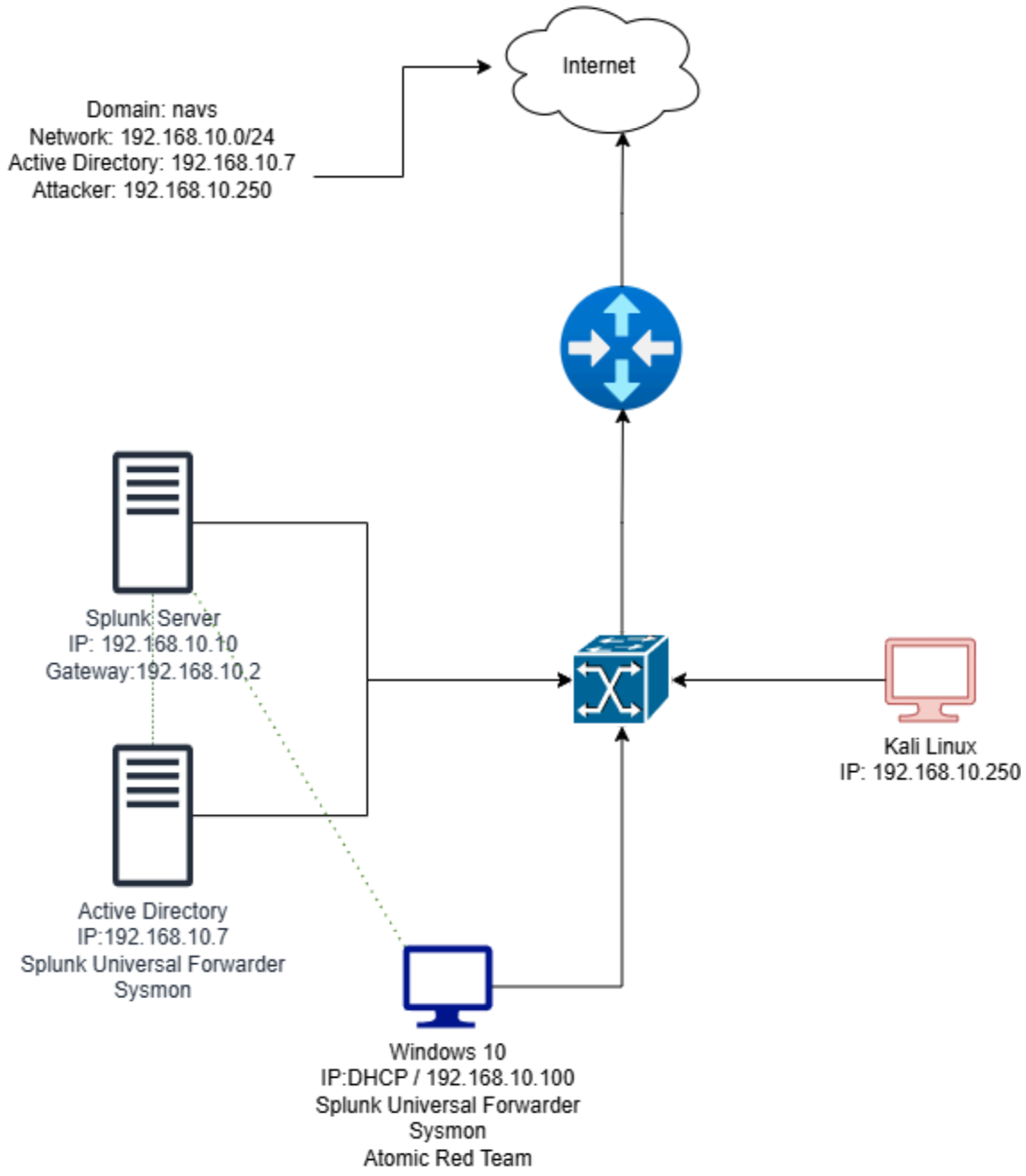
Active Directory & Attack Detection Lab

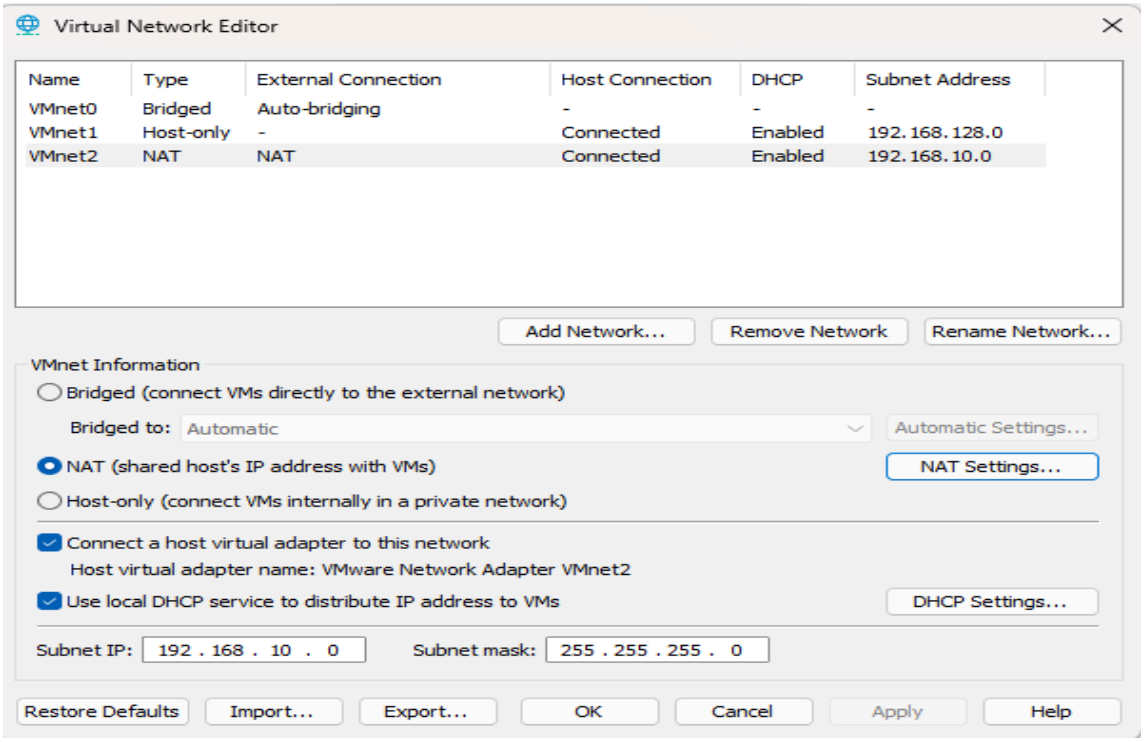
🏗️ Lab Architecture

- **SIEM:** Splunk Enterprise (Ubuntu)
- **Domain Controller:** Windows Server 2022 (Active Directory DS)
- **Target:** Windows 10 (Sysmon & Splunk Universal Forwarder)
- **Attacker:** Kali Linux (Hydra)
- **Network:** Private NAT Network



