

CHAPTER 9

APPLICATION SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 9: Application Security

Exercise 1:

Implement Application Whitelisting using AppLocker

05

Exercise 2:

Blacklist Application using ManageEngine Desktop Central

49

Exercise 3:

Perform Application Sandboxing using Sandboxie

75

Exercise 4:

Detect Web Application Vulnerabilities using OWASP ZAP

83

Exercise 5:

Detect Injection Vulnerability using Burp Suite

92

Exercise 6:

Determine Application-Level Attacks

119

Exercise 7:

Perform Web Server Footprinting using Various Footprinting Tools

144

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 An outdated or insecure application can pose a serious security threat and, in turn, affect network security.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.

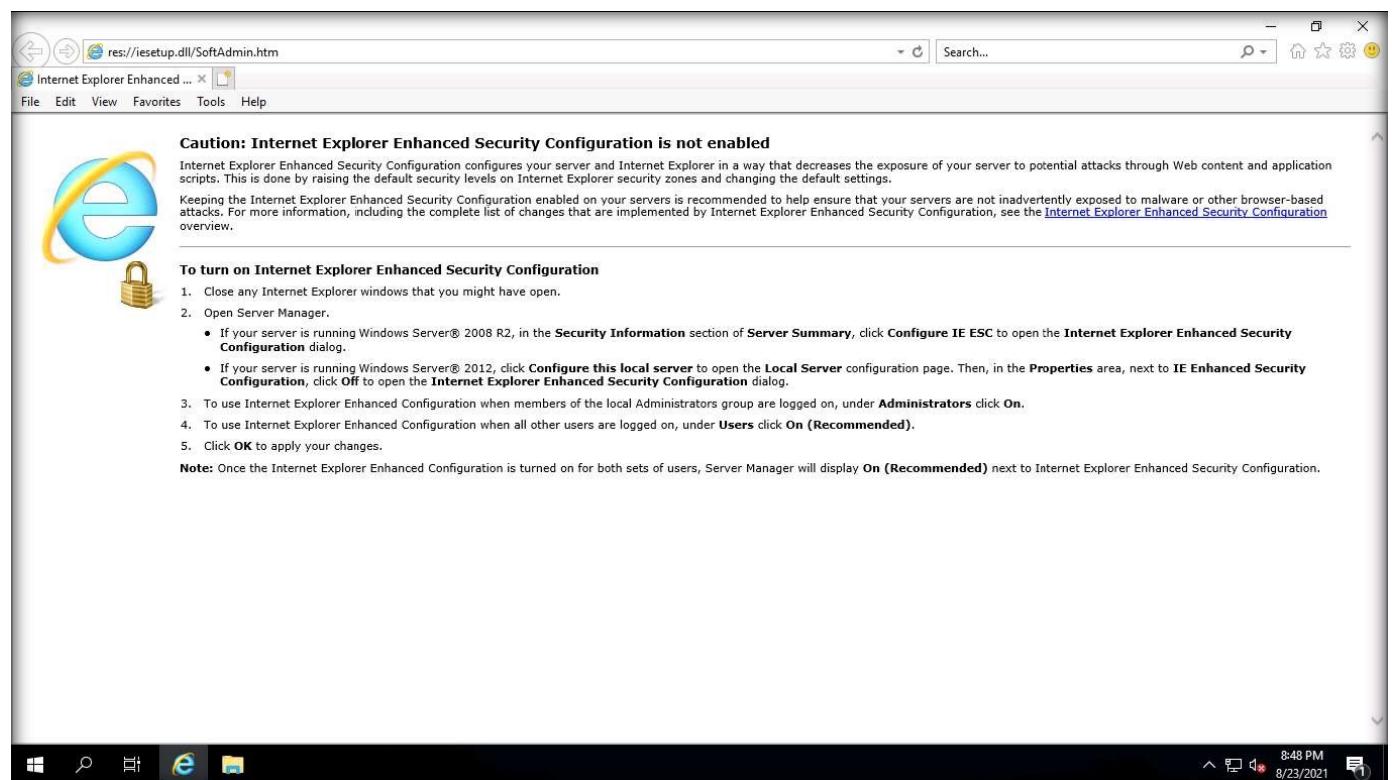
Note: If the network screen appears, click Yes.

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 APPLCKER

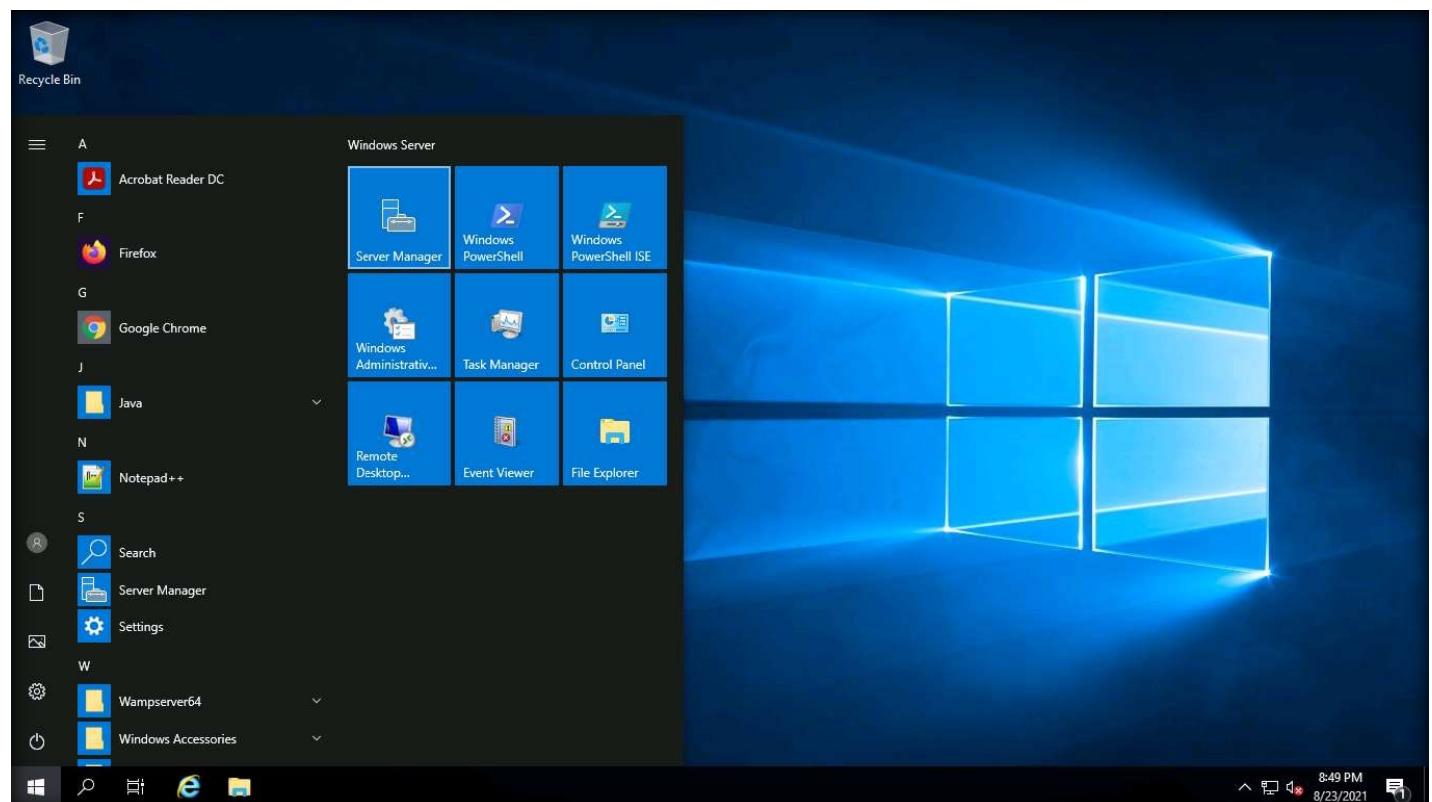


Note: As per policy, employees of several organizations are barred from using Internet Explorer. In this case, a security professional must know how to block Internet Explorer using AppLocker.

5. The Internet Explorer can be blocked using AppLocker.

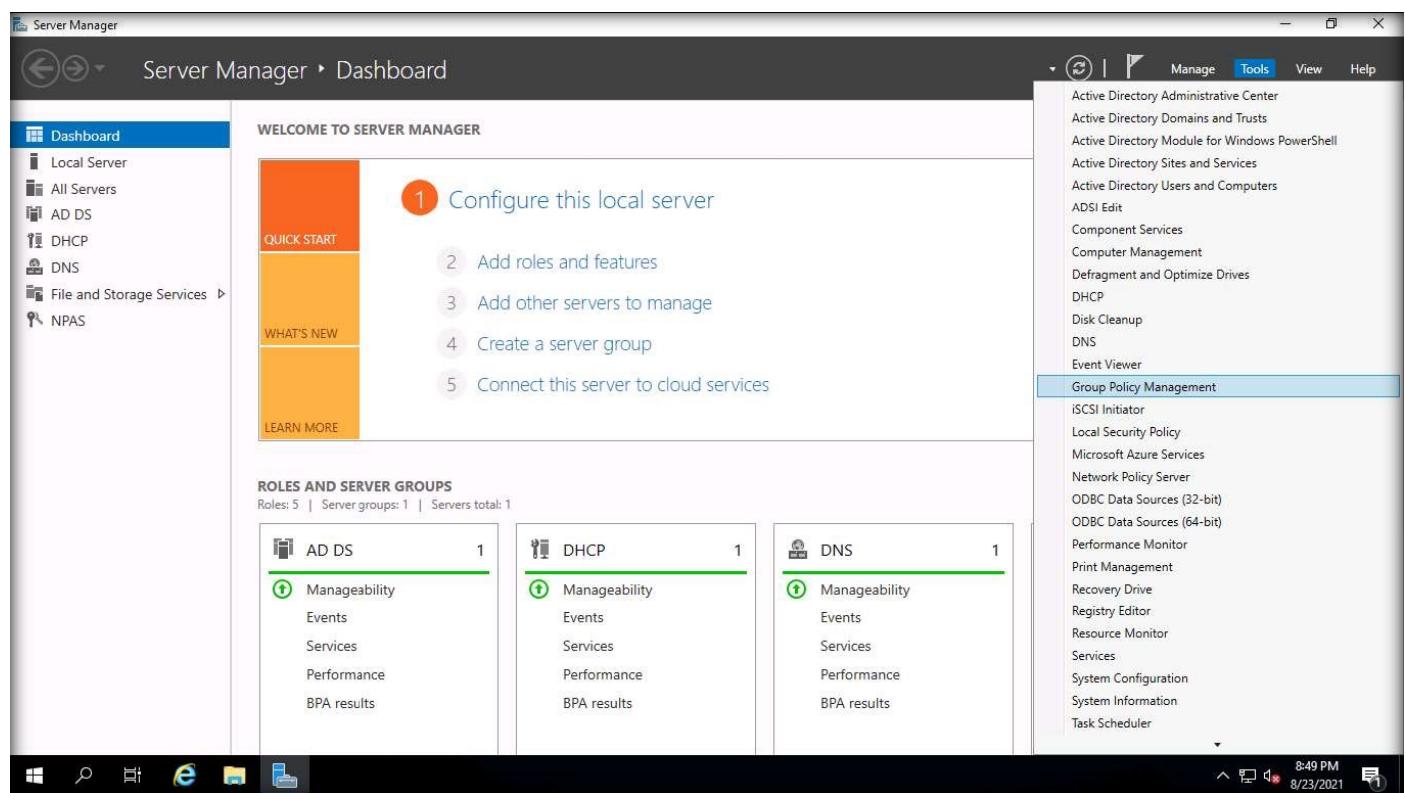
6. Click on Windows Start icon, select Server Manager.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



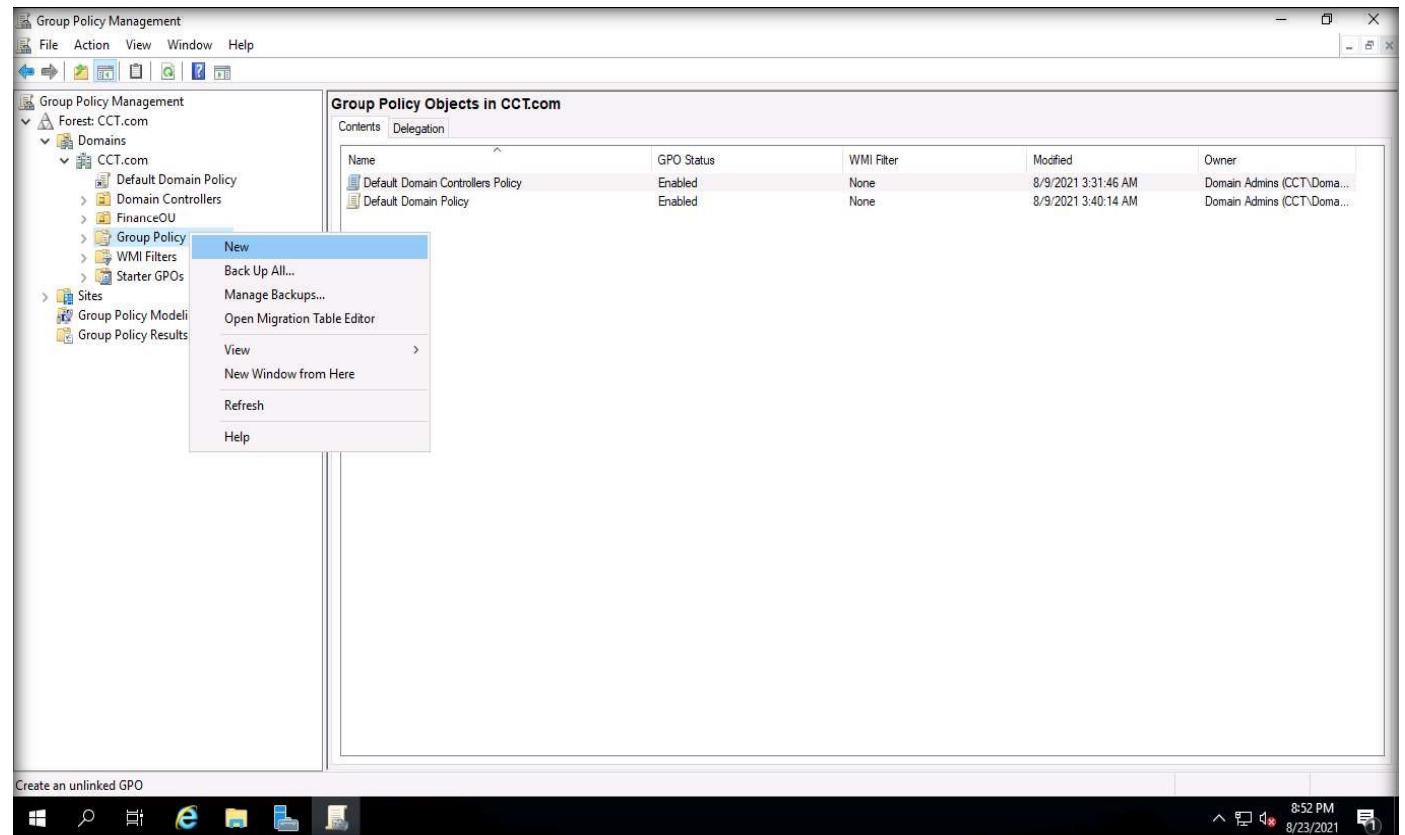
7. The Server manager window will open, navigate to the Tools menu, and select Group Policy Management.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

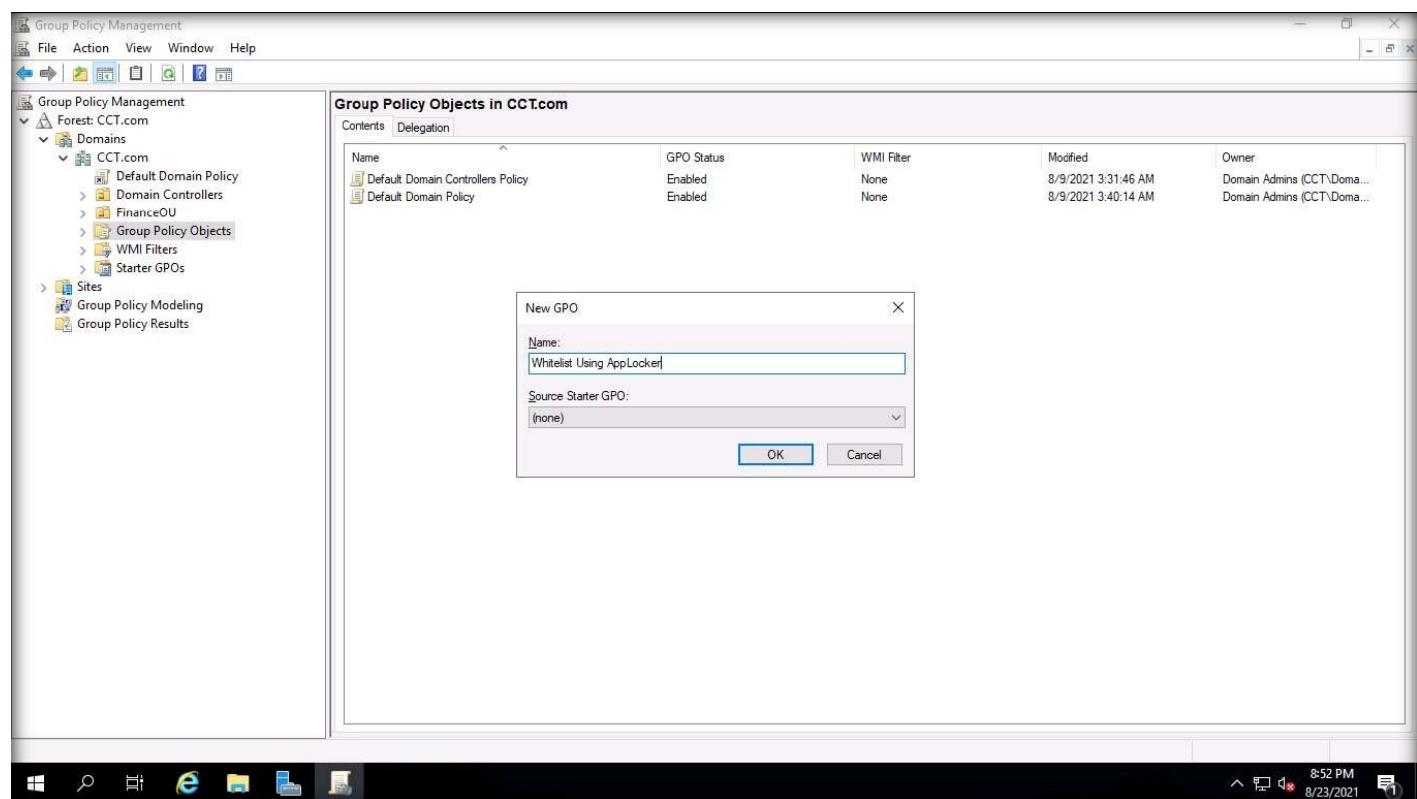


8. The Group policy Management window will open. Expand Forest: CCT.com, Domains, and CCT.com, navigate and select Group Policy Objects. Right-click on the Group Policy Objects (GPO) and select New.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

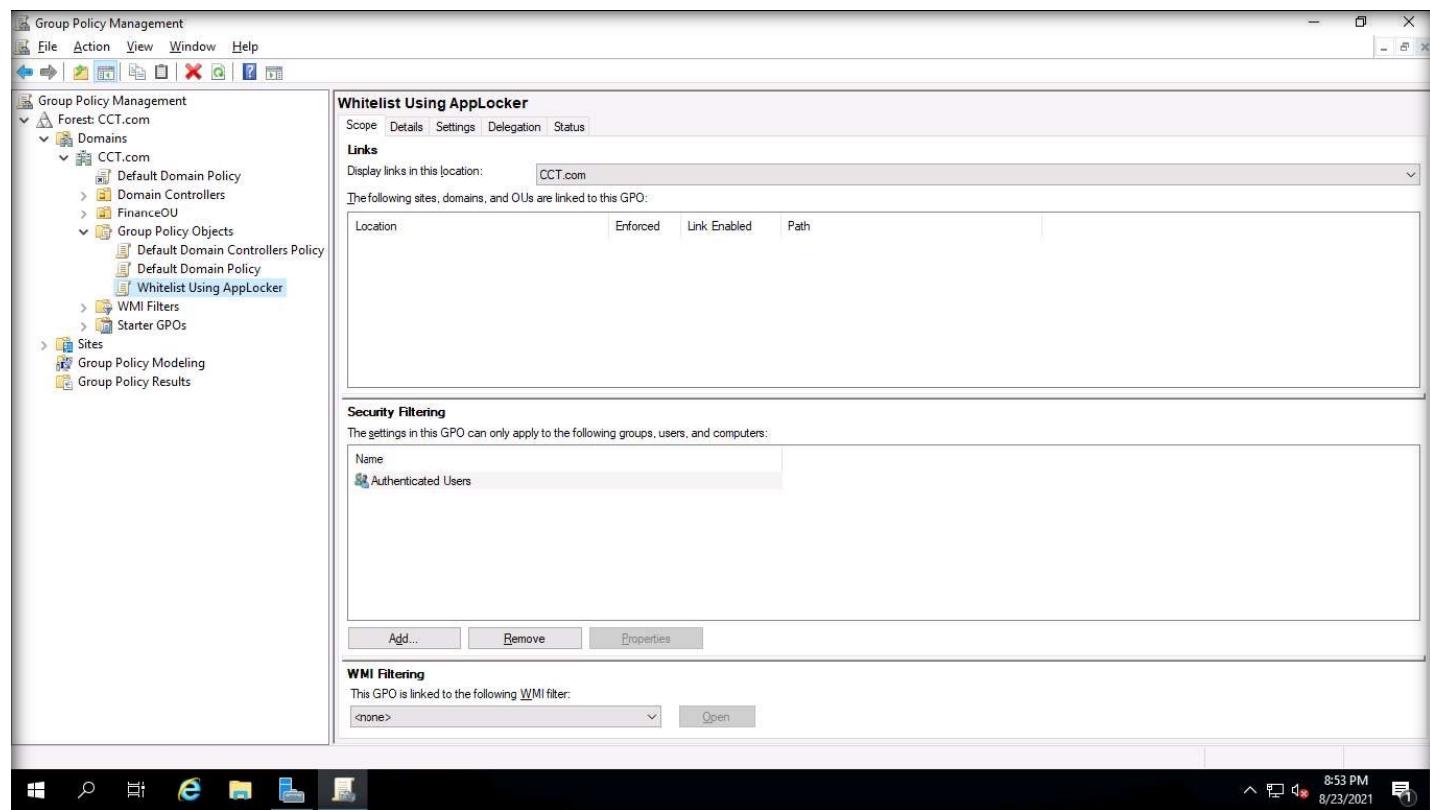


EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



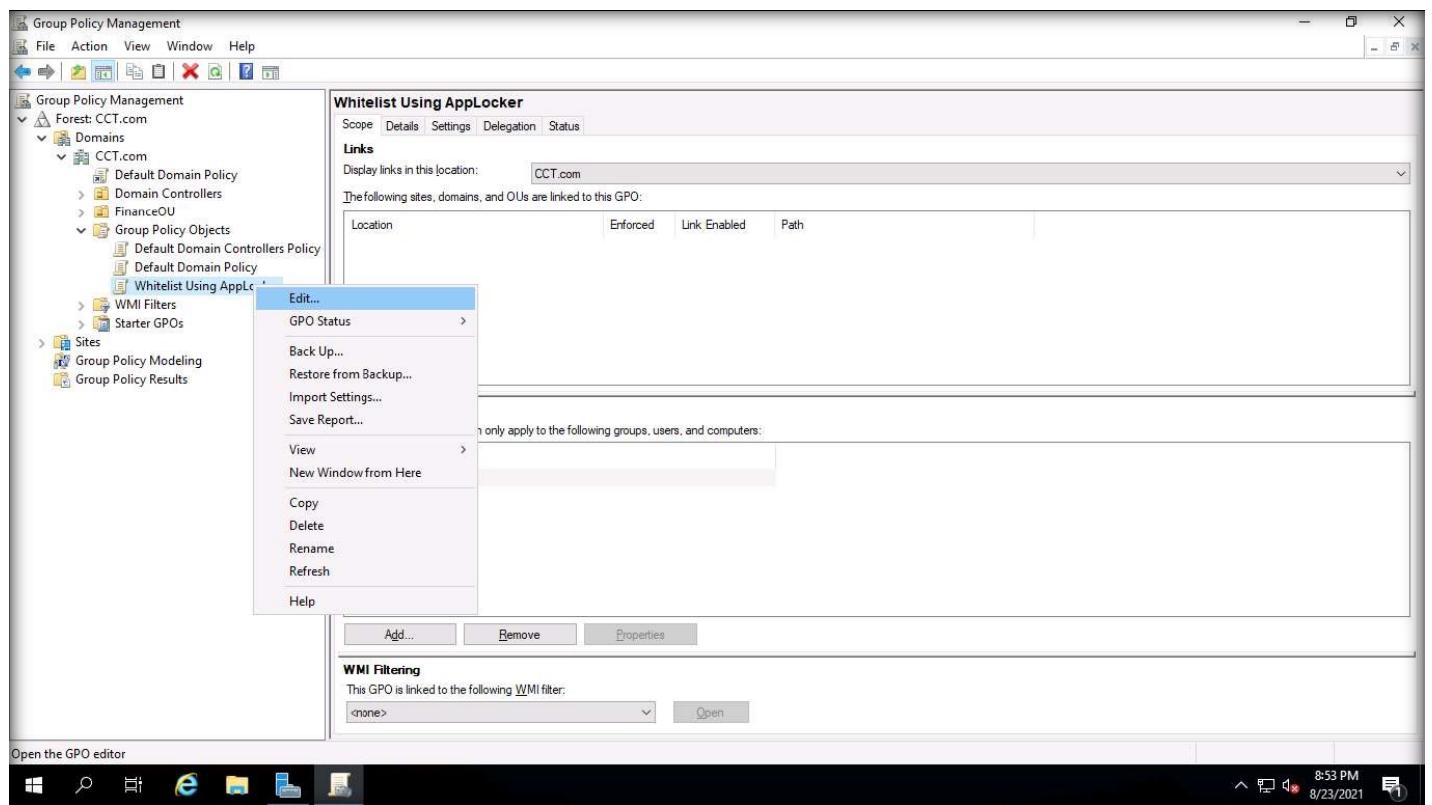
10. A new GPO named Whitelist Using AppLocker will be created in the Group Policy Objects folder.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

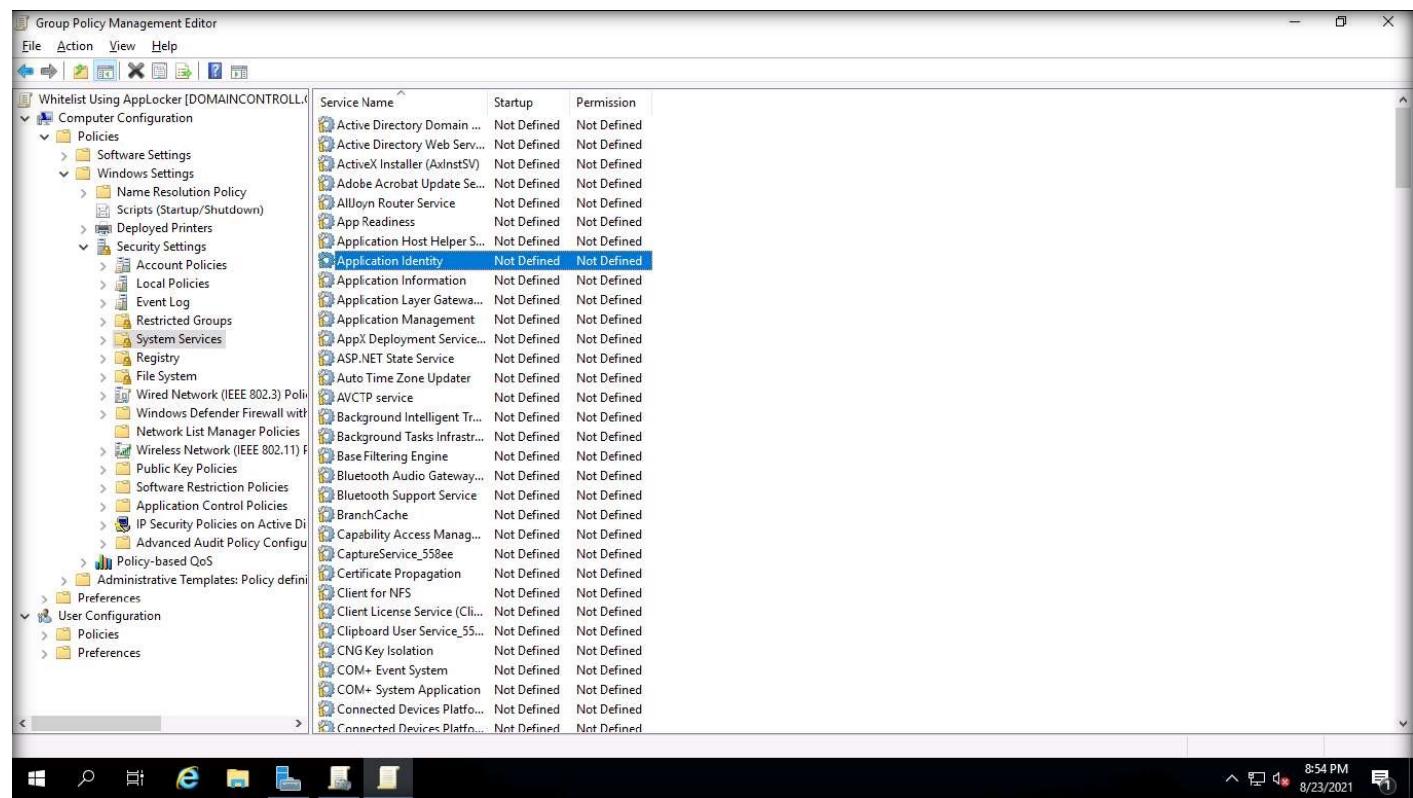
11. Right-click on the Whitelist Using AppLocker and select the Edit option.



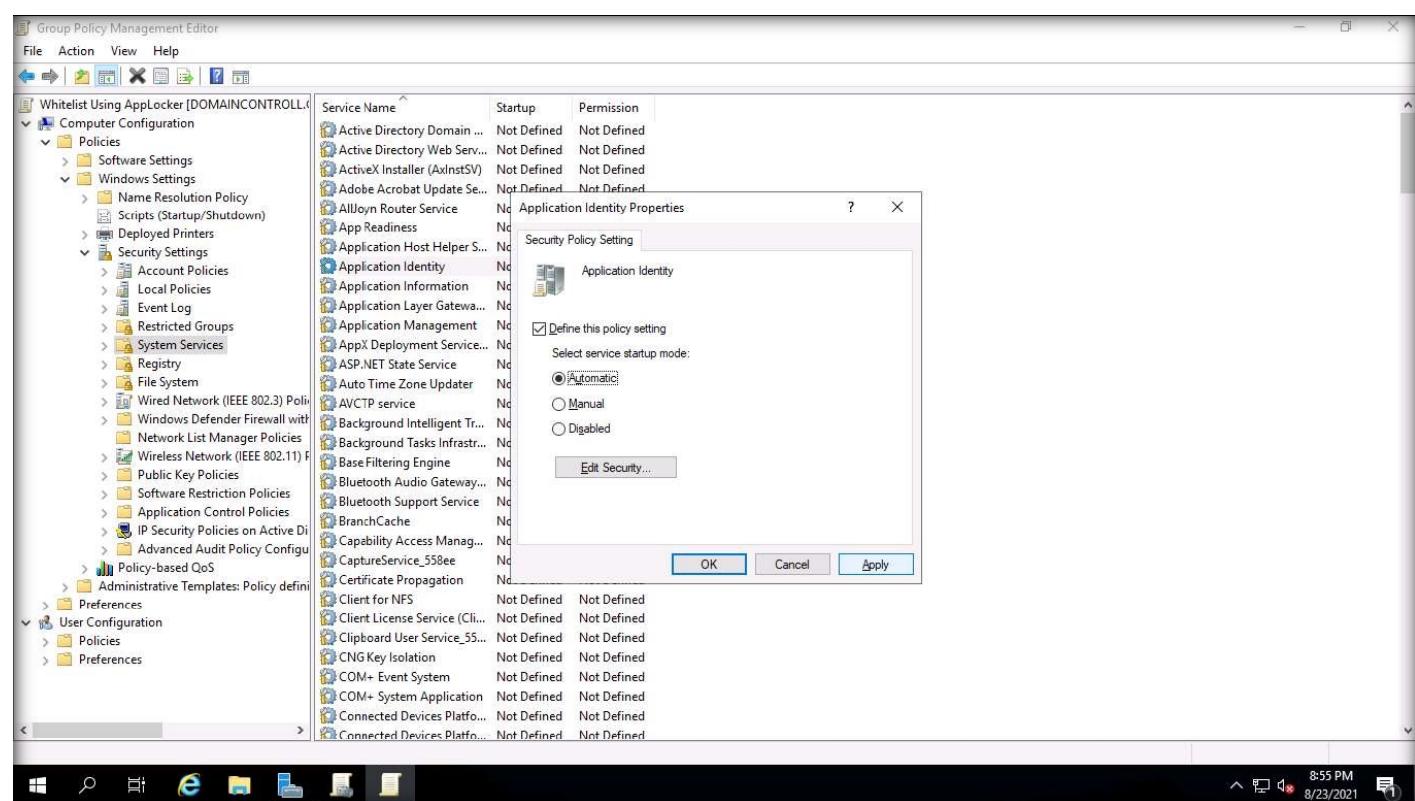
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

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.



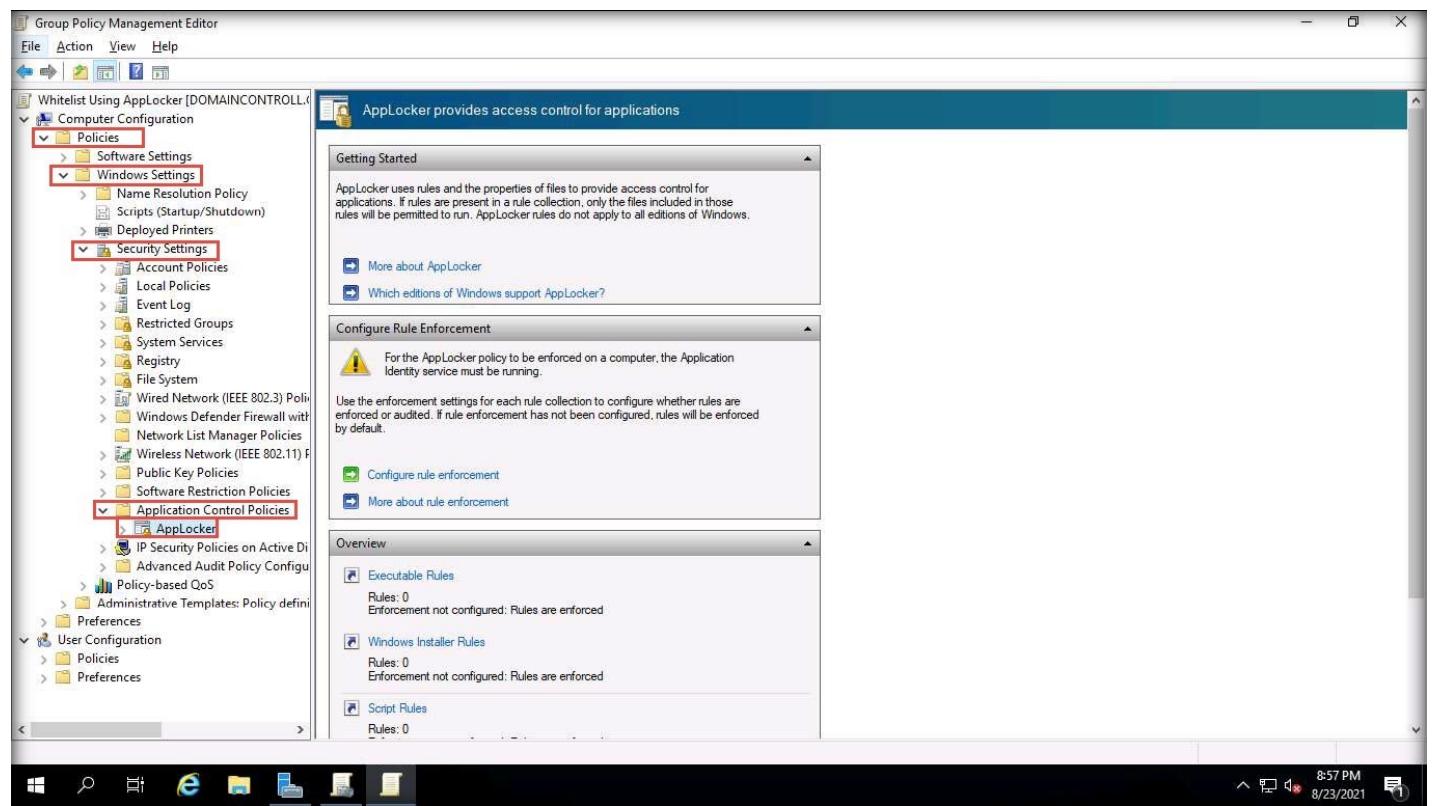
14. The Application Identity Properties window opens, check Define this policy setting, select Automatic, and click on Apply and OK.



EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

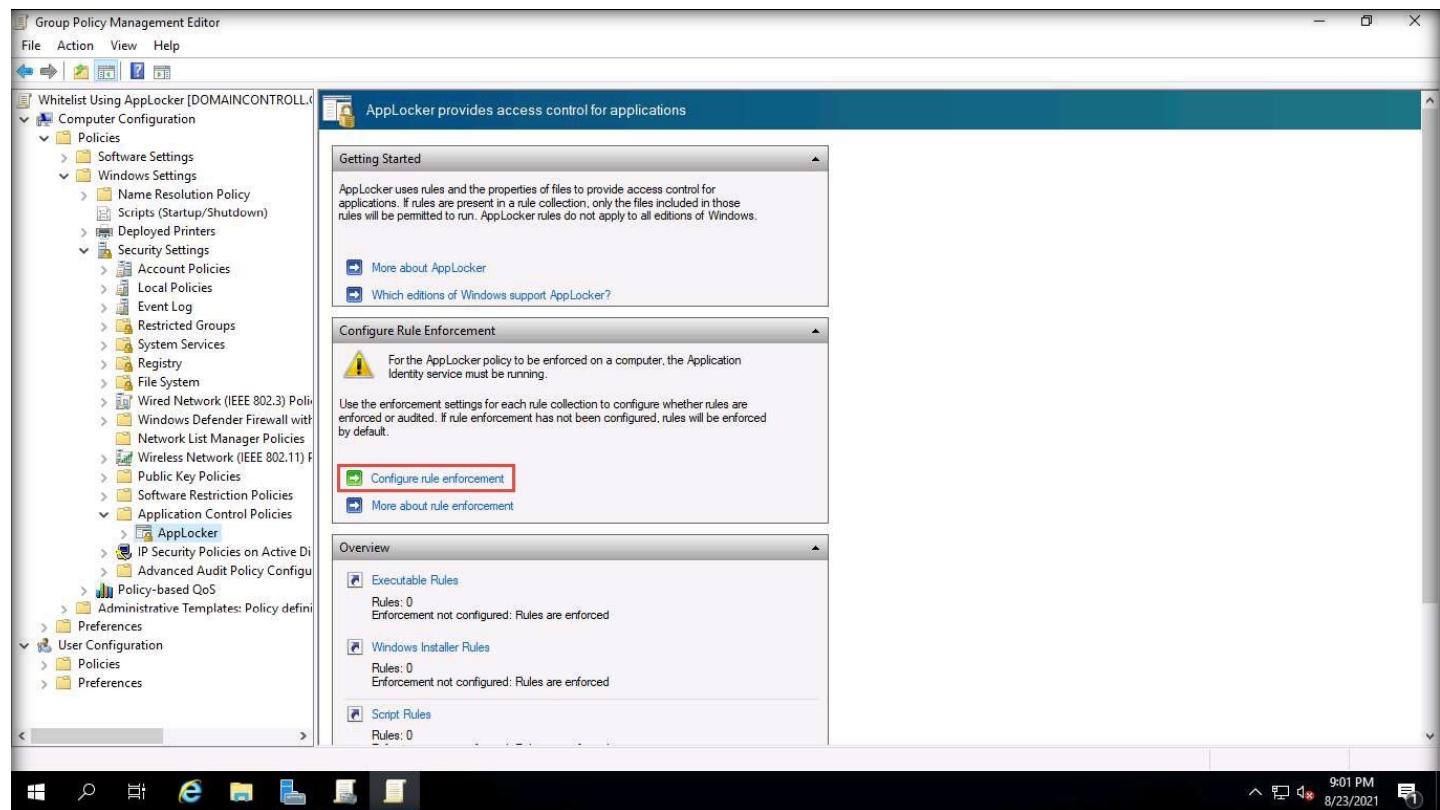
15. Next, scroll down under the left sidebar and navigate to Computer configuration → Policies → Windows Settings → Security Settings → Application Control Policies. Expand Application Control Policies, select and click on AppLocker.

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.

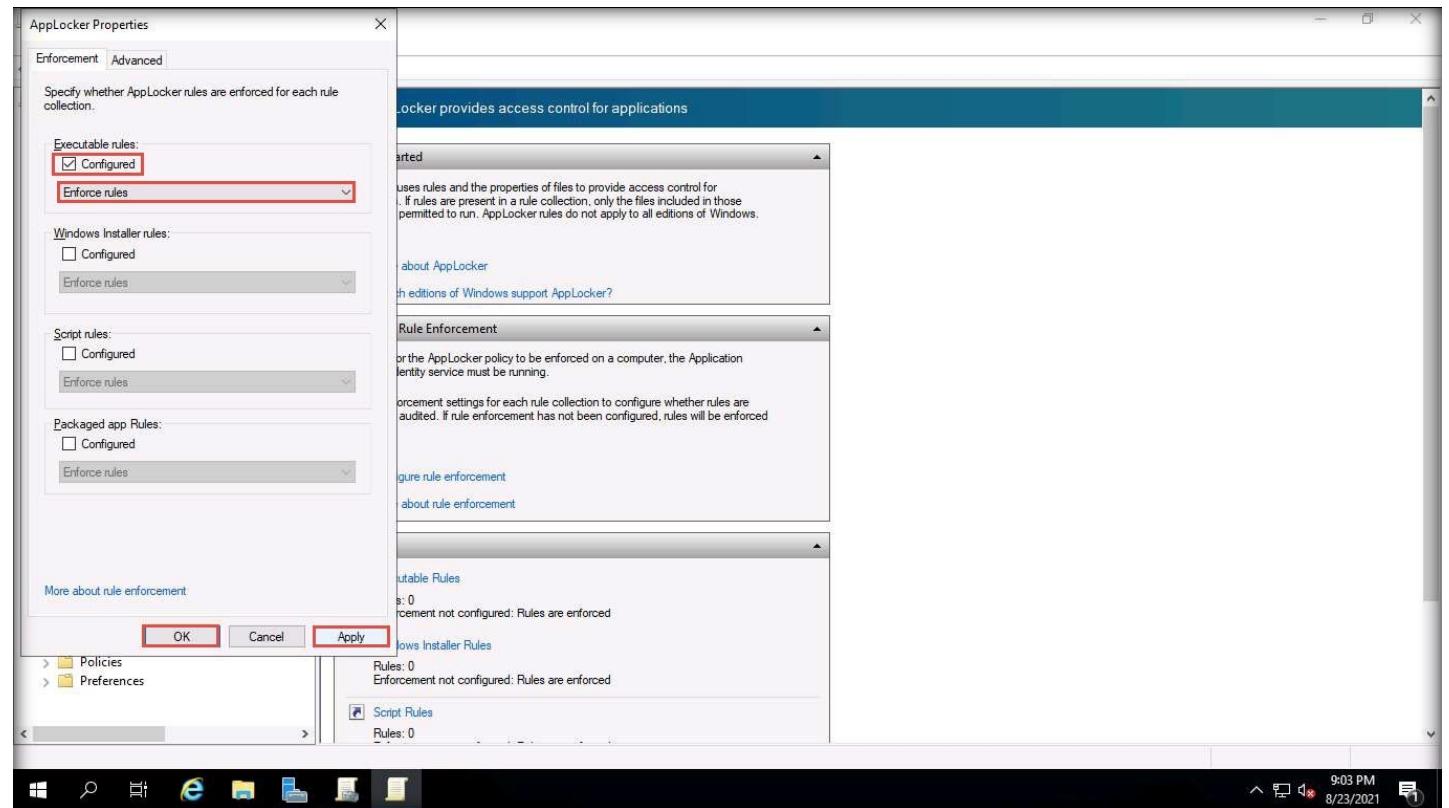
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



EXERCISE 1:
IMPLEMENT
APPLICATION
WHITELISTING USING
APPLocker

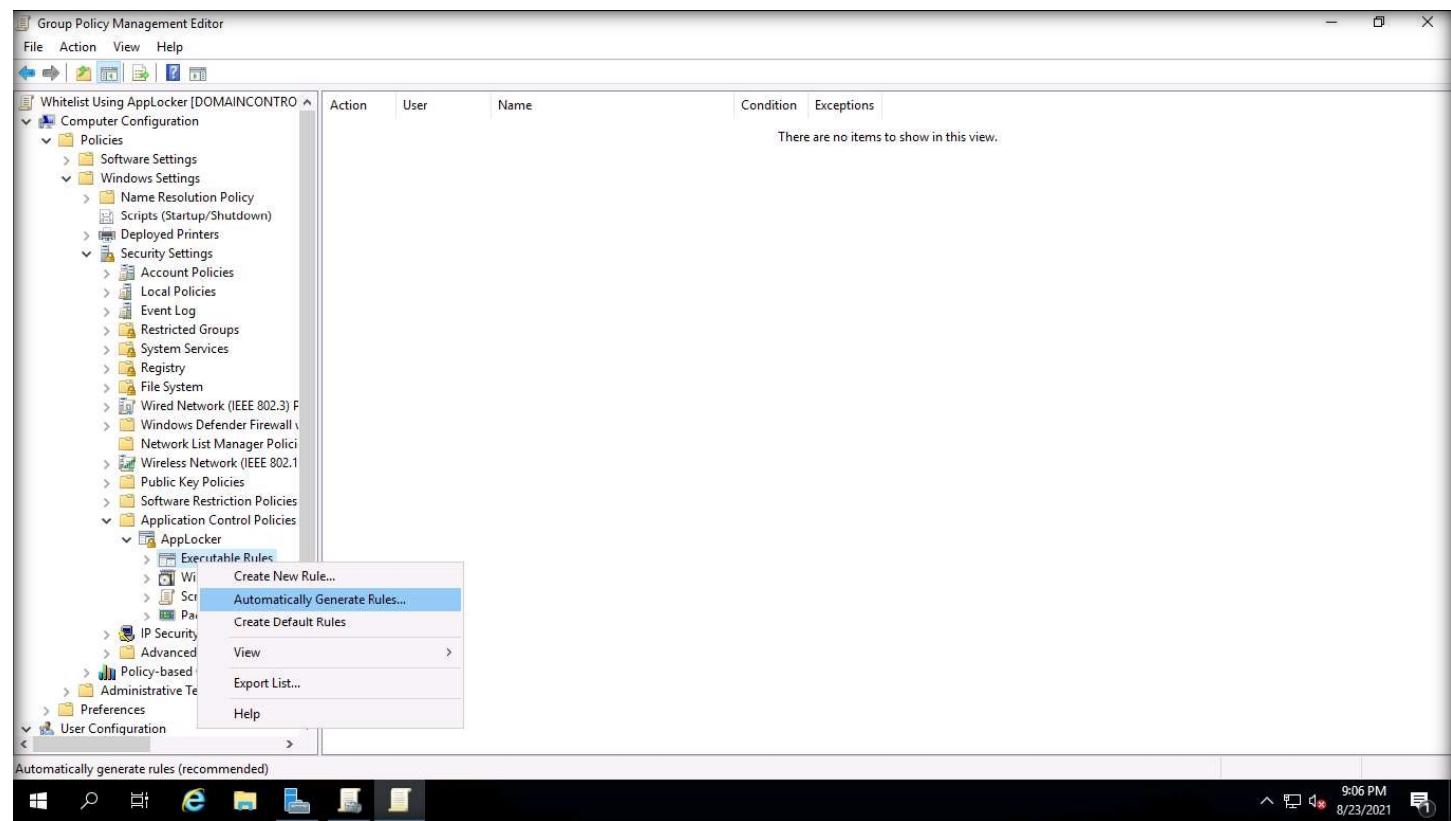
17. The AppLocker Properties window appears, here, the security professional can choose various enforcement rules to configure AppLocker. We choose the first option, that is, Executable rules: Configured.

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)

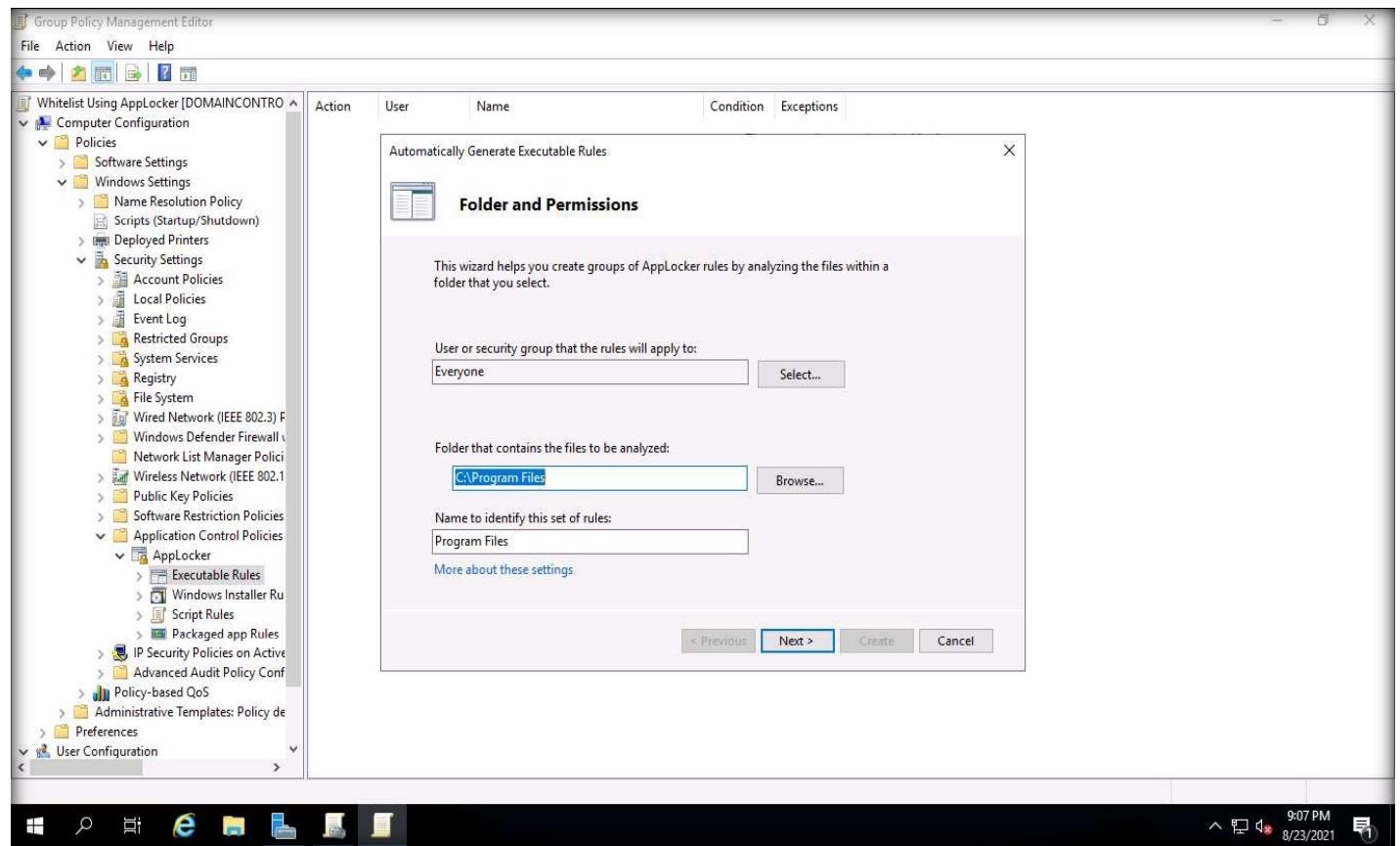


19. Expand AppLocker and right-click on the Executable Rules tab. Select Automatically Generate Rules....

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

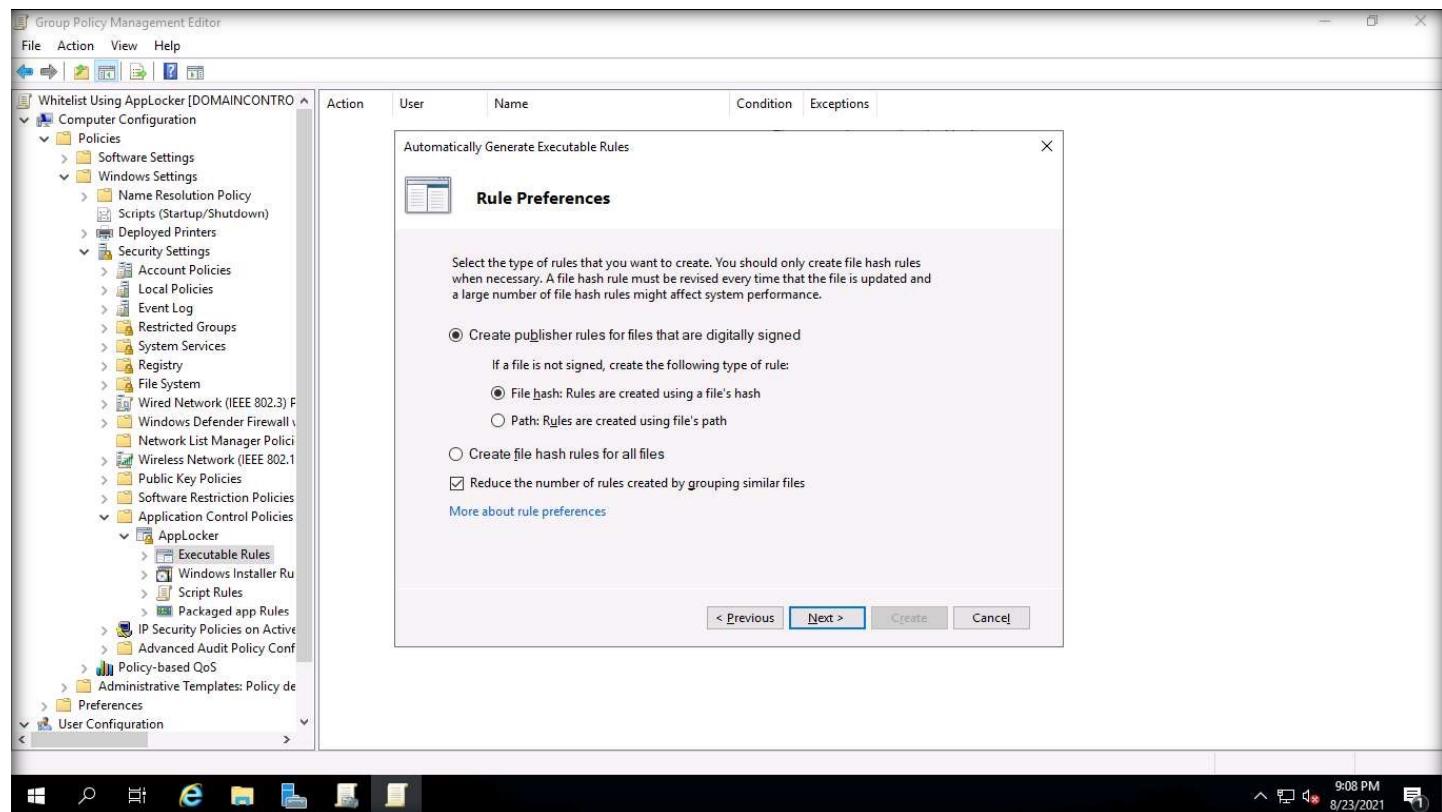


20. The Automatically Generate Executable Rules wizard appears, retain the default options and click on Next.



EXERCISE 1:
IMPLEMENT
APPLICATION
WHITELISTING USING
APPLocker

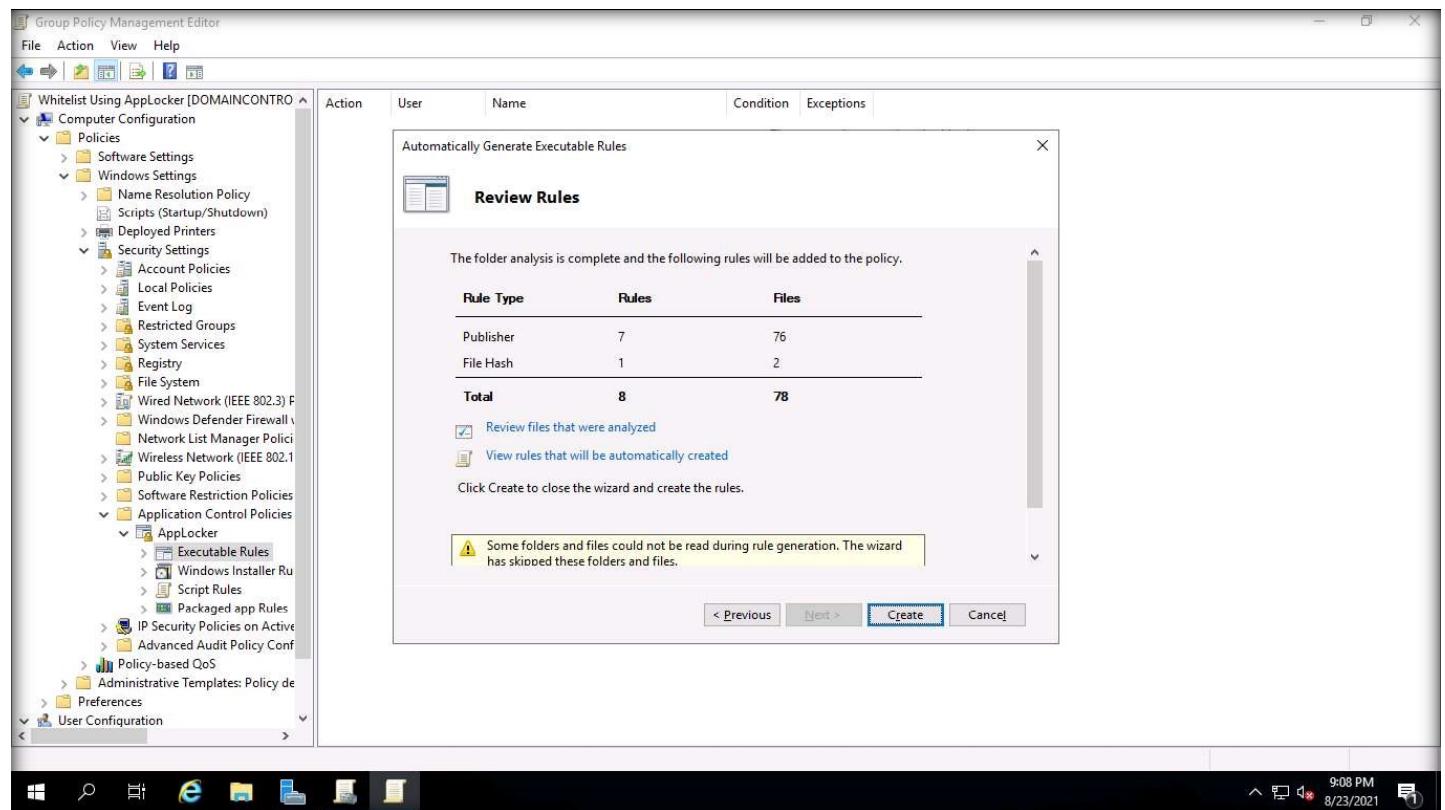
21. Retaining the default publisher rules, click on Next.



