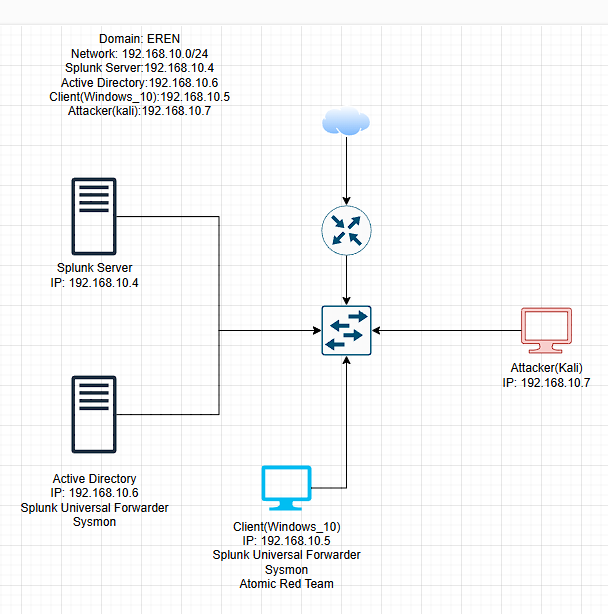
**Project:**

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

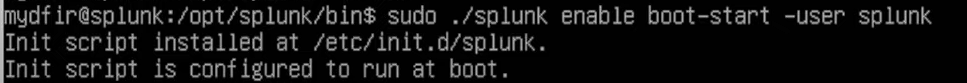
After installing all the machines need to update and upgrade the ubuntu and kali machines:

Command : sudo apt-get update && sudo apt-get upgrade.

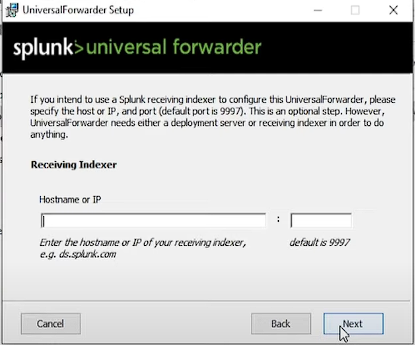
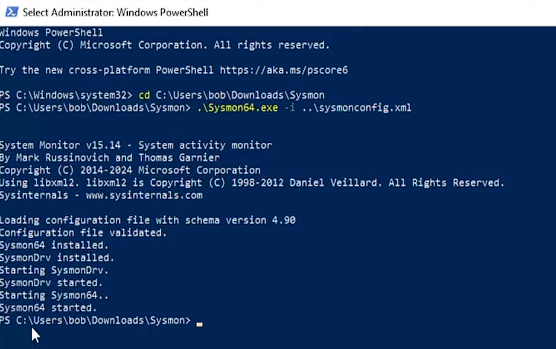
Now I’m creating a Nat Network profile for this lab and making sure all the machines are using this network.

