

**Project:**  
**Network-Based IDS**



**Haris ali**

"CompTIA Security+ Certified | Cybersecurity Analyst"

**WARE**



## **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.

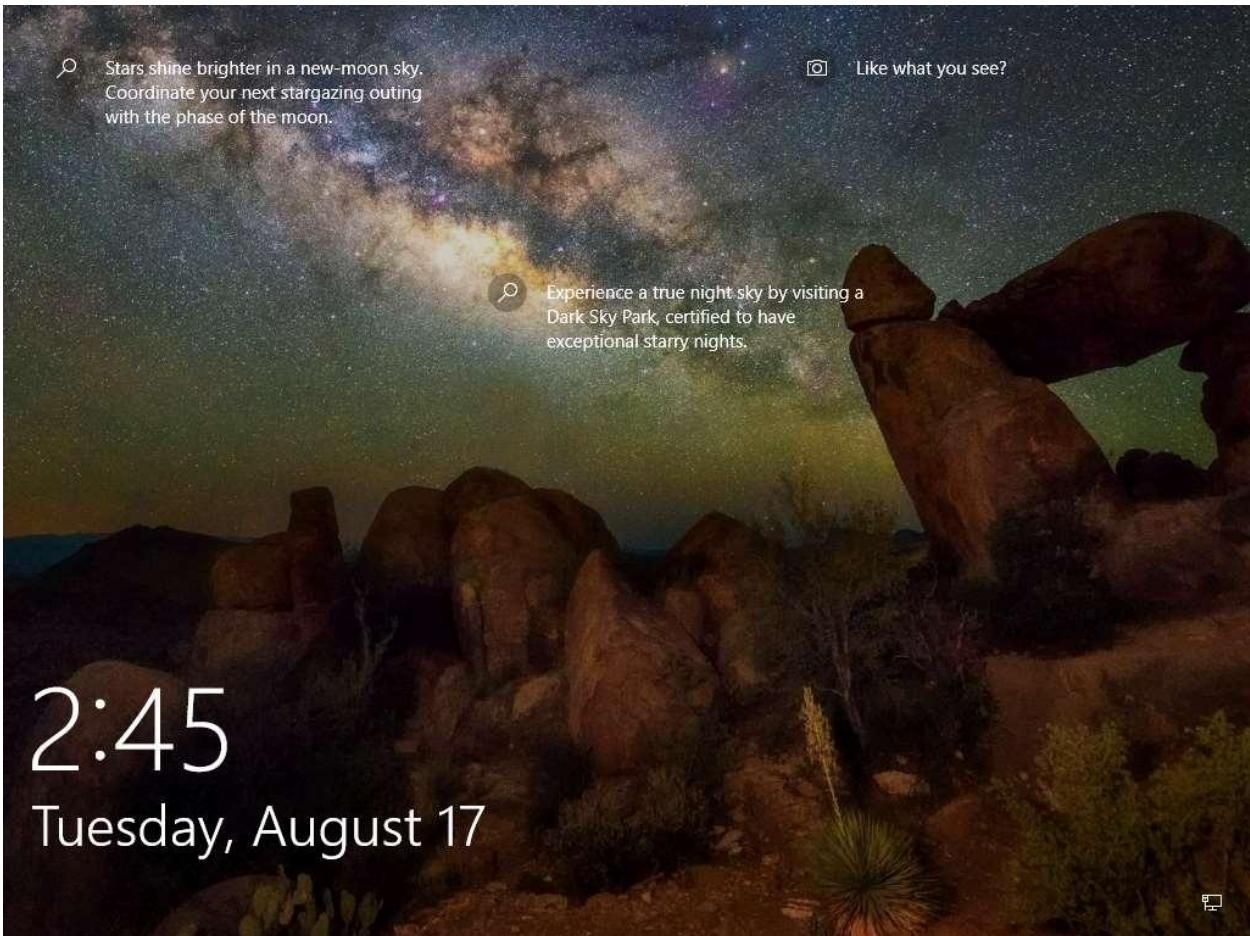
### Overview of Network-based IDS

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.

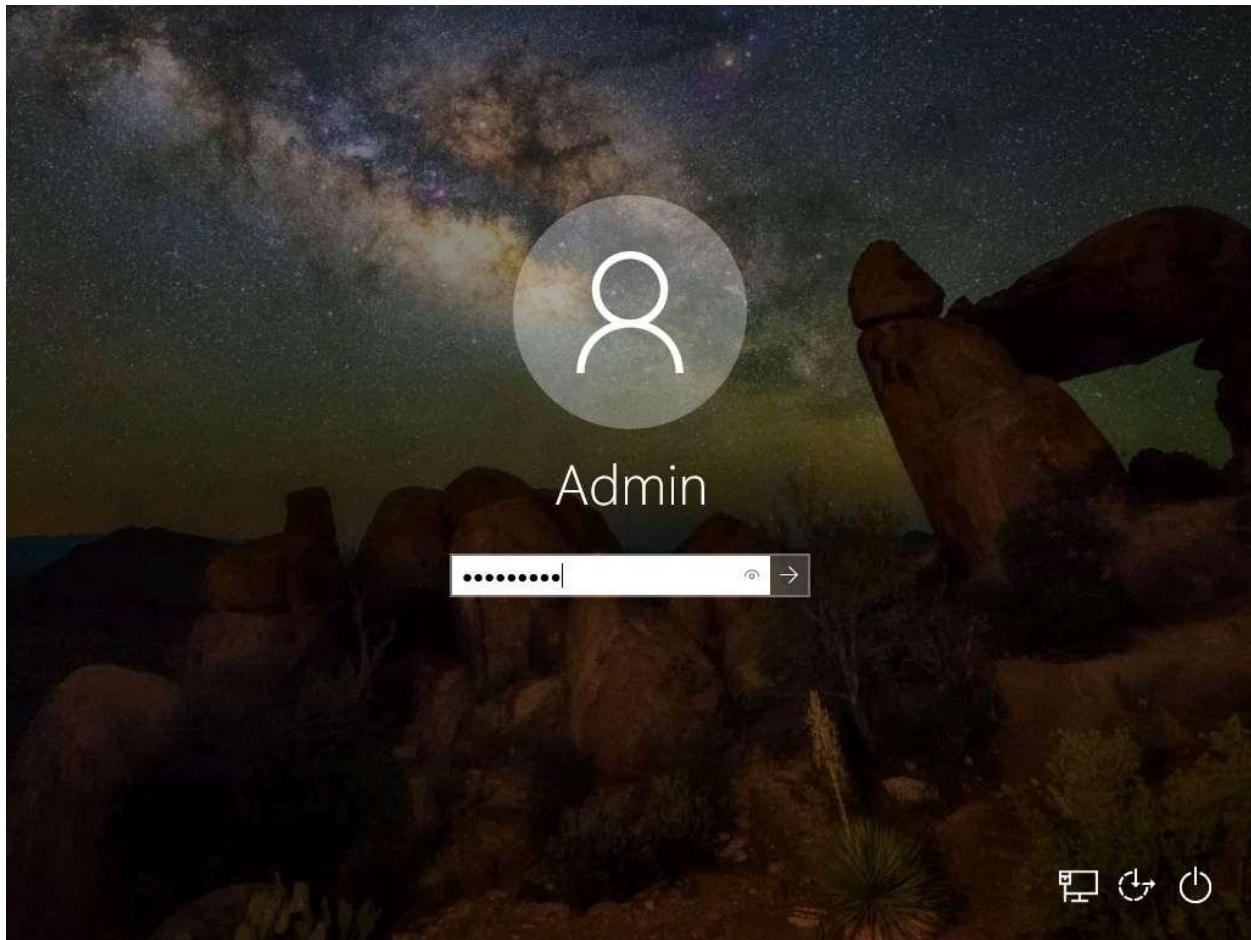
### Lab Tasks

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

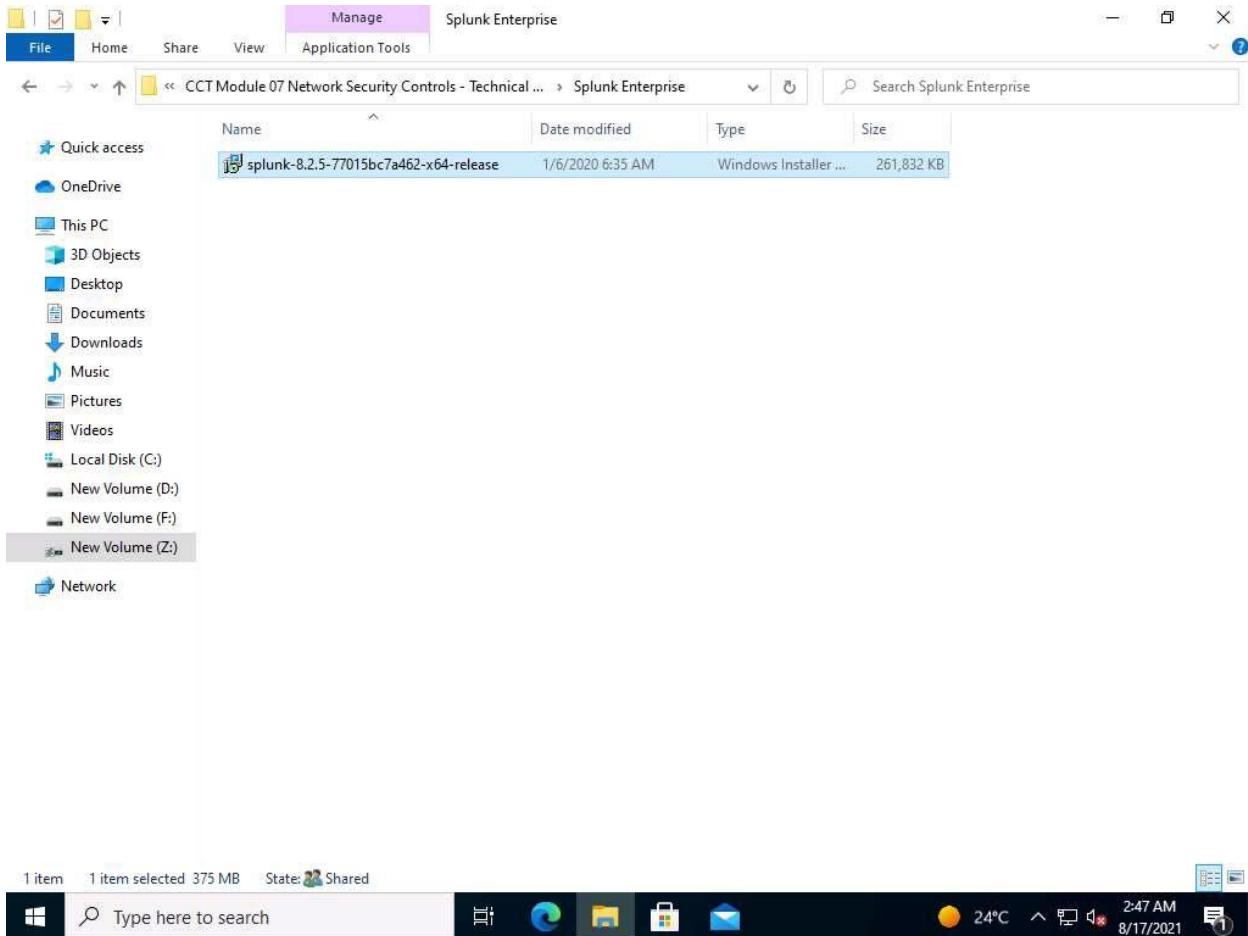
1. Click [Admin Machine-1](#) to launch the Admin Machine-1 machine.  
Click [Ctrl+Alt+Delete](#).



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



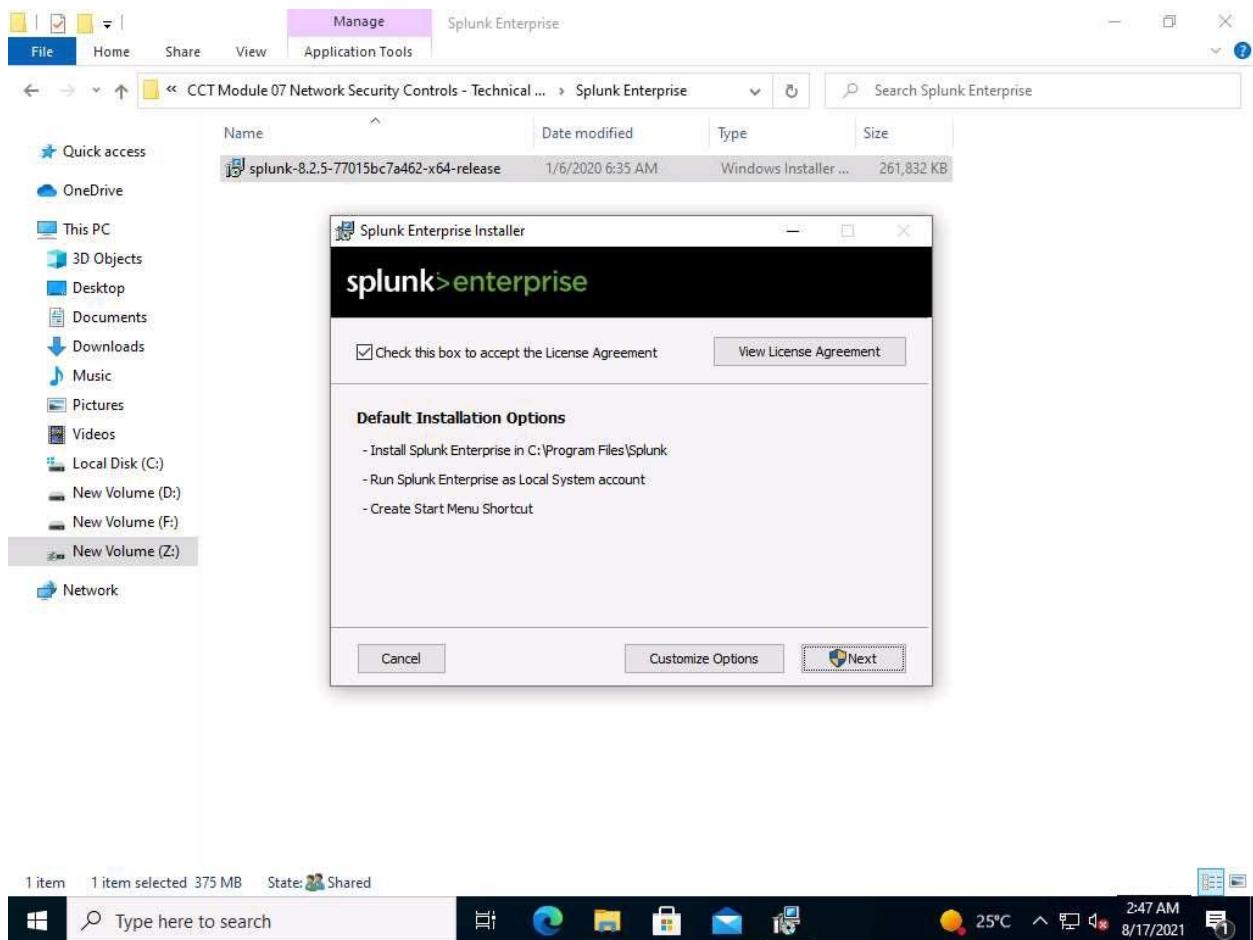
3. Next, install Splunk Enterprise SIEM, to view the captured Suricata logs in SIEM.
4. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Splunk Enterprise.



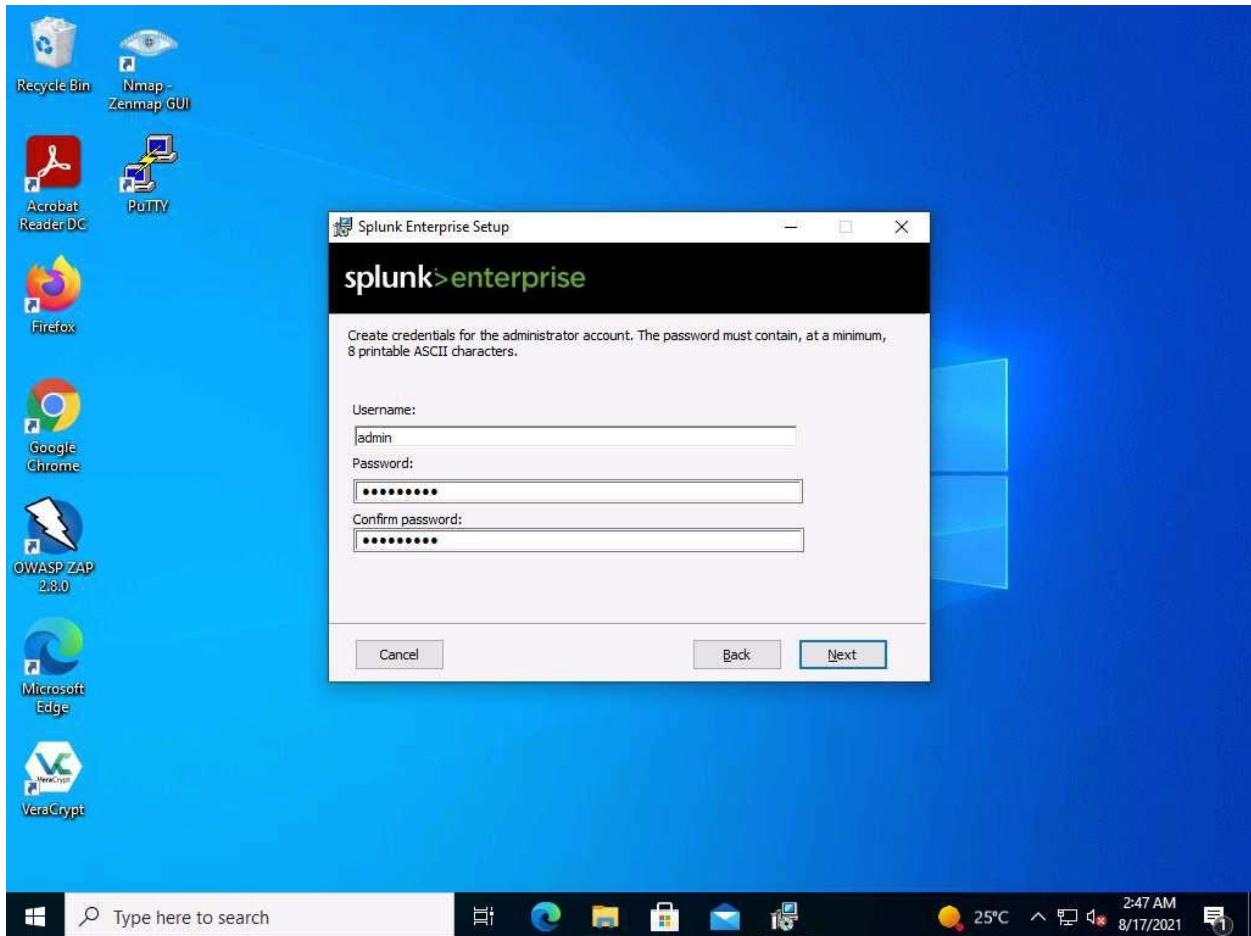
- Double-click `splunk-8.2.5-77015bc7a462-x64-release.msi` to start the installation. If the Open File - Security Warning pop-up appears, click Run.

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

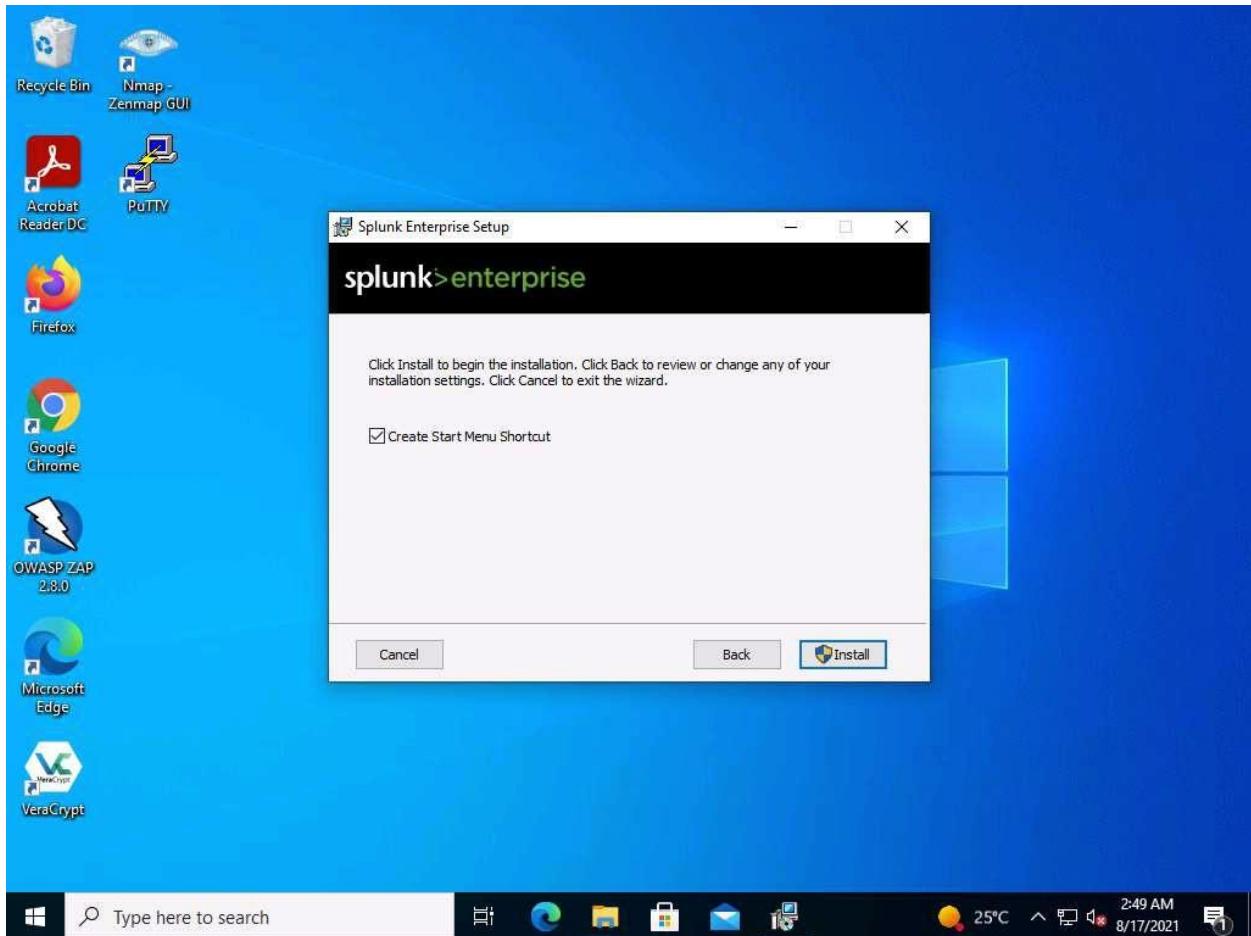
- The Splunk Enterprise Installer window appears. Click checkbox to accept the license agreement and click Next.



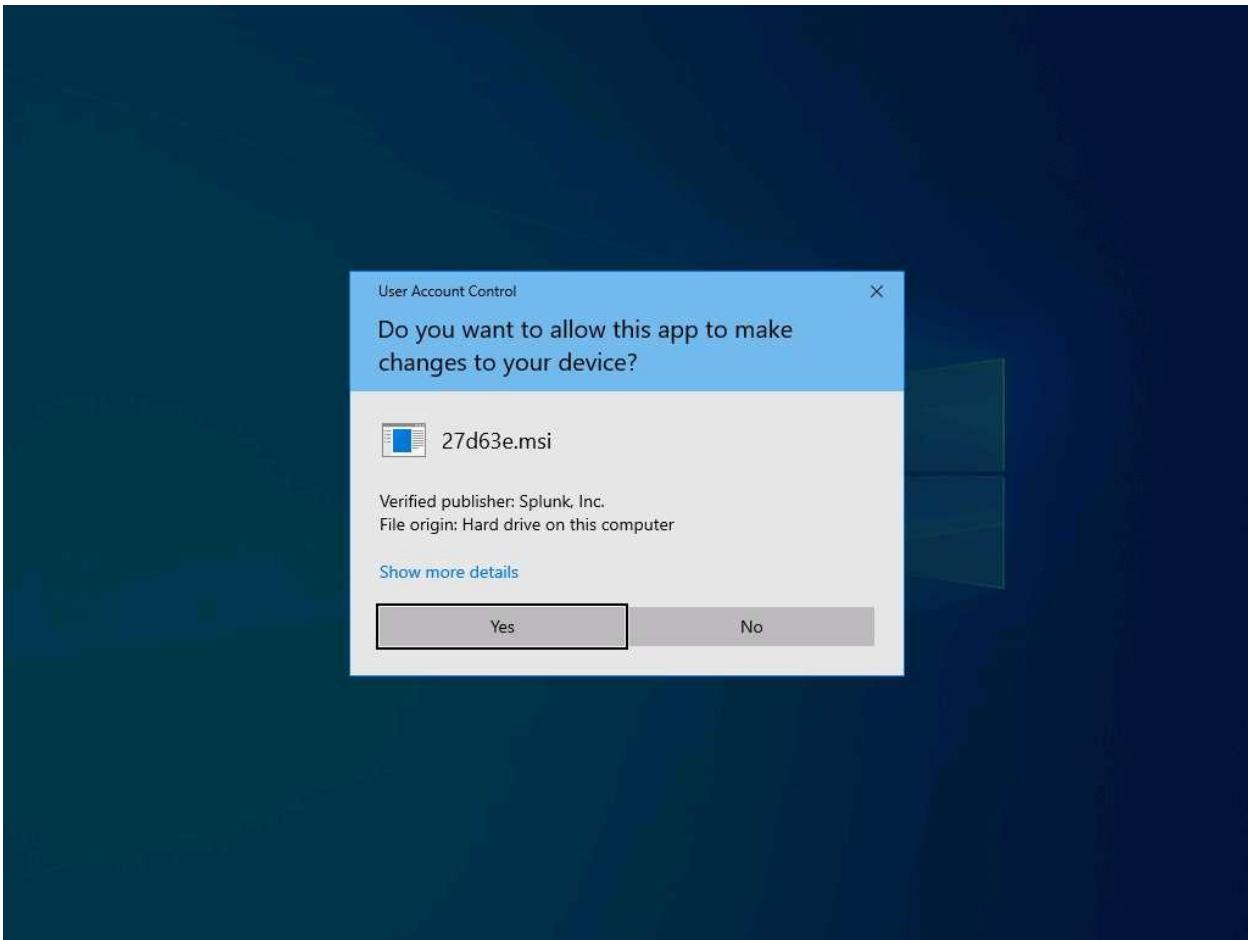
7. Enter the credential for Splunk Enterprise with username admin, password and confirm password as admin@123. Click Next.



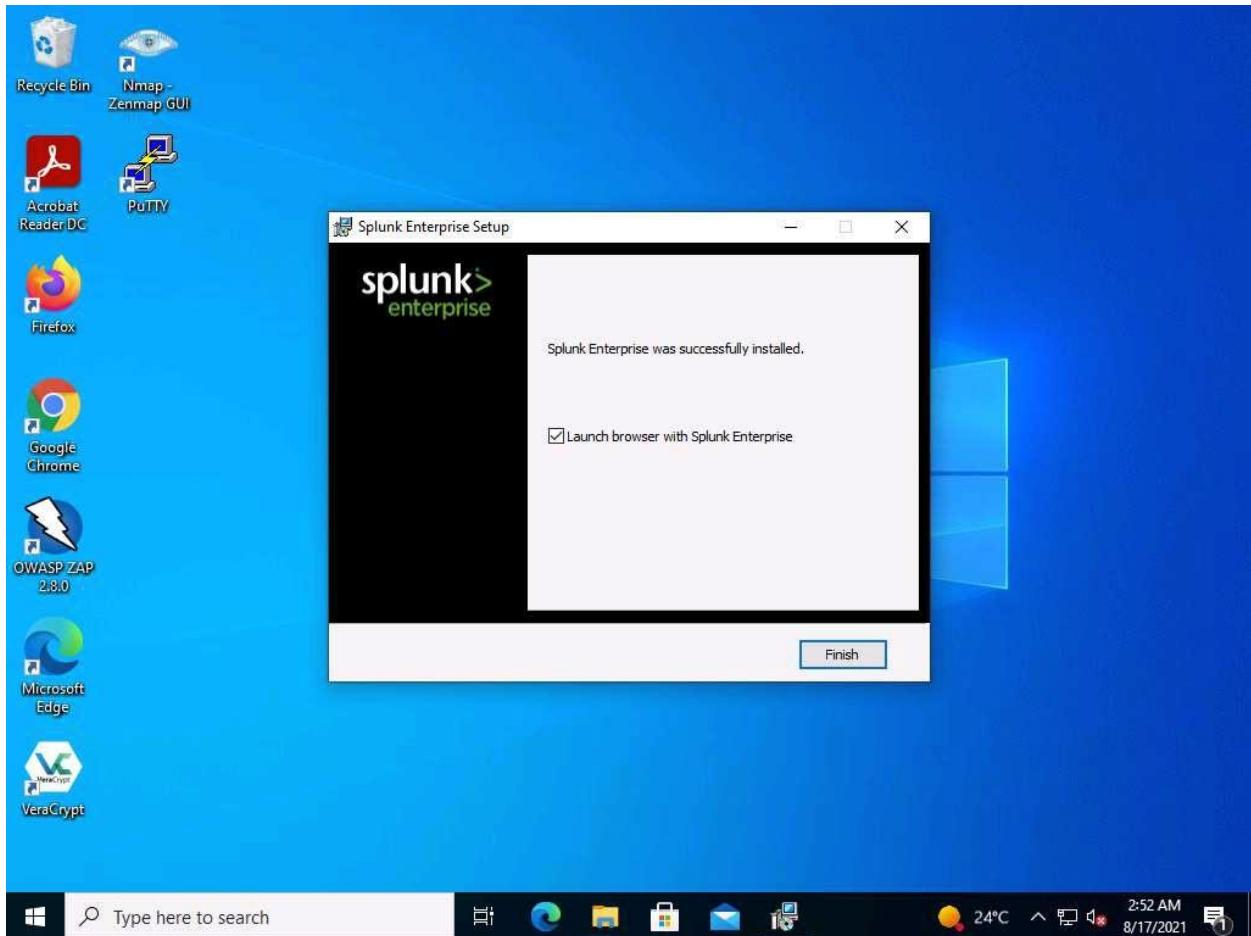
8. Click Install to install Splunk Enterprise.



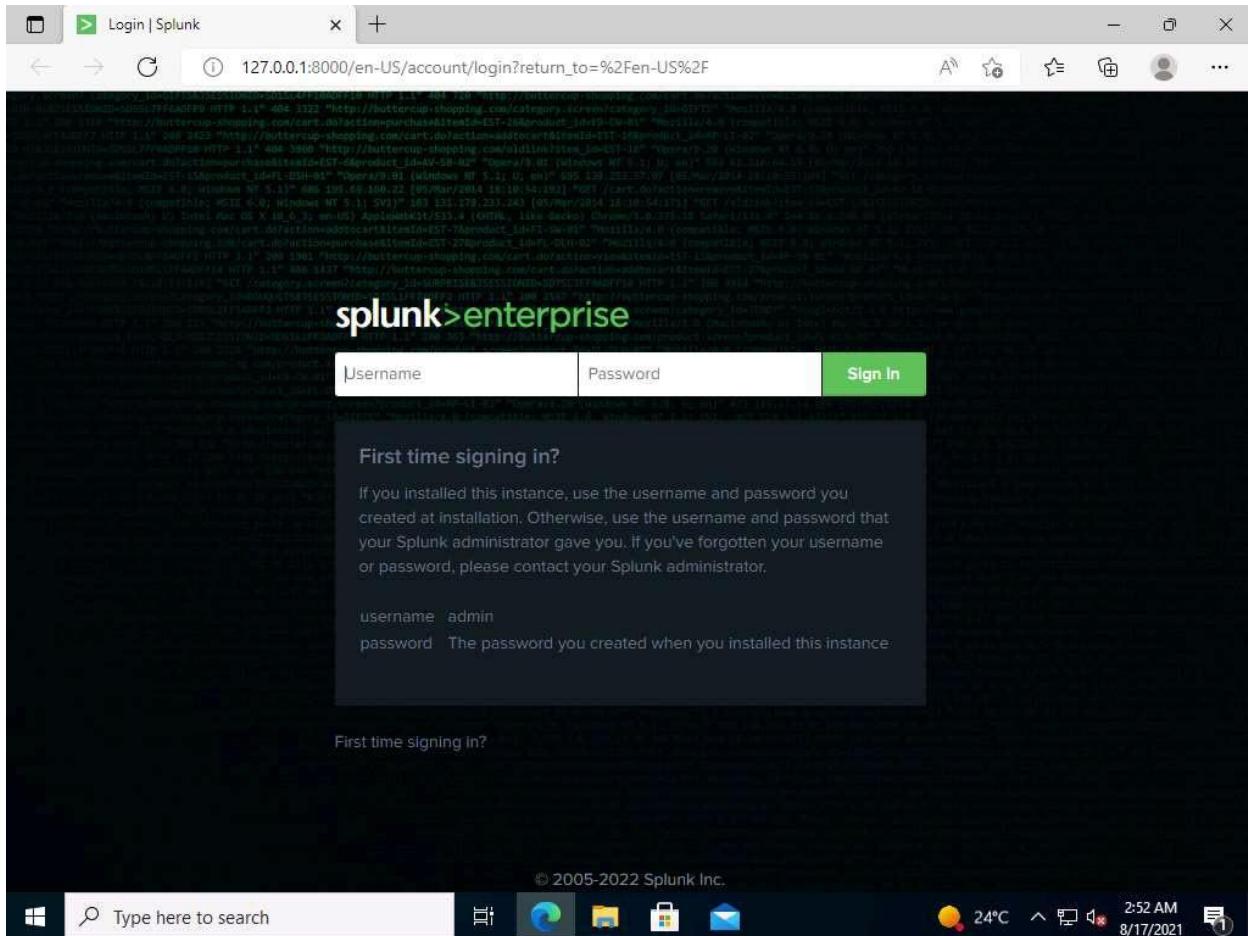
9. The User Account Control pop-up window appears; click Yes to continue.



