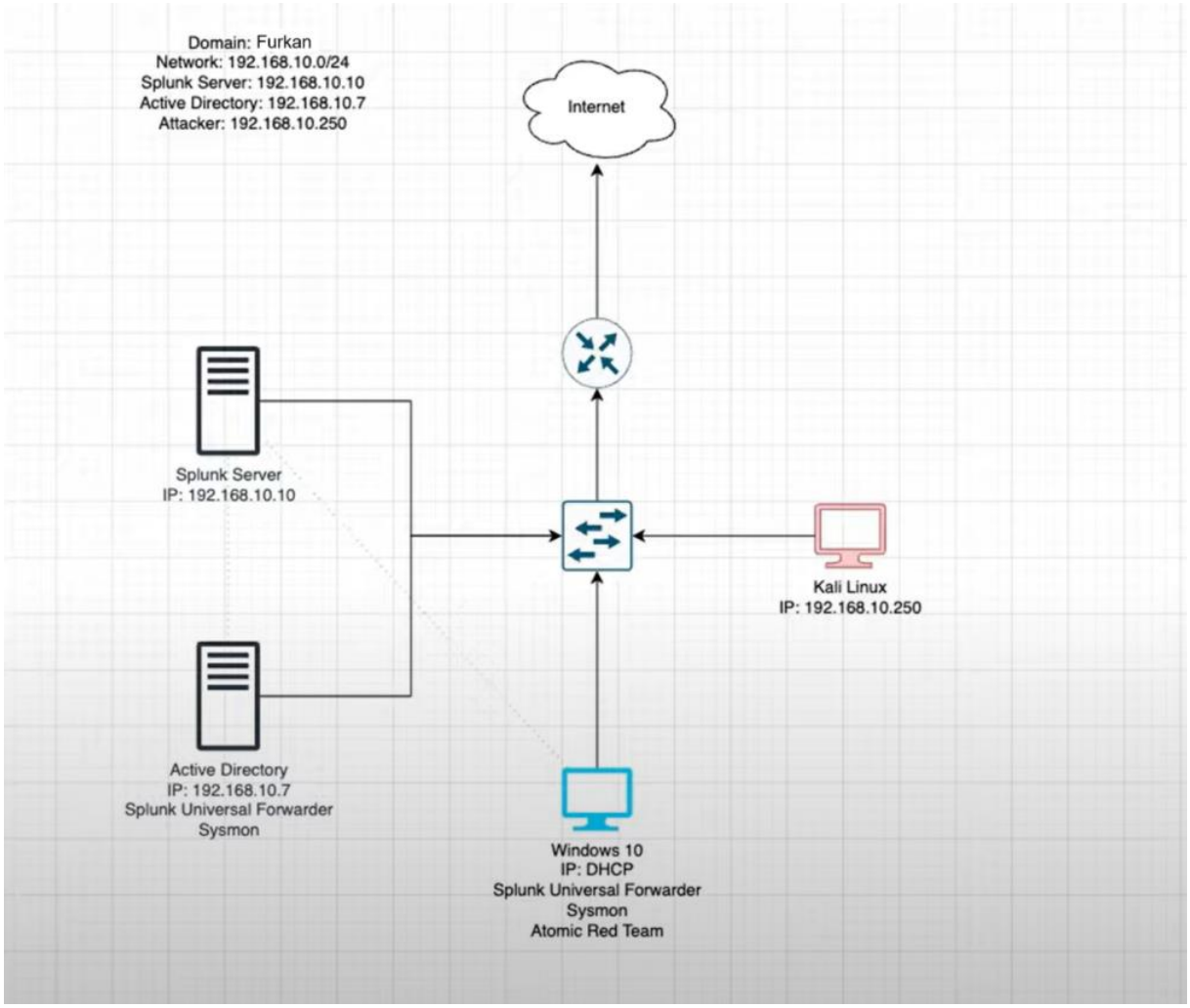

Active Directory Project - Siber Güvenlik İzleme ve Saldırı Simülasyonu

1. Proje Genel Yapısı:

Bu projede, bir Active Directory (AD) ortamında siber güvenlik olaylarını izleme ve saldırı simülasyonları gerçekleştirmek için bir yapı kurulmuştur. Aşağıdaki bileşenler proje kapsamında yer almaktadır:

- **Domain**: Furkan
- **Ağ**: 192.168.10.0/24
- **Splunk Sunucusu**: 192.168.10.10
- **Active Directory (AD) Sunucusu**: 192.168.10.7
- **Saldırgan Makinesi (Kali Linux)**: 192.168.10.250
- **Windows 10 İstemcisi**: DHCP ile IP alan bir sistemdir.