22. Once the rules are generated, you will be able to review publisher rules. Click on Create.

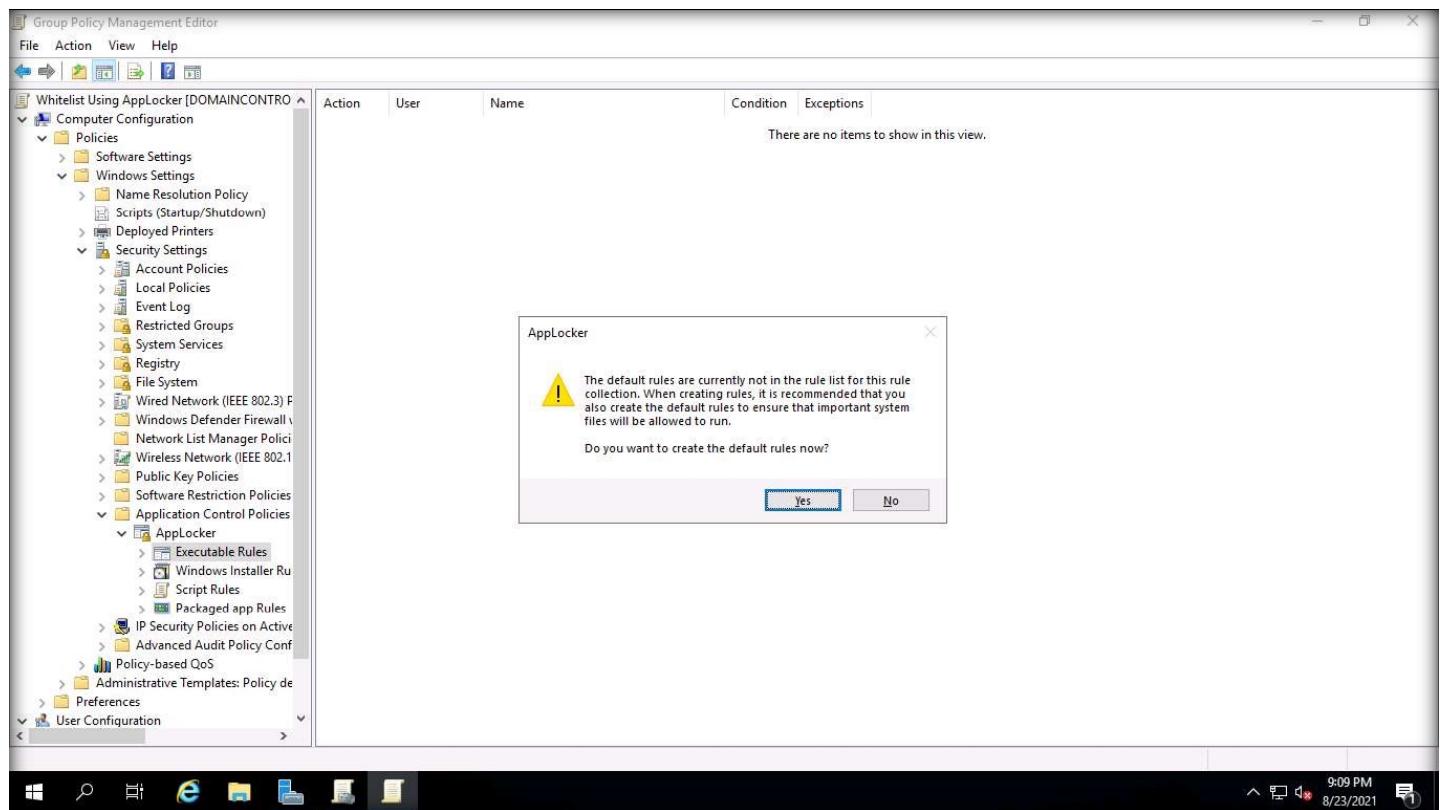
Note: The number of Rules and Files might differ in your lab environment.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



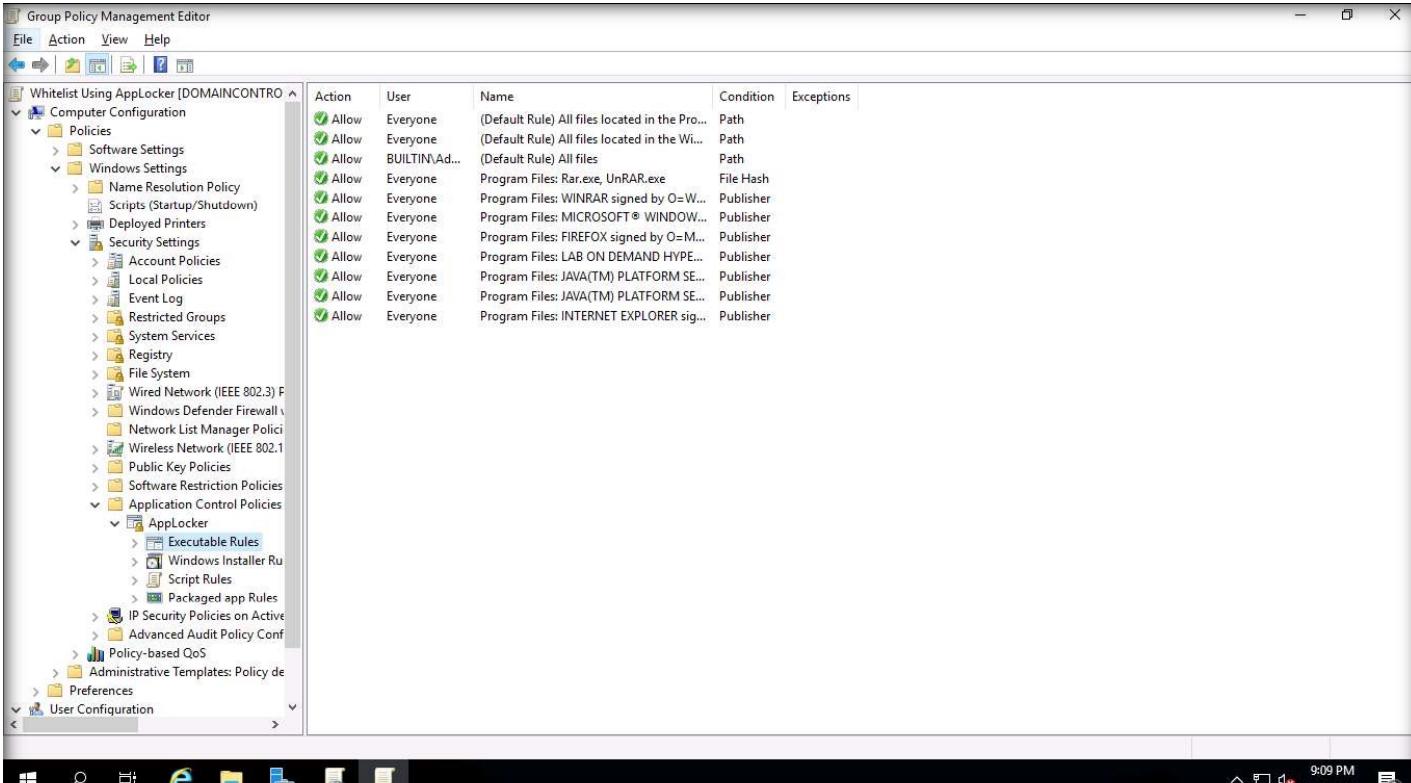
23. The default rule creation alert message box appears, click on Yes; this will automatically generate the executable rules.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



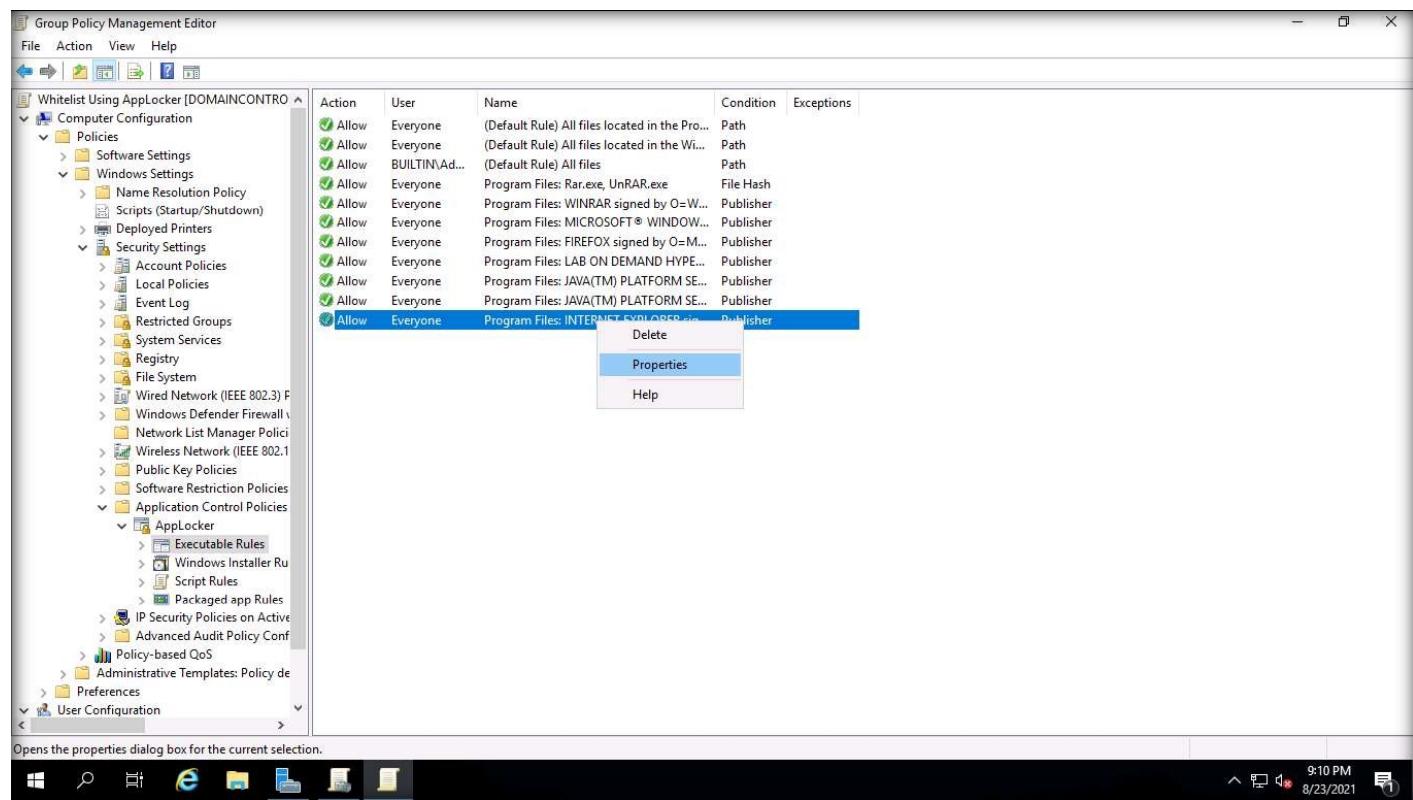
24. In the above list, the automatically generated rule for Internet Explorer is whitelisted. However, our intent is to deny user's access to Internet Explorer. The below steps demonstrate how to deny access to Internet Explorer using AppLocker.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



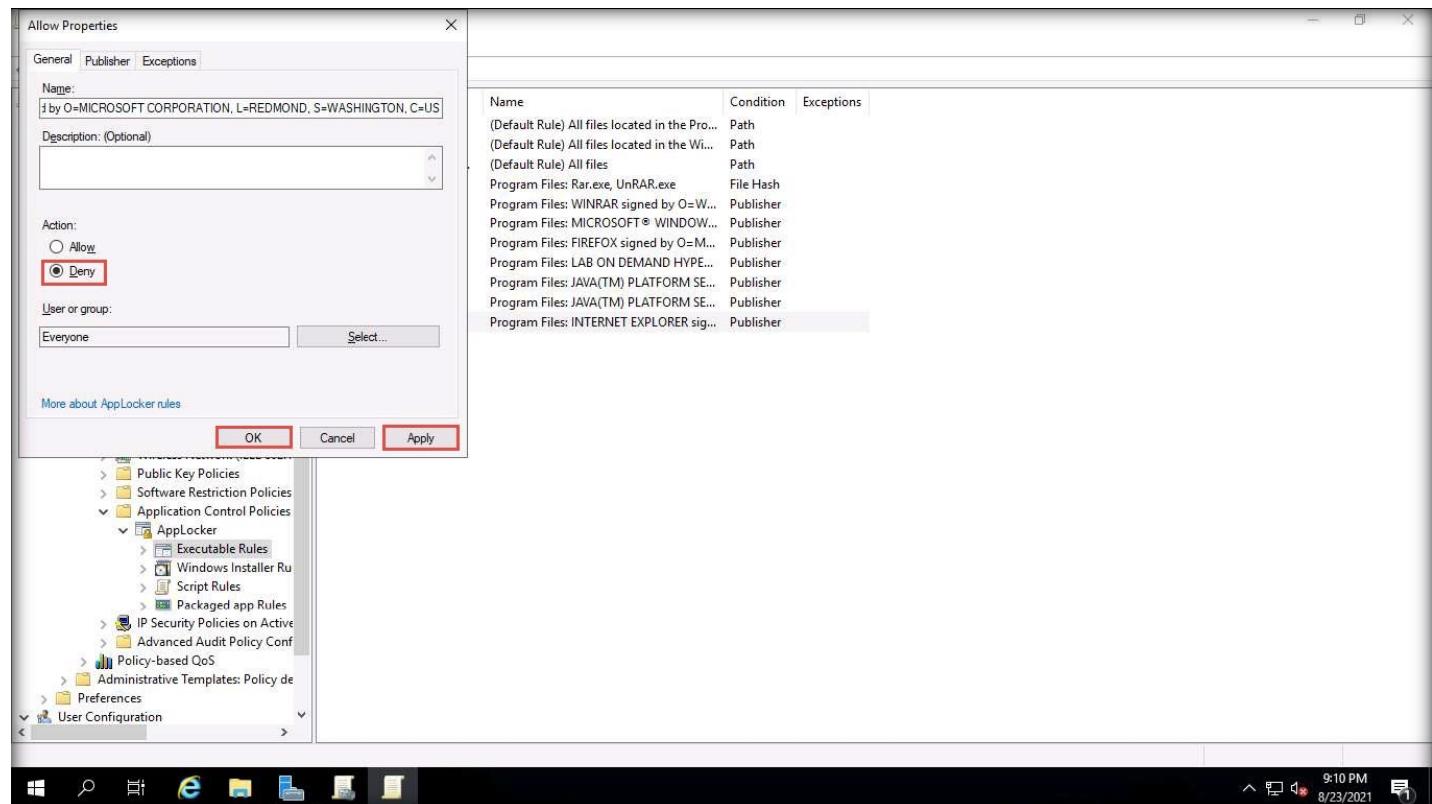
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	Program Files: Rar.exe, UnRAR.exe	File Hash	
Allow	Everyone	Program Files: WINRAR signed by O=WinRAR...	Publisher	
Allow	Everyone	Program Files: MICROSOFT® WINDOW...	Publisher	
Allow	Everyone	Program Files: FIREFOX signed by O=Mozilla...	Publisher	
Allow	Everyone	Program Files: LAB ON DEMAND HYPE...	Publisher	
Allow	Everyone	Program Files: JAVA(TM) PLATFORM SE...	Publisher	
Allow	Everyone	Program Files: JAVA(TM) PLATFORM SE...	Publisher	
Allow	Everyone	Program Files: INTERNET EXPLORER sig...	Publisher	

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



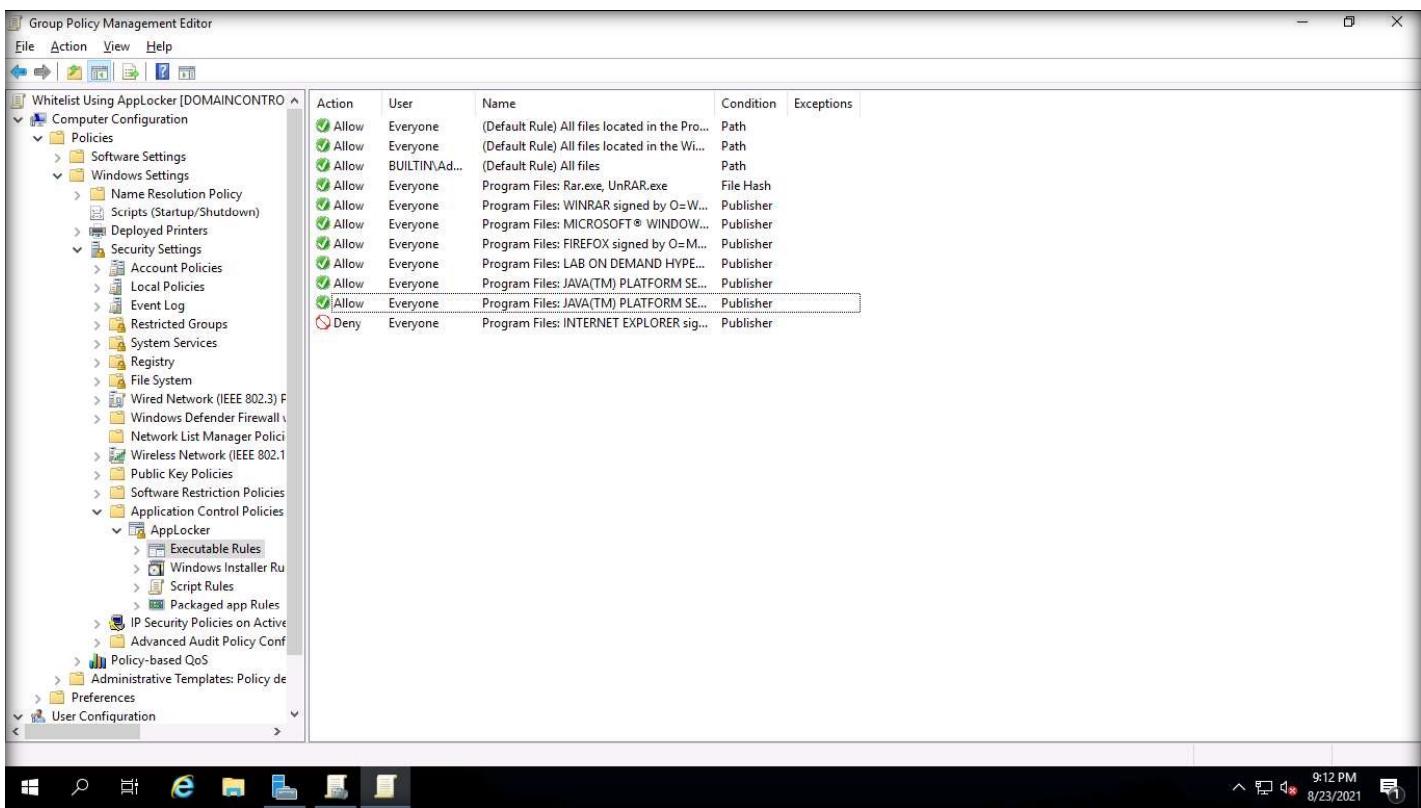
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

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



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

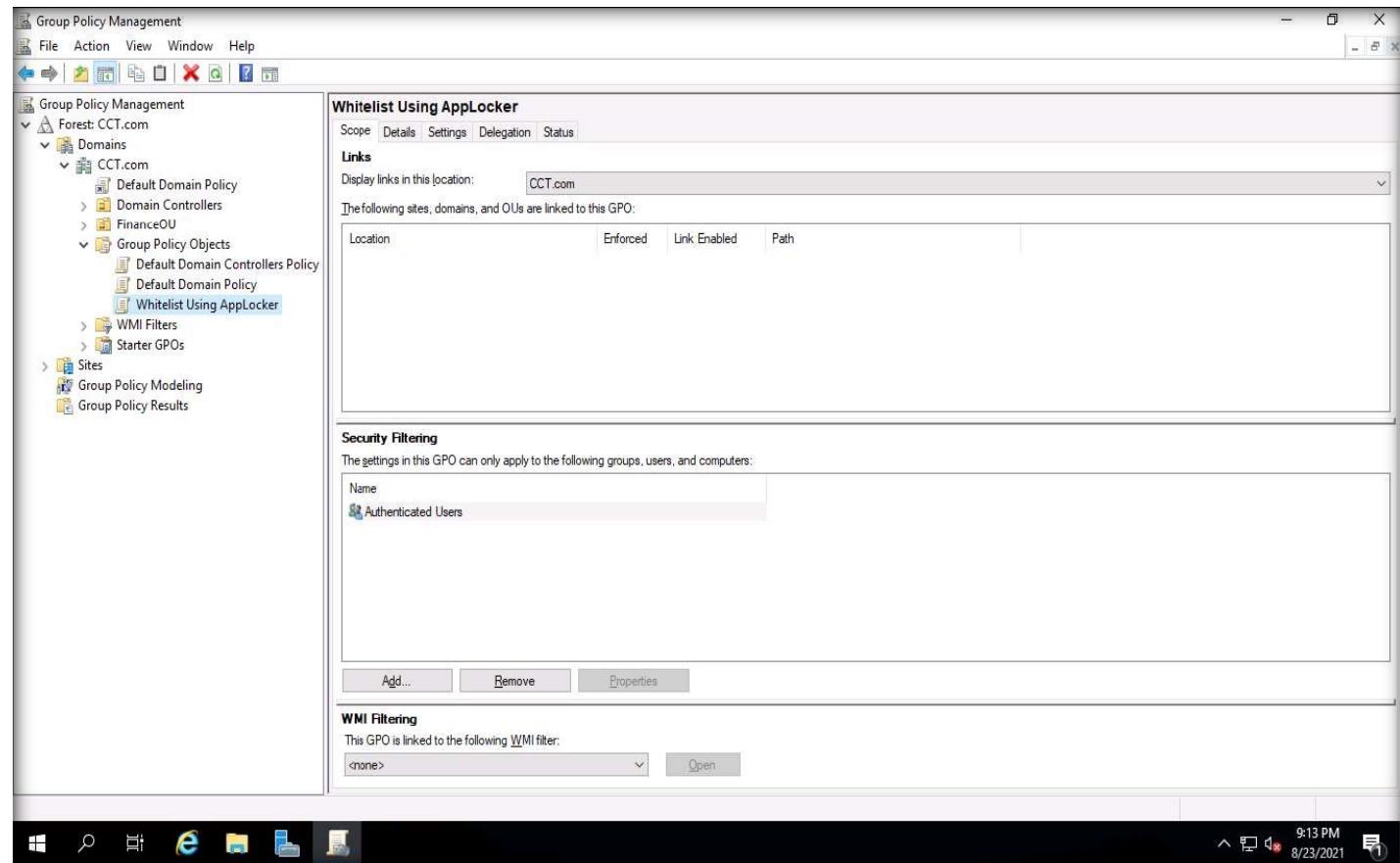
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



The screenshot shows the Group Policy Management Editor window. The left pane displays a tree structure under 'Computer Configuration' with 'Policies' expanded, showing various policy categories like Software Settings, Windows Settings, Security Settings, Application Control Policies, and AppLocker. The right pane is a table titled 'Whitelist Using AppLocker [DOMAINCONTRO...' showing a list of rules. The table has columns for Action, User, Name, Condition, and Exceptions. There are ten 'Allow' rules listed, each with a green checkmark icon. The last rule in the list is a 'Deny' rule, indicated by a red crossed-out checkmark icon, which is highlighted with a red box. The rule details are: Action: Deny, User: Everyone, Name: Program Files: INTERNET EXPLORER sig..., Condition: Publisher, Exceptions: None.

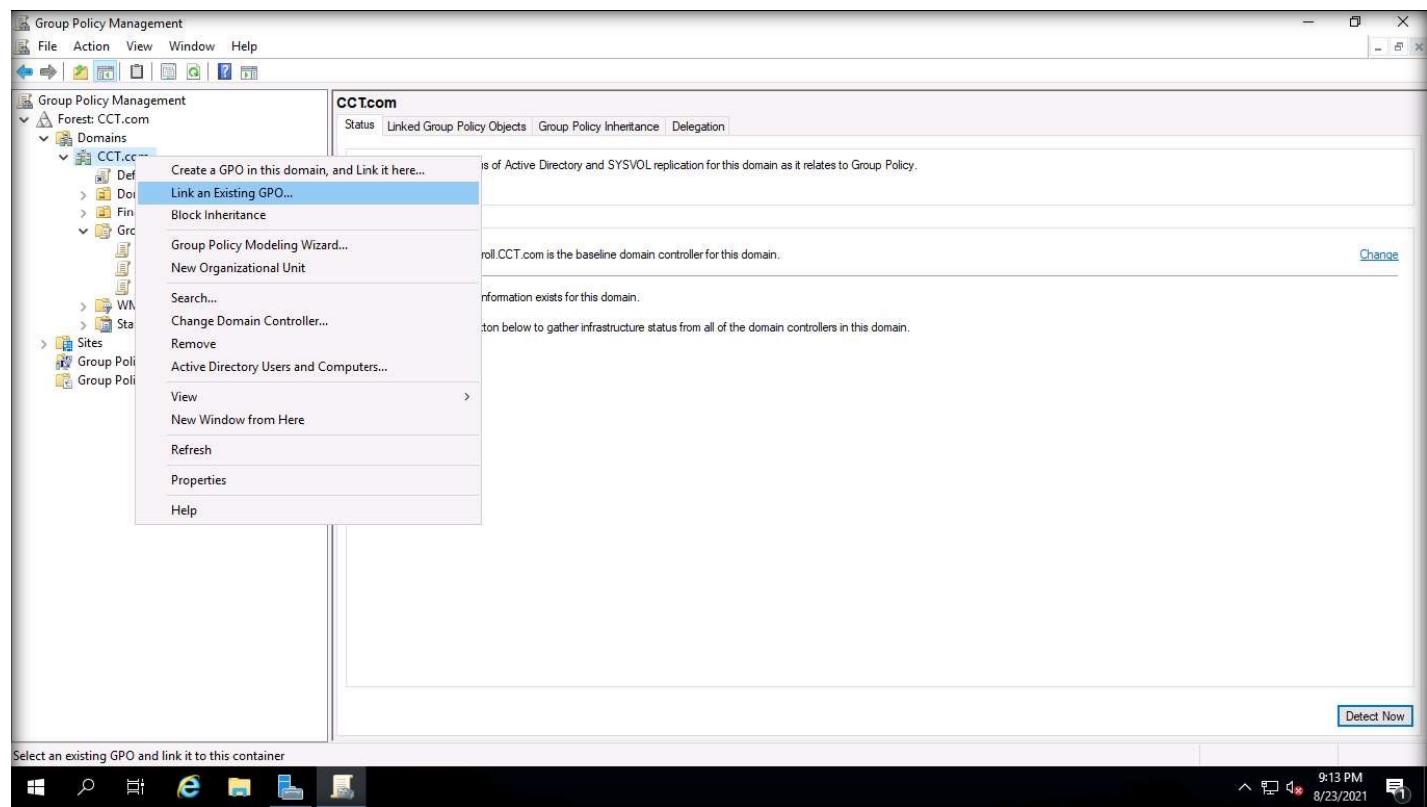
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	Program Files: Rar.exe, UnRAR.exe	File Hash	
Allow	Everyone	Program Files: WINRAR signed by O=WinRAR...	Publisher	
Allow	Everyone	Program Files: MICROSOFT® WINDOW...	Publisher	
Allow	Everyone	Program Files: FIREFOX signed by O=Mozilla...	Publisher	
Allow	Everyone	Program Files: LAB ON DEMAND HYPERLINK...	Publisher	
Allow	Everyone	Program Files: JAVA(TM) PLATFORM SE...	Publisher	
Deny	Everyone	Program Files: INTERNET EXPLORER signed by O=...	Publisher	

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



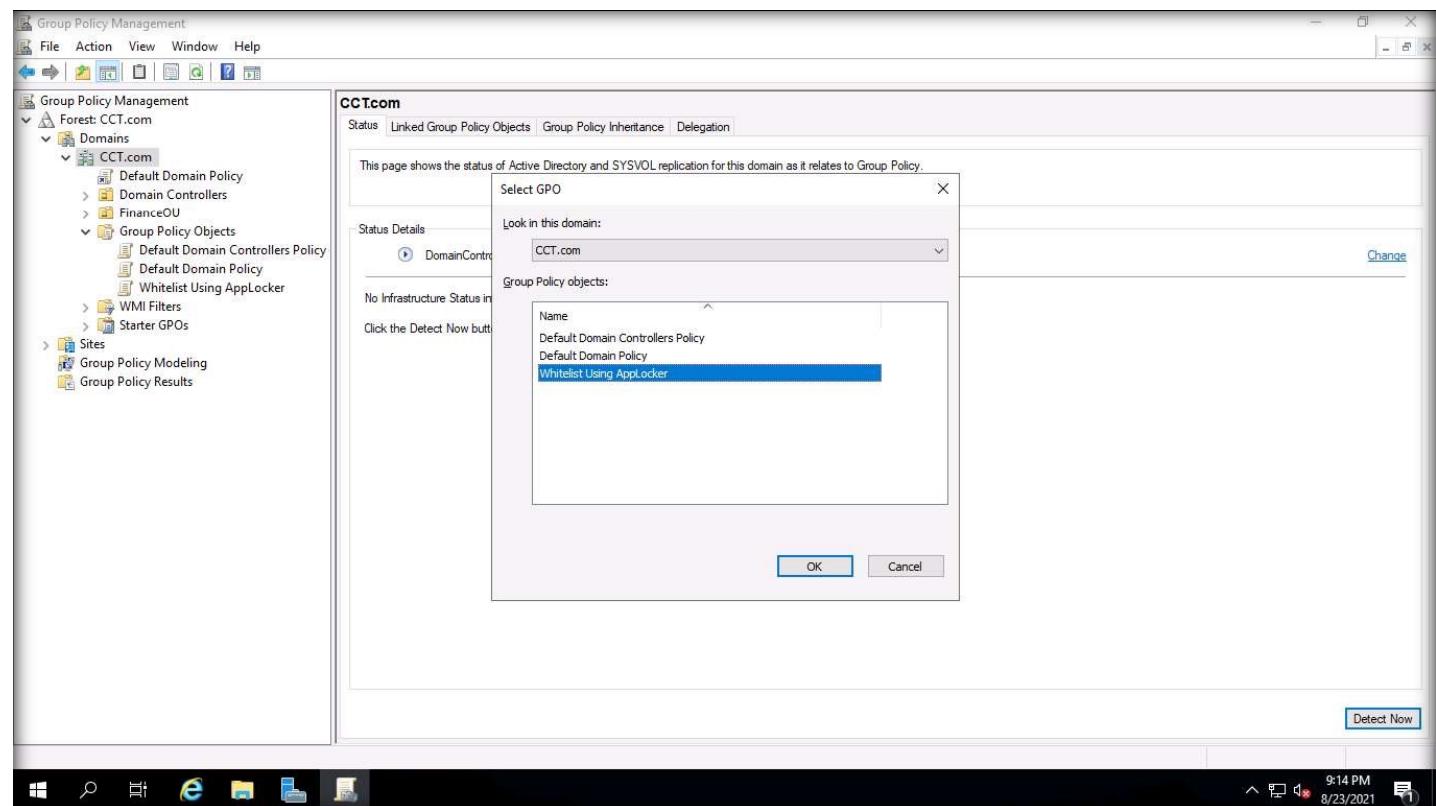
29. Right-click on cct.com under Domains and select the Link an Existing GPO... option.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

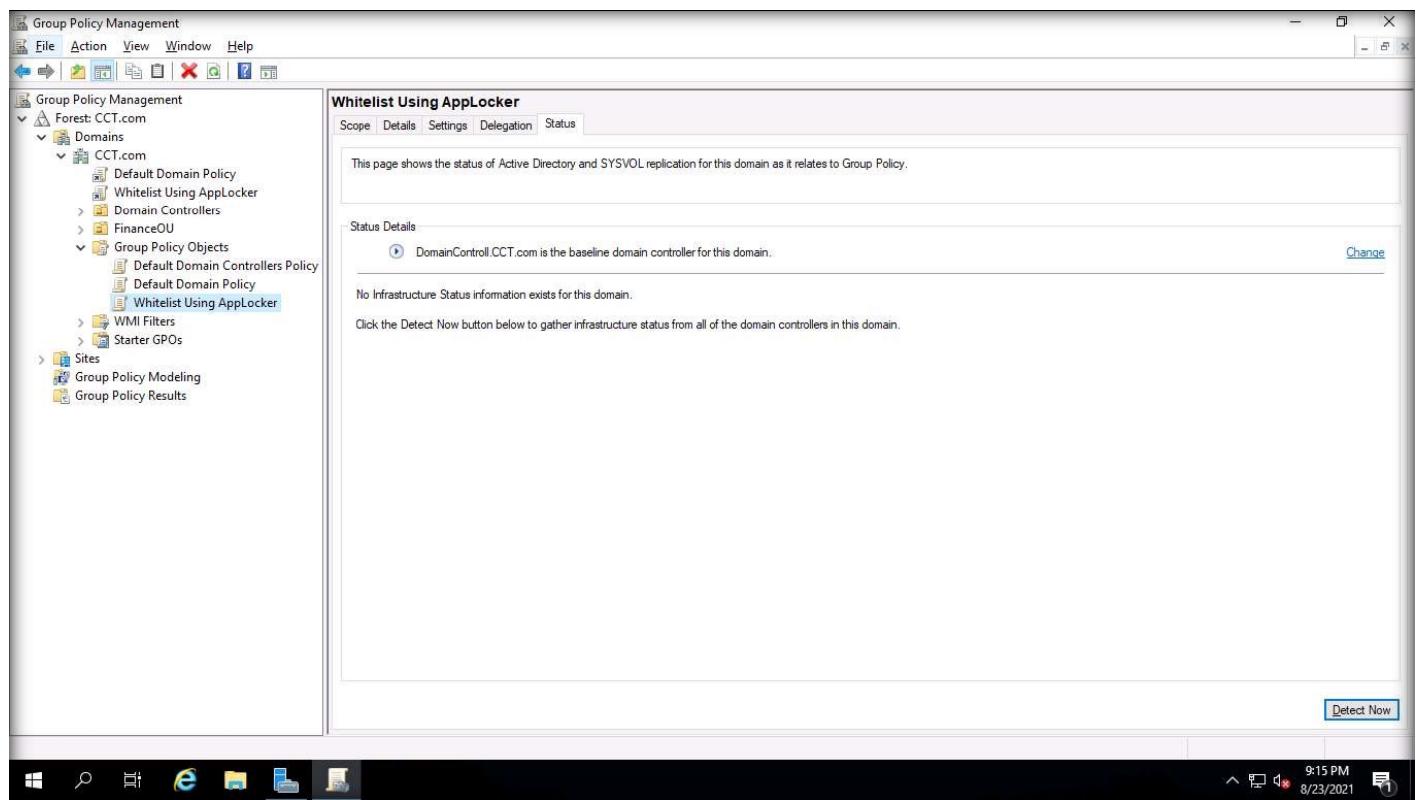


30. The Select GPO window opens, select Whitelist Using AppLocker under Group Policy Objects and click on OK.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker

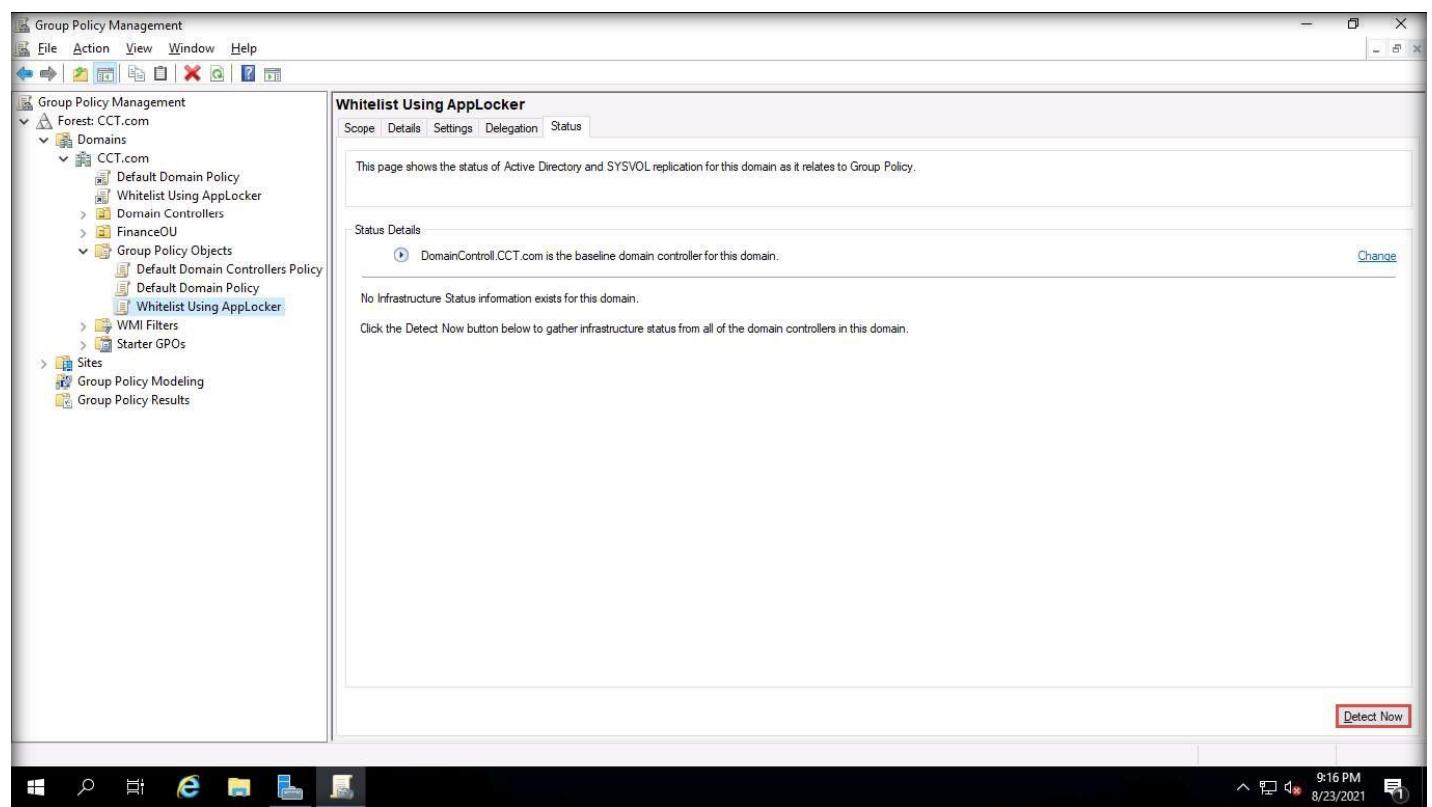


EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



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

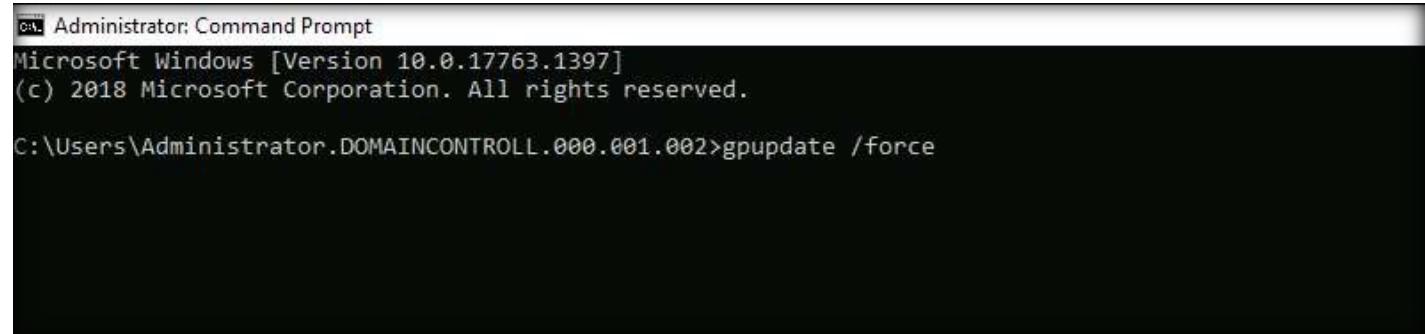
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



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 APPLCKER

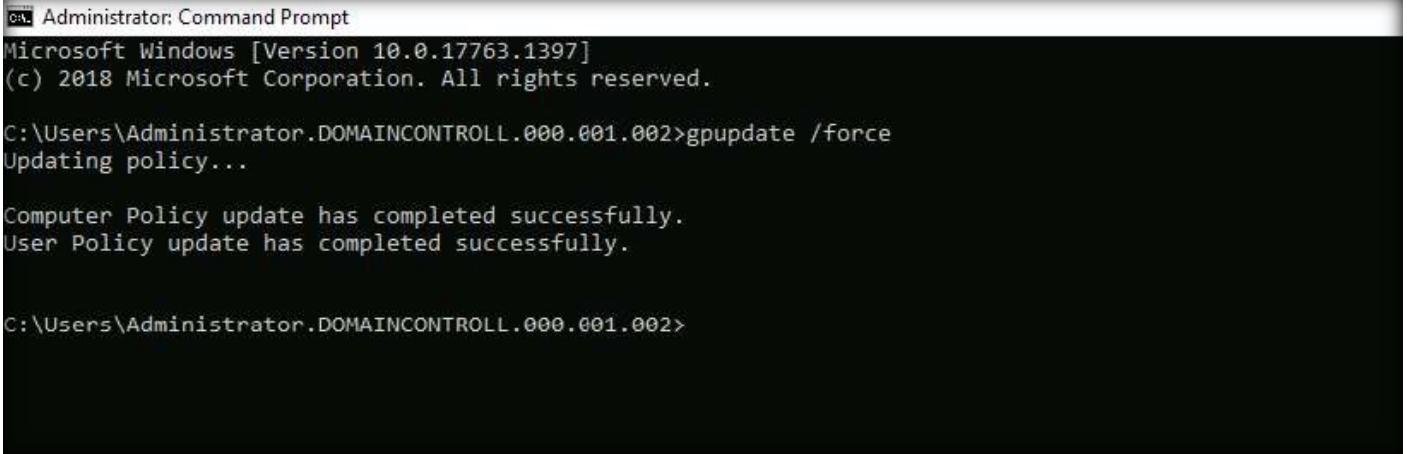


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1397]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.DOMAINCONTROLL.000.001.002>gpupdate /force
```

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

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1397]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.DOMAINCONTROLL.000.001.002>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

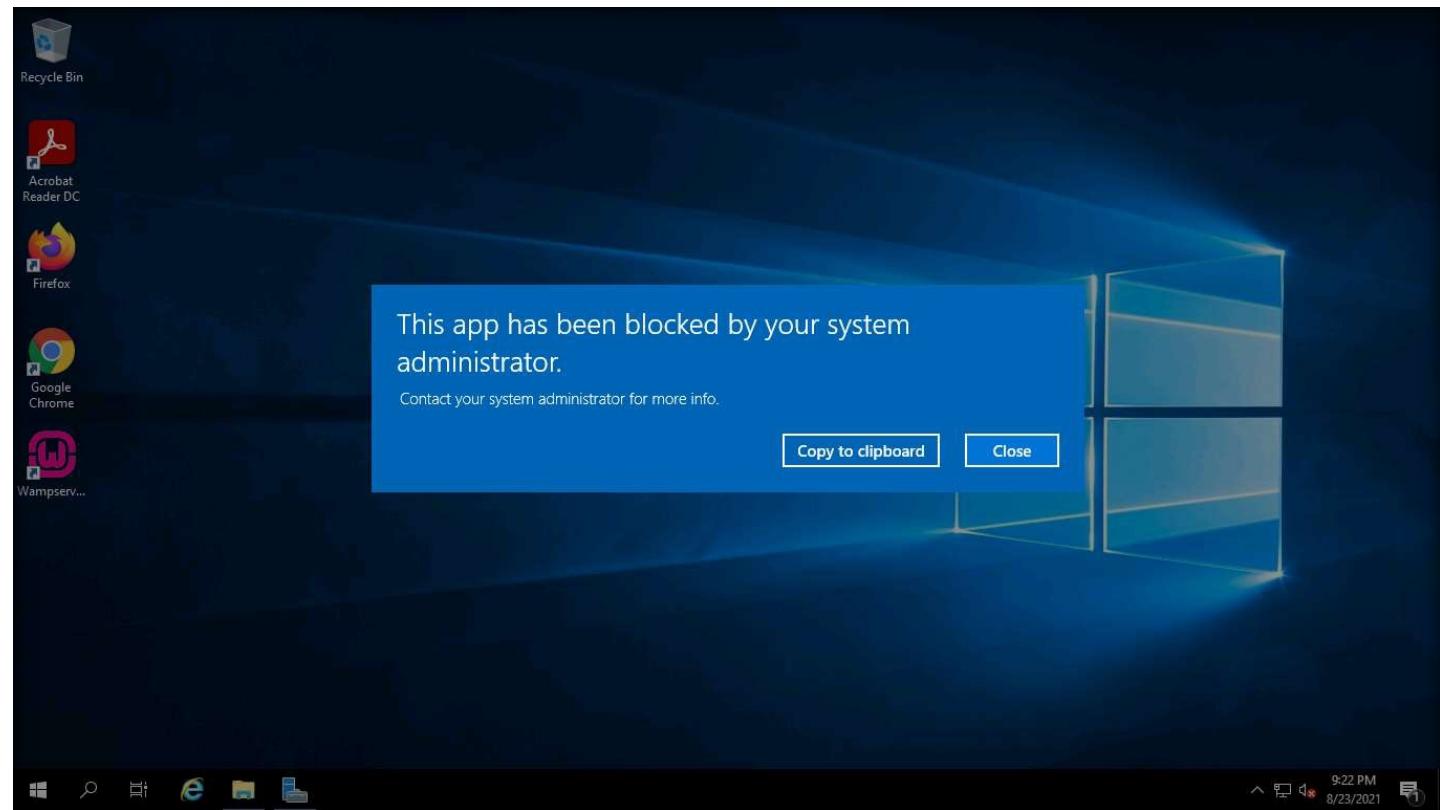
C:\Users\Administrator.DOMAINCONTROLL.000.001.002>
```

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.

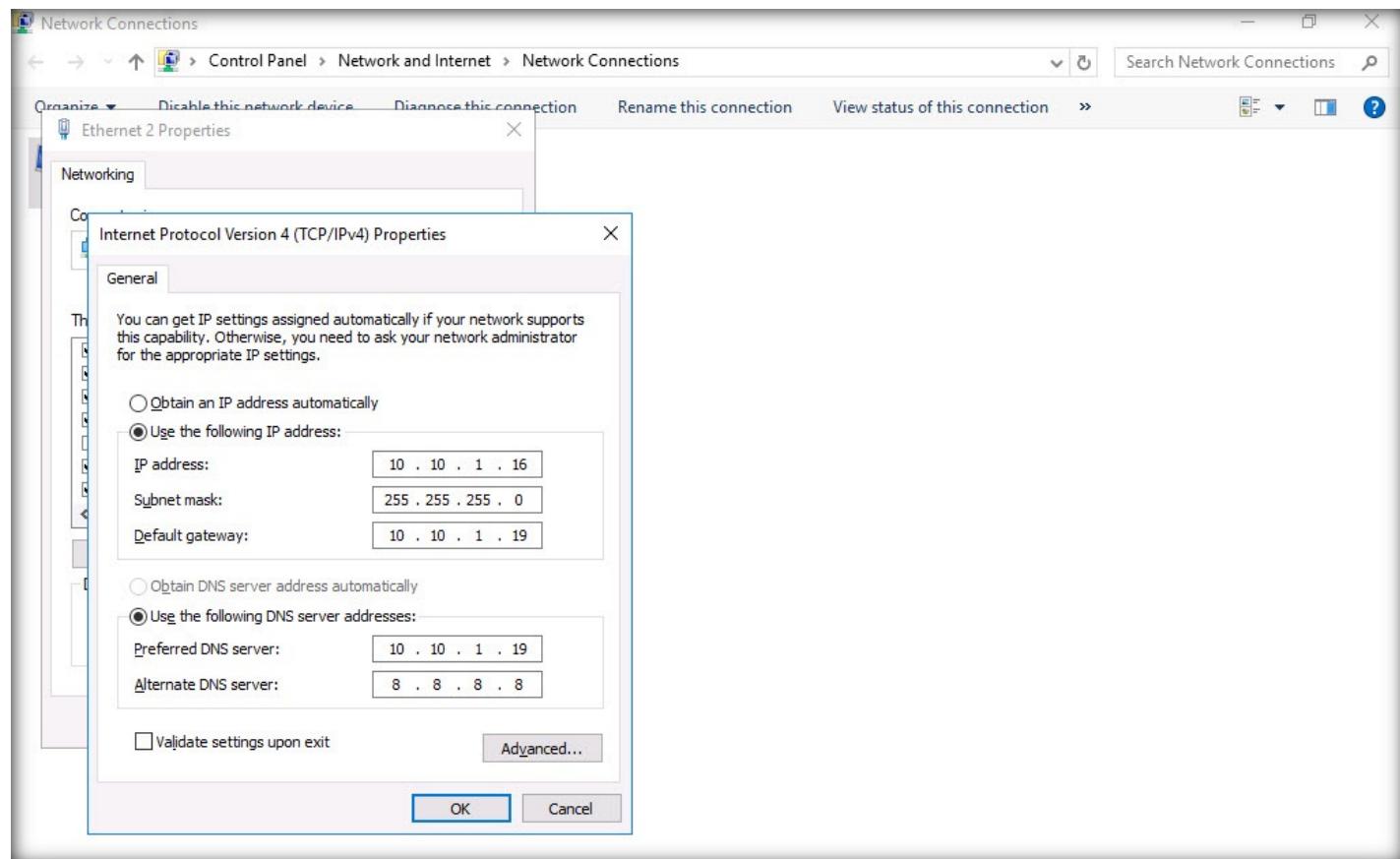
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



38. Switch to the Web Server virtual machine.

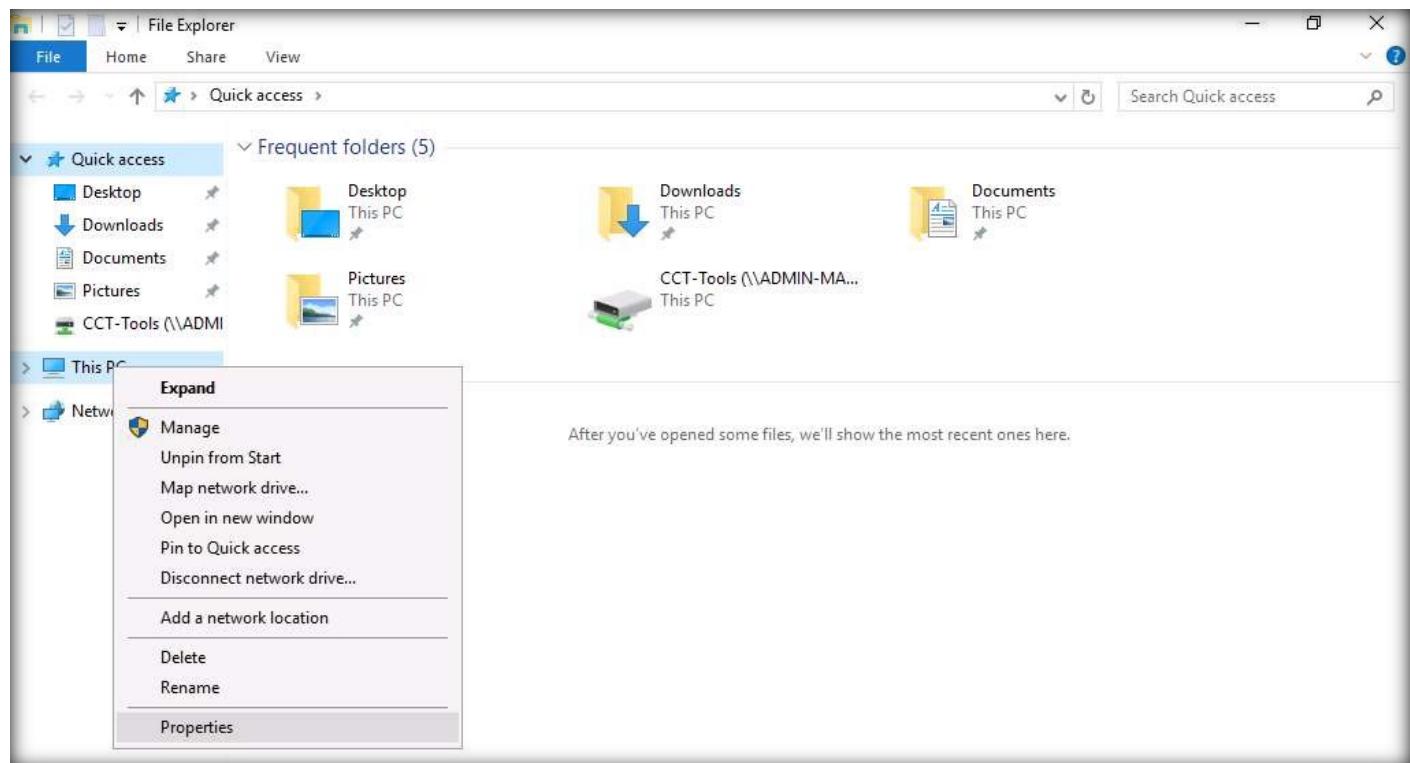
39. Log in with the credentials Administrator and admin@123.

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.

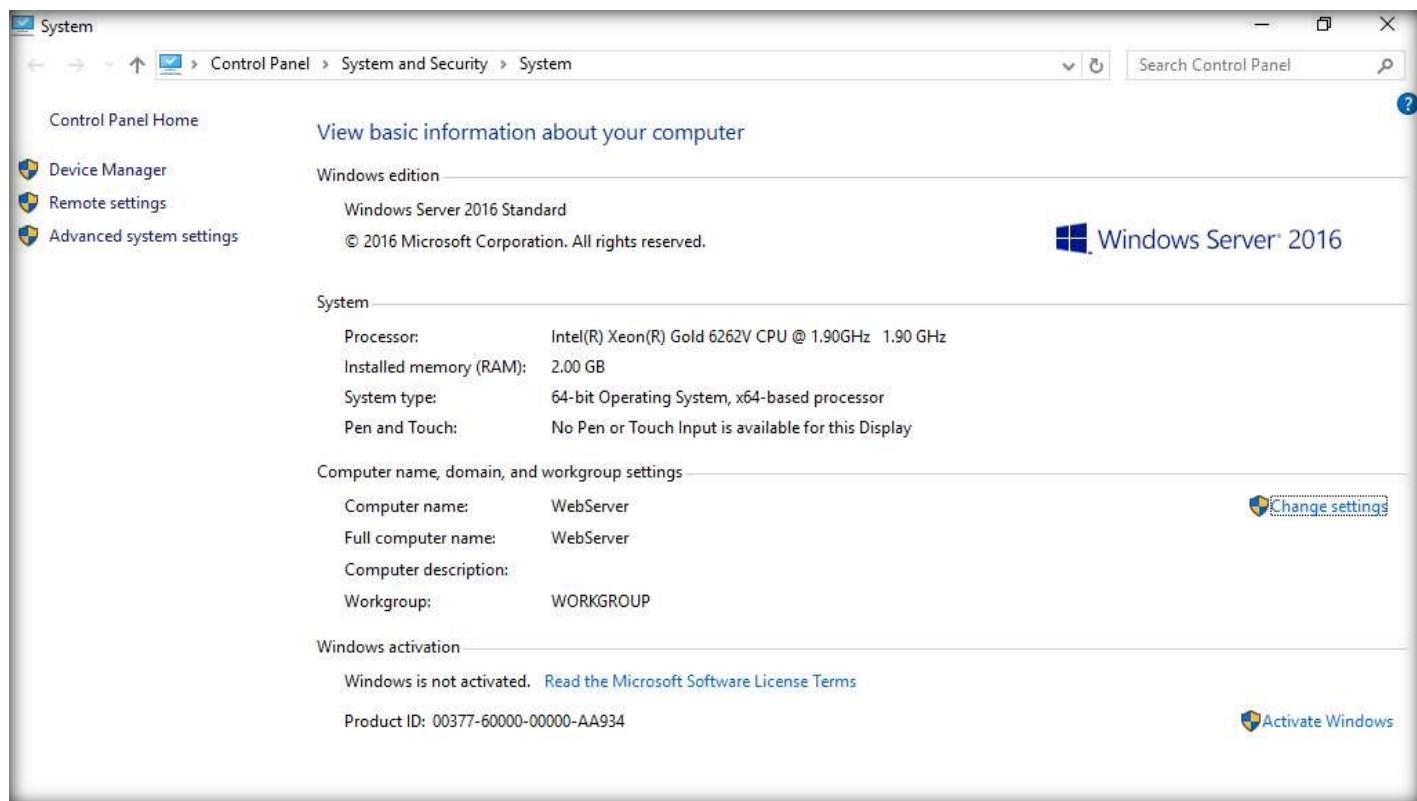


41. Open File Explorer and right-click on This PC, select Properties.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLCKER

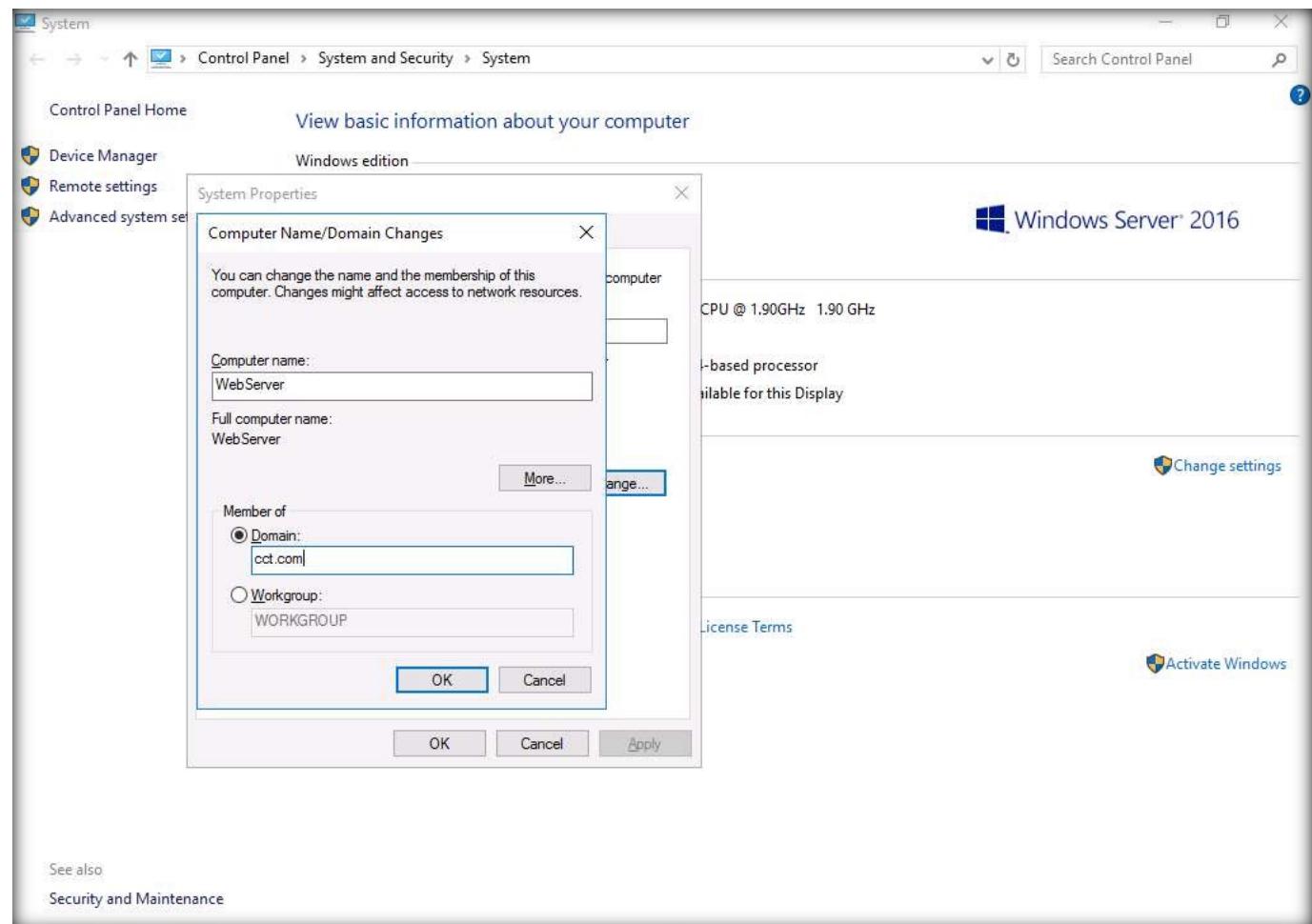


42. The System window opens, click Change Settings.



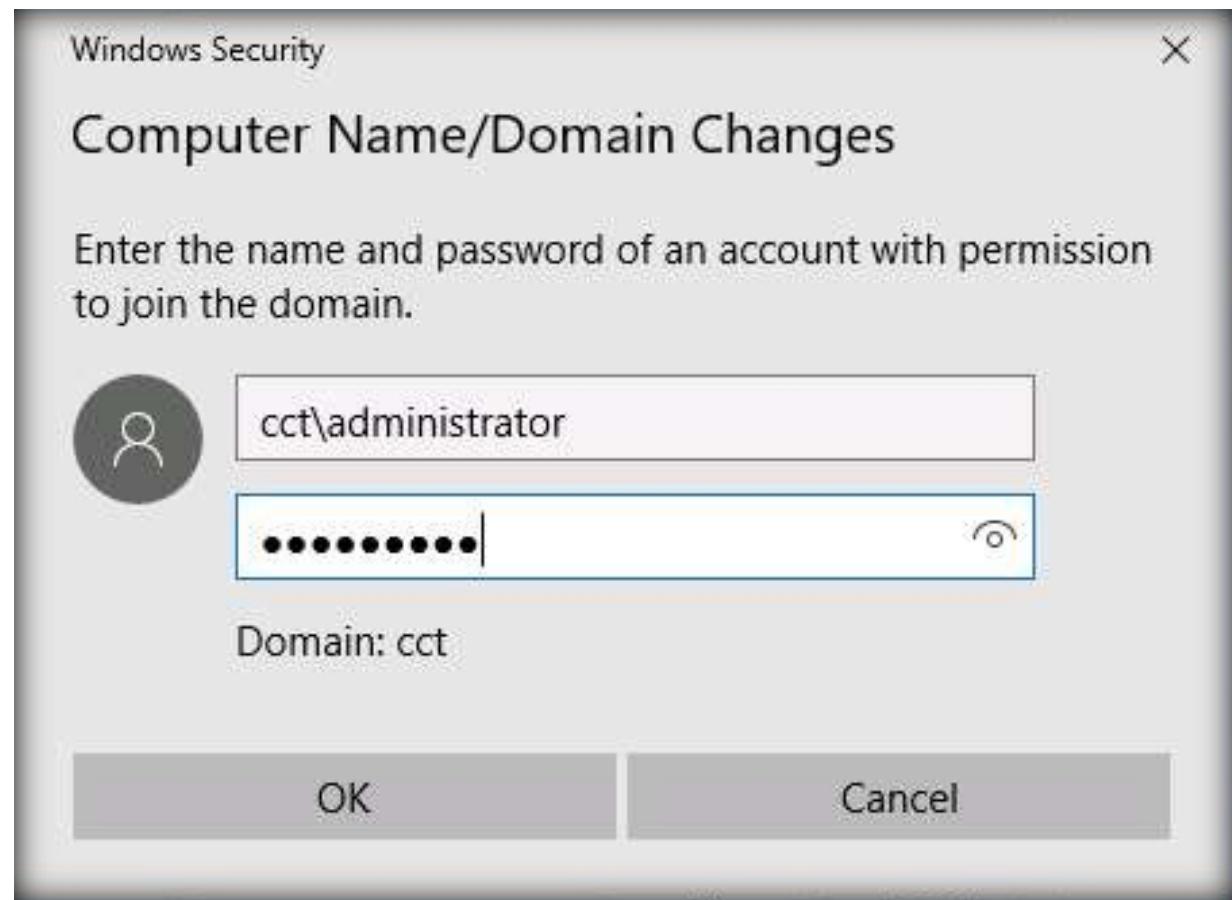
43. The System Properties Window opens, click Change....

