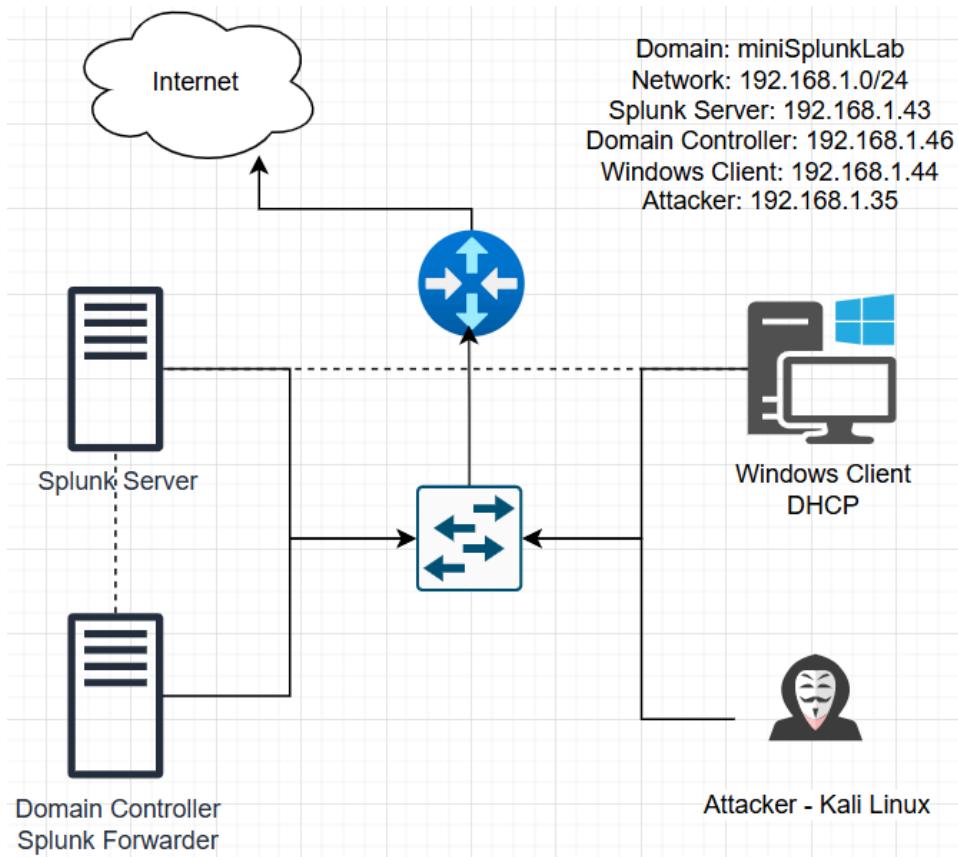
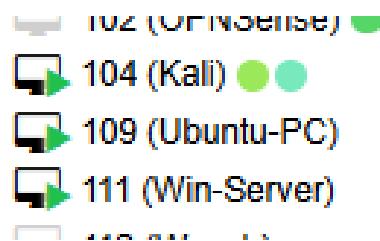
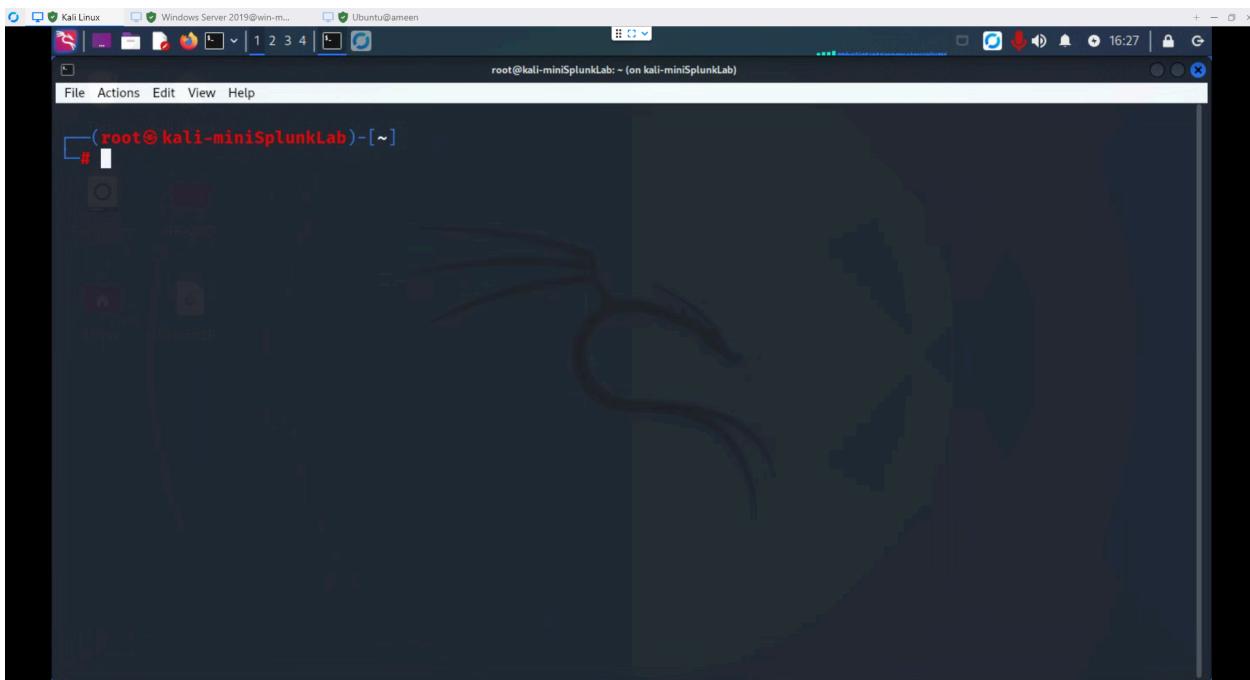


# Screenshots



## Setting up VMs on ProxmoxOS





The screenshot shows the Windows Server Manager interface for a local server named "WIN-M64R25I4KLP".

**PROPERTIES**

Computer name	WIN-M64R25I4KLP	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Today at 5:10 AM

