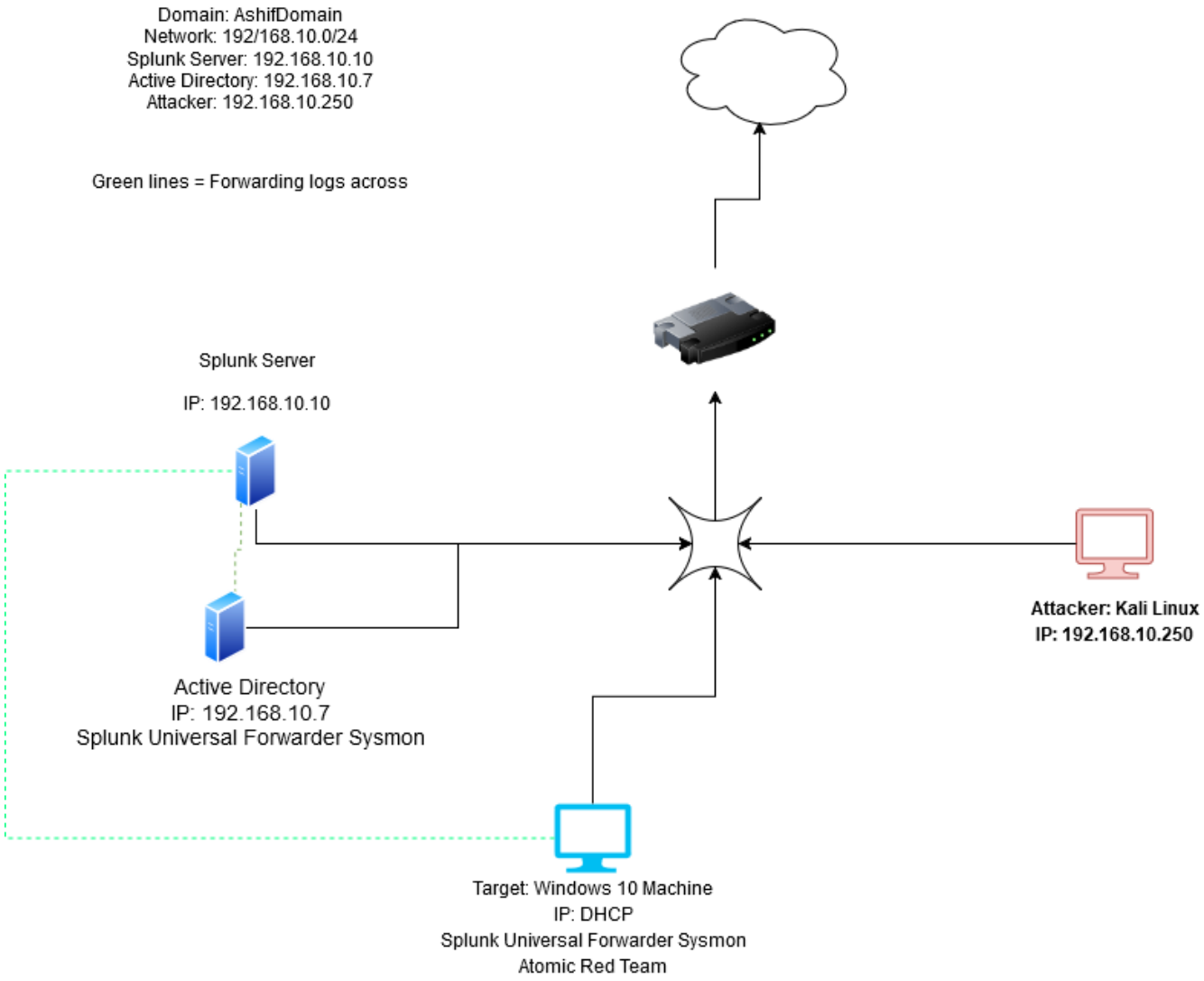
Active Directory Project

Creating a Logical Diagram:



A **switch** connects multiple devices (like computers and printers) in the same network so they can share data.

A **router** connects different networks (like your home Wi-Fi to the internet) and directs data between them.

Target Machine:

- Sysmon is on the target machine to help with telemetry
- Splunk Universal forwarder will be installed to send data back to Splunk
- Atomic Red Team in our target machine just in case we want to generate interesting data
    - **Atomic Red Team** helps test a computer system's security by running small, safe cyberattack simulations. It checks if security tools can detect and stop threats, helping improve protection against real hackers.

Installations:

- **Windows 10** – Target Machine
- **Kali Linux** – Attacker
- **Splunk** – Collects Data
- **Windows Server** – Active Directory Management

Set up static IP addresses for all required virtual machines.

Sysmon and Splunk universal forwarder on both target machine and server.

Whilst setting up the static IP address for Windows Server, I ran into an issue where the server wouldn't connect to the internet. I was stuck on this for a couple of days, and to make matters worse, my computer was incredibly slow and laggy. It took ages to start up and was a struggle to navigate, making troubleshooting even more frustrating!

After constant days trying to troubleshoot the issue, from changing IP addresses to different addresses, and turning on and off the internet, playing with the settings, I finally found the issue, and I hoped I found it earlier, but the server was connected to NAT, not NAT 'Ashif-AD', which I created for this project!

Credentials for Virtual Machines:

Splunk:

a7hxf

A123!

Kali:

Ashif

A123!

Windows Server:

Administrator

A123!

Windows 10:

Ashif

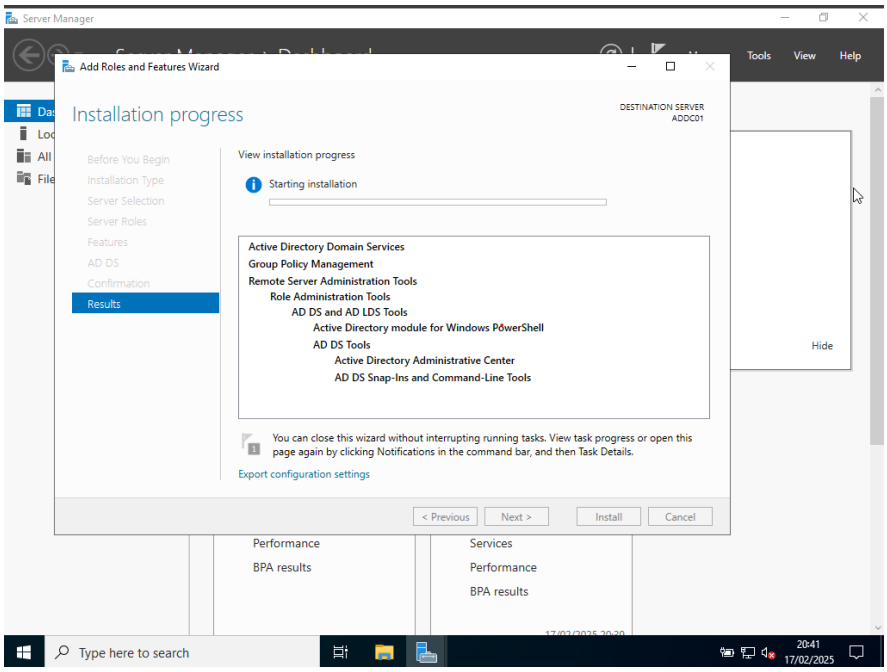
L123!

Johnny Zayed

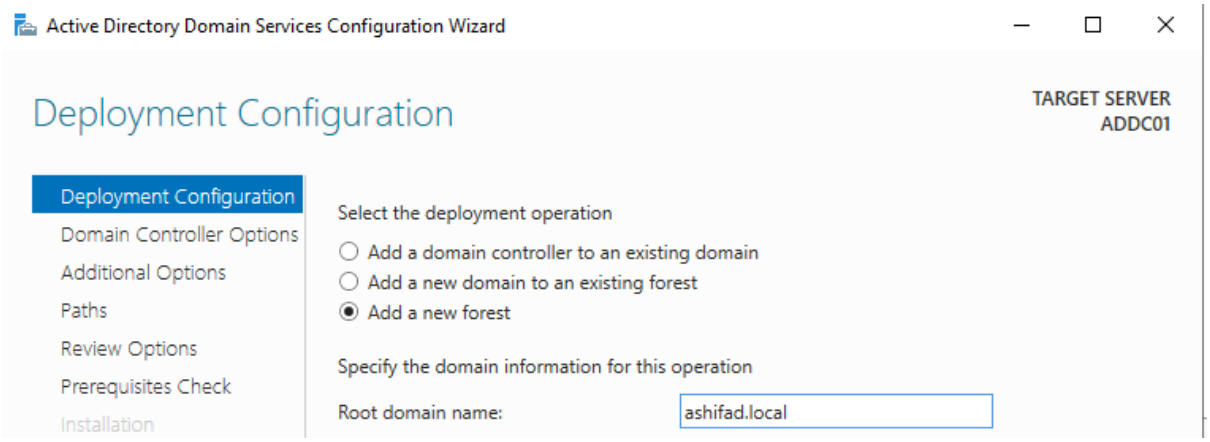
L123!

