

BİR HACKERİN EL KİTABI

Enes ÖZKAN,2024

ÖN SÖZ

Herkese selamlar, bu yazı birçok alanında uzman insanların tamamen Türkçe olarak bize sundukları bilgilerin benim tarafımıştır ve sadelikle toplanmış, gerekli düzenlemeler yapılmış ve "Bir Hackerin el kitabı" çatısı altında toplanmıştır. Bu yazı tamamıyla bitirildiğinde Siber Güvenlik gibi uşusuz bucaksız birçok farklı alanı kapsayan derin bir konu kümесinin temellerini atmış olacaksınız. Bu yazı tamamen ücretsiz bir şekilde <http://www.github.com/hackwithenes> adresinden erişilebilir.

Anahtar Kelimeler: Siber Güvenlik, Ağ, Kriptografi, Ağ Güvenliği, Veri Güvenliği, Ağ Güvenlik Duvarı (firewall), Güvenlik Açıkları, Siber Saldırı Türleri, Siber Tehdit.

1. GİRİŞ

Bu Makalede okuyacağınız bilgiler sayesinde siber güvenlik alanında temellerinizi sapasağlam atacaksınız veya var olan temelinizi daha da güçlendireceksiniz. Bu makale ağ, siber güvenlik, kriptografi vb. alanlarda temel bilgileri içerir. Günümüzün dijital çağında, siber güvenlik giderek daha önemli bir konu haline gelmektedir. İnternetin yaygın kullanımıyla birlikte, bireyler, kuruluşlar ve hükümetler, bilgi ve verilerinin çeşitli tehditlere karşı korunması konusunda daha da hassas hale gelmiştir. Siber güvenlik, bilgisayar sistemlerini, ağları, cihazları ve verileri korumak için gerekli olan önlemleri ve uygulamaları içeren disiplinlerarası bir alandır.

Bu makalede, "Bir hackerin el kitabı" olarak adlandırdığımız bir kılavuz sunacağız. Bu kılavuzda, siber güvenliğin temellerini bilmediğiniz yönleriyle anlatacağız. Ayrıca, güvenlik önlemleri ve en iyi uygulamalar hakkında genel bir bakış sunarak, siber güvenlik alanında bilgi sahibi olmayanlar için bir başlangıç noktası oluşturmayı amaçlıyoruz.

İçeriğimiz, siber güvenlik alanında daha derinlemesine bir anlayış geliştirmek isteyen bireyler için bir temel oluşturacaktır. Bilgi teknolojisi alanındaki hızlı değişimler ve artan dijital tehditler göz önüne alındığında, herkesin siber güvenlik konusunda bilinçli olması ve uygun önlemleri alması son derece önemlidir.

Şimdi, siber güvenliğin temellerine doğru bir yolculuğa çıkalım ve dijital dünyayı daha güvenli bir yer haline getirmek için atılacak adımları keşfedelim.

Basit Terimler

Zafiyet nedir: Bir sistemi siber saldırırlara açık hale getiren hatalara zafiyet denir.

Tehdit nedir: Bilgisayar sistemlerine yönelik potansiyel tehlikeleri ifade eden bir terimdir.

Risk nedir: Herhangi bir olay ve buna bağlı olarak itibar, data, finansal kayıp yaşama ihtimaline risk denir.

Ping: iki cihaz arasındaki bağlantıyı test eden teşhis aracıdır.

Genellikle ağın sahip olduğu hataları kontrol etmek için kullanılır.

***Ping ICMP Protokolünü kullanır ve bu protokol Port numarası ile çalışmaz yani Ping port numarası kullanmaz.

AES: 128 bit veri blokların 128, 192, 256 Bit anahtar seçenekleri ile şifreleyen bir algoritmadır.

128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 anahtarlar için sırasıyla 12 ve 14 döngüde Şifreleme Yapmaktadır.

DES: Şifrelmek ve Şifrelenmiş veriyi açmak için Geliştirilmiş bir standarttır . DES yapısı itibariyle Blok şifreleme örneğidir yani şifrelenecek metni Parçalara böler ve her parçayı birbirinden bağımsız olarak şifreler. Bu blokların uzunluğu 64 bitdir.

RC-4: Şifrelenenek veriyi akan bir bit dizisi olarak kullanır. Genelde hız gerektiren uygulamalarda yaygın olarak kullanılır. Güvenliği rastgele bir anahtar kullanımına bağlıdır.

MD5: Veri bütünlüğünü test etmek için kullanılır. Girdi farketmeksiz 128 bit çıktı üretir. En küçük değişiklik tüm bitlerin kaymasına sebep olur. Genelde dosyanın eksiksiz transfer edilip edilmediğini test etmek için kullanılır.

SHA-1 : Çalışma prensibi olarak MD5 ile benzerdir. Uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. 160 bitlik mesaj özeti üreten SHA-1 çakışmalara karşı 80 bitlik güvenlik sağlar.

Klasik Şifreleme Teknikleri

Steganography: Şifrelenmemiş Düz bir metni çeşitli dönüşümler kullanarak bir metin haline getirilmesi işlemidir. Verilebilecek en basit örnek, Bir metnin tüm harflerinin başka bir metnin içindeki kelimelerin ilk harflerine gizlenmesidir.

İlkel bir şifreleme metodudur ve kırılması kolaydır.

Örneğin;

“Sezen Aksu Ve Aşk Şarkılar Benim İçin Tüm Tesellilerden İyidir.

“SAVAŞ BİTTİ”

Caesar Cipher: Bilinen en eski tekniklerden birisidir. Julius Caesar tarafından geliştirilmiştir. Mantık Her harfi kendisinden sonra gelen üçüncü harfle çembersel olarak değiştirmeye dayanır.

“Brute Force” gibi saldırı teknikleri ile bile rahatlıkla çözülebilir.

Dili çok rahatlıkla anlaşılabilir.

Örneğin;

“Bilgisayarların şifreleri kırıldı”

Şifrelenmiş metin: “DLOİUÖCBÇTOÇTKÖ ÜLHTĞOĞTLNKTOKGK”

ROT13: Yer değiştirme tekniğini kullanan bir Ceasar Şifreleme türüdür. Mantığı İngiliz alfabetesindeki bir harfin 13 harf sonraki harf ile eşleşmesidir.

Parolalar Veritabanında nasıl saklanmalı?

Aklımıza gelen ilk yöntem Belirlenmiş Şifreleme tekniklerini kullanmak olabilir fakat bu hackerlar içinde düşünmesi çok kolay bir teknik olacaktır. Veritabanını AES ile şifrelediğimizi varsayılmı. Veritabanımızın Calındığında AES ile birlikte Şifrenin kendisininde çalınması basit bir hash işlemi ile şifreleri gün yüzüne çıkartacaktır.

Bir başka yöntem Peki parolamızda Hash olarak tutsak nasıl olur?

Bu mantıklı görünse de Rainbow Attack adı verilen önceden hesaplanmış veri tabanları ile yapılmış ataklara karşı korumasızdır.

Bir başka yöntem ise Parolayı bir kere değil X kere Hash işlemine maruz bırakmak olacaktır. Fakat gelişen teknoloji ile X kere Hash işlemi uygulanmış Rainbow Table lar da bulunmaktadır ve onlarda kırılabilir.

Bir başka yöntem ile Salting yöntemidir. Rainbow Attacklara karşı önlem olarak kullanılmaktadır.

Bu Yöntemde her bir parola için özel rastsal bir salt ürettilir ve veri tabanında saklanır.

Parola ve tuz birleştirilerek Hash’i alıp veri tabanında saklanır. Bu işlemi Kırmanın yolu ise Modern GPU ler ile yapılan Brute Force ataklarıdır.

2017 itibarıyle güvenli sayılan ilk yöntem Password Based Key Derivation Functions (PBKDF2) dir. Bu Yöntemle Tuz ve parola Hashlenir ve bu sonuç bir sonraki iterasyonda tuz olarak kullanılır ve bu işlem X kere tekrarlanır. Modern frameworklerde X 1000 olarak belirlenmiştir.

Güvenli sayılan bir diğer yöntem BCRYPT parola hash uygulamasıdır. Genel amaçlı hash uygulamalarına göre milyarlarca kez yavaş çalıştığı için Brute force ataklara ve Kullandığı salt ile Rainbow attack lara karşı dayanıklı kabul edilmektedir.

Owasp nedir?

OWASP açılımı Open Web Application Security Project olarak tanımlanmaktadır. Web uygulamalarındaki güvenlik açıklarının kapatılması ve bu uygulamaların güvenli bir şekilde korunmasını sağlamak için çalışmalar yapan özgür bir topluluktur. OWASP'ye ait dokümanlar ve araçlar tüm dünyadaki herkesin kullanımına açık ve ücretsizdir. OWASP' in hiçbir özel şirket ve kuruluşla herhangi bir bağı yoktur.

Çalışmalarını tamamen insanların ihtiyaçlarını gidermek üzere yürütmektedir. OWASP' in web sitesinde, web uygulamalarındaki zafiyetleri, bu zafiyetlerin nasıl olduğunu, hangi açıklıklardan kaynaklandığını, bu zafiyetlerin nasıl exploit edilebileceğini ve bu zafiyetlerin nasıl önlenebileceği ile ilgili ayrıntılı dokümanlar da mevcuttur.

Web dünyasındaki en yaygın 10 Güvenlik Açığı

1- SQL Injection

SQL Enjeksiyonu, bir saldırganın kullanıcı tarafından sağlanan verileri manipüle ederek arka uç SQL ifadelerini değiştirmesine olanak tanıyan bir güvenlik açığıdır. Enjeksiyon, kullanıcı girdisi komut veya sorgunun bir parçası olarak bir yorumlayıcıya gönderildiğinde ve yorumlayıcıyı istenmeyen komutları yürütmesi için kandırıldığından ve yetkisiz verilere erişim sağladığında meydana gelir.

Gerekli önlem alınmadıysa ve kullanıcı adı biliniyorsa şu komut SQL injectionu tetikleyebilir.

Kullanıcı Adı: Admin
Şifre 1=1' or pass123

Bu durumda muhtemel SQL şu şekilde olacaktır.

```
SELECT * FROM Users WHERE User_Name = admin AND Password = 1=1' or pass123;
```

Ve bu ifade TRUE Değeri döndüreceği için sisteme admin olarak girmiş olacağız.

Öneriler:

Giriş sayfalarınız için beyaz liste olarak tabir edilen sadece belirli veri tipi ve özelliklerini içeren bir liste oluşturun.

Saldırgan için yararlı olabilecek ayrıntılı hata mesajlarından kaçının.

Örneğin Kullanıcı adı doğru parolası yanlış ise Parolanız yanlış demek yerine Girdığınız Bilgileri kontrol ediniz. Gibi bir ibare kullanınız.

2- Cross site Scripting (XSS)

XSS güvenlik açıkları, istemci tarafında, yani sunucu tarafında değil, kullanıcı tarayıcısında yürütülen bir sayfaya gömülü komut dosyalarını çalıştırmayı hedefler.

Bu açıklar, güvenilmeyen verilerin alınıp uygun doğrulama olmadan web tarayıcısına gönderildiğinde ortaya çıkabilir. Tarayıcı komut dosyasının güvenilir olup olmadığını bileyemeceği için komut dosyası çalıştırılır ve saldırgan oturum tanımlama bilgilerini ele

geçirebilir, web sitelerini bozabilir veya kullanıcıyı istenmeyen ve kötü niyetli web sitelerine yönlendirebilir.

XSS, saldırganın komut dosyalarını kurbanın tarayıcısında çalıştırmasına izin veren bir saldırırıdır.

Örnekler:

```
http://www.yoursite.com/anasayfa? "< script > alert (" you are hacked! ")
```

Yukarıdaki komut dosyası bir tarayıcıda çalıştırıldığında, site XSS'ye açıksa bir mesaj kutusu görüntülenir. Daha ciddi saldırırlarda, oturum tanımlama bilgileri görüntülenebilir veya depolanabilir.

```
http://www.yoursite.com/search.php?txtSearch< iframe>< /iframe> < src 500="" google.com="" height="" width="500" >
```

Yukarıdaki komut dosyası çalıştırıldığında, tarayıcı http://google.com'u gösteren bir "iframe" yükleyecektir.

Öneriler:

Giriş sayfalarınız için beyaz liste olarak tabir edilen sadece belirli veri tipi ve özelliklerini içeren bir liste oluşturun.

Giriş Çıkış verilerinin temizlenerek gönderilmesini (Sanitize) sağlayın.

3-Broken Authentication and Session Management

Web siteleri genellikle her geçerli oturum için oturum cerezi ve oturum kimliği oluşturur. Bu cerezler kullanıcı adı, parola vb. gibi hassas verileri içerebilir. Oturum, oturum veya tarayıcı kapatılarak sona erdirildiğinde, önceki cerezler geçersiz kılınmalıdır, yani her oturum için yeni bir cerez oluşturulmalıdır.

Oturum kapatıldığında cerezler geçersiz kılınmazsa, hassas veriler halen sistemde kalacaktır. Örneğin, halka açık bir internet kafede bilgisayar kullanan bir kullanıcı, - güvenlik açığı bulunan sitenin cerezleri sistemde halen bulunacağı için-, bir saldırgan tarafından istismar edilebilir. Saldırgan bir süre sonra aynı ortak bilgisayarı kullandığında hassas veriler tehlikede olabilir.

Aynı şekilde ortak bilgisayar kullanan bir kullanıcı, oturumu kapatmak yerine tarayıcıyı kapatıp çıktıığında, saldırgan, savunmasız siteye göz atıp, kurbanın önceki oturumunun açık olduğunu görebilir. Saldırgan, kullanıcının profil bilgilerini, kredi kartı bilgilerini vb. çalabilir.

Muhtemel Saldırı Alanları:

- URL'de gösterilen oturum kimlikleri, oturum sabitleme (Session Fixation) saldırısına neden olabilir.
- Oturum açmadan önce ve sonra aynı olan Oturum kimlikleri.
- Oturum Zaman Aşımları doğru şekilde uygulanmayan uygulamalar.

- Her yeni oturum için aynı oturum kimliğini atamayan uygulamalar.
- Oturum, düşük yetkili bir kullanıcı tarafından yeniden kullanılabilir.

Etkileri;

Bu güvenlik açığından yararlanan bir saldırgan, bir oturumu ele geçirebilir ve sisteme yetkisiz erişim sağlayabilir.

Oturum yetkisi, çalınan cerezler kullanılarak veya XSS ile yüksek seviyeye çıkarılabilir.

Örnekler:

Havayolu rezervasyonu uygulamasında oturum kimliği URL'de görülmektedir:

<http://bookingair.com/sale/saleitems;jsessionid=MEOC2oJM0DPXS2P0PL3/dest=Antalya>

Sitenin gerçek bir kullanıcısı, arkadaşlarına satış hakkında bilgi vermek istiyor ve bir e-posta gönderiyor. Bu e-posta kötü niyetli kişilerin eline geçtiğinde, oturum kimliği çalınabilir.

Saldırganın, XSS'e karşı savunmasız bir uygulamadan oturum kimlik bilgilerini XSS ile ele geçirip kullanması.

Uygulama zaman aşırıları doğru ayarlanmamış uygulamalarda, kullanıcı genel bir bilgisayar kullanır ve oturumu kapatmak yerine tarayıcıyı kapatıp, uzaklaşır. Saldırgan bir süre sonra aynı tarayıcıyı kullanır ve açık oturumdan istediği değişiklikleri yapabilir veya bilgileri çalabilir.

Öneriler:

- Tüm kimlik doğrulama ve oturum yönetimi gereksinimleri, OWASP Uygulama Güvenliği Doğrulama Standardına göre tanımlanmalıdır.
- Kimlik bilgilerini asla URL'lerde veya Log'larda göstermeyin.
- Oturum kimliklerini çalmak için kullanılabilecek XSS açıkları için de çok dikkatli olmak gereklidir.

4- Insecure Direct Object References (IDOR)

Geliştirici, bir dosya, dizin veya veritabanı anahtarı gibi dahili nesnelere ulaşım için bir referansı URL'de açığa çıkardığında zafiyet de ortaya çıkar. Saldırgan bu bilgileri diğer nesnelere erişmek için kullanabilir ve yetkisiz verilere erişmek için bir saldırısı oluşturabilir. Bu zafiyet gerçek kullanıcılar tarafından da istismar edilebilir, bu sebepten oturum açma yetkisi olan kullanıcılar da bu açığa dikkat etmek gereklidir.

MUHTEMEL AÇIK

Veritabanıyla etkileşime giren URL'ler.

Örnekler:

Aşağıdaki URL'deki "kullanıcı id – user_id" değiştirilerek diğer kullanıcıların bilgilerini görüntülemek mümkün olabilir.

http://www.website.com/user_id=789563

Öneriler:

- Erişim kontrollerini sıkı bir şekilde uygulayın.
- URL'lerde nesne referanslarını göstermekten kaçının.

Tüm referans nesneler için yetkilendirmeye göre doğrulama talep edin. User_id ile birlikte her kullanıcı için oluşturduğunuz bir user_token kullanabilirsiniz, bu sayede saldırgan user_id'yi değiştirse bile user_token tahmin edemeyeceği için bilgileri görüntüleyemeyecektir, aşağıdaki URL'yi inceleyin:

https://www.website.com/user_id=789563&user_token=14lxHK5f8Z6x6QunGaqduiPDoxcgMJtD

5-Siteler Arası İstek Sahteciliği (Cross Site Request Forgery) CSRF

Siteler Arası İstek Sahteciliği, siteler arası gerçekleştirilen bir sahte taleptir (http request). CSRF saldırısı, kötü amaçlı bir web sitesi, e-posta veya program vasıtasiyla kullanıcının tarayıcısının o anda kimliğini doğruladığı güvenilen bir sitede istenmeyen bir eylem gerçekleştirmesine neden olduğunda meydana gelir.

Bir CSRF saldırısında, oturum açmış bir kurbanın tarayıcısını, kişinin kimlik doğrulama bilgileri dahil olmak üzere tüm bilgilerini, savunmasız bir web uygulamasına sahte bir HTTP isteği göndermeye zorlar.

Örneğin, kullanıcının orijinal web sitesinde (Banka uygulaması olabilir) oturum açtığını ve aynı zamanda da maillerini kontrol ettiğini düşünelim. Maillerinden birinde nereden gönderildiği tam olarak bilinmeyen veya kendisi ile ilgili olduğunu düşündüğü zararlı bir linke tıkladığında, saldırgan tarafından hazırlanmış düzenek sayesinde yan sekmede açık olan orijinal web sitesinin kullanıcı bilgilerini çalabilir.

Muhtemel Saldırı Alanları:

- Kullanıcı Profili sayfaları
- Kullanıcı hesap formları
- Ticari işlem sayfaları

Örnekler:

Kurbanın, geçerli kimlik bilgilerini kullanarak bir bankanın web sitesinde oturum açtığını düşünelim. Aynı zamanda da maillerini kontrol ettiğini ve “Banka hesaplarınızda bir problem var, detaylar için lütfen tıklayın” yazan sanki kendi bankasından gönderilmiş gibi bir mail aldığıını düşünelim.

Bu linke tıkladığında, bankanın başka bir hesaba para transferi yapan formunu iyice analiz etmiş ve buna göre bir talep oluşturmuş olan saldırganın linki çalışır; oturum doğrulandığından ve talep bankanın kendi web sitesinden geldiğinden dolayı, banka şüphelenmeden talebi işleme koyar ve saldırganın hesabına para aktarılır.

Öneriler:

- Hassas eylemler gerçekleştirirken kullanıcının varlığını ispatlamasını zorunlu kılmak.

- CAPTCHA, Yeniden Kimlik Doğrulama ve Benzersiz İstek Belirteçleri (User Token) gibi mekanizmalar kullanın.

6-Yanlış Güvenlik Yapılandırması (Security Misconfiguration)

Güvenlik Yapılandırması, uygulamalar, uygulama sunucusu, web sunucusu, veritabanı sunucusu ve platform için tanımlanmalı ve dağıtılmalıdır. Bunlar doğru şekilde yapılandırılmadığında, saldırganın hassas verilere veya işlevlere yetkisiz erişime sahip olması mümkün olabilir.

Bu güvenlik açığından yararlanan saldırgan, kullanılan teknolojiyi ve uygulama sunucusunun bilgilerini (sürüm bilgileri, veritabanı bilgileri vb.) görüntüleyebilir ve saldırı gerçekleştirmek için uygulama hakkında bilgi edinebilir.

Muhtemel Saldırı Alanları:

- URL
- Form Alanları
- Giriş alanları

Örnekler:

- Uygulama sunucusu yönetici konsolu otomatik olarak yüklenebilir. Varsayılan hesaplar değiştirilmez. Saldırgan, varsayılan parolalarla oturum açabilir ve yetkisiz erişim elde edebilir.
- Sunucunuzda Dizin Listeleme devre dışı bırakılmamışsa saldırgan herhangi bir dosyayı bulmak için dizinleri listeleyebilir.

Öneriler:

- Bileşenleri birbirinden ayıran ve güvenlik sağlayan güçlü uygulama mimarisi oluşturun.
- Varsayılan kullanıcı adlarını ve şifreleri değiştirin.
- Dizin listelerini devre dışı bırakın ve erişim kontrol denetimlerini uygulayın.

7-Insecure Cryptographic Storage (Güvensiz Criptografik Depolama)

Güvensiz Criptografik depolama, hassas verilerin güvenli bir şekilde depolanmadığı zaman ortaya çıkan yaygın bir güvenlik açığıdır.

Kullanıcı kimlik bilgileri, profil bilgileri, sağlık bilgileri, kredi kartı bilgileri vb. hassas verilerdir.

Bu veriler, uygulama veritabanında saklanabilir. Bu veriler, şifreleme veya karma oluşturma (Hash) kullanılmayarak uygunuz bir şekilde depolandığında, saldırganlara karşı savunmasız olacaktır.

Etkileri:

Bir saldırgan bu güvenlik açığını kullanarak, kimlik hırsızlığı, kredi kartı dolandırıcılığı veya diğer suçları gerçekleştirmek için bu tür zayıf korunan verileri çalabilir, değiştirebilir.

Muhtemel Saldırı Alanları:

- Uygulama veritabanı.

Örnekler:

Bir uygulama kullanıcıların şifrelerini salt (Salt, orijinal verilere eklenen rastgele bir veridir. Hashing işleminden önce şifreye eklenir ve şifrenin tahmin edilmesini zorlaştırır) ve hash olmadan saklar. Saldırgan, SQL enjeksiyonu (SQL Injection) saldırısı ile parola dosyasına erişim sağlar. Salt ve Hash uygulanmamış şifreler kaba kuvvet ile (Brute Force) ile kolayca tespit edilebilirken, salt ve hash yapılmış şifrelerini çözümlemesi yıllar sürebilir.

Öneriler:

- Hassas bilgilerde şifreleme yaparken uygun güçlü standart algoritmalar kullanın.
- Kendi şifreleme algoritmalarınızı kullanmayın. Yalnızca AES, RSA genel anahtar şifreleme ve SHA-256 gibi onaylanmış genel algoritmaları kullanın.
- Site dışı yedeklemelerin şifreli olduğundan, ancak anahtarların ayrı olarak yönetildiğinden ve yedeklendiğinden emin olun.

8-Failure to restrict URL Access

Web uygulamaları, korumalı bağlantıları ve butonları işleme almadan önce URL erişim haklarını kontrol eder. Uygulamaların, bu sayfalara her erişildiğinde benzer erişim kontrollerini gerçekleştirmesi gereklidir.

