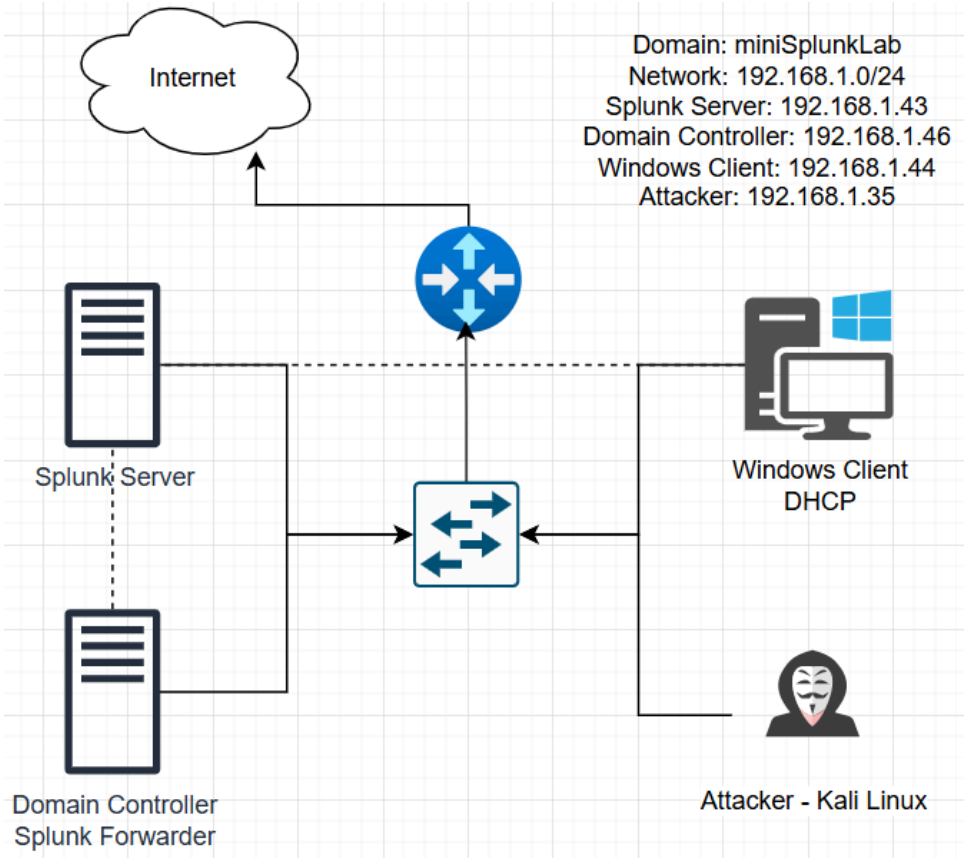
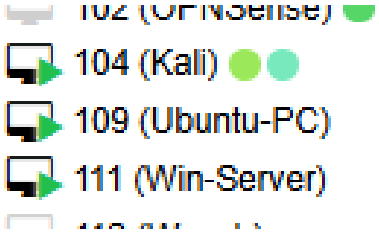
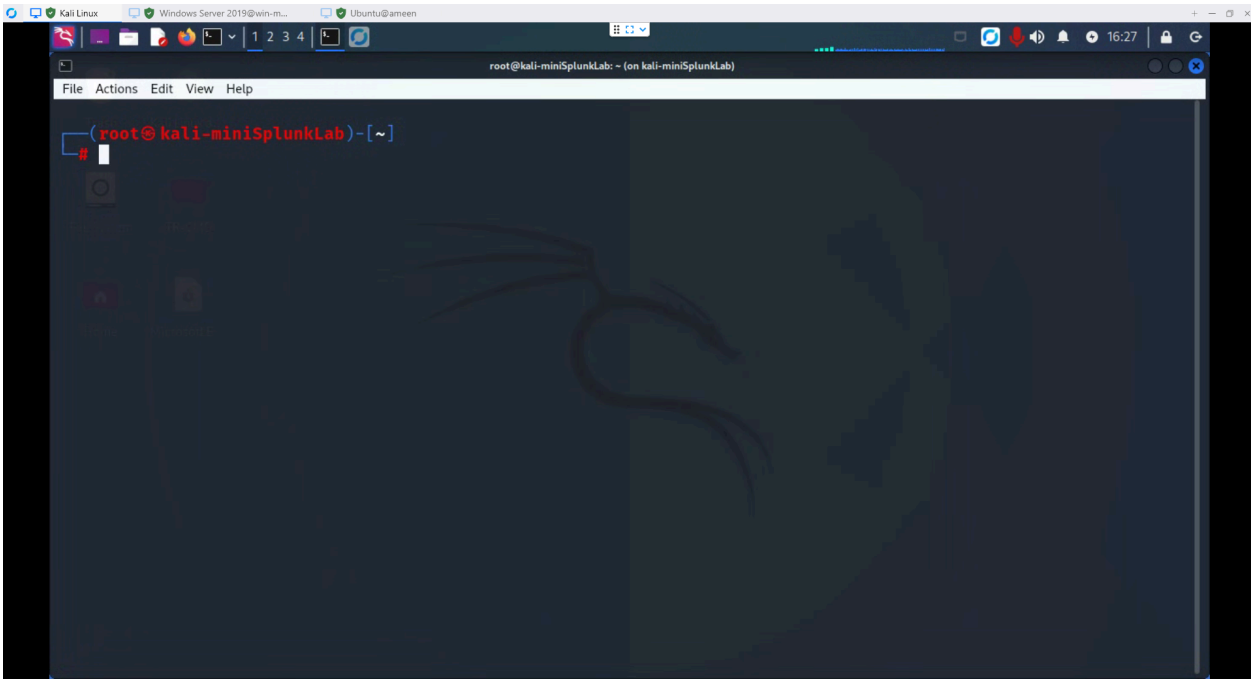
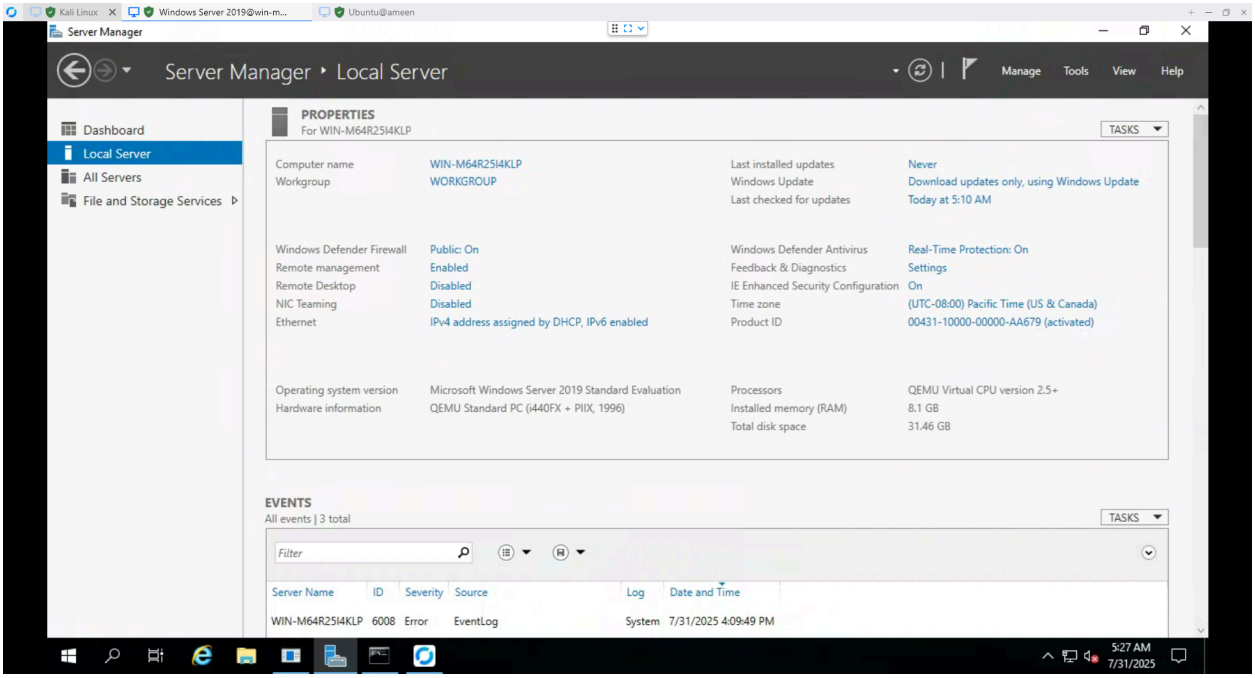
Screenshots

