Project:

Network-Based IDS

Haris ali

"CompTIA Security+ Certified | Cybersecurity Analyst"

Exercise:

Implement Network-based IDS Functionality using Suricata IDS

Network-based intrusion detection systems (NIDS) check every packet entering the network for the presence of anomalies and incorrect data.

Lab Scenario

A security professional must have the required knowledge to use Suricata for real-time Intrusion Detection System (IDS), inline Intrusion Prevention System (IPS), Network Security Monitoring (NSM), and offline pcap processing.

Lab Objectives

This lab will demonstrate how to use Suricata IDS. In this lab, you will also learn how to:

- Use the intrusion detection tool Suricata
- Review information in the Suricata Logs.

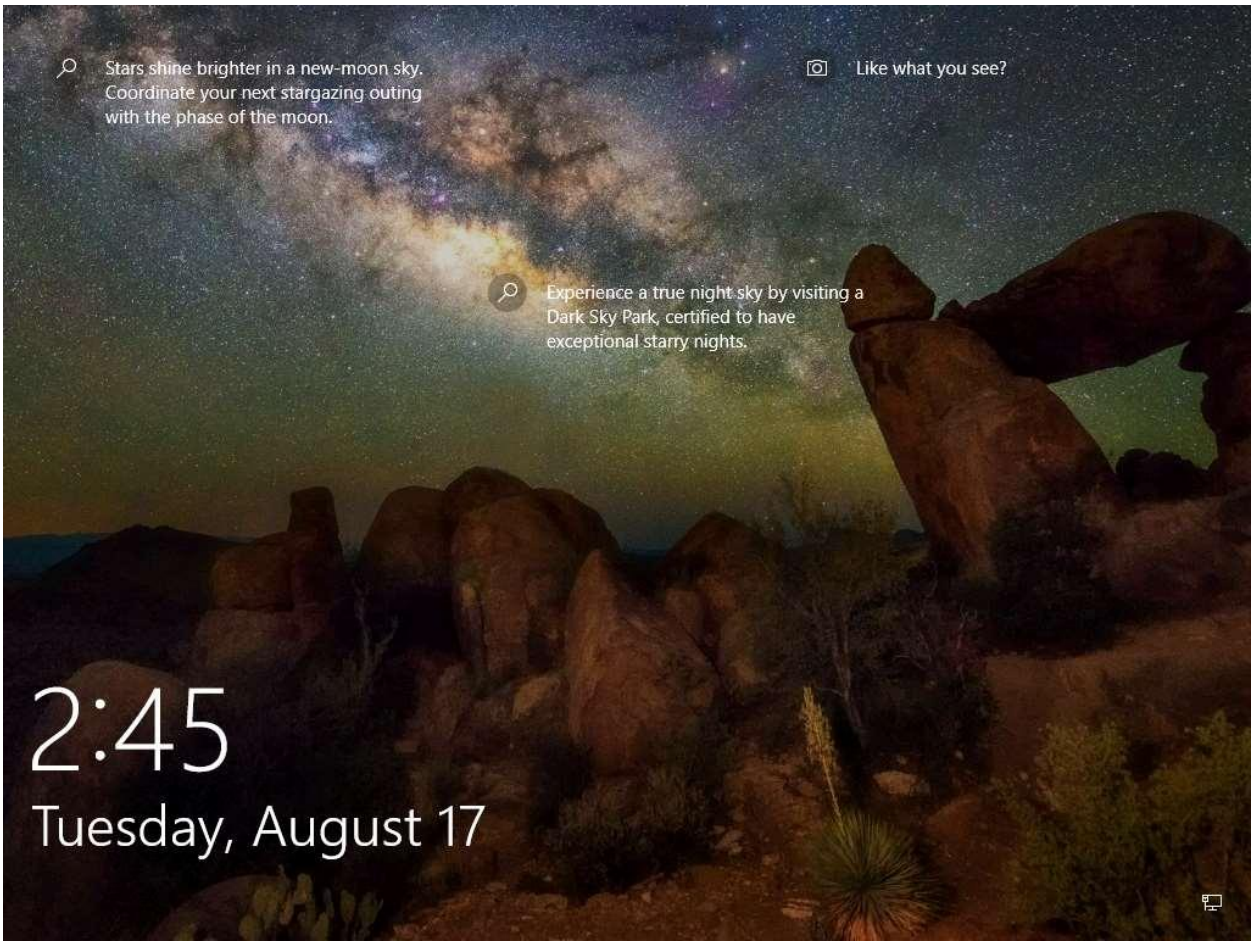
Overview of Network-based IDS

By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts at the IP or application level based on the content. NIDS are more distributed than host-based IDS. The NIDS identifies the anomalies at the router and host levels. It audits the information contained in the data packets and logs the information of malicious packets; furthermore, it assigns a threat level to each risk after receiving the data packets.

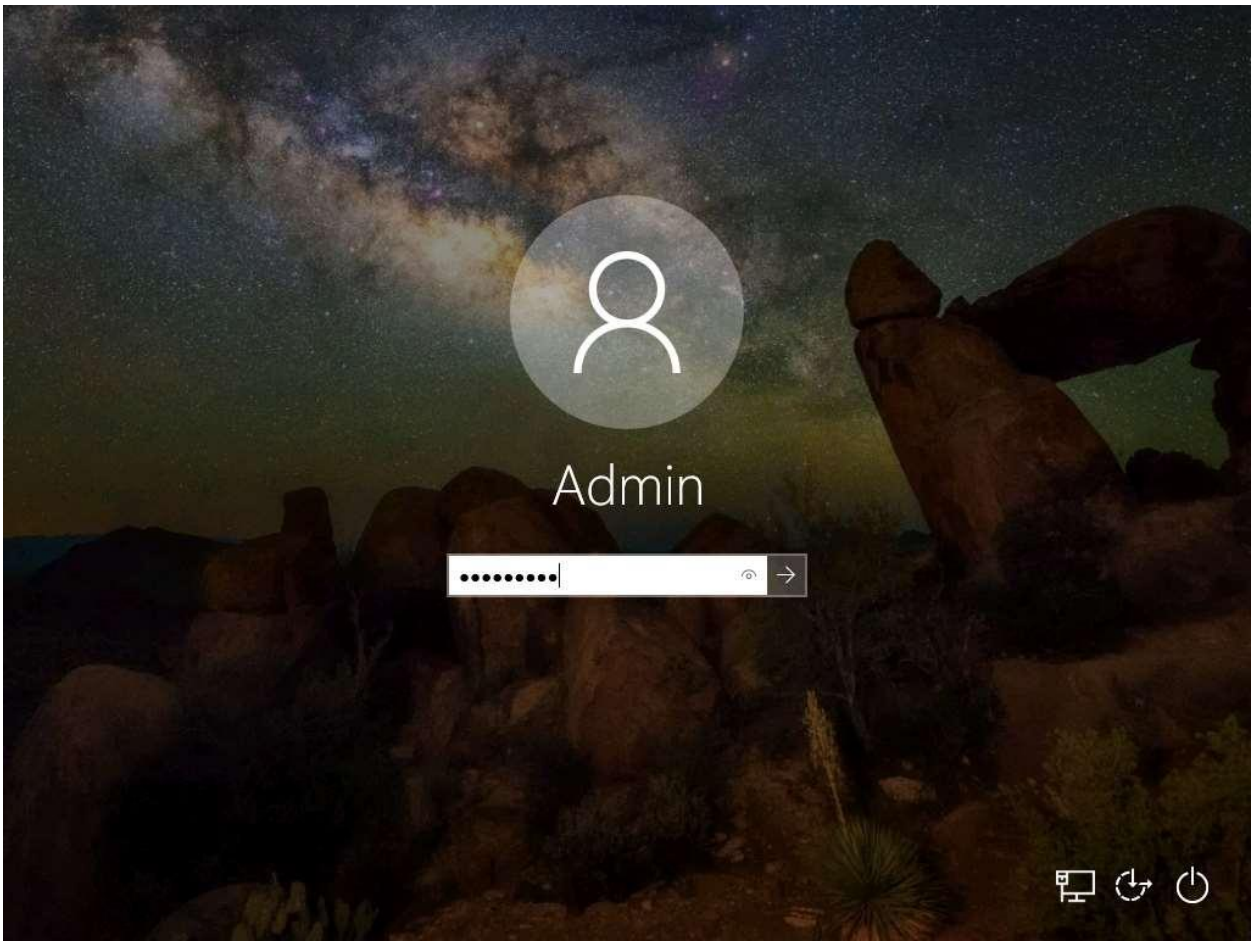
Lab Tasks

If you are already logged into the Admin Machine-1, then skip to Step#3.

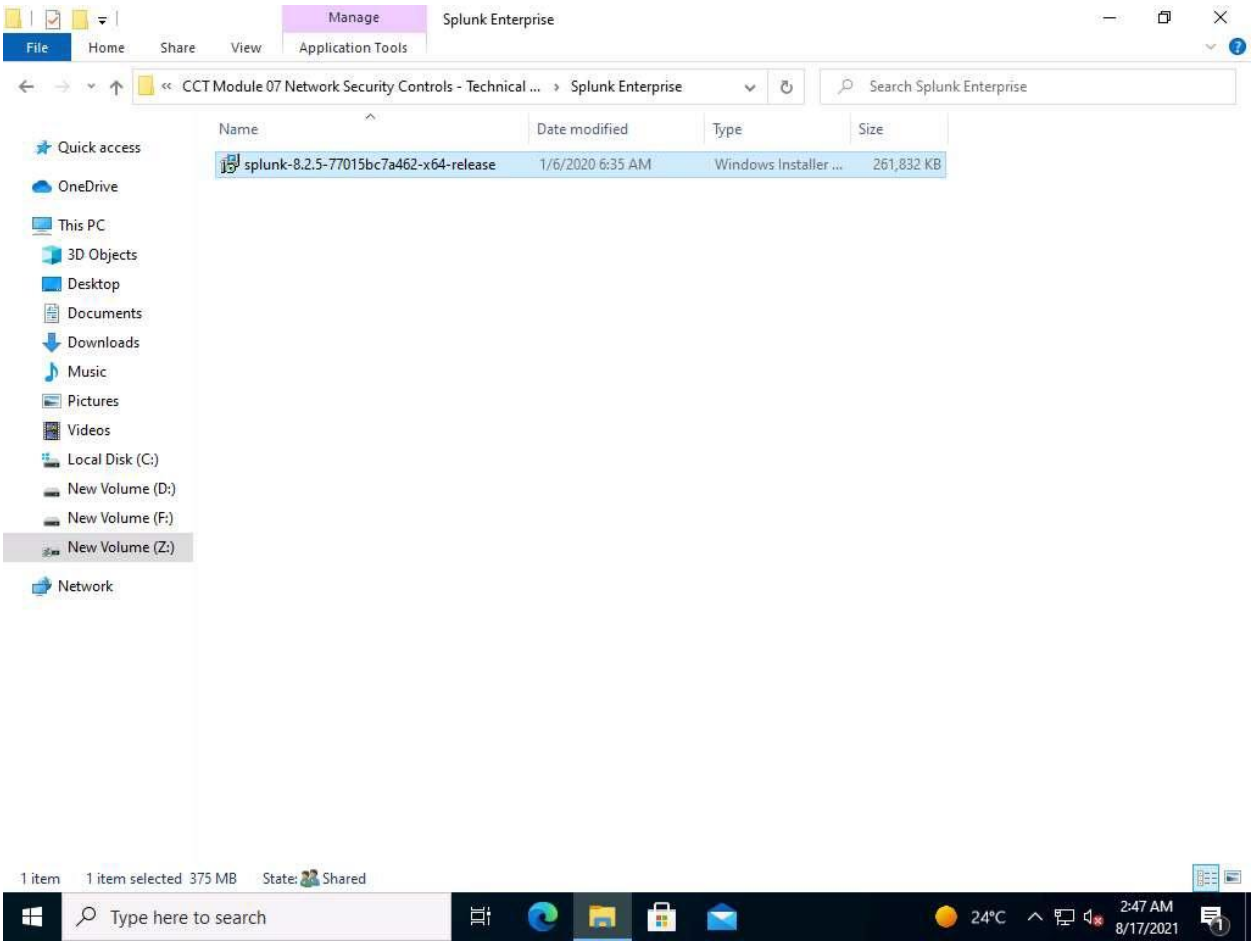
1. Click Admin Machine-1 to launch the Admin Machine-1 machine. Click Ctrl+Alt+Delete.



2. By default, the Admin account is selected, click admin@123 and press Enter to login.



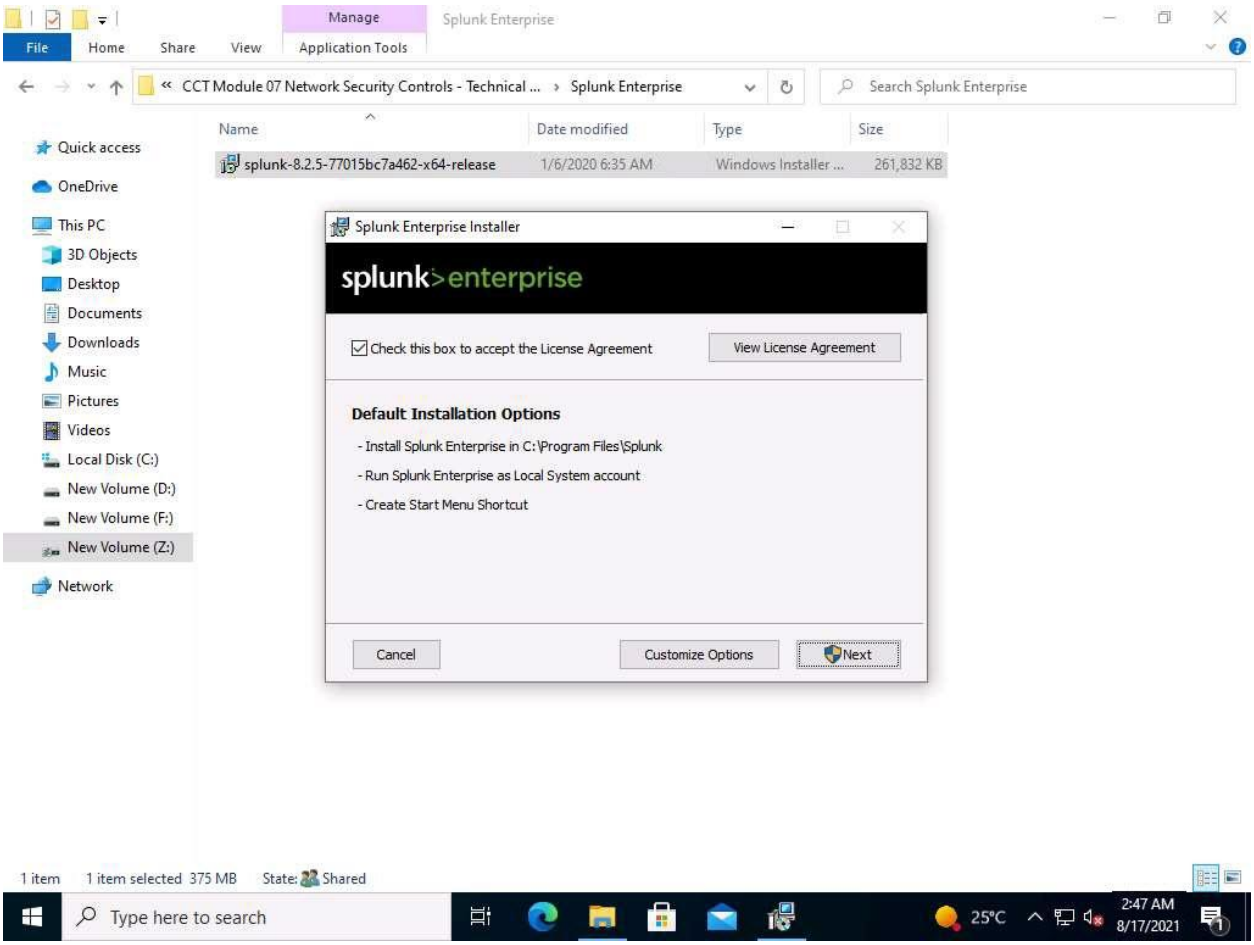
3. Next, install Splunk Enterprise SIEM, to view the captured Suricata logs in SIEM.
4. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Splunk Enterprise.



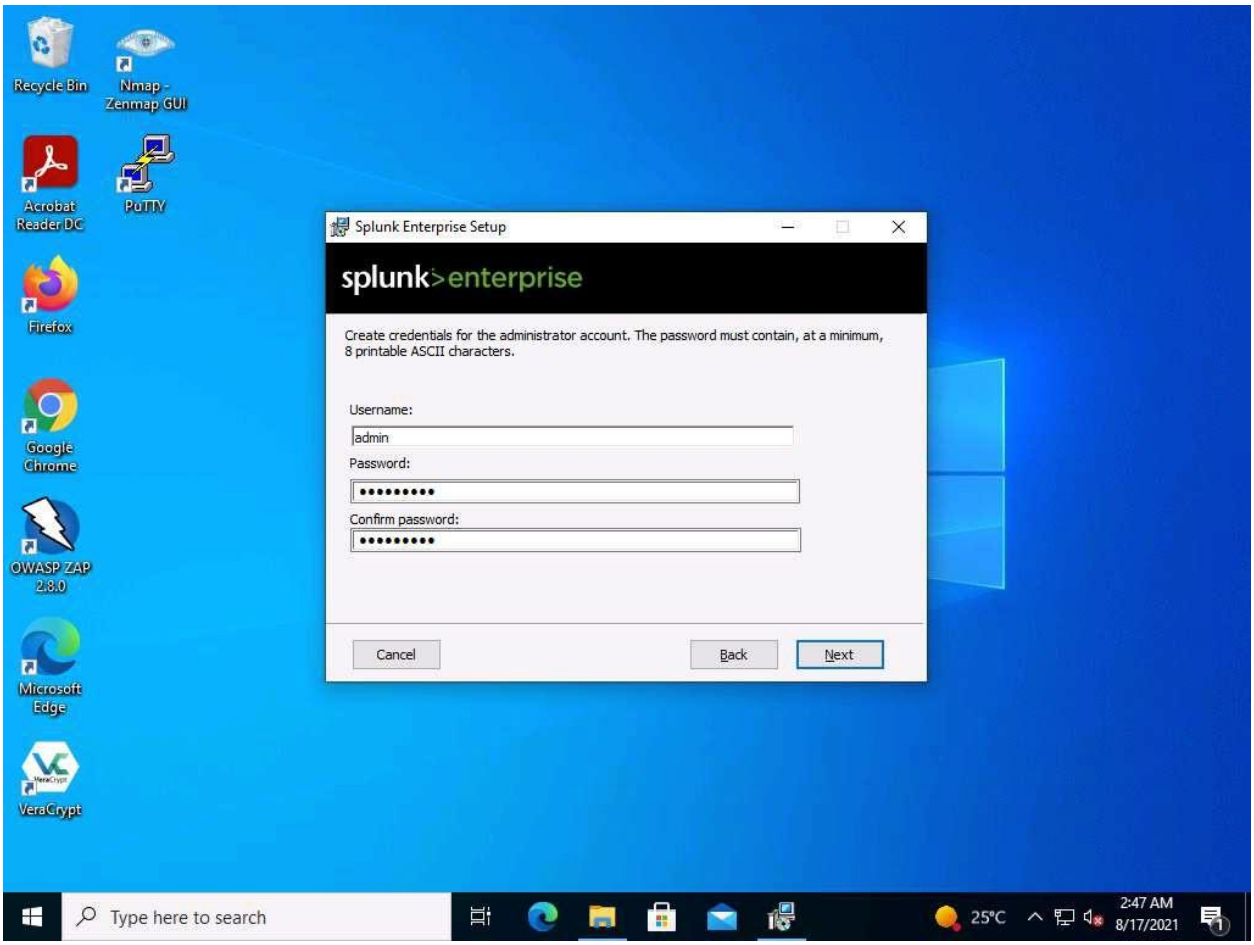
5. Double-click splunk-8.2.5-77015bc7a462-x64-release.msi to start the installation. If the Open File - Security Warning pop-up appears, click Run.

If a "SmartScreen has prevented the app from running" message appears, click More info, and then click Run anyway.

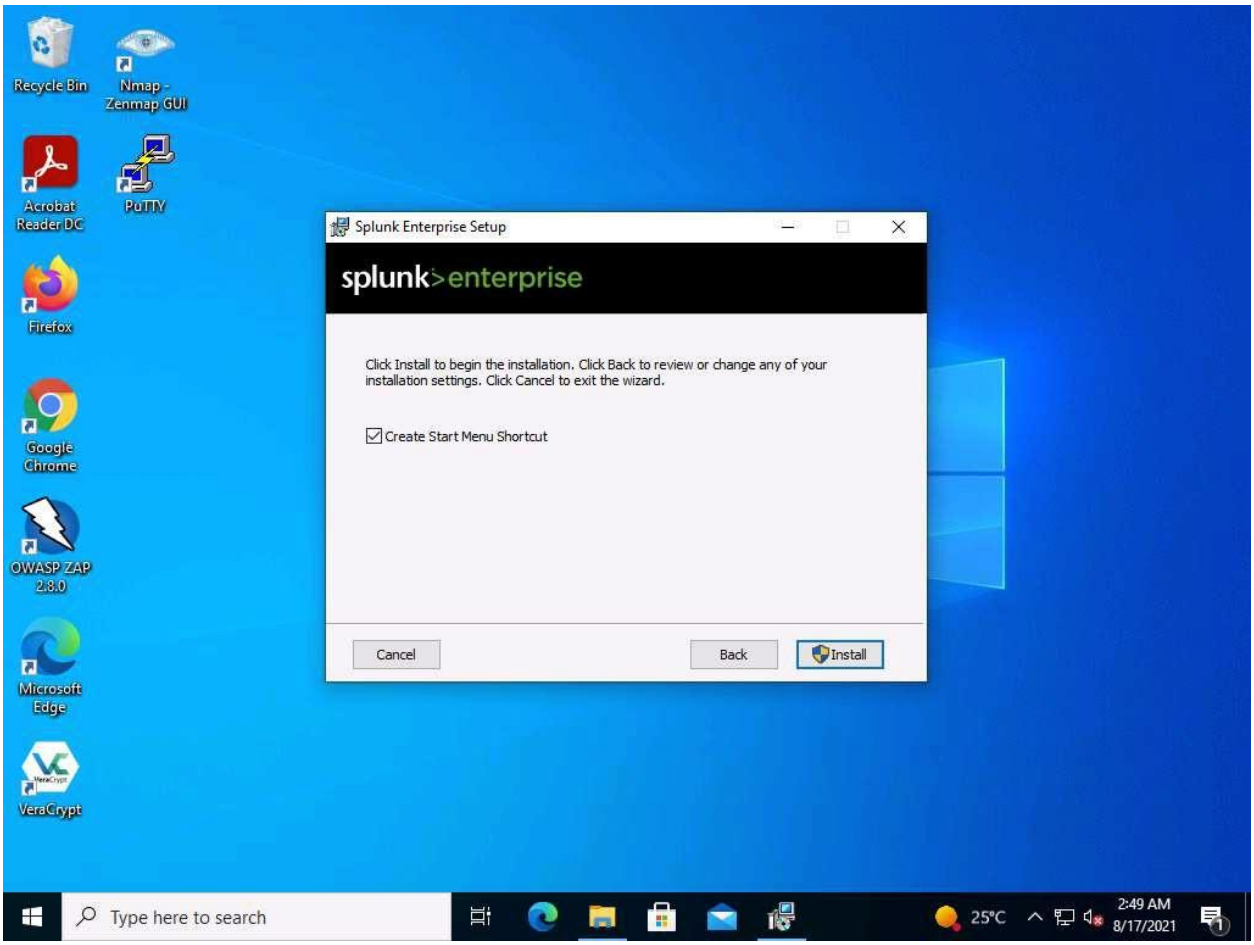
6. The Splunk Enterprise Installer window appears. Click checkbox to accept the license agreement and click Next.



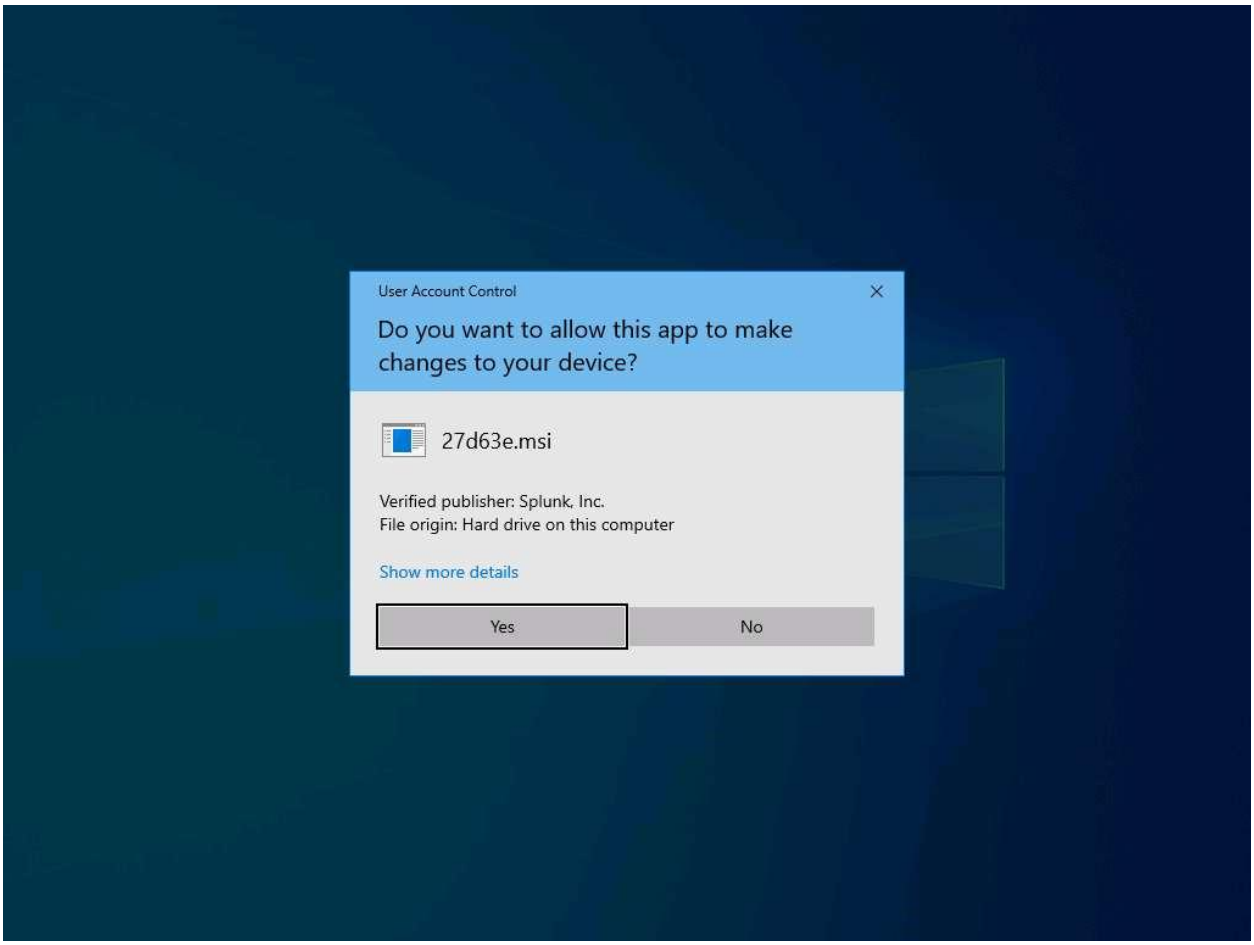
7. Enter the credential for Splunk Enterprise with username admin, password and confirm password as admin@123. Click Next.



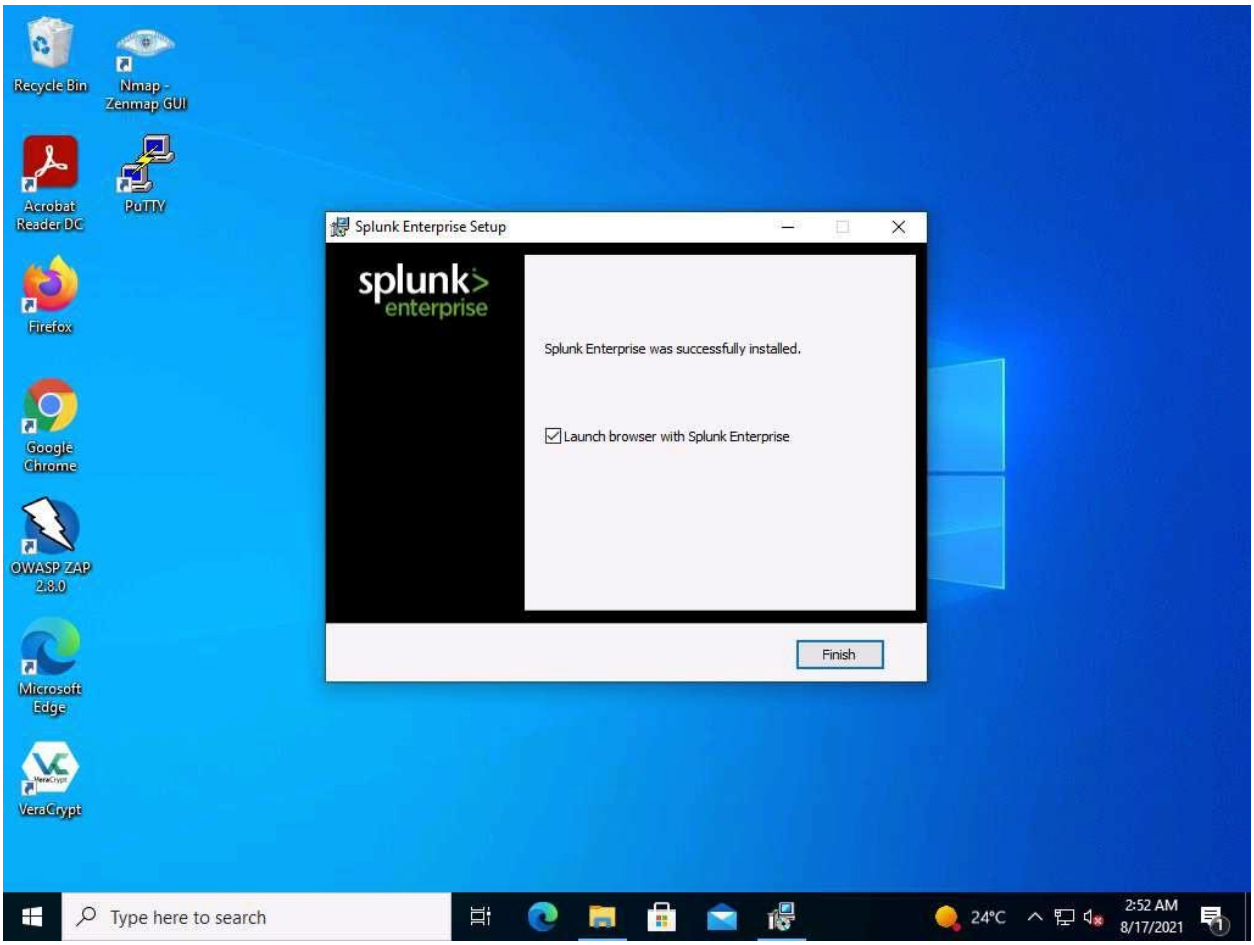
8. Click Install to install Splunk Enterprise.



9. The User Account Control pop-up window appears; click Yes to continue.

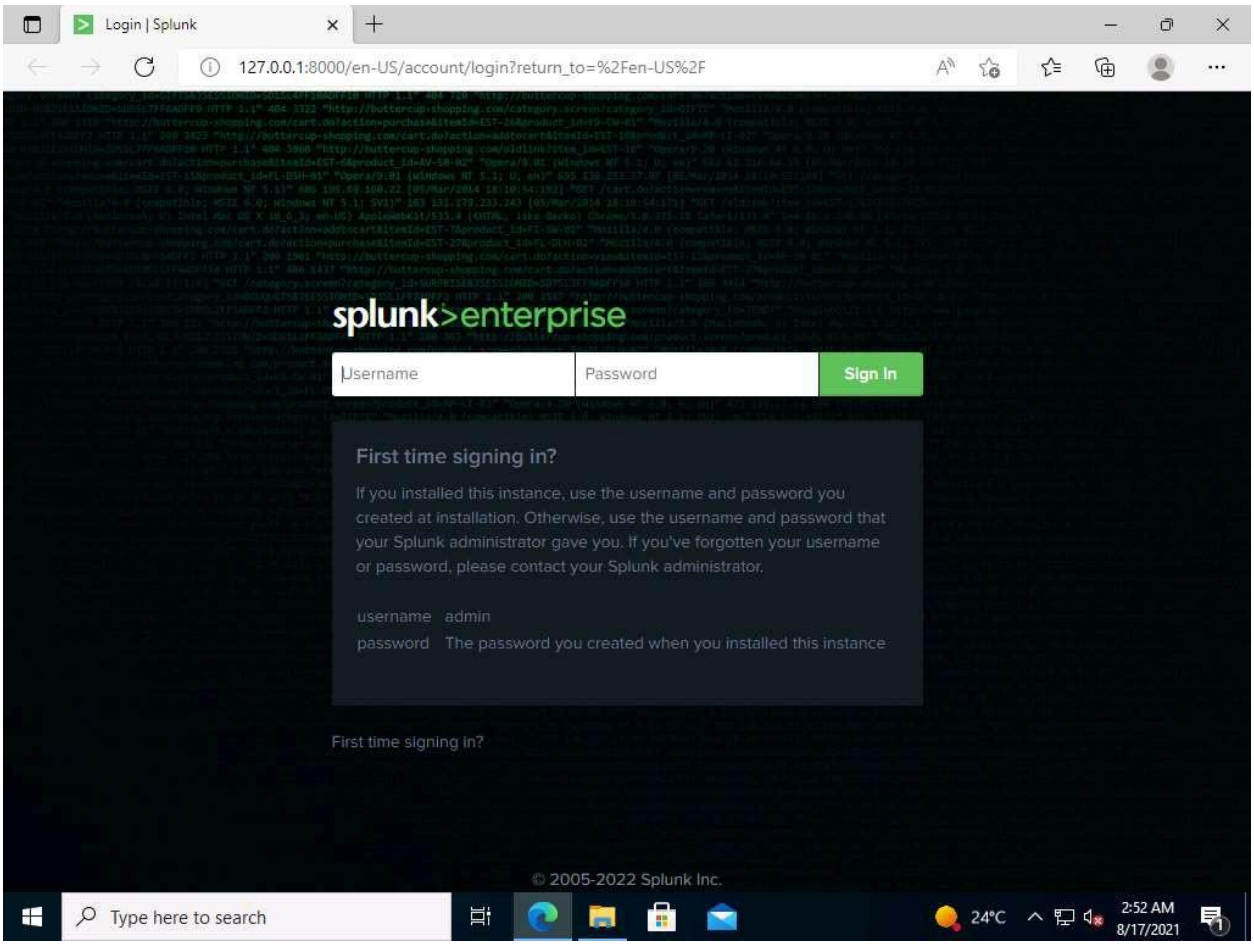


10. Wait for the installation to complete. Click Finish to complete the Splunk Enterprise setup.



11. Splunk Enterprise launches in your default browser.

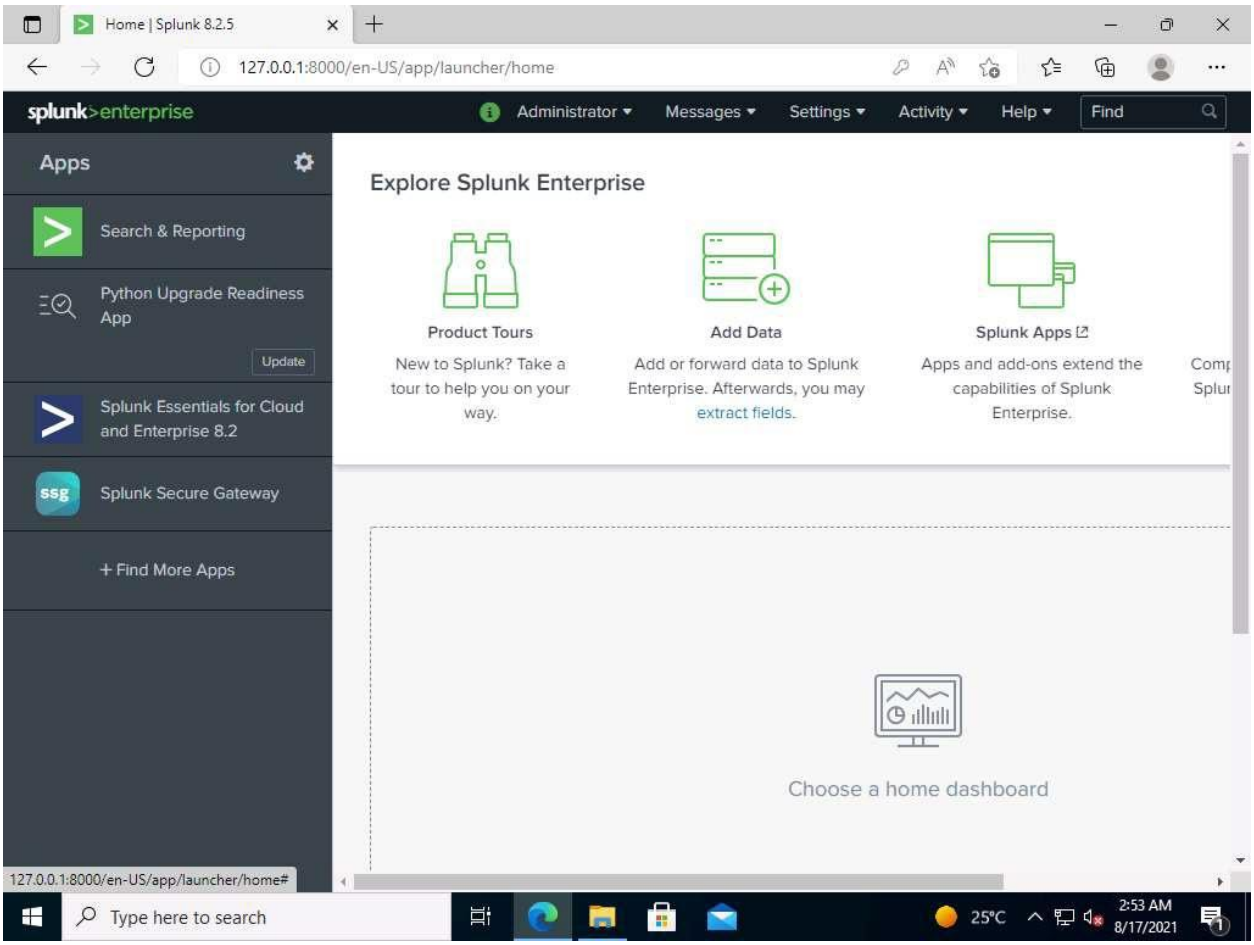
12. The First time signing in? page appears. Enter the username (admin) and password (provided while installation as admin@123) in their respective fields and click Sign In.



