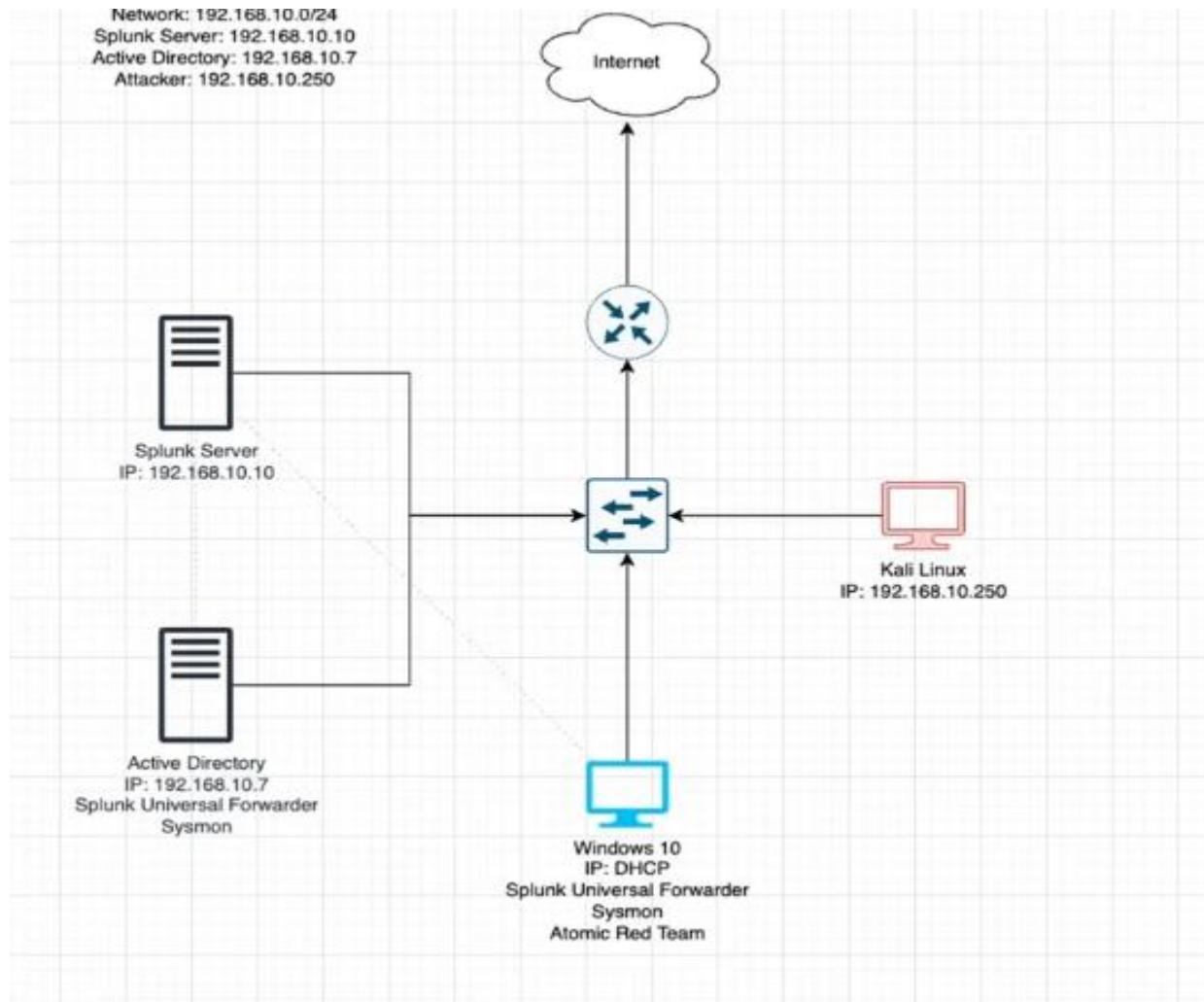


Active Directory Project

The lab environment consisted of Windows Server configured as a Domain Controller, multiple Windows client machines joined to the domain, Splunk for centralized log monitoring, and Kali Linux for security testing and attack simulation.

