22.12.2021

TRAKYA ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

PROJE 1: Bilgisayar Ağlarına Yapılan Saldırıların Sınıflandırılması

Ad Soyadı: Emre Özen / Berkay Cihan
Numara: 1181602054 / 1191602801

GİRİŞ

Teknolojinin gelişmesi ile birlikte bilgiye erişim olanakları artar. Ancak bilgiye erişimin kolaylaşması da bilginin güvenliğinin sağlanmasını zorlaştırır. Günümüz bilişim sistemlerinin hayatın her alanında kullanılmaya başlaması ile siber saldırı şikâyeti kavramı ön plana çıkmıştır. İnternet, gündelik yaşamdan devlet kurumlarına, ekonomiden ticarete, bankalardan hastanelere kadar geniş bir alana yayılmış durumdadır.

Cep telefonu, sosyal medya, web siteleri ve e-posta aracılığı ile bir kişi ya da grup tarafından bireyi küçük düşürücü duyuru ve yayınlar yapılmasına siber saldırı denir. Bu saldırılar sonucunda sitelere veya bilgisayarlara trojanlar ve solucanlar sokulabilir. Açıklar bulunarak bilgiler ele geçirilebilir veya yok edilebilir.

Bazen şahıslar bazen de ülkeler birbirleri ile siber savaş içine girerler. Saldırılar sadece veri çalmak veya veriyi ele geçiren saldırganlara misilleme yapmak amacı ile gerçekleşebilir. Siber saldırılarda verilebilecek hasarın büyüklüğü, saldırıyı yapan kişilerin bu alandaki uzmanlığına bağlıdır.

Tehdit türleri aşağıdaki şekilde sınıflandırılabilir;

a) Erişim Kontrolü Saldırıları (Access Control Attacks)

b) Gizlilik Saldırıları (Confidentiality Attacks)

c) Bütünlük Doğrulama Saldırıları(Integrity Attacks)

d) Kimlik Doğrulama Saldırıları (Authentication Attacks)

e) Kullanılabilirlik saldırıları (Availability Attacks)

a) Erişim Kontrolü Saldırıları (Access Control Attacks)

Bu saldırılar, Erişim Noktası MAC filtrelemesi ve 802.1X port erişim kontrolü gibi Kablosuz Ağ erişim kontrol önlemlerine karşı, radyo frekanslarını gizlice dinleyerek ağ girmeyi dener. Kısaca Kablosuz Ağda bulunan Erişim kontrol önlemlerini anlayarak bunları delip sisteme girmek için yapılan ataklardır,

Kablosuz Ağları Tarama (War Driving)

Wardriving, ilk ve en çok bilinen kablosuz ağ tespit etme (tabii ki güvenliği olmayan ya da az olan) metodudur. Genellikle bir gezici birim ile mesela dizüstü veya el bilgisayarları ile kullanılır. Wardriving taraması son derece ustalıkla ve çok basit

yollarla gerçekleşir: Saldırgan dizüstü veya el bilgisayarı ile arabasında otururken bir kablosuz ağ tespit edebilir. Bir kere uygun bir AP tespit edildikten sonra saldırgan bunu kullanılabilir klasör olarak tanımlar ve araştırabilir. Ve hatta internete ulaşmasını

engelleyebilir. Wardriving için kullanılan ‘war’ kelimesi aslında eski zamanlarda kullanılan Wardialing’den gelmektedir. Wardialing, saldırı amacıyla kullanmak üzere bir telefon numarasının bütün ihtimallerini deneyerek modem takılı olan hattı bulmak olarak tanımlanabilir. Bu yazıda kullanılan Wardriving de kablosuz ağlar için aynı mantıkta kullanılmaktadır.

Yetkisiz Erişim Noktası (Rogue Access Point)

Bir yetkisiz erişim noktası, hassas bilgilere erişmek isteyen kötü niyetli kişilerin kullandığı ya da yeterince güvenlik bilgisi olmayan yöneticilerin kendi veya şirket faydası için ofislerine kurdukları AP'lerdir. Her iki durumda da, bu yetkisiz AP'ler

güvenliği tehdit etmektedir. Yetkisiz AP'ler, karışmaya (interference) neden olacaklar ve sistem başarımını düşüreceklerdir. Daha da kötüsü, yetkisiz kişilerin (saldırgan) ağa erişmesine neden olmaktadır. Telsiz ağ durakları, ilişkilendirildikleri AP'den ayrılıp, kendilerine daha yakın olana bir yetkisiz AP ile ilişkilenebilirler. Bu durum WEP'in etkin duruma getirilmemesinde oluşur. Yetkisiz AP'den faydalanan bir saldırgan, yetkisiz AP ile ilişkilenen diğer ağ duraklarına erişebilir. Yetkisiz AP'nin kablolu ağ tarafına da bağlı olması, saldırganların kablolu ağa da erişmesini sağlamaktadır.

