Cybersecurity Home Lab Setup Running Active Directory (Oracle VirtualBox & Windows PowerShell)

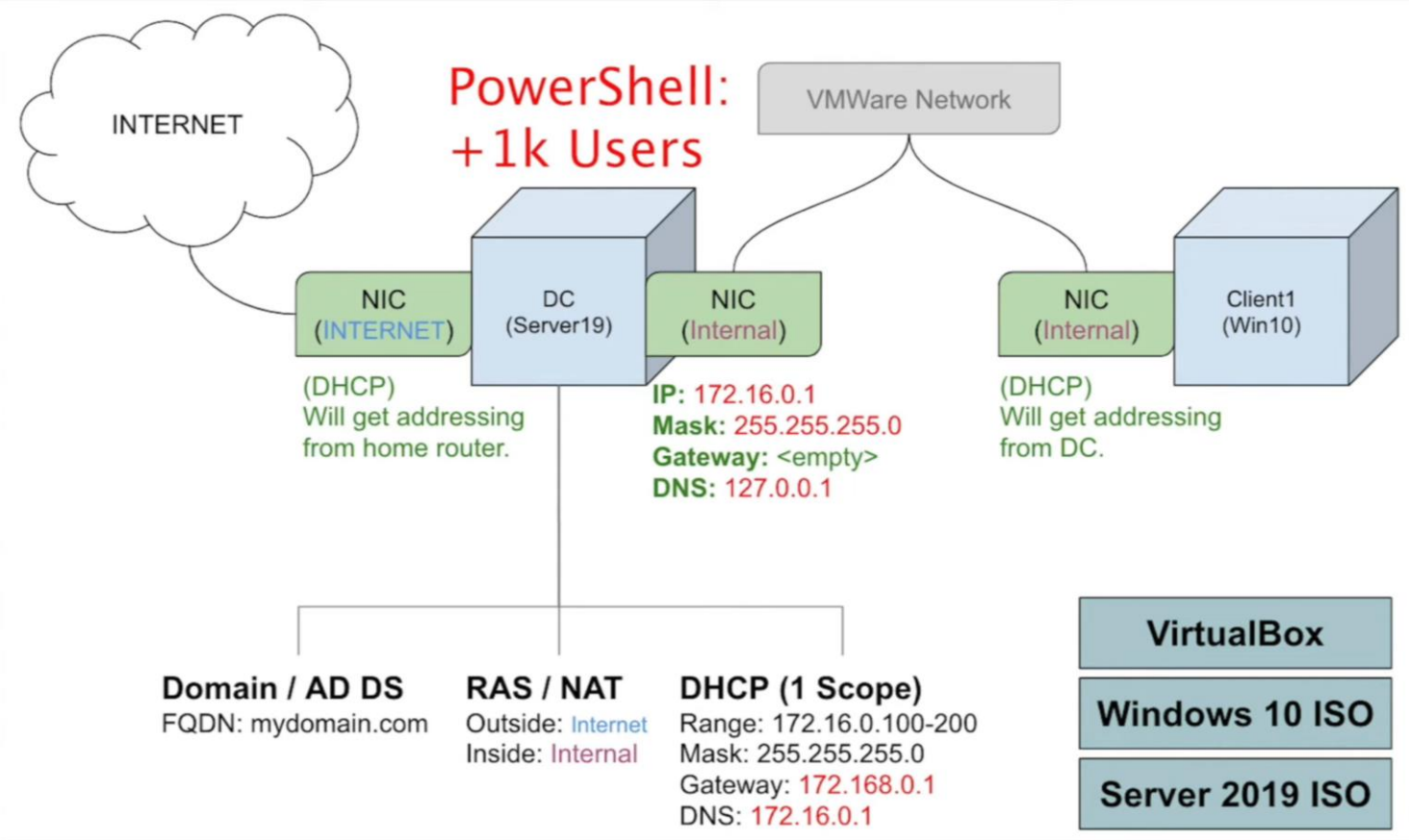
By: Ahoura Minaeian

Abstract

This project involves creating a virtualized environment using Oracle VirtualBox to host a Windows Server 2019 virtual machine configured as a Domain Controller with Active Directory. The lab also includes automating user account creation using PowerShell scripts. This setup provides a controlled platform to practice and understand enterprise-level network configurations, user management, and scripting for administrative tasks.

