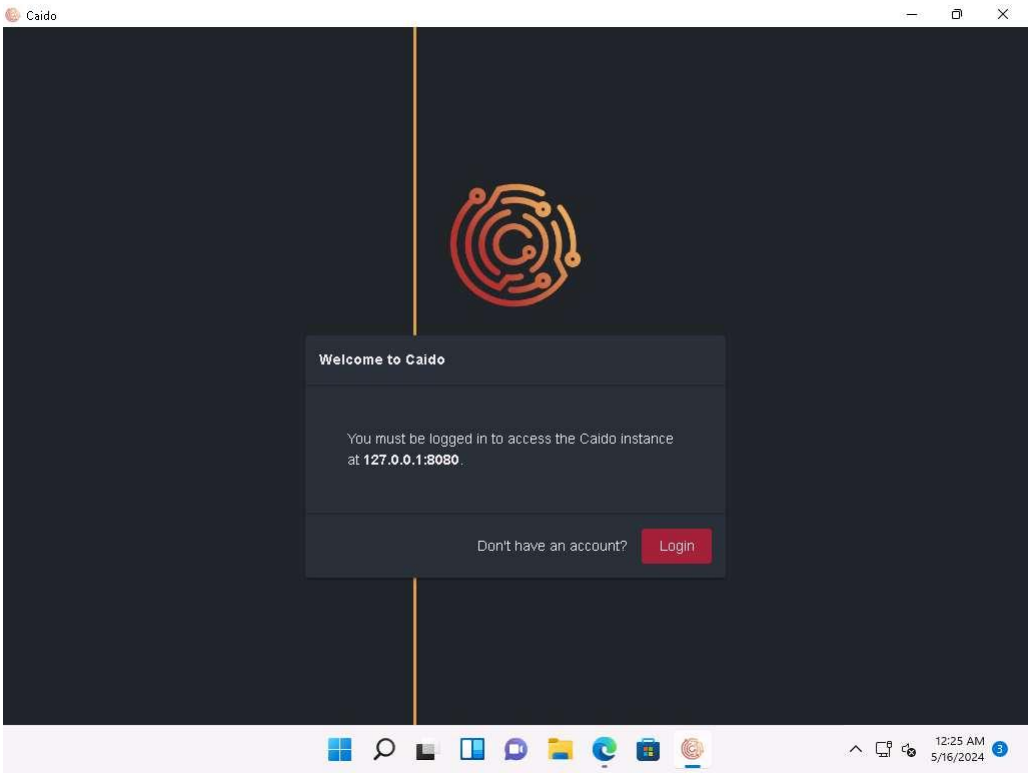
10. Login to your mail account, you will receive a verification mail from **Team Caido** copy the code and paste it in the Caido verification window.



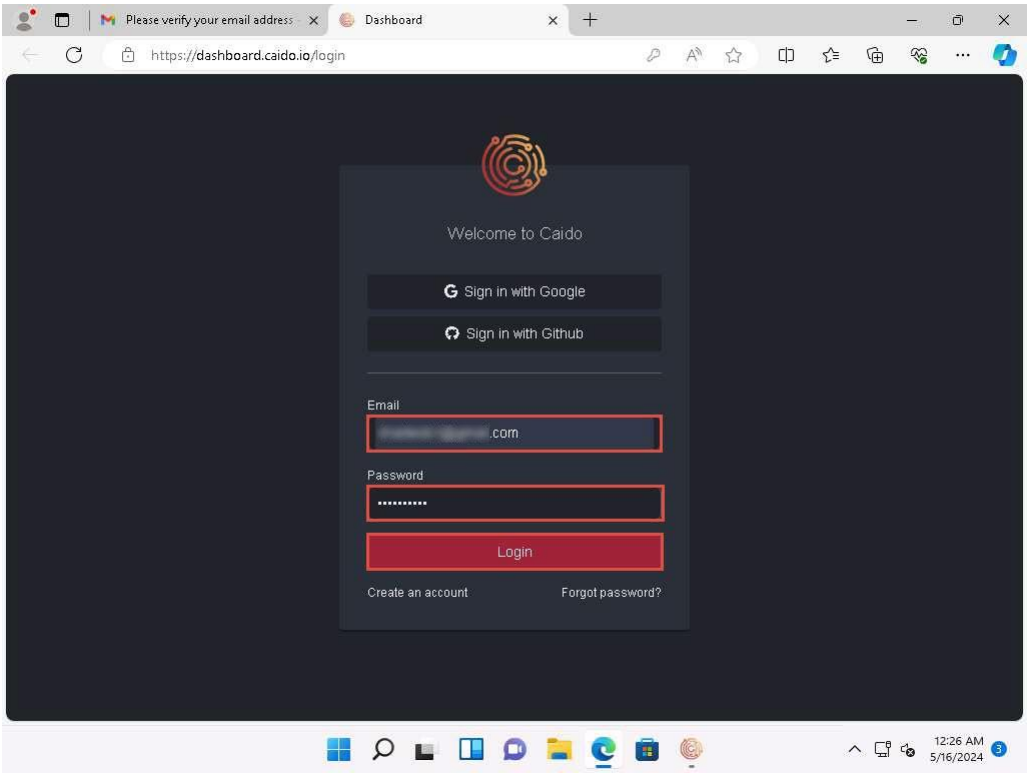
11. After entering the code, your account will be activated as shown in the screenshot.



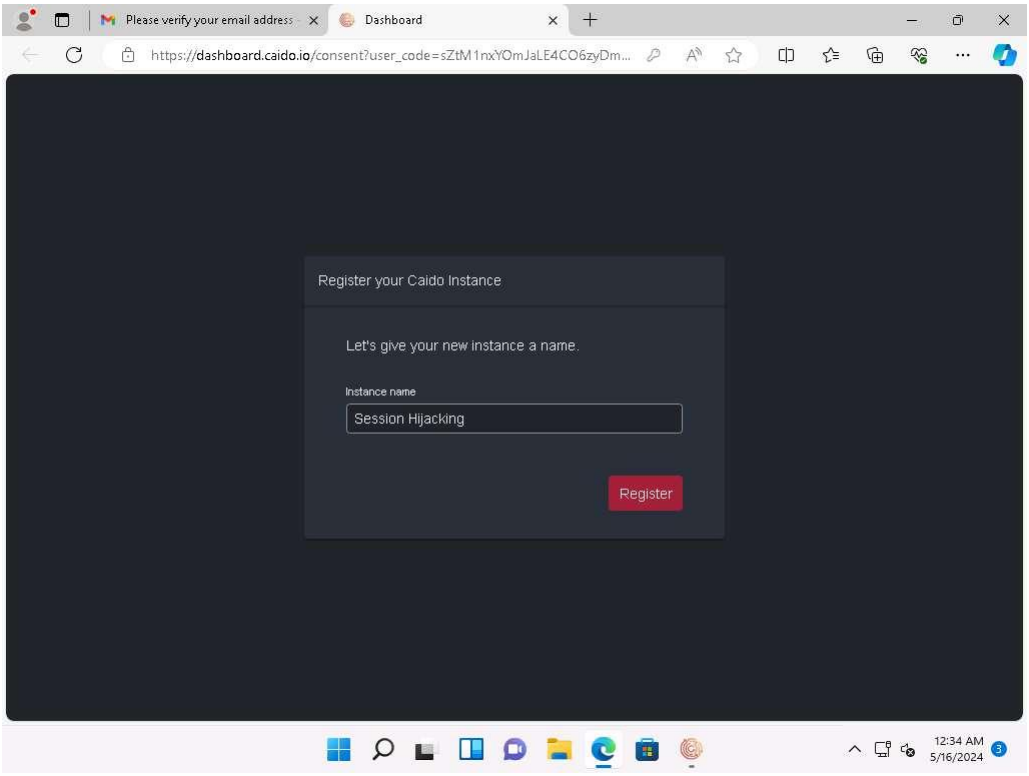
12. Navigate back to Caido application, in **Welcome to Caido** pop-up click on **Login**.



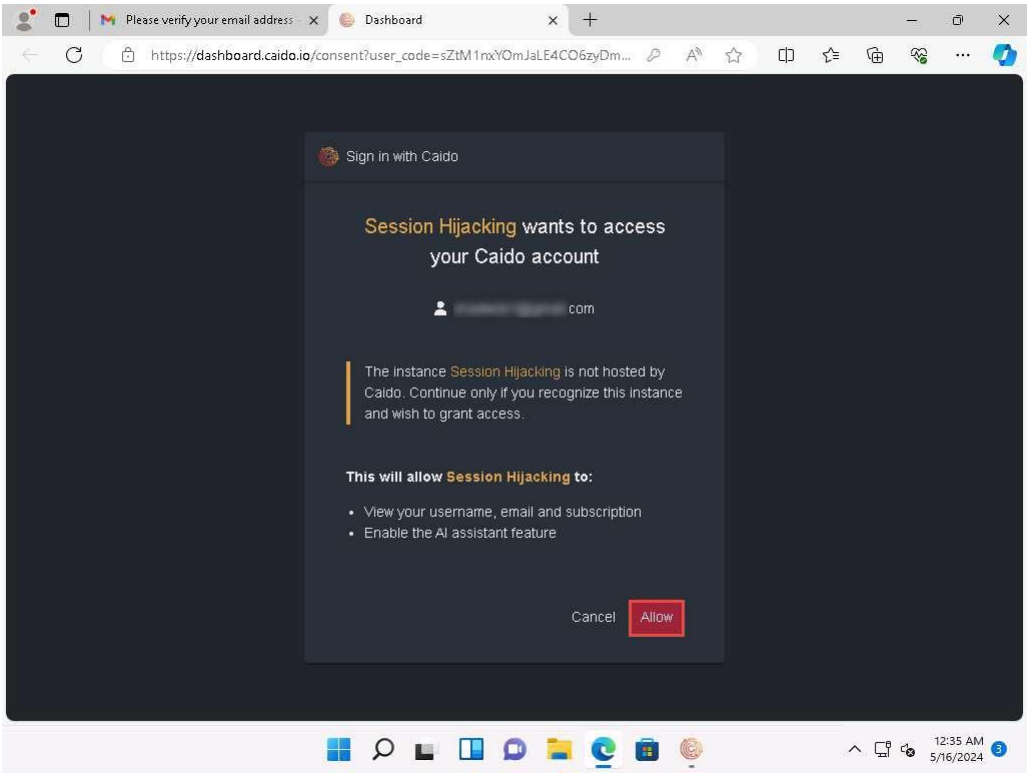
13. **Welcome to Caido** page will appear, enter your credentials and click **Login**.

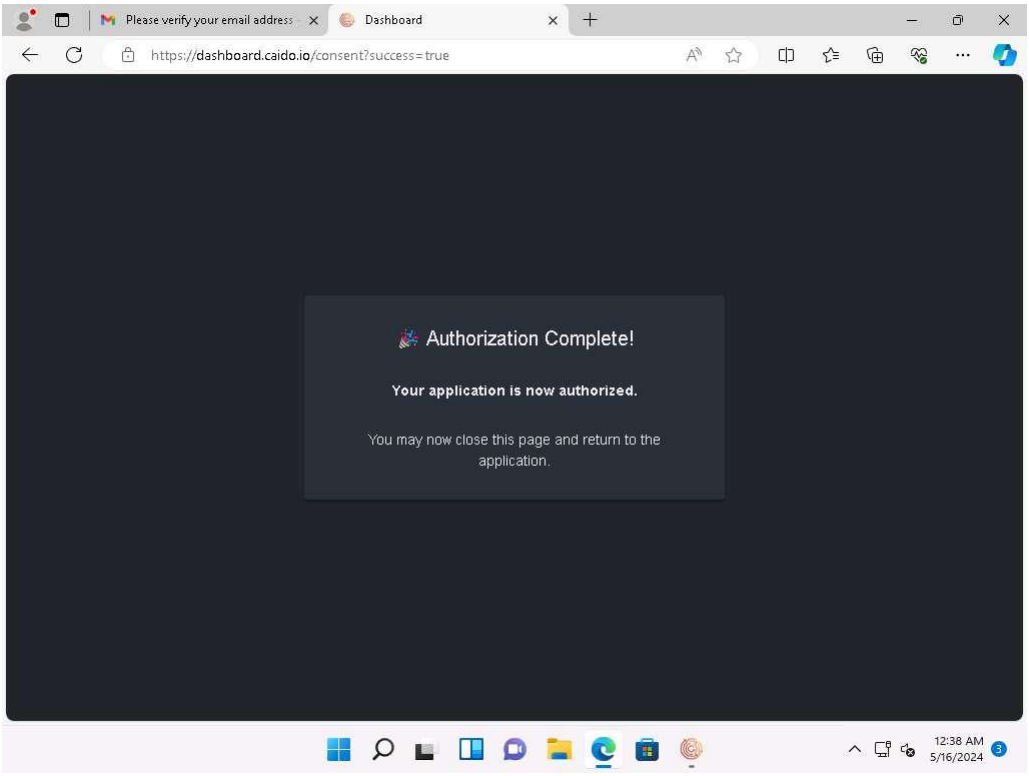


14. Once logged in, **Register your Caido Instance** pop-up will appear. Type **Session Hijacking** and click **Register**.



