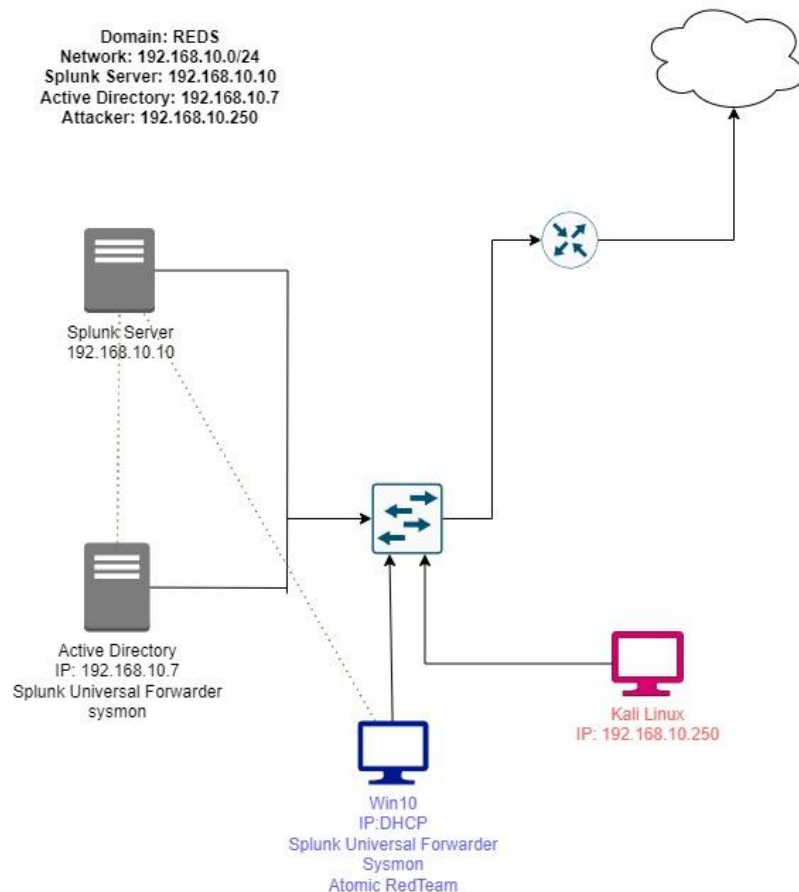


# Active Directory Project (HOMELAB) -Part1

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

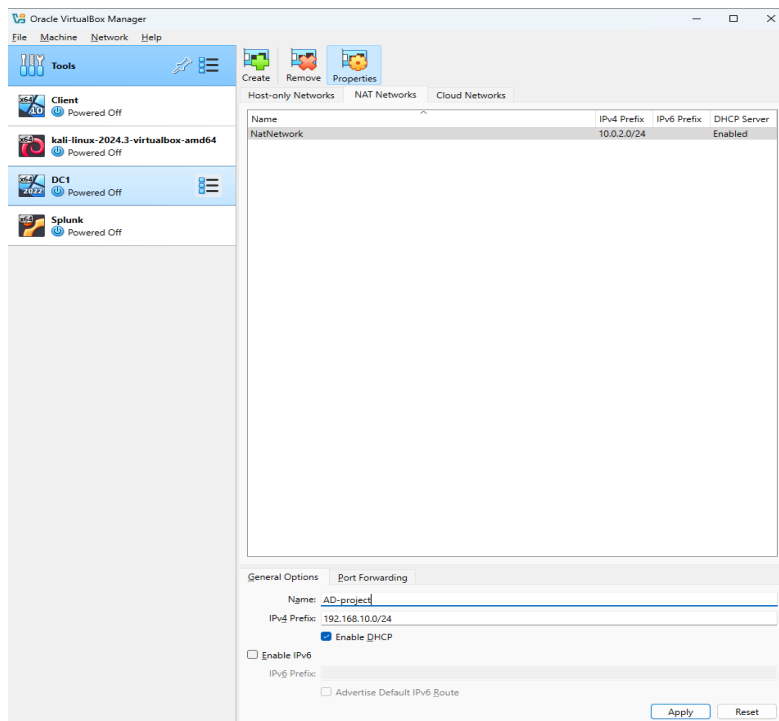
- Configure the homelab Network to be on the same Network according to our diagram above
- Setup splunk server on Ubuntu
- Install and configure Splunk and Sysmon onto our windows target machine and windows server to collect telemetry and send logs to splunk server

## Installing VMs

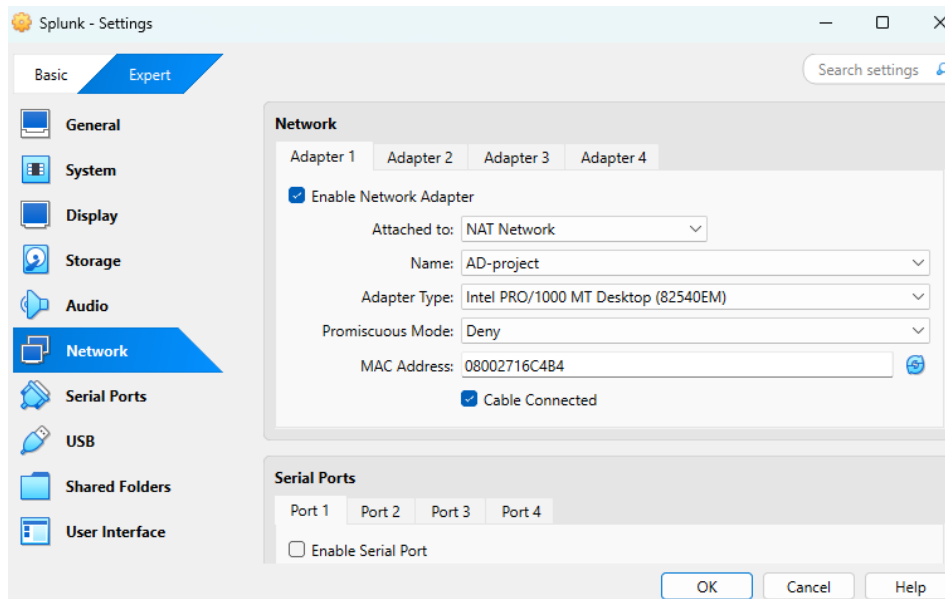
Because I had already installed windows10, windows Server and kali for a previous project, I only had to install Ubuntu server this time.

## 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

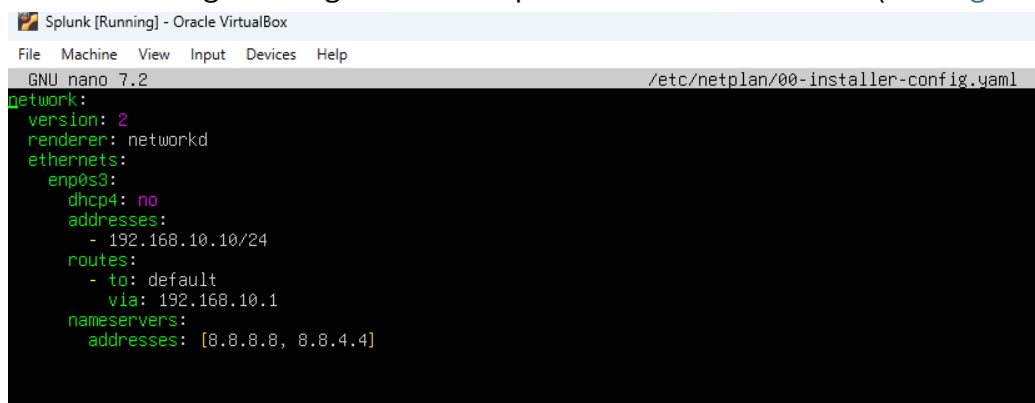


- Enable and hit Apply
- Now goto each of the VMs to configure the network settings
- Change to NatNetwork under Adapter settings



