Module 11: Session Hijacking

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 Zed Attack Proxy (ZAP)
- Intercept HTTP traffic using bettercap
- 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 Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

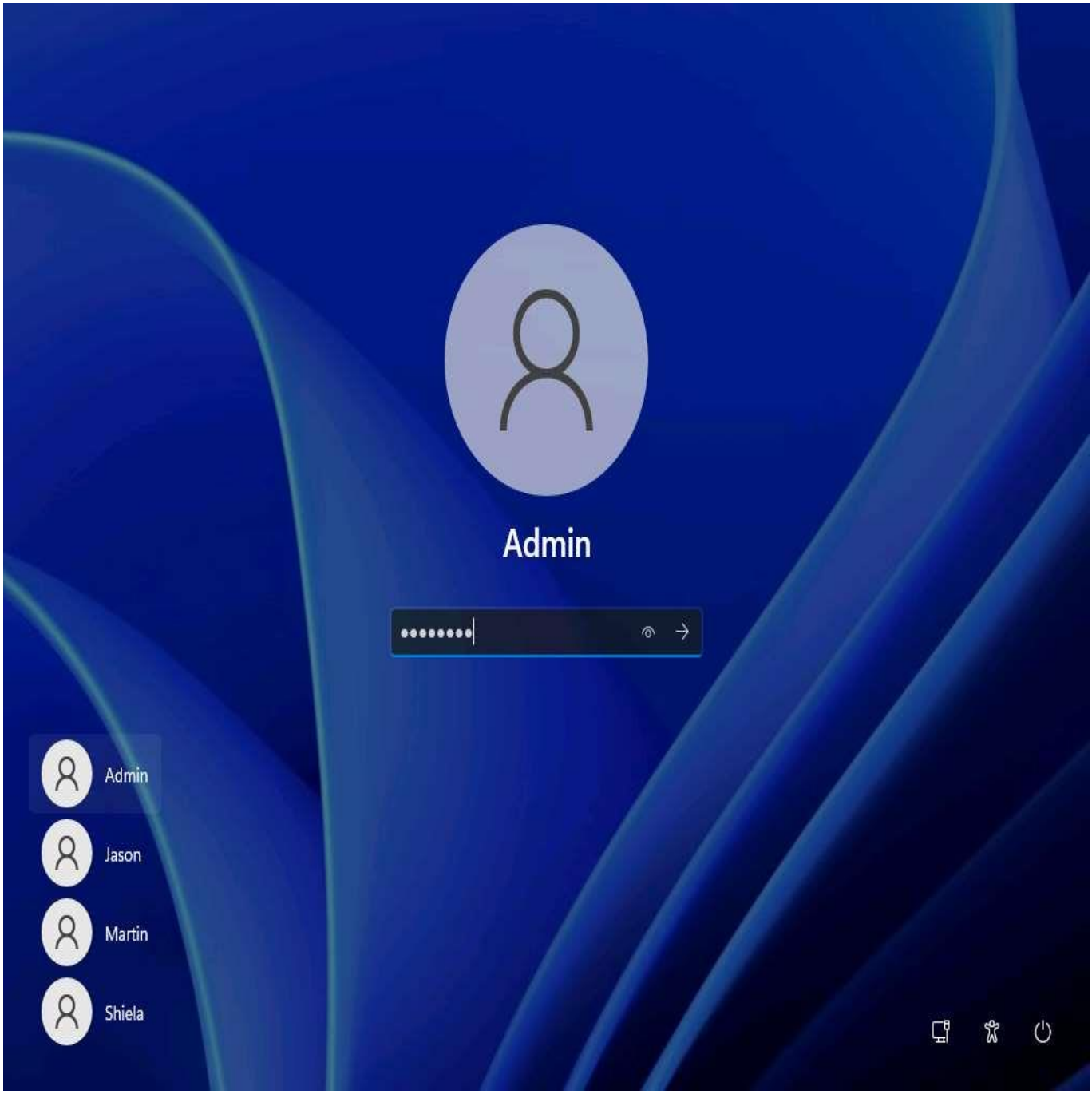
Before starting this task, we need to configure the proxy settings in the victim's machine, which in this task will be the **Windows 11** machine.

1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete.

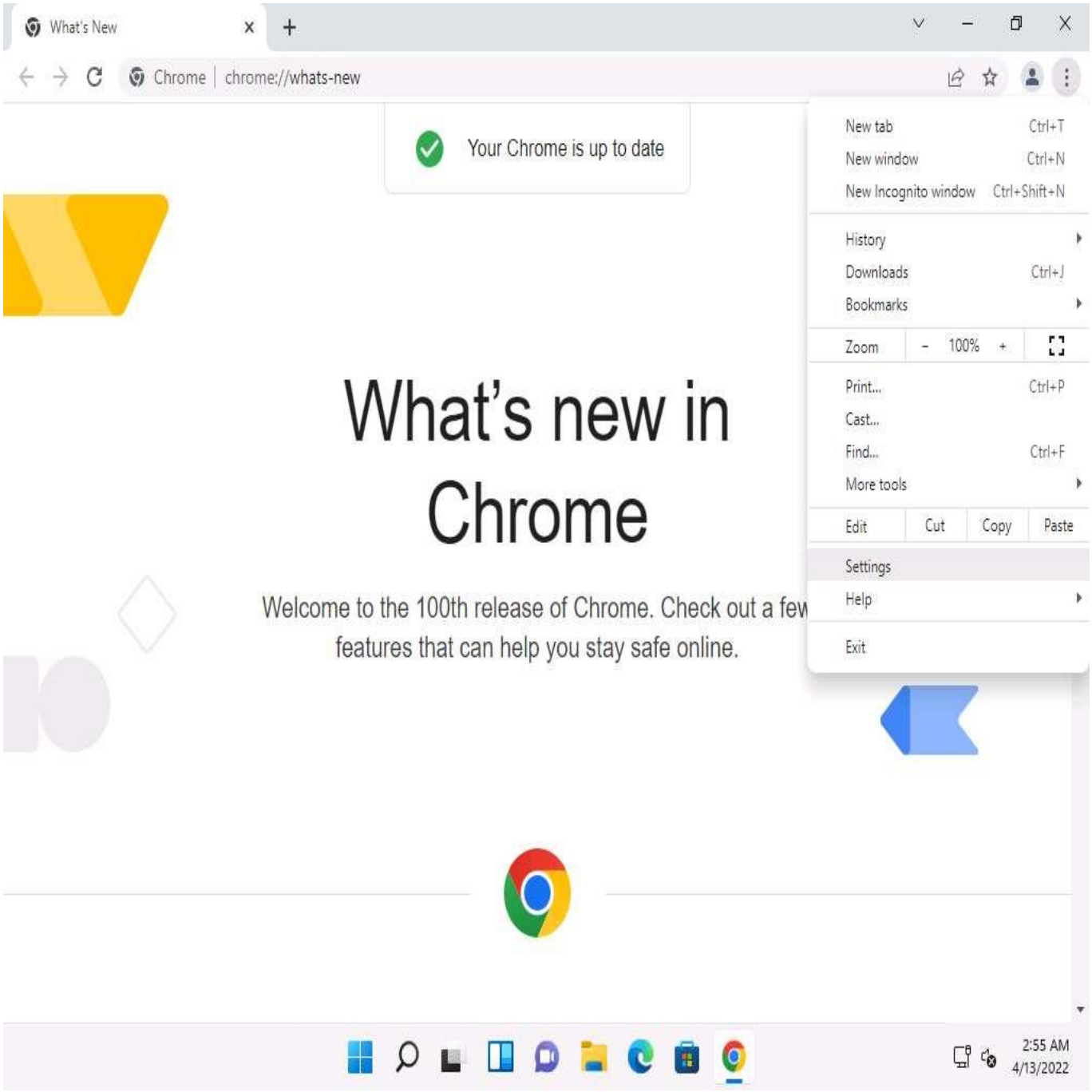
   Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

2. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

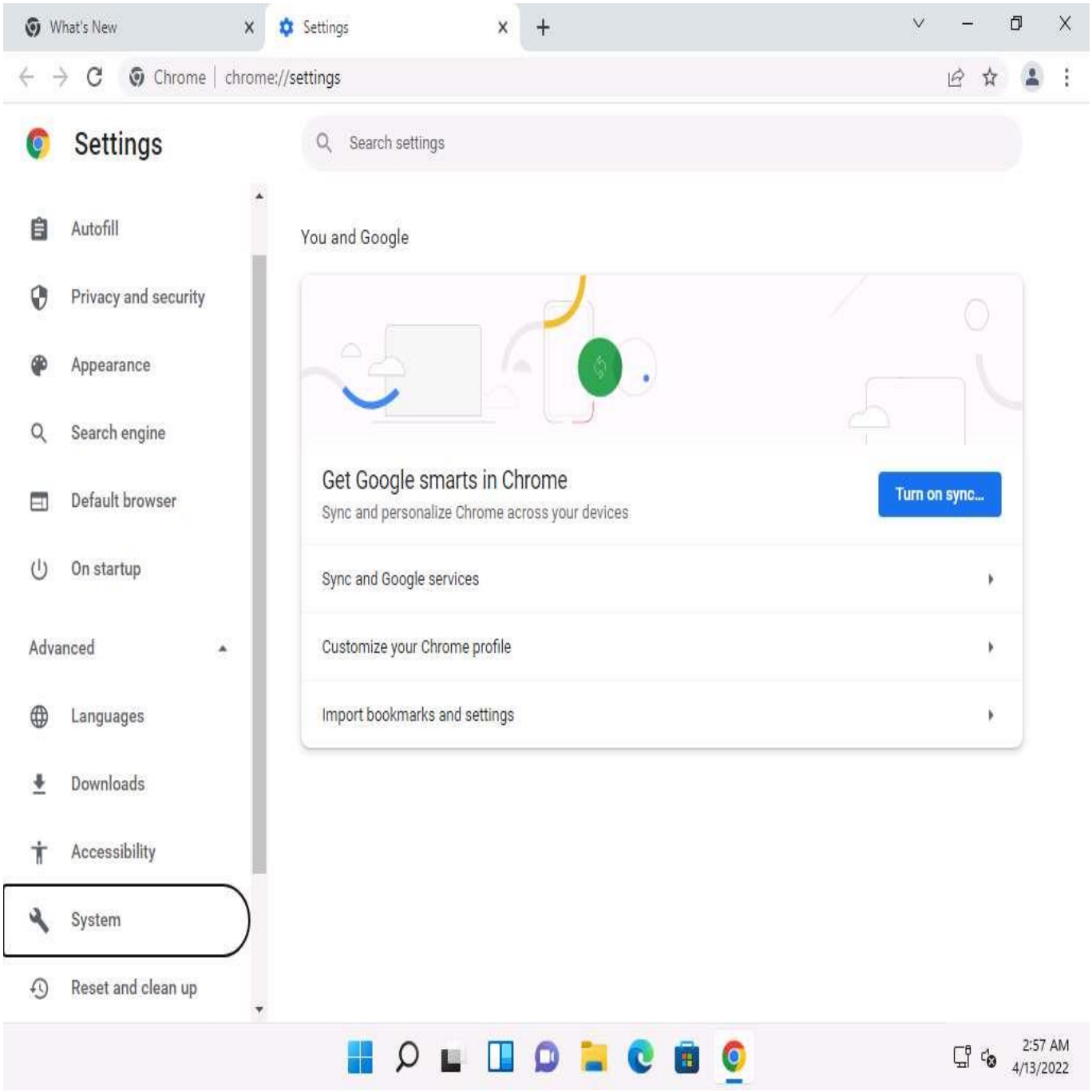
Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
If **Welcome to Windows** wizard appears, click Continue. In the **Sign in with Microsoft** wizard click **Cancel** to continue.
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



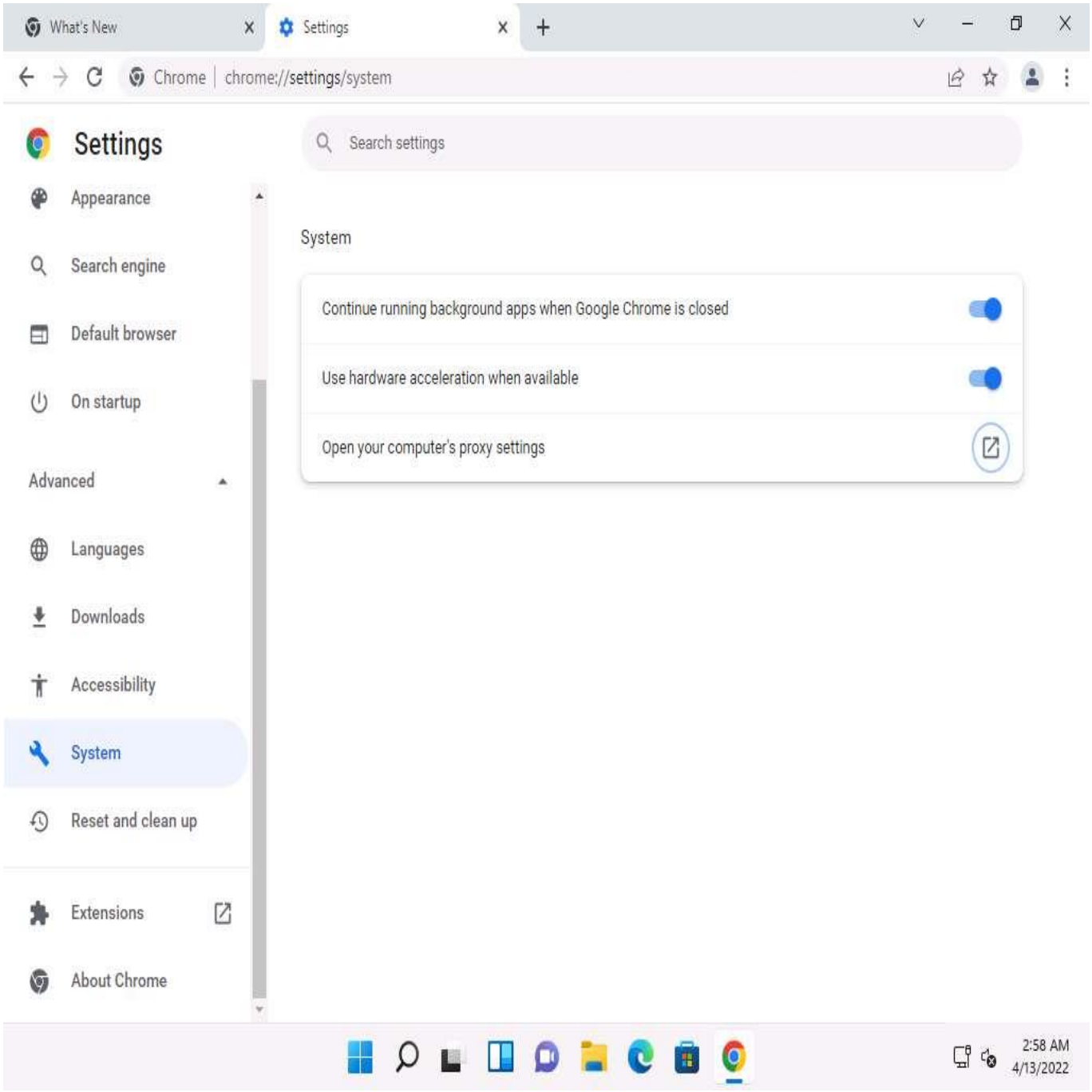
3. Open any web browser (here, **Google Chrome**), click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



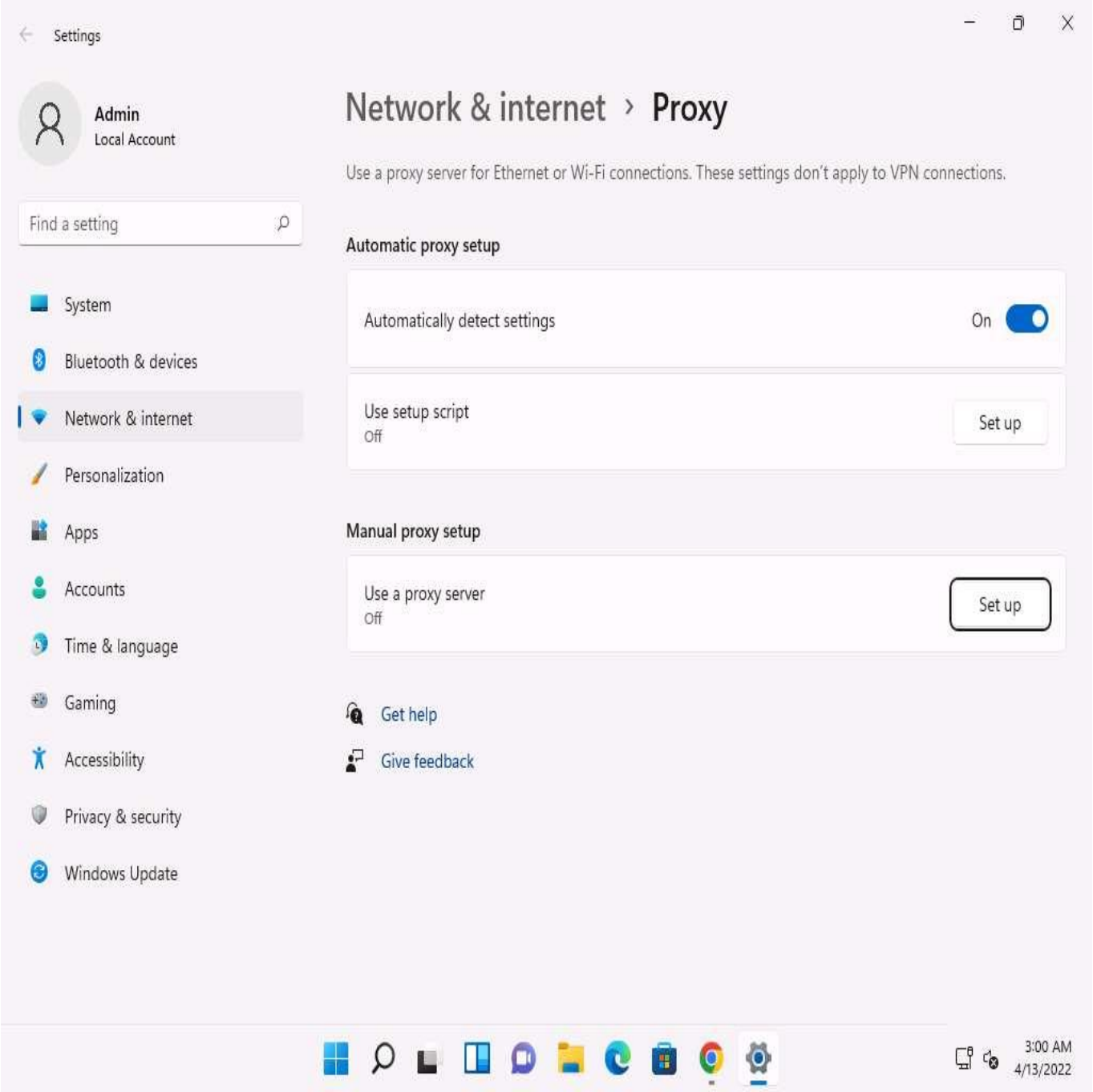
4. ☐ On the **Settings** page, scroll down, expand the **Advanced** settings and select **System** option from the left pane.



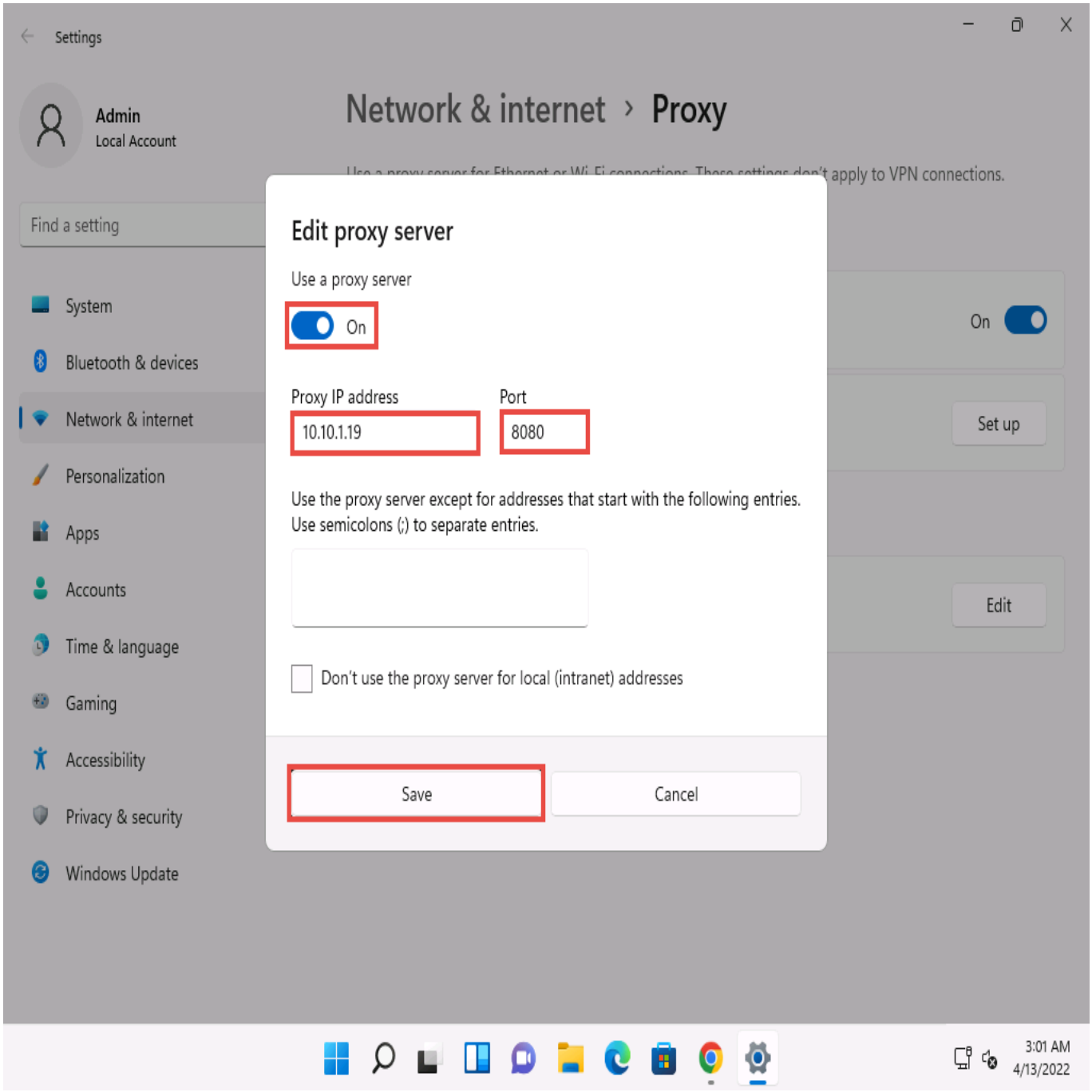
5. **System** page appears and click **Open your computer's proxy settings** to configure a proxy.



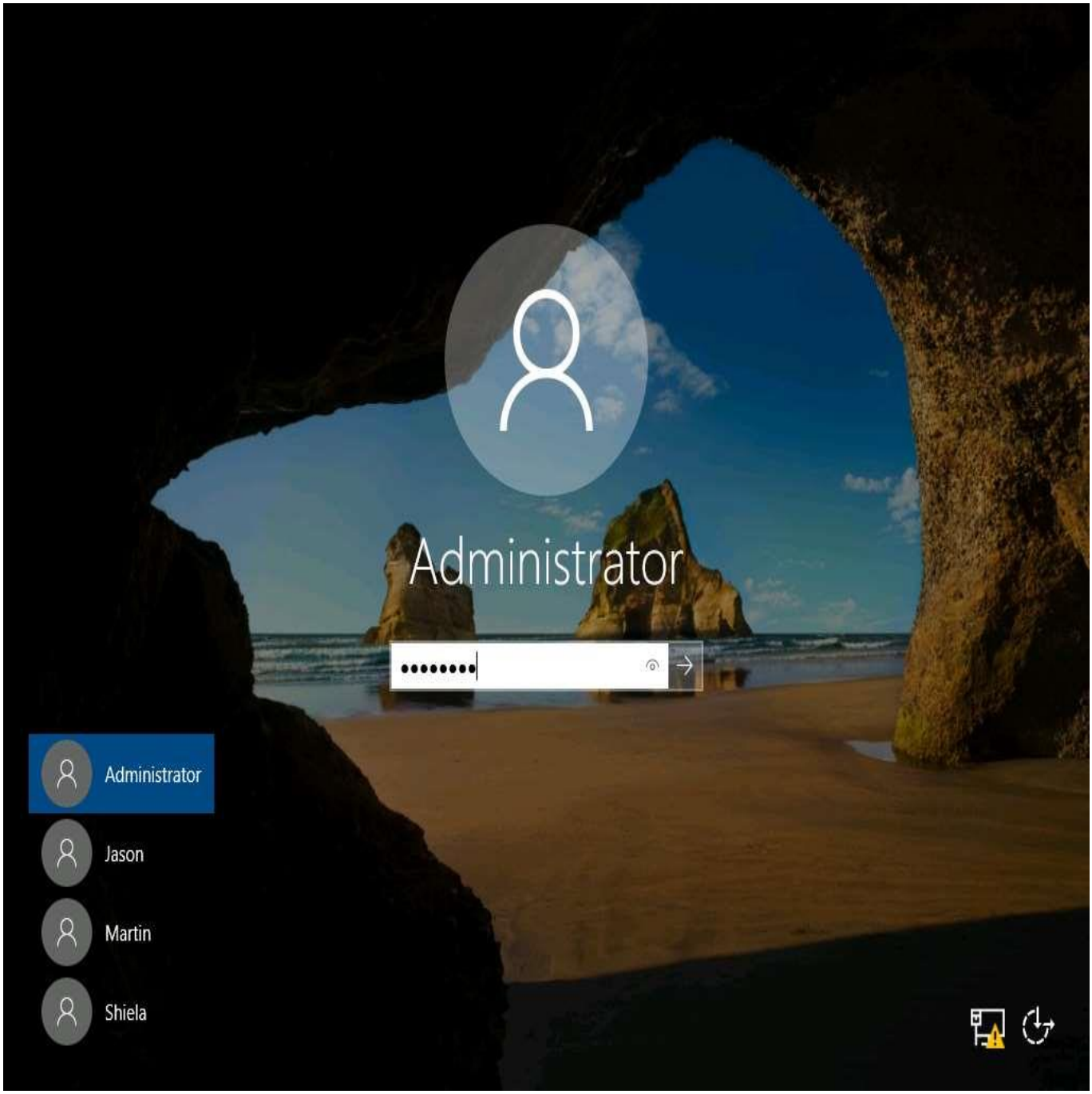
6. ☐ A **Settings** window opens, with the **Proxy** settings in the right pane.
7. ☐ Click **Set up** button under **Manual proxy setup** section.