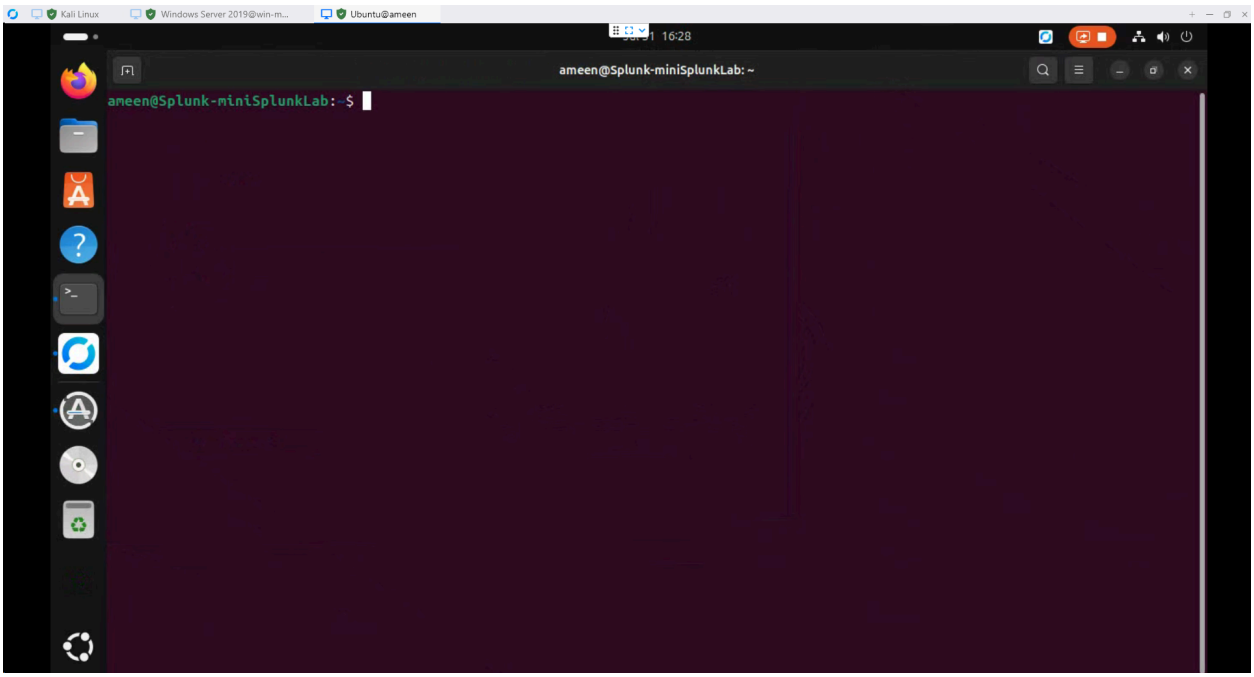


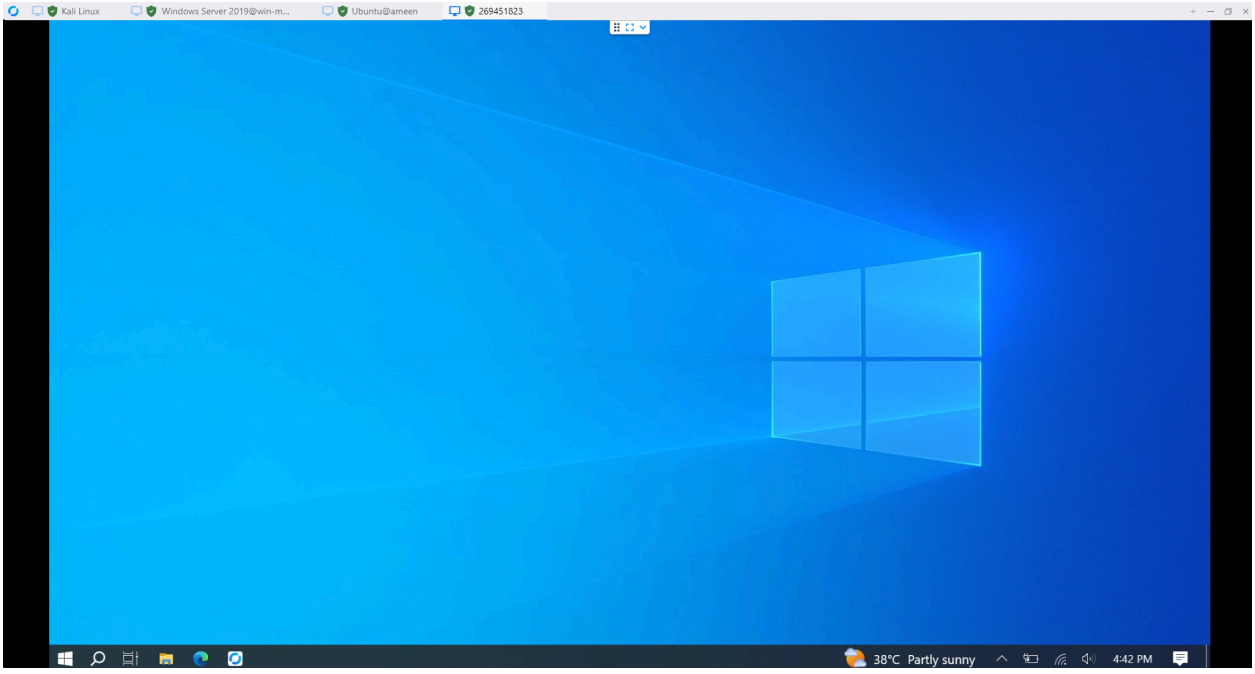
Setting up VMs on ProxmoxOS



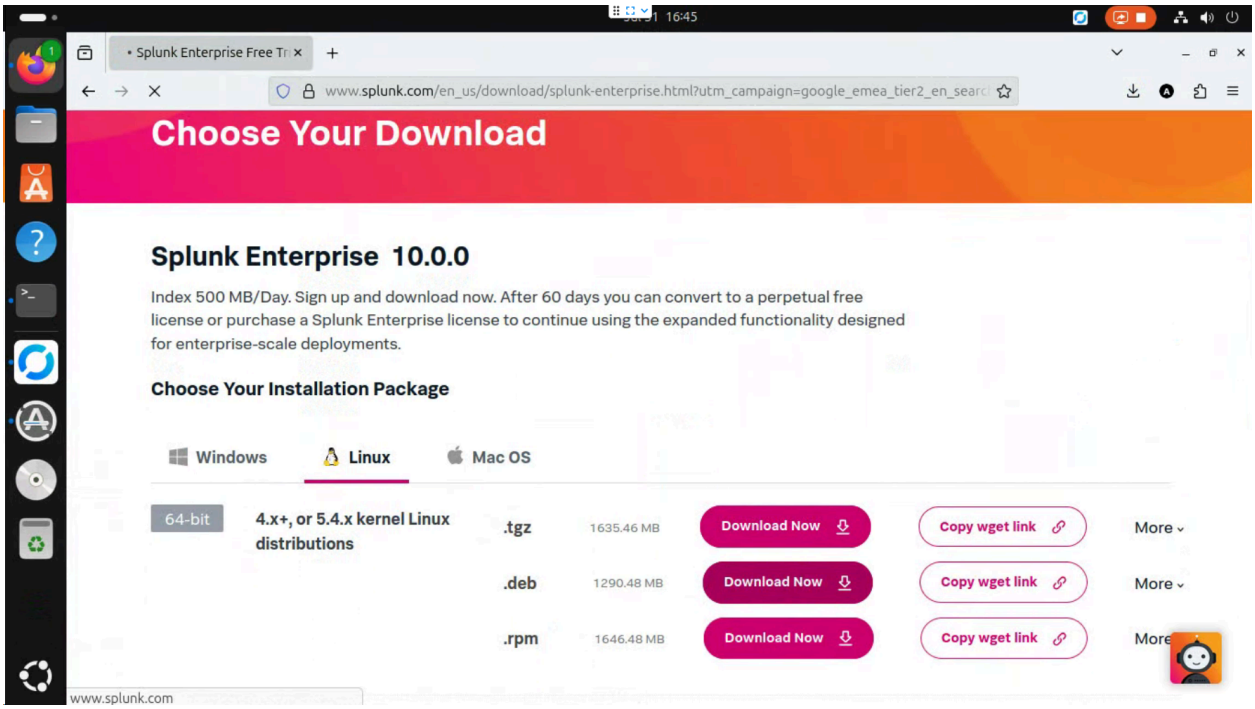

Kali Linux
Windows Server 2019@win-m...
Ubuntu@ameen
16:27
root@kali-miniSplunkLab: ~ (on kali-miniSplunkLab)
File Actions Edit View Help
(root㉿kali-miniSplunkLab)-[~]
#

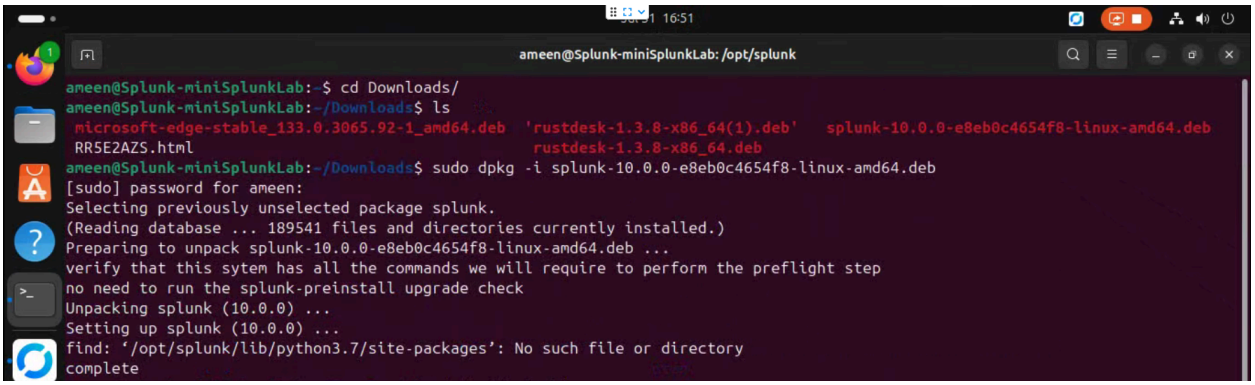

Server Manager
Server Manager • Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For WIN-M64R25I4KLP
TASKS
Computer name WIN-M64R25I4KLP
Workgroup WORKGROUP
Last installed updates Never
Windows Update Download updates only, using Windows Update
Last checked for updates Today at 5:10 AM
Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID 00431-10000-00000-AA679 (activated)
Operating system version Microsoft Windows Server 2019 Standard Evaluation
Hardware information QEMU Standard PC (i440FX + PIIX, 1996)
Processors QEMU Virtual CPU version 2.5+
Installed memory (RAM) 8.1 GB
Total disk space 31.46 GB
EVENTS
All events | 3 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
WIN-M64R25I4KLP 6008 Error EventLog System 7/31/2025 4:09:49 PM
5:27 AM
7/31/2025

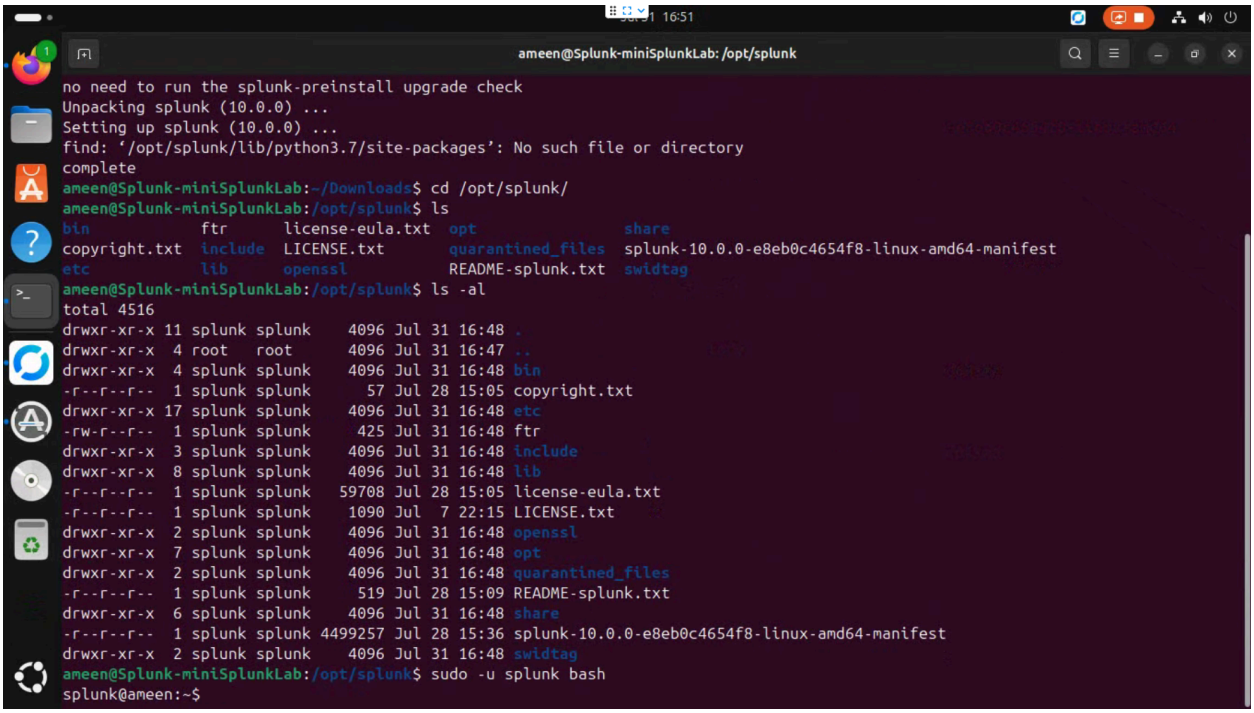




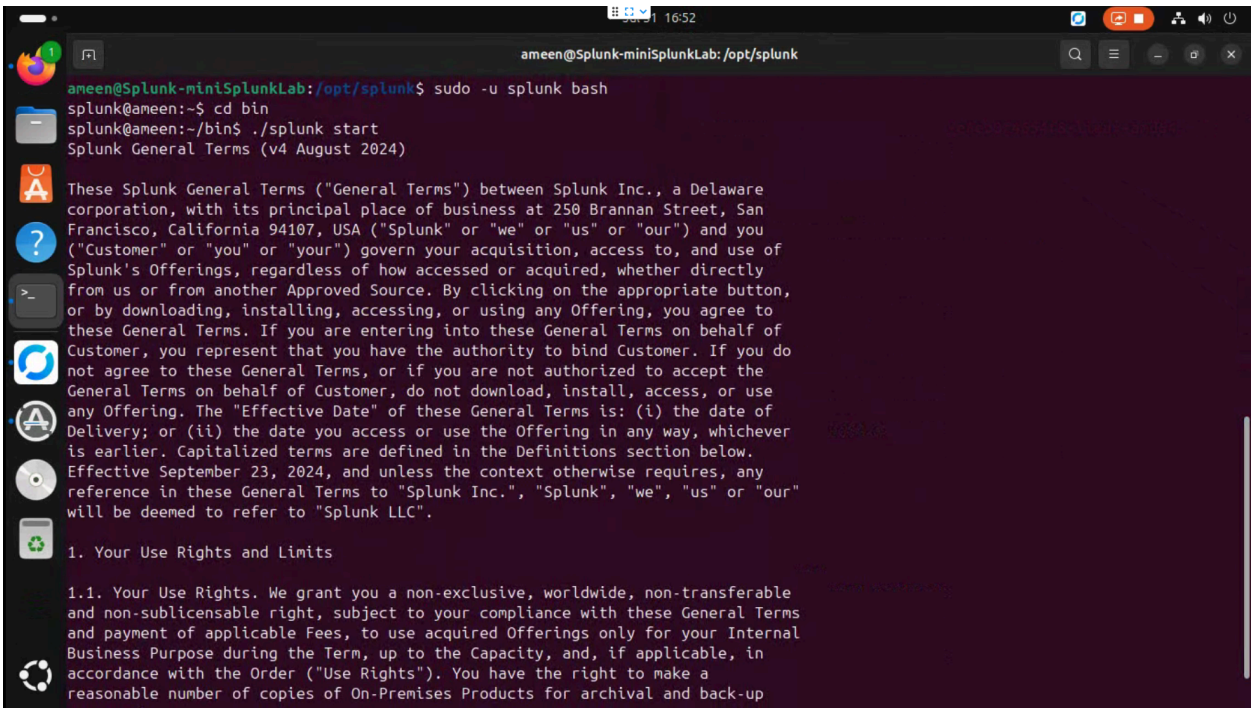
Downloading Splunk on Ubuntu Machine


16:45
• Splunk Enterprise Free Tr
www.splunk.com/en_us/download/splunk-enterprise.html?utm_campaign=google_emea_tier2_en_sear
Choose Your Download
Splunk Enterprise 10.0.0
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.
Choose Your Installation Package
Windows
Linux
Mac OS
64-bit
4.x+, or 5.4.x kernel Linux distributions
.tgz
1635.46 MB
Download Now
Copy wget link
More
.deb
1290.48 MB
Download Now
Copy wget link
More
.rpm
1646.48 MB
Download Now
Copy wget link
More
www.splunk.com