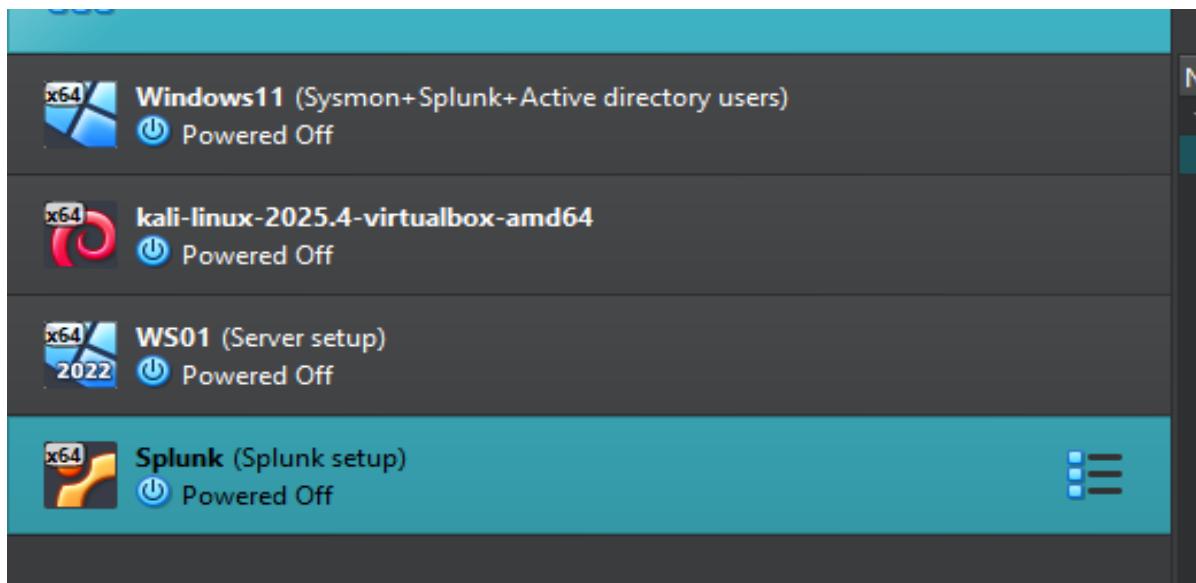
Active Directory was used to manage users, groups, and Group Policy Objects (GPOs). User accounts were created with different privilege levels to simulate real organizational roles. Security policies such as password complexity, account lockout policies, and access control rules were enforced through GPOs.

Splunk was integrated to collect and analyze Windows event logs, including authentication attempts, account changes, and security alerts. This enabled real-time monitoring and detection of suspicious activity such as failed login attempts and privilege escalation events.



Active Directory setup

Kali Linux was used to perform penetration testing techniques against the domain, including password attacks and enumeration, to evaluate the effectiveness of implemented security controls.

