

**INFO39207 Advanced Information Systems
Forensics and Electronic Discovery**

Submitted By:Chris Miele

Submitted To:Prof GM

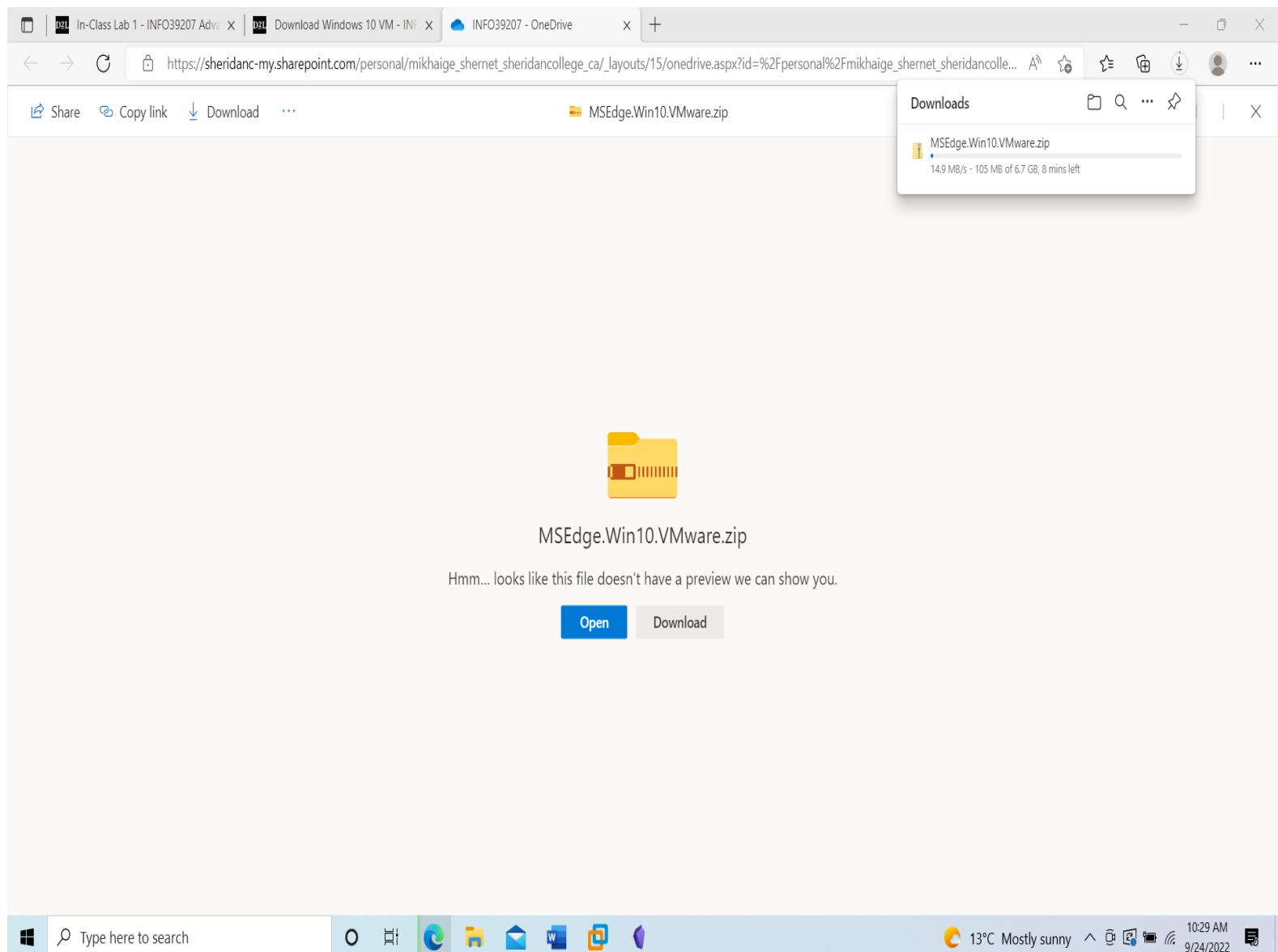
Table of Contents

Lab 1	3
MS-Win10 Download	3
Import MS-Win10	4
MS-Win10 New User	5
MS-Win10 Desktop Background	7
MS-Win10 Disable(AV, Firewall, Updates)	8
MS-Win10 VM NAT/Disk Space	10
Lab 2	11
Splunk Search	11
Boss of SOC Walkthrough	12
Lab 3	34
Event Log	34
Lab 4	45
Reference	46

Lab 1

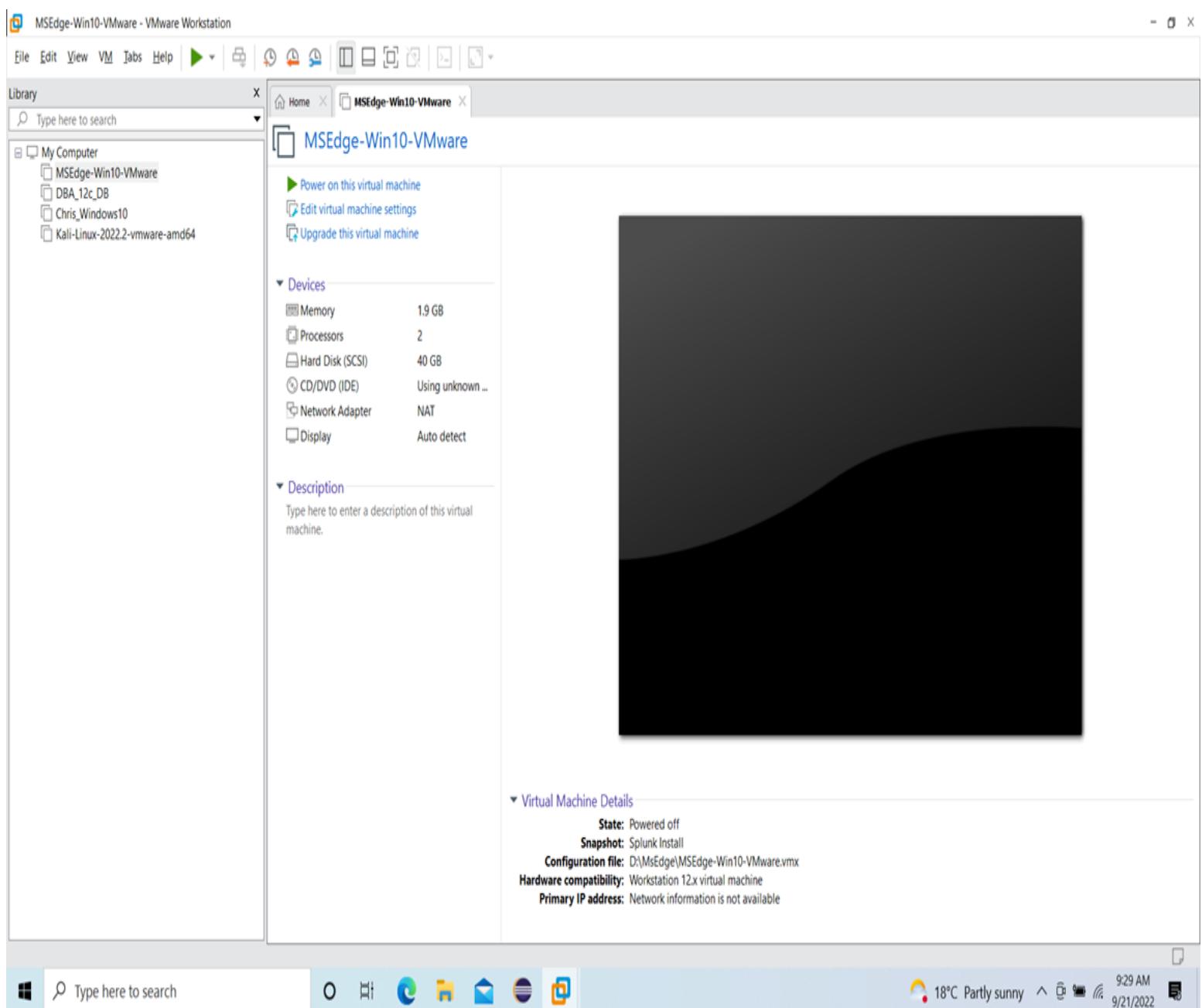
MS-Win10 Download

Figure 1: Downloading MSEdge.Win10



Import MS-Win10

Figure 2: Import Vm File -> Open -> Choose MSEdge-Win10-Vmware.



MS-Win10 New User

Figure 3: Type Settings in search -> Accounts -> Family & Other Accounts -> Click + -> Add My Student # 991609577 Assign Administrator to Account.

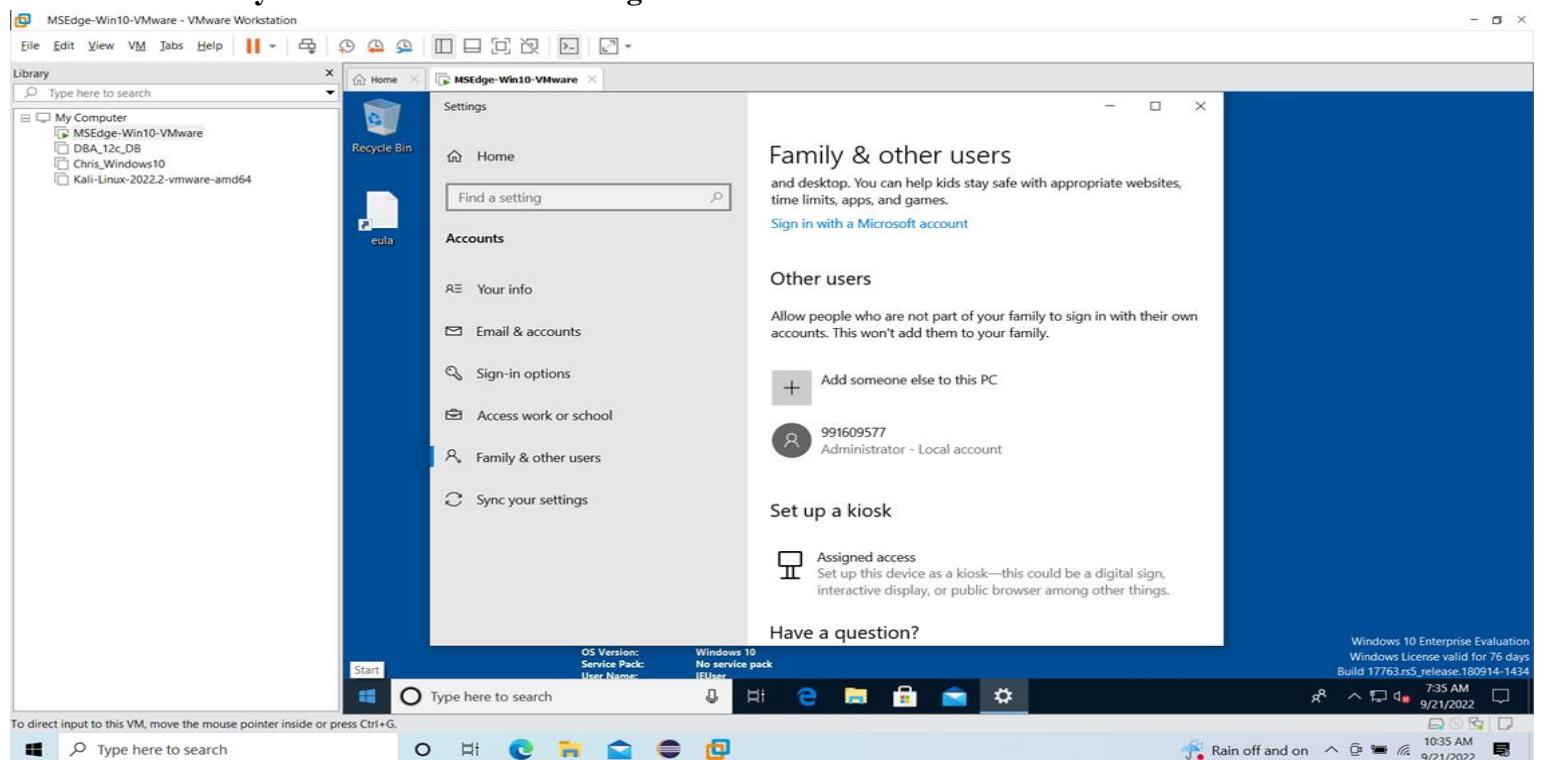


Figure 4: Sign Out -> Sign In using My Student #991609577.

