Monitoring of Active Directory and Windows Client using Sysmon and Splunk

Objectives
1. Install AD and promote it to the Domain Controller.
2. Join Windows client to the domain
3. Configure Sysmon to collect event logs on AD and Windows client
4. Install Splunk forwarder to send the event logs to Splunk Server
5. Configure the Splunk server to receive the event logs from the AD and Windows client for further analysis
6. Conduct a brute force attack on the AD from Kali Linux, Examine the details of the attack on Splunk.

Introduction

Active Directory (AD) is a directory service developed by Microsoft that centralises the management of users, computers, groups, and other resources in a networked environment it provides authentication authorization and policy enforcement, enabling streamlined administration and secure access to network resources across an organisation.

An AD is highly appealing to attackers because it serves as the central repository for an organisation's authentication and authorisation data. By compromising the AD, attackers can gain access to user's credentials, escalate privileges and move laterally across the network, effectively controlling the entire domain. Additionally, misconfiguration and legacy vulnerabilities within the AD environment can provide opportunities for exploitation making it a lucrative target for persistent access and data exfiltration. This makes monitoring and securing an AD highly essential for any organisation.

This project will describe the installation of an AD, promotion of the AD to a domain controller, configure Sysmon on the AD that will collect event logs, and Install a Splunk forwarder that will send the collected event logs to Splunk for analysis. A Windows client computer with users, joining the domain configure Sysmon, An Ubuntu server hosting Splunk. Sysmon will collect the logs event that the Splunk forwarder will send to the Splunk server.
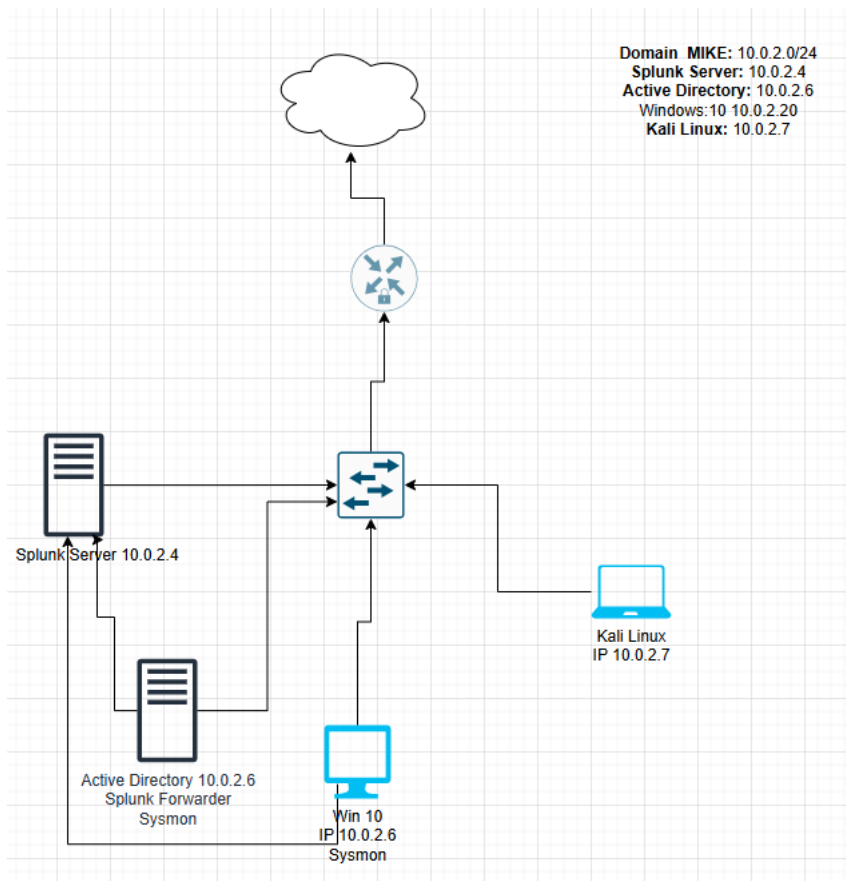
Figure 1

Splunk Server setup

Install Ubuntu server. Once the installation is done. Check that the server has internet connectivity by sending a ping request to google.com and set the IP addresses to match the address in the diagram

Figure 2

Download Splunk for the official website. And install splunk using the command **sudo dpkg <splunk package>**

Figure 3

Type y to agree to the licensing

```
Usage Data: Data generated from the usage, configuratio
and performance of an Offering.

Use Rights: As set out in section 1.1.

Do you agree with this license? [y/n]: y
```

Figure 4

Provide a username and password that will administrate on the Splunk web interface

```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
```

Figure 5

Let Splunk installation complete. The presentation of the web-access details will indicate the installation is complete. To access the web interface, use either the hostname or the IP address followed by the port 8000 (Default port). Configure Splunk to start at boot time by issuing the command
sudo ./splunk enable boot-start -user splunk

```
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-ser01:8000

splunk@splunk-ser01:~/bin$ exit
exit
mike@splunk-ser01:/opt/splunk$ cd bin
mike@splunk-ser01:/opt/splunk/bin$
mike@splunk-ser01:/opt/splunk/bin$
mike@splunk-ser01:/opt/splunk/bin$
mike@splunk-ser01:/opt/splunk/bin$
mike@splunk-ser01:/opt/splunk/bin$
mike@splunk-ser01:/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.
mike@splunk-ser01:/opt/splunk/bin$
```

Figure 6

Windows 10 Client Setup, Install Sysmon and Splunk Forwarder

Window 10 client the device that the client will use to log on to access organisation resources on the domain. Sysmon will be installed to collect events generated on the device and Splunk forwarder will send the logs to Splunk.
After installation is done make sure to change the name of the device. By right-clicking **ThisPC** navigate to properties. Under Device Specifications Click on **Rename this PC.** Enter a name of your choice. Restarting the pc is required for the changes to take effect.

Device specifications

Device name	Mike-PC
Processor	Intel(R) Xeon(R) CPU E5-1620 v3 @ 3.50GHz 3.49 GHz
Installed RAM	4.00 GB
Device ID	AA3B2E8F-E429-4F98-82D9-F2A83D8A4F5C
Product ID	00330-80000-00000-AA237
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Figure 7

Download Sysmon from **https://learn.microsoft.com/en-us/sysinternals**

Sysmon v15.15

Article • 07/23/2024 • 9 contributors

In this article

Introduction

Overview of Sysmon Capabilities

Screenshots

Usage

Show 5 more

By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

Figure 8

Navigate to the Downloads to the location of the Sysmon download

Figure 9

For the installation of sysmon xml instructions need to be downloaded. The xml instructions are to guide Sysmon on what needs to be installed.

