Active Directory Ortamlarında Siber Güvenlik

Sanal Makine Üzerinde Brute-Force Saldırılarının Simülasyonu ve Splunk ile İncelenmesi

Mehmet Furkan KAPLAN – Bilgisayar Mühendisi

Özet

Active Directory (AD), büyük ölçekte kimlik doğrulama ve yetkilendirme işlemlerini yöneten bir teknoloji olup, siber saldırıların sık hedefi haline gelmektedir. Bu makalede, AD ortamına yönelik bir brute-force saldırısının simülasyonu gerçekleştirilmiş ve saldırı Splunk aracılığıyla incelenmiştir. Bu çalışma, AD ve güvenlik izleme sistemlerinin entegrasyonunu anlamaya yönelik kapsamlı bir uygulamayı ele almaktadır. Kullanılan sanal ortamlar ve siber güvenlik araçları detaylandırılarak saldırı analizine dair çıkarımlar yapılmıştır.

Giriş

Active Directory, kullanıcı ve kaynakların merkezi olarak yönetildiği bir sistem olarak, modern kurumsal ağlarda önemli bir yer tutmaktadır. Ancak, AD'nin merkezi yapısı, bir saldırgan için hedeflendiğinde büyük bir potansiyele sahip olabilir. Bu makale, AD ortamının güvenliğinin nasıl test edilebileceğini ve potansiyel saldırılara nasıl yanıt verileceğini göstermek amacıyla tasarlanmış bir proje üzerinden yürütülmüştür. Proje kapsamında sanal makineler üzerinde hem saldırı hem de savunma senaryoları uygulanmıştır.

Yöntem

Bu çalışmada dört farklı sanal makine kurulumu gerçekleştirilmiştir:

1. **Ubuntu Server (Splunk)**: Saldırılar sırasında ağdaki veri akışlarını ve güvenlik olaylarını izlemek için kullanılan Splunk burada barındırılmaktadır. Splunk, geniş çapta veri analizi ve güvenlik izleme sunan bir platformdur.
2. **Windows Server (Active Directory)**: Projenin Active Directory hizmetini sağlamak amacıyla kullanılmıştır. Bu makine üzerinde kullanıcı hesapları ve grup politikaları yapılandırılmış, AD ortamına saldırı düzenlenmiştir.
3. **Windows 10 (Target-PC)**: Kullanıcıların AD ortamına giriş yaptığı ve saldırının hedefi olan bilgisayardır. Bu makine, saldırganın brute-force denemeleri yapması için hedef olarak seçilmiştir.
4. **Kali Linux**: Bu makinede, Target-PC'ye brute-force saldırısı gerçekleştirmek için Crowbar aracı kullanılmıştır. Crowbar, özellikle RDP, SSH ve VNC protokollerine yönelik brute-force saldırıları yapabilen bir araçtır.

Saldırının Gerçekleştirilmesi

Saldırı senaryosu şu şekilde gerçekleşmiştir:

- Kali Linux makinesi, Crowbar aracı kullanılarak Windows 10 (Target-PC) üzerinde Remote Desktop Protocol (RDP) bağlantısı üzerinden brute-force saldırısı düzenlemiştir. Bu saldırı, Active Directory ortamında bulunan bir kullanıcı hesabına yönelik olup, 3389 numaralı port üzerinden gerçekleştirilmiştir.

- Bu brute-force saldırısı, belirli bir kullanıcı adı ve parolayı denemek suretiyle hedef sisteme erişim sağlamaya çalışmıştır. Saldırı sırasında yapılan giriş denemeleri, hedef Windows 10 makinesi ve AD üzerinde güvenlik olayları oluşturmuştur.

Splunk ile İzleme ve Analiz

Saldırılar sırasında ağdaki tüm olaylar Splunk tarafından toplandı ve analiz edildi. Splunk'ın temel amacı, ağ trafiğini ve olay kayıtlarını toplamak, işlemek ve anlamlandırmaktır. Saldırı sırasında kaydedilen güvenlik olayları şunları içerir:

- **Başarısız Giriş Denemeleri**: Brute-force saldırısı sırasında başarısız giriş denemelerinin sayısı hızla arttı. Splunk bu denemeleri güvenlik olayları olarak kaydetti.
- **Aşırı Sayıda Giriş Denemesi**: Splunk, anormal giriş denemelerini algılayarak sistem yöneticisine uyarılar gönderdi.
- **Kullanıcı Kilitleme Olayları**: Birden fazla başarısız giriş denemesi sonrasında, Active Directory politikalarına göre kullanıcının hesabı kilitlendi. Bu olaylar Splunk tarafından tespit edildi ve raporlandı.

Atomic Red Team ile Ek Testler

Saldırının ardından, Atomic Red Team aracı kullanılarak ek güvenlik testi gerçekleştirildi. **Atomic Red Team**, MITRE ATT&CK çerçevesi üzerinden çeşitli siber saldırı tekniklerini simüle edebilen bir araçtır. Bu çalışmada, **T1059.001 (PowerShell Kullanarak Komut Çalıştırma)** saldırı tekniği incelendi.

- **T1059.001 - PowerShell**: Bu teknik, bir saldırganın hedef sistem üzerinde PowerShell komutları çalıştırmasına dayanır. PowerShell, Windows sistemlerinde yaygın olarak kullanılan bir yönetim aracıdır ve saldırganlar tarafından kötüye kullanılabilir. Atomic Red Team aracılığıyla bu saldırı simüle edilmiş ve Splunk tarafından takip edilmiştir. Bu sayede PowerShell tabanlı saldırılarının tespit edilme yöntemleri analiz edilmiştir.

Sonuçlar

Bu proje, bir AD ortamında gerçekleşen siber saldırıların nasıl simüle edilebileceğini ve bu saldırıların Splunk gibi bir güvenlik bilgi ve olay yönetimi (SIEM) platformu kullanılarak nasıl analiz edilebileceğini göstermektedir. Projede gerçekleştirilen brute-force saldırısı ve PowerShell komut çalıştırma teknikleri, gerçek dünyada sıklıkla karşılaşılan tehditlerin simülasyonunu içermektedir.

Splunk’ın bu tür saldırıları tespit etme yetenekleri, olay yanıt sürelerini azaltma ve güvenlik ihlallerini önleme açısından son derece önemlidir. Atomic Red Team kullanılarak yapılan saldırı testleri ise, MITRE ATT&CK çerçevesine dayalı saldırı tekniklerini daha iyi anlamayı sağlamıştır.

Sonuç

Bu çalışma, sanal makine ortamında AD sistemlerine yönelik saldırıları simüle ederek, güvenlik testleri ve saldırı tespiti konusunda derinlemesine bir anlayış sunmuştur. Active Directory ortamlarının güvenliğini artırmak ve siber saldırılara karşı dayanıklılık kazandırmak için Splunk gibi güçlü izleme araçlarının kullanımının önemi bir kez daha vurgulanmıştır.