# 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.

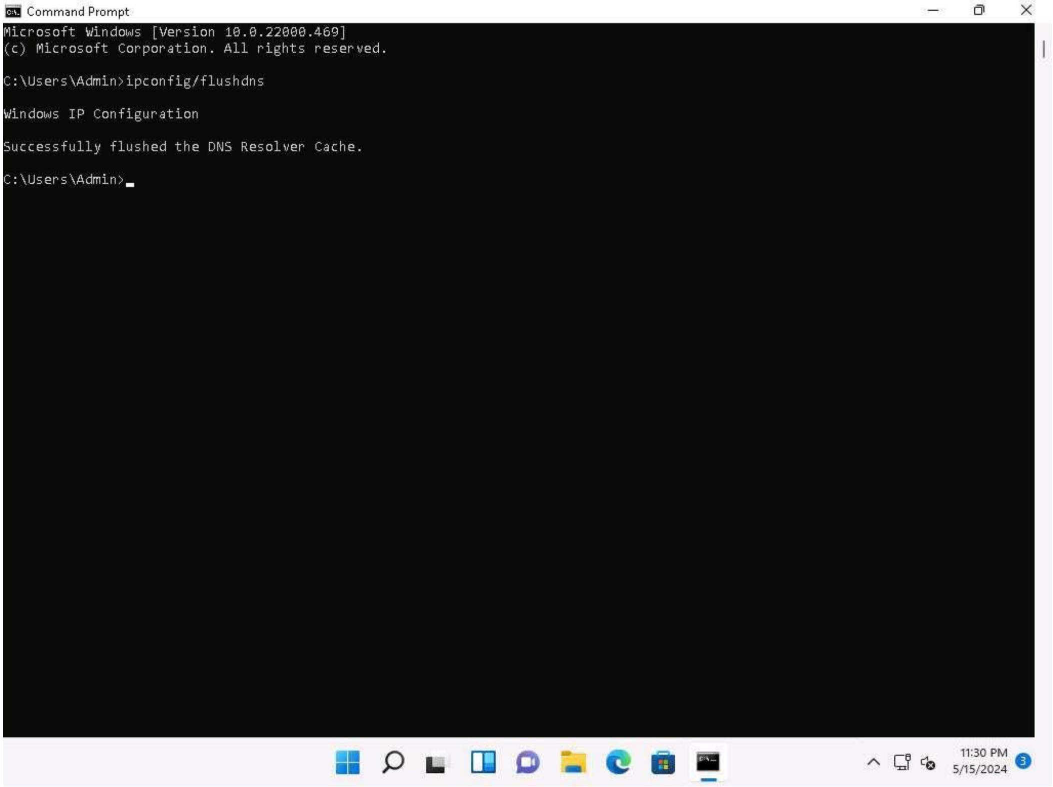
Here, we will use Caido to perform session hijacking on the target machine.

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.

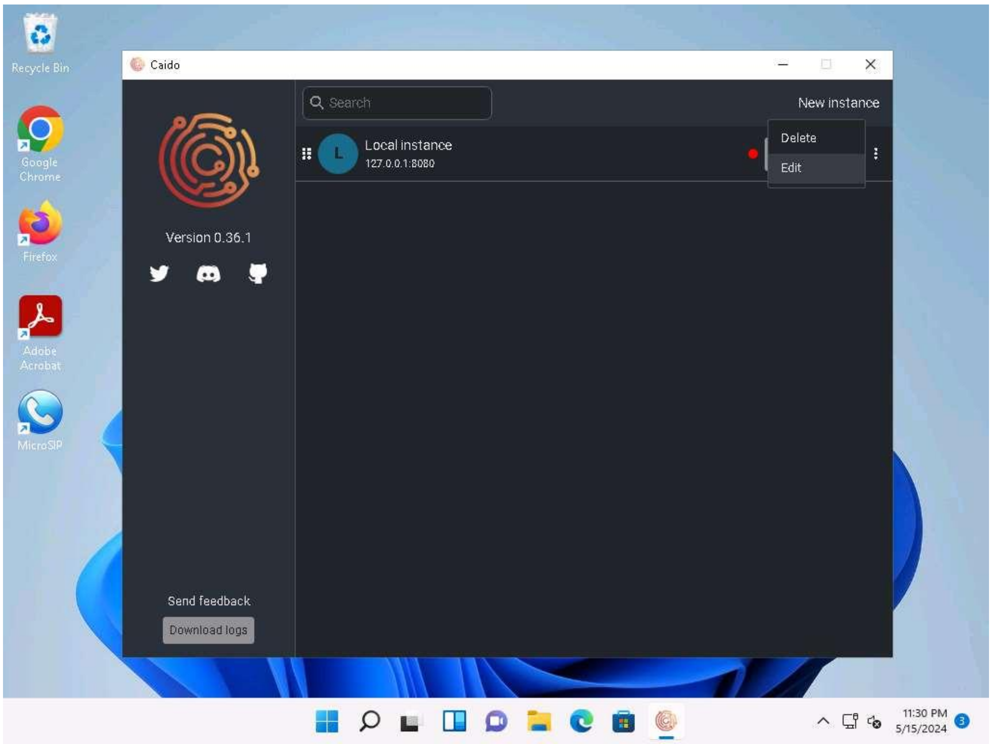
3. Run ipconfig/flushdns command to reset dns cache and close the Command Prompt.



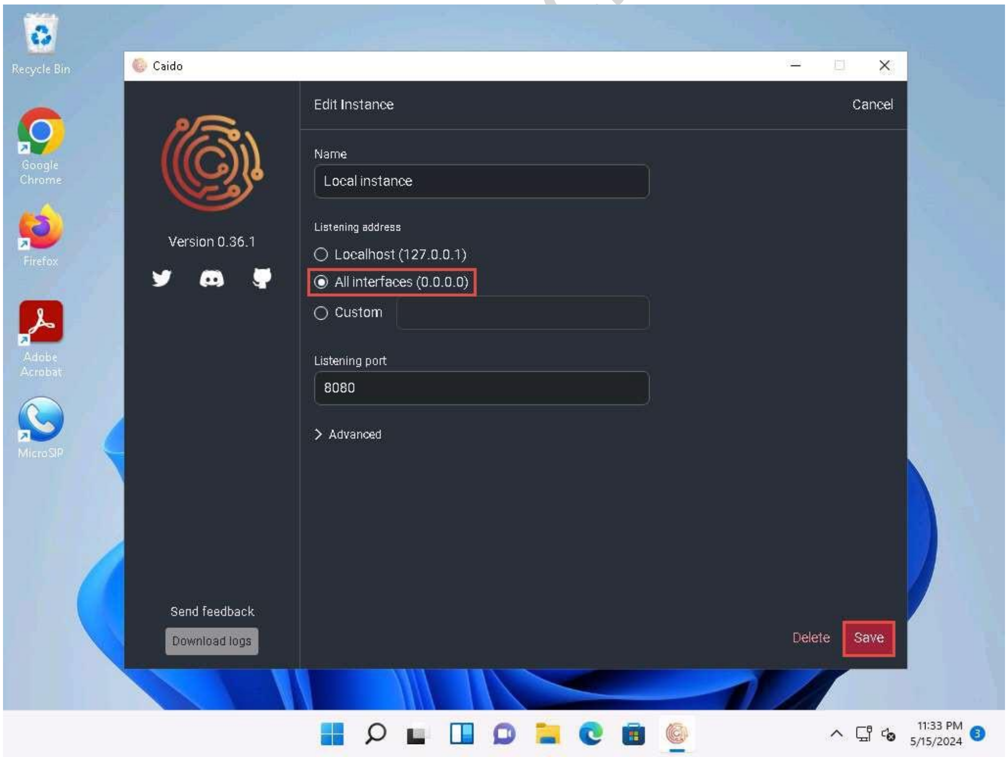
```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Admin>
```

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.



Name: Local instance

Listening address

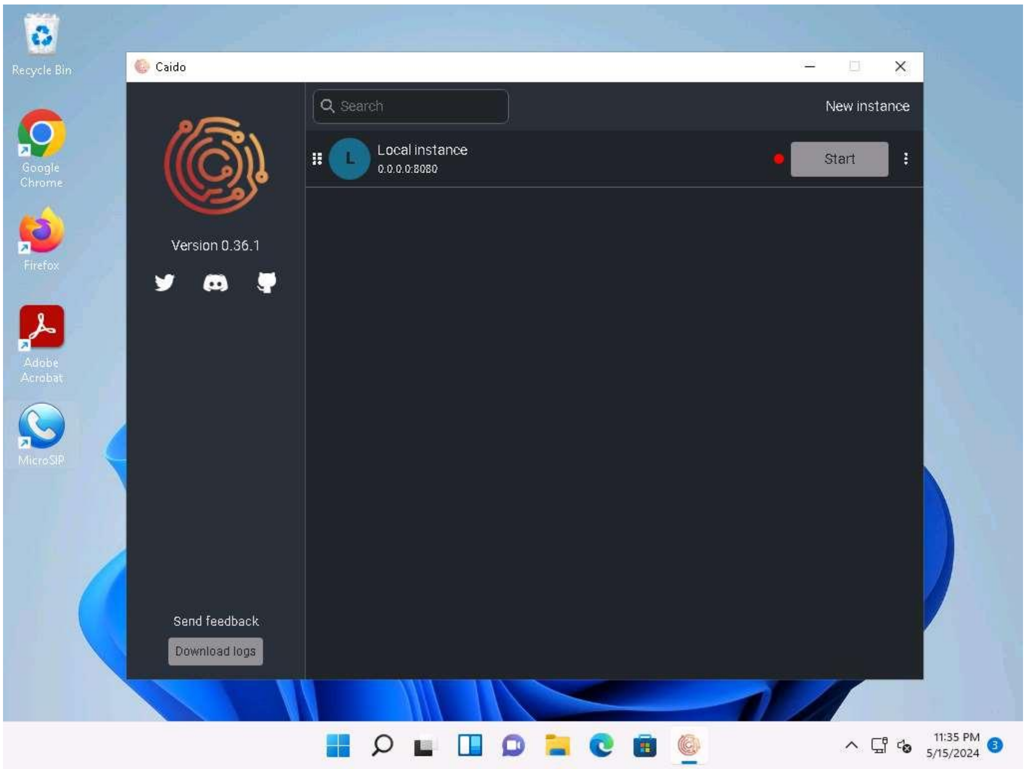
○ Localhost (127.0.0.1)

● All interfaces (0.0.0.0)

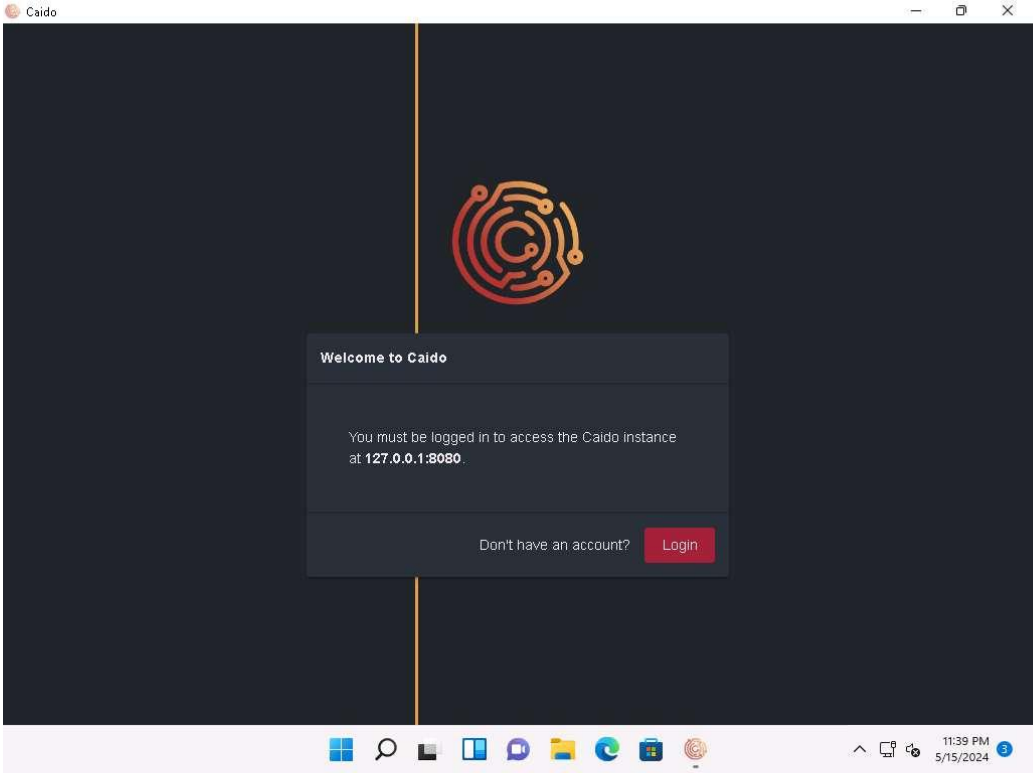
○ Custom

Listening port: 8080

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



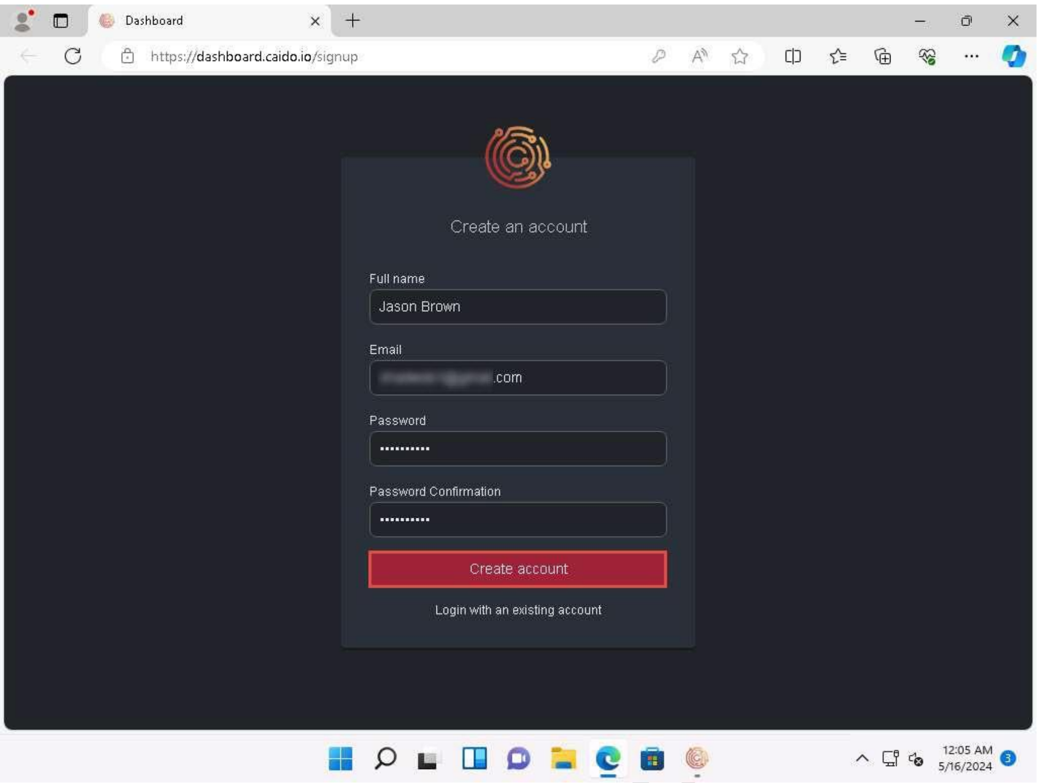
8. Welcome to Caido pop-up appears, click on Login if you have an account already. If not, select Don't have an account?, you will be redirected to Dashboard.



**Welcome to Caido**

You must be logged in to access the Caido instance at **127.0.0.1:8080**.

