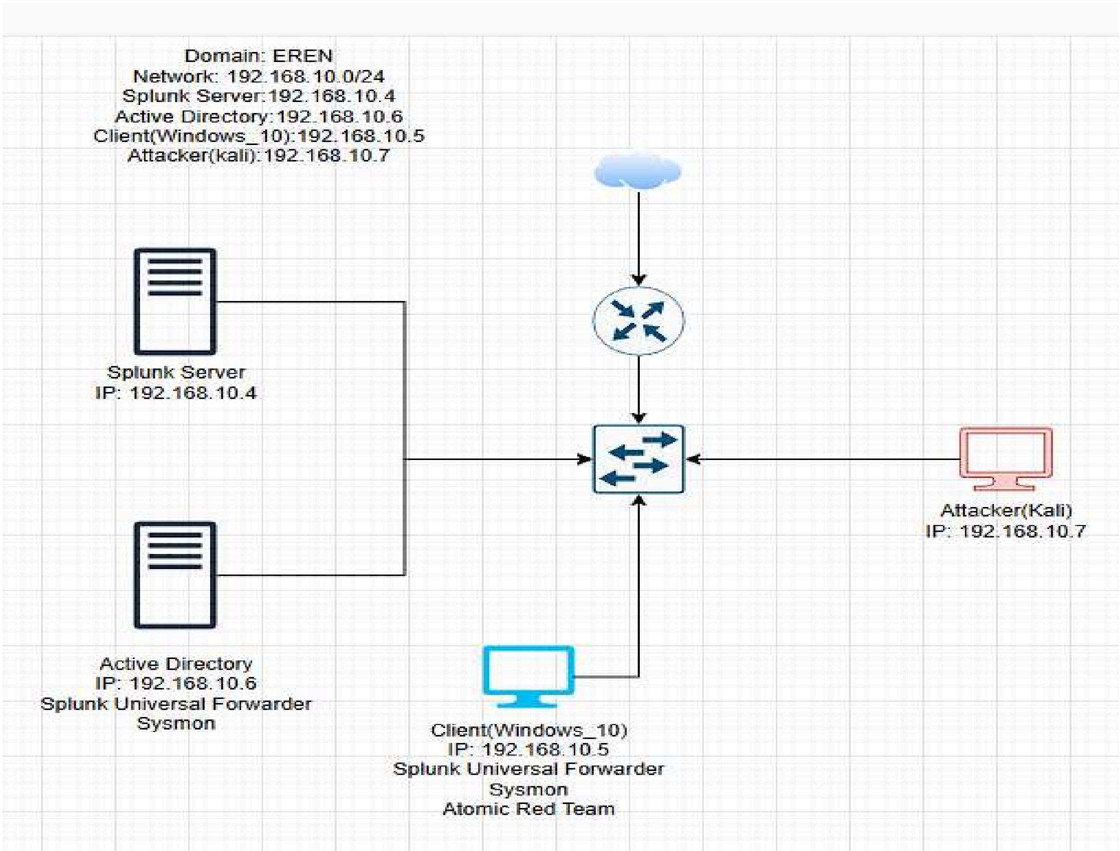
Project:

This lab is dedicated to maintain Active Directory, simulating cyber attacks and monitor them in a SIEM. I'll be using virtual machines for this lab and I'll be using splunk as the SIEM. I'll use sysmon and atomic red team as well. Below is diagram:



VM Installation:

The first step is to install total of four VM.

1. Installing a Windows 10 as Client
2. Installing a Windows server as Active directory domain controller
3. Installing a ubuntu live server(22.04.x version is preferred) as Splunk server
4. Installing a Kali linux as Attacker

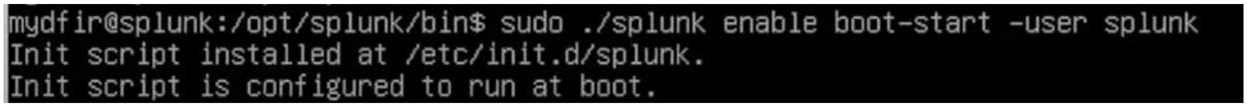
After installing all the machines need to update and upgrade the ubuntu and kali machines:
Command : sudo apt-get update && sudo apt-get upgrade.

Now I'm creating a Nat Network profile for this lab and making sure all the machines are using this network.

Setup:

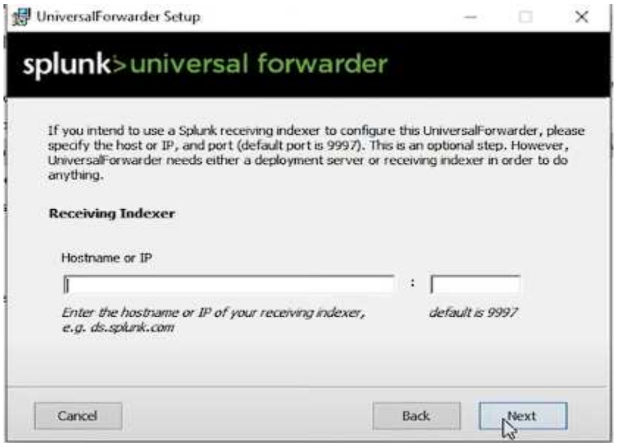
Now lets setup splunk on the ubuntu server. Download the splunk enterprise free from their website for ubuntu (.deb) . Then install splunk using dpkg.

Now change the user to splunk and go to “/opt/splunk/bin” directory and start splunk. Set username and password for login. Then add splunk in boot-start.



```
mydfir@splunk:/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.
```

Now downloaded Universal splunk forwarder and sysmon on both client and active directory machine.