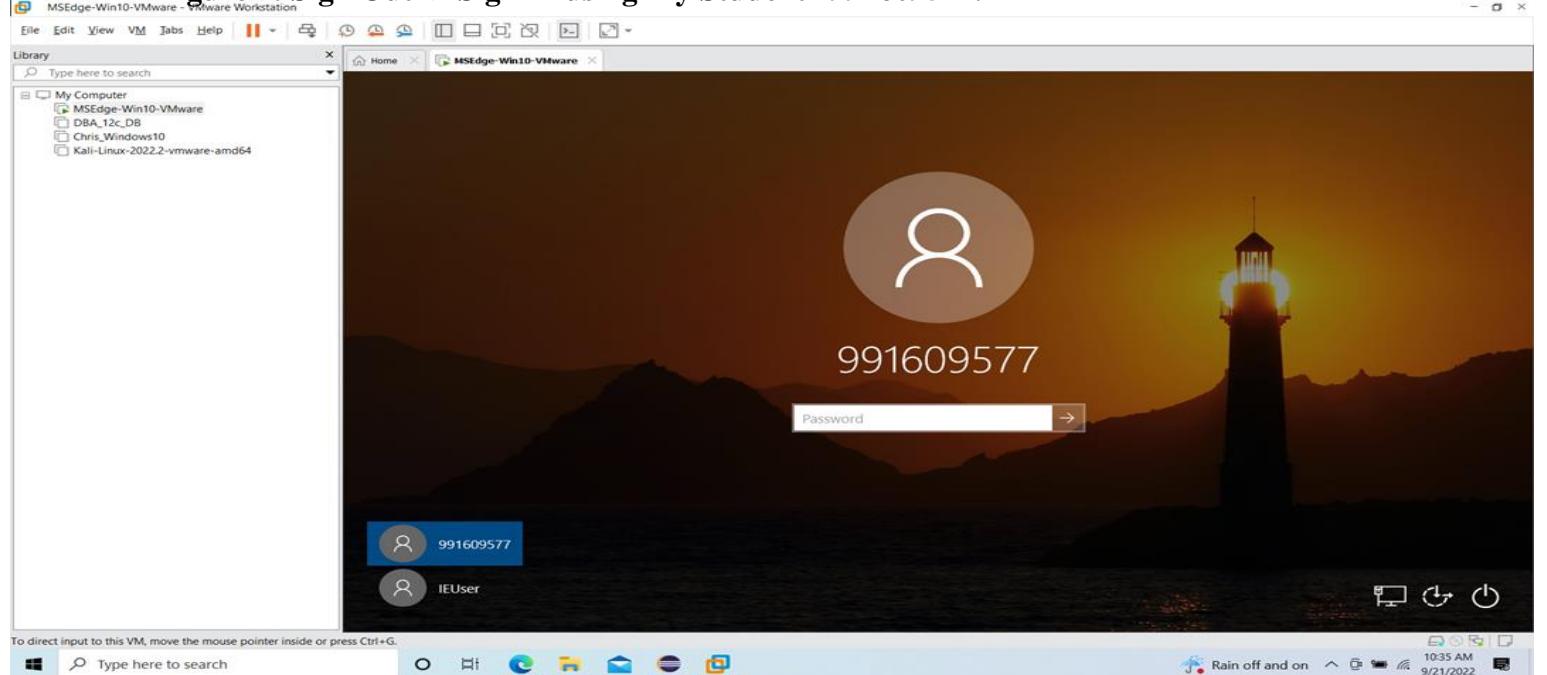
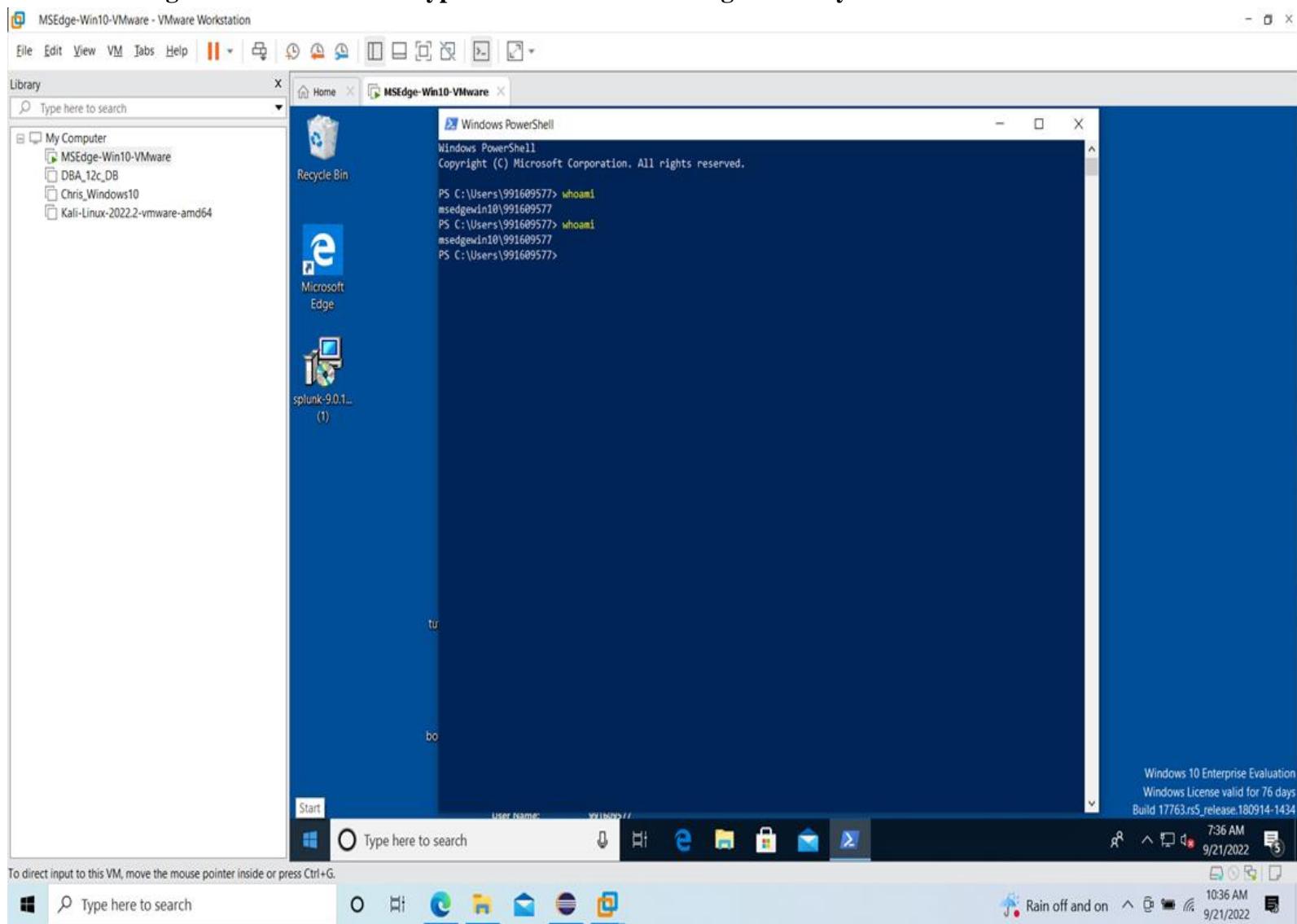
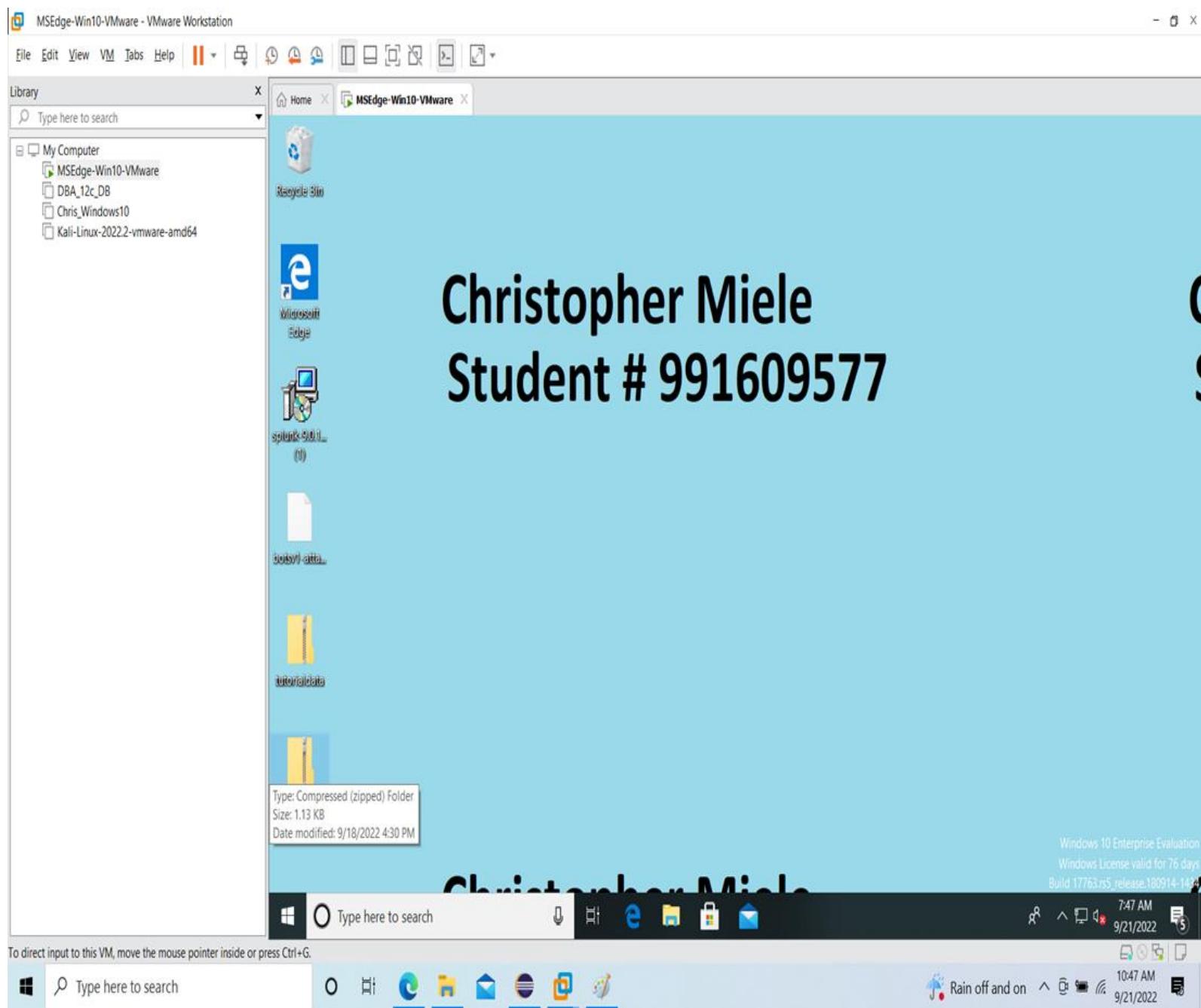


Figure 5: Powershell -> Type whoami -> Confirm Signed In My Student #991609577



MS-Win10 Desktop Background

Figure 6: Confirming Desktop Background.



MS-Win10 Disable(AV, Firewall, Updates)

Figure 7: Settings -> Update and Security -> Windows Security Virus Threat Protection-> Manage Settings Turn Everything Off.

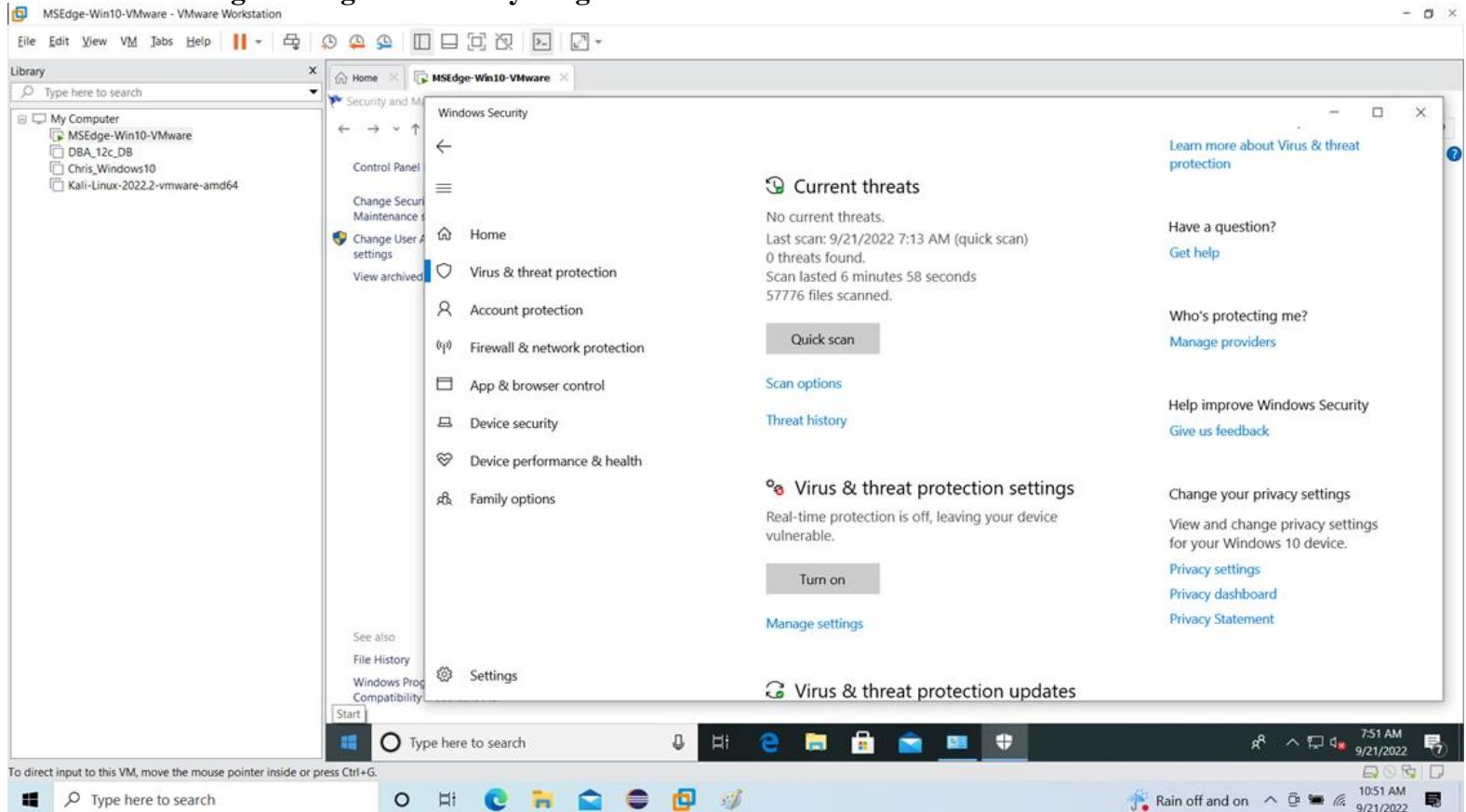


Figure 8: Settings -> Update and Security -> Firewall & Network Protection -> Click Domain Network/Private Network/Public Network -> Turn Off.

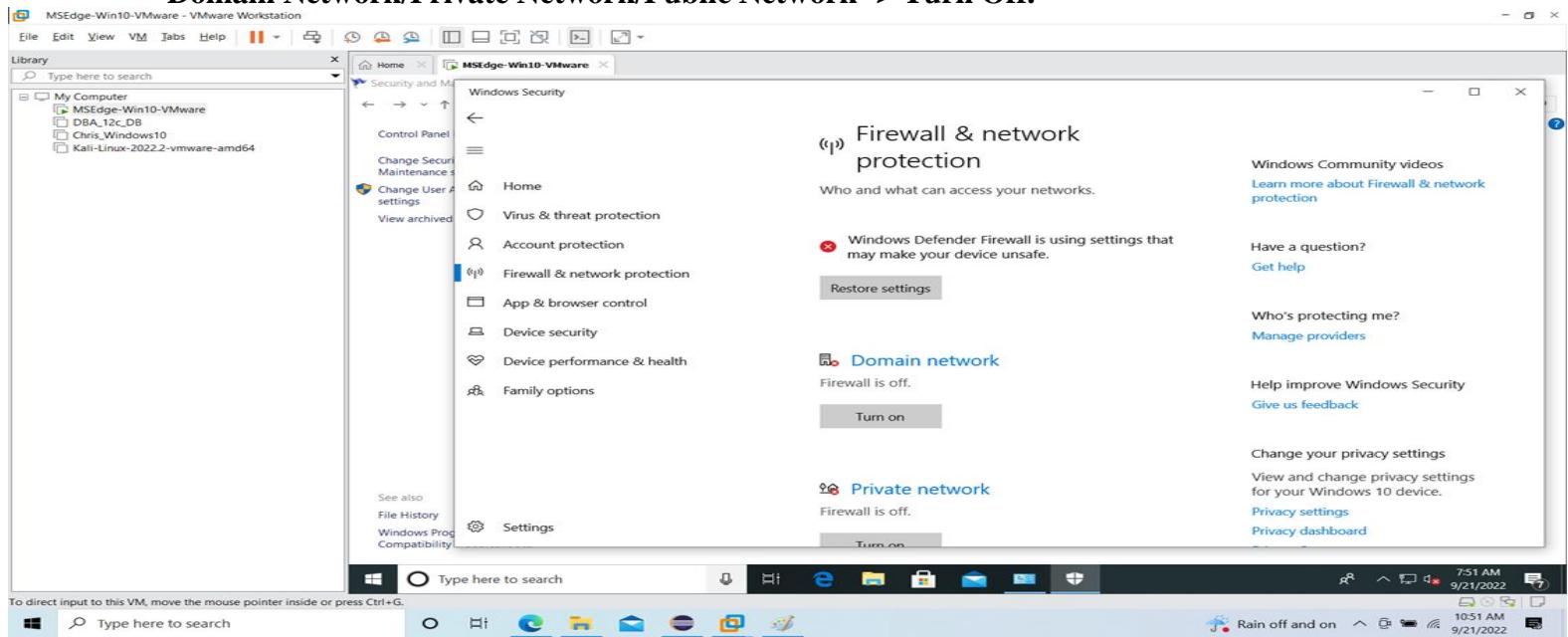


Figure 9: Settings -> Update and Security -> Firewall & Network Protection -> Click Domain Network/Private Network/Public Network -> Turn Off.