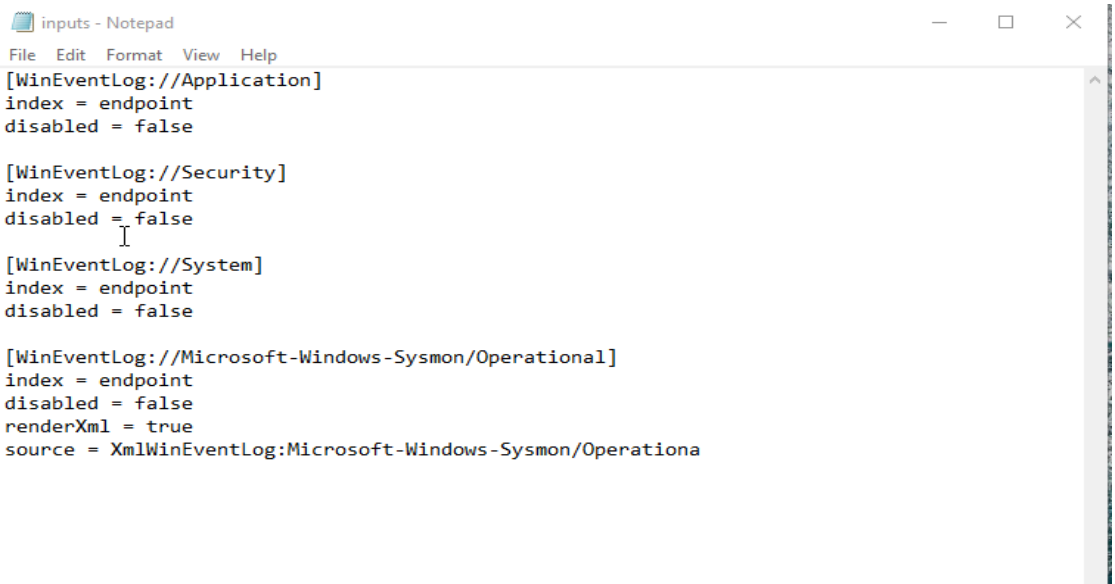
#1

Used NAT for sharing IP across 4 Virtual Machines used in this project, The Network address that was used is 192.168.10.0/24



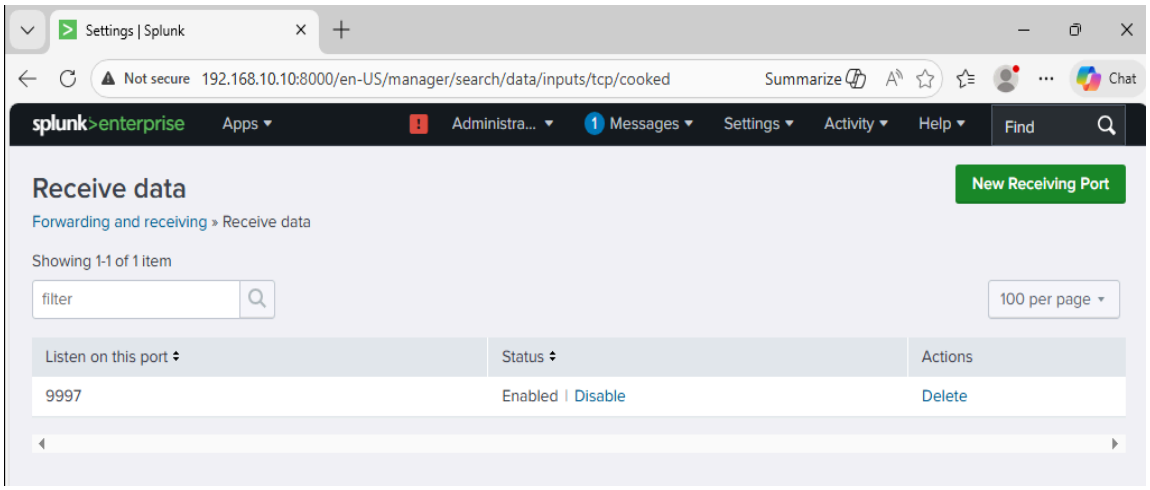
#2

Configured Sysmon with sysmonconfig.xml through Powershell and also created a inputs.conf file for SplunkForwarder in the local folder (never configure files in the default folder) The conf file below shows what Event Logs to grab and what index to put it under, this being index=endpoint. (This process was the same for the Target-PC and Windows AD Server)



