Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 42, S. 100-107, Ekim 2022

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 42, pp. 100-107, October 2022

Research Article

Ortadaki Adam Saldırısı (MITM)

Salih Zafer Dicle[1*]

[1*] Dokuz Eylül Üniversitesi, Mühendislik Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, İzmir, Türkiye, (ORCID: 0000-0002-6689-7987), zafer@deu.edu.tr

(2nd International Conference on Engineering and Applied Natural Sciences ICEANS 2022, October 15 - 18, 2022)

(**DOI:** 10.31590/ejosat.1187984)

ATIF/REFERENCE: Dicle, S. Z. (2022). Ortadaki Adam Saldırısı (MITM). *Avrupa Bilim ve Teknoloji Dergisi*, (42), 100-107.

Öz

Yaşadığımız çağın en hayati kaynağının bilgi olduğunu herkes kabul etmiştir. Bilgi her geçen gün daha fazla güç faktörü olarak hissedilirken, düşünme ve algılama biçimlerimizde, araştırma yöntemlerimizde ve yaşam tarzlarımızda büyük değişiklikler meydana gelmektedir. Bu bağlamda özellikle son yıllarda siber tehditlerin önemi ortaya çıkmakta ve bu tehditlerden korumanın yolları tartışma konusudur. Ortadaki Adam Saldırısı (Man in The Middle MITM), aynı ağda bulunan bir kişisel bilgisayar ile saldırganın etkileşiminden başka bir deyişle, kişisel bilgisayar ile bilgisayar ağı arasına saldırganın girmesi sonucu ortaya çıkan durumdur. Saldırgan, kişisel bilgisayarın ağ bağlantısı ile arasına girerek, kişisel bilgisayarın tüm ağ trafiğinin kendi üzerinde akmasını sağlayarak tüm bilgileri anında yakalamasına ve değiştirmesine izin verdiği için ağ güvenliği için önemli bir tehdit oluşturur. Bu süreçte mağdur (kişisel bilgisayar) hiçbir şey olmamış gibi internete işlem yapmaya devam eder ancak kişisel bilgisayar ile bağlı olduğu tüm siteler ve sistemler artık saldırgan tarafında izlenebilir ve görünür durumdadır. Bu saldırı, saldırganın tüm konuşmayı kontrol ettiği bir gizli dinleme biçimidir.
Bu çalışmada, sistem ya da bir başka deyişle ağ yöneticisi olarak, söz konusu atakların bilgisayar ağında akıllı yönetilebilir anahtar cihazlar kullanarak ve gerekli düzenlemeleri yaparak ağ güvenliğini tam olarak sağlanması garanti altına alınmıştır.

Anahtar Kelimeler: Ortadaki adam saldırısı, siber saldırı, Siber güvenlik, Bilgisayar ağ güvenliği, MITM .

Man-In-The-Middle Attack

Abstract

Everyone has accepted that the most vital resource of our age is information. As information is felt more and more as a power factor, great changes are taking place in our ways of thinking and perceiving, our research methods and our lifestyles. In this context, the importance of cyber threats has emerged especially in recent years and the ways to protect these threats are a matter of discussion. MITM attacks pose a significant threat to network security as they interrupt communication between two systems and allow an attacker to instantly capture and manipulate critical information. In this process, the victim continues to connect to the internet as if nothing has happened, but all the sites you are connected to with the computer are now visible. This attack is a form of eavesdropping in which the attacker controls all speech.
In this study, as the system, or in other words, the network administrator, it is ensured that the network security is fully ensured by using smart manageable switch devices in the computer network of the said attacks and making the necessary arrangements.

Keywords: man-in-the-middle attack, Cyber security, Computer network security, MITM.

[*] Sorumlu Yazar: zafer@deu.edu.tr

1. Giriş

1.1. Ağ Kavramı

Aralarında elektronik bir bağlantı bulunan bir grup bağımsız bilgisayara bilgisayar ağı denilmektedir. Burada bilgisayarların birbirine bağlı olması, birbirleriyle veri alışverişi yapabilmeleri anlamı taşımaktadır. Bilgisayarlar arasındaki bağlantı bakır tel, optik kablo, radyo iletişim sistemleri, iletişim uyduları ve kısa mesafeler için kızılötesi iletişim sistemleri veya radyo dalgalarıyla haberleşen iletişim sistemleri olabilmektedir.

Bilgisayarların özerk olması, diğer bilgisayarlar tarafından kontrol edilmedikleri anlamına gelir. Bir bilgisayarı başka bir bilgisayar başlatılabiliyor, durdurulabiliyor ve kontrol edilebiliyorsa bağımsız değildir. Bir kontrol ünitesi ve birkaç bağımlı bilgisayardan veya birkaç uzak terminal ve yazıcıdan oluşan bir sistem, bir bilgisayar ağı olarak kabul edilmez.

Dağıtılmış sistem ve bilgisayar ağları arasında bazı farklar vardır. Bunlardan en önemlisi, dağıtık sistemlerde birden çok işlemcinin (ayrı bilgisayarlar) kullanıcıya şeffaf (kullanıcıya görünmez) olmasıdır. Kullanıcı bir komut girdiğinde isteği yerine getirilir. İşletim sisteminin görevi en uygun işlemciyi seçmek, girdi dosyalarını bulmak, bu işlemciye aktarmak ve sonuçları uygun yerlere yerleştirmektir. Bu eylemler otomatik olarak gerçekleştirilmektedir. Diğer bir deyişle, dağıtık bir sistemin kullanıcısı birden fazla işlemci olduğunu fark etmez; sistemi tek bir işlemci olarak kabul eder. Ağ içinde, kullanıcılar makineye net bir şekilde bağlanır ve görevi açıkça tanımlar, doğrudan istedikleri yerde dosyalar ve ağı kendileri yönetebilir. Merkezi olmayan bir sistemde işlemler açık olarak yapılmaz, tüm işlemler kullanıcının bilgisi dışında otomatik olarak yapılmaktadır (Tanenbaum, 2003).

