

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

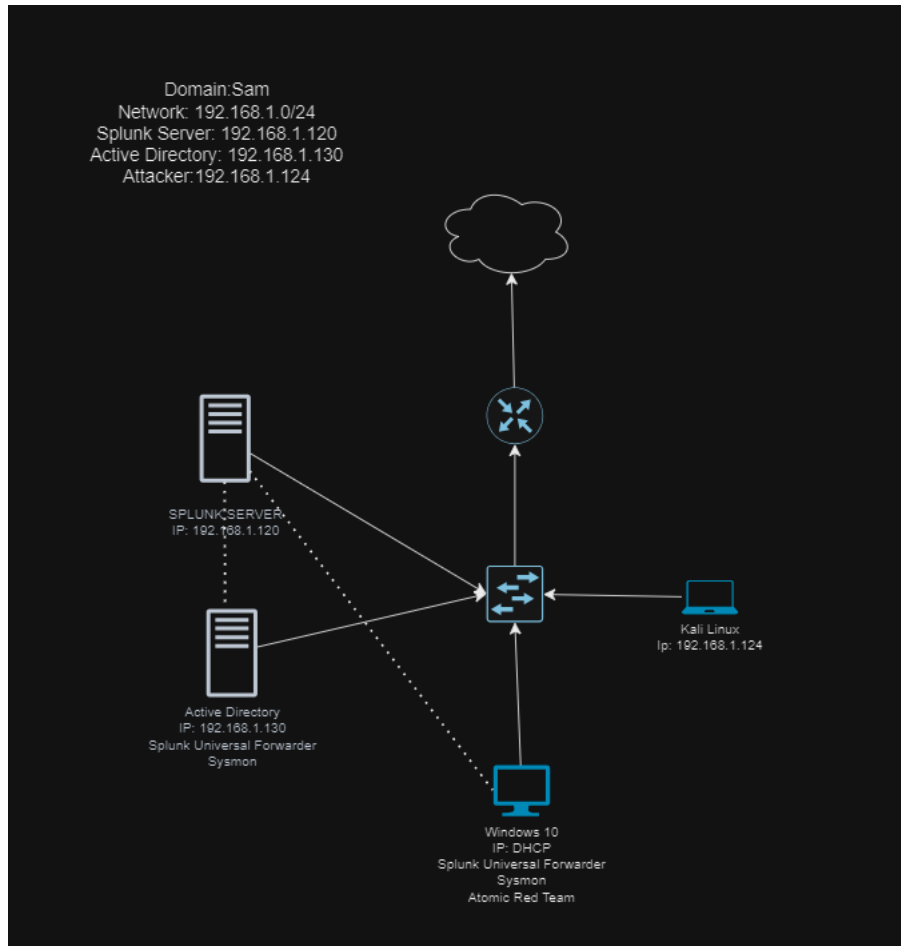
Lessons Learned 26

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.

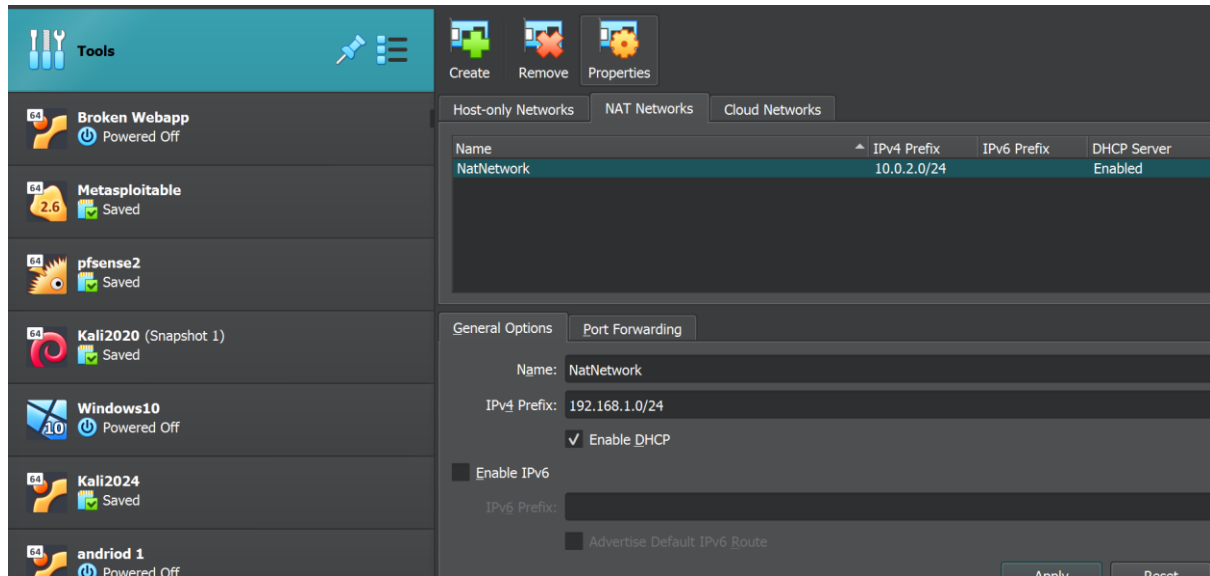
Windows 10: The target machine, user skabir.

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

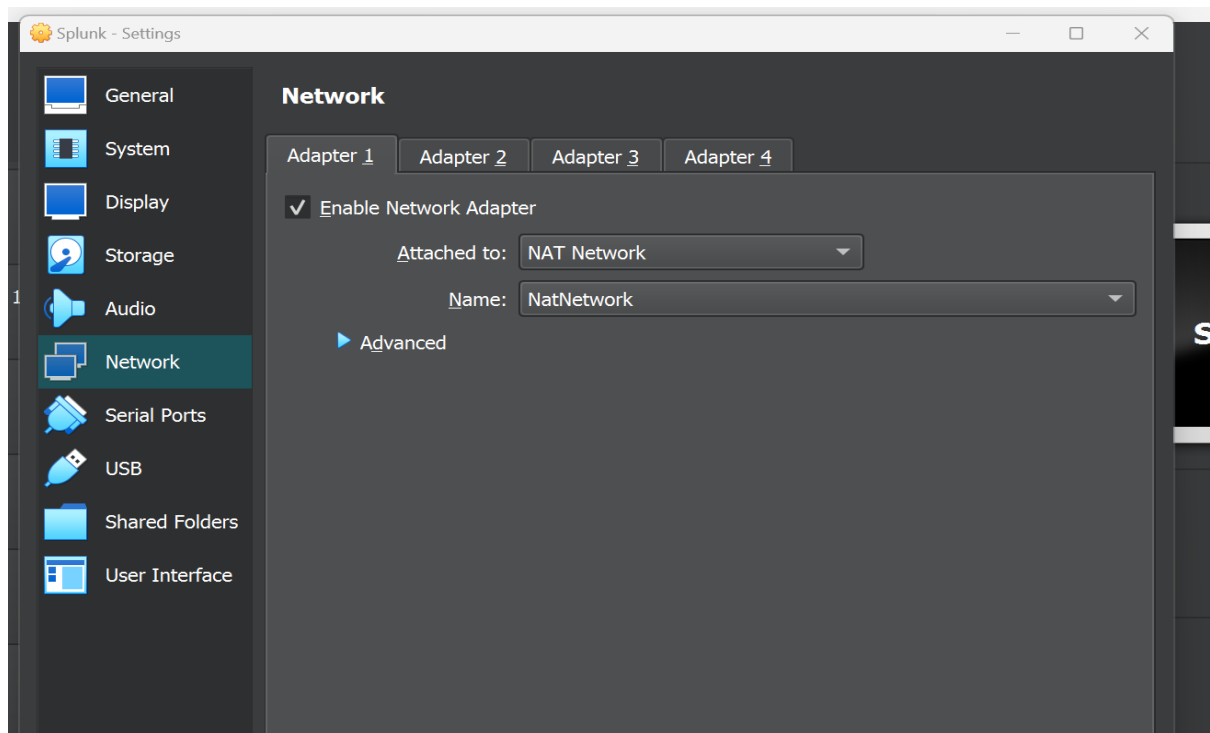
Splunk Server (Ubuntu): For telemetry data collection and analysis.

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

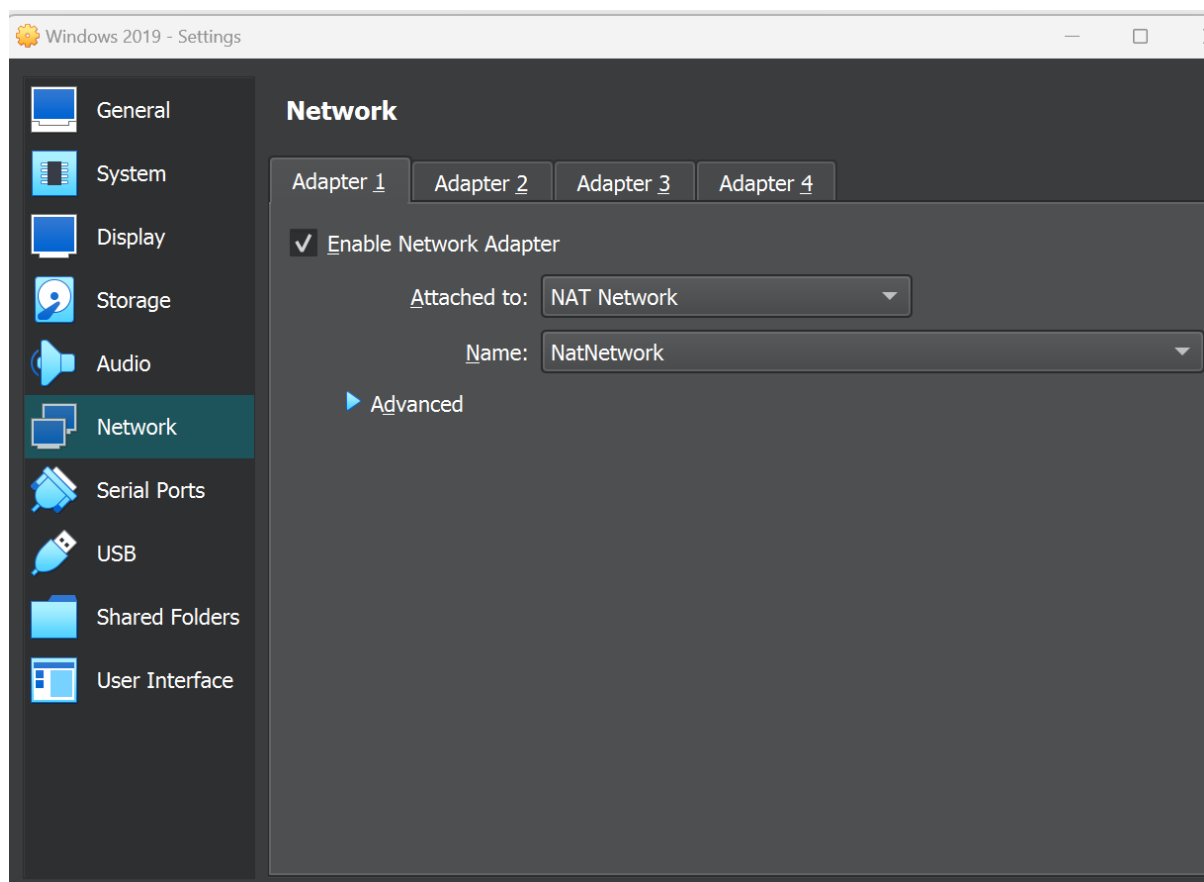
configurations. To establish the lab environment, we will set up and install Windows 10, Kali Linux, Windows Server 2019, and Ubuntu for the Splunk server. The first step involves creating a custom NAT network within VirtualBox. This configuration ensures that all virtual machines can communicate effectively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



