Project Name: BlueWatch Lab

1. VirtualBox Network Configuration

- **Configure NAT Network in VirtualBox:**
  1. Open VirtualBox Network Manager.
  2. Create a NAT Network.
  3. Configure network properties (IP range: 192.168.10.0/24).
  4. Enable DHCP.
  5. Set DHCP address bounds.
  6. Save configuration.
- **Explanation:**
  - Creates a private network for VMs with internet access.
  - NAT allows VMs to access the internet through the host.
  - DHCP automatically assigns IP addresses to VMs.

2. Splunk Installation

- **Splunk Installation:**
  - Download the Splunk installer from the Splunk website.
  - Run the installer for your OS (Windows, Linux, macOS).
  - Follow the installation prompts, providing admin credentials.
  - Access Splunk web interface via http://<your_host_machine>:8000.
- **Explanation:**
  - Splunk is used for collecting and analyzing machine-generated data.
  - Installation allows ingesting data for insights and troubleshooting.

3. Setting a Static IP Address on Ubuntu

- **Setting a Static IP Address on Ubuntu:**
  - Edit the Netplan configuration file. For example:

    ```
    sudo nano /etc/netplan/00-installer-config.yaml
    ```

  - Configure the file with the desired static IP address, subnet mask, gateway, and DNS settings.
  - Based on the screenshot, the configuration should look like this (but verify with your specific network setup):

    ```
    network:
     version: 2
     renderer: networkd
     ethernets:
       enp0s3: #  <--  Your network interface name might be different (e.g., ens33)
       dhcp4: no
    ```

```
    addresses: [192.168.10.10/24]  #  <--  Your desired static IP and subnet
    gateway4: 192.168.10.1      #  <--  Your network's gateway IP
  nameservers:
    addresses: [8.8.8.8, 8.8.4.4]  #  <--  DNS servers (Google's, in this example)
```

- Apply the changes:

```
sudo netplan apply
```

- **Explanation:**
  - By default, Ubuntu might use DHCP, resulting in a dynamically assigned IP.
  - Setting a static IP ensures the server has a consistent and predictable address, which is often necessary for server applications like Splunk.

4. Troubleshooting Static IP Configuration on Ubuntu

- **Problem:** After setting a static IP address, the system also obtains a DHCP-assigned IP address.
- **Possible Causes:**
  - Incorrect Netplan configuration.
  - DHCP client service is still active.
- **Solution:**
  1. **Verify Netplan Configuration:**
     - Ensure the Netplan configuration file (/etc/netplan/*.yaml) has the correct static IP settings and dhcp4: no.
     - Double-check the network interface name (e.g., enp0s3) using ip a.
  2. **Apply Netplan Changes:**

     ```
     sudo netplan apply
     ```

  3. **Reboot:**
     - If the issue persists, reboot the system.
- **Explanation:**
  - This ensures that the system uses the intended static IP address and doesn't rely on DHCP.

5. Downloading Splunk on the Host Machine

- **Download Splunk Enterprise:**
  1. Go to the Splunk website: https://www.splunk.com/?locale=en_us
  2. Navigate to the download section: Products / Free Trials & Downloads / Splunk Enterprise / Get My Free Trial
  3. Log in to your Splunk account (or create one if you don't have one).
  4. Select the download option for Ubuntu (Linux) and download the .deb file.

- **Downloaded File Location:**
  - The Splunk .deb file was saved to the following location: C:\Users\Dell\Downloads\ADS

6. Installing VirtualBox Guest Additions on Ubuntu VM

- **Install VirtualBox Guest Additions:**
  - Open a terminal in your Ubuntu VM.
  - Run the following command:

    ```
    sudo apt-get install virtualbox-guest-additions-iso
    ```

  - You might be prompted to enter your password.
- **Explanation:**
  - This command installs the VirtualBox Guest Additions, which improve integration between the host and the VM (e.g., shared folders, better screen resolution).

