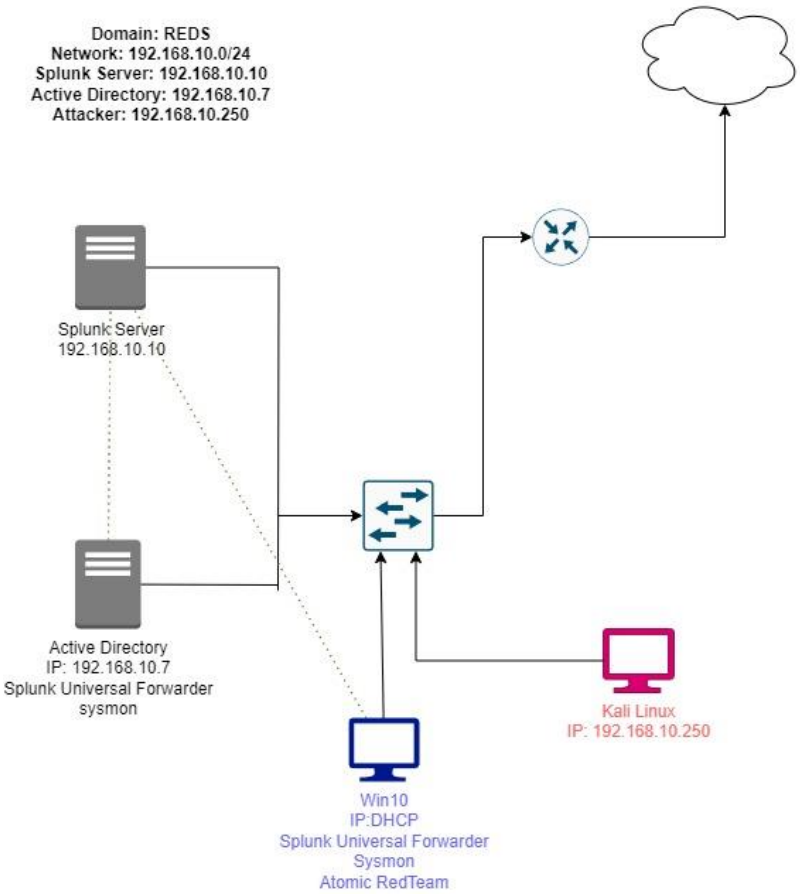
Active Directory Project (HOMELAB) -Part1

In line with my previous project; which was my homelab and active directory setup (homelab-setup) . I took a few steps further in this project. It includes:

- Windows10 which serves as my Target-PC
- WindowsServer22 which serves as my Domain controller
- Ubuntu server which serves as my splunk server
- Kali Linux which I use to perform attacks
- Splunk Universal Forwarder on my Target-PC and Server
- Sysmon on my Target-PC and Server
- AtomicRedTeam to carry out tests
- Crowbar on kali Linux to carry out attack



The objectives of this part is to:

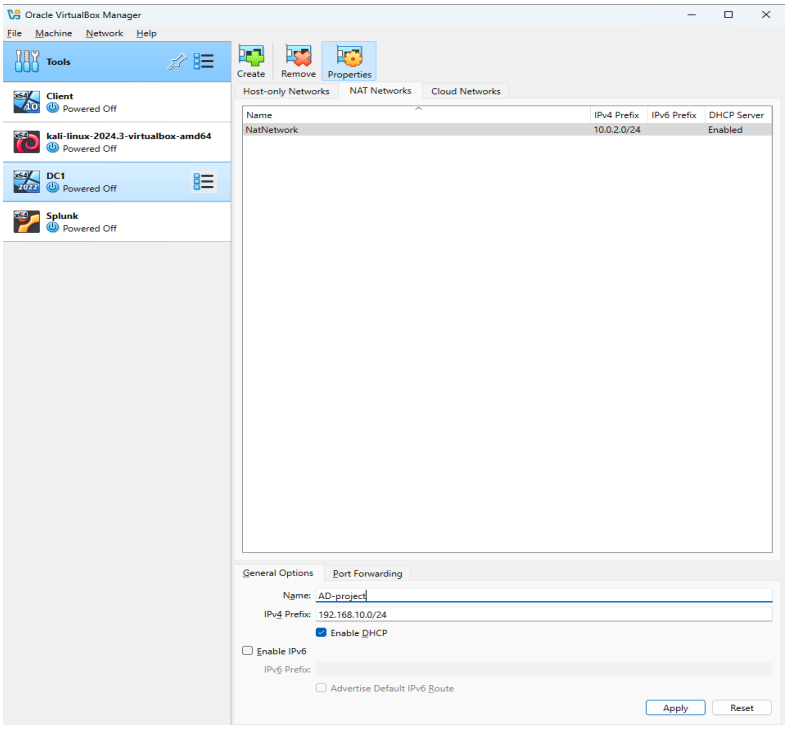
- Install and configure my required VMs

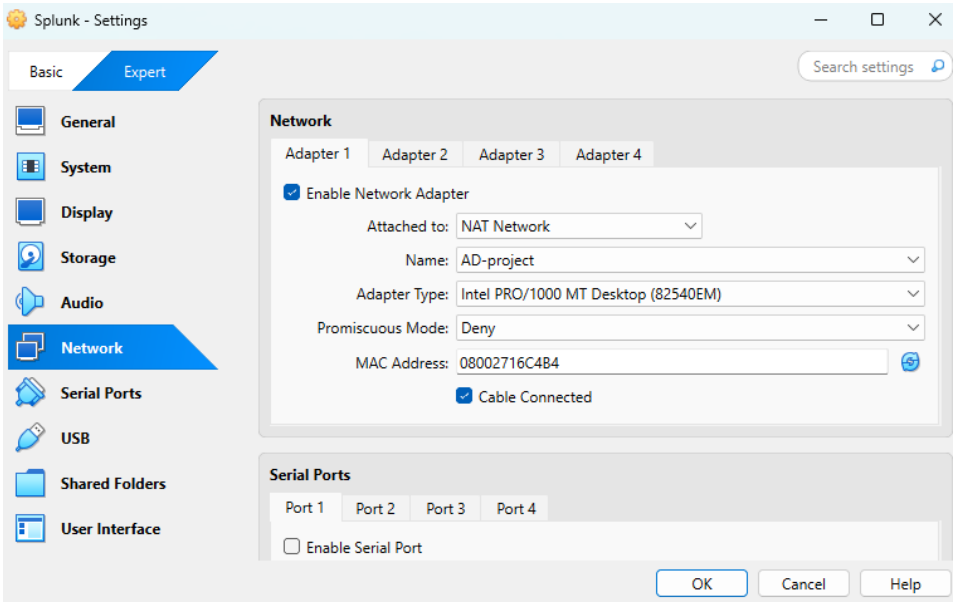
- Configure the homelab Network to be on the same Network according to our diagram above
- Setup splunk server on Ubuntu
- Install and configure Splunk and Sysmon onto our windows target machine and windows server to collect telemetry and send logs to splunk server

Installing VMs

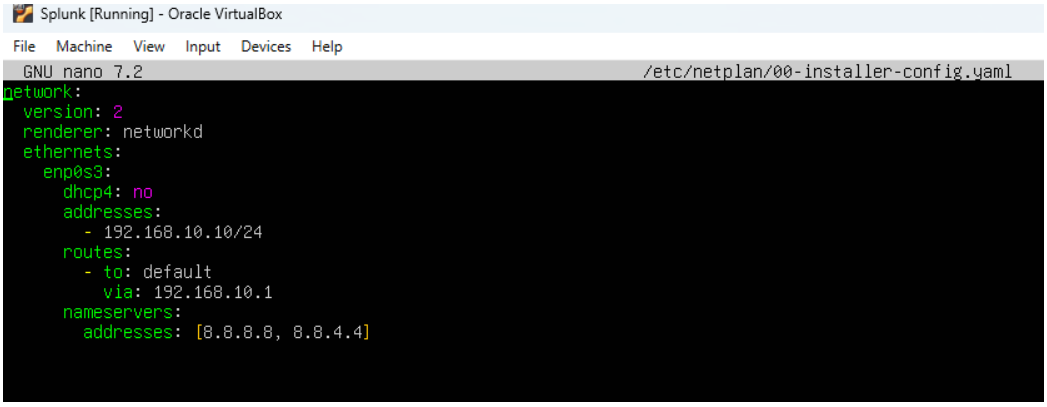
Because I had already installed windows10, windows Server and kali for a previous project, I only had to install Ubuntu server this time.

Network Configuration

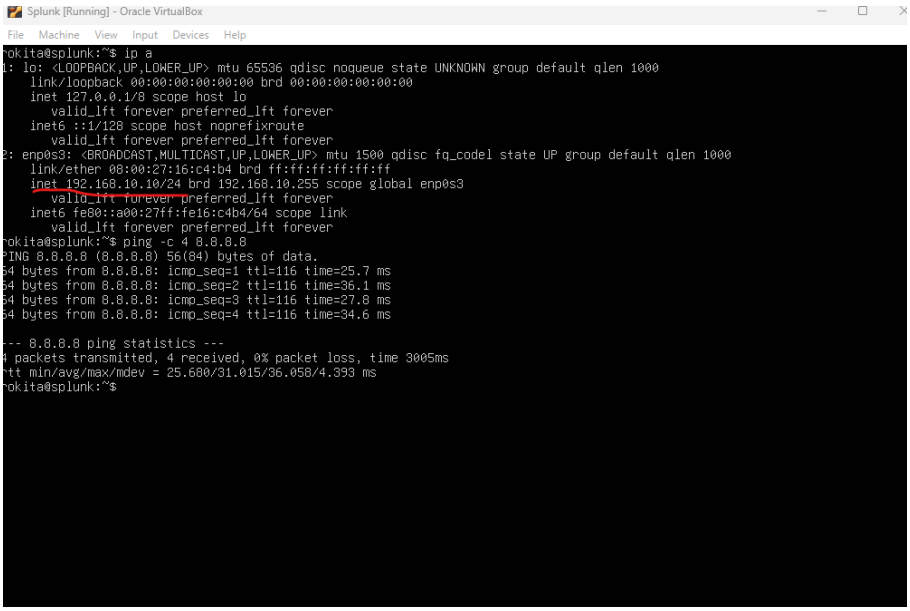
- On virtualBox, goto tools and click the bulletpoints icon, click on Networks and go to NATNetworks
- Create new Network, then go to properties
- Name the Network and then modify IPv4 Prefix according to network design
- 