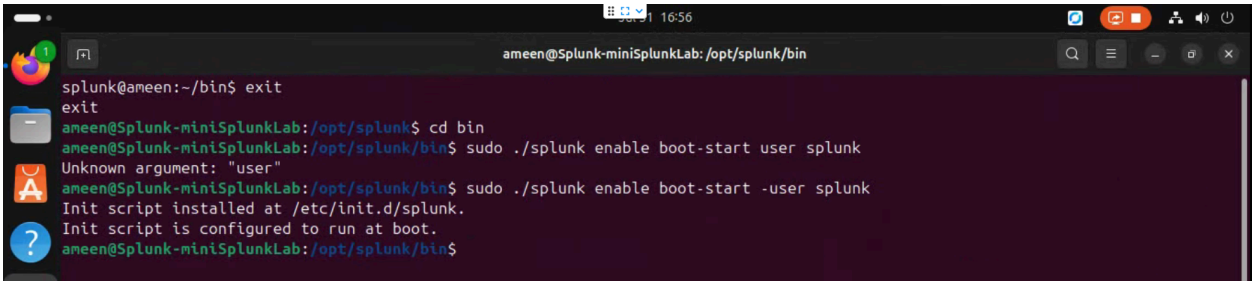

16:51
ameen@Splunk-miniSplunkLab: /opt/splunk
ameen@Splunk-miniSplunkLab:~$ cd Downloads/
ameen@Splunk-miniSplunkLab:~/Downloads$ ls
microsoft-edge-stable_133.0.3065.92-1_amd64.deb 'rustdesk-1.3.8-x86_64(1).deb' splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
RR5E2AZS.html rustdesk-1.3.8-x86_64.deb
ameen@Splunk-miniSplunkLab:~/Downloads$ sudo dpkg -i splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
[sudo] password for ameen:
Selecting previously unselected package splunk.
(Reading database ... 189541 files and directories currently installed.)
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.0) ...
Setting up splunk (10.0.0) ...
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory
complete



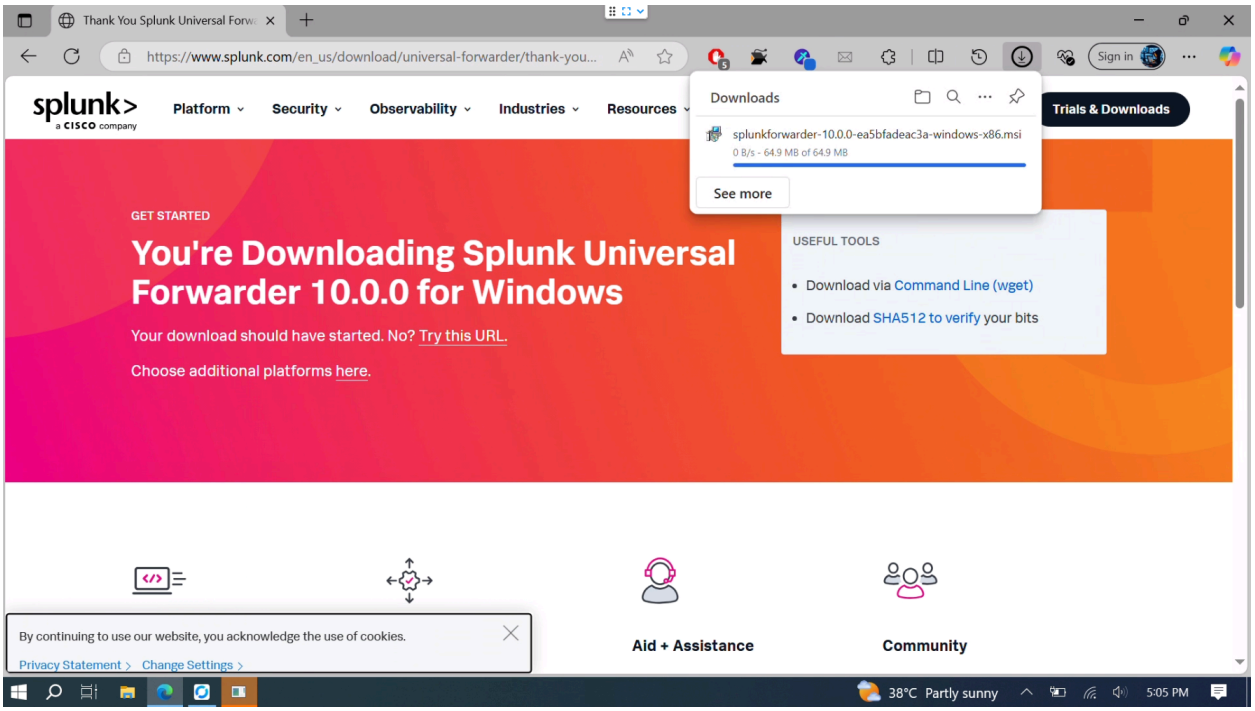
Completing Install

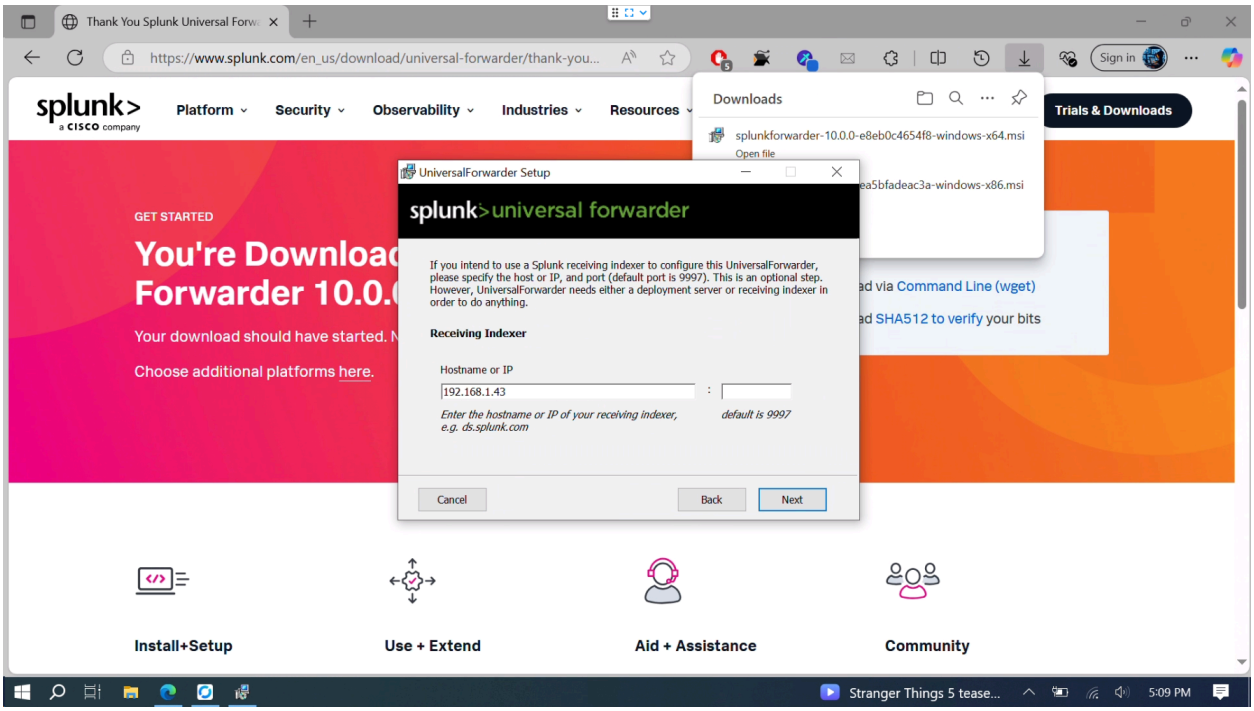


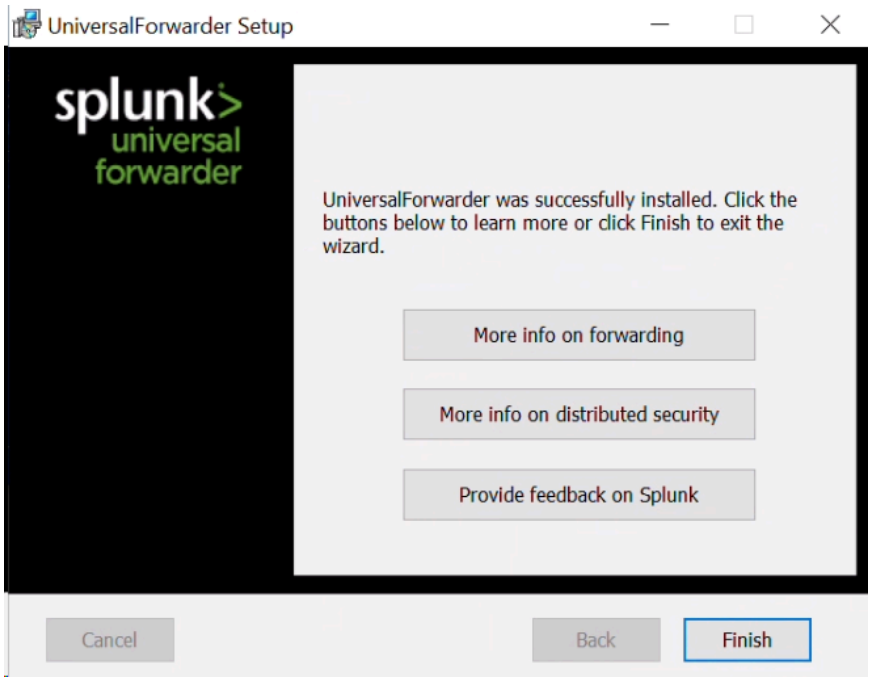
Enabling Auto-start at Boot



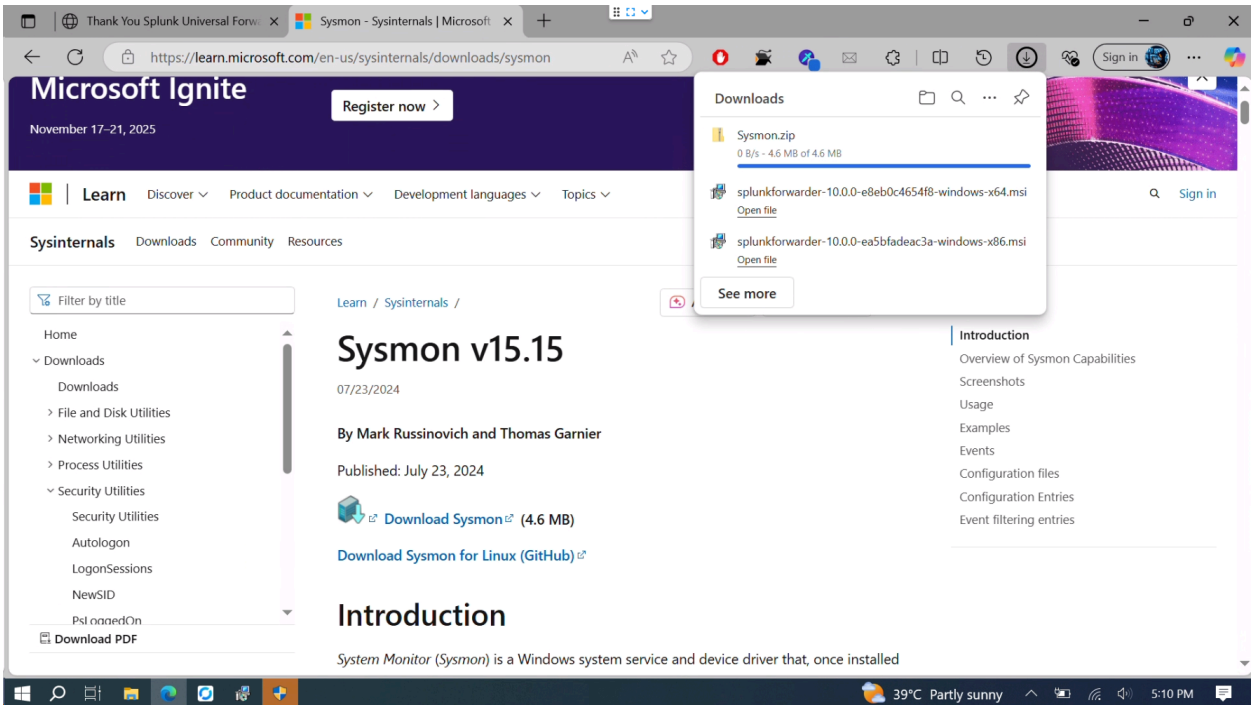
Downloading Universal Forwarder on Windows Target PC