Günümüzde yaygınlaşan bilgisayar ağları, işletmeler için kaynak paylaşımı, iletişim ortamları ve elektronik ticaret fırsatları sağladıkları için maliyet, güvenilirlik ve ölçeklenebilirlik açısından büyük bilgisayar sistemlerine göre avantajlara sahiptir; Kişisel kullanıcılar için bilgiye, iletişime ve interaktif eğlenceye uzaktan erişim sağlamaktadır. Bilgisayar ağları, kullanılan aktarım teknolojisine göre iki kategoriye ayrılmaktadır: yayın ağları (LAN, MAN ve uydu ağları) ve noktadan noktaya ağlar (WAN ve Bağlı Ağlar). Öte yandan fiziksel boyutlarına göre küçükten büyüğe dört kategoriye ayrılırlar: LAN, MAN, WAN ve bağlı ağlar (internetler). LAN'lar üç tür bağlantı kullanmaktadır: paylaşılan yol, halka ve yıldız. MAN'ler iki veri yolu ile bir DQDB mimarisi kullanmaktadır. WAN'lar yıldız, halka, ağaç, tam bağlantı, çapraz halka ve düzensiz bağlantı türlerini kullanabilir. Kamu yayın ağları ile ilgili en önemli şey, birçok kullanıcının tek bir iletim ortamı kullanması ve bilgilerini çerçeveler halinde göndermesidir; MAC protokolü, iletim ortamına kullanıcı erişimi sağlar. WAN'lar ağ alt ağlarından ve bilgisayarlardan oluşmaktadır. Alt ağlar, yönlendiricileri ve bunları birbirine bağlayan iletim hatlarını içermektedir. Yönlendiriciler ayrıca "paket anahtarlama düğümleri" olarak da bilinir. Birbirine bağlı ağlarda iletişimin en yaygın örneği internettir. Radyo dalgaları veya kızılötesi ışınlar yayan ağlara kablosuz veya kablosuz ağlar denmektedir. Kızılötesi iletişim, birbirini görebilen ve kısa mesafede bulunan vericiler ve alıcılar arasında kullanılabilir.

1.2. Siber Güvenlik

Siber güvenlik, sunucuların, bilgisayarların, elektronik sistemlerin, mobil cihazların, ağların ve verilerin kötü niyetli saldırılara karşı korunmasıdır. Buna BT bilgi güvenliği veya elektronik bilgi güvenliği de denmektedir. Terim, işten mobil bilişime kadar birçok bağlam için geçerlidir ve birkaç kategoriye ayrılmaktadır.

- Ağ güvenliği; bir bilgisayar ağını hedeflenen saldırganlardan ve/veya kötü amaçlı yazılımlardan ve davetsiz misafirlerden koruma uygulaması.

- Uygulama güvenliği; Cihazları ve yazılımları tehditlerden kurtarmaya odaklanmaktadır. Güvenliği ihlal edilmiş bir uygulama, korumak için tasarlandığı verilere erişime izin verebilir. Başarılı bilgi güvenliği, program veya cihaz uygulanmadan çok önce planlama aşamasında başlar.

- Bilgi Güvenliği; kullanım, aktarım ve depolama esnasında verilerin gizliliğini ve bütünlüğünü korur.

- Operasyonel güvenlik, veri varlıklarını işleme ve korumaya yönelik süreçleri ve kararları içerir. Bir kullanıcının ağa erişmek için hangi izinlere sahip olduğunu ve verilerin nasıl ve nerede saklanabileceğini veya paylaşılabileceğini belirlemeye yönelik tüm adımlar bu çatı altında toplanıyor.

- Olağanüstü durum kurtarma ve iş sürekliliği, bir şirketin bir siber güvenlik ihlaline veya operasyon veya veri kaybına neden olan başka bir olaya nasıl yanıt vereceğini tanımlar. Acil durum kurtarma ilkeleri, kuruluşun olaydan öncekiyle aynı operasyonel kapasiteye geri dönmek için operasyonlarını ve verilerini nasıl kurtaracağını tanımlar. İş sürekliliği, bir kuruluşun belirli kaynaklar olmadan çalışmaya çalışırken geri döndüğü plandır.

1.3. Siber Saldırı

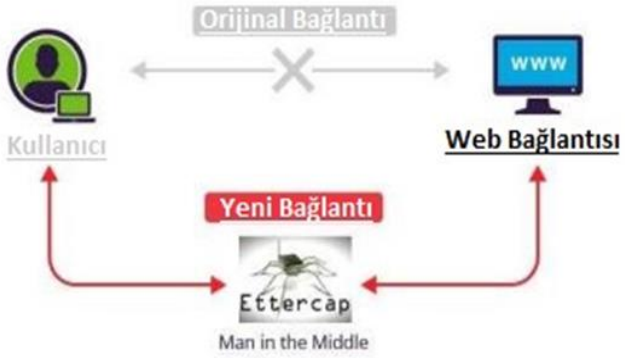
Siber uzayın olanaklarını kullanarak bilgi çalma veya değiştirme ve bilgi sistemlerinde tahribat veya bozulmaya neden olma girişimi siber saldırı olarak adlandırılabilir. Siber savaş ise bu eylemlerin devlet tarafından veya devletler düzeyinde gerçekleştirilmesi anlamına gelmektedir. Siber savaşın en kafa karıştırıcı yönlerinden biri, siber savaşçılar veya devlet destekli bilgisayar korsanları veya bilgisayar korsanları diğer ülkelere saldırdığında siber savaş olarak adlandırılması gerekip gerekmediğidir. Söz konusu durumda gerçek hayatta olduğu gibi siber uzayda da vekalet savaşları stratejisi izlenmektedir. Ülkeler, uluslararası yasalarla temastan kaçınmak için genellikle bu tür çatışmaları hizipler aracılığıyla yürütürler. Başka bir ülkeye saldıran bir grup siber savaşçı aslında bir tür siber savaştır.

2. Man In The Middle Kavramı (MITM)

Ortadaki adam saldırısı (Man İn The Middle, MITM), ağ cihazları ve kurban bilgisayarlar arasında yetkisiz erişim yoluyla verilerin şifrelenmesi ve şifrelenmemiş verilerin izlenmesi ilkesine dayanan bir saldırı türüdür.

MITM saldırıları, OSI modelinin ikinci katmanında (veri bağlantı katmanı) uygulandığından, saldırgan başarılı olursa, saldırgan tüm trafik akışını kontrol edebilir. Bu hakimiyet, şifrelenmemiş trafikten şifreli "HTTPS" trafiğine kadar sınırsızdır. Başarılı bir MITM saldırısı sırasında saldırganın yapabileceği işlemler tamamen onların bilgisine, becerisine ve

hayal gücüne bırakılmıştır. Güvenlik önlemleri, ağ güvenliğine karşı iyi bilinen bir saldırı türü olmasına rağmen, en az sayıda saldırıyı içerir.



Şekil 1. MITM atağının Örnek resmi

Kullanıcıların bir kuruluş içinde bilgileri paylaşmalarının ve iletişim kurmalarının birincil yolu, bir ağ altyapı hizmetidir. Veri paketi ağda serbestçe dolaşır. Kendi IP adresine ait olmayan bir paket alan cihazlar, isteğe bağlı olarak o paketin içeriğini görebilir veya değiştirebilir. (Man-in-the-middle saldırısı, 2018; Rouse & Cobb, 2015) MITM saldırısı, ağdaki paketleri ele geçirmek ve manipüle etmek olarak da özetlenebilir.