## 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](#) )



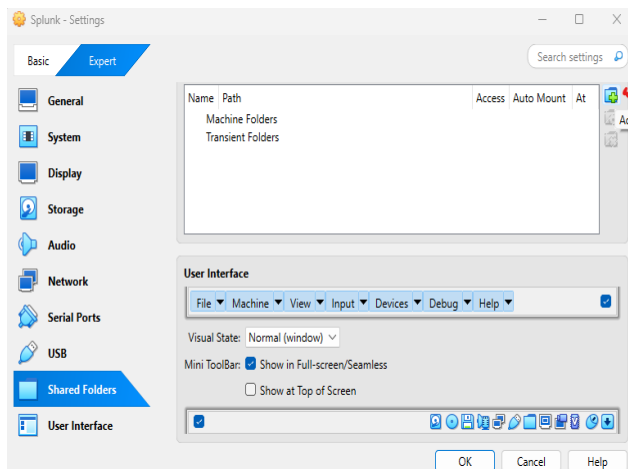
- Save the file
- Run 'sudo netplan apply' for the changes to take effect
- Run ip a to confirm changes

```
Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help

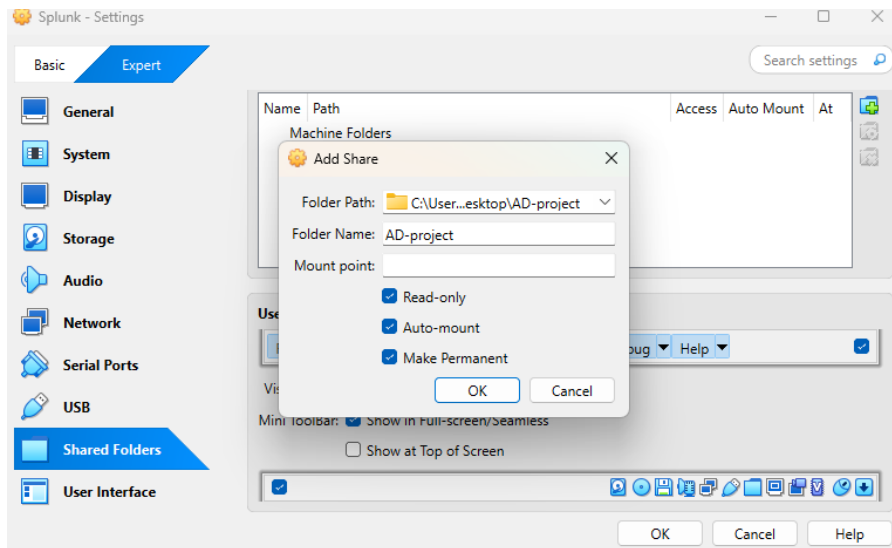
rokita@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:16:c4:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe16:c4b4/64 scope Link
        valid_lft forever preferred_lft forever
rokita@splunk:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
 64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=25.7 ms
 64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=36.1 ms
 64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=27.8 ms
 64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=34.6 ms

--- 8.8.8.8 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3005ms
 rtt min/avg/max/mdev = 25.600/31.015/36.058/4.393 ms
rokita@splunk:~$
```

- 
- 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'

```
Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rokita@splunk:~$ sudo adduser rokita vboxsf
[sudo] password for rokita:
info: Adding user `rokita' to group `vboxsf' ...
rokita@splunk:~$
```

- 
- 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/'

```
Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rokita@splunk:~$ sudo adduser rokita vboxsf
[sudo] password for rokita:
info: Adding user `rokita' to group `vboxsf' ...
rokita@splunk:~$ mkdir share
rokita@splunk:~$ ls
share snap
rokita@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 AD-project share/
rokita@splunk:~$ ls
share snap
rokita@splunk:~$
```

- 
- Change directory into the share directory and install splunk

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

```

Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rokita@splunk:~$ sudo adduser rokita vboxsf
(sudo) password for rokita:
info: Adding user `rokita' to group `vboxsf' ...
rokita@splunk:~$ mkdir share
rokita@splunk:~$ ls
share snap
rokita@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 AD-project share/
rokita@splunk:~$ ls
snap
rokita@splunk:~$ cd share
rokita@splunk:~/share$ ls -la
[ 890.794726] UBSAN: array-index-out-of-bounds in /build/linux-uoESLx/linux-6.8.0/drivers/virt/vboxguest/vboxguest_utils.c:367:20
[ 890.794789] index 1 is out of range for type '___u64 [1]'
total 898913
drwxrwxrwx 1 rokita rokita      4096 Jan 24 17:15 .
drwxr-x--- 7 rokita rokita      4096 Jan 24 17:07 ..
-rwxrwxrwx 1 rokita rokita    64867 Jan 24 17:00 addsharedfolder2.png
-rwxrwxrwx 1 rokita rokita    45207 Jan 24 16:55 addsharedfolder.png
-rwxrwxrwx 1 rokita rokita     7842 Jan 24 17:04 adduservboxsf.png
-rwxrwxrwx 1 rokita rokita       206 Jan 24 17:05 desktop.ini
-rwxrwxrwx 1 rokita rokita    12346 Jan 24 17:15 mountsharedfolder.png
-rwxrwxrwx 1 rokita rokita    48496 Jan 22 22:31 NatNetwork2.png
-rwxrwxrwx 1 rokita rokita    42600 Jan 22 22:27 NatNetwork.png
-rwxrwxrwx 1 rokita rokita    58623 Jan 21 19:47 'Screenshot 2025-01-21 144746.png'
-rwxrwxrwx 1 rokita rokita 920120936 Jan 24 16:36 splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
-rwxrwxrwx 1 rokita rokita    16923 Jan 23 21:08 splunknetplan.png
-rwxrwxrwx 1 rokita rokita    27678 Jan 24 16:10 SPLUNKnewIP.png
-rwxrwxrwx 1 rokita rokita    10963 Jan 24 16:12 splunkYAML.png
rokita@splunk:~/share$ ls -la
total 898565
drwxrwxrwx 1 rokita rokita      4096 Jan 24 17:18 .
drwxr-x--- 7 rokita rokita      4096 Jan 24 17:07 ..
-rwxrwxrwx 1 rokita rokita       206 Jan 24 17:05 desktop.ini
-rwxrwxrwx 1 rokita rokita 920120936 Jan 24 16:36 splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
rokita@splunk:~/share$ sudo dpkg -i splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 99196 files and directories currently installed.)
Preparing to unpack splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.0) ...
Setting up splunk (9.4.0) ...
complete
rokita@splunk:~/share$ _

```

- 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

```
Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rokita@splunk:/opt/splunk$ ls -la
total 5256
drwxr-xr-x 11 splunk splunk 4096 Jan 24 17:27 .
drwxr-xr-x 3 root root 4096 Jan 24 17:21 ..
drwxr-xr-x 4 splunk splunk 12288 Jan 24 17:27 bin
-r--r--r-- 1 splunk splunk 57 Dec 11 01:47 copyright.txt
drwxr-xr-x 17 splunk splunk 4096 Jan 24 17:27 etc
-rw-r--r-- 1 splunk splunk 426 Jan 24 17:27 ftr
drwxr-xr-x 4 splunk splunk 4096 Jan 24 17:26 include
drwxr-xr-x 10 splunk splunk 4096 Jan 24 17:27 lib
-r--r--r-- 1 splunk splunk 59904 Dec 11 01:47 license-eula.txt
-r--r--r-- 1 splunk splunk 1090 Dec 7 06:06 LICENSE.txt
drwxr-xr-x 3 splunk splunk 4096 Jan 24 17:26 openssl
drwxr-xr-x 4 splunk splunk 4096 Jan 24 17:25 opt
drwxr-xr-x 2 splunk splunk 4096 Jan 24 17:26 quarantined_files
-r--r--r-- 1 splunk splunk 522 Dec 11 01:51 README-splunk.txt
drwxr-xr-x 5 splunk splunk 4096 Jan 24 17:26 share
-r--r--r-- 1 splunk splunk 5247185 Dec 11 02:18 splunk-9.4.0-6b4ebe426ca6-linux-amd64-manifest
drwxr-xr-x 2 splunk splunk 4096 Jan 24 17:27 swidtag
rokita@splunk:/opt/splunk$ sudo -u splunk bash
[sudo] password for rokita:
splunk@splunk:~$ cd bin
splunk@splunk:~/bin$ ./splunk start
```