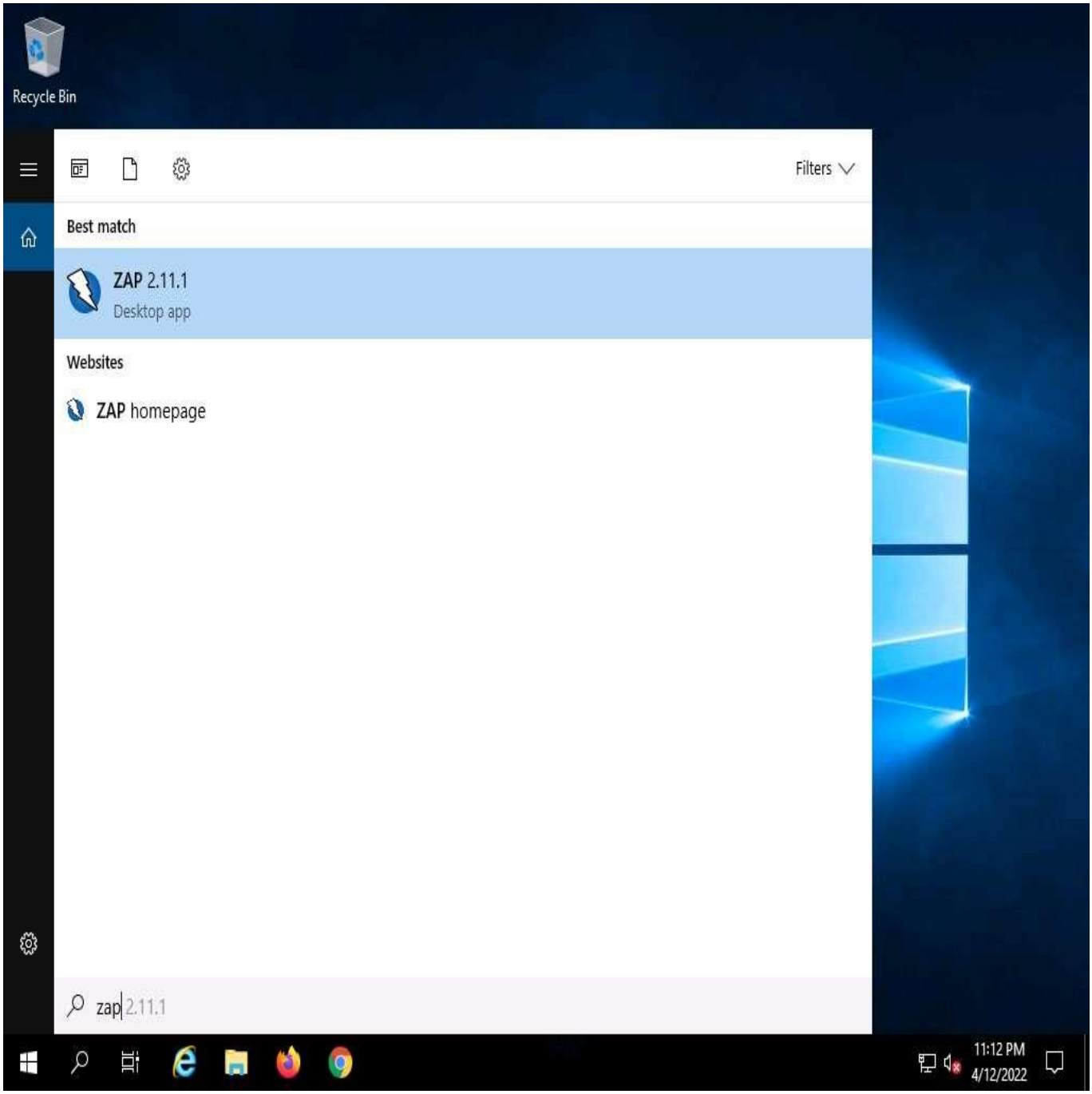
8. **Edit proxy server** window appears, make the following changes:
   - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
   - In the **Proxy IP address** field, type **10.10.1.19** (the IP address of the attacker's machine).
   - In the **Port** field, type **8080**.
   - Click **Save**.



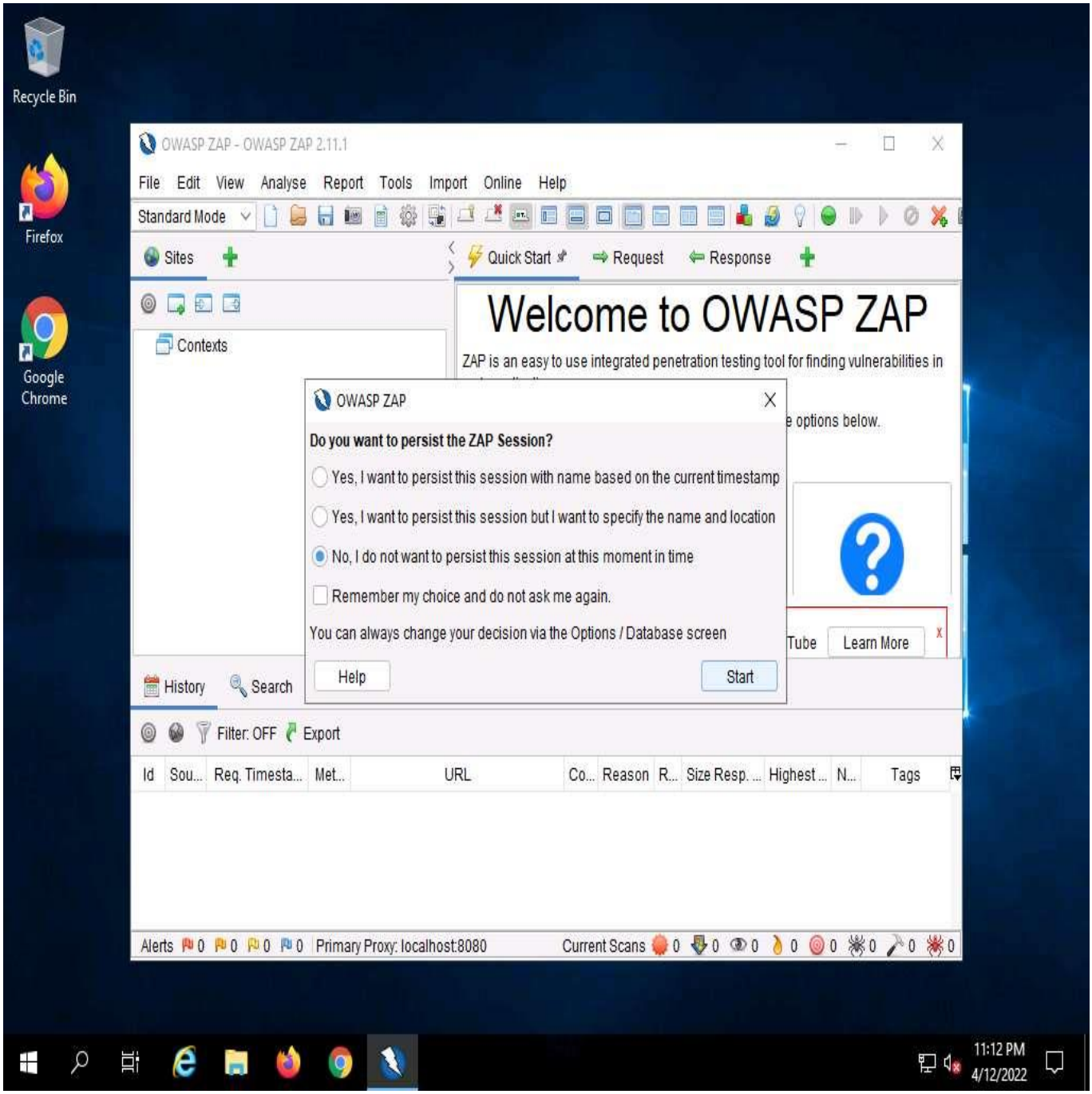
9. ☐ After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
10. ☐ Click Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**



11. ☐ Click **Type here to search** icon ( ) on the **Desktop**. Type **zap** in the search field, the **ZAP 2.11.1** appears in the result, press **Enter** to launch it.



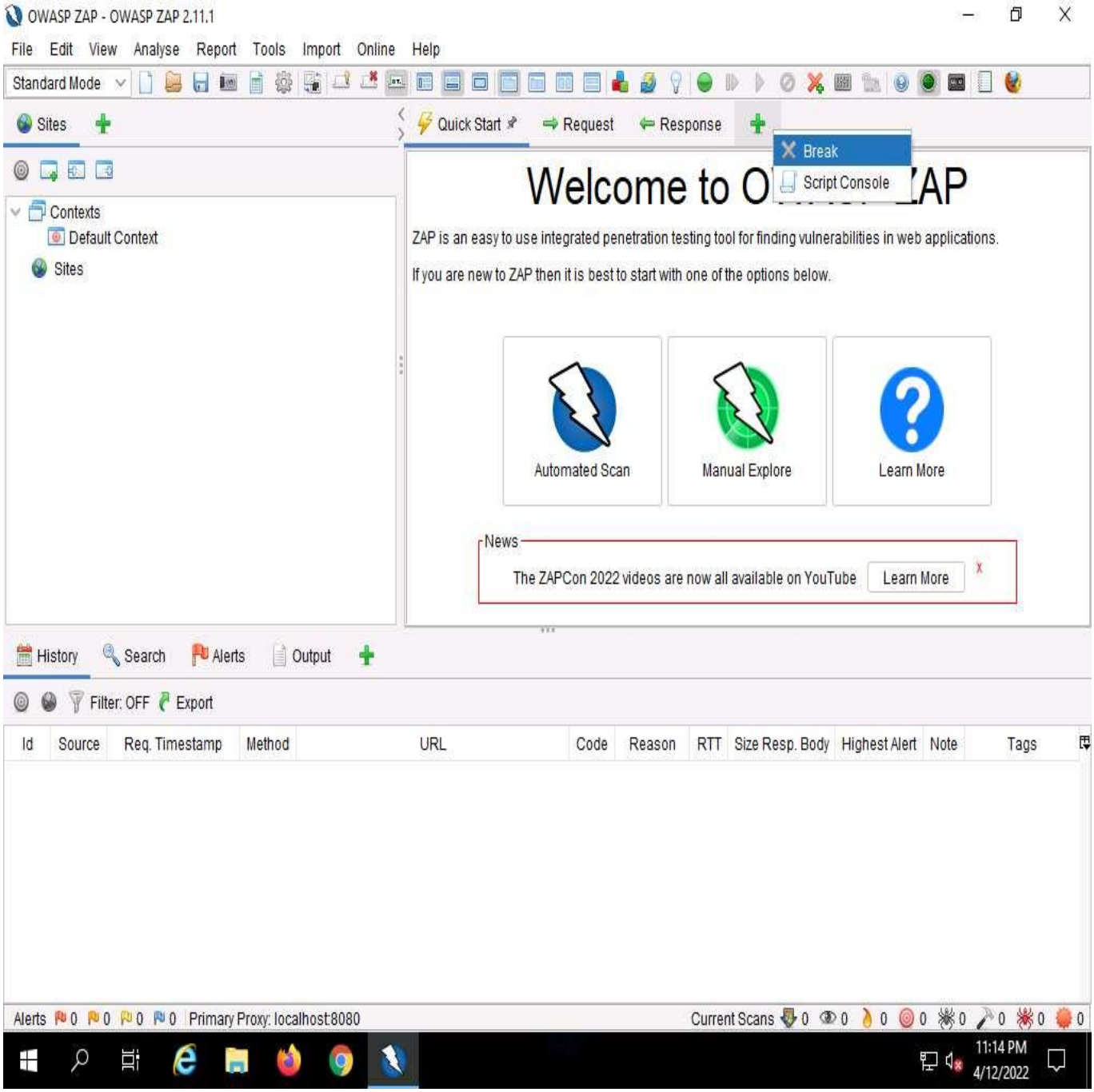
12. **OWASP ZAP** initializes and a prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.



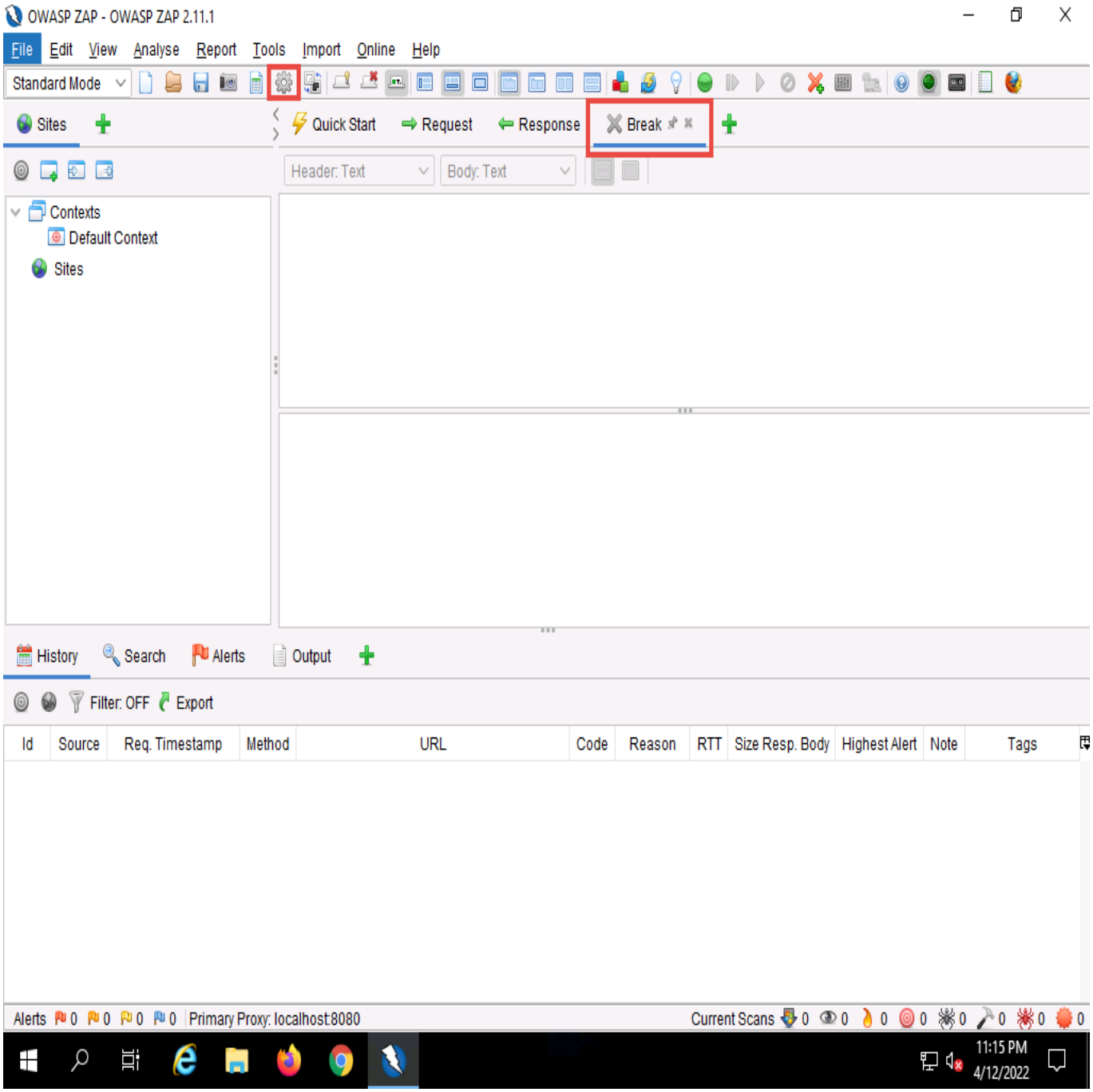
13. ☐ The **OWASP ZAP** main window appears. Click on the "**+**" icon in the right pane and select **Break** from the options.

If a OWASP ZAP pop-up appears, click **OK** in all the pop-ups.
The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

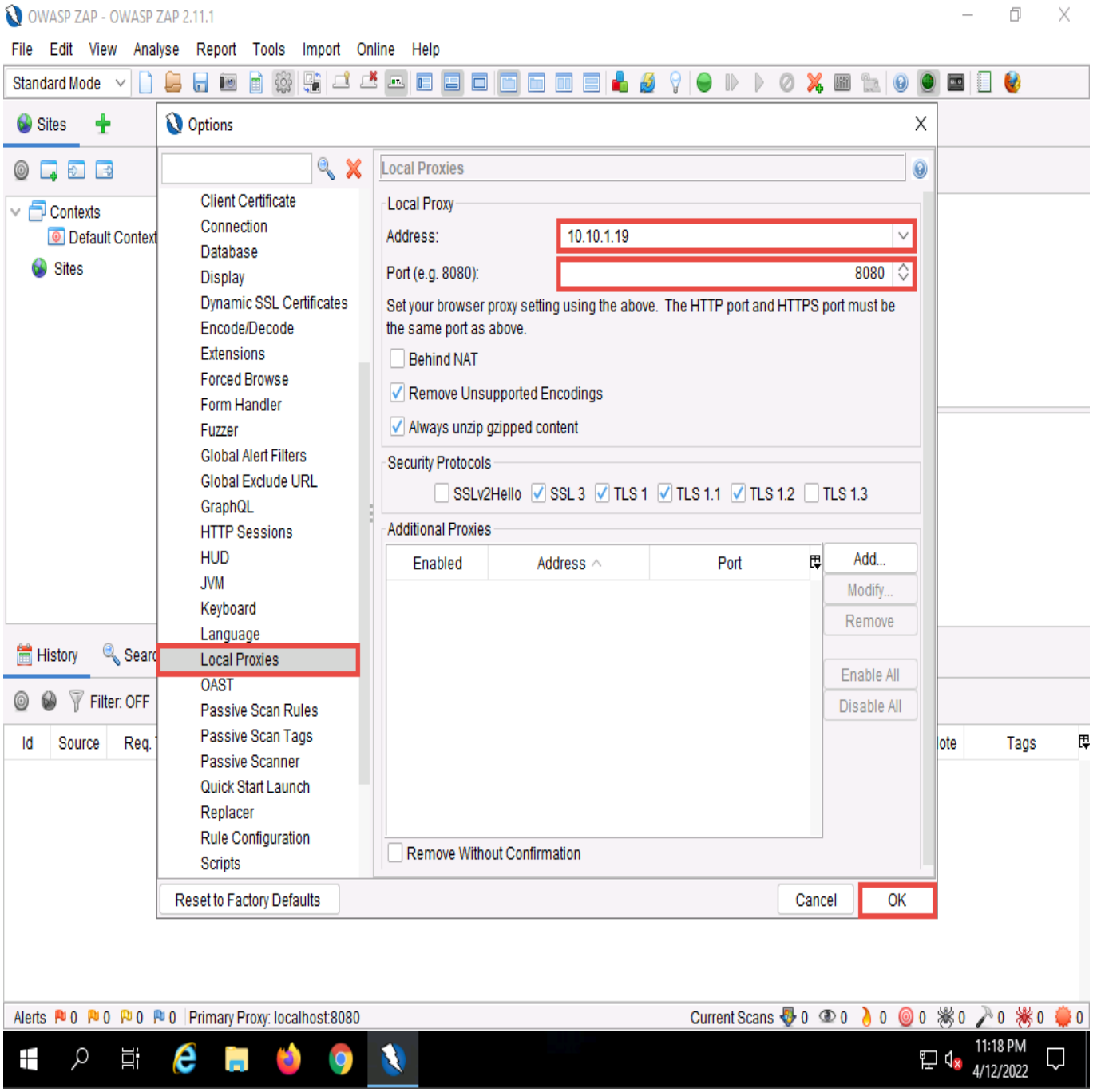
- The header
- Hidden fields
- Disabled fields
- Fields that use JavaScript to filter out illegal characters



14. ☐ The **Break** tab is added to your **OWASP ZAP** window.
15. ☐ To configure ZAP as a proxy, click the **Options...** icon from the toolbar.

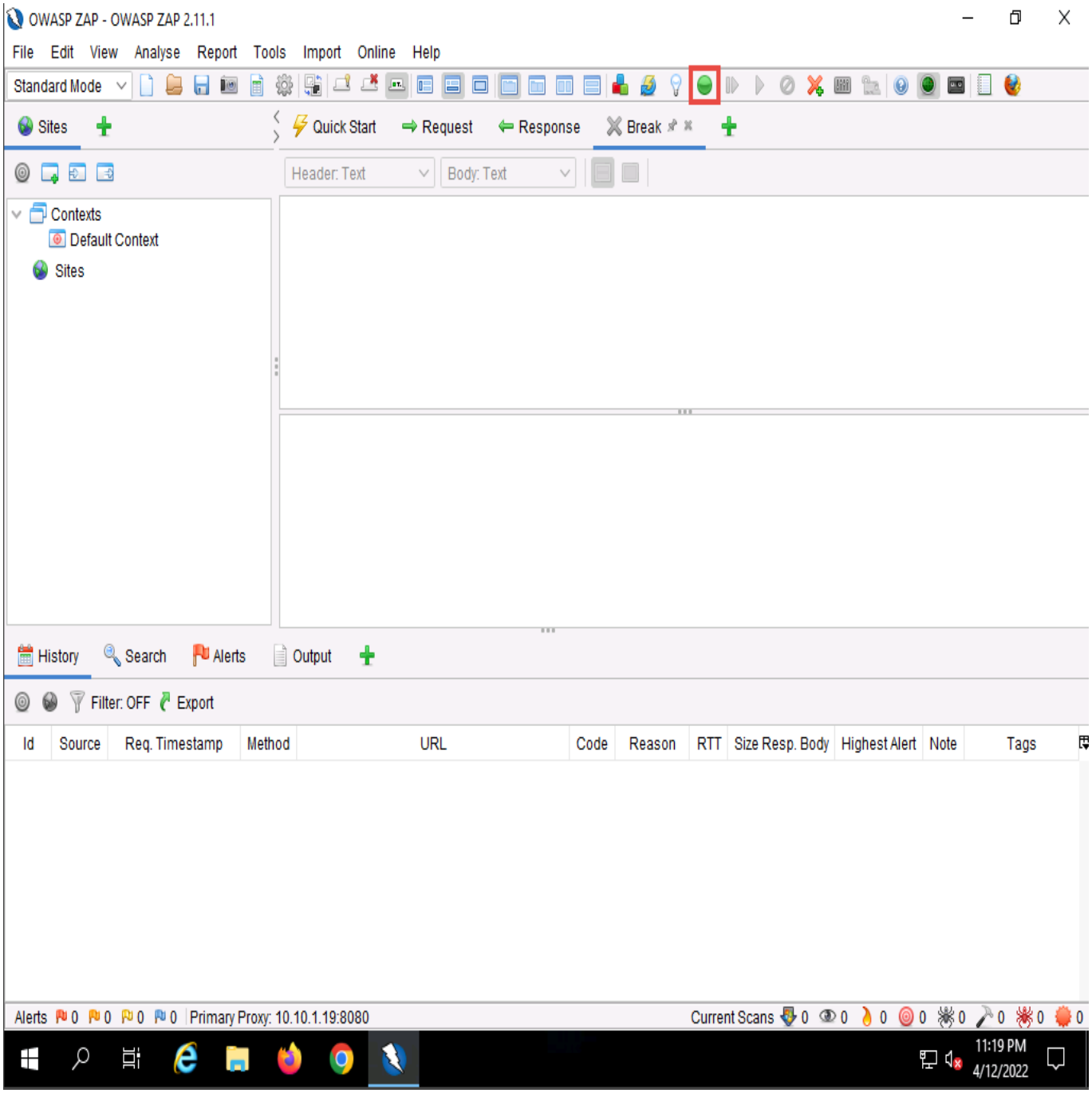


16. ☐ In the **Options** window, scroll-down in the left-pane and click **Local Proxies**. In the right pane, under the **Local Proxy** section, type **10.10.1.19** (the IP address of the **Windows Server 2019** machine) in the **Address** field and leave the **Port** value to the default, **8080**; click **OK**.