MITM saldırıları, iki sistem arasındaki iletişimi kestikleri ve bir saldırganın kritik verileri anında ele geçirmesine ve değiştirmesine izin verdiği için ağ güvenliği için önemli bir tehdit oluşturur. Bu süreçte kurban hiçbir şey olmamış gibi internete bağlanmaya devam eder ancak bilgisayarla iletişim kurduğunuz tüm siteler artık görünür durumdadır. Bu saldırı, saldırganın tüm konuşmayı kontrol ettiği bir gizli dinleme biçimidir.

Örneğin, istemci ile ana bilgisayar arasında TCP bağlantısının olduğu bir HTTP işleminde, farklı teknikler kullanan bir saldırgan, orijinal TCP bağlantısını iki yeni bağlantıya böler (Toward More Resilient Cyber Infrastructure: A Practical Approach, 2016). İlk bağlantı kurban ile saldırgan arasında, ikinci bağlantı ise saldırgan ile sunucu arasındadır. Saldırgan TCP bağlantısını kestiğinde, ele geçirilen iletişimin verilerini okuyabilir veya değiştirebilir. Alternatif olarak, bir saldırgan kullanıcının tanımlama bilgilerini çalabilir. Bu çalınan çerezler, bir kullanıcının oturumunu ele geçirmek ve bir saldırganın bir web sitesinde bu kullanıcıyı taklit etmesine izin vermek için kullanılabilir.

Aynı teknik kullanılarak https bağlantısı üzerinden MITM saldırısı da yapılabilir; Tek fark, her bir TCP bağlantısı yerine yeni SSL oturumlarının kurulmasıdır. Bu sefer farklı olan, tarayıcı ile saldırgan arasındaki SSL bağlantısı ve saldırgan ile web sunucusu arasındaki diğer SSL bağlantısıdır. Genellikle, bu gibi durumlarda, tarayıcı kullanıcıyı dijital sertifikanın kabul edilebilir olmadığı konusunda uyarır, ancak kullanıcı potansiyel tehdidin farkında olmadığı için uyarıyı yok sayar. SSL kullansanız bile, bir saldırgan HTTP trafiğinizi SSLstrip ile yeniden yönlendirebilir. Tüm trafiğinizi izleyen bir saldırgan, girdiğiniz tüm sitelere kullanıcı adınızın ve şifrenizin gönderildiğini açıkça görebilir. Saldırgan, girdiğiniz tüm bilgileri düz metin olarak da görebilir. Kısacası, bir saldırgan verilerinizin çoğunu çalabilir (Rouse 2015).

MITM saldırıları, DNS sunucularını da hedefleyebilir. DNS araması, web tarayıcılarının alan adlarını IP adreslerine çevirerek web sitelerini bulmasını sağlar. DNS, DNS sahtekarlığı ve DNS ele geçirme gibi MITM saldırılarında, bir saldırgan DNS arama sürecini tehlikeye atabilir ve kullanıcıları yanlış sitelere gönderebilir, genellikle kötü amaçlı yazılım yayabilir ve/veya hassas bilgiler toplayabilir. Saldırgan daha sonra gerçek web sitesiyle yeni bir bağlantı kurabilir ve kullanıcı ile orijinal web sitesi arasındaki trafiği izlemek ve işlemek için bir proxy görevi görebilir. MITM saldırıları genellikle çevrimiçi bankacılık ve e-ticaret sitelerini hedef alır ve bu da izinsiz giriş yapanların oturum açma kimlik bilgilerini ve alternatif kritik ve değerli bilgileri ele geçirmesine neden olabilir.

MITM sadece bir saldırı tekniği değildir, aynı zamanda web uygulaması geliştirme ve web güvenlik açığı değerlendirmesinde de kullanılabilir.

2.1. MITM Saldırı Türleri

2.1.1. ARP Zehirlenmesi

Adres Çözümleme Protokolü (ARP), mantıksal ağ adreslerini ikinci katman (Veri Bağlantısı katmanı) aracılığıyla fiziksel adreslere dönüştürmek için OSI modelinde kullanılan bir iletişim protokolüdür (Infosec Kılavuzu: Ortadaki Adam Saldırılarına Karşı Savunma, 2017).

Bilgisayarların iletişim kurabilmesi için ağlarda iki adresi olması gerekmektedir. Birinci adres verisi mantıksal IP adresidir ve ikinci adres verisi fiziksel MAC adresidir. Anahtarlar, trafiği bir yerel alan ağı (LAN) üzerinden yönlendirmek ve trafiği bu adres bilgilerine göre yönlendirmek için ağa bağlı bilgisayarların fiziksel MAC adres bilgilerini kullanmaktadır.

Cihazın fiziksel MAC adresinin bilinmediği durumlarda cihazın MAC adresinin IP adresi üzerinden belirlenmesi istenir. Bilgisayarlar, mantıksal IP adresiyle bilinen bir bilgisayarın fiziksel MAC adresini, ARP protokolünü kullanan bir ağ üzerindeki bir ARP tablosu aracılığıyla öğrenir. Bu bilinen ve öğrenilen adres bilgileri, bilgisayarların ağ üzerinde birbirleriyle iletişim kurmasını sağlar. Farklı bir ana bilgisayarın kimliğine bürünmek isteyen bir saldırgan, MAC adresiyle yanıt vermemesi gere Arp zehirlenmesi, ağ IP ve MAC adres eşlemelerine müdahale ederek ağ ekipmanına ve bilgisayarlara erişim sağlayan davetsiz misafirler olarak tanımlanabilir. Bu saldırıların amacı, hedef sunucuya hedeflenen tüm trafiği bloke ettikten sonra, istenen MAC adresini hedef sunucunun IP adresiyle eşleştirmektir. Bir saldırgan, ağ hedefinin ve ağ cihazının ARP tablolarını zehirlerse, bunlar ele geçirilecektir. Yani saldırgan, hedef bilgisayarın tablosundaki MAC adresini "ağ aygıtının MAC adresi" ve ağ aygıtının ARP tablosunu "hedef bilgisayarın MAC adresi" olarak yazdırırsa başarılı olur. Bu durumda hedef bilgisayar ile ağ cihazı arasındaki trafik saldırganın üzerinden geçer. Saldırgan, bu trafiği gizlice dinleyebilir ve değiştirebilir ve ele geçirilen verileri, casusluk yapmak veya taraflar arasındaki bağlantıyı değiştirmek gibi kötü amaçlı amaçlar için kullanabilir.ken isteklere yanıt verebilir.

