Ethical Hacking Project: Red Team and Blue Team Roles in Cyber Attack Scenarios

Contents

Introduction 2

Overview of Project Objectives 2

Target Environment Setup 2

Red Team Activities 18

Attack Stages 18

Weaponization: 19

Delivery: 19

Exploitation: 19

Installation: 19

Command and Control: 19

Actions on Objectives: 19

Tools and Techniques 19

Blue Team Activities 22

Analysis of the Attack 22

Detection Strategies 22

Mitigation and Response 22

Documentation: 22

Discussion 26

Evaluation of Strategies 26

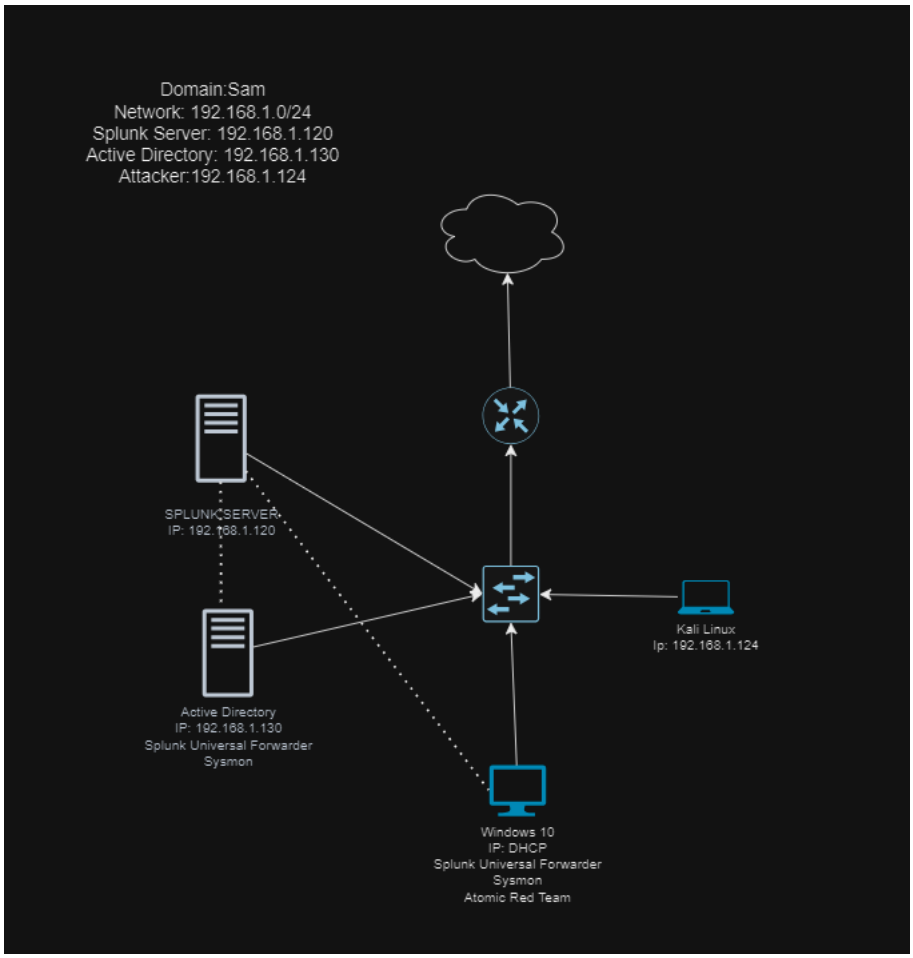
Lessons Learned 26

Conclusion 26

1. Introduction

Overview of Project Objectives

This project aims to explore the roles of Red Team and Blue Team in cybersecurity by simulating a multi-phase cyber-attack scenario. The focus is on conducting an ethical hacking exercise where the Red Team performs various attacks on a configured network environment while the Blue Team works to detect and mitigate these threats.



Images:Lab set up

Target Environment Setup: The lab environment is composed of the following components:

Kali Linux: Used as the attacking machine.

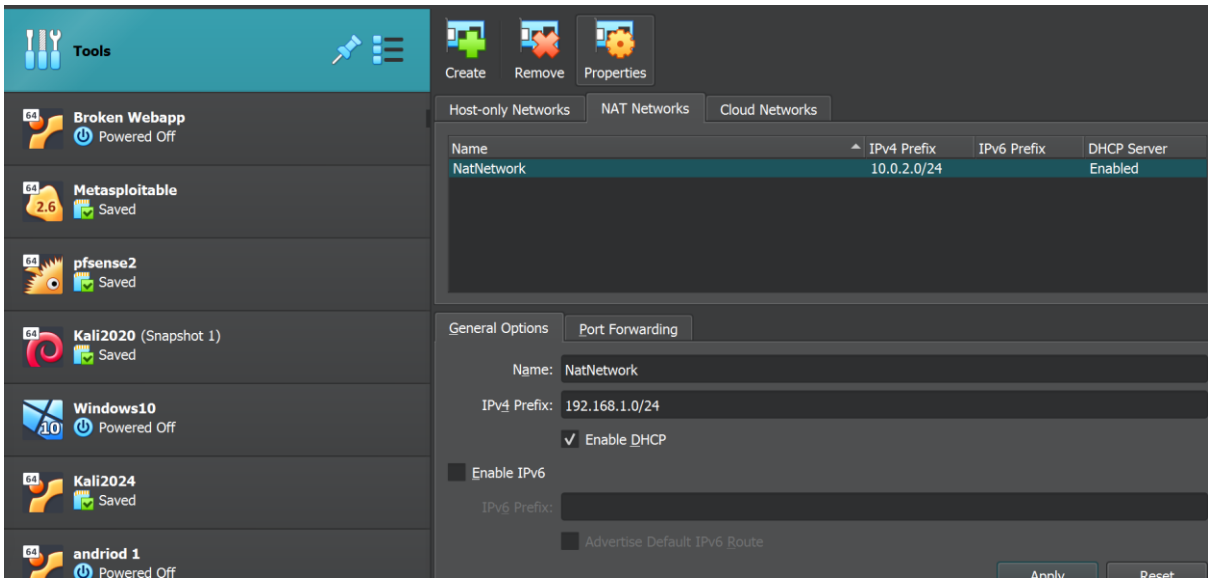
Windows 10: The target machine, user skabir.

Windows Server 2019: Configured as an Active Directory Domain Controller.

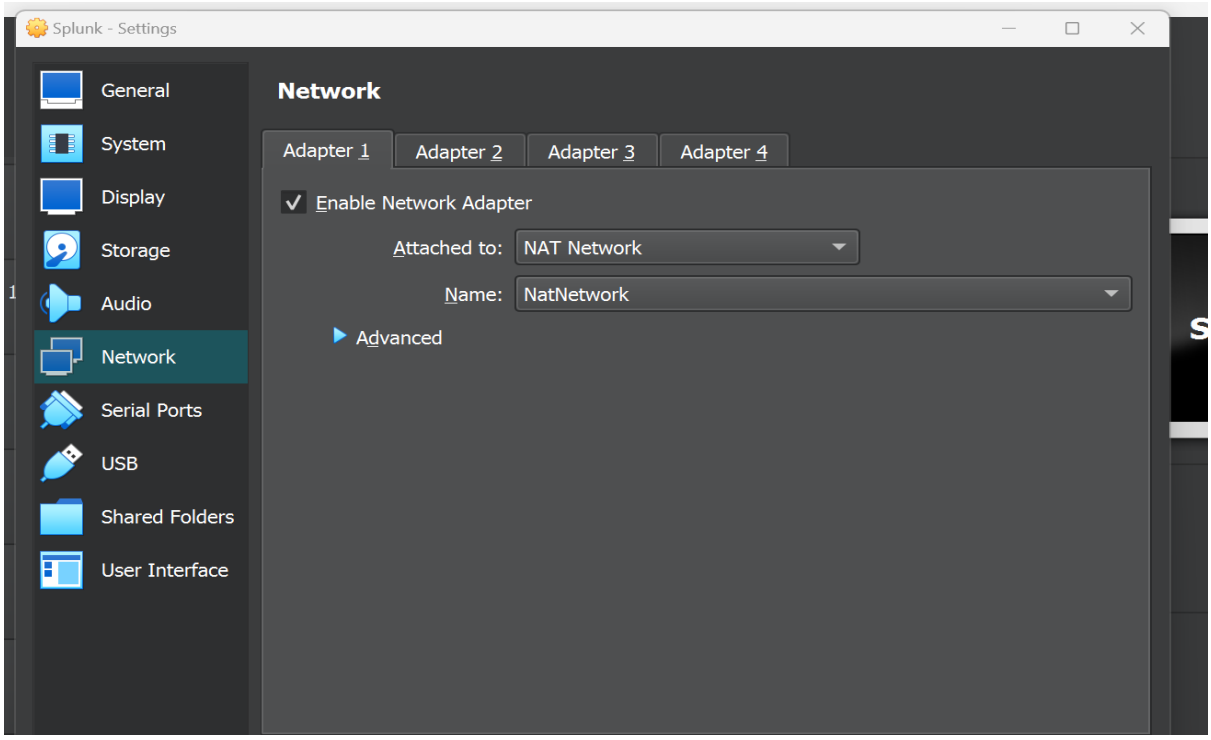
Splunk Server (Ubuntu): For telemetry data collection and analysis.

The environment is set up using a NAT network in VirtualBox to ensure all machines can communicate within the same subnet. Static IPs were assigned to each machine to facilitate network

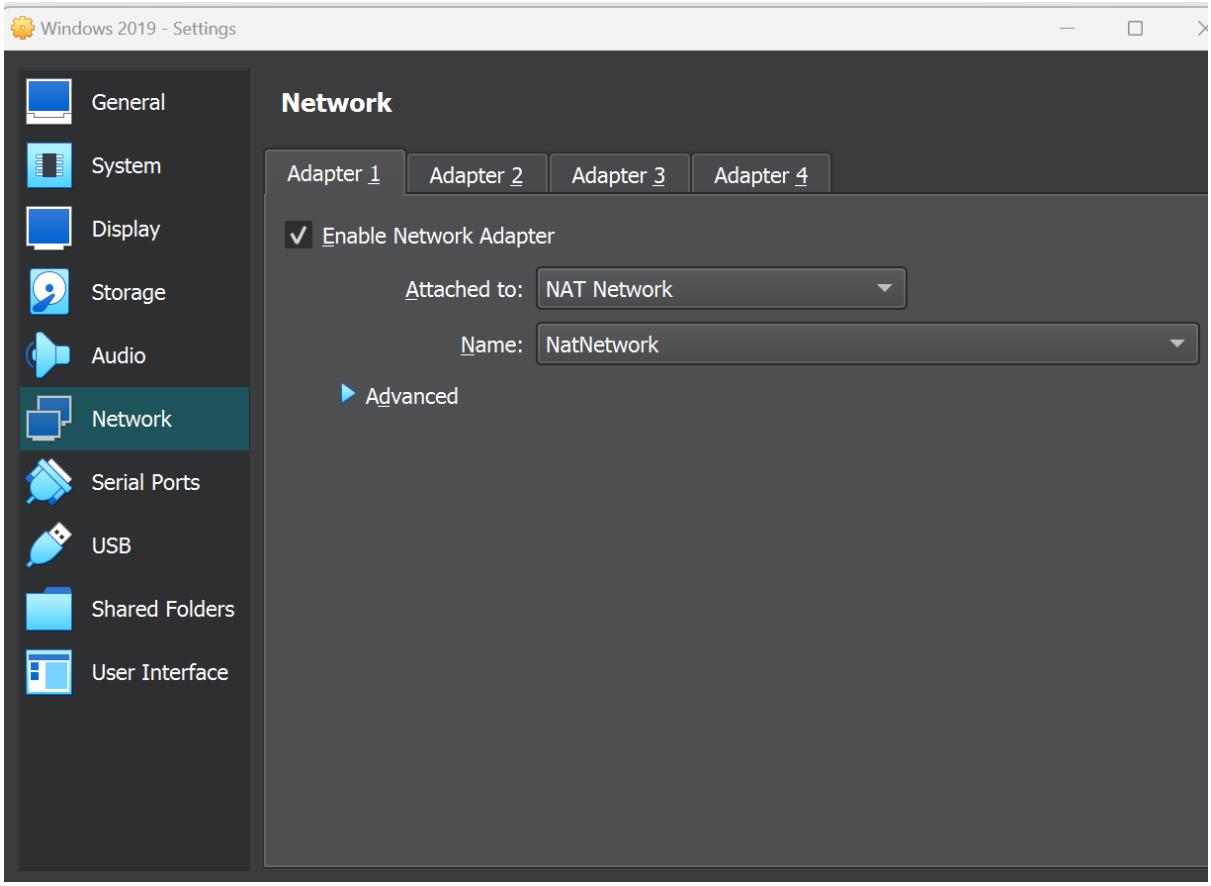
configurations.To establish the lab environment, we will set up and install Windows 10, Kali Linux, Windows Server 2019, and Ubuntu for the Splunk server. The first step involves creating a custom NAT network within VirtualBox. This configuration ensures that all virtual machines can communicate effectively by setting their network settings to NAT, allowing them to operate within the same network.