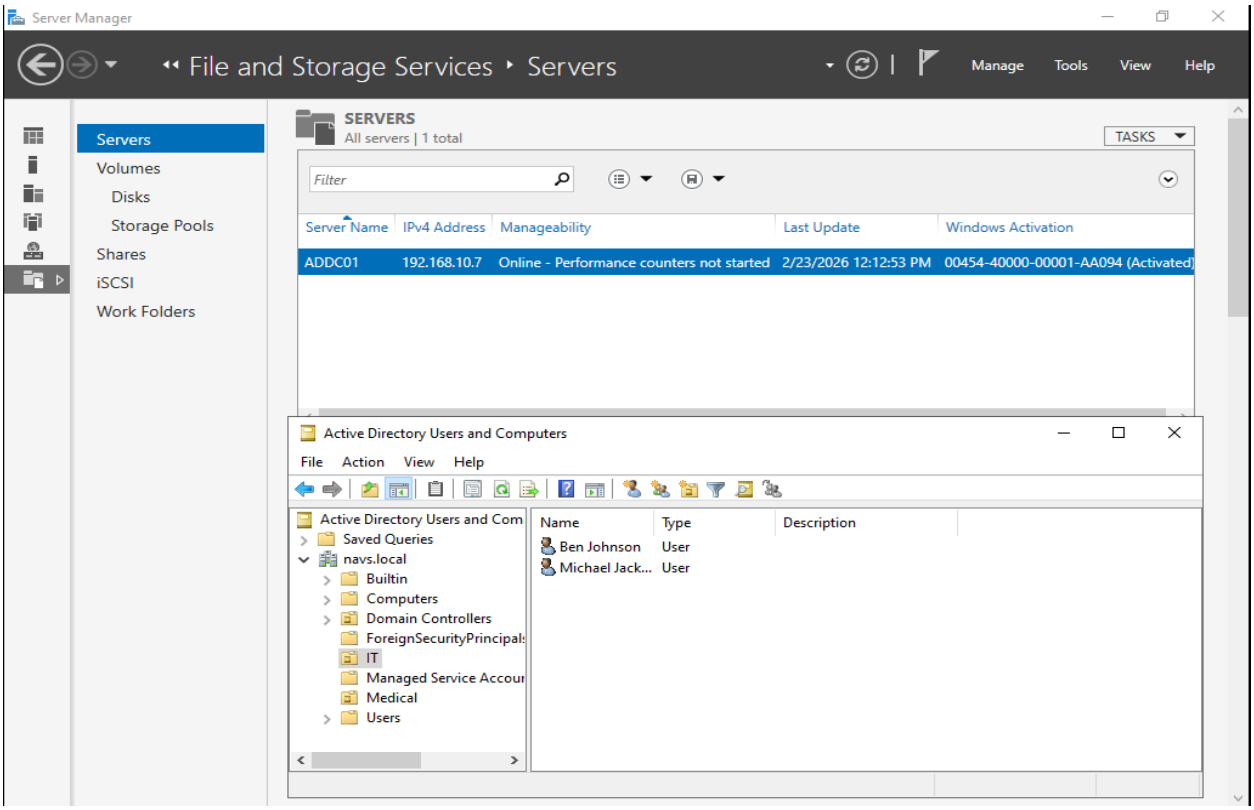
#3

Splunk Enterprise IP address was changed to static (default gateway is 192.168.10.2) and receiving port 9997 was enabled via Splunk Web Interface so it can ingest data from Target-PC and Windows AD Server



#4

Established a navs.local domain and created test users for the brute force attack



#5

After linking the Target-PC with navs.local domain and logging into a user account, I proceeded with the Brute Force Attack using hydra on Kali Linux. After creating a password.txt file with a random generation of passwords I purposely included the password that logins to the Victims account to see what result I would get.

```
Session   Actions   Edit   View   Help

┌──(kali㉿kali)-[~/Desktop/AD-Project]
└─$ hydra -t 1 -l JMendoza1 -P passwords.txt rdp://192.168.10.100
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-23 14:
18:29
[WARNING] the rdp module is experimental. Please test, report - and if possib
le, fix.
[DATA] max 1 task per 1 server, overall 1 task, 22 login tries (l:1/p:22), ~2
2 tries per task
[DATA] attacking rdp://192.168.10.100:3389/
[3389][rdp] host: 192.168.10.100   login: JMendoza1   password: Hereiam15@
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-23 14:18:51

┌──(kali㉿kali)-[~/Desktop/AD-Project]
└─$
```

After enabling RDP for this type of attack it was able to return the correct password which would then compromise the victims account

The command used was

hydra -t 1 -l JMendoza1 -P passwords.txt rdp://192.168.10.100

#6

Going onto the detection part of this project I will be querying for index=endpoint alongside the user who was attacked Account_Name="JMendoza1", I will also search for Event ID of 4625 (Failed Login) and Event ID of 4624 (Successful Login) which will show us how many times the brute force attack failed to login before successfully getting the password correct.

New Search

```
index=endpoint Account_Name="JMendoza1" EventCode=4625
```

i	Time	Event
>	2/23/26 10:59:38.961 PM	02/23/2026 02:59:38.961 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Target-PC.navs.local Show all 61 lines host = Target-PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	2/23/26 10:59:37.945 PM	02/23/2026 02:59:37.945 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Target-PC.navs.local Show all 61 lines host = Target-PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	2/23/26 10:59:36.923 PM	02/23/2026 02:59:36.923 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Target-PC.navs.local Show all 61 lines host = Target-PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	2/23/26 10:59:35.905 PM	02/23/2026 02:59:35.905 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Target-PC.navs.local Show all 61 lines host = Target-PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	2/23/26 10:59:34.888 PM	02/23/2026 02:59:34.888 PM LogName=Security EventCode=4625 EventType=0 ComputerName=Target-PC.navs.local Show all 61 lines host = Target-PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security

The images above show events which have a time difference of a few milliseconds, which is a key indicator of a potential brute force attack as it is trying to use multiple passwords at the same time.

