Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Eğitim Modülü

Çalışanlar için Bilgi Güvenliği **Ünite 2 Hafta 4** **Birim adı: Kötü Amaçlı Yazılım ve En Yaygın Saldırılar**	
Öğrenme Aktiviteleri	❑ **Web Semineri** ❑**Alıştırmalar** ❑**Atölye Çalışması** ❑**Sunum** ❑Diğer
Öğrenme Sorumlusu	Claudio Fornaro
Öğrenme Etkinliği Hedefleri	1. Çeşitli kötü amaçlı yazılım türlerine giriş 2. En yaygın saldırı türleri hakkında bilgi
Kazanılacak Beceriler	• Kötü amaçlı yazılımın ne olduğu ve bilgisayar sistemlerine yönelik en yaygın saldırılar hakkında temel bilgiler Yumuşak Beceri 2 - SS2
Öğrenme aktivitesinin süresi	1 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • Önceden özel bilgi gerekmez

Modül hakkında bilgi

Kötü amaçlı yazılım söz konusu olduğunda, isim zaten kötü amaçlı bir şey ima ediyor. Bu terim genellikle, özellikle (ancak bunlarla sınırlı olmamak üzere) çeşitli türlerde hasara neden olmak için kasıtlı olarak tasarlanmış yazılımları ifade eder: hizmetlerin ve iletişimin engellenmesi, aktarımların engellenmesi, özel bilgilerin (kişisel, kurumsal veya devlet) ve kişisel kimliklerin çalınması, bilgi veya sistemlere yetkisiz erişim, kullanıcıların bilgiye erişimden yoksun bırakılması gibi durumlar anlatılmıştır.
Giriş bölümünden sonra, kötü amaçlı yazılımların temel kavramları, ana türlerin tanımı, içerdikleri riskler ve bunların nasıl azaltılabileceği ile özetlenmiştir.
Modülün ikinci kısmı, bir sistemin maruz kalabileceği en yaygın saldırılara genel bir bakış sunmayı amaçlamaktadır; bu liste, her gün yeni saldırı türleri keşfedildiğinden hiçbir şekilde eksiksiz değildir. Bu saldırılar, bir bilgisayar sistemine erişim sağlama veya hizmetlerini kesintiye uğratma girişimleridir. Açıklama, en yaygın ve en kolay saldırılardan (Kimlik Avı) daha karmaşık olanlara doğru başlar: Parola Saldırıları, Arabellek Taşması, SQL Ekleme, Siteler Arası Komut Dosyası Çalıştırma (XSS), Siteler Arası İstek Sahteciliği (CSRF), Dosyayla İlgili Saldırılar, Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS), Ortadaki Adam (MITM) , ARP Kimlik Sahtekarlığı veya ARP Zehirlenmesi, DNS Kimlik Sahtekarlığı, Drive-by Saldırıları, Kimlik Bilgilerini Yeniden Kullanma, Web Oturumu Ele Geçirme, TCP Oturumu Ele Geçirme, IP Kimlik Sahtekarlığı, Sıfır Gün Açıklarından Yararlanma ve Kod Sızıntısının Sonuçları ile devam edecektir.

Öğrenme Materyalinin İçeriği

Bilgisayar bilimlerinde, "hacker" ve "cracker", bilgisayar sistemleri hakkında büyük bilgiye sahip insanları belirtmek için kullanılan iki terimdir. İkisi arasındaki temel fark, hareket ettikleri tutumda yatmaktadır. Bir hacker (terim 1900'lerin ikinci yarısında MIT'de doğdu), nasıl çalıştıklarını daha iyi anlamak için sistemleri keşfederek ve bunları çözmek için yeni kusurlar keşfetmeye çalışarak hareket eder ve bu nedenle bir sistemin güvenliğini arttırır. Bazı eylemler yalnızca gösterişli veya etik nedenlerle olabilir, ancak asla kar amacı gütmez. Öte yandan bir kraker, yeteneklerini yasadışı bir şekilde, veri çalarak veya yıkıcı bir şekilde **kar elde etmek için** sistemlere girmeye çalışırken kullanır.

Bilgisayar korsanları, bilgisayar sistemlerini daha iyi anlamak veya işlevlerini, performanslarını ve güvenliklerini geliştirmek için sürekli olarak bilgisayar sistemleri hakkında yeni bilgiler edinmeye çalışıyorlar. Bazıları aynı zamanda gösterici ve etik eylemlerde bulunur, ancak asla kar amacı gütmez; Bu nedenle bilgisayar korsanları genellikle takma adların arkasına saklanır. Hacker eylemleri neredeyse her zaman izinsiz olarak gerçekleştirilir, bu nedenle Yasa onları cezalandırır (ülkeler arasında büyük farklılıklar göstererek). Bazen, bilgisayar korsanlarını kovuşturmak yerine

bilge güvenlik veya BT şirketleri, genellikle yüksek becerilerinden ve yaratıcılıklarından yararlanmak için onları işe alır (muhtemelen J ustice'e olan borçlarının bir kısmını ödeyerek). Daha sonra, saldırıları engellemek ve gelecekte sistem hatalarından kaynaklanabilecek sorunları önlemek için hem üretimde hem de halihazırda piyasada bulunan uygulamaları, güvenlik sistemlerini ve programları test etmek için kullanılırlar.

Gerçek hackers uzman olarak bir üne sahiptir ve toplumlarında oldukça saygı duyulur. Bu nedenle yarışmalar, bir sistemi veya programı en kısa sürede "delmek" amacıyla düzenlenmektedir. Bu yarışmalara *hackathon* denir ve genellikle bilgisayar endüstrisinin devleri tarafından desteklenir.