Objective

Establish a virtualized home lab environment using Oracle VirtualBox and Windows Server 2019 to simulate an Active Directory (AD) domain. This setup is ideal for practicing cybersecurity tasks such as user management, group policies, and PowerShell scripting.



- Visual overview of the project and all the included elements providing an insight as to how educational and/or corporate offices network environments would look like.

Prerequisites

- A host machine with at least 8 GB of RAM (16 GB recommended) and sufficient storage space.
- Oracle VirtualBox installed.
- Windows Server 2019 ISO file (available from Microsoft's official website).
- Optional: Windows 10 ISO for client machine setup.

Part I: Oracle VirtualBox Installation & Setup

- Download and install Oracle VirtualBox and its extension pack from the official Oracle website.
- Download Windows Server 2019 ISO from the official Microsoft website.
- Open VirtualBox and click on "New"
    - Name the VM “AD-Server" and select "Microsoft Windows" as the type and "Windows 2019 (64-bit)" as the version.
    - In the advanced tab:
        - In General:
            - Change the Shared Clipboard to: Bidirectional
            - Change Drag’n’Drop to: Bidirectional
                - ➔ This setting allows control between the computer and the VM
        - In Network:
            - Set Adapter 1 to NAT
                - ➔ This connects to the home internet
            - Set Adapter 2 to Internal Network
    - Allocate at least 2 GB of RAM.
    - Create a virtual hard disk (VDI) with at least 20 GB of storage
    - Attach the Windows Server 2019 ISO to the VM's optical drive

Part II: Install Windows Server 2019

- Start the VM and follow the on-screen instructions to install Windows Server 2019.
- Choose the "Desktop Experience" version for a GUI interface.
- Set a strong administrator password when prompted.
    - As this is a home lab project, you may choose a simple password like “Password1”

Part III: Configuration of Systems & Network Settings

- In Network Connections settings
    - Find the network connected to home internet (home IP) and rename it “Internet”
    - The other network that is not connected to home internet should be renamed “Internal”
        - Assign IP to the network by:
            - Right click → Properties → Change IPv4 (double click) → Use the following IP Address → IP: 172.16.0.1 | Subnet Mask: 255.255.255.0 | Preferred DNS Server: 127.0.0.1 (Automatic Self Pinging) → Click OK and exit
- In Settings, rename the PC by going into the “about” section and clicking “Rename this PC”:
    - Rename it “DC” for Domain Controller
    - Restart the PC by clicking the “Restart Now” pop-up option

Part IV: Active Directory Domain Services (AD DS) Installation

- On Server Manager dashboard:
  - Select “Add roles and features”
  - Click “Next” until the Server Selection tab and select the one main server and click “Next”
  - In Server Roles tab:
    - Select Active Directory Domain Services and click “Add Features” when prompted
  - Click “Next” twice and then “Install”
  - After installation is complete, on the top right of the Server Manager dashboard, click the yellow tab to continue with “Post-deployment Configuration”:
    - Click “Promote this server to domain controller”
    - Select “Add a new forest” → type “mydomain.com” in the Root domain name
    - Click “Next” → enter password (Password1) → Continue clicking “Next” until install becomes available and the install.
  - Computer will restart
  - Sign in again and go to start menu
    - In the Windows Administrative Tools select Active Directory Users and Computers
    - Right click on mydomain.com and add a new Organizational Unit
    - Rename it to _ADMINS and uncheck “protect container from accidental deletion” and click “OK”
    - On the newly created _ADMINS folder, right click → New → User
      - Enter personal first/last name
      - User logon name: a-first/last name (e.g. a-aminaeian)
      - Enter password (Password1)
        - ➔ Uncheck “User must change password at next logon”
        - ➔ Check “Password never expires”
        - ➔ Click “Next” and “Finish”
    - Right click the new account → properties → select “Member Of” tab → click “add” → type “Domain Admins” → click “Check names” → click “Ok”
  - Sign out and sign in through other account with newly created admin account

Part V: RAS / NAT Installation

- On Server Manager dashboard:
  - Select “Add roles and features”
  - Click “Next” until the Server Selection tab and select the one main server and click “Next”
  - In Server Roles tab:
    - Select Remote Access
      - In the Role Services tab → select “Routing” → “Add Features”
  - Click “Next” until “Install”
  - Click “Close” after installation
  - Click on “Tools” on the top right of the dashboard → Routing and Remote Access
    - Right click on “DC (local)” → Configure and Enable Routing and Remote Access → Select NAT → Select Internet → Finish
    - DC (local) should have gone green indicating proper configuration