Figure 10

Splunk Forwarder is next to be installed on the Windows client. Download the forwarder for Windows double-click. The first steps do not need any changes until the window for the receiver is reached

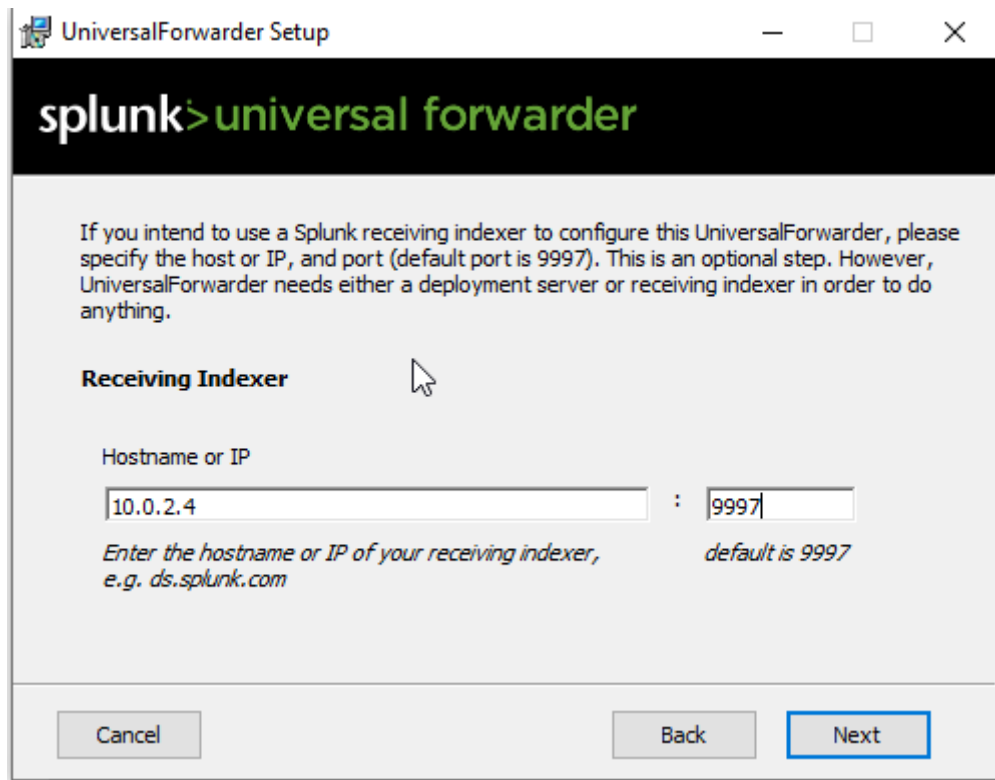fill in the IP address of the Splunk server and port 9997
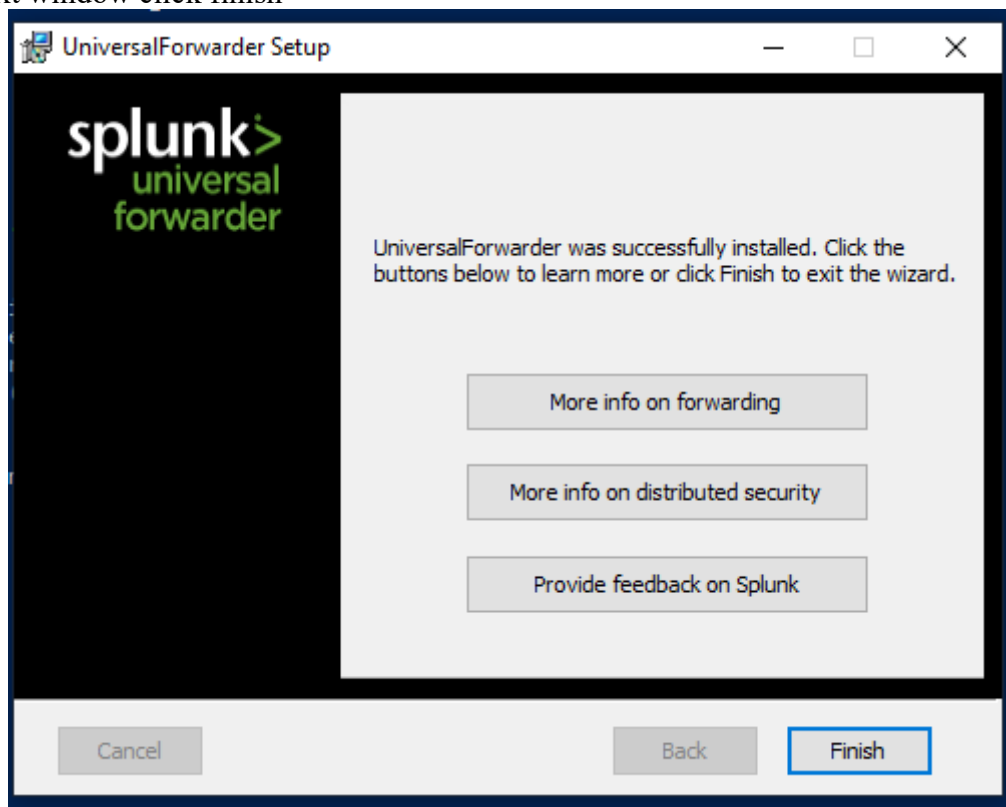
Figure 11

On the next window click finish

Figure 12

The next step is to configure the inputs file. The inputs file will contain instructions on what data is going to be collected. Make a copy of the inputs.conf from the defaults into the local directory
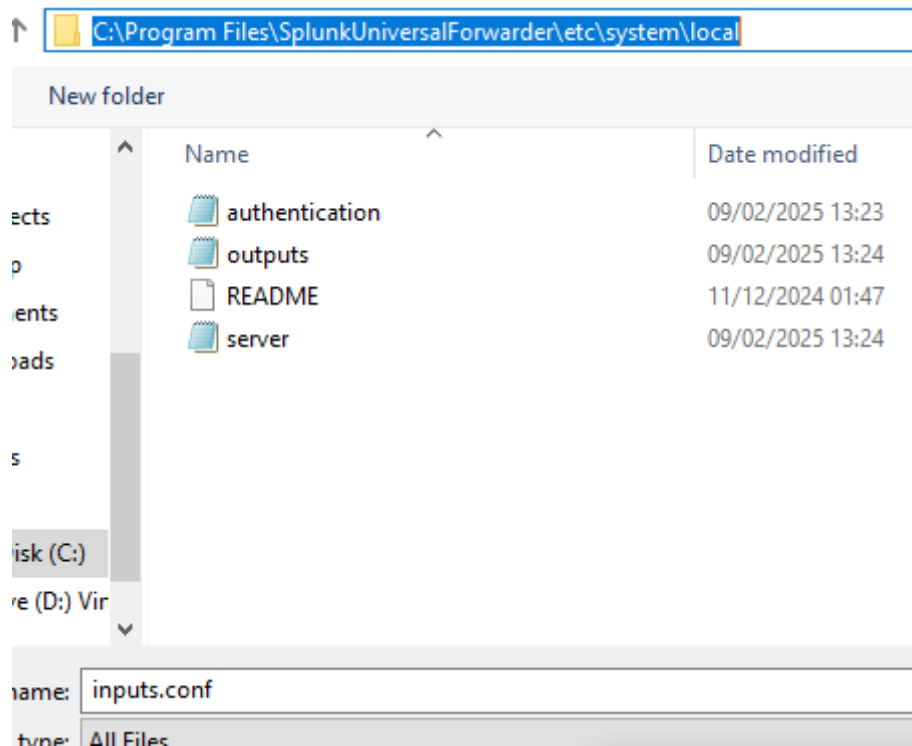
Figure 13