"Kraker" terimi Richard Stallman'a (özgür yazılım hareketinin tanınmış bir figürü, GNU projesinin yaratıcısı ve 1970'lerden beri hacker topluluğunun üyesi) atfedilir. "Hacker" teriminin kötüye kullanılmasından kaçınmak, kimin zarar vermeye istekli olmadan hareket ettiğini ve aksine, kar elde etmek veya sadece zarar vermek için hareket ettiğini ayırt etmek istedi. Bir kraker, bilgisayar sistemlerine yetkisiz ve yasadışı bir şekilde, kötü niyetle saldırmaya çalışan, henüz bilinmeyen ve çözülmemiş güvenlik açıklarından yararlanarak onlardan hileli bir şekilde yararlanmaya çalışan bir siber suçludur. Krakerler genellikle endüstriyel casusluk, veri hırsızlığı ve ağların ve web sitelerinin engellenmesi, vandalizm vb. İle uğraşır.

Hacker ve cracker terimleri, onları bölen ince sınırlara sahiptir. Örneğin, bir izinsiz giriş, bazıları için değil, bazı insanlar için yasadışı bir eylem olarak kabul edilebilir ve Yasa bu görüşleri yansıtır; ancak belgesi etik veya yasama yönleriyle ilgili değildir. Bunun yerine, bugün, ne yazık ki, iki terimin eş anlamlı olarak kabul edildiğini düşünmeliyiz.
Bu belgede, bilge okuyucunun bir bilgisayar korsanı (hacker) ile bir kraker arasında ayrım yapabileceğinden emin olarak, her iki kategori için de daha yaygın ve yanlış kullanılan hacker terimini kullanacağız**.**

"Bilgisayar korsanları" kabaca birkaç kategoriye ayrılabilir, en yaygın kullanılanlar şunlardır.

Siyah şapkalı bilgisayar korsanları, bilgilerini kötü niyetli veya cezai amaçlar için kullanırlar ve izlenmemeye dikkat ederler.

Beyaz şapkalı bilgisayar korsanları , olası güvenlik açıklarını belirlemek ve istenmeyen erişimi önlemek için bunları ortadan kaldırmak için sistemleri test eder. Genellikle bu amaç için ödenen güvenlik uzmanlarıdır.

Gri şapkalı bilgisayar korsanları beyaz şapkalılara benzer, ancak genellikle yetkisiz olarak sistem güvenlik açıkları hakkında araştırma yaparlar ve bu güvenlik açıkları keşfedildikten sonra, satıcıları sorunu çözmeye zorlamak için genellikle ücretsiz olarak kullanırlar. Bazı satıcılar onları parayla ödüllendirir, bazıları ise onları kovuşturur (cezalandırmak için gerekli işlemlere başvurmak).

İntihar korsanları genellikle siyah / beyaz şapkalardan daha az yetkindir, ancak ideolojik nedenlerle hareket ederler ve kimliklerini gizlemekle ilgilenmezler.

Devlet destekli bilgisayar korsanlarına, başka bir Ülkeye karşı siber saldırılar başlatmaları için bir Hükümet tarafından ödeme yapılır; Devlet tarafından sağlanan büyük kaynaklara erişimlerinin yanı sıra işlenen suçlar için kovuşturmaya karşı koruma sağlarlar. Gizli bilgileri, planları veya projeleri çıkarmak veya genelleşmiş bozukluklar yaratmak ve nüfusa, Orduya, Devlet yönetimine, hastanelere, enerji, su ve güç kaynağı üretimi için tesislere vb. zarar vermek için hareket ederler. Bu eylemler gerçek savaş eylemleri olarak kabul edilir.

Senaryo çocukları henüz büyük becerilere sahip değiller veya henüz kazanmamışlar, genellikle diğer bilgisayar korsanları tarafından oluşturulan komut dosyalarını ve araçlarını kullanıyorlar. Büyük beceriler kazanmadan önceki tüm bilgisayar korsanları senaryo çocuklarıdır.

Siber teröristler, genellikle bir Ülkede kaos yaratmayı amaçlayan düşmanca niyetlere sahip bireyler veya gruplardır; devlet destekli bilgisayar korsanlarına benzerler, ancak (henüz) onları destekleyecek bir Hükümete sahip değildirler veya destek açık değildir.

Kötü amaçlı yazılım

Kötü amaçlı yazılım, bir sisteme zararlı herhangi bir kötü amaçlı programı tanımlayan genel bir terim olan "mal icious soft**ware**" in kısaltmasıdır. Kötü amaçlı yazılım, bilgisayar korsanlarının hedeflerine ulaşmak için oluşturdukları yazılımdır: para kazanmak, veri çalmak, faaliyetleri kesintiye uğratmak vb.

En yaygın kötü amaçlı yazılımlardan biri, yararlı bir yazılım gibi görünen ve genellikle böyle davranan, ancak uygulama başlatıldığında normal olarak etkinleştirilen ile birlikte yürütülecek gizli bir işlev taşıyan bir program olan **Truva atı**[1] (veya sadece **Truva atı**) olarak adlandırılır. Bunlar genellikle Truva atını taşımak için değiştirilmiş olarak dağıtılan shareware programları veya kırık programlardır. Diğer durumlarda, yararlı bir yazılım gibi görünmesini sağlayan yanıltıcı bir ada sahip kötü amaçlı yazılımdır. Truva atları genellikle e-postalarla veya Web üzerinden program indirerek yayılır ve genellikle kendi başlarına diğer bilgisayarlara yayılmazlar. Kötü amaçlı kod örnekleri, *keylogger'lar* (şifreleri çalan ve bunları bilgisayar korsanına gönderen programlar), *arka kapılar* (terminal sunucusu olarak çalışan ve uzak bilgisayar korsanının normal kimlik doğrulama prosedürlerini atlayarak bir şekilde bilgisayara erişmesine izin veren programlar), kripto madencileri (kripto para birimi madenciliği yapan programlar), *botlar* (robotların kısaltması, örneğin dağıtılmış bir hizmet reddi saldırısı için kullanılır).