13. You will be successfully logged in to Splunk Enterprise.

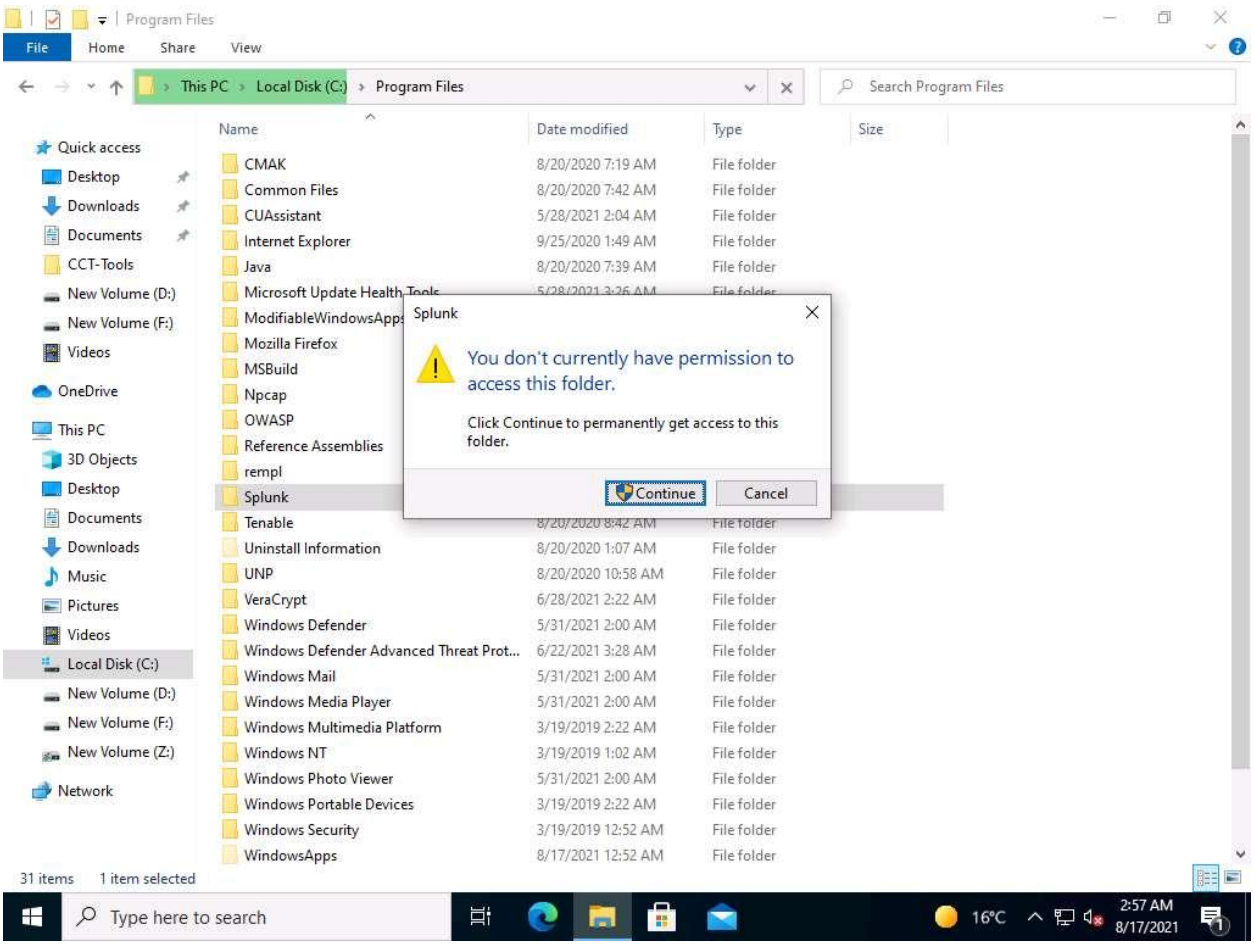
If Helping You Get More Value from Splunk Software window appears, click on Got it!, in Important changes coming! window click on Don't show me this again.

If Save password pop-up appears, click on Never.



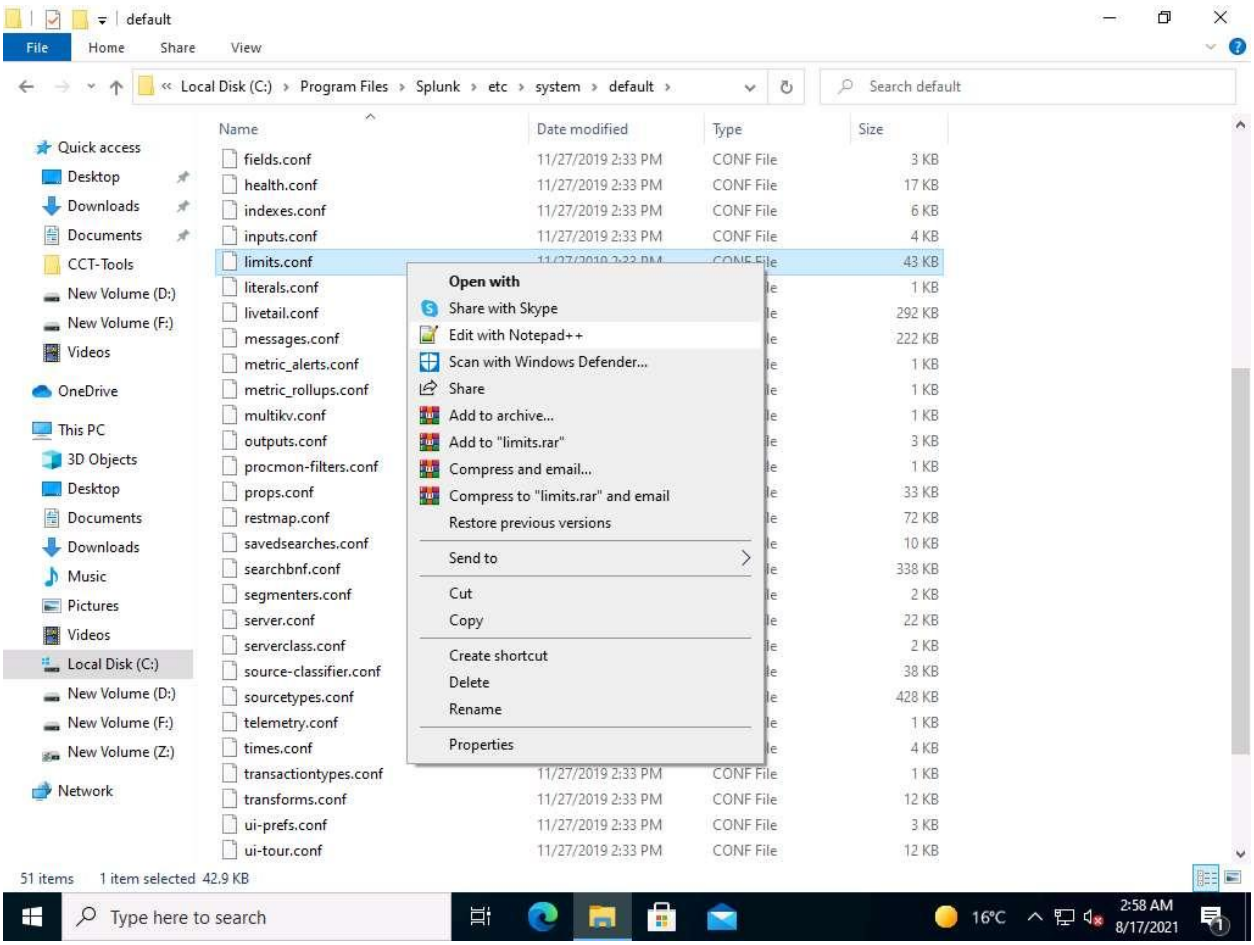
14. Close the browser, to increase the default maximum number of concurrent of searches per CUP in Splunk Enterprise, navigate to C:\Program Files\Splunk\etc\system\default.

15. If the permission alert window opens, click Continue to access the Splunk folder.

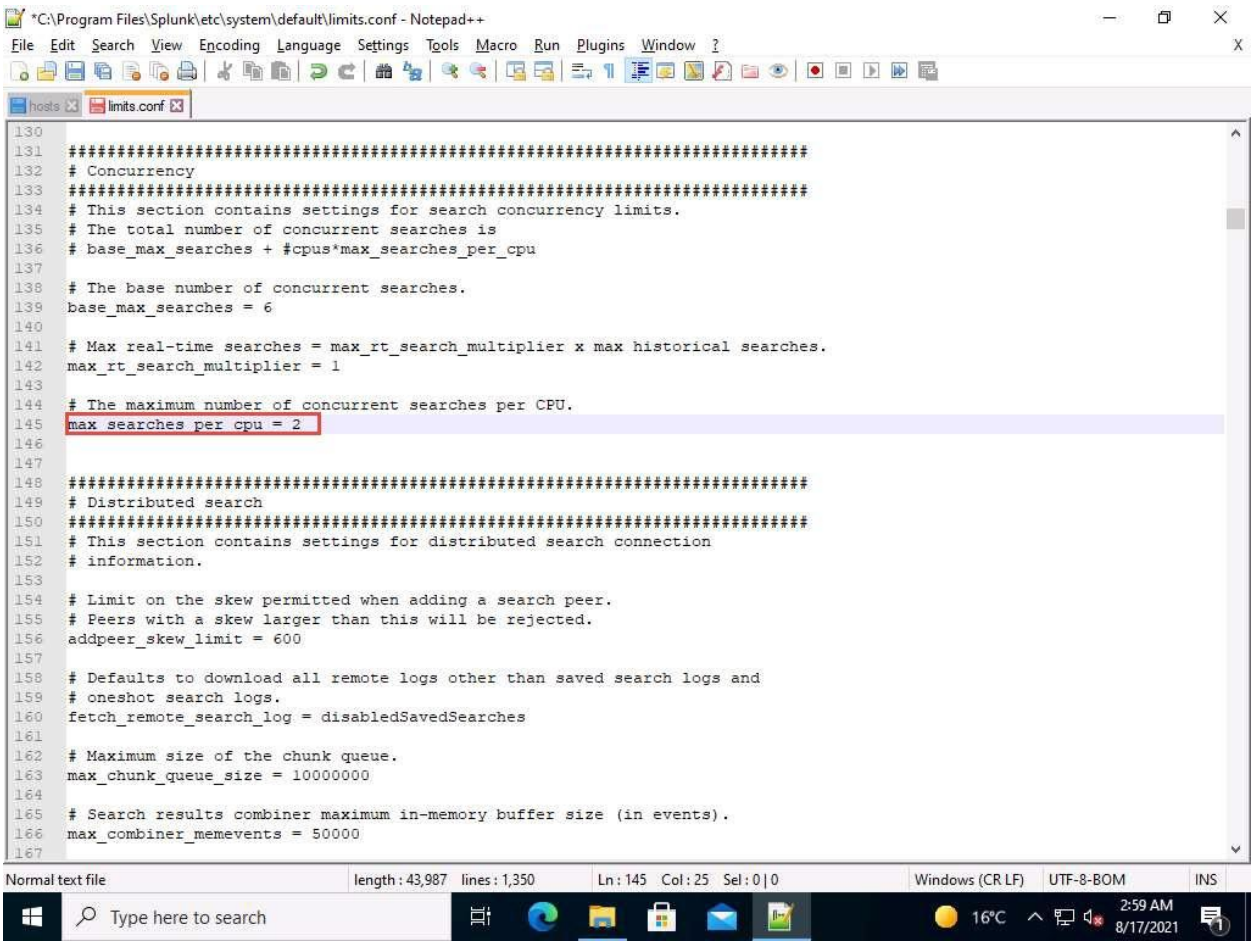


16. Open limits.conf with Notepad++.

If the Notepad++ update pop-up appears click No.



17. Go to line number 145 and set max_searches_per_cpu=2; click save and close the file.



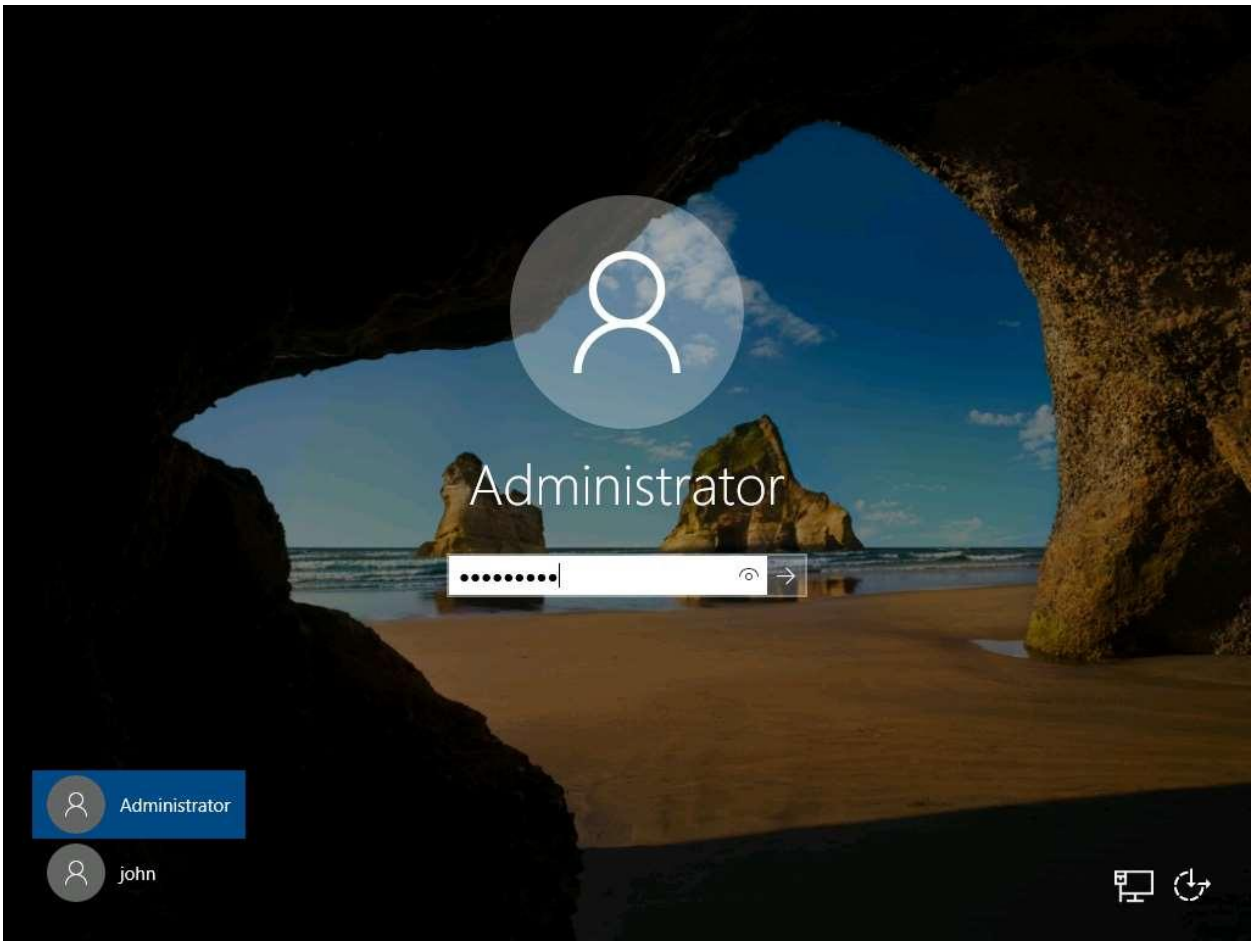
18. Restart the Admin Machine-1

19. The Suricata IDS configuration needs to be on the web server; therefore, we need to configure the Suricata IDS on Web Server.

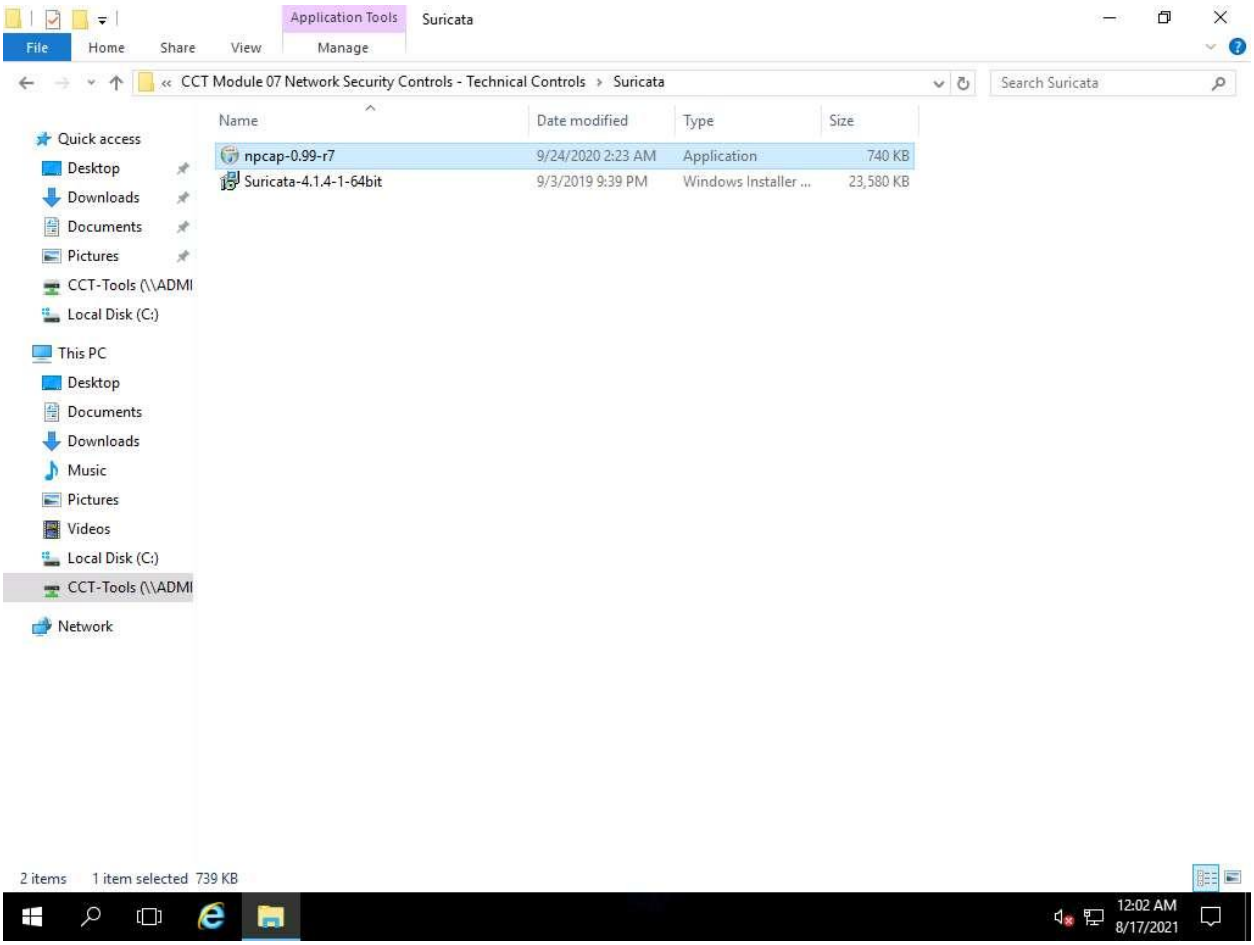
20. Click Web Server to switch to the Web Server machine. Click Ctrl+Alt+Delete link to log in.

If you are already logged into the Web Server machine, then skip to Step#22.

21. By default, the Administrator user is selected type password as admin@123 and press Enter.



22. Navigate to Z:\CCT Module 07 Network Security Controls - Technical Controls\Suricata and copy npcap-0.99-r7.exe



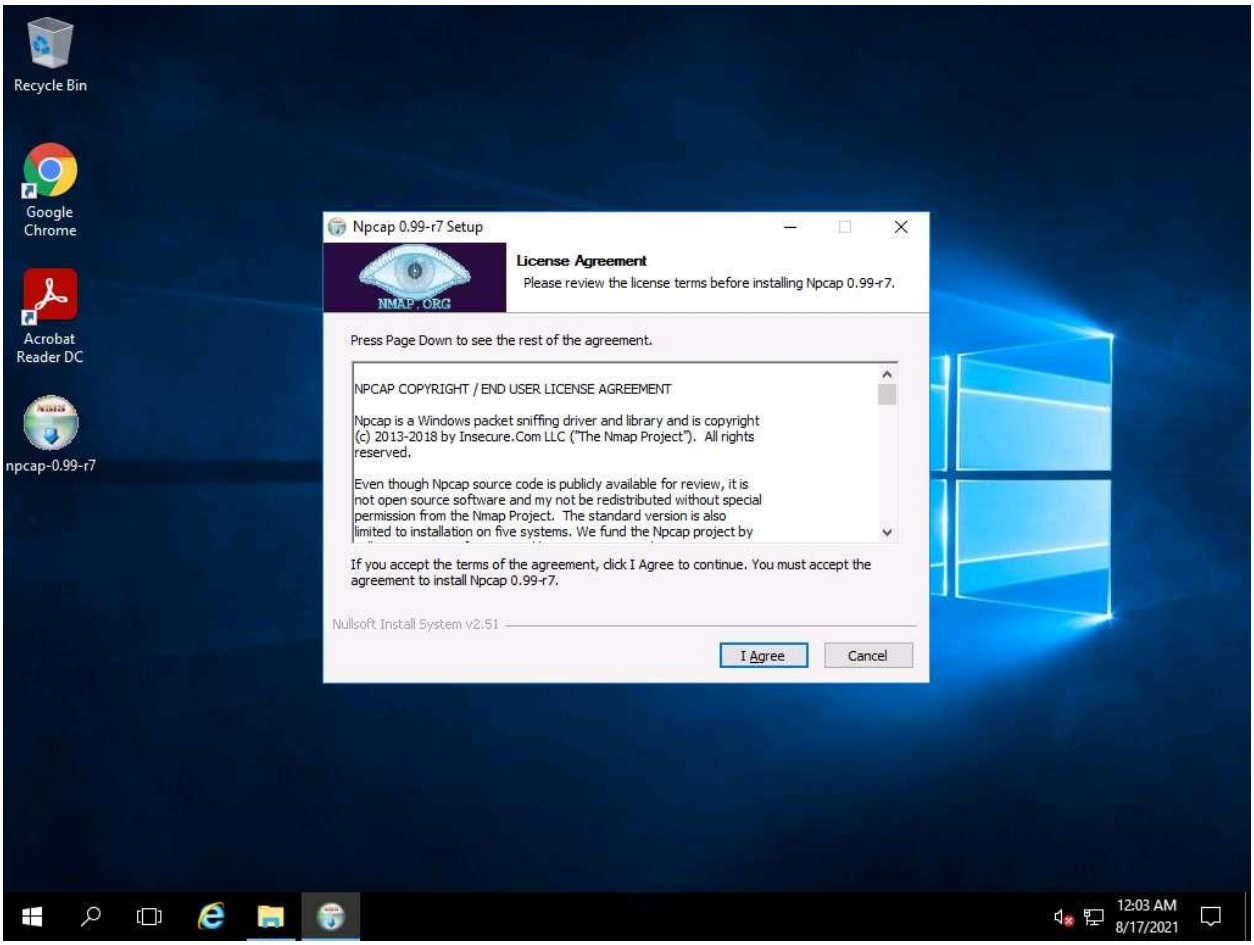
23. Paste the npcap-0.99-r7.exe file on the Desktop.

24. Npcap is a tool used for network packet capturing and injection library for Windows.

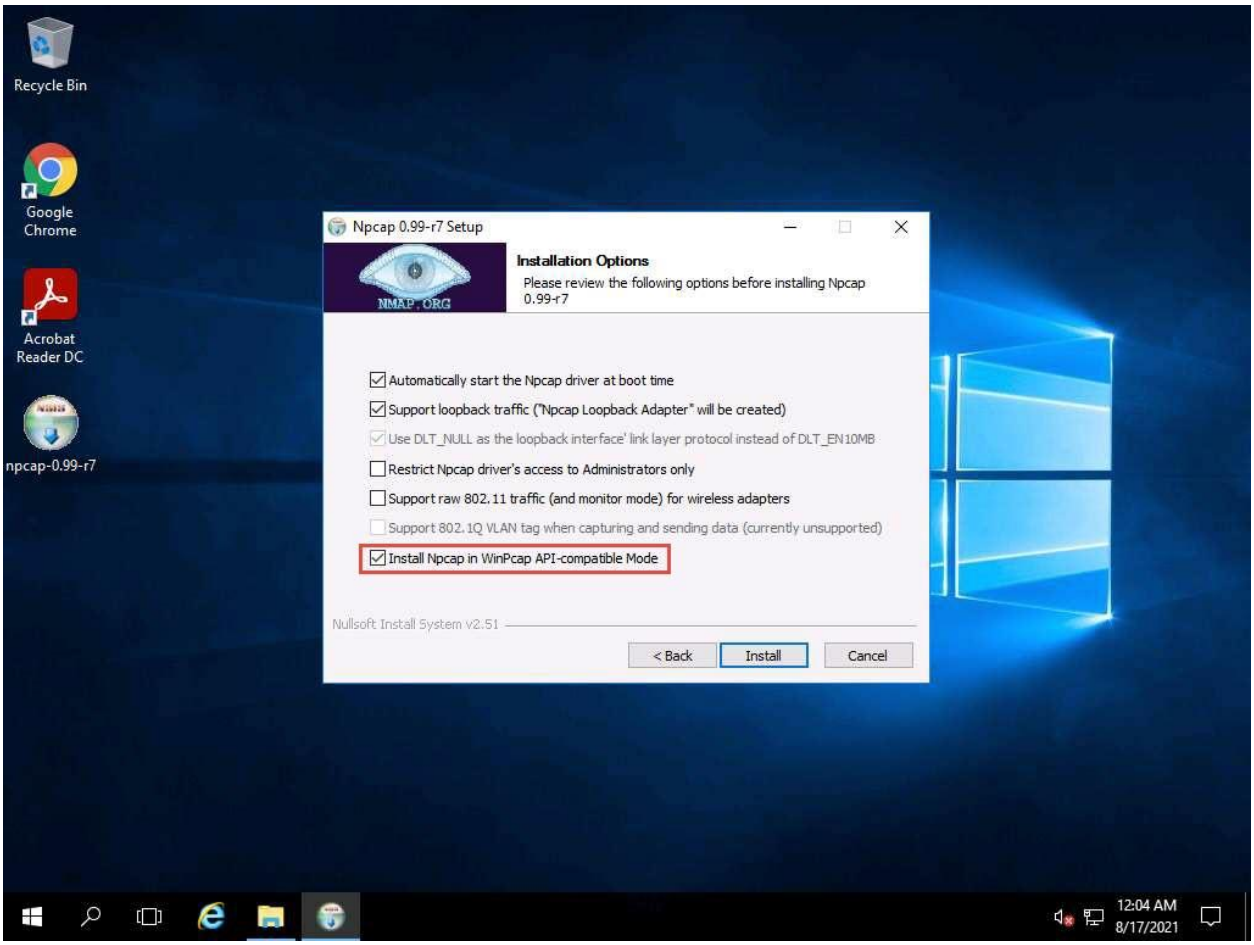
25. Suricata uses npcap for capturing network packets and alerts. The following steps demonstrate the installation of the npcap tool.

26. Double click on npcap-0.99-r7.exe. Click on I Agree to continue the installation.

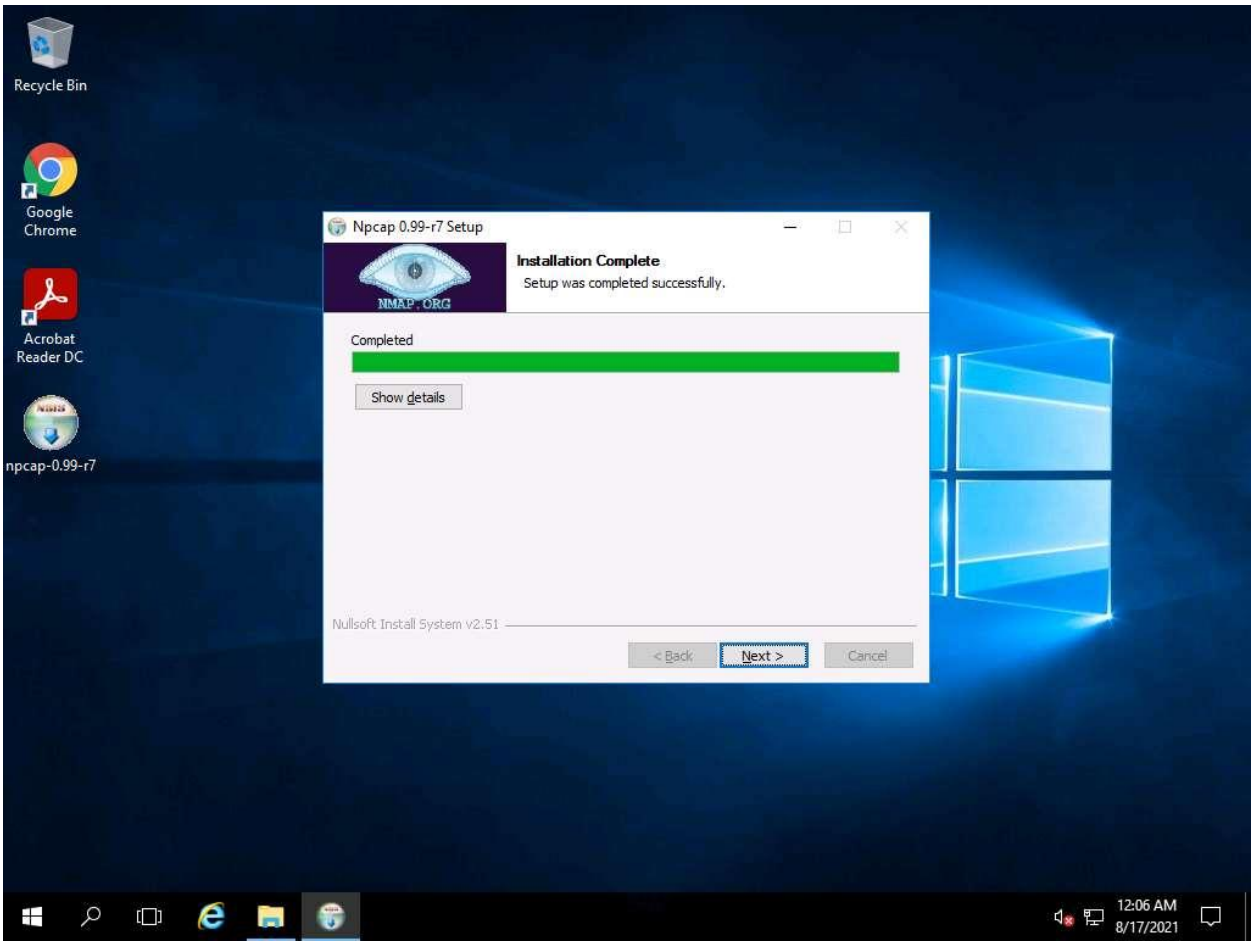
If the Security Warning pop-up appears, click Run.



27. Check Install Npcap in WinPcap API-compatible Mode, and click Install.

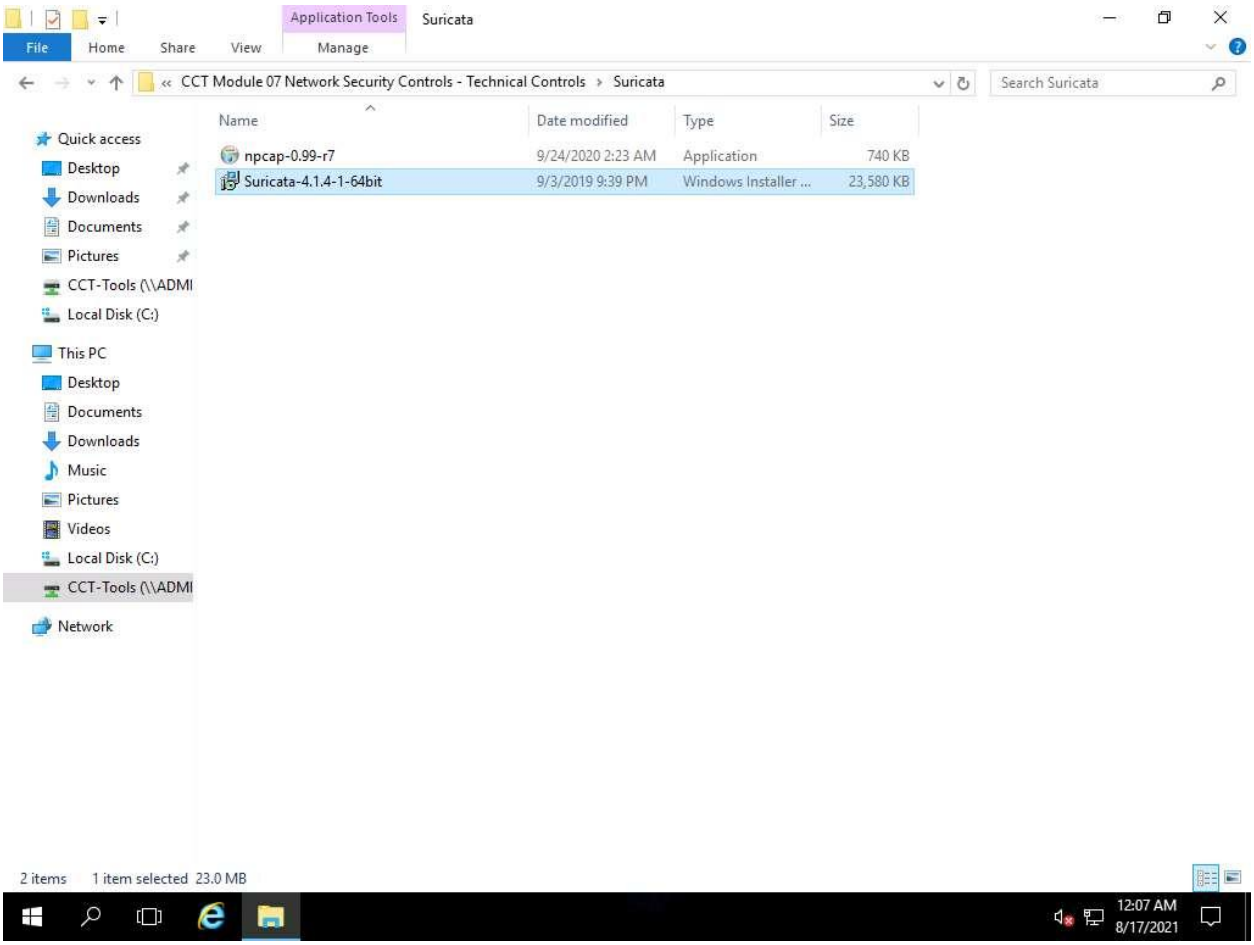


28. The installation will start in a few seconds. Once the installation is completed successfully, click Next to continue.



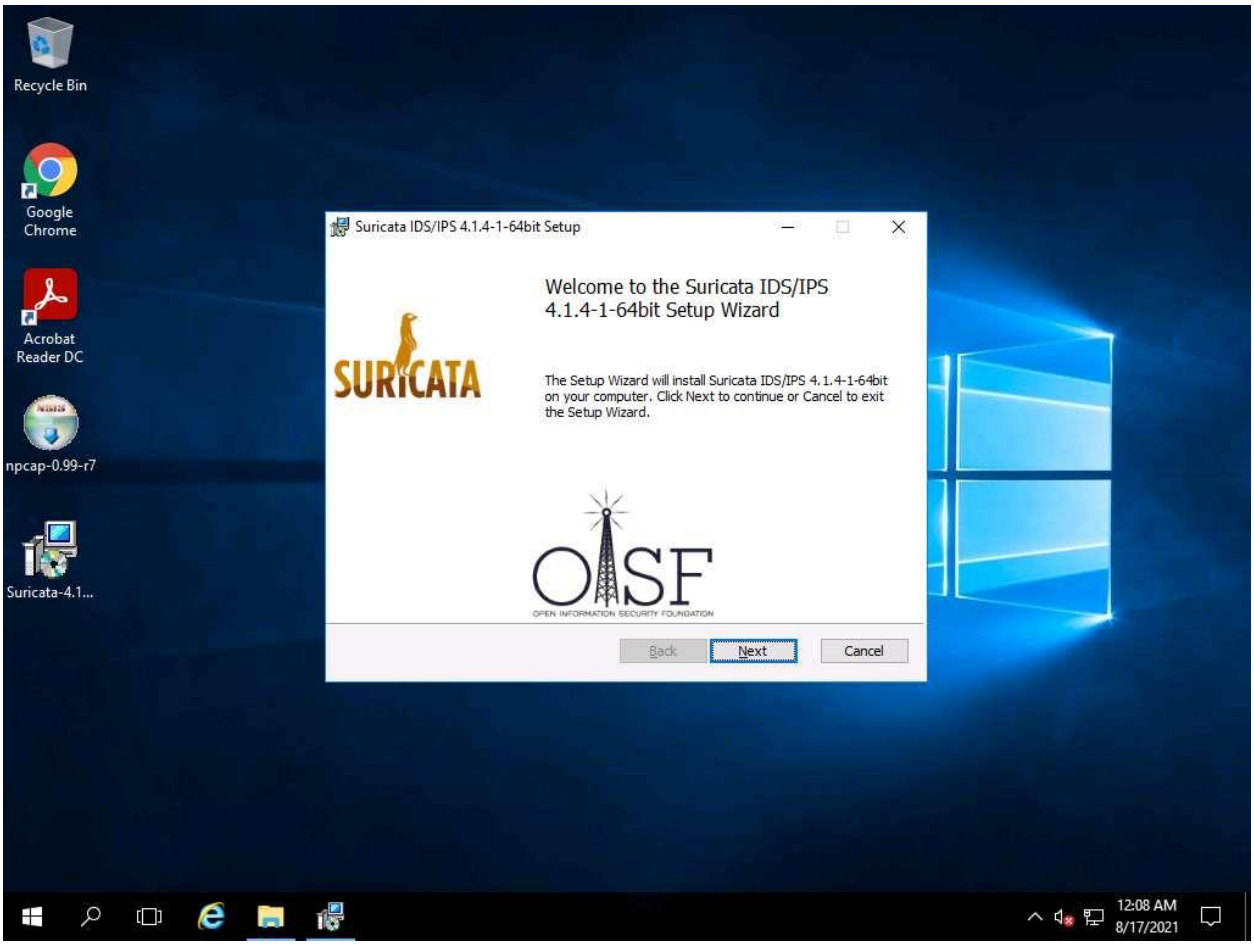
29. Click Finish to complete the installation.

30. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Suricata and copy Suricata-4.1.4-1-64bit.msi

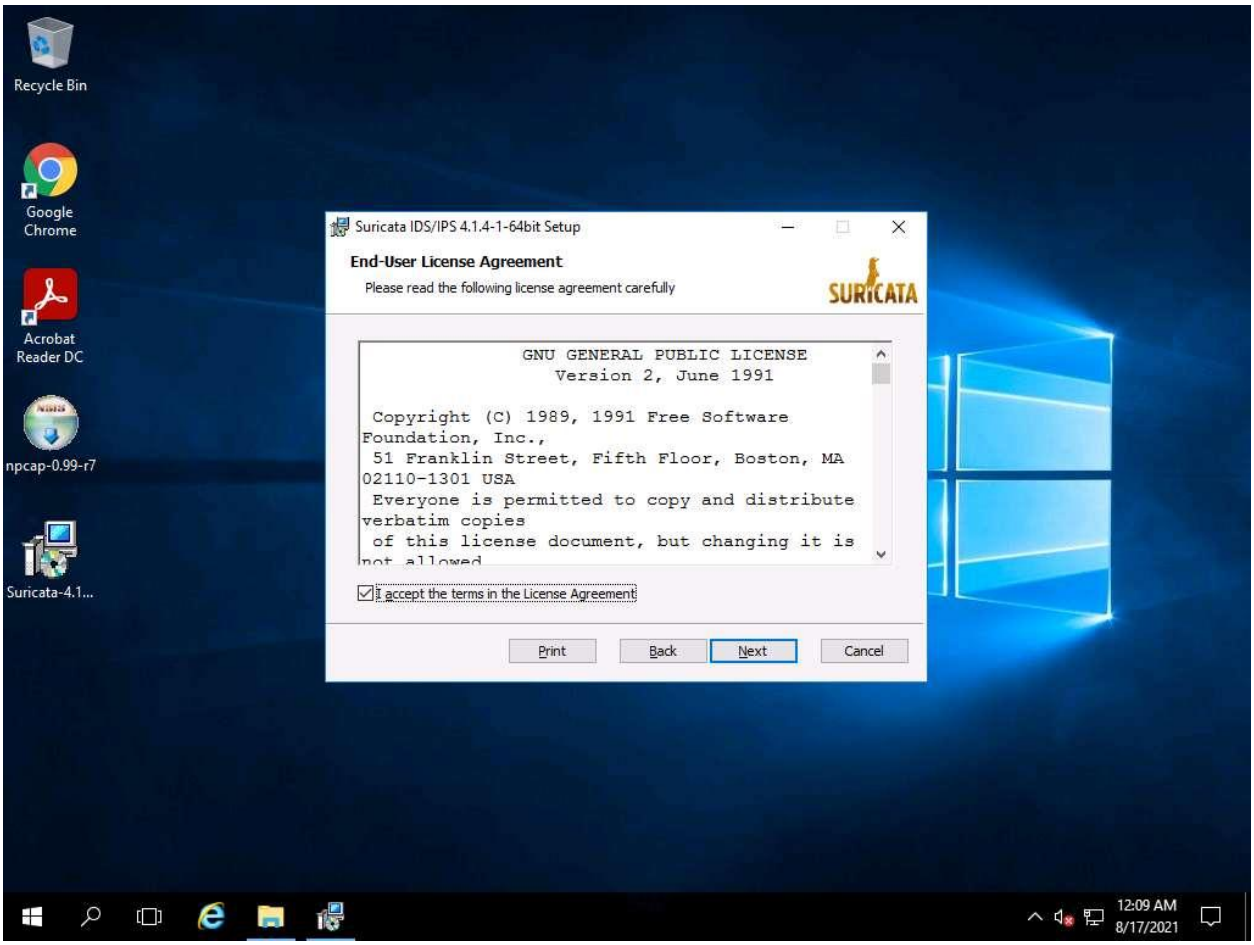


31. Paste the Suricata-4.1.4-1-64bit.msi file on the desktop.

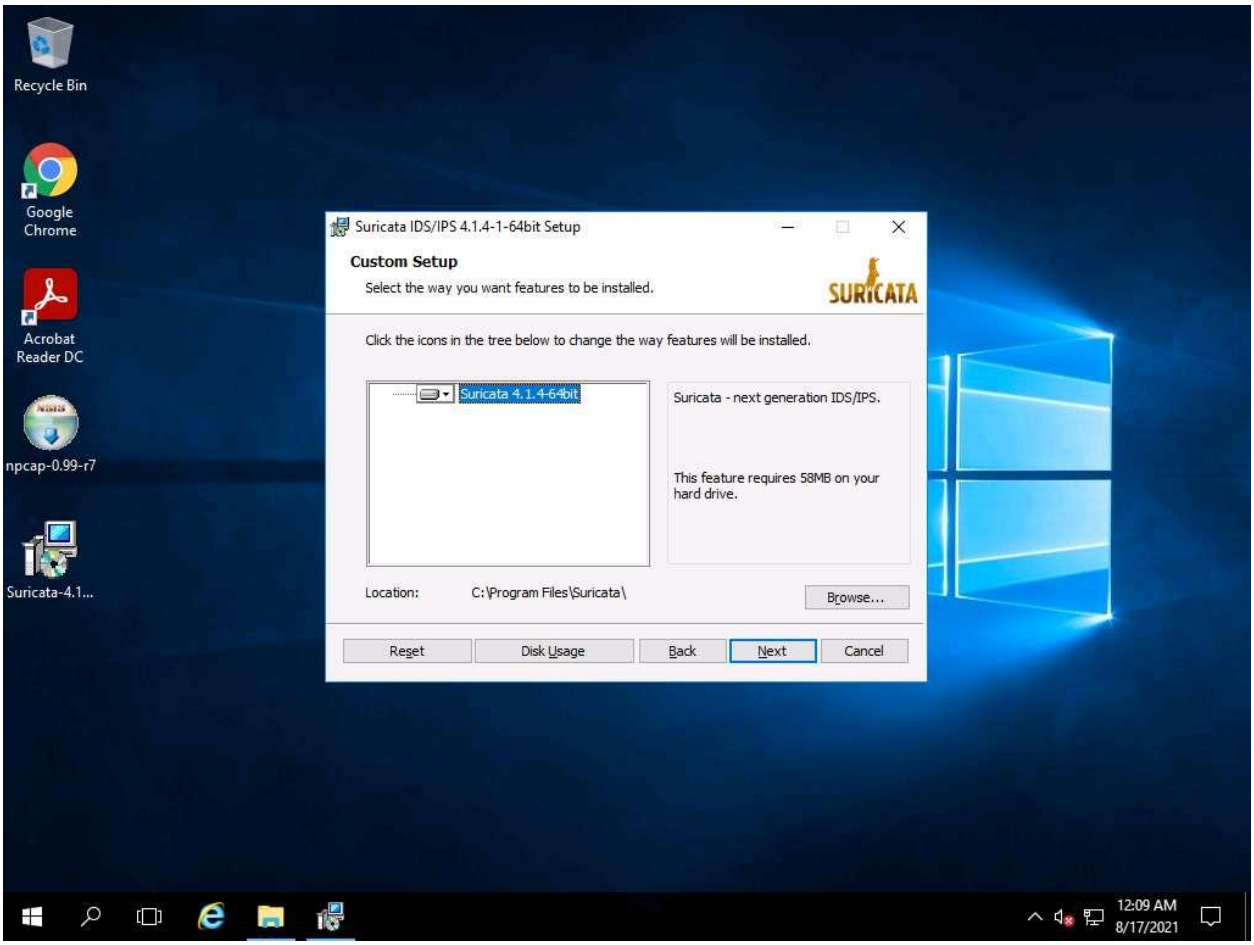
32. Double click Suricata-4.1.4-1-64bit.msi. The Suricata.IDS/IPS2.1.2-1-64bit Setup window will appear. Click Next.



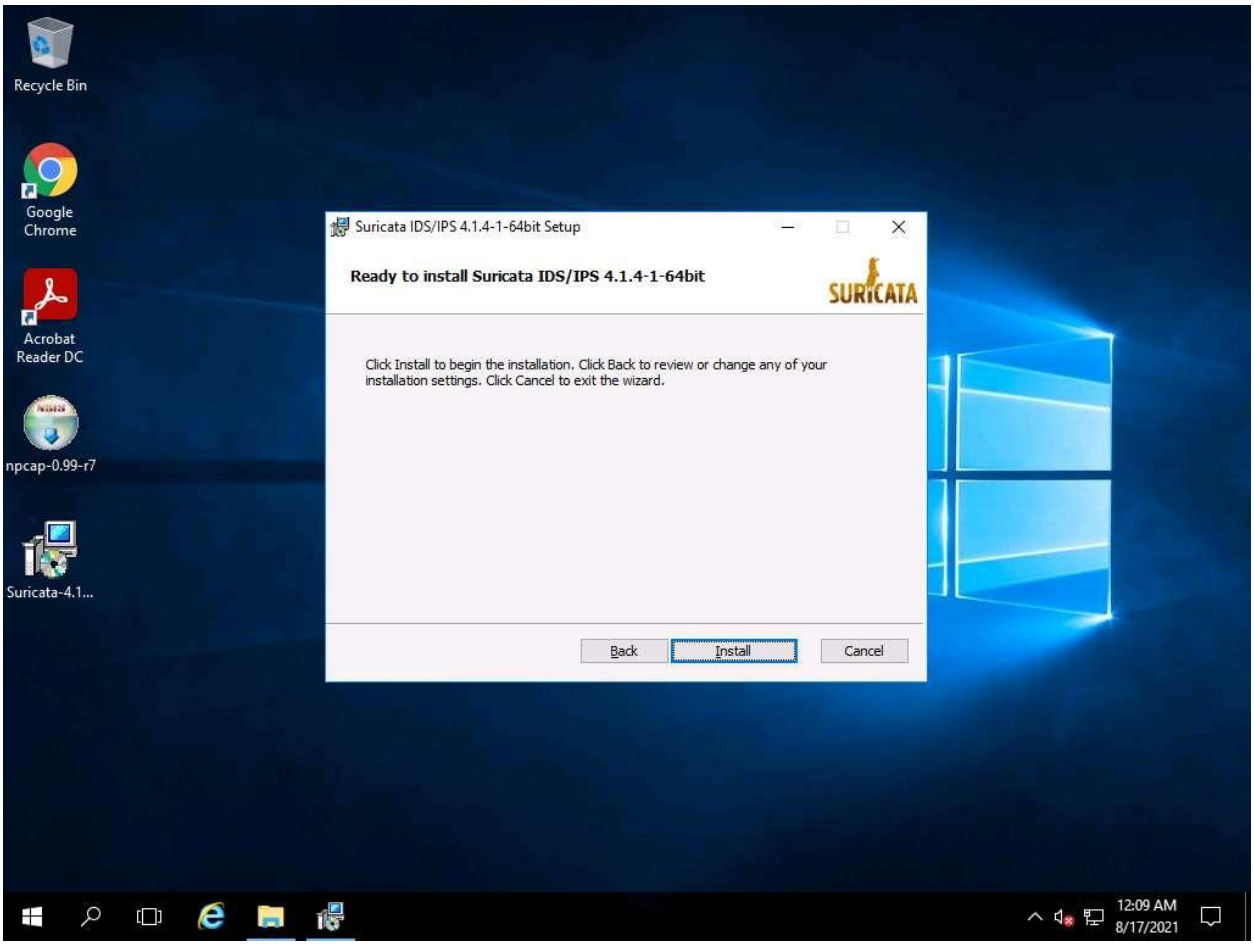
33. Check I accept the terms in the License Agreement to accept the license, and click Next.



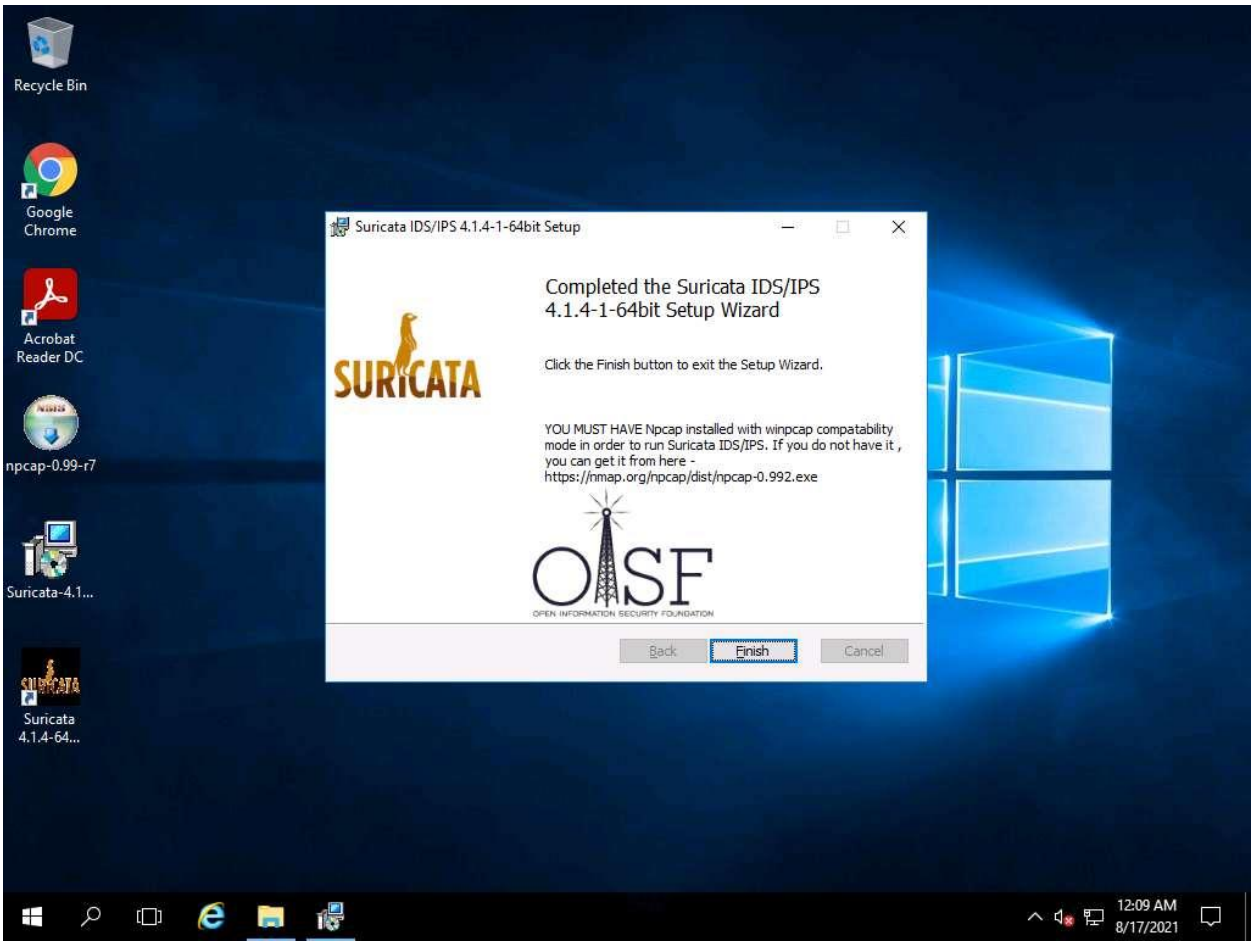
34. Click Next to continue the installation as shown in the screenshot below.



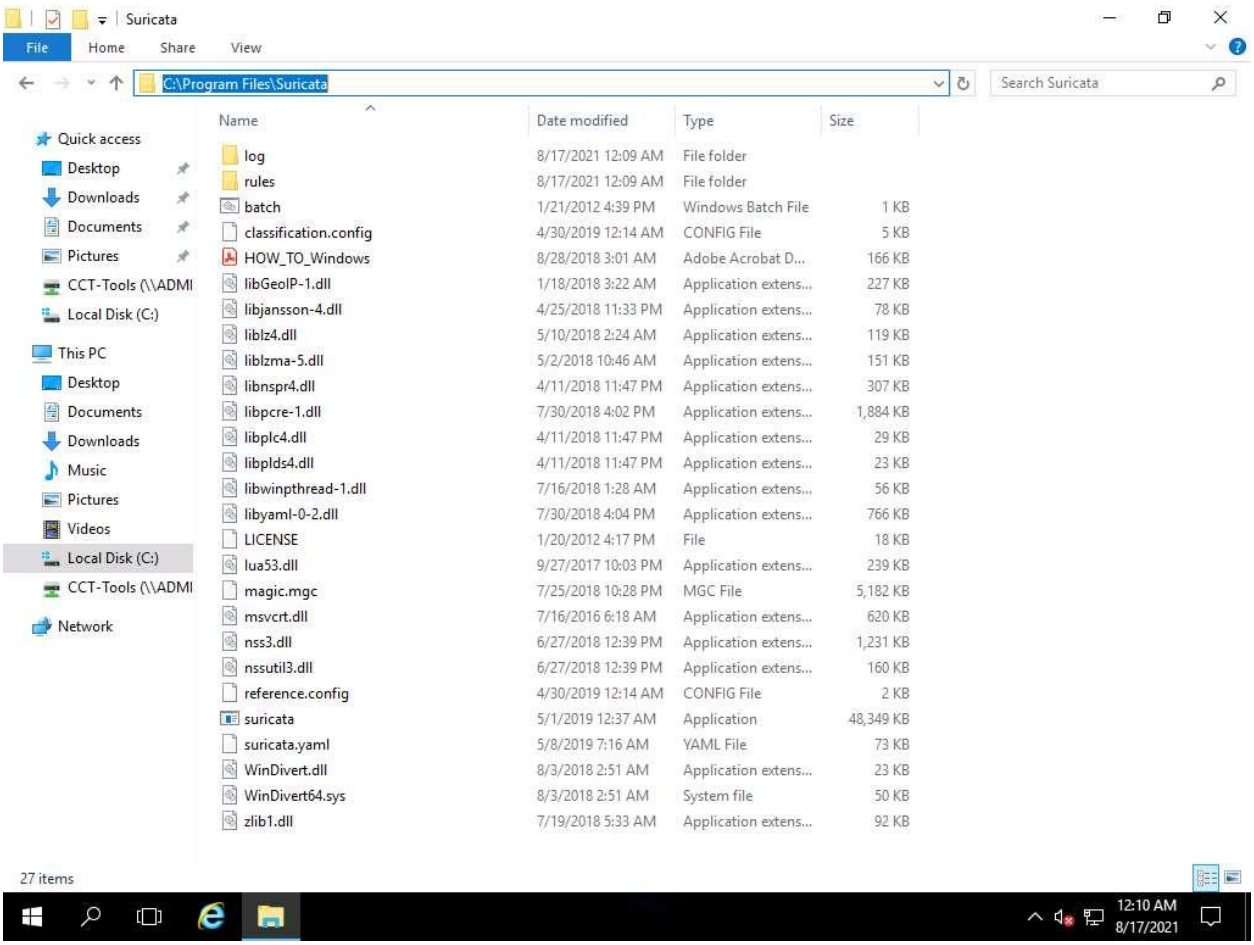
35. Click Install to continue the installation process.



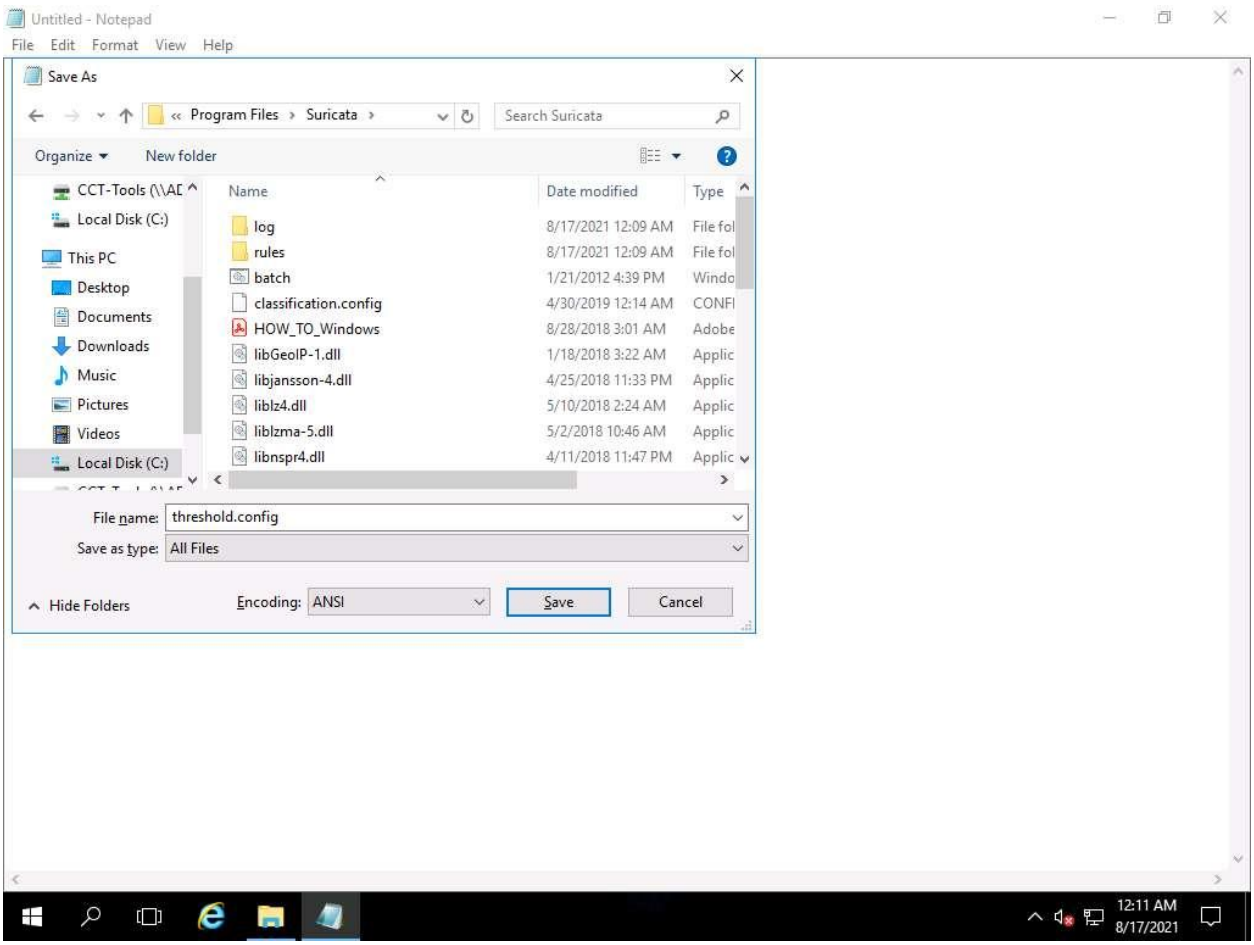
36. Click Finish to complete the installation process.



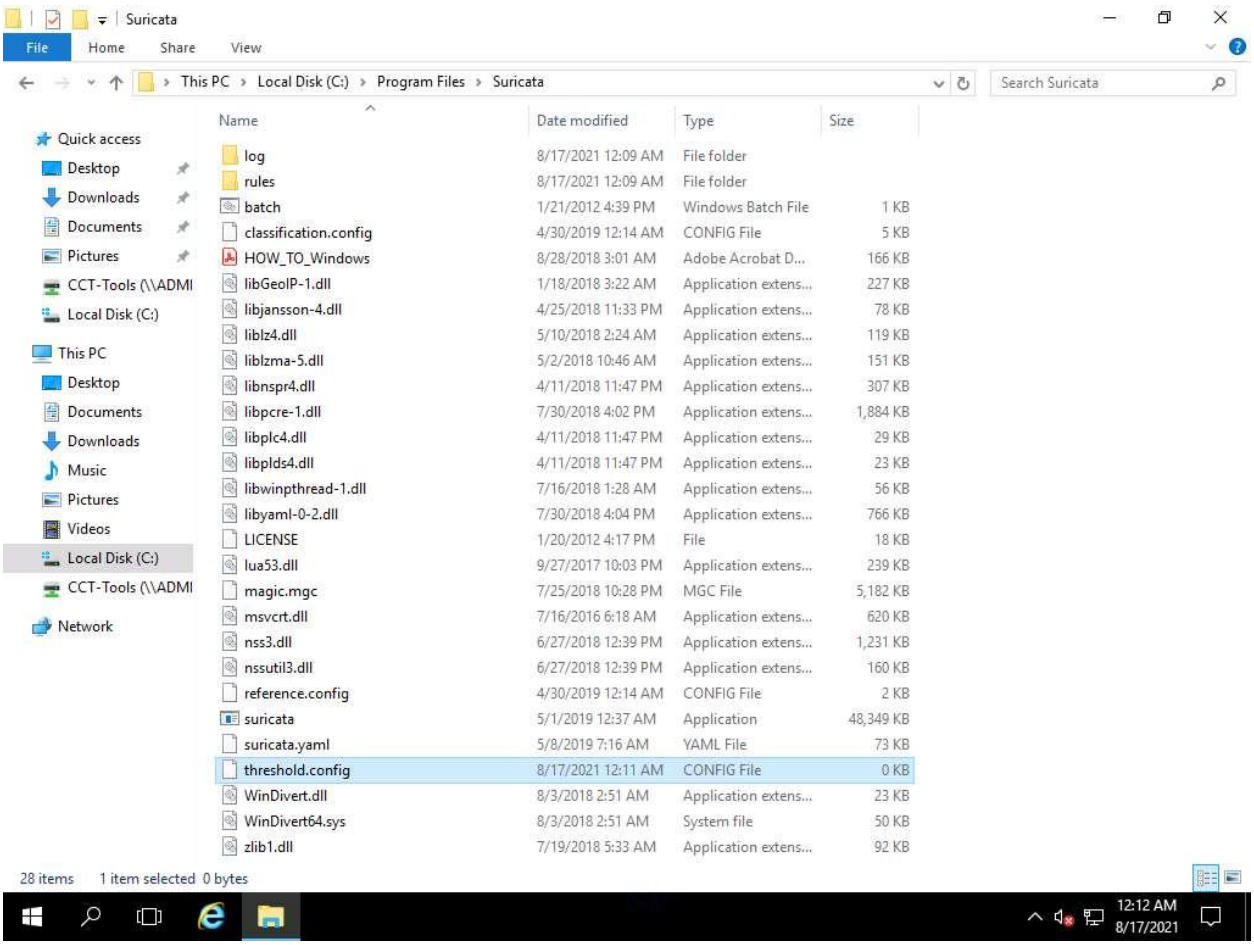
37. After Suricata IDS is successfully installed, the Suricata directory will be created under the C:\Program Files\Suricata.



38. From Windows search, Open Notepad and save the empty threshold.config file under C:\Program Files\Suricata\ location, as shown in the screenshot below (ensure that you have selected All Files in the Save as type: option while saving the file).



39. The threshold.config file will be created as shown in the screenshot below.



40. The Suricata IDS generates the alert based on the ruleset. A security professional can set the custom rule using the .rule file as shown in the following steps.

41. First, the local.rules file needs to be created. The local.rules file includes custom rules. We can create 'n' number of files for various rules (the rule file must have a .rule extension).

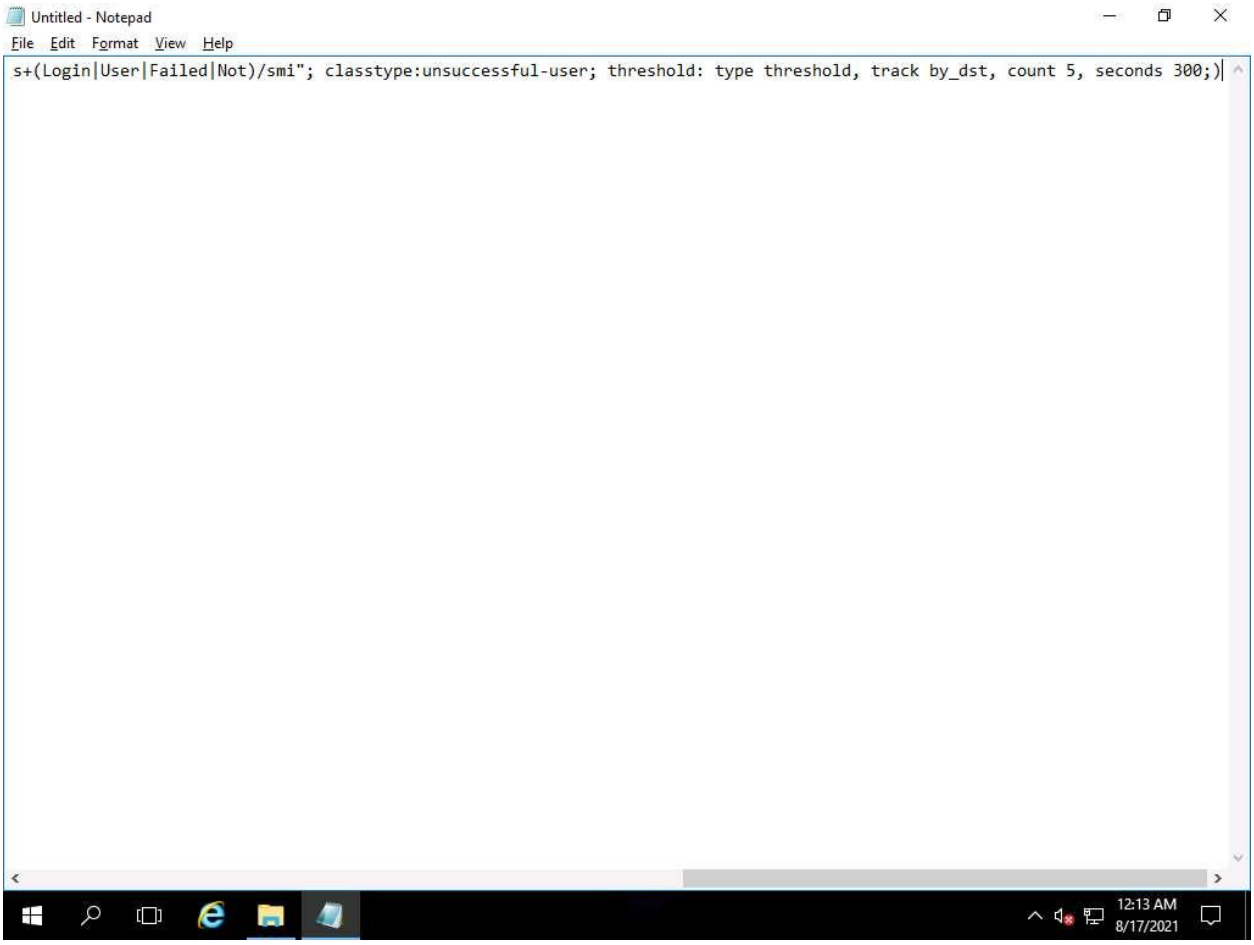
42. Here, we have created a rule for generating a PING alert.

43. Open Notepad, and type the following:

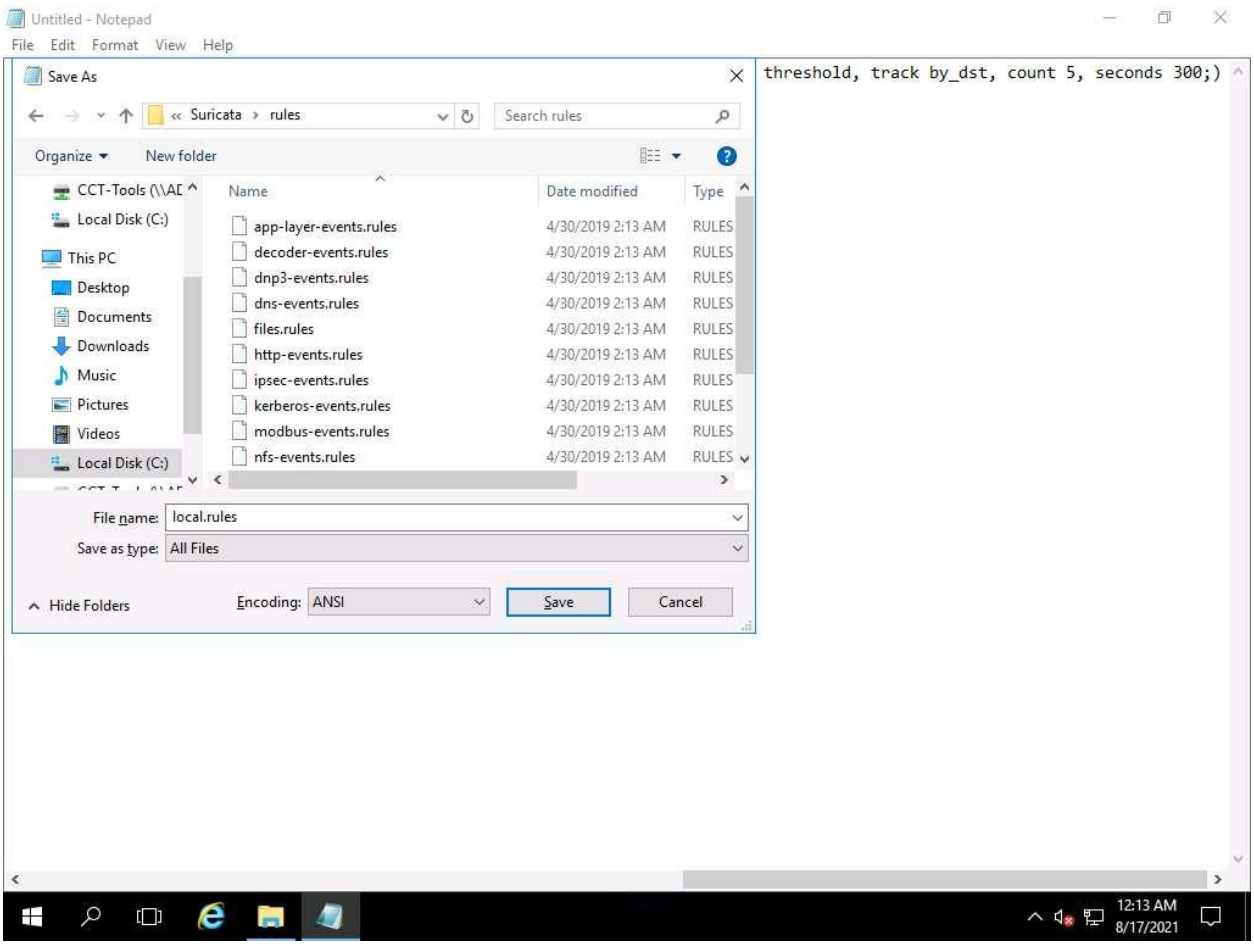
TypeCopy

alert tcp any 21 -> any any (msg:”ET SCAN Potential FTP Brute-Force attempt”; flow:from_server,established; dsize:<100; content:”530 “; depth:4;

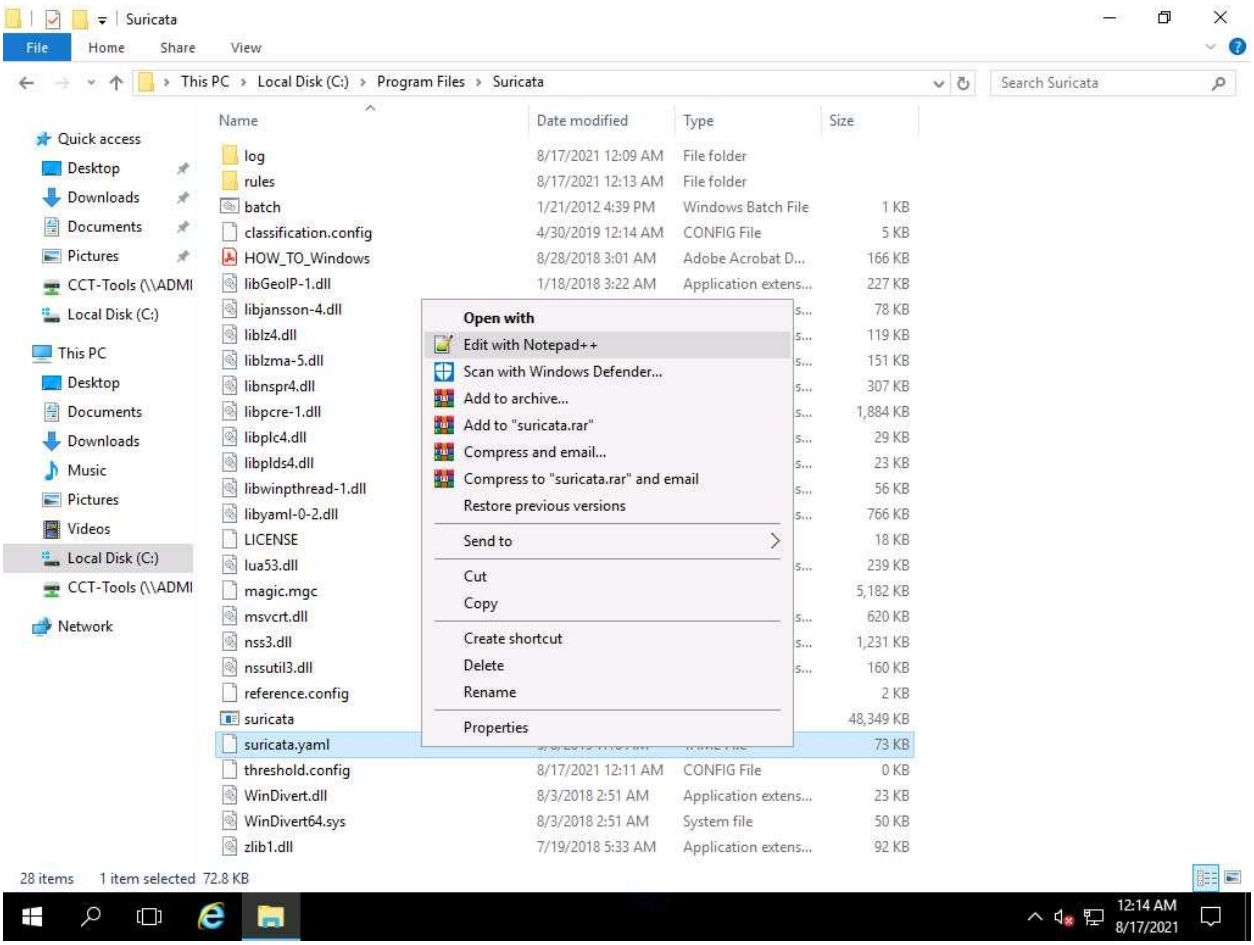
pcre:"/530\s+(Login|User|Failed|Not)/smi"; classtype:unsuccessful-user; threshold: type threshold, track by_dst, count 5, seconds 300;)



44. Save the file as local.rules under the C:\Program Files\Suricata\rules location as shown in the screenshot below (ensure that you have selected All Files in the Save as type option while saving the file).



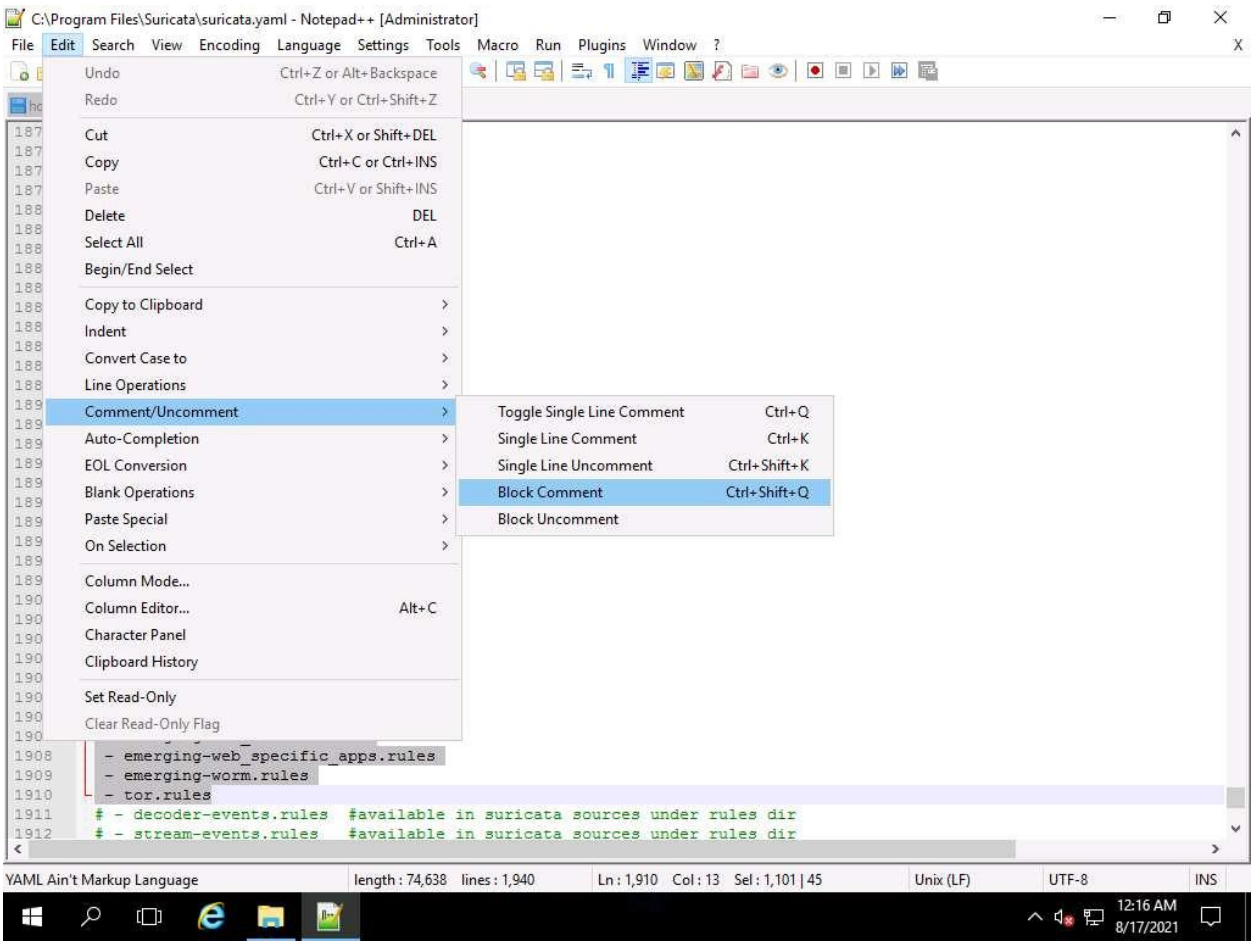
45. Navigate to C:\Program Files\Suricata, and open suricata.yaml file in Notepad++.