Next navigate to the services and click on the properties of the Splunk forwarder. Ensure that the local services is selected this is due to the permission as the default NT may be denied permission to collect data.
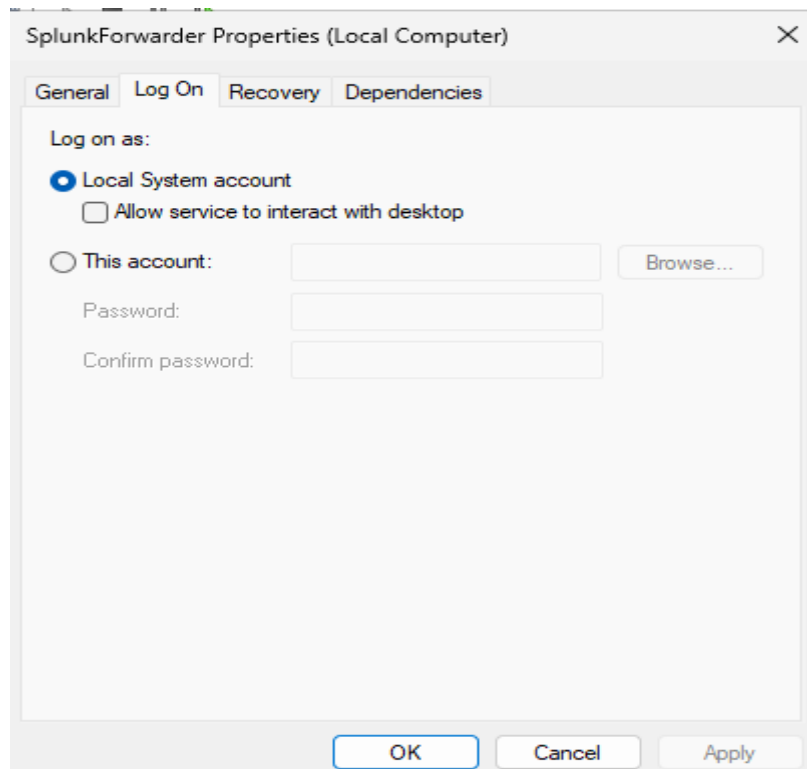
Figure 14

Restart the Splunk forwarder services for the changes to take effect.
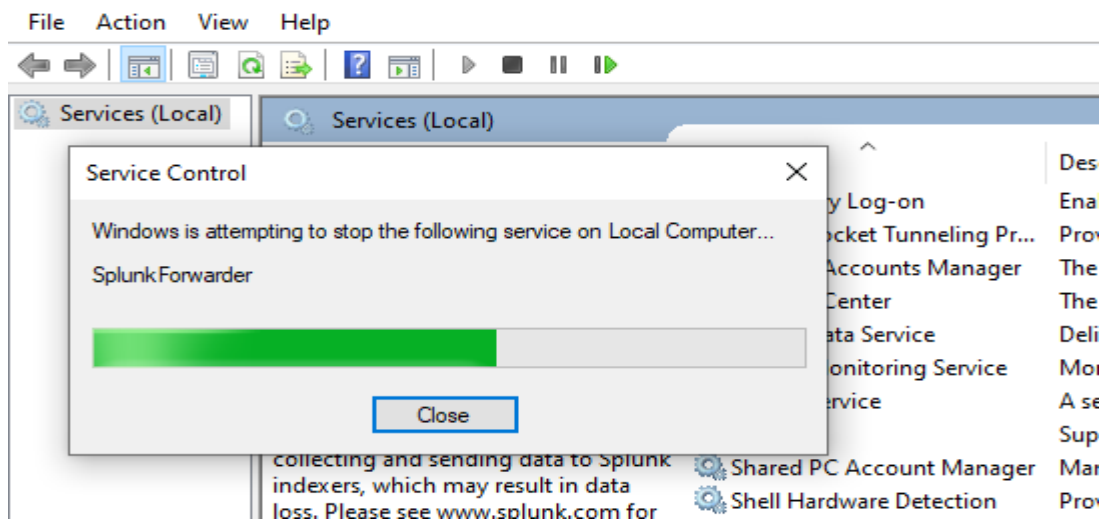
Figure 15

On the Splunk server Login and navigate to create a new index.
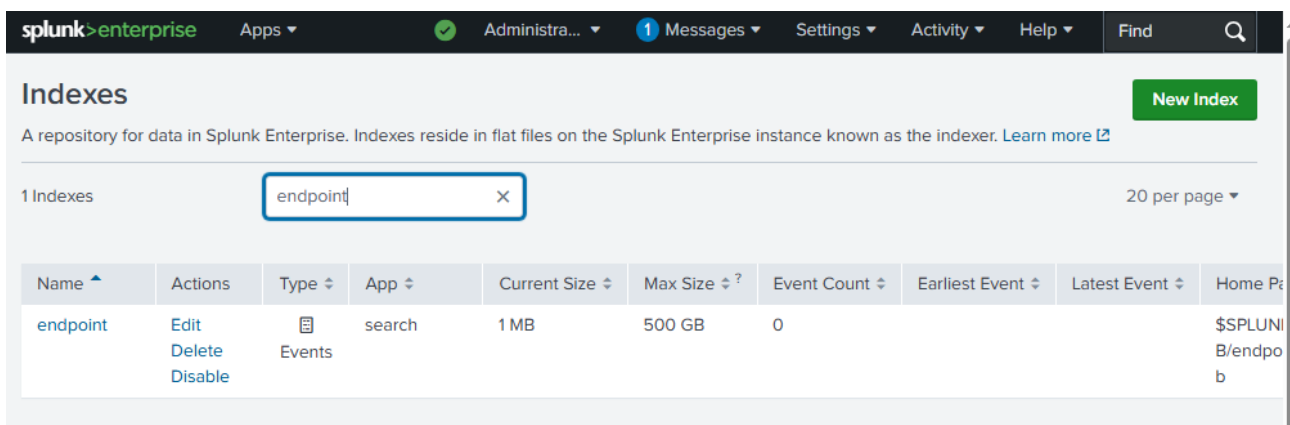
Figure 16