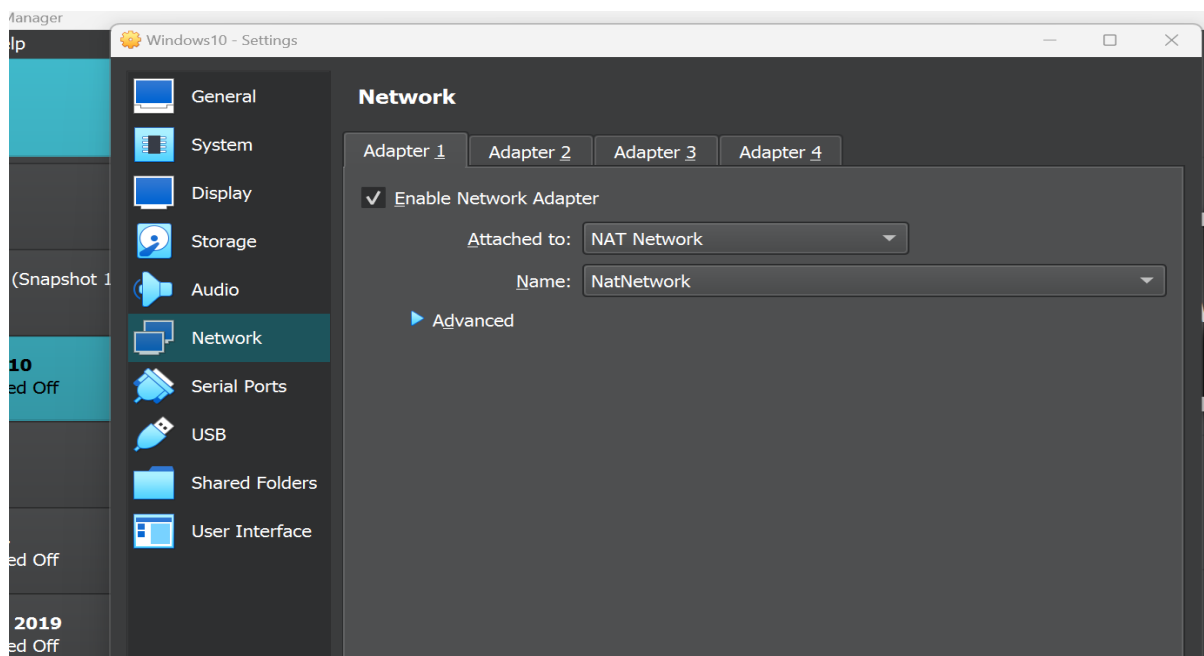
NAT Network



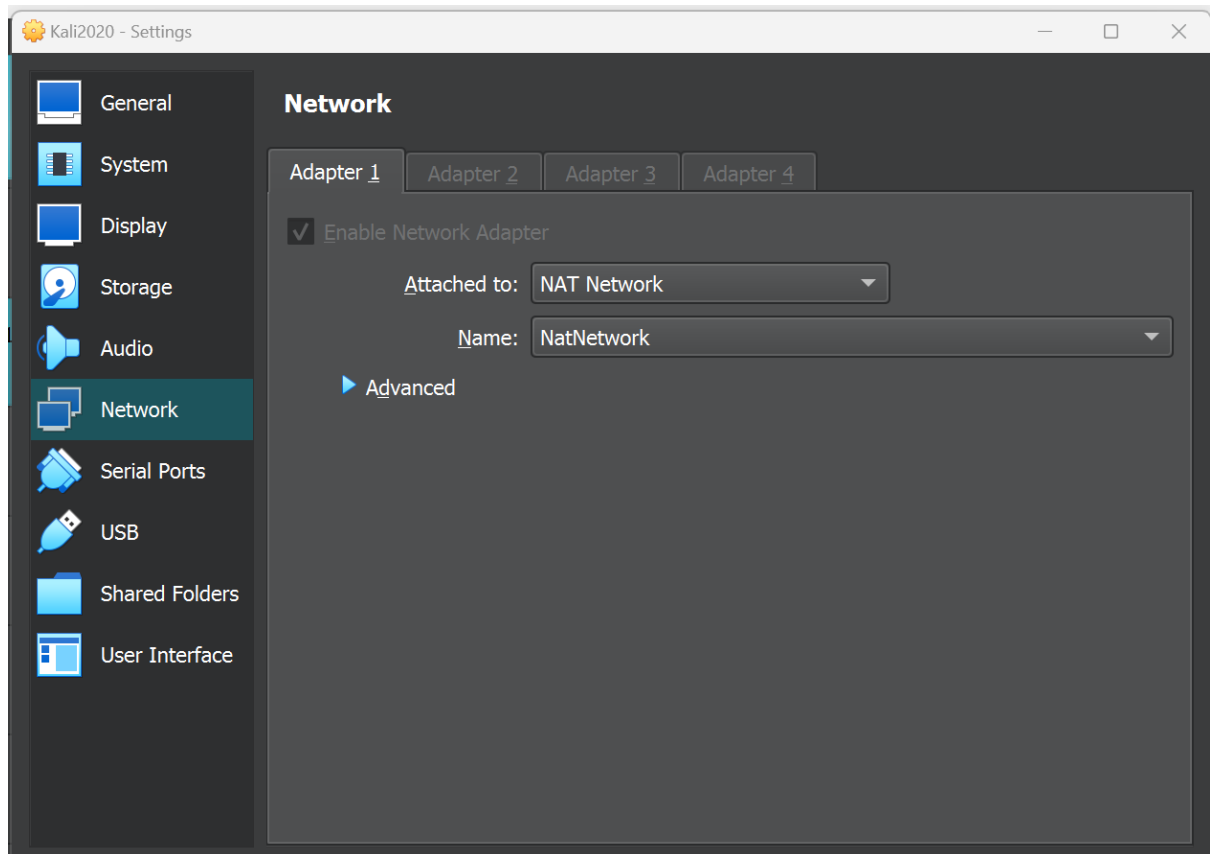
Splunk server on NAT NETWORK



Active Director server on NAT NETWORK

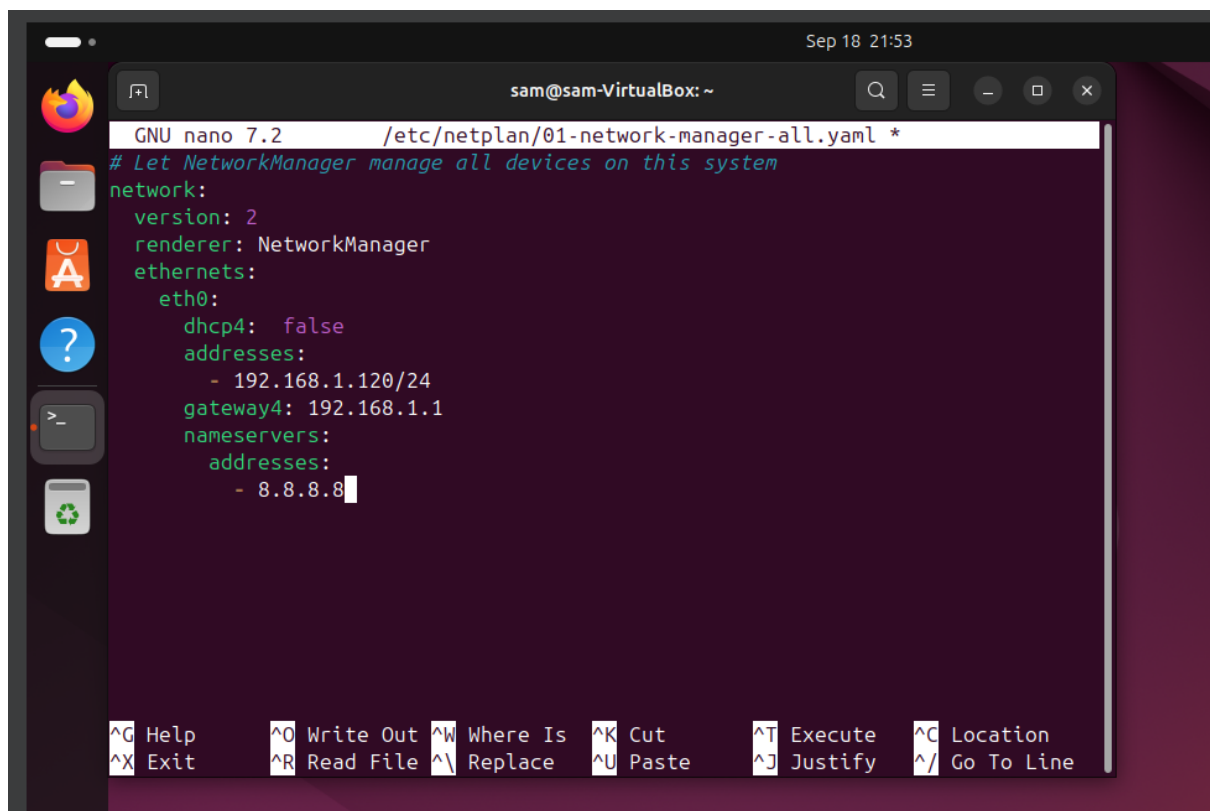


Windows 10 on NAT NETWORK



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

```
sam@sam-VirtualBox:~$ nmcli connection modify "netplan-enp0s3" ipv4.method manual
ipv4.addresses 192.168.1.120/24 ipv4.gateway 192.168.1.1 ipv4.dns 8.8.8.8
sam@sam-VirtualBox:~$ nmcli connection down "netplan-enp0s3" && nmcli connection
up "netplan-enp0s3"
Connection 'netplan-enp0s3' successfully deactivated (D-Bus active path: /org/fr
eedesktop/NetworkManager/ActiveConnection/2)
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkMa
nager/ActiveConnection/3)
sam@sam-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:58:13:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.120/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe58:131e/64 scope link
        valid_lft forever preferred_lft forever
sam@sam-VirtualBox:~$
```

