AD_HOME_LAB_PROJECT

DOCUMENTATION

TABLE OF CONTENTS

INTRODUCTION

Presenting AD
Presenting SIEM
Project Overview
Workflow
Environment

PHASE 1

Preparing Window's VM
Preparing Kali Linux VM
Preparing Ubuntu Server
Preparing Windows Server

PHASE 2

Install & Configure
Sysmon & Splunk
on Windows VM &
Windows server

PHASE 3

Install & configure
Active Directory on
Windows Server
and promoting it to
Domain Controller
And adding users to
new Domain

PHASE 4

Brute Force Attack
using Kali linux
Install & Configure
AtomicRedTeam

SUMMARY

ANNEX

INTRODUCTION

MODULE 1

What is Active Directory?

Active Directory (AD) is a Microsoft directory service that centralizes user and resource management in Windows networks. It provides authentication, authorization, and policy enforcement for users and devices. AD allows administrators to efficiently manage security and resources across the organization.

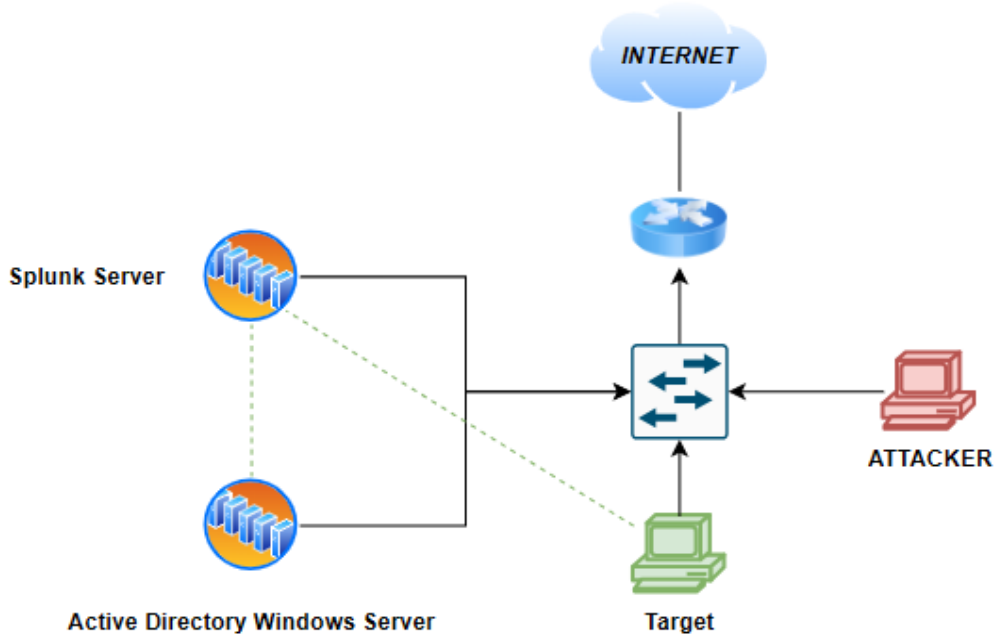
What is SIEM ?

SIEM (Security Information and Event Management) is a cybersecurity solution that aggregates and analyzes security data from various sources within an organization in real-time. It helps identify potential threats by correlating logs and events, providing insights for incident response and compliance. SIEM tools enhance security posture by enabling proactive monitoring, alerting, and reporting on security incidents.

Project Overview:

In this project, a Windows Server was configured with Active Directory and integrated with a SIEM (Splunk) for real-time telemetry updates. An attack scenario was simulated using Atomic Red Team, generating event logs in the SIEM, such as multiple failed login attempts. This setup enabled the detection of potential threats and facilitated rapid response actions by the security team.

Workflow:



Environment

This Active Directory Home Lab project utilizes a combination of virtualization, Active Directory, security information and event management (SIEM) platform, and simulated threat tools (Atomic Red Team). Here's a detailed look at each component:

1. Windows VM [TARGET]:

- Operating System: Windows 10 Enterprise (version can be specified, e.g., Windows 22H2)
- Purpose: Acts as the target endpoint for attacker (KALI LINUX)

2. VirtualBox:

- Type: Open-source hypervisor for x86 virtualization
- Purpose: Hosts the virtual machines
- Benefits: Allows for isolated testing environment, easy snapshot and rollback capabilities

3. Kali Linux [ATTACKER]:

- Operating System: Ubuntu (64-bit)
- Purpose: Acts as the attacker, performing login attempts on the target machine to test security defenses and assess vulnerabilities.

4. Windows Server:

- Operating System: Windows 2022
- Purpose: Provides a centralized platform for managing Active Directory

5. Splunk Server:

- Operating System: Ubuntu Server (version can be specified e.g. Ubuntu 24.04.1)
- Purpose: Centralise Log management and analysis

Conclusion

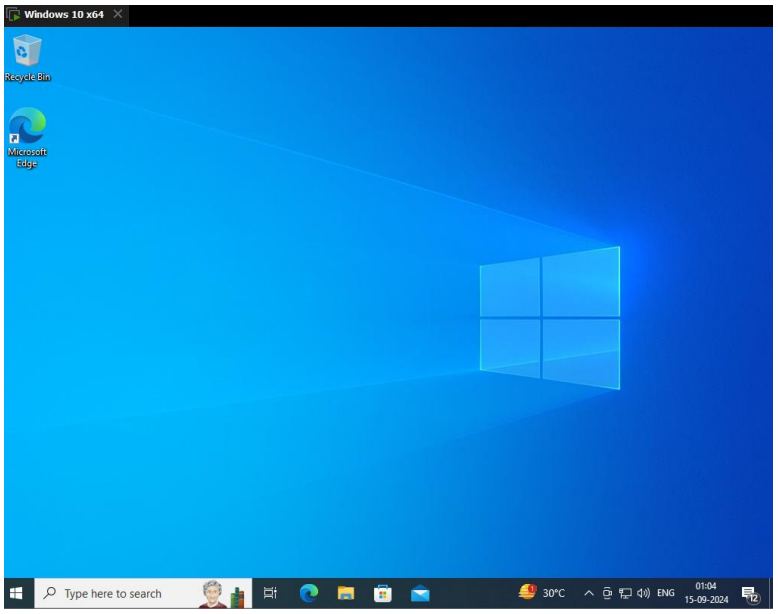
In conclusion, this Active Directory project establishes a solid foundation for centralized user management and security monitoring. By integrating Active Directory with a SIEM system, the environment enables effective logging and analysis of security events, facilitating the detection of potential threats. The simulated attack scenarios provide practical insights into vulnerabilities, while the real-time telemetry updates enhance situational awareness. Overall, this setup empowers the security team to proactively manage risks and respond swiftly to incidents, ensuring a robust security posture for the organization.