7. Configuring Shared Folders in VirtualBox

- Open the VirtualBox settings for your Ubuntu VM.
- Navigate to "Shared Folders".
- Click on the "Add" button (the icon usually looks like a folder with a plus sign).
- In the "Add Share" dialog box:
  - Folder Path: Specify the path to the folder on your host machine that you want to share. In your case, this is C:\Users\Dell\Downloads\ADS.
  - Folder Name: Enter a name for the shared folder as you want it to appear in the VM.
  - Read-only: Check this box if you only want the VM to be able to read files in the shared folder, not write to them.
  - Auto-mount: Check this box to automatically mount the shared folder when the VM starts.
  - Make Permanent: Check this box to make the shared folder settings permanent.
- Click "OK" to save the shared folder settings.

8. Accessing the Shared Folder in Ubuntu

- **After rebooting the Ubuntu VM:**
  - The shared folder should be automatically mounted (if you checked the "Auto-mount" option).
  - By default, shared folders are typically mounted under /media/sf_<shared_folder_name>. In your case, it might be /media/sf_ADS.

- Open a terminal in Ubuntu and navigate to the shared folder:

```
cd /media/sf_ADS
```

- You should now be able to access the files in your shared folder.

9. Installing VirtualBox Guest Utilities on Ubuntu VM

- **Install VirtualBox Guest Utilities:**
  - Open a terminal in your Ubuntu VM.
  - Run the following command:

```
sudo apt-get install virtualbox-guest-utils
```

  - You might be prompted to enter your password.
- **Reboot the Ubuntu VM:**

```
sudo reboot
```

- **Explanation:**
  - This command installs the VirtualBox Guest Utilities, which provide additional utilities and tools for better integration between the host and the VM (e.g., improved clipboard sharing, seamless window management, and time synchronization).

10. Post-Reboot Configuration for Shared Folders

- **Add user to the vboxsf group:**
  - This step adds your user to the group that has permissions to access shared folders.
  - Open a terminal in your Ubuntu VM and run the following command, replacing decjag with your actual username:

```
sudo adduser decjag vboxsf
```

- **Create a mount point directory (if it doesn't exist):**
  - This is the directory where the shared folder will be mounted in your Ubuntu VM. You can create it with any name and in any location where you have write permissions.
  - In a terminal, run the following command. In this example, the directory is named share and is created in the user's home directory:

```
mkdir ~/share
```

11. Mounting the Shared Folder

- To make the shared folder accessible, you need to mount it to the directory you created (the mount point).
- Open a terminal in your Ubuntu VM and run the following command.
- Replace ADS with the name of your shared folder as it is defined in VirtualBox.
- Replace sharedj/ with the path to the directory where you want to mount the shared folder.
  sudo mount -t vboxsf -o uid=1000,gid=1000 ADS sharedj/

12. Installing Splunk from the Shared Folder

- **Navigate to the shared folder:**
  - Open a terminal in your Ubuntu VM.
  - Change the current directory to the location where you mounted the shared folder. Based on previous steps, this is likely:

  cd ~/share

- **List the contents of the shared folder:**
  - To verify that the Splunk installer is present, list the files in the directory:

    ls -la

  - You should see the Splunk .deb file that you downloaded.
- **Install the Splunk package:**
  - Use the dpkg command to install the Splunk package. Replace splunk-<version>-<build>-Linux-x86_64.deb with the actual name of the Splunk .deb file.

    sudo dpkg -i splunk-<version>-<build>-Linux-x86_64.deb

  - The installation process will take some time. You'll see output in the terminal as Splunk is installed. It will ask for your input.