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



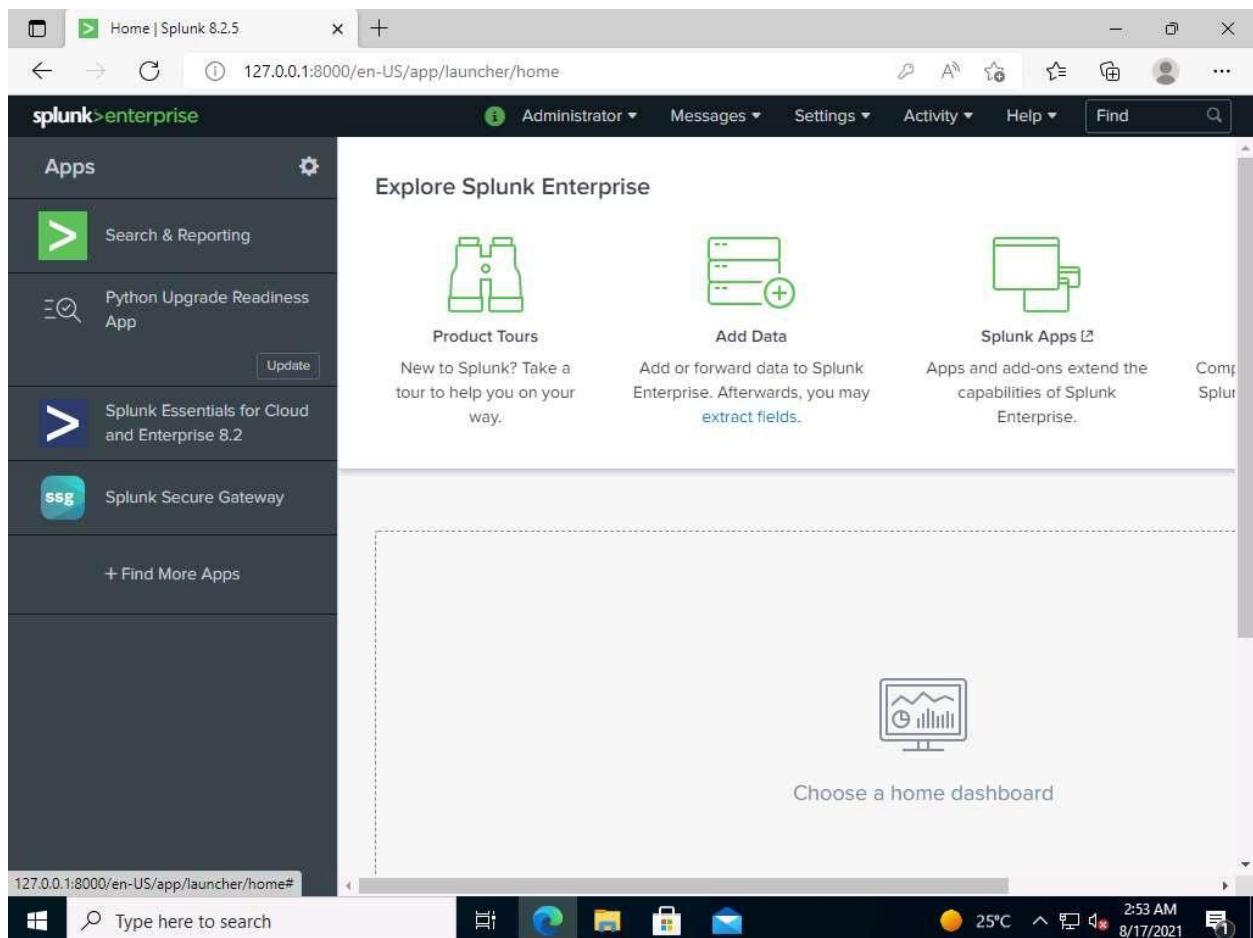
11. Splunk Enterprise launches in your default browser.
12. The First time signing in? page appears. Enter the username (admin) and password (provided while installation as admin@123) in their respective fields and click Sign In.



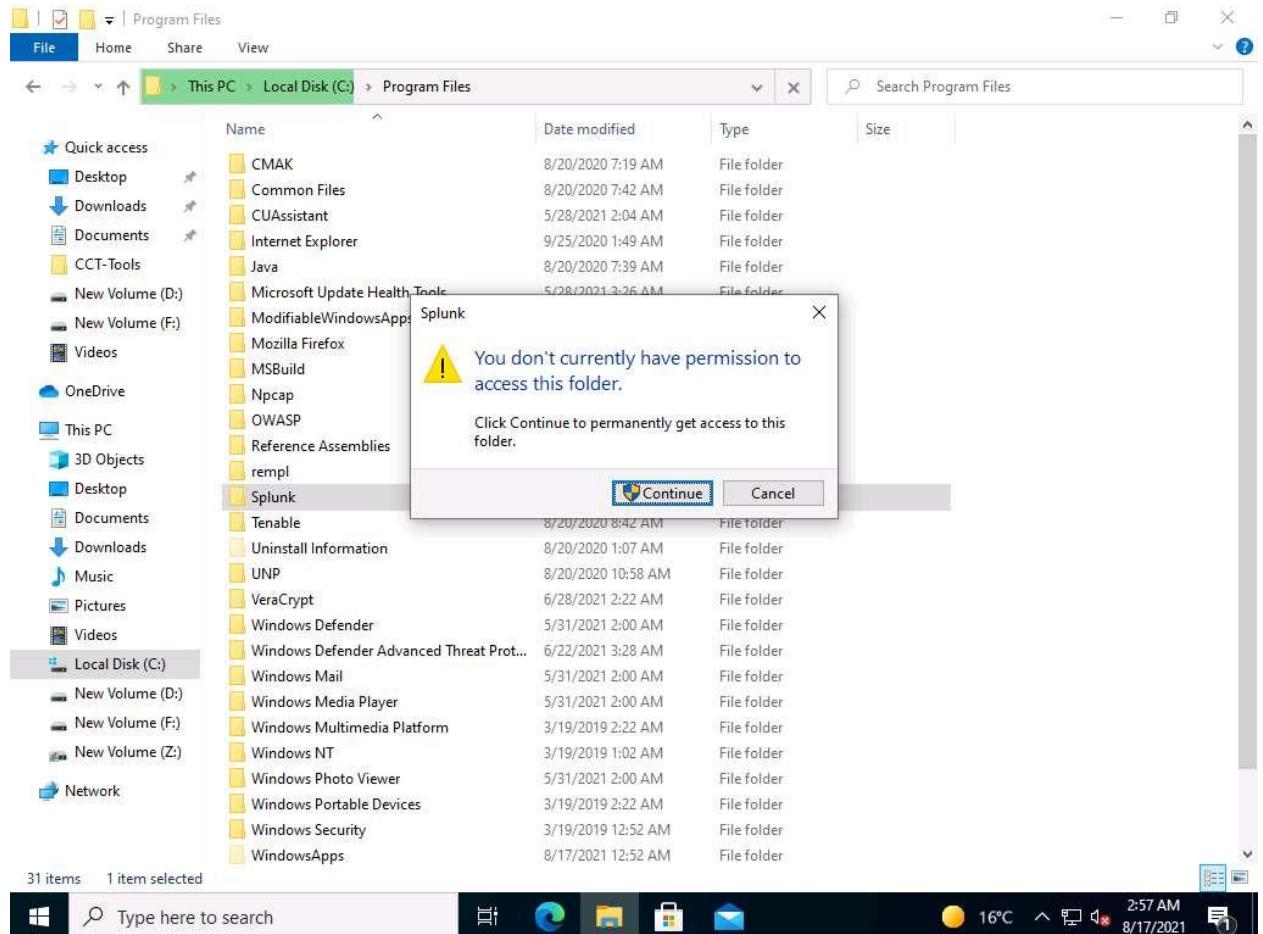
13. You will be successfully logged in to Splunk Enterprise.

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**.

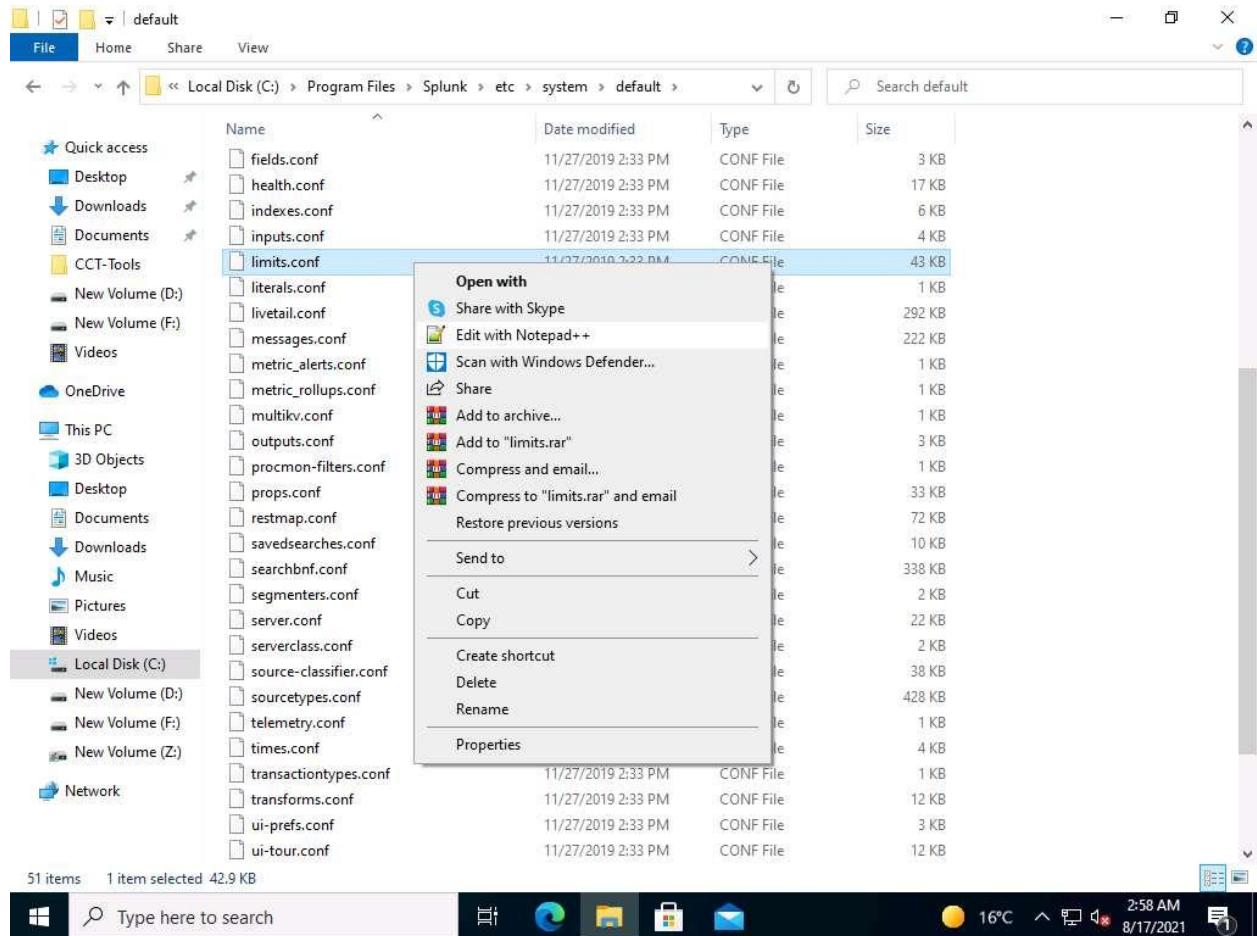


14. Close the browser, to increase the default maximum number of concurrent of searches per CUP in Splunk Enterprise, navigate to C:\Program Files\Splunk\etc\system\default.
15. If the permission alert window opens, click Continue to access the Splunk folder.

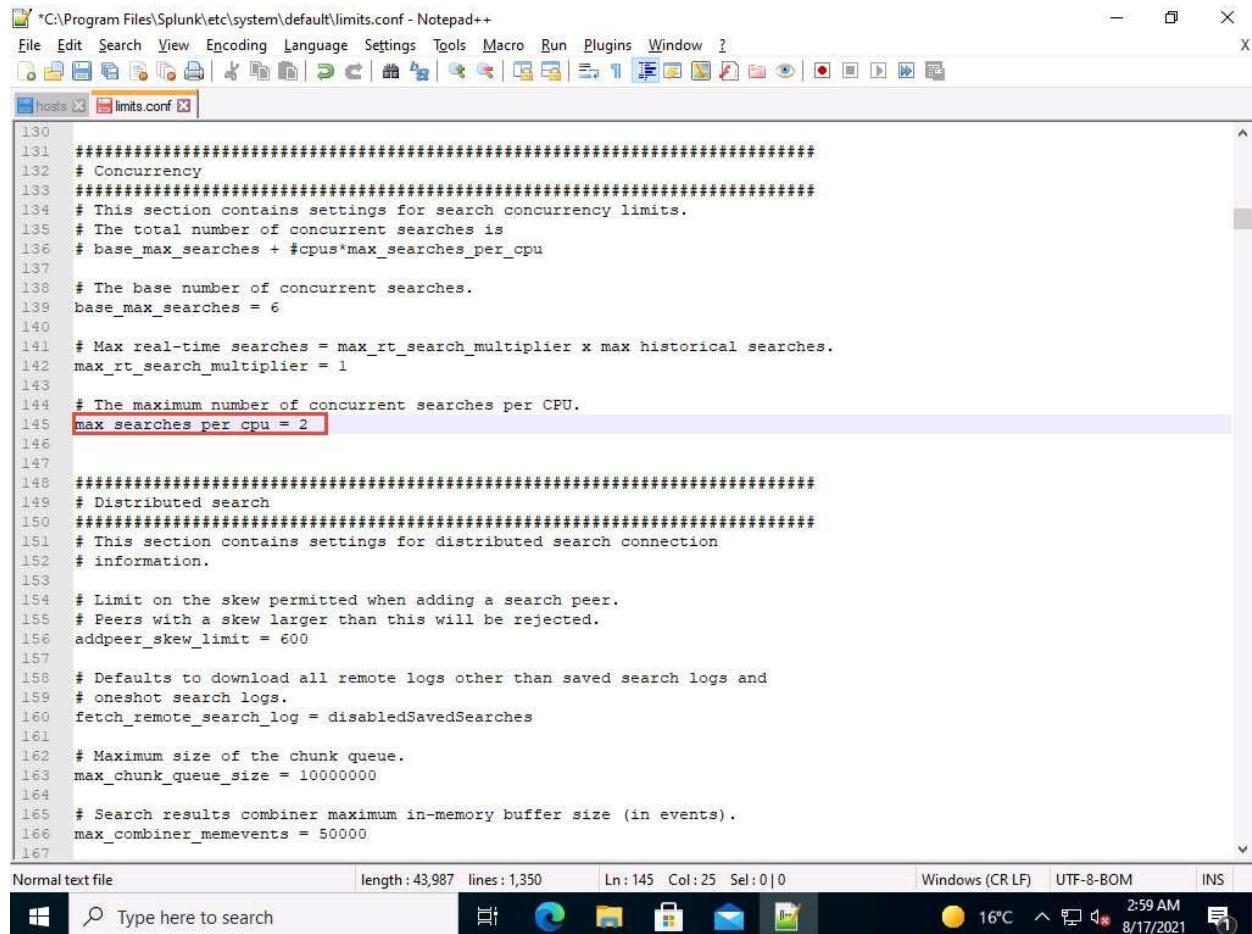


## 16. Open limits.conf with Notepad++.

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.



```
*C:\Program Files\Splunk\etc\system\default\limits.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts limits.conf

130 #####
131 # Concurrency
132 # This section contains settings for search concurrency limits.
133 # The total number of concurrent searches is
134 # base_max_searches + #cpus*max_searches_per_cpu
135
136 # The base number of concurrent searches.
137 base_max_searches = 6
138
139 # Max real-time searches = max_rt_search_multiplier x max historical searches.
140 max_rt_search_multiplier = 1
141
142 # The maximum number of concurrent searches per CPU.
143 max searches per cpu = 2
144
145 #####
146 # Distributed search
147 # This section contains settings for distributed search connection
148 # information.
149 # Limit on the skew permitted when adding a search peer.
150 # Peers with a skew larger than this will be rejected.
151 addpeer_skew_limit = 600
152
153 # Defaults to download all remote logs other than saved search logs and
154 # oneshot search logs.
155 fetch_remote_search_log = disabledSavedSearches
156
157 # Maximum size of the chunk queue.
158 max_chunk_queue_size = 10000000
159
160 # Search results combiner maximum in-memory buffer size (in events).
161 max_combiner_memevents = 50000
162
163
164
165
166
167
```

18. Restart the Admin Machine-1

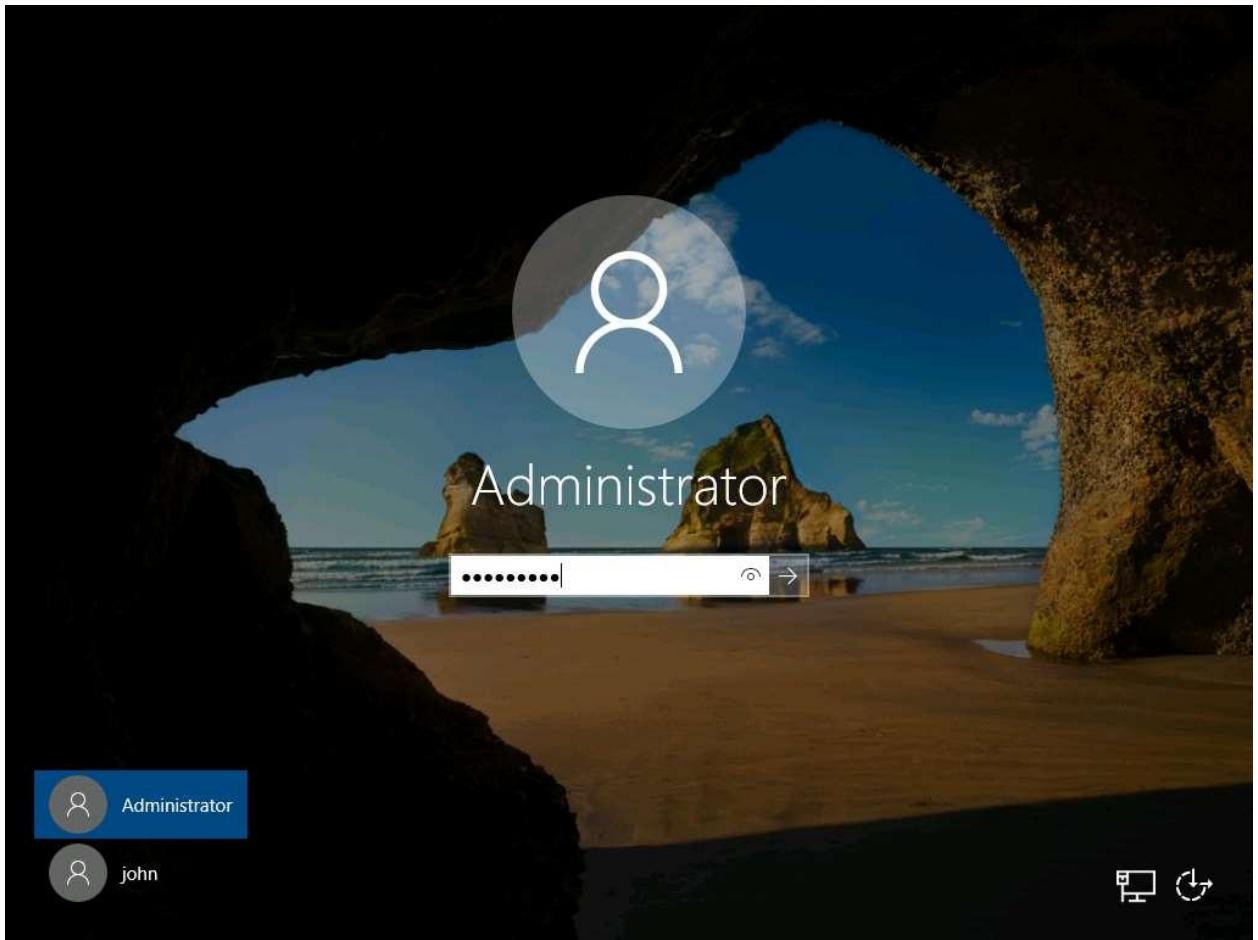
19. The Suricata IDS configuration needs to be on the web server; therefore, we need to configure the Suricata IDS on Web Server.

20. Click [Web Server](#) to switch to the Web Server machine. Click [Ctrl+Alt+Delete](#) link to log in.

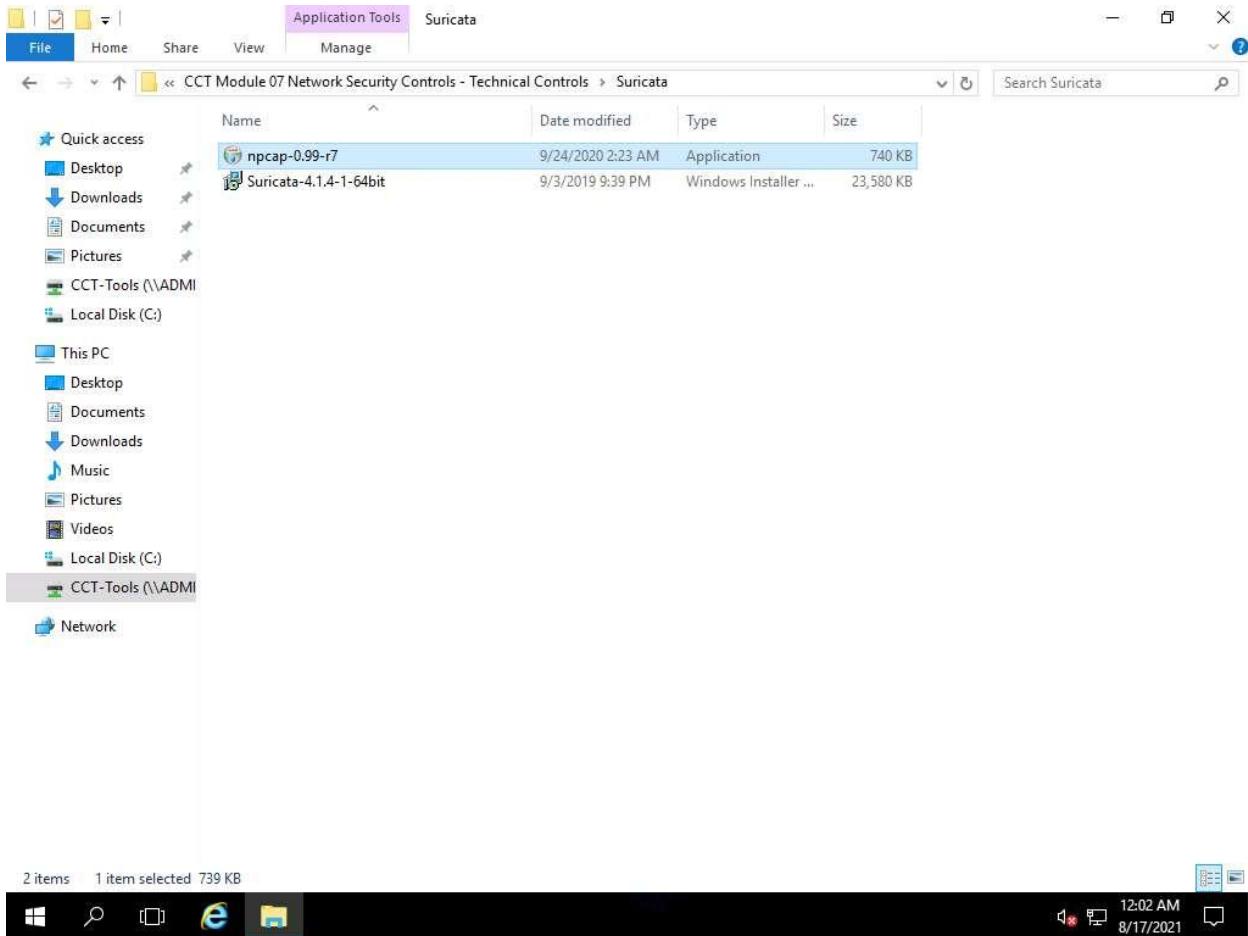
If you are already logged into the Web Server machine, then skip to Step#22.



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

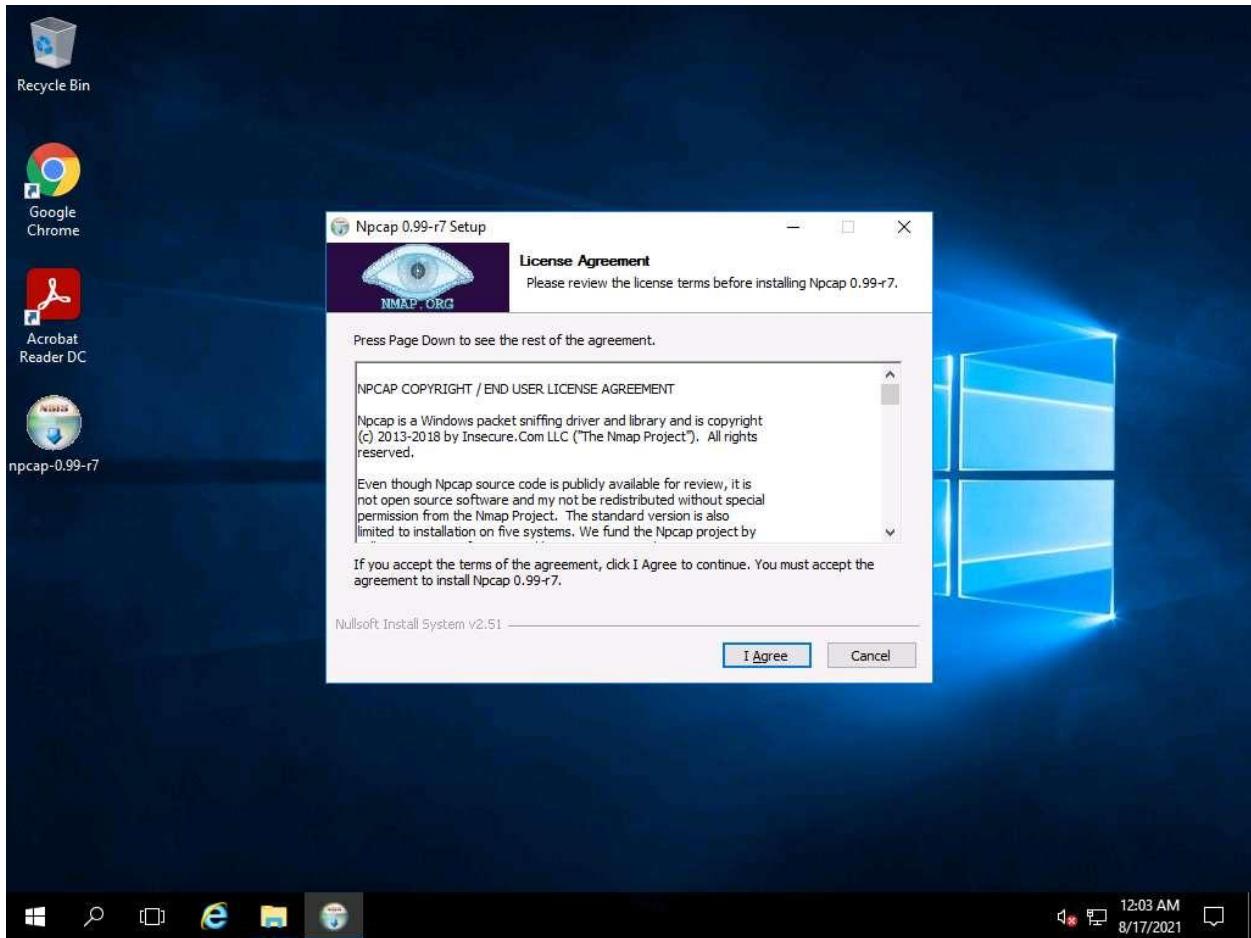


22. Navigate to Z:\CCT Module 07 Network Security Controls - Technical Controls\Suricata and copy npcap-0.99-r7.exe

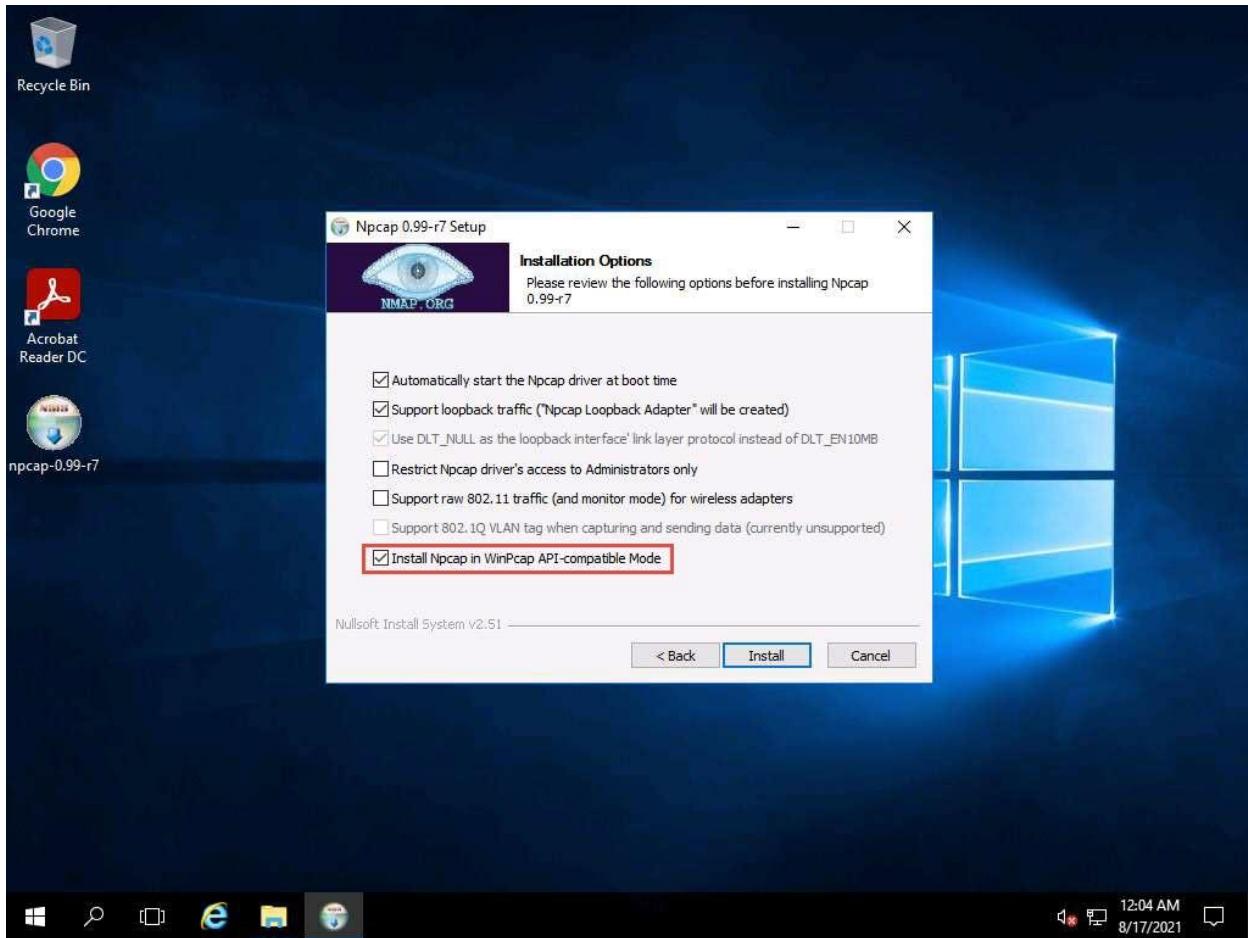


23. Paste the npcap-0.99-r7.exe file on the Desktop.
24. Npcap is a tool used for network packet capturing and injection library for Windows.
25. Suricata uses npcap for capturing network packets and alerts. The following steps demonstrate the installation of the npcap tool.
26. Double click on npcap-0.99-r7.exe. Click on I Agree to continue the installation.