[1] Terim, Truva şehrini gizlice işgal etmek için kullanılan Truva atının Eski Yunan hikayesinden türetilmiştir.

Rootkit'ler, bir kötü amaçlı yazılımın varlığını algılamadan gizlemeye çalışan kötü amaçlı yazılımlar tarafından yüklenen yazılımlardır; işletim sistemlerini değiştirerek bunu başarırlar.

Diğer yazılımlara bulaşan kötü amaçlı yazılım bir virüs veya solucan olabilir. Bunlar adlarını, herhangi bir belirli davranış türünden ziyade yayılma şekillerinden alırlar. Bilgisayar **Virüsü** , Truva atına benzer bir yazılımdır, ancak işletim sistemi dosyaları da dahil olmak üzere diğer yazılımlara virüs bulaştırarak (kendini tanıtarak) kendi kopyalarını üretebilir. Virüs, virüslü yazılımlar kopyalandığında ve bu sistemlerde çalıştırıldığında diğer sistemlere yayılır.

Bir virüsün bir **Solucan** olmasına benzer şekilde, bu bir bilgisayarda çalışan ve ağ üzerinden diğer bilgisayarlara bulaşan, ancak dosyalara virüs bulaştırmadan tek başına bir yazılımdır.

Fidye Yazılımı, virüslediği cihaza erişimi kısıtlayan ve kısıtlamayı kaldırmak için fidye ödenmesini gerektiren bir kötü amaçlı yazılım türüdür. Başlıca fidye yazılımı türleri şunlardır: 1) Korkutucu bir yasadışı davranış suçlamasıyla ekranları engelleyen ve kurbanlardan bir ücret ödemelerini isteyen *ekran kilitleme* fidye yazılımı; 2) Kötü amaçlı yazılımın bir tür dosya (resim, belge) veya virüslü bir makinedeki tüm dosyaların bulunduğu *şifreleme tabanlı fidye yazılımı*. Tam şifreleme tamamlandığında, bir açılır pencere genellikle kullanıcıya (tüm) dosyaların şifrelendiğini ve genellikle kripto para biriminde bunları kurtarmak için bir ücret ödenmesi gerektiğini bildirir. Şifreleme tabanlı fidye yazılımlarına örnek olarak CryptoLocker ve WannaCry verilebilir. Silecek olarak bilinen bir varyant bir fidye yazılımına benziyor, ancak genellikle bir ödeme gerekli olsa bile verileri yok ediyor.

Greyware farklı bir kötü amaçlı yazılım kategorisidir: bu programlar bilgisayarların performansını kötüleştirebilir ve güvenlik risklerine neden olabilir, can sıkıcı veya istenmeyen bir şekilde davranabilir, ancak genellikle önceki kötü amaçlı yazılım kategorilerinden daha az tehlikelidir (bu göreceli bir görüştür). Casus yazılımlar (ör. keylogger'lar, klavyede basılan tüm tuşları kaydeden programlar), reklam yazılımları (ekrandaki veya tarayıcıdaki reklam pencereleri, sahte çeviriciler vb.), Potansiyel Olarak İstenmeyen Programlar (PUP'lar, kullanıcının başka bir program yüklemesi sırasında bir anlaşma penceresindeki bir hata nedeniyle yüklediği uygulamalar) tipik gri yazılım biçimidir. Tarayıcılar gibi diğer programlar için bağımsız programlar veya eklentiler olabilirler. Bazen, örneğin kullanıcıyı belirli bir reklam web sitesine getirmek veya tarayıcı her başlatıldığında veya ara sıra bir reklam sayfası göstermek için diğer programların ayarlarını değiştirmek için kendilerini sınırlarlar. Anahtarın bir kısmının bilinmesi durumunda, Düz Metin'deki ilgili kısmı kurtarmak mümkündür, ancak Anahtarın geri kalanı olmadan *Düz* Metin'in diğer bitleri hakkında bilgi eksikliği yoktur. Bu nedenle, daha önce bahsedilen kriptanaliz etkili değildir. Bu durumda, özgün iletinin kalan kısmını bulmak için, Anahtarın kalan kısmı gereklidir. Anahtar tarafından iletilen tüm bilgiler, metnin tüm bilgilerini kurtarmak için gereklidir.

Antivirüsler

Antivirüs motorları kötü amaçlı yazılımları algılama güçlerini artırdıkça, algılama ve analizden kaçınmaya çalışmak için çeşitli tekniklerin bir kombinasyonu kullanılır. Daha yeni kötü amaçlı yazılımlar, aşağıdakiler gibi sofist buzlu karşı önlemleri benimseyebilir:

- belirli gizleme yöntemlerini benimsemek için çevrenin parmak izini alarak analiz etmek ve tespit etmek;
- diğerleri kötü amaçlı yazılım imzasına dayalı antivirüs algılamasını karıştırmak için kendilerini gizlemeye çalışırlar;
- Bazı kötü amaçlı yazılımlar, anormal davranışların algılanmasını kandırmak için zamanlamaya dayalı bir kaçınma benimser, kötü amaçlı yazılım normalde sessizdir ve çok özel dönemlerde (örneğin önyükleme işlemi sırasında) veya kullanıcı tarafından gerçekleştirilen belirli eylemleri izleyerek kendini etkinleştirir.