**Windows Defender Firewall**

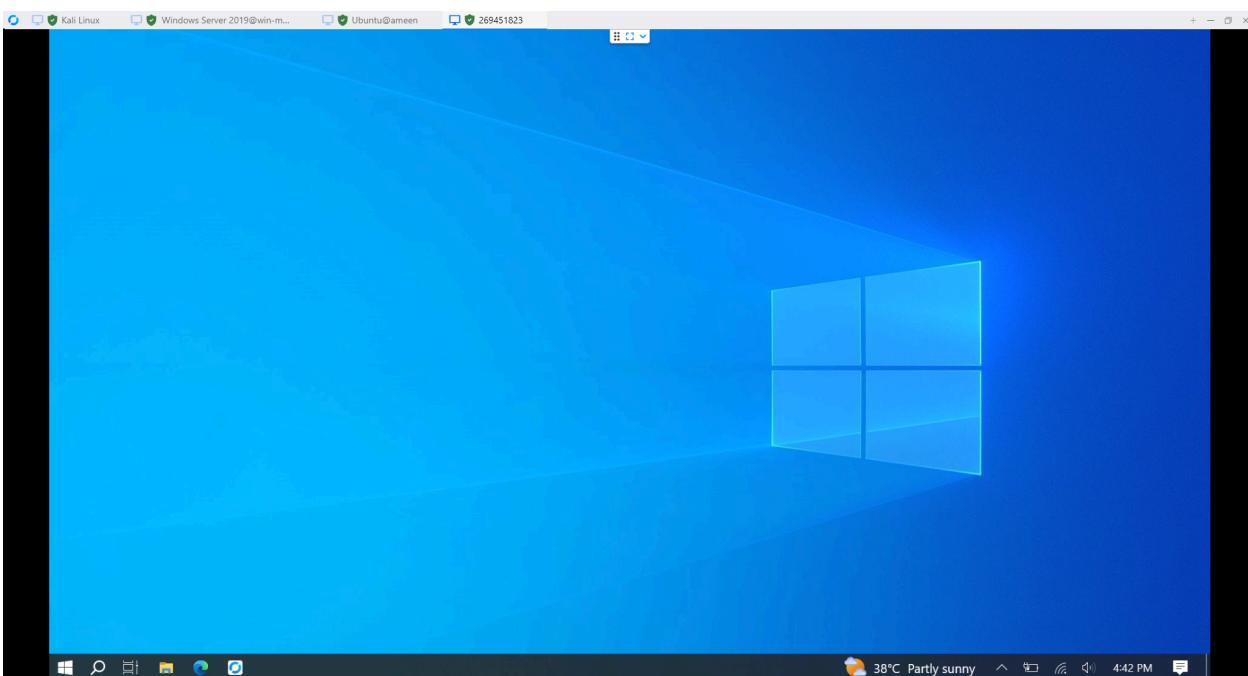
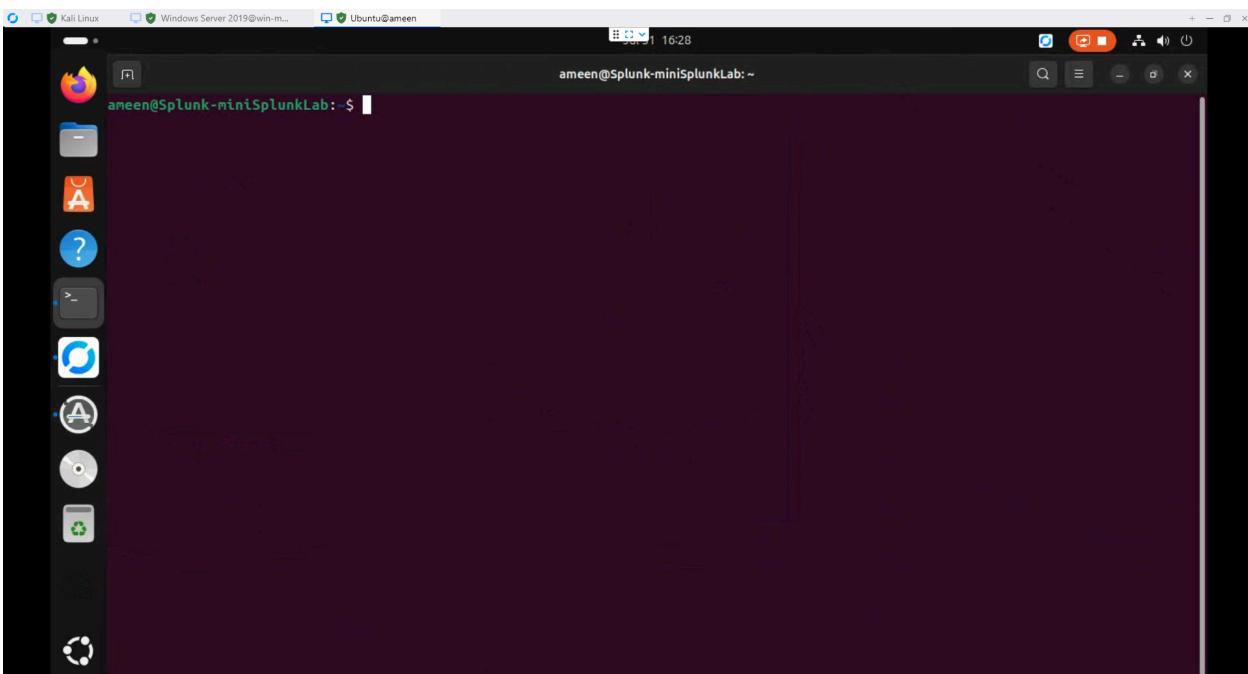
Public: On	Windows Defender Antivirus	Real-Time Protection: On
Enabled	Feedback & Diagnostics	Settings
Disabled	IE Enhanced Security Configuration	On
Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00431-10000-00000-AA679 (activated)

**Operating system version**

Microsoft Windows Server 2019 Standard Evaluation	Processors	QEMU Virtual CPU version 2.5+
QEMU Standard PC (i440FX + PIIX, 1996)	Installed memory (RAM)	8.1 GB
	Total disk space	31.46 GB

**EVENTS**

Server Name	ID	Severity	Source	Log	Date and Time
WIN-M64R25I4KLP	6008	Error	EventLog	System	7/31/2025 4:09:49 PM



## Downloading Splunk on Ubuntu Machine

The screenshot shows a web browser window with the URL [www.splunk.com/en\\_us/download/splunk-enterprise.html?utm\\_campaign=google\\_emea\\_tier2\\_en\\_search](http://www.splunk.com/en_us/download/splunk-enterprise.html?utm_campaign=google_emea_tier2_en_search). The page title is "Choose Your Download". Below it, a section for "Splunk Enterprise 10.0.0" is displayed, stating: "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." A "Choose Your Installation Package" section follows, with tabs for Windows, Linux (selected), and Mac OS. Under the Linux tab, the "64-bit" section lists three packages: ".tgz" (1635.46 MB), ".deb" (1290.48 MB), and ".rpm" (1646.48 MB). Each package has a "Download Now" button and a "Copy wget link" button.

```
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 system 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
```

```
ameen@Splunk-miniSplunkLab:~/Downloads$ cd /opt/splunk/
ameen@Splunk-miniSplunkLab:/opt/splunk$ ls
bin          ftr      license-eula.txt  opt           share
copyright.txt  include  LICENSE.txt    quarantined_files  splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest
etc          lib       openssl        README-splunk.txt  swidtag
ameen@Splunk-miniSplunkLab:/opt/splunk$ ls -al
total 4516
drwxr-xr-x 11 splunk splunk  4096 Jul 31 16:48 .
drwxr-xr-x  4 root  root   4096 Jul 31 16:47 ..
drwxr-xr-x  4 splunk splunk  4096 Jul 31 16:48 bin
-r--r--r--  1 splunk splunk   57 Jul 28 15:05 copyright.txt
drwxr-xr-x 17 splunk splunk  4096 Jul 31 16:48 etc
-rw-r--r--  1 splunk splunk  425 Jul 31 16:48 ftr
drwxr-xr-x  3 splunk splunk  4096 Jul 31 16:48 include
drwxr-xr-x  8 splunk splunk  4096 Jul 31 16:48 lib
-r--r--r--  1 splunk splunk 59708 Jul 28 15:05 license-eula.txt
-r--r--r--  1 splunk splunk 1090 Jul  7 22:15 LICENSE.txt
drwxr-xr-x  2 splunk splunk  4096 Jul 31 16:48 openssl
drwxr-xr-x  7 splunk splunk  4096 Jul 31 16:48 opt
drwxr-xr-x  2 splunk splunk  4096 Jul 31 16:48 quarantined_files
-r--r--r--  1 splunk splunk  519 Jul 28 15:05 README-splunk.txt
drwxr-xr-x  6 splunk splunk  4096 Jul 31 16:48 share
-r--r--r--  1 splunk splunk 4499257 Jul 28 15:36 splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest
drwxr-xr-x  2 splunk splunk  4096 Jul 31 16:48 swidtag
ameen@Splunk-miniSplunkLab:/opt/splunk$ sudo -u splunk bash
splunk@ameen:~$
```

## Completing Install

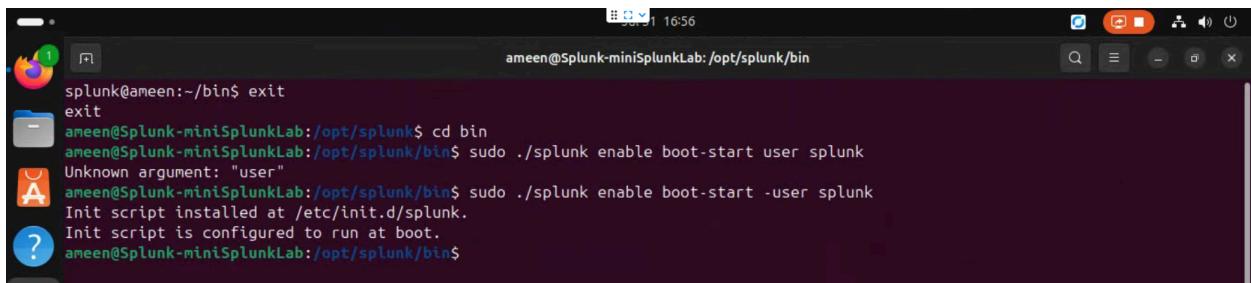
```
ameen@Splunk-miniSplunkLab:/opt/splunk$ sudo -u splunk bash
splunk@ameen:~$ cd bin
splunk@ameen:~/bin$ ./splunk start
Splunk General Terms (v4 August 2024)

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 250 Brannan Street, San Francisco, California 94107, USA ("Splunk" or "we" or "us" or "our") and you ("Customer" or "you" or "your") govern your acquisition, access to, and use of Splunk's Offerings, regardless of how accessed or acquired, whether directly from us or from another Approved Source. By clicking on the appropriate button, or by downloading, installing, accessing, or using any Offering, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of Customer, do not download, install, access, or use any Offering. The "Effective Date" of these General Terms is: (i) the date of Delivery; or (ii) the date you access or use the Offering in any way, whichever is earlier. Capitalized terms are defined in the Definitions section below. Effective September 23, 2024, and unless the context otherwise requires, any reference in these General Terms to "Splunk Inc.", "Splunk", "we", "us" or "our" will be deemed to refer to "Splunk LLC".
```