- 
- 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'
- 

```
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation;
preter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Do

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

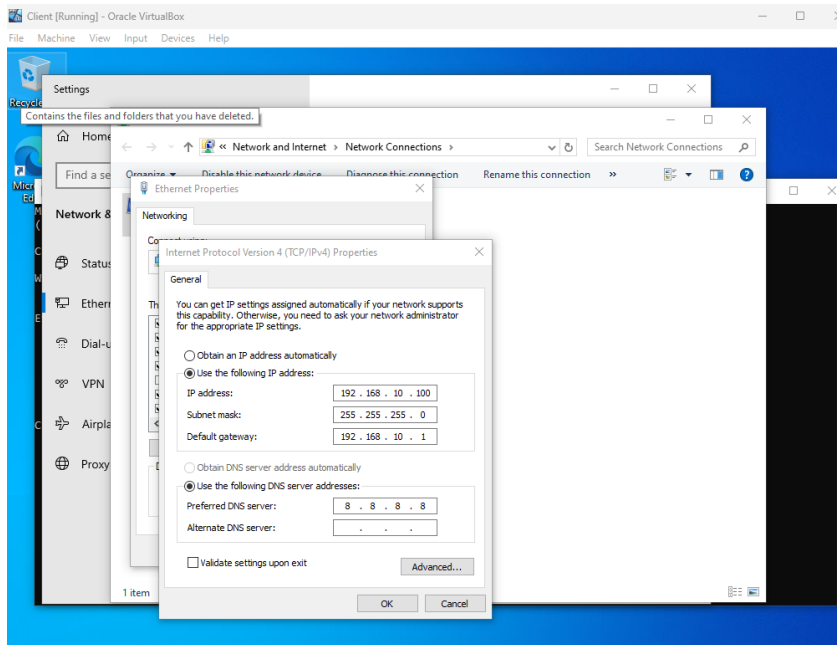
The Splunk web interface is at http://splunk:8000

splunk@splunk:~/bin$ exit
exit
rokita@splunk:/opt/splunk$ cd bin
rokita@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
rokita@splunk:/opt/splunk/bin$
```

## Part2

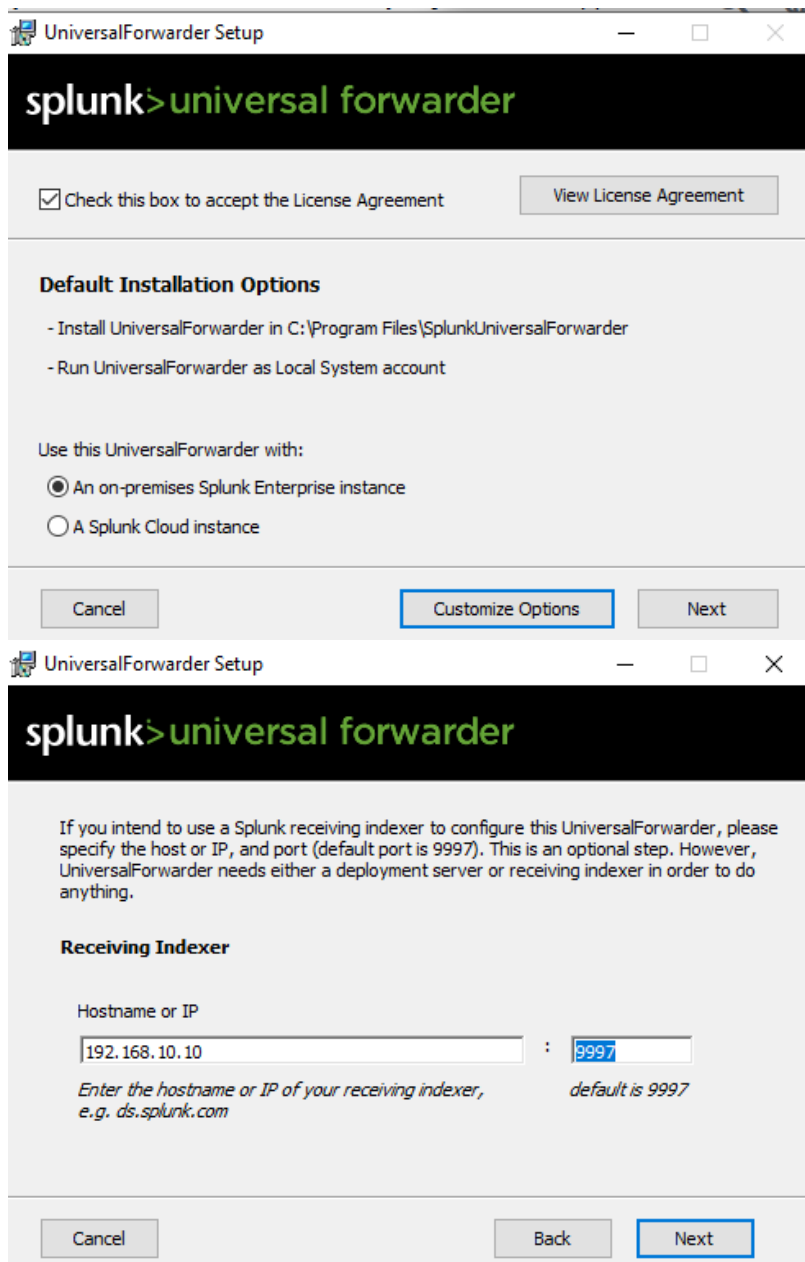
Now we install and configure Splunk Universal Forwarder and Sysmon on both our Target-PC and Windows Server

- 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)