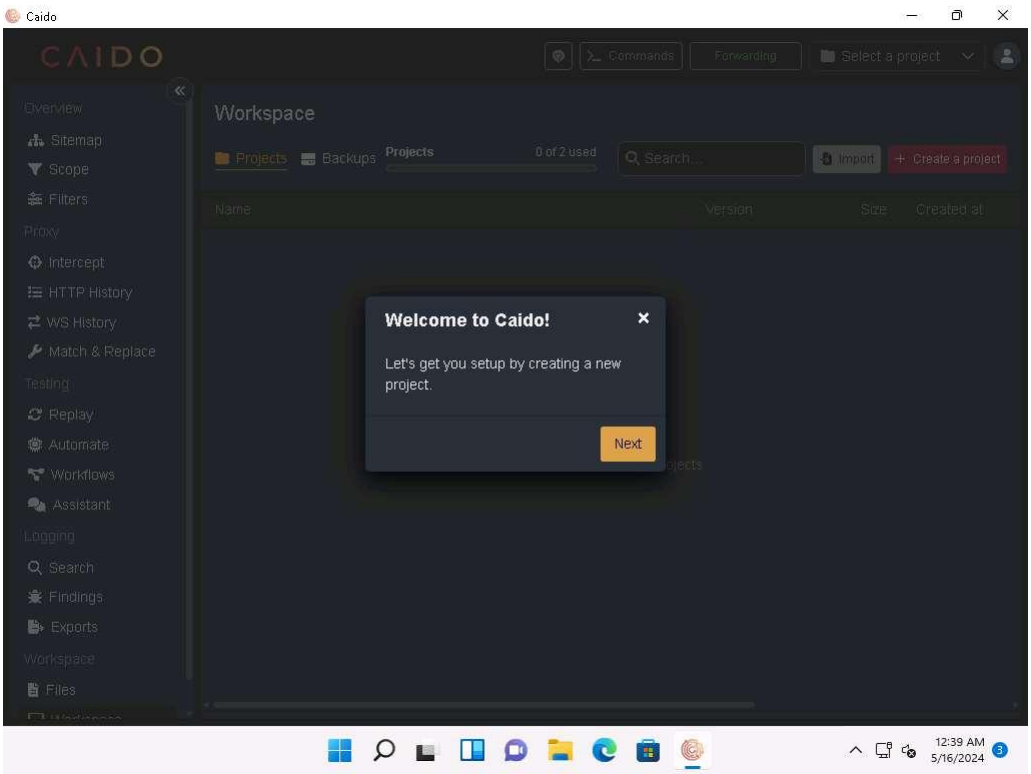
15. **Sign in with Caido** window appears, click **Allow** to allow the access. **Authorization Complete!** pop-up appears, close the web browser and return to the application.



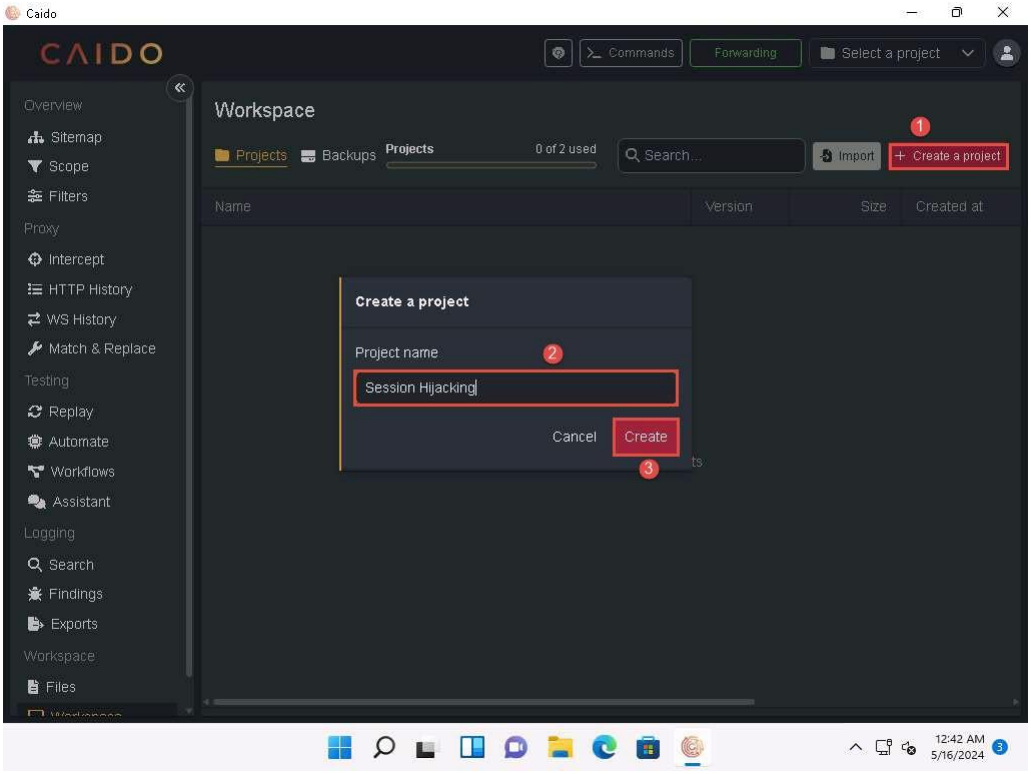


16. The **Caido** main window appears.

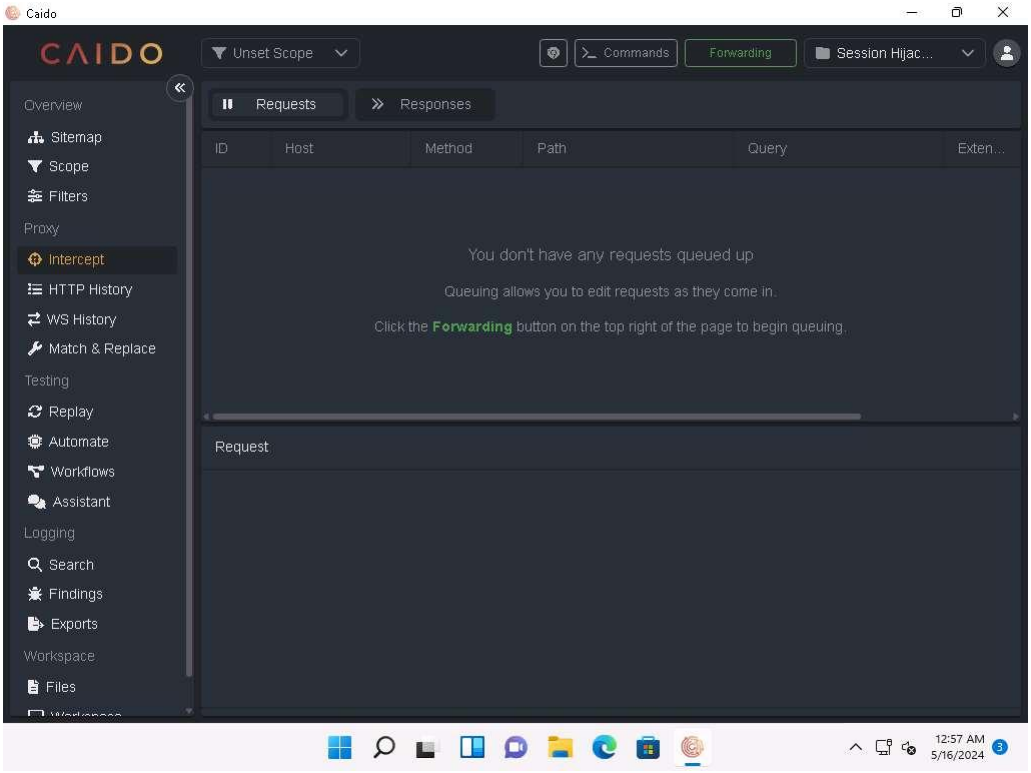
    If a Caido pop-up appears, click **Next** or **Ok** in all the pop-ups.



17. Click on **+ Create a project** button to create a new project. **Create a project** pop-up appears, name it as **Session Hijacking** and click **Create**.

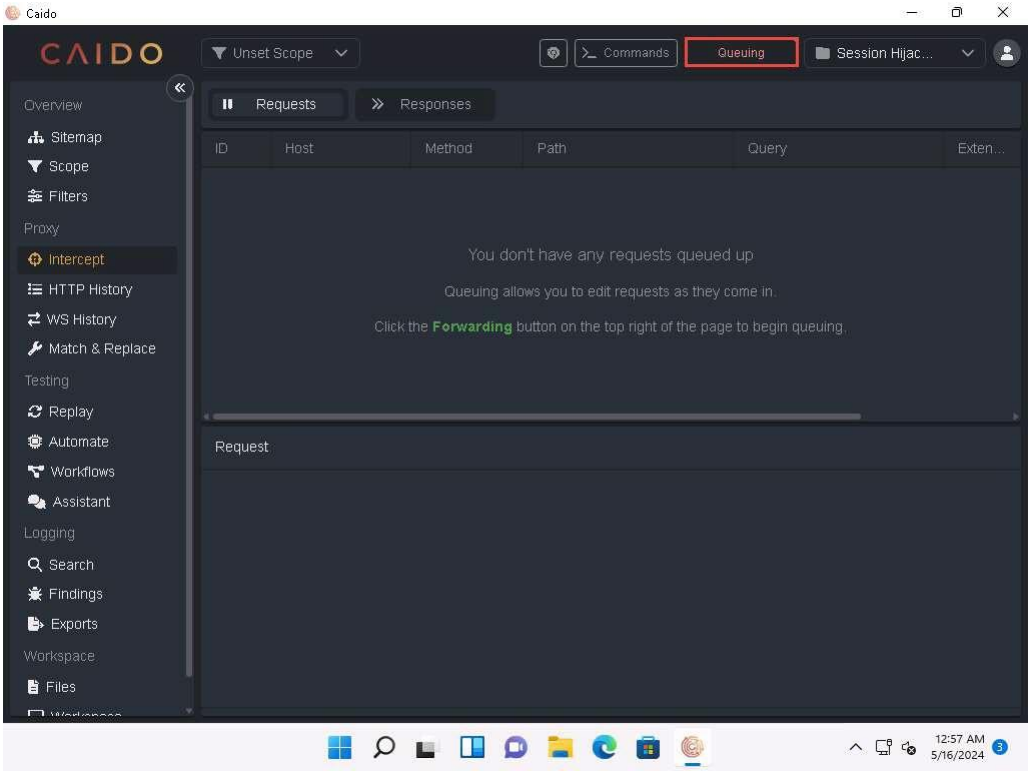


18. Click on **Intercept** option on the left pane, as shown in the screenshot below.



19. Click the **Forwarding** icon and wait until it changes to **Queuing**. This button will trap and display the next response or request from the victim's machine in the **Intercept** tab.

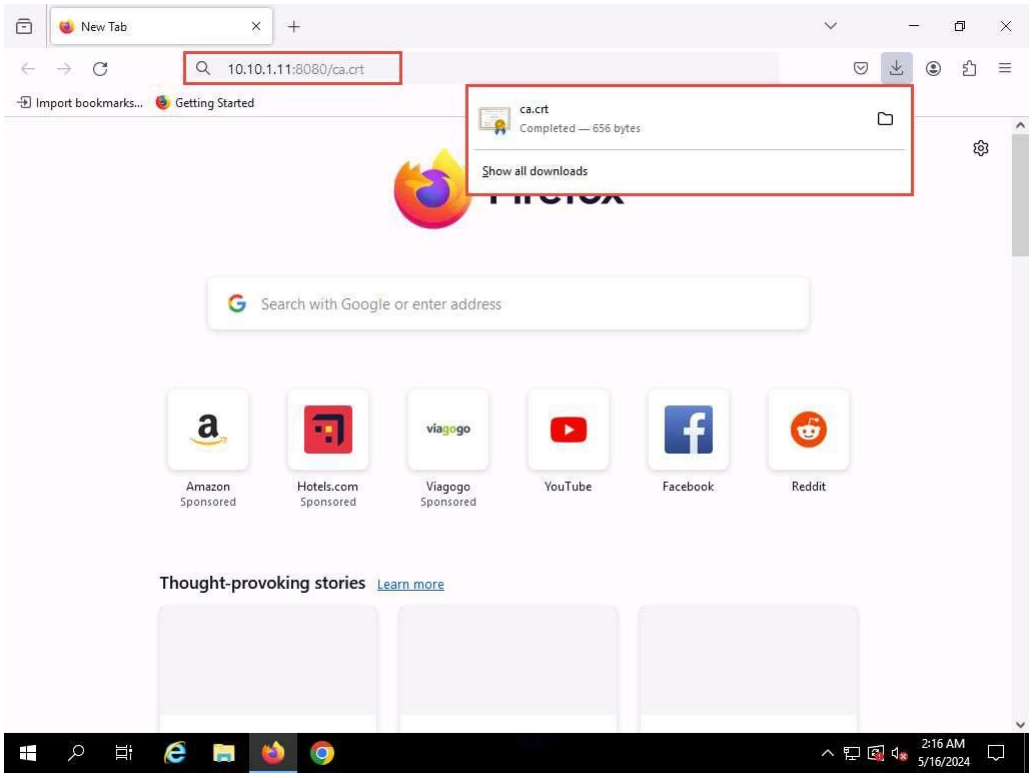
The **Forwarding** icon turns automatically from green to red.