Kaçınma için keşfedilmesi çok zor bir teknik, *Dosyasız kötü amaçlı yazılım* veya *Gelişmiş Uçucu Tehditlerdir*. Bu tür kötü amaçlı yazılımlar bellekte çalışır ve çalışması için bir dosya gerektirmez. Etkinliğini gerçekleştirmek için mevcut sistem araçlarını kullanır. Dosya sisteminde herhangi bir dosyanın bulunmaması, kısmen sistemin kaynak kullanımını ve davranışını kontrol eden izleme araçları dışında, onları algılamayı ve analiz etmeyi oldukça zorlaştırır. Bu tür saldırıların artışı çok yüksektir.

Risk

Güvenlik açığından etkilenen yazılımlar, sorun düzeltilene kadar ayrıcalıklar kazanmak veya savunmaları atlamak için kullanılabilir; Yazılımın, özellikle de İşletim Sistemi'nin güncel olmasının ana nedeni budur. Güvenlik Duvarları ve İzinsiz Giriş Algılama Sistemleri LAN üzerindeki trafik düzenlerini izler.

En az ayrıcalık kuralı, kullanıcıların ve programların ihtiyaç duyduklarından daha fazla ayrıcalığa sahip olmaması gerektiğini, aksi takdirde kötü amaçlı yazılımların bundan yararlanabileceğini söyler.

Azaltma

Virüsten koruma yazılımı bazı kötü amaçlı yazılım türlerini engeller ve muhtemelen kaldırır, kötü amaçlı yazılım yazılımının bir bilgisayara yüklenmesine karşı gerçek zamanlı koruma sağlayabilir ve potansiyel tehditleri arayan dosyaların ve yapılandırmaların (örneğin Windows kayıt defteri) tam olarak taranmasını sağlayabilir.

Kişisel güvenlik duvarları herhangi bir ağ bağlantısını analiz eder ve olağandışı etkinlikleri tespit edebilir.

Korumalı alan, sistemin geri kalanından yalıtılmış bir uygulama çalıştırır, bazı uygulamalar belirli bir uygulamayı çalıştırabilirken, daha karmaşık sistemlerde bir sanal makine daha uygun olabilir.

Web sitesi güvenlik açığı taramaları, bazı virüsten koruma yazılımları tarafından iyi bilinen tehlikeli sitelerin bir listesine karşı gerçekleştirilir ve bunlarla bağlantıyı engeller.

Ağ Ayrımı, bir ağı parçalara böler ve yalnızca aralarındaki meşru olduğu bilinen trafiği etkinleştirir, bu da kötü amaçlı yazılımların ağa yayılmasını önler. Modern Yazılım Tanımlı Ağ Oluşturma teknikleri, bu ayrımcılığı gerçekleştirebilir.

"Hava boşluğu" izolasyonu veya "paralel ağ", bir ağın bir bölümünü tamamen izole ederek ve dış dünyadan yazılım ve verilerin giriş ve çıkışı üzerinde gelişmiş kontroller sağlayarak Ağ Ayrımını sınıra getirir. Bu çözüm bile kesin değildir, çünkü yazılım ve veriler yalıtılmış sisteme girmelidir, örneğin yamalama için. İzole edilmiş bir ağı ihlal etmenin iyi bilinen bir örneği, yakınlarda "rasgele" unutulan, tesis personeli tarafından alınan ve içeriği görmek için tesis bilgisayarlarına yerleştirilen USB sürücüler aracılığıyla hedef ortama tanıtılan ünlü Stuxnet kötü amaçlı yazılımıdır. Stuxnet'in üç modülü vardır: saldırıyı kontrol eden bir solucan; bir Windows bilgisayara eklendiğinde solucanı otomatik olarak yürüten bir bağlantı dosyası; ve algılanmasını önlemek için tüm kötü amaçlı dosyaları ve işlemleri gizlemekten sorumlu bir rootkit bileşeni. Hava boşluklarını geçmenin diğer yolları elektromanyetik, termal ve akustik emisyonları analiz eder.

En Yaygın Saldırı Türleri

Bu bölümde, bir bilgisayar sistemine yönelik en yaygın saldırılardan bazıları açıklanmaktadır. Saldırıların çeşitliliği son derece büyük olduğundan, her birinin birçok çeşidi olduğundan ve her gün birçok saldırı ve varyant yaratılıp keşfedildiğinden (ve çözüldüğünden) tam değildir ve tamamlanamaz. Bu, bu bölümün amacının tam bir sınıflandırma sağlamak değil, hem saldırıları gerçekleştirmek hem de karşı koymak için gereken yüksek bilgi seviyesi hakkında bir fikir vermek olduğu anlamına gelir.

Kimlik avı

Kimlik avı saldırıları çok yaygındır ve gerçekleştirilmesi kolaydır. Bunlar, kurbanı belirli bir işlem türü yapması için kandırmak amacıyla bir meslektaş veya banka gibi güvenilir bir gönderenden geliyormuş gibi görünen e-postalar göndermekten oluşur.