13. Post-Installation Configuration

- **Navigate to the Splunk installation directory:**
  - Open a terminal:

  cd /opt/splunk

- **Verify user and group ownership:**
  - List the files and directories and check their permissions:

    ls -la

    - You should see that the user and group ownership is set to splunk.
- **Switch to the Splunk user:**
    - Use sudo to execute a shell as the splunk user:

      sudo -u splunk bash

    - You are now in a new shell session as the splunk user.
- **Start Splunk:**
    - Navigate to the Splunk bin directory:

      cd bin

    - Start Splunk:

./splunk start

14. Enable Splunk to Start on Boot

- To configure Splunk to start automatically whenever your virtual machine restarts:
    1. **Exit the Splunk user shell:**

       exit

    2. **Navigate to the Splunk bin directory:**

       cd /opt/splunk/bin

    3. **Enable boot-start for the Splunk service:**

sudo ./splunk enable boot-start -user splunk

15. Installing Windows 10 on VirtualBox

- **Obtain a Windows 10 ISO file:** * Download a Windows 10 ISO file from the Microsoft website.
- **Create a new Virtual Machine in VirtualBox:**
    1. Open VirtualBox.
    2. Click "New".
    3. Name the VM (e.g., "Windows 10").
    4. Select "Microsoft Windows" and "Windows 10 (64-bit)".
    5. Allocate memory (e.g., 4096 MB).
    6. Create a virtual hard disk (VDI), dynamically allocated, with 50 GB space.
    7. Click "Create".
- **Configure the Virtual Machine Settings:**
    1. Select the VM and click "Settings".

2. Go to "Storage".
3. Click the empty CD/DVD icon, then the CD/DVD icon next to "Optical Drive".
4. Select the downloaded Windows 10 ISO file.
5. Go to "Network".
6. Select "NAT" for the network adapter.
7. Click "OK".

- **Start the Virtual Machine and Install Windows 10:**
  1. Start the VM.
  2. Follow the Windows 10 installation instructions.
  3. Once complete, Windows 10 will start.

16. Configuring the Windows 10 Virtual Machine's IP Address

- **Change the PC name (Optional):** * To change the Windows 10 VM's name: * Open "Settings" in Windows 10, go to "System" -> "About", and click "Rename this PC". Enter a new name and restart.
- **Open Command Prompt:** * Search for "cmd" in the Start menu.
- **Check the current IP address:** * In the Command Prompt, type ipconfig and note the "IPv4 Address" (e.g., 192.168.10.8).
- **Configure a static IP address:**
  1. Open "Network & Internet Settings" (right-click the network icon in the system tray).
  2. Click "Change adapter options".
  3. Right-click your Ethernet adapter (e.g., "Ethernet") and select "Properties".
  4. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".
  5. Select "Use the following IP address" and enter:
     - IP address: 192.168.10.100
     - Subnet mask: 255.255.255.0
     - Default gateway: 192.168.10.1
  6. For "Preferred DNS server", enter 8.8.8.8.
  7. Click "OK".

17. Verifying Splunk is Running

- **From your Windows 10 VM, open a web browser.**
- **In the address bar, type the following URL:** 192.168.10.10:8000
- **Explanation:**
  - 192.168.10.10 is the static IP address you assigned to your Ubuntu VM.
  - 8000 is the default port that Splunk uses for its web interface.
- **If Splunk is running correctly, you should see the Splunk login page.**
- **Log in with your Splunk credentials.** * This will be the username and password

you set during the Splunk installation process on Ubuntu.

- **Important Note:** * The Ubuntu VM where Splunk is installed must be running for you to access the Splunk web interface. If the Ubuntu VM is shut down or Splunk is not running, you will not be able to connect.

18. Installing Splunk Universal Forwarder on Windows 10

- **Download Splunk Universal Forwarder:**
  - On your Windows 10 VM, use a web browser to go to the Splunk website.
  - Log in with the same Splunk credentials you used to install Splunk Enterprise on Ubuntu.
  - Navigate to the download section and download the Splunk **Universal Forwarder** for Windows (64-bit in your case).
- **Run the Splunk Universal Forwarder installer:**
  - Locate the downloaded installer and run it.
- **Follow the installation steps:**
  1. **Accept license agreement.**
     - Why? To agree to Splunk's terms.
  2. **Set deployment settings:**
     - Enter Splunk Enterprise (indexer) IP and port: 192.168.10.10:9997.
     - Set username and password.
     - Why? To tell the forwarder where to send data. Port 9997 is the default.
     - Why no deployment server? We're configuring manually for a simple setup.
     - **What does a Splunk forwarder do?** It collects data from various sources on a machine, like logs and system metrics, and sends it to a Splunk Enterprise instance for centralized analysis.
  3. **Click "Install."**
     - Why? To copy files and begin installation. * **Splunk Universal Forwarder Installation Complete:**
- The forwarder is now on your Windows 10 machine, configured to send data to your Splunk Enterprise instance on Ubuntu.