#7

This shows that when searching for Event ID 4624 (Successful Login) will also show how many times it occurs along the IP address so we can see if it's coming from the attacker's IP address (192.168.10.250) or the Victims (192.168.10.100). The highlighted parts below show the victims account name and the source.

Attackers Machine

i	Time	Event
	2/23/26 10:46:34.220 PM	02/23/2026 02:46:34.220 PM LogName=Security EventCode=4624 EventType=0 ComputerName=ADDC01.navs.local Show all 70 lines Event Actions

Type	Field	Value
Selected	host	ADDC01
	source	WinEventLog:Security
	sourcetype	WinEventLog:Security
Event	Account_Name	-
		JMendoza1
	Message	An account was successfully logged S-1-5-21-1252493999-2771870793-34 mation: Process ID: 0x0 Process Nam LM only): - Key Length: 0 This event is or a local process such as Winlogon.e was logged on. The network fields inc entication information fields provide c Package name indicates which sub-p
	Source_Network_Address	192.168.10.100
Time	_time	2026-02-23T22:46:34.220+00:00
Default	index	endpoint
	linecount	70
	splunk_server	su1

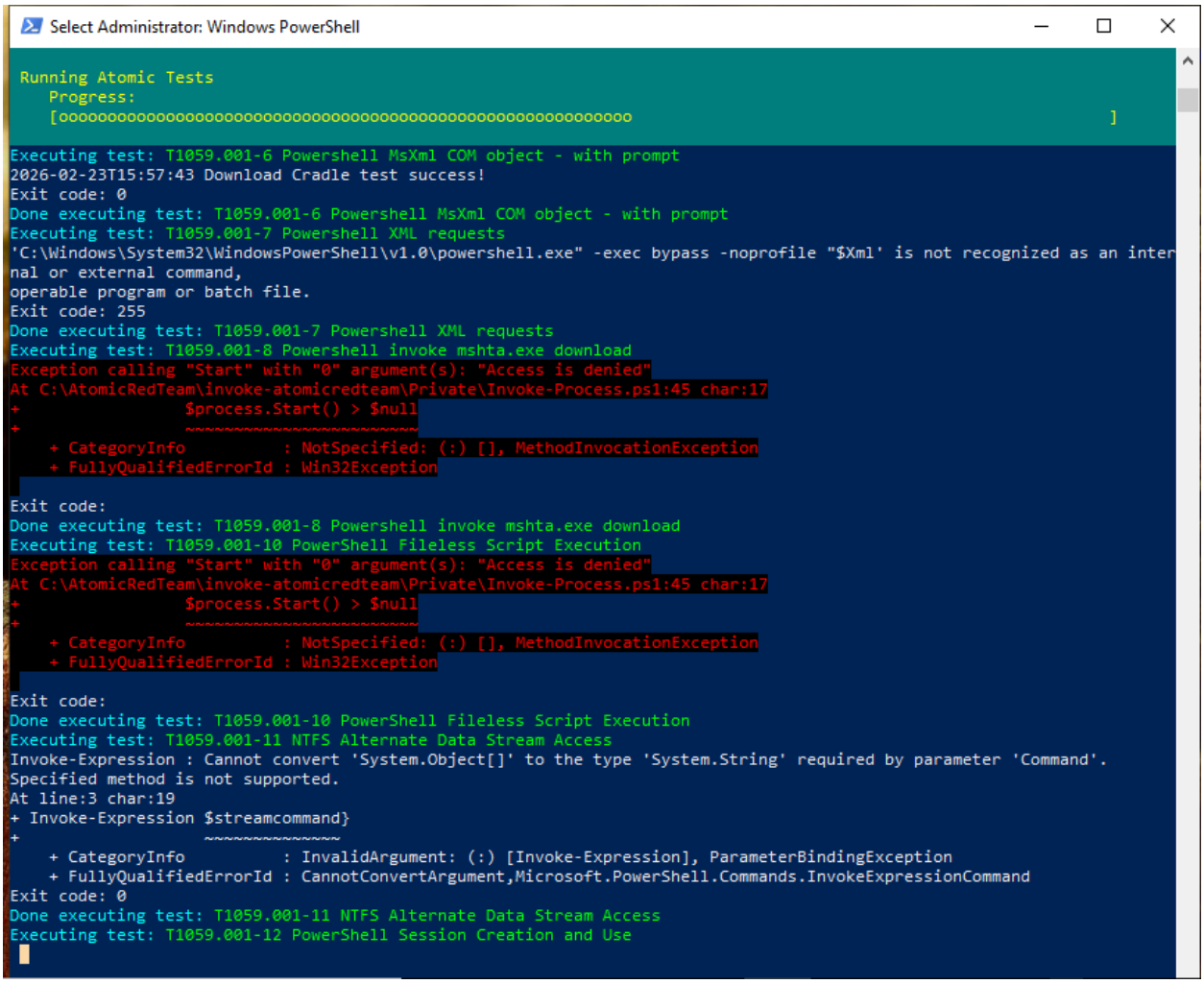
Targets Machine

i	Time	Event
	2/23/26 10:59:39.981 PM	02/23/2026 02:59:39.981 PM LogName=Security EventCode=4624 EventType=0 ComputerName=Target-PC.navs.local Show all 70 lines Event Actions ▾

Type	Field	Value
Selected	host ▾	Target-PC
	source ▾	WinEventLog:Security
	sourcetype ▾	WinEventLog:Security
Event	Account_Name ▾	-
		JMendoza1
	Message ▾	An account was successfully logged o -1-5-21-1252493999-2771870793-3466 ion: Process ID: 0x0 Process Name: - N NTLM V2 Key Length: 128 This event is e, or a local process such as Winlogon at was logged on. The network fields i uthentication information fields provide st. - Package name indicates which sul
	Source_Network_Address ▾	192.168.10.250
Time	_time ▾	2026-02-23T22:59:39.981+00:00
Default	index ▾	endpoint
	linecount ▾	70
	splunk_server ▾	su1

#8

Lastly I installed AtomicRedTeam to simulate a MITRE ATT&CK T1059.001(Malicious Powershell Command Executions) and verified the telemetry within Splunk.



#9

Splunk shows how this Telemetry test was displayed in the events section, it shows T1059.001 which is a type of abuse of powershell for malicious execution, in this instance there was nothing malicious related but it shows key things like asmi.dll which is used when bypassing security scanning to run scripts.

i	Time	Event
>	2/24/26 12:17:27.932 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-24T00:17:27.9321721Z'/><EventRecordID>21242</EventRecordI ta Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='U ='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4 a Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9 ata Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data>< host = Target-PC | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operationa | sourcety