Uygulamaların çoğunda ayrıcalıklı sayfalar, konumlar ve kaynaklar kullanıcılar sunulmaz. Fakat incelemeler sonrası iyi bir tahminle, bir saldırıgın ayrıcalıklı sayfalarla erişebilir, işlevleri çalıştırabilir ve gizli bilgileri görüntüleyebilir.

Etkileri:

- Bu güvenlik açığı ile saldırıgın uygulamaya giriş yapmadan yetkisiz URL'lere erişim sağlayabilir, özel sayfalarla erişebilir, işlevleri çalıştırabilir ve gizli bilgileri görüntüleyebilir.

Muhtemel Saldırı Alanları:

- URL'ler

Örnekler:

- Saldırgan, URL'nin kullanıcı rolünü "/kullanici/detaylar" olarak gösterdiğini fark eder. "/admin/detaylar" olarak değiştirerek yetkisiz olduğu admin sayfalarına erişim sağlayabilir.

Öneriler:

- Güçlü erişim kontrolleri uygulayın.
- Kimlik doğrulama ve yetkilendirme politikaları rol tabanlı olmalıdır.
- İstenmeyen URL'lere erişimi kısıtlayın.

9-Insufficient Transport Layer Protection (Yetersiz Taşıma Katmanı Koruması)
Kullanıcı (istemci) ve sunucu arasındaki bilgi alışverişi ile ilgili bir zafiyettir. Uygulamalar genellikle bir ağ üzerinden kimlik doğrulama ayrıntıları, kredi kartı bilgileri, oturum bilgileri gibi hassas bilgileri iletir.

Uygulama üzerinde zayıf algoritmalar kullanmak veya süresi dolmuş veya geçersiz sertifikalar kullanmak veya SSL kullanmamak, iletişim güvenilmeyen kullanıcılarla açık olmasına izin verebilir, bu da web uygulamasının güvenliğini tehlikeye atabilir.

Etkileri:

- Bu web güvenlik açığından yararlanan bir saldırgan, gerçek kullanıcının kimlik bilgilerini ele geçirip uygulamaya erişim sağlayabilir.
- Kredi kartı bilgileri çalınabilir.

Muhtemel Saldırı Alanları:

- Ağ üzerinden gönderilen veriler.

Öneriler:

- Güvenli HTTP'yi etkinleştirin ve yalnızca HTTPS üzerinden kimlik bilgisi aktarımını zorunlu kılmın.
- Sertifikanızın geçerli olduğundan ve süresinin dolmadığından emin olun.

Örnekler:

SSL kullanılmayan bir uygulamada, saldırgan sadece ağ trafiğini izleyerek kimliği doğrulanmış bir kurbanın oturum şerezini elde edebilir. Bu şerez çalınarak “Ortadaki Adam – Man In The Middle” saldırısı gerçekleştirilebilir.

10- Unvalidated Redirects and Forwards(Doğrulanmamış Yönlendirmeler)

Web uygulamalarında, kullanıcıları başka sayfalara yönlendirmek için birkaç yöntem kullanılır. Başka sayfalara yönlendirilirken uygun bir doğrulama yoksa, saldırganlar bunu kullanarak kurbanlarını kimlik avı veya kötü amaçlı yazılım sitelerine yönlendirebilir veya yetkisiz sayfalara erişmek için yönlendirmeleri kullanabilir.

Etkileri:

Saldırgan, kullanıcıya kodlanmış kötü amaçlı URL eklenmiş gerçek bir URL gönderebilir. Kullanıcı, saldırganın gönderdiği URL'nin yalnızca ilk kısmına bakar ve kurban olabilir.
Örnekler:

<http://www.website.com/login.php?redirectURL=digersite.com>

Bu şekle çevrilebilir:

<http://www.website.com/login.php?redirectURL=tehlikelisite.com>

Öneriler:

- Uygulamalarınızda yönlendirmeleri kullanmaktan kaçının. Kullanılacaksa bile varış yerinin hesaplanmasında kullanıcı parametrelerinin kullanılmasına dikkat edin.
- Hedef parametreler olmak zorundaysa, sağlanan değerin geçerli ve kullanıcı için yetkilendirilmiş olduğundan emin olun.

SSL sertifikası nedir?

Secure Sockets Layer (SSL), internet üzerinden hassas bilgi göndermek ve almak için modern bir şifreleme yöntemi güvenlik protokolüdür. Bir kullanıcının tarayıcısı ile kullanıcının istediği web sitesinin sunucusu arasında güvenli bir kanal oluşturarak çalışır. Bu kanaldan geçen herhangi bilgi, bir ucta şifrelenir ve diğer uçtan alındığında şifre çözülür. Böylece, birisi bu bilgileri eline geçirse bile, bilginin şifreli olmasından ötürü hiçbir fayda sağlayamayacaktır.

TLS Sertifikası nedir?

TLS ise Transport Layer Security (TLS) ve ziyaretçilere hassas bilgilerini sunucuya güvenli şekilde iletebilmelerine olanak sağlar. Bütün veri transferlerini, hackerlar ve dolandırıcılar gibi üçüncü partiler tarafından çözülemeyecek bir şekilde şifrelerler. SSL güvenlik için önemli bir sertifikadır.

HTTP Nedir?

Http anlamı en basit haliyle, sizlerin internet siteleri ile bağlantı kurmanızı sağlayan anahtar olarak tanımlanabilir. İnternet kullanırken web sitesine bağlanmak için adres çubuguuna site ismi girildiğinde başına http yazmasanız bile sistem otomatik olarak site isminin önüne getirecektir. Çünkü protokoller gereği erişilmek istenilen alana http tarafından yöneltlen komut sayesinde bağlantı gerçekleştirilir.

HTTP, ağ ortamında veri sunmak için kullanılmakta olan TCP/IP tabanlı iletişim protokolüdür ve bağlantı noktası olarak TCP 80 portu sıkılıkla kullanılır.

HTTPS ise HTTP nin SSL/TLS Sertifikası ile korunan halidir.

IPS (Intrusion Prevention System) Nedir?

Bir siber saldırı önleme sistemi olan IPS (Intrusion Prevention System), tehlikeli, şüpheli ve risk oluşturabilecek aktiviteleri izleyerek engellenmesini sağlar. IPS, sürekli olarak ağ üzerindeki trafiği takip eder ve kontrol eder. Normal dışı bir durum belirlediğinde ise veri akışını kısıtlar ve ağ yöneticisine uyarı iletir.

IPS (Intrusion Prevention System) Nasıl Çalışır?

IPS sistemi genel olarak güvenlik duvarının arkasında yer alır. Kötü amaçlı aktivitenin tespit edildiği durumlarda bağlantryı sıfırlamak, yöneticileri uyarmak ve kaynak adresinden gelen trafiği engellemek gibi birçok otomatik eylemi gerçekleştirir.

Ayrıca tehditleri belirlemek için kullanılan birkaç farklı yöntem bulunmaktadır:

İmza Tabanlı: Tespit edilen tehditlerin anti-virus programları tarafından imza olarak ifade edilmesinden bu terminoloji ortaya çıkmıştır. Bu yaklaşım daha önce bilinen ağ tehditlerinin tekrar bir probleme yol açmasını engellemek için kullanılır.

Anomali Tabanlı: İmza tabanlı izlemeye göre daha güvenilir olan anomali tabanlı yöntemde, ağ üzerindeki aktiviteleri temel standartlarla karşılaştırır. Yapay zeka ve makine öğrenimi bu yöntemi desteklemek için kullanılır.

İlke Tabanlı: İmza tabanlı veya anormal tabanlı yönteme göre daha az yaygındır. Kuruluş tarafından tanımlanan güvenlik ilkelerini tehdit eden veya şüpheli durum oluşturan faaliyetler engellenir. Bunun için daha önce güvenlik ilkelerini belirlenip, yapılandırmak gereklidir.

IPS (Intrusion Prevention System) Türleri Nelerdir?

NBA (Network Behavior Analysis): DDoS saldırıları gibi ağıda gerçekleştirilen olağan dışı trafik davranışını tespit etmek için kullanılır.

HIPS (Host Based Intrusion Prevention): Tüm ağı kontrol etmez sadece kurulduğu bilgisayardaki trafiği kontrol eder.

NIPS (Network-Based Intrusion Prevention): Proaktif tarama yapılması için ağ trafiğindeki tehditleri izlemeye yardımcı olur.

WIPS (Wireless Intrusion Prevention Systems): Wi-Fi ağı üzerindeki tehditleri izlemek ve yetkisiz erişimleri önlemek için kullanılır.

IDS (Intrusion Detection System) Nedir?

Bir ağı sürekli olarak izleyerek ve tarayarak güvenlik açıkları, potansiyel saldırular, şüpheli aktiviteler gibi durumlara karşı kullanılan yazılım ya da donanım güvenlik sistemidir. IDS sistemi temel olarak meydana gelen saldıruları tespit etmenin yanı sıra karantinaya almak, raporlamak, kaydetmek gibi farklı işlevleri de bulunmaktadır. Ayrıca IPS sistemi ile entegre bir şekilde kullanılabilir.

IDS Türleri Nelerdir?

Network Intrusion Detection System (NIDS): Ağdaki tüm cihazlardan gelen trafiği incelemek için ağ içinde planlı bir noktada kurulur. Bir saldırının tespiti edildiğinde veya anormal bir etkinlik gözlemlendiğinde uyarı gönderilebilir.

Host Intrusion Detection System (HIDS): Ağ üzerinde bulunan bağımsız ana bilgisayarlar ya da aygıtlar üzerinde çalışır. Gelen ve giden trafiği izleyerek şüpheli bir etkinlik algılandığında yöneticiyi uyarır.

Protocol-based Intrusion Detection System (PIDS): Kullanıcı ya da cihaz ile sunucu arasındaki protokolü kontrol eder.

Özetle, her iki sistem de güvenlik duvarı arkasında çalışabilir. Ayrıca hem donanım hem de yazılımsal olarak faaliyet gösterebilir. IDS kullanılarak potansiyel saldırular tespit etmek hedeflenir ve alınacak aksiyon raporları IPS otomatik olarak aksiyona geçebilir. IPS kullanılarak saldıruları durdurmak ve önlemek amaçlanır.

C: Gizlilik (Confidentiality)

I: Bütünlük (Integrity)

A: Erişilebilirlik (Availability)

Kriptografi : Şifreleme algoritmaları kullanarak şifreleme oluşturma bilimidir.

Kriptanaliz : Şifre ya da anahtar kullanmadan deşifre etme yöntem ve prensipleri.

Kriptoloji : Hem kriptografiyi hem de kriptanalizi kapsar.

Kriptografide kullanılan bazı temel kavramlar;

- Plaintext : Orijinal, düz metin.
- Ciphertext : Şifrelenmiş metin.
- Cipher : Düz metni, şifrelenmiş metne çeviren algoritma. Şifreleme algoritması.
- Encipher (encrypt): Düz metni şifrelenmiş metne çevirme.
- Decipher (decrypt): Şifreli metinden düz metni kurtarma.

Simetrik Anahtarlı Algoritmalar

Simetrik şifreleme, bilgileri şifrelemek ve deşifre etmek için yalnızca bir gizli anahtar içeren en basit şifreleme türüdür. Simetrik şifreleme, kriptografi teknikleri ve şifreleme algoritmaları içinde en eski ve en iyi bilinen tekniktir. Bir sayı, bir kelime veya rastgele harfler dizisi olabilen gizli bir anahtar kullanılır. Gönderen ve alıcı, tüm mesajları şifrelemek ve şifresini çözmek için kullanılan gizli anahtarı bilmelidir. İşlem süresinin hızlı olması simetrik şifreleme algoritmalarının en önemli avantajlarındandır. Blowfish, AES, RC4, DES, RC5 simetrik şifrelemeye örnektir.

Blowfish

Piyasada kullanılan en hızlı blok şifreleyicilerdir. Karmaşık anahtar çizelgesi kullanarak kırılmasını zorlaştırır. Blowfish, 23'den 448 bite kadar anahtar uzunluklarına sahiptir. Çalışabilmesi için 4 kilobyte RAM'den daha fazla belleğe ihtiyaç duyurlar. Bu nedenle en küçük gömülü sistemlerde kullanılamazlar.

DES (Data Encryption Standart)

Dünyada en çok kullanılan simetrik şifreleme algoritmalarından birisidir. Feistel şifreleme metodunu kullanır. Blok şifreleme kullanan DES, işlem sırasında 64 bitlik veriyi 56 bitlik anahtar kullanarak şifreler. Anahtar uzunluğunun kısa olması nedeniyle kırılmıştır. Bunun üzerine Triple-DES, (encrypt-decrypt-encrypt)yani 3DES olarak geliştirilmiştir. 3DES, DES'in üst üste 3 kere kullanılmasıdır. Yani normal DES'e göre 3 kat yavaştır ama

günümüzde SSH gibi uygulamalarda kullanılır. AES'in çıkışması üzerine DES popülerliğini kaybetmiştir. Çünkü AES'e göre 6 kat daha yavaştır.

AES (Advanced Encryption Standard)

DES kırıldıktan sonra yeni bir arayışa girilmiş ve AES simetrik şifreleme algoritması oluşturulmuştur. DES'in zayıf yönleri kuvvetlendirilmiş halidir ve blok şifreleme algoritmasını kullanır. DES'e göre daha hızlı ve güvenlidir. Uzunluk olarak 128, 192 ve 256 bit anahtarları destekler. DES'e göre anahtar boyu ve block size daha uzundur. Bu da daha güçlü bir anahtar sağlar. Günümüzde de en popüler algoritmaların birisidir ve brute force saldırılara karşı dayanıklı olduğu düşünülmektedir.

RC4 (Rivest Encryption 4)

Şifrelenecek veriyi akan bir bit dizisi olarak algılar. RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır. Genellikle hız gerektiren uygulamalarda kullanılır. Şifreleme hızı yüksektir ve MB/sn seviyesindedir. Güvenliği rastgele bir anahtar kullanımına bağlıdır. Anahtar uzunluğu değişkendir. 128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme olarak kabul edilir. Bankacılık ve Dökümantasyon(PDF) şifrelemelerinde yaygın olarak kullanılır.

RC5 (Rivest Encryption 5)

Modern şifreleme algoritmaları sınıfında yer almaktadır. 16–32 ve 64 bitli kelime uzunlukları ile çalışabilmektedir. Anahtar boyutu ve döngü sayısı değişken olarak alınabilir. Böylece, yüksek anahtar boyutu ve fazla döngü sayısı ile uzun çalışma zamanı fakat kırılması neredeyse imkansız şifreler; düşük anahtar boyutu ve az döngü sayısı ile kısa çalışma zamanı ve bununla beraber daha güclü şifreler arasında seçim yapılabilmeye olanacağını sağlar. Bellek gereksiniminin de düşüklüğü ile cep telefonlarından süper bilgisayarlara kadar her yerde çalışabilir bir algoritmadır.

TWOFISH

AES kadar hızlıdır. DES gibi Feistel yapısını kullanır. DES'den farklı anahtar kullanılarak oluşturulan değişken S-boxlara(Blok şifrelerde genellikle anahtar ve şifre metni arasındaki ilişkiyi gizlemek için kullanılırlar.) sahip olmasıdır. Metinleri 32 bitlik parçalara ayırarak işleme sokar ve blok algoritması olarak çalışır. Şifreleme ve deşifreleme algoritmalarının birbirinden farklı olması uygulama maliyetini arttırmış, aynı zamanda yazılım uygulamalarını yavaşlatmıştır.

IRON

Feistel yapısını kullanır. 64 bitlik veri bloklarını 128 bit anahtarla şifreler ve 16 ile 32 döngü sayısında çalışır. Alt anahtarların sayısı döngü sayısına eşittir. Bu nedenden dolayı algoritma anahtar bağımlıdır. Bu algoritmanın avantajı, bitler yerine 16-tabanındaki sayılarla kullanılması, dezavantajı ise yazılım için tasarlanmış olmasıdır.

IDEA

Açılımı “International Data Encryption Algorithm” olan IDEA bir blok şifreleme algoritmasıdır. Aynı zamanda Ascom tech adlı firmanın tescilli algoritmasıdır. PGP'nin temelini oluşturan algoritmaların birisidir. Bilinen en güçlü algoritmalarndandır. IDEA, şifrelenecek olan 64 bitlik metin ve 128 bitlik anahtarları kullanarak 64 bitlik şifrelenmiş metni oluşturur.

CAST-128

PGP ve PGP'nin bazı versiyonlarında varsayılan şifre olarak birçok ürününde kullanılan simetrik bir anahtar blogu şifresidir. Kanada Hükümeti'nin kullanımı tarafından kullanılmaktadır. 64 bit blok boyutu ve anahtar boyutu 40 ile 128 bit arasında olan (ancak yalnızca 8 bitlik artışlarla) 12 veya 16 yuvarlak Feistel bir ağdır. Anahtar boyutu 80 bit'ten uzun olduğunda 16 turun tamamı kullanılır .

Asimetrik Anahtarlı Algoritmalar

Şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğer açık (gizli olmayan) anahtاردır. Bu anahtarlardan bir tanesiyle şifreleme yapılrken diğeryle de şifre çözme işlemi gerçekleştirir. Bu iki anahtar çifti matematiksel olarak birbirleriyle bağlantılıdır. Gizli anahtarın sadece bir sahibi vardır. Gizli anahtara sahip olan taraf gizli anahtar aracılığıyla, kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir. Açık anahtar herkesin erişimine açıktır. Bu algoritma açık anahtarla şifreleme ve gizli anahtarla deşifreleme yapılmasını kolayca gerçekleştirirken, yalnızca açık anahtarı bilerek gizli anahtarın bulunmasını zor kılar. Bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir. Açık anahtar altyapısı internet üzerinde güvenli haberleşmeyi sağlayan TLS (SSL'in gelişmiş hali) protokolü, güvenli e-posta haberleşmesinde kullanılan PGP protokolü ve dosya şifreleme ve çözmeye yarayan GPG gibi protokollerde kullanılmaktadır.

(D-H) Diffie-Hellman anahtar değişimi

Diffie ve Hellman tarafından bulumus ilk asimetrik şifreleme algoritmasıdır. DH iki katılımcının öncesinde herhangi bir bilgi alışverişi yapmadan güvenli olmayan bir kanal vasıtasyyla (güvenli bir şekilde) ortak bir şifrede karar kılmlarına yaranan bir protokoldür. Algoritma anahtar değişimi ile asıl amacı, iki kullanıcının bir anahtarı güvenli bir şekilde birbirlerine iletmemeleri ve daha sonrasında da bu anahtar yardımı ile şifreli mesajları birbirlerine gönderebilmelerini sağlamaktır. Diffie–Hellman algoritması oluşturularak simetrik şifreleme algoritmaları için büyük problemi olan gizli anahtarları koruma ve dağıtım büyük ölçüde aşılmıştır. Bununla birlikte Diffie-hellman algoritması sadece ortak gizli anahtarı belirlemekte kullanılmaktadır.

RSA (Rivest-Shamir-Adleman)

Üç bilim adamının baş harflerinden oluşan RSA, dijital imzalama içinde kullanılmaktadır. Güvenilirliği, çok büyük asal sayıların işlem yapma zorluğuna dayanan bir algoritmadır. Günümüzde bankacılık sistemleri ve ticari sistemlerde öncelikli tercih edilen şifreleme tekniğidir. Bu büyük sayılar nedeniyle oldukça güvenilirdir ama işlemler yavaştır. Bu nedenle fazla bant genişliği harcaması yüzünden kablosuz ağ sistemlerinde kullanılması bazı sorunlara yol açabilir.

El Gamal

Diffie-Hellman anahtar alışverişine dayanan bir açık anahtarlı şifreleme yöntemidir. Anahtar üretimi ve şifreleme/açma olarak iki aşamadan oluşur. Matematiksel zorluk olarak dairesel gruplar üzerindeki ayriksız logaritmalara dayanan bir dijital imzadır.

DSA (Digital Signature Algorithm)

NIST tarafından sayısal imza standarı olarak tasarlanmıştır. DSA algoritması da, RSA gibi açık anahtarlı bir kriptografik algoritmadır. Dijital imza algoritması, ElGamal imza algoritmasının bir varyantıdır.

Merkle-Hellman

RSA asimetrik şifreleme sisteminden farkı şifreleme işleminin tek yönlü çalışmasıdır. Açık anahtar sadece şifreleme yaparken, gizli anahtar sadece şifre çözme işlemini gerçekleştirir. Bu nedenle de Dijital İmzalama için kullanılamaz. Düşünce olarak RSA'dan daha basit ve zekice olmasına rağmen kırılmıştır.

(ECC) Elliptic Curve Cryptography

Eliptik Eğri Kriptolojisi (Elliptic Curve Cryptography), sonlu cisimler üzerindeki eliptik eğrilerin cebirsel topolojisine dayanan bir açık anahtar şifrelemesidir. Eliptik eğri kriptografisinin en büyük özelliği depolama ve iletme gereksinimlerini azaltarak daha küçük anahtar boyutuna sahip olmasınadır. Bir eliptik eğri grubu, büyük modülerli ve buna bağlı olarak büyük anahtar boyutlu RSA tabanlı sistem ile aynı güvenlik seviyesi sunabilir. Örneğin; Eliptik eğri ile 256-bitlik anahtar boyutunda elde edeceğimiz güvenliği RSA 'de 3072-bitlik anahtar ile sağlanabilir. Bu algoritma IHA'larda güvenlik açısından kullanılabilir. Ayrıca ECC smart kartlar, cep telefonları, PDA'lar (personal digital assistant), sayısal posta işaretleri gibi zorunlu ortamlara uygundur.

Bazı güvenlik sistemleri 1024-bit RSA genel anahtarlama planının uygulamasını yaymaya çalışır, çünkü kuruluşlar bunun yeterince iyi olduğunu düşünürler. Bununla birlikte bu tehlikeli bir yaklaşımdır. Çünkü genel anahtarlama sisteminin güvenliği kullanılan simetrik şifrelemeyle birebir eşleşmiş olmalıdır. Tabloda görüldüğü gibi, 1024-bit RSA simetrik şifrelemede kullanılan 128-bit güvenlik seviyesiyle uyışmuyor. Bu gereksinimi karşılamak yani genel anahtarlama planını eşleştirmek için istenen 3072- bit RSA ya da 256-bit ECC kullanılmasıdır. Bu sayede işlemci gücü, saklama kapasitesi, bant genişliği, güç tüketimi gibi durumlarda RSA'ya göre avantaj sağlar.

FTP, SFTP ve FTPS nedir? Farkları Nelerdir?

Temelinde dosya transferi olan bu protokoller bir çok defa kafa karışıklığına neden olmaktadır. SFTP ve FTPS sundukları kimlik doğrulama seçenekleriyle FTP'den çok daha güvenilirdirler.

FTP komut kanalı ve veri kanalı olmak üzere iki ayrı kanal tarafından veri transferi yapar. Bu iki kanalda da veriler şifrelenmez ve araya girebilecek saldırganlar tarafından kolaylıkla okunabilir. Bu noktada saldırganların kullandıkları en bilinen yöntemler ortadaki adam saldırısı ve ARP zehirlenmesi saldırıdır. PCI DSS, HIPAA gibi bir çok standart tarafından FTP kullanımını kabul edilmez. Bu üç protokolden en son tercih edilmesi gerekeni FTP'dir.