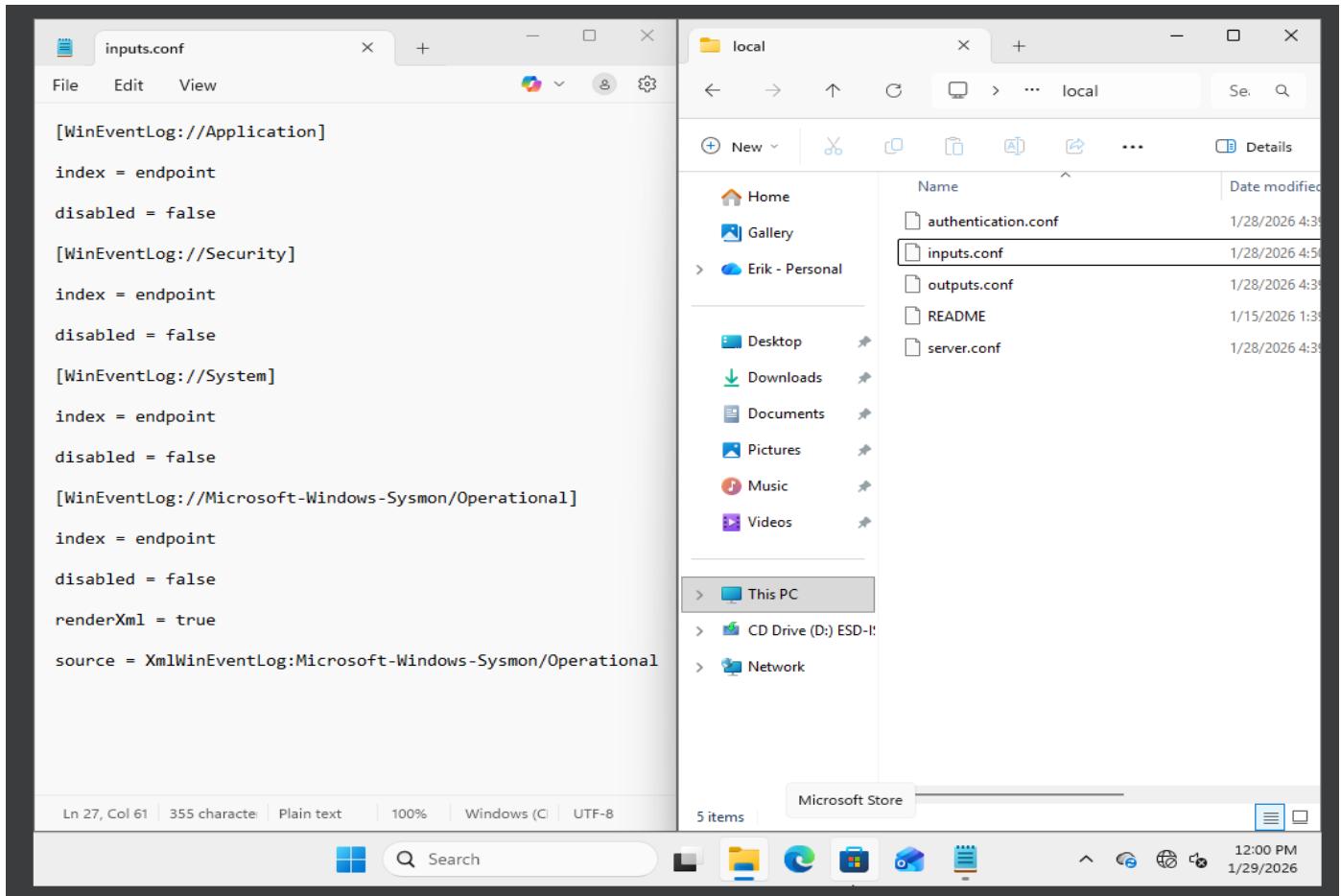


Virtual machines setup with snapshots

```
GNU nano 6.2                               /etc/netplan/00-installer-config.yaml *
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
        addresses: [8.8.8.8]
      routes:
        - to: default
          via: 192.168.10.1
  version: 2
```

The image shows the Netplan network configuration used to assign a static IP address to the Splunk server in the lab environment.

Splunk was configured with a static IP address (192.168.10.10/24) to ensure consistent and reliable connectivity with other systems, such as the Windows Server Domain Controller and Windows client machines. DHCP was disabled to prevent IP address changes that could disrupt log forwarding.



Splunk Universal Forwarder setup with an inputs.conf(For the targeted machine and the windows server) to define which logs or data sources should be monitored, specify where the logs are located (files, Windows Event Logs, directories, etc.) Control how often data is read, decide what data gets sent to Splunk.

