***AÇIK KAYNAK ARAÇLAR İLE***

***AĞ GÜVENLİĞİ DERSİ***

***ÖDEVİ RAPORU***

***12/12/2023***

***Karadeniz Teknik Üniversitesi***

***Bilgisayar Mühendisliği Bölümü***

***Raporu Hazırlayan:***

***İsim: Arif Kaan BİTGİN***

***Numara: 402514***

***Proje Github Linki: https://github.com/kaanbtgn/Odev***

***Güvenlik Duvarı Nedir ve Önemi***

Güvenlik duvarı, bir bilgisayar ağının giriş ve çıkışlarını kontrol eden, yetkisiz erişimleri engelleyen bir güvenlik sistemidir. Güvenlik duvarları, bir ağın dış dünyayla olan bağlantısını filtreleyerek, kötü amaçlı yazılımların, virüslerin, spam'lerin ve diğer zararlı içeriklerin ağın içine girmesini önler.

Güvenlik duvarları, bir ağın güvenliğini sağlamada önemli bir rol oynar. İnternet, bilgi hırsızlığı, siber saldırılar ve diğer güvenlik tehditleri açısından riskli bir ortamdır. Güvenlik duvarları, bu tehditlere karşı bir ilk savunma hattı görevi görür ve ağların ve verilerin korunmasına yardımcı olur.

Güvenlik duvarları, iki temel kategoriye ayrılır: yazılım güvenlik duvarları ve donanım güvenlik duvarları. Yazılım güvenlik duvarları, bir bilgisayarın işletim sistemiyle birlikte gelen veya ayrı olarak yüklenebilen yazılımlardır. Donanım güvenlik duvarları ise, özel olarak güvenlik duvarı işlevi gören fiziksel cihazlardır.

Güvenlik duvarları, çeşitli filtreleme yöntemleri kullanarak yetkisiz erişimleri engeller. Bu filtreleme yöntemleri arasında port filtreleme, protokol filtreleme, izin tabanlı filtreleme ve akıllı filtreleme yer alır.

**Port Filtreleme**

Port filtreleme, bir güvenlik duvarının kullandığı en temel filtreleme yöntemlerinden biridir. Bu yöntemde, güvenlik duvarı paketlerin geldiği ve gittiği portları kontrol eder. Örneğin, bir ağ yöneticisi, yalnızca web sitelerinin kullandığı 80 numaralı portu açık tutabilir. Bu durumda, güvenlik duvarı yalnızca 80 numaralı porttan gelen ve giden trafiği izin verecektir.

Port filtreleme, basit ve etkili bir filtreleme yöntemidir. Ancak, bazı dezavantajları da vardır. Örneğin, güvenlik duvarı yalnızca açık portları kontrol eder. Bu nedenle, güvenlik duvarının arkasındaki bir bilgisayar, açık olmayan bir portu kullanarak ağdaki diğer bilgisayarlara erişebilir.

**Protokol Filtreleme**

Protokol filtreleme, port filtrelemesine benzer bir filtreleme yöntemidir. Bu yöntemde, güvenlik duvarı paketlerin kullandığı protokolleri kontrol eder. Örneğin, bir ağ yöneticisi, yalnızca web sitelerinin kullandığı HTTP protokolünü açık tutabilir. Bu durumda, güvenlik duvarı yalnızca HTTP protokolünü kullanan trafiği izin verecektir.

Protokol filtreleme, port filtrelemesine benzer avantajlara ve dezavantajlara sahiptir.

**İzin Tabanlı Filtreleme**

İzin tabanlı filtreleme, güvenlik duvarının kullandığı en karmaşık filtreleme yöntemlerinden biridir. Bu yöntemde, güvenlik duvarı, belirli kaynakların yalnızca belirli kullanıcılara erişmesine izin veren kurallar kümesi kullanır. Örneğin, bir ağ yöneticisi, yalnızca belirli kullanıcıların belirli bir web sitesine erişmesine izin verebilir. Bu durumda, güvenlik duvarı bu web sitesine erişmeye çalışan diğer kullanıcıları engelleyecektir.

İzin tabanlı filtreleme, en etkili filtreleme yöntemlerinden biridir. Ancak, bu yöntemin karmaşıklığı nedeniyle, doğru bir şekilde yapılandırılması zor olabilir.