1. Your Use Rights and Limits

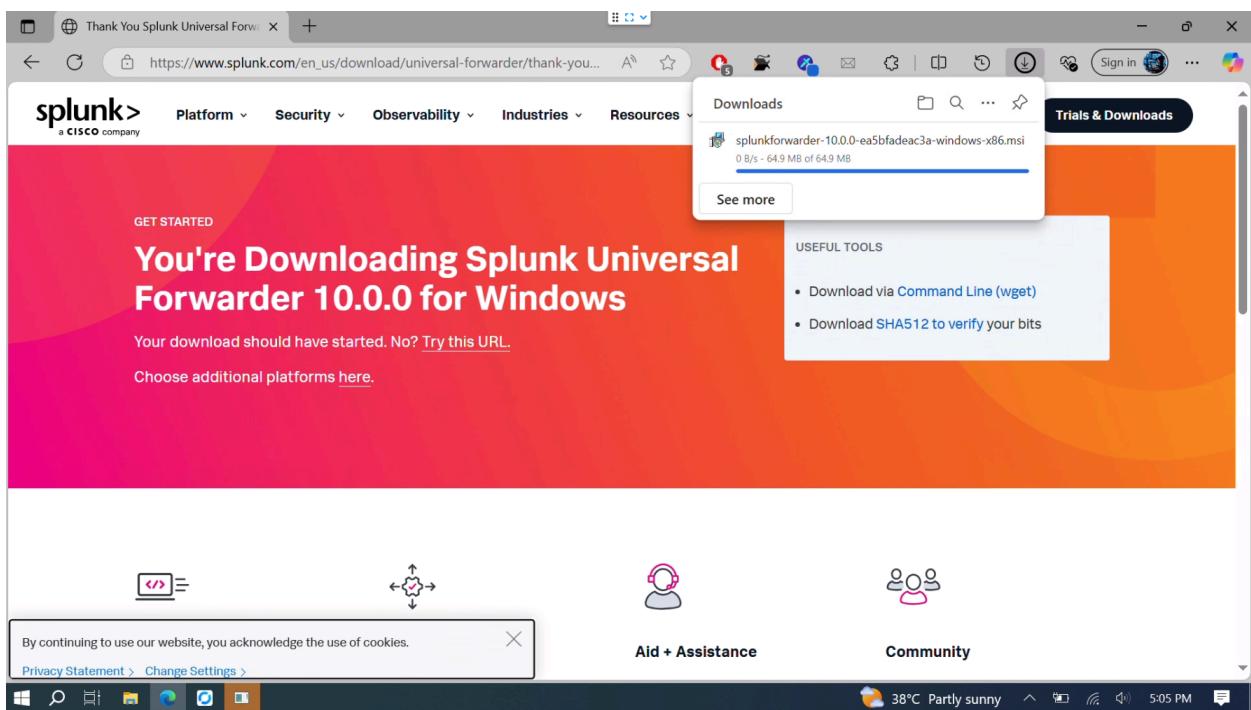
1.1. Your Use Rights. We grant you a non-exclusive, worldwide, non-transferable and non-sublicensable right, subject to your compliance with these General Terms and payment of applicable Fees, to use acquired Offerings only for your Internal Business Purpose during the Term, up to the Capacity, and, if applicable, in accordance with the Order ("Use Rights"). You have the right to make a reasonable number of copies of On-Premises Products for archival and back-up.