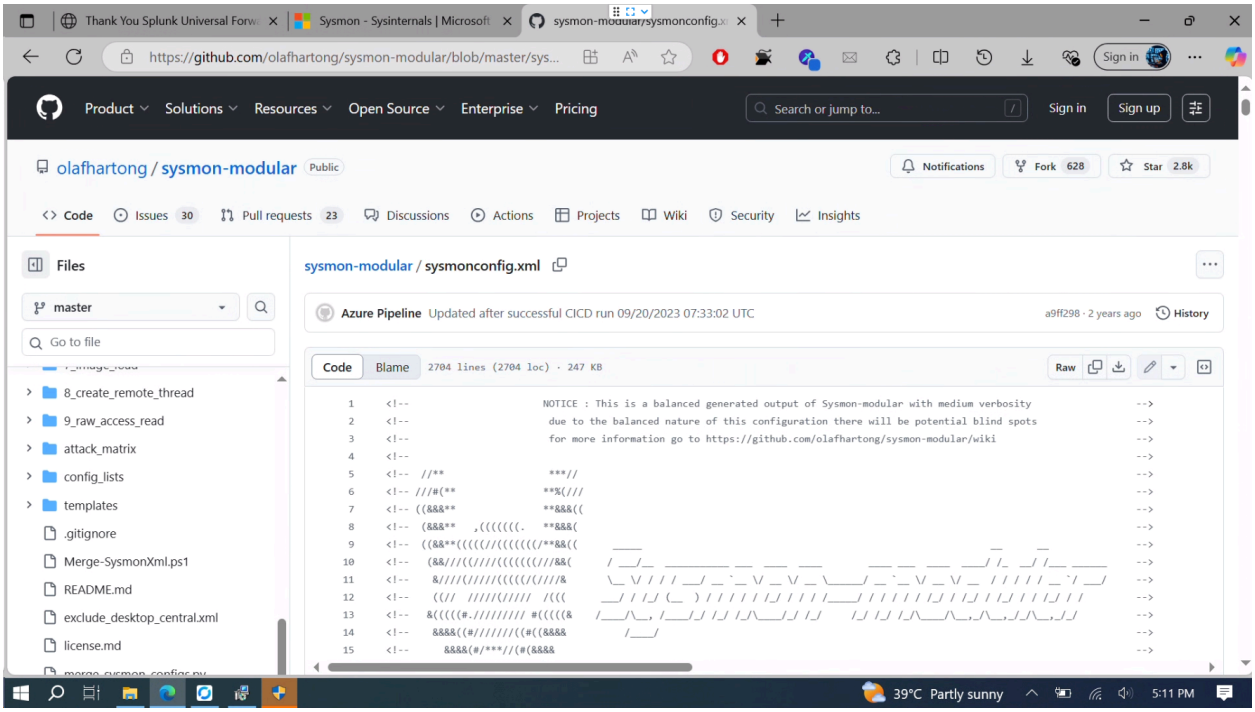




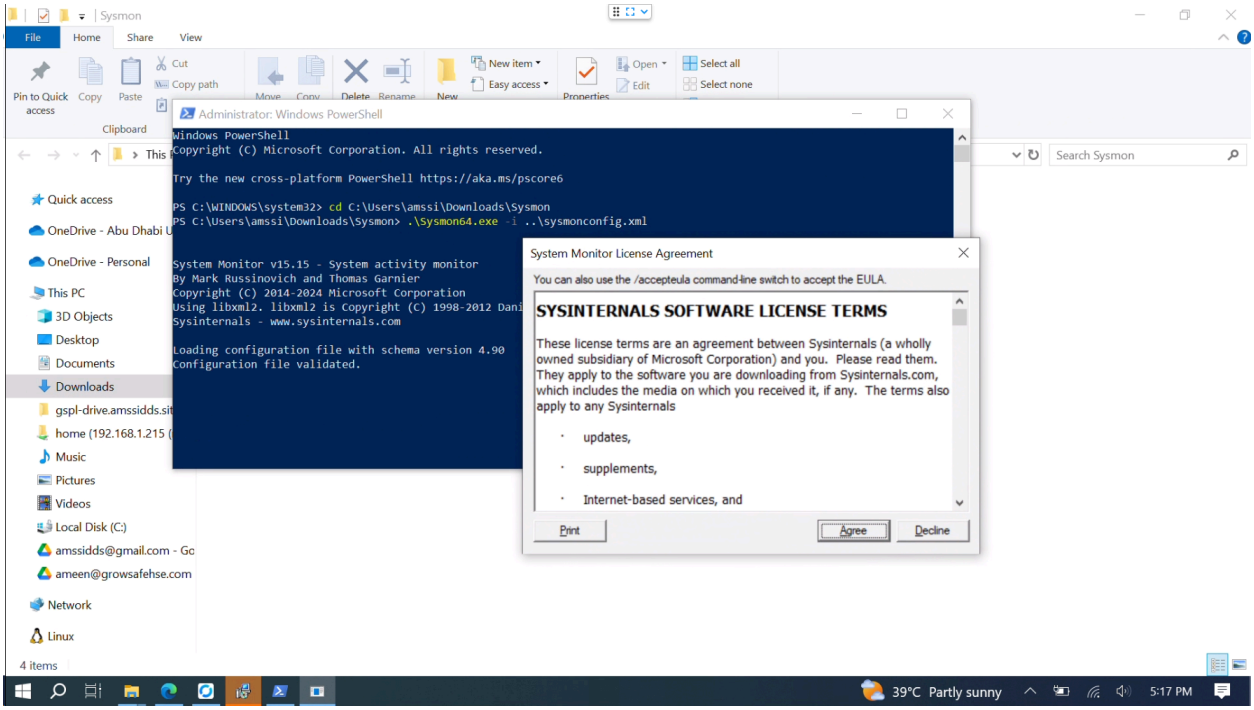
Downloading Sysmon on Target Windows Machine

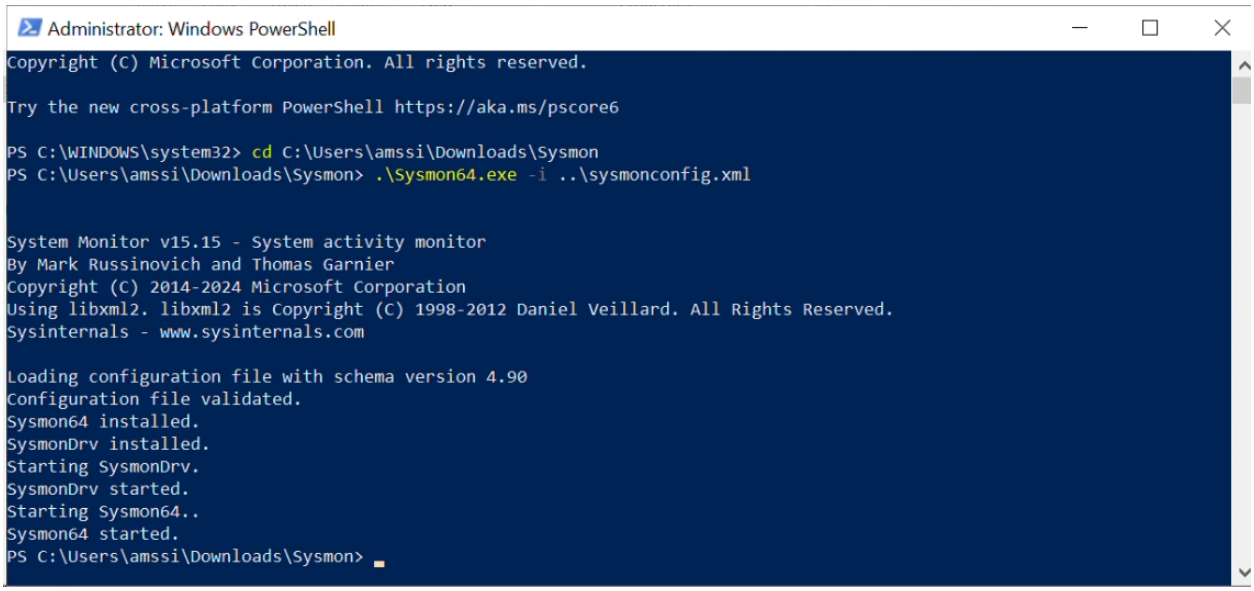


Downloading Sysmon Config by “olaf”

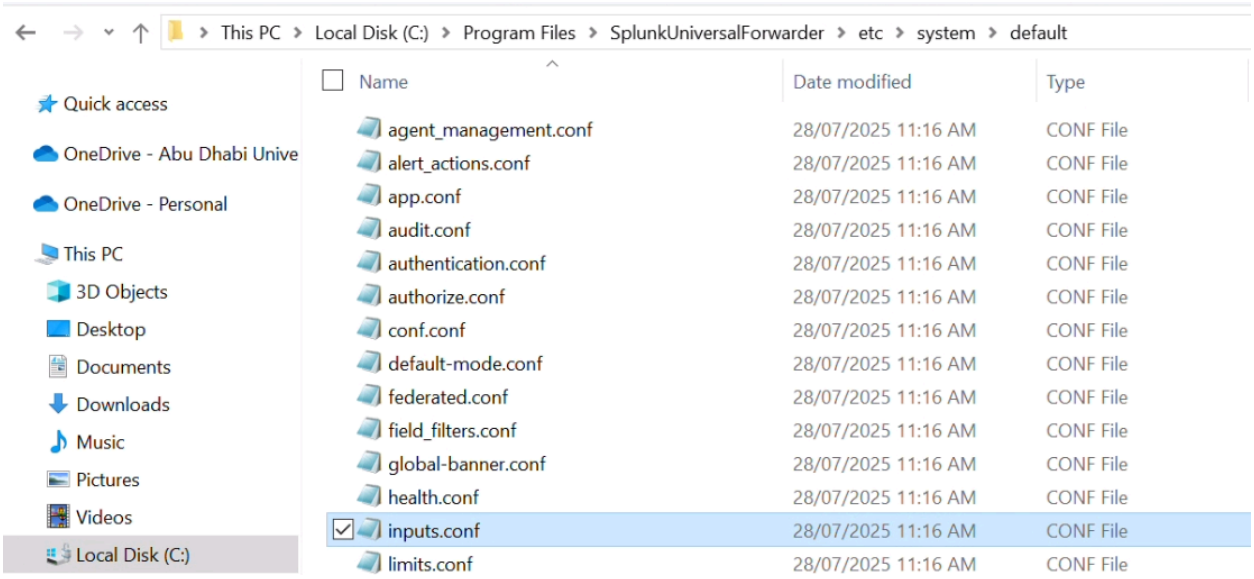


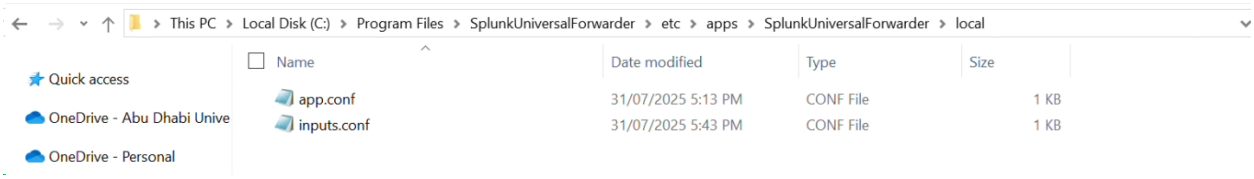
Configuring Sysmon with sysmonconfig.xml downloaded