PHASE 1

MODULE 2

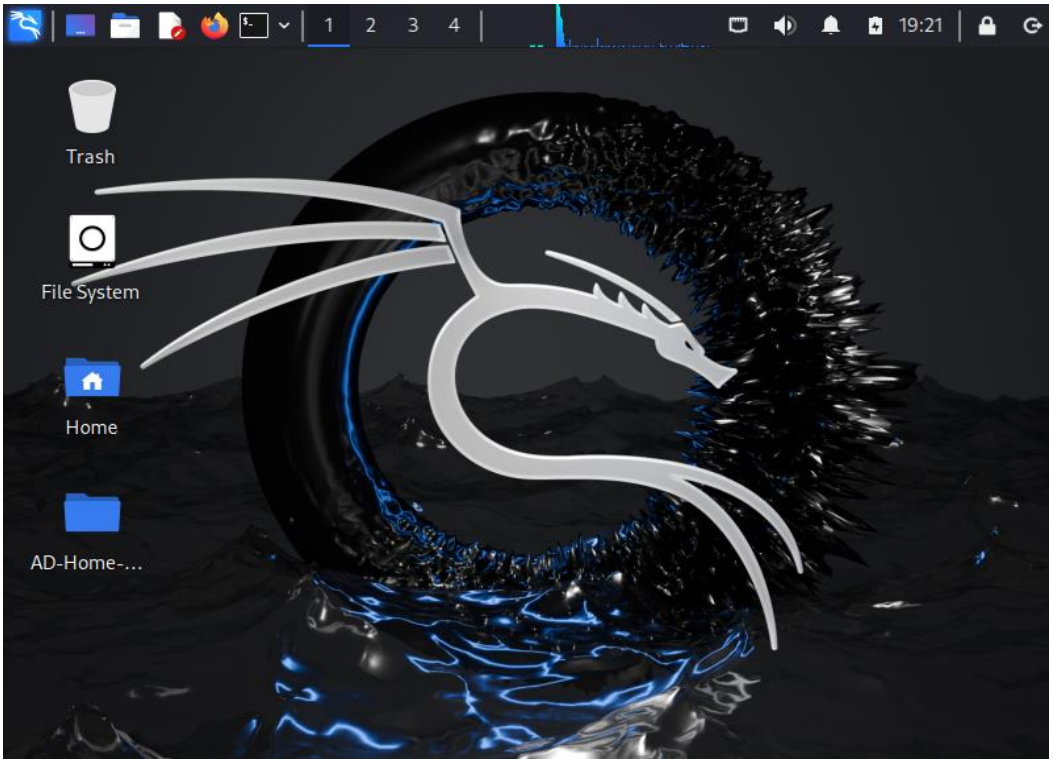
Preparing Windows VM

- Install Windows VM on VirtualBox (https://www.microsoft.com/en-in/software-download/windows10)
- Ensure the system is updated



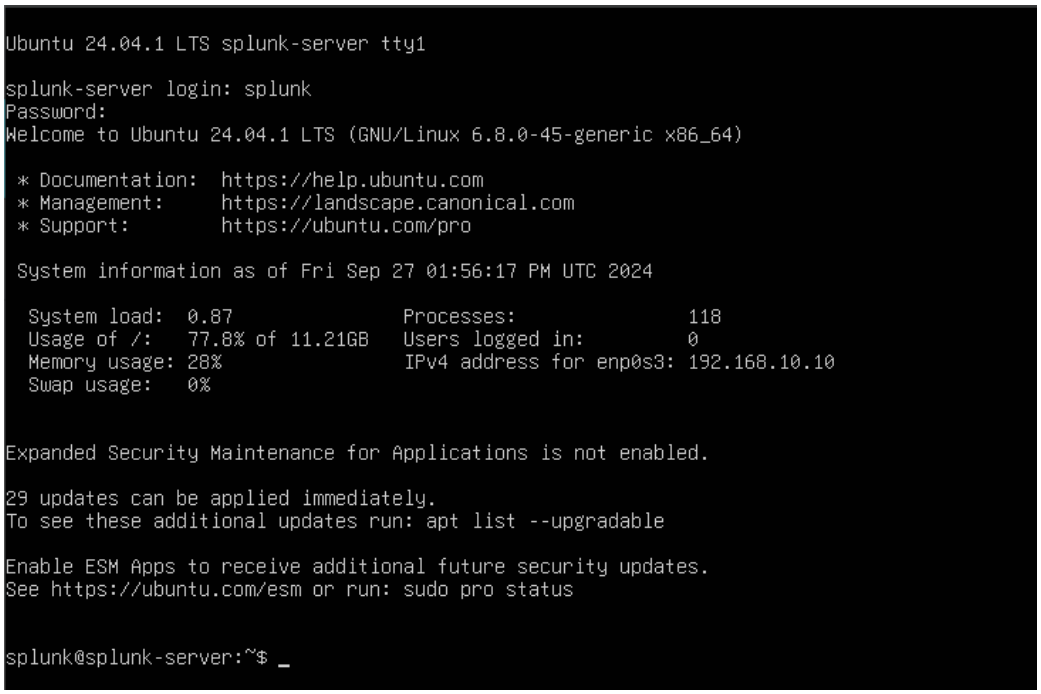
Preparing Kali Linux VM

- Install Kali Linux VM on VirtualBox (https://www.kali.org/get-kali/#kali-installer-images)
- Ensure the system is updated



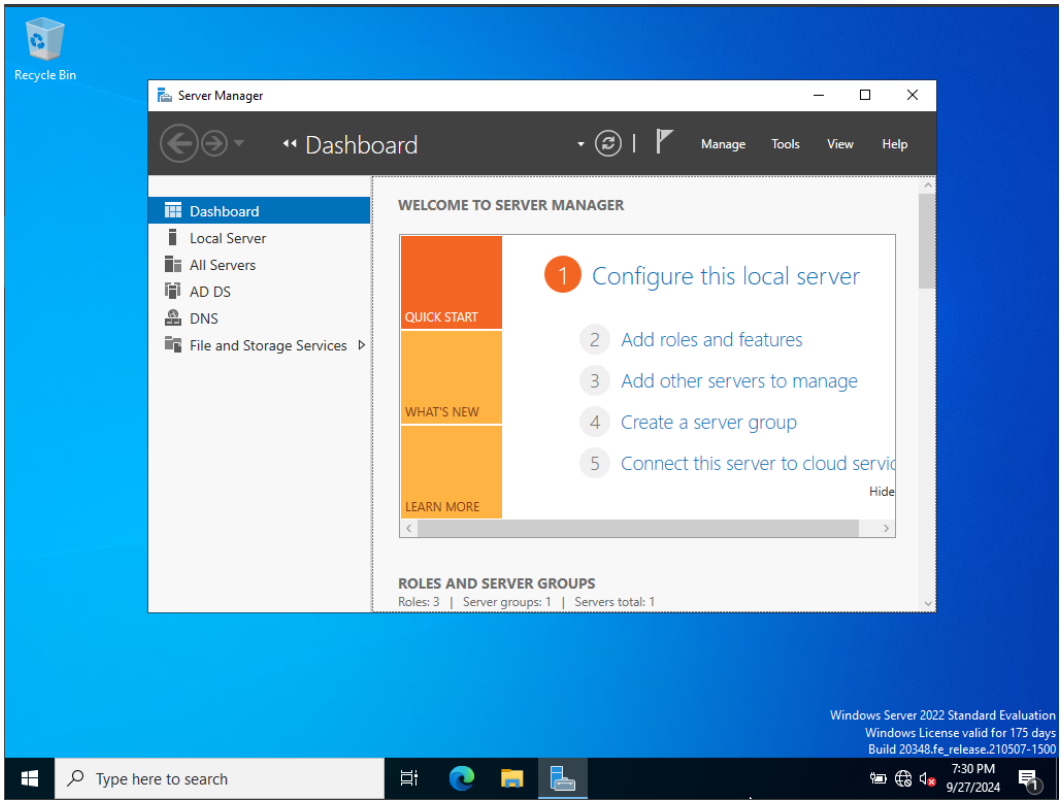
Preparing Ubuntu Server

- Install Ubuntu Server on VirtualBox (https://ubuntu.com/download/server)
- Ensure the system is updated