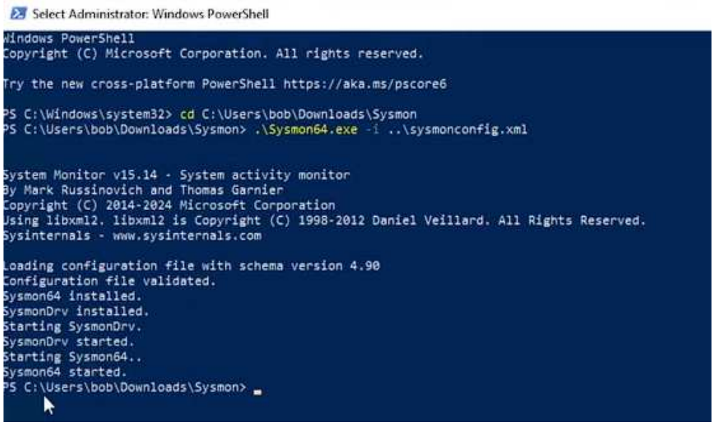
If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

default is 9997



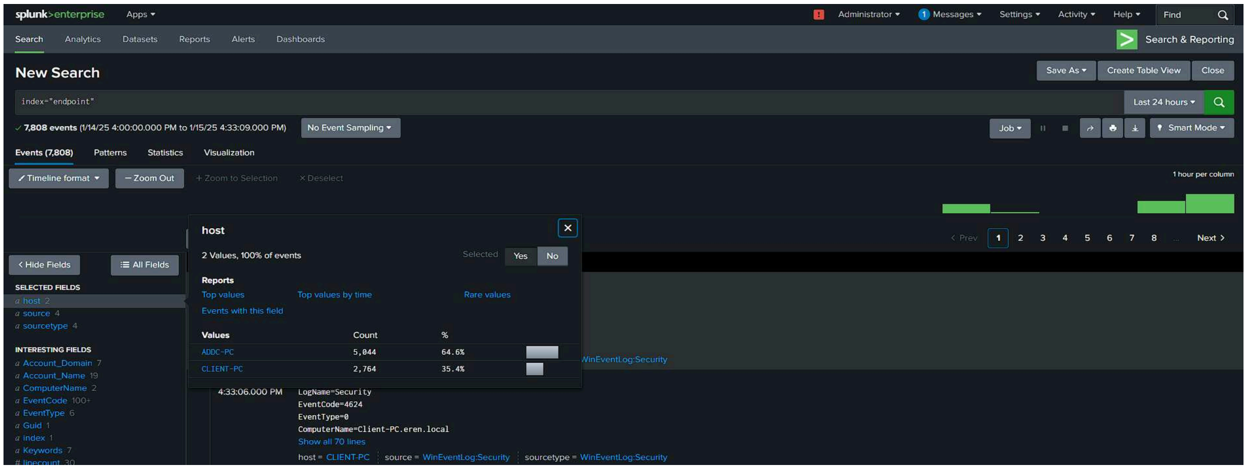
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Windows\system32> cd C:\Users\bob\Downloads\Sysmon
PS C:\Users\bob\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml


System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\bob\Downloads\Sysmon>
```

Now create a file named ‘inputs.conf’ in “C:\Program Files\SplunkUniversalForwarder\etc\system\local\”. Now edit that file:

```
[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
```

Splunk will collect log from these sources only. Now from services restart the SplunkForwarder service to apply this settings. Did this for both client and active directory machines. Now create a index named “endpoint” on the splunk server as I have defined this index in the config file. Lets check on the splunk that the logs are being generated from this two machines.



New Search

```
index="endpoint"
```

✓ 7,808 events (1/14/25 4:00:00.000 PM to 1/15/25 4:33:09.000 PM) No Event Sampling

Events (7,808) Patterns Statistics Visualization

SELECTED FIELDS
a host 2
a source 4
a sourcetype 4

INTERESTING FIELDS
a Account_Domain 7
a Account_Name 19
a ComputerName 2
a EventCode 100+
a EventType 6
a Guid 1
a index 1
a Keywords 7
# linecount 30

host

2 Values, 100% of events

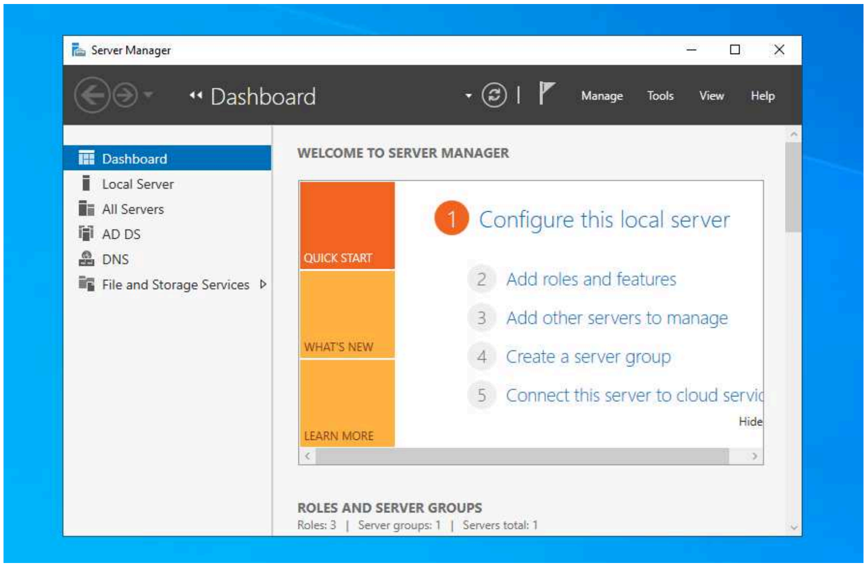
Selected Yes [✓ No]

Reports
Top values Top values by time Rare values
Events with this field

Values	Count	%
ADDC-PC	5,044	64.6%
CLIENT-PC	2,764	35.4%