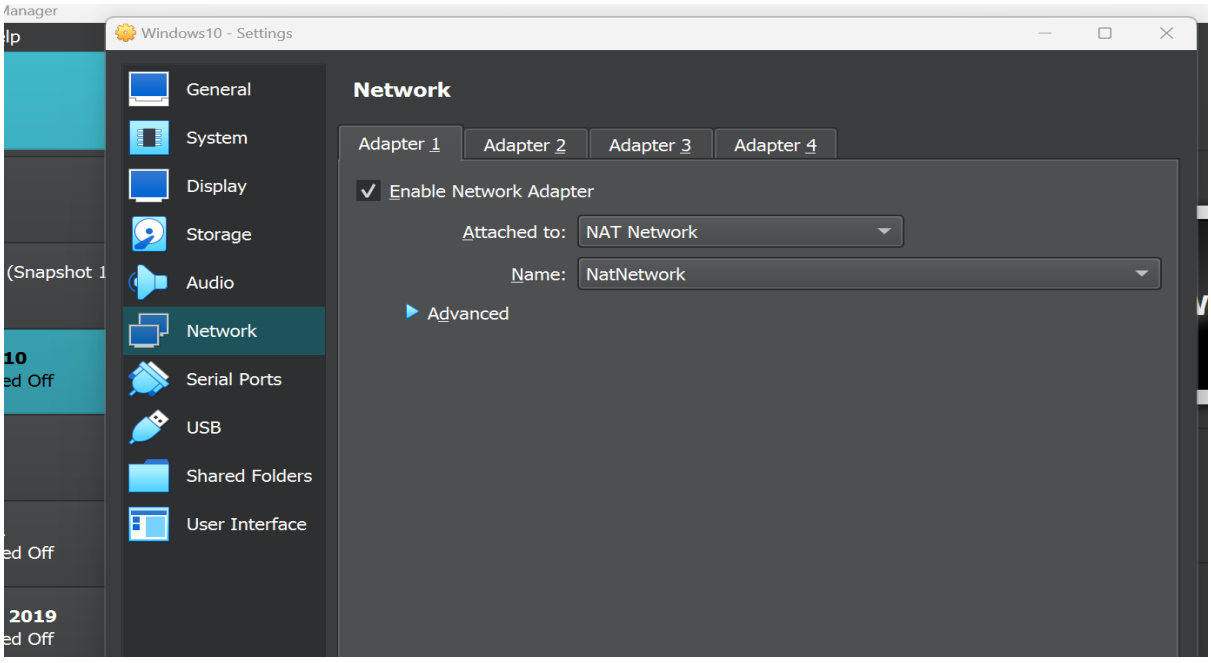
NAT Network



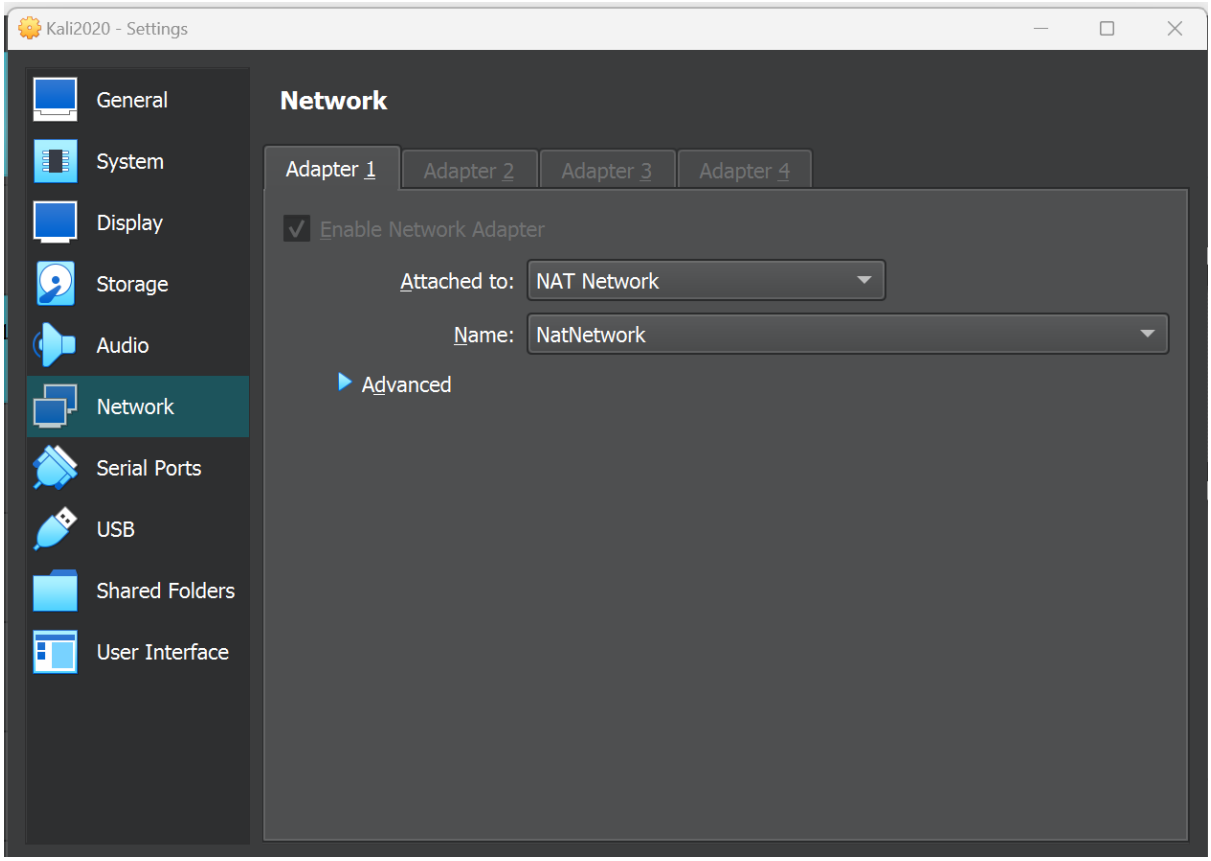
Splunk server on NAT NETWORK



Active Director server on NAT NETWORK

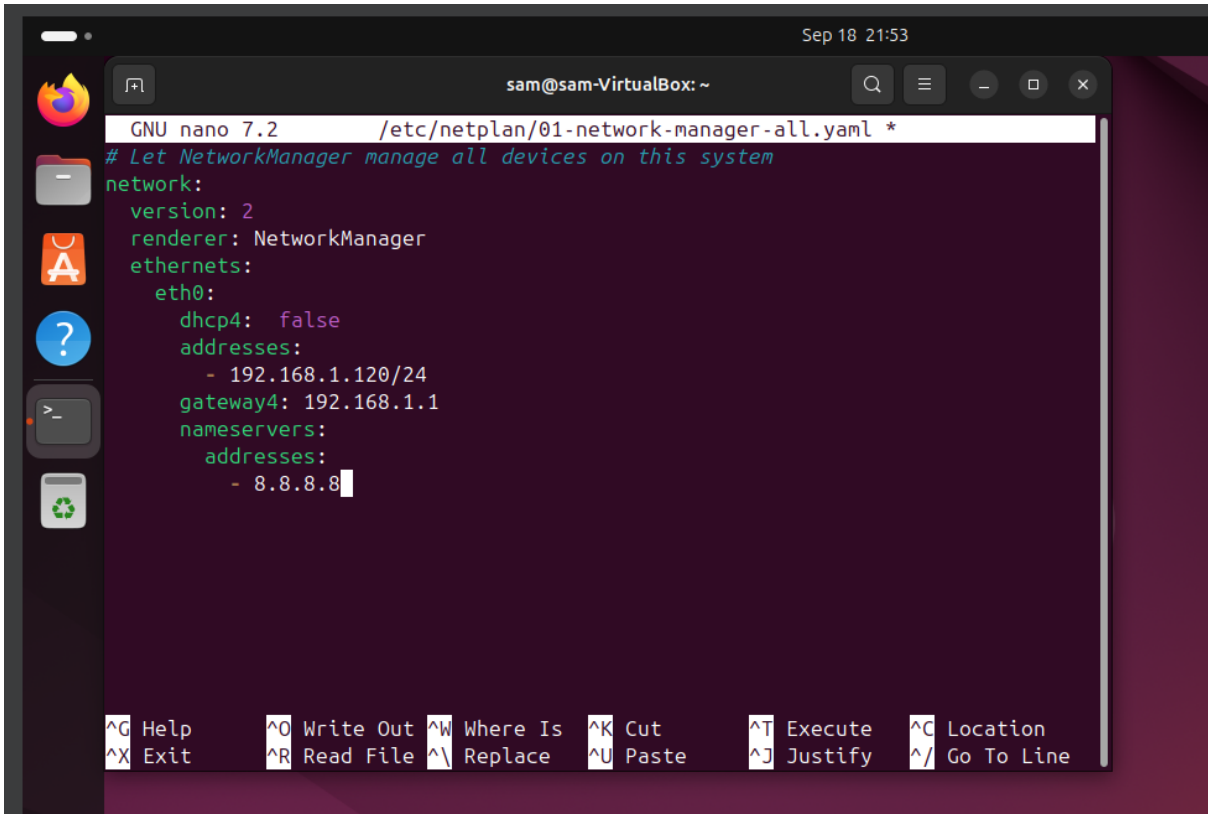


Windows 10 on NAT NETWORK

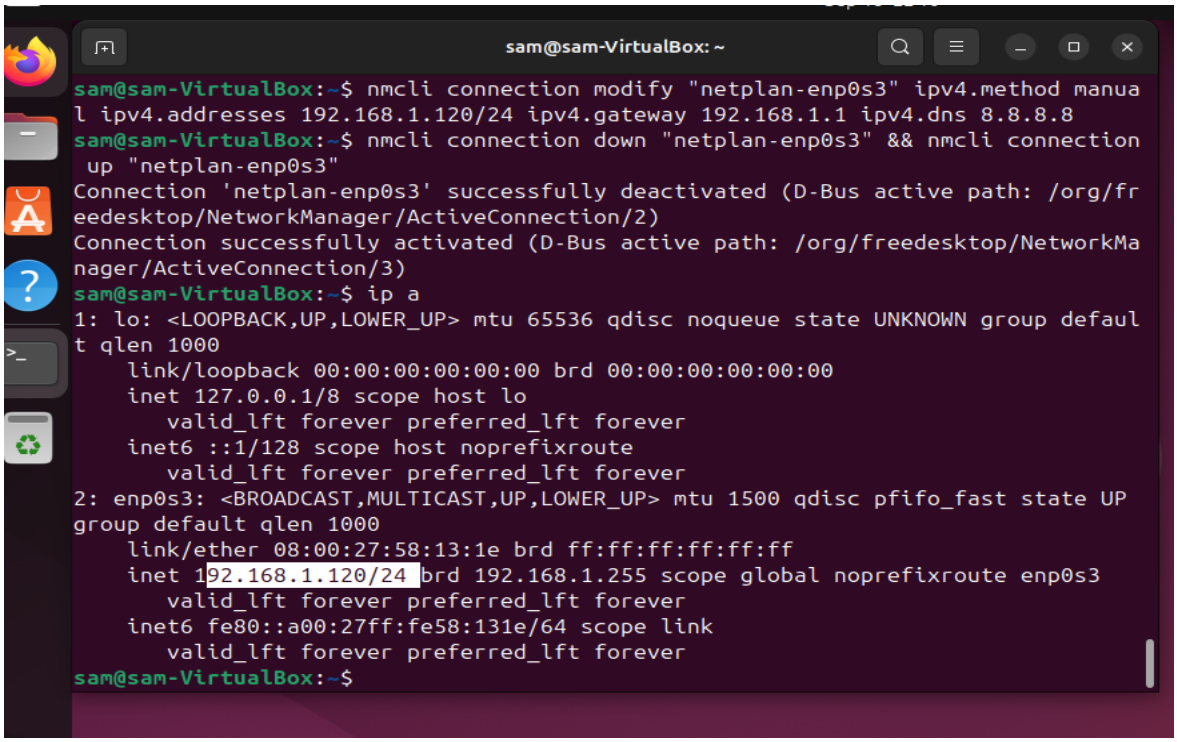


Kali on NAT NETWORK

Now we will set up the static IP addresses. Splunk server static IP changed to 192.168.1.120