Search | Splunk 10.2.0

Not secure 192.168.10.10:8000/en-US/app/search/search?q=search%20index%3D"endpoint"&sid... A Chat

index="endpoint" Time range: Last 24 hours

✓ 65,444 events (1/28/26 12:00:00.000 PM to 1/29/26 12:12:39.000 PM)

No Event Sampling ▾

Events (65,444) Patterns Statistics Visualization

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

Jan 28, 2026 12:00 PM Jan 29, 2026 1:00 PM

1,096 events at 6 PM on Wednesday, January 28, 2026
1 day 1 hour

Format Show: 20 Per Page View: List ▾

host X

Selected Yes No

2 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
TargetedPC	51,934	79.356%
WS01	13,510	20.644%

6:43:24.277 AM LogName=Security
EventCode=5379
EventType=0

< Hide Fields All Fields

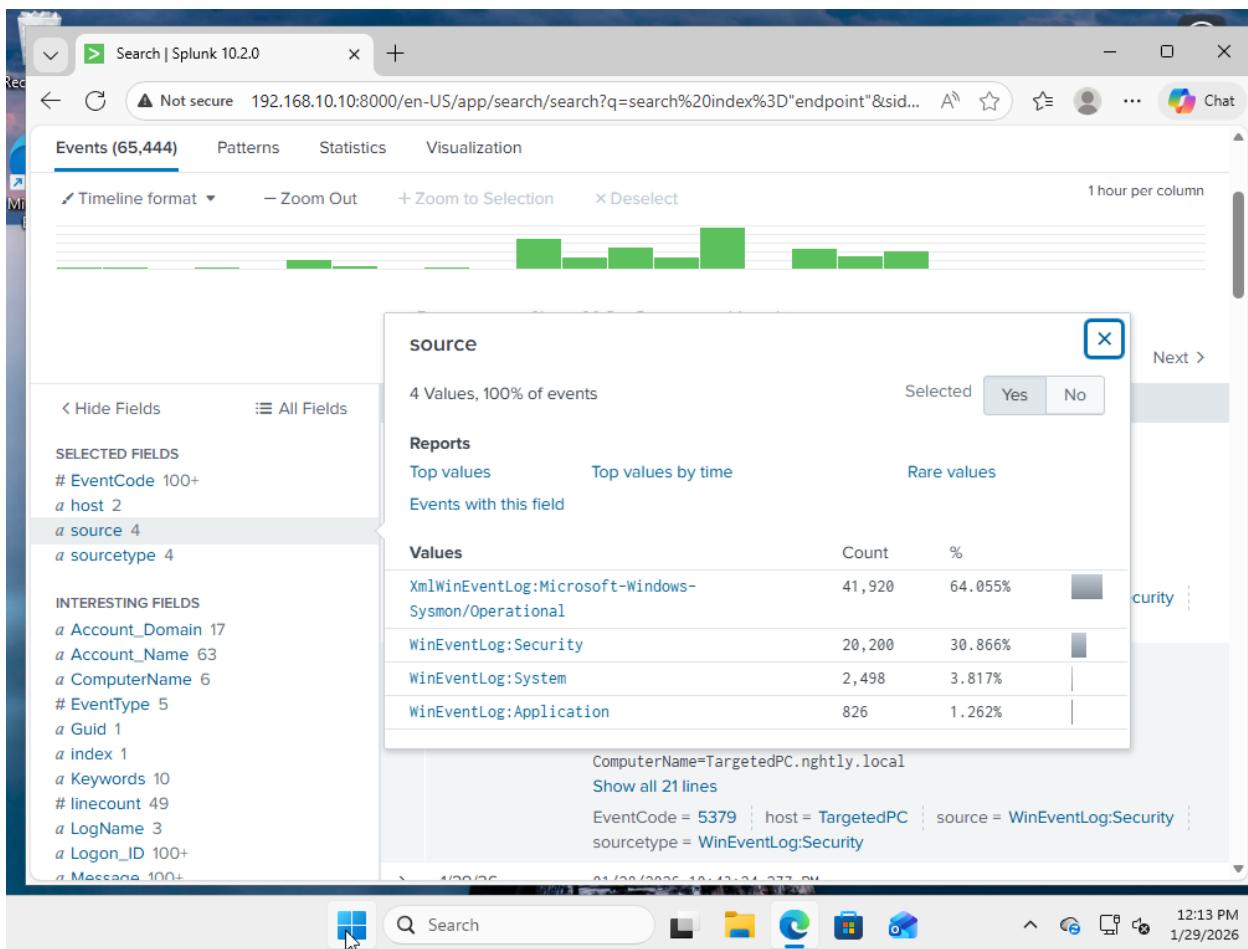
SELECTED FIELDS

- # EventCode 100+
- a host 2
- a source 4
- a sourcetype 4

INTERESTING FIELDS

- a Account_Domain 17
- a Account_Name 63
- a ComputerName 6
- # EventType 5
- a Guid 1
- a index 1

12:13 PM 1/29/2026



The images show the Splunk Search & Reporting interface, displaying events collected from the environment, and forwarded to the Splunk server.