```
4:33:06.000 PM   LogName=Security
                 EventCode=4624
                 EventType=0
                 ComputerName=Client-PC.eren.local
                 Show all 70 lines
                 host = CLIENT-PC   source = WinEventLog:Security   sourcetype = WinEventLog:Security
```

Lets configure the Active Directory machine now. Firstly open the server manager.

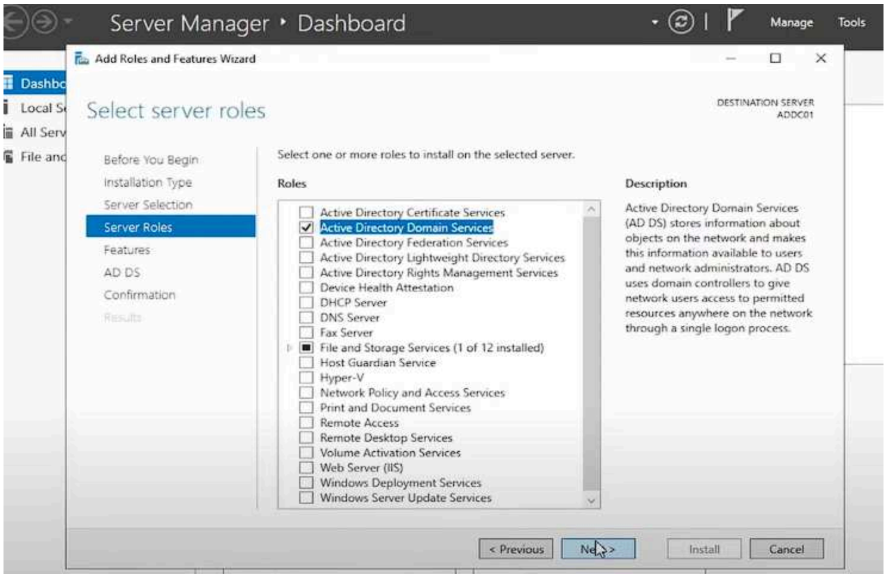


WELCOME TO SERVER MANAGER

1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud servic

ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1

Then from the manage option selecting “Add roles and Features” and start setting up.



Select server roles

DESTINATION SERVER
ADDC01

Select one or more roles to install on the selected server.

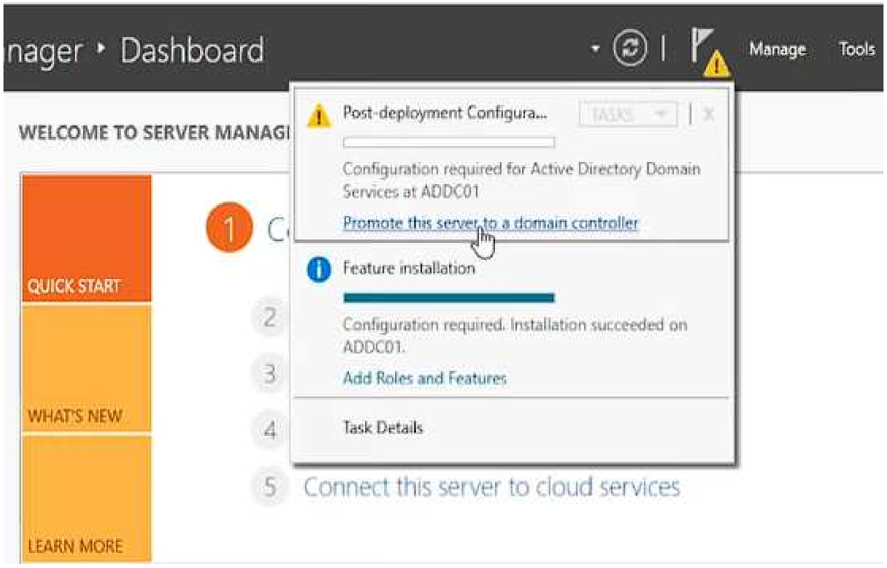
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Then from the flag option promote this server to domain controller



Post-deployment Configura...

Configuration required for Active Directory Domain Services at ADDC01

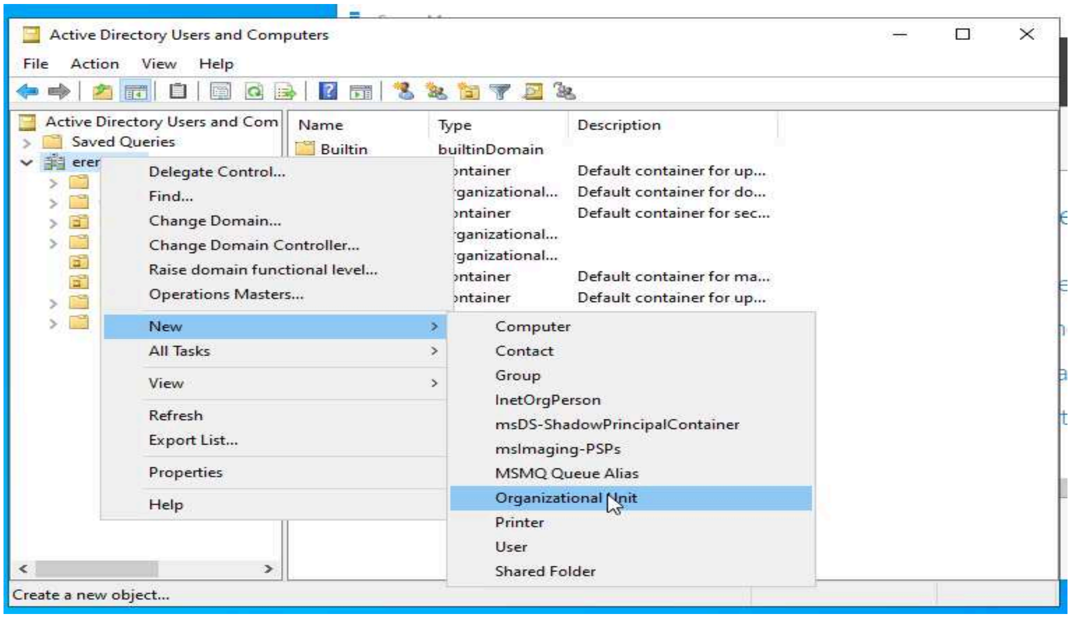
Promote this server to a domain controller

Feature installation

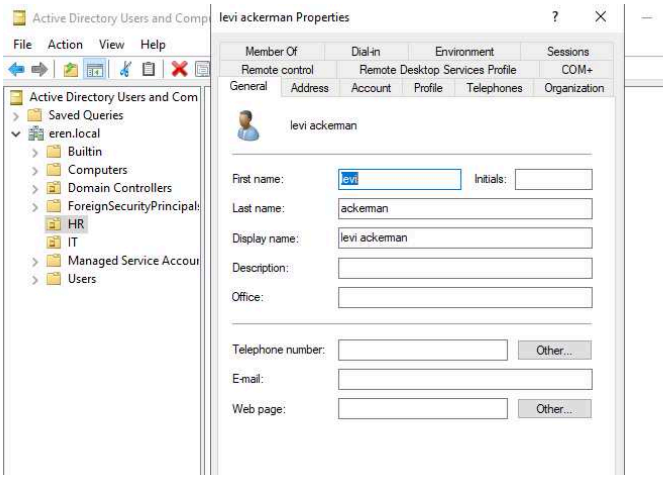
Configuration required. Installation succeeded on ADDC01.

Add Roles and Features

Select “add a new forest” from the next window and complete the setup. The machine will restart and active directory domain controller installation is done. Now let's add some users. Open the tools section, then open active directory users and computers. I have created two Organizational Units named HR and IT . Then added one user in each Unit.