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



Dashboard
https://dashboard.caido.io/signup

Create an account

Full name: Jason Brown

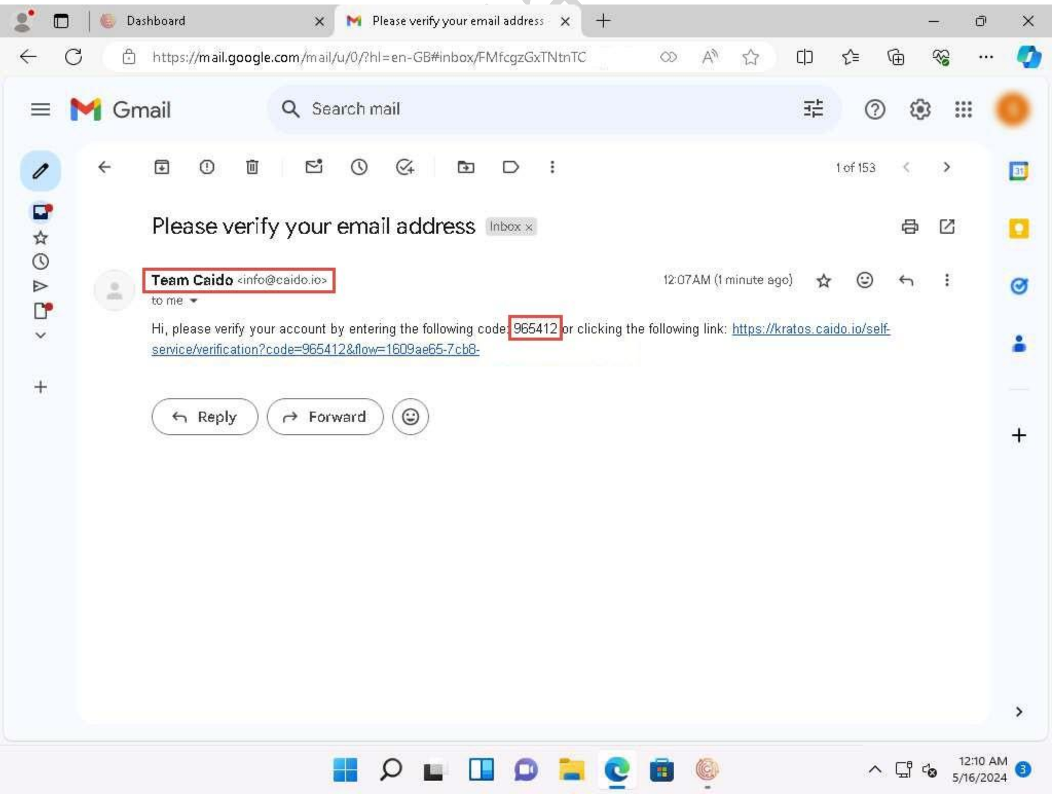
Email: [redacted].com

Password: ••••••••••

Password Confirmation: ••••••••••

Create account
Login with an existing account
12:05 AM
5/16/2024

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.



Dashboard
Please verify your email address
https://mail.google.com/mail/u/0/?hl=en-GB#inbox/FMfcgzGxTNtnTC
Gmail
Search mail
1 of 153

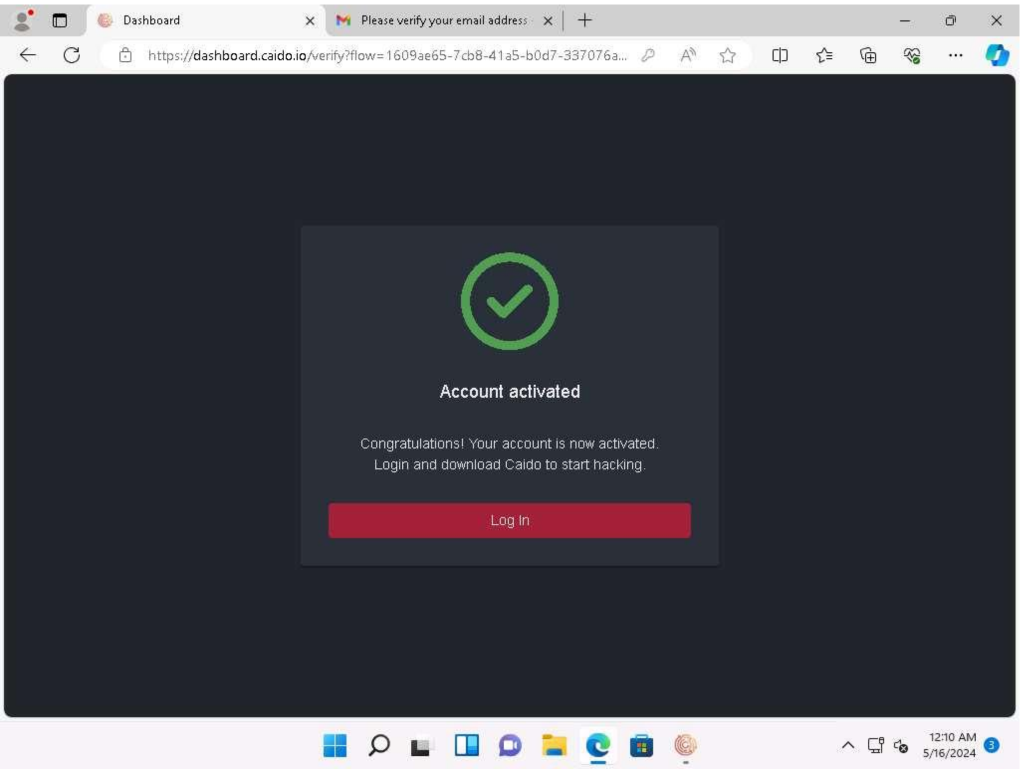
Please verify your email address Inbox ×

Team Caido <info@caido.io>
to me
12:07 AM (1 minute ago)

Hi, please verify your account by entering the following code: 965412 or clicking the following link: https://kratos.caido.io/self-service/verification?code=965412&flow=1609ae65-7cb8-

Reply
Forward
12:10 AM
5/16/2024

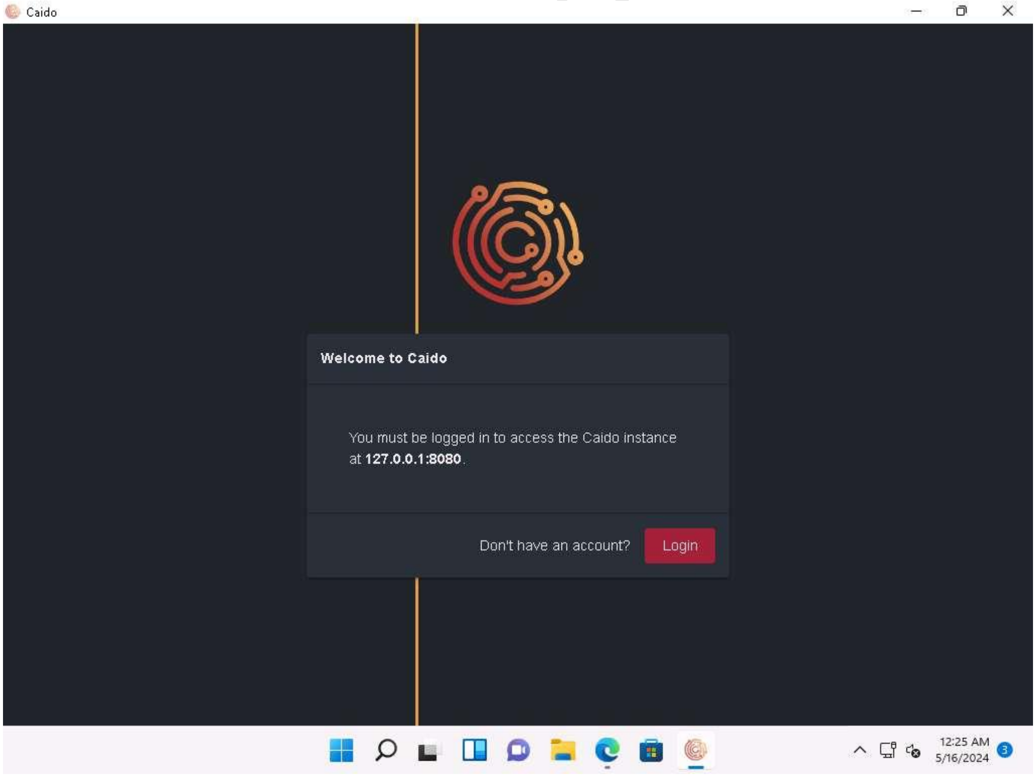
11. After entering the code, your account will be activated as shown in the screenshot.


Dashboard
Please verify your email address
https://dashboard.caido.io/verify?flow=1609ae65-7cb8-41a5-b0d7-337076a...
Log In
12:10 AM
5/16/2024

Account activated

Congratulations! Your account is now activated.
Login and download Caido to start hacking.

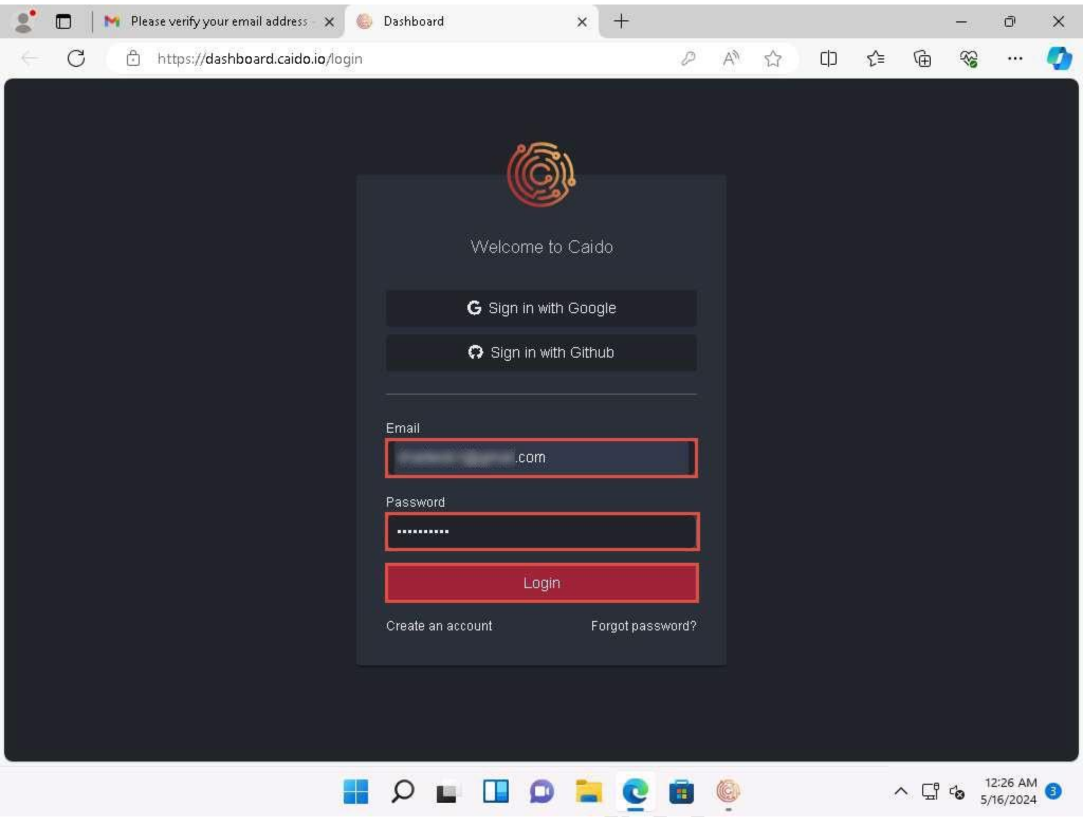
12. Navigate back to Caido application, in Welcome to Caido pop-up click on Login.



Welcome to Caido

You must be logged in to access the Caido instance at **127.0.0.1:8080**.

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


Please verify your email address
Dashboard
https://dashboard.caido.io/login

Welcome to Caido

Sign in with Google

Sign in with Github

Email

[redacted].com

Password

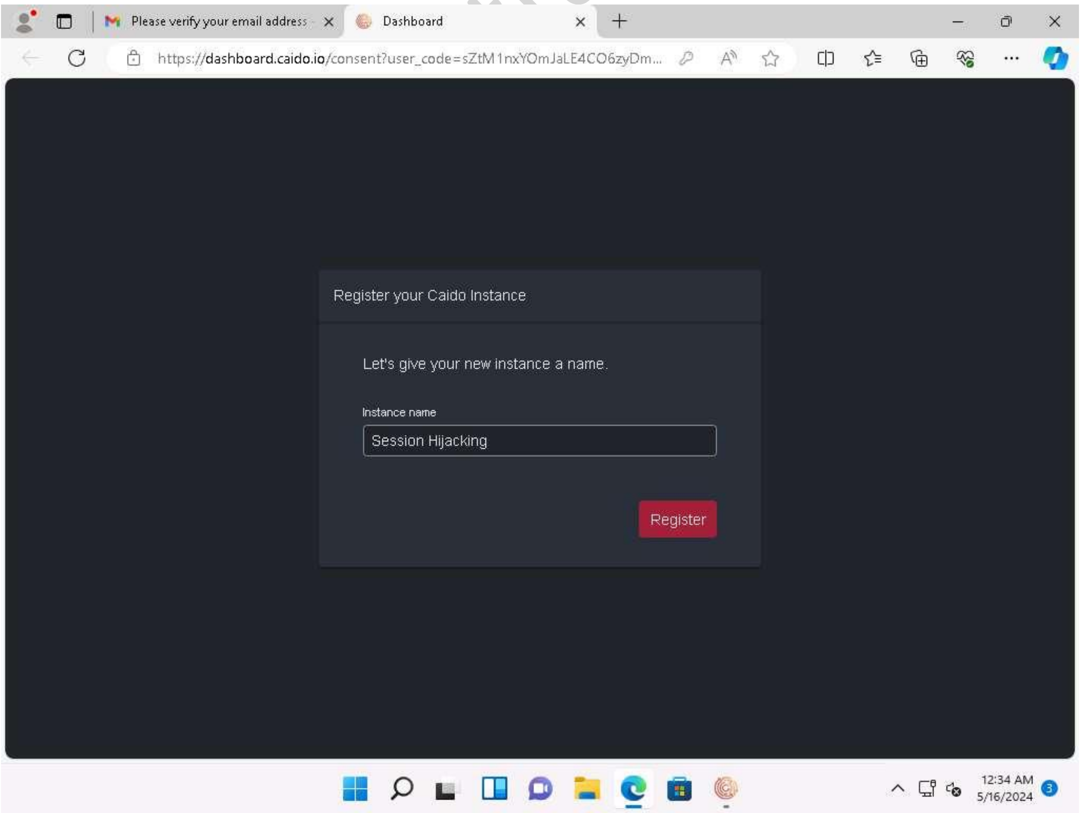
••••••••••

Login

Create an account

Forgot password?

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


Please verify your email address
Dashboard
https://dashboard.caido.io/consent?user_code=sZtM1nxYOmJaLE4CO6zyDm...

Register your Caido Instance

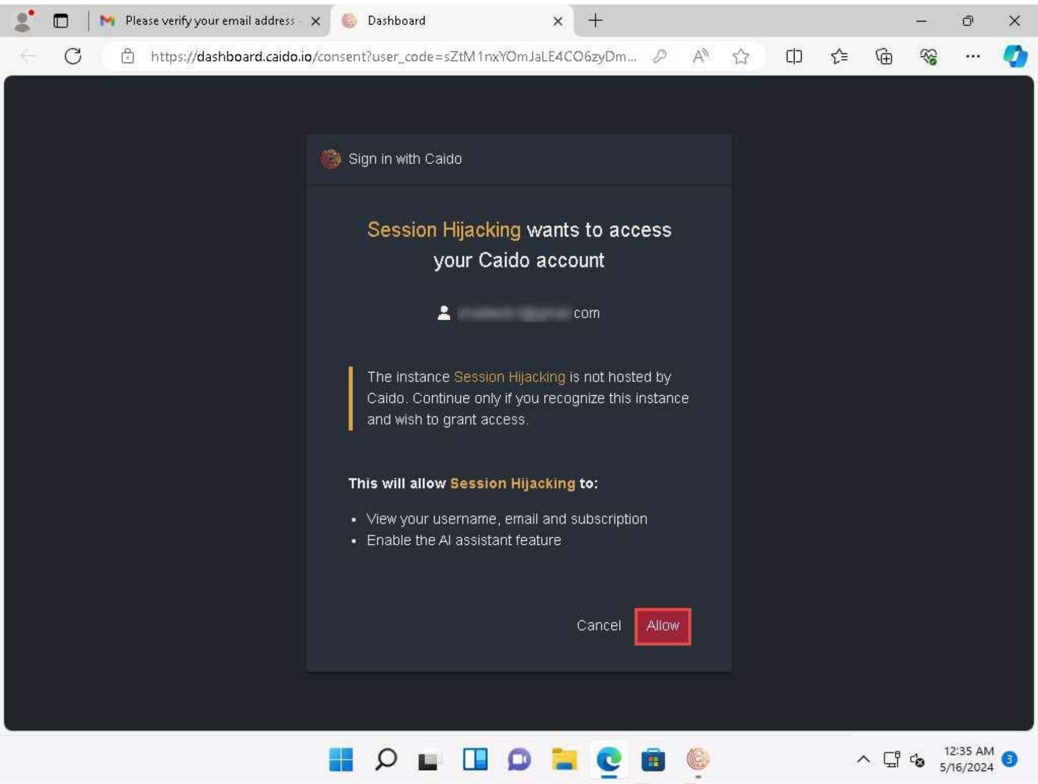
Let's give your new instance a name.