Under forwarding and receiving create a new listening port 9997
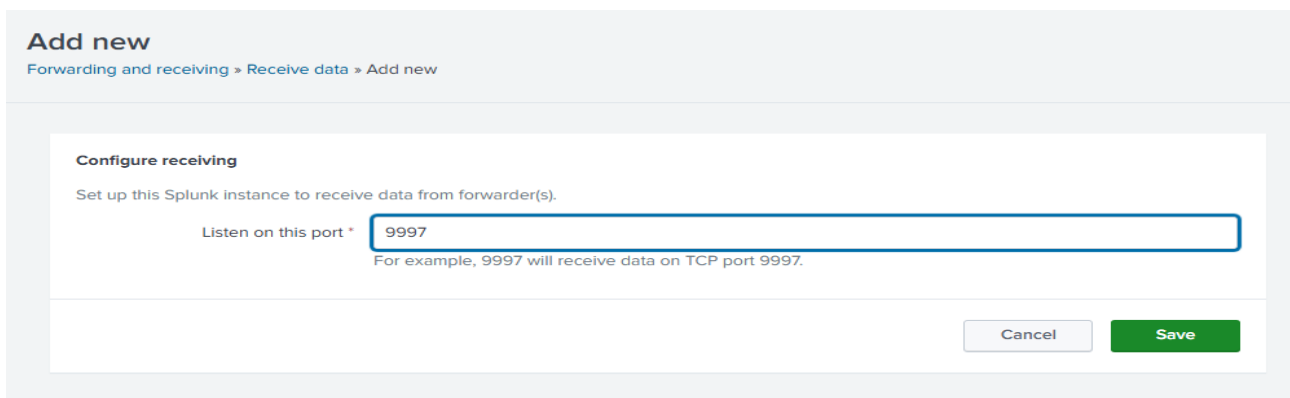
Figure 17

On the Splunk server begin a new search index=endpoint

Figure 18

In the selected fields see 1 host value Mike-PC the name of Windows 10 PC.

Install Active Directory.

Download and install Windows Server. Once the installation is done ensure that there is an internet connection, and the server can also ping the Splunk server.

```
PS C:\Users\Administrator\Downloads\Sysmon> ping google.com

Pinging google.com [209.85.202.139] with 32 bytes of data:
Reply from 209.85.202.139: bytes=32 time=31ms TTL=54
Reply from 209.85.202.139: bytes=32 time=37ms TTL=54
Reply from 209.85.202.139: bytes=32 time=32ms TTL=54
Reply from 209.85.202.139: bytes=32 time=29ms TTL=54

Ping statistics for 209.85.202.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 37ms, Average = 32ms
PS C:\Users\Administrator\Downloads\Sysmon> ^C
PS C:\Users\Administrator\Downloads\Sysmon>
PS C:\Users\Administrator\Downloads\Sysmon>
PS C:\Users\Administrator\Downloads\Sysmon>
PS C:\Users\Administrator\Downloads\Sysmon> ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator\Downloads\Sysmon>
```

Figure 19

Rename the server same steps taken when renaming the Windows 10 client in the case Mike-DC, including restarting so the changes take effect.

Install Active Directory services on the server. In the right-hand corner under Manage click on Add Roles and Features

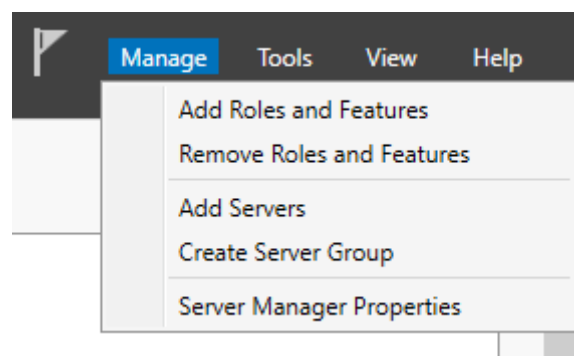|	Manage	Tools	View	Help
	Add Roles and Features			
	Remove Roles and Features			
	Add Servers			
	Create Server Group			
	Server Manager Properties			

Figure 20

On the Installation type window select Role-based and feature based installation
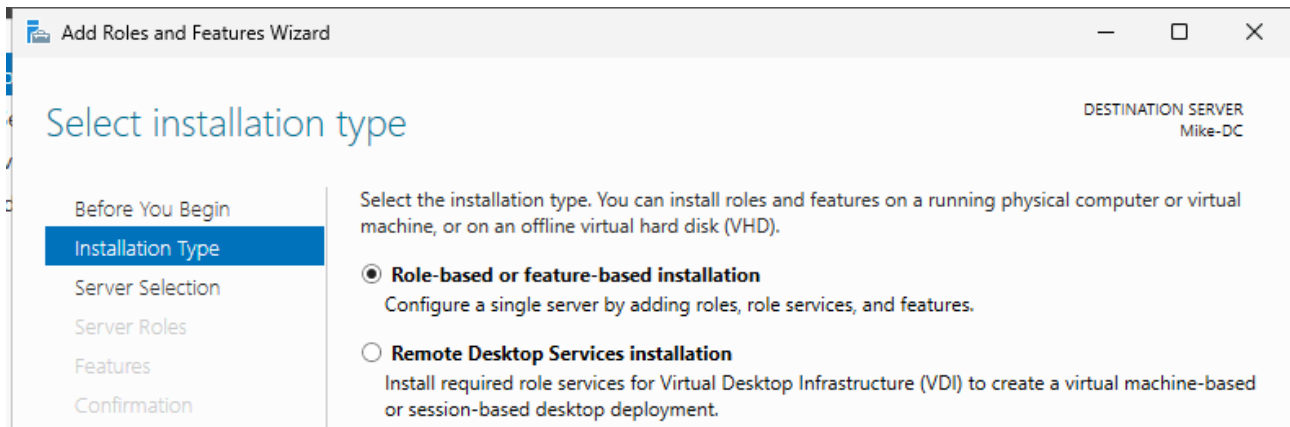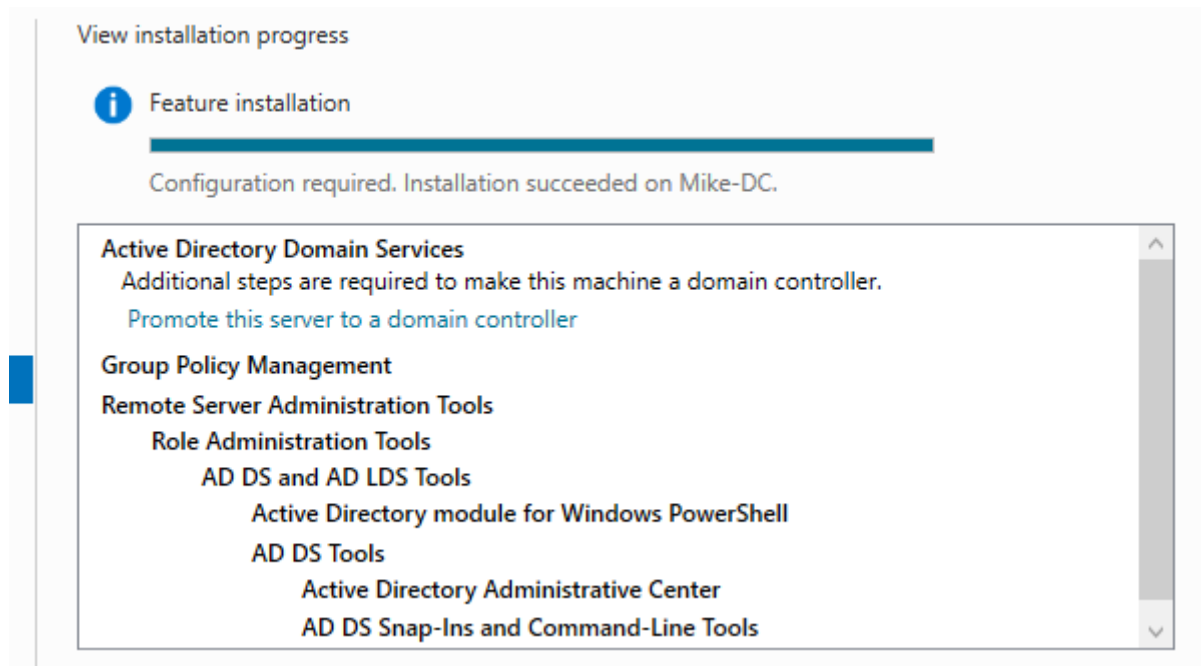

