ACTIVE DIRECTORY LAB

SUMMARY

The purpose of this lab is to create a basic Windows networking environment with Active Directory, utilizing VirtualBox on a MacBook Pro. This lab will cover the setup of a virtualized domain controller, a client machine, and the configuration of essential networking services.

HARDWARE EQUIPMENT

- MacBook Pro (2013)

SOFTWARE

- VirtualBox 7.0.20 for macOS/Intel Hosts
- VirtualBox 7.0.20 Oracle VirtualBox Extension Pack
- Windows 10 ISO
- Windows Server 2019 ISO

OBJECTIVES

1. Install and configure VirtualBox on macOS to host virtual machines.
2. Set up a Windows Server 2019 virtual machine as a domain controller.
3. Set up a Windows 10 virtual machine as a client connected to the domain.
4. Configure internal networking, NAT, DHCP, and Active Directory.
5. Use PowerShell to automate the creation of 1,000 users in Active Directory.

VIRTUAL MACHINE SETUP

1. Install VirtualBox & Extension Pack

- Download and install VirtualBox 7.0.20 and the Oracle VirtualBox Extension Pack on macOS.
- Ensure virtualization is enabled on your MacBook Pro.

2. Download ISOs

- Download Windows Server 2019 ISO and Windows 10 ISO.
- In VirtualBox, create a new virtual machine for each ISO.

WINDOWS SERVER 2019 SETUP

1. Create a Virtual Machine for Windows Server 2019

- Name the VM appropriately (e.g., "DomainController").
- Assign two network adapters: one for external internet (NAT) and one for internal networking.
- Install Windows Server 2019, selecting a Desktop Experience option for GUI access.

2. Configure Internal IP Addressing

- Open Network and Internet Settings > Change Adapter Settings.
- Rename the adapters: "INTERNET" for external and "X_INTERNAL_X" for internal.
- Assign an IP address to the internal network (e.g., 172.16.0.1) with a subnet mask of 255.255.255.0.
- Set the DNS server to 127.0.0.1 (loopback address).

3. Install and Configure Active Directory Domain Services

- In Server Manager, select Add Roles and Features > Active Directory Domain Services.
- After installation, promote the server to a domain controller by creating a new forest (e.g., "mydomain.com").
- Create an Organizational Unit (OU) named "Admins" and a new admin account within this OU.

4. Install RAS (Remote Access Server) and NAT (Network Address Translation)

- Add the Remote Access role via Server Manager, ensuring the Routing option is selected.
- Configure Routing and Remote Access to enable NAT, selecting the "INTERNET" adapter for public access.

5. Set Up DHCP Server

- Add the DHCP role in Server Manager and configure a new scope (e.g., 172.16.0.100-200).
- Authorize and activate the DHCP server for the internal network.

POWERSHELL SCRIPT TO ADD USERS

1. Automate User Creation

- Download and place the PowerShell script and user name file on the VM desktop.
- Run the script in Windows PowerShell ISE as an Administrator.
- Set execution policy to unrestricted and navigate to the script directory.
- Execute the script to add 1,000 users to Active Directory.

WINDOWS 10 CLIENT SETUP

1. Create a Virtual Machine for Windows 10

- Name the VM "Client1" and connect it to the internal network.
- Install Windows 10, selecting the option for an organization setup.
- Configure the VM to join the domain "mydomain.com" using the admin credentials created earlier.

2. Verify Network Connectivity

- Run `ipconfig` to confirm the IP address and default gateway.
- Run `ping google.com` to ensure DNS resolution and internet connectivity.
- Rename the computer to "CLIENT1" and confirm it has joined the domain.

CONCLUSION

With the completion of this lab, you have successfully set up a virtualized Active Directory environment, configured essential network services, and automated user creation using PowerShell. This environment can now be used to simulate and practice real-world IT support scenarios.