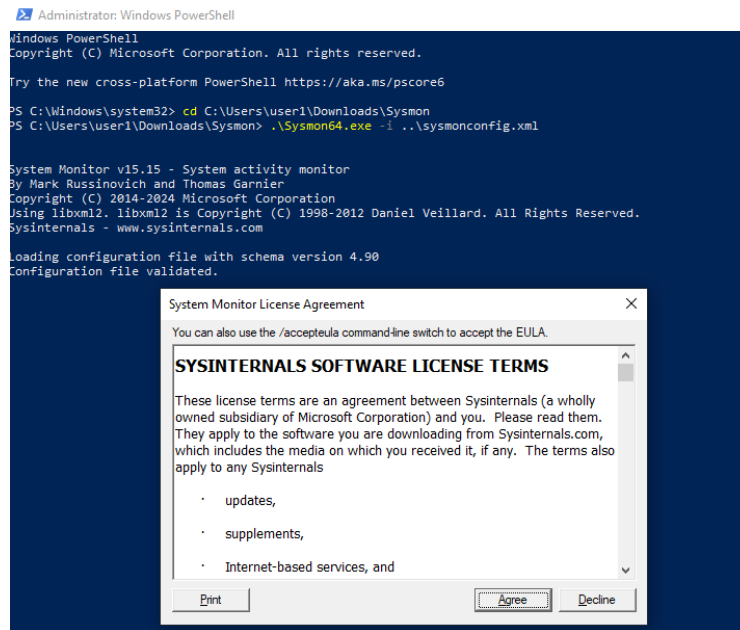




## Download Sysmon by Sysinternals

- 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





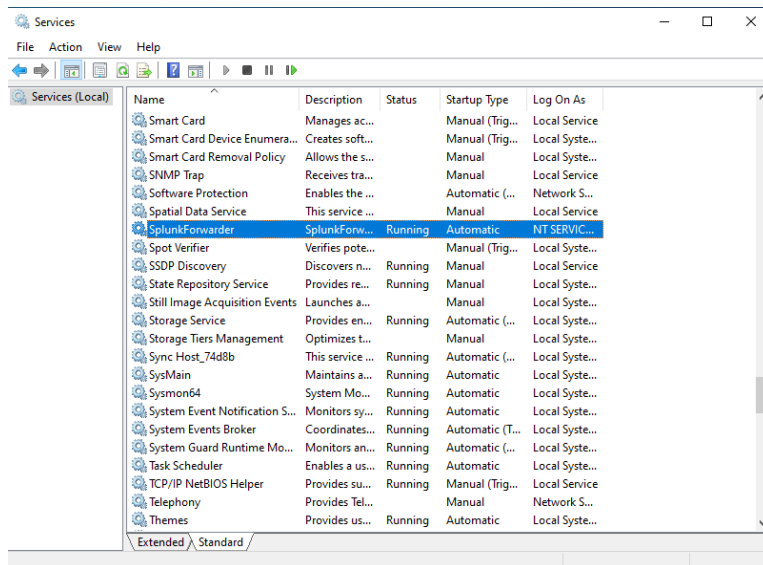
## Part 3

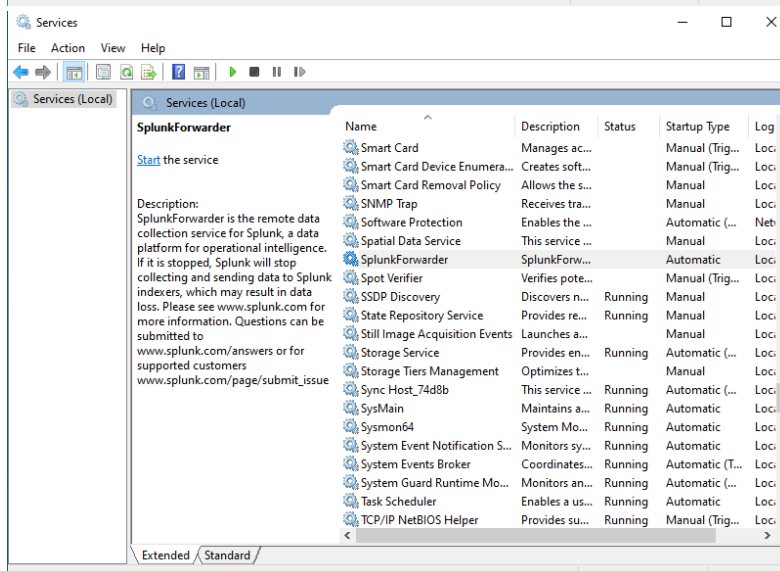
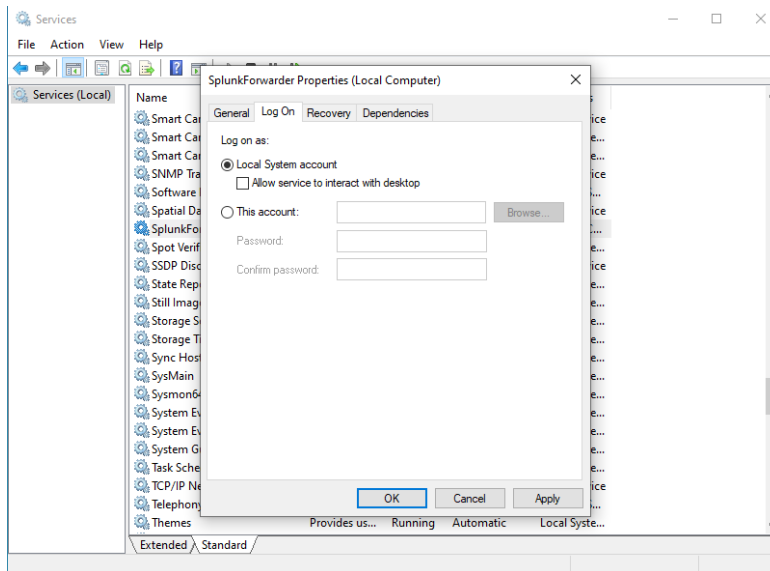
### Splunk Configuration

- 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.

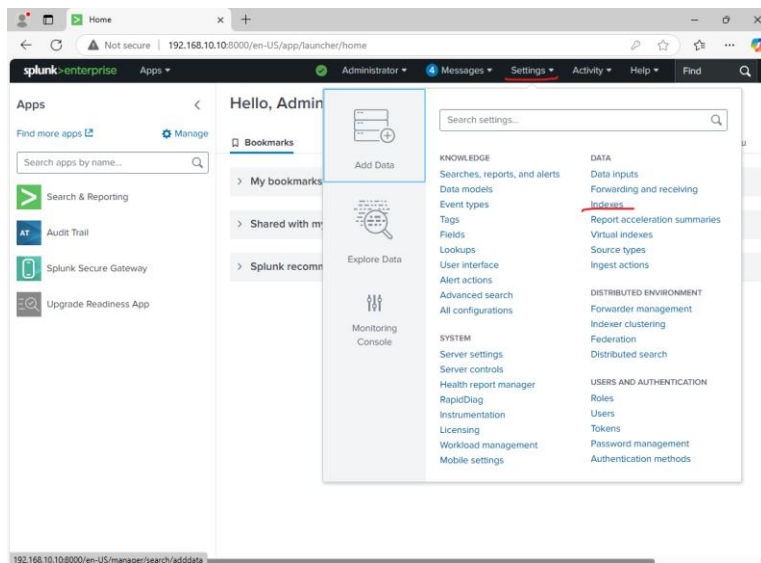
## Restart SUF service

- 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 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.

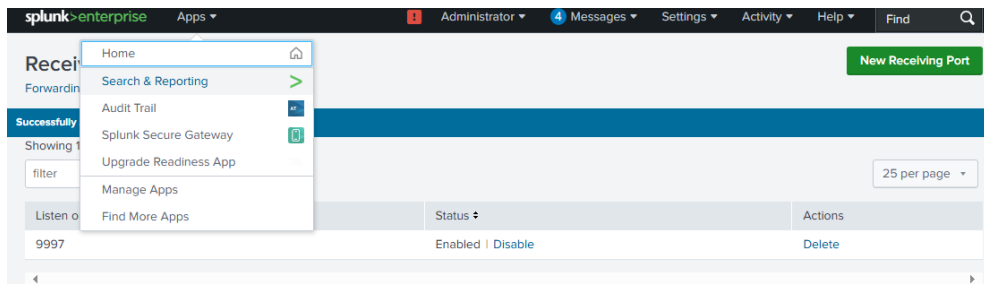


The 'New Index' configuration window is shown. It contains the following settings:

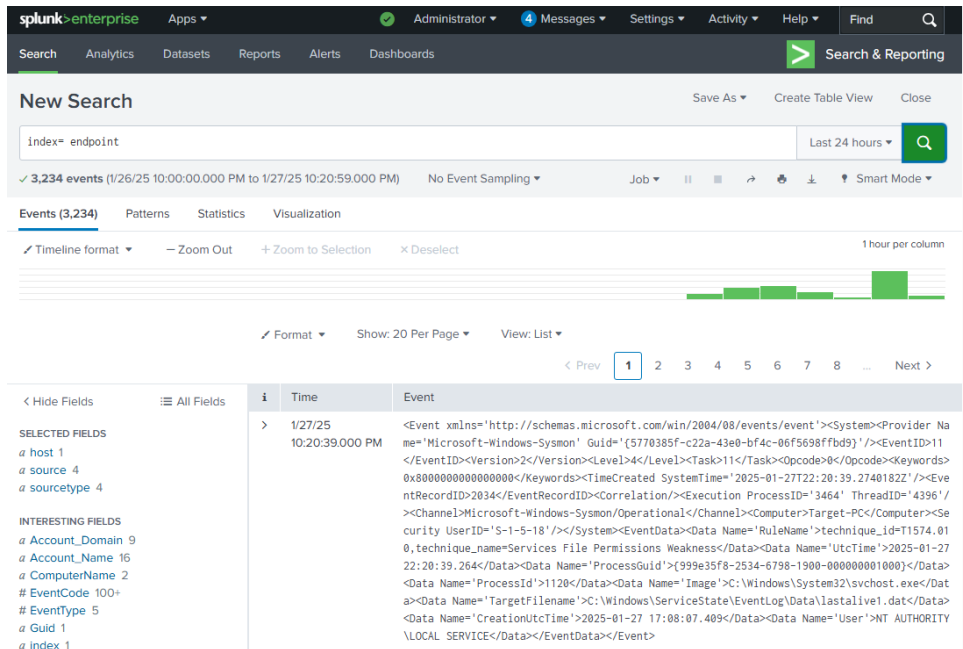
- Index Name:** endpoint
- Index Data Type:** Events (selected), Metrics
- Home Path:** optional
- Cold Path:** optional
- Thawed Path:** optional
- Data Integrity Check:** Enable (selected), Disable
- Max Size of Entire Index:** 500 GB
- Max Size of Hot/Warm/Cold Bucket:** auto GB

At the bottom right, there are 'Save' and 'Cancel' buttons.