SFTP ve FTPS sundukları kimlik doğrulama seçenekleriyle daha güvenli bir şekilde dosya transferi yaparlar. Bu iki protokol arasındaki temek fark portları kullanım şekillerindedir. SFTP tüm transfer işlemlerini tek port üzerinden yaparken FTPS birden çok port kullanır. FTPS'in birden çok portu kullanılması güvenlik duvarında daha çok porta izin verilmesi anamina geliyor. Bundan dolayı SFTP'nin güvenliği FTPS'e göre daha iyidir.

FTPS'de kullanıcı adı ve parolaya ek olarak sertifikanın kullanılması gereklidir. Sertifikanın bilinen sertifika yetkilileri(CA) tarafından onaylanması gerekiyor. CA'lara alternatif olarak

dosya transferi yapacak olan sunucular tarafından da bu sertifikalar tanımlanabilir. FTPS önlem olarak FTP'ye ayrı bir katman ekliyor diyebiliriz. Hem kullanıcı adı ve parola hem de sertifika yöntemleri aynı anda kullanılabilir.

SFTP ise SSH protokolü kullanır. Tek port üzerinden dosya transferi yapar ve hem kimlik doğrulama bilgilerini hem de veriyi şifreler. SFTP doğrulama için iki farklı yöntem kullanır.

FTP'de olduğu gibi kullanıcı adı ve parola ile doğrulama yapılabilir. FTP'ye ek olarak girilen kullanıcı adı ve parola bilgilerini şifrelemekte ve bu şekilde güvenli hale gelmektedir.

Diğer yöntem olarak SSH Anahtarları kullanılır. Bu yöntemde genel(public) ve özel(private) olmak üzere iki farklı anahtar oluştursunuz ve genel anahtarınızı dosya transferi yapmak istediğiniz tarafa gönderirsiniz. Sizin genel anahtarınızı hesabınızla ilişkilendirmelerinden sonra başarılı bir şekilde doğrulama işlemi yapılır. Hem kullanıcı adı ve parola hem de anahtarlar aynı anda kullanılabilir. Güvenlik duvarında tek porta ihtiyacı olmasından dolayı SFTP tercih edilebilir.

Özellikler	SFTP (SSH üzerinden FTP)	FTPS (SSL üzerinden FTP)
 Güçlü Şifreleme Algoritmalarını Uygulama	✓ AES ve Üçlü DES gibi şifreleme yöntemlerini kullanır	✓ AES ve Üçlü DES gibi şifreleme yöntemlerini kullanır
 Kullanıcı Adı ve Parolalarını Şifreleme	✓ Kullanıcı bilgilerini şifreler	✓ Kullanıcı bilgilerini şifreler
 Anahtar Tabanlı Kimlik Doğrulama	✓ Anahtarlı doğrulama vardır. Şifreye ek olarak ya da sadece Anahtarla doğrulama yapılabilir	X Anahtar tabanlı kimlik doğrulama yoktur
 Sertifika Tabanlı Kimlik Doğrulama	X Sertifika tabanlı kimlik doğrulama yoktur	✓ Sertifikalı doğrulama vardır. Kullanıcı adı, parola ve sertifika kullanılabilir
 Güvenlik Duvarı Dostu	✓ Güvenlik duvarında tek porta ihtiyaç vardır. Varsayılan olarak 22 kullanılır	X Birden çok port kullanımı vardır. Bu yüzden güvenlik duvarında sıkı bir şekilde kontrol edilmesi gereklidir

Kara Kutu (Black Box) Yaklaşımı

Bu yaklaşımda sizme testinin yapılacağı sistem ile ilgili bir bilgi önceden verilmez. Test edici bir bilgisayar korsanı gibi sisteme sizmeye çalışır. Hedef sisteme sizmek için sistemle ilgili bilgi toplanır; zafiyetler ve açıklar taranır. Harici veya son kullanıcı bakış açısından test etmeyi içerir. Test edicinin yanlışlıkla sisteme zarar verme ihtimali bulunmaktadır.

Beyaz Kutu (White Box) Yaklaşımı

Sizme testini yapacak ekibe firmada bulunan tüm sistemler hakkında bilgiler verilir. Black box yaklaşımına göre kuruma daha fayda sağlanır. Zafiyetleri bulmak kolaylaşır ve önlem alınması için geçen süre de azalmaktadır. Ekibin zarar verme riski çok azdır.

Gri Kutu (Gray Box) Yaklaşımı

Gray box testinde firma hakkında sınırlı bilgi verilerek sizme test gerçekleştirilir. Bu test ile firma içerisinde düşük ayrıcalıklara sahip kullanıcıların sistemlere ve firmaya verebileceği zararın test edilebilmesi hedeflenmektedir.

	Black Box	White Box
Tanım	Sistemin yapısı hakkında bilgi edinilmeden yapılan testtir.	Sistem hakkında bilgiler testi gerçekleştirecek ekibe verilmiştir.
Amaç	Black box testinin temel amacı, sistem işlevsellliğini test etmektir.	White box test yönteminin temel amacı, kod kalitesini kontrol etmektir.
Programlama Bilgisi	Black Box testi yapmak için programlama bilgisine gerek yoktur.	White Box testini yapmak için programlama bilgisi gereklidir.
Zaman Tüketimi	Daha az yorucu ve zaman tüketimi azdır.	Kapsamlı ve zaman alıcı bir yöntemdir.
Kod Erişimi	Kod erişimi gereklidir.	Kod erişimi zorunludur.
Yetenek Seviyesi	Ortalama becerilerin altında olmak yeterlidir. Düşük vasıflı test uzmanları, programlama dili veya işletim sistemi uygulaması hakkında hiçbir bilgi olmadan uygulamayı test edebilir.	Uzman test bilgisi gereklidir. Beyaz kutu testi yapmak için test edicinin yüksek deneyime sahip olması gereklidir.
Kod Erişimi	Kod erişimi gereklidir.	Kod erişimi zorunludur.
Test Metodu	Bu yöntem deneme yanlışına yönelik tekniklerle dayanmaktadır.	Veri alanları ve iş sınırları test edilebilir.
Düzenleme	Veri odaklı, kutu testi, veri ve fonksiyonel test olarak da bilinir.	Yapısal test, açık kutu testi, kod tabanlı test veya cam kutu testi olarak da adlandırılır.
Test Temeli	Uygulama içi davranışları bilinmemekle birlikte dış bektilerle dayalı test yapılır.	İç çalışma yapısı bilinmektedir. Test yapan kişi bunu göre test yapar.
Kullanım	Bu tür testler; Sistem Testi, Kabul testi gibi daha yüksek test seviyeleri için idealdir.	Ünite Testi, Entegrasyon testi gibi daha düşük testler için uygundur.
Uygulama Bilgisi	Uygulama bilgisi gerekmeyen.	Faaliyet ve sonuçları anlamak için uygulama bilgisi esastır.

Otomasyon	Black Box Testleri, test ediciler ve programcılar arasında iyi bir koordinasyon gerektirir. Dolayısıyla, süreci kolayca otomatikleştirmek mümkün değildir.	White box testi otomatikleştirmek kolaydır.
Başlamadan Önce	Gereksinim özellikleri belgesini (Bir sistem veya yazılım uygulamasının davranışı açıklayan belge) hazırladıktan sonra teste başlayabilirsiniz.	Ayrıntılı tasarım dokumanı (Bir sistem veya yazılım uygulamasının veri tasarımını, mimari tasarımını, arayüz tasarımını ve prosedür tasarımını tanımlar.) hazırlandıktan sonra başlanır.
Derinlik (Ayrıntı)	Derinlik azdır.	Derinlik çoktur.
Test Ediciler	Son kullanıcılar, geliştiriciler, test uzmanları tarafından gerçekleştirilebilir.	Geliştiriciler, test uzmanları tarafından uygulanabilir
Algoritma Testi	Algoritma testi için iyi bir yöntem değildir.	Algoritma testi için en uygun yöntemdir.
Avantaj	Büyük kod bölümleri için çok uygun ve verimlidir.	Gizli hataları getirebilecek ekstra kod satırlarının kaldırılmasını sağlar.
Teknikler	Equivalence Partitioning Boundary Value Analysis Error Guessing vb.	Statement Coverage Branch Coverage Path Coverage vb.
Dezavantajları	Test kapsamı sınırlıdır. Belirli modüllerin test işlemi yapılmayabilir, atlanabilir.	Yetenekli bir test uzmanı gerektirdiği için maliyet artar. Gizli hataları bulmak için her üç noktaya bakmak mümkün olmadığı için problemler yaşanabilir. Kod analizcisi ve hata ayıklayıcı gibi bazı özel araçların kullanımını gerektirir

HTTP Durum Kodları

1xx: Tarayıcı tarafından gönderilen isteğin sunucuya ulaştığını ve işlemin başladığını bildiren bilgilendirme kodlarını ifade eden durum kodlarıdır.

2xx: Tarayıcı tarafından gönderilen isteğin sunucuya ulaştığını, anlaşıldığını ve başarılı olduğunu ifade eden durum kodlarıdır.

3xx: Erişimlmek istenen kaynağın başka bir kaynağa taşındığını ve bir yönlendirmenin söz konusu olduğunu ifade eden durum kodlarıdır.

4xx: İsteğin yerine getirilemediğini, ilgili web sayfasına ya da web sitesine ulaşamadığını ifade eden durum kodlarıdır.

5xx: Tarayıcı tarafından gönderilen isteğin başarıyla sunucuya ulaştığını fakat sunucu tarafından sorunlar nedeniyle isteğin yerine getirilemediğini ifade eden durum kodlarıdır.

200 Durum Kodu (Başarılı)

En kısa tanımıyla ideal durum kodudur. Bir web sayfası sorunsuz şekilde açılıyorsa sunucudan tarayıcıya 200 durum kodu gönderilir. Sunucudan tarayıcıya 200 durum kodu iletiliyorsa ziyaretçi ve web sitesi için her şey olması gerektiği gibidir diyebiliriz.

301 Durum Kodu (Kalıcı Yönlendirme)

Bir web sayfasının kalıcı olarak bir başka web sayfasına yönlendirildiği ve sayfayı ziyaret eden kullanıcının da otomatik olarak yönlenmesini sağlayan durum kodudur. 301 durum kodu kullanılarak yönlendirilen sayfalar içerik bakımından çok benzer ya da alakalı olduğunda güç kaybı en aza indirilebilir. Bu nedenle web sitesi taşıma gibi işlemlerde kullanılması önerilen en önemli durum kodlarından biridir.

302 Durum Kodu (Geçici Yönlendirme)

Bir web sayfasının geçici olarak bir başka web sayfasına yönlendirildiğini ifade eden durum kodudur. 301 yönlendirme kodundan farkı ilgili sayfanın test aşamasında olması, bakıma alınması ya da bir e-ticaret sitesi için ilgili ürünün stoklarının geçici olarak tükenmesi gibi ilgili sayfanın tekrar aktif edileceği durumlarda kullanılmasıdır. Fakat kullanıcılar 301 yönlendirmesi ile 302 yönlendirmesi arasındaki farkı anlamayacaktır. İlgili sayfaya giriş yapan kullanıcılar direkt olarak diğer sayfaya yönlendirilecektir

403 Durum Kodu (Erişim İzni Sorunu)

Kullanıcının bir web sayfasına erişmek adına sunucuya gönderdiği istege karşılık ilgili web sayfasına erişim izni olmadığı ya da ilgili web sayfasının yasaklandığını ifade eden durum kodudur.

404 Durum Kodu (Bulunamadı)

Kullanıcının görüntülemek istediği web sayfasının ilgili sunucuda bulunmadığını ifade eden durum kodudur. İlgili web sayfası silinmiş ya da URL'si değiştirilmiş olabilir. Fakat 404 durum kodları ilgili sayfanın geçici ya da kalıcı olarak ulaşamadığı hakkında bir fikir vermez. Kullanıcılar ulaşmak istedikleri bir web sayfasında 404 durum kodu ile karşılaşıklarında genelde siteyi terk ederek farklı web sitelerine yönelirler. Özellikle çok trafik alan ya da URL'i kullanıcılar tarafından bilinen bir sayfa ise bu durum ilgili web sitesini kötü etkileyecektir. Bu nedenle 404 durum kodu içeren sayfaların alakalı karşılaşıkları varsa yönlendirilmesi önerilir.

Fakat ilgili web sayfası bir süre sonra tekrar aktif olacak ya da bir e-ticaret sitesi için ilgili ürün tekrar stoklarda yer alacaksa ilgili sayfanın 404 durum kodu içerecek şekilde kalması daha doğru olacaktır. 404 şeklinde bırakılan web sayfalarındaki kullanıcıları kaybetmeyip farklı sayfalara yönlendirerek web sitesi içerisinde tutmaya çalışmalıyız. Bu nedenle özel olarak tasarlanan custom 404 sayfaları ile kullanıcıların web sitesini terk etmek yerine farklı sayfalara yönləmələrə yardımcı olabiliriz.

Firewall Nedir, Nasıl Çalışır, Türleri Nelerdir?

Firewall, ağları ve bilgisayar sistemlerini korumak için kullanılan bir yazılım veya donanımdır.

Firewalllar ilgili sistemdeki ağ girişi üzerindeki ilk güvenlik önlemidir. Yani herhangi bir verinin internetten veya diğer ağlardan sizin ağınıza ulaşabilmesi için güvenlik duvarını geçmesi gereklidir.

Bu sistem veri paketlerinin tanımlı kurallara uygun olup olmadığını kontrol eder ve paket geçiş iznini belirler. Yetkisiz erişim, virüs veya diğer kötü amaçlı yazılımların ağa sızması engellenebilir.

Güvenlik duvarları, yazılım ve donanım olmak üzere iki türe ayrılmaktadır. Firewall yazılımları, bir bilgisayar veya sunucuya yüklenen yazılımlardır. Donanımsal firewall'lar ise özel bir CPU, bellek, işletim sistemi ve yazılımla donatılmış cihazlardır.

Güvenlik duvarı çözümü, bireysel kullanımın yanı sıra işletmeler için de veri güvenliği açısından son derece önemlidir. Bu sistem, şirket bilgisayarlarındaki önemli verileri korur ve dış kaynaklardan gelen tehditlere karşı engel oluşturur. Güvenlik duvarı kullanımı, şirketteki değerli bilgilerin çalınmasını engeller ve siber saldırı riskini en aza indirir. İyi bir firewall ile ağınızı koruyabilir, zararlı yazılımlardan ve siber saldırılardan korunabilirsiniz.

Firewall Nasıl Çalışır?

Firewall, veri aktarımı sırasında güvenlik mekanizması oluşturarak yetkisiz kaynaklardan gelen trafiği otomatik olarak engelleme özelliğini sunar.

Bu sayede sahte ve yetkisiz erişim önlenecek siber saldırganların ağıdaki cihazlara sızma ihtimali ortadan kalkar.

Güvenlik duvarları, ağ güvenliğinin karmaşık bir kısmını oluşturur, sadece önceden yapılandırılmış kriterlere uyan trafiği ağa kabul eder.

Bu sistemin çalışma mantığında öncelikli konulardan biri erişimi kontrol edebilme yeteneğidir. Bu sistem tarafından yönetilen bazı görevler şunlardır:

- Önceden tanımlanmış güvenlik özelliklerini yönetme
- Ağ geçidi (gateway) savunması
- Dahili ağ adreslerini (NAT) koruma
- Ağıdaki güvenilir etkinlikleri ayırma
- Çeşitli uyarı ve etkinlikleri özetleme

Firewall Türleri Nelerdir?

Firewall türleri üç ana kategoride incelenir: yazılım, donanım amaçlı, ve mimariye göre.

1- Yazılımsal Firewall

Bilgisayarların arka planında aktif olarak çalışan programlar olan yazılımsal firewall, özellikle bireysel internet kullanıcıları tarafından tercih edilir. Bu tür güvenlik duvari uygulamaları sadece bir sistemi veya ağı korur. Birden fazla sistem için ayrı bir firewall programı kullanmanız önerilir, eğer ağınızda birden çok sistem varsa.

2- Donanımsal Firewall

Donanım kısmında kullanılan firewall ürünleri, tüm ağı kapsayacak şekilde koruma sunar. İnterneti olan ve birden çok bilgisayarı olan işletmeler, donanımsal güvenlik duvarlarını tercih eder. Bu tür güvenlik duvarları bilgisayar üzerinde çalışmadığı için performans ve hız düşüklüğüne neden olmaz. Ayrıca, uzaktan çalışan personel için tasarlanmış VPN bağlantısına imkan sunar.

3- Mimarisine Göre Firewall

Mimarisine göre güvenlik duvarı çeşitleri, sistemin trafiği nasıl kontrol ettiğine göre farklı şekillerde gruplandırılır. Kullanılan teknolojiye göre öne çıkan çeşitler şunlardır:

Paket Denetimli Güvenlik Duvarı (Packet Filtering Firewall)

Paket denetimli firewall, ağ trafiğini izleyerek güvenlik kontrolü ile eşleşmeyen veri paketlerini engeller. Durum bilgisi olan ve olmayan olmak üzere iki alt kategoriye ayrılır.

Proxy Tabanlı Güvenlik Duvarı (Application Level Gateways)

Proxy tabanlı güvenlik duvarı, istemci ve sunucu arasında doğrudan bağlantı kurulmasını engeller. Uygulama düzeyinde güvenlik sağlar ancak yoğun trafik dönemlerinde gecikmelere yol açabilir.

Devre Düzeyi Güvenlik Duvarı (Circuit Level Gateways)

Devre düzeyi firewall sistemleri, paket bağlantılarını ya da veri paketlerini doğrulayarak çalışır. TCP tokalaşmasını gözlemleyebilen bu sistem, tek başına yeterli olarak görülmez.

Durum Tabanlı Güvenlik Duvarı (Stateful Firewall)

Bağlantılarla ilgili bilgileri kayıt altına alan stateful firewall, gelen-giden trafiği analiz etmek için ilgili verileri kullanır. Bağlantı noktası tarama saldırısını azaltmaya yardımcı olur ancak JavaScript kodları ile kandırılmaya açık olabilir.

Yeni Nesil Güvenlik Duvarı (New Generation Firewall)

NGFW olarak bilinen yeni nesil firewall çözümleri, geleneksel güvenlik duvarlarına ek olarak yenilikçi özelliklere sahiptir. Paket denetimini durum denetimiyle birleştirir ve derin paket denetimi gerçekleştirebilir. NGFW, antivirüs, kötü yazılım tespiti, saldırı önleme gibi özelliklere sahiptir ve internet trafiğini analiz ederek korur. Kurallar bütününe bağlı olan NGFW, sahtecilik, SQL enjeksiyonu, dosya ekleme gibi saldırılara karşı etkilidir.

Firewall Siber Güvenlik için Neden Önemlidir?

Firewall, güvenlik ağını kontrol ederek zararlı yazılımların ve siber suçluların bilgisayarınıza ulaşmasını engeller. Güvenlik duvarı, yetkisiz erişimi durdurarak bilgilerin ve ağını ele geçirilmesini engeller. Firewall çözümleri, işletmeler ve bireysel kullanıcılar için önemlidir ve güncellemelerle veri güvenliğini sağlar.

Firewall Cihazı Nedir?

Bağımsız bir donanım aygıtı olarak tasarlanan firewall cihazı, işlemci, bellek ve işletim sisteminden oluşur. Firewall cihazlarının çoğu, kolay kurulabilir şekilde üretilmiş olup standart boyutlara sahiptir.

Bazı cihazlar, bağımsız bir aygit olarak kullanılmasının yanı sıra ağ yönlendiricisinin bir parçası olarak da kullanılabilir. Yani, ağ yönlendiricilerinde dahili bir firewall cihazı bulunabilir.

Cihazlar, yönlendirici ile internet veya diğer ağlar arasında yer alır. Bu nedenle, ağın girişinde savunma hattı gibi çalışır. Herhangi bir veri, yönlendirici ile ağ bilgisayarlarına ulaşmadan önce güvenlik duvarı cihazının kontrolünden geçer. Firewall cihazları, bilgisayarları veya yerel ağı dış dünyadan gizlemeye olanak tanımı ile öne çıkar.

Firewall Cihazı ve Firewall Yazılımı Arasındaki Farklar

Donanımsal ve yazılımsal firewall sistemleri arasında birtakım farklar bulunmaktadır. Bilgisayar ve internet arasında kurulan firewall cihazları, tek bir fiziksel aygıtlı tüm ağınızı dış dünyaya karşı korumanızı sağlar. Çevre güvenlik duvarı olarak da bilinen bu aygıtlar, ağ yöneticisine ağın nasıl kullanıldığına dair kontrol imkanı sunar. Donanımsal sistemler, yerleşik güvenlik duvarı olmayan yazılıcısı veya diğer akıllı cihazları da koruma özelliğine sahiptir.

Diğer güvenlik sistemleriyle kolayca entegre olabilen firewall cihazı çeşitleri, VPN ve yük dengeleme gibi ekstra özelliklerle sunulabilir. Tüm ağınızın güvenliğini tek bir noktadan gerçekleştirmenize imkan tanıyan bu cihazlar, zaman ve kaynak tasarrufu anlamına gelir. Çok sayıda bilgisayara sahip firmalarda, firewall yazılımlarını yönetebilmek büyük bir BT ekibine ihtiyaç duymaya yol açabilir. Donanımsal sistemler, özelleştirme konusunda da kullanıcılarla katkı sunar.

BT ekipleri, cihazları sektörde, konuma veya şirketin güvenlik duvarı açıklarına göre yapılandırabilir. Benzersiz kurallar oluşturarak cihazları etkin bir biçimde kullanmak mümkündür.

Öte yandan, firewall yazılımları siber saldırılara karşı ikincil bir savunma mekanızması olarak düşünülebilir. Yazılımsal güvenlik duvarı sistemleri, çeşitli kurallar ışığında veri gönderme veya alma trafığını engelleyebilir.

Yazılımsal güvenlik duvarları, kara listedeki IP adresleri, şüpheli uygulamalar ve kötü amaçlı yazılımları risk seviyelerine göre yasaklayabilir. Bu yazılımlar, farklı kullanıcılar için değişen dözyelerde erişim ve izin ataması yapılmasına imkan sunar. Bu açıdan, sistemler kullanıcılarla esneklik tanır.

İşletmeler Neden Firewall Cihazı Kullanmalı?

Firewall yazılımları, büyük kurumlarda ve bilgisayar sayısının fazla olduğu işletmelerde maliyetli ve zaman alıcı olabilir. Ağdaki her bilgisayara yazılım yüklemek, BT ekipleri için yorucu bir süreç olabilir.

Ayrıca, uygun fiyatlı yazılımlar genellikle hassas ve kurumsal verileri saklamak açısından güvenli olmayabilir. Tüm bu nedenlerden ötürü, işletmeler için firewall cihazı kullanmak daha mantıklı bir seçenekdir.

Kötü amaçlı yazılımlara karşı daha dayanıklı olan cihazların işletim sistemleri, yaygın işletim sistemlerinden farklı çalışabilir.

Siber güvenliğin önemsendiği büyük kurumlarda, BT ekipleri tarafından kurulan cihazlar, veri güvenliğini üst seviyeye taşıyabilir.

WAF (Web Uygulaması Güvenlik Duvarı) nedir?

Web uygulaması güvenlik duvarları, web uygulamalarının robotlar, enjeksiyon ve uygulama katmanı hizmet reddi (DoS) dahil olmak üzere kötü amaçlı saldırılara ve istenmeyen internet trafiğine karşı korunmasına yardımcı olur. WAF, IP adresleri, HTTP üstbilgileri, HTTP gövdesi, URI dizeleri, siteler arası betik çalışma (XSS), SQL enjeksiyonu ve diğer OWASP tanımlı güvenlik açıkları dahil olmak üzere internet tehditlerini önlemeye yönelik kurallar belirlemenize ve yönetmenize yardımcı olur. Web uygulaması güvenlik duvarı, web'e yönelik uygulamaları korumak ve uyumluluk ve analistikler için erişim günlüklerini toplamak için dağıtırılır.