Preparing Windows Server

- Install Windows Server on VirtualBox (Windows Server 2022 | Microsoft Evaluation Center)
- Ensure the system is updated



PHASE 2

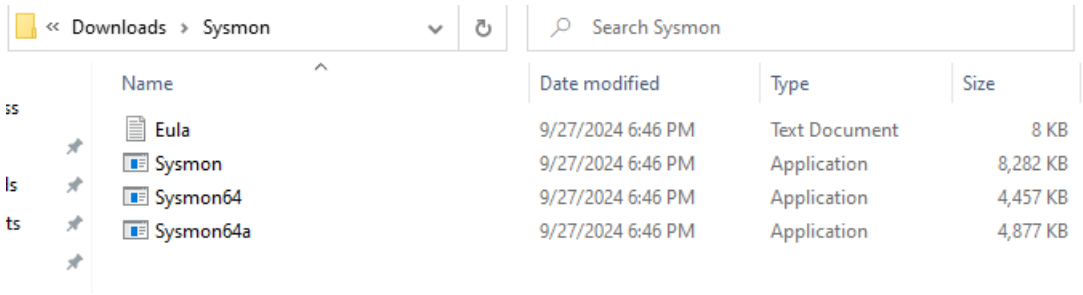
MODULE 3

Introducing Sysmon

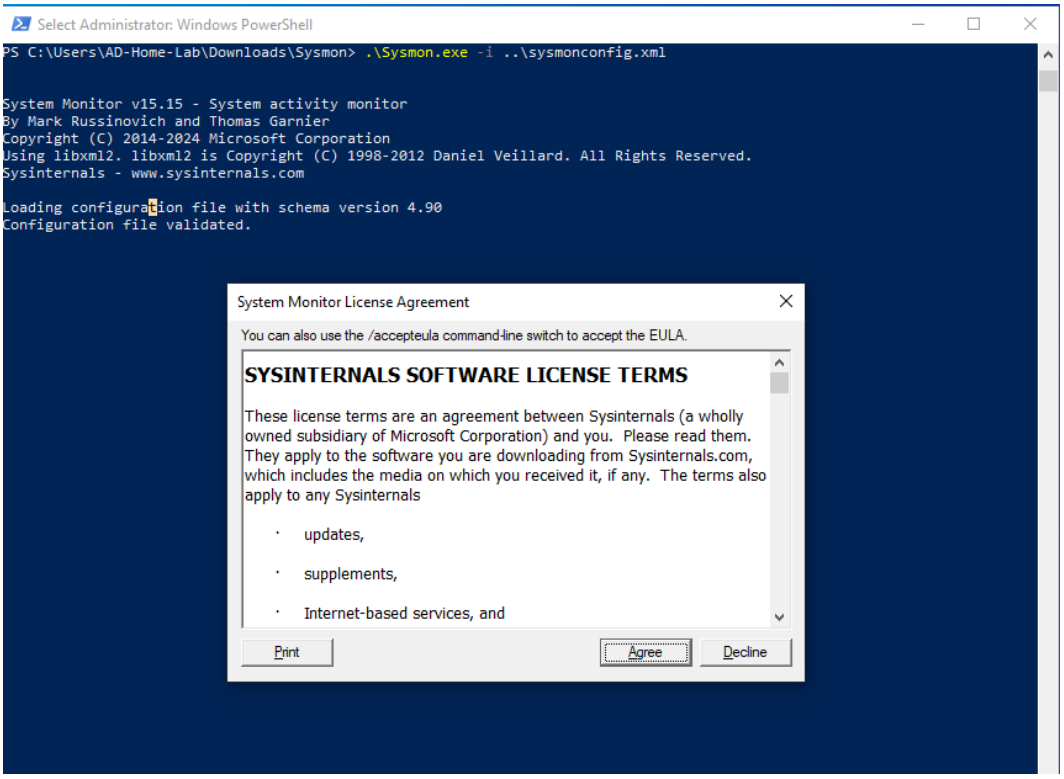
- Sysmon (System Monitor) is a Windows service that logs detailed system activity to the event log, including process creations, network connections, and file modifications. It enhances security monitoring by providing valuable data for threat detection and forensic analysis. This tool is crucial for understanding and investigating suspicious behavior on a system.

Setting up Sysmon

- Download Sysmon from its official page (Sysmon - Sysinternals | Microsoft Learn)
- Extract it



- Now we'll be using olaf sysmon config (https://raw.githubusercontent.com/olafhartong/sysmon-modular/refs/heads/master/sysmonconfig.xml)
- Execute ".\Sysmon.exe -i ..\sysmonconfig.xml" in powershell and install sysmon

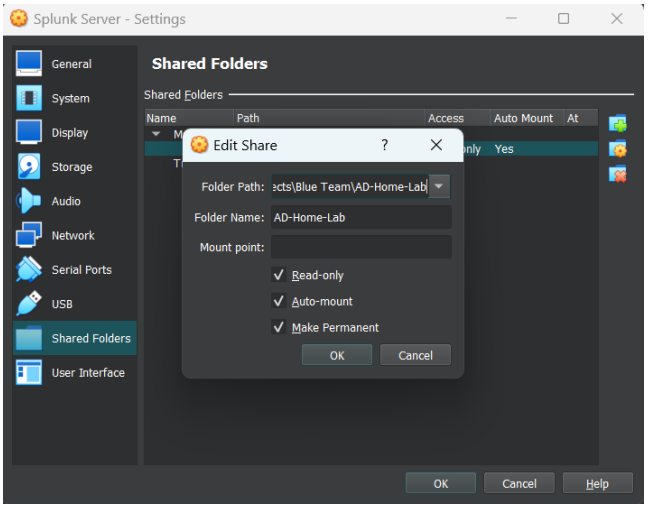


Introducing Splunk (SIEM)

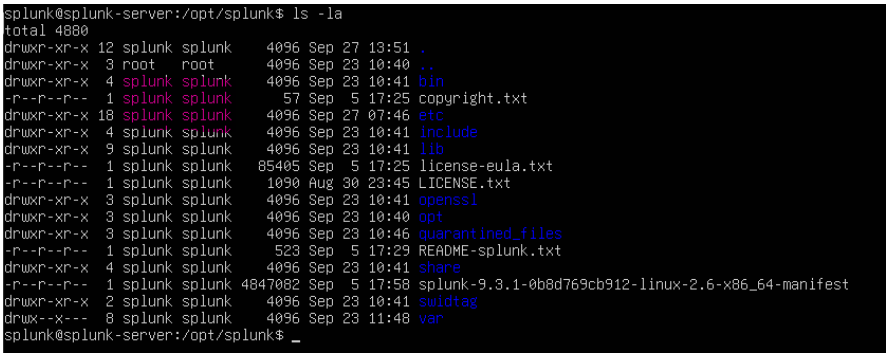
- Splunk is a powerful data analytics platform designed for searching, monitoring, and analyzing machine-generated data in real-time. It enables organizations to collect and index large volumes of data from various sources, providing insights through visualization and reporting tools. Splunk is widely used for security information and event management (SIEM), operational intelligence, and business analytics.