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

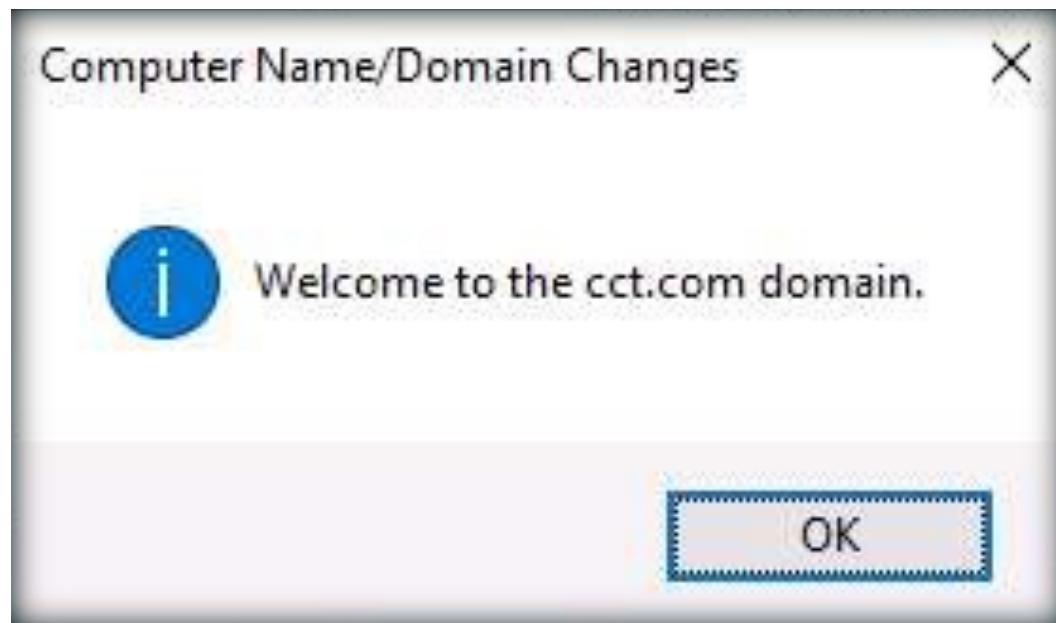
45. The Window Security credential window opens, type username as cct\administrator and type password as admin@123 and click OK



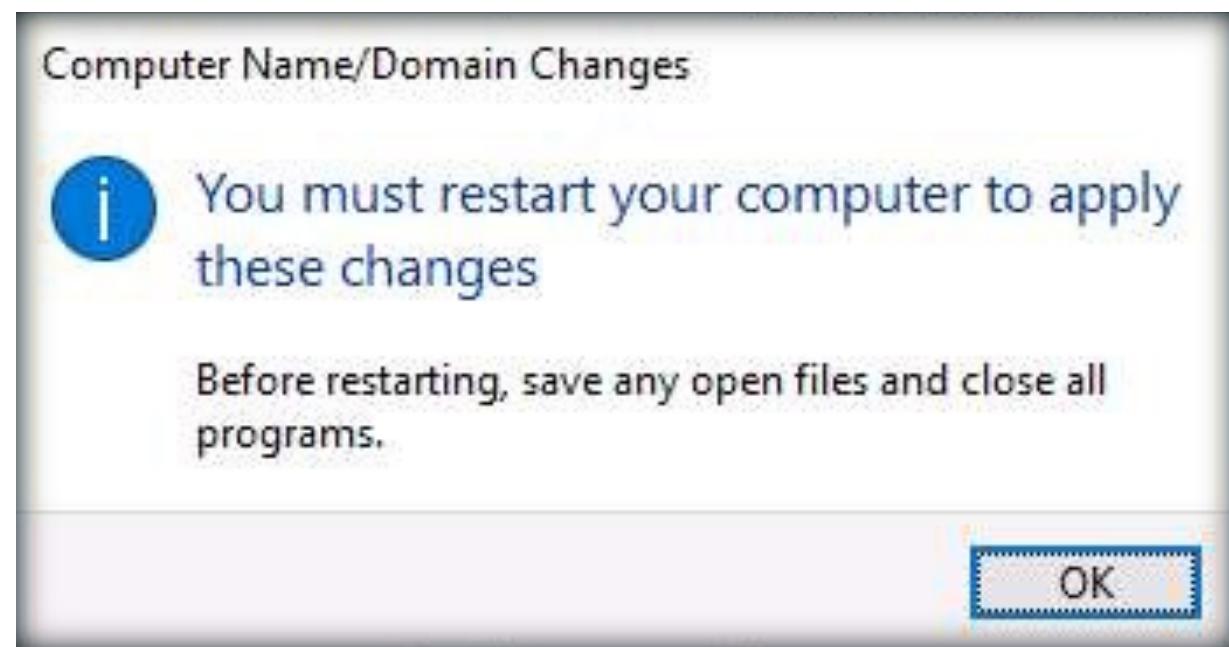
EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLCKER

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

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLCKER



47. The restarting confirmation popup appears, Click OK.



EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APLOCKER

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

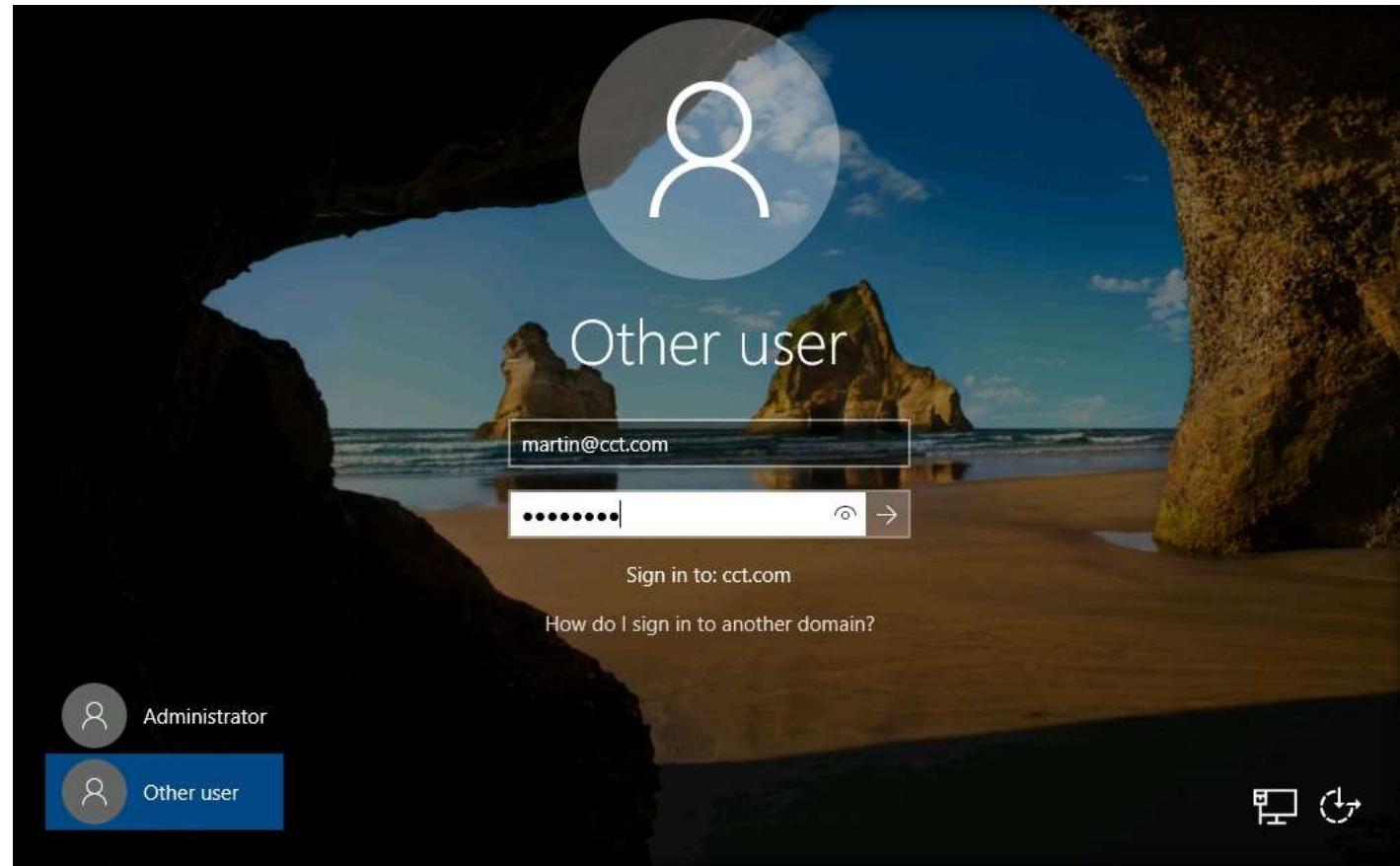
49. The Microsoft windows message box opens, click Restart Now button to restart the system.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APLOCKER



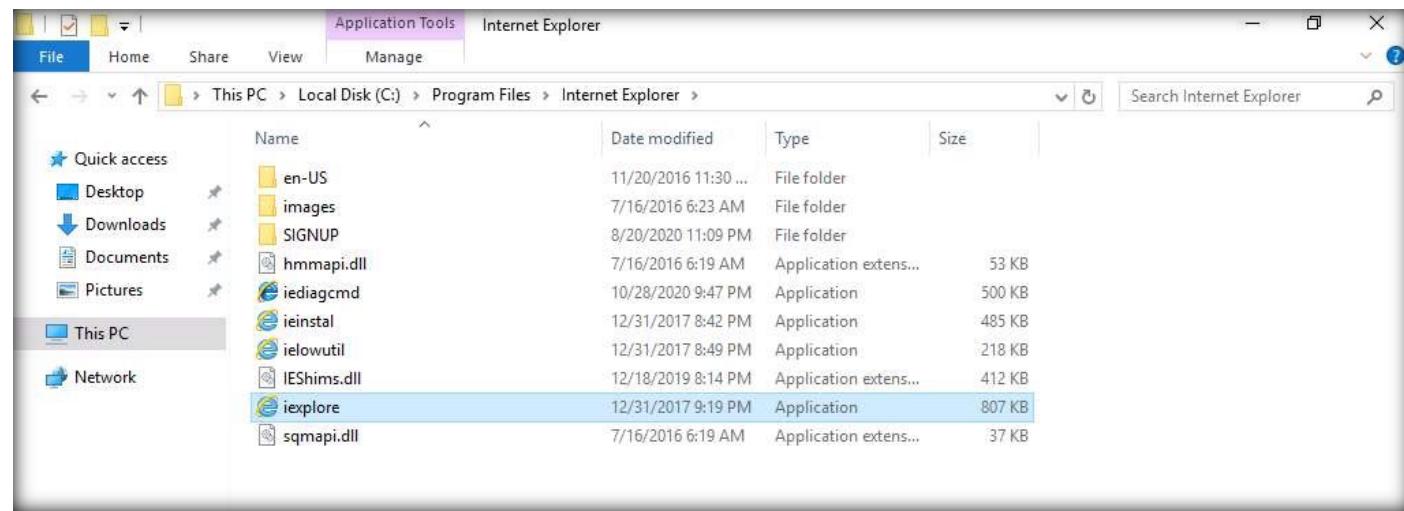
50. The system will restart. Choose Other user username as martin@cct.com and type password as user@123 and press Enter.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLocker



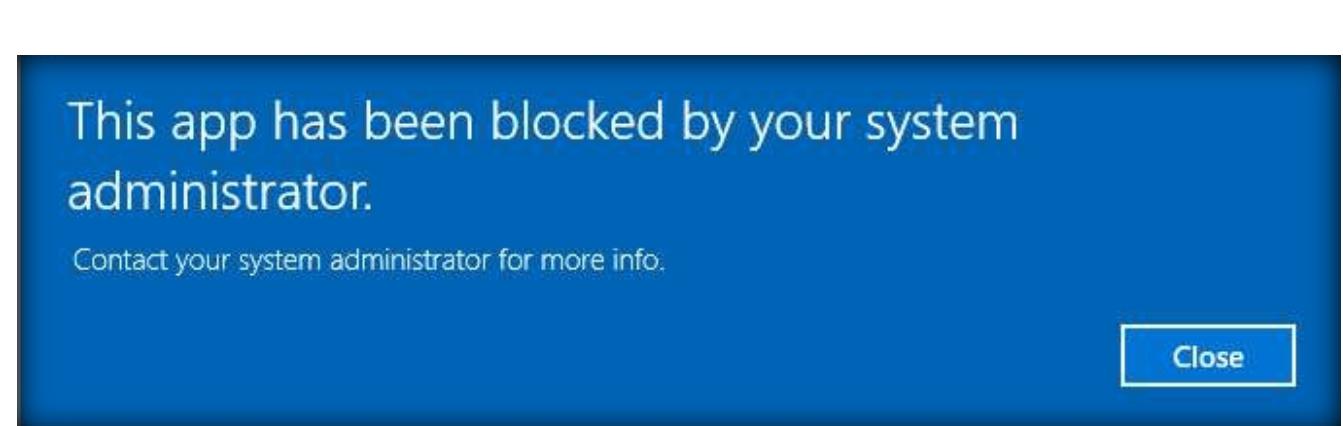
51. Navigate to C:\Program Files\Internet Explorer and try to execute iexplorer.exe.

EXERCISE 1: IMPLEMENT APPLICATION WHITELISTING USING APPLCKER



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 APLOCKER



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

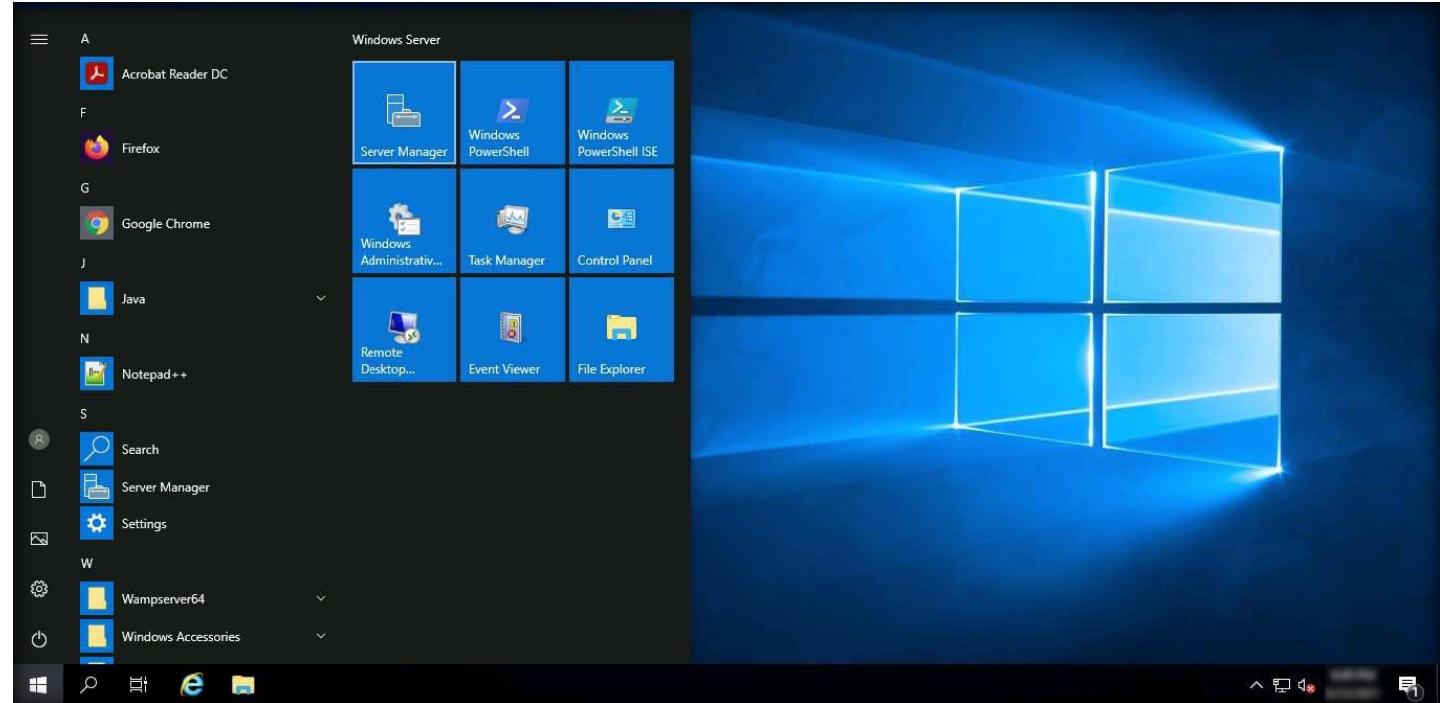
Note: Since administrative rights are required to proceed to the next exercise, we will unlink the created Whitelist Using AppLocker policy.

55. Switch to the AD Domain Controller virtual machine.

56. Log in with the credentials CCT\Administrator and admin@123.

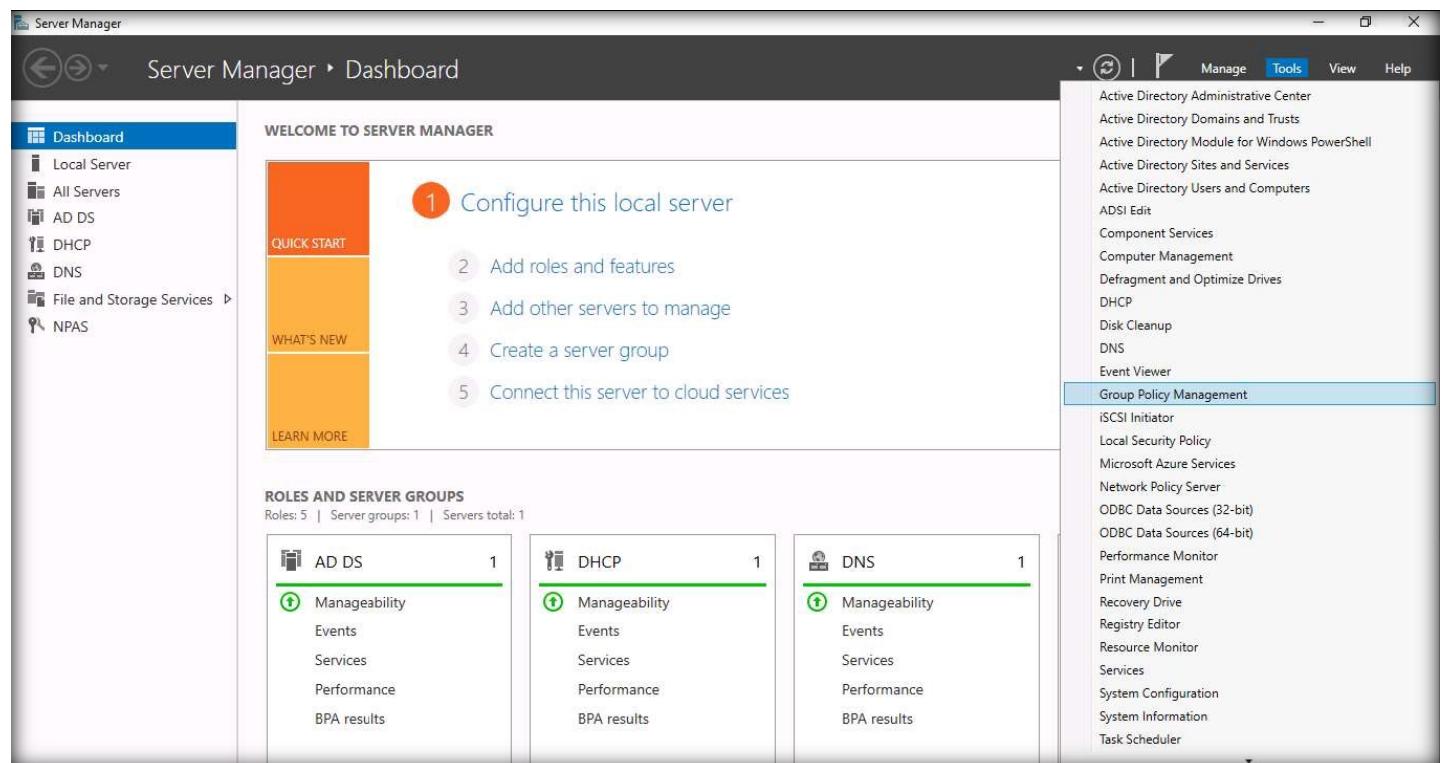
57. Click on Windows Start icon, select Server Manager.

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 APPLCKER



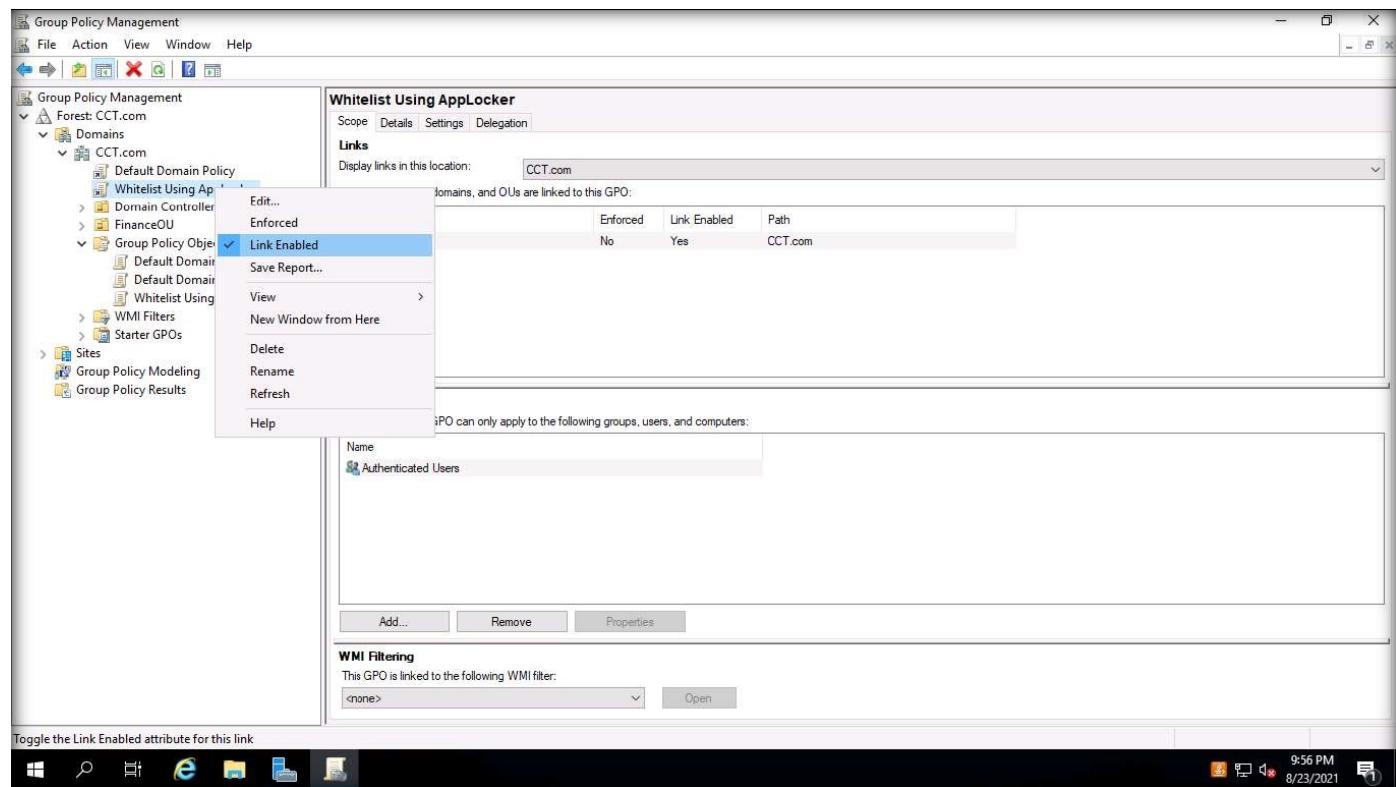
59. The Group Policy Management console opens, expand the cct.com domain, right-click on Whitelist Using AppLocker policy, and click on the Link Enabled option to disable the link.

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.

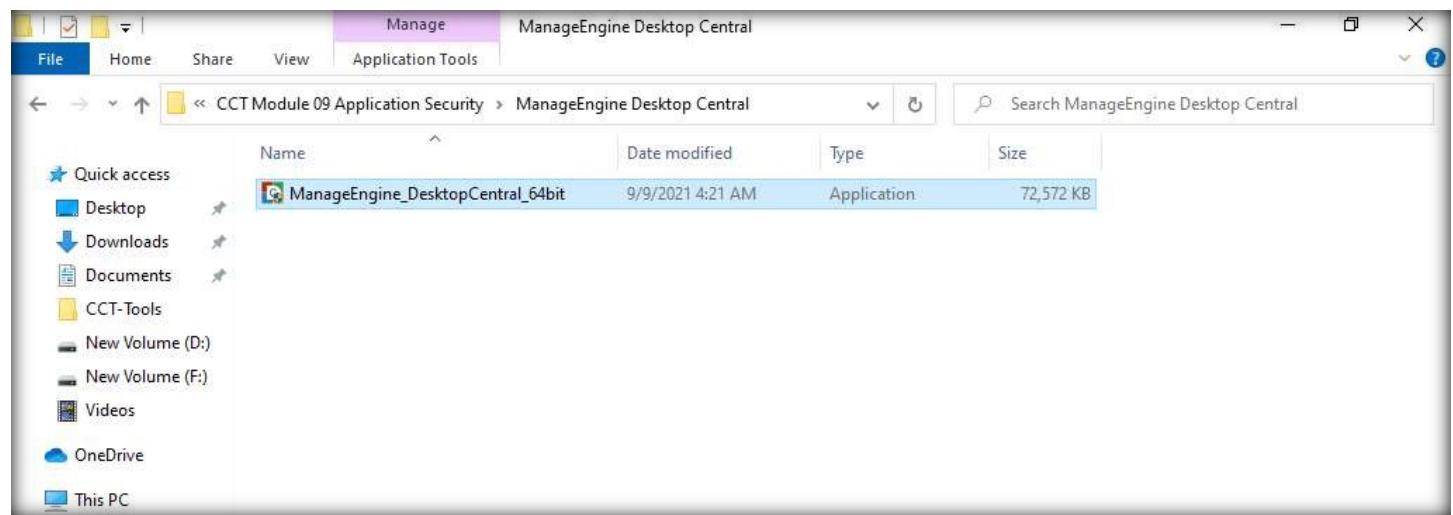
Note: Ensure that PfSense Firewall virtual machine is running.

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.

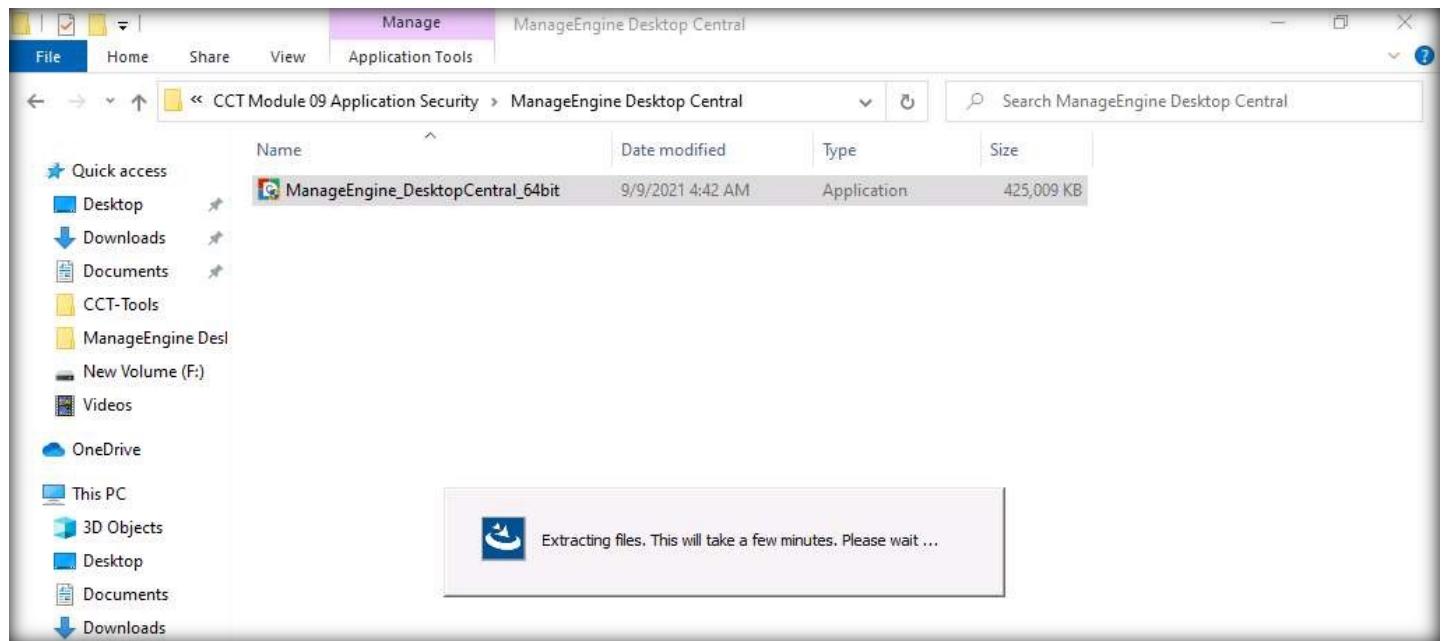
3. Navigate to Z:\CCT-Tools\CCT Module 09 Application Security\ManageEngine Desktop Central.
4. Double-click ManageEngine_DesktopCentral_64bit.exe to start the installation.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



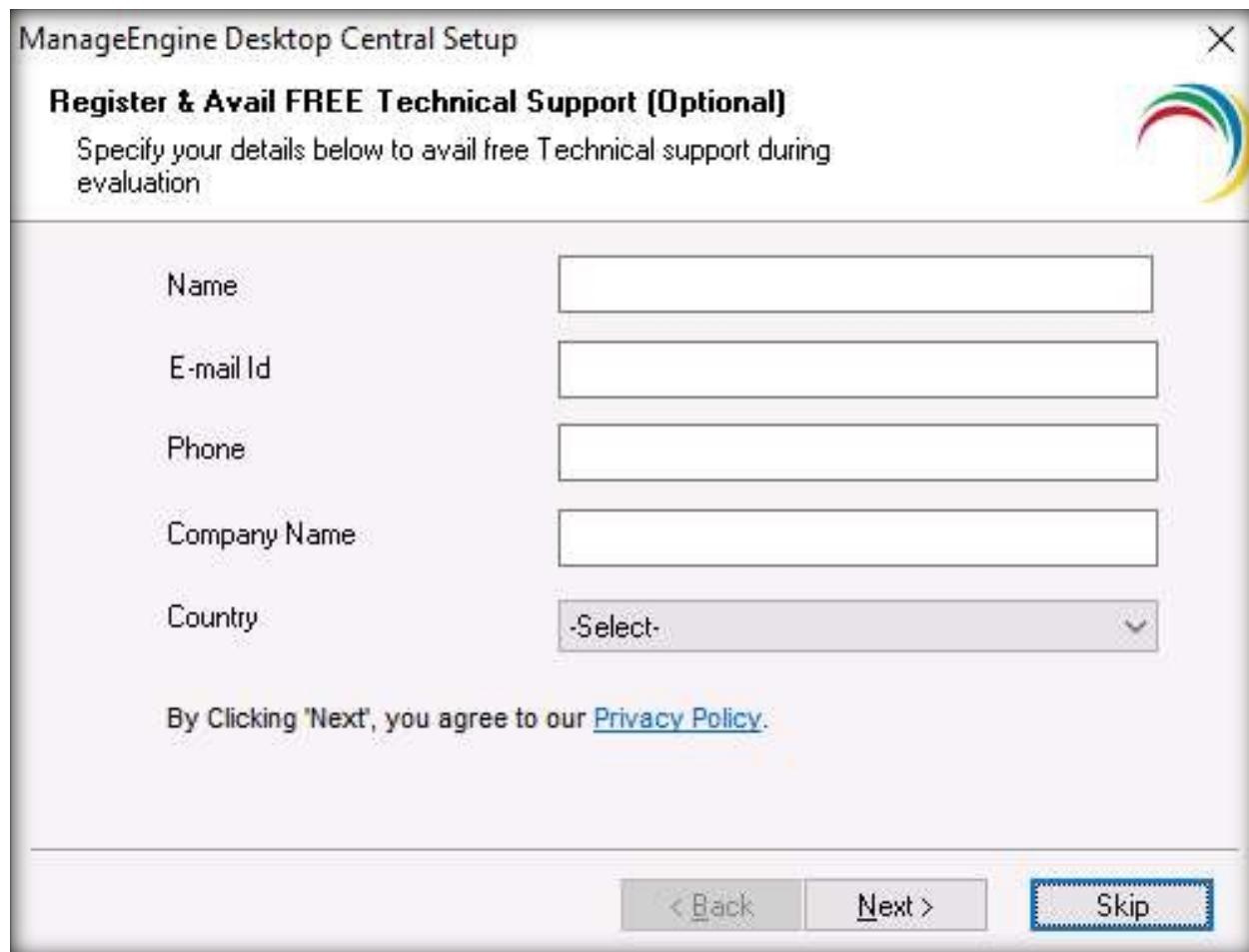
- EXERCISE 2:
BLACKLIST APPLICATION USING
MANAGEENGINE
DESKTOP CENTRAL
5. A User Account Control window appears, click Yes to continue.
 6. ManageEngine Desktop Central Setup window appears, click Next to proceed with the installation process.
 7. Follow the wizard driven installation to install the 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.

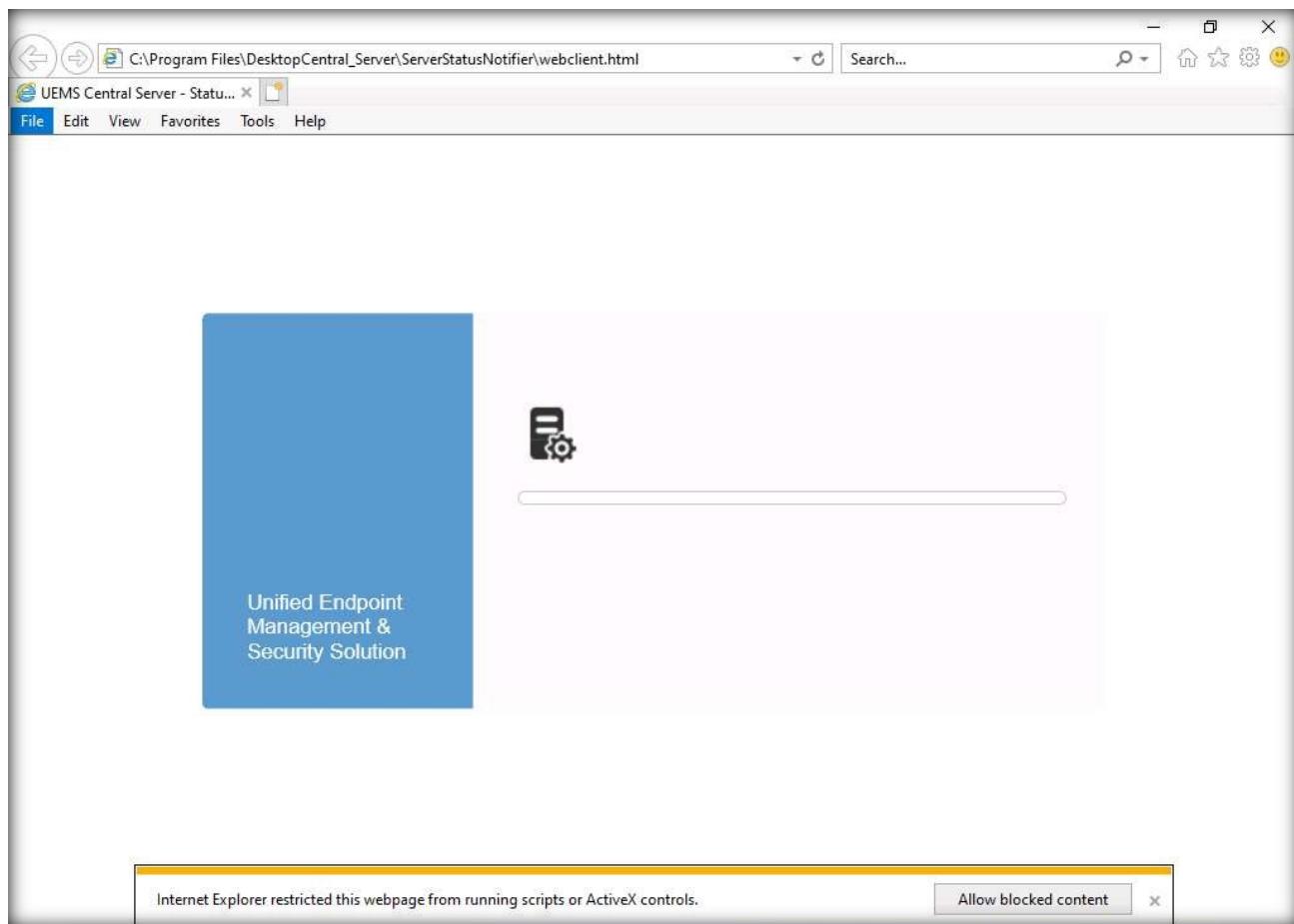


EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL

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

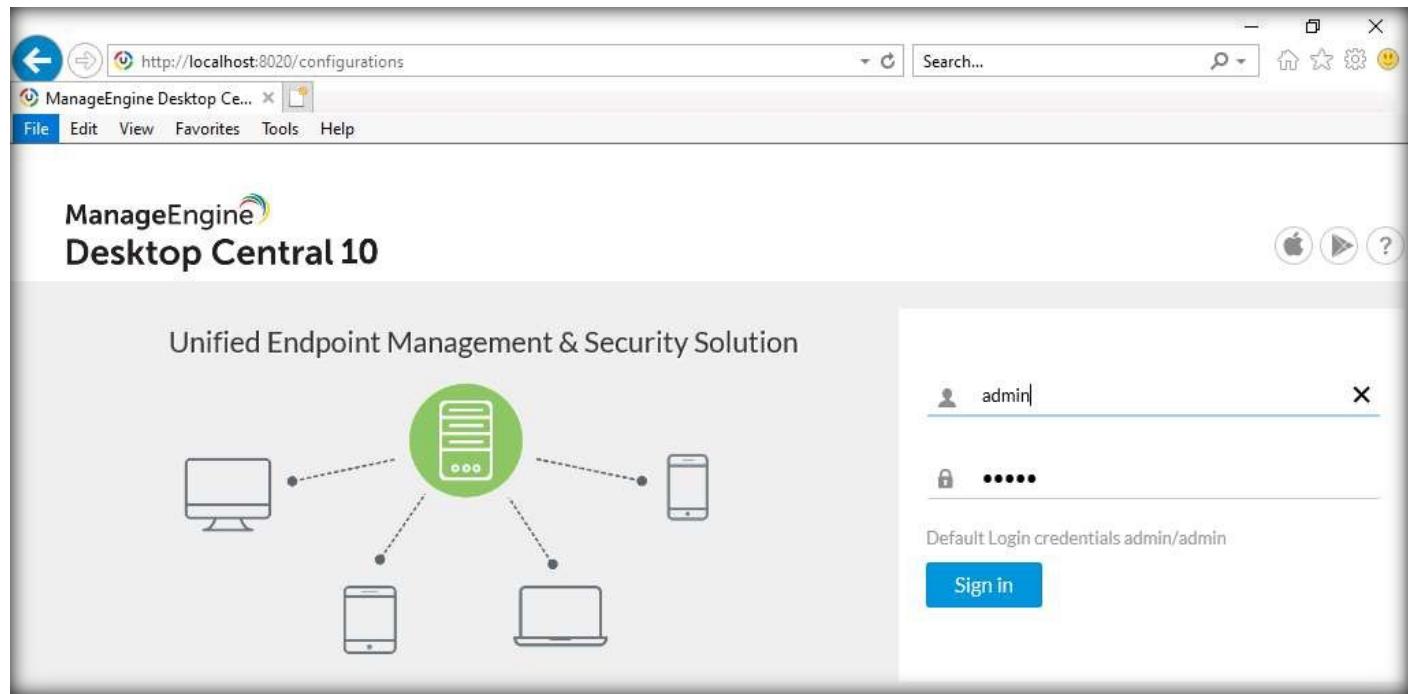


EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



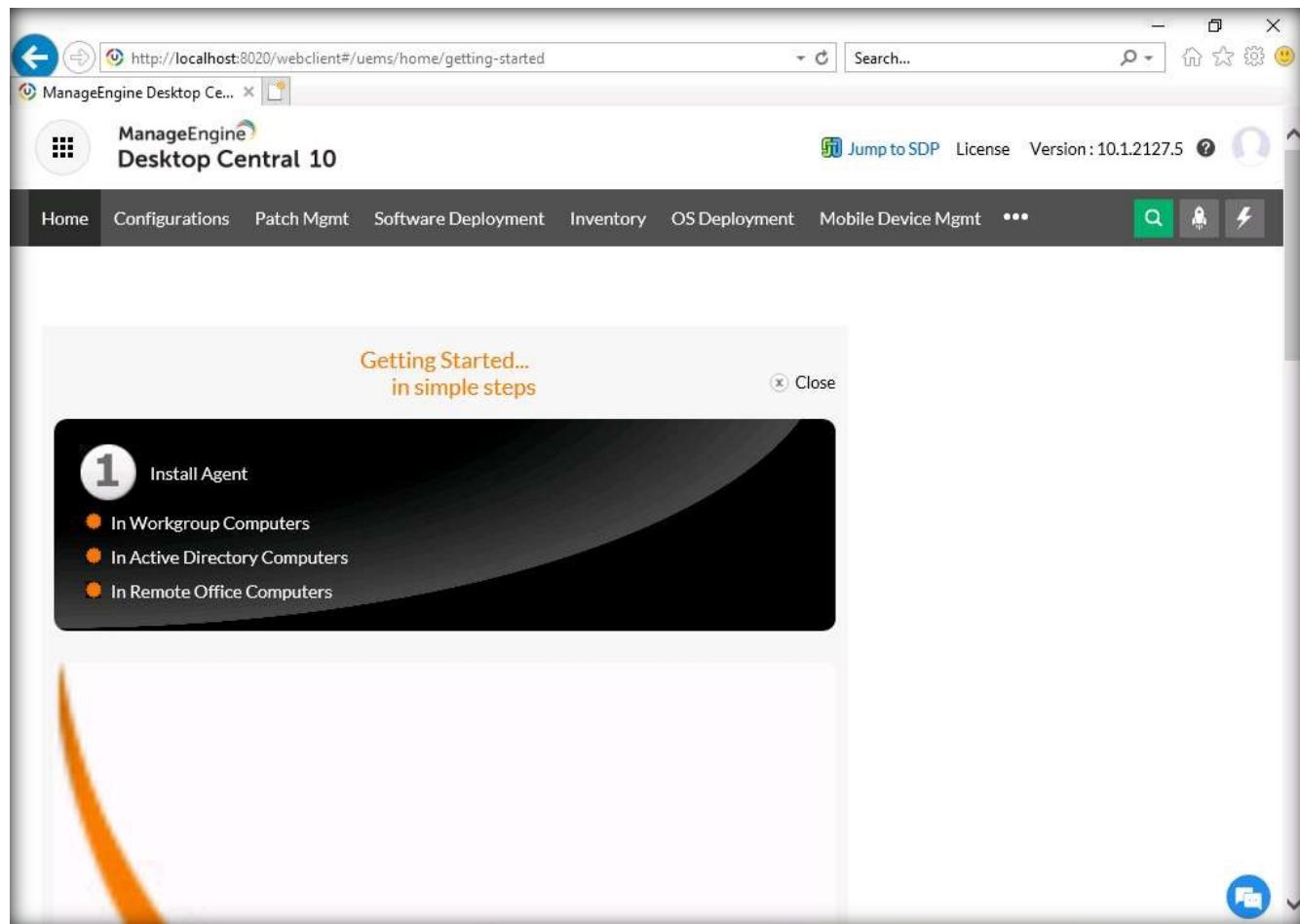
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL

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.



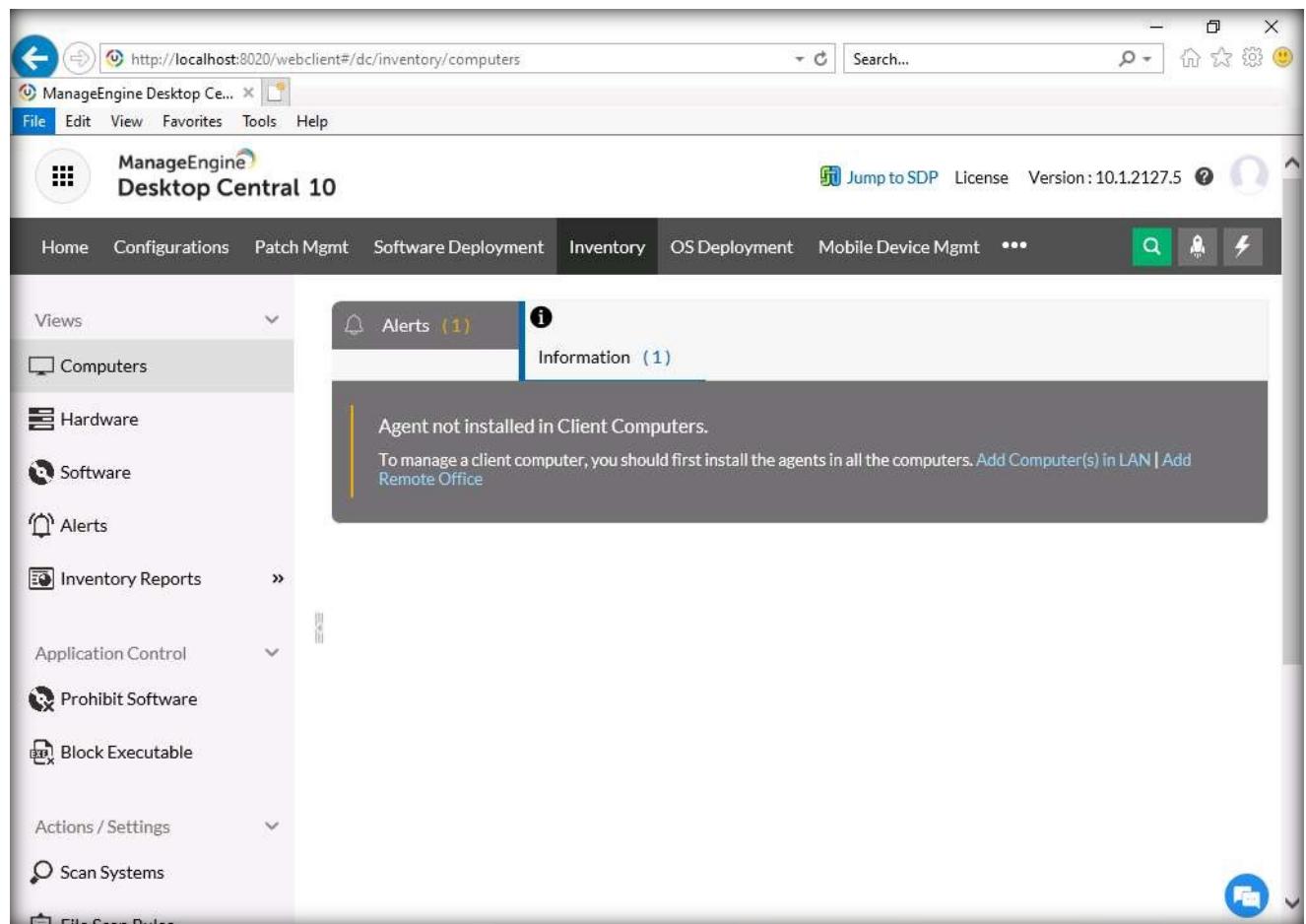
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL

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



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

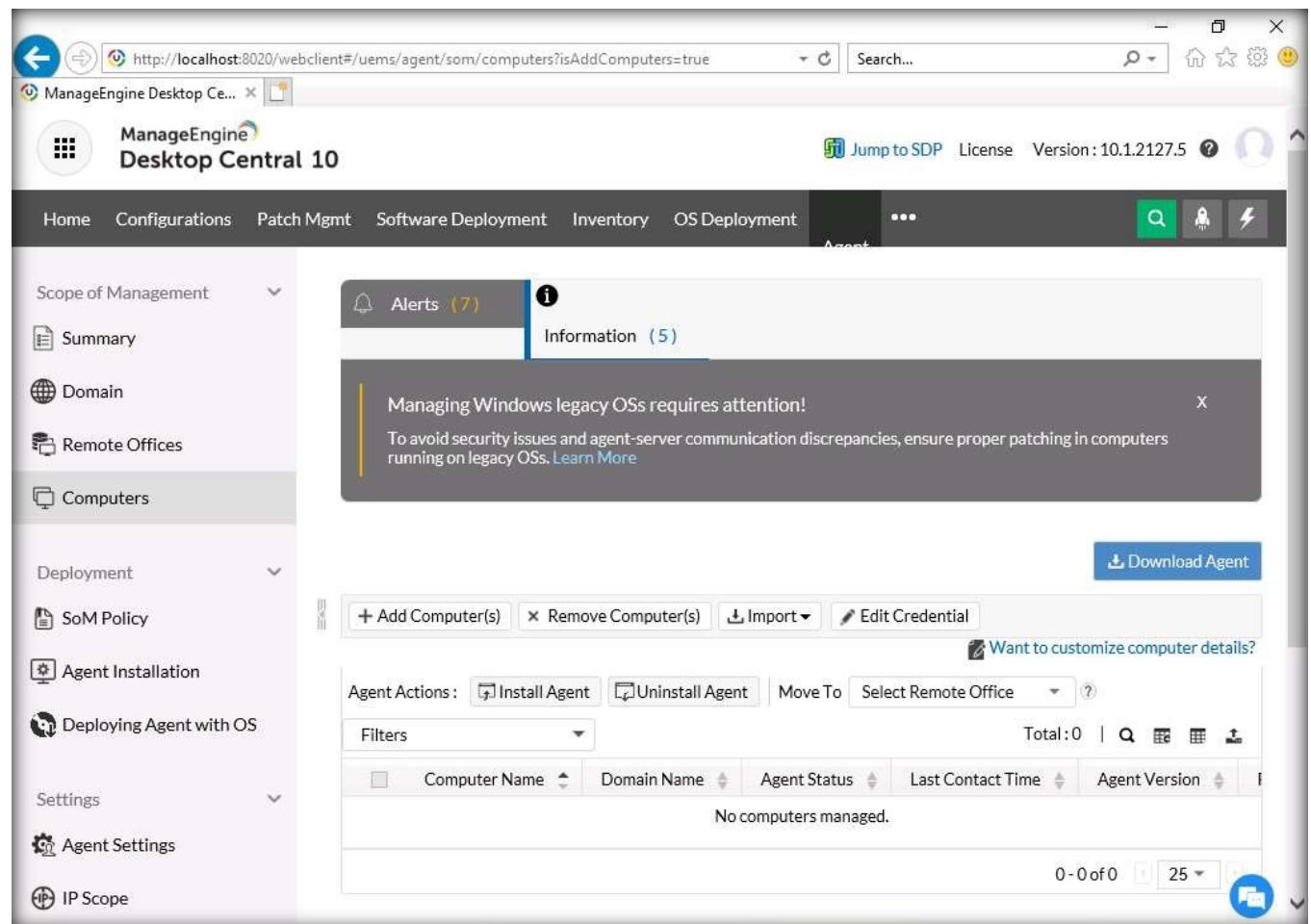
22. Navigate to the Computers option from the left-pane. In the right-pane, click Add Computer(s) in LAN link.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the browser is <http://localhost:8020/webclient#/dc/inventory/computers>. The main navigation bar includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory (which is selected), OS Deployment, Mobile Device Mgmt, and other options. On the left, a sidebar lists Views (Computers, Hardware, Software, Alerts, Inventory Reports), Application Control (Prohibit Software, Block Executable), Actions / Settings (Scan Systems, File Scan Rules), and a bottom section for Scan Systems. The right pane displays an 'Alerts (1)' section with a message: 'Agent not installed in Client Computers.' It also shows an 'Information (1)' section with the text: 'To manage a client computer, you should first install the agents in all the computers. [Add Computer\(s\) in LAN](#) | [Add Remote Office](#)'. There are also search and filter icons at the top right of the main content area.

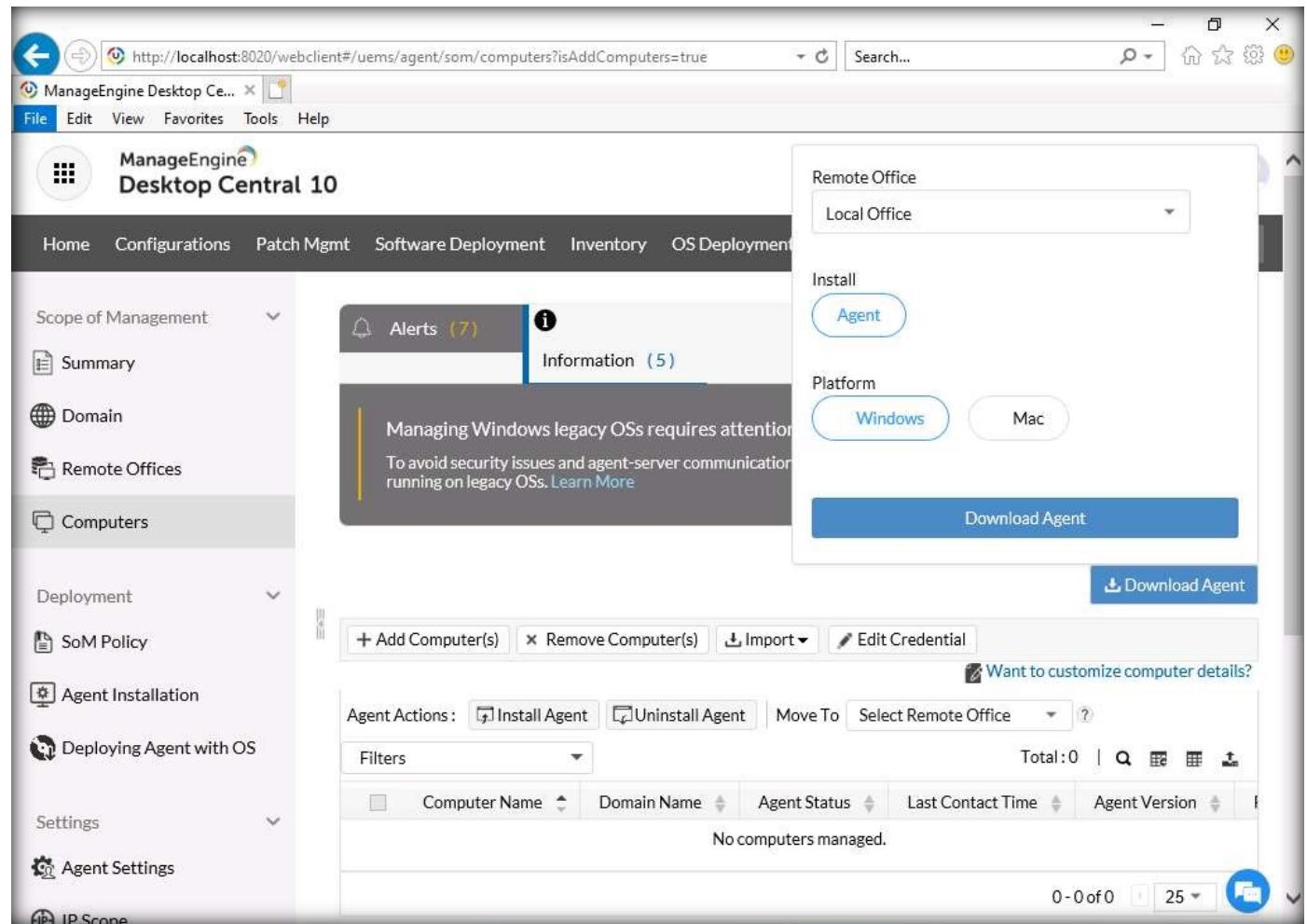
23. Add Computer(s) wizard appears, close it.

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



The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the browser is <http://localhost:8020/webclient#/uem/agent/som/computers?isAddComputers=true>. The page title is "ManageEngine Desktop Ce...". The top navigation bar includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory, OS Deployment, Agent (selected), and other options. A sidebar on the left lists Scope of Management (Summary, Domain, Remote Offices, Computers - selected), Deployment (SoM Policy, Agent Installation, Deploying Agent with OS), Settings (Agent Settings, IP Scope), and a message about managing legacy OSs. The main content area features an "Information" card with a warning about managing legacy OSs and a "Download Agent" button. Below this is a table header for managing computers, with columns for Computer Name, Domain Name, Agent Status, Last Contact Time, and Agent Version. The table body displays "No computers managed.".

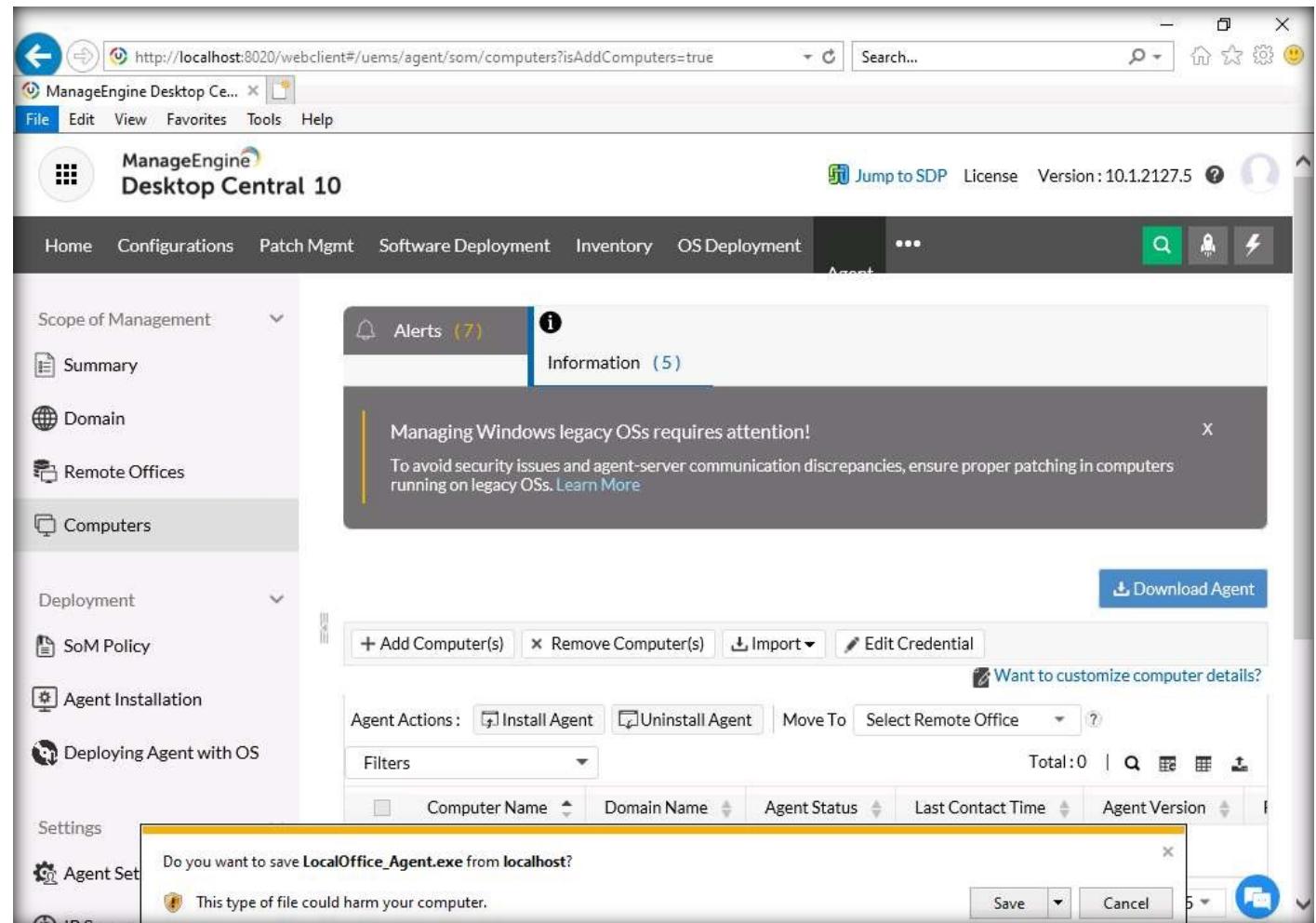
25. A pop-up appears, ensure that Windows is selected under Platform section and click Download Agent.