Splunk Static IP assigned to 192.168.1.120

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

```
Sam@sam-VirtualBox: /opt/splunk
/var/lib/dpkg/info/splunk.postinst: line 123: curl: command not found
complete
Sam@sam-VirtualBox:~/share$ cd /opt/splunk
Sam@sam-VirtualBox:/opt/splunk$ ls -la
total 4880
drwxr-xr-x 11 splunk splunk 4096 Sep 18 23:04 .
drwxr-xr-x  3 root  root   4096 Sep 18 23:03 ..
drwxr-xr-x  4 splunk splunk 4096 Sep 18 23:04 bin
-r--r--r--  1 splunk splunk   57 Sep  6 03:25 copyright.txt
drwxr-xr-x 17 splunk splunk 4096 Sep 18 23:04 etc
-rw-r--r--  1 splunk splunk  434 Sep 18 23:04 ftr
drwxr-xr-x  4 splunk splunk 4096 Sep 18 23:04 include
drwxr-xr-x  9 splunk splunk 4096 Sep 18 23:04 lib
-r--r--r--  1 splunk splunk 85405 Sep  6 03:25 license-eula.txt
-r--r--r--  1 splunk splunk 1090 Aug 31 09:45 LICENSE.txt
drwxr-xr-x  3 splunk splunk 4096 Sep 18 23:04 openssl
drwxr-xr-x  3 splunk splunk 4096 Sep 18 23:04 opt
drwxr-xr-x  2 splunk splunk 4096 Sep 18 23:04 quarantined_files
-r--r--r--  1 splunk splunk  523 Sep  6 03:29 README-splunk.txt
drwxr-xr-x  4 splunk splunk 4096 Sep 18 23:04 share
-r--r--r--  1 splunk splunk 4847082 Sep  6 03:58 splunk-9.3.1-0b8d769cb912-linux
-2.6-x86_64-manifest
drwxr-xr-x  2 splunk splunk 4096 Sep 18 23:04 swidtag
Sam@sam-VirtualBox:/opt/splunk$
```

```

sam@sam-VirtualBox: /opt/splunk/bin
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available.....
Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://sam-VirtualBox:8000

splunk@sam-VirtualBox:~/bin$ exit
exit
sam@sam-VirtualBox:/opt/splunk$ cd bin
sam@sam-VirtualBox:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
sam@sam-VirtualBox:/opt/splunk/bin$
```

Splunk installed in Splunk server

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

```

C:\Users\Windows10>ipconfig

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::7b7f:7997:dd94:30af%4
IPv4 Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Users\Windows10>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : hub

Ethernet adapter Ethernet 2:

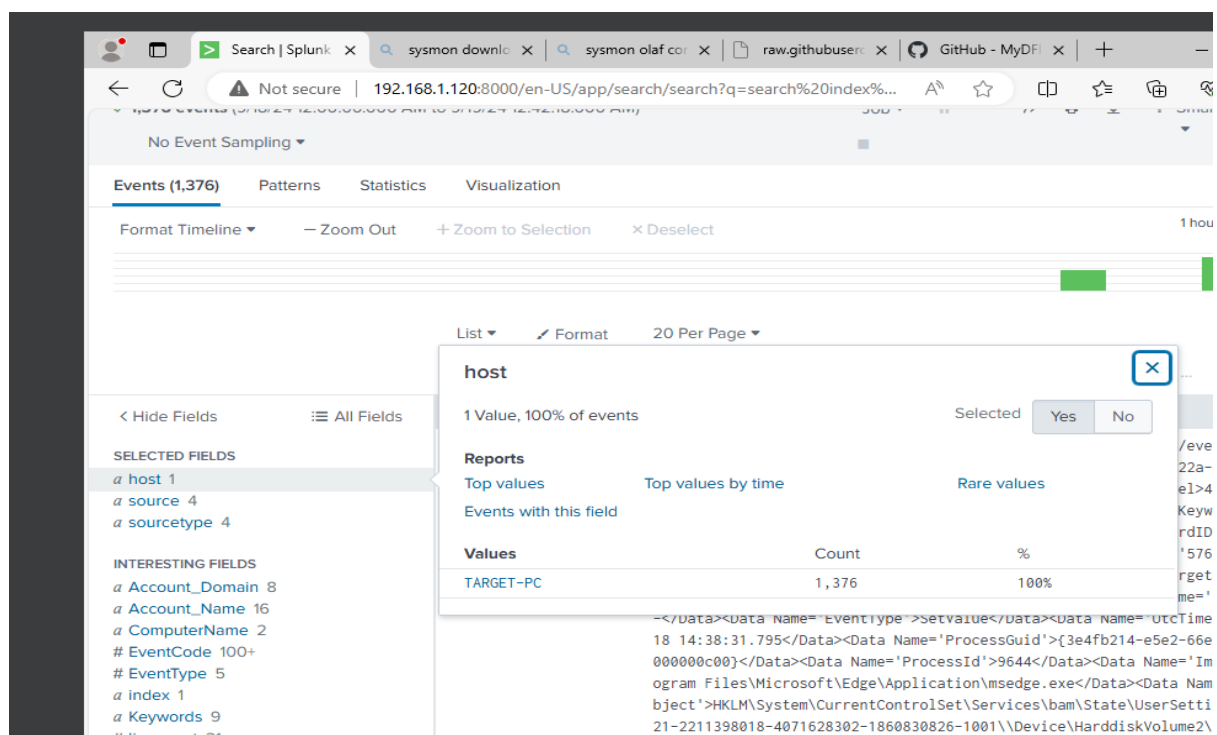
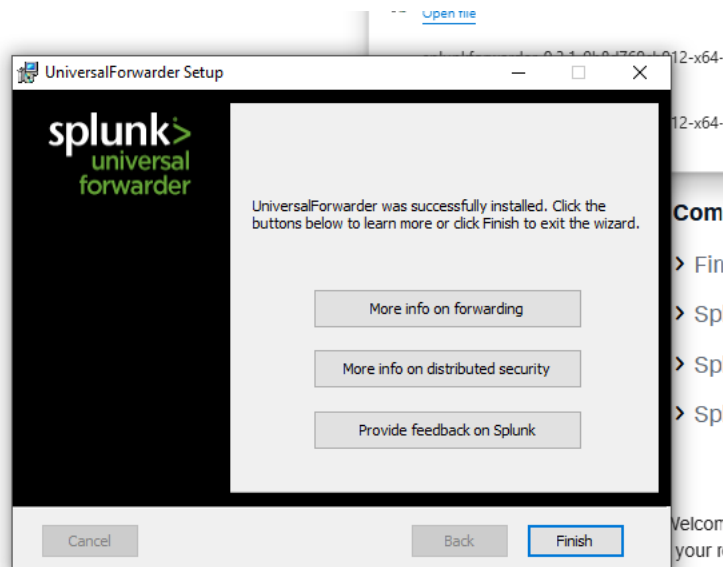
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::7b7f:7997:dd94:30af%4
IPv4 Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Users\Windows10>
```

Windows 10 Static IP configured

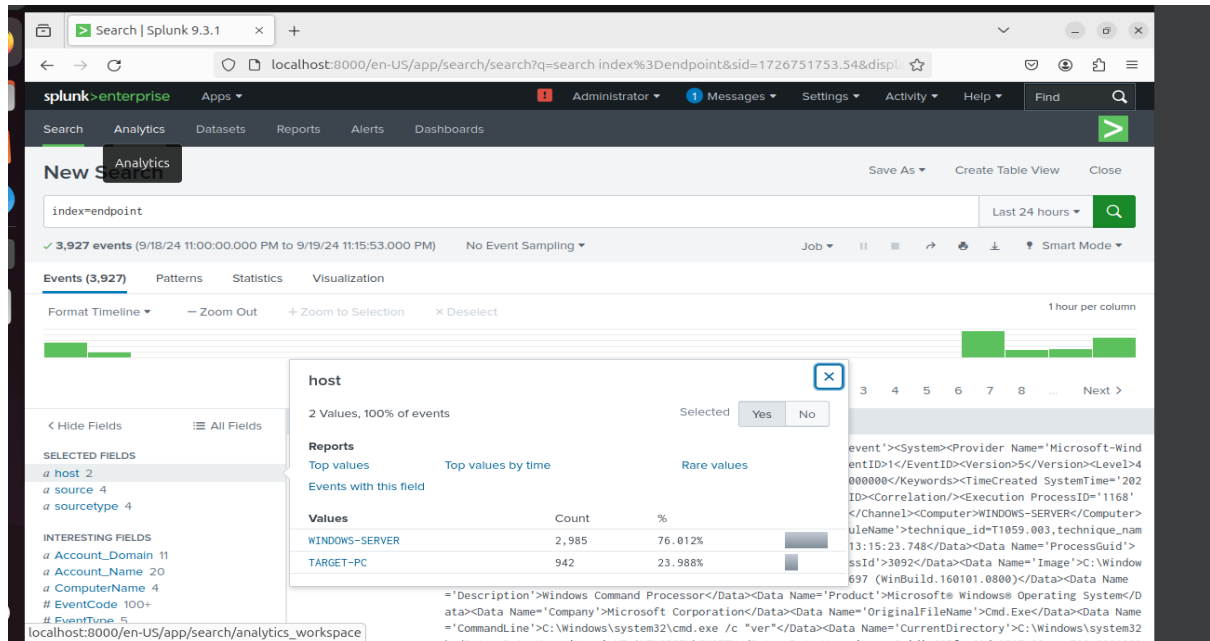
We will also install Sysmon and Splunk universal forwarder both into our target machines and server. Both collect telemetry and send logs over to Splunk server.

order



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.

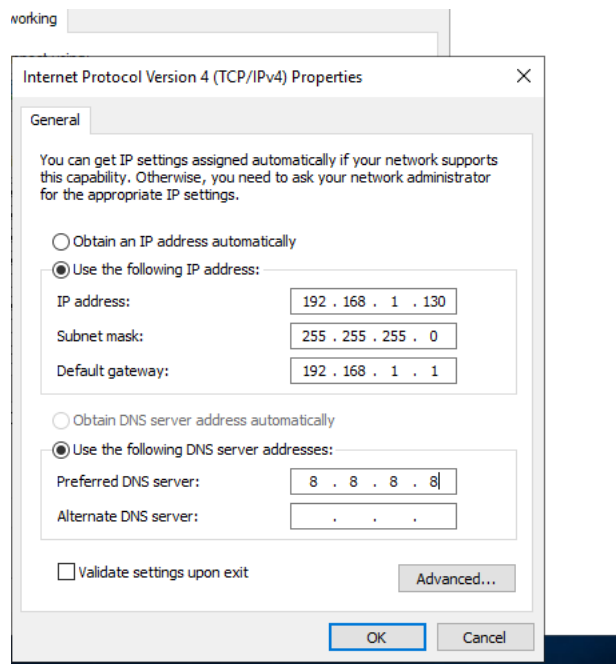


Splunk log showing 2 hubs

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.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