Saldırgan, kurbanı bir eki açmaya ikna etmeye çalışır veya orijinal sayfaya çok benzer bir sayfaya, örneğin bir banka ana sayfasına, ancak saldırgan tarafından oluşturulan bir sayfaya yönlendiren bir bağlantı sağlar, ardından kurbandan kimlik bilgilerini girmesini ister. Bu tür bir saldırıyı optimize etmek için, sözde sosyal mühendisliğin bir parçası olan bir dizi teknik vardır, çünkü bu durumda,

bilgisayar sisteminin güvenlik açığı, aldatılan ve istemeden kimlik bilgilerini sağlayan kullanıcının kendisinde tanımlanmalıdır.

Bu saldırılara karşı savunmak için, bağlantının dikkatli bir şekilde incelenmesi gerekir (küçük harf L 'l' ile bir '1' rakamı arasında ayrım yapmak veya bir URL'de .it ve .lt arasındaki farkı fark etmek neredeyse imkansızdır). Dahası, ciddi şirketlerin e-postalarına asla bir giriş sayfasına gelen bağlantılar koymadıklarının farkında olunmalıdır.

Şifre Saldırıları

Bir kurbandan şifre almak için bir bilgisayar korsanı, önceki paragrafta görüldüğü gibi sosyal mühendisliği deneyebilir veya bir şifre saldırısı başlatabilir. Parolalar genellikle karma olarak depolanır ve karmaların tersine çevrilmesi çok zordur. Temel olarak iki durum vardır: şifreli parola kullanılabilir veya bilinmemektedir ve bu tür bir saldırı farklı şekillerde gerçekleştirilebilir:

- **Kaba kuvvet saldırısı:** Bu durumda program, bir setten karakterlerin olası tüm kombinasyonlarını deneyecektir;
- **Sözlükle saldırı:** Program yaygın olarak kullanılan şifrelerin bir dizisini (sözlük) test edecektir;
- **Gökkuşağı dosyalarıyla saldırı:** Gökkuşağı tablosu, parola için kullanılan karma işlevlerinin çıktısını listeleyen önceden hesaplanmış bir tablodur. Bu, milyonlarca olası şifrenin hash fonksiyonunu hesaplamak oldukça zaman kaybı olduğu için aramayı hızlandırır. Tuz kullanan önemli bir türevin kullanılması bu saldırıyı olanaksız kılar.

System yöneticileri, sistemlerinin kullanıcılarının şifre dosyalarını, hem kaba kuvvet hem de sözlük ile şifre saldırıları gerçekleştirebilen programları ile düzenli olarak test etmelidir.

Bu saldırılara karşı korunmak için, bir sistem kullanıcının parola ayarlamasına izin vermeden önce parola kalitesini test etmeli ve farklı kümelerden (büyük ve küçük harfler, rakamlar, noktalama işaretleri) en az sayıda karakter (ör. 10) kullanılmasını zorunlu kılmalıdır. Şifrelenmiş parola bilinmiyorsa, birkaç geçersiz denemeden sonra bir hesap kilitleme veya gecikme ilkesi benimsenmeli ve böylece saldırganın birçok birleşimi denemesi engellenmelidir.

Arabellek Taşması

Arabellek taşması (veya taşması), bir arabelleğe tutabileceğinden daha fazla veri gönderdiğinizde, arabellek bunları tutmak ve diğer verileri değiştirmek için tasarlanan arabellekten taşan veriler veya İşletim Sistemine ve dosya türüne bağlı olarak yürütülebilir makine kodu enjekte ettiğinizde oluşur. Modern İşletim Sistemleri, karışık veri ve kod içeren yürütülebilir bir dosyanın çalıştırılmasını engelleyebilirken, bu, çoğu durumda hiçbir İşletim Sisteminin bulunmadığı gömülü sistemlerde sıklıkla bulunan daha basit İşletim Sistemleri için geçerli değildir.

SQL Ekleme

Çok yaygın bir saldırı SQL Enjeksiyonu'dur. SQL dili ilişkisel veritabanlarında kullanılır; Bu nedenle, bu tür saldırılar bilgi hırsızlığına yöneliktir. Temel olarak, SQL sorgusunun yorumlanan doğası nedeniyle, kötü amaçlı SQL kodu, kullanıcıya sunulacak verileri toplamak için bir SQL sorgusu kullanmayı bilen bir web sayfasına gönderilir. Kötü amaçlı SQL kodu, özgün sorgunun yazıldığından başka verileri açığa çıkaran değiştirilmiş bir sorgu olan önceden tanımlanmış SQL sorgusunu değiştirir (bazen yalnızca başka sözdizimsel parçalar ekler).

Bu tür saldırıları önlemek karmaşık olmasa da (örneğin, özgün sorguyu gerçekleştirmek için gerekenler dışında veritabanının diğer tablolarına erişimi engellemek), SQL ekleme hala en yaygın saldırılardan biridir.

Siteler Arası Komut Dosyası Çalıştırma (XSS)

Siteler arası komut dosyası çalıştırmada (XSS) kötü amaçlı yürütülebilir komut dosyaları, güvenilir bir web uygulamasının (eklenti) veya web sitesi sayfasının koduna eklenir ve sonuç olarak diğer kişiler (izleyiciler) tarafından indirilir. Sunucu güvenliği ihlal edilmiş web sayfasını geri gönderdiğinde, kullanıcının web tarayıcısı güvenilir bir kaynaktan teslim edildiğini düşünür ve ardından eklenen kodun kötü amaçlı olduğu tanımlanmaz. Etkin içerik genellikle, bir saldırganın hassas sayfa içeriğine, oturum tanımlama bilgilerine veya tarayıcının kullanıcı adına tuttuğu diğer bilgilere erişmesine izin verebilen bir komut dosyasıdır (tarayıcı tarafından yürütülen programlama kodu). XSS saldırılarıyla, virüslü sitelere erişen tüm kullanıcıların hassas verilerini çalmak mümkündür. Örneğin, bir web sitesi oturumunun SESSIONID'sini çalmak (aynı web sitesine yapılan her bağlantının birincisinin ötesinde kimlik doğrulaması gerektirmesini önlemek için kullanılan kullanıcı tarayıcı çerezlerinde bulunur), bir sahtekârın oturum açma aşamasını atlamasına ve yasadışı olarak kullanıcı adına çalışmasına izin verebilir.

