İki Faktörlü Kimlik Doğrulama (2FA)

İki Faktörlü Kimlik Doğrulama (2FA), dijital güvenliği artırmak amacıyla kullanılan bir kimlik doğrulama yöntemidir. Kullanıcıların yalnızca bir şifre ile kimlik doğrulaması yapmalarını yeterli görmeyen bu yöntem, ek bir güvenlik katmanı sunarak hesapların daha iyi korunmasını sağlar. 2FA, kullanıcının kimliğini doğrulamak için iki farklı doğrulama bileşeni kullanır: **Bildiğin şey** (şifre) ve **sahip olduğun şey** (mobil cihaz, doğrulama uygulaması veya SMS).

İki Faktörlü Kimlik Doğrulamanın Avantajları

- **Artan Güvenlik**: 2FA, kullanıcı adı ve şifreye ek olarak ikinci bir doğrulama katmanı sunduğu için saldırganların hesaplara izinsiz erişim sağlamasını zorlaştırır.
- **Şifre Hırsızlığını Önleme**: Şifrelerin çalınması durumunda bile, saldırganın ikinci faktöre ulaşması gerektiği için hesaba erişim engellenir.
- **Hesap Güvenliği**: Özellikle finansal hizmetler, sosyal medya platformları ve e-posta gibi kritik hesaplarda ekstra koruma sağlar.

İki Faktörlü Kimlik Doğrulamanın Dezavantajları

- **Ekstra Adım Gerektirir**: 2FA, kullanıcı için ek bir doğrulama adımı gerektirir ve bu süreç kullanıcı deneyimini uzatabilir.
- **Cihaz Kaybı Durumu**: Kullanıcılar doğrulama cihazını (telefon, donanım anahtarı) kaybederse, hesaba erişim zorlaşabilir.
- **SIM Kart Saldırıları**: SMS tabanlı 2FA, SIM kart değişikliği saldırılarına karşı savunmasız olabilir. Saldırgan, telefon numarasını ele geçirerek doğrulama kodlarına ulaşabilir.
- **Sistemlerin Güvenliği**: 2FA sistemlerinin kendisi de güvenlik açıklarına sahip olabilir. Doğrulama uygulamalarının veya biyometrik verilerin çalınması risk yaratabilir.

SSH Anahtarları

1. SSH Nedir?

SSH (Secure Shell), uzak bilgisayar bağlantılarının güvenli bir şekilde gerçekleştirilmesini sağlayan bir protokoldür. Güçlü bir güvenlik yapısına sahip olduğu için özellikle uzak masaüstü bağlantılarında sıkça tercih edilir. SSH anahtarları, kullanıcılara ait parmak izi niteliğinde olan bir anahtar çiftidir: **Özel Anahtar (Private Key)** ve **Açık Anahtar (Public Key)**.

2. SSH Anahtarlarının Bileşenleri

- **Özel Anahtar**: Kullanıcı tarafından gizli tutulan ve yalnızca kullanıcının erişebileceği bir anahtardır. Bu anahtar, kullanıcı tarafından kimlik doğrulama işlemlerinde kullanılır.
- **Açık Anahtar**: Özel anahtar ile ilişkili olan ve herkesle paylaşılabilen bir anahtardır. Sunucuya veya başka bir kullanıcıya gönderilir ve kimlik doğrulama sürecinde kullanılır.

3. SSH Anahtarlarının Avantajları

- **Güvenlik**: Şifreler yerine anahtarlar kullanıldığı için daha güçlü bir güvenlik sağlar. Şifreler genellikle tahmin edilebilirken, anahtarlar çok daha karmaşıktır.
- **Kolaylık**: SSH anahtarları ile kullanıcılar her seferinde şifre girmek zorunda kalmadan sunuculara bağlanabilirler. Özellikle çok sayıda sunucuya erişim sağlanıyorsa, bu işlem büyük kolaylık sunar.
- **Otomasyon**: Anahtar tabanlı kimlik doğrulama, otomatik görevler için idealdir. Örneğin, bir script üzerinden sunucuya bağlanma işlemleri kolayca yapılabilir.