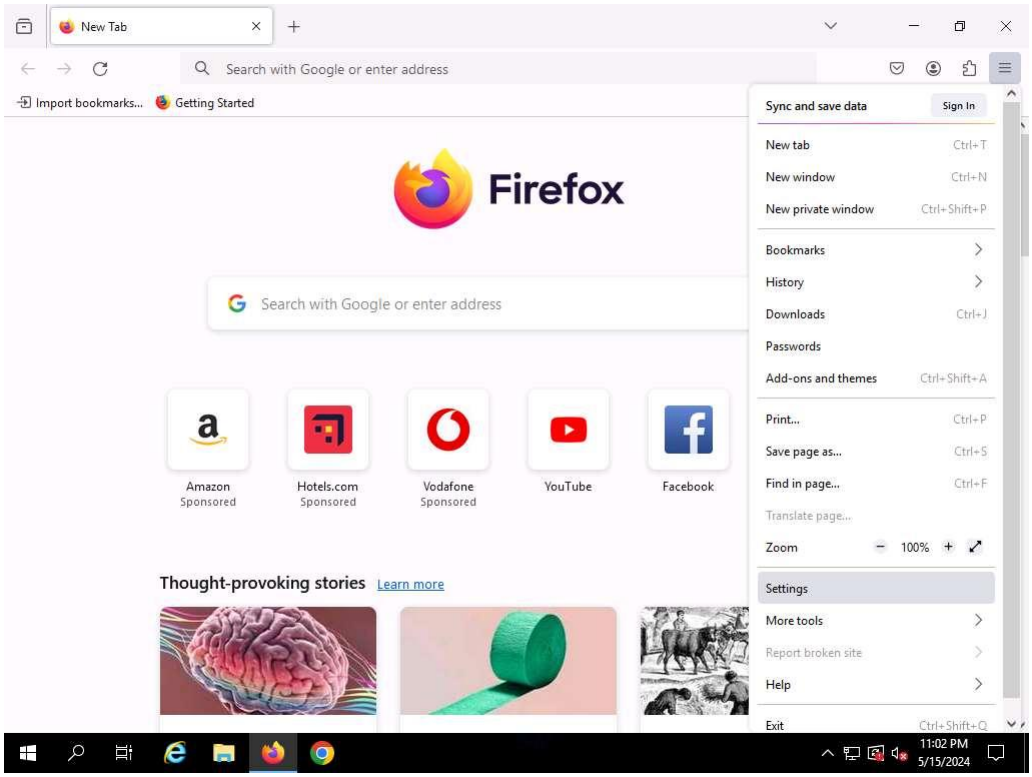
20. Click Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine and login using **Administrator**/**Pa$$w0rd**.

    Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

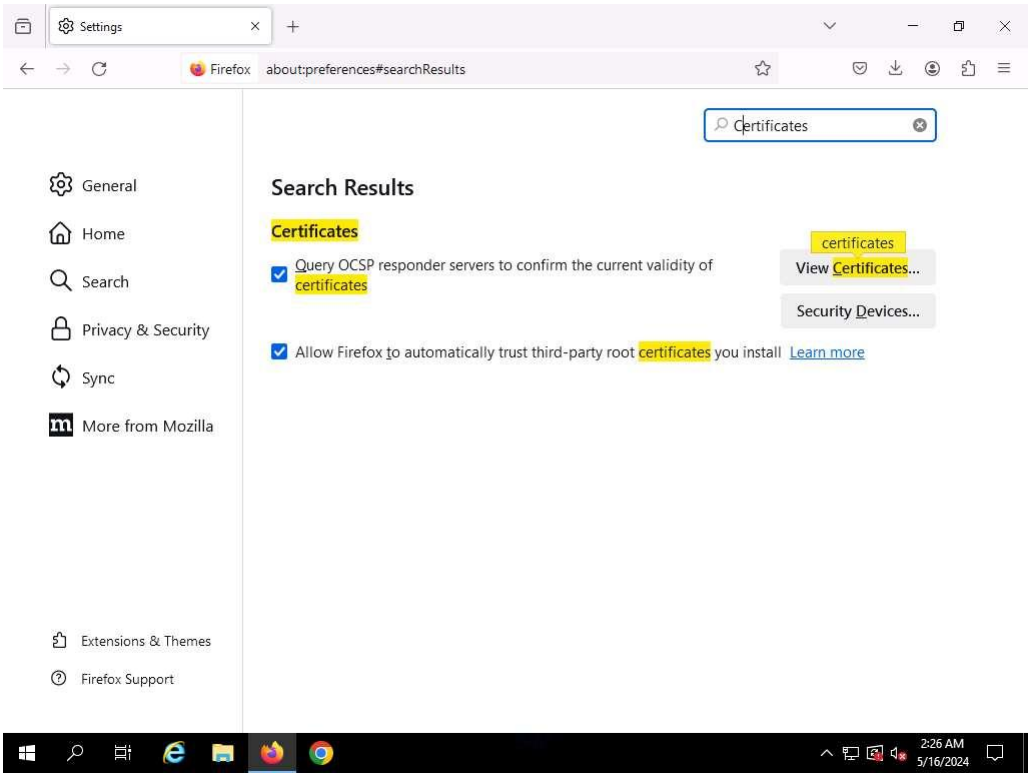
21. Open **Firefox** web browser and navigate to **http://10.10.1.11:8080/ca.crt**. CA certificate will be downloaded automatically as shown in the screenshot.



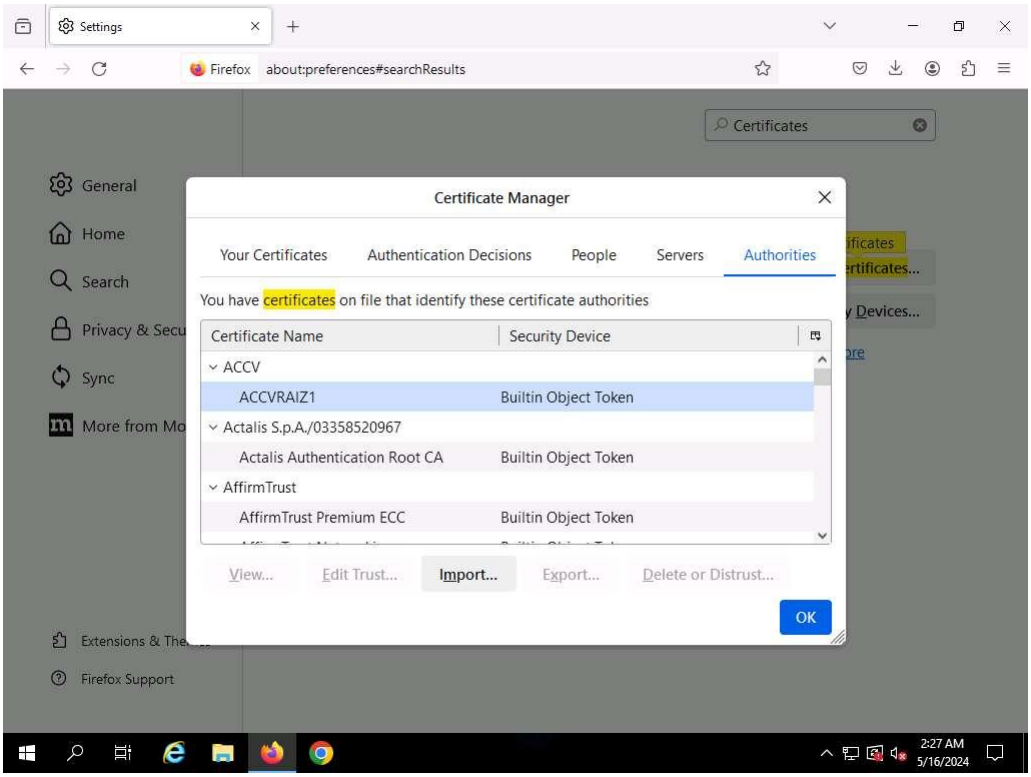
22. In **Firefox** web browser, select **Settings** from the context menu.



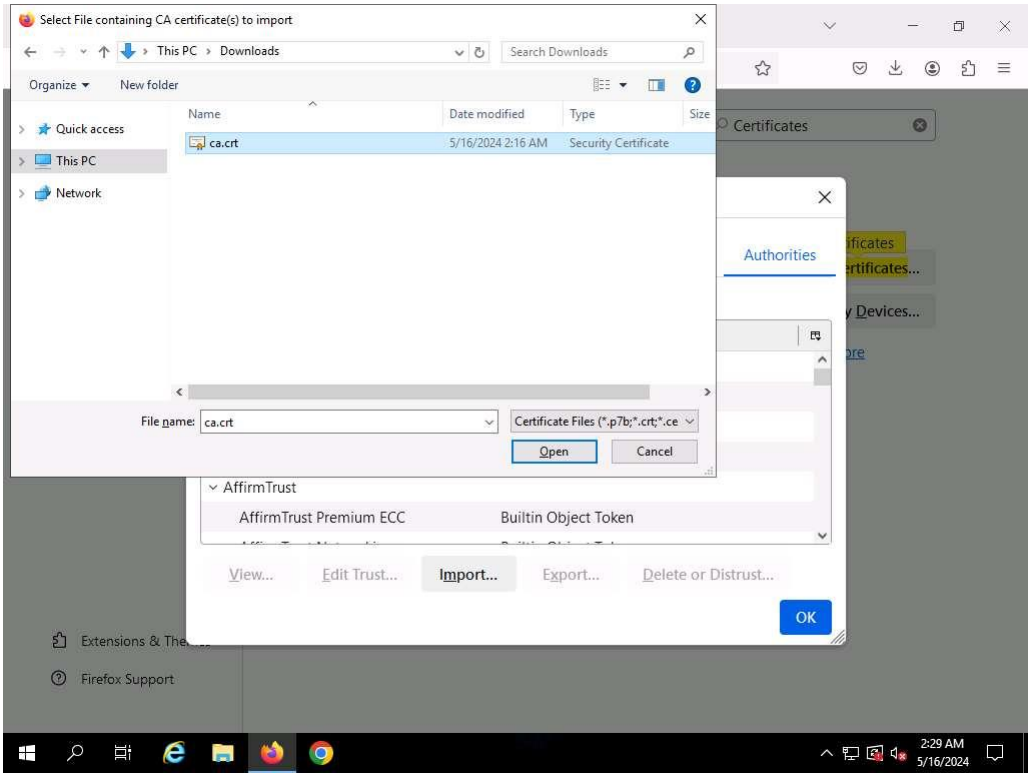
23. On the **Settings** page, search for **Certificates** and open **View Certificates**.



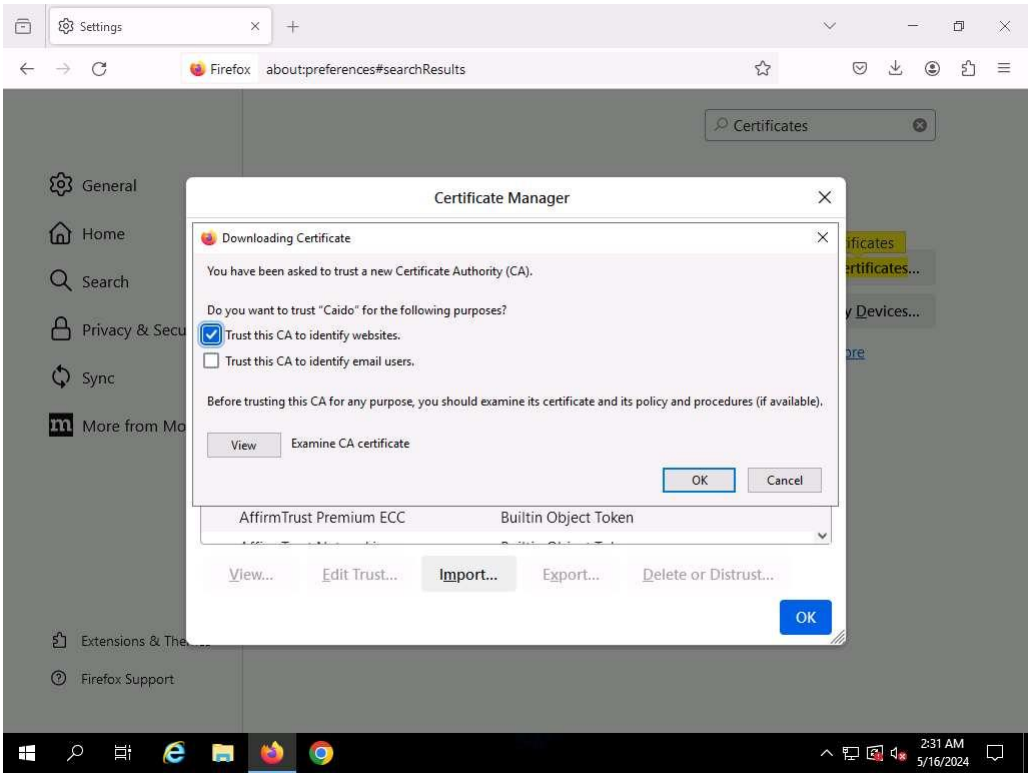
24. Navigate to **Authorities** tab and click on **Import…**



