BİLGİ GÜVENLİĞİ

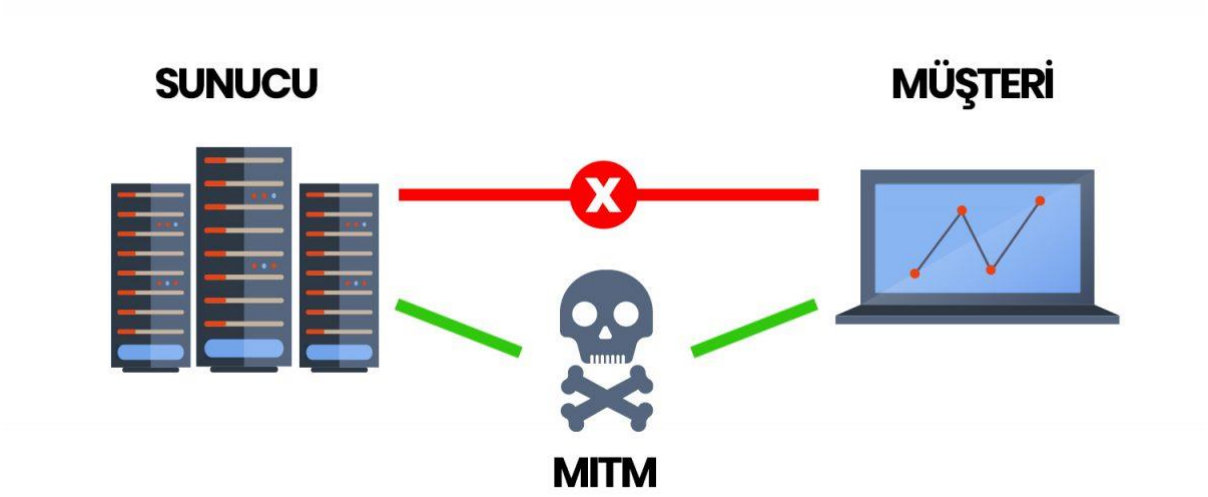
Araştırma Ödevi

Man-in-the-middle saldırısı

Yusuf Seyitoğlu
1030516739@erciyes.edu.tr
1030516739

Man in the middle attack nedir?

Man in the middle saldırısı kötü niyetli biri tarafından bir ağ üzerindeki 2 bağlantı arasında geçen verileri ele geçirmesi ve hatta ele geçirilen veriler üzerinde değişiklik yapmasına ortam sağlayan bir saldırı türüdür



Kablosuz ağlarda paketlerin tümü broadcast olarak yayıldığı için hiçbir ön işlem olmadan tüm paketler saldırgan tarından ele geçirilebilir. Bu yüzden ücretsiz Wi-Fi bulunan ortamlarda bu saldırının gerçekleştirilmesi daha uygundur. Saldırganlar şifrelenmemiş paketlerin verilerine çok kolay bir şekilde ulaşabilir. Ücretsiz Wi-Fi bulunan ortamda olan saldırgan, network trafiğini kendi üzerinden geçirir bu sayede ağdakilerin verileri saldırganın üzerinden geçmeye başlamış olur.

Bu saldırının amacı kişisel verileri, mail şifreleri, banka bilgileri gibi verilere erişmek veya taraflardan birini taklit etmektir. Bu bilgilere erişebilir ve bunları değiştirebilir. Örneğin bankacılık işlemlerini gören bir saldırgan gönderilen hesap numarasını veya girilen para miktarını değiştirebilir.

Saldırgan kişi bu yöntemle başarılı olabilmek için, kurbanı gerçek sunucu yerine Proxy sunucusuna yönlendirmelidir. Aşağıdakiler dâhilinde birçok farklı çeşidi vardır.

1. YEREL AĞ ÜZERİNDE YAPILABİLECEK SALDIRILAR [1]

1.1 ARP poisoning (ARP zehirlenmesi): Saldırgan sahte ARP Request ile kendisini hedef olarak gösterir. Bu sayede gerçek hedefe gitmesi gereken paketler saldırgana gider. Saldırgan MAC Adresini hedef bilgisayarın tablosuna 'Ağ Cihazı MAC Adresi' olarak eşleştirme yaptırır. Trafik bu şekilde kendi üzerinden akmaya başlar.

1.2 DNS Spoofing (DNS önbellek zehirlenmesi, aldatma): DNS zehirlenmesi ya da diğer adıyla DNS önbellek zehirlenmesi en basit tanımı ile bir bilgisayar saldırısıdır. Alan adı sunucusunun önbellek veri tabanına eklenen verilerle ya da oradaki verilerin sabote edilmesi ile birlikte sizin bilgisayarınızın yani istemcinin saldırganın belirlediği ip adresine yönlenmesi sağlanmaktadır ve bu sayede siz istediğiniz siteye giriş yaptığınızı zannederken aslında saldırganın ip adresine yönlendirilmiş olursunuz.

1.3 Port Stealing: Saldırgan, sahte ARP çerçevesi oluşturarak hedef sunucunun MAC adresini kaynak adres olarak kullanır. Switch, kurban bilgisayarın aslında bir saldırganın bağlı olduğu porta bağlı olduğunu sanarak kandırılır. Böylece kurbanın bilgisayarı için gönderilen tüm veri çerçeveleri, saldırganın switch portuna gönderilir.