Part VI: DHCP Setup

- On Server Manager dashboard:
  - Select “Add roles and features”
  - Click “Next” until the Server Selection tab and select the one main server and click “Next”
  - In Server Roles tab:
    - Select Remote Access
      - In the Role Services tab → select “DHCP Server” → “Add Features”
  - Click “Next” until “Install”
  - Click “Close” after installation
  - Click on “Tools” on the top right of the dashboard → DHCP
    - Drop down dc.mydomain.com → Right click IPv4 → New scope → name the scope after the desired IP range “172.16.0.100-200”
      - Start IP Address: 172.16.0.100
      - End IP Address: 172.16.0.200
      - Length: 24
      - Subnet Mask: 255.255.255.0
    - Click “Next” until Router (Default Gateway):
      - IP Address: 172.16.0.1 → click “Add” on its right
    - Click “Next” → Domain Name and DNS Servers:
      - Remove listed IP and replace with:
        - → IP: 172.16.0.1 → Add
    - Click “Next” until “Finish”
    - Right click dc.mydomain.com and select “Authorize” → right click on IPv4 and select “Refresh”
      - Both IPv4 and IPv6 should now be green

Part VII: Creating Users in Active Directory via PowerShell

- On Server Manager dashboard:
  - Disable IE Enhanced Security Configuration
    - Turn off both options
- Copy and extract the PowerShell files needed from desktop to VM via GitHub link
  - Open the names file and add your own name (Ahoura Minaeian)
  - Close the file
- From start menu → Run Windows PowerShell ISE via Run as administrator
  - Open the extracted folder and select “1_CREATE_USERS” to import the script
  - Before running the script → remove restrictions by running:
    - Set-ExecutionPolicy unrestricted
    - Press Enter
  - Change the directory in order to successfully run the script
    - cd C:\User\a-aminaeian\Desktop\AD_PS-master
    - Press Enter
  - Select Run and let the users be imported and created → Domain with new users setup is done

Part VIII: Testing & Validation

- Create a new VM on VirtualBox for clients with the same physical requirements as before
    - Open VirtualBox and click on "New"
        - Name the VM “Client1" and select "Microsoft Windows" as the type and "Windows 2019 (64-bit)" as the version.
    - Allocate at least 2 GB of RAM.
    - Create a virtual hard disk (VDI) with at least 20 GB of storage.
    - Attach the Windows Server 2019 ISO to the VM's optical drive
    - In the advanced tab:
        - In General:
            - Change the Shared Clipboard to: Bidirectional
            - Change Drag’n’Drop to: Bidirectional
                - ➔ This setting allows control between the computer and the VM
        - In Network:
            - Set Adapter 1 to Internal Network
- Double click and power on the Client1 VM
    - Setup and install but choose Windows 10 Pro during the setup process
- After installation is finished:
    - Log in to the Windows 10 Pro client using one of the newly created domain user accounts.
    - Verify access to domain resources and apply group policies as needed.
        - In command prompt, run:
            - ipconfig /renew
            - ipconfig
                - ➔ This tests out whether our IP configuration is working
        - In System Settings → About → Rename this PC (advanced):
            - Computer name: Client1
            - Member of → Domain:
                - ➔ mydomain.com
                - ➔ use domain credentials
        - On Server Manager dashboard:
            - Tools → DHCP panel → Scope → Address Leases
                - ➔ DHCP has assigned an address to client computer automatically
            - Tools → Active Directory Users and Computers → mydomain.com (drop down) → Computers
                - ➔ Client1 shows as a computer type

Final Thoughts

Setting up a home lab with Active Directory provides hands-on experience crucial for understanding enterprise environments. It allows you to practice user and group management, understand domain structures, and automate tasks using PowerShell. This foundational knowledge is invaluable for aspiring cybersecurity professionals.

Project Outcome

The successful completion of this project resulted in a fully functional, isolated virtual lab that simulates a real-world corporate IT environment. Through the setup of a Windows Server 2019 Domain Controller, the implementation of Active Directory, and the automation of user account creation via PowerShell, valuable hands-on experience was gained in core areas of system administration and cybersecurity. This environment provides a practical foundation for exploring advanced topics such as group policy management, network segmentation, and domain security. Overall, the project enhanced technical proficiency and reinforced critical skills necessary for entry-level roles in IT support and cybersecurity.