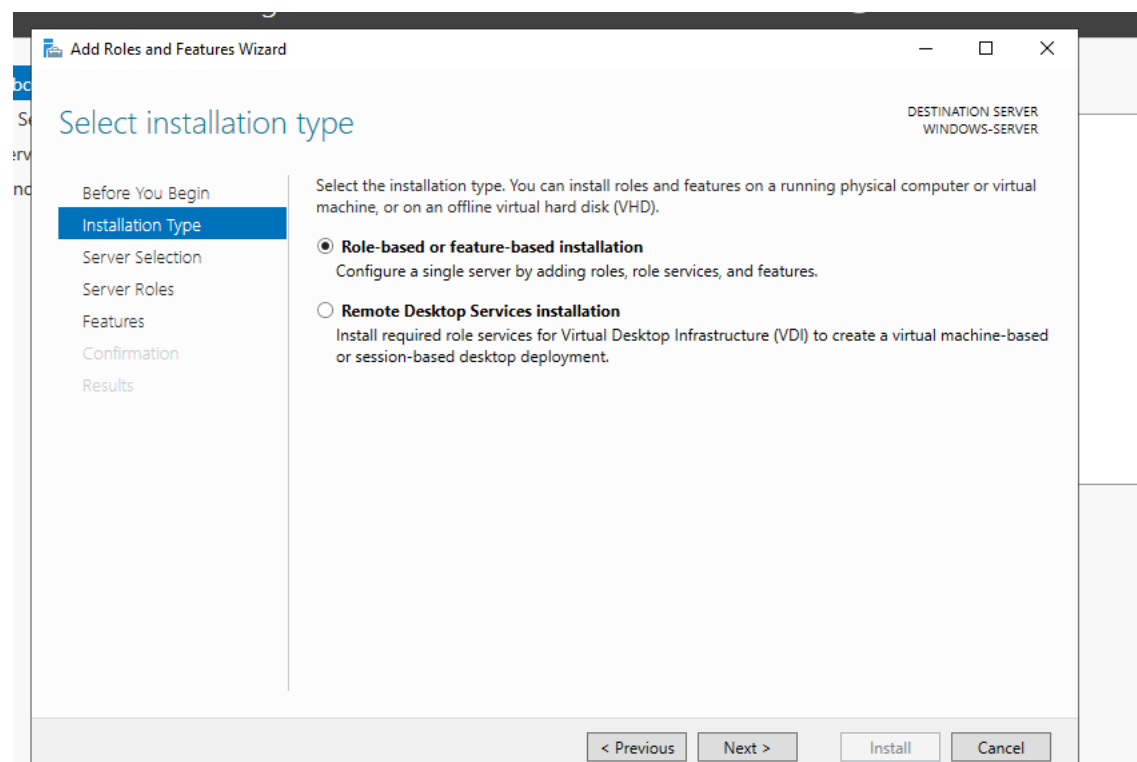
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.1.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