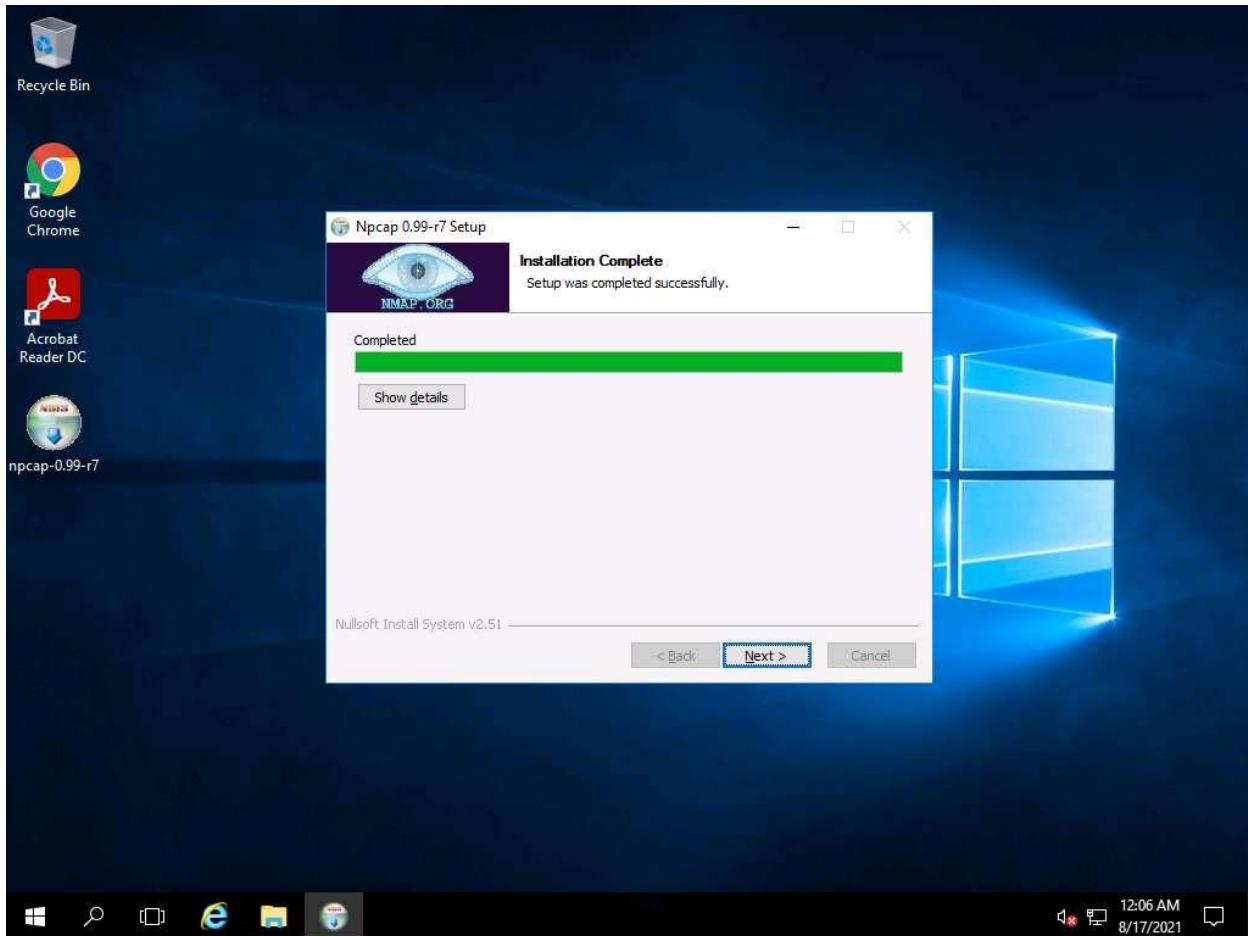
If the Security Warning pop-up appears, click Run.



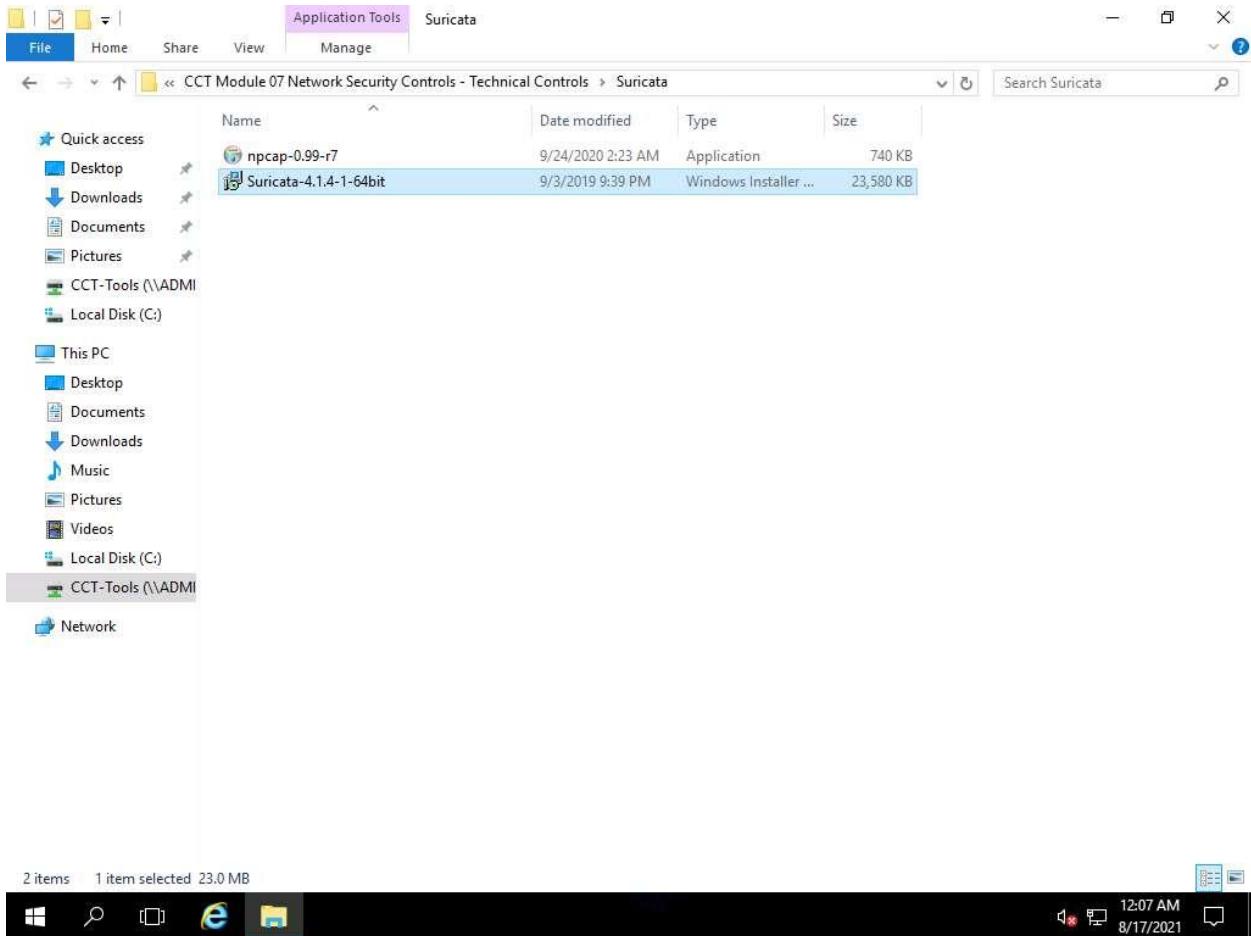
27. Check Install Npcap in WinPcap API-compatible Mode, and click Install.



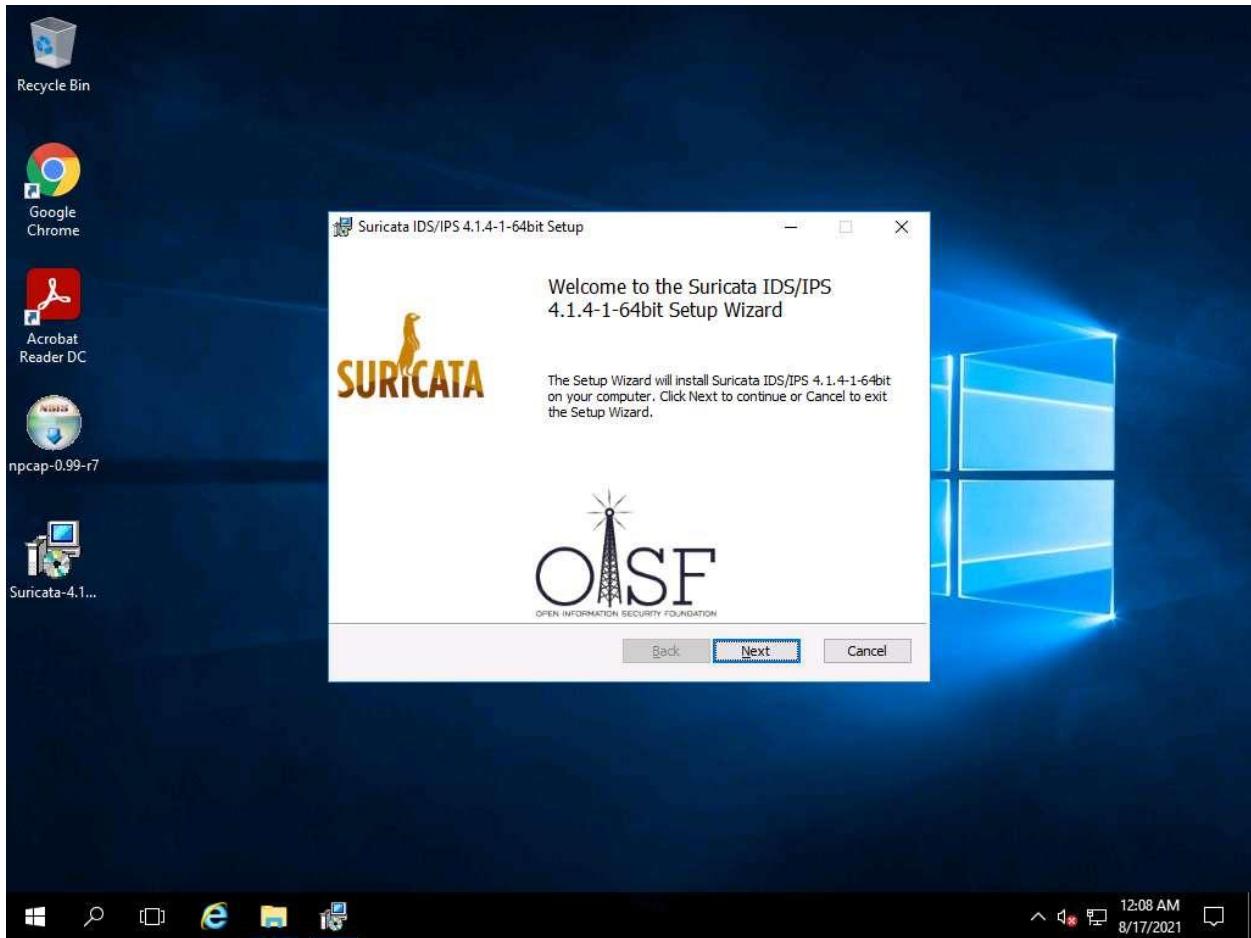
28. The installation will start in a few seconds. Once the installation is completed successfully, click Next to continue.



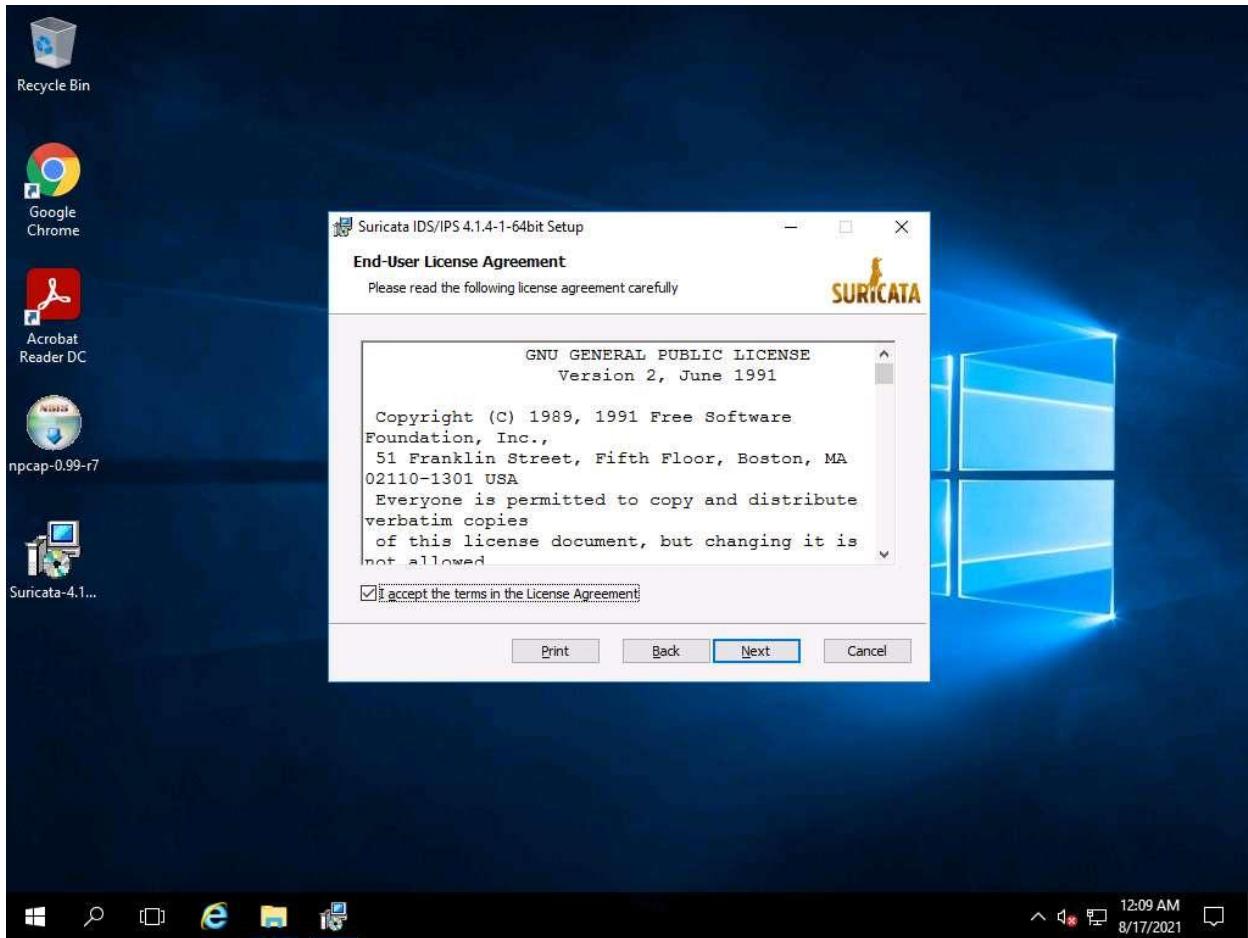
29. Click Finish to complete the installation.
30. Navigate to Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Suricata and copy Suricata-4.1.4-1-64bit.msi



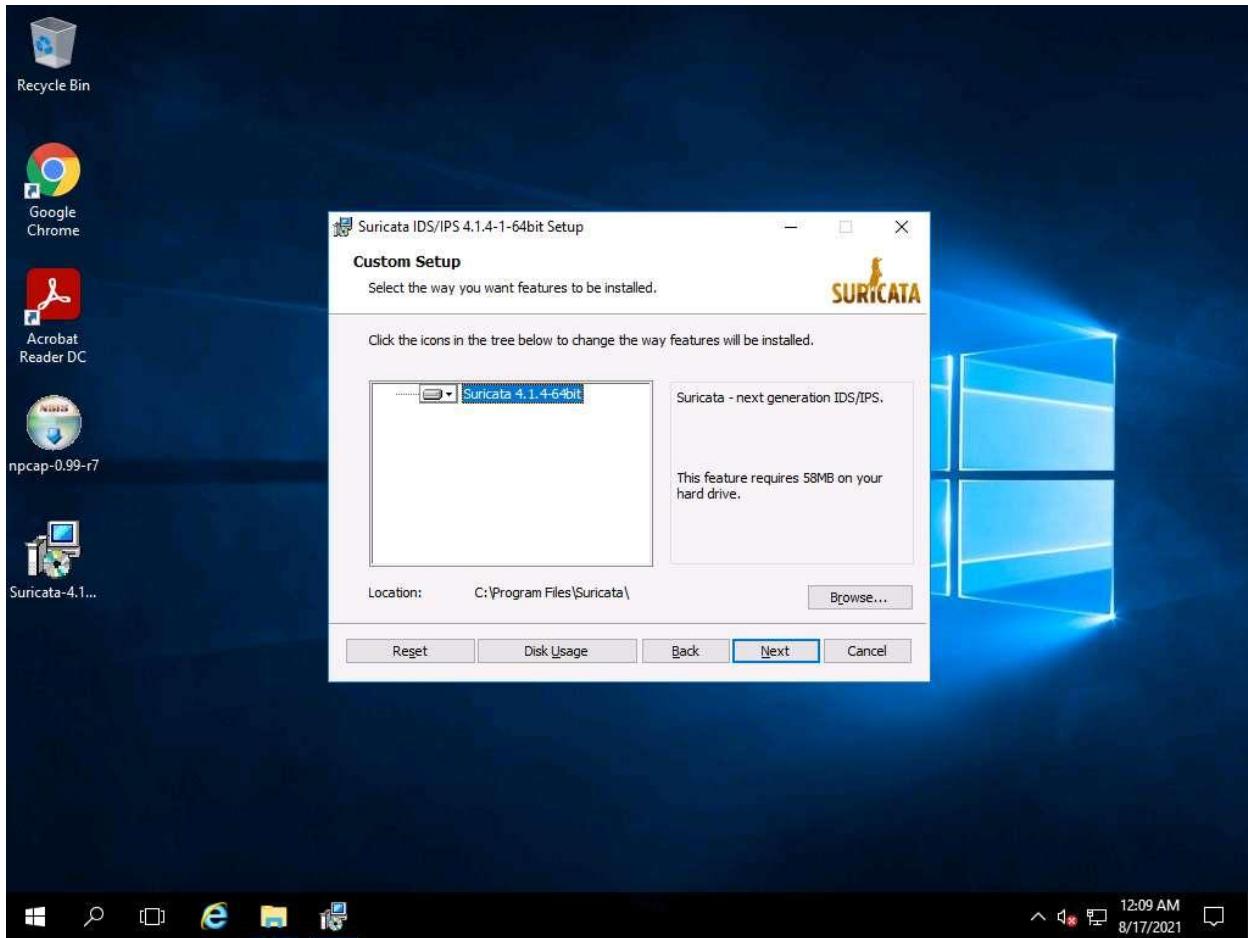
31. Paste the Suricata-4.1.4-1-64bit.msi file on the desktop.
32. Double click Suricata-4.1.4-1-64bit.msi. The Suricata.IDS/IPS2.1.2-1-64bit Setup window will appear. Click Next.



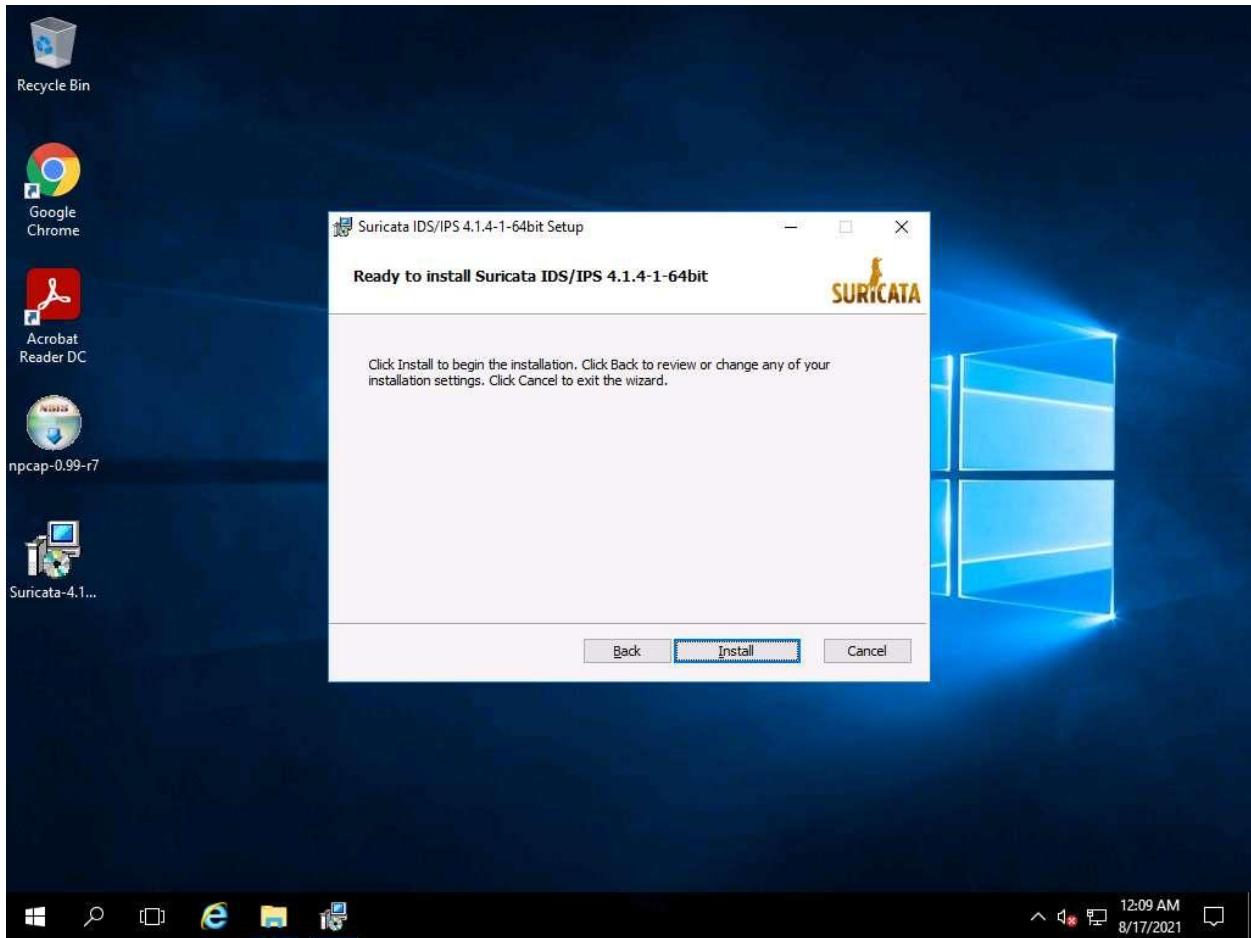
33. Check I accept the terms in the License Agreement to accept the license, and click Next.



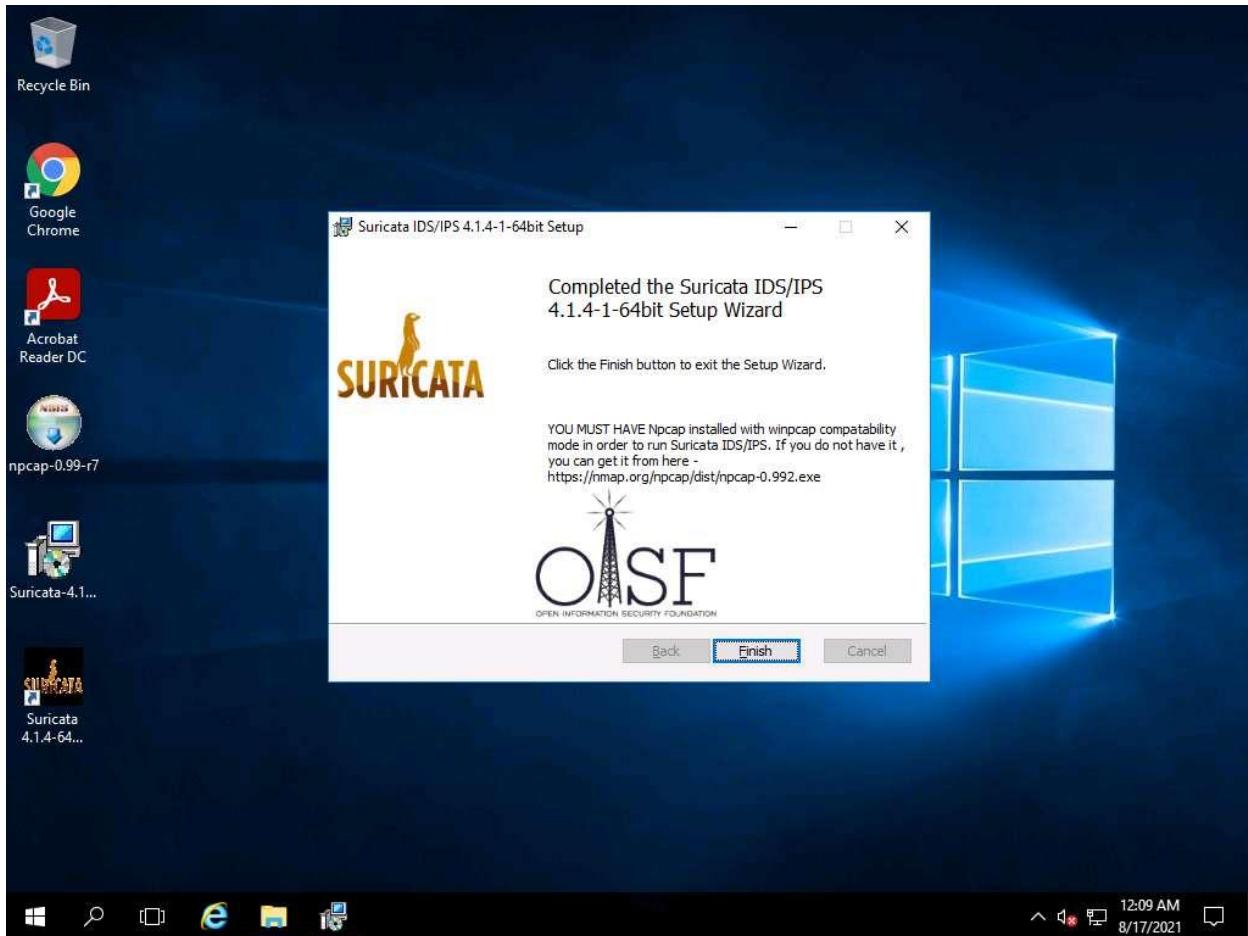
34. Click Next to continue the installation as shown in the screenshot below.



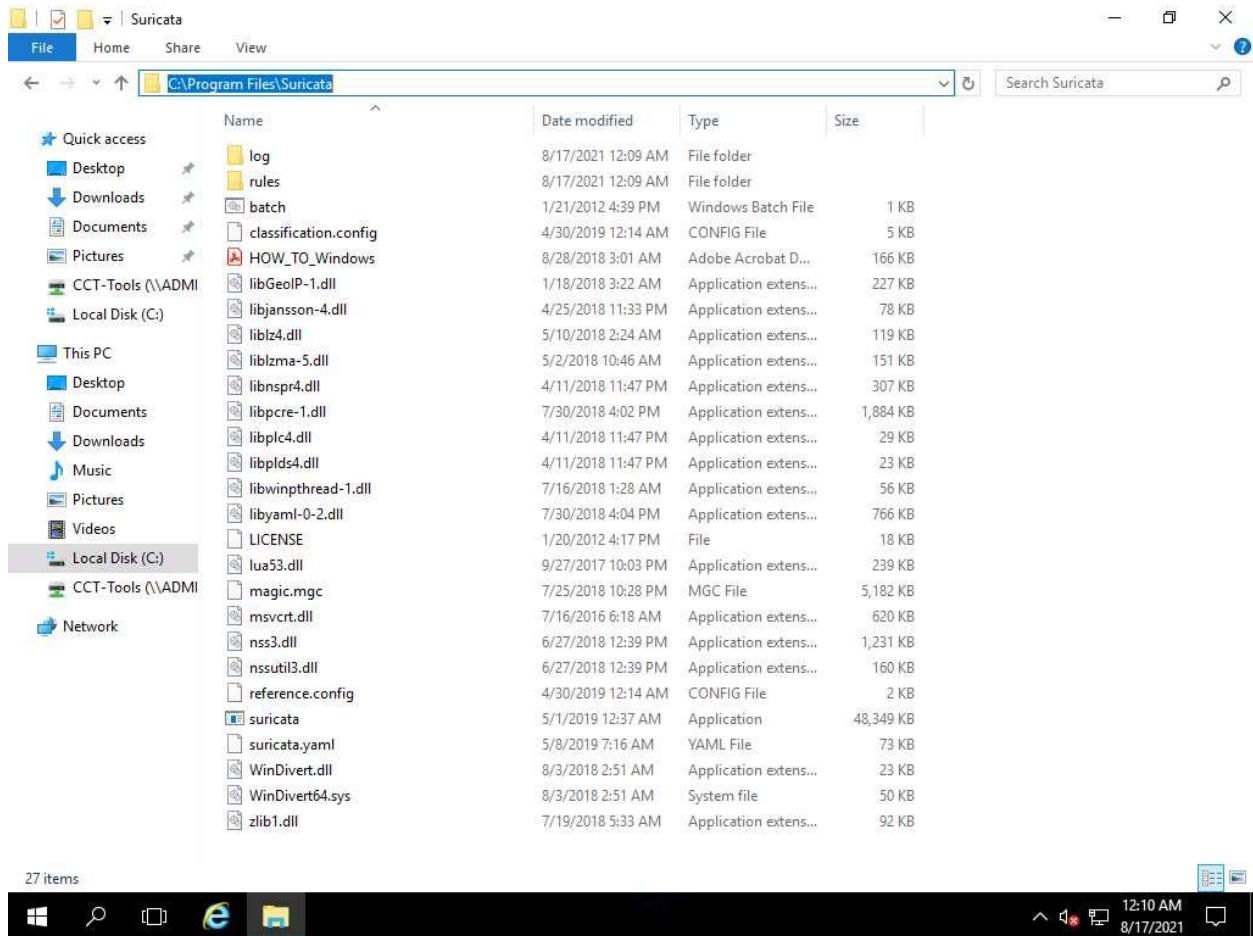
35. Click Install to continue the installation process.



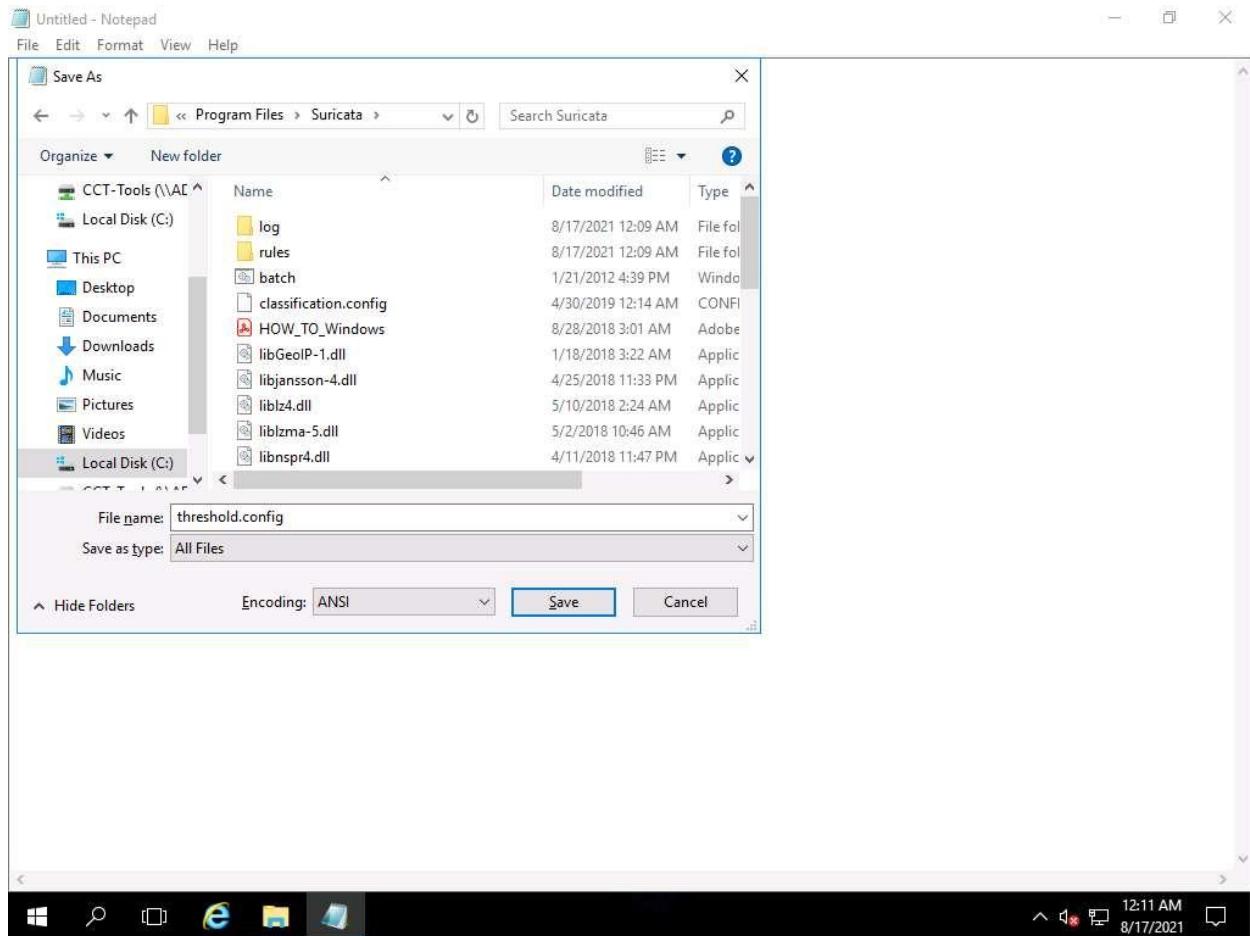
36. Click Finish to complete the installation process.