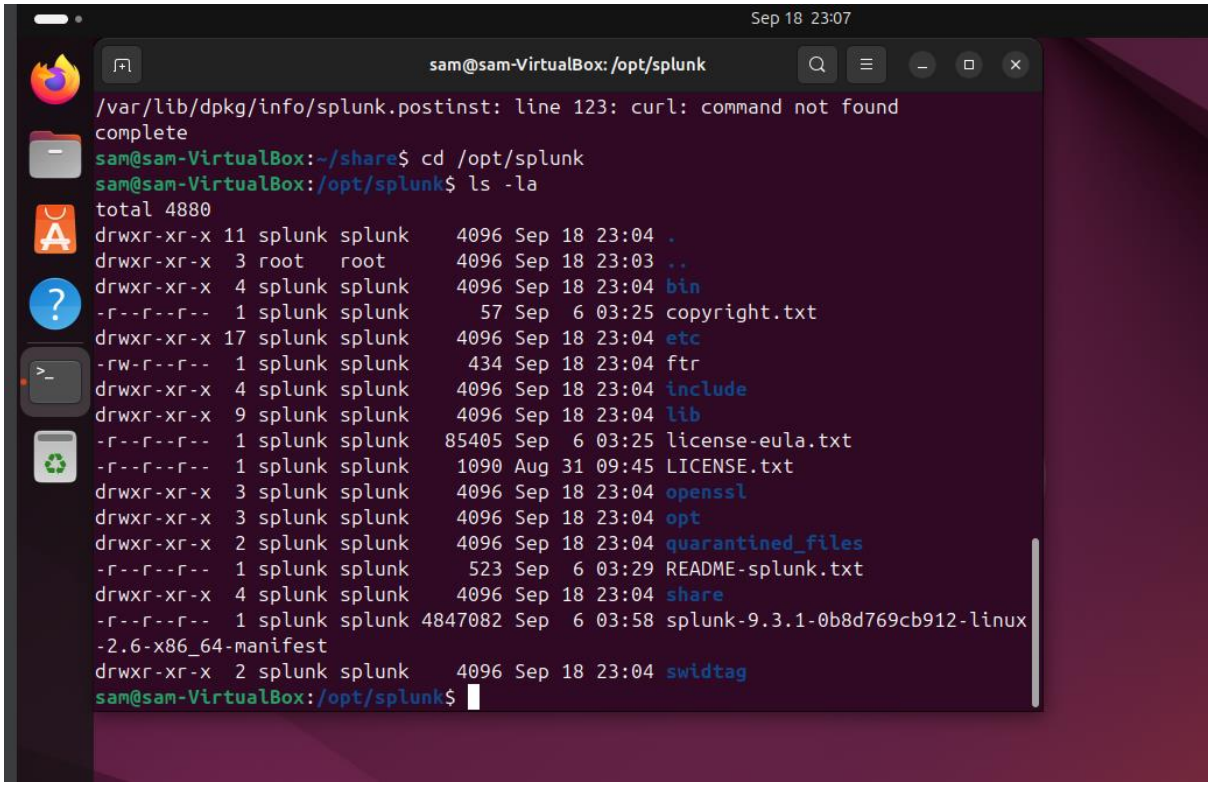


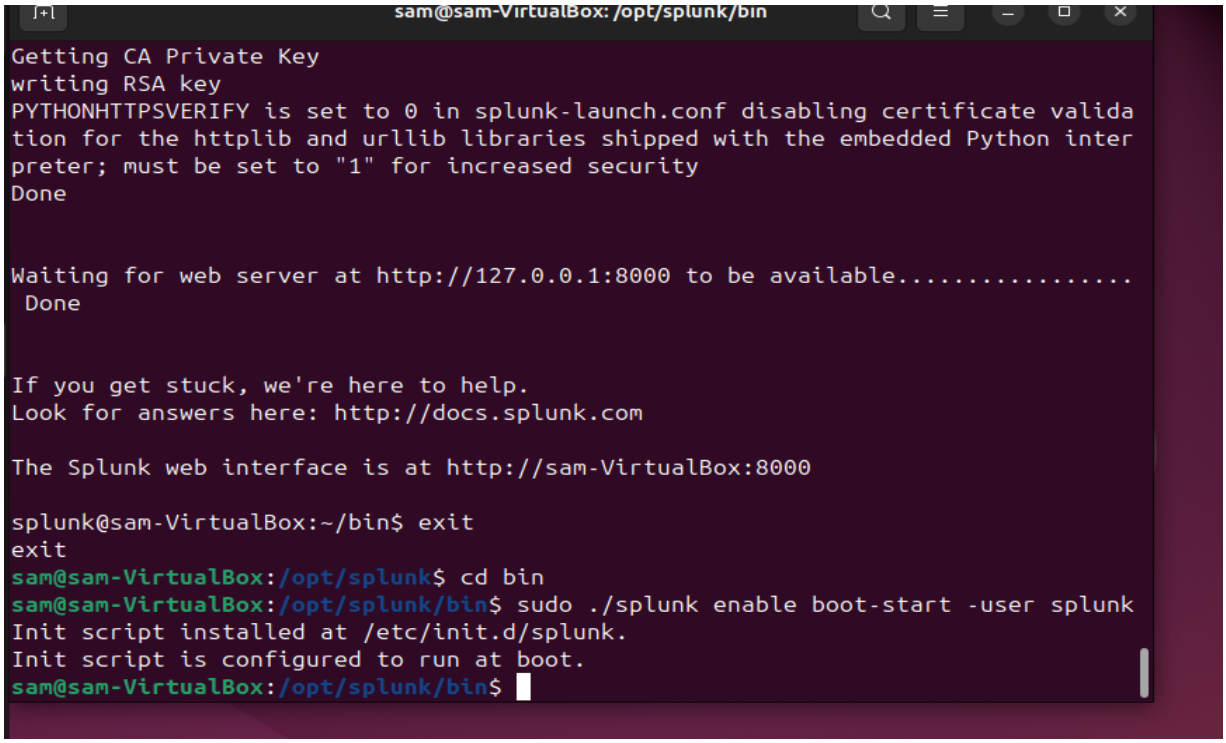
Edited 01-network-manager-all.yaml



Splunk Static IP assigned to 192.168.1.120

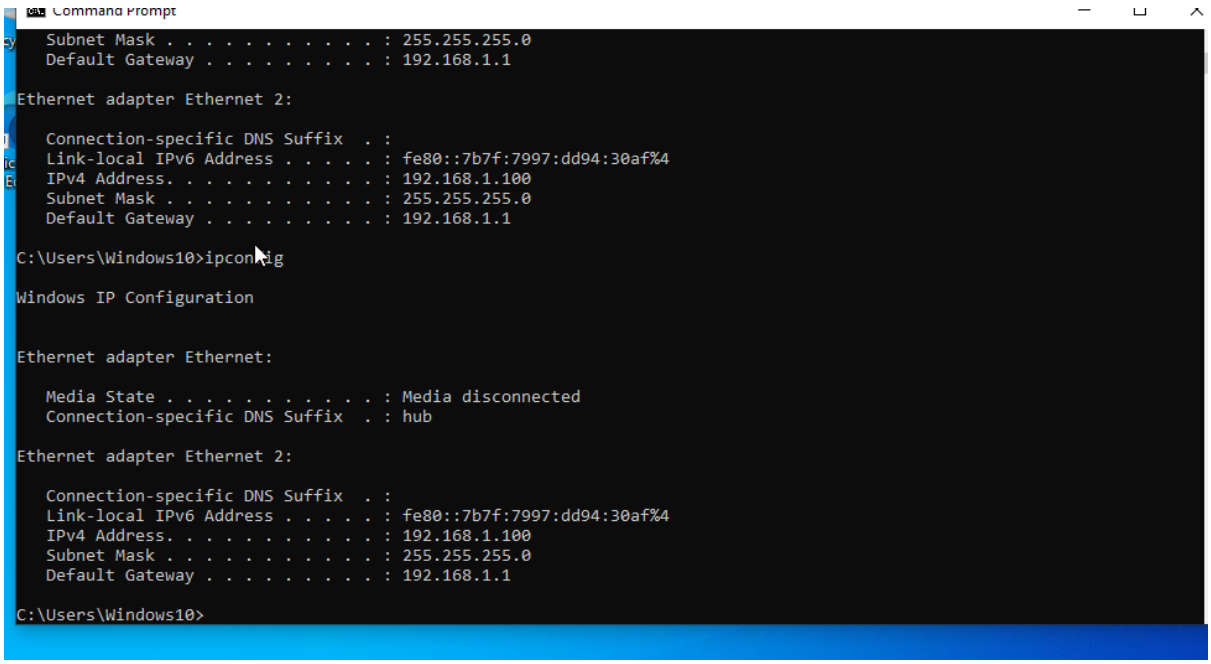
Now we will download Splunk in our host and can install in Splunk server.





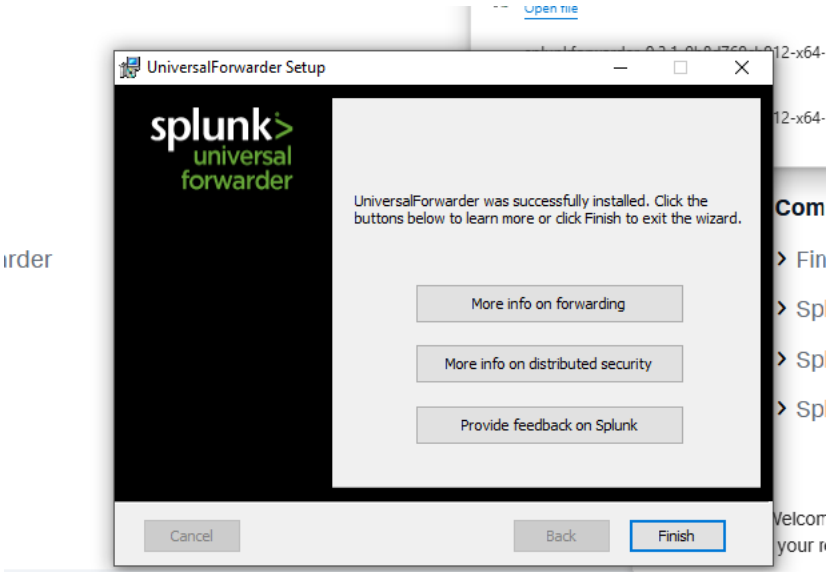
Splunk installed in Splunk server

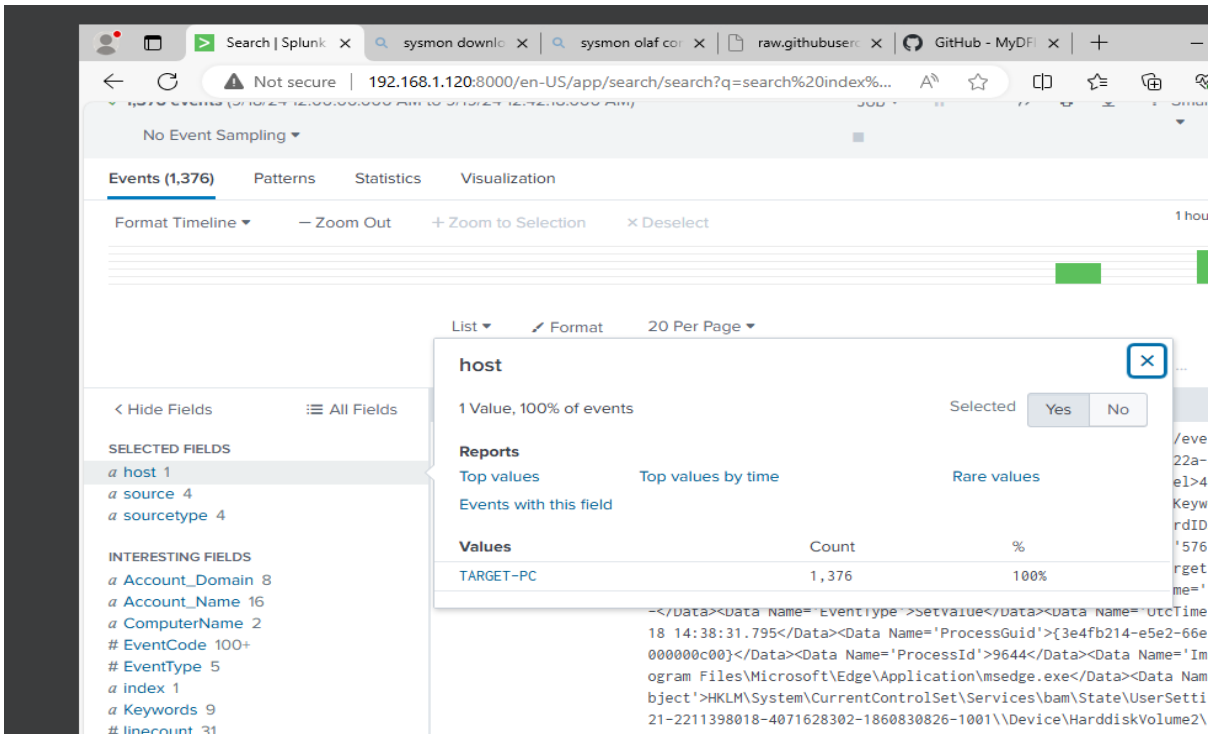
Now we will configure the static IP of the attacker machine.



Windows 10 Static IP configured

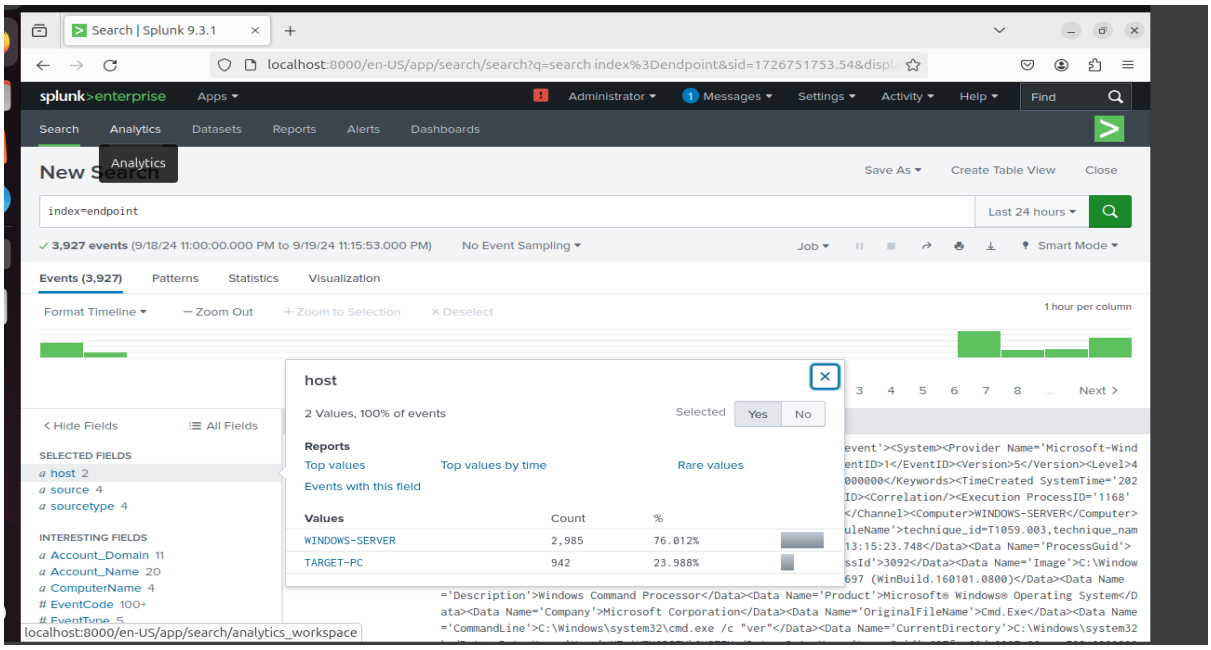
We will also install Sysmon and Splunk universal forwarder both into our target machines and server. Both collect telemetry and send logs over to Splunk server.





Splunk forwarder and Sysmon installed in Target Machine

Now we will install Splunk forwarder and Sysmon after giving the static IP to the Windows server 2019.

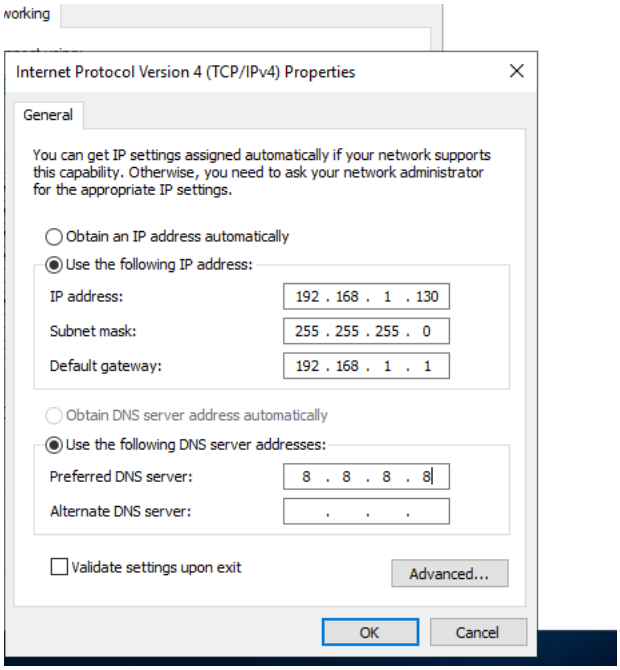


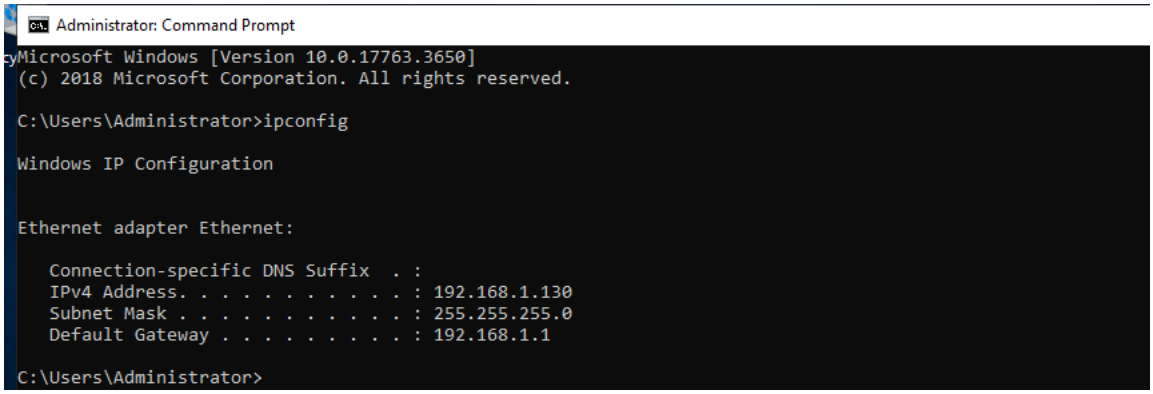
Splunk log showing 2 hubs

That means both Windows server and Target machine has Splunk forwarder and Sysmon installed successfully.

