MITM Saldırı Tespit ve Önleme Sistemleri

Şevval CANLI[1] ve Öznur KALAFAT[2]

[1]Bilgisayar Mühendisliği Bölümü, Mimarlık Mühendislik Fakültesi, Nişantaşı Üniversitesi, 34485 İstanbul (20182013053@std.nisantasi.edu.tr)
[2]Bilgisayar Mühendisliği Bölümü, Mimarlık Mühendislik Fakültesi, Nişantaşı Üniversitesi, 34485 İstanbul (20182013067@std.nisantasi.edu.tr)

ÖZET

Gelişen teknoloji ile bilgi güvenliği çok önemli bir unsur haline gelmiştir. Kişisel verilerimizi elde etmek isteyen saldırganlar her geçen gün yeni teknikler keşfetmektedir. En çok kullanılan tekniklerden biri de ortadaki adam (MITM) saldırısıdır. Saldırganlar bu teknikle yerel ağ trafiğini dinleyebilir; kötü amaçlı yazılımlar olmadan ve herhangi bir manipülasyona maruz bırakmadan ağ trafiğindeki kullanıcı verilerini çalabilir. Yeterli kimlik doğrulama güvenliğine sahip olmayan kriptografik sistemlerin çoğu ortadaki adam saldırısına uğrama tehdidi altındadır. Kriptografi kısaca bilginin anlaşılabilir olduğu bir formattan anlaşılamaz bir formata dönüştürülmesidir. Bu çalışmada ortadaki adam saldırısı tekniği açıklanmış, Kali Linux işletim sistemi üzerinde uygulanmıştır. Çeşitli yöntemlerle geliştirilen bu saldırıya yönelik korunma yöntemleri incelenmiştir.

Anahtar Kelimeler: MITM Saldırısı, MITM Savunma Teknikleri, Bilgi Güvenliği, Siber Güvenlik, Siber Suçlar, Kali Linux.

ABSTRACT

With the developing technology, information security has become a very important element. Attackers who want to obtain our personal data are discovering new techniques every day. One of the most used techniques is the man-in-the-middle (MITM) attack. With this technique, attackers can eavesdrop on local network traffic; It can steal user data in network traffic without malware and without subjecting it to any manipulation. Most cryptographic systems that do not have adequate authentication security are at risk of man-in-the-middle attack. Cryptography is the conversion of information from an understandable format to an incomprehensible format. In this study, man-in-the-middle attack technique is explained and implemented on Kali Linux operating system. Protection methods against this attack, which were developed with various methods, were examined.

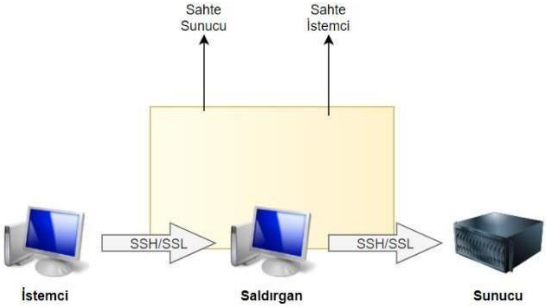
Keywords: MITM Attack, MITM Defense Techniques, Information Security, Cyber Security, Cybercrime, Kali Linux.

I. GİRİŞ

Bilgi güvenliğinde ortadaki adam saldırısı (MITM); saldırganın kullanıcı ile doğrudan iletişim kurabileceği, kullanıcının verilerini gizlice aktarabileceği ve değiştirebileceği bir saldırıdır. Saldırganlar, bir ağ içerisinde hedef ile ağ unsurları (sunucu, switch, router ya da modem) arasında geçen trafiği izleyebilir, sonlandırabilir veya sahte bir iletişim oluşturabilir. Ortadaki adam saldırıları OSI modeli 2.katmanında (Veri Bağlantı Katmanı- Data Link) gerçekleştiği için saldırganlar bu saldırı başarılı olduktan sonra tüm trafiği ele geçirebilir. Bu saldırı güvenlik korumalı olan https trafiğinden güvenlik korumalı olmayan trafiğe kadar gerçekleştirilebilir. [1] MITM saldırısının amacı; kişisel verileri, şifreleri, banka bilgilerini ele geçirmek veya birini taklit etmektir. Örneğin banka bilgilerinin ele geçirilmesiyle oturum açma bilgileri değiştirilebilir ya da istenen kişiye para transferi yapılabilir. Bu yüzden ortadaki adama; ortadaki canavar, ortadaki maymun, ortadaki makine veya ortadaki kişi de denmektedir.

Kablosuz ağlarda paketler tamamen broadcast olarak yayıldığı için ön işleme gerek olmadan tüm paketler saldırgan tarafından yakalanabilir. Bu sebeple ortak kullanım alanlarındaki wi-fi'ler saldırganların vazgeçilmez alanlarıdır. Savunmasız IoT cihazlarının yaygınlaşması ve henüz yeterli güvenliğe sahip olmaması ile bilgilerimiz daha korunmasız hale gelmiştir. Siber saldırılar arasında oldukça kullanılmasına rağmen

güvenlik önlemi en az alınabilen saldırı sistemidir. Bu siber güvenlik tehdidi kullanıcılar haricinde işletmeleri ve kuruluşları da etkilemektedir. Ortak bir erişim noktasını, mesajlaşma hizmetlerini, dosya depolama sistemlerini veya uzaktan çalışma uygulamalarını işletmelerin ağlarına giriş yolu olarak kullanıp birçok bilgi ele geçirilebilir. Casusluk veya finansal kazanç amacıyla yapılan bu saldırılar kablosuz ağlarda önemli bir tehdit oluşturmaktadır. [2] MITM saldırısında, saldırgan hem sunucuyu hem istemciyi taklit eder. İstemciden talep geldiğinde saldırgan kendisini sunucu olarak tanıtır. Sunucuya bağlandığında ise kendisini istemci olarak tanıtır. Her iki oturum da şifrelidir, ancak saldırgan her bilgiyi şifresiz olarak görebilmekte ve komut ekleme yapabilmektedir. Saldırı esnasında istemcide SSH açık anahtarının veya SSL sertifikasının değişmiş olduğu veya güvenilmez olduğu uyarısı gelecektir, saldırı istemcinin soruyu kabul edeceği prensibi ile çalışmaktadır [3].

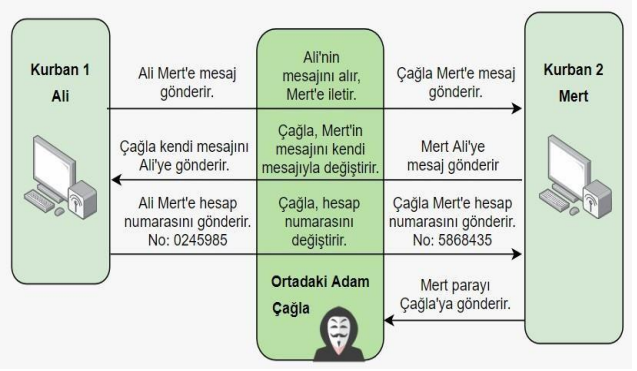


Şekil 1: Bir MITM saldırısında bir saldırganın hem sunucuyu hem de istemciyi taklit etmesi.