The highlighted source field breakdown shows the origin of the collected logs. In this case, Splunk has received events from four main sources:

- **Microsoft-Windows-Sysmon/Operational** – most events, used for detailed system activity monitoring such as process creation and network connections
- **WinEventLog:Security** – Windows security logs, including authentication attempts and account-related events
- **WinEventLog:System** – system-level events related to services and OS behavior
- **WinEventLog:Application** – application-related logs

The event counts and percentages demonstrate that logs are being successfully forwarded from Windows hosts to Splunk

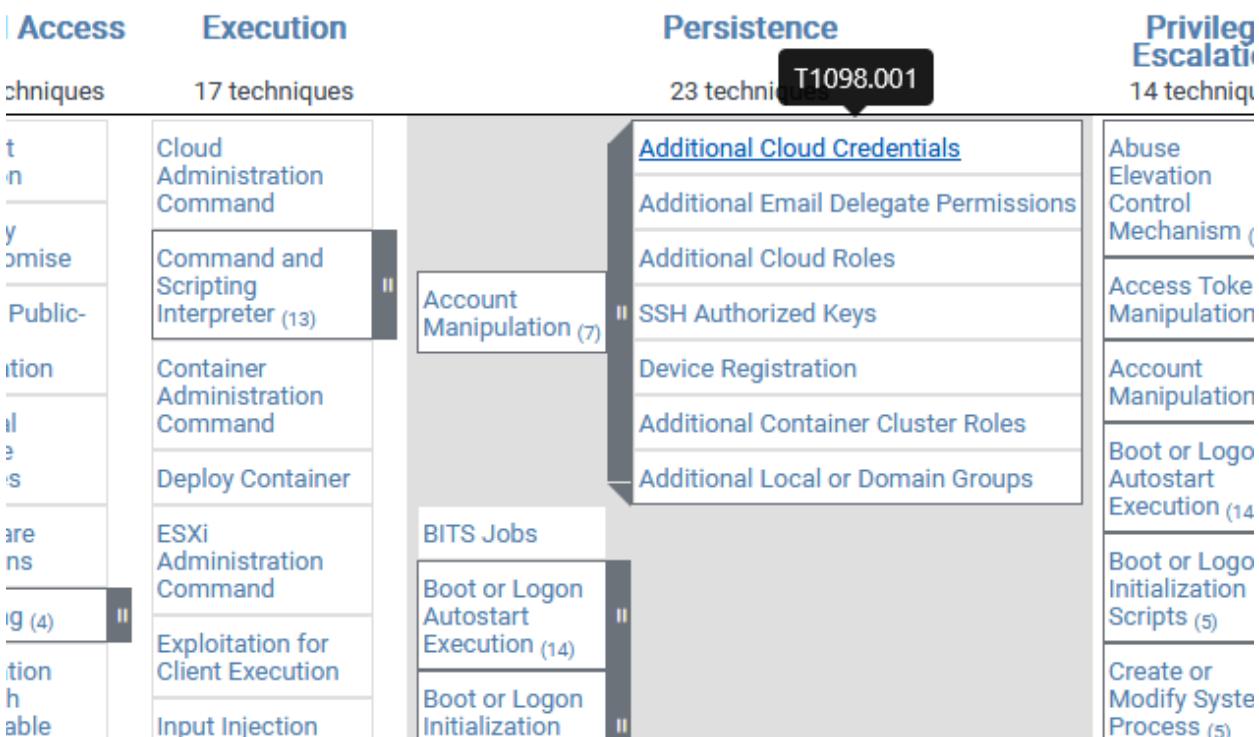
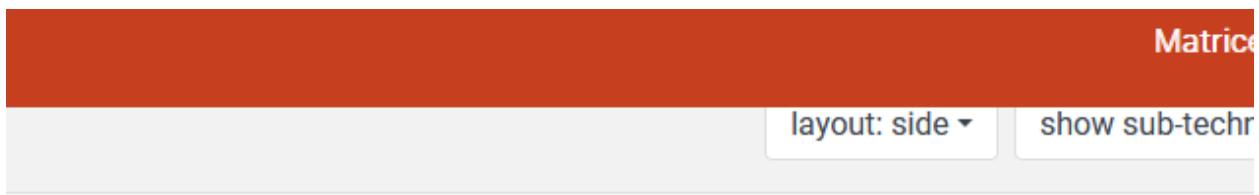
A screenshot of the Windows Server Manager interface. The left navigation pane shows 'Active Directory Users and Computers' under 'All Servers'. The main pane displays a table of users in the domain 'nightly.local'. One user, 'Steve Adams', is listed as a 'User'. The table has columns for Name, Type, and Description.