4. SSH Anahtarlarının Dezavantajları

- **Anahtar Kaybı**: Eğer özel anahtar kaybolursa veya ele geçirilirse, ilgili sunucuya erişim tehlikeye girer. Bu nedenle özel anahtarların güvenli bir şekilde saklanması gerekir.
- **Yönetim Zorluğu**: Birden fazla anahtarın yönetilmesi zor olabilir. Kullanıcılar, hangi anahtarın hangi sunucu için kullanıldığını takip etmekte zorluk çekebilir.
- **Kurulum ve Yapılandırma**: Başlangıçta SSH anahtarlarının oluşturulması ve yapılandırılması bazı kullanıcılar için karmaşık olabilir.

Güvenlik Duvarları (Firewalls)

Güvenlik duvarları, bir bilgisayar veya ağ üzerinde güvenlik kurallarına göre veri trafiğini kontrol eden yazılım veya donanım araçlarıdır. Sunucu güvenliği açısından kritik bir rol oynarlar.

Güvenlik Duvarlarının İşlevi

- **Gelen ve Giden Trafiği Kontrol Etme**: Güvenlik duvarları, dışarıdan gelen tehditlerin içeriye ulaşmasını önlerken, içeriden dışarıya çıkan trafiği de kontrol altında tutarak yetkisiz erişimleri engeller.
- **Filtreleme Kuralları**: Kullanıcıların belirlediği kurallar doğrultusunda trafiği filtreler. Bu kurallar IP adreslerine, port numaralarına veya protokollere göre belirlenebilir.

Güvenlik Duvarı Türleri

- **Donanım Güvenlik Duvarları**: Fiziksel bir cihaz olarak ağın giriş noktasında bulunur. Genellikle daha yüksek güvenlik sağlar.
- **Yazılım Güvenlik Duvarları**: Tek bir bilgisayara veya sunucuya yüklenebilen yazılım tabanlı güvenlik çözümleridir. Daha esnek ve özelleştirilebilir.
- **Uygulama Güvenlik Duvarları**: Belirli bir uygulama veya servisin trafiğini kontrol eden özel güvenlik duvarlarıdır. Web uygulamalarını korumada etkilidir.

Güvenlik Duvarlarının Avantajları

- **Yetkisiz Erişim Engelleme**: Dışarıdan gelen tehditlere karşı etkili bir savunma sağlar.
- **Ağ İzleme**: Güvenlik duvarları, ağ trafiğini izleyerek anormal davranışları tespit edebilir.

- **Politika Uygulama**: Organizasyonların güvenlik politikalarını uygulamalarına yardımcı olur.

Güvenlik Duvarlarının Dezavantajları

- **Yanlış Konfigürasyon**: Güvenlik duvarları yanlış yapılandırıldığında, hem güvenlik açıklarına hem de işlevselliğe zarar verebilir.
- **Performans Etkisi**: Trafiği filtreleme işlemi, ağın performansını olumsuz etkileyebilir.
- **Sosyal Mühendislik**: Kullanıcıların güvenlik duvarlarının varlığını ve işleyişini yanlış anlamaları, sosyal mühendislik saldırılarına karşı daha savunmasız hale getirebilir.

TLS/SSL Sertifikaları

TLS (Transport Layer Security) ve SSL (Secure Sockets Layer), internet üzerindeki iletişimin güvenliğini sağlamak için kullanılan protokollerdir. SSL, TLS'nin daha eski bir sürümüdür ve günümüzde güvenlik açıkları nedeniyle TLS daha yaygın olarak kullanılmaktadır. Bu protokoller, verilerin şifrelenmesi ve kimlik doğrulamasını sağlayarak veri bütünlüğünü korur. TLS/SSL sertifikaları, bir web sunucusunun kimliğini doğrulamak ve şifreli bir bağlantı sağlamak için kullanılır.

TLS/SSL Sertifikalarının Bileşenleri

- **Açık Anahtar**: Sertifikanın içinde bulunan ve herkese açık olarak dağıtılabilen anahtardır.
- **Sertifika Sahibi**: Sertifikanın kimlik bilgilerini doğrulamak için kullanılan bilgi (örneğin, alan adı, kuruluş adı).
- **Sertifika Yetkilisi (CA)**: Sertifikayı veren güvenilir bir üçüncü şahıs. CA, sertifikanın geçerliliğini ve kimliğini doğrular.
- **Geçerlilik Süresi**: Sertifikanın ne kadar süreyle geçerli olduğunu belirten tarih.