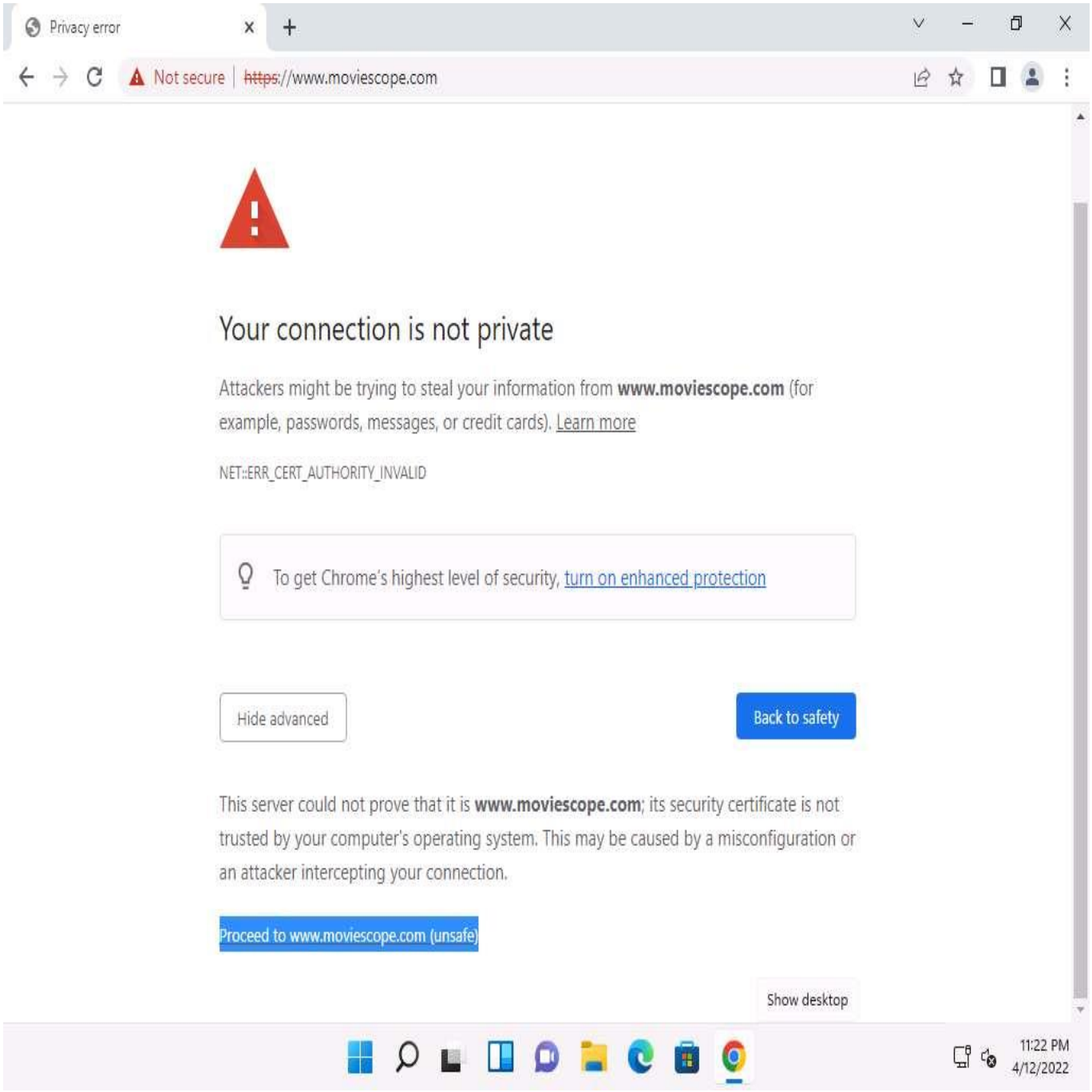


17. ☐ Click the **Set break on all requests and responses** icon on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

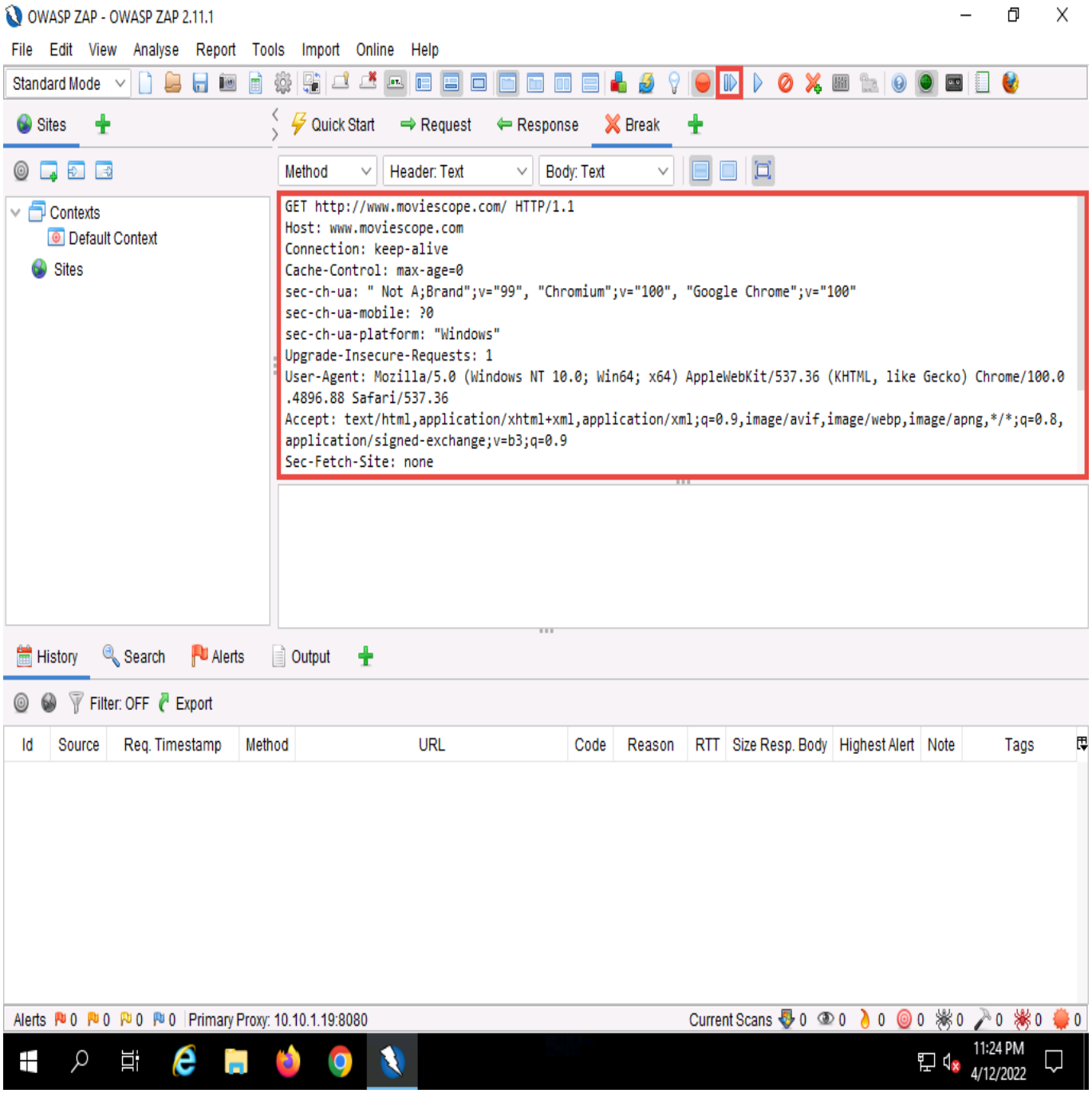
The **Set break on all requests and responses** icon turns automatically from green to red.



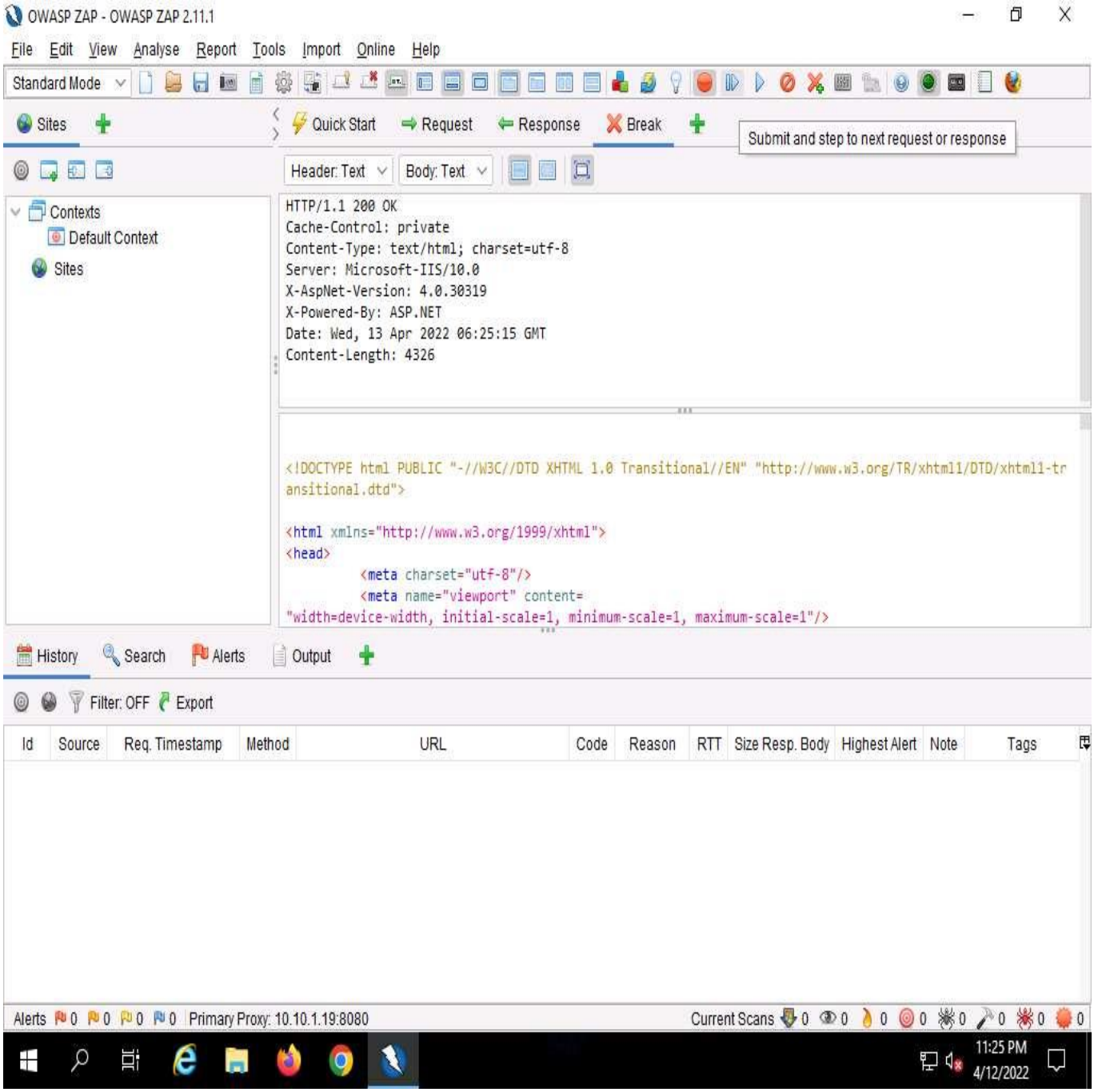
18. ☐ Now, click Windows 11 to switch back to the victim's machine (**Windows 11**) and launch the same browser in which you configured the proxy settings. In this task, we have configured the **Google Chrome** browser.
19. ☐ Place your mouse cursor in the address bar, type **www.moviescope.com** and press **Enter**.
20. ☐ A message appears, stating that **Your connection is not private**. Click the **Advanced** button.
21. ☐ On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.



22. ☐ Now, click Windows Server 2019 to switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.
23. ☐ In Steps **19-21**, we have visited **www.moviescope.com** in the victim's browser. Look in the **Break** tab and click the **Submit and step to next request or response** icon on the toolbar to capture the **www.moviescope.com** request.



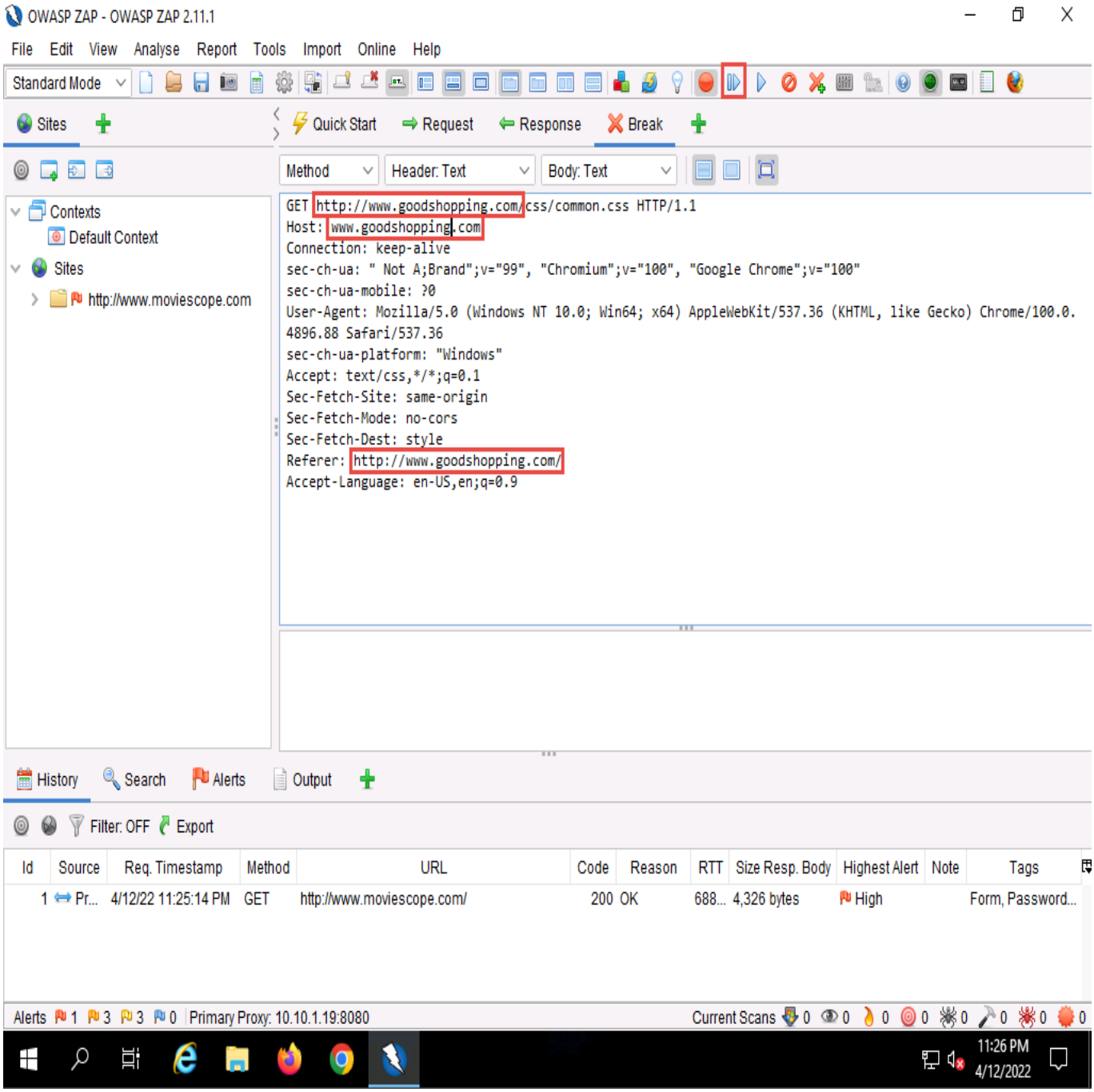
24. ☐ A **HTTP response** appears; click the **Submit and step to next request or response** icon again on the toolbar.



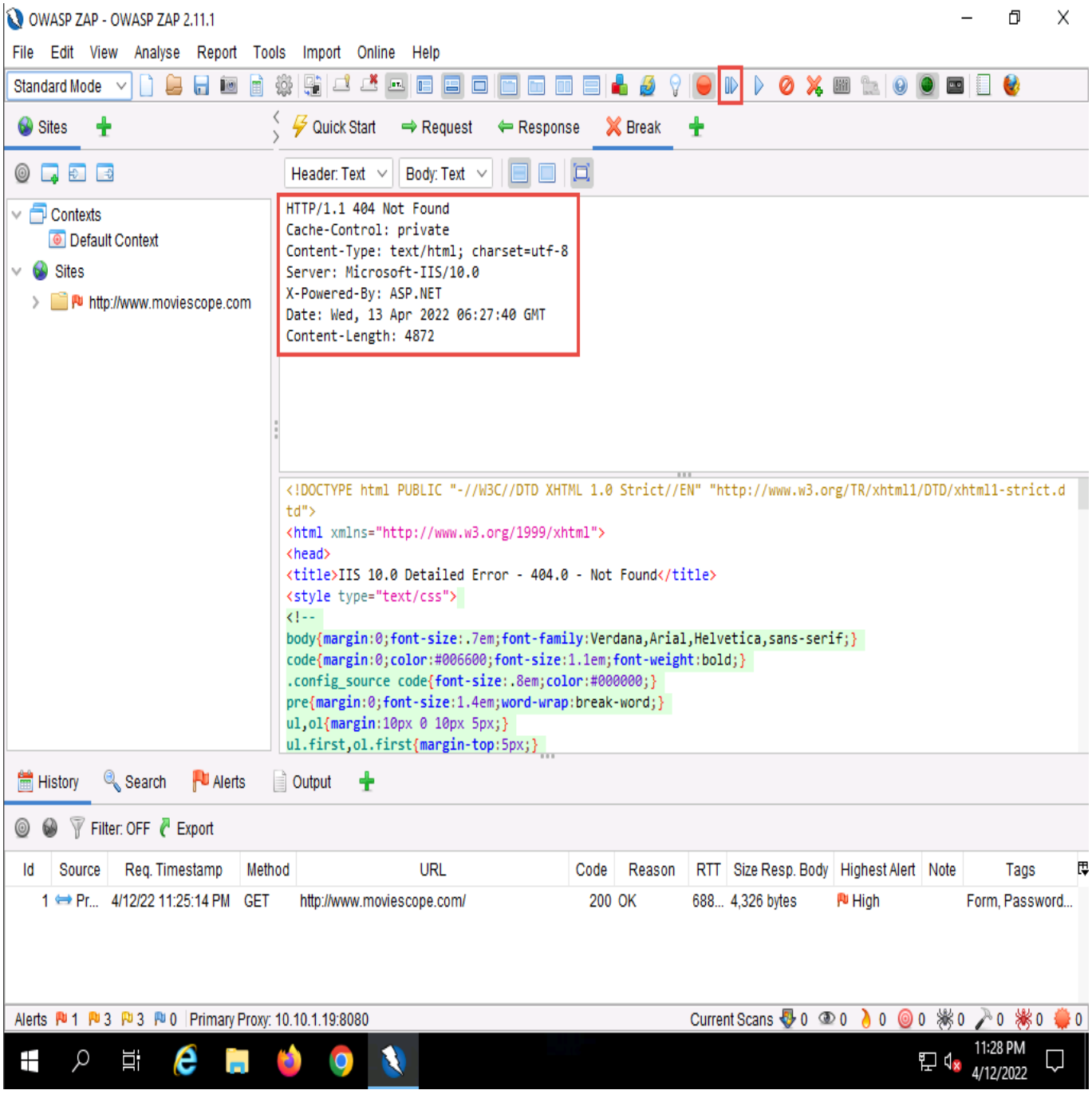
25. ☐ Now, in the **Break** tab, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests.

If you find any URL starting with **https**, modify it to **http**.

26. ☐ Once you have modified the GET requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic to the victim's machine.



27. ☐ In all the **HTTP Not Found** requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic.



28. ☐ In a similar way, modify every **GET** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

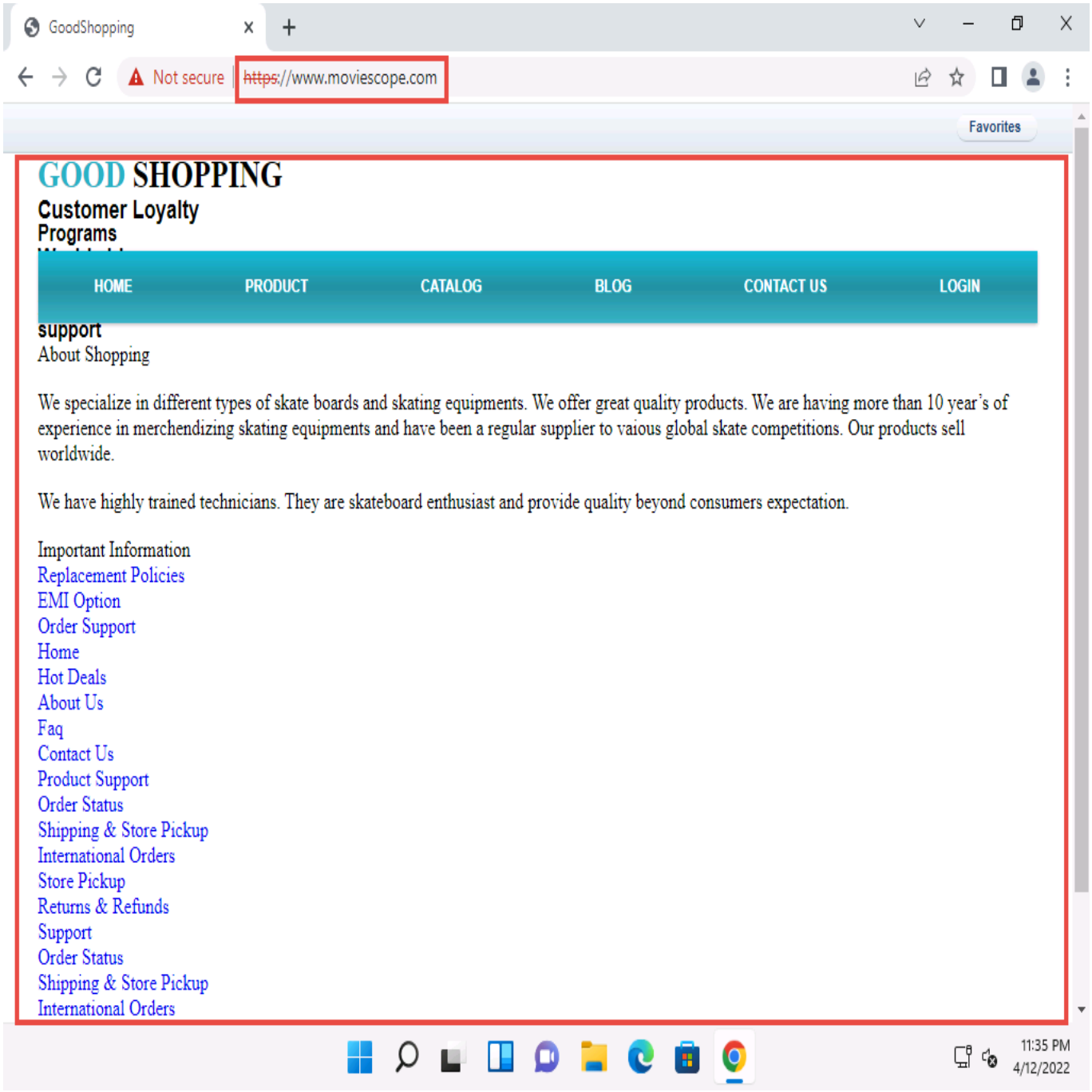
You will need to switch back and forth from the victim's machine to see the browser status while you do this.

If you do not receive any request or you see a blank break tab then switch to **Windows 11** machine and refresh the browser to capture the request again.

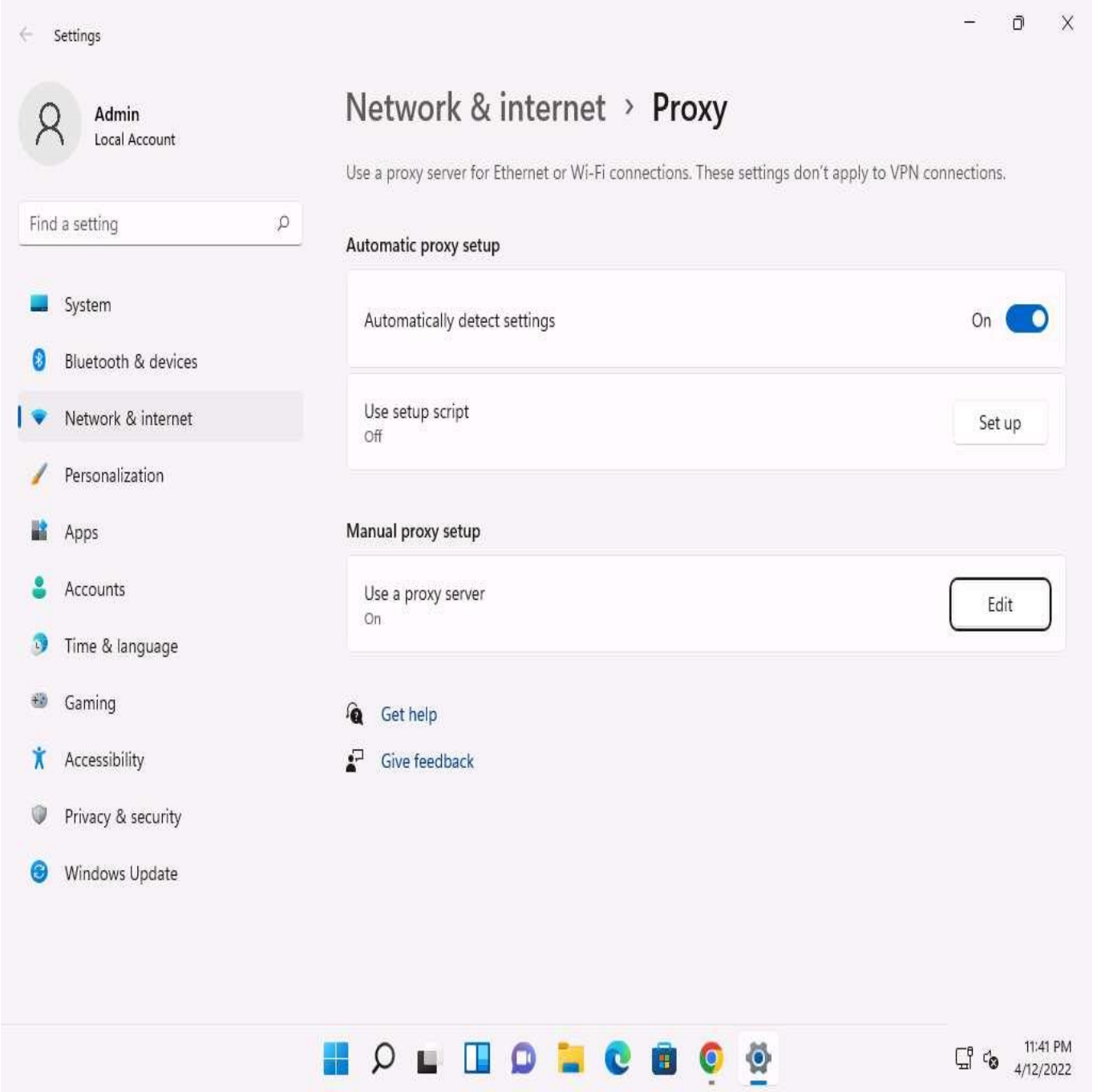
29. ☐ Now, click on Windows 11 to switch to the victim's machine (**Windows 11**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

It takes multiple iterations to open the Good Shopping site in the victim's machine.

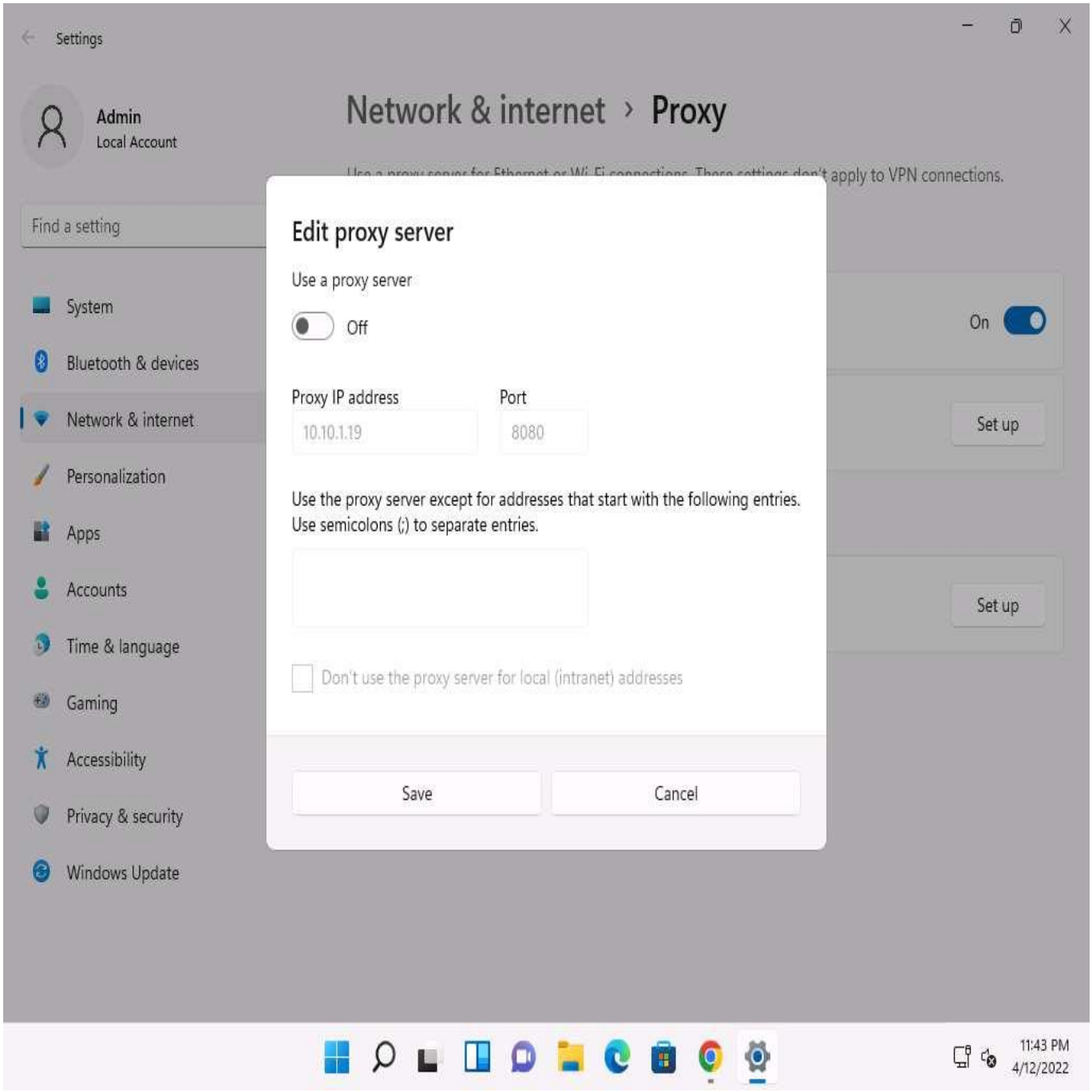
30. ☐ The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www. moviescope.com**, the window displays **www.goodshopping.com**.