**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.



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

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

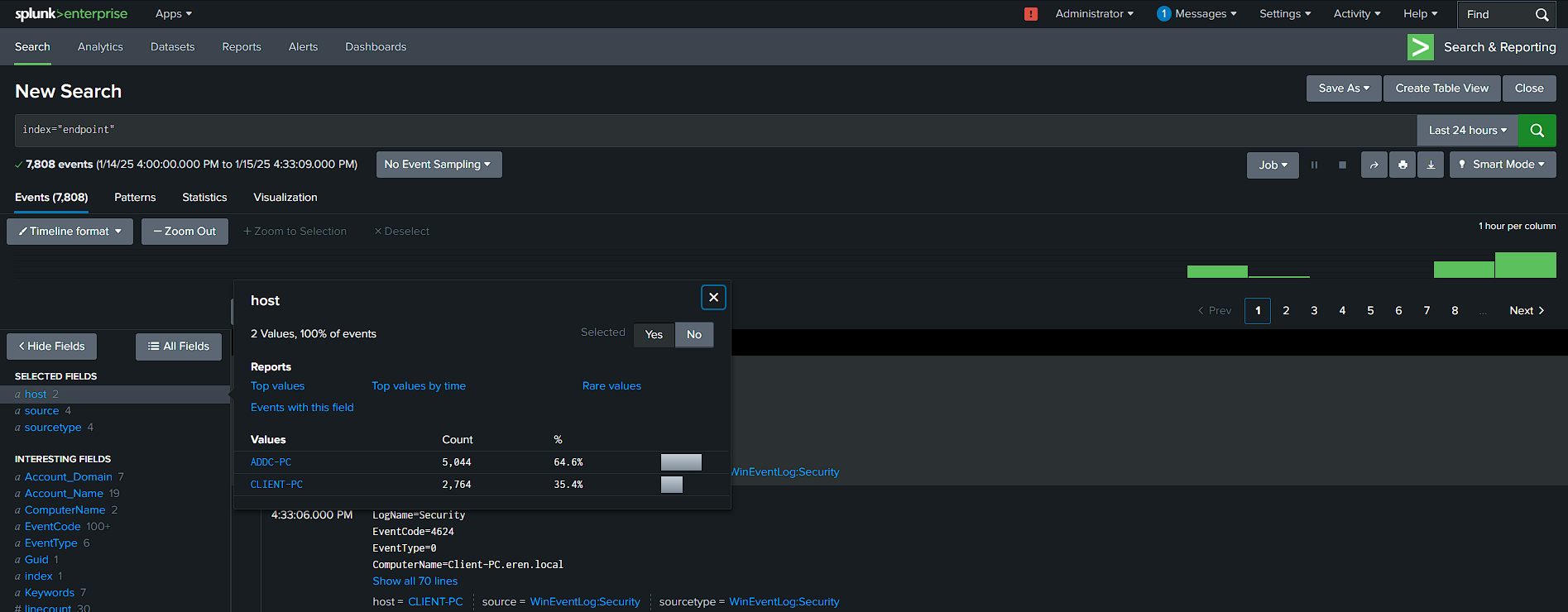
disabled = false

renderXml = true

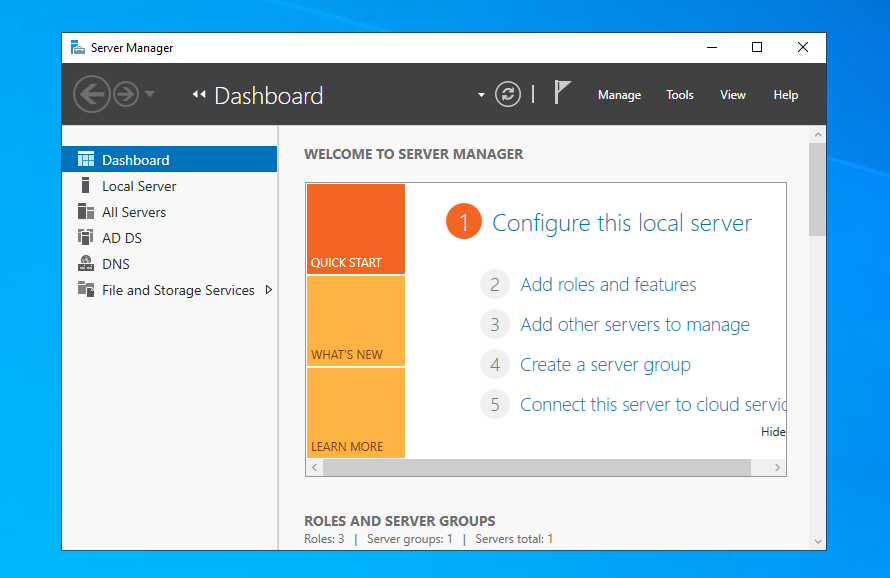
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

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.