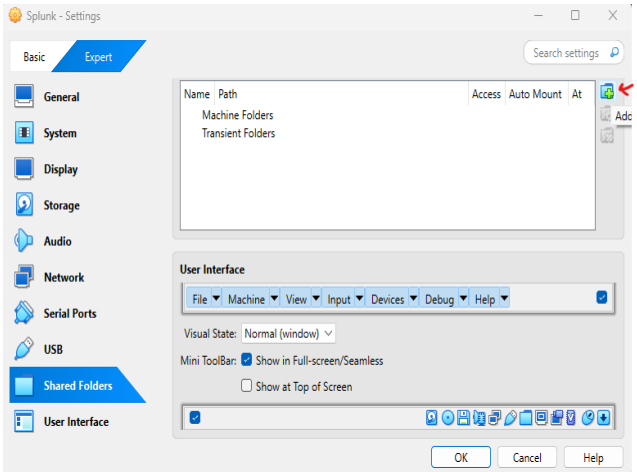
- Enable and hit Apply
- Now goto each of the VMs to configure the network settings
- Change to NatNetwork under Adapter settings
- 

Configure Splunk Server on Ubuntu

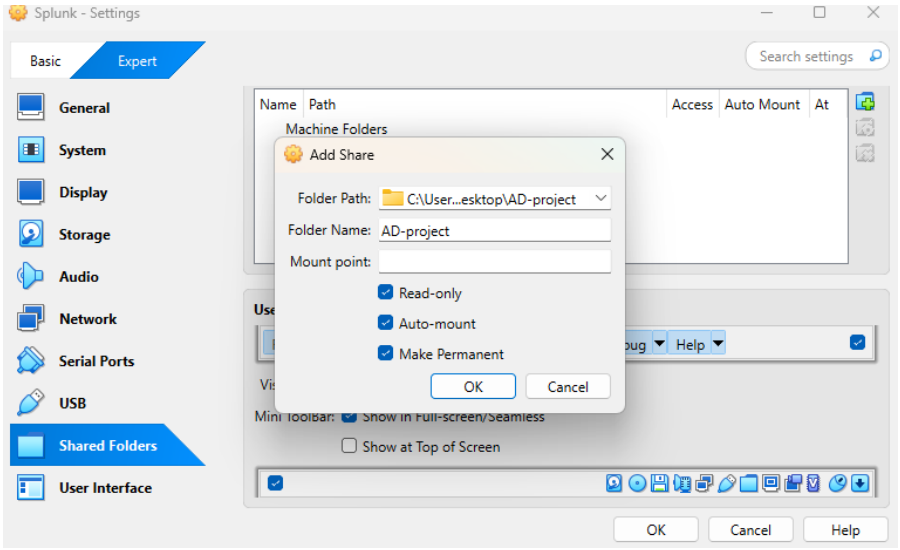
- First set static IP of splunk Server according to my network design
- To do this run the command ‘sudo nano /etc/netplan/00-installer-config.yaml’. Normally they ought to be an existing file that just needed some update but i didnt have this file so I just did a whole new configuration.
- I found a configuration guide on the splunk documentation site (settingstaticIP)
- 

- Save the file
- Run ‘sudo netplan apply’ for the changes to take effect
- Run ip a to confim changes

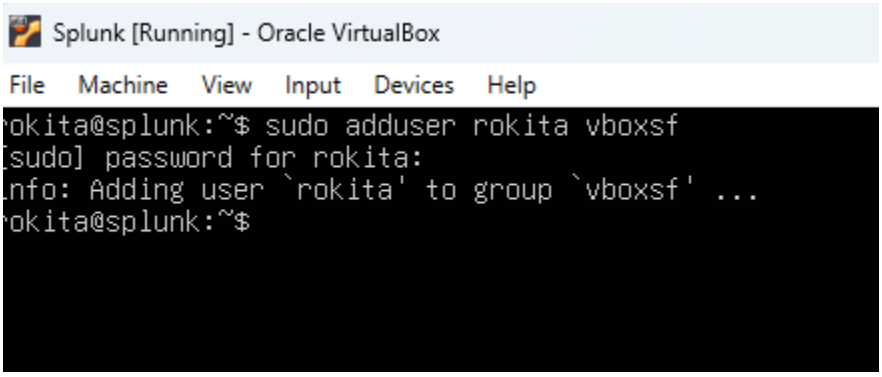


- Now download splunk on host(main machine)
- Goto splunk website and sign up
- Head over to products, click on ‘free trials & downloads’
- Scroll down to splunk enterprise and select ‘get my free trial’ Ensure to select the right version to download (deb)
- Now head back to splunk VM and install guest Add-ons for Virtual Box; Run the command: ‘sudo apt-get install virtualbox-guest-additions-iso'
- Head over to Devices and click on shared folders, then settings
- Add shared folder, The folder where the splunk download is on the host.
- 

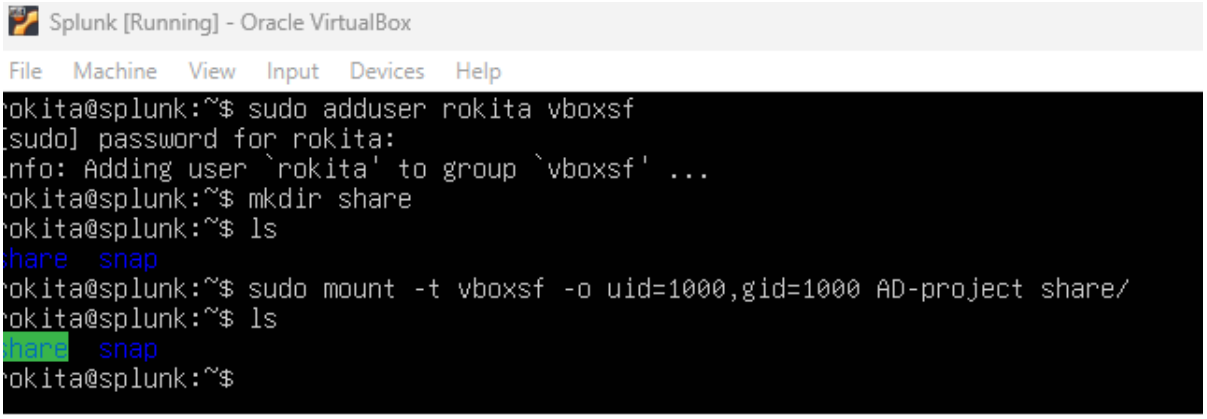
- Select the path where splunk download is
- Check the boxes and hit okay



- Reboot splunk VM
- Now Add user to the Vbox sharedfolder group by running the command: ‘sudo adduser username vboxsf’

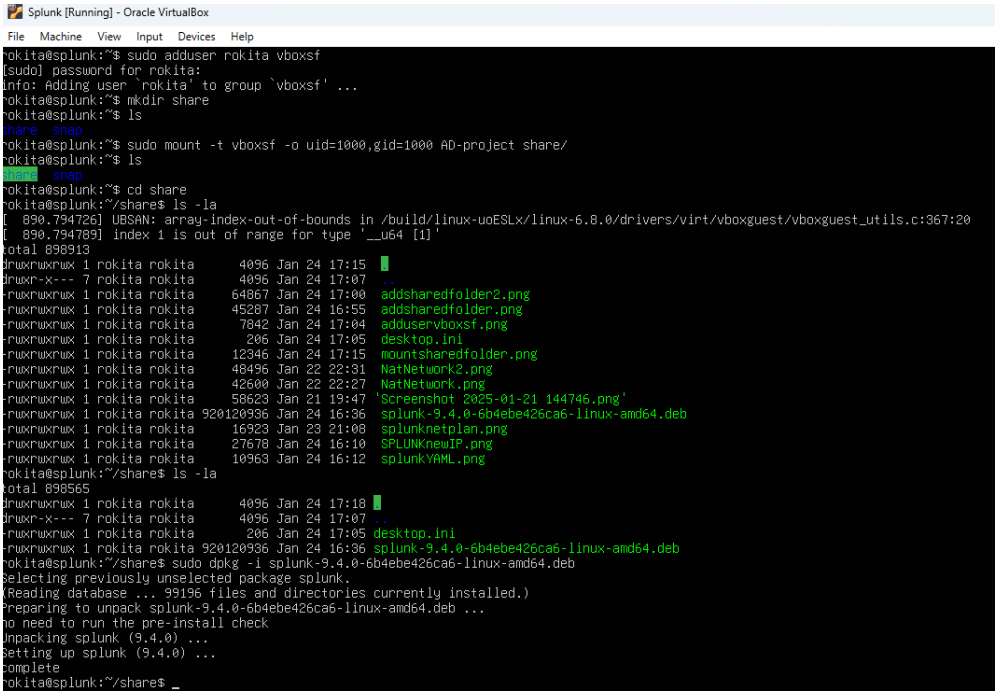


- Create a new directory called share; ‘mkdir share’
- Now mount the shared folder unto the share directory that was just created
- Run ‘sudo mount -t vboxsf –o uid=1000,gid=1000 AD-project share/

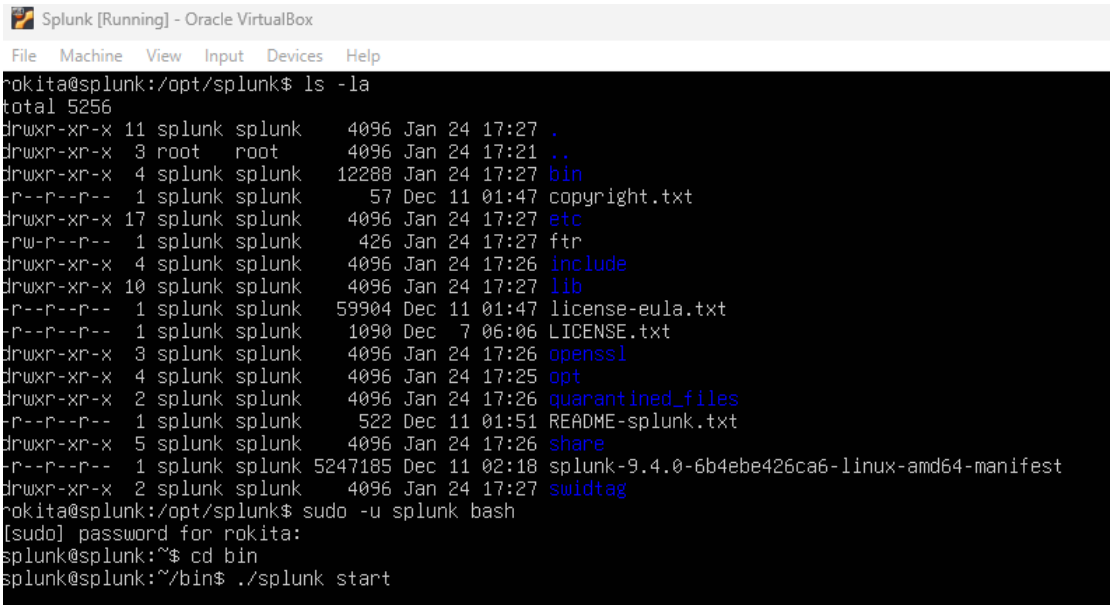


- Change directory into the share directory and install splunk

- Run ‘sudo dpkg –i splunk……’ (use tab to complete). This may take some time



- Now we change into the directory where splunk is located on our server
- ‘cd /opt/splunk’
- Since all the users and groups in this directory is splunk, we will change user to ‘splunk’
- ‘sudo -u splunk bash’
- Change into ‘bin’ directory
- Run ‘./splunk start’
- Hit space until the end of the user agreement and type y
- Enter an admin username and password
- Installation complete