WAF güvenliği neden önemlidir?

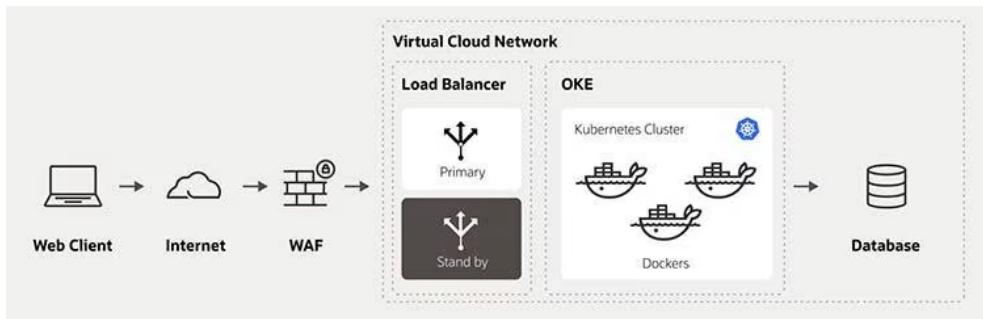
Web uygulaması güvenlik duvarları, coğrafi konum verilerine, beyaz listeye ve kara listeye alınmış IP adreslerine, Yardımlı Metin Aktarım Protokolü Tekdüzen Kaynak Bulucu (HTTP URL) ve HTTP üstbilgisine dayalı erişim kontrolleriyle genel bulutta, şirket içinde ve çoklu bulut ortamlarında dağıtılan uygulama yazılımlarının korunmasına yardımcı olur.

İnsan ve Bilgisayar Ayrımı (CAPTCHA), cihaz yorumlama ve insan etkileşimi algoritmalarına bildirmek için JavaScript, Tam Otomatik Genel Turing Testi dahil olmak üzere bir dizi gelişmiş doğrulama yöntemi ile kötü amaçlı robot trafiğini belirler ve engeller. WAF'ler, birden çok kaynaktan toplanan entegre tehdit zekası ve Açık Web Uygulaması Güvenlik Projesi (OWASP) algılama kurallarının bir sonucu olarak internete yönelik uygulama yazılımlarını saldırılara karşı korur.

Web uygulaması güvenlik duvarı hizmet bileşenleri

WAF'nin bir dizi bileşeni vardır, özellikle:

- Web uygulaması güvenlik duvarı ilkesi^[1]WAF ilkeleri, kaynak yönetimi, koruma kuralı ayarları ve robot algılama özellikleri dahil olmak üzere WAF hizmetinizin genel konfigürasyonunu kapsar.
- Kaynak WAF ilkenizde tanımlandığı gibi, koruma kuralları veya diğer özellikleri ayarlamak için tasarlanmış web uygulamanızın kaynak ana bilgisayar sunucusu.
- Koruma kuralları Koruma kuralları, bir koruma kuralının belirtilen ölçütlerini karşıladıklarında ağ isteklerine izin verecek, engelleyecek veya günlüğe kaydedecek şekilde konfigüre edilebilir. WAF, zaman içinde web uygulamaniza gelen trafiği gözlemleyecek ve uygulanacak yeni kurallar önerecektir.
- Bot yönetimi WAF hizmeti, web uygulamalarınıza gelen tanımlanmış robot trafiğini algılamanıza ve engellemenize veya izin vermenize olanak tanıyan çeşitli özellikler içerir. Robot yönetimi özellikleri arasında JavaScript sorgulaması, CAPTCHA parola kodlaması ve GoodBot beyaz listeleri bulunur. Robot yönetimi çözümleri, web uygulamalarınızdaki şüpheli robot etkinliğini belirlemek ve engellemek için IP hızı sınırlama, CAPTCHA, cihaz parmak izi ve insan etkileşimi parola kodlaması gibi algılama tekniklerini kullanabilir. Aynı zamanda WAF, yasal robot sağlayıcılarından gelen meşru robot trafiğinin bu kontrolleri atlamasına izin verebilir.



Web uygulaması güvenlik duvarlarının özellikleri

WAF'lerin en önemli yetenekleri ve özellikleri şunlardır:

- Etki alanı sistemi (DNS) aracılığıyla dinamik trafik yönlendirmesi: En düşük gecikme süresine sahip yolları belirlemek için binlerce global konumdan kullanıcı gecikme süresini dikkate alan DNS tabanlı trafik yönlendirme algoritmalarından yararlanır.
- WAF hizmetlerinin yüksek erişilebilirliği: Web uygulaması dağıtımını konfigüre ederken WAF'ler, birden çok kaynak sunucusu ekleme yeteneğiyle birlikte birkaç yüksek erişilebilirlik konfigürasyonu seçeneği sunabilir. Bu ayarlar, birincil kaynak sunucuların çevrimdışı olduğu veya sağlamlık denetimlerine doğru yanıt vermediği durumlarda kullanılabilir.
- İlkeleri yönetmek için esnek yöntemler: WAF konfigürasyonları, organizasyonunuzun ihtiyaçlarını karşılamak için özellikleri ve işlevleri konfigüre etmenize ve yönetmenize olanak tanır.
- İzleme ve raporlama: WAF'ler, kullanıcılara uyumluluk ve analiz için içerik kitaplıklarıyla ilgili raporlara erişme yeteneği verir.
- Üst merciye iletme: WAF'lerden gelen bilgiler, destek ekiblerine aciliyete bağlı olarak bir bilet düzenleme ve bilet üst merciye iletme yeteneği sağlar.

Bulut tabanlı Web Uygulaması Güvenlik Duvarı Dağıtma

Bulut tabanlı bir WAF, şirket içi, bulut, hibrit ve çoklu bulut dahil olmak üzere birden çok web uygulaması barındırma ortamını desteklemelidir. Bu da WAF'nin, kullanılan altyapı sağlayıcısına bakılmaksızın bir ağ ucunu kötü amaçlı trafikten koruyabileceği anlamına gelir. Doğru bulut tabanlı WAF, nerede bulunursa bulunsun, internete yönelik tüm uygulama yazılımlarının ve API'lerin güvenliğini sağlamak için bağımsız bir platform sunacaktır.

En iyi bulut tabanlı WAF'ler, bir ortamı izleyen ve sorunlar ortaya çıktığında performansı kanıtlanmış tehdit azaltma adımları öneren deneyimli internet güvenliği uzmanlarından oluşan bir ekip tarafından 7/24 yönetilir.

Riskin önemli ölçüde azaltılması tönenilen bir WAF hizmetinin avantajları arasında yer alır. Bulut sağlayıcısının sorumluluğunda olan WAF konfigürasyonu, izleme, ayarlama ve olay

müdahalesi sayesinde yönetim yükü de azaltılır. Sürekli izleme, organizasyonları planlanmamış kapalı kalma sürelerinden ve bunun sonucunda marka itibarına yönelik olacak zarardan korur. Ayrıca, yönetilen hizmetler, temel iş görevlerine odaklanmak ve kârlılığı iyileştirmek için daha fazla zaman sağlar.

Bulut tabanlı WAF'ler, kaynaklara büyük bir ön yatırım yapmadan veya bakım, donanım değiştirme ve yazılım yükseltmeleriyle ilgili devam eden maliyetler olmadan en yüksek düzeyde web uygulaması güvenliği sağlar. Bulut tabanlı WAF'ler, dağıtım kolaylığı ve öngörülebilir abonelik fiyatlandırması sunarak bütçe planlamasını kolaylaştırır.

Web uygulaması güvenlik duvarlarının avantajları

Web Uygulaması Güvenlik Duvarı (WAF), web uygulamasına veya API'ye yönelik kötü amaçlı istekleri filtreler. Ayrıca, trafiğin nereden geldiği konusunda daha fazla görünürlük sağlar ve uygulama yazılımı erişilebilirliği elde etmeye ve uyumluluk zorunluluklarını daha iyi uygulamaya yardımcı olmak için Katman 7 dağıtılmış hizmet redi (DDos) saldıruları hafifletilir.

Robot yönetimi çözümü, kötü ve/veya şüpheli robot etkinliğinin rekabetçi veriler için web sitenizi taramasını belirlemek ve engellemek için IP hızı sınırlama, CAPTCHA, cihaz parmak izi ve insan etkileşimi parola kodlaması gibi algılama tekniklerini kullanır. Aynı zamanda WAF; Google, Facebook ve diğerlerinden gelen yasal robot trafiğinin amaçlandığı şekilde web uygulamalarınıza erişmeye devam etmesine izin verebilir. WAF, belirli bir kullanıcıya gerçek zamanlı olarak hizmet summak için en iyi global varlık noktasını (POP) belirleyen, veriye dayalı bir algoritma kullanan akıllı bir Etki Alanı Sistemi (DNS) kullanır. Sonuç olarak, kullanıcılarla mümkün olan en iyi çalışma süresi ve hizmet seviyeleri sunulurken kullanıcılar global ağ sorunları ve olası gecikme süresi konusunda yönlendirilir.

Dos ve DDos Nedir?

Dos (Denial Of Service- Servis Hizmet Reddi) saldırısı bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini, kullanıcıların sisteme erişmesini engelleyen bir saldırı türüdür. Her sistemin kaldırabileceği bir ağ trafiği hacmi vardır. Sistemin sahip olduğu bu kaynaklara saldırganlar tarafından aşırı yüklenildiğinde sistem hizmetleri yavaşlamakta hatta sistemin verdiği hizmetler bu saldırular sonucunda tamamen çökmektedir. DDos (Distributed Denial of Service- Dağıtılmış Hizmet Reddi) ise saldırının bir kaynaktan değil de fazla sayıda farklı kaynaktan başlatılmasıyla gerçekleşir. DDos saldırularını gerçekleştirmek için zombi adı verilen cihazlardan oluşan botnetler kullanılmaktadır. Bu zombi cihazlar, internet korsanları tarafından ele geçirilmiş elektronik cihazlardır ve saldırganların amaçları doğrultusunda kullanırlar. DDos saldıruları istenilene ulaşmakta Dos saldırularına göre daha başarılıdır. Birden fazla kaynaktan hedefe doğru gerçekleştirildiği için de ana kaynağı tespit etmek zorlaşmaktadır.

İlk Dos saldırısı 1974'te bir lise öğrencisi tarafından gerçekleştirilirken ilk DDos saldırısı ise 1999'da Minnesota Üniversitesine karşı Trinoo adlı araç kullanılarak gerçekleştirılmıştır. Dos ve DDos saldırıyla amaçlanan sisteme sizmek değil, sistemin verdiği hizmetleri aksatmaktır. Saldırı hedefi olan kurum hizmet veremediği süre boyunca maddi ve manevi olarak zarara uğratır. Uluslararası siber savaşlarda da sıkılıkla kullanılan saldırılardır. Günümüzde çok kolay bir şekilde yapılabilir hale gelmiştir. Kolayca ulaşılabilen, basit araçlarla bu saldırular gerçekleştirilebilir.

Dos ve DDos Saldırı Belirtileri

Sistem hızının normale göre oldukça yavaşlaması ya da artık kullanılamaz hale gelmesi
Normalin dışında sistem ağ trafiği olması Aşırı UDP, SYN ve GET/POST isteklerinin
bulunması

Dos ve DDos Türleri

Volume Based DDoS (Hacim Odaklı Saldırılar): Sunucunun sahip olduğu bant
genişliğinin üstünde istek paketleri gönderilmesidir.

Protocol Based DDoS (Protokol Odaklı Saldırılar): OSI protokolünün 3.Katman
(Network) ve 4.Katmanındaki (Transport) zafiyetin kullanılmasıyla gerçekleştirilir.

Application Layer DDoS (Uygulama Katmanlı Saldırılar): OSI protokolünün 7.katmanı
olan uygulama katmanında bulunan servislerin açıklarının kullanılmasıyla saldırısı yapılır.

HTTP Flood: Hedef sayfaya sürekli olarak get veya post istekleri gönderilerek sistemi
zorlamaktır.

UDP Flood: UDP protokolü kullanılarak saldırısı gerçekleştirilir. Saldırgan tarafından bir
bilgisayarın portlarına çok sayıda UDP paketi gönderilir. Saldırının hedefi olan bilgisayar
portun kullanım durumunu kontrol eder kullanılmıyorsa ICMP paketi ile cevap verir. Çok
sayıda UDP paketine karşılık çok sayıda ICMP paketi gönderilir. Sistem böylece erişilemez
hale gelir.

ICMP Flood: ICMP protokolü kurban sisteme ICMP istek paketleri yollar ve karşı
sistemden cevap bekler. Bu şekilde çok sayıda istege karşılık cevap vermeye çalışan sistem
zorlanır.

Ping of Death: Büyük boyutlu ICMP istek paketinin hedef sisteme yollandanak hedef
sistemin yorulmasıdır.

Syn Flood: Tcp protokolü üçlü el sıkışma ile bağlantı gerçekleştirir. Bu üçlü el sıkışma
işlemi, istemcinin sunucuya SYN mesajı göndererek bağlantı kurmak istediğini belirtir.
Sunucu bu mesajı SYN-ACK mesajı göndererek kabul eder. Ardından istemci ACK yanıyla
bağlantıyı gerçekleştirir. SYN flood saldırısı ise sunucunun beklediği ACK mesajını
göndermez. İstekler sürekli artar ve sistem artık bağlantı kuramaz hale gelir.

TearDrop: UDP protokolünde paketler parçalanarak bir sisteme gönderilir ve bu paketler
ofsetlere bölünerek numaralandırılır. Ofset değerlerine göre tekrar birleştirilir. Bu ofset
değerleri çakışmamalıdır. Eğer çakışma durumu yaşanırsa sisteme işlem yapılamaması
gibi durumlar ortaya çıkar. Teardrop saldırısında is bu ofsetler çakıştırılıp gönderilerek
gerçekleştirilir.

Smurf: Hedefe ping istek paketleri ağır directed broadcast adresine gönderilir paket bu
şekilde ağdaki tüm cihazlara ping istek paketleri göndermiş olur. Ping istek paketlerinin
dönüş adresleri değiştirilerek hedefin ip adresi yapılır. Ağdaki tüm cihazlar da hedef cihaza

ping paketlerini yollar. Böylece saldırı hem gerçekleştirilirken hem de saldırganın kimliği saklanmış olur.

DNS Poisoning: Dns alan adı ip eşleşmelerini sağlayarak kişinin web sitesine erişimini sağlayan sunuculardır. Saldırgan ulaşımak istenen web sitesinin eşleşmesini bozarak başka bir ip adresine yönlendirerek buradaki hazırlamış olduğu zararlı içreklerle kurbana zarar verir.

Dos ve DDos Saldırı Engelleme Yöntemleri

Bu saldırılardan gerçekleştirilmemesi günümüzde oldukça basit olduğu için kurumlar ve sistemler için önemli bir tehdit unsurudur. Bu saldırılardan özellikle DDos saldırısının tamamen engellenmesi için kesin bir yöntem bulunmamakla birlikte saldırıcıları hafifletmek için önlemler alınıp sistemin ağ altyapısının sağlam yapılandırılması gereklidir. Saldırının engellemesinden önce saldırı öncesi önlemlerin alınması ve erken tespiti daha önemlidir.

- Güvenlik duvarı ve antivirüs yazılımı veya donanımı kullanılmalıdır.
- Sistem güncellemeleri zamanında yapılmalıdır.
- Ağ trafigi izlenilmelidir, olağanüstü durumlar için ağ cihazları yapılandırılmalıdır. Yönlendiriciler için rate limiting özelliği, sahte ve bozuk paketlerin engellenmesi, SYN, ICMP ve UDP paketlerinin eşik değerlerinin belirlenmesi gibi yöntemler uygulanabilmektedir.
- Bant genişliği kurumun ihtiyacı olandan fazla olmalıdır.
- Büyük ölçekli kurumlar için İçerik Dağıtım Ağı (CDN) verilerin dünyada birden çok sunucuda saklanması- kullanımı uygulanabilir.

Chmod 777 nedir ?

Chmod 777 genellikle yazılımcıların daha iyi bildiği bir yetki adıdır. Bu yetki adı belirlediğiniz dosyaya yada programa tüm izinleri verir.

Genellikle GNU/LINUX gibi işletim sistemlerinde kullanılan bu izin sayesinde seçtiğiniz program bilgisayarın tamamının erişimine sahip olarak programın herşeyi yapabilir. Bilmemiğiniz yada şüphelendiğiniz program veya dosyalara bu yetkiyi verirseniz zarar görebilirsiniz.

Chmod 777'nin 3 farklı terimi vardır bunlar;

r – w – x'dir. Bunların açılımı ise;

r = Read Permission = Okuma izni w = Write Permission = Yazma izni x = Execute Permission = Çalıştırma izni'dir.

Chmod 777 nasıl kullanılır ?

Chmod 777 adlı yetkilendirme GNU/LINUX gibi işletim sistemlerinde Dosyaya yetkiyi ekleme; “chmod +x (dosyaadi.dosyaturu)” “chmod +w (dosyaadi.dosyaturu)” “chmod +r (dosyaadi.dosyaturu)” Dosyadan yetkiyi silme; “chmod -x (dosyaadi.dosyaturu)” “chmod -w (dosyaadi.dosyaturu)” “chmod -r (dosyaadi.dosyaturu)”

gibi terimlerde kullanılmaktadır. Çoklu yetki eklemek isterseniz bunu “chmod +rx (dosyaadi.dosyaturu)” gibi terimlerde yazarak yapabilirsiniz. Bu komutu yazdıktan sonra seçtiğiniz doya yada program verdığınız yetki türüne göre yetkilendirilecektir.

Chmod 777 nerelerde kullanılır ?

Chmod 777 genellikle GNU/LINUX gibi işletim sistemlerinde kullanılmaktadır. GNU/LINUX gibi işletim sistemlerinde genellikle terminal ekranı olduğundan dolayı coğunlukla kullanılmaktadır.

Chmod 777'nin açılımı nedir ?

Chmod 777'nin açılımı “Change Mod” dur. Türkçe anlamı ise “Mod Değiştirme” anlamına gelmektedir. Genellikle konuşulduğunda daha kısa ve genel bir kelime olduğu için “Chmod” olarak söylemimi tercih edilmektedir.

Chmod 777 ne işe yarar ?

Chmod 777 coğunlukla Programa yada dosyaya yetkilendirmeye yaramaktadır. Yetkilendirebildiğiniz anda verdığınız yetkiyi silme özelliğinде sahipsiniz,hatta eklemek istediğiniz yetkinin bulunduğu yada bulunmadığını bile öğrenebilirsınız. Bu yetkilendirme en çokta yazılımcıların işine yaramıştır. İstedığınız dosyanın yada programın hangi izinlerinin olduğunu görmek için “ls-all” yazmanız yeterlidir.

Chmod 777 için olası ve gereken bilgiler nelerdir ?

Kullanıcı türü seçimleri için kullanıcı terimleri; u = user = kullanıcı g = group = grup o = other = diğer a = all = herkes

Dipnot: Chmod 777 yetkisi verdığınız bir dosyaya veya programa kendini belli etmesi için dosyanın yada programın yazısı yeşil renge bürünmektedir.

777'nin anlamı nereden geliyor ?

r – w – x bunlar 111'e eşittir. rwx'in chmod değeri 7 dir. $7 \times 111 = 777$ ettiği için adı “Chmod 777” olarak yapılmıştır.

Diğer kullanılan izin türleri;

777 = RWX/RWX/RWX 666 = RW/RW/RW 755 = RWX/RW/RW 644 = RW/R/R 700 = RWX/-

GNU/LINUX gibi işletim sistemlerine göre yetki değerleri;
Okuma = 4 Yazma = 2 Çalıştırma = 1

Chmod 777 için dosya – dizin türleri;

– = Normal dosya

d = Dizin

b = Özel dosyaları

c = Özel metin dosyaları

l = Sembolik dosya

P = Özel adlandırılmış pipe dosyası

Chmod ekleme – silme değişkenleri;

– = izin sil (remove permission)

+ = izin ekle (add permission)

== izin koy (set permission)

Dosyaya yetki verildiğinde Chmod'un verdiği bilgilerin örneği;

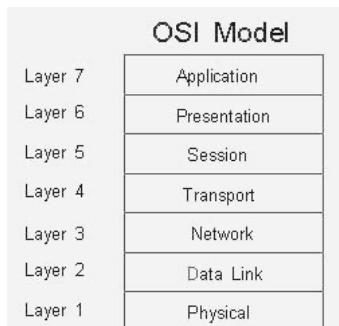
Tür	sahip	grup	diger
(Type)	(user)	(group)	(other)

OSI Katmanları

OSI (Open Systems Interconnection) modelini ISO (International Organization for Standardization) geliştirmiştir. Amaç iki bilgisayar arasındaki iletişimın nasıl olacağını tanımlamaktır.

1978 yılında ilk defa ortaya çıkarılan bu standard 1984 yılında yeni bir düzenleme yardımıyla OSI (Open System Interconnect) referans modeli olarak yayınlanmıştır. OSI öncesindeki dönemde, yalnızca bilgisayar donanımı üreten kuruluşlara özgü ağlar vardı. Bu ağların özellikleri, çoğunlukla yalnızca o üreticinin donanımının bağlanmasına izin verecek biçimde tanımlanmıştı. Onlardan ayrı olarak OSI, çeşitli üreticilerin ürünlerinin bağlanabileceği bir ağ için, bir sektör etkinliği olarak ortaya çıkmıştır.

OSI Modeli herhangi bir donanım ya da bilgisayar ağı tipine göre değişiklik göstermemektedir. OSI'nin amacı ağ mimarilerinin ve protokollerinin bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır. OSI modeli 7 katmana ayrılmıştır.

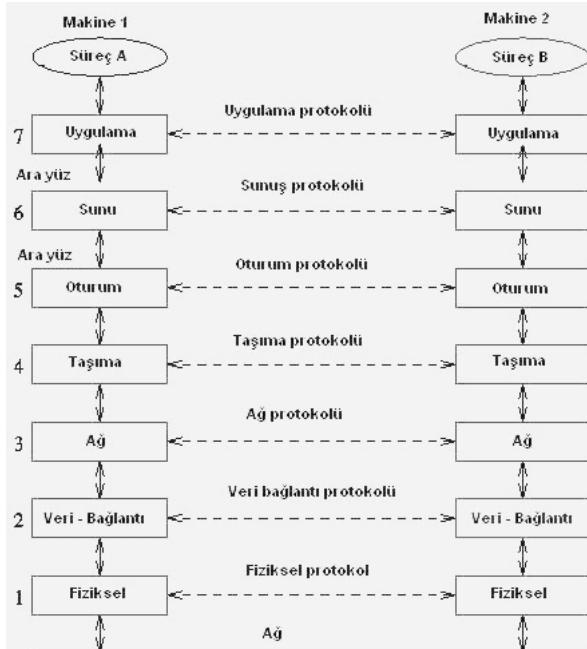


1. Physical (Fiziksel Katman)
2. Data Link (Veri Bağlantı Katmanı)
3. Network (Ağ Katmanı)
4. Transport (Taşıma Katmanı)
5. Session (Oturum Katmanı)
6. Presentation (Sunu Katmanı)
7. Application (Uygulama Katmanı)

Katmanlar Arasındaki İlişki

Her bir katmanın görevi bir üst katmana servis sağlamakta. İki bilgisayar arasındaki iletişimde katmanlar sırasıyla iletişim kurarlar; eş düzeydeki katmanlar aslında doğrudan iletişim kurmazlar ancak aralarında sanal bir iletişim oluştur.