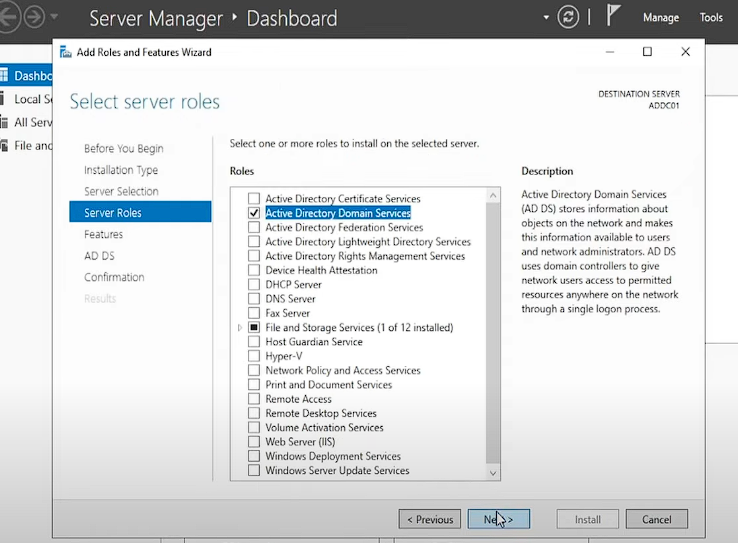
Lets check on the splunk that the logs are being generated from this two machines.



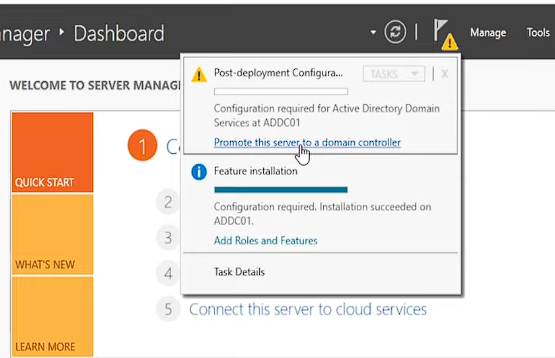
Lets configure the Active Directory machine now. Firstly open the server manager.