Instance name

Session Hijacking

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.


Please verify your email address
Dashboard
https://dashboard.caido.io/consent?user_code=sZtM1nxYOmJaLE4CO6zyDm...
12:35 AM
5/16/2024

Sign in with Caido

Session Hijacking wants to access your Caido account

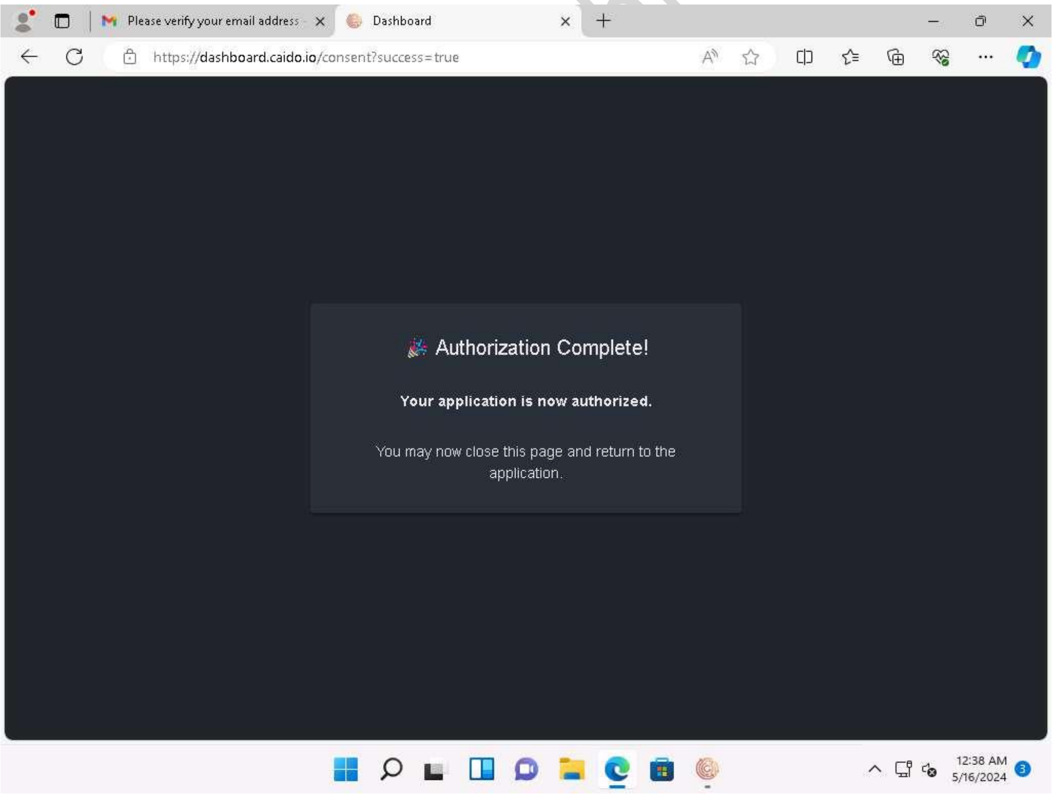
[redacted] com

The instance Session Hijacking is not hosted by Caido. Continue only if you recognize this instance and wish to grant access.

**This will allow Session Hijacking to:**

- View your username, email and subscription
- Enable the AI assistant feature

Cancel Allow


Please verify your email address
Dashboard
https://dashboard.caido.io/consent?success=true
12:38 AM
5/16/2024

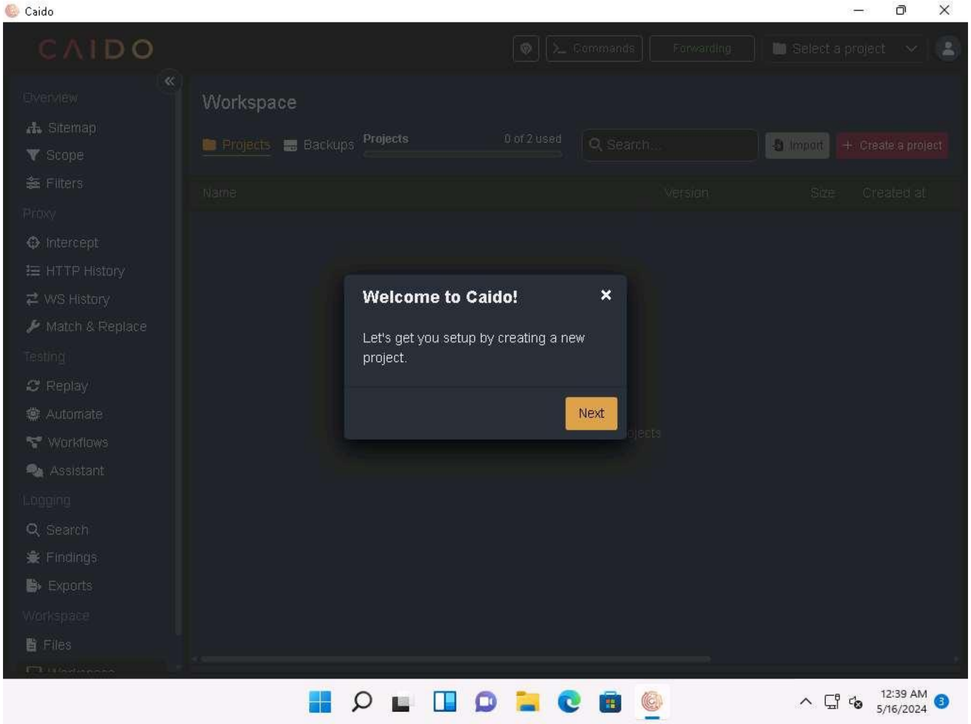
🎉 Authorization Complete!

**Your application is now authorized.**

You may now close this page and return to the application.

16. The Caido main window appears.

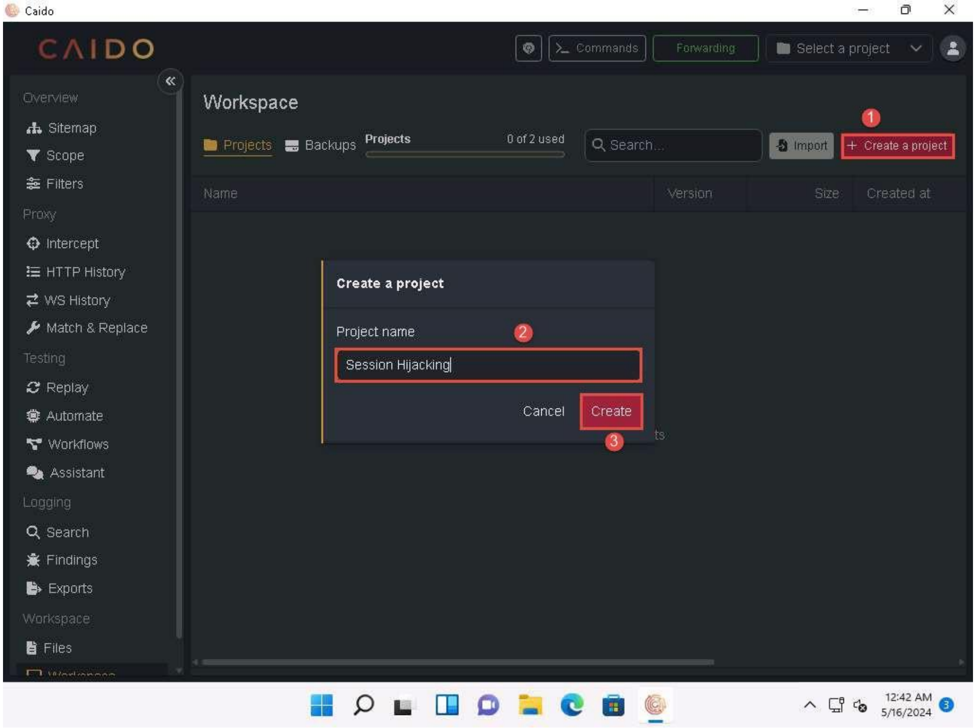
If a Caido pop-up appears, click Next or Ok in all the pop-ups.



Welcome to Caido!

Let's get you setup by creating a new project.

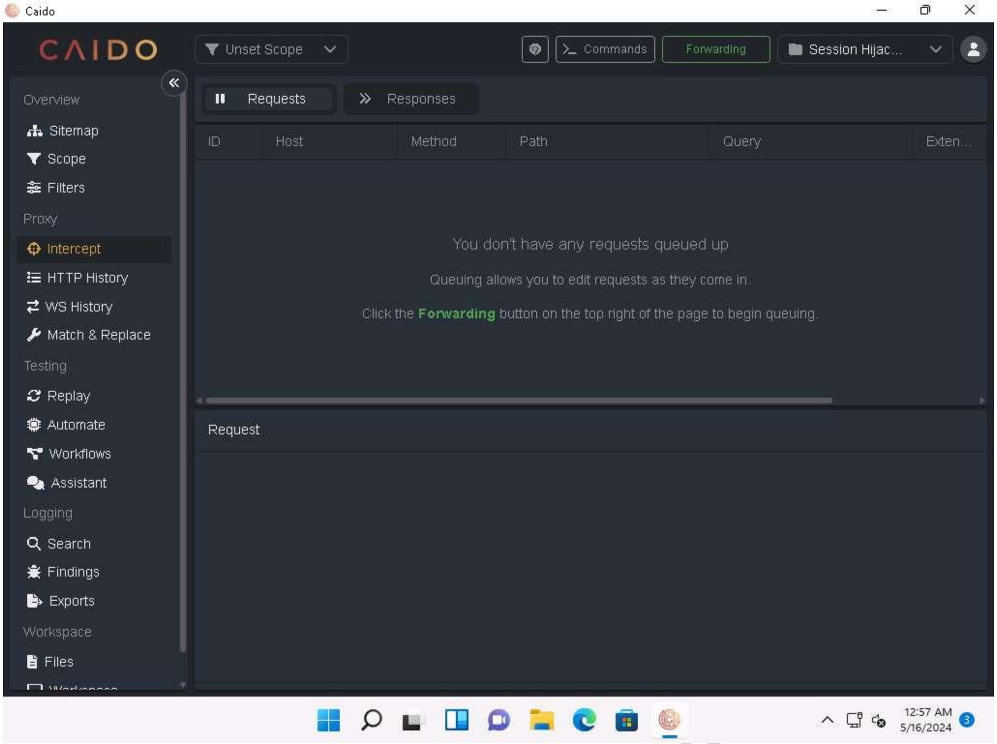
17. Click on + Create a project button to create a new project. Create a project pop-up appears, name it as Session Hijacking and click Create.



Create a project

Project name: Session Hijacking

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



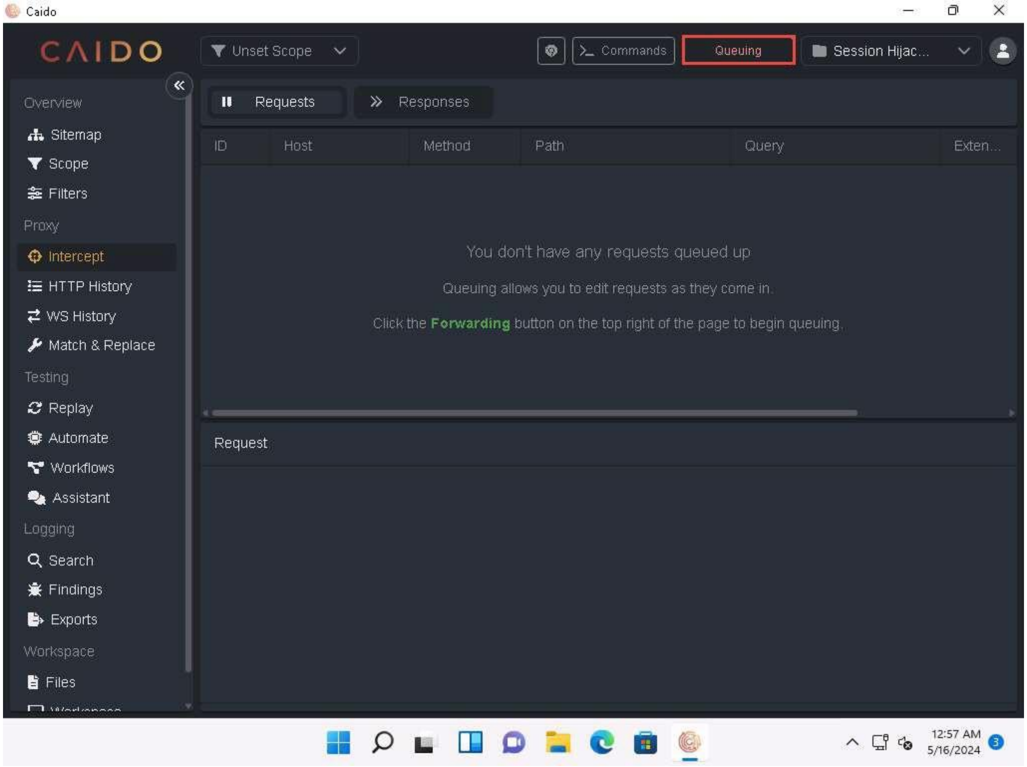
You don't have any requests queued up

Queuing allows you to edit requests as they come in.

Click the **Forwarding** button on the top right of the page to begin queuing.

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.



You don't have any requests queued up

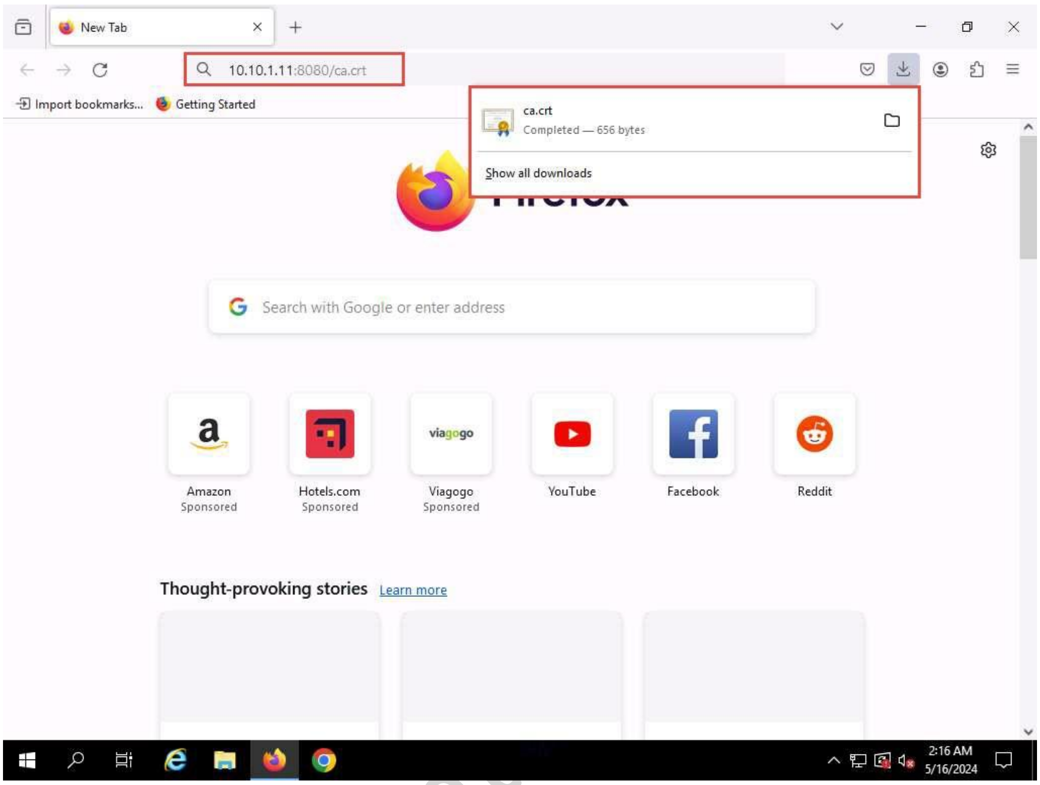
Queuing allows you to edit requests as they come in.

Click the **Forwarding** button on the top right of the page to begin queuing.