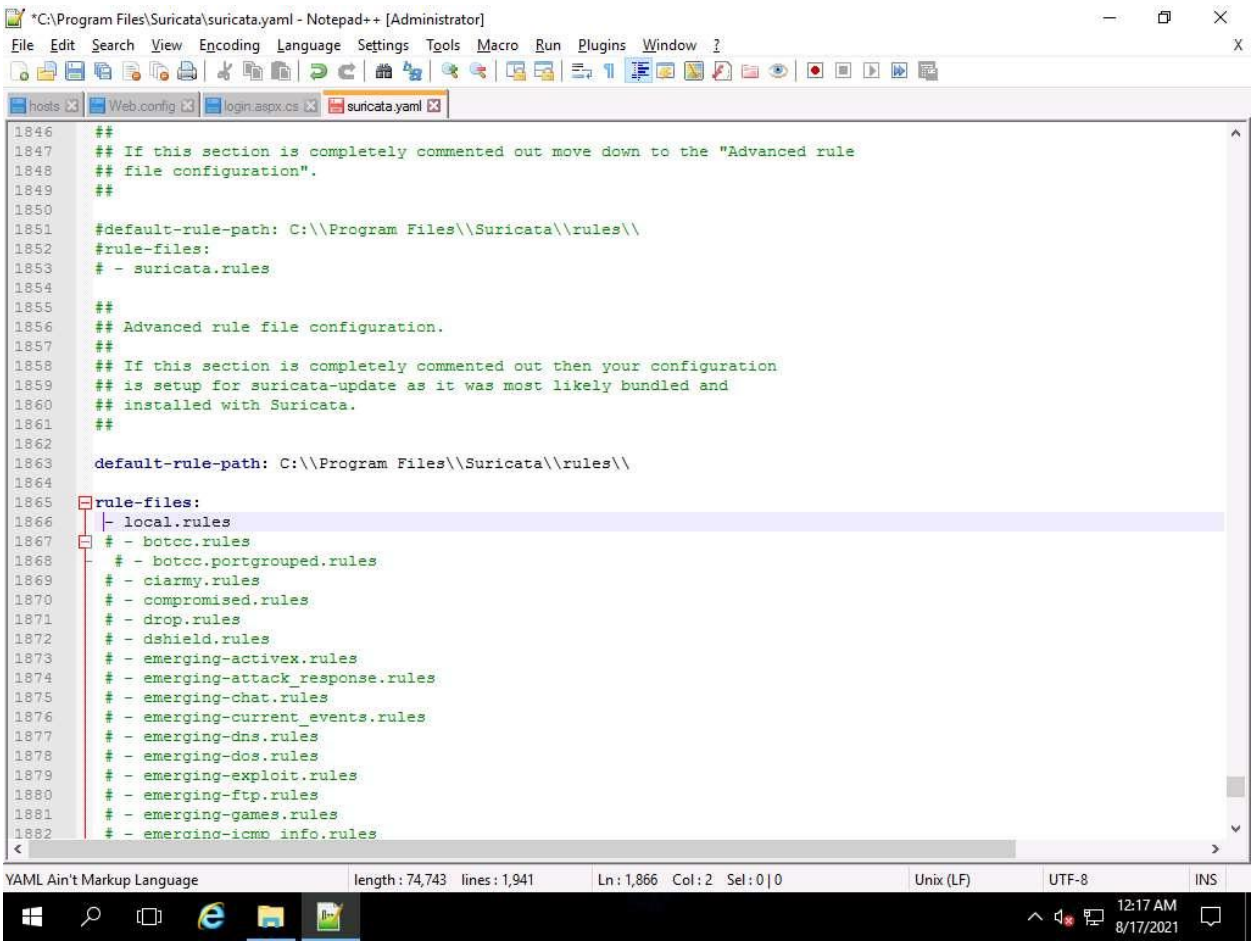
46. The suricata.yaml file opens in Notepad++.

If the Notepad++ update pop-up appears, click No.

47. To comment on the default rules files, select line numbers 1866 to 1910, navigate to the Edit menu, and select Comment/Uncomment->Block Comment as shown in the screenshot below.



48. Add – local.rules below the line number 1865 as shown in the screenshot below, and click Save.



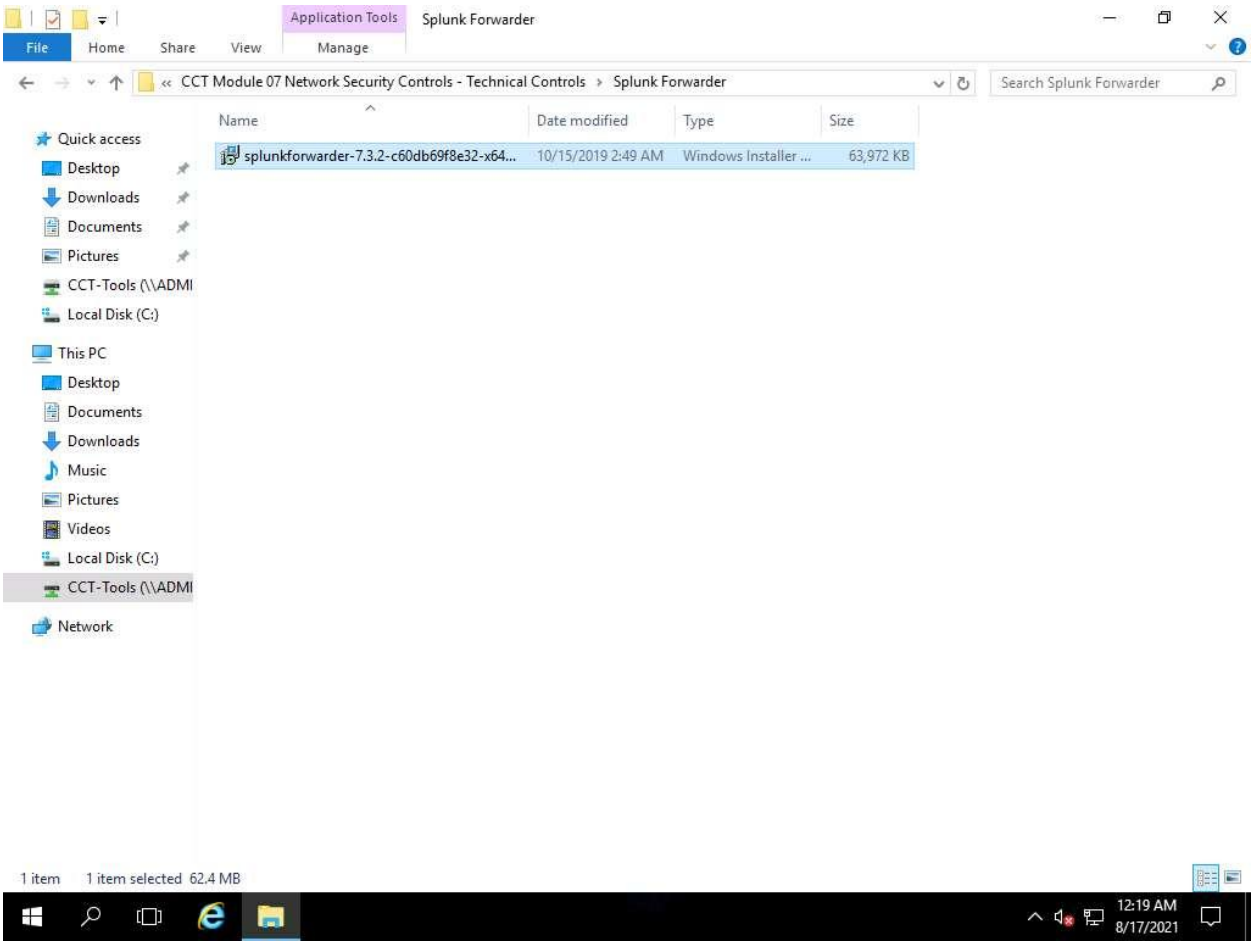
49. Close all open folders and files.

50. Navigate to C:\Program Files\Suricata\log. Observe that there is no log file under the log\files directory.

51. We will capture the Suricata logs in Splunk, next we forward Suricata logs to Splunk on the monitoring machine using Splunkforwarder.

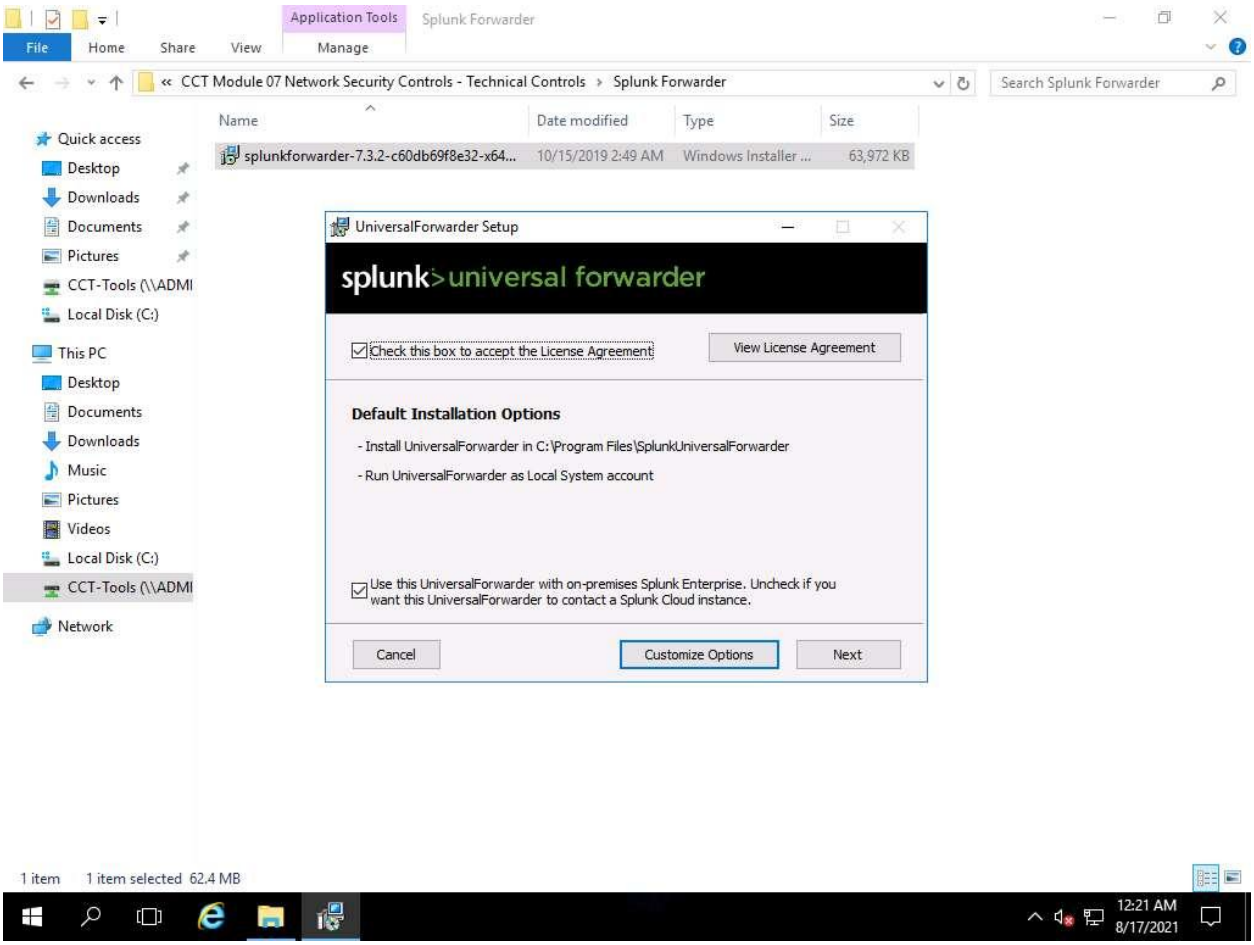
52. To install Splunk forwarder, navigate to Z:\CCT Module 07 Network Security Controls - Technical Controls\Splunk Forwarder

53. Double-click on splunkforwarder-7.3.2-c60db69f8e32-x64-release.msi.

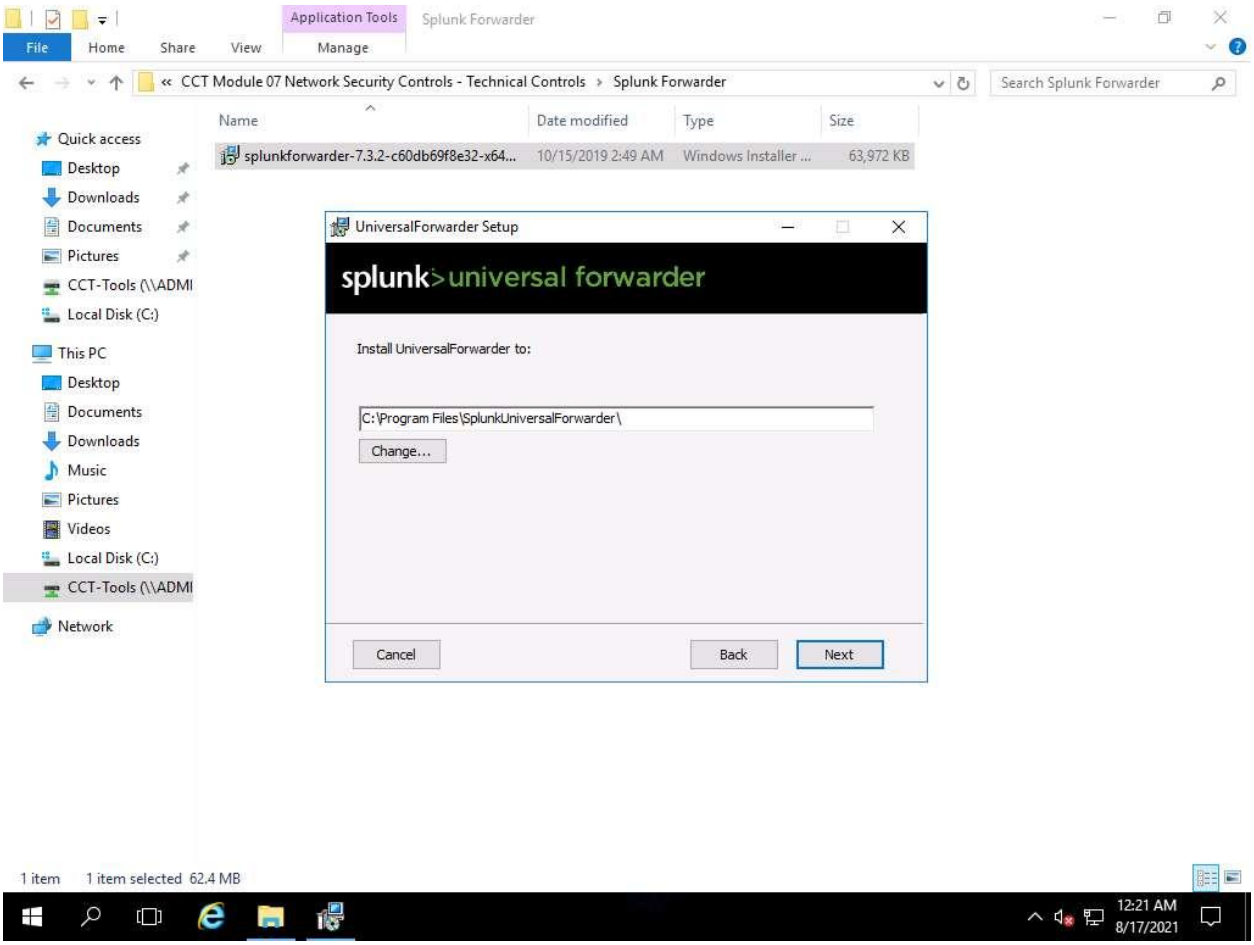


If a Security Warning pop-up appears, click on Run.

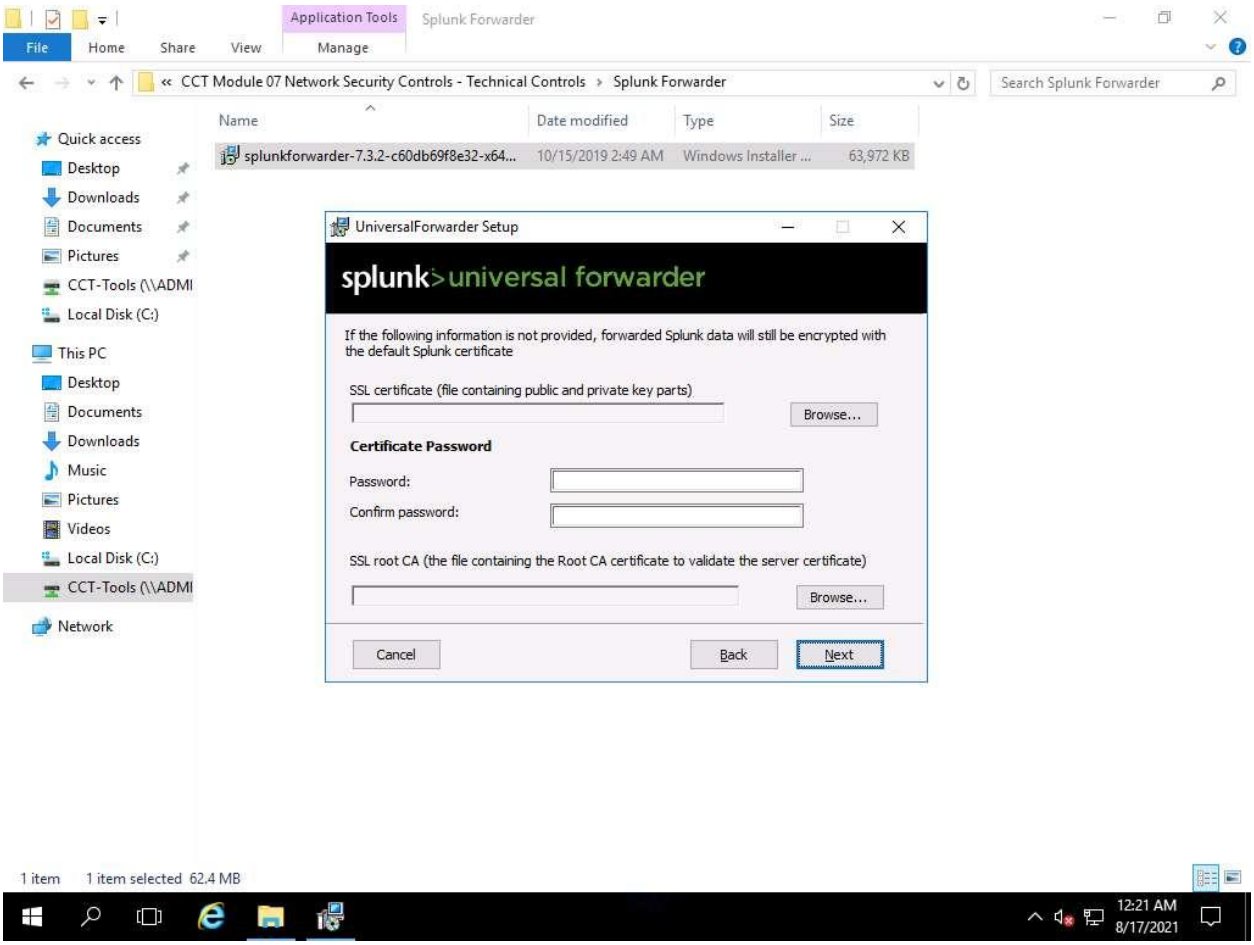
54. Once the UniversalForwarder Setup window appears, check Check the box to accept the License Agreement and click on Customize Options.



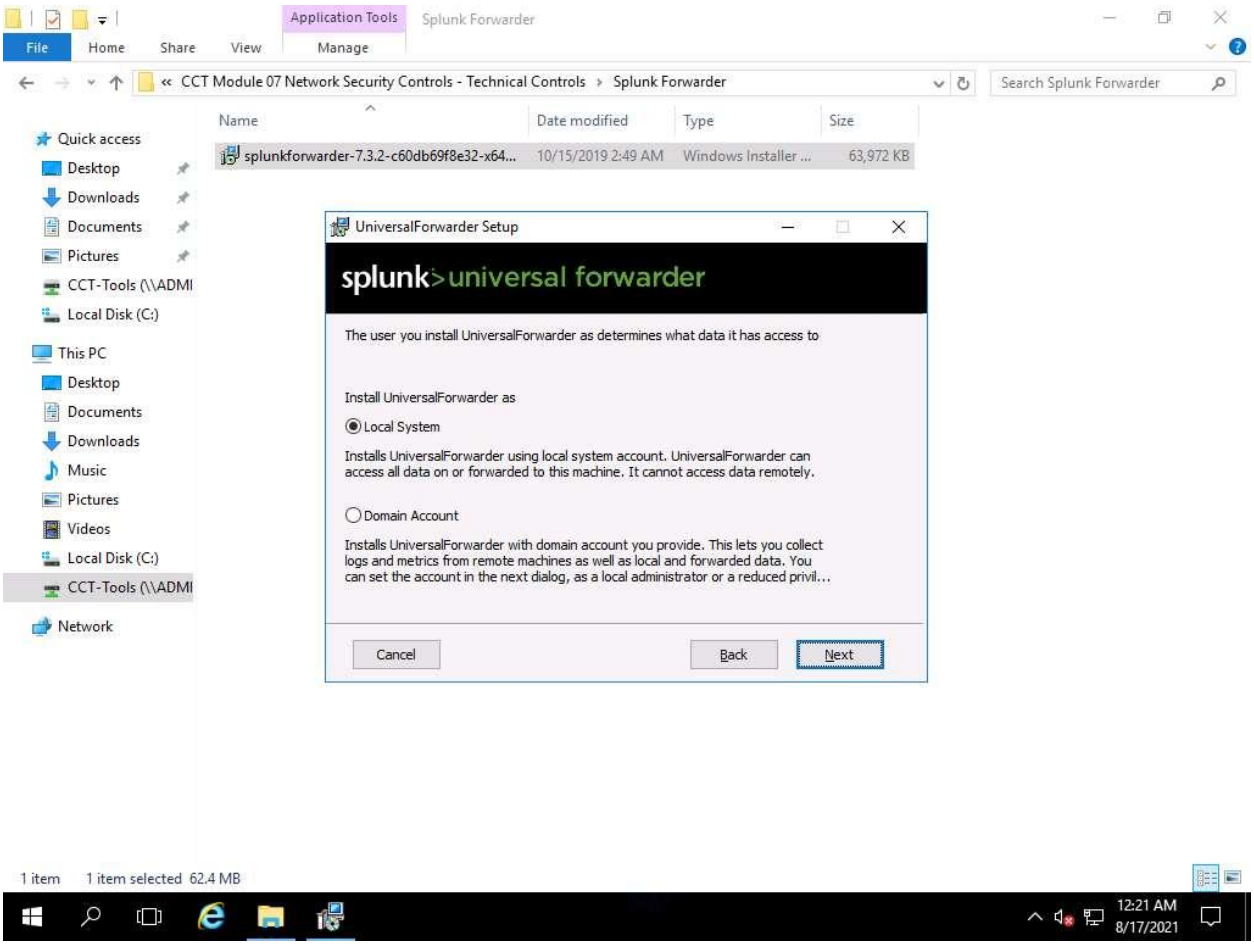
55. Leave the installation path set to the default location and click on Next.



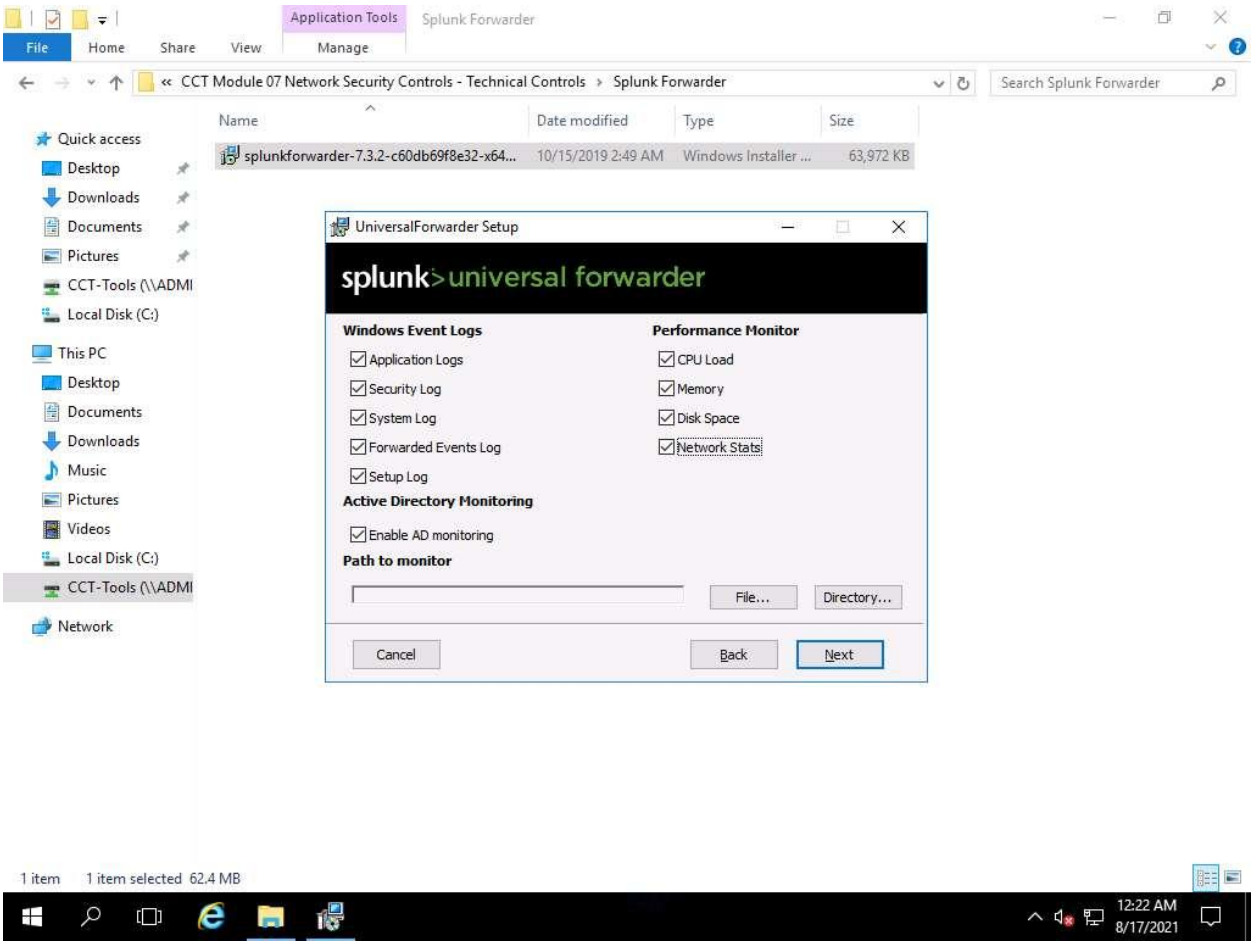
56. Click on Next in the Splunk certificate section.



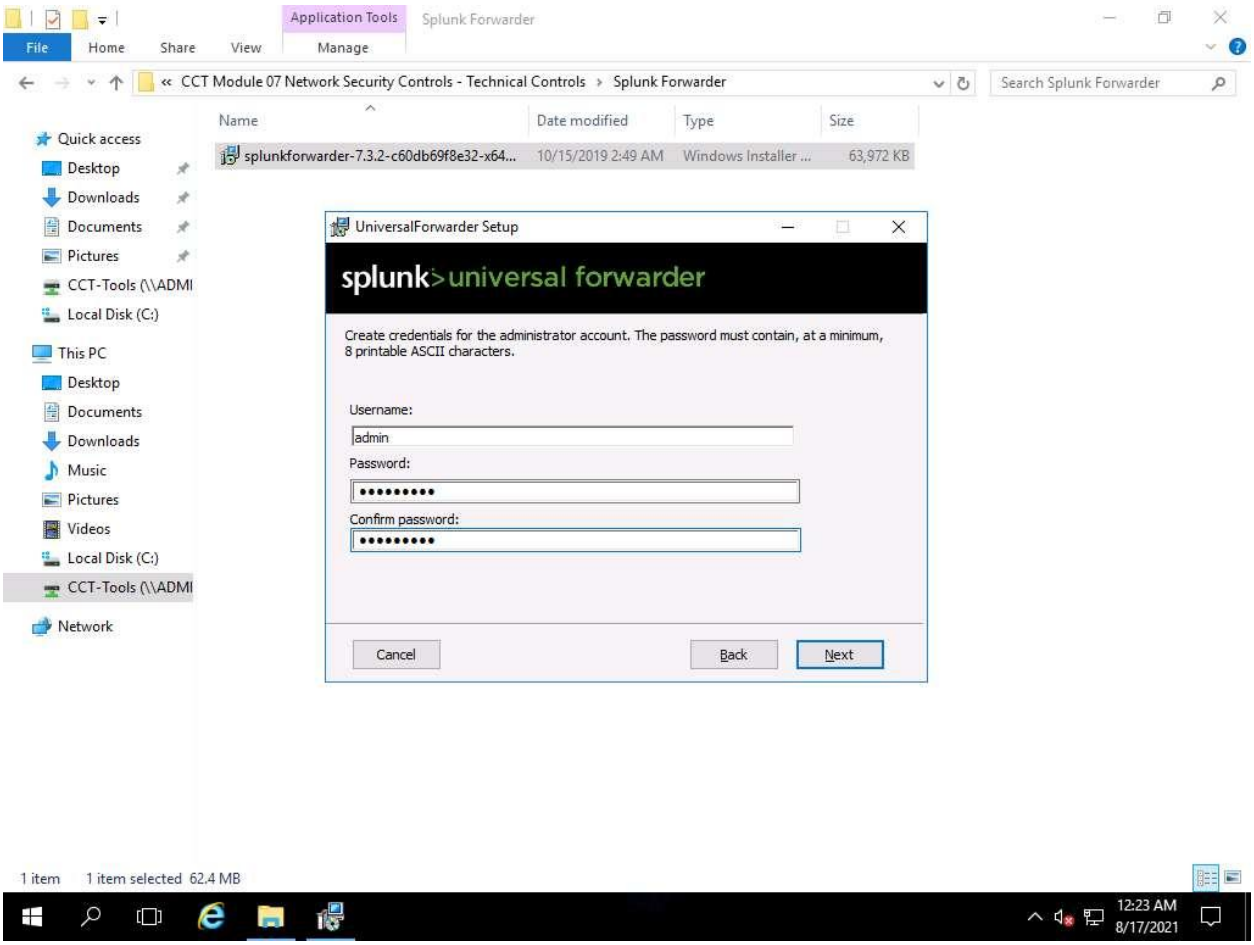
57. In the next step, select the Local System radio button to install Universal Forwarder as a Local System and then click on Next.



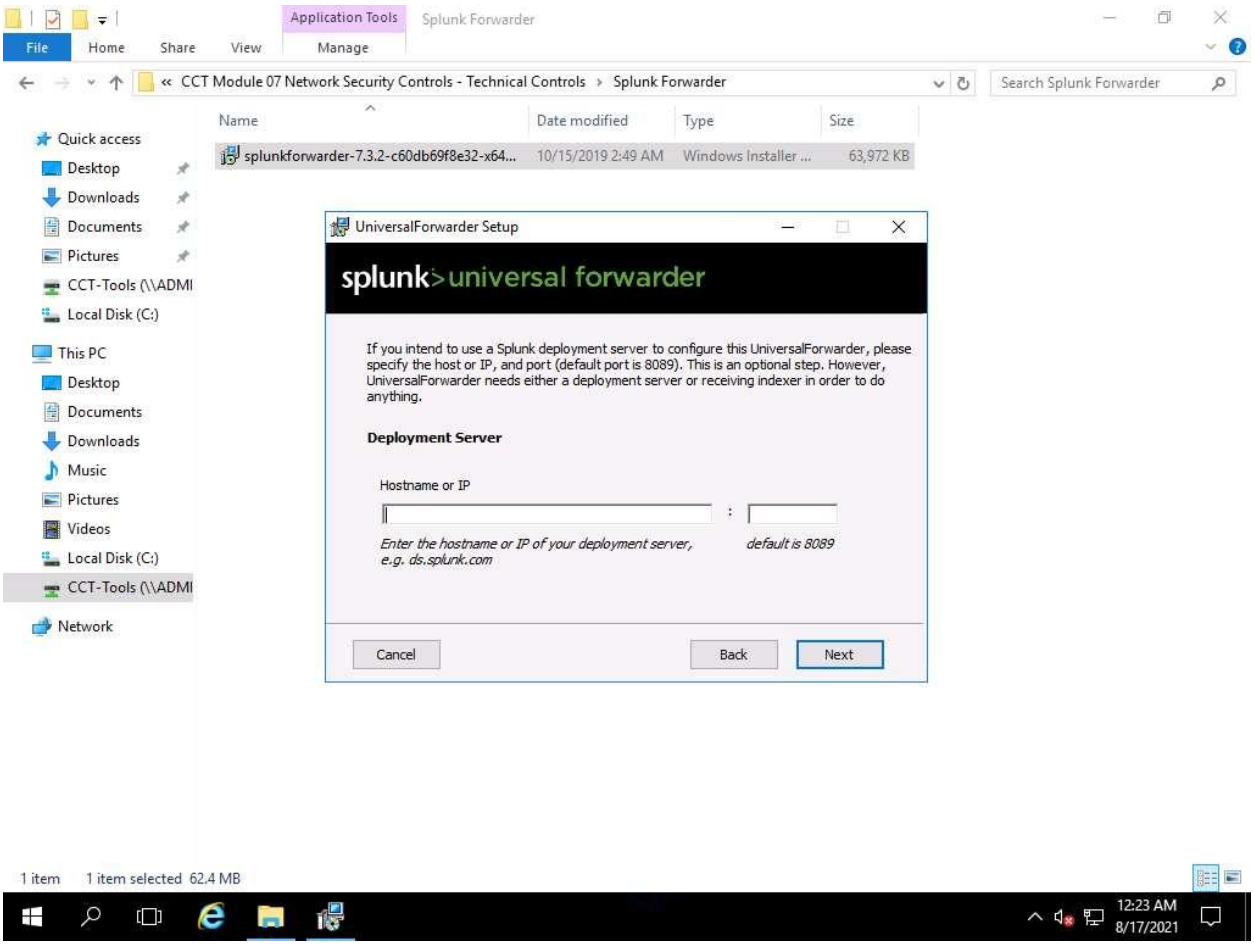
58. Next, check all entities under Windows Event Logs, Active Directory Monitoring and Performance Monitor and click on Next.



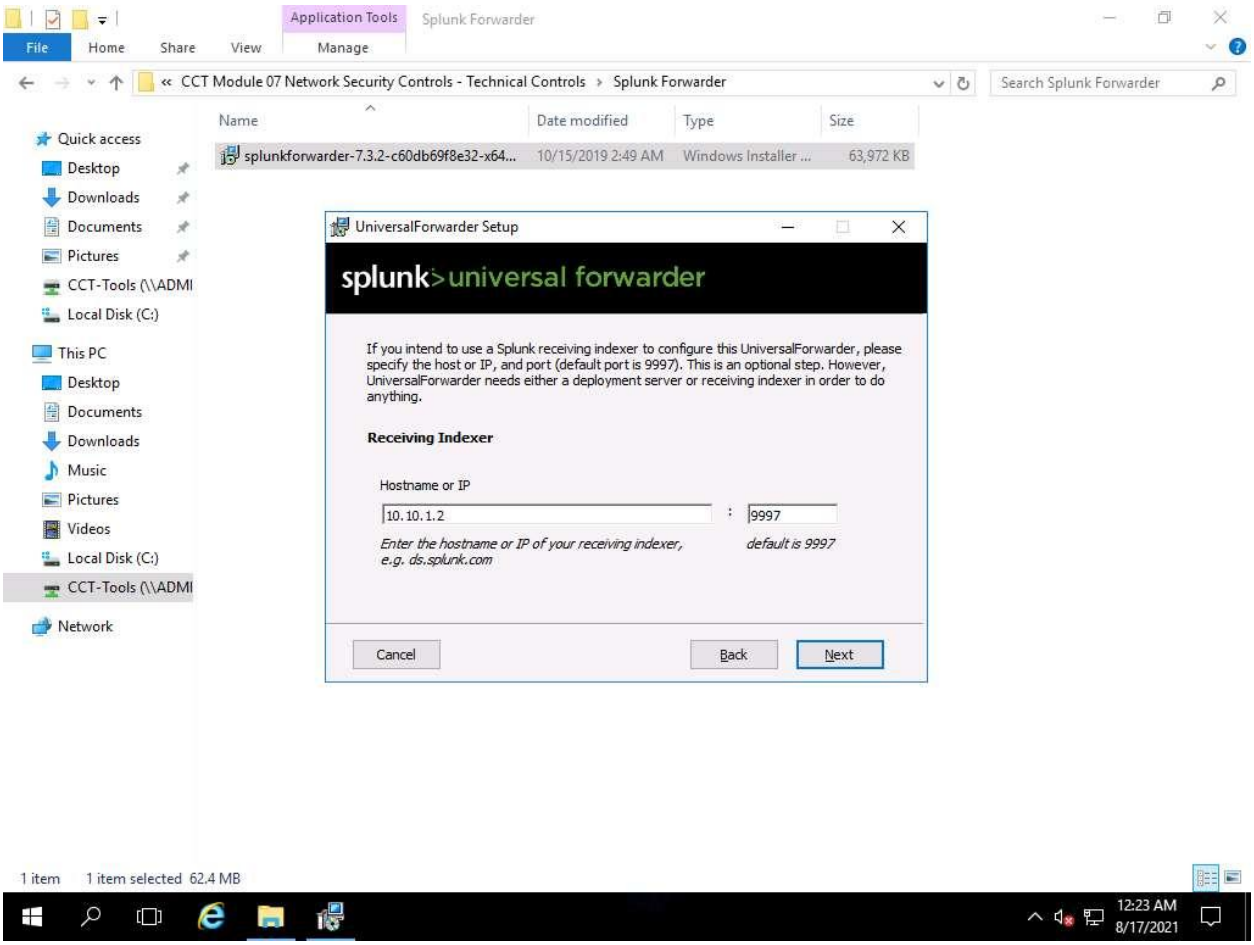
59. Create credentials for the administrator account; type username "admin" and password "admin@123" and click on Next.