19. Installing and Configuring Sysmon

- **Download and configure Sysmon:**
  - Download Sysmon from the Sysinternals website.
  - Download the Sysmon configuration (e.g., sysmonconfig.xml) from a trusted source (like the one provided), ensuring you download the raw file.
  - Save the configuration file (e.g., to C:\Users\DJ\Downloads).
  - Extract the Sysmon zip file to a directory (e.g.,

C:\Users\DJ\Downloads\Sysmon).
- Open Windows PowerShell as an administrator.
- Run these commands (adjust paths if needed):

```
cd C:\Users\DJ\Downloads\Sysmon
.\Sysmon.exe -i ..\sysmonconfig.xml
```

- cd C:\Users\DJ\Downloads\Sysmon: Navigates to the extracted Sysmon directory.
- .\Sysmon.exe -i ..\sysmonconfig.xml: Installs Sysmon and applies the configuration file. The ..\ assumes the config is in the parent directory (Downloads). Adjust the path if it's elsewhere.

20. Configuring Data Inputs for Splunk

- To configure what data the Splunk server receives:
  1. **Create a new input.conf file:**
     - Do **NOT** modify the original input.conf file.
     - Open Notepad in administrator mode.
     - Copy and paste the following configuration:

```
[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
```

     - Save the file to this location: C:\Program Files\SplunkUniversalForwarder\etc\system\local\input.conf
  2. **Modify the Splunk Forwarder service:**
     - Open the Windows Services application.
     - Find the "SplunkForwarder" service.
     - Double-click on the "SplunkForwarder" service.
     - Go to the "Log On" tab.
     - Select "Local System account".

        - Click "OK" on the warning message.
        - Verify that the "SplunkForwarder" service is running as "Local System".
    3. **Restart the Splunk Forwarder service:**
        - Restart the "SplunkForwarder" service to apply the changes to the input.conf file.

21. Configuring Splunk Enterprise

- **Access Splunk Enterprise:**
    - On your Windows VM, open a web browser and go to: 192.168.10.10:8000
    - Enter your Splunk username (e.g., "decjag") and password.
- **Configure Splunk Indexes:**
    1. Go to "Settings" and click on "Indexes".
    2. Click on "New Index".
    3. In the "Index Name" field, type endpoint.
    4. Save the new index.
- **Configure Receiving Port:**
    1. Go to "Settings" and click on "Forwarding and receiving".
    2. Click on "Configure receiving".
    3. Click on "New receiving port".
    4. In the "Port" field, enter 9997 (the same port used by the forwarder).
    5. Save the port configuration.
- **Verify Data Ingestion:**
    1. Go to "Apps" and select "Search & Reporting".
    2. In the search bar, type index=endpoint.
    3. Click on "Host" in the search results.
    4. You should see your Windows VM's hostname (e.g., "DJ"), indicating that data is being received.

22. Installing Windows Server

- **Download Windows Server:**
    - You can download Windows Server from the official Microsoft website: https://info.microsoft.com/ww-landing-windows-server-2022.html
    - Click on the download button.
- **Installation:**
    - During the installation process, check the box for "Untended installation".
    - Choose "Windows Server (Desktop Experience)" as the installation option.
    - The rest of the installation process is similar to Windows 10.
    - After installation on the lock screen, use Ctrl+Alt+Delete to unlock.