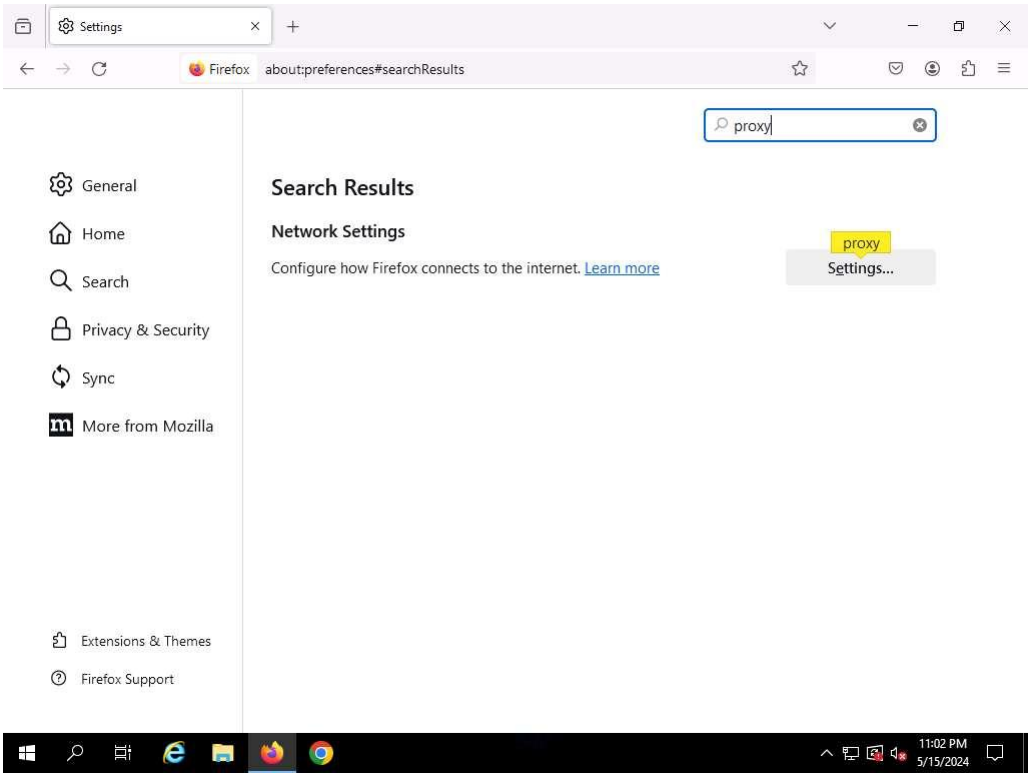
25. In **Select File containing CA certificate(s) to import** window, select the recently downloaded **ca.crt** file and click **Open**.



26. When prompted, click the **Trust this CA to identify websites** checkbox and click on **OK**. Click **OK** in the **Certificate Manager** window.

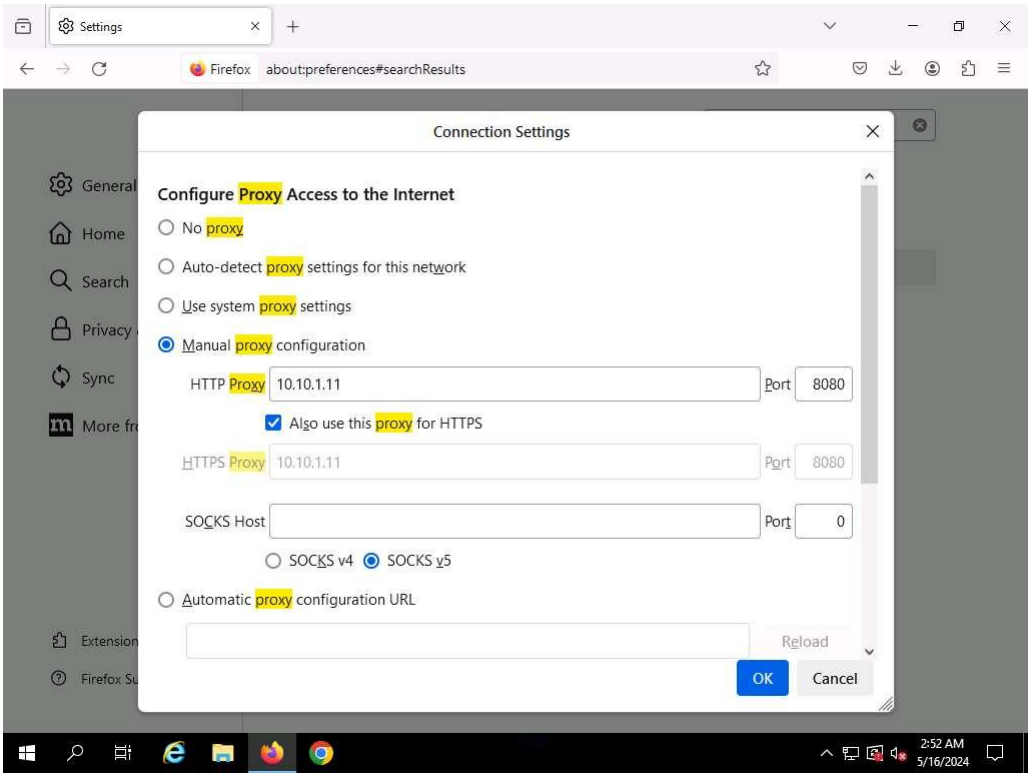


27. On the **Settings** page, search for **proxy** and open it.



28. **Connection Settings** page appears and click **Manual proxy configuration** to configure a proxy.

29. Set HTTP Proxy to **10.10.1.11** and port to **8080**, check the **Also use this proxy for HTTPS** box and click **OK**.



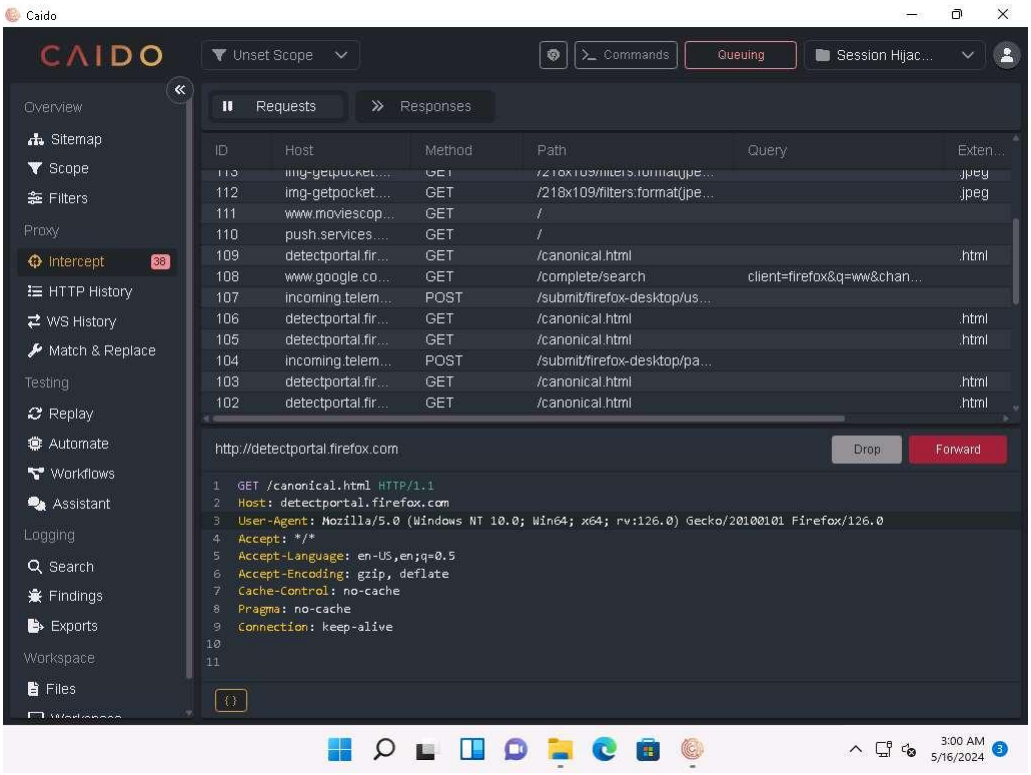
30. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.

31. Open a new tab in **Firefox** web browser and place your mouse cursor in the address bar, type **www.moviescope.com** and press **Enter**.

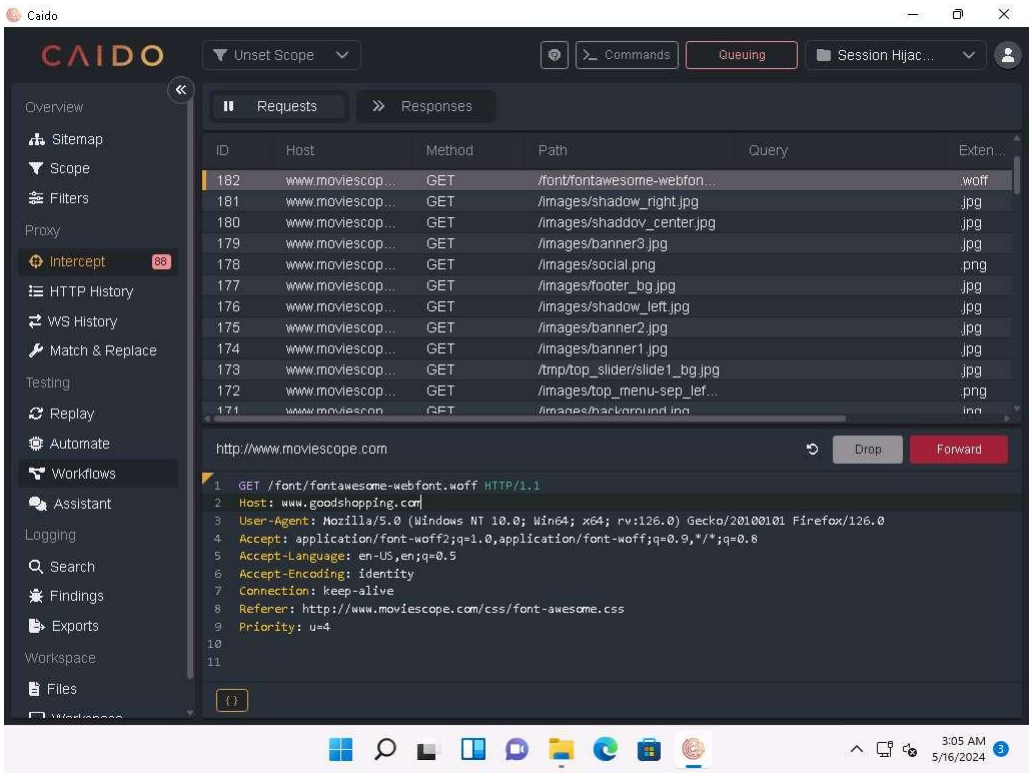
32. If a message appears, stating that **Your connection is not private**. Click the **Advanced** button.

33. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.

34. Now, click Windows 11 to switch back to the attacker machine (**Windows 11**) and observe that **Caido** has begun to capture the requests of the victim's machine.



35. On the **Requests** tab, for all www.moviescope.com requests, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET **requests** and **Forward** all the requests.

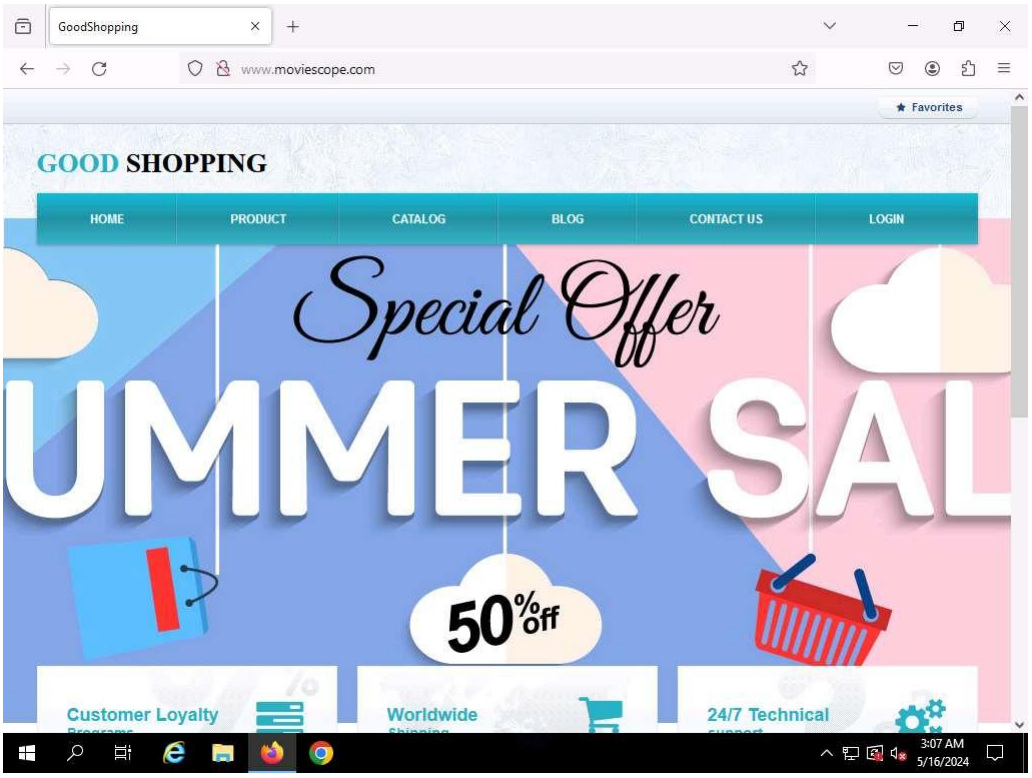


36. In a similar way, modify every **GET** request captured by **Caido** until you see the **www.goodshopping.com** page in the victim's machine. You will need to switch back and forth from the victim's machine to see the browser status while you do this.