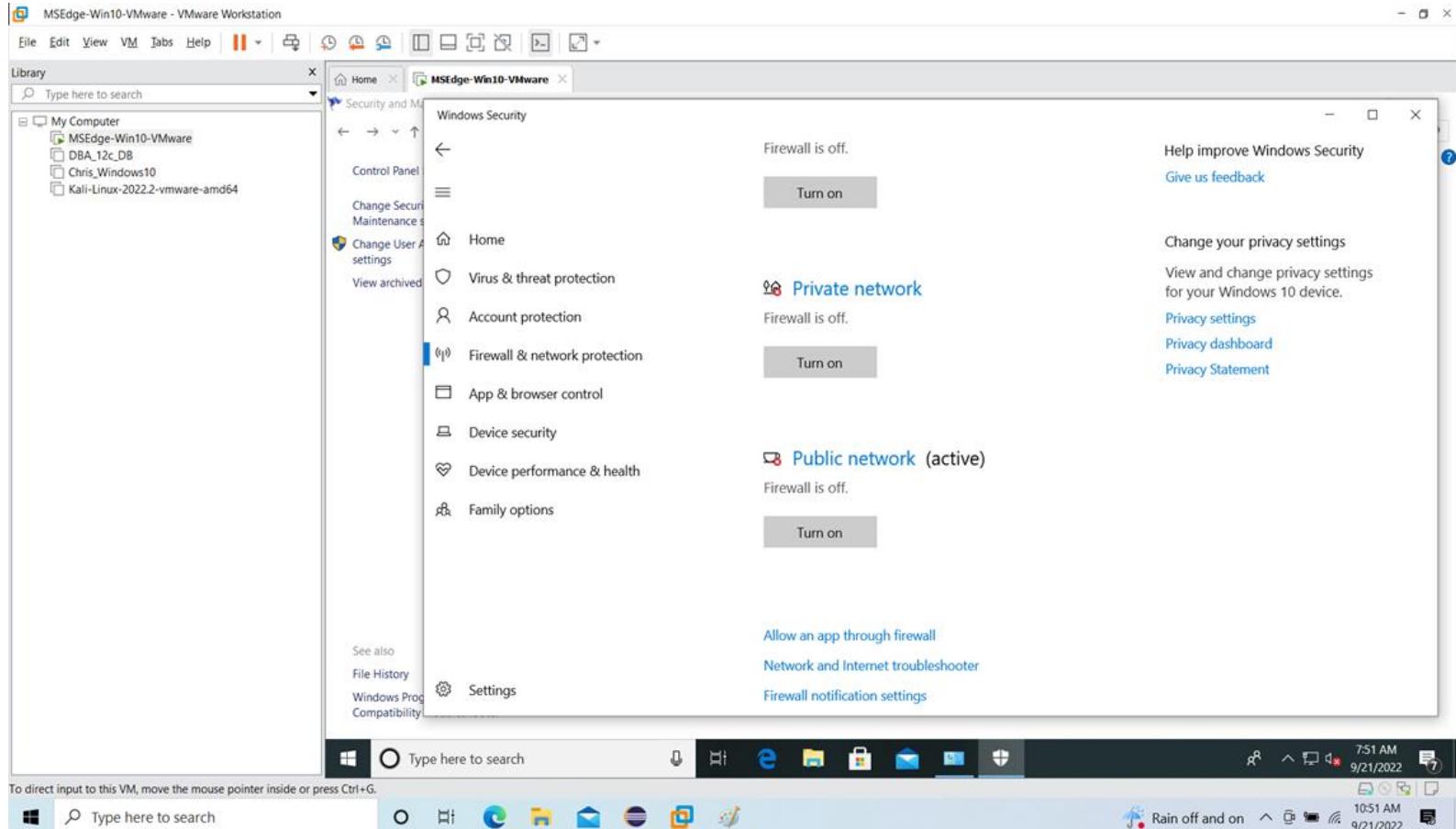
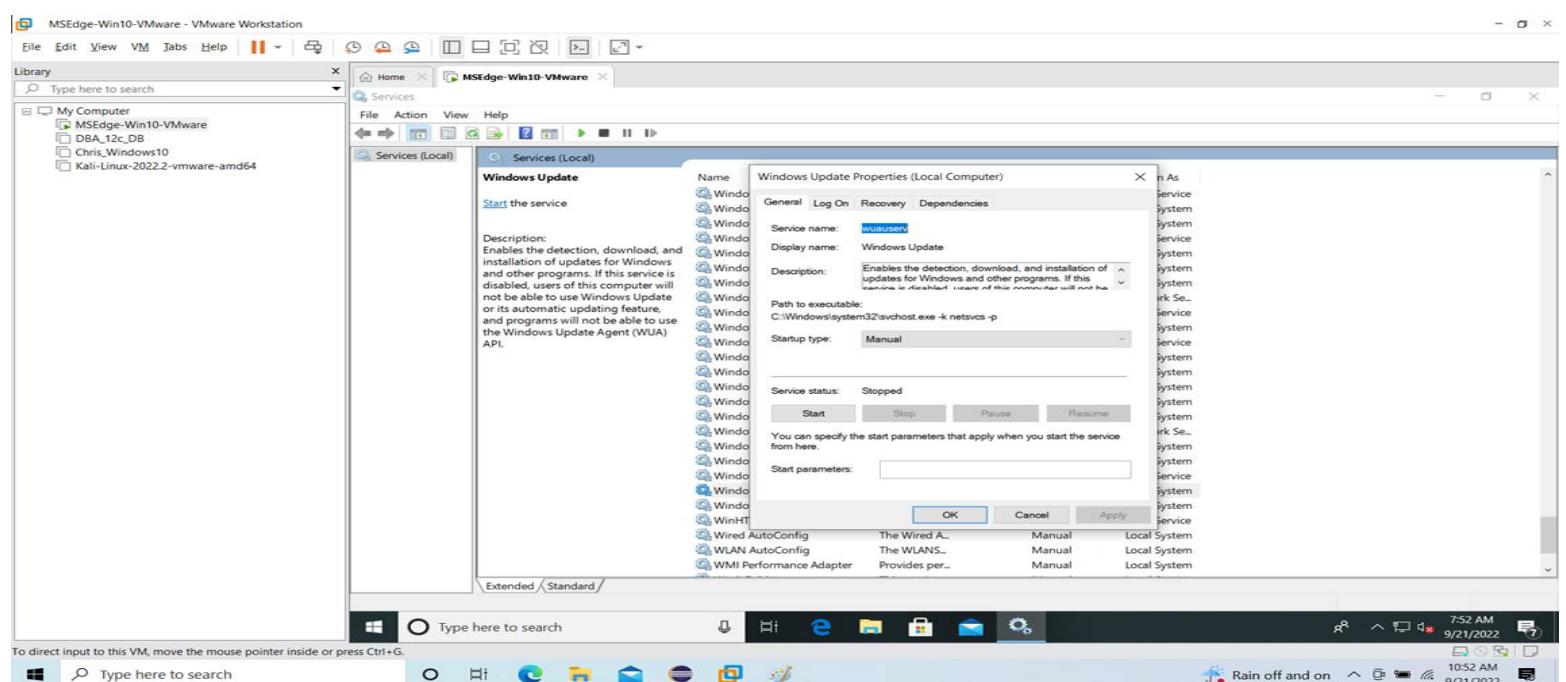
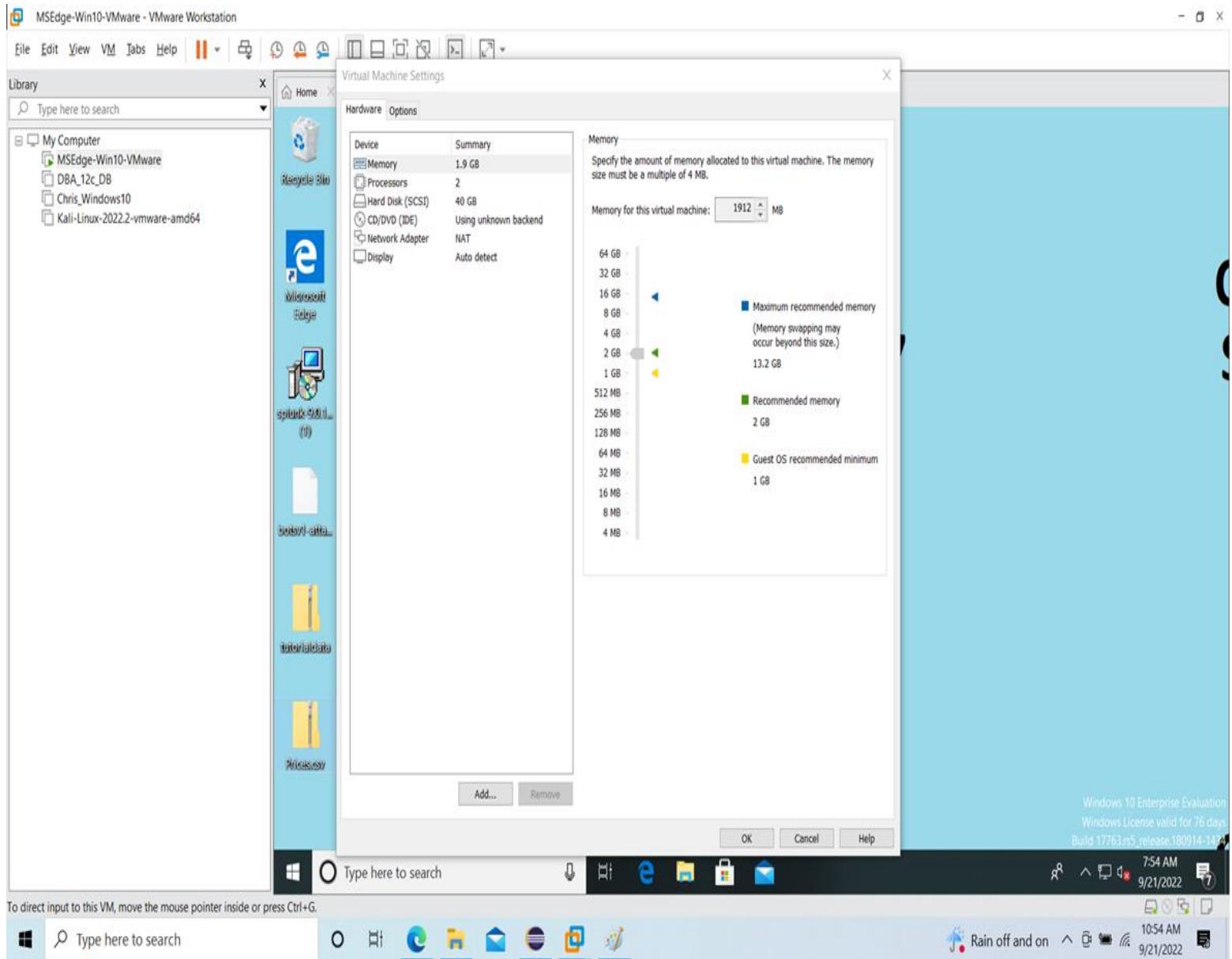


Figure 10: Services -> Windows Updates Properties(Local Computer) -> Stop Updates.



MS-Win10 VM NAT/Disk Space

Figure 11: Click MSEdge-Win10-VMWare -> VM -> Settings -> Hardware.



Lab 2

Splunk Search

Figure 12: Run search on tutorialdata.zip specify client ip address as a filter.

The screenshot shows the Splunk 9.0.1 interface. The search bar contains the query: `source="tutorialdata.zip:*" clientip="87.194.216.51"`. The results section displays 3,108 events found before 9/29/22 3:16:14.000 PM. The Events tab is selected, showing a timeline visualization and a list of events. The list includes two entries:

Time	Event
9/8/22 6:08:53.000 PM	87.194.216.51 - [08/Sep/2022:18:08:53] "POST /oldlink?itemId=EST-15&JSESSIONID=SD6SL4FF7ADFFF53055 HTTP/1.1" 200 3635 "http://www.w.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 175 clientip = 87.194.216.51 host = www2 price = 39.99 productName = Orvil the Wolverine source = tutorialdata.zip:\www2\access.log
9/8/22 6:08:53.000 PM	87.194.216.51 - [08/Sep/2022:18:08:53] "POST /oldlink?itemId=EST-15&JSESSIONID=SD6SL4FF7ADFFF53055 HTTP/1.1" 200 3635 "http://www.w.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 175 clientip = 87.194.216.51 host = www2 price = 39.99 productName = Orvil the Wolverine source = tutorialdata.zip:\www2\access.log

The bottom status bar shows the URL `127.0.0.1:8000/en-US/app/search/search?q=search source%3D"tutorialdata.zip%3A*" clientip%3D"87.194.216.51"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1664489...`.

Boss of SOC Walkthrough

Figure 13: Upload bots-attack-only.tgz

Explain: Splunk Add Data Upload the botsv1-attack-only.tgz

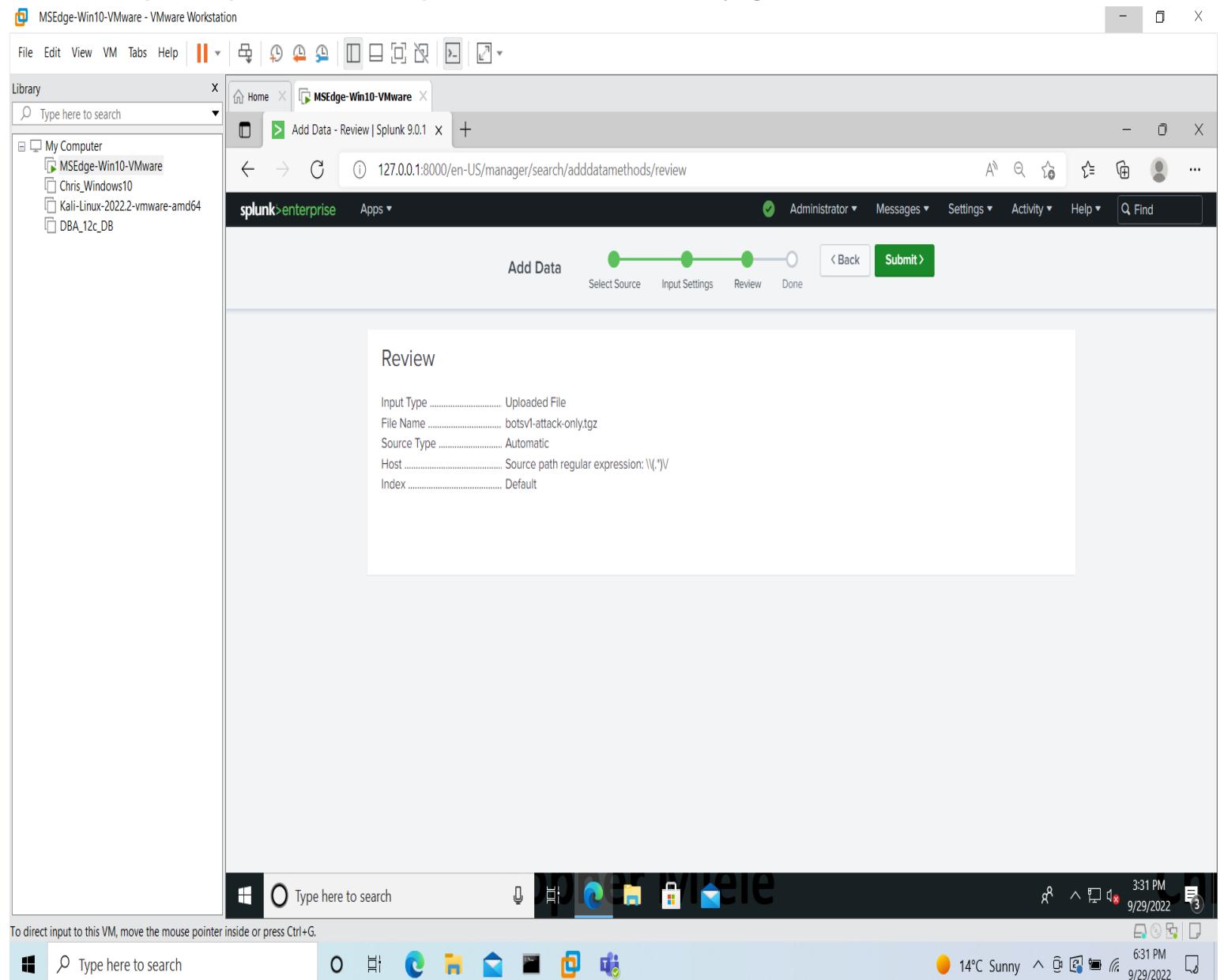


Figure 14: Q2 What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

Command: source="botsv1-attack-only.tgz:/*" imreallynotbatman.com srcip="40.80.148.42"

Explain: The command above allows you to search(Query) tgz file using the parameters imreallynotbatman and srcip.

The screenshot shows the Splunk 9.0.1 interface. The top navigation bar includes File, Edit, View, VM, Tabs, Help, and various icons. A sidebar on the left shows a Library with items like My Computer (MSEdge-Win10-VMware, Chris_Windows10, Kali-Linux-2022.2-vmware-amd64, DBA_12c_DB). The main search bar contains the query: source="botsv1-attack-only.tgz:/*" imreallynotbatman.com srcip="40.80.148.42". Below the search bar, it says "25,364 events (before 9/29/22 4:14:49:000 PM) No Event Sampling". The Events tab is selected, showing a timeline chart and a list of 25,364 events. One event is highlighted with a yellow box, showing details: host = botsv1_data_set/var/lib/splunk/botsv1/db/db_1470868141_1470799731_28/raw... source = botsv1-attack-only.tgz:1:botsv1_data_set/var/lib/splunk/botsv1/db/db_1470868141... srcip = 40.80.148.42. The bottom status bar indicates "421 PM 9/29/2022".

Figure 15: Q3 What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example, “Microsoft” or “Oracle”)

Command: source="botsv1-attack-only.tgz:" imreallynotbatman.com
srcip="40.80.148.42"

Answer: Acunetix

Explain: Searching tgz file using the parameters imreallynotbatman.com and source ip(Attacker) to find the Web Vulnerability Scanner Information.

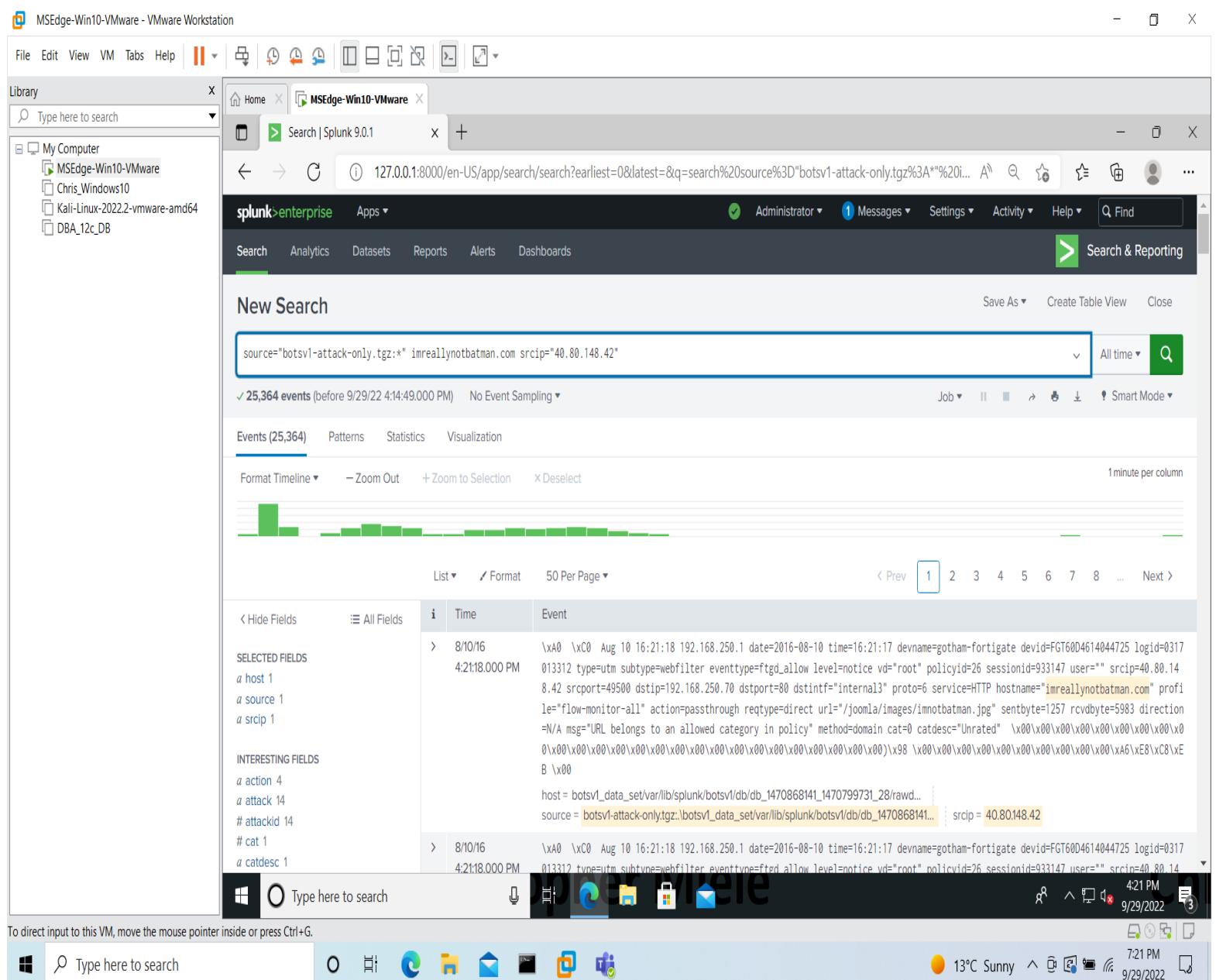


Figure 16:

The screenshot shows a Microsoft Edge browser window titled "MSEdge-Win10-VMware" displaying a Splunk search results page. The URL in the address bar is 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3Dbotsv1%20imreallynotbatman.com&display.p... The search results table has columns for Time and Event. One event entry is visible, showing a complex JSON-like log entry. The browser interface includes a navigation bar, a search bar, and a status bar at the bottom indicating the date and time.