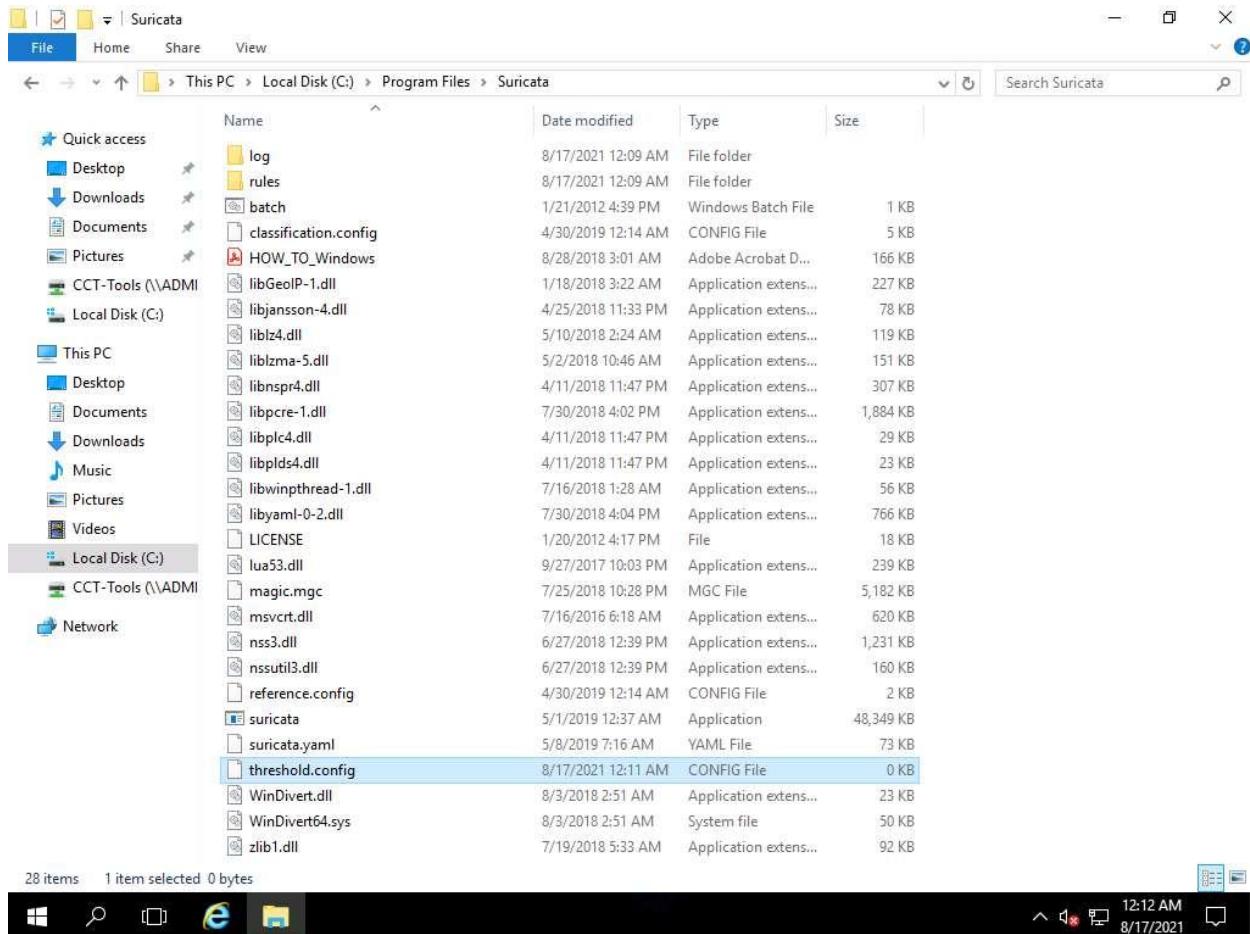
37. After Suricata IDS is successfully installed, the Suricata directory will be created under the C:\Program Files\Suricata.



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.

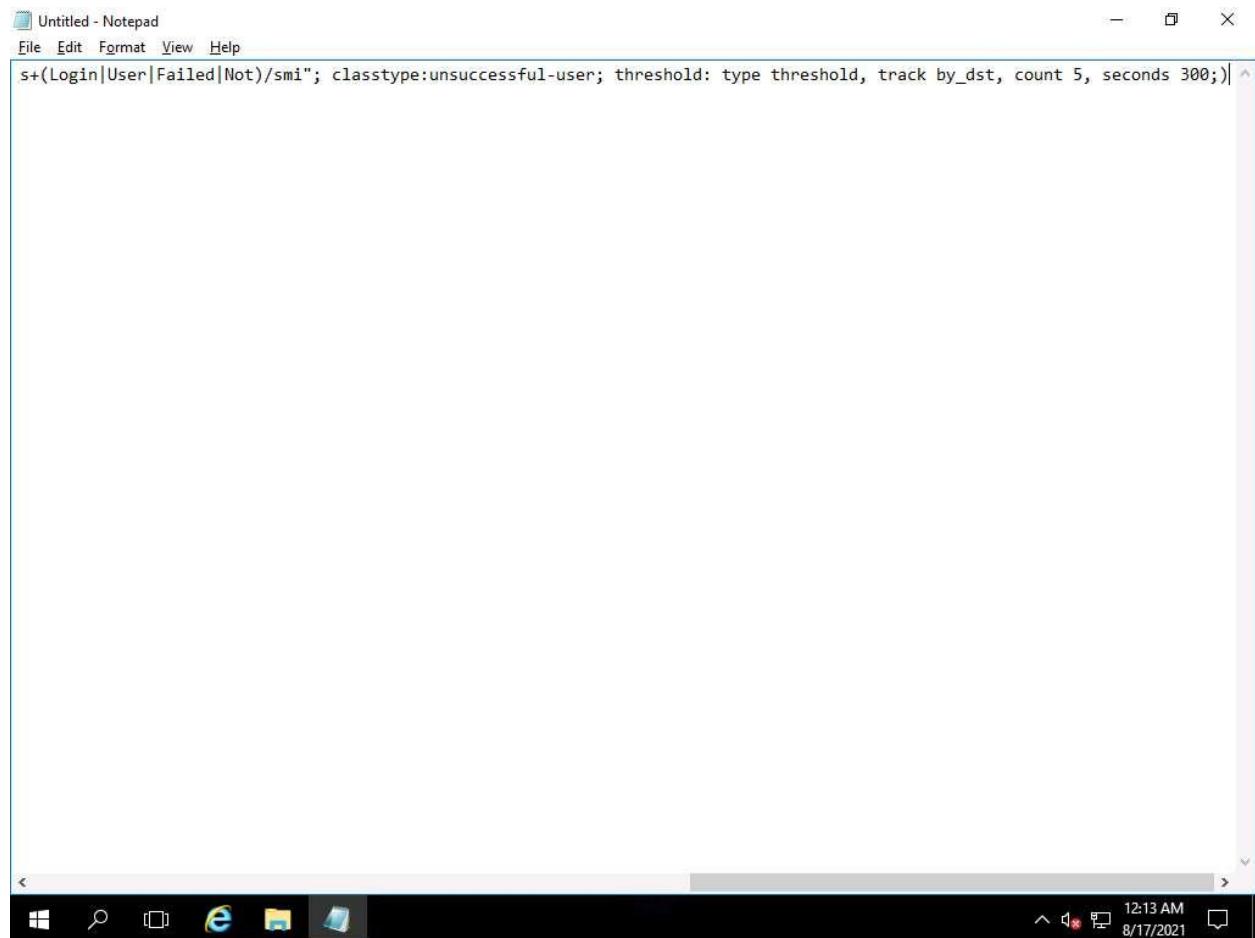


40. The Suricata IDS generates the alert based on the ruleset. A security professional can set the custom rule using the .rule file as shown in the following steps.
41. First, the local.rules file needs to be created. The local.rules file includes custom rules. We can create 'n' number of files for various 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:

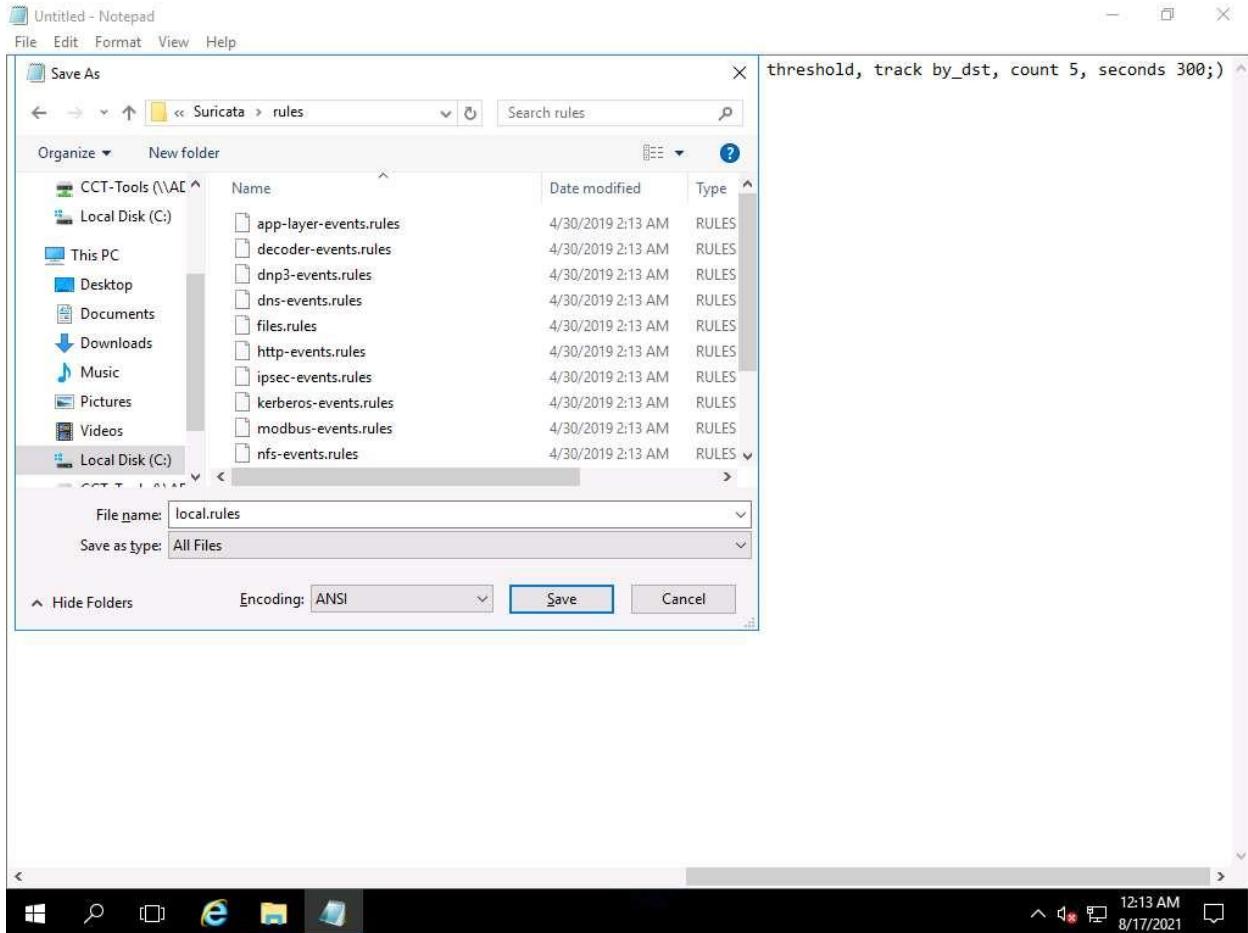
TypeCopy

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

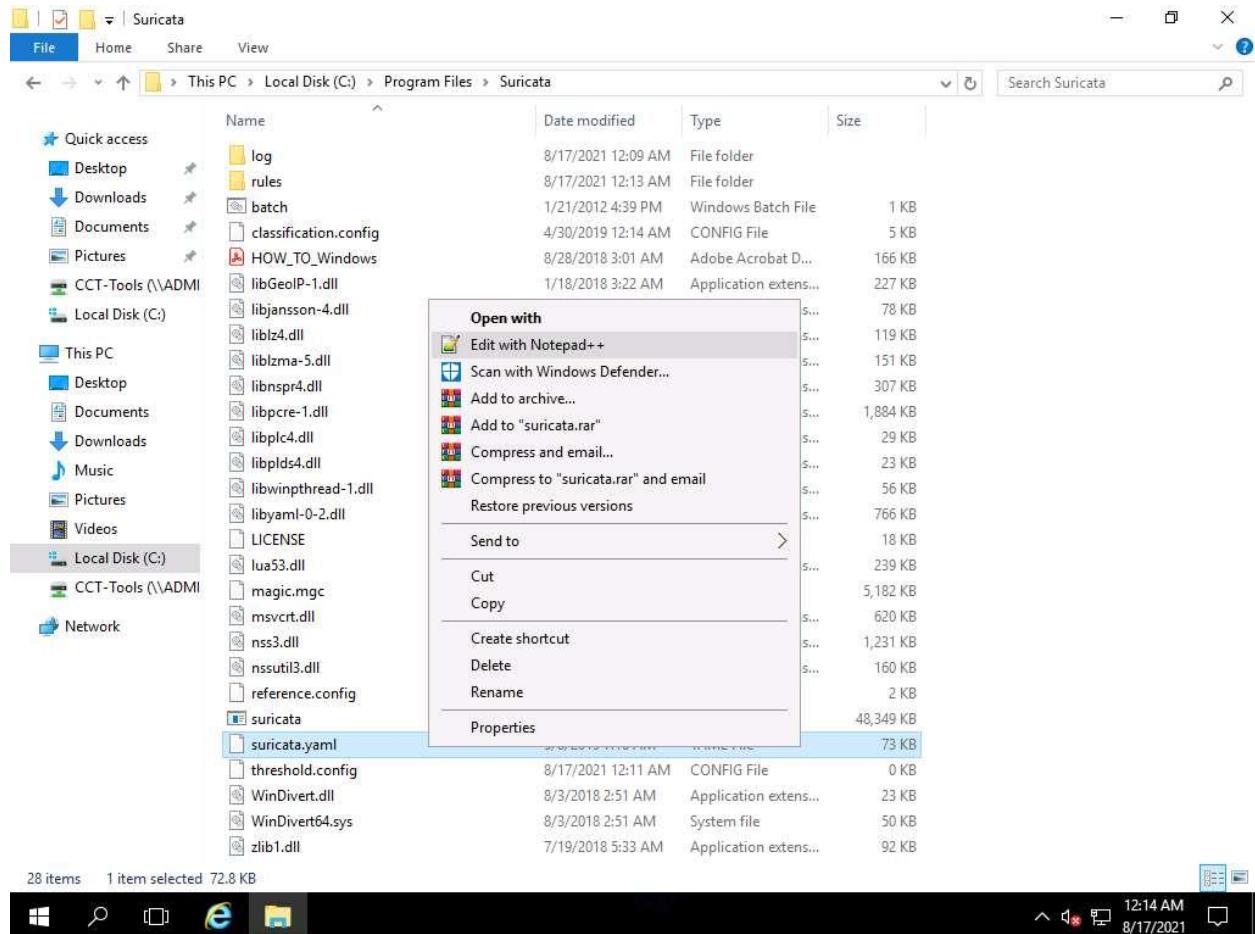
```
pcre:"/530\s+(Login|User|Failed|Not)/smi";      classtype:unsuccessful-user;  
threshold: type threshold, track by_dst, count 5, seconds 300;)
```



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.

C:\Program Files\Suricata\suricata.yaml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Undo Ctrl+Z or Alt+Backspace  
Redo Ctrl+Y or Ctrl+Shift+Z

Cut Ctrl+X or Shift+DEL  
Copy Ctrl+C or Ctrl+INS  
Paste Ctrl+V or Shift+INS  
Delete DEL  
Select All Ctrl+A  
Begin/End Select

Copy to Clipboard >  
Indent >  
Convert Case to >  
Line Operations >

Comment/Uncomment > **Block Comment Ctrl+Shift+Q**

Auto-Completion >  
EOL Conversion >  
Blank Operations >  
Paste Special >  
On Selection >

Column Mode...  
Column Editor... Alt+C  
Character Panel  
Clipboard History

Set Read-Only  
Clear Read-Only Flag

- emerging-web\_specific\_apps.rules  
- emerging-worm.rules  
- tor.rules  
# - decoder-events.rules #available in suricata sources under rules dir  
# - stream-events.rules #available in suricata sources under rules dir

YAML Ain't Markup Language length: 74,638 lines: 1,940 Ln: 1,910 Col: 13 Sel: 1,101 | 45 Unix (LF) UTF-8 INS

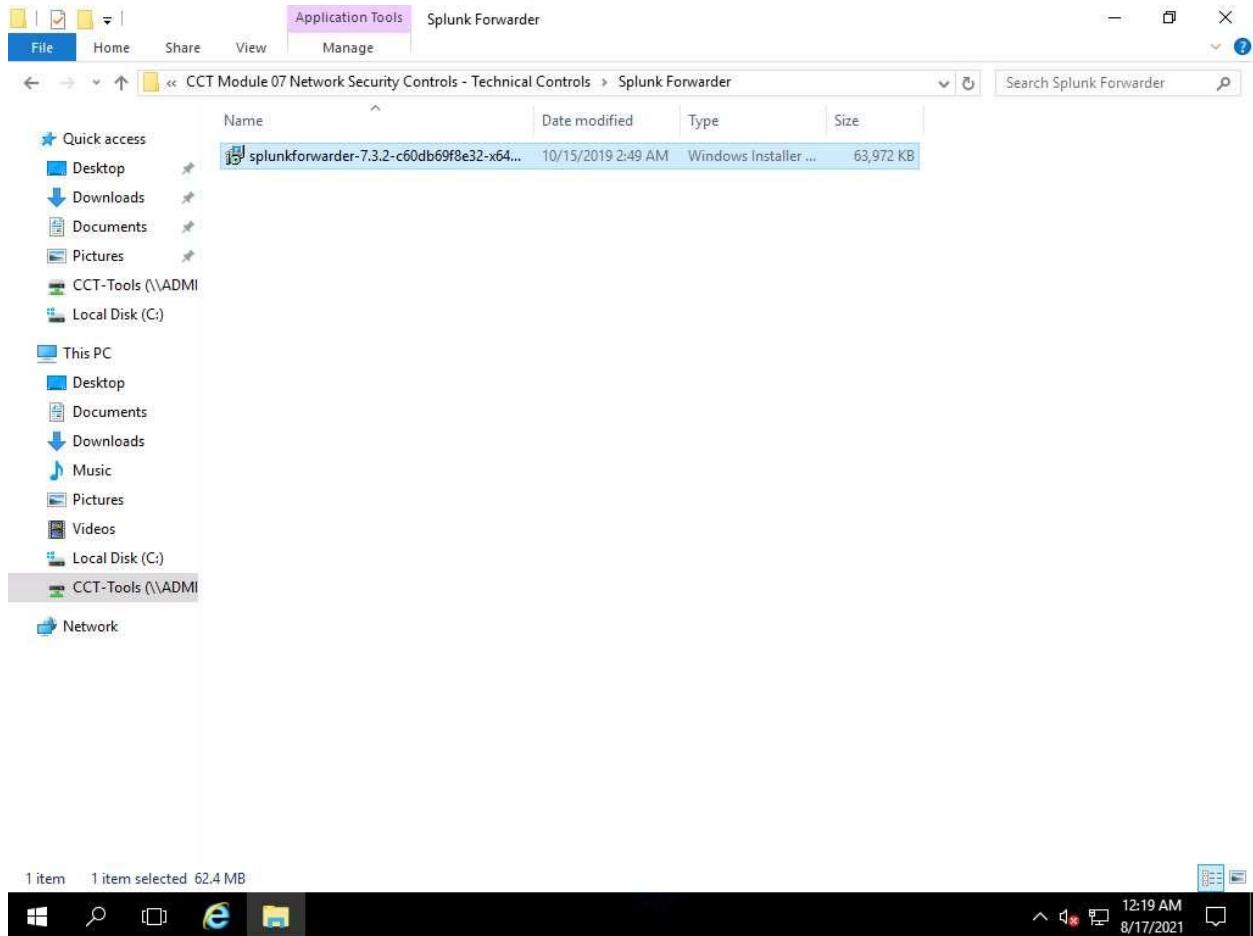
12:16 AM 8/17/2021

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

The screenshot shows the Notepad++ application window with the file 'suricata.yaml' open. The code is written in YAML and defines rule paths and files. A red box highlights the 'rule-files:' section, which contains several sub-rules like 'local.rules', 'botcc.rules', etc.

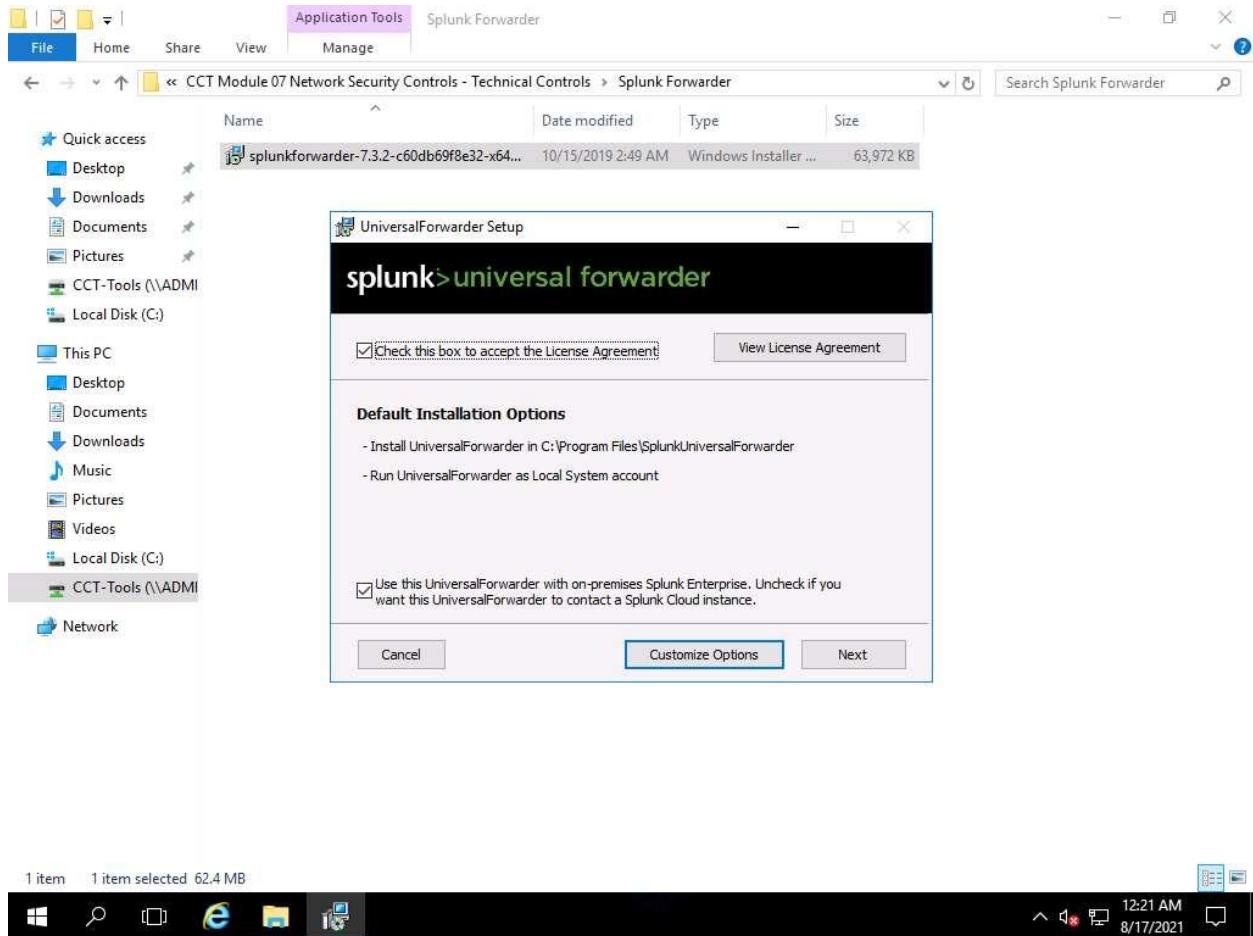
```
1846 ##  
1847 ## If this section is completely commented out move down to the "Advanced rule  
1848 ## file configuration".  
1849 ##  
1850  
1851 #default-rule-path: C:\\Program Files\\Suricata\\rules\\\\  
1852 #rule-files:  
1853 # - suricata.rules  
1854  
1855 ##  
1856 ## Advanced rule file configuration.  
1857 ##  
1858 ## If this section is completely commented out then your configuration  
1859 ## is setup for suricata-update as it was most likely bundled and  
1860 ## installed with Suricata.  
1861 ##  
1862  
1863 default-rule-path: C:\\Program Files\\Suricata\\rules\\\\  
1864  
1865 rule-files:  
1866   |- local.rules  
1867   |- botcc.rules  
1868   |- botcc.portgrouped.rules  
1869   |- ciarmy.rules  
1870   |- compromised.rules  
1871   |- drop.rules  
1872   |- dshield.rules  
1873   |- emerging-activex.rules  
1874   |- emerging-attack_response.rules  
1875   |- emerging-chat.rules  
1876   |- emerging-current_events.rules  
1877   |- emerging-dns.rules  
1878   |- emerging-dos.rules  
1879   |- emerging-exploit.rules  
1880   |- emerging-ftp.rules  
1881   |- emerging-games.rules  
1882   |- emerging-icmp_info.rules
```

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.

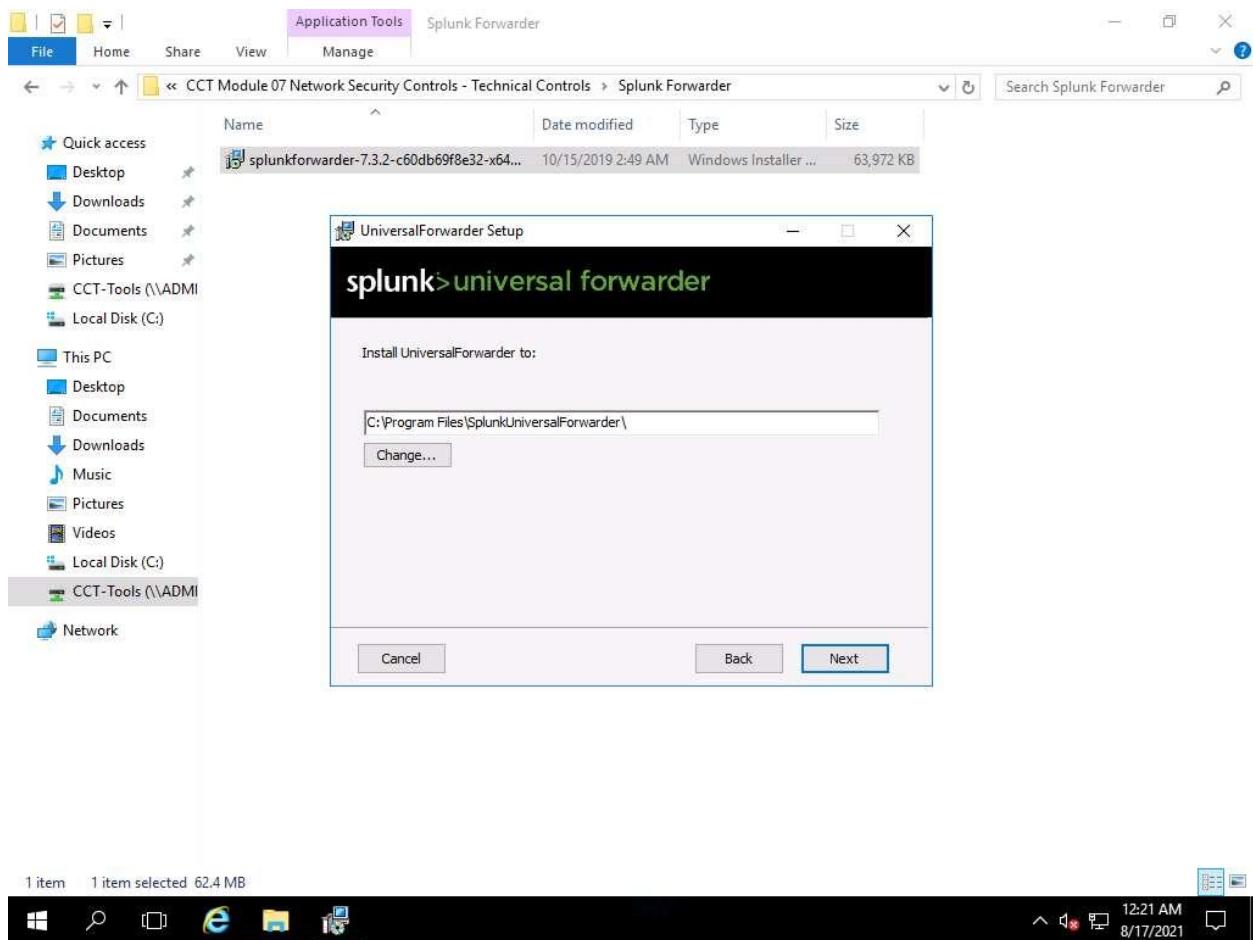


If a Security Warning pop-up appears, click on Run.

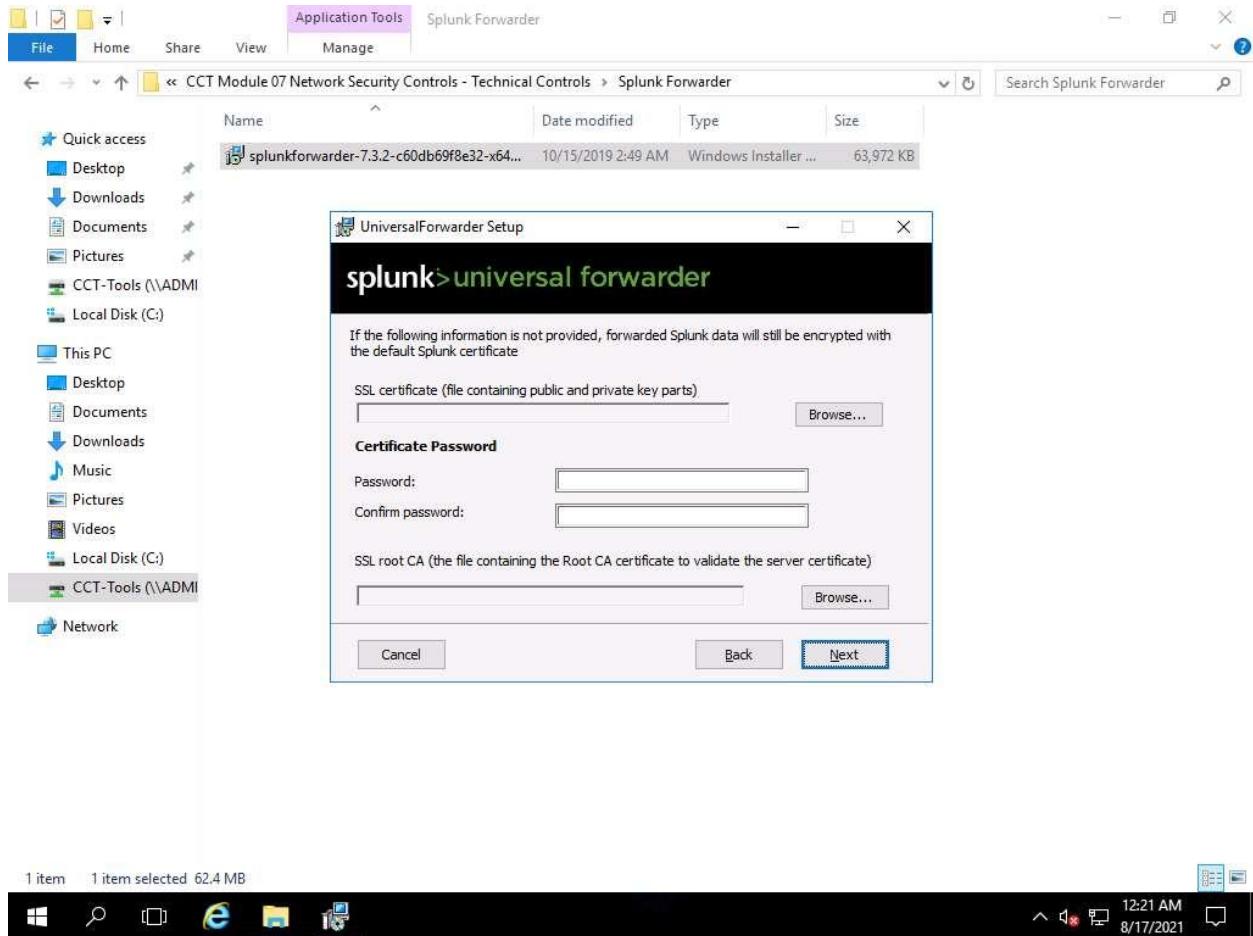
54. Once the UniversalForwarder Setup window appears, check Check the box to accept the License Agreement and click on Customize Options.