31. ☐ Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 3-5** again.
32. ☐ In the **Settings** window, under the **Manual proxy setup** section in the right-pane, click the **Edit** button.



33. **Edit proxy server** window appears, under the **Use a proxy server** option, click the **On** button to switch it **Off** and click **Save**.



34. ☐ This concludes the demonstration of performing session hijacking using ZAP.
35. ☐ Close all open windows and document all the acquired information.

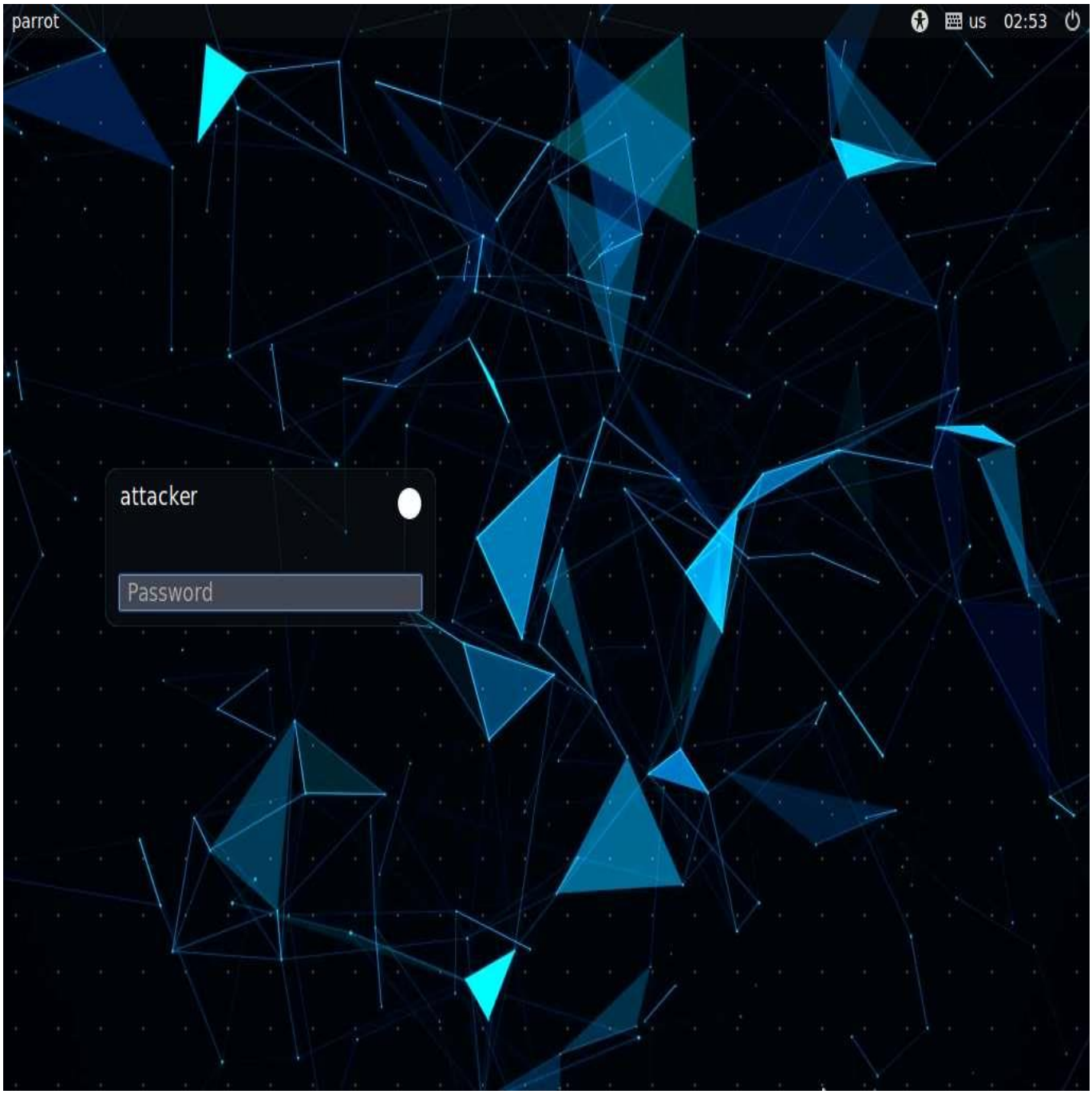
Task 2: Intercept HTTP Traffic using bettercap

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

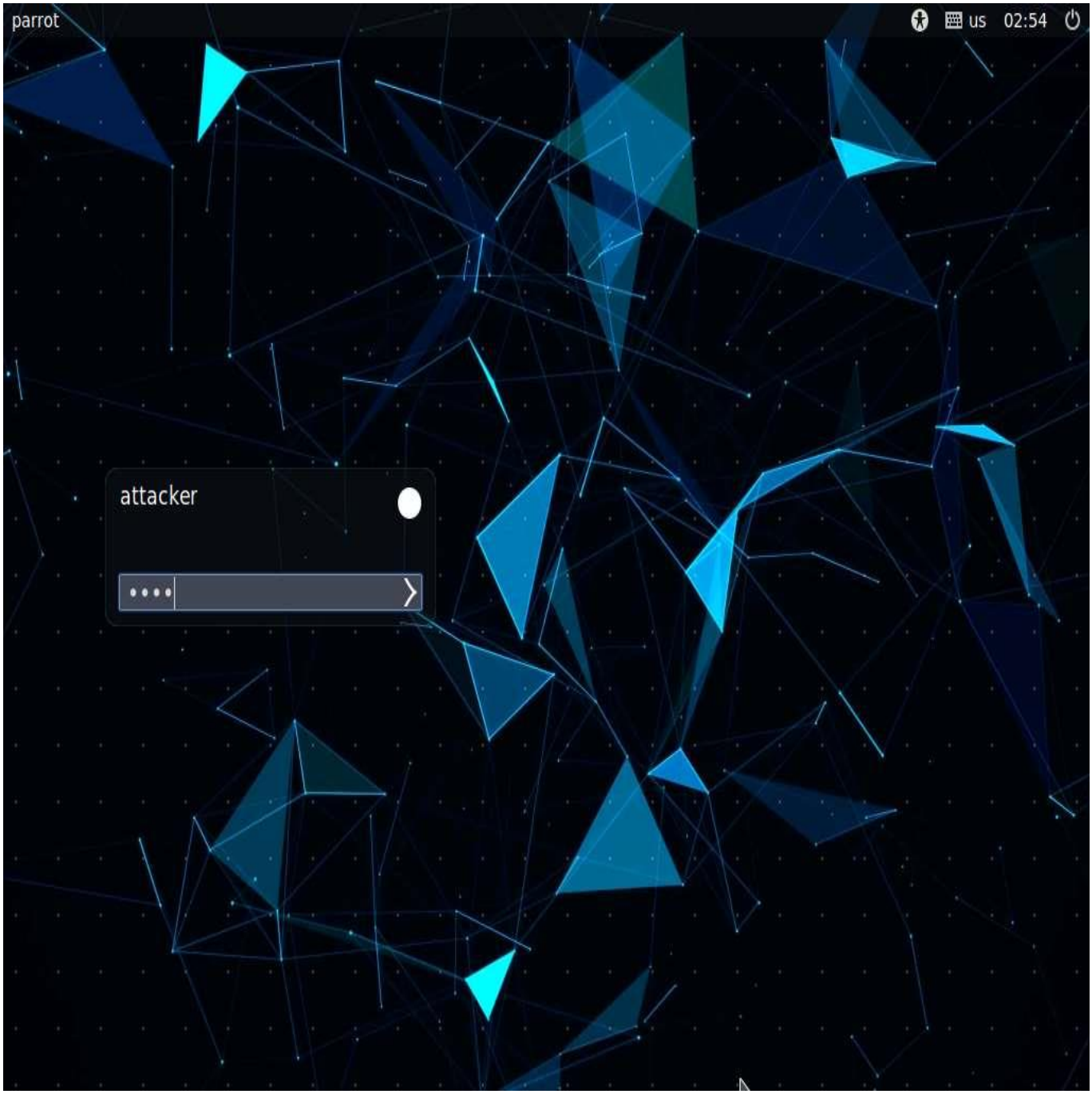
An ethical hacker or a penetration tester, you must know how MITM attacks work, so that you can protect your organization's sensitive information from them. bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network; manipulate HTTP, HTTPS, and TCP traffic in real-time; sniff for credentials; etc.

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

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

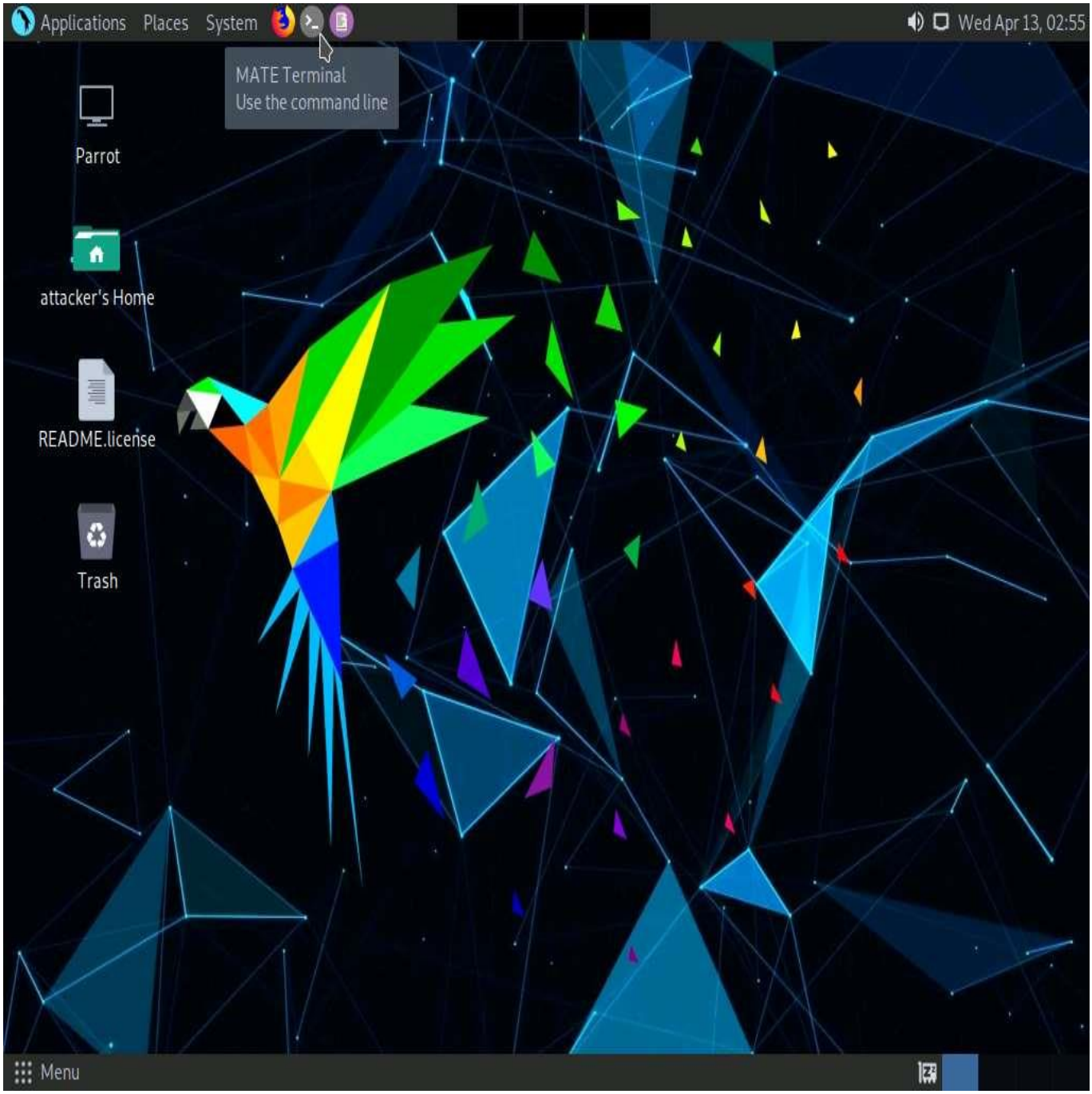


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

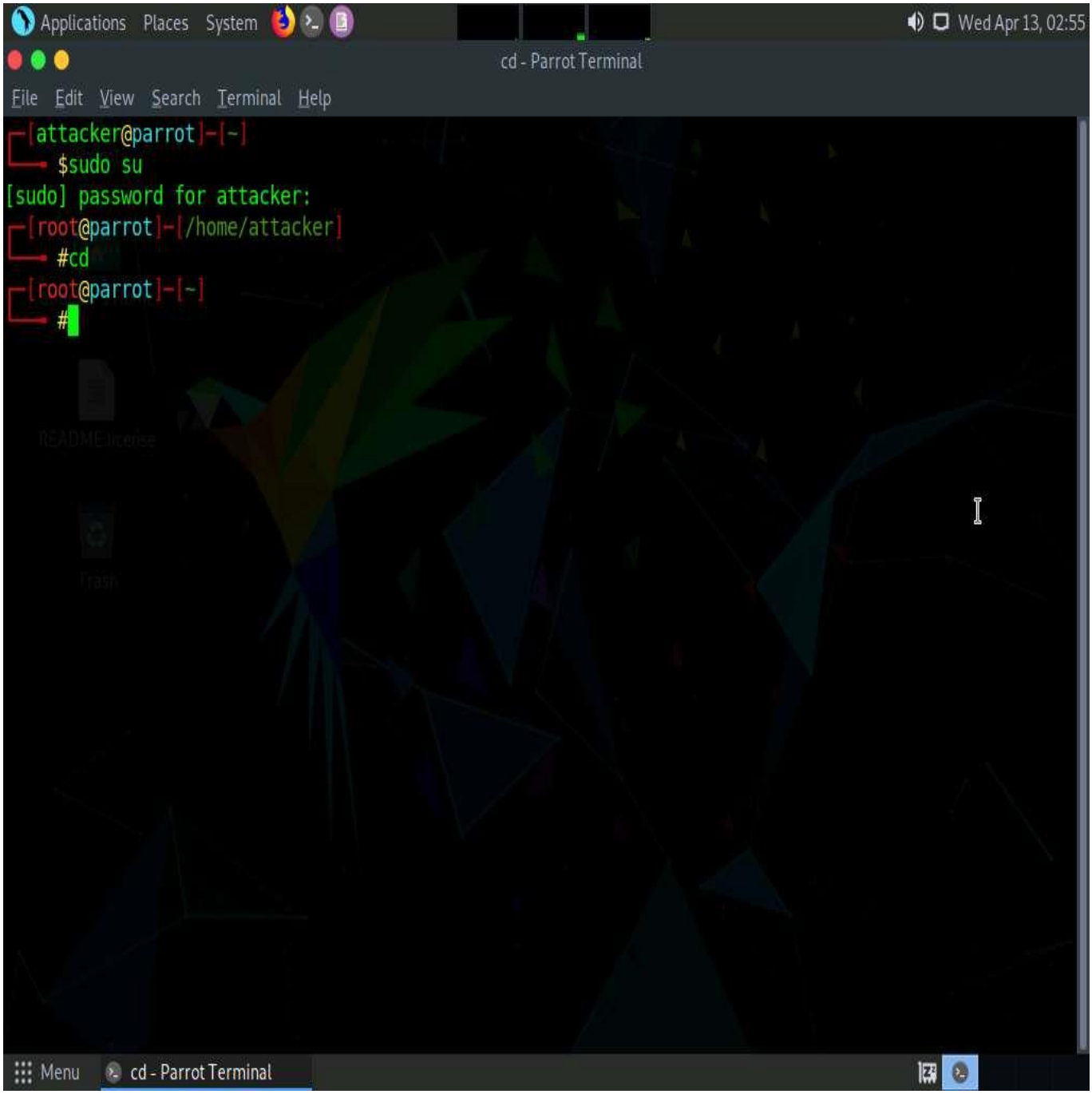
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

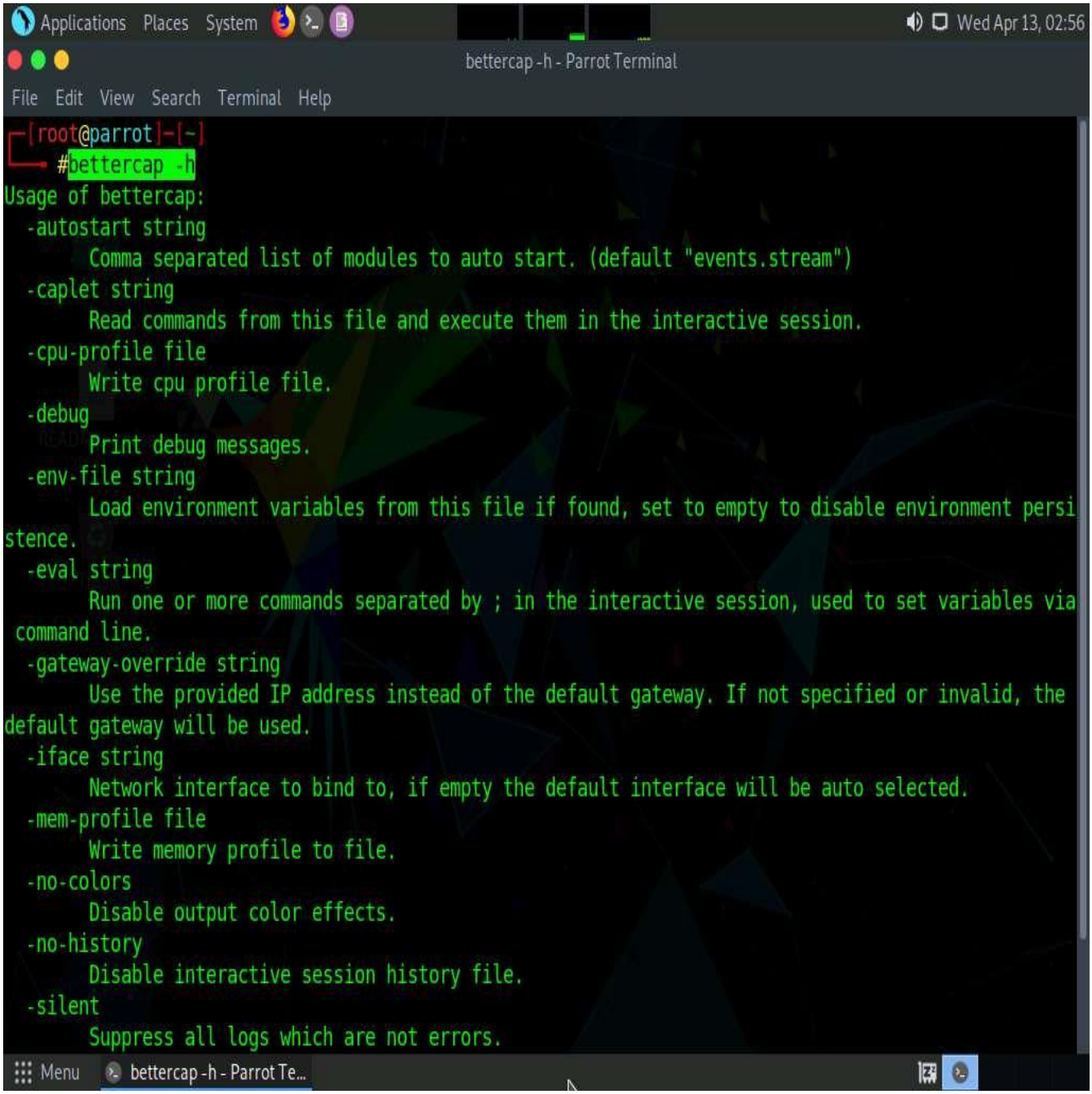
The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



7. ☐ In the terminal window; type **bettercap -h** and press **Enter**.

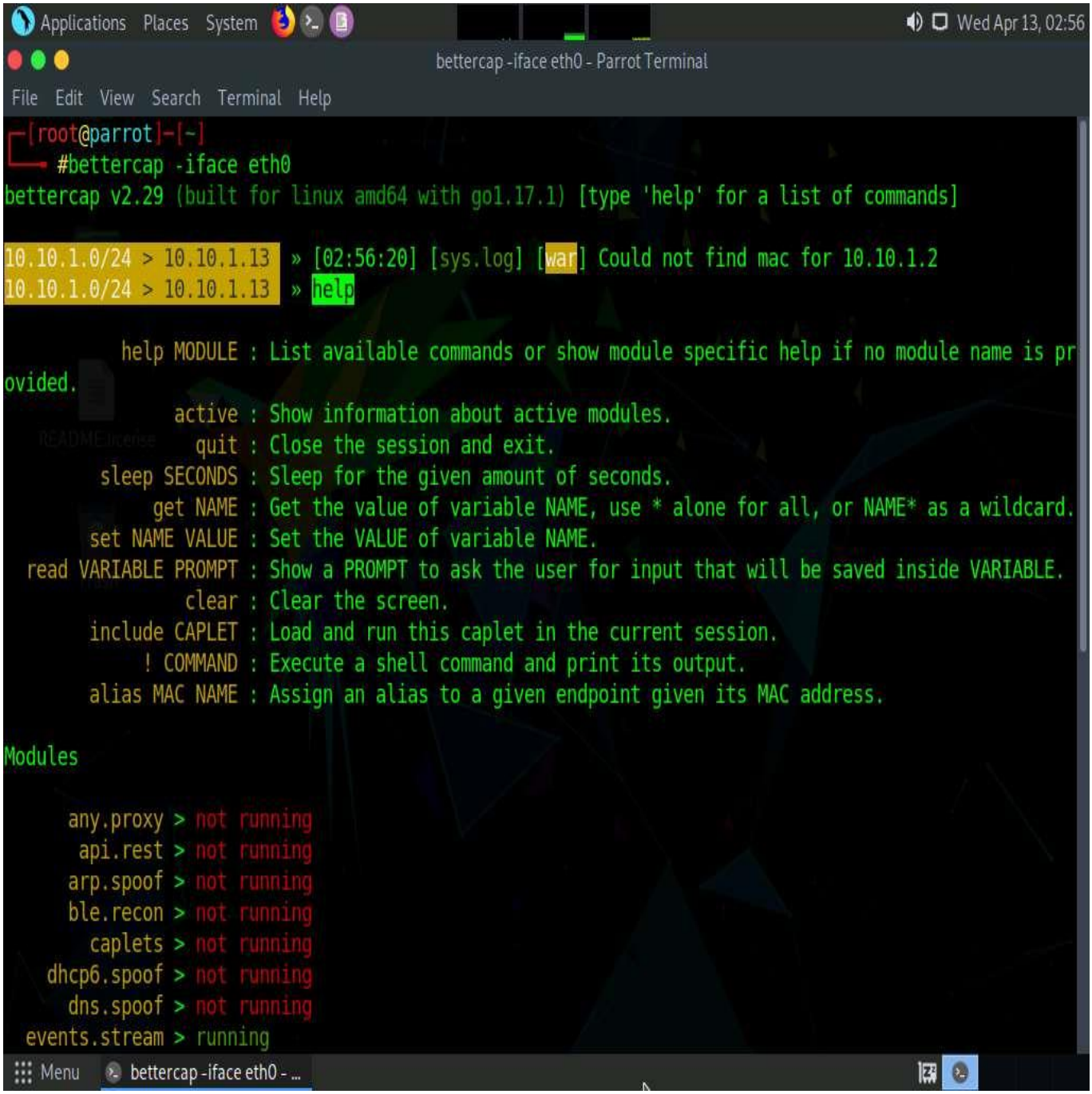
In this command, **-h**: requests a list of the available options.



8. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

-iface: specifies the interface to bind to (in this example, **eth0**).

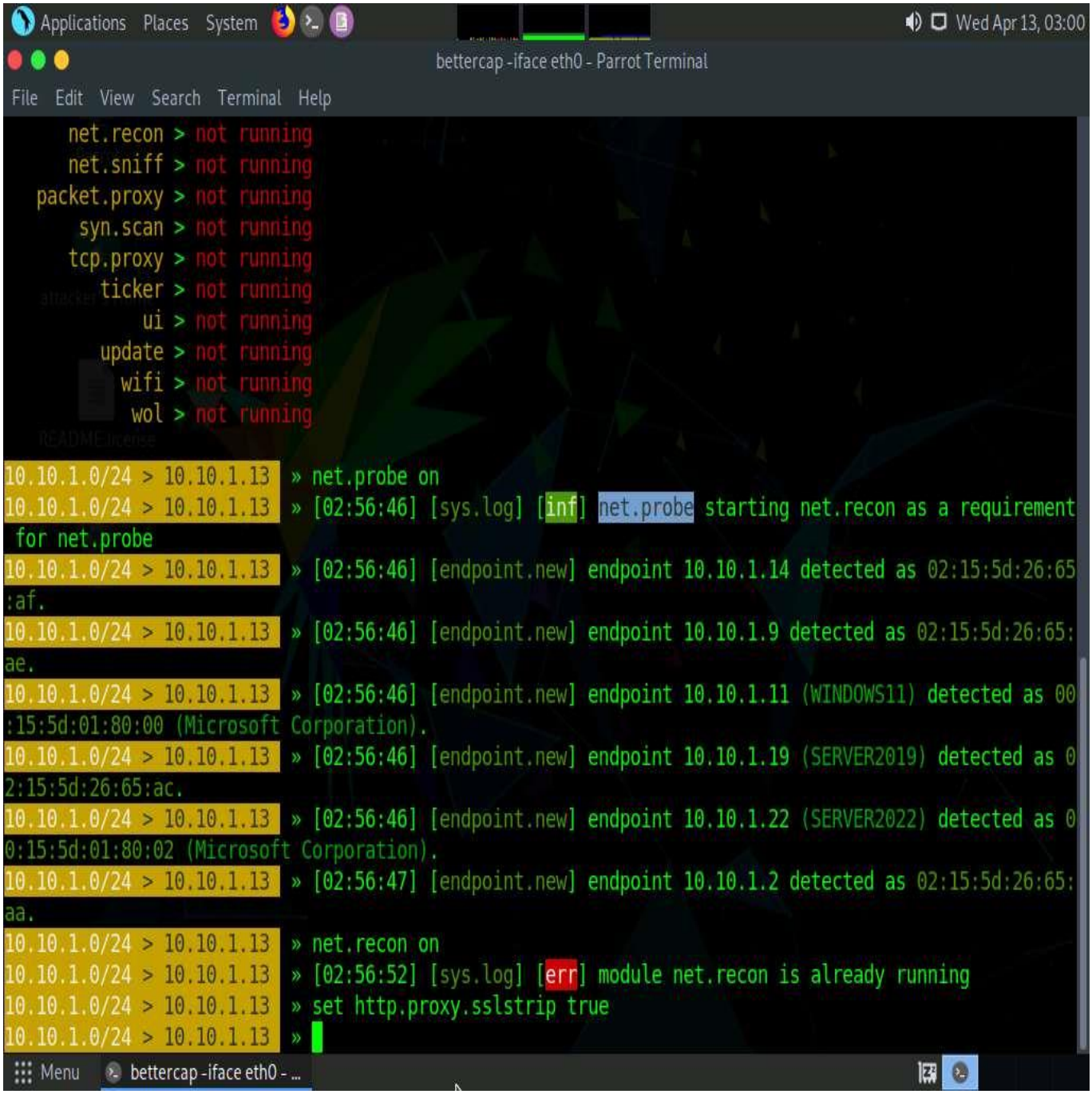
9. Type **help** and press **Enter** to view the list of available modules in bettercap.