Figure 17:

This screenshot shows the same MSEdge browser window and Splunk search results page as Figure 16, but with a different log entry displayed. The event details show a POST request to /joomla/index.php/component/search/ with various headers and parameters. The browser interface and system tray are also visible.

Figure 18: Q4 What Content Management System is imreallynotbatman.com likely using?

Command: index=botsv1 imreallynotbatman.com

Answer: Joomla

Explain: Searching the Index has events(bots-attack-only.tgz) the argument is imreallynotbatman.com. The Content Management System is Joomla

The screenshot shows the Splunk 9.0.1 interface with a search bar containing "index=botsv1 imreallynotbatman.com". The results pane displays 78,683 events. A detailed view of one event is shown, highlighting fields such as app_proto, dest_ip, dest_port, event_type, fileinfo, flow_id, http, in_iface, proto, src_ip, and src_port. The event timestamp is 8/10/16 3:23:09.473 PM. The event type is fileinfo, and the fileinfo field contains a JSON object with various file metadata. The Splunk interface includes a timeline, search filters, and a bottom navigation bar.

Figure 19:

This screenshot is identical to Figure 18, showing the same search results and event details for the Joomla CMS. The event highlighted in the previous screenshot is also present here, showing a fileinfo event with a JSON payload containing file metadata like name, size, and type. The Splunk interface remains consistent with the previous screenshot.

Figure 20: Q5 What name of the file that defaced the imreallynotbatman.com website?

Command: index=botsv1 c_ip="192.168.250.70"

Answer: poison-ivy-is-coming-for-you-batman.jpeg

Explain: Search the events located in the botsv1 using the argument 192.168.250.70. The File that defaced the website is poison-ivy-is-coming-for-you-batman.jpeg.

The screenshot shows the Splunk interface with the search bar containing "index=botsv1 c_ip=192.168.250.70". The results pane displays 9 events. One event is selected, showing a detailed log entry. The log entry is extremely long and contains various system and network details, including timestamps, hostnames, and file paths. The Splunk interface also includes a sidebar with "My Computer" and "splunk>enterprise" sections, and a bottom taskbar with icons for file operations and system status.

Figure 21 Answer

The screenshot shows the Splunk interface with the search bar containing "index=botsv1 c_ip=192.168.250.70". The results pane displays 9 events. One event is selected, showing a detailed log entry. The log entry is extremely long and contains various system and network details, including timestamps, hostnames, and file paths. The Splunk interface also includes a sidebar with "My Computer" and "splunk>enterprise" sections, and a bottom taskbar with icons for file operations and system status.

Figure 22: Q6 This attack used dynamic DNS to resolve the malicious IP. What is the Fully Qualified Domain Name (FQDN) associated with this attack?

Command: index=botsv1 c_ip="192.168.250.70"

Answer: prankglasslinebracket.jumpingcrab.com

Explain: Search the botsv1 the c_ip is the destination ip address. The fully qualified domain name is prankglasslinebracket.jumpingcrab.com

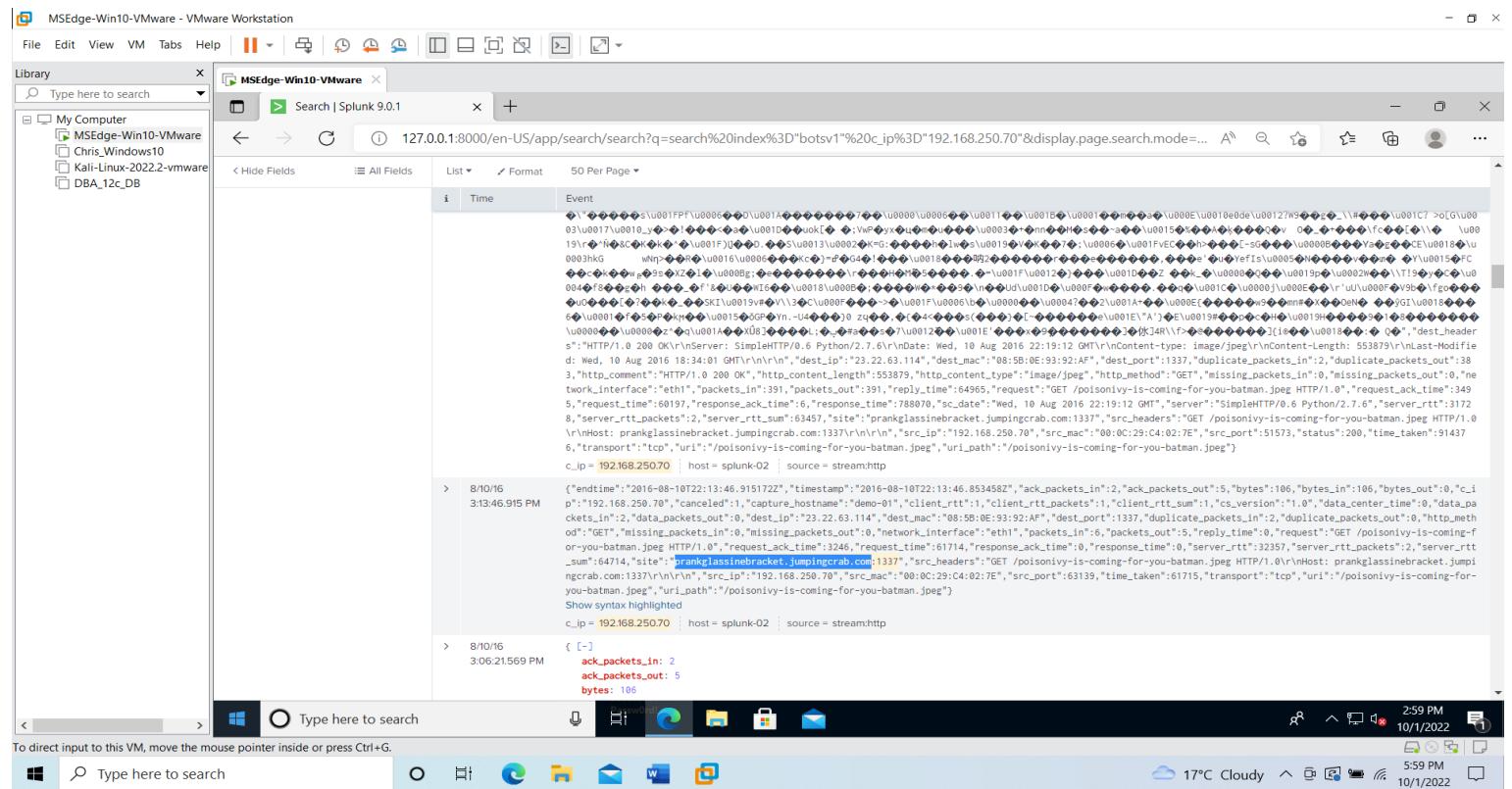


Figure 23: Q7 What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

Command: index="botsv1" imreallynotbatman srcip="23.22.63.114"

Answer: 23.22.63.114

Explain: Search the botsv1 the arguments are website name imreallynotbatman and the source ip address is attack wayne enterprises. To confirm this lookup ip in virustotal(Get info about IP Address/Domain/Hashes/etc).

Splunk search results for index='botsv1' imreallynotbatman srcip='23.22.63.114' showing 1,236 events. The results list three log entries from August 10, 2016, at 15:46:51, each detailing a connection attempt from host 192.168.250.1 to port 514 on 23.22.63.114 via HTTP.

Time	Event
Aug 10 15:46:51 2016	Aug 10 15:46:51 192.168.250.1 date=2016-08-10 time=15:46:51 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=26 sessionid=922313 user="" srcip=23.22.63.114 srport=47317 dstip=192.168.250.70 dstport=80 dstinf="internal" proto=6 service=HTTP hostname="imreallynotbatman.com" profile="flow-monitor-all" action="passthrough retype=direct url="/joomla/administrator/index.php" sentbyte=223 rcvbyte=0 direct ion=N/A msg="URL belongs to an allowed category in policy" method=domain cat=0 catdesc="Unrated" devname = gotham-fortigate host = 192.168.250.1 service = HTTP source = udp:514 srcip = 23.22.63.114
Aug 10 15:46:51 2016	Aug 10 15:46:51 192.168.250.1 date=2016-08-10 time=15:46:51 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=26 sessionid=922313 user="" srcip=23.22.63.114 srport=47316 dstip=192.168.250.70 dstport=80 dstinf="internal" proto=6 service=HTTP hostname="imreallynotbatman.com" profile="flow-monitor-all" action="passthrough retype=direct url="/joomla/administrator/index.php" sentbyte=223 rcvbyte=0 direct ion=N/A msg="URL belongs to an allowed category in policy" method=domain cat=0 catdesc="Unrated" devname = gotham-fortigate host = 192.168.250.1 service = HTTP source = udp:514 srcip = 23.22.63.114
Aug 10 15:46:51 2016	Aug 10 15:46:51 192.168.250.1 date=2016-08-10 time=15:46:51 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=26 sessionid=922313 user="" srcip=23.22.63.114 srport=47315 dstip=192.168.250.70 dstport=80 dstinf="internal" proto=6 service=HTTP hostname="imreallynotbatman.com" profile="flow-monitor-all" action="passthrough retype=direct url="/joomla/administrator/index.php" sentbyte=223 rcvbyte=0 direct ion=N/A msg="URL belongs to an allowed category in policy" method=domain cat=0 catdesc="Unrated" devname = gotham-fortigate host = 192.168.250.1 service = HTTP source = udp:514 srcip = 23.22.63.114

Figure 24 Answer

VirusTotal analysis for IP address 23.22.63.114. The analysis shows 0 detected files and 3 communicating files. The results include passive DNS replication data and communication details for 3 files.

Date resolved	Detections	Resolver	Domain
2019-12-01	0 / 94	VirusTotal	waynecorpinc.com
2019-11-30	0 / 94	VirusTotal	waneCorpinc.com
2019-11-29	0 / 94	VirusTotal	wynecorpinc.com
2019-11-28	0 / 94	VirusTotal	wayneCorpinc.com
2019-11-05	0 / 94	VirusTotal	wayncorpinc.com
2019-09-30	0 / 94	VirusTotal	waynecrpinc.com
2019-09-28	0 / 94	VirusTotal	waynecorpnc.com
2019-04-19	0 / 93	VirusTotal	ec2-23-22-63-114.compute-1.amazonaws.com
2018-07-18	0 / 94	VirusTotal	po1s0n1vy.com
2018-05-19	0 / 94	VirusTotal	www.po1s0n1vy.com

Figure 25: Q10 What is the name of the executable uploaded by Po1son1vy? Please include the file extension. (For example, “notepad.exe” or “favicon.ico”?)

Command: index="botsv1" dest_ip="192.168.250.70" sourcetype="stream:http" "multipart/form-data"

Answer: 3791.exe

Explain: The Command will search the botsv1 events. The arguments are Destination IP the traffic is http(Hyper Text Transfer Protocol). The executable that was uploaded was 3791.exe.

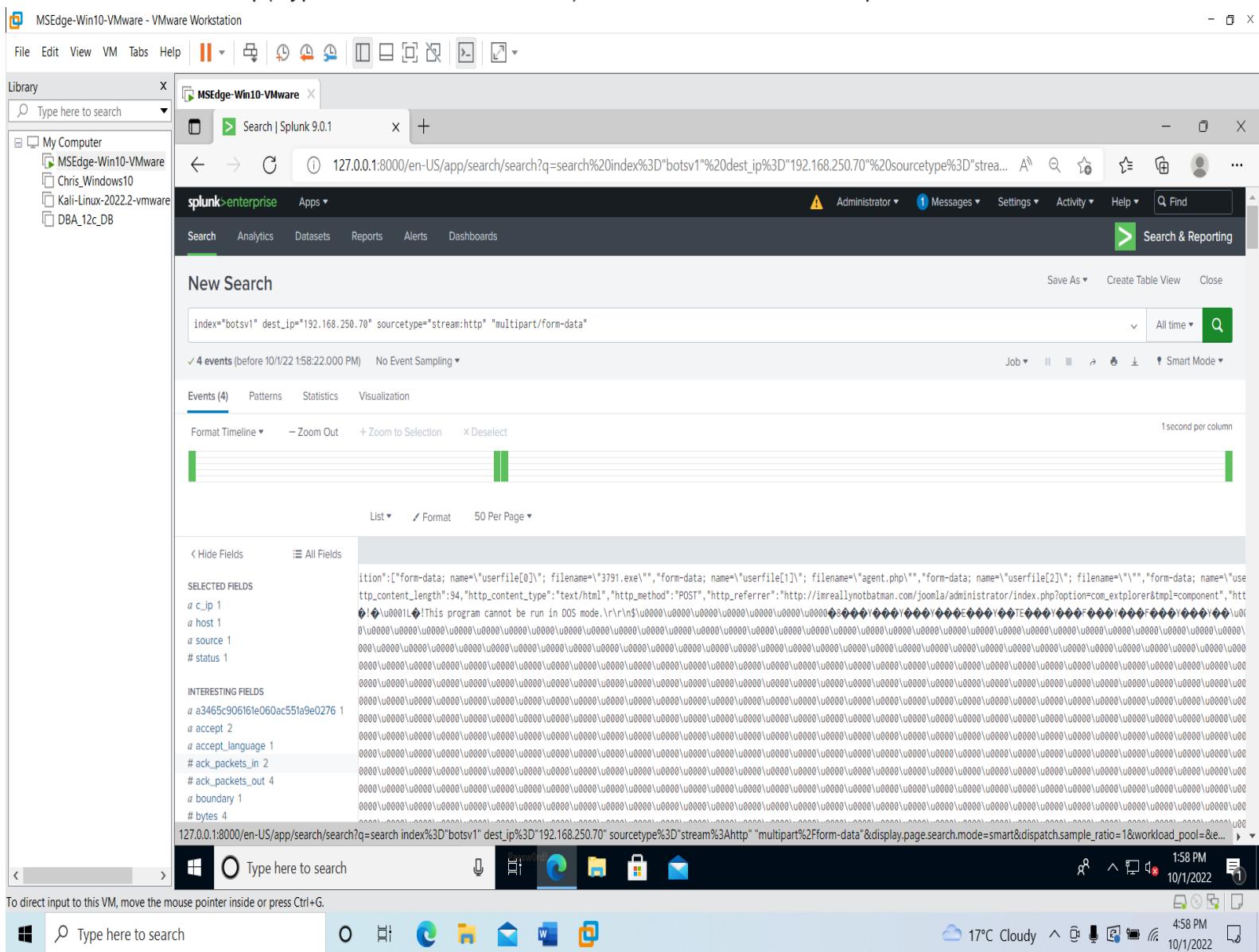


Figure 26: Question 11: What is the MD5 hash of the executable uploaded?

Command: index="botsv1" 3791.exe md5

Answer: AAE3F5A29935E6ABCC2C2754D12A9AF0

Explain: The index is botsv1 the command you run is 3791.exe command line, the md5 is the argument to find a search.