Ortadaki adam saldırısı 90'lı yıllardan itibaren kullanılıyor olmasına rağmen günümüzde de oldukça işe yarayan bir yöntemdir. Bu saldırı türü çevrim içi saldırı ve çevrim dışı olarak iki şekilde incelenebilir. Çevrim dışı saldırıda, saldırganlar iki kullanıcının kişisel yazışmalarını okuyabilir ve bu yazışmaları düzenleyebilir. Gerçekleşen saldırıdan iki kullanıcının da haberi olmaz. Ancak bu işlem emek gerektirir.

Çevrim dışı yöntemler yerine çevrim içi bir şekilde yazılım kullanılarak otomatikleştirilmiş yöntemle yapmak daha kolaydır. Çevrim içi ortadaki adam saldırısında dijital donanımlar ve bilgisayarlar kullanılırken çevrim dışında postalar yani yazışmalar kullanılır [5]. Saldırganlar çevrim içi saldırı yöntemini kullanarak halka açık wi-fi üzerinden kullanıcı bilgilerine erişmeye çalışır. Saldırganlar bu bilgilere eriştikten sonra kullanıcı herhangi bir banka web sitesine bağlanırsa bu web sitesi uygun şifreleme sertifikasının olmadığını gösteren bir uyarı yayınlar. Ne yazık ki bazı kullanıcılar bu uyarıyı dikkate almaz ve bilgilerini siteye girmeye devam eder. Aynı zamanda bu saldırganlar bir banka web sitesini taklit ederek kullanıcı bilgilerine erişebilir. Bu sahte banka sunucusuna bağlanıldığında tüm bilgiler direkt olarak ortadaki adam sunucusuna gönderilir. Bu senaryoda şifreleme sertifikası uyarı vermiştir ancak ortadaki adam sunucusu banka ile aynı güvenlik sertifikasına sahip olmamasına rağmen farklı bir yerden güvenlik sertifikası almış olabilir [1]. Son 10 yılda bu senaryoya benzer olaylar daha sık yaşanmaya başlamıştır. Sahte sertifikaların işlenmesi, ortadaki adam saldırılarına yol açmakta ve Stuxnet gibi büyük çaplı siber saldırıları mümkün kılmaktadır. Bu yüzden Sertifika Otorite yetkilerinin dağıtılması için çalışmalar yapılmaktadır. Bu duruma karşı pek çok kuruluş çevrim dışı olarak oluşturdukları kendi Sertifika Otoritesini yönetmeye başlamıştır [6].

Günümüzde MITM gibi siber saldırılar kişisel bilgileri çalma faaliyetlerinden yolcu uçaklarını ele geçirip çeşitli zararlar verene kadar yıpratıcı boyutlara ulaşmıştır.



Şekil 2: Ortadaki adam saldırı senaryosu.

Ortadaki adam (Çağla) kendisini banka gibi gösterecek sahte bir sohbet hizmeti kurar. Hedef (Mert) ile bankaymış gibi sohbet başlatır. Daha sonra gerçek banka sitesinde (Ali) hedefmiş gibi davranır. Saldırgan (Çağla) hedefin (Ali) hesabına erişmek için hesap bilgilerini bankaya iletir. Saldırgan ücreti kendi banka hesabına aktarılmasını sağlar. Kurbanlar her iki uçta da birbirleriyle güvenli bir şekilde iletişim kurduklarını sanarlar. Ali ve Mert bir saldırganın hesabı yerine kendi hesaplarıyla iletişim kurduklarından emin olmalılar. Çeşitli teknikler MITM saldırılarına karşı korunmaya yardımcı olabilir. Kişisel bilgileriniz önemlidir ve her daim korunmaya ihtiyaç duyarlar.

Bu çalışmanın devamında bölüm II ilgili çalışmalar aktarılmıştır. Bölüm III'te MITM saldırı yöntemlerine değinilmiştir. Bölüm IV'te MITM saldırı uygulaması örneği yapılmıştır. Bölüm V'te bu saldırılardan korunma yöntemleri açıklanmıştır. Son olarak bölüm VI'da çalışmanın sonuç kısmına ve önerilere yer verilmiştir.

II. İLGİLİ ÇALIŞMALAR

Ortadaki adam saldırıları başlığı altında literatür çalışması yapılmıştır. Söz konusu literatür araması, 2017-2021 yılları arasında yapılmış olan ve Türkiye'de var olan dergi ve sempozyumlar da yayınlanmış bildirileri, makale ve tez çalışmalarını kapsamaktadır.

Ünlü (2018), internet bankacılığı sisteminde tüketicilerin karşılaşacağı saldırılar ve bu saldırıların çözüm yolları hakkında bir çalışma yapmıştır. Çalışmada internet bankacılığında yapılan saldırıları

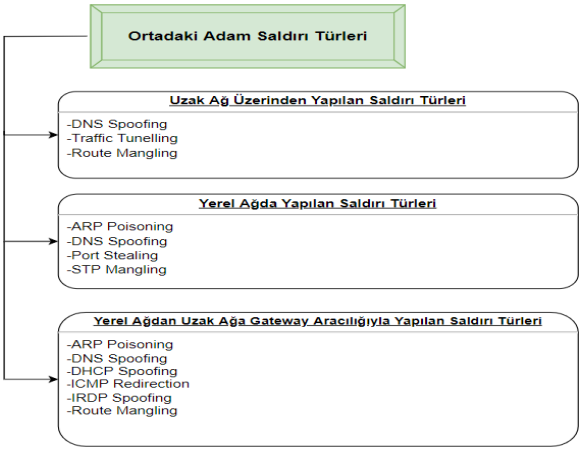
sınıflandırmıştır. Bunlar ortadaki adam saldırısı, uygulama marketlerinden yüklenen sahte internet bankacılığı uygulamaları, sosyal mühendislik çeşitleri (phishing, smishing ve vishing), sim kart yenileme/operatör değişikliği ve spam e- postalar değişikliği eylemleridir [7].

Angin (2020), bir askeri otonom sistem ağındaki İHA'lar ve yer kontrol istasyonları dahil tüm taraflar arasında değiş tokuş edilen mesajların bütünlük güvencesini ve kalıcı bir kaydını garanti eden blokzincir tabanlı bir iletişim mimarisi üzerine bir yöntem önermiştir. Önerilen iletişim mimarisi açısından siber saldırı türlerine dayanıklığı açıklanmıştır. Ortadaki adam saldırısı, gizli mesaj saldırılarının blokzincir tabanlı bir iletişim mimarisi ile tespiti ve engellenmesi üzerine bir çalışma gerçekleştirmiştir. Önerilen iletişim mimarisinin kimlik denetimini yanıltma saldırılarına karşı koruma sağladığı tespit edilmiştir [8].

III. MITM SALDIRI YÖNTEMLERİ

Saldırganlar, ortadaki adam saldırısını gerçekleştirmek için kullanıcıyı sahte bir web sitesine yönlendirebilir, wi-fi erişim noktasının simülasyonunu yapabilir, kullanıcı bilgilerini içeren tarayıcı çerezlerini çalabilir.