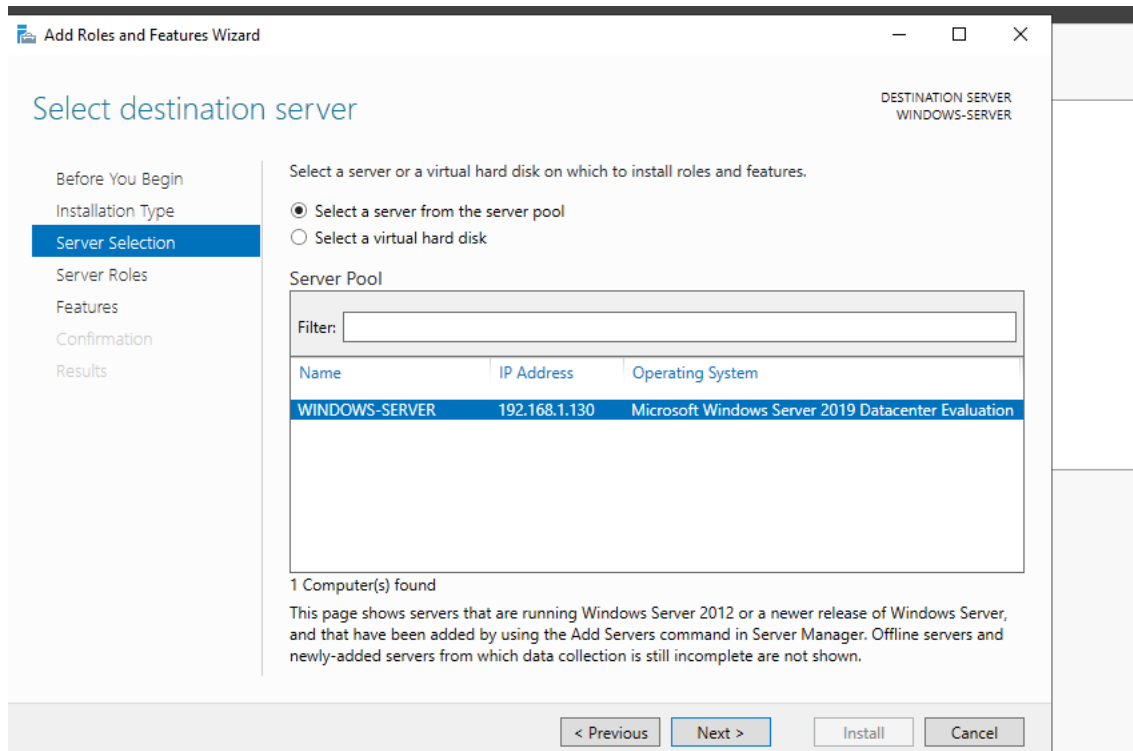
C:\Users\Administrator>
```

Static IP for windows server 2019

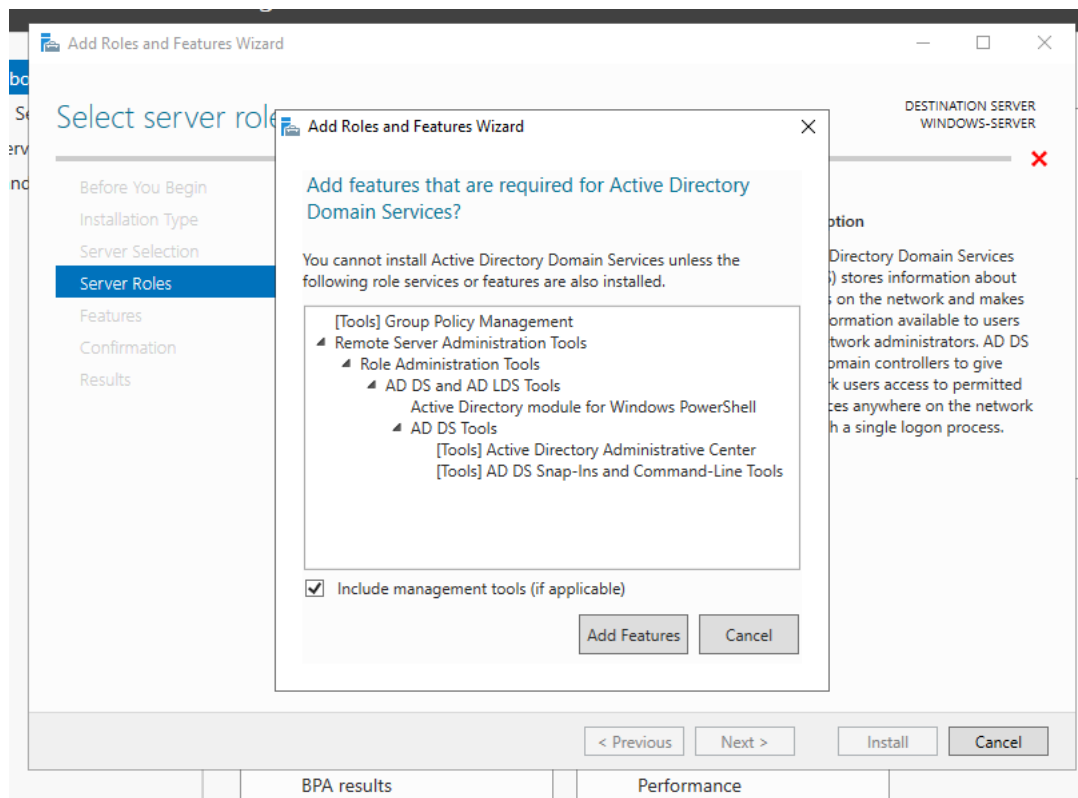
Now we will configure server manager "Add roles and features".



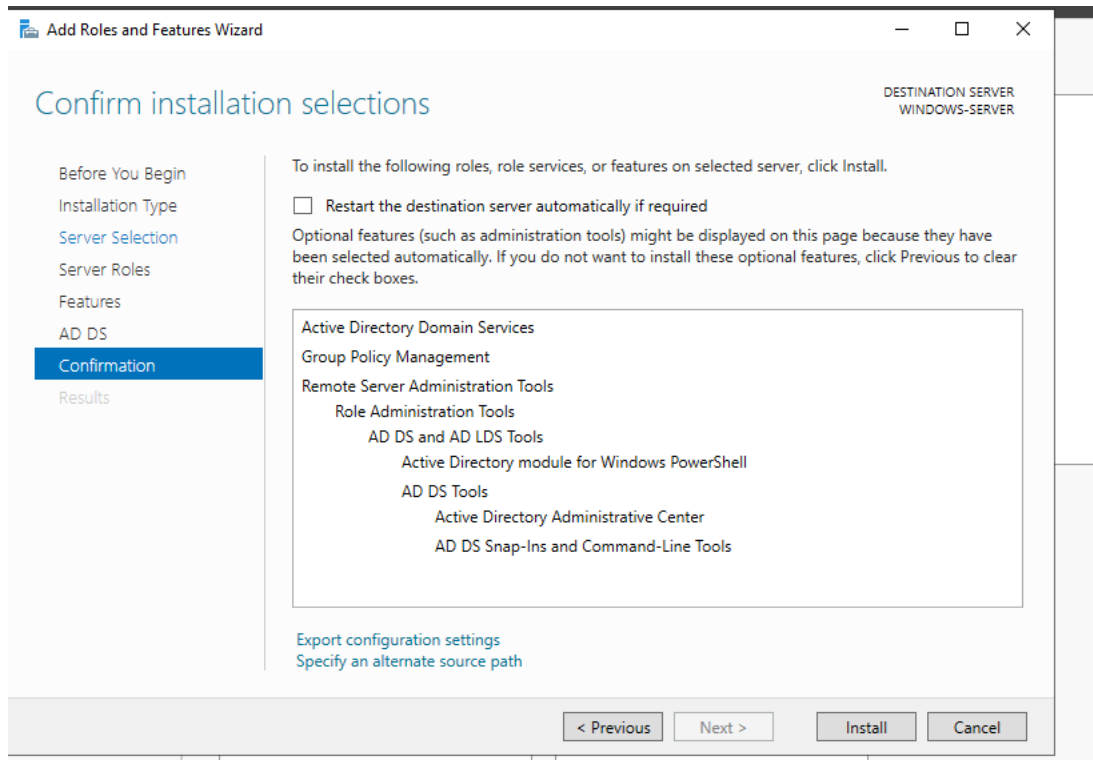
Selected Installation Type



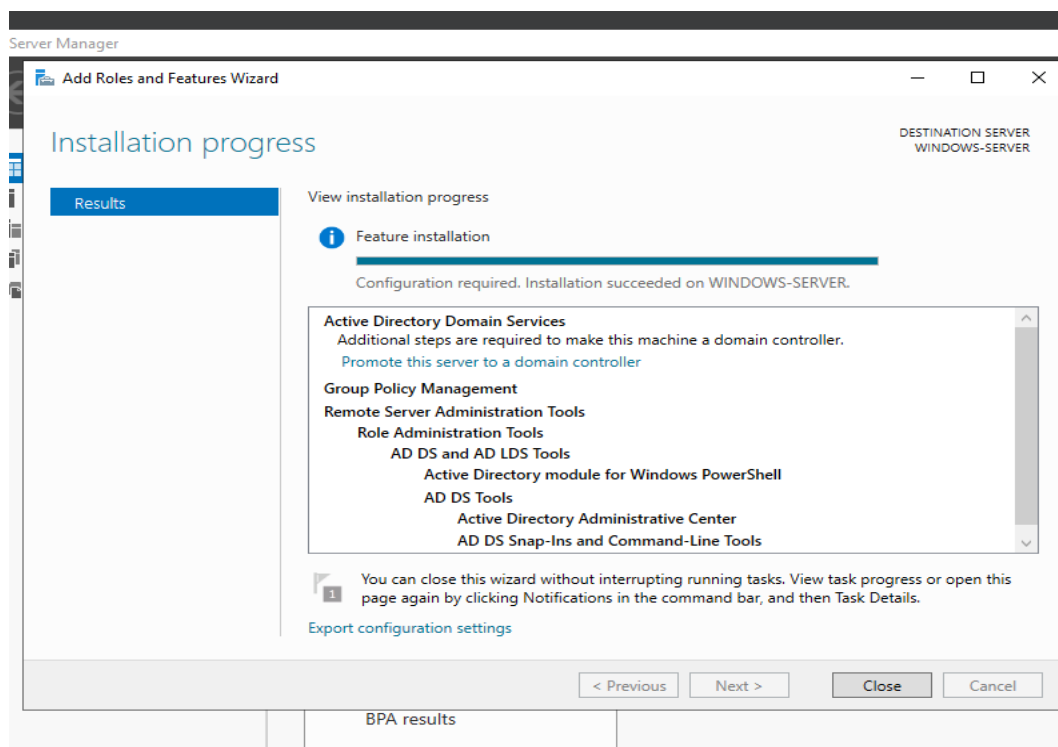
Selected Destination Server



Added Features

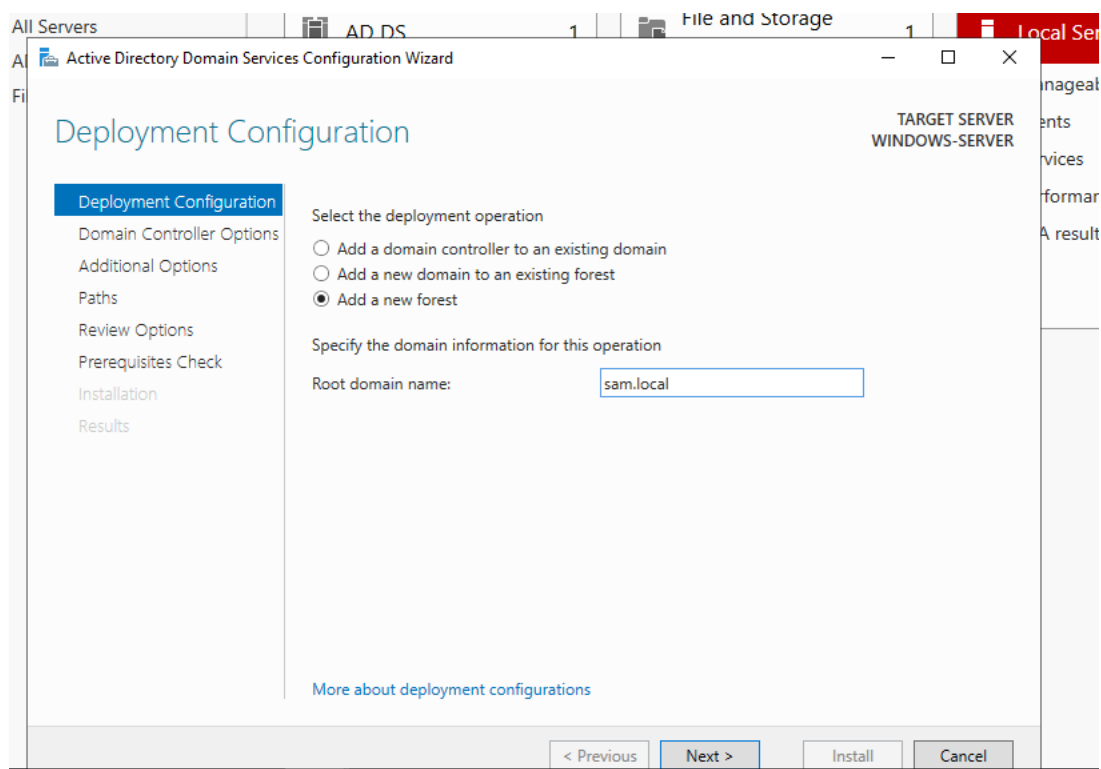


Confirmed Installation

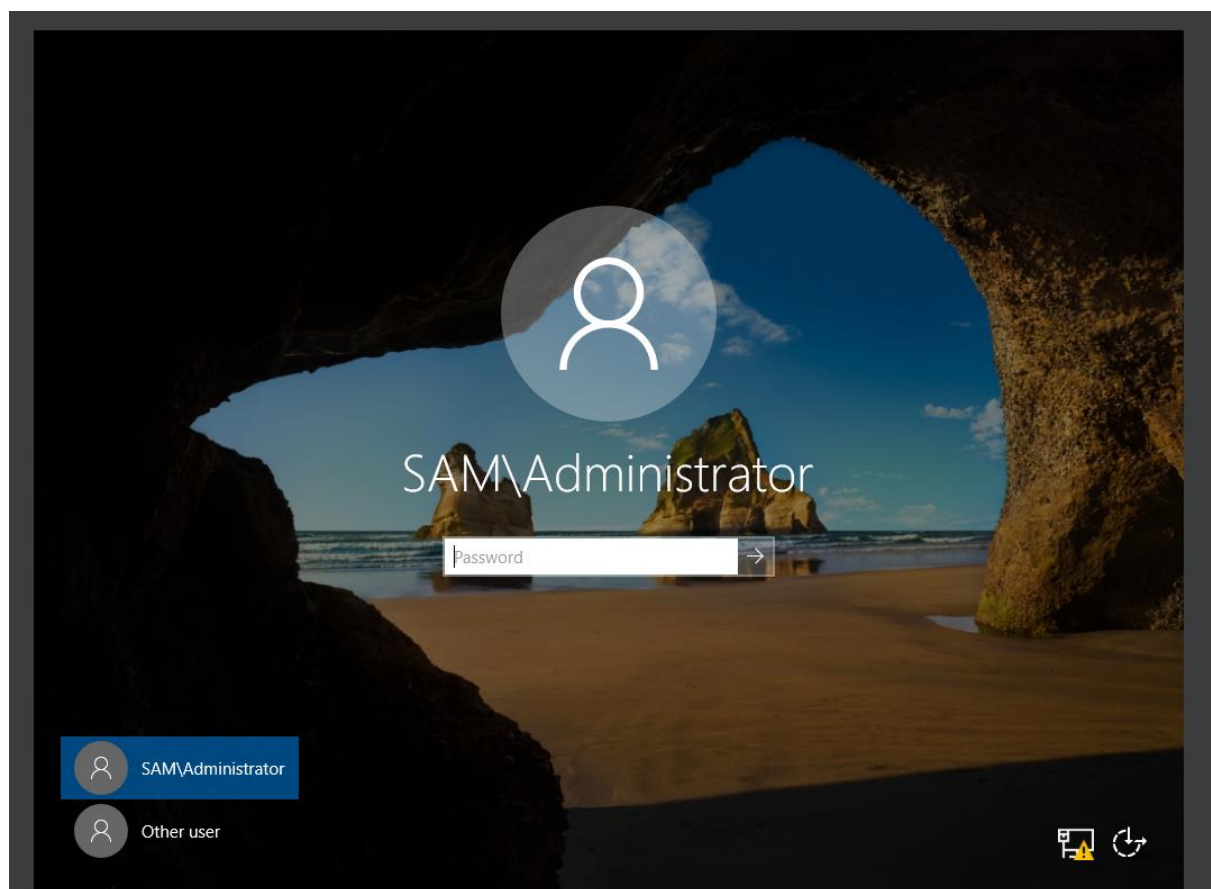


Added Active Directory Domain Services

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

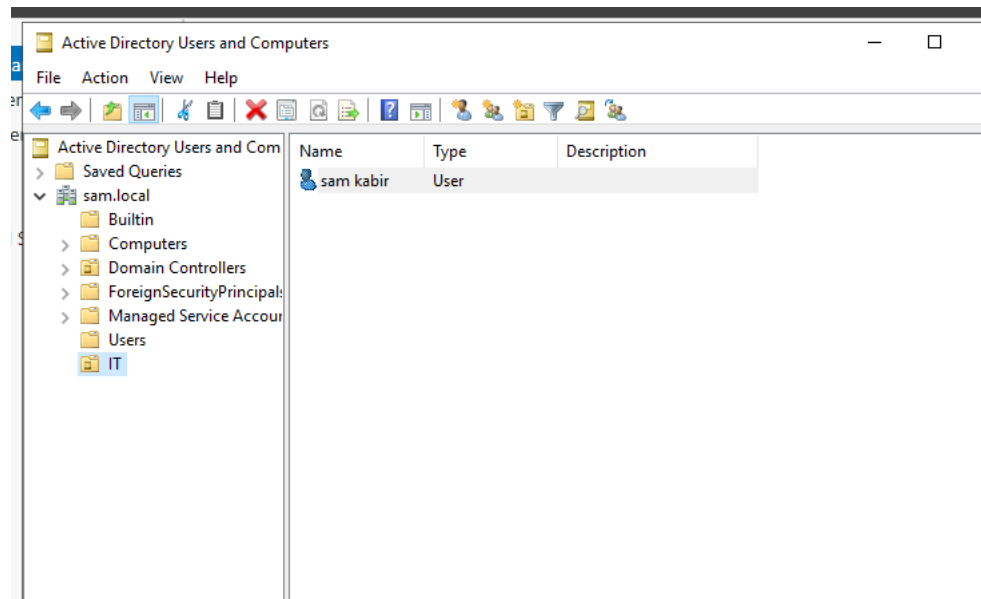


Domain name

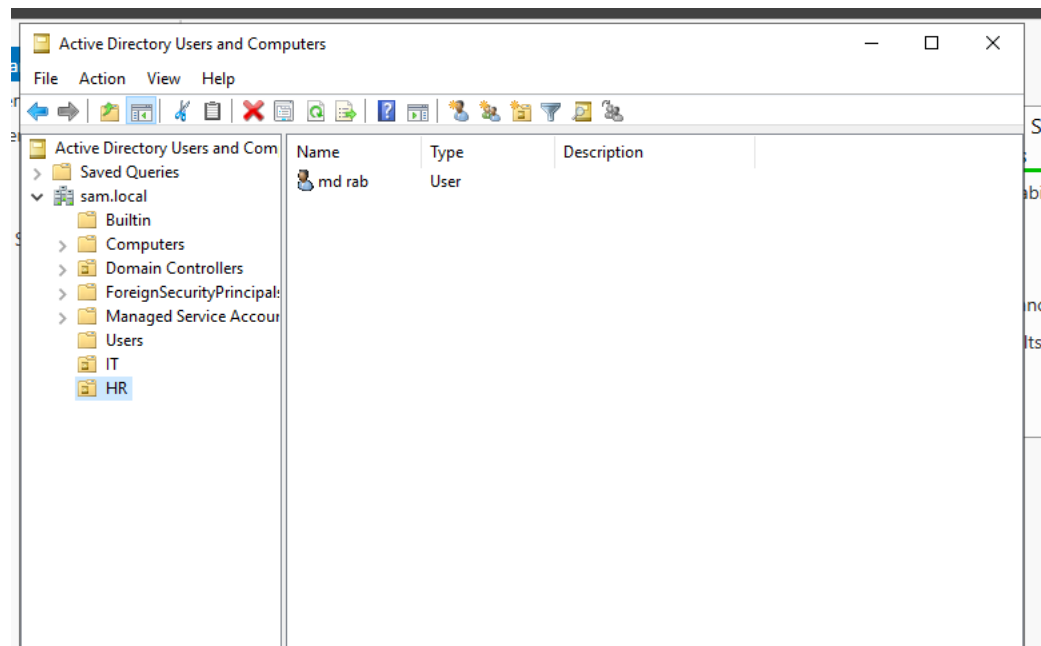


Login page Indicates AD-DS successfully created

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

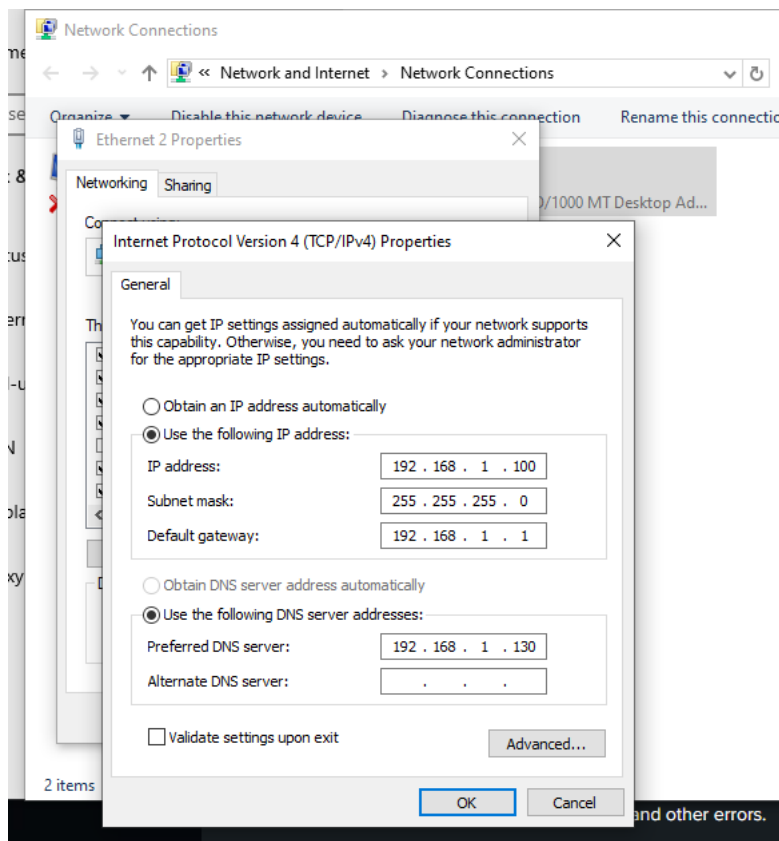
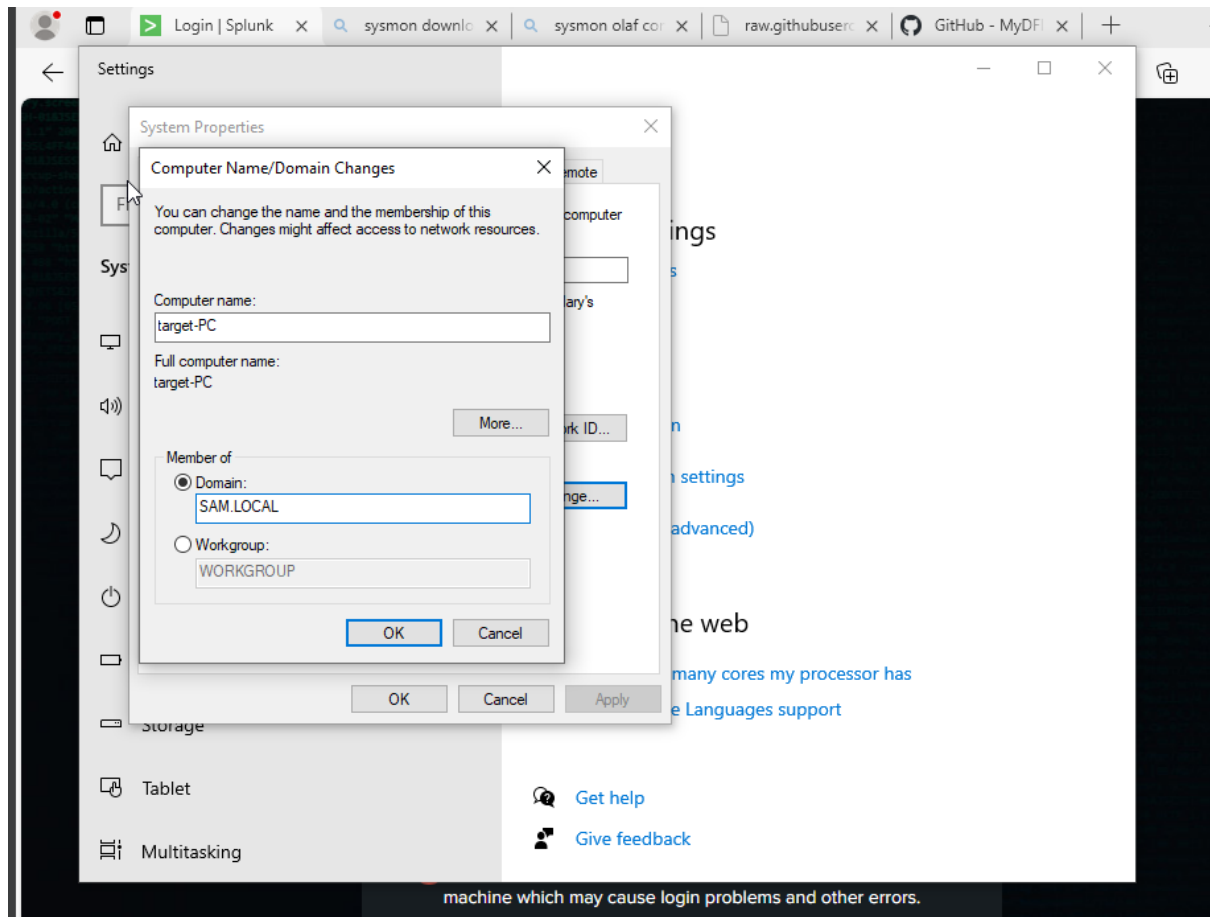


User "sam kabir" created



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.