Install & Configure Active Directory on to our Windows Server, then promote to Domain Controller, and then finally configure Windows PC (Target machine), to join our newly created domain!

We are installing Active Domain Services:



Creating a brand domain:

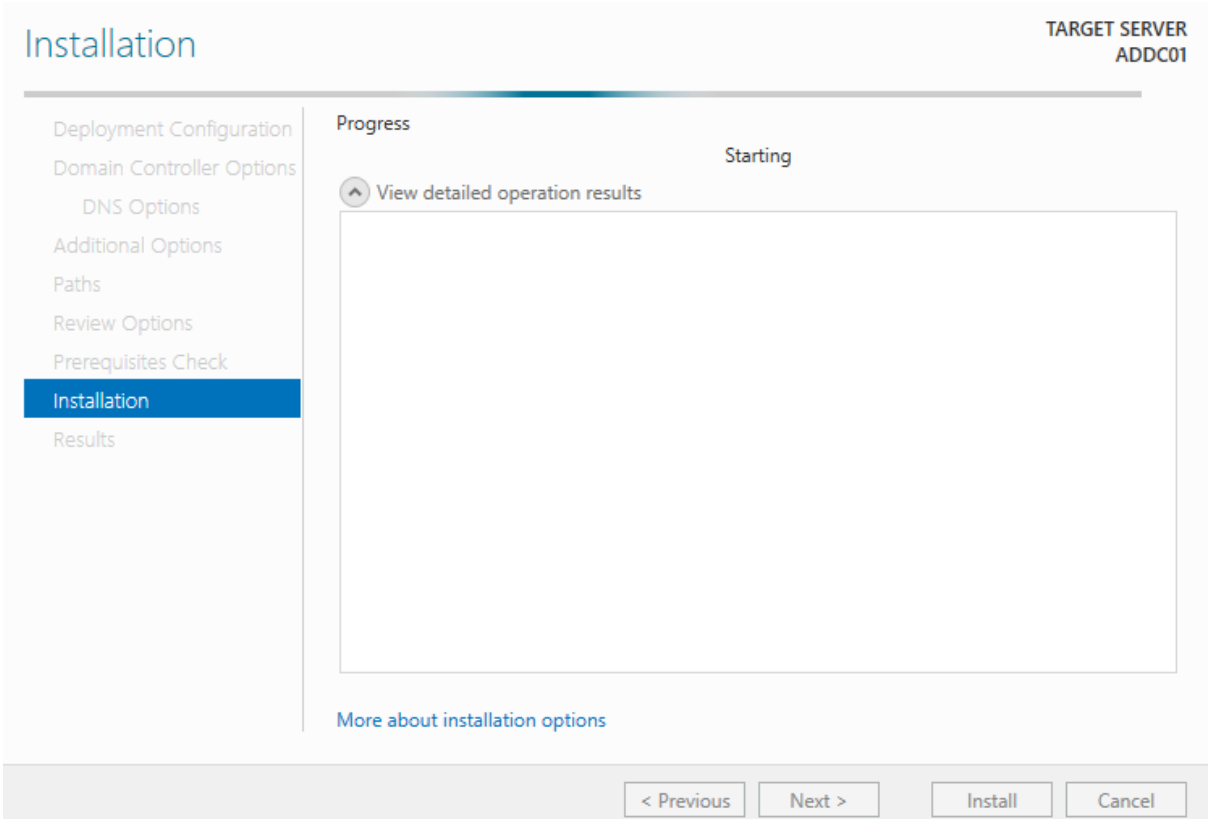


- The domain must have a top-level domain, it must have a dot something.

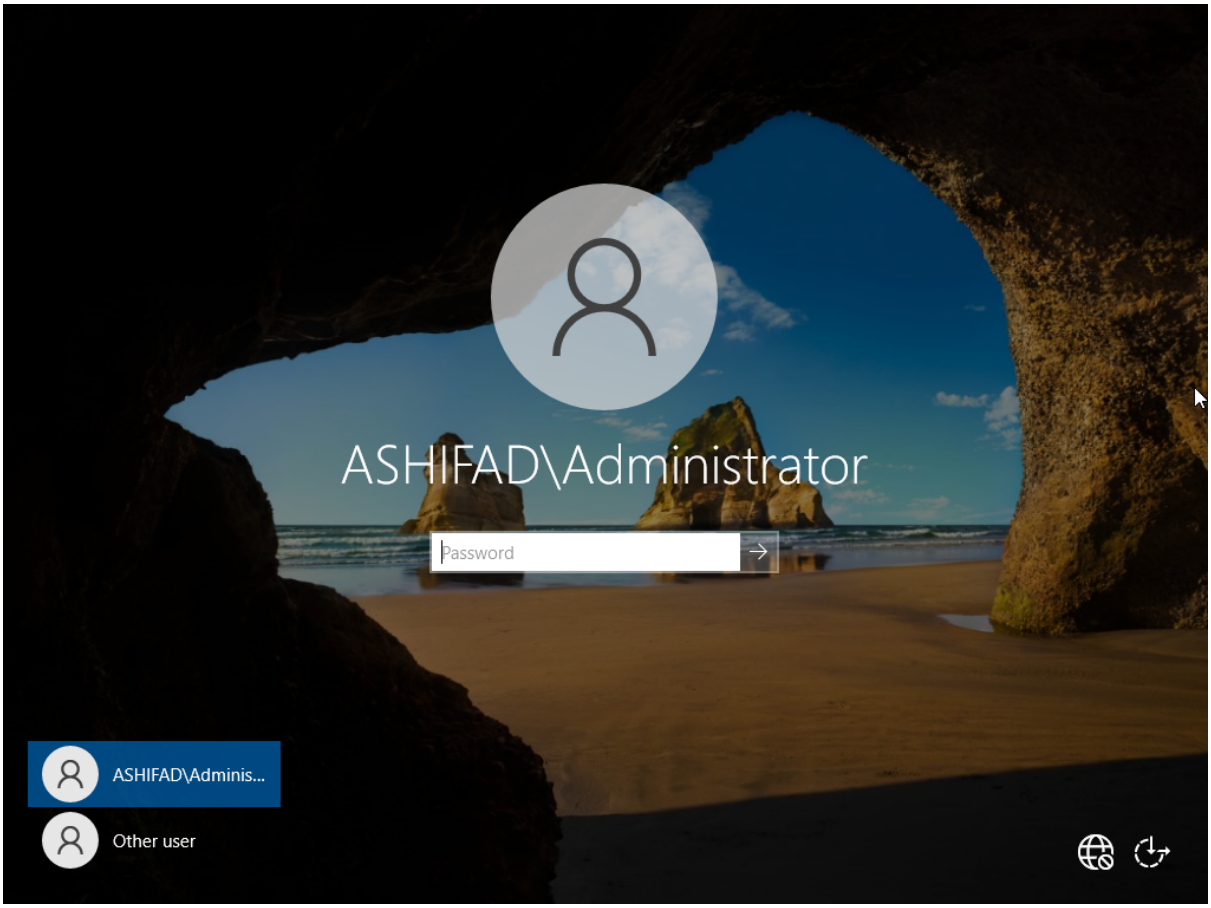
DSRM Password: A123!

Paths are used to store our database file names, ntds.dt. Attackers love to attack domain controllers as they contain files related to the active directory, including password hashes.

- If you suspect any unusual activity, your domain is most likely compromised.