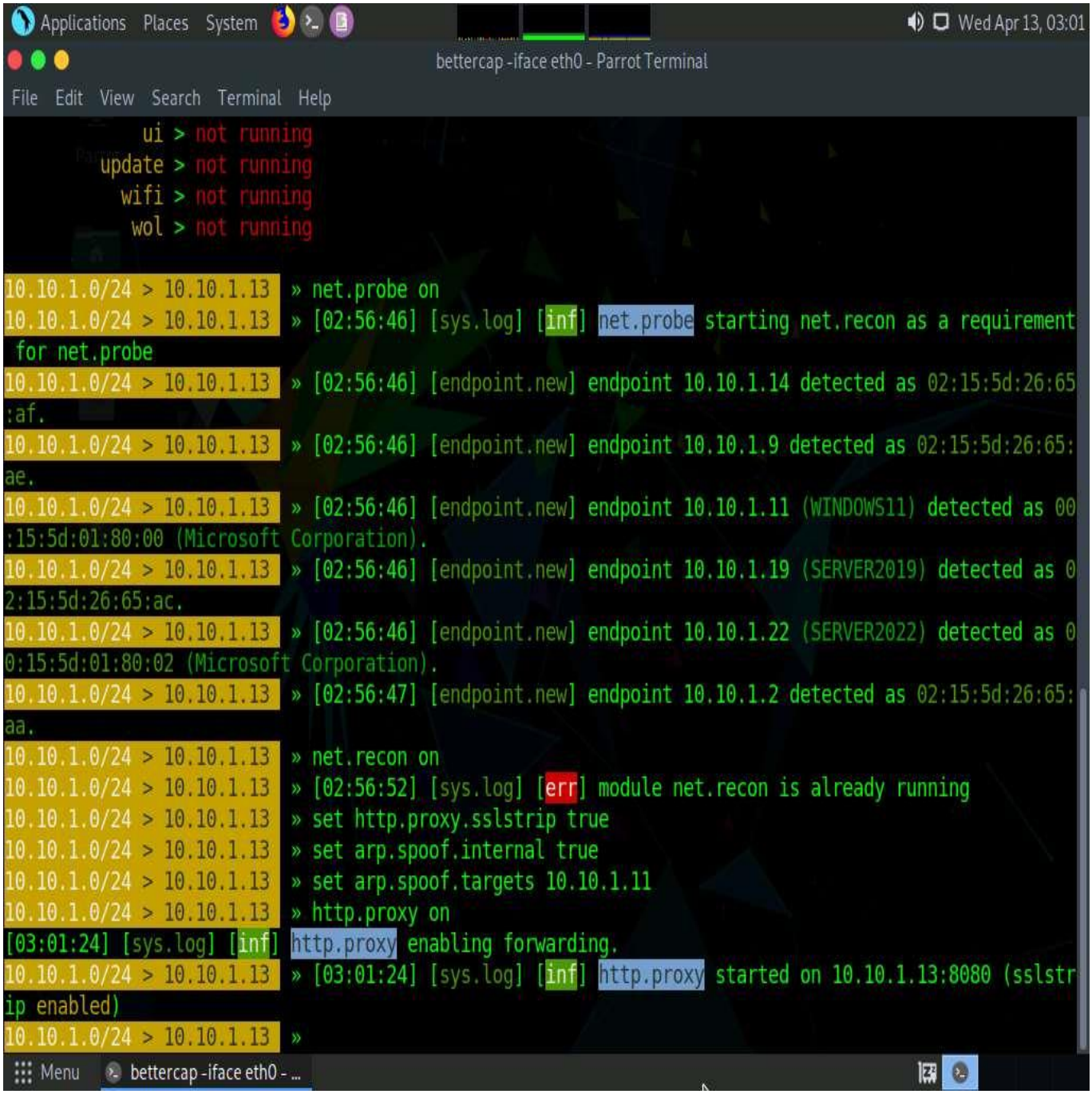
10. ☐ Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.
11. ☐ Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table 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.

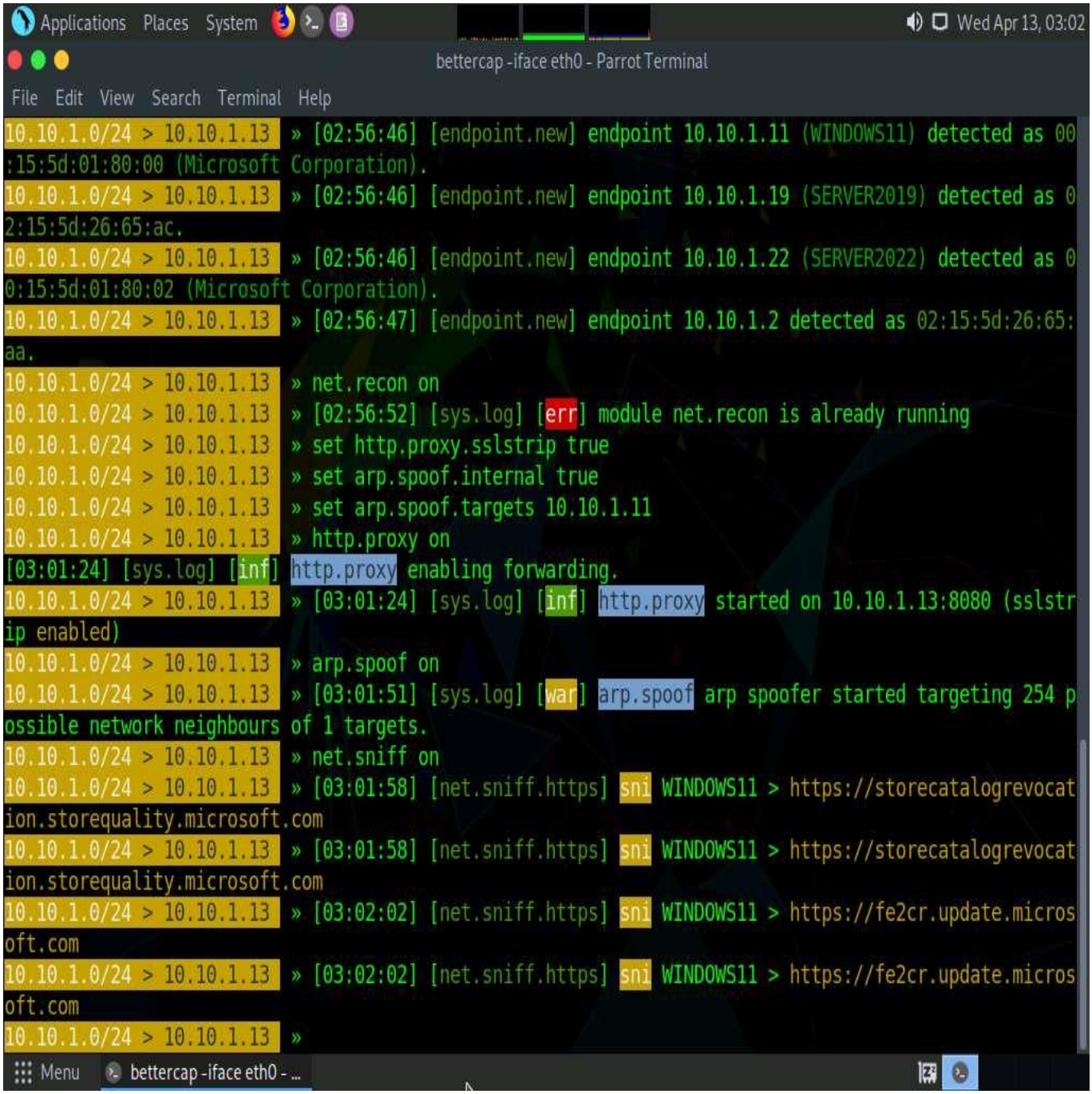
12. ☐ Type **set http.proxy.sslstrip true** and press **Enter**. This module enables SSL stripping.



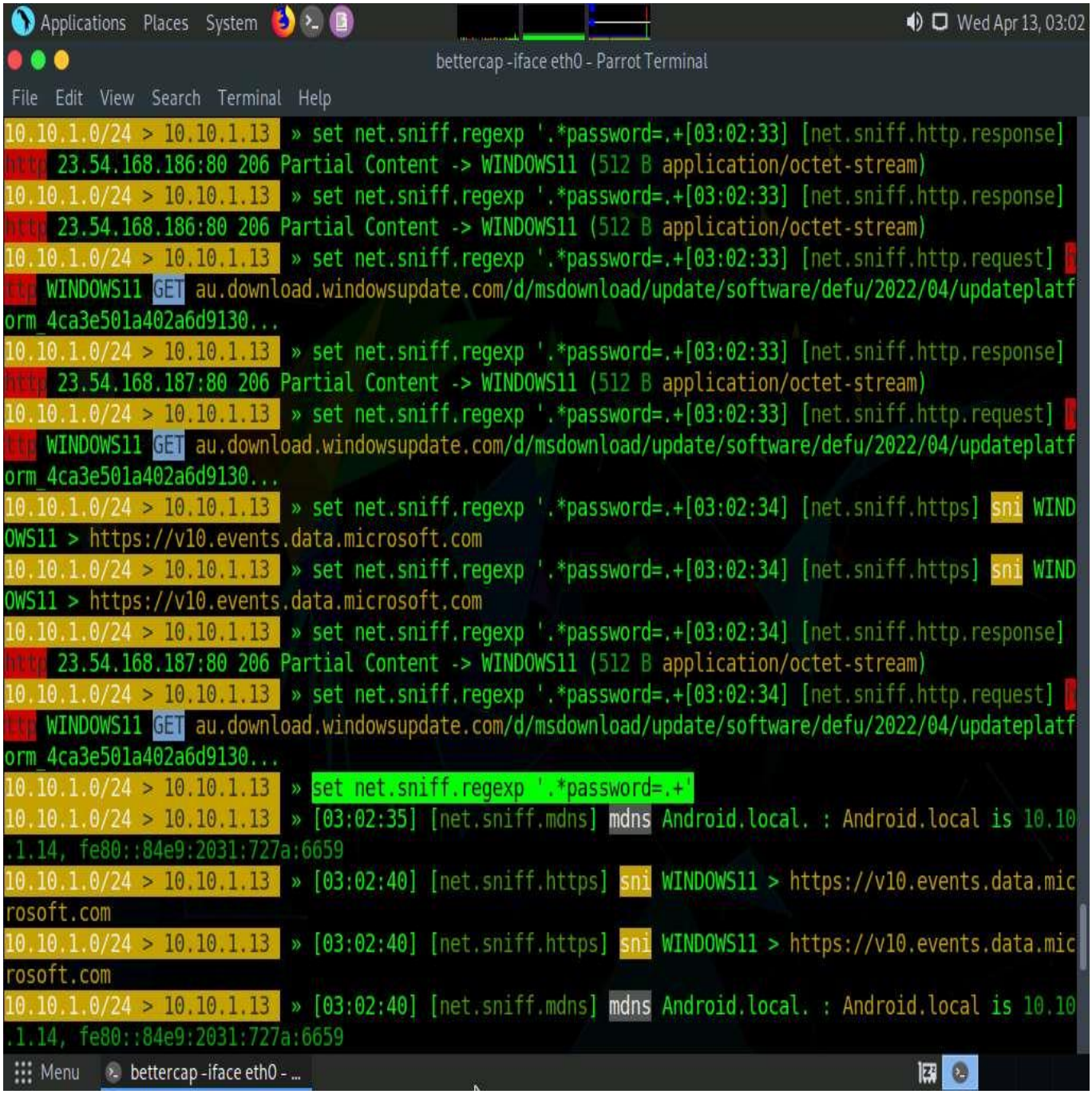
13. ☐ Type **set arp.spoof.internal true** and press **Enter**. This module spoofs the local connections among computers of the internal network.
14. ☐ Type **set arp.spoof.targets 10.10.1.11** and press **Enter**. This module spoofs the IP address of the target host.
15. ☐ Type **http.proxy on** and press **Enter**. This module initiates http proxy.



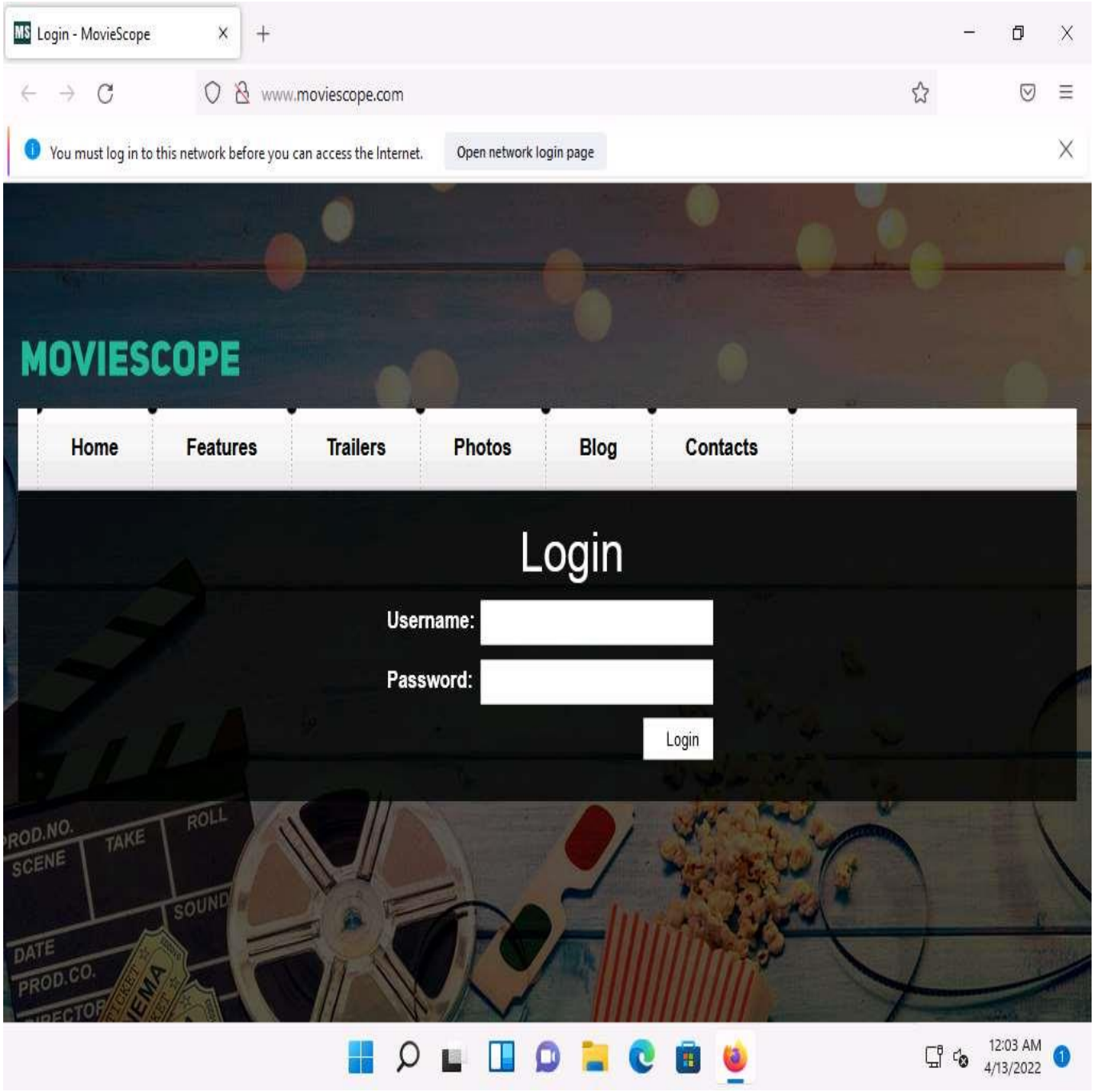
16. ☐ Type **arp.spoof on** and press **Enter**. This module initiates ARP spoofing.
17. ☐ Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.



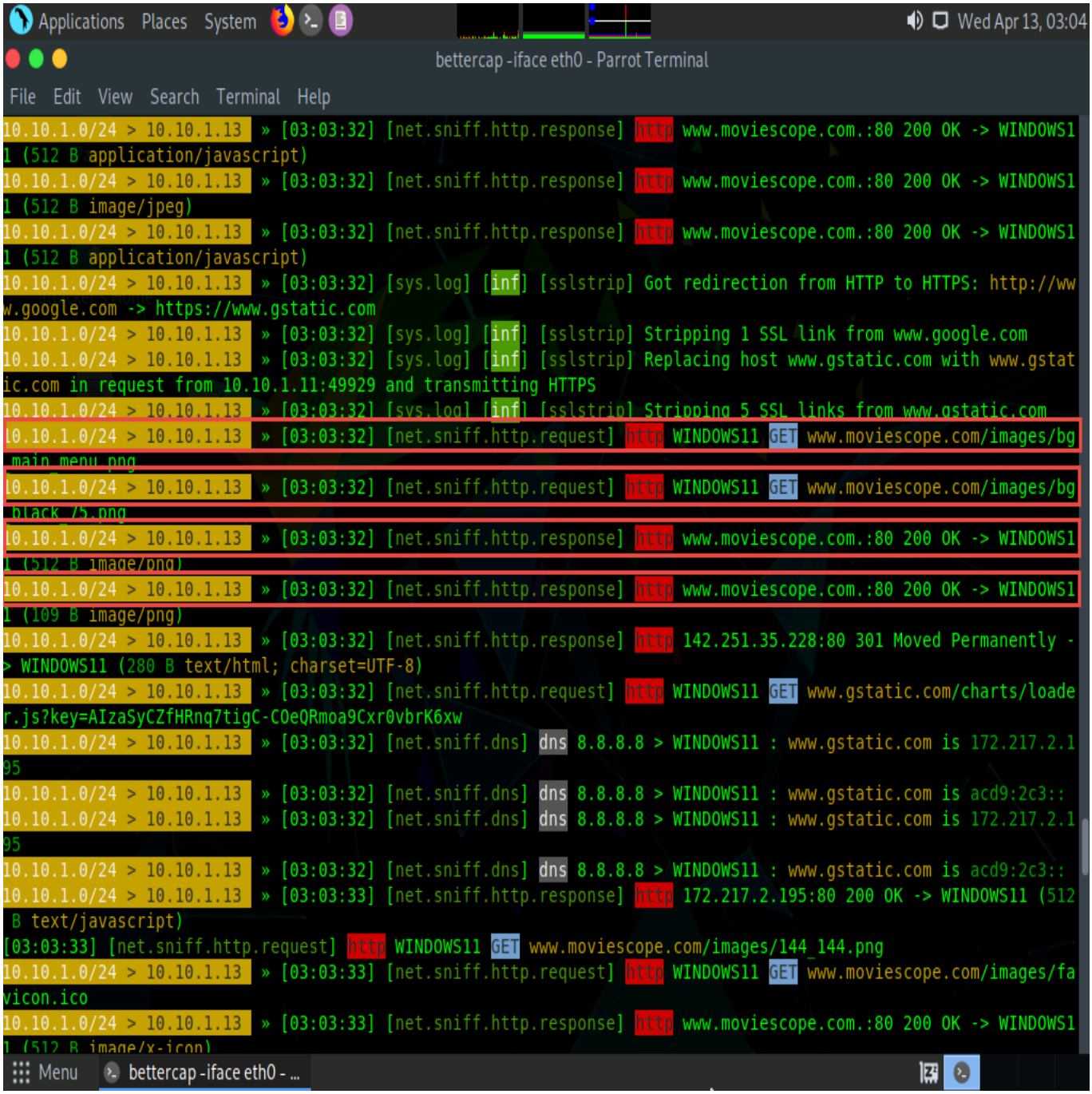
18. ☐ Type **set net.sniff.regexp '.*password=.+'** and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.+'**).



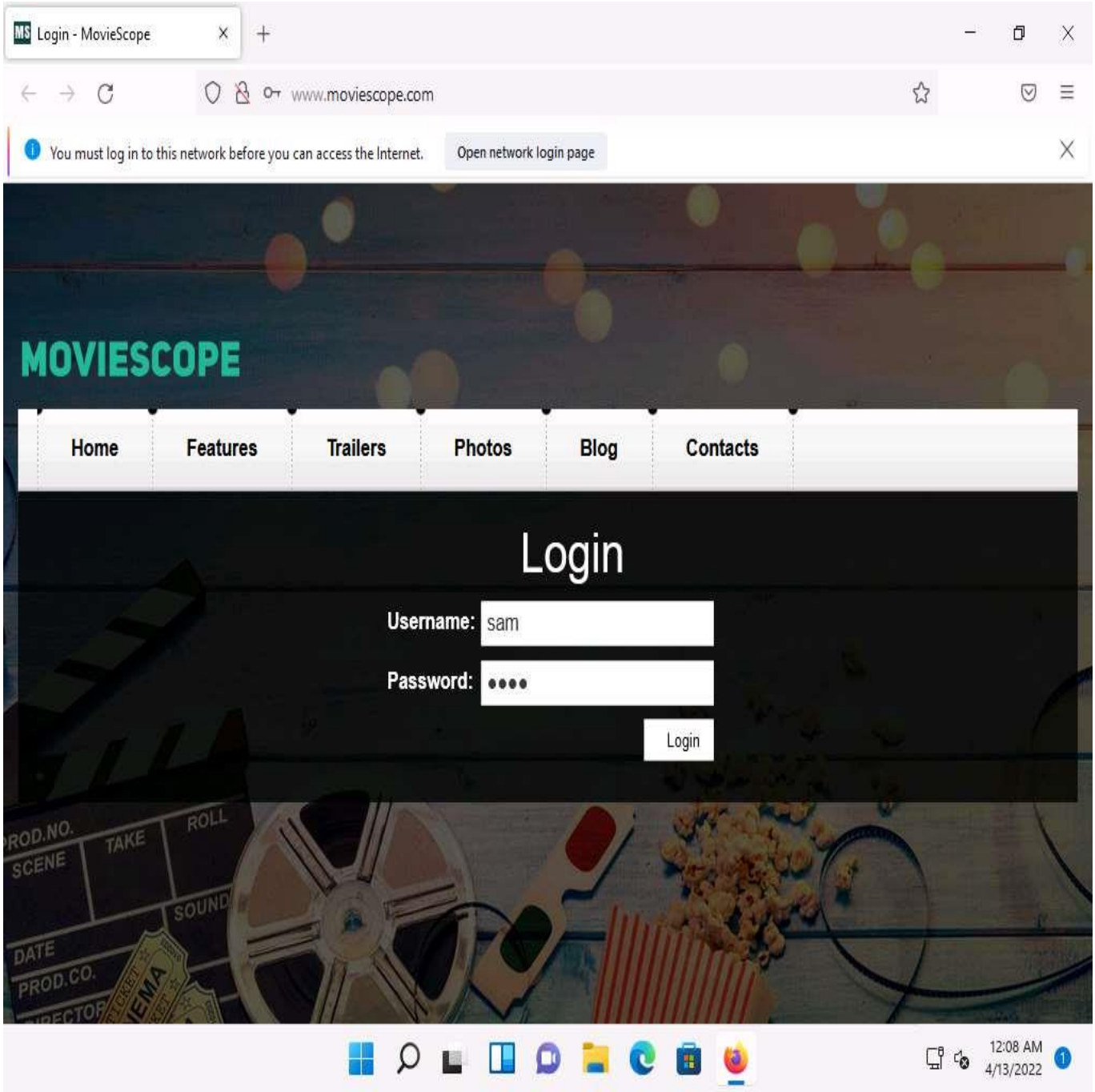
19. ☐ You can observe that bettercap starts sniffing network traffic on target machine **Windows 11**.
20. ☐ Now, click Windows 11 to switch to the **Windows 11** machine. Open any web browser (in this case, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.