    If you do not receive any request or you see a blank Requests tab then switch to **Windows Server 2019** machine and refresh the browser to capture the request again.

37. Now, click on Windows Server 2019 to switch to the victim's machine (**Windows Server 2019**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

38. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www.moviescope.com**, the window displays **www.goodshopping.com**.



39. Now, we shall change the proxy settings back to the default settings. To do so, in the **Firefox** browser, select **Settings** from the context menu. On the **Settings** page, search for **proxy** and open it. **Connection Settings** page appears, check **No Proxy** radio button and click **OK**.

40. This concludes the demonstration of performing session hijacking using Caido.

41. Close all open windows and document all the acquired information.

Question 11.1.1.1

Use Caido tool on the attacker machine (10.10.1.11) to hijack a session established when a user on the victim machine (10.10.1.19) visits the website www.moviescope.com and redirect to www.goodshopping.com using the Firefox browser. Under which section does the Responses tab is located.

Task 2: Intercept HTTP Traffic using Hetty

Hetty is an HTTP toolkit for security research. It aims to become an open-source alternative to commercial software such as Burp Suite Pro, with powerful features tailored to the needs of the InfoSec and bug bounty communities. Hetty can be used to perform Machine-in-the-

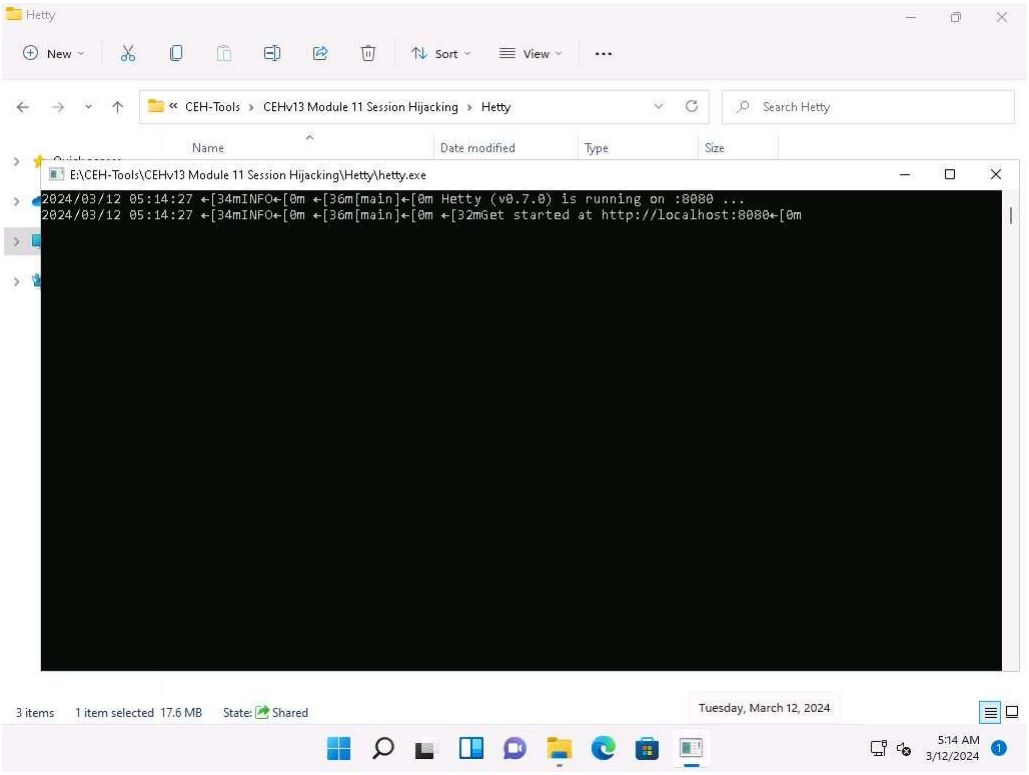
middle (MITM) attack, manually create/edit requests, and replay proxied requests for HTTP clients and further intercept requests and responses for manual review.

Here, we will use the Hetty tool to intercept HTTP traffic on the target system.

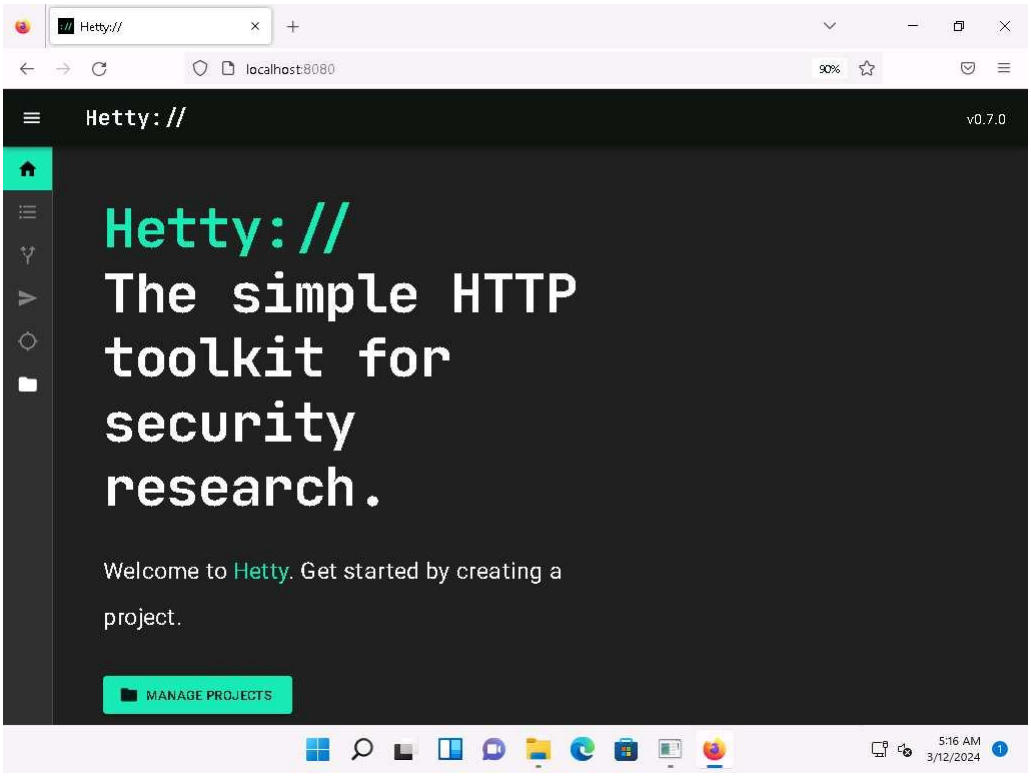
Here, we will use **Windows 11** machine as an attacker machine and **Windows Server 2022** machine as a target machine.

1. Click Windows 11 to switch to the **Windows 11** machine.
2. Navigate to **E:\CEH-Tools\CEHv13 Module 11 Session Hijacking\Hetty** and double-click **hetty.exe**.

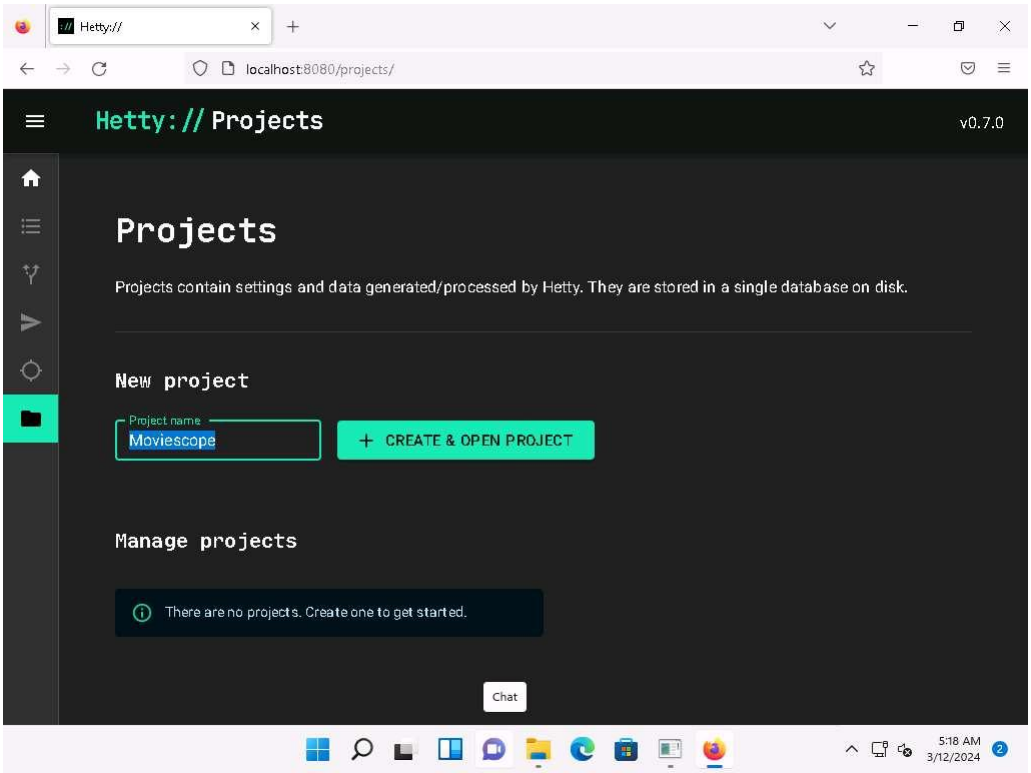
   If an **Open File - Security Warning** window appears, click **Run**.
3. A **Command Prompt** window appears, and Hetty initializes.



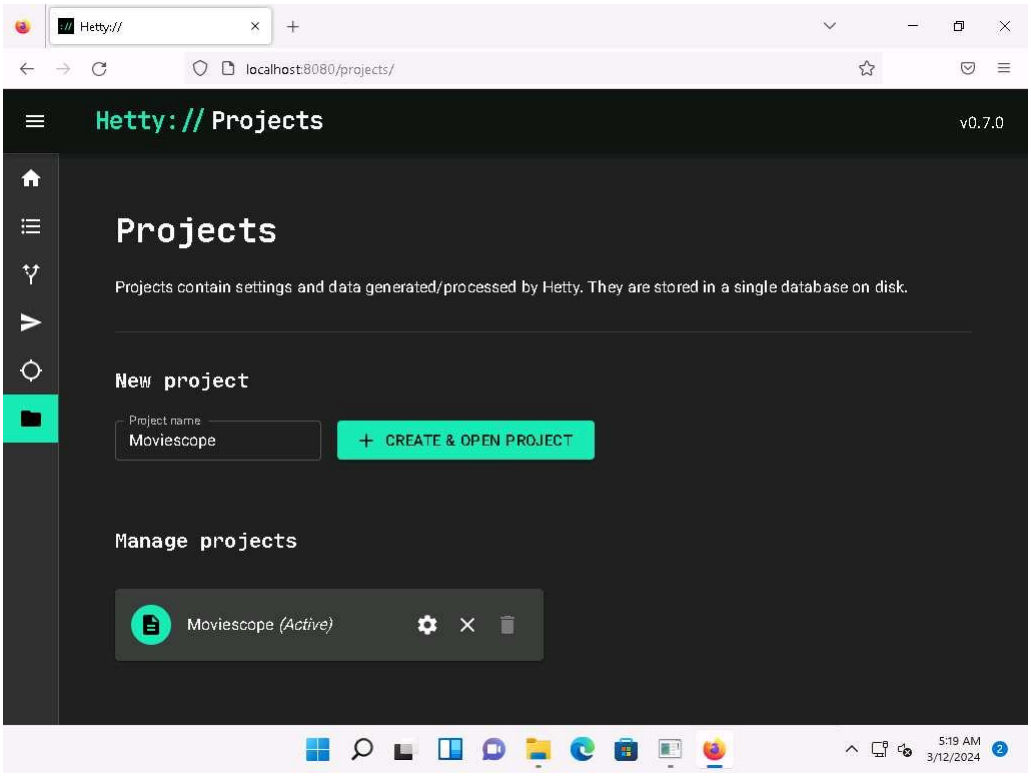
4. Now, minimize all the windows and launch any web browser (here, **Mozilla Firefox**). Go to **http://localhost:8080** to open Hetty dashboard.
5. In the Hetty dashboard, click **MANAGE PROJECTS** button.



6. **Projects** page appears, type **Project name** as **Moviescope** and click + **CREATE & OPEN PROJECT** button.