MITM saldırıları genelde iki aşamadan oluşur: müdahale (Interception) ve şifre çözme (Decryption). Müdahale aşamasında DNS sunucularıyla ya da wi-fi aracılığıyla manipüle ederek ağda güvenlik açığı ararlar ve olası giriş noktaları bulmaya çalışırlar. Şifre çözme aşamasında ise çalınan verilerin şifresi çözülerek anlaşılır hale getirilir. Şifresi çözülen veriler dolandırıcılık amaçlı banka faaliyetlerinde kullanılabilir [9]. MITM yani ortadaki adam saldırıları yerel alan ağından, uzakta bulunan yerel alan ağından (yönlendiricilere bağlı ağlar) ya da uzakta bulunan ağdan yapılabilir. Yerel Ağ ortamda olan fiziksel bağlantıların tümüne denir. Uzak ağlar ise yönlendiricilere bağlı ağlardır.



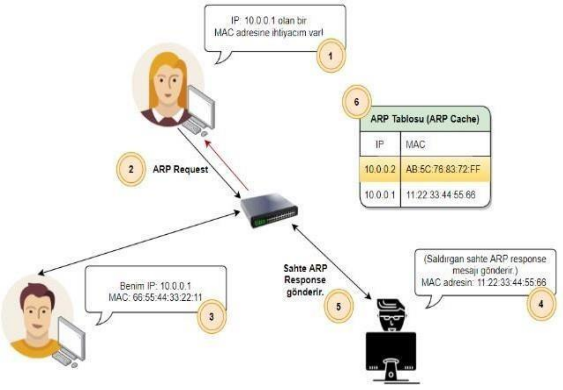
Şekil 3: MITM saldırı türleri.

a. Yerel Ağda Yapılan Saldırı Türleri

a1. ARP Zehirlenmesi (ARP Poisoning)

ARP (Adres Çözümleme Protokolü), ağdaki paketlerin adresleme işlemlerini düzenleyerek cihazlar arasında ağ iletişimini sağlar. Ana bilgisayar ARP önbelleğini tutar, ağda bulunan web sitelere ve diğer hedeflere bağlanmak için kullanır. Ağda bilgisayarların haberleşmesi için iki adet adres bilgisi kullanılmaktadır. Bunlar Mantıksal IP adresi ve Fiziksel MAC adresidir. Ana bilgisayar IP adresi için bir MAC adresine sahip değilse, ARP istek paketi gönderir ve ağda bulunan bilgisayarlardan eşleşen bir MAC adresi ister. Özetle, bilgisayarlar ağda ARP kullanarak mantıksal IP adresini bildiği bir bilgisayarın fiziksel MAC adresini ARP tablosu üzerinden öğrenir. MAC ve IP adres bilgileriyle bilgisayarlar ağ içerisinde birbirleriyle haberleşebilir [10]. ARP zehirlenmesi (ARP Poisoning) ise, yerel alan ağı üzerinden sahte bir adres çözümleme protokolü ile bilgileri gönderen bir saldırıdır. Bu saldırıda iki taraf üzerindeki iletişim gözetlenebilir. İstemci tarafından bir ARP isteği gönderilir ve saldırgan sahte bir yanıt üretir. Bu durumda saldırgan bilgisayar modemi gibidir. Ve bu saldırganın trafik akışını dinleyebilmesini sağlar. Genellikle bu yöntem ARP kullanan yerel alan ağları (LAN) ile sınırlıdır. ARP mesajlarını doğrulamak için kimlik doğrulama sistemi yoktur. Aslında ARP güvenlik için değil, verimlilik için tasarlanmıştır. Kısaca, aynı ağdaki bir cihaz orijinal mesaj kendisi için istenmese bile ARP isteğini yanıtlayabilir.

Saldırganlar ağdan IP ve MAC adreslerinin eşleştirmelerinde araya girerek ağ cihazı ilebilgisayarın haberleşmesini düzenler. Saldırgan kendi MAC adresini hedef bilgisayarın ARP tablosuna "Ağ Cihazı MAC Adresi", ağ cihazı ARP tablosuna ise "Hedef Bilgisayar MAC Adresi" yazarak ARP tablolarını zehirler. Böylelikle hedef bilgisayar ile ağ cihazı arasındaki iletişim saldırganın görebileceği ve değiştirebileceği şekilde ilerler [11].



Şekil 4: ARP Zehirlenme senaryosu.

Bir ARP Zehirlenmesi saldırısının etkisi, yerel ağdaki ana bilgisayara yönlendirilen trafiğin saldırganın seçtiği hedefe gönderilmesidir. Saldırı ilk durumda yalnızca gözlemlenebilir. Yani, bir etkisi olmayabilir. Lakin daha sonrasında ağa erişimi engelleyebilir. ARP önbellek zehirlenmesinin kalıcı bir etkisi yoktur. ARP

girişleri, uç cihazlarda birkaç dakikada, anahtarlar için birkaç saate kadar herhangi bir yerde önbelleğe alınır. Saldırgan tabloları aktif olarak zehirlemeyi bıraktığı anda bozuk girişler eskir ve uygun trafik akışı kısa sürede yeniden başlar. ARP zehirlenmesi tek başına kalıcı bir problem bırakmaz ancak siber suçlular çoğu zaman birçok saldırı türünü birlikte kullanır. Böylelikle, ARP zehirlenmesi daha büyük bir saldırının parçası haline gelebilir [12].

Korunma Yöntemleri:

VPN Kullanımı: İnternete bağlanıldığında bir web sitesine girmek için önce bir internet servis sağlayıcısına (ISS) bağlanılır. Ancak VPN kullanıldığında ARP zehirlenmesi yapan saldırganlardan büyük ölçüde engelleyen şifreli bir tünel kullanılabilir. Hem çevrimiçi etkinlik yürütülür hem de içinden geçen veriler şifrelenir. VPN kullanımı çok güvenli bir yöntem olsa da şifreleme ve şifre çözme işlem gücü nedeniyle çevrim içi erişimleri yavaşlatabilir [13].

Statik ARP Tabloları: Birbiriyle düzenli olarak iletişim kuran iki ana makinede statik bir ARP girişi ayarlamak, ARP önbelleğindeki saldırılara karşı bir koruma katmanı oluşturarak kalıcı bir giriş sağlayabilir. Bir ağdaki tüm MAC adresleri doğru IP adreslerine statik olarak eşlenebilir. Bu statik tablolar ARP zehirlenmesini korumakta başarılıdır, lakin ağda yapılan bir değişiklik, tüm ana bilgisayarlarda ARP tablolarını manuel güncellenmesini gerektirmesi sebebiyle bu tablolar büyük kuruluşlar için çok maliyetli hale gelecektir [13].

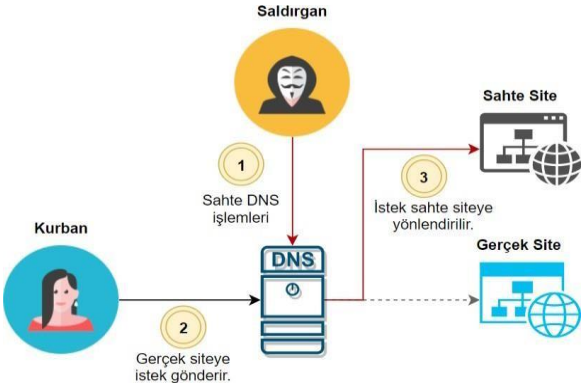
Anahtar Güvenliği: Birçok Ethernet anahtarları, ARP zehirlenmesine karşı tasarlanmıştır. Dinamik ARP Denetimi (DAI) olarak bilinen bu özellikler, her ARP mesajının geçerliliğini değerlendirir ve şüpheli veya kötü niyetli görünen paketleri bırakır.