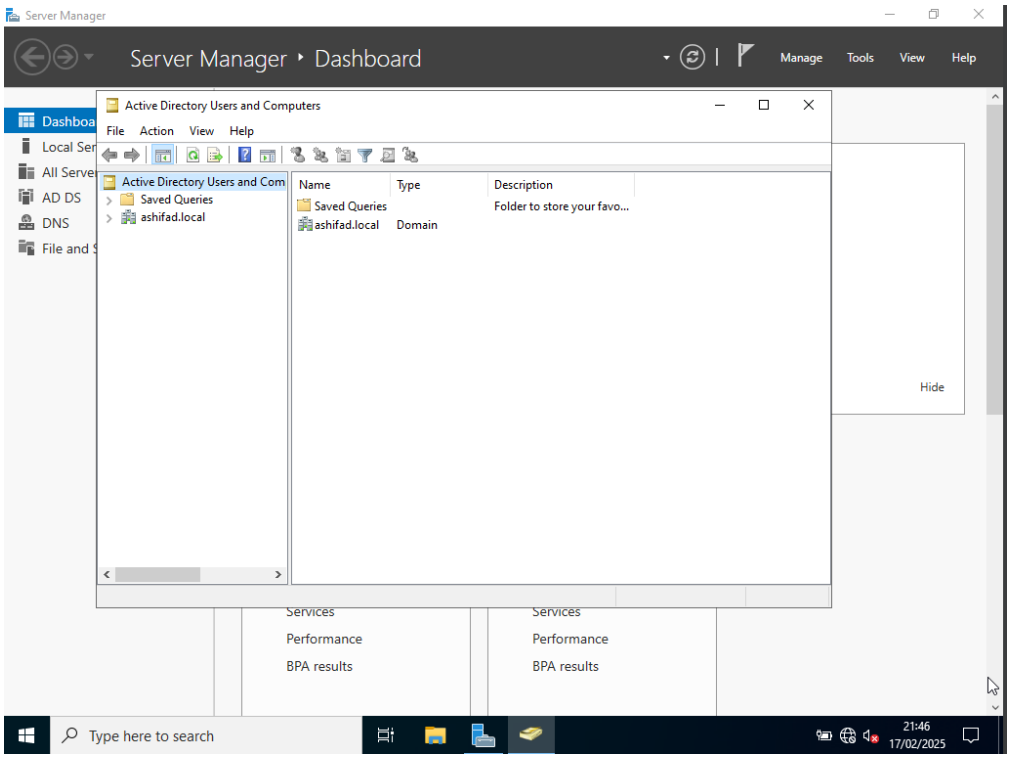


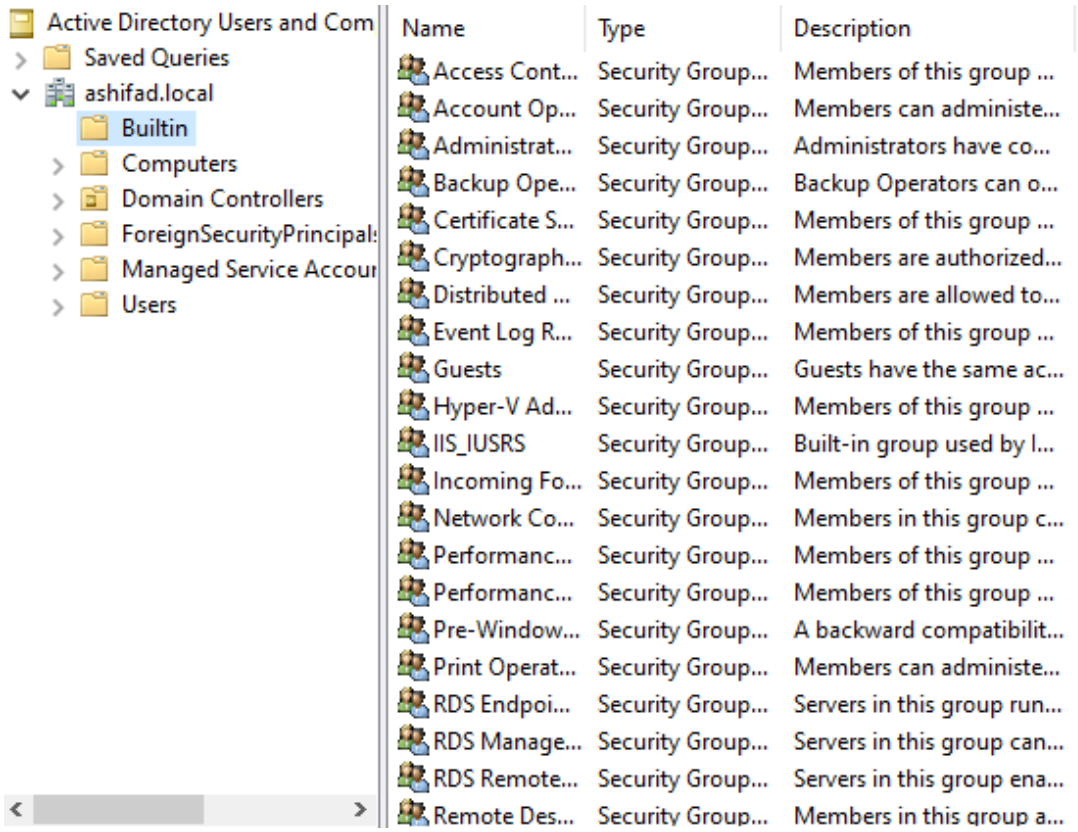
Here goes the installation, and sever will restart to show a sign that we have successfully installed AADF and promoted our server



Creating some users for the active directory

We got to go to Tools and click on AD Users and Computers, where we can create objects such as users, groups, computers, and etc.

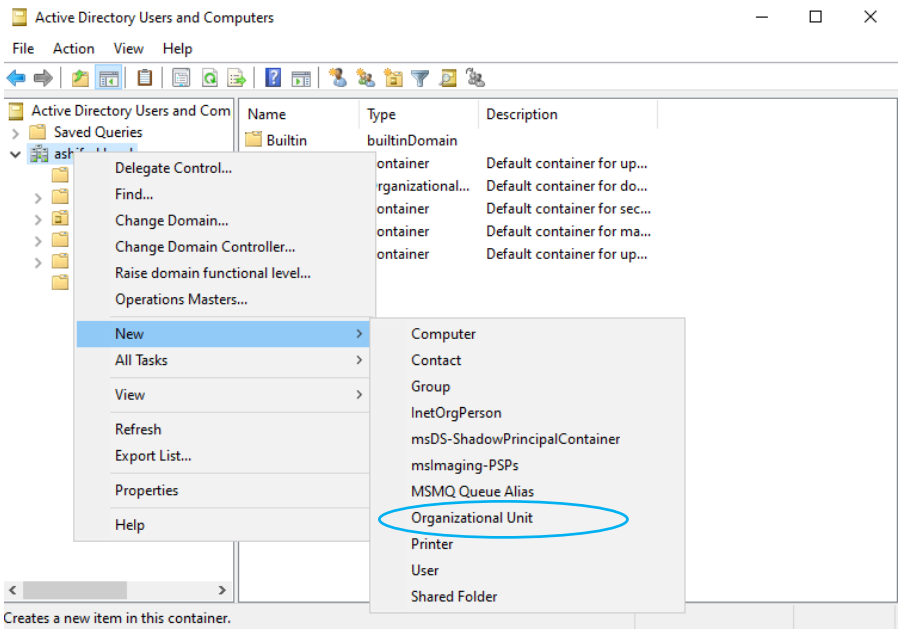




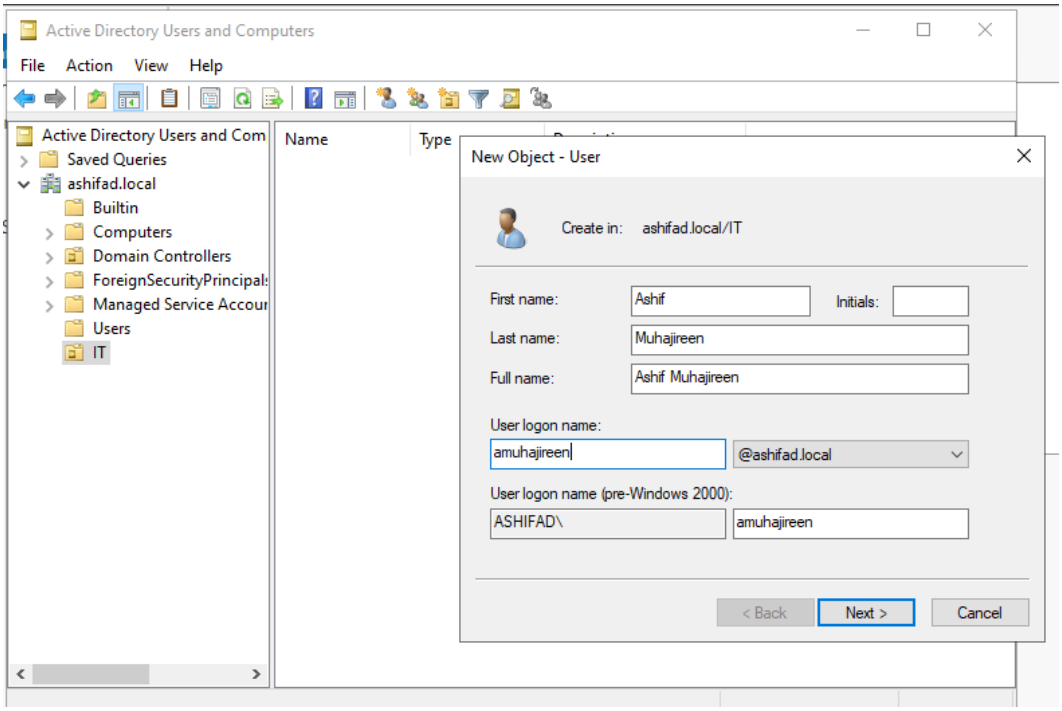
- Built in. here are all the groups listed automatically built by AD!

- If we click and see the object, it will give details such as: name, description, who's assigned to this group.
    - Under tab 'Member Off'. What other groups this group is in! You cannot add to built in groups, but can add them groups to new groups you create.