MSEdge-Win10-VMware

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- MSEdge-Win10-VMware
- Chris_Windows10
- Kali-Linux-2022.2-vmware
- DBA_12c_DB

MSEdge-Win10-VMware

Search | Splunk 9.0.1

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

index="botsv1" 3791.exe md5

67 events (before 10/1/22 2:07:15.000 PM) No Event Sampling

Events (67) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

1 minute per column

List Format 50 Per Page

< Prev 1 2 Next >

Hide Fields	All Fields	i Time	Event
SELECTED FIELDS	# EventCode_2 # host 1 # source 1	8/10/16 2:56:18.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>7</EventID><Version>3</Version><Level>4</Level><Task>7</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.158042500Z' /><EventRecordID>428923</EventRecordID><Correlation><Execution ProcessID='1296' ThreadID='1416' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149sr.vaynecorpinc.local</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.158</Data><Data Name='ProcessID'>E50000E0-A302-57AB-0000-0010B0D65C301</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla3791.exe</Data><Data Name='ImageLoaded'>C:\Windows\SysWOW64\apphelp.dll</Data><Data Name='Hashes'>SHA1=A8B065578C1843A0EFB344A9968844CE0B7AC2,MD5=950EDB4F82F895AD003C0F01E40D35,SHA256=C6B87BEDCCA74292812A16FE0E8315EAF0E24E6222F75800F38ED23AA5,IMPHASH=8E1A2561CD562E77B201BC61500B3668</Data><Data Name='Signed'>true</Data><Data Name='Signature'>Microsoft Windows</Data></EventData></Event>
INTERESTING FIELDS	# Channel 1 # dvc 1 # dvc_nt_host 1 # event_id 67 # EventData_Xml 65 # EventID 2 # EventRecordID 67 # eventtype 2	8/10/16 2:56:18.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>7</EventID><Version>3</Version><Level>4</Level><Task>7</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.158042500Z' /><EventRecordID>428922</EventRecordID><Correlation><Execution ProcessID='1296' ThreadID='1416' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149sr.vaynecorpinc.local</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.158</Data><Data Name='ProcessID'>E50000E0-A302-57AB-0000-0010B0D65C301</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla3791.exe</Data><Data Name='ImageLoaded'>C:\Windows\SysWOW64\kernelbase.dll</Data><Data Name='Hashes'>SHA1=5A1029189E442A172A86E77F3B8A003E454C4D,MD5=04B04C070EE3F41EDF92F253C0D52A404,SHA256=2EA797486F125269</Data></EventData></Event>

2:09 PM 10/1/2022

Type here to search

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

209 PM 10/1/2022

17°C Cloudy 5:09 PM 10/1/2022

Figure 27 Answer

MSEdge-Win10-VMware - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- MSEdge-Win10-VMware
- Chris_Windows10
- Kali-Linux-2022.2-vmware
- DBA_12c_DB

MSEdge-Win10-VMware

Search | Splunk 9.0.1

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

index="botsv1" 3791.exe md5

67 events (before 10/1/22 2:07:15.000 PM) No Event Sampling

Events (67) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect

1 minute per column

List Format 50 Per Page

< Prev 1 2 Next >

Hide Fields	All Fields	i Time	Event
SELECTED FIELDS	# EventCode_2 # host 1 # source 1	8/10/16 2:56:18.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>7</EventID><Version>3</Version><Level>4</Level><Task>7</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.158042500Z' /><EventRecordID>70188F-C22A-43E0-BF4C-06F5698FFBD9</EventRecordID><Correlation><Execution ProcessID='1296' ThreadID='1420' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149sr.vaynecorpinc.local</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.158</Data><Data Name='ProcessID'>E50000E0-A302-57AB-0000-0010B0D65C301</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla3791.exe</Data><Data Name='ImageLoaded'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='Hashes'>SHA1=650F73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABC2C2754D12A9AF0,SHA256=EC78C93803A517319C2A3709C275971EC46CAF6E4790E2B2D04E97CC7FA45D,IMPHASH=481F4788B2C9C21E10B065F52B04C448</Data><Data Name='Signed'>false</Data><Data Name='Signature'></Data></EventData></Event>
INTERESTING FIELDS	# Channel 1 # dvc 1 # dvc_nt_host 1 # event_id 67 # EventData_Xml 65 # EventID 2 # EventRecordID 67 # eventtype 2	8/10/16 2:56:18.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>7</EventID><Version>3</Version><Level>4</Level><Task>7</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.158042500Z' /><EventRecordID>428910</EventRecordID><Correlation><Execution ProcessID='1296' ThreadID='1416' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149sr.vaynecorpinc.local</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.158</Data><Data Name='ProcessID'>E50000E0-A302-57AB-0000-0010B0D65C301</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla3791.exe</Data><Data Name='ImageLoaded'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='Hashes'>SHA1=650F73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABC2C2754D12A9AF0,SHA256=EC78C93803A517319C2A3709C275971EC46CAF6E4790E2B2D04E97CC7FA45D,IMPHASH=481F4788B2C9C21E10B065F52B04C448</Data><Data Name='Signed'>false</Data><Data Name='Signature'></Data></EventData></Event>

2:11 PM 10/1/2022

Type here to search

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

209 PM 10/1/2022

17°C Cloudy 5:11 PM 10/1/2022

Figure 28: Question 15: What was the first brute force password used?

Command: index="botsv1" sourcetype=stream:http imreallynotbatman.com

http_method=POST | stats count by src_ip, form_data, timestamp

Answer: 2016-08-10T21:45:14.774439Z

Explain: Indexes botsv1 the sourcetype is http traffic you are looking for on the website imreallynotbatman.com the POST sends data to the server.

The screenshot shows a Microsoft Edge browser window running on a Windows 10 VM. The URL is 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3Dstream%3Ahttp%20method%3DPOST%20|stats%20count%20by%20src_ip%2C%20form_data%2C%20timestamp. The search interface includes a sidebar with 'My Computer' options like MSEdge-Win10-VMware, Chris_Windows10, Kali-Linux-2022.2-vmware, and DBA_12c_DB. The main area shows a 'New Search' results table with columns: src_ip, form_data, timestamp, and count. The results list numerous entries from IP 23.22.63.114, each containing a different password value in the form_data column. The timestamp for all entries is 2016-08-10T21:45:14.774439Z. The bottom status bar shows the date as 10/1/2022 and the time as 3:51 PM.

src_ip	form_data	timestamp	count
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=12345678905e26acb2d4e136a4d7c64e08e62a58=1	2016-08-10T21:45:14.774439Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=1313138&9f2ed9f9ca6e1dc64840e5d128da80=1	2016-08-10T21:45:41.583263Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=20008204faf0060cec14a7b7daadf76e7174=1	2016-08-10T21:46:12.339620Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=21128489eb6cd88dc5b8d4b3949703a422423=1	2016-08-10T21:46:31.751455Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=222228771cb481c90942b16a708f2fd645c63=1	2016-08-10T21:46:35.060975Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=2222228857cef8afed2d52b0f11604085634bd5=1	2016-08-10T21:46:10.796908Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=5150&65bc0fd2b56c63120fedbf76e43d451=1	2016-08-10T21:46:11.062783Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=5555558ce580d48c605e0b80d447091acf1d52b=1	2016-08-10T21:46:33.781467Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=66666683b3c9e1b5cf66f1995013d3b746453c6=1	2016-08-10T21:45:15.884305Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&password=69698e90034a8e58d4c4f00908f51f68e39dd=1	2016-08-10T21:45:14.51958Z	1

Figure 29: Question 16 One of the passwords in the brute force attack is James Brodsky's Favorite Cold Play Song.

Command: index="botsv1" sourcetype=stream:http imreallynotbatman.com http_method=POST yellow | stats count by src_ip, form_data

Answer: Yellow

Explain: The command searches botsv1 for traffic http on the website imreallynotbatman.com the method is POST(Send Data Server). Yellow is one of the brute force passwords.

MSEdge-Win10-VMware - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- MSEdge-Win10-VMware
- Chris Windows10
- Kali-Linux-2022.2-vmware
- DBA_12c_DB

MSEdge-Win10-VMware x

Search | Splunk 9.0.1

127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3Dstream%3Ahttp%2... A Q F

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

New Search

index="botsv1" sourcetype=stream:http imreallynotbatman.com http_method=POST yellow | stats count by src_ip, form_data

✓ 1 event (before 10/1/22 4:06:55.000 PM) No Event Sampling ▾

Events Patterns Statistics (I) Visualization

10 Per Page ▾ Format Preview ▾

src_ip	form_data	count
23.22.63.114	username=admin&task=login&return=a\5k2YguGh&option=com_login&passwd=yellow&e445198b23c3d02dc9b25bb13c3e241=1	1

Type here to search

4:08 PM 10/1/2022

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

16°C Cloudy 7:08 PM 10/1/2022

Figure 30: Question 17 What was the correct password for admin access to the content management system running “imreallynotbatman.com”?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd* |stats count by src_ip, form_data, timestamp

Answer: batman

Explain: Search botsv1 for http traffic and the website form inputs you are looking for is username and passwords.

MSEdge-Win10-VMware - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- MSEdge-Win10-VMware
- Chris_Windows10
- Kali-Linux-2022.2-vmware
- DBA_12c_DB

MSEdge-Win10-VMware

Search | Splunk 9.0.1

127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3Dstream%3Ahttp%2...

splunk>enterprise Apps

Administrator Messages Settings Activity Help

New Search

Save As Create Table View Close

index="botsv1" sourcetype=stream:http form_data=*username*passwd* |stats count by src_ip, form_data, timestamp

✓ 413 events (before 10/1/22 4:13:53.000 PM) No Event Sampling

Events Patterns Statistics (413) Visualization

10 Per Page Format Preview

src_ip	form_data	timestamp	count
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=yellow&e445198b23c30d02dc9b25bb13c3e241=1	2016-08-10T21:45:18.889296Z	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=zxvcvn&cf5378040a86e9eb8345af0dd6ef4177=1	2016-08-10T21:45:42.833525Z	1
40.80.148.42	username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1	2016-08-10T21:48:04.185612Z	1

Start Type here to search

4:14 PM 10/1/2022

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search

7:14 PM 10/1/2022

Figure 31: Question 18 What was the average password length used in the password brute forcing attempt?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd*
| rex field=form_data "&passwd=(?<password>[\w\d]+)&"
| eval lenpassword=len(password)
| stats avg(lenpassword) as avglen

Answer: 6.179710144927537

Explain: Search botsv1 the arguments are http traffic, form inputs usernames, passwords. You are searching for the average password length used in brute forcing attempt.

The screenshot shows a Microsoft Edge browser window running on a Windows 10 VM. The URL is 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=8&q=search%20index%3D"botsv1"%20sourcetype%3Dstream%3Ahttp%2... The Splunk interface is visible, with the search bar containing the command: index="botsv1" sourcetype=stream:http form_data=*username*passwd* | rex field=form_data "&passwd=(?<password>[\w\d]+)&" | eval lenpassword=len(password) | stats avg(lenpassword) as avglen. The search results show 413 events, with the average password length (avglen) listed as 6.179710144927537.

Figure 31: Question 19 How many seconds elapsed between the brute force password scan identified the correct password and the compromised login?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd*

```
| rex field=form_data "&passwd=(?<password>[\w\d]+)&"
```

```
| search password = "batman"
```

Answer: 92.17

Explain: Search botsv1 for http traffic and form data username, password. The correct password was batman. You minus the Times and get the result of 92.17

Figure 32: Question 20 How many unique passwords were attempted in the brute force attempt?

Command: index="botsv1" sourcetype=stream:http form_data=*username*passwd*
| rex field=form_data "&passwd=(?<password>[\w\d]+)&"

Answer: 412

Explain: Search botsv1 the arguments are http traffic, form data is username and password.
The &passwd is any type of password that means the regular expression requirements.

The screenshot shows the Splunk interface with a search bar containing the command: index="botsv1" sourcetype=stream:http form_data=*username*passwd* | rex field=form_data "&passwd=(?<password>[\w\d]+)&". The search results indicate 413 events found. The event list table includes columns for Time and Event. The event details show a timestamp of 8/10/16 2:48:05.858 PM, a URL like 248.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3Dstream%3Ahttp%20form_data%3D*username*passwd%0A%7Crex field%3Dform_data "%26passwd%3D(%3F<password>%5B%5Cw%5C... and various HTTP headers and parameters. The bottom of the screen shows the Windows taskbar with the Start button, a search bar, and icons for File Explorer, Mail, and Microsoft Edge. The system tray shows the date as 10/1/2022 and the time as 7:45 PM.

Figure 33: Question 21 What was the most likely IP of we8105desk in 24AUG2016?

Command: index="botsv1" we8105desk

| stats count by src_ip

Answer: 192.168.250.100

Explain Search botsv1 the argument is we8105desk and you are determining what ip address is associated with we8105desk on the date of Aug 24 2016.

The screenshot shows the Splunk interface within a VMware Workstation window titled 'MSEdge-Win10-VMware - VMware Workstation'. The search bar contains the command: `index="botsv1" we8105desk | stats count by src_ip`. The search results table has 'Statistics (6)' selected, showing the following data:

src_ip	count
127.0.0.1	1
192.168.2.50	2744
192.168.250.100	145
192.168.250.20	1
::1	3
FE80:0000:0000:0000:9DAC:222E:C1F8:D3D8	12

The Windows taskbar at the bottom shows various icons and the date/time: 10/1/2022, 4:51 PM.

Figure 34: Question 22 Amongst the Suricata signatures that detected the Cerber Malware, which one alerted the fewest number of times?

Command: index="botsv1" host="suricata-ids.waynecorpinc.local" cerber

Answer: 2816763

Explain: Obtain search info about botsv1 the host is suricata ids information the cerber is the malware.

The screenshot shows the Splunk 9.0.1 interface with a search bar containing the query: index="botsv1" host="suricata-ids.waynecorpinc.local" cerber. The results show 5 events found before 10/1/22 4:58:33.000 PM. A context menu is open over the first row of the table, specifically over the "alert.signature_id" field. The menu options include "List", "Format", and "50 Per Page". The "Format" tab is selected, displaying a table with three rows of data:

Values	Count	%
2816764	2	40%
2820156	2	40%
2816763	1	20%

Figure 35: Question 26 What is the name of the USB key inserted by Bob Smith?

Command: index="botsv1" sourcetype=winregistry friendlyname

Answer: MIRANDA-PRI

Explain: Search botsv1 the source is winregistry freindlyname is one of the directories.

The screenshot shows a VMware Workstation window titled "MSEdge-Win10-VMware - VMware Workstation". Inside, a Splunk 9.0.1 search interface is displayed. The search bar contains the command: `index="botsv1" sourcetype=winregistry friendlyname`. The results show two events from 10/22/2016 at 9:42:17 AM. Both events are from the host "weB05disk" and source "WinRegistry", with status "success". The first event is for a registry entry under "HKEY\SYSTEM\ControlSet001\Enum\usb\1\137c188d80Storage\Volume_7\usbstorndisk\ven_genericprod\flash_disk\arev_0.07170901190000\friendlyname". The second event is for a registry entry under "HKEY\SYSTEM\ControlSet001\Enum\usb\1\137c188d80Storage\Volume_7\usbstorndisk\ven_genericprod\flash_disk\arev_0.07170901190000\friendlyname". A context menu is open over the second event, with the option "Start" highlighted. A modal dialog box titled "registry_value_data" is also visible, showing a single value: "MIRANDA_PRI". The Splunk interface includes a sidebar with "My Computer" and a "Search" bar at the top.

Figure 36: Question 27 Bob Smith's workstation (we8105desk) was connected to a file server during the ransomware outbreak what is the IP address of the file server?

Command: index="botsv1" sourcetype="stream:smb" src_ip=192.168.250.100 | stats count by path

Answer: 192.168.250.20

Explain: search botsv1 the source is smb traffic, the source ip is 192.168.250.100 you are determining the ip address of the file server.

The screenshot shows a Microsoft Edge browser window running on a Windows 10 VM. The URL in the address bar is 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3D"stream%3Asmb"... The Splunk interface displays a search titled "New Search" with the command: index="botsv1" sourcetype="stream:smb" src_ip=192.168.250.100 | stats count by path. The results show 39,304 events found. The "Statistics" tab is selected, showing a table of file paths and their counts. The top result is '\\192.168.250.20\IPC\$', with a count of 10. Other entries include '\\192.168.250.20\fileshare' (1), '\\WE8105DESK\IPC\$' (1), '\\WE9041SRV\IPC\$' (34), '\\WE9041SRV\NETLOGON' (1), '\\WE9041SRV\SYSVOL' (2), '\\WE9041SRV\fileshare' (3), '\\waynecorpinc.local\IPC\$' (1), '\\we9041srv.waynecorpinc.local\IPC\$' (12), and '\\we9041srv.waynecorpinc.local\sysvol' (3).

path	count
\\192.168.250.20\IPC\$	10
\\192.168.250.20\fileshare	1
\\WE8105DESK\IPC\$	1
\\WE9041SRV\IPC\$	34
\\WE9041SRV\NETLOGON	1
\\WE9041SRV\SYSVOL	2
\\WE9041SRV\fileshare	3
\\waynecorpinc.local\IPC\$	1
\\we9041srv.waynecorpinc.local\IPC\$	12
\\we9041srv.waynecorpinc.local\sysvol	3

Figure 37: Question 28 How many Distinct PDFs did the ransomware encrypt on the remote file server?

Command: index="botsv1" .pdf
| stats dc(Relative_Target_Name)

Answer: 258

Explain: Search botsv1 for pdfs on file server. 258 files were encrypted.

The screenshot shows a Microsoft Edge browser window titled 'MSEdge-Win10-VMware - VMware Workstation'. The address bar displays the URL: 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20.pdf%20%0A%7C%20stats%20dc(%20Relative_Target_Name)%20)". The Splunk interface is visible, with the 'enterprise' instance selected. The search bar contains the command: 'index="botsv1" .pdf | stats dc(Relative_Target_Name)'. Below the search bar, it says '865 events (before 10/1/22 5:40:17.000 PM) No Event Sampling'. The 'Statistics' tab is selected under the results view. The result table shows one row with 'dc(Relative_Target_Name)' and the value '258'. The bottom status bar of the browser shows the date and time as '10/1/2022 5:41 PM'.

Figure 38: Question 31 The malware downloads a file that contains the Cerber ransomware crypto code. What is the name of that file?

Command: index="botsv1" sourcetype="suricata" src_ip=192.168.250.100 solidaritedeproximite.org

Answer: mhtr.jpg Explain: Search botsv1 for source suricata(IDS) source ip 192.168.250.100 and the url is solidaritedeproximite.org.