The screenshot shows the ManageEngine Desktop Central 10 web interface at <http://localhost:8020/webclient#/uem/agent/som/computers?isAddComputers=true>. The main menu includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory, and OS Deployment. The left sidebar shows Scope of Management (Summary, Domain, Remote Offices, Computers), Deployment (SoM Policy, Agent Installation, Deploying Agent with OS), and Settings (Agent Settings, IP Scope). A central panel displays Alerts (7) and Information (5). A prominent message states: "Managing Windows legacy OSs requires attention. To avoid security issues and agent-server communication running on legacy OSs. Learn More". On the right, there's a "Remote Office" dropdown set to "Local Office", an "Install" section with an "Agent" button, a "Platform" section with "Windows" selected, and two "Download Agent" buttons. A tooltip "Want to customize computer details?" is visible near the bottom right.

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.



The screenshot shows the ManageEngine Desktop Central 10 web interface at <http://localhost:8020/webclient#/uem/agent/som/computers?isAddComputers=true>. The main dashboard displays alerts (7) and information (5). A prominent message box states: "Managing Windows legacy OSs requires attention! To avoid security issues and agent-server communication discrepancies, ensure proper patching in computers running on legacy OSs. Learn More". Below the message, there are buttons for "Download Agent" and "Want to customize computer details?". In the bottom right corner, a modal dialog box asks: "Do you want to save LocalOffice_Agent.exe from localhost?". It includes a warning: "This type of file could harm your computer." and two buttons: "Save" and "Cancel".

27. After the completion of download, click Run to install the tool.

Note: If User Account Control window appears, click Yes.

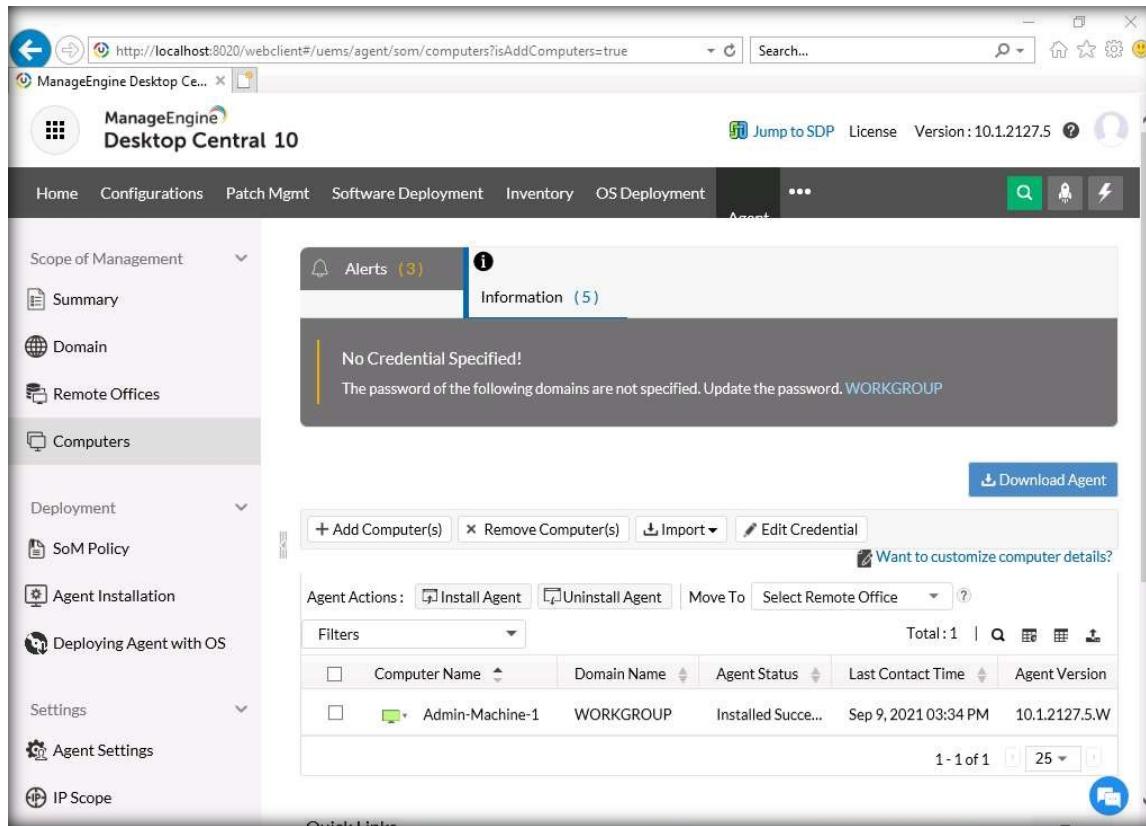
28. Follow the wizard driver installation to install the tool with default settings.

29. After the installation completes, click Close and refresh the page.

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

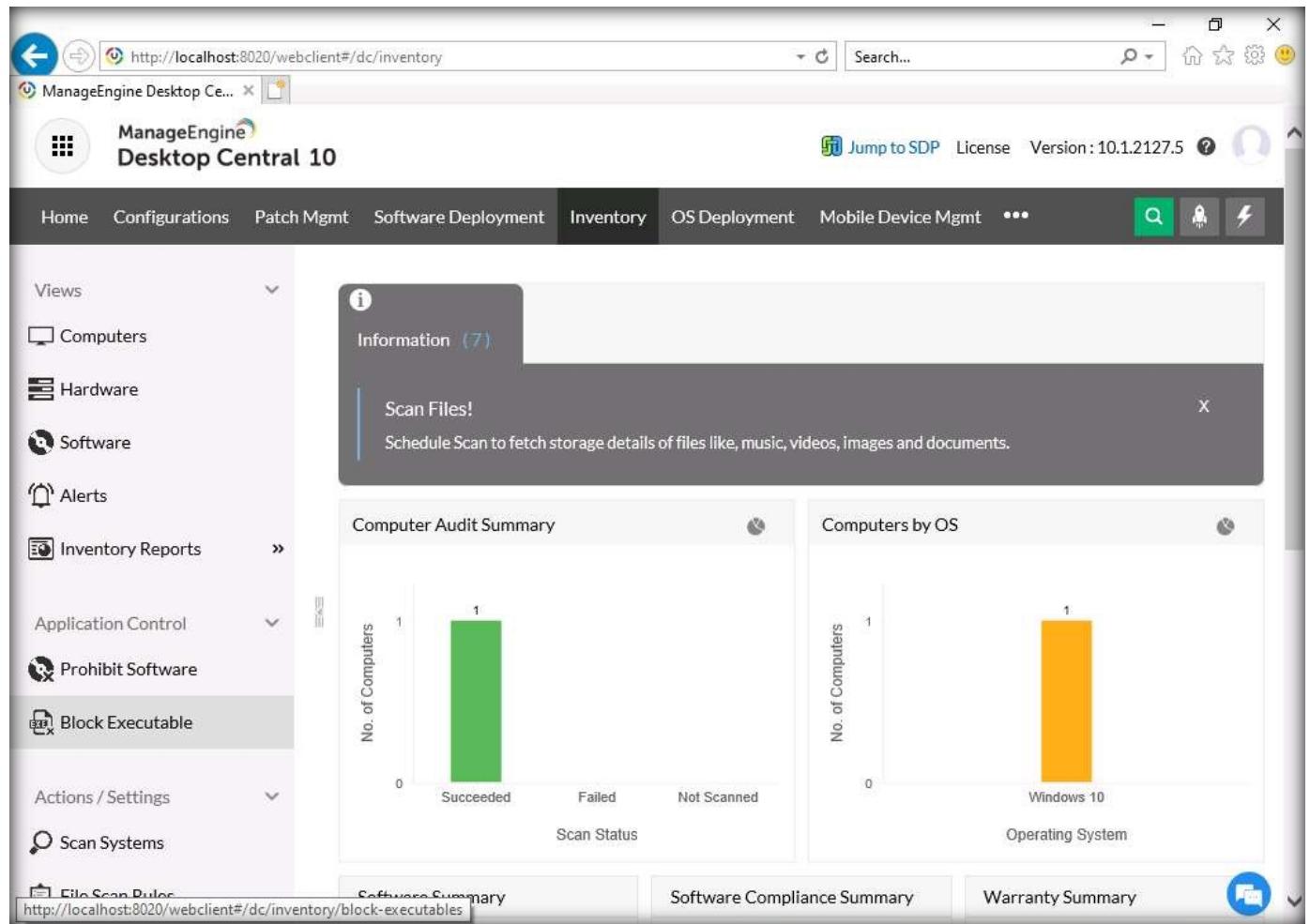
Note: If Register for free demo wizard appears, click Skip.

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



The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the address bar is <http://localhost:8020/webclient#/uem/agent/som/computers?isAddComputers=true>. The main navigation menu includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory, OS Deployment, Agent (selected), and other options. On the left, there's a sidebar with sections for Scope of Management (Summary, Domain, Remote Offices, Computers - highlighted), Deployment (SoM Policy, Agent Installation, Deploying Agent with OS), and Settings (Agent Settings, IP Scope). The main content area displays an alert about 'No Credential Specified!' for a domain named 'WORKGROUP'. Below the alert, there are buttons for '+ Add Computer(s)', 'Remove Computer(s)', 'Import', 'Edit Credential', and 'Download Agent'. A section titled 'Want to customize computer details?' is present. At the bottom, a table lists one computer entry: Admin-Machine-1, WORKGROUP, Installed Success..., Sep 9, 2021 03:34 PM, 10.1.2127.5.W. The table includes filters for Computer Name, Domain Name, Agent Status, Last Contact Time, and Agent Version.

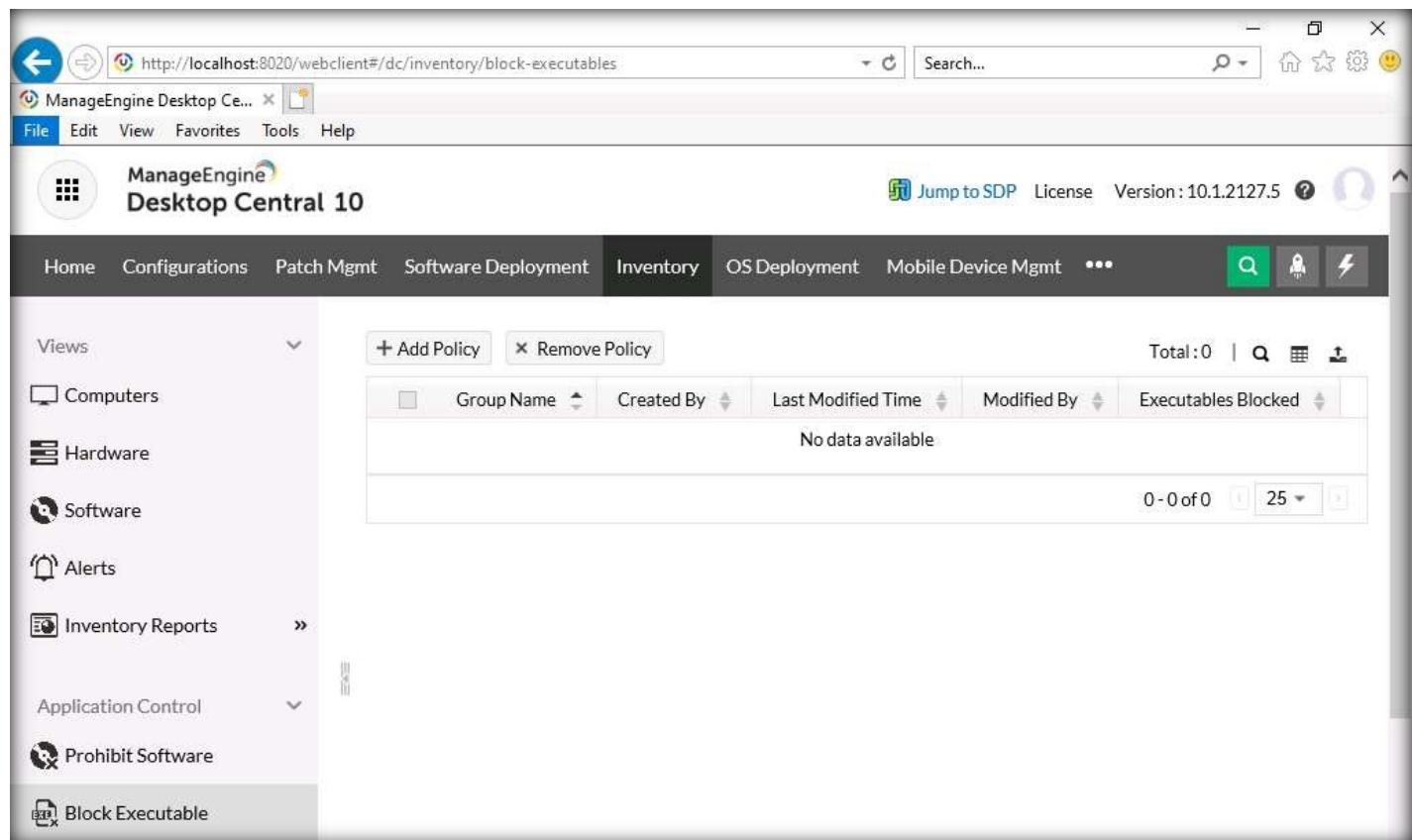
- EXERCISE 2:
BLACKLIST APPLICATION USING
MANAGEENGINE
DESKTOP CENTRAL
32. Now, click Inventory option again from the top-section of the page.
 33. Inventory page appears, click Block Executable option from the left-pane.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The left sidebar has a 'Views' section with options: Computers, Hardware, Software, Alerts, Inventory Reports (selected), Application Control, Prohibit Software, and Block Executable (highlighted in grey). Below this are Actions / Settings and Scan Systems. The main content area has tabs: Computer Audit Summary, Computers by OS, Software Summary, Software Compliance Summary, and Warranty Summary. A modal window titled 'Information (7)' says 'Scan Files!' and 'Schedule Scan to fetch storage details of files like, music, videos, images and documents.' The URL in the browser bar is <http://localhost:8020/webclient#/dc/inventory/block-executables>.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL

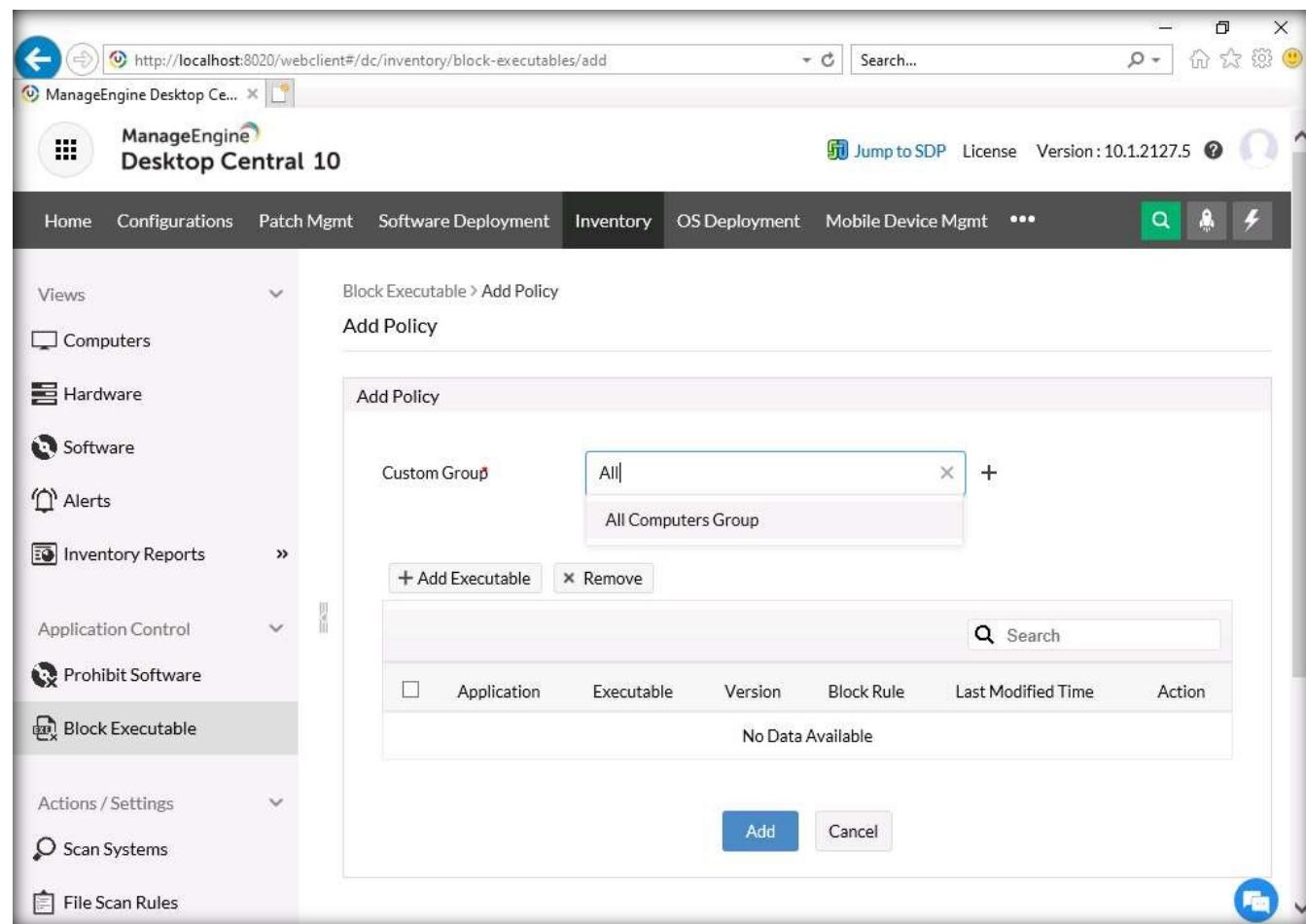
34. Block Executables page appears, click + Add Policy button from the right-pane.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the browser is <http://localhost:8020/webclient#/dc/inventory/block-executables>. The main content area is titled "Block Executables". It features a table with the following columns: Group Name, Created By, Last Modified Time, Modified By, and Executables Blocked. A message "No data available" is displayed below the table. At the top right of the table area, there are two buttons: "+ Add Policy" and "x Remove Policy". The top navigation bar includes links for Home, Configurations, Patch Mgmt, Software Deployment, Inventory (which is selected), OS Deployment, Mobile Device Mgmt, and more. The left sidebar contains links for Views, Computers, Hardware, Software, Alerts, Inventory Reports, Application Control, Prohibit Software, and Block Executable.

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.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the browser is <http://localhost:8020/webclient#/dc/inventory/block-executables/add>. The main title is "ManageEngine Desktop Central 10". The navigation bar includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory (which is selected), OS Deployment, Mobile Device Mgmt, and other options. On the left, there's a sidebar with Views (Computers, Hardware, Software, Alerts, Inventory Reports), Application Control (Prohibit Software, Block Executable - which is selected), and Actions / Settings (Scan Systems, File Scan Rules). The central content area is titled "Block Executable > Add Policy" and "Add Policy". It shows a "Custom Group" dropdown with "All" selected, and a sub-menu showing "All Computers Group". Below this are buttons for "+ Add Executable" and "Remove". A search bar and a table with columns Application, Executable, Version, Block Rule, Last Modified Time, and Action are shown, with a message "No Data Available". At the bottom are "Add" and "Cancel" buttons.

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.

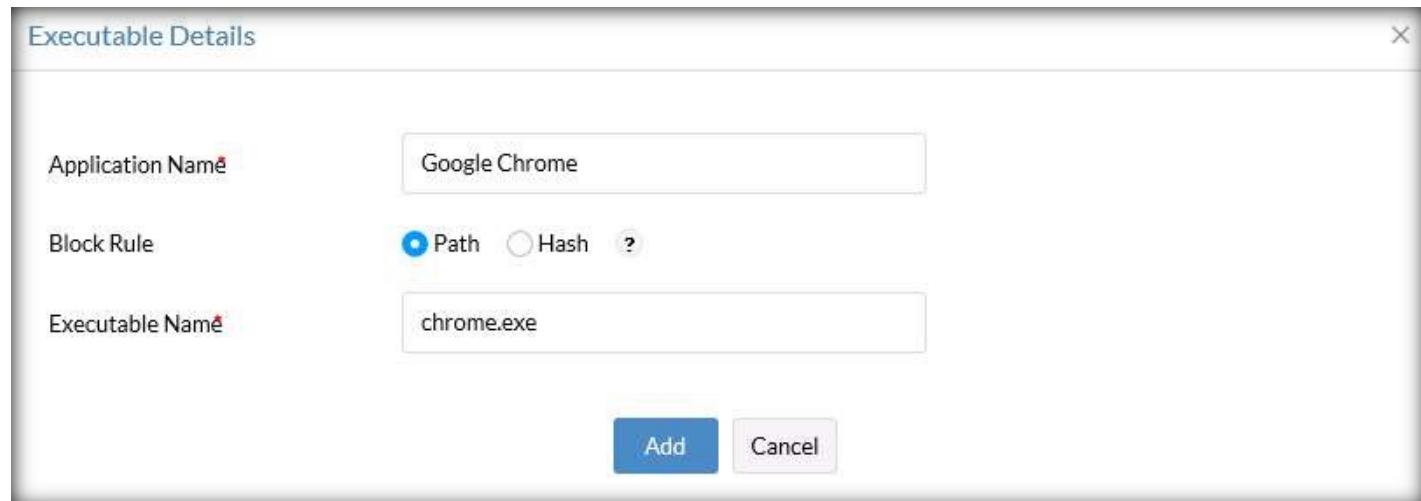
37. Leave Block Rule option set to default (Path). In the Executable Name field, type chrome.exe and click Add button.

Note:

There are two methods to block an executable/application:

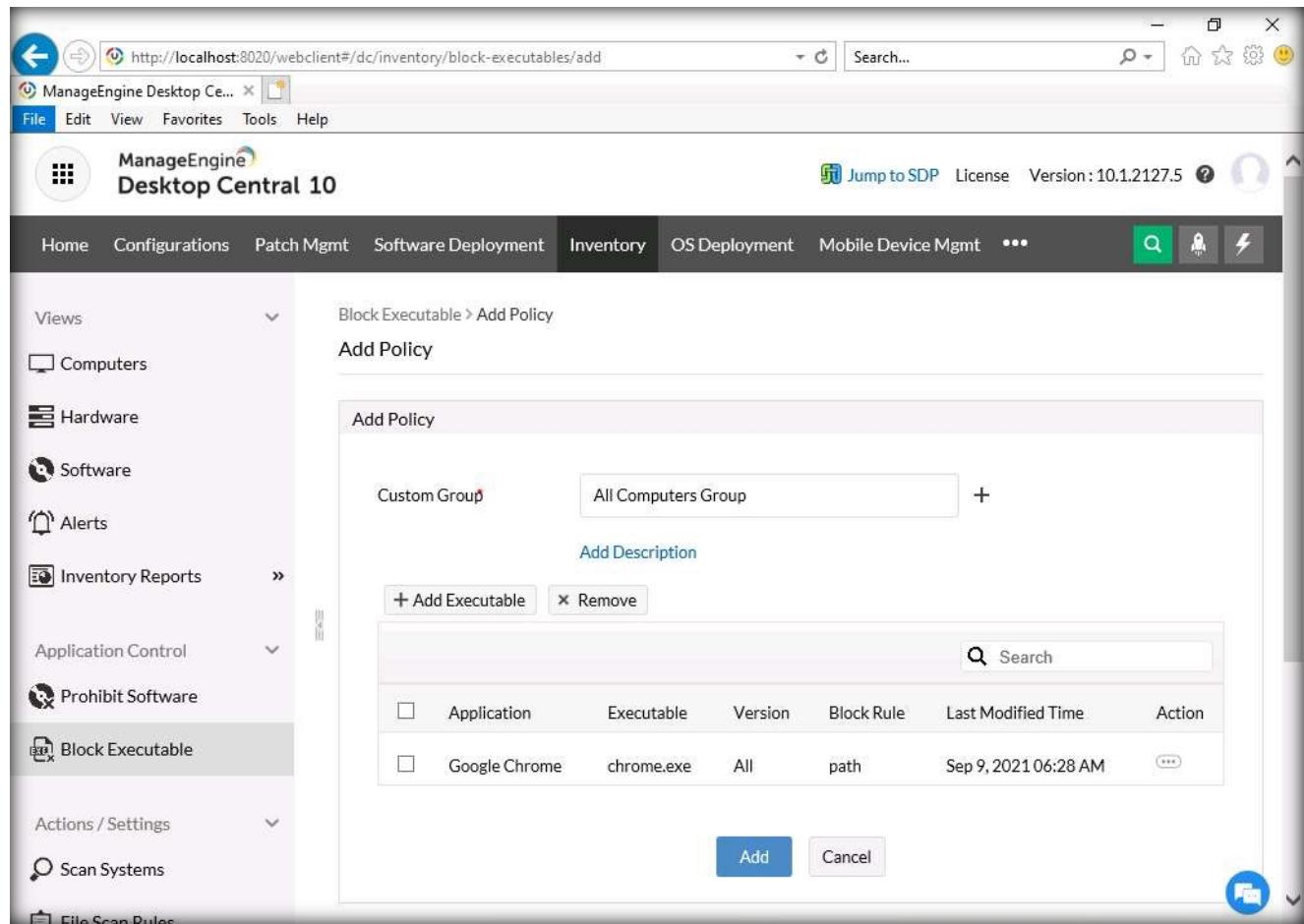
- A path rule can be used to block all versions of specific applications based on the name of the executable and its file extension.
- A hash value can be used to block executables even if they are renamed.

EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



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

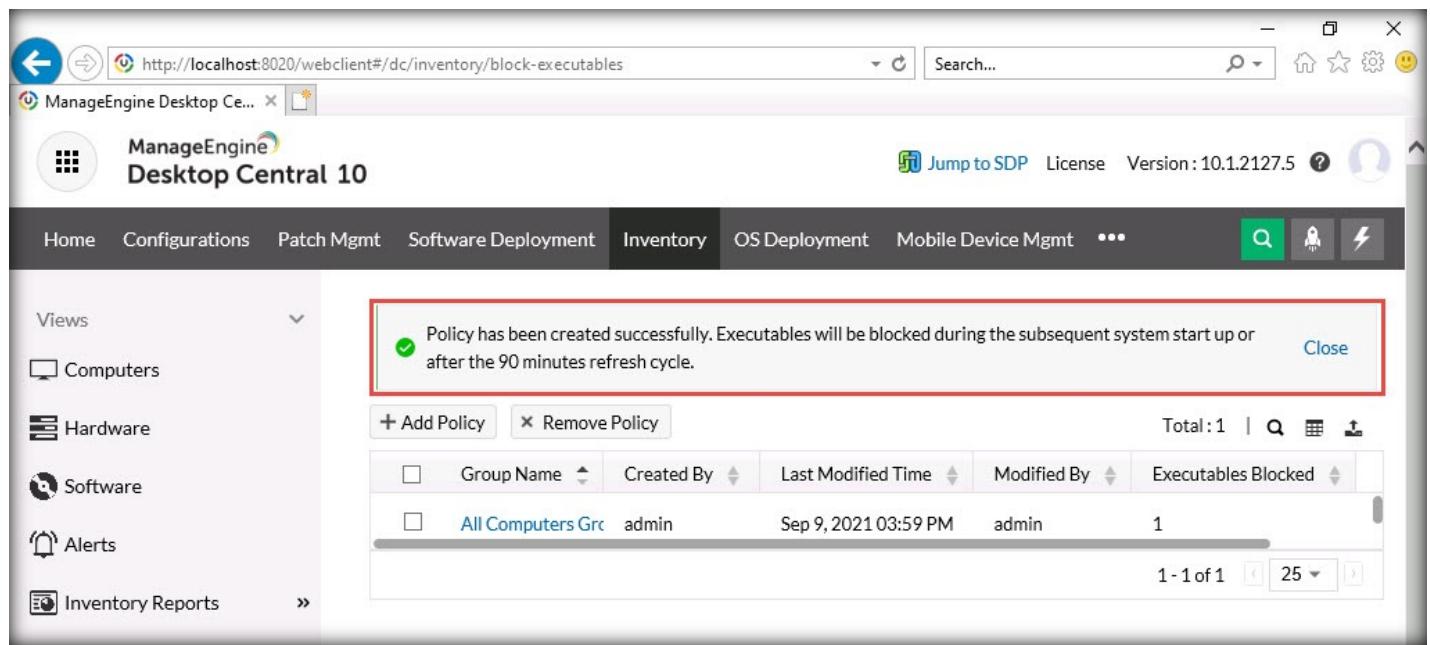
EXERCISE 2: BLACKLIST APPLICATION USING MANAGEENGINE DESKTOP CENTRAL



The screenshot shows the ManageEngine Desktop Central 10 web interface. The left sidebar contains navigation links: Home, Configurations, Patch Mgmt, Software Deployment, Inventory (selected), OS Deployment, Mobile Device Mgmt, and three more options. Under the Inventory section, 'Block Executable' is highlighted. The main content area displays the 'Block Executable > Add Policy' page. It includes a 'Custom Group' dropdown set to 'All Computers Group' with a '+' button, an 'Add Description' field, and two buttons: '+ Add Executable' and 'Remove'. A search bar is present above a table. The table lists a single entry: Google Chrome, executable chrome.exe, version All, block rule path, last modified time Sep 9, 2021 06:28 AM, and an ellipsis button. At the bottom are 'Add' and 'Cancel' buttons.

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



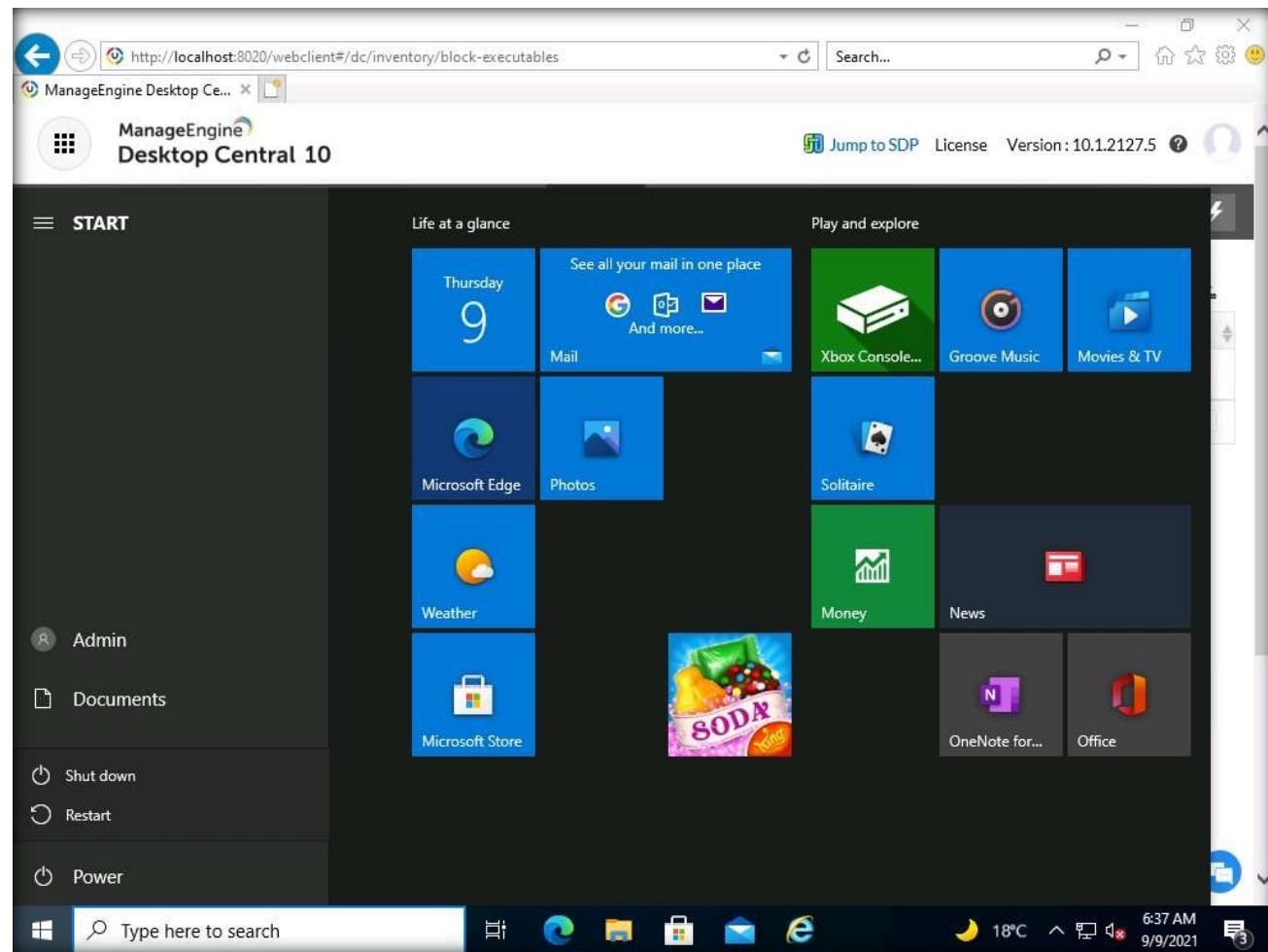
The screenshot shows the ManageEngine Desktop Central 10 web interface. The URL in the browser is <http://localhost:8020/webclient#/dc/inventory/block-executables>. The main menu includes Home, Configurations, Patch Mgmt, Software Deployment, Inventory (which is selected), OS Deployment, Mobile Device Mgmt, and other options. On the left, there's a sidebar with Views (Computers, Hardware, Software, Alerts, Inventory Reports). In the center, a message box says: "Policy has been created successfully. Executables will be blocked during the subsequent system start up or after the 90 minutes refresh cycle." Below this, there's a table with one row:

<input type="checkbox"/>	Group Name	Created By	Last Modified Time	Modified By	Executables Blocked
<input type="checkbox"/>	All Computers Grp	admin	Sep 9, 2021 03:59 PM	admin	1

At the bottom, it says "1 - 1 of 1" and there are pagination controls for 25 items.

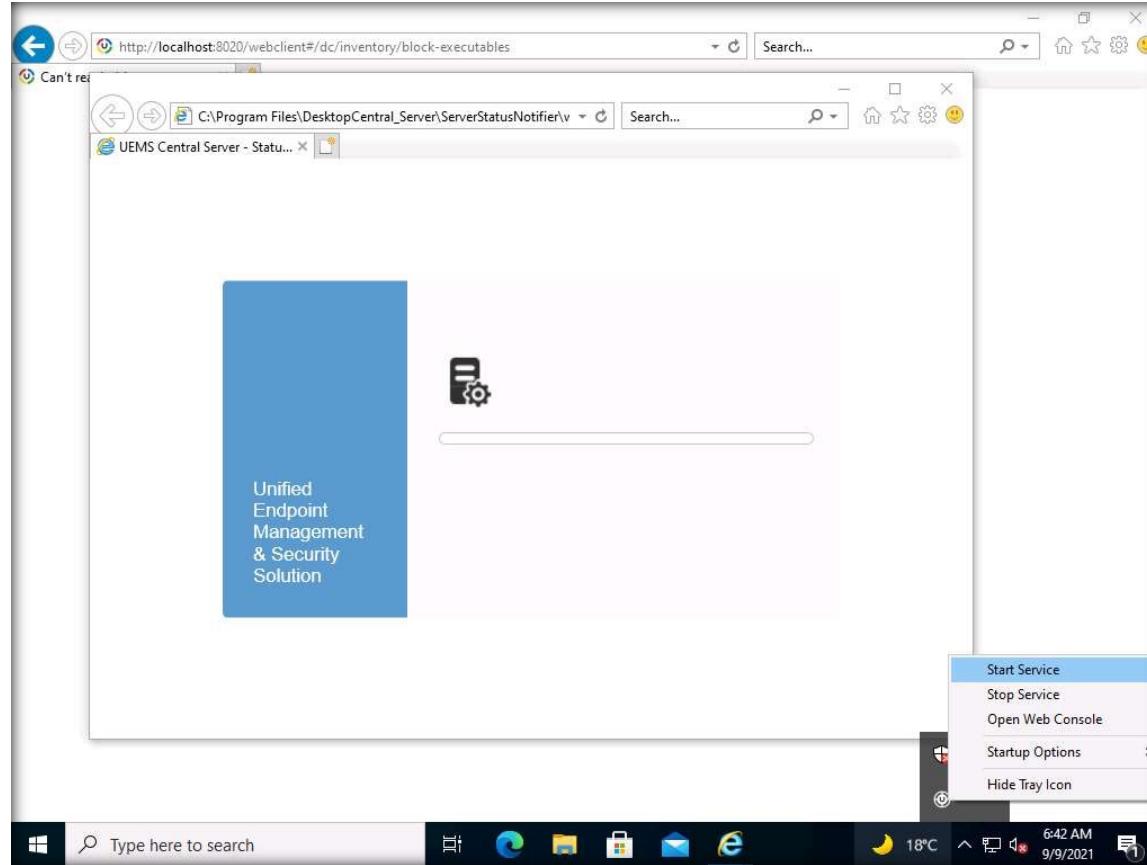
40. To block the executables, we need to Restart the system.

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

- 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.



46. If User Account Control window appears, click Yes.

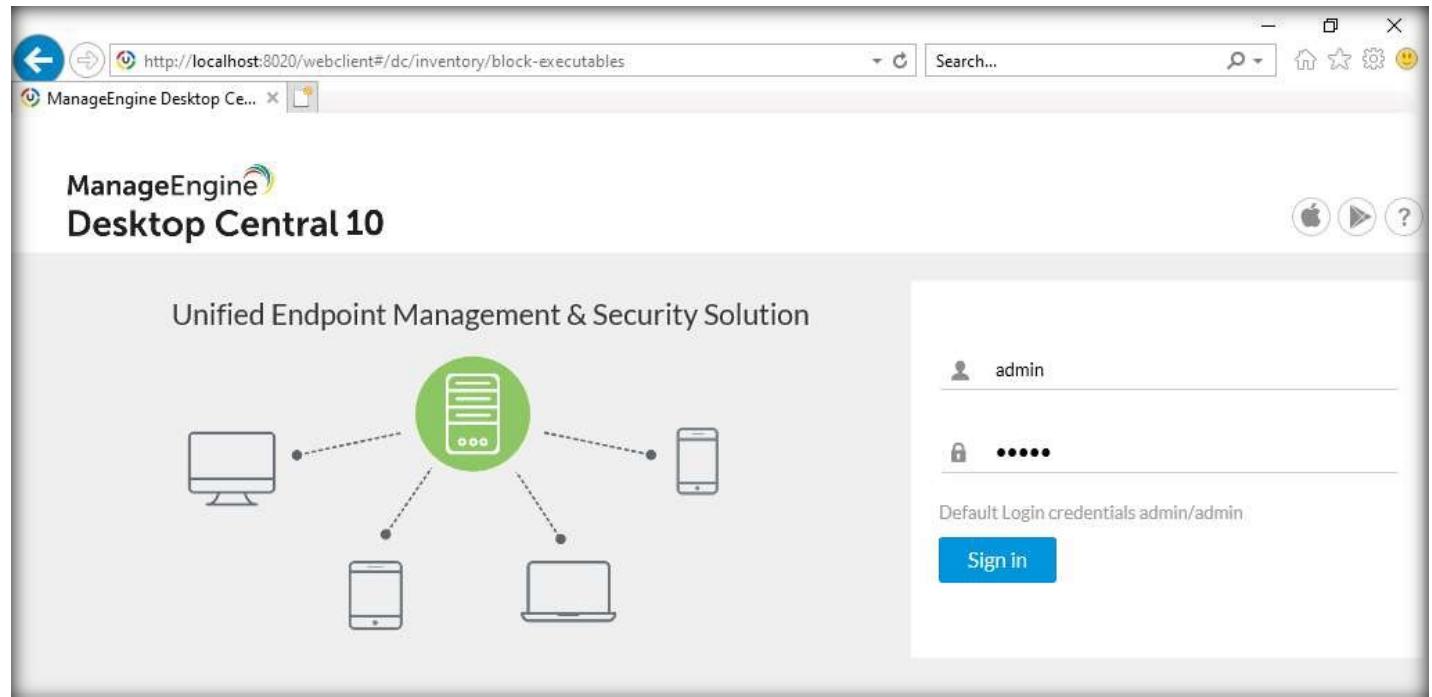
47. Navigate to Internet Explorer browser window where <http://localhost:8020> is opened. Click Refresh icon (), present in the top-section of the window next to the URL field.

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.

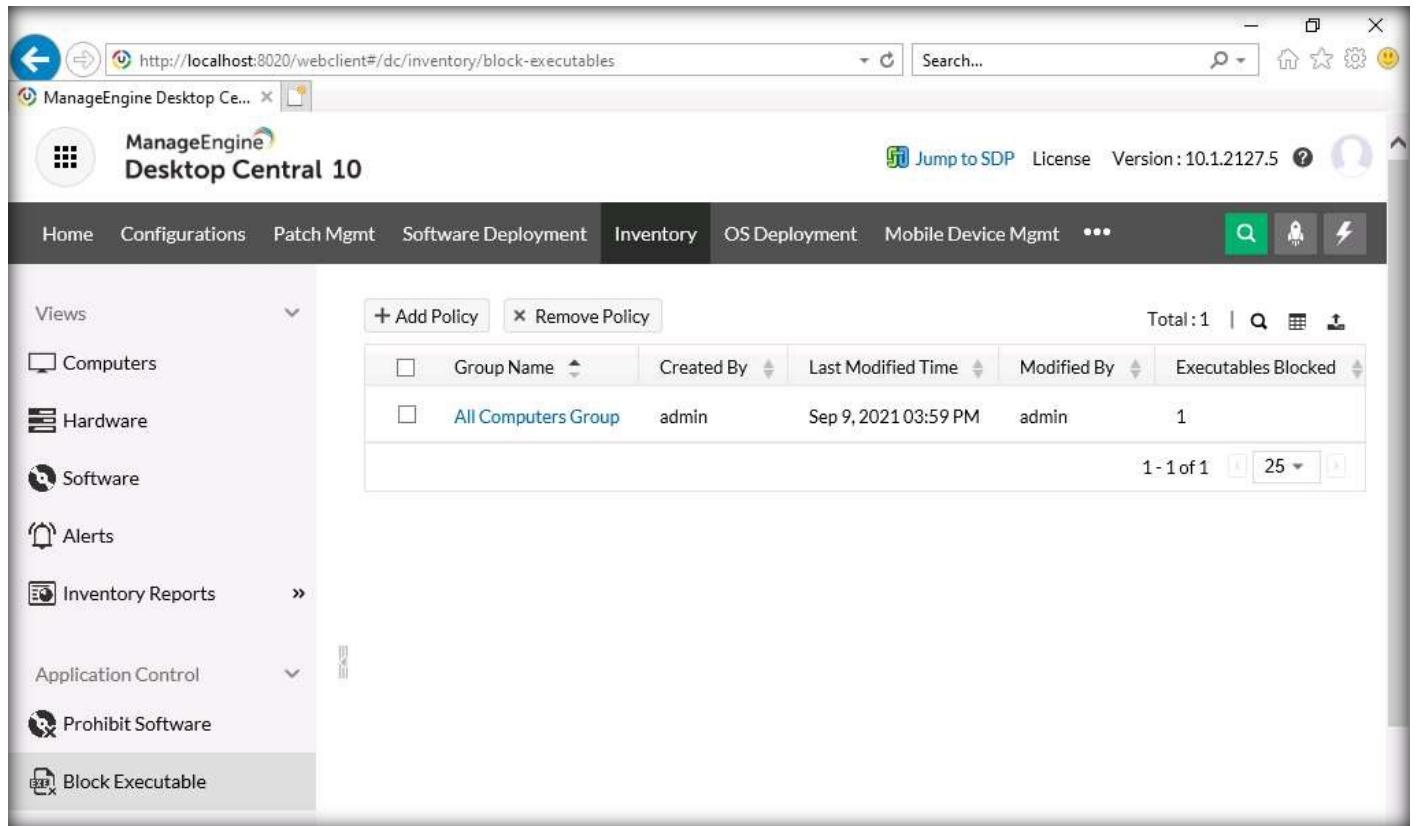
48. The main page of ManageEngine Desktop Central appears along with a login form. You can observe that, by default, credentials are entered. Click Sign in to proceed.

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.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The title bar displays "ManageEngine Desktop Ce..." and "ManageEngine Desktop Central 10". The top navigation bar includes links for Home, Configurations, Patch Mgmt, Software Deployment, **Inventory**, OS Deployment, Mobile Device Mgmt, and more. On the left sidebar, under the "Views" section, the "Block Executable" option is selected. The main content area shows a table titled "Block Executable Policies". The table has columns for Group Name, Created By, Last Modified Time, Modified By, and Executables Blocked. One policy is listed: "All Computers Group" created by "admin" on "Sep 9, 2021 03:59 PM" with "1" executable blocked. There are buttons for "+ Add Policy" and "Remove Policy".

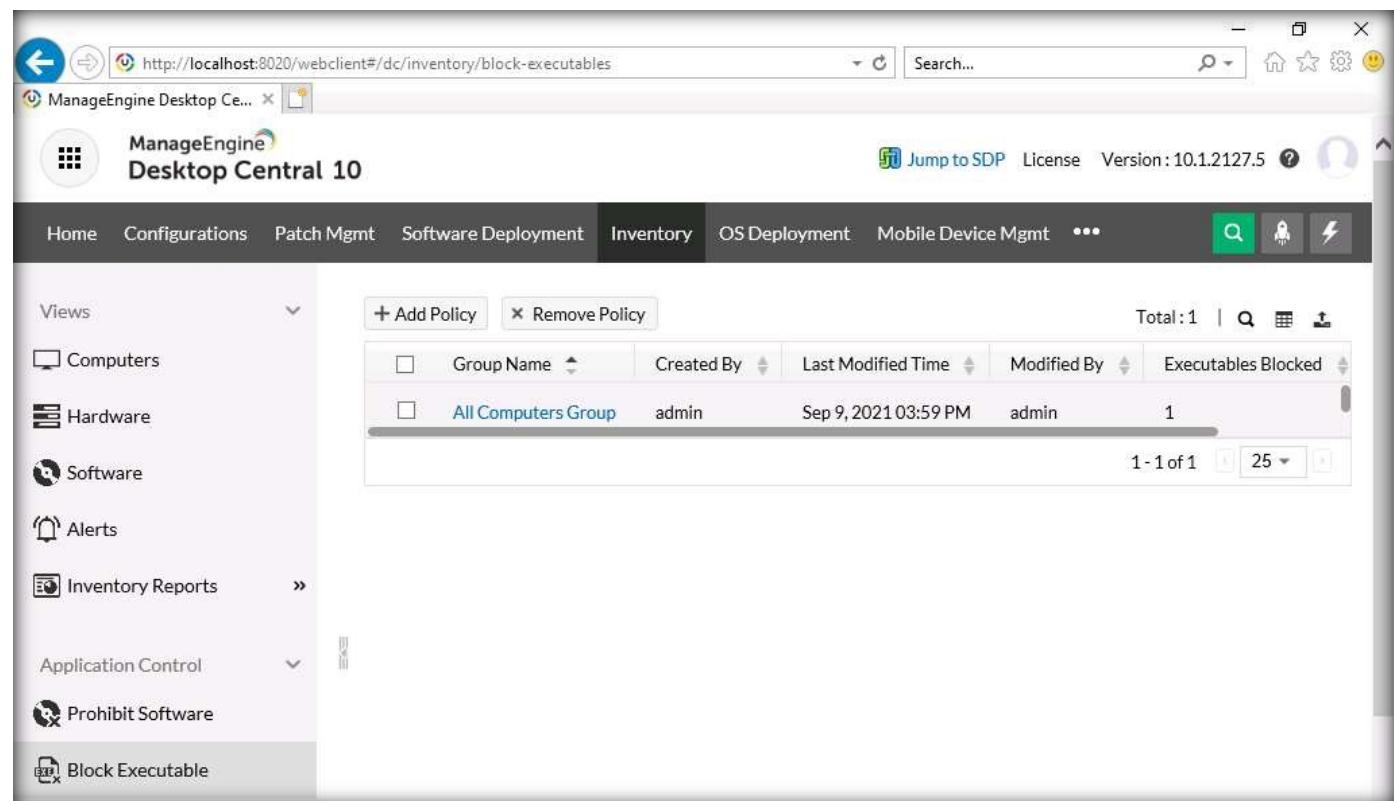
Group Name	Created By	Last Modified Time	Modified By	Executables Blocked
All Computers Group	admin	Sep 9, 2021 03:59 PM	admin	1

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.

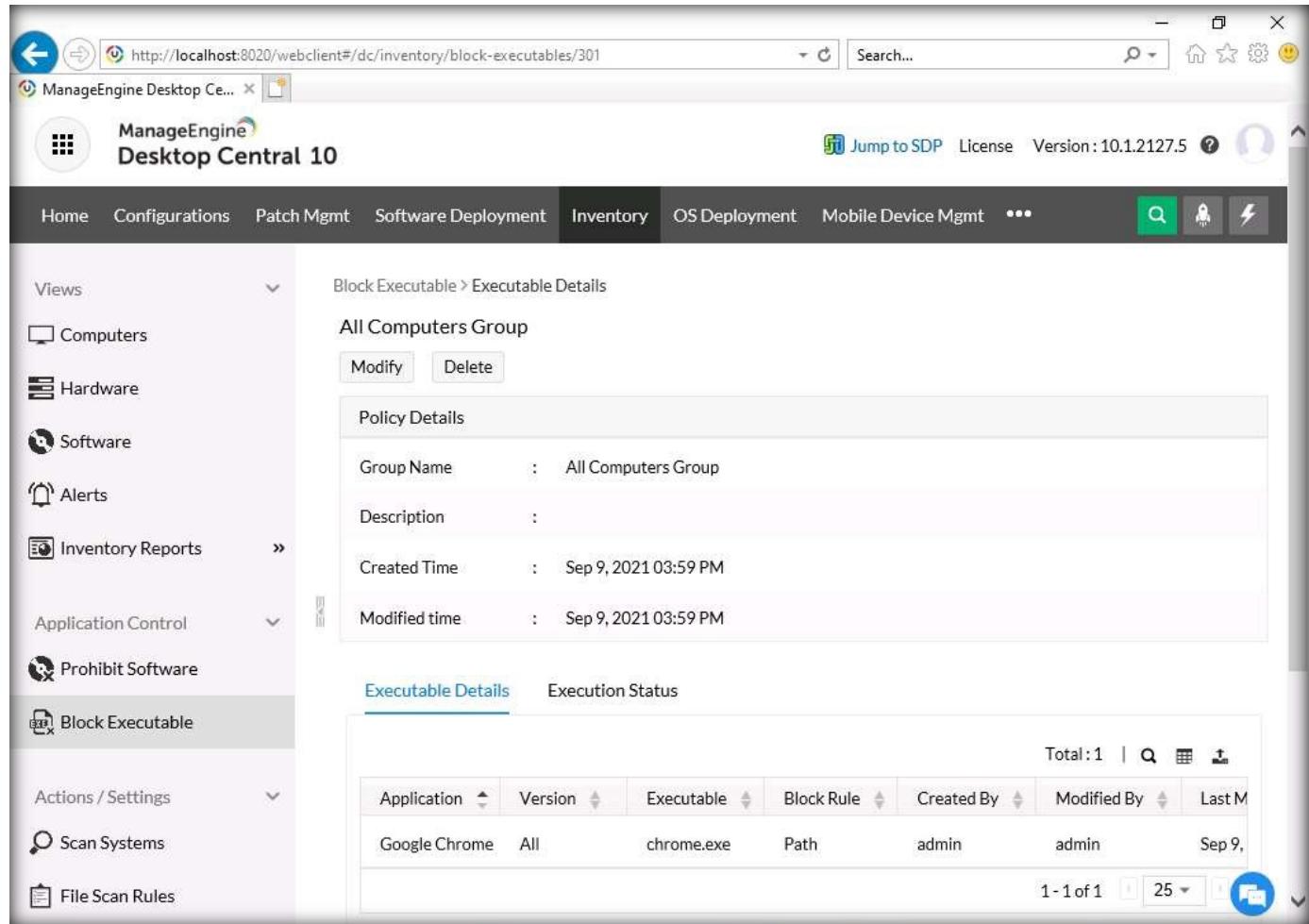
52. You can observe that the application does not open up, indicating that it has been blocked.

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



Group Name	Created By	Last Modified Time	Modified By	Executables Blocked
All Computers Group	admin	Sep 9, 2021 03:59 PM	admin	1

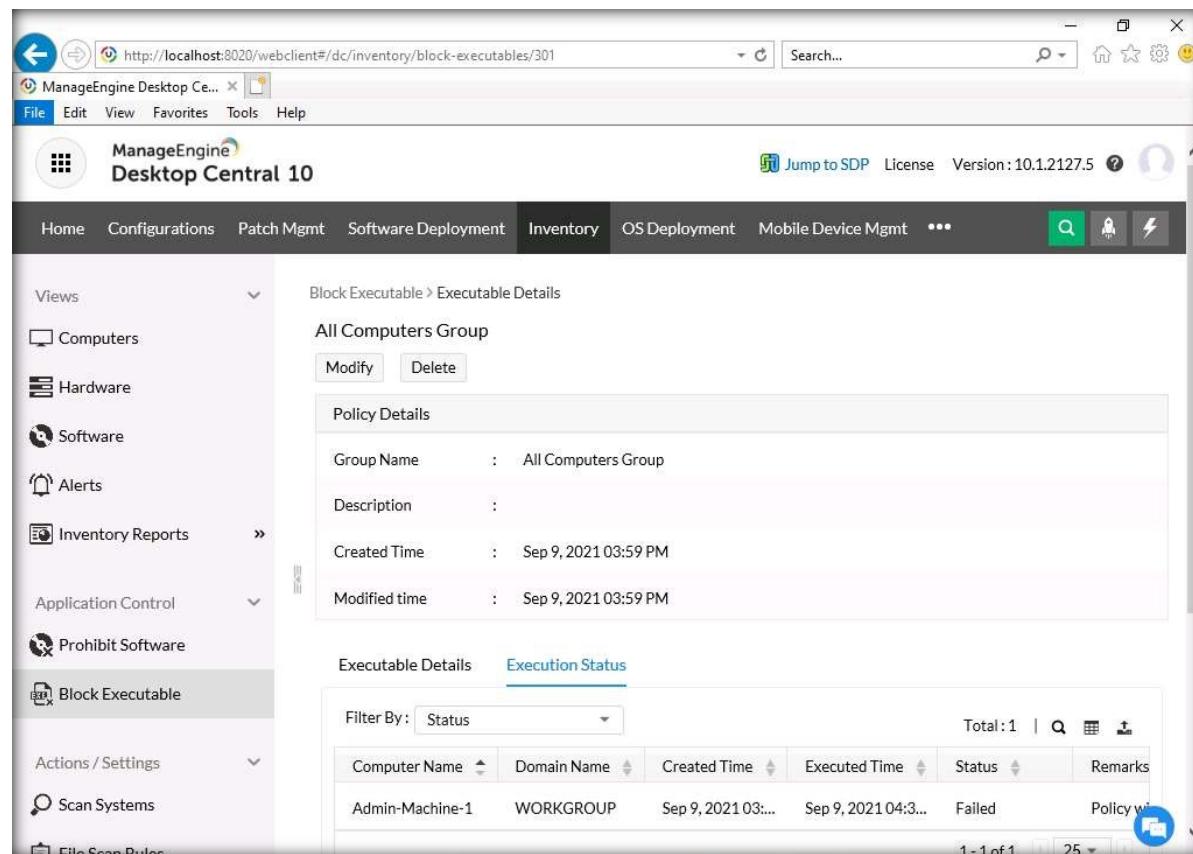
54. All Computers Group policy details appears, as shown in the screenshot below.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The left sidebar has categories like Home, Configurations, Patch Mgmt, Software Deployment, Inventory (selected), OS Deployment, Mobile Device Mgmt, and more. Under Application Control, 'Block Executable' is selected. The main content area shows 'Block Executable > Executable Details' for the 'All Computers Group'. It displays policy details: Group Name (All Computers Group), Description (empty), Created Time (Sep 9, 2021 03:59 PM), and Modified time (Sep 9, 2021 03:59 PM). Below this is an 'Executable Details' table with one entry: Application (Google Chrome), Version (All), Executable (chrome.exe), Block Rule (Path), Created By (admin), Modified By (admin), and Last M (Sep 9, 2021).

Application	Version	Executable	Block Rule	Created By	Modified By	Last M
Google Chrome	All	chrome.exe	Path	admin	admin	Sep 9, 2021

- 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.



The screenshot shows the ManageEngine Desktop Central 10 web interface. The left sidebar has a 'Block Executable' item selected under 'Application Control'. The main content area shows 'All Computers Group' policy details, including group name, description, creation time, and modification time. Below this, the 'Execution Status' tab of the 'Executable Details' section is active, displaying a table of execution results. One row is visible for 'Admin-Machine-1', showing a failed status with a comment 'Policy will be applied after system restart'.

Computer Name	Domain Name	Created Time	Executed Time	Status	Remarks
Admin-Machine-1	WORKGROUP	Sep 9, 2021 03:...	Sep 9, 2021 04:3...	Failed	Policy will be applied after system restart

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.

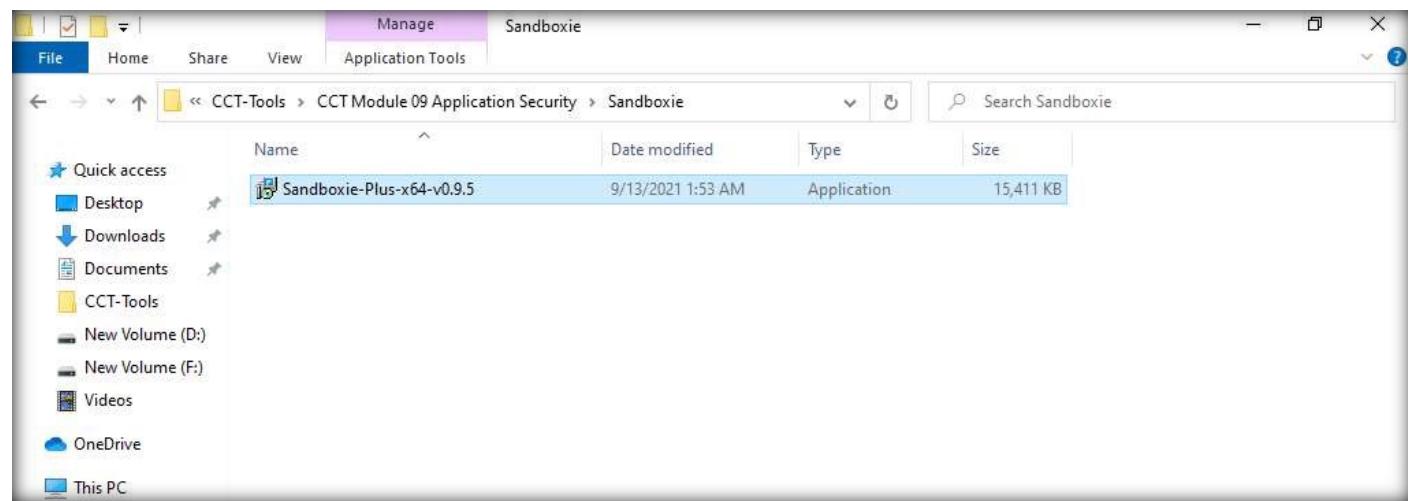
Installing a sandboxed app in a system creates a specific directory (sandboxed directory). By default, the app has unlimited read and write access to the directory. However, apps within the directory are not allowed to read or write the files outside the directory or access other system resources, unless authorized.

EXERCISE 3:

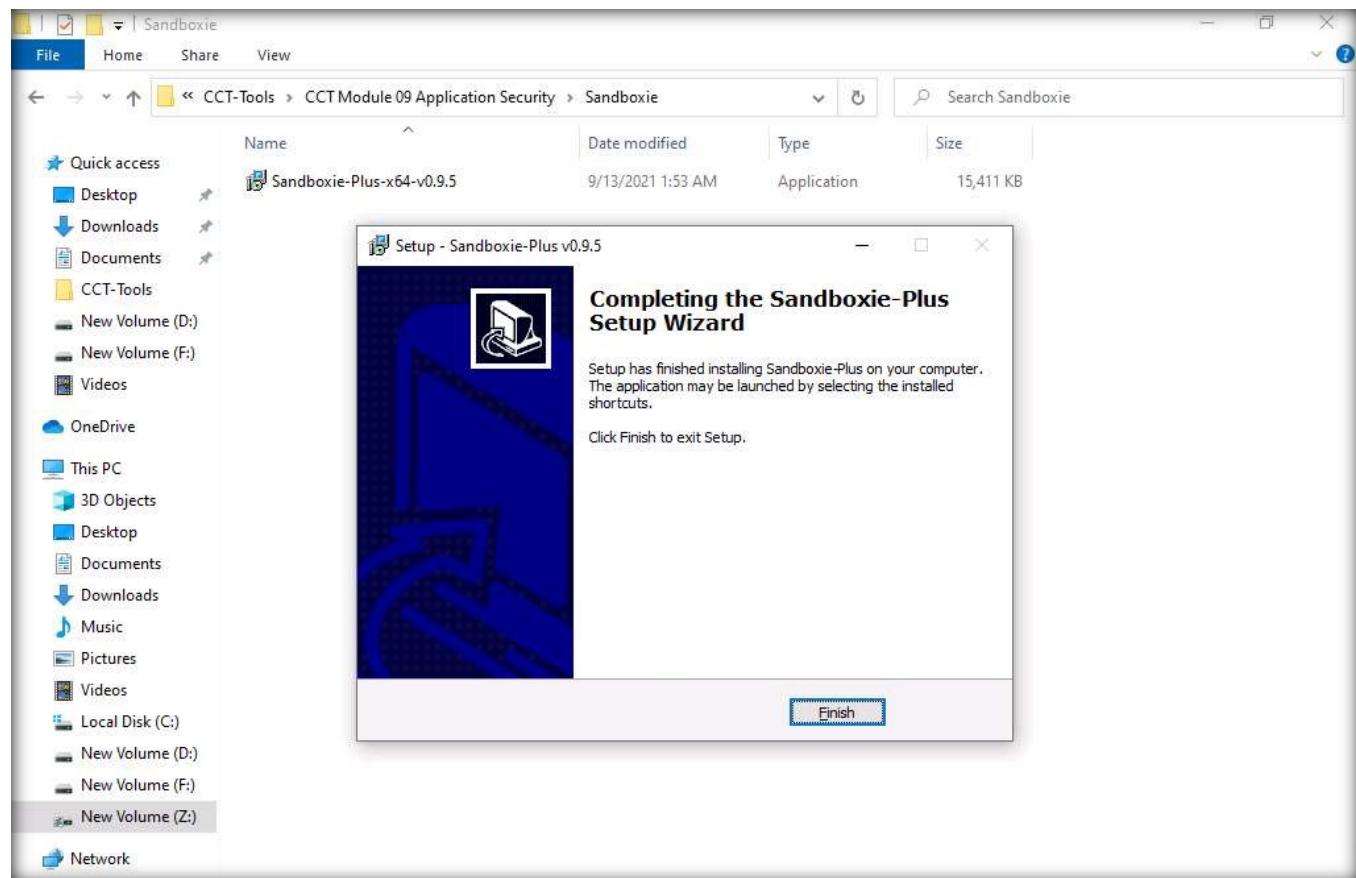
PERFORM APPLICATION SANDBOXING USING SANDBOXIE

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.