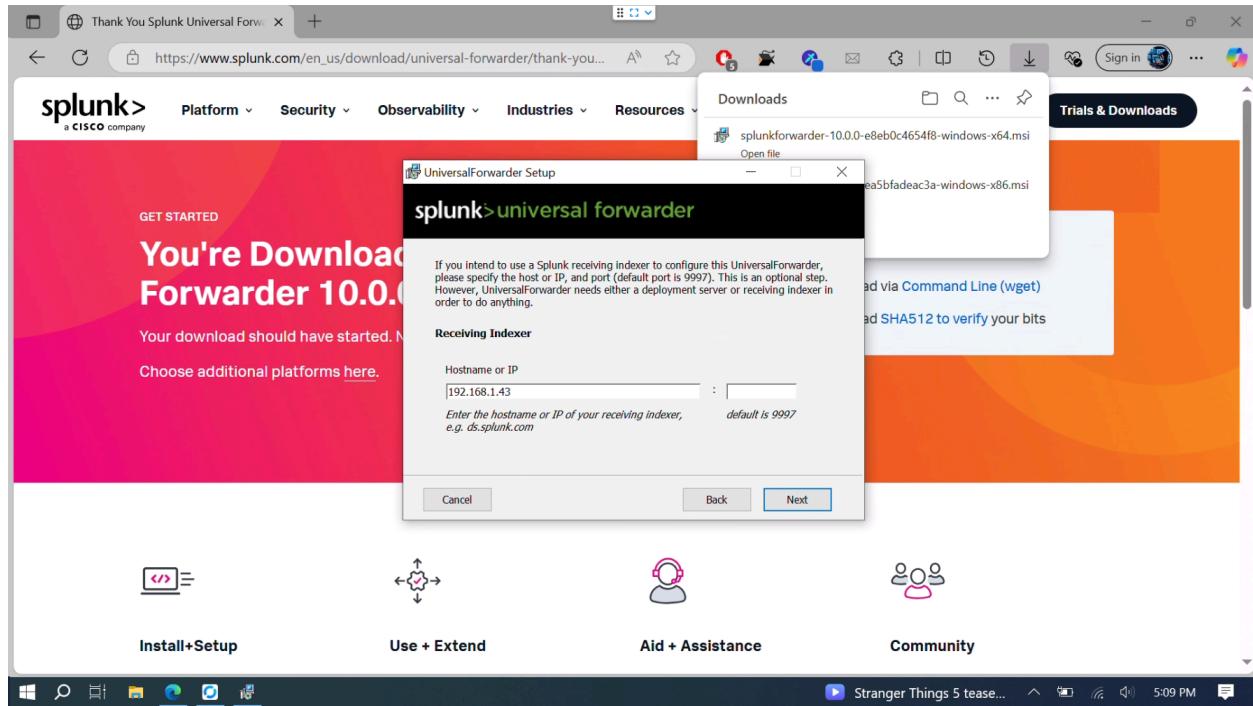
## Enabling Auto-start at Boot



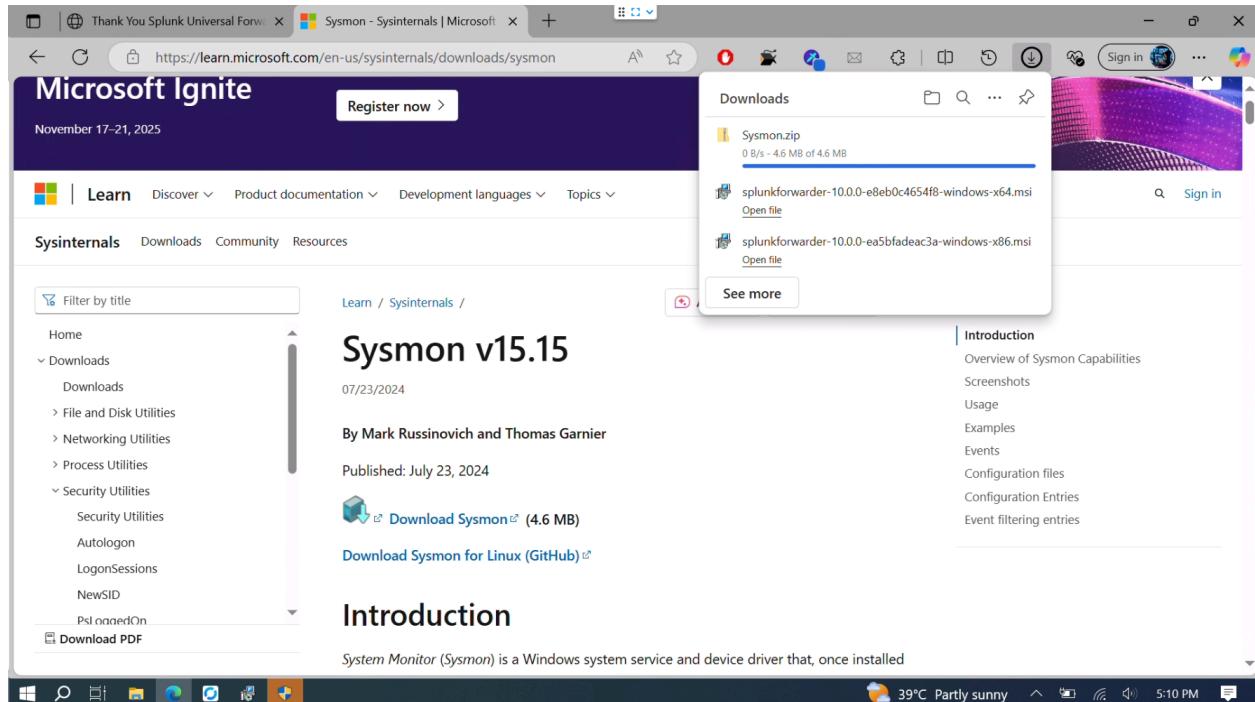
```
splunk@ameen:~/bin$ exit
exit
ameen@Splunk-miniSplunkLab:/opt/splunk$ cd bin
ameen@Splunk-miniSplunkLab:/opt/splunk/bin$ sudo ./splunk enable boot-start user splunk
Unknown argument: "user"
ameen@Splunk-miniSplunkLab:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
ameen@Splunk-miniSplunkLab:/opt/splunk/bin$
```

# Downloading Universal Forwarder on Windows Target PC

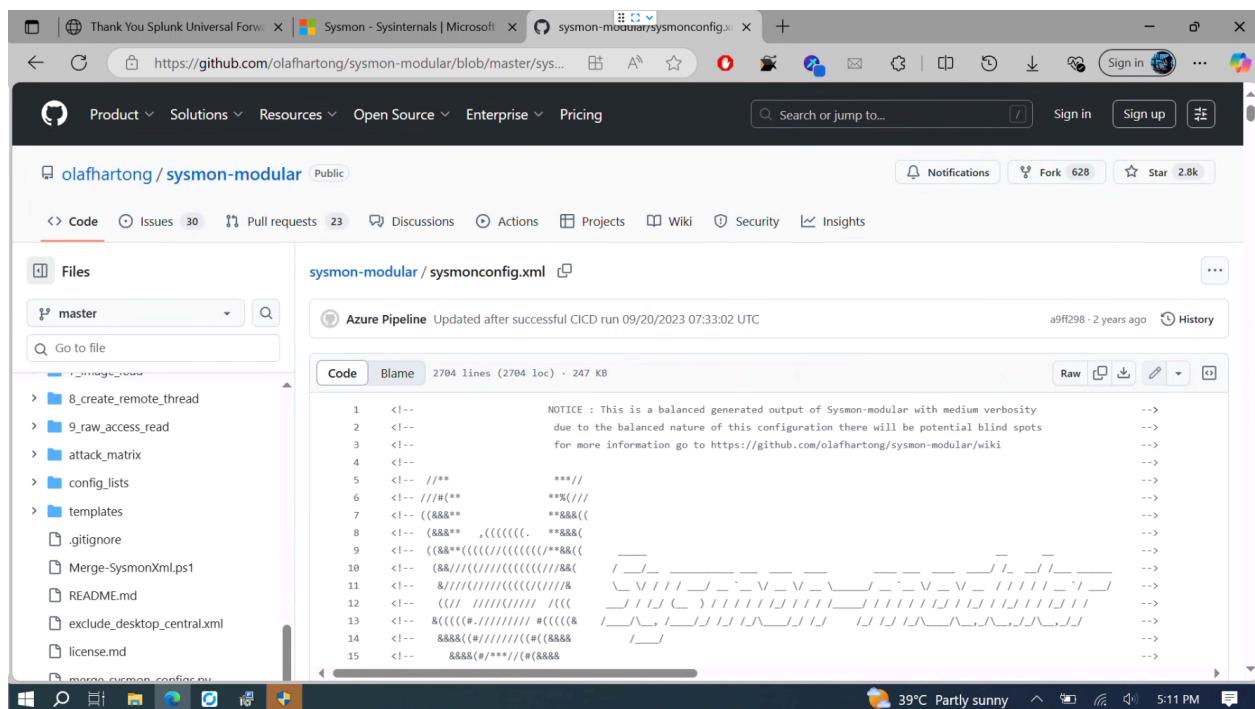




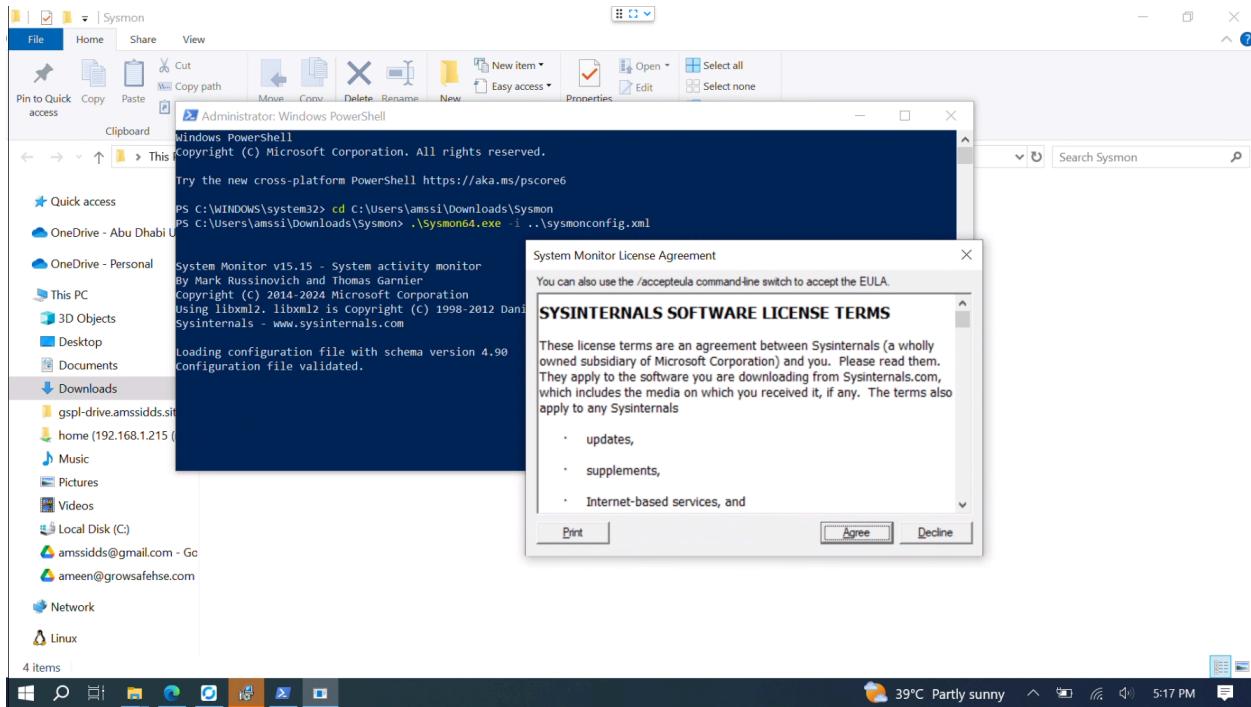
## Downloading Sysmon on Target Windows Machine



# Downloading Sysmon Config by “olaf”



# Configuring Sysmon with sysmonconfig.xml downloaded



```
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Windows\system32> cd C:\Users\amssi\Downloads\Sysmon
PS C:\Users\amssi\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\amssi\Downloads\Sysmon>
```

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

File Explorer window showing the file structure:

```

This PC > Local Disk (C:) > Program Files > SplunkUniversalForwarder > etc > system > default

```

Content of the 'default' folder:

	Name	Date modified	Type
	agent_management.conf	28/07/2025 11:16 AM	CONF File
	alert_actions.conf	28/07/2025 11:16 AM	CONF File
	app.conf	28/07/2025 11:16 AM	CONF File
	audit.conf	28/07/2025 11:16 AM	CONF File
	authentication.conf	28/07/2025 11:16 AM	CONF File
	authorize.conf	28/07/2025 11:16 AM	CONF File
	conf.conf	28/07/2025 11:16 AM	CONF File
	default-mode.conf	28/07/2025 11:16 AM	CONF File
	federated.conf	28/07/2025 11:16 AM	CONF File
	field_filters.conf	28/07/2025 11:16 AM	CONF File
	global-banner.conf	28/07/2025 11:16 AM	CONF File
	health.conf	28/07/2025 11:16 AM	CONF File
<input checked="" type="checkbox"/>	inputs.conf	28/07/2025 11:16 AM	CONF File
	limits.conf	28/07/2025 11:16 AM	CONF File

File Explorer window showing the file structure:

```

This PC > Local Disk (C:) > Program Files > SplunkUniversalForwarder > etc > apps > SplunkUniversalForwarder > local

```

Content of the 'local' folder:

	Name	Date modified	Type	Size
	app.conf	31/07/2025 5:13 PM	CONF File	1 KB
	inputs.conf	31/07/2025 5:43 PM	CONF File	1 KB

## Changing the values to new values

[WinEventLog://Application]

index = endpoint

disabled = false

[WinEventLog://Security]

index = endpoint

disabled = false

[WinEventLog://System]

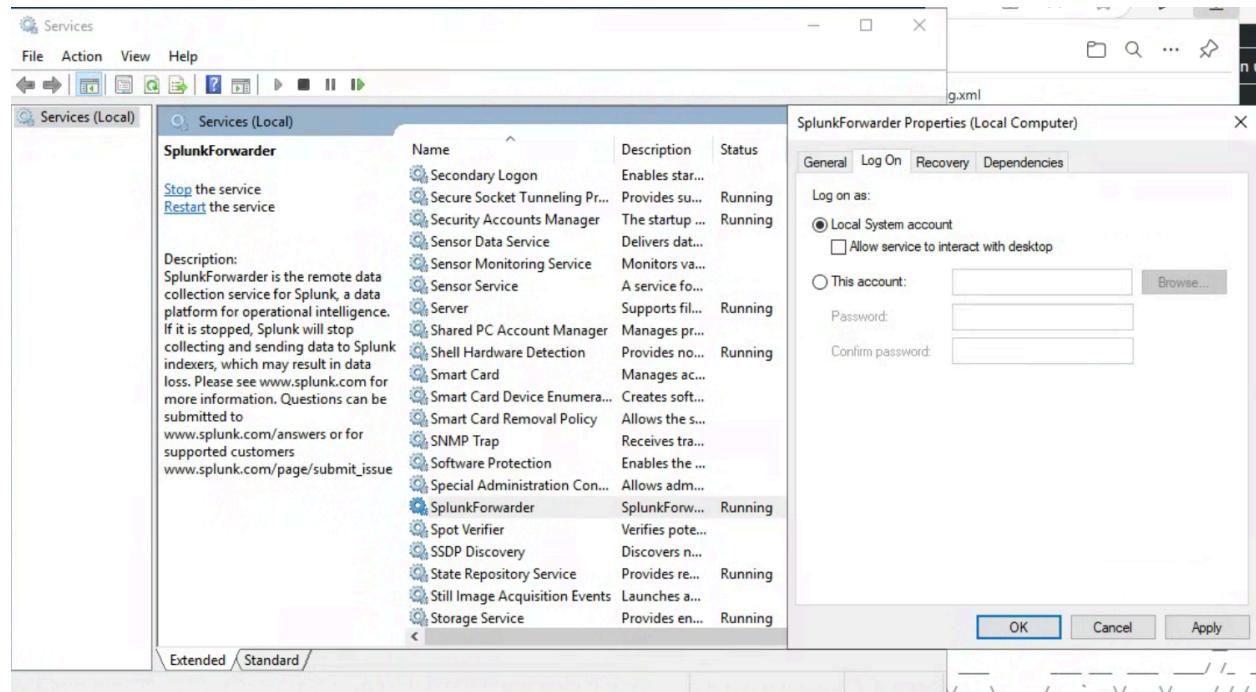
index = endpoint

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

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the index store.

Name	Actions	Type	App	Current Size	Max Size	Events	Last Update
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	10K	an hour ago
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	25K	a few seconds
_dsappear	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	\$SPLUNK_DB/_dsappear
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	\$SPLUNK_DB/_dsclient
_dsphonehome	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0	\$SPLUNK_DB/_dsphonehome
_internal	Edit Delete Disable	Events	system	2 MB	488.28 GB	16K	an hour ago

192.168.1.43:8000/en-US/manager/launcher/data/indexes

Add Data

Explore Data

Monitoring Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- OTel Collectors
- Agent management
- Indexer clustering
- Federation
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- RapidDiag
- Instrumentation
- Licensing
- Workload management
- Mobile settings

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods

We can see all events being logged

## Creating a new Index as Endpoint

New Index

General Settings

Index Name	endpoint
Index Data Type	<input checked="" type="radio"/> Events <input type="radio"/> Metrics
Home Path	optional
Cold Path	optional
Thawed Path	optional
Data Integrity Check	Enable      Disable
Max Size of Entire Index	500 GB

Save Cancel

## Configuring Receiving data on Forwarder

The screenshot shows the Splunk interface with a navigation bar at the top. Below the navigation bar, there are several cards: 'Add Data' (with a plus icon), 'Explore Data' (with a magnifying glass icon), and a search bar labeled 'Search settings...'. To the right, there are two columns of links under 'KNOWLEDGE' and 'DATA' categories.

KNOWLEDGE	DATA
Searches, reports, and alerts	Data inputs
Data models	Forwarding and receiving
Event types	Indexes
Tags	Report acceleration summaries
Fields	Virtual indexes
Lookups	Source types
User interface	Ingest actions

Below this, the 'Receive data' section is shown with a table:

Type	Actions
Configure receiving	+ Add new

The screenshot shows the 'Configure receiving' dialog box. It has a title 'Configure receiving' and a subtitle 'Set up this Splunk instance to receive data from forwarder(s.)'. A field 'Listen on this port \*' contains the value '9997'. Below the field is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom are 'Cancel' and 'Save' buttons.

## To check if the Connector is connected

Go to Apps > Search and Reporting

In the field type `index="endpoint"`

New Search

index="endpoint"

2,834 events (7/30/25 5:00:00.000 PM to 7/31/25 5:50:19.000 PM) No Event Sampling

Events (2,834) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection Deselect 1 hour per column

**host**

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
DESKTOP-QJC74CV	2,834	100%

event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='(5770385f-2c<Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0xT13:24:03.5128772Z'><EventRecordID>2834</EventRecordID><Correlation/><EventID>19756</EventID><Channel><Computer>DESKTOP-QJC74CV</Computer><RuleName>'</RuleName></Data><Data Name='UtcTime'>2025-07-31 13:24:03.512Z</Data><Data Name='ProcessId'>19756</Data><Data Name='Image'>C:\WINDOWS\sysFile\WindowsApps\MSTeams\_25185.410.3812.8024\_x64\_8wekyb3d8bbw\desk</Image><Data Name='CreationUtcTime'>2025-07-31 13:24:03.512Z</Data><Data Name='User'>

host = DESKTOP-QJC74CV | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

We can see host connected

## Downloading Splunk Forwarder on Active Directory

New Search

index="endpoint"

2,834 events (7/30/25 5:00:00.000 PM to 7/31/25 5:50:19.000 PM) No Event Sampling

Events (2,834) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection Deselect 1 hour per column