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

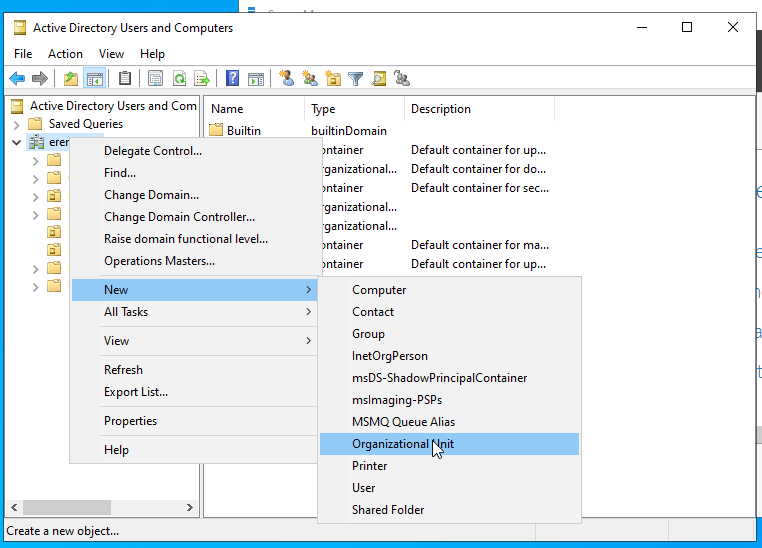


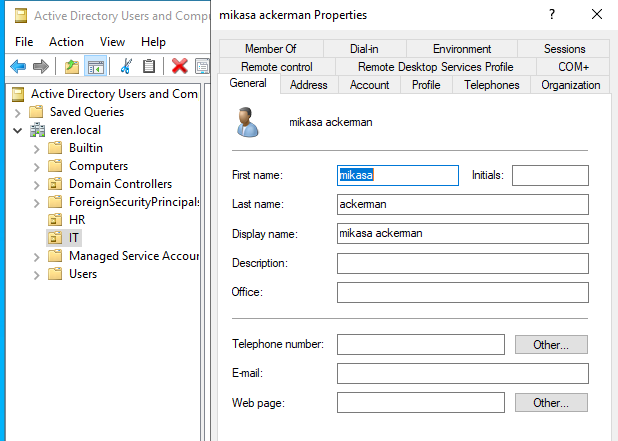
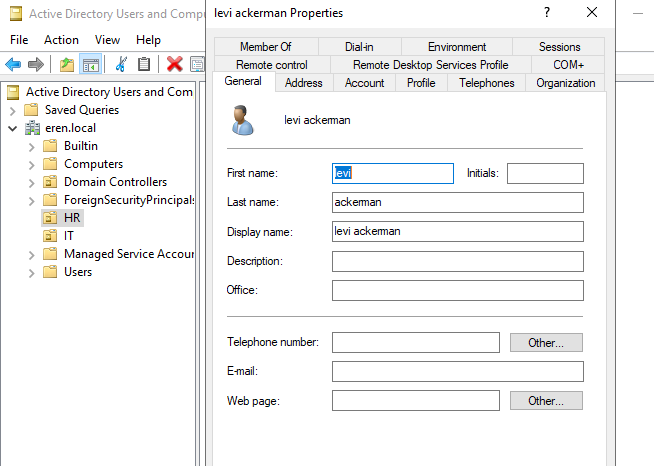
Then from the flag option promote this server to domain controller



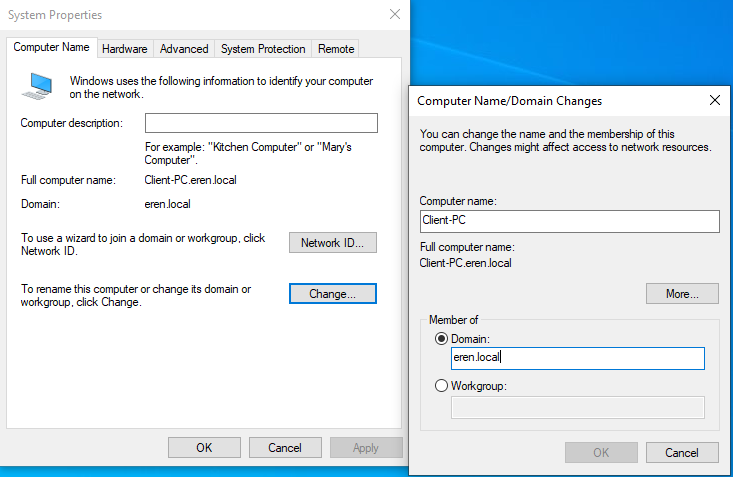
Select “add a new forest” from the next window and complete the setup. The machine will restart and active directory domain controller installation is done. Now let's add some users.

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.