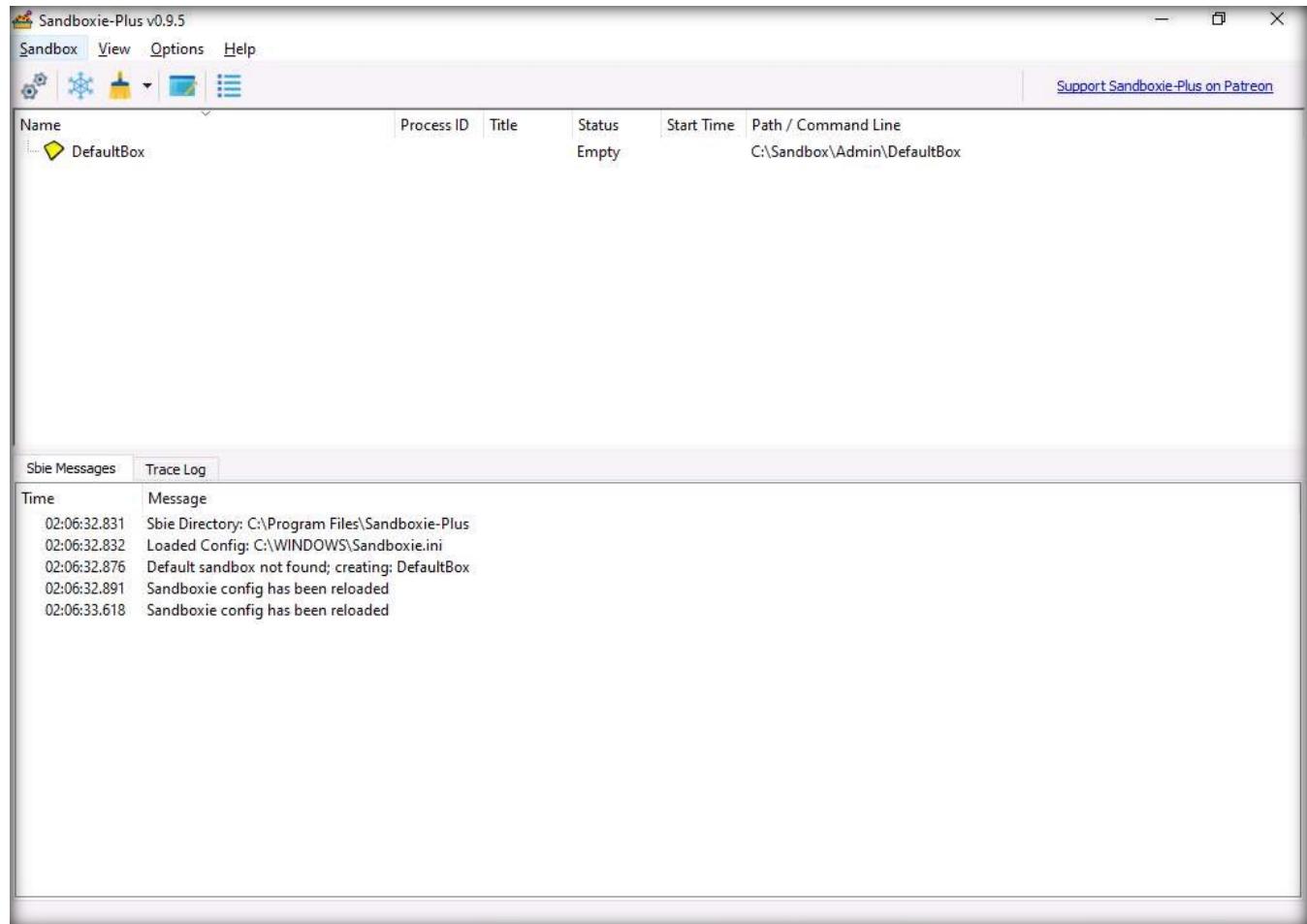


- EXERCISE 3:
PERFORM APPLICATION SANDBOXING USING SANDBOXIE
2. A User Account Control pop-up appears, click Yes.
 3. Select Setup Language wizard appears, leave default language selected as English, click OK.
 4. Follow the wizard driven installation and install the tool with the default settings.
 5. After the installation completes, click Finish.



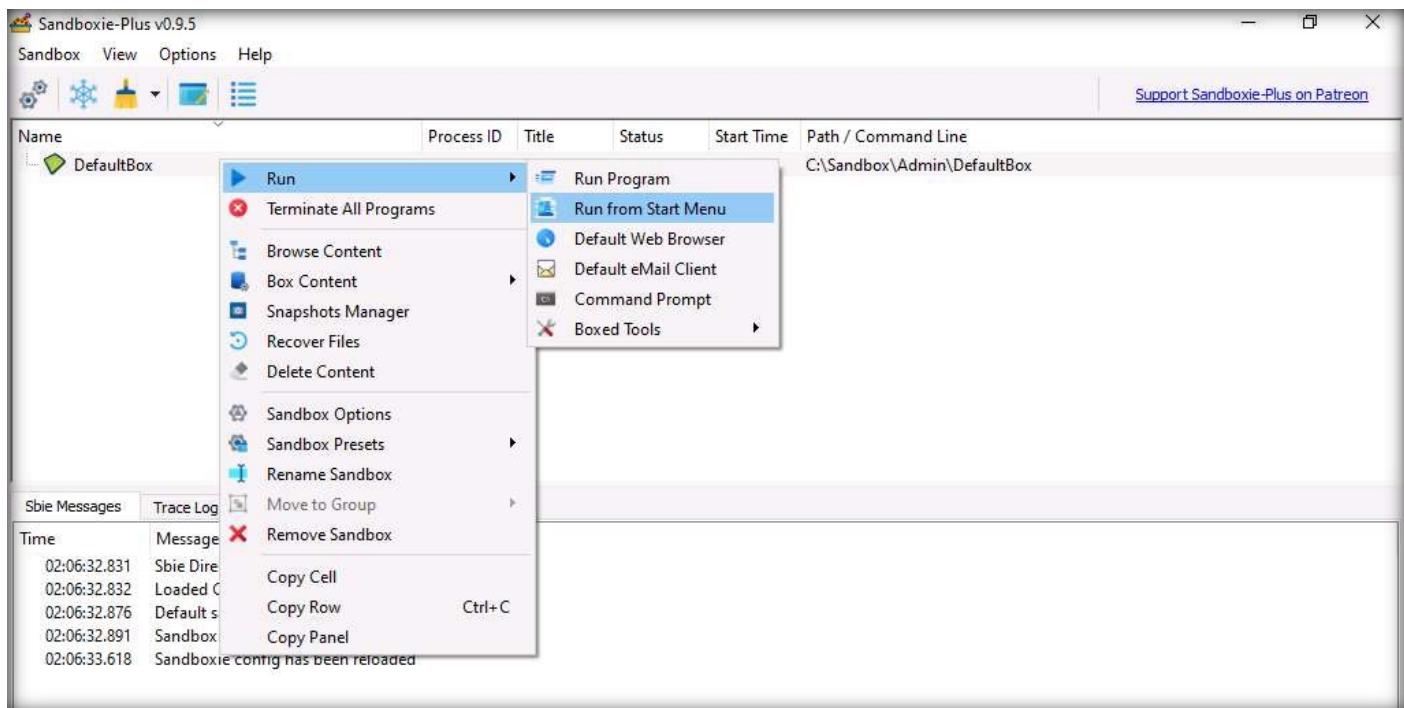
6. Now, close the File Explorer window and double-click Sandboxie-Plus shortcut present on the Desktop.

7. Sandboxie window appears, maximise it.



EXERCISE 3: PERFORM APPLICATION SANDBOXING USING SANDBOXIE

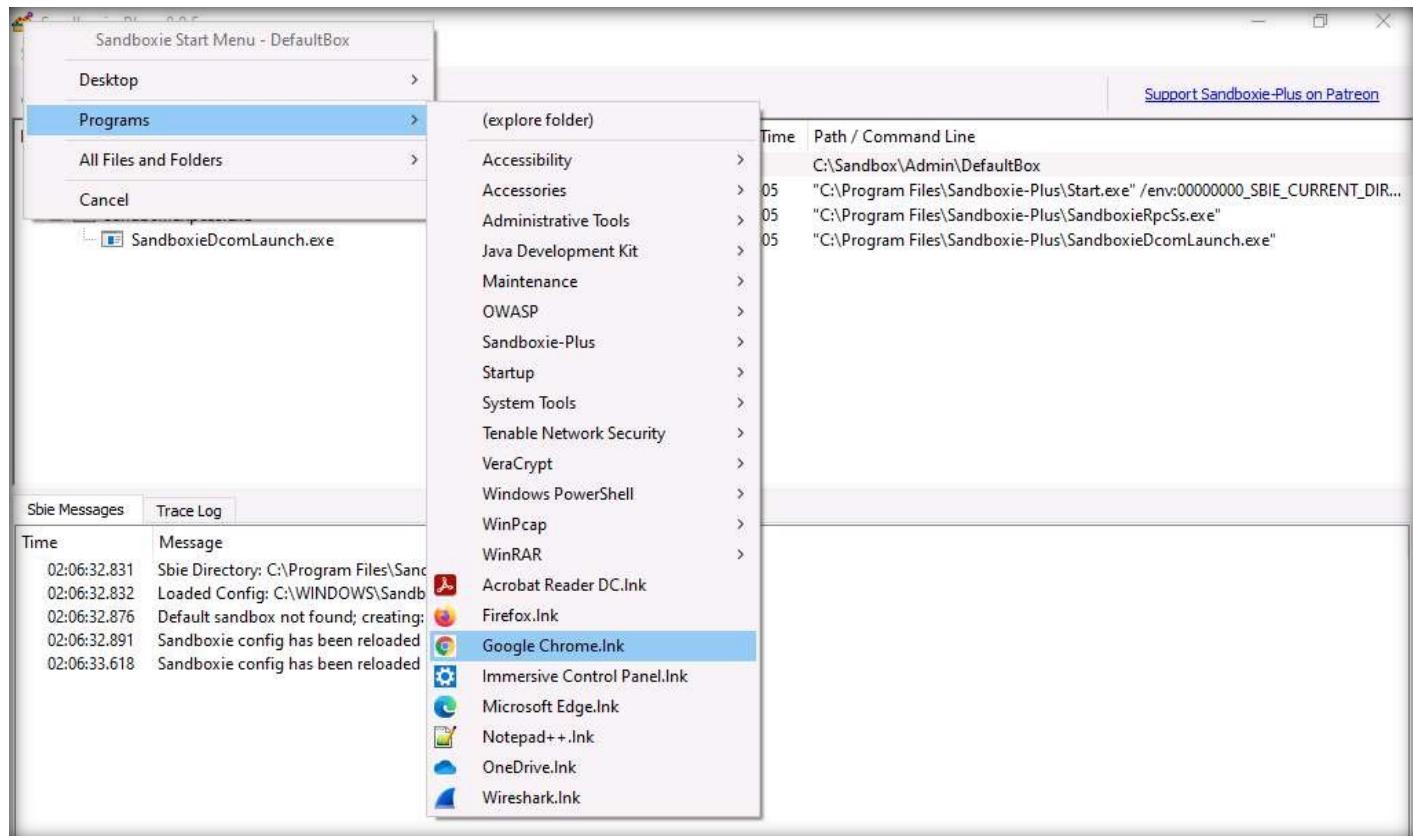
8. You can observe that a DefaultBox is present by default with the Status as Empty. Right-click on it and navigate to Run → Run from Start Menu.



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

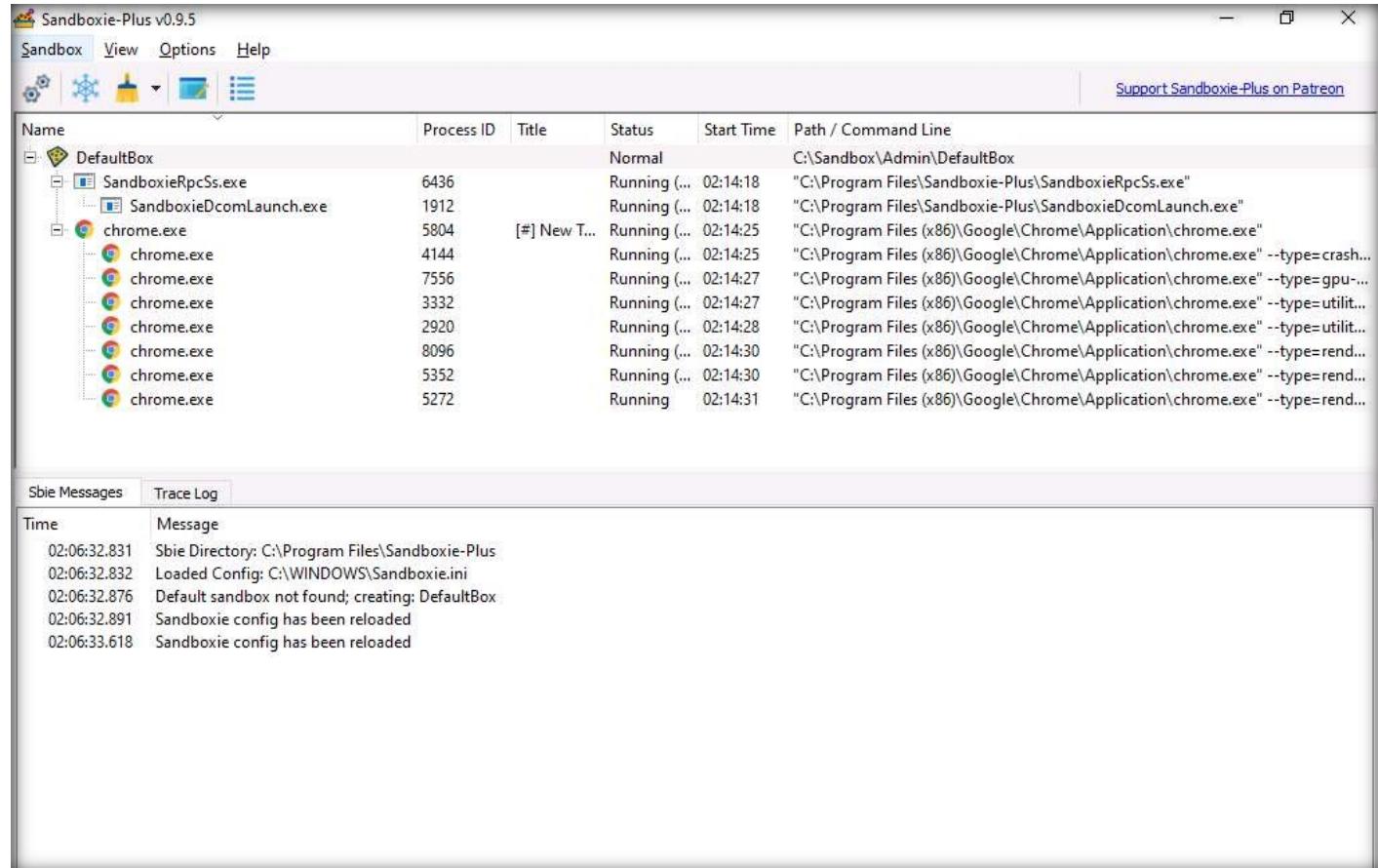
10. Navigate to Programs → Google Chrome.lnk.

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.



Name	Process ID	Title	Status	Start Time	Path / Command Line
DefaultBox			Normal		C:\Sandbox\Admin\DefaultBox
SandboxieRpcSs.exe	6436		Running (...)	02:14:18	"C:\Program Files\Sandboxie-Plus\SandboxieRpcSs.exe"
SandboxieDcomLaunch.exe	1912		Running (...)	02:14:18	"C:\Program Files\Sandboxie-Plus\SandboxieDcomLaunch.exe"
chrome.exe	5804	[#] New T...	Running (...)	02:14:25	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
chrome.exe	4144		Running (...)	02:14:25	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crash..."
chrome.exe	7556		Running (...)	02:14:27	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu..."
chrome.exe	3332		Running (...)	02:14:27	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utilit..."
chrome.exe	2920		Running (...)	02:14:28	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utilit..."
chrome.exe	8096		Running (...)	02:14:30	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=rend..."
chrome.exe	5352		Running (...)	02:14:30	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=rend..."
chrome.exe	5272		Running	02:14:31	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=rend..."

Sbie Messages

Time	Message
02:06:32.831	Sbie Directory: C:\Program Files\Sandboxie-Plus
02:06:32.832	Loaded Config: C:\WINDOWS\Sandboxie.ini
02:06:32.876	Default sandbox not found; creating: DefaultBox
02:06:32.891	Sandboxie config has been reloaded
02:06:33.618	Sandboxie config has been reloaded

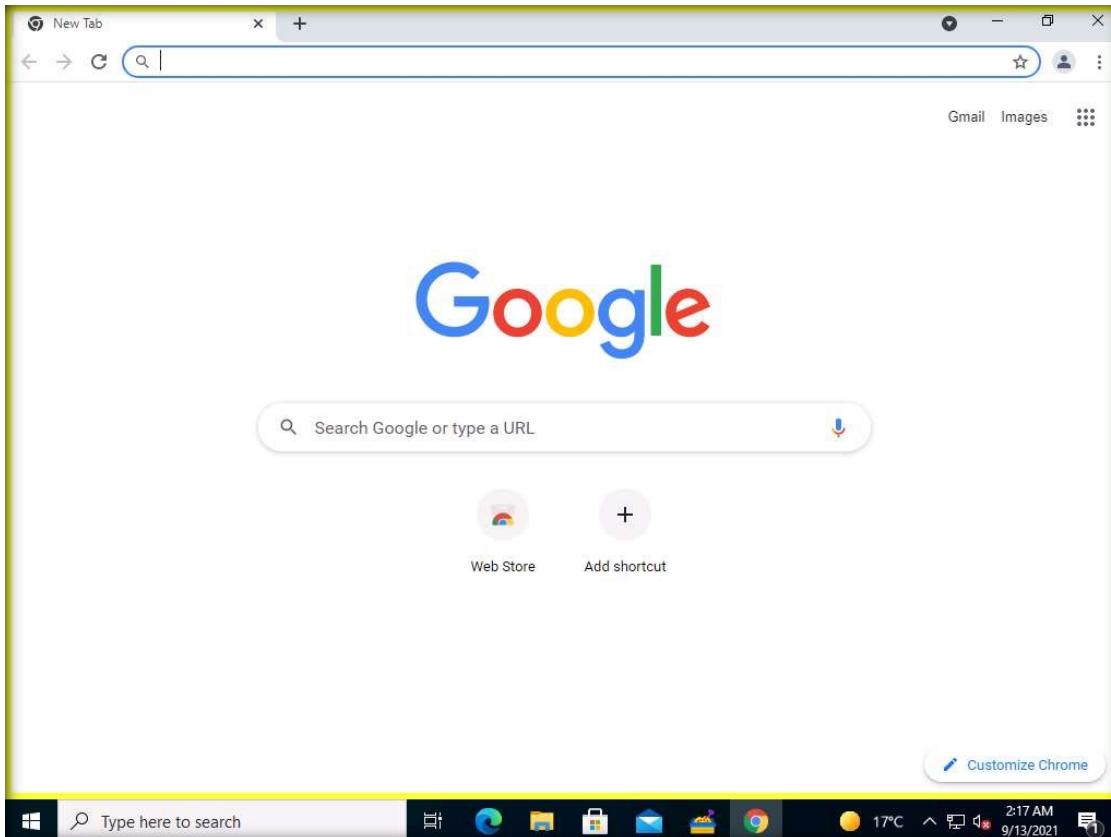
Trace Log

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 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.

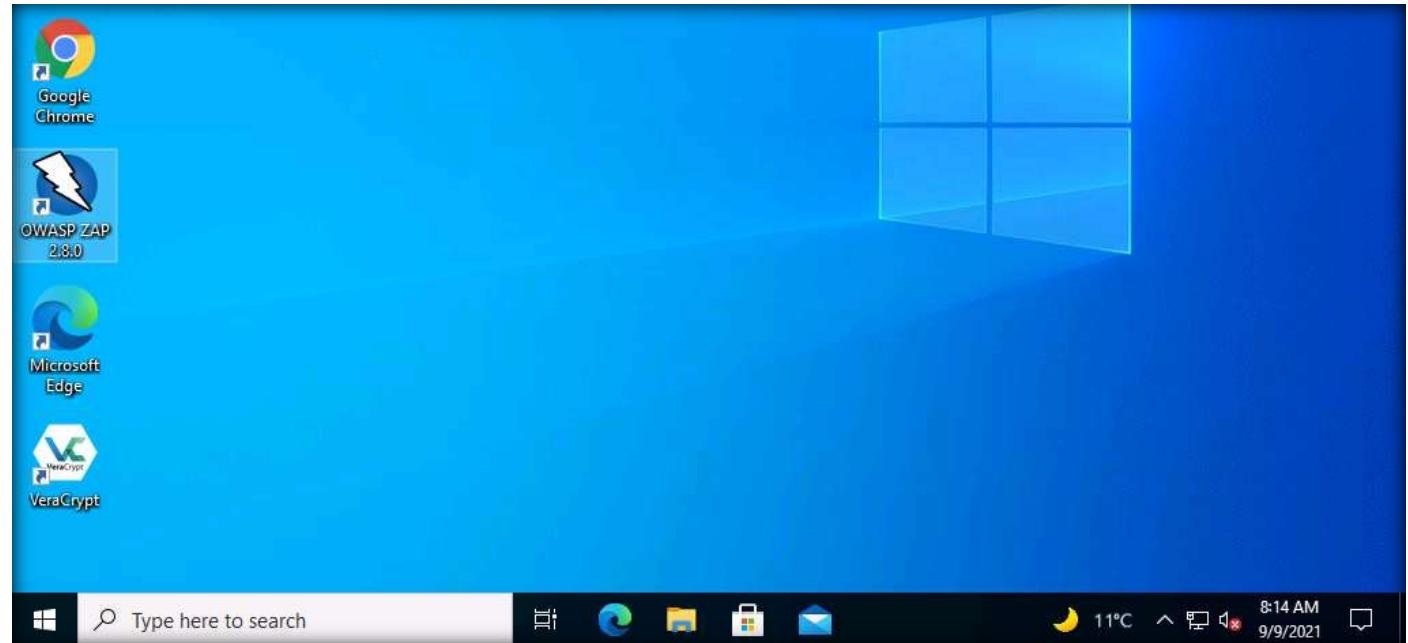
1. In the Admin Machine-1 virtual machine, double-click the OWASP ZAP shortcut on Desktop to launch the application.

Note: Wait for a while for OWASP ZAP to get launched.

Note: If an OWASP ZAP pop-up window appears, click OK.

EXERCISE 4:

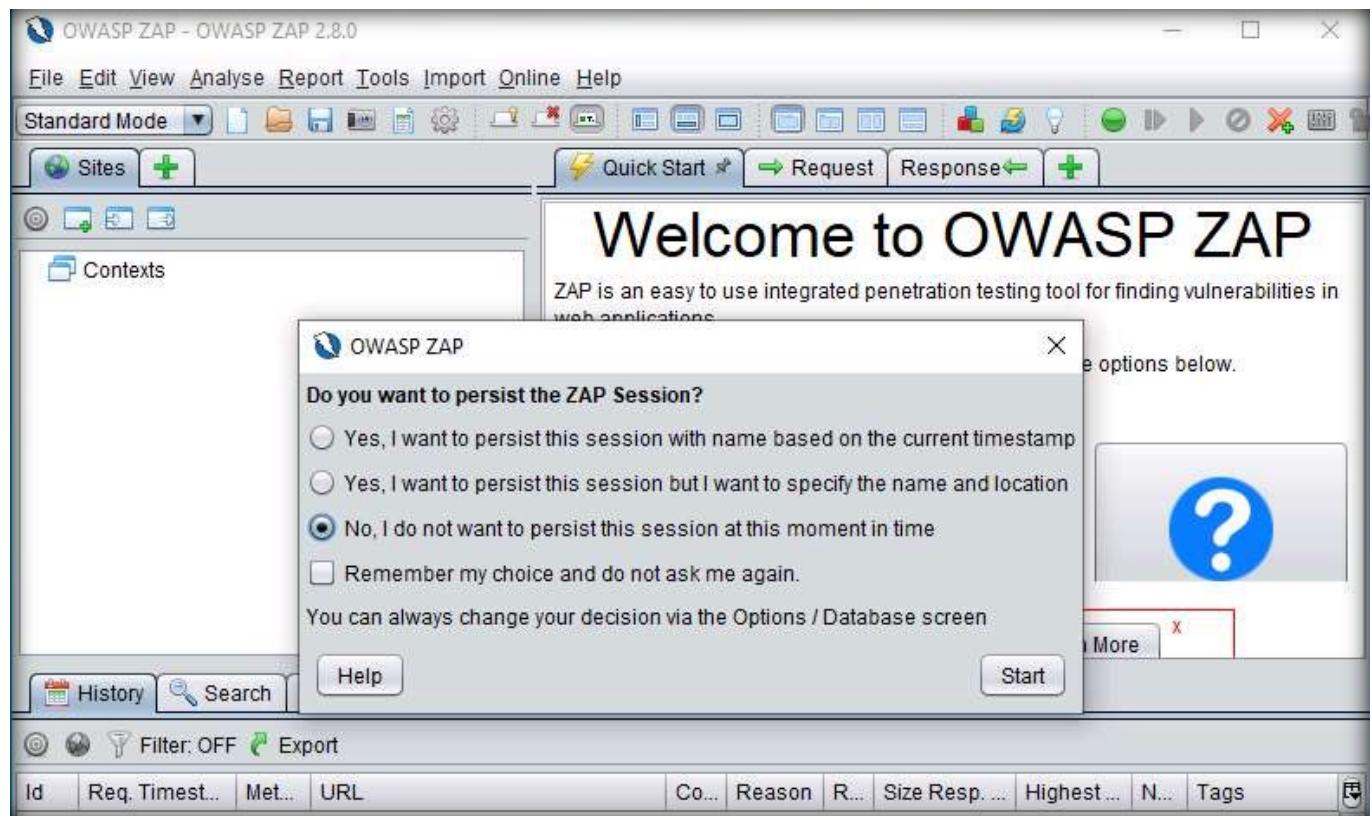
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



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.

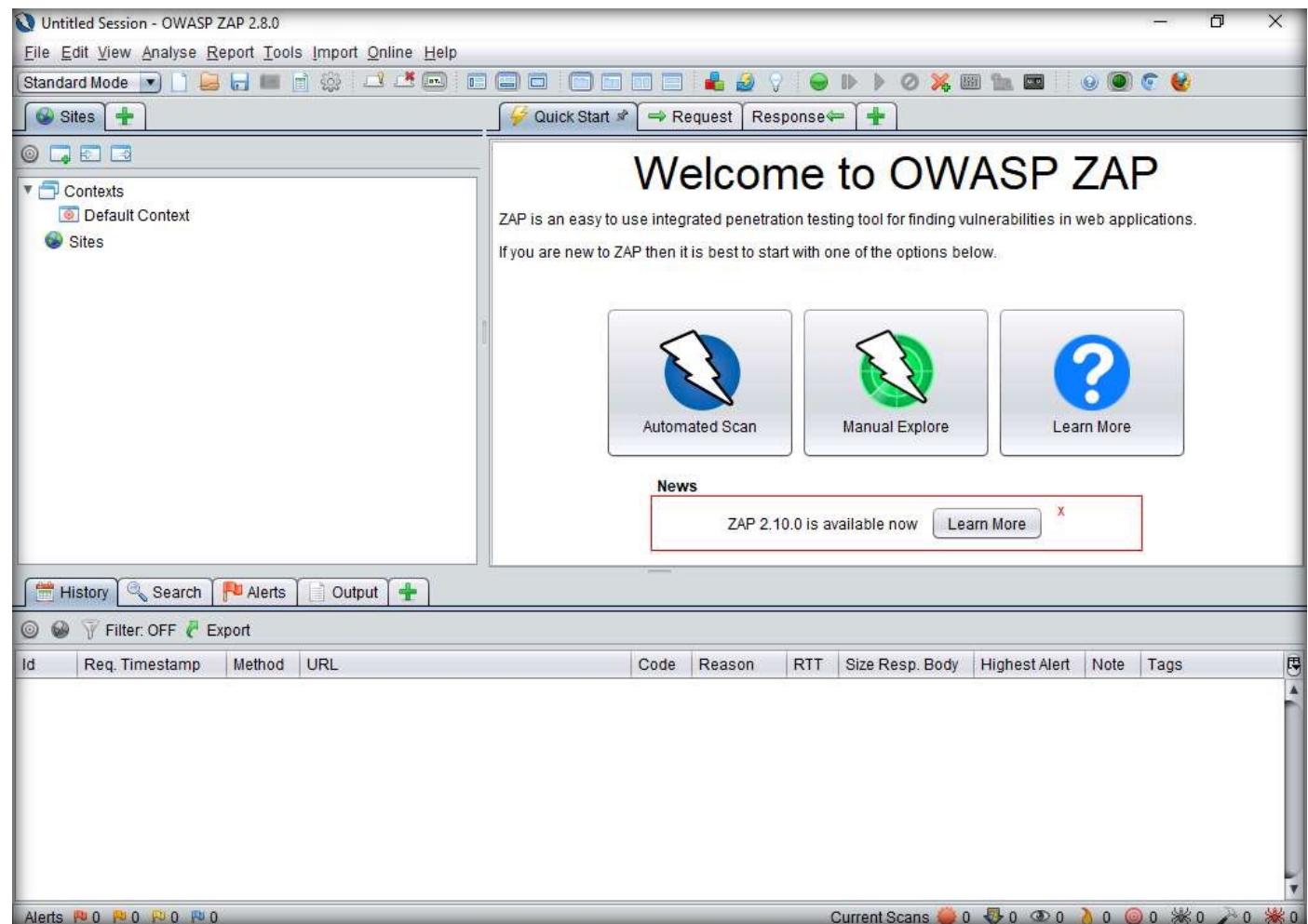
Note: If a Manage Add-ons window appears, close it.



EXERCISE 4:

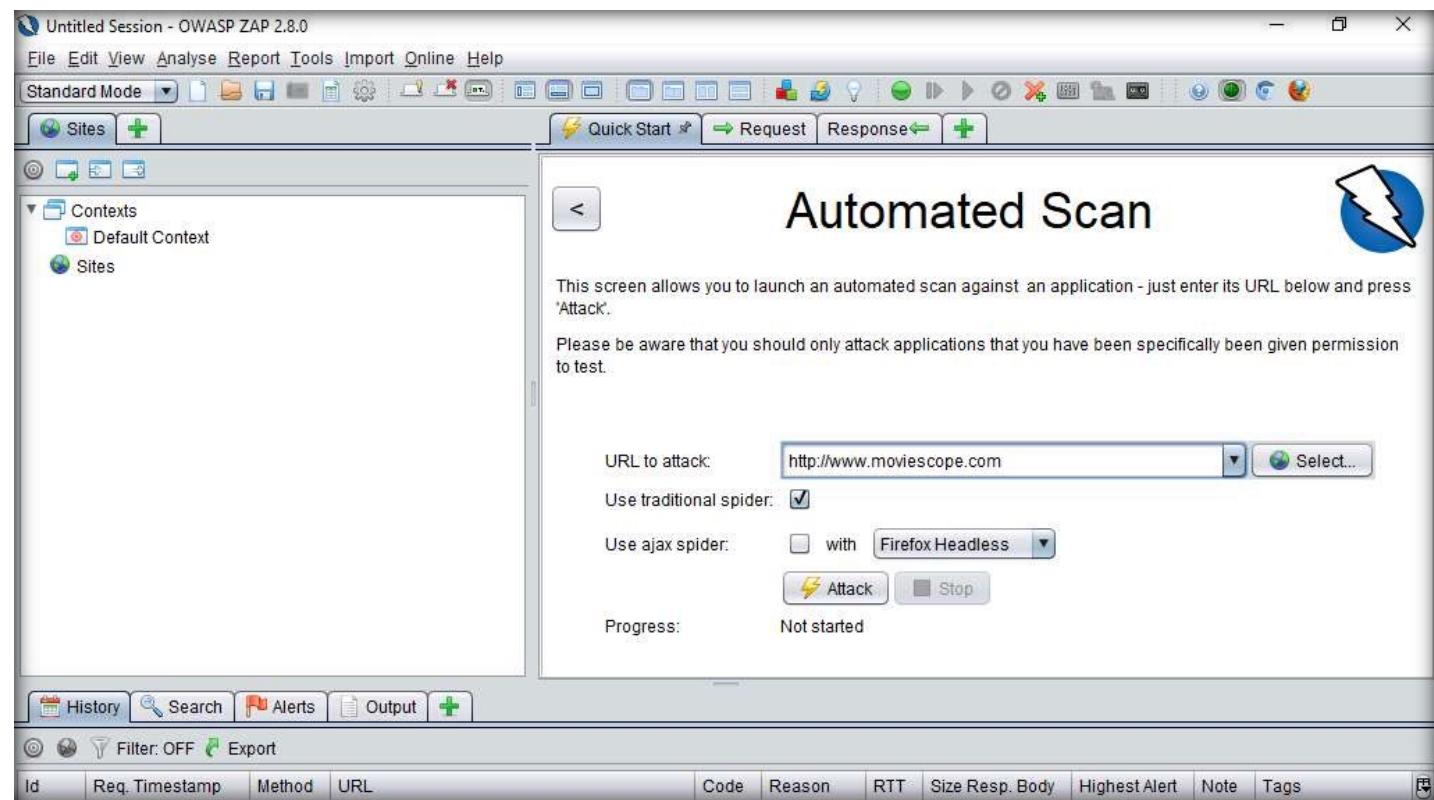
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP

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



EXERCISE 4:

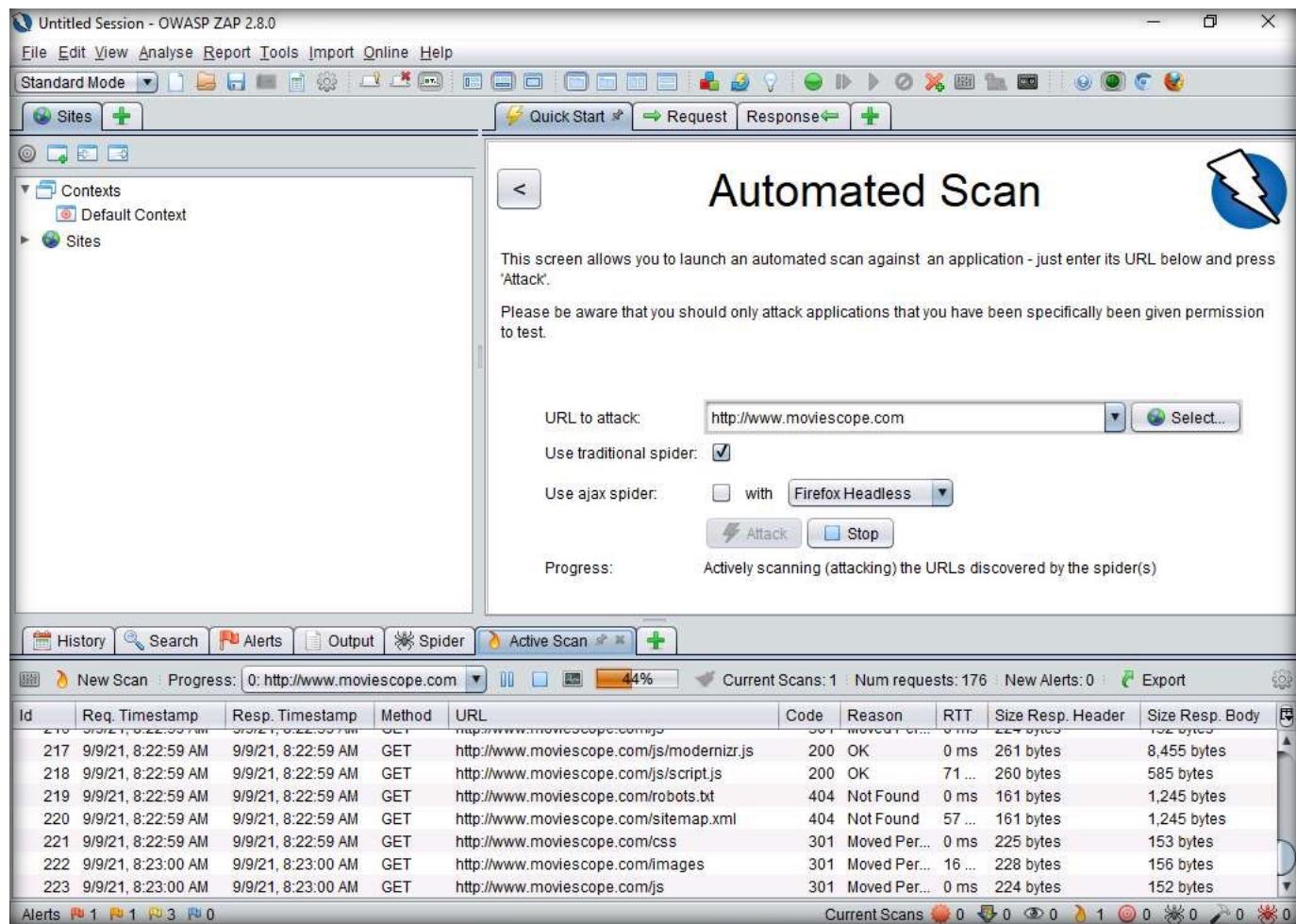
DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP



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.

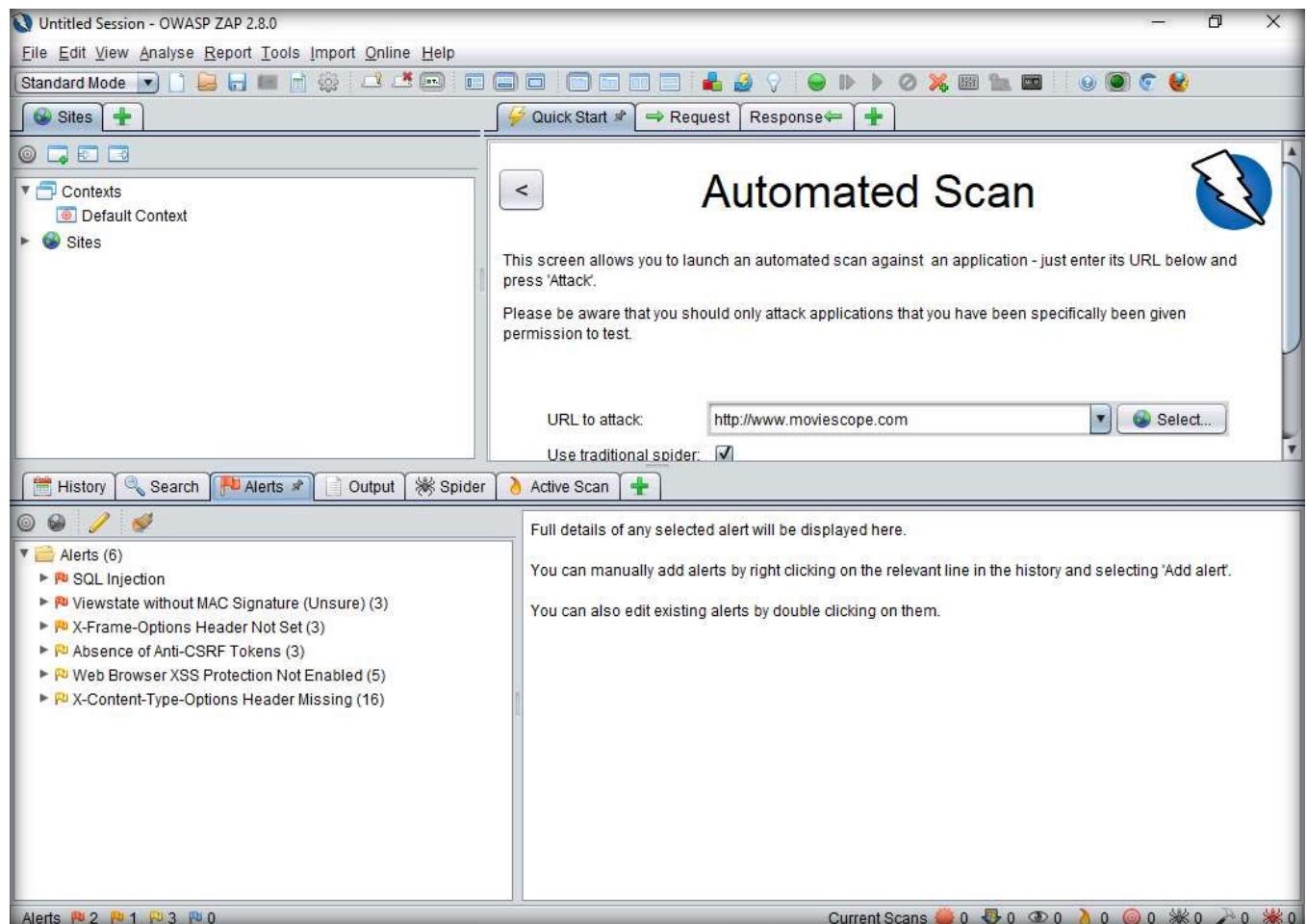


The screenshot shows the OWASP ZAP interface with the title bar "Untitled Session - OWASP ZAP 2.8.0". The main window is titled "Automated Scan" with a sub-instruction: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." It includes a note: "Please be aware that you should only attack applications that you have been specifically been given permission to test." A URL input field contains "http://www.moviescope.com". Below it are checkboxes for "Use traditional spider:" (checked) and "Use ajax spider:" (unchecked). Buttons for "Attack" and "Stop" are present. The status message says "Actively scanning (attacking) the URLs discovered by the spider(s)". At the bottom, a table lists network traffic with columns: Id, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. The table shows 223 rows of data, with the last few rows visible: 217, 218, 219, 220, 221, 222, 223. The bottom navigation bar includes tabs for History, Search, Alerts, Output, Spider, and Active Scan, along with various status indicators like "Current Scans: 1", "Num requests: 176", and "New Alerts: 0".

EXERCISE 4: DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP

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

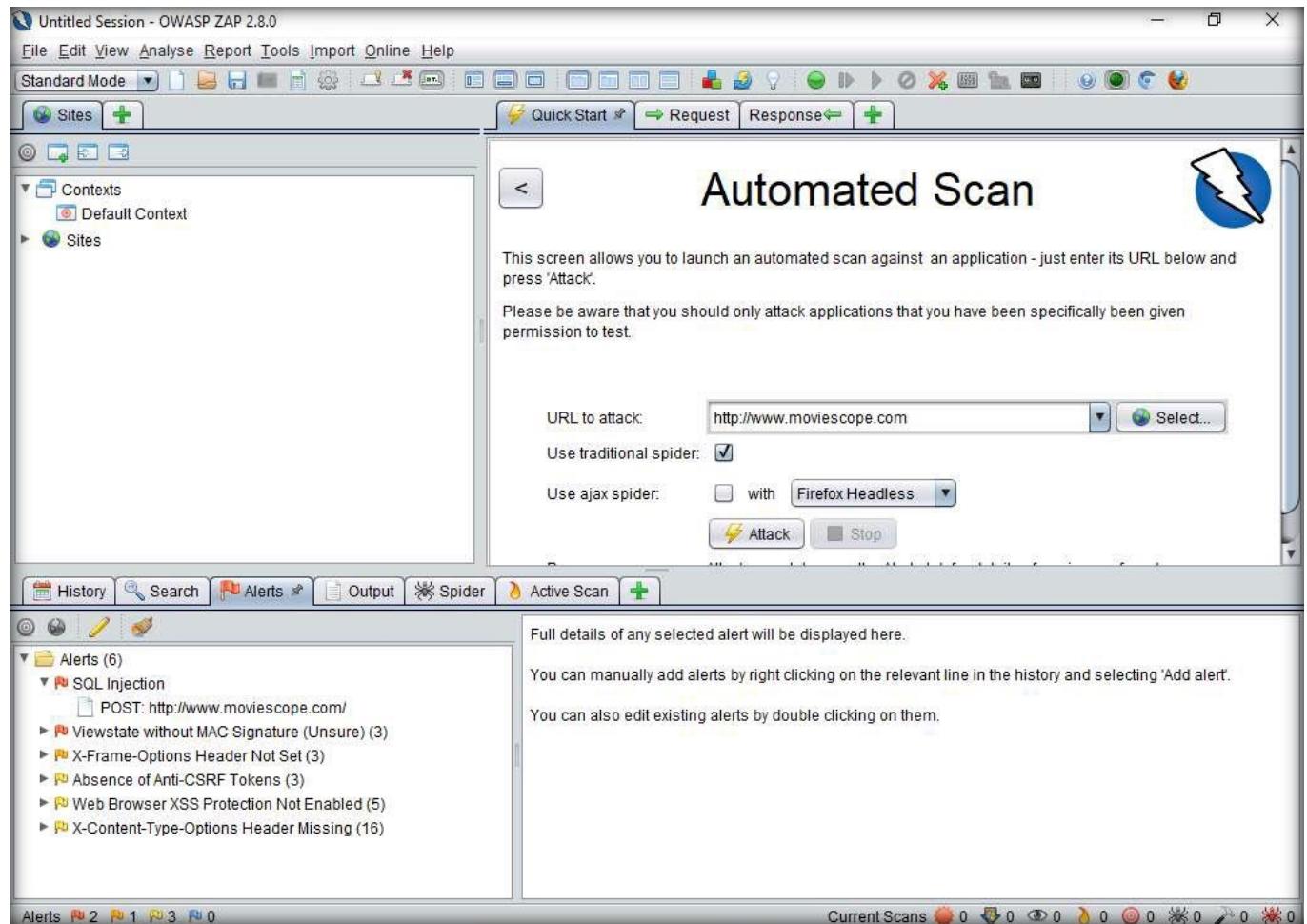
7. You can observe the vulnerabilities found on the website under the Alerts tab.



EXERCISE 4:

DETECT WEB APPLICATION VULNERABILITIES USING OWASP ZAP

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



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:

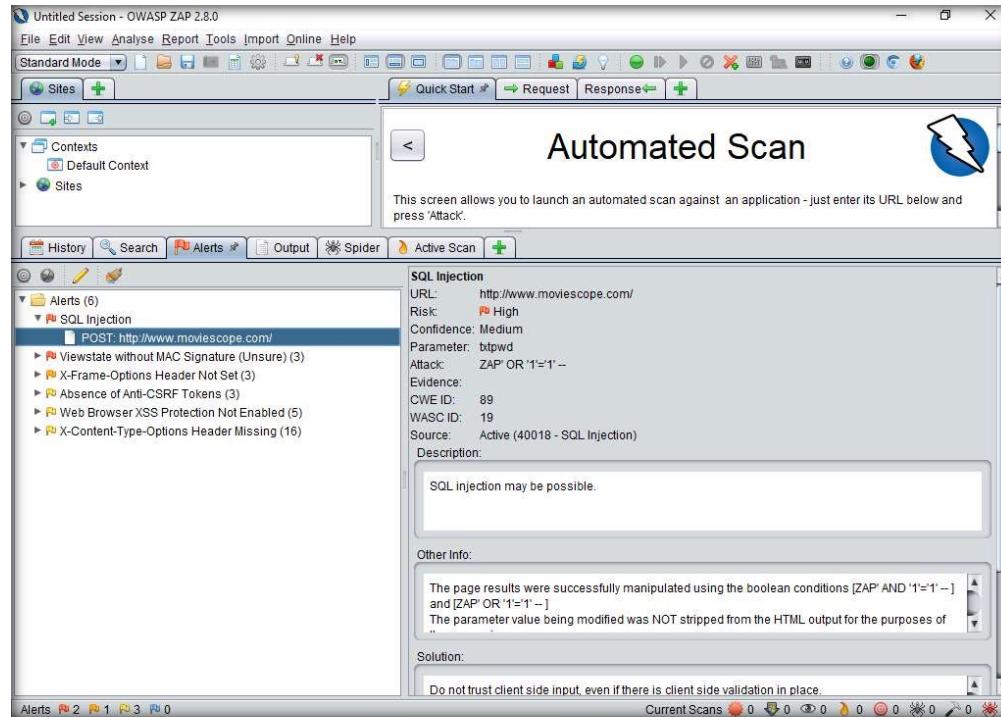
- Red Flag: High risk • Orange Flag: Medium risk • Yellow Flag: Low risk • Blue Flag: Provides details about information disclosure vulnerabilities

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.

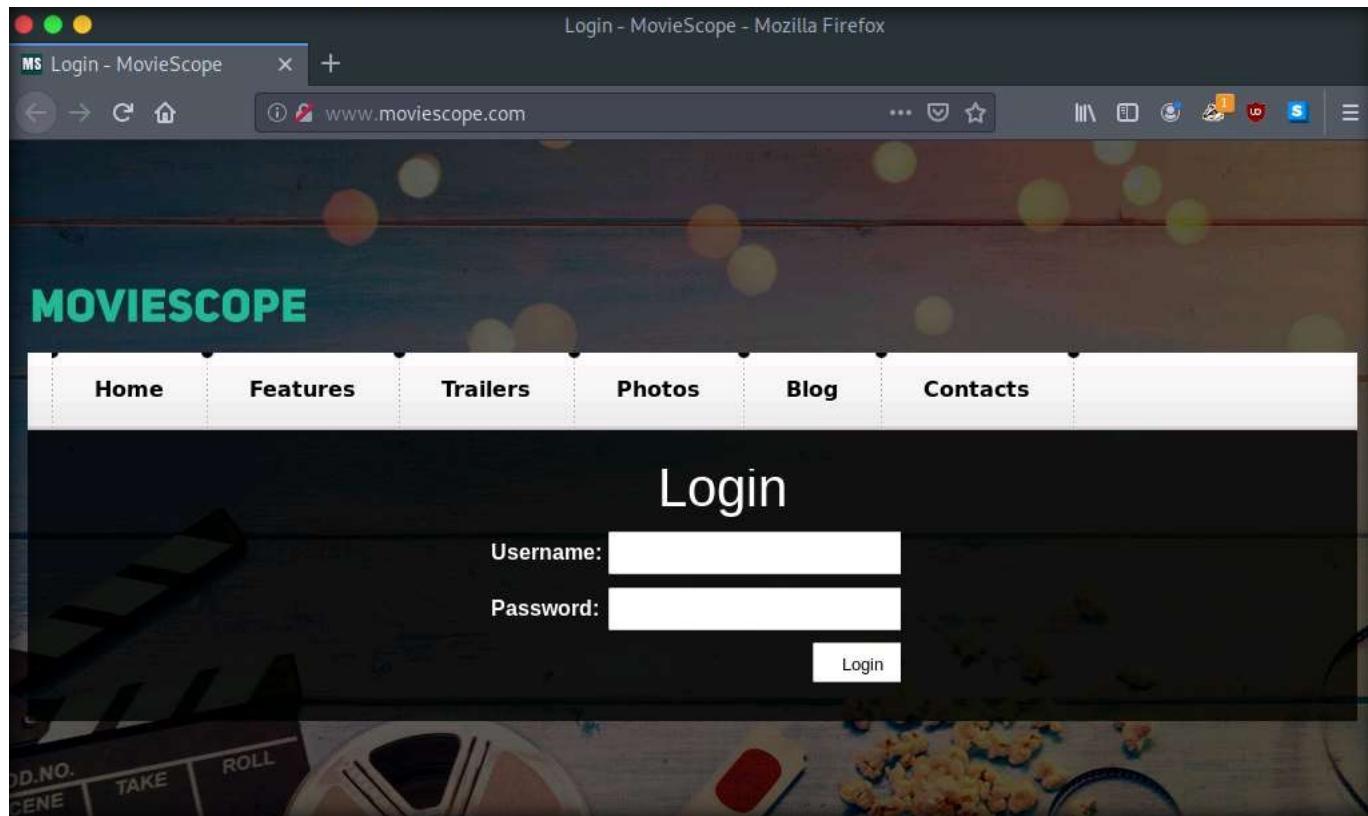
Attackers inject malicious code, commands, or scripts in the input gates of flawed web applications such that the applications interpret and run the newly supplied malicious input, which in turn allows them to extract sensitive information. By exploiting injection flaws in web applications, attackers can easily read, write, delete, and update any data (i.e., relevant or irrelevant to that particular application).

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

Note: Ensure that PfSense Firewall virtual machine is running.

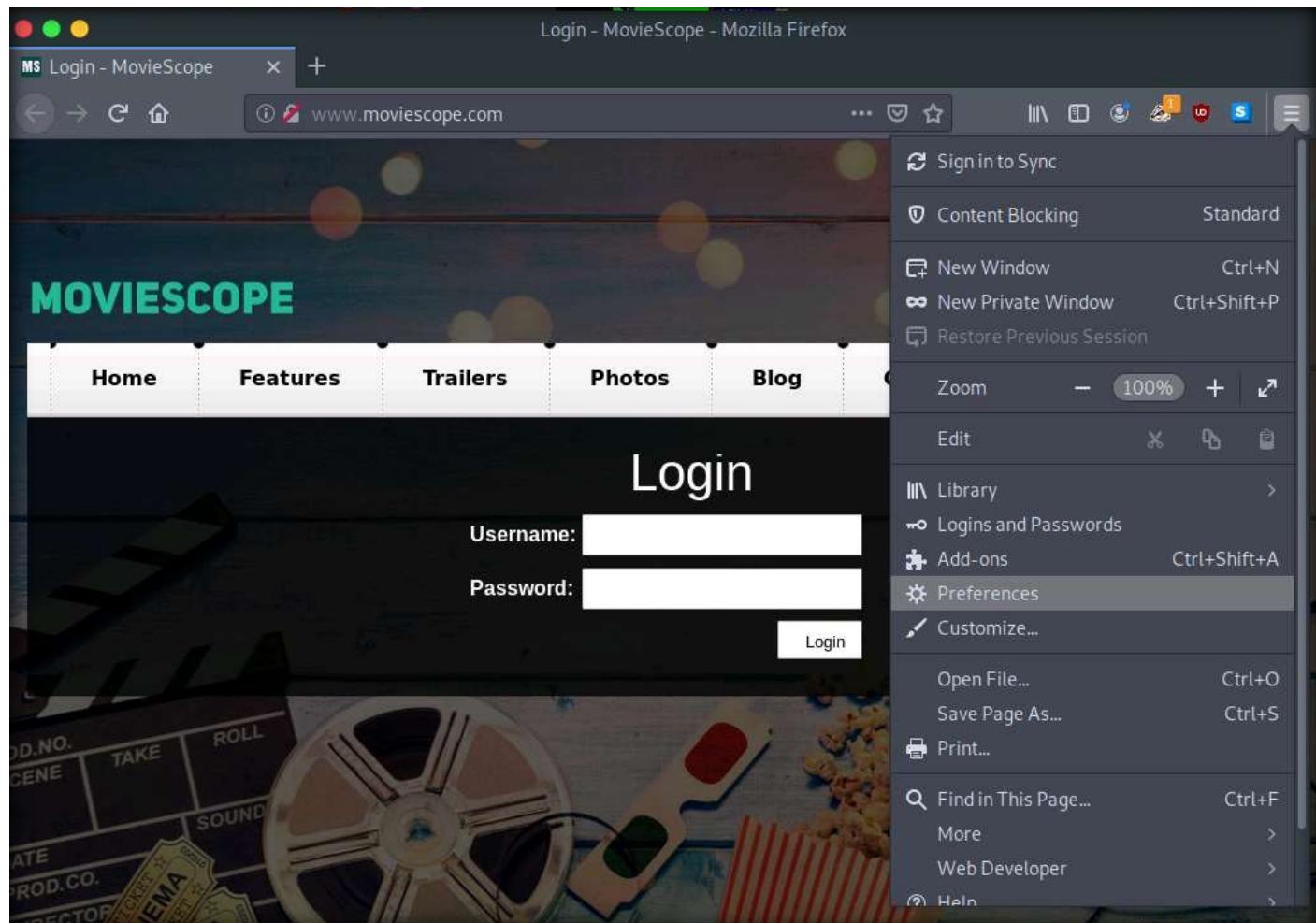
Note: In this task, the target website (www.moviescope.com) is hosted by the victim machine, Web Server. Here, the host machine is the Attacker Machine-2 machine.

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.



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.

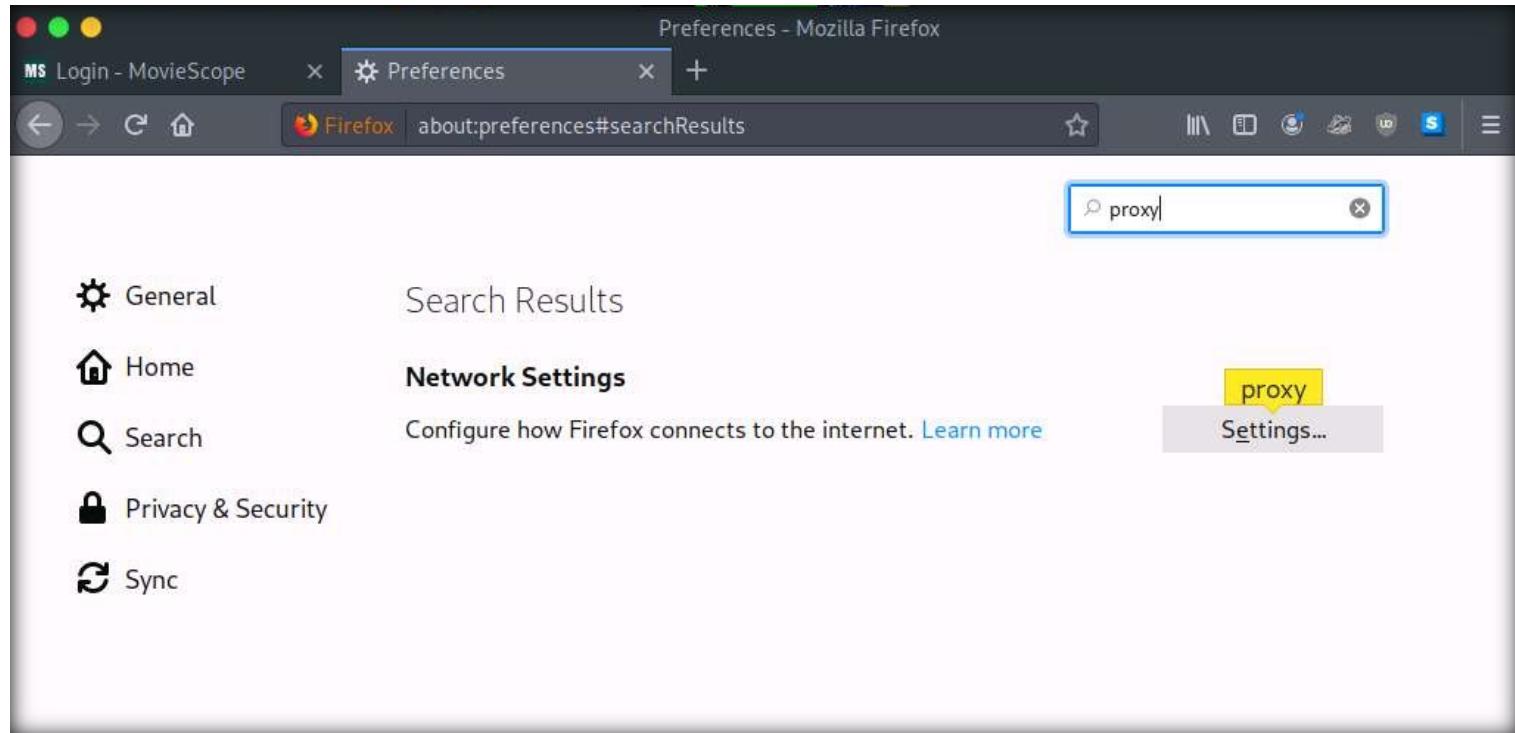


EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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

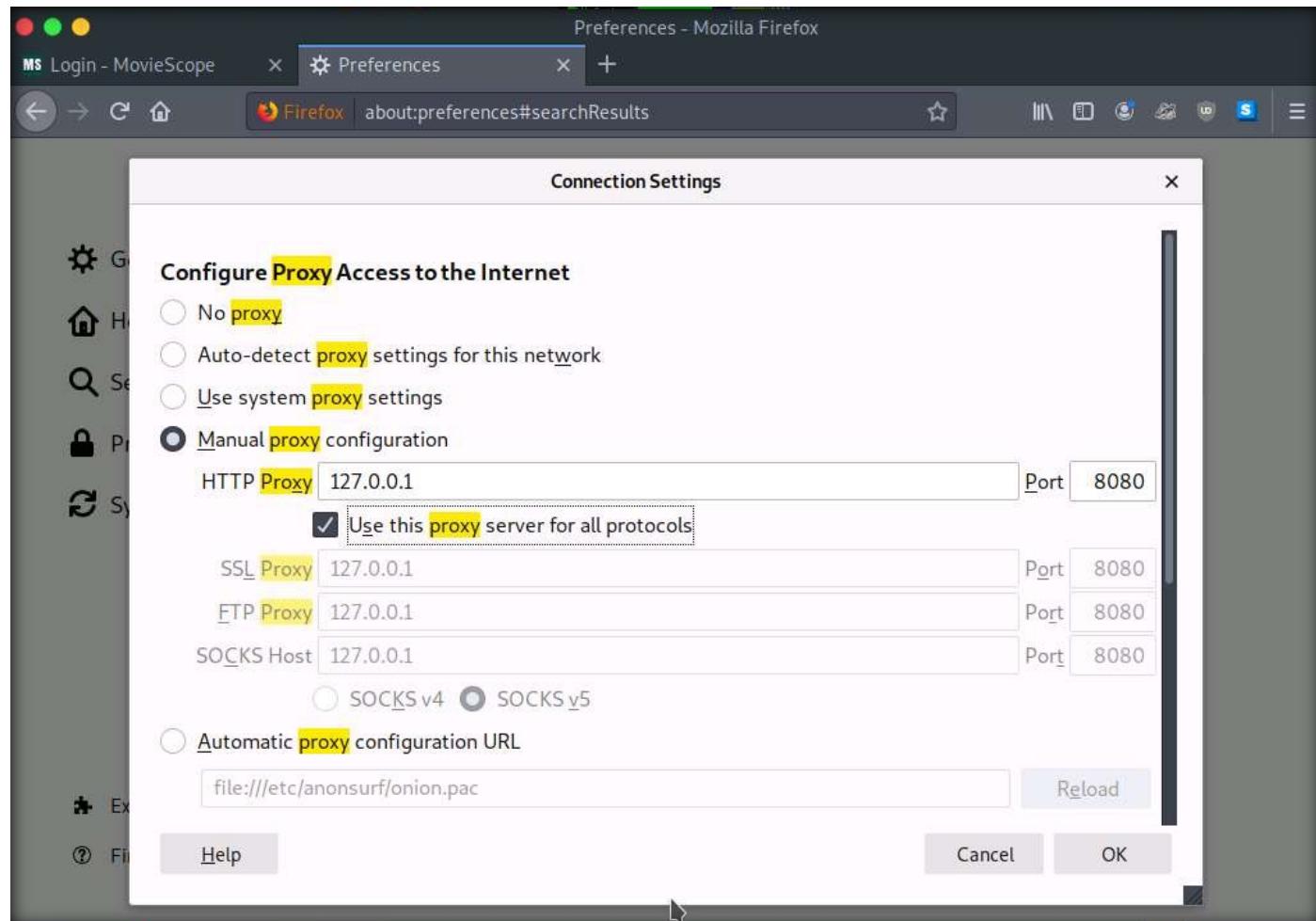
8. The Search Results appear. Click the Settings button under the Network Settings option.

