EC-Council

codered
FROM EC-COUNCIL

CHAPTER 9

APPLICATION SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 9:
Application Security

SCENARIO

The evolution of the Internet and web technologies, combined with rapidly increasing Internet connectivity, has led to the emergence of a new business landscape. Web applications are an integral component of online businesses. Everyone connected via the Internet is using various web applications for different purposes, including online shopping, email, chats, and social networking. Web applications are becoming increasingly vulnerable to sophisticated threats and attack vectors. An outdated or insecure application can pose a serious security threat and, in turn, affect network security.
Hence, a security professional must manage the security of the deployed applications and constantly monitor, patch, and upgrade the installed applications.

OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing application security. This includes knowledge of the following tasks:

- Implementing application whitelisting using AppLocker
- Performing application blacklisting using ManageEngine Desktop Central
- Performing application sandboxing using Sandboxie
- Detecting web application vulnerabilities using OWASP ZAP
- Testing injection vulnerability using Burp Suite
- Determining application-level attacks using various techniques
- Gathering information on a web server using various footprinting tools

OVERVIEW INTERRUPTED SESSIONS

Secure application means that the application ensures confidentiality, integrity, and availability of its restricted resources throughout the application lifecycle. The securing process involves some tools and procedures to protect the application from cyber-attacks. Cybercriminals are motivated to target vulnerabilities present in an application and exploit them to steal confidential data, tampering code, and compromise the whole application.
The process of securing an application involves deploying, inserting, and testing every component of an application. This procedure finds out all the vulnerabilities present in restricted resources such as object, data, feature, or function of an application designed to be accessed by only authorized users.

LAB TASKS

A cyber security professional or security professional uses numerous tools and techniques to implement network security policies. The recommended labs that will assist you in learning the implementation of network security controls include:

01 **Implement Application Whitelisting using AppLocker**

02 **Blacklist Application using Manage Engine Desktop Central**

03 **Perform Application Sandboxing using Sandboxie**

04 **Detect Web Application Vulnerabilities using OWASP ZAP**

05 **Detect Injection Vulnerability using Burp Suite**

06 **Determine Application-Level Attacks**

07 **Perform Web Server Footprinting using Various Footprinting Tools**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: **IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER**

Implement Defense-in Depth using the AppLocker tool.

LAB SCENARIO

By implementing AppLocker, security professionals can control software access to executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers. AppLocker enables security professionals to maintain application inventory, prevent unwanted software infection, and standardize software within an organization's network.

OBJECTIVE

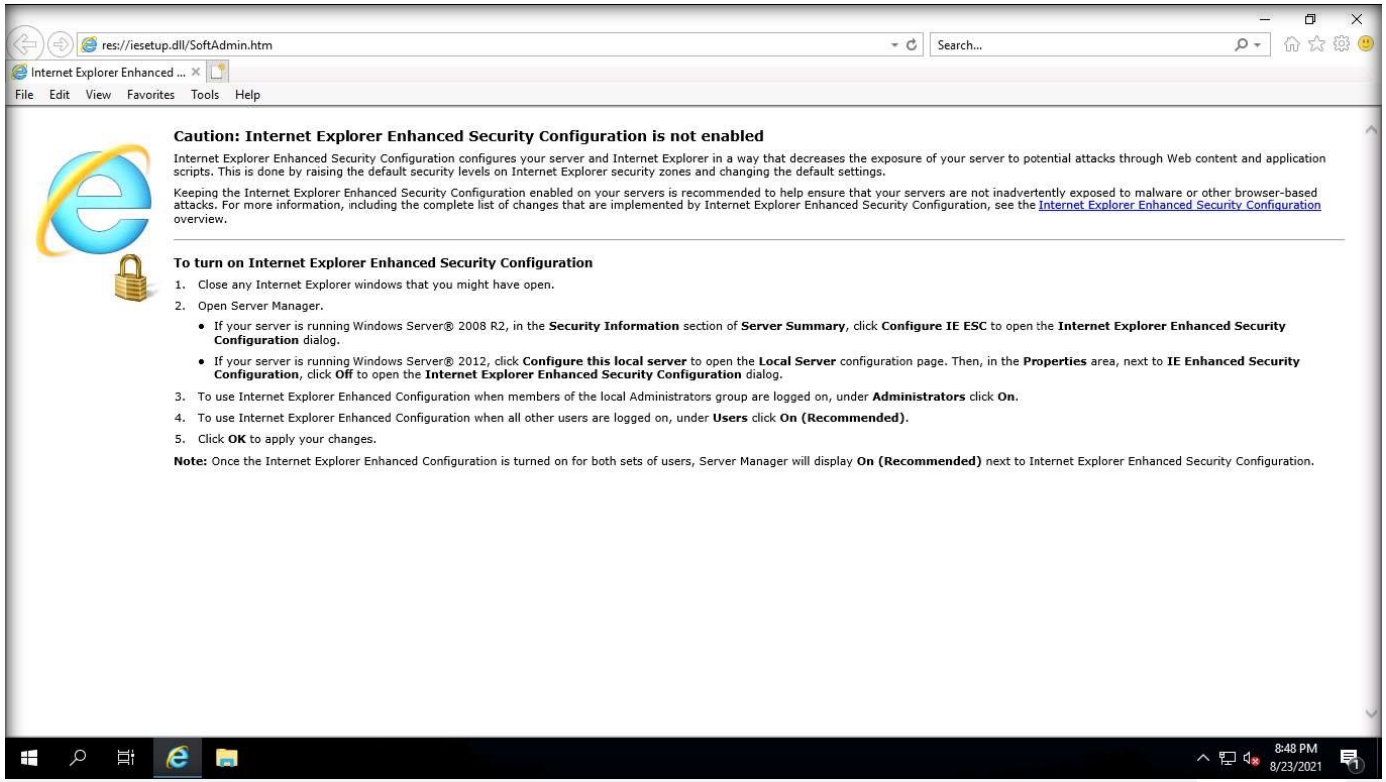
The objective of this lab is to deploy application whitelisting on the domain network using group policy.

OVERVIEW OF APPLOCKER

AppLocker is an in-built Windows security program that can be used to control which applications the users can run. When AppLocker rules are enforced, apps that are excluded from the list of allowed apps are blocked from running. The apps include executable files, windows installer files, and DLLs. The default executable rules are based on paths and all files under those paths are included in the list of allowed apps. Group policy application rules can be implemented in a domain using AppLocker.

Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on AD Domain Controller and Web Server virtual machines.
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.
Note: If the network screen appears, click Yes.
3. Launch Internet Explorer from the taskbar.
Note: If a Set up Internet Explorer window appears, click on Ask me later.
4. The Internet Explorer page will open. Close the Internet Explorer.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

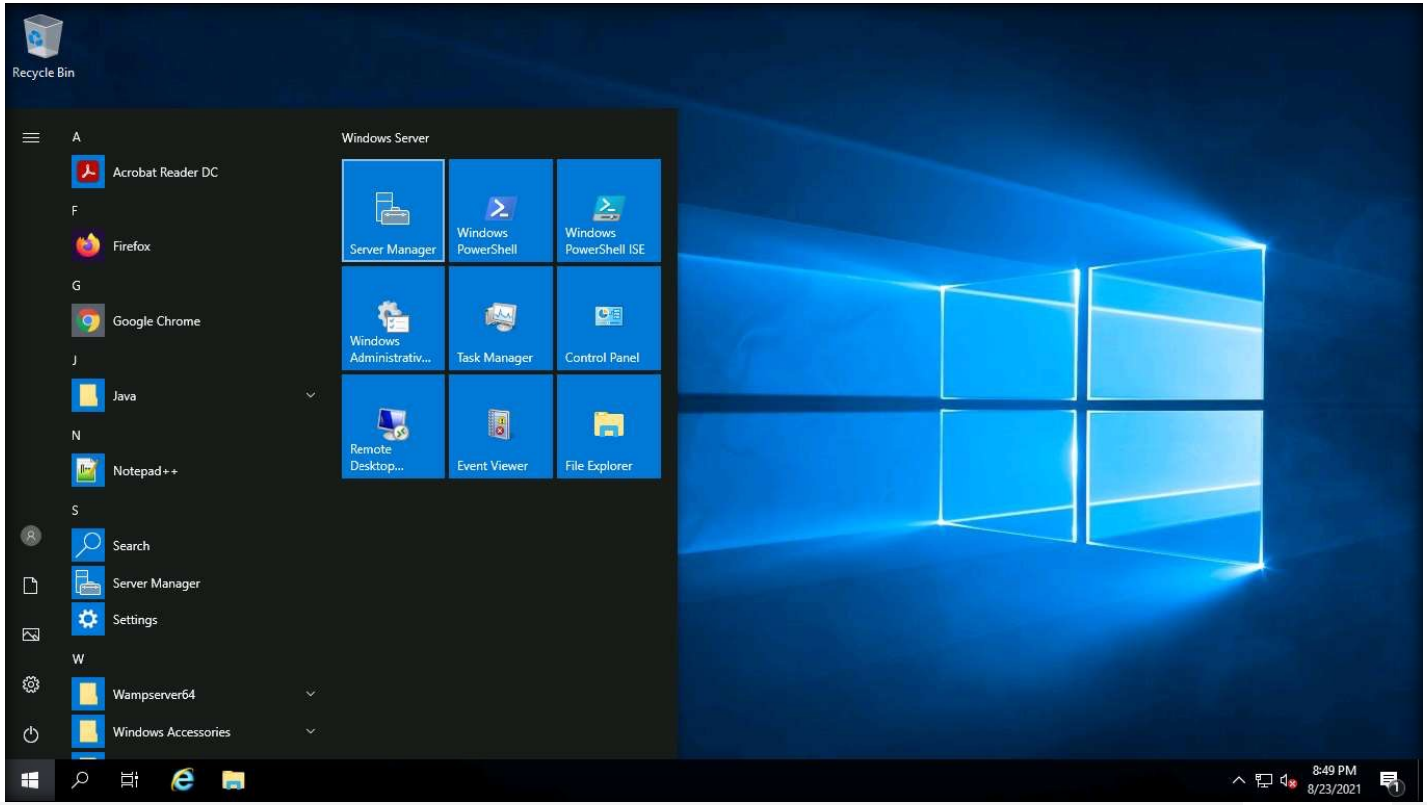


Note: As per policy, employees of several organizations are barred from using Internet Explorer. In this case, a security professional must know how to block Internet Explorer using AppLocker.

5. The Internet Explorer can be blocked using AppLocker.

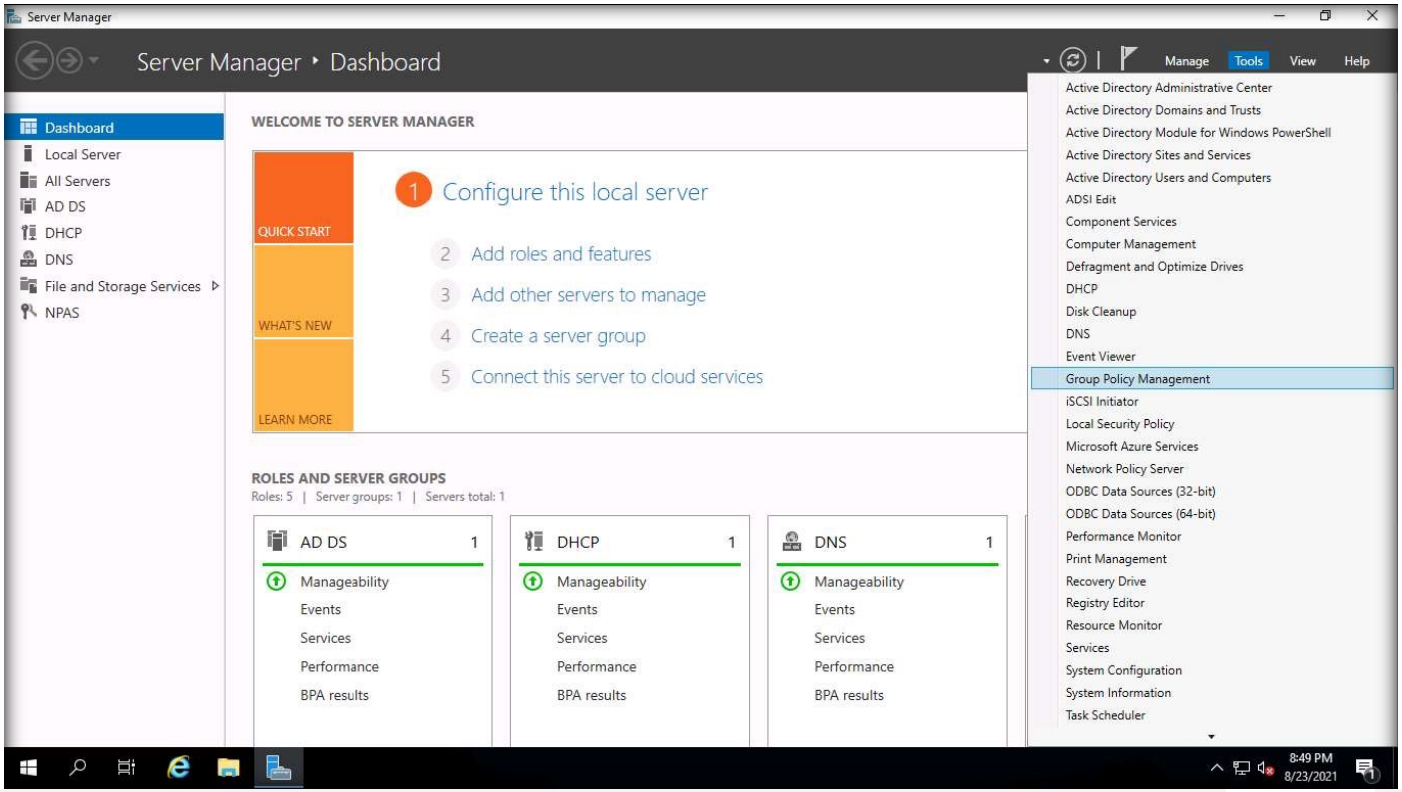
6. Click on Windows Start icon, select Server Manager.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



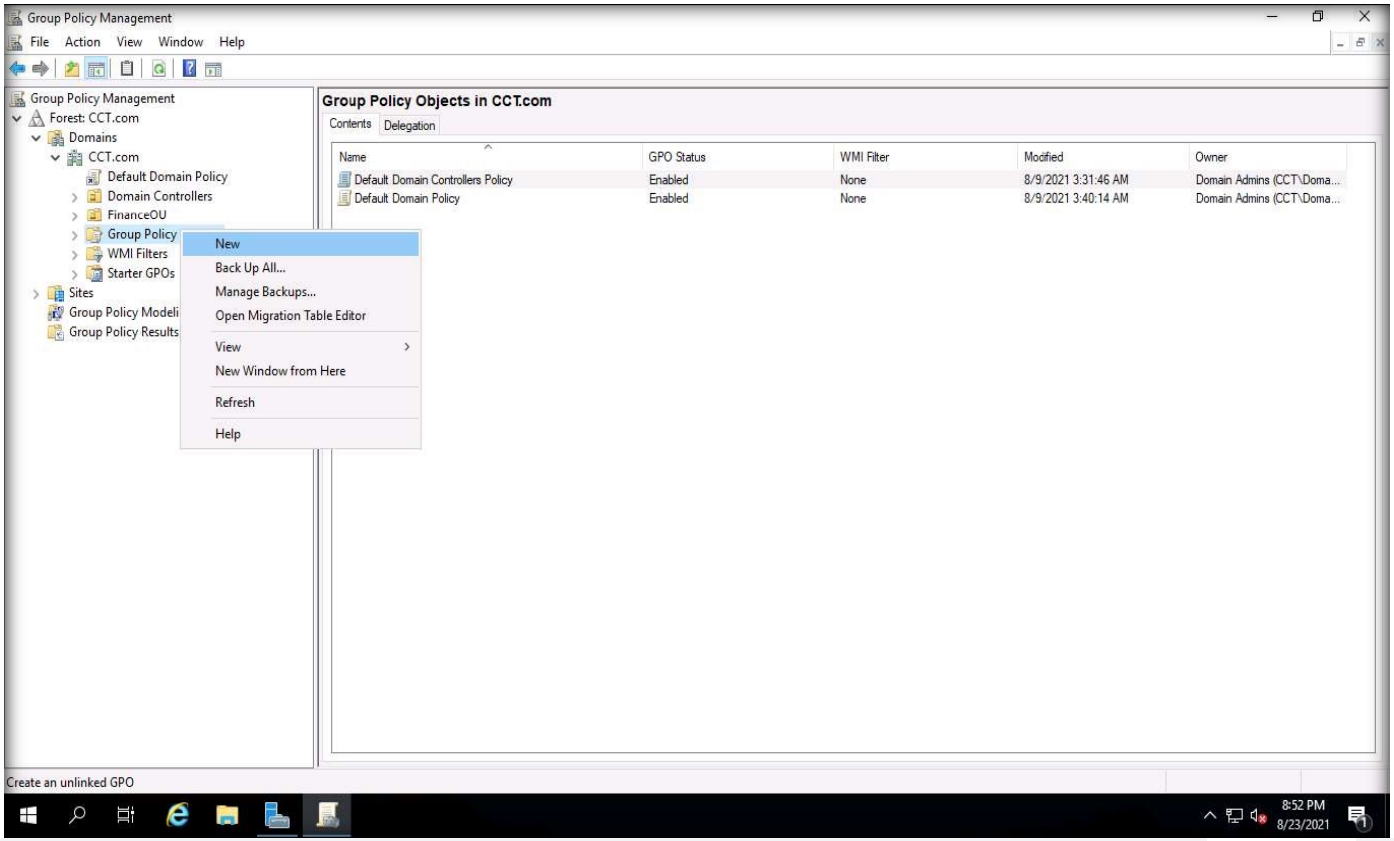
7. The Server manager window will open, navigate to the Tools menu, and select Group Policy Management.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



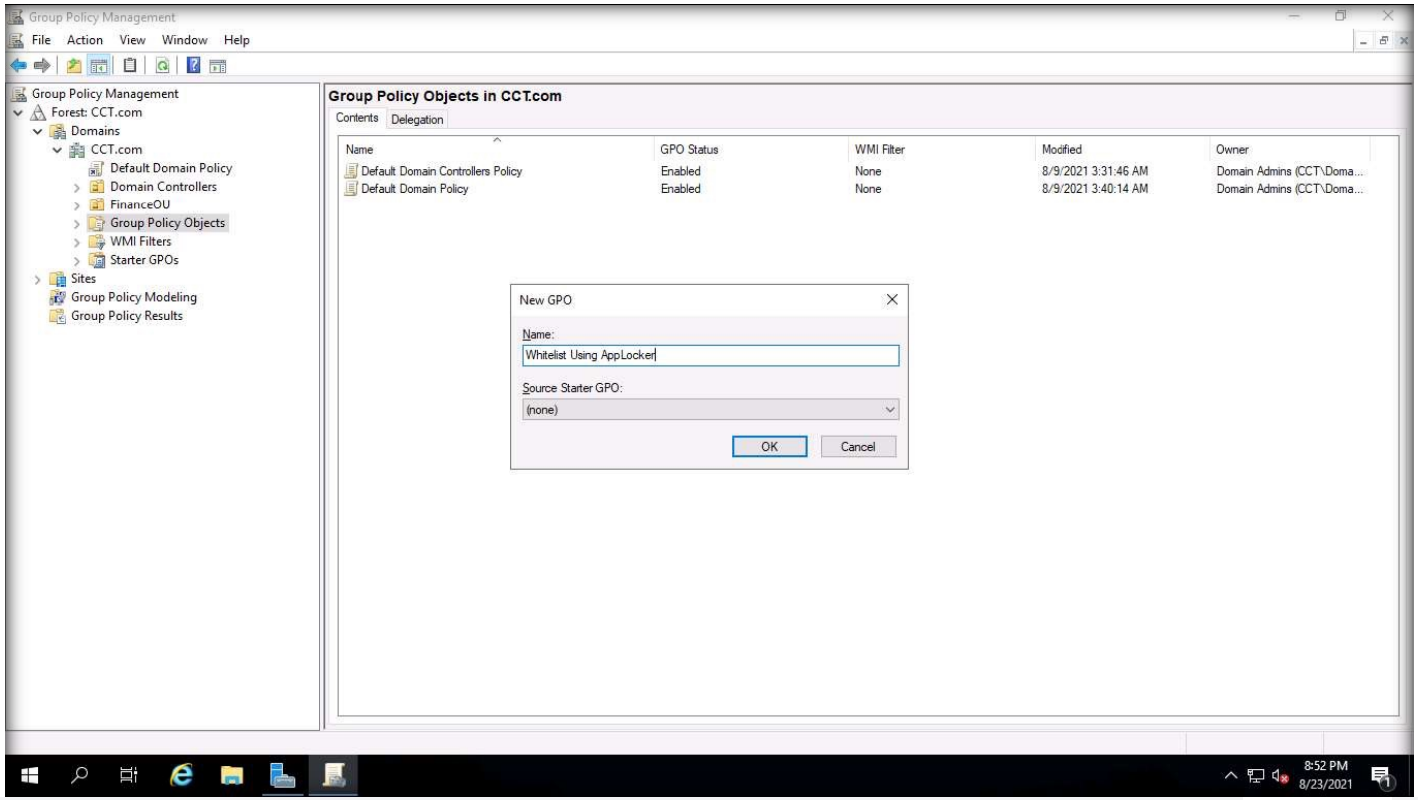
8. The Group policy Management window will open. Expand Forest: CCT.com, Domains, and CCT.com, navigate and select Group Policy Objects. Right-click on the Group Policy Objects (GPO) and select New.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



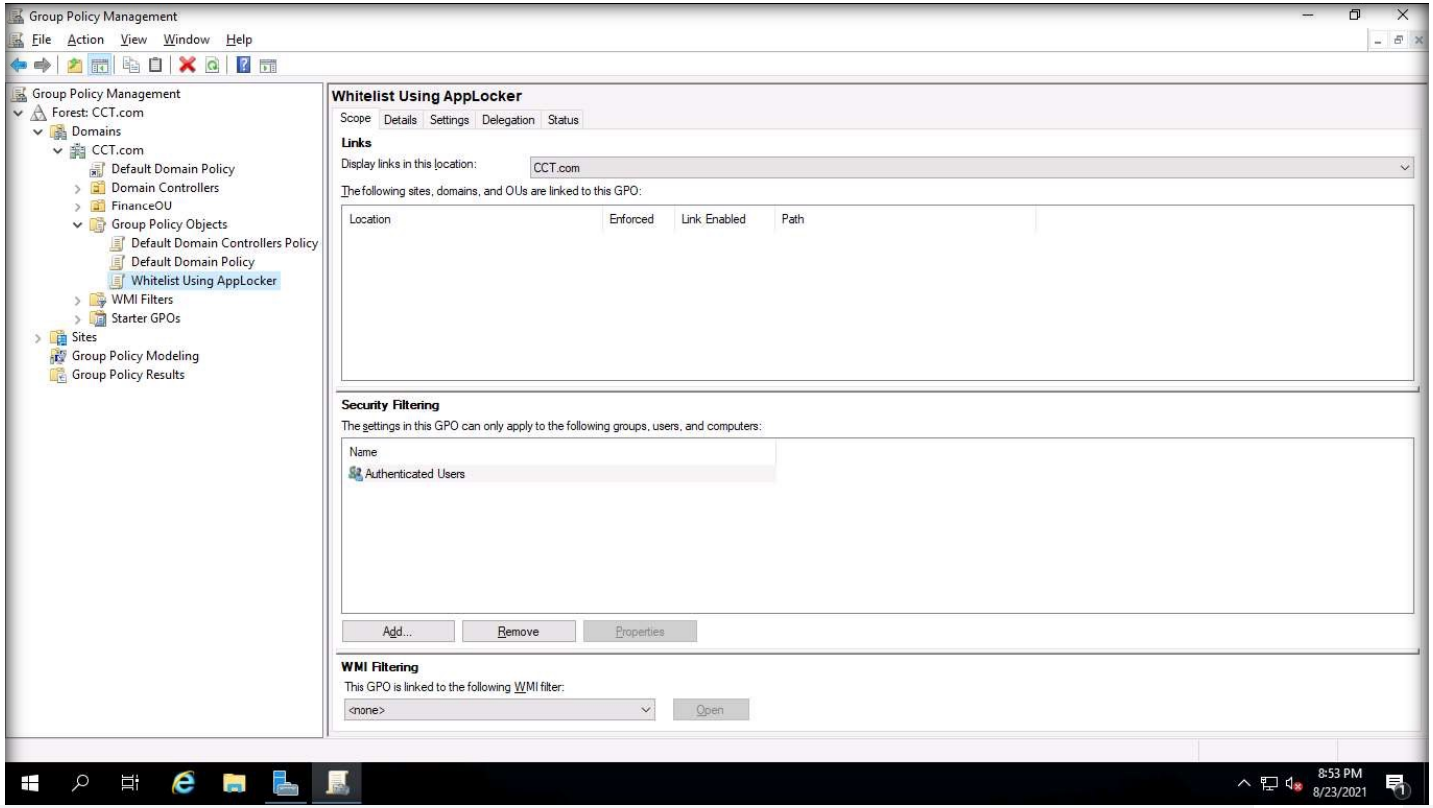
9. The New GPO prompt opens, type Whitelist Using AppLocker, and click on OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



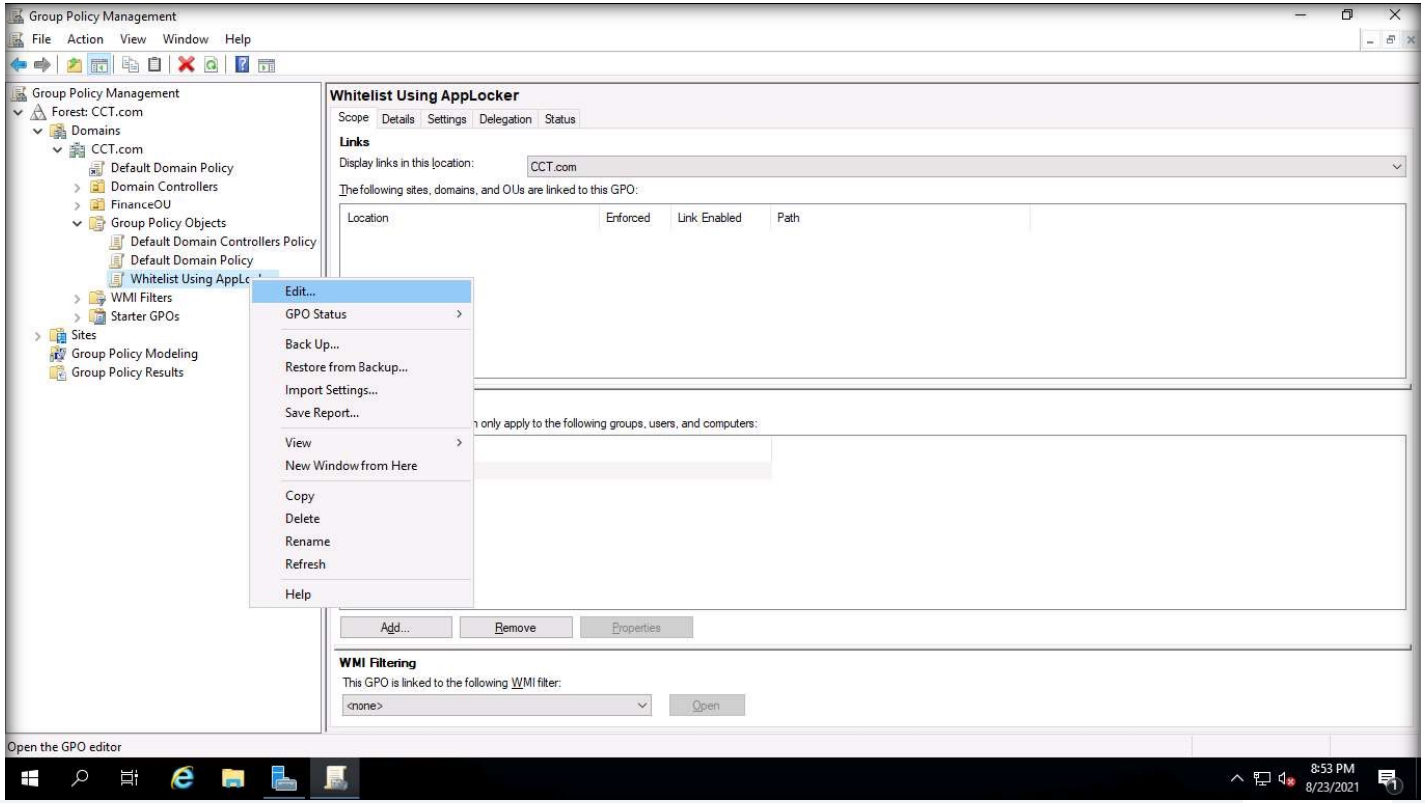
10. A new GPO named Whitelist Using AppLocker will be created in the Group Policy Objects folder.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



11. Right-click on the Whitelist Using AppLocker and select the Edit option.

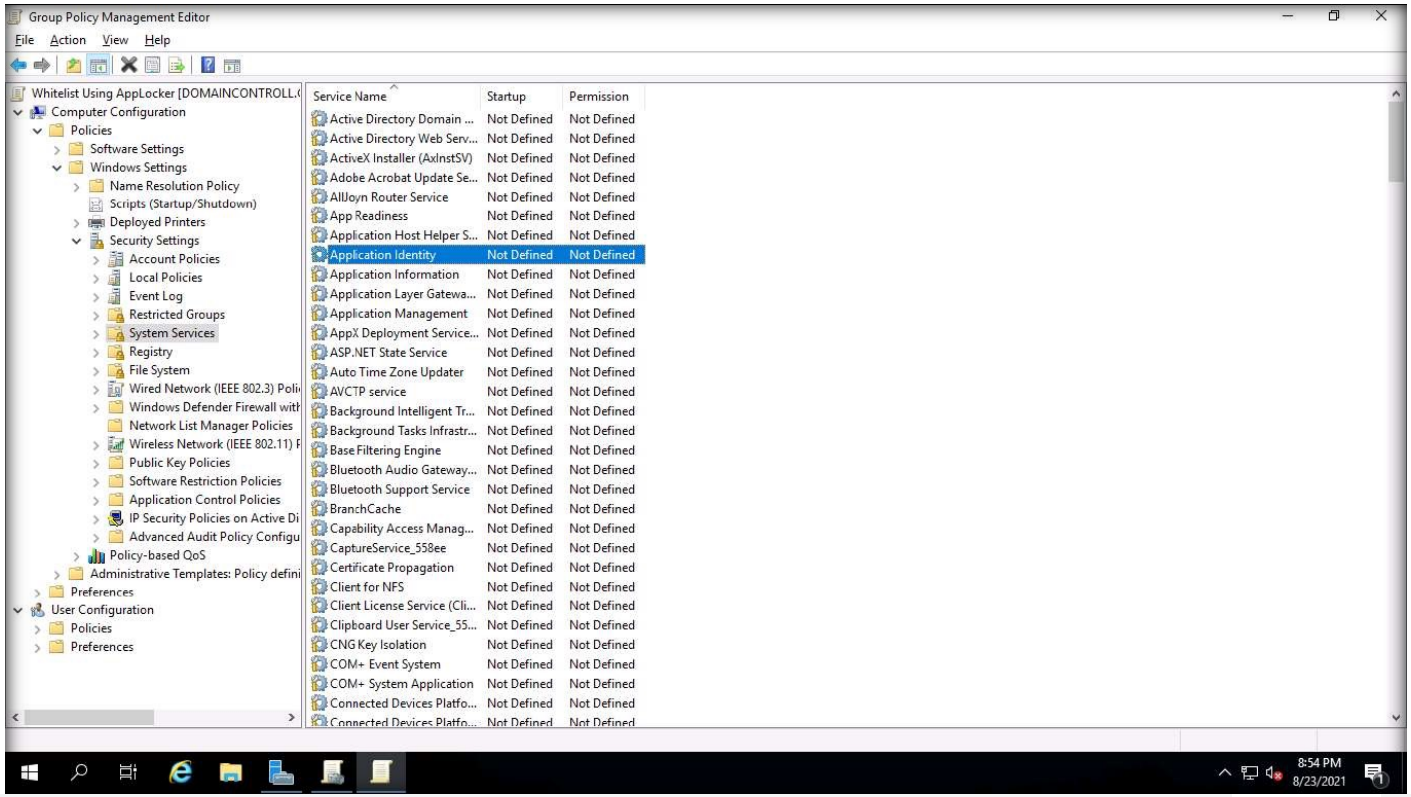
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



12. The Group Policy Management Editor window opens, expand and follow the path: Computer configuration → Policies → Windows Settings → Security Settings, select System Services.

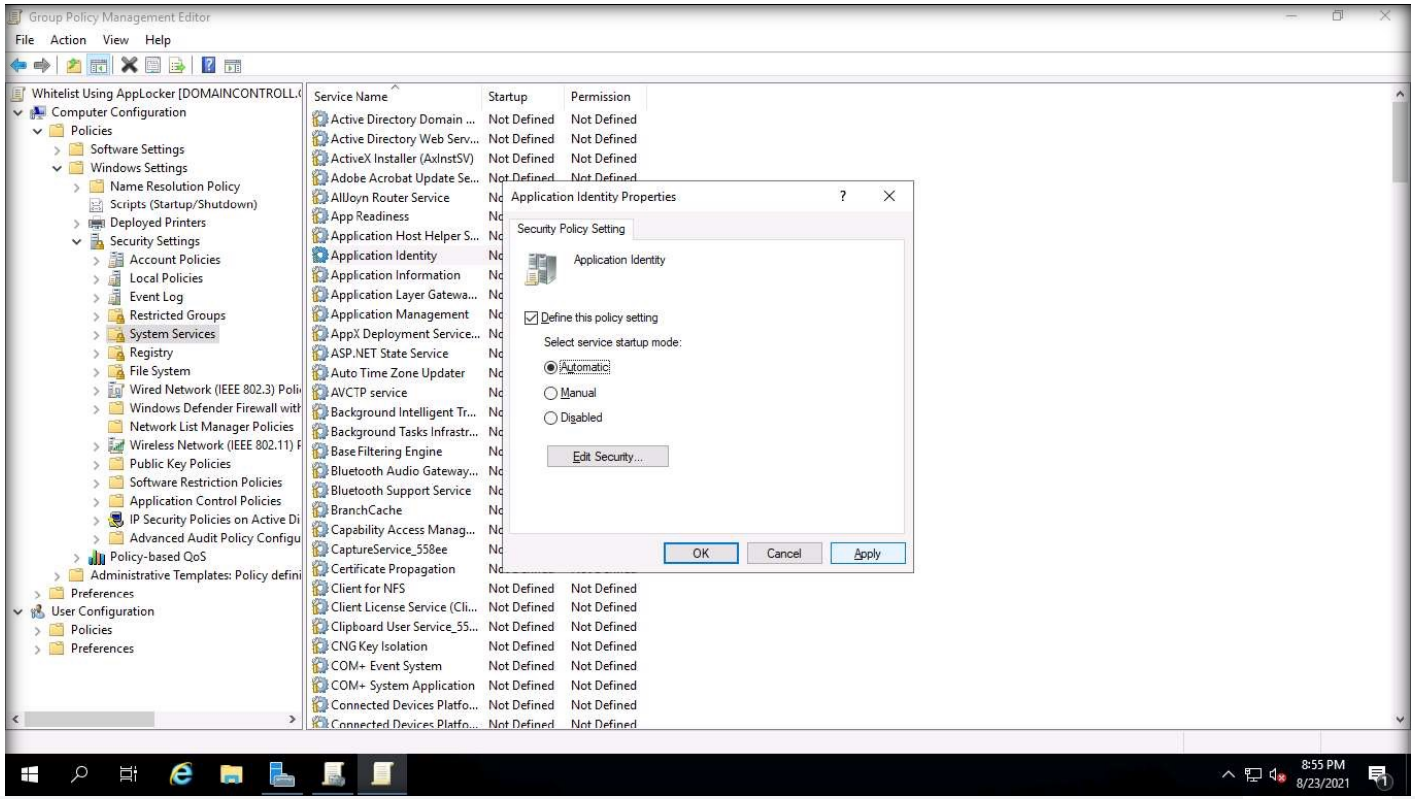
13. From the list of services visible on the right-side pane, double-click on Application Identity under Service Name in the right pane.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



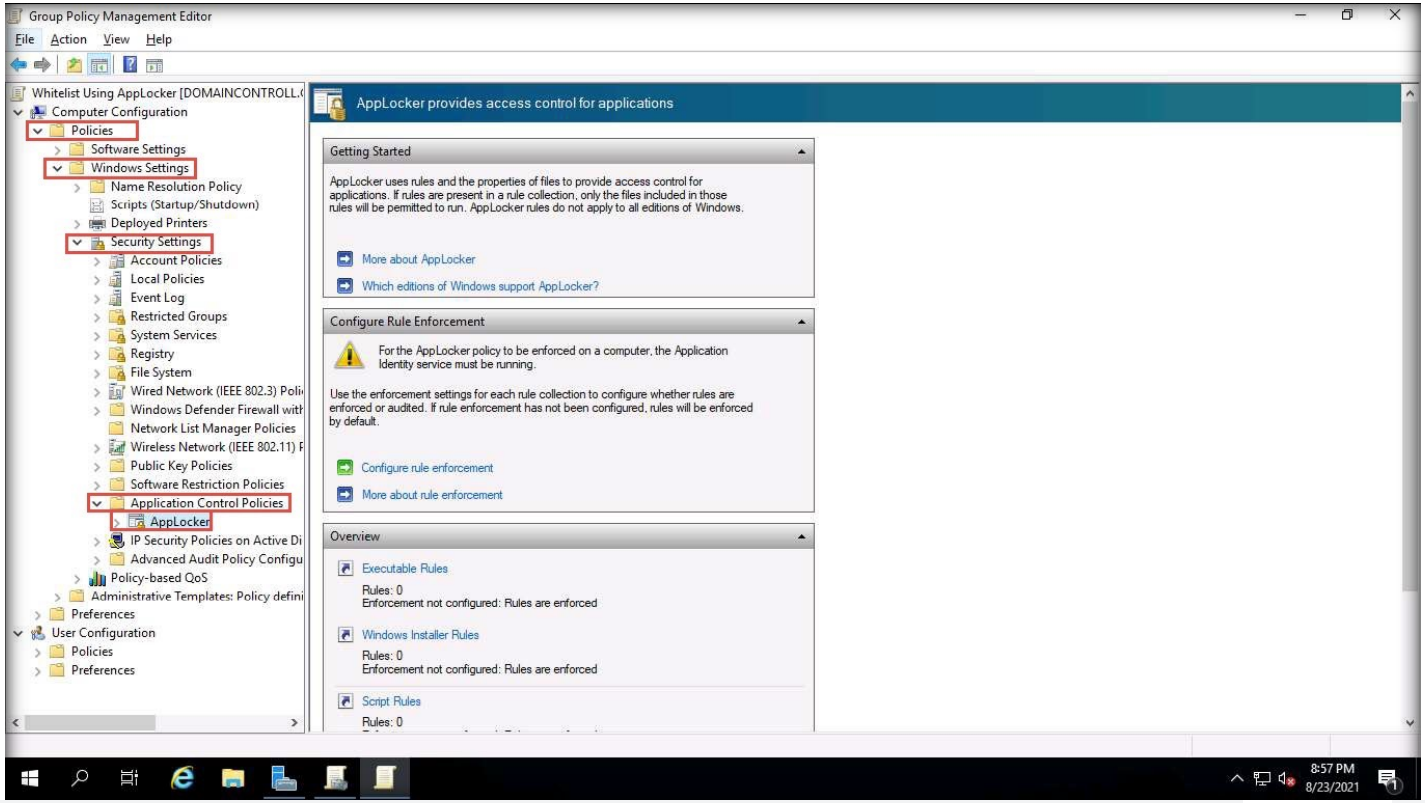
14. The Application Identity Properties window opens, check Define this policy setting, select Automatic, and click on Apply and OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



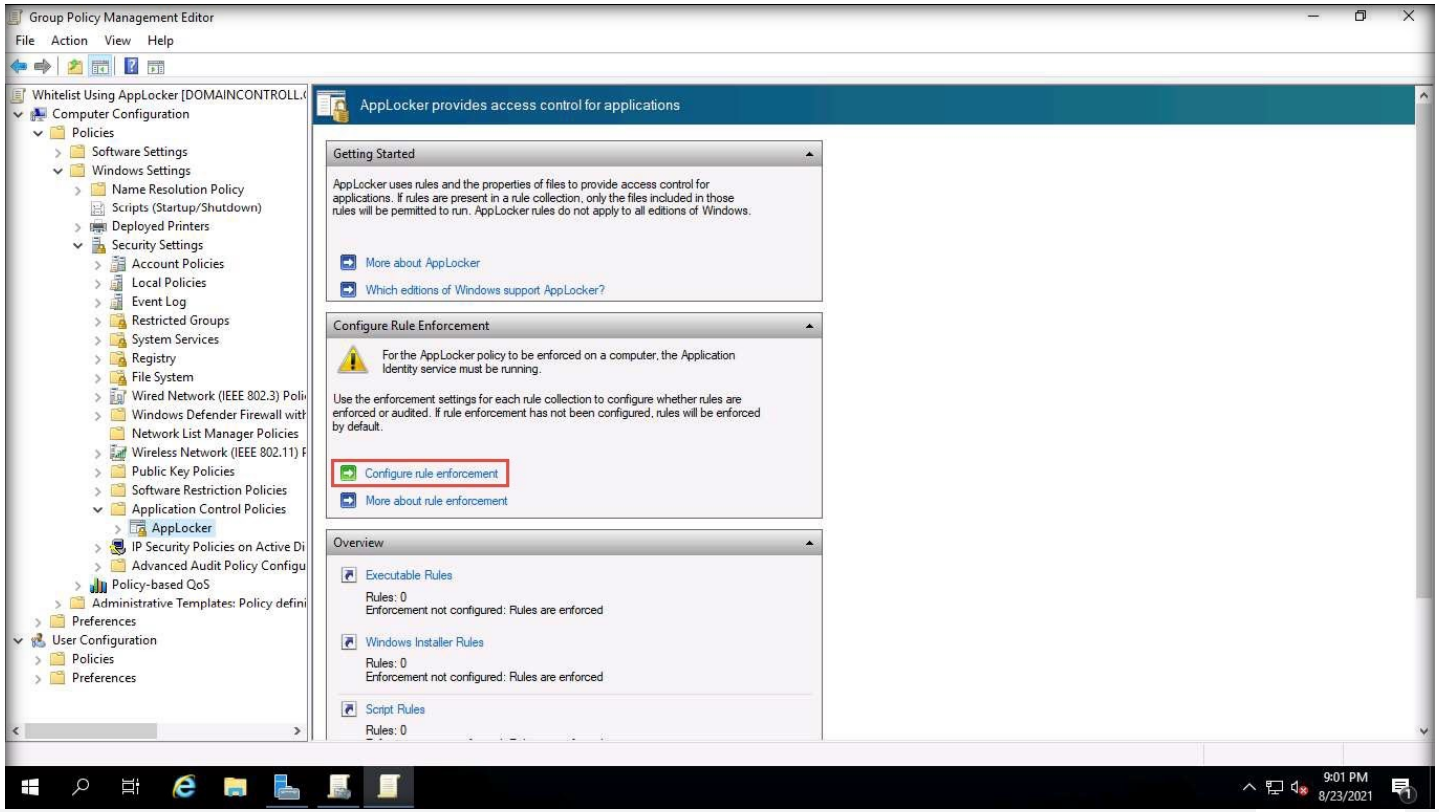
15. Next, scroll down under the left sidebar and navigate to Computer configuration → Policies → Windows Settings → Security Settings → Application Control Policies. Expand Application Control Policies, select and click on AppLocker.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



16. The AppLocker configuration option will appear in the right pane, click on the Configure rule enforcement link under the Configure Rule enforcement tab.

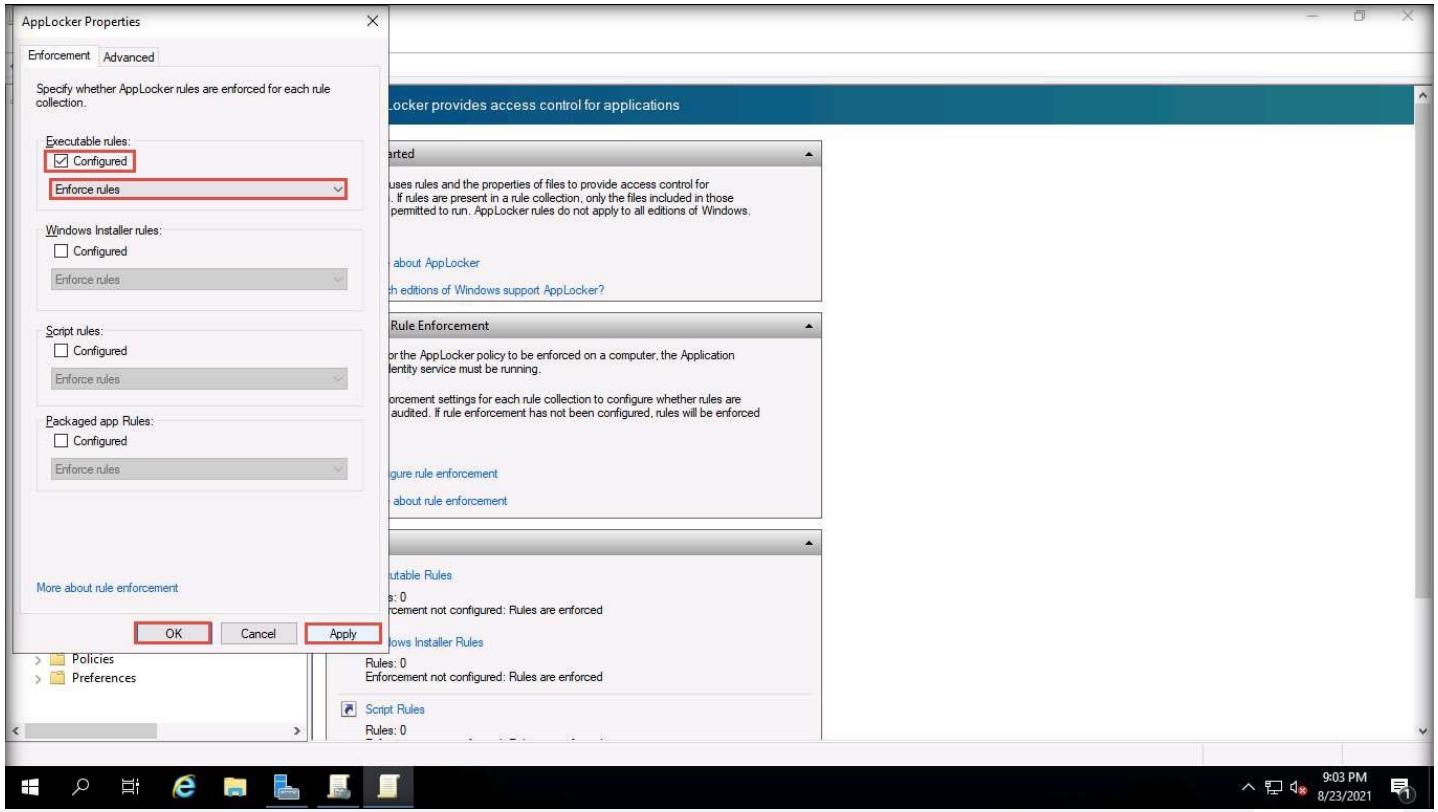
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



17. The AppLocker Properties window appears, here, the security professional can choose various enforcement rules to configure AppLocker. We choose the first option, that is, Executable rules: Configured.

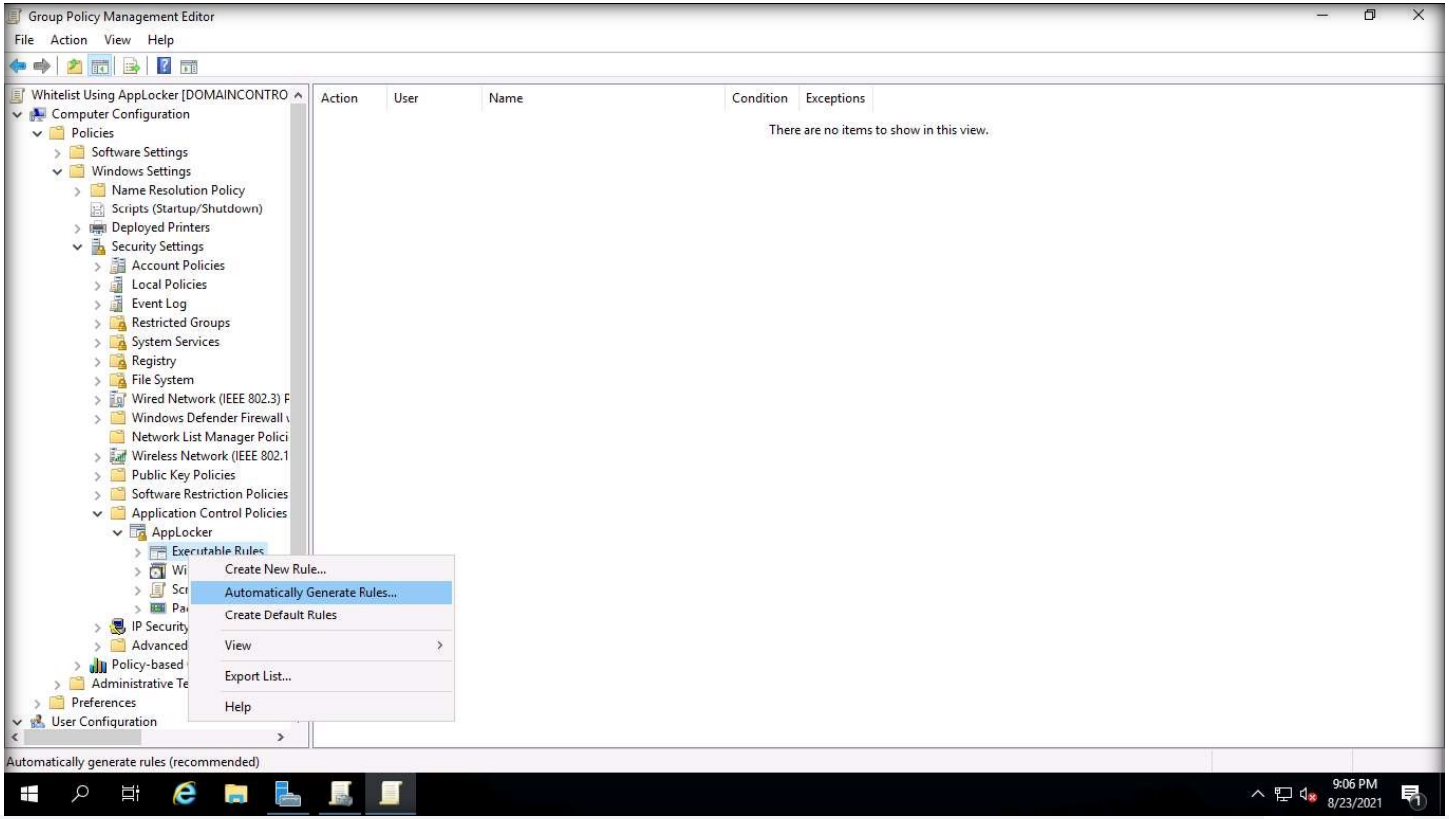
18. Check the Configured box and select Enforce rules from the dropdown list under the Executable rules section. Click Apply and then click OK. (Use the tab button in case you are having any difficulty in clicking Apply and OK button)

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



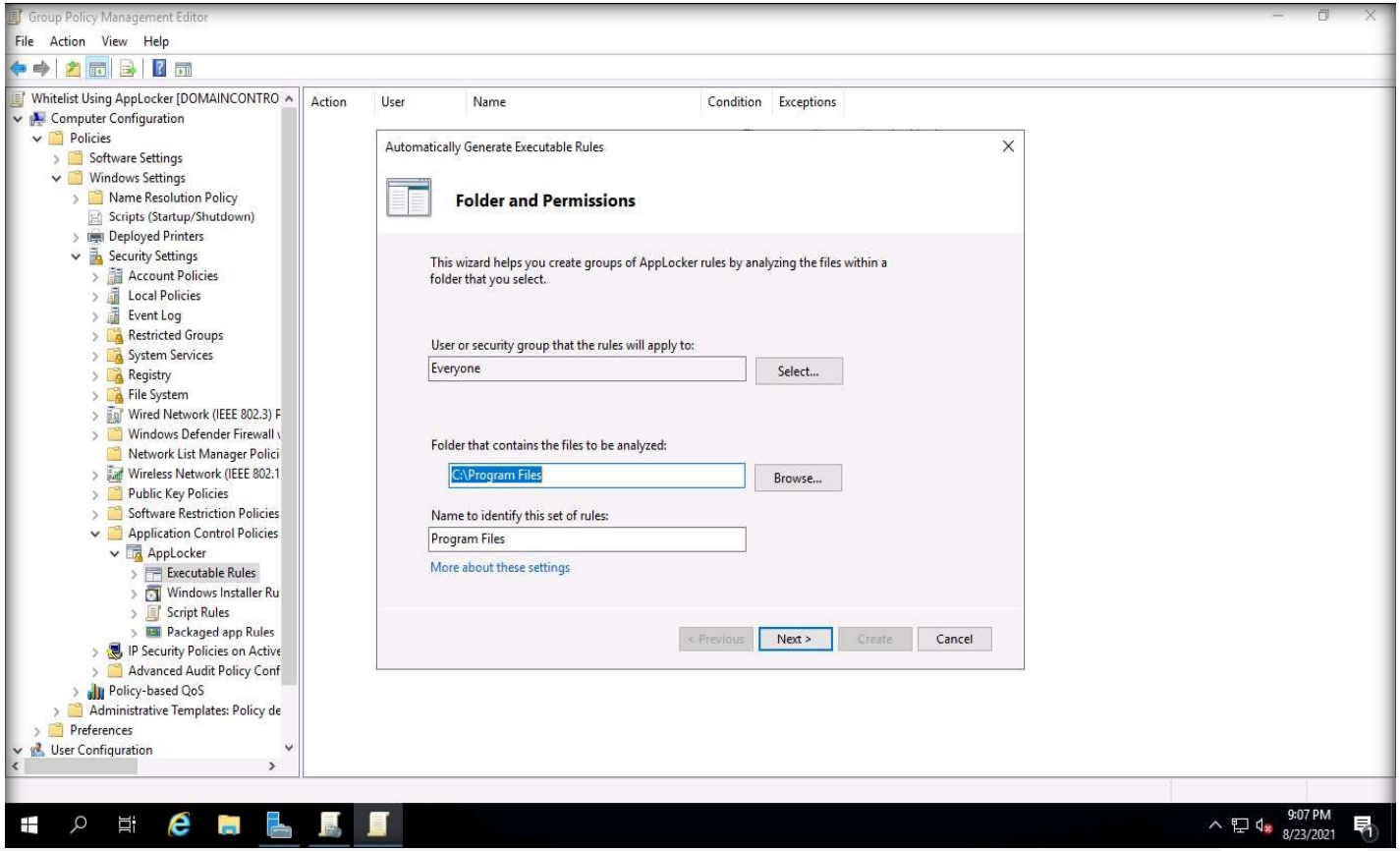
19. Expand AppLocker and right-click on the Executable Rules tab. Select Automatically Generate Rules....