Copying Contents of input.conf and creating a new file in local directory





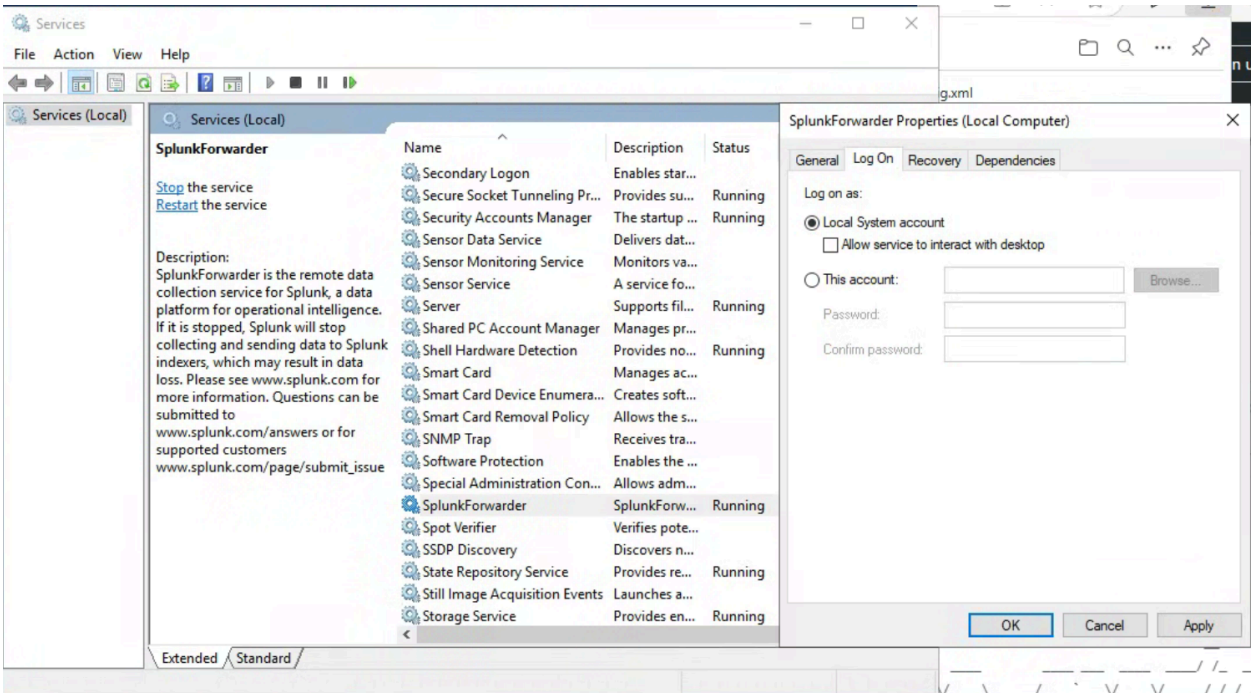
Changing the values to new values

```
[WinEventLog://Application]
index = endpoint
disabled = false

[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false
```

```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Make Sure the “endpoint” is under “index”

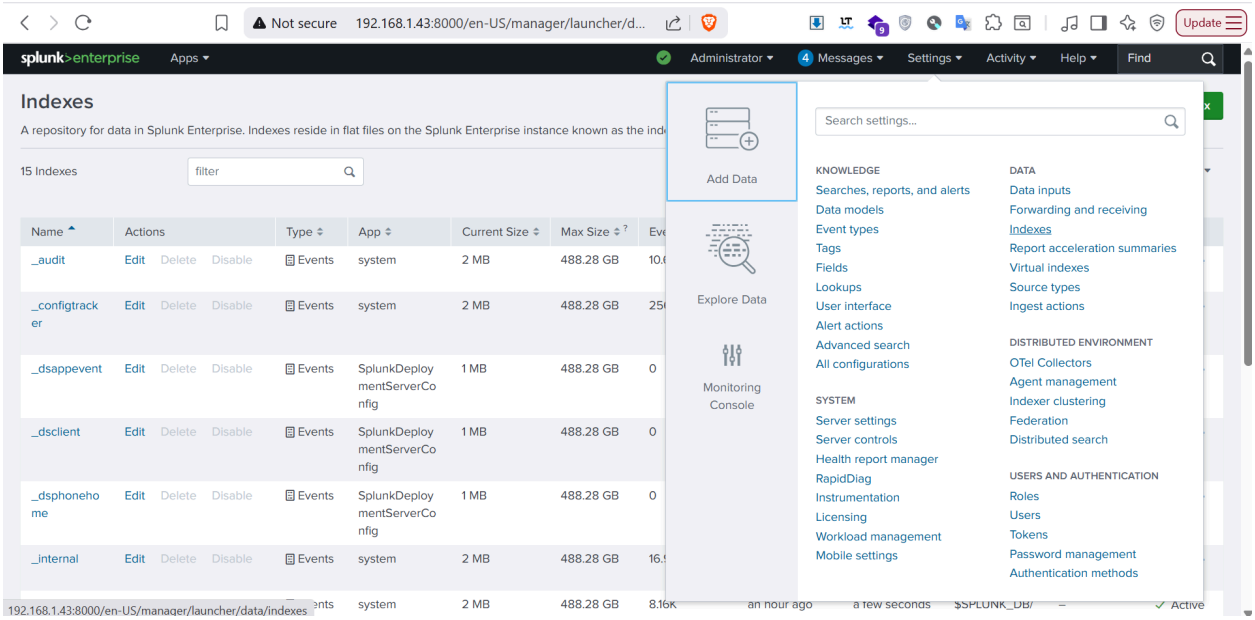
Changing logon to local for logs storing



Then Restart the service

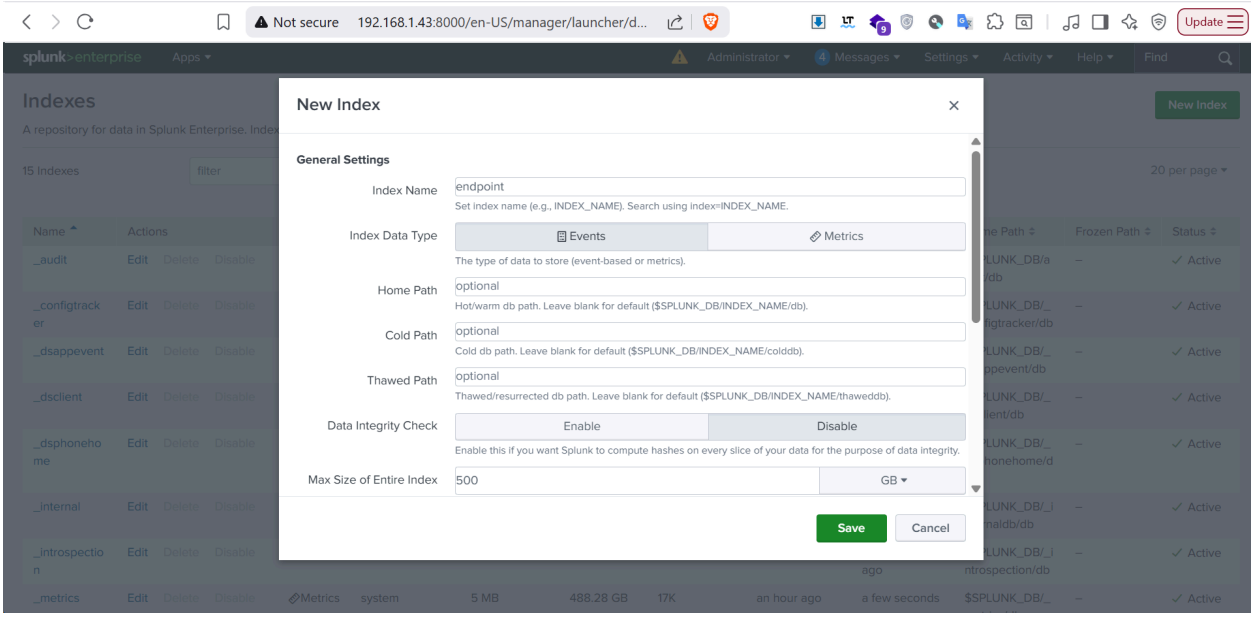
Opening Splunk Dashboard

And going to settings > indexes

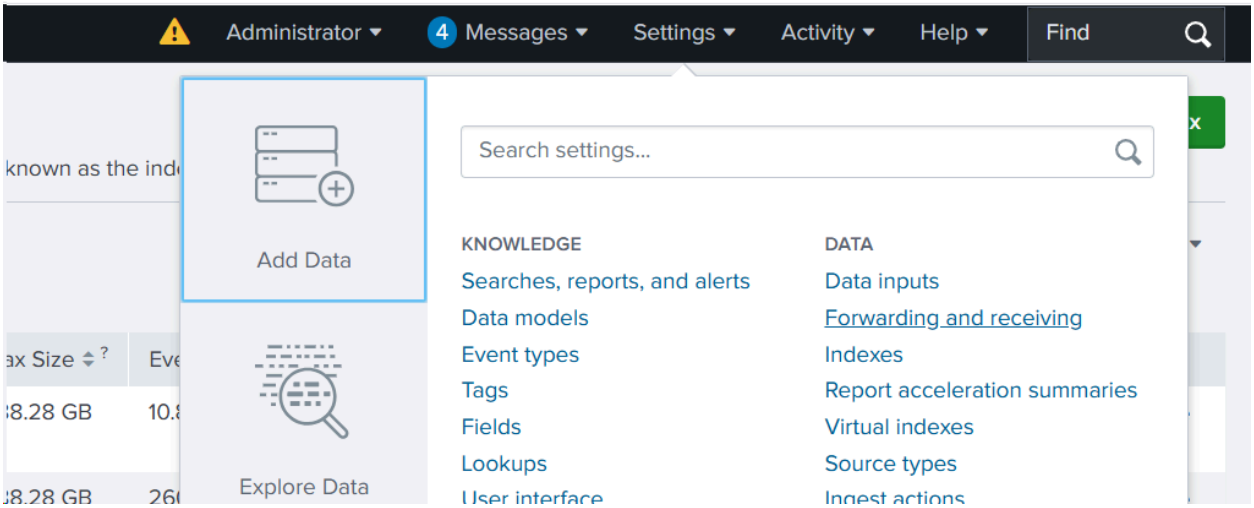


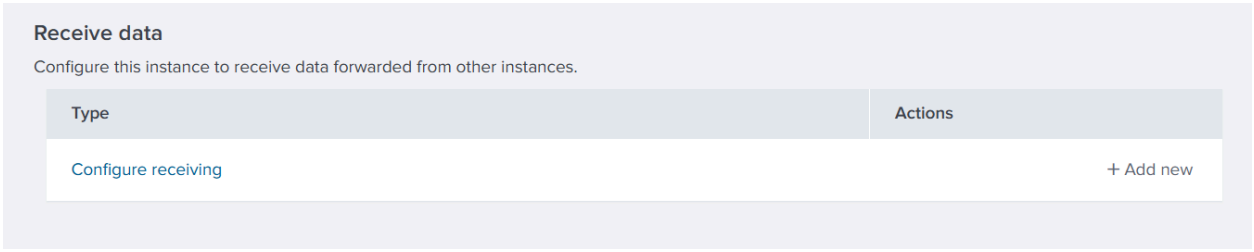
We can see all events being logged

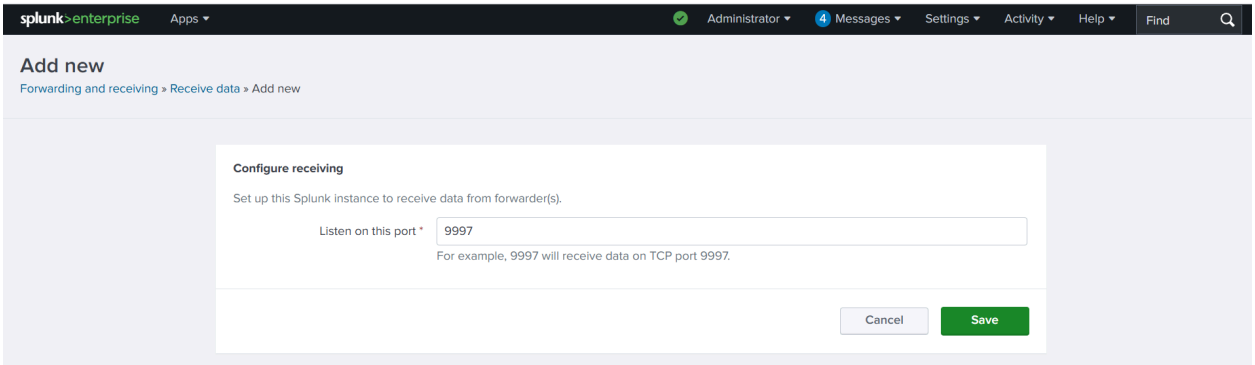
Creating a new Index as Endpoint



Configuring Receiving data on Forwarder



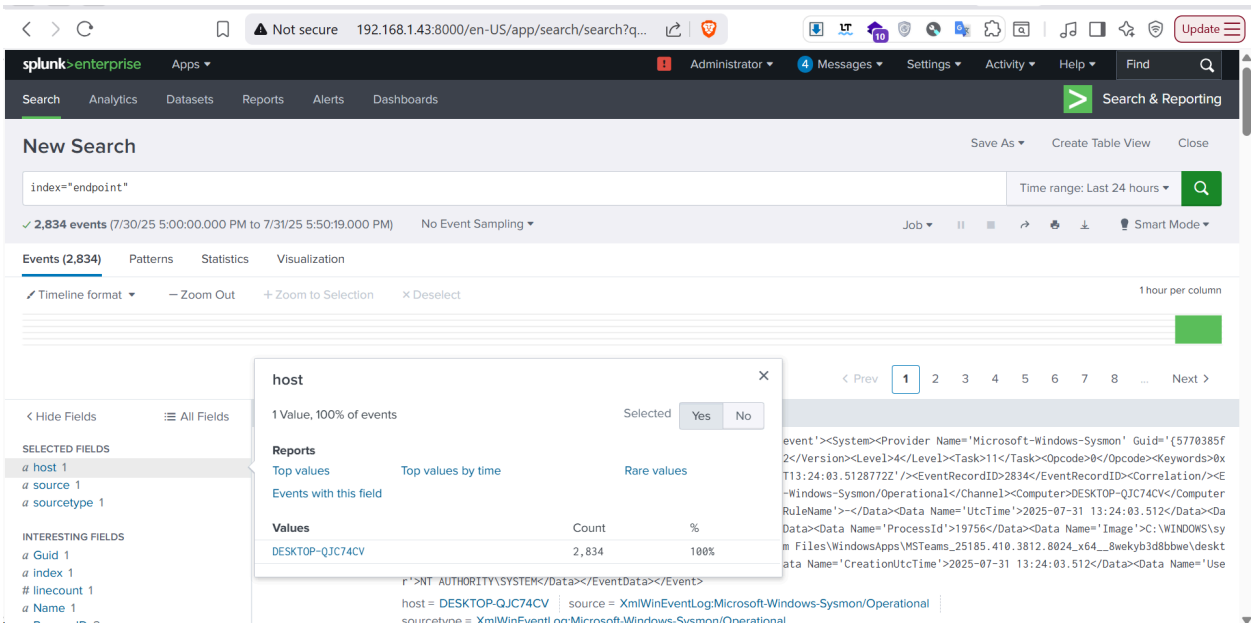




To check if the Connecter is connected