Name	Type	Description
Builtin	builtinDomain	
	ontainer	Default container for up...
	ganizational...	Default container for do...
	ontainer	Default container for sec...
	ganizational...	
	ganizational...	
	ontainer	Default container for ma...
	ontainer	Default container for up...



First name: levi Initials:

Last name: ackerman

Display name: levi ackerman

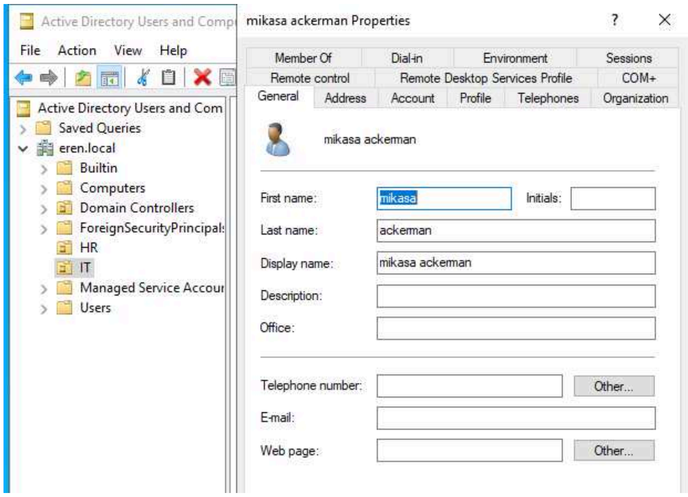
Description:

Office:

Telephone number:

E-mail:

Web page:



First name: mikasa Initials:

Last name: ackerman

Display name: mikasa ackerman

Description:

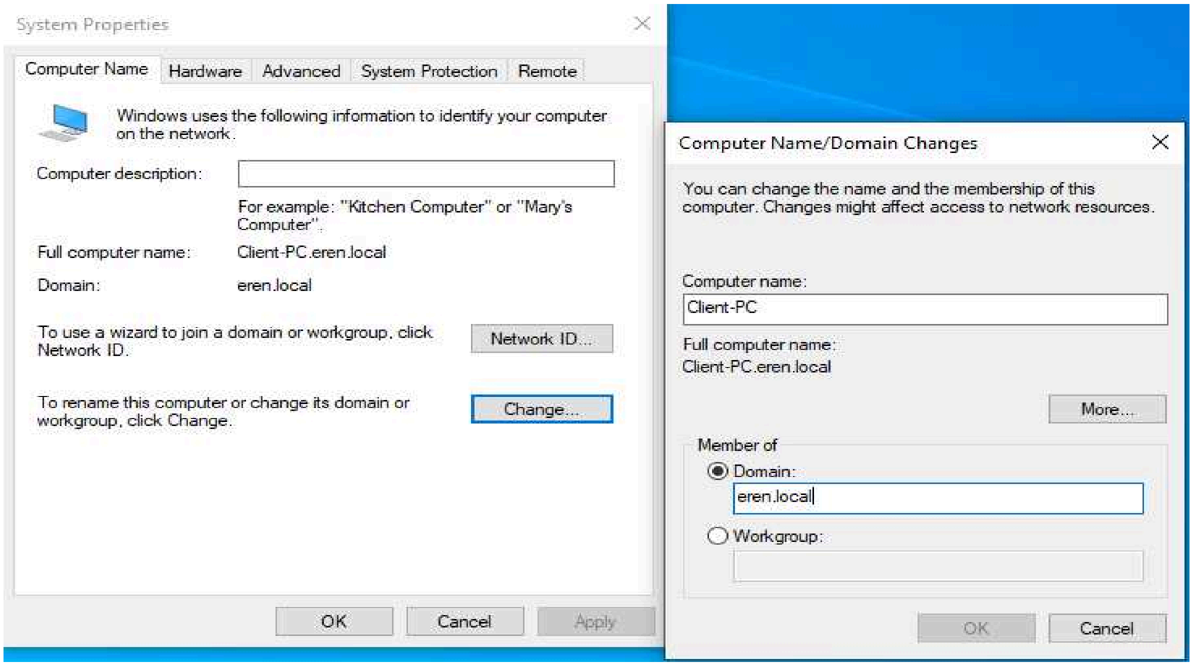
Office:

Telephone number:

E-mail:

Web page:

Now for the client machine changed the dns server IP to the Domain controller machines IP. Added this client machine into the domain from advance system settings.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Client-PC.eren.local

Domain: eren.local

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
Client-PC

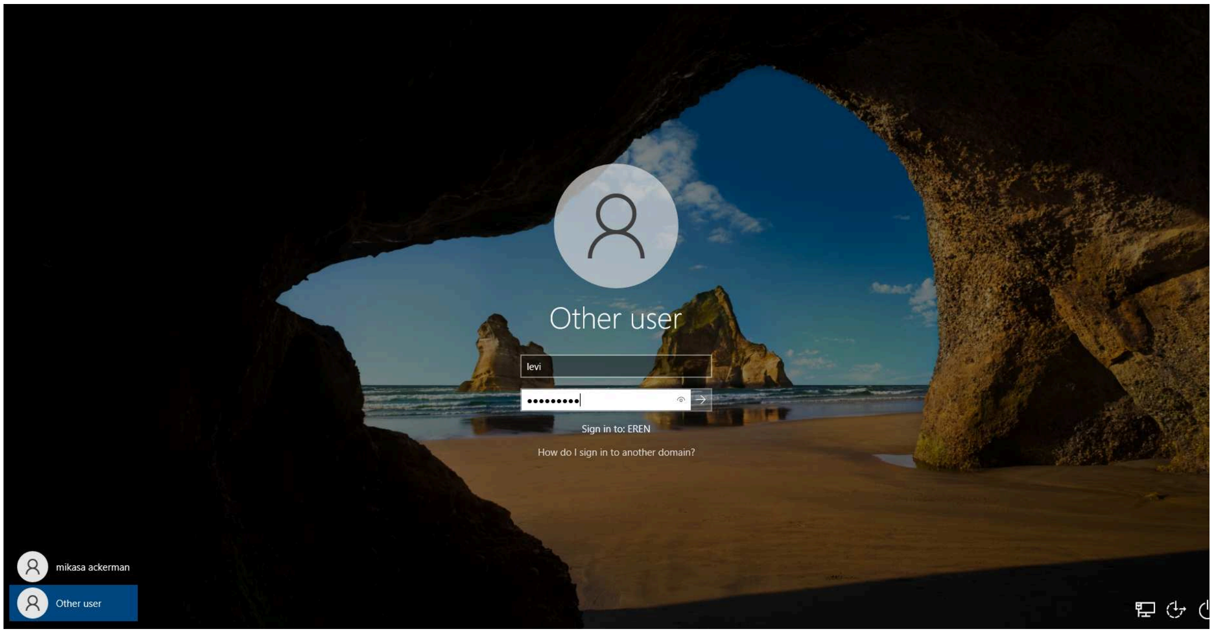
Full computer name:
Client-PC.eren.local

Member of

● Domain:
eren.local

○ Workgroup:

After rebooting I logged in using any user credential from that two I created earlier in Active Directory.



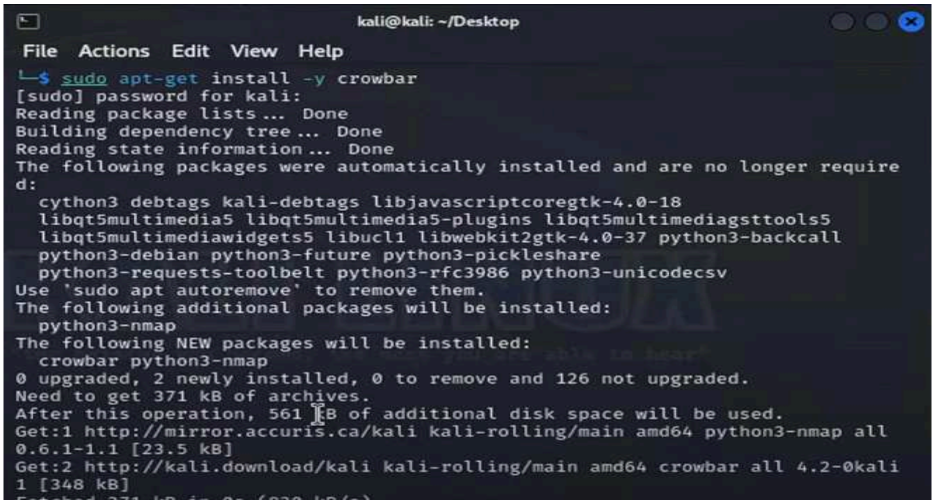
Other user

levi

•••••••••

Sign in to: EREN

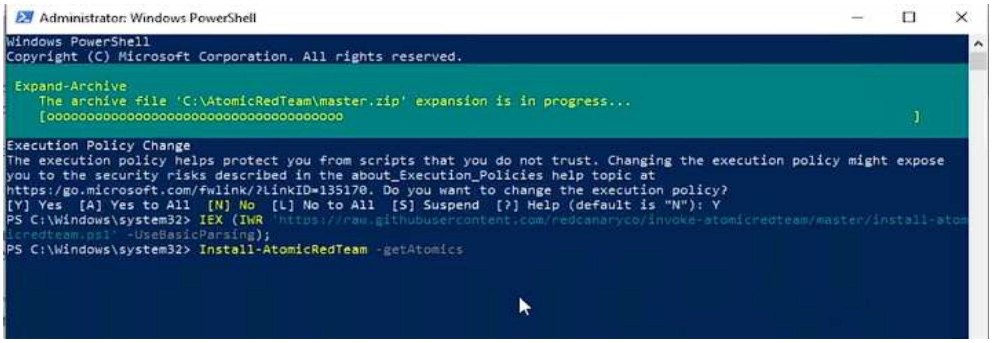
Now for the attacker machine(Kali) logged in using default credential. Lets install crowbar.