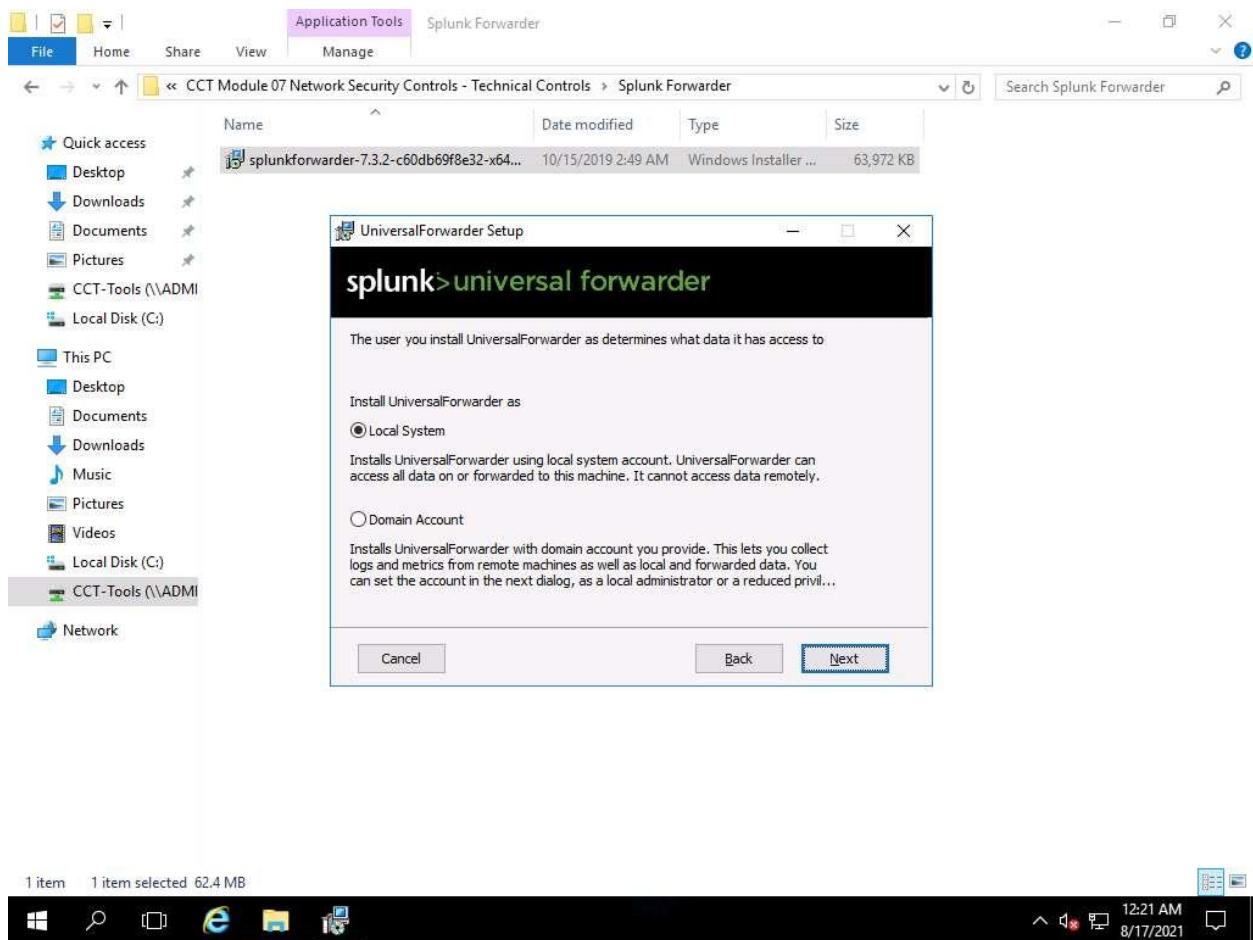
55. Leave the installation path set to the default location and click on Next.



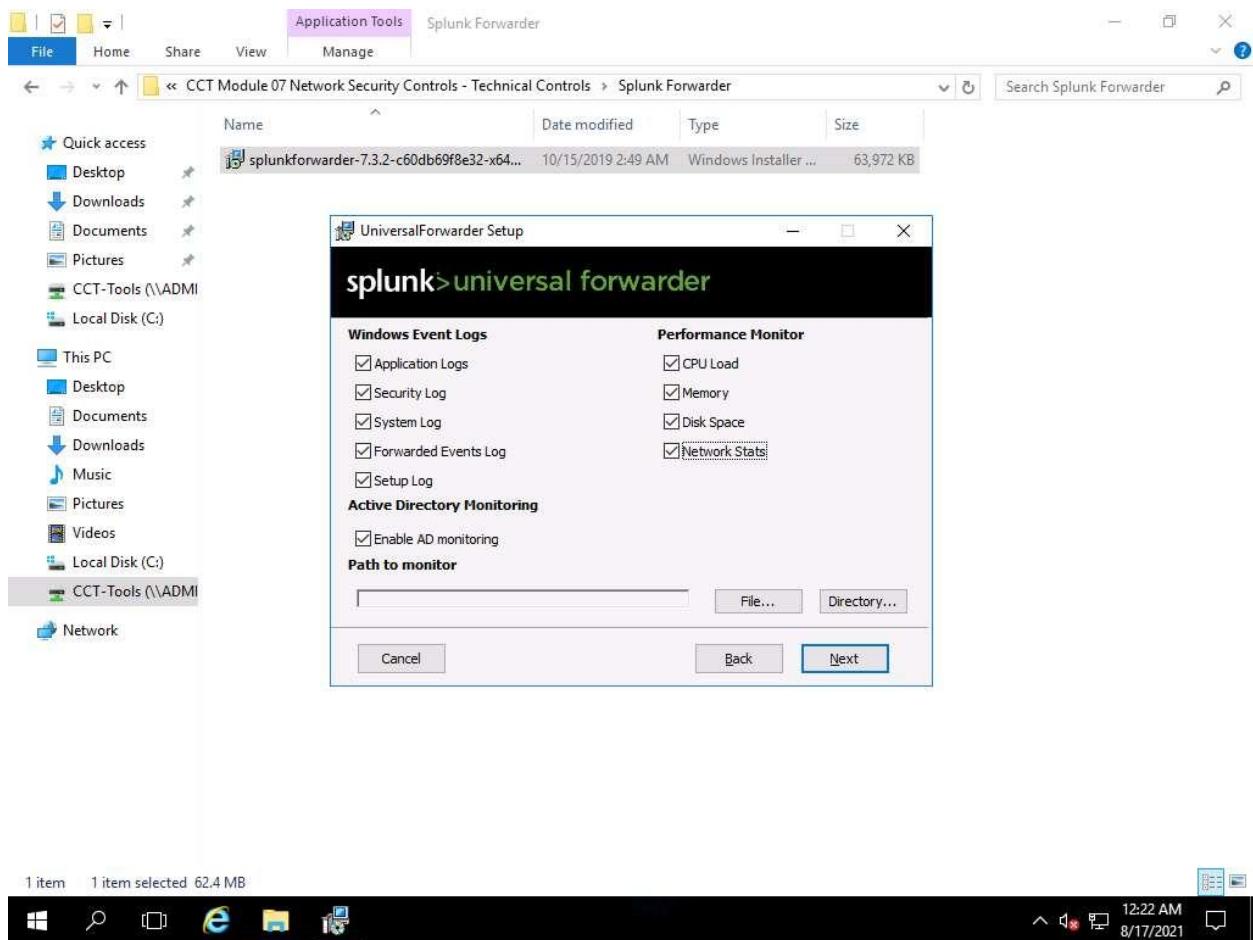
56. Click on Next in the Splunk certificate section.



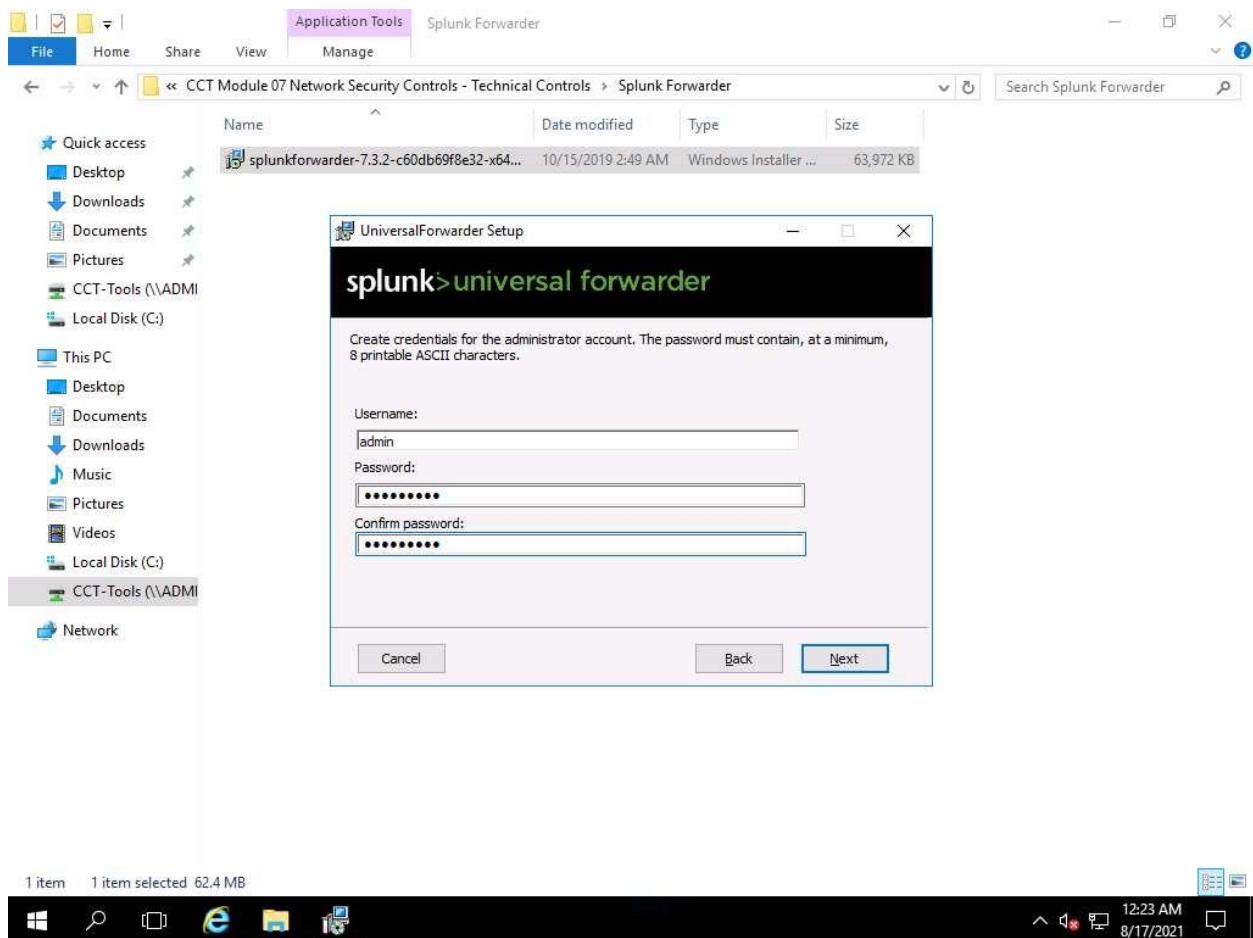
57. In the next step, select the Local System radio button to install Universal Forwarder as a Local System and then click on Next.



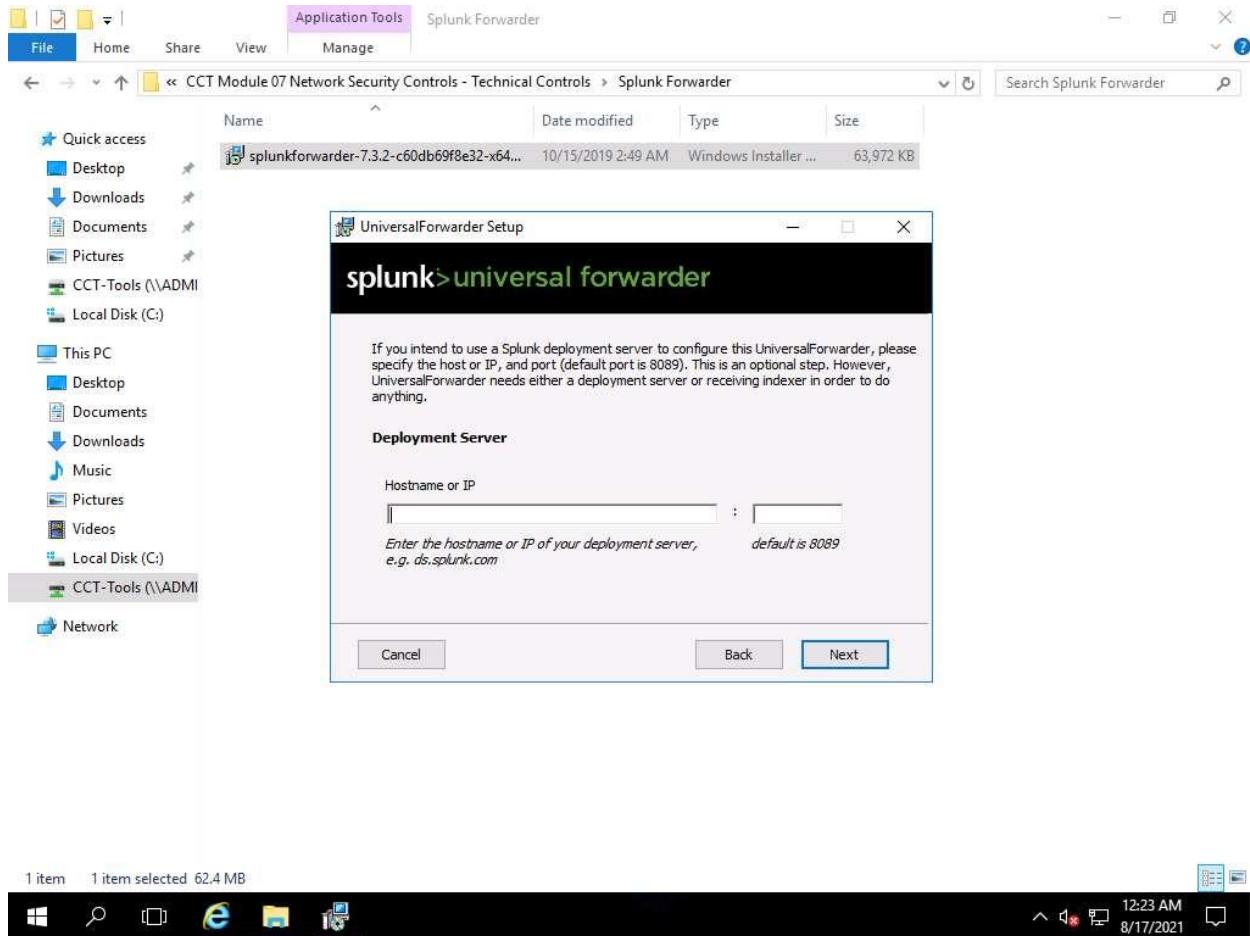
58. Next, check all entities under Windows Event Logs, Active Directory Monitoring and Performance Monitor and click on Next.



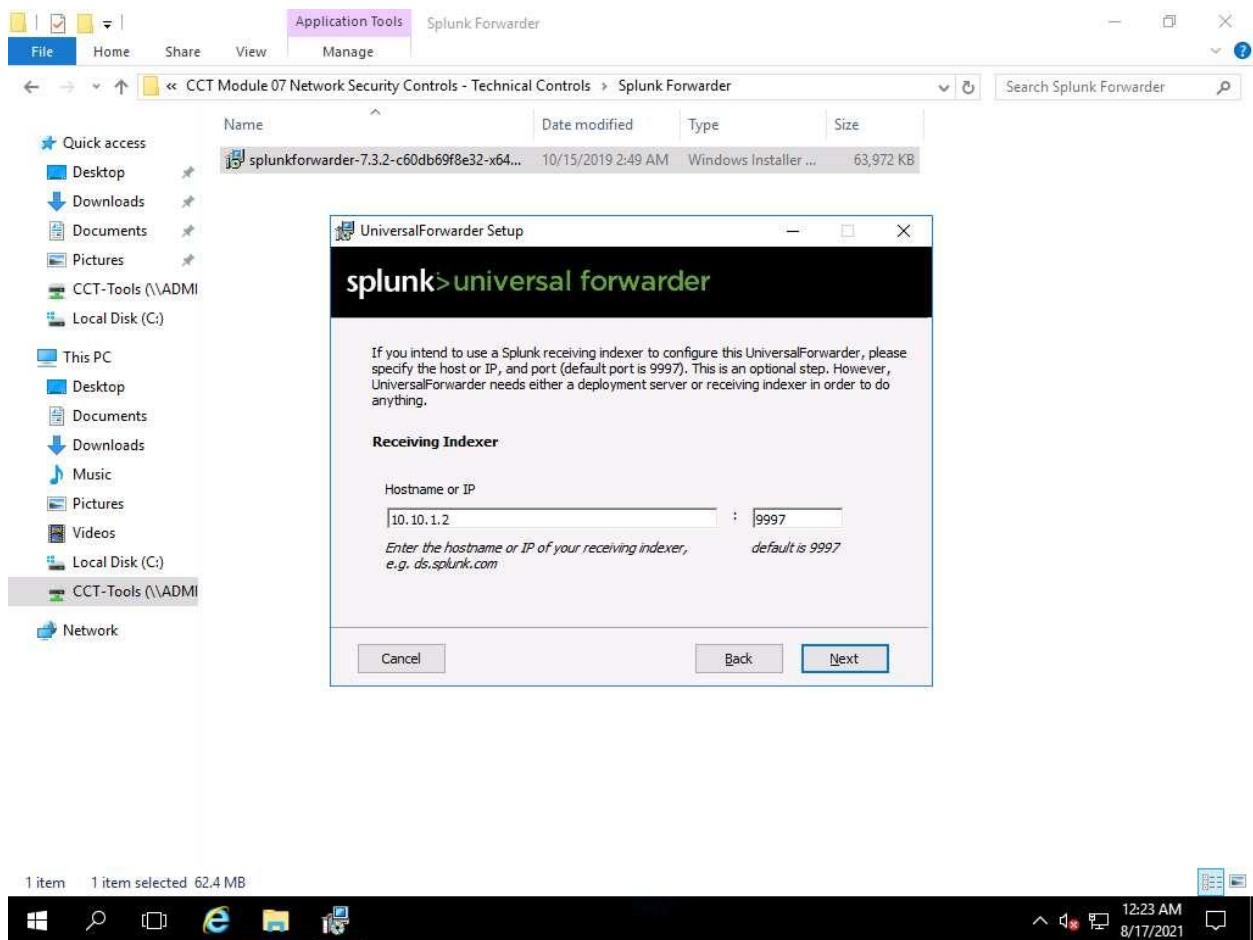
59. Create credentials for the administrator account; type username "admin" and password "admin@123" and click on Next.



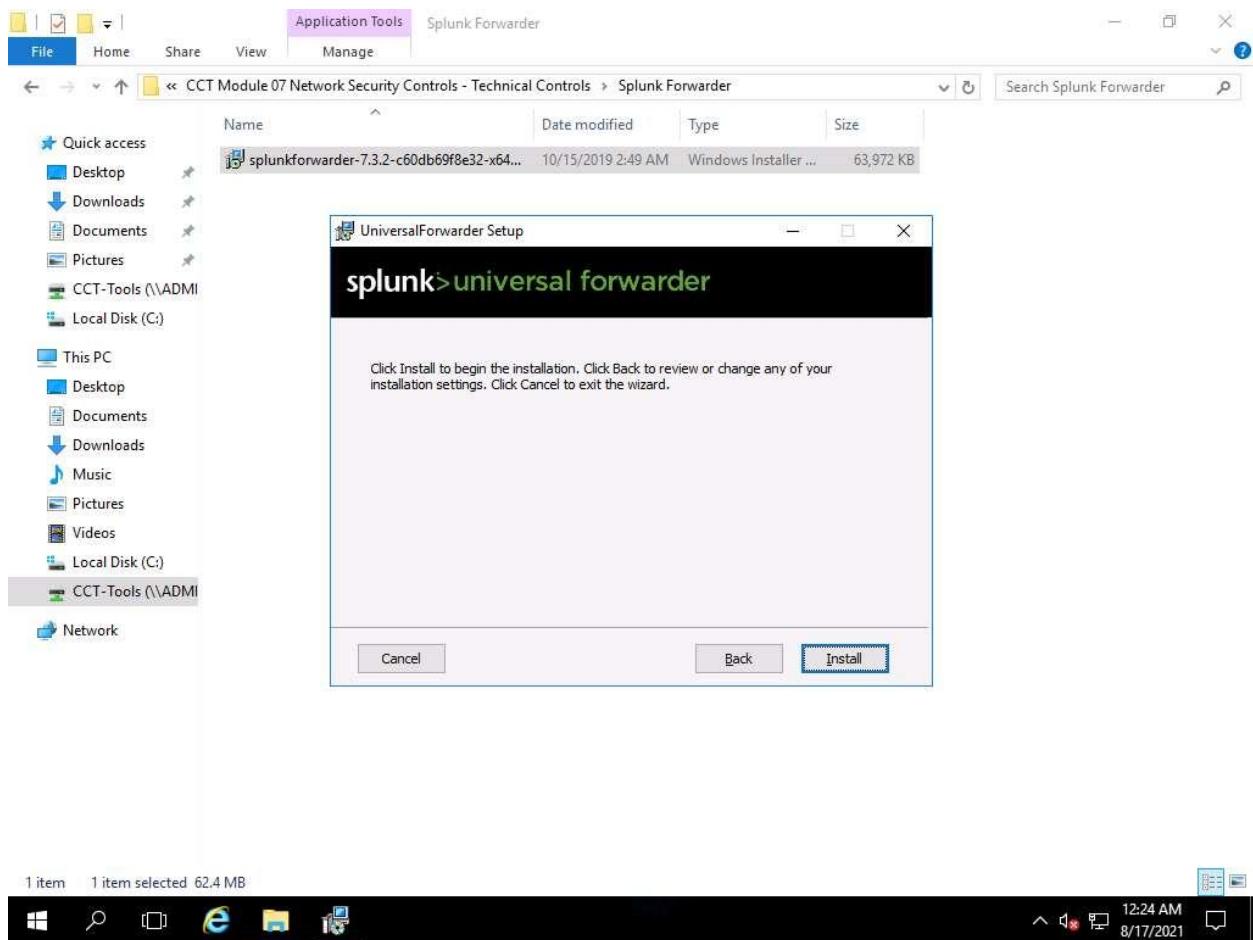
60. Leave the Deployment Server section without issuing the deployment IP and port number details, and click on Next.



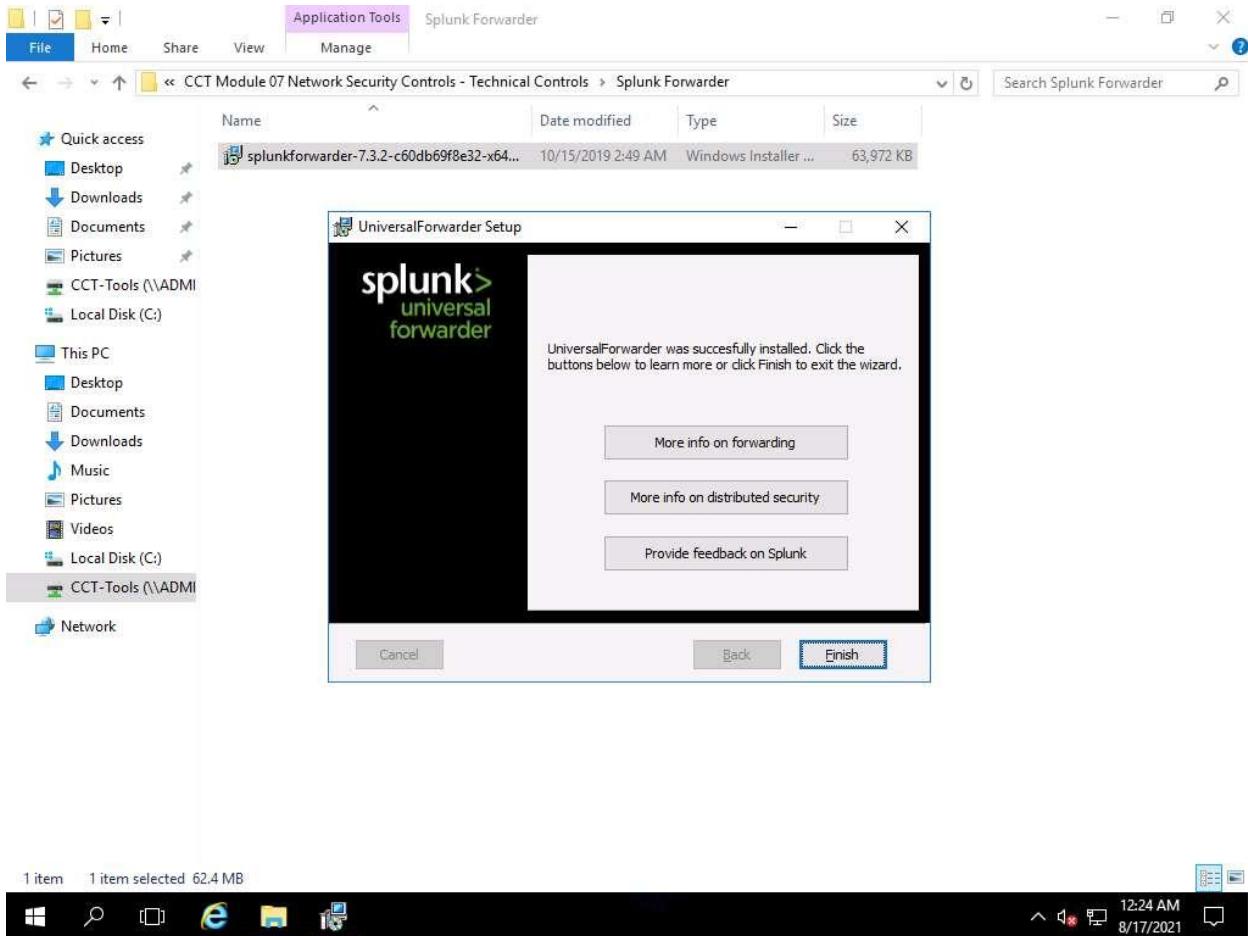
61. In the Receiving Indexer section, enter the IP address for Admin Machine-1, namely, 10.10.1.2 in the Hostname or IP field; enter Port 9997 in the port field and click on Next.



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.

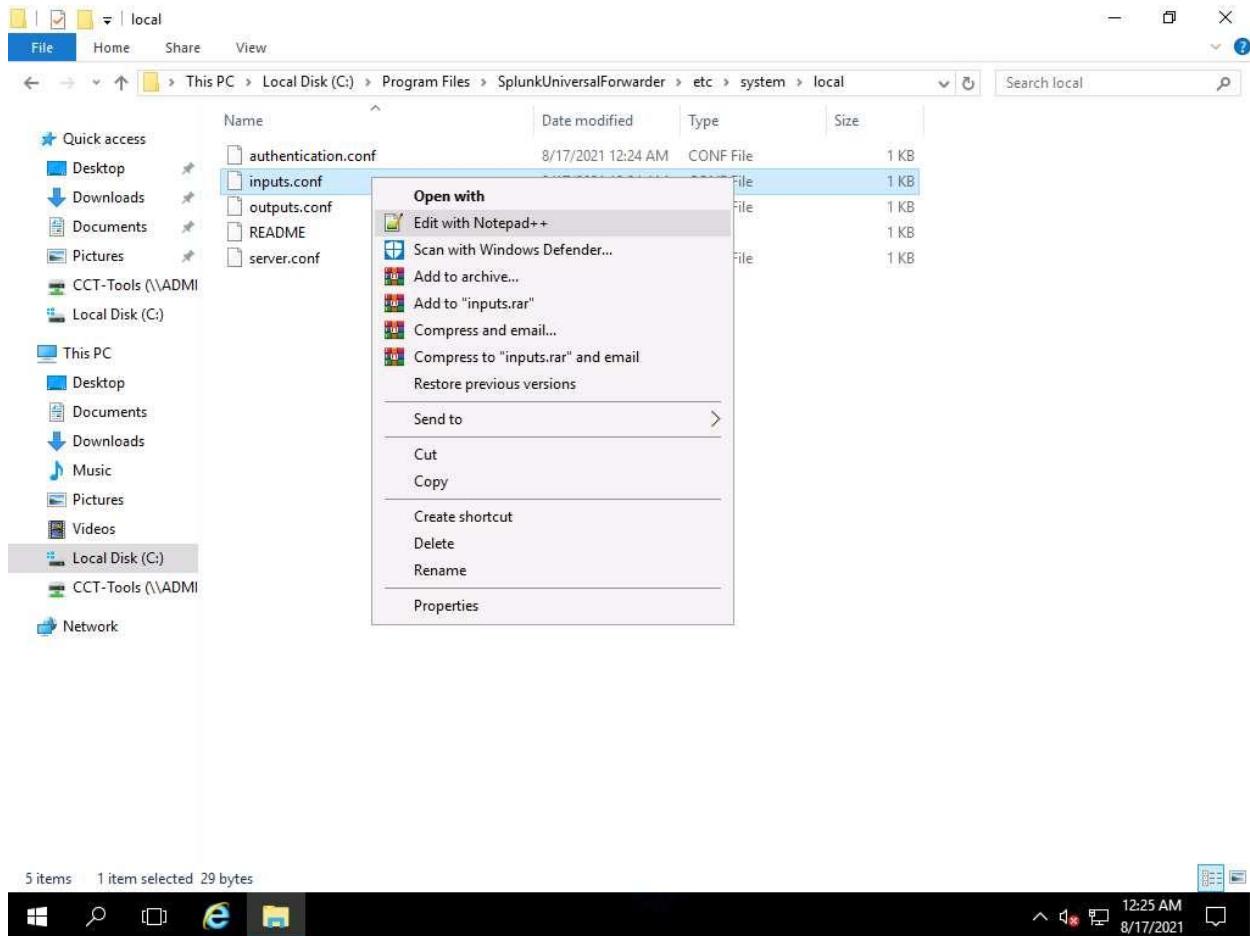


63. Click on Finish after the installation completes.



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

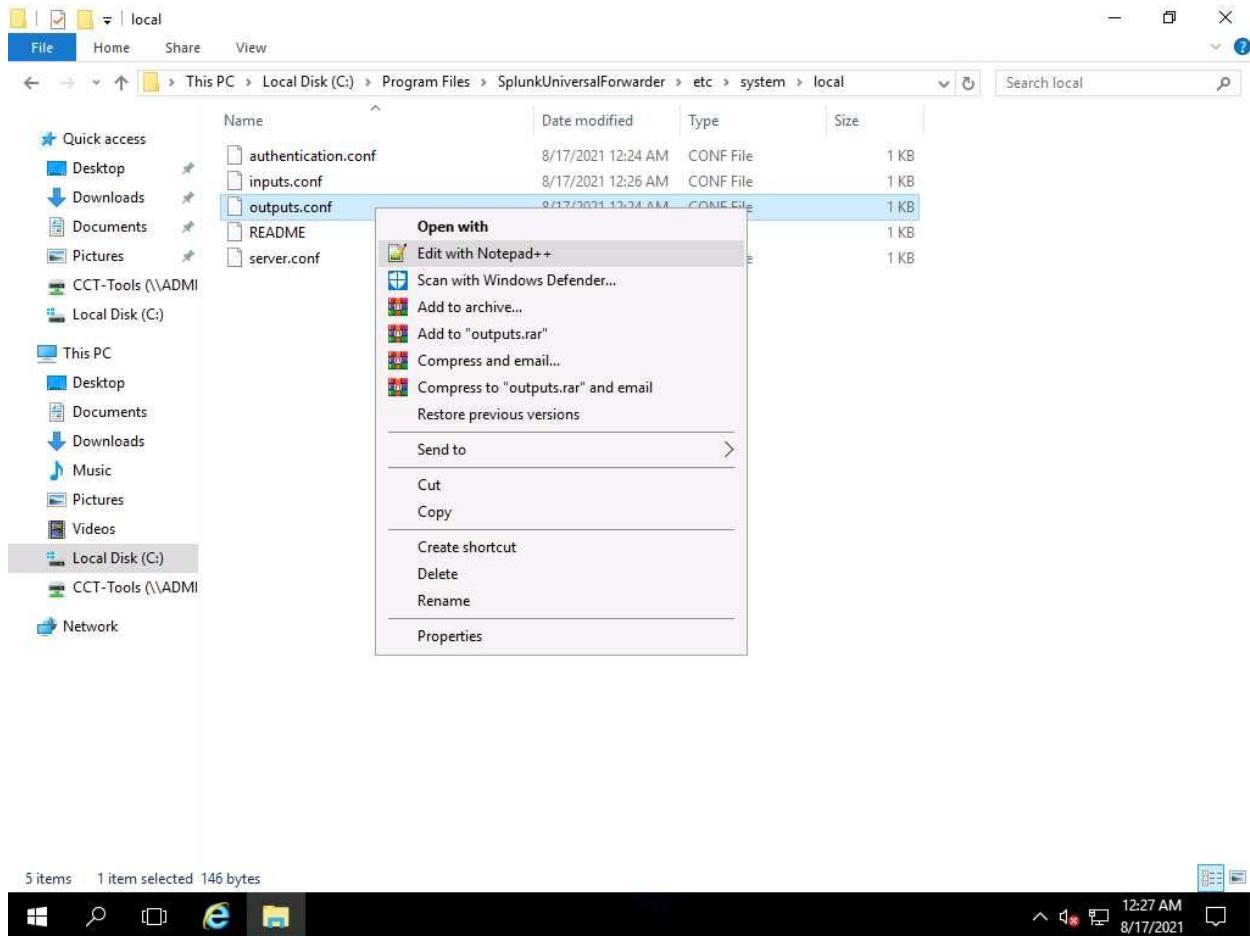
[monitor://C:\inetpub\logs\LogFiles]