1.4 STP Mangling:

STP (Spannig Tree Protokol): 7 seviyeli bir OSI modelinde veri bağlantı katmanında yer alan, topolojide döngü oluşmasını engelleyen bir standarttır. İsminden de anlaşılacağı üzere STP karışık ağ yapısının bir ağaç ya da net açıklamak gerekir ise bir topolojiye sahip olmasını sağlayan paketlerin cihazlar arasında sonsuz bir döngüye girmesine engel olmasını sağlar.

Mangling: STP mangling ise STP protokolünün çalışmasını engelleyen ve sürekli topoloji değişim isteği yollayan bir saldırı türüdür.

2. YEREL AĞDAN UZAK AĞA GATEAWAY İLE YAPILABİLECEK SALDIRILAR [1]

2.1 ARP poisoning

2.2 DNS spoofing

2.3 DHCP spoofing: Saldırgan DHCP sunucusu görevi görerek kurban bilgisayarlara IP dağıtır ve gateway olarak kendi adresini verir. Bu şekilde ağ trafiği kendi üzerinden akar.

2.4 ICMP Redirection: Yayınlanan ICMP Redirect mesajları saldırı amacıyla saldırganlar tarafından trafiğini üzerlerine almak için kullanılan saldırı yöntemidir.

2.5 IRDP Spoofing: ICMP Router keşif protokolü, ana bilgisayarın aktif yönlendiricilerin IP adresini keşfetmesini sağlar. Saldırgan, sahte ağdaki IRDP yönlendirici reklam iletisini alt ağdaki ana bilgisayara göndererek varsayılan yönlendiricisini değiştirmesine neden olur.

2.6 Route Mangling: Saldırgan internetteki istemci için en iyi route olduğunu gatewaye sahte paketler yollayarak kandırır. Paketler gatewaye uğramadan doğruca istemciye iletilir.

3.1 DNS Poisoning [1]

3.2 Traffic Tunneling: Saldırganın bir tünel oluşturarak kendisini iç ağa yerleştirmesine olanak tanıyan saldırı türüdür

3.3 Route Mangling

Tespit ve Korunma Yöntemleri

Bu saldırıyı yapan kişiyi bulmak oldukça zordur. Bu yüzden saldırıyı yapan kişiyi bulmak yerine öncelikle saldırıdan korunmak için önlem almak gerekir.

-Saldırıların çoğunun temeli kötü amaçlı yazılımlara dayandığı için virüs koruma yazılımları kullanmak MITM saldırılarının tespiti için uygundur

-Özel Wi-Fi ağlarının kullanılması, Wi-Fi'nin gizlice dinlenmesini önleyebilmektedir.

- Ağ güvenliği açısından herhangi bir olağandışı davranışı tespit etmek veya tanımlamak için trafik kalıpları arada bir analiz edilmelidir. Ağ kullanıcılarının güçlü parolalar seçmesi ve bunları düzenli olarak değiştirmesi sağlanmalıdır. Potansiyel ihlallerin kontrol altına alındığından emin olmak için ağı bölümlere ayırmak önerilir. [2]

- Mümkün olan her yerde çok faktörlü kimlik doğrulama etkinleştirilmelidir.

- VPN kullanmak, MITM saldırılarını önlemeye yardımcı olabilir. VPN'ler verileri İnternet üzerinden iletilirken şifreler. Bu sizi MITM saldırılarına karşı tamamen koruyamaz ama saldırganların işini daha da zorlarlar ve başka kolay hedef aramalarına neden olabilir.

- Kendi Wi-Fi ağınızın güvenliği için zaman zaman tüm bağlı aygıtlardaki tüm varsayılan kullanıcı adlarını ve parolaları güçlü, benzersiz parolalar ile güncellemeniz tavsiye edilir.

Ayrıca tarayıcıları güncel tutmak, SSL/TLS kullanmak, HTTPS bulunmayan web sitelerini ziyaret etmekten kaçınmak MITM saldırılarını önlemek adına yardımcı olabilir.

Kaynakça

[1] [Çevrimiçi]. Available: https://www.beyaz.net/tr/guvenlik/makaleler/ortadaki_adam_mitm_saldirisi_nedir.html.

[2] [Çevrimiçi]. Available: https://www.turhost.com/blog/ortadaki-adam-mitm-saldirisi-nedir/.

[3] [Çevrimiçi]. Available: https://oguzalbastr02.medium.com/ortadaki-adam-sald%C4%B1r%C4%B1s%C4%B1-mitm-detayl%C4%B1-anlat%C4%B1m-5e5f86af1d6a.

[4] [Çevrimiçi]. Available: https://tr.wikipedia.org/wiki/Man-in-the-middle_sald%C4%B1r%C4%B1s%C4%B1.

[5] [Çevrimiçi]. Available: https://www.siberegitmen.com/man-in-the-middle-attack-nedir/.

[6] [Çevrimiçi]. Available: https://fordefence.com/mitm-ortadaki-adam-saldirilari/.