Figure 21

Let the installation complete

Figure 22

When the installation is complete the server needs to be promoted to Domain Controller
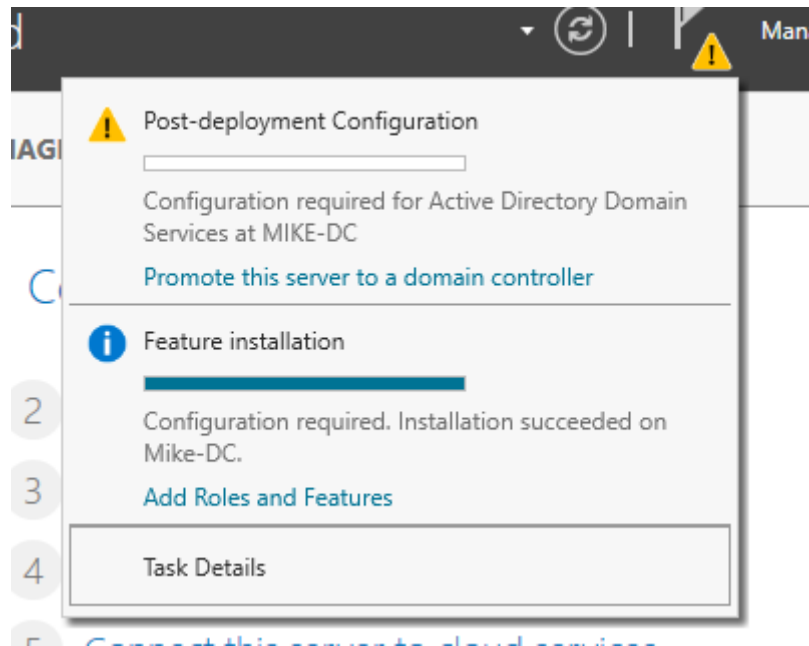

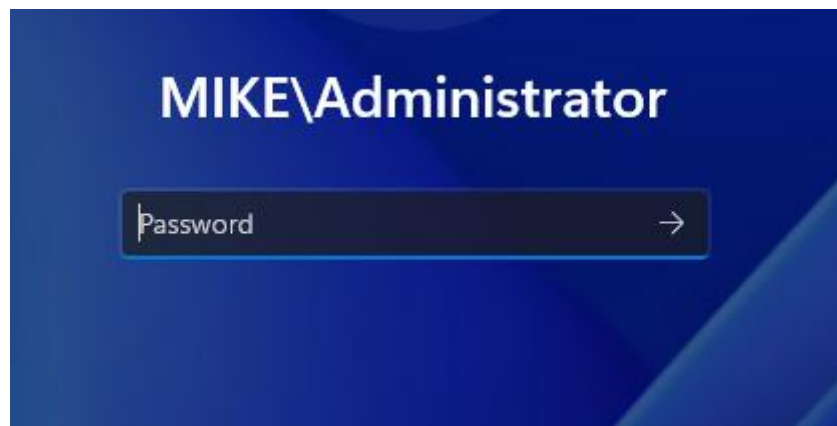
Figure 23

On restart, you can log as administrator.

Figure 24

Create users who will log on the Windows 10 client device which will in turn be joined to the domain MIKE.LOCAL
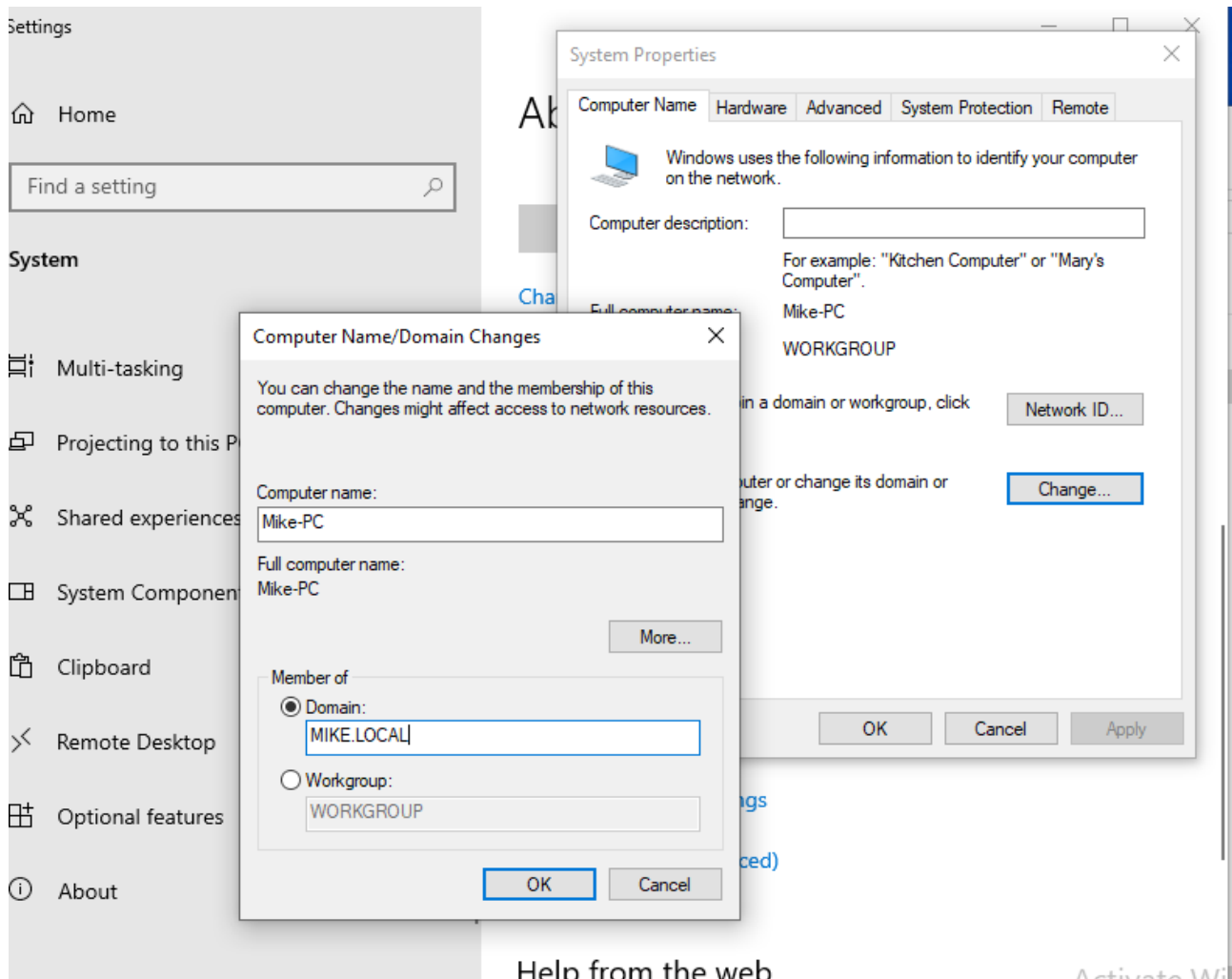
Join the Windows 10 Client to the Domain