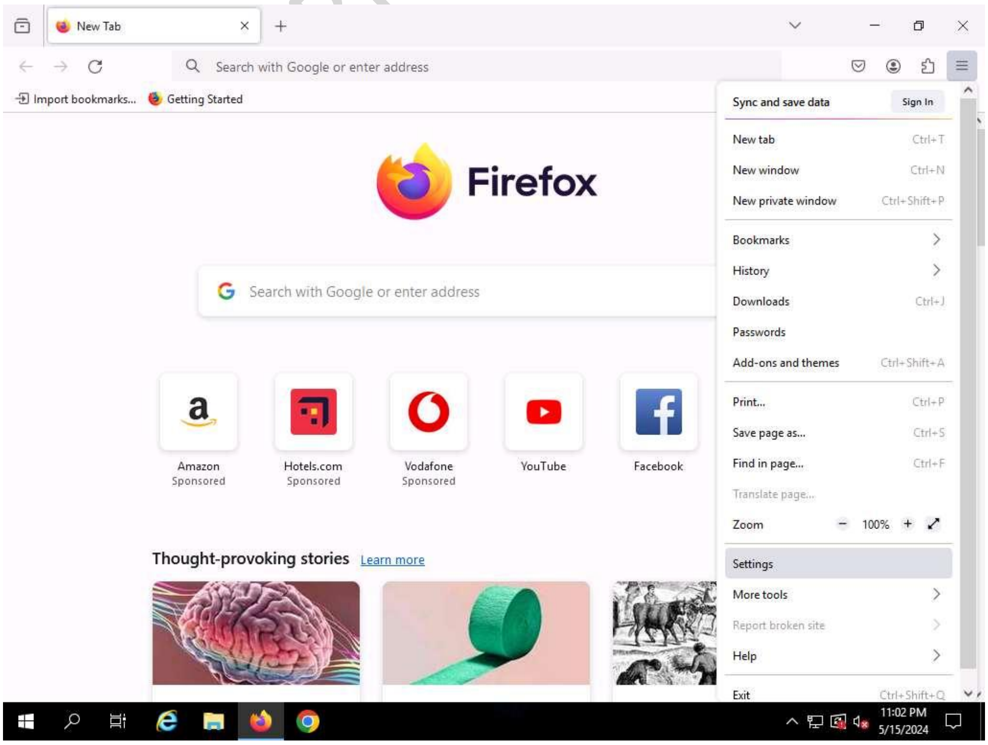
20. Click Windows Server 2019 to switch to the Windows Server 2019 machine.
    Click Ctrl+Alt+Delete to activate the machine and login using Administrator/Pa$$w0rd.

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

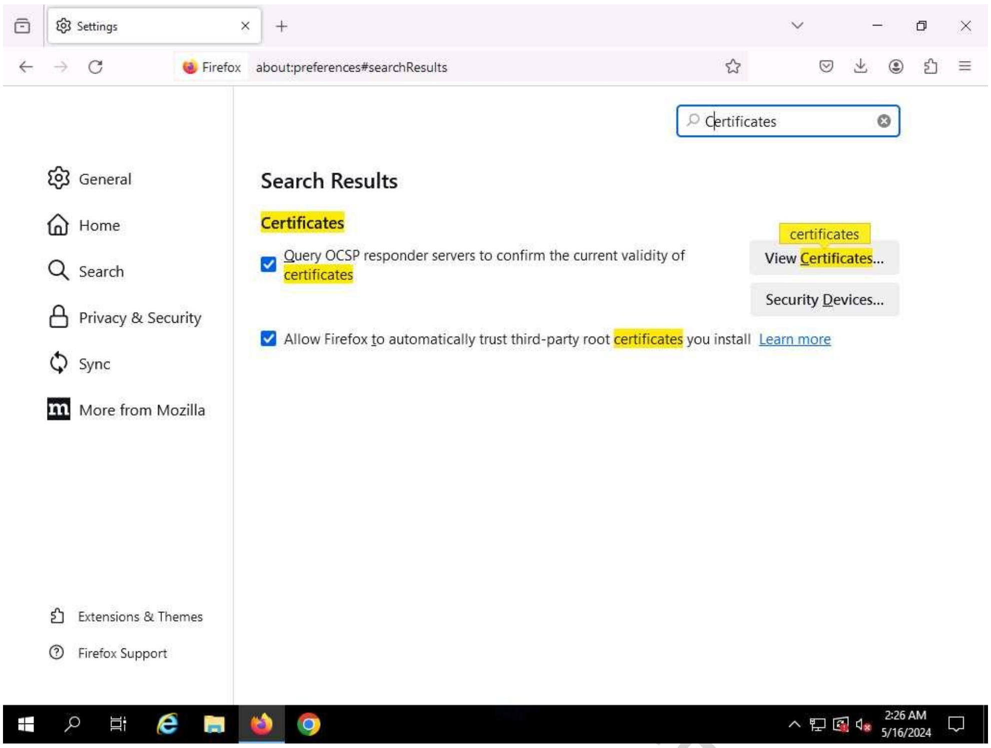
**21.** Open Firefox web browser and navigate to http://10.10.1.11:8080/ca.crt. CA certificate will be downloaded automatically as shown in the screenshot.



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



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


Settings

Firefox about:preferences#searchResults

Certificates

Search Results

Certificates

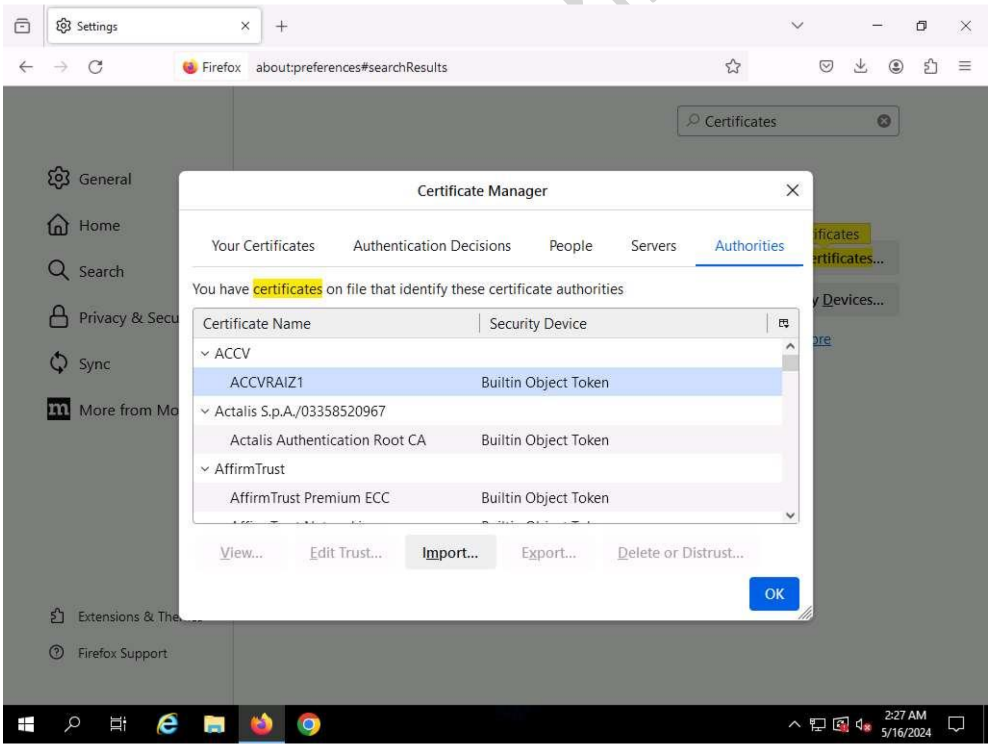
☑ Query OCSP responder servers to confirm the current validity of certificates

View Certificates...

Security Devices...

☑ Allow Firefox to automatically trust third-party root certificates you install Learn more

24. Navigate to Authorities tab and click on Import…


Certificate Manager

Your Certificates | Authentication Decisions | People | Servers | Authorities

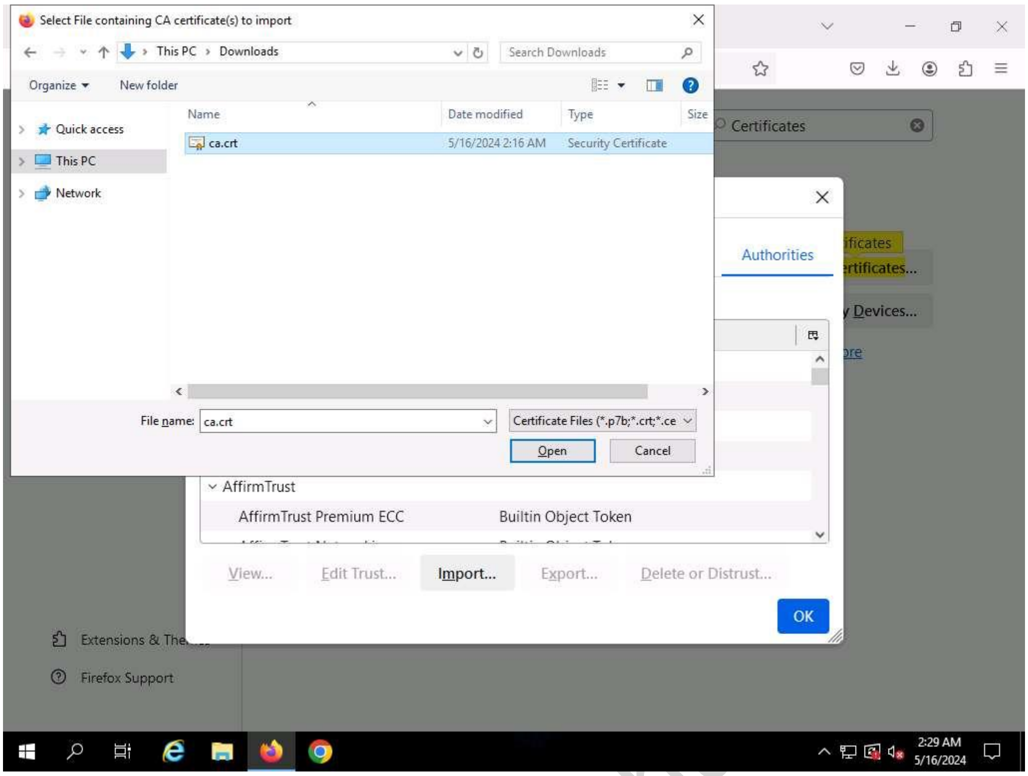
You have certificates on file that identify these certificate authorities

| Certificate Name | Security Device |
|---|---|
| ACCV | |
| ACCVRAIZ1 | Builtin Object Token |
| Actalis S.p.A./03358520967 | |
| Actalis Authentication Root CA | Builtin Object Token |
| AffirmTrust | |
| AffirmTrust Premium ECC | Builtin Object Token |

View... | Edit Trust... | Import... | Export... | Delete or Distrust...

OK

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


Select File containing CA certificate(s) to import

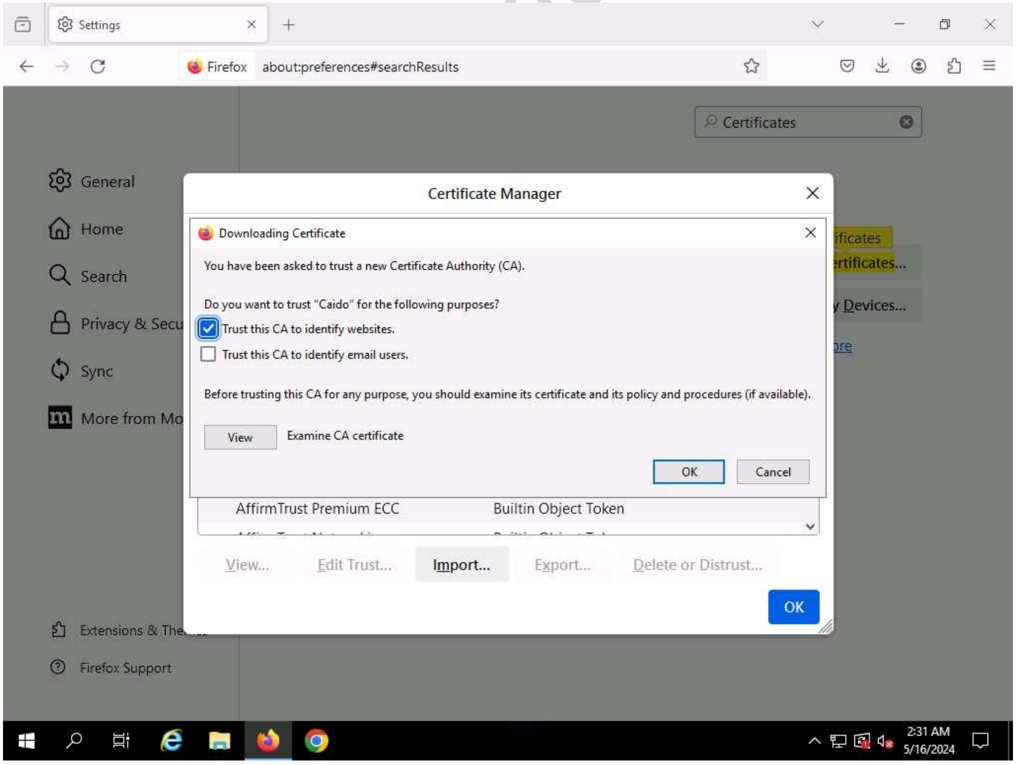
This PC › Downloads

| Name | Date modified | Type | Size |
|---|---|---|---|
| ca.crt | 5/16/2024 2:16 AM | Security Certificate | |

File name: ca.crt

Certificate Files (*.p7b;*.crt;*.ce

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


Certificate Manager

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust “Caido” for the following purposes?

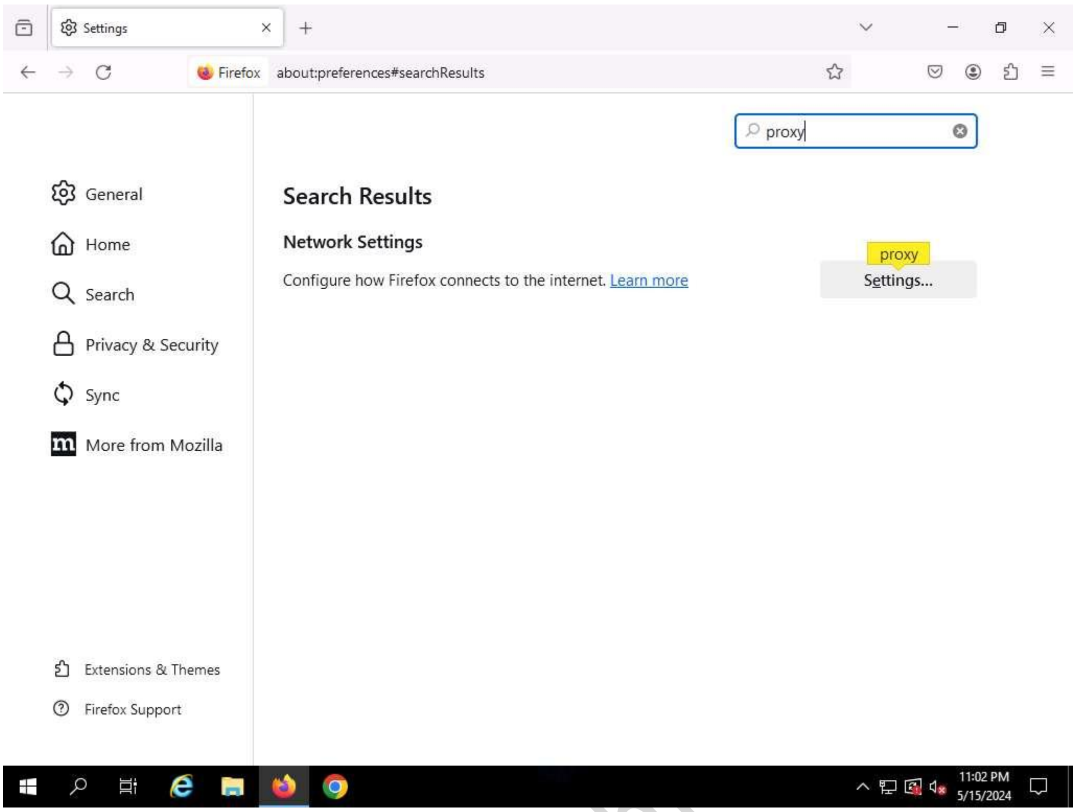
☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

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



Search Results

Network Settings

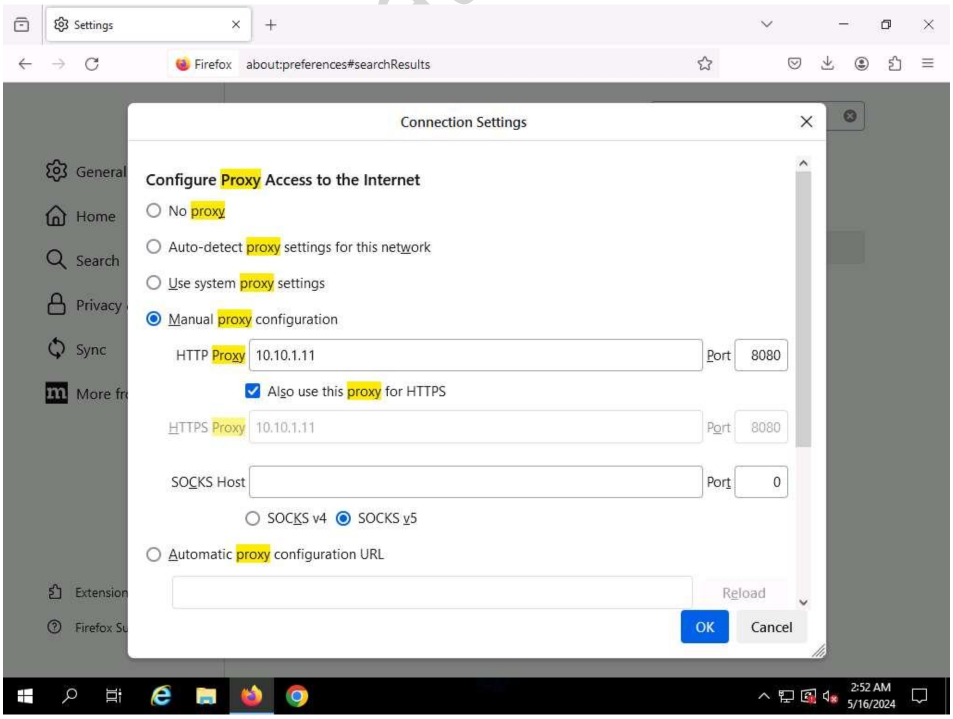
Configure how Firefox connects to the internet. Learn more

proxy

Settings...