- 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

DC1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Search | Splunk 9.4.0 | Thank You Splunk Universe | sysmon config olaf - Search | +

Not secure | 192.168.10.10:8000/en-US/app/search/search?q=s... | Search & Report

splunk>enterprise Apps Admin... Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

New Search Save As Create Table View

index= endpoint Last 24 hours

✓ 5,569 events (1/27/25 4:00:00.000 PM to 1/28/25 4:10:41.000 PM) Job || Smart Monitor

No Event Sampling

Events (5,569) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per

host

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
TARGET-PC	3,987	71.593%
DC1	1,582	28.407%

1/28/25 01/28/2025 08:10:11 AM  
4:10:11.000 PM LogName=Security  
EventCode=4624  
EventType=0  
ComputerName=DC1.Redsdomain.com  
Show all 70 lines

< Hide Fields All Fields

SELECTED FIELDS

- host 2
- source 4
- sourcetype 4

INTERESTING FIELDS

- Account\_Domain 10
- Account\_Name 22
- ComputerName 3
- EventCode 100+
- EventType 5
- Guid 1
- index 1
- Keywords 9
- Process 22

- 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.

Server Manager Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

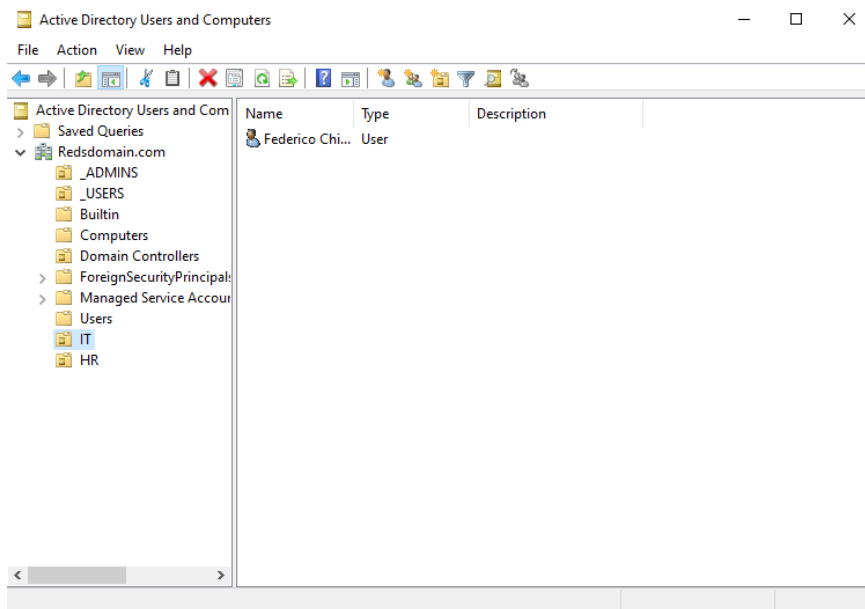
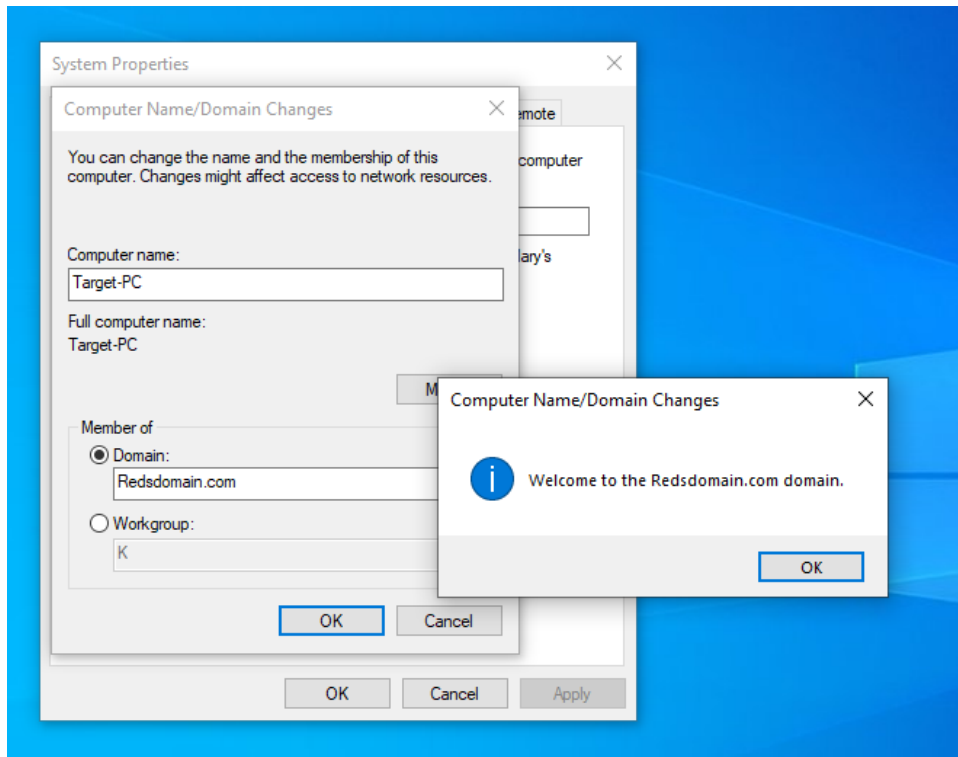
5 Connect this server to cloud services

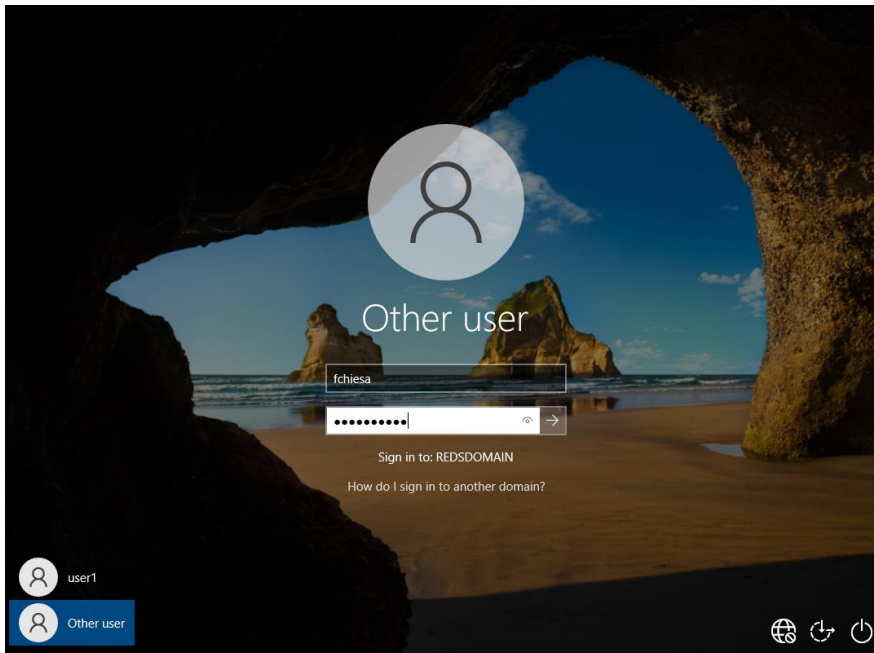
ROLES AND SERVER GROUPS

Roles: 6 | Server groups: 1 | Servers total: 1

Role/Server Group	Count	Management	Events	Services	Performance	BPA results
AD DS	1	Manageability	Events	Services	Performance	BPA results
DHCP	1	Manageability	Events	Services	Performance	BPA results
DNS	1	Manageability	Events	Services	Performance	BPA results
File and Storage Services	1	Manageability	Events	Services	Performance	BPA results
IIS	1	Manageability	Events	Services	Performance	BPA results
Remote Access	1	Manageability	Events	Services	Performance	BPA results
Local Server	1	Manageability	Events	Services	Performance	
All Servers	1	Manageability	Events	Services	Performance	