Setting up Splunk on Ubuntu Server

- Download virtualbox-guest-additions-iso, virtualbox-guest-utils on ubuntu server using command “sudo apt-get install virtualbox-guest-additions-iso virtualbox-guest-utils”
- Now, we’ll be using shared folders



- Add our user to group ‘vboxsf’, command: “sudo adduser {USER_NAME} vboxsf”
- Now, we have to mount our shared folder to newly created directory ‘share’
- Command: sudo mount -t vboxsf -o uid=1000, gid=1000 {SHARE_FOLDER_NAME} share/
- Now, navigate to share directory and run command: “sudo dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb” as if it doesn’t run that means you need to reboot system to share folder take effect.
- Navigate to /opt/splunk and run “ls -la”, owner of this directory is splunk



```
splunk@splunk-server:/opt/splunk$ ls -la
total 4880
drwxr-xr-x 12 splunk splunk    4096 Sep 27 13:51 .
drwxr-xr-x  3 root   root      4096 Sep 23 10:40 ..
drwxr-xr-x  4 splunk splunk    4096 Sep 23 10:41 bin
-r--r--r--  1 splunk splunk      57 Sep  5 17:25 copyright.txt
drwxr-xr-x 18 splunk splunk    4096 Sep 27 07:46 etc
drwxr-xr-x  4 splunk splunk    4096 Sep 23 10:41 include
drwxr-xr-x  9 splunk splunk    4096 Sep 23 10:41 lib
-r--r--r--  1 splunk splunk   85405 Sep  5 17:25 license-eula.txt
-r--r--r--  1 splunk splunk    1090 Aug 30 23:45 LICENSE.txt
drwxr-xr-x  3 splunk splunk    4096 Sep 23 10:41 openssl
drwxr-xr-x  3 splunk splunk    4096 Sep 23 10:40 opt
drwxr-xr-x  3 splunk splunk    4096 Sep 23 10:46 quarantined_files
-r--r--r--  1 splunk splunk     523 Sep  5 17:29 README-splunk.txt
drwxr-xr-x  4 splunk splunk    4096 Sep 23 10:41 share
-r--r--r--  1 splunk splunk 4847082 Sep  5 17:58 splunk-9.3.1-0b8d769cb912-linux-2.6-x86_64-manifest
drwxr-xr-x  2 splunk splunk    4096 Sep 23 10:41 swidtag
drwx--x---  8 splunk splunk    4096 Sep 23 11:48 var
splunk@splunk-server:/opt/splunk$ _
```

- Now, we login to splunk user by “sudo -u splunk bash”
- Navigate to /bin and run “./splunk start”
- It would run splunk installer and typr ‘y’ to accept aggrement and splunk gets installed.
- Now, to enable boot-start for splunk on ubuntu server, firstly log out as splunk user and navigate to /bin and run command: “sudo ./splunk enable boot-start -user splunk”

Introducing Splunk Universal Forwarder (SUF)

- The Splunk Universal Forwarder is a lightweight agent that collects and forwards log data from various sources to a Splunk instance for indexing and analysis. It operates with minimal resource usage, making it ideal for deployment across multiple servers and environments. The Universal Forwarder ensures efficient and secure data transmission, enabling real-time visibility into system performance and security events.

Setting up SUF on Windows VM & Win - Server

- Download Splunk Universal Forwarder ([Download Universal Forwarder for Remote Data Collection | Splunk])
- Install it and when prompted for receiving indexer

IP: {YOUR_SPLUNK_SERVER_IP} PORT: 9997

In our case, IP: 192.168.10.10

IMPORTANT

- We need to configure a inputs.conf for Splunk Universal Forwarder
- Location: C:\Program Files\SplunkUniversalForwarder\etc\system\local
- First open Notepad as Adminisrator and save this file at Location