2.1.2. DNS Yanıltması

Etki Alanı Adı Sunucusu (DNS), ARP yönteminin IP adreslerini MAC adreslerine çözmesi gibi, etki alanı adlarını IP adreslerine çözümler. Siber suçlular genellikle ağlara sızmak için

kimliğe bürünme kullanır. Bu taktikler, saldırganların görmemeleri gereken bilgilere erişmelerini sağlar. Dolandırıcılık başka bir yaygın saldırı türüdür ve farklı biçimler alabilir. DNS sahtekarlığı, MITM saldırılarında yaygın olarak kullanılmaktadır (Tanmay, 2013).

DNS sahtekarlığı veya DNS önbellek zehirlenmesi, bir DNS sunucusuna sızmayı ve bir web sitesinin adres kaydını değiştirmeyi içerir. Bir DNS saldırganı, DNS yazılımı önbelleğine zehirli bir DNS erişimi enjekte ederek DNS yazılımındaki kusurlardan yararlanan bir DNS sahtekarlığı saldırısı gerçekleştirir. Bu saldırı genellikle saldırganın, kimlik avı gibi başka amaçlar için kullanılan kötü amaçlı bir web sitesine yanlış bir IP adresi döndürmesine neden olur.

Örneğin, bir DNS sızdırma saldırganı, www.internetbanking.com gibi bir alan adı kullanarak başka bir ana bilgisayara ulaşmaya çalışır ve ana bilgisayara bozuk DNS önbellek bilgilerini eklemeye çalışır. (Man in the Middle (MITM) Attacks, 2018) Böylece kurban, bilgiyi güvenilir bir kaynağa gönderdiğine inanarak, kötü niyetli bilgisayara hassas bilgiler gönderir.

Sonuç olarak, siteye erişmeye çalışan kullanıcılar, değiştirilen DNS kaydı üzerinden saldırganın sitesine gönderilir. Siber suçlular genellikle meşru görünen kötü niyetli web siteleri oluşturduğundan, DNS sahteciliğini tespit etmek zordur.

ARP sahtekarlığı, bir saldırganın IP/ağ geçidini veya bu durumda kurbanın DNS sunucularını değiştirmek için yetkisiz bir DHCP sunucusundan ARP mesajları göndermesidir. Saldırgan, kurbanın DNS sunucusunu değiştirerek bir DNS sahtekarlığı saldırısı başlatabilir, bu da kurbanın DNS isteklerinin artık bankanın IP adresini taklit edebilecek yetkisiz bir DNS sunucusuna yönlendirildiği anlamına gelir. Her iki yöntem de aynı şeyi dener (trafiği kötü amaçlı makinelere yönlendirir veya iletir), ancak farklı bir düzeyde çalışırlar, ARP yalnızca bir sonraki LAN yönlendiricisini kandırır. Saldırı, bir kurbanın geçerli bir banka SSL sertifikası kullanarak http://www.yourbank.com'a göz atmasına izin verir, ancak sunucunun IP adresi farklı bir IP'dir. Bu şekilde, bir saldırgan banka bilgilerinize erişebilir ve hesabınızı boşaltabilir. WEB tarayıcıları, bir SSL sertifikasındaki yanlış bir URL'den şikâyet etmez (Tanmay, 2013).

Adres Çözümleme Protokolü (ARP) sahtekarlığı, bir saldırganın bir ARP isteğine yanlış yanıtlar göndermesidir. Bu genellikle yönlendiricinin kimliğine bürünmek ve böylece bir saldırganın trafiği kesebilmesi için yapılır.

Etki Alanı Adı Hizmeti (DNS) sahtekarlığı, bir saldırganın (bir ana bilgisayar adının IP adresini çözmek için gönderilen) DNS isteklerine yanlış IP bilgileriyle yanıt vermesidir. Bu genellikle kullanıcıları yanlış web sitelerine yönlendirmek için kullanılır.

ARP sahtekarlığı, ARP zehirlenmesi olarak da bilinir. Ağ IP ve MAC adreslerini birleştirerek saldırganları kesintiye uğratarak bir ağ cihazını bilgisayara tanımlama olarak tanımlanabilir. Yukarıda, bilgisayarların ağ içinde iletişim kurmak için öncelikle ARP protokolünü kullandığı belirtilmişti. Saldırgan, hedef ağ içindeki ve ağ aygıtındaki ARP tablolarını zehirleyebilirse, bu nedenle hedef bilgisayar tablosunda "MAC Pandiyaraja'nın ağ aygıtının MAC adresi", "hedef bilgisayar ağ aygıtının MAC adresini ARP olarak yazdırır. tablo" girilir. bir arada. Bu durumda, hedef bilgisayar, saldırgan ile ağ aygıtı arasındaki trafikten geçer. Bu trafiği dinleyebilir ve düzenleyebilirsiniz (Hugo, 2016).

Linux işletim sisteminin doğası gereği ağ bilgisayarınıza test etmek için kullandığımız gelen paketler için Kali. Eğer öyleyse, test tamamlanamazsa, MITM IP Yönlendirme. İkinci çağrı yönlendirme işlemi nedeniyle IP yönlendirme ağındaki IP paketleri ağı ve öncelikle MITM'yi IP yeniden yönlendirmesi etkinken test etmelidir. Linux çekirdeği, IP yönlendirme için tüm altyapıyı gizler ve dağıtımı çok kolaydır.

Terminalde IP yayın durumunu öğrenmek için aşağıdaki komutu çalıştırınız:

cat/proc/sys/net/ipv4/ip_forward

Dönüş değeri 0 (sıfır) ise IP yönlendirme aktif değildir. Etkinleştirmek için aşağıdaki komutu çalıştırınız.

echo 1 >/proc/sys/net/ipv4/ip_forward

Şimdi IP yönlendirme sistemini açınız.

Kali Linux ile birlikte gelen "arpspoof" aracı ile kurban, cihaz ve ağ arasına enjekte edilebilir. "Arpspoof" aracı ağ üzerinde istenilen ARP paketlerini oluşturup hedefe gönderir ve hedef ARP tablosunu zehirlemeye çalışır. "Arpspoof" aracı aşağıdaki gibi komutlarla kullanılabilir: Ağa bağlı tüm bilgisayarlar hedef IP adresinin sonuna 102 24/Arptable eklenerek zehirlenebilir. Yalnızca bir bilgisayarda ve ağ aygıtında metin araması yapın (Ramadhan, 2018),

Öncelikle hedefin ARP tablosu zehirlenir. Bunun için aşağıdaki komut kullanılmaktadır:

arpspoof-i [network interface]-t [destination ip] [network device ip]

Yukarıdaki komut, hedef bilgisayarın ARP tablosunda yürütülür ve ARP'yi zehirlemek için sürekli olarak REPLY paketlerini hedefe göndermektedir. Daha sonra ağ cihazının ARP tablosu zehirlenir, bunun için aşağıdaki komut kullanılır.

arpspoof-i [network interface]-t [network device ip] [destination ip]

Komut, ARP tablosu ağ cihazını sürekli olarak çalıştırdığında, hedefe toksik ARP REPLY paketleri gönderilir. Ağ cihazı ile hedef bilgisayara gönderilen ARP REPLY paketleri arasına eklenir. Hedef bilgisayarın ARP zehir tablosunu falan kastediyorum. AR çağrısının girildiği hedef bilgisayarı ve ağ cihazını agresif bir şekilde hedefliyoruz. Hedef ile ağ cihazı arasındaki trafiği iletebilirsiniz ve saldırgan bunu değiştirebilir, trafik akışını dinleyebilir (Rangwala, 2015).