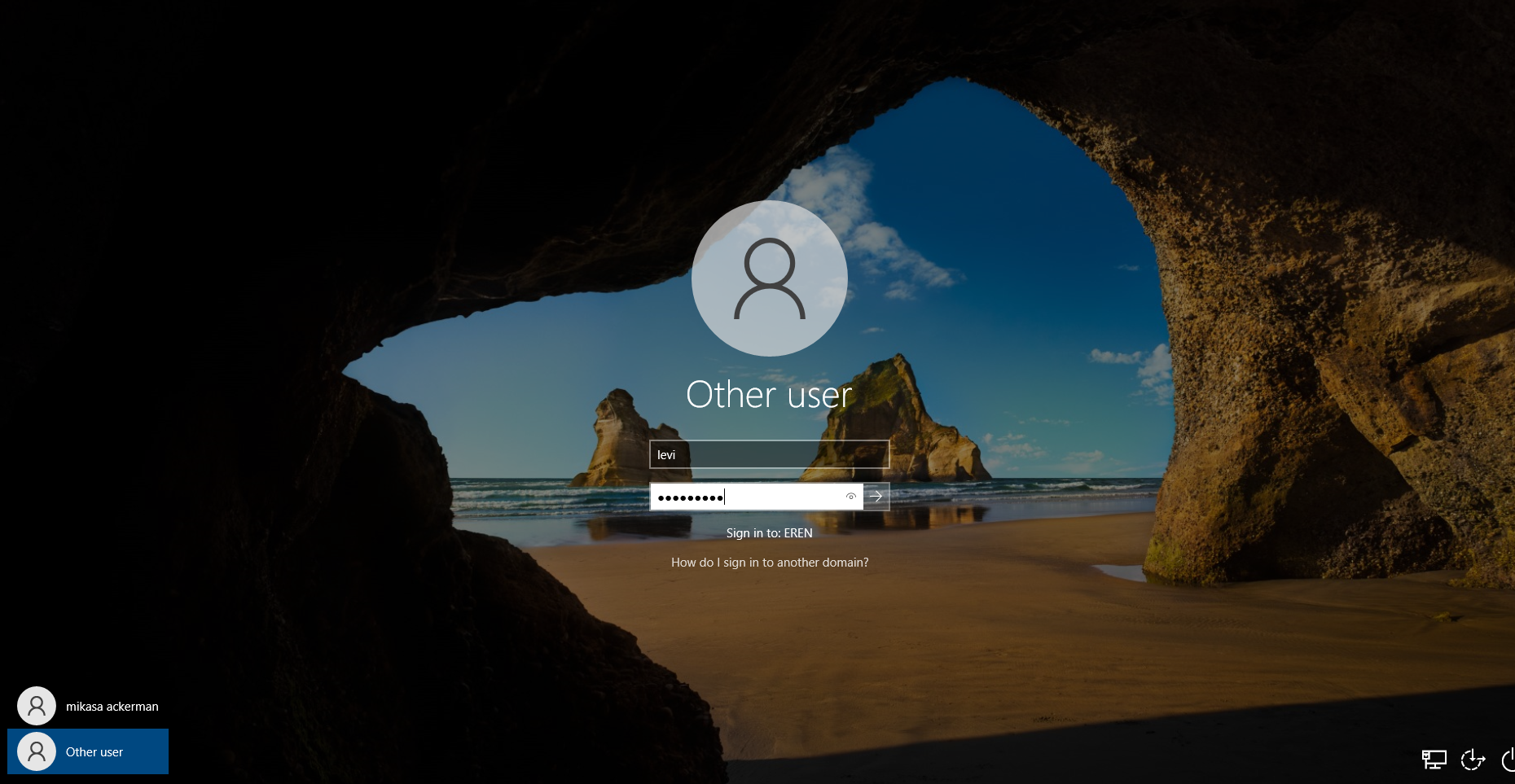




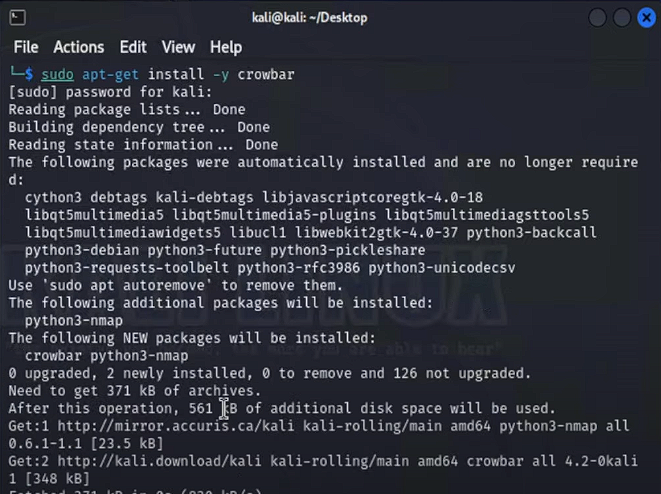
Now for the client machine changed the dns server IP to the Domain controller machines IP. Added this client machine into the domain from advance system settings.