```
└─$ sudo apt-get install -y crowbar
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer require
d:
  cython3 debtags kali-debtags libjavascriptcoregtk-4.0-18
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libucl1 libwebkit2gtk-4.0-37 python3-backcall
  python3-debian python3-future python3-pickleshare
  python3-requests-toolbelt python3-rfc3986 python3-unicodecsv
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-nmap
The following NEW packages will be installed:
  crowbar python3-nmap
0 upgraded, 2 newly installed, 0 to remove and 126 not upgraded.
Need to get 371 kB of archives.
After this operation, 561 kB of additional disk space will be used.
Get:1 http://mirror.accuris.ca/kali kali-rolling/main amd64 python3-nmap all
0.6.1-1.1 [23.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 crowbar all 4.2-0kali
1 [348 kB]
```

Then installed Atomic Red Team using the following command:

IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1' -UseBasicParsing);
Install-AtomicRedTeam -getAtomics

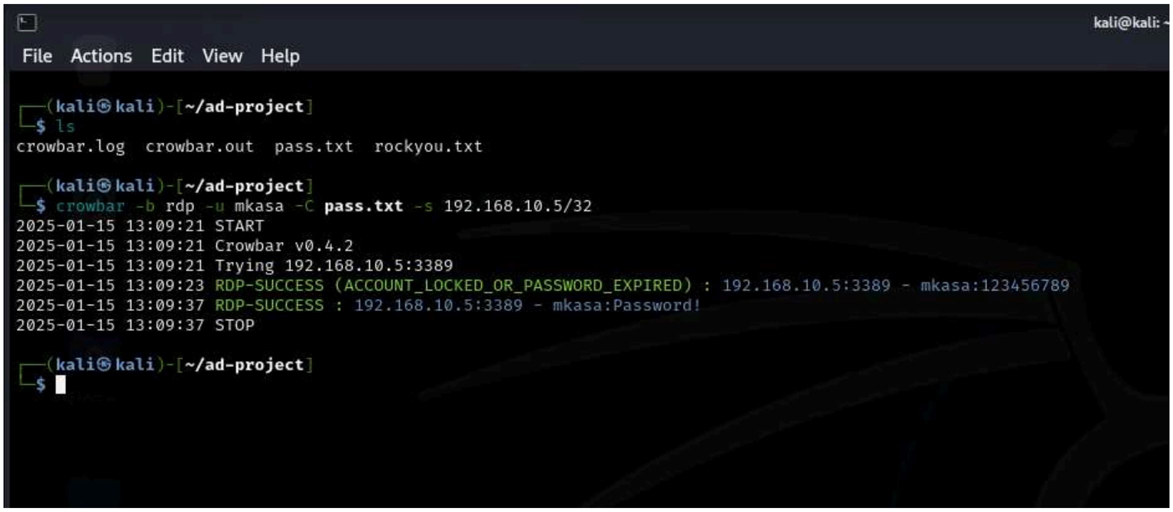


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Expand-Archive
    The archive file 'C:\AtomicRedTeam\master.zip' expansion is in progress...
    [oooooooooooooooooooooooooooooooooooo                                          ]

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> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atom
icredteam.ps1' -UseBasicParsing);
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomics
```