Mac Adres Sahteciliği (Mac Spoofing)

Güçlü kimlik formları kullanıldığında ALC (Erişim Kontrol Listeleri) ler kabul edilebilir bir güvenlik seviyesi sağlamaktadırlar. Ne yazık ki ayni şey MAC adresleri için geçerli değildir. MAC adresleri WEB kullanılabilir durumda iken dahi şifresiz metin olarak saldırgan tarafından kolaylıkla dinlenebilir. Ayrıca, kablosuz ağ kartlarının bir yazılım vasıtası ile MAC adresleri kolaylıkla değiştirilebilir. Saldırgan tüm bu avantajları kullanarak ağa nüfuz edebilmektedir. MAC adresini dinlemek çok kolaydır. Paket yakalama yazılımı kullanarak saldırgan kullanılan bir MAC adresini tespit eder. Eğer kullandığı kablosuz ağ kartını izin veriyorsa MAC adresini bulduğu yeni MAC adresine değiştirebilir ve artik hazırdır. Eğer saldırgan yanında kablosuz ağ donanımı bulunduruyorsa ve yakınında bir kablosuz ağ varsa, artik aldatma saldırısı yapabilir demektir. Aldatma saldırısı yapabilmek için,

saldırgan kendine ait olan AP'yi yakınındaki kablosuz ağa göre veya güvenebileceği bir internet çıkısı olduğuna inanan bir kurbana göre ayarlamalıdır. Bu sahte AP'nin sinyalleri gerçek AP den daha güçlüdür. Böylece kurban bu sahte AP'yi seçecektir.

Kurban bir kere iletişime başladıktan sonra, saldırgan onun şifre, ağ erişim ve diğer önemli bütün bilgilerini çalacaktır. Bu saldırının genel amacı aslında şifre yakalamak içindir. Bunu yapmanın birkaç yolu vardır.

Kendimiz adres değişikliği yapabiliriz. Ağ üzerinde bir Ethernet frame gönderdiğimizde yazılım vasıtasıyla bu alana müdahale edip, tekrardan configüre edebiliriz.

Bazı kartlar Windows'taki denetim ayarları vasıtasıyla MAC adreslerini düzenlemeye yardımcı olur. Kart içerisindeki adresi

yenileyebiliriz. Bunun için kullanılan chipset'in özelliklerini bilen bir yazılıma ihtiyaç duyup, kart üzerine yeni bir adres atanması sağlanabilir. Anakart üzerindeki dâhili ethernet kartlarının MAC adresleri de BIOS ayarlarından değiştirilebilir. Linux

kullanıcıları aldatma yazılımı olmaksızın "ifconfig" gibi tek bir parametre kullanarak MAC adreslerini değiştirebilir. Aynı zamanda Mac adres değiştiren birçok program internette mevcuttur.

Ip Adresi Yanıltma (Ip Spoofing)

İnternetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek

davranılmıştır. Bu esneklik IP adreslerinin aldatılabilir (spoofed) olmasını sağlamıştır. Ip spoofing yaparak başkasının IP adresinden istenilen internet aktivitesi yapılabilir. Son yazdığımız cümle bundan on sene öncesi için geçerli olsa da günümüzde pratik olarak geçersizdir. Bunun temel nedeni günümüz modern işletim sistemlerinin protokoldeki eksik noktalara kalıcı çözüm getirmeleridir. Özellikle internet de en sık kullanılan HTTP, SMTP, HTTPS gibi protokollerin temelinde bulunan TCP bu tip sahtecilik işlemlerini engelleme amaçlı bir yöntem kullanır.

Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)

Araçların direk olarak birbirleriyle iletişimine imkân sağlar. Araçlar ağ içerisinde hareket edebilir ve kendi kapsama alanında olan herhangi bir araca bağlanabilir. Baz istasyonu yoktur. Düğümler sadece kapsama alanındaki diğer düğümler ile haberleşir. Düğümler ağ içinde kendilerini organize eder.

802.1x Radius Cracking

Şeytan İkizi Erişim Noktası(Evil twin AP)'nın kullanması için kaba kuvvet (brute force) yoluyla 802.1x erişim isteklerinden RADIUS gizlilerini elde etme yöntemidir. Bir başka deyişle bu saldırıyı yapacak saldırgan, yerel alan ağları ya da erişim noktası ile RADIUS Server arasındaki ağ yolu üzerinde veri paketlerini toplamak için uğraşır.

b) Gizlilik Saldırıları (Confidentiality Attacks)

İster Yüksek katman protokolleri olsun, ister 802. 11 içinde şifreli ya da açık gönderimler olsun, Bu ataklar kablosuz bağlantılar üzerinden gönderilen özel bilgileri engellemek için girişimde bulunurlar.