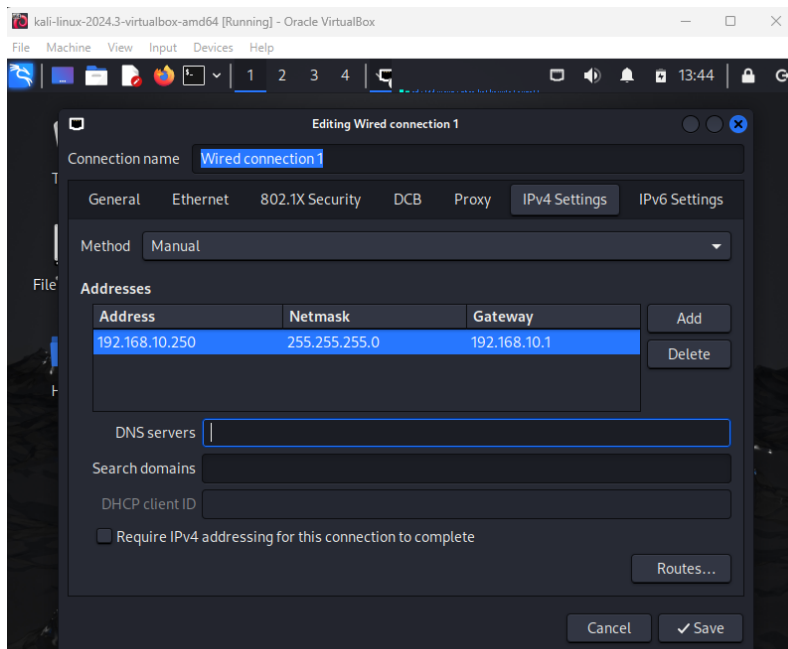
## Part 5

### 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



```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.250/24 brd 192.168.10.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::de53:14ad:5e:a6a6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
└─$ ping google.com
PING google.com (142.251.41.78) 56(84) bytes of data.
64 bytes from yyz10s20-in-f14.1e100.net (142.251.41.78): icmp_seq=1 ttl=115 t
ime=24.7 ms
64 bytes from yyz10s20-in-f14.1e100.net (142.251.41.78): icmp_seq=2 ttl=115 t
ime=24.4 ms
64 bytes from yyz10s20-in-f14.1e100.net (142.251.41.78): icmp_seq=3 ttl=115 t
ime=26.1 ms

```

- 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.

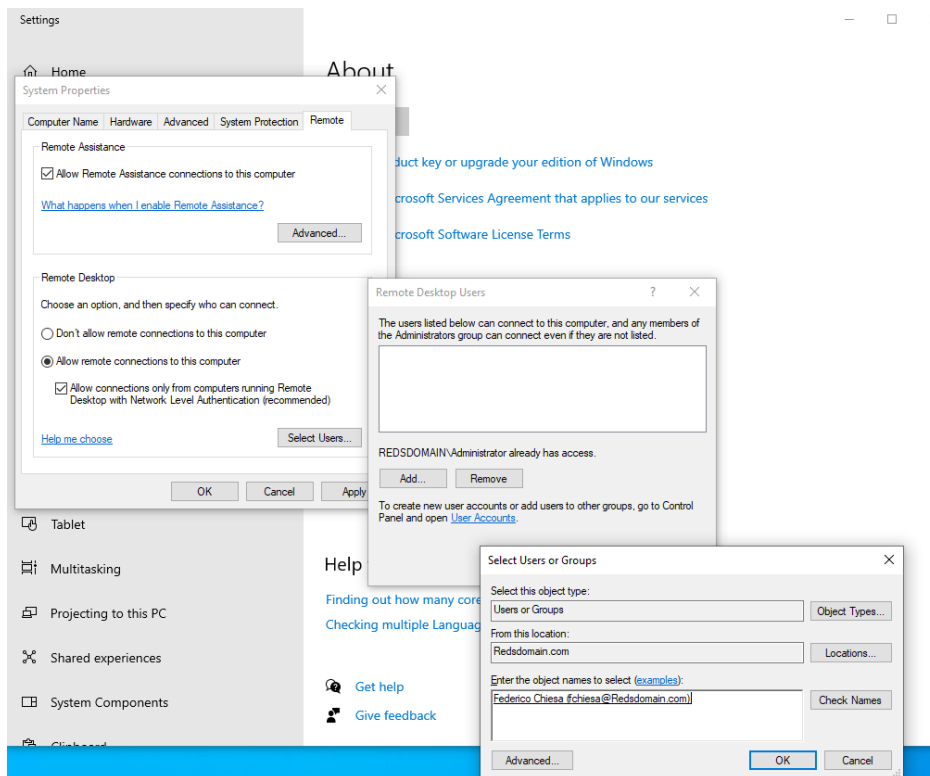
- Run 'nano passwords.txt' and put in the actual password.

```
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
P
```

-

# 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

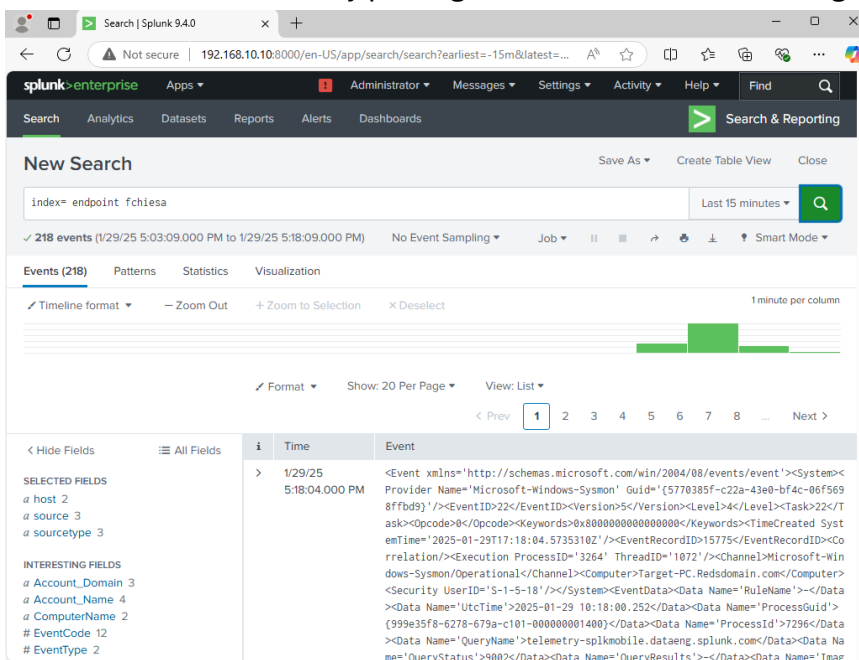
- Run 'crowbar -h' to view help menu.
- Now to perform attack
- Run 'crowbar -b rdp -u fchiesa -C passwords.txt -s 192.168.10.100/32'
  - -b to specify the service for crowbar (rdp)
  - -u to specify the user account
  - -C to specify the passwords file
  - -s to indicate source IP
  - /32 because we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

```
(kali@kali)-[~/Desktop/ad-project]
$ crowbar -b rdp -u fchiesa -C passwords.txt -s 192.168.10.100/32
2025-01-28 16:49:27 START
2025-01-28 16:49:27 Crowbar v0.4.2
2025-01-28 16:49:27 Trying 192.168.10.100:3389
2025-01-28 16:49:41 RDP-SUCCESS : 192.168.10.100:3389 - fchiesa:P[REDACTED]
2025-01-28 16:49:41 STOP
```