Attack and Log Investigation:

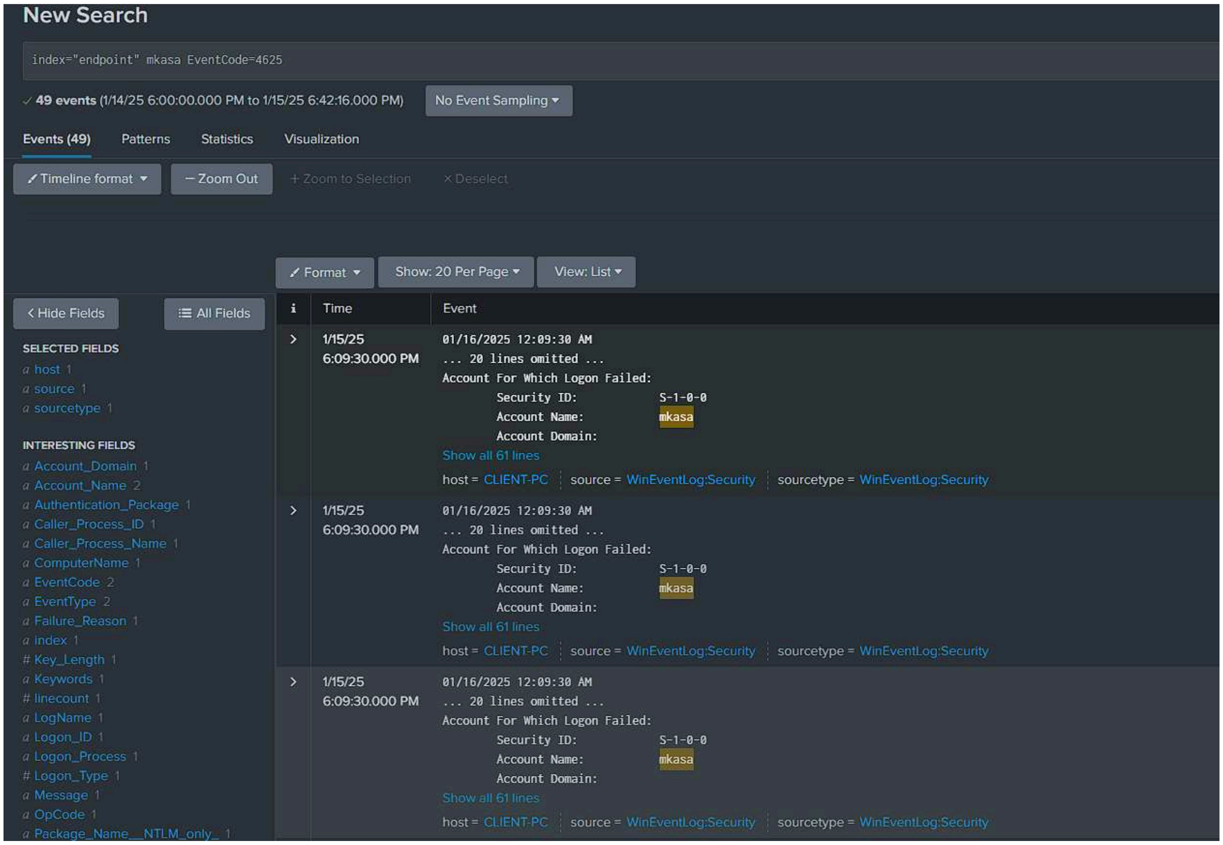
On the kali machine edited the rockyou.txt file and added my two users password that I created earlier.

On the client machine enabled the RDP and added the two users there. Its time to generate the brute force attack on the client pc using crowbar.



```
┌──(kali㉿kali)-[~/ad-project]
└─$ ls
crowbar.log  crowbar.out  pass.txt  rockyou.txt

┌──(kali㉿kali)-[~/ad-project]
└─$ crowbar -b rdp -u mkasa -C pass.txt -s 192.168.10.5/32
2025-01-15 13:09:21 START
2025-01-15 13:09:21 Crowbar v0.4.2
2025-01-15 13:09:21 Trying 192.168.10.5:3389
2025-01-15 13:09:23 RDP-SUCCESS (ACCOUNT_LOCKED_OR_PASSWORD_EXPIRED) : 192.168.10.5:3389 - mkasa:123456789
2025-01-15 13:09:37 RDP-SUCCESS : 192.168.10.5:3389 - mkasa:Password!
2025-01-15 13:09:37 STOP

┌──(kali㉿kali)-[~/ad-project]
└─$ 
```

Found the brute force attack. Here I had total 50 password in my rockyou.txt including one correct password on the last line. So 49 failed login attempt happened.



```
index="endpoint" mkasa EventCode=4625
```

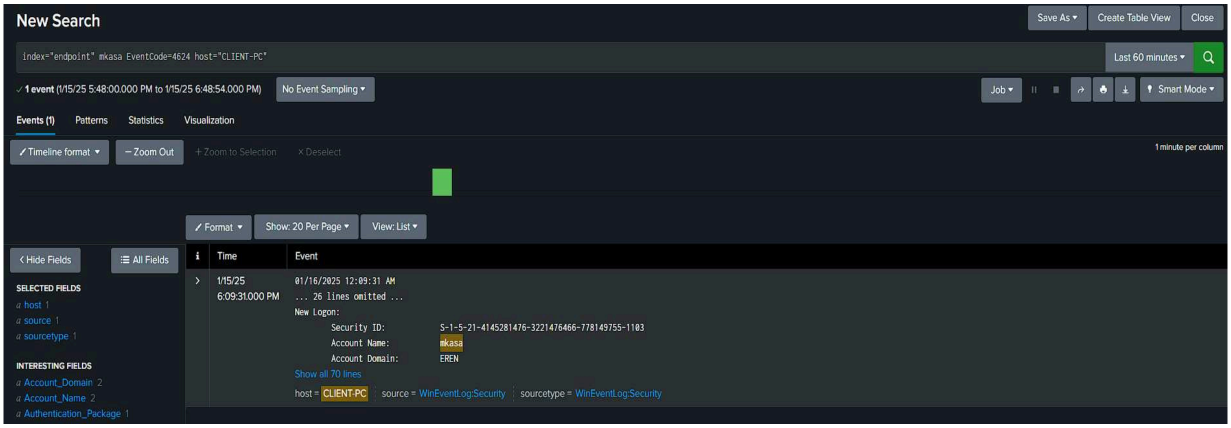
✓ 49 events (1/14/25 6:00:00.000 PM to 1/15/25 6:42:16.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
a EventCode 2
a EventType 2
a Failure_Reason 1
a index 1
Key_Length 1
a Keywords 1
# linecount 1
a LogName 1
a Logon_ID 1
a Logon_Process 1
Logon_Type 1
a Message 1
a OpCode 1
a Package_Name__NTLM_only_ 1

```
1/15/25 6:09:30.000 PM
01/16/2025 12:09:30 AM
... 20 lines omitted ...
Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           mkasa
        Account Domain:
Show all 61 lines
host = CLIENT-PC   source = WinEventLog:Security   sourcetype = WinEventLog:Security

1/15/25 6:09:30.000 PM
01/16/2025 12:09:30 AM
... 20 lines omitted ...
Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           mkasa
        Account Domain:
Show all 61 lines
host = CLIENT-PC   source = WinEventLog:Security   sourcetype = WinEventLog:Security

1/15/25 6:09:30.000 PM
01/16/2025 12:09:30 AM
... 20 lines omitted ...
Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           mkasa
        Account Domain:
Show all 61 lines
host = CLIENT-PC   source = WinEventLog:Security   sourcetype = WinEventLog:Security
```