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.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 10.10.1.11 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 10.10.1.11 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

OK Cancel

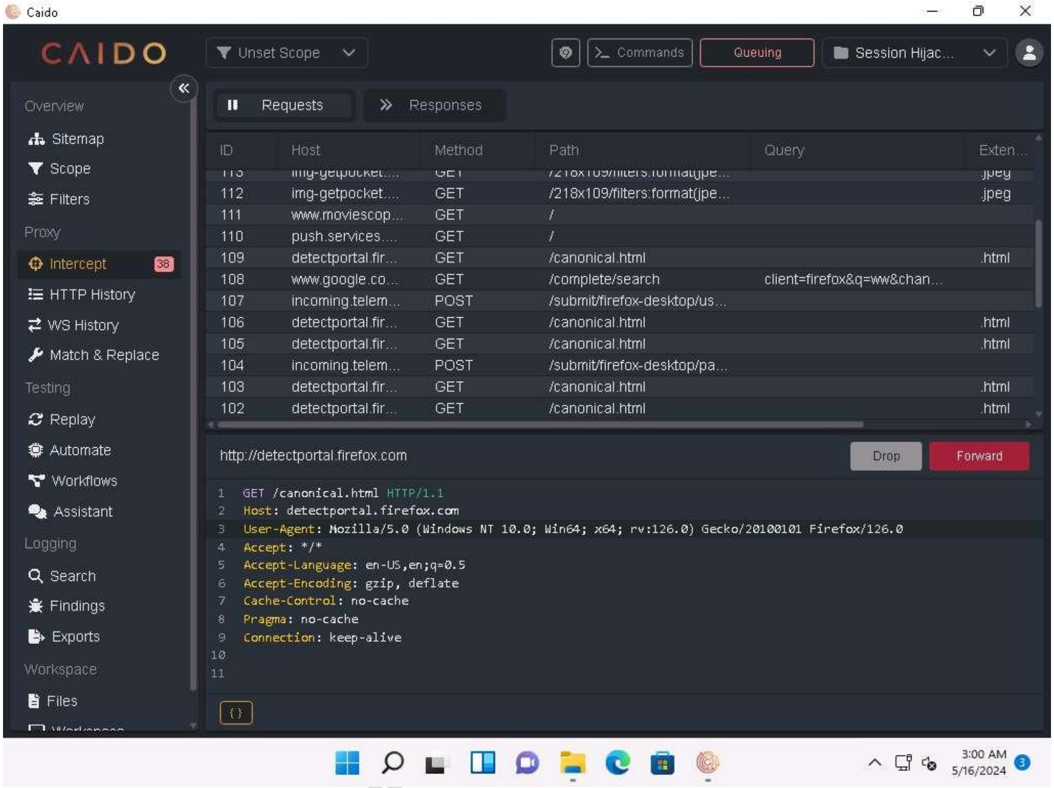
30. After saving, close the Settings and browser windows. You have now configured the proxy settings of the victim’s machine.

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.

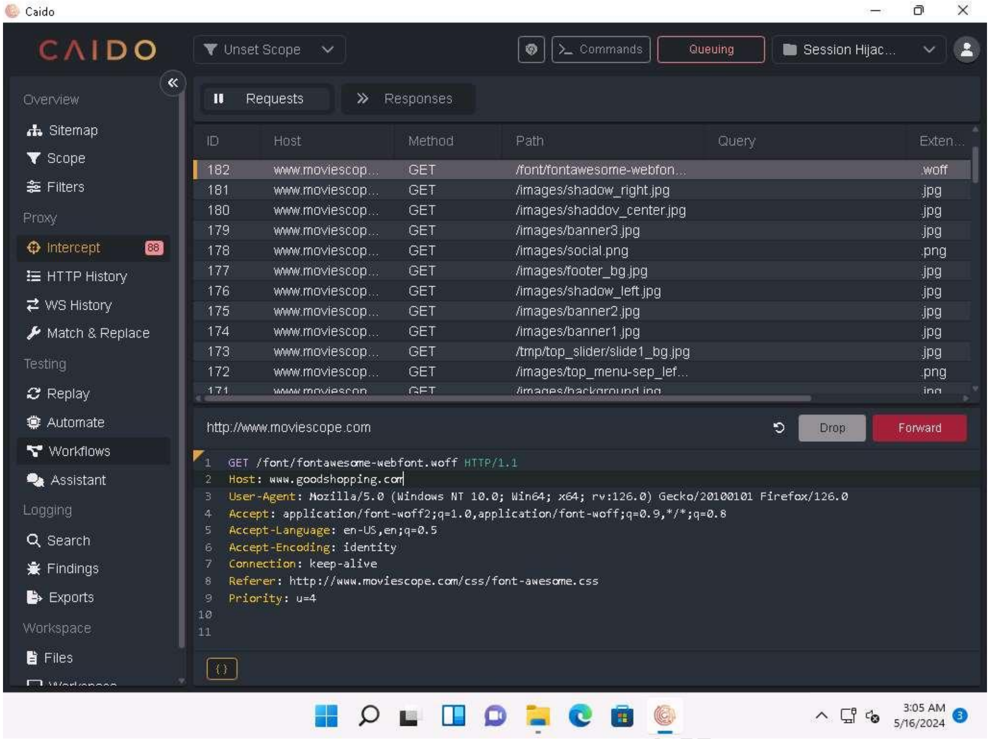


| ID | Host | Method | Path | Query | Exten... |
|---|---|---|---|---|---|
| 113 | img-getpocket.... | GET | /218x109/filters:format(jpe... | | .jpeg |
| 112 | img-getpocket.... | GET | /218x109/filters:format(jpe... | | .jpeg |
| 111 | www.moviescop... | GET | / | | |
| 110 | push.services.... | GET | / | | |
| 109 | detectportal.fir... | GET | /canonical.html | | .html |
| 108 | www.google.co... | GET | /complete/search | client=firefox&q=ww&chan... | |
| 107 | incoming.telem... | POST | /submit/firefox-desktop/us... | | |
| 106 | detectportal.fir... | GET | /canonical.html | | .html |
| 105 | detectportal.fir... | GET | /canonical.html | | .html |
| 104 | incoming.telem... | POST | /submit/firefox-desktop/pa... | | |
| 103 | detectportal.fir... | GET | /canonical.html | | .html |
| 102 | detectportal.fir... | GET | /canonical.html | | .html |

http://detectportal.firefox.com

```
GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive


```

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.



| ID | Host | Method | Path | Query | Exten... |
|---|---|---|---|---|---|
| 182 | www.moviescop... | GET | /font/fontawesome-webfon... | | .woff |
| 181 | www.moviescop... | GET | /images/shadow_right.jpg | | .jpg |
| 180 | www.moviescop... | GET | /images/shaddov_center.jpg | | .jpg |
| 179 | www.moviescop... | GET | /images/banner3.jpg | | .jpg |
| 178 | www.moviescop... | GET | /images/social.png | | .png |
| 177 | www.moviescop... | GET | /images/footer_bg.jpg | | .jpg |
| 176 | www.moviescop... | GET | /images/shadow_left.jpg | | .jpg |
| 175 | www.moviescop... | GET | /images/banner2.jpg | | .jpg |
| 174 | www.moviescop... | GET | /images/banner1.jpg | | .jpg |
| 173 | www.moviescop... | GET | /tmp/top_slider/slide1_bg.jpg | | .jpg |
| 172 | www.moviescop... | GET | /images/top_menu-sep_lef... | | .png |
| 171 | www.moviescop... | GET | /images/background.jpg | | .jpg |

http://www.moviescope.com

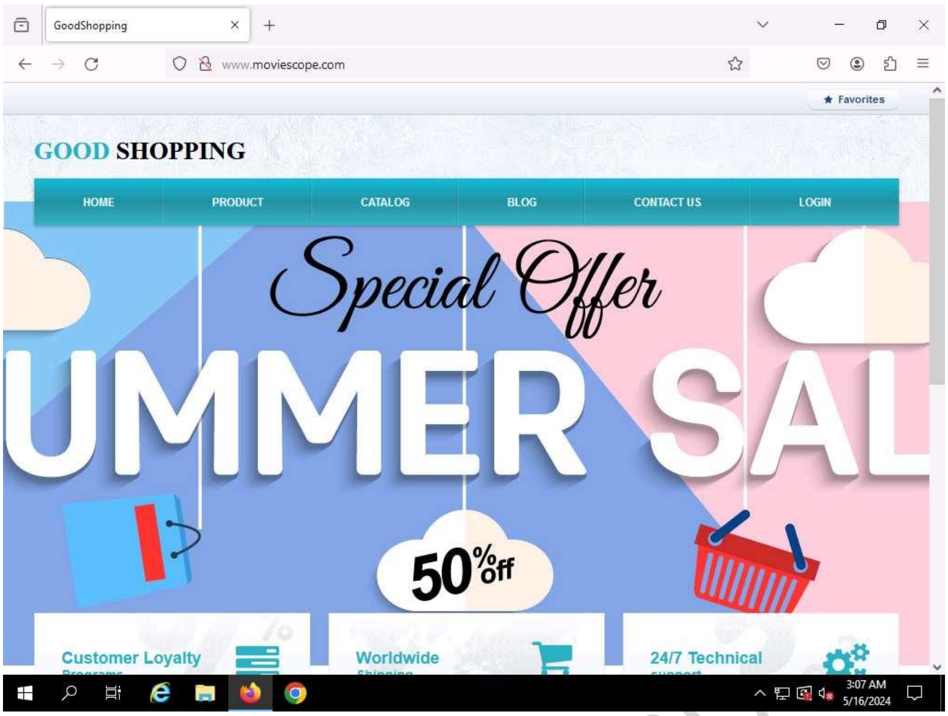
```
GET /font/fontawesome-webfont.woff HTTP/1.1
Host: www.goodshopping.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: application/font-woff2;q=1.0,application/font-woff;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: identity
Connection: keep-alive
Referer: http://www.moviescope.com/css/font-awesome.css
Priority: u=4


```

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.

### 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.

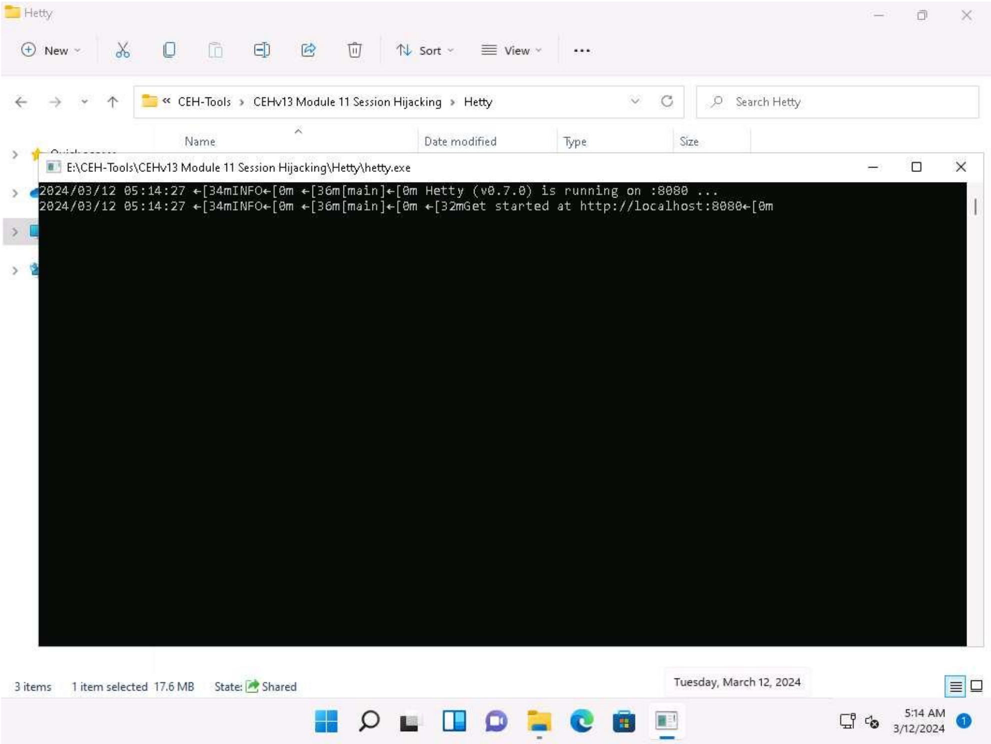
Here, we will use Windows 11 machine as an attacker machine and Windows Server 2022 machine as a target machine.

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.