Paket Filtreleme: Saldırganlar LAN üzerinden saldırganın MAC adresini ve kurbanın IP adresini içeren ARP paketlerini gönderir. Paketler gönderildiktensonra saldırgan veri almaya başlayabilir veya bir takip saldırısı başlatabilir. Zararlı paket sisteme sızdığında takip edilen saldırıyı durdurmak ve sistemin temizolduğundan emin olmak çok zordur. Paket filtreleme ve inceleme zararlı paketleri hedeflerine ulaşmadan yakalamaya yardımcı olabilir [14].

a2. DNS Önbellek Zehirlenmesi (DNS Spoofing)

Alan Adı Sistemi (DNS) bir alan adını belirli IP adresine çevirmek için kullanılır. DNS önbelleği alan adlarına yapılan ziyaretleri içeren geçici bir veri tabanıdır. En son ziyaret edilen sunucunun IP adresi TTL süresi (Time To Live) bitene kadar DNS önbelleğinde saklanır. Bunun amacı ise sorgulara çok hızlı yanıt verilmesidir [14].

DNS Önbellek Zehirlenmesi, bir alan adının farklı bir IP adresine yönlendirilmesiyle oluşan bir saldırıdır. Saldırgan DNS kayıtlarını değiştirerek çevrim içi trafiği sahte bir web sitesine yönlendirir. DNS önbelleğine erişen saldırganlar gerçek web sitesinin IP adresini alarak saldırganın hazırladığı dolandırıcılık içeren sahte web sitesinin IP adresiyle değiştirir ve kurbanın sahte web sitesine ulaşarak kişisel verilerini çalmayı hedefler. Bu sahte web sitesi orijinaliyle birebir aynısı olduğu için DNS sahtekarlığını tespit etmek çok zordur. DNS zehirlenmesinde saldırgan kullanıcının virüslü dosya indirmesini sağlayabilir, ortadaki adam saldırıları ile trafiği izleyebilir, banka hesap bilgileri gibi verileri toplayabilir.



Şekil 5: Saldırgan, kurbanın ulaşmak istediği sitenin IP adresiyle sahte bir sitenin IP adresini değiştirir.

DNS, trafiği yönlendirmek için kullanıcıların girdiği alan adını uygun IP adresine eşler ve bu eşleme Kullanıcı Veri Bilimi Protokolü (UDP) kullanılarak gerçekleşmesi nedeniyle göndericilerin veya alıcıların kimlik doğrulamaları gerekmez. DNS zehirlenmesi için kötü amaçlı yazılımlar kullanılabilir. Bunun bir popüler örneği: Windows Trojen Win32/DNSChanger'dir. Bu dosyanın boyutu sadece birkaç kilobayt olmasına rağmen trafiği yeniden yönlendirmek için DNS ayarlarını değiştirmeyi mümkün kılar [13].

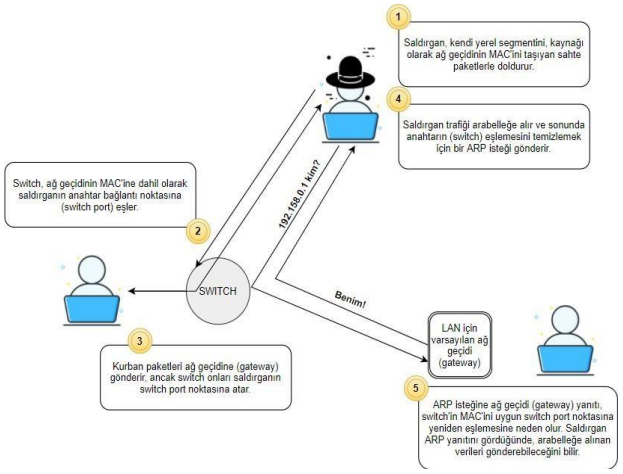
Korunma Yöntemleri:

DSNSEC Kullanımı: DNS zehirlenmesinden korunmak için tasarlanmış bir projedir. Doğrulama olarak ortak anahtarlı şifrelemeyi kullanır. Bu verileri gerçek ve güvenilir olarak imzalamanın bir yoludur.

Uçtan Uca Şifreleme: Tüm istekler ve yanıtlar için uçtan uca şifreleme kullanılabilir. Bu yöntem verilere müdahale edebilecek saldırganlara karşı ek bir koruma katmanı sunar.

a3. Port Hırsızlığı (Port Stealing)

Port çalma yani port hırsızlığı, bir yerel alan ağ anahtarından giden paketlerin, amaçlanan bağlantı noktasından çalınarak başka bir ana bilgisayara gitmesi gereken paketlerin engellenmesidir. Saldırgan, sahte ARP çerçevesi oluşturarak hedefin MAC adresini kaynak adres olarak kullanır ve kurbanın bilgisayarına gönderilen paketlerin saldırganın bağlı olduğu bağlantı noktasına gönderilmesine sebep olur. Bu sayede saldırgan paketlerdeki bilgileri okuyabilir ve paketleri silebilir [12].



Şekil 6: Port hırsızlığı senaryosu.

Örneğin, bir çevrim içi yarışma oyunu esnasında port hırsızlığı yapılabilir. Saldırgan, bir rakibin sisteminden geçen paketleri yavaşlamaya neden olacak şekilde geciktirebilir. Gecikme şüphe uyandırmayacak şekilde az olmasına rağmen saldırgan oyunu kazanabileceği bir avantaja sahip olabilir. Oyun esnasında önemli anlarda saldırgan gecikmeyi arttırabilir hatta paketleri bırakabilir. Bu girişim trafiği tamamen engellemez.

a4. STP Mangling

STP (Spanning-Tree Protocol) mangling saldırısı, saldırganın ana bilgisayardan yayılan ağaç üzerinde yeni root bridge olarak seçilmesi için kullanılan tekniktir. Saldırgan, root bridge olarak trafiğin büyük bir kısmını ele geçirebilir. STP mangling ile STP protokolünün çalışması engellenir ve sürekli topoloji değişim isteği yollanarak trafik ele geçirilir.

b. Yerel Ağdan Uzak Ağa Gateway Aracılığıyla Yapılan Saldırı Türleri

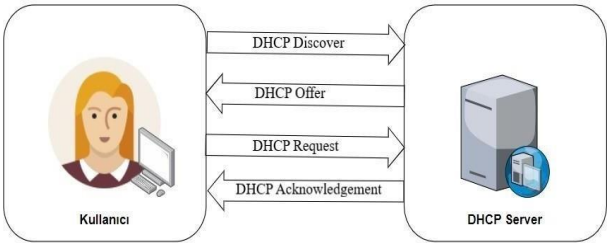
b1. ARP Zehirlenmesi (ARP Poisoning)

b2. DNS Önbellek Zehirlenmesi (DNS Spoofing)

b3.DHCP Aldatma (DHCP Spoofing)

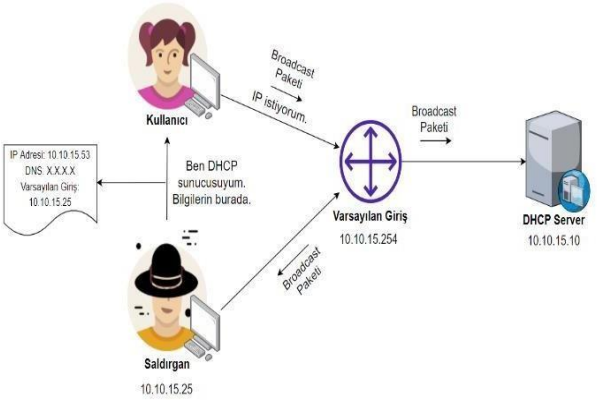
DHCP (Dynamic Host Configuration Protocol), ağ üzerinde, istemcilere kendi IP havuzundan otomatik olarak IP tanımlayan protokoldür. Günden güne ağa bağlı cihazlar arttığı için manuel bir şekilde IP atamak zordur. Bu yüzden DHCP protokolü oldukça faydalıdır.