Figure 25

Enter the administrator password to allow the client to join the domain
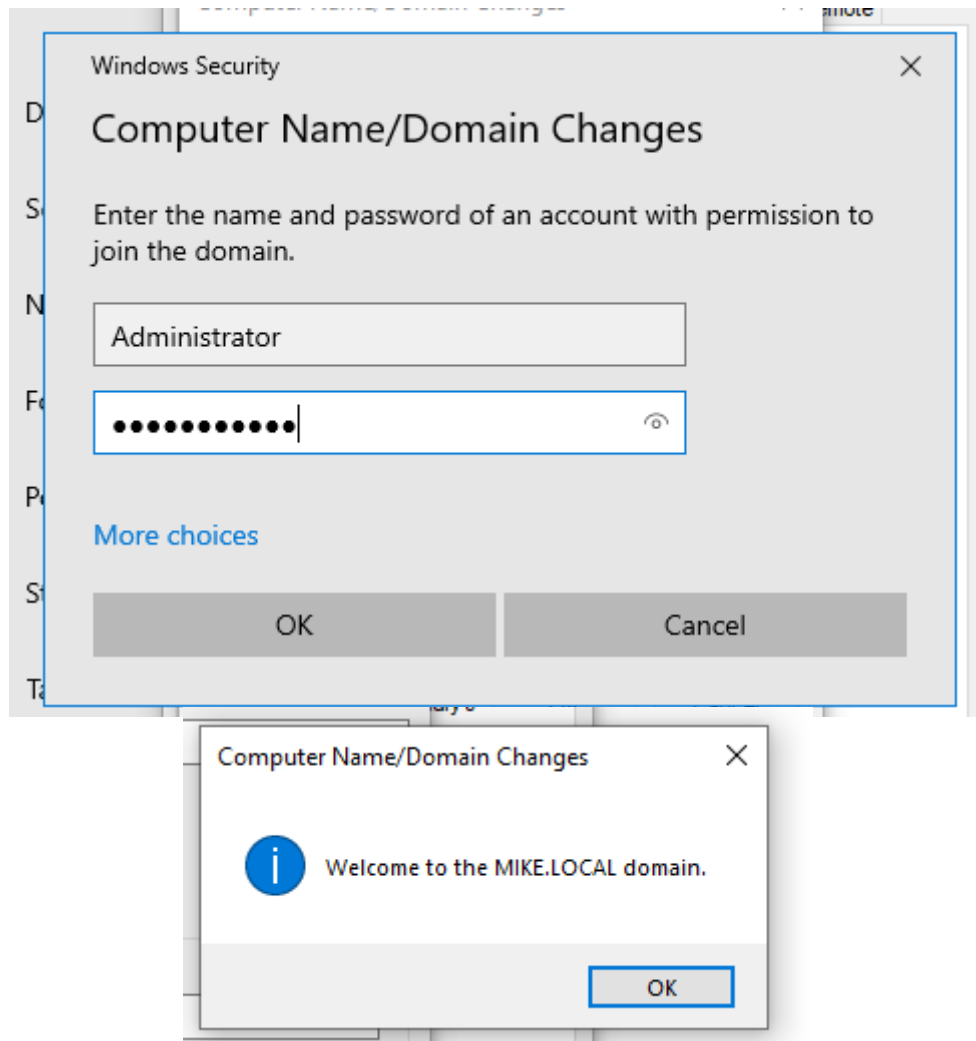
Figure 26

Restart the Windows 10 client.

Use the credentials of one of the users created in the previous step to log into the Windows 10 client
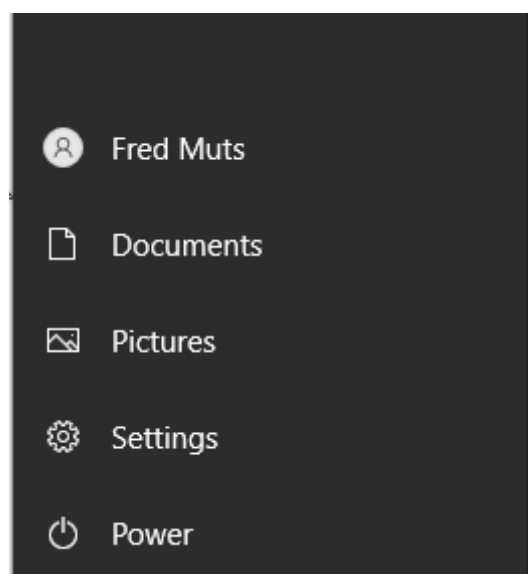
Figure 27

Install Splunk Forwarder and Sysmon. follow the same steps as on the Windows 10 client.