```

C:\Users\Windows10>ipconfig /all

Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : hub
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Physical Address. . . . . : 08-00-27-60-43-34
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

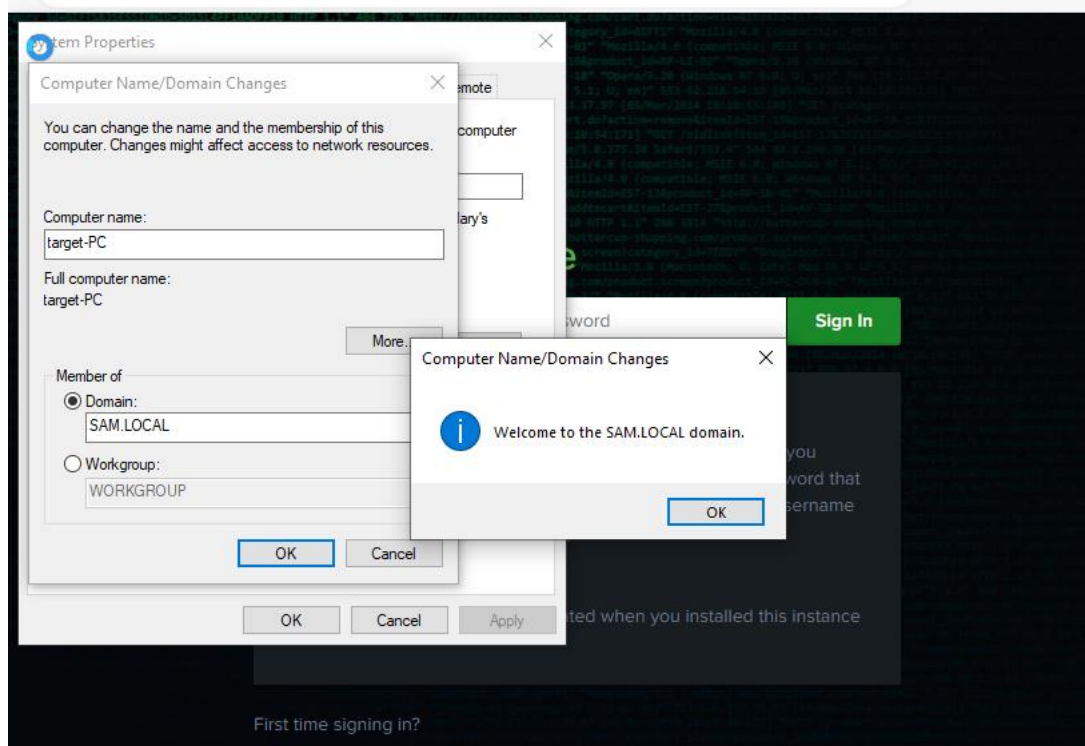
Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
    Physical Address. . . . . : 08-00-27-24-A5-CB
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::7b7f:7997:dd94:30af%4(Preferred)
    IPv4 Address. . . . . : 192.168.1.100(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 168296487
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-6B-57-F8-08-00-27-60-43-34
    DNS Servers . . . . . : 192.168.1.130
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Windows10>