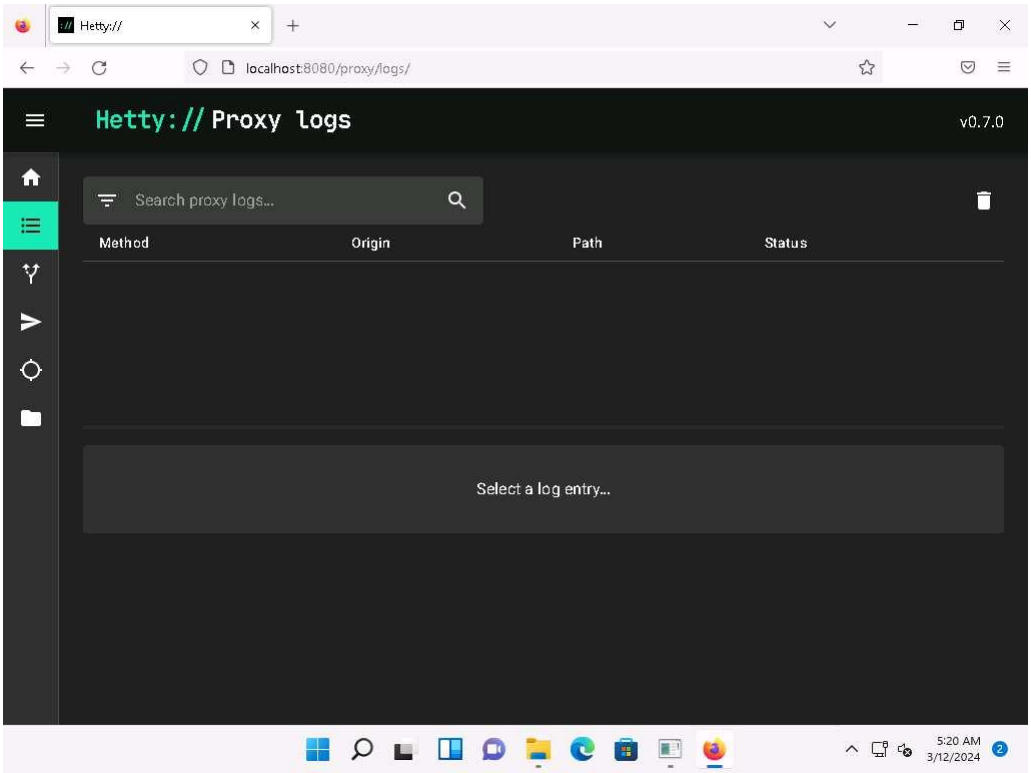


7. You can observe that a new project name **Moviescope** has been created under **Manage projects** section with a status as **Active**.



8. Click **Proxy logs** icon ( ) from the left-pane.

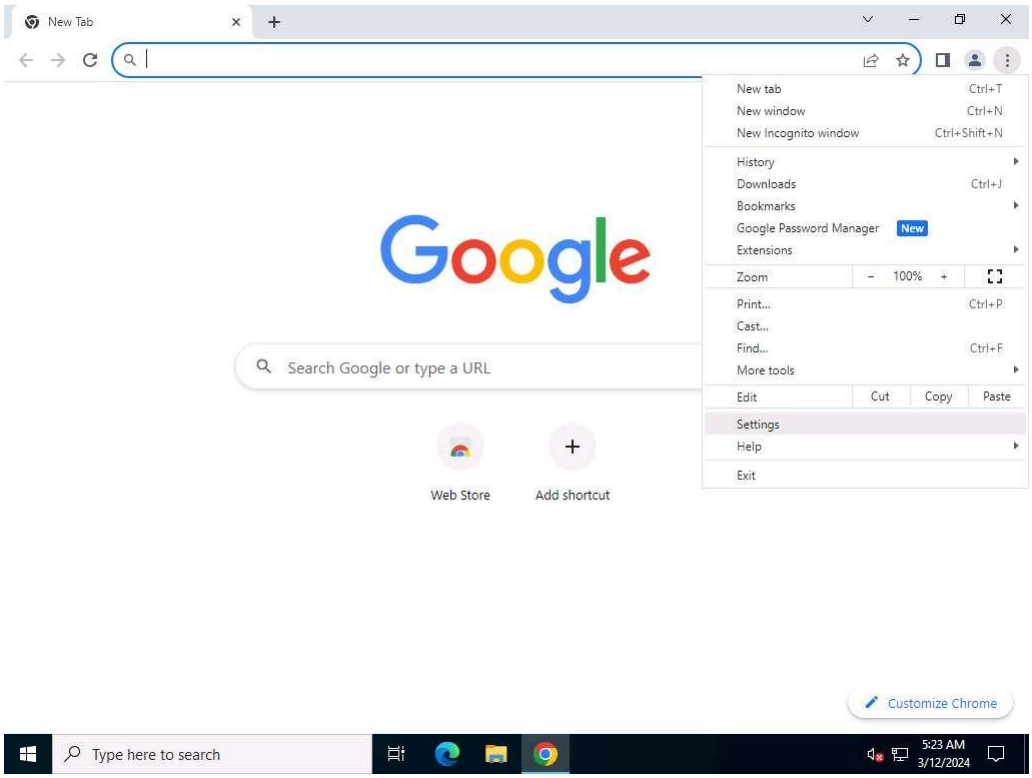
9. A **Proxy logs** page appears, as shown in the screenshot.



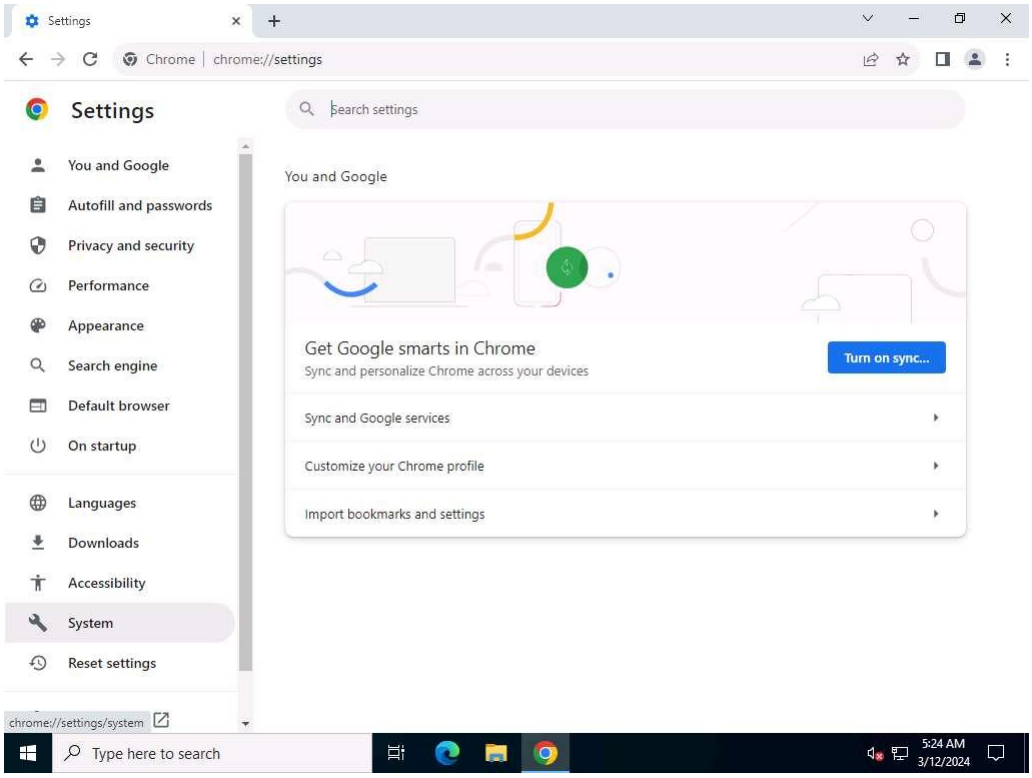
10. Now, click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine and login using **Administrator/Pa$$w0rd**.

    Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

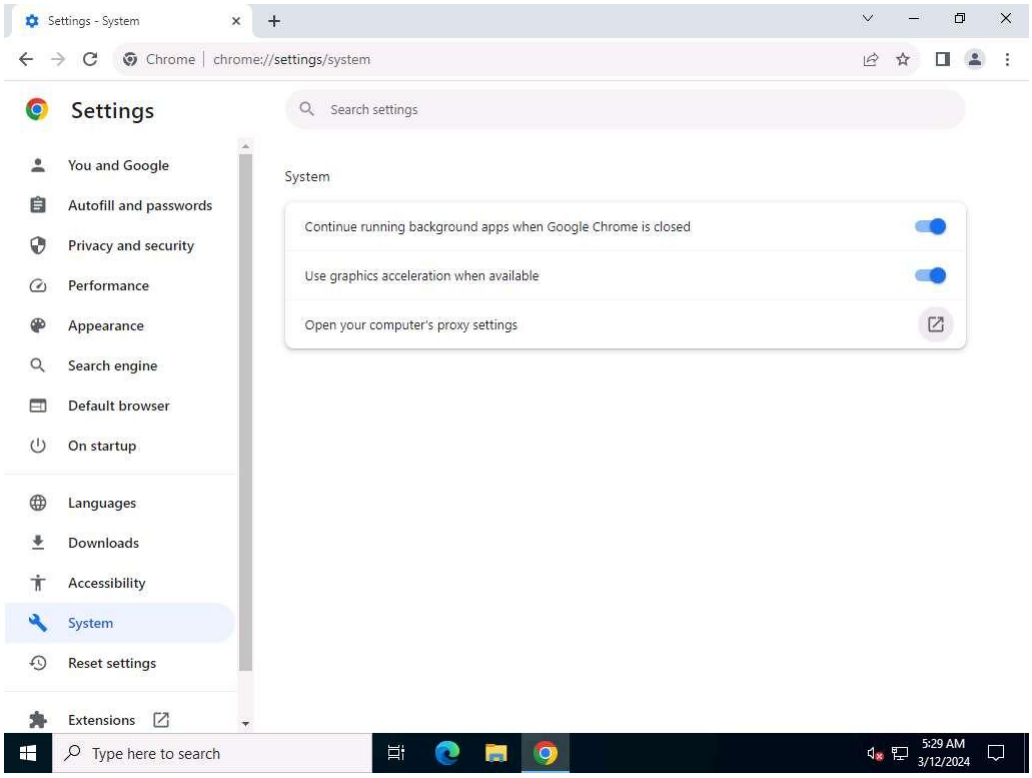
11. Open **Google Chrome** web browser, click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



12. On the **Settings** page, scroll-down and click **System** in the left-pane.



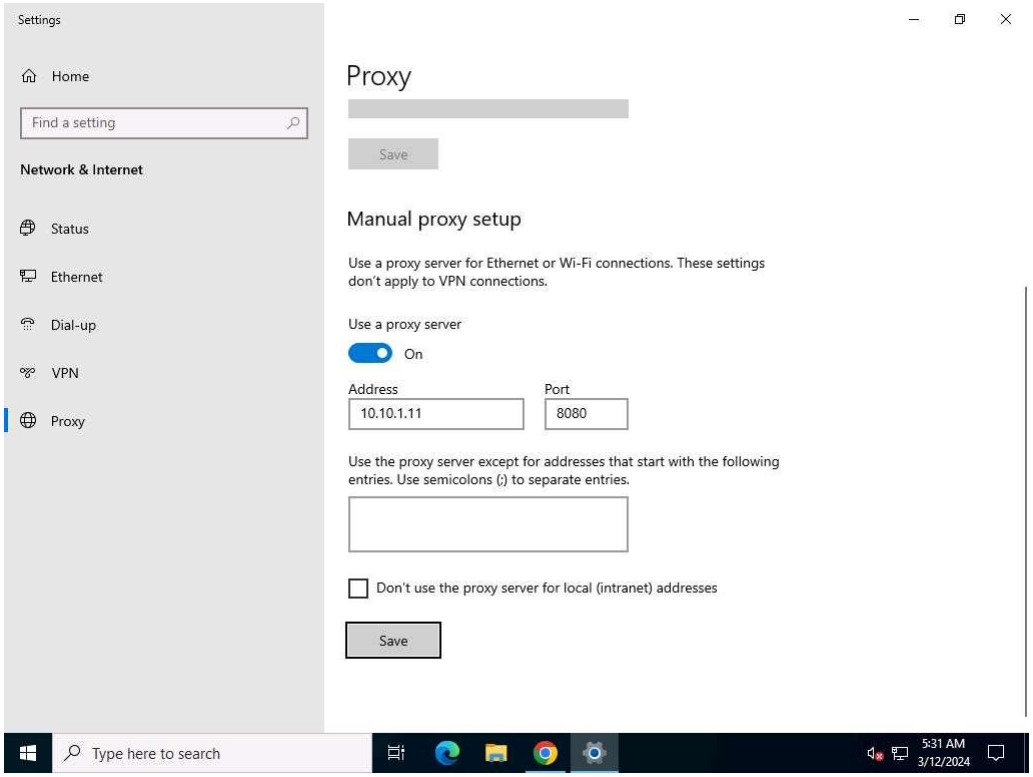
13. Scroll-down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.