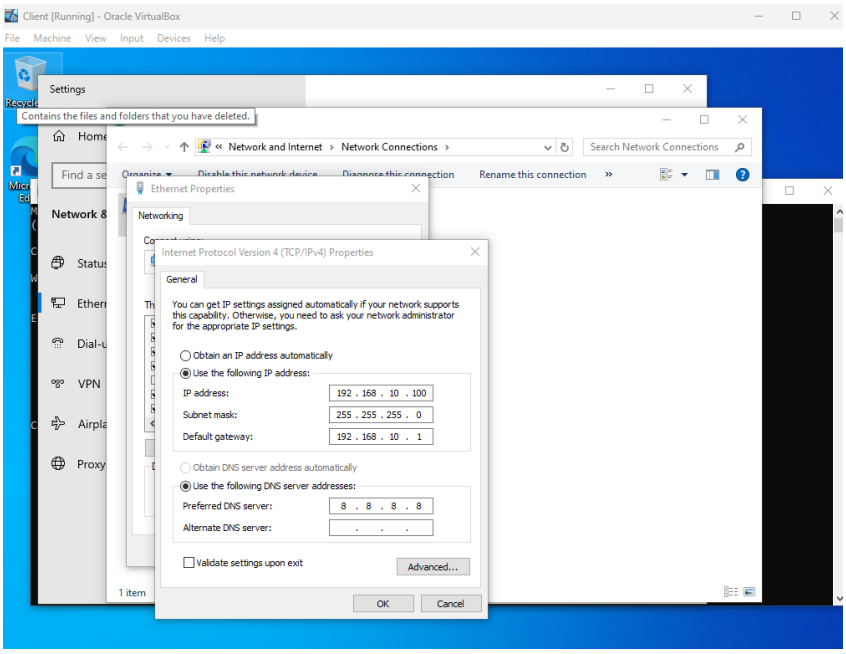


- Now we run a command to ensure our splunk starts up everytime our VM reboots
- Exit out of splunk
- Change to ‘bin’ directory
- Run ‘sudo ./splunk enable boot-start –user splunk’
- Anytime Ubuntu VM reboots, splunk will run automatically with the user ‘splunk’

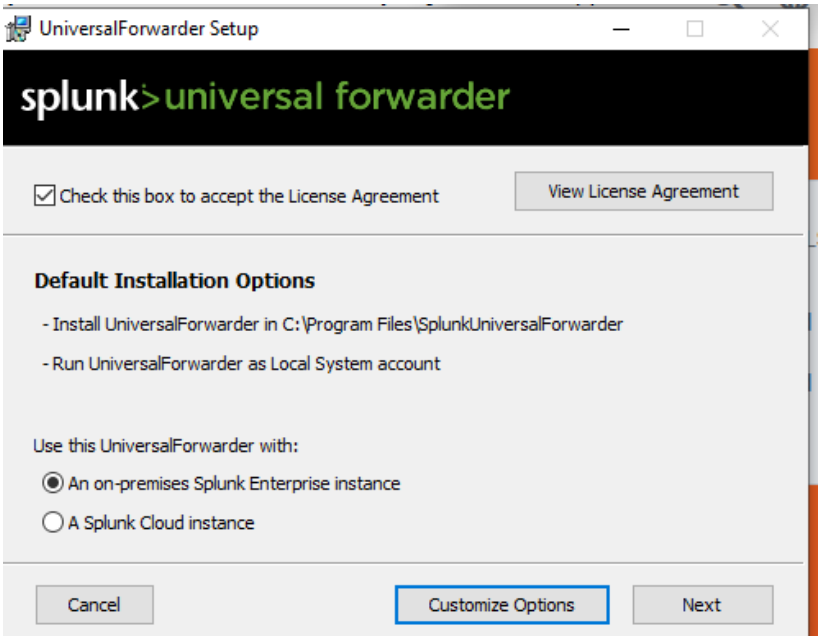
Part2

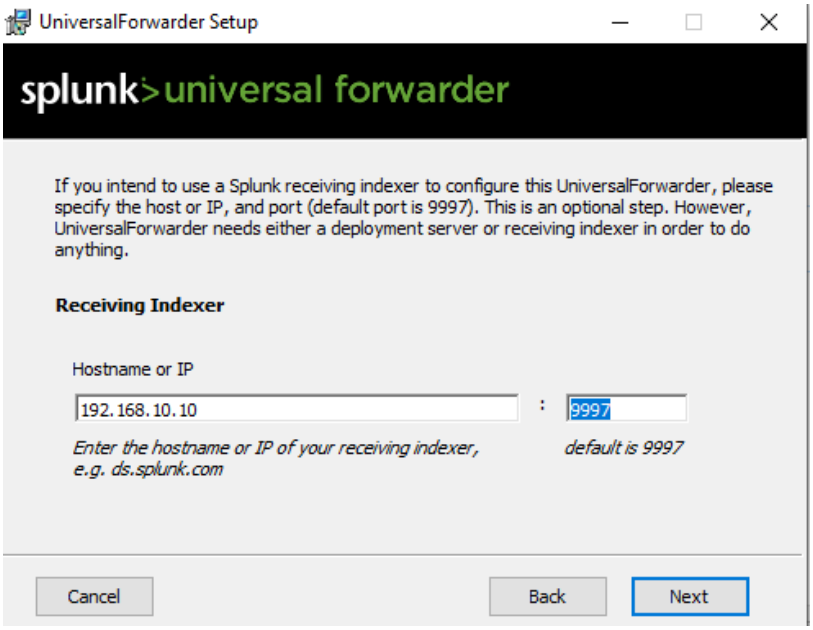
Now we install and configure Splunk Universal Forwarder and Sysmon on both our Target-PC and Windows Server

- Goto internet settings, Change adapter options.
- Change IPv4 address according to Network design.

- 

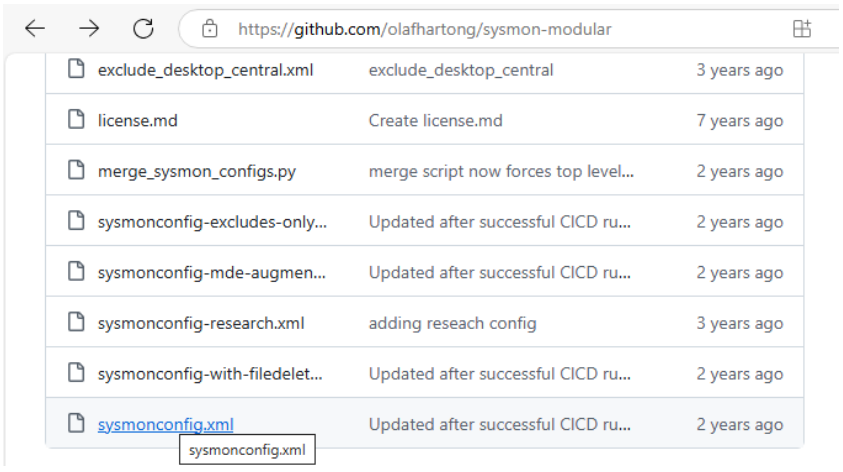
- Open web browser and access splunk server on 192.168.10.10:8000 (splunk listens on port 8000).
- Head over to splunk website to download Splunk Universal Forwarder
- Go to free trials & downloads
- Select and download the appropriate version of Splunk Universal Forwarder suitable for system
- Click on the downloaded SUF
- Accept agreement and ensure ‘on-premise option’ is selected
- Generate random password
- Skip Deployment server because I don’t have one
- Receiving indexer: This is going to be our splunk server; IP: splunk server IP, Default Port: 9997 (default port for receiving events)

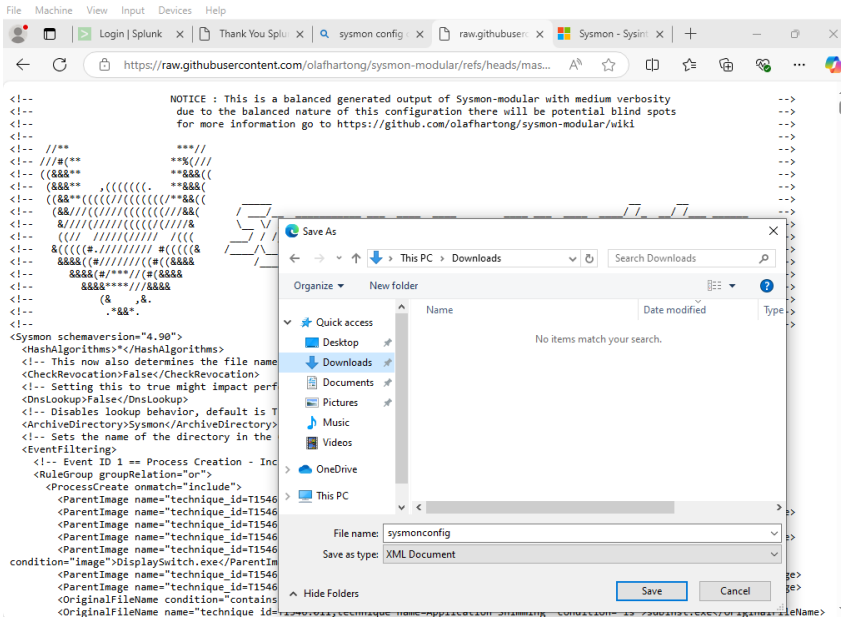




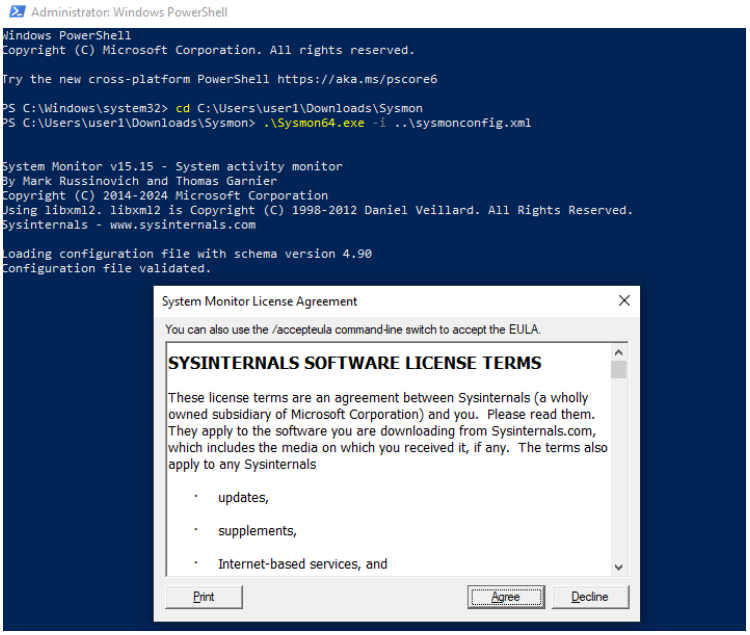
Download Sysmon by Sysinternals

- Search for sysmon on web browser, select sysmon by sysinternals and download sysmon.
- Now download sysmon config by olaf (search for this on browser)
- Click on his github, scroll down and select ‘sysmonconfig.xml’
- Click on Raw, right click and save as