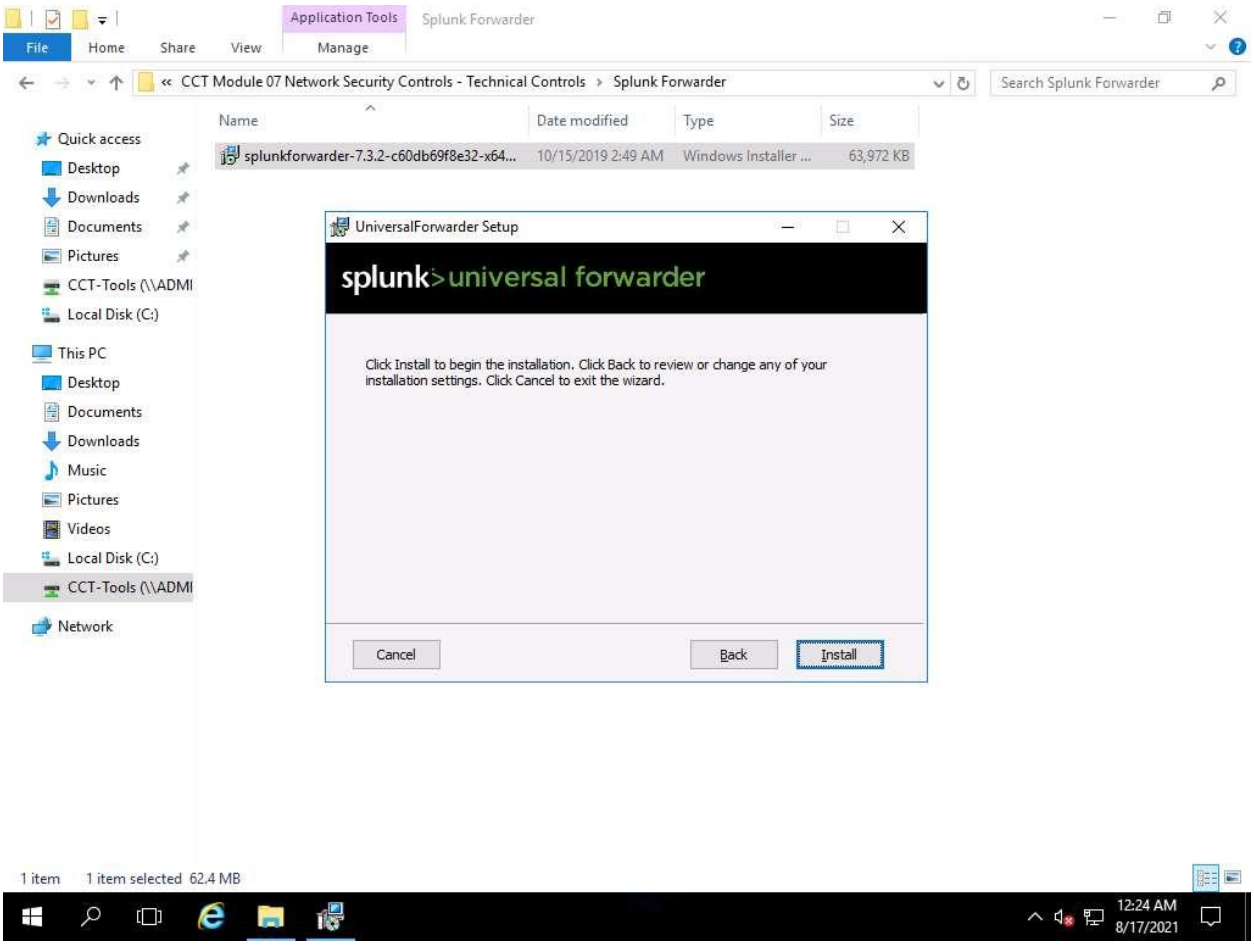
60. Leave the Deployment Server section without issuing the deployment IP and port number details, and click on Next.



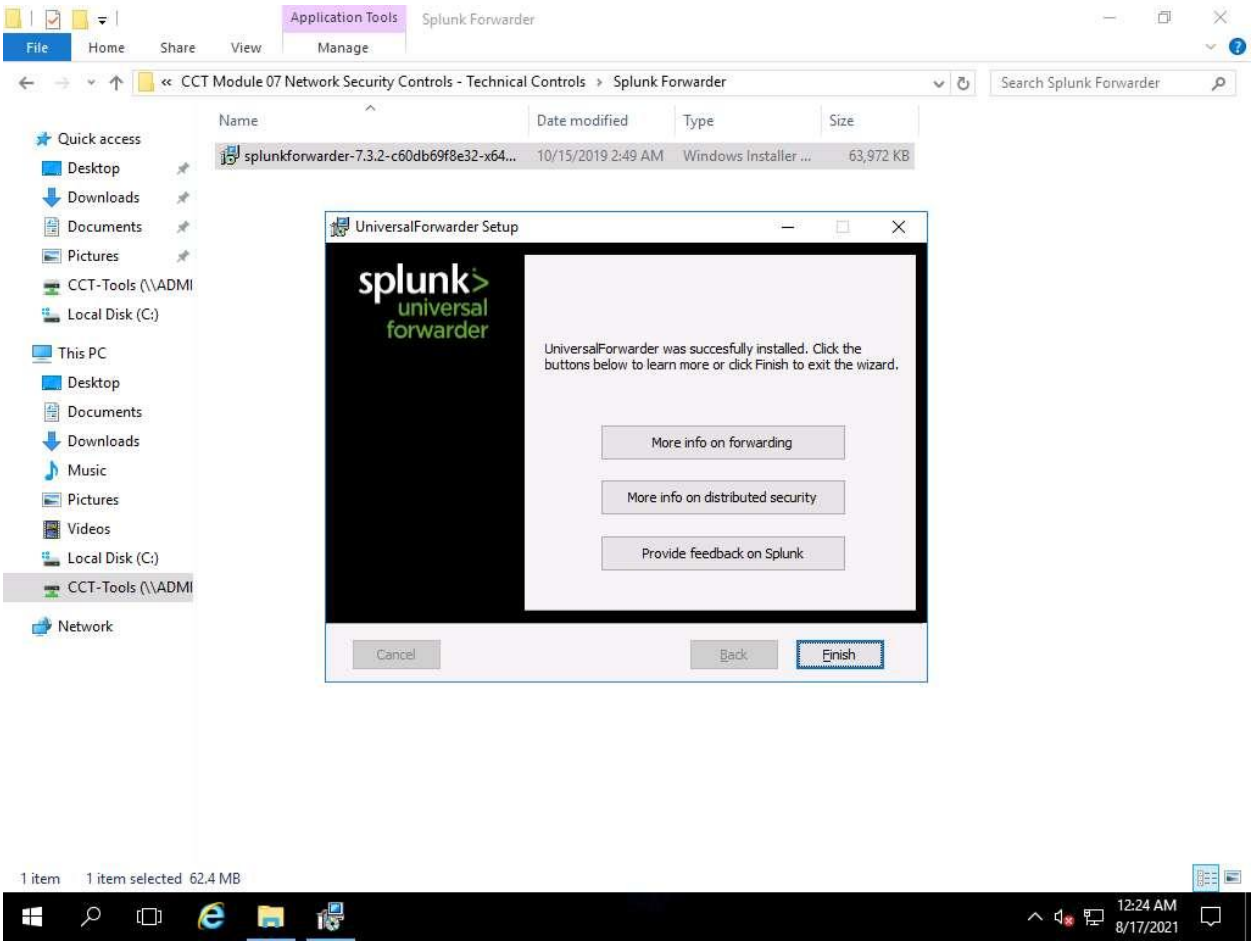
61. In the Receiving Indexer section, enter the IP address for Admin Machine-1, namely, 10.10.1.2 in the Hostname or IP field; enter Port 9997 in the port field and click on Next.



62. Once you are through with the configuration, click on Install. At this time, if a User Account Control pop-up appears, click on Yes.



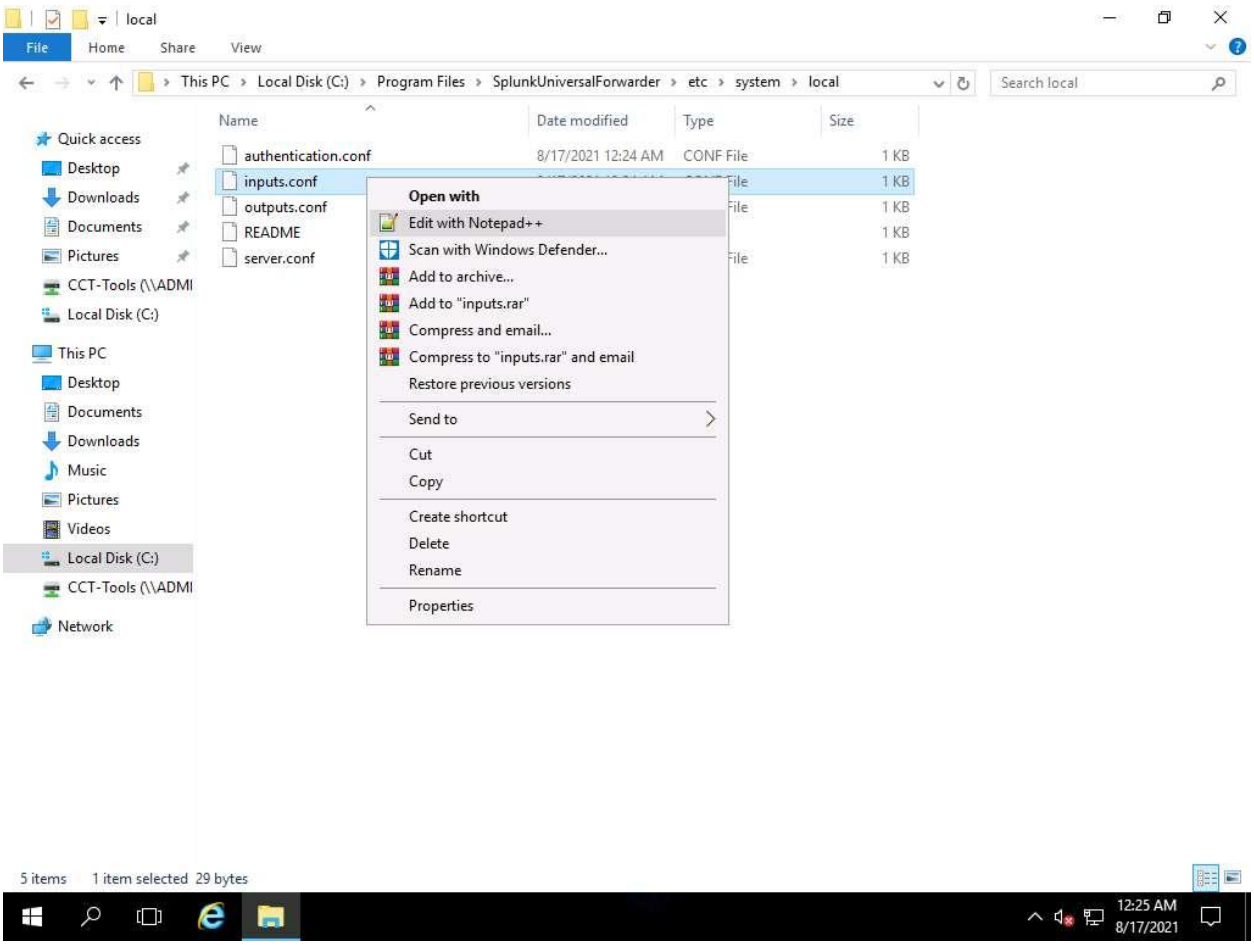
63. Click on Finish after the installation completes.



You do not need any explicit configuration for Splunk Forwarder to collect Windows event logs, since Splunk Forwarder has default configuration done during installation. You need to configure Splunk Forwarder explicitly to collect logs from IIS and Snort IDS.

64. To configure Splunk Universal Forwarder to collect IIS logs from the Web Server machine, go to the Web Server machine.

65. Navigate to C:\Program Files\SplunkUniversalForwarder\etc\system\local, right-click on inputs.conf, and then on Edit with Notepad++.



66. Add the following lines in the inputs.conf file like in the below screenshot.

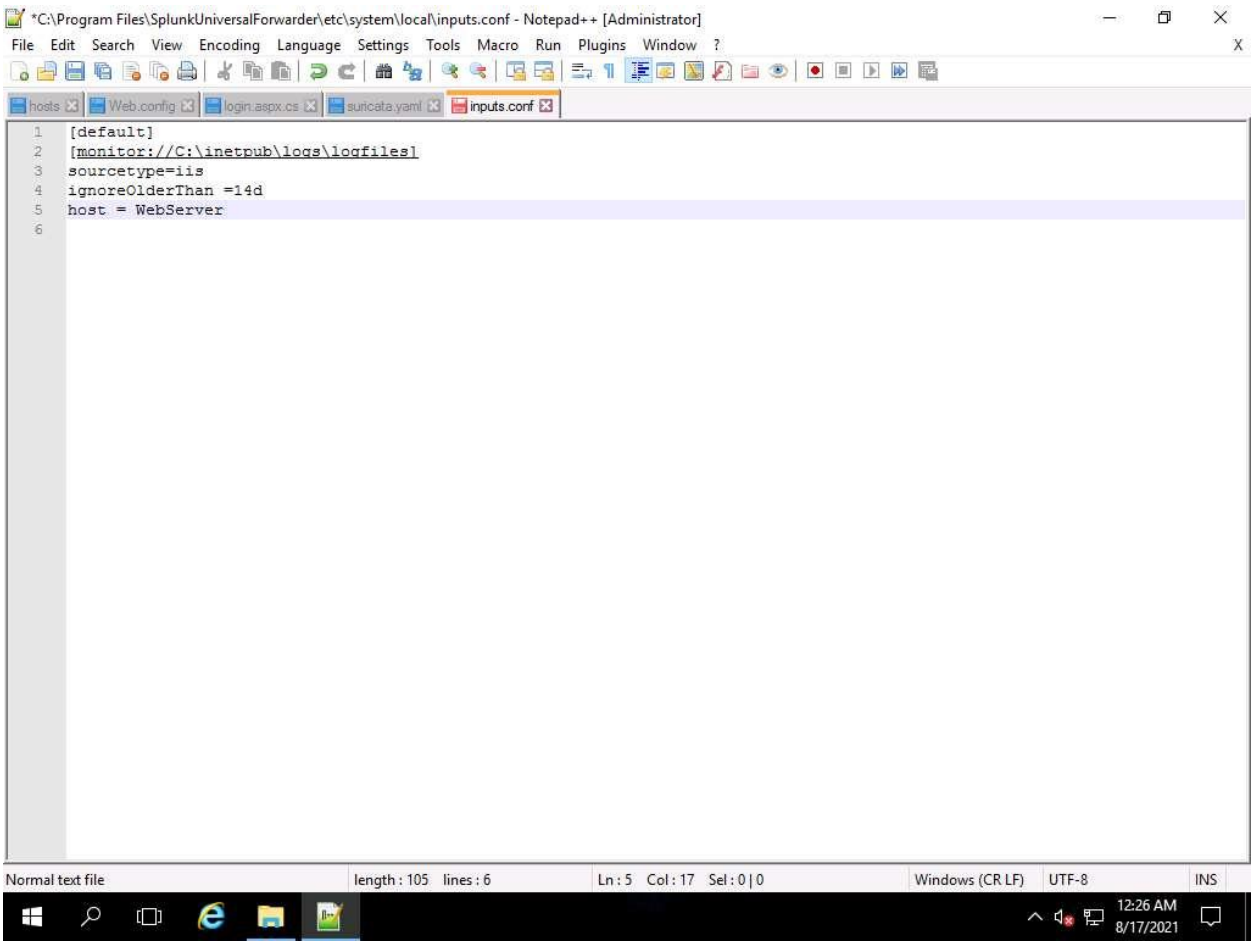
TypeCopy

[monitor*://C:\inetpub\logs\logfiles]*

sourcetype=iis

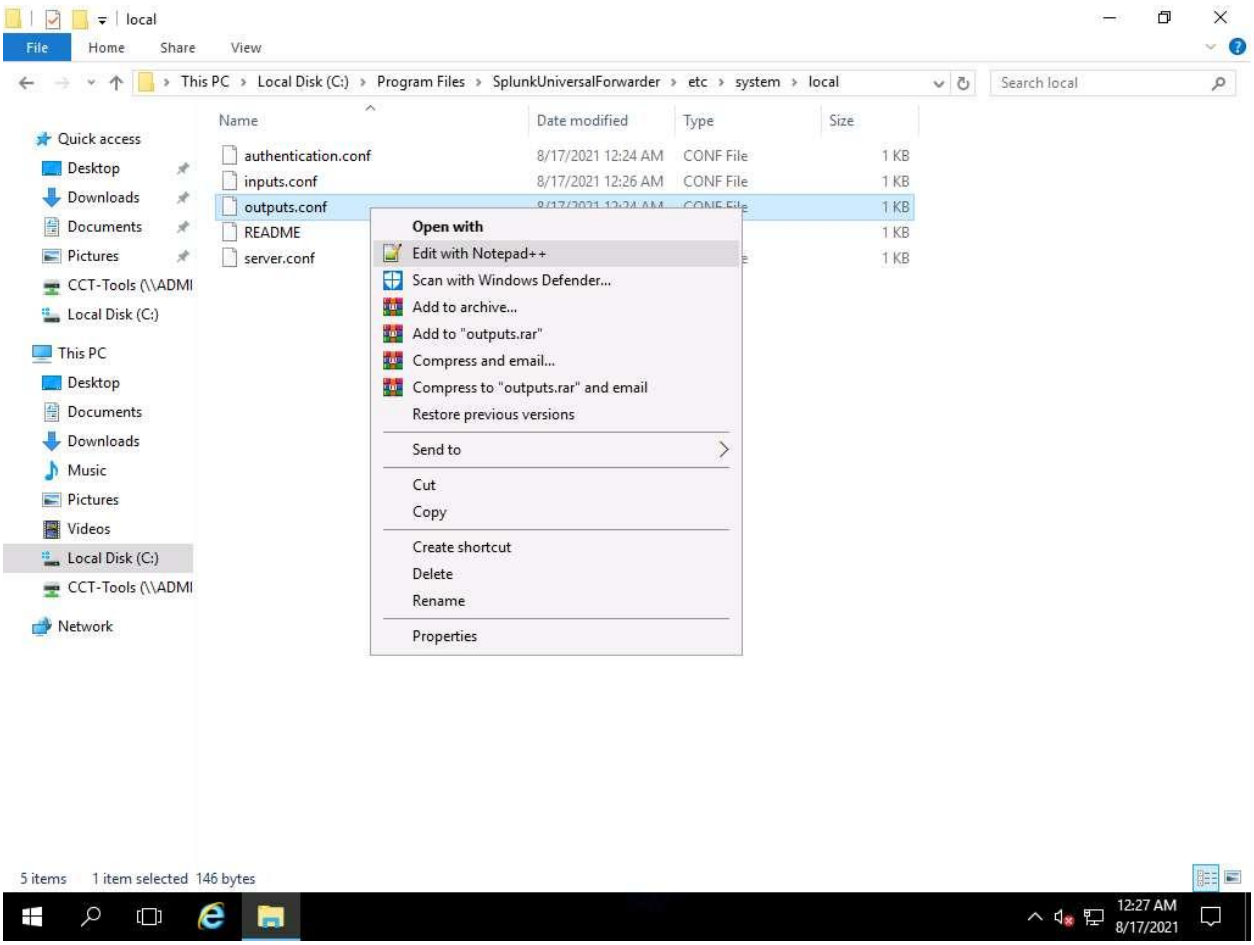
ignoreOlderThan =14d

host = WebServer



67. Click on Save to save the file and close it.

68. Right-click on outputs.conf, and then on Edit with Notepad++.



69. Add the following lines in the outputs.conf file, as shown in the screenshot below.

TypeCopy

[iis*]

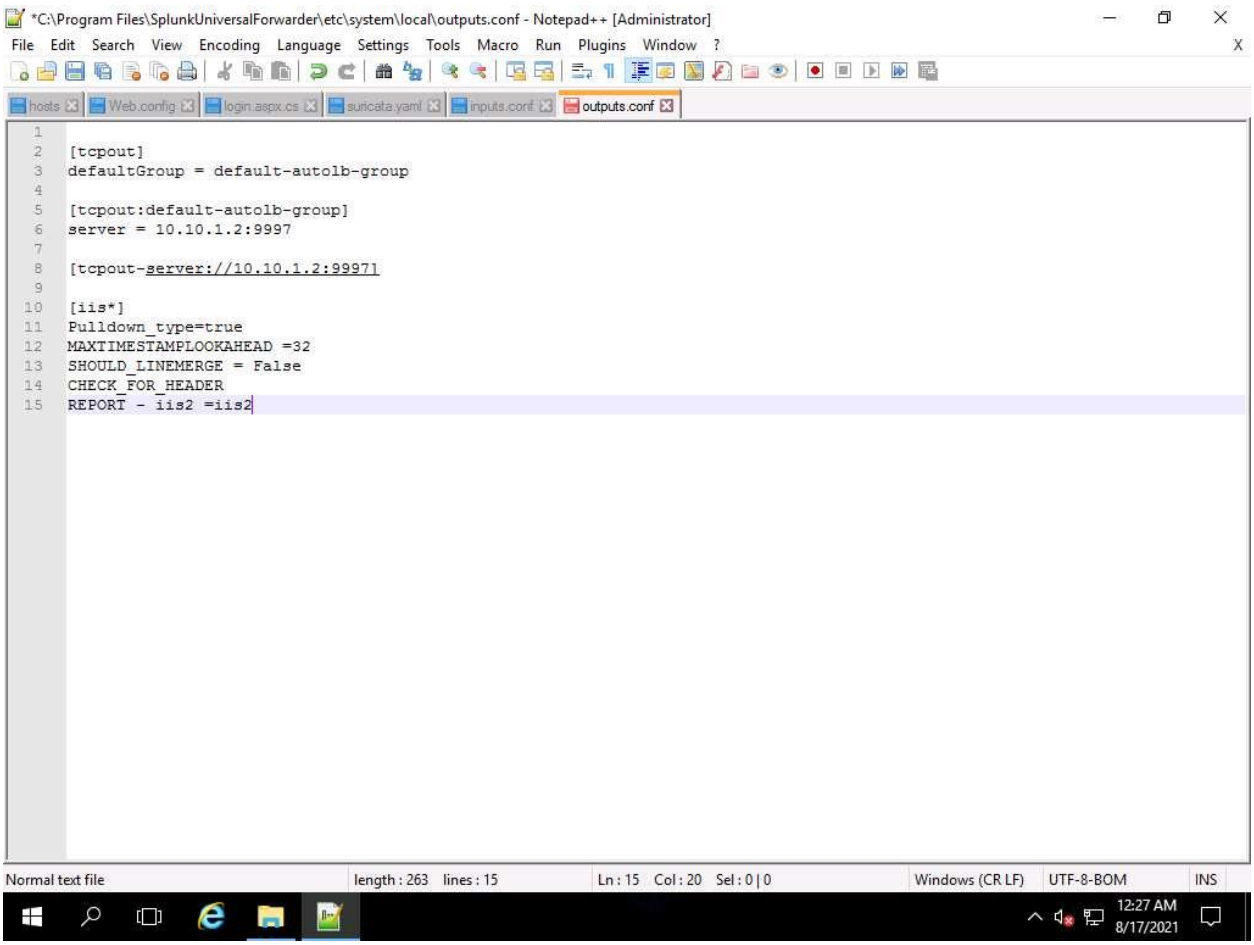
Pulldown_type=true

MAXTIMESTAMPLOOKAHEAD =32

SHOULD_LINEMERGE = False

CHECK_FOR_HEADER

REPORT – iis2 =iis2



70. Click on Save to save the file and then Close it.

71. Open Notepad and type the below code.

TypeCopy

[iis*]

Pulldown_type=true

MAXTIMESTAMPLOOKAHEAD =32

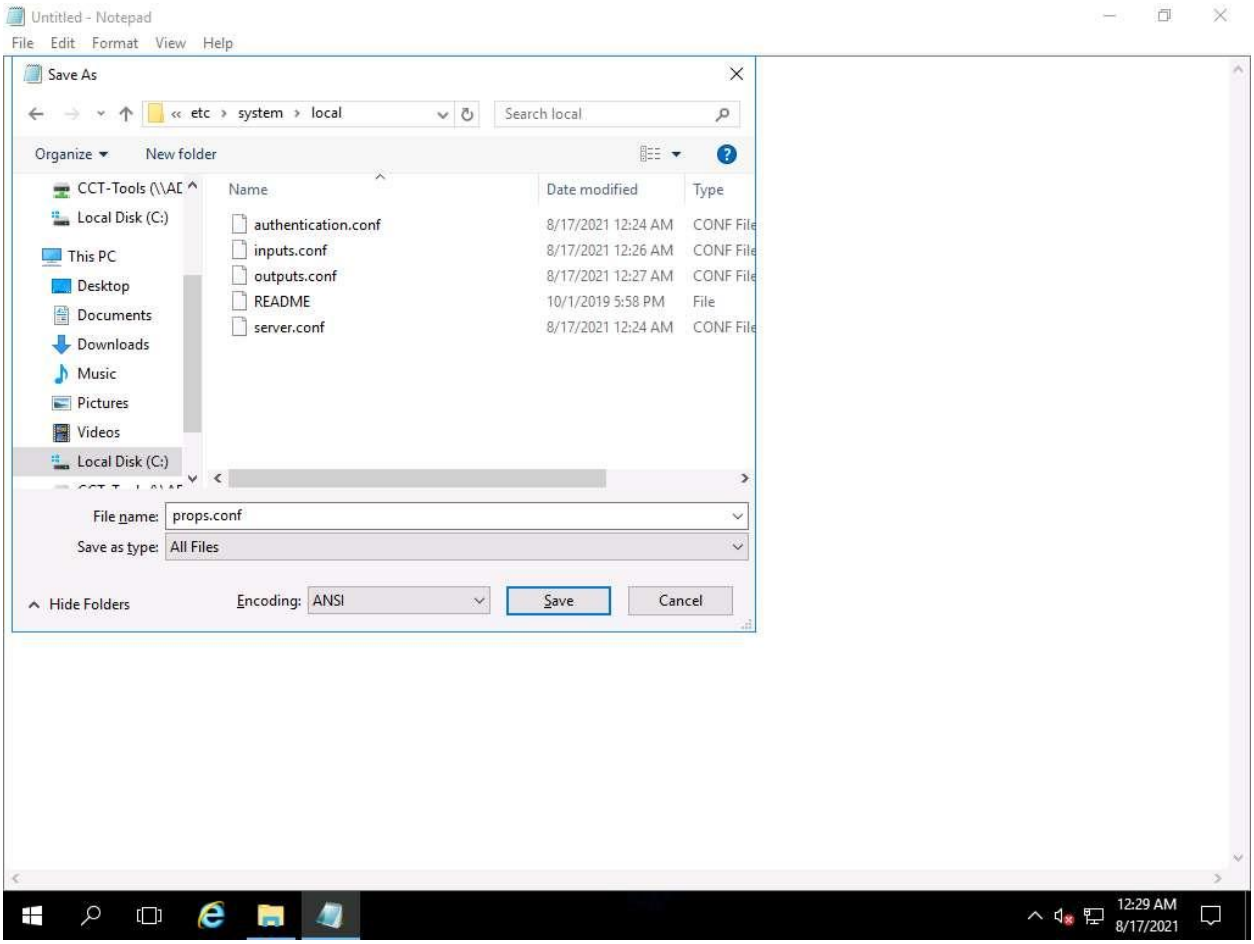
SHOULD_LINEMERGE =False

CHECK_FOR_HEADER

REPORT -iis2 =iis2

72. Save the notepad as props.conf at C:\Program Files\SplunkUniversalForwarder\etc\system\local path and close the file.

Ensure you have selected Save type as: All Files while saving the props.conf file.



73. Open Notepad again, add the following lines in the new opened file and save the file as transforms.conf at C:\Program Files\SplunkUniversalForwarder\etc\system\local.

Ensure you have selected Save type as: All Files while saving the transforms.conf file.

TypeCopy

[default]

host -WebServer

[ignore_comments]

REGEX = ^#.*

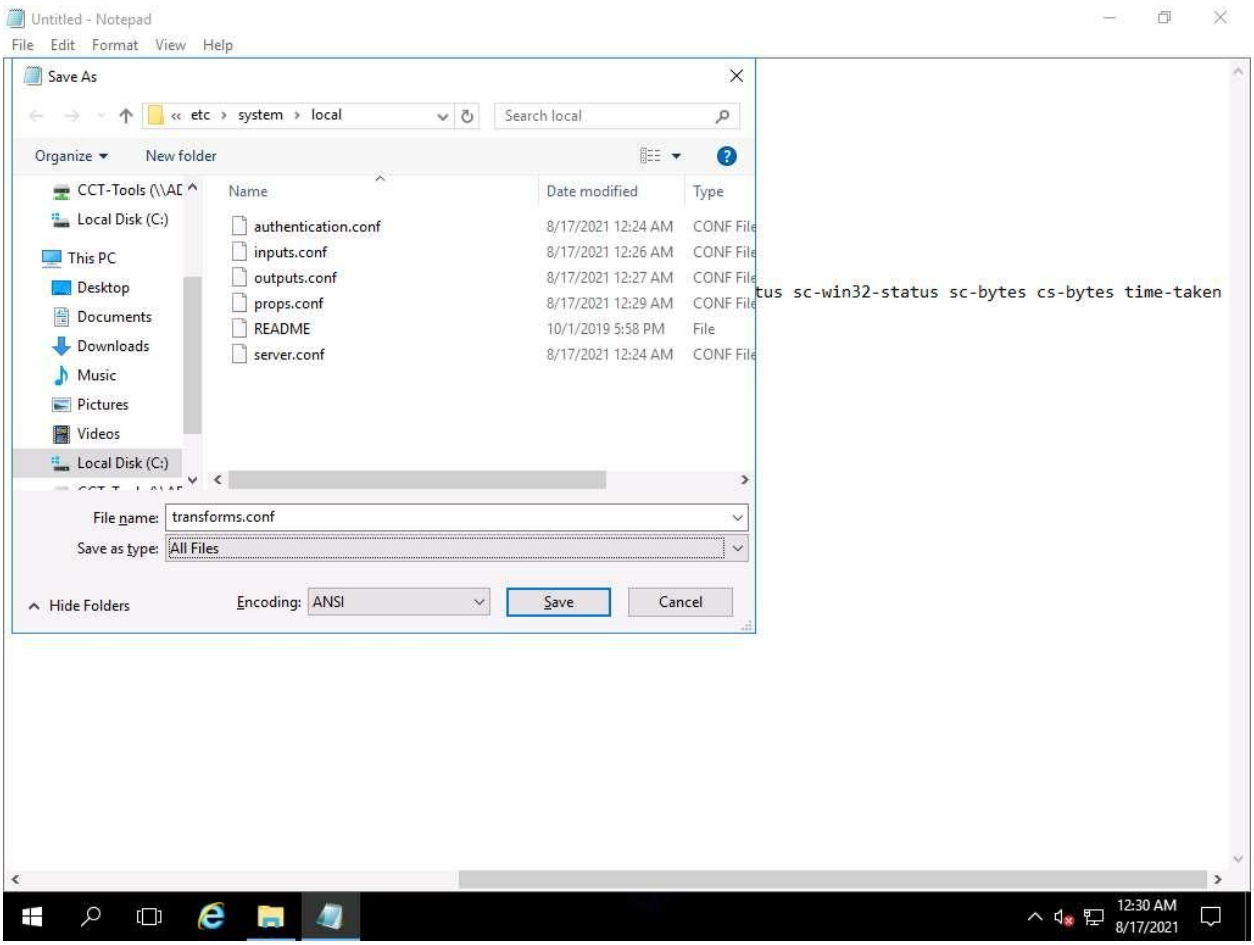
DEST_KEY =queue

FORMAT =nullQueue

[iis2]

DELIMS =" "

FIELDS = date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken



74. To forward the Suricata logs, navigate to the C:\Program Files\SplunkUniversalForwarder\etc\system\local folder and open inputs.conf file Edit with Notepad++. Add the following configuration lines of code at the end of the file and Save. Close the file.

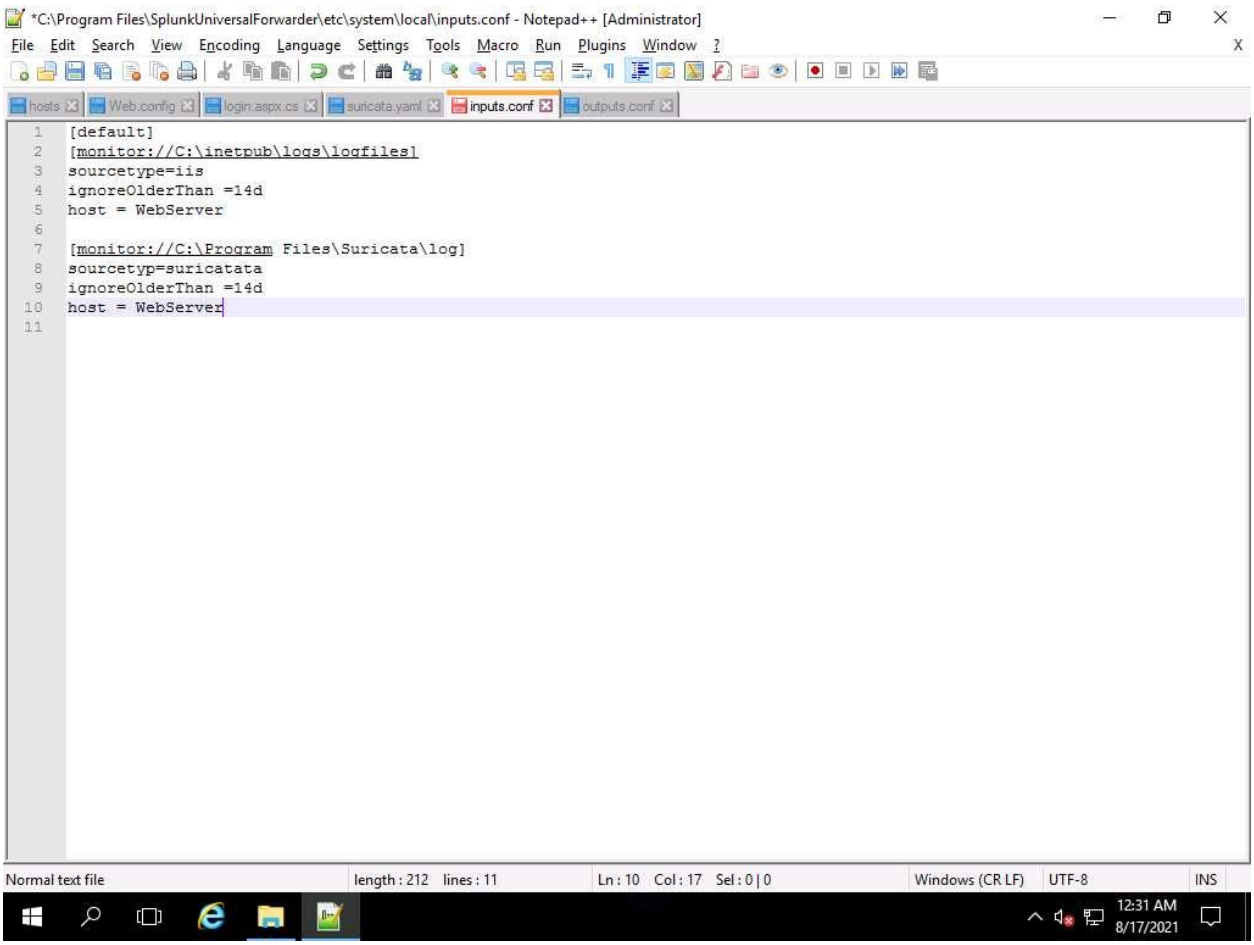
TypeCopy

[monitor*://C:\Program Files\Suricata\log]*

sourcetyp=suricatata

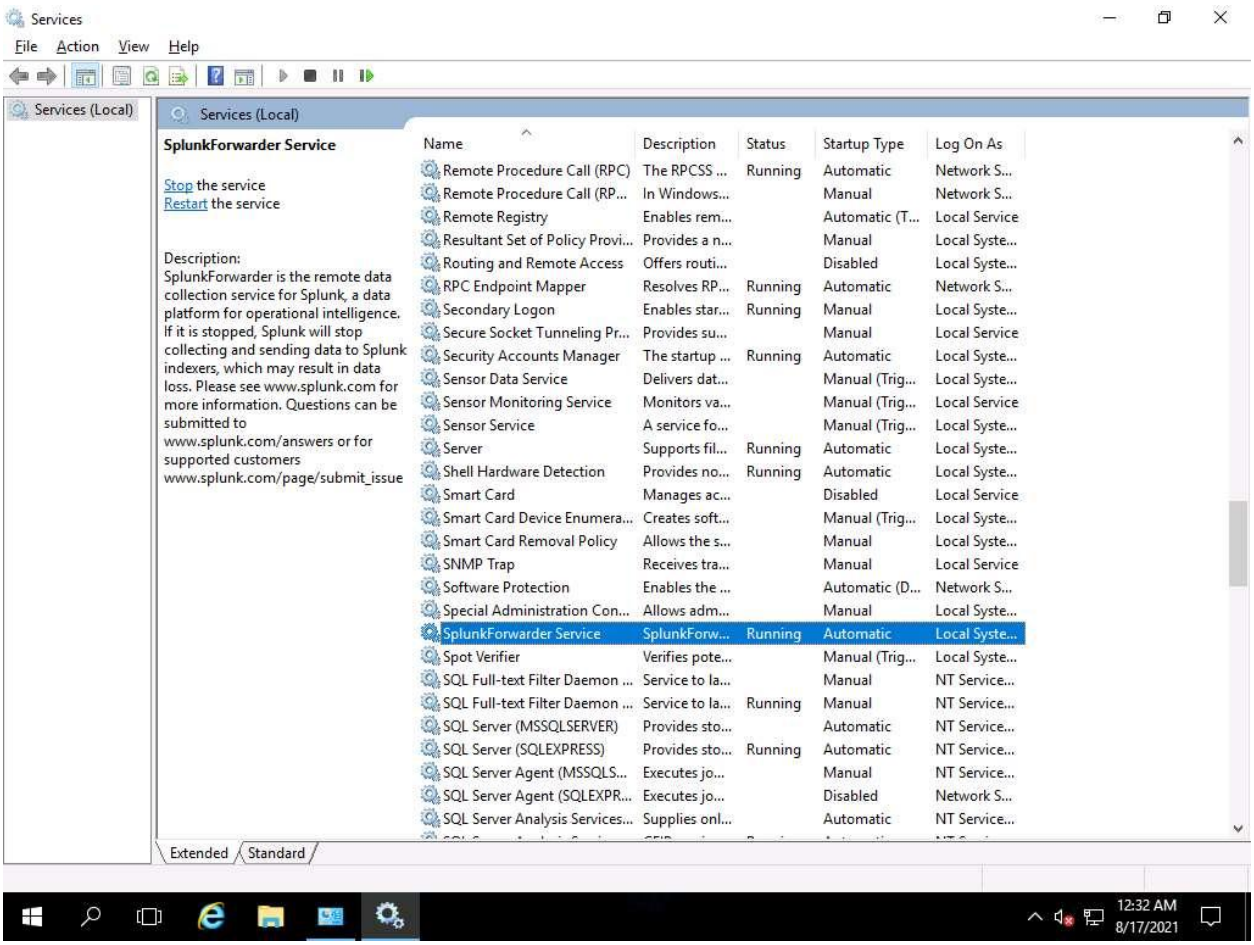
ignoreOlderThan =14d

host = WebServer

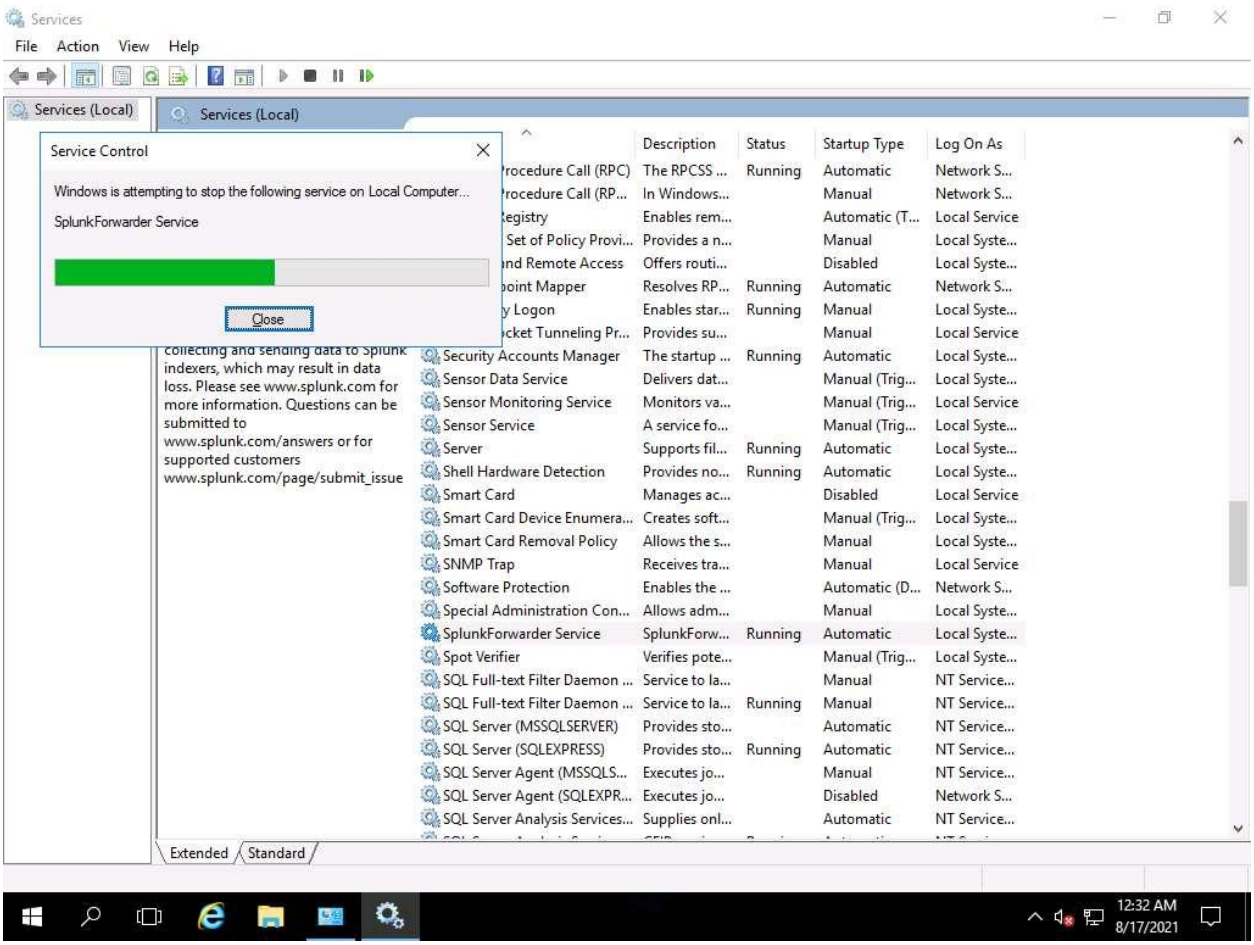


75. Close all open files in Notepad.

76. Navigate to Windows Start -> Administrative Tools. Double-click on Services in the Administrative Tools window. The services window opens, search for SplunkForwarder Service.