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

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

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

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
```

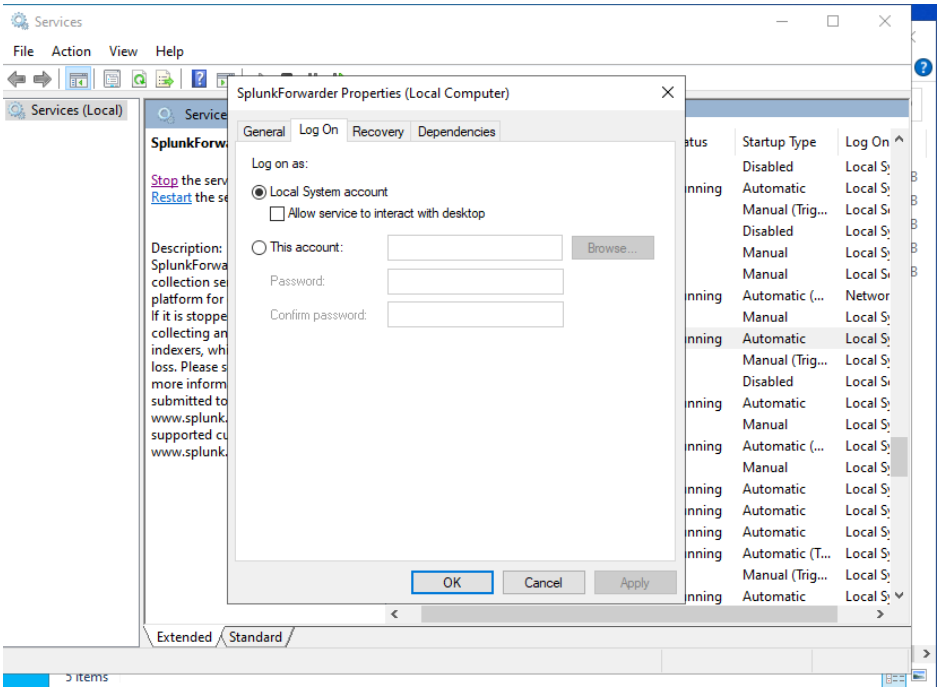
index = endpoint

disabled = false

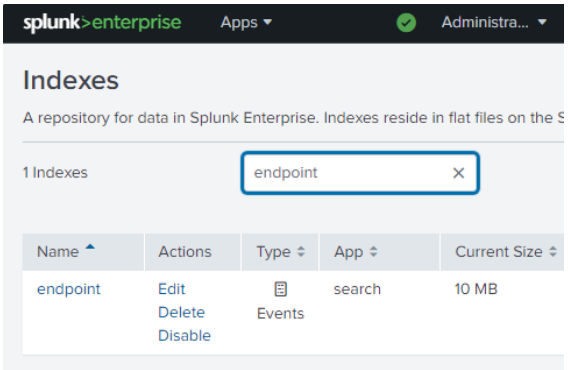
renderXml = true

source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

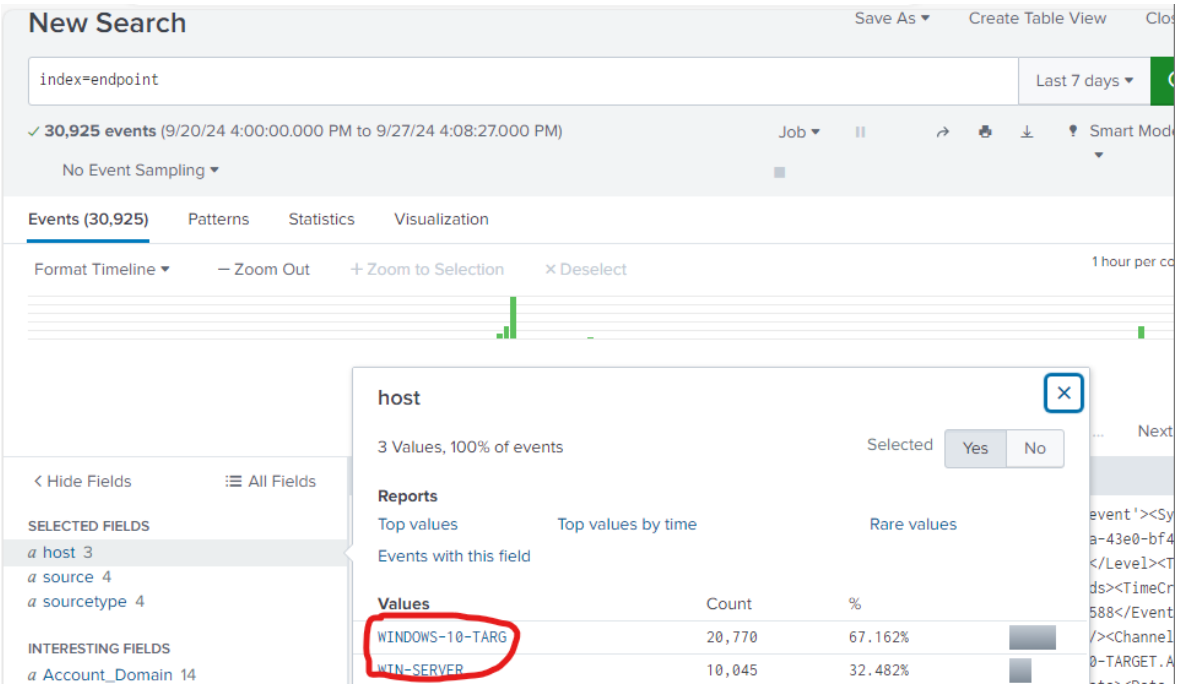
- Go to services app and change SplunkForwarder log on to as local system.
- And restart splunk service



- Now, we log in to our splunk web interface at http://192.168.10.10:8000 and login to our account
- Navigate to Settings→Indexes, create new index named “endpoint”



- Navigate to Settings→Forwarding and receiving→Configure receiving, click on new receiving and listen to port 9997.



- We got event logs in splunk from both our Windows VM [TARGET] and Windows Server,

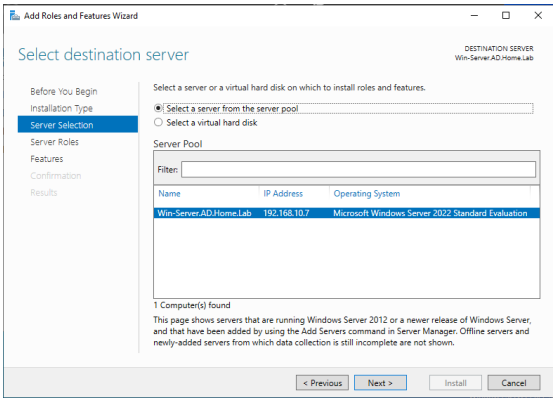
  [The steps to setup Splunk Universal Forwarder and sysmon on windows server are same as on windows vm.]

PHASE 3

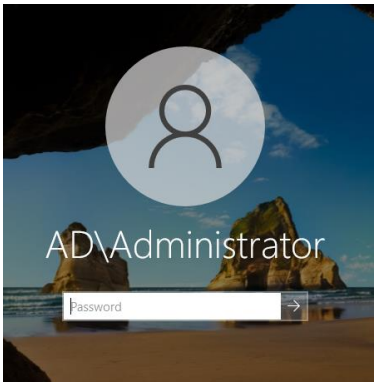
MODULE 4

Setting up Active Directory

- Navigate to Manage→Add Roles and Features



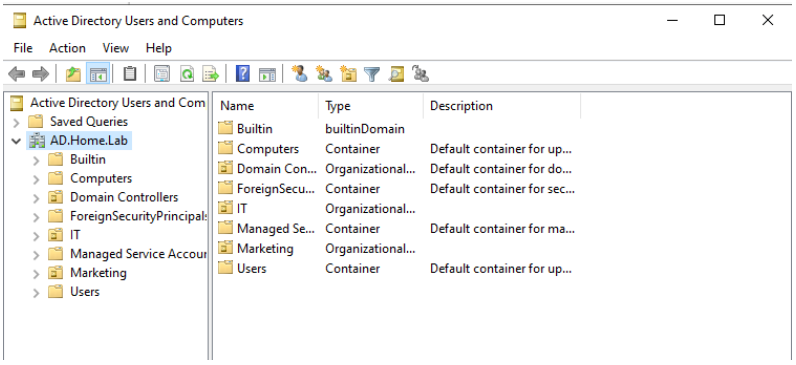
- Server Roles→check Active Directory Domain Services and click next and install
- Click on Flag icon on home page of Service Manager and click on promote to Domain Controller.
- Choose Add a Forest and give a domain name, in our case it's 'AD.Home.Lab' and install



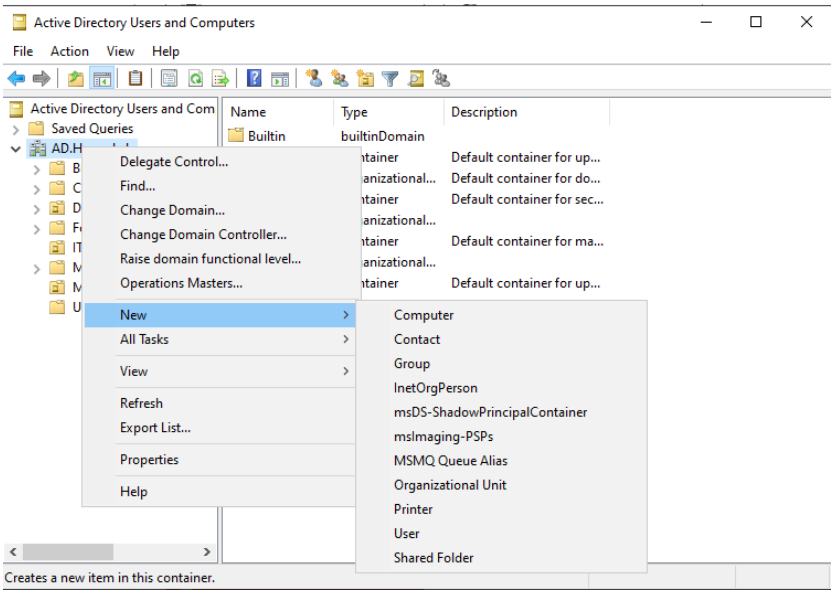
- Domain successfully configured

Adding Users in Domain

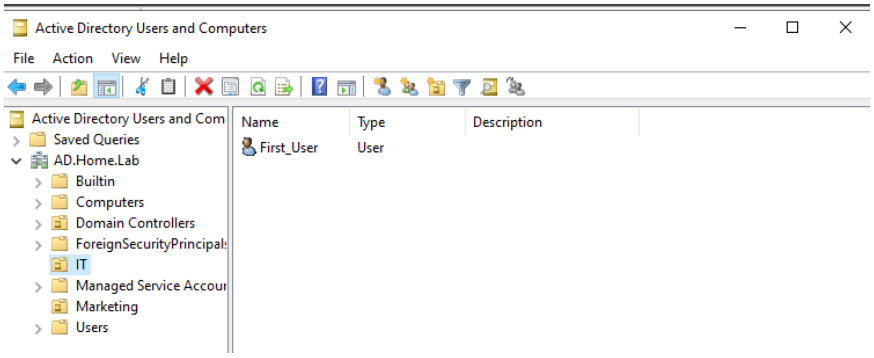
- Navigate to Tools→Active Directory Users and Computers



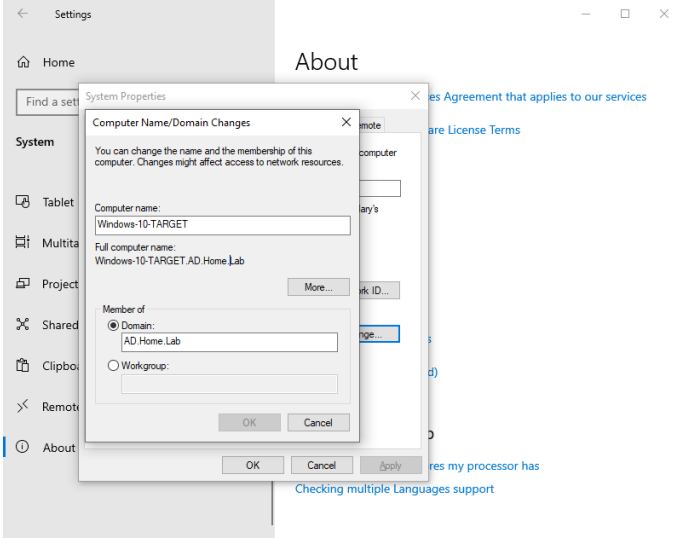
- Now, we can make Organizational units by right clicking on domain (OPTIONAL we can also add users straight forward but in real-world scenarios organization will have multiple departments)