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\*]

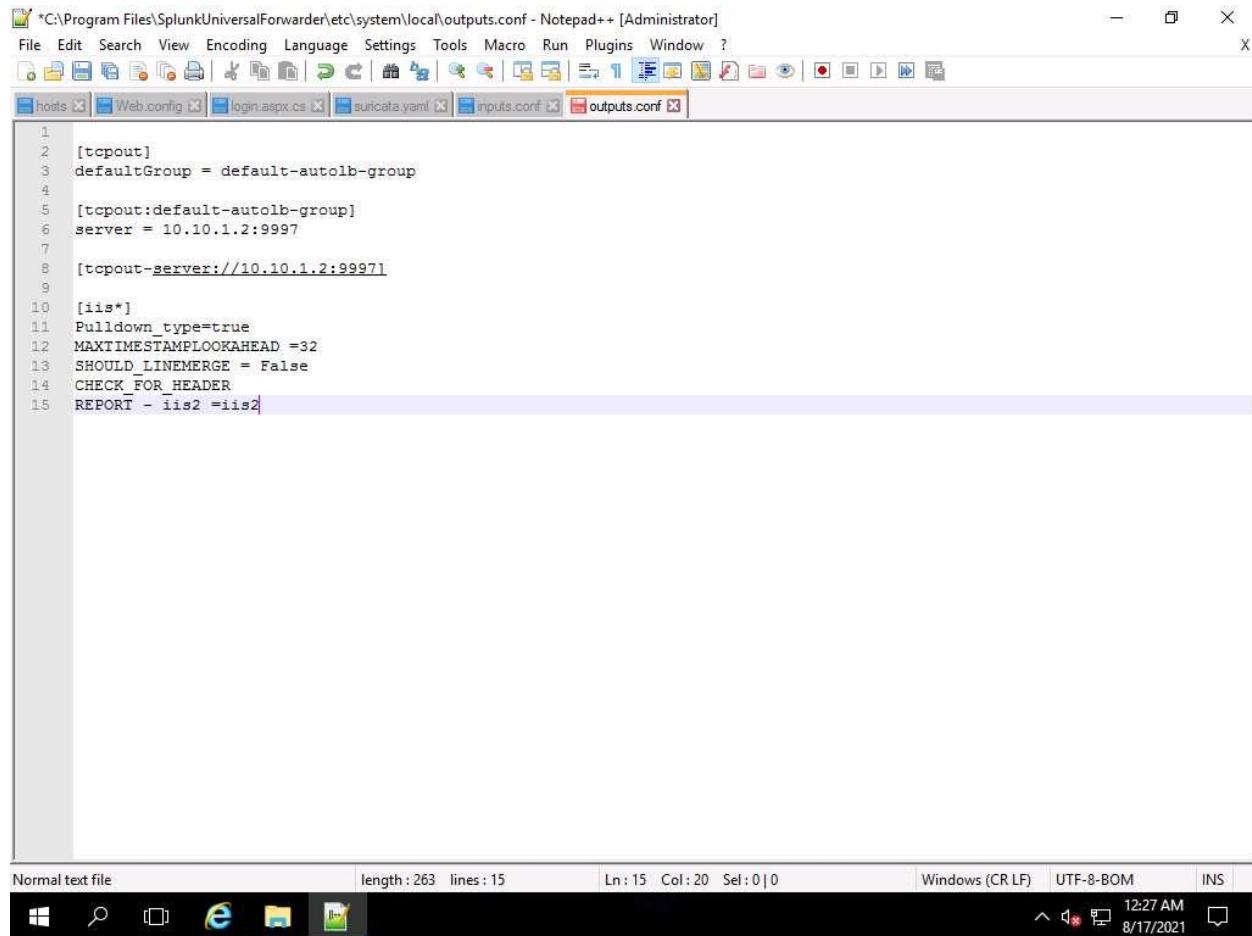
Pulldown\_type=true

MAXTIMESTAMPLOOKAHEAD =32

SHOULD\_LINEMERGE = False

CHECK\_FOR\_HEADER

REPORT – iis2 =iis2



```
1  [tcpout]
2  defaultGroup = default-autolb-group
3
4  [tcpout:default-autolb-group]
5  server = 10.10.1.2:9997
6
7  [tcpout-server://10.10.1.2:9997]
8
9  [iis*]
10 Pulldown_type=true
11 MAXTIMESTAMPLOOKAHEAD =32
12 SHOULD_LINEMERGE = False
13 CHECK_FOR_HEADER
14 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

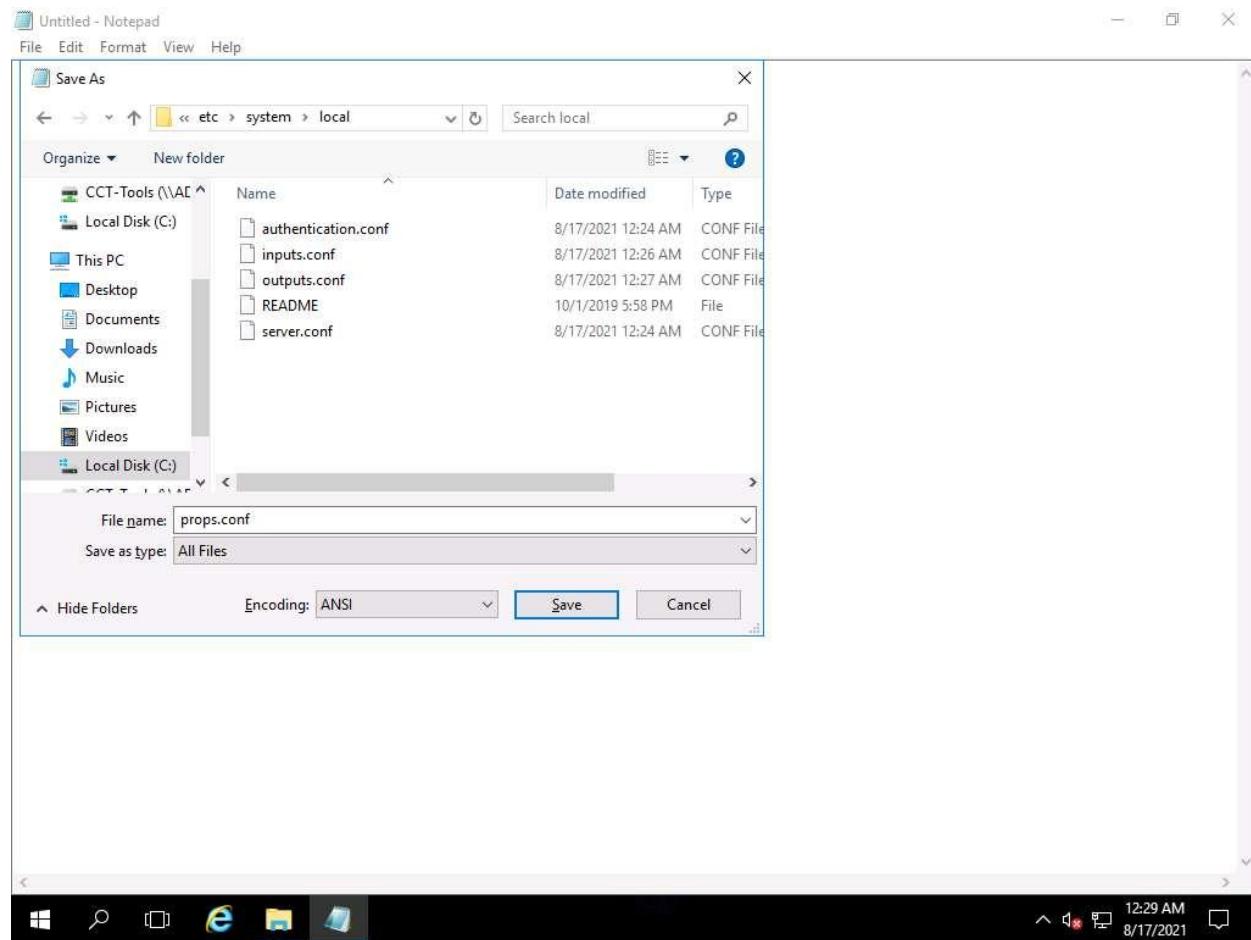
SHOULD\_LINEMERGE =False

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 = ^#.\*

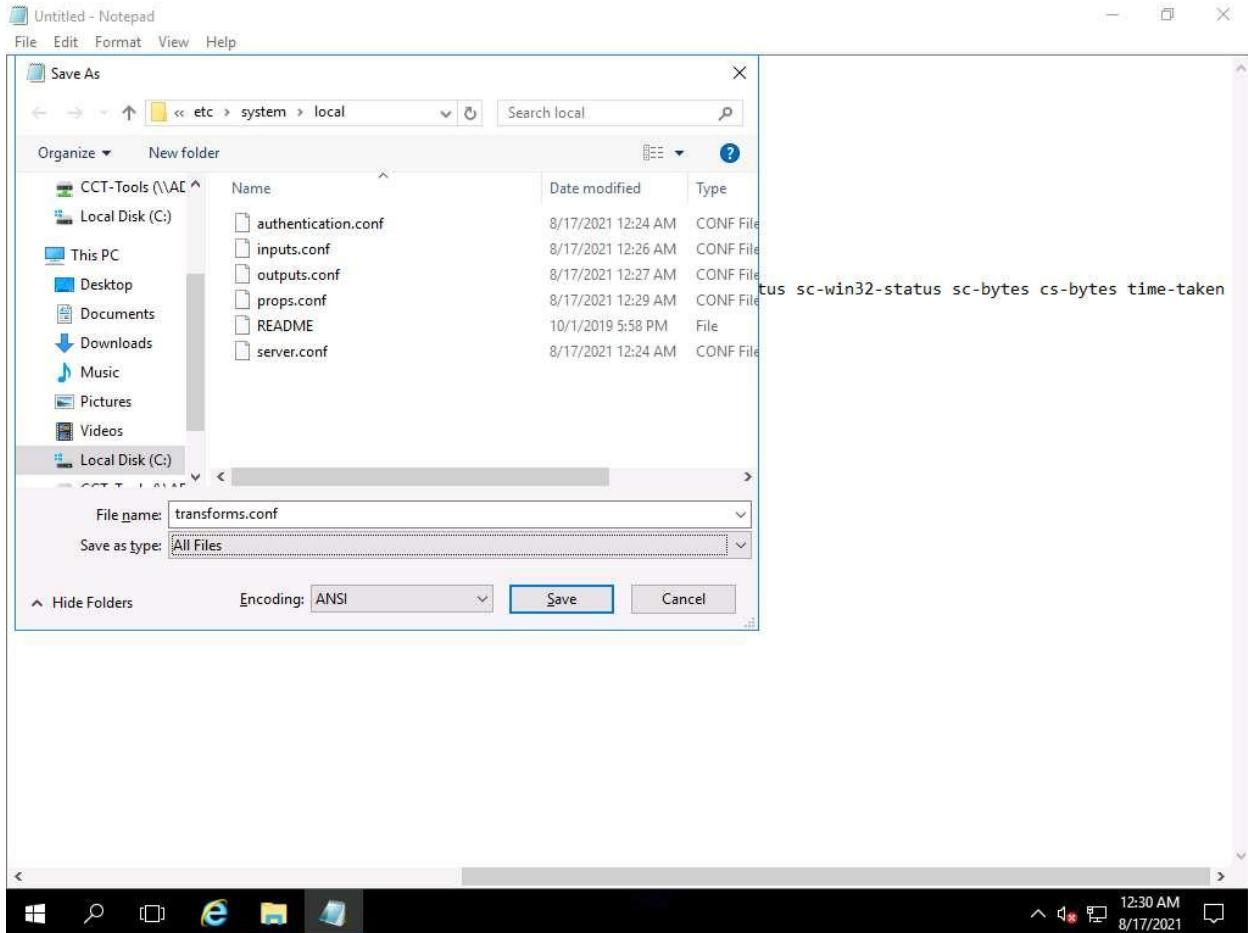
DEST\_KEY =queue

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.

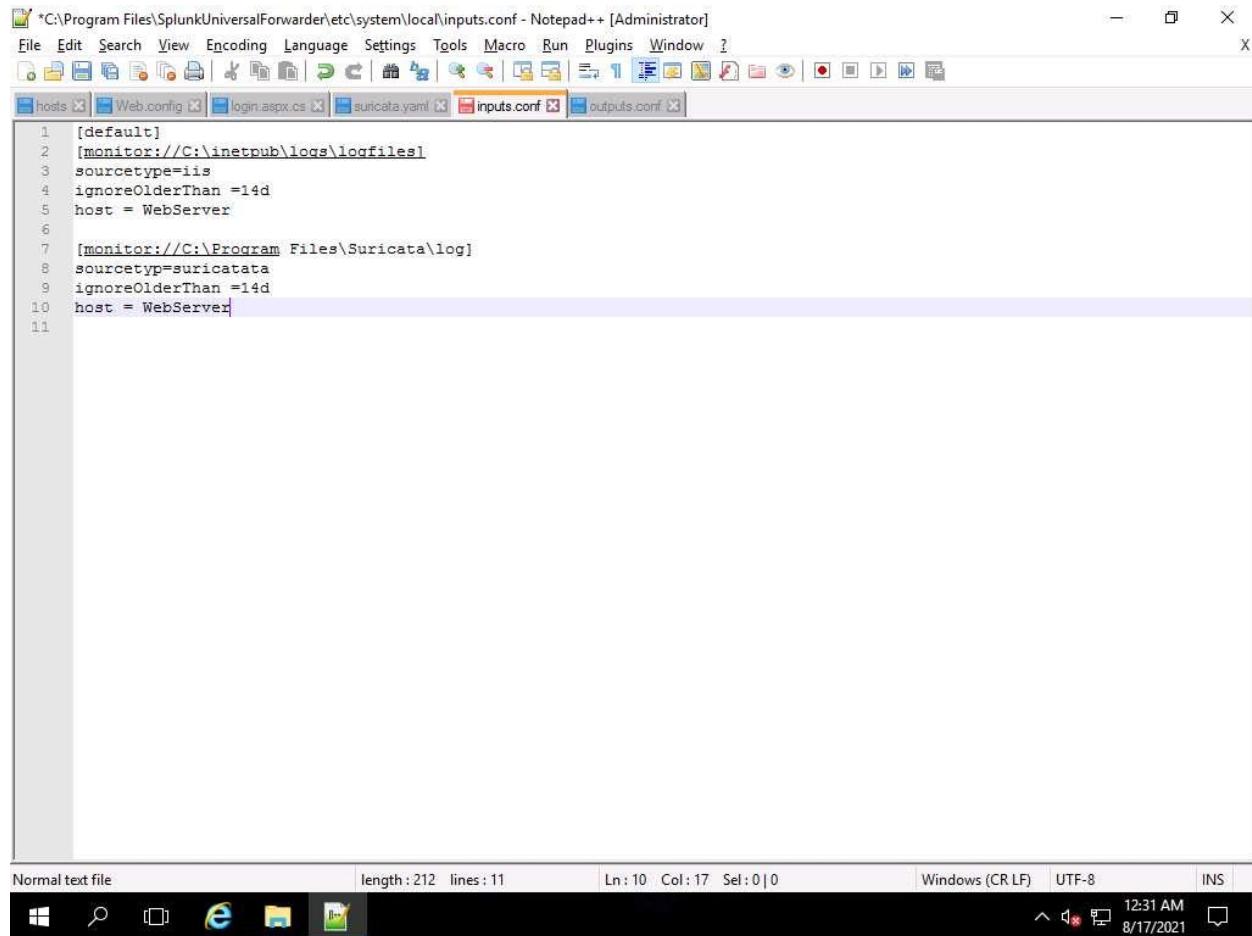
TypeCopy

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

sourcetype=suricatata

ignoreOlderThan =14d

host = WebServer



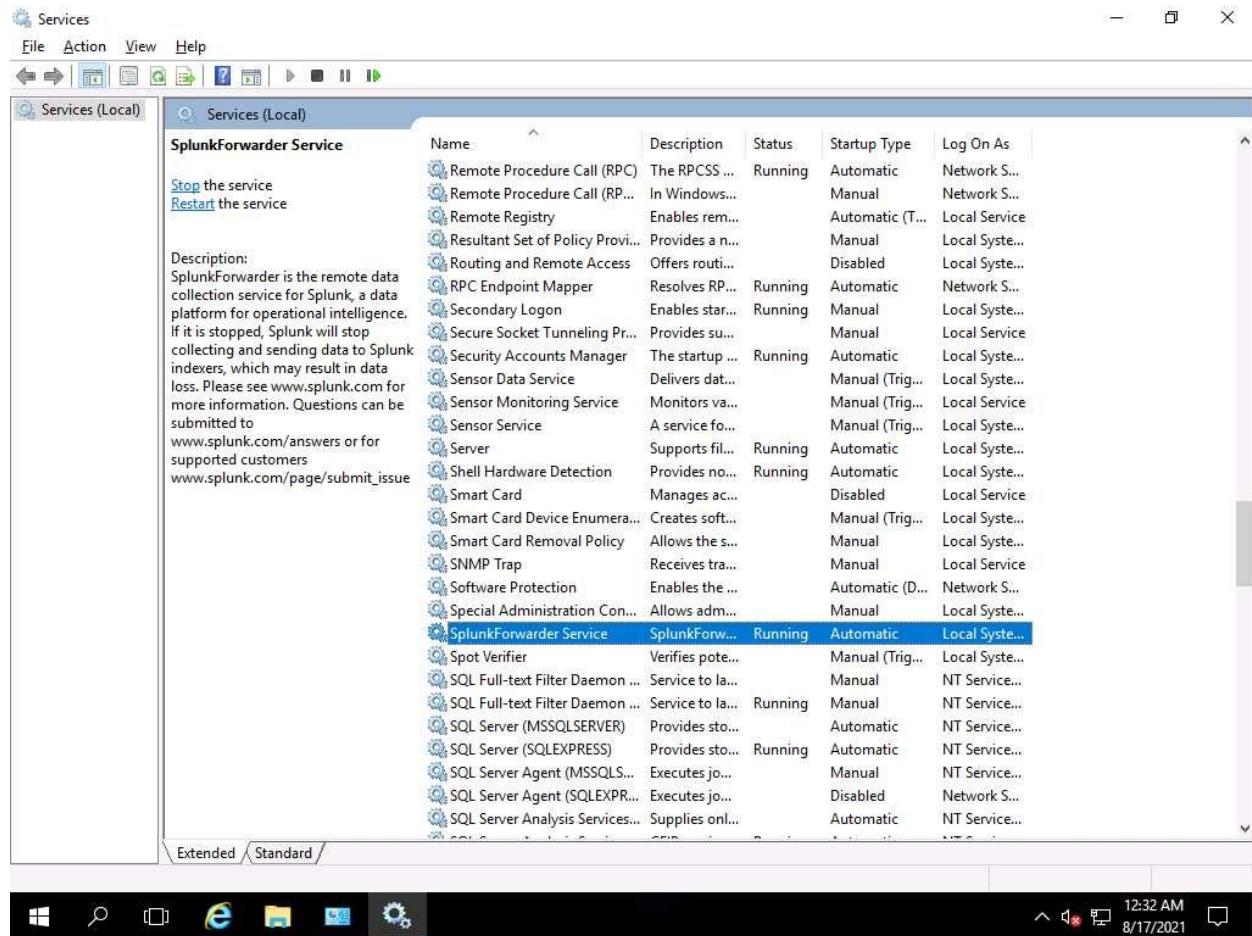
The screenshot shows a Notepad++ window with the title bar reading "C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++ [Administrator]". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and Help. Below the menu is a toolbar with various icons. The main editor area contains the following configuration code:

```
1 [default]
2 [monitor://C:\inetpub\logs\LogFiles]
3 sourcetype=iis
4 ignoreOlderThan =14d
5 host = WebServer
6
7 [monitor://C:\Program Files\Suricata\log]
8 sourcetype=suricatata
9 ignoreOlderThan =14d
10 host = WebServer
11
```

The status bar at the bottom displays "Normal text file", "length: 212 lines: 11", "Ln: 10 Col: 17 Sel: 0 | 0", "Windows (CR LF)", "UTF-8", and "INS". The taskbar at the bottom shows icons for Start, Task View, File Explorer, Internet Explorer, and Notepad++, along with the system tray showing the date and time.

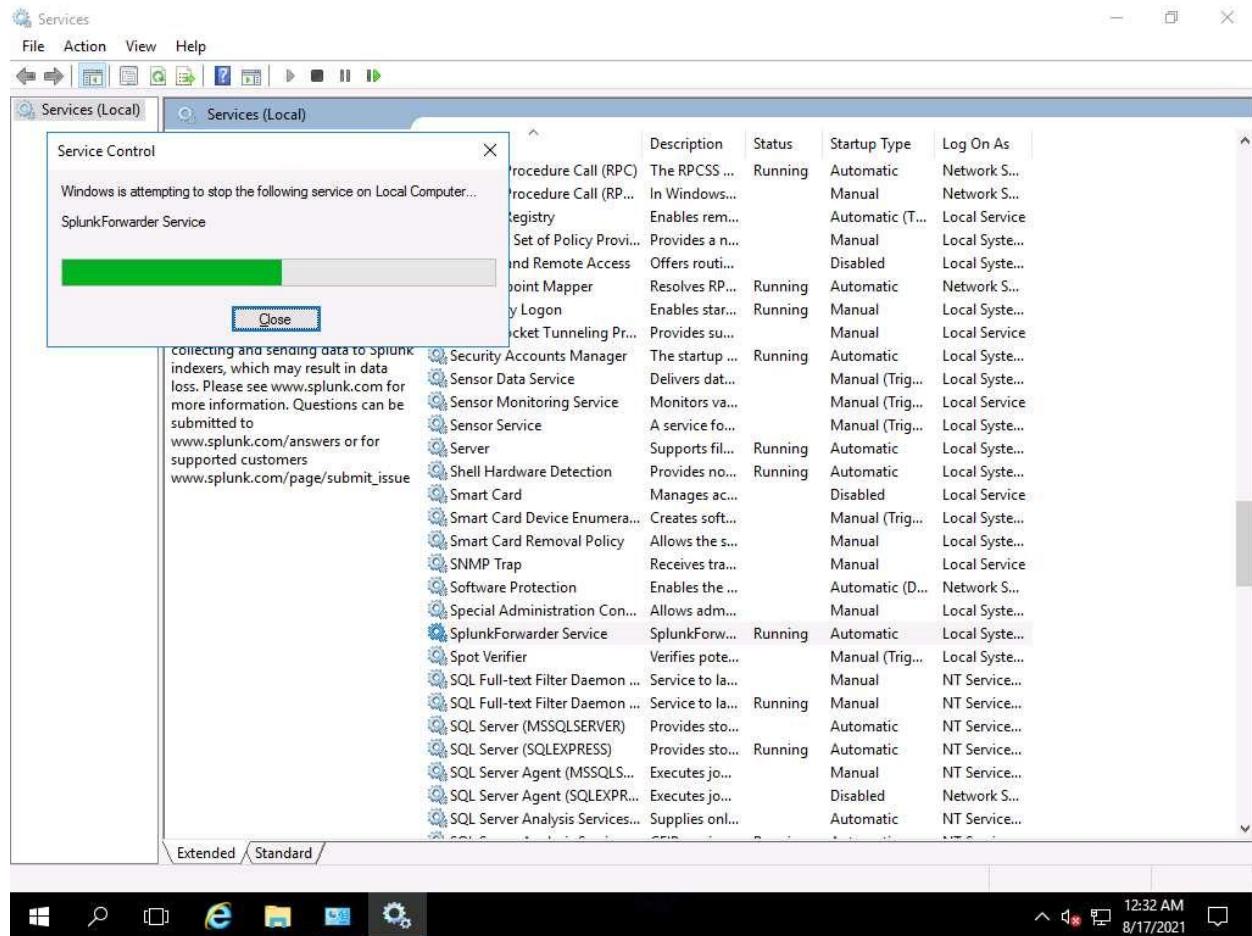
75. Close all open files in Notepad.

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.

```
Administrator: C:\Windows\system32\cmd.exe
--runmode <runmode_id>
: specific runmode modification the engine should run. The argument
supplied should be the id for the runmode obtained by running
--list-runmodes
: print reports on analysis of different sections in the engine and exit.
Please have a look at the conf parameter engine-analysis on what reports
can be printed
--pidfile <file>
: write pid to this file
--init-errors-fatal
: enable fatal failure on signature init error
--disable-detection
: disable detection engine
--dump-config
: show the running configuration
--build-info
: display build information
--pcap[=<dev>]
: run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-continuous
: when running in pcap mode with a directory, continue checking directory for pc
aps until interrupted
: when running in replay mode (-r with directory or file), will delete pcap file
--pcap-file-delete
s that have been processed when done
: size of the pcap buffer value from 0 - 2147483647
--pcap-buffer-size
--simulate-ips
: force engine into IPS mode. Useful for QA
--erf-in <path>
: process an ERF file
--windivert <filter>
: run in inline WinDivert mode
--windivert-forward <filter>
: run in inline WinDivert mode, as a gateway
--set name=value
: set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata.exe -c suricata.yaml -s signatures.rules -i eth0

C:\Program Files\Suricata>
```

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

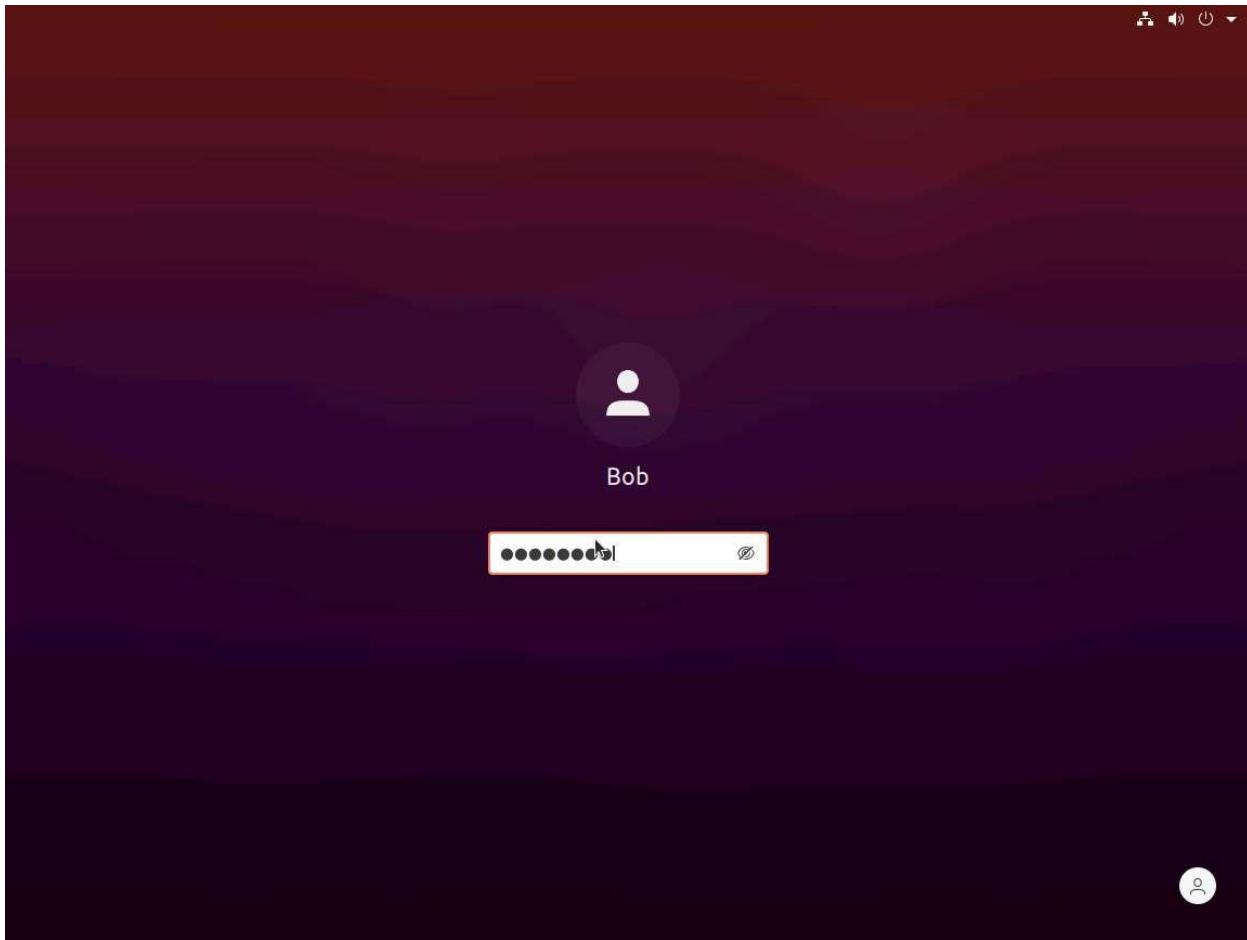
The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe - suricata.exe -c suricata.yaml -i 10.10.1.16". The window displays the Suricata command-line interface help text, which includes various runmode options like --runmode, --engine-analysis, and --pcap. Below the help text, a command is run: "suricata.exe -c suricata.yaml -s signatures.rules -i eth0". The output shows the engine starting up, translating the interface to a pcap device, and initializing threads. The taskbar at the bottom shows icons for File Explorer, Task View, and Start.