**Akıllı Filtreleme**

Akıllı filtreleme, port filtreleme, protokol filtreleme ve izin tabanlı filtrelemeyi birleştiren bir filtreleme yöntemidir. Bu yöntemde, güvenlik duvarı, paketlerin içeriğini ve amacını analiz ederek, daha doğru bir şekilde filtreleme yapabilir. Örneğin, bir ağ yöneticisi, yalnızca belirli türde verileri içeren paketlerin geçmesine izin verebilir.

Akıllı filtreleme, en etkili filtreleme yöntemlerinden biridir. Ancak, bu yöntemin karmaşıklığı nedeniyle, doğru bir şekilde yapılandırılması zor olabilir.

**Güvenlik Duvarı Türleri**

Güvenlik duvarları, iki temel kategoriye ayrılır: yazılım güvenlik duvarları ve donanım güvenlik duvarları.

**Yazılım Güvenlik Duvarları**

Yazılım güvenlik duvarları, bir bilgisayarın işletim sistemiyle birlikte gelen veya ayrı olarak yüklenebilen yazılımlardır. Yazılım güvenlik duvarları, genellikle kişisel bilgisayarlar ve küçük işletmeler için kullanılır.

Yazılım güvenlik duvarlarının avantajları şunlardır:

* Genellikle ücretsiz veya düşük maliyetlidir.
* Kurulumu ve kullanımı kolaydır.
* Ağ trafiğini analiz etmek için gelişmiş özellikler içerebilir.

Yazılım güvenlik duvarlarının dezavantajları şunlardır:

* Performansı etkileyebilir.
* Ağın tümünü korumak için birden fazla yazılım güvenlik duvarı kurulması gerekebilir.

**Donanım Güvenlik Duvarları**

Donanım güvenlik duvarları, özel olarak güvenlik duvarı işlevi gören fiziksel cihazlardır. Donanım güvenlik duvarları, genellikle büyük işletmeler ve kurumlar için kullanılır.

Donanım güvenlik duvarlarının avantajları şunlardır:

* Yüksek performans sağlar.
* Ağın tümünü tek bir cihazla koruyabilir.
* Gelişmiş güvenlik özellikleri sunar.

Donanım güvenlik duvarlarının dezavantajları şunlardır:

* Daha pahalıdır.
* Kurulumu ve kullanımı daha zordur.

**Güvenlik Duvarı Seçimi**

Bir güvenlik duvarı seçerken, aşağıdaki faktörleri göz önünde bulundurmak gerekir:

* Ağın boyutu ve karmaşıklığı
* Ağın ihtiyaçları
* Bütçe

Küçük bir işletme için, yazılım güvenlik duvarı yeterli olabilir. Ancak, büyük bir işletme veya kurum için, donanım güvenlik duvarı daha iyi bir seçenek olabilir.

Güvenlik duvarı seçerken, aşağıdaki güvenlik özelliklerine dikkat etmek önemlidir:

* Port filtreleme
* Protokol filtreleme
* İzin tabanlı filtreleme
* Akıllı filtreleme
* Saldırı tespiti ve önleme (IDS/IPS)
* VPN desteği
* Gelişmiş güvenlik özellikleri

Güvenlik duvarı, bir ağın güvenliğini sağlamada önemli bir rol oynar. Ancak, tek başına güvenlik sağlayamaz. Güvenlik duvarlarının etkinliğini artırmak için, diğer güvenlik önlemleri ile birlikte kullanılması önemlidir.

***IDS/IPS'nin Önemi***

Saldırı tespiti ve önleme (IDS/IPS), bir ağın güvenlik durumunu izlemek ve olası saldırıları tespit etmek ve önlemek için kullanılan bir güvenlik teknolojisidir. IDS/IPS sistemleri, ağ trafiğini analiz ederek, kötü amaçlı yazılımlar, virüsler, spam'ler ve diğer zararlı içerikler gibi tehditleri tespit eder.