**host**

2 Values, 100% of events

Selected Yes No

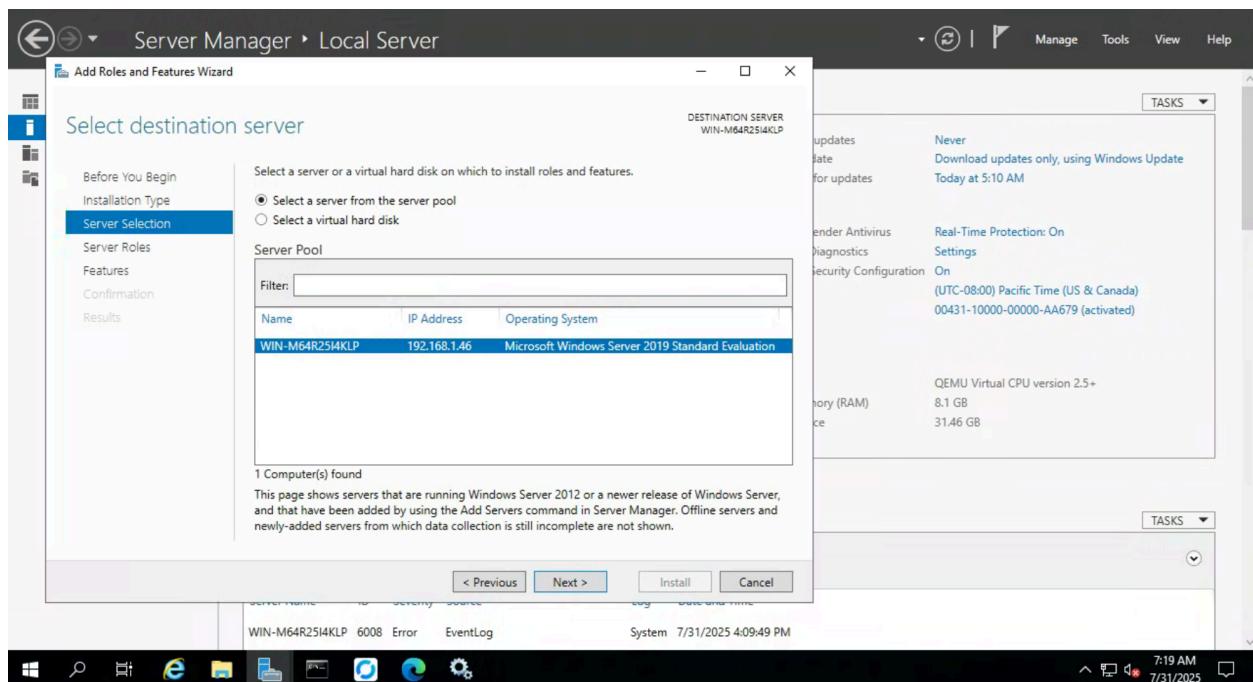
Reports

Top values Top values by time Rare values

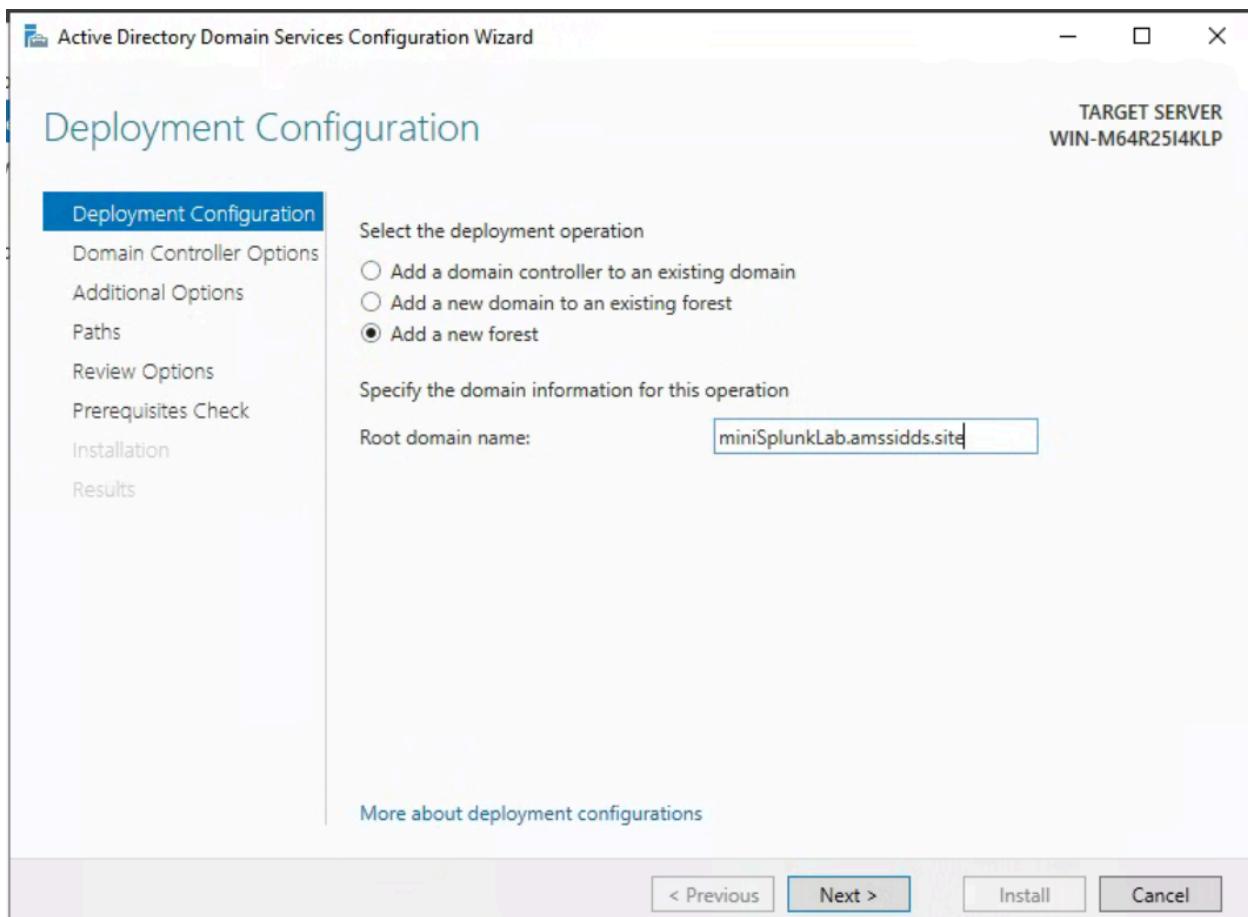
Events with this field

Values	Count	%
DESKTOP-QJC74CV	17,452	95.591%
WIN-M64R25I4KLP	805	4.409%

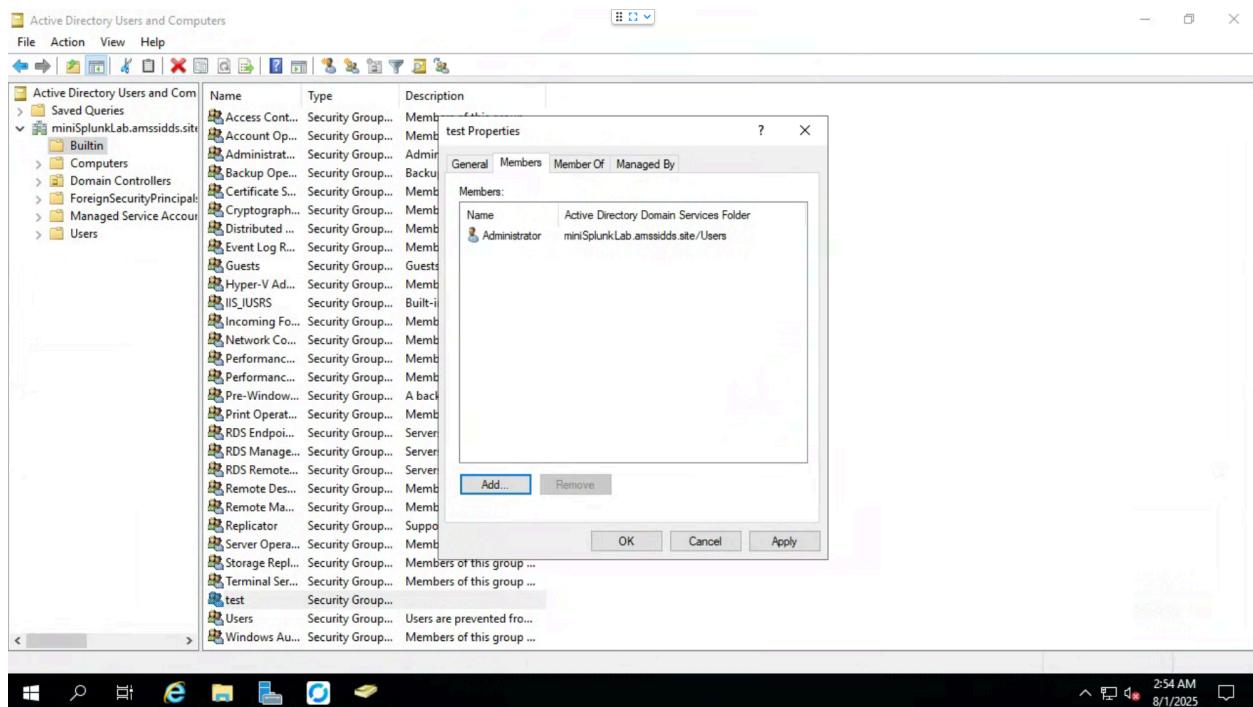