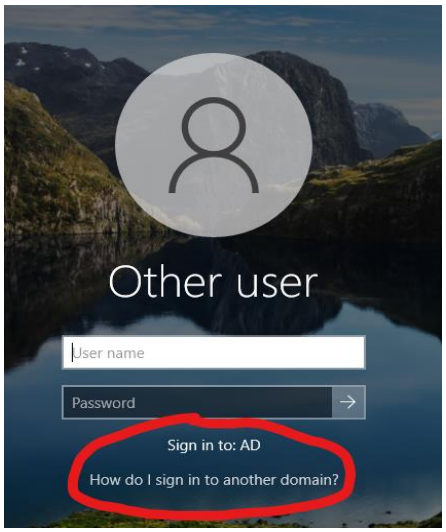
- For now, we made two organizational units IT and marketing each having one user

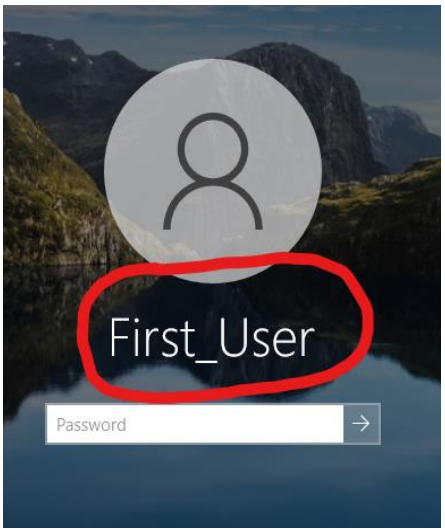


- Now, we change Computer Name/Domain changes to Member of Domain: AD.Home.Lab (Only available in Windows Enterprise) and remember to change DNS of this machine to our Domain Controller i.e. 192.168.10.7



- We successfully added our newly created users to our Domain





PHASE 4

MODULE 5

Brute Force Attack using Kali Linux

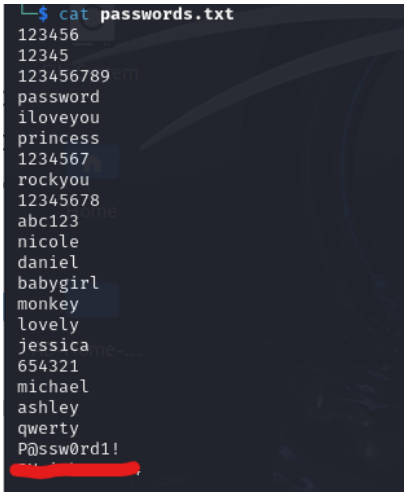
- A brute force attack using Kali Linux involves systematically trying numerous password combinations to gain unauthorized access to a system. Crowbar is a tool specifically designed for this purpose, allowing attackers to automate the process against various services. It supports multiple protocols and can leverage both dictionary and brute force methods to crack passwords efficiently.

Requirements

- Crowbar: Crowbar is a penetration testing tool used to perform brute force attacks against various services by automating password guessing techniques.
- Rockyou wordlist: The Rockyou wordlist is a popular collection of over 14 million passwords originally extracted from a data breach of the Rockyou social networking application. It is commonly used in password cracking and security testing to enhance brute force and dictionary attack efforts.

Setting up Attack

- First, we need to install crowbar on kali linux using command: “sudo apt-get install -y crowbar”, remember to update and upgrade your kali linux before running this.
- Now we, gonna use rockyou.txt as our password file but just to inform the password set by us doesn’t seem tto be in rockyou.txt. So, just to mimic real-world scenario we took some passwords from rockyou.txt and appended into a new file ‘passwords.txt’ and also added our passord { OUR_PASSWORD_OF_TARGET_MACHINE } in it.



