**Active Directory Project - Step-by-Step Guide**

**1. Logical Diagram Creation**

* Before building your infrastructure, start by designing a clear **logical diagram** outlining the structure of your network. This should include all key components such as your **Windows Server**, **Ubuntu**, **Windows 10**, **Kali Linux** instances, and their relationships with one another.
* **Pro Tip**: Use a consistent IP scheme to avoid conflicts later during the configuration process. Refer to your diagram as you proceed to ensure the setup mirrors the design.

**2. Setting Up Virtual Machines**

* Download and install **Ubuntu**, **Windows 10**, **Kali Linux**, and **Windows Server** on **VirtualBox**.
* Configure each machine to use a **NAT Network** for seamless internal communication. In VirtualBox:
  1. Click on **Devices** > **Network** > **NAT Network**.
  2. Create a new NAT network and name it (e.g., AD-Network).
  3. Ensure the IP matches the one you set in your logical diagram.
* **Note**: Use the same NAT network for all machines to allow communication between them without exposing them to the internet.

**3. Installing and Configuring Splunk**

* Download the **Splunk** Linux version from the Splunk website and transfer it to the Ubuntu machine using shared folders in VirtualBox.
* Run the following commands to install and configure Splunk:

bash

Copy code

sudo dpkg -i splunk\_package\_name.deb

* + Ensure that Splunk is configured to start at boot:

bash

Copy code

sudo systemctl enable splunk

sudo systemctl start splunk

* After installation, open the Splunk web interface by visiting http://<your-splunk-server-ip>:8000 in your browser.

**4. Configuring Splunk Add-ons and Data Forwarding**

* Install **Splunk Universal Forwarder** on your Windows Server and client machines (e.g., Windows 10). During installation, configure the forwarder to send logs to your Splunk server (using the IP address 192.168.10.10 and default port 9997).

Download and install **Sysmon** on the Windows machines for detailed event logging.

* Copy the Sysmon config file from GitHub and configure it:

bash

Copy code

wget https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig-export.xml

**Insert Screenshot of Sysmon Configuration Download Here**

**5. Configuring Inputs for Splunk**

* Create the inputs.conf file on your Splunk forwarder with the following content to collect logs from **Application**, **Security**, **System**, and **Sysmon** logs:

bash

Copy code

[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

**6. Setting Up Active Directory**

* On the **Windows Server**, open the **Server Manager** and add the **Active Directory Domain Services (ADDS)** role.
* Once installed, click the **flag icon** and promote the server to a **Domain Controller**.
* Choose a new forest and name your domain.
* Set a strong password for the domain controller and complete the ADDS installation.

**7. Creating User Accounts in Active Directory**

* Open the **Active Directory Users and Computers** console.
* Create new **Organizational Units (OUs)** for departments (e.g., HR, IT, etc.).
* Inside each OU, create users by right-clicking, selecting **New > User**, and filling out the required details.

**8. Brute Force Attack Simulation Using Kali Linux**

* On your **Kali Linux** machine, set a static IP address and verify connectivity by pinging your Splunk server and other machines.
* Install **Crowbar**, a tool for brute-force attacks, and use it to simulate an attack on one of the accounts created in Active Directory.
* Capture the brute-force attack logs in Splunk and verify that the events are logged under the **Search & Reporting** app.

**Insert Screenshot of Splunk Capturing Brute Force Logs Here**

**9. Testing with Atomic Red Team**

* On your target Windows machine, install the **Atomic Red Team** framework to simulate real-world adversary techniques.
* Exclude the **C:/** drive in **Windows Defender** to prevent interference.
* Run a specific technique using **PowerShell** as Administrator, and verify that the simulated attack is logged in Splunk.

**10. Finalizing and Verifying Setup**

* Test connectivity between all machines (e.g., ping Google and the Splunk server).
* Ensure that all user login events, security logs, and attack simulations appear in Splunk’s **Search & Reporting** interface.
* Verify that the **Active Directory** setup is functioning by logging in as one of the newly created users.