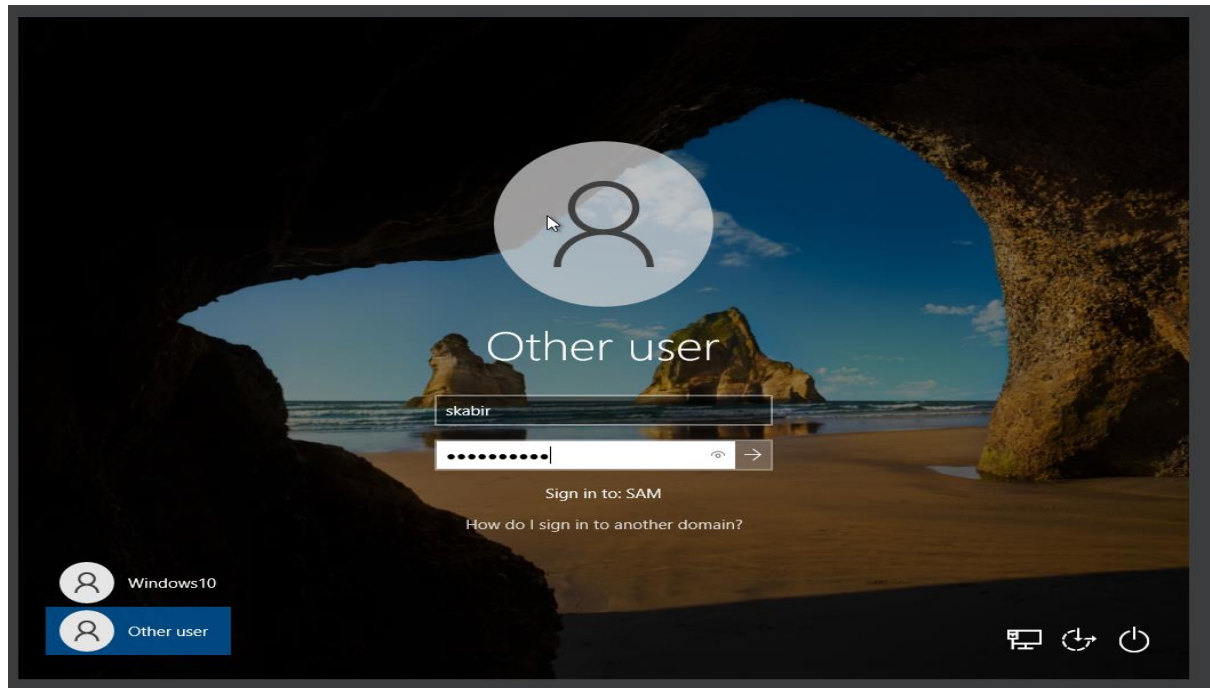
```

machine which may cause login problems and other errors.



Domain and DNS server Set UP

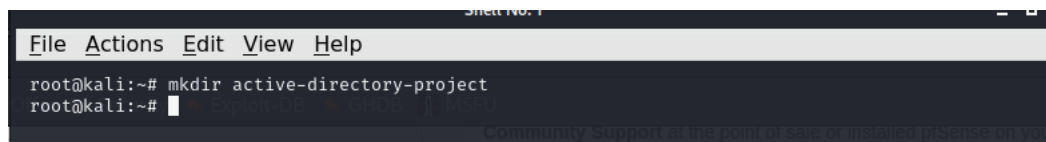
Now we will restart the windows 10 and will log in with newly created user skabir.



Logged In as "skabir" user

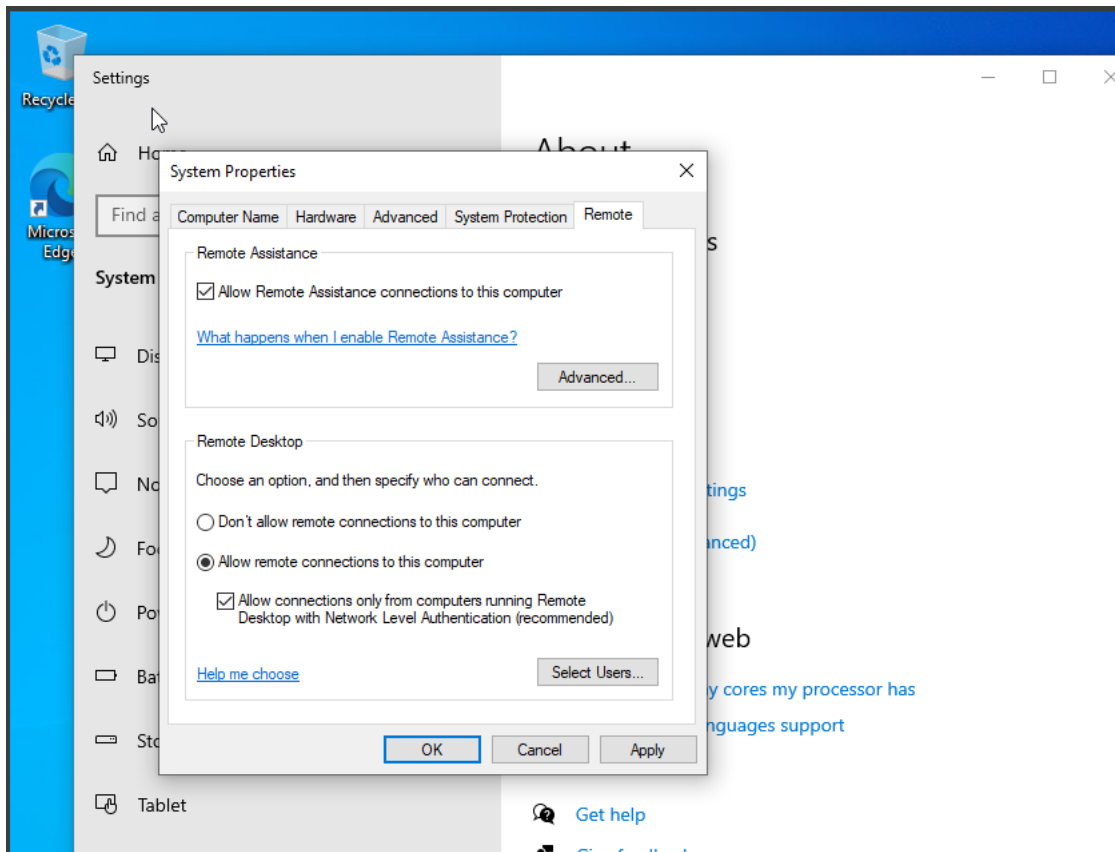
Now we will brute force attack from kali linux to user "skabir" and also we will set up atomic red team to run a test to generate telemetry and detect similar attack in future.

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

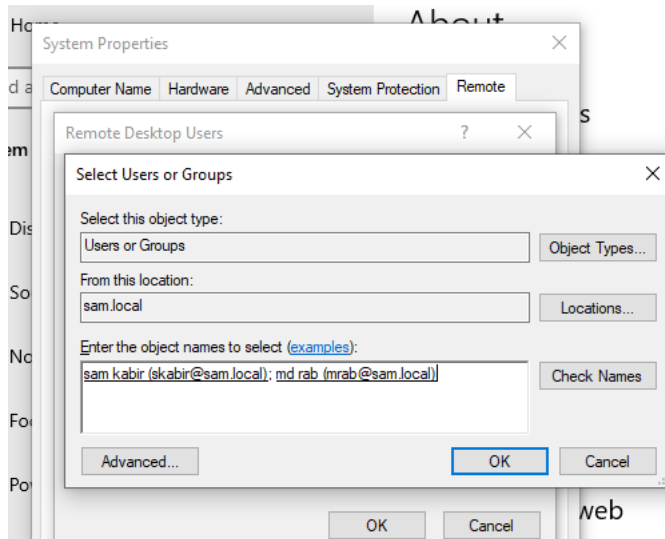


Created Directory

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.

```
root@kali:~/Desktop/active-directory-project# hydra -l skabir -P passwords.txt rdp://192.168.1.100
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 20:10:45
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 23 login tries (l:1/p:23), ~6 tries per task
[DATA] attacking rdp://192.168.1.100:3389/
[3389][rdp] host: 192.168.1.100 login: skabir password: Password.!2023
[3389][rdp] host: 192.168.1.100 login: skabir password: Password.!2023
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 20:10:54
root@kali:~/Desktop/active-directory-project#
```

RDP successful and Password generated



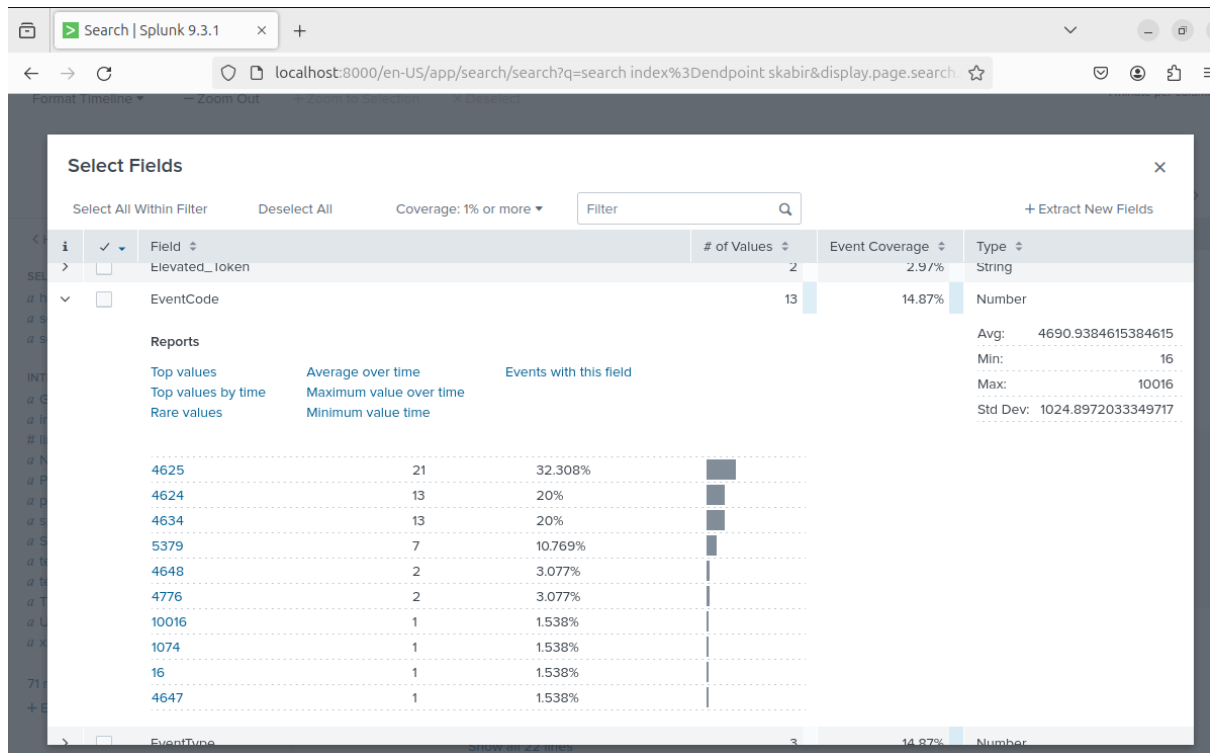
Now we can see the telemetry in the Splunk.

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

The screenshot shows the Splunk web interface. At the top, there's a search bar with the query "index=endpoint skabir". Below the search bar, it indicates "437 events" and a time range from "9/20/24 10:05:36.000 AM to 9/20/24 10:20:36.000 AM". The interface includes a navigation bar with tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. Below the search bar, there's a timeline visualization showing event distribution over time. The main content area displays a list of events. The first event is from "9/20/24 10:18:47.000 AM" and contains details such as "Security ID: S-1-5-21-1446815482-3529454313-1208060103-1107", "Account Name: skabir", "Account Domain: SAM", and "Logon ID: 0x1332780". The second event is from "9/20/24 10:18:45.000 AM" and also contains similar details. The interface also includes a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS" sections.

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 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.

The image shows a Splunk search results page for the query: `search index%3Dendpoint skabir EventCode%3D4625`. The results show multiple failed login attempts for the account 'skabir' on 9/20/2024 at 10:10:58.000 AM. The events are grouped by time, showing that all attempts occurred at the same time.

Time	Event
9/20/2024 10:10:58.000 AM	Security ID: S-1-0-0 Account Name: skabir Account Domain: TARGET-PC host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
9/20/2024 10:10:58.000 AM	Security ID: S-1-0-0 Account Name: skabir Account Domain: TARGET-PC host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
9/20/2024 10:10:58.000 AM	Security ID: S-1-0-0 Account Name: skabir Account Domain: TARGET-PC host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
9/20/2024 10:10:58.000 AM	Security ID: S-1-0-0 Account Name: skabir Account Domain: TARGET-PC host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security

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.

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background with white text. The text shows the PowerShell prompt at "PS C:\Windows\system32>" followed by the command "Set-ExecutionPolicy Bypass CurrentUser". Below the command, a message appears: "Execution Policy Change". It states: "The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?". It then lists options: "[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is 'N'):". The user has entered 'y' at the end of the line, and the prompt returns to "PS C:\Windows\system32>".

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

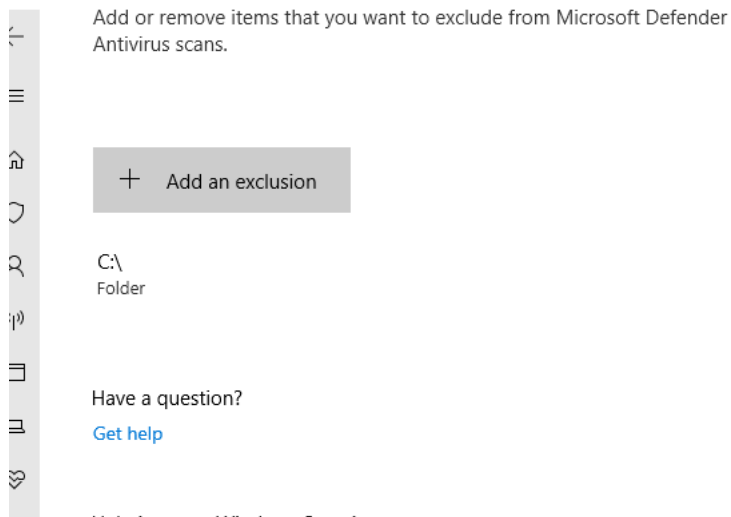
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-ExecutionPolicy Bypass CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32>
```