- For Brute Force Attack to work, we need to enable remote desktop in our target machine in our case Windows 10
- Navigate to Settings→About→Advance System Settings→Remote→Allow Remote Connections, and add users to it i.e First_user_it and First_user_marketing.

- Run Command: “crowbar -b rdp -u first_user_marketing -C passwords.txt -s 192.168.10.100/32”

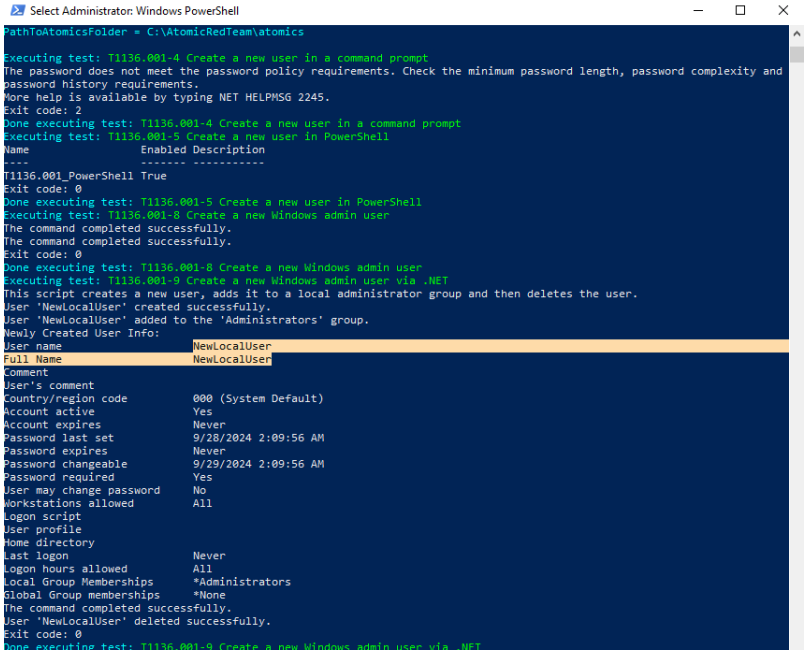
```
2024-09-27 12:57:27 START
2024-09-27 12:57:27 Crowbar v0.4.2
2024-09-27 12:57:27 Trying 192.168.10.100:3389
2024-09-27 12:57:33 RDP-SUCCESS : 192.168.10.100:3389 - first_user_marketing:[redacted]
```

Atomic Red Team (ART)

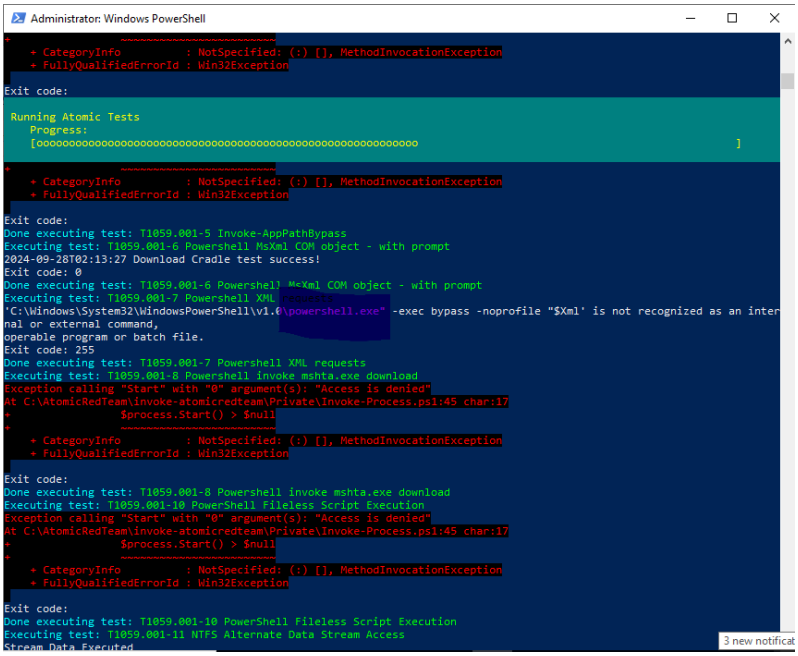
- Atomic Red Team is a collection of small, highly portable testing tools designed to simulate various tactics and techniques used by adversaries in cybersecurity. It provides security teams with a framework to validate their detection and response capabilities against known threats. The tests are based on the MITRE ATT&CK framework, enabling organizations to assess their defenses effectively.

Setting up on Windows 10 [TARGET]

- Open Powershell as administrator, type command: “Set-ExecutionPolicy Bypass CurrentUser” and type ‘y’
- Now, before starting to install ART set an exclusion for entire ‘C:\’ otherwise windows defender will remove files from ART framework after install.
- Install ART by typing commands in powershell:
  - IEX (IWR ‘raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/refs/heads/master/install-atomicredteam.ps1’ -UseBasicParsing);
  - Install-AtomicRedTeam -getAtomics
- Run AtomicRedTeam: “Invoke-Atomic Test T1136.001” (for clearity T1136 is for Creating Account) and more information at MITRE ATT&CK®



- We doing one more AtomicTest T1059.001 (For Powershell) for more information MITRE ATT&CK®