14. A **Settings** window appears, with the **Proxy** settings in the right pane.

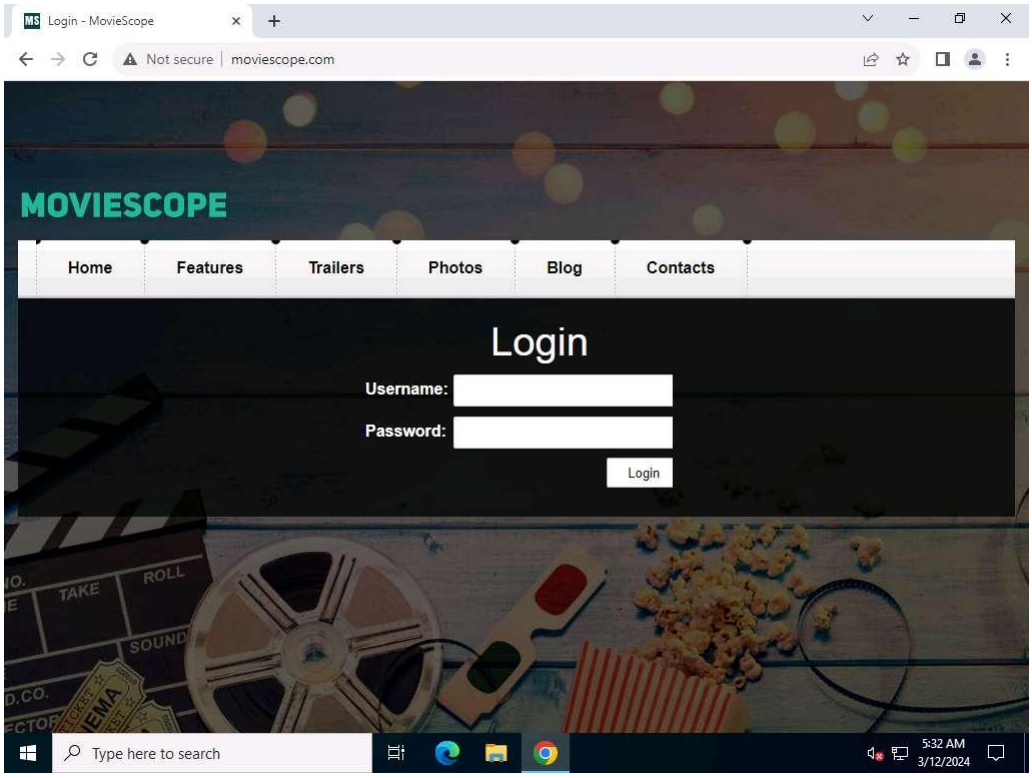
15. In the **Manual proxy setup** section, make the following changes:

- Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
- In the **Address** field, type **10.10.1.11** (the IP address of the attacker's machine, here, **Windows 11**).
- In the **Port** field, type **8080**.
- Click **Save**.



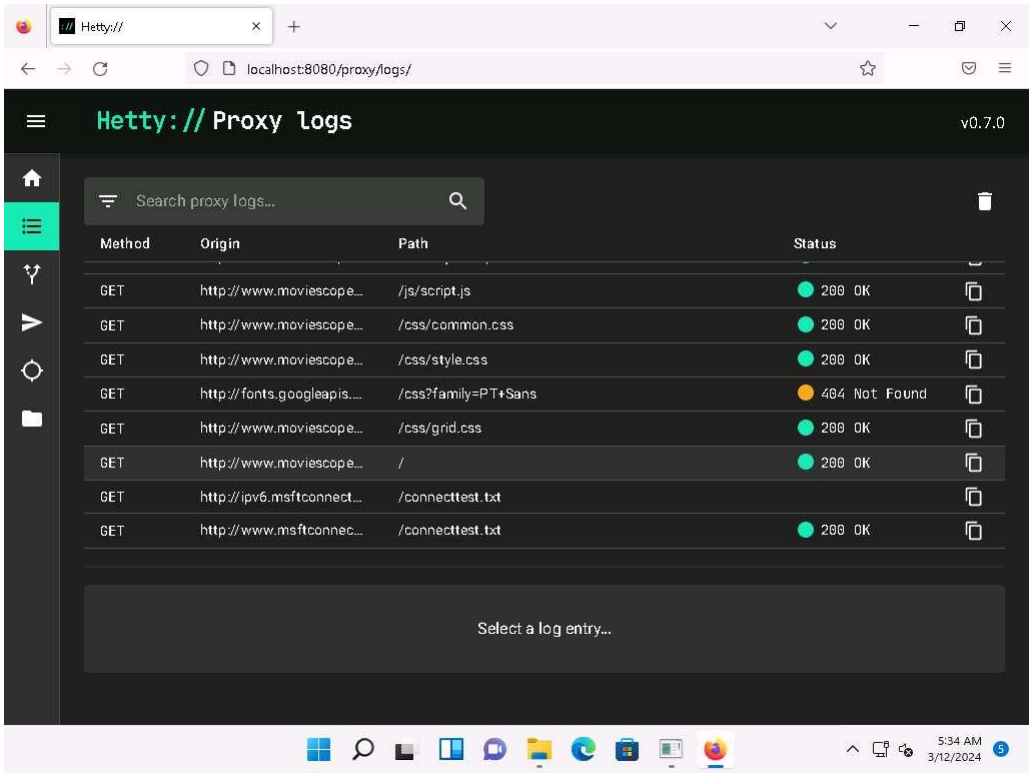
16. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.

17. Now, in the web browser go to **http://www.moviescope.com**.



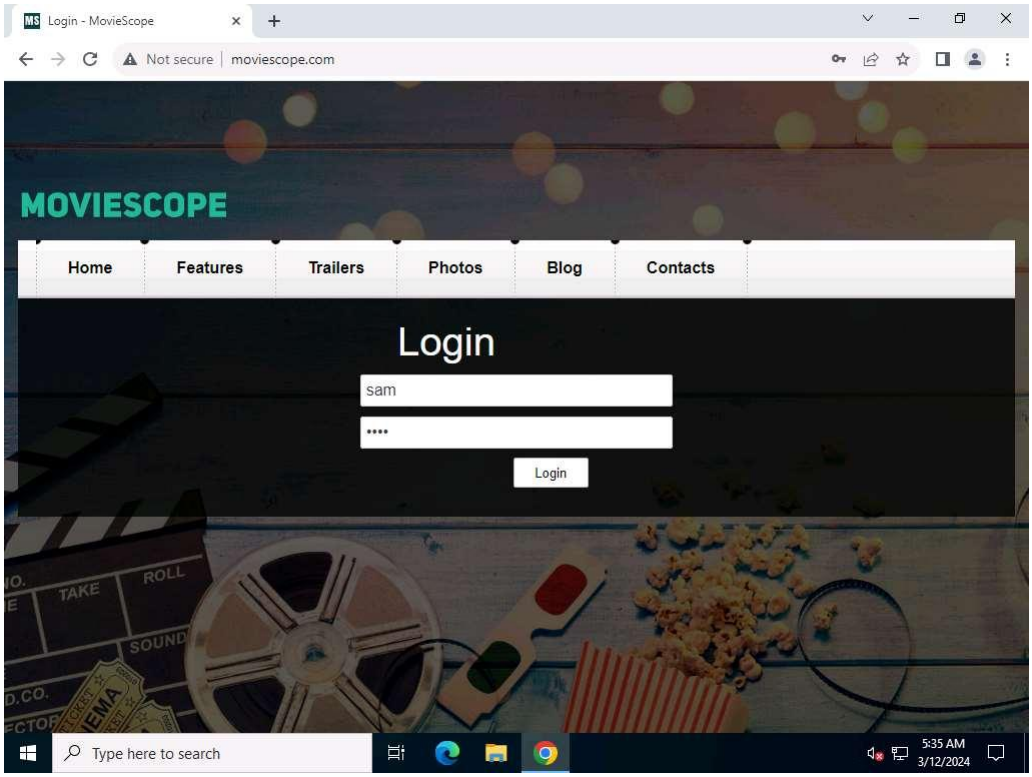
18. Click Windows 11 to switch to the **Windows 11** machine.

19. You can observe that the logs are captured in the **Proxy logs** page. Here, we are focusing on logs associated with moviescope.com website.



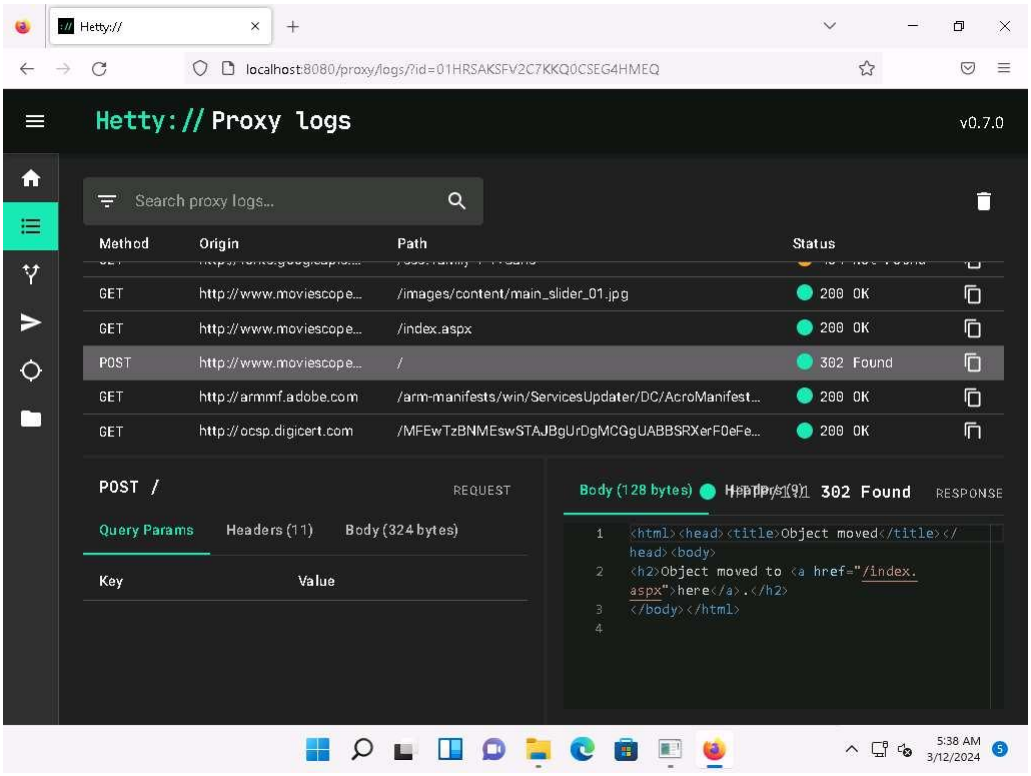
20. Click Windows Server 2022 to switch back to the **Windows Server 2022** machine.

21. In the **MovieScope** website, login as a victim with credentials as **sam**/**test**.



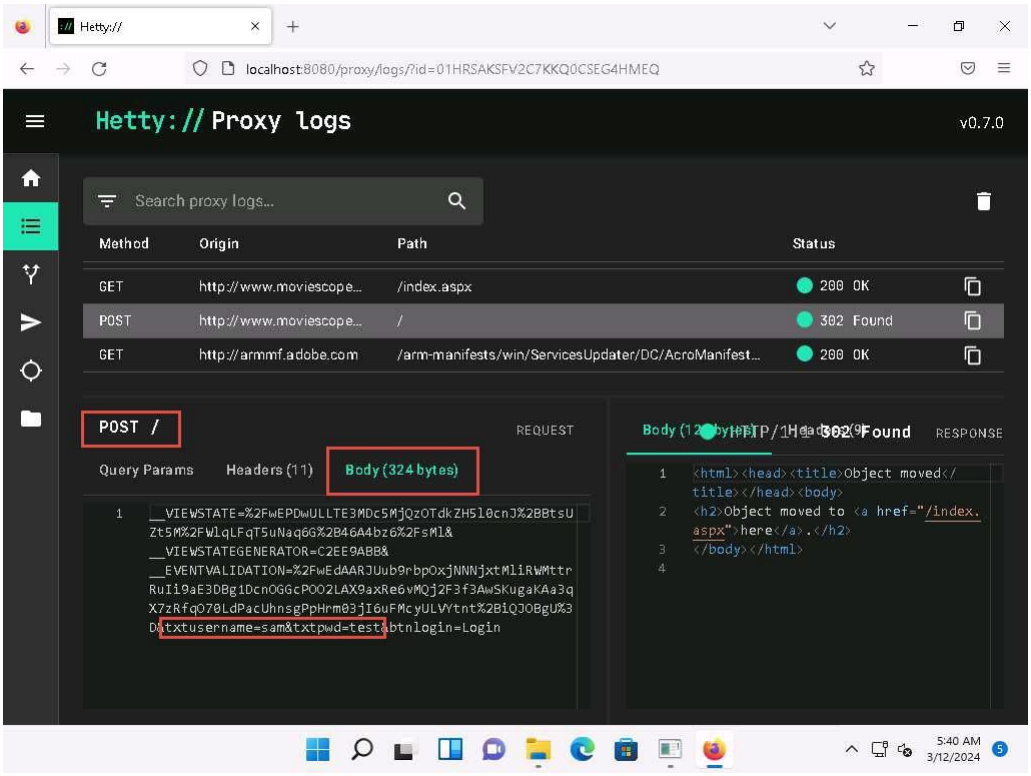
22. Now, click Windows 11 to switch to the **Windows 11** machine.