Check on the Splunk server to ensure there 2 hosts are listed
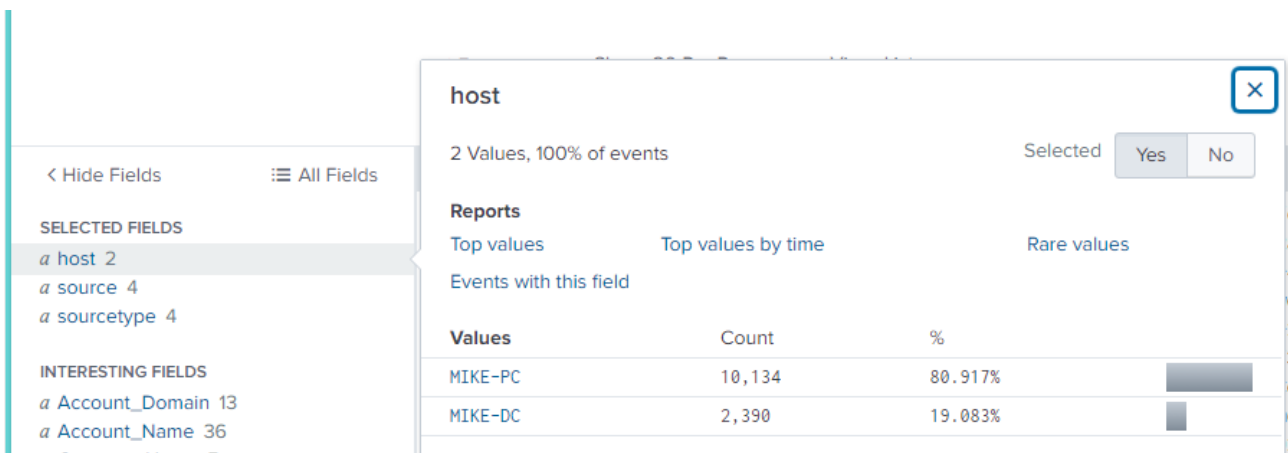
Figure 28

To conduct a brute force test remote login needs to be enabled for a few users On the Windows 10 client device in the properties Add a few users in the remote tab
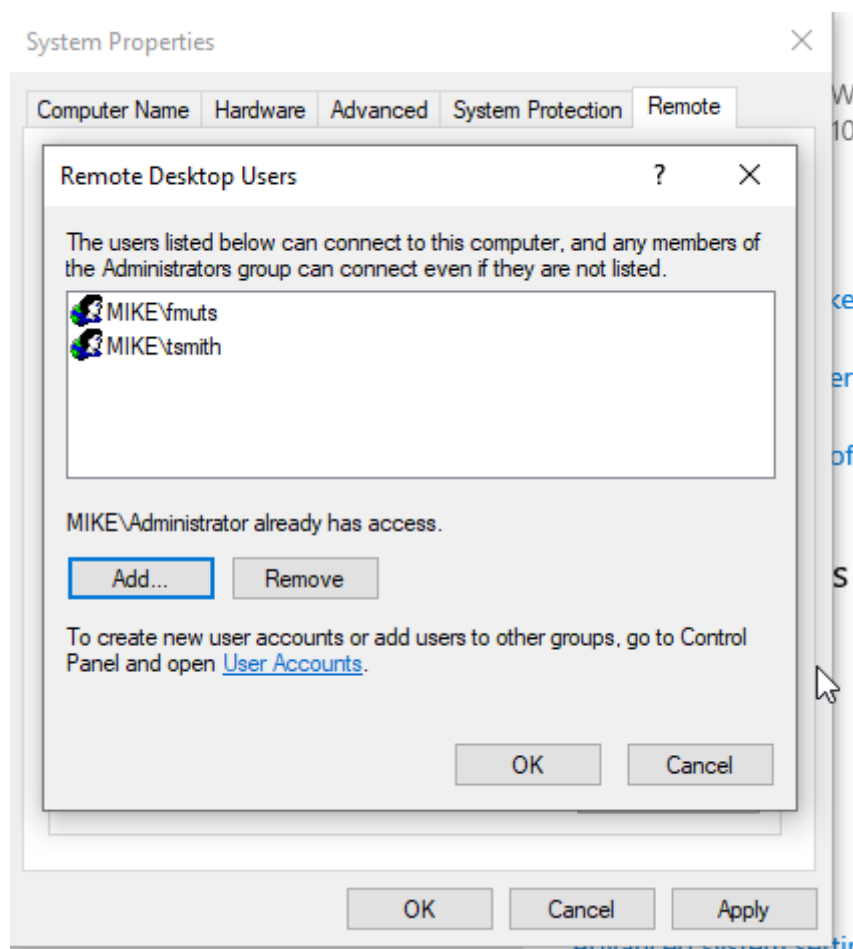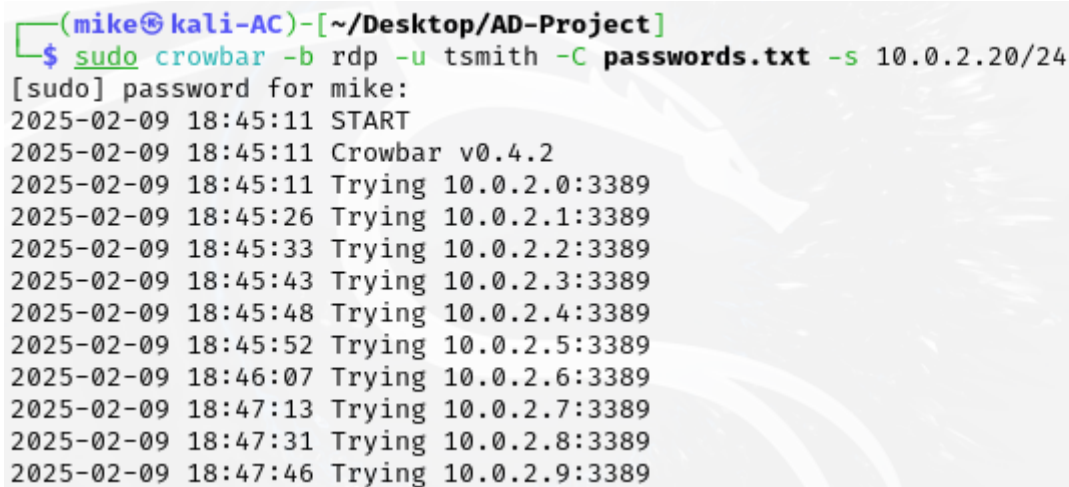
Figure 29

Brute force attack

On the Kali Linux device install crowbar. With crowbar installation complete and a text file with common passwords available. -b (service rdp) -u (user tsmith) -s IP address range
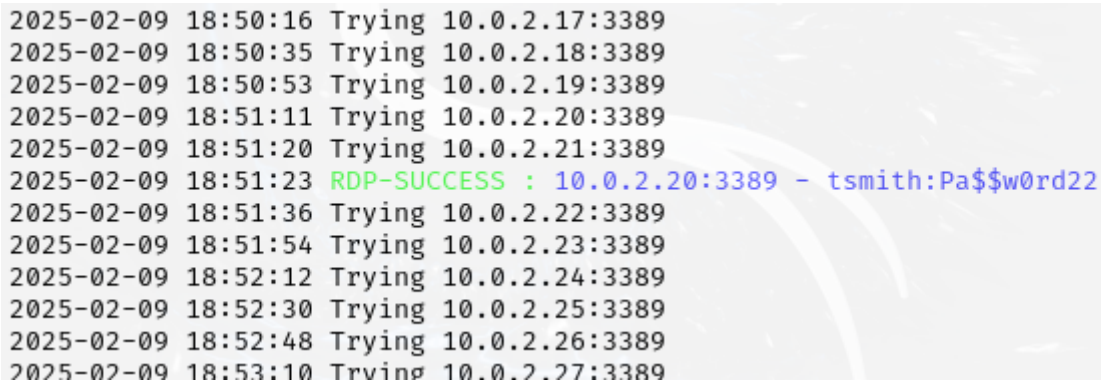
Figure 30

Crowbar will use the provided list of passwords and iterate through the IP range provided in this case /24 = 253 IP address. It will take some time.