```
Administrator: C:\Windows\system32\cmd.exe - suricata.exe -c suricata.yaml -i 10.10.1.16
--runmode <runmode_id>
: specific runmode modification the engine should run. The argument supplied should be the id for the runmode obtained by running
--list-runmodes
: print reports on analysis of different sections in the engine and exit.
Please have a look at the conf parameter engine-analysis on what reports can be printed
--pidfile <file>
: write pid to this file
--init-errors-fatal
: enable fatal failure on signature init error
--disable-detection
: disable detection engine
--dump-config
: show the running configuration
--build-info
: display build information
--pcap[=<dev>]
: run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-continuous
: when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
--pcap-file-delete
: when running in replay mode (-r with directory or file), will delete pcap file
-s that have been processed when done
--pcap-buffer-size
: size of the pcap buffer value from 0 - 2147483647
--simulate-ips
--erf-in <path>
--windivert <filter>
--windivert-forward <filter>
--set name=value
: set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata.exe -c suricata.yaml -s signatures.rules -i eth0

C:\Program Files\Suricata>suricata.exe -c suricata.yaml -i 10.10.1.16
17/8/2021 -- 00:35:07 - <Info> - Running as service: no
17/8/2021 -- 00:35:07 - <Info> - translated 10.10.1.16 to pcap device \Device\NPF_{4145D27B-2359-4013-9F71-D0D908E70D6A}
17/8/2021 -- 00:35:07 - <Notice> - This is Suricata version 4.1.4 RELEASE
17/8/2021 -- 00:35:08 - <Warning> - [ERRCODE: SC_ERR_NIC_OFFLOADING(284)] - NIC offloading on \Device\NPF_{4145D27B-2359-4013-9F71-D0D908E70D6A}: Checksum IPv4 Rx: 0 Tx: 0 IPv6 Rx: 1 Tx: 1 LSOv1 IPv4: 0 LSOv2 IPv4: 0 IPv6: 0
17/8/2021 -- 00:35:08 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
```

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 suricata.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.

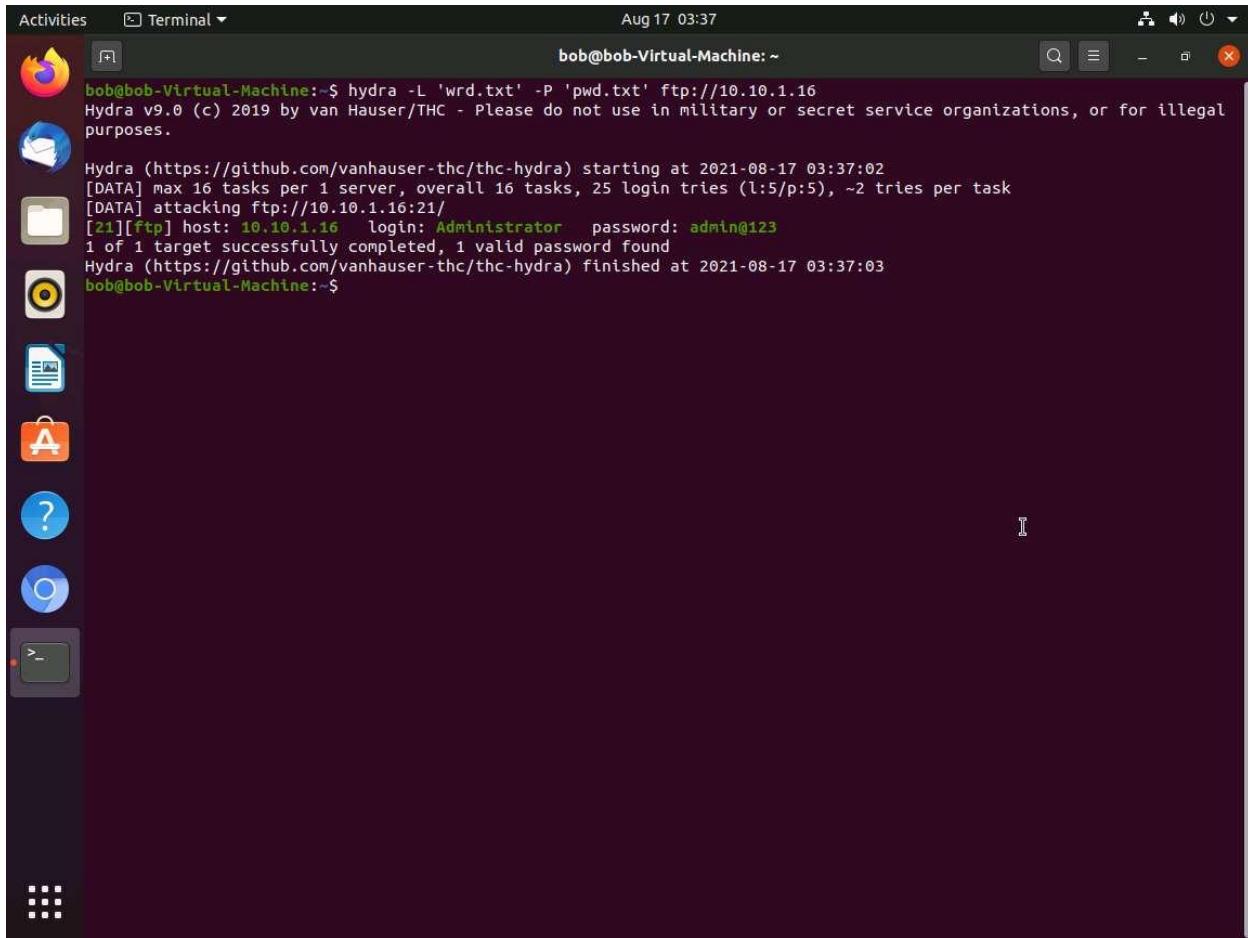
87. Press Ctrl + Alt + T to open the terminal, type `hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16`, and press Enter.

A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window. The terminal window has a dark background and contains the following text:

```
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
```

The terminal window is titled "Terminal". The desktop interface includes a vertical dock on the left with icons for various applications like a browser, file manager, and terminal, and a dock at the bottom with several application icons.

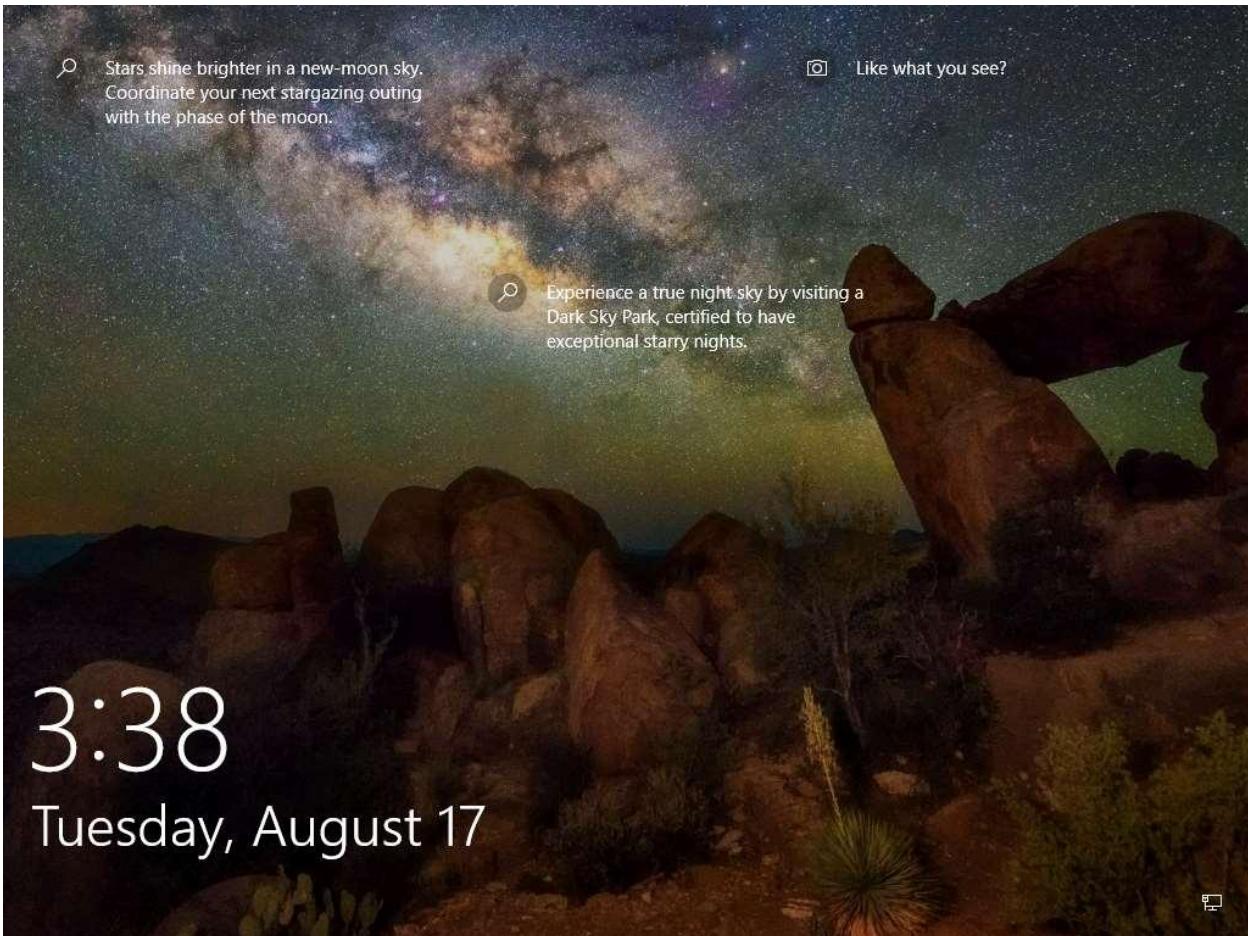
88. The Attacker Machine-1 will try to match the combination of usernames and passwords with the Web Server.
  89. The matched username and password are shown in the terminal in green color. Close the terminal window.



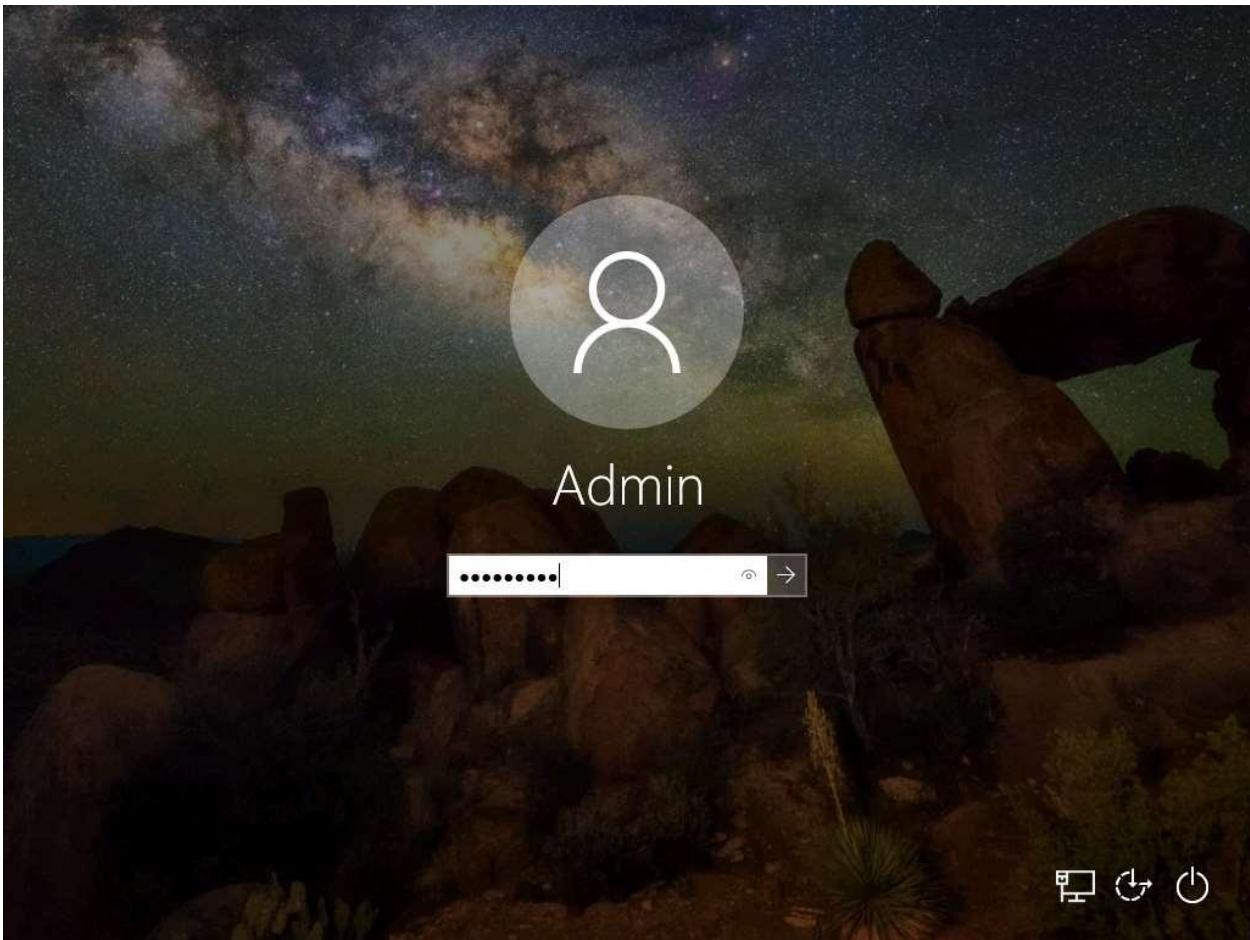
The image shows a screenshot of a Linux desktop environment, specifically Ubuntu, with a terminal window open. The terminal window title is "Terminal" and the date and time are "Aug 17 03:37". The terminal content is as follows:

```
Activities Terminal ▾ Aug 17 03:37
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-17 03:37:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][Ftp] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-17 03:37:03
bob@bob-Virtual-Machine:~$
```

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.

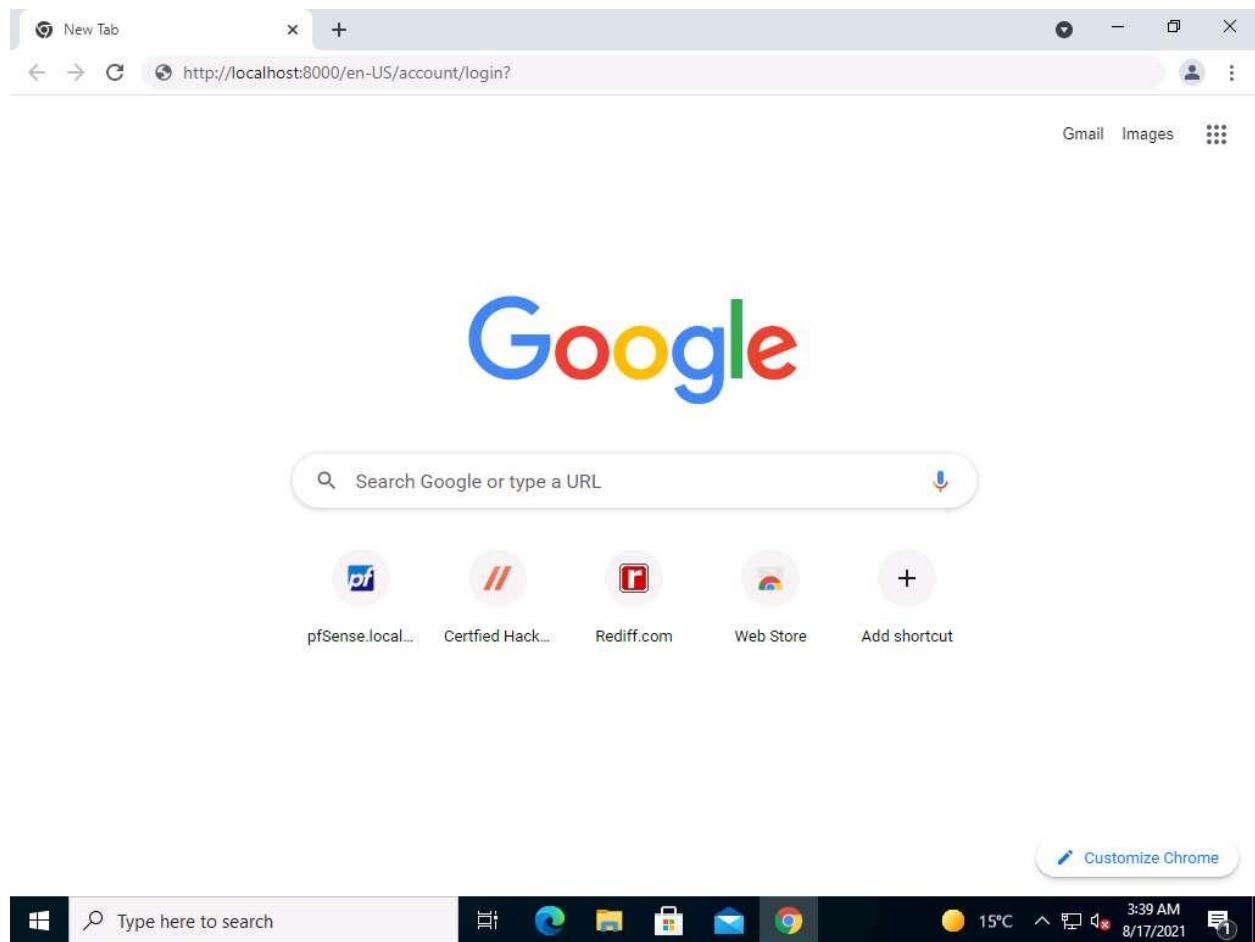


91. By default, the username Admin is selected. Type password admin@123 and press Enter.

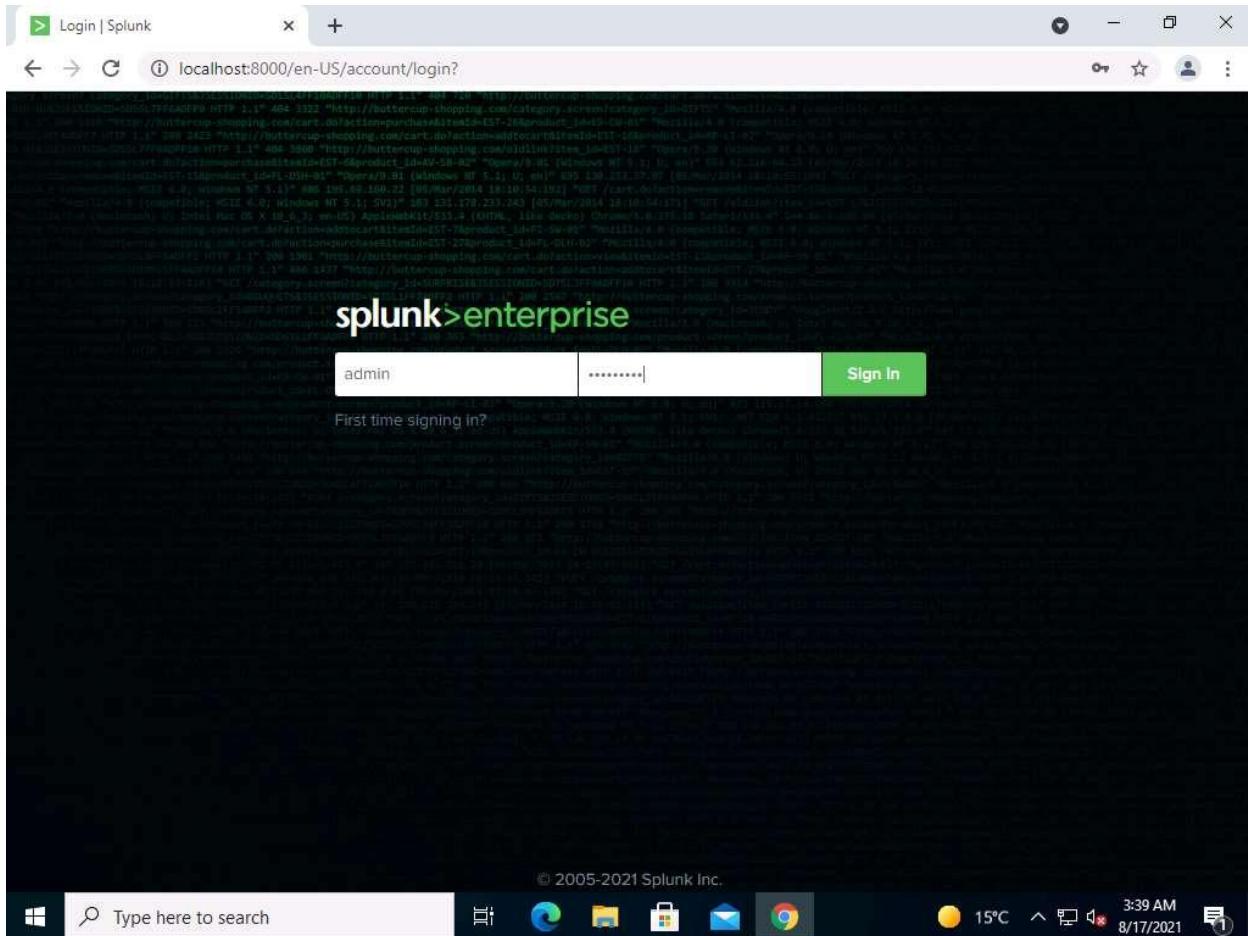


If the network screen appears, click Yes.

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



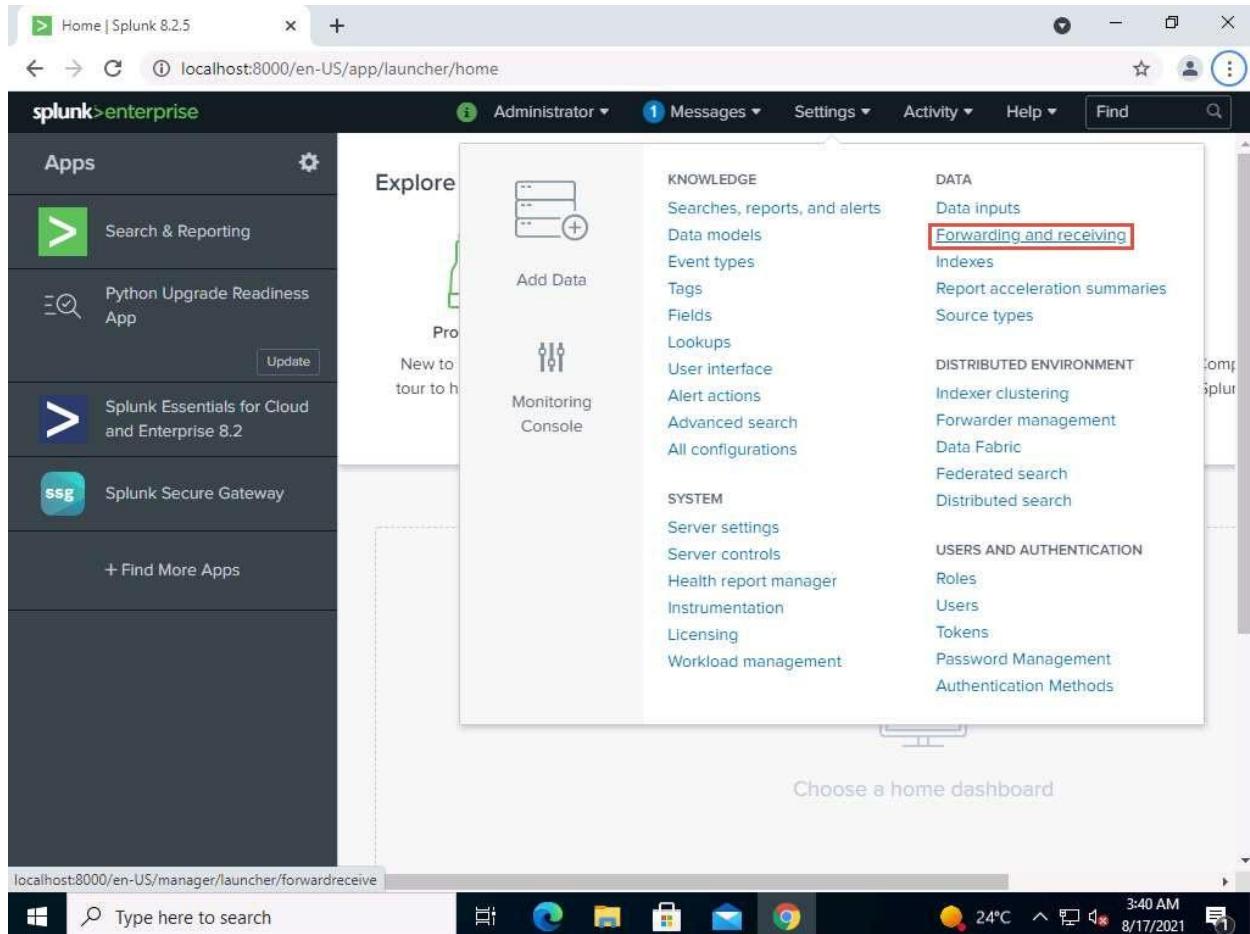
93. Log in with the username admin and password admin@123



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.

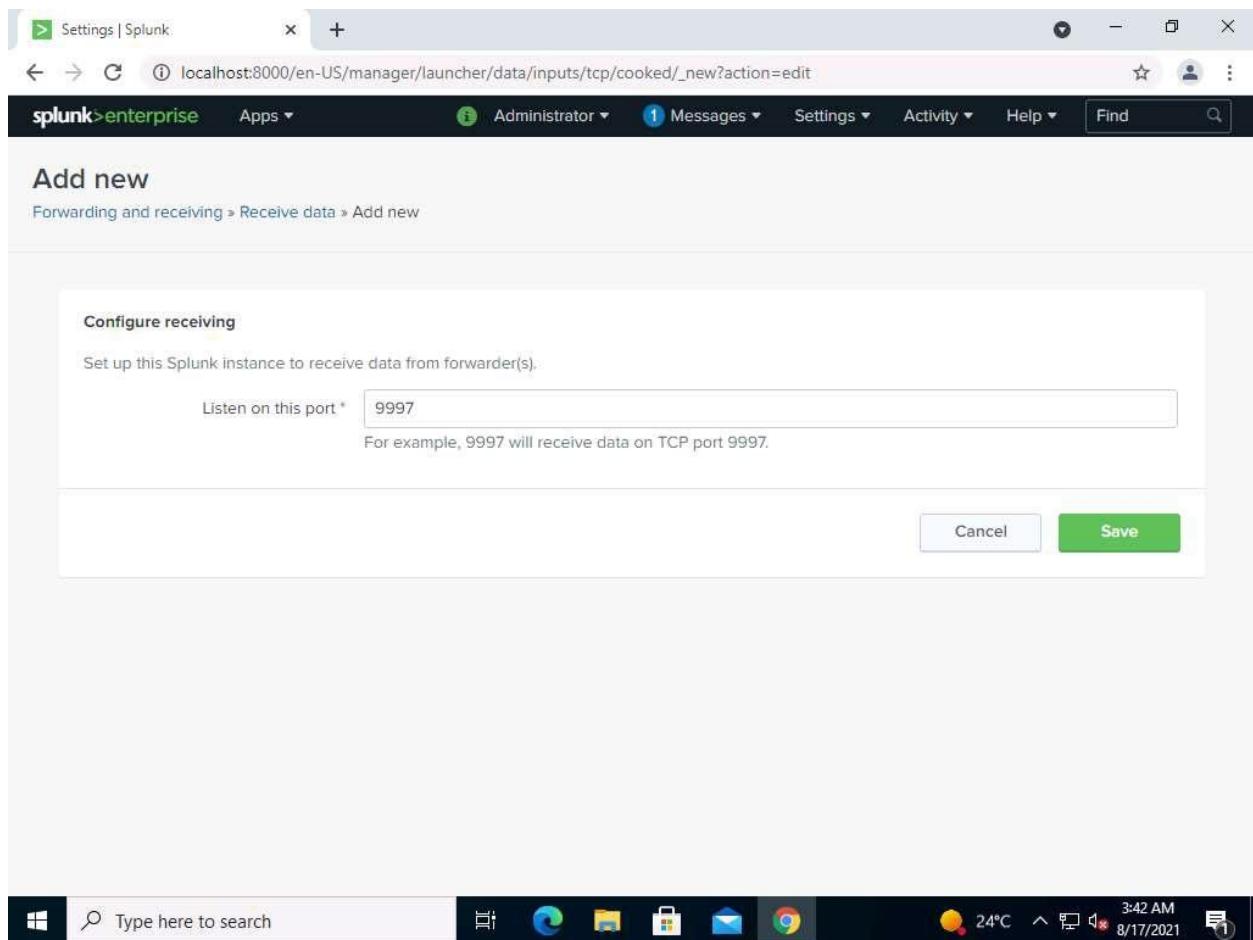
94. The Splunk web console appears; click Settings menu, select Forwarding and receiving link under the DATA section.



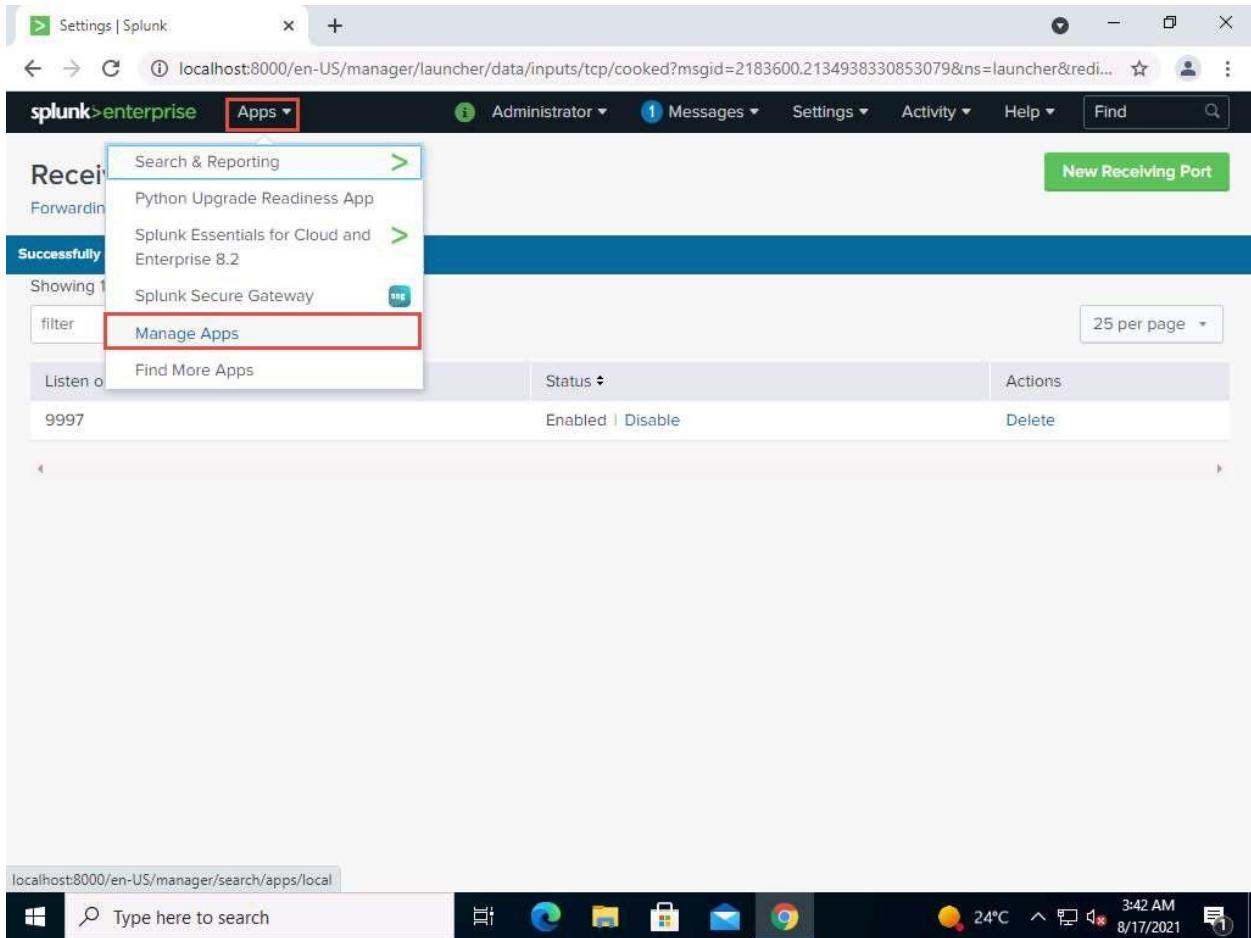
95. The Forwarding and receiving console will appear. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click on the +Add new link in the bottom right corner to Configure receiving.

The screenshot shows the Splunk Enterprise Settings interface. The title bar reads "Settings | Splunk" and the URL is "localhost:8000/en-US/manager/launcher/forwardreceive". The top navigation bar includes "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". The main content area is titled "Forwarding and receiving". It has two sections: "Forward data" and "Receive data". The "Forward data" section contains "Forwarding defaults" and "Configure forwarding" with a "+ Add new" button. The "Receive data" section contains "Configure receiving" with a "+ Add new" button. Below the browser window is the Windows taskbar, which includes the Start button, a search bar, pinned icons for File Explorer, Edge, Microsoft Store, Mail, and Google Chrome, and system status icons for battery level, temperature (24°C), time (3:41 AM, 8/17/2021), and a notification icon.

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.

The screenshot shows the Splunk Enterprise Settings interface with the 'Apps' page selected. The table lists various applications with columns for Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The 'SplunkForwarder' row is highlighted, and the 'Edit' button in the Actions column is highlighted with a red box.

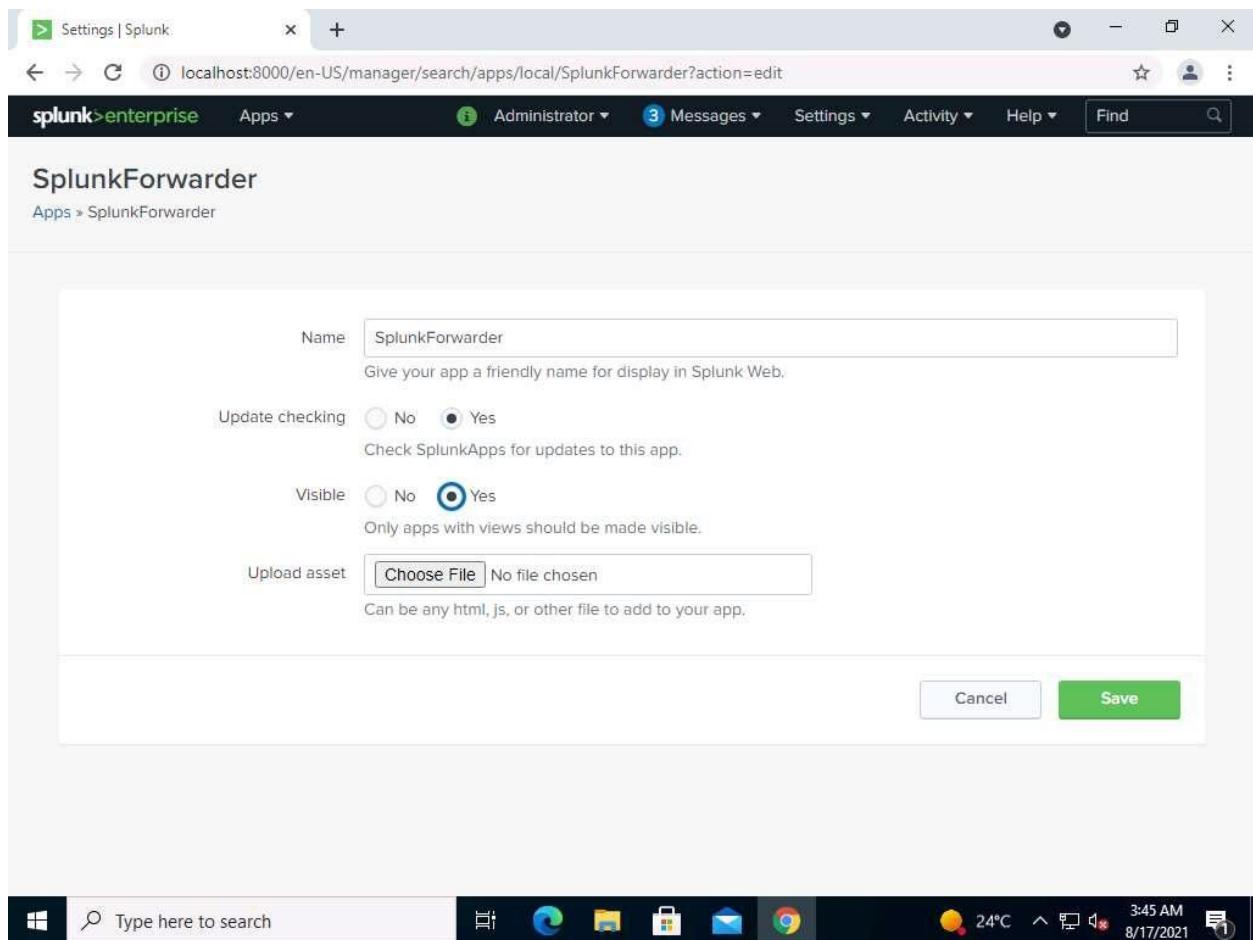
Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App   Permissions	Disabled	<a href="#">Edit</a>
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
Log Event Alert Action	alert_logevent	8.2.5	Yes	No	App   Permissions	Enabled   Disable	
Webhook Alert Action	alert_webhook	8.2.5	Yes	No	App   Permissions	Enabled   Disable	
Apps Browser	appsbrowser	8.2.5	Yes	No	App   Permissions	Enabled	
introspection_generator_addon	introspection_generator_addon	8.2.5	Yes	No	App   Permissions	Enabled   Disable	
Home	launcher		Yes	Yes	App   Permissions	Enabled	
learned	learned		Yes	No	App   Permissions	Enabled   Disable	
legacy	legacy		Yes	No	App   Permissions	Disabled   Enable	
Python Upgrade Readiness App	python_upgrade_readiness_app	1.0.0   Update to 4.0.2	Yes	Yes	App   Permissions	Enabled   Disable	
sample data	sample_app		Yes	No	App   Permissions	Disabled   Enable	
Search & Reporting	search	8.2.5	Yes	Yes	App   Permissions	Enabled	

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

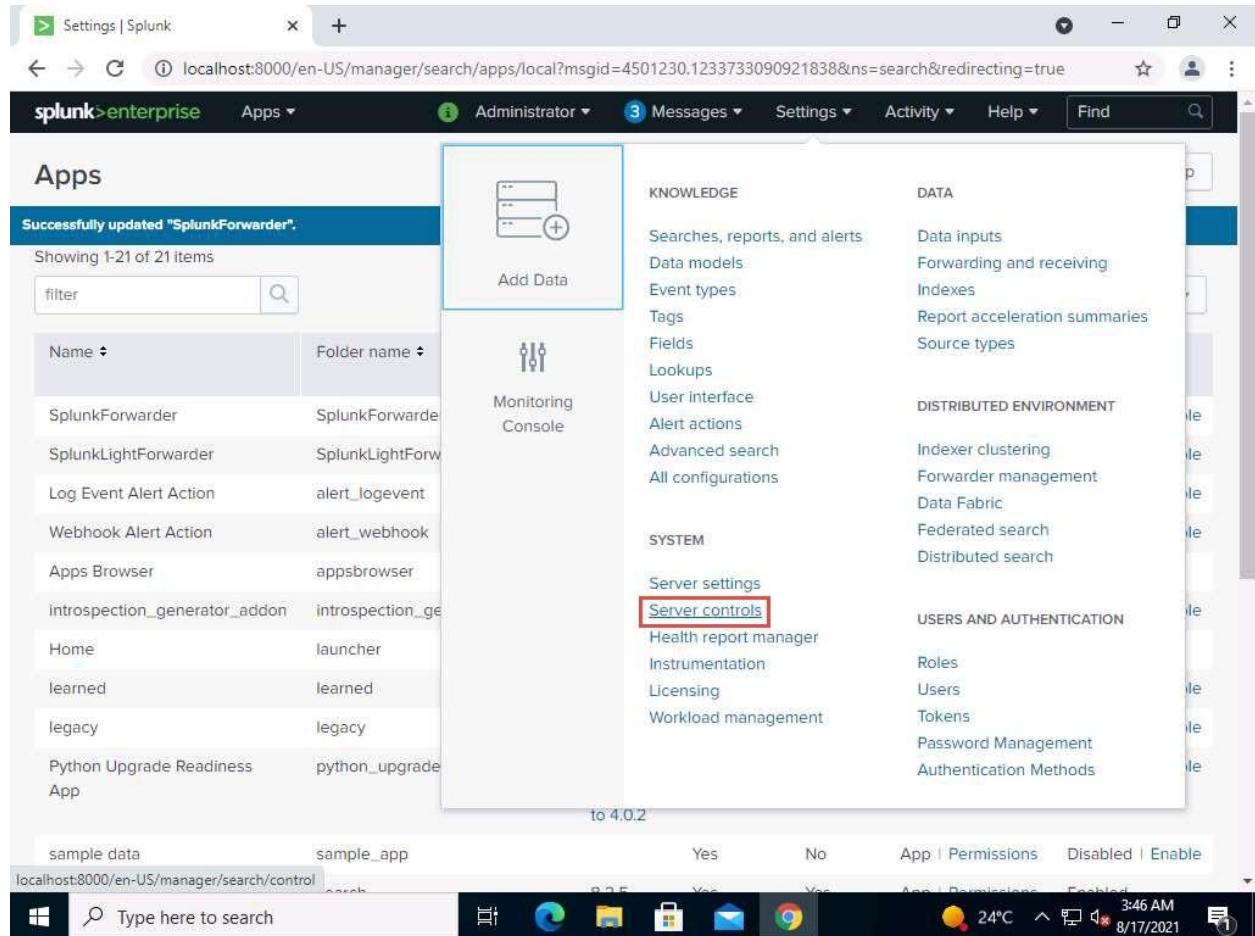
The screenshot shows the Splunk Enterprise Settings interface with the 'Apps' page selected. The title bar indicates the URL is `localhost:8000/en-US/manager/search/apps/local?app_only=False&msgid=4022340.9465813222414073`. The top navigation bar includes links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and search functions. Below the navigation is a toolbar with 'Browse more apps', 'Install app from file', and 'Create app' buttons. The main content area displays a table titled 'Enabled SplunkForwarder.' showing 21 items. The columns include 'Folder name', 'Version', 'Update checking', 'Visible', 'Sharing', 'Status', and 'Actions'. The first item, 'SplunkForwarder', has its 'Edit properties' link highlighted with a red box. The table also lists other apps like 'SplunkLightForwarder', 'alert\_logevent', 'alert\_webhook', 'appsbrowser', etc. At the bottom of the table, there is a note: 'python\_upgrade\_readiness\_app 1.0.0 | Update to 4.0.2'. The bottom of the screen shows a Windows taskbar with icons for File Explorer, Mail, and Google Chrome, along with system status information like battery level, temperature (24°C), and date/time (8/17/2021).

Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder		Yes	No	App   Permissions	Enabled   Disable	<a href="#">Edit properties</a>   View objects
SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
alert_logevent	8.2.5	Yes	No	App   Permissions	Enabled   Disable	<a href="#">Edit properties</a>   View objects
alert_webhook	8.2.5	Yes	No	App   Permissions	Enabled   Disable	<a href="#">Edit properties</a>   View objects
appsbrowser	8.2.5	Yes	No	App   Permissions	Enabled	<a href="#">Edit properties</a>   View objects
introspection_generator_addon	8.2.5	Yes	No	App   Permissions	Enabled   Disable	<a href="#">Edit properties</a>   View objects
launcher		Yes	Yes	App   Permissions	Enabled	<a href="#">Launch app</a>   <a href="#">Edit properties</a>   View objects
learned		Yes	No	App   Permissions	Enabled   Disable	<a href="#">Edit properties</a>   View objects
legacy		Yes	No	App   Permissions	Disabled   Enable	
python_upgrade_readiness_app	1.0.0   Update to 4.0.2	Yes	Yes	App   Permissions	Enabled   Disable	<a href="#">Launch app</a>   <a href="#">Edit properties</a>   View objects
sample_app		Yes	No	App   Permissions	Disabled   Enable	

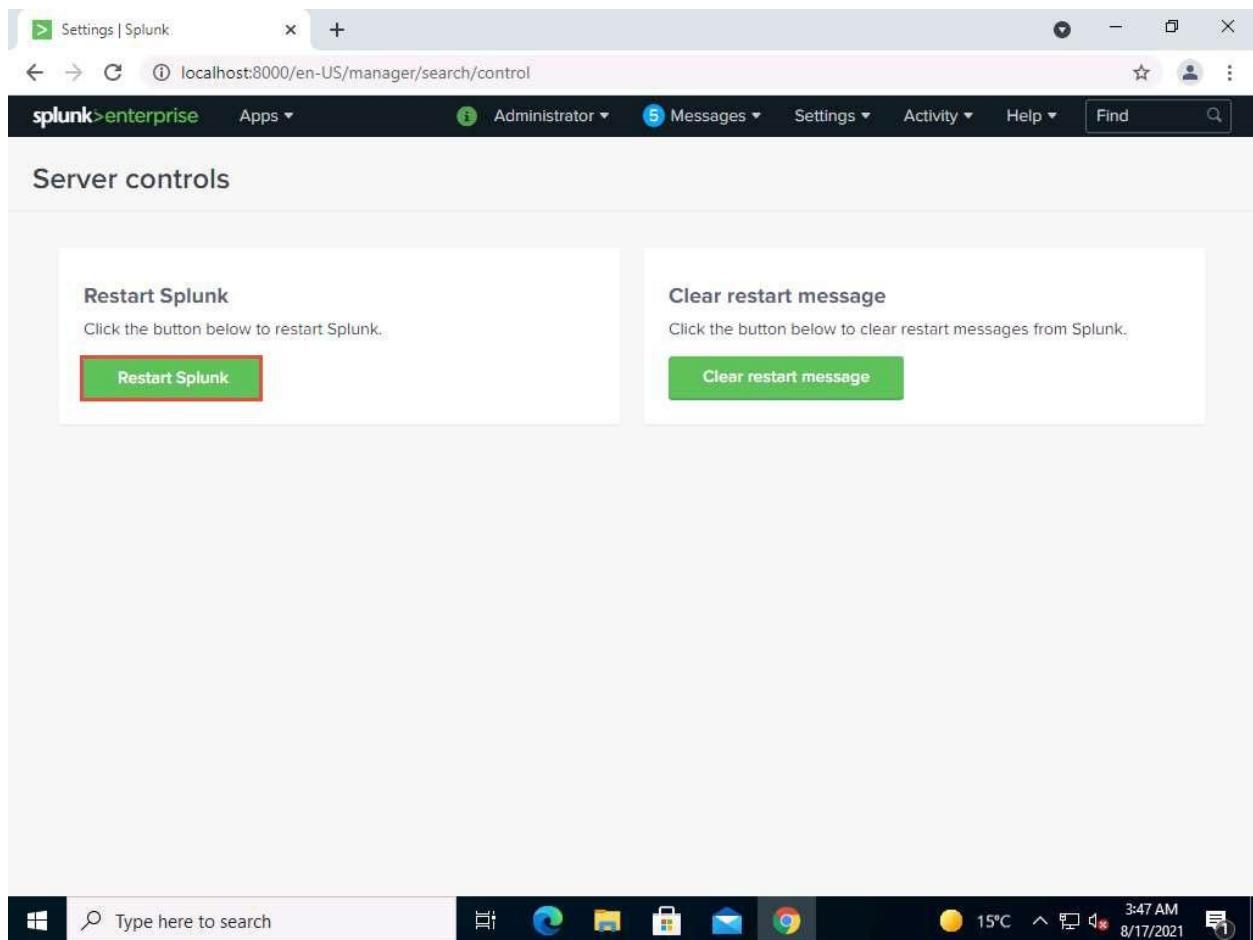
100. The SplunkForwarder console appears; click on Yes under the Visible section, and then on Save.



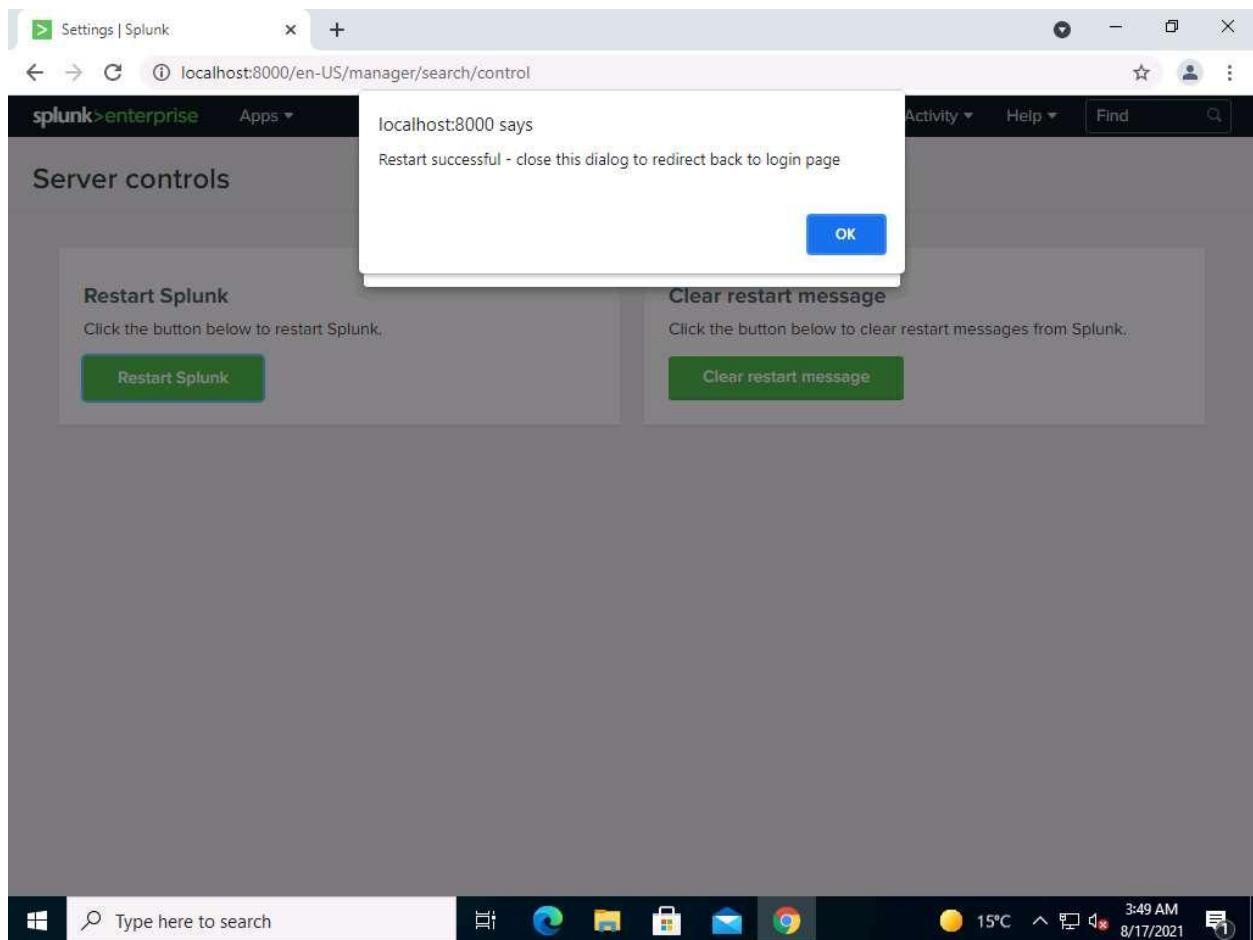
101. Go to Settings and select Server controls under the SYSTEM section.



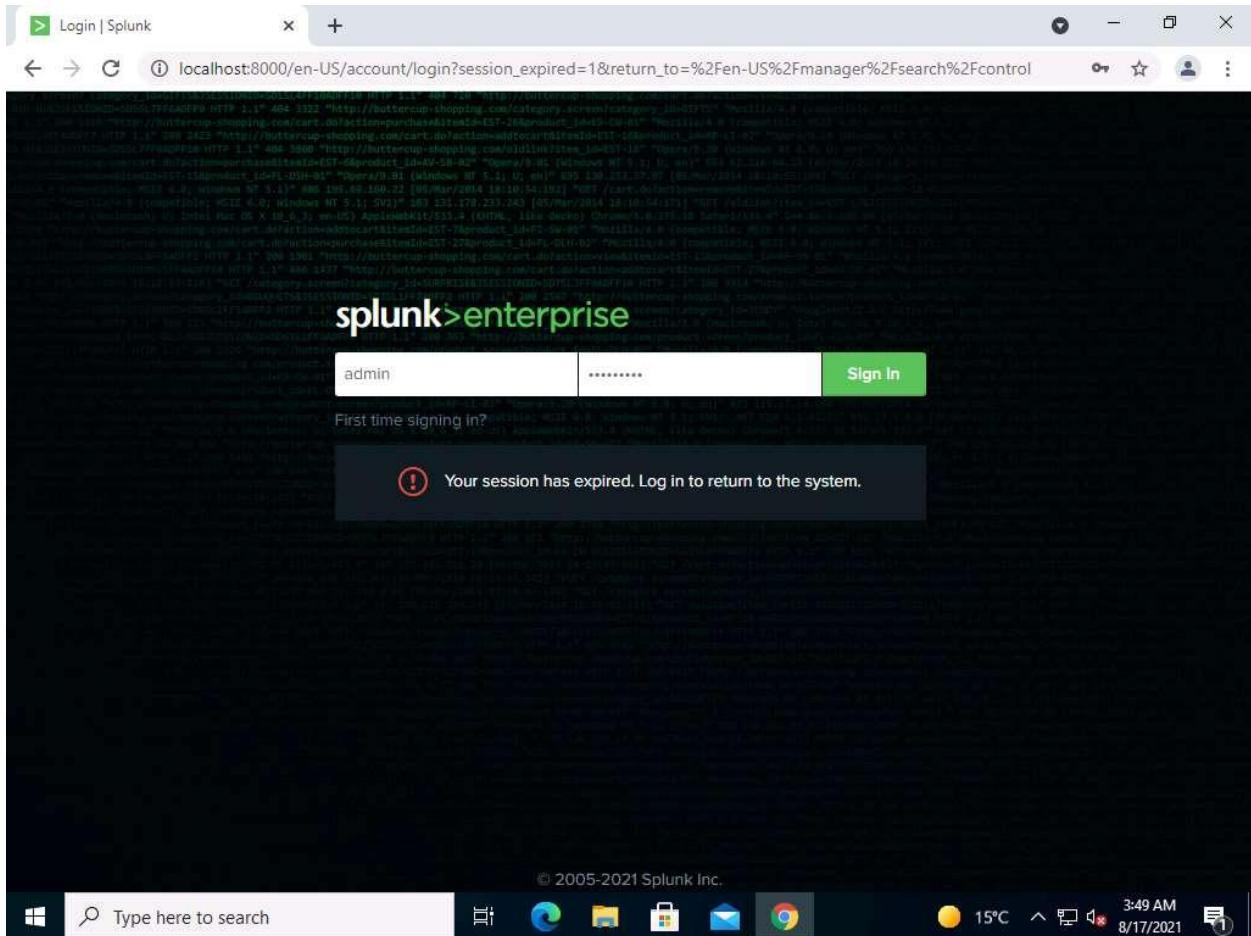
102. The Server controls console appears; click on Restart Splunk. A confirmation pop-up appears; click on OK.



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.

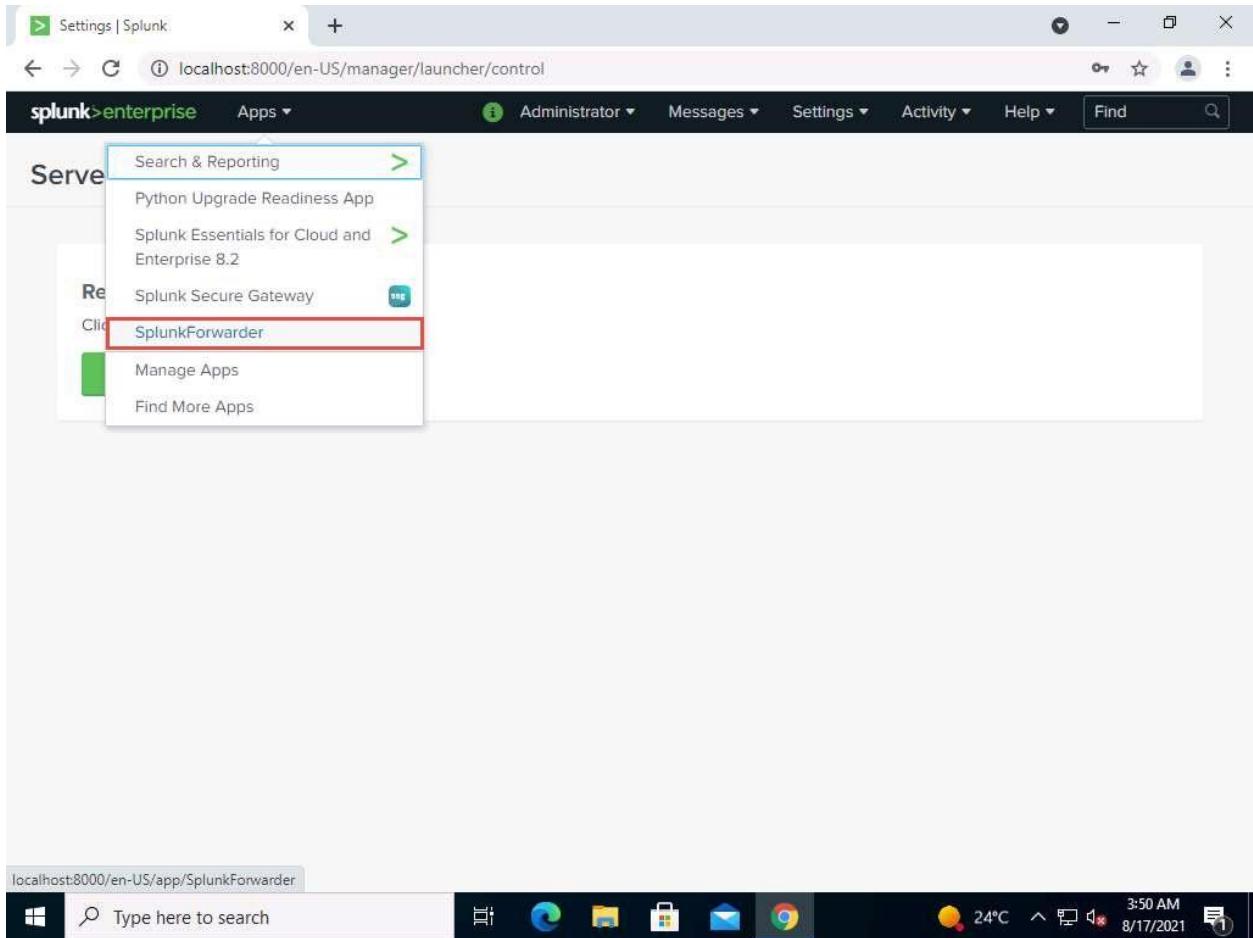


104. You will be redirected to the login page. Enter the user credentials (username admin and password admin@123) and click on Sign In.



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.

The screenshot shows the Splunk 8.2.5 web interface. At the top, the URL is localhost:8000/en-US/app/SplunkForwarder/search. The header includes the 'splunk>enterprise' logo, user 'Administrator', and various navigation links like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A search bar at the top has 'enter search here...' and a 'Last 24 hours' dropdown. Below the search bar, there's a 'No Event Sampling' dropdown and a 'Smart Mode' link. A 'Search History' section is present. On the left, a 'How to Search' panel contains links for 'Documentation', 'Tutorial', and 'Data Summary' (which is highlighted with a red border). On the right, a 'Table Views' section is shown with a 'Create Table View' button. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Edge, File Explorer, Mail, Google Chrome, Task View, and a battery icon. The date and time are 8/17/2021, 3:50 AM.

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.

The screenshot shows the Splunk 8.2.5 interface. The title bar says "Search | Splunk 8.2.5" and the URL is "localhost:8000/en-US/app/SplunkForwarder/search". The main menu includes "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". A sidebar on the left has sections for "Default Views", "Search" (with a search bar), "How to Search", and "Documents". The main content area is titled "Data Summary" and shows three tabs: "Hosts (2)", "Sources (11)" (which is selected), and "Sourcetypes (11)". Below the tabs is a search bar with a "filter" field and a magnifying glass icon. The main table lists sources with columns: "Source", "Count", and "Last Update". One row, "C:\Program Files\Suricata\log\fast.log", is highlighted with a red box. The table data is as follows:

Source	Count	Last Update
C:\Program Files\Suricata\log\eve.json	508	8/17/21 3:48:05.000 AM
<b>C:\Program Files\Suricata\log\fast.log</b>	<b>9</b>	8/17/21 3:46:12.000 AM
C:\Program Files\Suricata\log\stats.log	478	8/17/21 3:48:05.000 AM
C:\Program Files\Suricata\log\suricata.log	3	8/17/21 3:46:08.000 AM
C:\inetpub\logs\LogFiles\FTPSVC3\u_ex220927.log	164	8/17/21 3:46:14.000 AM
Perfmon:Available Memory	176	8/17/21 3:46:04.000 AM
Perfmon:CPU Load	255	8/17/21 3:46:04.000 AM
Perfmon:Network Interface	361	8/17/21 3:46:04.000 AM
WinEventLog:Application	3,114	8/17/21 3:48:05.000 AM
WinEventLog:Security	21,521	8/17/21 3:48:05.000 AM

The taskbar at the bottom shows the Windows Start button, a search bar with "Type here to search", and icons for File Explorer, Mail, and Google Chrome. The system tray shows the date and time as "3:51 AM 8/17/2021".

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.

The screenshot shows the Splunk 8.2.5 interface. At the top, there's a navigation bar with links for 'Search | Splunk 8.2.5', 'localhost:8000/en-US/app/SplunkForwarder/search?q=search%20source%3DC%3A%5C%5CProgram%20Files%5C%5CSur...', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a header bar with 'splunk>enterprise' and 'App: SplunkForwarder'. A 'Default Views' dropdown is open. On the right of the header is a user icon and a 'SplunkForwarder' button.

The main area is titled 'New Search' with a search bar containing 'source="C:\Program Files\Suricata\log\fast.log"'. To the right of the search bar are buttons for 'Last 24 hours' and a magnifying glass icon. Below the search bar, it says '✓ 9 events (8/16/21 3:00:00.000 AM to 8/17/21 3:52:21.000 AM)' and 'No Event Sampling'. There are also buttons for 'Job', 'Smart Mode', and a 'Save As' dropdown.

The search results are displayed in a table with columns: 'Events (9)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is selected. Below the table are buttons for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A note indicates '1 hour per column'.

The event table has a header row with 'List', 'Format', and '20 Per Page' buttons. The data rows show two events:

	i	Time	Event
< Hide Fields	i	8/17/21 3:37:03.488 AM	08/17/2021-00:37:03.488827 [**] [1:0:0] ET SCAN Potential FTP Brute-Force at tempt [**] [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
SELECTED FIELDS	i	8/17/21 3:37:03.472 AM	08/17/2021-00:37:03.472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force at tempt [**] [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
INTERESTING FIELDS	i	8/17/21 3:37:03.472 AM	08/17/2021-00:37:03.472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force at tempt [**] [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

At the bottom of the interface is a search bar with placeholder text 'Type here to search' and a toolbar with icons for file operations, a magnifying glass, and system status (15°C, 3:53 AM, 8/17/2021).

110. Click on Statistics tab and Quick Reports.

Search | Splunk 8.2.5

localhost:8000/en-US/app/SplunkForwarder/search?q=search%20source%3D"C%3A%5C%5CProgram%20Files%5C%5CSuricata%5C%5Clog%5C%5Cfast.log"

splunk>enterprise App: SplunkForwarder Administrator Messages Settings Activity Help Find Default Views SplunkForwarder

## New Search

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

Events (9) Patterns Statistics Visualization

Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.

**Pivot**

Build tables and visualizations using multiple fields and metrics without writing searches.

**Quick Reports**

Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.

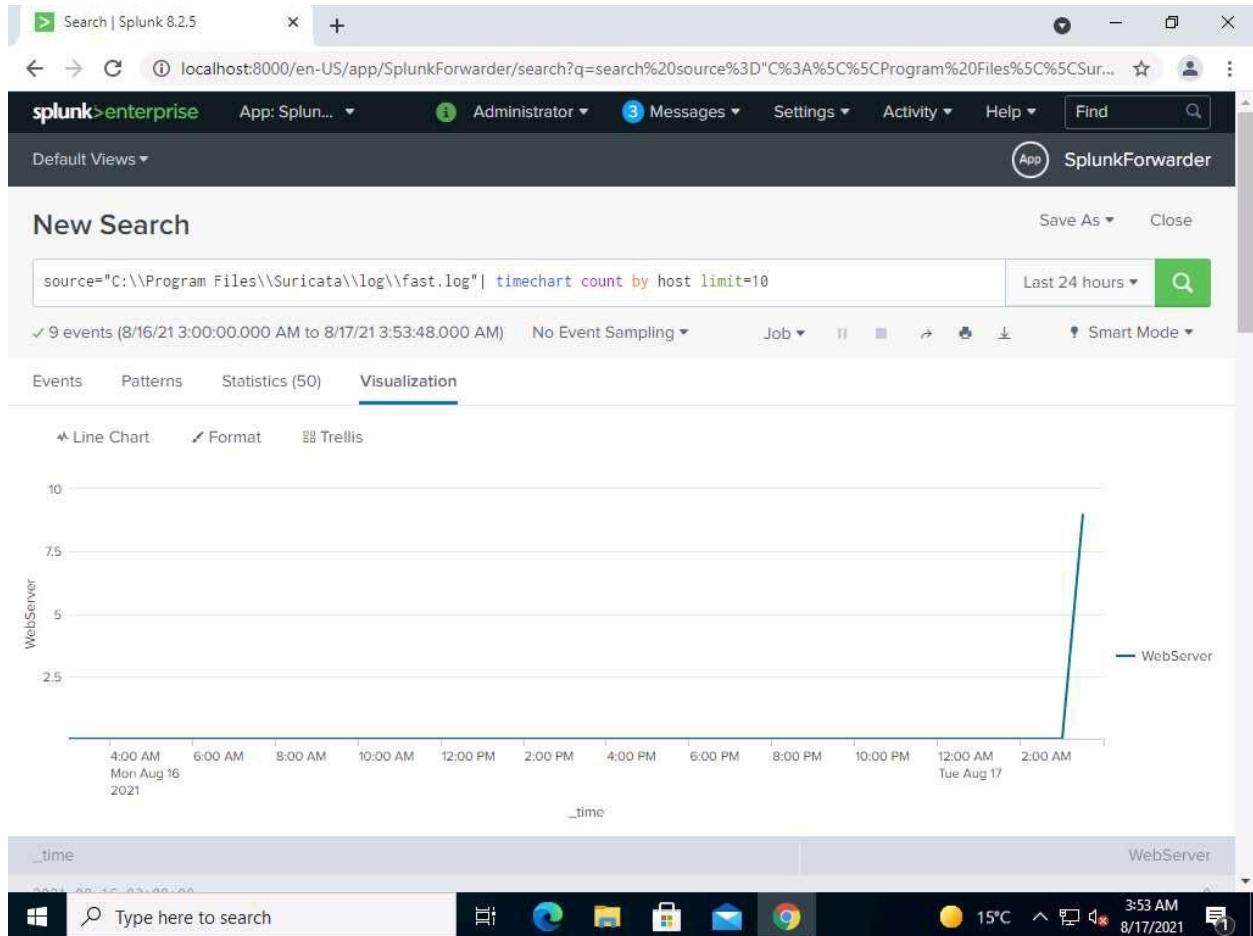
**Search Commands**

Use a transforming search command, like timechart or stats, to summarize the data.

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.

The screenshot shows the Splunk 8.2.5 interface. At the top, the URL is `localhost:8000/en-US/app/SplunkForwarder/search?q=search%20source%3DC%3A%5C%5CProgram%20Files%5C%5CSur...`. The search bar contains the query `source="C:\Program Files\Suricata\log\fast.log"`. Below the search bar, it says "9 events (8/16/21 3:00:00.000 AM to 8/17/21 3:52:21.000 AM)" and "No Event Sampling". The "Events (9)" tab is selected. A context menu is open over the "host" field, which has a value of "WebServer". The menu options are "Selected", "Yes", and "No". To the right of the menu, there are two items: "Brute-Force at [Priority: 1]" and "Brute-Force at [Priority: 1]". The bottom status bar shows the URL `localhost:8000/en-US/app/SplunkForwarder/search?q=search source%3DC%3A%5C%5CProgram Files%5C%5CSuricata%5C%5Clog%5C%5Cfast.log&sid=1629186741.47&display.pag...`, the date `8/17/2021`, the time `3:53 AM`, the temperature `15°C`, and a battery icon.

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.

The screenshot shows the Splunk 8.2.5 interface with the URL `localhost:8000/en-US/app/SplunkForwarder/search?q=search%20source%3D%C3%A5%C5CProgram%20Files%5C%5CSur...`. A modal window titled "Select Fields" is open, listing various log fields. The table has columns for Field, # of Values, Event Coverage, and Type. Fields listed include host, source, sourcetype, splunk\_server, date\_hour, date\_mday, date\_minute, date\_month, date\_second, date\_wday, date\_year, date\_zone, index, and linecount. All fields have 100% event coverage and are of type String or Number.

	Field	# of Values	Event Coverage	Type
>	host	1	100%	String
>	source	1	100%	String
>	sourcetype	1	100%	String
>	splunk_server	1	100%	String
>	date_hour	1	100%	Number
>	date_mday	1	100%	Number
>	date_minute	2	100%	Number
>	date_month	1	100%	String
>	date_second	3	100%	Number
>	date_wday	1	100%	String
>	date_year	1	100%	Number
>	date_zone	1	100%	String
>	index	1	100%	String
>	linecount	1	100%	Number

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

The screenshot shows the Splunk 8.2.5 interface. The search bar contains the query "source='C:\Program Files\Suricata\log\fast.log'". The results show two events from 8/17/21 at 3:37:03 AM. Both events are related to potential FTP brute-force attempts. The timeline at the bottom indicates hourly intervals.

Time	Event
8/17/21 3:37:03 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

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%3DC%3A%5C%5CProgram%20Files%5C%5CSur...

splunk>enterprise App: Splunk... Administrator Messages Settings Activity Help Find SplunkForwarder Default Views ▾

New Search

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 X Deselect 1 hour per column

Aug 16, 2021 3:00 AM 9 events at 3 AM on Tuesday, August 17, 2021 3:00 AM

1 day 1 hour

List Format 20 Per Page

< Hide Fields i 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  
a date\_month 1

	i 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