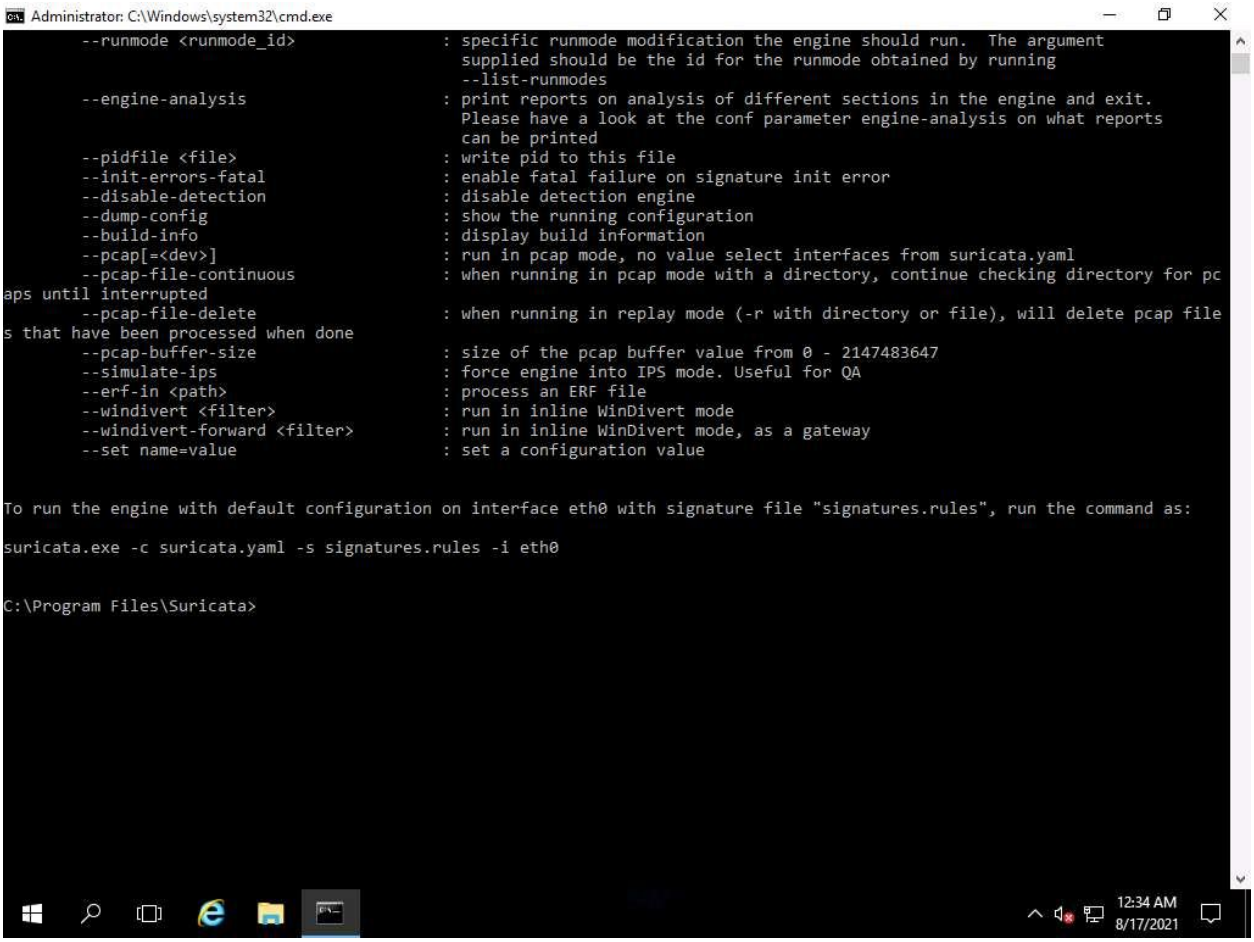


77. Click on SplunkForwarder Service, and then Restart the service. If an error occurs while restarting, click Start again.

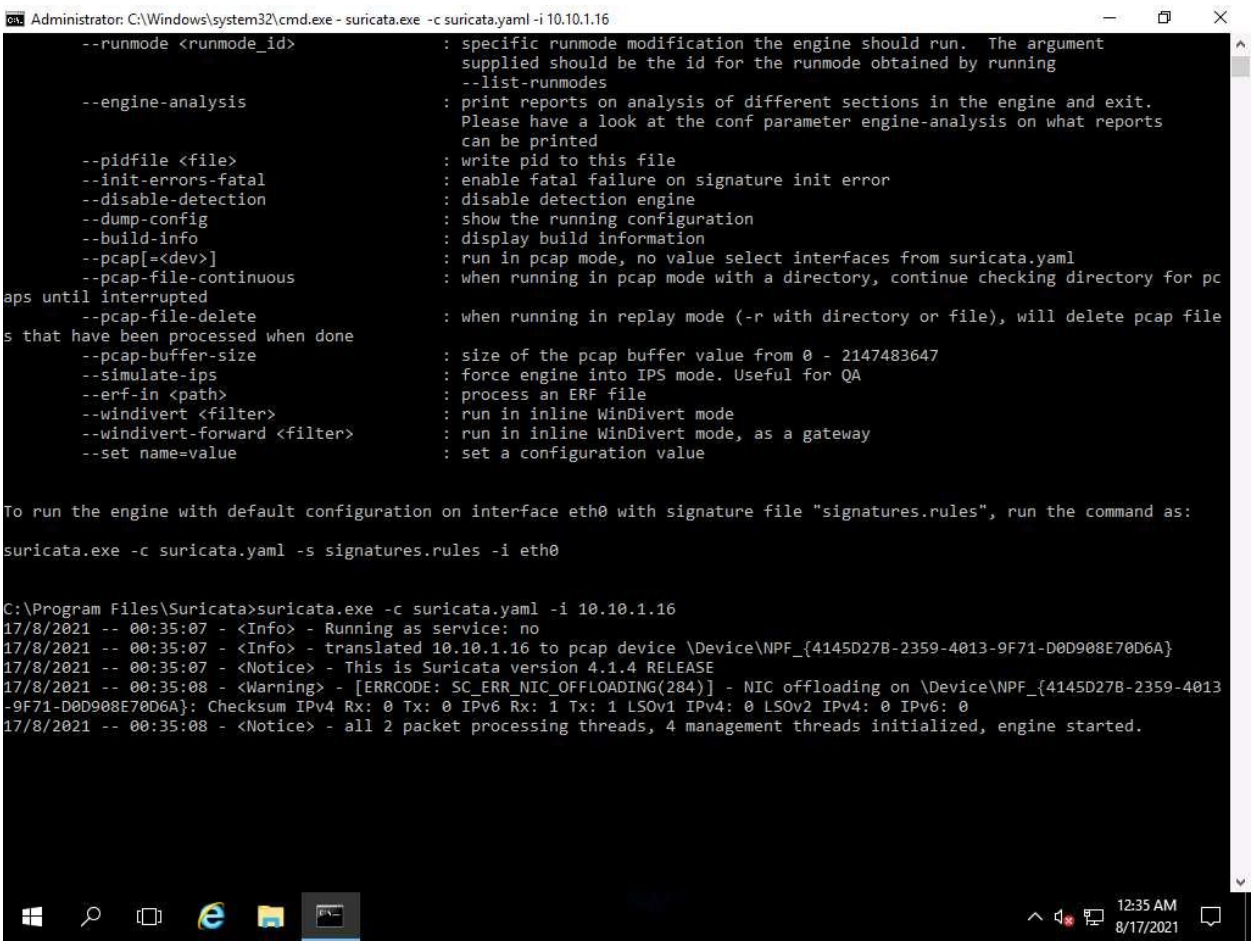


78. Next, launch Suricata to capture the network traffic, navigate to the desktop, and double click the Suricata-4.1.4-64bit IDS-IPS shortcut.

79. The Suricata Command Prompt will open.



80. Type the suricata.exe -c suricata.yaml -i 10.10.1.16 command to run Suricata for capturing network traffic, and press Enter.



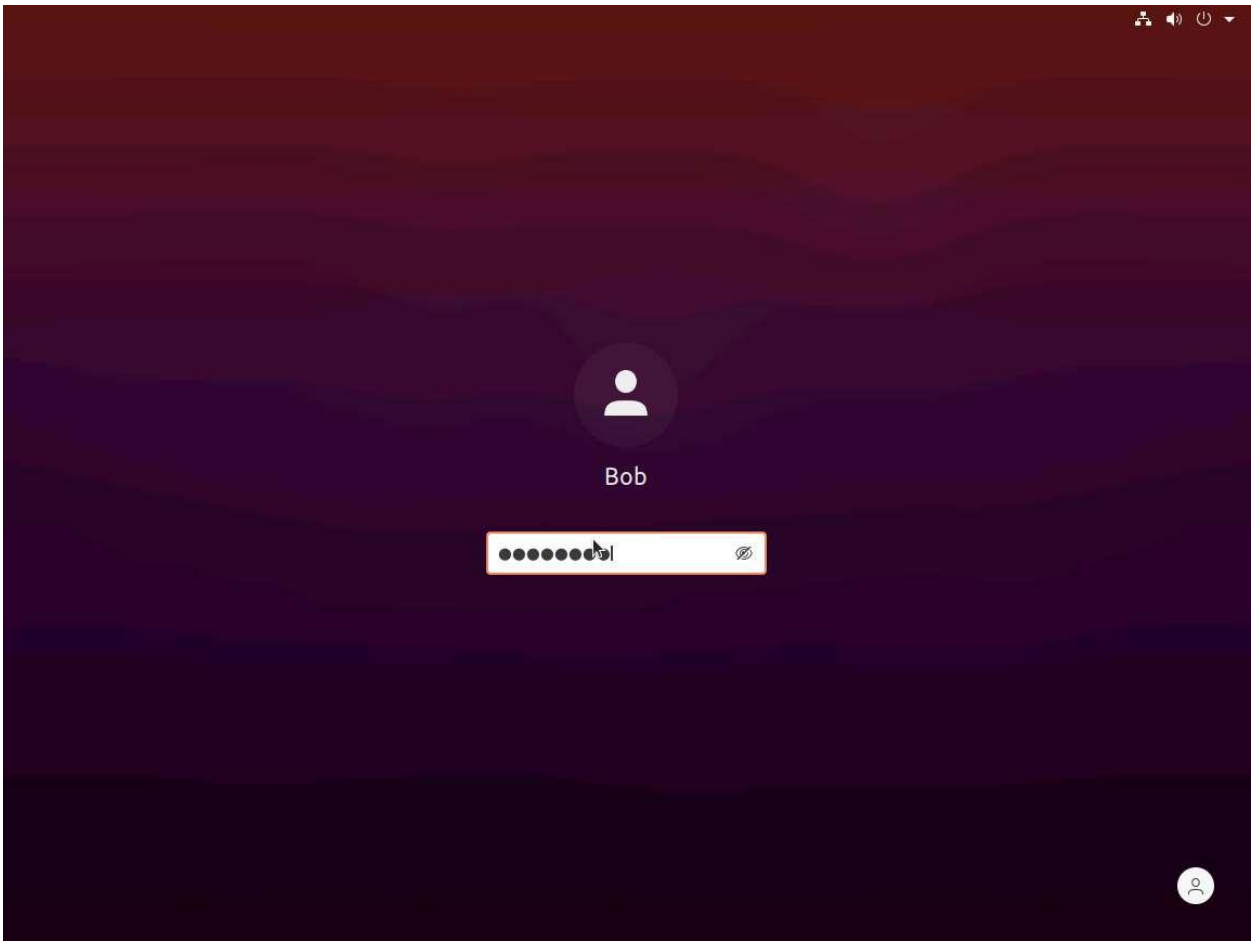
81. The Suricata engine will start. Leave the command prompt open and Suricata running.

82. We need to perform the attack from the attacker machine to the Web Server. Suricata will then generate the alert and store it in the fast.log file.

83. The fast.log file is the default alert log file that is already set into the suricatata.yaml file.

84. Click Attacker Machine-1 to switch to the Attacker Machine-1 machine.

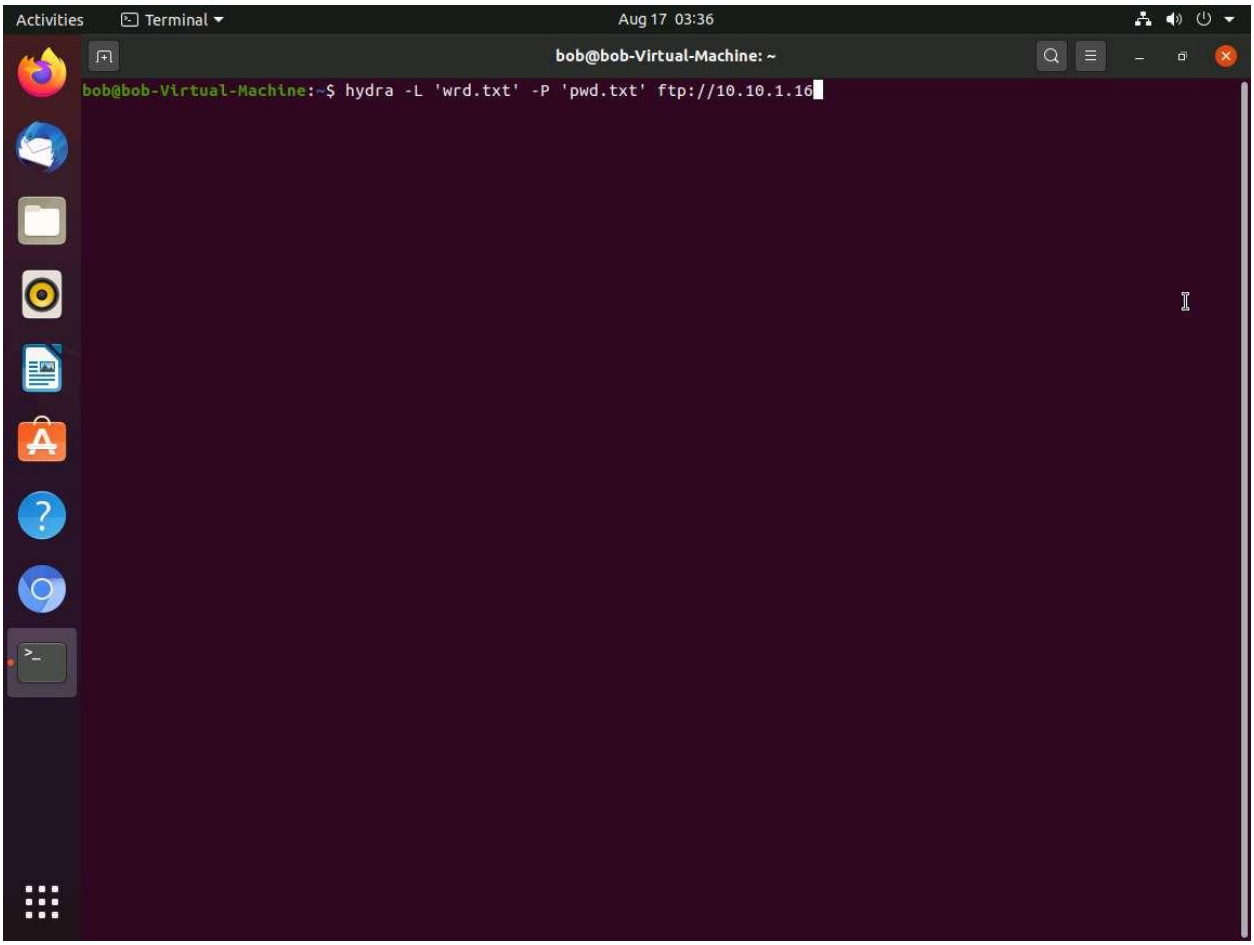
85. Select username as Bob and type password as user@123 and press Enter.



86. To perform a brute-force attack, use the tool Hydra from Ubuntu OS (Attacker Machine).

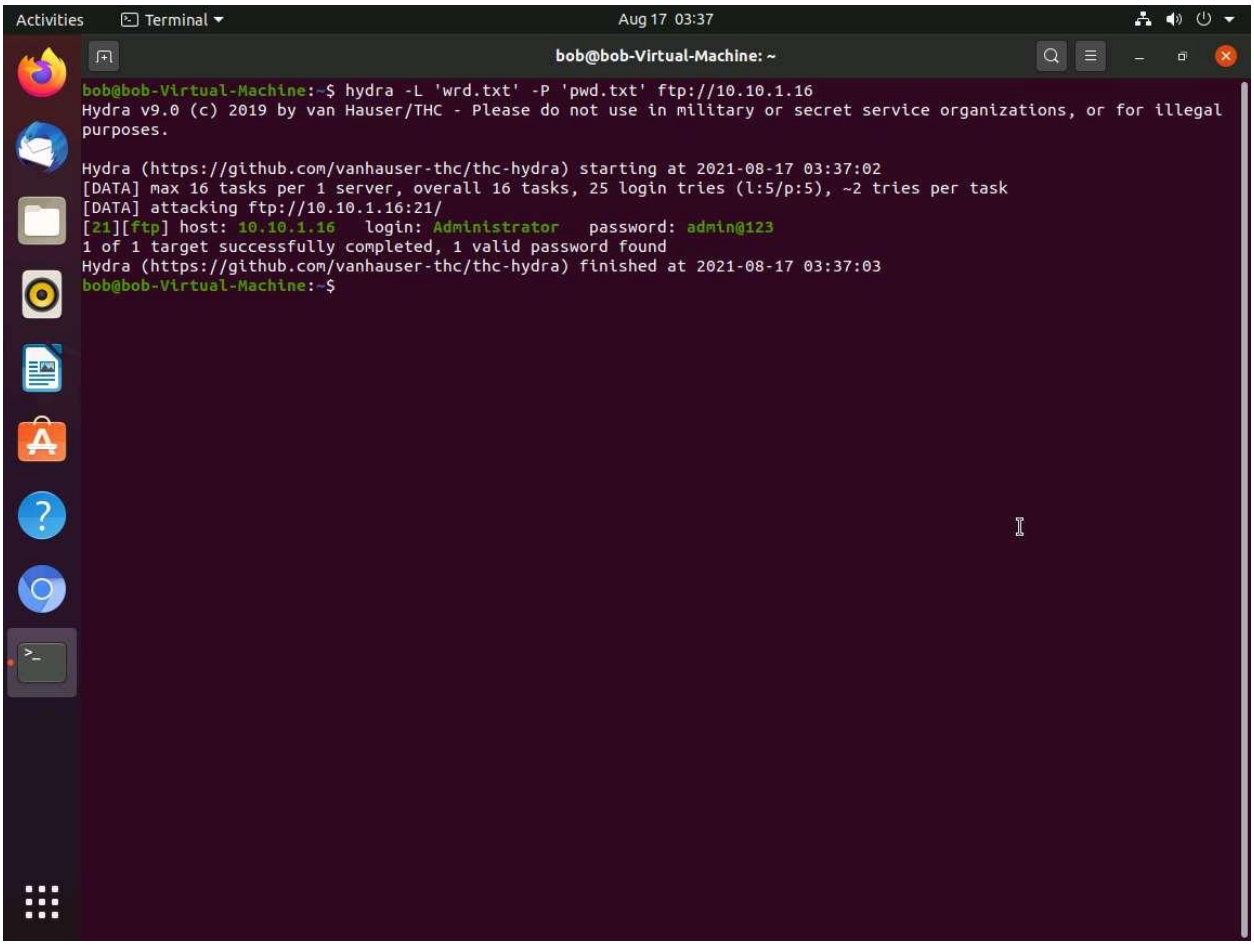
Hydra uses two files for performing a brute-force attack. The first file has the list of usernames, and the second file has a list of passwords. Hydra uses these lists of usernames and passwords for performing a brute-force attack.

87. Press Ctrl + Alt + T to open the terminal, type hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16, and press Enter.

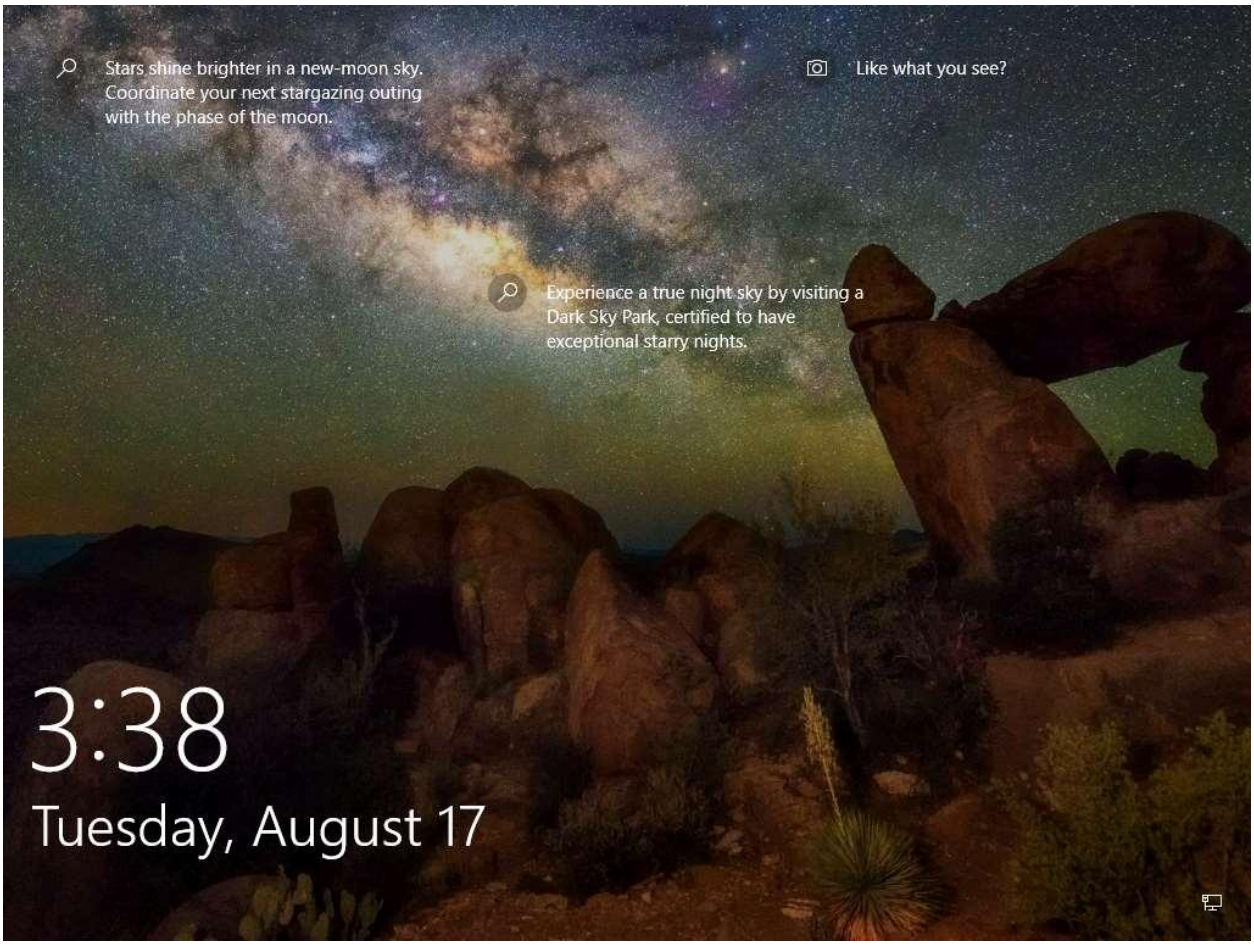


88. The Attacker Machine-1 will try to match the combination of usernames and passwords with the Web Server.

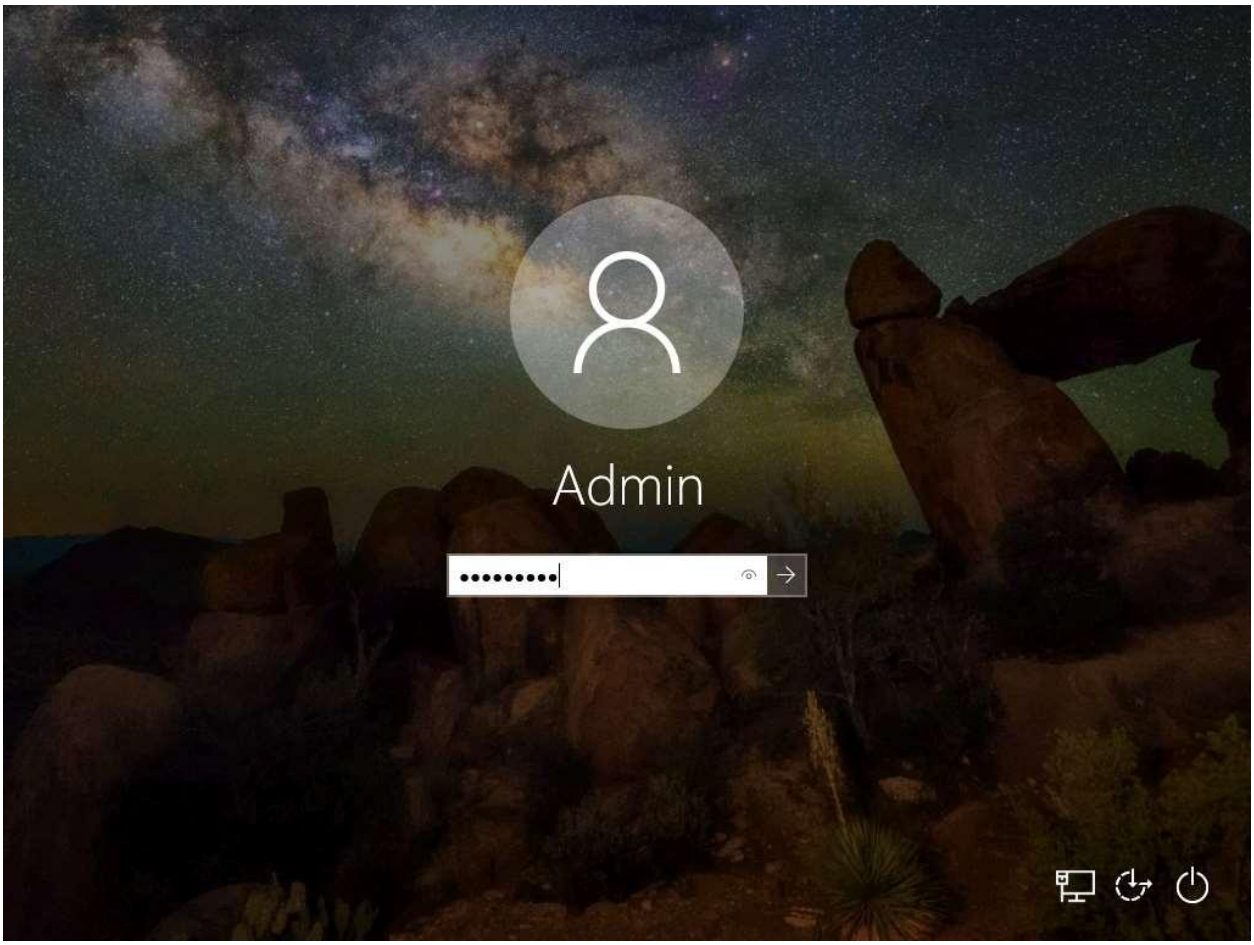
89. The matched username and password are shown in the terminal in green color. Close the terminal window.



90. After the attack is complete, click Admin Machine-1 to switch to the Admin Machine-1 machine. Click Ctrl+Alt+Delete Link to login.

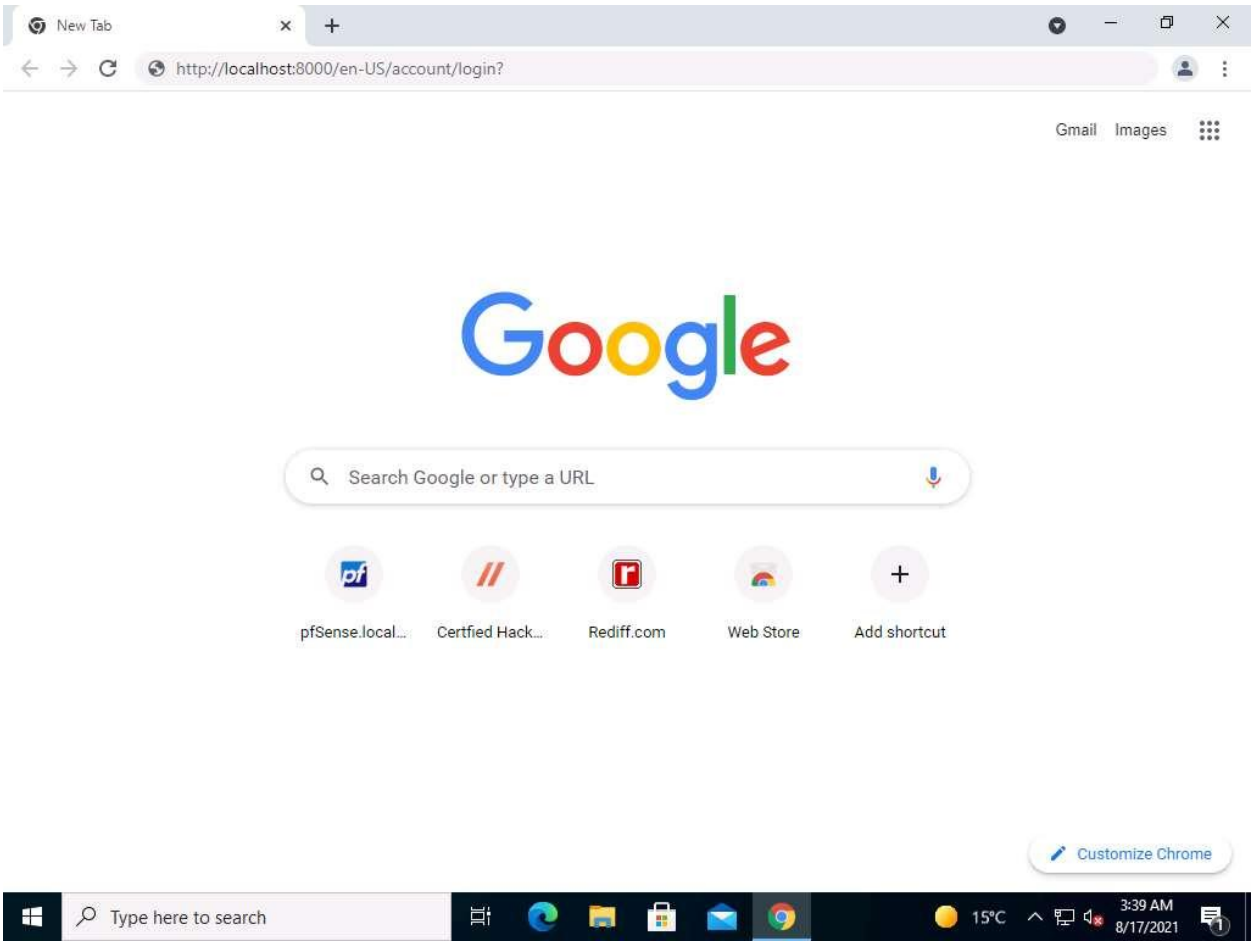


91. By default, the username Admin is selected. Type password admin@123 and press Enter.

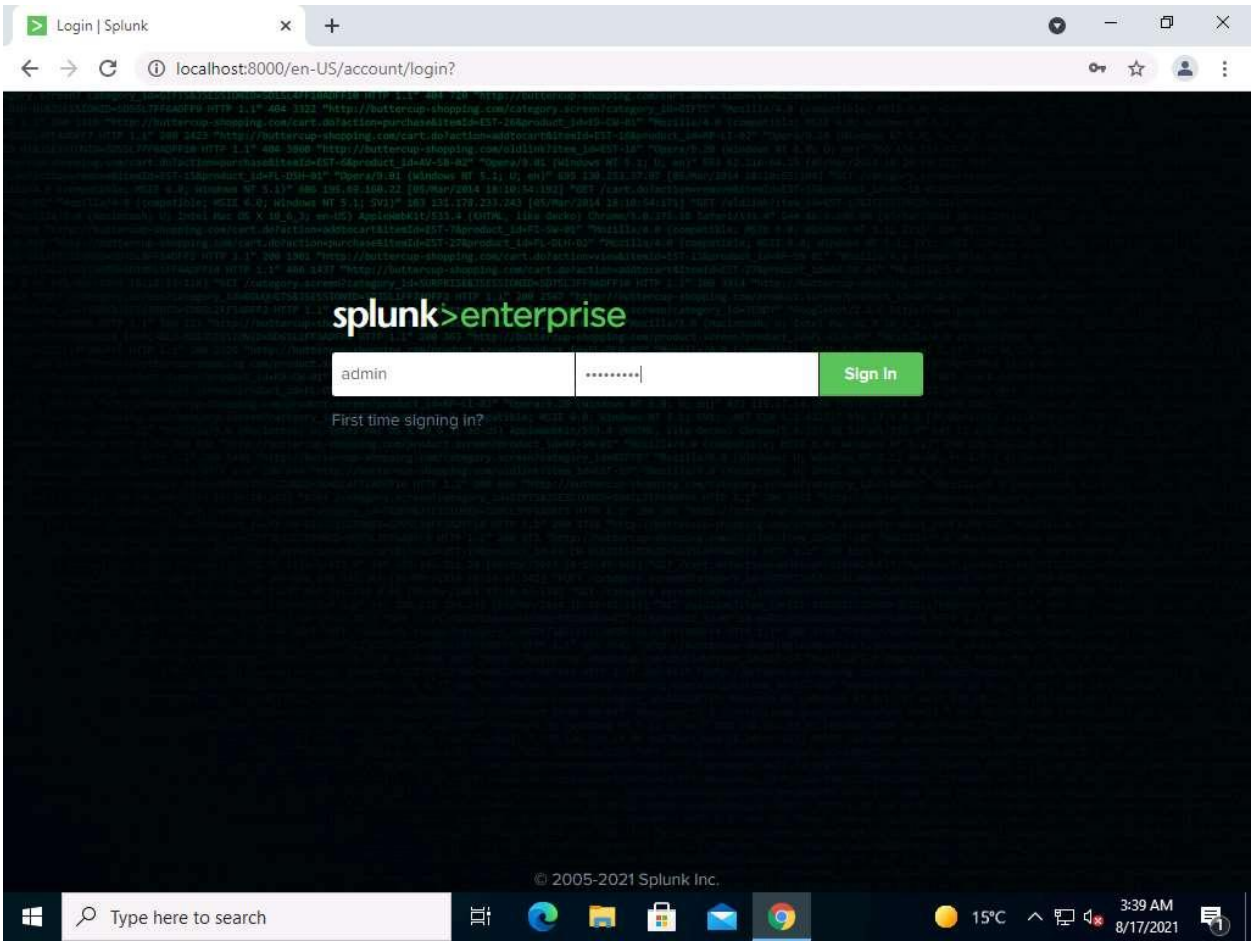


If the network screen appears, click Yes.

92. Launch the web browser, and access Splunk Enterprise with the URL http://localhost:8000/en-US/account/login? and press Enter.