IDS/IPS sistemleri, bir ağın güvenliğini sağlamada önemli bir rol oynar. IDS/IPS sistemleri, aşağıdakiler de dahil olmak üzere çeşitli şekillerde bir ağı koruyabilir:

* Saldırı tespiti ve bildirimi: IDS/IPS sistemleri, bir saldırı tespit edildiğinde yöneticilere bir uyarı göndererek, yöneticilerin saldırıyı önlemek veya azaltmak için adımlar atmasını sağlar.
* Saldırı önleme: Bazı IDS/IPS sistemleri, saldırıları otomatik olarak önleyebilir. Bu, saldırının ağa zarar vermesini önlemeye yardımcı olur.
* Durum izleme: IDS/IPS sistemleri, ağ trafiğini izleyerek, ağdaki olağandışı aktiviteleri tespit edebilir. Bu, yöneticilerin potansiyel tehditleri belirlemesine yardımcı olabilir.

**IDS/IPS Sistemlerinin Çeşitleri**

IDS/IPS sistemleri, iki temel kategoriye ayrılır:

* Gerçek zamanlı IDS/IPS: Gerçek zamanlı IDS/IPS sistemleri, ağ trafiğini gerçek zamanlı olarak analiz eder. Bu, saldırıların daha hızlı tespit edilmesini sağlar.

Gerçek zamanlı IDS/IPS sistemleri, ağ trafiğini sürekli olarak analiz eder. Bu, saldırıların mümkün olan en kısa sürede tespit edilmesini sağlar. Gerçek zamanlı IDS/IPS sistemleri, genellikle ağdaki tüm trafik için kullanılır. Bu, saldırıların tüm ağda tespit edilmesini sağlar.

**Gerçek zamanlı IDS/IPS sistemlerinin bazı avantajları şunlardır:**

* Saldırılar daha hızlı tespit edilir.
* Saldırıların yayılmasını önlemek için daha fazla zaman vardır.

**Gerçek zamanlı IDS/IPS sistemlerinin bazı dezavantajları şunlardır:**

* Daha fazla kaynak kullanır.
* Daha karmaşıktır.
* Yedek IDS/IPS: Yedek IDS/IPS sistemleri, ağ trafiğini daha sonra analiz eder. Bu, daha fazla veri analizine izin verir, ancak saldırıların tespit edilmesini daha yavaş yapabilir.

Yedek IDS/IPS sistemleri, genellikle ağdaki belirli trafik için kullanılır. Bu, belirli tehditleri tespit etmek için daha fazla uzmanlık sağlar. Yedek IDS/IPS sistemleri, genellikle gerçek zamanlı IDS/IPS sistemleriyle birlikte kullanılır. Bu, saldırıların daha hızlı ve daha doğru bir şekilde tespit edilmesini sağlar.

**Yedek IDS/IPS sistemlerinin bazı avantajları şunlardır:**

* Daha fazla veri analizine izin verir.
* Daha az kaynak kullanır.

**Yedek IDS/IPS sistemlerinin bazı dezavantajları şunlardır:**

* Saldırılar daha yavaş tespit edilir.
* Saldırıların yayılmasını önlemek için daha az zaman vardır.

**IDS/IPS Sistemlerinin Seçimi**

Bir IDS/IPS sistemi seçerken, aşağıdaki faktörleri göz önünde bulundurmak gerekir:

* Ağ boyutu ve karmaşıklığı: Büyük bir ağ için, daha gelişmiş bir IDS/IPS sistemi gerekebilir.
* Ağ ihtiyaçları: Ağ, hangi tehditlere karşı korunmak istiyor?
* Bütçe: IDS/IPS sistemleri, maliyeti değişen karmaşık cihazlardır.

Küçük bir işletme için, basit bir IDS/IPS sistemi yeterli olabilir. Ancak, büyük bir işletme veya kurum için, daha gelişmiş bir IDS/IPS sistemi gerekebilir.

**IDS/IPS Sistemlerinin Bakımı**

IDS/IPS sistemlerinin etkinliğini korumak için, düzenli olarak bakım yapılması gerekir. Bu bakım, şunları içerebilir:

* Güncellemeler: IDS/IPS sistemlerinin, en son tehditleri tespit etmek için güncel olması gerekir.
* Konfigürasyon: IDS/IPS sistemlerinin, ağ gereksinimlerini karşılayacak şekilde yapılandırılması gerekir.
* Test: IDS/IPS sistemlerinin, düzgün çalıştığını test etmek için düzenli olarak test edilmesi gerekir.