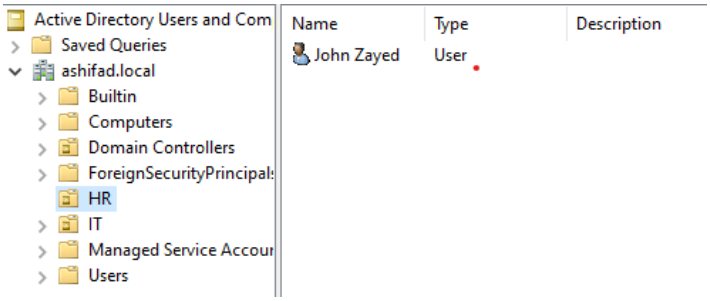
We can create users easily by right click and create, in the users sub folder, however it is ideally broken up to different parts in an organisation such as HR, finance, IT, etc.



- Clicking on organisational unit to create groups.



Within that group we create new users.

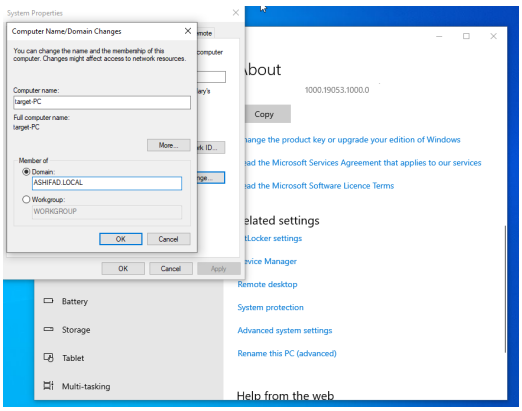


There are many scripts to aid auto auto-creating users computers and groups. In this project, it is just manual creation.

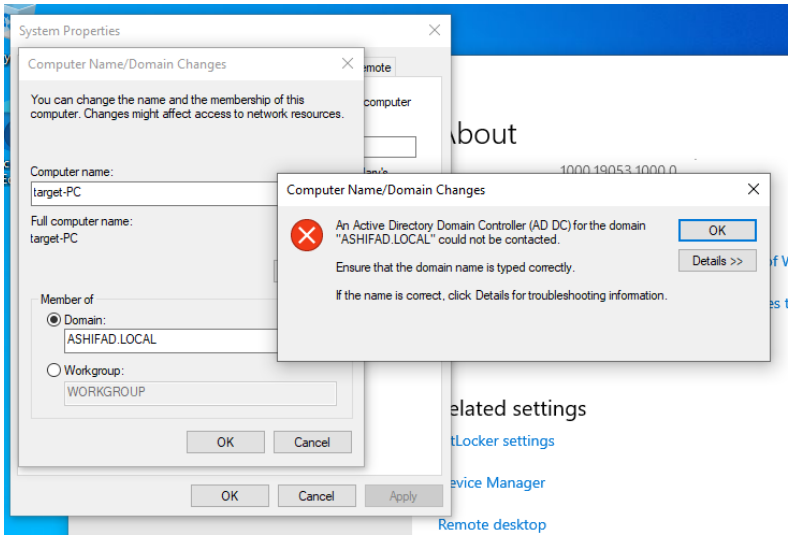
We have our AD set up, and our server is now a domain controller.

We will join our newly created domain (ashifad.local) on the Windows (Target) machine.

- Also to authenticate using one of the accounts!



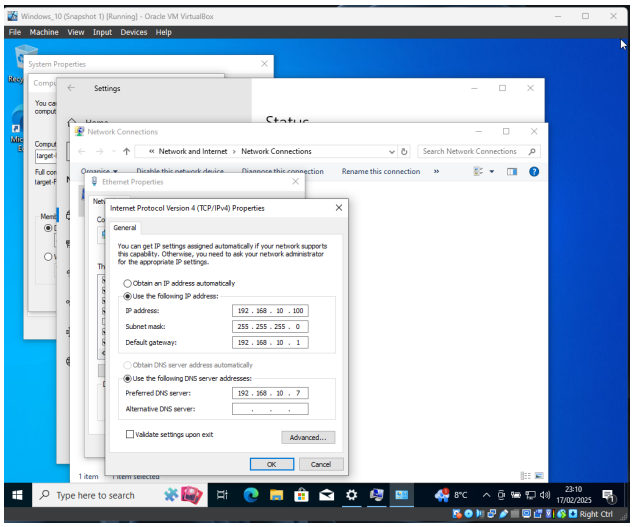
We are changing the domain from local to our domain

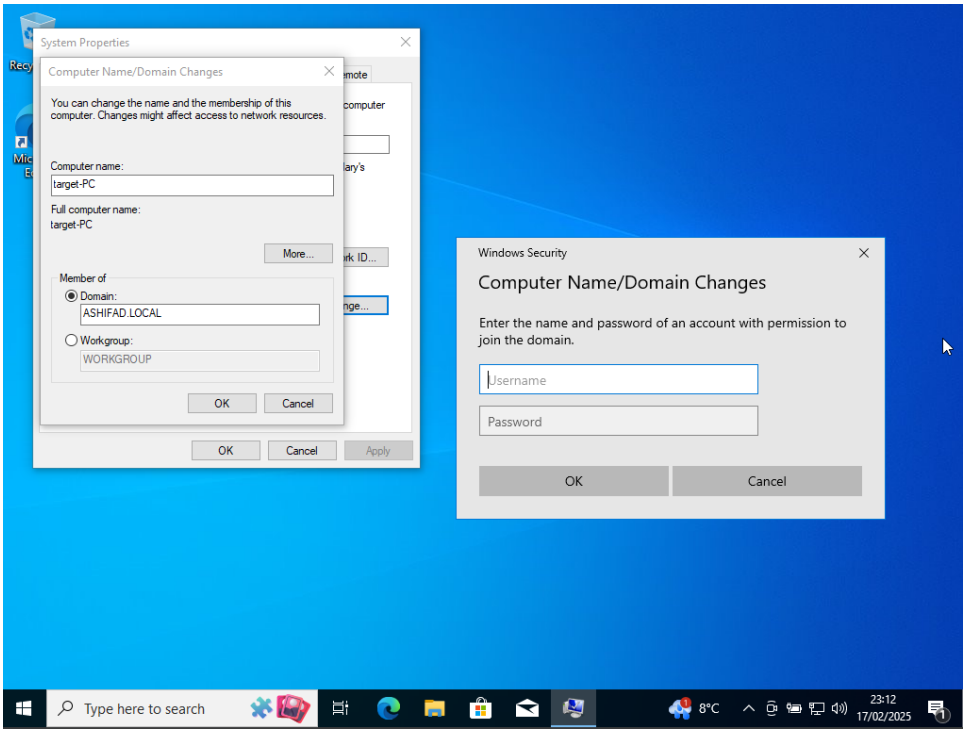


We are faced with this error because, our target machine does not know how to resolve ‘ashifad.local’, based on DNS.

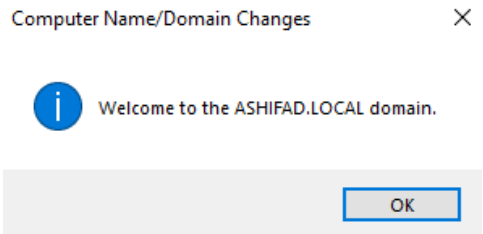
To fix:

- Go to the network adapter, same way to change IP address, and then, change google DNS to our domain controller.

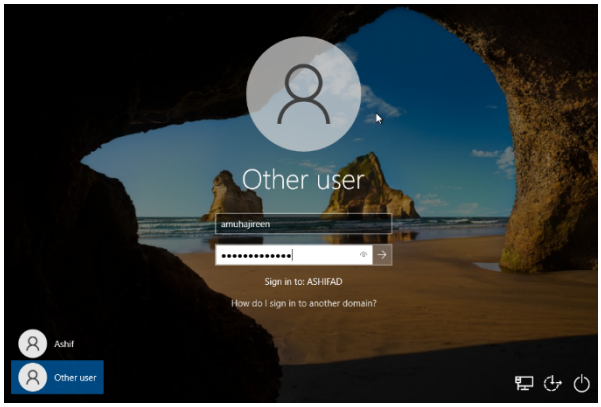


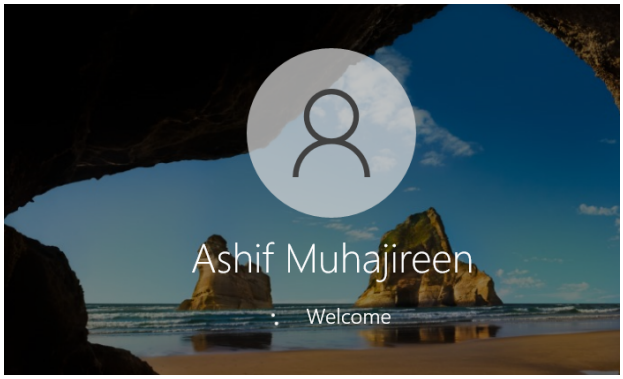


Now we get access! And can log in using our admin account of the server to log in, as this account will have the proper permissions.



