Intro

Most organisations are using Active Directory to manage computers, groups, and users. How is this built up and working? In this home lab, I will build a relatively simple home lab, with:

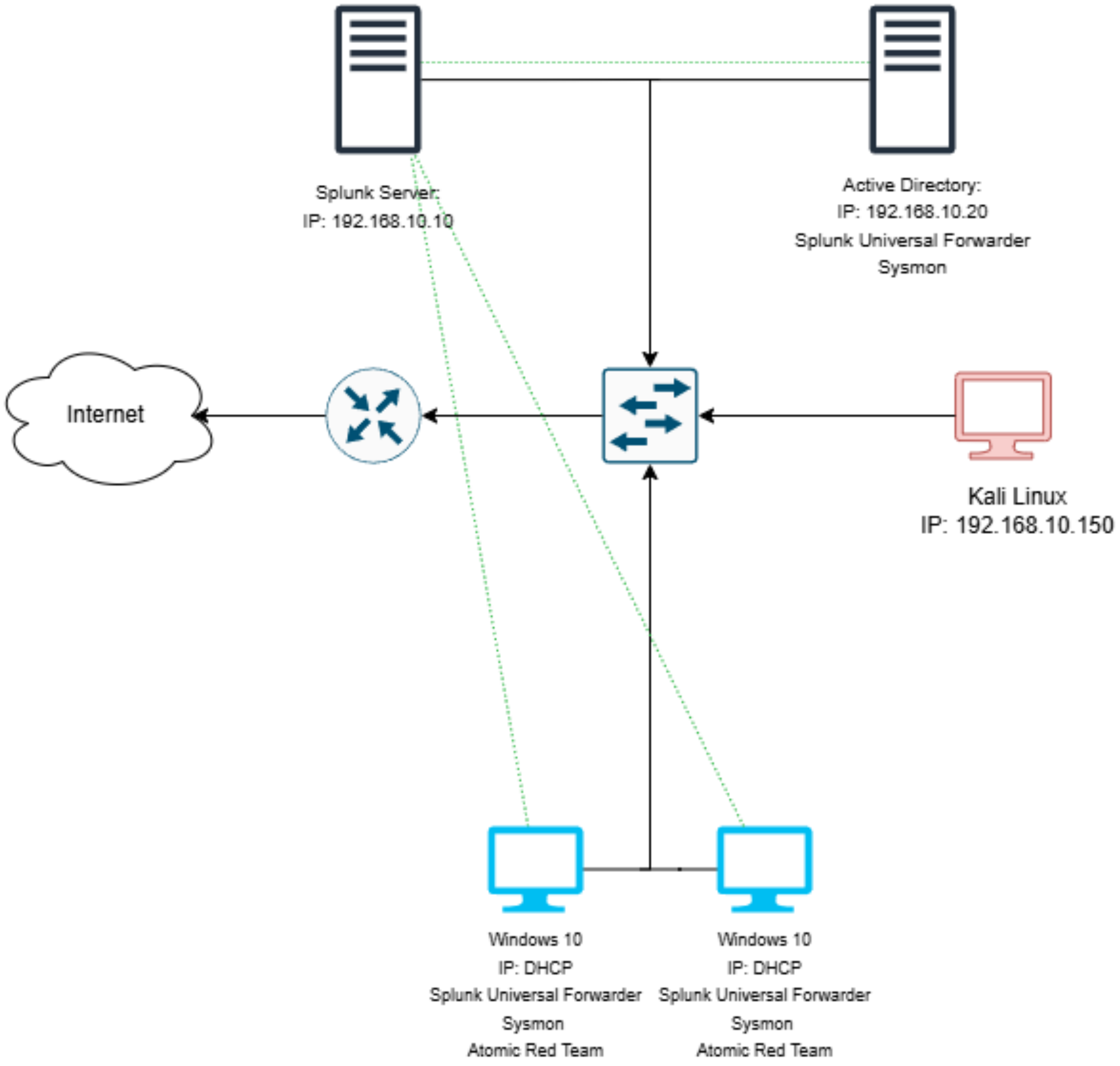
- 2 Windows 10 machines
- 1 Windows Server 2022 ,
- 1 Splunk server,
- 1 Kali Linux attacker machine,
- SySmon for logging,
- Splunk for SIEM.

The main purpose of this home lab is to get familiar with settings, Splunk, "real-world" experience with logging, and real-time searching.

I will use VirtualBox to install these machines in a virtual environment. The Splunk server will be an Ubuntu server. I will install Splunk Universal Forwarder on Win10 machines as well as Active Directory. Sysmon will be installed for logging. I will simulate a brute force attack by the Kali machine and Atomic Red Team to see what kind of telemetry is generated.

This home lab will be divided into multiple parts.

Domain: zero-day
Network:192.168.10.0/24
Splunk Server: 192.168.10.10
Active Directory: 192.168.10.20
Attacker: 192.168.10.150


Splunk Server:
IP: 192.168.10.10
Active Directory:
IP: 192.168.10.20
Splunk Universal Forwarder
Sysmon
Internet
Kali Linux
IP: 192.168.10.150
Windows 10
IP: DHCP
Splunk Universal Forwarder
Sysmon
Atomic Red Team
Windows 10
IP: DHCP
Splunk Universal Forwarder
Sysmon
Atomic Red Team