İki Bilgisayar Arasındaki Katmanlar, Gerçek ve Sanal İletişim Arasındaki İlişki

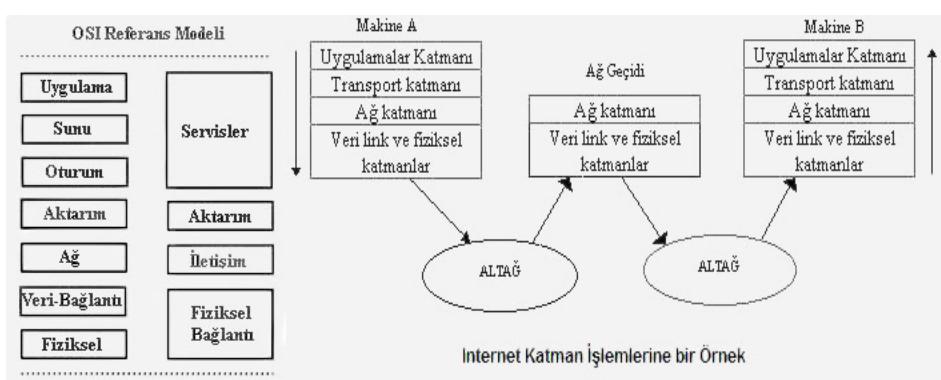


Veri alt katmanlara iletilirken iletim şekli şu şekilde olur: Veri (data) halinde alınan bilgi, taşıma katmanında kesim (segment) adı verilen birimlere ayrılır.

Bu şekilde veri alıcı makinede tekrar biraraya getirilirken doğru sıralanması sağlanmış olur. Ağ katmanına segment şeklinde gelen verilere burada adres bilgileri eklenir; böylece kesimler paket haline dönüşür. Veri-bağlantı katmanında paketlere MAC adresleri eklenerek çerçeve (frame) adını verdigimiz yapı oluşur.

En son aşama olarak fiziksel katmana gelen çerçeveler burada bir bit dizisine dönüştürülerek iletme hazır hale getirilir.

Verinin iletimi üst katmandan alt katmana doğru olur. Verinin kablo ile iletimi fiziksel katman tarafından gerçekleştirilir. Diğer bilgisayarda ise önce fiziksel katman ile karşılanan veri üst katmanlara doğru hareket eder.



1. Fiziksel Katman

Fiziksel katman verinin kablo üzerinde alacağı yapıyı tanımlar. Veriler bit olarak iletilir. Bu katman bir ve sıfırların nasıl elektrik, ışık veya radyo sinyallerine çevrileceğini ve aktarılacağını tanımlar. Gönderen tarafta fiziksel katman bir ve sıfırları elektrik sinyallerine çevirip kabloya yerleştirirken, alıcı tarafta fiziksel katman kablodan okuduğu bu sinyalleri tekrar bir ve sıfır haline getirir.

Fiziksel katman veri bitlerinin karşı tarafa, kullanılan medya(kablo, fiber optik, radyo sinyalleri) üzerinden nasıl gönderileceğini tanımlar. Veri iletiminin mümkün olabilmesi için iki tarafın aynı kurallar üzerinde tanımlanmış olması gereklidir. Hub (Göbek) 1.katmanda çalışan bir cihazdır. Bu cihazlar gelen veriyi bir takım elektrik sinyalleri olarak gören ve bu sinyalleri çoğaltıp, diğer portlarına gönderen bir cihazdır.

2. Veri Bağlantı Katmanı

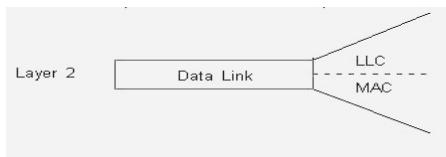
Veri bağlantı katmanı fiziksel katmana erişmek ve kullanmak ile ilgili kuralları belirler. Bu katmandada Ethernet ya da Token Ring olarak bilinen erişim yöntemleri çalışır. Bu erişim yöntemleri verileri kendi protokollerine uygun olarak işleyerek iletilerler.

Veri bağlantı katmanında veriler ağ katmanından fiziksel katmana gönderilirler. Bu aşamada veriler belli parçalara bölünür. Bu parçalara paket ya da çerçeve (frame) denir. Çerçeveler verileri belli bir kontrol içinde göndermeyi sağlayan paketlerdir.

Veri bağlantı katmanının büyük bir bölümü ağ kartı içinde gerçekleşir. Veri bağlantı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığından tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir.

Veri bağlantısı katmanı iki alt bölüme ayrılır:

- Media Access Control (MAC)
- Logical Link Control (LLC)



MAC alt katmanı veriyi hata kontrol kodu(CRC), alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır. Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.

LLC alt katmanı bir üst katman olan ağ katmanı için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur(Service Access Points, SAPs). Böylece kaynak makinada ve hedef makinada aynı protokoller iletişime geçebilir(örneğin TCP/IP<-->TCP/IP). LLC ayrıca veri paketlerinden bozuk gidenlerin(veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. Flow Control yani alıcının işleyebileğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

Ağlarda bulunan çerçeve tipleri şöyledir:

- 802.2 Ethernet II
- 802.3 Ethernet
- 802.4 Token Bus
- 802.5 Token Ring

Ayrıca switch (anahtar) 2.katmanda çalışan bir cihazdır. Çünkü 2. katmanda tanımlı MAC adreslerini algılayabilirler ve bir porttan gelen veri paketini (yne elektrik sinyalleri halinde) sadece gerekli olan porta (o porttaki makinanın MAC adresini bildiği için) yollayabilirler.

3. Ağ Katmanı

Ağ katmanı veri paketine farklı bir ağa gönderilmesi gerekiğinde yönlendiricilerin kullanacağı bilginin eklendiği katmandır. Bu katmanda veriler paket olarak taşınır.^[1]Ağ katmanında iki istasyon arasında en ekonomik yoldan verinin iletimi kontrol edilir. Bu katman sayesinde verinin yönlendiriciler (router) aracılığıyla yönlendirilmesi sağlanır.^[2]Ağ aşamasında mesajlar adreslenir ayrıca mantıksal adresler fiziksel adreslere çevirilir. Bu aşamada ağ trafiği, yönlendirme gibi işlemler de yapılır.^[3]IP protokolü bu katmanda çalışır.

4. Taşıma Katmanı

Taşıma katmanı üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler. TCP, UDP, SPX protokoller bu katmanda çalışır. Bu protokoller hata kontrolü gibi görevleri de yerine getirir.^[4]Bu katmanda veriler kesim (segment) halinde taşınır.^[5]Taşıma katmanı üst katmanlara taşıma servisi sağlar ayrıca ağıın servis kalitesini artırır (QoS – Quality of Service).^[6]Taşıma katmanı verinin uçtan uca iletimini sağlar. Verinin hata kontrolü ve zamanında ulaşıp ulaşmadığı kontrol edilir. Taşıma katmanı ayrıca veriyi üst katmanlara taşıma görevi yapar.

5. Oturum Katmanı

Oturum katmanında iki bilgisayardaki uygulama arasındaki bağlantının yapılması, kullanılması ve bitilmesi işlemleri yapılır. Bir bilgisayar birden fazla bilgisayarlarla aynı anda iletişim içinde olduğunda, gerekiğinde doğru bilgisayarla konuşabilmesini sağlar. Bu, sunum katmanına yollanacak veriler farklı oturumlarla birbirinden ayrılarak yapılır.^[7]NetBIOS, RPC, Named Pipes ve Sockets gibi protokoller bu katmanda çalışır.

6. Sunuş Katmanı

Sunuş katmanının en önemli görevi yollanan verinin karşı bilgisayar tarafından anlaşılacak şekilde çevrilmesidir. Bu sayede farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Sunum katmanı uygulama katmanına verileri yollar daha sonra bu katmanda verinin yapısı, biçimi ile ilgili düzenlemeler yapılır, verinin formatı belirlenir. Ayrıca verinin şifrelenmesi, açılması, sıkıştırılması da bu katmanda yapılır. GIF, JPEG, TIFF, EBCDIC, ASCII vb. bu katmanda çalışır.

7. Uygulama Katmanı

Uygulama katmanı bilgisayar uygulaması ile ağ arasında bir arabirim sağlar. OSI katmanları arasında sadece bu katman diğer katmanlara servis sağlamaz. Uygulamaların ağ üzerinde çalışması sağlanır. Uygulama katmanı ağ servisini kullanacak olan programdır. Bu katman kullanıcıların gereksinimini karşılar. SSH, telnet, FTP, TFTP, SMTP, SNMP, HTTP, DNS protokoller ve tarayıcılar bu katmanda çalışır. E-posta ve veritabanı gibi uygulamalar bu katman aracılığıyla yapılır.

ARP Poisoning

ARP (Address Resolution Protocol): Adres çözümleme protokolü olarak ip adresi bilinen hedefin fiziksel adresini (MAC adresini) bulmaya yarayan bir protokoldür. Bu protokolün kullanılma amacı ise, aynı ağ üzerinde paketler fiziksel adreslerine göre yönlendirilir.

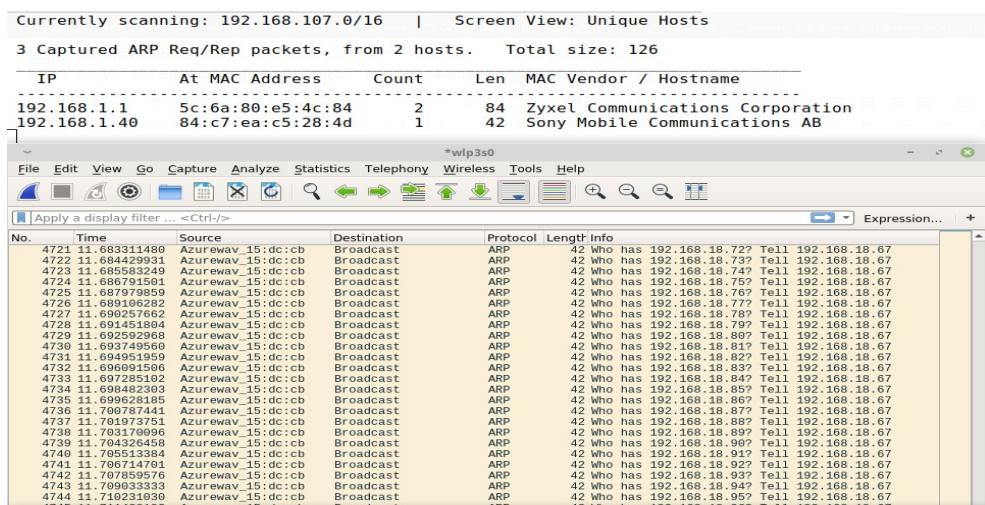
Bir ağa bağlandığımız zaman ağda haberleşme sağlanırken sürekli olarak ARP istekleri yapılır. Geri dönen cevaplar ise ARP tablosunda saklanır. Bilgisayarımızın ARP tablosunu terminal üzerinde ARP komutu ile görebiliriz.

```
hakacu@hakacu:~$ arp
Address          HWtype  HWaddress          Flags Mask   Iface
192.168.1.41    ether    5c:6a:80:e5:4c:84  C      wlp3s0
MitraStar.Home   ether    5c:6a:80:e5:4c:84  (incomplete)
192.168.1.33    ether    5c:6a:80:e5:4c:84  (incomplete)
192.168.1.34    ether    5c:6a:80:e5:4c:84  (incomplete)
192.168.1.45    ether    34:78:d7:2f:fc:84  C      wlp3s0
hakacu@hakacu:~$
```

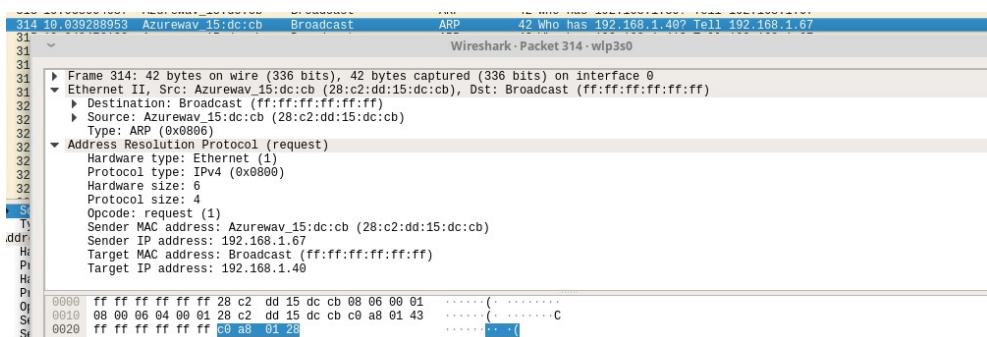
Bir ağa bağlandığımız zaman bilgisayarımıza sürekli olarak ARP paketleri gönderilir. Bunun nedeni ağ üzerindeki gateway dahil olmak üzere ağ üzerindeki bilgisayarlar sürekli olarak paket göndermektedir.

Gönderilen paketlerin MAC adresi ile bizim MAC adresimiz eşleşiyor mu diye kontrol edilmektedir. Örnek olarak Netdiscover aracı ile bizimle aynı ağdaki cihazları tespit belirlenen ip aralığına ARP request paketleri gönderir. Sırasıyla bu ip adresi kime ait anlamındadır. Karşı taraftan ARP Reply paketi gelir ise bu paketin içerisinde MAC adresi bulunur.

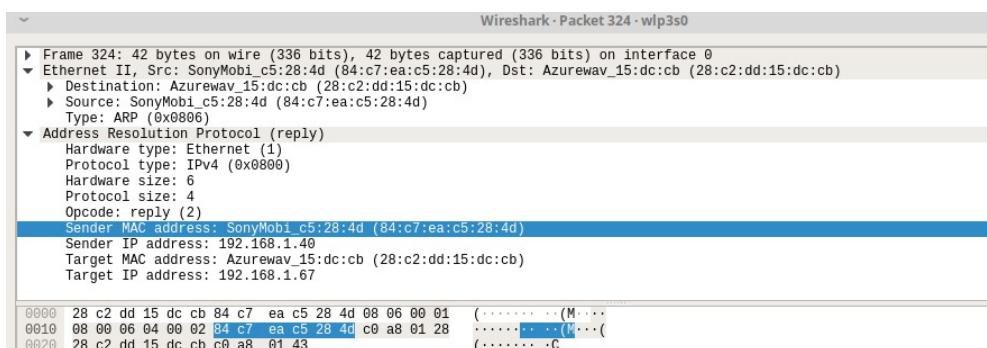
Bu paketleri Wireshark aracıyla dinlemeye alabiliriz.



Gönderilen paketin içeriğine bakıldığı zaman MAC adresi bilinmediği için broadcast yayın yapıldığı gözükmemektedir. Bu istek tarama aralığında bulunan tüm adreslere iletilmektedir.



İstek yapılan adreste eğer bir cihaz varsa cihaz MAC adresini isteğin geldiği adrese gönderir. Bu sayede adresin MAC adresi ARP tablosuna eklenir. Bir sonraki istekte ağa broadcast yollamadan iletişim sağlanabilmektedir.



MAC adresleri insanların kimlik numaraları gibi tekil olarak belirlenir. Bağlandığımız bir ağa ise diğer bağlanan cihazların MAC adreslerini kolay bir şekilde öğrenebiliriz. Bizler internete ilk bağlandığımızda bizi yönlendirecek ağ cihazına sürekli olarak paketler göndeririz.

Bu gönderdiğimiz paketler aynı ağa olduğuümüzden dolayı MAC adresine göre yönlendirilmektedir.

ARP poisoning saldırısının amacı ise ağa MAC adresine göre giden paketi, aynı MAC adresini taklit ederek paketi ele geçirme işlemi yapılmasına dayanır. Bu sayede yönlendiriciye gitmesi gereken paket saldırgan kişinin eLINE geçer. ARP zehirlenmesinin olmadığı bir anda kullanıcı ARP tablosuna baktığı zaman MAC adreslerinin tekil olduğunu görecektir.

```
C:\>arp -a
Arabirim: 192.168.140.129 --- 0xb
    Internet Adresi      Fiziksel Adres      Türü
192.168.140.2          00-50-56-f9-ae-a4      dinamik
192.168.140.128        00-0c-29-62-72-e9      dinamik
```

ARP tablosunun zehirlenmesi işlemine başlamadan önce gelen paketleri yönlendirmek amacıyla ip yönlendirmeyi aktif etmemiz gerekmektedir. IP yönlendirmenin aktif olması için ip_forward 'in değerinin 1 yani aktif olması gerekmektedir. Kullandığımız komut ile dosyanın içerisinde 1 değeri atmış oluruz.

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

Saldırgan ip adresi : 192.168.140.128

Hedef ip adresi : 192.168.140.129

Saldırımızı gerçekleştirirken ARPSpoof aracını kullanacağımız. Aracın manuel notunda kullanımı gösterilmektedir.

```
ARPSP0OF(8)                               System Manager's Manual                               ARPSP0OF(8)

NAME
arp spoof - intercept packets on a switched LAN

SYNOPSIS
arp spoof [-i interface] [-c own|host|both] [-t target] [-r] host

DESCRIPTION
arp spoof  redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP
replies. This is an extremely effective way of sniffing traffic on a switch.

Kernel IP forwarding (or a userland program which accomplishes the same, e.g. fragrouter(8)) must be turned on ahead of
time.

OPTIONS
-i interface
    Specify the interface to use.

-c own|host|both
    Specify which hardware address t use when restoring the arp configuration; while cleaning up, packets can be send
    with the own address as well as with the address of the host. Sending packets with a fake hw address can disrupt con-
    nectivity with certain switch/ap/bridge configurations, however it works more reliably than using the own address,
    which is the default way arpspoof cleans up afterwards.

-t target
    Specify a particular host to ARP poison (if not specified, all hosts on the LAN). Repeat to specify multiple hosts.

-r    Poison both hosts (host and target) to capture traffic in both directions. (only valid in conjunction with -t)
```

Kullanacağımız parametreler

-i = Arayüz belirlemek için kullanılacaktır. (ip adresimizi öğrenirken hangi arayüzün ip adresine sahip olduğu gözükmektedir.)

-t = Hedef adres belirlemek için kullanılacaktır.

Hedef sistemin ARP tablosunu zehirleyerek işlemlere başlayabiliriz. Hedefimize sürekli olarak ARP reply paketleri yollamaktır.

```
arp spoof -i eth0 -t 192.168.140.129 192.168.29.128
```

Şimdi ise sürekli olarak ARP Reply paketleri yollanarak araya girme işlemi yapılacaktır.
arp spoof -i eth0 -t 192.168.140.128 192.168.29.129

ARP poisoning saldırılarda ki hedef aslında gateway in MAC adresini zehirleyerek, giden gelen paketleri ele geçirmek diyebiliriz. Saldırıya uğrayan kullanıcının ARP tablosuna baktığımızda tabloda ki MAC adreslerinin aynı olduğunu görüyoruz. Saldırımız başarıyla gerçekleşmiştir.

```
C:\Users\hakacu>arp -a
Arabirim: 192.168.140.129 --- 0xb
        Internet Adresi      Fiziksel Adres      Türü
        192.168.140.2          00-0c-29-62-72-e9      dinamik
        192.168.140.128         00-0c-29-62-72-e9      dinamik
```

Fark edildiği gibi bu saldırı gerçekleştiği anda ARP tablomuzda aynı MAC adreslerinin olduğu gözükmüyor. Yazının en başında dediğimiz gibi her MAC adresinden yalnızca bir tane olabilmektedir. Bu durumda saldırıyı tespit edebiliriz.

Günümüzdeki En Yaygın 10 Siber Saldırı

1) Malware

Malware kötü niyetli yazılımların kısaltmasıdır. Solucanlar, virüsler, truva atları bunlara örnek olarak verilebilir. Kişilerin izni olmadan bilgisayar sistemlerine sızdırılan kötü amaçlı yazılımlardır.

Bilgisayarları veya ağları çalışmaz hale getirebilir, gizlenebilir, çoğalabilir veya saldırganlara erişim izni verip sistemi uzaktan kontrol edebilme şansı verebilirler.

2) Phishing

Kimlik avı saldıruları olarak adlandırılan bu yöntemde ise saldırganlar kişilere güvenilir kaynaklardan gelmiş gibi gösterilen e-postalar yollayarak kişilerin site bilgilerini, kredi kartı bilgilerini çalmaya çalışırlar. Genellikle e-posta yoluyla gönderdikleri linklere tıklayan mağdurlar, klonlanmış sitelere yönlendirilir ve girdikleri bilgileri saldırganlarla paylaşmış olurlar.

3) DoS ve DDoS

İngilizce açılımı Denial of Services ve Distributed Denial of Services olan bu yöntemler ise bazı çevrimiçi hizmetlerin düzgün çalışmasını engellemeye çalışmak için yapılan saldırılardır. Saldırganlar bir web sitesine veya bir veri tabanına çok fazla sayıda istek yollayıp sistemi meşgul ederler ve bu da sistemlerin çalışmasını durdurmasına yol açabilir. DDoS ise bu saldıruların birden fazla bilgisayardan yapılması ile olur.

4) Man in The Middle

Bu siber saldırı çeşidine ise saldırganlar kurbanlar ile erişmek istedikleri web servisi arasında kendilerini gizleyerek, kurbanları kendi ağları üzerinden erişmek istedikleri servise yönlendirirler. Örneğin bir Wi-Fi ağını taklit ederler ve kurbanlar erişmek istedikleri Wi-Fi ağının yerine saldırganların Wi-Fi ağına girmiş olurlar. Bundan sonraki yaptıkları her işlemi saldırganlar görebilir ve kullanıcıların verilerini toplayabilirler.

5) SQL Injection

Günümüzde birçok veri tabanı SQL ile yazılmış komutlara uymak için tasarlanmıştır ve kullanıcılarından bilgi alan birçok web sitesi bu verileri SQL veri tabanlarına gönderir. Saldırganlar SQL güvenlik açıklarından faydalananak kurbanların veri tabanlarını kontrol altına alırlar. Örneğin bir SQL enjeksiyon saldırısında bir bilgisayar korsanı, bazı SQL komutlarını ad ve adres bilgisi isteyen bir web formuna yazar; web sitesi ve veri tabanı doğru programlanmadıysa, veri tabanı bu komutları çalıştırmayı deneyebilir.

6) Cryptojacking

Cryptojacking, başkasının bilgisayarının sizin için cryptocurrency üretme işini yapmasını içeren özel bir saldırıdır. Saldırganlar gerekli hesaplamaları yapmak için kurbanın bilgisayarına kötü amaçlı yazılım yüklerler veya bazen kötü amaçla kullandıkları kodları kurbanın tarayıcısında çalışan JavaScript'te çalıştırırlar.

7) Zero Day Exploit

Adını bir yama yayınlandıktan sonra, kullanıcıların güvenlik güncellemelerini indirirken az sayıda bilgisayara ulaşmalarından alır. Yazılımdaki açıklar henüz daha düzeltilmemiştir ve bu da saldırganlara fırsat sağlar. Bu tür güvenlik açıklarından yararlanma teknikleri günümüzde Darkweb üzerinden yayılmamakta veya satılmaktadır.