Örnek olarak aşağıdaki iki örnek diğer trafikte verilmiştir. Kali kurulumuyla birlikte gelen Linux "urlsnarf" istek hedefleme aracı trafiği azaltabilir. Bunun için kullanılacak komutlar aşağıdadır.

urlsnarf – click [network interface]

"Driftnet" aracı ile Kali Linux kurulumu, ARP Spoofing ve MITM saldırır kurbanın tarayıcı isteklerine yönelik olarak sayfalarda yer alan resimlerin ortamları gerçekleştirilmektedir. Aşağıdaki komut ile yürütülür.

driftnet-click [network interface]

2.1.3. SSL ve TLS Sıyırma

HTTP en yaygın İnternet protokolüdür. Çevrimiçi olarak yaptığımız işlerin çoğu, günlük web taramasından anlık sohbete

kadar HTTP üzerinden yapılır. Bununla birlikte, HTTP iletişimleri güvensizdir ve ele geçirilmesi nispeten kolaydır, bu da özellikleri nedeniyle onları MITM saldırıları için ana hedef haline getirir.

Çoğu şifreleme protokolü, özellikle MITM saldırılarını önlemek için bir tür uç nokta kimlik doğrulaması içermektedir. TLS (Aktarım Katmanı Güvenliği) ve SSL (Güvenli Yuva Katmanı) protokolleri, güvenilir bir ağ bağlantısı sağlamak için ağ şifrelemesini kullanır. En yaygın SSL protokolü türü, en yaygın kullanıcıların karşılaştığı HTTPS'dir. Bu protokol, geleneksel HTTP protokolü (Köprü Metni Aktarım Protokolü) aracılığıyla iletişimden oluşur ve SSL ve TLS şifrelemesi ile korunur. Bu protokoller ağ iletişimi için daha iyi koruma sağlasa da, MITM saldırılarına karşı savunmasız olabilirler. Kullanıcı şüpheli bir sertifika gönderme konusunda uyarılmazsa, saldırgan sahte sertifikalarla MITM saldırısı gerçekleştirebilir (Rouse & Cobb, 2015).

HTTPS kullanımı, ARP zehirlenmesine veya DNS sahteciliğine karşı kapsamlı bir savunma olduğundan, saldırganlar paketleri engellemek ve HTTPS tabanlı adres isteklerini HTTP eşdeğeri uç noktalara iletmek için SSL soymayı kullanır ve sunucunun şifrelenmemiş bir sunucu istemesini gerektirir (Ramadhan, 2018).

SSL/TLS sertifikaları, saldırganların güvenli bağlantılardan ödün vermek için ek adımlar atması gerektiğinden, etkin MITM saldırılarını da zorlaştırır. Bir saldırgan, bir web sitesinin SSL protokolünü modüle eden SSLstrip gibi araçlar kullanılarak yararlanılabilen bağlantı ele geçirme saldırılarını kullanarak bu adımın 103 güvenliğini ihlal edebilir. Bilgisayar korsanları TLS'ye girmenin yolunu buldu. Örneğin, HTTPS yazsanız bile (örneğin https://www.example.com), bilgisayar korsanları http://www.example.com yazıp onu HTTP olarak değiştirerek şifrelenmesini engelleyebilir. Bu arada, tüm kullanıcı oturumu saldırgan tarafından görülebilir.

2.1.4. MAC Address Attact

Portlar arası iletişim, switchler tarafından sahip oldukları MAC adres tablolarına bakılarak gerçekleştirilir. MAC adres tablosundaki port numaralarında bilgisayarların MAC adresleri porta bağlı olup, söz konusu portun hangi VLAN'a (Sanal Yerel Alan Ağı) ait olduğu bilgisi bulunmaktadır. Switchler önce portlara gelen çerçevenin hedef MAC adresi kısmına bakar, ardından çerçevedeki hedef MAC adresinin kendi MAC adres tablosunda olup olmadığını sorgular, adres tabloda bulunuyorsa çerçeve gönderilir. İlgili bağlantı noktası, bu işleme anahtarlama denir. Ancak, anahtar çerçevesinin hedef MAC adresi, anahtarın MAC adres tablosunda bulunmadığında, anahtar çerçeveyi tüm bağlantı noktalarına gönderir. Bu, ilgili bağlantı noktasının diğer tüm bağlantı noktalarına iletilmesine neden olur. Bu, bir saldırganın tüm anahtar trafiğini gizlice dinlemesine ve anahtarın bağlantı noktalarını yok sayarak MAC adres tablosunu yanlış MAC adresleriyle doldurmasına neden olur. Bu, anahtarın verimliliğini olumsuz yönde etkiler. Anahtarlama cihazlarının MAC adres tablosu doldurulurken sorunlar ortaya çıkar çünkü switchlerin MAC adres tabloları için bir limiti vardır ve bu limit cihazın marka, model ve donanımına göre değişiklik gösterir.

3. MITM Saldırısından Nasıl Korunabilir

Ortadaki adam saldırısına karşı birçok savunma mekanizması vardır. Başlıca ortadaki adam saldırıları, SSL saldırısı, DNS saldırısı ve ARP zehirlenmesidir. Bu saldırıya karşı önlemler aşağıda listelenmiştir.

3.1. SSL'nin Zayıf Yönlerini Ortaya Çıkaran Saldırılar ve TLS İle Alınan Önlemler

TLS Aktarım Katmanı Güvenliğinin (TLS) kısaltması. TLS, SSL protokolünün halefi ve İnternet Mühendisliği Görev Gücü (IETF) tarafından SSL tabanlı geliştirilen bir güvenlik protokolüdür. Ağ üzerinden veri gönderilip alınmasını ve veri aktarımı sırasında şifrelemeyi sağlar. STARTTLS, yalnızca metin mesajlarını korumak için farklı bir bağlantı noktası kullanmak yerine şifreli bağlantı olarak güncellenen bağlantı protokolleri için TLS tarafından geliştirilmiş bir çözümdür. SMTP kullanırken TLS, güvenli olmayan bir sunucu bağlantısıyla başlar ve STARTTLS komutuyla devam eder. Daha sonra veri aktarımı sırasında güvenli bir bağlantıya geçer.