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



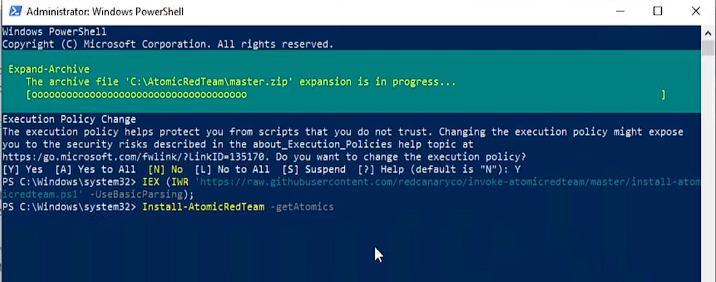
Now for the attacker machine(Kali) logged in using default credential. Lets install crowbar.



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



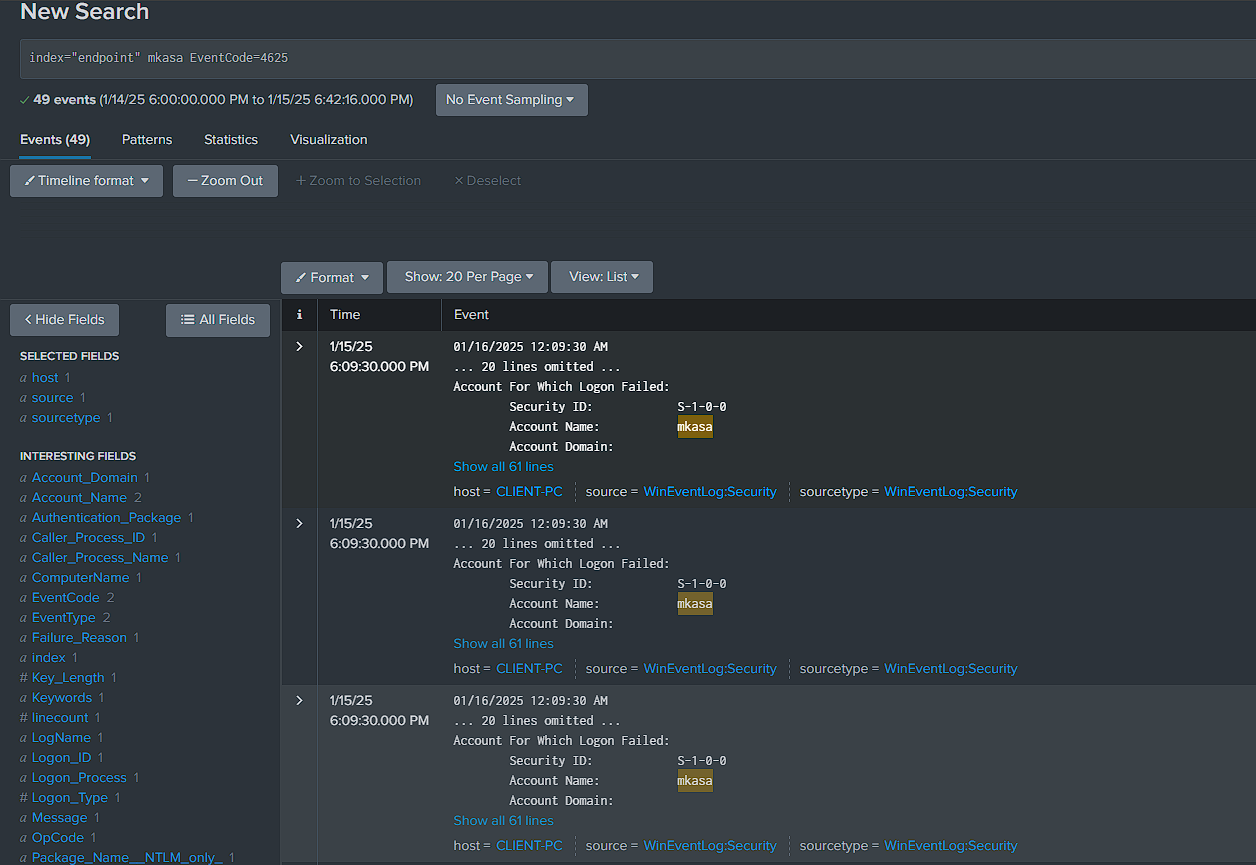