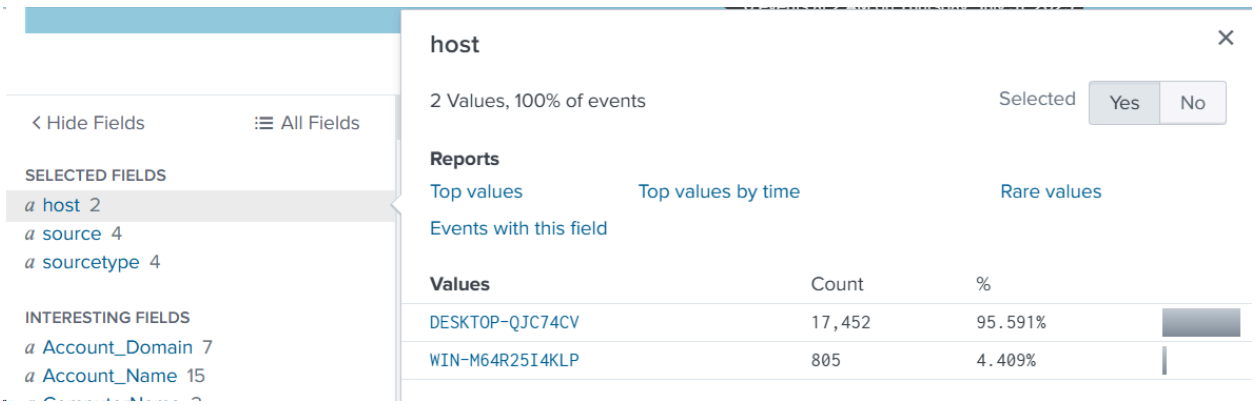
Go to Apps > Search and Reporting

In the field type `index="endpoint"`

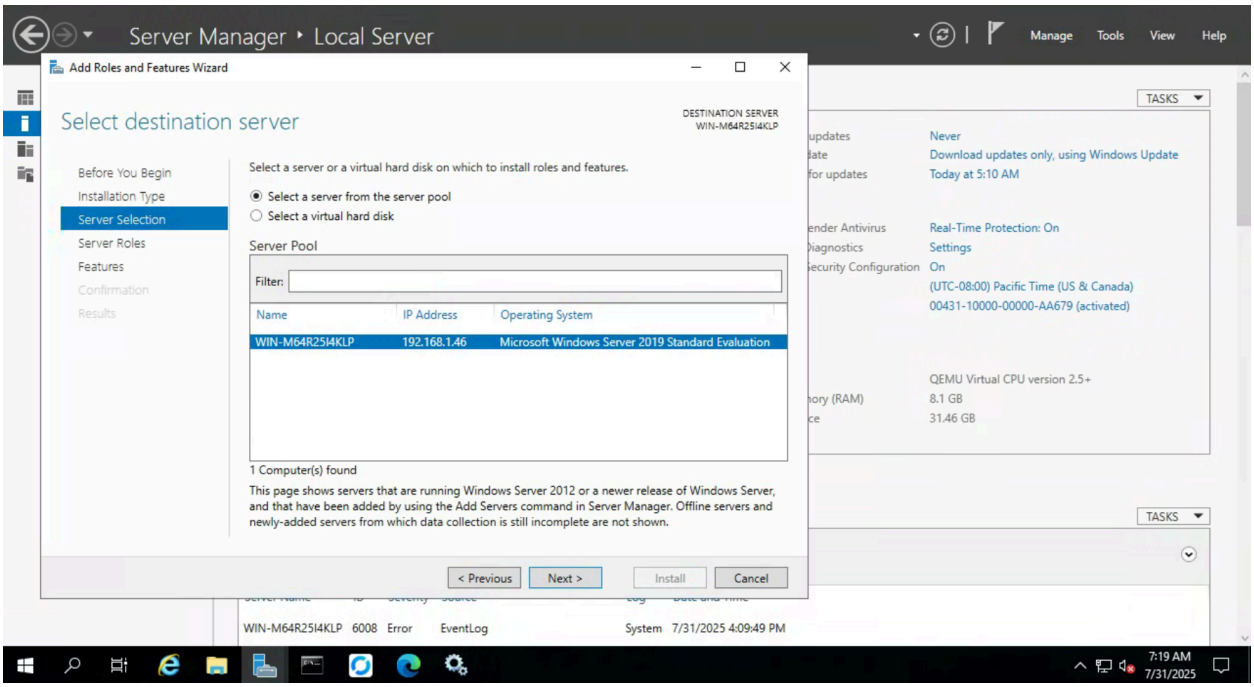


We can see host connected

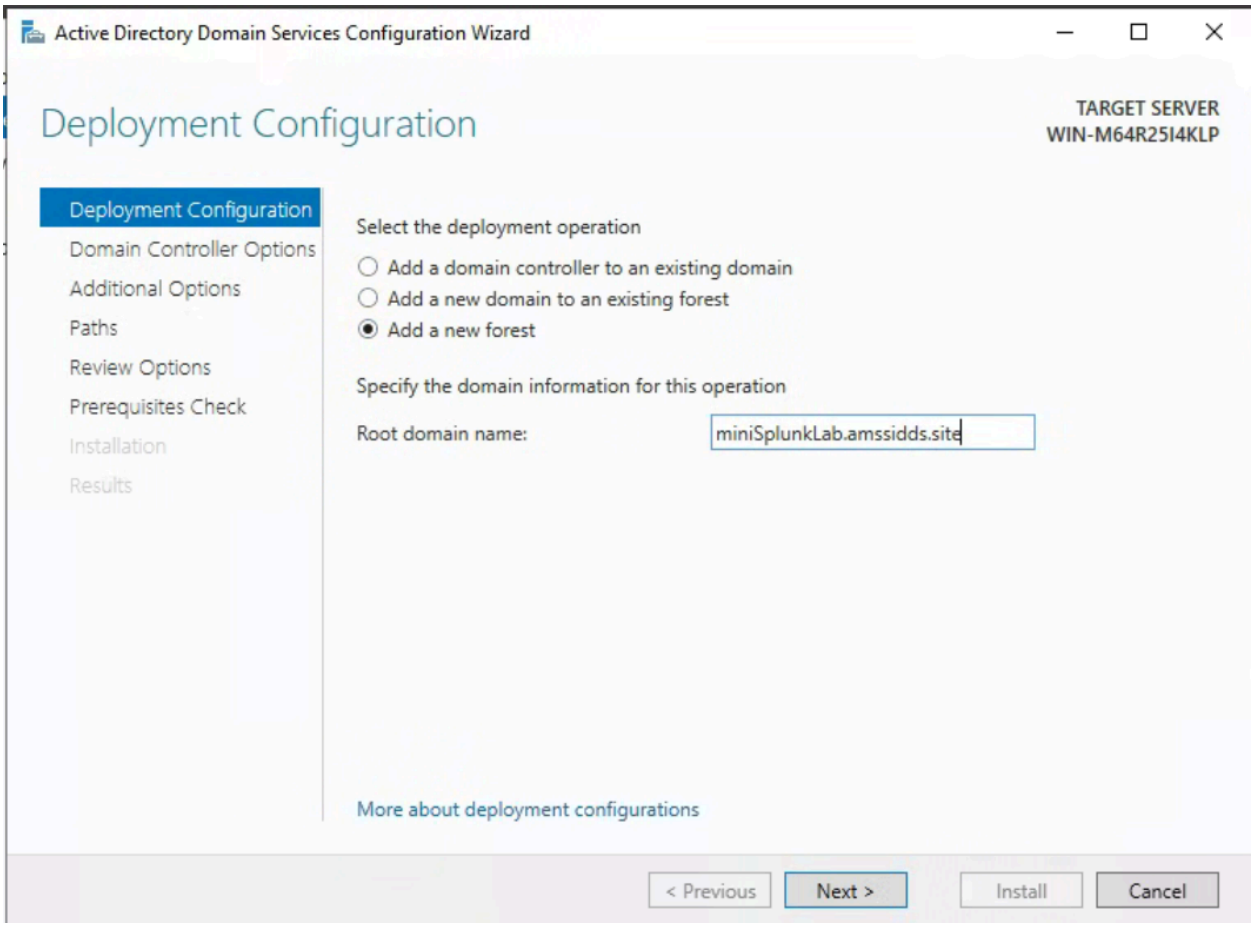
Downloading Splunk Forwarder on Active Directory



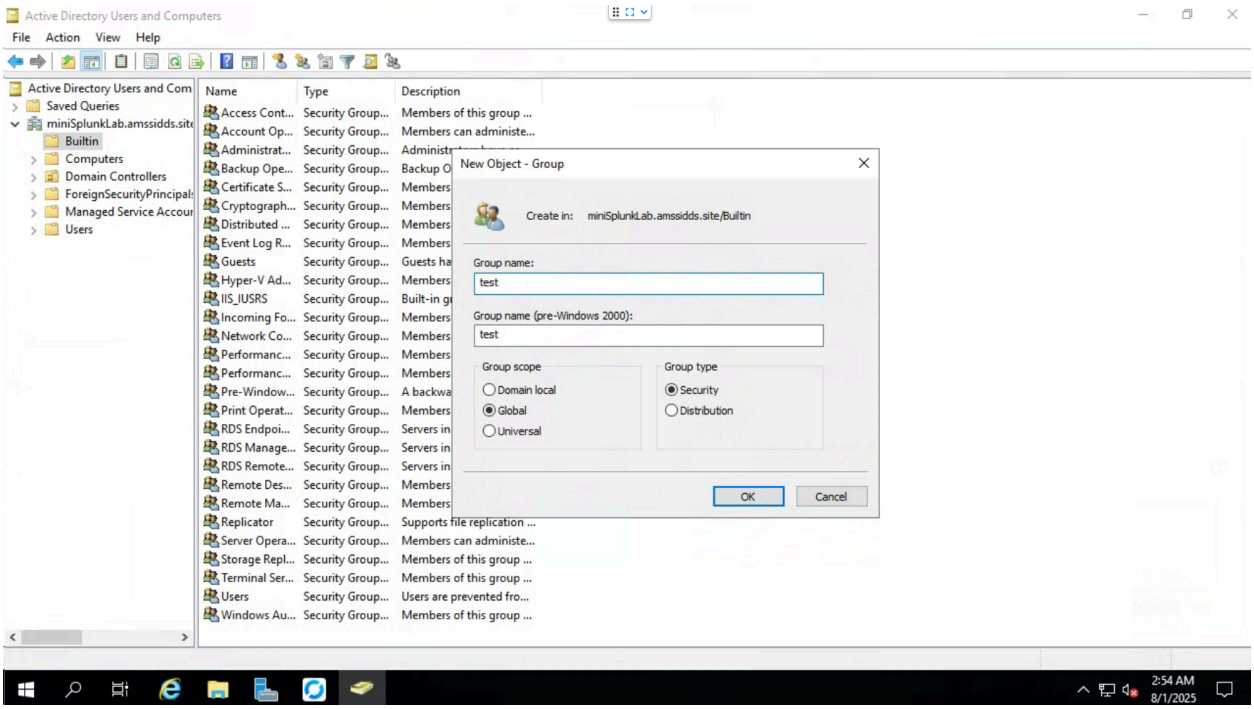
Configuring Active Directory and Promoting to DC

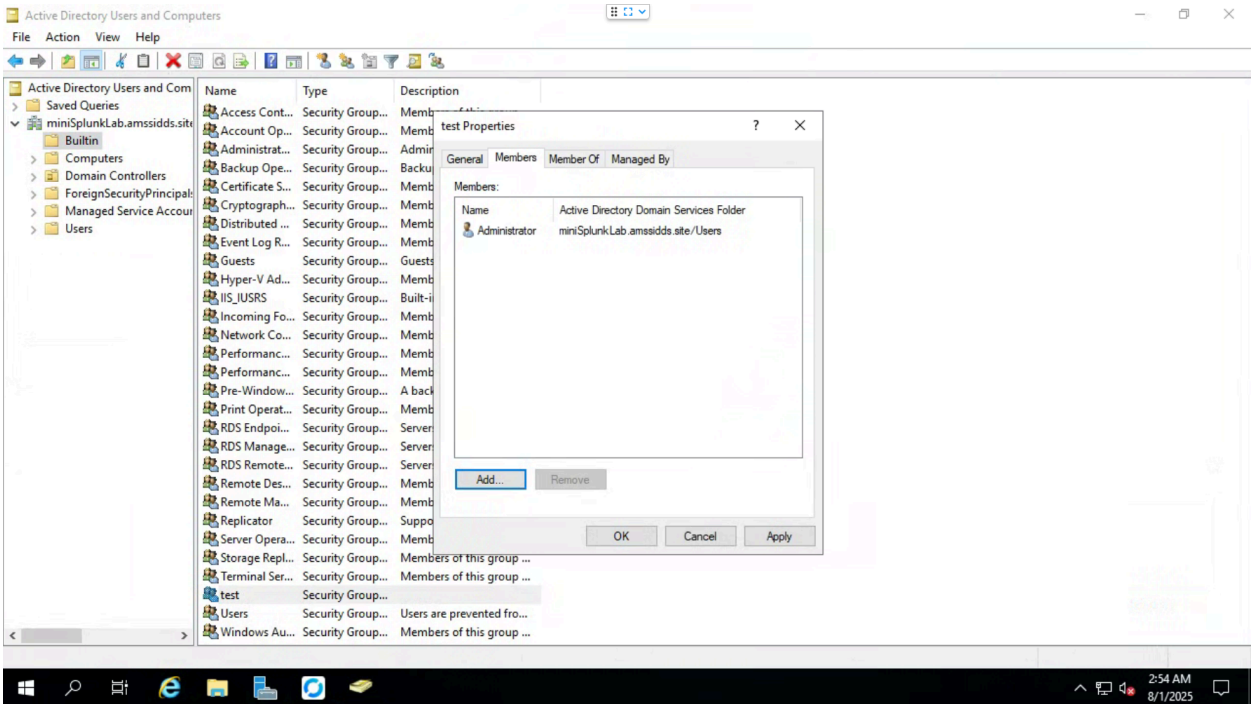


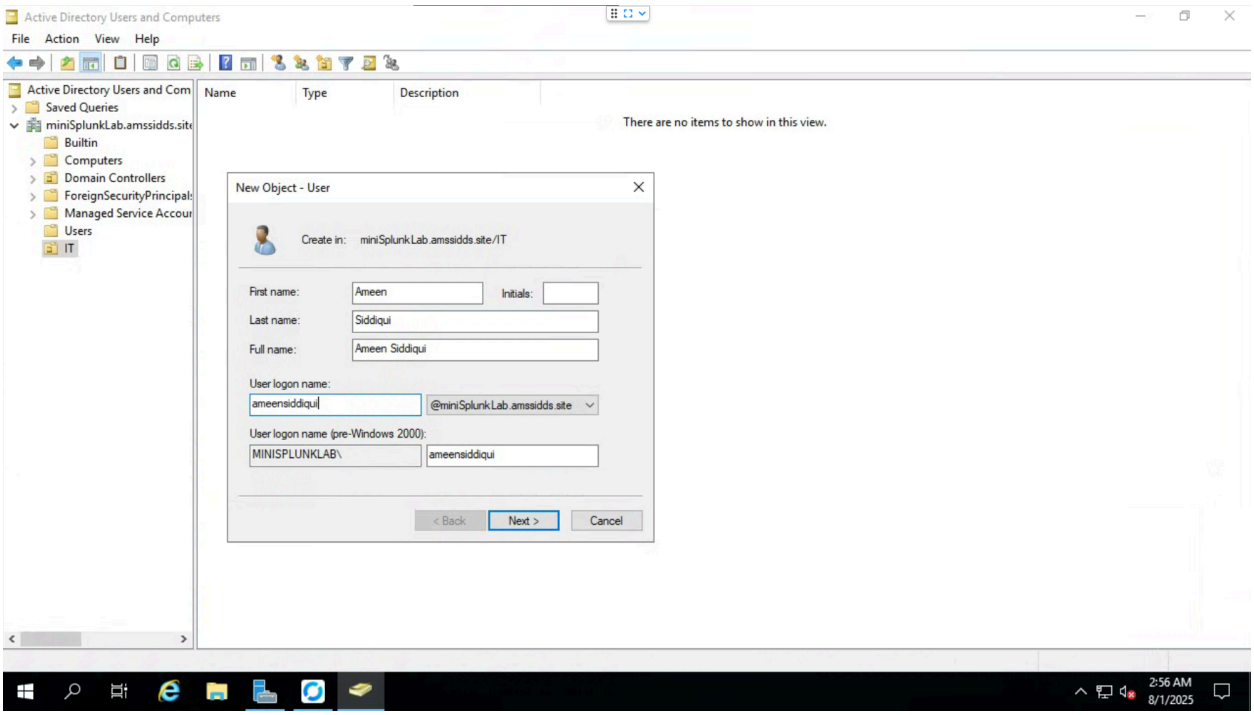
Promoting it to DC



Creating Global Test Group under Administrator and a DL group under Test Group

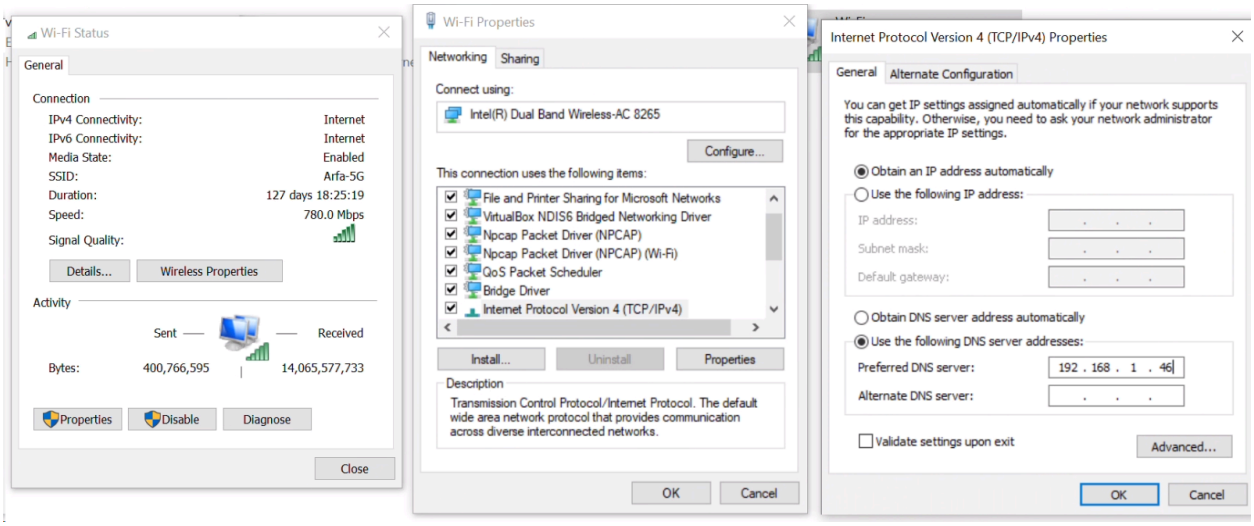

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
miniSplunkLab.amssidds.site
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Type
Description
New Object - Group
Create in: miniSplunkLab.amssidds.site/Builtin
Group name:
test
Group name (pre-Windows 2000):
test
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel
2:54 AM
