### **Active Directory Setup**

This is a detailed step by step guide on how I created an Active Directory lab at home.

#### **Network Overview**

In this carefully designed home lab environment, I’ve set up a comprehensive network infrastructure that simulates a small enterprise network while incorporating security monitoring and analysis tools. Let me walk you through the intricate details of this setup.

#### **Network Configuration**

* **Domain**: Home Domain
* **Network Range**: 192.168.10.0/24
* **Total Devices**: 4 key systems

#### **Key Components**

#### **1. Network Router/Switch**

* Central networking device
* Connects all lab components
* Provides internet connectivity
* Enables communication between different network segments

#### **2. Active Directory Server**

* **IP Address**: 192.168.10.7
* Runs Windows Server
* Responsible for:
* User authentication
* Network policy management
* Domain controller functionality
* Hosts Sysmon for advanced system monitoring

#### **3. Splunk Infrastructure**

* **Splunk Server IP**: 192.168.10.10
* Runs Splunk Universal Forwarder
* Central log management and security information and event management (SIEM) system
* Collects and analyzes logs from multiple sources

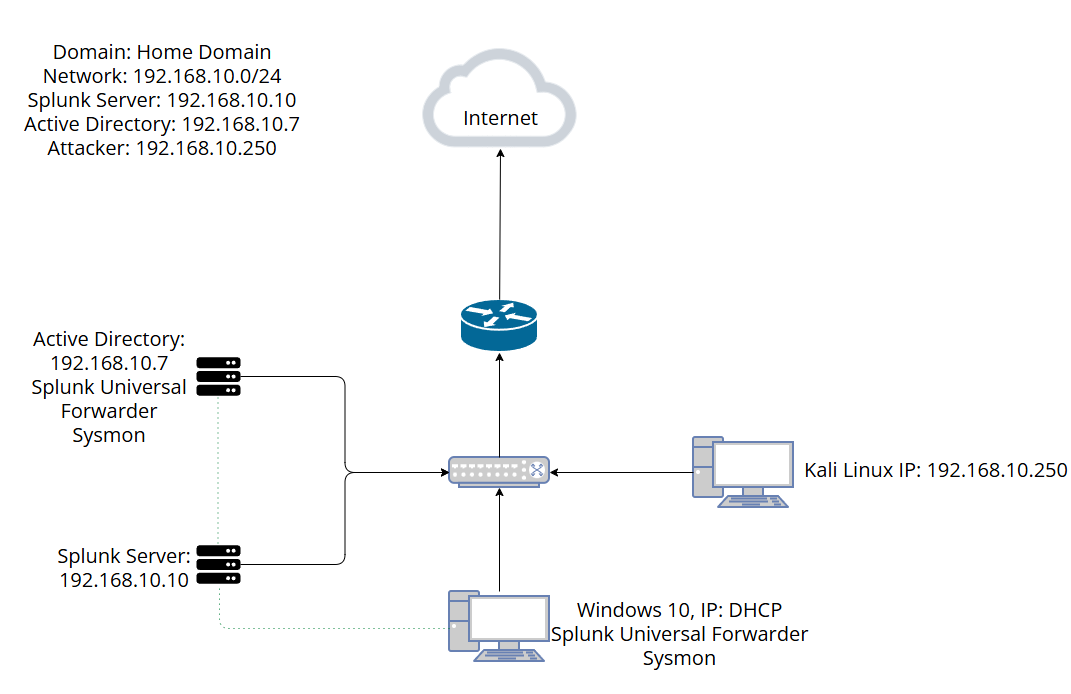
#### **4. Client Machines**

#### **Windows 10 Client**

* IP Address: Dynamically assigned via DHCP
* Runs Splunk Universal Forwarder
* Sysmon installed for detailed system event logging
* Represents a typical enterprise workstation

#### **Kali Linux Machine**

* **IP Address**: 192.168.10.250
* Cybersecurity-focused distribution
* Used for penetration testing and security research
* Potentially simulates an “attacker” perspective in lab scenarios

Network Diagram