Now we are attempting to login to the accounts we created earlier for IT and HR, by using ‘Other User’.

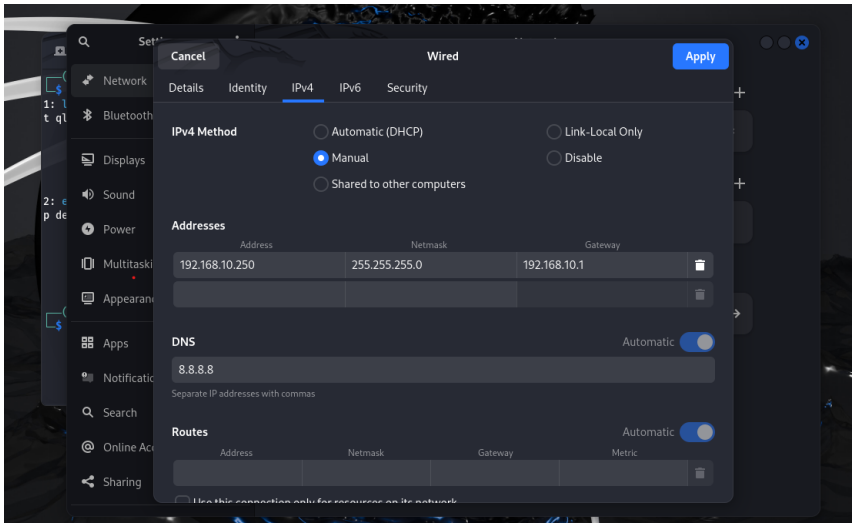




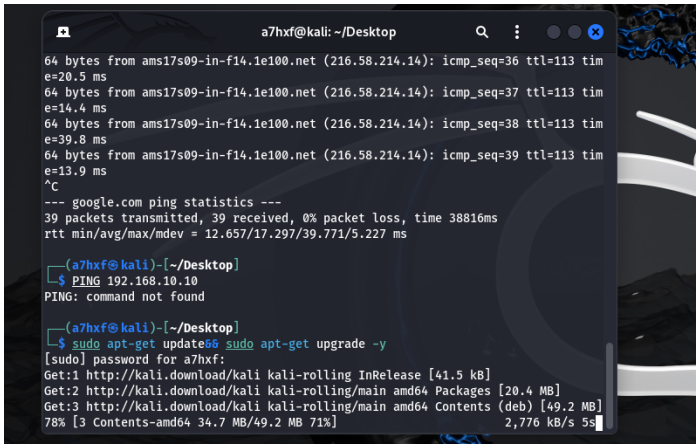
We can see that on sign-in to is pointed to my domain: ‘ASHIFAD’.

Using Kali Linux to perform a brute force attack on our users, and also using Splunk to view the activity!

- Afterwards, we will set up and install Atomic Red Team! And Run Atomic Tests.
- We will run Atomic tests, so in the future so in the future I will know how to use Atomic Red Team to generate telemetry and detect similar attacks in the future.



We change IPv4 from automatic to static! Using the IP configurations from our initial set up



Upgrading our repository to the latest versions

Setting up the attack:

1) Create a new directory called: ad-project, all files we will use and create will be there.
2) Installing crowbar to perform brute force attack, and we can target our domain controller or target machine!
3) Installing RockYou.txt is a word list used in Kali

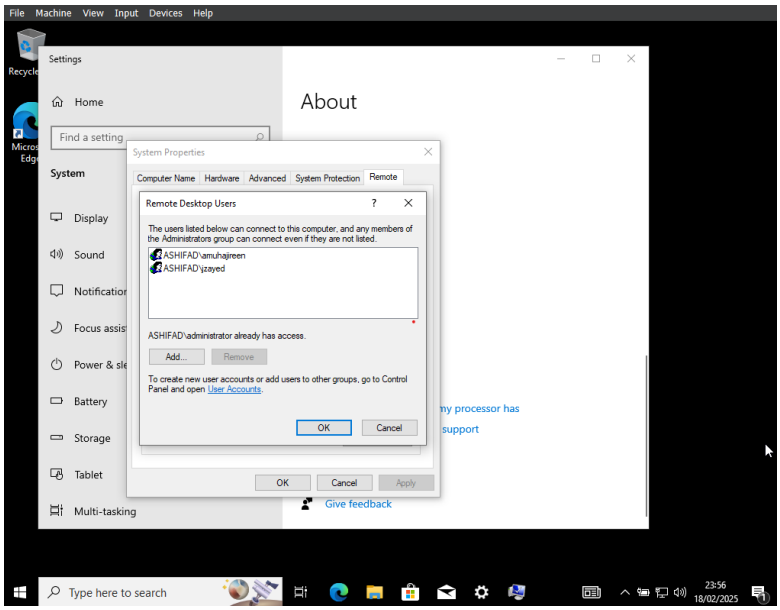
The file of rockyou.text size is about 134 megabytes! We will use only 20 lines for this project. We will make a new file called ‘passwords.txt’, and we will get 20 words from the file ‘rockyou.txt’ and past it there, with the addition of typing the account password for ‘amuhajireen’, and ‘jzayed’.

```
┌──(a7hxf㉿kali)-[~/Desktop/ad-project]
└─$ head -n 20 rockyou.txt > passwords.txt

┌──(a7hxf㉿kali)-[~/Desktop/ad-project]
└─$ ls
passwords.txt  rockyou.txt

┌──(a7hxf㉿kali)-[~/Desktop/ad-project]
└─$ cat passwords.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
```

We have allowed remote access to both users on Target machine!

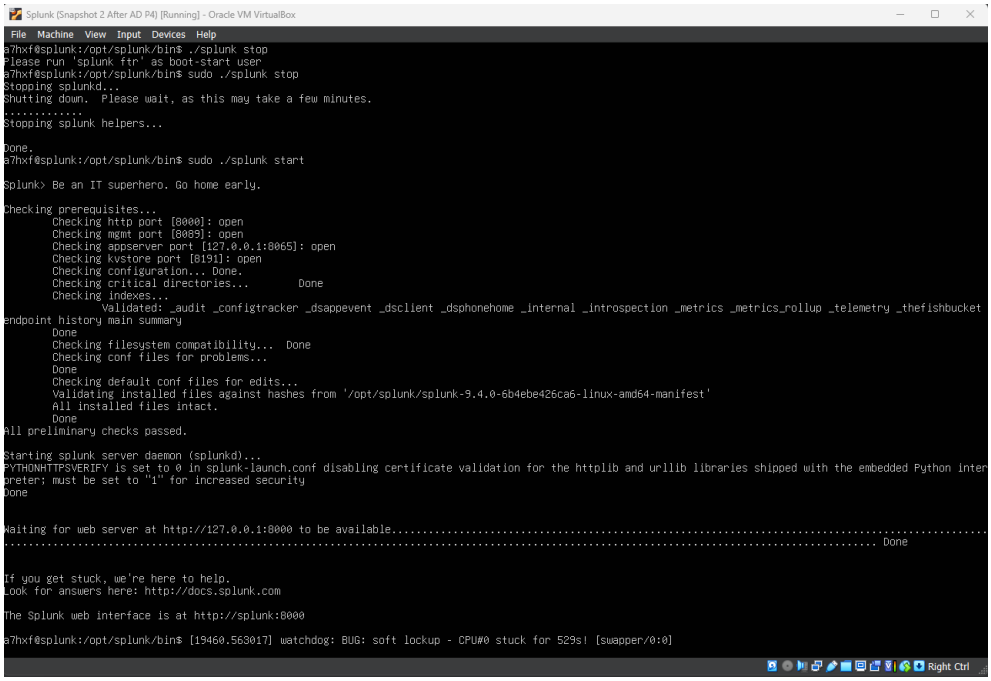



```
┌──(a7hxf㉿kali)-[~/Desktop/ad-project]
└─$ crowbar -b rdp -u amuhajireen -C passwords.txt -s 192.168.10.100/32
2025-02-19 17:55:23 START
2025-02-19 17:55:23 Crowbar v0.4.2
2025-02-19 17:55:23 Trying 192.168.10.100:3389
2025-02-19 17:55:29 RDP-SUCCESS : 192.168.10.100:3389 - amuhajireen:Liverpool123!
2025-02-19 17:55:29 STOP

┌──(a7hxf㉿kali)-[~/Desktop/ad-project]
└─$ crowbar -b rdp -u jzayed -C passwords.txt -s 192.168.10.100/32
2025-02-19 17:56:52 START
2025-02-19 17:56:52 Crowbar v0.4.2
2025-02-19 17:56:52 Trying 192.168.10.100:3389
2025-02-19 17:56:56 RDP-SUCCESS : 192.168.10.100:3389 - jzayed:Liverpool123!
2025-02-19 17:56:56 STOP
```

We have an RDP success, with the username and password of both users, as they are matched in the ‘passwords.txt’ by bruteforce attack using Crowbar!