Name	Type	Description
Steve Adams	User	

Active Directory user's setup with passwords on a local server

A screenshot of a Windows desktop environment. The taskbar at the bottom shows the Start button, a search bar, and several pinned icons for File Explorer, Microsoft Edge, and other applications. A user profile for 'Steve Adams' is displayed in the top right corner, indicating they are currently signed in. The background of the desktop is a scenic view of green hills and blue water.

User logged on the targeted domain



ITRE ATT&CK Enterprise Matrix, and it's essentially a map of how attackers operate, step by step, once they target an environment like Active Directory.

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Invoke-AtomicTest T1053.005
PathToAtomsicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-1 Scheduled Task Startup Script
SUCCESS: The scheduled task "T1053_005_OnLogon" has successfully been created.
SUCCESS: The scheduled task "T1053_005_OnStartup" has successfully been created.
Exit code: 0
Done executing test: T1053.005-1 Scheduled Task Startup Script
Executing test: T1053.005-2 Scheduled task Local
SUCCESS: The scheduled task "spawn" has successfully been created.
Exit code: 0
Done executing test: T1053.005-2 Scheduled task Local
Executing test: T1053.005-3 Scheduled task Remote
ERROR: No mapping between account names and security IDs was done.
Exit code: 1
Done executing test: T1053.005-3 Scheduled task Remote
Executing test: T1053.005-4 Powershell Cmdlet Scheduled Task
TaskPath                               TaskName           State
-----                               -----           -----
\\                                         AtomicTask        Ready
Exit code: 0
Done executing test: T1053.005-4 Powershell Cmdlet Scheduled Task
Executing test: T1053.005-5 Task Scheduler via VBA
New-Object : Retrieving the COM class factory for component with CLSID {00000000-0000-0000-0000-000000000000} failed
At line:70 char:12
+     $app = New-Object -ComObject "$officeProduct.Application"
+     ~~~~~~: ResourceUnavailable: () [New-Object], COMException
+     FullyQualifiedErrorMessage : NoCOMClassIdentified,Microsoft.PowerShell.Comma
```

Scheduled task attack

The screenshot shows the Splunk web interface. At the top, there's a search bar with the query "index=windows EventCode=4698". Below the search bar, it says "0 events (before 1/29/26 12:59:01.000 PM)" and "No Event Sampling". The main area displays the message "No results found." There are tabs for "Events (0)", "Patterns", "Statistics", and "Visualization". At the bottom right, there's a small "Outlook" button.

Splunk showcasing that we're not protected against a scheduled task attack