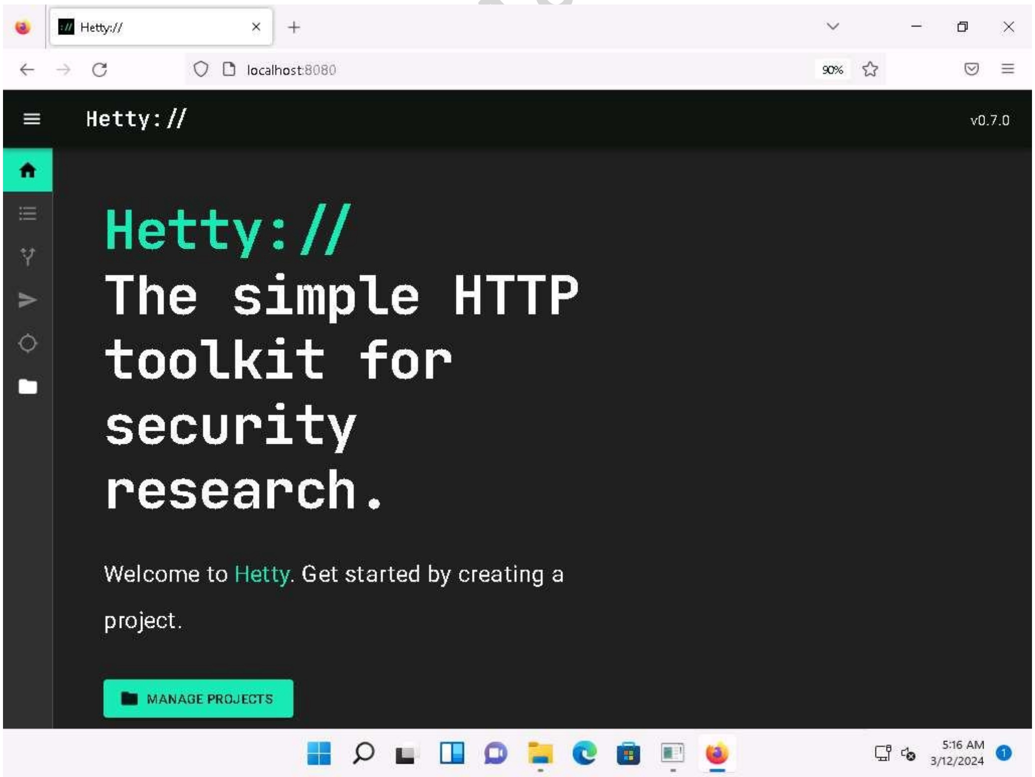
E:\CEH-Tools\CEHv13 Module 11 Session Hijacking\Hetty\hetty.exe

```
2024/03/12 05:14:27 ←[34mINFO←[0m ←[36m[main]←[0m Hetty (v0.7.0) is running on :8080 ...
2024/03/12 05:14:27 ←[34mINFO←[0m ←[36m[main]←[0m ←[32mGet started at http://localhost:8080←[0m
```

Hetty
New
Sort
View
CEH-Tools › CEHv13 Module 11 Session Hijacking › Hetty
Search Hetty
Name
Date modified
Type
Size
3 items 1 item selected 17.6 MB State: Shared
Tuesday, March 12, 2024
5:14 AM
3/12/2024

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

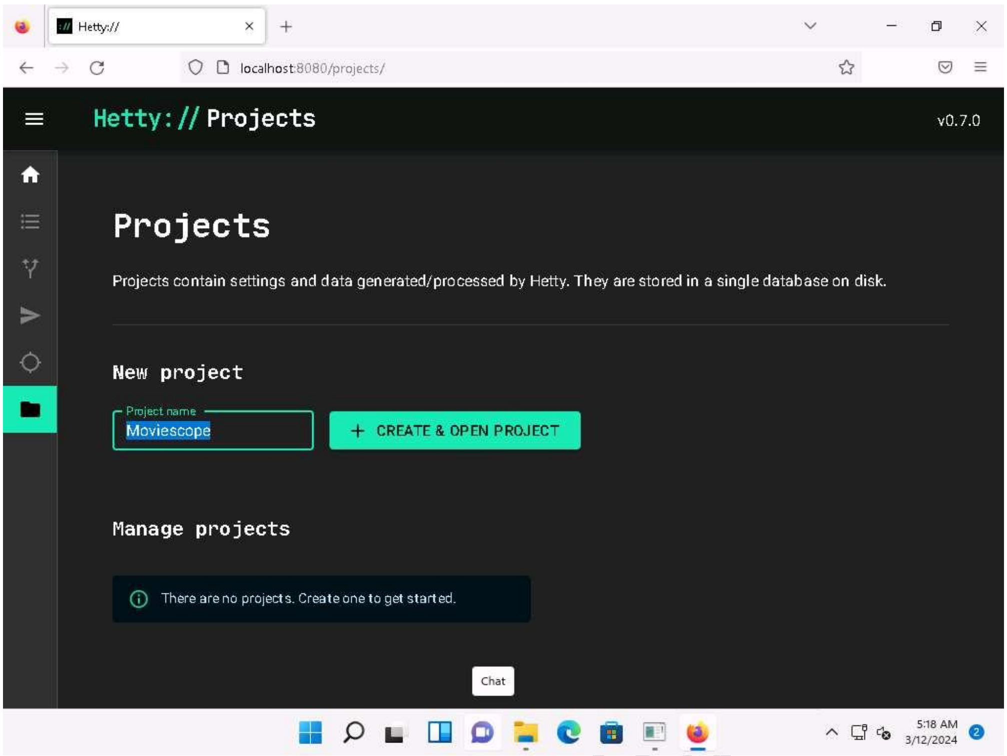
5. In the Hetty dashboard, click MANAGE PROJECTS button.



Hetty://
The simple HTTP toolkit for security research.

Welcome to Hetty. Get started by creating a project.

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



Hetty://

localhost:8080/projects/

Hetty:// Projects

v0.7.0

Projects

Projects contain settings and data generated/processed by Hetty. They are stored in a single database on disk.

New project

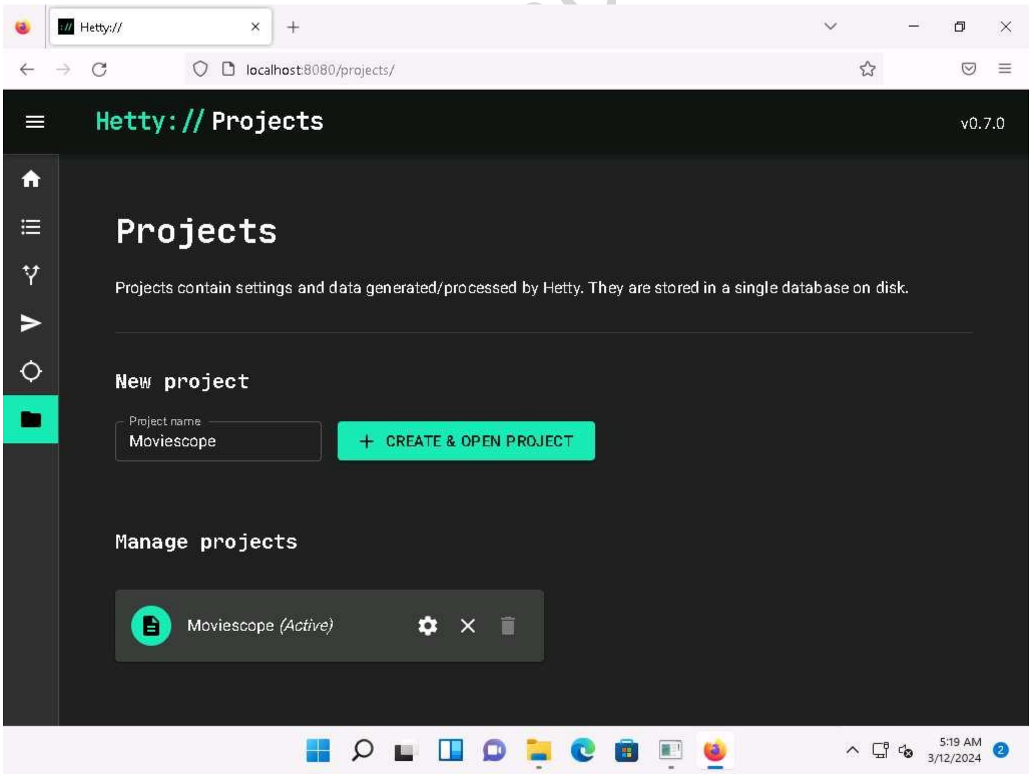
Project name: Moviescope

+ CREATE & OPEN PROJECT

Manage projects

ⓘ There are no projects. Create one to get started.

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



Hetty://

localhost:8080/projects/

Hetty:// Projects

v0.7.0

Projects

Projects contain settings and data generated/processed by Hetty. They are stored in a single database on disk.

New project

Project name: Moviescope

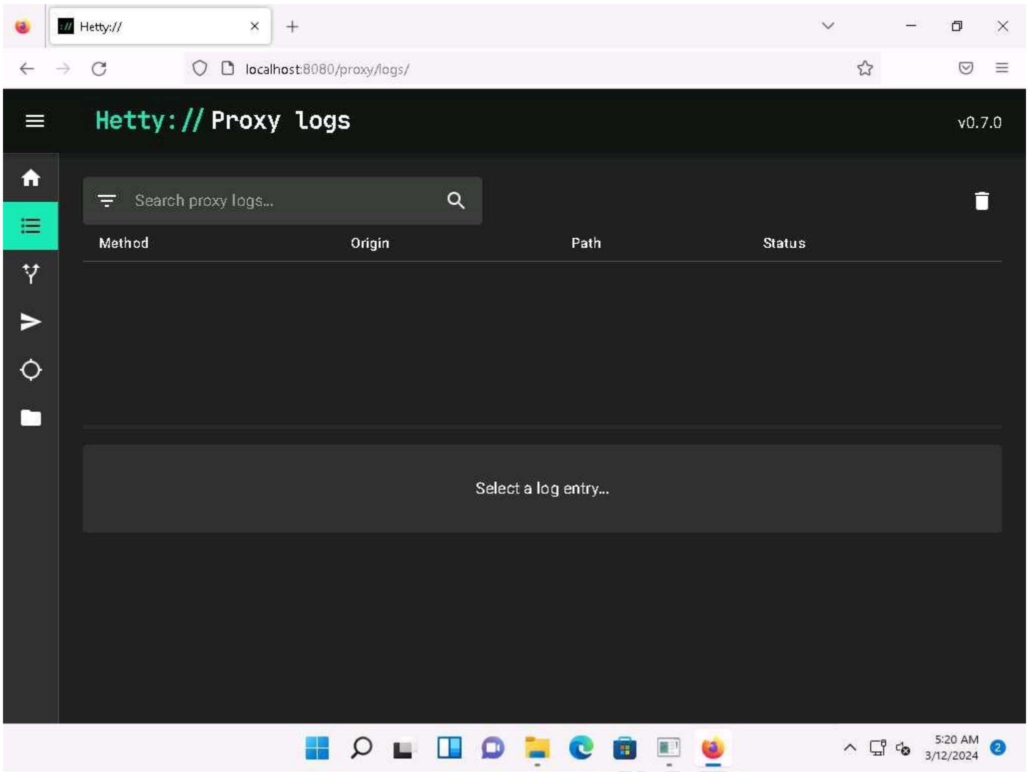
+ CREATE & OPEN PROJECT

Manage projects

Moviescope *(Active)*

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

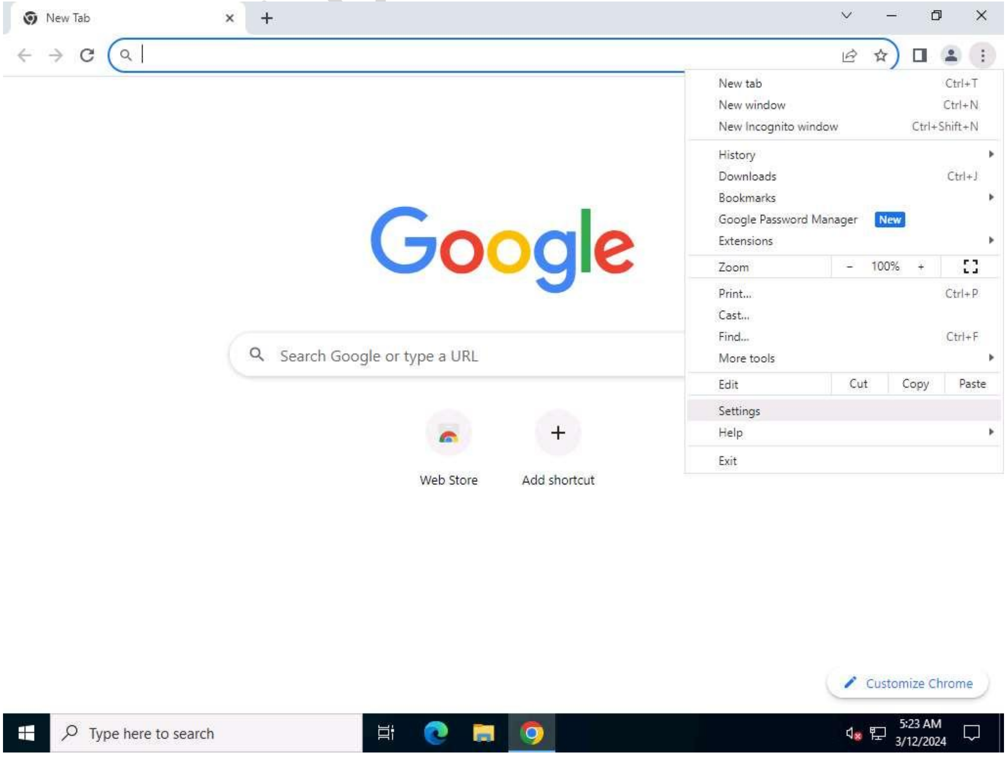
**9.** A Proxy logs page appears, as shown in the screenshot.



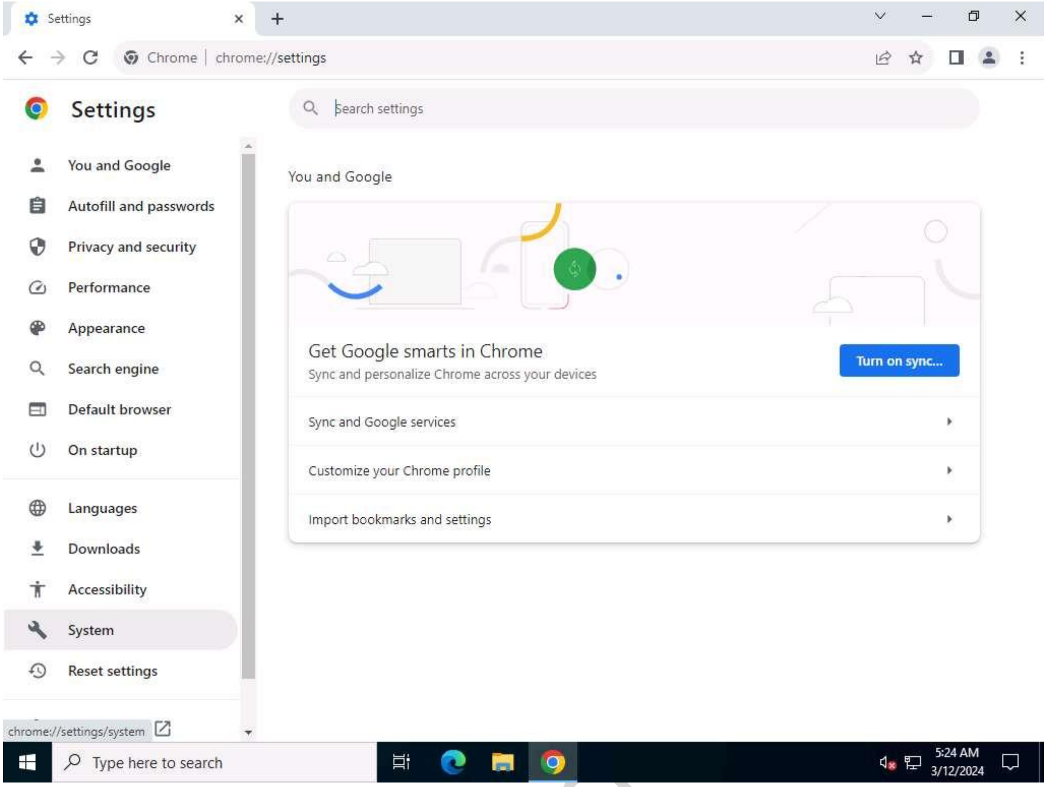
10. Now, click Windows Server 2022 to switch to the Windows Server 2022 machine. Click Ctrl+Alt+Delete to activate the machine and login using Administrator/Pa$$w0rd.

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

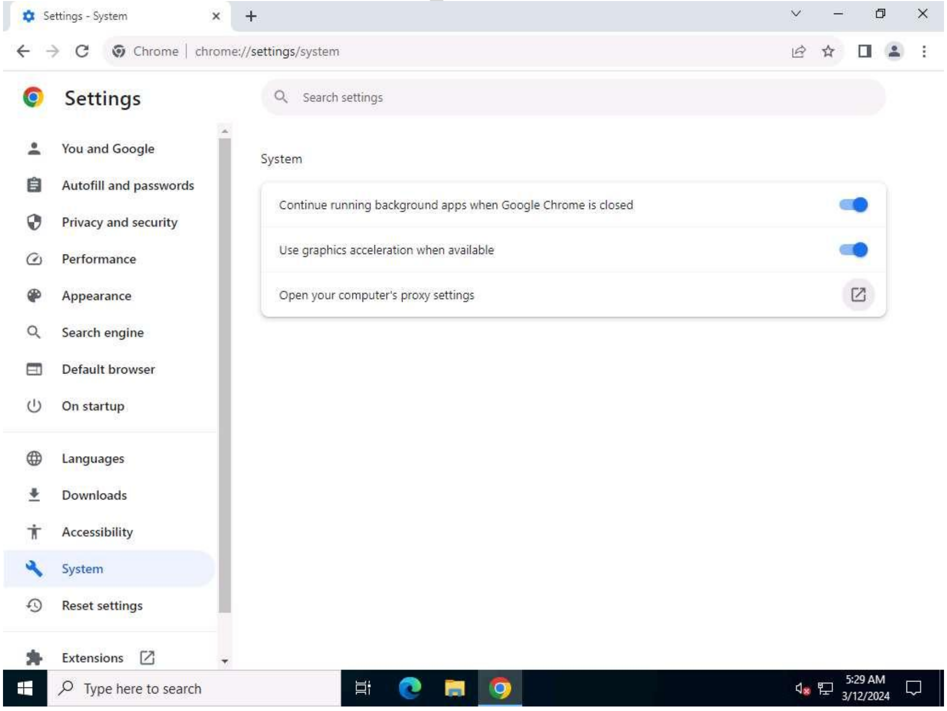
**11.** Open Google Chrome web browser, click the Customize and control Google Chrome icon, and select Settings from the context menu.