>	2/24/26 12:11:56.932 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-24T00:11:56.9325700Z'/><EventRecordID>21185</EventRecordI ta Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='U ='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4 a Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9 ata Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data>< host = Target-PC | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operationa | sourcety
>	2/24/26 12:02:12.206 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-24T00:02:12.2063380Z'/><EventRecordID>20925</EventRecordI ta Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='U ='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4 a Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9 ata Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data>< host = Target-PC | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operationa | sourcety
>	2/24/26 12:02:05.312 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-24T00:02:05.3125575Z'/><EventRecordID>9158</EventRecordID ame='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTi ageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.20348.1 (Wi ='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=3E0854E036C75F2BB7F0817C9F7 me='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data><Data N host = ADDC01 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetyp
>	2/23/26 11:54:26.258 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-23T23:54:26.2585611Z'/><EventRecordID>20630</EventRecordI ta Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='U rm\4.18.26010.5-0\MsMpEng.exe</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.d ame='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>amsi.dll</Data>< 51D4D2</Data><Data Name='Signed'>true</Data><Data Name='Signature'>Microsoft Windows</D host = Target-PC | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operationa | sourcety
>	2/23/26 11:53:56.453 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider meCreated SystemTime='2026-02-23T23:53:56.4531613Z'/><EventRecordID>20509</EventRecordI ta Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='U ='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4 a Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9 ata Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data>< host = Target-PC | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operationa | sourcety