23. Configuring Windows Server

- **Setting a Static IP Address:**
  - Set a static IP address of 192.168.10.7 on the Windows Server.
  - The steps to do this are the same as in Windows 10 (see section XIX).
  - Before, the IP address was 192.168.10.9, and now it should be changed to 192.168.10.7.
- **Adding Roles and Features:**
  - Open Server Manager.
  - In the top right corner, click "Manage" and select "Add Roles and Features".
  - In the "Installation Type" section, choose "Role-based or feature-based installation" and click "Next".
- **Troubleshooting the missing IP:**
  - You might encounter an issue where you cannot see 192.168.10.10. To resolve this:
  - The problem is likely that the server is trying to register its connection in DNS, but since its not a domain controller, it fails.
  - Open the properties of the network adapter and uncheck "Register this connection's address in DNS".

24. Setting up Active Directory Domain Services

- After choosing your server in Server Manager, click "Active Directory Domain Services" and then "Add Features". Continue until you find the "Install" button and click it.
- Once the installation is complete, a flag icon will appear in the top right corner. Click it and select "Promote this server to a domain controller".
- In the configuration wizard, select "Add a new forest". Enter your desired domain name (e.g., "decjag.dj") and click "Next".
- Keep the default settings and enter a strong password when prompted. Click "Next" through the remaining options until you find the "Install" button.
- The server will automatically reboot. After the reboot, you should see "DECjag\Administrator" on the lock screen, indicating that you are now logged in to the domain.

25. Creating Users and Groups in Active Directory

- **Open Active Directory Users and Computers:**
  - Click on "Tools" and select "Active Directory Users and Computers".
  - This tool allows you to create and manage users, computers, and groups.
- **Create Organizational Units (OUs):**
  - To organize your users and groups (mimicking real-world scenarios), right-click on your domain (e.g., "decjag.dj") in the left pane.

    - Select "New" and then "Organizational Unit".
    - Enter a name for the OU (e.g., "IT") and click "OK".
- **Create Users within OUs:**
    - In the left pane, right-click on the "IT" OU you just created.
    - Select "New" and then "User".
    - Enter the user's details (e.g., first name: "Jenny", last name: "Smith"). The "User logon name" (e.g., "jsmith") will be used for login.
    - Set a strong password for the user. You might get a warning if the password is not strong enough.
    - Click "Next" and then "Finish" to create the user.
- **Create another OU and user:**
    - Follow the same steps to create another OU (e.g., "HR") and a user within that OU (e.g., "Terry Smith").

26. Joining Windows 10 to the Domain

- **On your Windows 10 VM:**
    - Open "Settings" and go to "About".
    - Click on "Advanced system settings".
    - Go to the "Computer Name" tab and click "Change".
    - In the "Computer Name/Domain Changes" dialog box, select "Domain" and enter your domain name (e.g., "decjag.dj").
- **Resolve Domain Join Errors:**
    - If you encounter a "domain could not be found" error, it's likely a DNS issue.
    - To fix this, go to "Network and Sharing Center" -> "Change adapter settings".
    - Right-click on your Ethernet adapter and select "Properties".
    - Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".
    - Change the "Preferred DNS server" to the IP address of your Windows Server (e.g., "192.168.10.7"). This ensures that the Windows 10 VM can resolve the domain name.
    - Click "OK" to save the changes.
- **Verify DNS Configuration:**
    - Open Command Prompt and type ipconfig /all.
    - Check the output for "DNS Servers". It should now show "192.168.10.7" as the DNS server.
- **Join the domain:**
    - Go back to the "Computer Name / Domain Changes" dialog box.
    - Once your lab environment is fully set up:
        - At the Windows 10 lock screen, click on **Other User**.
        - Login using:

- **Username:** jsmith
- **Password:** *(the one you configured in Windows Server)*

🛡️ *Next Step: Brute Force Attack Simulation*

After completing the sandbox setup:

- *Launch **Kali Linux**.*
- *Perform a **brute-force attack** targeting the Windows 10 machine.*
- *Purpose:*
  *➔ To verify that **Splunk** and **Sysmon** are properly capturing and logging the attack events.*

Note 😁 for next step you have go next file name (attack_time)