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



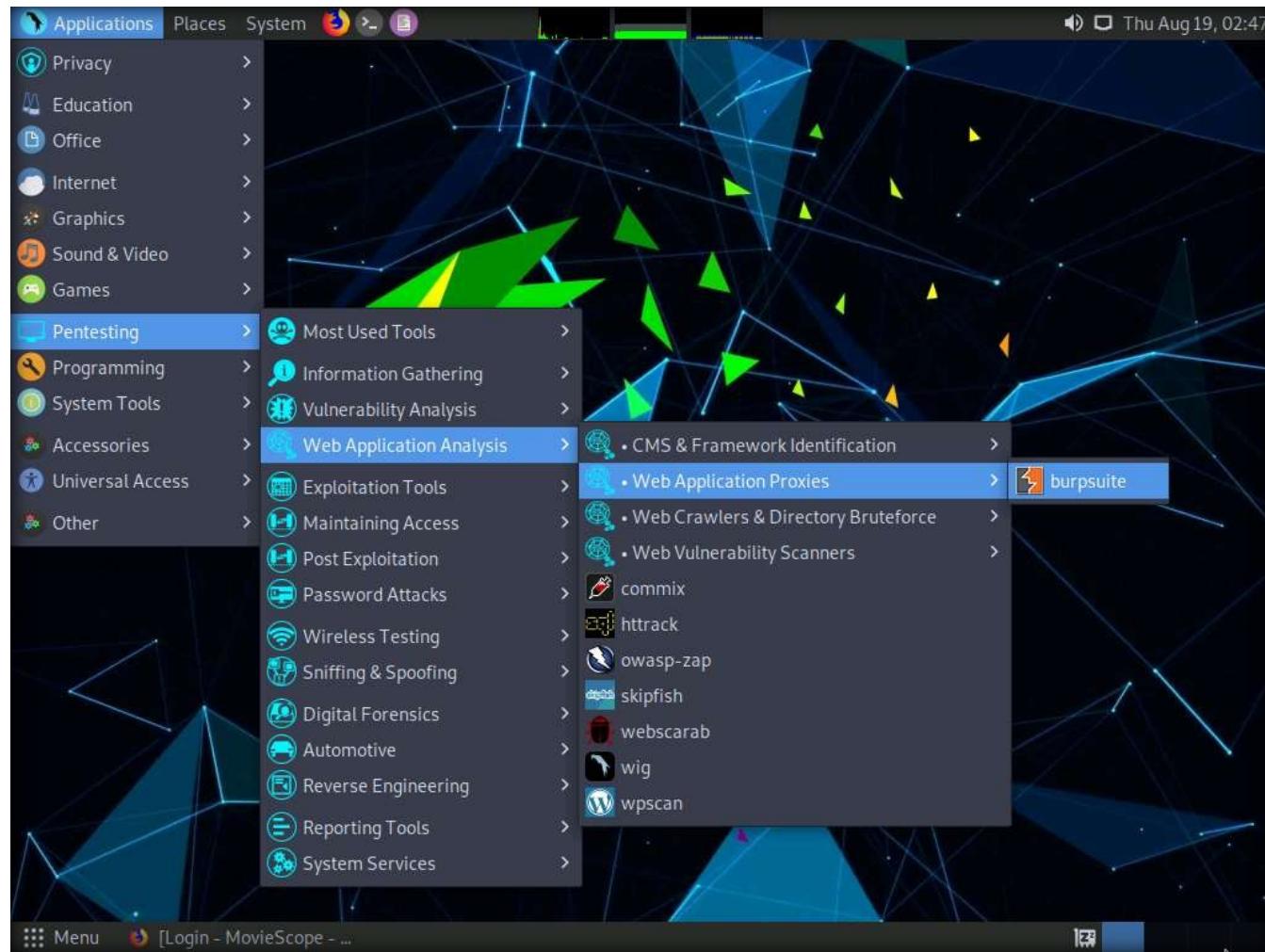
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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

10. Now, minimize the browser window, click the Applications menu from 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

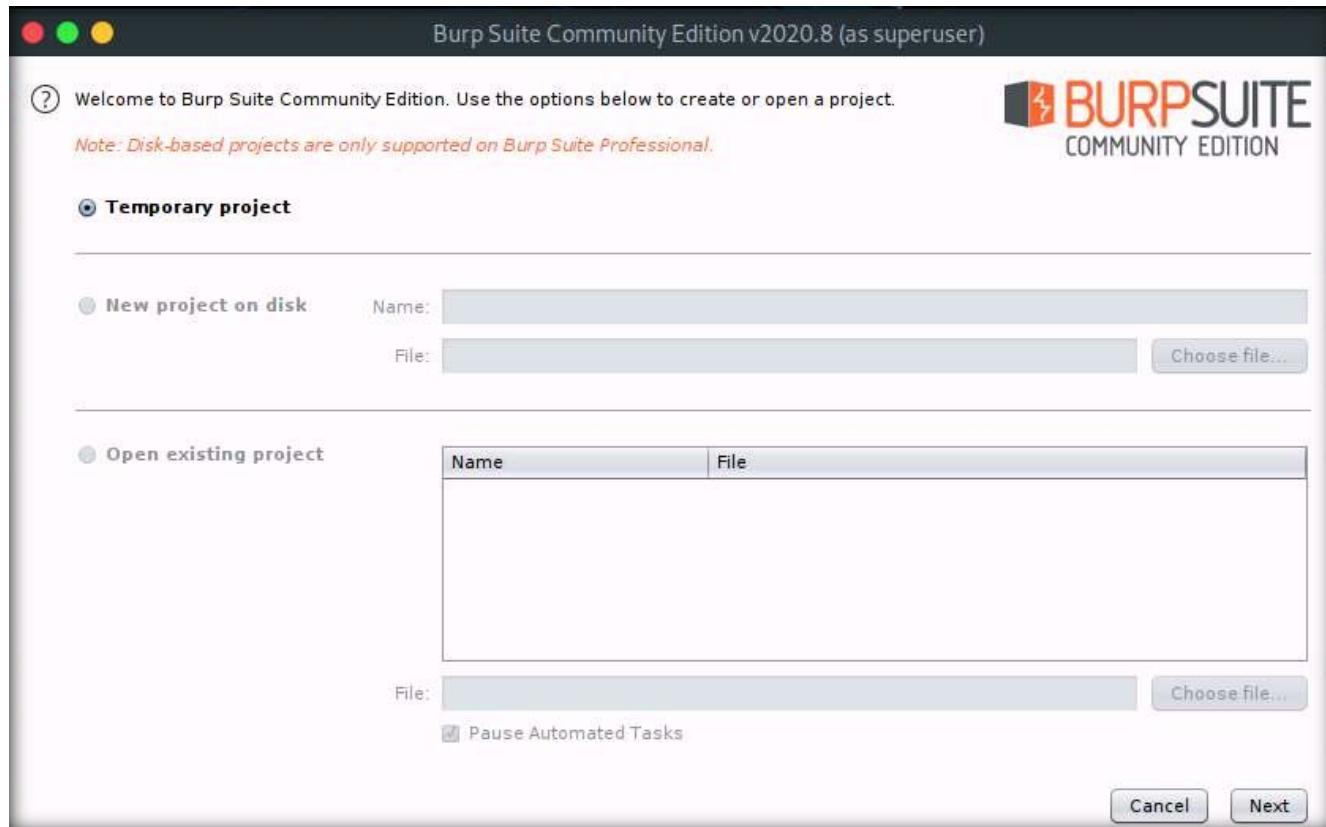


13. Burp Suite initializes. If a Burp Suite Community Edition notification saying An update is available appears, click Close.

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

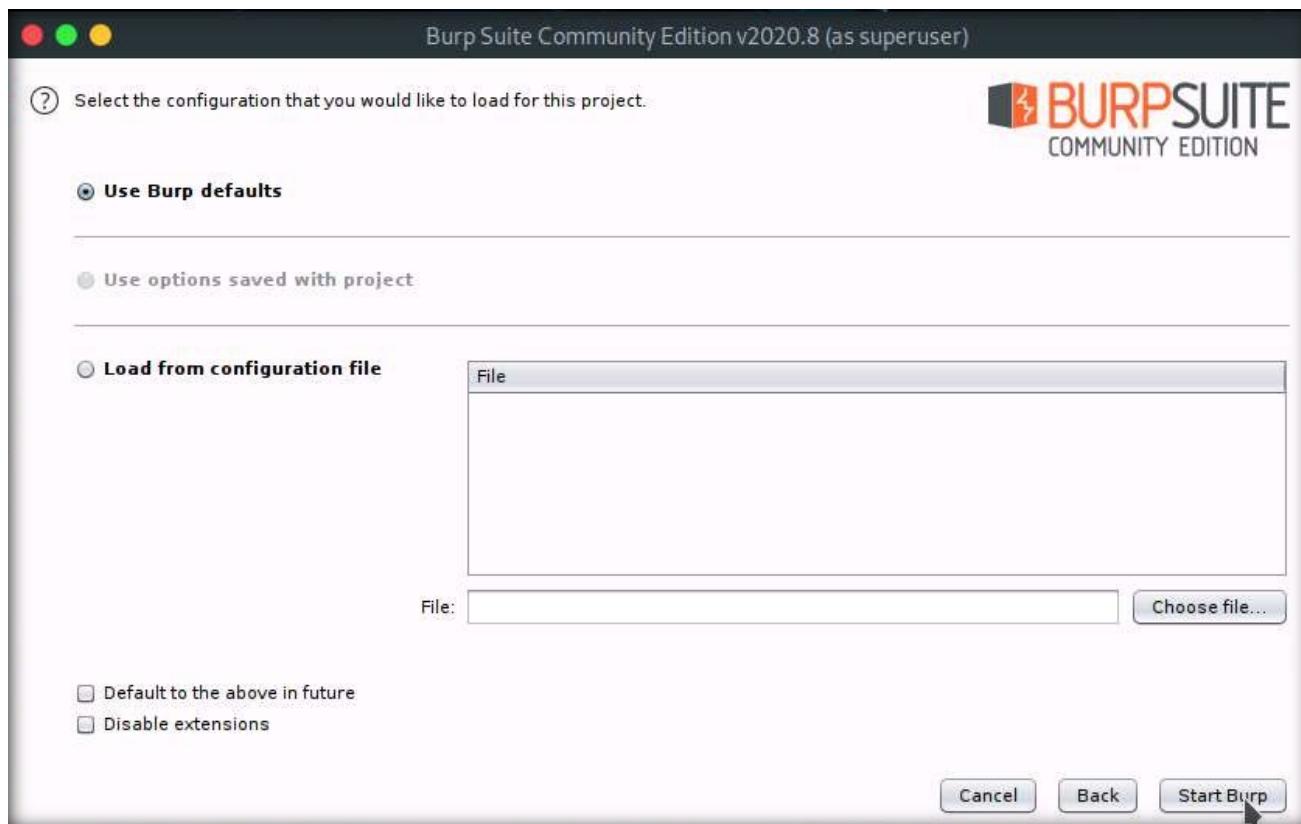
14. The Burp Suite main window appears; ensure that the Temporary project radio button is selected and click the Next button, as shown in the screenshot below.

Note: If an update window appears, click Close.



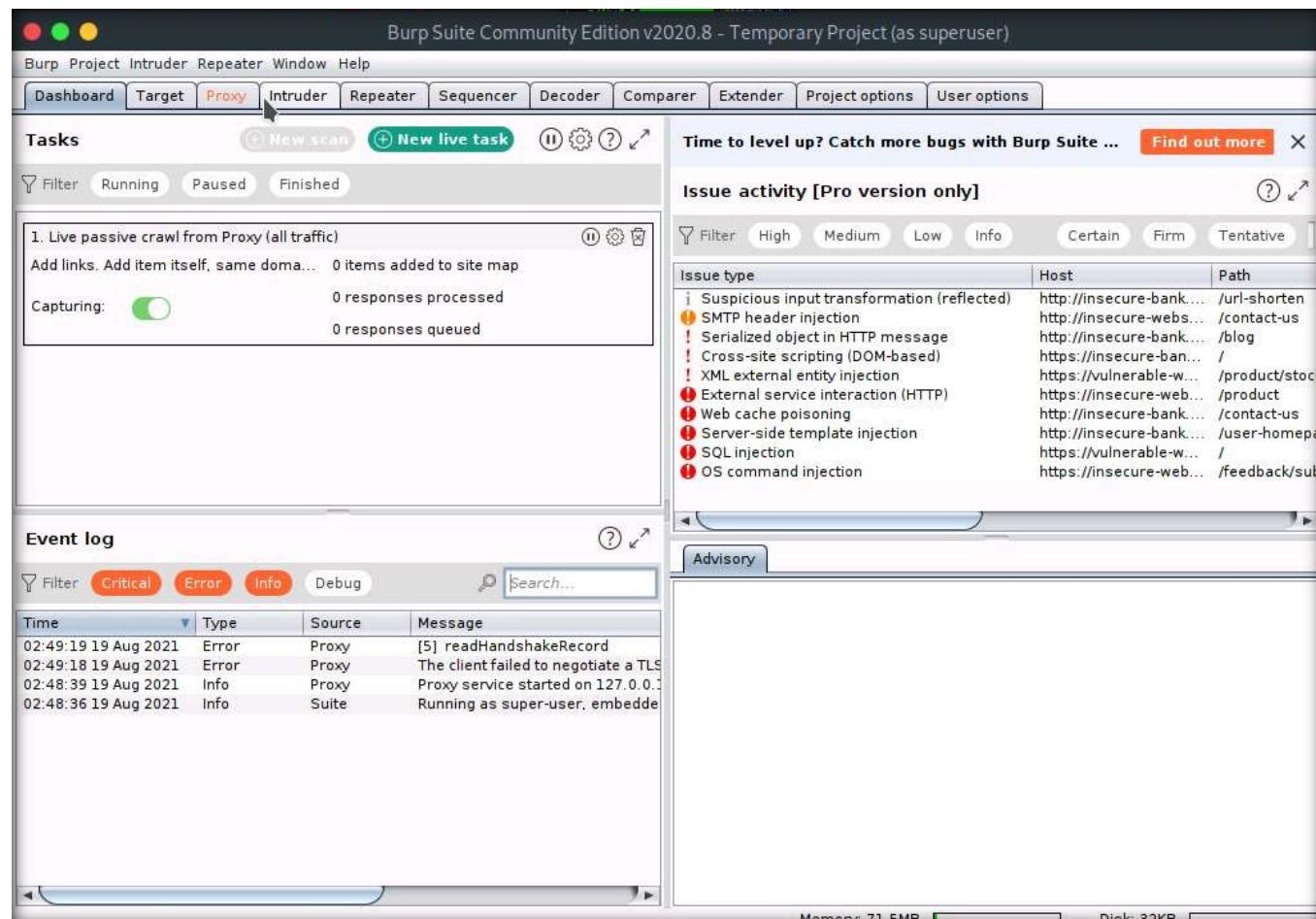
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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



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

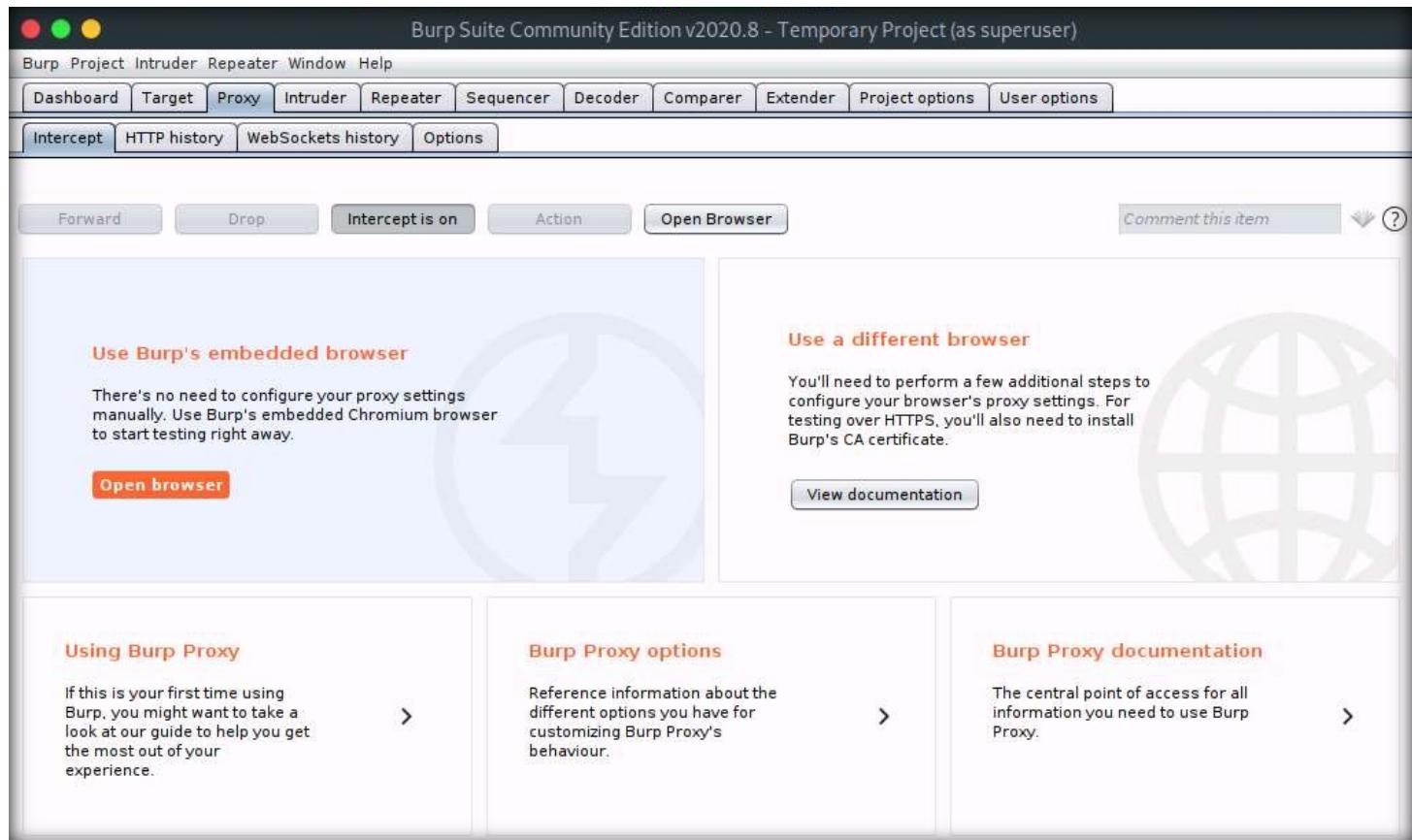
Note: In the right-pane of the tool window, you can observe the vulnerabilities in the target website that have been detected by the tool under Issue activity. You can click on each vulnerability to explore them one-by-one.



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.

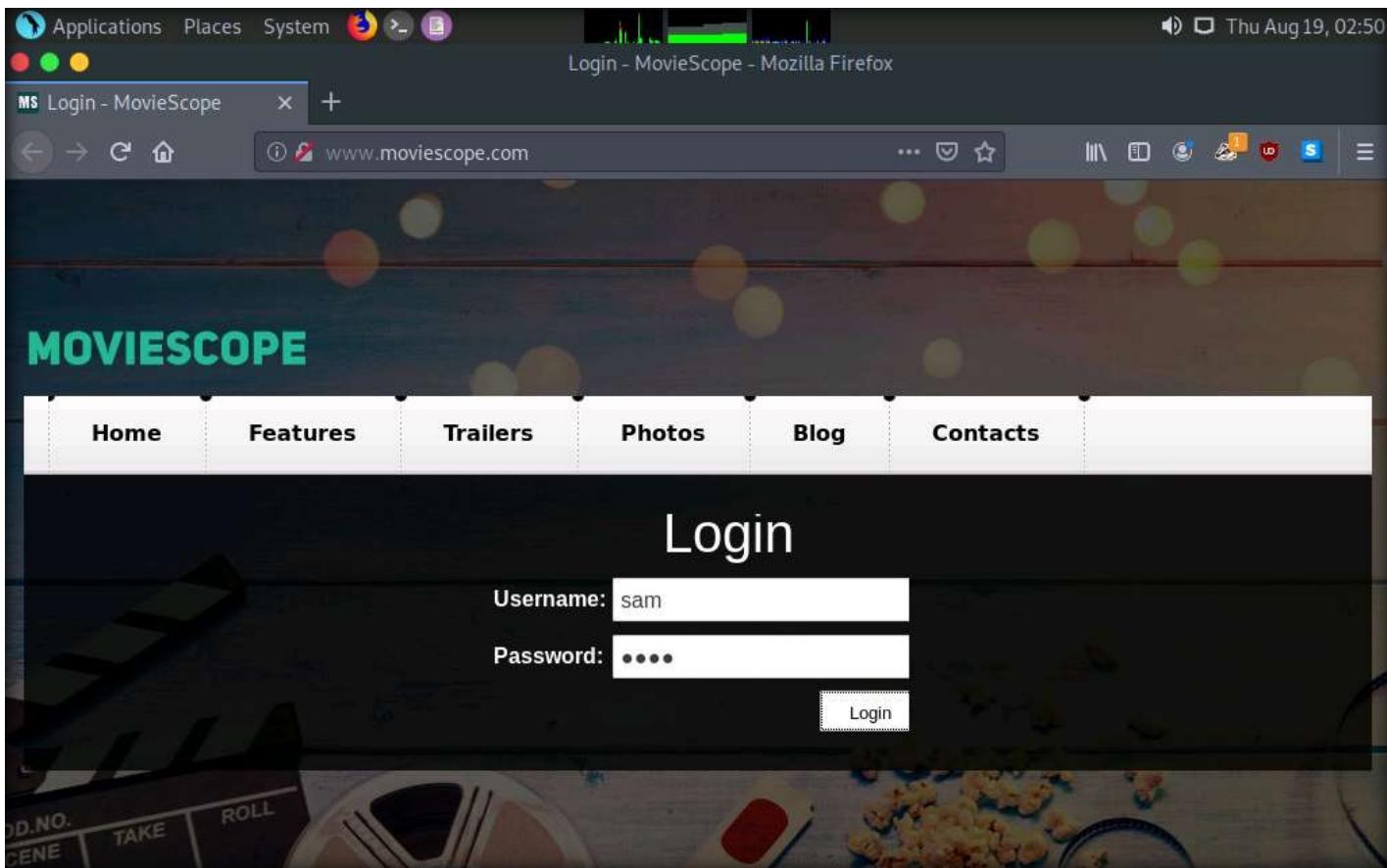
Note: Turn the interception on if it is off.

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.

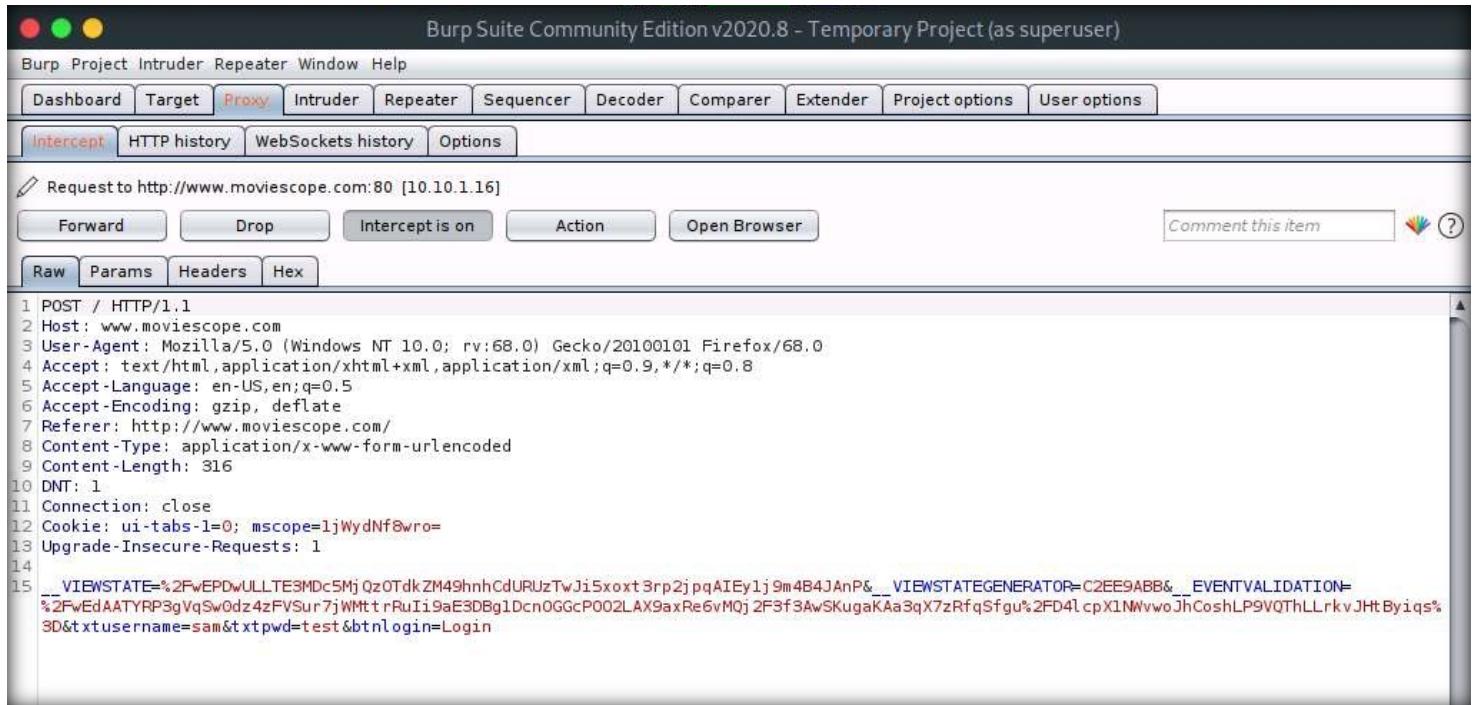


EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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.

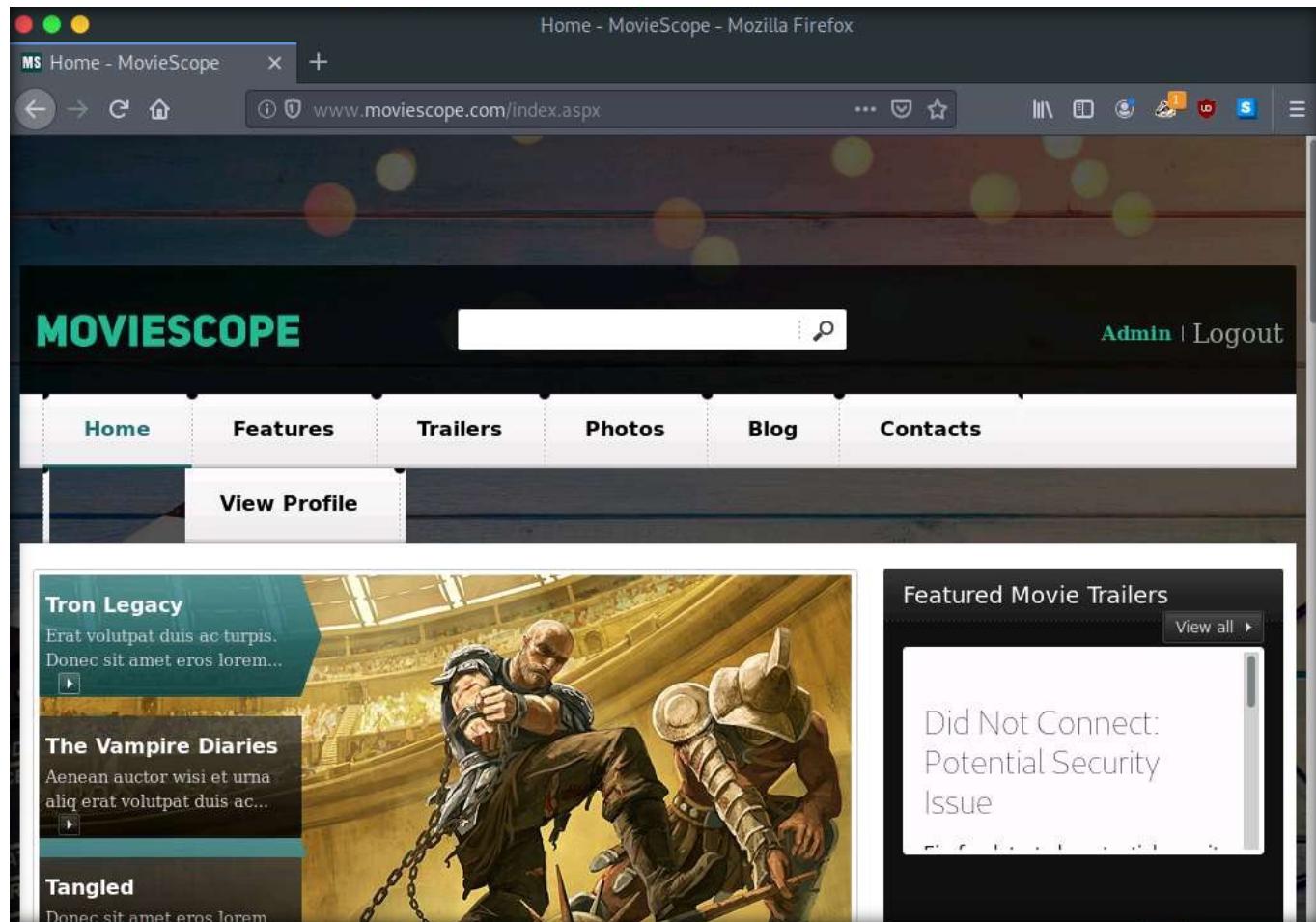
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



```
1 POST / HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 316
10 DNT: 1
11 Connection: close
12 Cookie: ui-tabs-1=0; mscore=1jWydNf8wro=
13 Upgrade-Insecure-Requests: 1
14
15 --VIEWSTATE=%2FwEPDwULLTE3MDc5MjQzOTdkZM49hnhCdURUzTwJi5xoft3rp2jpqAIEy1j9m4B4JAnP&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=%2FwEdAAcYRP3gVqSw0dz4zFVSur7jWhtrRuIi9aE3DBg1DcnOGGcP002LAX9axRe6vM0j2F3f3AwSKugaKaa3qX7zRfqSfgu%2FD4lcpX1NWvwoJhCoshLP9VQThLLrkvJHtByiqs%3D&txusername=sam&txtpwd=test&bttnlogin=Login
```

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

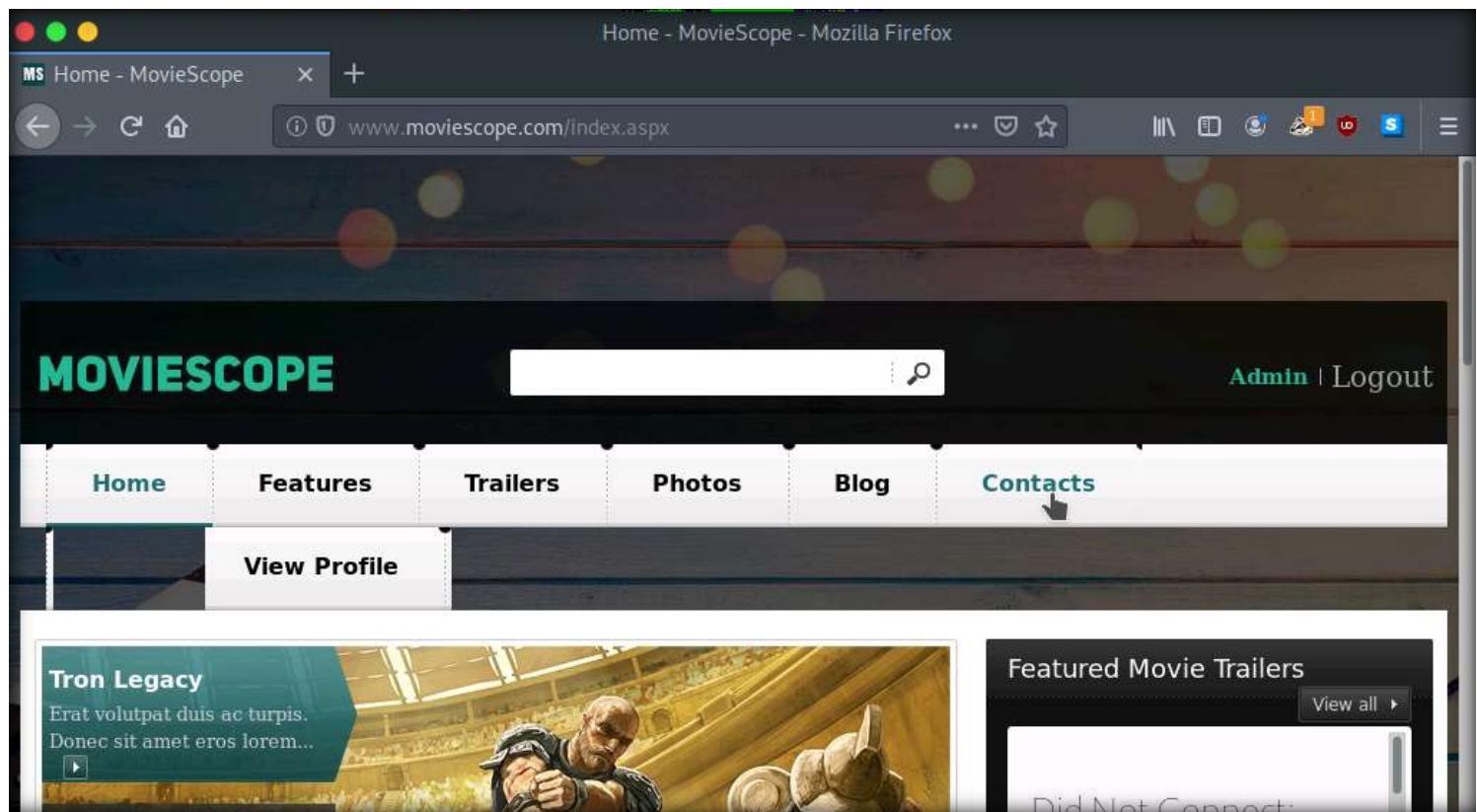
21. Switch to the browser and observe that you are now logged into the user account, as shown in the screenshot below.



EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

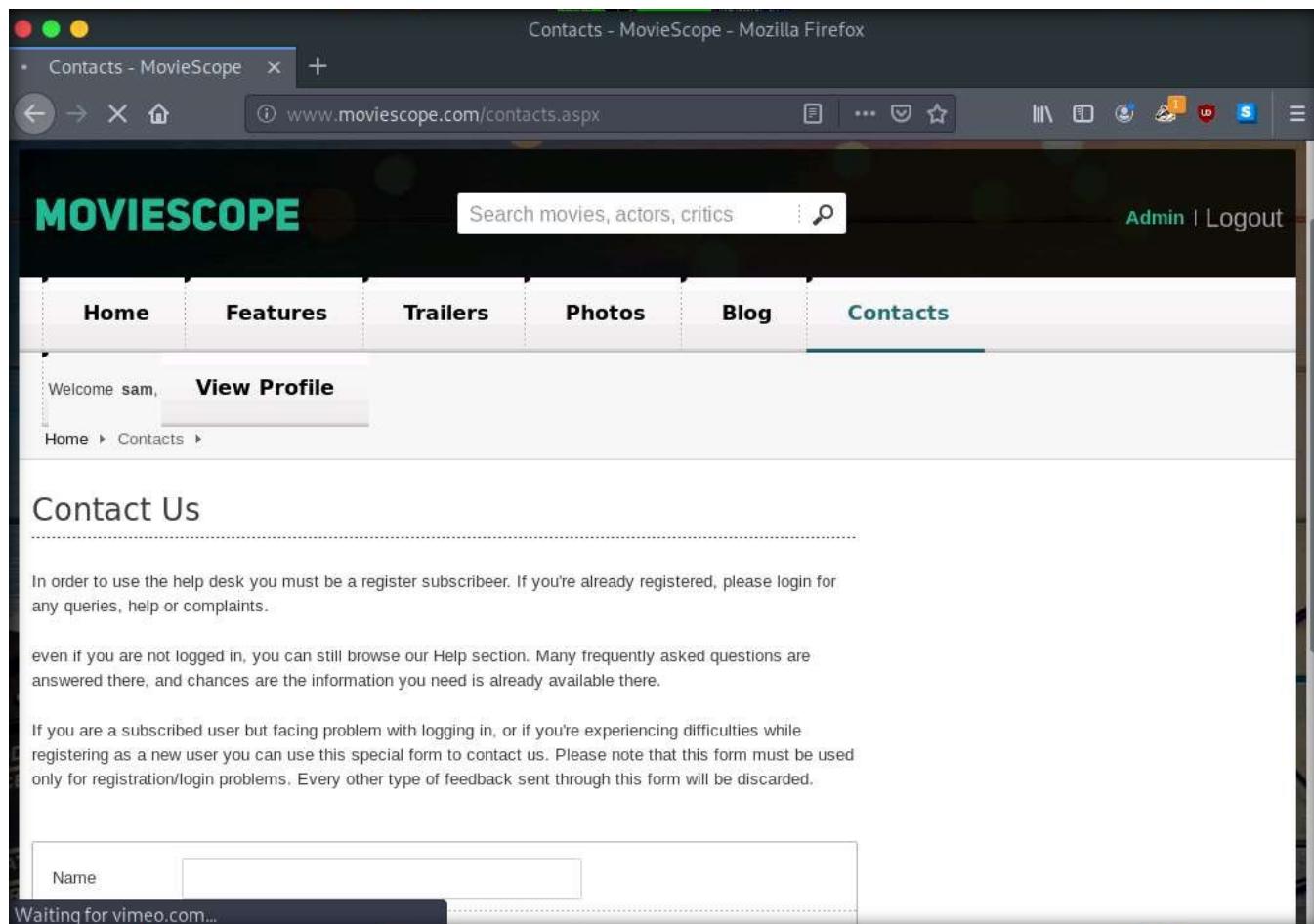
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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

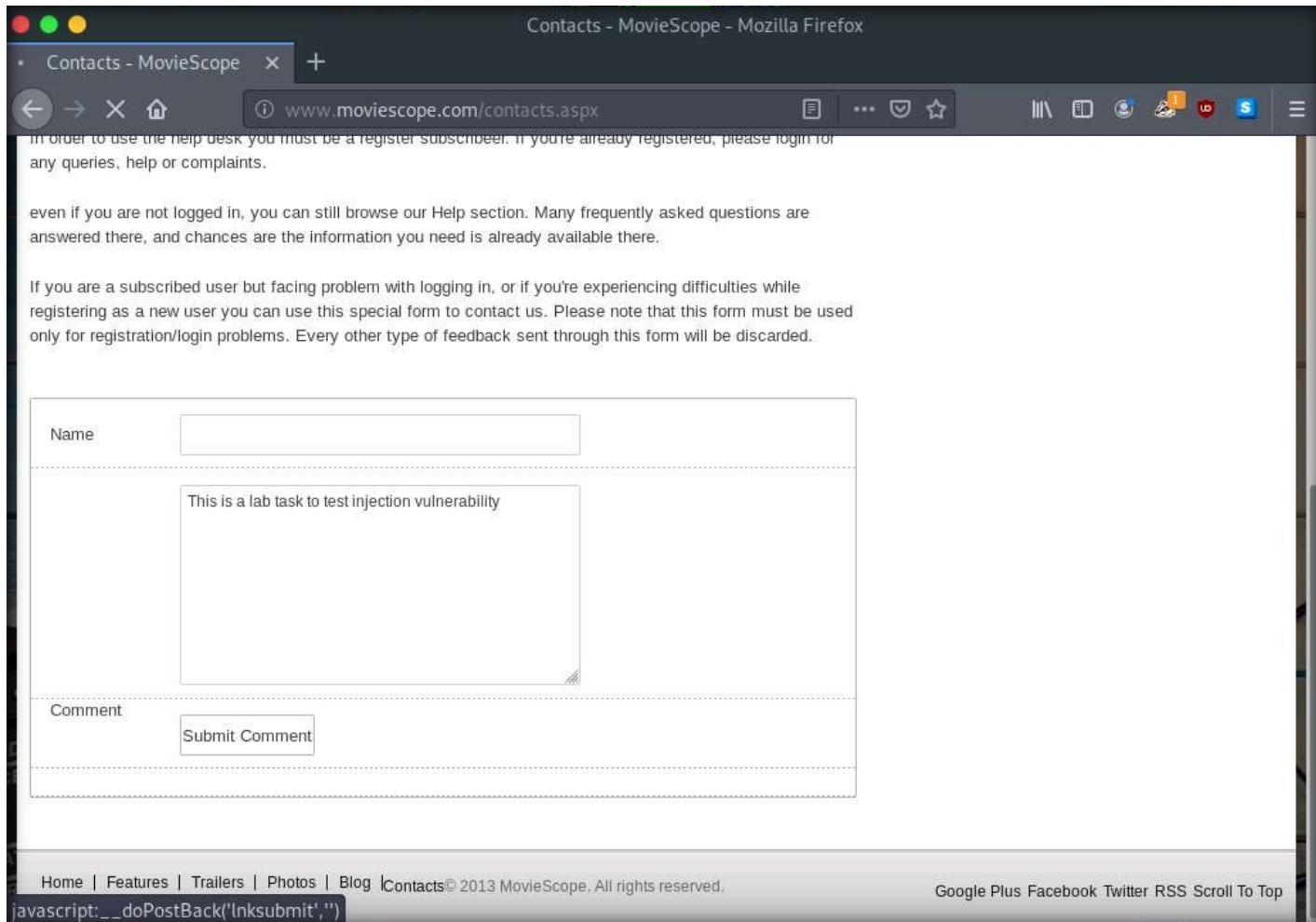


23. After clicking the Contacts tab, switch back to the Burp Suite window and keep clicking the Forward button until you get the HTTP request.

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



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.



Contacts - MovieScope - Mozilla Firefox

www.moviescope.com/contacts.aspx

In order to use the help desk you must be a register subscriber. If you're already registered, please login for any queries, help or complaints.

even if you are not logged in, you can still browse our Help section. Many frequently asked questions are answered there, and chances are the information you need is already available there.

If you are a subscribed user but facing problem with logging in, or if you're experiencing difficulties while registering as a new user you can use this special form to contact us. Please note that this form must be used only for registration/login problems. Every other type of feedback sent through this form will be discarded.

Name

This is a lab task to test injection vulnerability

Comment

Submit Comment

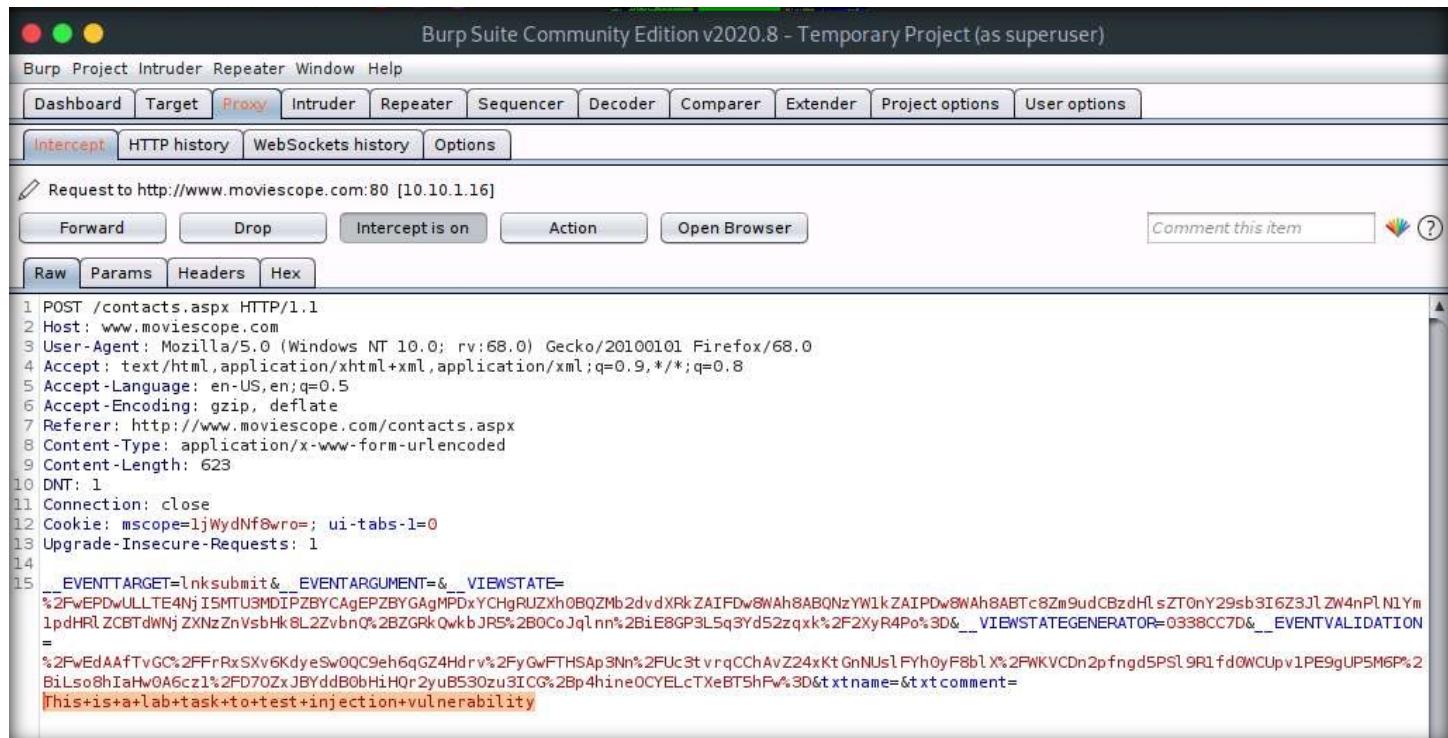
Home | Features | Trailers | Photos | Blog | Contacts © 2013 MovieScope. All rights reserved.
javascript:_doPostBack('lnksubmit','')

Google Plus Facebook Twitter RSS Scroll To Top

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.

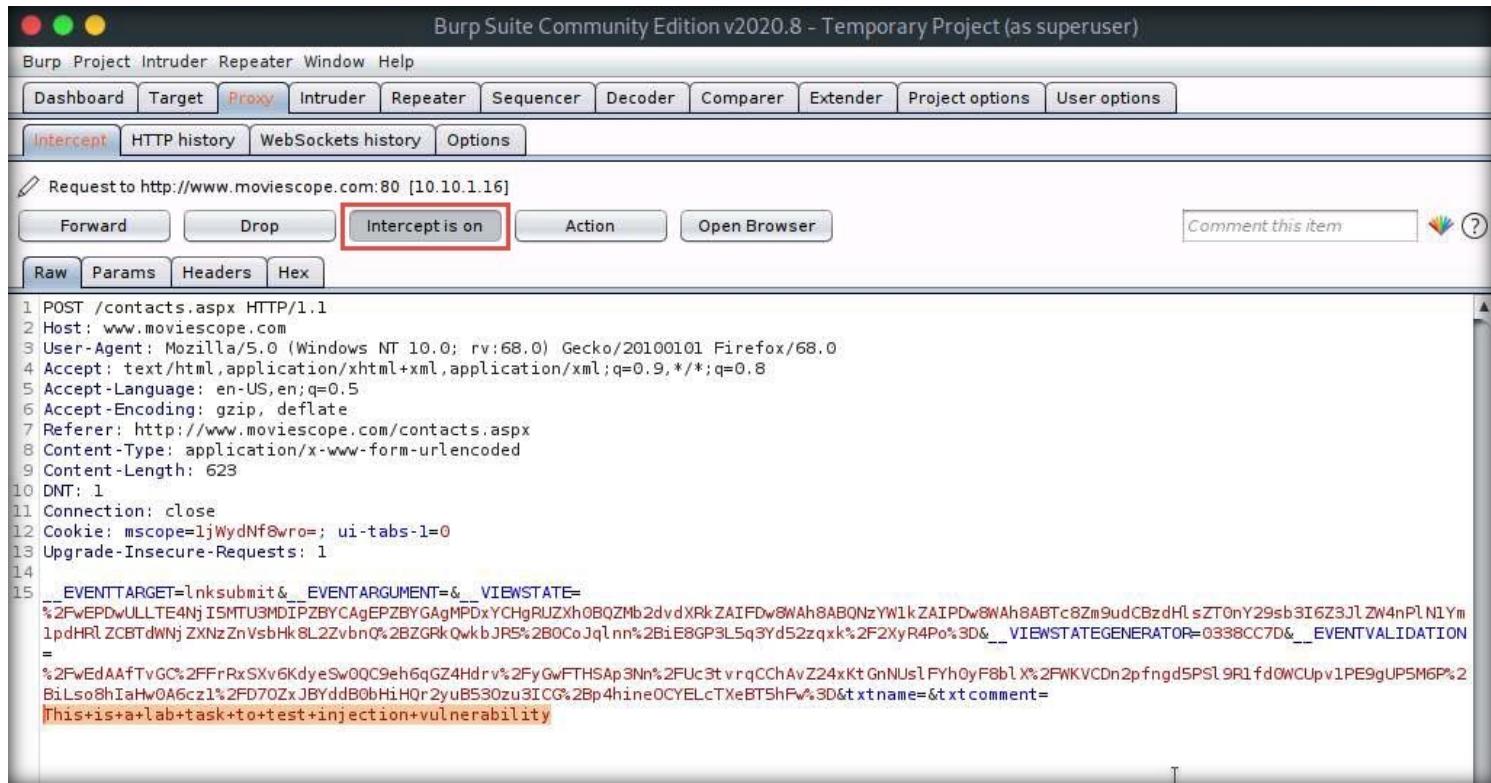
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE



```
Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.moviescope.com:80 [10.10.1.16]
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Params Headers Hex
1 POST /contacts.aspx HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/contacts.aspx
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 623
10 DNT: 1
11 Connection: close
12 Cookie: mscope=ljWydNf8wro=; ui-tabs-l=0
13 Upgrade-Insecure-Requests: 1
14
15 __EVENTTARGET=lnksubmit&__EVENTARGUMENT=&__VIEWSTATE=
%2FwEPDwULLTE4njI5MTU3MDIPZBYCAgEPZBYGAgMPDxYChgRUZXh0BQZMb2vdXPKZAIFDw8NAh8AB0NzYW1kZAIPDw8NAh8ABTc8Zm9udCBzdHlsZT0nY29sb3I6Z3JlZW4nPnIYm
1pdHRLZCBTdWNjZXNzZhVsBhk8L2Zvbnn%2BZGrkQwkjRS%2B0CoJqlnn%2BiE8GP3L5q3Yd52zqxk%2F2XyR4Po%3D&__VIEWSTATEGENERATOR=0338CC7D&__EVENTVALIDATION=
=
%2FwEdAAfTvGC%2FFrRxSxv6KdyeSw0QC9eh6qGZ4Hdrv%2FyGwFTHSAp3Nn%2FUc3tvrqCChAvZ24xKtGnNuJlFYh0yF8blX%2PWVKCDn2pfngd5PSl9R1fd0WCUpv1PE9gUP5M6P%2
BiLso8hIaHw0A6czl%2FD70ZxJBYddB0bHiHOr2yuB530zu3ICG%2Bp4hineOCYELcTxeBT5hFw%3D&xtname=&xtcomment=
This is+a+lab+task+to+test+injection+vulnerability
```

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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



Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://www.moviescope.com:80 [10.10.1.16]

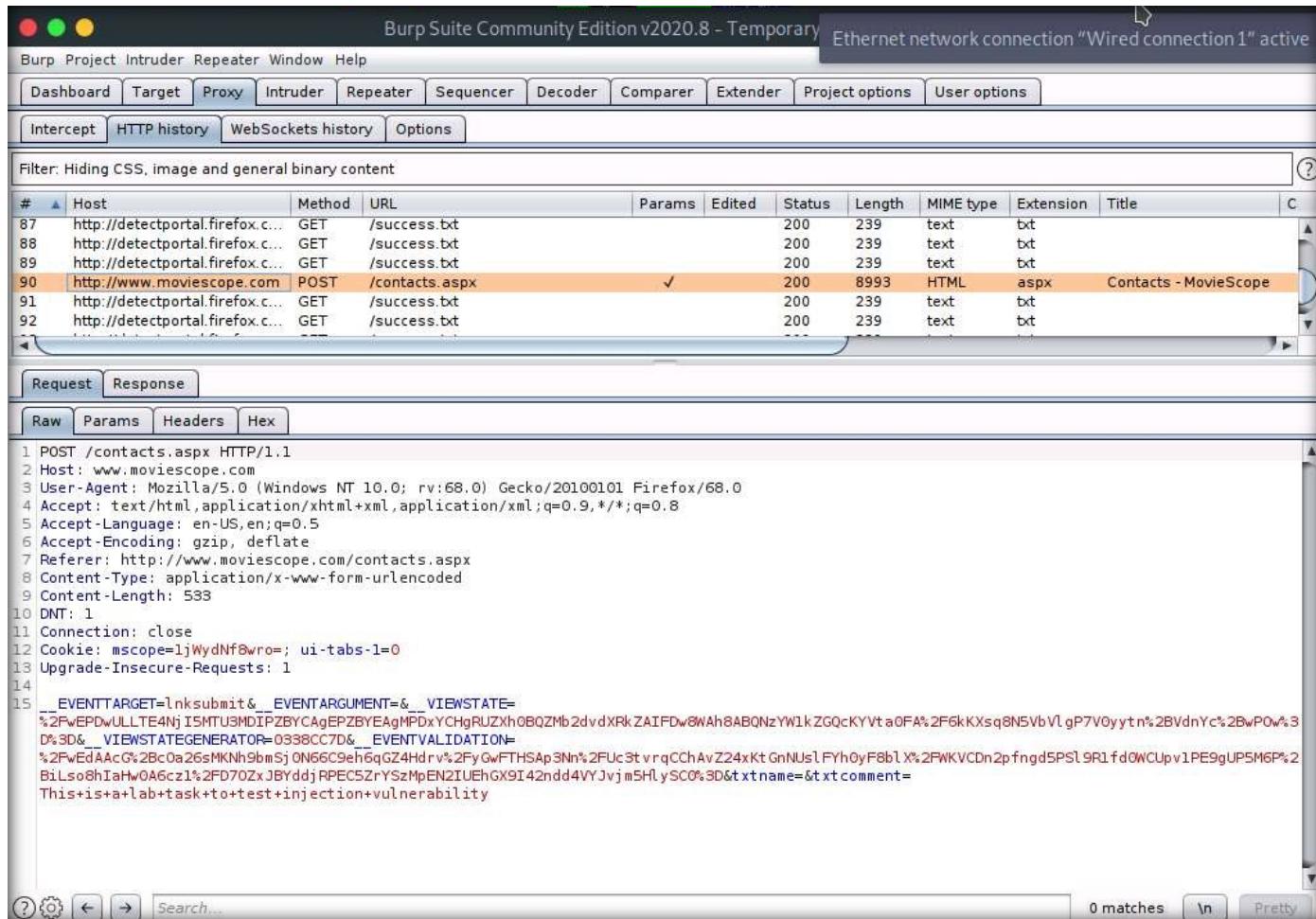
Forward Drop Intercept is on Action Open Browser

Comment this item ?

Raw Params Headers Hex

```
1 POST /contacts.aspx HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/contacts.aspx
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 623
10 DNT: 1
11 Connection: close
12 Cookie: mscoope=ljWydNf0wro=; ui-tabs-l=0
13 Upgrade-Insecure-Requests: 1
14
15 __EVENTTARGET=lnksubmit&__EVENTARGUMENT=&__VIEWSTATE=
%2FwEPDwULLTE4NjI5MTU3MDIPZBYCAgEPZBYGAgMPDxYCHgRUZxh0BQZMb2vdXRkZAIFdw8WAh8ABQnZyW1kZAIPDw8WAh8ABTc8Zm9udCBzdHlsZT0nY29sb3I6Z3JlZW4nPlN1Ym
1pdHRIZCBTdWnjZXNzZnVsBh8L2Zvbn0%2BZGRkQwkbJR5%2B0CoJqlnn%2BiE8GP3L5q3Yd52zqxk%2F2XyR4P0%3D&__VIEWSTATEGENERATOR=0388CC7D&__EVENTVALIDATION=
=
%2FwEdAAfTvGC%2FFrRxSXv6KdyeSw0QC9eh6qGZ4Hdrv%2FyGwFTHSAp3Nn%2Fu3tvrqCChAvZ24xKtGnNuSlFyh0yF8blX%2FWKVCdn2pfngd5PSl9R1fd0WCUpv1PE9gUPSM6P%2
B1Lso8hIahw0A6c1%2Fd702xJByddB0bHiH0r2yuB53Ozu3LCG%2Bp4hine0CYELcTxetBTSFw%3D&txtname=&txtcomment=
This+is+a+lab+task+to+test+injection+vulnerability
```

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.