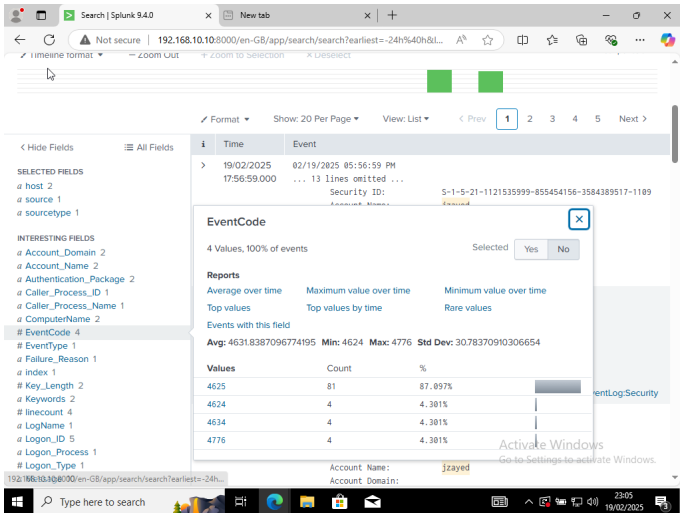
We use /32 as we only want to target this one IP, instead of using /24



I was stuck on this for ages! The Splunk server was online, but I couldn't access the web interface from my target machine. I tried everything I could think of, checking settings and troubleshooting different possibilities, but nothing worked. After a few hours of frustration, I finally came across some documentation online that explained:

- Sudo ./splunk ftr – FTR - **First Time Run** and is used to complete the initial Splunk setup.
- Sudo ./splunk stop
- Sudo ./spunk start

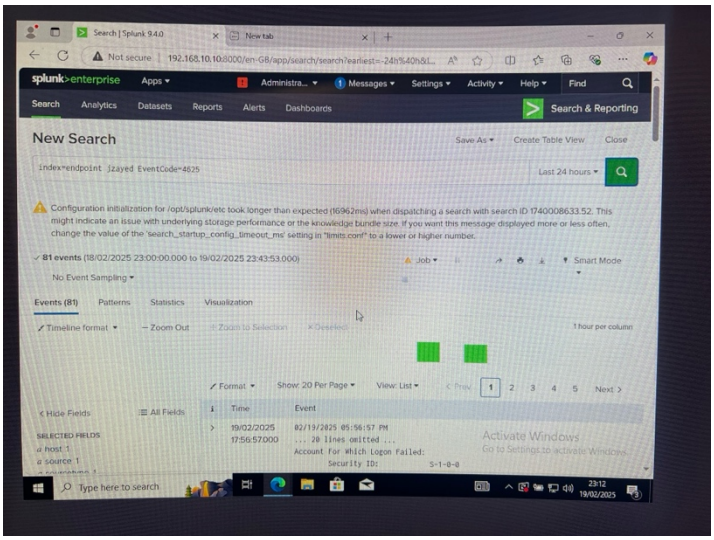
We entered privileged Splunk mode and then stopped the server and restarted the server again, and it worked!

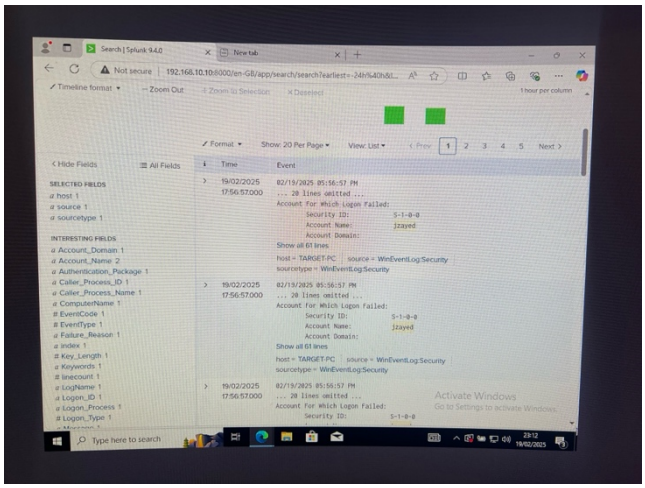


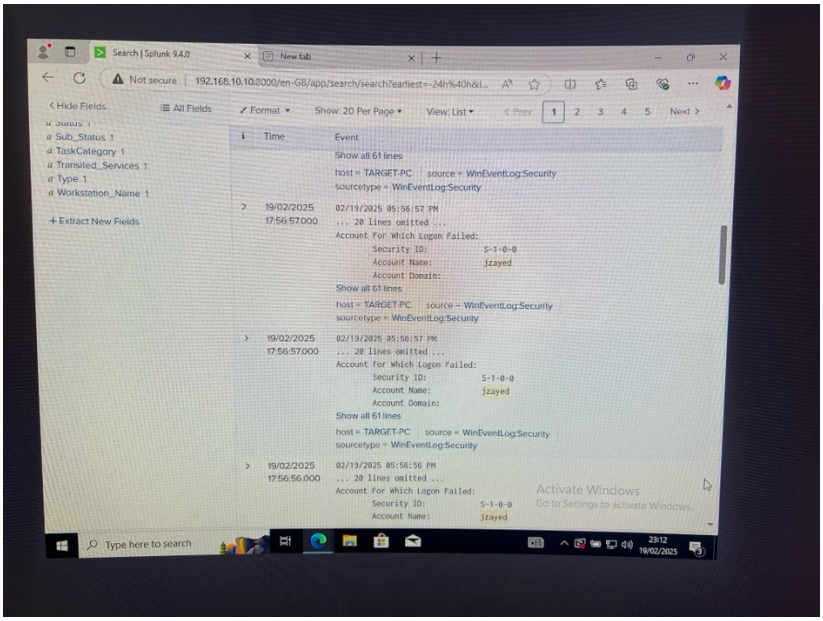
For 'jzayed' there is the event id 4625, it means there has been 81 failed attempts to log into that account. As we done multiple times, as earlier the Splunk web interface wouldn't connect to my web interface.

www.ultimatewindowssecurity.com

From this point, I had to use my phone to take pictures instead of taking screenshots and documenting, as having four virtual machines up was causing a lot of stress on my computer, leading to overheating and extremely laggy!



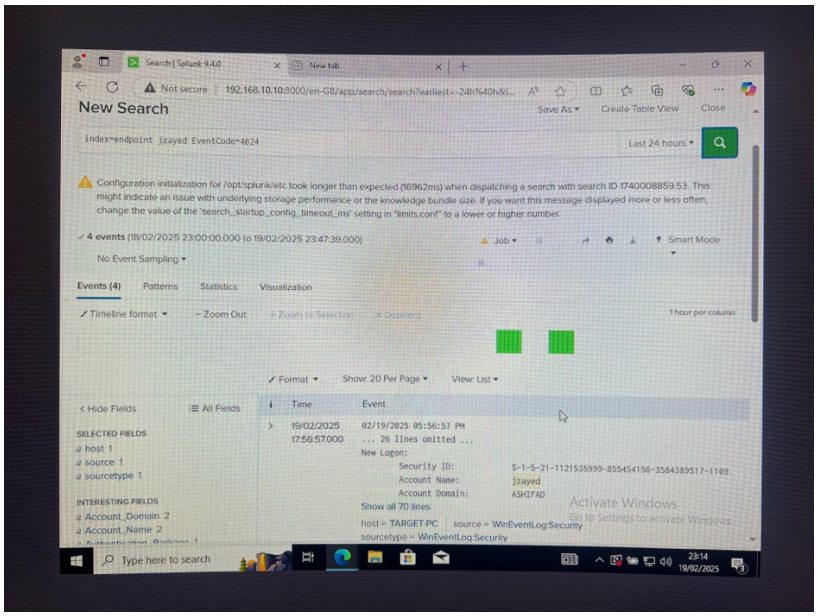


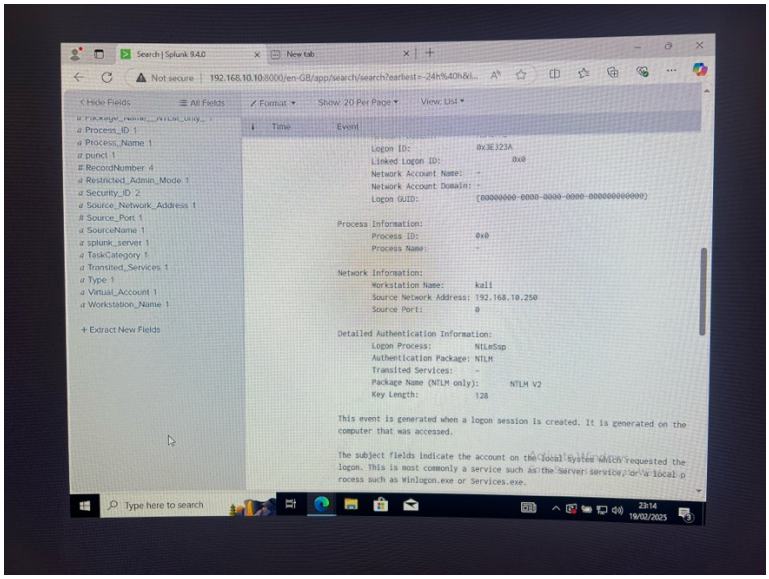


We can see that the time is almost/if not the same across multiple logs with the event ID: 4625 in our Splunk log, as, of course, we are doing a brute force attack, and it indicates that it is brute force attack!