Ağda saldırgan kendisini DHCP sunucusu gibi gösterip ağa sürekli broadcast olarak DHCP Offer paketleri gönderir. DHCP Offer paketlerinde bulunan Gateway adresini kendi IP adresi olacak şekilde değiştirir. IP almak isteyen kurban, ağa DHCP Discover paketi gönderir ve DHCP offer paketini bekler. Böylece saldırganın broadcast olarak ağa yaymış olduğu DHCP Offer paketi kurbana gider. Saldırgana yani sahte DHCP sunucusuna IP almak istediğini belirten DHCP Request paketini gönderir. Saldırgan bunun üzerine kurbana bir DHCP Acknowledgement paketi gönderir. Böylelikle saldırgan tarafından belirlenen IP adresi ve default gateway adresi kurbana iletilmiştir [14].



Şekil 7: DHCP sunucusu ve kullanıcı iletişimi.

Kurbanın ağda yapacağı bir trafik saldırgan tarafından takip edilebilir. Giden paket üzerinde şifreleme katmanı kullanmamak saldırganın paketleri görmesine olanak sağlar.



Şekil 8: DHCP aldatma senaryosu.

Korunma Yöntemleri:

Ağda broadcast olarak paket paylaşımının önüne geçmek için Switch üzerinde PortSecurity aktif edilmelidir.

Switch üzerinde DHCP Snooping özelliği aktif edilerek tüm portları güvenilmeyen moda alınabilir. Böylelikle güvenilmeyen portlardan gelen DHCP paketleri yok edilerek kullanıcıya ulaşmaz.

b4.ICMP Yönlendirmesi (ICMP Redirection)

ICMP (İnternet Kontrol Mesaj İletişim Protokolü), TCP/IP protokolünde hataları kontrol etmek ve hataları raporlamak için kullanılan bir protokoldür. IP ile ICMP aynı düzeydedirler, lakin IP hatayı düzeltme ve raporlama mekanizmasına sahip değildir. Bu yüzden hata düzeltme ve raporlamada ICMP kullanılır [15].

ICMP Redirect, ağ içerisinde bulunan bilgisayarların iletişimi esnasında fazladan yol almalarına engel olmak için gönderilen uyarı mesajlarıdır. Örneğin; yönlendiriciye gelen ağ paketi, geldiği ağ ara yüzü üzerinden geri dönüyorsa bu fazladan yol almaktır. Bu paketin yönlendiriciye geri dönmesine gerek yoktur. İşte bu durumda ICMP Redirect mesajı ile paketin kaynağına bilgi verilir, gönderdiği paketi direkt erişilmesi istenen bilgisayara göndermesi istenir.

Bir saldırgan, ICMP yönlendirme (Redirect) paketlerini kullanarak, yönlendiriciye kurban için hedeflenen paketleri saldırganın kendi makinesi aracılığıyla iletmesi talimatını verebilir. Saldırgan daha sonra paketleri hedeflerine gönderilmeden önce izleyebilir veya değiştirebilir. Buna ICMP Redirection denir.

Korunma Yöntemleri:

Kurumsal Mobil Güvenlik Programları: Kurumsal mobil güvenlik sistemleri, ağ trafiğini koklamadan (sniffing) ağ saldırılarını tespit edebilir.

Örneğin; Zimperium Mobil Güvenlik Sistemi, ağ ve ana bilgisayar saldırılarını tamamen kullanıcı modunda algılamak için makine öğrenimini kullanır. Zimperium Mobile IPS (zIPS) uygulaması, işletim sistemindeki kalıpları analiz ederek, DoubleDirect gibi ICMP Yönlendirme saldırılarını herhangi bir ek güncelleme olmadan algılayabilir ve azaltabilir.

b5.IRDP Zehirlenmesi (IRDP Spoofing)

IRDP diğer bir deyişle ICMP yönlendirici keşif protokolü, ana bilgisayarların yerel alt ağdaki yönlendiricileri bulmasını ve bunları diğer ağlara ulaşmak için bir ağ geçidi olarak kullanmasını sağlar. Alt ağdaki ana bilgisayara sahte IRDP yönlendirici reklam mesajı göndererek, varsayılan yönlendiricisini saldırganın seçeceği şekilde değiştirmesine neden olur.

b6.Rota Yönetimi (Route Mangling)

Saldırganlar, kendisini router (yönlendirici) gibi gösterebilir ve kullanıcının paketlerini kendine gönderebilir. Saldırganlar kendisini istemci için en iyi router olduğunu gateway'e sahte paketler göndererek kandırır. Paketler gateway'e gönderilmeden direkt istemciye iletilir. Saldırganlar kendini router olarak gösterdiği için gerçek router üzerinden internete erişim sağlanamayacaktır [16].

c. Uzak Ağ Üzerinden Yapılan Saldırı Türleri

c1.DNS Önbellek Zehirlenmesi (DNS Spoofing)

c2.Rota Yönetimi (Route Mangling)

c3.Traffic Tunneling

Tünel protokolü, bir ağ protokolü farklı bir yük taşıma protokolü içerdiğinde bilgisayar ağ bağlantısı, bir tünel protokolü kullanır. Tünel protokolü kullanılarak, uyumsuz olan bir iletim protokolü üzerinde bir yük taşınabilir ya da güvenilmeyen ağlarda güvenli bir yol oluşumu sağlanabilir. Saldırganın bir tünel oluşturarak kendisini ağa yerleştirmesine olanak tanıyan saldırı türüdür.

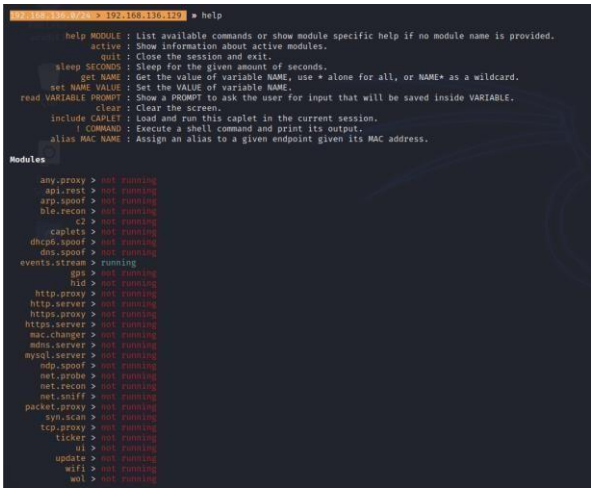
IV. MITM SALDIRI UYGULAMASI

Ortadaki adam saldırısında en popüler olan ARP zehirlenmesi incelenmiştir. Bu çalışmada ARP

zehirlenmesi gerçek saldırı amaçlı yapılmamıştır. VMware Workstation üzerinden Kali Linux ve Windows 10 sanal makineleri aracılığıyla sanal bir ağ oluşturularak gerçekleştirilmiştir.