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.



System

Continue running background apps when Google Chrome is closed ●

Use graphics acceleration when available ●

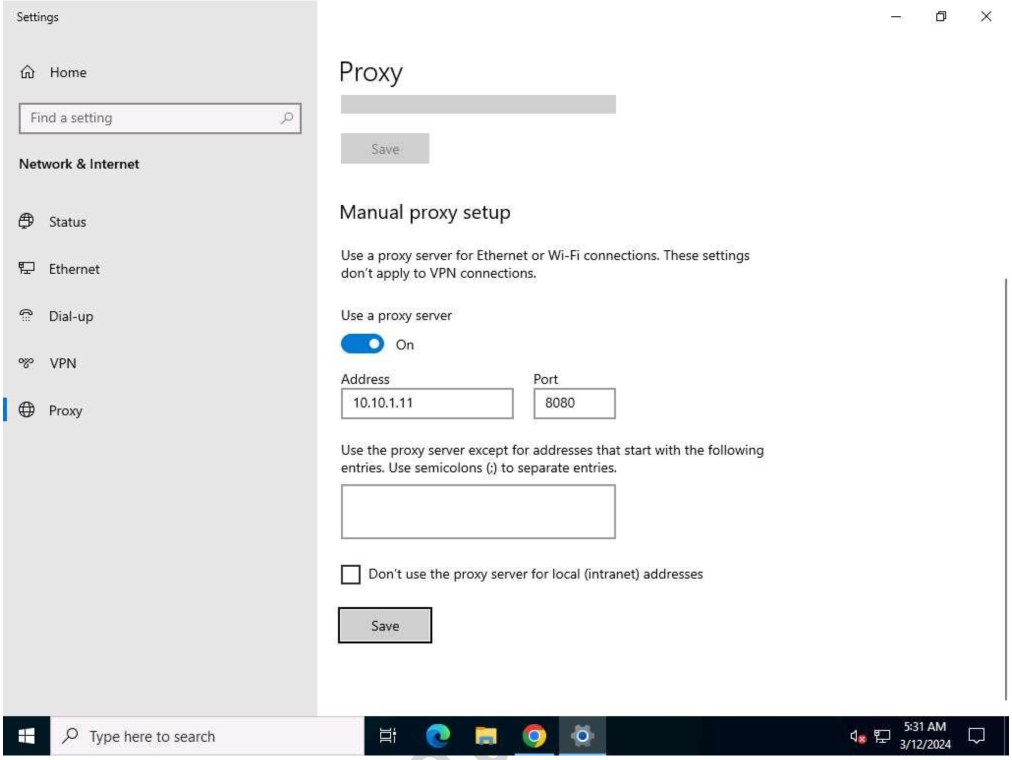
Open your computer's proxy settings

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.



Proxy

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don’t apply to VPN connections.

Use a proxy server: On

Address: 10.10.1.11

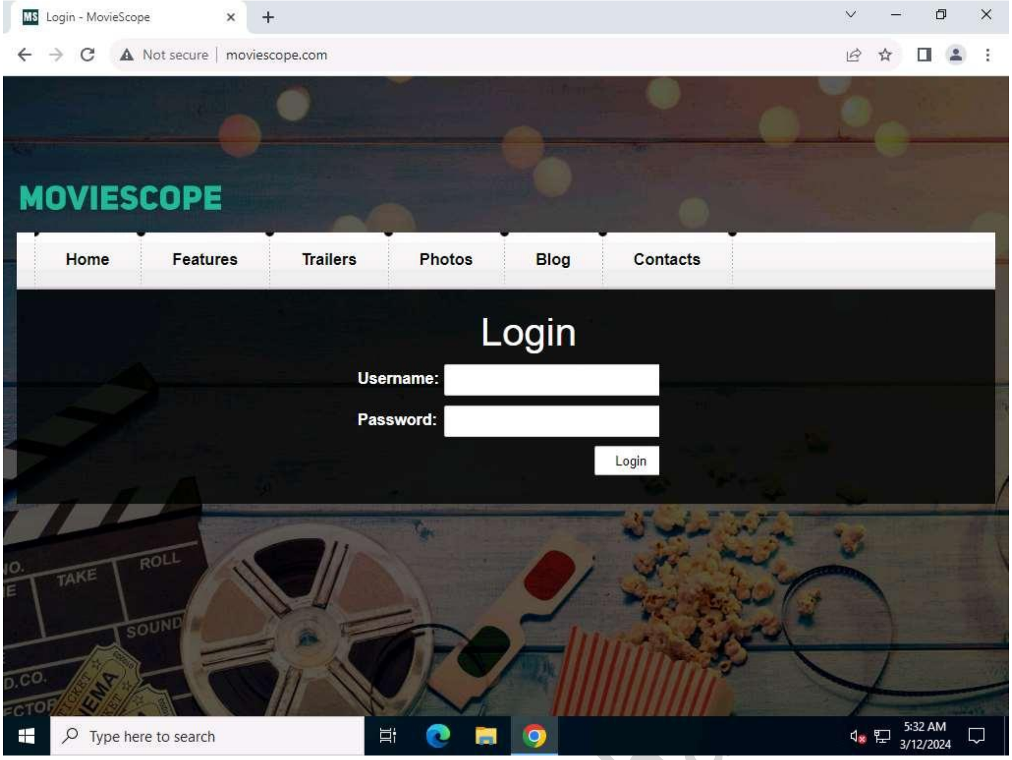
Port: 8080

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

□ Don't use the proxy server for local (intranet) addresses

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.



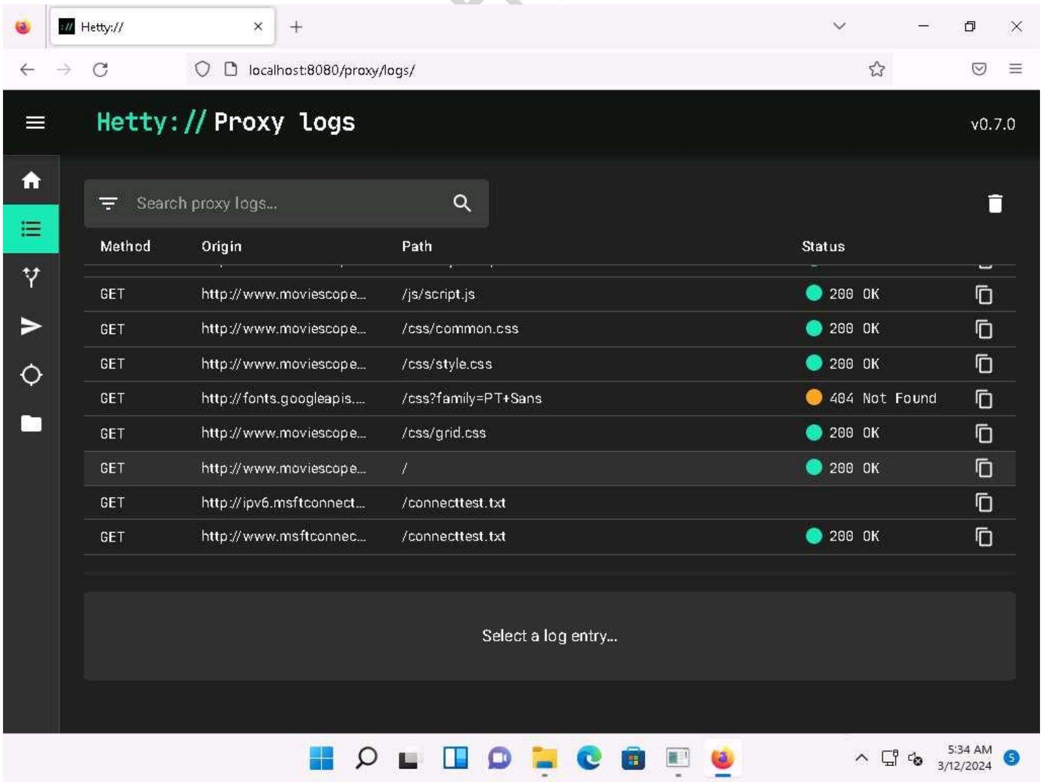
Login

Username:

Password:

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

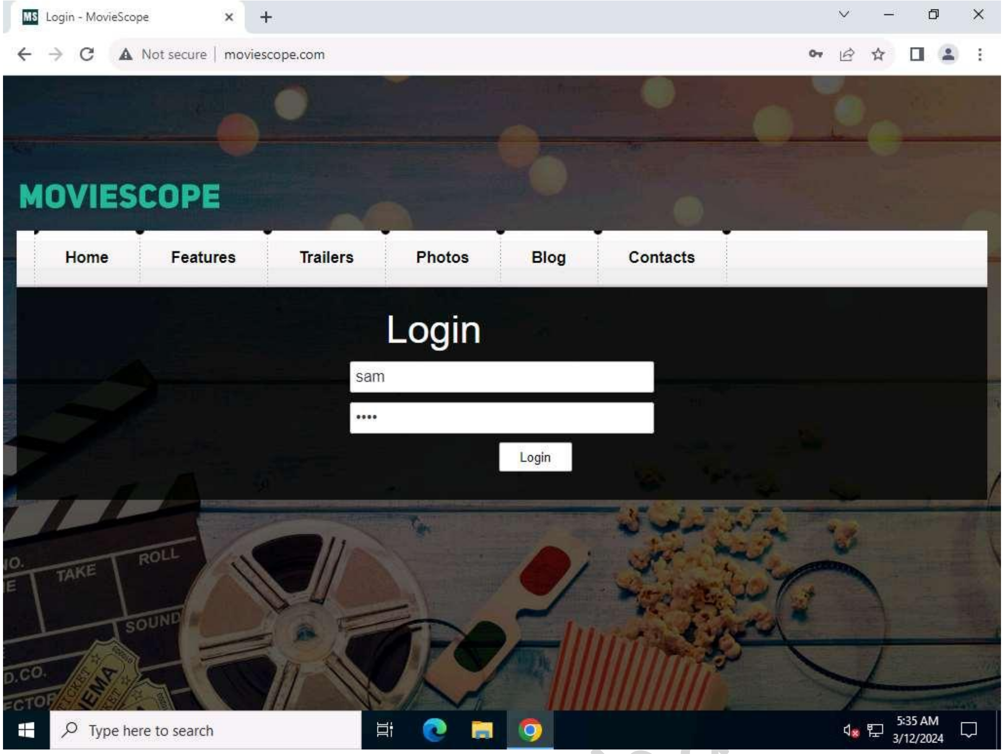
19. You can observe that the logs are captured in the Proxy logs page. Here, we are focusing on logs associated with moviescope.com website.



| Method | Origin | Path | Status |
|---|---|---|---|
| GET | http://www.moviescope... | /js/script.js | ● 200 OK |
| GET | http://www.moviescope... | /css/common.css | ● 200 OK |
| GET | http://www.moviescope... | /css/style.css | ● 200 OK |
| GET | http://fonts.googleapis.... | /css?family=PT+Sans | ● 404 Not Found |
| GET | http://www.moviescope... | /css/grid.css | ● 200 OK |
| GET | http://www.moviescope... | / | ● 200 OK |
| GET | http://ipv6.msftconnect... | /connecttest.txt | |
| GET | http://www.msftconnec... | /connecttest.txt | ● 200 OK |

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.

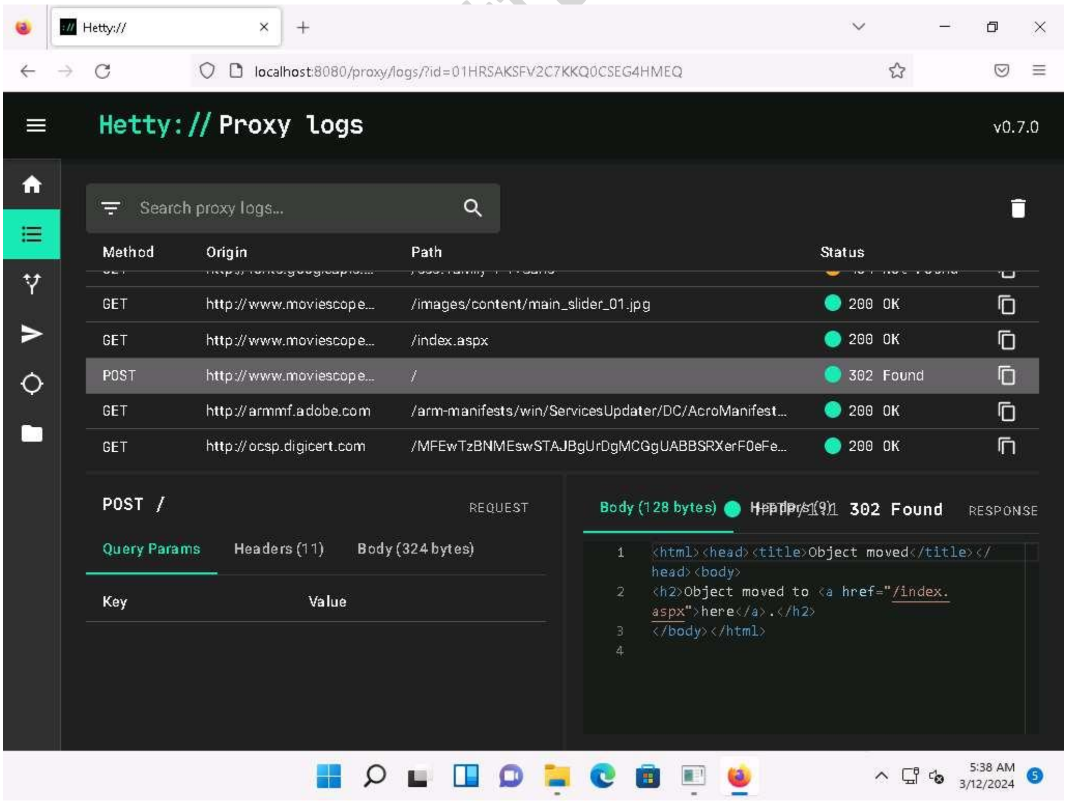


sam

••••

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.



| Method | Origin | Path | Status |
|---|---|---|---|
| GET | http://www.moviescope... | /images/content/main_slider_01.jpg | ● 200 OK |
| GET | http://www.moviescope... | /index.aspx | ● 200 OK |
| POST | http://www.moviescope... | / | ● 302 Found |
| GET | http://armmf.adobe.com | /arm-manifests/win/ServicesUpdater/DC/AcroManifest... | ● 200 OK |
| GET | http://ocsp.digicert.com | /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFe... | ● 200 OK |

POST / REQUEST

Query Params | Headers (11) | Body (324 bytes)

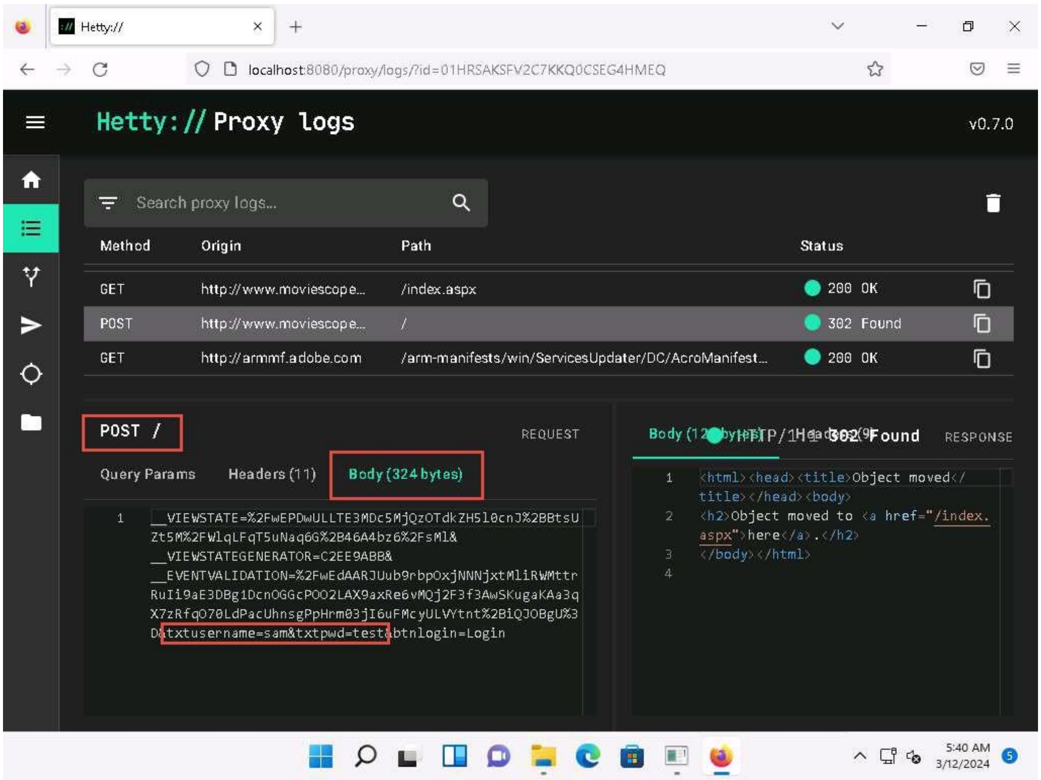
| Key | Value |
|---|---|

Body (128 bytes) | Headers (9) ● HTTP/1.1 302 Found RESPONSE

```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/index.aspx">here</a>.</h2>
</body></html>
```