21. Click Parrot Security to switch back to the **Parrot Security** machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

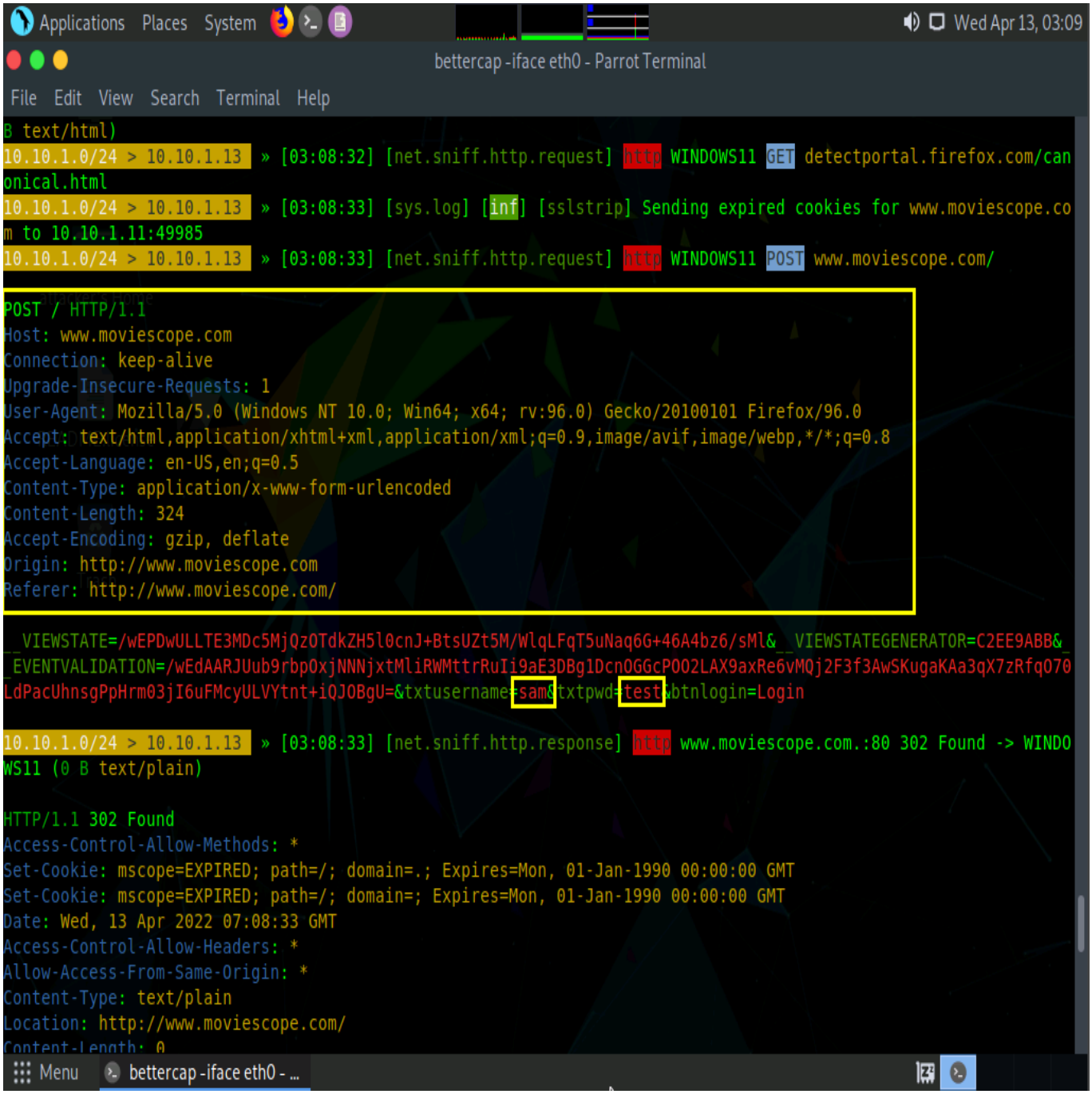


22. Click Windows 11 to switch to the **Windows 11** machine. On the **MovieScope** website, enter any credentials (here, **sam**/**test**) and press **Enter** to log in.

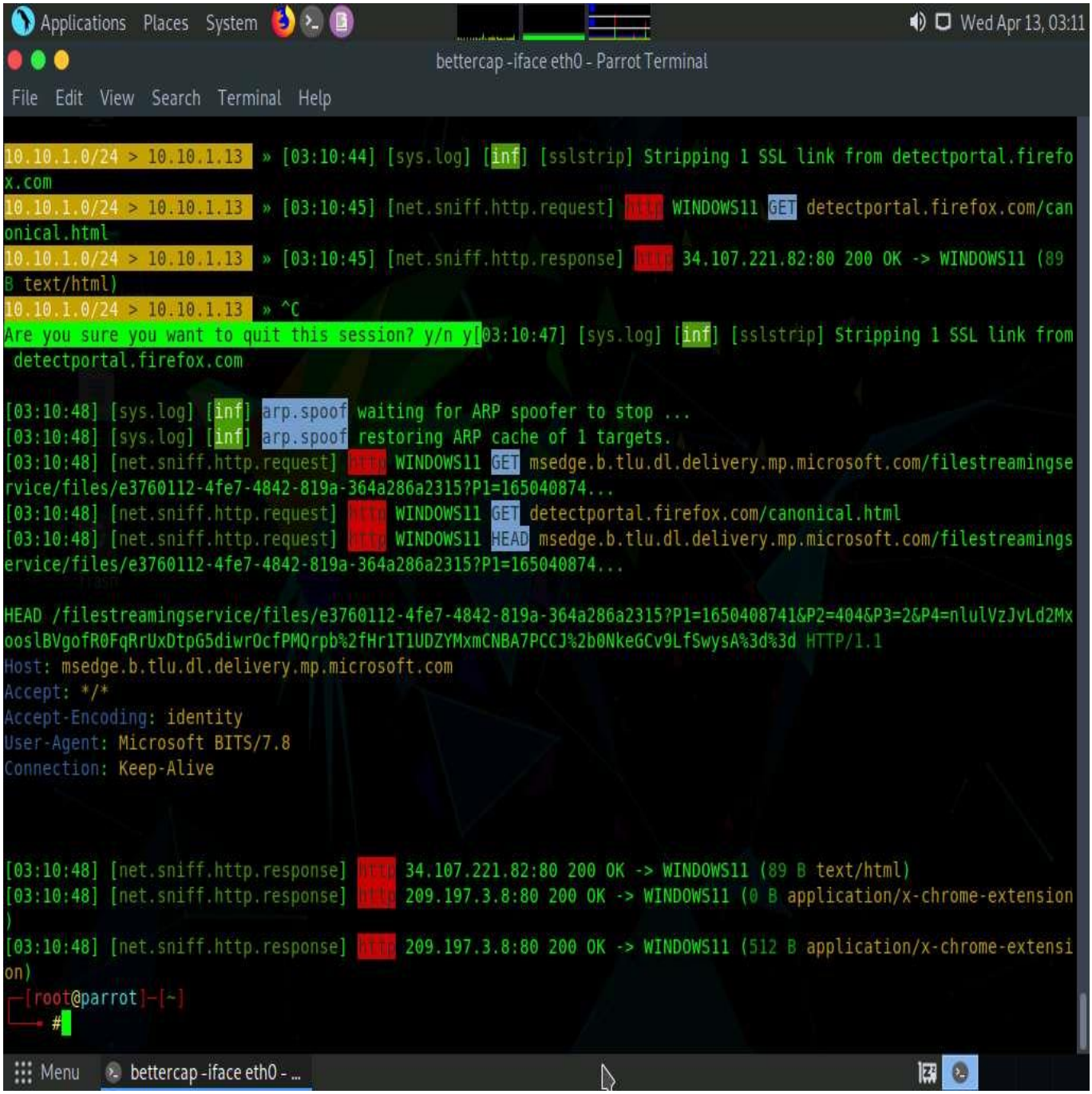


23. Click Parrot Security to switch to the **Parrot Security** machine. You can observe the details of both the browsed website and the credentials obtained in plain text, as shown in the screenshot.

bettercap collects all http logins used by routers, servers, and websites that do not have SSL enabled. In this task, we are using **www.moviescope.com** for demonstration purposes, as it is http-based. To use bettercap to sniff network traffic from https-based websites, you must enable the SSL strip module by issuing the command **set http.proxy.sslstrip true**.



24. ☐ After obtaining the credentials, press **Ctrl+C** to terminate bettercap. The credentials can be used to log in to the target user's account and obtain further sensitive information.
25. ☐ When the **Are you sure you want to quit this session?** message appears, press **y**, and then **Enter**.



26. ☐ This concludes the demonstration of how to intercept HTTP traffic using bettercap.
27. ☐ Close all open windows and document all the acquired information.

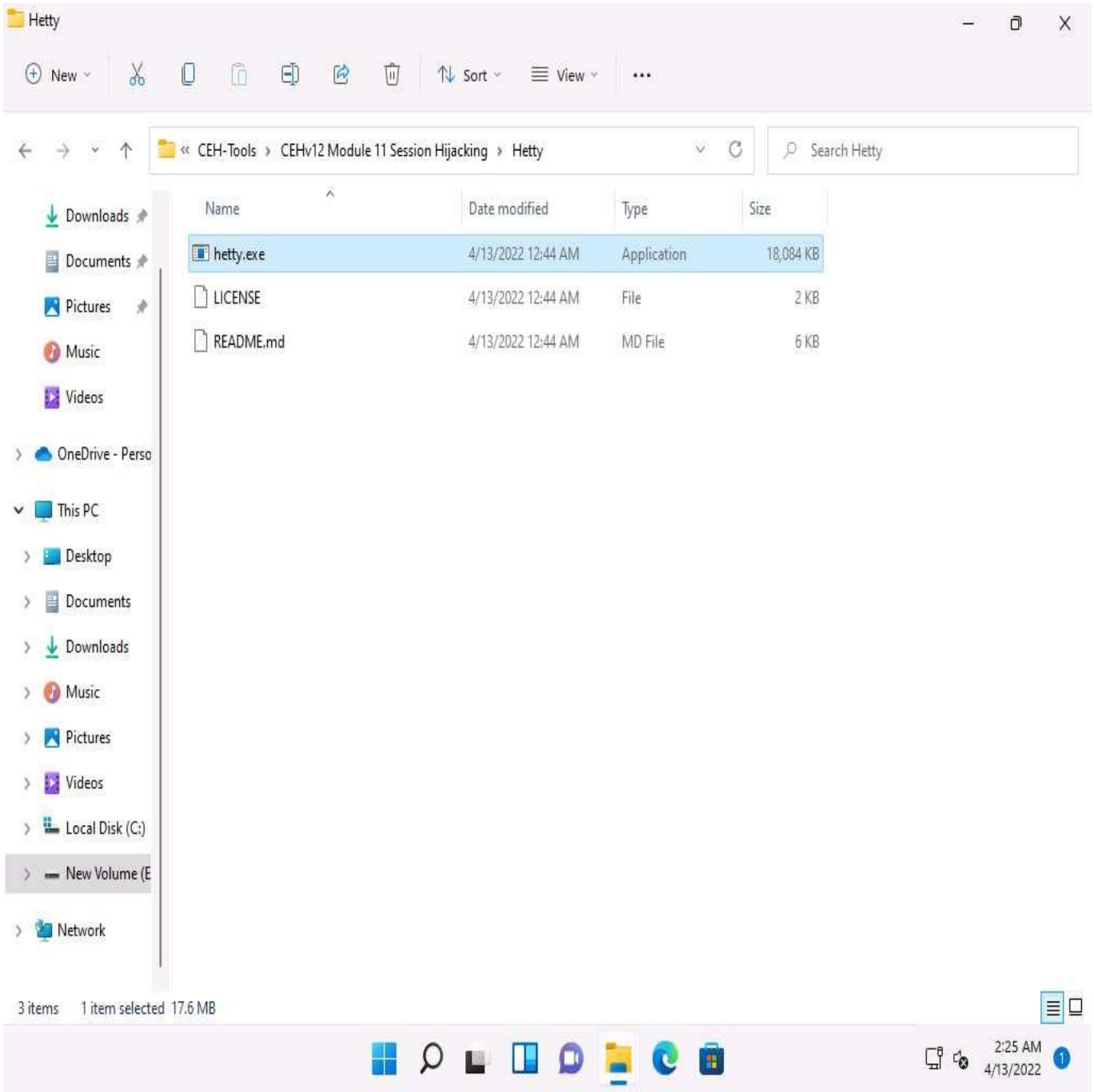
Task 3: Intercept HTTP Traffic using Hetty

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.

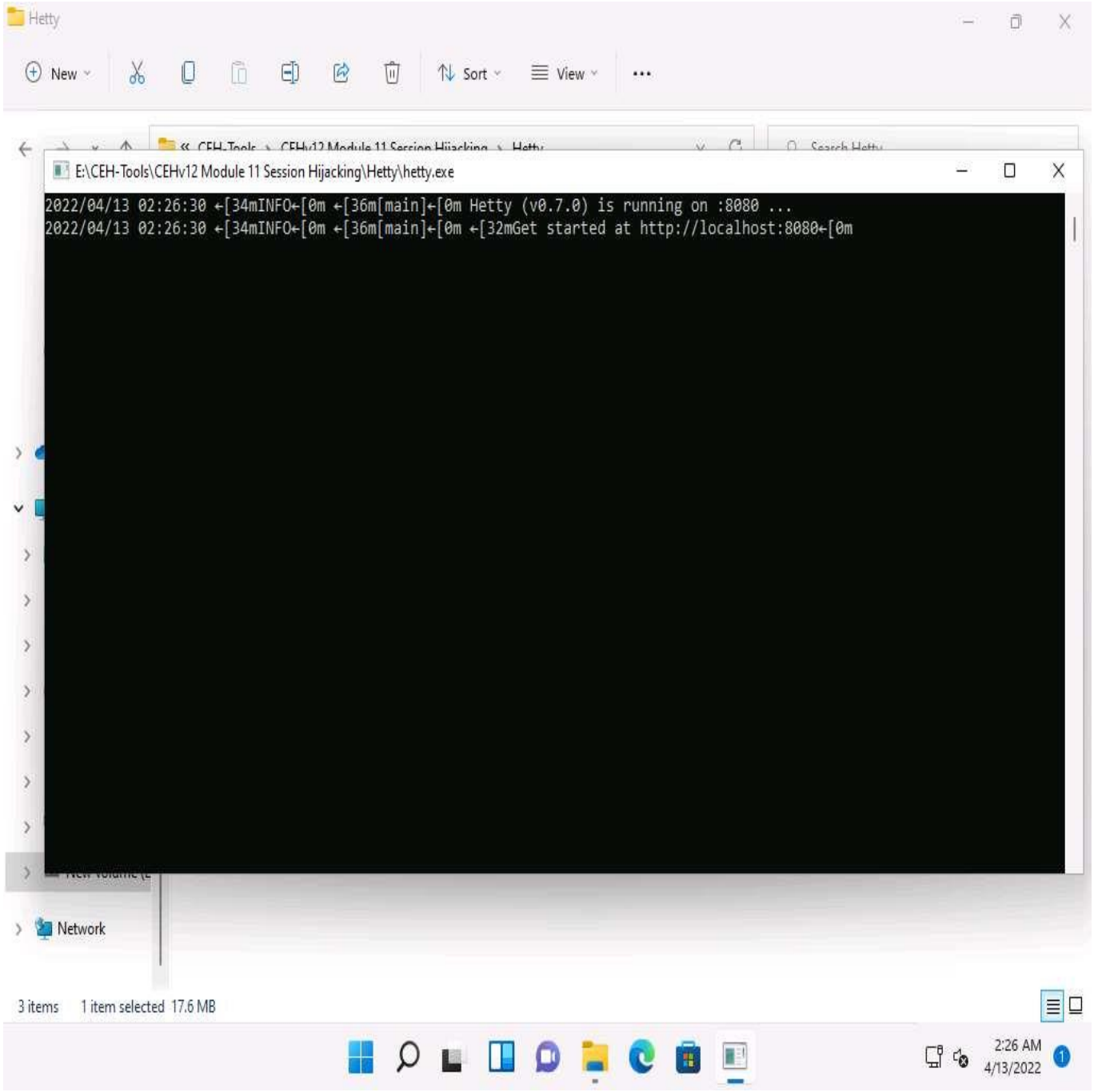
Here, we will use the Hetty tool to intercept HTTP traffic on the target system.

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

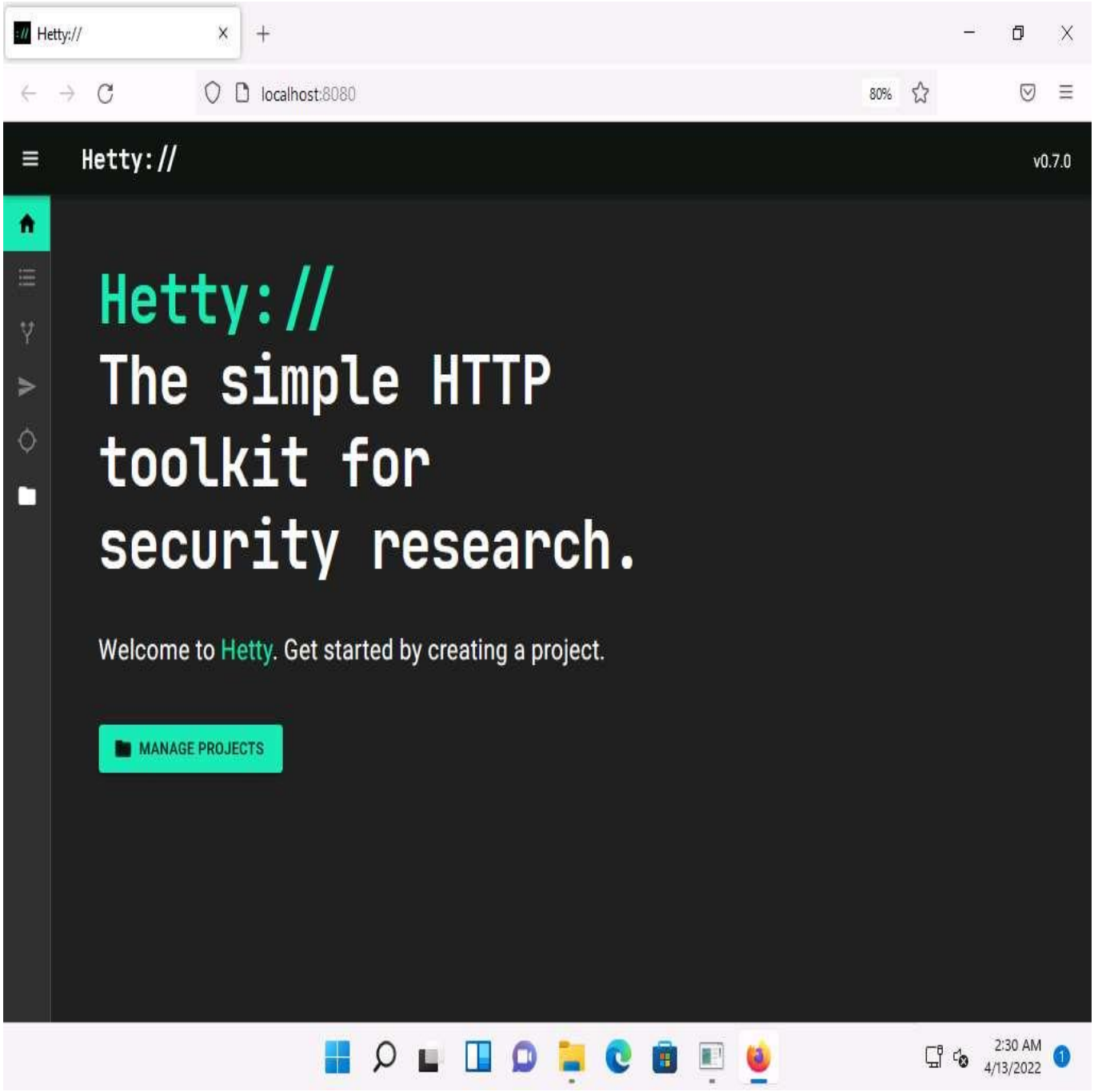
1. Click Windows 11 to switch to the **Windows 11** machine.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 11 Session Hijacking\Hetty** and double-click **hetty.exe**.



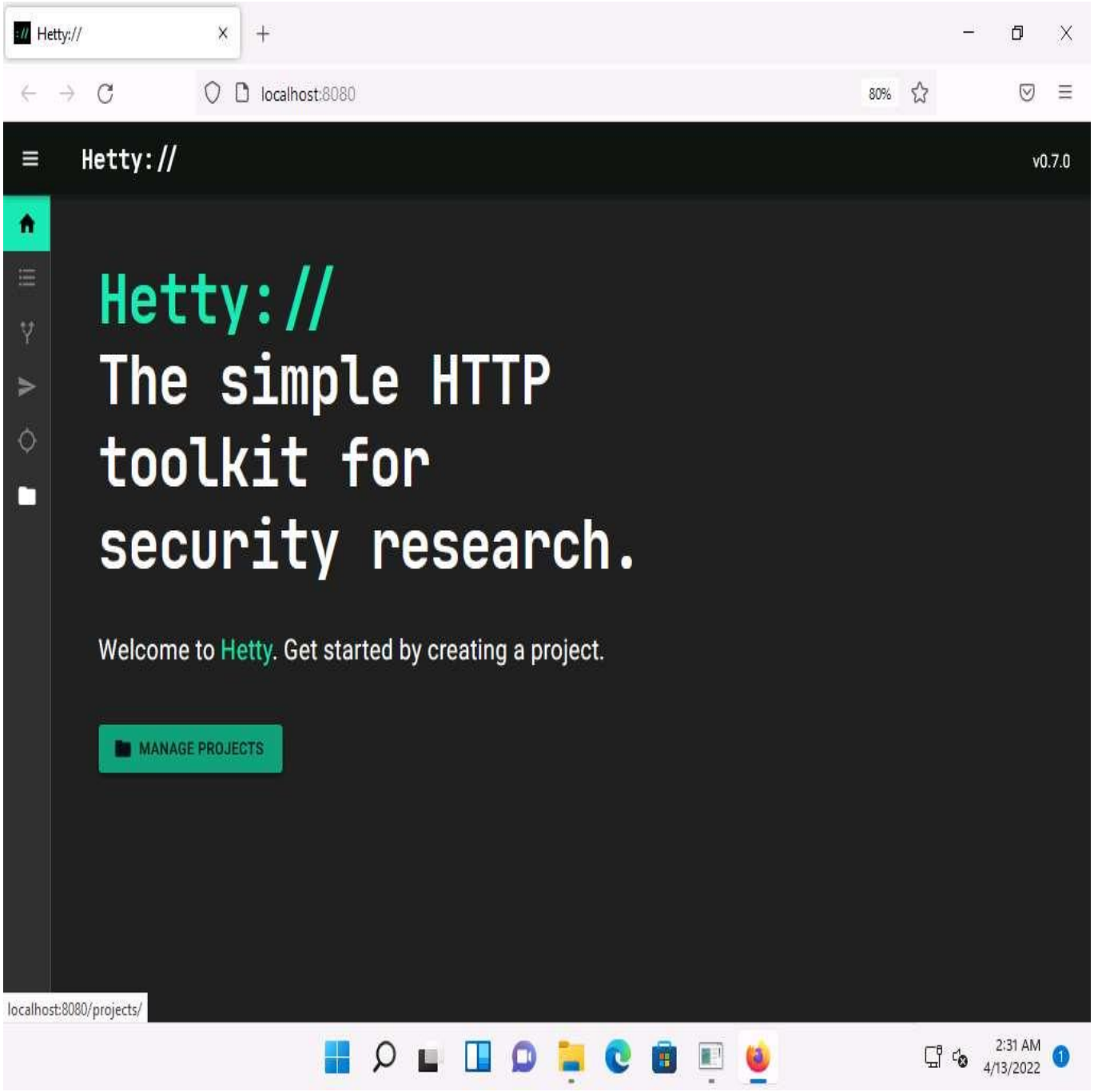
3. **Open File - Security Warning** window appears, click **Run**.
4. A **Command Prompt** window appears, and Hetty initializes.



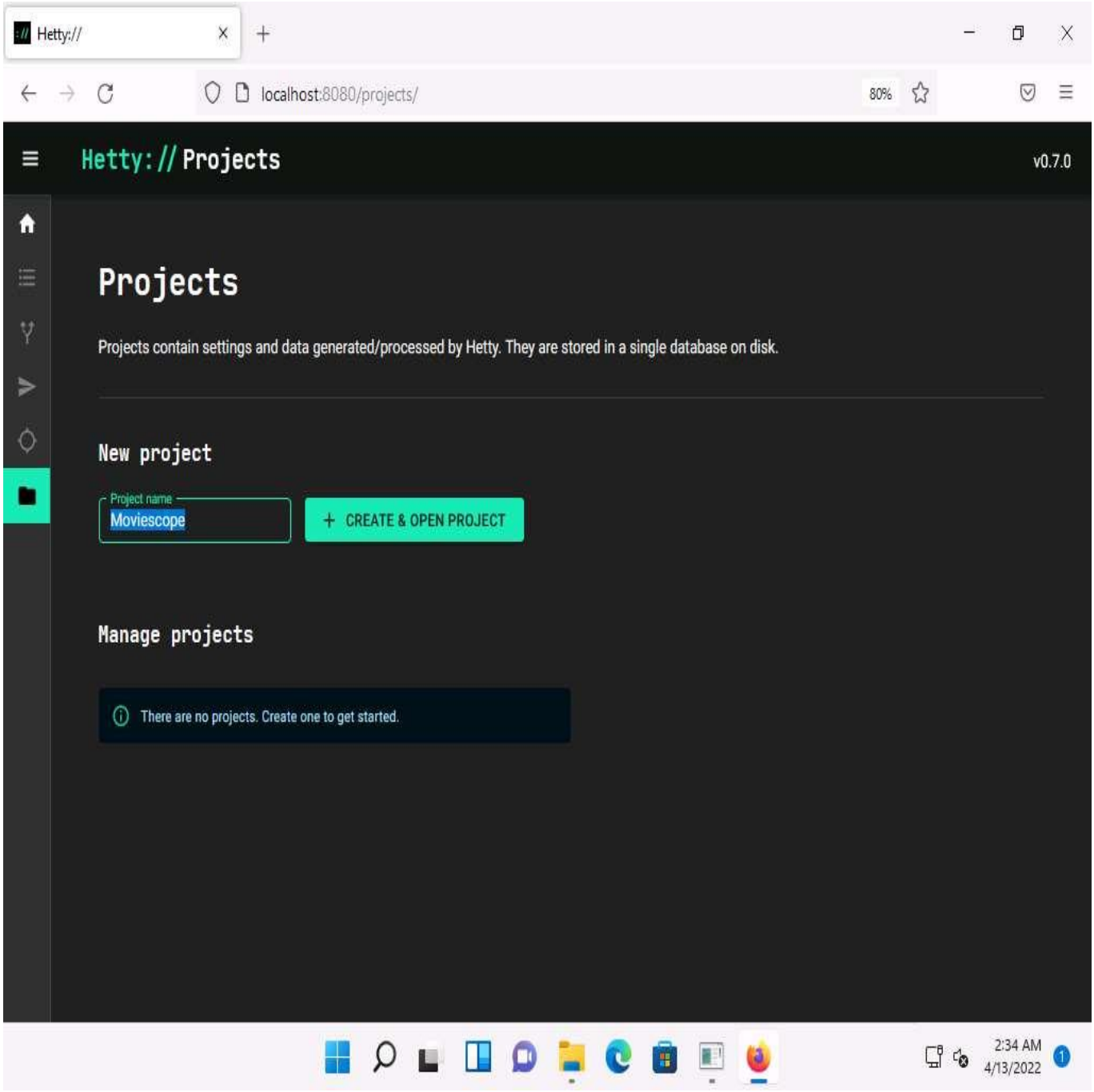
5. ☐ Now, minimize all the windows and launch any web browser (here, **Mozilla Firefox**).
6. ☐ A browser window, in the address bar, type **http://localhost:8080** and press **Enter** to open Hetty dashboard.