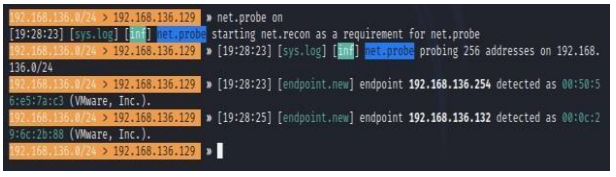
Şekil 9: Kali Linux üzerinde "bettercap"in başlatılması.

Bettercap, gelişmiş ataklar yapmaya olanak veren bir komut istemi aracıdır. İletişim protokolü analizinde ve bilgisayar güvenliği denetiminde kullanılabilir."bettercap -iface eth0" komutu ile sahip olunan eth0 arayüzünde bettercap çalıştırılmıştır.



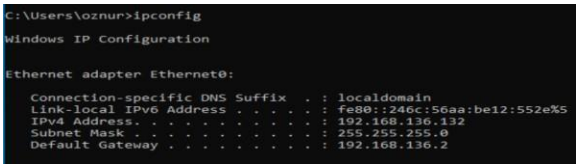
Şekil 10: "help" komutunun Kali Linux üzerinde çalıştırılması.

"help" komutunu girerek kullanılacak olan bettercap'in modüllerinin aktif olup olmadıkları incelenmiştir.



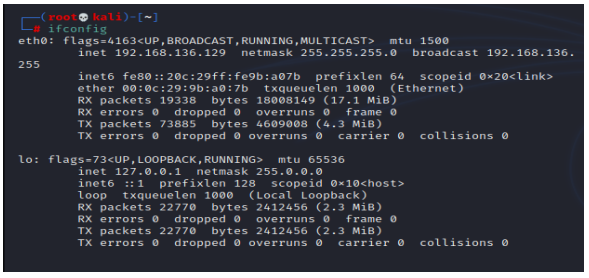
Şekil 11: "net.probe on" komutunun Kali Linux üzerinde çalıştırılması.

"net.probe on" komutu aktif edilerek yerel ağdaki cihazların IP ve MAC adreslerine ulaşılmıştır. Ağdaki cihazlar bu komut ile taranır.



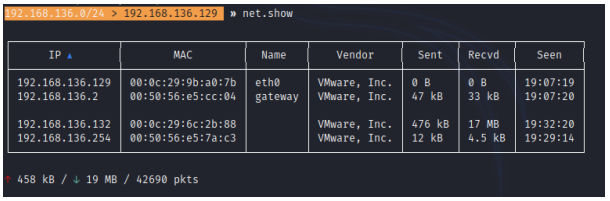
Şekil 12: Windows 10 işletim sisteminde "ipconfig" komutunun çalıştırılması.

"ipconfig" komutu, Windows işletim sisteminde bağlı olunan cihazın IP ve MAC adresini gösterir. Şekil 11'de Kali Linux üzerinden yapılan "net.probe on" komutunda da Windows cihazının IP ve MAC adreslerine ulaşılmıştır.



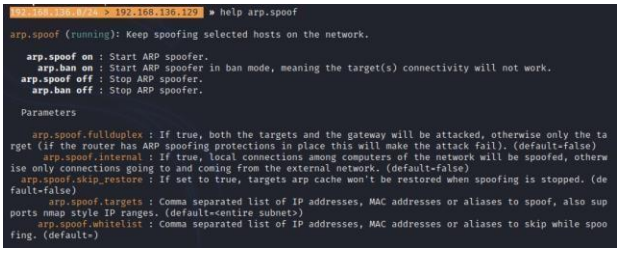
Şekil 13: Kali Linux işletim sisteminde "ifconfig" komutunun çalıştırılması.

"ifconfig" komutu, Kali Linux işletim sisteminde bağlı olunan cihazın IP ve MAC adresini gösterir.



Şekil 14: "net.show" komutunun Kali Linux üzerinde çalıştırılması.

"net.show" komutu, "net.probe on" komutu ile görülen verileri görselleştirir. En üstte bulunan satırda kendi (Kali Linux) IP ve MAC adresleri gösterilir. İkinci satırda gateway IP ve MAC adresleri bulunur. Üçüncü satırda aynı ağda bulunan Windows 10 işletim sistemine sahip olan cihazın (kurban) IP ve MAC adresleri gösterilir.



Şekil 15: "help arp.spoof" komutunun Kali Linux üzerinde çalıştırılması.

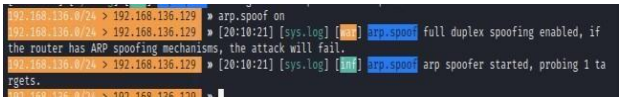
"help arp.spoof" komutu "arp.spoof" hakkında bilgi verir. "arp.spoof.fullduplex" komutu hem modeme hem belirlenen kurbana atak yapar. Çıktıda default'un false olduğuna dair uyarı verir. Arp zehirlenme saldırısının yapılması için default değerini true yapılması gerekir. "rp.spoof.internal" ise true değeri verildiği takdirde yerel bağlantıları sahte yapacaktır. Sanal makine kullananlar için bu komut şart değildir. "arp.spoof.skip_restore" ile saldırı durdurulduğunda ARP önbelleği geri yüklenmez. "arp.spoof.targets" ile hedef olarak kurbanın IP adresi atanır. "arp.spoof.whitelist" ise saldırı esnasında atanacak bilgilerin liste halinde dökümanıdır.

Şekil 16: "set arp.spoof.fullduplex true" komutunun Kali Linux üzerinde çalıştırılması.

Şekil 15'te bahsedildiği üzere bu komut ARP zehirlenmesi için default değerini true olarak çevirir.

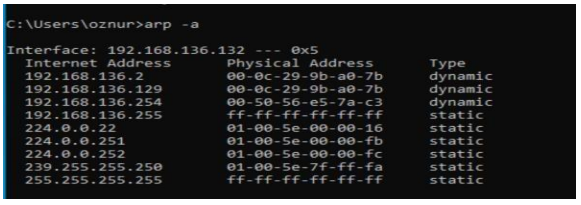
Şekil 17: "set arp.spoof.targets <hedefmakineip>" komutunun Kali Linux üzerinde çalıştırılması.

Şekil 15'te bahsedildiği üzere bu komut ARP zehirlenmesi için kurbanın IP'sini hedefe atar.



Şekil 18: "arp.spoof on" komutunun Kali Linux üzerinde çalıştırılması.

Bu komut yardımı ile arp.spoof modülü aktif konuma getirilip ARP zehirlenmesi işlemi başlatılır. Burada görüldüğü üzere ARP zehirlenmesine karşı mekanizması varsa atak gerçekleşemez. ARP zehirlenmesinde bir hedefin olduğu hakkında bilgi verir.