- 

- 

- Goto Downloads, click on the zipped sysmon folder and extract
- Enter the folder, right click on the file expplorer bar and copy the file path
- Open powershell and run as administrator
- Change directory into the copied file path
- Run the command '.\sysmon64.exe -i ..\sysmonconfig.xml'
- In the command above i use the -i flag to indicate that i want to specify a configuration file and the '.' before '.\sysmonconfig.xml' is because we are moving one directory back to where our configfile is saved.
- Agree to the license agreement and start sysmon

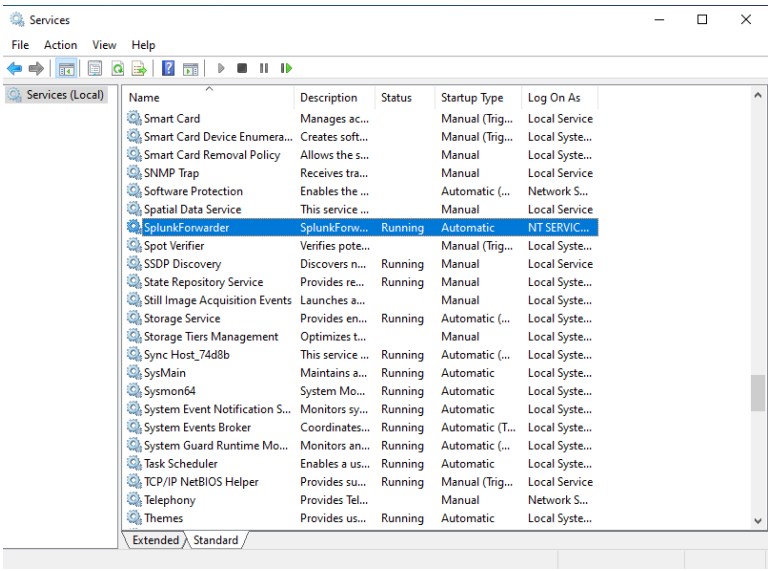
- 

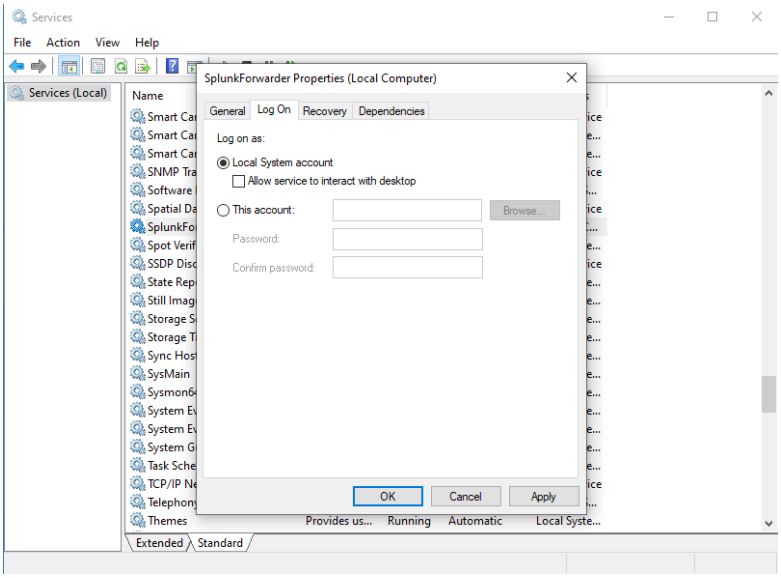
Part 3

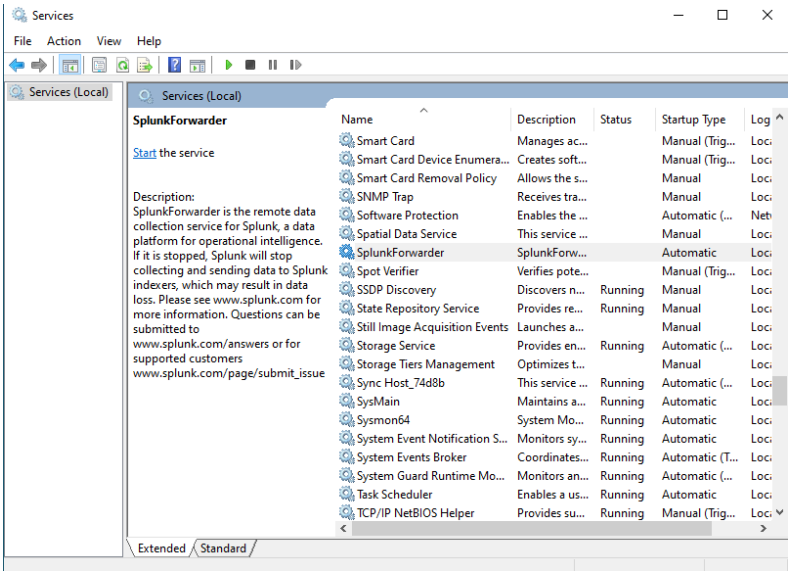
Splunk Configuration

- Instruct splunk universal forwarder on what to send to my splunk server
- We must configure a file called ‘inputs.conf’ on our Target-PC
- This file already exists and can be found by navigating to Cdrive>program files>Splunkuniversalforwarder>etc>system>default
- But we do not configure the file in the defaults folder because it is some sort of fallback incase of an issue
- Open up notepad as an administator
- I input the contents of the inputs.conf file copied from instructor
- This is basically instructing splunk forwarder to push events to relating to Applications, security, system and sysmon over to splunk server. In this conf file; index = endpoint.
- Save this file under the local directory instead of defaults. Local directory still in the same system directory as default.

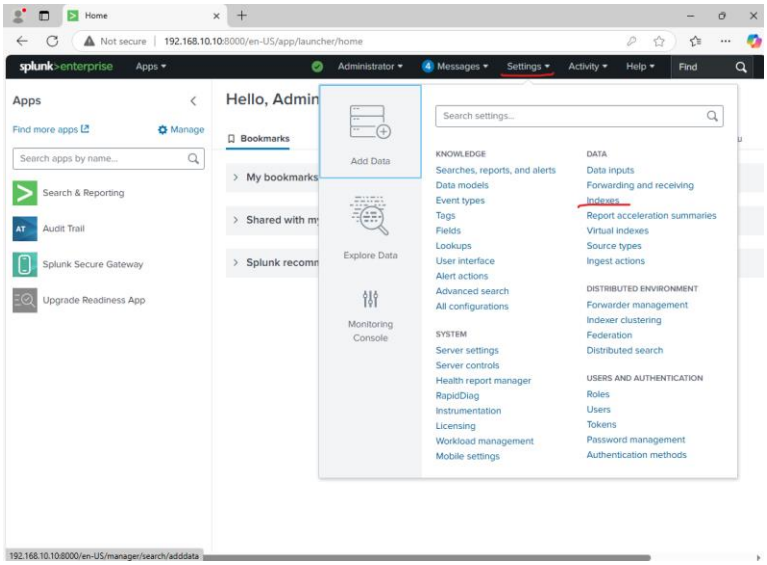
Restart SUF service

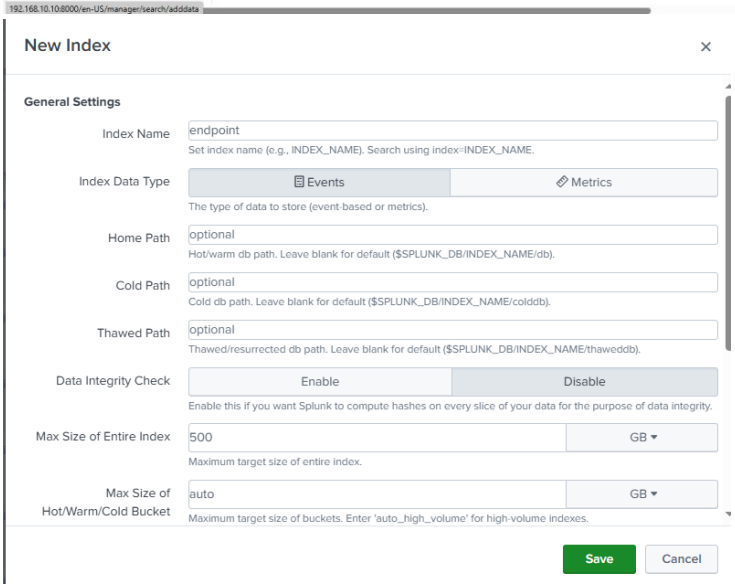
- Any time inputs.conf file is modified, Splunk universal forwarder service must be restarted.
- Search up services on PC, run as administrator
- Find splunk forwarder service
- Scroll to the right to to confirm ‘log-on as’ is local system instead of NT\service. Otherwise it might not be able to collect some logs due to some permissions
- If it is NT\service, double click on the service and select local system account instead.
- Hit apply, then restart the service
- Error notification may pop up, just click okay.
- Then start the service
- 