**Attack and Log Investigation:**

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

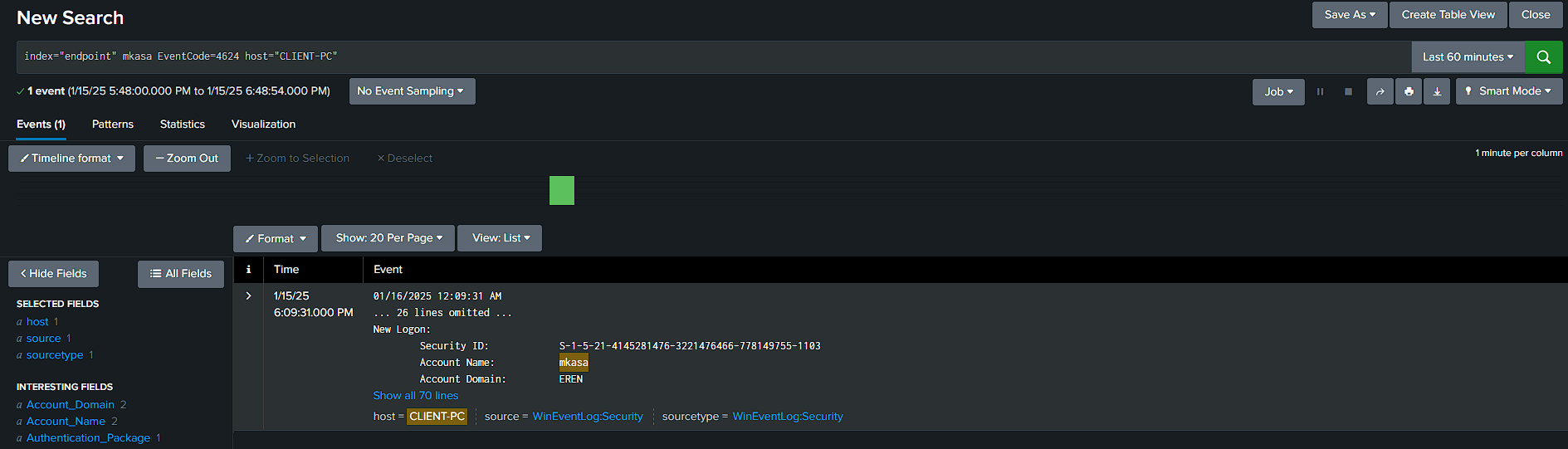
On the client machine enabled the RDP and added the two users there. Its time to generate the brute force attack on the client pc using crowbar.