Şekil 19: "arp -a" komutunun Windows 10 üzerinde çalıştırılması.

"arp -a" komutu, ARP önbellek tablosunu gösterir. Kurban bu yöntemle ARP zehirlenmesine maruz kaldığını anlayabilir. Görüldüğü üzere; saldırgan, gateway'in fiziksel MAC adresini kendi fiziksel MAC adresine atamıştır. Bu adreslerin türleri dinamik'tir. Türü statik olsaydı ARP zehirlenmesi gerçekleştirilemezdi.

Şekil 20: "net.sniff on" komutunun Kali Linux üzerinde çalıştırılması.

Tüm bu işlemler yapıldıktan sonra geriye kalan tek iş trafiği dinlemektir. "net.sniff on" komutu ile kurbanın ağ trafiği dinlenir.

Şekil 21: Windows 10 üzerinden yapılan ağ trafiğinin Kali Linux üzerinden incelenmesi.

Şekil 20'de yazılan komut aracılığıyla Windows 10 işletim sistemine sahip kurbanın girdiği internet siteleri, kullanıcı adı ve şifreleri Kali Linux işletim sisteminde görüntülenir.

V. MITM SALDIRILARINI ÖNLEME YÖNTEMLERİ

Ortadaki adam (MITM) saldırıları, bilgisayar saldırganlarına belirli bir düzeyde gizlilik sunar. Dikkatli bir şekilde yapıldığında, ortadaki adam saldırıları tespit edilemeyebilir, bu nedenle siber güvenlik önlemleri saldırıya uğrayan organizasyon ekibi sorunu kontrol edemez ve çözemez. Sonuç olarak ortadaki adam ataklarının çok ciddi bir tehdit oluşturduğu söylenebilir. Bu sebeple ortadaki adam saldırılarını önlemek oldukça önemlidir.

Güvenli Bağlantı: Güvenli bir internet bağlantısı, en önemli korunma yöntemlerinden birisidir. Yalnızca SSL teknolojisini kullanan güvenli bir http bağlantısına sahip web siteleri ziyaret edilmelidir. URL, "http://" ile değil "https://" ile başladığından bu siteler daha güvenlidir. Sadece güvenli web sitelerine girmek yüzde yüz koruma sağlamamaktadır. Güvenli olmayan halka açık wi-fi bağlantılarını kullanmaktan kaçınılmalıdır. Güvenlik olmadan ziyaret edilen web sitelerinin hacklenmesi oldukça kolaydır.

VPN: Ağ güvenliği için en iyi yöntemlerden biri, çevrim içi bağlanırken bir VPN (sanal özel ağ) kullanmaktır.

Bir VPN, çevrim içi olarak gönderilen verileri şifreler. Bu şifreleme, MITM saldırısının ağ trafiğine sızılmasını engeller. Bir suçlu ağa erişmeyi başarsa bile, şifrelenmiş veriler mesajları okuyabilmesini ve hangi web sitelerine girdiğinin bilmesini engeller. Ayrıca herkese açık wi-fi'ye bağlanılması gerekiyorsa, bunu bir VPN aracılığıyla yapmak koruma sağlar.

Uç Nokta Güvenliği (Endpoint Security): Uç nokta güvenliği, bir siber saldırının kurbanı olmaktan kaçınılması için tehlikeli web siteleri ve e-postaları kontrol eder. Cihaza veya ağa kötü amaçlı yazılım bulaşırsa, bu güvenlik yazılımı kurbanı savunmak için devreye girer [17].

Çok Faktörlü Kimlik Doğrulama: Bir MITM saldırganı, kurbanın oturum açma kimlik bilgilerini sahte bir web sitesi aracılığıyla alırsa, çok faktörlü kimlik doğrulama (MFA) kullanıldığı takdirde her şey kaybolmaz. MFA, hesabına giriş yapmak için yalnızca kullanıcı adına ve şifreye ihtiyaç duyulmaz, aynı zamanda başka bir doğrulama biçimi kullanılan bir güvenlik geliştirmesidir. Örneğin, bir PIN (kişisel kimlik numarası) veya cep telefona kısa mesaj olarak gönderilen özel bir kodun girilmesini içerir [18].

Kolayca çalınan bir oturum açmanın ötesinde kimlik doğrulamak için birden fazla yol talep ederek; bir suçlunun, kurbanın bilgilerine veya parasına erişimi engeller.

HTTP Katı Taşıma Güvenliği (HSTS): HTTP katı aktarım güvenliği veya HSTS, siteye başlık bilgilerine dahil edilebilecek bir web sitesi güvenlik politikasıdır. Amacı, tarayıcıları güvenli HTTPS bağlantıları kullanarak web sitesini yüklemektir. Çoğu kişi bir web sitesine ulaşmak için yalnızca alan adını yazar [7].

Örneğin, tam "https://www.cheapsslsecurity.com" yazmak yerine "cheapsslsecurity.com" yazabilirler. Bazı durumlarda tarayıcı, sitenin HTTP aracılığıyla sağlanan güvenli olmayan bir sürümünü yükleyebilir. Bu durumda, kullanıcı, ortadaki bir adam saldırısına açık, güvenli olmayan bir web sitesiyle bilgi paylaşabilir. Sitede bir HSTS başlığı kullanmak, tarayıcılara web sitenizin HTTPS sürümünü yüklemelerini söyler. Bir kullanıcı web sitesini ilk kez açtığında, tarayıcı HTTPS sürümünü depolayacaktır. Bu, kullanıcı web sitesini alan adını veya HTTP sürümünü kullanarak yüklese bile, tarayıcının onları HTTPS sürümüne yeniden yönlendirmesini sağlar.

HSTS'nin bir diğer sınırlaması, yalnızca kullanıcı sunucuda ilk kez oturum açtıktan sonra çalışacak olmasıdır. O zamana kadar kullanıcı korunmaz. Bu sorunla başa çıkmak için Google, en modern tarayıcılar tarafından desteklenen bir "HSTS ön yükleme listesi" hazırlamıştır. Ön yükleme listesi özelliği, tarayıcıya bir HTTP web sitesini yüklemeye çalıştığını bildirir. Ayrıca, HSTS başlığındaki maksimum sürenin sona ermesi ve HTTP sitesinin yüklenmesi durumunda tarayıcıya yardımcı olur [7].

Wi-Fi Korumalı Erişim (WPA): WPA, WPA2 ve WPA3; kablosuz bilgisayar ağlarının güvenliğini sağlamak için wi-fi Alliance tarafından geliştirilen şifreleme protokolleridir. WPA protokolü, her paket için yeni bir dinamik 128 bit anahtar oluşturan geçici anahtar bütünlüğü protokolünü (TKIP) kullanır. 2018'de piyasaya sürülen WPA3, wi-fi Alliance'a göre en güçlü protokoldür ve tüm wi-fi onaylı cihazlar için gereklidir. Kişisel ve kurumsal müşterilerine sağlam güvenlik

sağlamak için SHA-384 ile 256 bite kadar gelişmiş şifreleme standardı (AES) gücü kullanır.