8/1/2025


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
miniSplunkLab.amssidds.site
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Type
Description
test Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Administrator
miniSplunkLab.amssidds.site/Users
Add...
Remove
OK
Cancel
Apply
test
Security Group...
2:54 AM
8/1/2025

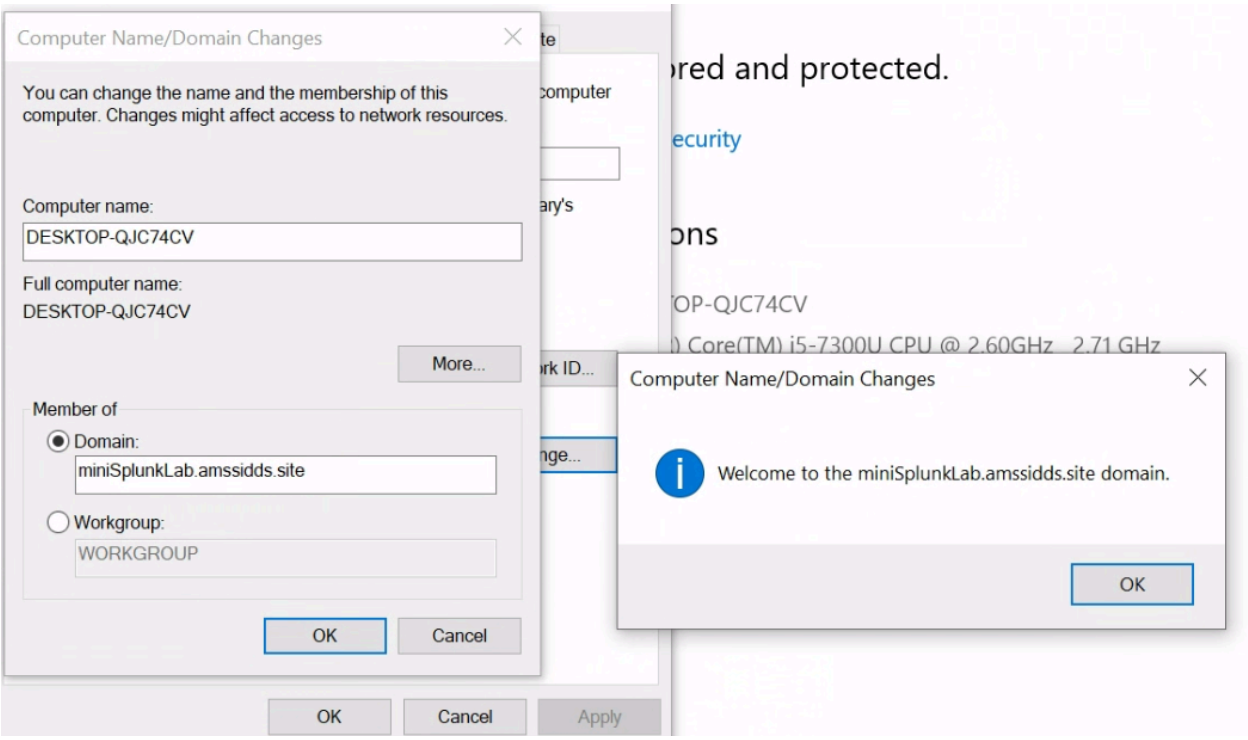


Connecting Windows Client Victim PC to the Domain Controller

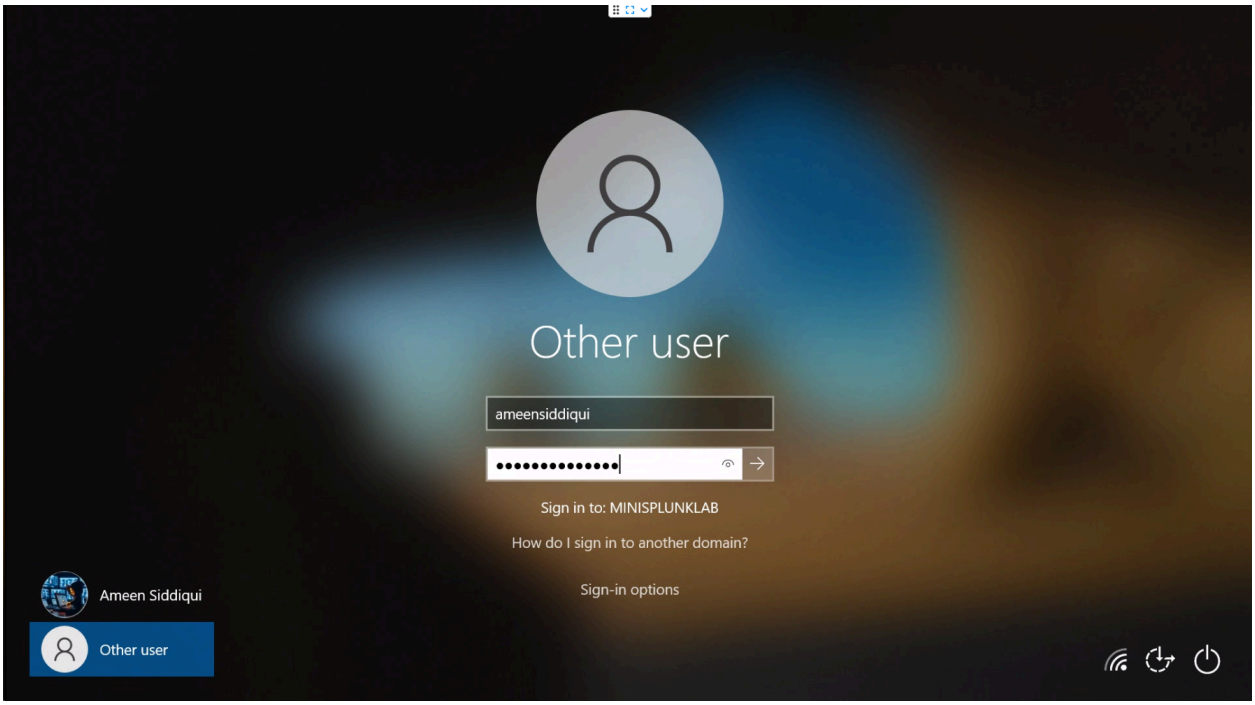
We will first change the DNS to the IP of the Active Directory Server (DC).



Then we go to Settings > System > About > Advanced System Settings > Change Computer Name / Domain > Add the domain



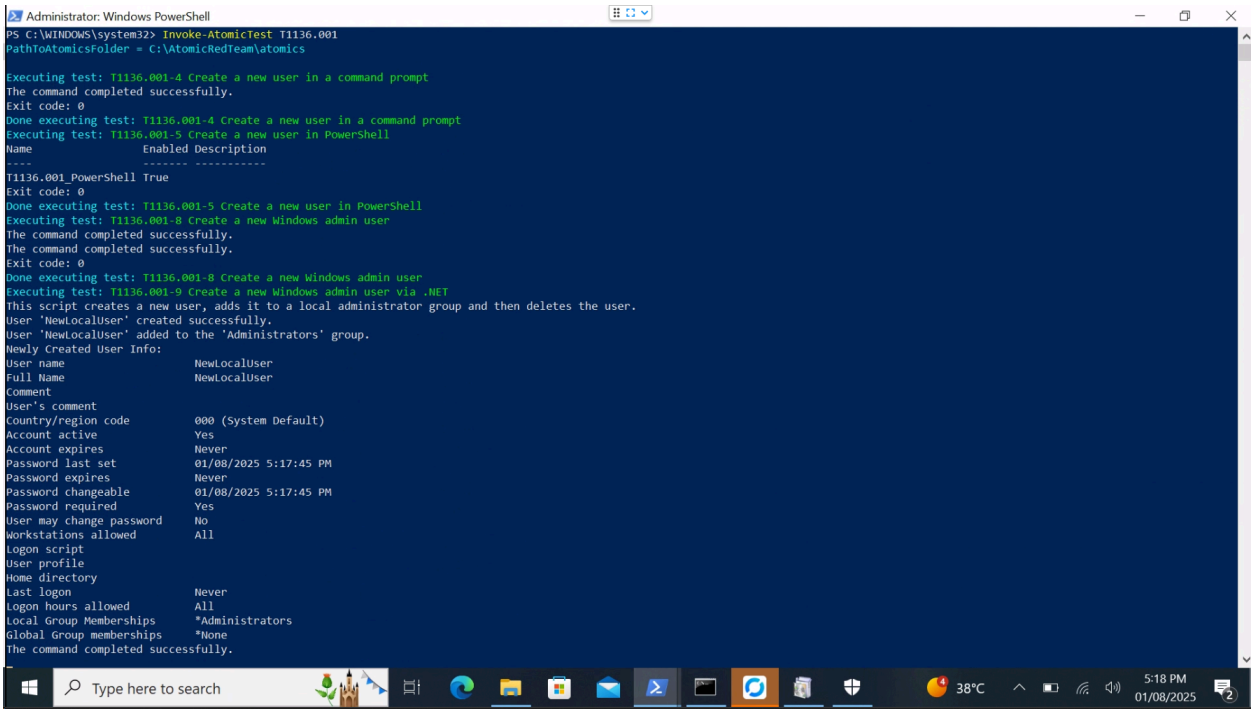
Once restarted we can test it

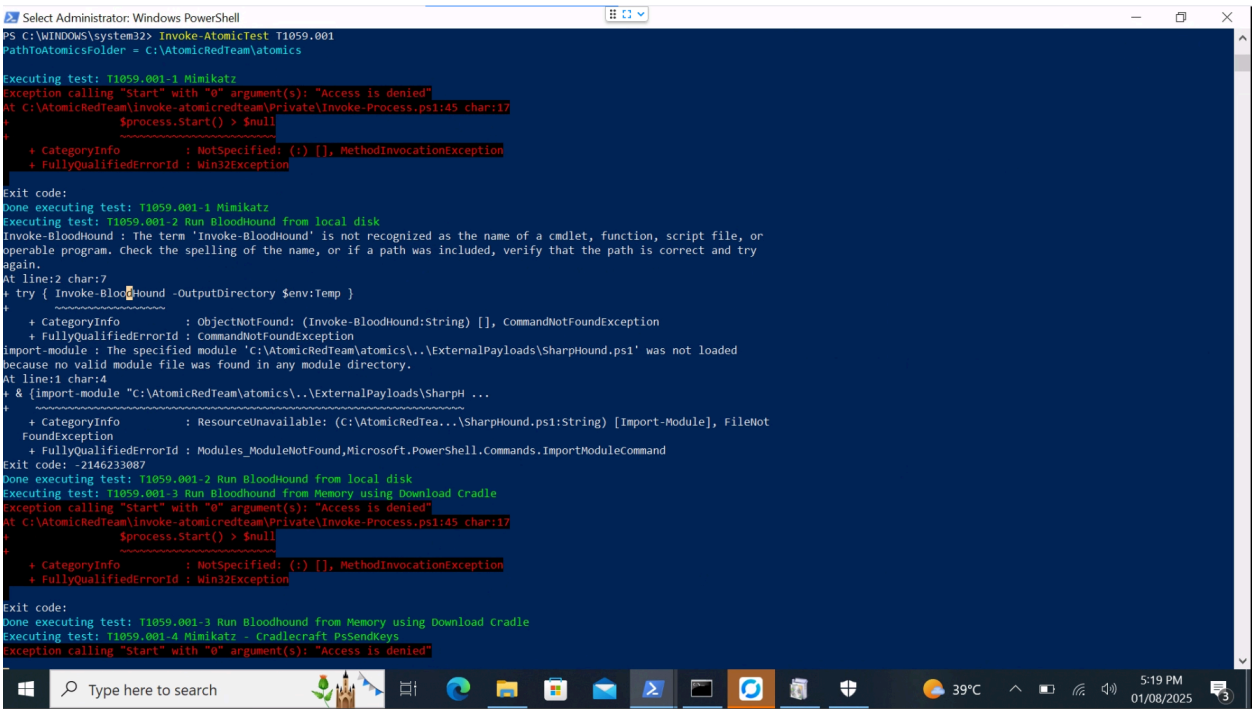


Final Stage, Attacking using Kali

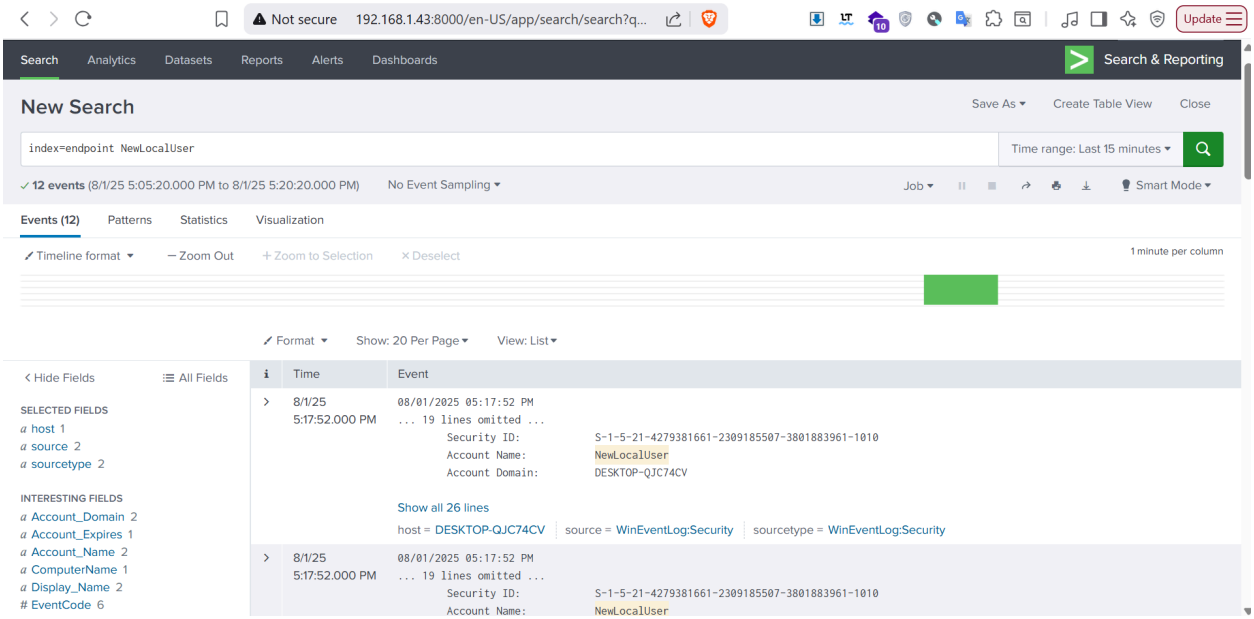
Atomic Red Team Tool

Initiating an Attackk





Now Splunk Search Shows it


Not secure 192.168.1.43:8000/en-US/app/search/search?q...
Update
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=endpoint NewLocalUser
Time range: Last 15 minutes
12 events (8/1/25 5:05:20.000 PM to 8/1/25 5:20:20.000 PM)
No Event Sampling
Job
Smart Mode
Events (12)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 2
INTERESTING FIELDS
a Account_Domain 2
a Account_Expires 1
a Account_Name 2
a ComputerName 1
a Display_Name 2
EventCode 6
Time
Event
8/1/25 5:17:52.000 PM
08/01/2025 05:17:52 PM
... 19 lines omitted ...
Security ID: S-1-5-21-4279381661-2309185507-3801883961-1010
Account Name: NewLocalUser
Account Domain: DESKTOP-QJC74CV
Show all 26 lines
host = DESKTOP-QJC74CV
source = WinEventLog:Security
sourcetype = WinEventLog:Security
8/1/25 5:17:52.000 PM
08/01/2025 05:17:52 PM
... 19 lines omitted ...
Security ID: S-1-5-21-4279381661-2309185507-3801883961-1010
Account Name: NewLocalUser