8) Passwords Attack

Şifreleme bir sisteme girerken kullandığımız en yaygın mekanizma olduğundan, parola saldıruları en yaygın saldırular arasındadır. Brute Force olarak adlandırılan bir çeşidine şifre tahmini için aralıksız olarak rastgele şifre deneyen bir kötü amaçlı teknik kullanılır.

Bunu engellemenin en kolay yolu çok kez denenen parola girişiminin ardından kendini kilitleyen bir hesap kilitleme politikası uygulamaktır.

9) Eavesdropping Attack

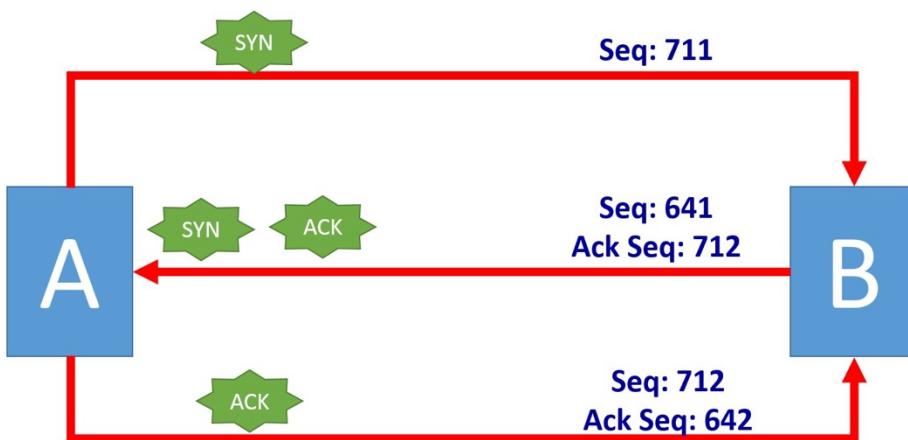
Bu saldırının tipinde saldırganlar bir ağa sızarlar ve gizlice dinleme yaparak kullanıcıların o ağ üzerinden göndereceği kredi kartı bilgileri, şifreler ve konuşmalar gibi kişisel verileri dinlerler. Pasif olan yönteminde genellikle sadece dinleme yaparak bilgiler toplanır fakat aktif yönteminde ise saldırganlar kullanıcılarla ağıdaki dost bir birim gibi gözüker sorular sorarak bilgi toplarlar.

10) Birthday Attack

Doğum günü saldıruları, bir mesajın, yazılımın veya dijital imzanın bütünlüğünü doğrulamak için kullanılan karma algoritmalarla karşı yapılır. Bir karma işlevi tarafından işlenen bir mesaj, giriş mesajının uzunluğundan bağımsız olarak sabit uzunlukta bir mesaj özetini (MD) üretir. Bu MD, mesajı benzersiz bir şekilde karakterize eder. Doğum günü saldırısı, bir karma işlevi tarafından işlendiğinde aynı MD'yi üreten iki rastgele mesaj bulma olasılığını ifade eder. Bir saldırgan, kullanıcısı olduğu gibi mesajı için aynı MD'yi hesaplarsa, kullanıcının mesajını güvenle onunla değiştirebilir ve alıcı MD'leri karşılaştırsa bile değiştirmeyi tespit edemez.

TCP Üçlü El Sıkışma – TCP Three Way Handshake

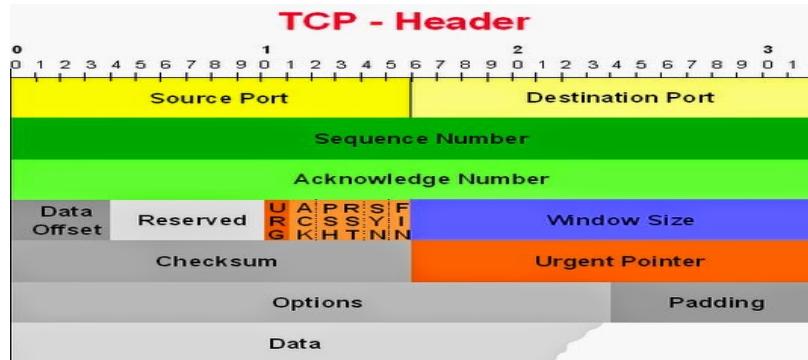
TCP üçlü el sıkışma adından da anlaşılacağı üzere, 3 adımdan oluşur. Hem son adım, hem de ilk adım hizmeti almak isteyen istemci tarafından gerçekleştirilir. Bu 3 adım gerçekleştikten sonra, sunucu taraf, hizmet vermeye başlar. TCP üçlü el sıkışmayı betimleyen bir şekil aşağıdaki gibidir. Bu şekilde, A istemci tarafı, B ise sunucu tarafı temsil eder.



TCP üçlü el sıkışmanın adımları yukarıdaki şekile göre şu şekilde özetlenebilir:

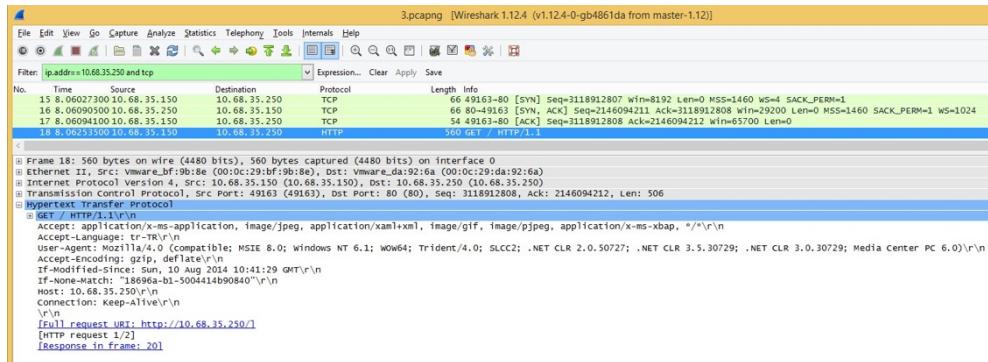
- İlk adım istemci tarafından gerçekleştirilir. İstemci işletim sistemi rastgele bir sıra numarası (Sequence Number) ile sunucuya, SYN (Synchronize) biti / bayrağı “1” olarak ayarlanmış bir paket gönderir. Şekilde sıra numarasının 711 olduğu görülmektedir. Bu sıra numarası sayesinde, paketler TCP iletişimini gerçekleştirken sıralı gelmese bile, alıcı taraf bu paketleri sıraya koymasını sağlar. Özetle; istemci sunucuya SYN bayrağı aktif edilmiş ve sıra numarası 711 olan paketi yollar.
- İkinci adım sunucu tarafından gerçekleştirilir. İstemcinin gönderdiği paketi alan sunucu, istemciye sonraki paketi hazırlar. Göndereceği paketin SYN (Synchronize) ve ACK (Acknowledgement) bayraklarını “1” olarak ayarlar. Ayrıca, istemciden gelen paketin sıra numarasına bakar ve istemcinin gönderdiği sıra numarasını 1 arttırarak göndereceği paketin ACK numarasını (Acknowledgement Number) 712 olarak ayarlar. Böylece, sunucu taraf (B tarafı), hem gönderdiği paketin, istemci tarafından doğru sıraya koymasını sağlamış olur; hem de istemci tarafın bir sonraki göndereceği ve sunucu tarafından kabul edilecek olan sıra numarası belirtilmiş olur. Diğer bir deyişle, sunucu “sıra numarası 712 olan paketi bekliyorum” diye belirtmiş olur. Benzer şekilde, sunucu işletim sistemi, rastgele bir sıra numarası (Sequence Number) üretir. Şekilde sıra numarasının 641 olduğu görülmektedir. Bu sıra numarası, gönderdiği paketin cevabını doğru sıraya koymak için kullanılacaktır. Özetle; sunucu istemciye SYN ve ACK bayrakları aktif edilmiş ve sıra numarası 641, ACK numarası 712 olan paketi yollar.
- Son adım istemci tarafından gerçekleştirilir. Sunucunun gönderdiği paketi alan istemci, sunucuya sonraki paketi hazırlar. Göndereceği paketin ACK (Acknowledgement) bayrağını “1” olarak ayarlar. Ayrıca, sunucudan gelen paketin sıra numarasına bakar ve sunucunun gönderdiği sıra numarasını 1 arttırarak göndereceği paketin ACK numarasını (Acknowledgement Number) 642 olarak ayarlar. Bir önceki adımda sunucu tarafından gönderilen ACK numarası (Acknowledgement Number), istemcinin göndereceği paketin sıra numarasına (Sequence Number) eşit olacak şekilde ayarlanır. Şekilde sıra numarasının 712 olduğu görülmektedir. Özetle; istemci sunucuya ACK bayrağı aktif edilmiş ve sıra numarası 712, ACK numarası 642 olan paketi yollar.

Üçlü el sıkışmayı daha iyi anlamak için TCP başlığını (TCP Header) incelemek gerekebilir. TCP başlığı ise şu şekildedir:

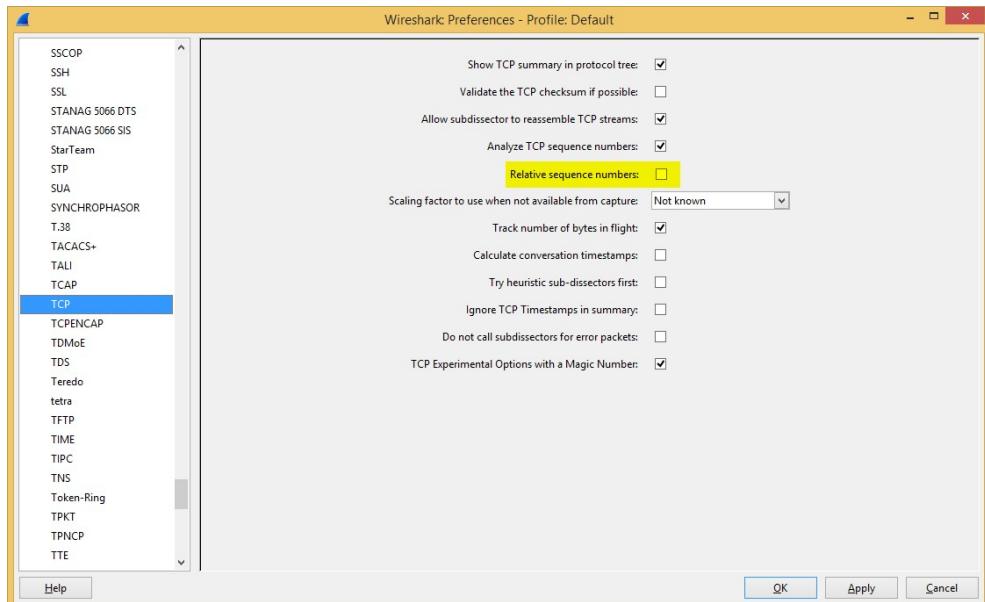


TCP üçlü el sıkışma sürecinin adımlarını uygulamalı olarak görmek için Wireshark aracı kullanılabilir. 10.68.35.150 IP adresli istemci, 10.68.35.250 IP adresli web sunucusundan hizmet alması sırasında gerçekleşen TCP üçlü el sıkışma adımlarına ait Wireshark ekran görüntüleri aşağıdaki gibidir.

ip.addr==10.68.35.250 and tcp



Not: Sıra numaraları, anlaşılırlığı artırmak ve sadeleştirme yapmak için, Wireshark varsayılan olarak 0'dan başlatılır. Bu sıra numaralarının orijinal değerleri için “Wireshark > Edit > Preferences... > Protocols > TCP” ekranında “Relative sequence numbers:” seçeneği devre dışı bırakılmalıdır.



TCP üçlü el sıkışmanın adımları Wireshark üzerinde aşağıdaki gibi izlenebilir.

- İstemci tarafından hazırlanan ilk pakette, SYN bayrağının aktif edildiği ve rastgele bir sıra numarasının oluşturulduğu görülmektedir.

The screenshot shows a Wireshark packet capture window. The filter bar at the top is set to 'ip.addr==10.68.35.250 and tcp'. The second packet in the list is highlighted. This packet is a SYN-ACK segment with the following details:

- Time: 16.8.06027300 10.68.35.150
- Source: 10.68.35.250
- Destination: 10.68.35.150
- Protocol: TCP
- Length: 66
- Info: 49163->80 [SYN, ACK] Seq=2146094211 Ack=3118912808 win=29200 Len=0 MSS=1460 WS=4 SACK_PERM=1

The 'Sequence number' field in the info pane shows '3118912807'. The 'Ack sequence number' field shows '8192'. The 'Header Length' is listed as 32 bytes. Below the packet list, the hex and ASCII panes show the raw data of the selected SYN-ACK packet.

- Sunucu tarafından hazırlanan ikinci pakette, SYN ve ACK bayraklarının aktif edildiği ve ACK numarasının, istemciye ait paketin sıra numarasının bir fazlası; sıra numarasının ise rastgele oluşturulduğu görülmektedir.

```

ip.addr==10.68.35.250 and tcp
Expression.. Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000000 10.68.35.130 10.68.35.250 TCP 60 <18163>-80 [SYN] Seq=3118912807 win=8192 Len=0 MSS=1460 ws=1 SACK_PERM=1
2 0.000005100 10.68.35.130 10.68.35.250 TCP 60 <18163> [SYN, ACK] Seq=3118912808 win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024
3 0.000009100 10.68.35.130 10.68.35.250 TCP 54 49103>-80 [ACK] Seq=3118912808 Ack=3118912807 win=65706 Len=0
4 0.002535000 10.68.35.130 10.68.35.250 HTTP 560 GET /HTTP/1.1

■ Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
■ Ethernet II, Src: vmsware_da92:6a (00:0c:29:da:92:6a), Dst: Vmware_bf9b:8e (00:0c:29:bf:9b:8e)
■ Internet Control Message Protocol, Src Port: 80 (HTTP), Dst Port: 49163 (49163), Seq: 2146094211, ACK: 3118912808, Len: 0
■ Transmission Control Protocol, Src Port: 80 (HTTP), Dst Port: 49163 (49163), Seq: 2146094211, ACK: 3118912808, Len: 0

Source Port: 80 (HTTP)
Destination Port: 49163 (49163)
[Stream Index: 0]
[Tcp Options Length: 0]
Sequence number: 2146094211
Acknowledgment number: 3118912808
Header Length: 32 bytes
[Data Offset: 0x0000000000000000]
[Checksum: 0x00000000] [Checksum Status: SYN, ACK]

000... = Reserved: Not set
000... = ...: Not set
000... = ...: Congestion Window Reduced (CWR): Not set
000... = ...: ECN-Echo: Not set
000... = ...: Urgent: Not set
000... = ...: Acknowledgment: set
000... = ...: Push: Not set
000... = ...: Reset: Not set
000... = ...: SACK: Not set

■ [Event: rx packet (Chat/Sequence): Connection establish acknowledgement (SYN+ACK); server port 80]
[Connection establish acknowledgement (SYN+ACK); server port 80]
[Severity level: chat]
[Group: Standard]
000... = ...: P=1 Not set
window size value: 29200
[calculated window size: 29200]
■ Checksum: 0xd4fd [validation disabled]
[Checksum Status: SYN+ACK]
[Options: ]
[Data Offset: 0x0000000000000000]
[Checksum: 0xd4fd]
[Checksum Status: SYN+ACK analysis]

0000 00 04 29 bf 9b 8e 00 00 00 29 da 92 6a 08 00 45 00 ..J...J...J..E.
0010 00 00 04 00 40 00 40 00 04 06 dc aa 9c 23 fa 04 ..D..D
0020 23 96 00 50 00 0b 7f ee cc 83 b9 e6 d5 28 20 02 #,P,...D
0030 00 00 04 fd 00 02 00 04 03 b1 01 04 02 01 03 ..D..D
0040 03 04 ..D..D


```

- İstemci tarafından hazırlanan son pakette, ACK bayrağının aktif edildiği ve ACK numarasının, sunucuya ait paketin sıra numarasının bir fazlası; sıra numarasının ise sunucuya ait paketin ACK numarasına eşit olduğu görülmektedir.

Filter:	ip.addr==10.68.35.250 and tcp	Expression...	Clear	Apply	Save	
Nr.	Time	Source	Destination	Protocol	Length	Info
15	8.0602730010.68.35.150	10.68.35.250	TCP	66	49163-80 [RPN] Seq=3118912807 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	
16	8.0609042110.68.35.150	10.68.35.150	TCP	64	49163-80 [SYN, ACK] Seq=2146094211 Ack=3118912808 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024	
17	8.06091210010.68.35.150	10.68.35.250	TCP	54	49163-80 [ACK] Seq=3118912808 Ack=2146094212 Win=63700 Len=0	
		10.68.35.250	HTTP	360	GET / HTTP/1.1	

Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

ETHERNET II, Src: vmware_pf9b:0b:00 (00:0c:29:bf:9b:8e), Dst: VMware_da:92:6a (00:0c:29:d9:92:6a)

Internet Protocol Version 4, Src: 10.68.35.150 (10.68.35.150), Dst: 10.68.35.250 (10.68.35.250)

Transmission Control Protocol, Src Port: 49163 (49163), Dst Port: 80 (80), Seq: 3118912808, Ack: 2146094212, Len: 0

Source Port: 49163 (49163)
Destination Port: 80 (80)
[Stream index: 0]
[TCP Segment Len: 0]

Sequence number: 3118912808
Acknowledge number: 2146094212
Header Length: 20 bytes

..... 0000 0001 0000 = Flags: 0x10 (ACK)

000.0= Reserved: Not set
.0.... .0= More Fragments: Not set
...0.... .0= Connection window Reduced (CWR): Not set
.0.... .0= Urgent: Not set
..0.... .1= Acknowledgment: Set
....0.... .0= Window scale: 0
....0.... .0= Reset: Not set
....0.... .0= Sync: Not set
....0.... .0= Fin: Not set
window size value: 16425
(calculated window size: 65700)
(window size scaling factor: 4)

Checksum: 0x5c32 [validation disabled]
urgent pointer: 0

[SEQ/ACK analysis]

Aynı iletişime ait sunucu tarafından trafik “tcpdump” komut satırı aracı ile izlendiğinde benzer adımların gerçekleştiği görülmektedir.

```
tcpdump -i eth0 -ttt -vv host 10.68.35.150 and tcp
```

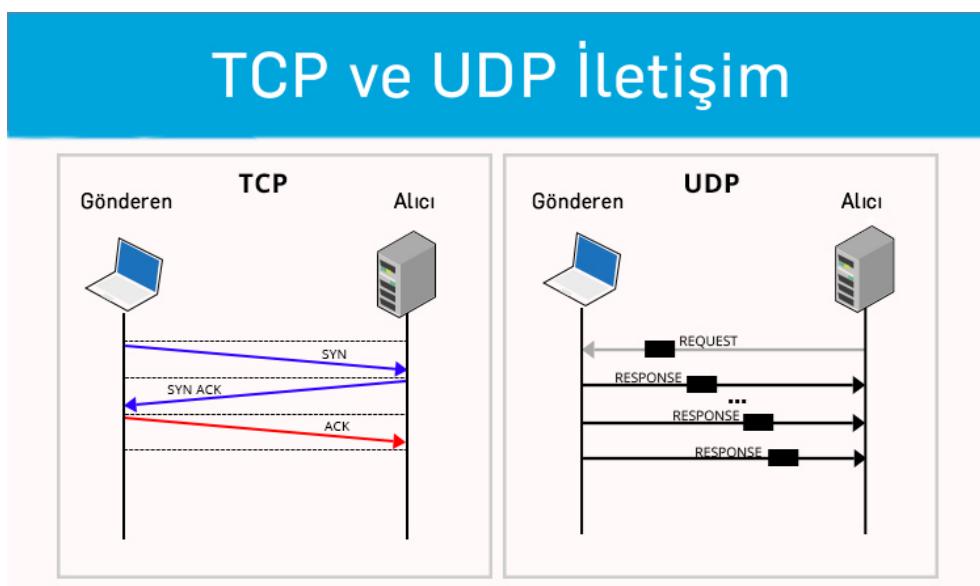
```

root@kali:~# tcpdump -i eth0 -ttt -vv host 10.68.35.150 and tcp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
00:00:00.000000 IP (tos 0x0, ttl 128, id 526, offset 0, flags [DF], proto TCP (6), length 52)
    10.68.35.150.49163 > 10.68.35.250.http: Flags [S], cksum 0xa394 (correct), seq 3118912807, win 8192, options [mss 146
0,nop,wscale 2,nop,nop,sackOK], length 0
00:00:00.000033 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
    10.68.35.250.http > 10.68.35.150.49163: Flags [S.], cksum 0x5c3e (incorrect -> 0x04fd), seq 2146094211, ack 311891280
8, win 29200, options [mss 1460,nop,nop,sackOK,nop,wscale 10], length 0
00:00:00.000763 IP (tos 0x0, ttl 128, id 527, offset 0, flags [DF], proto TCP (6), length 40)
    10.68.35.150.49163 > 10.68.35.250.http: Flags [.], cksum 0x7b79 (correct), seq 1, ack 1, win 16425, length 0
00:00:00.001479 IP (tos 0x0, ttl 64, id 528, offset 0, flags [DF], proto TCP (6), length 546)
    10.68.35.150.49163 > 10.68.35.250.http: Flags [P.], cksum 0xec98 (correct), seq 1:507, ack 1, win 16425, length 506
00:00:00.000040 IP (tos 0x0, ttl 64, id 8616, offset 0, flags [DF], proto TCP (6), length 40)
    10.68.35.250.http > 10.68.35.150.49163: Flags [.], cksum 0x5c32 (incorrect -> 0xb5ca), seq 1, ack 507, win 30, length 0
00:00:00.000770 IP (tos 0x0, ttl 64, id 8617, offset 0, flags [DF], proto TCP (6), length 250)
    10.68.35.250.http > 10.68.35.150.49163: Flags [P.], cksum 0x5d04 (incorrect -> 0xc03b), seq 1:211, ack 507, win 30, l
length 210
00:00:00.200401 IP (tos 0x0, ttl 64, id 8618, offset 0, flags [DF], proto TCP (6), length 250)
    10.68.35.250.http > 10.68.35.150.49163: Flags [P.], cksum 0x5d04 (incorrect -> 0xc03b), seq 1:211, ack 507, win 30, l
length 210
00:00:00.000803 IP (tos 0x0, ttl 128, id 529, offset 0, flags [DF], proto TCP (6), length 52)
    10.68.35.150.49163 > 10.68.35.250.http: Flags [.], cksum 0xa55a (correct), seq 507, ack 211, win 16372, options [nop,
nop,sack 1 {1:211}], length 0           "the quieter you become, the more you are able to hear"
00:00:04.804477 IP (tos 0x0, ttl 64, id 8619, offset 0, flags [DF], proto TCP (6), length 40)
    10.68.35.250.http > 10.68.35.150.49163: Flags [F.], cksum 0x5c32 (incorrect -> 0xb4f7), seq 211, ack 507, win 30, len
gth 0
00:00:00.000548 IP (tos 0x0, ttl 128, id 533, offset 0, flags [DF], proto TCP (6), length 40)

```

Not: Tcpdump aracının çıktısında, bayraklardaki “.” ifadesi ACK bayrağının aktif olduğunu belirtir.

TCP ve UDP Nedir



TCP/IP TCP (Transmission Control Protocol) ve IP (Internet Protocol) protokollerinin birleştirilmesiyle oluşturulan internet üzerindeki bir iletişim metodudur.