Sıfır Güven Mimarisi (Zero Trust Architecture): SonicWall Siber Tehdit Raporu, 2020'de 4,77 trilyon izinsiz girişin olduğunu, 2019'da ise 3,99 trilyondur. Görüldüğü üzere bir yıl içerisinde keskin bir artış söz konusudur. 2020'deki girişimlerin %56,44'ü Kuzey Amerika'dadır. Sıfır güven mimarisi kullanmak, bu büyüyen sorunu çözmenin bir yoludur [17].

Sıfır güven mimarisi kavramı, Forrester Research'teki güvenlik ve risk ekibinde başkan yardımcısı ve baş analist olan John Kindervag tarafından tanıtılmıştır. Sıfır güven tekniği, doğrulama olmadan hiç kimseye ve hiçbir cihaza güvenmemek anlamına gelir. Ancak sıfır güven, MFA veya 2SV'den çok daha fazlasıdır. Bu mimari, tüm çalışanların bilgilere erişmek için uygun kimlik doğrulamasını kullanmasını ve bilgilere erişme yetkisine sahip olmalarını sağlar [19].

Temel olarak, buradaki fikir, hiçbir çalışanın özel olarak yetkilendirilmediği bilgileri alamamasıdır. Her kişiye potansiyel bir tehdit olarak muamele edilir, bu da sıfır güven modelini inanılmaz derecede güçlü kılar.

VI. SONUÇLAR VE ÖNERİLER

Ortadaki adam saldırı türleri kapsamında; ARP Poisoning, DNS Spoofing, Port Stealing, STP Mangling, Traffic Tuneling, Route Mangling, DHCP Spoofing, ICMP Redirection ve IRDP Spoofing incelenmiştir. MITM saldırısı senaryosu uygulamalı olarak gerçekleştirilmiştir. Bu saldırılara karşı korunma yöntemleri olarak; güvenli bağlantı, VPN, uç nokta güvenliği (endpoint security), çok faktörlü kimlik doğrulama, HTTP katı taşıma güvenliği (HSTS), Wi-Fi korumalı erişim (WPA) ve sıfır güven mimarisi (zero trust architecture) önerilmiştir.

Ağa bağlanan cihazları kullanırken veri güvenliğimiz için dikkatli olmalıyız. Teknoloji her ne kadar hayatı kolaylaştırsa da aynı zamanda bilgi güvenliği nedeniyle hayatı zorlaştırma niteliğine de sahiptir. Ortadaki adam saldırıları fark edilmeden gerçekleştirilebilir. Her daim güvenliğe önem verilmelidir.

KAYNAKLAR

1. Avijit Mallika, Abid Ahsanb, Mhia Md. Zaglul Shahadata and Jia-Chi Tsou (2019), “International Journal of Data and Network Science”, 3, 77-92, https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words.
2. Danilo Bruschi, Andrea Di Pasquale, Silvio Ghilardi, Andrea Lanzi, Elena Pagani (2021), " Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency”, IEEE Transactıons On Dependable And Secure Computıng, 1-16, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9563245.
3. Fatih Özavcı, Özgür Yazılımlarla Saldırı Yöntemleri, 1-70, https://ab.org.tr/ab12/sunum/Ozgur_Yazilimlarla_Saldiri_Yontemleri.pdf.
4. Ahmet Efe, Gizem Kalkancı, Mehmet Donk, Serhat Cihangir, Ziya Uysal (2019), ” A Hidden Hazard: Man-in-The-Middle Attack in Networks”, Anatolian Journal of Computer Science, vol: 4, no: 2, https://dergipark.org.tr/tr/download/article-file/833633.
5. Yaoqı Yang, Xıanglın Weı, Renhuı Xu, Laıxıan Peng, Leı Zhang, And Lın Ge (2020), “Man-in-the-Middle Attack Detection and Localization Based on Cross-Layer Location Consistency”, IEEE Access, 1-15, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9106317.
6. Alıreza Esfahanı, Georgıos Mantas, José Rıbeıro, Joaquım Bastos, Shahıd Mumtaz, Manuel A. Vıolas, A. Manuel De Olıveıra Duarte, Jonathan Rodrıguez, “An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain”, IEEE Access, 1-9, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8704724.
7. Ünlü, U. (2018). “İnternet Bankacılığı Sisteminde Tüketicilerin Karşılaşacağı Olası Saldırılar ve Çözüm Önerileri”. Bankacılar Dergisi, 104, 82-96, https://www.tbb.org.tr/Content/Upload/dergiler/dosya/79/Bankacilar_Dergisi_104.pdf.
8. Angin, P. (2020). Blockchain-Based data security in military autonomous systems. Avrupa Bilim ve Teknoloji Dergisi, Özel Sayı, 362-368, https://dergipark.org.tr/en/download/article-file/1390795.
9. Radhika P, Ramya G, Sadhana K, Salini (2017), “Defending Man In The Middle Attacks. International Research Journal of Engineering and Technology (IRJET)”, 579-585, https://www.academia.edu/32530601/Defending_Man_In_The_Middle_Attacks.
10. Mahmut Alperen Güner (Ocak 2021), Yaygın Ağ Saldırıları ve Genel Hatlarıyla Ağ Savunması, 1-5, https://www.researchgate.net/publication/348098380_Yaygin_Ag_Saldirilari_ve_Genel_Hatlariyla_Ag_Savunmasi.
11. Hitesh Mohapatra, Subhashree Rath, Subarna Panda, Ranjan Kumar (2020), vol: 8, no: 5, 1-8, https://www.researchgate.net/publication/341776424_Handling_of_Man-In-The-Middle_Attack_in_WSN_Through_Intrusion_Detection_System
12. Sahil Dambee, Nikhita Mangaonkar (2018). Detecting man in the middle attack, vol: 4, issue: 3,

2356-2358, https://www.academia.edu/37640161/Detecting_man_in_the_middle_attack.
13. Zouheir Trabelsi, Khaled Shuaib (2006), Man in the Middle Intrusion Detection, IEEE Access, 1-6, https://www.academia.edu/7198942/Man_in_the_Middle_Intrusion_Detection
14. Alamsyah, Mengenal Serangan Man-in-The-Middle (MITM), 1-3, https://www.academia.edu/10169563/Mengenal_Serangan_Man_in_The_Middle_MITM.
15. Ahmet Çakmak, Web Güvenliğinde SSL/TLS Kriptografik Protokolü: Açıklıklar, Saldırılar ve Güvenlik Önlemleri, İstanbul Şehir Üniversitesi, 1-144, https://personel.omu.edu.tr/docs/ders_dokumanlari/9273_29675_1390.pdf
16. D. S. J. S. G. Greenwood and Z. L. L. Khan (2014), "Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps", 1-14, http://web.cse.ohio-state.edu/~lin.3021/file/NDSS14b.pdf
17. Adam Kostrzewa (2011), "Development of a man in the middle attackon the GSM Um-Interface", 1-72, https://www.academia.edu/7352630/Man_in_the_Middle_Attack.
18. Gürol Canbek, Şeref Sağıroğlu (2007), Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 1-7, https://dergipark.org.tr/tr/download/article-file/252301
19. Serkan Yenal, Naci Akdemir (Nisan 2020), Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi, ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi, vol: 11, 1-37, https://dergipark.org.tr/en/download/article-file/1114311.