Found the successful logged one.



```
index="endpoint" mkasa EventCode=4624 host="CLIENT-PC"
```

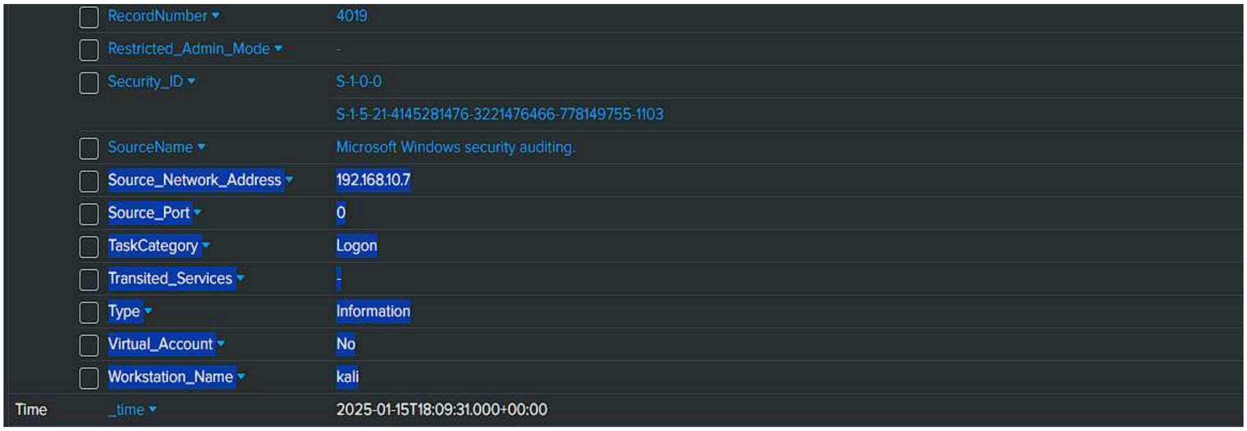
✓ 1 event (1/15/25 5:48:00.000 PM to 1/15/25 6:48:54.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 2
- a Account_Name 2
- a Authentication_Package 1

i	Time	Event
›	1/15/25 6:09:31.000 PM	01/16/2025 12:09:31 AM ... 26 lines omitted ... New Logon: Security ID: S-1-5-21-4145281476-3221476466-778149755-1103 Account Name: mkasa Account Domain: EREN Show all 70 lines host = CLIENT-PC source = WinEventLog:Security sourcetype = WinEventLog:Security

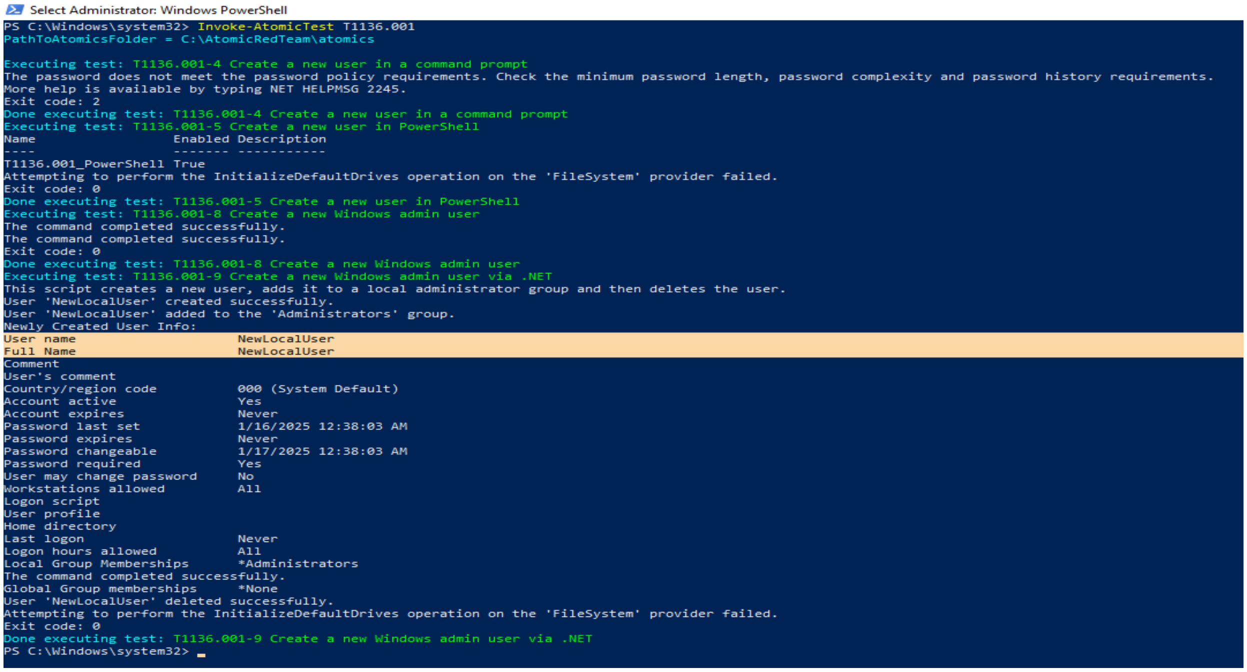
Here the Source Address and the Workstation Name shows the attacker machine IP address and name.