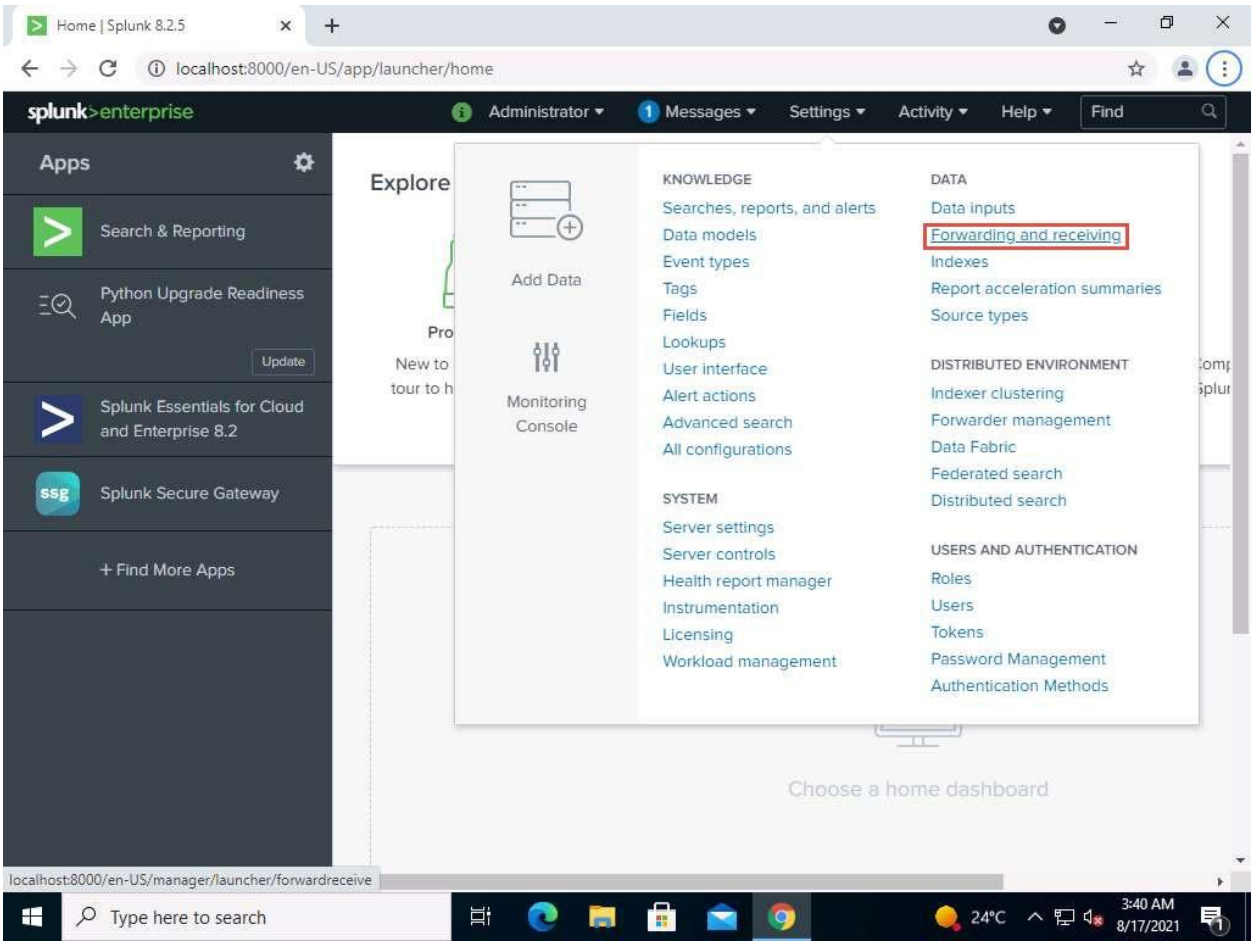
93. Log in with the username admin and password admin@123



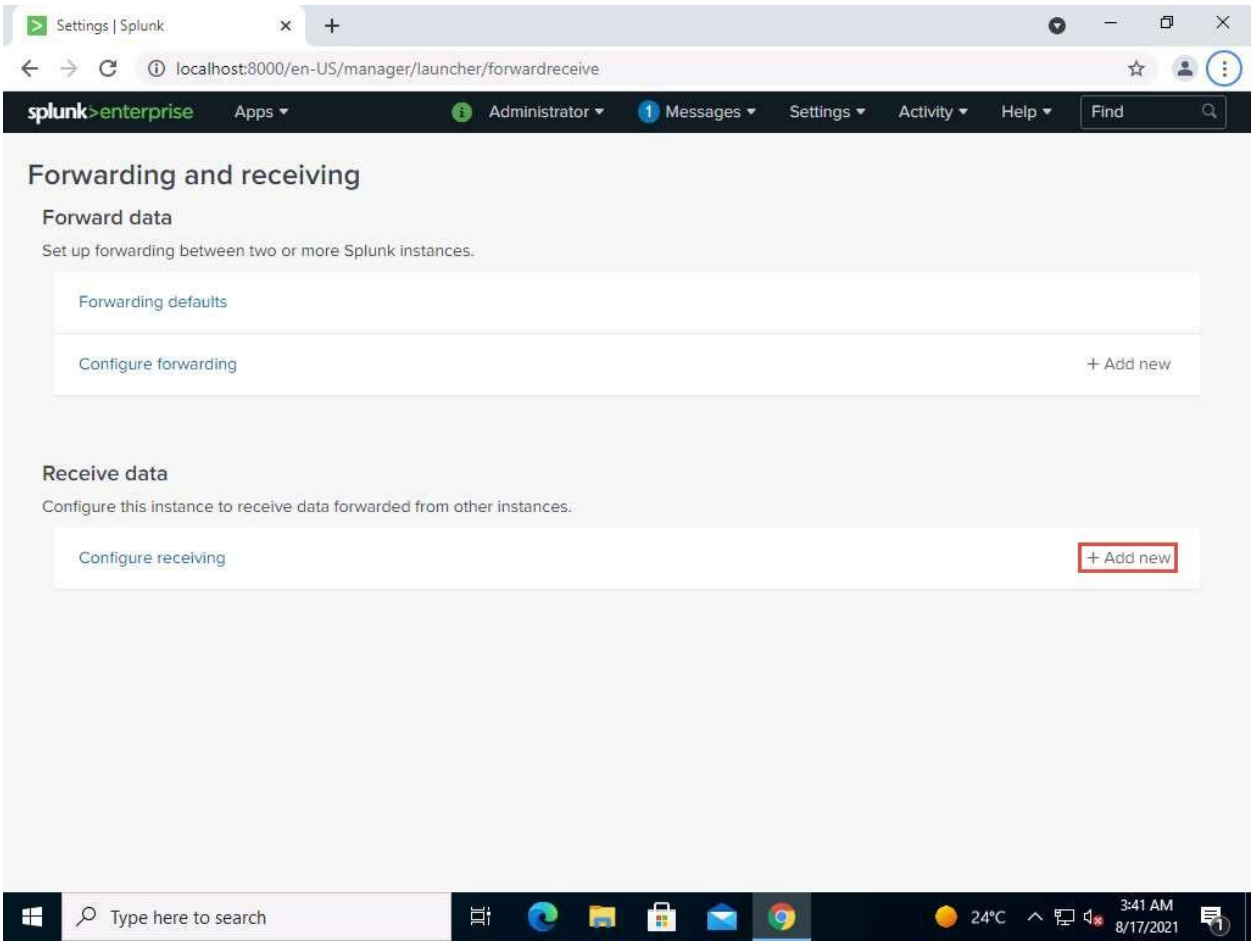
If the Splunk Enterprise page is not opening, make sure the splunkd service is running. If not, then press "Windows+R" on your keyboard and type "services.msc". Click on OK. Next, the Services window opens. Search for the splunkd service and restart. Wait for the service to start.

If Important Changes coming! pop-up appears, click Don't show me this again.

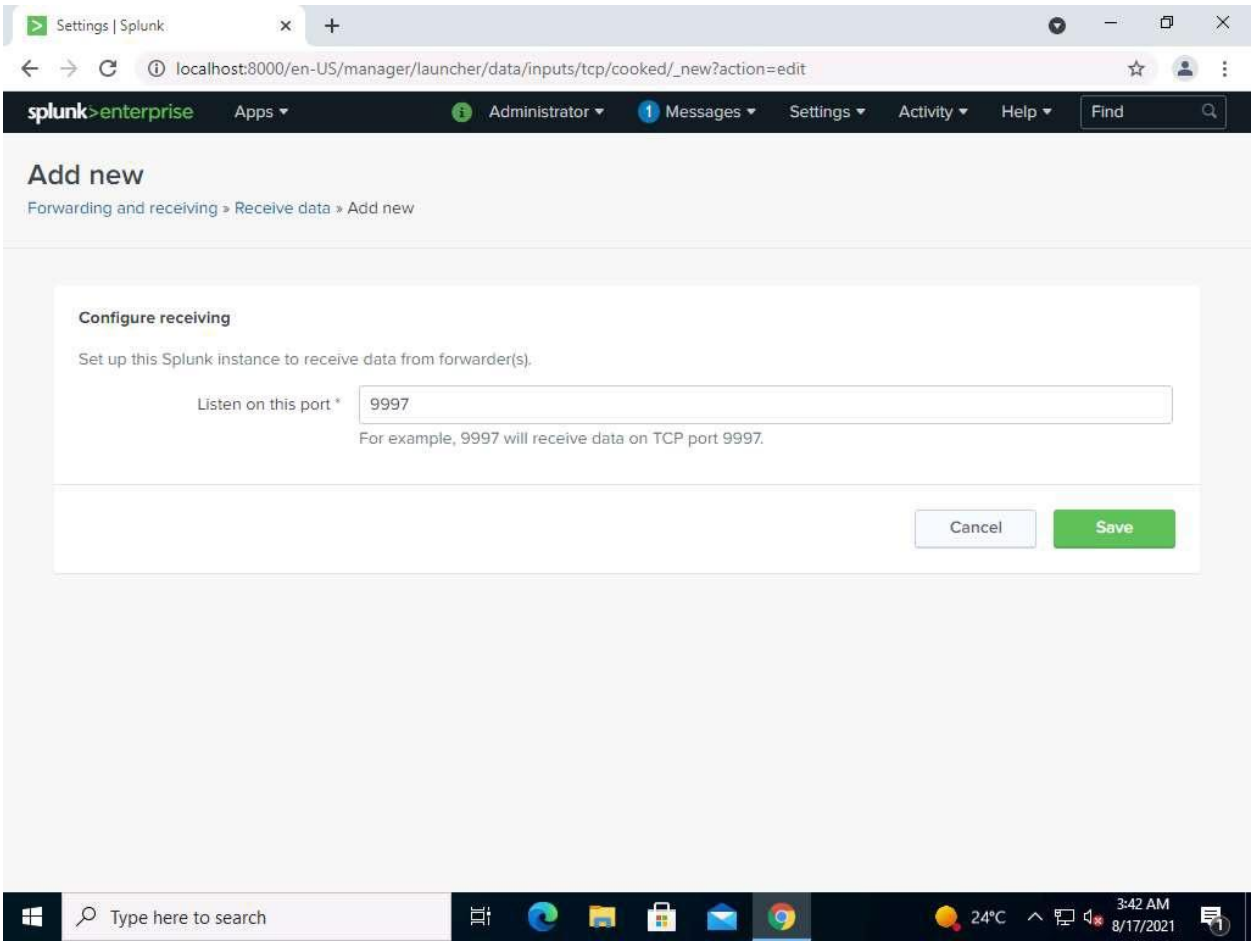
94. The Splunk web console appears; click Settings menu, select Forwarding and receiving link under the DATA section.



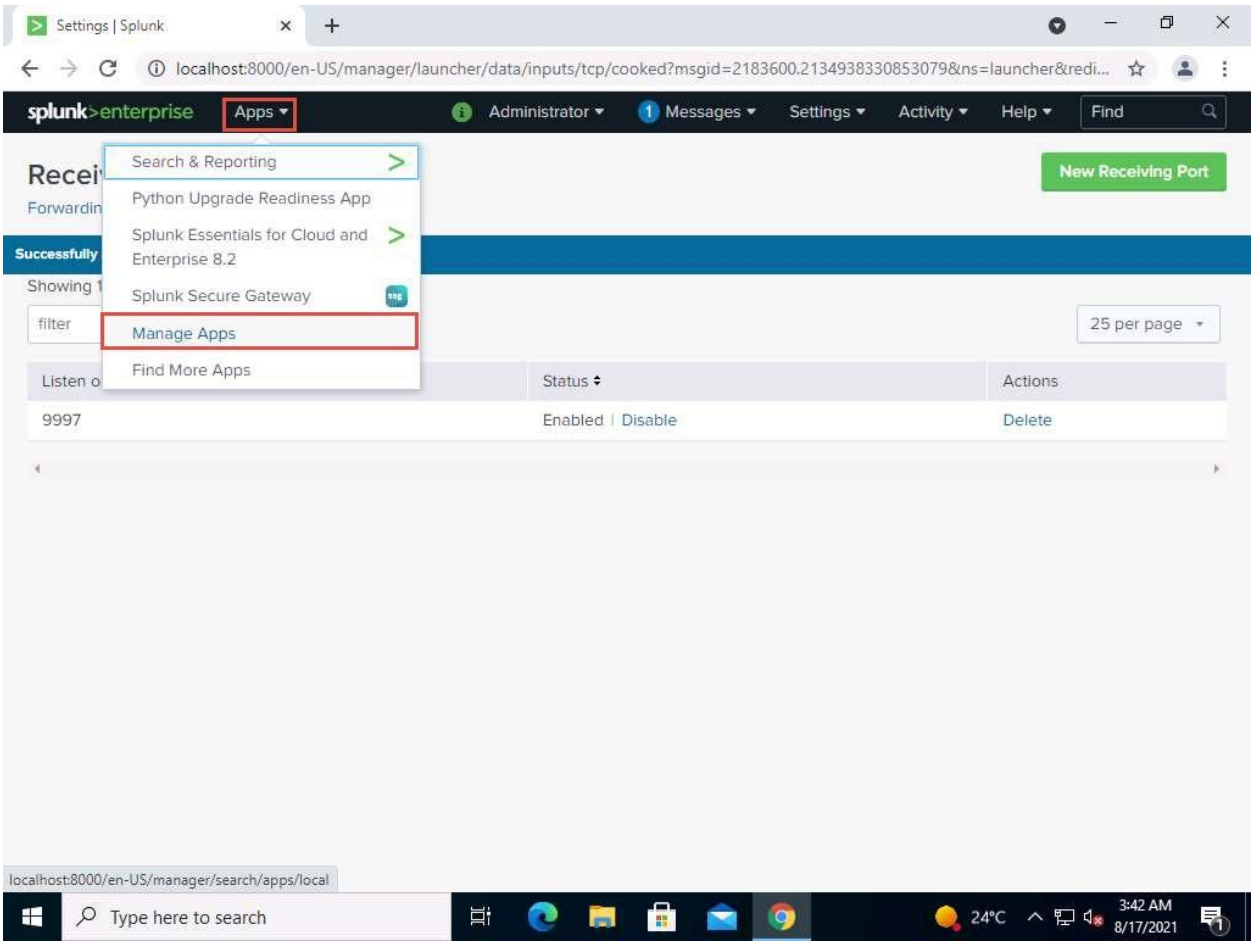
95. The Forwarding and receiving console will appear. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click on the +Add new link in the bottom right corner to Configure receiving.



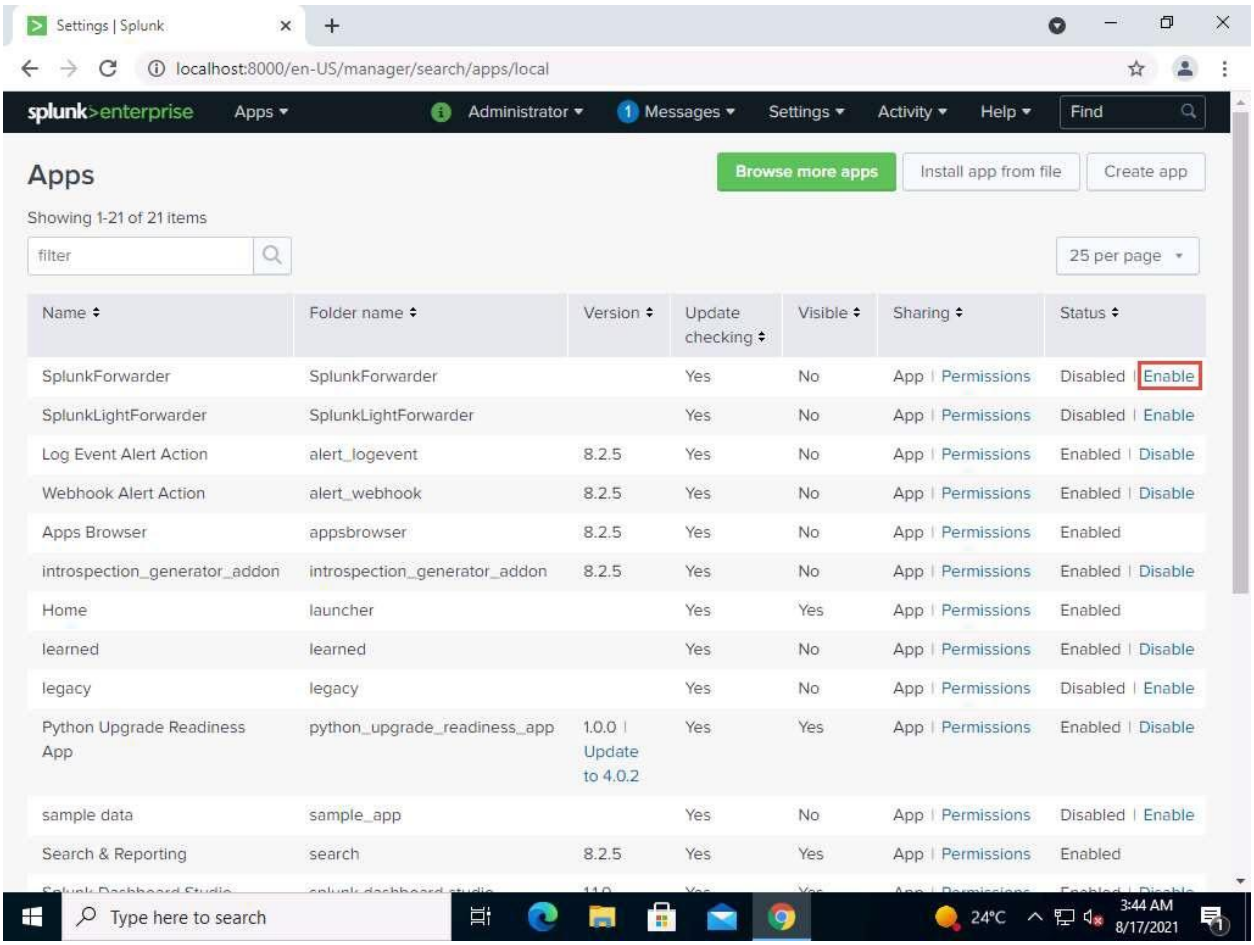
96. The Add new console appears; in the Listen on this port* field, type 9997 and click on Save.



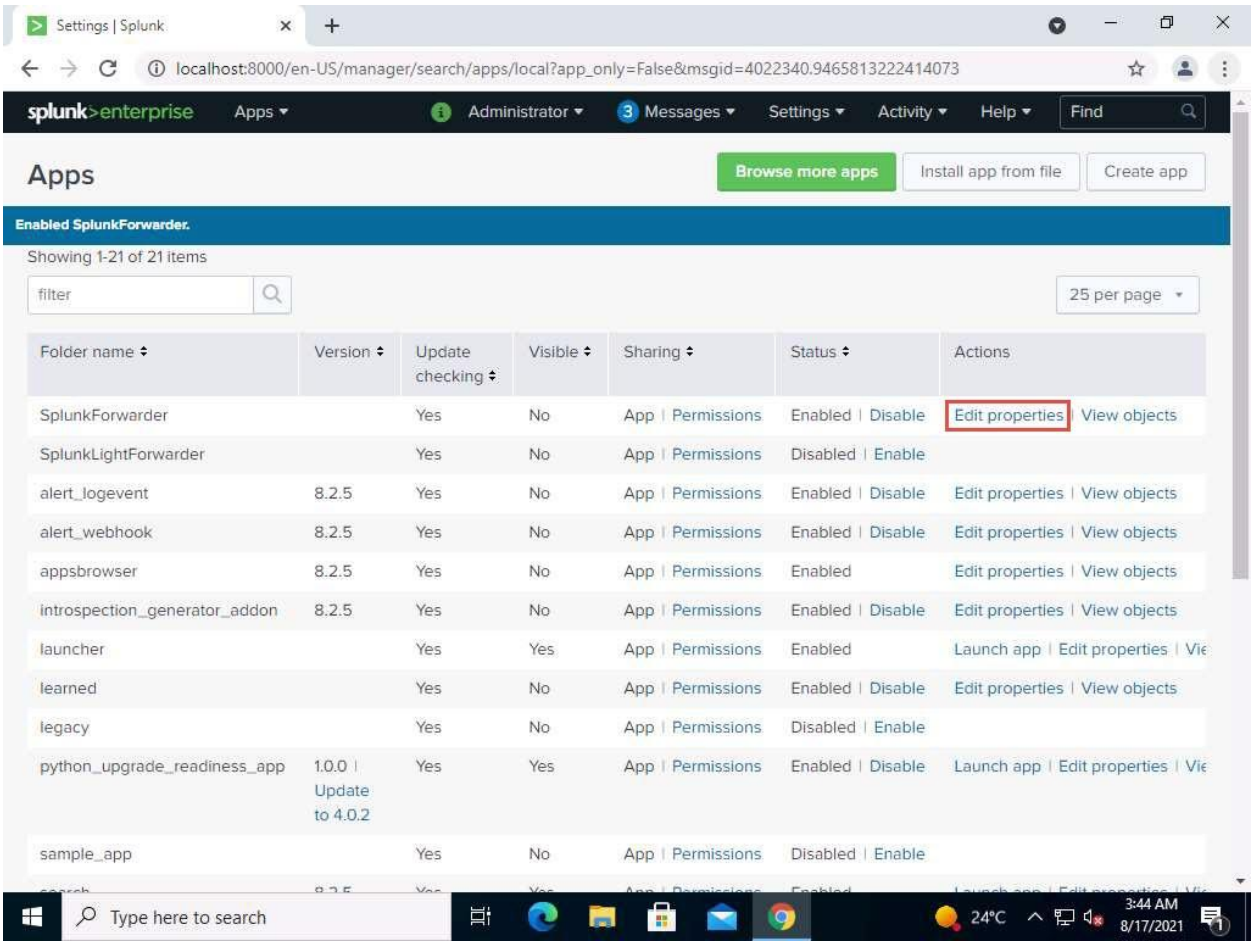
97. Once the port is added, go to Apps menu, and then select Manage Apps.



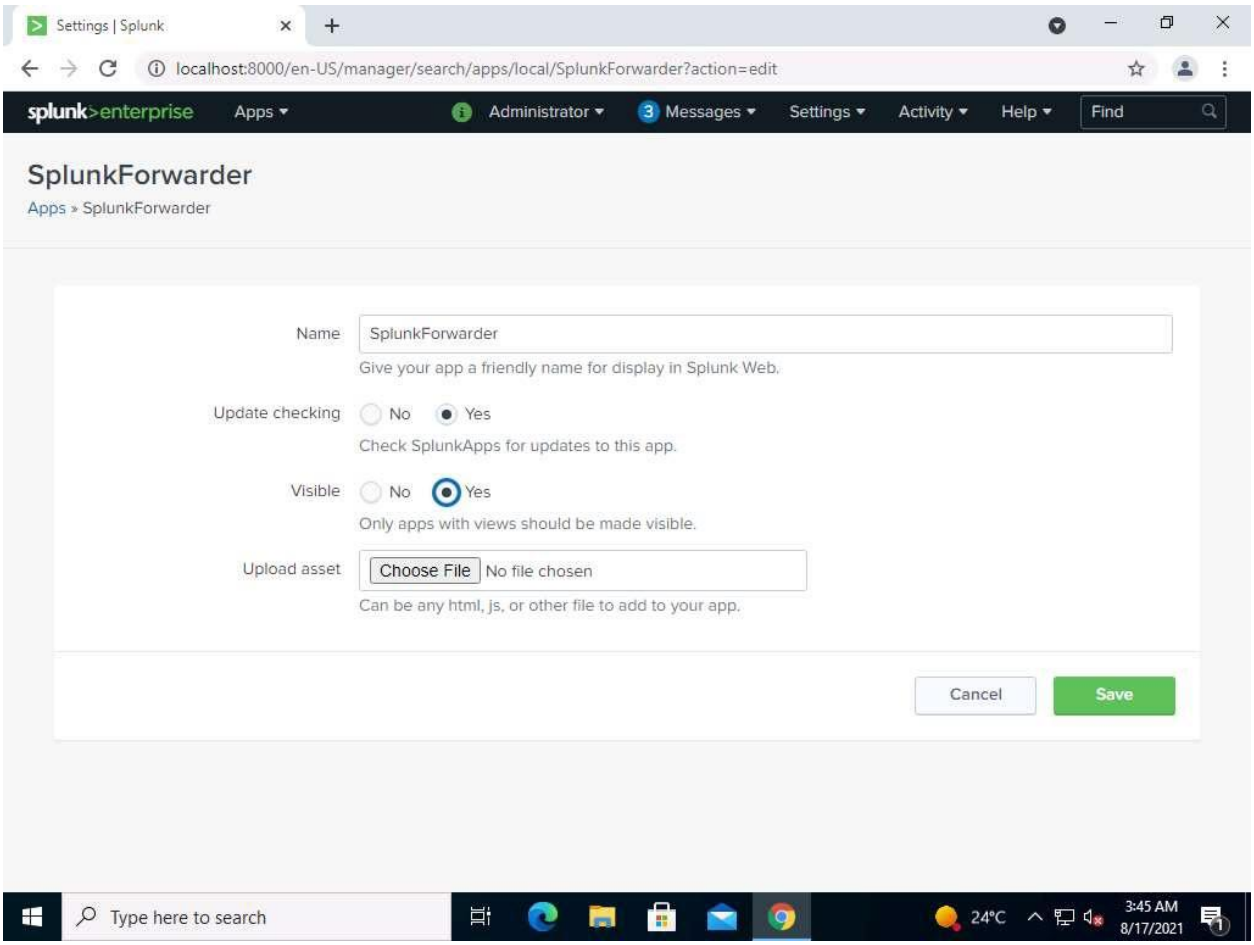
98. The Apps console appears; click on the Enable link toward the extreme right associated with the SplunkForwarder application.



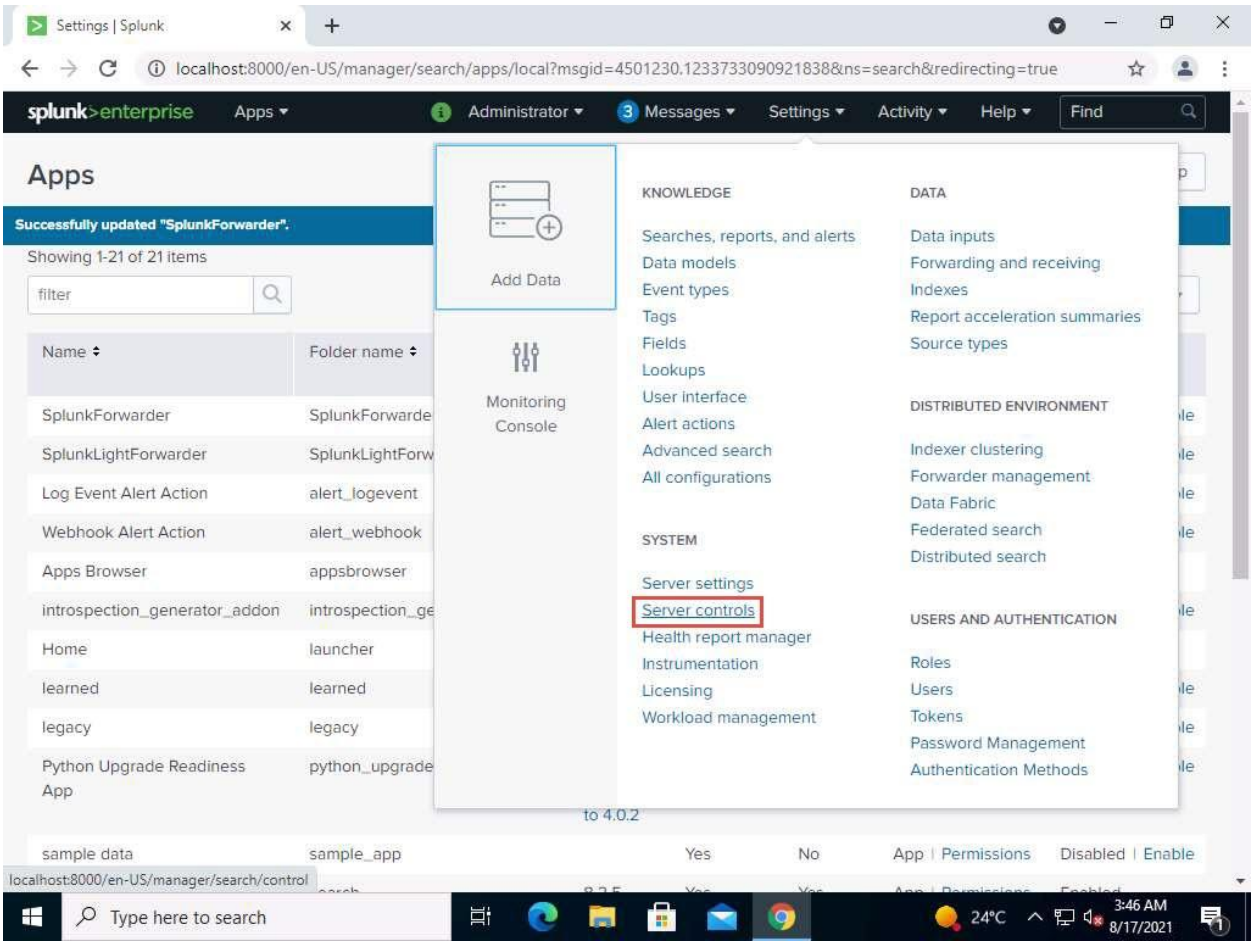
99. When the application is enabled, click on Edit properties under Actions column associated with SplunkForwarder.



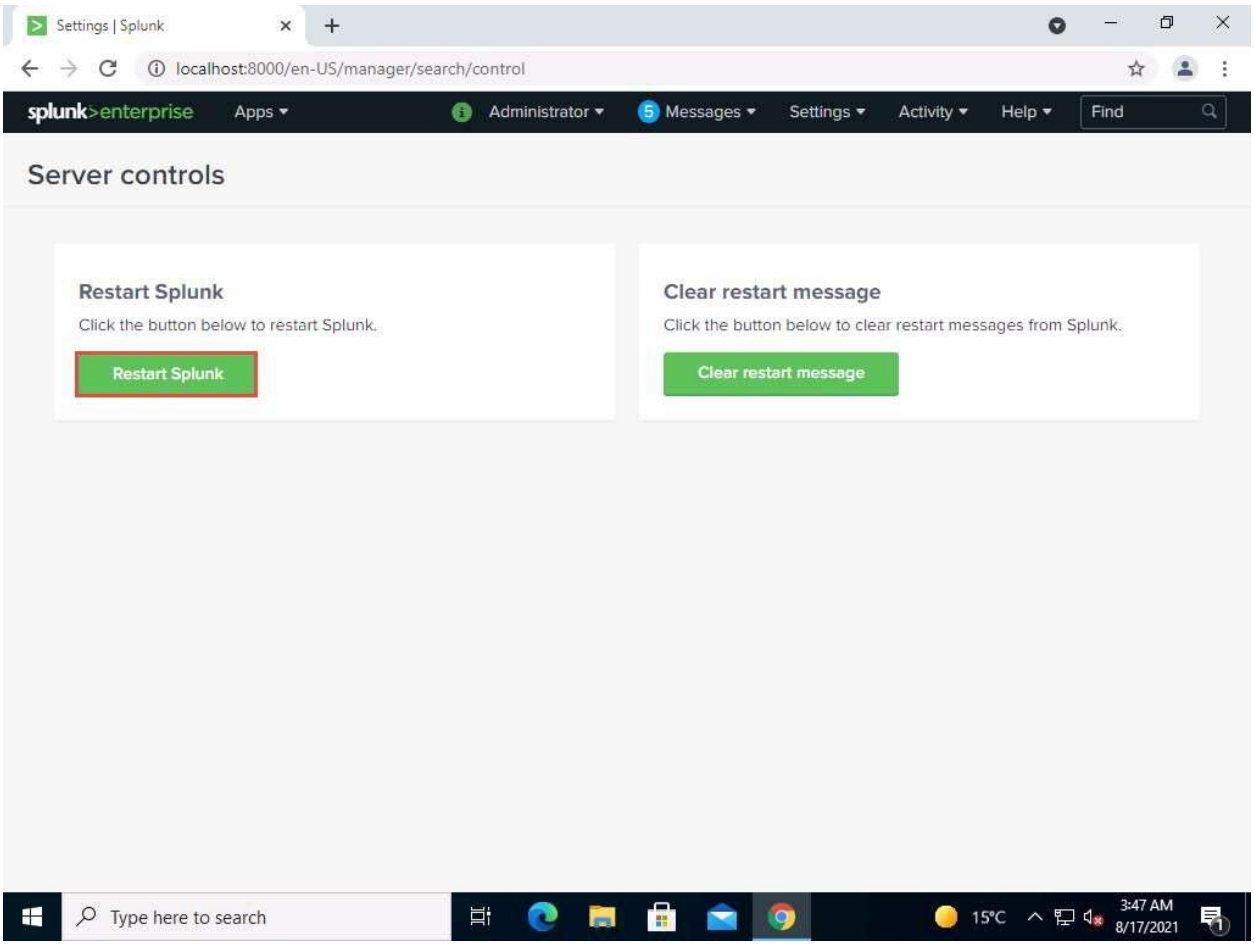
100. The SplunkForwarder console appears; click on Yes under the Visible section, and then on Save.



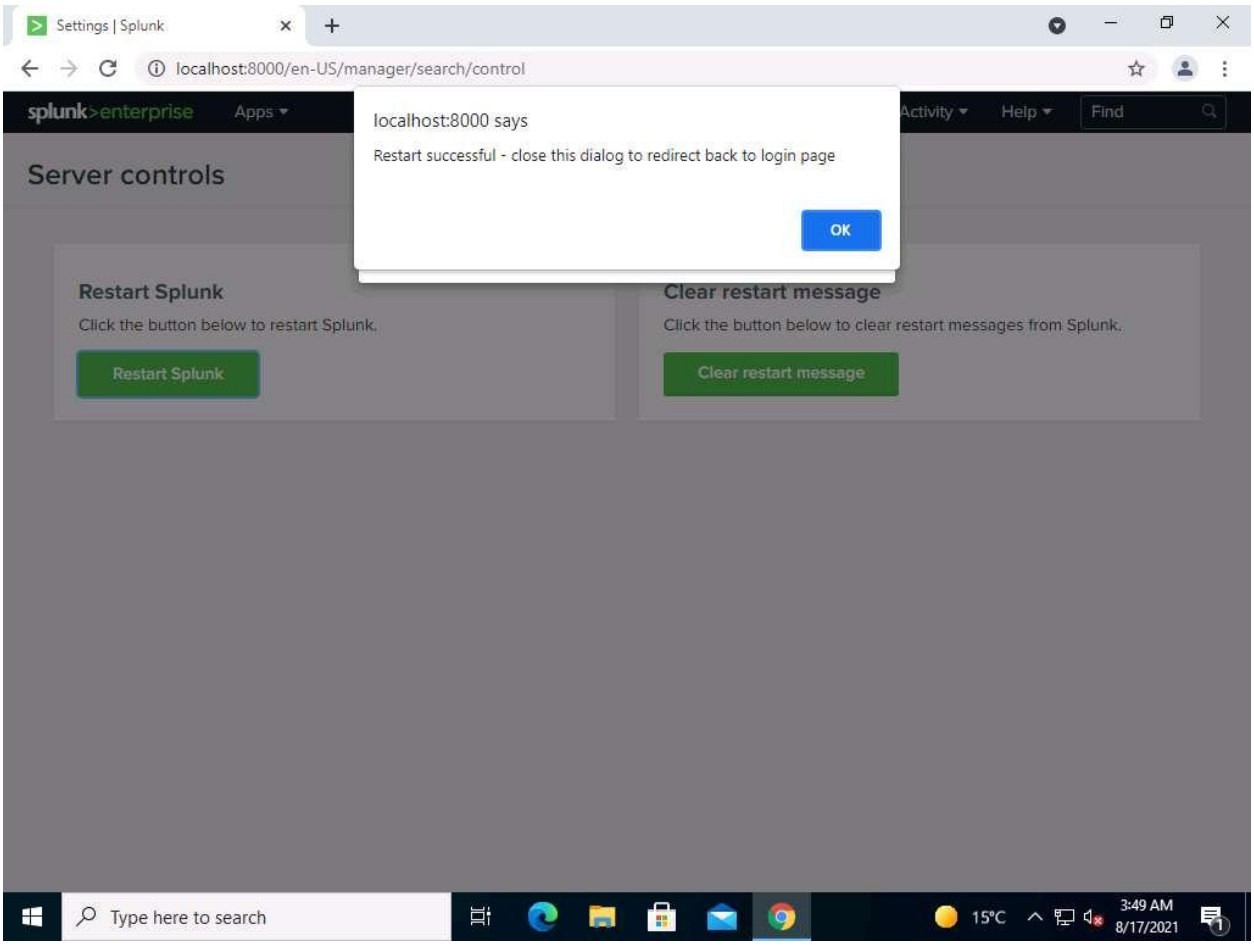
101. Go to Settings and select Server controls under the SYSTEM section.



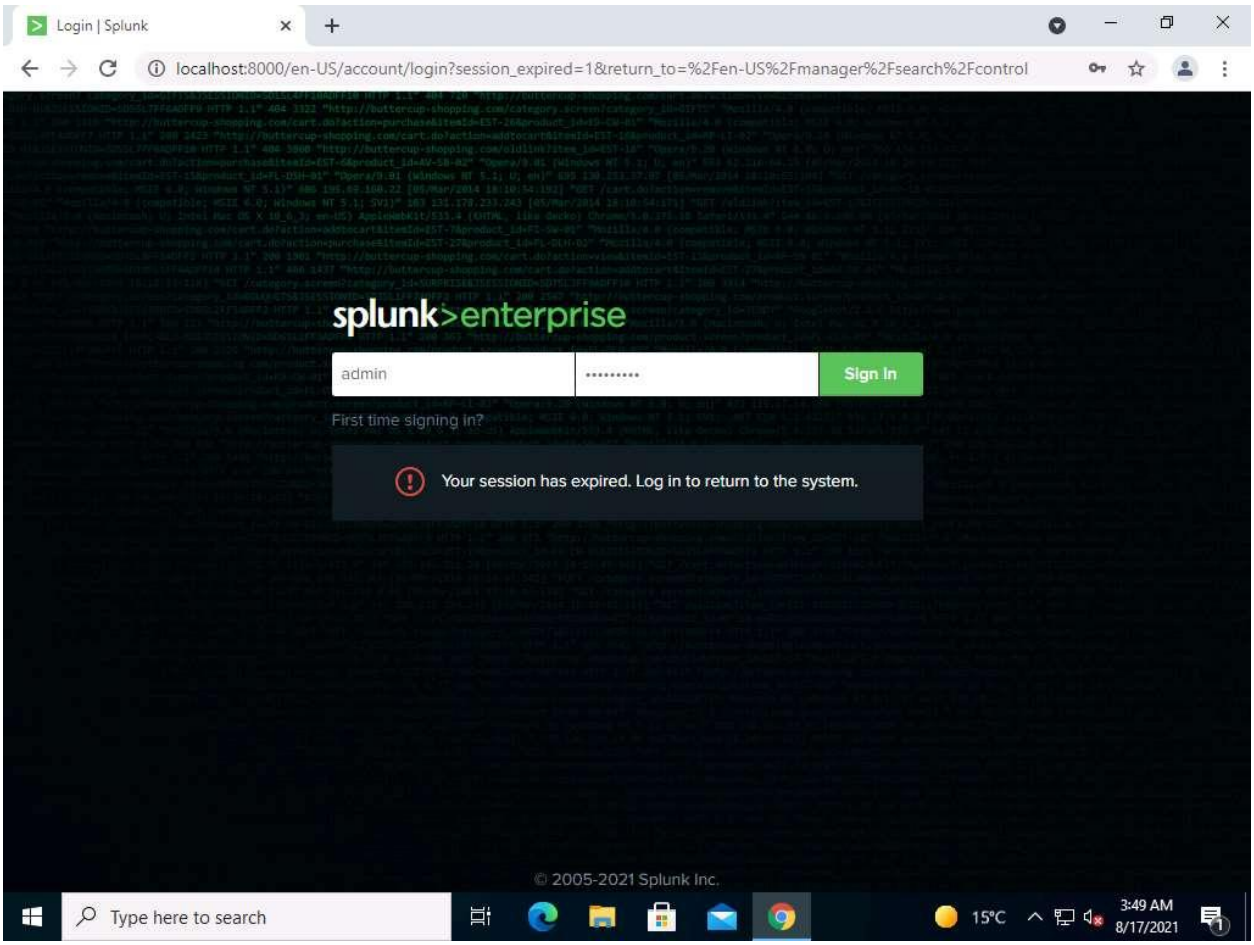
102. The Server controls console appears; click on Restart Splunk. A confirmation pop-up appears; click on OK.