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.



| Method | Origin | Path | Status |
|---|---|---|---|
| GET | http://www.moviescope... | /index.aspx | ● 200 OK |
| POST | http://www.moviescope... | / | ● 302 Found |
| GET | http://armmf.adobe.com | /arm-manifests/win/ServicesUpdater/DC/AcroManifest... | ● 200 OK |

```
__VIEWSTATE=%2FwEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ%2BBtsU
Zt5M%2FWlqLFqT5uNaq6G%2B46A4bz6%2FsMl&
__VIEWSTATEGENERATOR=C2EE9ABB&
__EVENTVALIDATION=%2FwEdAARJUub9rbpOxjNNNjxtMliRWMttr
RuIi9aE3DBg1DcnOGGcPOO2LAX9axRe6vMQj2F3f3AwSKugaKAa3q
X7zRfqO70LdPacUhnsgPpHrm03jI6uFMcyULVYtnt%2BiQJOBgU%3
D&txtusername=sam&txtpwd=test&btnlogin=Login
```

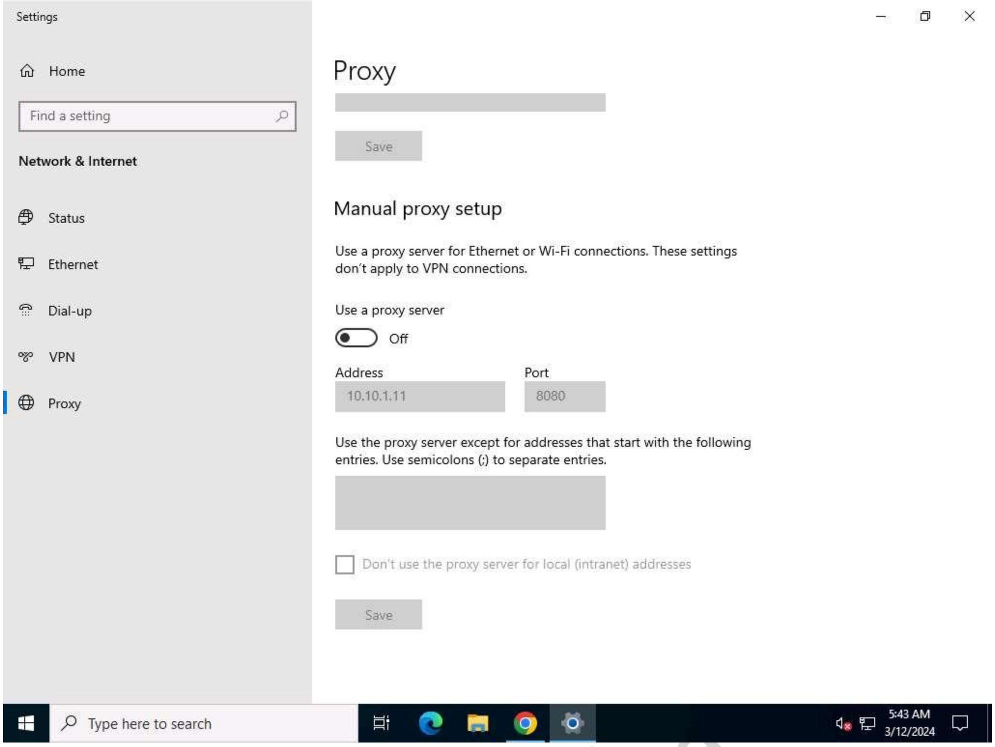
```
<html><head><title>Object moved</
title></head><body>
<h2>Object moved to <a href="/index.
aspx">here</a>.</h2>
</body></html>
```

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.



Proxy

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

Off

Address: 10.10.1.11

Port: 8080

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

□ Don't use the proxy server for local (intranet) addresses

Save

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

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

### 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.

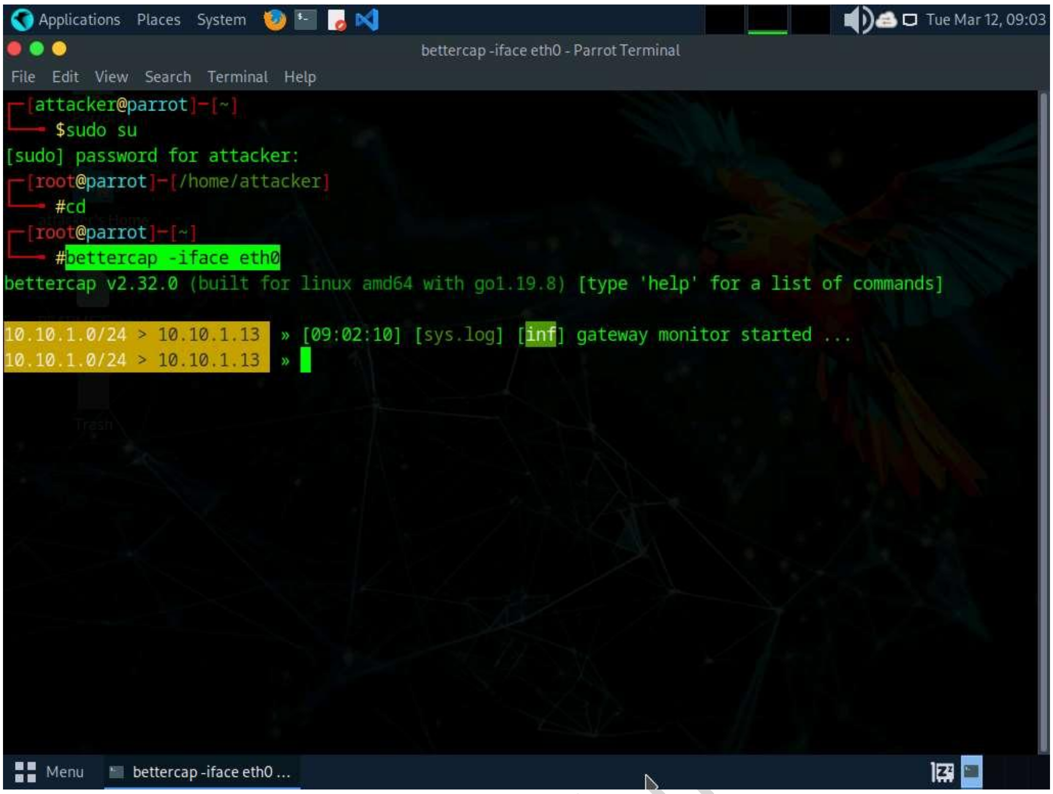
To do so, you may either follow Steps 8-11 below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

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).


Applications Places System
Tue Mar 12, 09:03
bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
Menu
bettercap -iface eth0 ...

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

10.10.1.0/24 > 10.10.1.13  » [09:02:10] [sys.log] [inf] gateway monitor started ...
10.10.1.0/24 > 10.10.1.13  »
```

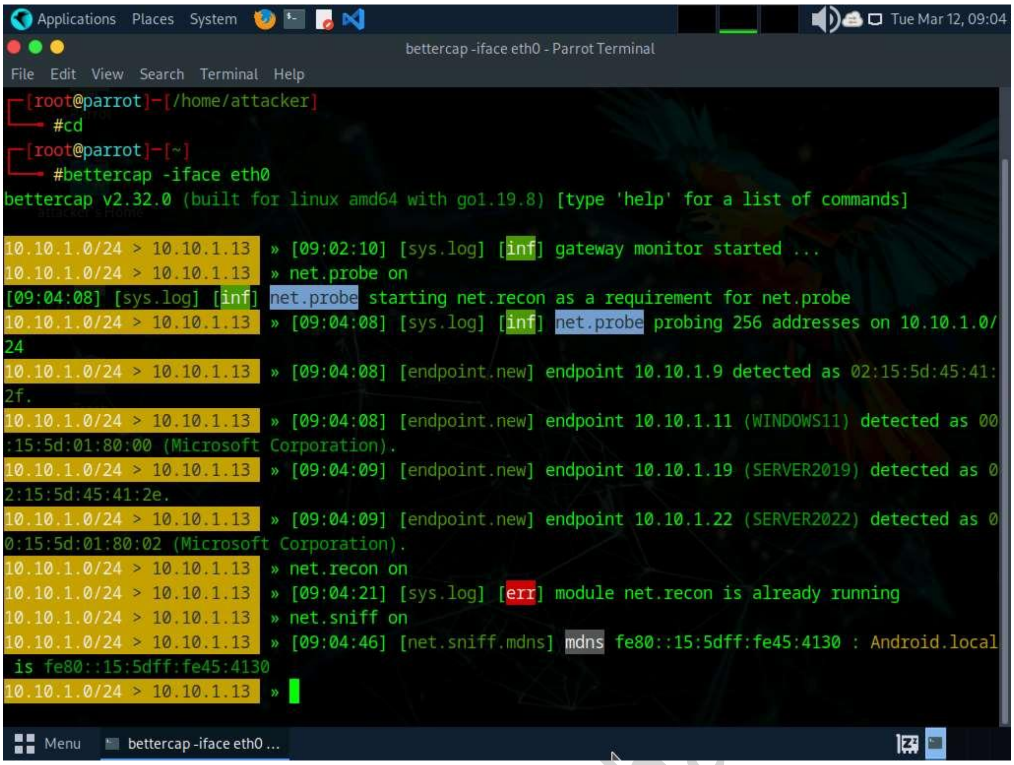
8. Type net.probe on and press Enter. This module will send different types of probe packets to each IP in the current subnet for the net.recon module to detect them.

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.

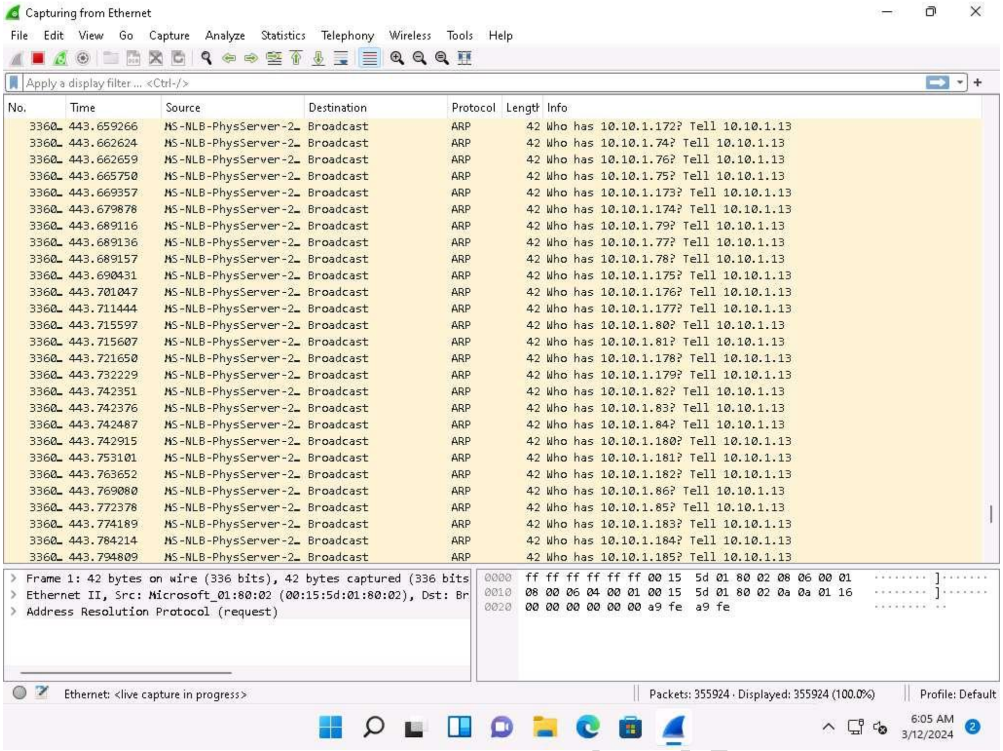


Applications Places System
Tue Mar 12, 09:04
bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
Menu
bettercap -iface eth0 ...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

10.10.1.0/24 > 10.10.1.13  » [09:02:10] [sys.log] [inf] gateway monitor started ...
10.10.1.0/24 > 10.10.1.13  » net.probe on
[09:04:08] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.10.1.0/24 > 10.10.1.13  » [09:04:08] [sys.log] [inf] net.probe probing 256 addresses on 10.10.1.0/
24
10.10.1.0/24 > 10.10.1.13  » [09:04:08] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:45:41:
2f.
10.10.1.0/24 > 10.10.1.13  » [09:04:08] [endpoint.new] endpoint 10.10.1.11 (WINDOWS11) detected as 00
:15:5d:01:80:00 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13  » [09:04:09] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:45:41:2e.
10.10.1.0/24 > 10.10.1.13  » [09:04:09] [endpoint.new] endpoint 10.10.1.22 (SERVER2022) detected as 0
0:15:5d:01:80:02 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13  » net.recon on
10.10.1.0/24 > 10.10.1.13  » [09:04:21] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13  » net.sniff on
10.10.1.0/24 > 10.10.1.13  » [09:04:46] [net.sniff.mdns] mdns fe80::15:5dff:fe45:4130 : Android.local
 is fe80::15:5dff:fe45:4130
10.10.1.0/24 > 10.10.1.13  » 
```

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.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
6:05 AM
3/12/2024

```
No.     Time        Source              Destination  Protocol Length Info
  3360… 443.659266  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.172? Tell 10.10.1.13
  3360… 443.662624  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.74? Tell 10.10.1.13
  3360… 443.662659  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.76? Tell 10.10.1.13
  3360… 443.665750  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.75? Tell 10.10.1.13
  3360… 443.669357  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.173? Tell 10.10.1.13
  3360… 443.679878  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.174? Tell 10.10.1.13
  3360… 443.689116  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.79? Tell 10.10.1.13
  3360… 443.689136  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.77? Tell 10.10.1.13
  3360… 443.689157  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.78? Tell 10.10.1.13
  3360… 443.690431  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.175? Tell 10.10.1.13
  3360… 443.701047  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.176? Tell 10.10.1.13
  3360… 443.711444  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.177? Tell 10.10.1.13
  3360… 443.715597  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.80? Tell 10.10.1.13
  3360… 443.715607  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.81? Tell 10.10.1.13
  3360… 443.721650  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.178? Tell 10.10.1.13
  3360… 443.732229  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.179? Tell 10.10.1.13
  3360… 443.742351  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.82? Tell 10.10.1.13
  3360… 443.742376  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.83? Tell 10.10.1.13
  3360… 443.742487  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.84? Tell 10.10.1.13
  3360… 443.742915  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.180? Tell 10.10.1.13
  3360… 443.753101  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.181? Tell 10.10.1.13
  3360… 443.763652  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.182? Tell 10.10.1.13
  3360… 443.769080  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.86? Tell 10.10.1.13
  3360… 443.772378  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.85? Tell 10.10.1.13
  3360… 443.774189  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.183? Tell 10.10.1.13
  3360… 443.784214  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.184? Tell 10.10.1.13
  3360… 443.794809  MS-NLB-PhysServer-2… Broadcast   ARP        42 Who has 10.10.1.185? Tell 10.10.1.13
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits
> Ethernet II, Src: Microsoft_01:80:02 (00:15:5d:01:80:02), Dst: Br
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 15  5d 01 80 02 08 06 00 01   ········ ]·······
0010  08 00 06 04 00 01 00 15  5d 01 80 02 0a 0a 01 16   ········ ]·······
0020  00 00 00 00 00 00 a9 fe  a9 fe                     ········ ··
```

```
Ethernet: <live capture in progress>    Packets: 355924 · Displayed: 355924 (100.0%)    Profile: Default
```

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.