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



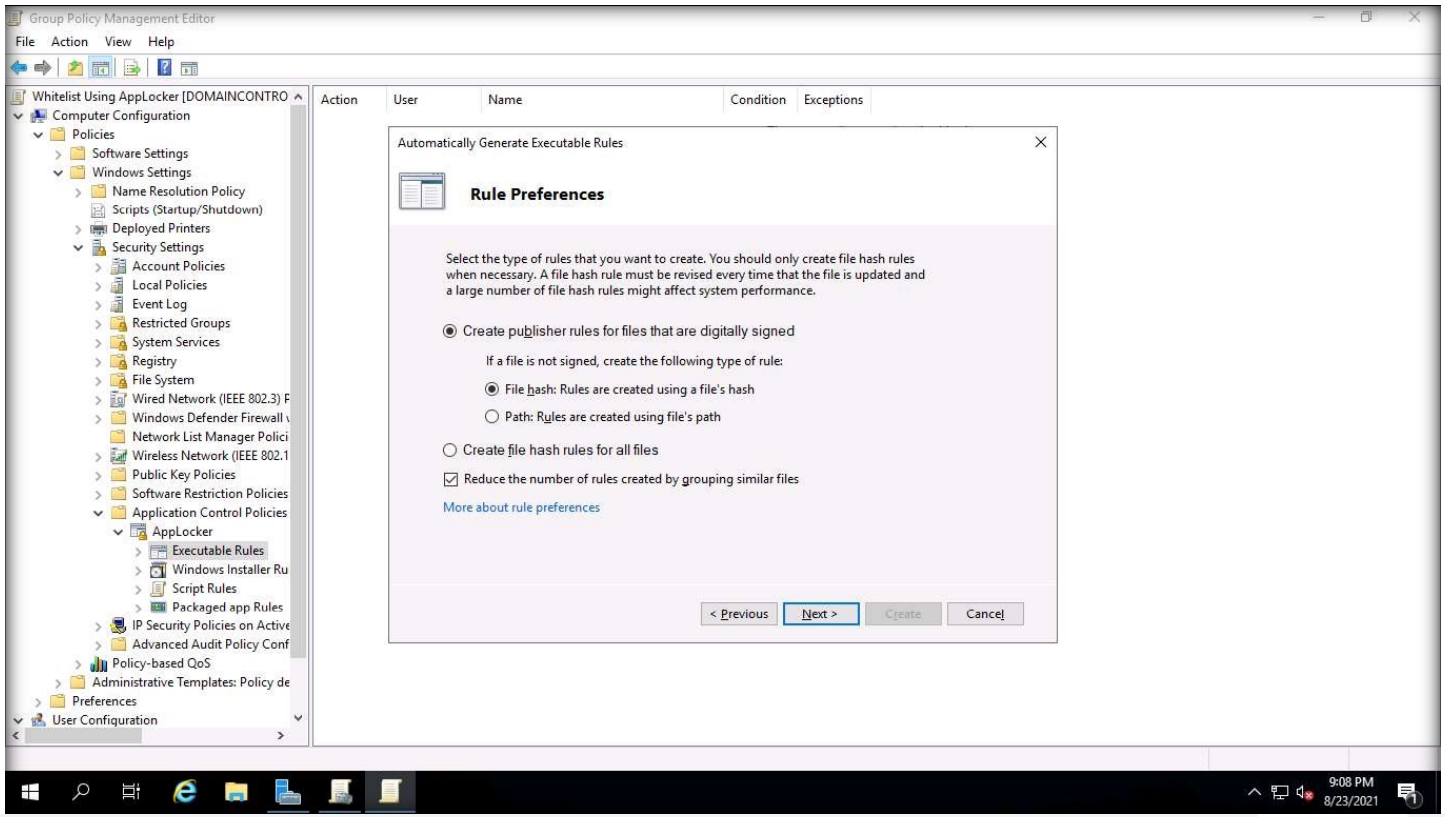
20. The Automatically Generate Executable Rules wizard appears, retain the default options and click on Next.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



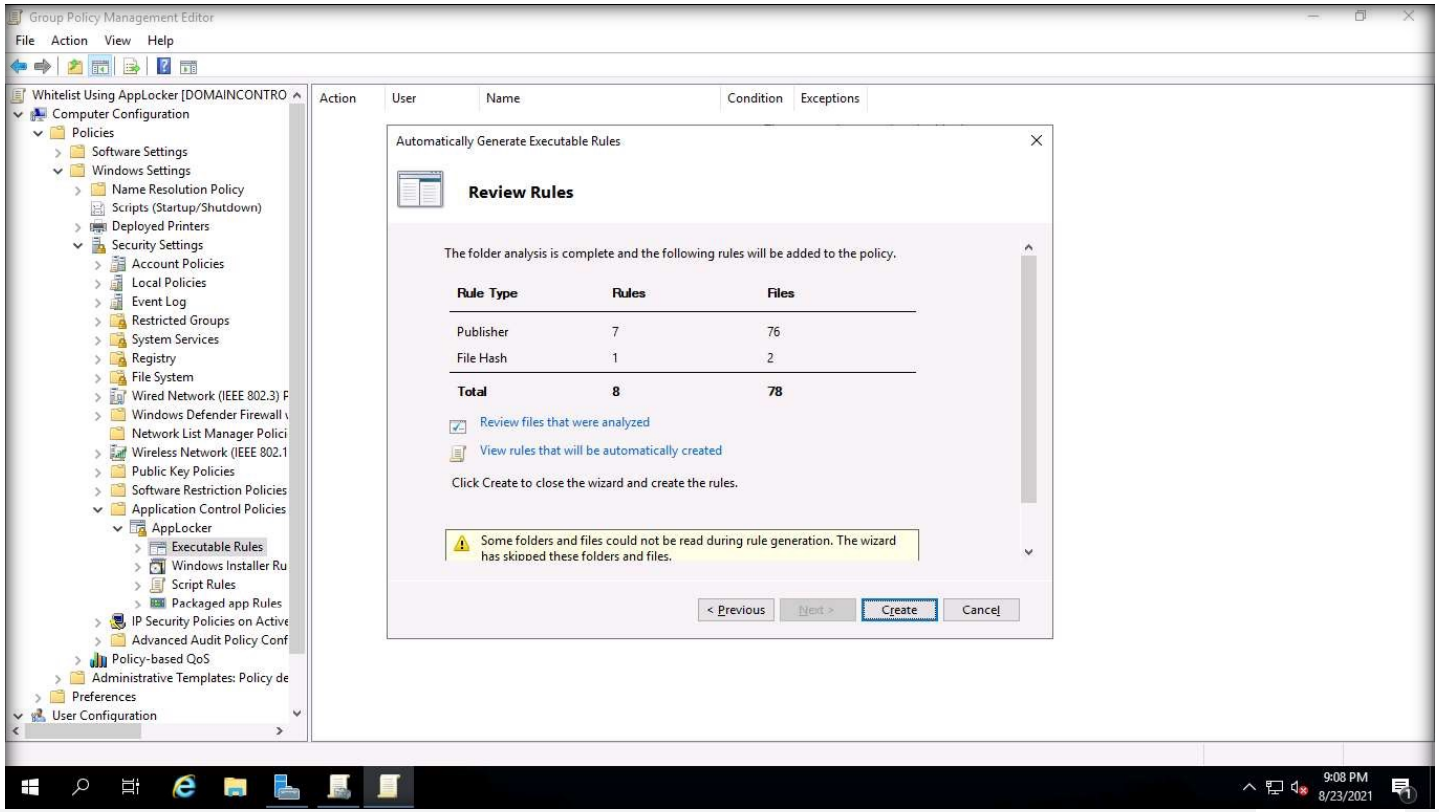
21. Retaining the default publisher rules, click on Next.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



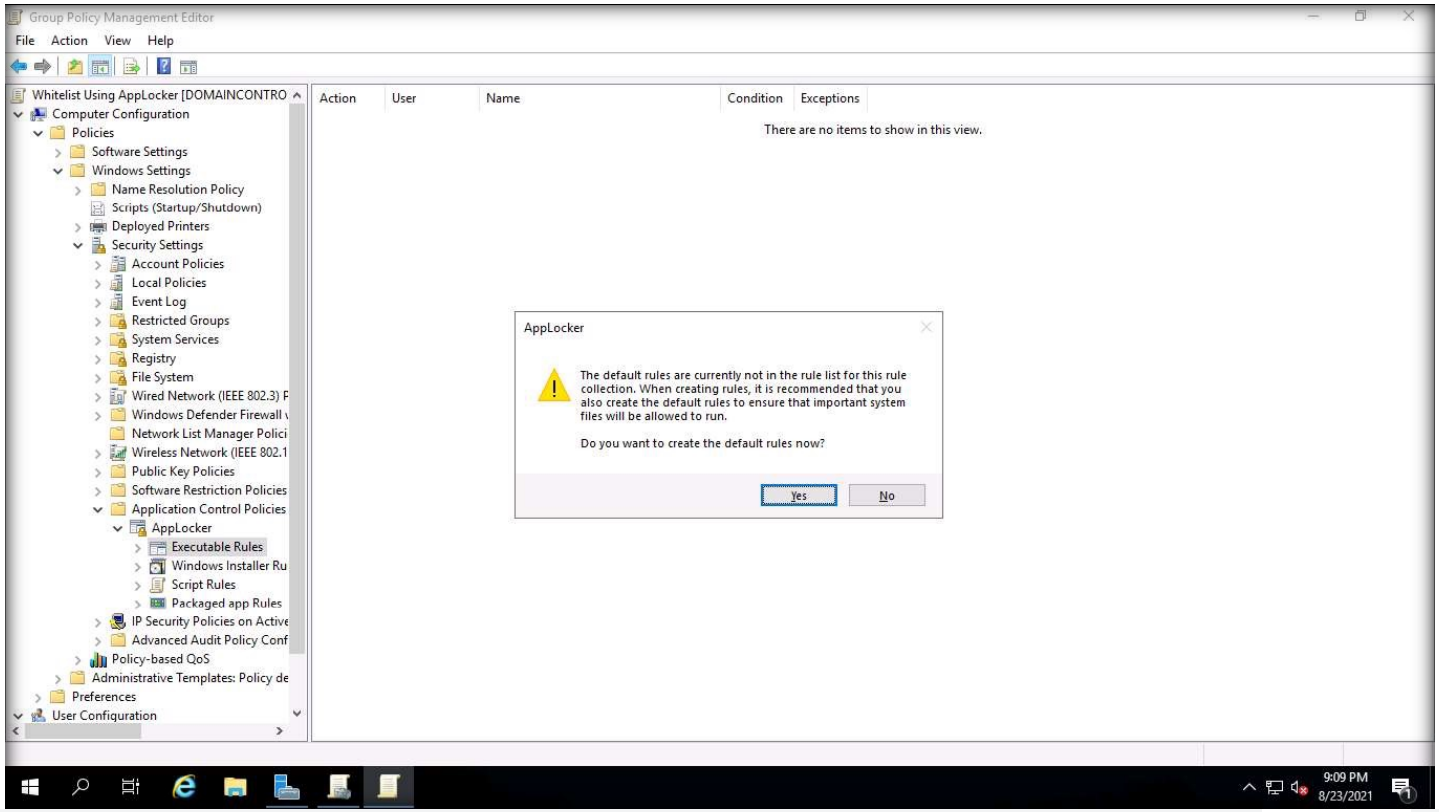
22. Once the rules are generated, you will be able to review publisher rules. Click on Create.
Note: The number of Rules and Files might differ in your lab environment.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



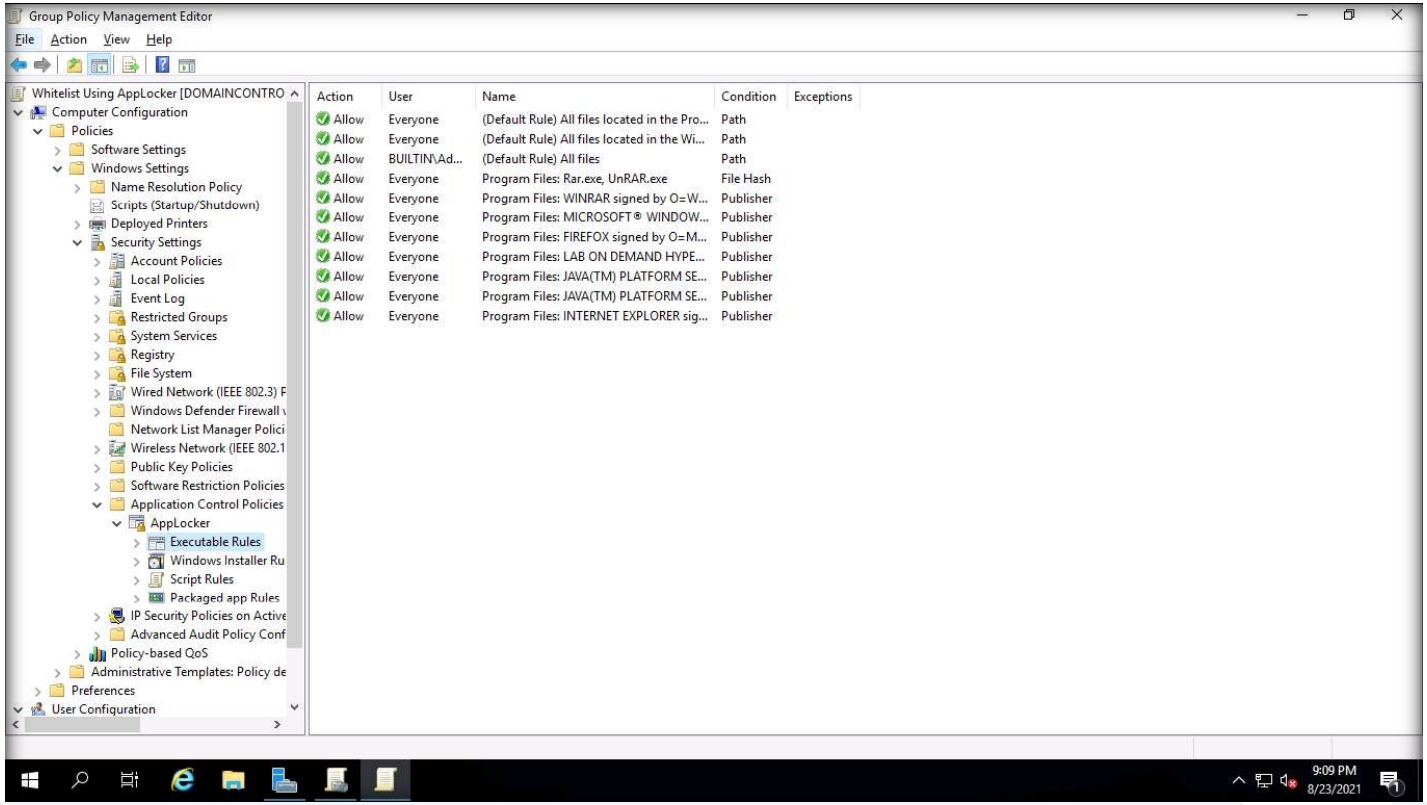
23. The default rule creation alert message box appears, click on Yes; this will automatically generate the executable rules.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



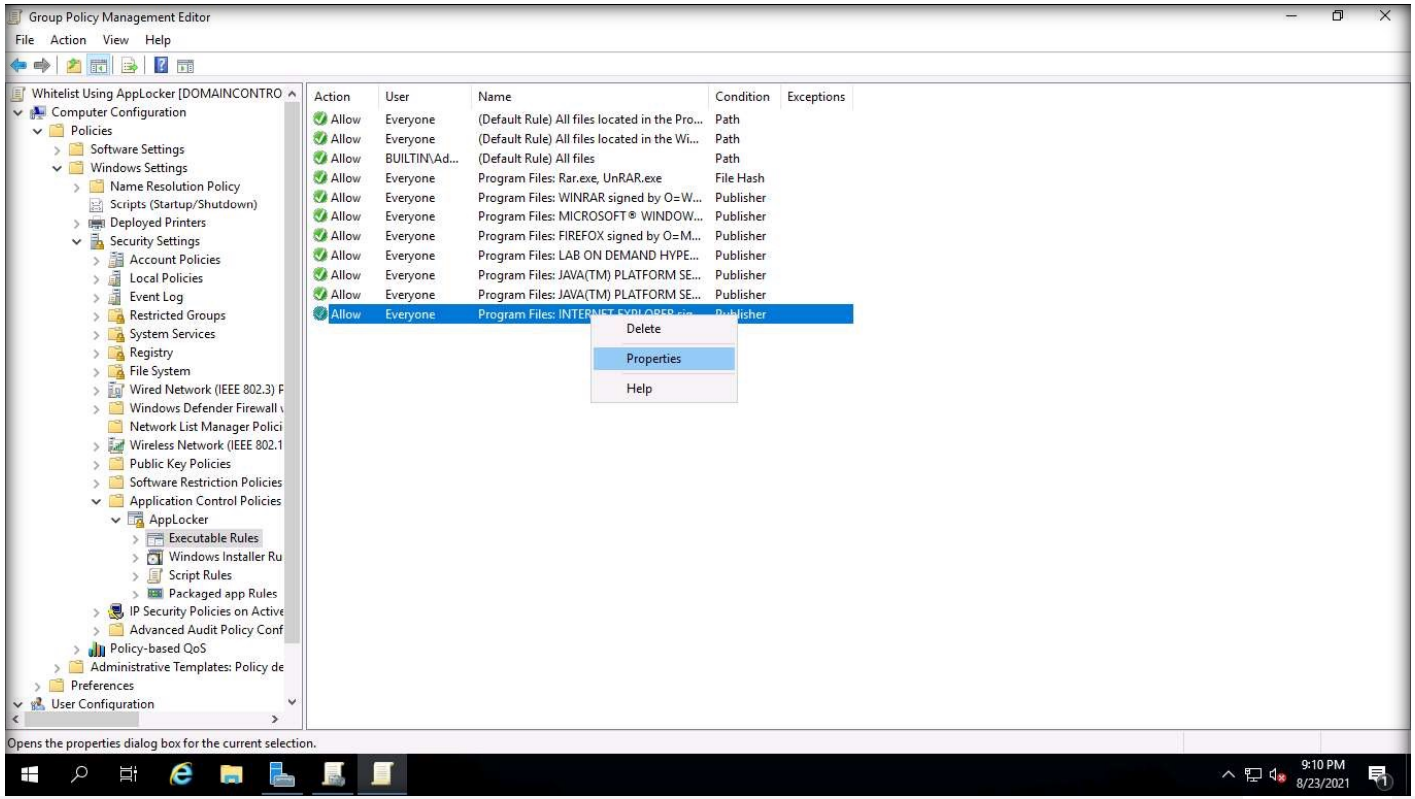
24. In the above list, the automatically generated rule for Internet Explorer is whitelisted. However, our intent is to deny user's access to Internet Explorer. The below steps demonstrate how to deny access to Internet Explorer using AppLocker.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



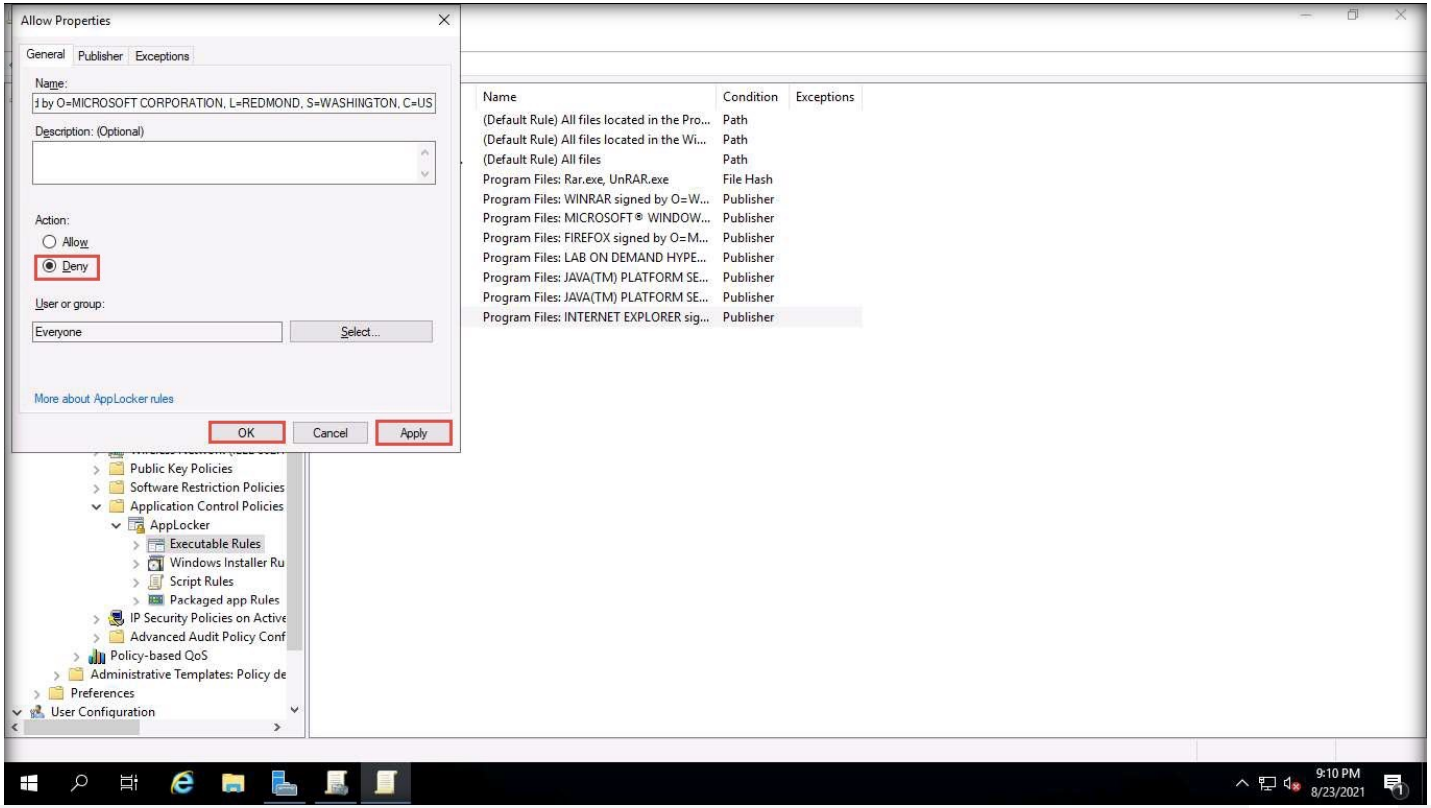
25. Right-click on the last rule from the list named Program Files: INTERNET EXPLORER and click on Properties.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



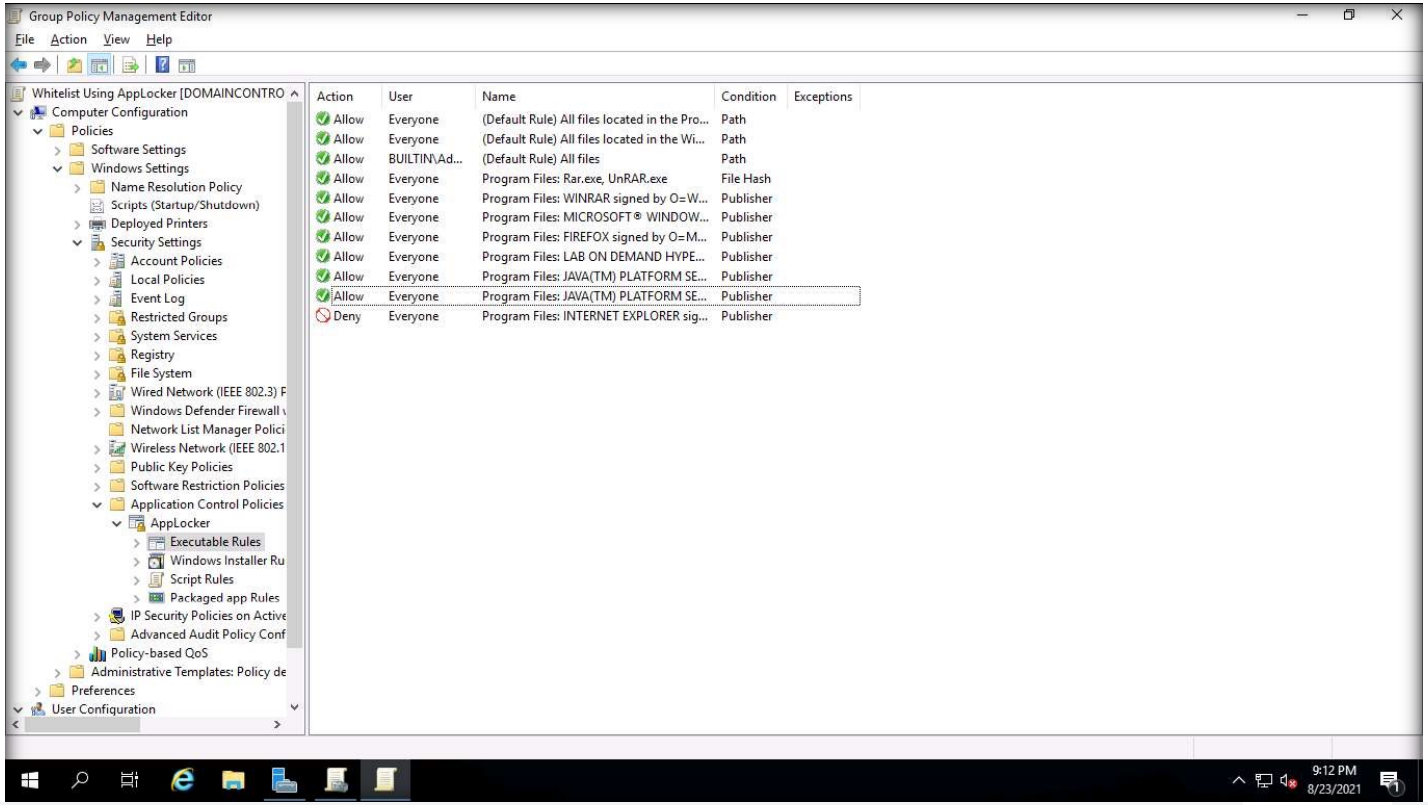
26. The Allow Properties window opens, check the Deny radio button, and click on Apply and OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



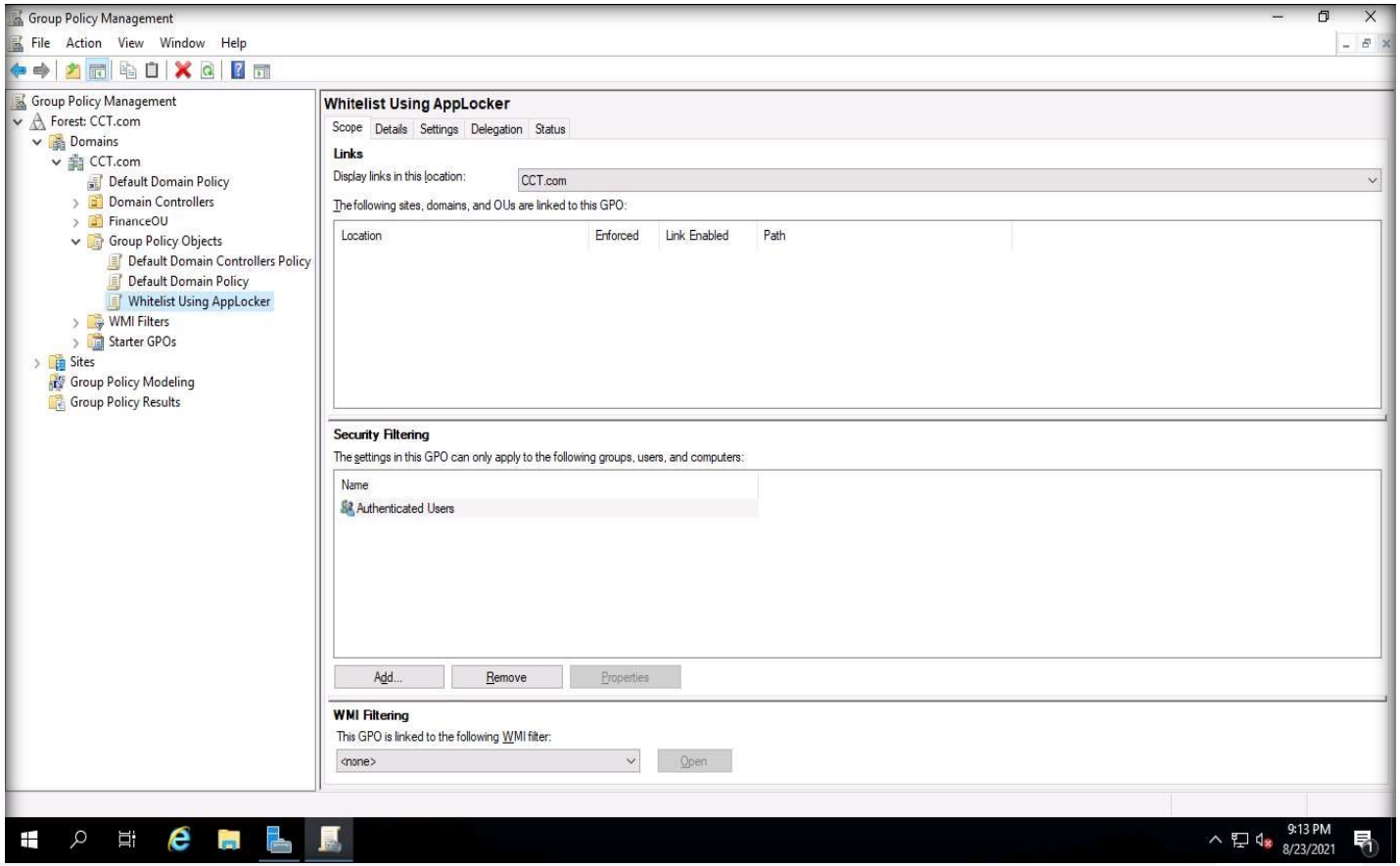
27. You will be able to see the Action of the last rule ID: Deny.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



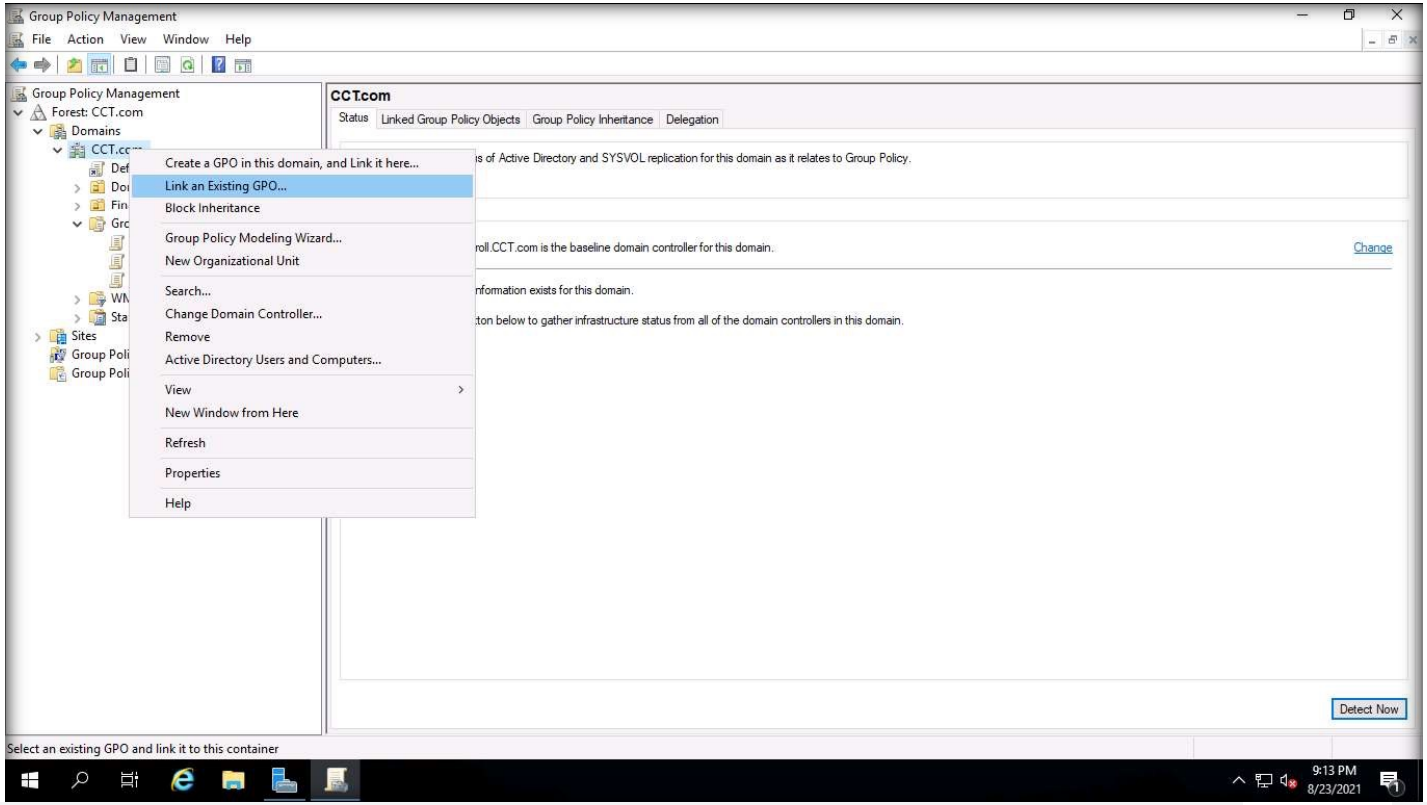
28. Close the Group Policy Management Editor to return to the Group Policy Management window.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



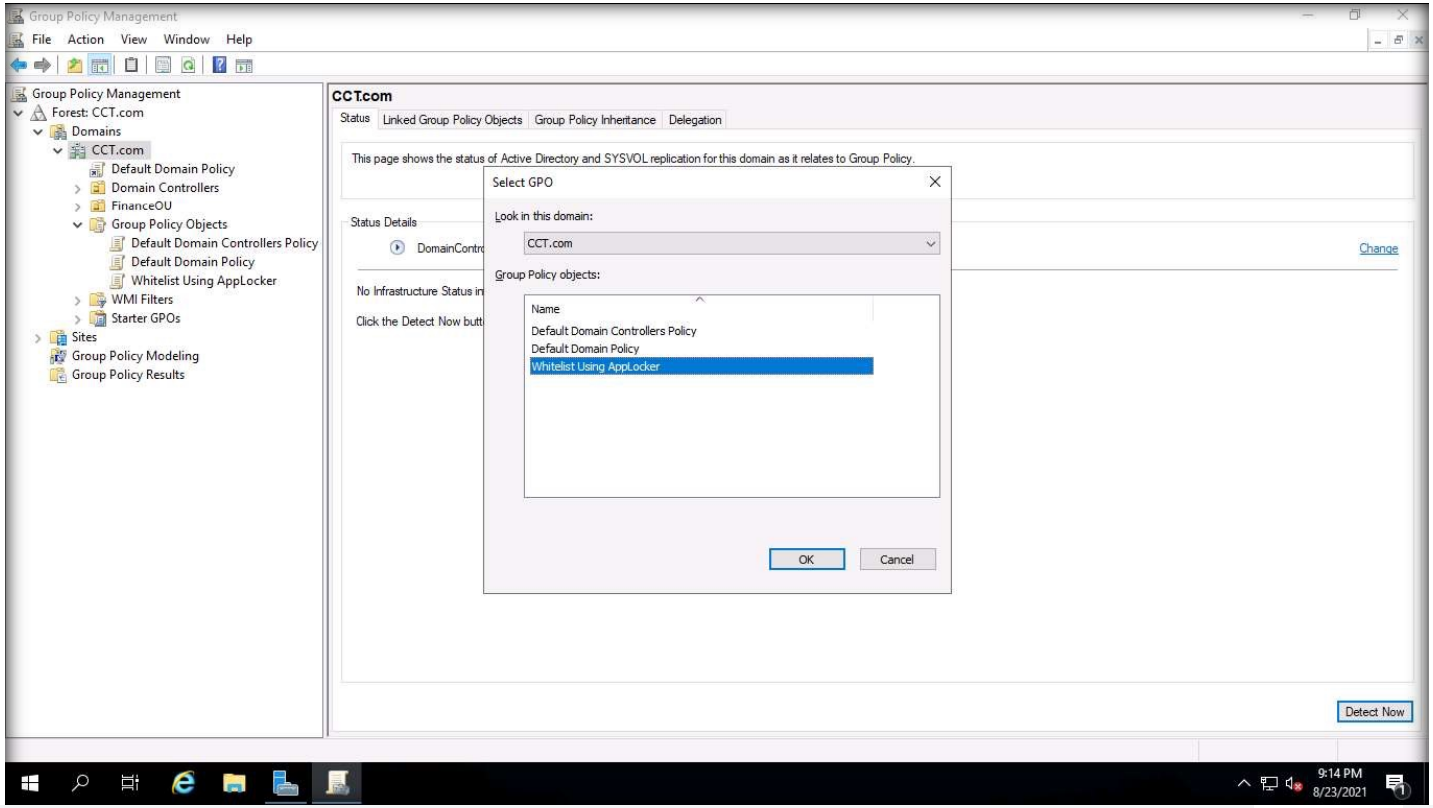
29. Right-click on cct.com under Domains and select the Link an Existing GPO... option.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



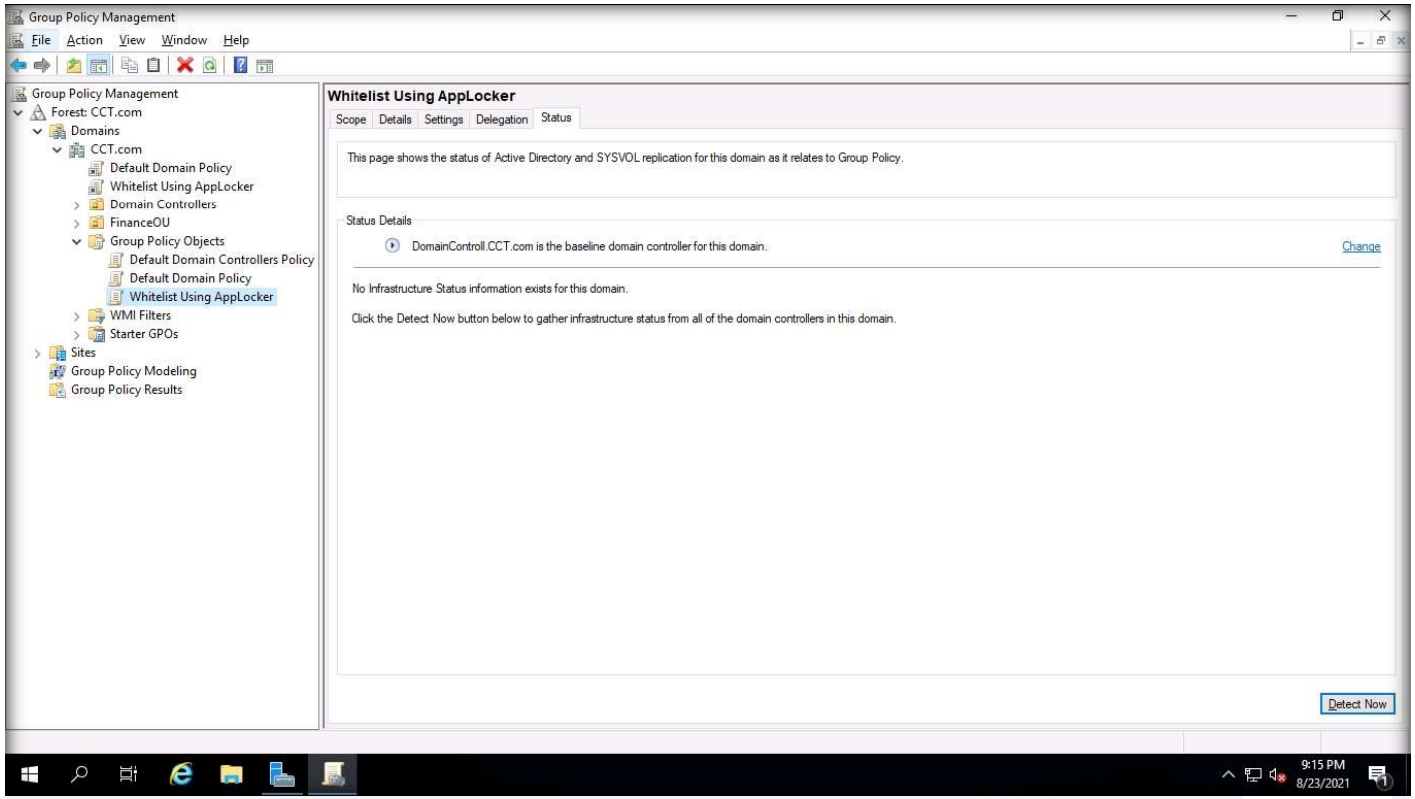
30. The Select GPO window opens, select Whitelist Using AppLocker under Group Policy Objects and click on OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



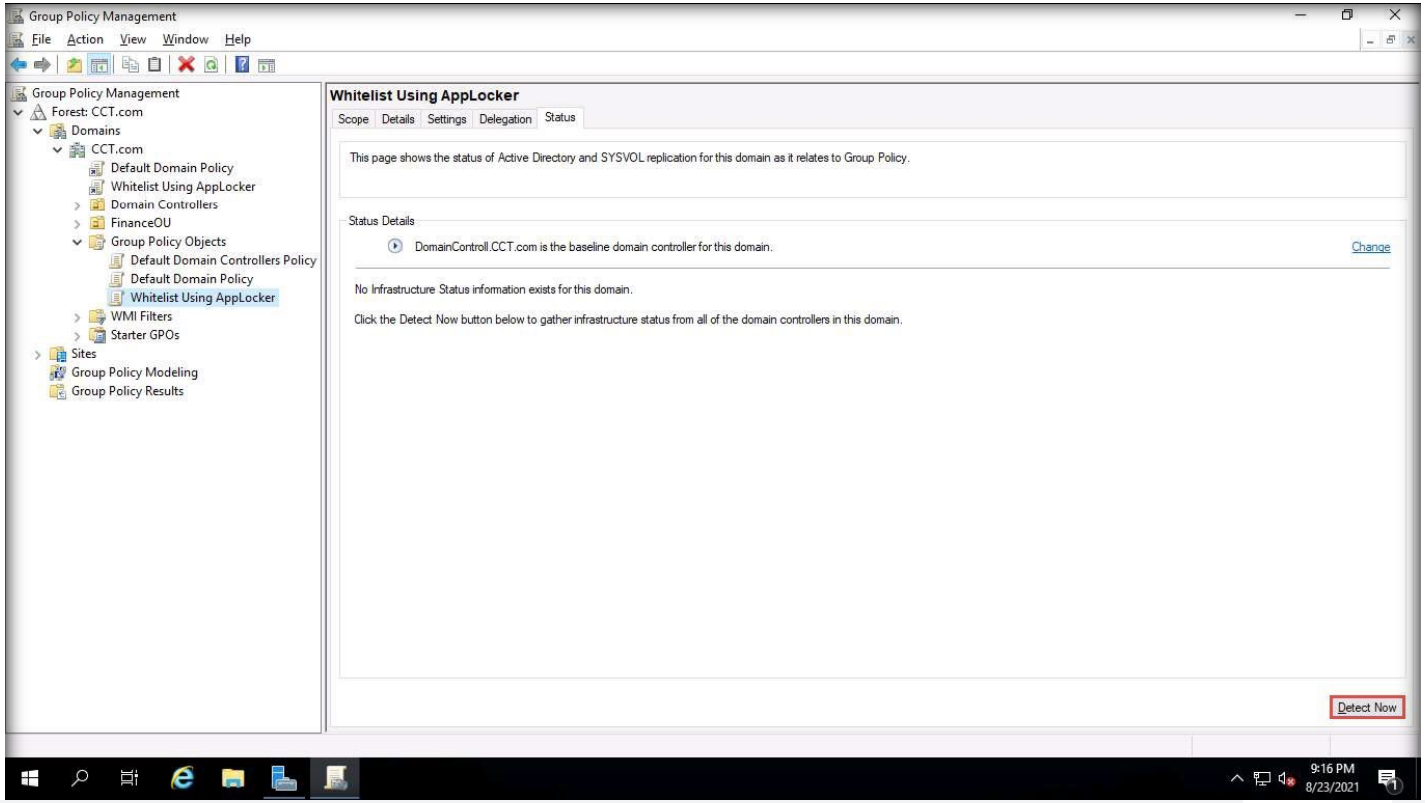
31. Navigate to Group Policy Objects, click on Whitelist Using AppLocker and then click on the Status tab.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



32. Click on Detect Now in the bottom right corner.

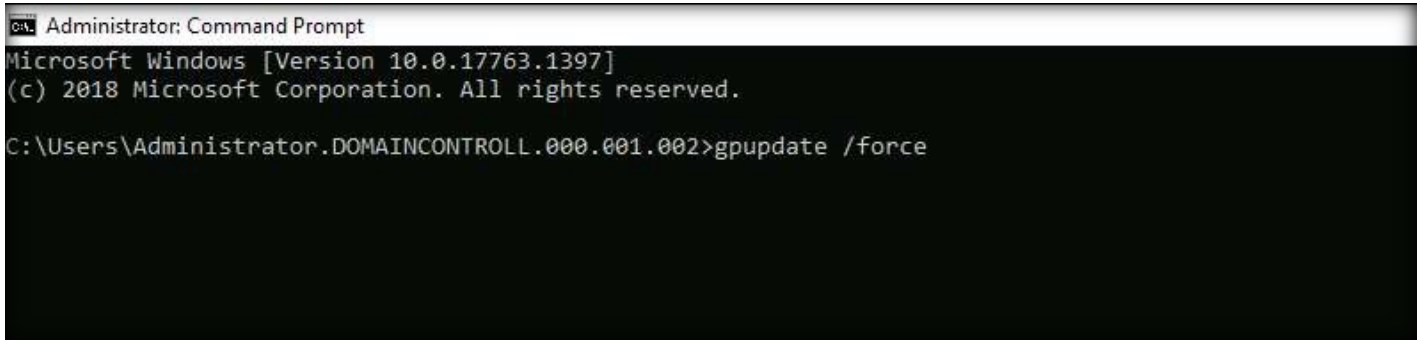
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



33. Close the Group Policy Management window. After a few seconds, the group policy will update.

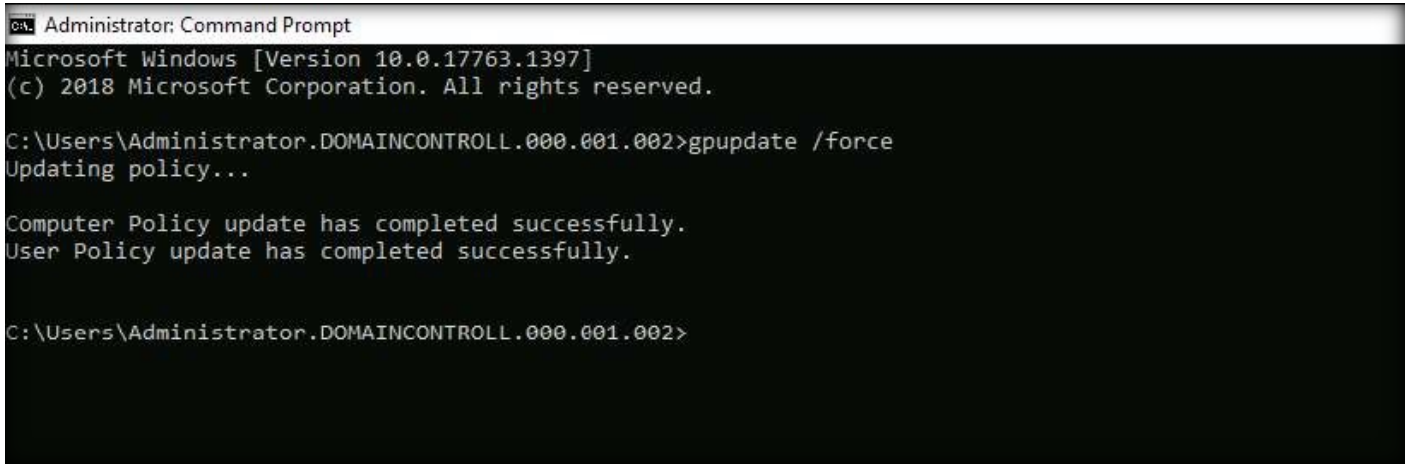
34. Open the command prompt, type gpupdate /force and press Enter to update the policy.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



35. Wait for a few seconds to update the group policy. Close the Command Prompt window.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

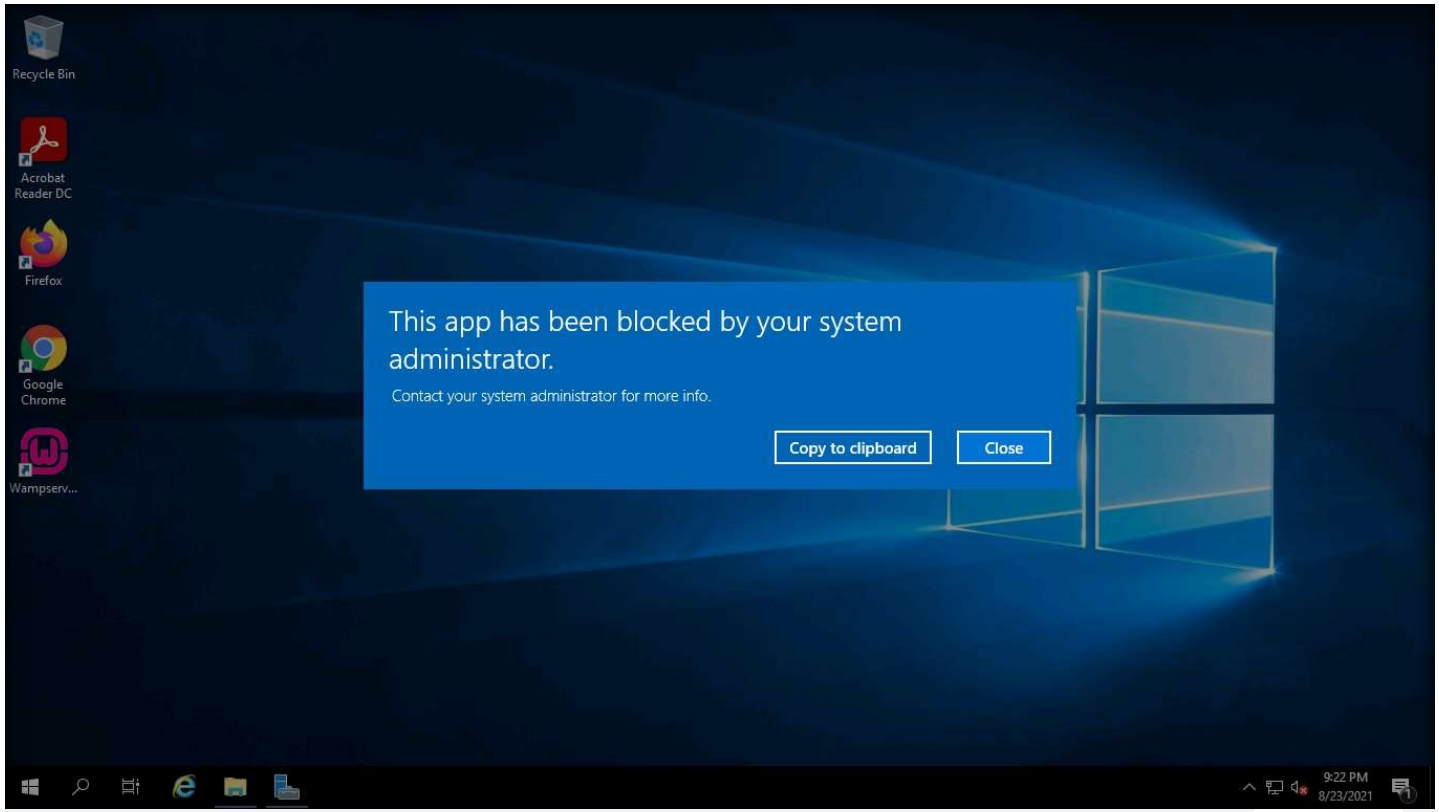


36. Next, try to open Internet Explorer.

37. You will receive the message that “This app has been blocked by your system administrator.” Click on Close.

Note: If you do not receive the above message, then restart the AD Domain Controller machine and repeat Step#36.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

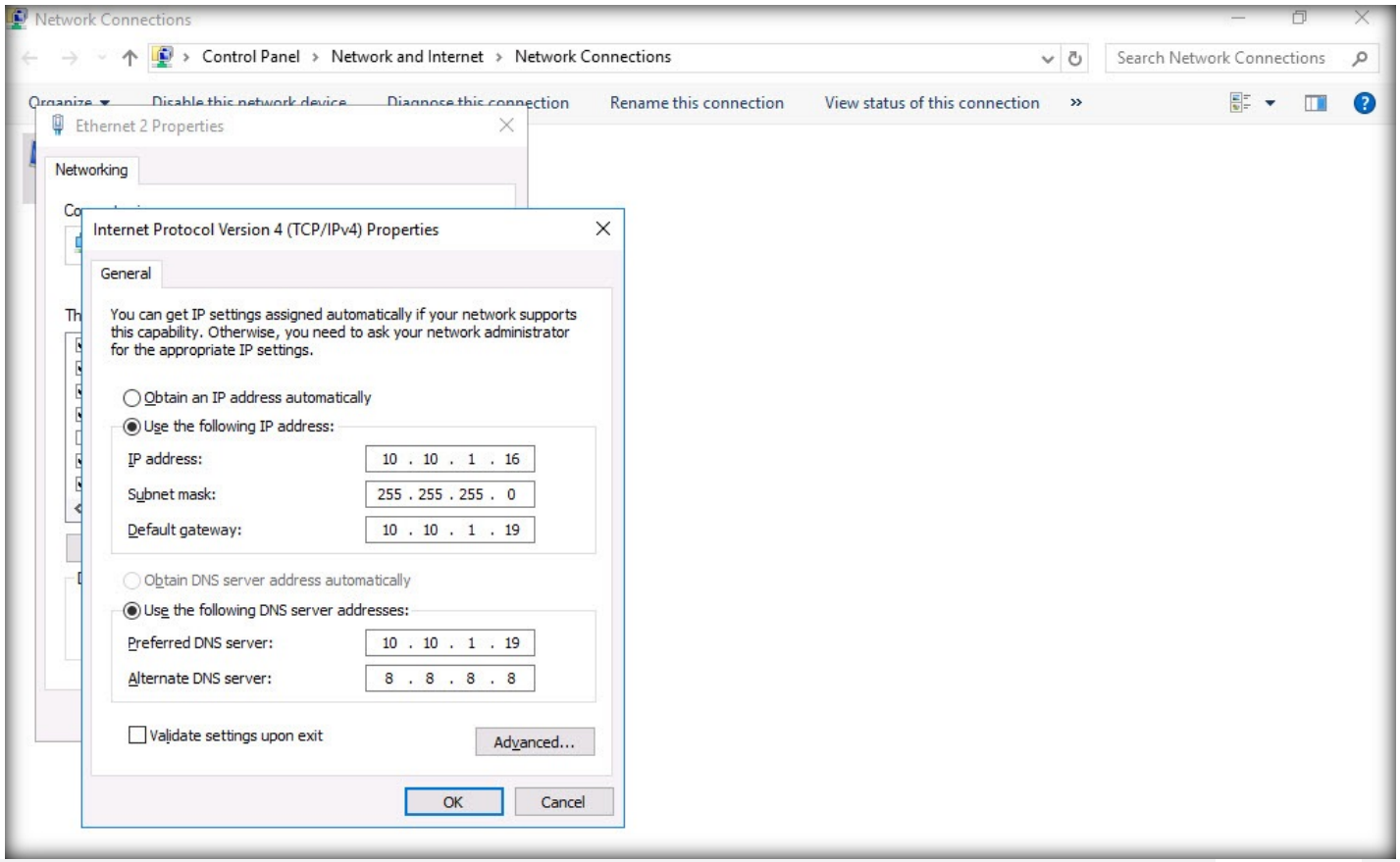


38. Switch to the Web Server virtual machine.

39. Log in with the credentials Administrator and admin@123.

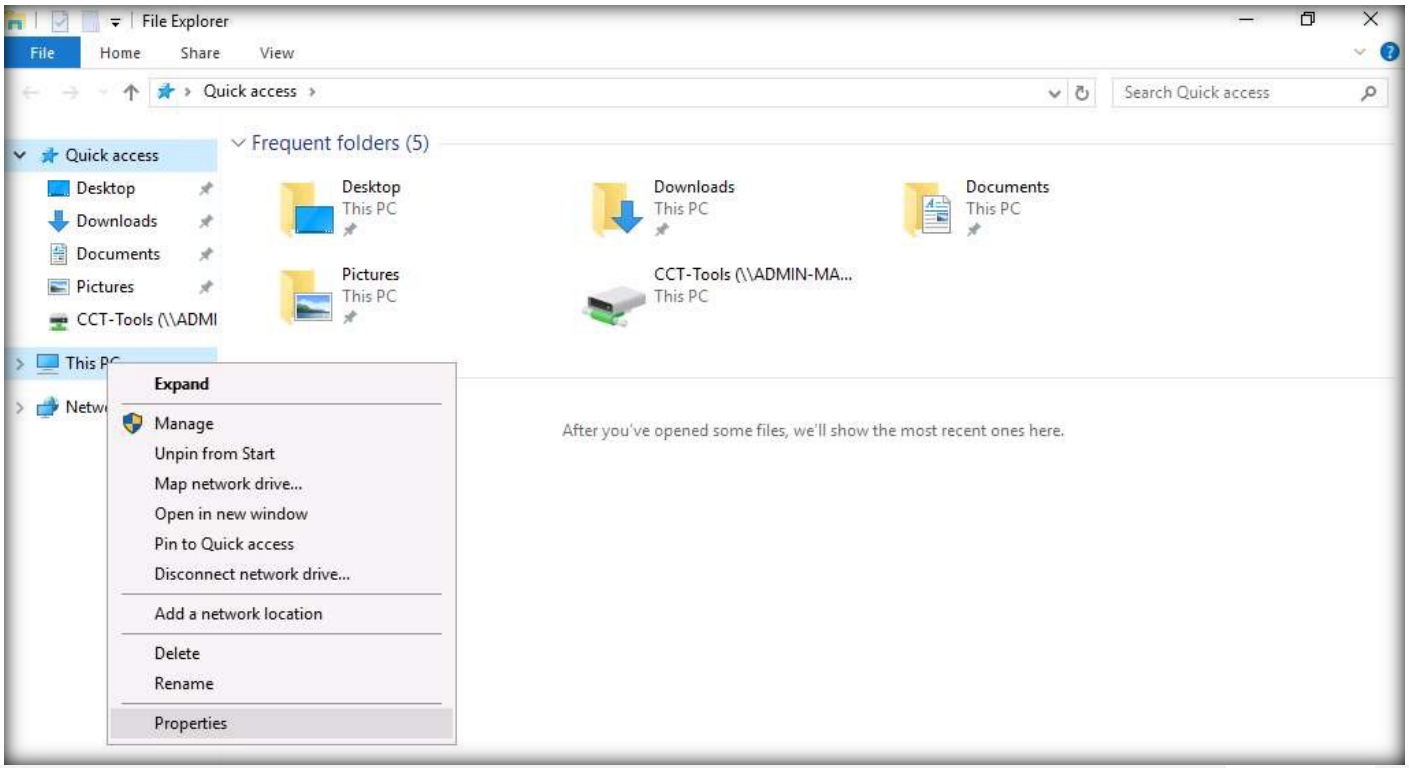
40. Open a Control Panel window and navigate to Network and Internet → Network and Sharing Center → Change adapter settings. In the Network Connections window, right-click the ethernet adapter (here, Ethernet 2) and select Properties from the drop-down options. Double-click Internet Protocol Version 4 (TCP/IPv4) and change the Default gateway address to 10.10.1.19. Click OK twice. Close the window.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



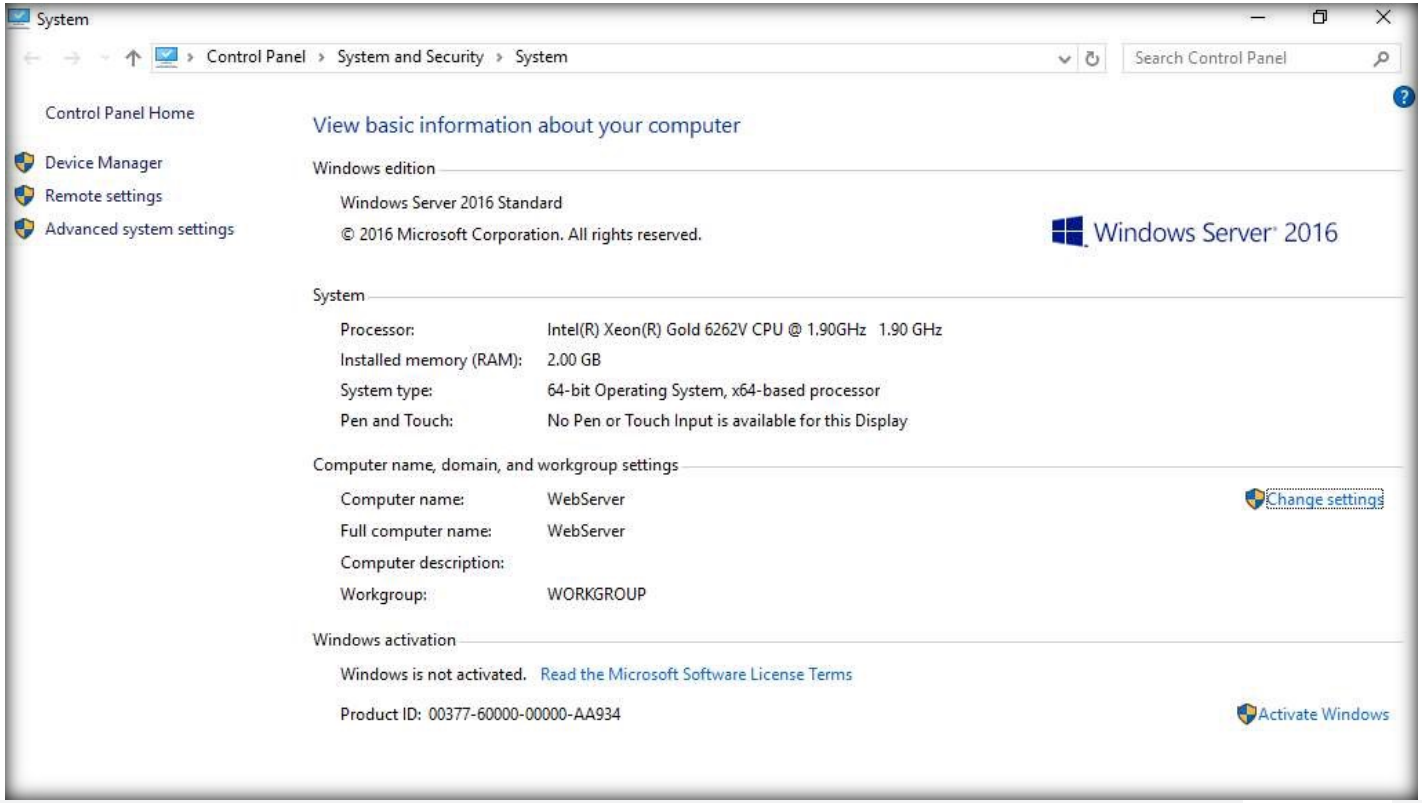
41. Open File Explorer and right-click on This PC, select Properties.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



42. The System window opens, click Change Settings.

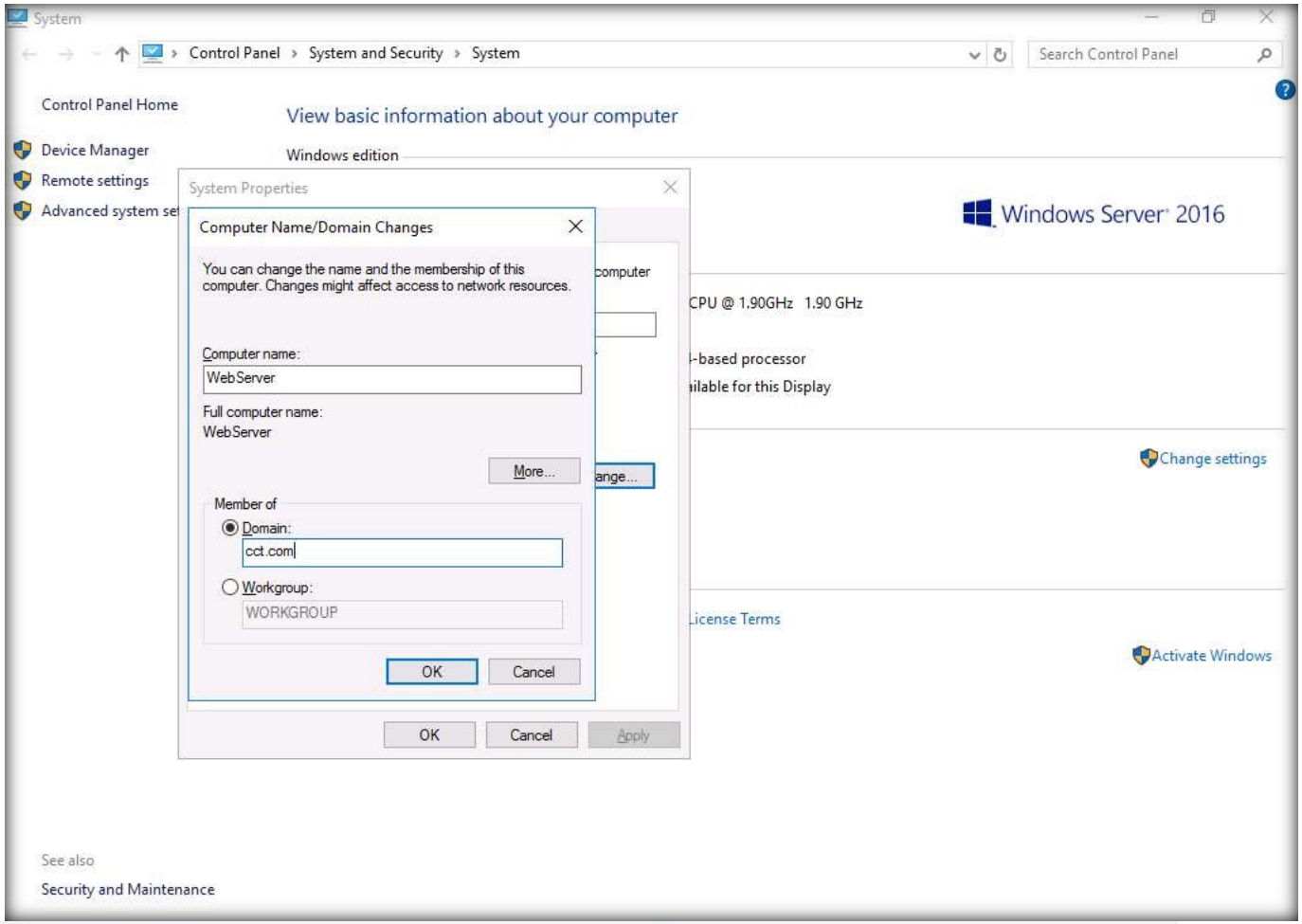
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