- 

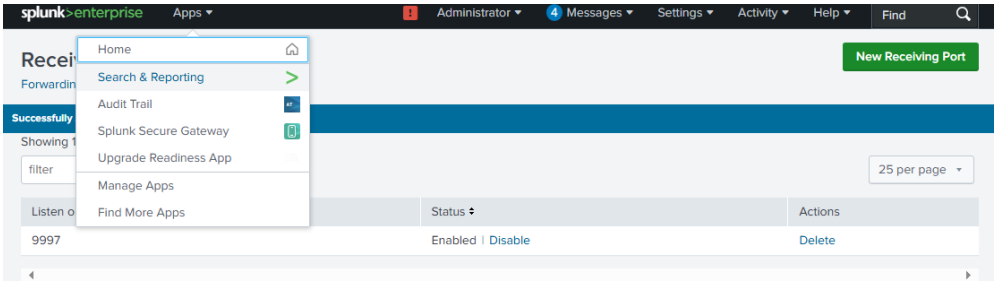
- 

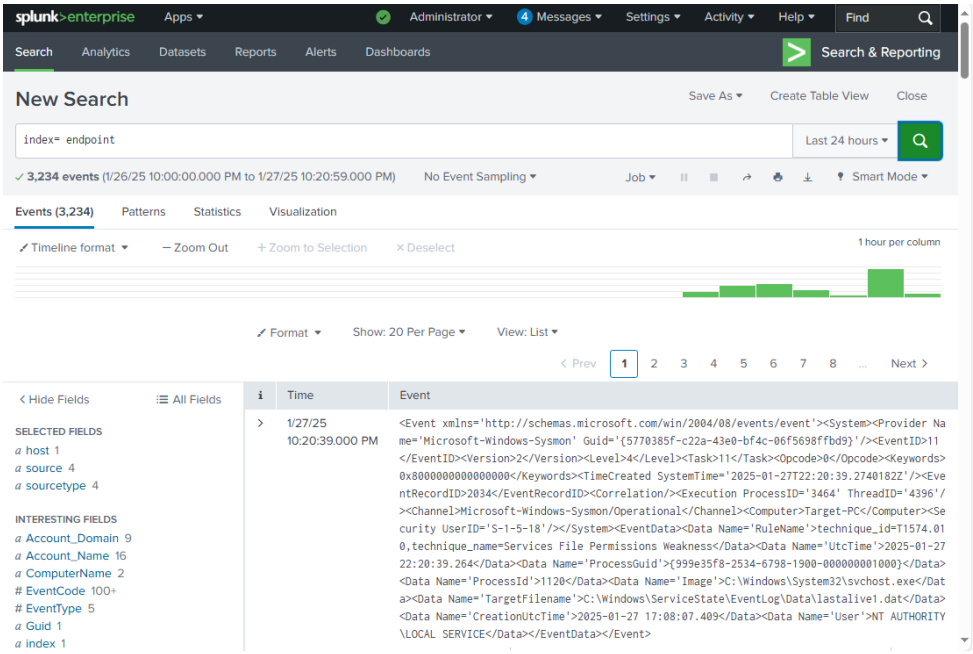
- Head over to splunk web portal and login with the credentials created
- After login, select settings at the top menu bar
- Head over to indexes
- Based on our inputs.conf file, all of the events are being sent to an index called ‘endpoint’
- Click new index, put in the name ‘endpoint’ and save.

- 

- 

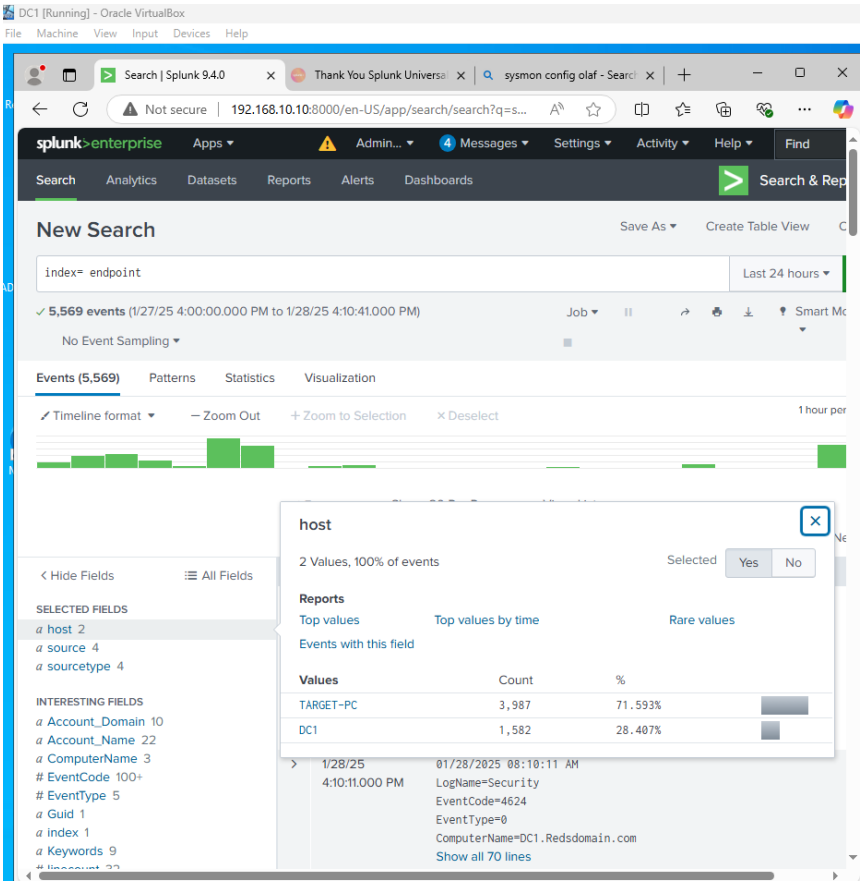
- Goto settings at the top bar again
- Click on ‘forwarding and receiving’
- Click on configure receiving
- Click on ‘new receiving port’ at the top right
- Type ‘9997’ hit save
- If everything is set correctly we can start seeing data coming in
- Click on Apps on the top bar
- Click on ‘search & reporting’

- 

- Search ‘index = endpoint’
- Now we see data being collected from Target-Pc
- 

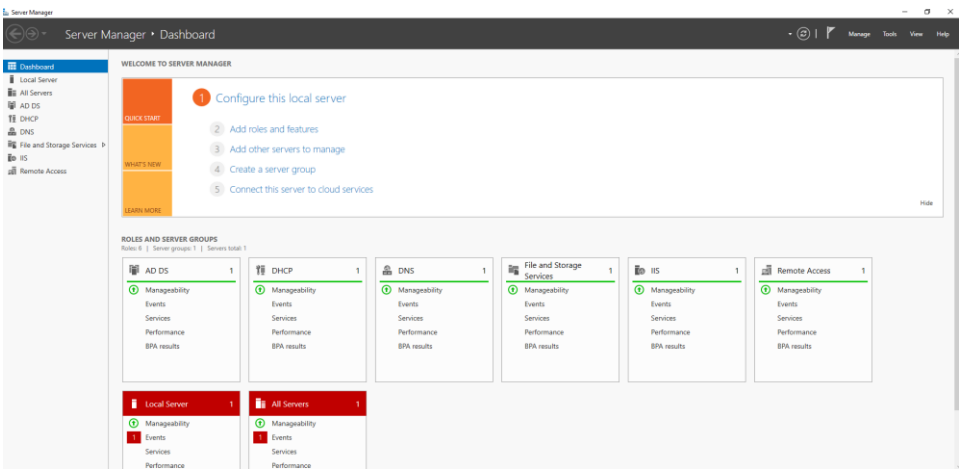
Perform the same Splunk Configuration for DC

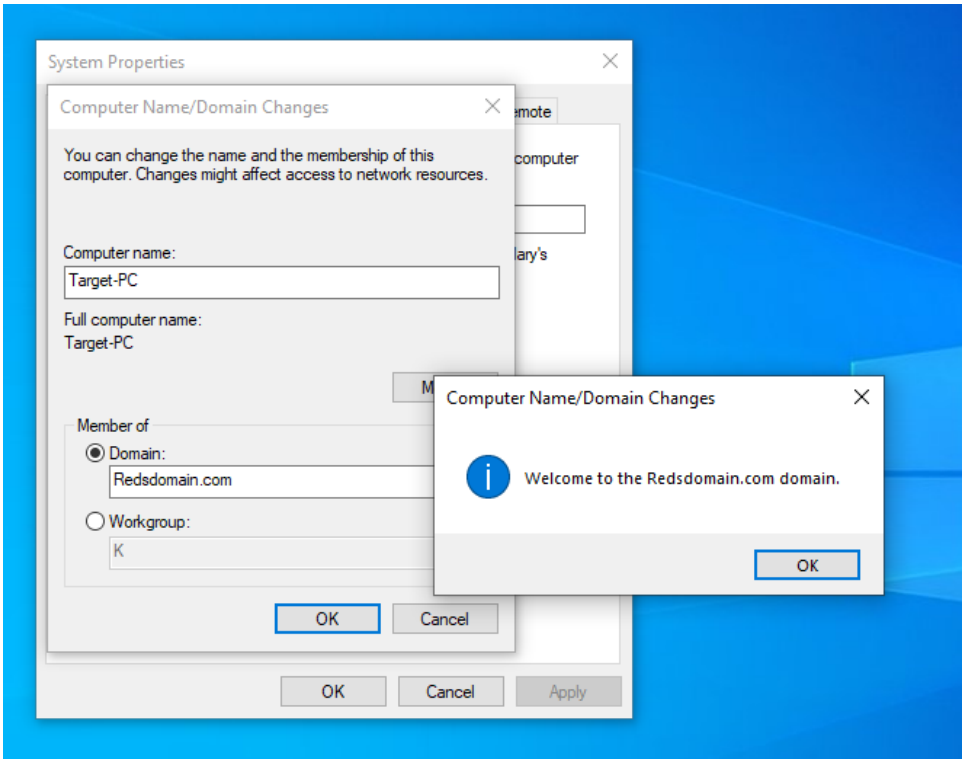
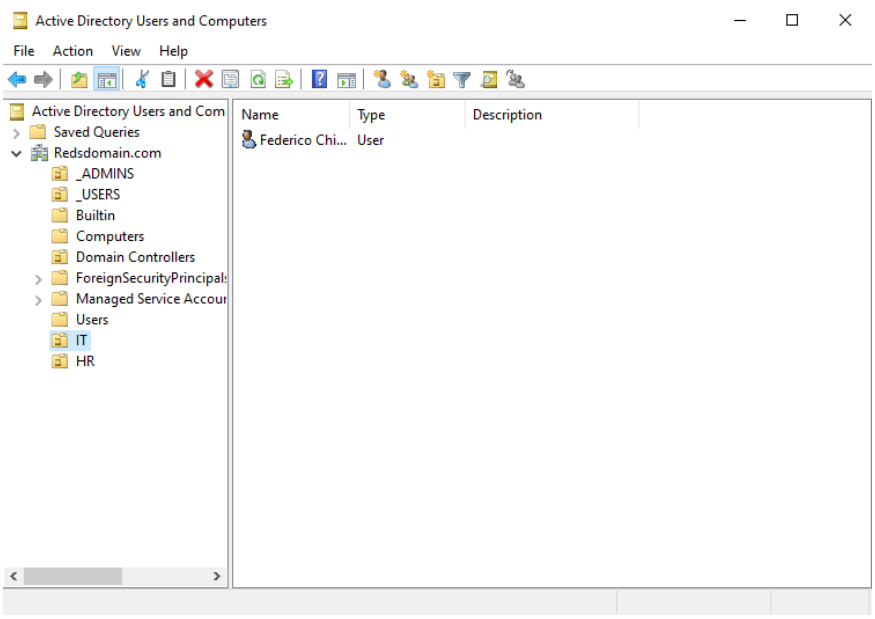
- Follow the same steps just as the Target-PC

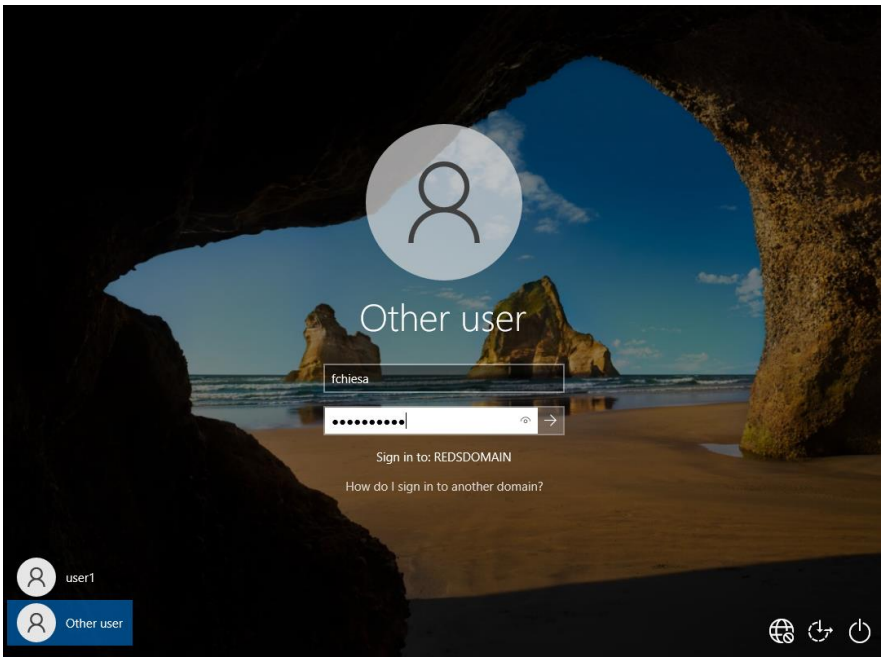
- 

- We now have Telemetry from two hosts.