IDS/IPS sistemleri, bir ağın güvenliğini sağlamada önemli bir rol oynar. Ancak, tek başına güvenlik sağlayamazlar. IDS/IPS sistemlerinin etkinliğini artırmak için, diğer güvenlik önlemleri ile birlikte kullanılması önemlidir.

**IDS/IPS Sistemlerinin Avantajları**

IDS/IPS sistemlerinin aşağıdaki avantajları vardır:

* Saldırıları tespit etme ve önleme: IDS/IPS sistemleri, bir ağı saldırılardan korumaya yardımcı olabilir.
* Durum izleme: IDS/IPS sistemleri, ağdaki olağandışı aktiviteleri tespit ederek, yöneticilerin potansiyel tehditleri belirlemesine yardımcı olabilir.
* Güvenlik politikalarının uygulanması: IDS/IPS sistemleri, güvenlik politikalarının uygulanmasını sağlayarak, ağ güvenliğini artırmaya yardımcı olabilir.

**IDS/IPS Sistemlerinin Dezavantajları**

IDS/IPS sistemlerinin aşağıdaki dezavantajları vardır:

* Maliyet: IDS/IPS sistemleri, maliyeti değişen karmaşık cihazlardır.
* Karmaşıklık: IDS/IPS sistemleri, karmaşık cihazlardır ve doğru şekilde yapılandırılması zor olabilir.
* Yanlış alarmlar: IDS/IPS sistemleri, bazen gerçek saldırıları yanlış alarmlar olarak tespit edebilir. Bu, yöneticilerin saldırılara müdahale etmesini zorlaştırabilir.

**IDS/IPS Sistemlerinin Kullanımı**

IDS/IPS sistemleri, bir ağın güvenliğini sağlamada önemli bir rol oynar. Ancak, tek başına güvenlik sağlayamazlar. IDS/IPS sistemlerinin etkinliğini artırmak için, diğer güvenlik önlemleri ile birlikte kullanılması

***Antivirüs Yazılımlarının Önemi***

Giriş

Kötü amaçlı yazılımlar, bilgisayarları, ağları ve verileri tehdit eden bir dizi zararlı yazılımdır. Kötü amaçlı yazılımlar, bilgisayarınızın performansını düşürebilir, verilerinizi çalabilir veya bilgisayarınızın kontrolünü ele geçirebilir.

Antivirüs yazılımları, bilgisayarınıza bulaşan kötü amaçlı yazılımları tespit etmek ve kaldırmak için tasarlanmıştır. Antivirüs yazılımları, bilgisayarınızı kötü amaçlı yazılımlara karşı korumanın en önemli yollarından biridir.

**Antivirüs Yazılımlarının Avantajları**

Antivirüs yazılımlarının aşağıdaki avantajları vardır:

* Kötü amaçlı yazılımları tespit etme ve kaldırma: Antivirüs yazılımları, bilgisayarınıza bulaşan kötü amaçlı yazılımları tespit etmek ve kaldırmak için tasarlanmıştır. Bu, bilgisayarınızın performansını düşürmesini, verilerinizi çalmayı veya bilgisayarınızın kontrolünü ele geçirmesini önlemeye yardımcı olabilir.
* Güvenlik açıklarını kapatma: Antivirüs yazılımları, genellikle güvenlik açıklarını kapatmak için yayınlanan yazılım güncellemelerini de algılayabilir. Güvenlik açıkları, bilgisayarınızı kötü amaçlı yazılımlara karşı daha savunmasız hale getirebilir.
* Güvenlik politikalarının uygulanması: Antivirüs yazılımları, güvenlik politikalarının uygulanmasına yardımcı olabilir. Örneğin, bazı antivirüs yazılımları, kullanıcıların yalnızca belirli web sitelerine erişmesine izin verecek şekilde yapılandırılabilir.