43. The System Properties Window opens, click Change....

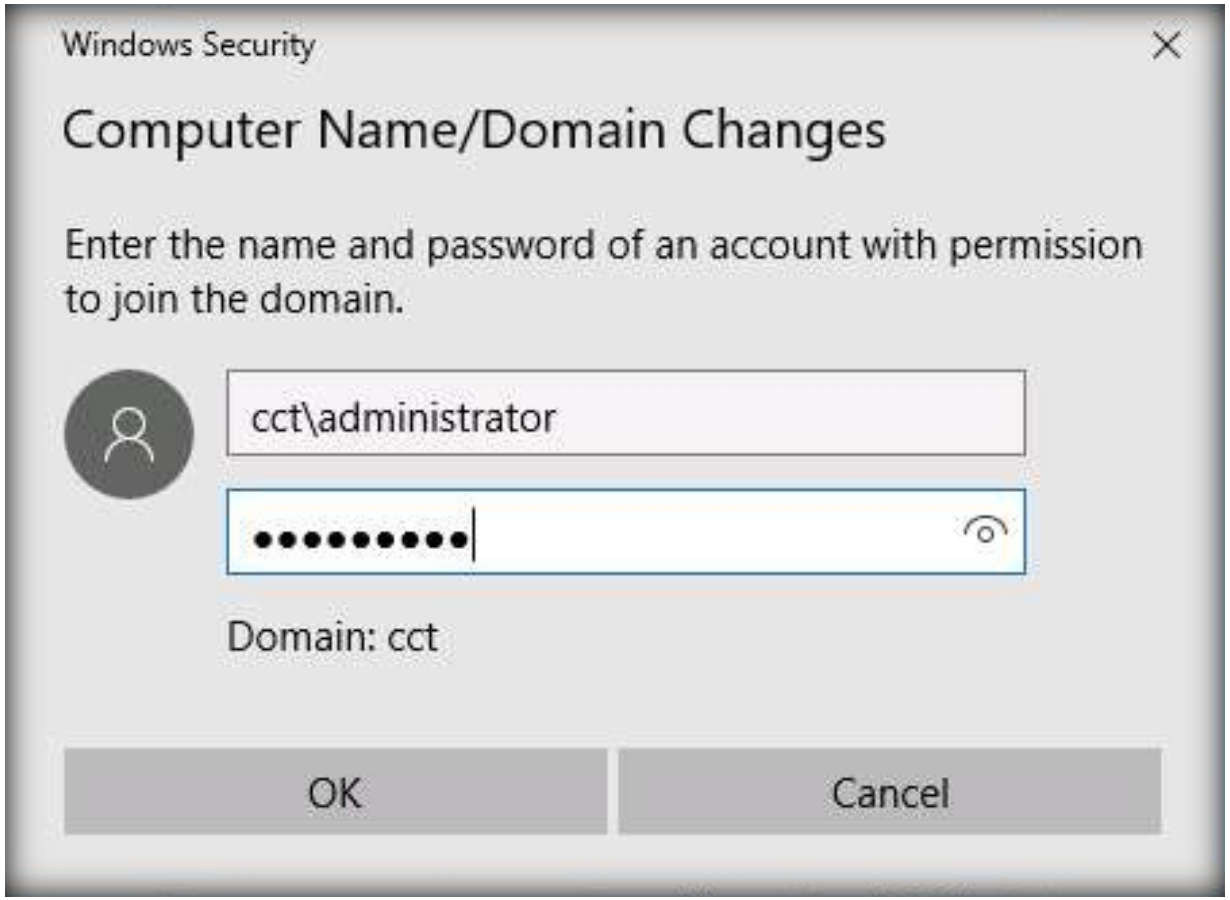
44. The Computer Name/Domain Changes sub-window opens, select the Domain radio button, and type cct.com under the empty text box. Click OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



45. The Window Security credential window opens, type username as cct\administrator and type password as admin@123 and click OK

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

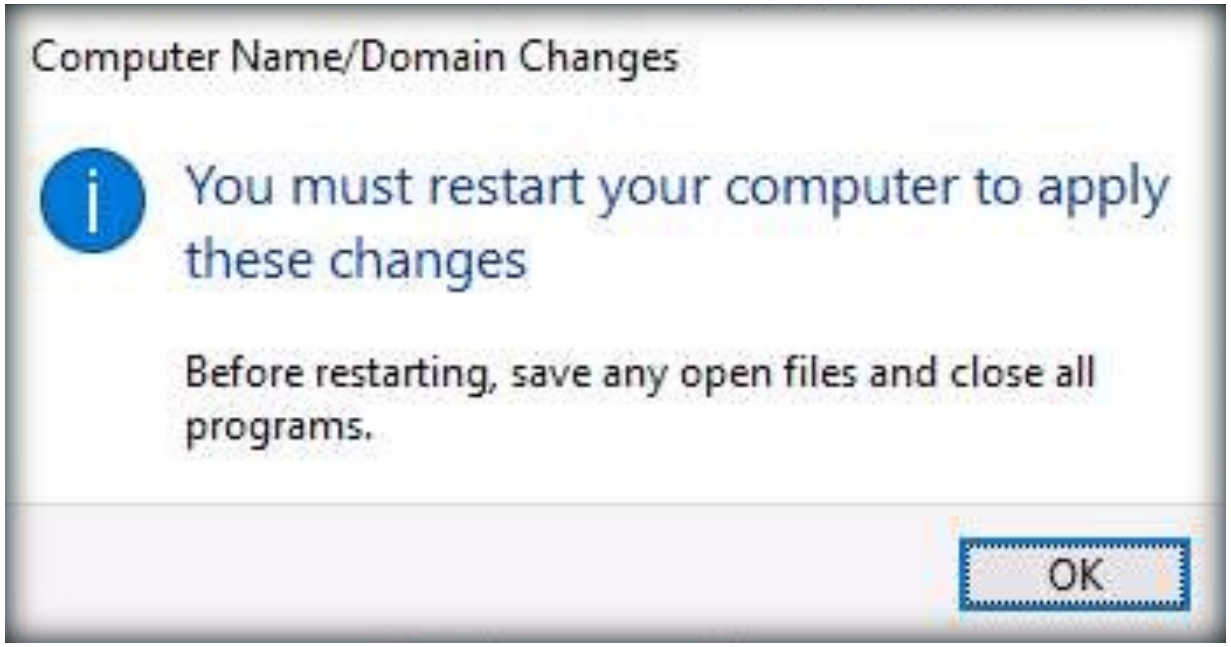


46. Wait for few seconds, the welcome to cct.com popup appears, click OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

47. The restarting confirmation popup appears, Click OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



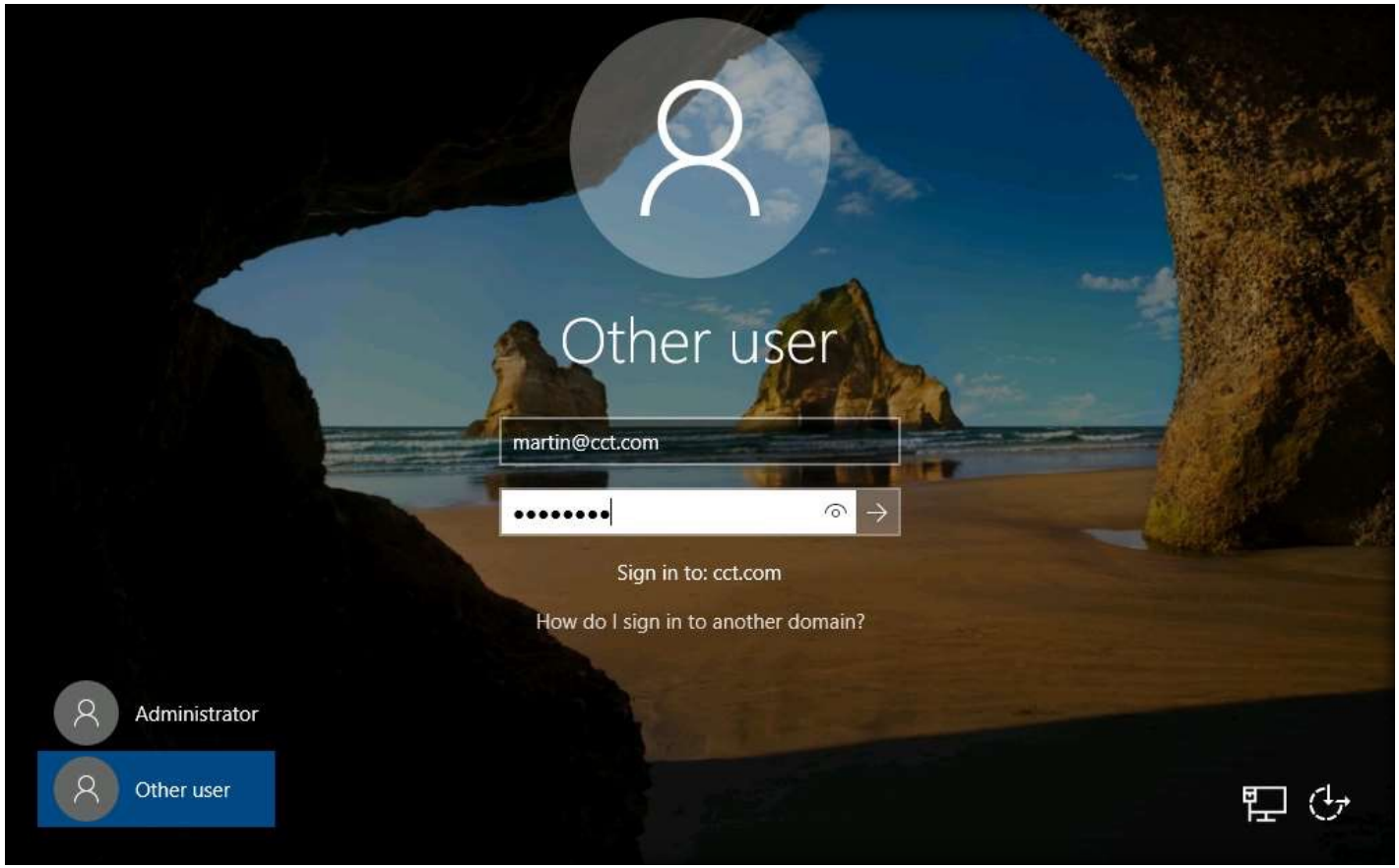
48. You will get back to the System Properties window. Click Close.

49. The Microsoft windows message box opens, click Restart Now button to restart the system.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

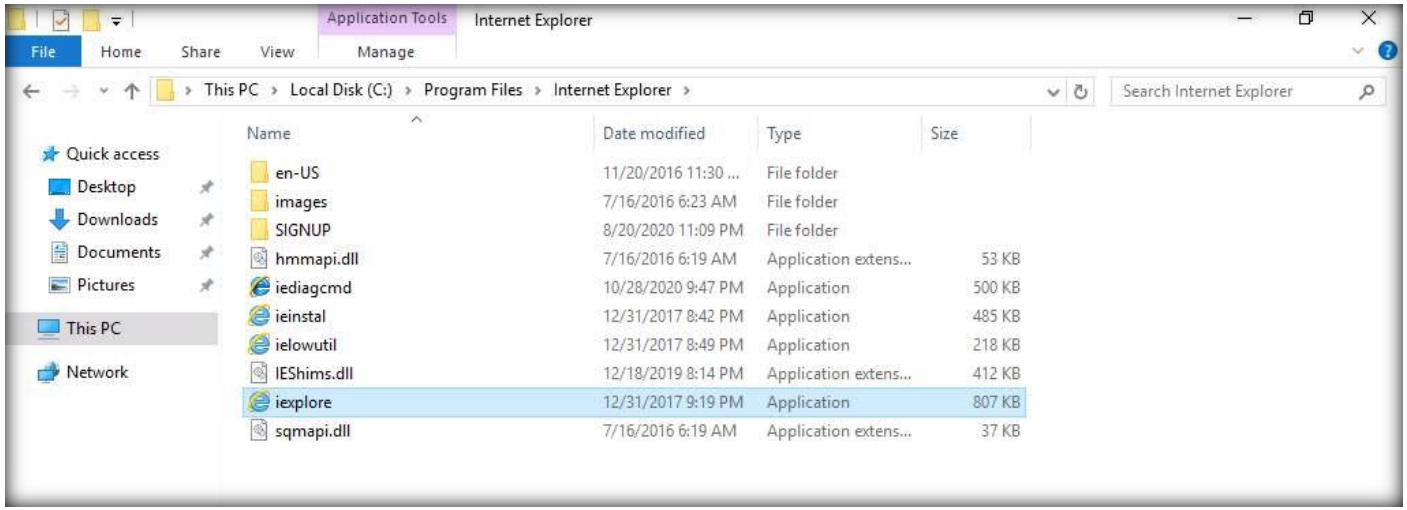
50. The system will restart. Choose Other user username as martin@cct.com and type password as user@123 and press Enter.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



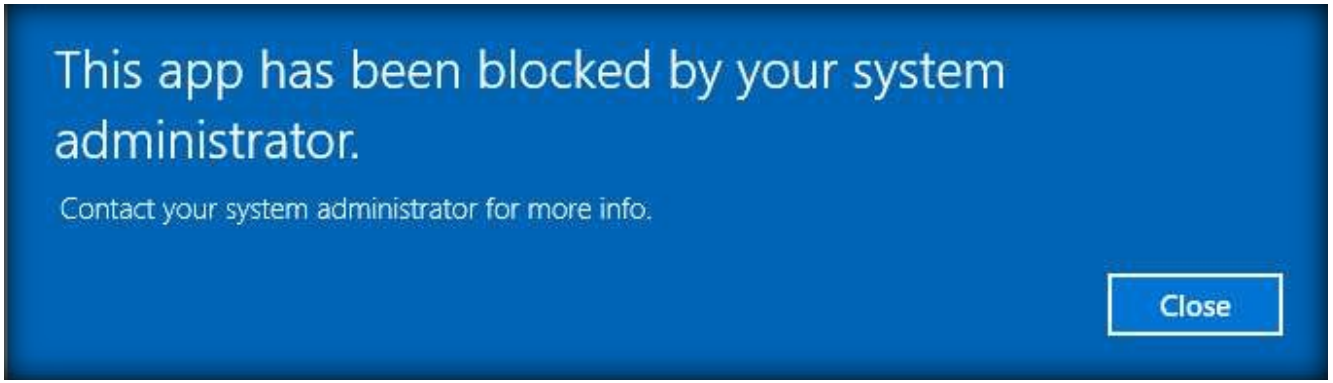
51. Navigate to C:\Program Files\Internet Explorer and try to execute iexplorer.exe.

EXERCISE 1:
IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



52. As soon as you double-click on iexplorer.exe file, you will receive an error message stating that the administrator has blocked the program.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

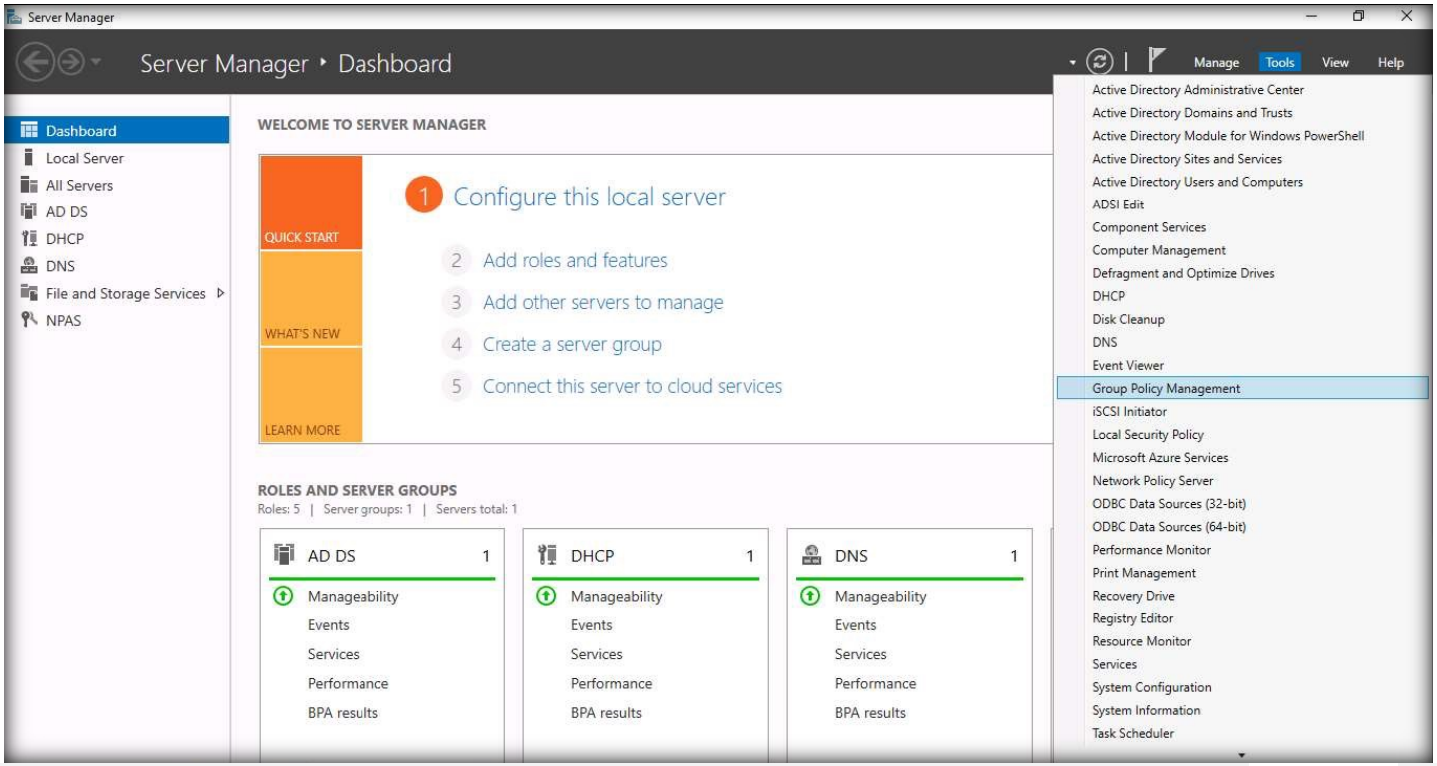


53. Click Close. Close the open window.
54. By implementing the aforementioned steps, security professionals can implement policies as per organizational requirements. You can apply whitelisting here. In this lab, we have demonstrated only one policy, which can be applied by every user to deny access to necessary resources
Note: Since administrative rights are required to proceed to the next exercise, we will unlink the created Whitelist Using AppLocker policy.
55. Switch to the AD Domain Controller virtual machine.
56. Log in with the credentials CCT\Administrator and admin@123.
57. Click on Windows Start icon, select Server Manager.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER

58. The Server manager window will open, navigate to the Tools menu, and select Group Policy Management.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



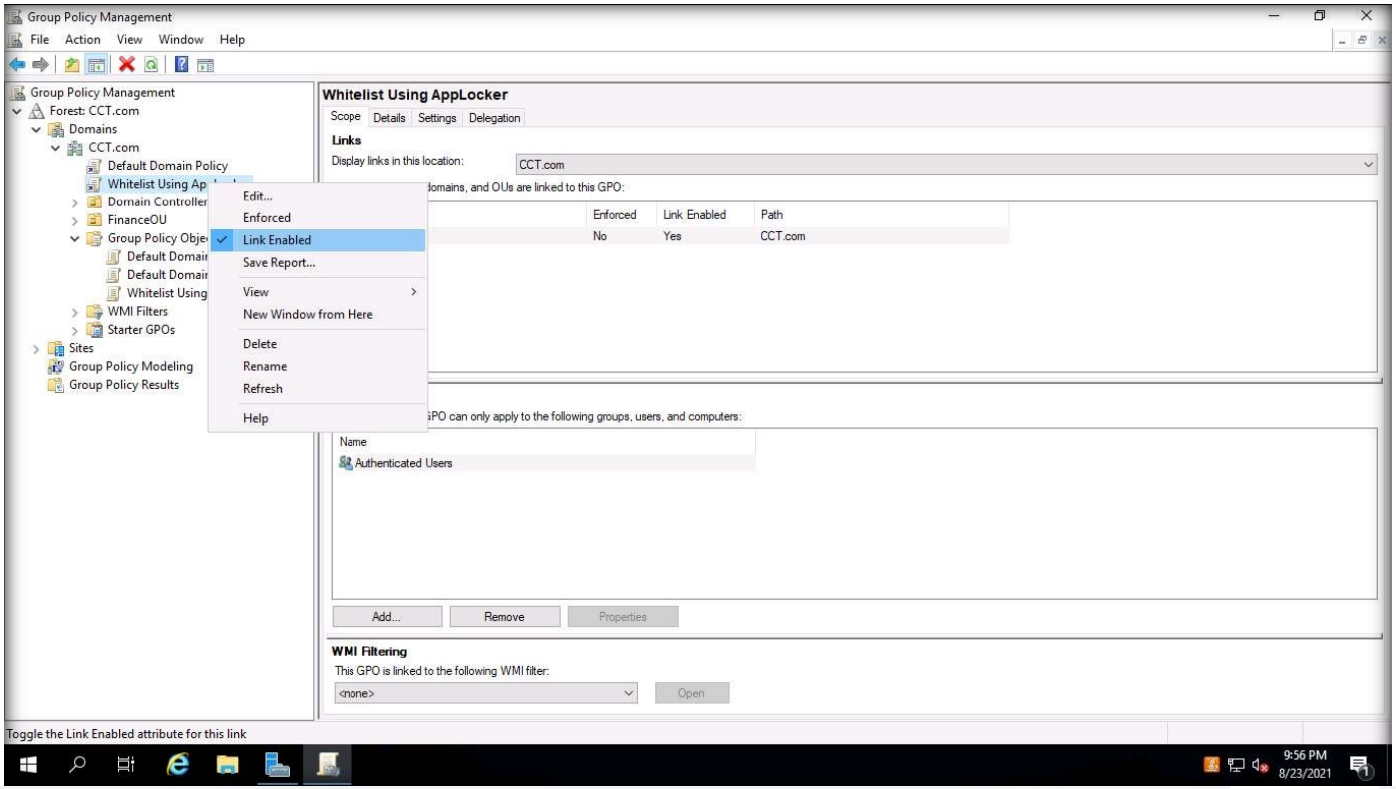
59. The Group Policy Management console opens, expand the cct.com domain, right-click on Whitelist Using AppLocker policy, and click on the Link Enabled option to disable the link.

60. This concludes the demonstration of showing how to implement application whitelisting using AppLocker.

61. Close all open windows.

62. Turn off AD Domain Controller and Web Server virtual machines.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLOCKER



EXERCISE 2: **BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL**

Application blacklisting is a security practice of blocking the running and execution of a list of undesirable programs.

LAB SCENARIO

Most antivirus programs, spam filters and other intrusion prevention or detection systems use the application blacklisting method. A blacklist often comprises malware, users, IP addresses, applications, email addresses, domains, etc. Knowledge of the threats associated with programs or applications is required to prepare an application blacklist

Security professionals must have proper knowledge regarding blocking executable files in the network or local system in order to maintain system security.

OBJECTIVE

The objective of this lab is to deploy application blacklisting using ManageEngine Desktop Central.

OVERVIEW OF APPLICATION BLACKLIST

Application blacklisting is threat centric. By default, it allows all applications that are not in the blacklist to be executed. To block any program or application, the security professional must add it in the application blacklist. There are many tools used in blacklisting applications, in this task, we will use ManageEngine Desktop Central to demonstrate application blacklisting.

ManageEngine Desktop Central prevents blacklisted applications based on the organization's policies. It helps in restricting the usage of blacklisted applications as well as portable executables, which can be accessed without installation. The Block Executable and Prohibit Software features of ManageEngine Desktop Central can be used for Application Blacklisting.

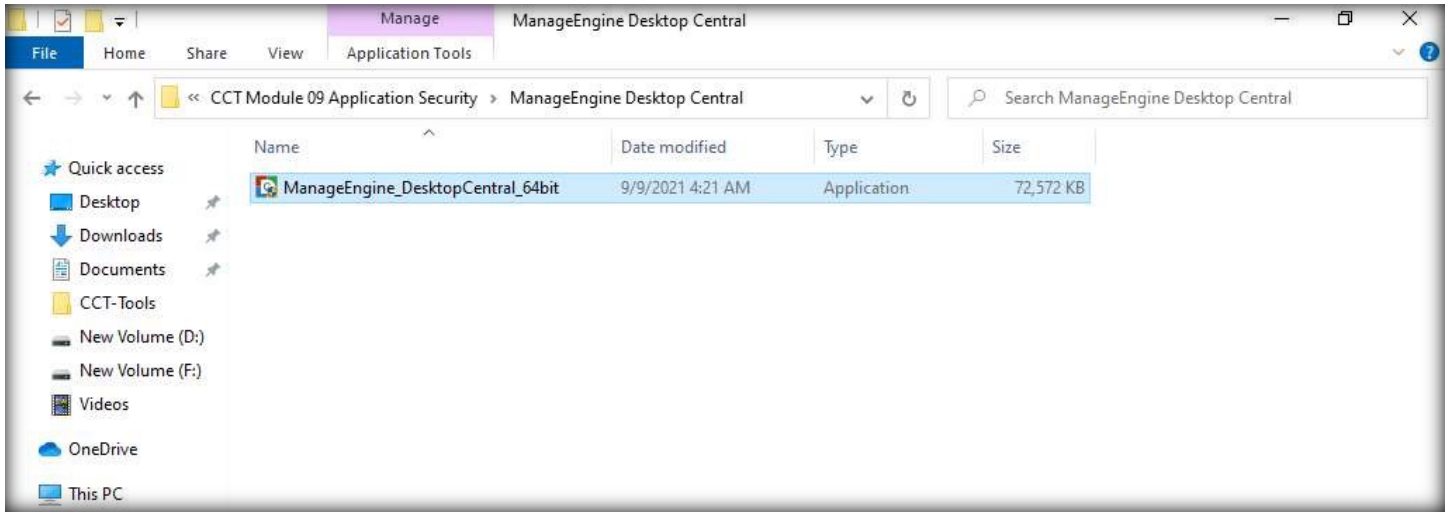
Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.
2. Log in with the credentials Admin and admin@123.

Note: If the network screen appears, click Yes.

3. Navigate to Z:\CCT-Tools\CCT Module 09 Application Security\ManageEngine Desktop Central.
4. Double-click ManageEngine_DesktopCentral_64bit.exe to start the installation.

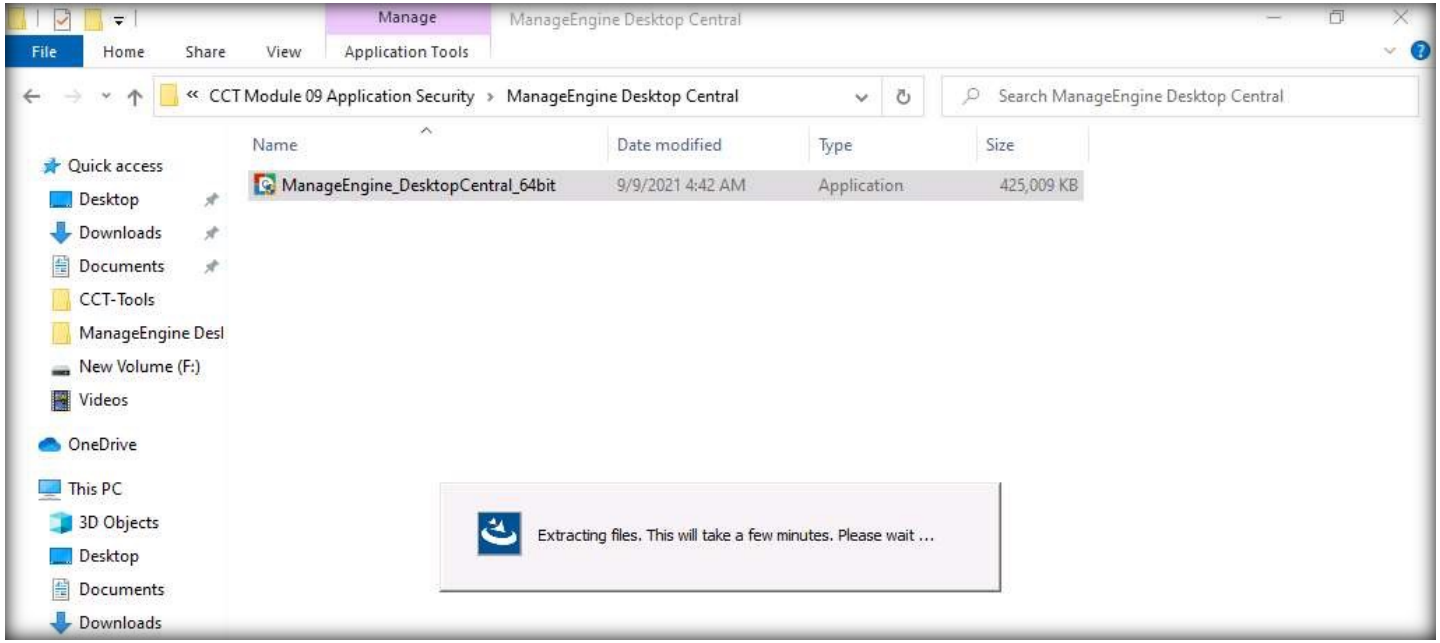
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



5. A User Account Control window appears, click Yes to continue.
6. ManageEngine Desktop Central Setup window appears, click Next to proceed with the installation process.
7. Follow the wizard driven installation to install the tool with default settings.
8. If an Antivirus Scanner pop-up appears, click OK.
9. In the Port Selection Panel wizard, leave the port number set to default (8020) and click Next.
10. Similarly, in the next wizard, click Next.
11. Extraction files pop-up appears and the tool starts to extract, wait for it to finish.

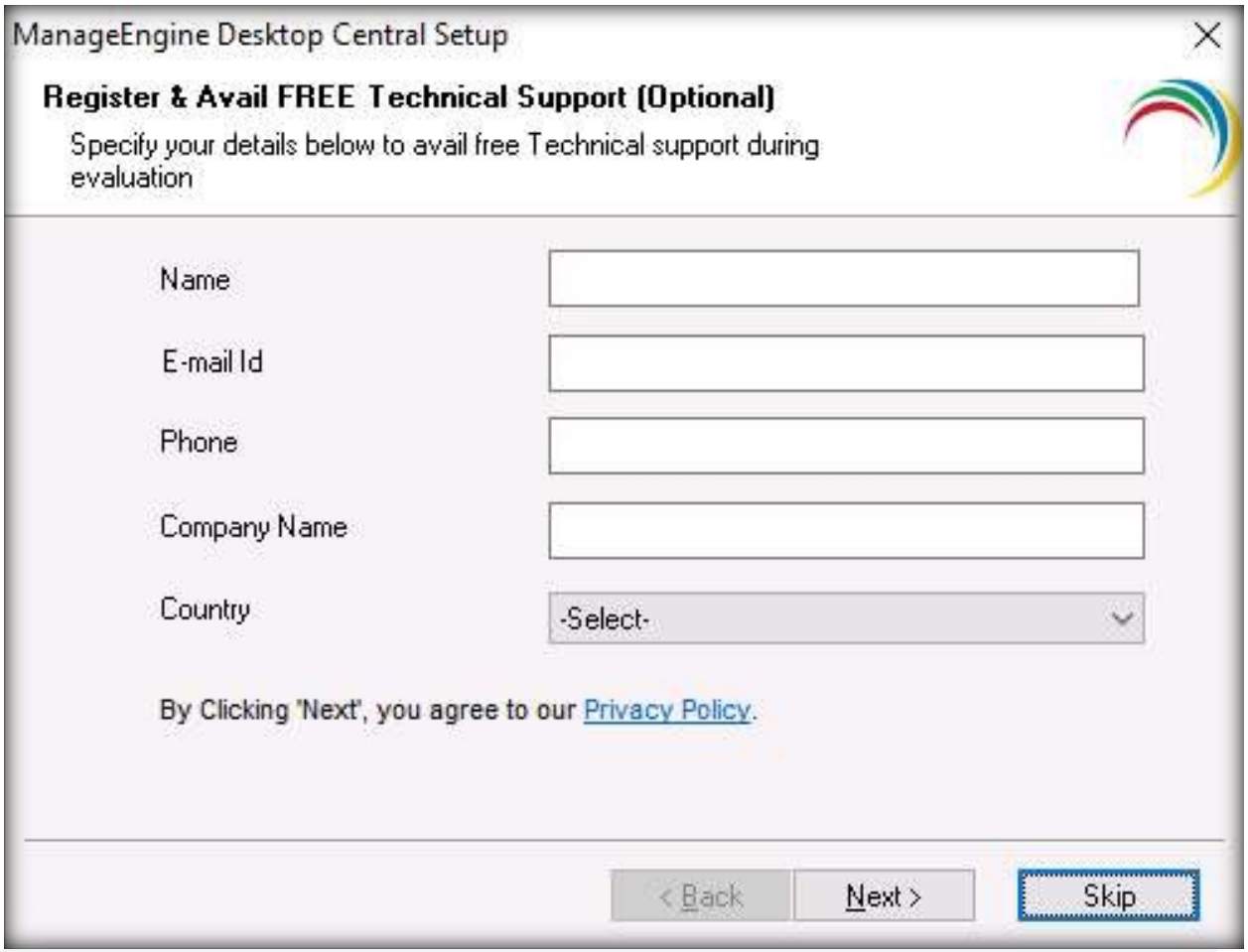
Note: The extraction and unpacking process takes approximately 5 minutes to complete.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



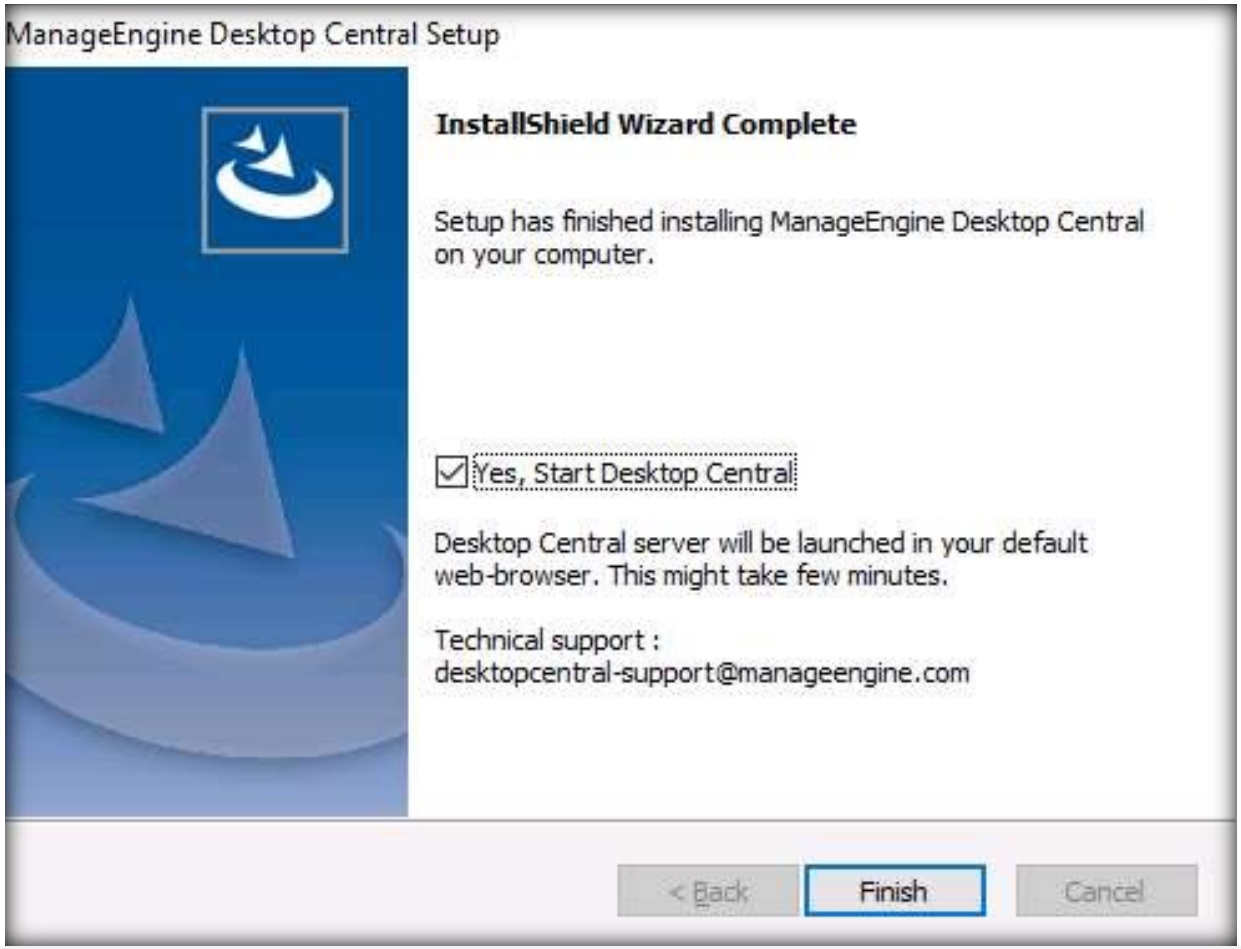
12. After the extraction and unpacking process, Register & Avail wizard appears. Click Skip.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



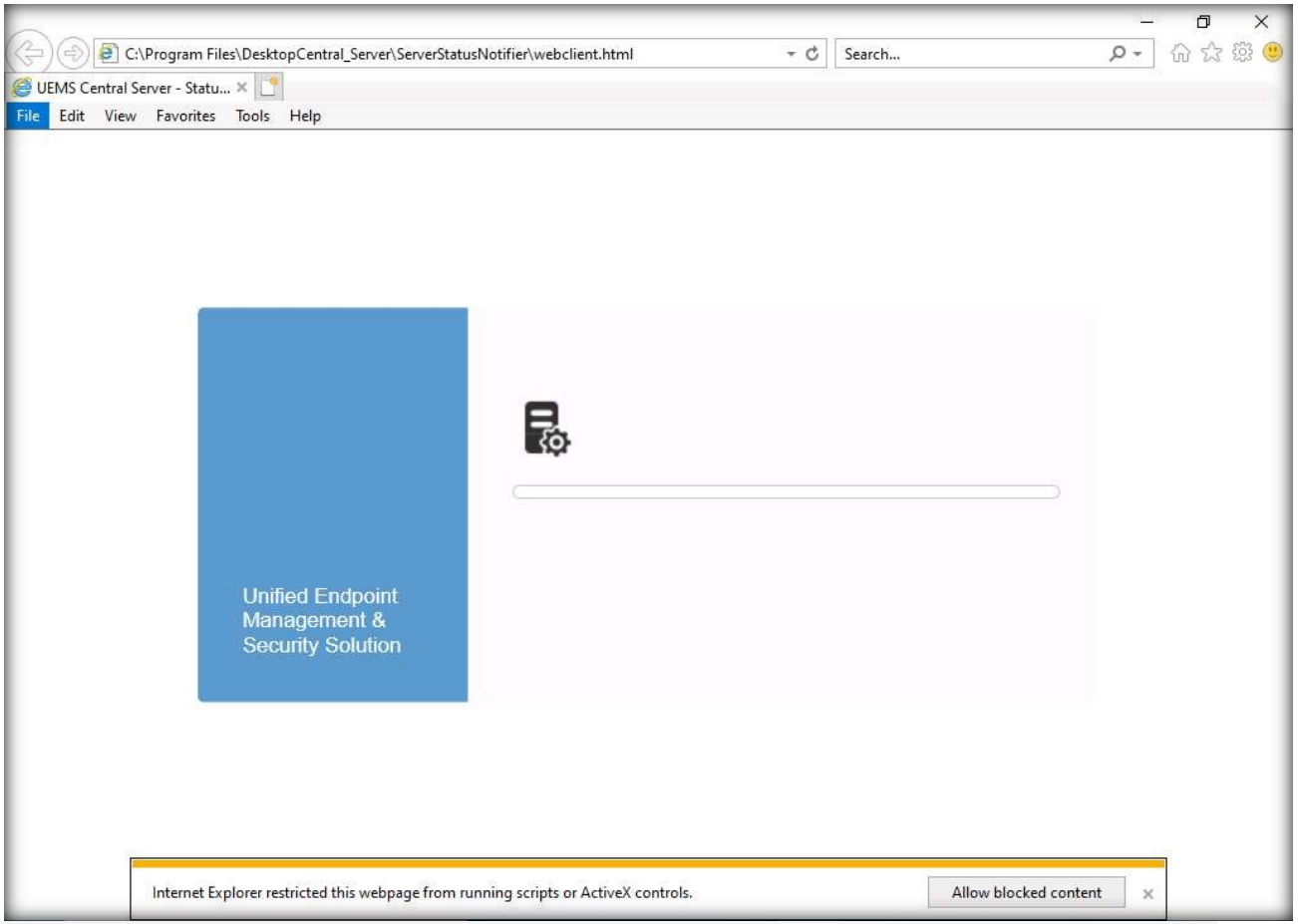
13. InstallShied Wizard Complete wizard appears, ensure that Yes, Start Desktop Central is checked and click Finish.

EXERCISE 2:
BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



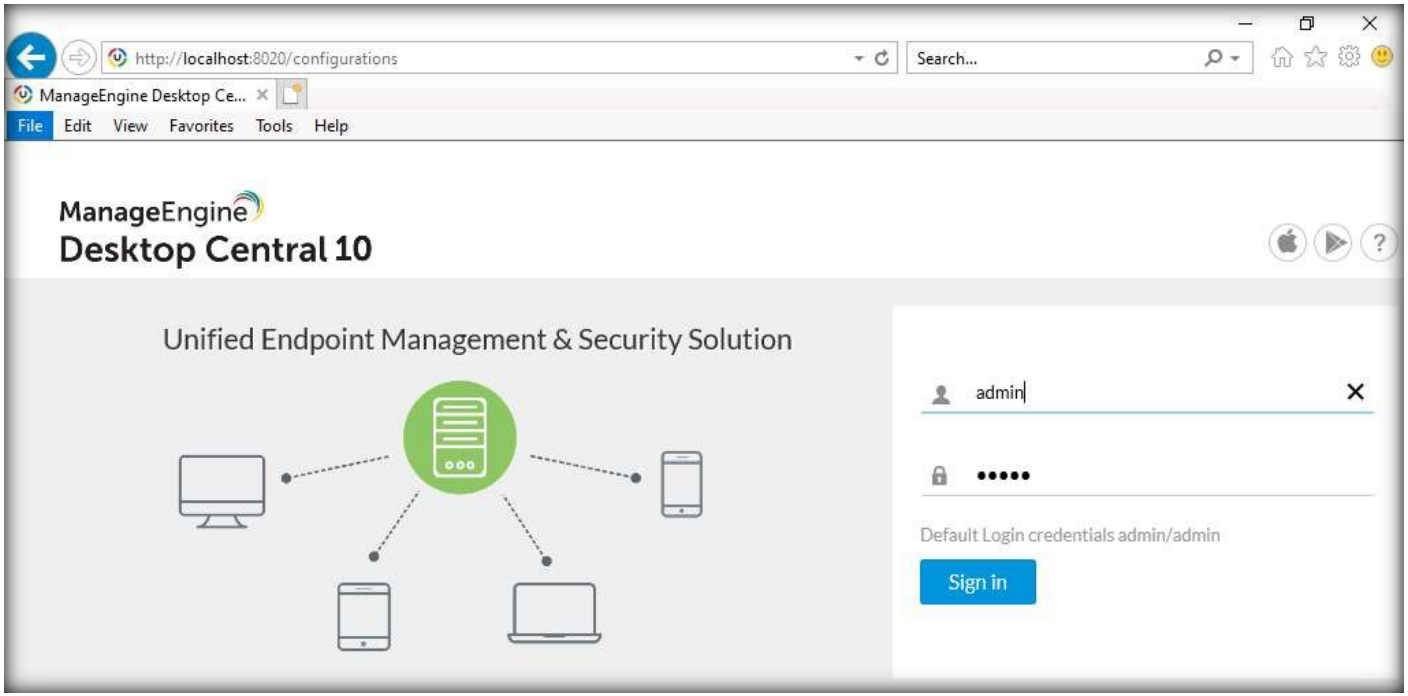
14. Microsoft Edge and Internet Explorer windows appear. Maximize Internet Explorer browser.
15. In the Internet Explorer 11 wizard, select Don't use recommended settings checkbox and click OK.
16. Close the tab with microsoft.com website loading on it.
17. In the first tab, UEMS Central Server website is open. Click Refresh icon ( ), present in the top-section of the window next to the URL field.
18. A notification appears in the lower section of the window, click Allow blocked content button.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



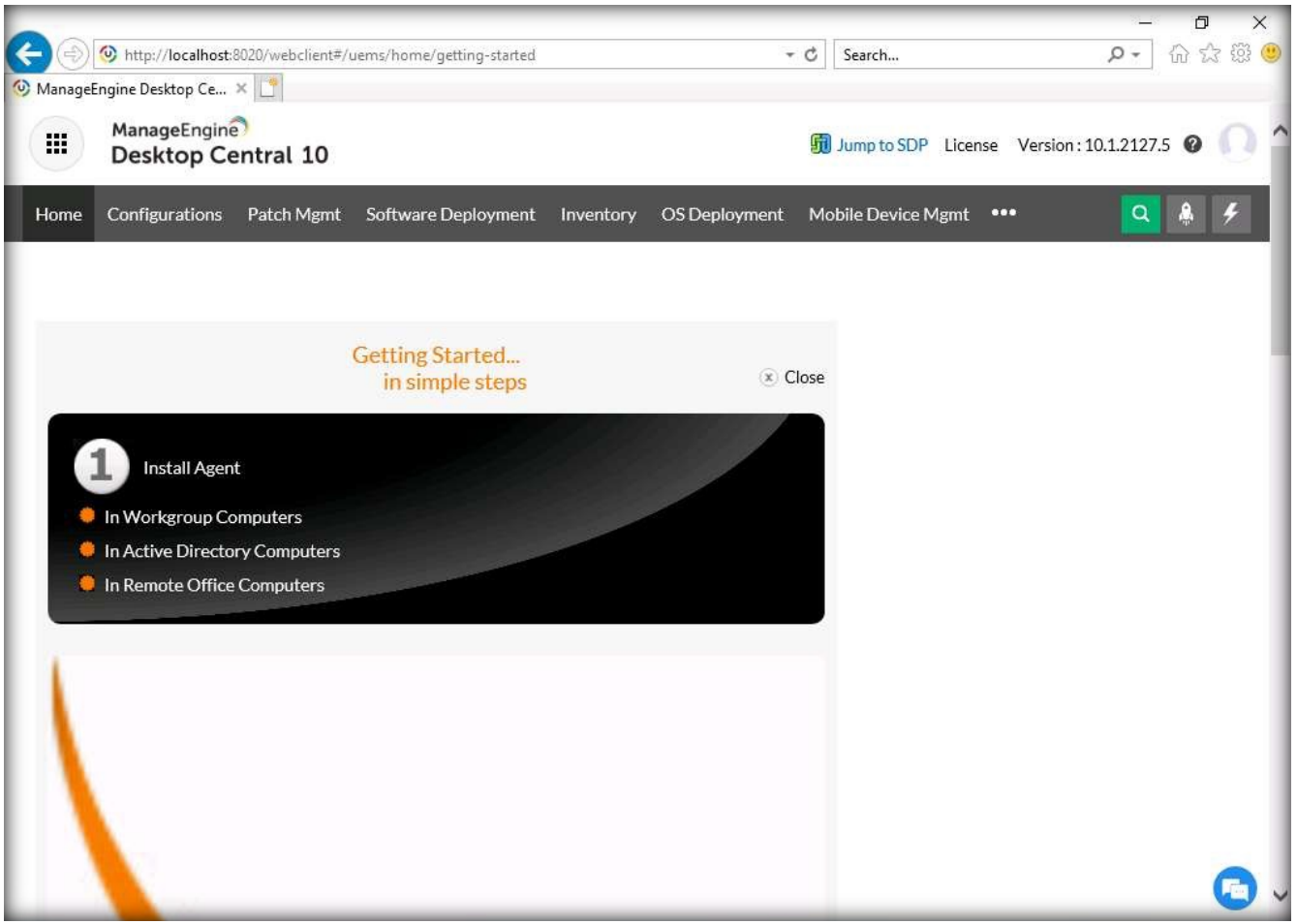
19. The main page of ManageEngine Desktop Central appears along with a login form. You can observe that, by default, credentials are entered. Click Sign in to proceed.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



20. ManageEngine Desktop Central dashboard appears, click Inventory option from the top-section of the page.

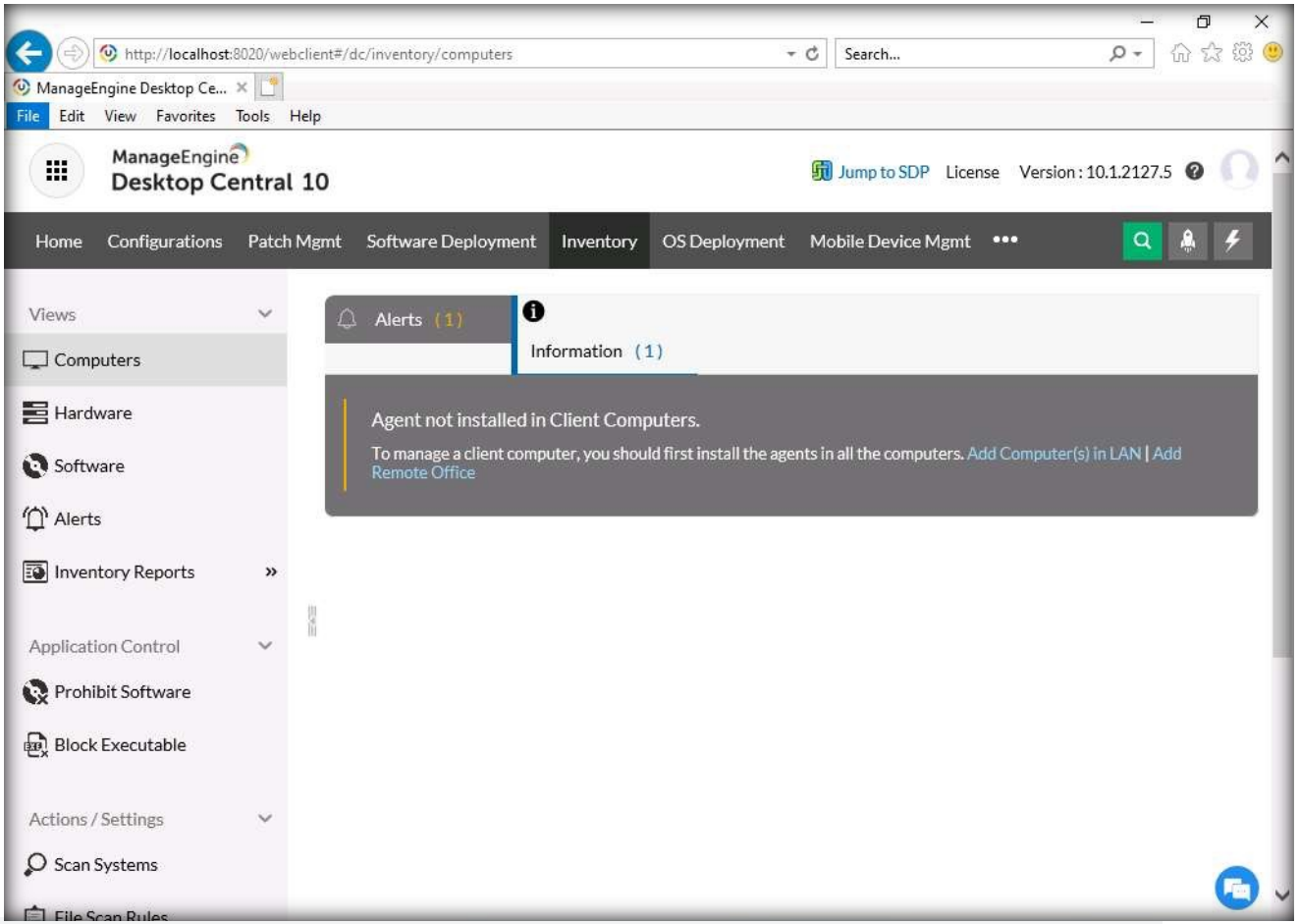
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



21. Steps involved in Asset Management diagram appears, click X to close it.

22. Navigate to the Computers option from the left-pane. In the right-pane, click Add Computer(s) in LAN link.

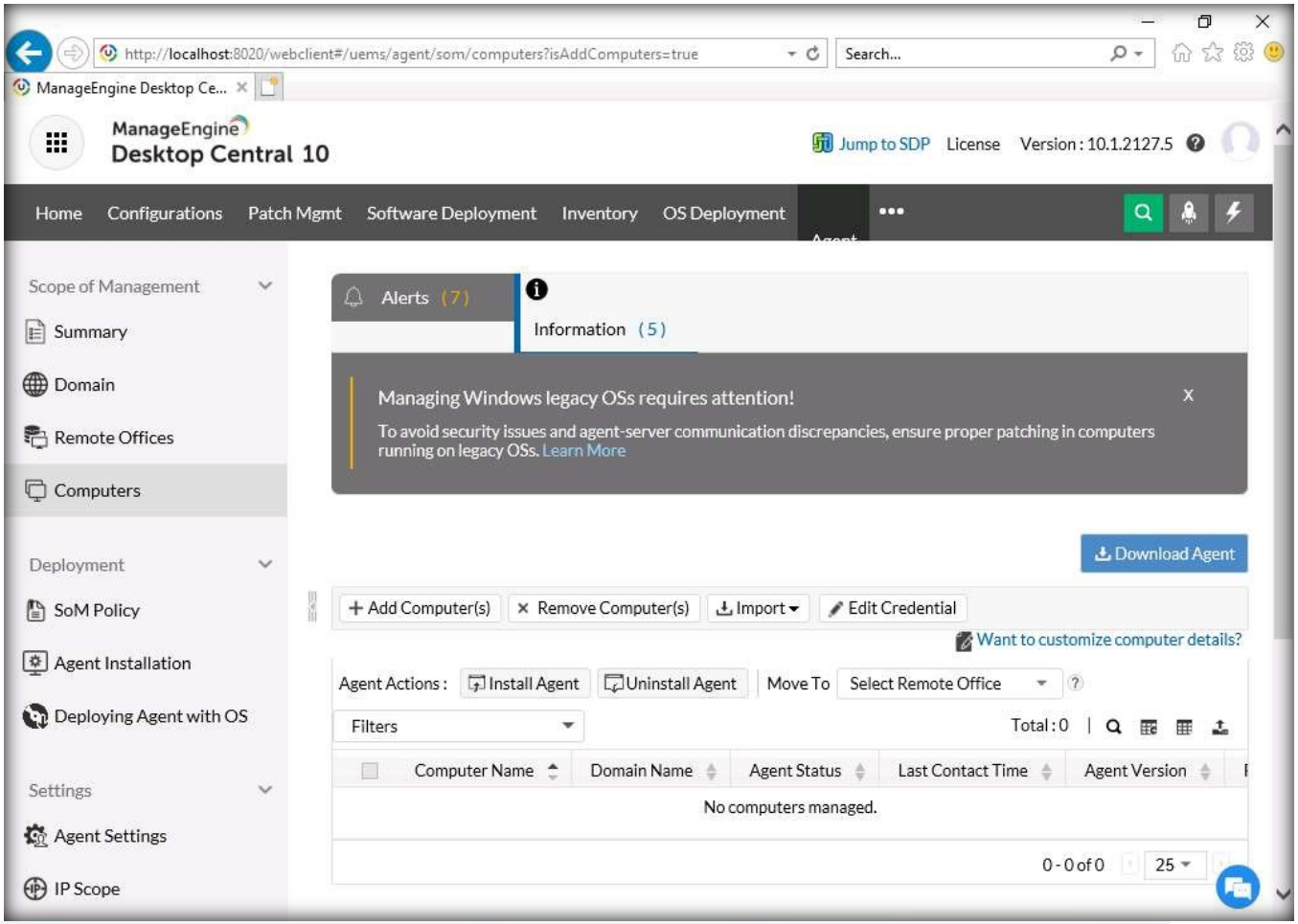
EXERCISE 2:
BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



23. Add Computer(s) wizard appears, close it.

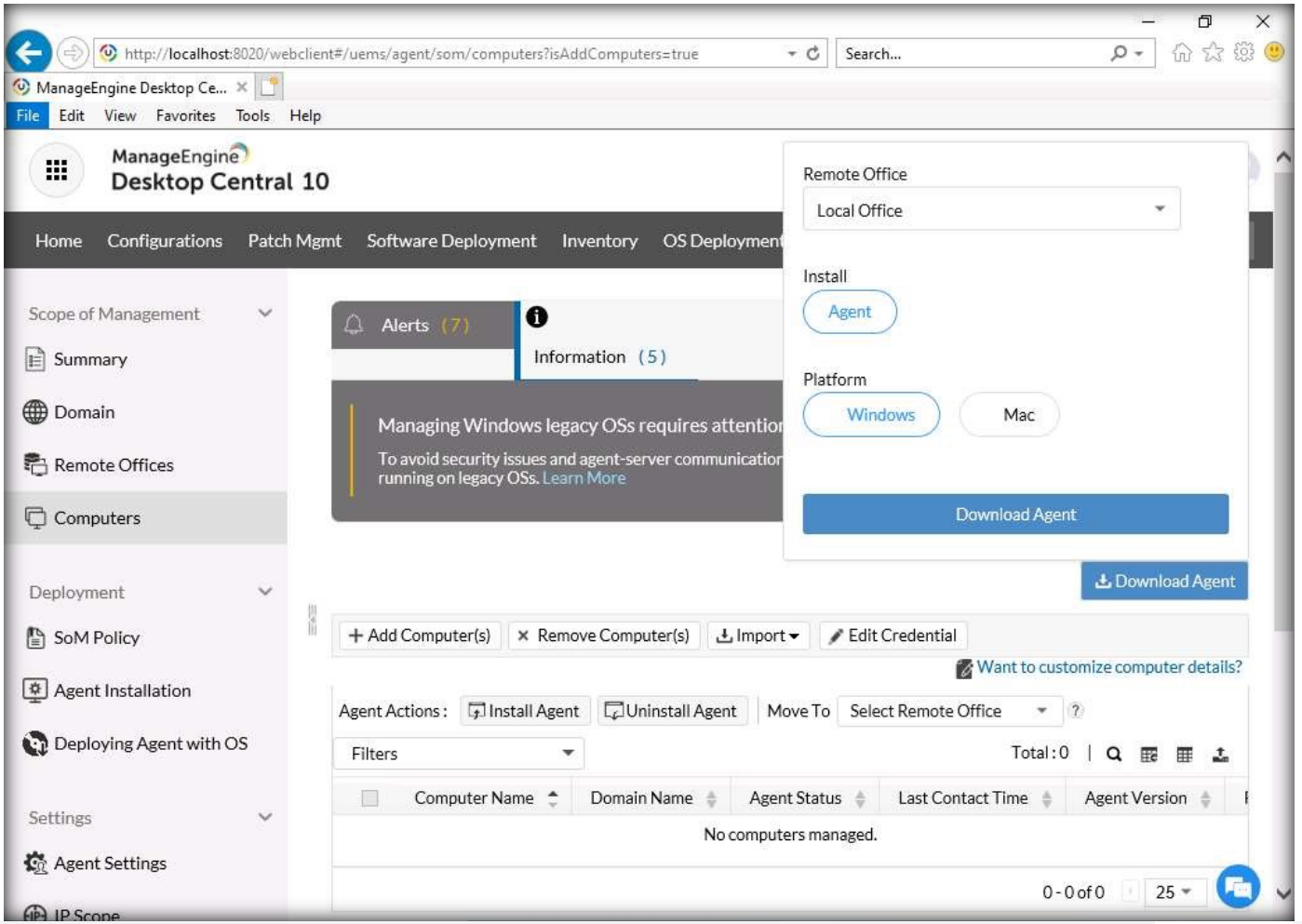
24. Observe that a blank table appears, click Download Agent button from the right-pane.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



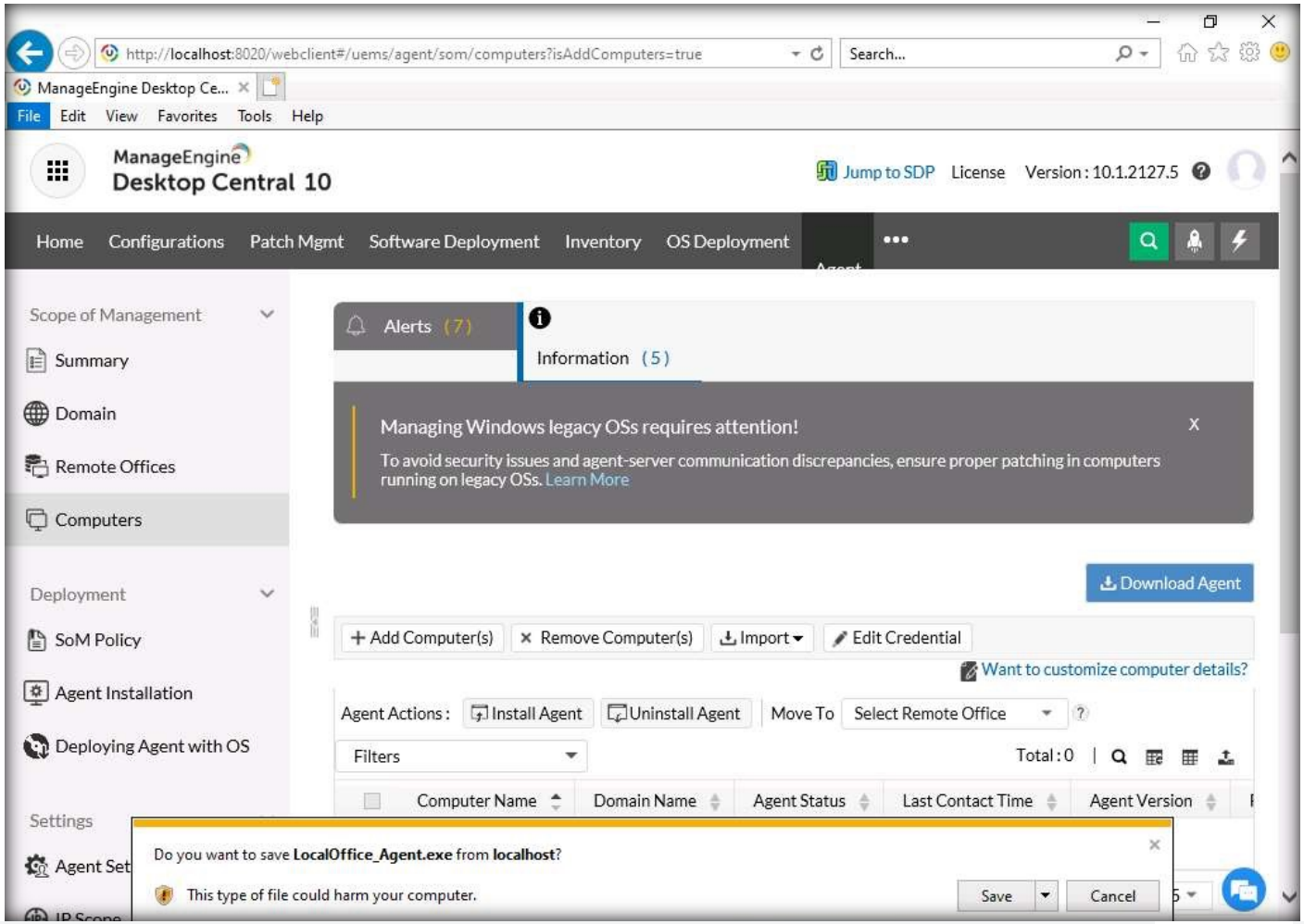
25. A pop-up appears, ensure that Windows is selected under Platform section and click Download Agent.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



26. Do you want to save LocalOffice_Agent.exe from localhost? pop-up appears in the lower-section of the page, click Save.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL

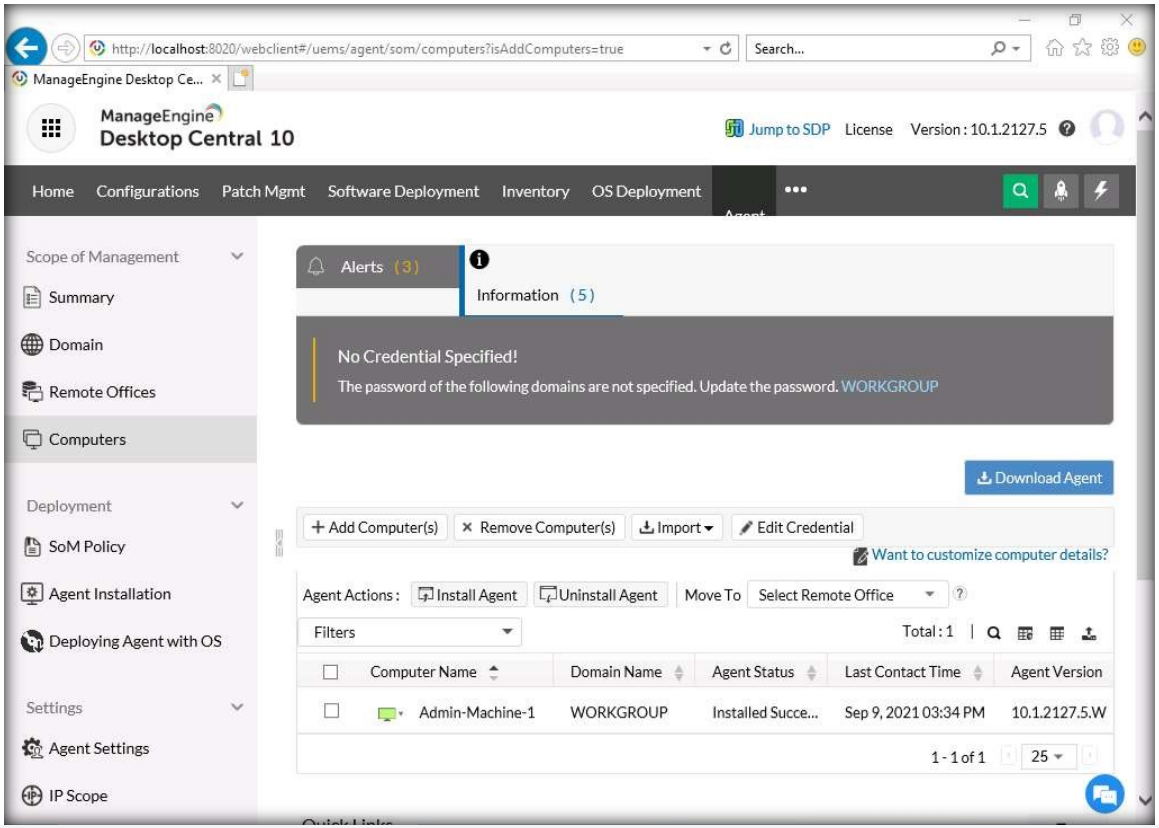


27. After the completion of download, click Run to install the tool.
Note: If User Account Control window appears, click Yes.