Standart algoritma, gönderilen ve alınan bilgilerin kesinlikle doğru olmasını ve doğru alıcının bilgileri göndermeden önce otomatik olarak şifresini çözebilmesini ve şifresini çözebilmesini amaçlar. İşlemlerin ve verilerin bütünlüğünü ve gizliliğini korumak için her iki tarafta doğrulama yapılır. SSL/TLS işleviyle çalışmak için sunucu tarafı anahtarına ve istemci tarafı sertifikasına ihtiyacınız vardır. Özellikleri aşağıdaki gibidir;

- Mesaj şifreleme ve şifre çözme için güvenlik ve gizlilik sağlar (Simetrik Anahtarlama).
- İletiyi gönderen ve alan etki alanının doğru konumda olmasını sağlar (Public/Private Key).
- Aktarılan belgelerin tarih ve saatini doğrular (Hashing tekniği ile).
- Belge arşivleri oluşturmayı kolaylaştırır (sıkıştırma teknikleri ile).

Tekrar HTTPS alırsak, HTTP trafiğini SSL protokolü tarafından sağlanan kanal üzerinden iletilecek şekilde yapılandırabiliriz. Bu kanal, şifreleme ve kimlik doğrulama seçenekleri veya her ikisi ile oluşturulabilir, ancak karşı tarafın hem şifrelemesi hem de kimlik doğrulaması gerekli değildir. OSI katmanı, HTTP'nin "Uygulama" katmanı ile TCP protokolü arasındaki gerçek veri trafiğinin "Taşıma" katmanı arasındaki SSL "Sunum" katmanında bulunan bir protokol yığınına sahiptir.

3.2. SSL 3.0 ve Poodle Saldırısı (2014)

TLS saldırısına karşı önlem, saldırganların protokolü düşürmesini engelleyen TLS_FALLBACK_SCSV eklentisidir. Buna göre istemci, sunucuya düşüşü bildirir. İstemci, sunucuya, oturumun daha yüksek bir sürüm protokolü kullanarak sunucuya bağlanmaya çalıştığını, ancak el sıkışma tamamlanmadan oturumun sonlandırıldığını bildirir. Bu durumda sunucu, istemci tarafından bildirilenden daha yüksek bir sürüm sağlayabiliyorsa bağlantıyı kapatmaktadır. Bu, saldırganların şifreleme protokolünü tersine mühendislik yapmasını engellemektedir.

3.3. Freak Saldırısı (2014)

Entrust'ın internet sitesinde yer alan bilgilere göre siber güvenlik araştırmacısı Ivan Ristic, FREAK'in pratikte çok etkili olabilmesi için birden fazla ajanın bir araya getirilmesi gerektiğini

vurguluyor; listede zayıf bir ihracat şifreleme algoritması sağlayan ve aynı anahtarı uzun süre kullanan bir sunucu, anahtar kırma, zayıf bir istemci bulma ve manipülasyon saldırısı bulunmuştur. Ortadaki adam (MITM) saldırısı, yerel bir ağ veya kablosuz WiFi ağında gerçekleştirilmesi kolay ancak gerçekleştirilmesi zor bir saldırıdır.

Bu saldırıya karşı önlem olarak sunucu taraflı çözümler daha etkilidir. Sunucular, zayıf güvenli şifreleme algoritmalarını desteklememelidir (Hekim, 2015).

3.4. Beast (Canavar) Saldırısı (2011)

BEAST'in iptali, parola blok zinciri (CBC) modunda kullanılan orijinal vektör (IV) değerini kullanır. Bu ağda gönderilen bir paket için kullanılan IV değeri, bir önceki paketin son şifreli mesaj bloğudur. Bu şekilde, şifreli trafiği izleyen bir saldırgan, oturumun çerez bilgisinde kullanılan IV değerini tespit edebilir. Saldırgan, önceki şifreli metin bloğu olan IV değerini aldıktan sonra, şifresini çözmek istediği şifreli metni içeren açık değeri ve ulaşmak istediği hassas değeri (örneğin, çerez bilgisi) iki değeri kullanarak tahmin etmeye çalışır. Saldırgan, düz metin tahmin edilebilirse IV'ü XOR yapabilir ve ilgili şifreli metinle aynı olup olmadığını kontrol edebilir. Aynıysa, saldırgan açık metni alır. Böyle rastgele bir değeri tahmin etmek zor olacağından, bu saldırı açık harf kod çözme yöntemini kullanır. Bunu yapmak için saldırganın kurbanla aynı ağda olması ve bir müdahale yapması gerekir. Ayrıca trafiği manipüle edebilmeli ve birden fazla istek paketi göndermeyi gerektiren olası sorunlu eşleşmeleri kontrol edebilmelidir. Saldırgan bir seferde yalnızca bir blok tahmin edebilir.

3.5. SSL Rc4'ün Açıkları

Bu saldırı en iyi sonucu RC4 çıkışına verilen orijinal hasarla verir. Bu nedenle kayan anahtarın ilk çıktı baytlarını azaltmak, RC4'teki zafiyete TLS çözümleri arasında yer alıyor ancak bunun tüm sunuculara ve istemcilere uygulanmasının zor olduğu vurgulanıyor. Bu nedenle uzmanlar, kötüye kullanımdan kaçınmak için TLS'de RC4'ten kaçınılması gerektiğini vurgulamaktadır (Hekim, 2015).

3.6. Heartbleed (Kalp Kanaması) Saldırısı (2014)

Bu güvenlik açığına yönelik OpenSSL yaması, yük uzunluğu alanı veri uzunluğundan büyükse HeartbeatRequest mesajını kaldırmaktadır. Bu güvenlik açığını önlemek kolaydır, ancak bir saldırganın hassas bilgiler içeren özel belleği okuyabilmesi nedeniyle güvenlik açığından kaynaklanan potansiyel risk büyük zarara neden olabilmektedir.

3.7. MITM'de DNS Değişikliği ve Yaralanma

3.7.1. DNS Önbelleğe Alma

Aynı problemde önbelleğe almak için kullanılan cihazları, çok fazla saldırıya sahip DNS sunucularını ve DNS sunucusu efektlerini önbelleğe alamaz.