Configure Windows Server 2019 for Active Directory and Promote Domain Controller and get the target machine to join newly created domain

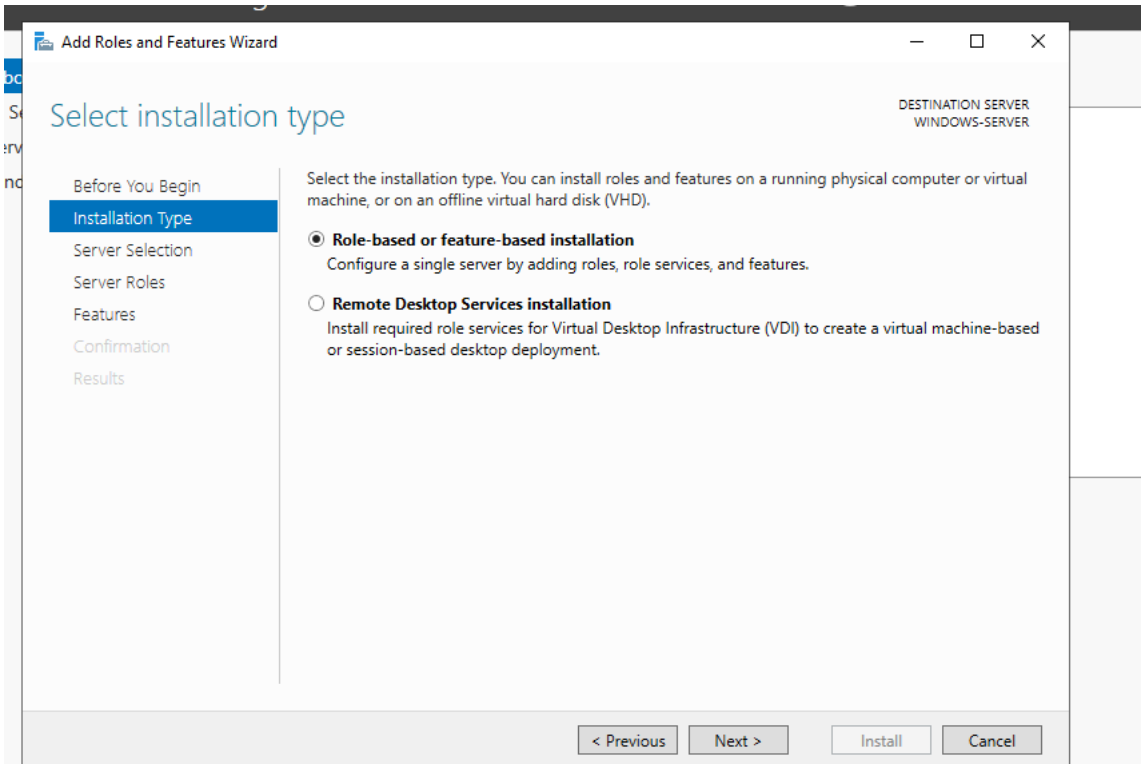
First, we'll configure static IP and then configure Windows Server as an Active Directory (AD) Domain Controller.



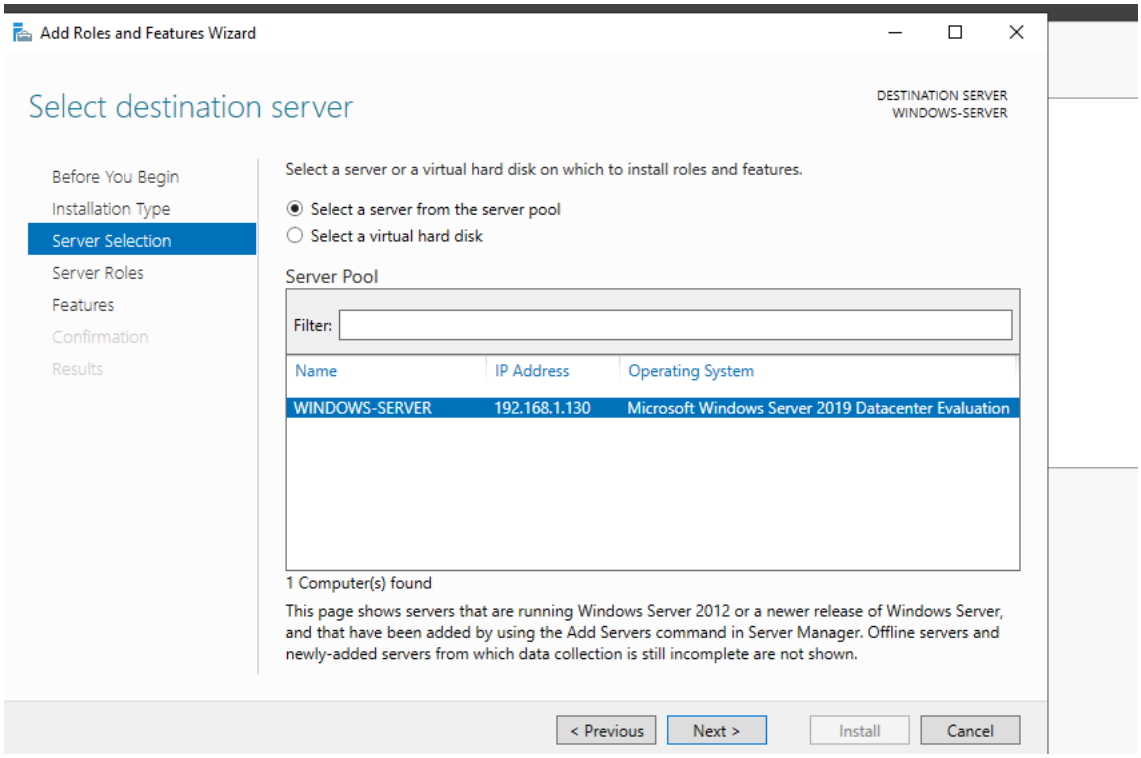


Static IP for windows server 2019

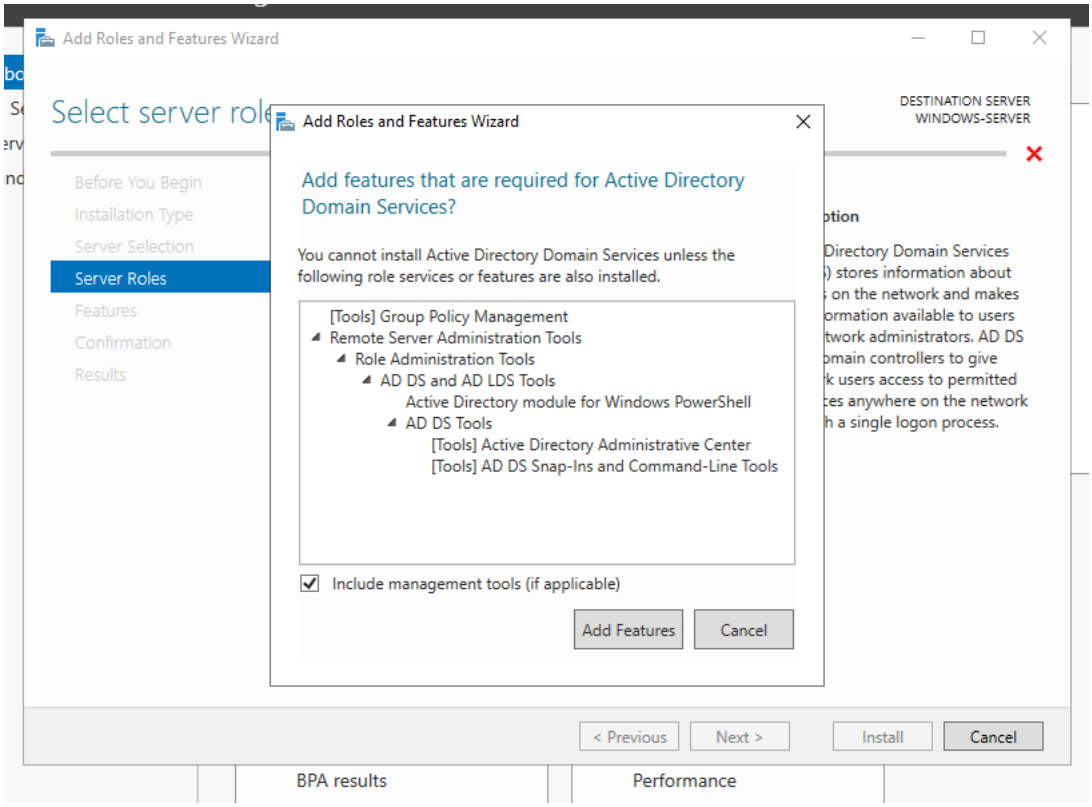
Now we will configure server manager "Add roles and features".