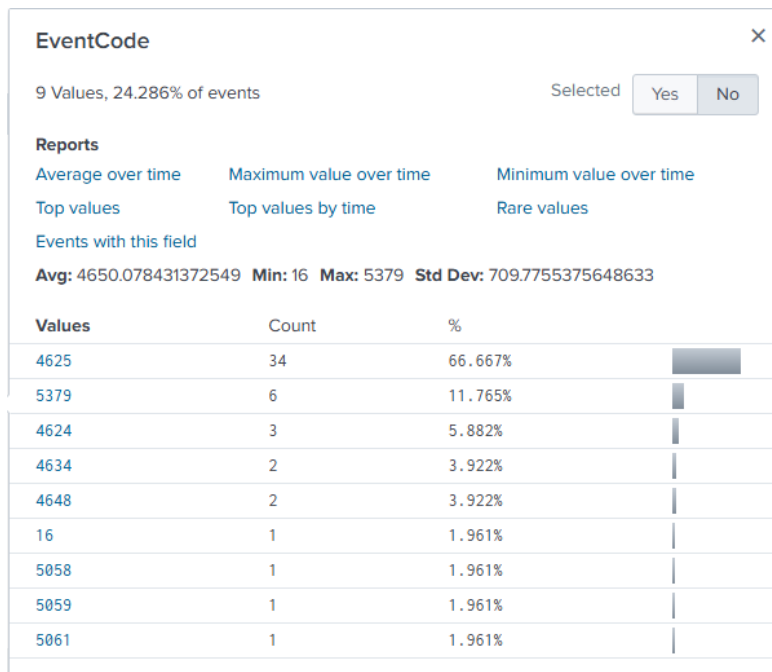
- Success.

## Viewing Telemetry on splunk

- On Plunk portal, we head over to ‘search & reporting’
- Put in search parameters ‘index = endpoint fchiesa’
- 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 occurred during the brute-force attack
- Then we see 4624, this eventID represents successful log on



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 Account Domain:

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

i	Time	Event
		Impersonation Level: Impersonation
		New Logon:
		Security ID: S-1-5-21-156145415-180932403-32154479-1168
		Account Name: fchiesa
		Account Domain: REDSDOMAIN
		Logon ID: 0x31A693
		Linked Logon ID: 0x0
		Network Account Name: -
		Network Account Domain: -
		Logon GUID: {00000000-0000-0000-0000-000000000000}
		Process Information:
		Process ID: 0x0
		Process Name: -
		Network Information:
		Workstation Name: kali
		Source Network Address: 192.168.10.250
		Source Port: 0
		Detailed Authentication Information:
		Logon Process: NTLmSsp
		Authentication 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.
		The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

## Download AomicRedTeam on Target-PC

- Open powershell as administrator
- Run 'set-executionpolicy Bypass CurrentUser'

```

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

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

PS C:\Windows\system32> Set-ExecutionPolicy Bypass CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?linkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32>

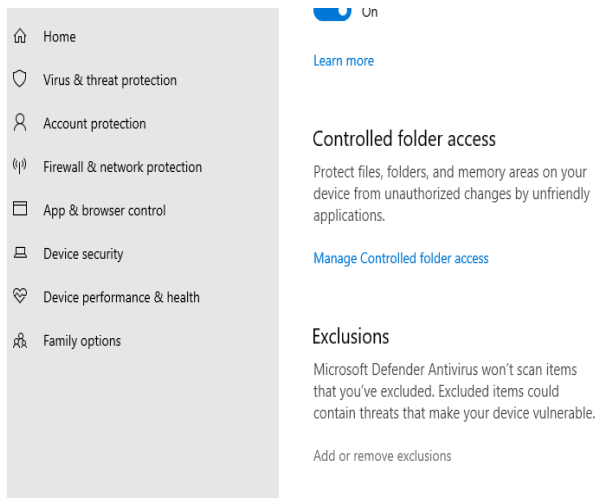
```

- 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

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

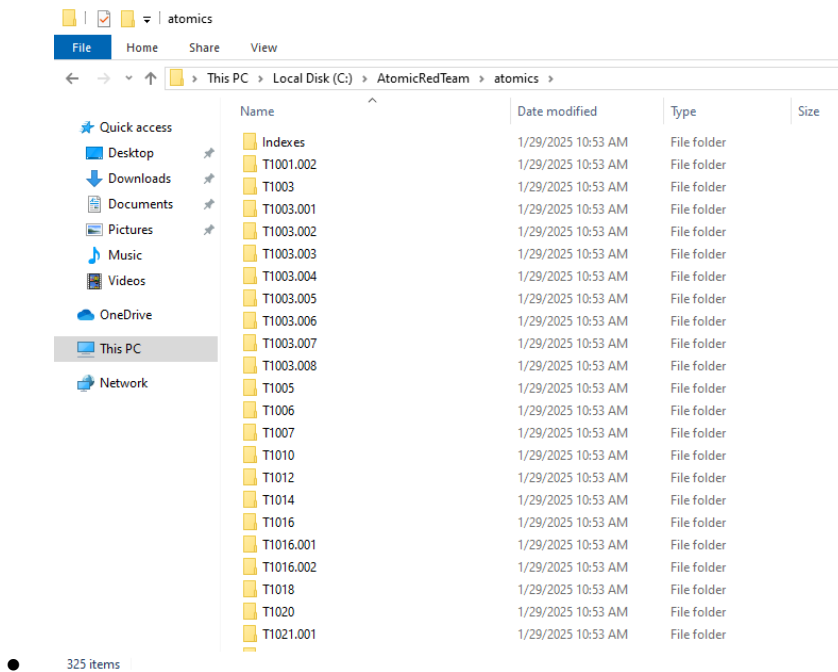
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-ExecutionPolicy Bypass CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Windows\system32> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/Invoke-AtomicRedTeam/master/install-atom
icredteam.ps1' -UseBasicParsing);
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomics

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/Invoke-AtomicRedTeam/wiki for complete details
PS C:\Windows\system32>
```

- 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'

MITRE | ATT&CK

Matrices • Tactics • Techniques • Defenses • CTI • Resources •

Benefactors Blog Search

## ATT&CK Matrix for Enterprise

layout: side

show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques
Active Scanning (3)	Acquire Access (3)	Content Injection (3)	Cloud Administration Command (3)	Account Manipulation (7)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise (3)	Command and Scripting Interpreter (11)	BITS Jobs (3)	Access Token Manipulation (3)	Access Token Manipulation (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application (3)	Container Administration Command (3)	Boot or Logon Autostart Execution (14)	Account Manipulation (3)	Build Image (3)
Gather Victim Network Information (6)	Compromise Infrastructure (3)	External Remote Services (3)	Deploy Container (3)	Boot or Logon Initialization Scripts (3)	Debugger Extension (3)	Debugger Extension (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions (3)	Exploitation for Client Execution (3)	Browser Extensions (3)	Deobfuscate Files or Information (3)	Deobfuscate Files or Information (3)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary (3)	Boot or Logon Initialization Scripts (3)	Deploy Container (3)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media (3)	Native API (3)	Local Account (3)	Create or Modify System Process (3)	Domain or Tenant Policy Modification (3)
Search Open Technical Databases (3)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Create Account (3)	Domain Account (3)	Execution Guardrails (3)
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship (3)	Serverless Execution (3)	Create or Modify System Process (3)	Cloud Account (3)	Exploitation for Defense Evasion (3)
Search Victim-Owned Websites (3)		Software Deployment Tools (3)	Shared Modules (3)	Event Triggered Execution (17)	Escape to Host (3)	File and Directory Permissions Modification (3)
		System Services (3)	External Remote (3)		Exploitation for Privilege Escalation (3)	Hide Artifacts (3)

https://attack.mitre.org/techniques/T1136.001

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Invoke-AtomicTest T1136.001
PathToAtomicFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-4 Create a new user in a command prompt
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.
Exit code: 2
Done executing test: T1136.001-4 Create a new user in a command prompt
Executing test: T1136.001-5 Create a new user in PowerShell
Name Enabled Description
-----
T1136.001 PowerShell True
Exit code: 0
Done executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-8 Create a new Windows admin user
The command completed successfully.
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-8 Create a new Windows admin user
Executing test: T1136.001-9 Create a new Windows admin user via .NET
This script creates a new user, adds it to a local administrator group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the 'Administrators' group.
Newly Created User Info:
User name NewLocalUser
Full Name NewLocalUser
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never
Password last set 1/29/2025 11:07:17 AM
Password expires Never
Password changeable 1/30/2025 11:07:17 AM
Password required Yes
User may change password No
Workstations allowed All
Logon script
User profile
Home directory
Last logon Never
Logon hours allowed All
Local Group Memberships
Global Group memberships *None
The command completed successfully.
User 'NewLocalUser' deleted successfully.
Exception calling "Add" with "3" argument(s): "An error (1789) occurred while enumerating the group membership. The member's SID could not be resolved."
At line:35 char:5
+ $adminGroup.Members.Add($localContext, [System.DirectoryServices. ...
+ ~~~~~
+ CategoryInfo          : NotSpecified (:) [], MethodInvocationException
+ FullyQualifiedErrorId : PrincipalOperationException
Exit code: 0
Done executing test: T1136.001-9 Create a new Windows admin user via .NET
PS C:\Windows\system32>
```

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

index=endpoint newlocaluser Last 15 minutes

✓ 12 events (1/29/25 6:56:57.000 PM to 1/29/25 7:11:57.000 PM) No Event Sampling Job Smart Mode

Events (12) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 minute per column

Format Show: 20 Per Page View: List

Hide Fields	All Fields	Time	Event
<p>SELECTED FIELDS</p> <ul style="list-style-type: none"> <li>host 1</li> <li>source 2</li> <li>source type 2</li> </ul> <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> <li>Account_Domain 2</li> <li>Account_Expires 1</li> <li>Account_Name 2</li> <li>ComputerName 1</li> <li>Display_Name 2</li> <li>EventCode 6</li> <li>EventType 1</li> <li>Home_Directory 1</li> <li>Home_Drive 1</li> <li>Index 1</li> <li>Keywords 1</li> <li>linecount 7</li> <li>LogName 1</li> <li>Logon_Hours 1</li> <li>Logon_ID 1</li> <li>Message 8</li> <li>New_UAC_Value 3</li> <li>Old_UAC_Value 3</li> </ul>		<p>1/29/25 7:07:26.000 PM</p>	<p>01/29/2025 11:07:26 AM</p> <p>LogName=Security</p> <p>EventCode=4726</p> <p>EventType=0</p> <p>ComputerName=Target-PC.Reddomain.com</p> <p>SourceName=Microsoft Windows security auditing.</p> <p>Type=Information</p> <p>RecordNumber=10860</p> <p>Keywords=Audit Success</p> <p>TaskCategory=User Account Management</p> <p>OpCode=Info</p> <p>Message=A user account was deleted.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-156145415-180932403-32154479-500</p> <p>Account Name: Administrator</p> <p>Account Domain: REDSDOMAIN</p> <p>Logon ID: 0x3C3A06</p> <p>Target Account:</p> <p>Security ID: S-1-5-21-2437161402-1197107365-299837250-1005</p> <p>Account Name: NewLocalUser</p> <p>Account Domain: TARGET-PC</p>

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

MITRE | ATT&CK

Matrices Tactics Techniques Defenses CTI Resources

Benefactors Blog Search

## ATT&CK Matrix for Enterprise

layout: side

show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
<p>10 techniques</p> <ul style="list-style-type: none"> <li>Active Scanning (3)</li> <li>Gather Victim Host Information (4)</li> <li>Gather Victim Identity Information (3)</li> <li>Gather Victim Network Information (6)</li> <li>Gather Victim Org Information (4)</li> <li>Phishing for Information (4)</li> <li>Search Closed Sources (2)</li> <li>Search Open Technical Databases (3)</li> <li>Search Open Websites/Domains (2)</li> <li>Search Victim-Owned Websites</li> </ul>	<p>8 techniques</p> <ul style="list-style-type: none"> <li>Acquire Access</li> <li>Acquire Infrastructure (8)</li> <li>Compromise Accounts (3)</li> <li>Compromise Infrastructure (3)</li> <li>Develop Capabilities (4)</li> <li>Establish Accounts (3)</li> <li>Obtain Capabilities (7)</li> <li>Stage Capabilities (6)</li> </ul>	<p>10 techniques</p> <ul style="list-style-type: none"> <li>Content Injection</li> <li>Drive-by Compromise</li> <li>Exploit Public-Facing Application</li> <li>External Remote Services</li> <li>Hardware Additions</li> <li>Phishing (4)</li> <li>Replication Through Removable Media</li> <li>Supply Chain Compromise (3)</li> <li>Trusted Relationship</li> <li>Valid Accounts (4)</li> </ul>	<p>14 techniques</p> <ul style="list-style-type: none"> <li>Cloud Administration Command</li> <li>Command and Scripting Interpreter (11)</li> <li>Container Administration Command</li> <li>Deploy Container</li> <li>Exploitation for Client Execution</li> <li>PowerShell (T1059.001)</li> <li>AppleScript</li> <li>Windows Command Shell</li> <li>Unix Shell</li> <li>Visual Basic</li> <li>Python</li> <li>JavaScript</li> <li>Network Device CLI</li> <li>Cloud API</li> <li>AutoHotKey &amp; AutoIT</li> <li>Lua</li> </ul>	<p>20 techniques</p> <ul style="list-style-type: none"> <li>Account Manipulation (7)</li> <li>BITS Jobs</li> <li>Boot or Logon Autostart Execution (14)</li> <li>Boot or Logon Initialization Scripts (3)</li> <li>Browser Extensions</li> <li>Compromise Host Software Binary</li> <li>Local Account</li> <li>Domain Account</li> <li>Cloud Account</li> <li>Create Account (3)</li> <li>Create or Modify System Process (3)</li> <li>Event Triggered Execution (17)</li> <li>External Remote</li> </ul>	<p>14 techniques</p> <ul style="list-style-type: none"> <li>Abuse Elevated Privileges</li> <li>Control Mechanisms</li> <li>Account Manipulation</li> <li>Account Manipulation</li> <li>Boot or Logon Autostart Execution</li> <li>Boot or Logon Initialization Scripts</li> <li>Browser Extensions</li> <li>Compromise Host Software Binary</li> <li>Create or Modify System Process</li> <li>Domain Account</li> <li>Domain Account</li> <li>Domain Account</li> <li>Domain Account</li> <li>Event Triggered Execution</li> <li>Exploitation for Client Execution</li> <li>Exploitation for Client Execution</li> </ul>

<https://attack.mitre.org/techniques/T1059/001>

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

a 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

a vendor 1

Time

Event

> 1/30/25 12:20:32.000 AM

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385f-c22a-43e0-bf4c-06f5 698ffb99}" /><EventID>13</EventID><Version>2</Version><Level>4</Level><Task>13</Task><Opcode>0</Opcode><Keywords>0x0000000000000000</Keywords><TimeCreated SystemTime="2025-01-30T00:20:32.6377574Z" /><EventRecordID>20859</EventRecordID><Correlation><Execution ProcessID="3384" ThreadID="756" /><Channel>Microsof t-Windows-Sysmon/Operational</Channel><Computer>Target-PC.Reddomain.com</Com puter><Security UserID="S-1-5-18" /></System><EventData><Data Name="RuleName">~</Data><Data Name="EventType">SetValue</Data><Data Name="UtcTime">2025-01-30 00:20:32.631</Data><Data Name="ProcessGuid">{999e35f8-c5ce-679a-ff04-00000000 1900}</Data><Data Name="ProcessId">10132</Data><Data Name="Image">C:\Windows \System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name="TargetObjec t">HKLM\System\CurrentControlSet\Services\wbem\State\UserSettings\S-1-5-21-156 145415-180932403-32154479-500\Device\HarddiskVolume2\Windows\System32\Window sPowerShell\v1.0\powershell.exe</Data><Data Name="Details">Binary Data</Data><Data Name="User">REDSDOMAIN\Administrator</Data></EventData></Event>

> 1/30/25 12:20:32.000 AM

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385f-c22a-43e0-bf4c-06f5 698ffb99}" /><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11