The screenshot shows the Burp Suite interface with the following details:

- HTTP history tab:** Selected tab.
- Selected Request:** POST /contacts.aspx (Line 90).
- Request Headers:**

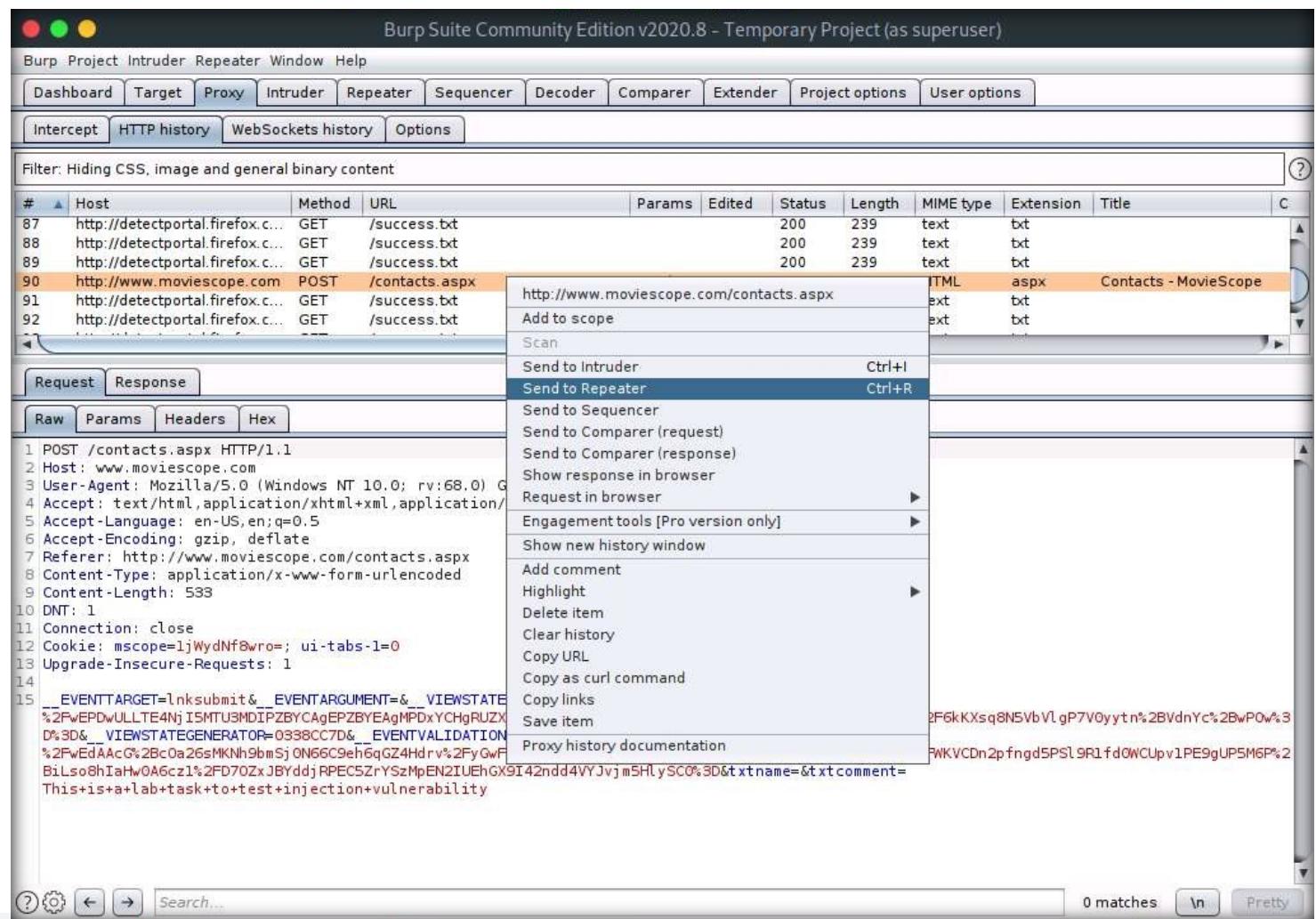
```
1 POST /contacts.aspx HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/contacts.aspx
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 533
10 DNT: 1
11 Connection: close
12 Cookie: mscope=1jWydNfBwro=; ui-tabs-1=0
13 Upgrade-Insecure-Requests: 1
14
15 --EVENTTARGET=lnksubmit&__EVENTARGUMENT=&__VIEWSTATE=
```
- Request Body:**

```
%2FwEPDwULLTE4njISMTU3MDIPZBYCAgEPZBYEAgMPDxYCHgRUXhOBQZMb2dvdXRkZAIFDw8WAh8ABQNZYWlkZGQcKYVta0FA%2F6kKXsq8NSVbVl.gP7V0yyt n%2BVdnYc%2BwP0w%3D%2D&__VIEWSTATEGENERATOR=0338CC7D&__EVENTVALIDATION=%2FwEdAAcG%2Bc0a26sMKNh9bmSjON66C9eh6qGZ4Hdrv%2FyGwFTHSAp3Nn%2FuC3tvrqCChAvZ24xKtGnNus1FYh0yF8blX%2FWKVCn2pfnngd5PSl9R1fd0WCUpv1PE9gUPSM6P%2B1Lso8hIaHw0A6cz1%2FD70ZxJByddjRPEC5ZrYSzMpEN2IUEhGX9I42ndd4VYJvjmSHlySC0%3D&t name=&t comment=This+is+a+lab+task+to+test+injection+vulnerability
```

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

EXERCISE 5:

DETECT INJECTION VULNERABILITY USING BURP SUITE

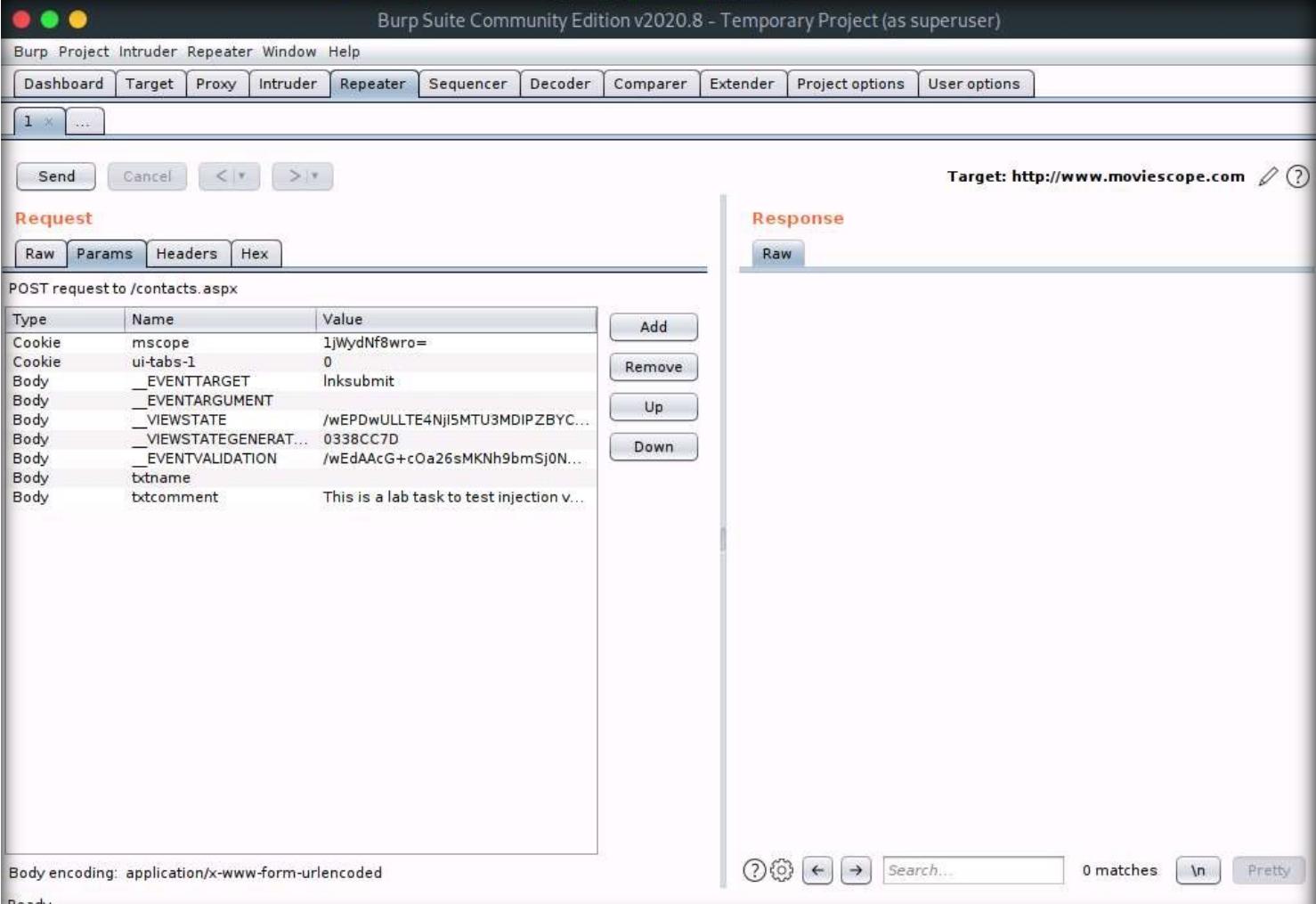


The screenshot shows the Burp Suite interface with the following details:

- Project:** Temporary Project (as superuser)
- Tab:** Intercept (selected)
- Request List:**
 - Host: http://detectportal.firefox.c... Method: GET URL: /success.txt Status: 200 Length: 239 MIME type: text Extension: txt Title:
 - Host: http://detectportal.firefox.c... Method: GET URL: /success.txt Status: 200 Length: 239 MIME type: text Extension: txt Title:
 - Host: http://detectportal.firefox.c... Method: GET URL: /success.txt Status: 200 Length: 239 MIME type: text Extension: txt Title:
 - Host: http://www.moviescope.com Method: POST URL: /contacts.aspx Status: 200 Length: 239 MIME type: HTML Extension: aspx Title: Contacts - MovieScope
 - Host: http://detectportal.firefox.c... Method: GET URL: /success.txt Status: 200 Length: 239 MIME type: text Extension: txt Title:
 - Host: http://detectportal.firefox.c... Method: GET URL: /success.txt Status: 200 Length: 239 MIME type: text Extension: txt Title:
- Request Details:**

```
1 POST /contacts.aspx HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) G
4 Accept: text/html,application/xhtml+xml,application/
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/contacts.aspx
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 533
10 DNT: 1
11 Connection: close
12 Cookie: mscoope=ljWydNfBwro=; ui-tabs-l=0
13 Upgrade-Insecure-Requests: 1
14
15 _EVENTTARGET=lnksubmit&__EVENTARGUMENT=&__VIEWSTATE
%2FwEPDwULLTE4njISMTU3MDIPZBYCAgEPZBYEagMPDxYCHgRUZX
D%3D&__VIEWSTATEGENERATOR=0338CC7D&__EVENTVALIDATION
%2FwEdAACg%2Bc0a26sMKNh9bmSj0N66C9eh6qGZ4Hdrv%2FyGwF
BiLso8hIahW0A6czl%2FD70ZxJBYddjRPEC5zrYSzMpEN2IUEhGX9I42ndd4VYJvjm5HlySC0%3D&txtname=&txtcomment=
This+is+a+lab+task+to+test+injection+vulnerability
```
- Context Menu (Open over POST request):**
 - Send to Intruder (Ctrl+I)
 - Send to Repeater (Ctrl+R) [Selected]**
 - Send to Sequencer
 - Send to Comparer (request)
 - Send to Comparer (response)
 - Show response in browser
 - Request in browser
 - Engagement tools [Pro version only]
 - Show new history window
 - Add comment
 - Highlight
 - Delete item
 - Clear history
 - Copy URL
 - Copy as curl command
 - Copy links
 - Save item
 - Proxy history documentation

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



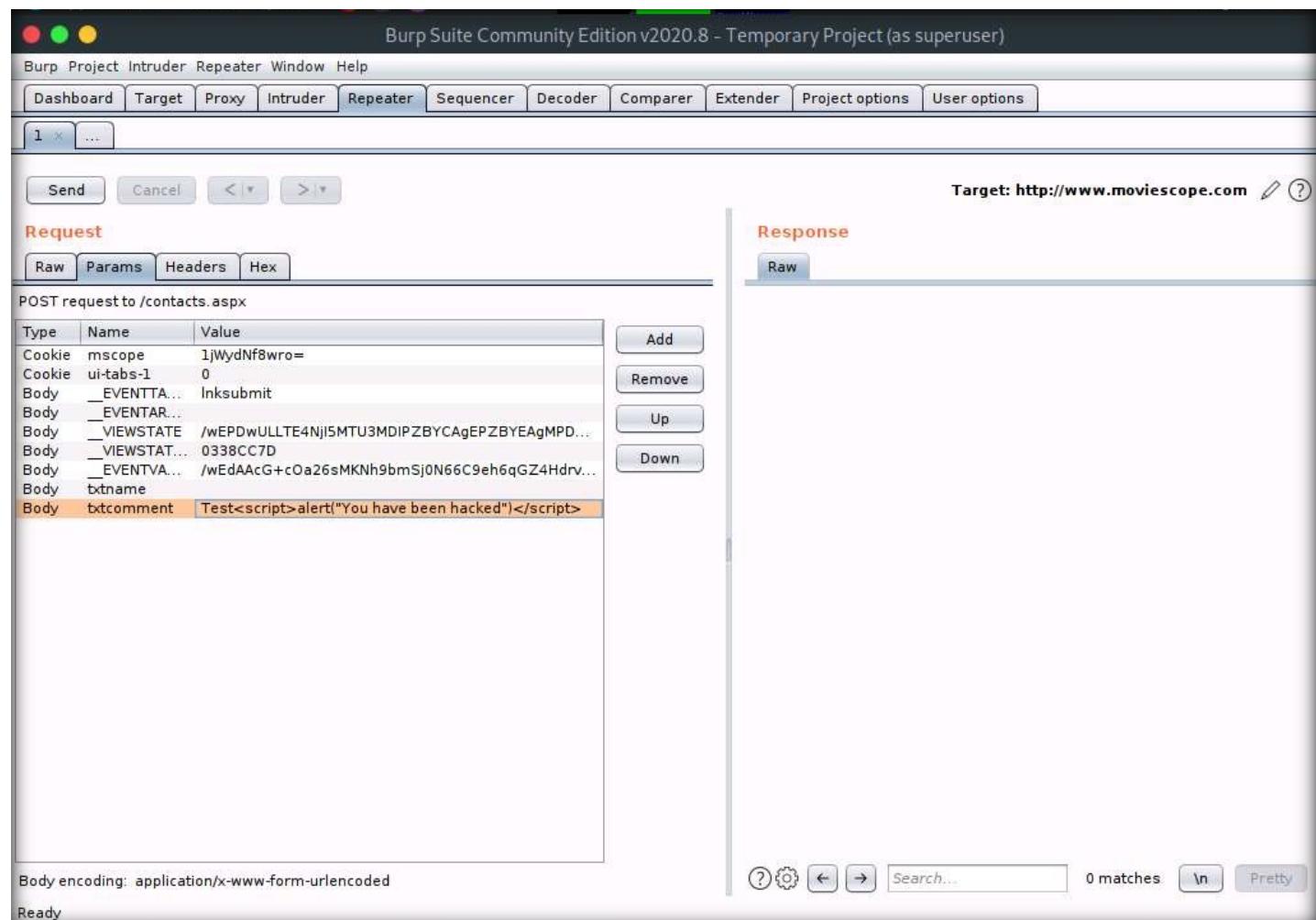
The screenshot shows the Burp Suite interface with the following details:

- Request Tab:** The "Params" tab is selected.
- Target:** http://www.moviescope.com
- Request URL:** POST request to /contacts.aspx
- Table:** A table showing parameters:

Type	Name	Value	Actions
Cookie	mscope	1jWydNf8wro=	Add
Cookie	ui-tabs-1	0	Remove
Body	_EVENTTARGET	Inksubmit	Up
Body	_EVENTARGUMENT		Down
Body	_VIEWSTATE	/wEPDwULLTE4NjI5MTU3MDIPZBYC...	
Body	_VIEWSTATEGENERAT...	0338CC7D	
Body	_EVENTVALIDATION	/wEdAACG+cOa26sMKNh9bmSj0N...	
Body	txname		
Body	txtcomment	This is a lab task to test injection v...	
- Response Tab:** The "Raw" tab is selected.
- Bottom Status:** Body encoding: application/x-www-form-urlencoded
- Bottom Buttons:** Search, 0 matches, Pretty

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>

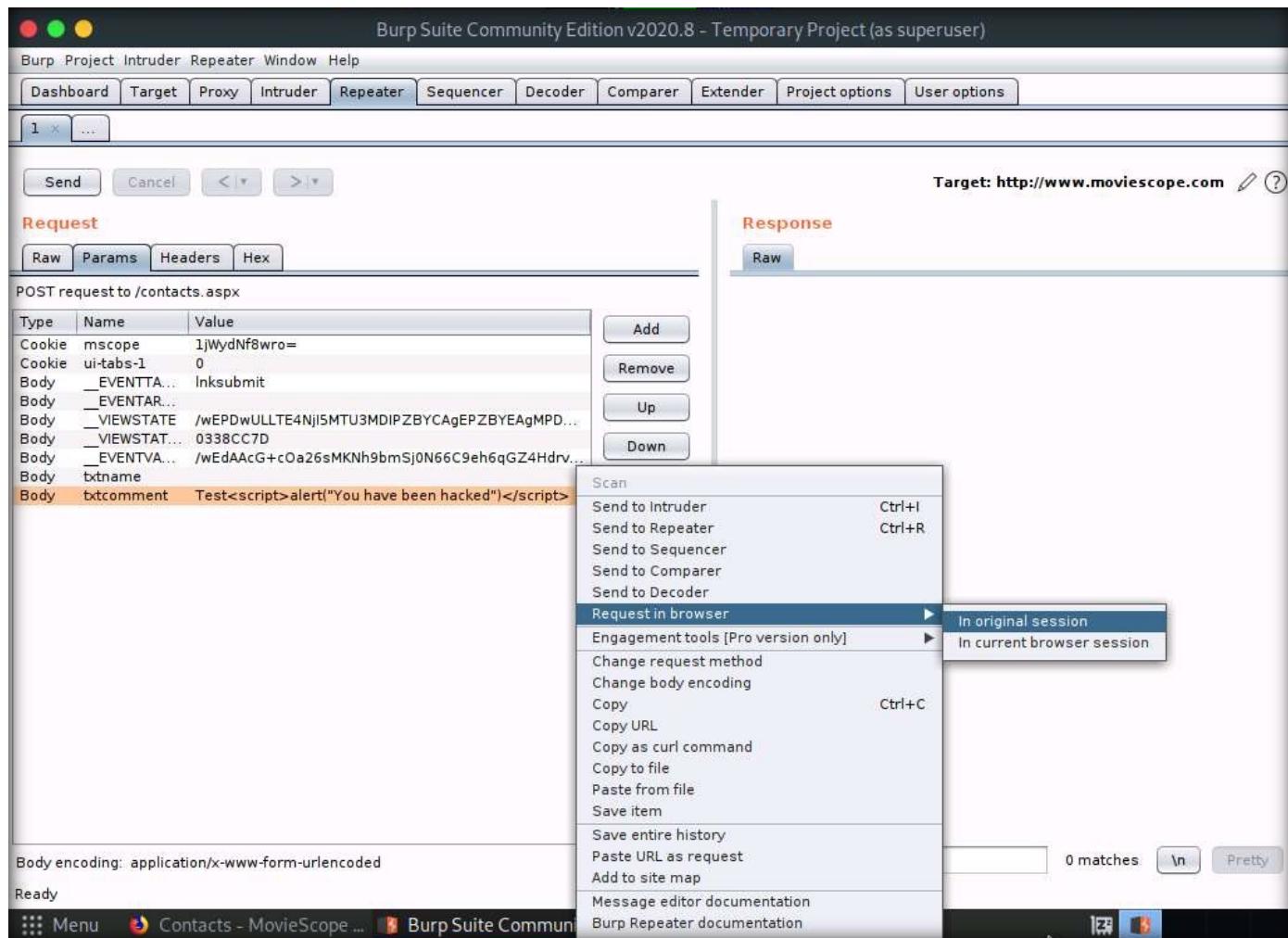


The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The toolbar has buttons for "Send", "Cancel", and navigation arrows. The main window is divided into "Request" and "Response" panes. The "Request" pane shows a "POST request to /contacts.aspx" with various form fields. One field, "txtcomment", is highlighted and contains the exploit script: "Test<script>alert('You have been hacked')</script>". To the right of the request pane are buttons for "Add", "Remove", "Up", and "Down". The "Response" pane is currently empty. At the bottom, there are buttons for "Body encoding: application/x-www-form-urlencoded", "Search...", and status indicators like "0 matches" and "Pretty".

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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



Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Target: <http://www.moviescope.com>

Request

Raw Params Headers Hex

POST request to /contacts.aspx

Type	Name	Value
Cookie	mscope	1jWydNf8wro=
Cookie	ui-tabs-1	0
Body	_EVENTTA...	Inksubmit
Body	_EVENTAR...	
Body	_VIEWSTATE	/wEPDwULLTE4Nj5MTU3MDIPZBYCAgEPZBYEAgMPD...
Body	_VIEWSTAT...	0338CC7D
Body	_EVENTVA...	/wEdAACG+cOa26sMKNh9bmSj0N66C9eh6qGZ4Hdrv...
Body	txtname	
Body	txtcomment	Test<script>alert("You have been hacked")</script>

Response

Raw

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser ▶
 - In original session
 - In current browser session
- Engagement tools [Pro version only] ▶
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Save entire history
- Paste URL as request
- Add to site map
- Message editor documentation
- Burp Repeater documentation

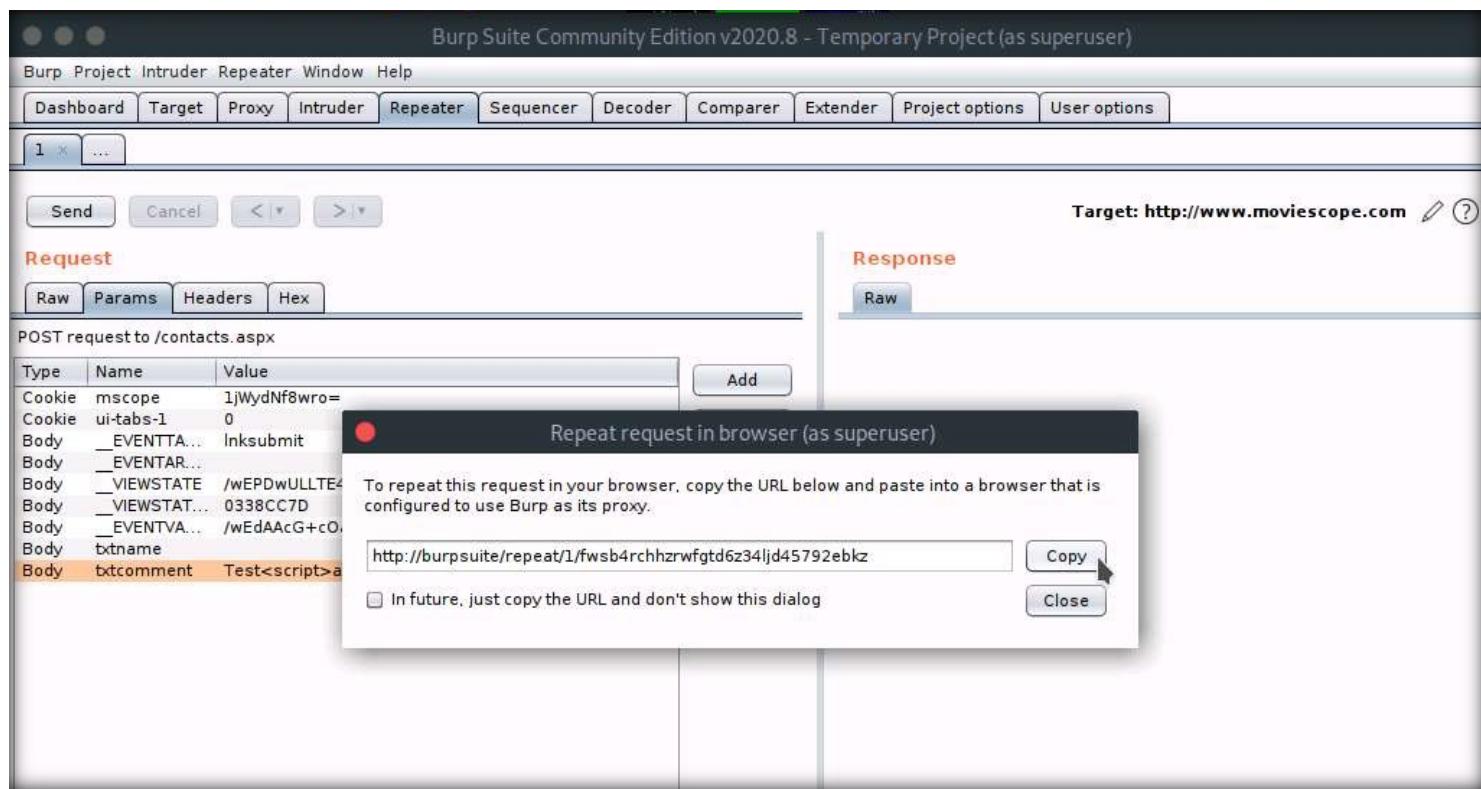
Body encoding: application/x-www-form-urlencoded

Ready

Menu Contacts - MovieScope ... Burp Suite Commun

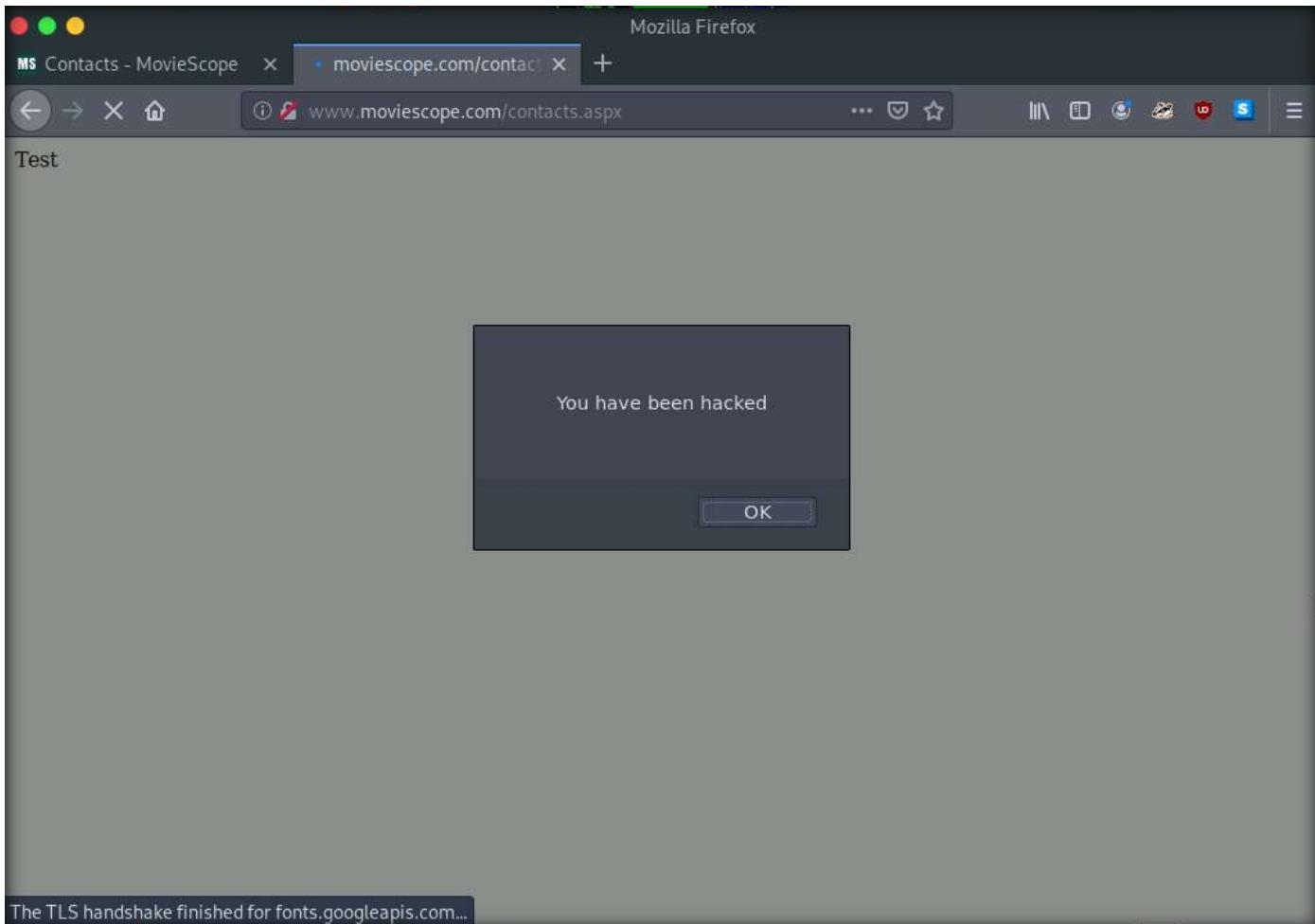
EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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



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.

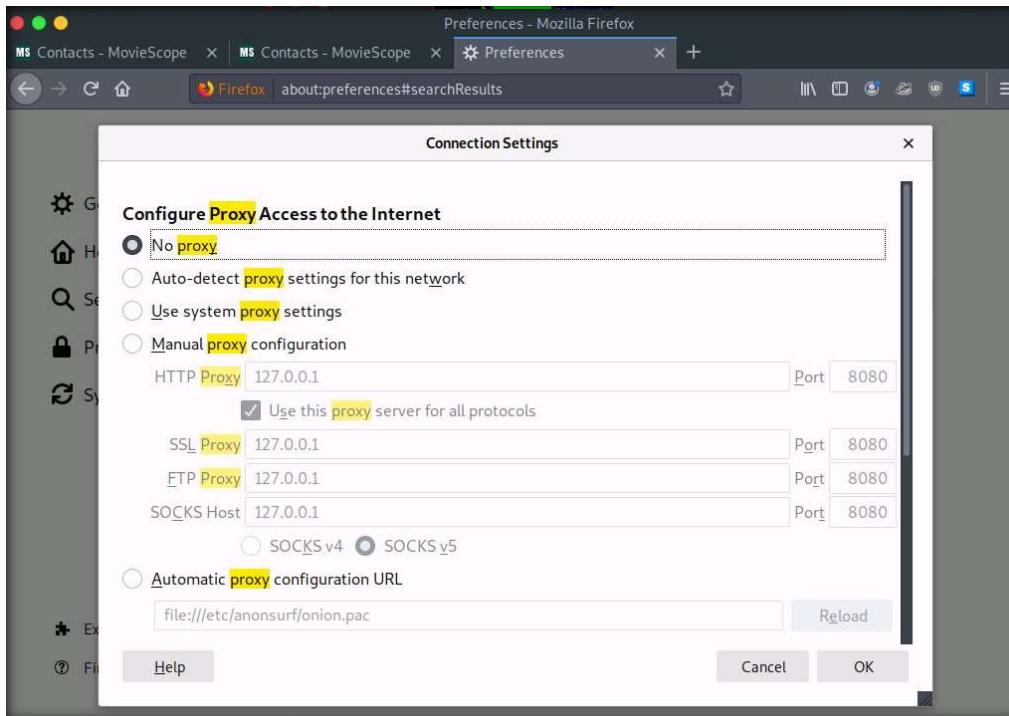


EXERCISE 5: DETECT INJECTION VULNERABILITY USING BURP SUITE

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 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.

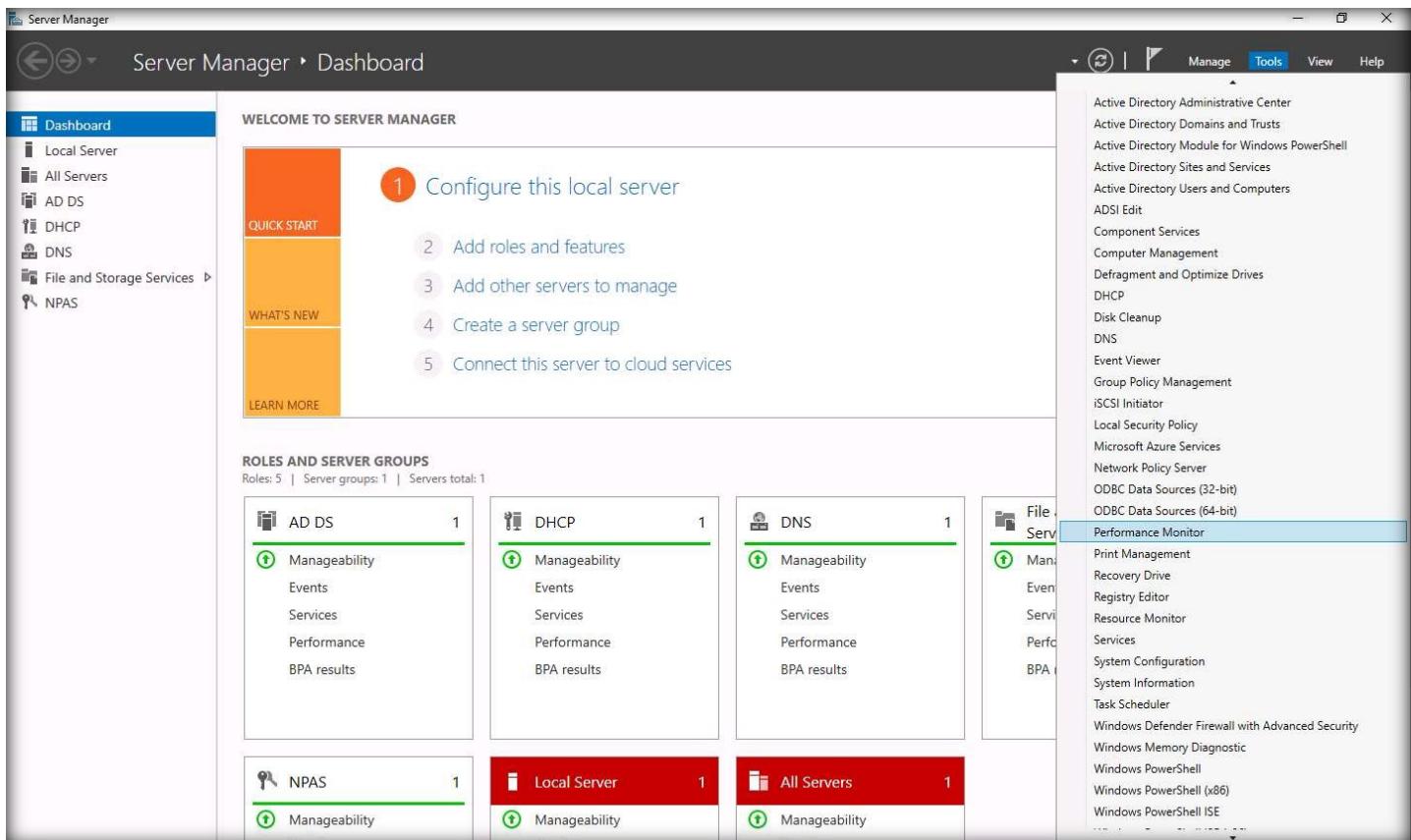
Attackers exploit vulnerabilities in the applications to launch various attacks and gain unauthorized access to resources. It is commonly assumed that perimeter security controls such as firewall and IDS systems can secure an application; however, this is not true as these controls are not effective 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.

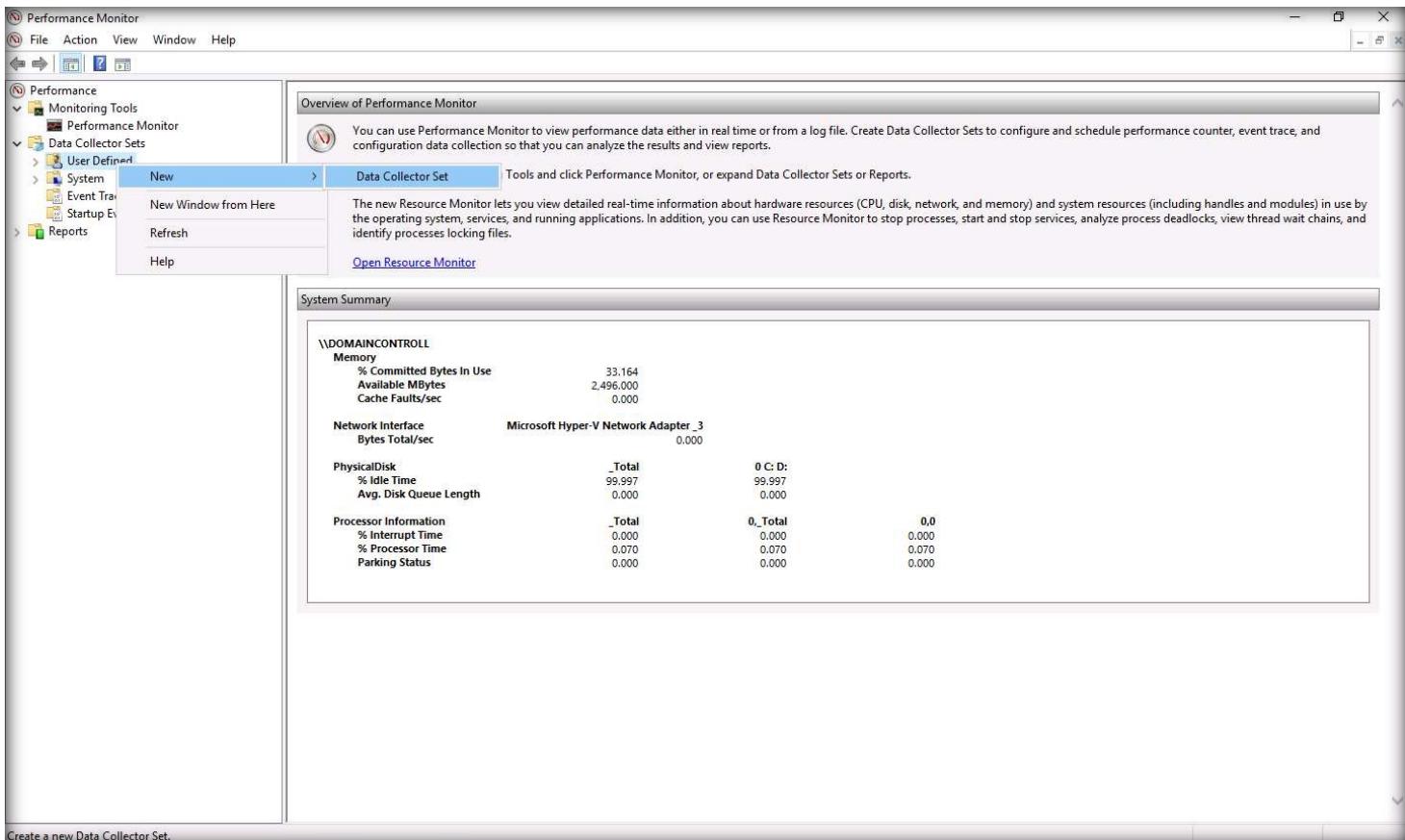
1. Turn on the AD Domain Controller machine.
2. Log in with the credentials CCT\Administrator and admin@123.

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.



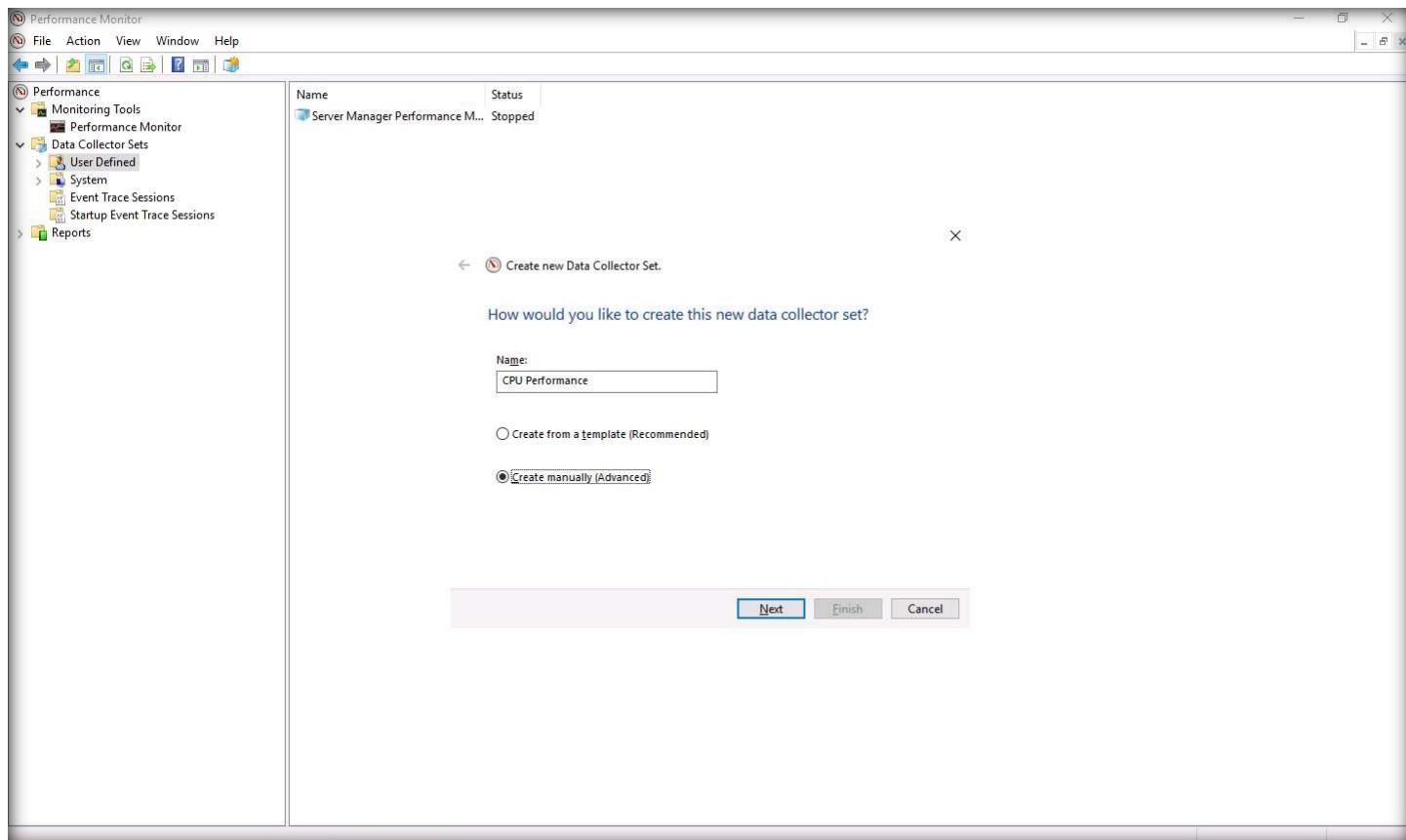
5. Performance Monitor window appears. From the left-pane, expand Data Collector Sets, right-click User Defined node and navigate to New > Data Collector Set.



EXERCISE 6:

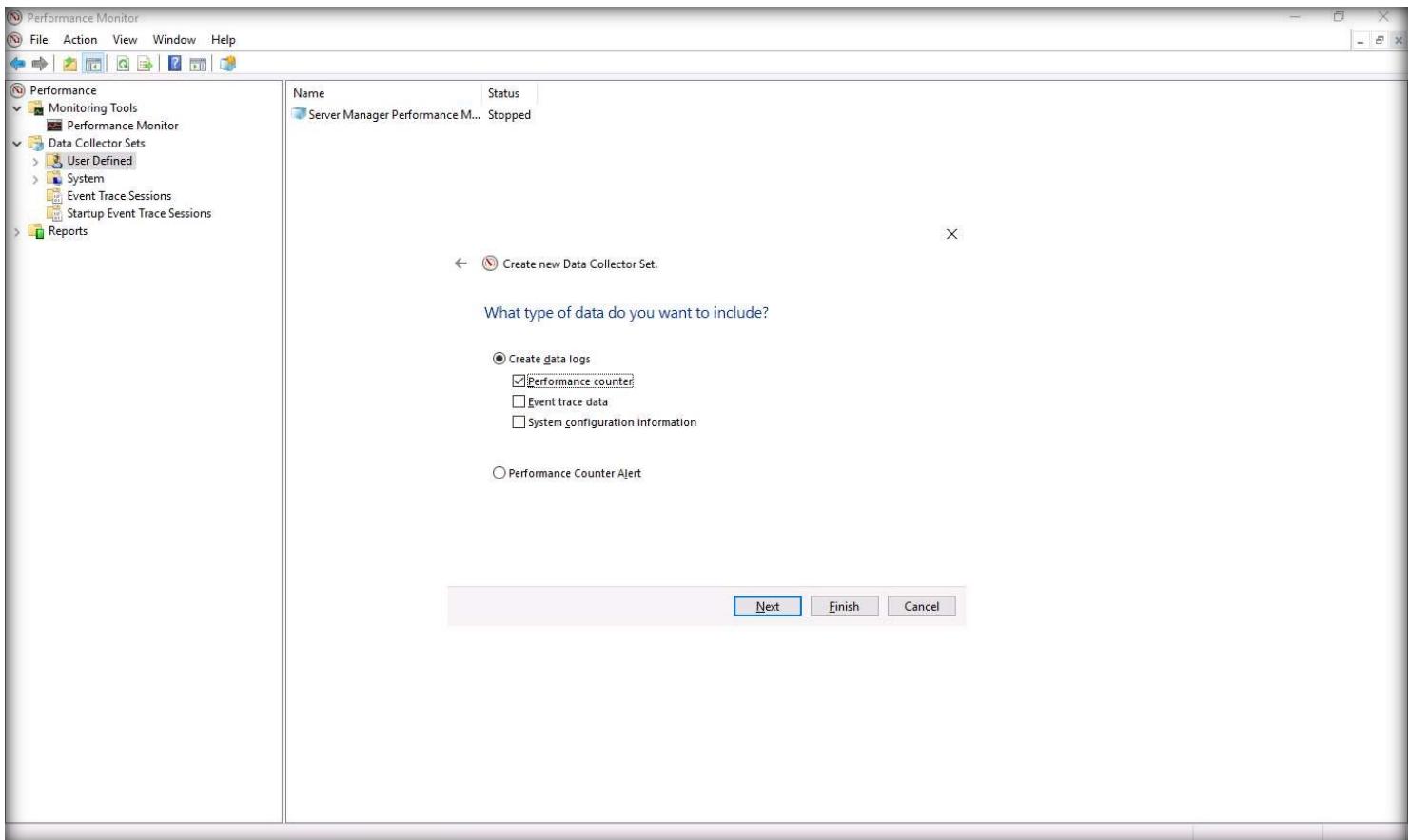
DETERMINE APPLICATION-LEVEL ATTACKS

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

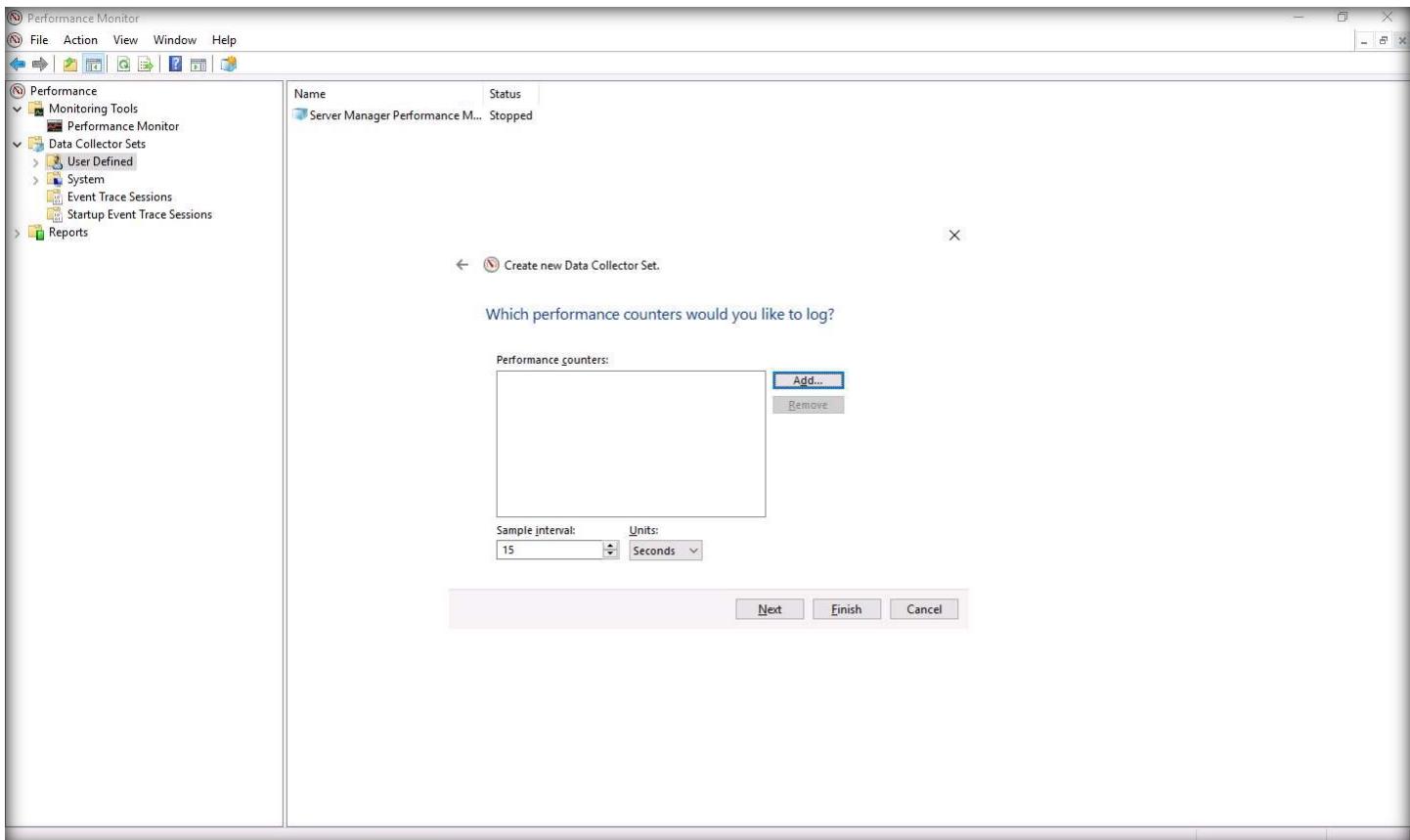
7. In the next wizard, select Performance counter checkbox under Create data logs radio button and click Next.



EXERCISE 6:

DETERMINE APPLICATION-LEVEL ATTACKS

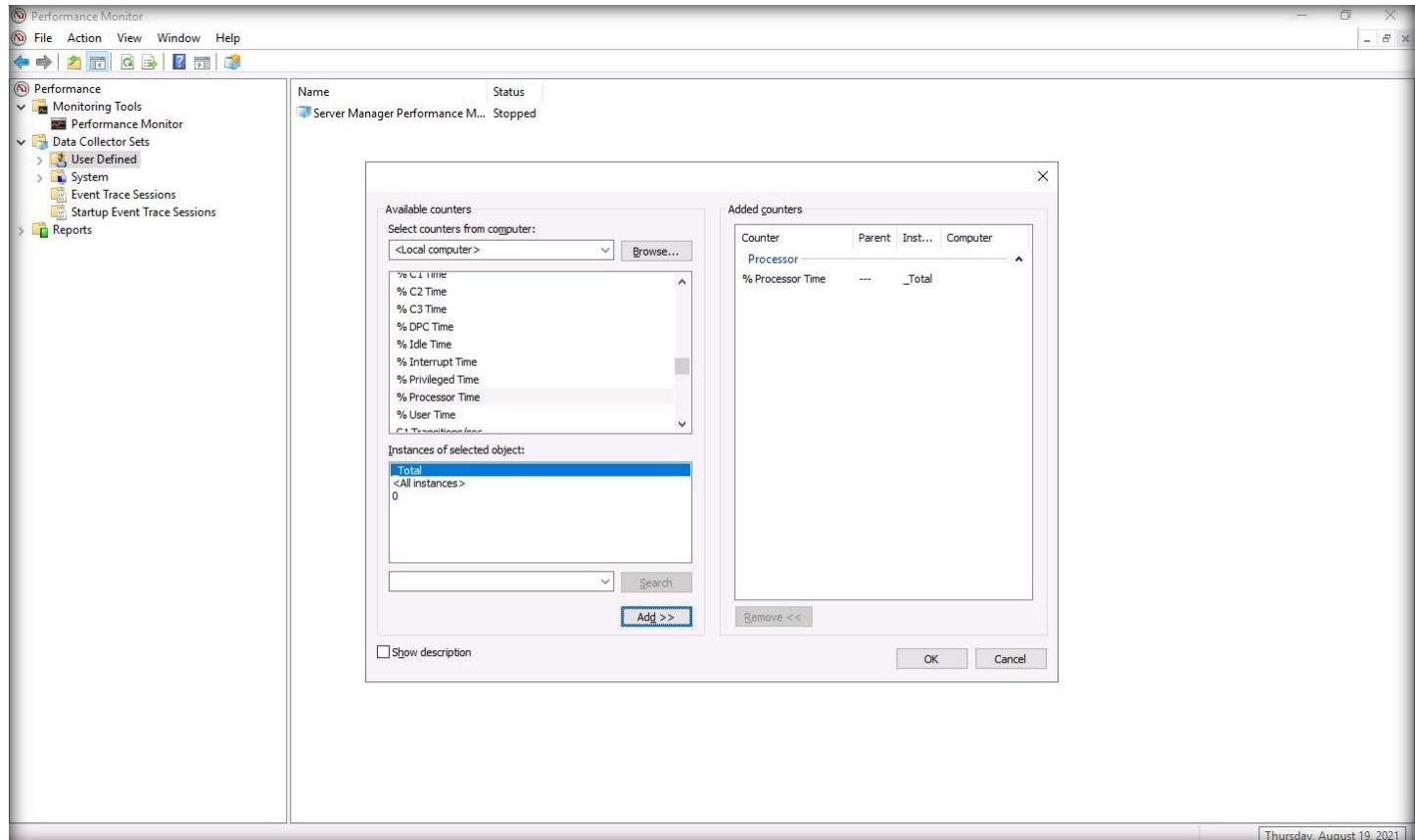
8. Which performance counters would you like to log? wizard appears, click Add... button.



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.

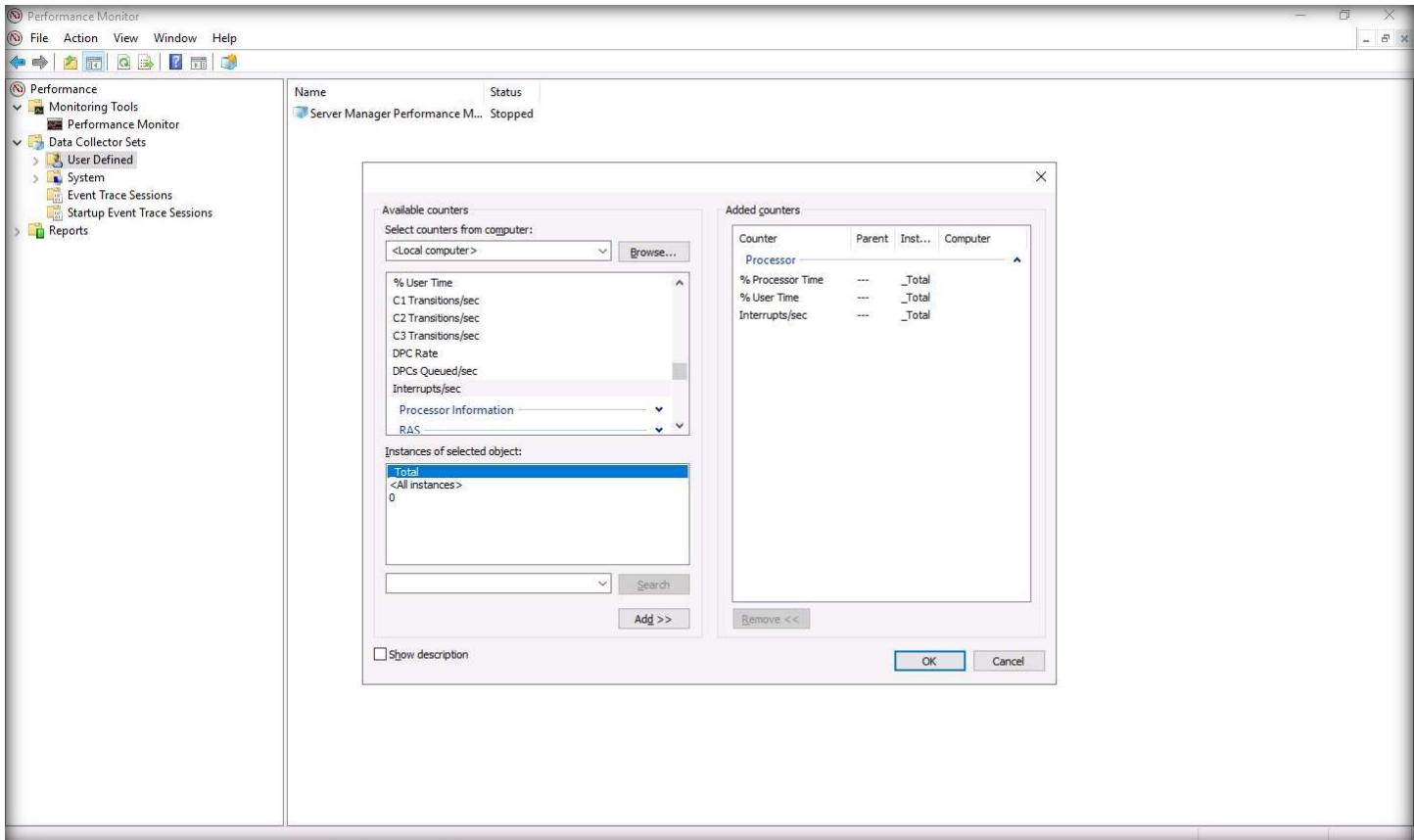
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



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

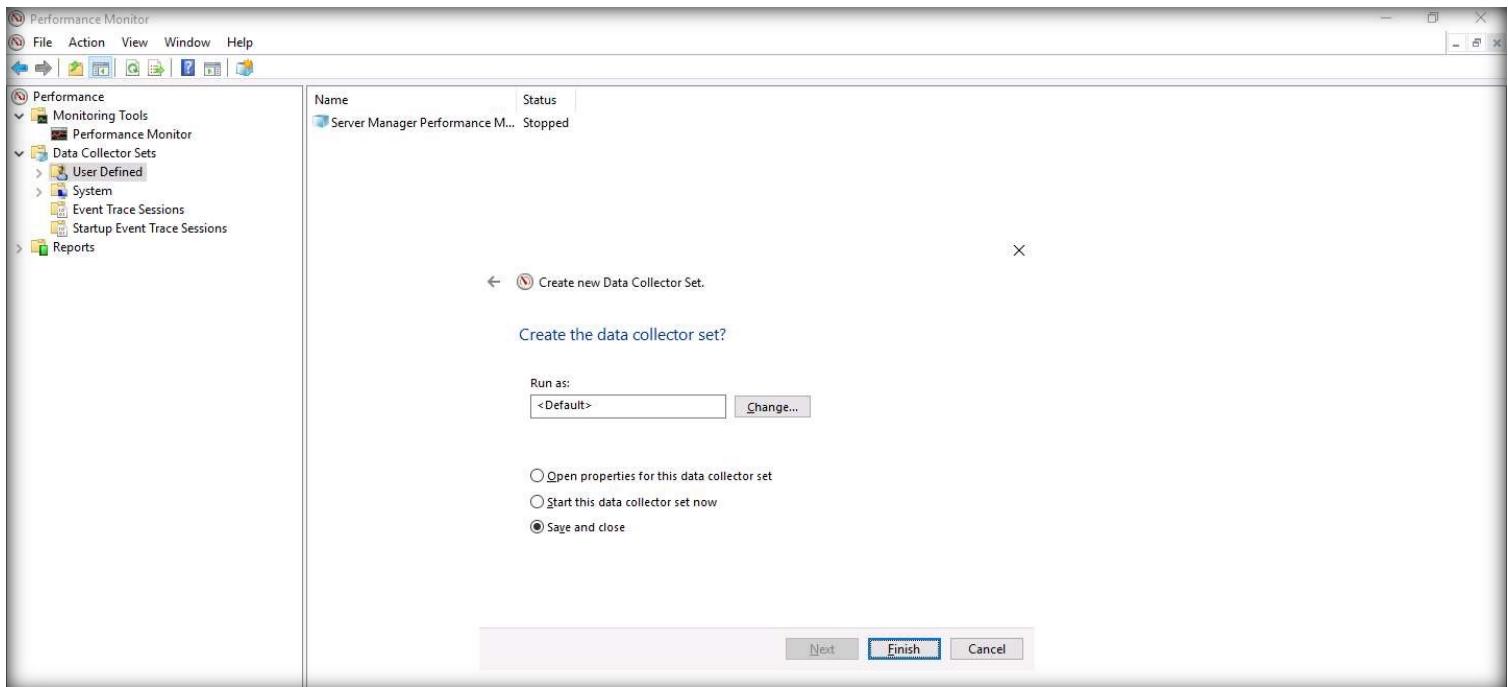
Note:

- % 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:

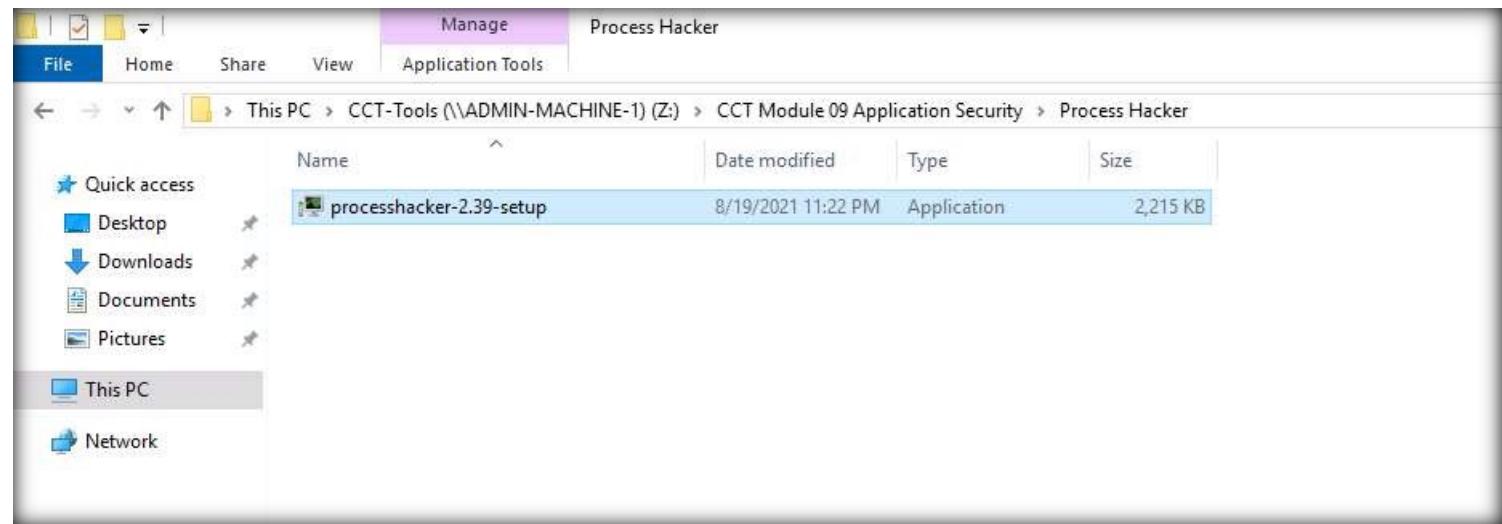
DETERMINE APPLICATION-LEVEL ATTACKS



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.