In case it finds a password that matches

Figure 31

The IP address of the Windows 10 Client the user **tsmith** and user's password.

On the Splunk server, this attempt can be seen in event ID 4625

Figure 32

Look up what event ID 4625 on Microsoft help page. It is associated with a failed log on
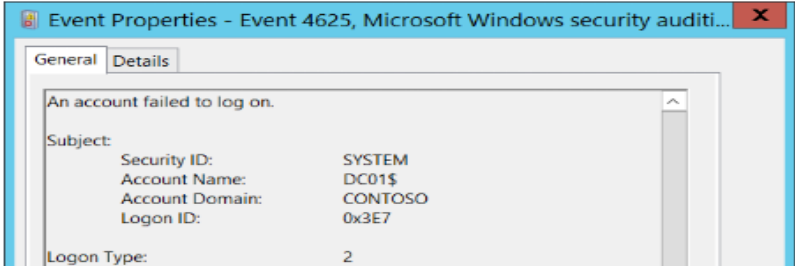
Figure 33

Figure 34

Expanding the event, it is noticed that the reason for the logon failure is an Unknown username or bad password, and the source IP address is the Kali Linux

And event ID 5379. When searched on Google this event is described as Credential manger were read.

Figure 35

These two events in the real world would trigger further investigation.

AtomicRedTeam & MITRE ATT&CK

For further testing on the alerts that can be generated on Splunk a tool Atomic Red Team can be used to run scripts to test the security of a device.

AtomicRedTeam is an open-source framework that provides a library of small independent tests referred to as "atomic tests" designed to simulate adversary techniques based on the MITRE ATT&CK framework. These tests allow security teams to

- Validate Security Controls: Emulate real-world attack behaviours to assess and improve detection, response and mitigation capabilities
- Enhance Threat Hunting: Identify gaps in the current security monitoring and fine tune defences against known attack tactics, techniques and procedures
- Streamline Testing: Easily integrate into existing workflows to run consistent and repeatable tests across various environments.

The C drive will need to be excluded in the Microsoft Defender settings otherwise some of the scripts will be removed.

Exclusions

Add or remove items that you want to exclude from Microsoft Defender
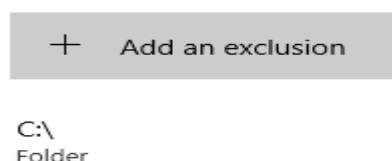anti-Virus scans.

+ Add an exclusion

C:\
Folder

Figure 36

Install AtomicRedTeam on the device in this case Windows 10 pc.

Figure 37

Navigate to C:\AtomicRedTeam\atomics to ensure the files exist.

On the MITRE ATT&CK select a tactic to test, ensure that it has a corresponding code number in the atomics

For example, T1136.001 is a script that will test creating a user on the local system

Figure 38

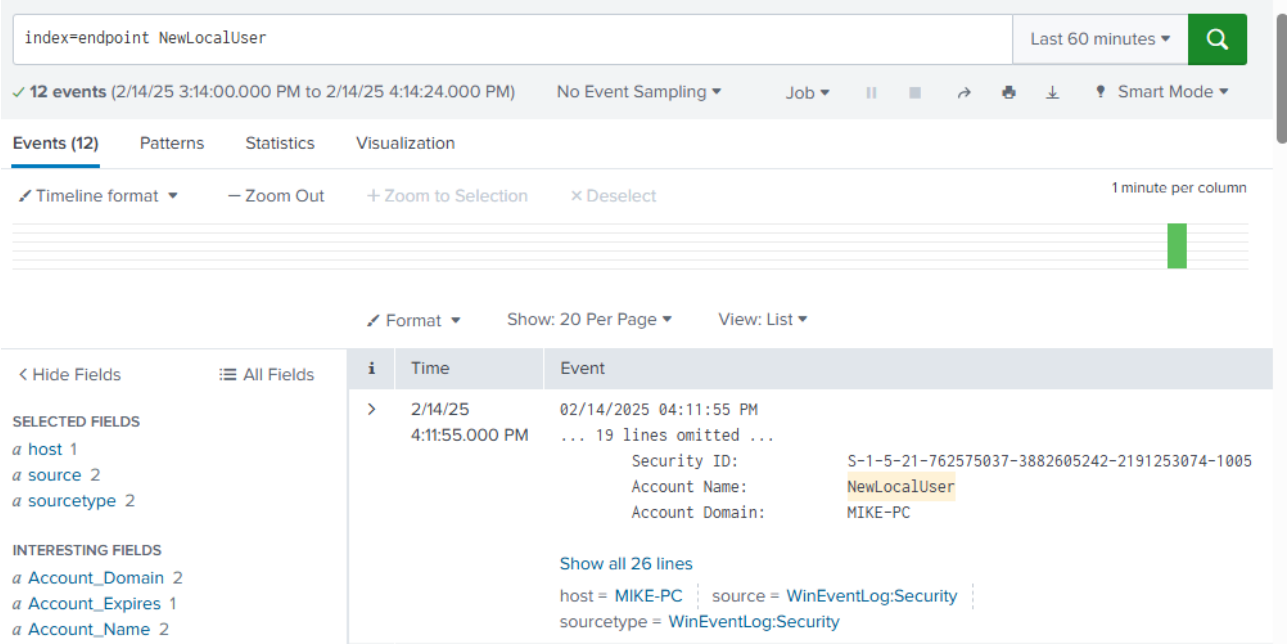When the script completes, Log on the Splunk server to check the activity

Figure 39

Conclusion

Implementing Splunk to monitor activities on the domain demonstrated how effective centralised logging and real-time alerting can be in detecting anomalies such as brute force attempts. Using AtomicRedTeam further highlights the importance of monitoring, MITRE ATT&CK helps fill the gaps that the tactic finds in the monitoring rules. This helps in detection and facilitates prompt incident response.

Lessons Learned
1. Installation of Active Directory and promotion of Domain Services
2. Installation of Splunk, configuration of the inputs files, and Searching of events
3. Using AtomicRedTeam and MITRE ATT&CK to test the security of a device