	□ RecordNumber ▾	4019
	□ Restricted_Admin_Mode ▾	-
	□ Security_ID ▾	S-1-0-0 S-1-5-21-4145281476-3221476466-778149755-1103
	□ SourceName ▾	Microsoft Windows security auditing.
	□ Source_Network_Address ▾	192.168.10.7
	□ Source_Port ▾	0
	□ TaskCategory ▾	Logon
	□ Transited_Services ▾	-
	□ Type ▾	Information
	□ Virtual_Account ▾	No
	□ Workstation_Name ▾	kali
Time	_time ▾	2025-01-15T18:09:31.000+00:00

Telemetry Generation and Log Investigation:

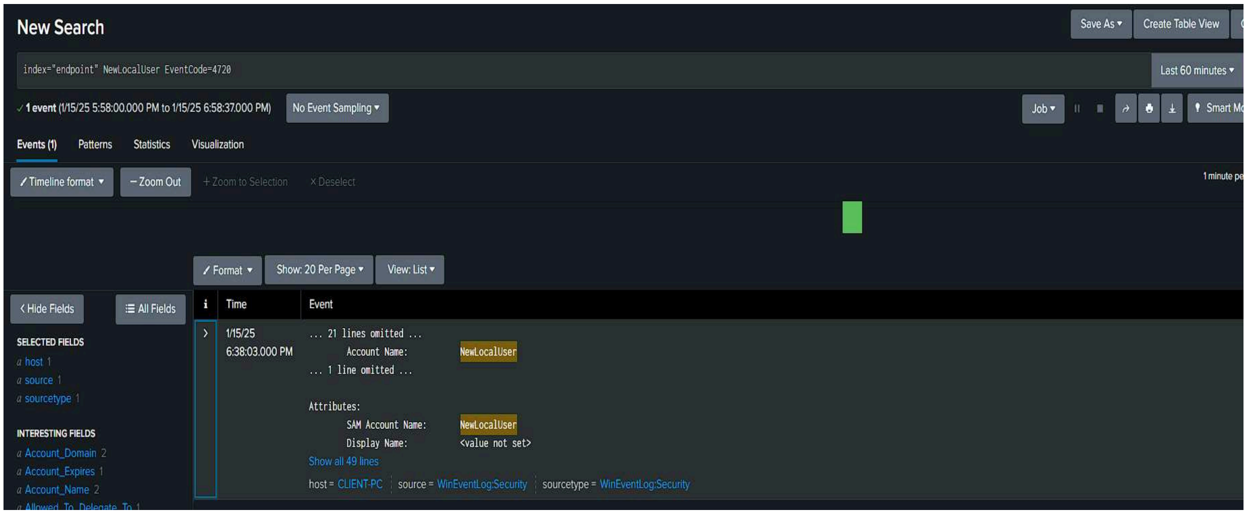
Now generating some telemetry using Atomic Red Team,



Select Administrator: Windows PowerShell

```
PS C:\Windows\system32> Invoke-AtomicTest T1136.001
PathToAtomicsFolder = 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
Attempting to perform the InitializeDefaultDrives operation on the 'FileSystem' provider failed.
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
Full Name                    NewLocalUser
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never
Password last set            1/16/2025 12:38:03 AM
Password expires             Never
Password changeable          1/17/2025 12:38:03 AM
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
The command completed successfully.
Global Group memberships     *None
User 'NewLocalUser' deleted successfully.
Attempting to perform the InitializeDefaultDrives operation on the 'FileSystem' provider failed.
Exit code: 0
Done executing test: T1136.001-9 Create a new Windows admin user via .NET
PS C:\Windows\system32> _
```

I have generated telemetry using atomic red team that creates a user. The username is NewLocalUser. Below is the log that was generated.

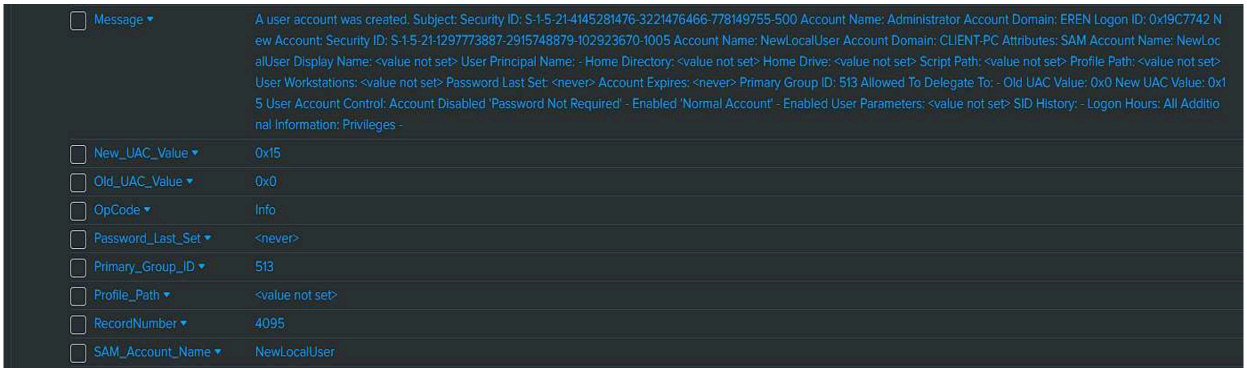


New Search

```
index="endpoint" NewLocalUser EventCode=4720
```

✓ 1 event (1/15/25 5:58:00.000 PM to 1/15/25 6:58:37.000 PM)

i	Time	Event
>	1/15/25 6:38:03.000 PM	... 21 lines omitted ... Account Name: NewLocalUser ... 1 line omitted ... Attributes: SAM Account Name: NewLocalUser Display Name: <value not set> Show all 49 lines host = CLIENT-PC source = WinEventLog:Security sourcetype = WinEventLog:Security



□ Message ▾	A user account was created. Subject: Security ID: S-1-5-21-4145281476-3221476466-778149755-500 Account Name: Administrator Account Domain: EREN Logon ID: 0x19C7742 New Account: Security ID: S-1-5-21-1297773887-2915748879-102923670-1005 Account Name: NewLocalUser Account Domain: CLIENT-PC Attributes: SAM Account Name: NewLocalUser Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value not set> SID History: - Logon Hours: All Additional Information: Privileges -
□ New_UAC_Value ▾	0x15
□ Old_UAC_Value ▾	0x0
□ OpCode ▾	Info
□ Password_Last_Set ▾	<never>
□ Primary_Group_ID ▾	513
□ Profile_Path ▾	<value not set>
□ RecordNumber ▾	4095
□ SAM_Account_Name ▾	NewLocalUser