Set Up Execution Policy

Now we will set up an exclusion for C Drive.



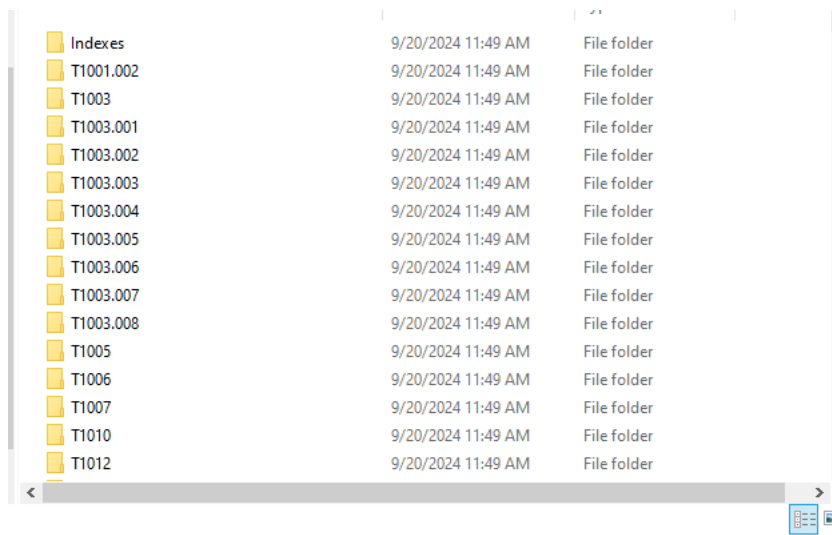
C Drive exclusion created

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

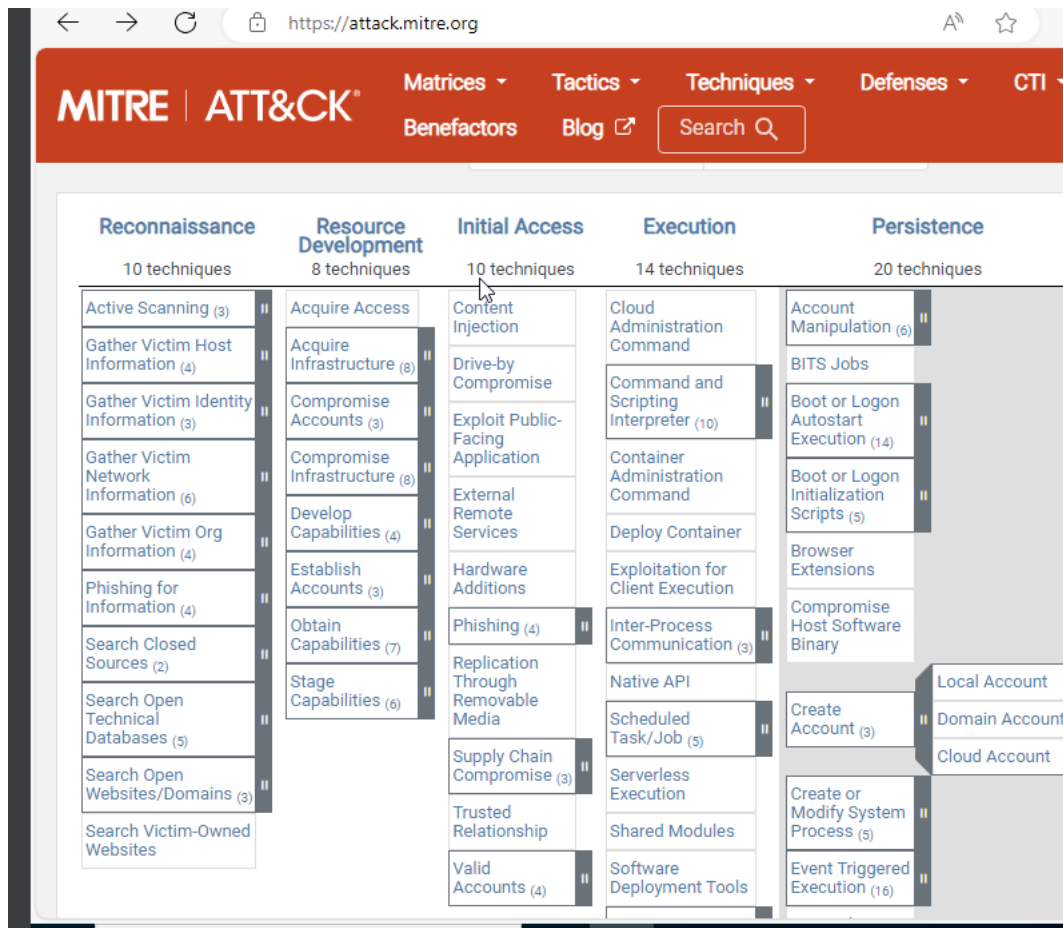
```
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomic
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
PS C:\Windows\system32>
```

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

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Register for in-person participation [here](#). Stay tuned for virtual registration!

TECHNIQUES ▾

Home > Techniques > Enterprise > Create Account > Local Account

Create Account: Local Account

Other sub-techniques of Create Account (3) ▾

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

For example, with a sufficient level of access, the Windows `net user /add` command can be used to create a local account. On macOS systems the `dscl -create` command can be used to create a local account. Local accounts may also be added to network devices, often via common [Network Device CLI](#) commands such as `username`, or to Kubernetes clusters using the `kubect1` utility.^{[1][2]}

ID: T1136.001
Sub-technique of: T1136
① **Tactic:** Persistence
① **Platforms:** Containers, Linux, Network, Windows, macOS
Contributors: Austin Clark, @c2defense
Version: 1.3
Created: 28 January 2020
Last Modified: 16 October 2023

Local account ID



```
Administrator: Windows PowerShell

PathToAtomicFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-4 Create a new user in a command prompt
The password does not meet the password policy requirements. Check the minimum password length, password complexity and
password history requirements.
More help is available by typing NET HELPMSG 2245.
Exit code: 2
Done executing test: T1136.001-4 Create a new user in a command prompt
Executing test: T1136.001-5 Create a new user in PowerShell
Name                Enabled Description
-----
T1136.001_PowerShell True
Exit code: 0
Done executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-8 Create a new Windows admin user
The command completed successfully.
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-8 Create a new Windows admin user
Executing test: T1136.001-9 Create a new Windows admin user via .NET
This script creates a new user, adds it to a local administrator group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the 'Administrators' group.
Newly Created User Info:
User name                NewLocalUser
Comment
Full Name                NewLocalUser
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never
Password last set        9/20/2024 12:05:18 PM
Password expires         Never
Password changeable      9/21/2024 12:05:18 PM
Password required        Yes
User may change password No
Workstations allowed     All
Logon script
User profile
Home directory
Last logon              Never
Logon hours allowed      All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
User 'NewLocalUser' deleted successfully.
Exit code: 0
```

NewLocalUser created

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Search | Splunk 9.3.1
- URL:** localhost:8000/en-US/app/search/search?q=search index%3Dendpoint NewLocalUser&display.page
- Fields List (Left):** Includes fields like `Logon_ID`, `Target Account`, `Security ID`, `Account Name`, `Account Domain`, `Privileges`, `host`, `source`, `sourcetype`, etc.
- Search Results (Table):**

Time	Event
9/20/24 12:05:26.000 PM	<p><Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-09-20T02:05:26.0018906Z' /><EventRecordID>20344</EventRecordID><Correlation><Execution ProcessID='2812' ThreadID='3392' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>target-PC.sam.local</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1018, technique_name=Remote System Discovery</Data><Data Name='UtcTime'>2024-09-20 02:05:25.986</Data><Data Name='ProcessGuid'>{3e4fb214-d865-66ec-9202-000000000000}</Data><Data Name='ProcessId'>7324</Data><Data Name='Image'>C:\Windows\System32\net1.exe</Data><Data Name='FileVersion'>10.0.19041.3636 (WinBuild.160101.0800)</Data><Data Name='Description'>Net Command</Data><Data Name='Product'>Microsoft Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>net1.exe</Data><Data Name='CommandLine'>C:\Windows\System32\net1 user NewLocalUser</Data><Data Name='CurrentDirectory'>C:\Users\administrator\AppData\Local\Temp</Data><Data Name='User'>SAM\Administrator</Data><Data Name='LogonGuid'>{3e4fb214-d2d8-66ec-5f5c-260000000000}</Data><Data Name='LogonId'>0x26c55f</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=3E46EB17B05B8785C0B6A64587886E95FACF66, MD5=4A26539015F4F0B3AC35EB14336C7A7, SHA256=B25CF32B78B76D5A5121919C63E6AE77262347F4AD7B29EE3C43CBAA61F43957, IMPHASH=D45C7E138CFAD11059C95018C99B7C96</Data><Data Name='ParentProcessGuid'>{3e4fb214-d865-66ec-9102-000000000000}</Data><Data Name='ParentProcessId'>6924</Data><Data Name='ParentImage'>C:\Window</p>

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>