I already have Active Directory set up with which i joined my Target-PC to my Domain, so I only created an extra Organisational Unit (IT) and one new user for the sake of this lab.

- 

- 
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
Target-PC
Full computer name:
Target-PC
Member of
Domain:
Redsdomain.com
Workgroup:
K
OK
Cancel
OK
Cancel
Apply
Computer Name/Domain Changes
Welcome to the Redsdomain.com domain.
OK
- 
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Redsdomain.com
_ADMINS
_USERS
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
IT
HR
Name
Type
Description
Federico Chi...
User

- 

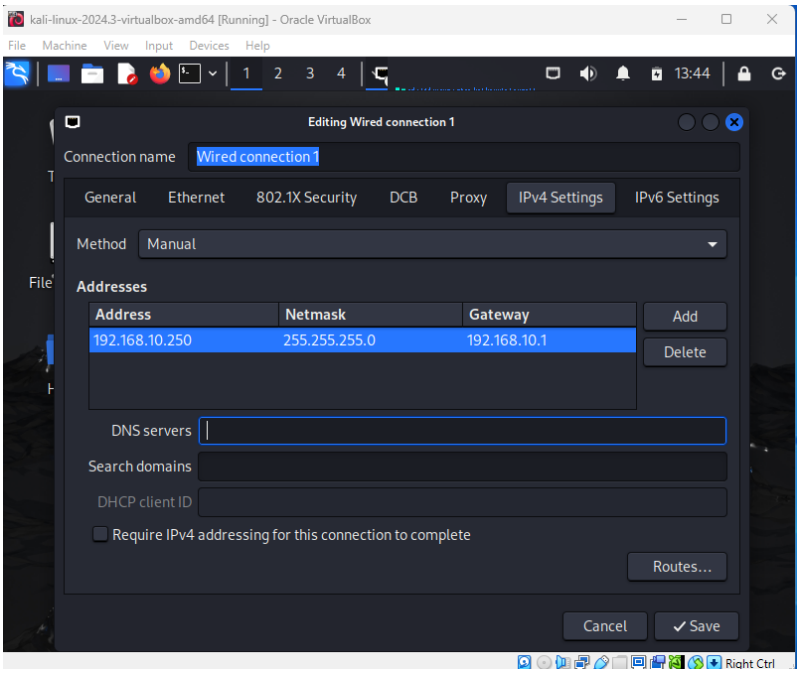
Part 5

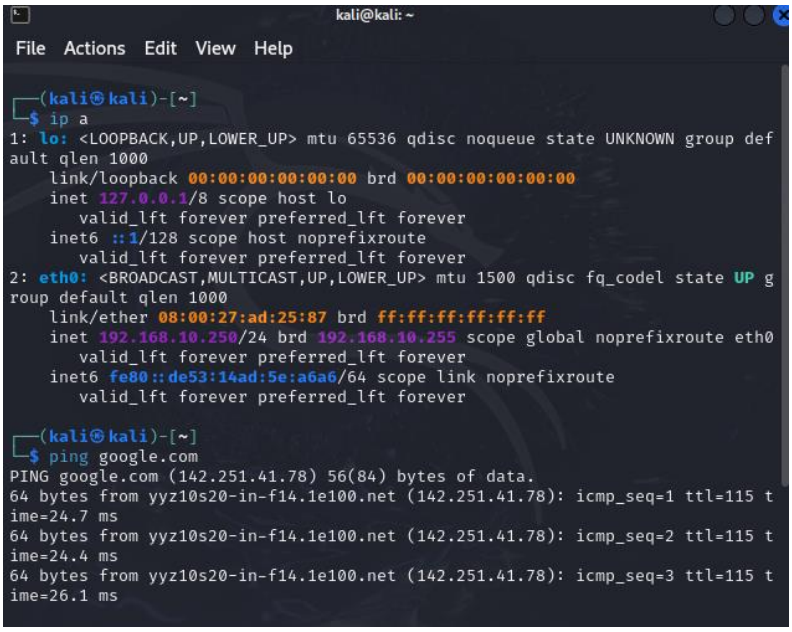
Objectives

- Use Kali Linux to perform attack with crowbar
- View telemetry via splunk
- Install and setup Atomic RedTeam (ART) on Target-PC
- Run tests with ART

On Kali Linux

- Login with default credentials
- Set a static IP for kali as per network design
- Click on the ethernet sign and navigate to IPv4 settings
- Set a static IP
- Disconnect and connect ethernet again to take effect

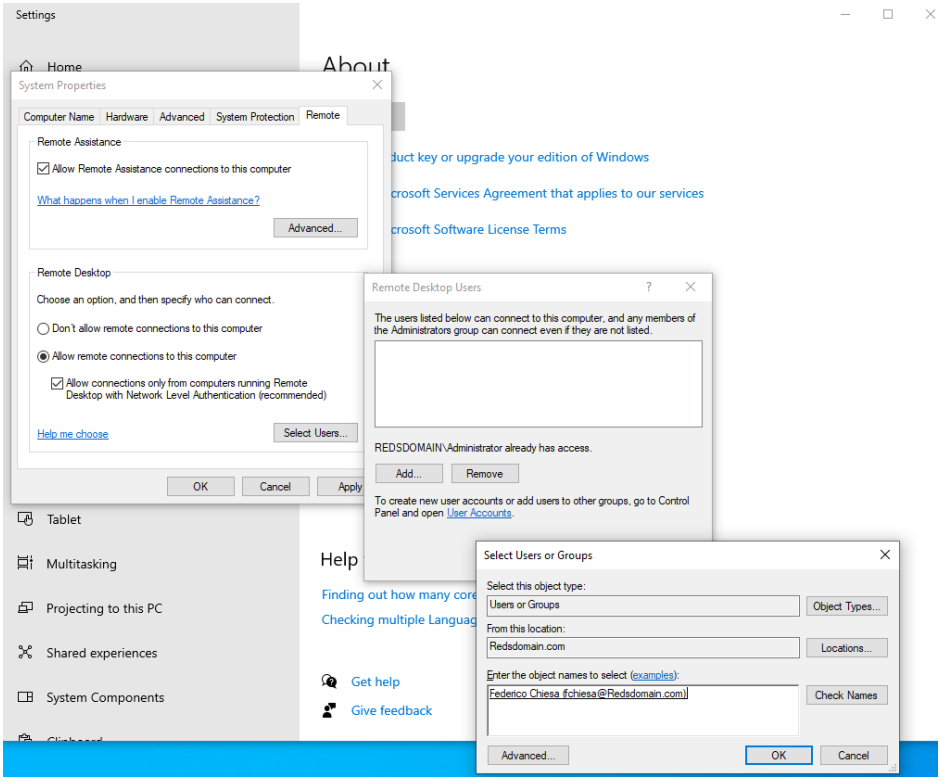
- 

- 

- Update and upgrade repositories ‘sudo apt-get update && sudo apt-get upgrade -y'
- Create new directory ‘ad-project’ on Desktop ‘mkdir ad-project'
- Now install Crowbar; ‘sudo apt-get install -y crowbar’
- We use crowbar to perform brute-force attacks on our Target-PC and Domain controller.
- To utilize the popular wordlist ‘rockyou.txt’ change directory to where its located, ‘cd /usr/share/wordlists’
- Run ‘sudo gunzip rockyou.txt.gz’