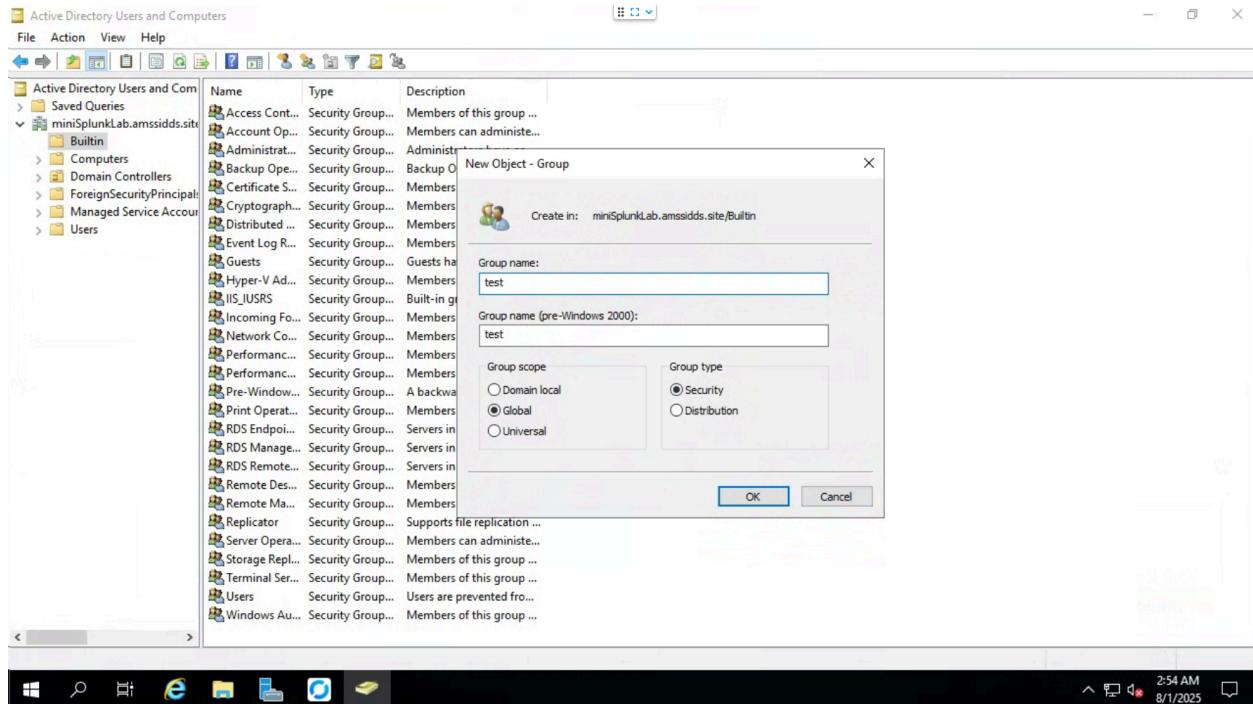
## Configuring Active Directory and Promoting to DC

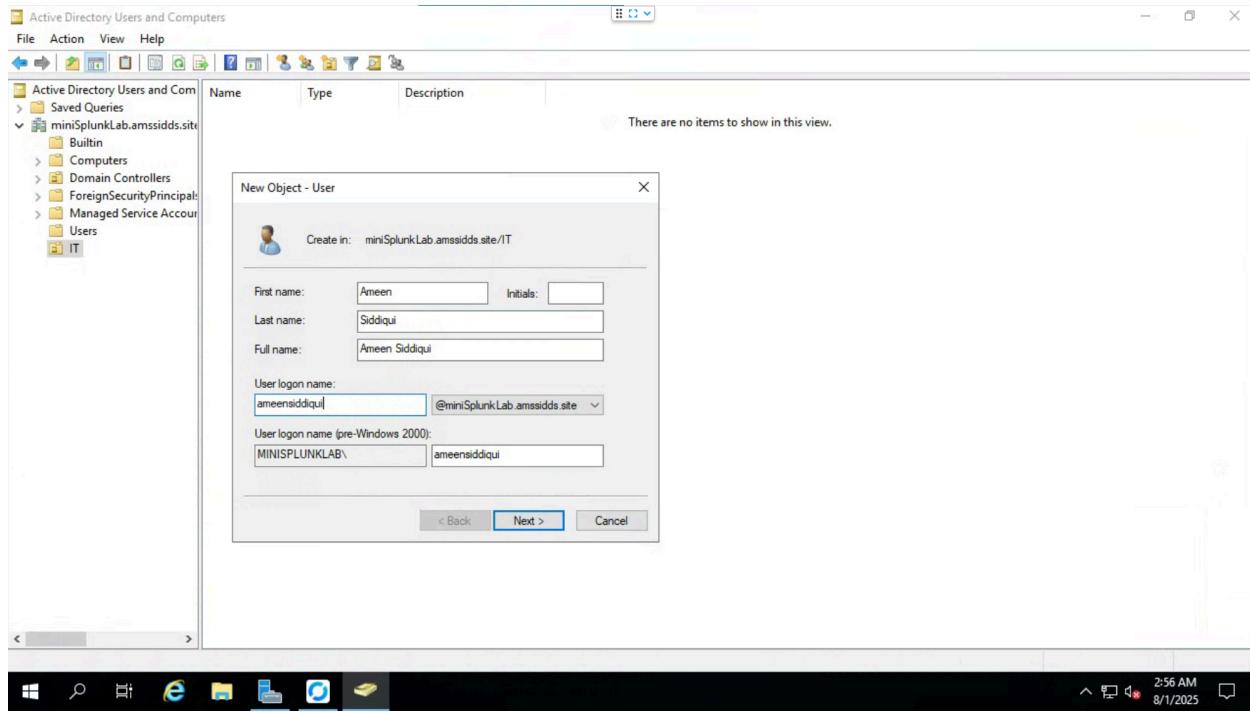


## Promoting it to DC



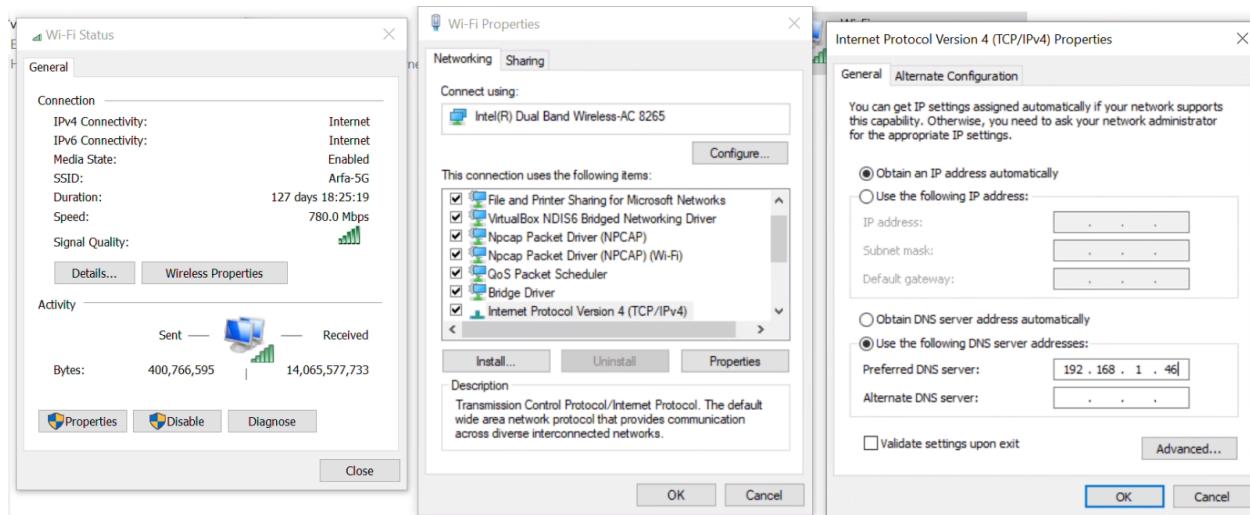
## Creating Global Test Group under Administrator and a DL group under Test Group