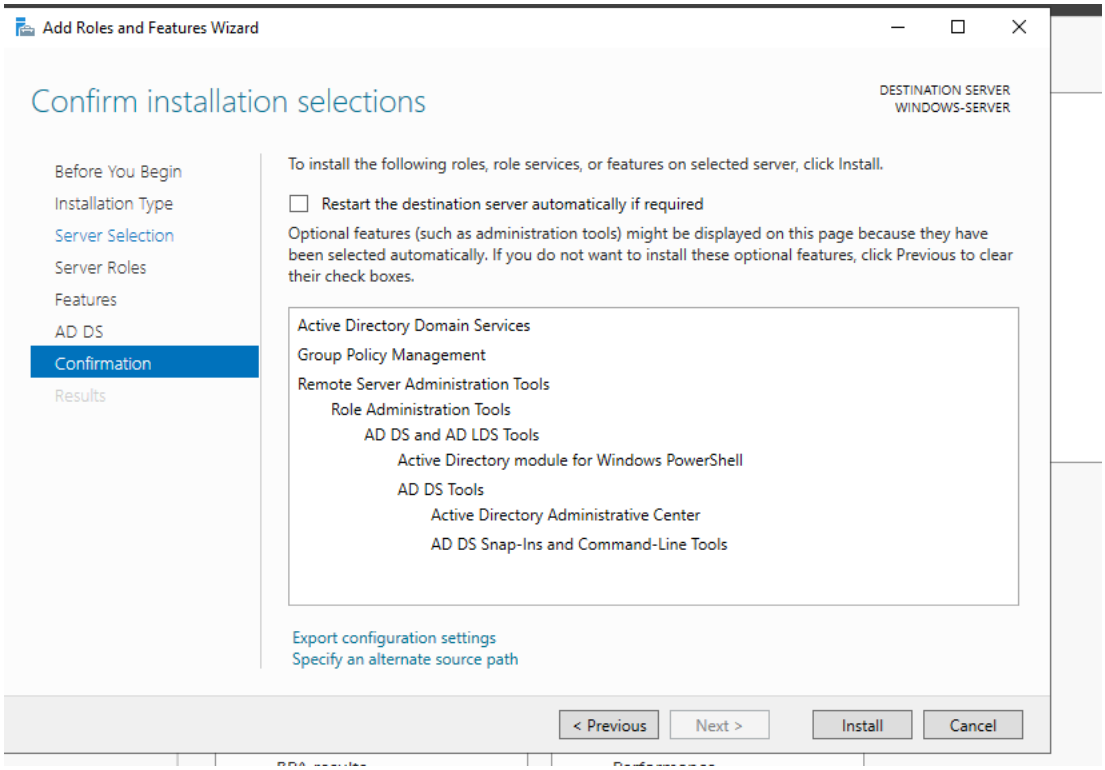
Selected Installation Type



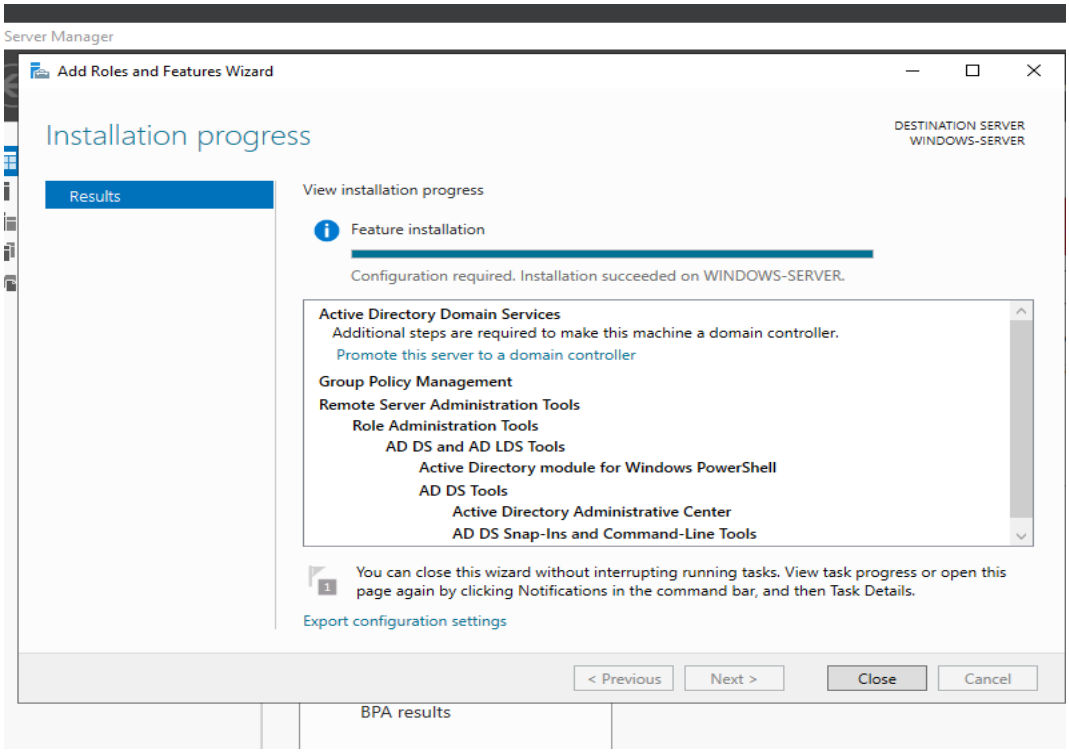
Selected Destination Server



Added Features

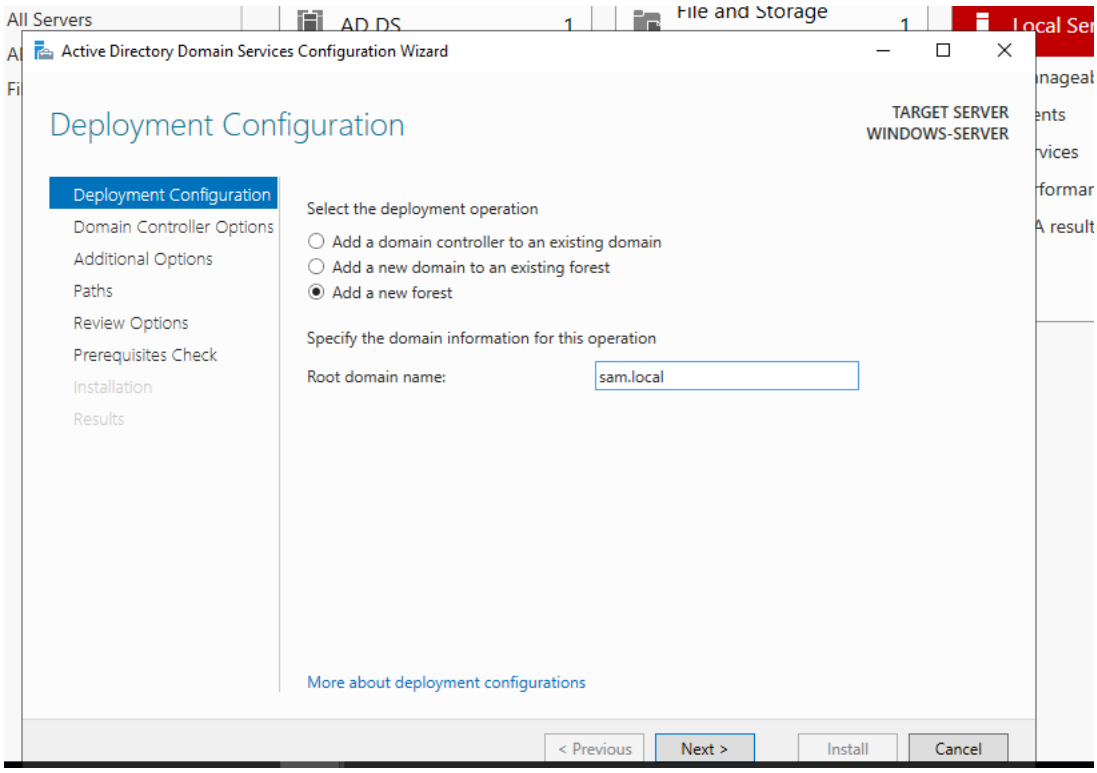


Confirmed Installation

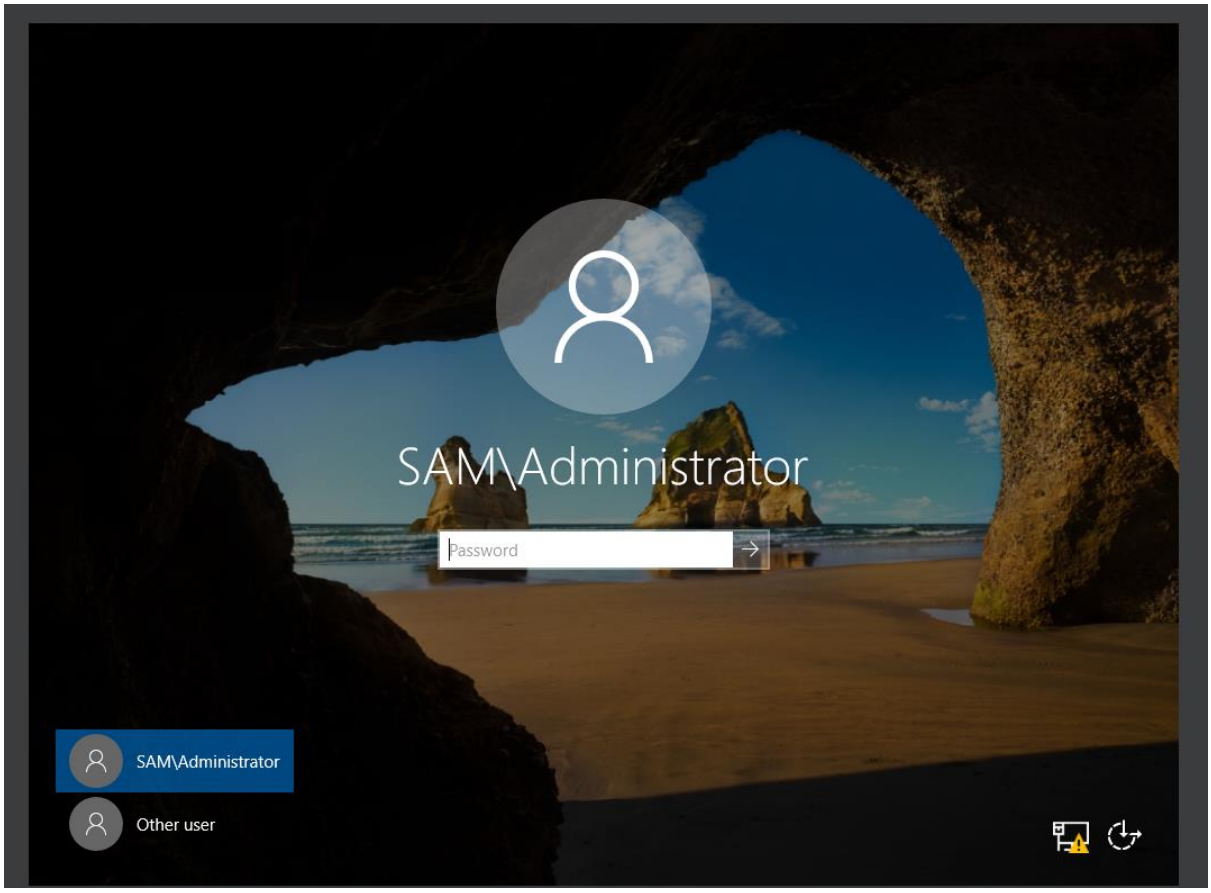


Added Active Directory Domain Services

After the installation we will configure Active Directory Domain Services. First, we will create a new Domain

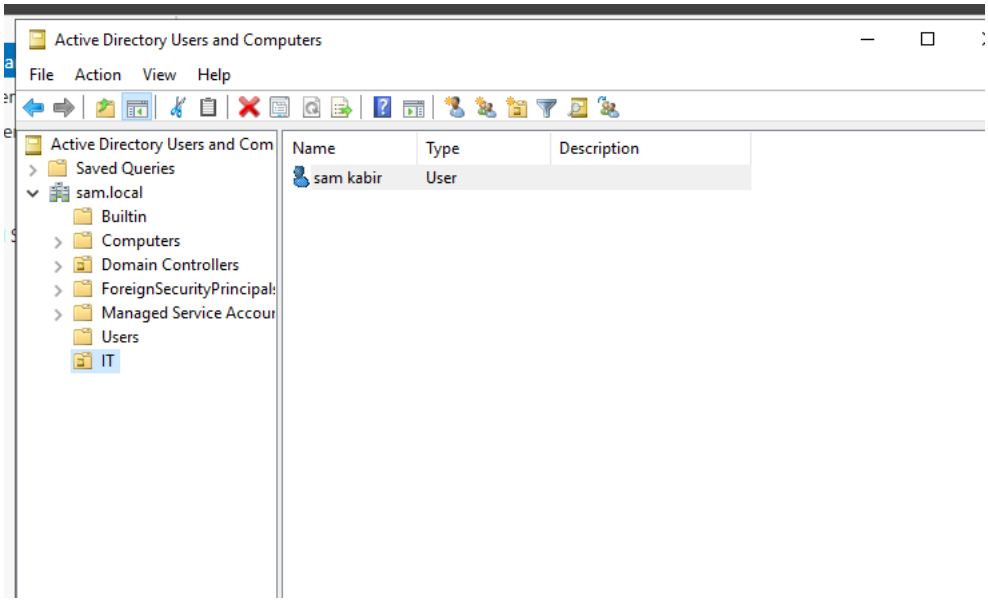


Domain name

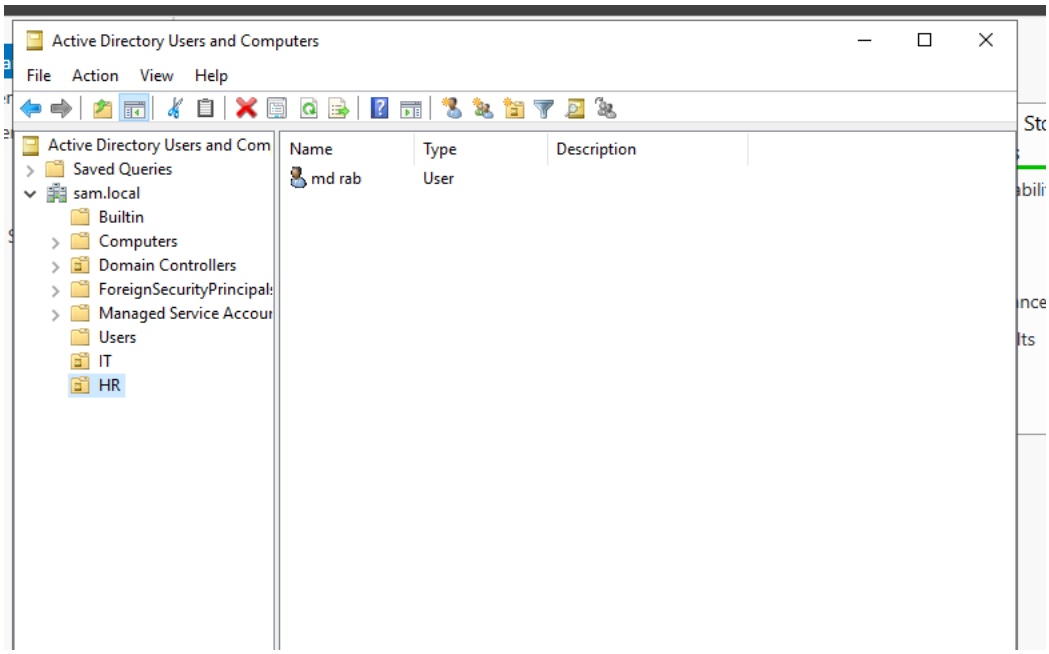


Login page Indicates AD-DS successfully created

Now we will create users on the Active Directory: Under new organisational unit we create two units IT and HR and under IT we create "skabir" user and under HR we create