When we look up the Event ID 4624:

- It shows it is an account which is successfully logged in!
    - Via: www.ultimatewindowssecurity.com



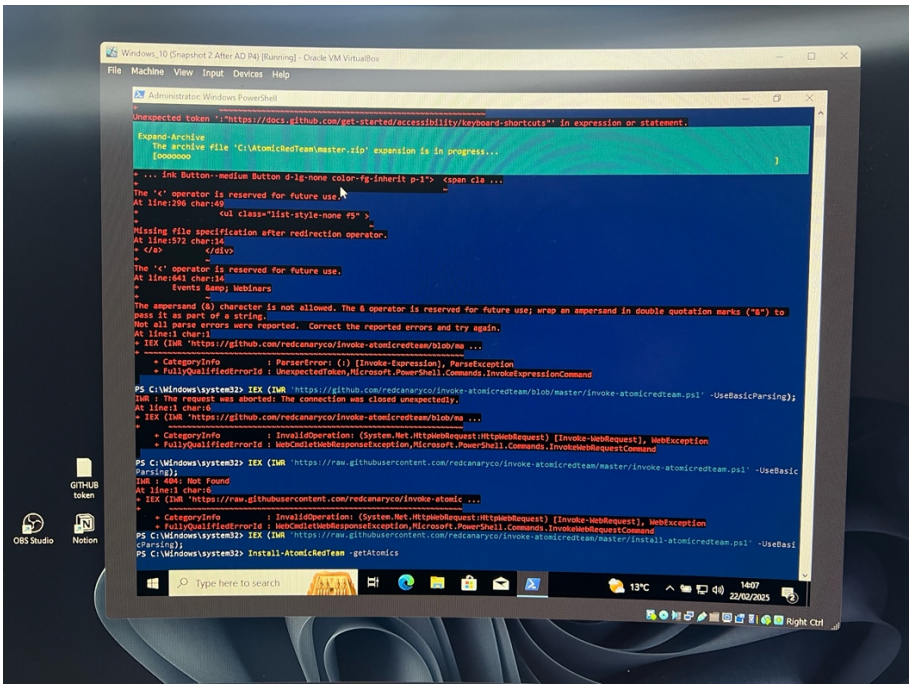


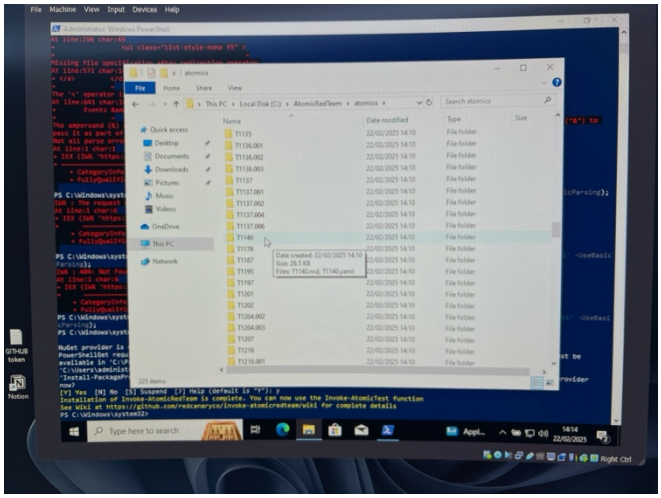
We can see that the account was successfully logged in, and the work stations Kali, and its associated IP address where its logging in from, which shows it's a clear attack!

Installing Atomic Red Team

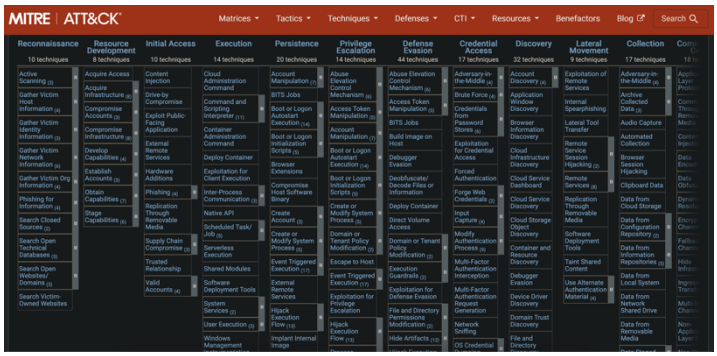
Before we install we got to make an exclusion for the entire C drive, as Windows Defender will detect and try to remove some files.

Now we install Atomic Red Team, using the GitHub file which was a pain to download!



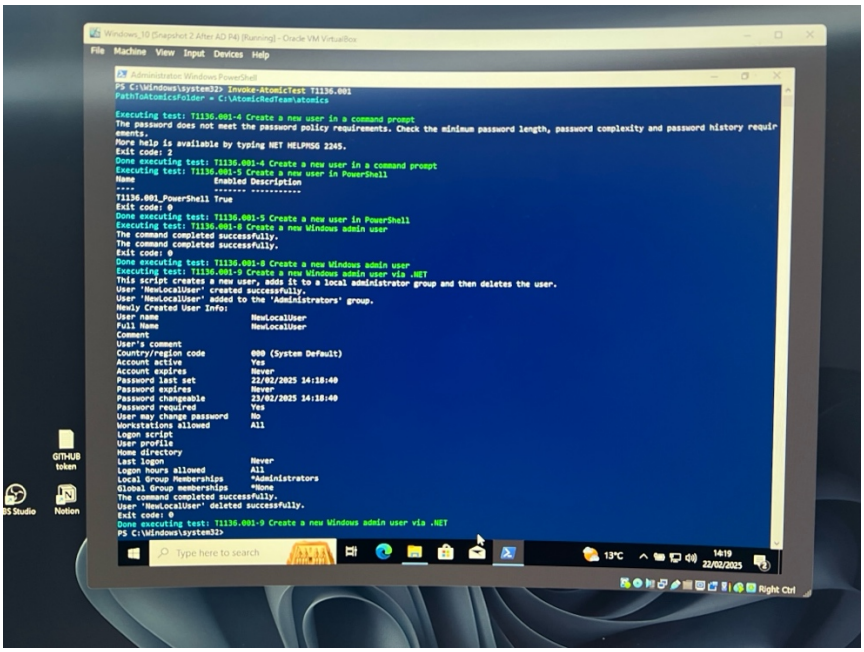


MITRE ATT&CK (https://attack.mitre.org/) is a website that explains how hackers attack and how to stop them. It lists different hacking methods, why they're used, and how to defend against them.

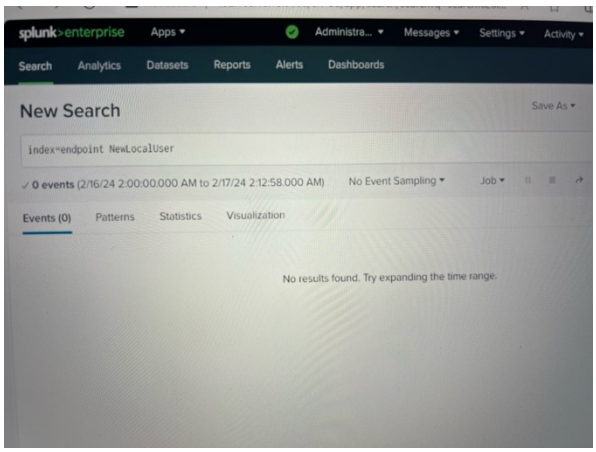


We will use the local account: T1136.001 – Creating Local Account

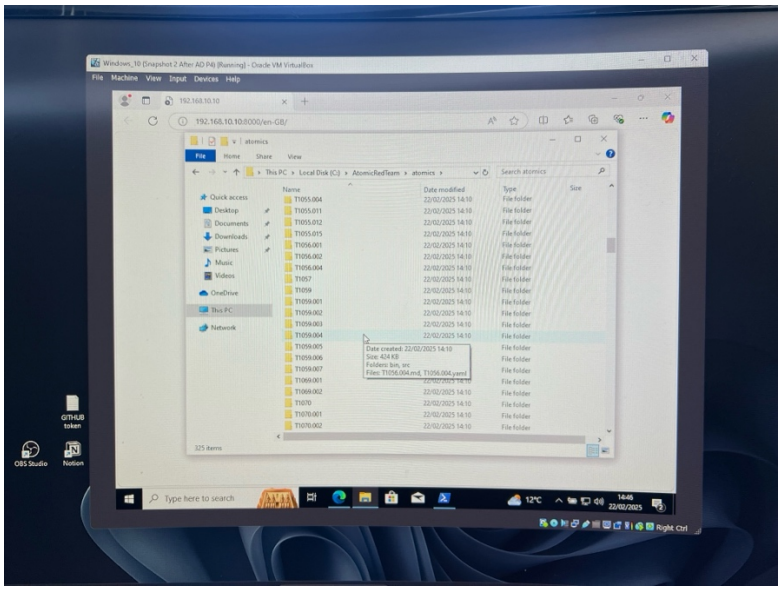
- This will automatically generate telemetry, based on creating a local account.
- Username is : NewLocaluser