3.7.2. DFAS

TCP üzerinden DDoS saldırılarını engellemenin nispeten kolay olduğunu söylenebilir. Bunun ana nedeni, TCP üzerinden saldırırken, saldırganın gerçek bir IP adresine mi yoksa sahte bir adrese mi saldırdığını anlayabilmesidir (basit bir Boolean 3 el sıkışması yapılırsa, IP gerçektir). UDP üzerinden DDoS saldırılarının (UDP taşması, DNS taşması vb.) engellenmesi zordur çünkü saldıran IP adreslerinin gerçek olup olmadığını belirlemenin kesin bir yolu yoktur. UDP kullanan saldırılar, genellikle ikinci bir paket bloğunu (DfA) kabul etmek gibi bir davranışsal engelleme yöntemi kullanır. DFAS yöntemi, TCP veya UDP olmak üzere ilk gelen paketi temel almaktadır. Aynı paket geri gelirse, pakete uygun şekilde yanıt verin ve ilgili IP adresine giriş yapmaya başlayın veya ilk paketin yanlış bir yanıt (yanlış sıra numarası SYN) döndürmesini bekleyin. -ACK) . istemci tarafından gönderilen TCP isteğine yanlış yanıt verir ve karşı taraftan RST paketi beklenir. RST paketini aldıktan sonra IP adresinin gerçek olup olmadığı belirlenerek paket belirlenir. DFAS yöntemi, saldırı anında ilk paketler üzerinde gerçekleştirilir (Sultana, 2018).

3.7.3. Hız Sınırlama

Hız sınırlama yöntemi, IP adresleri ve UDP/DNS kullanan saldırılarla bağlantılı olarak saldıran IP adresini engellemeyi amaçlar. Kaynak IP adresleri doğrulanamadığından, UDP saldırılarının bu yöntemi kullanarak engellenmesi zordur. Bu yöntem ile istenilen IP adresi bloke edilebilir (Sultana, 2018).

3.8. Arp Sahtekarlığını Önleme

3.8.1. Sanal Özel Ağlarla Şifreleme

Ağ trafiği şifreli ise paketler yakalansa dahi okunamayacağı için çalışmayacaktır. Verileri şifrelemenin ve ARP sahtekarlığının oluşmasını önlemenin bir yolu, sanal özel ağları (VPN'ler) kullanmaktır. Bir VPN kullanmak, ARP saldırılarını büyük ölçüde önlemektedir.

3.8.2. Statik ARP Kullanımı

ARP tablosunu statik olarak doldurmak, ARP duyurularına ihtiyaç duymadığı için bu saldırıyı engeller, ancak büyük ağlar için daha az karlıdır. Ortamınızda birbiriyle sürekli iletişim halinde olan iki sunucunuz varsa, ARP girişini statik olarak ayarlamak, ARP önbelleğinize herhangi bir saldırıya karşı bir koruma katmanı eklemenize yardımcı olabilir.

3.8.3. Algılama Aracı Alma

Yaygın uygulamalarda bile, yüksek ARP bilgisine sahip olsanız bile ARP saldırılarını tespit etmek kolay değildir. Müşteri, IDS (Intrusion Detection System) veya ARP Monitor ile sistemi dahili ağda izleyebilir. Örneğin, Arpon ve Arpalert gibi açık kaynak araçları kullanarak ARP protokolü güvenilir bir şekilde çalışır (Sultana, 2018).

Ağ şirketleri tarafından satılan ürünlere yönelik saldırıları önlemek için ARP koruması veya Dinamik ARP Denetimi özellikleri etkinleştirilebilir.

3.8.4. Paket Filtrelemeyi Ayarlama

Bazı ARP saldırılarında, saldırganın MAC adresini ve kurbanın IP adresini içeren ARP paketleri LAN üzerinden gönderilir. Bu gelen paketleri filtrelemek, bu toksik paketlerin hedeflenen hasara neden olmadan kullanılabilmesini sağlayabilir. Ek olarak, ağı daha küçük VLAN'lara bölmek ve yetkili kullanıcıları dışarıdan izole etmek, bir ARP zehirlenmesi saldırısının yüzey alanını azaltır.

4. Uygulanan Yöntem

Siber saldırılara karşı alınacak önlemler çok önemlidir. Son kullanıcının belli önlemleri alınması kesinlikle gereklidir. Ancak

sistem yöneticisi ya da bir başka deyişle bilgisayar ağ yöneticisi tarafından alınan önlemler çok daha önemli ve verimli olacaktır. Sonuç olarak kesin önleyici önlem olacaktır.

Sistem yöneticisinin alması gereken önlemleri ve kendi bilgisayar ağımızda almış olduğumuz önlemleri sırasıyla belirtelim.

4.1. Tüm Bilgisayar Ağında Yönetilebilir Akıllı Ağ Anahtarları Kullanılmalı

Bilgisayarı ağ yöneticisi, yönettiği sistemde kesinlikle akıllı yönetilebilir ağ anahtarları kullanmak zorundadır. Siber saldırılara karşı bilgisayar ağı üzerinde önlem almanın en temel koşulu budur.

Bizim yaptığımız çalışmada, kurumun tüm bilgisayar ağında yönetilebilir ve akıllı ağ anahtarları kullanılmıştır.

4.2. Olay Kayıt Sunucusu Kurularak Bilgisayar Ağındaki Tüm Ağ Anahtar Cihazlarının Tüm OlaylarıKayıt Altına Alması Sağlanmalı

Bizim yaptığımız çalışmada, tüm bilgisayar ağında kullanılan yönetilebilir ve akıllı ağ anahtarları olay kayıt sunucusuna bağlanmıştır.

4.3. Tüm Ağ Anahtar Cihazlarına Yabancı Bir Ağ Anahtar Cihazının Bağlanmasını Engelleyici Ayarlar Yapılmalıdır.

Bilgisayar ağ anahtarlarının tüm bağlantı uçlarının sadece bilgisayar bağlanabilecek konfigürasyonunda ayarlanması çok önemlidir. Bunun nedeni herhangi yetkisiz bir kişinin bilgisayar ağına sistem yöneticisinin kontrolü dışında farklı bir ağ anahtarı bağlanmasını ya da herhangi bir sunucu bağlanmasını engellenmesi içindir.

Yapılan ayarlar,

switchport mode access

switchport port-security

switchport port-security aging time 2

switchport port-security violation restrict

switchport port-security aging type inactivity

macro description cisco-desktop spaning-tree portfast

spaning-tree bpduguard enable

Yukarıda verilen tanımlamalar yapıldığında ağ anahtarını bağlantı uçlarına bilgisayar özelliği dışında hiçbir cihaz bağlanamaz. Eğer başka bir cihaz bağlanır ise port kendini kapatır. Aynı zamanda log sunucusuna da olay kaydı yapılmış olur.

4.4. DHCP Saldırılarını Önleyici Ayarlar Yapılır

ip dhcp snooping vlan 1

ip dhcp snooping information option allow-untrusted

ip dhcp snooping

ip dhcp snooping limit rate 100

Saniyede 100 paket sınırı normal olarak konulabilir. Ağ yöneticisinin kararına bağlı olarak değişebilir.