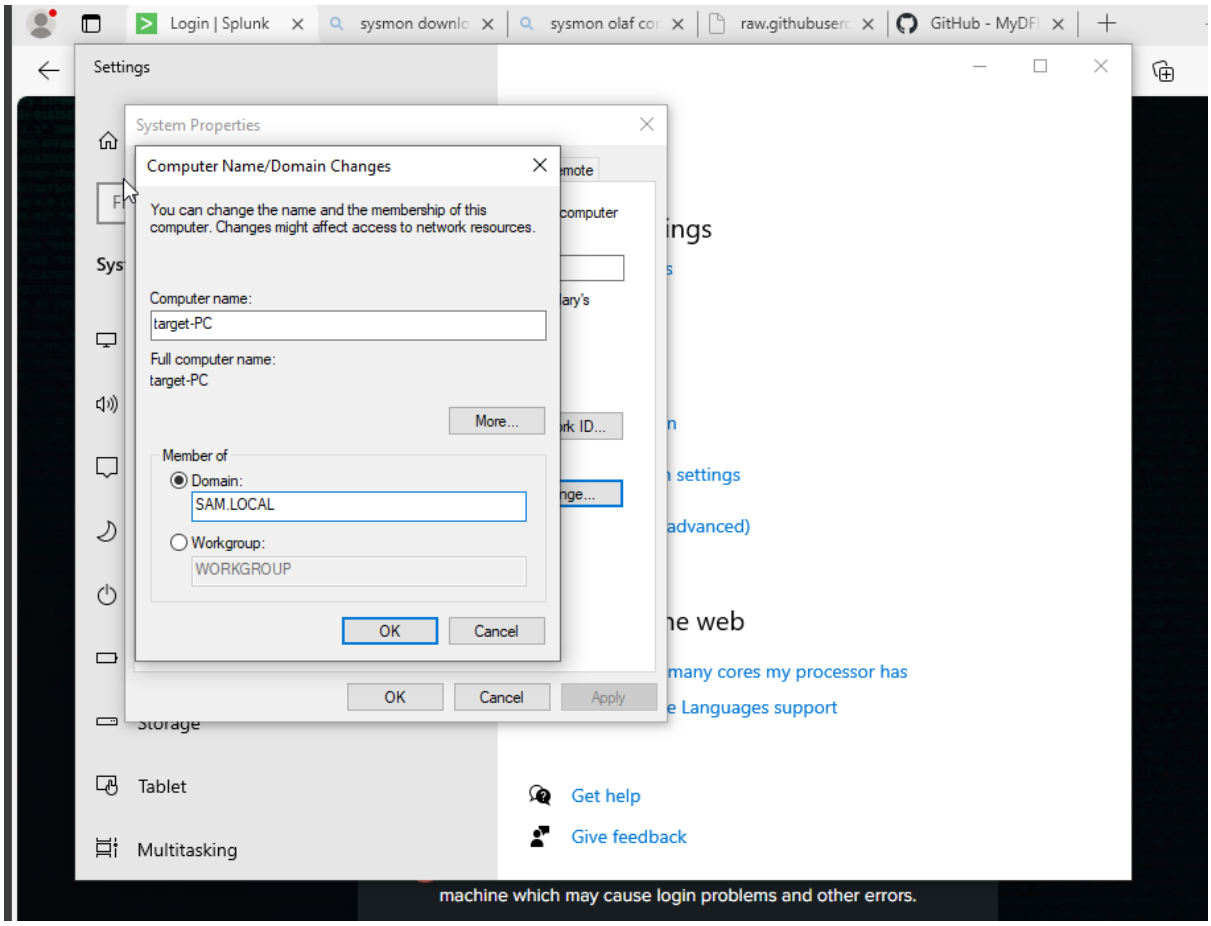


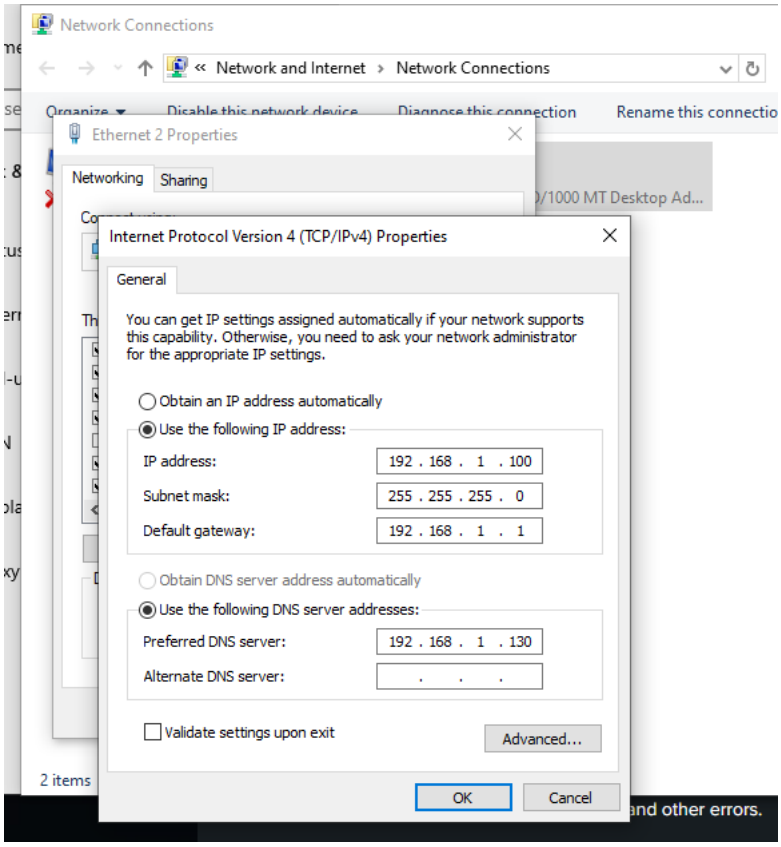
User "sam kabir" created

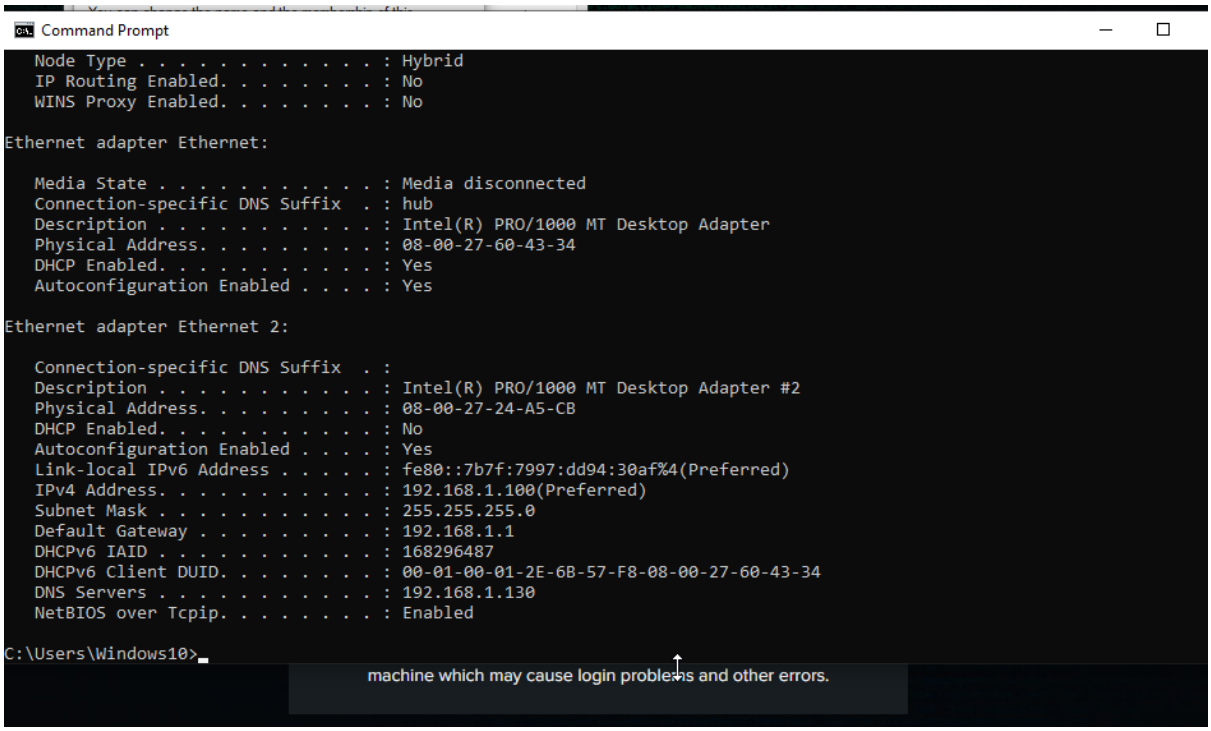


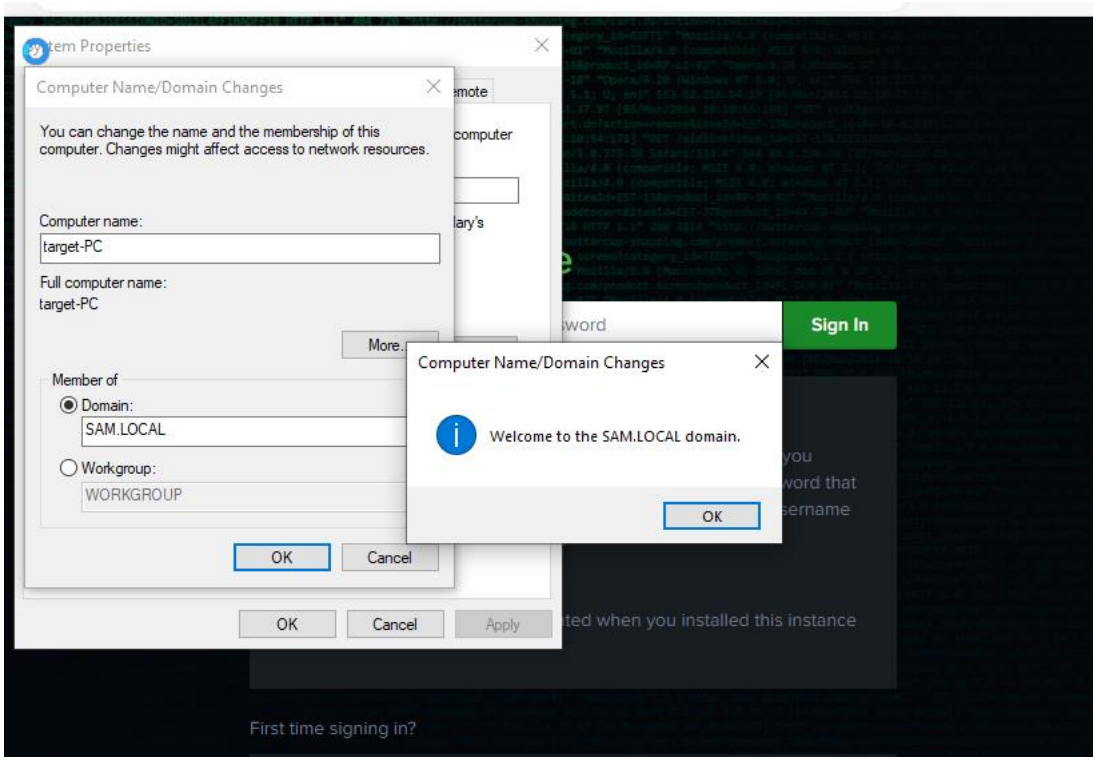
User "md rab" created

The server is set up and the server is now domain controller. Now on the target windows 10 we will join windows 10 to newly created domain.


Login | Splunk
sysmon downlc
sysmon olaf cor
raw.githubuserc
GitHub - MyDFI
Settings
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
target-PC
Full computer name:
target-PC
More...
Member of
Domain:
SAM.LOCAL
Workgroup:
WORKGROUP
OK
Cancel
Apply
Tablet
Multitasking
Get help
Give feedback
machine which may cause login problems and other errors.

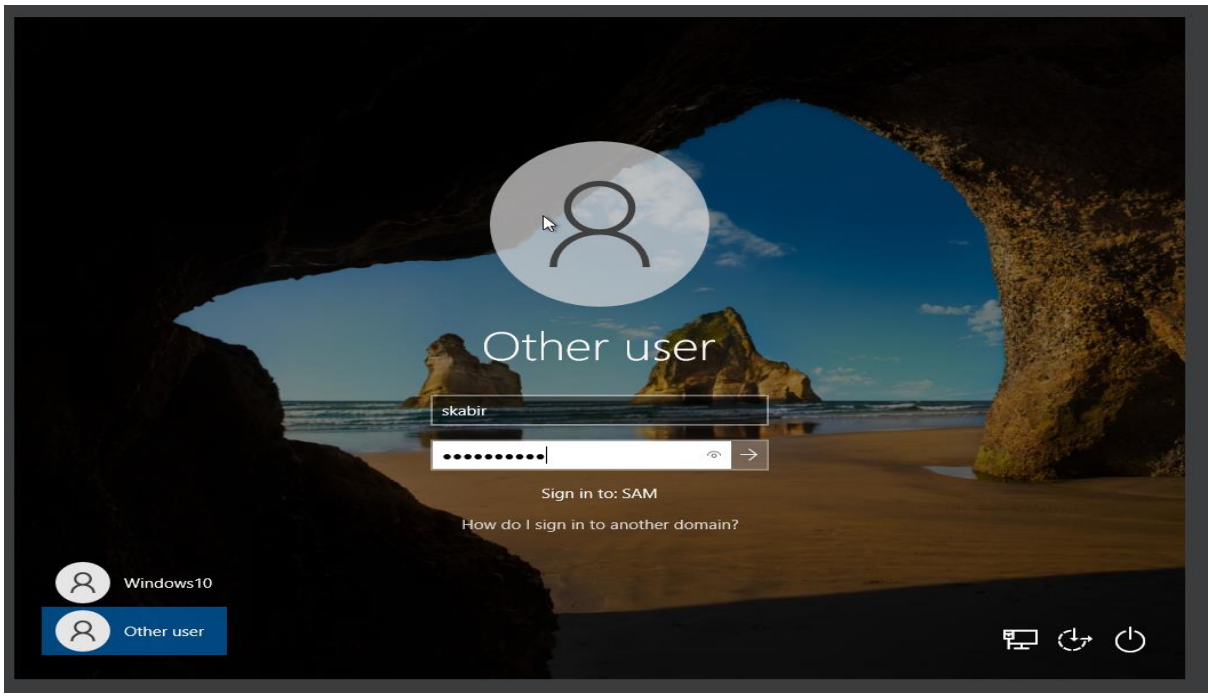

Network Connections
Network and Internet › Network Connections
Ethernet 2 Properties
Networking
Sharing
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 130
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
2 items





Domain and DNS server Set UP

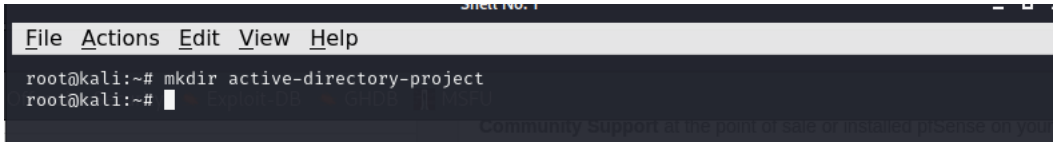
Now we will restart the windows 10 and will log in with newly created user skabir.



Logged In as "skabir" user

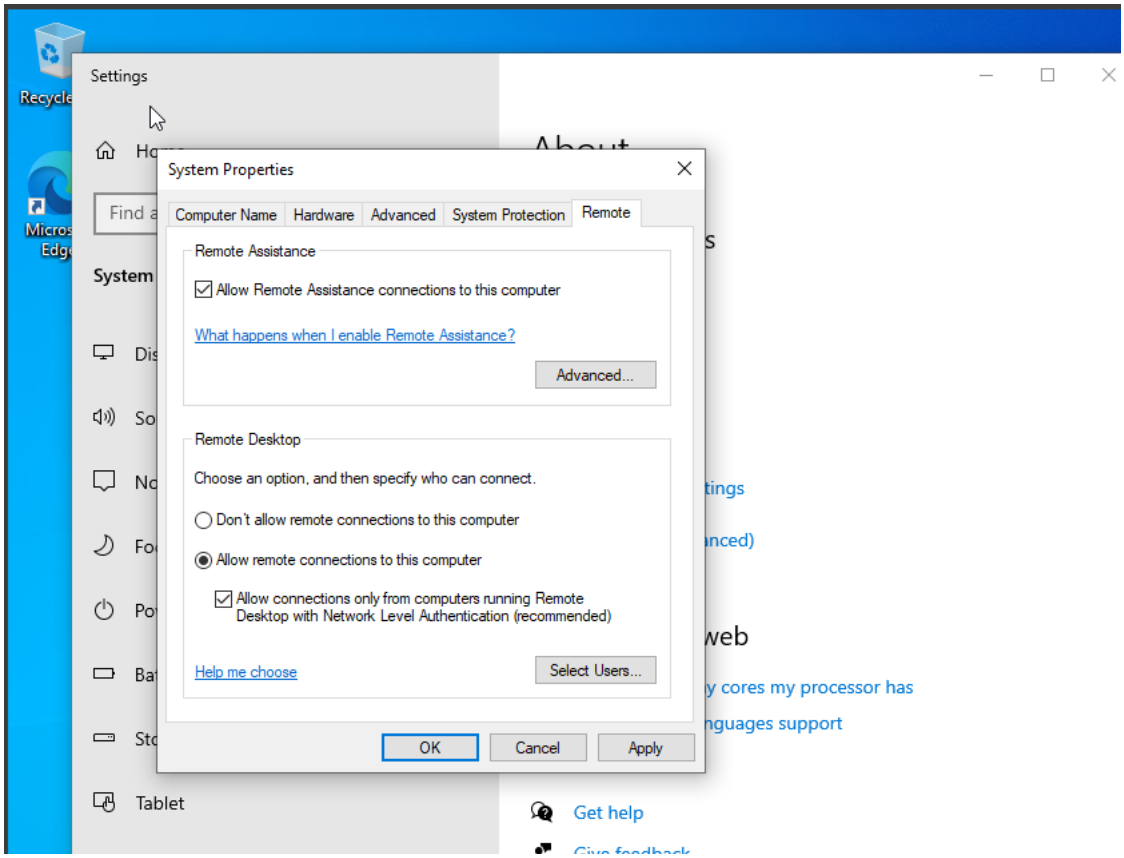
Now we will brute force attack from kali linux to user "skabir" and also we will set up atomic red team to run a test to generate telemetry and detect similar attack in future.

In kali we will set up a directory to attack the windows 10.

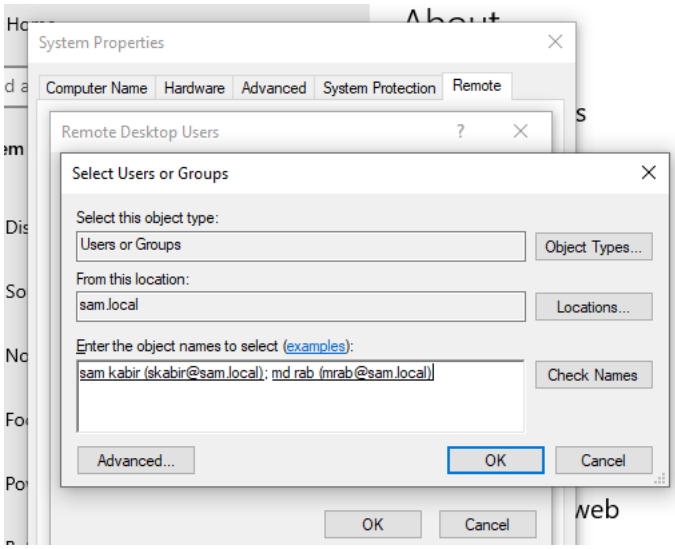


Created Directory

To execute the brute force attack, we will utilize the Hydra tool in conjunction with the Rockyou wordlist. We will copy the rockyou.txt file into the active directory project directory, selecting the first 20 lines for use in this demonstration due to the large size of the original file. These lines will be saved in a separate file named password.txt. Prior to initiating the attack on the target Windows machine, it is essential to configure the system to allow remote connections.



Allowed remote connection



Added remote connection to users

So, the lab is all set up.

Red Team Activities

Attack Stages: Reconnaissance:

Initial gathering of information about the target system, including network architecture and user accounts.

Weaponization:

Utilization of tools such as Hydra for brute-force attacks. The "Rockyou" wordlist was employed to attempt various password combinations against the "skabir" account.

Delivery:

The attack was conducted over Remote Desktop Protocol (RDP) by configuring the Windows 10 machine to allow remote connections.

Exploitation:

The Hydra tool executed a brute-force attack that successfully gained access to the skabir account, as evidenced by the successful RDP login.

Installation:

Post-exploitation, tools like Atomic Red Team were installed to generate telemetry data, which could later be analyzed for defense purposes.

Command and Control:

While the primary goal was to gain access, establishing command and control was not applicable in this scenario as it was an ethical exercise.

Actions on Objectives:

Actions included creating a new local user to simulate further compromise of the system.

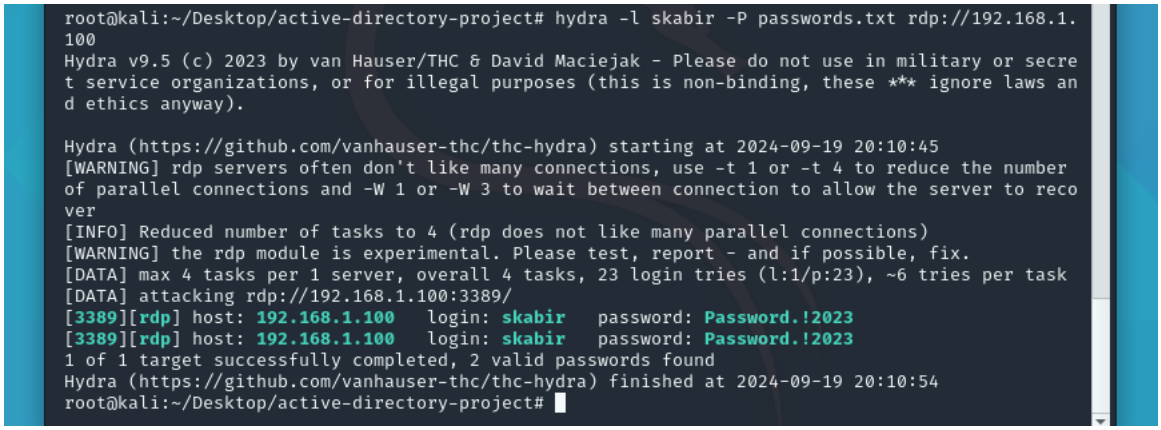
Tools and Techniques

Kali Linux: Used for launching attacks.