28. Follow the wizard driver installation to install the tool with default settings.
29. After the installation completes, click Close and refresh the page.
30. Add Computer(s) wizard appears, close it.
Note: If Register for free demo wizard appears, click Skip.

31. You can observe that a local computer appears in the table, as shown in the screenshot below.

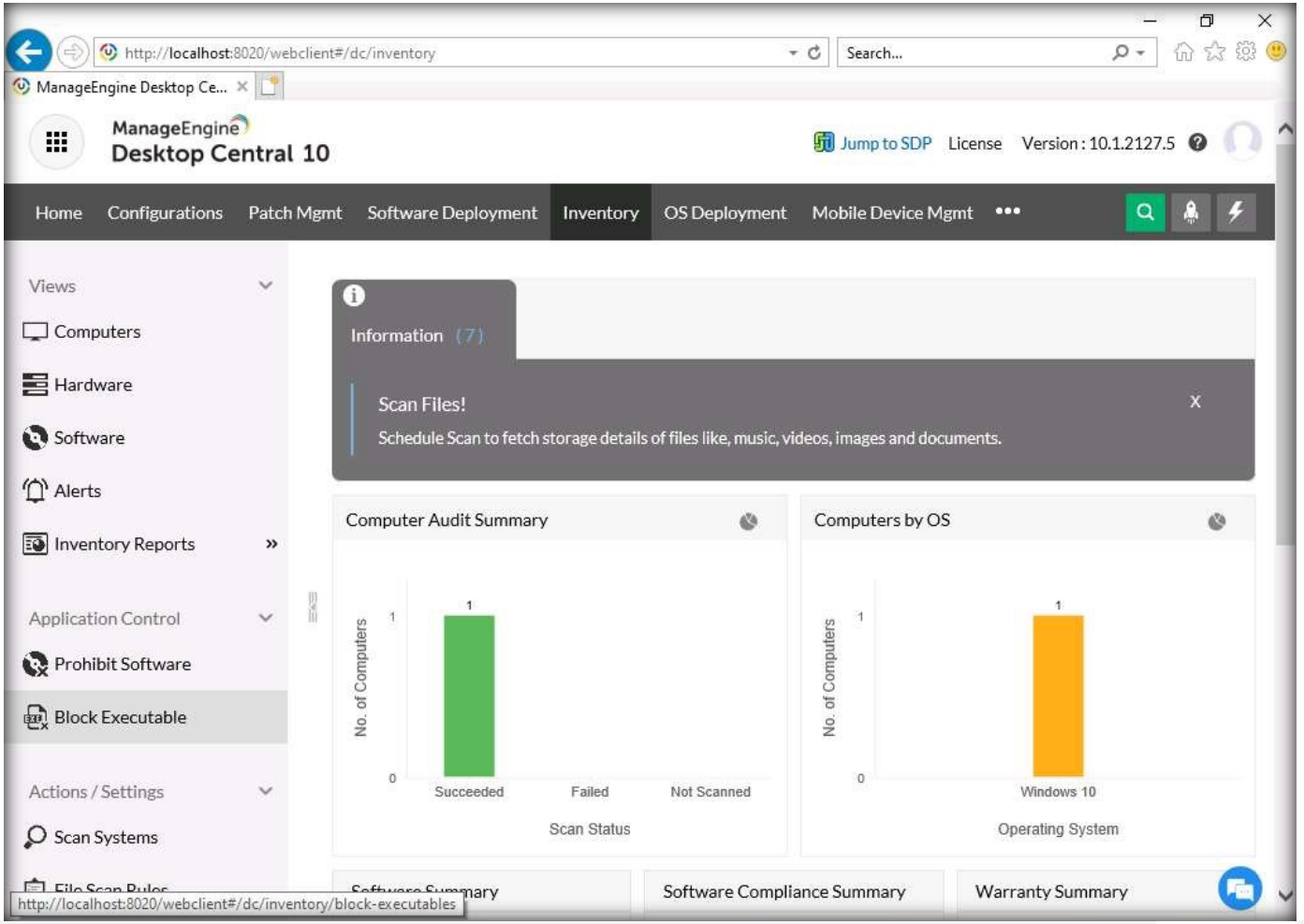
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



32. Now, click Inventory option again from the top-section of the page.

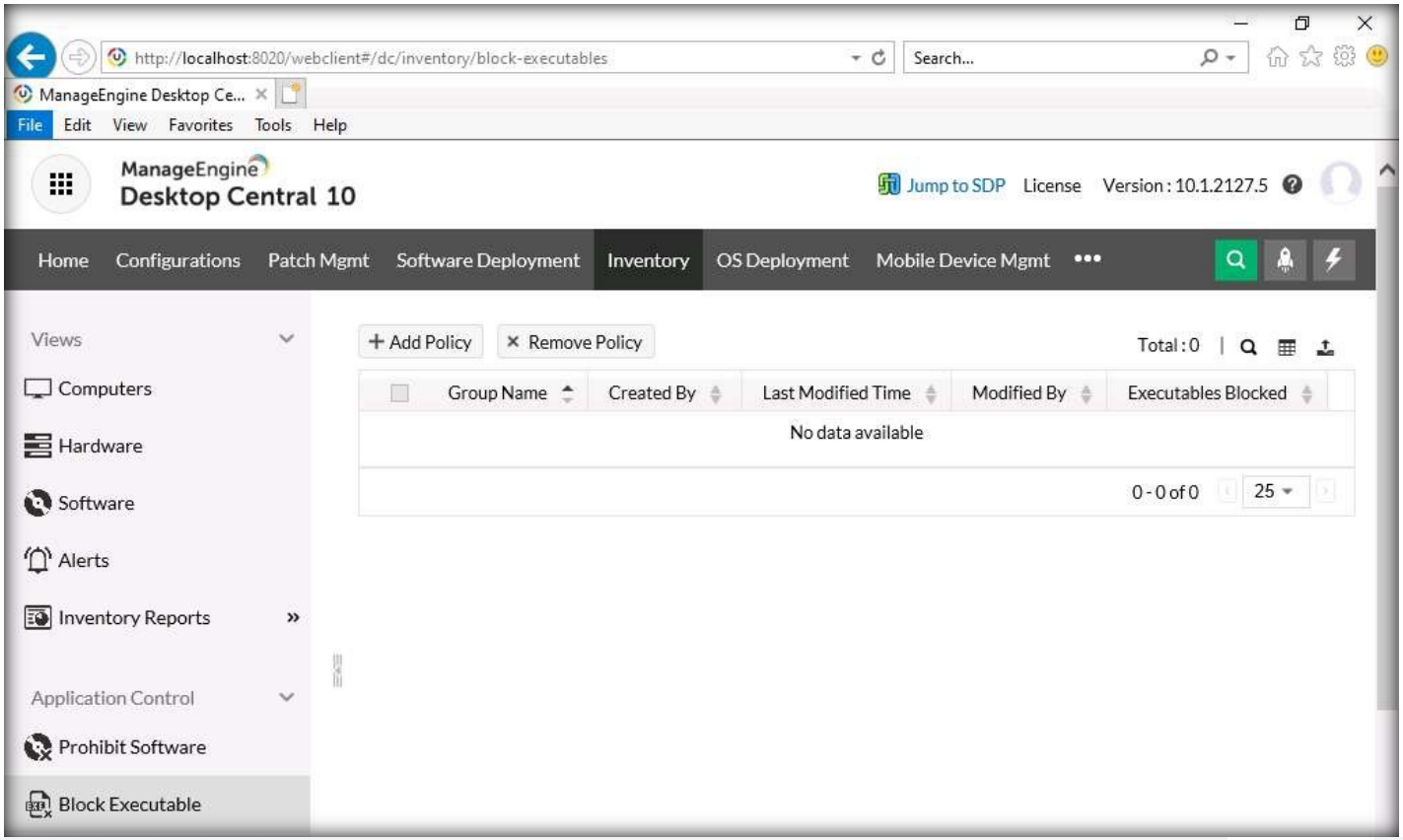
33. Inventory page appears, click Block Executable option from the left-pane.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



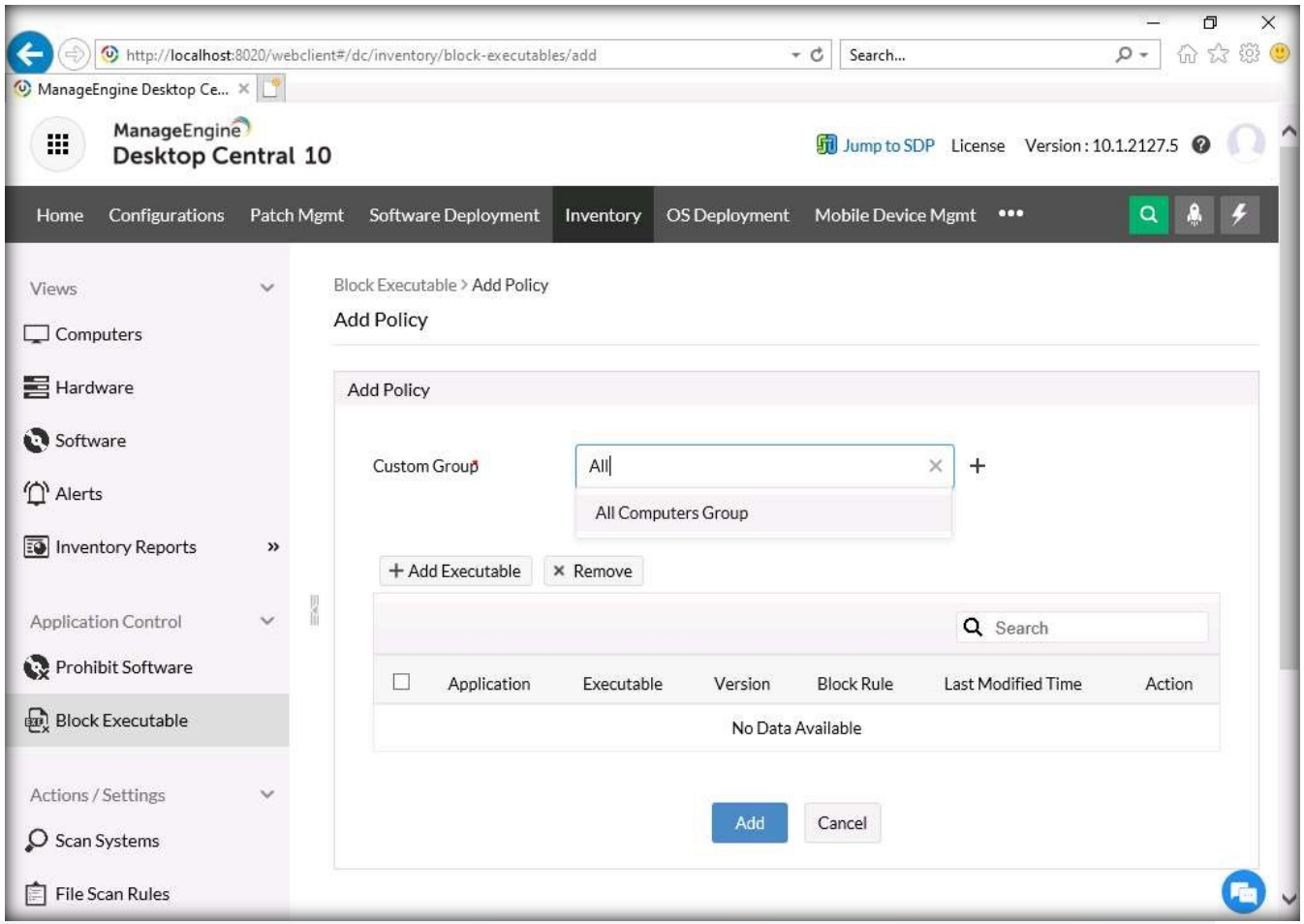
34. Block Executables page appears, click + Add Policy button from the right-pane.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



35. Add Policy page appears. In the Custom Group field, type All and All Computers Group option appears, select it.

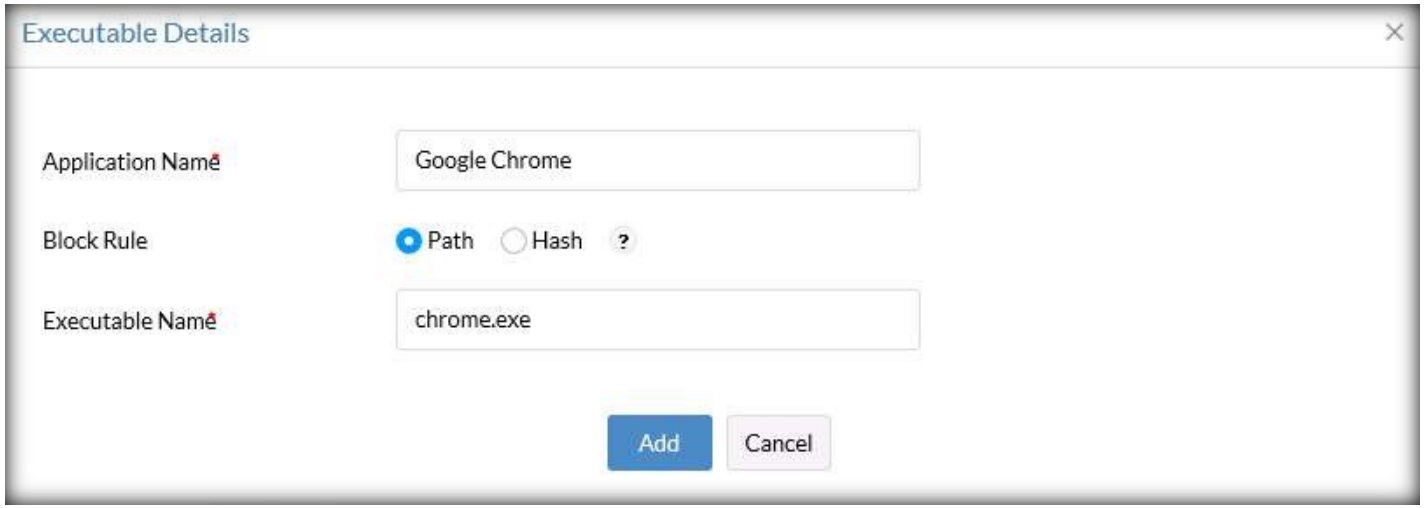
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



36. Click + Add Executable button. Executable Details pop-up appears, in the Application Name field, type Google Chrome.
Note: Here, we are blocking Google Chrome application. However, you can block an application of your choice.
37. Leave Block Rule option set to default (Path). In the Executable Name field, type chrome.exe and click Add button.

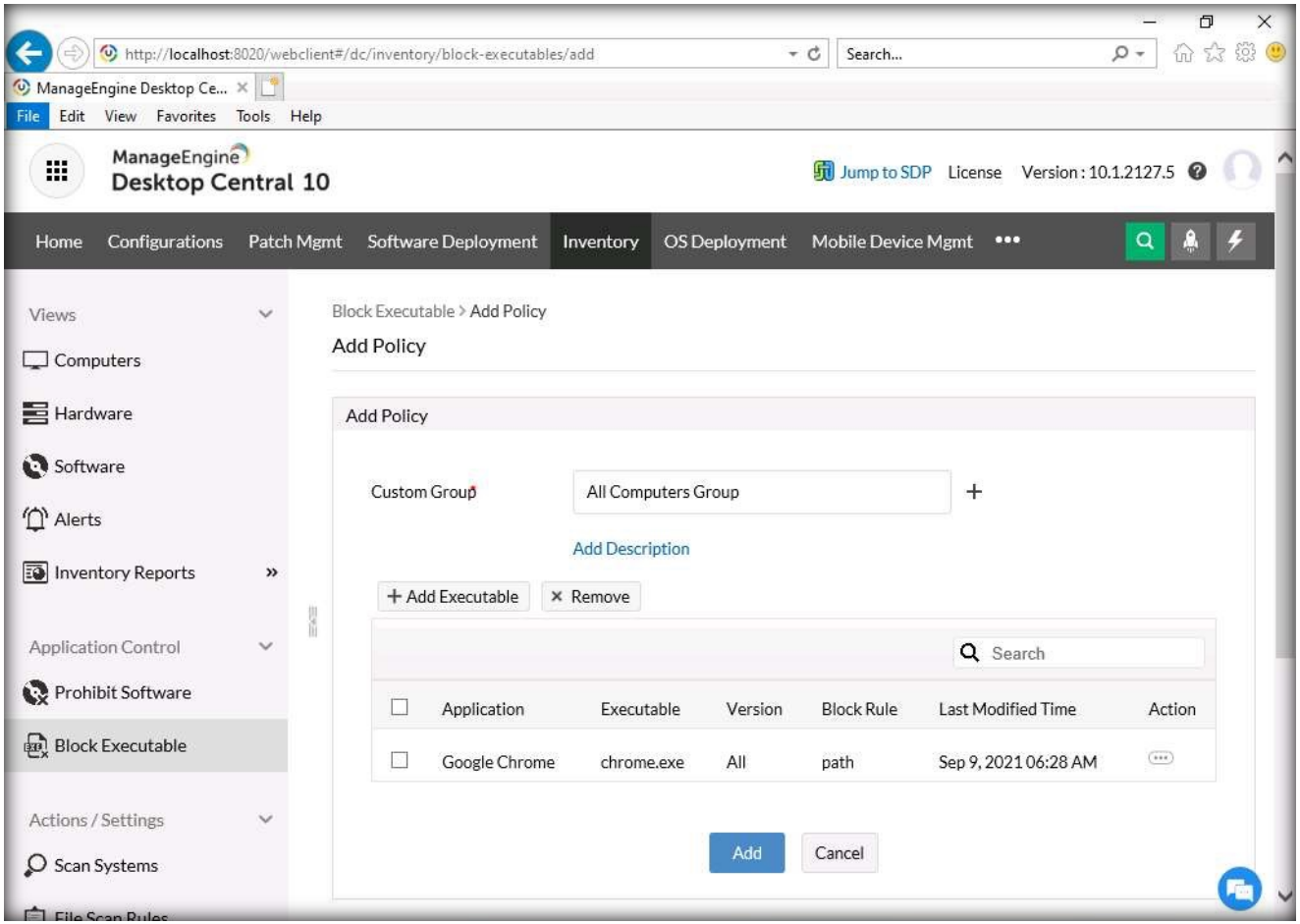
Note:
There are two methods to block an executable/application:
• A path rule can be used to block all versions of specific applications based on the name of the executable and its file extension.
• A hash value can be used to block executables even if they are renamed.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



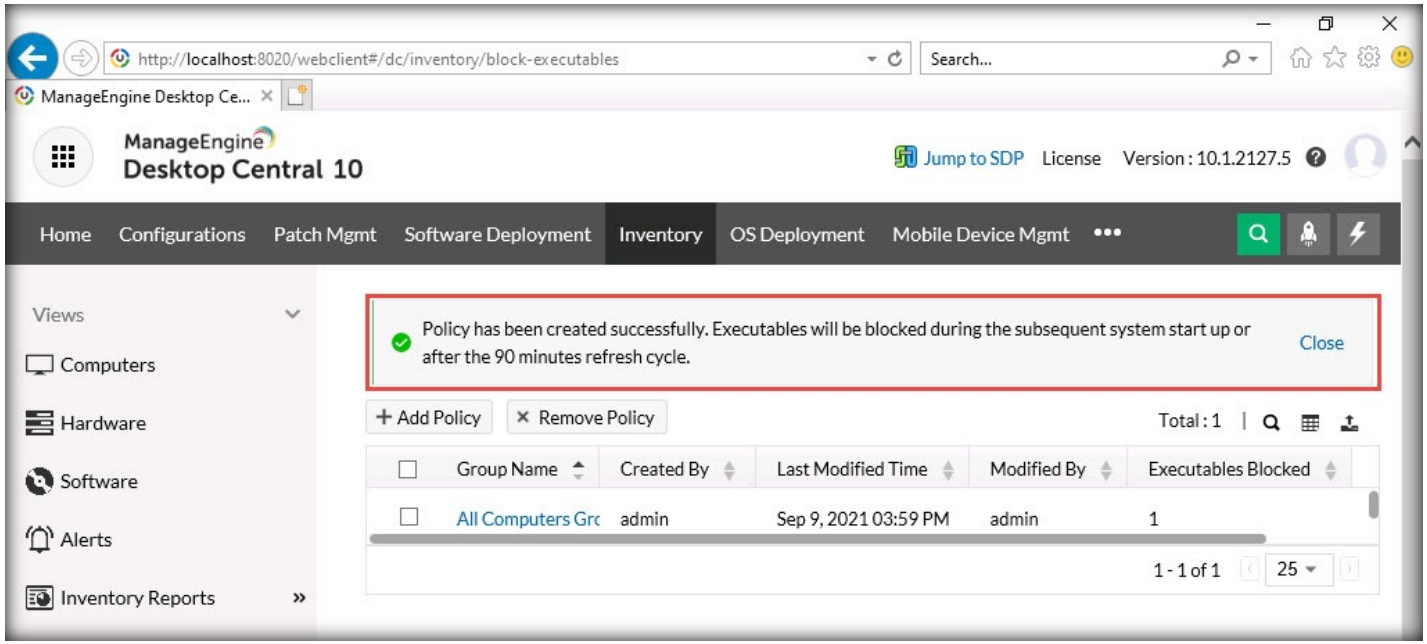
38. Observe that a policy has been created, click Add to add this policy.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



39. A notification appears confirming that the policy has been created successfully, as shown in the screenshot below.

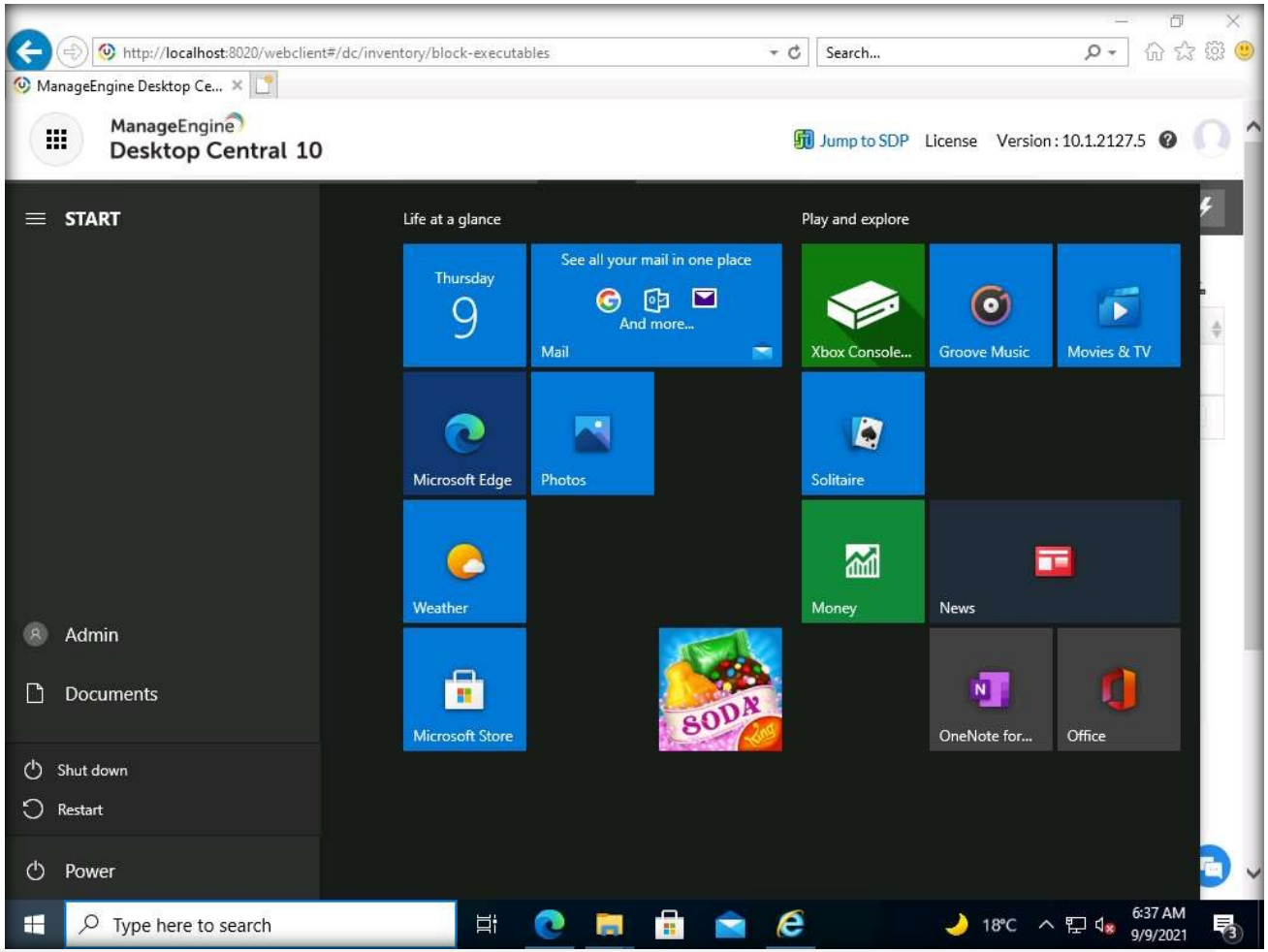
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



40. To block the executables, we need to Restart the system.

41. To restart the machine, click Windows Start icon, then Power icon. From the options, select Restart.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



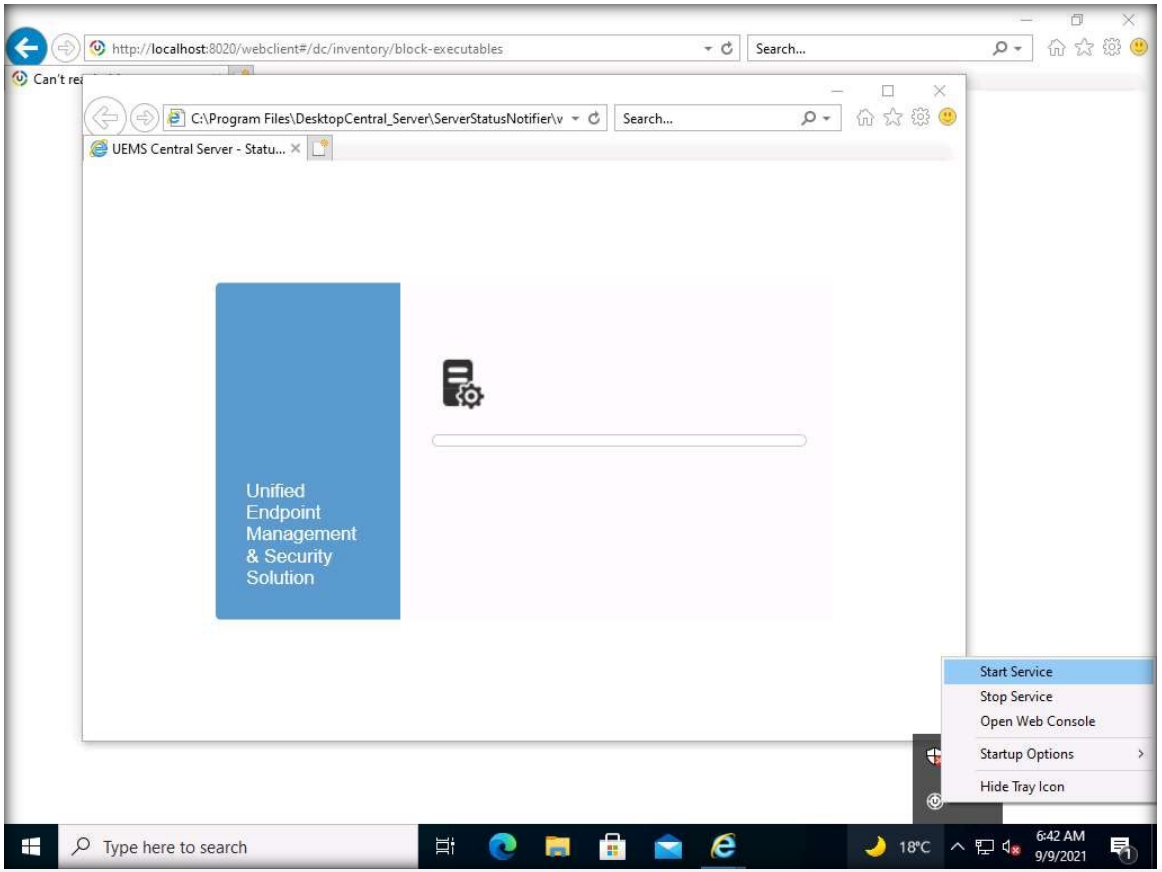
42. After the system reboots, log in with the credentials Admin and admin@123.

43. Microsoft Edge and Internet Explorer browser window appears. Close Microsoft Edge browser.

44. Click Show Hidden Icons (^) icon from the lower-right corner of the Desktop.

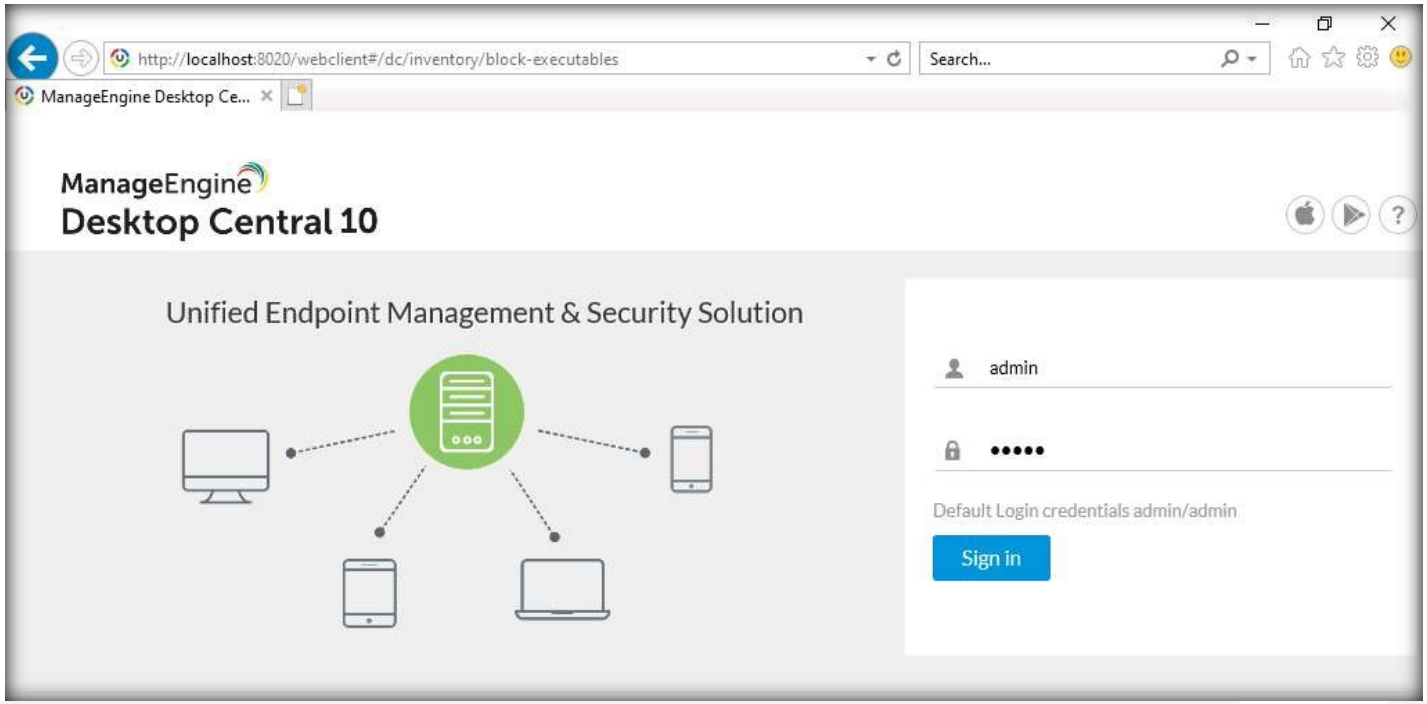
45. Right-click ManageEngine Desktop Central icon and click Start Service option.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



46. If User Account Control window appears, click Yes.
47. Navigate to Internet Explorer browser window where http://localhost:8020 is opened. Click Refresh icon ( ), present in the top-section of the window next to the URL field.
Note: If you are receiving Can't reach this page error, then navigate to Internet Explorer browser window where UEMS Central Server website is open. Click Refresh icon ( ), present in the top-section of the window next to the URL field.
Note: If a notification appears in the lower-section of the window, click Allow blocked content button.
48. The main page of ManageEngine Desktop Central appears along with a login form. You can observe that, by default, credentials are entered. Click Sign in to proceed.

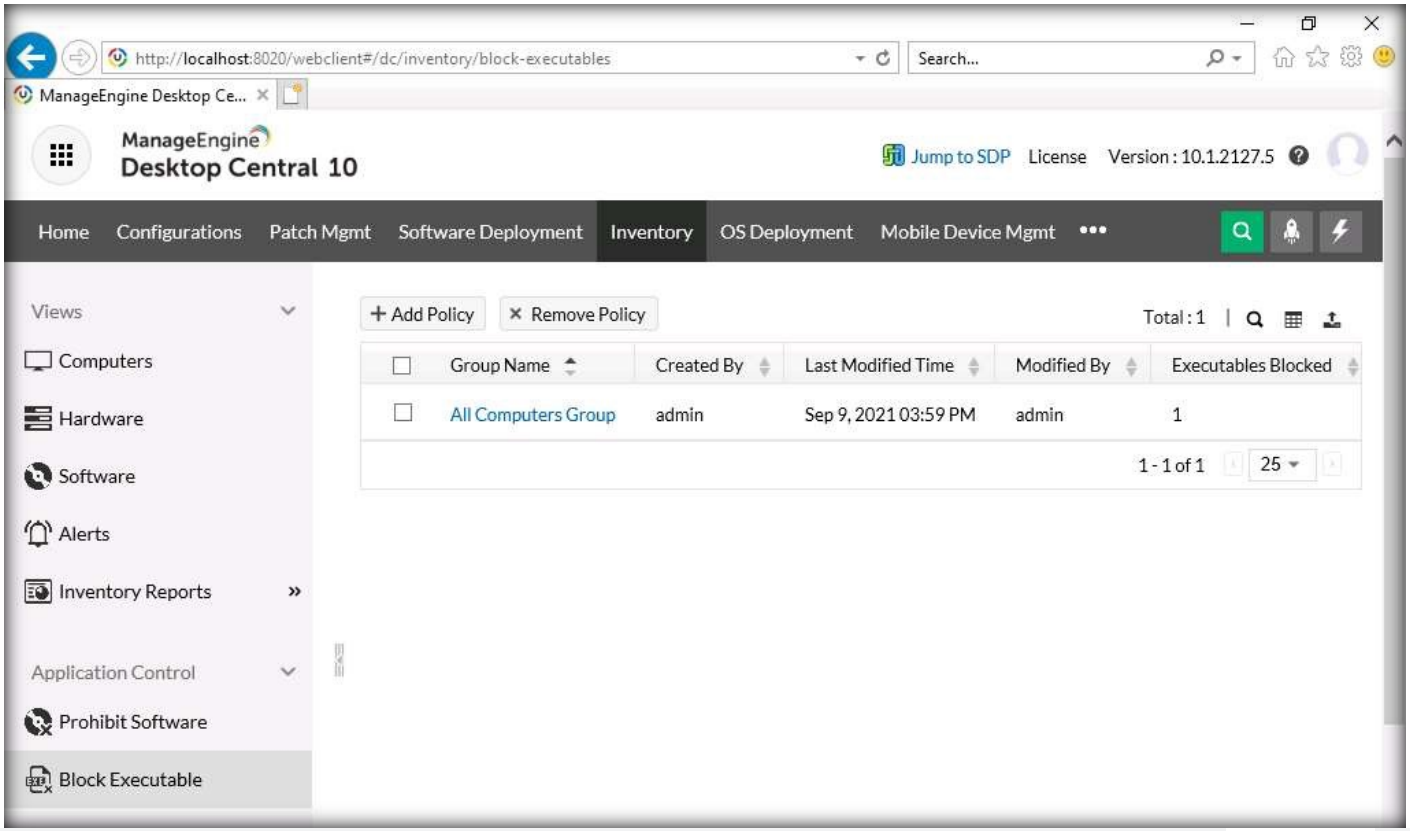
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



49. Block Executable page appears, along with the created policy.

Note: If Block Executable page does not appear automatically, navigate to Inventory and from the left pane select Block Executable.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



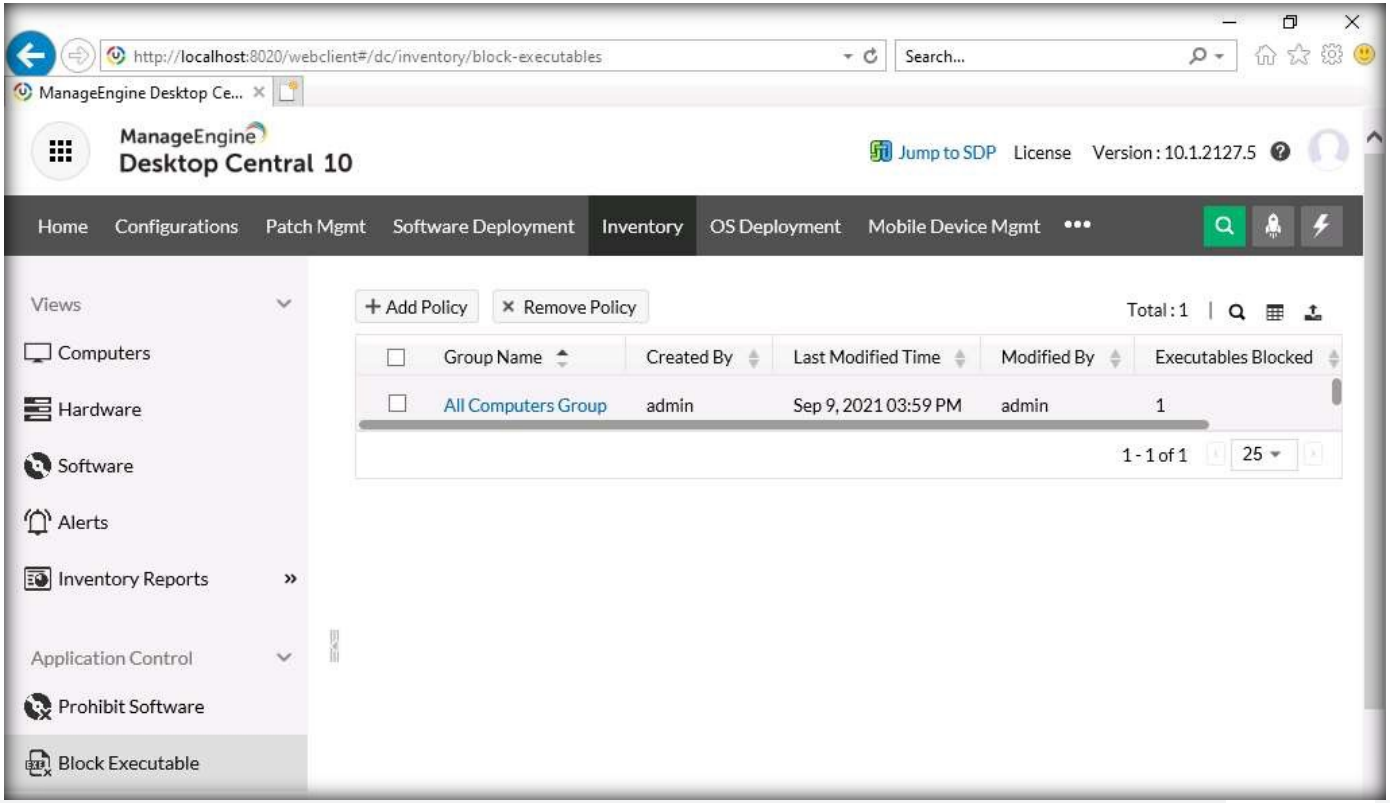
50. Now, click Show Hidden Icons (^) icon from the lower-right corner of the Desktop. Right-click ManageEngine Desktop Central - 10.1.2127.8.W icon and click Apply Configurations option.

51. Minimize the browser window and double-click Google Chrome icon on the Desktop to launch it.

52. You can observe that the application does not open up, indicating that it has been blocked.

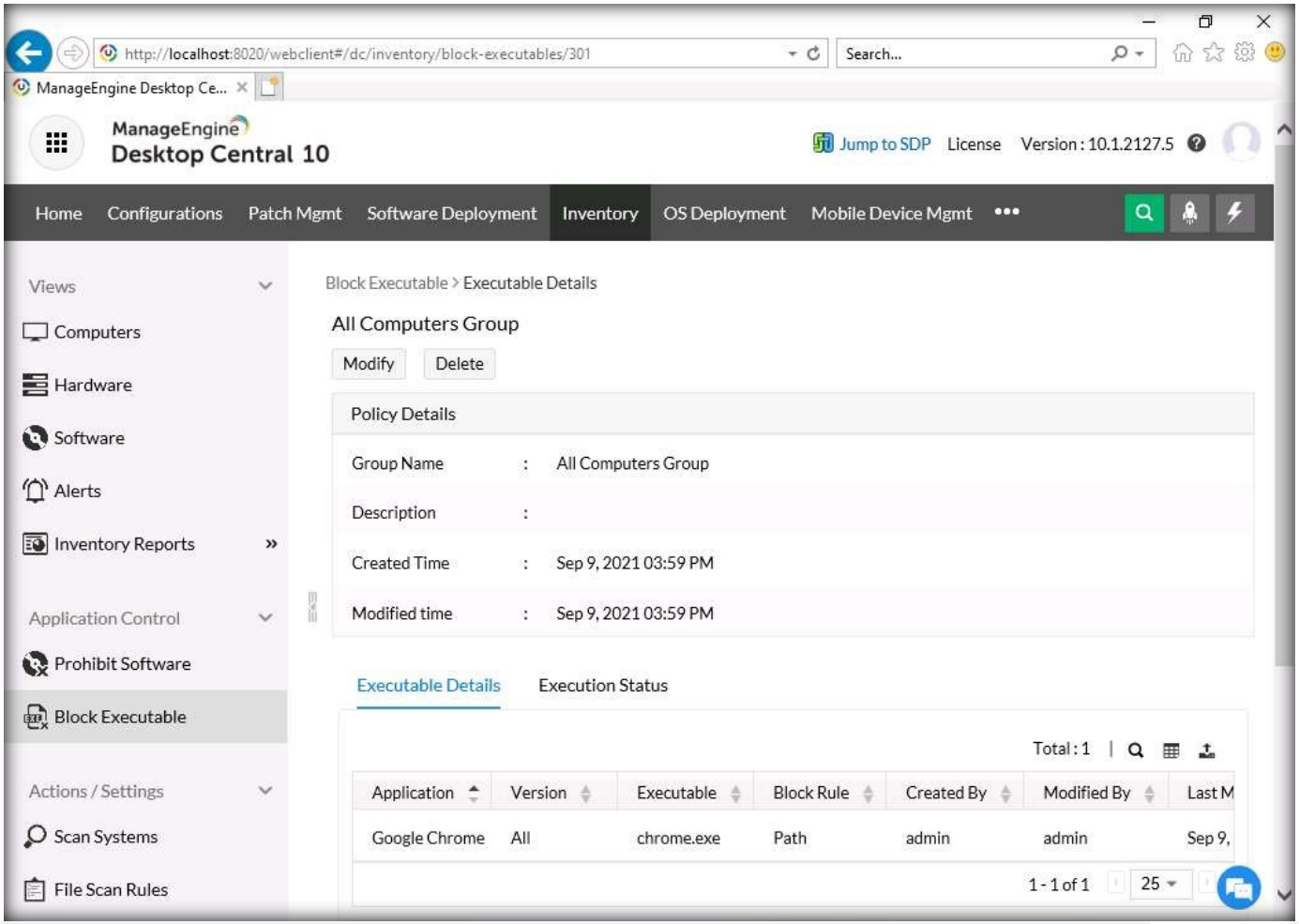
53. Switch back to the browser window. In the Block Executables page, click on All Computers Group link in the policy.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



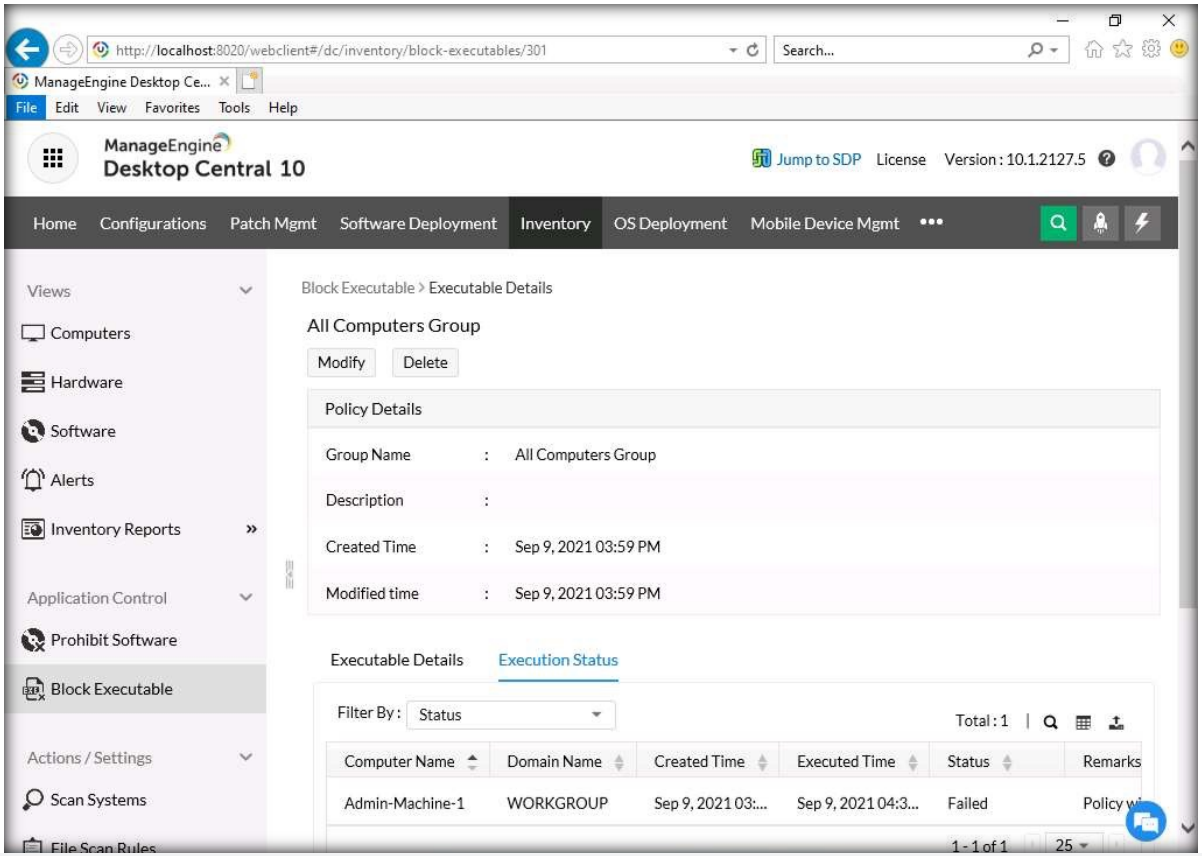
54. All Computers Group policy details appears, as shown in the screenshot below.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



55. Click on Execution Status option from the lower-section of the page.
56. It displays a list of machines (here, Admin Machine-1) that tried to access blocked application, as shown in the screenshot below.
57. This concludes the demonstration showing how to block application using ManageEngine Desktop Central.
58. You can further explore other options and features offered by the tool.
59. Close all open windows.
60. After the completion of this task, delete the executable policy to unblock the blocked applications on the system.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



EXERCISE 3: **PERFORM APPLICATION SANDBOXING USING SANDBOXIE**

Application sandboxing is the process of running applications in a sealed container (sandbox) so that the applications cannot access critical system resources and other programs.

LAB SCENARIO

In this lab, we will execute an application within a sandbox this will restrict the application's access to the system resources and data outside the sandbox. A security professional must have proper knowledge regarding application sandboxing in order to prevent cyber attacks on the system applications.

OBJECTIVE

The objective of this lab is to perform application sandboxing using tools such as Sandboxie.

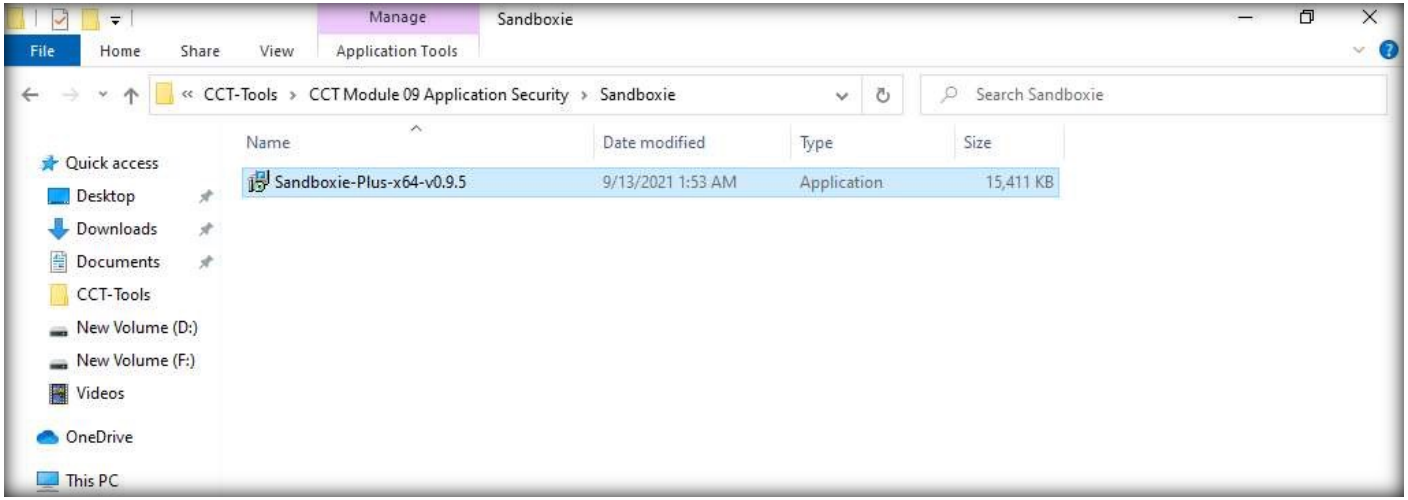
OVERVIEW OF APPLICATION SANDBOXING

Application sandboxing provides an extra layer of security and protects apps and the system from malicious apps. It is often used to execute untrusted or untested programs or code from untrusted or unverified third parties without risking the host system or OS. The protection provided by the sandbox is not sufficiently robust against advanced malware that target the OS kernel.
Installing a sandboxed app in a system creates a specific directory (sandboxed directory). By default, the app has unlimited read and write access to the directory. However, apps within the directory are not allowed to read or write the files outside the directory or access other system resources, unless authorized.

Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machine are running.

1. In the Admin Machine-1 virtual machine, navigate to Z:\CCT-Tools\CCT Module 09 Application Security\Sandboxie. Double-click Sandboxie-Plus-x64-v0.9.5.exe to start the installation.

EXERCISE 3: PERFORM APPLICATION SANDBOXING USING SANDBOXIE



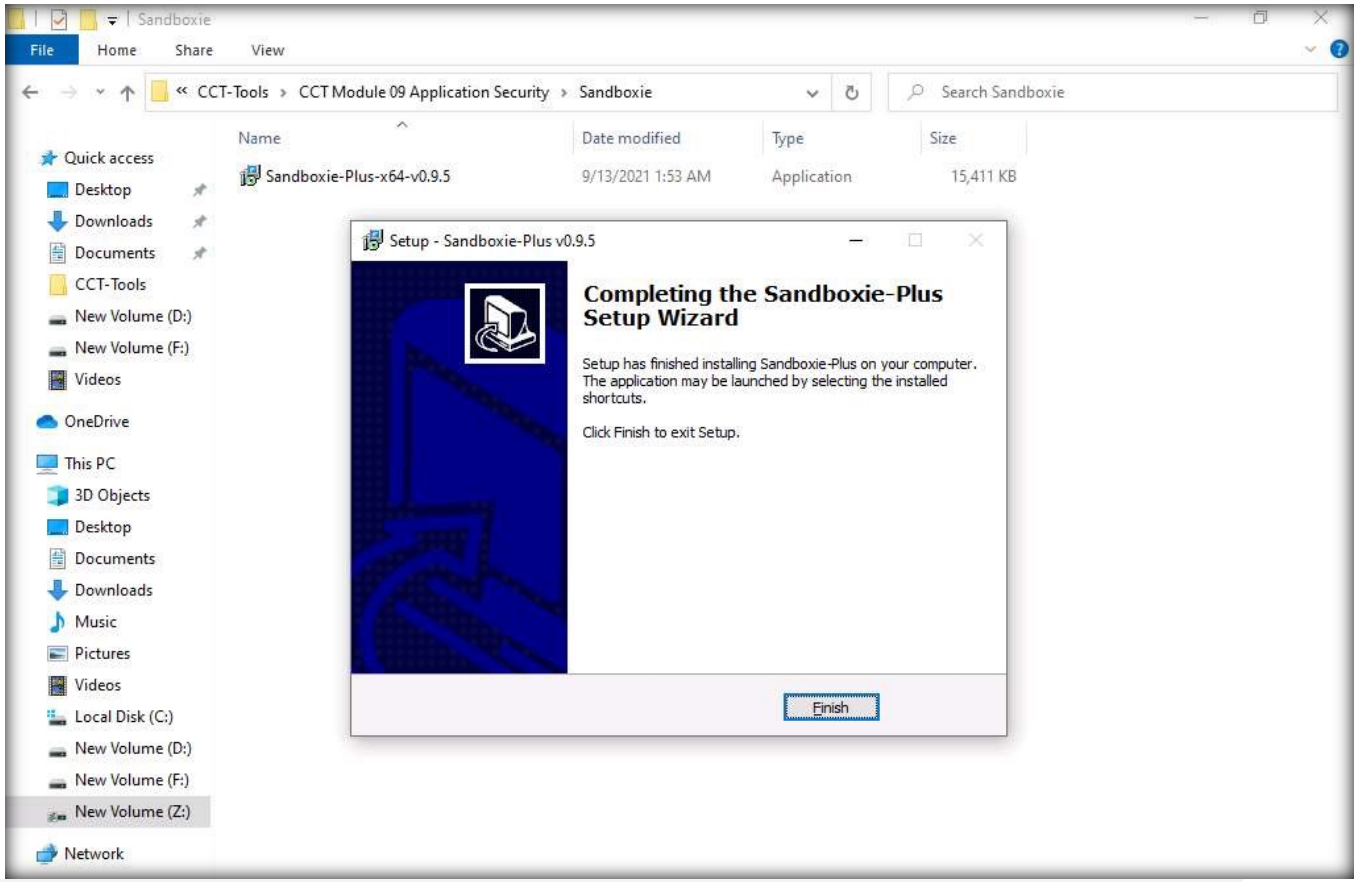
2. A User Account Control pop-up appears, click Yes.