Siteler Arası İstek Sahteciliği (CSRF)

CSRF, bir web sitesinde kimliği doğrulanmış bir kullanıcı tarafından gerçekleştirilen istemsiz bir http isteğidir (saldırgan tarafından istenen); Bu noktada web sitesi, saldırganın saldırısını gerçekleştirmesine izin vererek daha fazla doğrulama yapmadan isteği yerine getirecektir. Bu saldırı türü, örneğin bir e-ticaret sitesiyse, kullanıcı verilerinin değiştirilmesine veya istenmeyen satın alma işlemleri gibi istenmeyen işlemlerin gerçekleştirilmesine olanak tanır. Saldırganın CSRF saldırısı gerçekleştirebilmesi için söz konusu site hakkında çok iyi bilgiye sahip olması gerekir.

CSRF saldırısına bir örnek, bir URL değiştirilerek gerçekleştirilir. Örneğin, web sayfasının kaynak kodu, "Şifreyi değiştir" bağlantısını bulmak ve http GET yönteminin kullanıldığını doğrulamak için kötü amaçlı yazılım tarafından analiz edilir, ardından yeni bir şifreye sahip yeni bir bağlantı (saldırgan tarafından seçilen) oluşturulabilir ve kurbana, örneğin bir e-posta eki aracılığıyla gönderilebilir.

Bağlantı tıklanırsa ve kurbanın web sitesinde zaten kimliği doğrulanırsa, şifre değiştirme prosedürünün gizli bir başlangıcı etkinleştirilir ve hesabı bilgisayar korsanına etkili bir şekilde verir. İyi parola değiştirme yöntemleri eski parolayı da eklemenizi ister (ve GET yöntemi kullanılmaz). Ayrıca, bir CAPTCHA yönteminin kullanılması (kullanıcının insan mı yoksa bilgisayar mı olduğunu doğrulamak için yapılan bir test) oldukça etkilidir.

Dosyayla İlgili Saldırılar

Dosyalara yönelik birçok saldırı türü vardır. En bilinen güvenlik açıkları şunlardır:

- **Güvenli Olmayan Doğrudan Nesne Başvuruları:** Bir uygulama, adını anan bir sunucudan kaynak istediğinde, ancak kullanıcının başka bir kaynak istemek için ikincisini değiştirmesine izin verdiğinde oluşur.
- **Yerel Dosya Ekleme (LFI):** koda kötü amaçlı dosyalar eklemek için PHP dilinin GET ve POST işlevlerinin güvenlik açığından yararlanır.
- **Yol Geçişi:** Kötü niyetli bir kullanıcının sınırlı erişime sahip dizinlere erişmesine ve komutları yürütmesine izin verir. Çoğu zaman, sisteme derinlemesine girmek ve gerekli ayrıcalıkları elde etmek için bir LFI'yi takip ederek kullanılırlar.

Bu tür saldırılara karşı korunmak için, sunuculara dosya yüklenmesini önlemek, uzaktan kod yürütmeyi devre dışı bırakmak, dosya sistemine PHP erişimini kısıtlamak ve yazılımı periyodik olarak güncellemek önemlidir.

Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS)

Belki de en çok bilinen ağ saldırıları olan DoS saldırıları temel olarak diğer paketleri alma olasılığını engellemek için birçok paket göndermekten, böylece normal kullanıcılar için makineye erişimi engellemekten ve sunulan hizmetleri engellemekten ibarettir.

Bir DoS ve DDoS saldırısı arasındaki fark, ilk durumda saldırıyı gerçekleştirmek için tek bir ana bilgisayarın kullanılması, ikincisinde ise saldırının aynı anda birçok ana bilgisayarla (zombi olarak adlandırılır) gerçekleştirilmesi gerçeğinde yatmaktadır. Bu ana bilgisayarlara daha önce bir kötü amaçlı yazılım bulaşmış ve saldırganın komutuyla kurbanın makinesiyle bağlantıyı başlatmıştır.

DoS saldırıları arasında şunları hatırlayabiliriz:

- **Syn-Flood**: Çok sayıda bağlantı isteği göndermekten oluşur. İstemciden bir istek (SYN paketi) alan makine, istemciye bir ileti göndererek, bu bağlantı için bazı kaynaklar ayırarak ve kabul paketini (hiçbir zaman gelmeyecek) bekleyerek yanıt verir. Bu nedenle, bağlantı isteği bir zaman aşımı oluşana kadar etkin kalır. Tüm olası bağlantılar başlatılmışsa, makine tarafından sağlanan hizmet artık kullanılamaz. Zaman aşımı saniyeler içinde gerçekleşir, ancak büyük istek oranı makineyi tıkanmış halde tutar.
- Şirin: Bu saldırı, IP kimlik sahtekarlığı ve ICMP isteklerinin birleşimidir. IP sahtekarlığı, gönderenin IP'sinin sahte olduğu bir IP paketinin gönderilmesini ifade eder. Gönderen IP

adresini kurbanın IP adresiyle değiştirdikten sonra IP adreslerini yayınlamak için sürekli olarak *ICMP yankı istekleri* (ping komutu tarafından gönderilen ve bir makineye erişilip erişilemediğini doğrulamak için kullanılan mesaj) göndererek, kurban makine ağda etkin olan herhangi bir ana bilgisayardan gelen her istek için bir yanıt alacak ve böylece bağlantıyı engelleyecektir (sel). Bu saldırıların oluşmasını önlemek için, yönlendiricilerde yayın IP adreslerinin iletilmesini devre dışı bırakmak mümkündür.