Gizli Dinleme (Eavesdropping)

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce

"eavesdropping" (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik

parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

Wep Anahtarı Kırma (Wep Key Cracking)

WEP'in açıkları ile alakalı birden çok makale yayınlanmıştır. Wep'in zayıflıkları yüzünden günümüzde gelişmiş WPA, WPA-2 gibi daha güvenli standartlar oluşturulmuştur. Wep'in bu açıkları saldırganları aktif ya da pasif saldırılar düzenlenmesine olanak sağlar. Amaç WEP anahtarını kırılmasıdır. Frekans bandı dinlenerek sonuca varılmaya çalışılır. Pasif Saldırılar IV çakışmalarından elde edilen sonuçlara göre yapılan saldırılar olup, aktif saldırılar ise Replay (tekrar) saldırıları ve mesajın içeriğini değiştirerek yapılan saldırılardır.

Şeytan İkizi Erişim Noktası (Evil Twin Ap)

Saldırganlar, söz konusu sistemi şaşırtmak için, kullanılmakta olan Access Point'un benzerini yaratıp, kullanıcıların o, Erişim noktasını kullanmasını sağlayabilirler. Böylelikle, yaratılmış ikiz AP ye giren kullanıcının tüm bilgileri elde edilebilir.

Ap Üzerinde Sahte Portal Çalıştırmak (Ap Phishing)

Saldırganlar kullanıcıların Evil Twin AP'ye bağlanmasından sonra bir Web sunucusu kurarak, bu saldırganları çeşitli web sayfalarına yönlendirip, hedefi olduğu kişiler hakkında, sayfadaki zararlı kodlar vasıtasıyla bilgi toplayabilirler.

Ortadaki Adam Saldırısı (Man In The Middle)

Bu saldırı yöntemine bu alanda farklı kaynaklarda bucket brigade attack (elden ele kova saldırısı) ismi de verilir. Buradaki benzetme eski zamanlarda itfaiye erlerinin elden ele taşıdıkları ve yangını söndürmek için kullandıklara kovalardan gelmektedir.

Bu saldırıda, saldırgan hedef iki bilgisayar arasındaki iletişimi ele geçirmek üzere kendini araya ekler. Verilerin iki hedef arasında doğrudan iletilmesi yerine, saldırgan üzerinde değişime uğratılarak gönderilir. Fakat bu işlemi iki bilgisayarda anlayamaz.

1.) Kablosuz saldırgan, kablolu ağdaki anahtara takılı AP üzerinden aynı anahtara takılı olan 2 ayrı kullanıcıya ortadaki adam saldırısını gerçekleştirebilir.

2.) Kablosuz saldırgan, kablosuz bir kullanıcı üzerinden, AP nin takılı olduğu hub veya anahtara ortadaki adam saldırısı yapabilir.

3.) Kablosuz saldırgan farklı AP lerde olan kullanıcılara her iki AP'yi de kapsayan bir saldırı düzenleyebilir.

c) Bütünlük Doğrulama Saldırıları (Integrity Attacks)

Diğer atak tiplerini kolaylaştırmak ve ya alıcıyı yanıltmak için bu ataklar, sahte kontrol, yönetim ve ya kablosuz iletişim üzerinden veri paketleri gönderir DoS saldırıları buna örnektir. DoS saldırıları ayrı bir bölüm olarak incelenmiştir.

802.11 Paketi Püskürtme (Frame Injection)

Bu yöntem, sahte 802.11 paketlerini erişim noktalarına ya da saldırgana göndererek, bir süre sonra kaynağın ya servis dışı olmasına ya da gerekli bilgileri dışarı vermesini sağlar. Bunun çok çeşitli programlar vardır. Bu programlar için ya da başka deyişle püskürtme için önemli olan programlar şu mantığı uygular.

a) İlk önce Erişim noktası araştırılır.

b) Açıklar aranır.

c) De-Authentication ve De-association saldırıları için paket püskürtürler.

d) Her donanım sürücüsünü desteklemedir.

802.11 Veri Tekrarlama (802.11 Data Replay)

Bir saldırı tekrarı için hem paket toplamak, hemde aynı zamanda bu paketleri yineleyerek püskürtmek amaçlıdır. İşin içinde hem kayıt etmek hem de paket püskürtme tekrarları vardır.