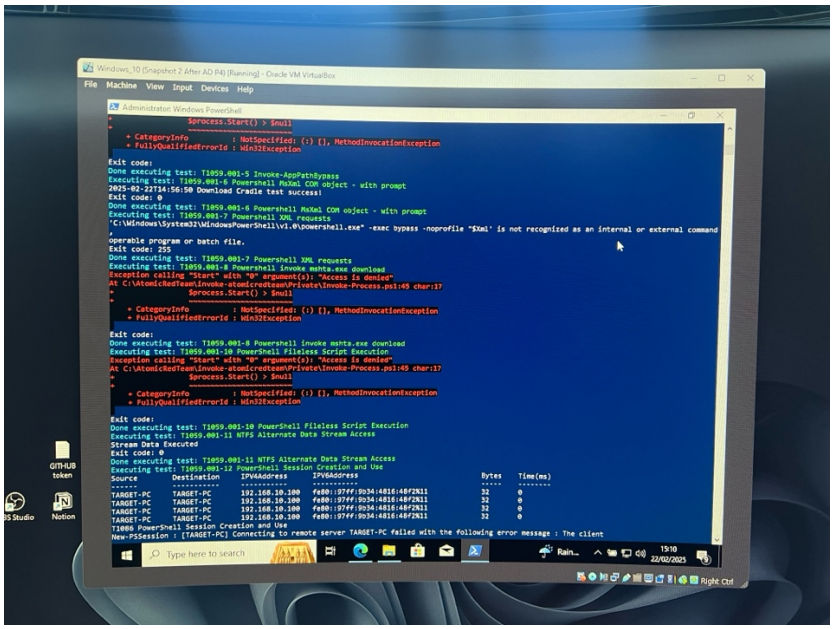


Now, looking at Splunk and searching for the endpoint, we find nothing when trying to detect the new user. This means that if an attacker were to compromise the system and create a local account, the current settings wouldn't pick up that activity—leaving it undetected.

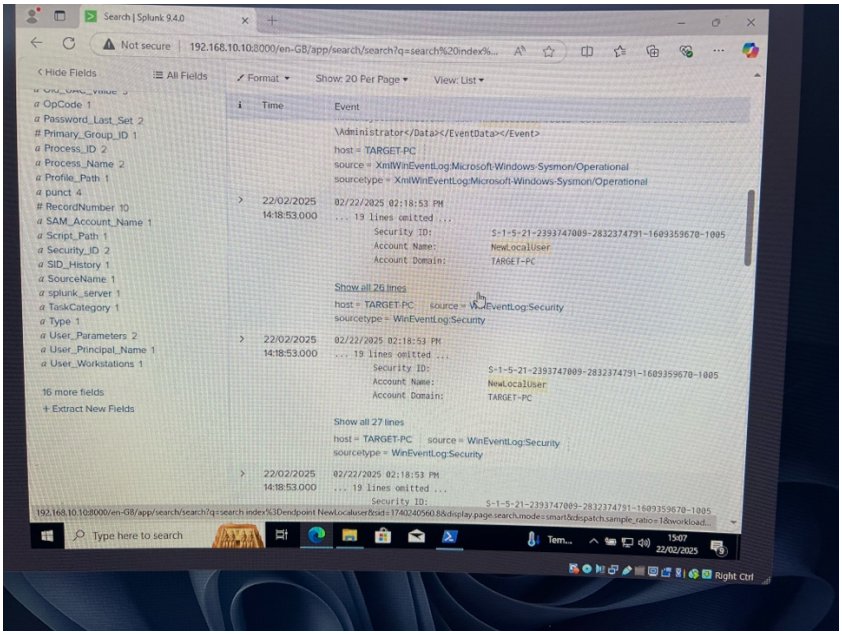


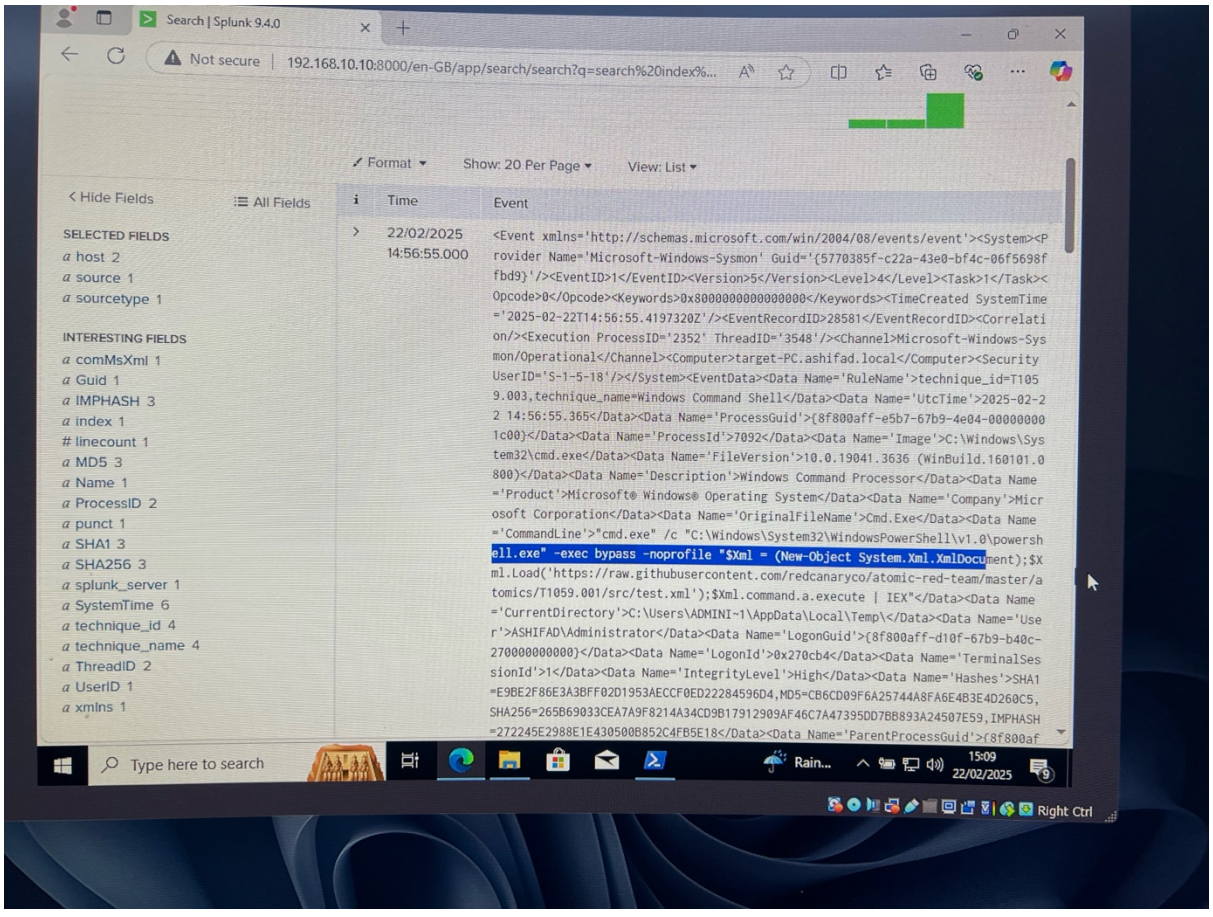
Now, let's do another: T1059 - **Command and Scripting Interpreter: PowerShell**





We had powershell command '-exec bypass -noprofile', we can search this in Splunk and see:





We can build alerts to detect activities in the future, in the future, along with creating a new local user account. The event generates it just takes a little bit of time!

Conclusion

I really enjoyed working on this Active Directory project. It was both engaging and challenging, pushing me to think outside the box and develop problem-solving skills that will be valuable in real-world scenarios. While it turned out to be more difficult than I initially expected, I remained committed to completing it—despite the frustration of dealing with an extremely slow computer at times! Overall, this experience has strengthened my technical skills, and now that it's completed, I'm excited to take on more projects and continue expanding my knowledge.