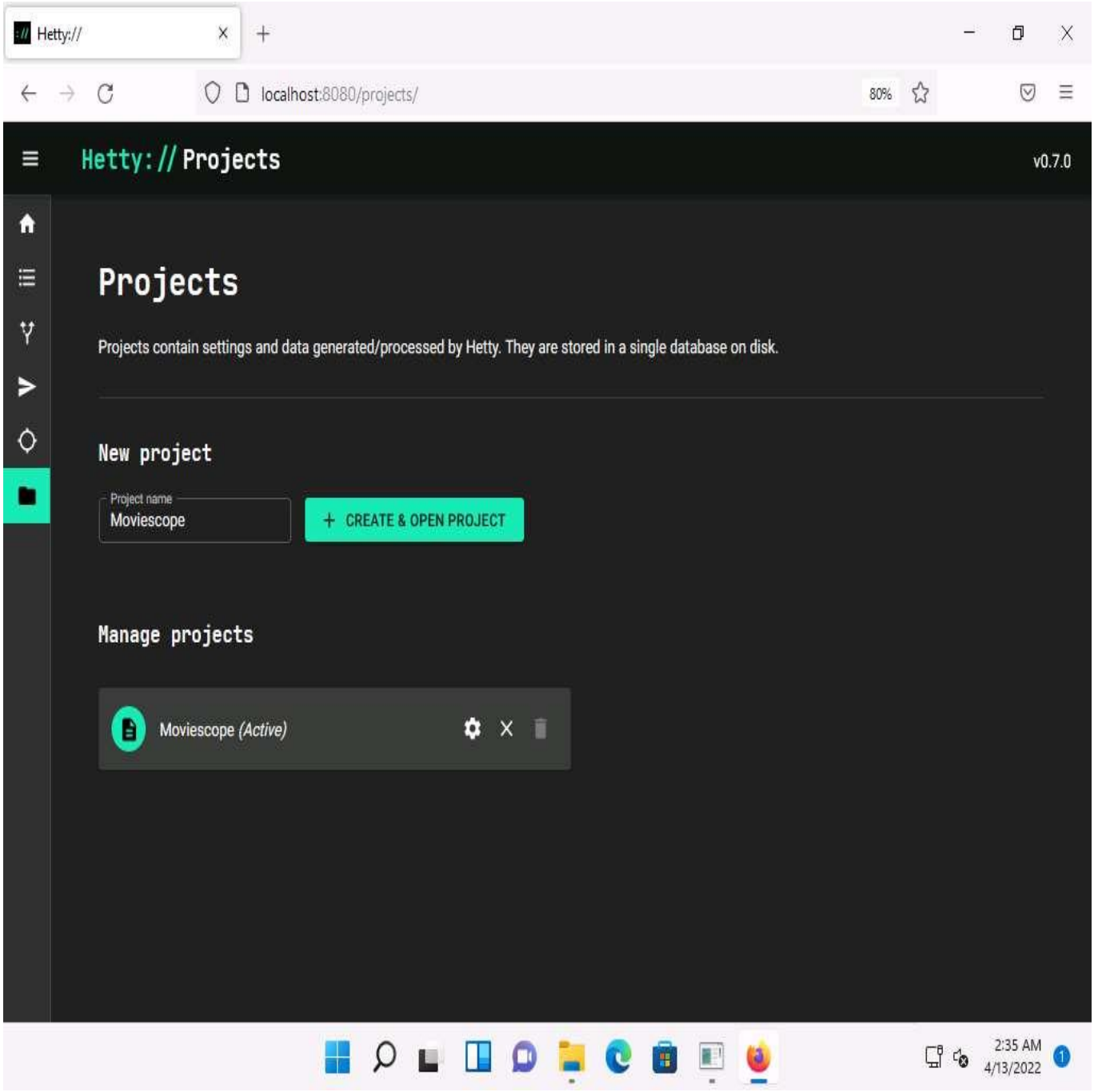
7. ☐ In the Hetty dashboard, click **MANAGE PROJECTS** button.



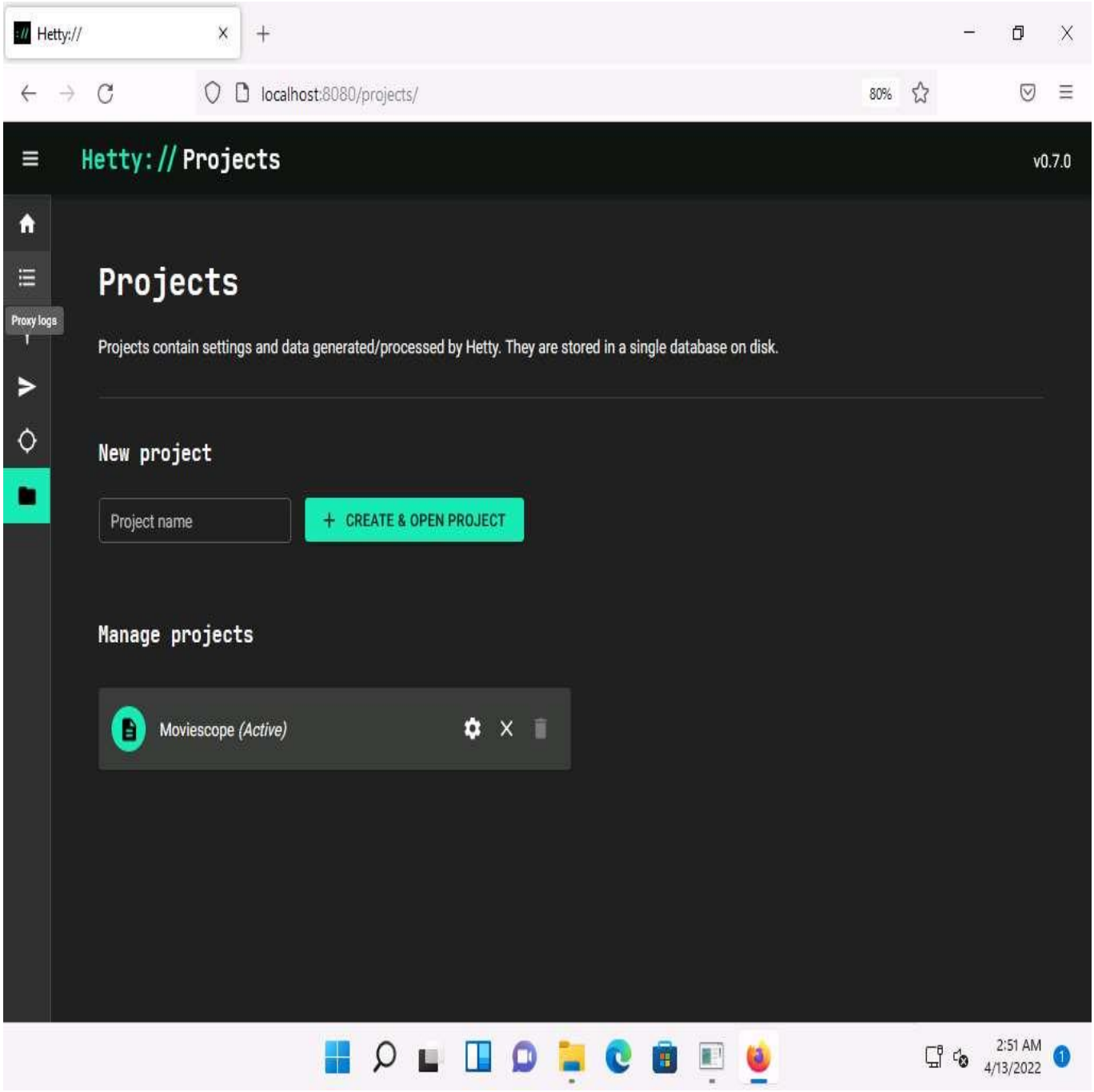
8. **Projects** page appears, type **Project name** as **Moviescope** under **New Project** section and click **+ CREATE & OPEN PROJECT** button.



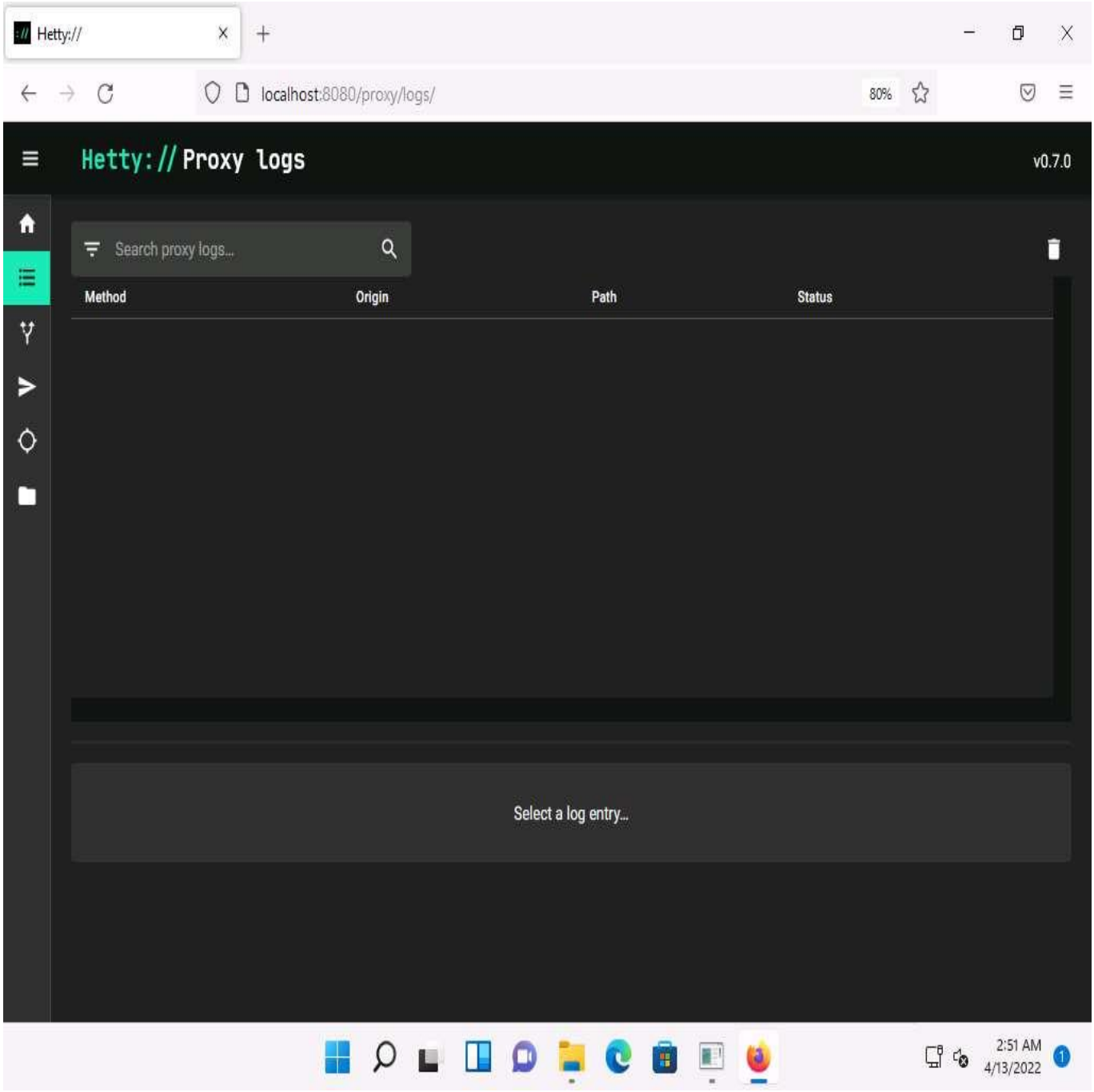
9. ☐ You can observe that a new project name **Moviescope** has been created under **Manage projects** section with a status as **Active**.



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

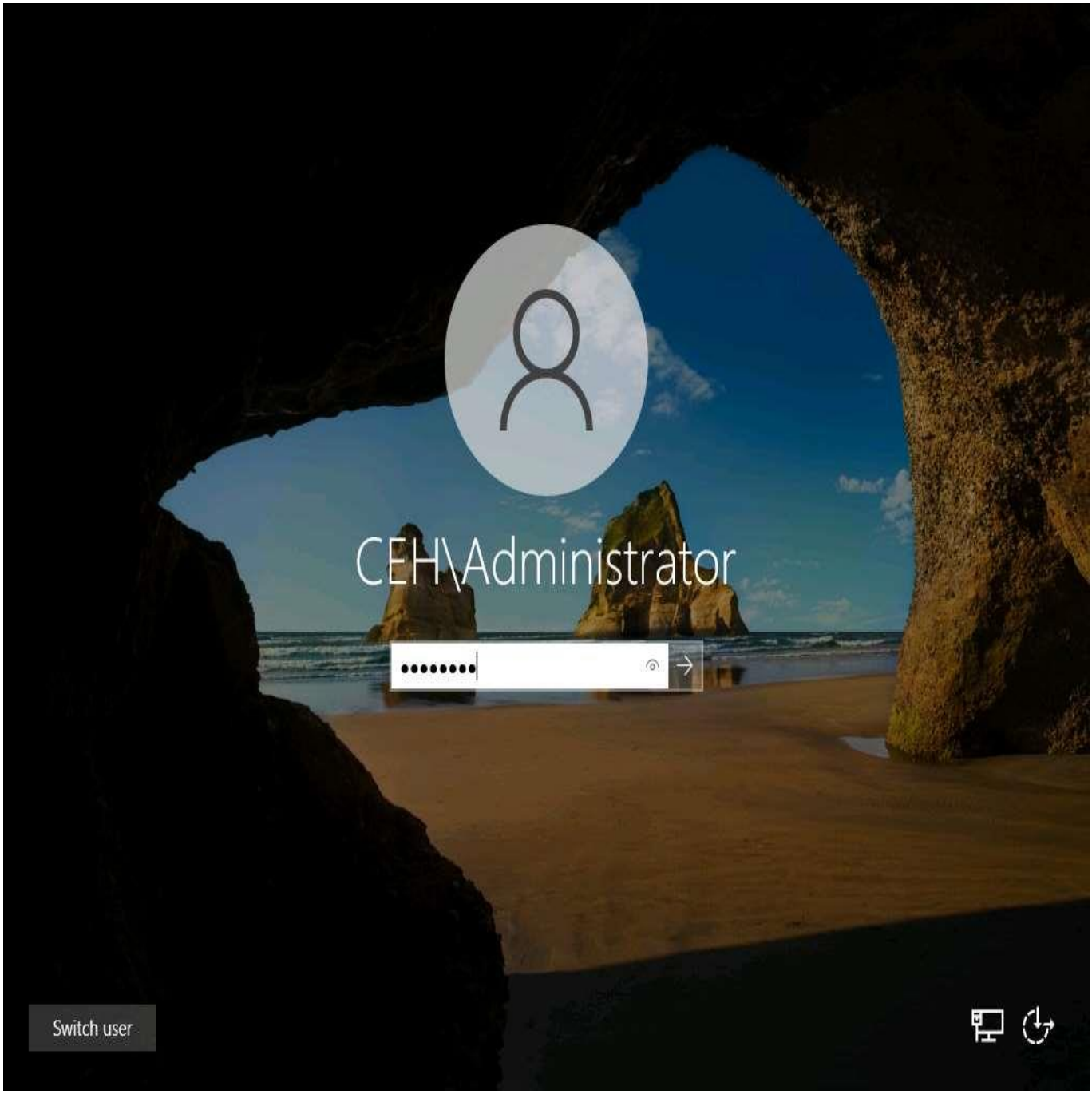


11. A **Proxy logs** page appears, as shown in the screenshot.

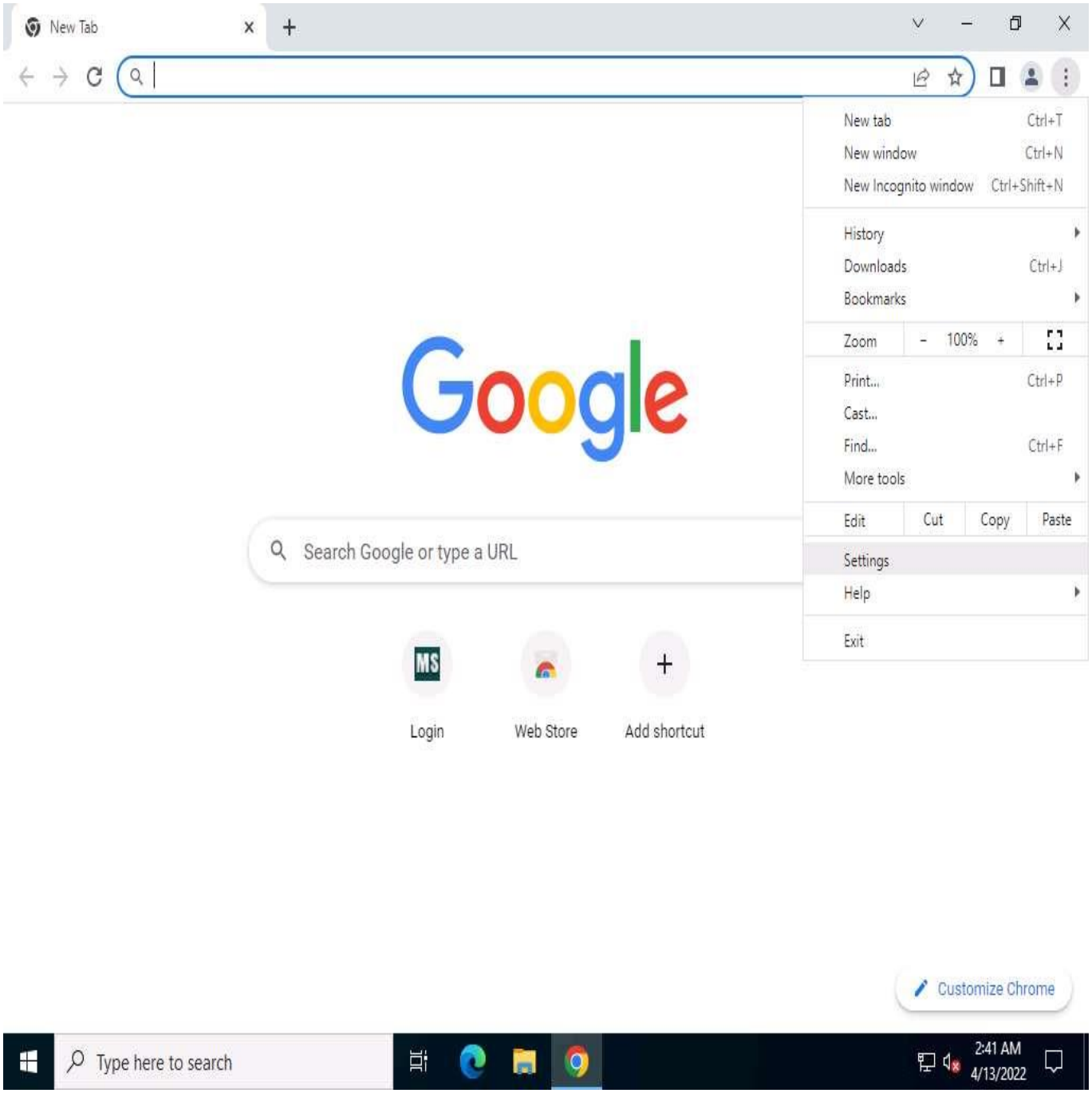


12. Now, click Windows Server 2022 to switch to the **Windows Server 2022** machine.
Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.

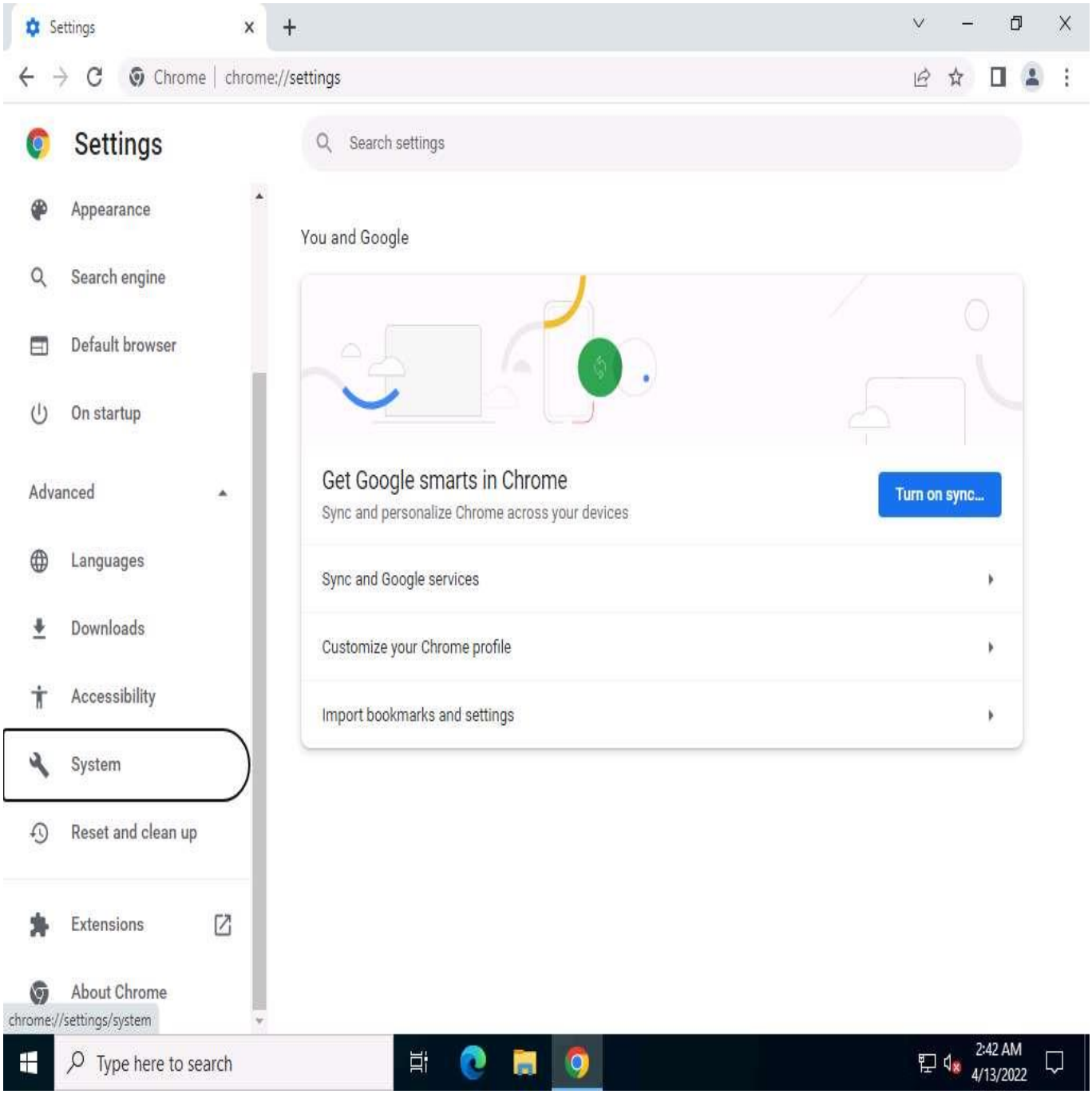
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



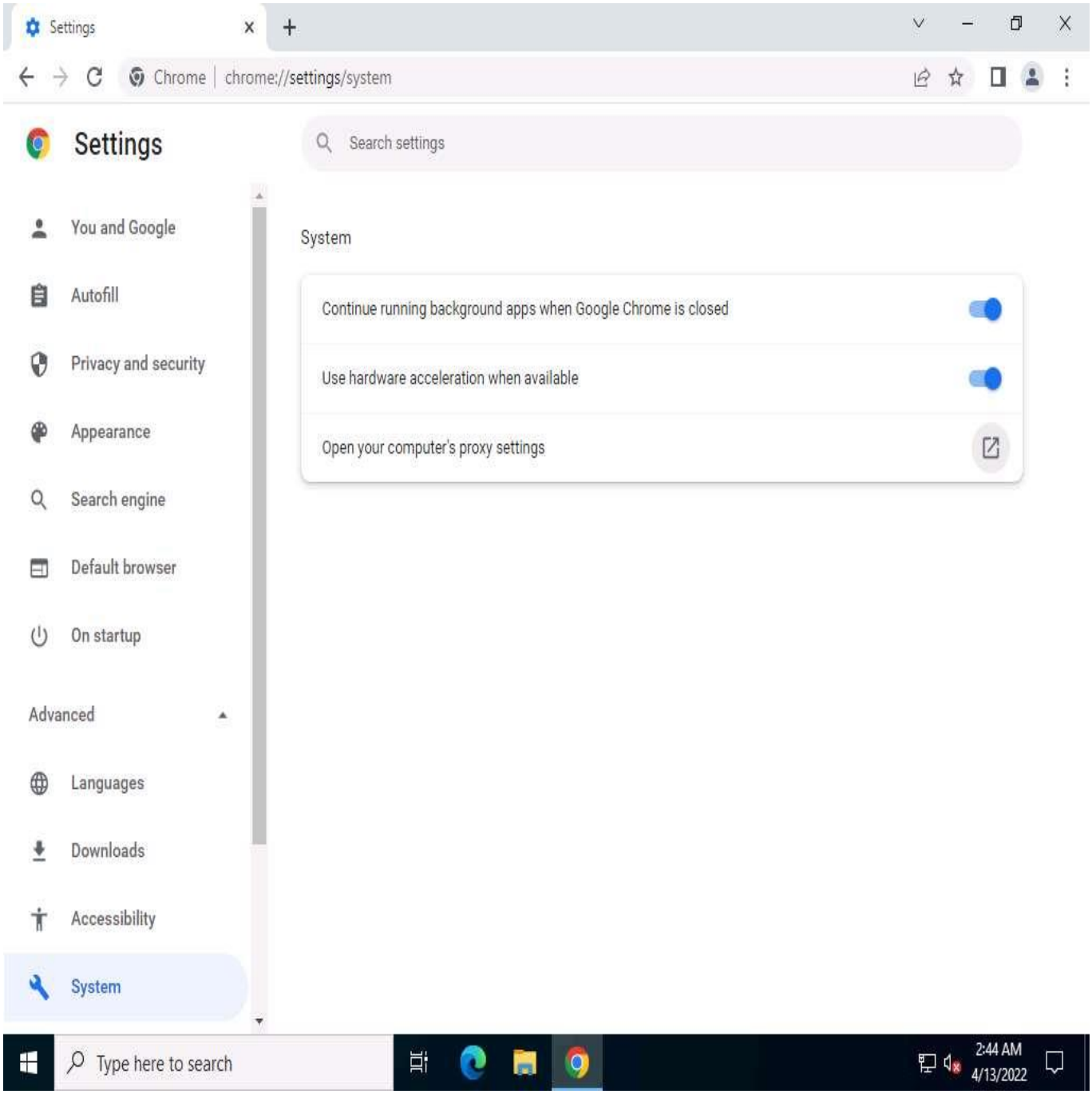
13. ☐ Open **Google Chrome** web browser, click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



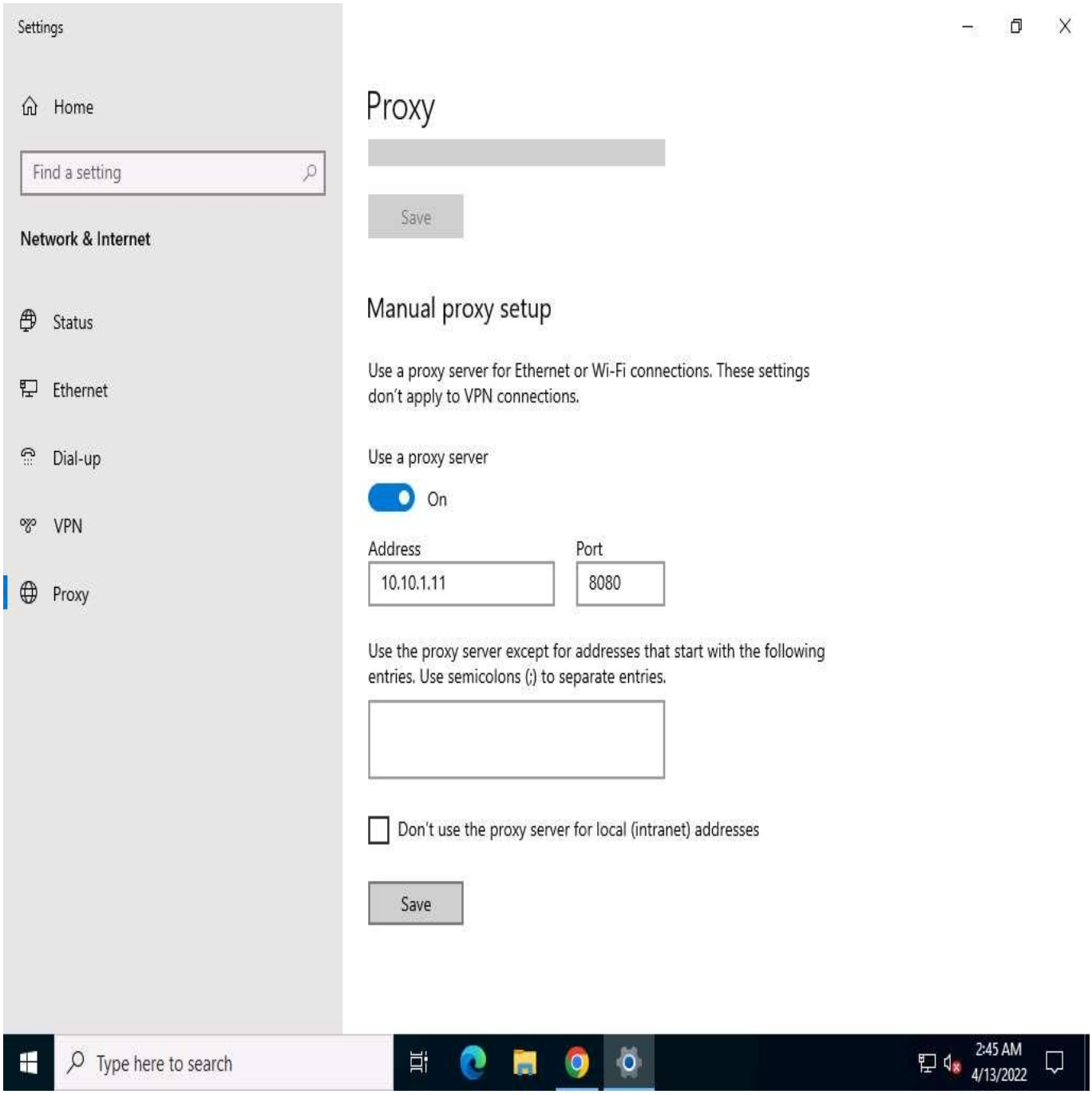
14. ☐ On the **Settings** page, expand **Advanced** settings and click **System** in the left-pane.