**Antivirüs Yazılımlarının Dezavantajları**

Antivirüs yazılımlarının aşağıdaki dezavantajları vardır:

* Maliyet: Antivirüs yazılımları, ücretsiz veya ücretli olarak kullanılabilir. Ücretli antivirüs yazılımları, genellikle daha fazla özellik ve koruma sunar.
* Performans: Antivirüs yazılımları, bilgisayarınızın performansını düşürebilir. Özellikle, bilgisayarınızın kaynaklarını yoğun kullanan antivirüs yazılımları, bilgisayarınızın performansını daha fazla düşürebilir.
* Yanlış alarmlar: Antivirüs yazılımları, bazen gerçek kötü amaçlı yazılımları yanlış alarmlar olarak tespit edebilir. Bu, kullanıcıların yanlışlıkla gerçek kötü amaçlı yazılımları kaldırmasına neden olabilir.

**Antivirüs Yazılımlarını Kullanma**

Antivirüs yazılımlarını etkin bir şekilde kullanmak için, aşağıdaki ipuçlarını takip etmeniz önemlidir:

* Antivirüs yazılımınızı güncel tutun: Antivirüs yazılımları, genellikle kötü amaçlı yazılım imzalarını içeren veritabanlarını günceller. Bu güncellemeleri zamanında uygulayarak, bilgisayarınızı en son kötü amaçlı yazılımlara karşı korumaya yardımcı olabilirsiniz.
* Antivirüs yazılımınızın tüm özelliklerini kullanın: Antivirüs yazılımlarınız, genellikle çeşitli özellikleri içerir. Bu özellikleri etkinleştirerek, bilgisayarınızı daha iyi koruyabilirsiniz.
* Antivirüs yazılımınızın ayarlarını yapılandırın: Antivirüs yazılımınızın ayarlarını, ihtiyaçlarınıza göre yapılandırın. Örneğin, bilgisayarınızın performansını korumak için, tarama ayarlarını azaltabilirsiniz.

**Antivirüs Yazılımı Seçimi**

Antivirüs yazılımı seçerken, aşağıdaki faktörleri göz önünde bulundurmanız önemlidir:

* Bilgisayarınızı ne için kullanıyorsunuz? Ev kullanıcıları için farklı antivirüs yazılımları, iş kullanıcıları için farklı antivirüs yazılımları mevcuttur.
* Bilgisayarınızın işletim sistemi nedir? Antivirüs yazılımları, farklı işletim sistemleri için tasarlanmıştır. Bilgisayarınızın işletim sistemine uygun bir antivirüs yazılımı seçmeniz önemlidir.
* Bütçeniz nedir? Antivirüs yazılımları, ücretsiz veya ücretli olarak kullanılabilir. Bütçenize uygun bir antivirüs yazılımı seçmeniz önemlidir.

**Sonuç**

Antivirüs yazılımları, bilgisayarınızı kötü amaçlı yazılımlara karşı korumanın en önemli yollarından biridir. Antivirüs yazılımları seçerken, ihtiyaçlarınıza ve bütçenize uygun bir yazılım seçmeniz önemlidir.

***Kriptografi ve Şifreleme Araçları***

Kriptografi, gizli bilgileri şifreleme ve şifreyi çözme bilimidir. Kriptografi, bilgi güvenliğini sağlamak için kullanılan önemli bir araçtır.

Şifreleme, bir metni veya diğer verileri, yalnızca yetkili kişilerin okuyabileceği şekilde dönüştürme işlemidir. Şifreleme, aşağıdakiler dahil olmak üzere çeşitli amaçlar için kullanılabilir:

* Gizlilik: Şifreleme, hassas bilgileri yetkisiz kişilerin erişimine karşı korumak için kullanılabilir. Örneğin, e-posta, bankacılık ve çevrimiçi alışveriş gibi uygulamalarda şifreleme kullanılır.
* Doğrulama: Şifreleme, bir mesajın gönderen ve alıcı tarafından doğrulanmasını sağlamak için kullanılabilir. Örneğin, dijital imzalarda şifreleme kullanılır.
* Kimlik doğrulama: Şifreleme, bir kişinin kimliğini doğrulamak için kullanılabilir. Örneğin, çevrimiçi oturum açmalarda şifreleme kullanılır.