- Copy the rockyou.txt into our ad-project directory ‘cp rockyou.txt ~/desktop/ad-project’
-
```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir ad-project

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt-get install -y crowbar
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
```
-
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst        wfuzz
dirb        fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst      wfuzz
dirb        fasttrack.txt  legion      rockyou.txt   wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$
```
-
- Run ‘head -n 30 rockyou.txt > passwords.txt’ To copy the first 30 lines of the file into a new file that we use.
- Run ‘nano passwords.txt’ and put in the actual password.
-
```
kali@kali: ~/Desktop/ad-project
File  Actions  Edit  View  Help
  GNU nano 8.3                    passwords.txt *
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
[redacted]
^G Help       ^O Write Out  ^F Where Is   ^K Cut        ^T Execute
^X Exit       ^R Read File  ^\ Replace     ^U Paste      ^J Justify
```

Enable Remote connection on Target-PC

- Goto PC settings, then advanced system settings, log in with the administrator credentials
- Click on the remote tab
- Select ‘allow remote connections to the computer’
- Select users, add users
- 

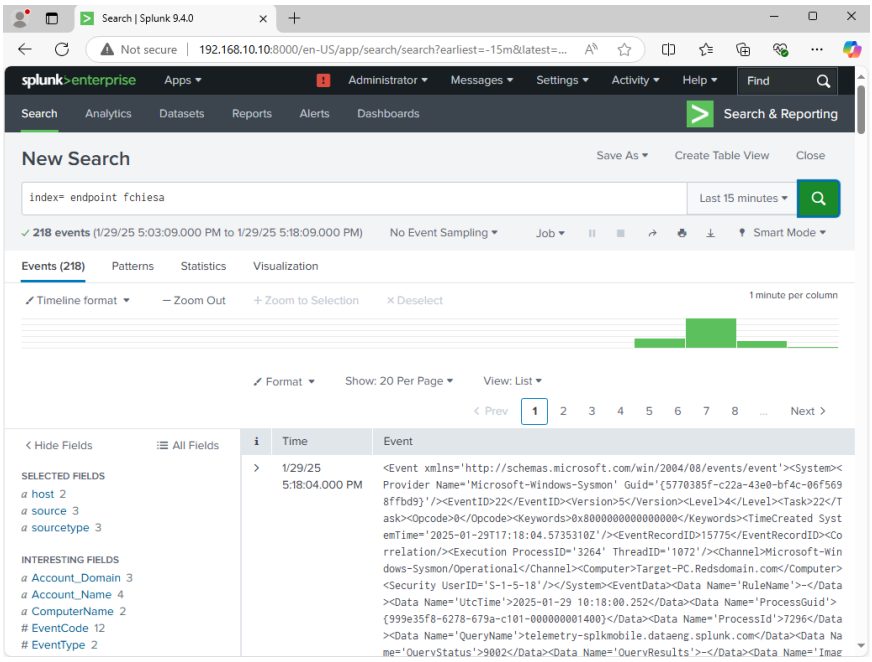
Back to Kali

- Run ‘crowbar -h’ to view help menu.
- Now to perform attack
- Run ‘crowbar -b rdp –u fchiesa –C passwords.txt -s 192.168.10.100/32’
    - -b to specify the service for crowbar (rdp)
    - -u to specify the user account
    - -C to specify the passwords file
    - -s to indicate source IP
    - /32 because we only want to taget only one IP and not other IPs on the network

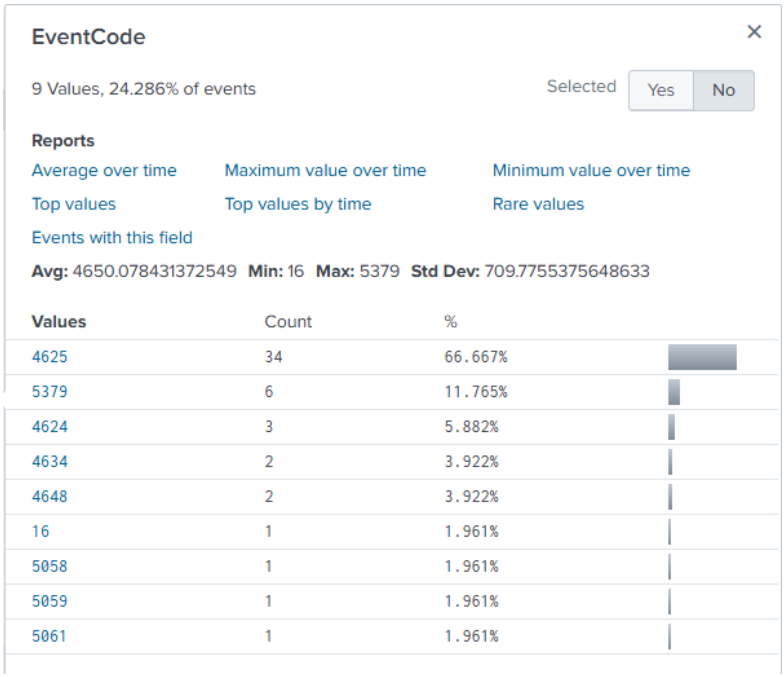
- 

- Success.

Viewing Telemetry on splunk

- On Plunk portal, we head over to ‘search & reporting’
- Put in search parameters ‘index = endpoint’
- Since attack just took place we can filter down the timeframe to last 15 minutes
- We can also filter more by putting the username that was targeted for the attack
- 

- Notice a few events code that we can pay attention to understand their meanings
- We see event ID 4625 occur multiple times, his eventID represents failed logon attempts which have occured during the brute-force attack
- Then we see 4624, this eventID represents successful log on

- 

EventCode

9 Values, 24.286% of events

Selected: Yes / No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

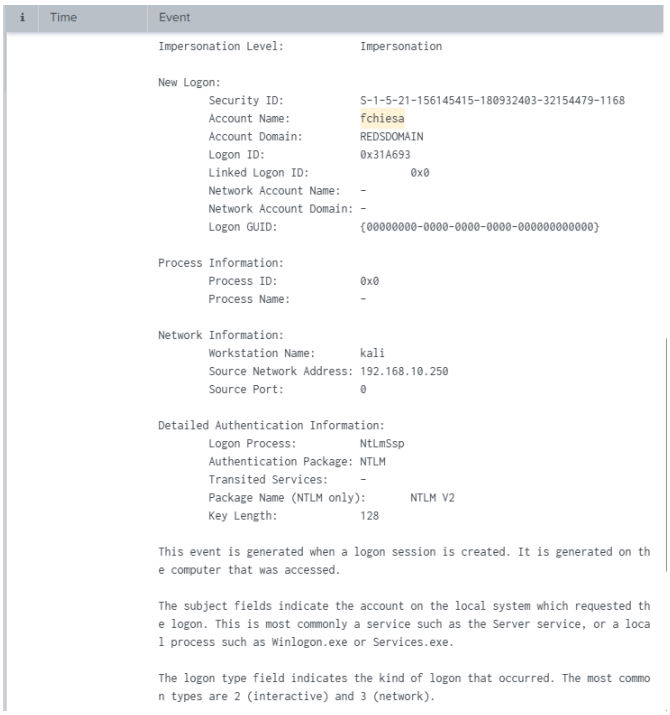
Avg: 4650.078431372549 **Min:** 16 **Max:** 5379 **Std Dev:** 709.7755375648633

Values	Count	%
4625	34	66.667%
5379	6	11.765%
4624	3	5.882%
4634	2	3.922%
4648	2	3.922%
16	1	1.961%
5058	1	1.961%
5059	1	1.961%
5061	1	1.961%

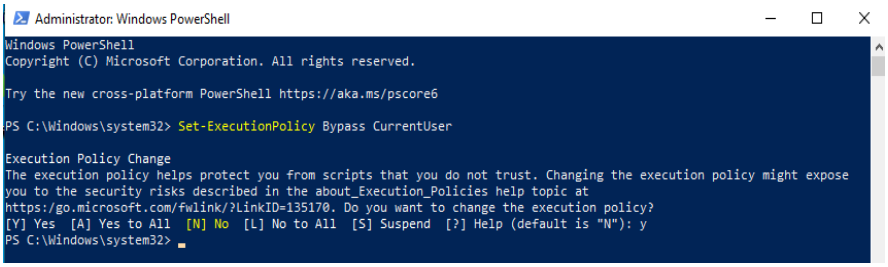
- 

i	Time	Event