2. Ağ Yapısı:

- **Ağ Topolojisi**: Ağ, bir yönlendirici üzerinden internet bağlantısına sahip ve sistemler arasında trafiğin yönetilmesini sağlayan bir switch ile bağlantılandırılmıştır.
    - **Splunk Sunucusu**: Güvenlik olaylarının toplanmasını sağlayan bir Splunk sunucusu, IP'si: 192.168.10.10.
    - **Active Directory Sunucusu**: Domain yapısını yönetmek için kullanılan ve aynı zamanda Sysmon ve Splunk Universal Forwarder yüklü, IP'si: 192.168.10.7.
    - **Windows 10 İstemcisi**: DHCP ile IP adresi atanmış ve üzerinde Sysmon, Splunk Universal Forwarder ve Atomic Red Team araçları kurulu bir Windows istemci.
    - **Kali Linux**: Saldırı simülasyonu için kullanılan sistem, IP'si: 192.168.10.250.

3. Projenin Aşamaları:

3.1. Splunk Kurulumu ve Yapılandırması

- Splunk sunucusu (192.168.10.10), ağdaki olayların ve logların toplanması amacıyla kurulmuştur.
- **Splunk Universal Forwarder** yazılımı, hem Windows 10 istemcisine hem de Active Directory sunucusuna kurulmuştur. Bu yazılım, cihazlardaki logların Splunk sunucusuna iletilmesini sağlar.

3.2. Sysmon Kurulumu

- **Sysmon (System Monitor)**, Windows makinelerinde güvenlik olaylarını daha detaylı takip edebilmek için kurulmuş bir araçtır. Sysmon, olayları loglayarak Splunk'a gönderen bir sistem izleyicisidir.
- Sysmon, hem Active Directory sunucusuna hem de Windows 10 istemcisine kurulmuştur.

3.3. Atomic Red Team Kurulumu

- Windows 10 istemcisinde, saldırı simülasyonları yapmak amacıyla **Atomic Red Team** kurulmuştur. Bu araç, siber saldırı simülasyonları yaparak güvenlik açıklarının tespit edilmesine ve sistemin bu saldırılara nasıl yanıt verdiğini görmeye olanak sağlar.
- Bu simülasyonlar sayesinde Splunk sunucusu üzerinde güvenlik olayları izlenebilir ve analiz edilebilir.

3.4. Kali Linux ile Saldırı Simülasyonu

- **Kali Linux (192.168.10.250)**, ağ üzerinde saldırgan rolünde yer alır. Bu sistem, çeşitli siber saldırı tekniklerini uygulamak ve AD ortamındaki güvenlik açıklarını test etmek için kullanılır.
- Kali Linux üzerinden gerçekleştirilen saldırılar sonucunda oluşan loglar, Splunk sunucusuna iletilir ve burada analiz edilir.

4. Projenin Hedefi:

Bu proje ile bir Active Directory ortamında gerçek zamanlı güvenlik izleme yapılması ve siber saldırılara karşı savunma yeteneklerinin test edilmesi amaçlanmaktadır. Splunk, Sysmon ve Kali Linux gibi araçlar kullanılarak saldırılar simüle edilebilir ve bu saldırıların sonuçları analiz edilerek sistemin güvenlik açıkları gözlemlenebilir.

5. Ağ Bileşenlerinin Rolleri:

- **Splunk Sunucusu**: Güvenlik olaylarının ve logların toplanması, izlenmesi ve analiz edilmesi için kullanılan merkezi sunucu.
- **Active Directory Sunucusu**: Ağdaki kullanıcıların ve sistemlerin yönetilmesini sağlayan, Sysmon ve Splunk Universal Forwarder ile log toplama görevini üstlenen sunucu.
- **Windows 10 İstemcisi**: Atomic Red Team ile saldırı simülasyonlarının gerçekleştirildiği, Sysmon ve Splunk Universal Forwarder ile logların toplandığı istemci.
- **Kali Linux**: Saldırı simülasyonlarının gerçekleştirildiği saldırgan sistemi.
-

Sonuç olarak

Bu yapıyla, bir Active Directory ortamında güvenlik olaylarının izlenmesi, saldırı simülasyonları ve olay yanıtı süreçlerinin etkin bir şekilde test edilmesi sağlanmaktadır. Splunk, Sysmon ve diğer araçlarla birlikte, gerçek dünyada karşılaşılabilecek tehditlere karşı hazırlıklı olmak ve güvenlik önlemlerini güçlendirmek için önemli bir projedir.