Hydra: Brute-force password cracking tool.

Atomic Red Team: Framework for executing attack simulations that align with MITRE ATT&CK tactics.

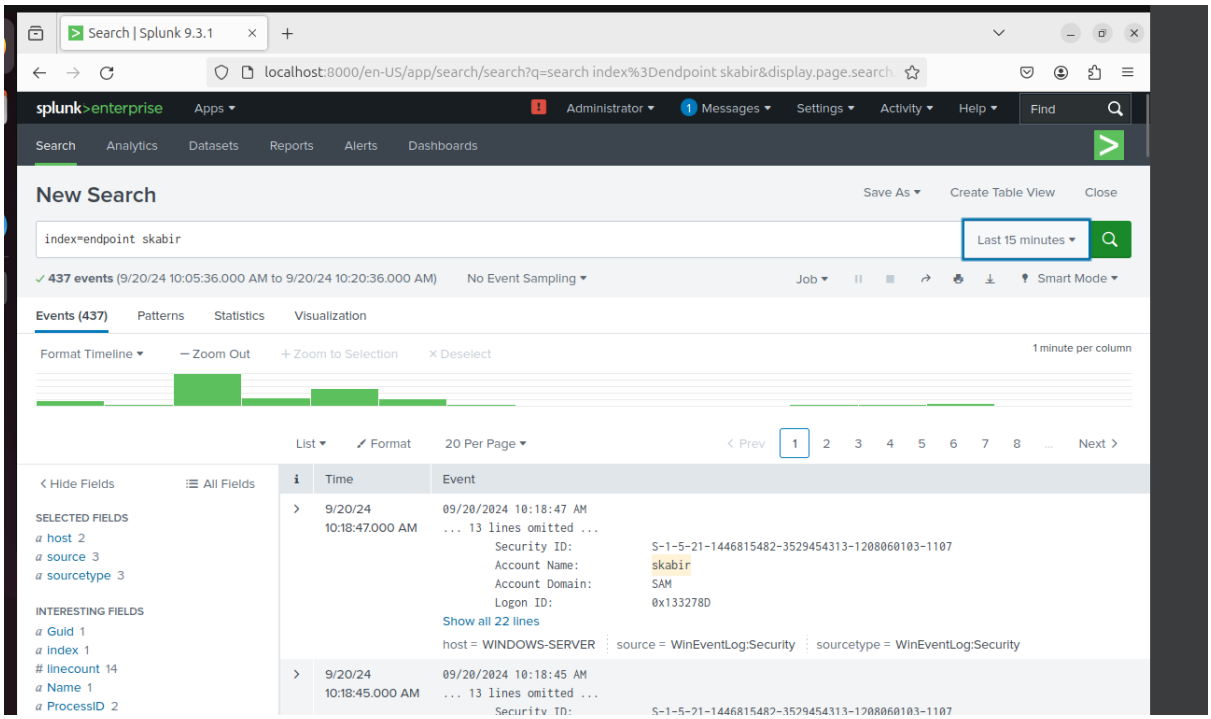
We will use the remote desktop protocol and hydra to get the password.



RDP successful and Password generated

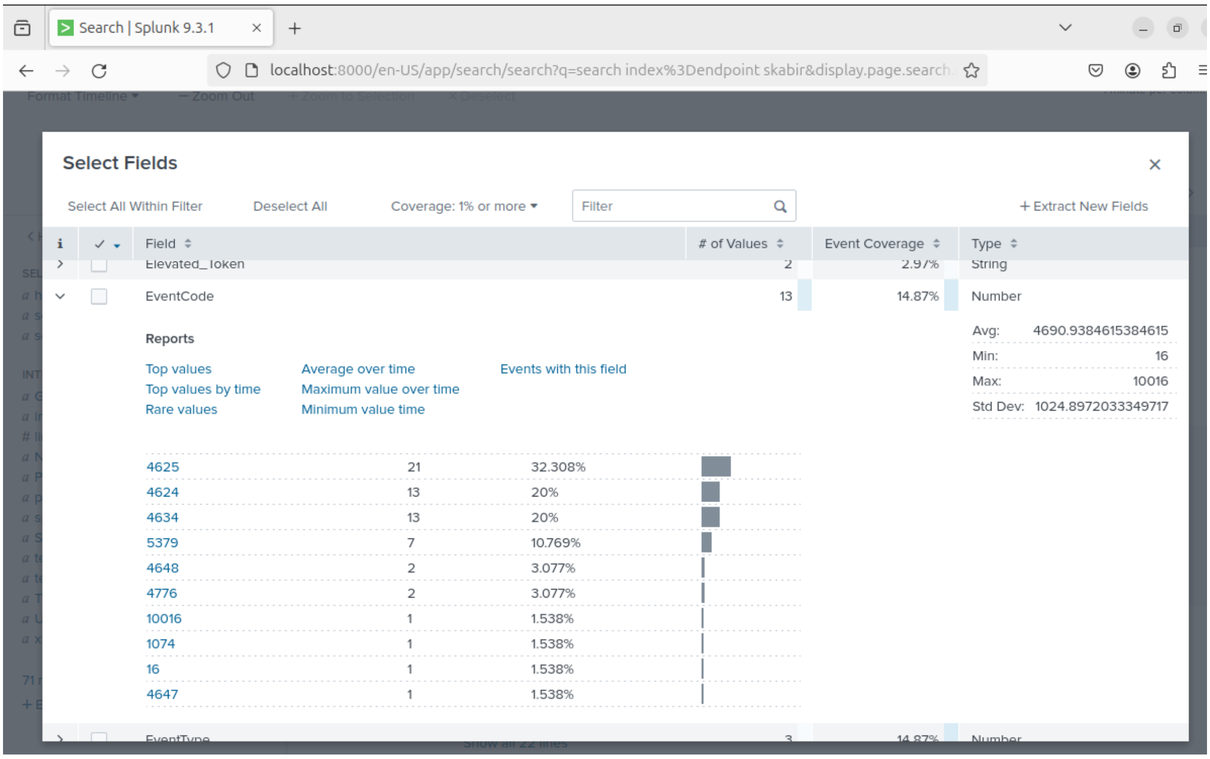
Now we can see the telemetry in the Splunk.

In the Splunk we will select search and reporting and we will narrow down our search to "index=endpoint skabir".



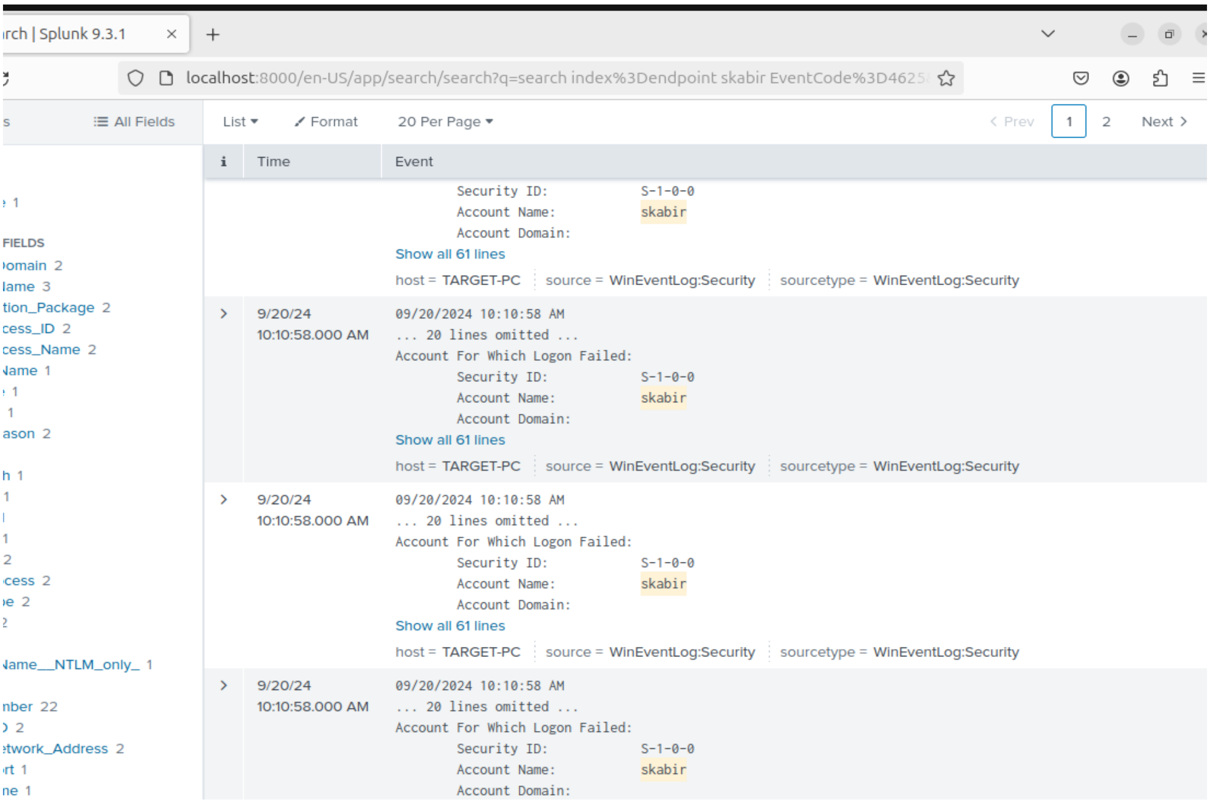
Splunk telemetry

In the "**Event Code**" section we can see there is 21 counts for the event ID 4625.



Event Code showing Counts and Events ID

Event Id "4625" means "an account to failed to log in". In this case 21 times failed attempts. If we look closely, we can see all the events happened exactly at the same time.



Login attempts at the same time

Blue Team Activities

Analysis of the Attack

The Blue Team's primary task was to analyze the telemetry data collected during the attack. Event ID 4625, indicating failed login attempts, was crucial for identifying signs of brute-force activity.

Detection Strategies

Splunk SIEM: Used to ingest logs from the Windows machines. A search was conducted to filter events related to the skabir account.

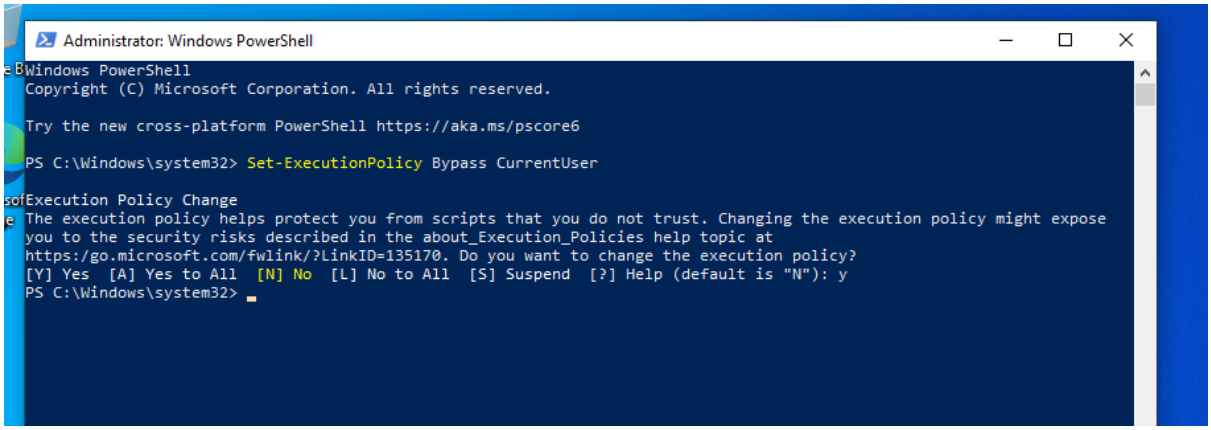
Sysmon: Installed on target machines to provide additional telemetry about system events and network connections.

Mitigation and Response

Response Strategy: Upon identifying the attack, measures were taken to lock the skabir account and notify the network administrator.

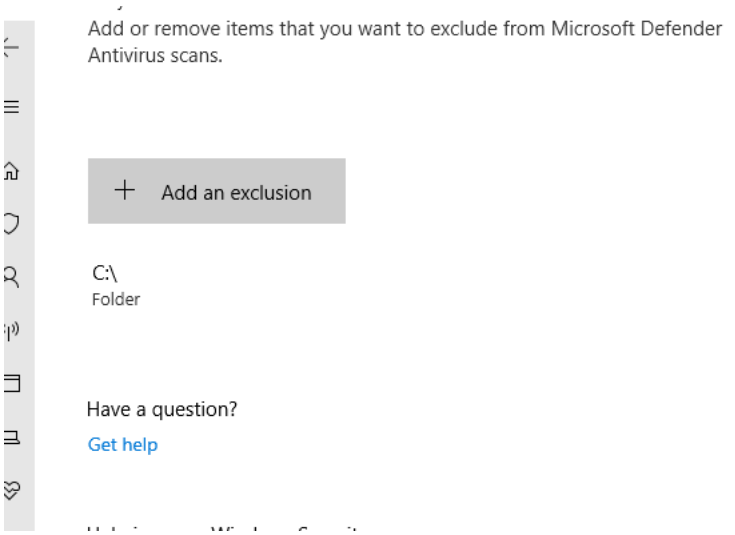
Documentation: A step-by-step account of actions taken during detection and mitigation was recorded for future reference.

This observation indicates the presence of a brute force attack activity. Next, we will proceed to install Atomic Red Team on the target machine and conduct a series of tests. To begin, we will configure the execution policy by executing the command "Set-ExecutionPolicy Bypass CurrentUser". This adjustment will allow us to run the necessary scripts without restrictions.



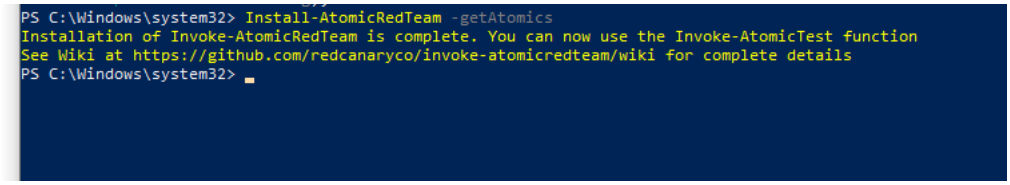
Set Up Execution Policy

Now we will set up an exclusion for C Drive.