>	1/29/25 5:15:53.000 PM	01/29/2025 09:15:53 AM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: fchiesa Account Domain: REDSDOMAIN Show all 61 lines host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
>	1/29/25 5:15:21.000 PM	01/29/2025 09:15:21 AM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: fchiesa Account Domain: Show all 61 lines host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
>	1/29/25 5:15:21.000 PM	01/29/2025 09:15:21 AM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: fchiesa Account Domain: Show all 61 lines host = TARGET-PC source = WinEventLog:Security sourcetype = WinEventLog:Security
>	1/29/25 5:15:20.000 PM	01/29/2025 09:15:20 AM ... 20 lines omitted ... Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: fchiesa

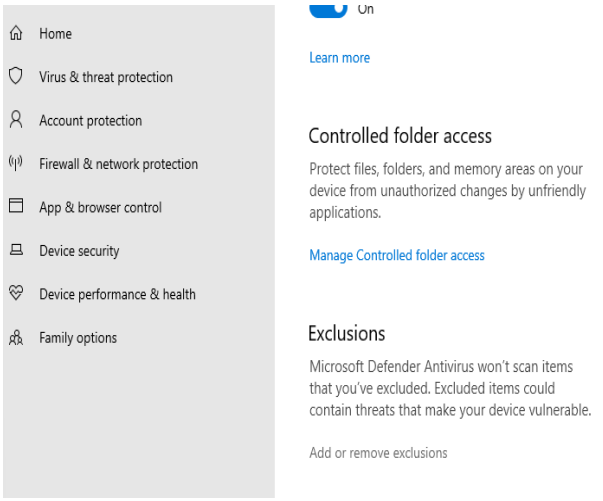
- Further review into the successful logon event, we can see the workstation name and IP and be able to identify when an attack has occured.

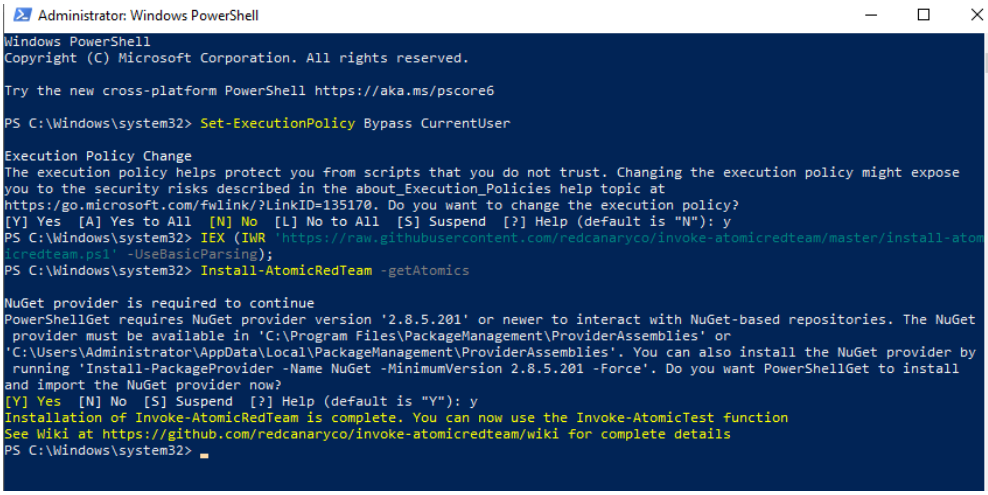
- 

Download AomicRedTeam on Target-PC

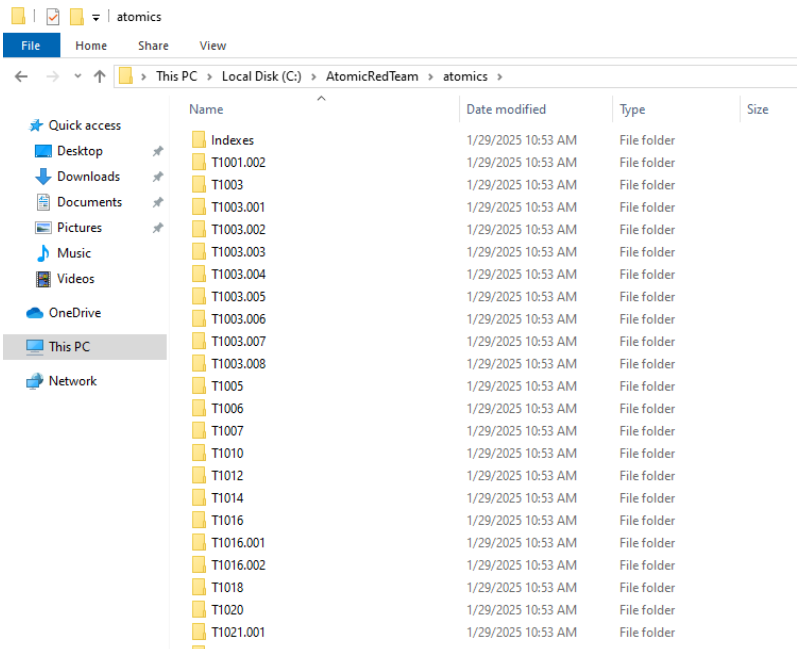
- Open powershell as administrator
- Run ‘set-executionpolicy Bypass CurrentUser’
- 

- Now, set an exclusion for the entire C drive as microsoft defender will detect and remove some of the files from ART
- Click on the up arrow on the bottom right of the target-pc to enter windows security
- 

- Click on virus & threat protection, manage settings
- Under exclusions, Add an exclusion, select folder
- Under ‘This Pc’, select the ‘C drive’
- 

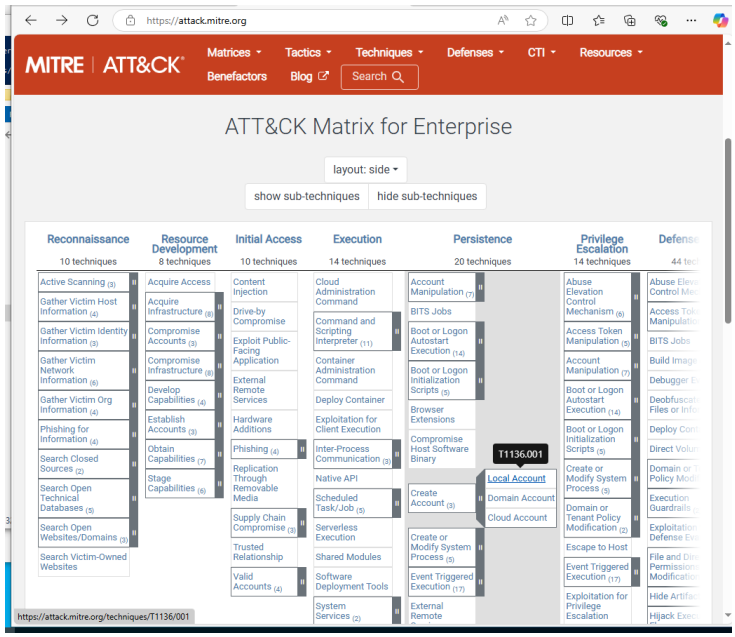
- Now we can install ART
- 

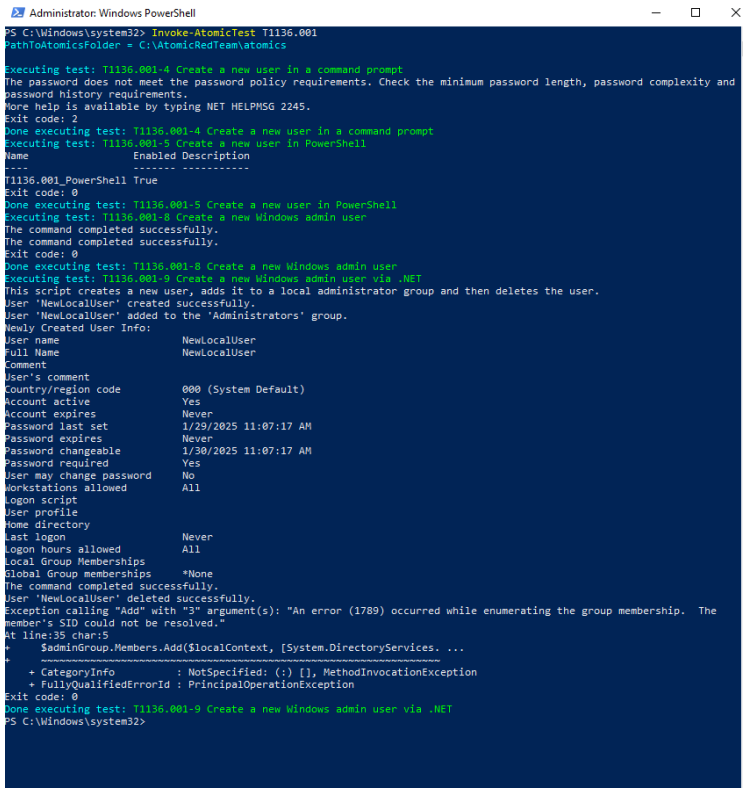
- Head over to C drive, Enter the ART directory, enter Atomics
- We see a bunch of techniques IDs which map back to the MITRE ATT&CK framework.



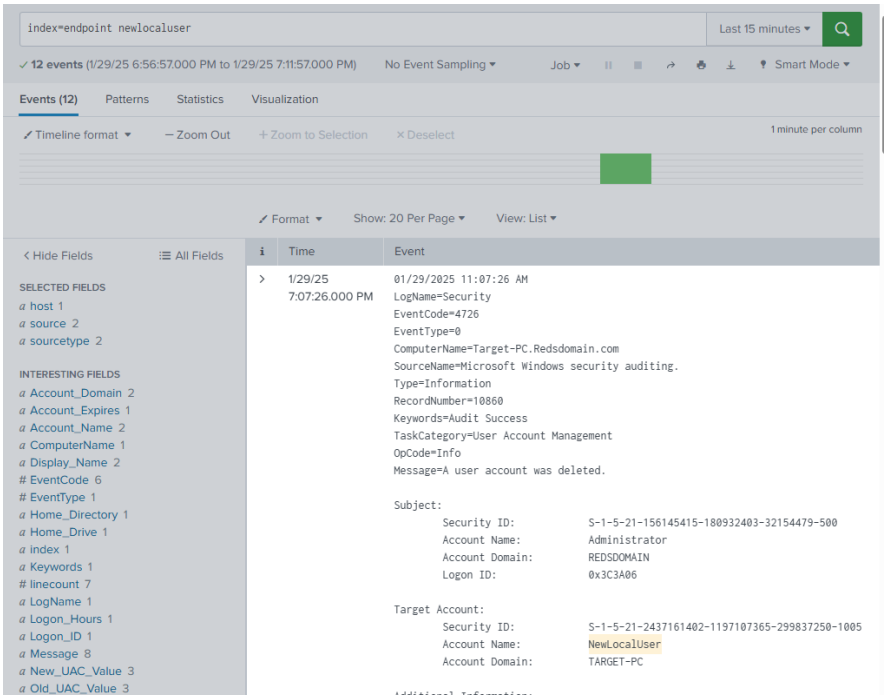
Run tests with AtomicRedTeam

- Head over to the Mitre ATT&CK framework to get a technique to test.
- In this case, we use the ‘create account’ technique under the ‘Persistence’ Tactic.
- There are 3 sub-techniques under this, we utilize the Local account subtechnique for this test . ID: T1136001
-
- Head back to powershell and run ‘Invoke-Atomictest T1136.001’

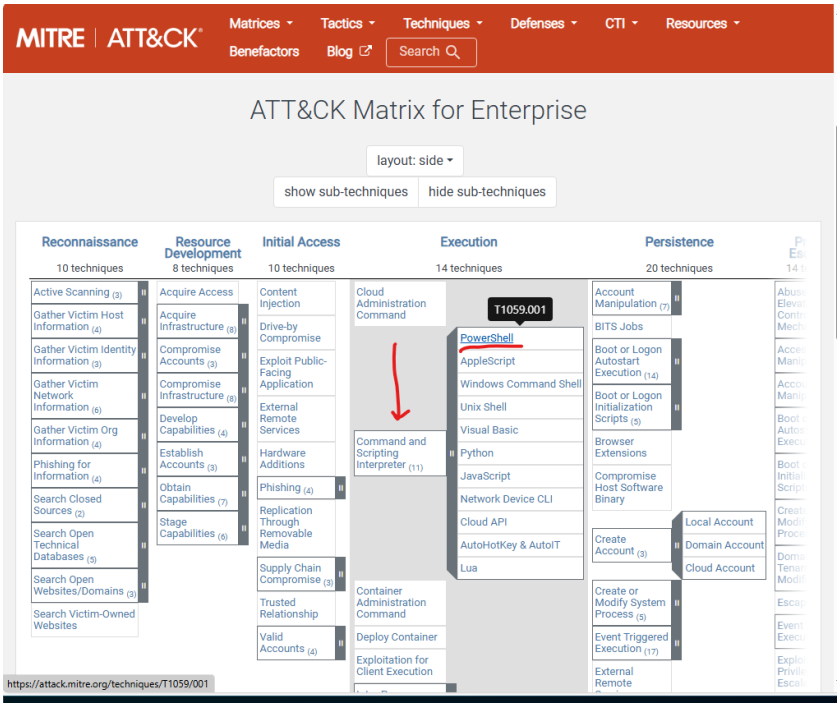
- 

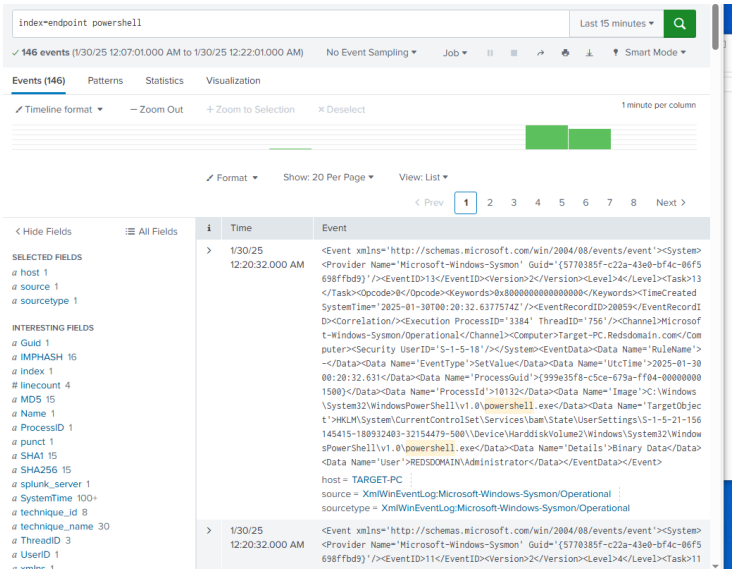
-
- 

- Now that the test is complete, we over to splunk to review telemetry
-



- I repeated this test for another technique that involved a powershell command just for extra practice.




index=endpoint powershell
Last 15 minutes
146 events (1/30/25 12:07:01.000 AM to 1/30/25 12:22:01.000 AM)
No Event Sampling
Job
Smart Mode
Events (146)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Guid 1
a IMPHASH 16
a index 1
linecount 4
a MD5 15
a Name 1
a ProcessID 1
a punct 1
a SHA1 15
a SHA256 15
a splunk_server 1
a SystemTime 100+
a technique_id 8
a technique_name 30
a ThreadID 3
a UserID 1
Time
Event
1/30/25 12:20:32.000 AM
host = TARGET-PC
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
1/30/25 12:20:32.000 AM