3. Select Setup Language wizard appears, leave default language selected as English, click OK.

4. Follow the wizard driven installation and install the tool with the default settings.

5. After the installation completes, click Finish.

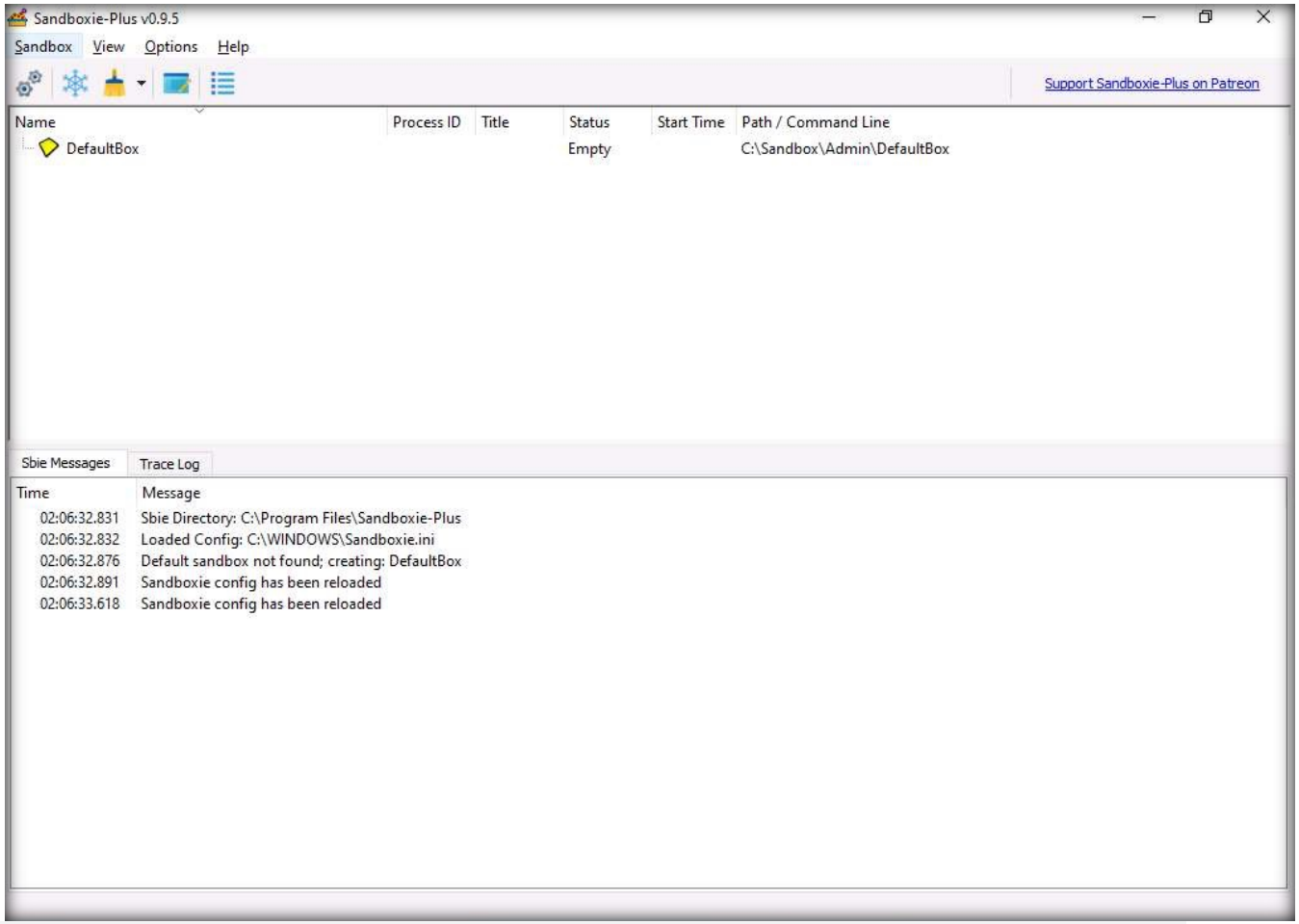
EXERCISE 3: PERFORM APPLICATION SANDBOXING USING SANDBOXIE



6. Now, close the File Explorer window and double-click Sandboxie-Plus shortcut present on the Desktop.

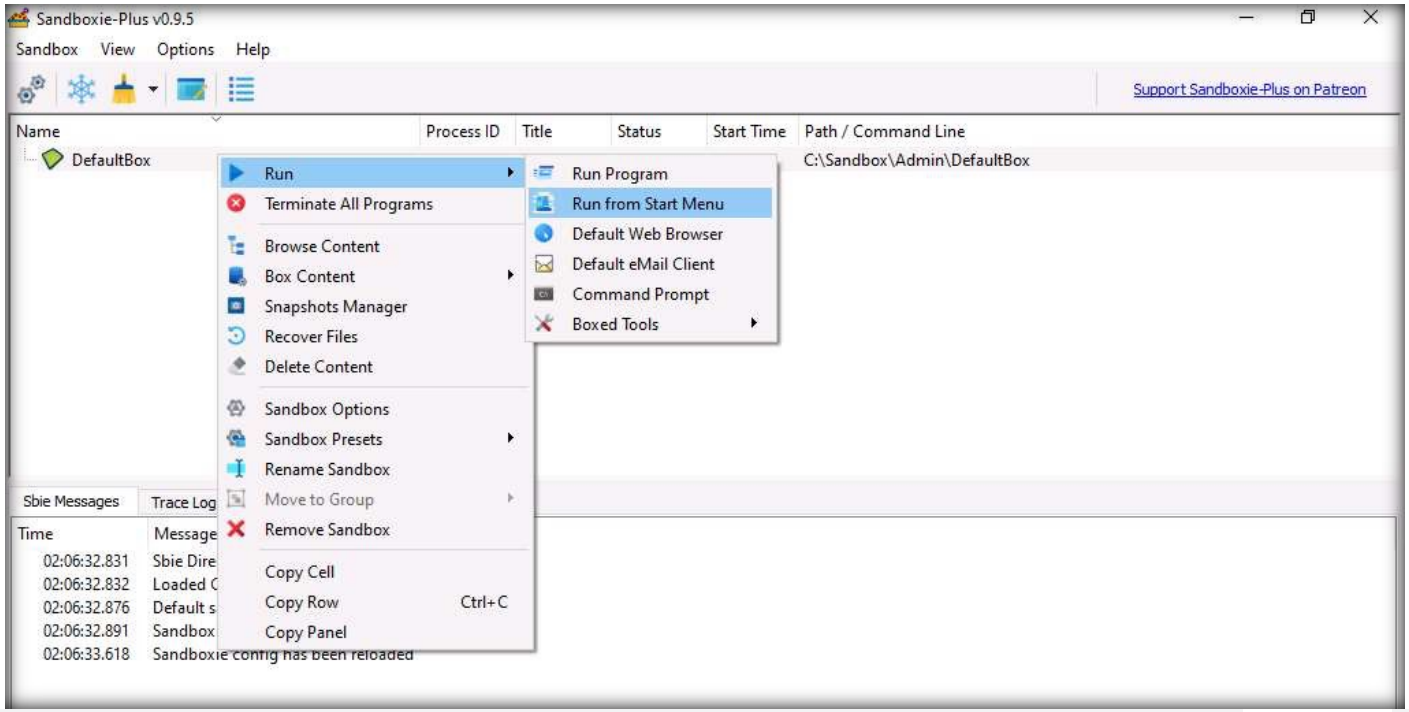
7. Sandboxie window appears, maximise it.

EXERCISE 3:
PERFORM APPLICATION SANDBOXING USING SANDBOXIE



8. You can observe that a DefaultBox is present by default with the Status as Empty. Right-click on it and navigate to Run → Run from Start Menu.

EXERCISE 3:
PERFORM
APPLICATION
SANDBOXING USING
SANDBOXIE

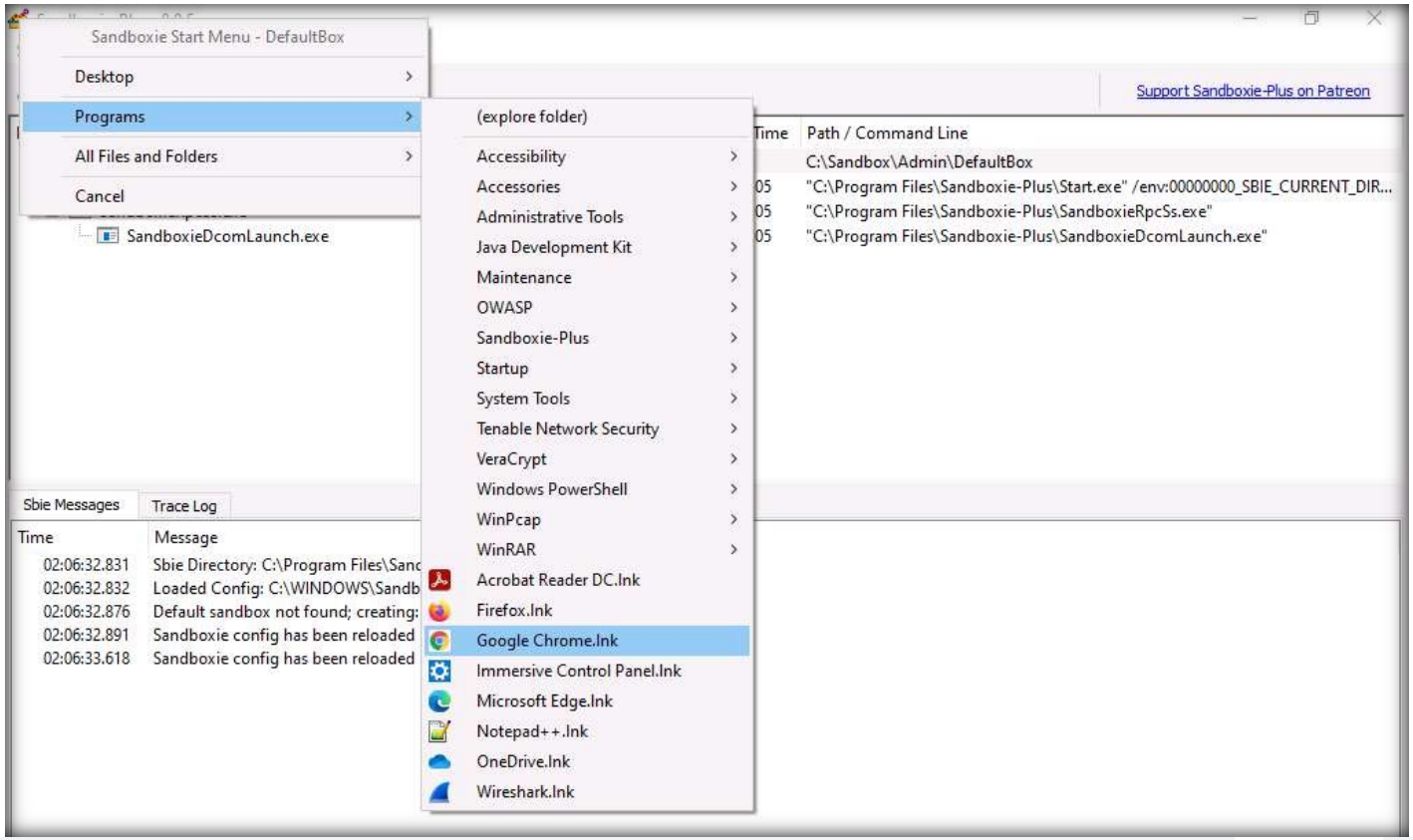


9. A pop-up appears with a list of options categorized with respect to the location of applications.

10. Navigate to Programs → Google Chrome.lnk.

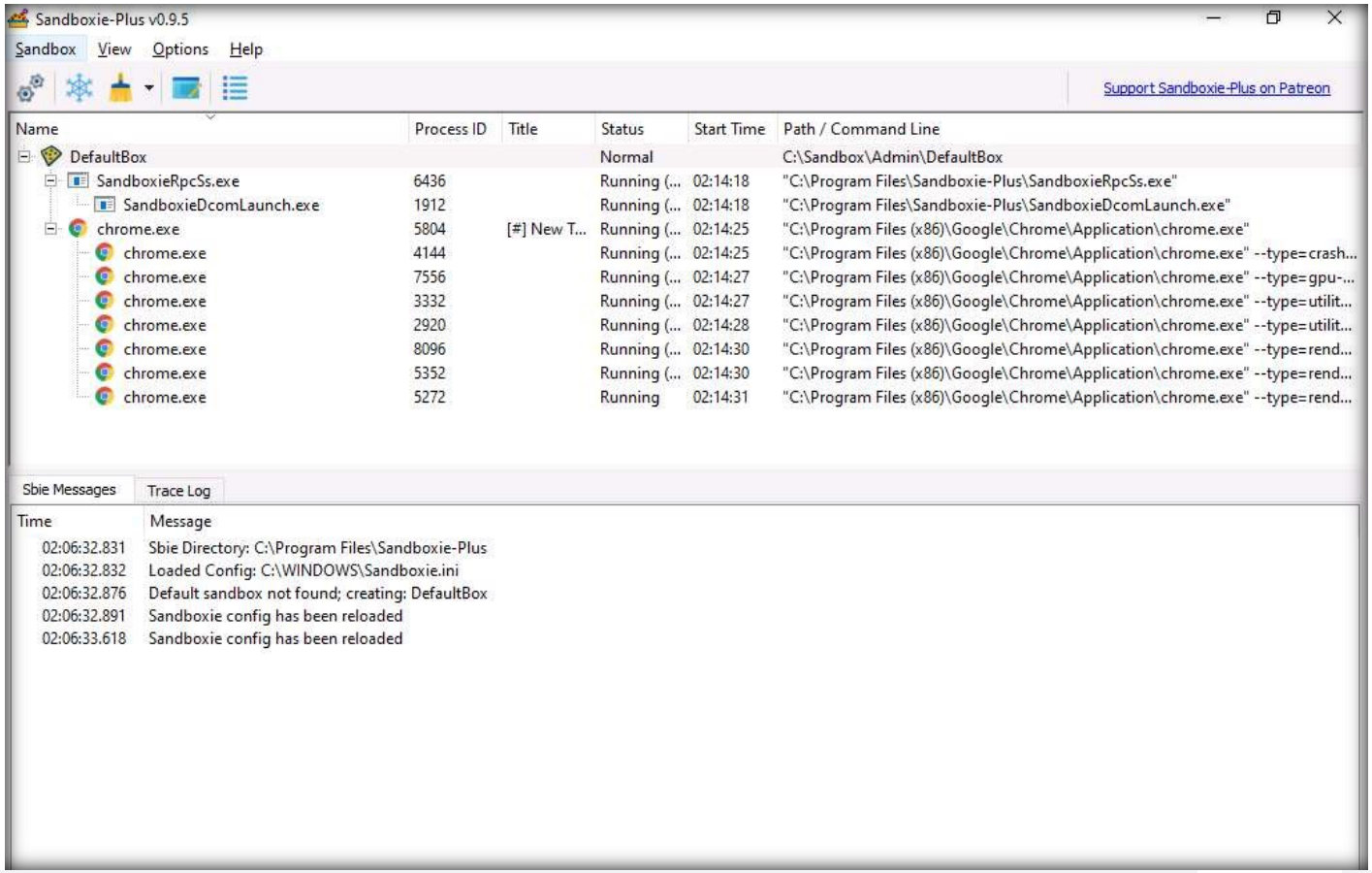
Note: Here, we have selected Google Chrome application. While performing the lab, you can select any application of your choice.

EXERCISE 3: PERFORM APPLICATION SANDBOXING USING SANDBOXIE



11. You can observe that Google Chrome application is launched under DefaultBox link, as shown in the screenshot below.

EXERCISE 3:
PERFORM APPLICATION SANDBOXING USING SANDBOXIE



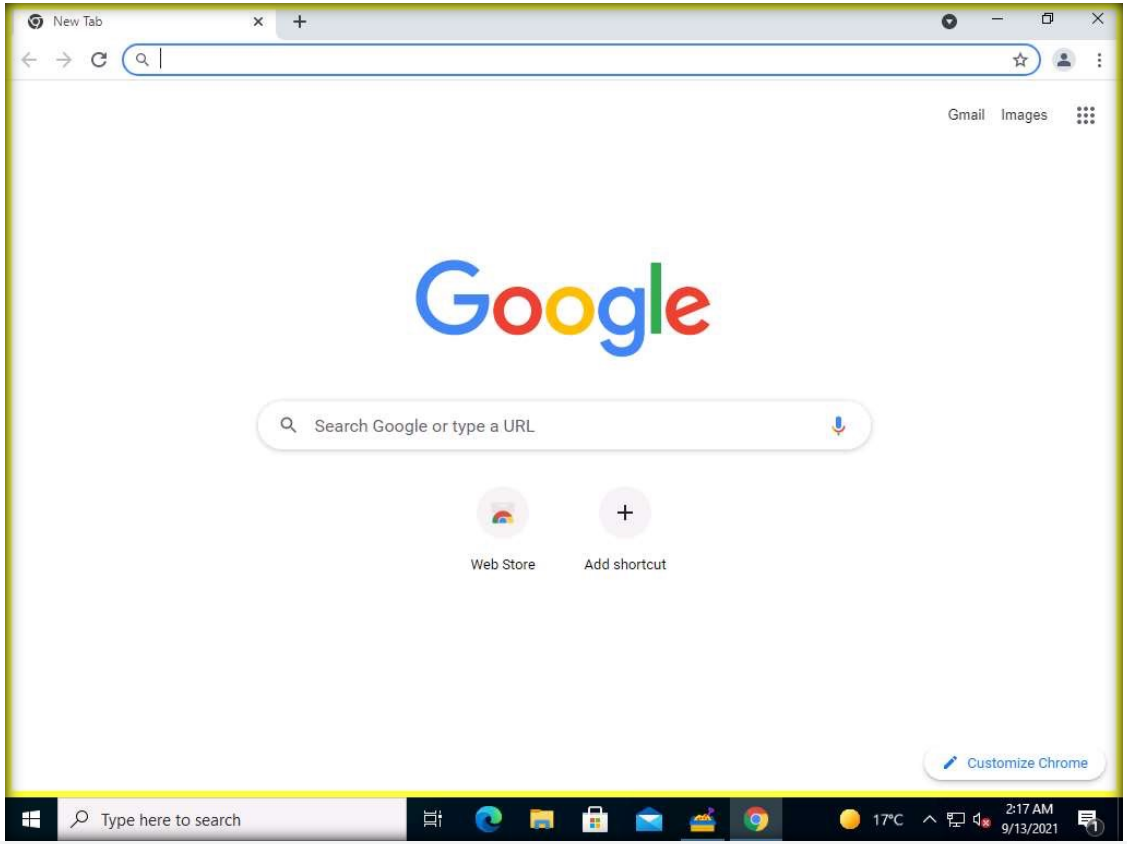
12. Maximize the Google Chrome window, you can browse the internet securely as the Sandboxie tool keeps the browser isolated and blocks malicious software, viruses, ransomware, and zero-day threats. It also prevents websites from modifying files and folders on the system.

13. Similarly, you can execute other applications securely using Sandboxie.

14. You can further explore the various other features and options within the tool.

15. This concludes the demonstration showing how to perform application sandboxing using Sandboxie.

EXERCISE 3:
PERFORM APPLICATION SANDBOXING USING SANDBOXIE



EXERCISE 4: **DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP**

Web applications are software programs that run on web browsers and act as the interface between users and web servers through web pages.

LAB SCENARIO

Organizations are increasingly using web applications to provide high-value business functions to their customers such as real-time sales, transactions, inventory management across multiple vendors including both B-B and B-C e-commerce, workflow and supply chain management, etc. Attackers exploit vulnerabilities in the applications to launch various attacks and gain unauthorized access to resources.
Hence, security professionals must have proper knowledge to detect vulnerabilities in target web applications hosted on web servers. They must scan applications for identifying vulnerabilities and detect attack surfaces on the target applications. Performing comprehensive vulnerability scanning can disclose security flaws associated with executables, binaries, and technologies used in a web application. Through vulnerability scanning, security professionals can also catalogue different vulnerabilities, prioritize them based on their threat levels, and mitigate them, so that, they are not exploited by the attackers.

OBJECTIVE

The objective of this lab is to detect web application vulnerabilities using tools such as OWASP ZAP.

OVERVIEW OF WEB APPLICATION

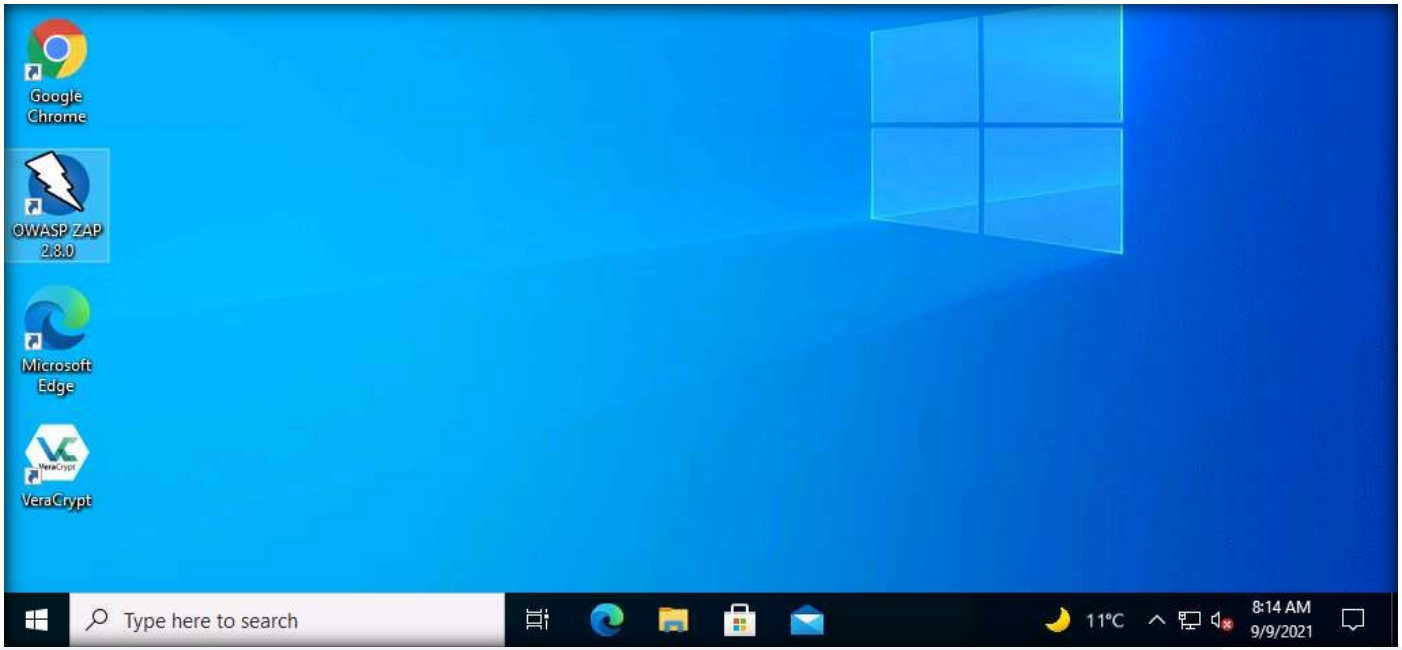
Web applications are developed as dynamic web pages, and they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing. Furthermore, there are several desktop applications that provide users with the flexibility to work using the Internet.
Increasing Internet usage and expanding online businesses have accelerated the development and ubiquity of web applications across the globe. A key factor in the adoption of web applications for business purposes is the multitude of features that they offer. Moreover, they are secure and relatively easy to develop. In addition, they offer better services than many computer-based software applications and are easy to install, maintain, and update.

Note: We will scan www.moviescope.com, a website that is hosted on the Web Server machine. Here, the host machine is the Admin Machine-1 machine.
Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, double-click the OWASP ZAP shortcut on Desktop to launch the application.

Note: Wait for a while for OWASP ZAP to get launched.
Note: If an OWASP ZAP pop-up window appears, click OK.

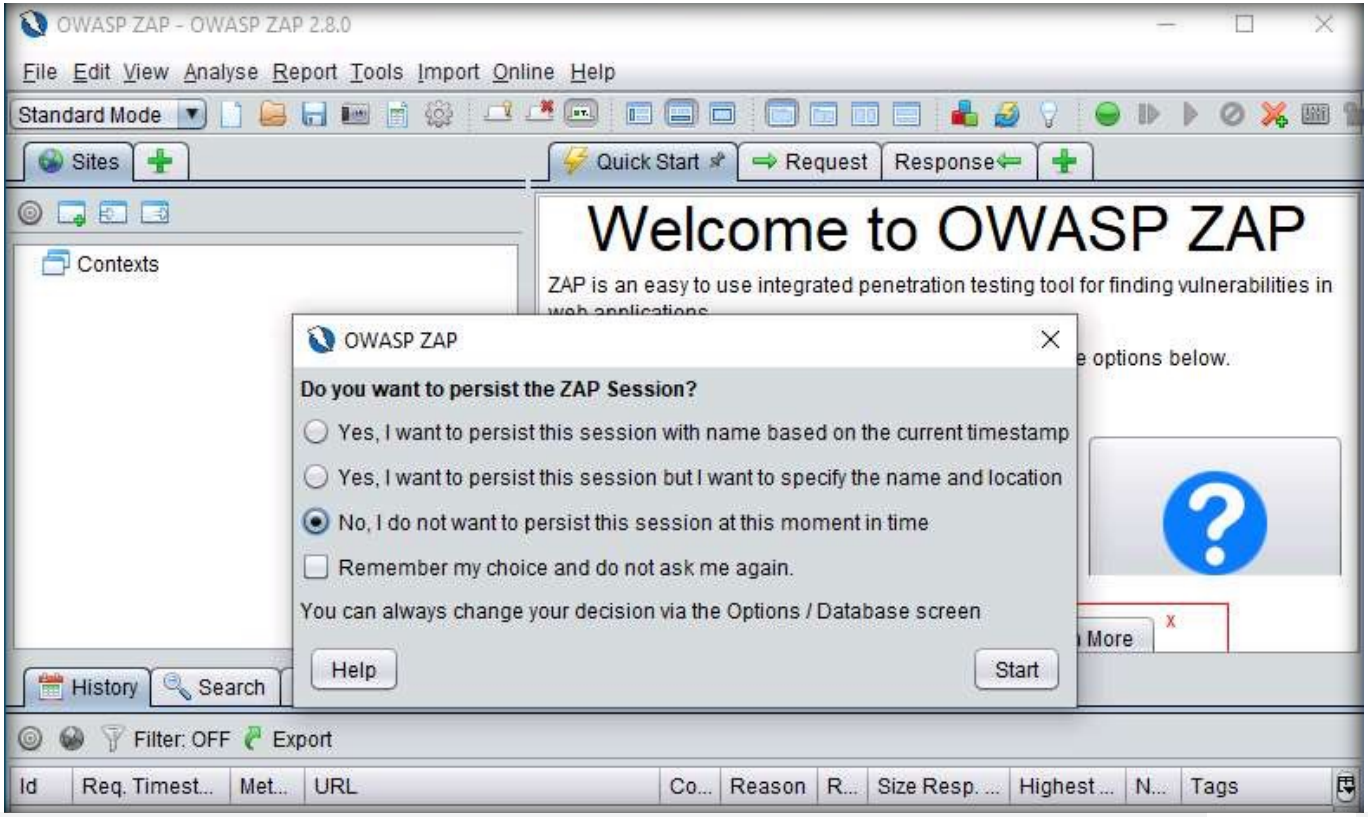
EXERCISE 4: DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



2. OWASP initializes, after the initialization completes 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.

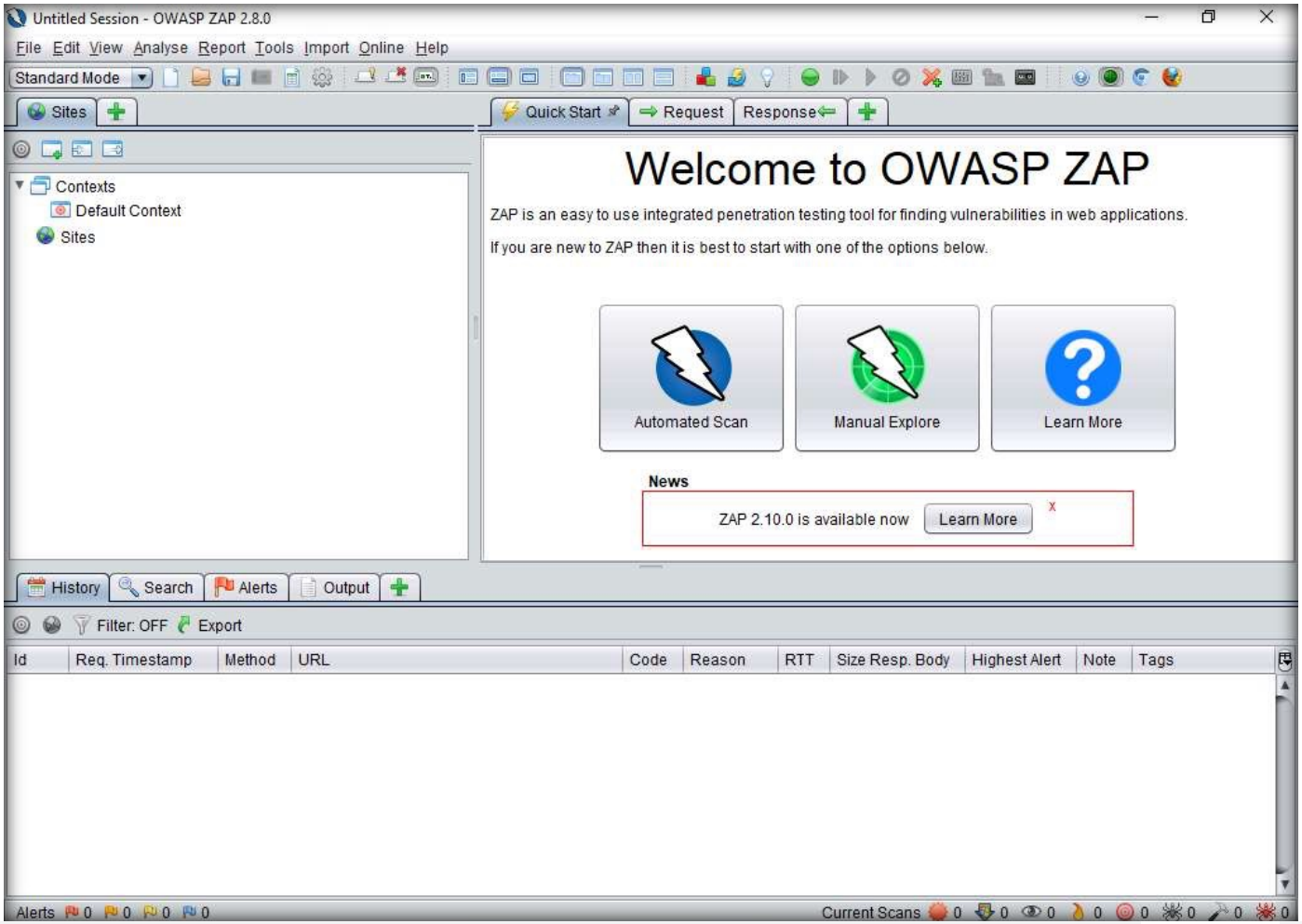
Note: If a Manage Add-ons window appears, close it.

EXERCISE 4: DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



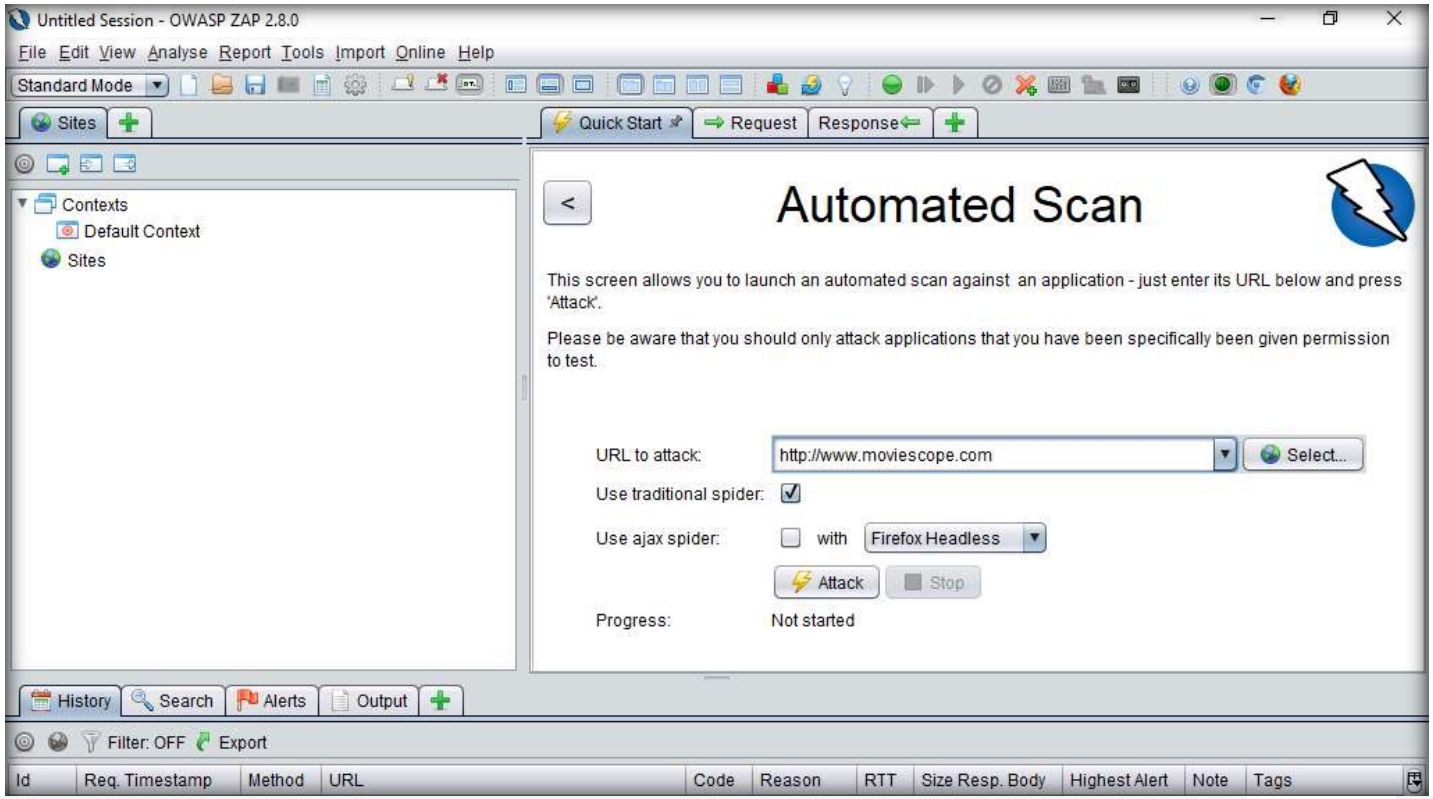
3. The OWASP ZAP main window appears; under the Quick Start tab, click the Automated Scan option.

EXERCISE 4:
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



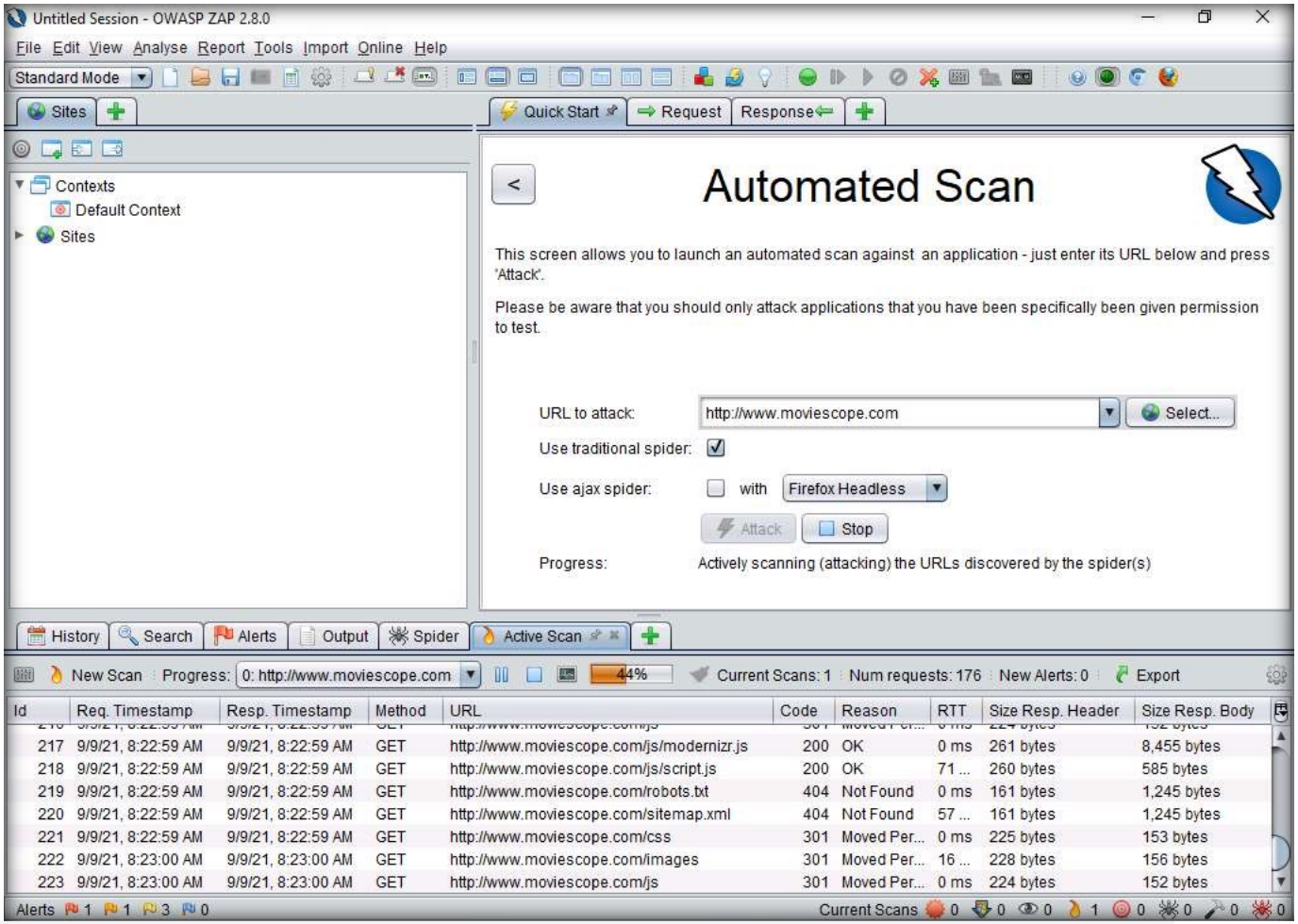
4. The Automated Scan wizard appears, enter the target website in the URL to attack field (in this case, http://www.moviescope.com). Leave other options set to default, and then click the Attack button.

EXERCISE 4:
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



5. OWASP ZAP starts performing Active Scan on the target website, as shown in the screenshot below.

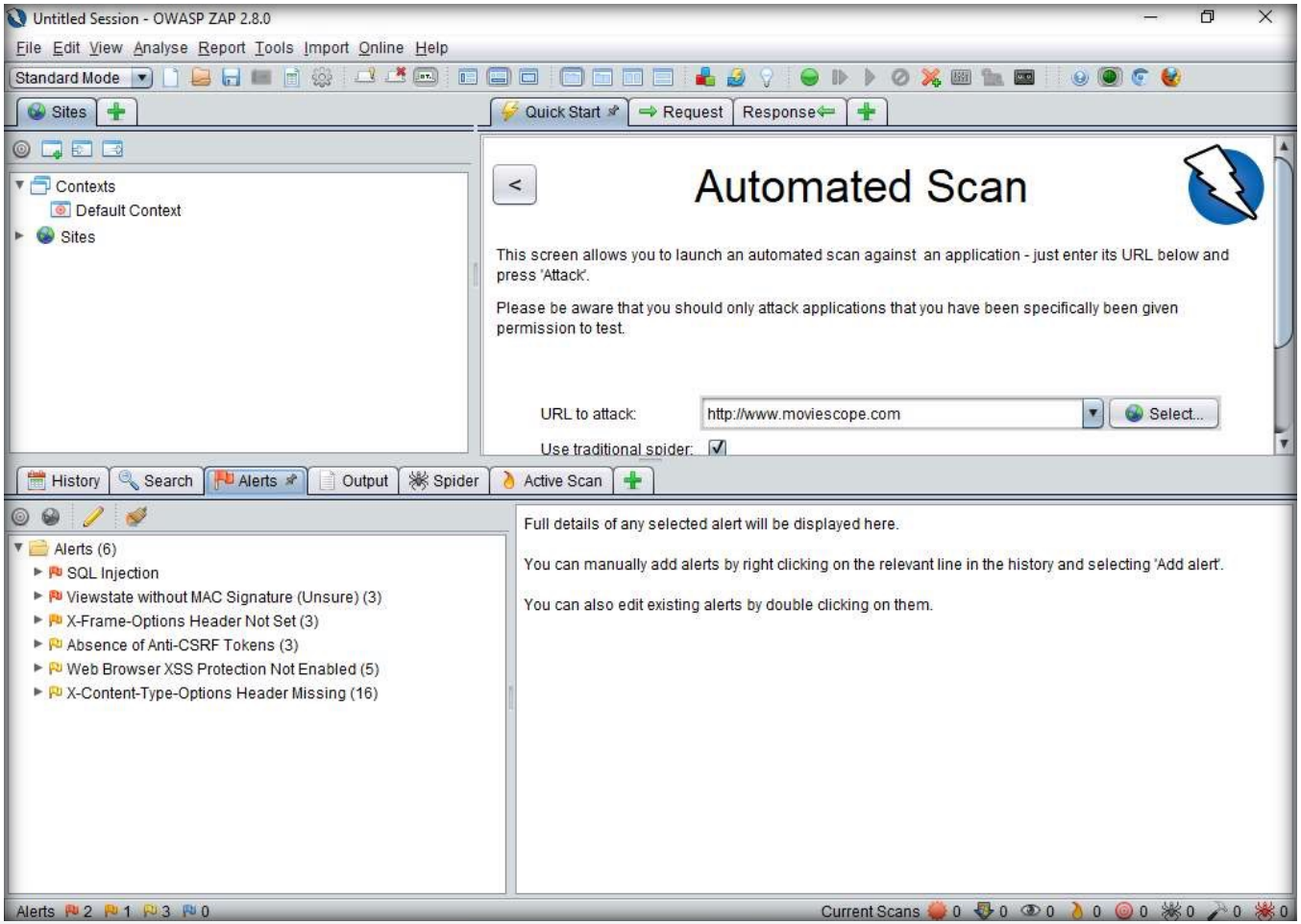
EXERCISE 4:
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



6. After the scan completes, Alerts tab appears, as shown in the screenshot below.

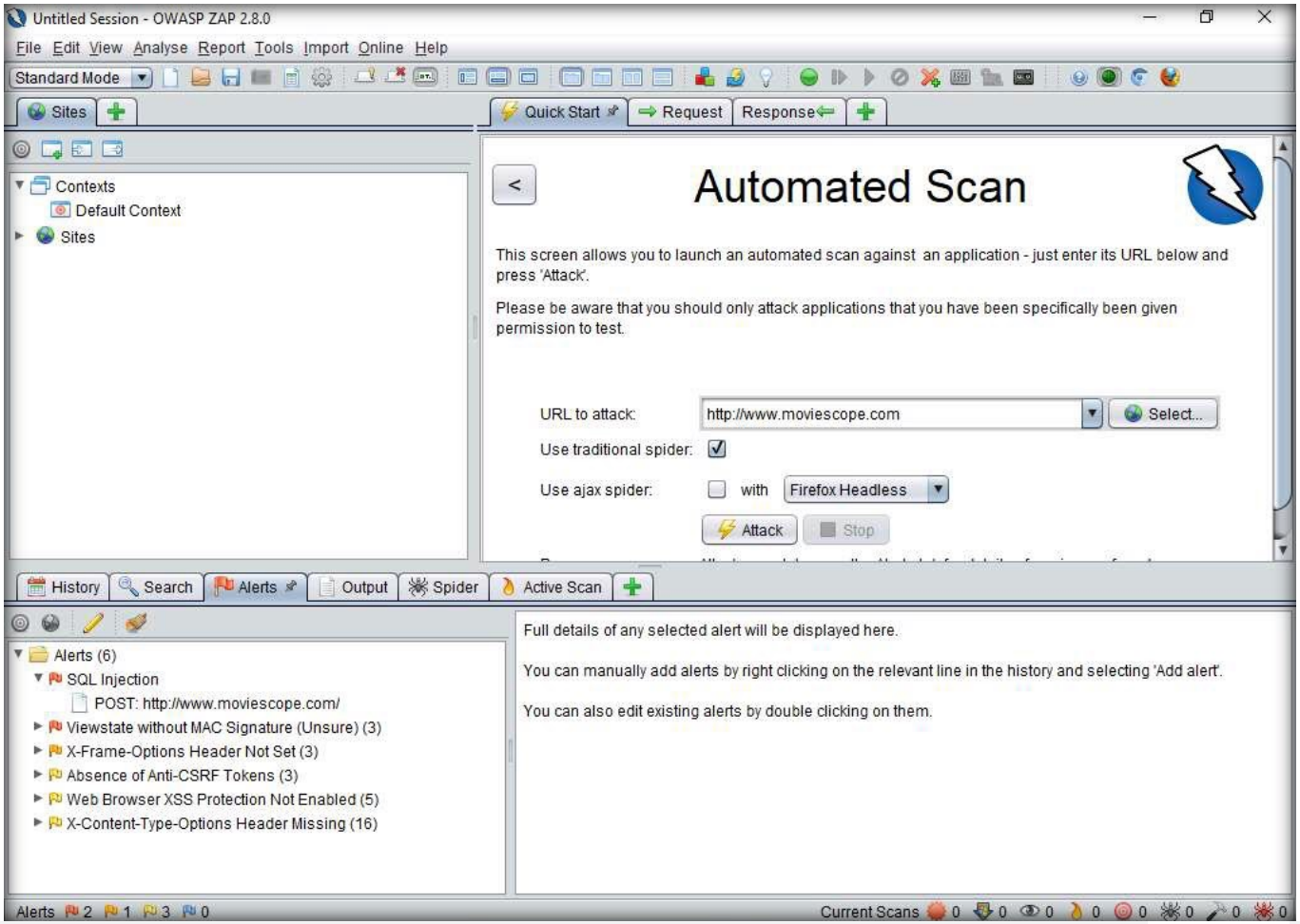
7. You can observe the vulnerabilities found on the website under the Alerts tab.

EXERCISE 4:
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



8. Now, expand any vulnerability (here, SQL Injection vulnerability) node under the Alerts tab.

EXERCISE 4:
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP

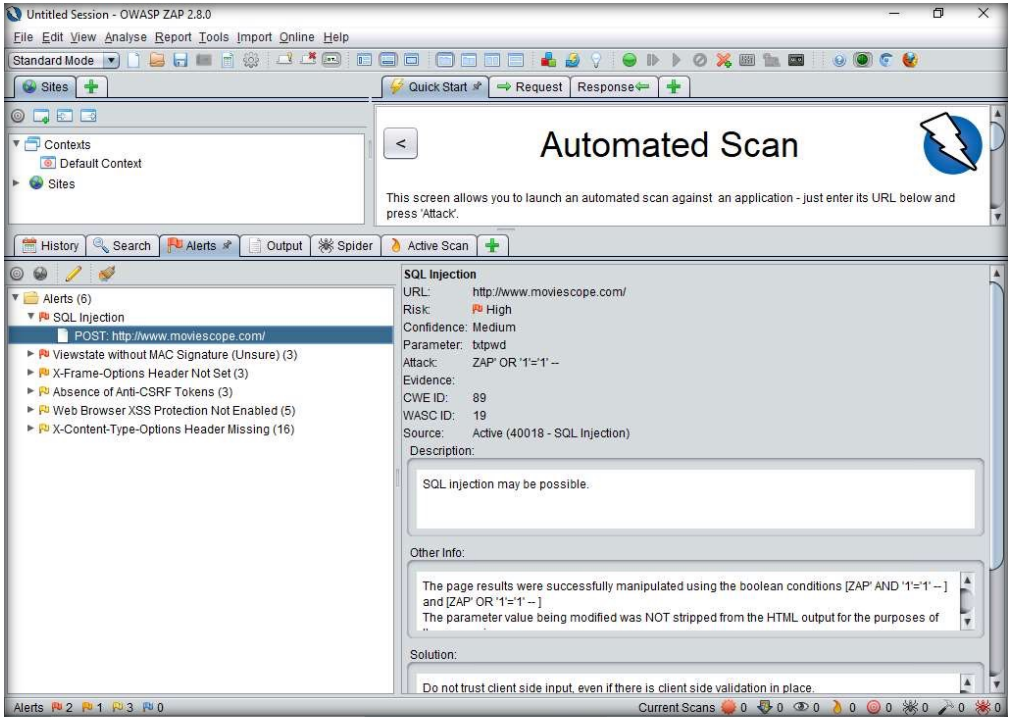


9. Click on the discovered SQL Injection vulnerability and further click on the vulnerable URL.
10. You can observe information such as Risk, Confidence, Parameter, Attack, etc., regarding the discovered SQL injection vulnerability in the lower right-area, as shown in the screenshot below.
Note: The risks associated with the vulnerability are categorized according to severity of risk as Low, Medium, High, and Informational alerts.

Each level of risk is represented by a different flag color:
• Red Flag: High risk • Orange Flag: Medium risk • Yellow Flag: Low risk • Blue Flag: Provides details about information disclosure vulnerabilities

11. Similarly, you can see other vulnerabilities discovered by the tool by clicking on them.
12. This concludes the demonstration showing how to detect web application vulnerabilities using OWASP ZAP.
13. Close all open windows and document all the acquired information.
14. Turn off the Admin Machine-1 virtual machine.

EXERCISE 4: DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



EXERCISE 5: **DETECT INJECTION VULNERABILITY USING BURP SUITE**

Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query.

LAB SCENARIO

A security professional must have the required knowledge to test various web application vulnerabilities such as injection vulnerability.

OBJECTIVE

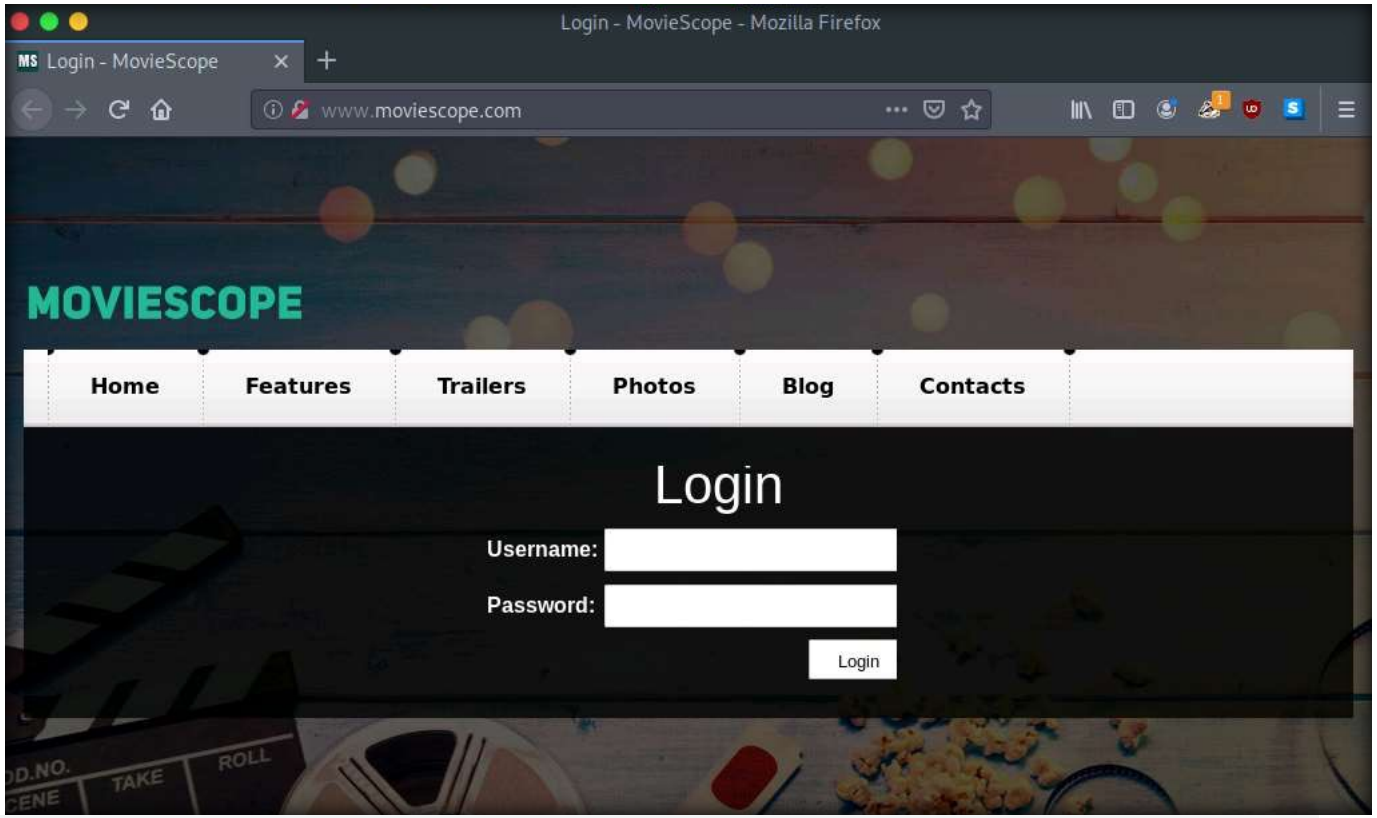
This lab will demonstrate how to test injection vulnerability using Burp Suite.

OVERVIEW OF WEB APPLICATION

Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access. Such flaws are prevalent in legacy code and often found in SQL, LDAP, and XPath queries. They can be easily discovered by application vulnerability scanners and fuzzers.
Attackers inject malicious code, commands, or scripts in the input gates of flawed web applications such that the applications interpret and run the newly supplied malicious input, which in turn allows them to extract sensitive information. By exploiting injection flaws in web applications, attackers can easily read, write, delete, and update any data (i.e., relevant or irrelevant to that particular application).

Note: Ensure that PfSense Firewall virtual machine is running.
Note: In this task, the target website (www.moviescope.com) is hosted by the victim machine, Web Server. Here, the host machine is the Attacker Machine-2 machine.
1. Turn on the Web Server and Attacker Machine-2 virtual machines.
2. In the Attacker Machine-2 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 Firefox icon from the top section of Desktop to launch the Mozilla Firefox browser.
4. The Mozilla Firefox window appears; type http://www.moviescope.com into the address bar and press Enter.

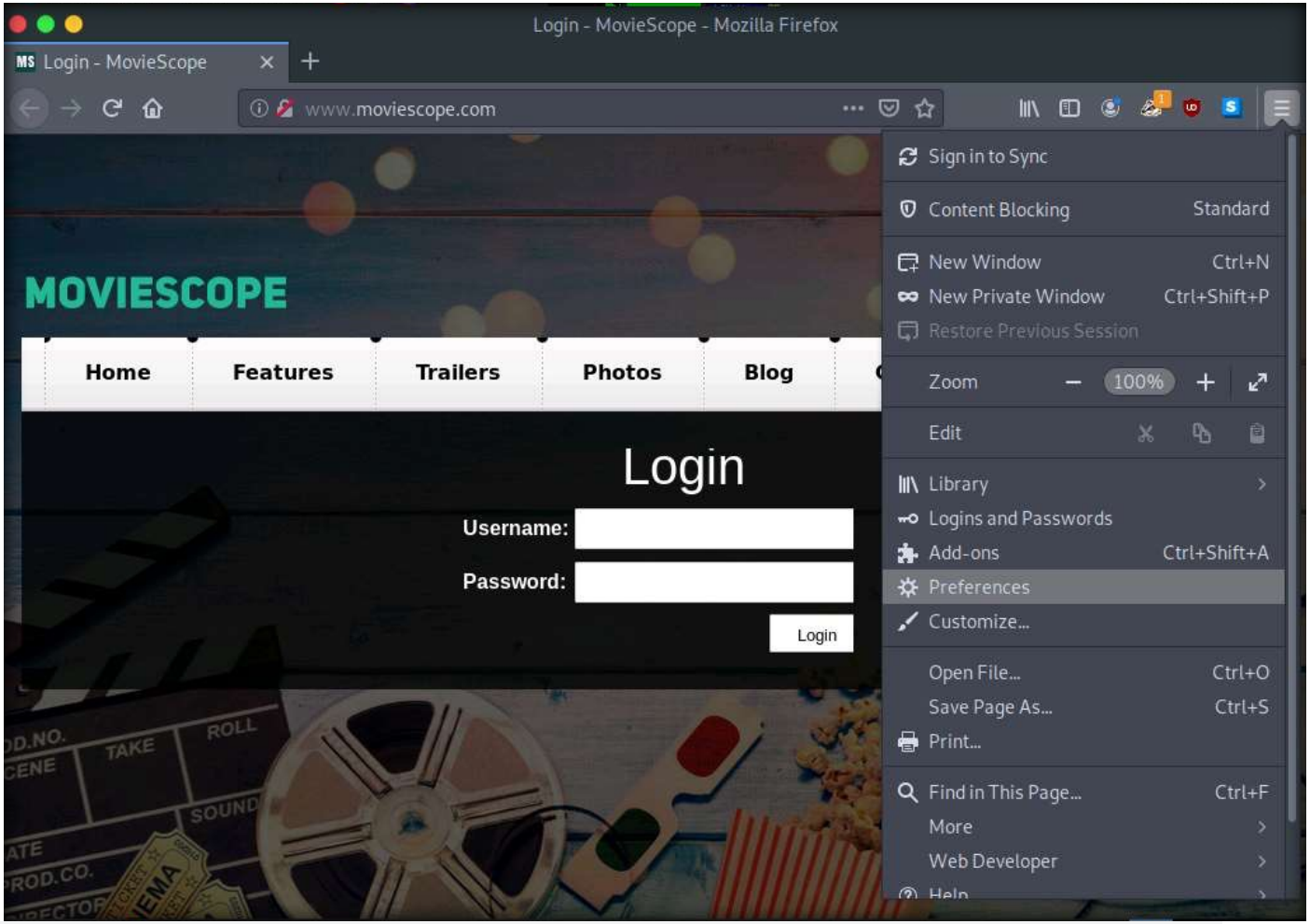
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



5. Now, set up a Burp Suite proxy by first configuring the proxy settings of the browser.

6. In the Mozilla Firefox browser, click the Open menu icon in the right corner of the menu bar and select Preferences from the list.