Bu metot sayesinde internete bağlanan tüm cihazlar birbirleri ile haberleşebilir. Bir ağa bağlanan bilgisayarlar veri iletmek ve almak için birbirleri arasında TCP/IP protokolü ile haberleşmektedir. Kısacası TCP/IP protokolü, bilgisayarlar arası veri iletişiminin kurallarını koyan bir iletişim protokollerini bütünüdür. Bilgisayarlar arası iletişim farklı protokol aileleri veya tipleri üzerinden gerçekleştirilir. Kullanım amacına göre ise bu protokoller birbirlerinden ayrılmaktadır.

TCP (Transmission Control Protocol) bilgisayarlar arasındaki iletişimin, küçük paketler hâlinde ve kayıpsız olarak gerçekleştirilmesini sağlayan bir protokoldür. Aslında TCP (Transmission Control Protocol) protokolünün en önemli özelliği kimlik doğrulaması yapması ve veriyi karşı tarafa gönderirken veya alırken verinin bütünlüğünü sağlamasıdır. Gelişmiş bilgisayar ağlarında ortaya çıkan kayıpları önlemek için TCP protokolü yazılmıştır. HTTP, HTTPS, POP3, SSH, SMTP, TELNET ve FTP gibi günlük hayatı sıkça kullandığımız protokollerin veri iletimi TCP vasıtasyyla yapılır.

UDP protokolüne göre yavaş ancak güvenli bir veri iletişimi sağlar. UDP (User Datagram Protocol) protokolünde ise verinin karşı bilgisayar tarafından alınıp alınmadığı kontrol edilmez ve veri iletişimi çok hızlı bir şekilde gönderilir.

TCP protokolü ilk olarak 1974 yılında A Protokol for Packet Network Intercommunication adı verilen bir makalede* duyurulmuştur. Veri bölünerek paketler halinde karşı tarafa iletilmesi sebebiyle paket anahtarlamalı olarak nitelendirilmektedir.

TCP (Transmission Control Protocol) Nasıl Çalışır?

TCP protokolünün çalışma mantığı üç başlıkta incelenebilir. Birinci aşamada hedefe bir bağlantı isteği gönderilir. İkinci aşamada bağlantının gerçekleştiği onaylanır ve veri transferi başlar. Üçüncü aşamada ise veri transferinin tamamlandığı taraflara iletilerek bağlantı sonlandırılır. Bu üç aşamanın gerçekleşmesi “State” işlemi olarak tanımlanır.

TCP Bağlantısı Nasıl Kurulur?

TCP'de bu üç ana aşamanın gerçekleşmesi için bazı ara durumlar da gerçekleşmektedir. Bu ara durumlar aşağıdaki gibi sıralanmaktadır.

LISTEN

Sunucu tarafından bir TCP bağlantı isteğinin beklenildiği durumdur. Dinleme modu olarak adlandırılır.

SYN-SENT

Karşı tarafa TCP bağlantısı isteği gönderildikten sonra karşı taraftan bağlantı isteğine cevap verilmesi beklenilen durum olarak adlandırılır.

SYN-RECEIVED

SYN bayrağı ile yapılan bağlantı isteği sunucunun SYN-ACK bayrağı ile cevap vermesi aşamasından sonraki bekleme durumu olarak adlandırılır.

ESTABLISHED

Bağlantı kurulduktan sonra gelen veri transferinin yapıldığı durumdur.

FIN-WAIT-1

Sunucu ve istemci tarafından bekleme durumudur.

FIN-WAIT-2

Karşı taraftan TCP bağlantısının bitirilme isteğinin bekleniği durumdur.

CLOSE-WAIT

Sunucu ve istemci tarafından bağlantı kapatma talebinin bekleniği durumudur.

CLOSING

Karşı tarafa bağlantının bitirilmesine dair bir ACK bayrağı gönderildikten sonra bağlantının bitmesini bekleme durumu olarak adlandırılır.

LAST-ACK

Sunucu ve istemci tarafında ACK bekleniği durumdur.

TIME-WAIT

Bekleme durumudur.

CLOSED

TCP bağlantısının tamamen bittiği durum olarak adlandırılır.

TCP bağlantısı kurulurken; yani iki bilgisayar birbiriyle TCP protokolü üzerinden bağlantı kurmak istediği sırada ile işlemler çalışmaya başlar:

1. X bilgisayarı Y bilgisayarına bir TCP SYN mesajı yollar.
2. Y bilgisayarı X bilgisayarının isteğini aldığına dair bir TCP SYN+ACK mesajı yollar.
3. X bilgisayarı Y bilgisayarına TCP ACK mesajı yollar.
4. Y bilgisayarı bir ACK "TCP connection is ESTABLISHED" mesajı alır.
- 5.

Üçlü el sıkışma adı verilen bu yöntem sonucunda TCP bağlantısı açılmış, süreç başarılı ve güvenli bir şekilde sağlanmış olur.

TCP Bağlantısının Aşamaları

Bir TCP bağlantısı yapılrken yukarıda anladığımız gibi üçlü el sıkışma adı verilen (3-Way Handshake) bir işlem gerçekleştirilmektedir. Bu işlem sırası aşağıdaki gibi belirtilmektedir:

6. İstemci, Sunucuya bir SYN paketi gönderir.
7. Sunucu bu pakete karşılık olarak SYN-ACK veri paketleriyle cevap verir.
8. Son aşamada İstemci bilgisayar, Sunucuya ACK mesajı gönderir ve ilk iletişim başlatılmış olur.

Eğer bu işlem sırasında İstemci karşı taraftaki Sunucunun dinlenmeyen (açık olmayan) bir portuna bağlantı isteği iletirse -ki bu işlem sırasında LISTEN modda olması gerekdir- Sunucudan yukarıda belirtmiş olduğumuz SYN-ACK paketi cevabı yerine RST-ACK cevap paketi gönderilir.

Bu noktada Sunucu bağlantıyı reddetmiş olur ve bağlantı kurulmaz. RST paketi “reset” olarak tanımlanır ve açık bir bağlantıyı kesmek için de kullanılır.

IP Nedir?

IP, Türkçe açılımı ve çevirisiyle internet protokolünün kısaltmasıdır. Bilgisayarların birbirleri ile iletişiminde en önemli nokta olan ağ adreslemede kullanılan düzendir. IP (internet protokolü), iki bilgisayar arasındaki paketlerin yönlendirilmesini sağlayan bir protokol olarak tanımlanır. Yönlendirme protokolü olarak tanımlanan IP, veri için gerekli olan yönlendirmenin kurallarını belirlemektedir. IP’de verinin niteliği önemli değildir ve veri içeriği ile ilgilenmeden bu protokol sadece gideceği adresi belirler.

IP (Internet Protocol) Nasıl Çalışır?

IP çalışma mantığında TCP veri paketinin izleyeceği yol belirlenir. Bu işlem yapılırken de TCP katmanından gelen veri paketine kendi SEGMENT başlığını ekler. Bu durumda ortaya datagram olmuş olur. IP (Internet Protocol), veriyi karşı tarafa yönlendirirken, alıcının bu veriyi kabul edeceğini veya etmeyeceği konusunda bir doğrulama yapmaz. Hata kontrolü bir üst katmanın işidir ve bu sayede IP kendi başına çalışabilen bir protokol olarak bilinir.

TCP/IP Katmanları Nelerdir?

TCP ve IP birleşerek TCP/IP protokol ailesini oluşturmaktadır. Bu sayede bilgisayarlar arasında birden fazla iletişim metodu kullanılabilir. Bu iletişim sırasında kullanılan TCP/IP katmanları ise aşağıdaki gibi belirtilmiştir.

TCP/IP Referans Modeli

4. Katman – Uygulama
3. Katman – Taşıma
2. Katman – İnternet
1. Katman – Ağ

Uygulama Katmanı: Uygulama katmanında farklı sunucular üzerindeki süreç ve uygulamalar arasındaki iletişim sağlanır. Bu iletişim sırasında ise HTTP, HTTPS, SSH, SMTP, TELNET ve FTP gibi protokoller kullanılmaktadır.

Taşıma Katmanı: Bir noktadan diğer noktaya veri akışını sağlayan katmandır. Bu katman üzerinde TCP ve UDP protokollerini kullanılmaktadır.

İnternet Katmanı: Router cihazları ile birbirlerine bağlanmış olan ağlar arasında verinin bir kaynaktan hedef bilgisayara kadar gerekli olan iletiminin sağlanması için kullanılır. Bu veri aktarımı sırasında kullanılan bilgiler internet katmanı ile transfer edilir.

Ağ Erişim Katmanı: Bu katmanda uç nokta ile ağ arasında yer alan bağlantı arabirimini kullanılır. Bilgisayar dili 0 ve 1'lerden oluşmaktadır ve bu katmandaki iletişim için veri paketleri 0 ve 1'lere dönüştürülerek taşınır.
Veri iletimi sırasında OSI Referans Modeline Göre aşağıdaki katmanlar kullanılır.

OSI Referans Modeline Göre Katmanlar

7. Katman – Uygulama
6. Katman – Sunum
5. Katman – Oturum
4. Katman – Taşıma
3. Katman – Ağ
2. Katman – Veri Bağlantısı
1. Katman – Fiziksel Bağlantı

TCP: UDP 'den daha yavaştır çünkü verinin karşı tarafa ulaşıp ulaşmadığını kontrol eder.

UDP Nedir?

Teknolojinin gelişmesi ile birlikte insanların daha önce duymadığı pek çok kavram ortaya çıkmıştır. Bu kavamlardan bir tanesi de yeni yeni duyulmaya başlanan UDP'dir. UDP'nin açılımı "User Datagram Protocol", Türkçe anlamı ile ise "Kullanıcı Veri Bloğu İletişim Kuralları" olmaktadır. TCP/IP adı verilen protokol takımları bulunmaktadır ve UDP bu protokollerden bir tanesidir. UDP iki katmanlı bir aktarım protokolüdür.

UDP: Ses ve video gönderiminde kullanılır. TCP'ye göre daha hızlıdır fakat güvenli değildir. Veri ismine datagram denilir. Datagramın segmentten farkı ise içerisinde sira numarasının bulunmamasıdır.

UDP Ne İşe Yarar?

UDP'nin temel işlevi verilerin gönderimini bağlantı kurulmaksızın gerçekleştirmektir. UDP protokolü yeni nesil bilgisayar ağlarında datagram modu oluşturabilmek için geliştirilmiştir. Böylelikle bilgisayarlarda paket anahtarlı bilgisayar iletişimi mümkün olabilmektedir. UDP kullanılmayan bilgisayarlarda sıkılıkla TCP adı verilen başka bir protokol kullanılmaktadır.

UDP ile veri gönderimi temel olarak az sayıda olmasına odaklanılarak oluşturulmuştur. Diğer protokoller ile kıyaslandığında az sayıda mesaj alışverişine hizmet etmektedir. Dikkat edilmesi gereken bir nokta ise gönderilen verilerin sürecidir. UDP çoğu protokolün aksine veriyi gönderdikten sonra ilettilip iletmediği ile ilgilenmez ve bu konuda kullanıcıya bilgi vermez.

Bu sebeple de UDP kullanıcılarına da tam bir güvenilirlik konusunda garanti vermemektedir. Verilerin aktarım sürecinde bilgi almadığı ve süreci takip etmediği için

daha hızlı bir şekilde aktarımı gerçekleştirir. Bu da UDP'yi aslında diğer protokollerden öne çıkan özelliktir. Özellikle hızı önem verenler UDP'yi kullanan kişilerdir. Buna ek olarak UDP 4 alandan oluşmaktadır. Bu alanların her birinin uzunluğu ise 16 bittir. Toplam 64 bit uzunlığında olan UDP 'nin güvenilirlik konusundaki sorunları ileriki yıllarda halledildiğinde kullanıcı sayısı da artacaktır.

Sonuç olarak TCP hızında daha yavaş olabilir ancak TCP protokolü daha hızlı. UDP protokolü üzerinde doğruluk ve güvenlik konusunda daha fazla seçenek sunmaktadır. UDP, ses veya video gibi verileri aktarmak için kullanışlıdır. UDP oyunlar için oldukça kullanışlıdır.

TCP'den Farkı Nelerdir?

Kullanıcılar hangi protokolü tercih edeceklerine karar vermek için mutlaka ayrıntılı bir şekilde araştırma yapmalıdır. Günümüzde en çok kullanılan protokoller UDP ve TCP'dir. UDP, WAN ağlarında veri aktarımında kullanılır. Ses ve görüntüler eş zamanlı aktarımını gerçekleştirebilir. UDP diğer protokollerin aksine kurulum ve akış kontrolü gerektirmediği için veri iletim hızı yüksektir.

UDP ve TCP'nin iletim yollarının aynı olduğunu düşünelim. UDP ile gerçekleştirilmiş bir gerçek zamanlı veri transferi ile TCP ile gerçekleştirilmiş veri transferinin servis kalitesi etkilendir. Bunun sebebi TCP'nin meydana getirdiği veri trafiginin yüksek olmasıdır. Böyle bir sorun yaşandığında UDP'nin servis kalitesi düşecektir.

Dikkat edilmesi gereken bir diğer nokta ise TCP ile UDP'nin bant genişlikleridir. TCP'nin bant genişliği daha fazla olduğu için daha sık tercih edilmektedir. UDP'nin ise bant genişliği daha azdır. TCP protokolünün tercih edilme sebeplerinden bir diğeri ise UDP protokolünden daha güvenilir olmasıdır. Örneğin TCP kullanılan bir cihazdan veri gönderimi gerçekleştirdiğinizde verinizin gidip gitmediğini kontrol edebilir ve bilgisine ulaşabilirsiniz.

UDP ise güvenilir olmayan protokol olarak nitelendirilmektedir. Kullanılan ağ üzerinden veriyi gönderdikten sonra gidip gitmediğinin bilgisine ulaşamazsınız. Bu durumda ise daha güvenli bir şekilde veri aktarımı gerçekleştirmek isteyen firmalar bunu kendi yöntemleri ile gerçekleştirmektedirler. TCP protokolü ile aktarım yaptığınızda verileriniz sıralı bir şekilde giderken UDP'de sıralı bir şekilde gitmez.

Buna ek olarak TCP ile kullanırsanız size kesintisiz bir bağlantı sunulur. Fakat UDP kullanımında ise yalnızca veri gönderme işlemi sırasında bağlantı kurulur ve gönderme işlemi tamamlandığında bağlantı kendiliğinden kapanır. Kısaca özetlemek gerekirse TCP protokolü size güvenliği garanti ederken UDP protokolü ise hızı garanti eder. Bu duruma dikkat ederek kendinize en uygun olanı seçebilirsiniz.

Encoding (Kodlama):

Buradaki amaç bilgiyi gizli tutmak değil, daha ziyade verilerin doğru bir biçimde tüketilmesini sağlamaktır. Kodlama, verileri halka açık bir şema kullanarak başka bir formata dönüştürür, böylece kolayca tersine çevrilebilir. Kodlama işlemindeki verilerin

geriye döndürülmesi için herhangi bir anahtar gerekmektedir. Sadece şifreleme için kullanılan algoritma ve ya veri tablosunun bilinmesi yeterlidir.

Kodlamaya örnek olarak, ASCII, Unicode, URL Kodlama, Base64 verilebilir.

Encryption (Şifreleme):

Şifrelemenin esas amacı, verilerin bir başka kullanıcıya gönderimi sırasında gizli tutulmasıdır. Örneğin sadece bir kişinin okuyup anlayabileceği bir mektup gönderimi veya internet üzerinden şifre, kimlik numarası, kredi kartı numarası gibi hassas verilerin gönderimi sırasında duruma bağlı olarak istemci-sunucu veya istemci-istemci arasında bir şifreleme kurulması gerekmektedir. Öztle amaç kullanılabilirlik den ziyade gizliliktir.

Şifrelemede veriler yalnızca belirli kullanıcıların şifreyi çözebileceği bir formata dönüştürülür. Şifreleme işleminin gerçekleştirilebilmesi için şifreli metin ile birlikte gizli tutulan bir anahtar kullanılır. Şifreyi çözmesi gereken kişi ise elindeki anahtarı kullanarak şifreyi düz metne çevirir.

Şifrelemeye örnek olarak AES, Blowfish, RSA verilebilir.

Hashing:

Hashing, veri bütünlüğünü sağlamak amacıyla kullanılmaktadır. Yani hashing deki asıl amaç bir şey değiştiğinde o şeyin değiştiğini anlayabilmemiz... Teknik olarak bir takım girdi alır ve sürekli aynı uzunlukta olacak çıktılar üretir. Bu çıktılar üretilirken dikkat edilmesi gereken özellikler şunlardır:

- Aynı girdi her zaman için aynı çıktıyı üretmelidir.
- Birden fazla girdi, asla aynı çıktıyı üretilmemelidir.
- Hash'ten ana veriye dönüş mümkün olmamalıdır.
- Verilen girdide yapılacak bir değişiklik, hashte büyük bir değişiklige yol açmalıdır.

Hashing, belirli bir verinin değişmediğine dair güçlü kanıtlar üretmek için kullanılır. Alıcı gönderilen mesajı açığında, gönderilen anahtar ile verinin değişmediğini teyit edebilir. Hashing işlemine örnek olarak: SHA-5, MD5 verilebilir.

Obfuscation (Gizleme):

Gizlemenin amacı kaynak kodda zafiyet bulmayı veya veriyi kopyalamayı zoraştırmak amacıyla herhangi bir verinin anlaşılmasıını zorlaştırmaktır. Böylece tersine mühendislik uygulandığında ürünü kopyalamak daha zor olmaktadır.

Gizlemenin güçlü bir şifreleme yöntemi olmadığı unutulmamalıdır. Kodlamada olduğu gibi verinin ilk baştaki haline ulaşım olasıdır. Ancak bu işlem manuel olduğundan oldukça zaman alacaktır.

Gizlemelarındaki bir diğer önemli detay ise gizlenecek şeyin ne kadar belirsiz hale getirileceği ile ilgilidir.

Örneğin bir bilgisayar kodunun anlaşılmasını zorlaştırmak istiyorsanız, Obfuscation işleminin ardından bilgisayarın bunu kolayca çözüldüğünden emin olmalısınız. Aksi takdirde uygulama çeşitli hatalar ile karşılaşacaktır.

Obfuscation işlemine örnek olarak javascript obfuscator, proguard verilebilir.

Özet olarak;

Encoding, veri kullanılabililığını korumak içindir. İçeriği herkes tersine çevrilebilir. Bu içeriği ham haline dönüştürme işleminde herhangi bir anahtar gerekmmez.

Encryption, verinin gizliliğini korumak içindir. İçeriğin ham haline dönüştürülebilmesi için anahtarın bilinmesi gerekmektedir.

Hashing, hash çıktısındaki değişikliklere bakarak içeriğin değişip değişmediğinin kontrolünü yapmak; veri bütünlüğünü sağlamak içindir.

Obfuscation, insanların bir veriyi anlamasını güçlendirmek için kullanılır. Genellikle tersine mühendislik işlemlerini zorlaştırmak amacıyla bilgisayar kodlarının karmaşıklaştırılmasında kullanılır.

Domain Nasıl Çalışır?

Domainler, internet üzerindeki web sitelerinin veya diğer çevrimiçi servislerin tanımlayıcılarıdır. Domainler, genellikle insanların kolayca hatırlayabileceği şekilde düzenlenmiş birer metin olarak görünürler (örneğin, "example.com"). Domain adları, IP adresleriyle ilişkilendirilir ve bu IP adresleri, web sunucularının fiziksel konumlarını belirtir.

ICANN (Internet Corporation for Assigned Names and Numbers)

İnternet Tahsisli Adlar ve Sayilar Kurumu), küresel internet alan adı sistemini ve kök DNS sunucularını yöneten, küresel bir karar alma ve koordinasyon kuruluşudur. ICANN, dünya genelindeki domain kayıt yetkilileri ve domain kayıt kurumlarıyla işbirliği yaparak, domain kayıtları, alan adı politikaları ve internet protokolü adres uzayı gibi internet kaynaklarının dağıtımını ve yönetimiyle ilgili kararları alır.

ICANN'in domainlerle olan bağlantısı şu şekillerde özetlenebilir:

1. **Domain Adı Kayıtları ve Akreditasyonu:** ICANN, domain kayıt hizmetlerini sağlayan kuruluşları akredite eder ve denetler. Bu, güvenilir ve düzenlenmiş bir domain kayıt süreci sağlamak için gereklidir.
2. **Alan Adı Kayıt Politikaları:** ICANN, domain kayıt politikalarını belirler ve yönetir. Bu politikalar, domain adlarının kullanımı, kayıt prosedürleri, sahiplik bilgileri gibi konuları kapsar.

3. **Üst Seviye Alan Adları (TLD'ler):** ICANN, üst seviye alan adları (TLD'ler) için yönetici kuruluştur. TLD'ler, .com, .org, .net gibi genel üst seviye alan adları ile ülke kodlu üst seviye alan adları (ccTLD'ler) gibi çeşitli türlerde olabilir.
4. **Root DNS Sunucuları:** ICANN, kök DNS sunucularını yönetir. Kök DNS sunucuları, internetin temel altyapısını oluşturur ve domain adlarının IP adreslerine çözümlenmesi için gerekli bilgileri sağlar.

Bu nedenle, ICANN, internet alan adı sistemini düzenleyen ve koordine eden bir kuruluş olarak, domainlerin düzenlenmiş ve güvenilir bir şekilde işlemesini sağlamak için kritik bir rol oynamaktadır.

Güvenlik duvarı nedir? Tanım ve açıklama

Güvenlik duvarı – Anlamı ve tanımı

Güvenlik duvarı, özel bir ağın içine, dışına yönelik veya özel ağın içindeki internet trafiğini kısıtlayan bir bilgisayar ağı güvenlik sistemidir.

Bu yazılım veya özel donanım-yazılım birimi, veri paketlerini seçici olarak engelleyerek veya izin vererek çalışır. Genellikle kötü niyetli etkinliklerin önlenmesine yardımcı olmayı ve özel bir ağın içinde veya dışında herhangi birinin yetkisiz web etkinliklerine karışmasını önlemeyi amaçlar.

Güvenlik duvarı nedir?

Güvenlik duvarları, özel bir ağda izin verilen ve yasaklanan web etkinliğinin hareketini yöneten çeşitli sınırlar veya ağ geçitleri olarak görülebilir. Terim, itfaiye yanğını söndürenе kadar yanının yayılmasını yavaşlatan fiziksel duvarlar kavramından gelmektedir. Buna karşılık, ağ güvenliği güvenlik duvarları, web trafiği yönetimi içindir — genellikle web tehditlerinin yayılmasını yavaşlatmayı amaçlar.

Güvenlik duvarları, web trafiğini yönlendirmek için 'tikanma noktaları' oluşturur ve bu noktalarda daha sonra bir dizi programlanmış parametre üzerinde gözden geçirilir ve buna göre hareket edilir. Bazı güvenlik duvarları, izin verilen veya engellenenlere atıfta bulunmak için denetim günlüklerindeki trafiği ve bağlantıları da izler.

Güvenlik duvarları tipik olarak özel bir ağın veya onun ana cihazlarının sınırlarını kapatmak için kullanılır. Bu nedenle güvenlik duvarları, daha geniş kullanıcı erişim kontrolü kategorisindeki bir güvenlik aracıdır. Bu engeller tipik olarak iki konumda kurulur: ağdaki özel bilgisayarlar veya kullanıcı bilgisayarları ve diğer uç noktaların kendileri (ana bilgisayarlar).

Güvenlik duvarları nasıl çalışır?