- **Ölüm pingi**: Toplam IP boyutu kurban makineye izin verilen maksimum değerden daha büyük olan parçalanmış bir paket göndermekten oluşur, makine paketi yeniden birleştirdikten sonra arabellek taşmalarına neden olabilir.

DDoS saldırılarının, saldırganın emriyle kurban bir sunucuda birlikte bir Syn-Flood saldırısı gerçekleştiren binlerce veya milyonlarca bilgisayarın kötü amaçlı yazılım bulaştığı bir Botnet kullanması yaygındır.

Ortadaki Adam (MITM)

MITM ile, birbirleriyle doğrudan iletişim kurduklarına inanan iki taraf arasındaki iletişimi engellemeyi, analiz etmeyi ve yeniden iletmeyi amaçlayan bir saldırı tipolojisini kastediyoruz.

Bu tür saldırılar genellikle IP sahtekarlığı kullanılarak gerçekleştirilir: ağ algılayıcıları bir bağlantıyı ve gönderenin ve alıcının IP adresini değiştirerek oluşturulan yeni paketleri gizlice dinler, böylece gönderen saldırgana veri gönderir ve saldırgan da bunları alıcıya yeniden gönderir ve bunun tersi de geçerlidir.

Bu tür saldırılara karşı savunmanın birçok yolu vardır; bugün en etkili ve kullanılanı, son öznelerin şifreleme/şifre çözme işlemini gerçekleştirdiği ve tüm ara sistemlerin yalnızca şifrelenmiş verileri görebildiği uçtan uca şifrelemeyi benimsemektir.

ARP Kimlik Sahtekarlığı veya ARP Zehirlenmesi

Adres Çözümleme Protokolü (ARP), ağ iletişimlerinin yerel ağdaki belirli bir aygıta ulaşmasını sağlar. IP adreslerini Ortam Erişim Denetimi (MAC) adresleriyle eşlemek için kullanılır (LAN üzerindeki ana bilgisayarları tanımlamak için kullanılır). Bir ana bilgisayar, Internet'e bağlanmak için yönlendiricinin/ağ geçidinin MAC adresini bilmek için ARP protokolünü kullanmalıdır. Her ana bilgisayar, önceden istenen ve bilinen IP/MAC çiftini eşlemek için bir ARP önbelleği tutar. Ana bilgisayar belirli bir yerel IP adresinin MAC adresini bilmiyorsa, yerel ağdaki diğer tüm ana bilgisayarlara IP adresine kimin sahip olduğunu soran bir yayın ARP istek paketi gönderir. Bu IP adresine sahip ana bilgisayar cevap verecek ve böylece MAC adresini sağlayacaktır.

ARP kimlik sahtekarlığı/zehirleme saldırısı, yerel ağ MITM saldırısı olarak sınıflandırılabilir. Saldırganın yerel ağa erişimi olması gerekir ve yönlendiricinin ve başka bir ana bilgisayarın IP adreslerini belirlemek için yerel ağı tarar. Saldırgan, yönlendiriciyi ve ana bilgisayarı, saldırganın MAC adresinin sırasıyla ana bilgisayar ve yönlendiriciden biri olduğuna inandıran sahte ARP yanıtları

gönderir. Bu, hem yönlendiriciyi hem de iş istasyonunu birbirlerine değil, saldırganın makinesine bağlanmak için kandırır. İki aygıt ARP önbellek girdilerini güncelleştirirken, konak ve yönlendirici birbirleriyle doğrudan iletişim kurmak yerine saldırganla iletişim kurar.

DNS Kimlik Sahtekarlığı

Etki Alanı Adı Sistemi (DNS), Internet adlarını (daha doğru bir şekilde FQDN - Tam Nitelikli Ayırt Edici Adlar, örneğin www.server.net) karşılık gelen IP adresine dönüştürmek için kullanılan adlandırma sistemidir. Sistem hiyerarşiktir ve bazı top-le vel sunucuları ile merkezi değildir. Sistem bir ağ kaynağına her ulaşmaya çalıştığında, kaynağın adını IP adresine dönüştürmek için DNS sunucusuna bağlantı kurulur. Kaynak kayıtları genellikle yönetim bilgilerini ve örneğin posta sunucuları tarafından kullanılan diğer verileri içerir.

Bir bilgisayar korsanı, yasal web sitesi yerine sahte veya "sahte" bir web sitesine trafik göndermek için DNS kayıtlarını değiştirmek isteyecektir. Sahte makine daha sonra MITM saldırıları, sahtekarlık vb. Yapabilir. DNS sahtekarlığını önlemek için, DNS sunucularının güncel tutulması gerekir.