103. Wait for few seconds, on a successful restart, a pop-up appears with the message “Restart successful. Click OK to log back into Splunk. Click on OK.

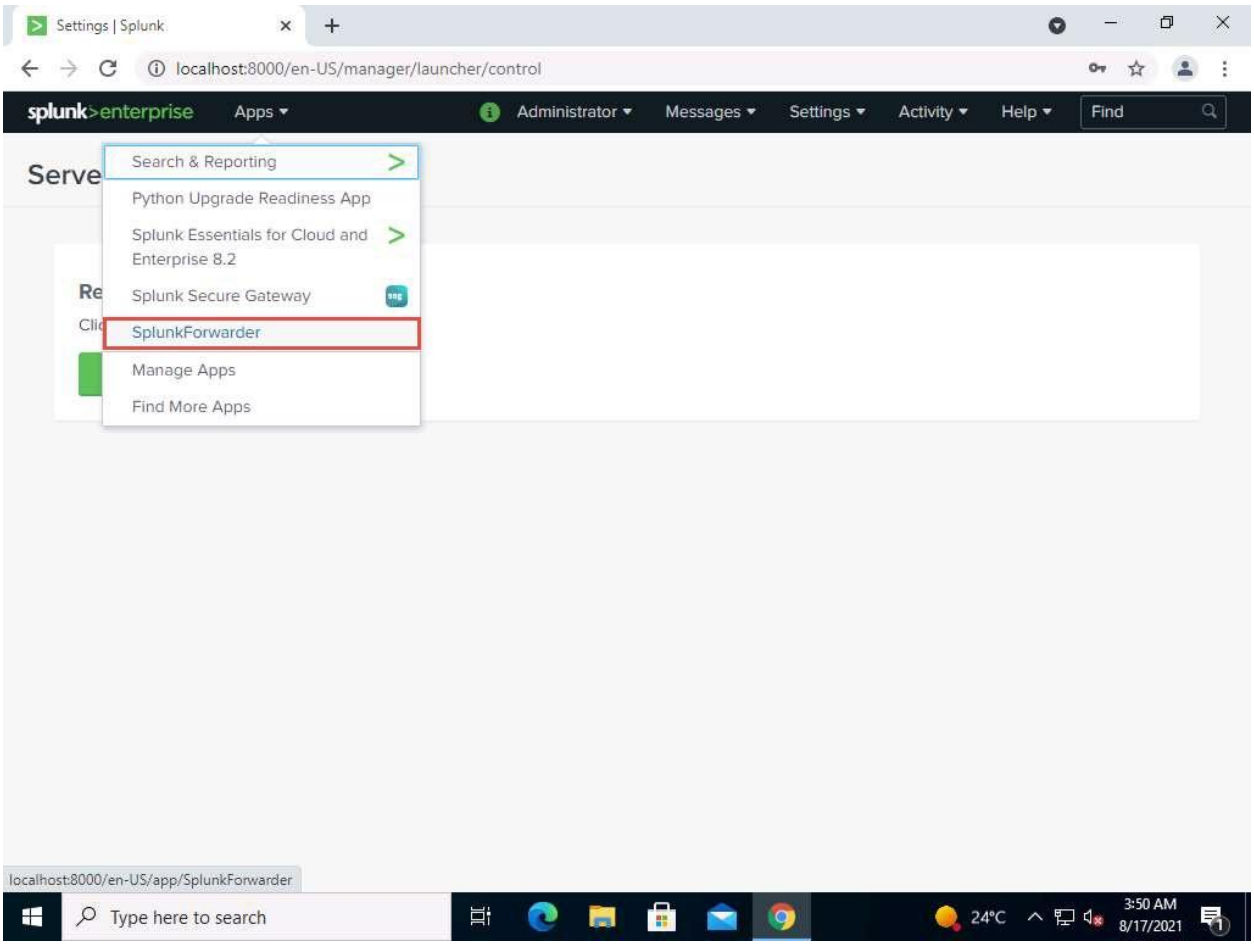


104. You will be redirected to the login page. Enter the user credentials (username admin and password admin@123) and click on Sign In.



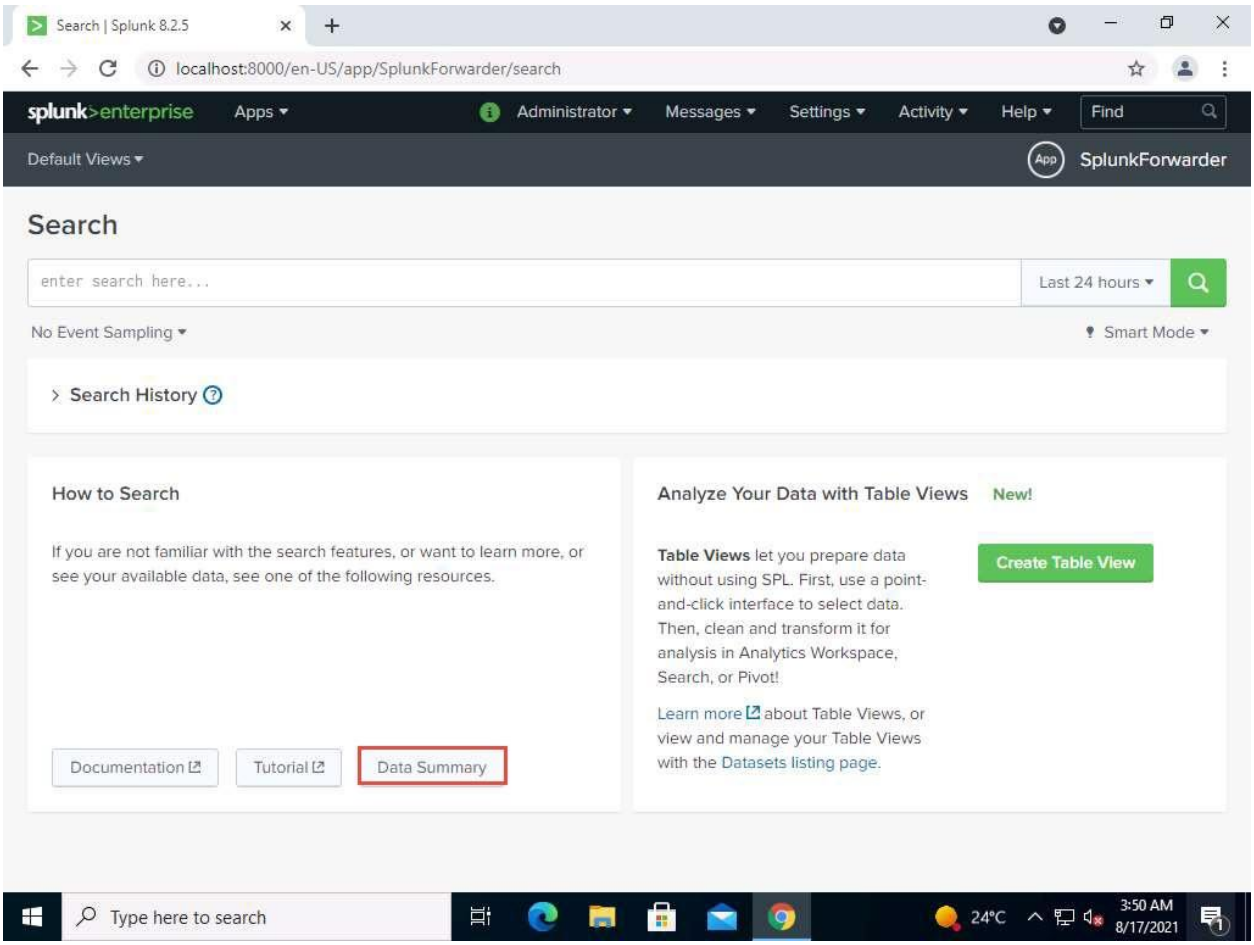
If Splunk is properly not restarted, click Restart Splunk again.

105. Once you log in, click on Apps -> SplunkForwarder from menu.

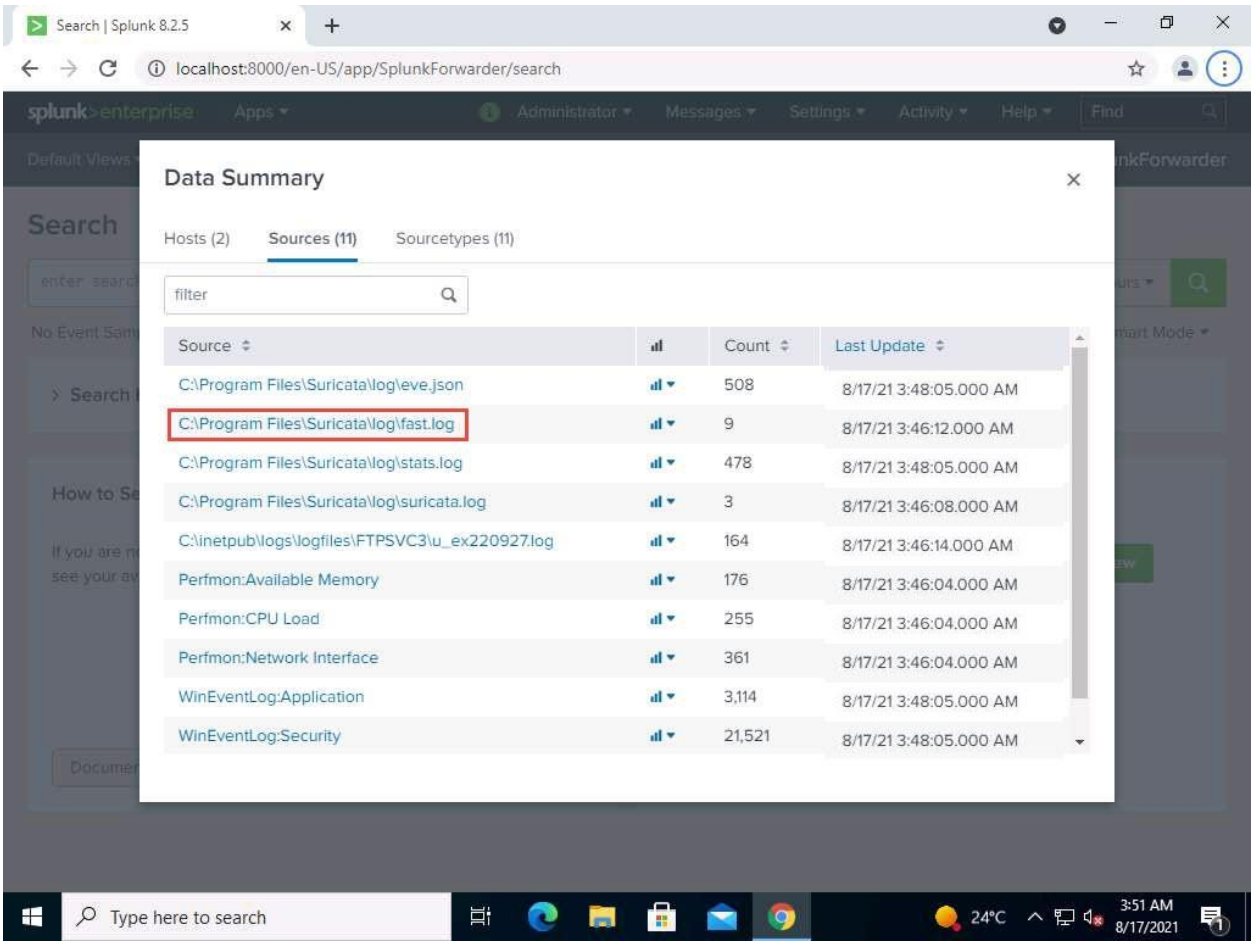


Make sure Splunk Forwarder service is running. If it is not running, start the Splunkforwarder service in Windows services.

106. The Search console appears; click on Data Summary under the What to Search section.



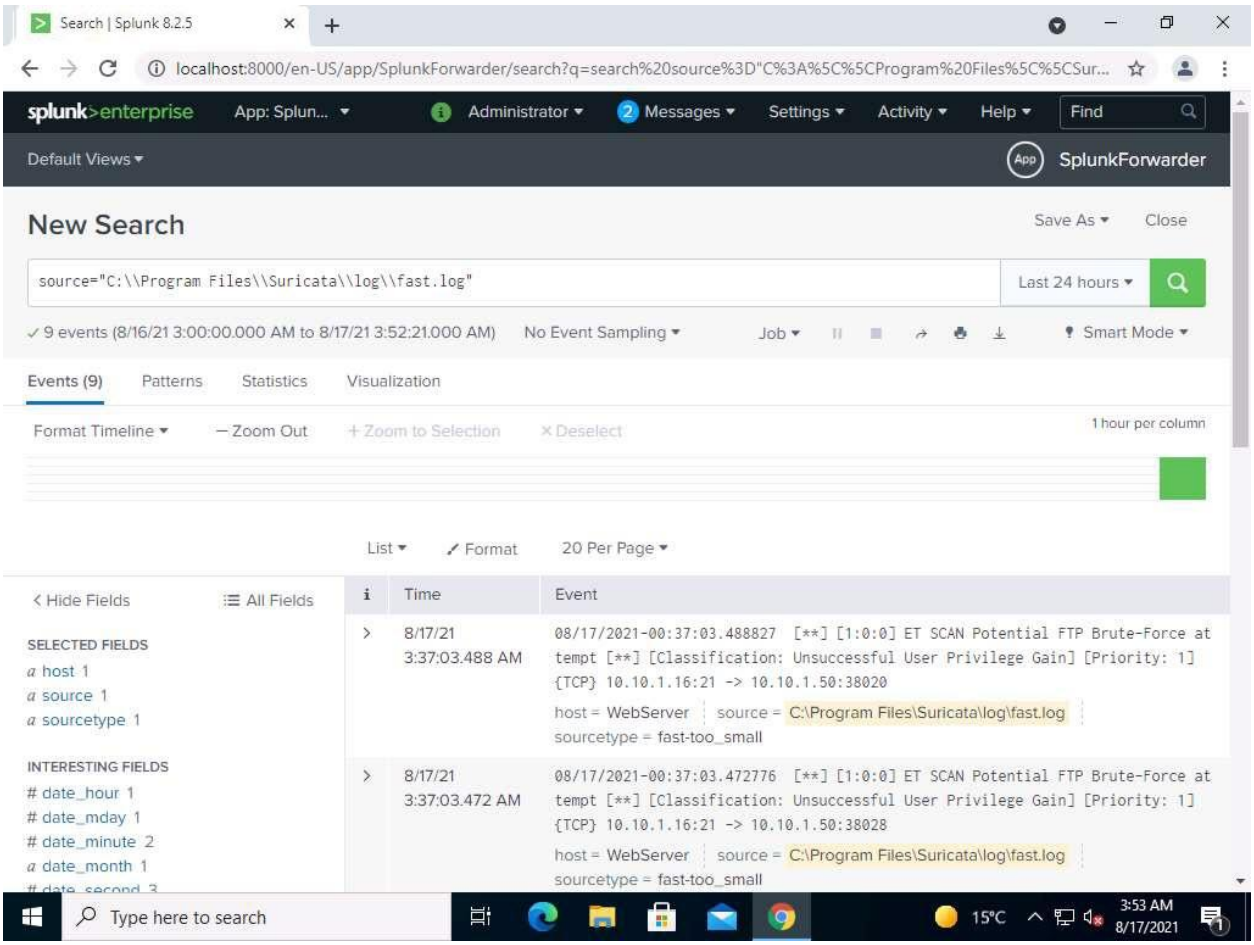
107. The Data Summary pop-up appears. Select the Sources(_) tab, wait for sometime, and then click the C:\Program Files\Suricata\log\fast.log link to continue.



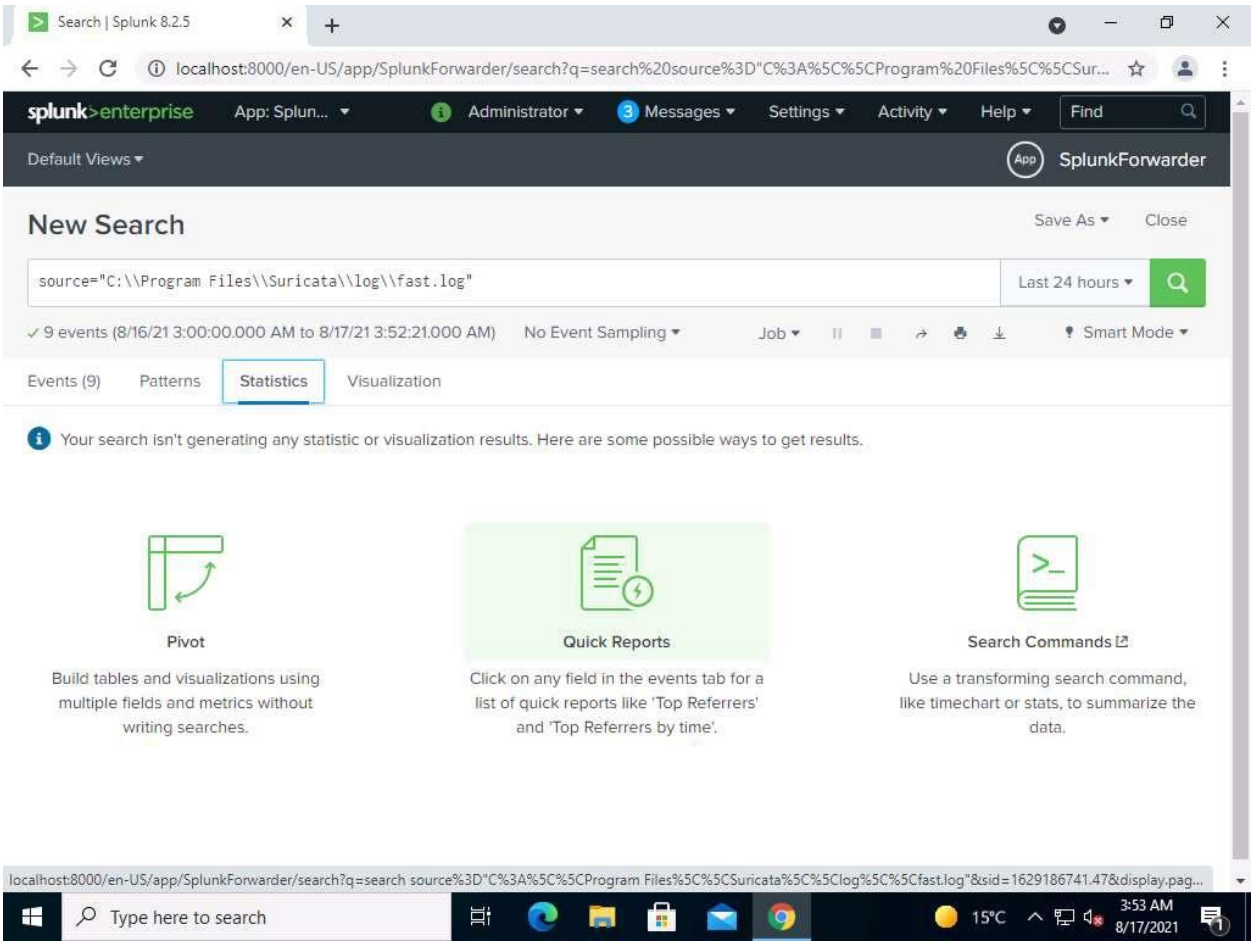
108. Once the fast.log file is selected, the page redirects to the search page and displays the detailed logs.

109. The brute-force attempt was made from Attacker Machine-1 (10.10.1.50) to the Web Server (10.10.1.16).

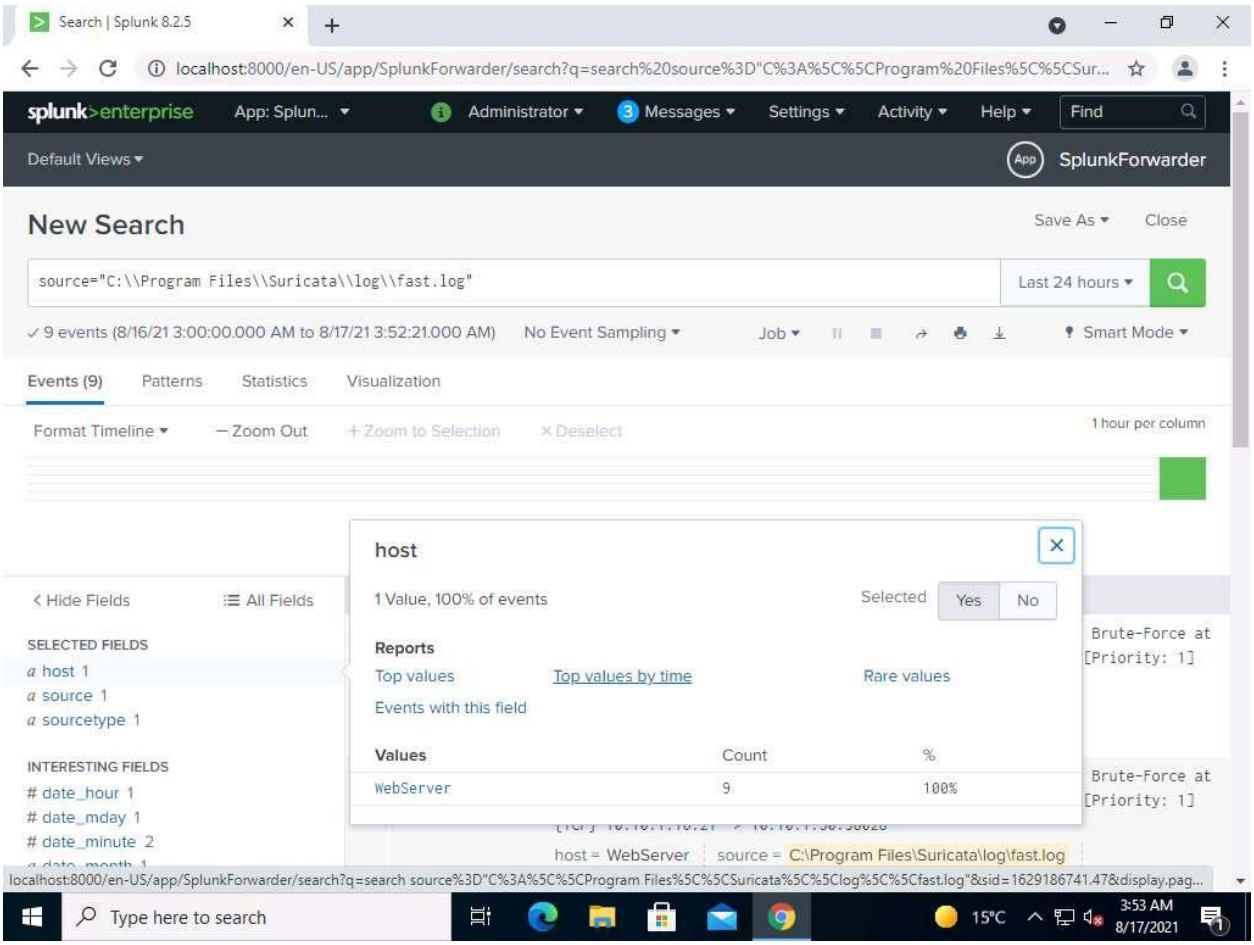
The number of Events might vary in your lab environment.



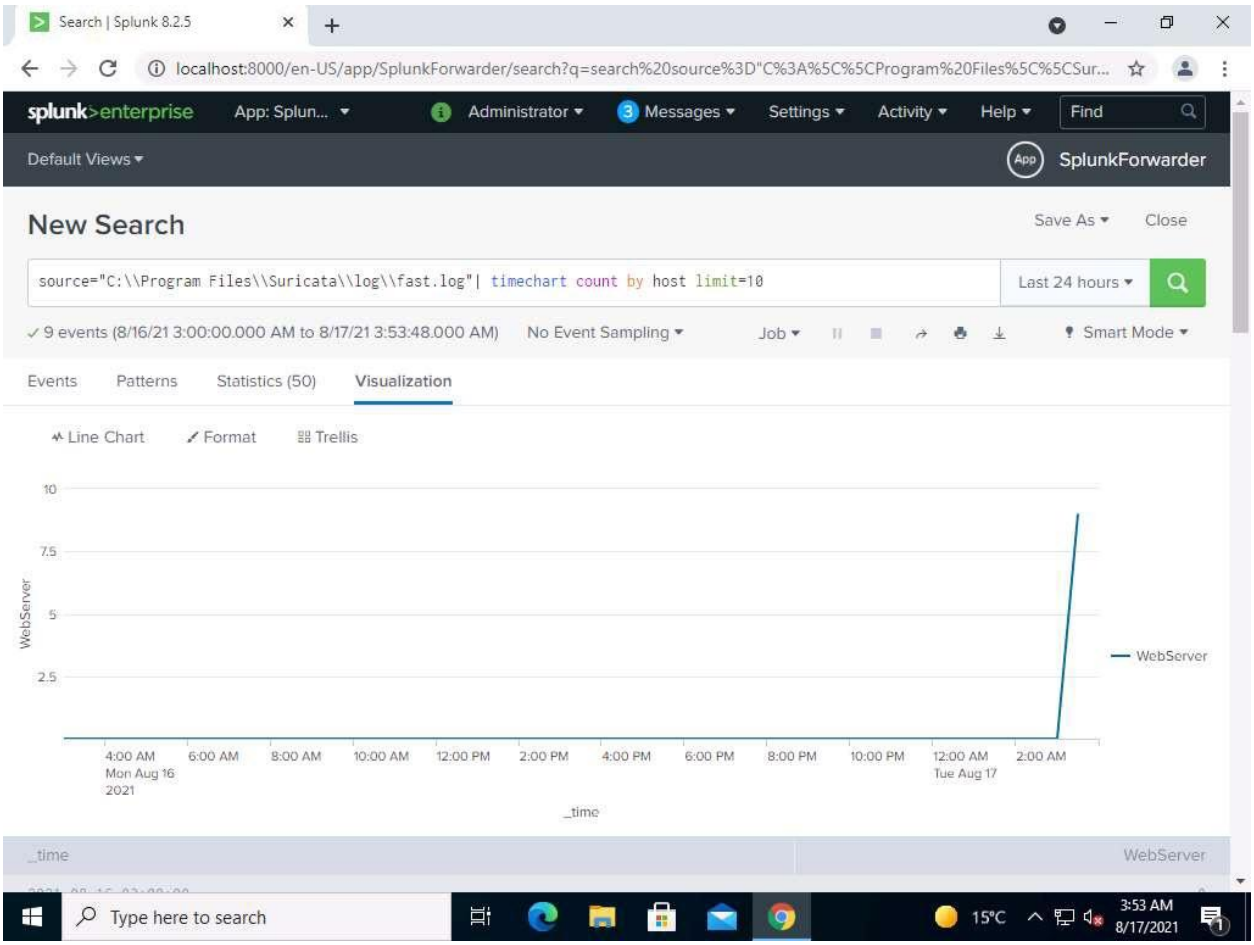
110. Click on Statistics tab and Quick Reports.



111. You will be redirected to the host window, in the host window click on any value under Reports to see the graphical representation of that value. Here we are selecting Top values by time.

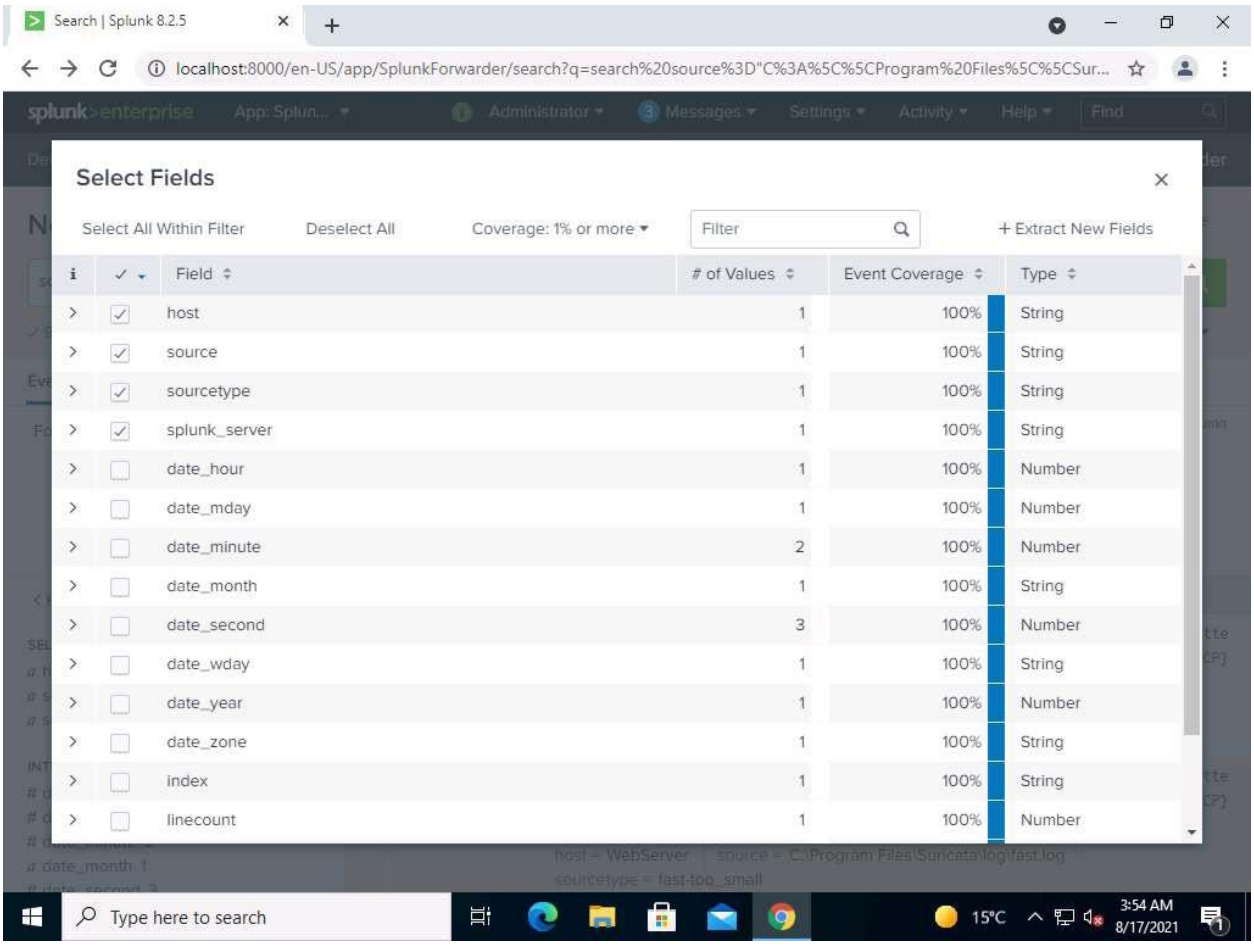


112. You will be redirected to Visualization tab where you can find the Line Chart of the selected option.

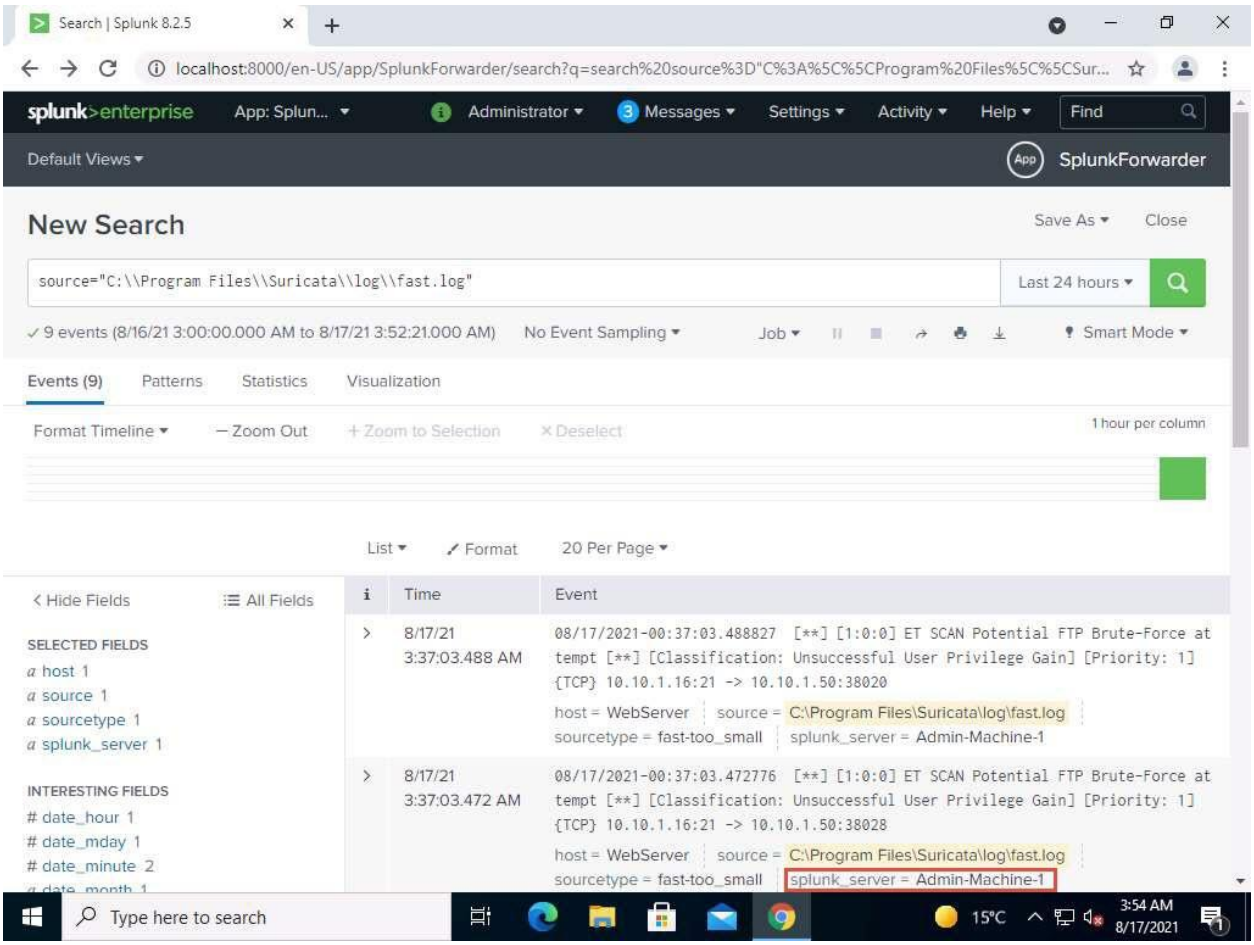


113. Click on back button on the chrome browser to get back to the Events tab.

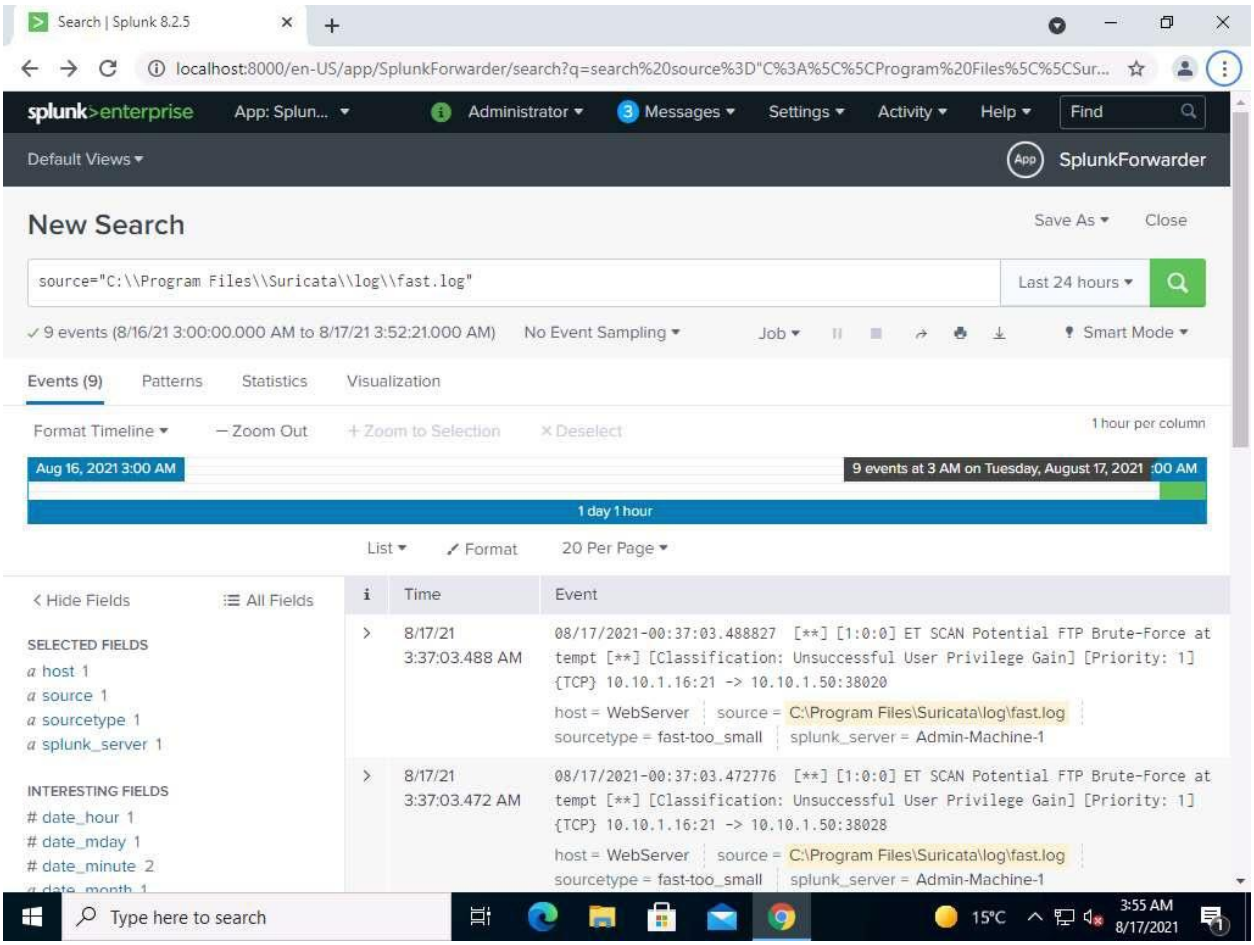
114. Click on All Fields option at the left panel of the window to select the options that can be visible in the events tab. Here we are selecting splunk_server option, after selecting the options close the Select Fields window.



115. We can see that the splunk_server (Admin Machine-1) is visible in the Event tab.



116. Scroll the cursor under the Format Timeline option you can see that the events are recorded in hourly basis, in real time the Administrator can just click on the time in which he wants to review the information.


Search | Splunk 8.2.5
localhost:8000/en-US/app/SplunkForwarder/search?q=search%20source%3D"C%3A%5C%5CProgram%20Files%5C%5CSur...
splunk>enterprise
App: Splun...
Administrator
3 Messages
Settings
Activity
Help
Find
Default Views
SplunkForwarder
New Search
Save As
Close
source="C:\\Program Files\\Suricata\\log\\fast.log"
Last 24 hours
✓ 9 events (8/16/21 3:00:00.000 AM to 8/17/21 3:52:21.000 AM)
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Aug 16, 2021 3:00 AM
9 events at 3 AM on Tuesday, August 17, 2021
1 day 1 hour
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
a splunk_server 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 2
Time
Event
8/17/21 3:37:03.488 AM
08/17/2021-00:37:03.488827 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38020
host = WebServer source = C:\Program Files\Suricata\log\fast.log
sourcetype = fast-too_small splunk_server = Admin-Machine-1
8/17/21 3:37:03.472 AM
08/17/2021-00:37:03.472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38028
host = WebServer source = C:\Program Files\Suricata\log\fast.log
sourcetype = fast-too_small splunk_server = Admin-Machine-1
Type here to search
15°C
3:55 AM
8/17/2021