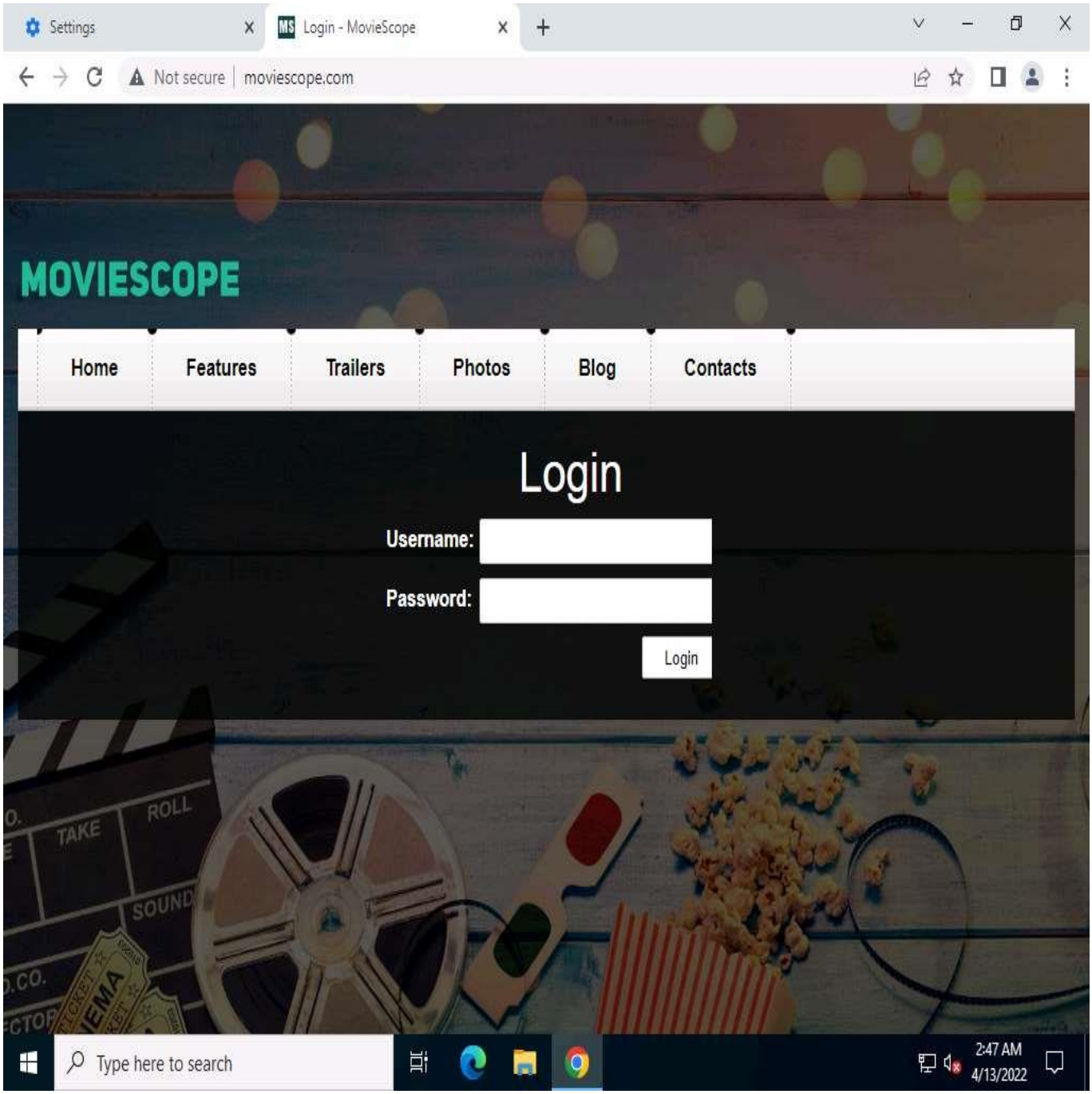
15. ☐ Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.



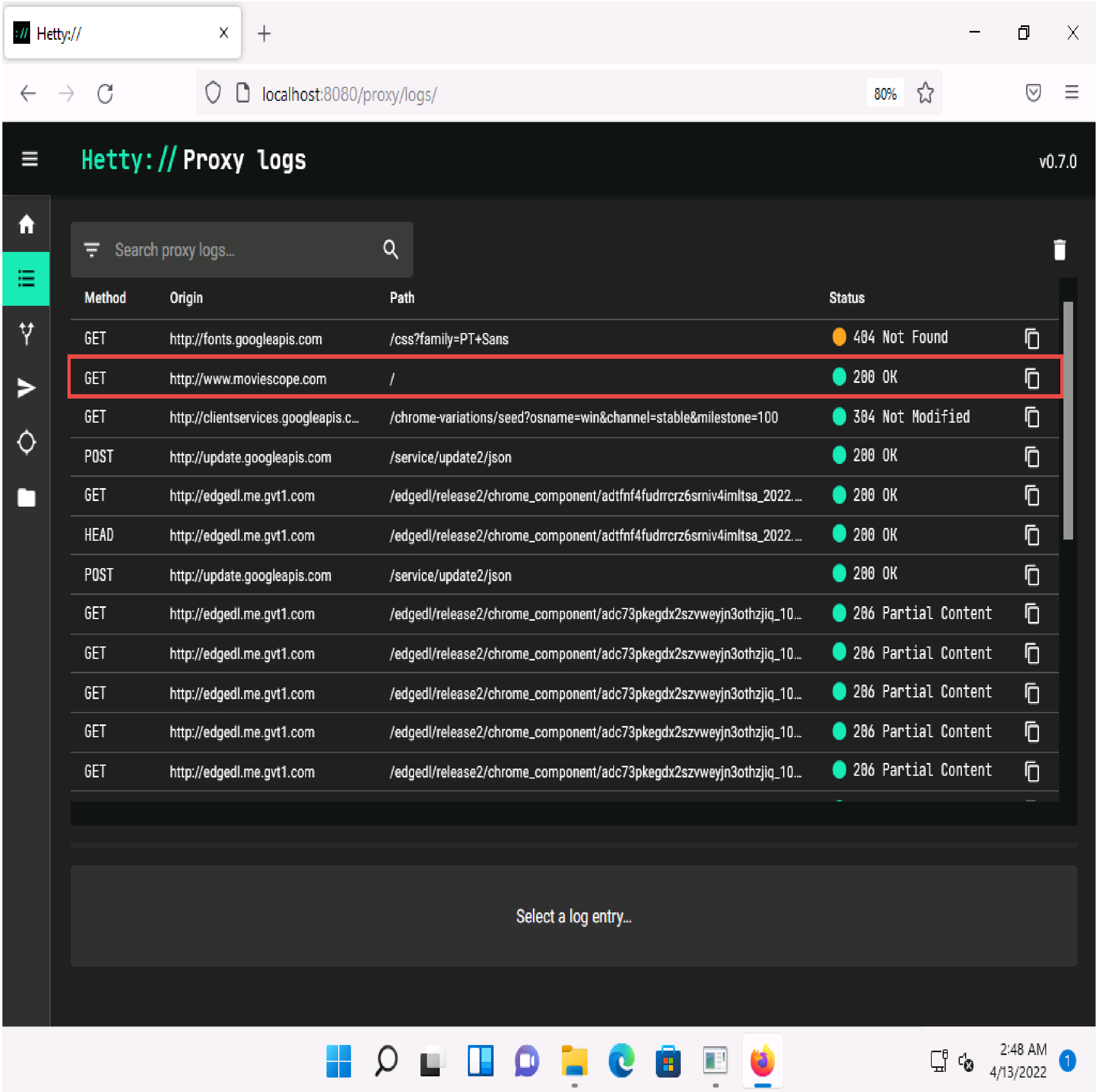
16. A **Settings** window appears, with the **Proxy** settings in the right pane.
17. In the **Manual proxy setup** section, make the following changes:
    - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
    - In the **Address** field, type **10.10.1.11** (the IP address of the attacker's machine, here, **Windows 11**).
    - In the **Port** field, type **8080**.
    - Click **Save**.



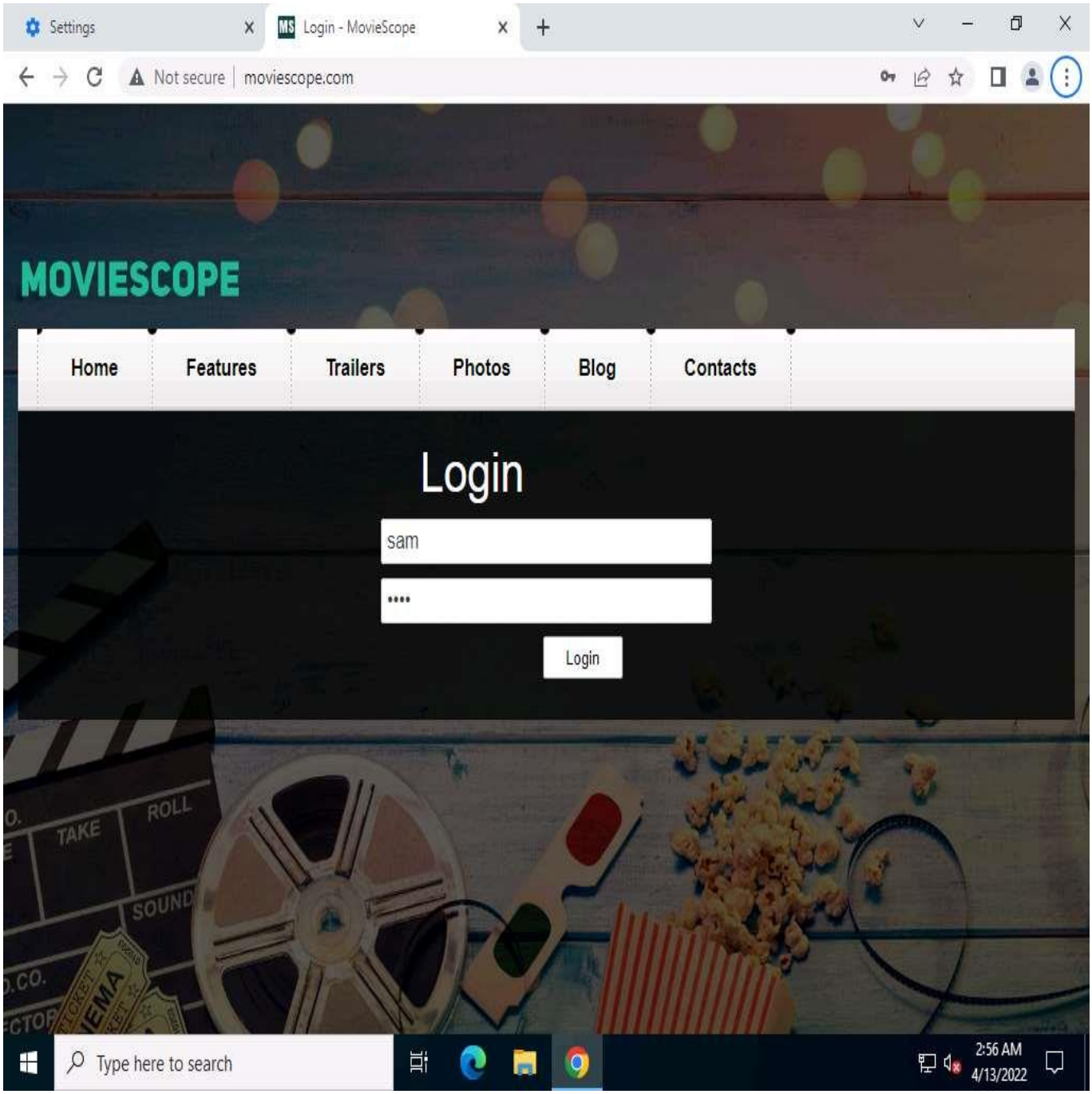
18. ☐ After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
19. ☐ Now, in the browser window open a new tab, in the address bar, type **http://www.moviescope.com** and press **Enter**.



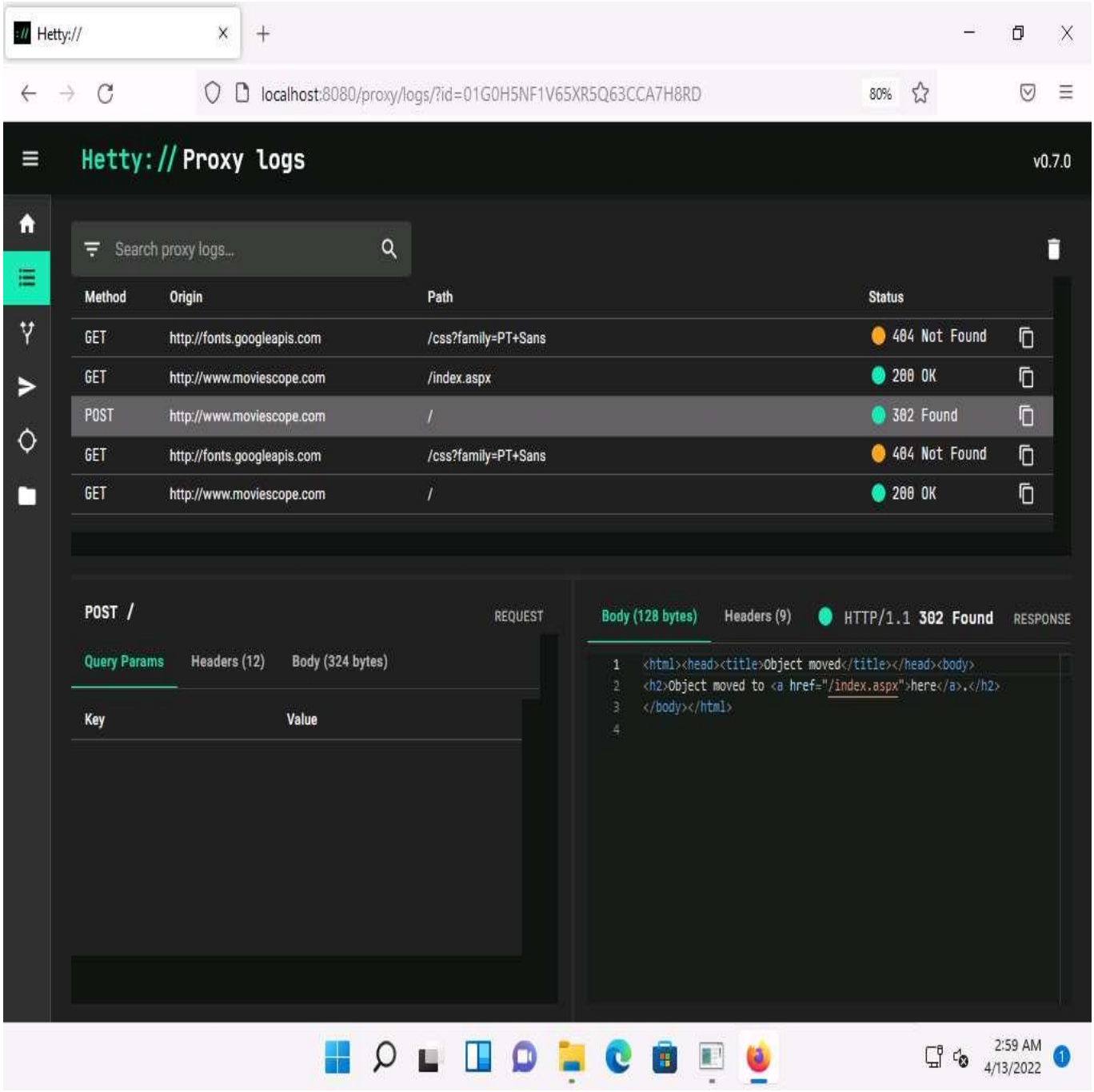
20. ☐ Click Windows 11 to switch to the **Windows 11** machine.
21. ☐ You can observe that the logs are captured in the **Proxy logs** page. Here, we are focusing on logs associated with moviescope.com website.



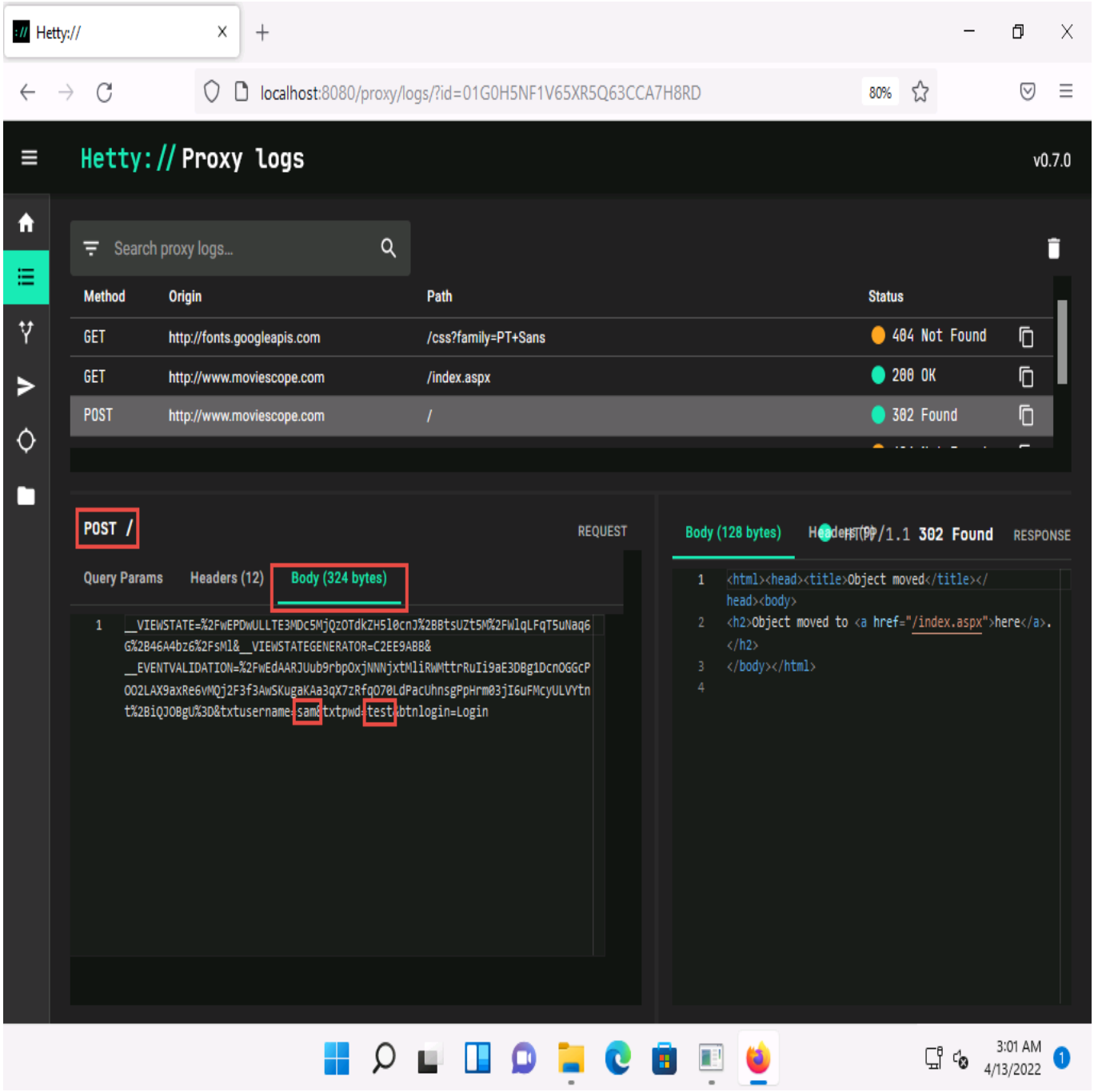
22. ☐ Click Windows Server 2022 to switch back to the **Windows Server 2022** machine.
23. ☐ In the **MovieScope** website, login as a victim with credentials as **sam**/**test**.



24. ☐ Now, click Windows 11 to switch to the **Windows 11** machine.
25. ☐ In the **Proxy logs** page, scroll-down to check more logs on moviescope website. Check for **POST** log captured for the target website.



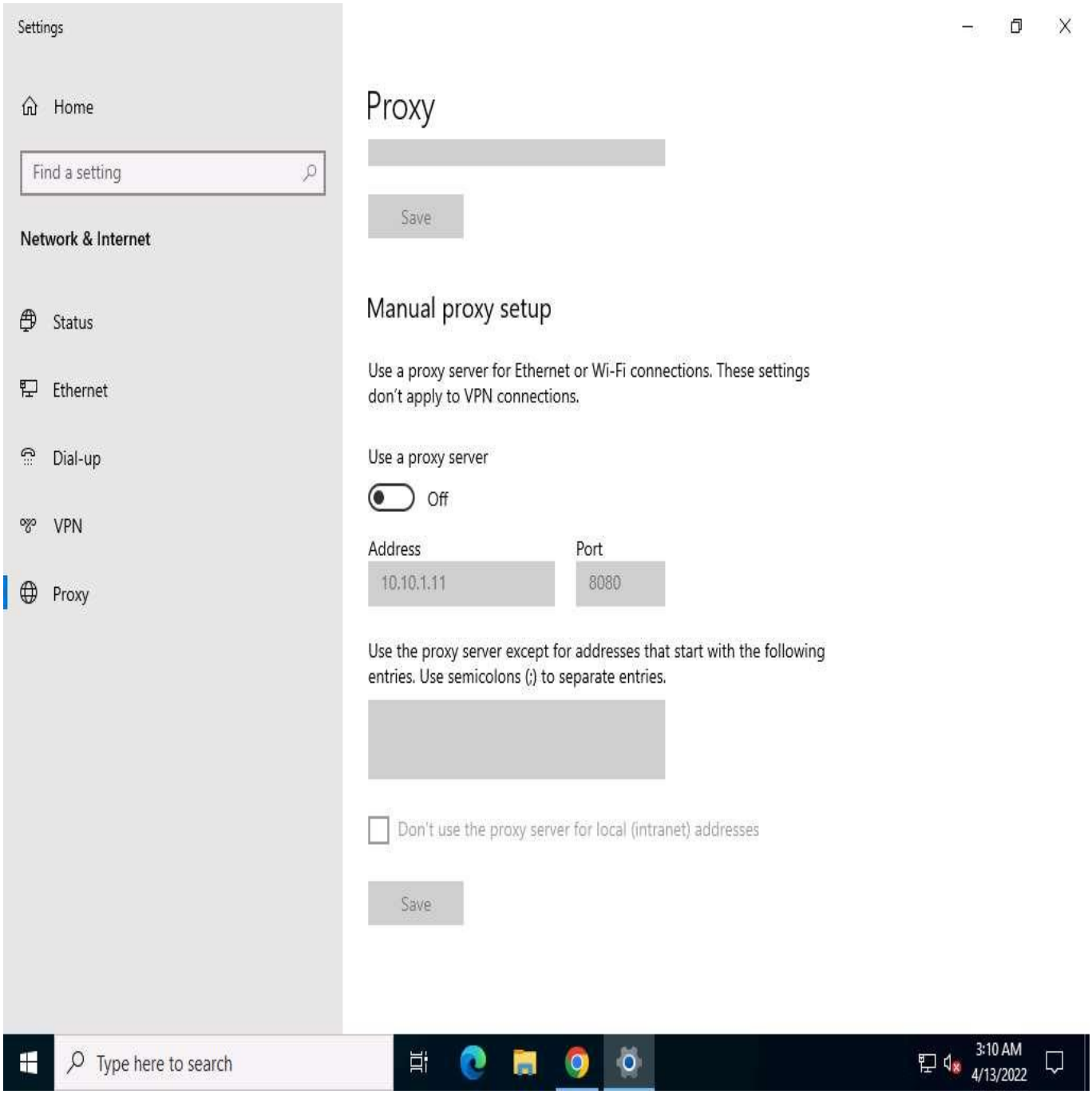
26. ☐ Select the **POST request** and in the lower section of the page, select **Body** tab under **POST** section.
27. ☐ Under the **Body** tab, you can observe the captured user credentials, as shown in the screenshot.



28. ☐ The captured credentials can be used to log in to the target user's account and obtain further sensitive information.
29. ☐ 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 13-16** again.

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

30. ☐ 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.



31. ☐ This concludes the demonstration of HTTP traffic interception using Hetty.
32. ☐ Close all open windows and document all the acquired information.