Drive-by Saldırıları

Bir drive-by saldırısında, kötü amaçlı kod güvenli olmayan bir web sitesine gömülür. Virüslü sayfa ziyaret edildiğinde, komut dosyası otomatik olarak kurbanın bilgisayarında yürütülür ve tehlikeye girer, sitede herhangi bir şey yapmanıza veya herhangi bir bilgi girmenize gerek yoktur. Bu durumda, güncellenmiş yeni ve iyi bir antivirüs ve / veya kişisel güvenlik duvarının kullanılması, bir kullanıcı veritabanından ziyaret etmeden önce bir sitenin güvensiz olup olmadığını tespit edebildikleri için tek korumadır.

Kimlik Bilgilerini Yeniden Kullanma

Birkaç hizmet için kimlik bilgilerine sahip olma ihtiyacı, kullanıcıların bazı parolalarını yeniden kullanmalarını sağlar. Bir saldırgan, güvenliği ihlal edilmiş web sitelerinin veya hizmetlerin kullanıcı adları ve parolalarının bir listesine sahip olduğunda (örneğin Karanlık Web'den elde edildiğinde), aynı kullanıcının diğer sistemlerde aynı kullanıcı/parola çiftini kullanması mümkündür. Bu, bir sözlük saldırısıyla kontrol edilecek parola sayısını büyük ölçüde azaltacaktır. Bu tür saldırıların karşıtlığını oluşturmak için, parola saldırılarına karşı koymak için benimsenen aynı karşı önlemler etkilidir. Birçok karmaşık şifreye ihtiyaç duyulduğunda, bazı insanlar şifre yöneticilerini yararlı bulur.

Web Oturumu Ele Geçirme

Oturum Ele Geçirme saldırısı, web tarayıcısı tarafından oturum denetim mekanizmaları olarak kullanılan oturum belirteçlerinin kullanılmasından oluşur. Web sunucusunun, her web sayfası için her öğe (metin, resim vb.) için bir TCP bağlantısı oluşturulduğundan, aynı kullanıcıdan farklı

bağlantıları ilişkilendirmesi gerekir. En çok kullanılan yöntem, Web Sunucusunun başarılı bir istemci kimlik doğrulamasından sonra istemci tarayıcısına gönderdiği bir belirteci temel alır. Oturum belirteci yalnızca bir tanımlayıcıdır, uzun benzersiz bir dizedir ve her bağlantı için bir kimlik doğrulama yordamı gerçekleştirme gereksinimini önlemek için kullanılabilir. Bu saldırı, Web Sunucusuna yetkisiz erişim elde etmek için geçerli bir oturum belirtecinin çalınması veya tahmin edilmesi yoluyla gerçekleştirilir.

TCP Oturumu Ele Geçirme

TCP bağlantıları, paketleri doğru sıralı sırada teslim etmeyi garanti etmelidir, bunu başarmak için onay paketleri ve sıra numaraları kullanır. 3 yönlü ilk el sıkışmasından sonra, bu onay paketleri yalnızca bir şekilde artırılmış sayılardır. TCP oturum korsanının amacı, istemcinin ve sunucunun veri alışverişinde bulunamadığı bir durum oluşturmaktır; gerçek paketleri taklit eden her iki uç için de kabul edilebilir paketler oluşturmasını sağlamak. Böylece, saldırgan oturumun kontrolünü ele geçirebilir. Dizi tahmin edilebiliyorsa, saldırgan kurban ana bilgisayarından geçerli olarak tanınan sahte paketler gönderebilir.

IP Kimlik Sahtekarlığı

IP sahtekarlığı genellikle bir DoS saldırısıyla gerçekleştirilir: çok sayıda bağlantı meşru sunucuyu engeller ve aynı zamanda sahte bir sunucu IP adresini meşru sunucunun numarasıyla ayarlar. Bu nedenle, kullanıcı, iletinin güvenilir bir ana bilgisayardan geldiğini belirten bir IP adresiyle ileti gönderen sahte sunucuya yönlendirilir.

Kör Ele Geçirme: Kaynak yönlendirmenin devre dışı bırakıldığı durumlarda, oturum korsanı, kötü amaçlı verilerini TCP oturumunda ele geçirilen iletişimlere enjekte ettiği kör ele geçirmeyi de kullanabilir. Buna kör denir çünkü cevabı göremez; Korsan verileri veya komutları gönderebilse de, temel olarak istemcinin ve sunucunun yanıtlarını tahmin ediyor.

Sıfır Gün Sömürüsü

Kesin konuşmak gerekirse, sıfır gün istismarı belirli bir saldırı değildir, çünkü siber suçlular belirli yazılım ve işletim sistemlerinde yeni keşfedilen bir güvenlik açığını öğrenir ve daha sonra bir düzeltme kullanıma sunulmadan önce bu yazılımı kullanan kuruluşları hedef alır.

Kod Sızıntısı

Uygulamaların kaynak kodu bazen hassas bilgiler içerebilir ve kodun kendisinin içsel ekonomik değerine ek olarak bir siber saldırı için değerli bilgiler sağlayabilir.

Co-funded by the
Erasmus+ Programme
of the European Union

Soru:

Ayrı bir dosyada.

Ekler (PowerPoint sunumu, dinleyici notları, baskılar, bağlantılar, video...):

Ayrı bir dosyada

Başvuru:

1. Malware, or malicious software
   URL: https://www.malwarebytes.com/malware
2. Cybersecurity for everyone.
   https://www.avast.com/c-malware
3. What are Cyber Security Threats?
   URL: https://www.imperva.com/learn/application-security/cyber-security-threats/
4. 21 Top Cybersecurity Threats and How Threat Intelligence Can Help
   URL: https://www.exabeam.com/information-security/cyber-security-threat/