Bir güvenlik duvarı, hangi ağ trafiğinin geçmesine izin verildiğine ve hangi trafiğin tehlikeli kabul edildiğine karar verir. Temelde, iyi kötüden veya güveniliri

güvenilmeyenden ayırarak çalışır. Ancak ayrıntılara girmeden önce web tabanlı ağların yapısını anlamamız bu konuda bize yardımcı olur.

Güvenlik duvarları, özel ağları ve bunların içindeki ağ ana bilgisayarları olarak bilinen üç nokta cihazlarını güvence altına almak için tasarlanmıştır. Ağ ana bilgisayarları, ağdaki diğer ana bilgisayarlarla 'konuşan' cihazlardır. Dahili ağlar arasında, ayrıca harici ağlar arasında giden ve gelen verileri gönderir ve alırlar.

Bilgisayarlar ve diğer üç nokta cihazları, internete ve birbirlerine erişmek için ağları kullanır. Ancak internet, güvenlik ve gizlilik için 'alt ağlara' ayrılmıştır. Temel alt ağ segmentleri aşağıdaki gibidir:

1. Harici genel ağlar tipik olarak genel/küresel internete veya çeşitli ekstranetlere denir.
2. Dahili özel ağ, bir ev ağını, kurumsal intranetleri ve diğer 'kapalı' ağları tanımlar.
3. Çevre ağları, savunma kaleşi ana bilgisayarlarından oluşan sınır ağlarını detaylandırır harici bir saldırıyla karşı koymaya hazır, sağlamlaştırılmış güvenlikle ayrılmış bilgisayar ana makineleri. Dahili ve harici ağlar arasında güvenli bir arabellek olarak bunlar, dahili ağ tarafından sağlanan herhangi bir dışa dönük hizmeti (yani web, posta, FTP, VoIP, vb. için sunucular) barındırmak için de kullanılabilir.

Bunlar harici ağlardan daha güvenli, dahili ağlardan ise daha az güvenlidir. Bunlar, ev ağları gibi daha basit ağlarda her zaman bulunmaz, ancak genellikle kurumsal veya ulusal intranetlerde kullanılabilirler.

Tarama yönlendiricileri, onu böümlere ayırmak için bir ağ üzerine yerleştirilmiş özel ağ geçidi bilgisayarlarıdır. Ağ düzeyinde ev güvenlik duvarları olarak bilinirler. En yaygın iki segment modeli, ekranolana bilgisayar güvenlik duvarı ve ekranolalt ağ güvenlik duvarıdır:

- Ekranolana bilgisayar güvenlik duvarları, harici ve dahili ağlar arasında tek bir tarama yönlendiricisi kullanır. Bu ağlar, bu modelin iki alt ağıdır.
- Ekranolalt ağ güvenlik duvarları bir harici ve çevre ağı arasında erişim yönlendiricisi olarak bilinen ve diğer çevre ve dahili ağ arasındaki kısma yönlendiricisi olarak bilinen iki tarama yönlendiricisi kullanır. Bu, sırasıyla üç alt ağ oluşturur.

Hem ağ çevresi hem de ana makinelerin kendileri bir güvenlik duvarı barındırabilir. Bunu gerçekleştirmek için, tek bir bilgisayar ile özel bir ağa olan bağlantısı arasına yerleştirilir.

- Ağ güvenlik duvarları, harici ağlar ve dahili özel ağlar arasında bir veya daha fazla güvenlik duvarının uygulanmasını içerir. Bunlar, küresel internet gibi harici genel ağları ev Wi-Fi ağları, kurumsal intranetler veya ulusal intranetler gibi dahili ağlardan ayırarak gelen ve giden ağ trafiğini düzenler. Ağ güvenlik duvarları, aşağıdaki araç türlerinden herhangi biri biçiminde olabilir: özel donanım, yazılım ve sanal.
- Ana bilgisayar güvenlik duvarları veya 'yazılım güvenlik duvarları', ağındaki cihazlar arasında bir bariyer olarak bireysel kullanıcı cihazlarında ve diğer özel ağ üç noktalarında güvenlik duvarlarının kullanılmasını içerir. Bu cihazlar veya ana bilgisayarlar, belirli bilgisayar uygulamalarına gelen ve giden trafiğin

özelleştirilmiş düzenlemesini alır. Ana bilgisayar güvenlik duvarları, yerel cihazlarda bir işletim sistemi hizmeti veya bir uç nokta güvenlik uygulaması olarak çalışabilir. Ana bilgisayar güvenlik duvarları, HTTP ve diğer ağ protokollerine dayalı olarak filtreleme yaparak web trafiğinin derinliklerine dalabilir ve makinenize hangi içeriğin nereden geldiği yerine hangi içeriğin geldiğinin yönetilmesine olanak tanır.

Bir ağ güvenlik duvarı, geniş bir bağlantı kapsamına karşı yapılandırma gerektirirken, bir ana bilgisayar güvenlik duvarı, her makinenin ihtiyaçlarına uyacak şekilde uyarlanabilir. Bununla birlikte, ana bilgisayar güvenlik duvarlarının özelleştirilmesi daha fazla çaba gerektirir; bu, ağ tabanlı güvenlik duvarlarının kapsamlı bir kontrol çözümü için ideal olduğu anlamına gelir. Ancak her iki güvenlik duvarının aynı anda her iki yerde kullanılması çok katmanlı bir güvenlik sistemi için idealdir.

Bir güvenlik duvarı aracılığıyla trafiği filtrelemek, denenen bağlantılarla izin vermek ve bunları reddetmek için önceden ayarlanmış veya dinamik olarak öğrenilmiş kuralları kullanır. Bu kurallar, bir güvenlik duvarının özel ağınız ve özel bilgisayar cihazlarınız üzerinden web trafiği akışını düzenlemeye şeklini oluşturur. Türü ne olursa olsun, tüm güvenlik duvarları aşağıdakilerin bazı kombinasyonlarına göre filtre uygulayabilir:

- Kaynak: Bağlantı girişiminin yapıldığı yer.
- Hedef: Bağlantı girişiminde bulunulan yer.
- İçindekiler: Denenen bir bağlantının göndermeye çalıştığı şey.
- Paket protokolleri: Denenen bir bağlantı, mesajını taşımak için hangi 'dili' konuşuyor. Ana bilgisayarların birbirleriyle 'konuşmak' için kullandıkları ağ protokolleri arasında, TCP/IP protokolleri öncelikle internet üzerinden ve intranet/alt ağlar içinde iletişim kurmak için kullanılır.
- Uygulama protokolleri: Ortak protokoller arasında HTTP, Telnet, FTP, DNS ve SSH bulunur.

Kaynak ve hedef, internet protokolü (IP) adresleri ve bağlantı noktaları ile iletilir. IP adresleri, her ana bilgisayar için benzersiz cihaz adlarıdır. Bağlantı noktaları, daha büyük bir binadaki ofis odalarına benzer şekilde, herhangi bir kaynak ve hedef ana bilgisayar cihazının bir alt düzeyidir. Bağlantı noktalarına genellikle belirli amaçlar atanır; bu nedenle olağandışı bağlantı noktaları veya devre dışı bırakılmış bağlantı noktaları kullanan belirli protokoller ve IP adresleri endişe kaynağı olabilir.

Bu tanımlayıcıları kullanarak, bir güvenlik duvari, bağlantı kurmaya çalışan bir veri paketinin -sessizce mi yoksa gönderene bir hata yanıtıyla mı- yok sayılacağına veya iletileceğine karar verebilir.

Güvenlik duvarı türleri

Farklı güvenlik duvari türleri, çeşitli filtreleme yöntemlerini içerir. Her tür, önceki nesil güvenlik duvarlarını aşmak için geliştirilmiş olsa da, çekirdek teknolojinin çoğu nesiller arasında geçmiştir.

Güvenlik duvari türleri, aşağıdakilere olan yaklaşımlarına göre ayırt edilir:

1. Bağlantı izleme
2. Filtreleme kuralları
3. Denetim günlükleri

Her tür, standartlaştırılmış iletişim modelinin, Açık Sistemler Ara Bağlantı modelinin (OSI) farklı bir düzeyinde çalışır. Bu model, her bir güvenlik duvarının bağlantılarla nasıl etkileşime girdiğine dair daha iyi bir görsel sağlar.

Statik Paket Filtreleme Güvenlik Duvarı

Durumsuz denetim güvenlik duvarları olarak da bilinen statik paketfiltreleme güvenlik duvarları, OSI ağ katmanında (katman 3) çalışır. Bunlar, bir ağ üzerinden gönderilen tüm bireysel veri paketlerini nereden geldiklerine ve nereye gitmeye çalışıklarına göre kontrol ederek temel filtreleme sunar. Özellikle, daha önce kabul edilen bağlantılar izlenmez. Bu, gönderilen her veri paketiyle her bağlantının yeniden onaylanması gerektiği anlamına gelir.

Filtreleme, IP adreslerine, bağlantı noktalarına ve paket protokollerine dayanır. Bu güvenlik duvarları en azından iki ağızın izinsiz olarak doğrudan bağlanması engeller.

Filtreleme kuralları, manuel olarak oluşturulan bir erişim kontrol listesine göre belirlenir. Bunlar çok katıdır ve ağ kullanılabilirliğinden ödün vermeden istenmeyen trafiği uygun şekilde kapatmak zordur. Statik filtreleme, sürekli manuel revizyonun etkin bir şekilde kullanılmasını gerektirir. Bu, küçük ağlarda yönetilebilir ancak daha büyük ağlarda hızla zorlaşabilir.

Uygulama protokollerini okuyamama, bir paket içinde teslim edilen bir mesajın içeriğinin okunamayacağı anlamına gelir. İçeriği okumadan, paket filtreleyen güvenlik duvarları sınırlı bir koruma kalitesine sahiptir.

Devre Düzeyinde Ağ Geçidi Güvenlik Duvarı

Devre düzeyindeki ağ geçitleri, oturum düzeyinde çalışır (katman 5). Bu güvenlik duvarları, denenen bir bağlantıda işlevsel paketleri kontrol eder ve — iyi çalışıyorsa — iki ağ arasında kalıcı bir açık bağlantıya izin verir. Güvenlik duvari, bu gerçekleştikten sonra bağlantıyı denetlemeyi durdurur.

Bağlantılara yaklaşımının yanı sıra, devre düzeyindeki ağ geçidi, proxy güvenlik duvarlarına benzeyebilir.

Devam eden izlenmeyen bağlantı tehliklidir; çünkü meşru araçlar bağlantıyı açabilir ve daha sonra kötü niyetli bir kişinin kesintisiz olarak girmesine izin verebilir.

Durum Denetimi Güvenlik Duvarı

Dinamik paketfiltreleme güvenlik duvarları olarak da adlandırılan durum denetimi güvenlik duvarları, devam eden bağlantıları izleme ve geçmiş bağlantıları hatırlama yetenekleri bakımından statik filtrelemeden benzersizdir. Bunlar, taşıma katmanı (katman 4) üzerinde çalışarak başladı, ancak günümüzde bu güvenlik duvarları, uygulama katmanı (katman 7) dahil olmak üzere birçok katmanı izleyebiliyor.

Statik filtreleme güvenlik duvarı gibi, durum denetleyici güvenlik duvarları da, belirli paket protokolleri, IP adresleri veya bağlantı noktaları gibi teknik özelliklere dayalı olarak trafiğe

izin verir veya trafiği engeller. Ancak, bu güvenlik duvarları ayrıca bir durum tablosu kullanarak bağlantıların durumunu benzersiz bir şekilde izler ve filtreler.

Bu güvenlik duvarı, tarama yönlendiricisi tarafından durum tablosunda günlüğe kaydedilen geçmiş bağlantı olaylarına dayalı olarak filtreleme kurallarını günceller.

Genel olarak, filtreleme kararları genellikle bilgisayar ve güvenlik duvarını ayarlarken yöneticinin kurallarını temel alır. Ancak durum tablosu, bu dinamik güvenlik duvarlarının 'öğrendiği' önceki etkileşimlere dayanarak kendi kararlarını vermelerine izin verir. Örneğin, geçmişte kesintilere neden olmuş trafik türleri gelecekte filtrelenir. Durum denetiminin esnekliği, onu mevcut en yaygın kalkan türlerinden biri olarak sağlamıştır.

Proxy Güvenlik Duvari

Uygulama düzeyinde güvenlik duvarları (katman 7) olarak da bilinen Proxy Güvenlik Duvarları, uygulama protokollerini okuma ve filtreleme konusunda benzersizdir. Bunlar, uygulama düzeyinde incelemeyi veya 'derin paket incelemesini (DPI)' ve durum denetimini birleştirir.

Proxy güvenlik duvarları, gerçek bir fiziksel engelle en yakın koruma biçimidir. Diğer güvenlik duvarlarından farklı olarak, harici ağlar ve dahili ana bilgisayarlar arasında, her ağ için bir temsilci (veya 'proxy') olmak üzere iki ek ana bilgisayar görevi görür.

Filtreleme, paket tabanlı güvenlik duvarlarında olduğu gibi yalnızca IP adresleri, bağlantı noktaları ve temel paket protokolleri (UDP, ICMP) yerine uygulama düzeyindeki verilere dayanır. FTP, HTTP, DNS ve diğer protokollerini okumak ve anlamak, birçok farklı veri özelliği için daha derinlemesine araştırma ve çapraz filtreleme sağlar.

Tipki kapıda bekleyen bir koruma gibi gelen verilere bakar ve değerlendirme yapar. Bir sorun algılanmazsa, verilerin geçerek kullanıcıya ulaşmasına izin verilir.

Bu tür bir ciddi güvenlik önleminin olumsuz tarafı, bazen gelen verilerden tehdit olmayanları da engellemesi ve bunun da işlevsel gecikmeye neden olmasıdır.

Yeni Nesil Güvenlik Duvari (NGFW)

Gelişmekte olan tehditler devamlı şekilde daha köklü çözümler gerektiriyor ve yeni nesil güvenlik duvarları, geleneksel bir güvenlik duvarının özelliklerini ağ izinsiz giriş engellemesi sistemleriyle birleştirerek bu sorunu kontrol altında tutuyor.

Tehdide özel yeni nesil güvenlik duvarları, gelişmiş kötü amaçlı yazılım gibi belirli tehlikeleri daha detaylı olarak incelemek ve tespit etmek üzere tasarlanmıştır. Daha sık biçimde işletmeler ve gelişmiş ağlar tarafından kullanılan bu güvenlik duvarları, tehlikeleri filtrelemek için bütünsel bir çözüm sağlar.

Hibrit Güvenlik Duvari

Adından da anlaşılacağı gibi, hibrit güvenlik duvarları, tek bir özel ağda iki veya daha fazla güvenlik duvarı türü kullanır.

Ağ İletişim Protokollerı ve Portlar

Ağ üzerinde birden fazla bilgisayar arasında iletişim kurulurken birçok protokol üzerinden bilgi alışverişi yapılır. Farklı amaçlar için farklı ağ iletişim protokol türleri bulunmaktadır. Bu ağ iletişimini sağlayan farklı iletişim türlerine protokol ağ iletişim protokolü adı verilir. İletişim protokolü veya ağ protokolü olarak adı geçen bu metodlar, iki ya da daha fazla bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye, belirlenmiş kurallar altında iletişim kurulmasına yarayan, kabul edilmiş standartlar dizisidir.

Bir nevi bilgisayarların veya elektronik cihazların birbirleri arasında konuşmak, veri transfer etmek amacıyla oluşturulmuş dil denilebilir. Kısacası iki sistem arasında iletişim için kullanılan dili, türünü ve alfabetesini belirler. Ağ üzerinde “iletim dili” kelimesi yerine “iletim protokolü” şeklinde tanımlama yapılmasının sebebi ise, bilgisayarlar icat edildiğinde bu kelimenin hali hazırlada bilgisayar dili için kullanılıyordu. Çünkü birçok iletişim metodunda tek bir dil yerine birden fazla bilgisayar protokolü (dili) kullanılmaktadır. Her protokolün belirli bir amacı vardır ve normalde belirli bir bağlantı noktası üzerinden çalışır.

Ağ İletişim Protokollerı Nelerdir?

Elektronik sistemler, ağ iletişimini için tek bir protokol kullanmazlar. Bunun yerine, birçok protokol birleştirilerek bir protokol ailesi üzerinden iletişim kurulur.

Aşağıdaki tablo, bilgisayarlar veya cihazlar arası kullanılan en önemli protokollerden bazlarını listelemektedir.

Protokol	Kullanım Amacı	Port
FTP (Dosya Aktarım Protokolü)	Bilgisayarlar arasında dosya aktarmak için kullanılır.	20,21
SSH (Güvenli Kabuk Sistemi)	Dosyaları aktarmanın ve bir sistemde uzaktan oturum açarak yönetmenin güvenli bir yoludur.	22
Telnet (Uzak Erişim)	Bir sisteme uzaktan giriş yapmak için kullanılır.	23
SMTP (Basit Posta Aktarım Protokolü)	E-posta göndermek için kullanılır.	25
DNS (Alan Adı Sistemi)	URL'leri IP adreslerine çevirmek için kullanılır.	53
TFTP (Güvensiz Dosya Aktarımı)	Hızlı ancak daha az güvenilir FTP sunucusu için kullanılır.	69
HTTP (Metin Aktarım Protokolü)	Web sayfalarını görüntülemek için kullanılır.	80
POP3 (E-posta İletişim Protokolü v3)	E-postayı almak için kullanılır.	110
NNTP (Ağ Haber Aktarım Protokolü)	Ağ haberleri grubu için kullanılır.	119

NetBIOS	Yerel ağdaki sistemleri isimlendirmek için kullanılan çok eski bir protokol	137, 138, 139
IRC (İnternet Sohbetleri)	Sohbet odası için kullanılır.	194
HTTPS (Güvenli Metin Aktarım Protokolü)	Şifrelenmiş olarak web sayfası görüntüleme protokolüdür. HTTP + (SSL / TLS)	443
SMB (Sunucu mesajları)	Microsoft Active Directory tarafından kullanılır.	445
ICMP (İnternet Kontrol Protokolü)	Hata mesajları, bilgi ve kontrol mesajları içeren basit paketler için kullanılır .	–

Bu listenin dışında yüzlerce daha farklı protokolün bulunduğu da hatırlatmak isteriz. Tüm bu protokoller, TCP / IP (İletim Kontrol Protokoli / İnternet Protokoli) olarak adlandırılan bir protokol grubunun parçasıdır. Siber güvenlik dünyasında bu protokoller ve portlar hakkında geniş bilgiye sahip olmanız gerektiğini de hatırlatmak isteriz. Bir siber güvenlik uzmanı sizin testi gerçekleştirirken, ağ iletişimini ve portların mantığını iyice kavramış ve tecrübe edinmiş olmak zorundadır.

Ağ iletişiminde en önemli nokta iletişimin paketler üzerinden gerçekleşmesi ve bu paketlerin, gerçekleşen iletişim türüne bağlı olarak belirli protokollere göre iletilmesidir.

Portlar ve Kullanımları

Port denildiğinde akla ilk olarak bilgisayarların arkasındaki veya anakart üzerinde olan USB, seri veya benzeri bağlantı noktaları akla gelebilir. Ancak ağ iletişiminde bahsettiğimiz portlar bilgisayarların çıkış / giriş yuvaları değildir! Bunu hatırlatarak devam edelim. Portlar ağ iletişiminde bir bağlantı noktası veya bir tanıtıcı noktasıdır. Belirli bir iletişim yolu için sayısal bir gösterimi (21, 22, 80, 443...) bulunur.

Kullanılan bağlantı noktasından bağımsız olarak, tüm ağ iletişimleri NIC (ethernet, wifi gibi) üzerindeki bağlantı aracılığıyla bilgisayarınıza gelir. Bir bağlantı noktasını TV'nizdeki bir kanal olarak düşünübilirsiniz. Muhtemelen televizyonunuza gelen bir uydu kablonuz bulunur. Ancak tek bir kablo üzerinden birçok kanalı izleyebilirsiniz. Kanal numaralarını port olarak düşünüp, her kanalı da bir protokol gibi varsayılabılır. Bilgisayarınıza gelen kablo ağ iletişimini sağlar. Aynı zamanda bu kablo üzerinden (veyahut Wifi) birçok farklı bağlantı noktası kullanabilir ve birçok farklı yöntemle iletişim kurabilirisiniz.

KAYNAKÇA

1. KASPERSKY. “Güvenlik duvari nedir? Tanım ve açıklama”,
<https://www.kaspersky.com.tr/resource-center/definitions/firewall>.
2. TIMUS. “Firewall nedir? Nasıl Çalışır? Türleri nelerdir?”,
<https://berqnet.com/blog/firewall-nedir>.
3. KERNEL BLOG. “Hashing vs encryption vs encoding vs obfuscation”,
<https://kernelblog.org/2021/02/hashing-vs-encryption-vs-encoding-vs-obfuscation/>.
4. TURKNET. “UDP User Datagram Protocol nedir?”,
<https://turk.net/blog/udp-user-datagram-protocol-nedir/>
5. TIMUS. “TCP/IP Nedir? Nasıl Çalışır?”,
<https://berqnet.com/blog/tcp-ip>
6. KAREL. “TCP ve UDP arasındaki farklar nedir?”,
<https://www.karel.com.tr/bilgi/tcp-ve-udp-arasindaki-farklar-nedir>.
7. SİBERPORTAL. “TCP üçlü el sıkışma”, <https://www.siberportal.org/yellow-team/constructing-network-environment/tcp-three-way-handshake/>.
8. PRİVİA. “Ağ iletişim protokollerı ve portları”,
<https://www.priviassecurity.com/ag-iletisim-protokoller-ve-portlar/>.
9. GAİS. “ARP Poisoning”,
<https://www.gaissecurity.com/blog/arp-poisoning>.
10. İTÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI. “OSI Katmanları”
<https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1>
11. MORADAM. “CHMOD 777 Nedir?”,
<https://www.moradam.com/20180211207214/chmod-777-nedir>.
12. BEYAZ. “Dos ve DDos Nedir?”,
https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html.
13. ZEO. “HTTP Durum Kodları Rehberi”,
<https://zeo.org/tr/kaynaklar/blog/http-durum-kodlari-rehberi>.
14. GOANYWHERE. “FTP, SFTP VE FTPS Nedir? Farkları Nelerdir?”,
<https://www.goanywhereturkiye.com/ftp-sftp-ve-ftps-nedir-farklari-nelerdir>.
15. MEDIUM. “Simetrik ve Asimetrik Şifreleme Algoritmaları”,
<https://medium.com/@hicranozkan/simetrik-ve-asimetrik-anahtarlar%C4%B1-%C5%9Fifreleme-algoritmalar%C4%B1-a60a4e0eb079>
16. TURKNET. “IPS ve IDS Nedir? Nasıl Çalışır?”,
<https://turk.net/blog/ips-ve-ids-nedir-nasil-calisir>

- 17.MEDIUM. “Parolalar veri tabanlarında nasıl saklanır? ”,
<https://medium.com/@gokhansengun/parolalar-veri-tabanlar%C4%B1nda-g%C3%BCvenli-olarak-nas%C4%B1l-saklan%C4%B1r-70c5df892d3e>
- 18.BEYAZ. “OWASP Nedir?”,
https://www.beyaz.net/tr/guvenlik/makaleler/owasp_nedir.html.
- 19.DIGIIST. “SHA ve AES Şifrelemesi arasındaki fark”,
<https://tur.digiist.com/windows/the-difference-between-sha-aes-encryption-106015.html>
- 20.MESUTPEK. “Şifreleme Çeşitleri Nelerdir”,
<https://mesutpek.com.tr/sifreleme-cesitleri-nelerdir>.