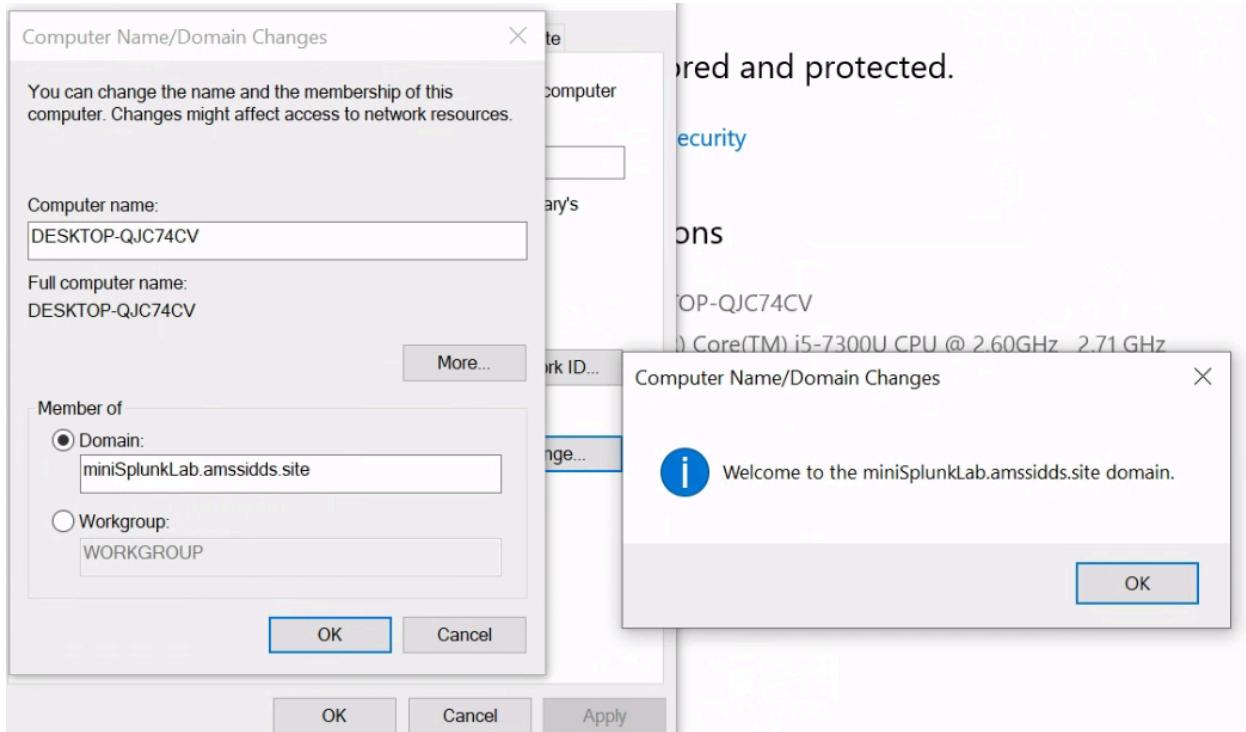


# Connecting Windows Client Victim PC to the Domain Controller

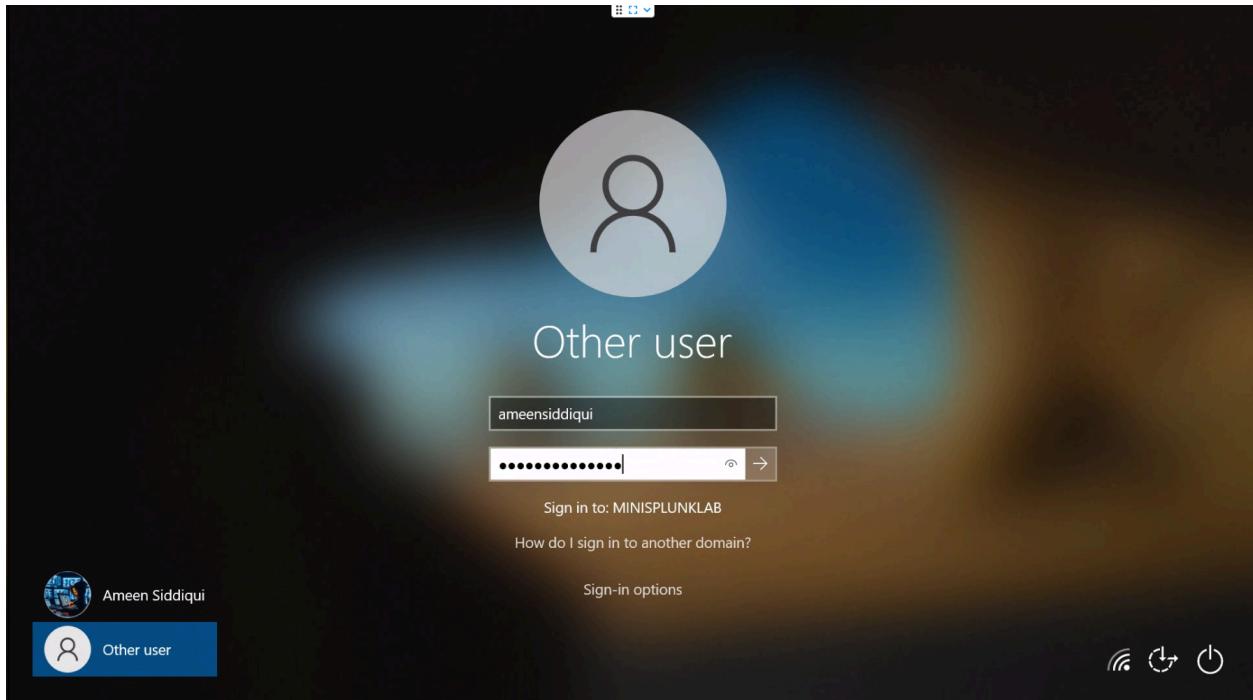
We will first change the DNS to the IP of the Active Directory Server (DC).



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

```

Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Invoke-AtomicTest T1136.001
PathToAtomsicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-4 Create a new user in a command prompt
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-4 Create a new user in a command prompt
Executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-8 Create a new Windows admin user
The command completed successfully.
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-8 Create a new Windows admin user
Executing test: T1136.001-9 Adds it to a local administrator group and then deletes the user.
This script creates a new user, adds it to a local administrator group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the 'Administrators' group.
Newly Created User Info:
User Name           NewLocalUser
Full Name          NewLocalUser
Comment
User's comment
Country/region code    000 (System Default)
Account active       Yes
Account expires      Never
Password last set   01/08/2025 5:17:45 PM
Password expires     Never
Password changeable  01/08/2025 5:17:45 PM
Password required    Yes
User may change password No
Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never
Logon hours allowed All
Local Group Memberships *Administrators
Global Group Memberships *None
The command completed successfully.

5:18 PM 01/08/2025

```

```

Select Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Invoke-AtomicTest T1059.001
PathToAtomsicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1059.001-1 Mimikatz
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+         $process.Start() > $null
+         ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-1 Mimikatz
Executing test: T1059.001-2 Run Bloodhound from local disk
Invoke-BloodHound : The term 'Invoke-BloodHound' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
At line:2 char:7
+ try { Invoke-BloodHound -OutputDirectory $env:Temp }
+         ~~~~~
+ CategoryInfo          : ObjectNotFound: (Invoke-BloodHound:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
Import-Module : The specified module 'C:\AtomicRedTeam\atomics..\ExternalPayloads\SharpHound.ps1' was not loaded
because no valid module file was found in any module directory.
At line:1 char:4
+ & {import-module "C:\AtomicRedTeam\atomics..\ExternalPayloads\SharpH ...
+         ~~~~~
+ CategoryInfo          : ResourceUnavailable: (C:\AtomicRedTea...\\SharpHound.ps1:String) [Import-Module], FileNot
FoundException
+ FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
Exit code: -2146233087
Done executing test: T1059.001-2 Run BloodHound from local disk
Executing test: T1059.001-3 Run Bloodhound from Memory using download Cradle
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+         $process.Start() > $null
+         ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-3 Run Bloodhound from Memory using Download Cradle
Executing test: T1059.001-4 Mimikatz - Cradlecraft_PsAndKeys
Exception calling "Start" with "0" argument(s): "Access is denied"

5:19 PM 01/08/2025

```

Now Splunk Search Shows it

Not secure 192.168.1.43:8000/en-US/app/search/search?q...

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

index=endpoint NewLocalUser

12 events (8/1/25 5:05:20.000 PM to 8/1/25 5:20:20.000 PM) No Event Sampling ▾

Events (12) Patterns Statistics Visualization

✓ Timeline format ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

✓ Format ▾ Show: 20 Per Page ▾ View: List ▾

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
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

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