**Kriptografi, iki temel yönteme dayanmaktadır:**

* Simetrik şifreleme: Simetrik şifreleme, şifreleme ve şifre çözme için aynı anahtarı kullanan bir şifreleme yöntemidir. Simetrik şifreleme, basit ve etkilidir, ancak anahtarın güvenli bir şekilde paylaşılması gerekir.
* Asimetrik şifreleme: Asimetrik şifreleme, şifreleme için bir anahtar ve şifre çözme için başka bir anahtar kullanan bir şifreleme yöntemidir. Asimetrik şifreleme, anahtarın güvenli bir şekilde paylaşılmasını gerektirmez, ancak daha karmaşık ve yavaştır.

**Kriptografi araçları, çeşitli şekillerde kullanılabilir. Örneğin, aşağıdakiler için kullanılabilir:**

* Veri şifreleme: Veri şifreleme, verileri diskte, ağda veya bulutta şifrelemek için kullanılabilir.
* İleti şifreleme: İleti şifreleme, e-posta, mesajlaşma ve diğer mesajlaşma uygulamalarında mesajları şifrelemek için kullanılabilir.
* Dijital imza: Dijital imza, bir mesajın gönderen ve alıcı tarafından doğrulanmasını sağlamak için kullanılabilir.
* Çevrimiçi oturum açma: Çevrimiçi oturum açma, bir kişinin çevrimiçi bir hizmete erişmesini sağlamak için kullanılabilir.

Kriptografi, bilgi güvenliğini sağlamak için önemli bir araçtır. Kriptografi araçları, çeşitli şekillerde kullanılarak, hassas bilgilerin yetkisiz kişilerin erişimine karşı korunmasına yardımcı olabilir.

**Kriptografi araçlarının bazı örnekleri şunlardır:**

* AES (Advanced Encryption Standard): AES, simetrik şifreleme için kullanılan bir standarttır.
* RSA (Rivest–Shamir–Adleman): RSA, asimetrik şifreleme için kullanılan bir standarttır.
* PGP (Pretty Good Privacy): PGP, e-posta ve diğer mesajlaşma uygulamalarında mesajları şifrelemek için kullanılan bir yazılımdır.
* SSL (Secure Sockets Layer): SSL, web sitelerini şifrelemek için kullanılan bir protokoldür.

**Kriptografi araçlarını kullanırken dikkat edilmesi gereken bazı noktalar şunlardır:**

* Anahtarları güvenli bir şekilde saklayın: Anahtarlar, şifrelenmiş verileri şifre çözmek için kullanılır. Anahtarların güvenli bir şekilde saklanması önemlidir.
* Güncellemeleri yükleyin: Kriptografi araçları, yeni güvenlik açıklarını kapatmak için güncellenir. Güncellemeleri yüklemek, verilerinizi korumak için önemlidir.
* Kriptografi araçlarını doğru kullanın: Kriptografi araçlarını doğru kullanmak önemlidir. Hatalar, şifrelenmiş verilerinizin yetkisiz kişiler tarafından okunmasına neden olabilir.

Kaynakça:

\* Resmi web siteleri: Antivirüs yazılımlarının resmi web siteleri, antivirüs yazılımları hakkında en güncel bilgileri sağlar.

\* Bağımsız güvenlik araştırma kuruluşları: Bağımsız güvenlik araştırma kuruluşları, antivirüs yazılımlarını düzenli olarak test eder ve raporlar yayınlar.

\* Teknoloji haber siteleri ve blogları: Teknoloji haber siteleri ve blogları, antivirüs yazılımları hakkında güncel haberler ve bilgiler sağlar.

- Avast: https://www.avast.com/

- Bitdefender: https://www.bitdefender.com/

- Kaspersky: https://www.kaspersky.com/

- Norton: https://us.norton.com/

\* Bağımsız güvenlik araştırma kuruluşları:

- AV-TEST: https://www.av-test.org/

- AV-Comparatives: https://www.av-comparatives.org/

- SE Labs: https://www.selabs.com/

- Teknoloji haber siteleri ve blogları:

- The Verge: https://www.theverge.com/

- CNET: https://www.cnet.com/

- PCMag: https://www.pcmag.com/

- Kriptografi ve Bilgi Güvenliği, Andrew S. Tanenbaum ve Maarten van Steen

- Kriptografi: Temelleri, Algoritmaları ve Uygulamaları, Bruce Schneier

- Kriptografi: Bir Giriş, Douglas Stinson