802.1x EAP Tekrarlama (802.1x EAP Replay)

802.1X Genişletilebilir Kimlik doğrulama protokollerinden paket yakalamak amaçlıdır. Böylece sisteme bu paketlerle tekrar saldırısı yapabilir.(Extensible Authentication Protocols) (v.s. EAP kimlik, başarı, Hata gibi paketleri yakalar)

802.1x Radius Tekrarlama (802.1x Radius Replay)

RADIUS Erişim Kabul ve ya Ret mesajlarını yakalamaktır. Erişim noktası ile Kimlik doğrulama ana makinesi arasında tekrar saldırıları yapmakta sonra gelen adımdır.

d) Kimlik Doğrulama Saldırıları (Authentication Attacks)

Davetsiz misafirler bu atakları, legal kullanıcıların kimlik ve kimlik bilgilerini çalarak özel bir ağa veya servise bağlanmak için kullanırlar

Shared KeyGuessing: Kırılmış WEP anahtarı ya da varsayılan sağlayıcı ile 802,11 paylaşımlı anahtar kimlik doğrulawasını tahmin etme girişiminde bulunmaktır.

PSK Cracking: Sözlük Saldırı araçları kullanarak kaydedilmiş anahtar tokalaşma (handshake) paketlerinden WPA/WPA2 PSK'yı elde etmektir.

Application Login Theft: Açık Metin uygulama protokollerinden kullanıcı bilgilerini ya kala madır.(e-mail, adres, şifre)

Doma in Login Cracking: Sözlük veya kaba kuvvet saldırıları kullanan karma NETBI OS şifre kırma işlemi yoluyla kullanıcı bilgilerini (Windows Giriş ve şifre) elde etmektir.

VPN Login Cracking: VPN kimlik doğrulama protokolleri üzerinde kaba kuvvet saldırıları kullanarak kullanıcı kimlik bilgilerini(PPTP şifresi veya I Psec Preshared Secret Key) elde etmektir.

802.1x Identity Theft: Açık metin 802.1X Kimlik yanıtlama paketlerinden kimlik bilgilerini yakalamaktır.

802.1x Password Guessing: Elde edilen bir kullanıcı adı ile 802.1X kimlik doğrulama yönteminde kullanıcın şifresini tahmin etmek için ardı ardına girişimde bulunmaktır.

e) Kullanılabilirlik Saldırıları (Availability Attacks)

Bu ataklar, yasal kullanıcılara yönelik kablosuz servislerin verimini azaltmak ve ya engellemek için kullanılır. Amaç, gerek bu kullanıcıların WLAN kaynaklarına erişimini engellemek gerekse de kaynaklarını azaltmaya yöneliktir.

AP Theft: Kullanım uzayından fiziksel olarak erişim noktasını çıkarmaktır.

Queensland DoS: Meşgul görünen bir kanal yapmak için CSMA/CA'dan yararlanma ktır.

802.11 Beacon Flood: İ stasyonların yasal bir erişim noktasını bulmasını zorlaştırmak için binlerce sahte 802.11 beacon(hat kesme iletisi) üretmektir.

802.11 Associate / Authenticate Flood: Bir erişim noktasının dahil olma (association) tablosunu doldurmak için rastgele MAC adreslerinden sahte kimlik doğrulama ve dahil olmaları göndermektir.

802.11 TKIP MIC Exploit: Geçersiz TKIP verileri üreterek, erişim noktasının MIC hata eşiğini aşmasını, WLAN servislerinin askıya alınmasını sağlar.

802.11 Deauthenticate Flood: Erişim noktasından, bağlı olmayan kullanıcıları istasyonlar aracılığıyla sahte kimlik doğrulamama ve dahil olmama mesajlarna boğmakbr.

802.1x EAP-Start Flood: Hedefi çökertmek ya da kaynakları tüketmek için EAP-Start mesajlarıaracılığıyla erişim noktasını boğmaktr.

802.1x EAP-Failure: Geçerli bir 802.1x EAP değişimini gözlemledikten sonra istasyona sahte EAP-Hata mesajları göndermektir.

802.1x EAP-ofDeath: Hatalı oluşturulmuş 802.1x EAP kimlik yanıtı göndererek bilinen bir erişim noktasını çökertmeye çalışır.

802.1x EAP Length Attacks: Kötü uzun alanlar aracılığıyla EAP özel tip mesajlar göndererek bir erişim noktası veya RADIUS sunucuyu çökertmeye çalışmayı denemektir. [1,2]

Kaynakça

https://www.avansas.com/blog/siber-saldiri-nedir-sirketler-siber-saldirilara-karsi-neler-yapmalidir

https://tr.linkedin.com/pulse/kablosuz-a%C4%9Flara-yap%C4%B1lan-sald%C4%B1r%C4%B1-t%C3%BCrleri-%C3%B6zden-er%C3%A7in-msc-

https://www.slideshare.net/bgasecurity/kablosuz-alara-yaplan-saldrlar

https://cdn-acikogretim.istanbul.edu.tr/auzefcontent/19_20_Bahar/acil_durum_teknolojileri_ve_haberlesme/7/index.html