```
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : Win32Exception

Exit code:

 Running Atomic Tests
    Progress:
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                        ]

+                 ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
    + FullyQualifiedErrorId : Win32Exception

Exit code:
Done executing test: T1059.001-5 Invoke-AppPathBypass
Executing test: T1059.001-6 Powershell MsXml COM object - with prompt
2024-09-28T02:13:27 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 [redacted]
'C:\Windows\System32\WindowsPowerShell\v1. -exec bypass -noprofile "$Xml' is not recognized as an inter
nal 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
Stream Data Executed
```

SUMMARY

This project demonstrates the integration of Active Directory with a Security Information and Event Management (SIEM) system, specifically Splunk, to enhance real-time threat detection and response capabilities. The key components and workflow are as follows:

1. Environment:

- Windows VM running on VirtualBox, simulating a target
- Kali Linux VM running on VirtualBox, simulating an attacker
- Configured Active Directory on Windows server on VirtualBox
- Ubuntu Server running Splunk (SIEM) on VirtualBox

2. Workflow:

- Target machine and Windows Active Directory Server sends telemetry to Splunk server
- Crowbar is used to simulate a Brute Force attack
- AtomicRedTeam also used to test various attacks
- Telemetry received on Splunk web interface

3. Key Achievements:

- Successfully set up Active Directory on Windows Server for efficient user management
- Integrated Splunk for real-time telemetry, enhancing monitoring capabilities
- Conducted realistic attack scenarios using Atomic Red Team, generating critical telemetry data
- Enabled timely identification of potential threats through comprehensive event analysis
- Equipped the security team to implement swift response actions based on detected anomalies

4. Benefits:

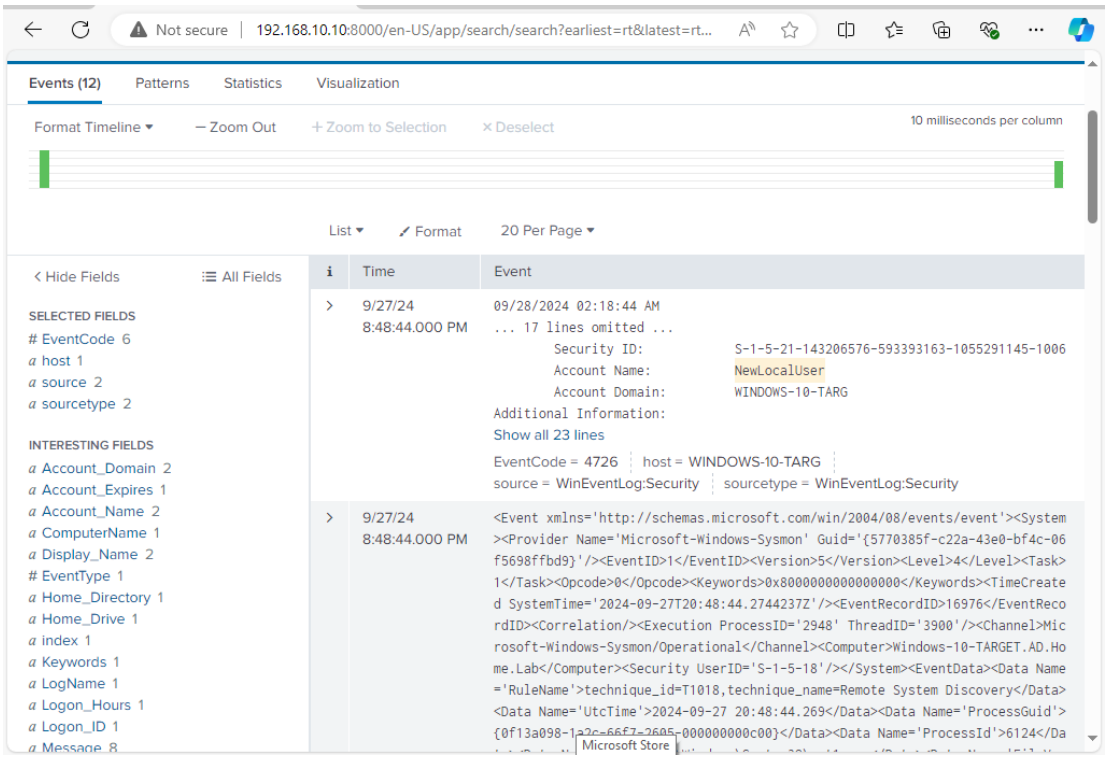
- Enhanced ability to detect and respond to potential threats in real time
- Consolidation of event telemetry in Splunk streamlines incident detection and analysis
- Simulation of attacks allows for identification of vulnerabilities before they can be exploited
- Rapid response capabilities minimize the impact of security incidents
- The integration can easily adapt to growing organizational needs and additional security tools

This project demonstrates the effectiveness of integrating Active Directory with a SIEM system to build a more responsive and robust cybersecurity infrastructure. By automating telemetry collection and providing clear workflows, it enhances the organization's ability to detect, analyze, and respond to threats quickly and consistently.

ANNEX

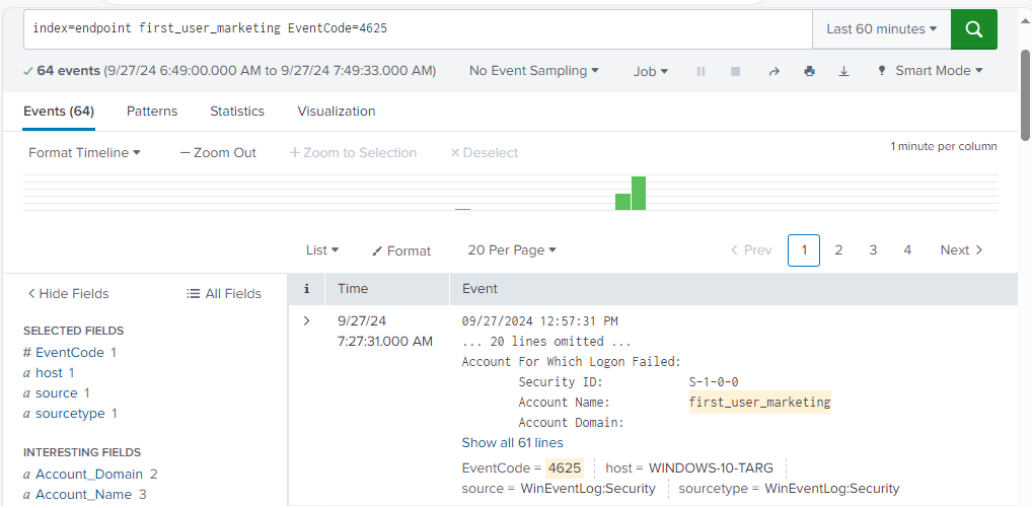
The Telemetry view on Splunk (SIEM)

- When AtomicRedTeam succesfully created new user: NewLocalUser



Failed Logon Attempts

- When Crowbar using Brute Force Attacks



Successful Logon Attempt

index=endpoint first_user_marketing EventCode=4624

Last 60 minutes

✓ 4 events (9/27/24 6:50:00.000 AM to 9/27/24 7:50:11.000 AM) No Event Sampling Job Smart Mode

Events (4) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS
EventCode 1
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2
a Account_Name 3
a Authentication_Package 2

i	Time	Event
>	9/27/24 7:27:31.000 AM	09/27/2024 12:57:31 PM ... 26 lines omitted ... New Logon: Security ID: S-1-5-21-2519334750-4260137159-2156265069-1105 Account Name: first_user_marketing Account Domain: AD Show all 70 lines EventCode = 4624 host = WINDOWS-10-TARG source = WinEventLog:Security sourcetype = WinEventLog:Security

EventCode

9 Values, 9.356% of events

Selected Yes No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

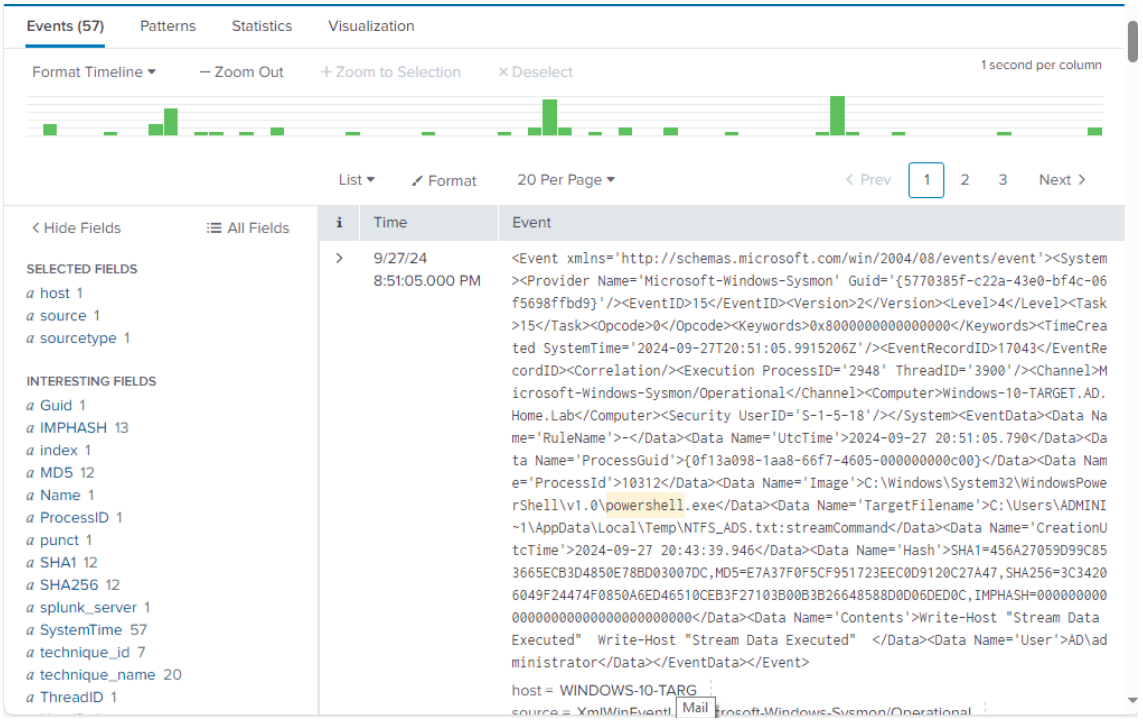
Events with this field

Avg: 4868.212765957447 **Min:** 16 **Max:** 5379 **Std Dev:** 807.1262320153481

Values	Count	%
4625	64	45.39%
5379	62	43.972%
4624	4	2.837%
16	3	2.128%
4634	3	2.128%
4648	2	1.418%
5058	1	0.709%
5059	1	0.709%
5061	1	0.709%

Atomic Test T1059.001

- When run AtomicTest for Command and scripting Interpreter (Powershell)



THANK YOU