4.5. ARP Saldırılarını Önleyici Ayarlar Yapılır

ip arp inspection vlan 1

Bu ayar ile varsayılan saniyedeki arp paket sınırı 15 adettir. İstendiğinde değişik paket sayıları da ayarlanabilir.

4.6. Otamatik Olarak Devre Dışı Kalan Uçlar

Kural dışı çalışma olduğunda ağ anahtarının ilgili ucu devre dışı kalır.

Devre dışı kalan uçları belli bir zaman sonra kendiliğinden tekrar devreye almak için belli ayarları yapmamız gerekecektir.

errdisable recovery cause arp-inspection

errdisable recovery cause bpduguart

errdisable recovery cause psecure-violation

errdisable recovery interval 300

Burada verilen 300 saniye sonra kendiliğinden ucun aktif olması komutudur. İstenirse zaman ayarı değiştirilebilir.

5. Sonuç

Katman 2 saldırıları, LAN'lar (Yerel Alan Ağları) nedeniyle güvenlik duvarlarına veya saldırı tespit sistemlerine müdahale etmez. Genel olarak, izinsiz giriş tespit veya önleme sistemleri, bir iç ağa girebilecek harici bir ağdan gelen saldırıları tespit etmek veya önlemek için kullanılır. Bu sistemler üçüncü ve daha üst düzey koruma için tasarlandığından, iç ağdaki bir saldırgan, iç ağdaki anahtarlara yapılan saldırıları algılayamaz veya önleyemez. Ağ güvenliğini sağlamak için tüm OSI katmanları korunmalıdır. Üst düzey güvenliğin olmaması ve ikinci düzey güvenliğin olmaması, yetersiz ağ güvenliğini gösterir. Birinci kat saldırıları da önemlidir. Örneğin, ağın sunucuları ve diğer cihazları kesintisiz bir güç kaynağına veya jeneratöre bağlı değilse, ağın tüm güvenlik önlemleri alınmış olsa bile, elektrik kesintisi durumunda ikinci katman ve daha yüksek güvenlik önlemleri çalışmayacaktır. Ya da güç anahtarı herkesin ulaşabileceği bir yerdeyse ve yeterli güvenlik önlemleri alınmazsa, elektrik kesintisi durumunda sistem çalışmayacağından üst katlarda alınan önlemler çalışmayacaktır.

Sunucu sertifikası doğrulaması yalnızca istemcide yapılır ve istemcinin sertifikası bir doğrulama noktası olduğundan sunucuya aktarılamamaktadır, bu nedenle istemci doğru sunucuyla konuştuğundan emin olmalıdır. Sunucu (güvenilmeyen) bu kararı istemciye vermektedir. SSL müdahalesinde, sunucunun bakış açısından TLS istemcisi bir güvenlik duvarı/AV'dir. Dolayısıyla sunucu tarafı sorunu, beklenen istemcinin (tarayıcının) konuşup konuşmadığını (güvenlik duvarı/AV) tespit etmektir. Bunu yapmanın en güvenli yolu, istemcinin kimliğini doğrulamak için istemci sertifikalarını kullanmaktır - ve örneğin, istemci kimlik doğrulaması kullanılırsa, MITM beklenen istemci sertifikasını sağlayamadığı için SSL korsanlığı çalışmamakta, TLS anlaşması başarısız olmaktadır. Yalnızca istemci sertifikaları nadiren kullanılmaktadır. Başarısız bir TLS anlaşması, istemcinin sunucuyla SSL güvenliğinden ödün vermeden iletişim kurabileceği anlamına gelmez, ancak istemci sunucuyla iletişim kuramamaktadır. Alternatif bir yaklaşım, TLS istemcisinin parmak izine, yani parolalara ve parolalara ve özel uzantıların kullanımına dayalı olarak TLS istemci türünü belirlemek için buluşsal yöntemleri kullanmaktır. Teori orijinali yanıltsa da, ClientHello aslında bir SSL yakalama proxy'sine sahip değildir.

İnternet kullanıcılarının SSL/TLS, DNS ve arpspoofing saldırılarına karşı alması gereken önlemler detaylı olarak analiz edilmektedir. Ağ güvenliğini değerlendirmede makine öğrenmesinin etkinliği nedeniyle; son zamanlarda daha da önem kazanmıştır. Benzer şekilde, veri vergilendirmesinde yeni makine öğrenimi teknikleri daha hızlı büyür ve daha verimlidir. Makine öğrenimini uygularken, ortadaki adamın doğası dinamik olduğu için dikkate alınması gereken farklı şeyler vardır. Bu nedenle, gözlem yönteminin uyarlanabilirliğine ihtiyaç vardır. Veri kümesi boyutunu azaltan sınıf parçalarıyla bir özellik seçme yöntemi geliştirmek, devam eden bir konudur.

Sonuç olarak, işin özüne bakarsak, bilgisayar ağ yöneticisinin alacağı önlemlerin kesin olarak etkili olacağı gözlemlenmiştir.

Kaynakça

Hekim, H. (2015). Oltalama (Phishing) Saldirilari. Retrieved from academia: http://www.academia.edu/35136881/Oltalama_Phishing_Saldirilari

Hugo, E. (2016, March 28). Performing Man-In-The-Middle Attack with ARPSpoof. Retrieved frommyhackingjournal.blogspot: http://myhackingjournal.blogspot.com/2016/03/performing-manin-middle-attack-with-arpspoof.html

Infosec Kılavuzu: Ortadaki Adam Saldırılarına Karşı Savunma, (2017).

Man-in-the-Middle (MITM) Attacks. (2018). Retrieved from rapid7: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Ramadhan, F. B. (2018). Kali Linux: Social Engineering Toolkit. Retrieved from linuxhint

Rangwala, S. (2015). Fake Website with DNS Spoofing in Kali Linux. Retrieved from linuxhacking-guide.blogspot: http://linux-hacking-guide.blogspot.com/2015/05/fake-website-withdns-spoofing-in-kali.html

Rouse, M., & Cobb, M. (2015). Man-in-the-middle attack (MitM). Retrieved from internetofthingsagenda.techtarget: https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM

Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2018). Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications.

Tanenbaum, Andrew S.,(2003). Computer Networks"ü, 4th ed, Prentice-Hall, Inc., New Jersey

Tanmay. (2013). How to defend yourself against MITM or Man-in-the-middle attack. Retrieved from thewindowsclub: http://www.thewindowsclub.com/man-in-the-middle-attack

Toward More Resilient Cyber Infrastructure: A Practical Approach, (2016).

Yüksel, M. ve Öztürk, N. (2017). SIP Saldırıları ve Güvenlik Yöntemleri BİLİŞİM Teknolojileri Dergisi, 10(3).