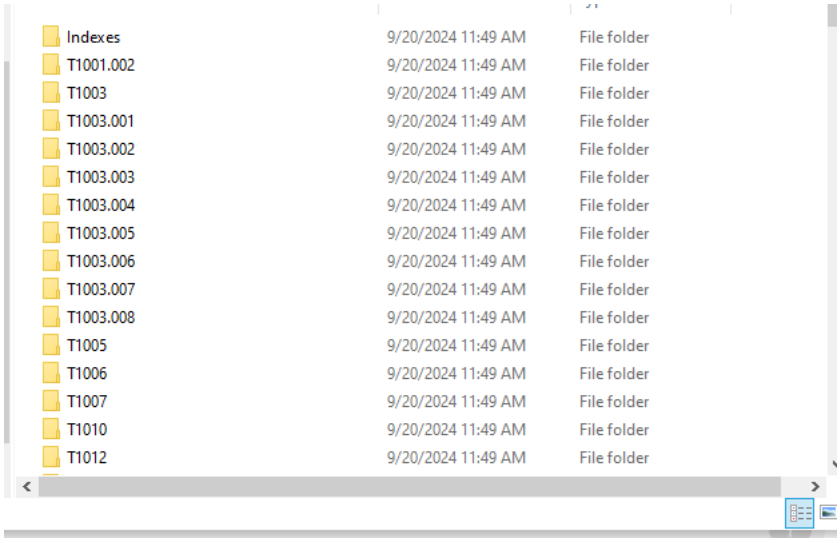
C Drive exclusion created

Now we will get Atomic Red Team by the "Install-AtomicRedTeam" -getAtomic

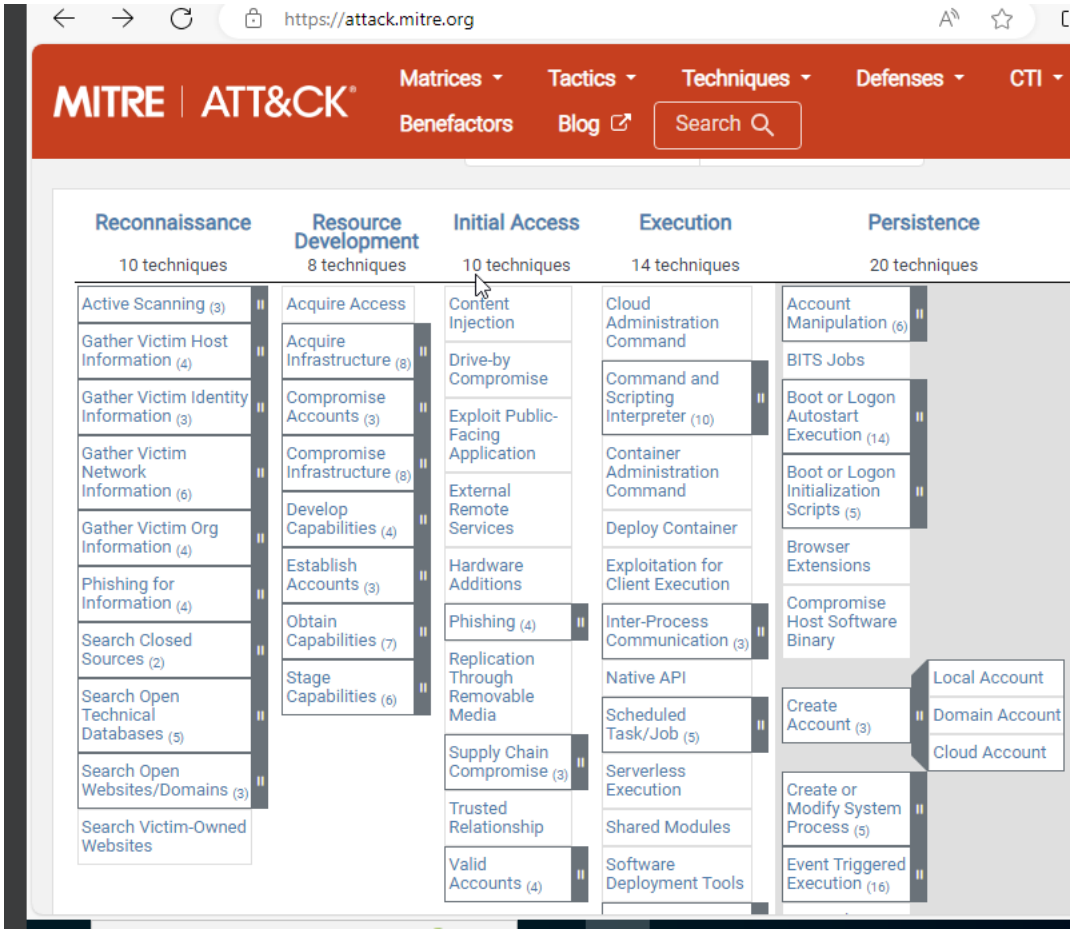


Atomic Red Team Installed

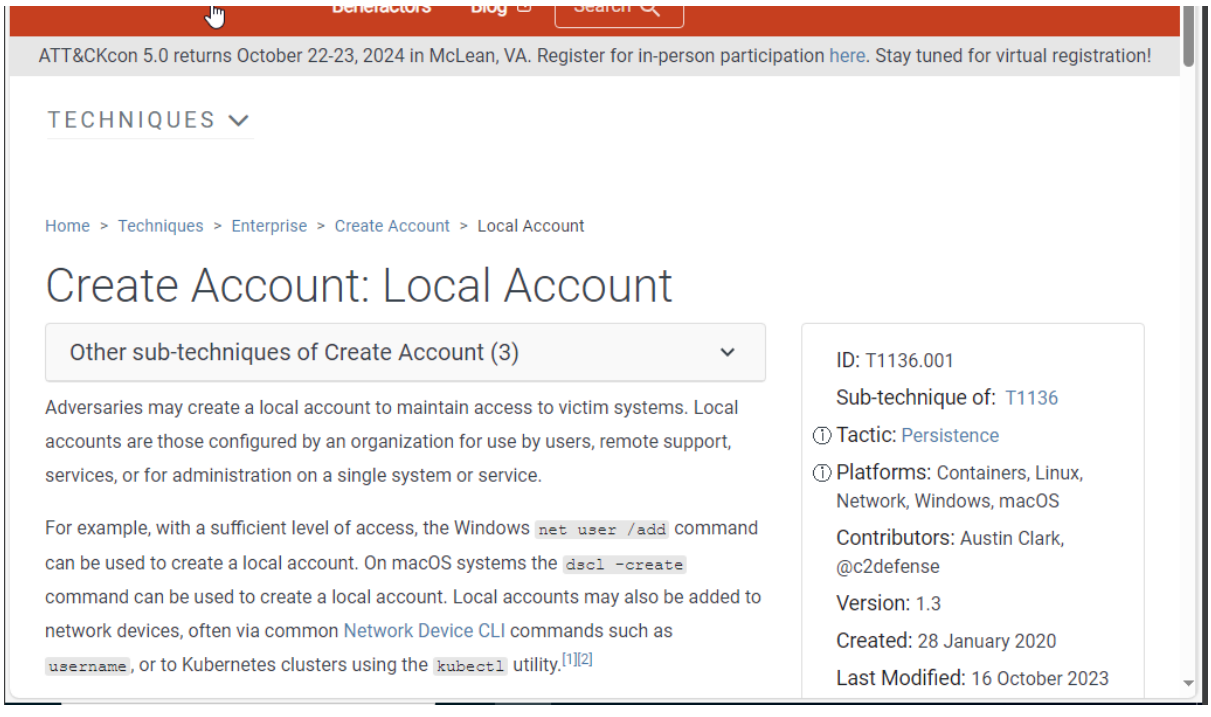
In "C:\AtomicRedTeam\atomic" we can see the technique ID's map back to MITRE attack framework.



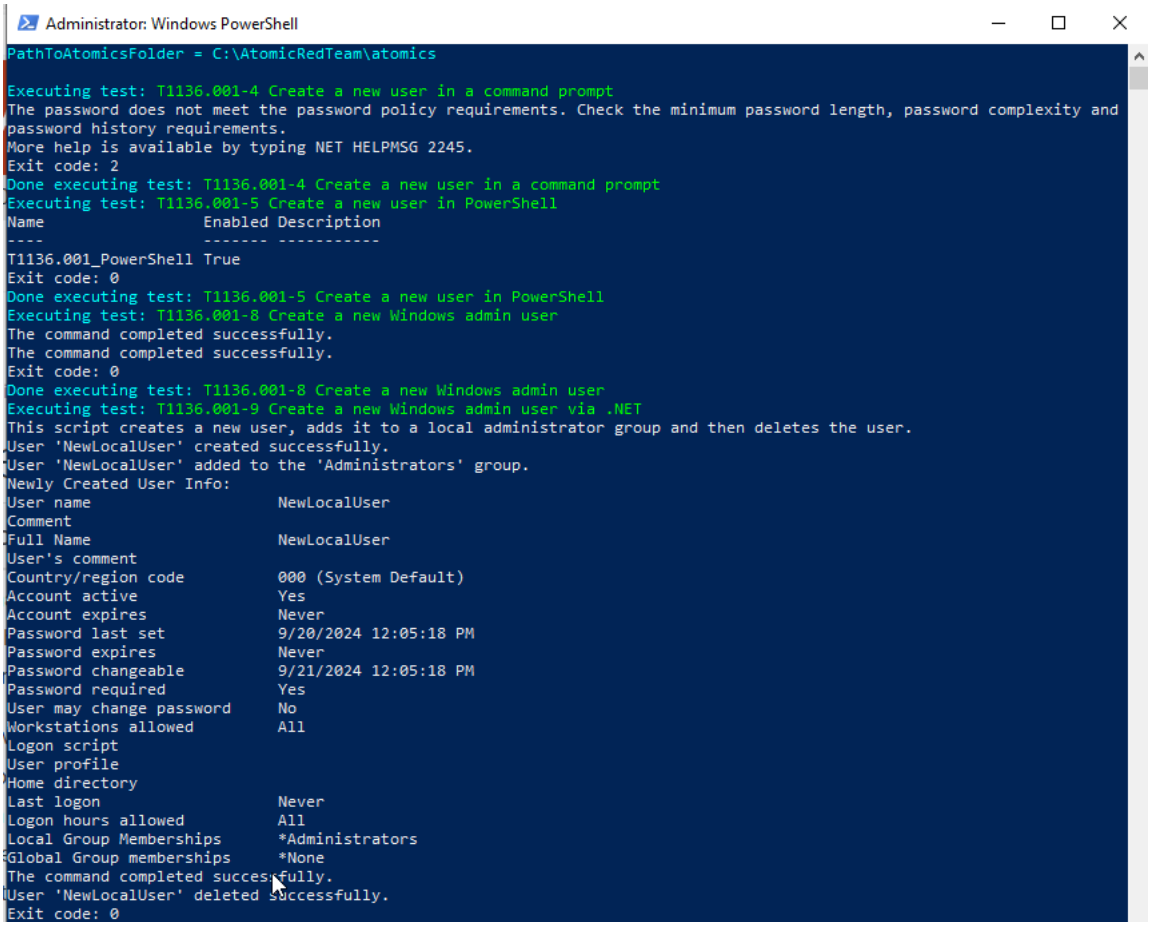
MT&T technique ID's



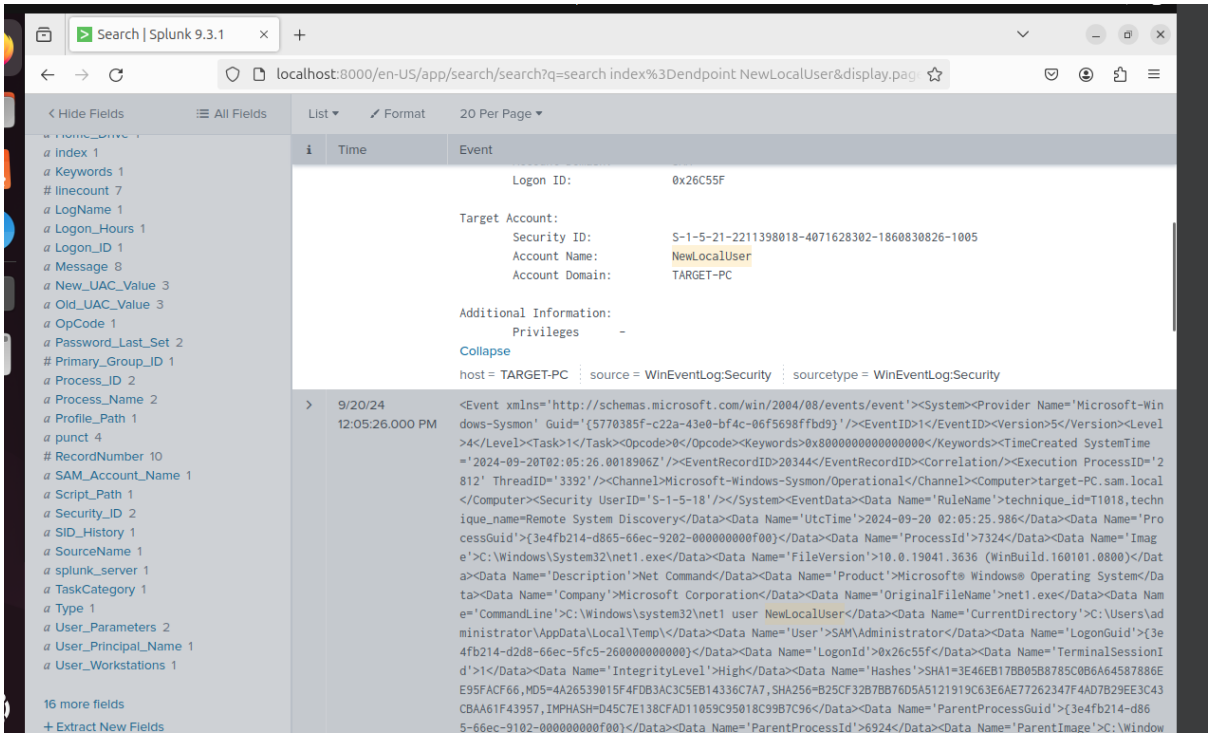
Inside the metre framework we can see the local account whose id is T1136.001



Local account ID



NewLocalUser created



Splunk detecting alert

Initially, we have identified the occurrence of a brute force attack. Following this attack, if the attacker successfully creates a local file on the victim machine, we can utilize Atomic Red Team to configure the victim machine for detecting this activity. By generating telemetry, we will be able to identify and analyse the local file created by the attacker, enhancing our understanding of the attack vector and its implications.

Discussion

Evaluation of Strategies

The Red Team's approach was methodical, effectively utilizing known vulnerabilities to exploit the target system. The Blue Team successfully detected the attack due to comprehensive logging and monitoring strategies. However, the attack highlighted vulnerabilities that could be addressed through more robust security measures.

Lessons Learned

Brute-force attacks remain a significant threat: Continuous monitoring and user education about strong passwords are crucial.

Importance of telemetry: The effectiveness of a SIEM like Splunk is underscored by its ability to provide real-time data analysis.

Recommendations

Implement multi-factor authentication to mitigate risks associated with brute-force attacks.

Regularly update and monitor logs in the SIEM to ensure timely detection of suspicious activities.

Conduct regular penetration testing and red teaming exercises to assess the resilience of security measures.

Conclusion

This project provided valuable insights into the dynamics between offensive and defensive cybersecurity roles. By simulating a controlled attack and analysing the responses, I gained practical knowledge on both the attack lifecycle and the necessary defense strategies to counteract such threats.

References

https://github.com/MyDFIR/Active-Directory-Project

https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml

https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/

https://www.splunk.com/en_us/download.html

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

https://ubuntu.com/download/server