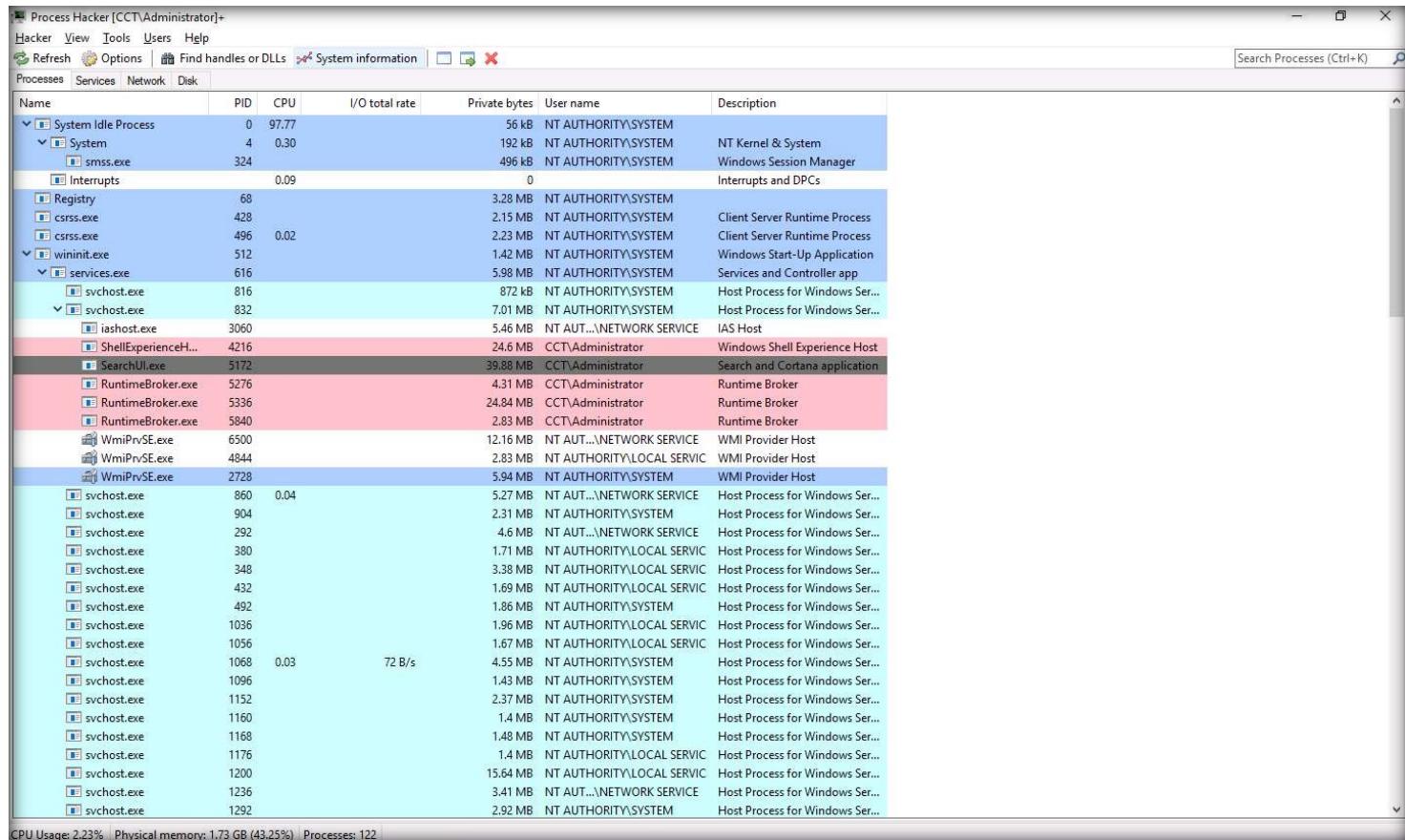
EXERCISE 6:

DETERMINE APPLICATION-LEVEL ATTACKS

Name	PID	CPU	I/O total rate	Private bytes	User name	Description
System Idle Process	0	97.88		56 kB	NT AUTHORITY\SYSTEM	
System	4	0.28		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	324			496 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Interrupts		0.09		0		Interrupts and DPCs
Registry	68			3.28 MB	NT AUTHORITY\SYSTEM	
csrss.exe	428			2.15 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
csrss.exe	496			2.23 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	512			1.42 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	616			5.88 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	816			872 kB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	832	0.01	88 B/s	6.96 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
lashost.exe	3060			5.46 MB	NT AUT...\\NETWORK SERVICE	IAS Host
ShellExperienceH...	4216	0.02		24.6 MB	CCT\Administrator	Windows Shell Experience Host
SearchH.exe	5172			39.88 MB	CCT\Administrator	Search and Cortana application
RuntimeBroker.exe	5276			4.38 MB	CCT\Administrator	Runtime Broker
RuntimeBroker.exe	5336			24.84 MB	CCT\Administrator	Runtime Broker
RuntimeBroker.exe	5840			2.9 MB	CCT\Administrator	Runtime Broker
svchost.exe	860			5.11 MB	NT AUT...\\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	904			2.26 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	292			4.39 MB	NT AUT...\\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	380			1.71 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	348			3.43 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	432			1.69 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	492			1.86 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1036			1.88 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	1056			1.59 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	1068			4.55 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1096			1.43 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1152			2.37 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1160			1.4 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1168			1.48 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1176			1.4 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	1200			15.92 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...
svchost.exe	1236			3.26 MB	NT AUT...\\NETWORK SERVICE	Host Process for Windows Ser...
svchost.exe	1292			2.81 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1320			2.32 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1388			1.16 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	1396			1.82 MB	NT AUTHORITY\\LOCAL SERVIC	Host Process for Windows Ser...

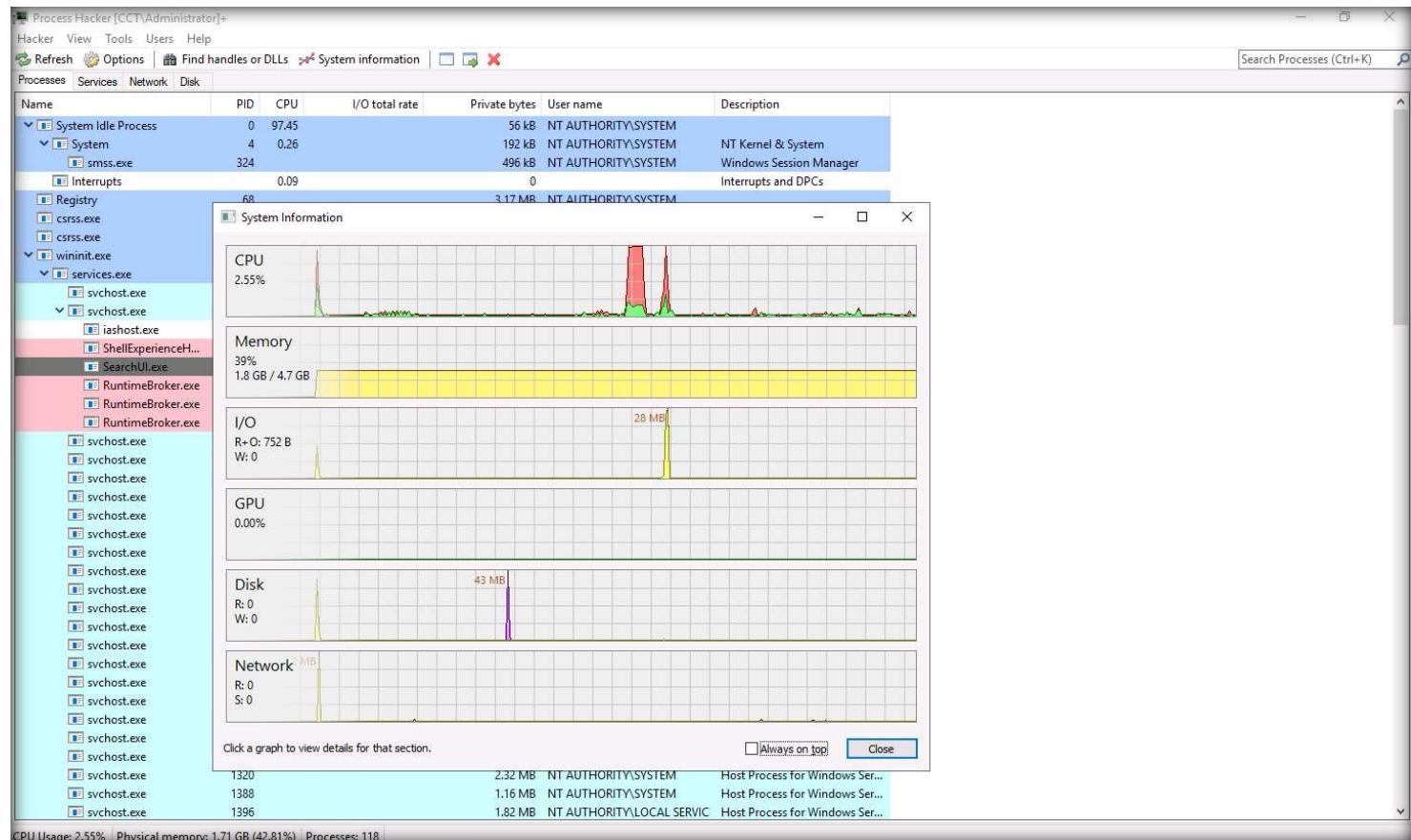
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS

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



EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS

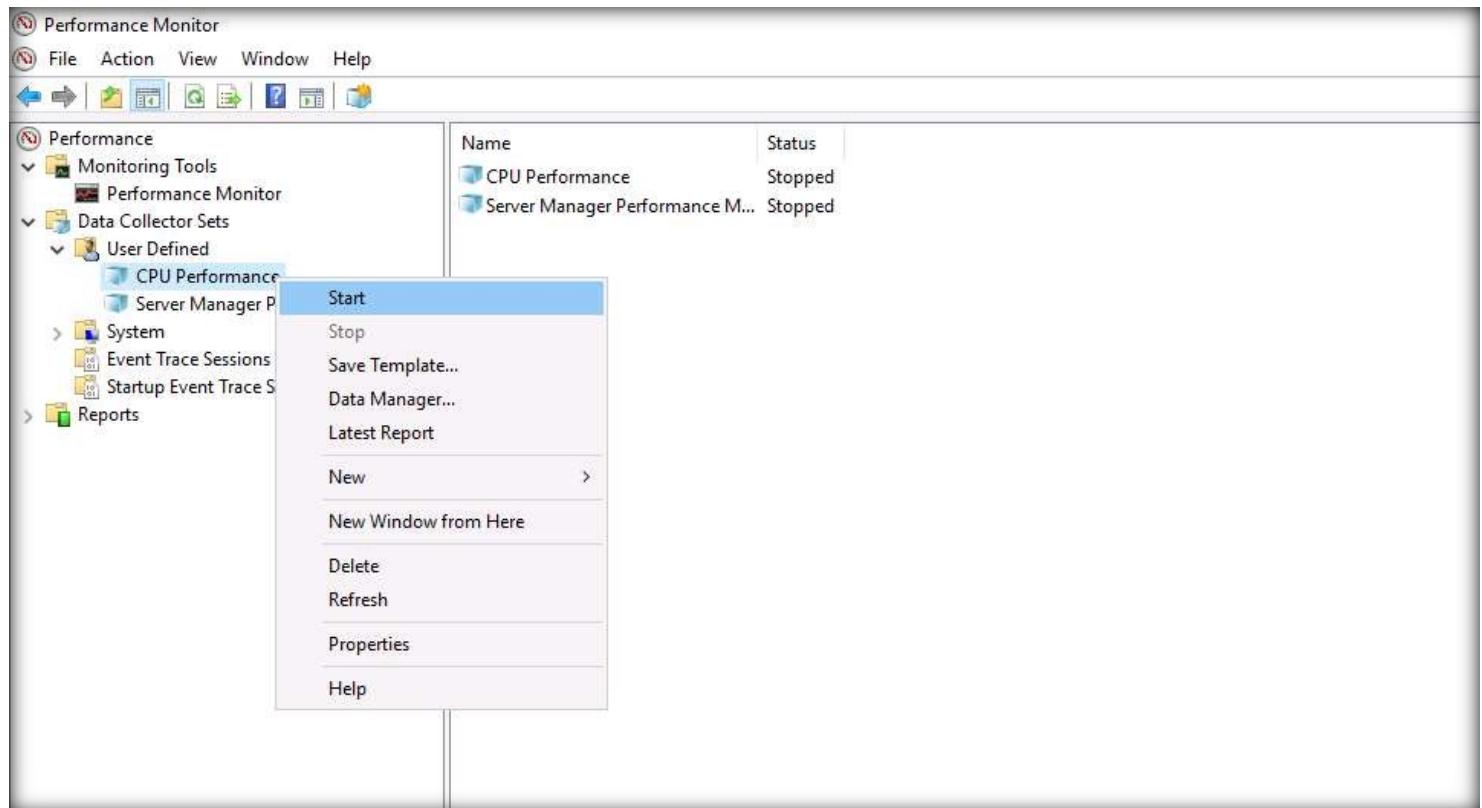
22. A System information window appears, displaying CPU, Memory, I/O, GPU, Disk, Network utilization, as shown in the screenshot below.



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.

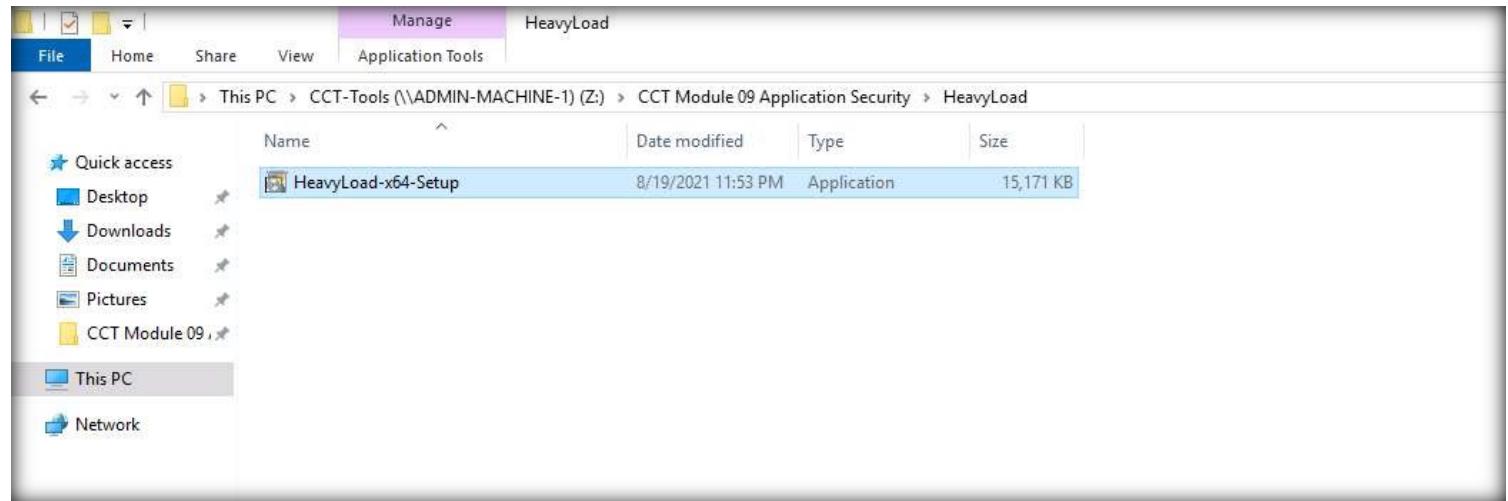
24. Maximize Performance Monitor window. From the left-pane, expand Data Collector Sets and User Defined node. Right-click CPU Performance node and click Start. Minimize the window.



EXERCISE 6:

DETERMINE APPLICATION-LEVEL ATTACKS

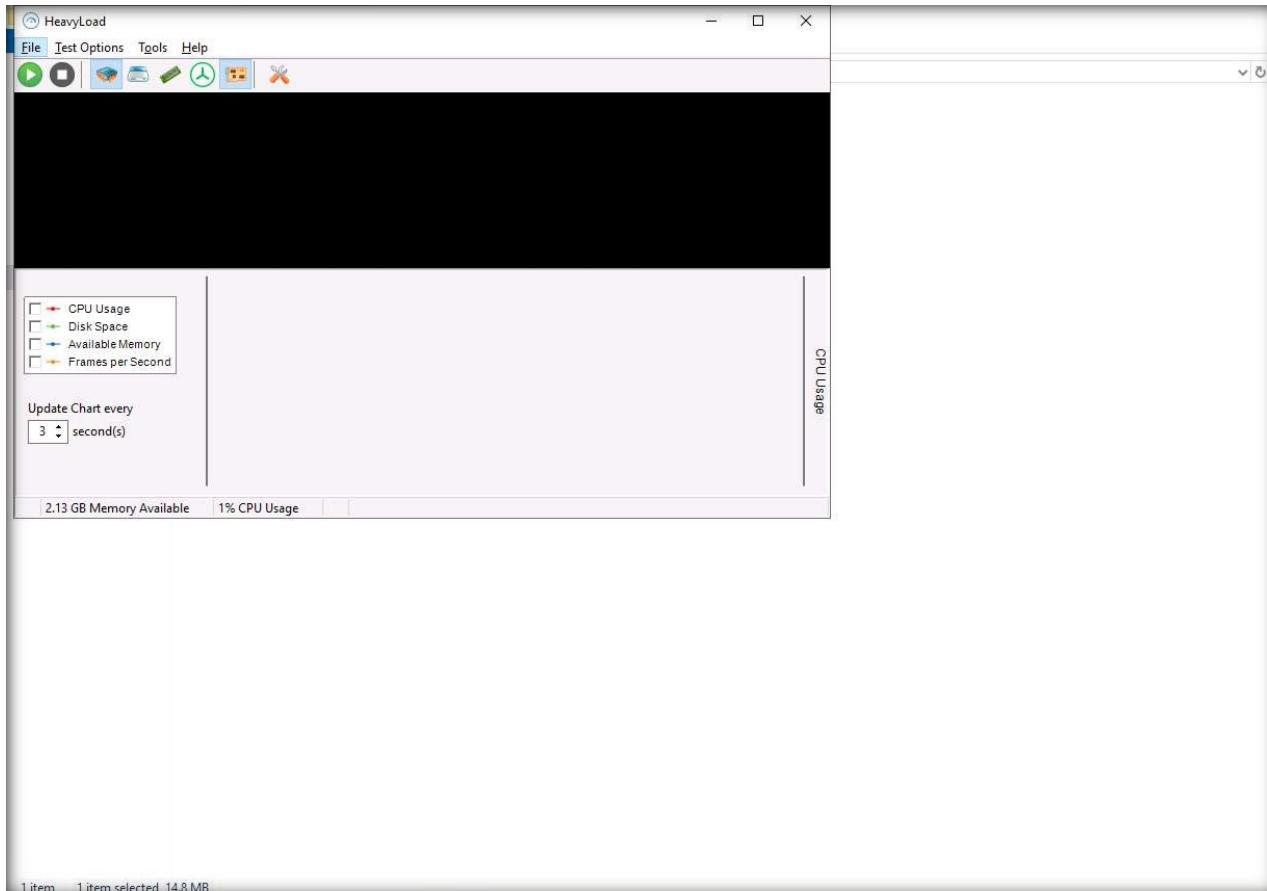
25. Maximize the File Explorer window and navigate to Z:\CCT Module 09 Application Security\HeavyLoad. Double-click HeavyLoad-x64-setup.exe.



EXERCISE 6:

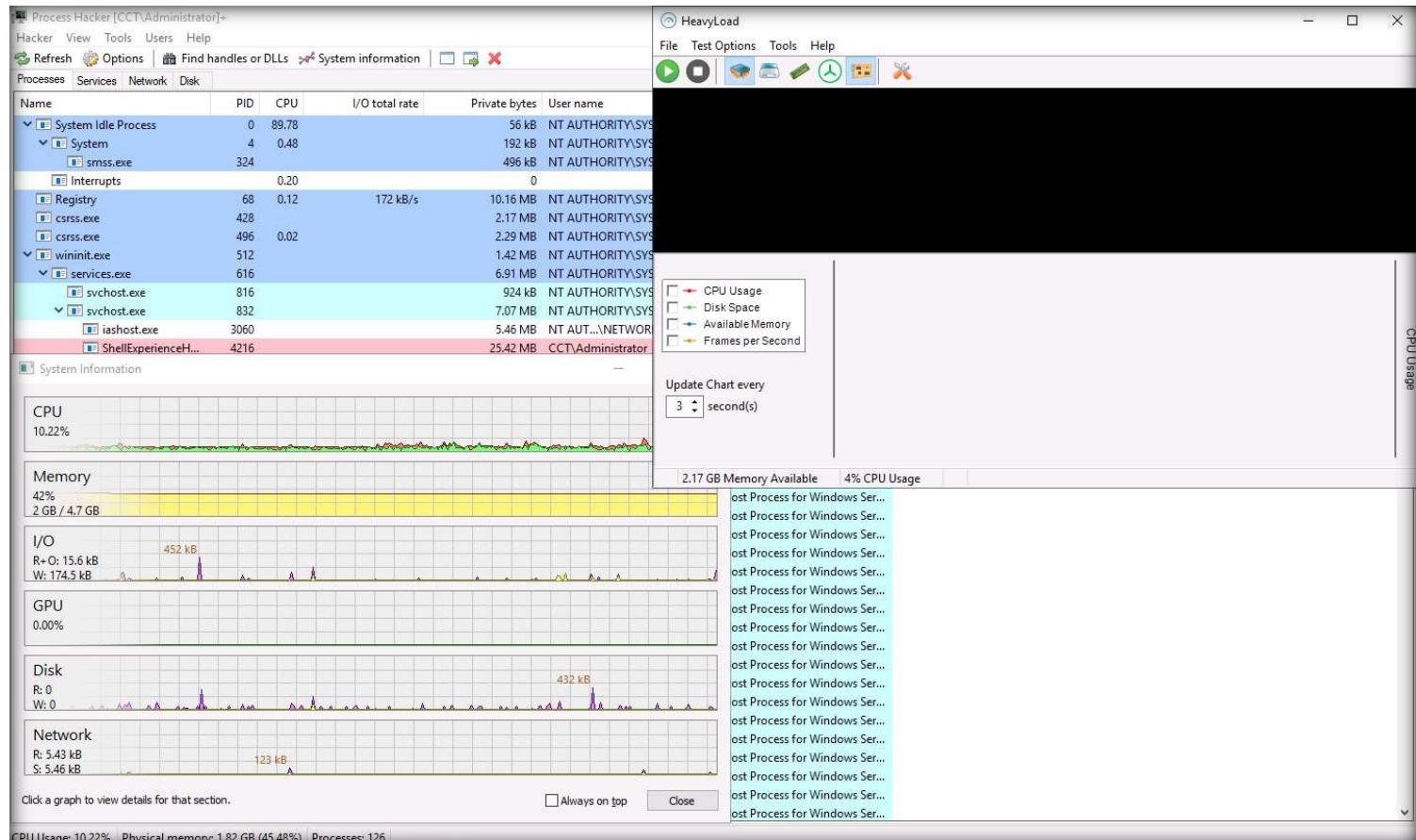
DETERMINE APPLICATION-LEVEL ATTACKS

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.



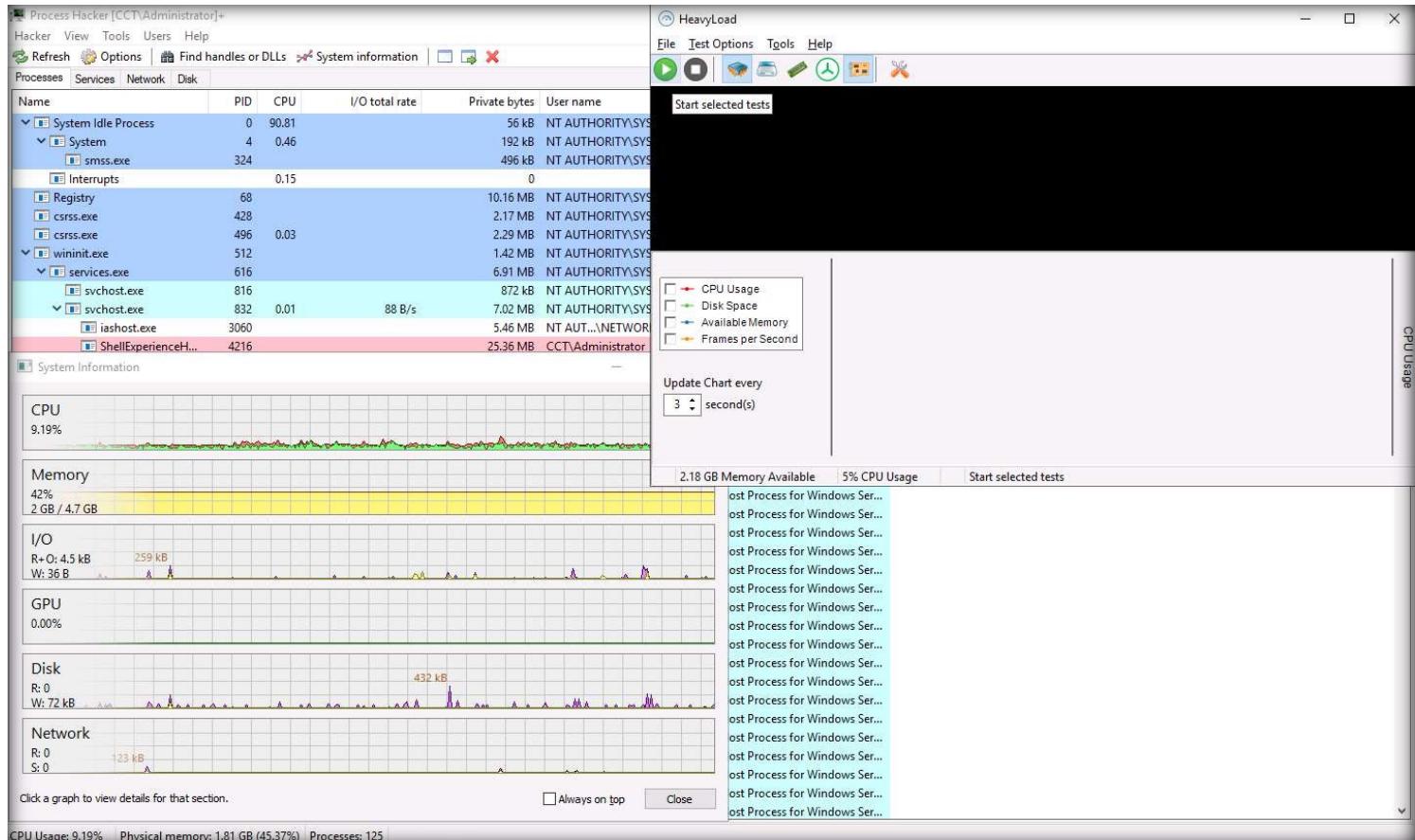
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS

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 start creating stress on the system.



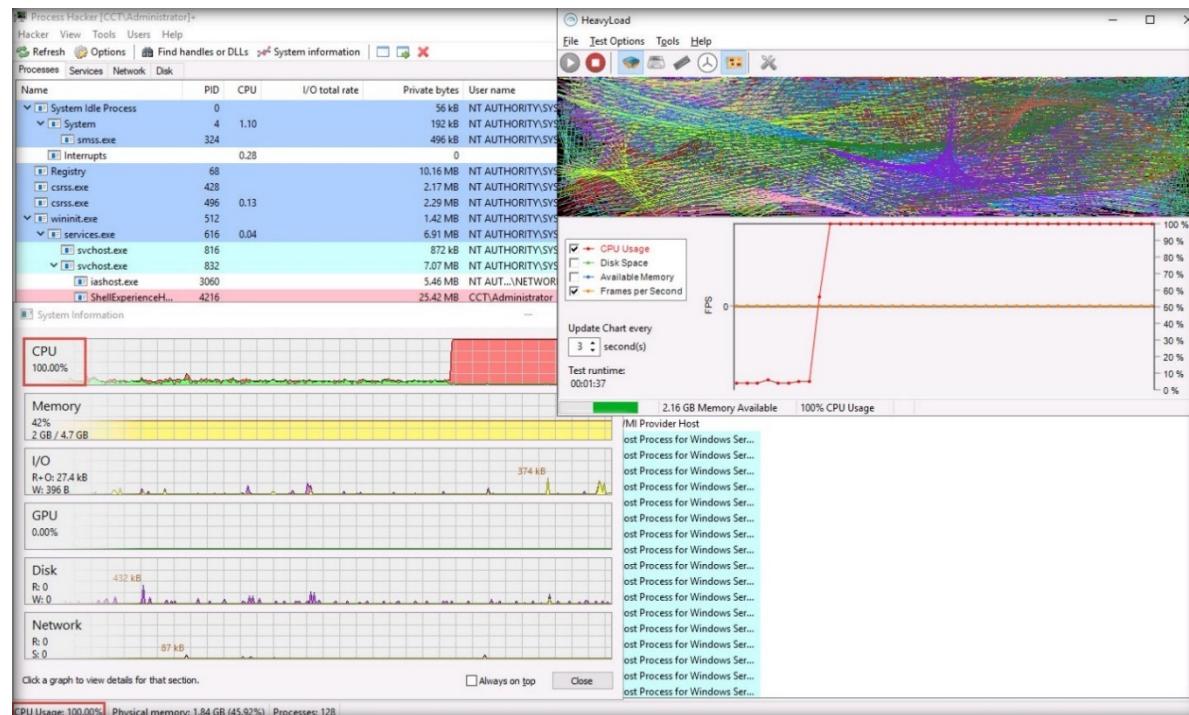
34. A Virtual machine detected window appears, click Continue.

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.

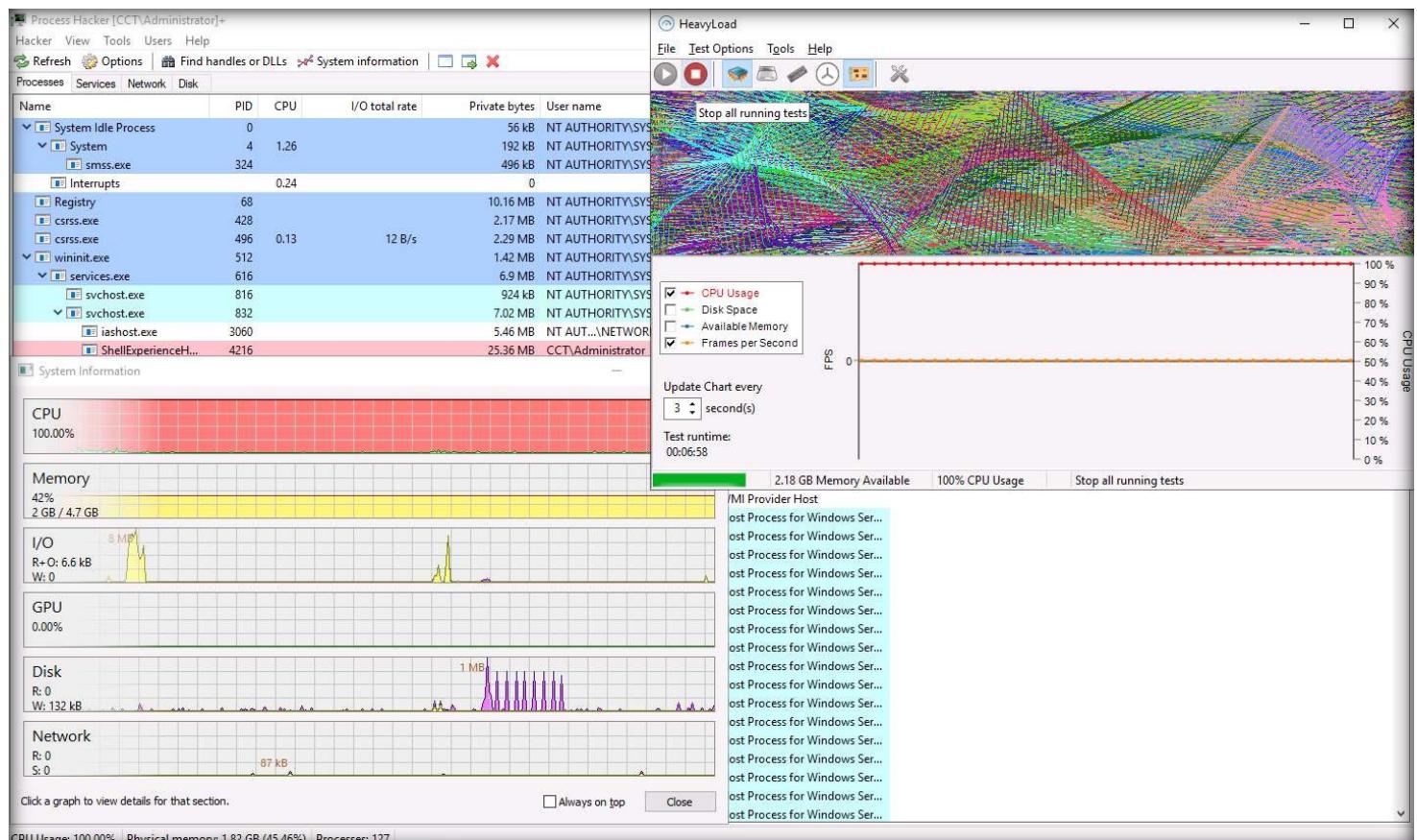
37. Similarly, you can observe the CPU Usage (100%) in the bottom-left corner of Process Hacker window.

EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



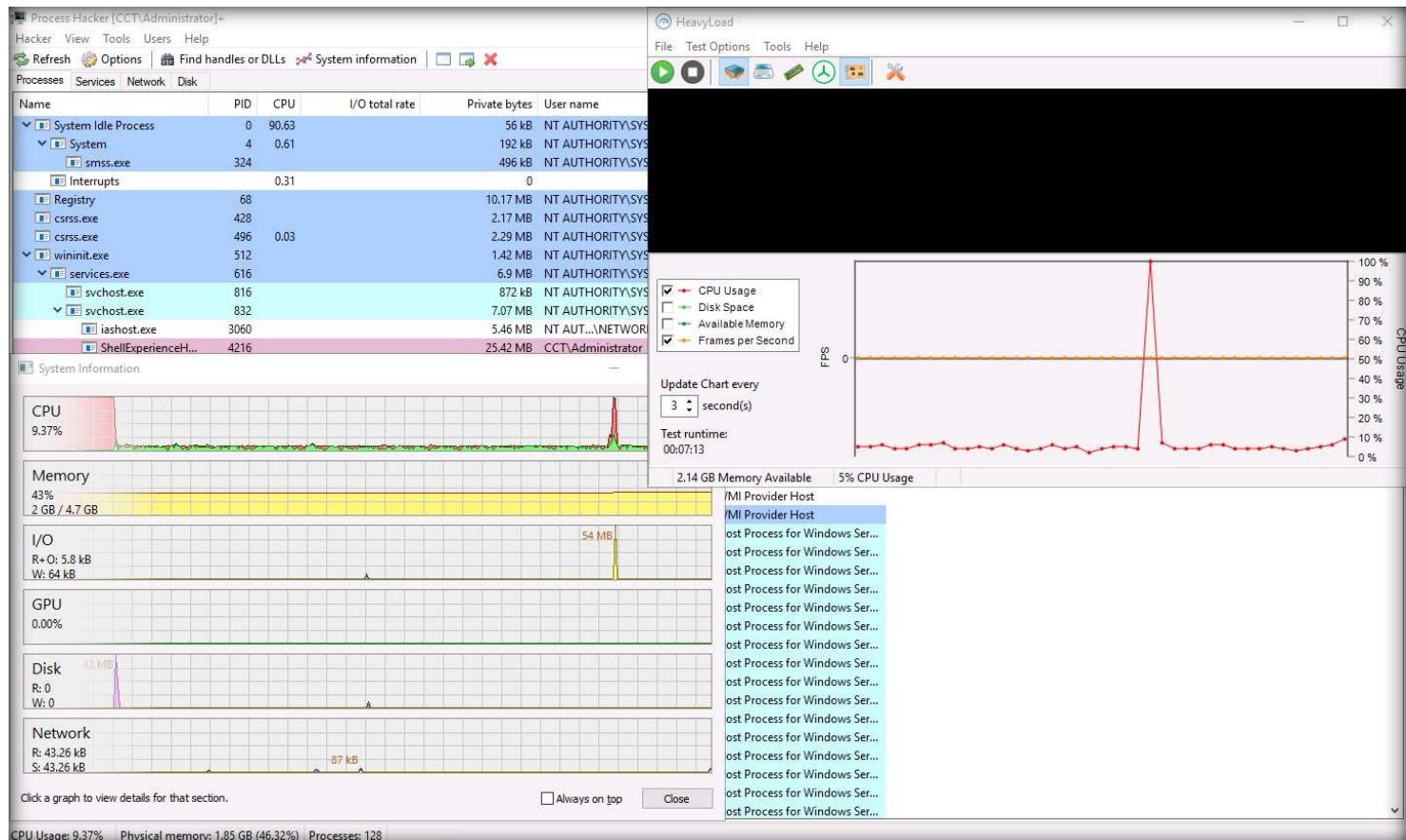
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS

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

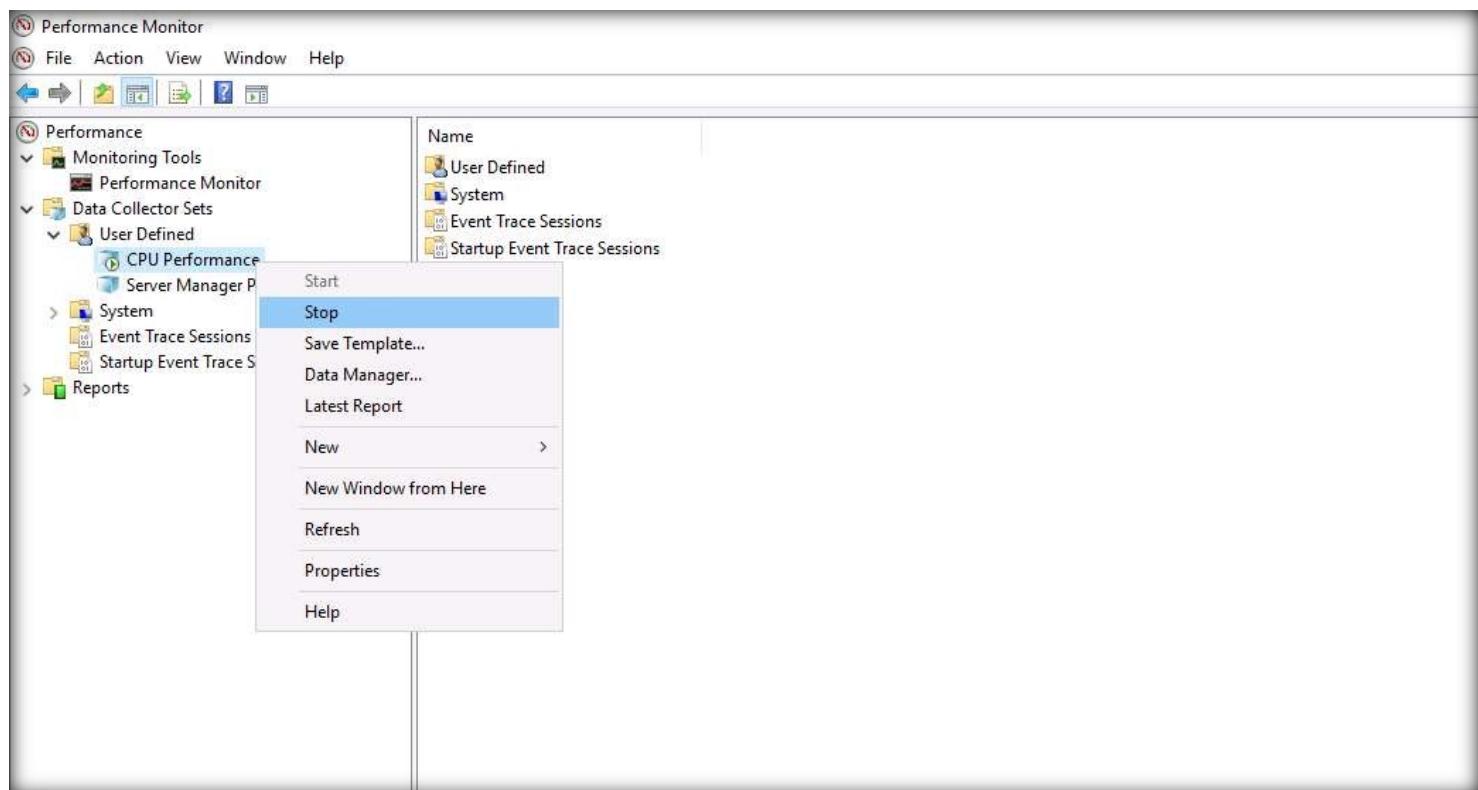
39. You can observe that the CPU utilization is back to normal levels.



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.

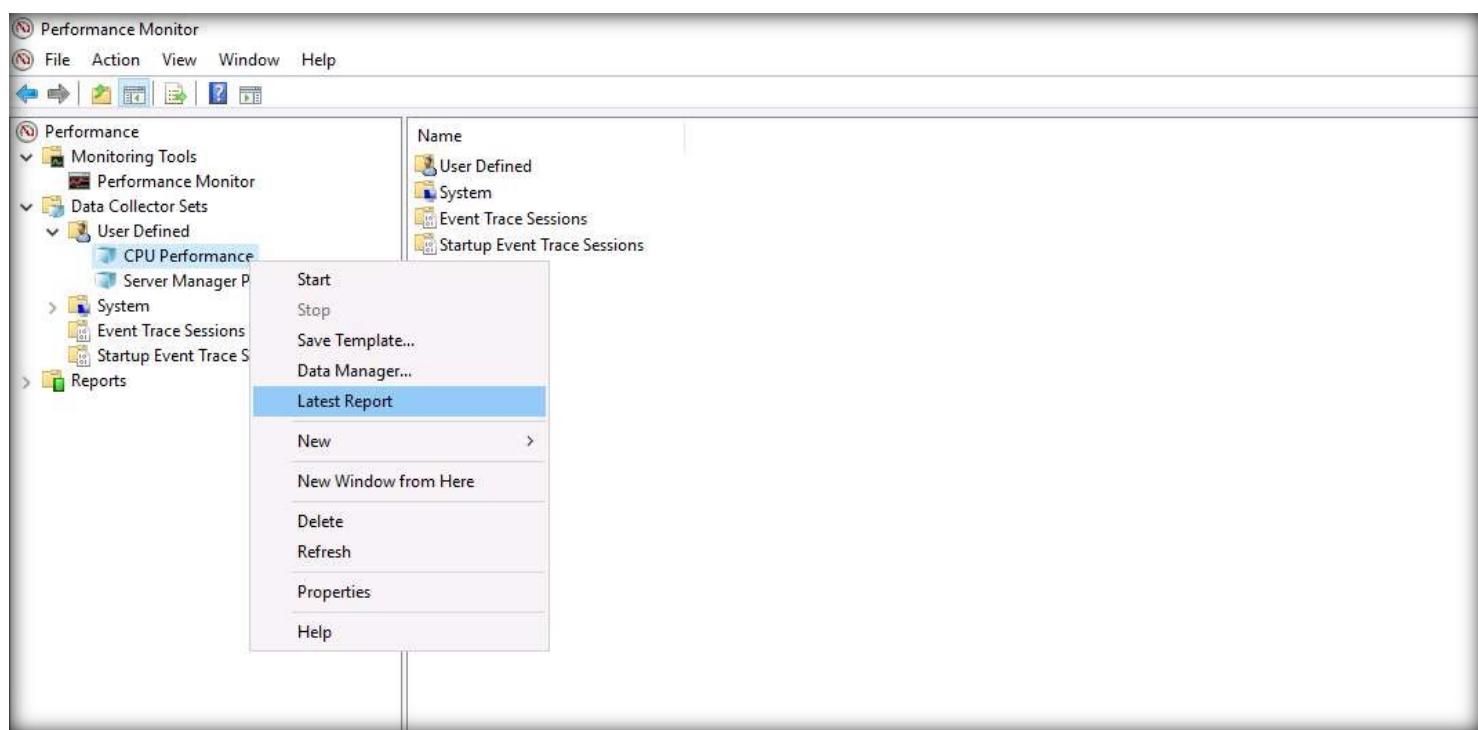
EXERCISE 6: DETERMINE APPLICATION-LEVEL ATTACKS



EXERCISE 6:

DETERMINE APPLICATION-LEVEL ATTACKS

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



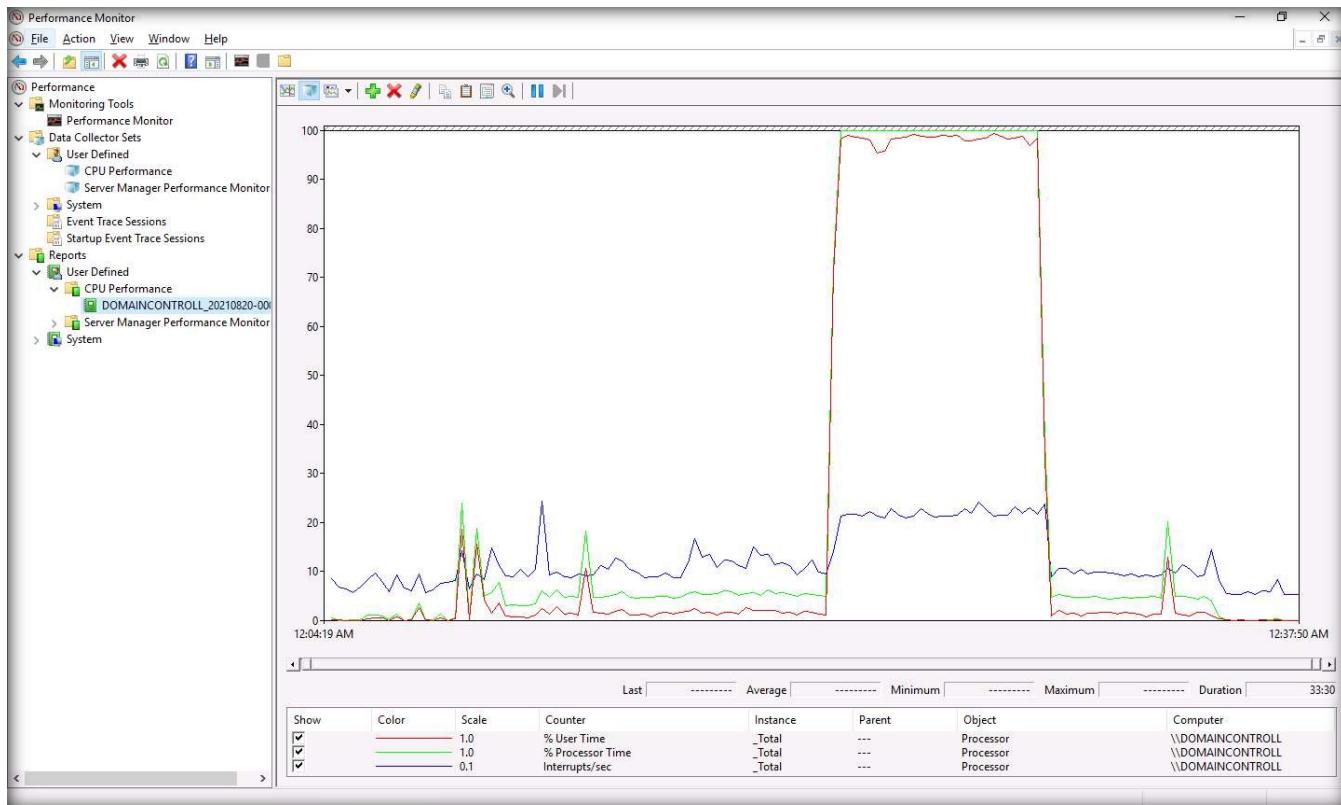
43. A graphical report appears, showing the amount of CPU utilization with respect of time, as shown in the screenshot below.
Note: The graphical report might differ when you perform the lab.

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.

EXERCISE 7:

PERFORM WEB SERVER FOOTPRINTING USING VARIOUS FOOTPRINTING TOOLS

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.

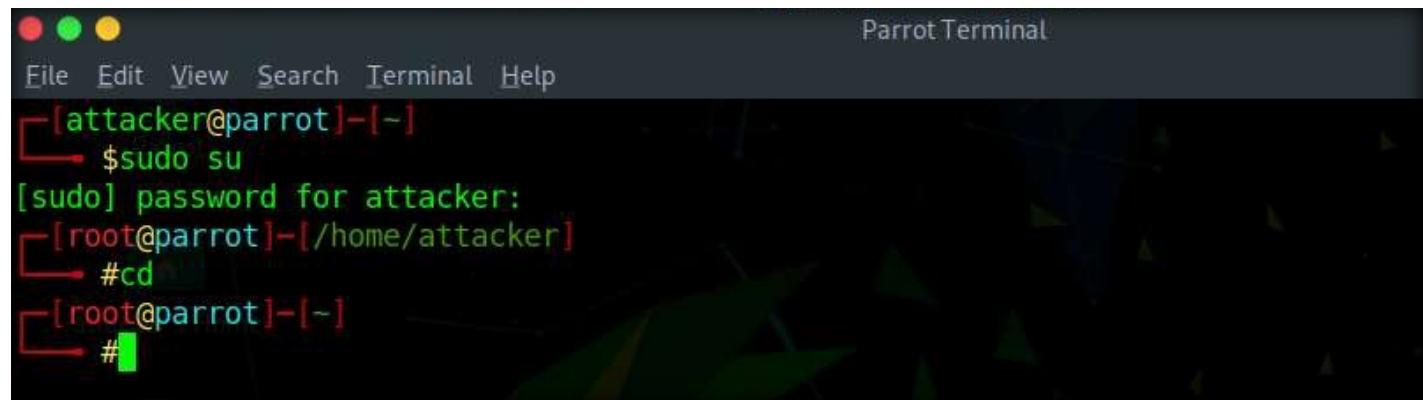
3. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.

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.



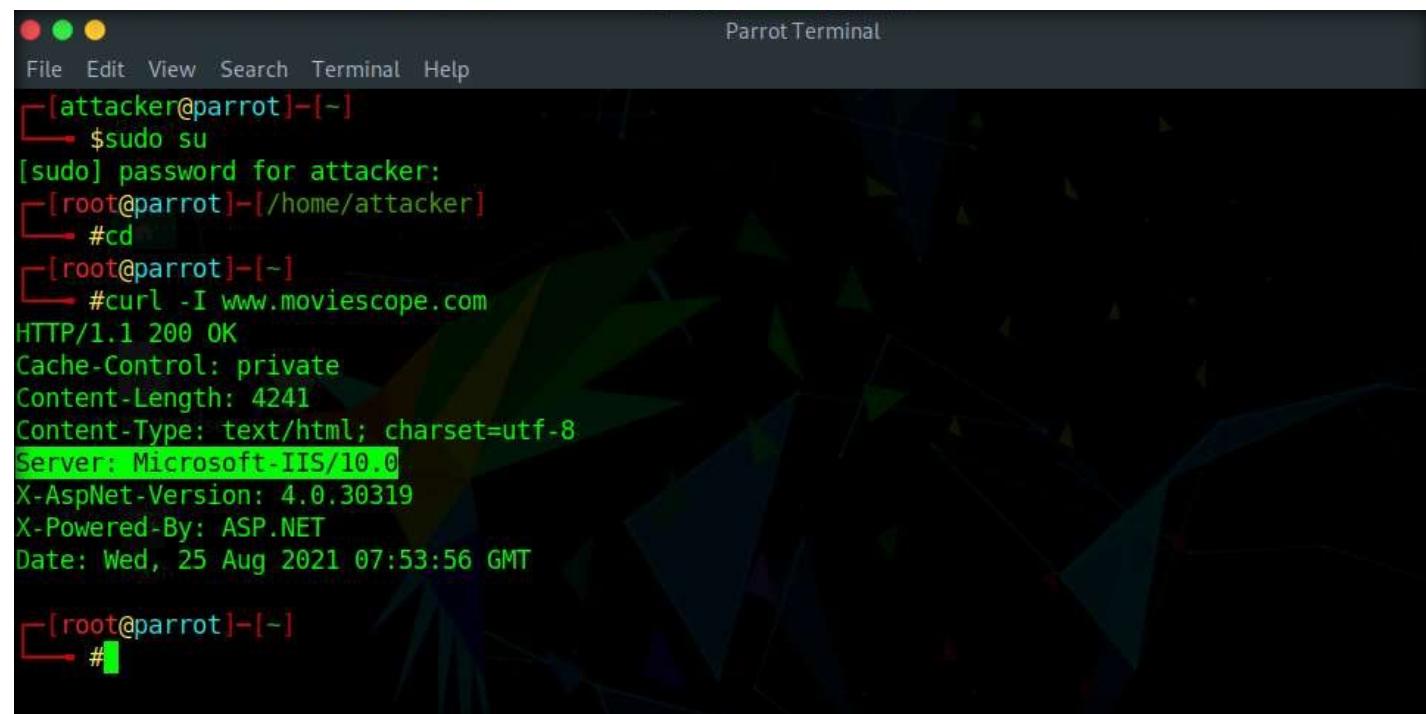
```
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~[/home/attacker]
#cd
[root@parrot] ~
#
```

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



The terminal window is titled "Parrot Terminal". The session shows the following commands and output:

```
File Edit View Search Terminal Help
[attacker@parrot]~
$ sudo su
[sudo] password for attacker:
[root@parrot]~
#cd
[root@parrot]~
#curl -I www.moviescope.com
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 4241
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 25 Aug 2021 07:53:56 GMT
[root@parrot]~
#
```

9. Type nc -vv www.moviescope.com 80 and press Enter to gather information such as server type and version.

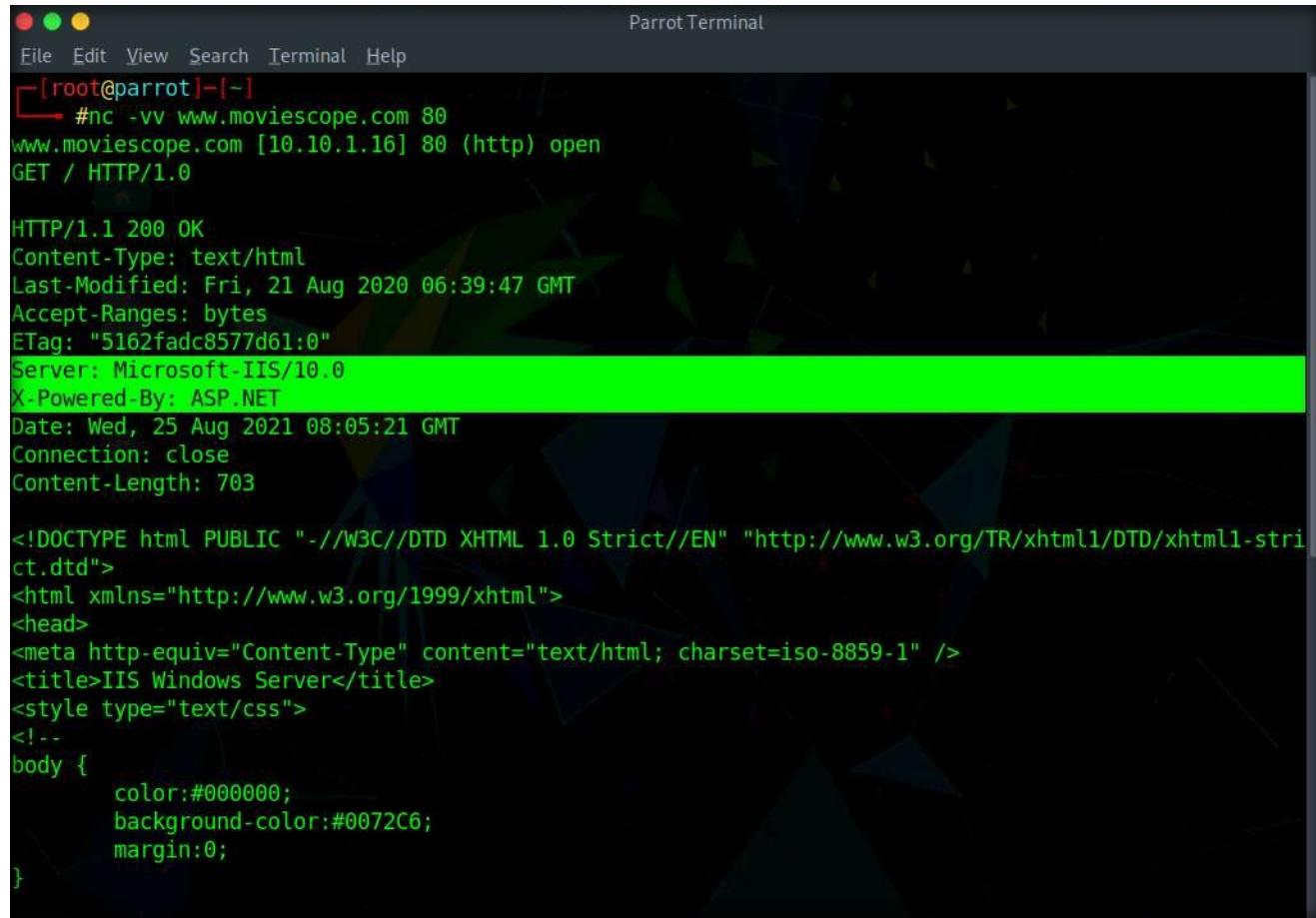
Note: -vv: Advanced verbose mode.

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



The screenshot shows a terminal window titled "Parrot Terminal". The command entered is "#nc -vv www.moviescope.com 80". The response indicates an open connection to port 80 of www.moviescope.com (10.10.1.16). The server returns an HTTP/1.1 200 OK response with headers including Content-Type: text/html, Last-Modified: Fri, 21 Aug 2020 06:39:47 GMT, Accept-Ranges: bytes, ETag: "5162fad8577d61:0", Server: Microsoft-IIS/10.0, X-Powered-By: ASP.NET, Date: Wed, 25 Aug 2021 08:05:21 GMT, Connection: close, and Content-Length: 703. The response body starts with an HTML document structure.

```
[root@parrot]~-[~]
#nc -vv www.moviescope.com 80
www.moviescope.com [10.10.1.16] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 21 Aug 2020 06:39:47 GMT
Accept-Ranges: bytes
ETag: "5162fad8577d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 25 Aug 2021 08:05:21 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}
```

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.

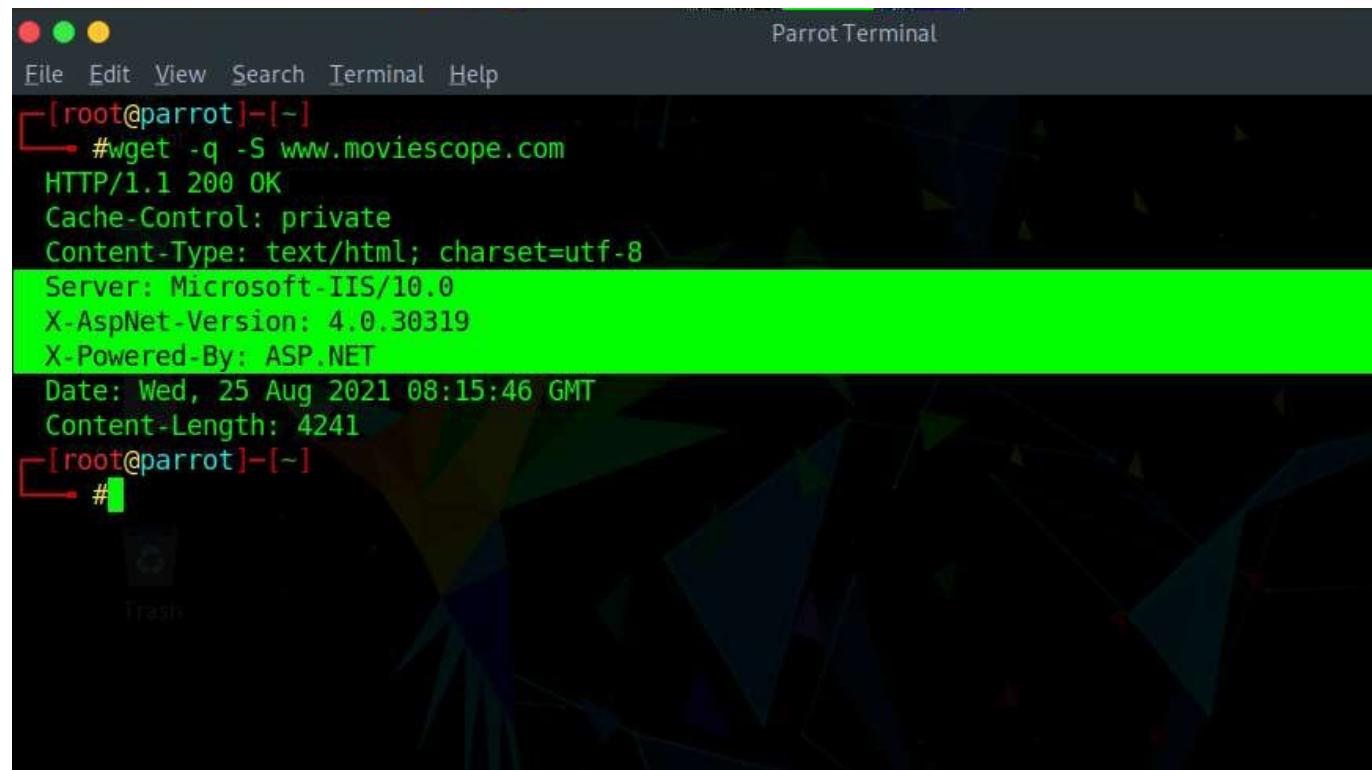
12. You can observe the HTTP information obtained, as shown in the screenshot below.

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.



```
[root@parrot] ~
[root@parrot] ~
# wget -q -S www.moviescope.com
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 25 Aug 2021 08:15:46 GMT
Content-Length: 4241
[root@parrot] ~
#
```

EC-Council