The screenshot shows the Splunk 9.0.1 interface with the following details:

- Search Bar:** 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D"botsv1"%20sourcetype%3D"suricata"%20src_i...
- Results:** 2 events (before 10/1/22 5:45:49.000 PM) No Event Sampling
- Event 1:**

```

@host:1
@source:1
#status:1

@bytes:1
@date_hour:1
@date_index:1
@date_minute:1
@date_month:1
@date_second:2
@date_year:1
@date_zone:1
@dest:1
@dest_ip:2
@dest_port:2
@dnsid:1
@dnsname:1
@dnsrtype:1
@dnsuid:1
@dnsxip:1
@dc:1
@event_type:2
@eventtype:2
@flow_id:2
@http_hostname:1
@http_http_content_type:1
@http_method:1
@http_user_agent:1
@http_length:1
@http_protocol:1
@http_status:1
@httpuri:1
@measure_content_type:1
Start End

```
- Event 2:**

```

@host:1
@source:1
#status:1

@bytes:1
@date_hour:1
@date_index:1
@date_minute:1
@date_month:1
@date_second:2
@date_year:1
@date_zone:1
@dest:1
@dest_ip:2
@dest_port:2
@dnsid:1
@dnsname:1
@dnsrtype:1
@dnsuid:1
@dnsxip:1
@dc:1
@event_type:2
@eventtype:2
@flow_id:2
@http_hostname:1
@http_http_content_type:1
@http_method:1
@http_user_agent:1
@http_length:1
@http_protocol:1
@http_status:1
@httpuri:1
@measure_content_type:1
Start End

```
- Visualizations:** A histogram visualization titled "http.url" is open, showing a single value: "/mhtr.jpg".
- Bottom Navigation:** Shows the Windows taskbar with icons for File Explorer, Mail, and Microsoft Edge, along with system status indicators like battery level, signal strength, and date/time (10/1/2022, 5:47 PM).

Lab 3

Event Log

Figure 39: Administrator Windows Powershell -> New-EventLog -LogName “Application” -Source “Chris Miele”.

Write-EventLog -LogName “Application” -Source “Chris Miele” -EventID 3908 -Message “Lab 3”.

Explain: Create PowerShell script to create a new event log the source Chris Miele(Must do this first before you write event log). Then you must Write the event log, the Event ID is 3908 and the Message is a custom message called Lab 3. This will show up in the eventlog on windows.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> New-EventLog -LogName "Application" -Source "Chris Miele"
PS C:\Windows\system32> Write-EventLog -LogName "Application" -Source "Chris Miele" -EventID 12293908 -Message "Lab 3"
Write-EventLog : Cannot validate argument on parameter 'EventId'. The 12293908 argument is greater than the maximum allowed range of 65535. Supply an argument
At line:1 char:70
+ ... LogName "Application" -Source "Chris Miele" -EventID 12293908 -Messag ...
+ ~~~~~~
+ CategoryInfo          : InvalidData: (:) [Write-EventLog], ParameterBindingValidationException
+ FullyQualifiedErrorId : ParameterArgumentValidationError,Microsoft.PowerShell.Commands.WriteEventLogCommand

PS C:\Windows\system32> Write-EventLog -LogName "Application" -Source "Chris Miele" -EventID 1229-3908 -Message "Lab 3"
Write-EventLog : Cannot bind parameter 'EventId'. Cannot convert value "1229-3908" to type "System.Int32". Error: "Input string was not in a correct format."
At line:1 char:70
+ ... gName "Application" -Source "Chris Miele" -EventID 1229-3908 -Messag ...
+ ~~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Write-EventLog], ParameterBindingValidationException
+ FullyQualifiedErrorId : CannotConvertArgumentNoMessage,Microsoft.PowerShell.Commands.WriteEventLogCommand

PS C:\Windows\system32> Write-EventLog -LogName "Application" -Source "Chris Miele" -EventID "12293908" -Message "Lab 3"
Write-EventLog : Cannot validate argument on parameter 'EventId'. The 12293908 argument is greater than the maximum allowed range of 65535. Supply an argument
At line:1 char:70
+ ... gName "Application" -Source "Chris Miele" -EventID "12293908" -Messag ...
+ ~~~~~~
+ CategoryInfo          : InvalidData: (:) [Write-EventLog], ParameterBindingValidationException
+ FullyQualifiedErrorId : ParameterArgumentValidationError,Microsoft.PowerShell.Commands.WriteEventLogCommand

PS C:\Windows\system32> Write-EventLog -LogName "Application" -Source "Chris Miele" -EventID 3908 -Message "Lab 3"
PS C:\Windows\system32>
```

Figure 40: Settings -> Forwarding and receiving -> Receive Data -> Default Port Receive Splunk 9997.

Explain: To forward event logs from host to guest(MSEdge) you must set up the Receive port which is splunk default 9997. The receive port will receive any data coming into splunk and make a connection with the host operating system.

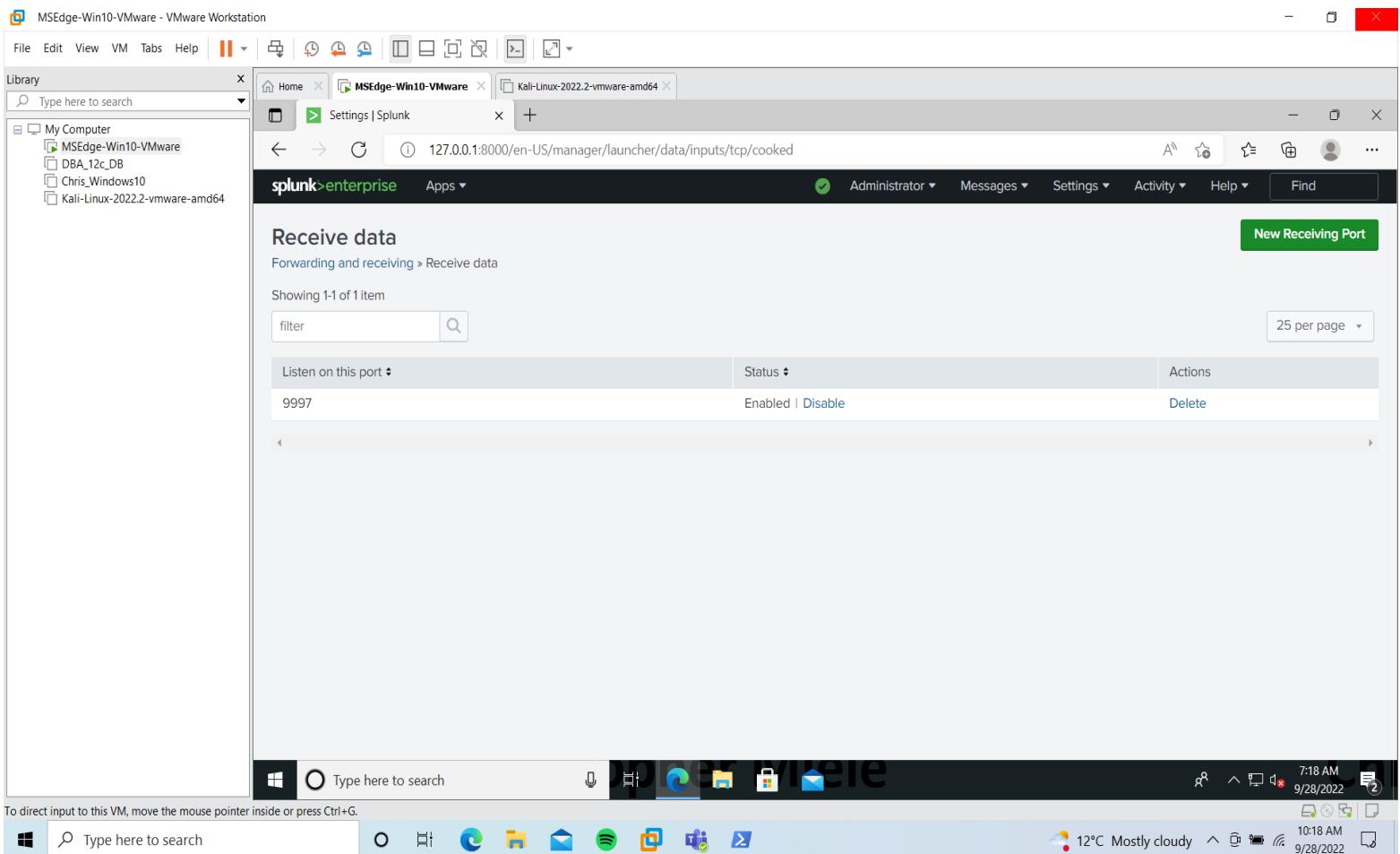


Figure 41:Settings -> Indexes(Events Coming In Sent To win10_events -> Create New Index.

Explain: Index is where you can parse Event logs to. Index makes it easier to search/Query information.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path
_audit	Edit Delete Disable	Events	system	5 MB	488.28 GB	43.4K	7 days ago	a few seconds ago	\$SPLUNK_D\B\audit\db	N/A
_configtracker	Edit Delete Disable	Events	system	5 MB	488.28 GB	256	7 days ago	an hour ago	\$SPLUNK_D\B\configtracker\db	N/A
_internal	Edit Delete Disable	Events	system	29 MB	488.28 GB	342K	7 days ago	a few seconds ago	\$SPLUNK_D\B\internal\db	N/A
_introspection	Edit Delete Disable	Events	system	64 MB	488.28 GB	34.2K	7 days ago	a few seconds ago	\$SPLUNK_D\B\introspection\db	N/A
_metrics	Edit Delete Disable	Metrics	system	19 MB	488.28 GB	263K	7 days ago	a few seconds ago	\$SPLUNK_D\B\metrics\db	N/A

Figure 42: Verify win10_events.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path
_metrics_rollover	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_D\B\metrics_rollover\db	N/A
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	5	7 days ago	2 hours ago	\$SPLUNK_D\B\telemetry\db	N/A
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_D\B\thefishbucket\db	N/A
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_D\B\history\db	N/A
main	Edit Delete Disable	Events	system	223 MB	488.28 GB	3.99M	10 years ago	20 days ago	\$SPLUNK_D\B\default\db	N/A
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_D\B\splunklogger\db	N/A
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_D\B\summary\db	N/A
win10_events	Edit Delete Disable	Events	search	1 MB	500 GB	0			\$SPLUNK_D\B\win10_events\db	N/A

Figure 43: Download Splunk Universal Forwarder(Allows you to send Win Events Logs From Host - Guest).

Explain: Download Splunk Universal Forwarder to forward information from host to guestOS.

The screenshot shows the Splunk website at https://www.splunk.com/en_us/download/universal-forwarder.html. The main heading is "Splunk Universal Forwarder 9.0.1". Below it, there's a section titled "Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data." There are two icons: one for "Collects Data From Remote Sources" showing a network connection, and one for "Scalable" showing a grid of squares. To the right, there's a form titled "Start Your Free Download" with fields for Business Email, Password, First Name, Last Name, Job Title, and Phone Number. The Windows taskbar at the bottom shows various pinned icons and the date/time as 10:36 AM 9/28/2022.

Figure 44: Type ipconfig to get VM IP Address.

The screenshot shows a Windows 10 desktop with a VMware Workstation window titled "MSEdge-Win10-VMware". Inside the window, a Command Prompt window is open. The user has typed "ipconfig" and is viewing the output for the "Ethernet adapter Ethernet0:". The output shows the following details:

```
Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . : localdomain
  Link-local IPv6 Address . . . . . : fe80::f0cf:857b:da02:7eaa%5
  IPv4 Address . . . . . : 192.168.112.128
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.112.2
```

The Windows taskbar at the bottom shows various pinned icons and the date/time as 10:36 AM 9/28/2022.

Figure 45: Run Splunk Universal Forwarder Installer.

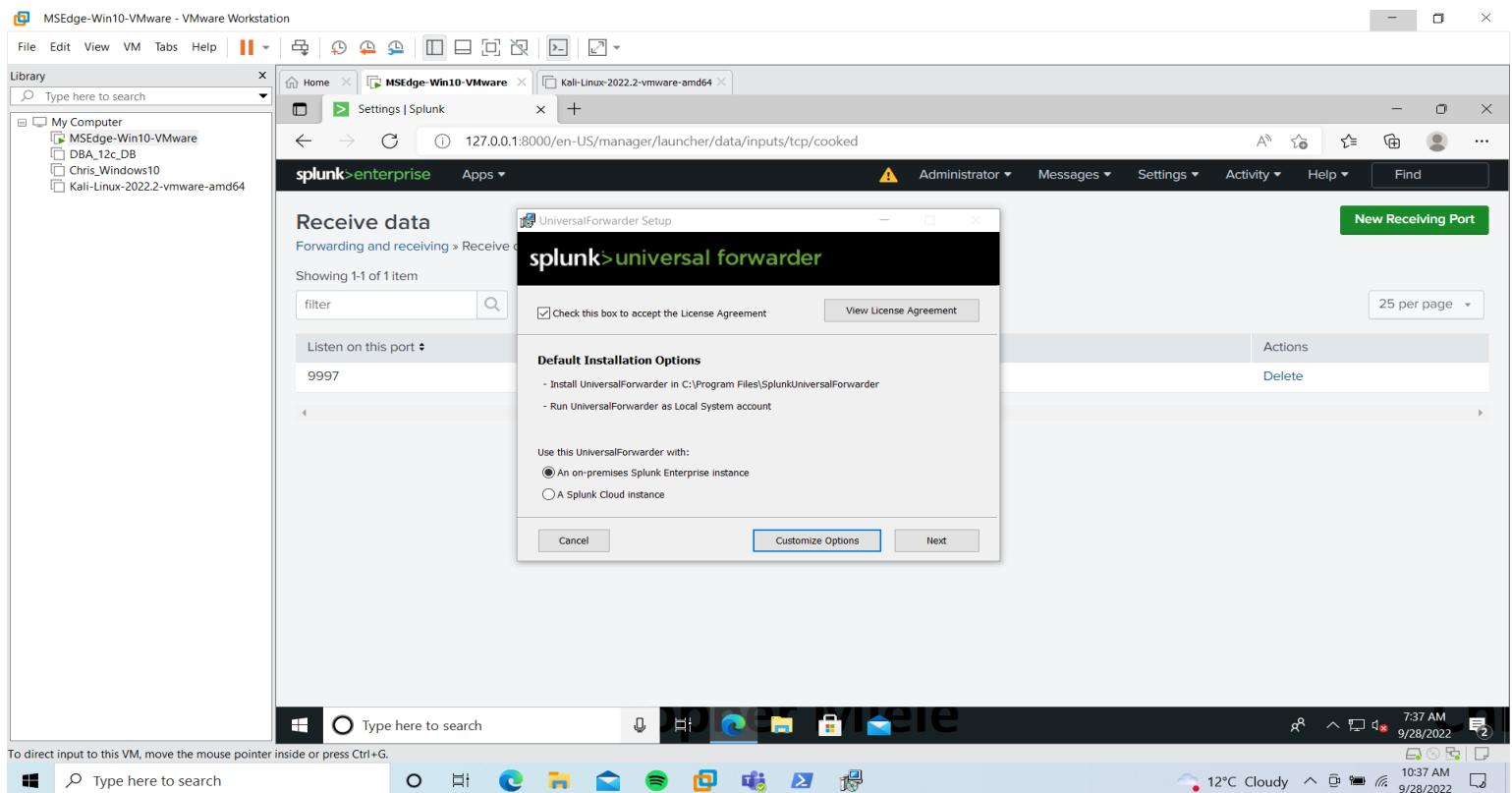


Figure 46: Insert Splunk Credentials.

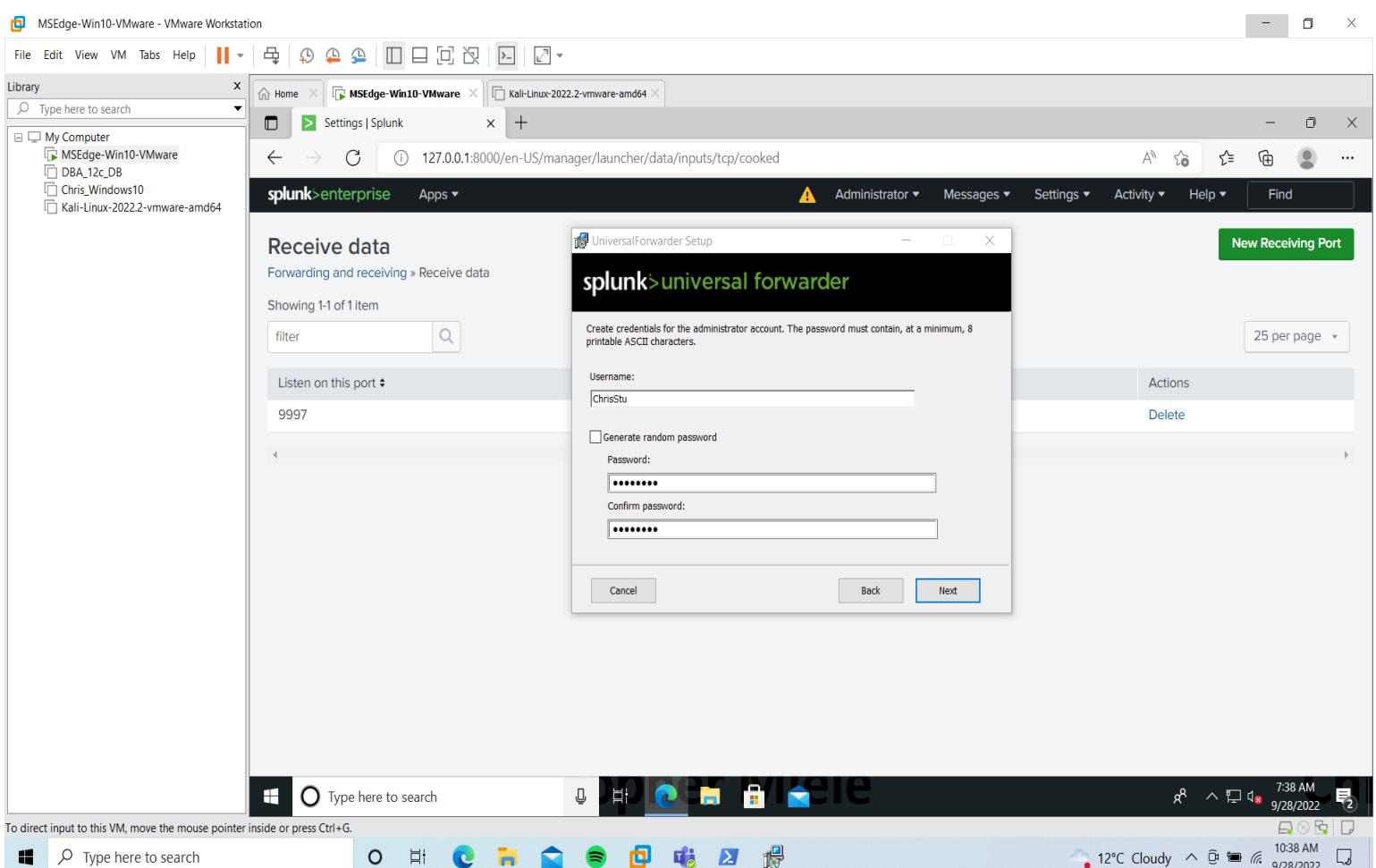


Figure 47: Deploy Server Host IP(Guest OS) VM IP “192.168.112.128” Port “8089”(Default Port Splunk)

Explain: Type in the GuestOS IP Address in the Splunk Forwarder. The port is 8089

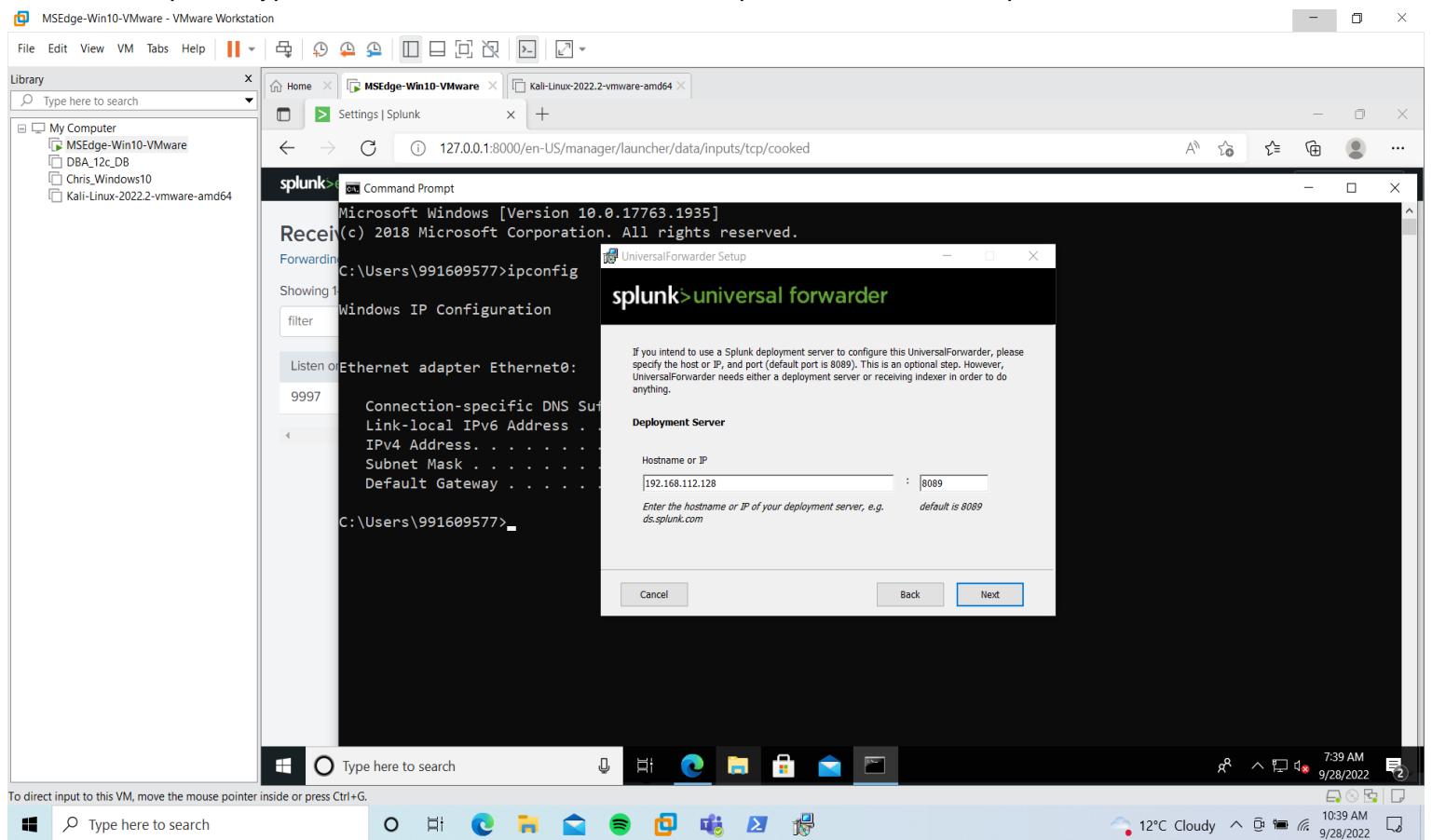


Figure 48: Receiving Indexer Host IP VM IP “192.168.112.128” Port “9997”(Default Port Splunk)

Explain: The Receiver Index is the Guest OS VM The Port is 9997. Splunk Forwarder will allow you to communicate and send logs from host to guest OS.

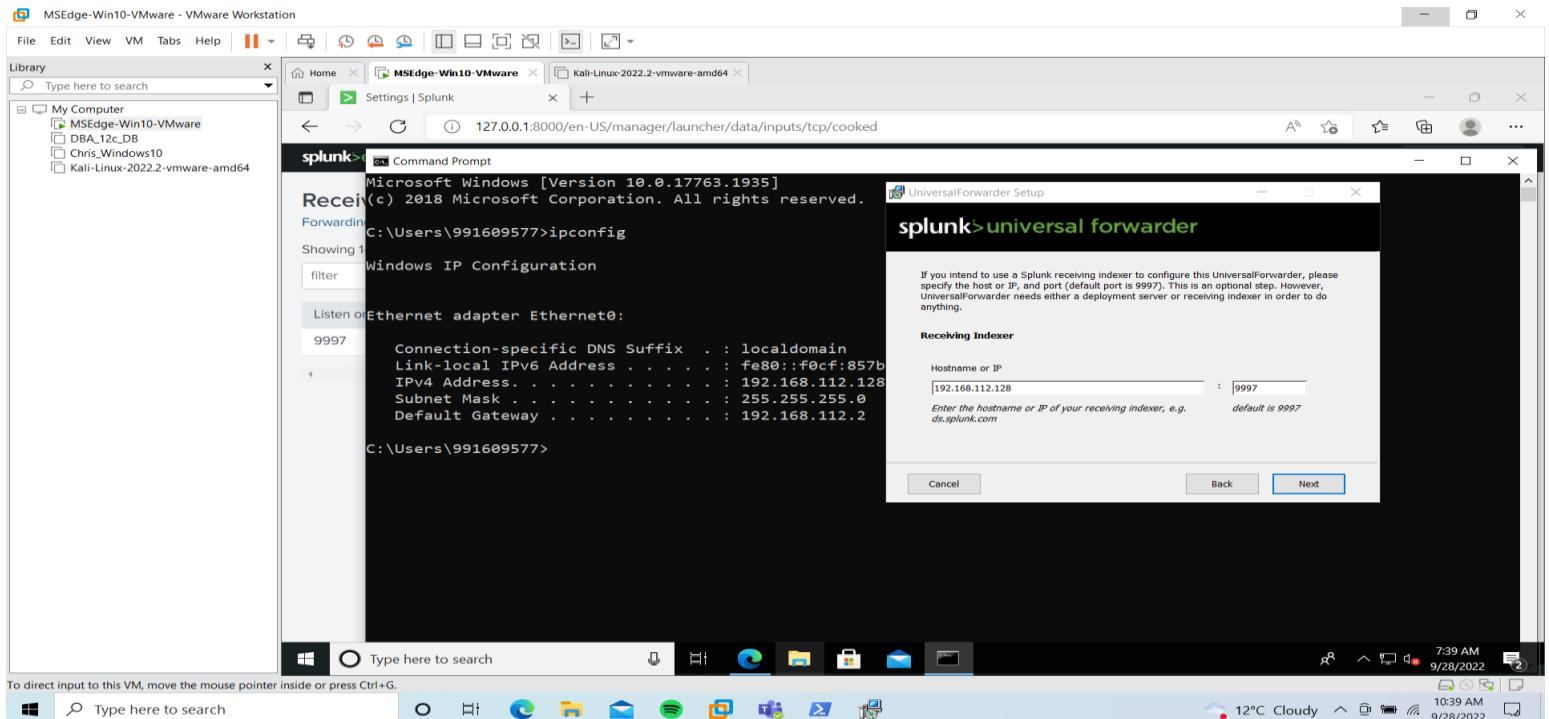


Figure 49: Finish Splunk Universal Forwarder Installer

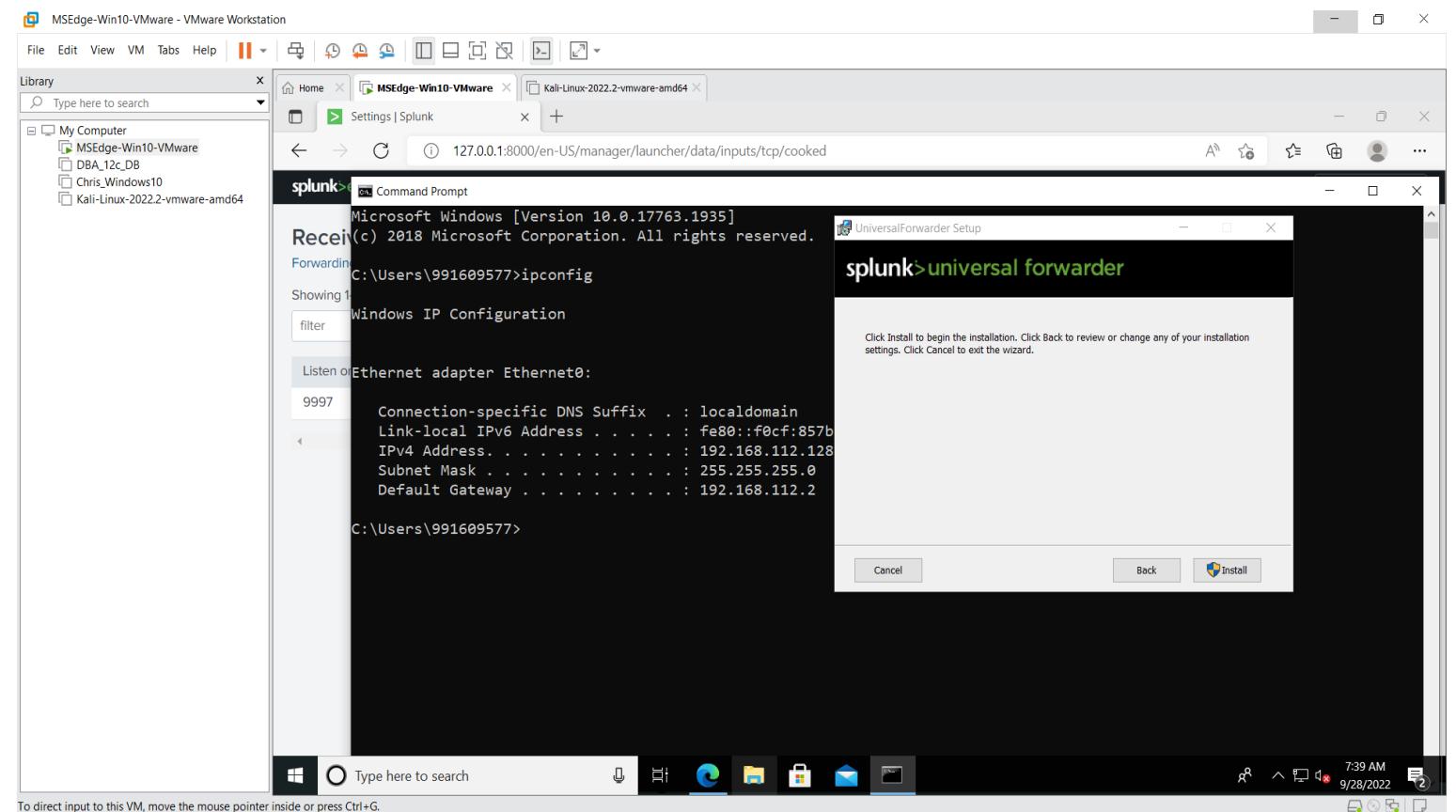


Figure 50: Add Data -> Forward.

Explain: Login to Splunk Click Splunk Forwader

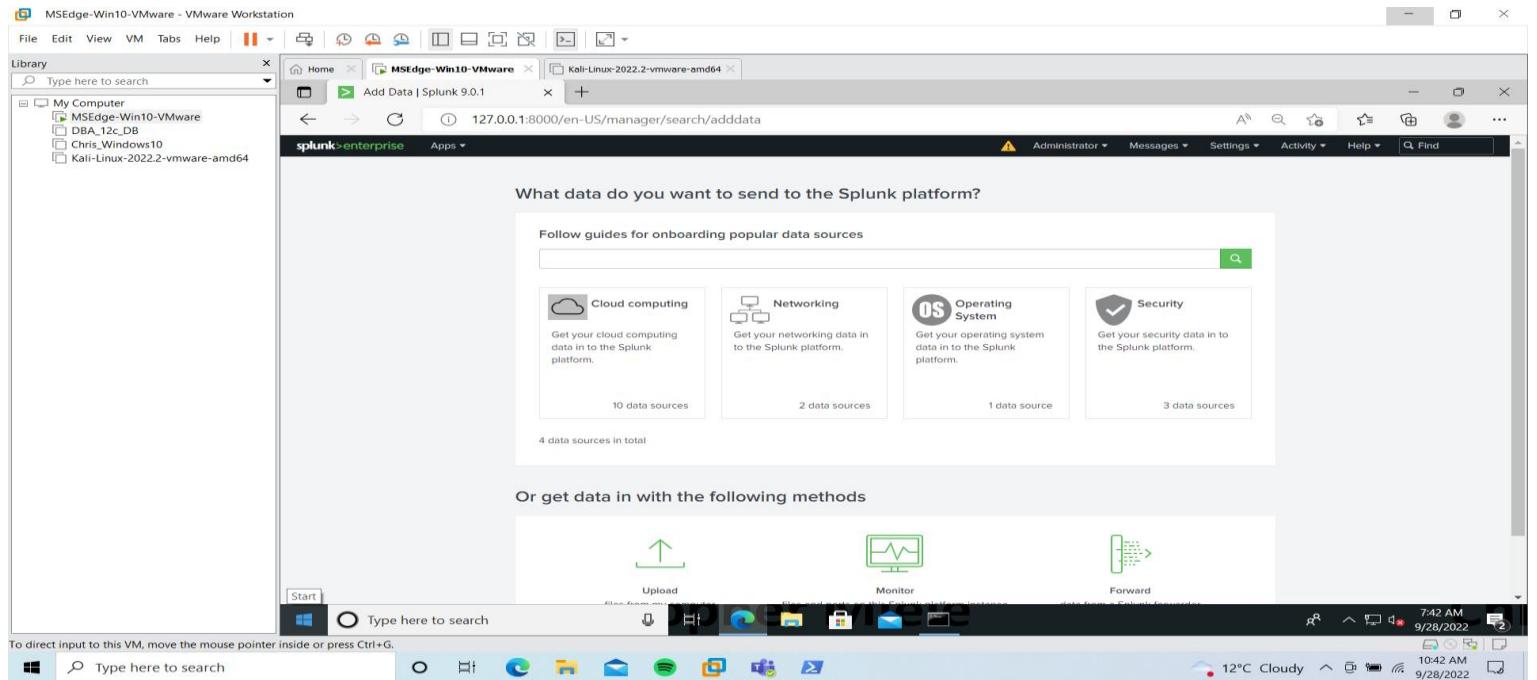


Figure 51: Verify Host Name Same As Host OS.

Explain: Compare the Host Name to Determine Same Name as Host OS

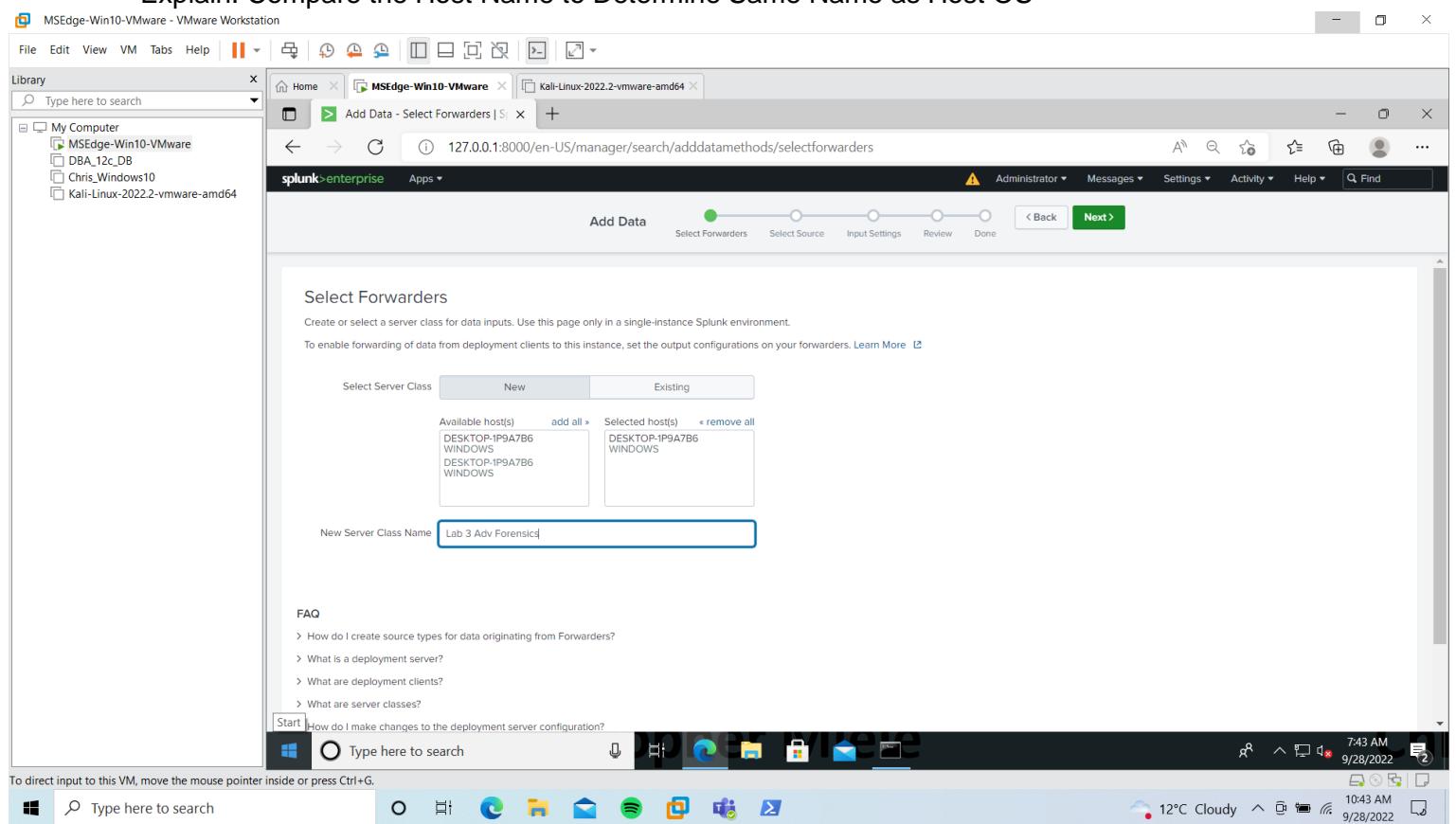


Figure 52:Run whoami in powershell Hostname matches Available Hosts Forwarders.

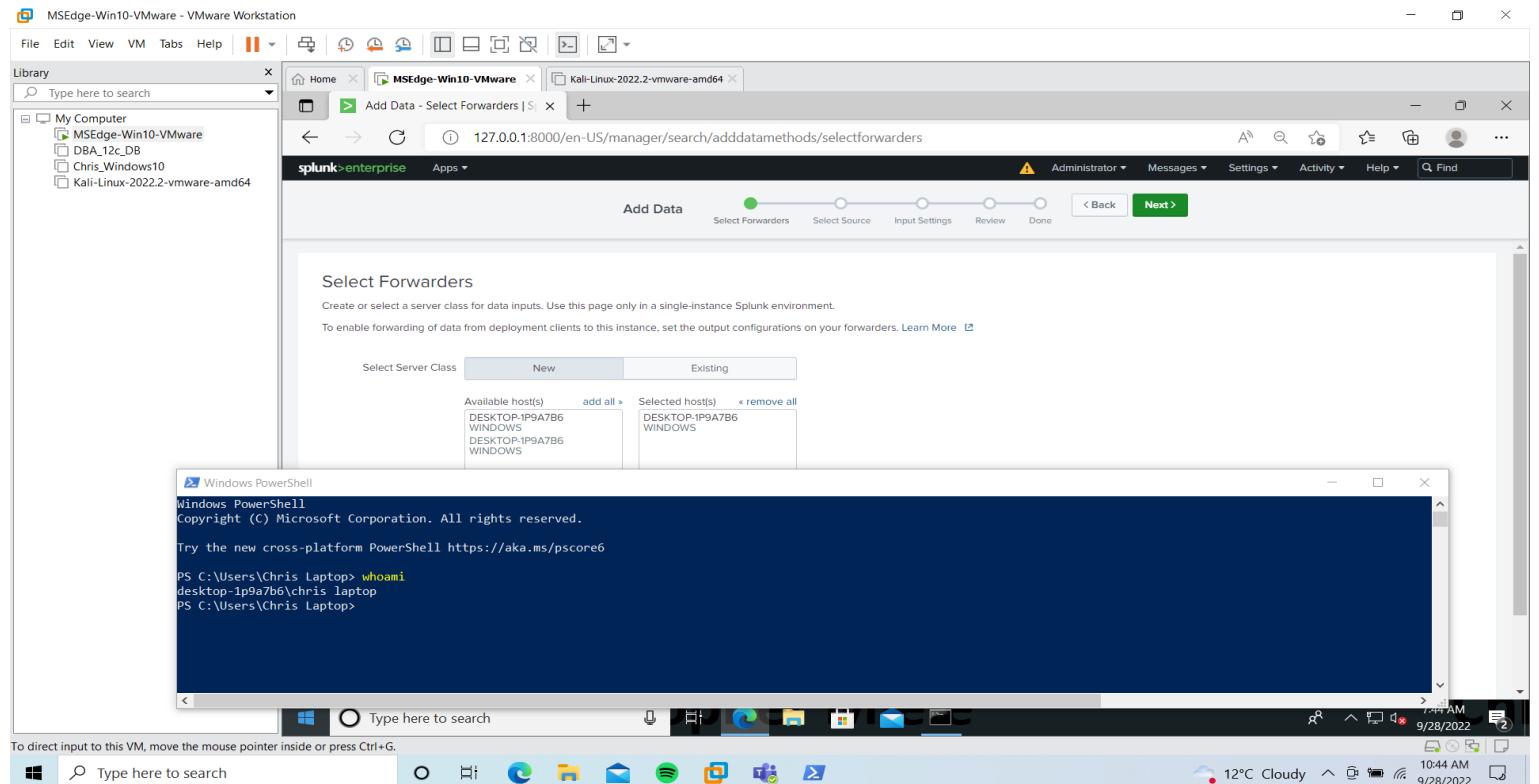


Figure 53:Add all Local Event Logs. Apps, Security, Setup, etc(Event Logs).

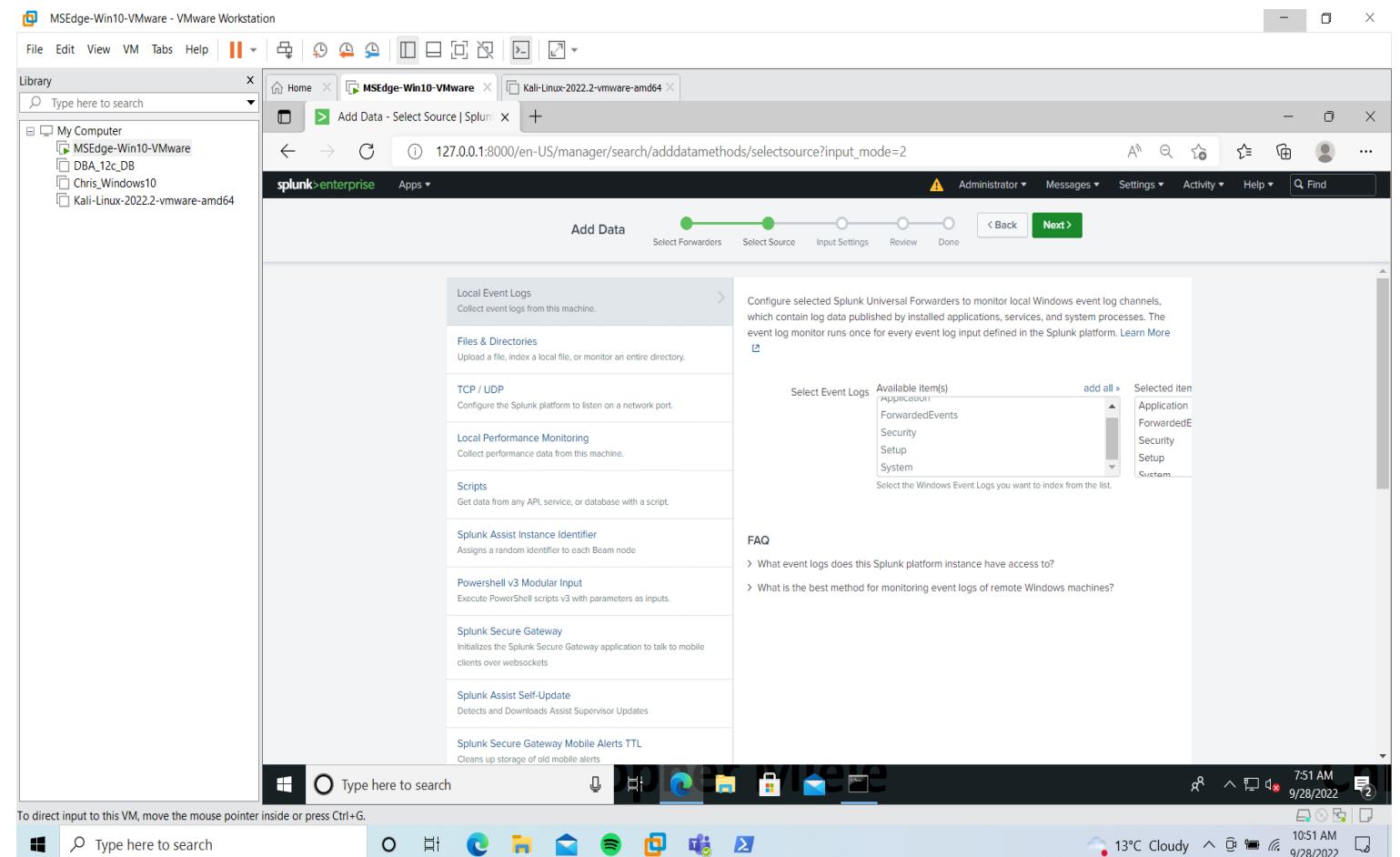
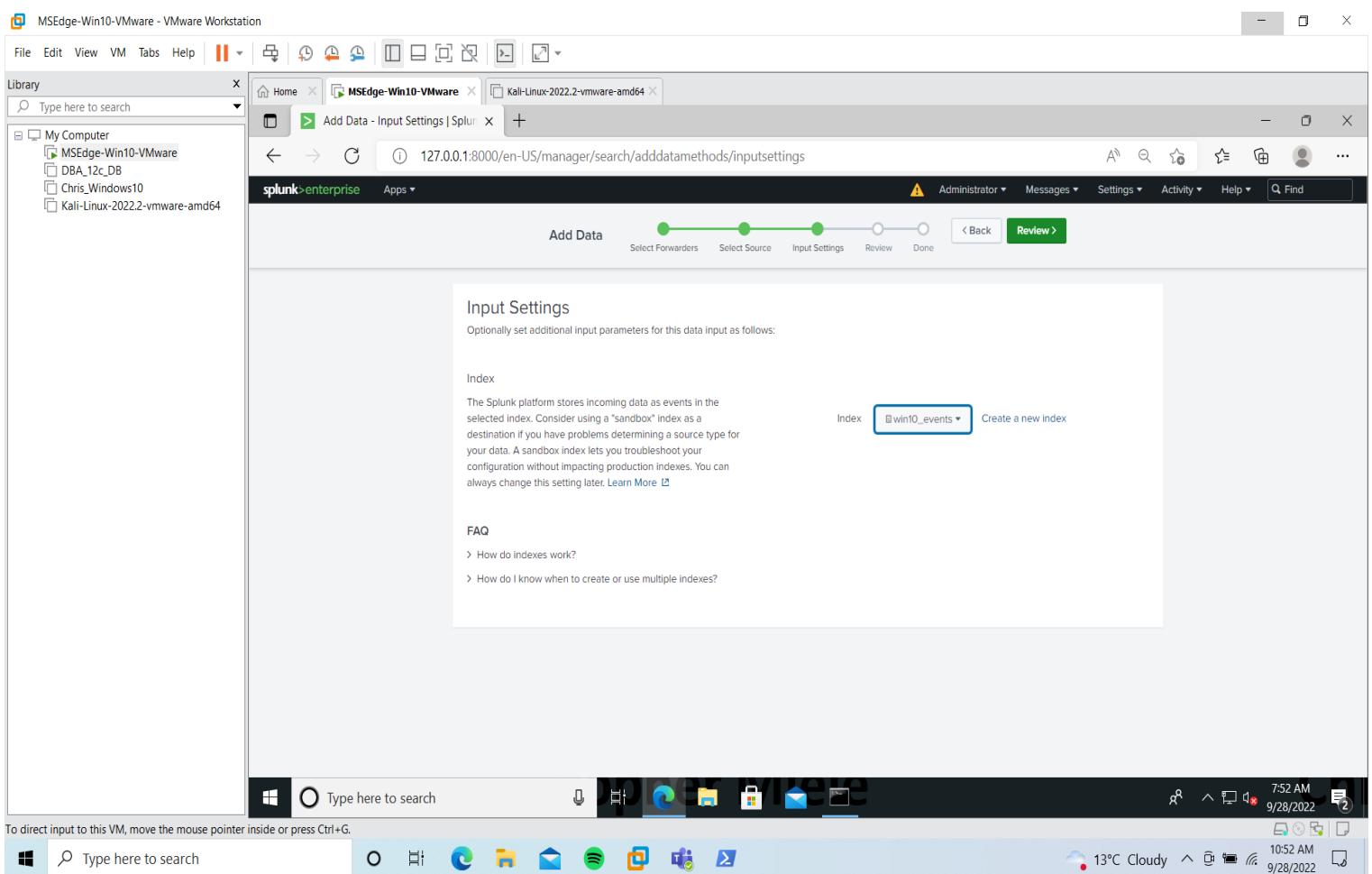


Figure 54:Choose win10_events Index(Stores Windows Event Logs) -> Review -> Search.



**Figure 55: source="WinEventLog:\"" index="win10_events"
source="WinEventLog:Application" EventCode="3908"**

**Explain: Search Windows Event Logs The Source is Application, The Event Code is 3908.
This Search will confirm that the powershell event that I created is the same event in
universal forwarder**

The screenshot shows the Splunk 9.0.1 interface with the following details:

- Search Bar:** The search bar contains the query: `source="WinEventLog:\"" index="win10_events" source="WinEventLog:Application" EventCode="3908"`.
- Results Summary:** It shows "1 event [before 9/29/22 8:03:55.000 PM] No Event Sampling".