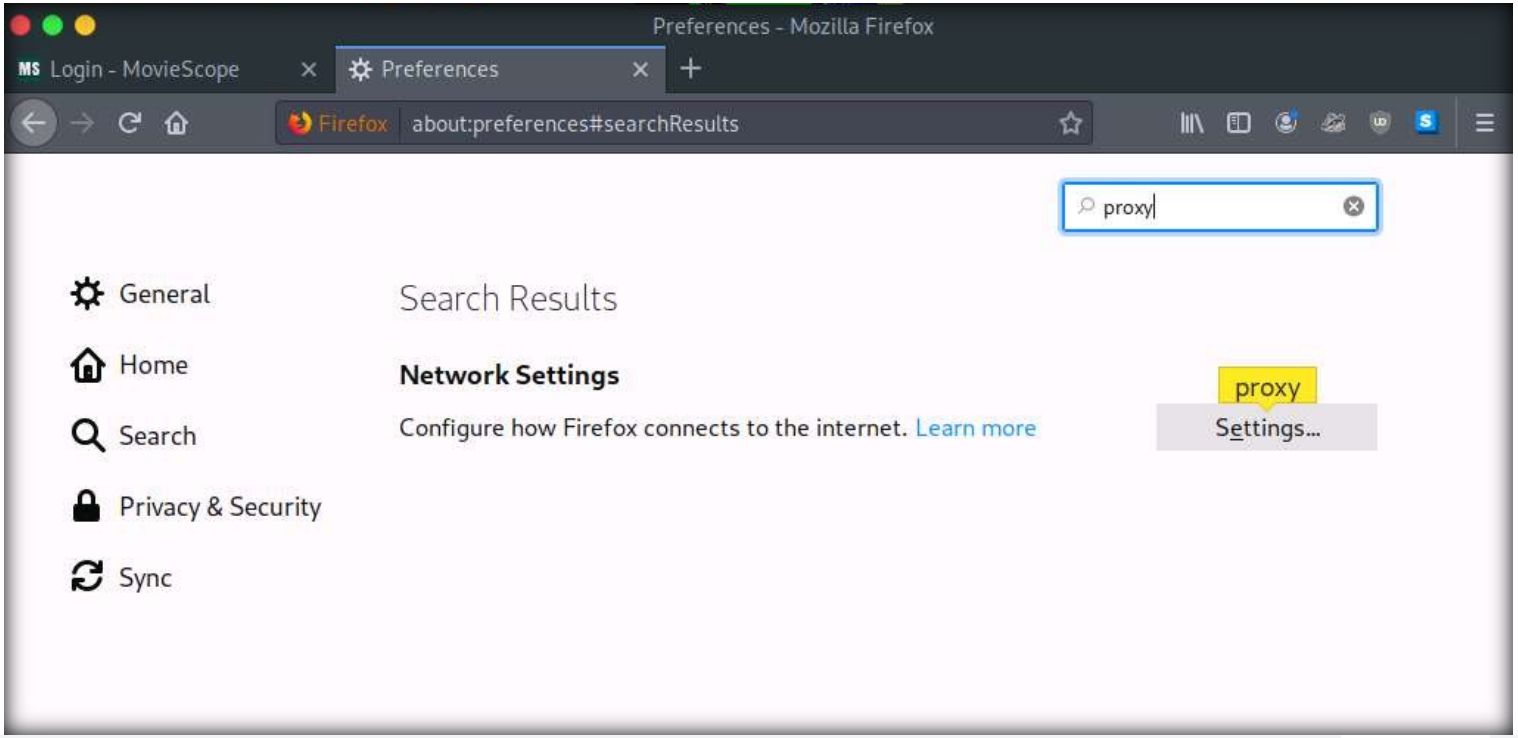
EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE



7. The General settings tab appears. In the Find in Preferences search bar, type proxy, and press Enter.

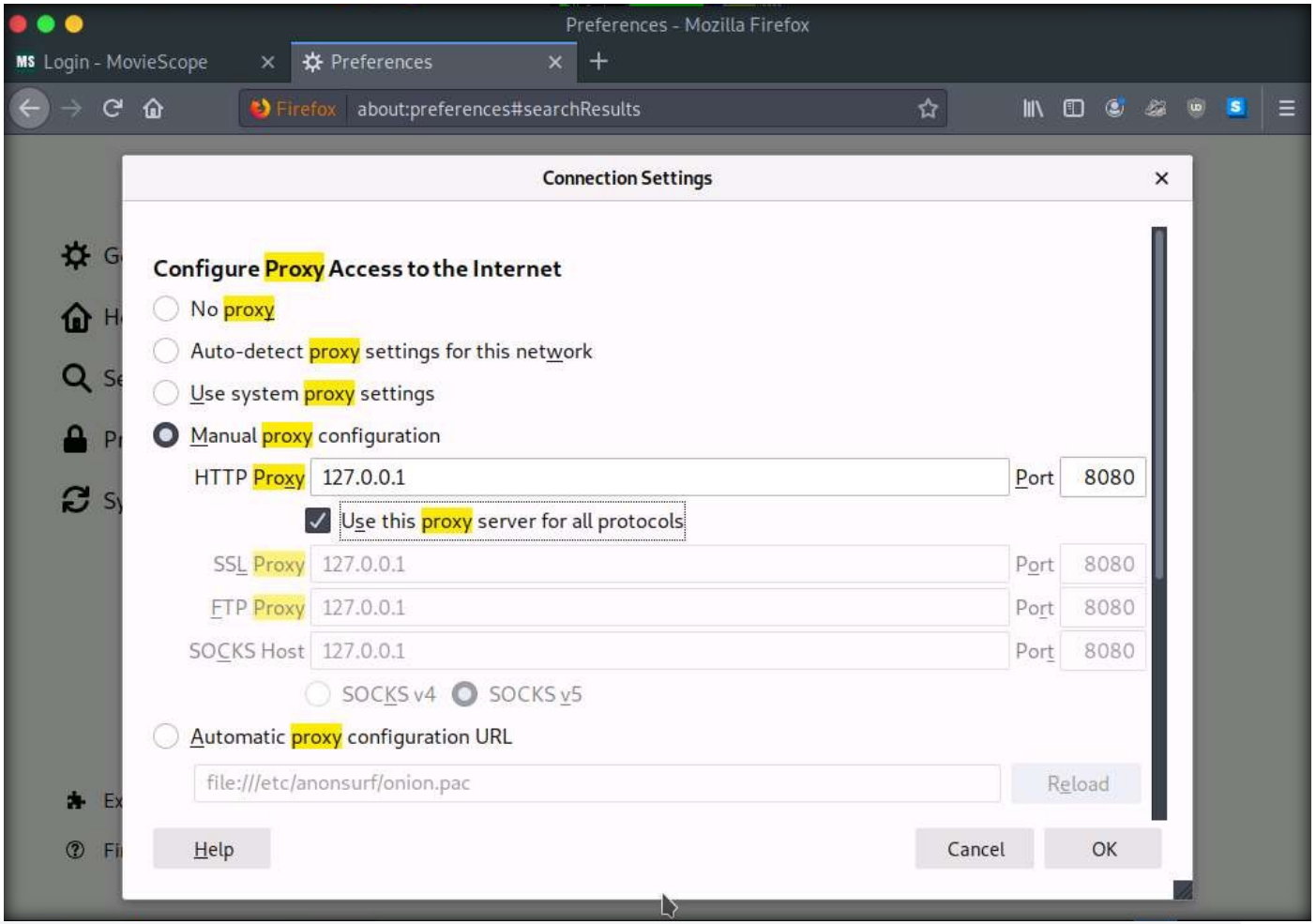
8. The Search Results appear. Click the Settings button under the Network Settings option.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



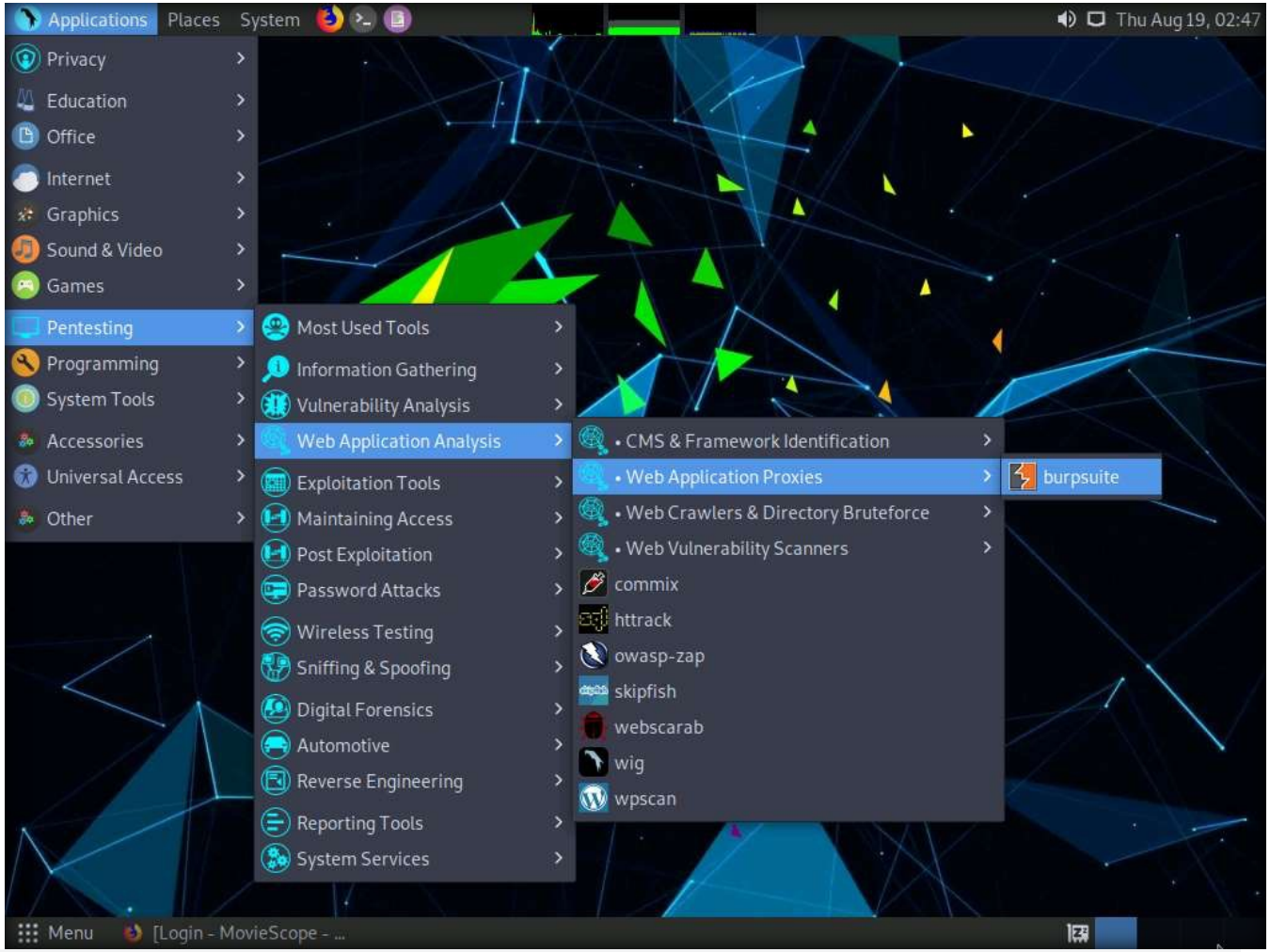
9. A Connection Settings window appears; select the Manual proxy configuration radio button and ensure that the HTTP Proxy is set to 127.0.0.1 and Port as 8080. Ensure that the Use this proxy server for all protocols checkbox is selected and click OK. Close the Preferences tab.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE

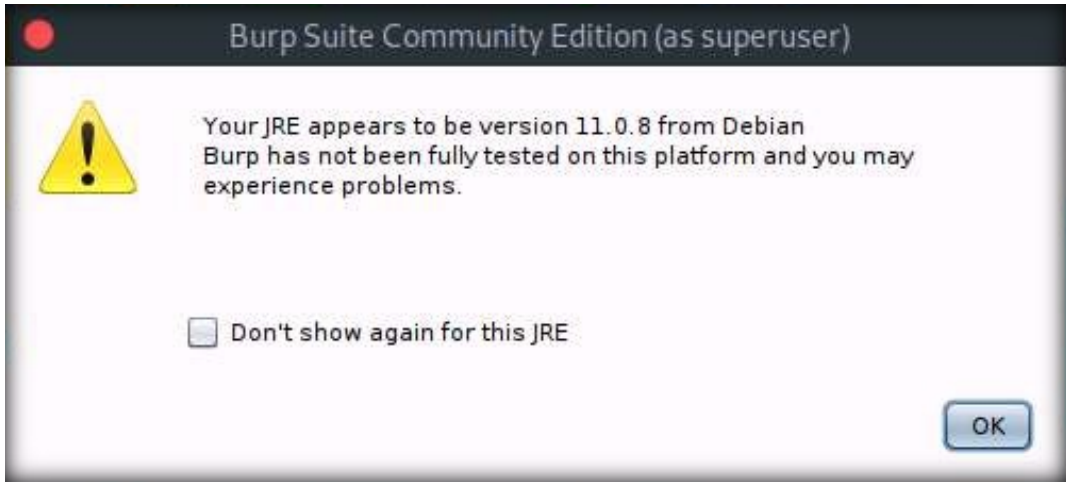
10. Now, minimize the browser window, click the Applications menu form the top left corner of Desktop, and navigate to Pentesting → Web Application Analysis → Web Application Proxies → burpsuite to launch the Burp Suite application.



11. A security pop-up appears, enter the password as toor in the Password field and click OK.

12. In the subsequent Burp Suite Community Edition notification, click OK.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



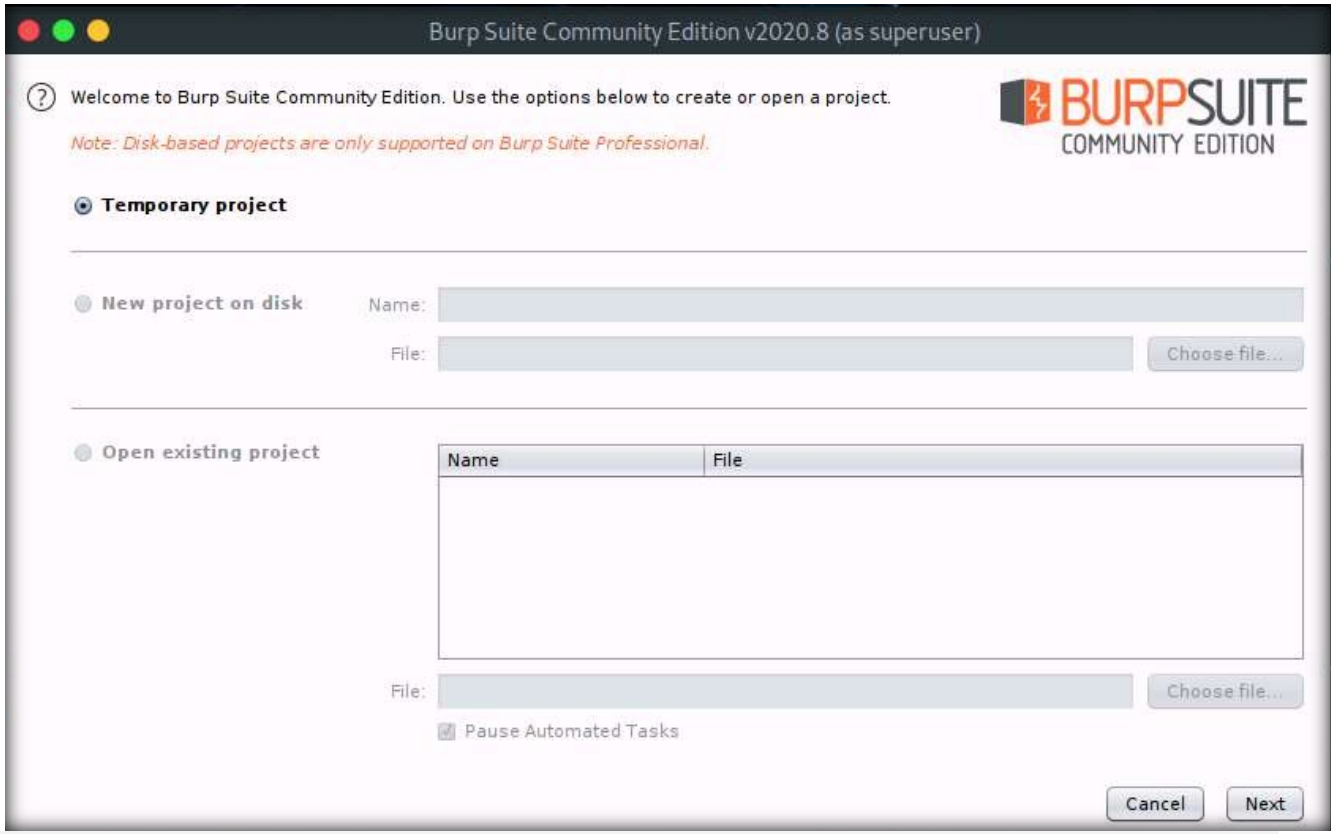
13. Burp Suite initializes. If a Burp Suite Community Edition notification saying An update is available appears, click Close.

Note: If a Terms and Conditions window appears click on I Accept.

14. The Burp Suite main window appears; ensure that the Temporary project radio button is selected and click the Next button, as shown in the screenshot below.

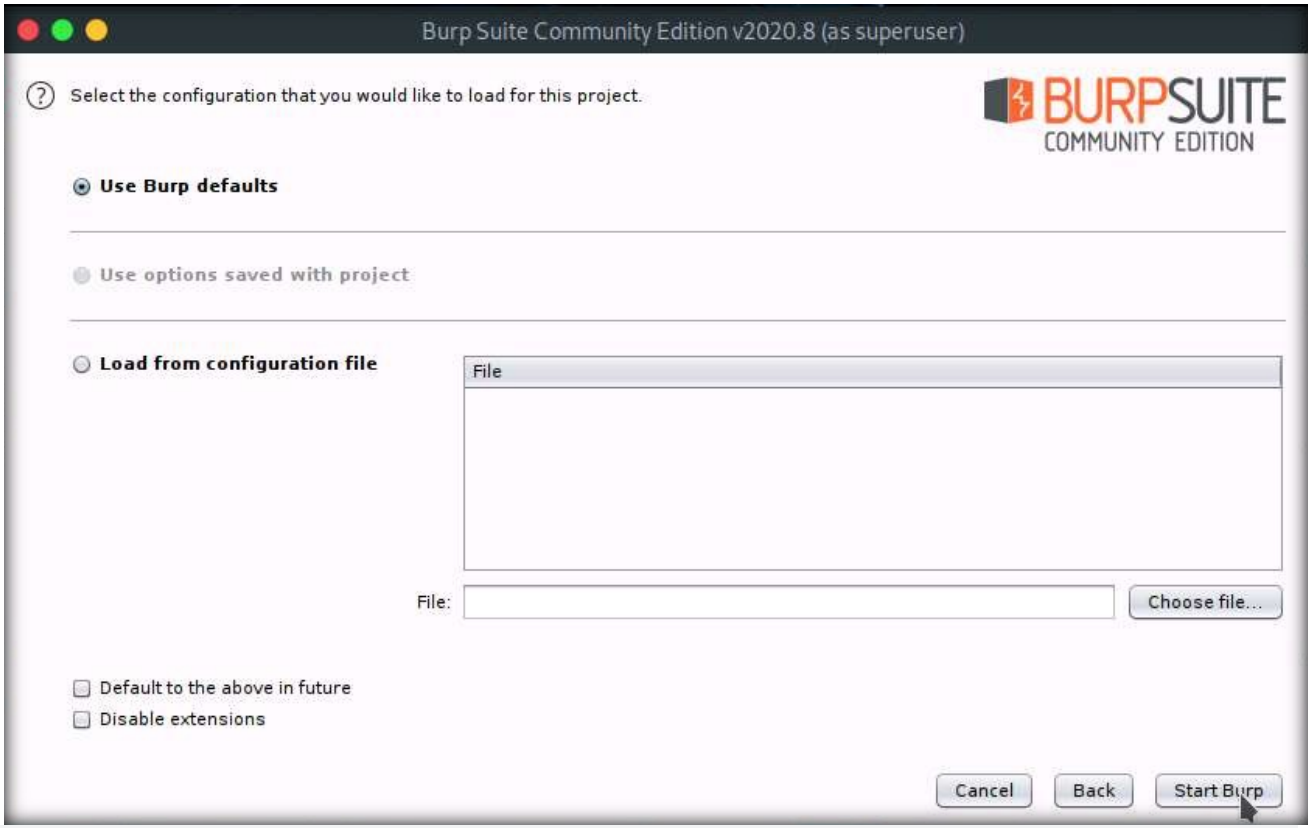
Note: If an update window appears, click Close.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



15. In the next window, select the Use Burp defaults radio-button and click the Start Burp button.

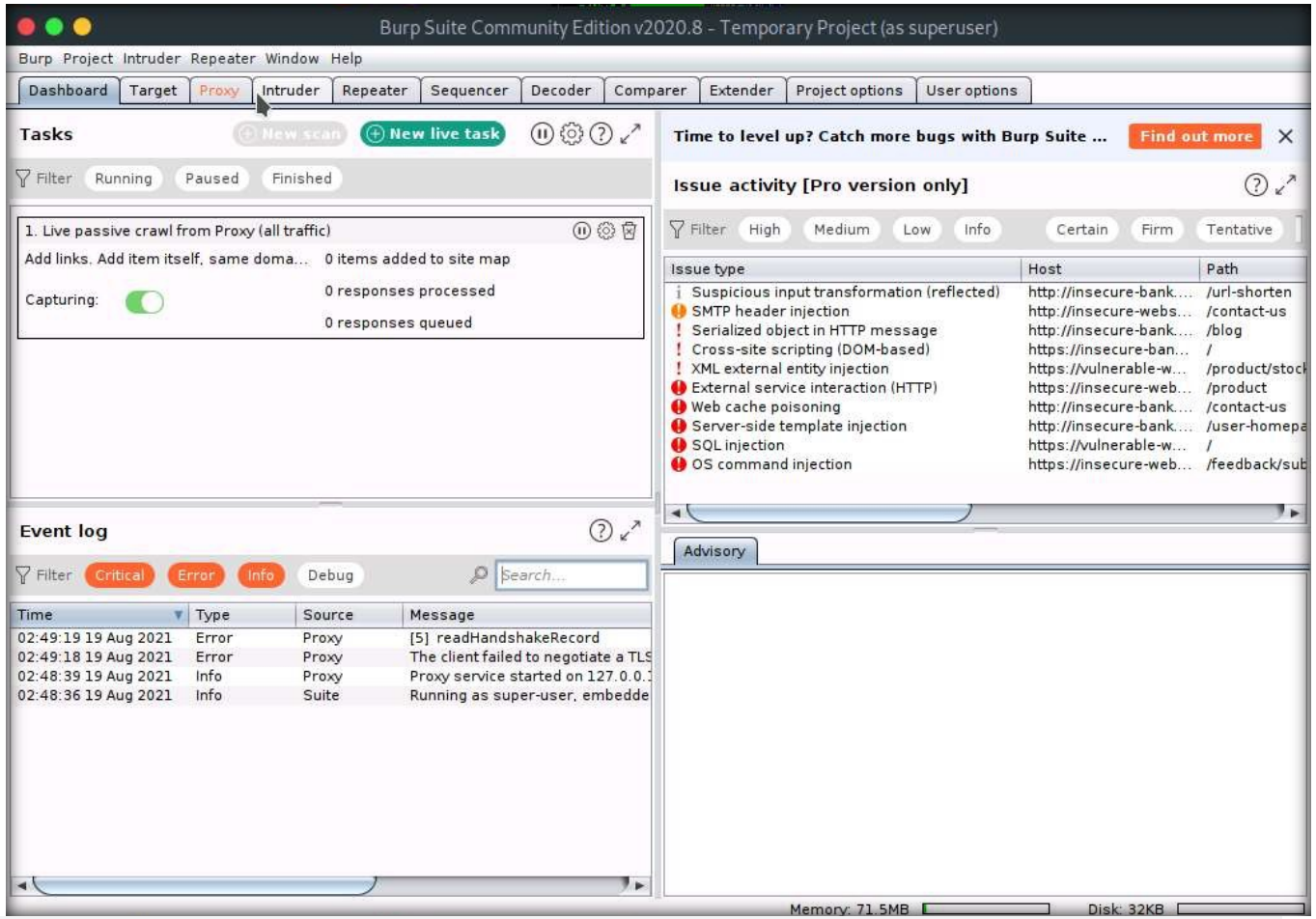
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



16. The Burp Suite main window appears; click the Proxy tab from the available options in the top section of the window.

Note: In the right-pane of the tool window, you can observe the vulnerabilities in the target website that have been detected by the tool under Issue activity. You can click on each vulnerability to explore them one-by-one.

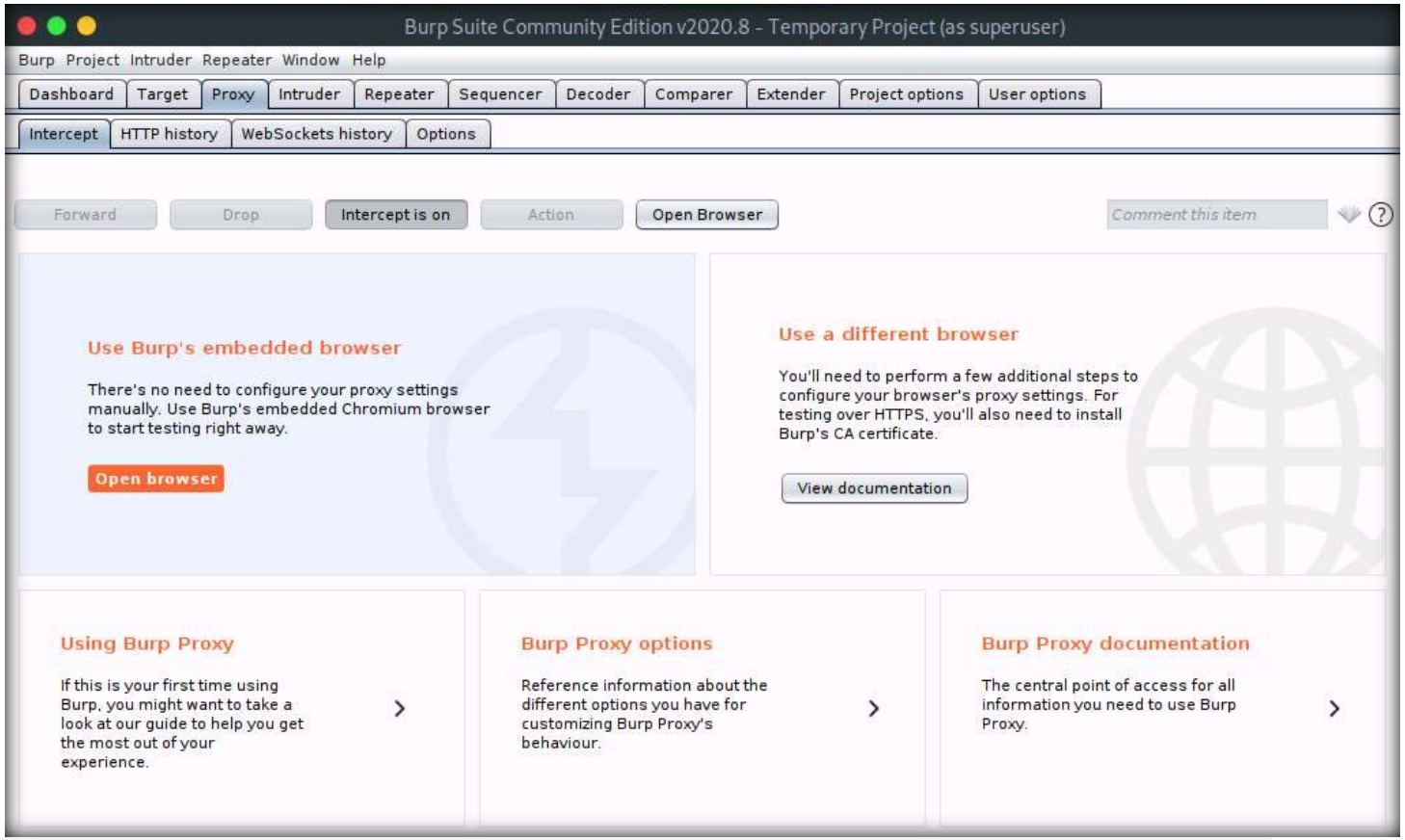
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



17. In the Proxy settings, by default, the Intercept tab opens-up. Observe that by default, the interception is active as the button says Intercept is on. Leave it running.

Note: Turn the interception on if it is off.

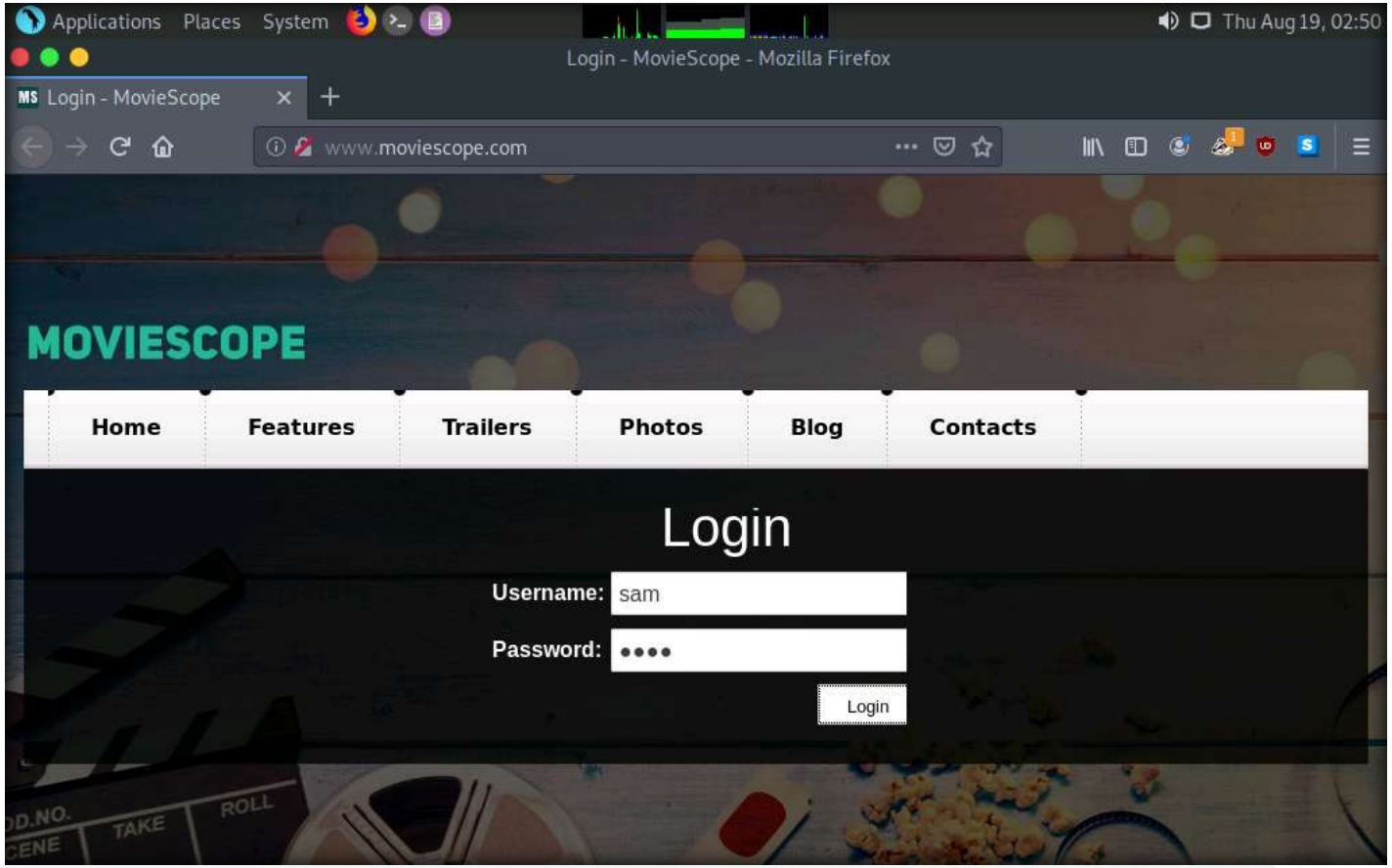
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



18. Switch back to the browser window, and on the login page of the target website (www.moviescope.com), enter the credentials sam and test. Click the Log In button.

Note: Here, we are logging in as a registered user on the website.

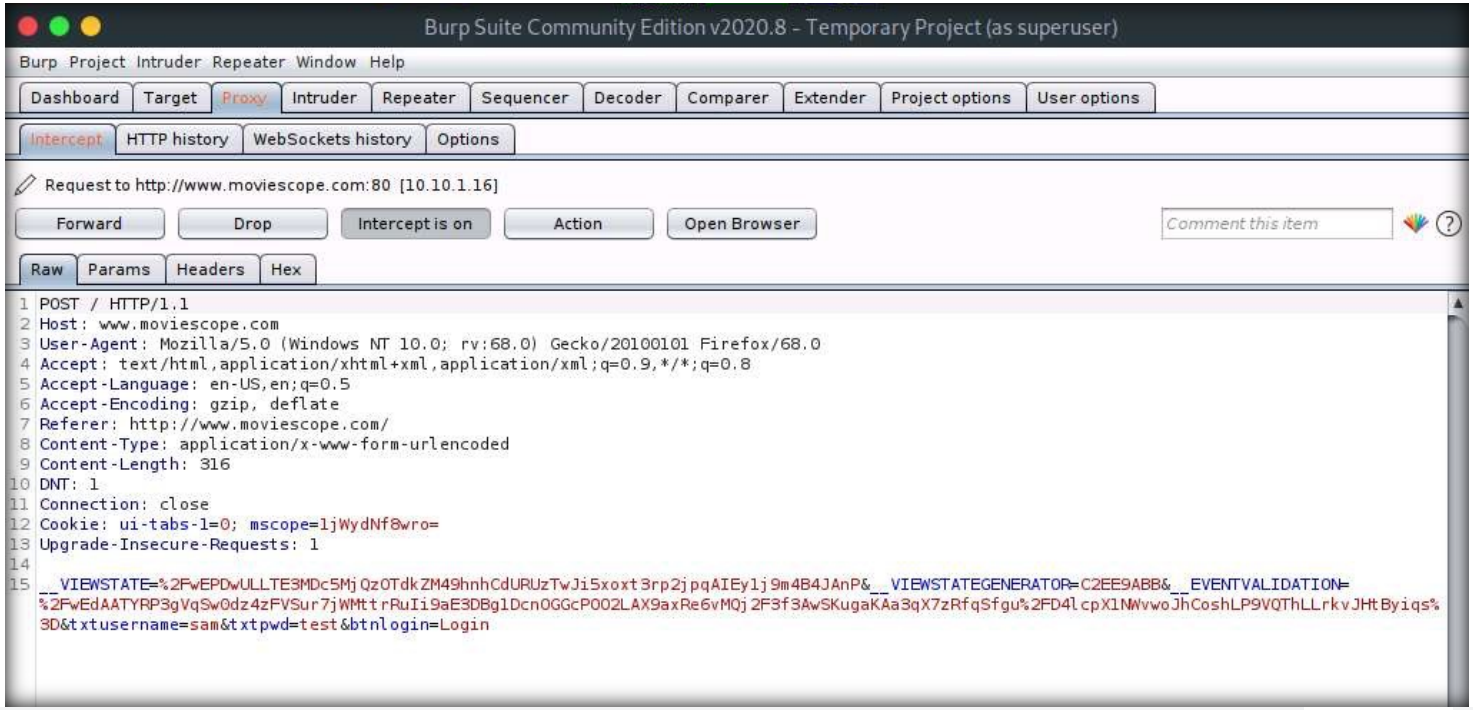
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



19. Switch back to the Burp Suite window and you can observe that a POST request of moviescope website and login credentials is captured.

Note: If you do not see the request as shown in the screenshot below, then click Forward button until to capture it.

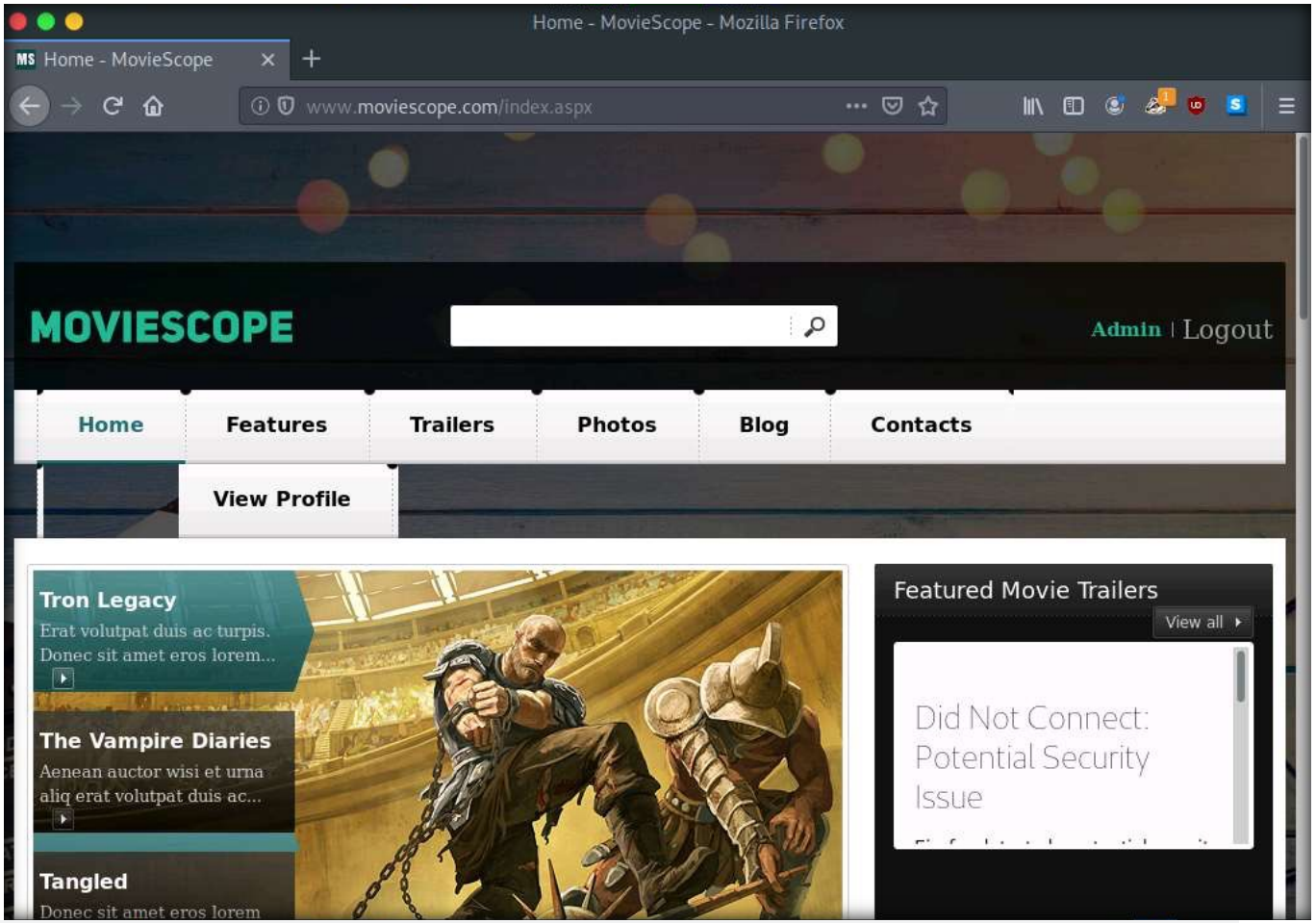
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



20. Now, keep clicking the Forward button until you are logged into the user account.

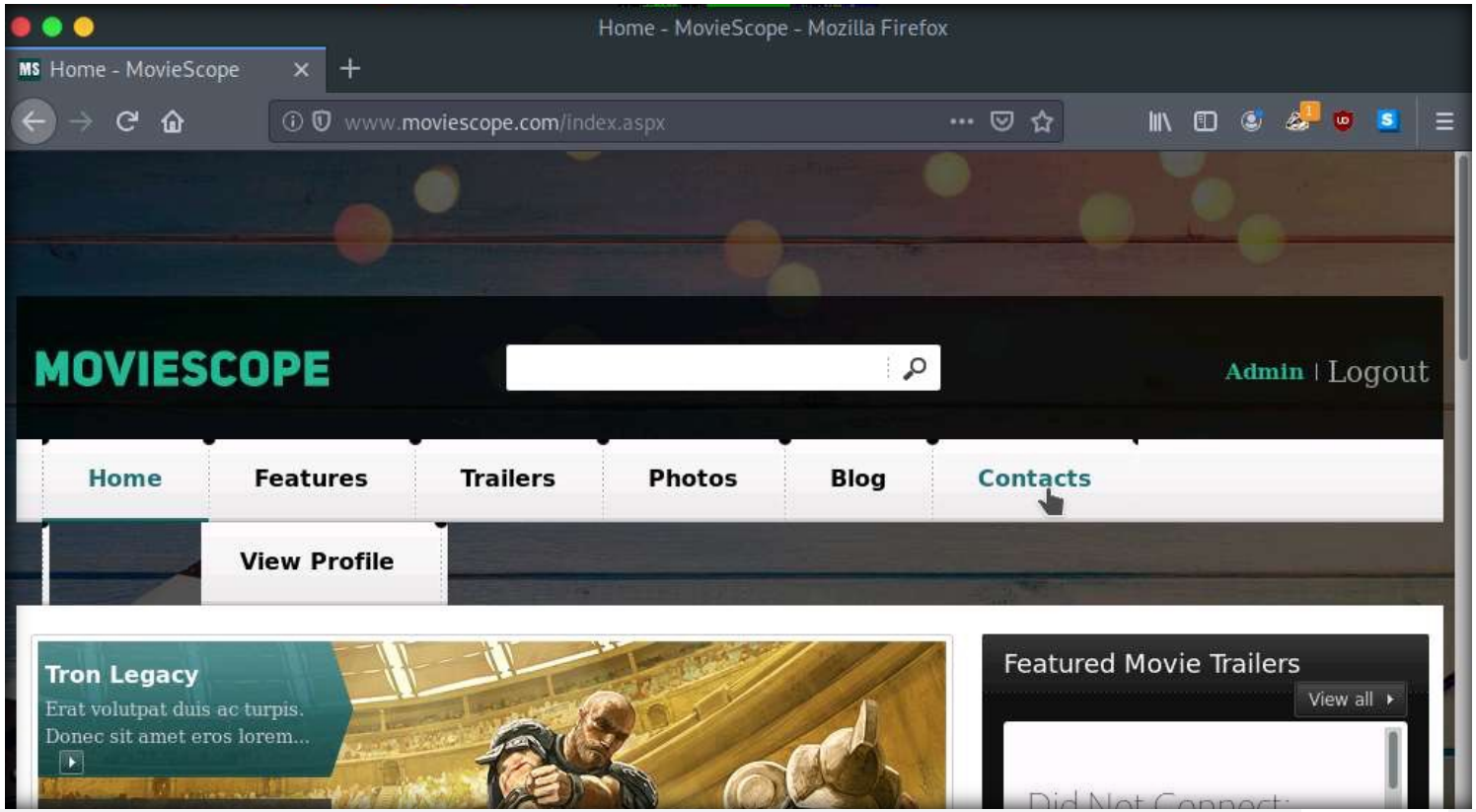
21. Switch to the browser and observe that you are now logged into the user account, as shown in the screenshot below.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



22. Now, click the Contacts tab from the menu bar to view the user information.

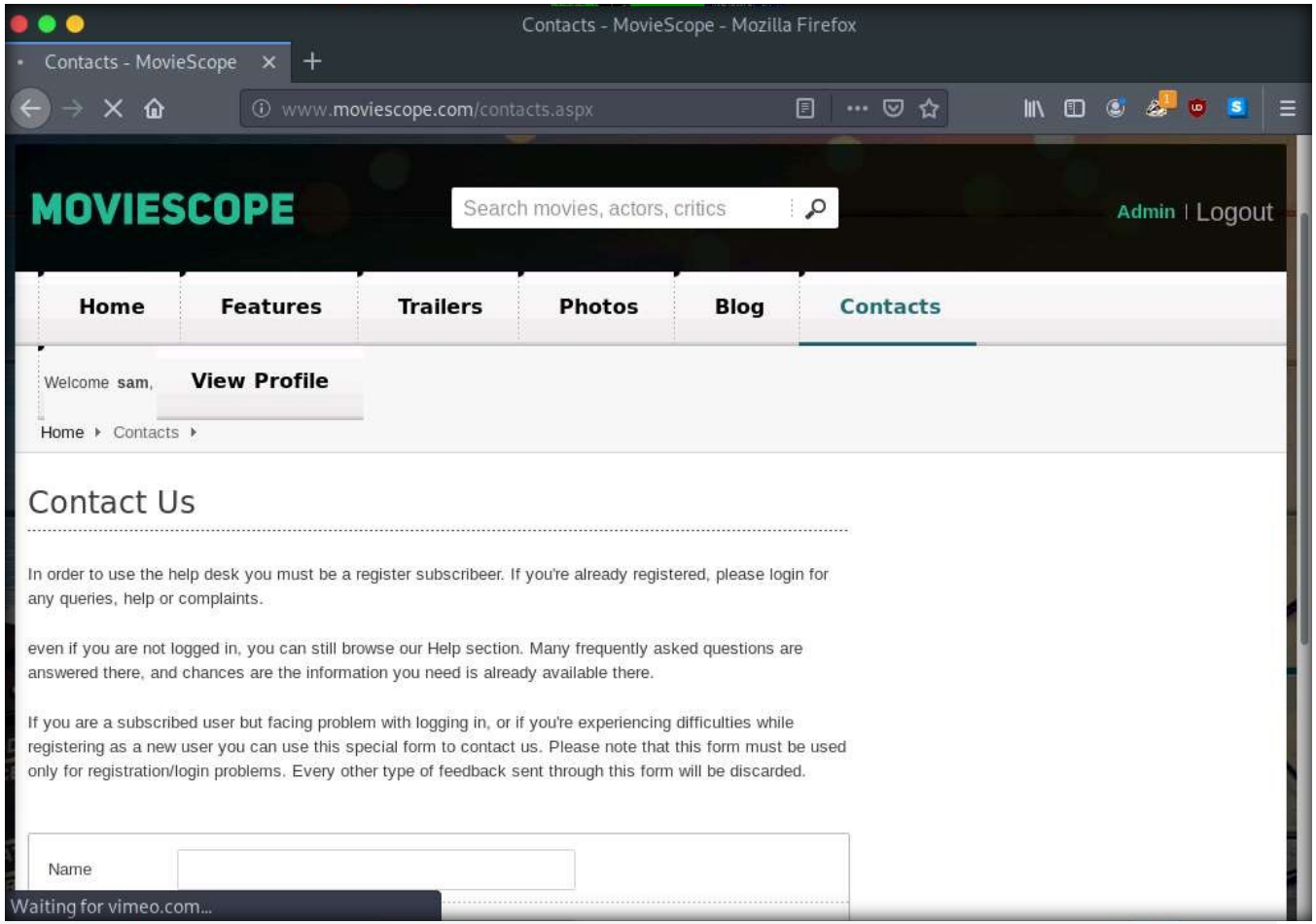
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



23. After clicking the Contacts tab, switch back to the Burp Suite window and keep clicking the Forward button until you get the HTTP request.

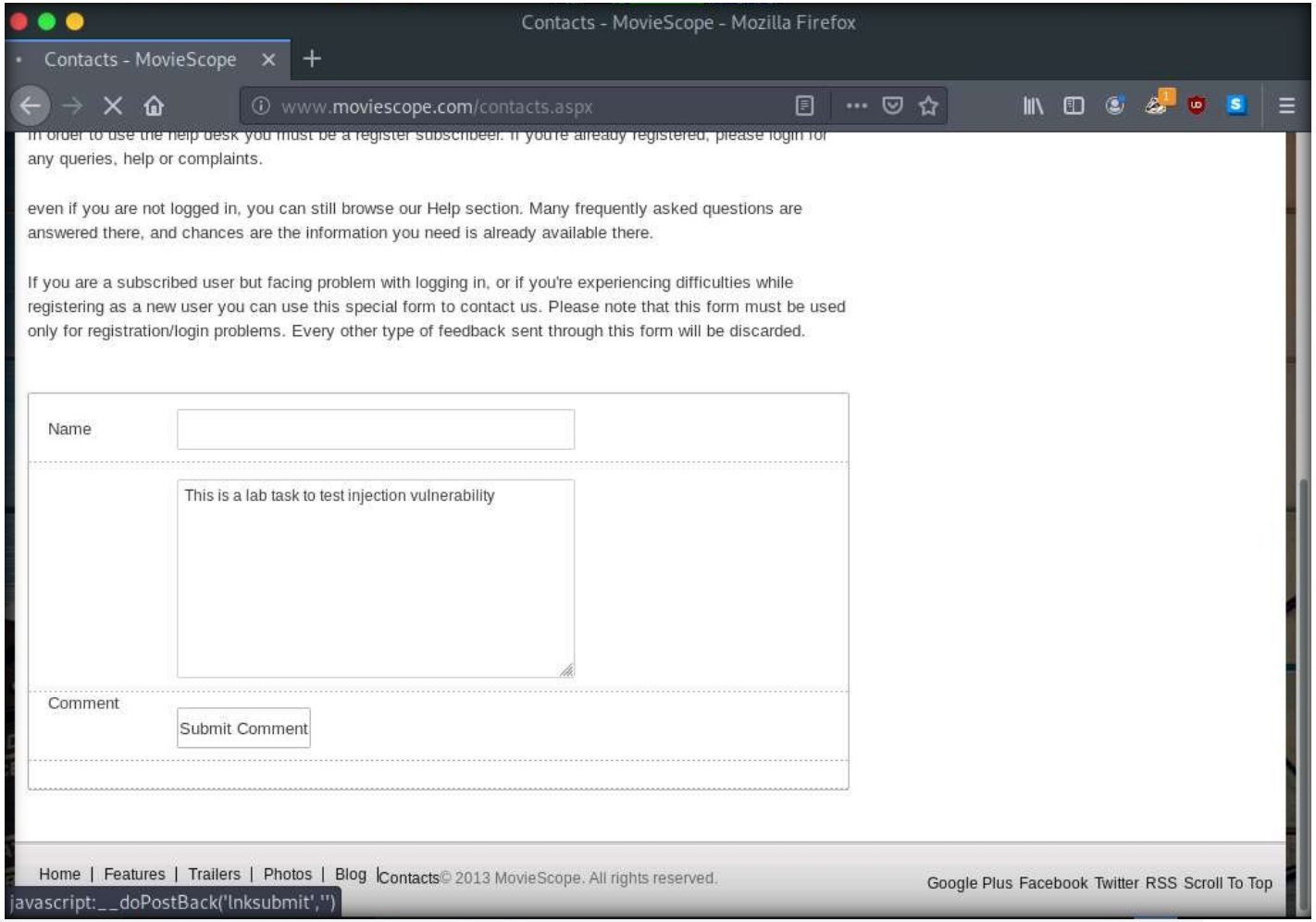
24. Switch to the browser, and observe that the Contacts tab appears, as shown in the screenshot below.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



25. Now, scroll-down and in the Comment field, type any random text (here, This is a lab task to test injection vulnerability); then, click Submit Comment button.

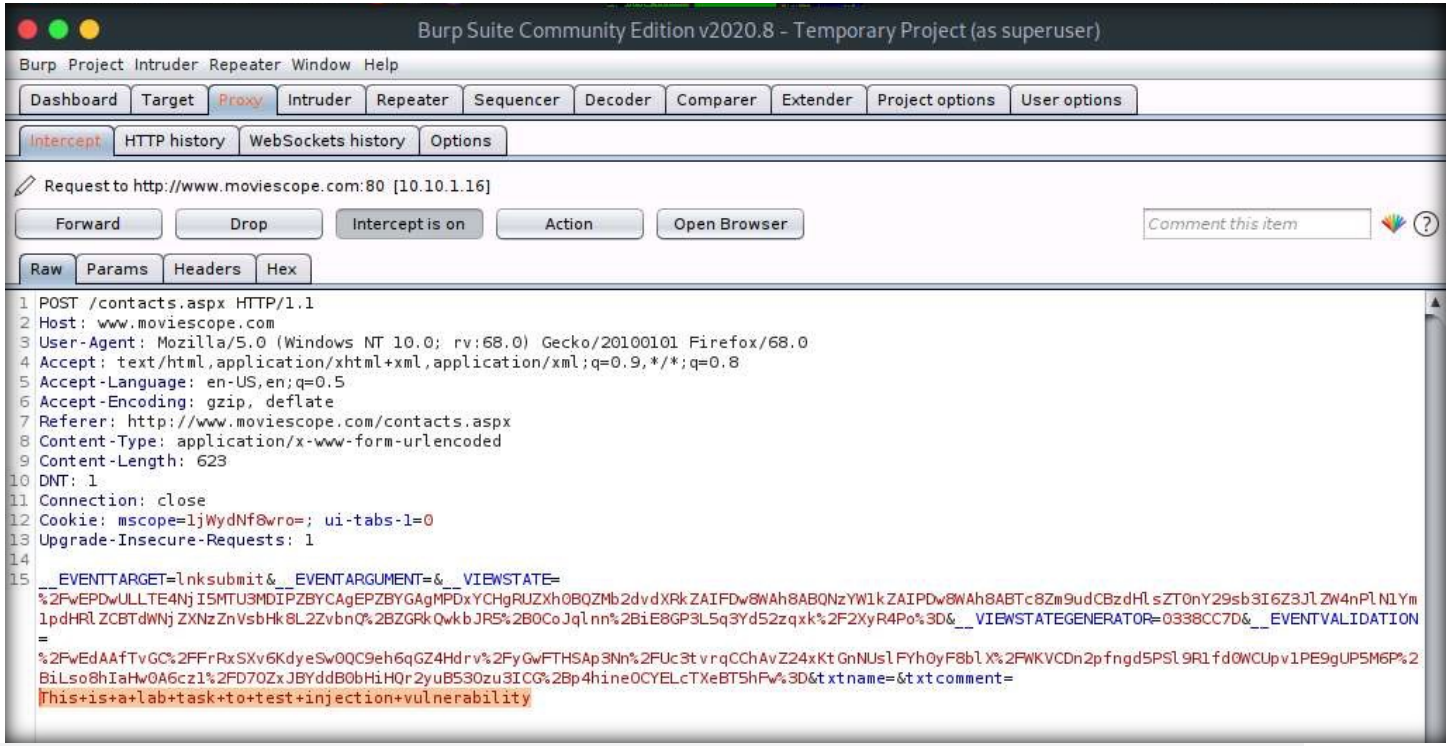
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



26. Switch back to the Burp Suite window and you can observe that a POST request has been captured and the comment is displayed in a plain text, as shown in the screenshot below.

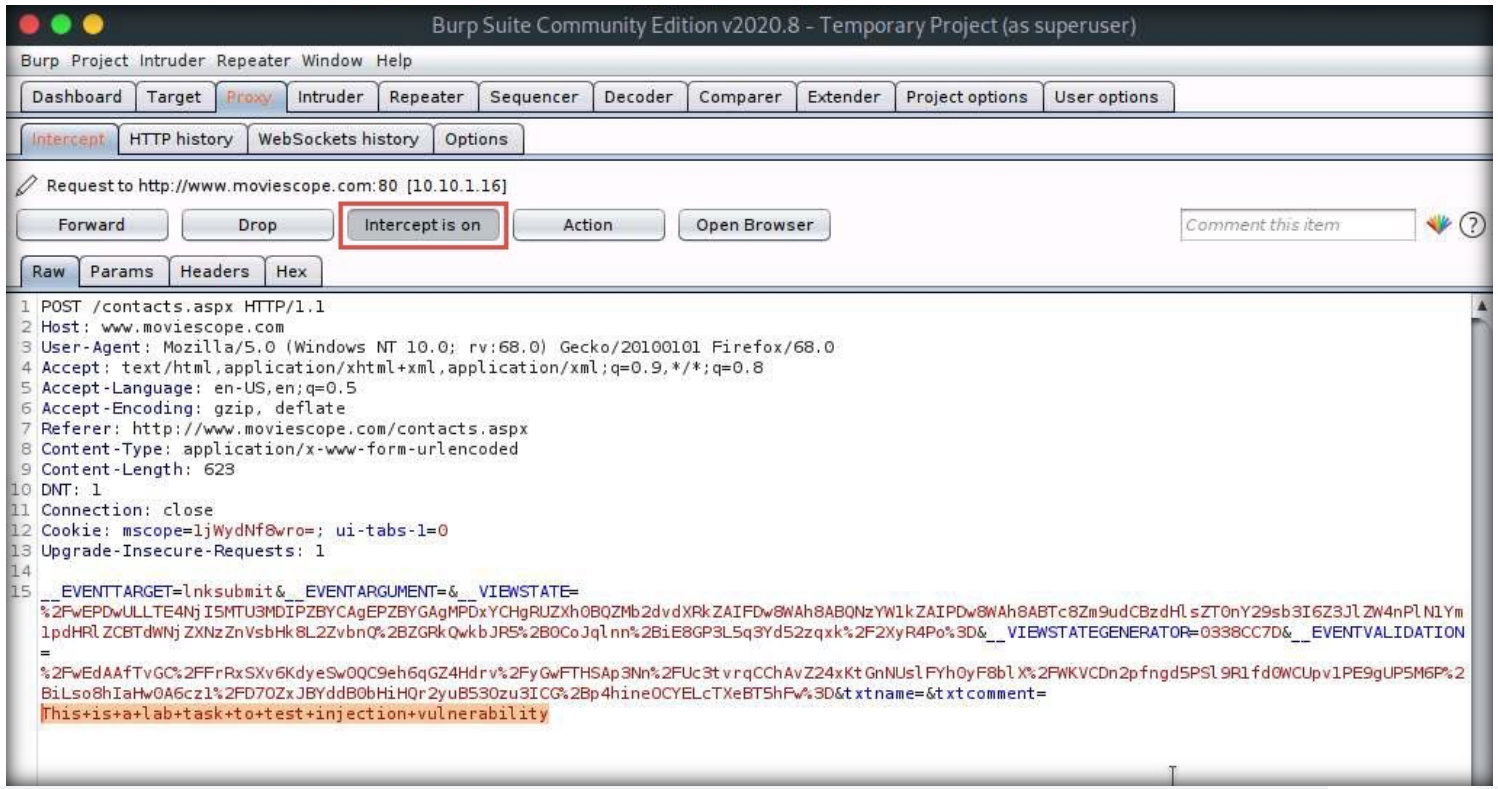
Note: If you do not see the request as shown in the screenshot below, then click Forward button until to capture it.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



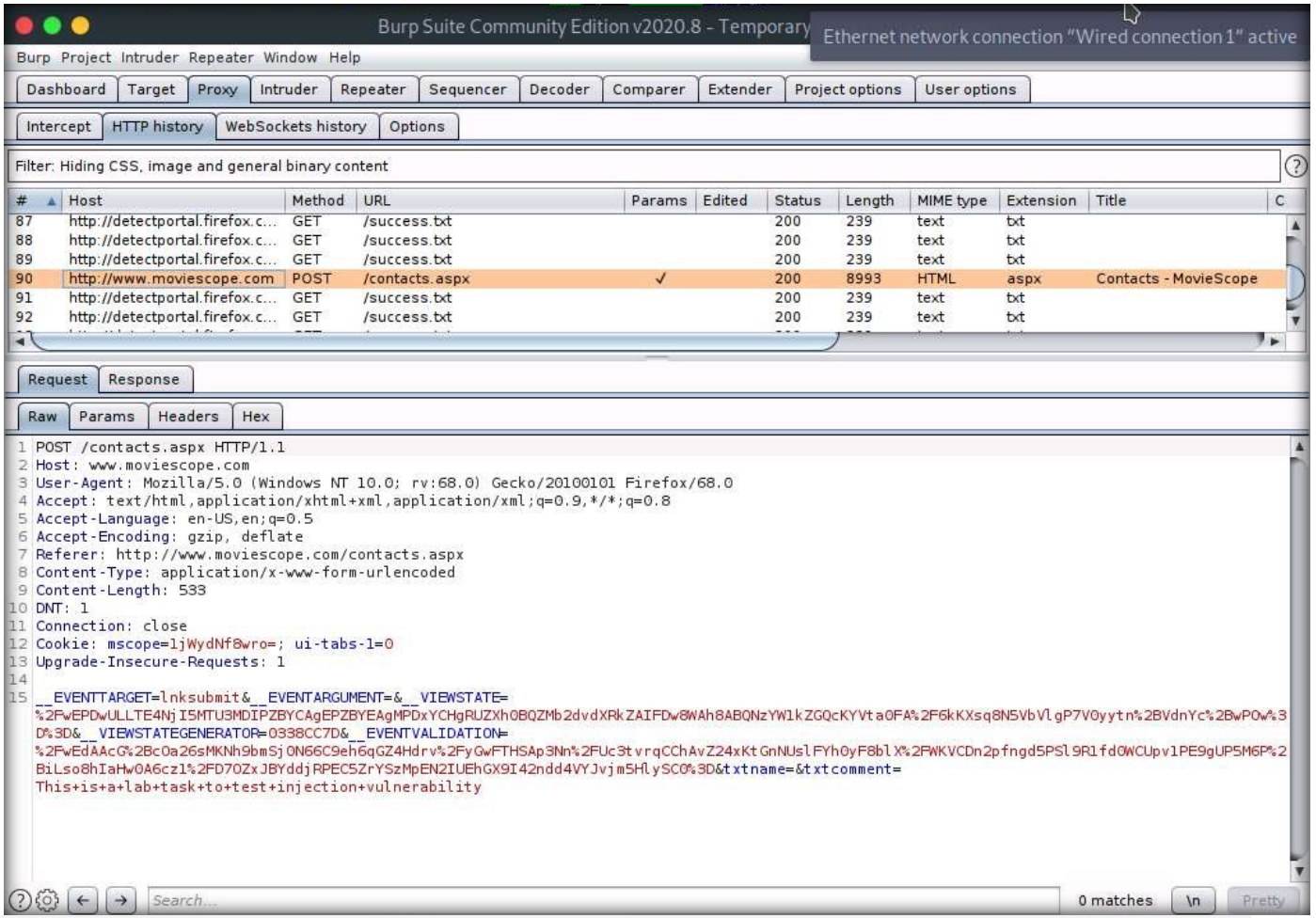
27. Click the Intercept is On button to switch it off.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



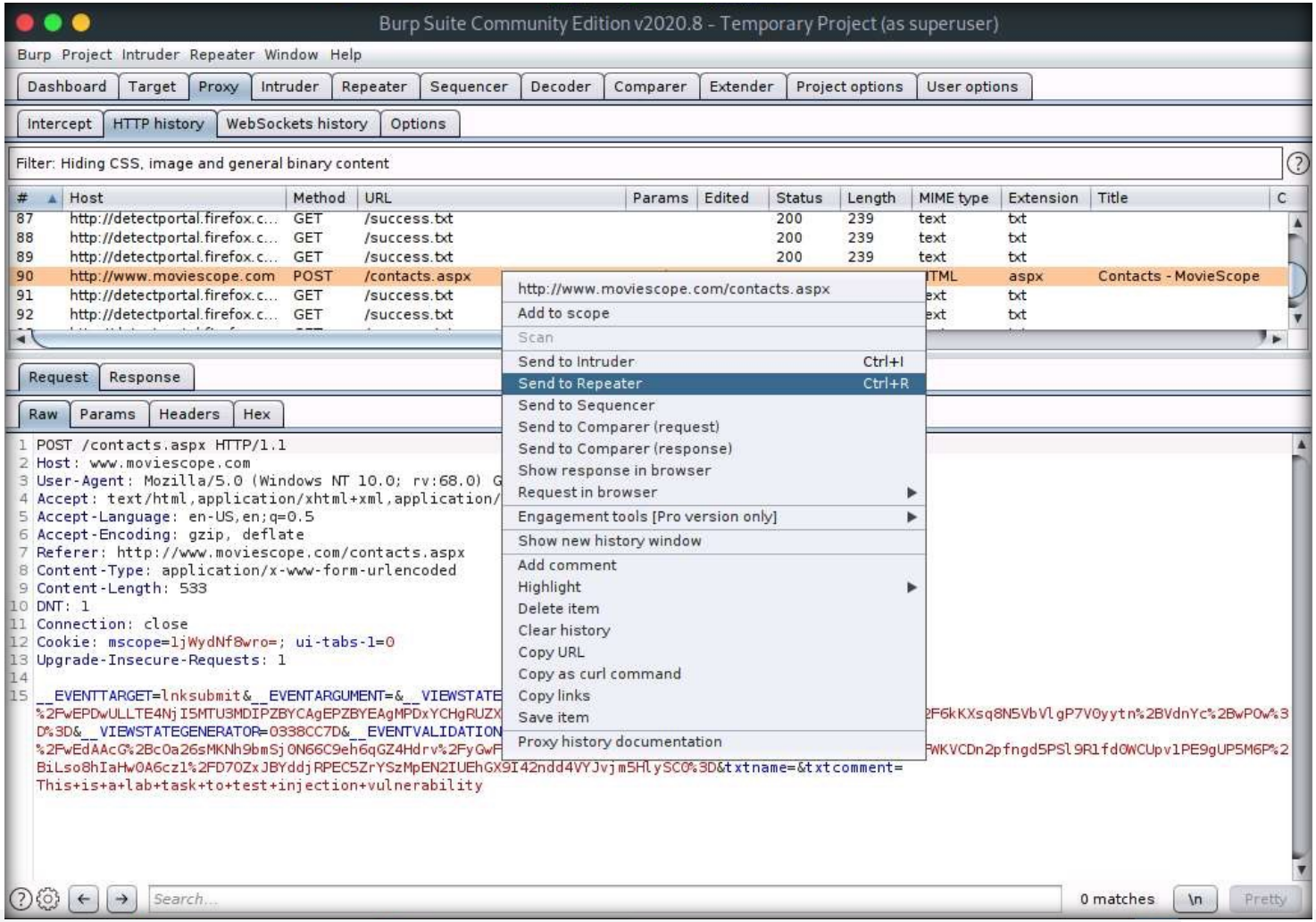
28. In the Burp Suite window, navigate to the HTTP history tab and locate POST request with /contacts.aspx in the URL column, as shown in the screenshot below.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



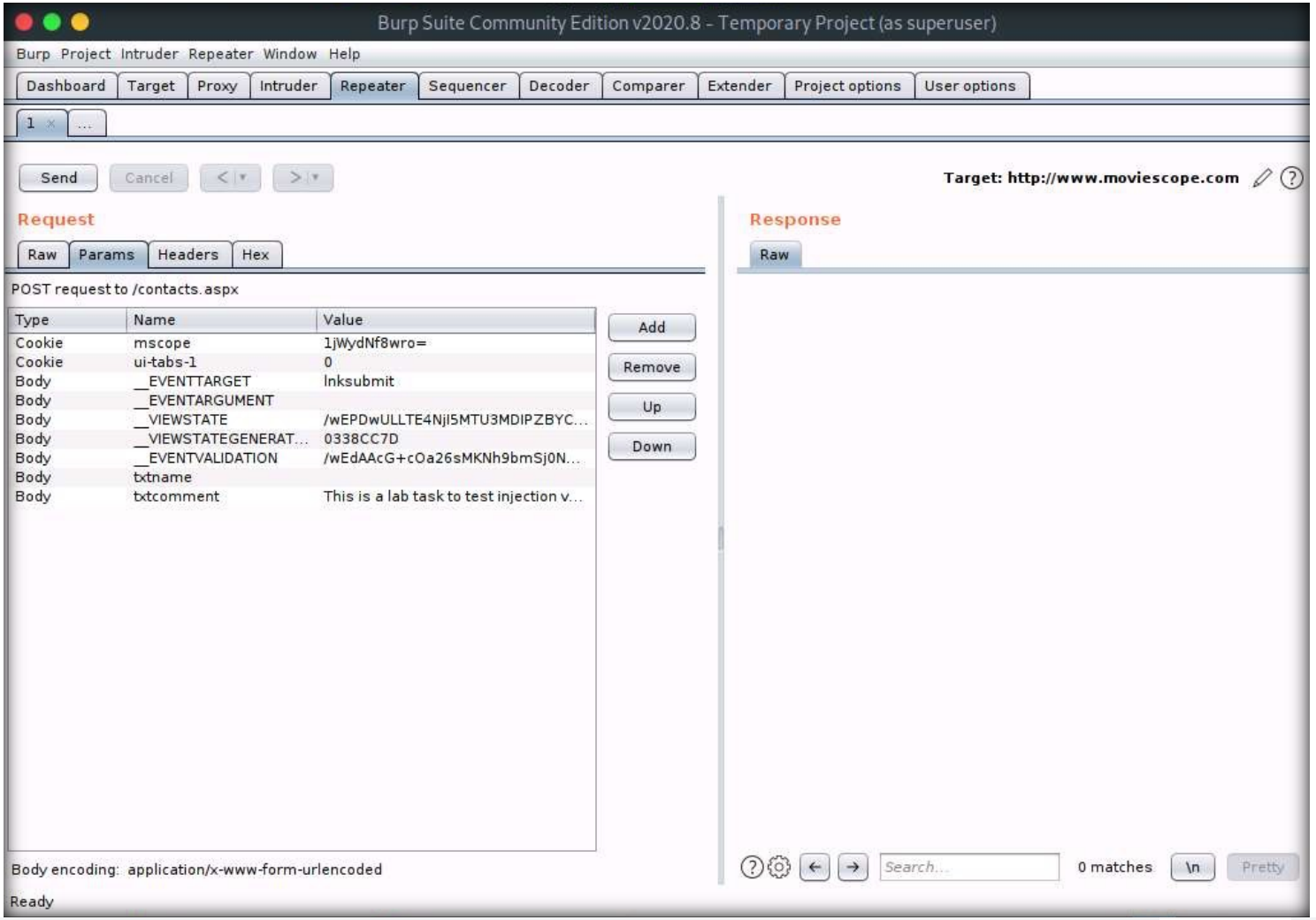
29. Right-click on the POST request and select Send to Repeater.

EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE



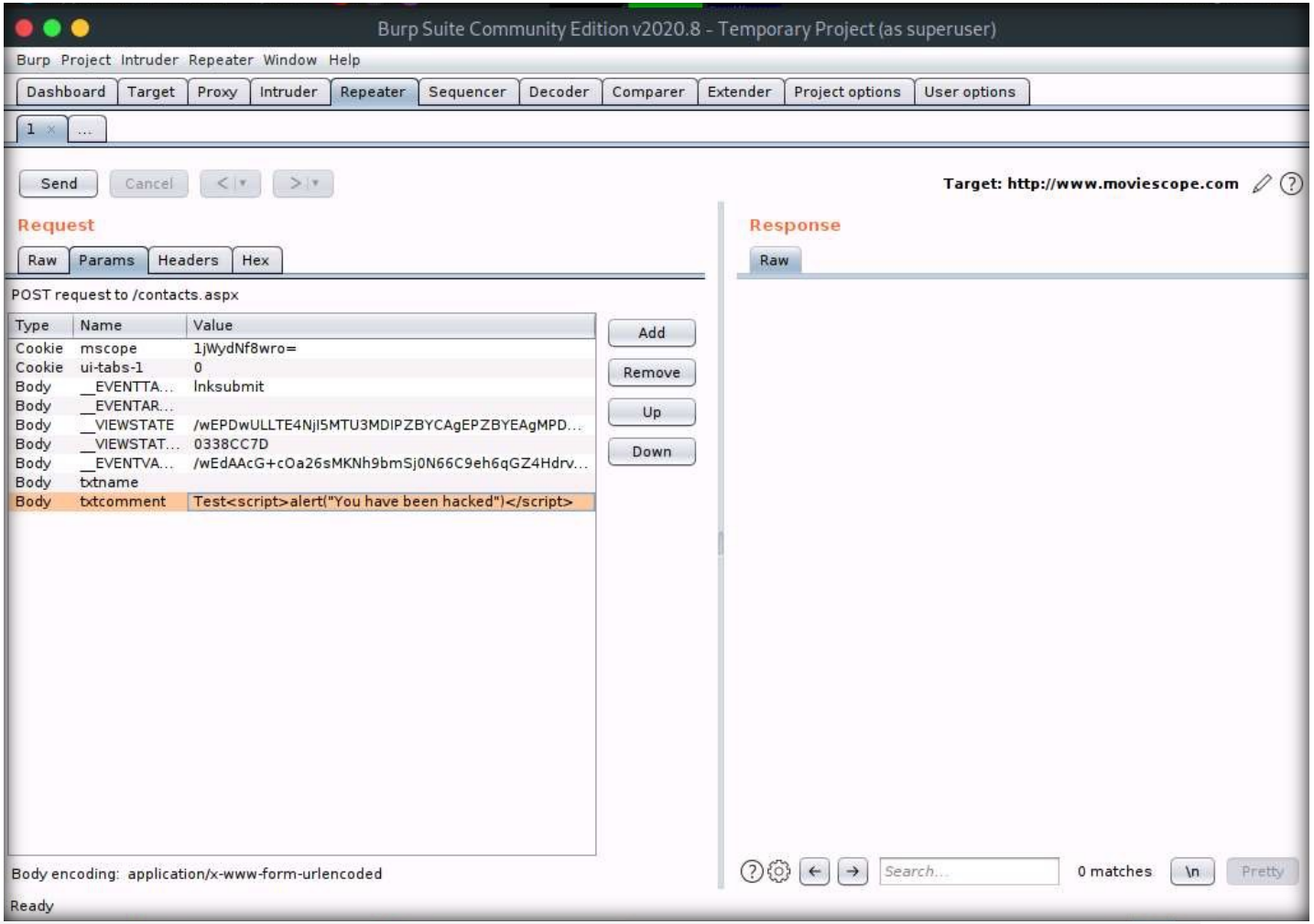
30. Now, navigate to the Repeater tab and navigate to Params tab under Request section.

EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE



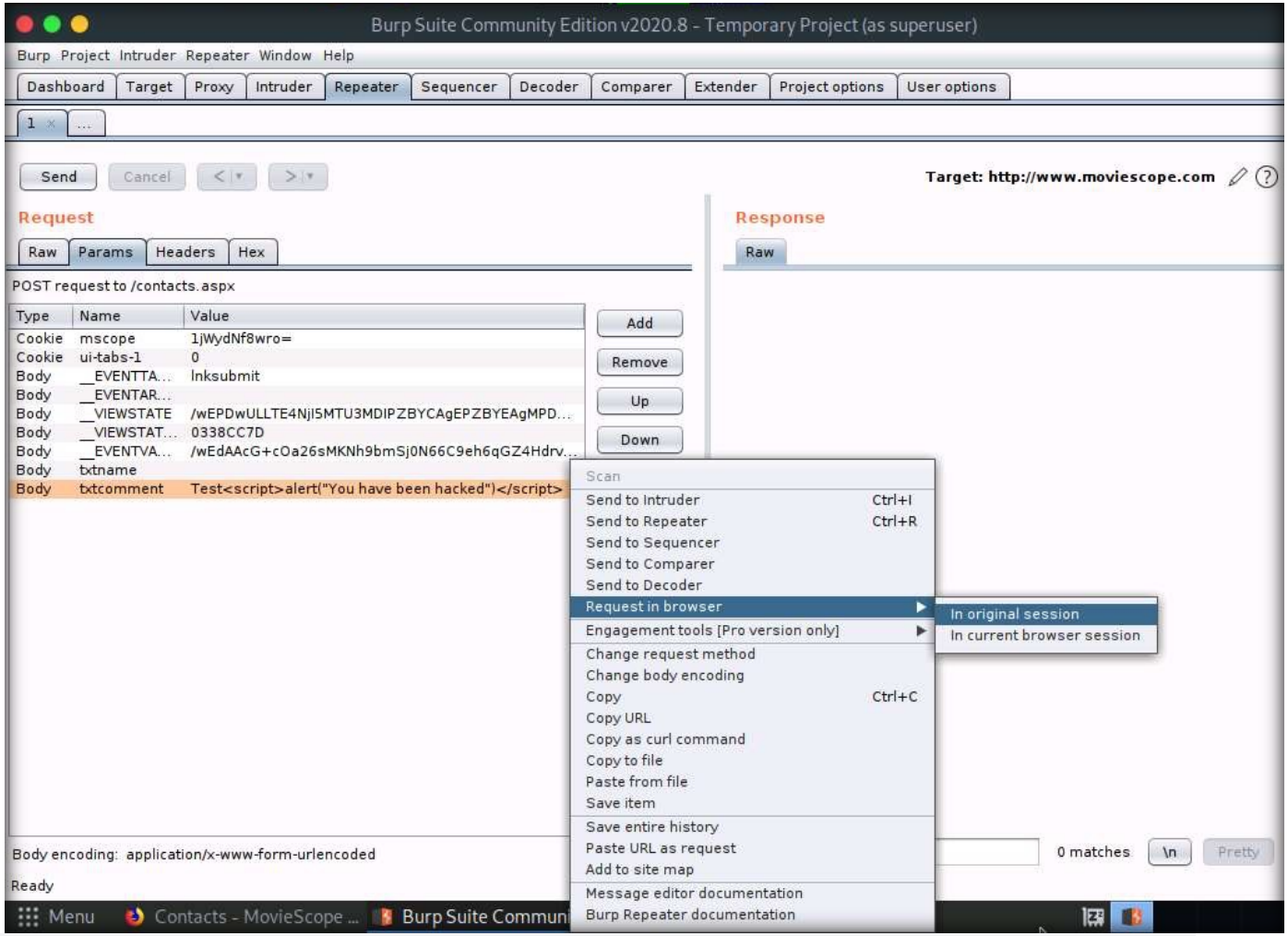
31. In the txtcomment box, replace the typed text with the following script and press Enter,
Test<script>alert("You have been hacked")</script>

EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE



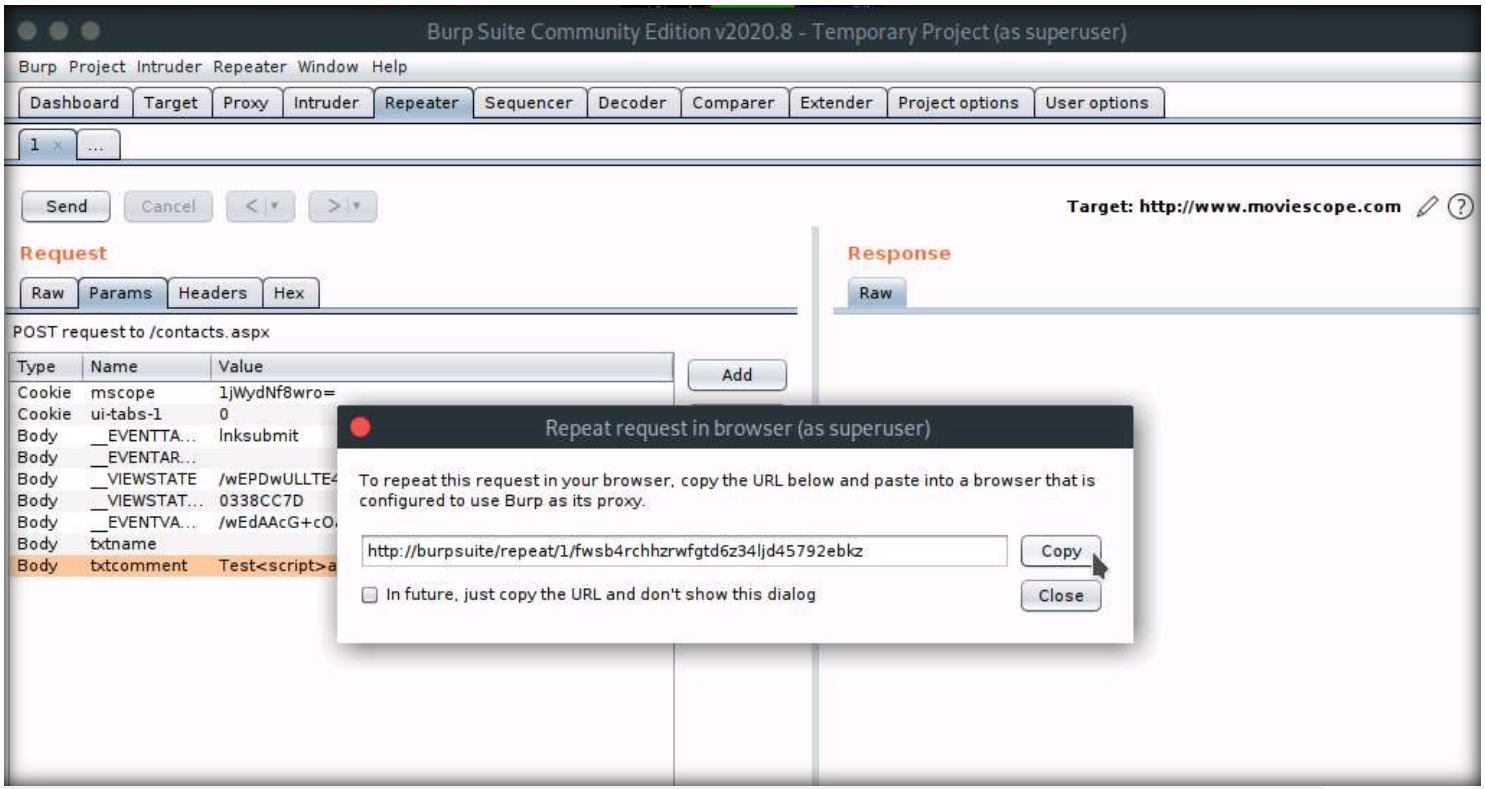
32. Right-click txtcomment row and navigate to Request in browser > In original session.

EXERCISE 5:
DETECT INJECTION VULNERABILITY USING BURP SUITE



33. Repeat request in browser dialog-box appears, click Copy button.

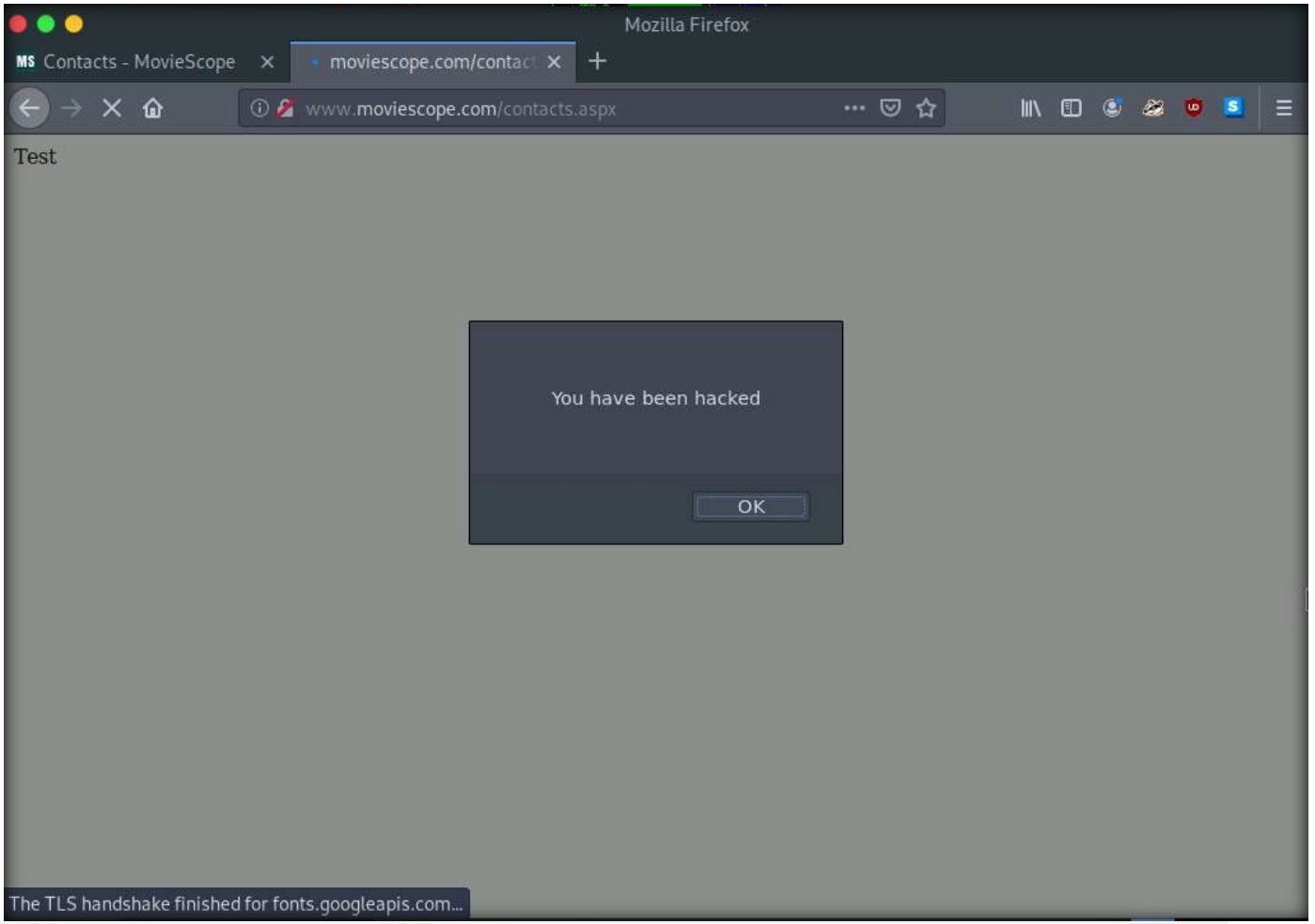
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



34. Switch to the browser window, open a new tab; paste the copied link and press Enter.

35. An alert displaying “You have been hacked” appears; click OK to close the pop-up.

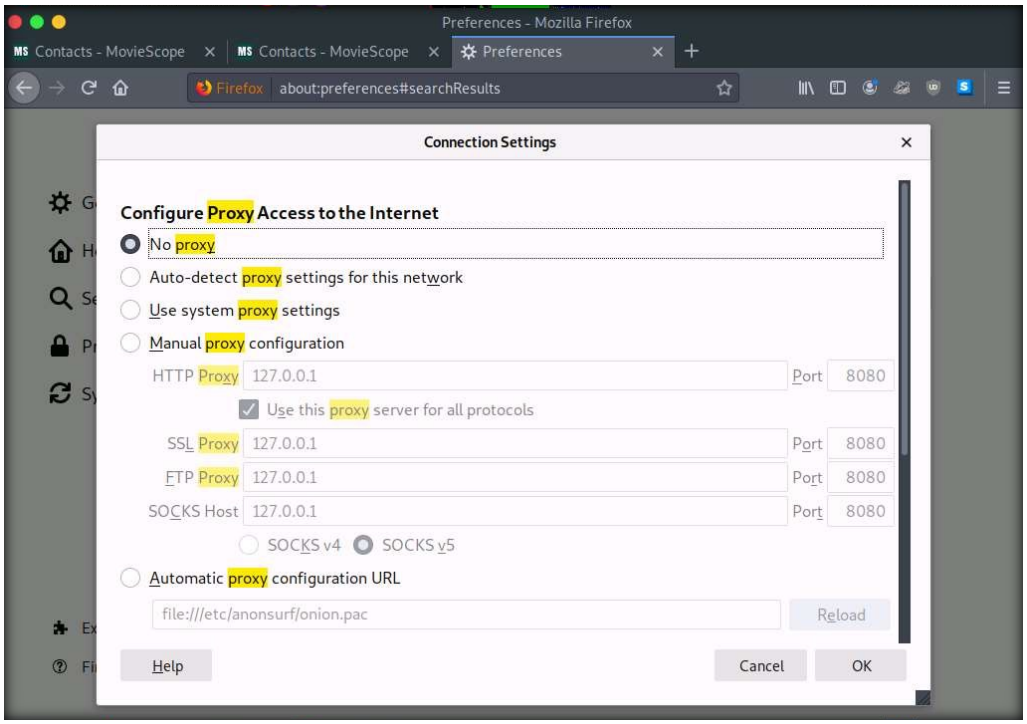
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



36. This alert appears when the user visits the Contacts tab of the website. This is a Cross Site Scripting (XSS) attack where the website allows the messages to be posted as comments to execute an embedded script.

37. In the browser, click the Open menu icon in the right corner of the menu bar and select Preferences from the list. The General settings tab appears. In the Find in Preferences search bar, type proxy, and press Enter.

38. The Search Results appear. Click the Settings button under the Network Settings option. A Connection Settings window appears; select No proxy radio-button and click OK.



39. This concludes the demonstration showing how to test injection vulnerability using Burp Suite
40. Close all open windows.
41. Turn off Web Server and Attacker Machine-2 virtual machines.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

EXERCISE 6: **DETERMINE APPLICATION-LEVEL ATTACKS**

Application-level attacks are used to compromise the security of web applications to commit fraud or steal sensitive information.

LAB SCENARIO

A security professional must have the required knowledge to determine application-level attacks against a Windows server machine. In this task, we will simulate an attack that utilizes CPU memory which makes the machine slow and non-responsive. Here, first, we will load CPU by using HeavyLoad tool and monitor the degradation in system performance by using Performance Monitor and Process Hacker tools.

OBJECTIVE

This lab will demonstrate how to identify application-level attack against a Windows server.

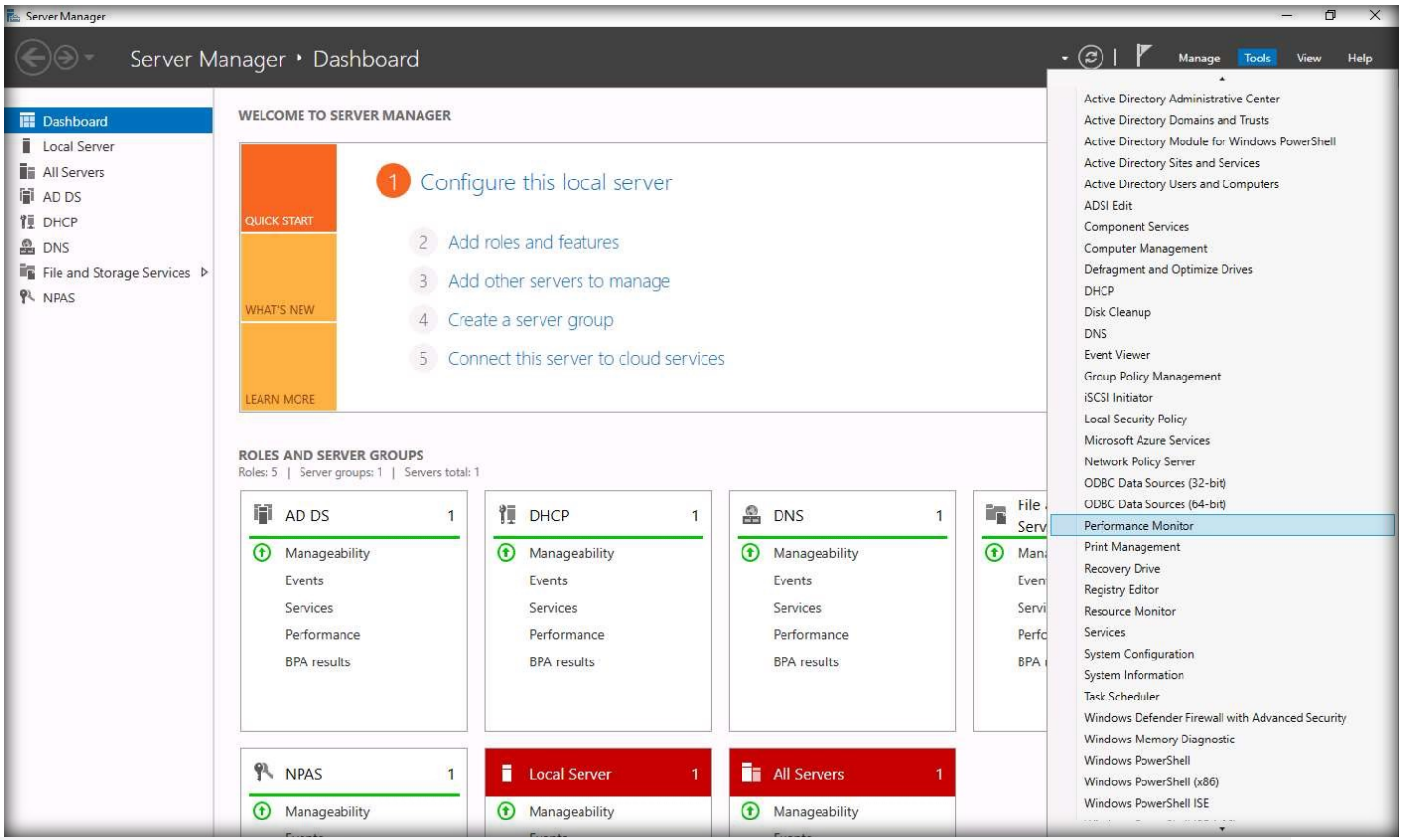
OVERVIEW OF WEB APPLICATION

Organizations are increasingly using web applications to provide high-value business functions to their customers such as real-time sales, transactions, inventory management across multiple vendors including both B-B and B-C e-commerce, workflow and supply chain management, etc.
Attackers exploit vulnerabilities in the applications to launch various attacks and gain unauthorized access to resources. It is commonly assumed that perimeter security controls such as firewall and IDS systems can secure an application; however, this is not true as these controls are not effective at defending against application layer attacks. This is because port 80 and 443 are generally open on perimeter devices for legitimate web traffic, which attackers can use to exploit application-level vulnerabilities and get into the network.

Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the AD Domain Controller machine.
2. Log in with the credentials CCT\Administrator and admin@123.

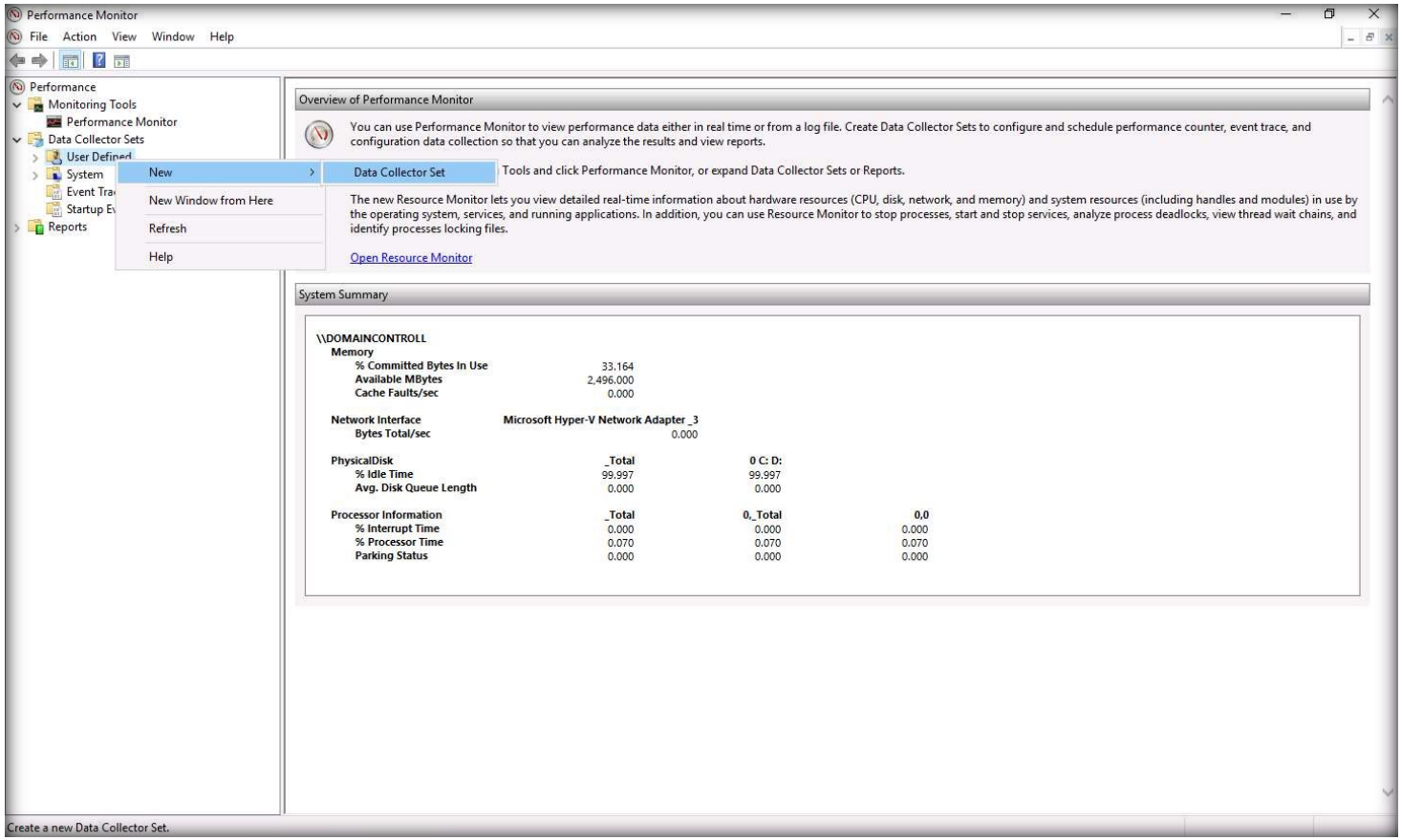
Note: The network screen appears, click Yes.
3. Click Start icon and select Server Manager.
4. The Server Manager window appears. Click Tools and select Performance Monitor option.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



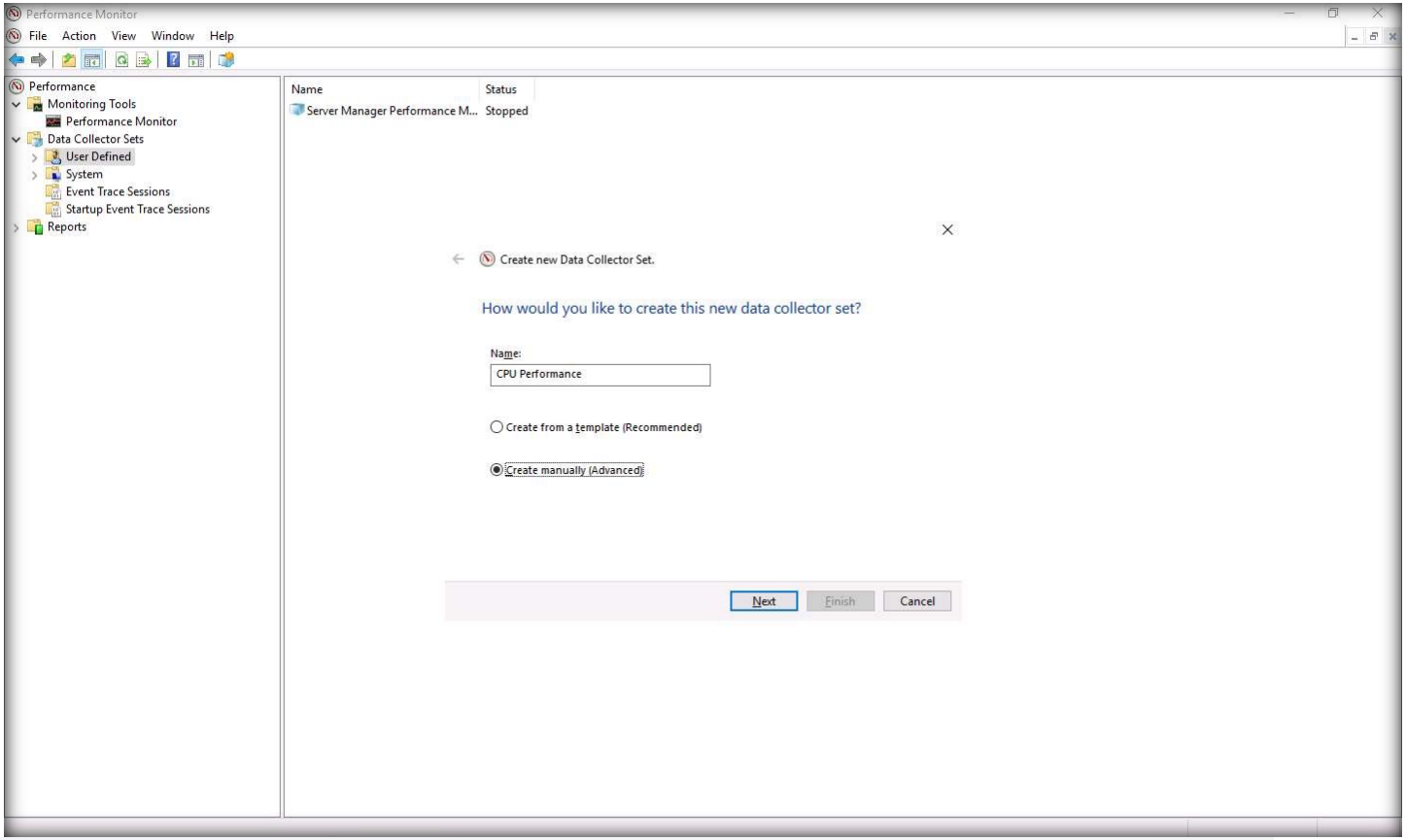
5. Performance Monitor window appears. From the left-pane, expand Data Collector Sets, right-click User Defined node and navigate to New > Data Collector Set.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



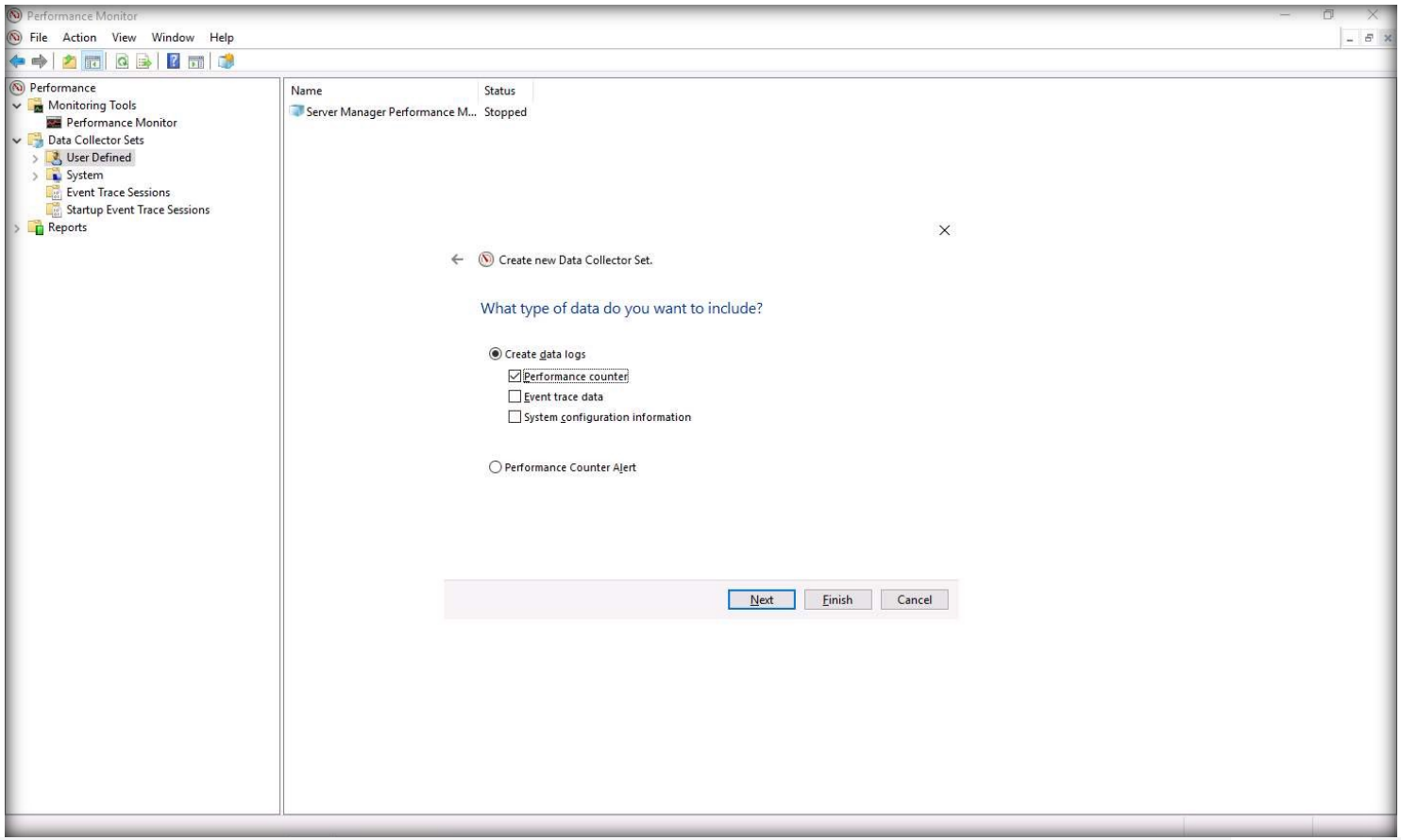
6. Create new Data Collector Set window appears. In the Name field enter the name as CPU Performance and select Create manually (Advanced). Click Next.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



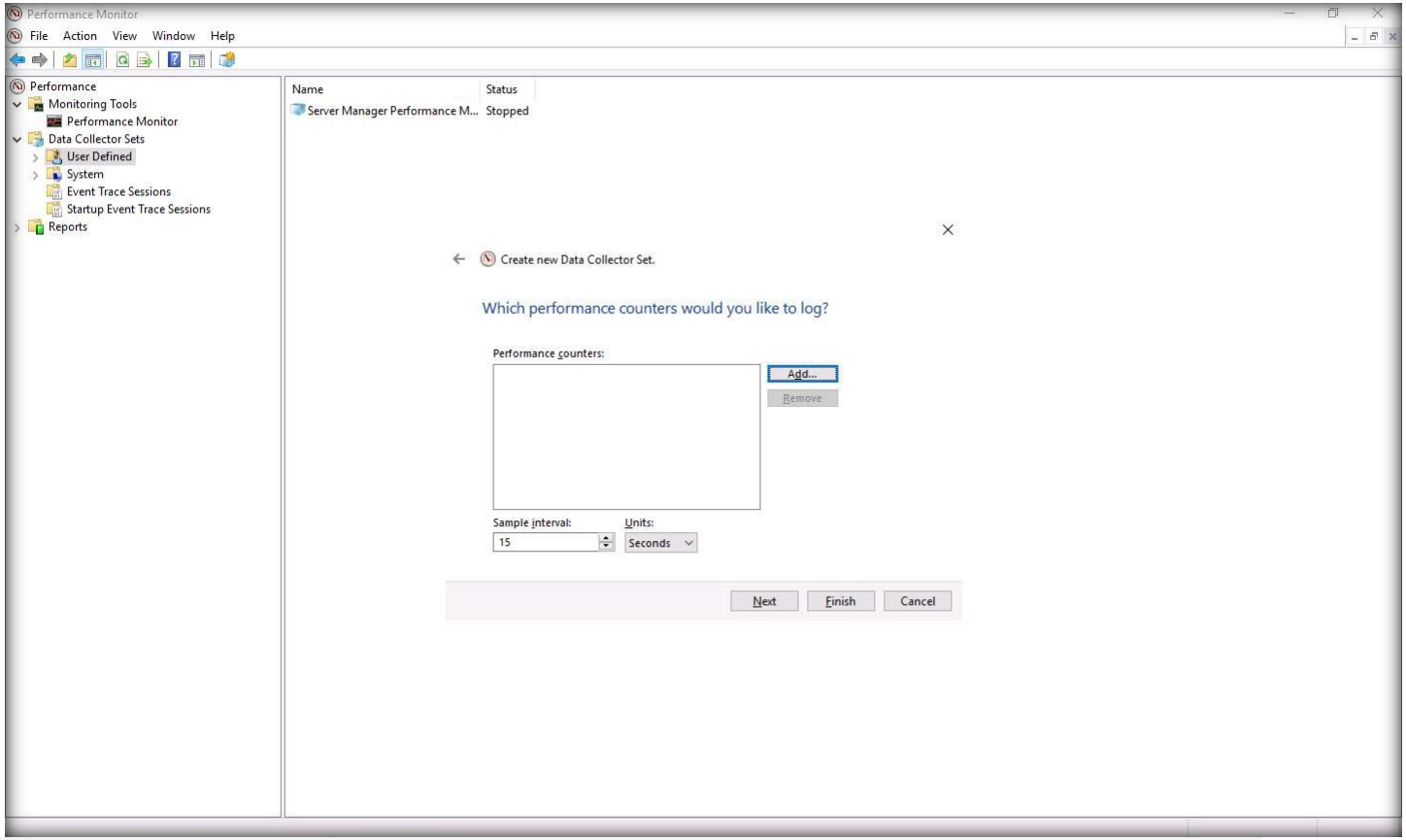
7. In the next wizard, select Performance counter checkbox under Create data logs radio button and click Next.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



8. Which performance counters would you like to log? wizard appears, click Add... button.

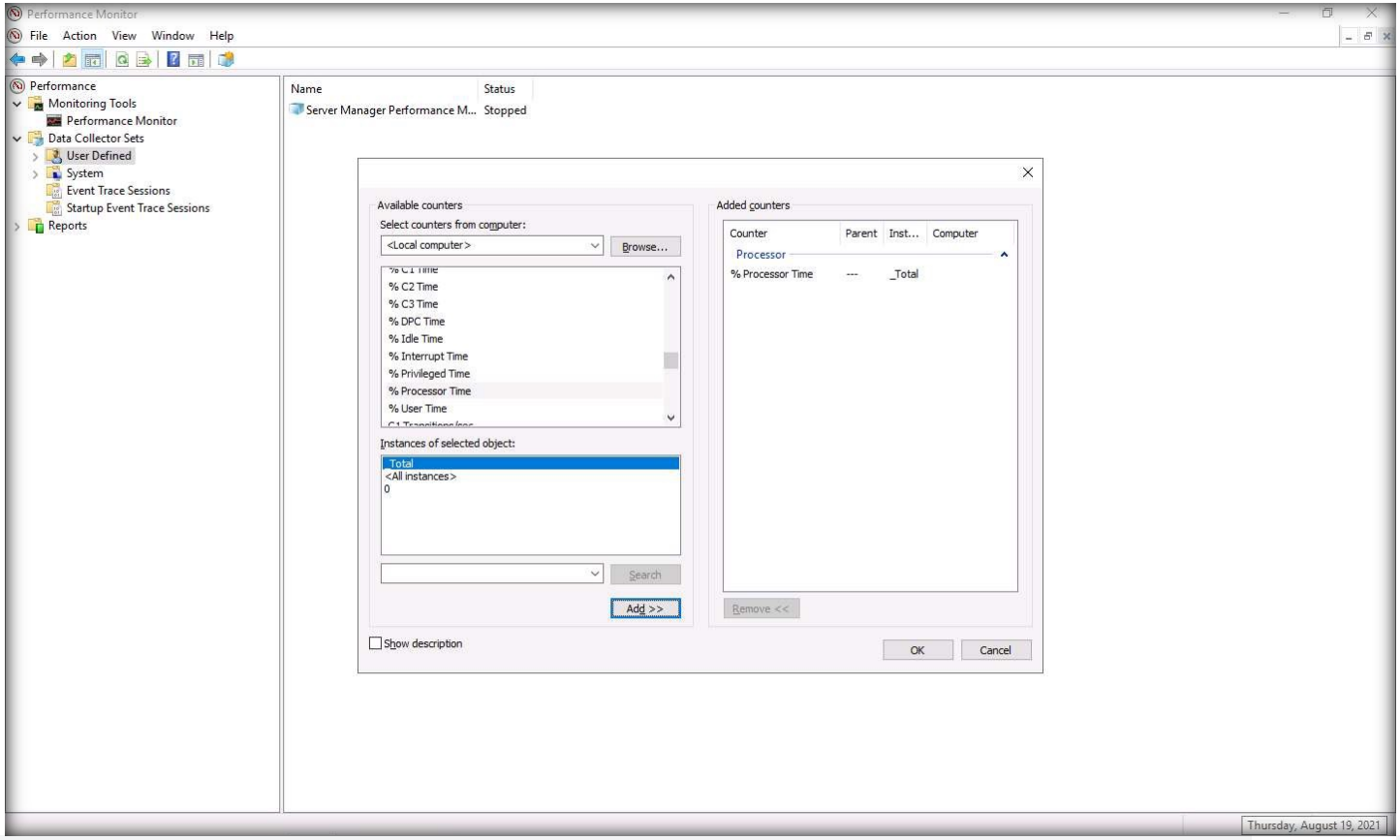
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



9. Available counters wizard appears. Ensure that Local computer is selected in the Select counters from computer field.

10. Under Select counters from computer option, scroll-down and expand Processor node. Processor option appears, select % Processor Time and click Add>> button under Instance of selected object field.

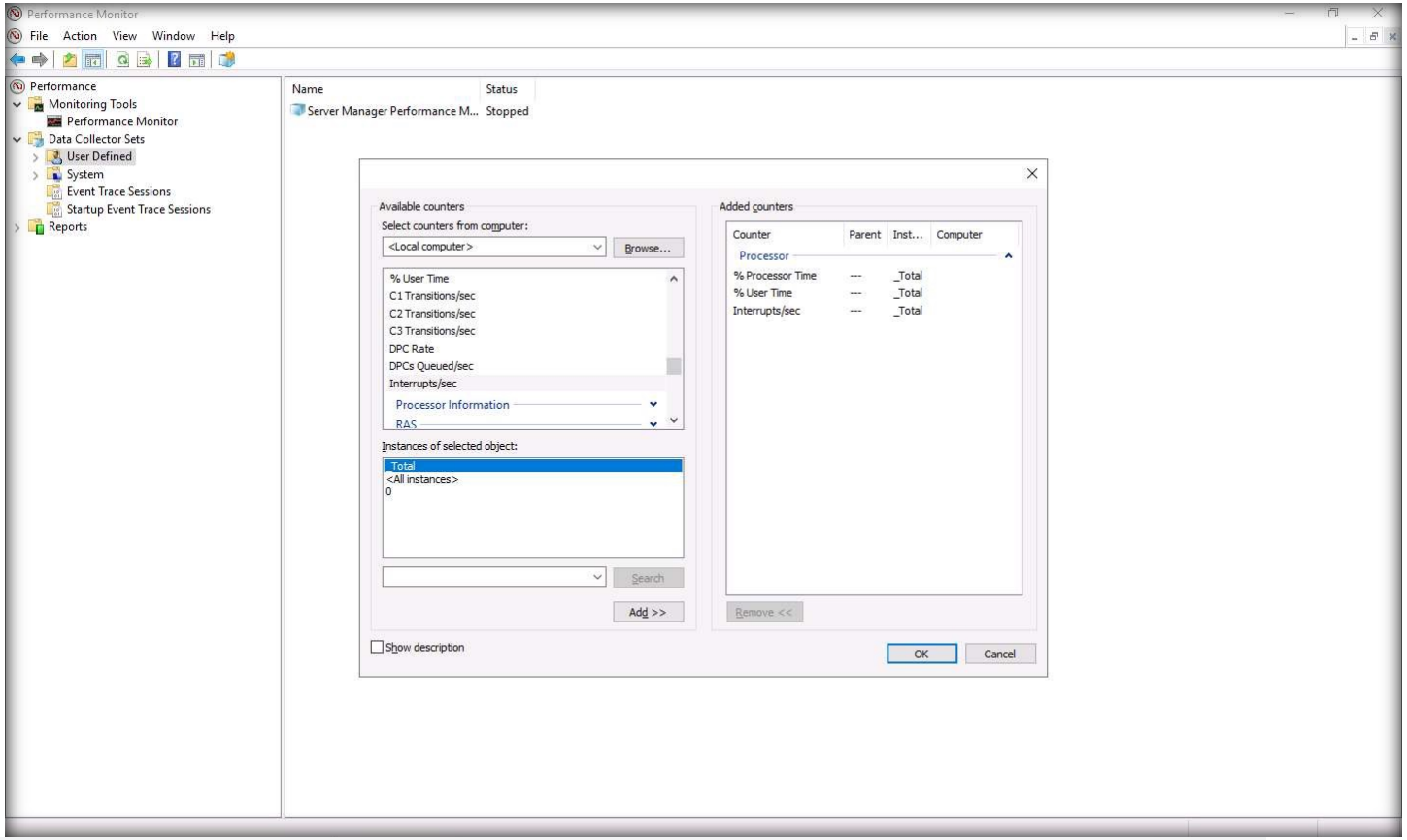
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



11. Similarly, select % User Time and Interrupts/sec option and click Add>> to add the options one-by-one. Click OK.

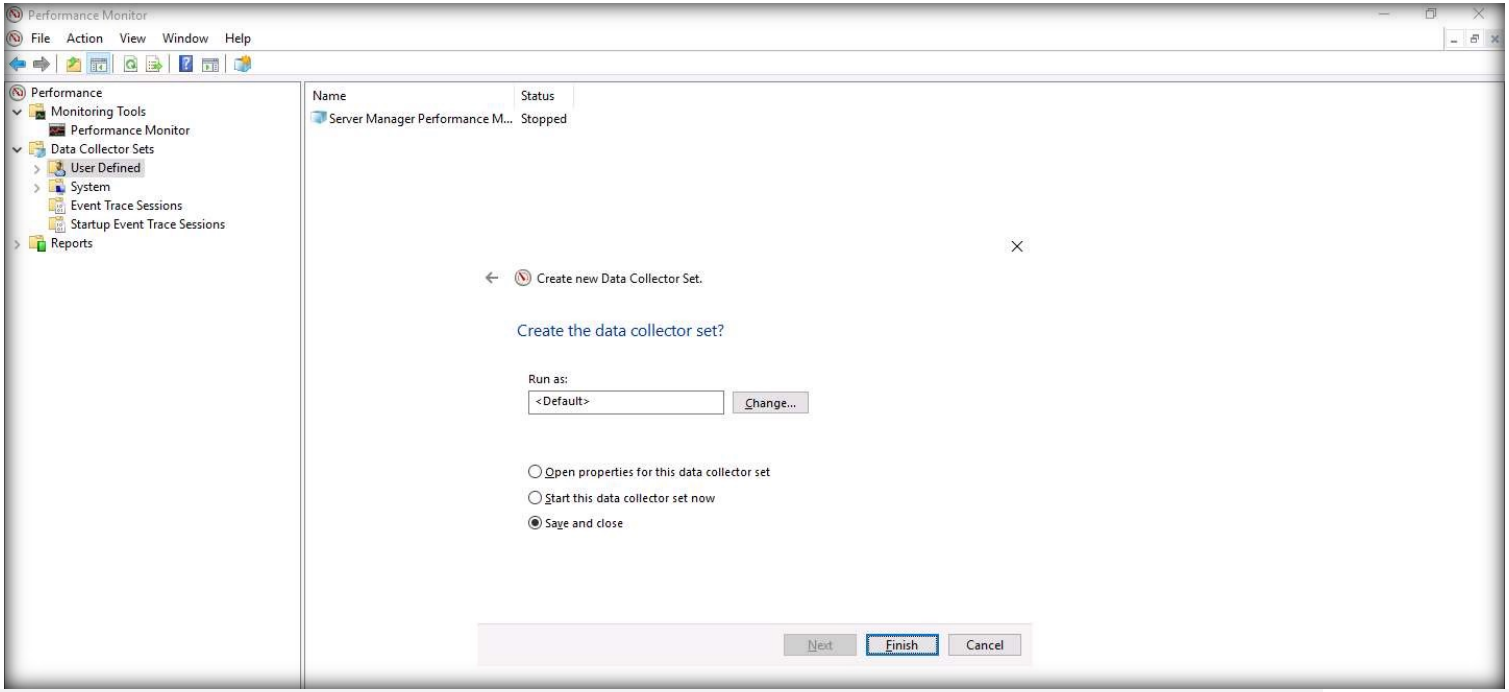
Note:
• % Processor Time: Indicates an overall activity level of the system.
• % User Time: Indicates time spent by the processor in managing system processes.
• Interrupts/sec: Indicates interrupts that the processor should handle instantly.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



12. In the next wizard, click Next button.
13. Similarly, in the next wizard, click Next and in the Create data collector set? wizard, click Finish.

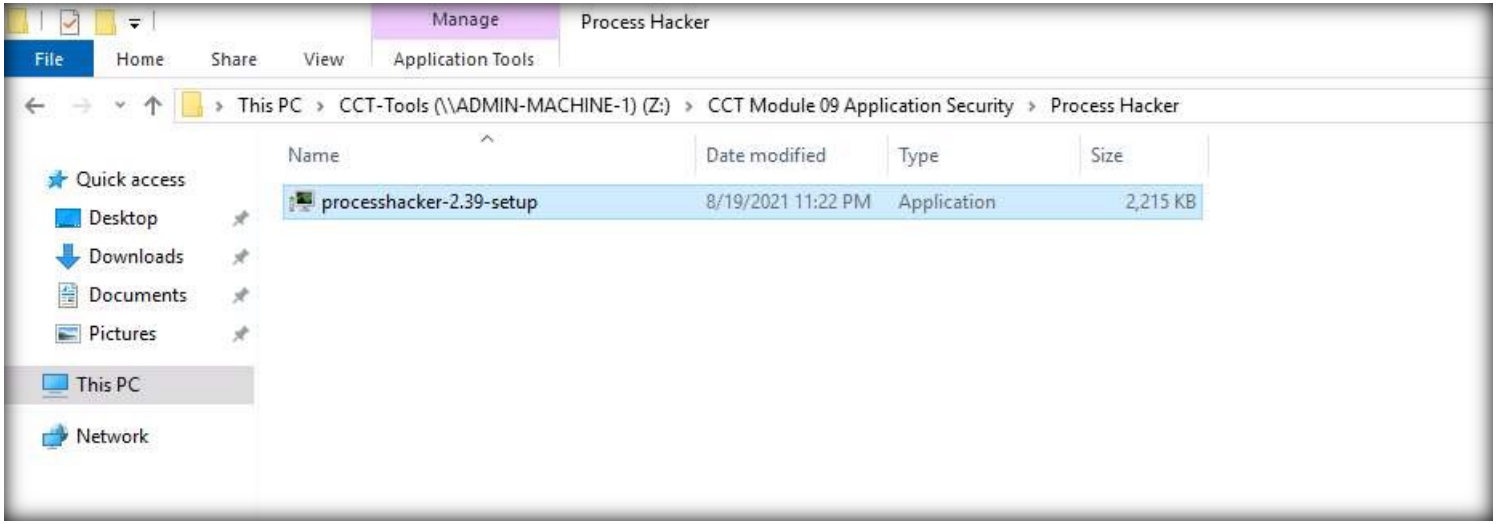
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



14. Minimize the Performance Monitor window.

15. Now, open a File Explorer window and navigate to Z:\CCT Module 09 Application Security\Process Hacker. Double-click processhacker-2.39-setup.exe.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



16. Open File - Security Warning window appears, click Run.

17. Setup - Process Hacker window appears, accept the license agreement and click Next.

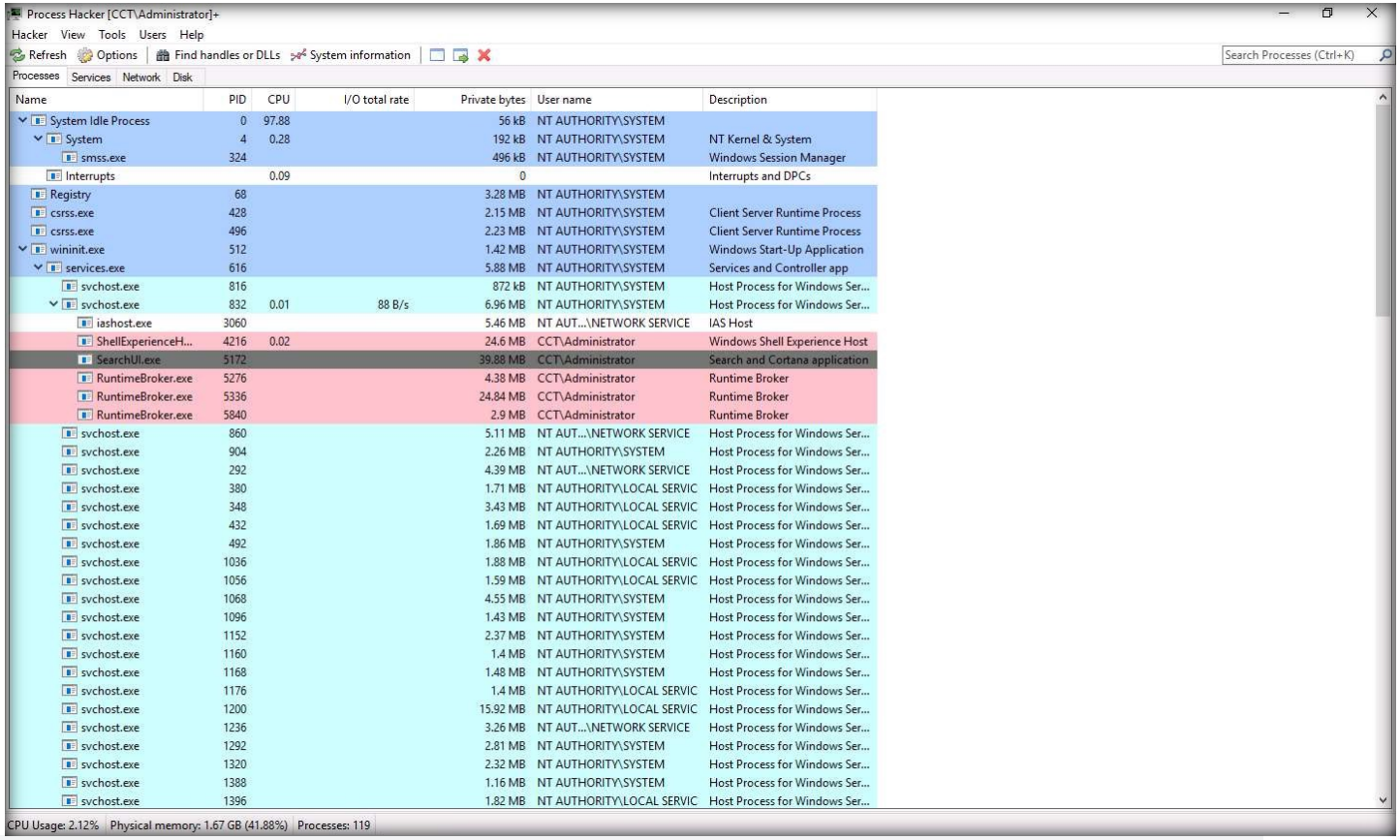
18. Click Next in all the windows leaving settings to default.