23. In the **Proxy logs** page, scroll-down to check more logs on moviescope website. Check for **POST** log captured for the target website.



24. Select the **POST request** and in the lower section of the page, select **Body** tab under **POST** section.

25. Under the **Body** tab, you can observe the captured user credentials, as shown in the screenshot.

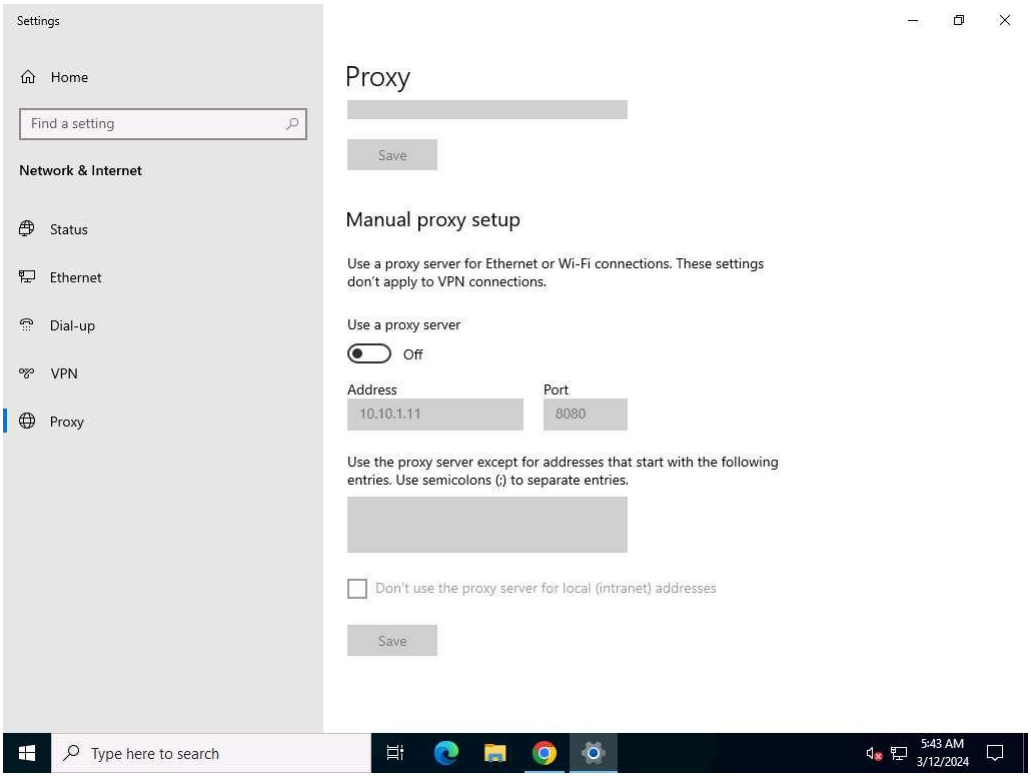


26. The captured credentials can be used to log in to the target user's account and obtain further sensitive information.

27. Now, we shall change the proxy settings back to the default settings. To do so, click Windows Server 2022 to switch back to the **Windows Server 2022** machine and perform **Steps 13-15** again.

    If you are logged out of the **Windows Server 2022** machine, click Ctrl+Alt+Delete, then login using **CEH\Administrator** / **Pa$$w0rd**.

28. In the **Settings** window, under the **Manual proxy setup** section in the right pane, click the **On** button to toggle it back to **Off**, as shown in the screenshot.



29. This concludes the demonstration of HTTP traffic interception using Hetty.

30. Close all open windows and document all the acquired information.

Question 11.1.2.1

Use the Hetty tool to intercept HTTP traffic on the Windows Server 2022 machine. Enter the url that was entered in the address bar of the browser to open Hetty dashboard.

Question 11.1.2.2

Use the Hetty tool to intercept HTTP traffic on the Windows Server 2022 machine. What was the password that was captured in Hetty tool by intercepting traffic of Windows Server 2022?

Lab 2: Detect Session Hijacking

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

As a professional ethical hacker or penetration tester, it is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect session hijacking using Wireshark

Overview of Detecting Session Hijacking

There are two primary methods that can be used to detect session hijacking:

- **Manual Method**: Involves using packet sniffing software such as Wireshark to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools
- **Automatic Method**: Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

Task 1: Detect Session Hijacking using Wireshark

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

We will use the **Parrot Security** (**10.10.1.13**) machine to carry out a session hijacking attack on the **Windows 11** (**10.10.1.11**) machine.

1. Click Windows 11 to switch to the **Windows 11** machine.

2. Click the windows **Search** icon on the **Desktop**, search for **Wireshark** in the search bar and launch it.

3. **The Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **Ethernet**).

4. Now, we shall launch a session hijacking attack on the target machine (**Windows 11**) using **bettercap**.

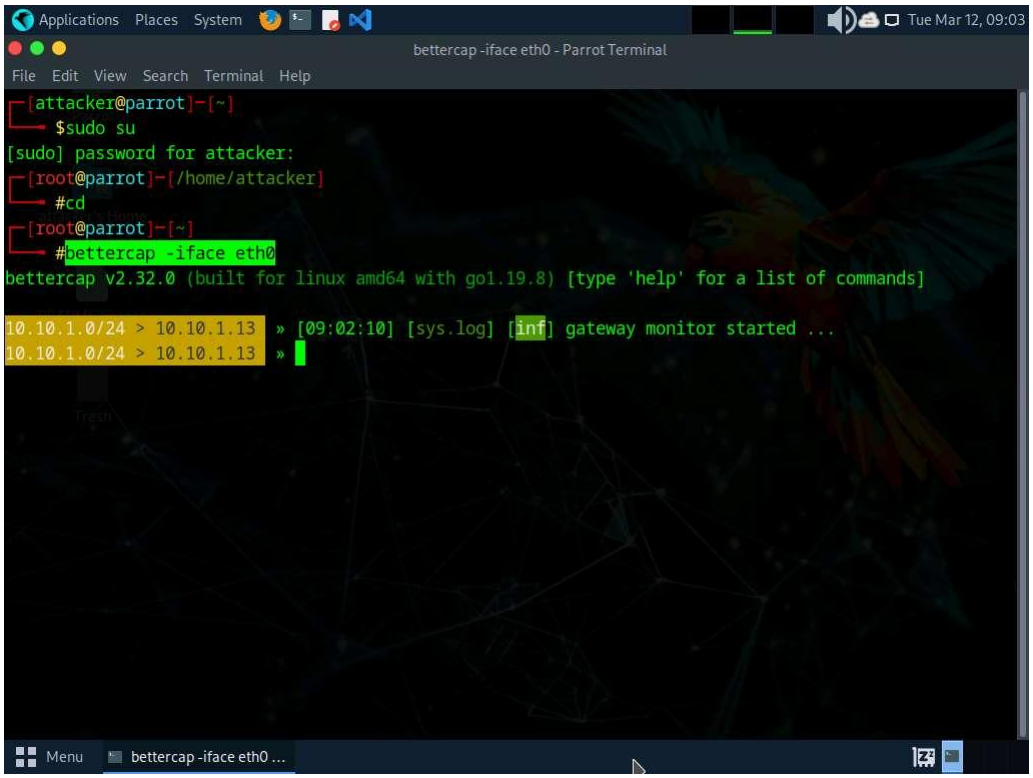
   To do so, you may either follow Steps **8-11** below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

5. Click Parrot Security to switch to the **Parrot Security** machine.

6. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** to jump to the root directory.

7. Run **bettercap -iface eth0** to set the network interface.

   -iface: specifies the interface to bind to (here, **eth0**).



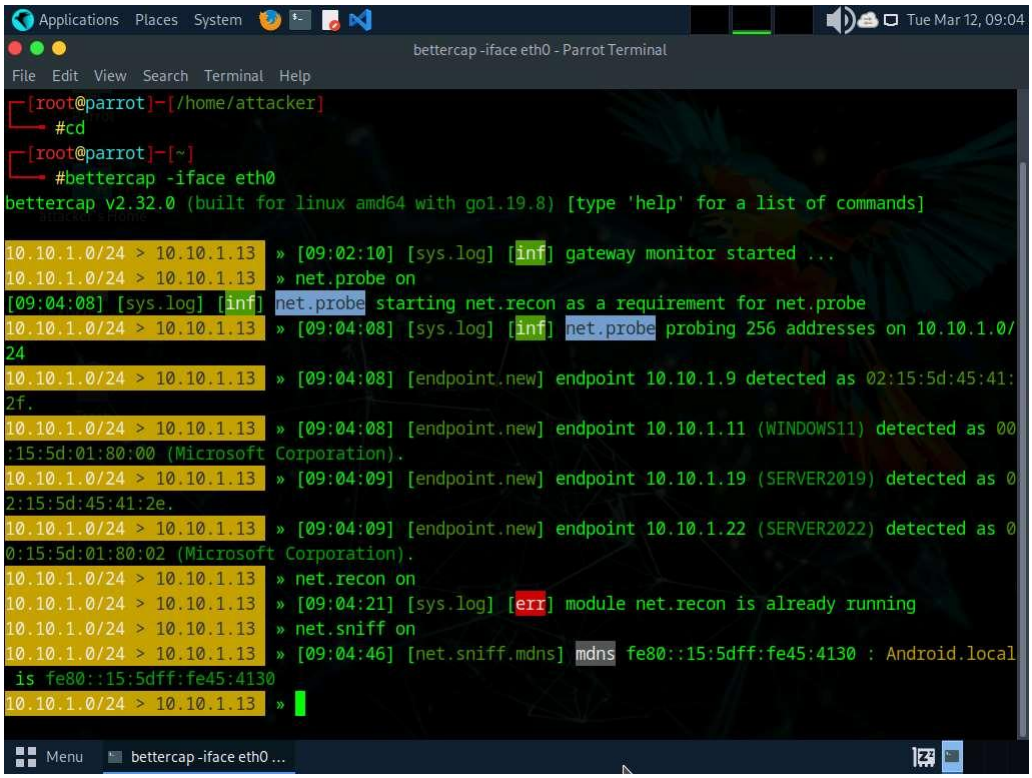
8. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.

9. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

10. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.

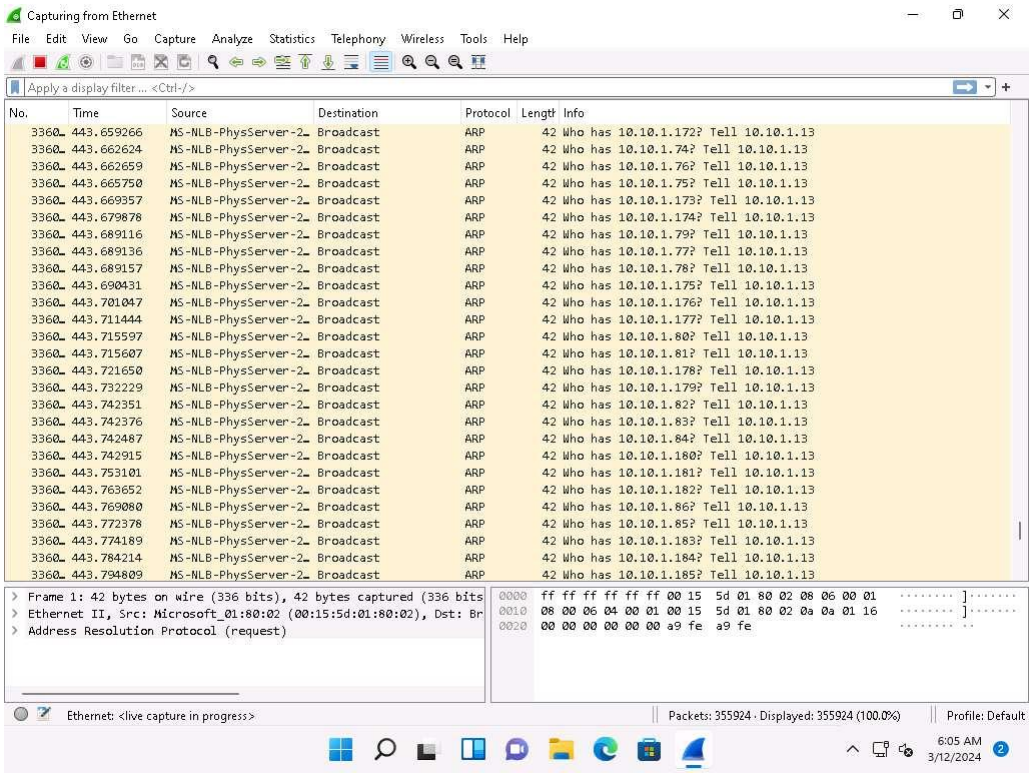
11. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.



12. Click Windows 11 to switch back to the **Windows 11** machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

    bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.1.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.1.11**) will first go to the host system (**10.10.1.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

    more...



13. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.

14. Close all open windows and document all the acquired information.

Question 11.2.1.1

Use the bettercap tool (available in the Parrot Security machine) to sniff the traffic on the target system (10.10.1.11). Use the Wireshark tool on the target system (10.10.1.11) to detect the session hijacking attempt. Traffic on which protocol indicates the session hijacking attempt in Wireshark?