- Event Details:** A single event is listed in the table:

	i	Time	Event
>	9/28/22 5:56:55.000 AM	09/28/2022 08:56:55 AM	LogName=Application EventCode=3908 EventType=4 ComputerName=DESKTOP-1P9A7B6 SourceName=Chris Miele Type=Information RecordNumber=10155 Keywords=Classic TaskCategory=1 OpCode=Info Message=Lab 3 Collapse EventCode = 3908 Type = Information host = DESKTOP-1P9A7B6 source = WinEventLog:Application
- Selected Fields:** The table includes fields like `# EventCode 1`, `a host 1`, `a source 1`, and `a Type 1`.
- Interesting Fields:** The table includes fields like `a ComputerName 1`, `# EventType 1`, `a index 1`, `a Keywords 1`, `# linecount 1`, `a LogName 1`, `a Message 1`, `a OpCode 1`, and `a punct 1`.
- System Status:** The bottom status bar shows "8:04 PM 9/29/2022" and "8°C Clear 11:04 PM 9/29/2022".

Lab 4

**Figure 56: source="WinEventLog:/*" index="win10_events" Type=Information
SourceName="Microsoft-Windows-WindowsUpdateClient" status=installed package=***

Explain: Find Updates that are downloaded on Host OS Type information, Source Windows Update Client, Status Installed Updates the Package = *(Wild card) search for different types of updates.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="WinEventLog:/*" index="win10_events" Type=Information SourceName="Microsoft-Windows-WindowsUpdateClient" status=installed package=*`. The results section displays 72 events from September 29, 2022, at 11:57:37 PM. The first few events are listed in the table below:

Time	Event
9/29/2022 11:57:37 PM 8:57:37000 PM	09/29/2022 11:57:37 PM LogName=System EventCode=19 EventType=4 ComputerName=DESKTOP-1P9A7B6 User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-WindowsUpdateClient Type=Information RecordNumber=13115 Keywords=Installation, Success TaskCategory=Windows Update Agent OpCode=Installation Message=Installation Successful: Windows successfully installed the following update: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.375.1243.0)

Reference

- [1] Cyberwox, D. (2021, June 16). *Cybersecurity Detection Lab: Forwarding windows event logs to Splunk using universal forwarder*. YouTube. Retrieved September 30, 2022, from https://www.youtube.com/watch?v=yP_PFRy-pdA
- [2] Satti, M. (2022, July 26). *Splunk -boss of the SOC v1 (walkthrough)*. Medium. Retrieved September 30, 2022, from <https://systemweakness.com/splunk-boss-of-the-soc-v1-walkthrough-a9550cde93f5>