19. In the final window of the wizard, ensure that Launch Process Hacker 2 checkbox is selected and click Finish.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS

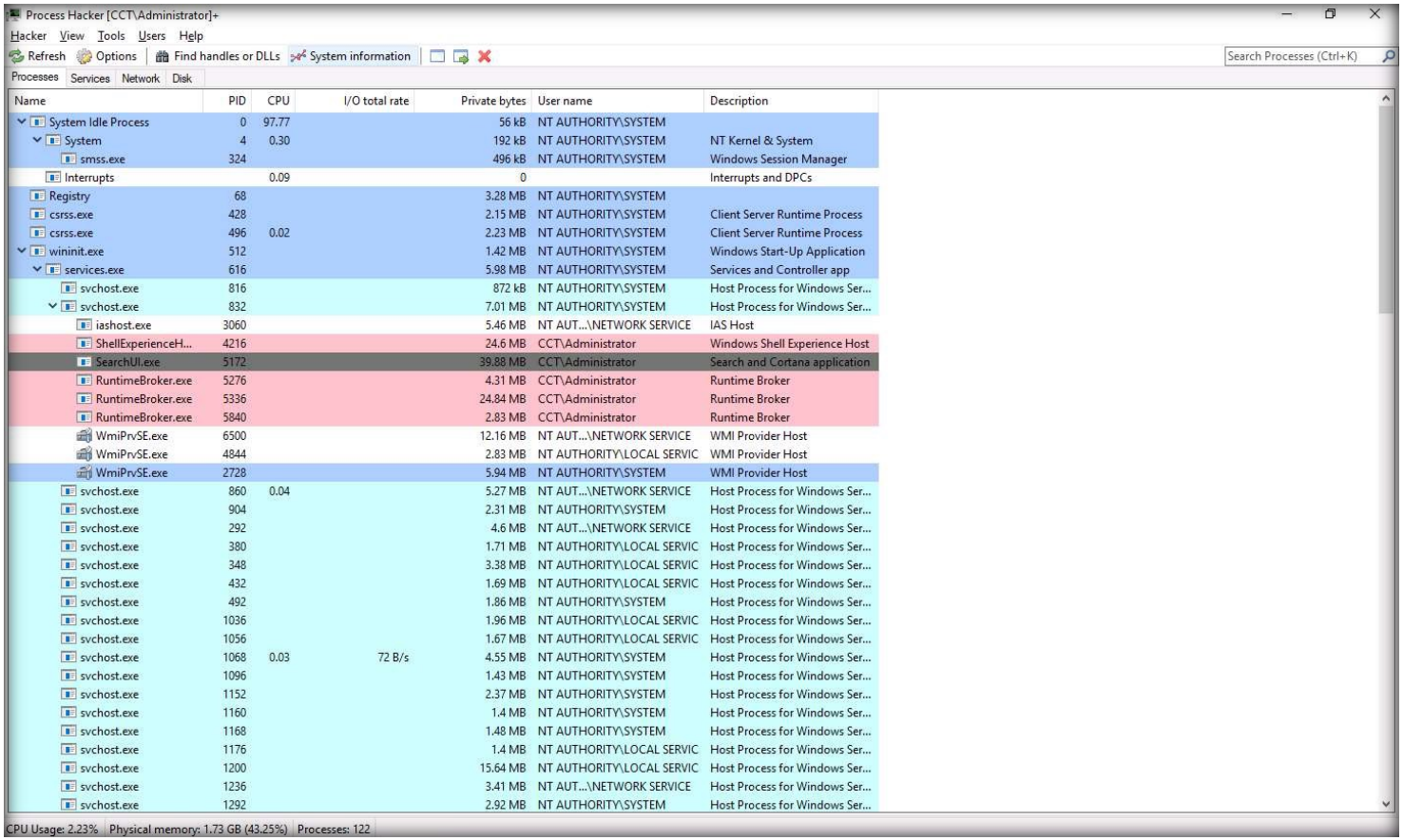
20. Process Hacker window appears. You can observe that a list of running processes are displayed along with their CPU utilization, I/O total rate, etc.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



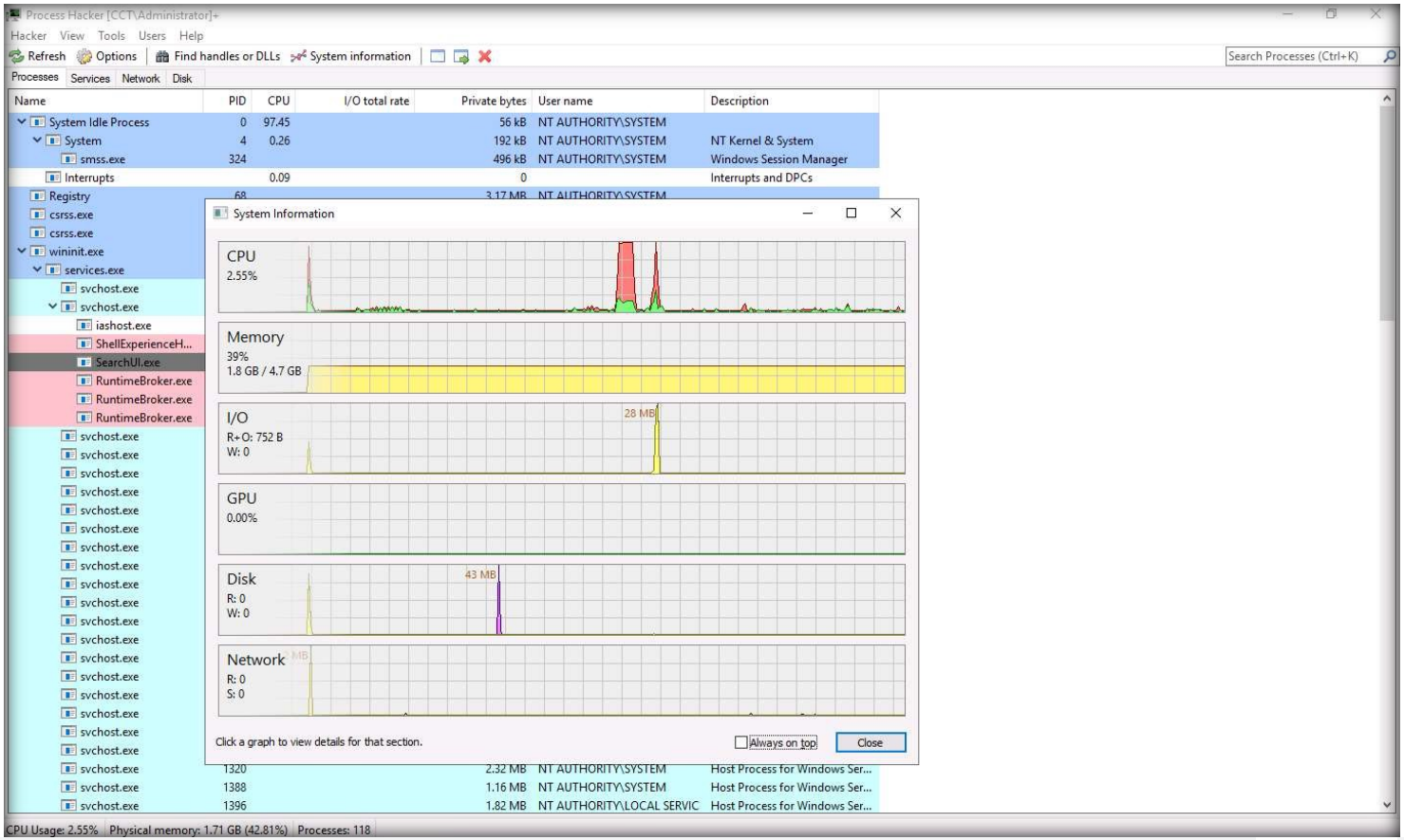
21. Now, click System information option from the toolbar.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



22. A System information window appears, displaying CPU, Memory, I/O, GPU, Disk, Network utilization, as shown in the screenshot below.

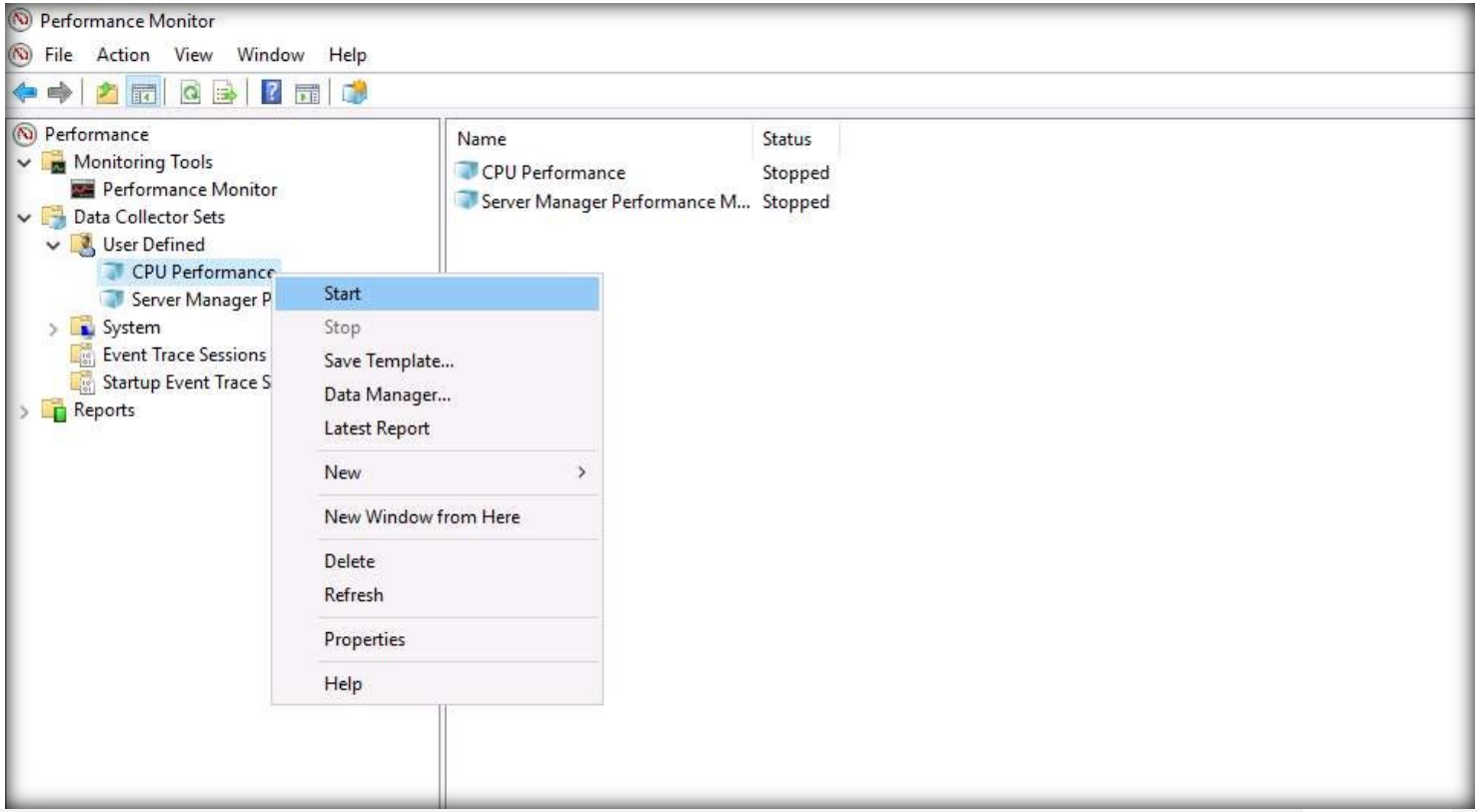
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



23. Now, we will create false stress on the system's processor using HeavyLoad tool. To monitor the stress on the CPU, we will use Performance Monitor and Process Hacker tools.

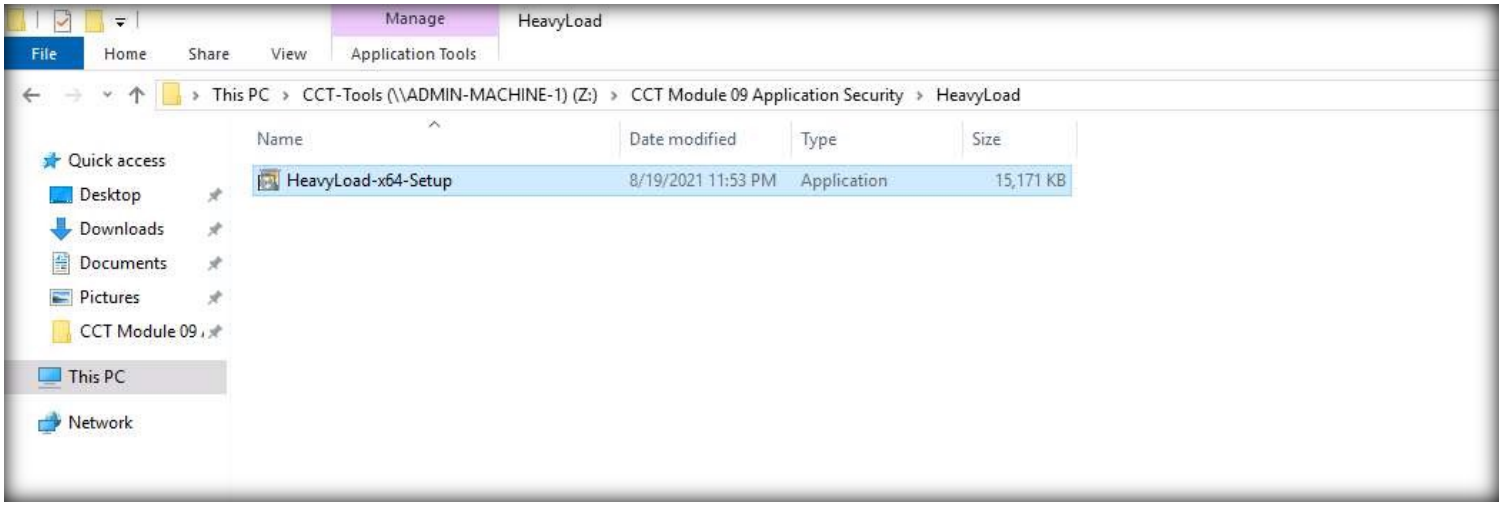
24. Maximize Performance Monitor window. From the left-pane, expand Data Collector Sets and User Defined node. Right-click CPU Performance node and click Start. Minimize the window.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



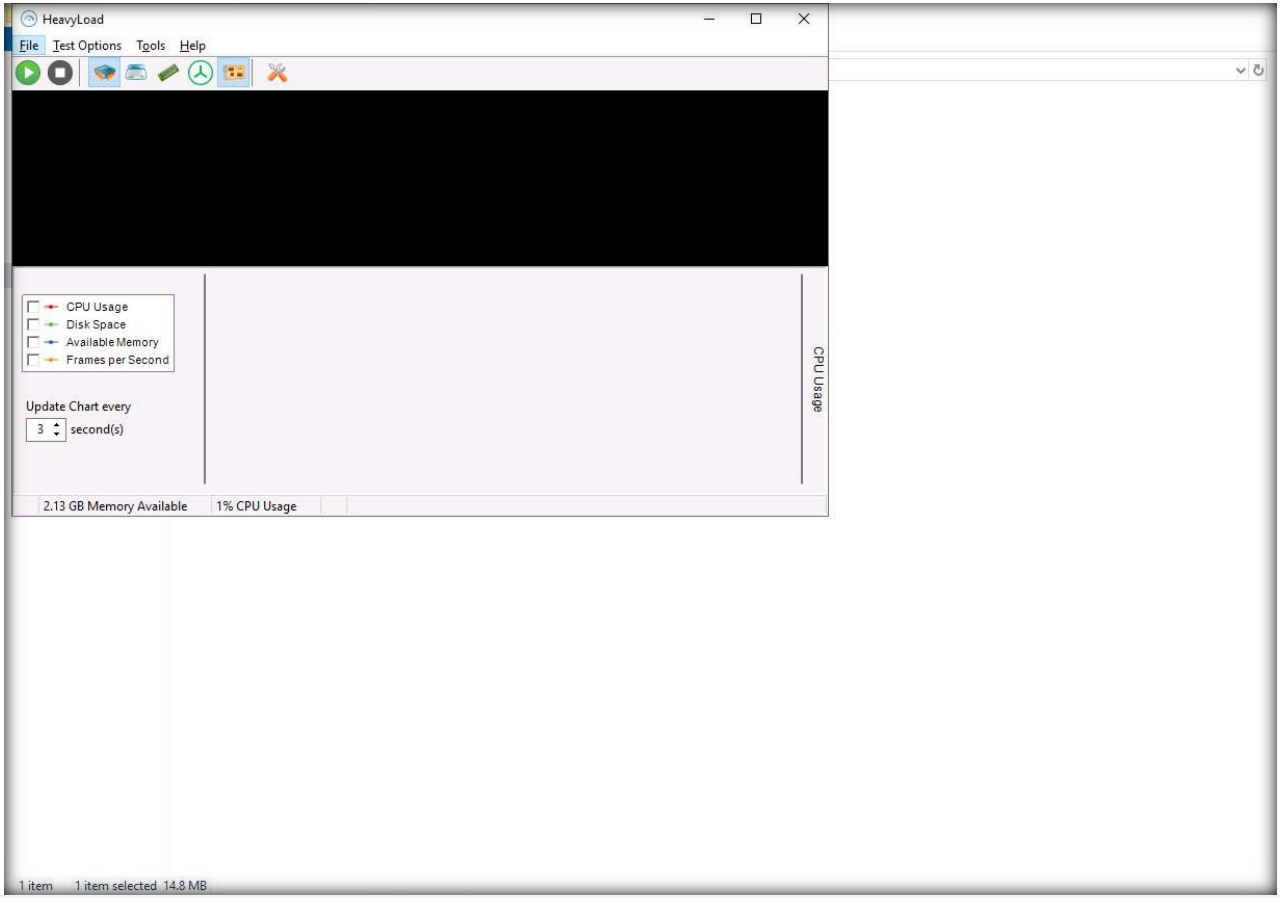
25. Maximize the File Explorer window and navigate to Z:\CCT Module 09 Application Security\HeavyLoad. Double-click HeavyLoad-x64-setup.exe.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



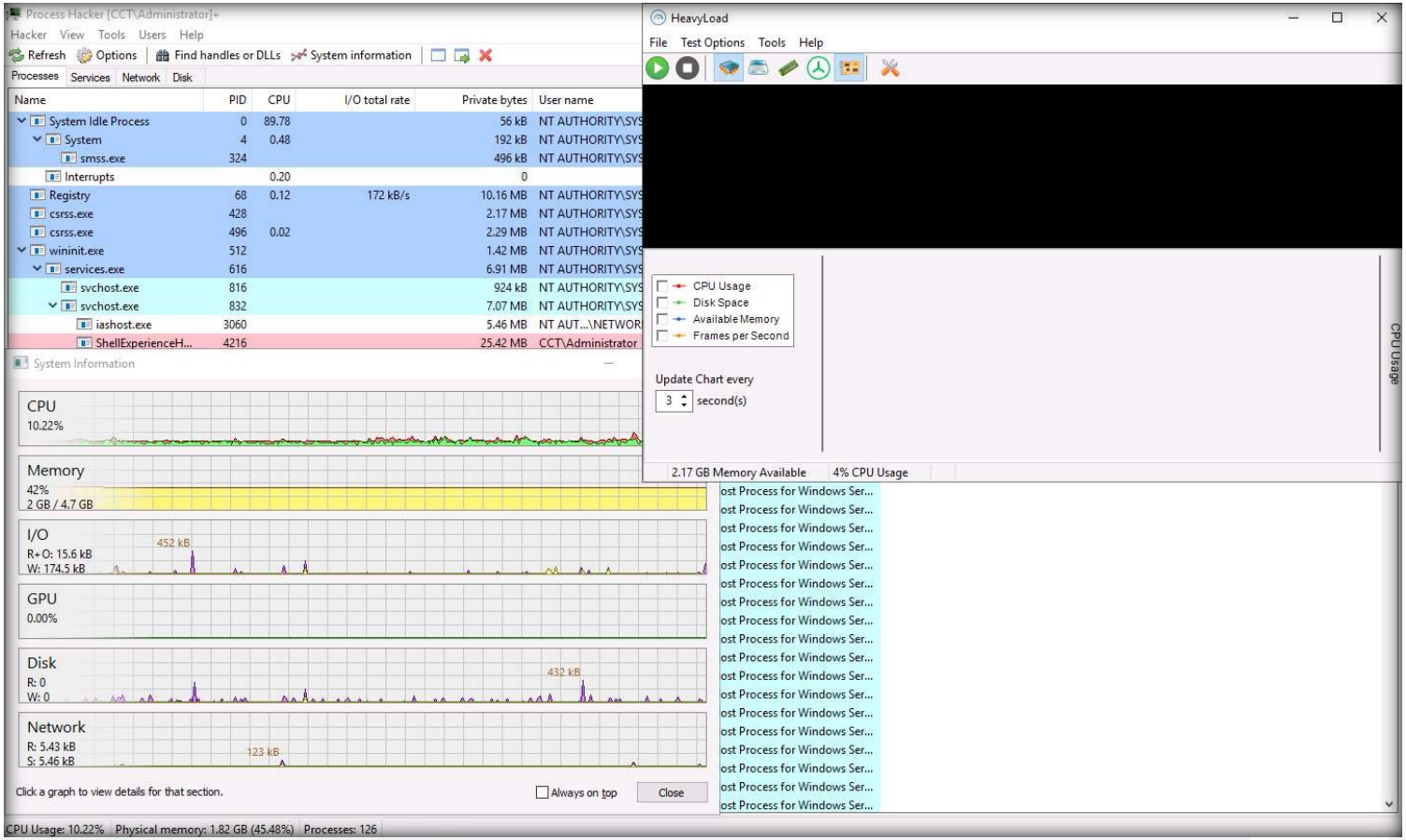
26. Open File - Security Warning window appears, click Run.
27. In Select Setup Language pop-up, choose English and click OK.
28. Setup - HeavyLoad window appears, accept the license agreement and click Next.
29. Click Next in all the windows leaving setting to default.
30. In the final window of the wizard, ensure that Launch HeavyLoad now checkbox is selected and click Finish.
31. HeavyLoad window appears, as shown in the screenshot below.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



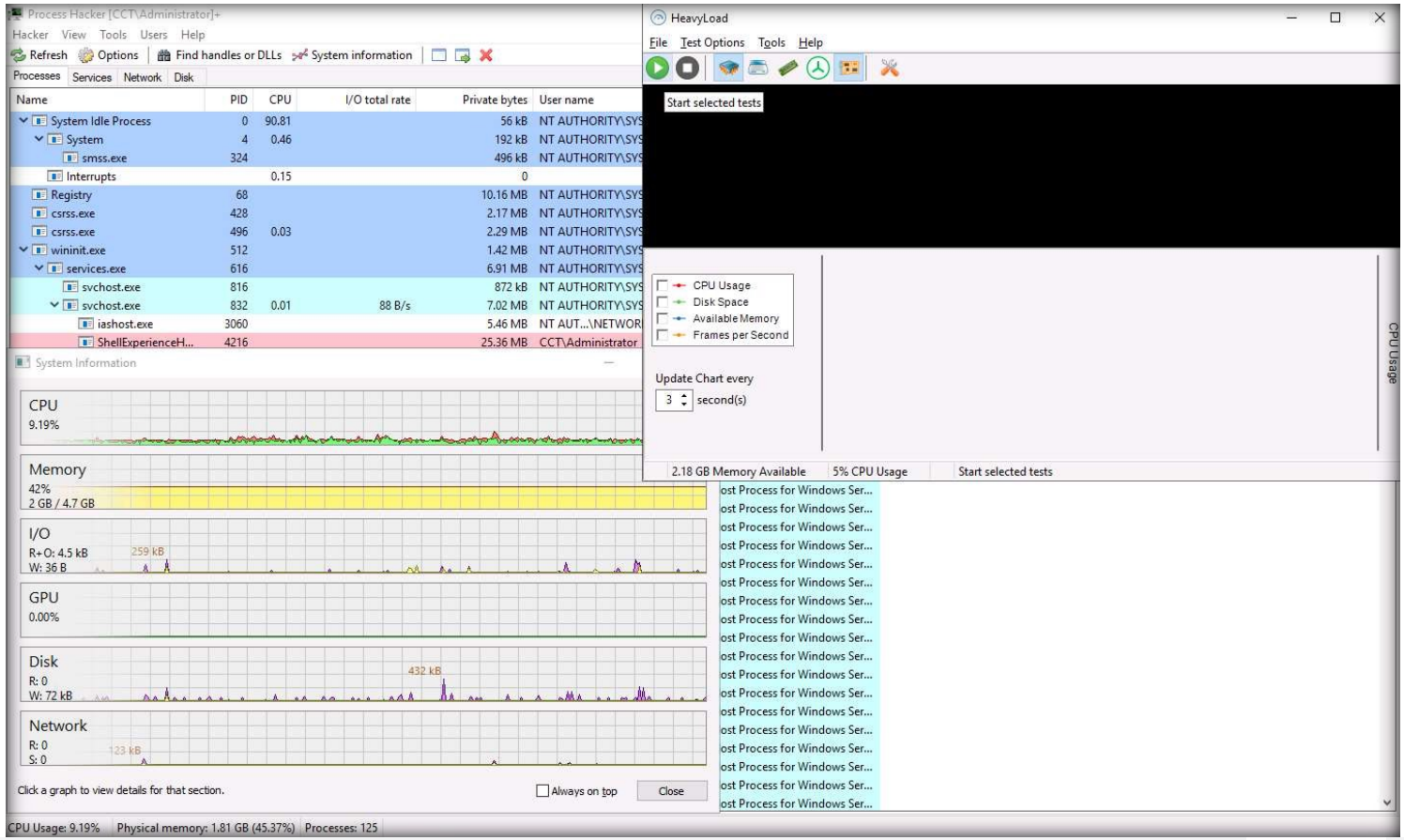
32. Now, reposition the Process Hacker, System information and HeavyLoad windows, so that you can view and observe them simultaneously, as shown in the screenshot below.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



33. In the HeavyLoad window, click Start selected tests icon to star creating stress on the system.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



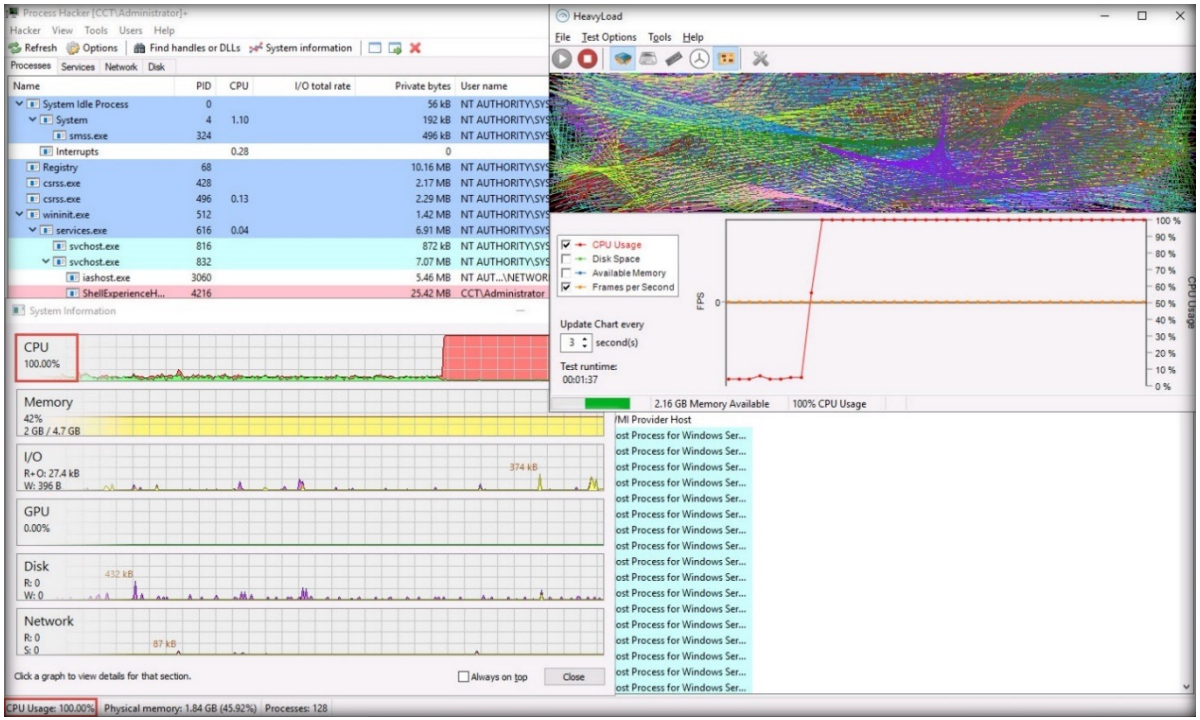
34. A Virtual machine detected window appears, click Continue.

35. If 3D Graphics not Supported window appears, close it.

36. You can observe that HeavyLoad starts creating load on the CPU and the CPU utilization reaches to 100% in the System information window.

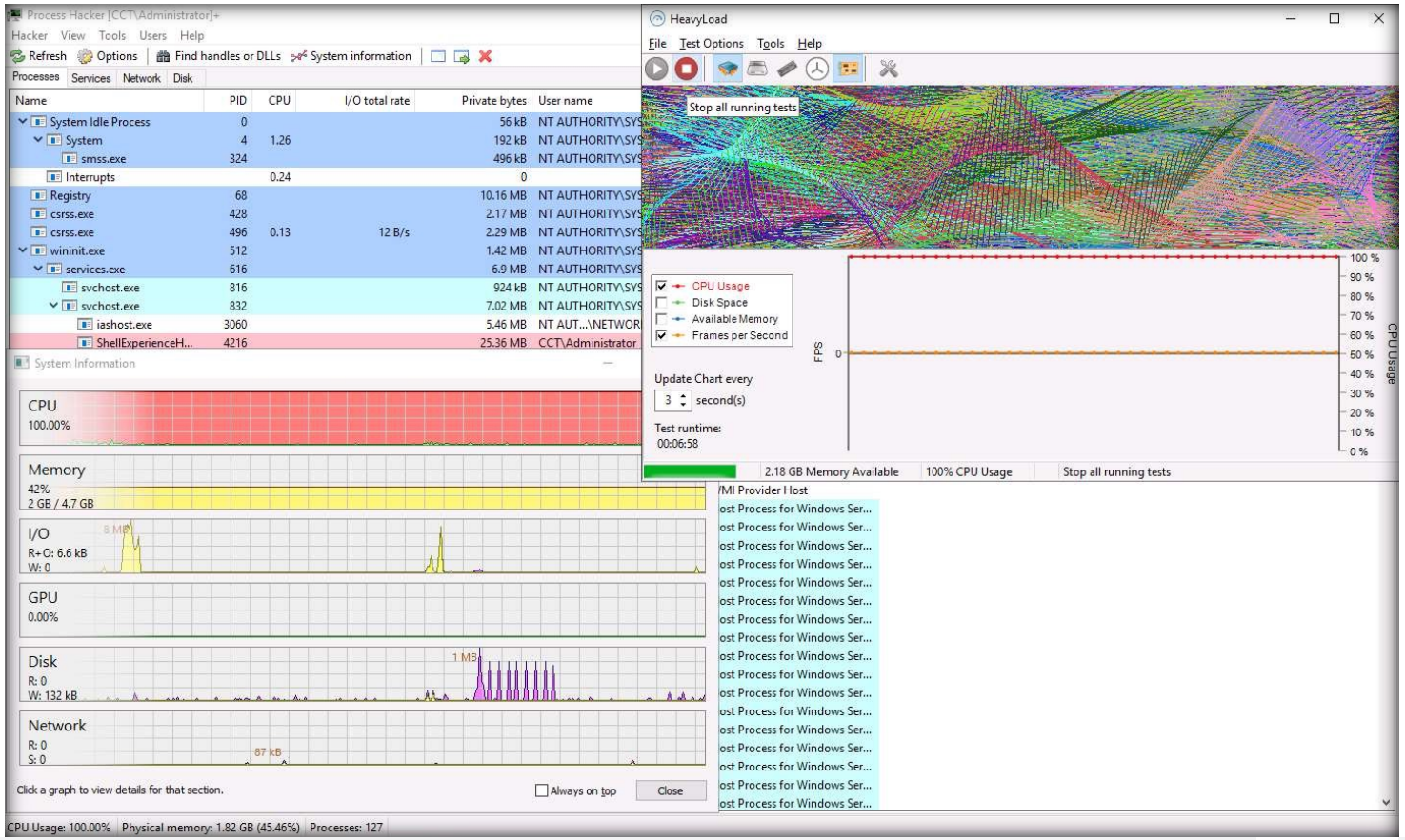
37. Similarly, you can observe the CPU Usage (100%) in the bottom-left corner of Process Hacker window.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



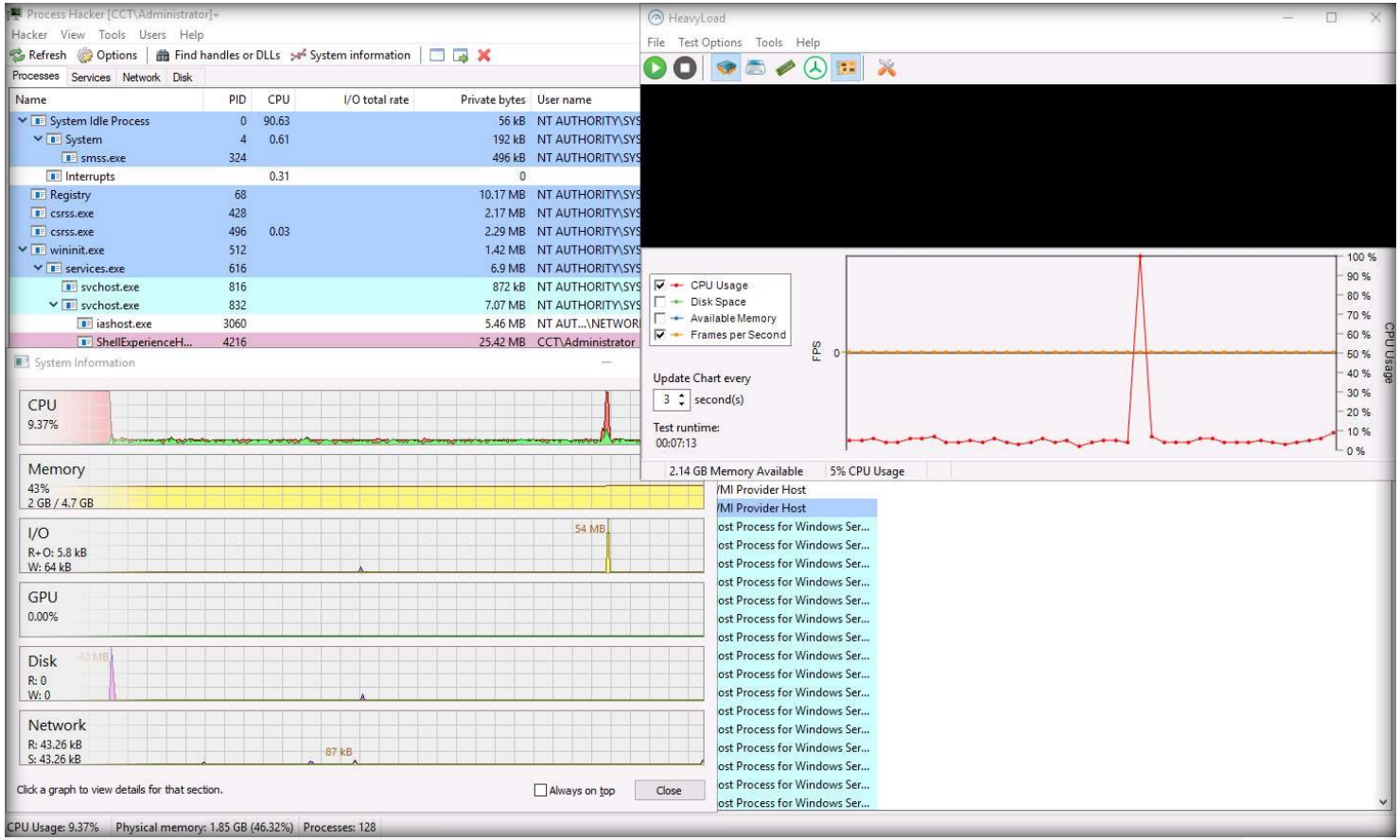
38. Now, in the HeavyLoad window, click Stop all running tests icon to stop the load on the system.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



39. You can observe that the CPU utilization is back to normal levels.

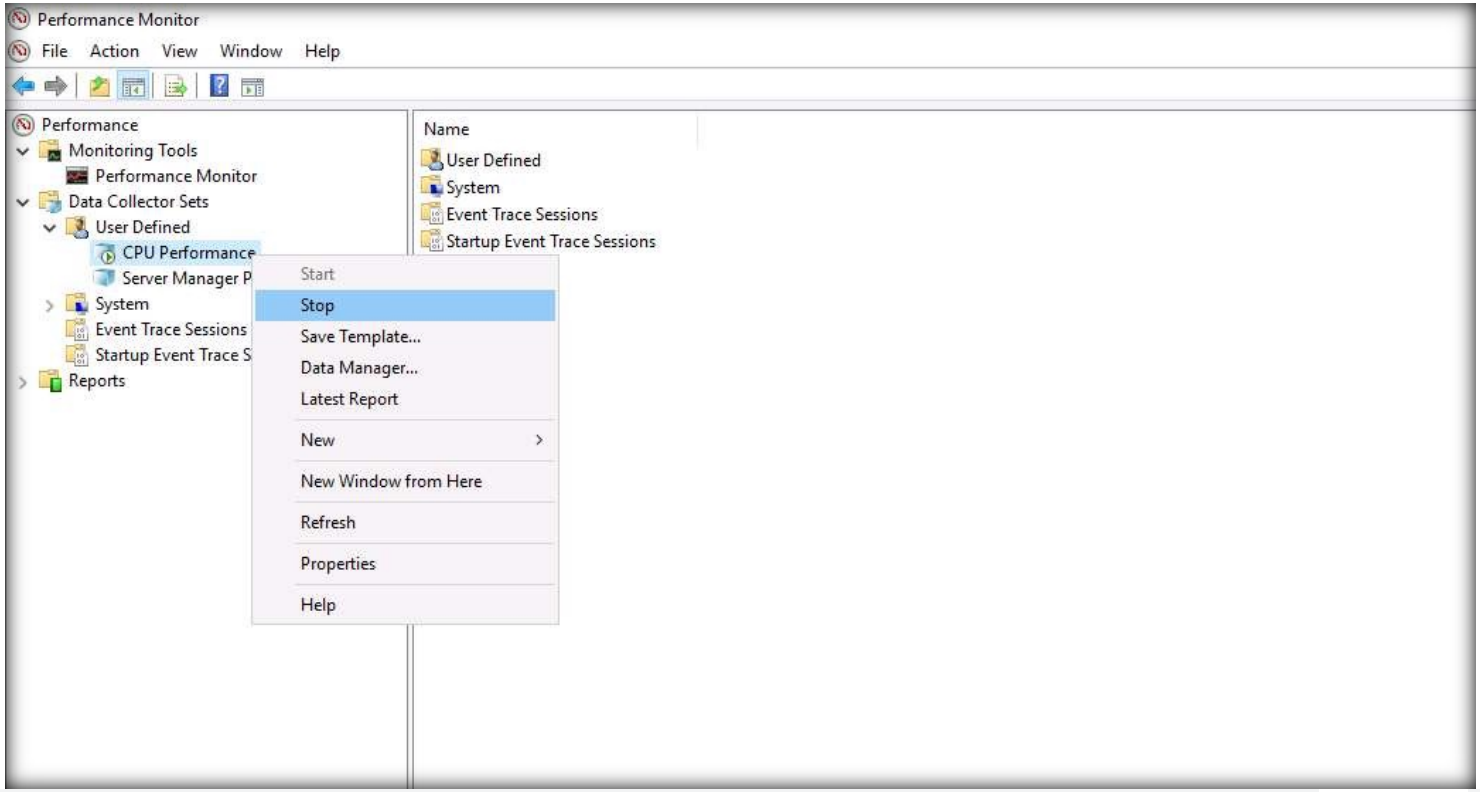
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



40. Close HeavyLoad, System Information and Process Hacker windows. Maximize Performance Monitor window.

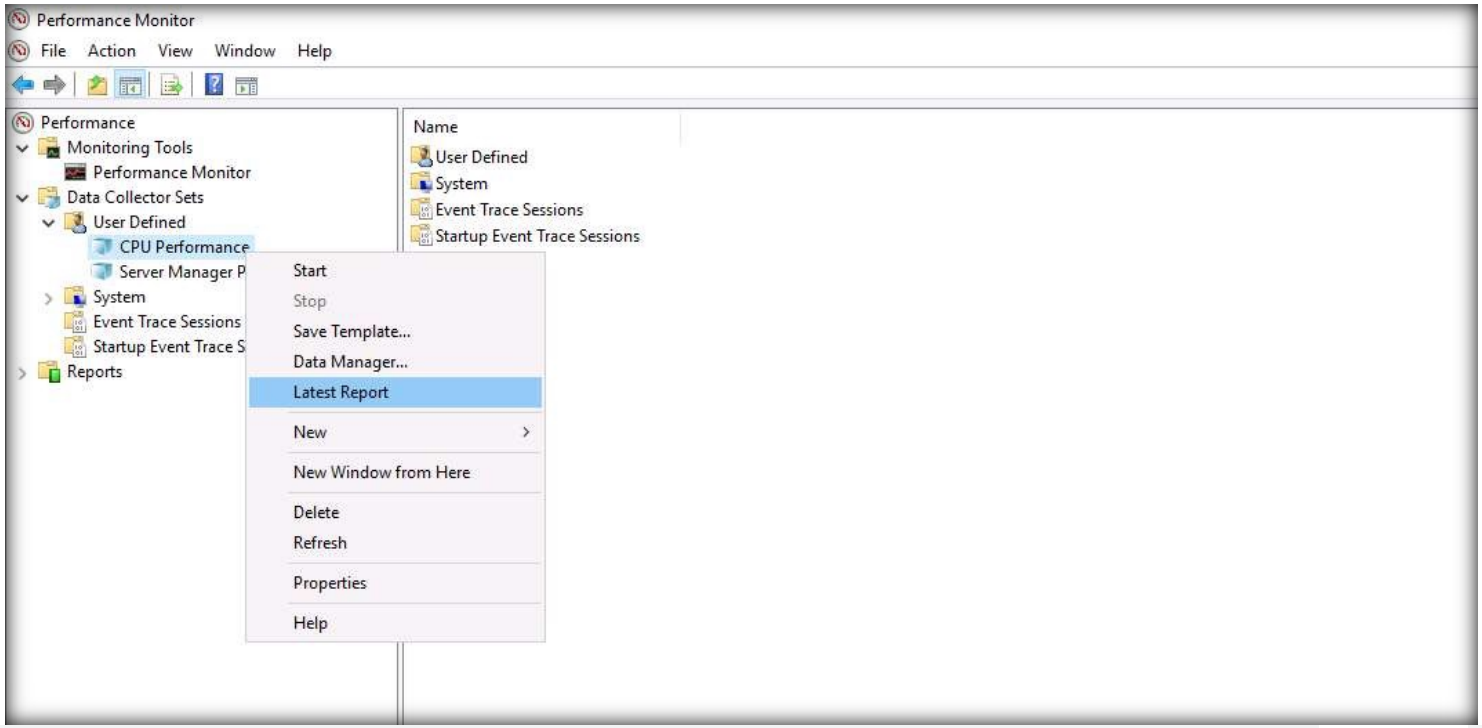
41. In the Performance Monitor window, right-click CPU Performance node from left-pane and click Stop.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



42. Right-click CPU Performance node and click Latest Report.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



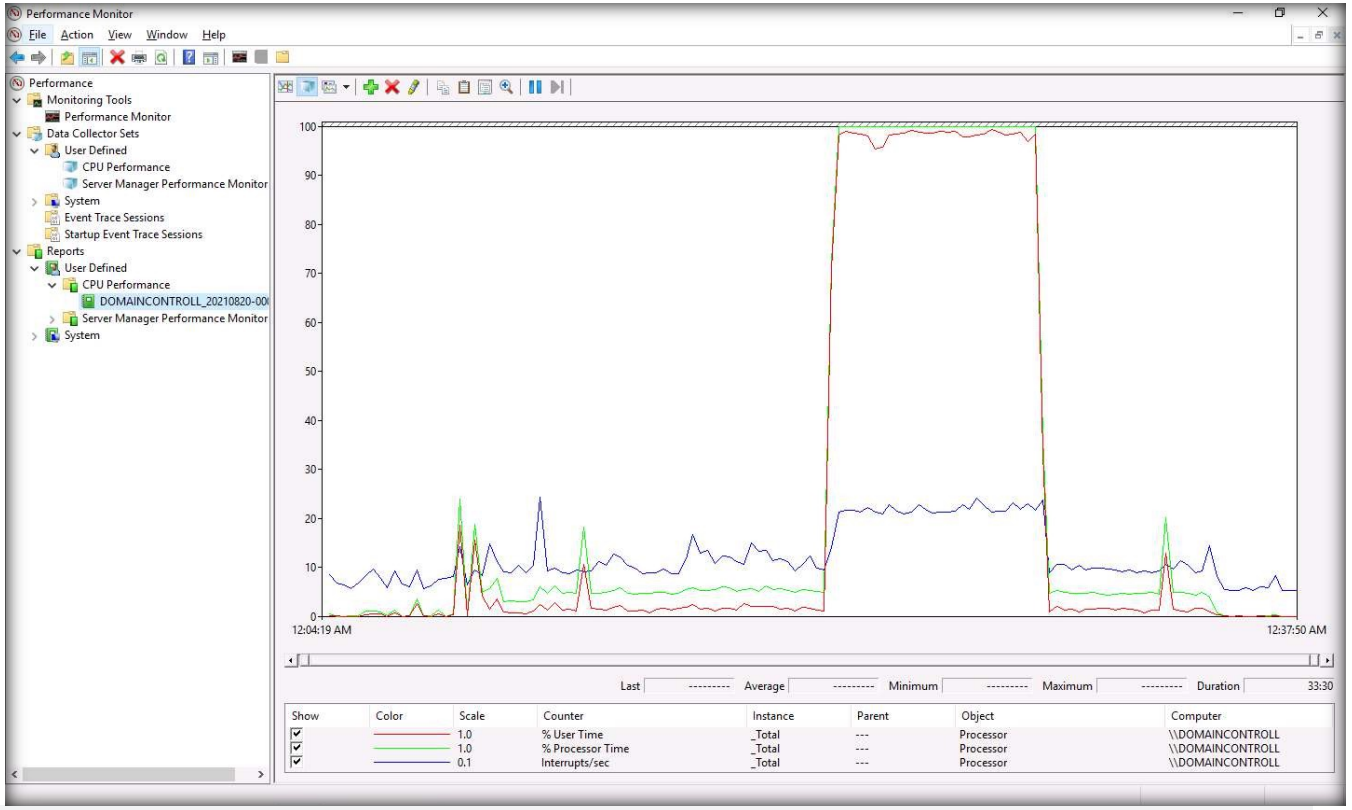
43. A graphical report appears, showing the amount of CPU utilization with respect of time, as shown in the screenshot below.
Note: The graphical report might differ when you perform the lab.

44. This concludes the demonstration showing how to check web application-based attack on the system.

45. Close all open windows.

46. Turn off the AD Domain Controller virtual machine.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



EXERCISE 7: **PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS**

Web server footprinting provides system-level data such as account details, OSs, software versions, server names, and database schema details.

LAB SCENARIO

A security professional must have the required knowledge to perform banner grabbing/footprinting on a target webserver using various footprinting tools.

OBJECTIVE

This lab will demonstrate how to conduct banner grabbing on a target web server using tools such as cURL, Netcat and Wget.

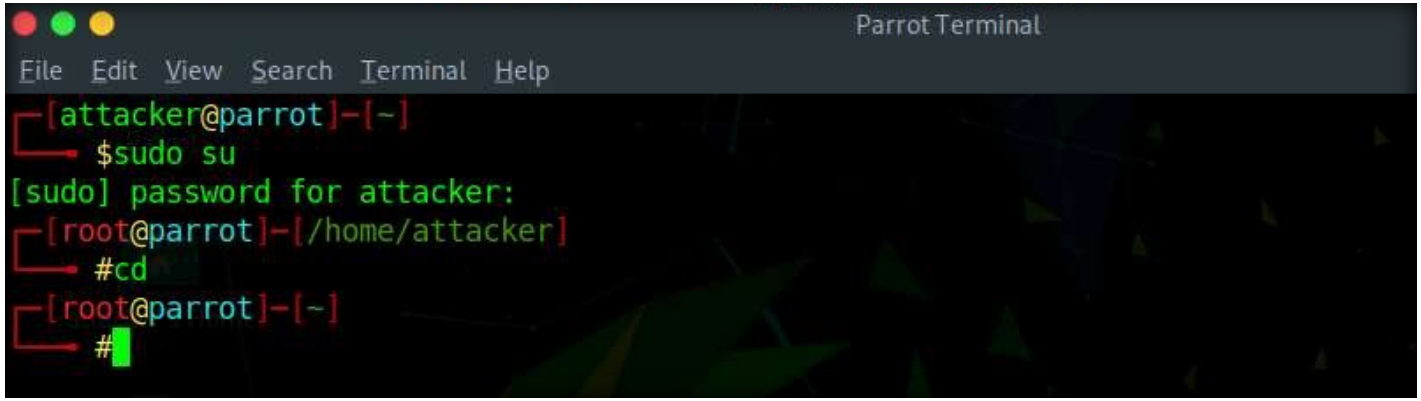
OVERVIEW OF WEB APPLICATION

The purpose of footprinting is to gather information about the security aspects of a web server with the help of tools or footprinting techniques. Through footprinting, the web server's remote access capabilities, its ports and services, and other aspects of its security can be determined. In addition, other valuable system-level data such as account details, OSs, software versions, server names, and database schema details can be gathered. The Telnet utility can be used to footprint a web server and gather information such as server name, server type, OSs, and running applications running. Furthermore, footprinting tools such as Netcraft, ID Serve, and httprecon can be used to perform web server footprinting. These footprinting tools can extract information from the target server.

Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on Attacker Machine-2 and Web Server virtual machines.
2. Switch to the Attacker Machine-2 virtual machine. 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.
Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.
3. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

EXERCISE 7: PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS

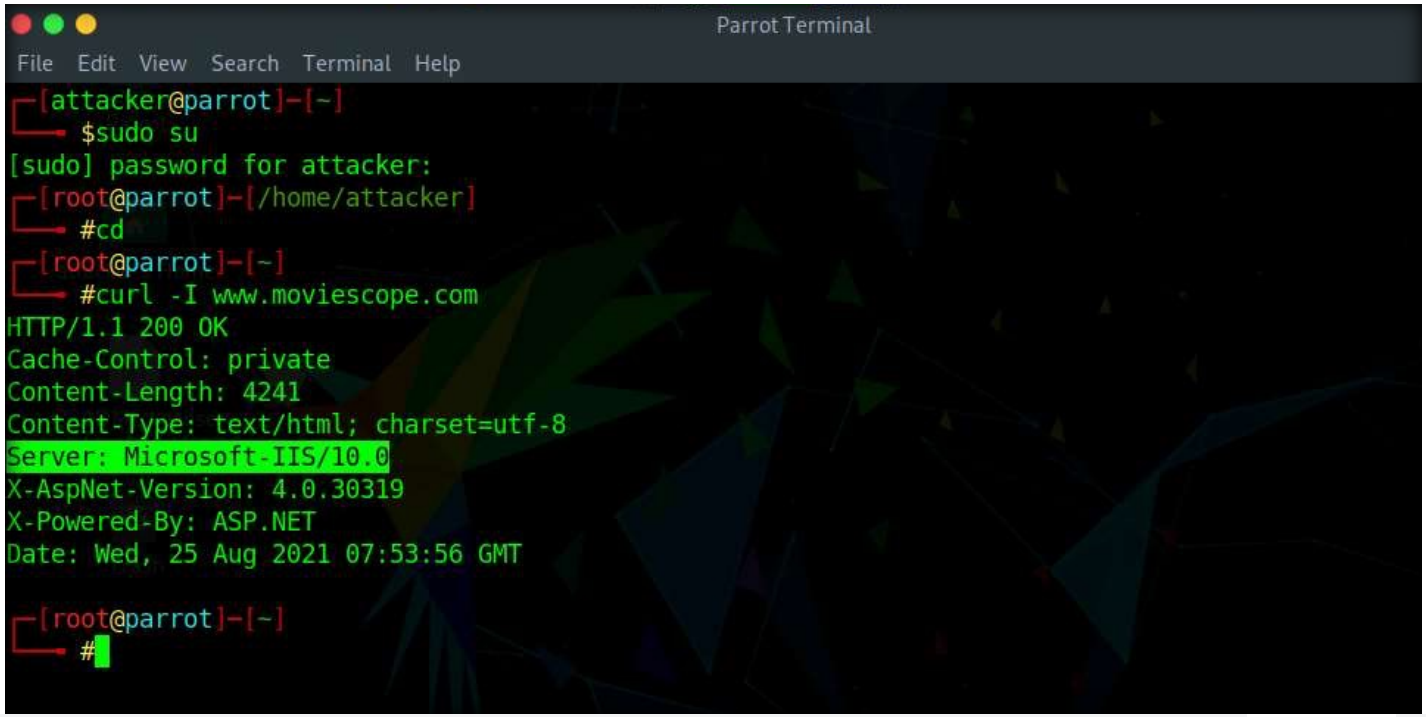
4. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run programs as the root user.
5. In the [sudo] password for attacker field, type toor as a password and press Enter.
Note: The password that you type will not be visible.
6. Now, type cd and press Enter to jump to the root directory.



7. In the Terminal window, type curl -I www.moviescope.com and press Enter to obtain information about services on the target website.
Note: -I: To fetch only HTTP-header.

8. From the Server information, you can observe that the server is running Microsoft-IIS/10.0, as shown in the screenshot below.
Note: cURL is command-line tool for transferring data using various network protocols such as HTTP, FTP, IMAP, SFTP, SMTP, etc.

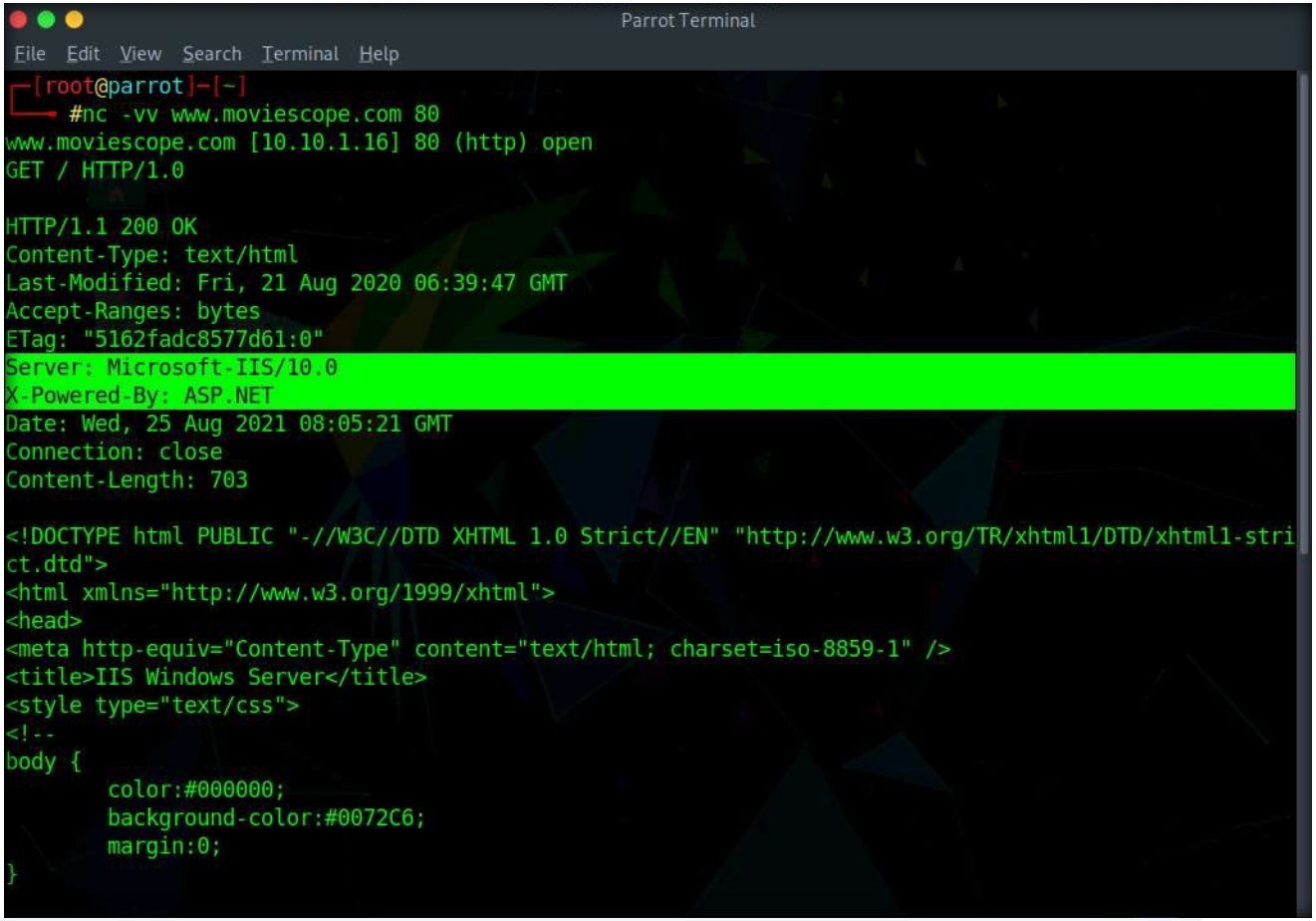
EXERCISE 7: PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS



9. Type nc –vv www.moviescope.com 80 and press Enter to gather information such as server type and version.
Note: -vv: Advanced verbose mode.

10. Connection open prompt appears, type GET / HTTP/1.0 and press Enter twice.
Note: Netcat is a networking utility that reads and writes data across network connections by using the TCP/IP protocol.

EXERCISE 7: PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS

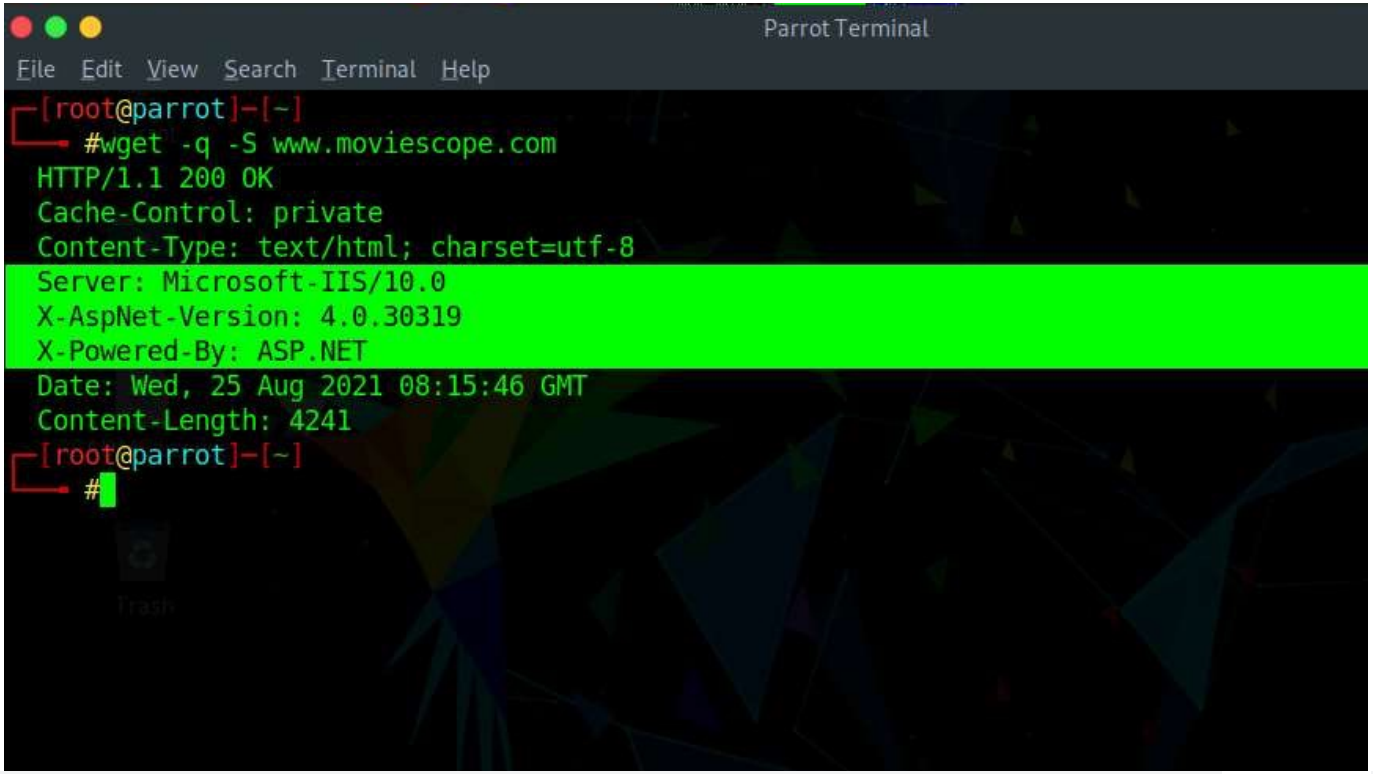


11. Type wget -q -S www.moviescope.com and press Enter to gather HTTP header response.
Note: -q: To turn off wget output, -S: To print HTTP headers.

12. You can observe the HTTP information obtained, as shown in the screenshot below.
Note: GNU Wget is a utility to retrieve content from Web Server.

13. This concludes the demonstration showing how to perform banner grabbing/footprinting on the target website.
14. Close all open windows.
15. Turn off Attacker Machine-2, Web Server, and PfSense Firewall virtual machines.

EXERCISE 7: PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS




EC-Council