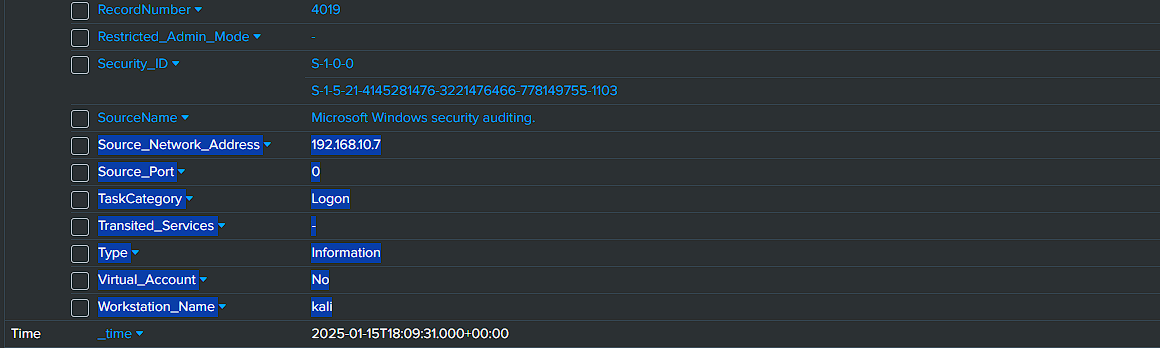
Found the brute force attack. Here I had total 50 password in my rockyou.txt including one correct password on the last line. So 49 failed login attempt happened.



Found the successful logged one.

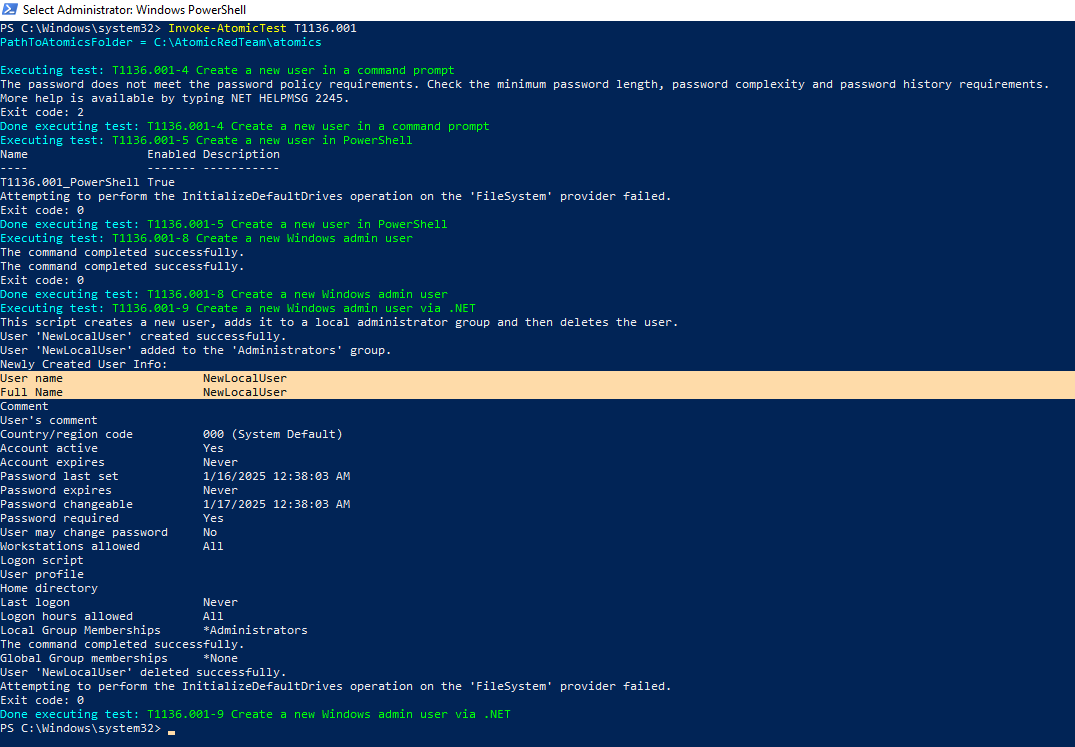


Here the Source Address and the Workstation Name shows the attacker machine IP address and name.



**Telemetry Generation and Log Investigation:**

Now generating some telemetry using Atomic Red Team,



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