TLS/SSL Sertifikalarının Avantajları

- **Veri Güvenliği**: TLS/SSL, verilerin uçtan uca şifrelenmesini sağlayarak, üçüncü şahısların verilere erişimini engeller.
- **Kimlik Doğrulama**: Sertifikalar, sunucunun kimliğini doğrulamak için kullanılır, böylece kullanıcılar sahte web siteleriyle karşılaşma riskini azaltır.
- **Veri Bütünlüğü**: Şifreleme, iletilen verilerin bütünlüğünü sağlar; bu, verilerin yol boyunca değiştirilmediğini garanti eder.
- **SEO Avantajı**: Arama motorları, HTTPS (TLS/SSL ile şifrelenmiş bağlantı) kullanan siteleri daha güvenilir bulur ve bu nedenle SEO sıralamalarında avantaj sağlar.
- **Kullanıcı Güveni**: HTTPS bağlantısına sahip siteler, kullanıcıların güvenini artırır. Kullanıcılar, verilerinin güvende olduğuna dair bir güvence hisseder.

TLS/SSL Sertifikalarının Dezavantajları

- **Maliyet**: Güvenilir bir Sertifika Yetkilisi (CA) tarafından sertifika almak genellikle maliyetlidir. Ücretsiz alternatifler (örneğin, Let's Encrypt) bulunsa da, bazıları sınırlı özelliklere sahip olabilir.

- **Yönetim Zorluğu**: Sertifikaların düzenli olarak yenilenmesi gerekir; yenileme süreci, özellikle birden fazla sertifika kullanılıyorsa yönetim zorluğu yaratabilir.
- **Sertifika Geçerlilik Süresi**: Sertifikaların geçerlilik süresi sınırlıdır ve süresi dolan sertifikalar, kullanıcıların siteye güvenini azaltabilir.
- **Yanlış Yapılandırma**: TLS/SSL sertifikaları yanlış yapılandırıldığında, kullanıcılar güvenlik uyarılarıyla karşılaşabilir. Bu durum, kullanıcı deneyimini olumsuz etkileyebilir.
- **Performans Etkisi**: Şifreleme ve şifre çözme işlemleri, sunucu üzerinde ek yük oluşturabilir. Ancak, bu etki genellikle modern sunucular ve optimizasyon teknikleri ile minimize edilebilir.

Loglama ve İzleme

Sunucu güvenliği, sistemlerde gerçekleşen olayların ve faaliyetlerin izlenmesi ile etkin bir şekilde sağlanabilir. Bu bağlamda, **loglama** (logging) ve **izleme** (monitoring) mekanizmaları, sunucuda yaşanan aktivitelerin ve performansın sürekli takibini mümkün kılar.

Loglama:

Loglama, sunucu üzerindeki çeşitli faaliyetlerin sistemli bir şekilde kaydedilmesidir. Bu kayıtlar, sistemin genel işleyişine dair geniş bir bilgi yelpazesi sunar. Loglama işlemleri, aşağıdaki faaliyetleri içerir:

- **Sistem giriş ve çıkışları**: Kullanıcıların oturum açma ve kapatma bilgileri.
- **Ağ trafiği**: Gelen ve giden ağ paketleriyle ilgili detaylar.
- **Uygulama hataları**: Uygulama seviyesindeki hata ve olay kayıtları.

Loglama, sunucunun geçmiş faaliyetlerine dair ayrıntılı bilgiler sunarak güvenlik ihlalleri veya sistem sorunlarıyla ilgili detaylı analiz yapma olanağı sağlar.

İzleme:

İzleme, sunucunun anlık performansını ve durumunu takip eden sürekli bir süreçtir. İzleme, aşağıdaki parametreleri takip eder:

- **CPU kullanımı**
- **Bellek ve disk alanı kullanımı**
- **Ağ trafiği**
- **Güvenlik tehditleri ve anormal aktiviteler**

İzleme araçları, sunucu üzerindeki potansiyel performans sorunlarını ve güvenlik tehditlerini anında tespit ederek, sistem yöneticilerine bildirimlerde bulunur.

Avantajlar:

1. **Güvenlik İhlallerini Erken Tespit Etme**: Loglama ve izleme sistemleri, olağandışı aktiviteleri fark ederek erken müdahale imkânı sunar. Örneğin, tekrarlayan hatalı giriş denemeleri veya yetkisiz erişim talepleri anında tespit edilebilir.

2. **Adli Analiz İmkanı**: Loglar, bir güvenlik ihlali sonrasında olayın nasıl gerçekleştiği ve saldırganın sistemde hangi işlemleri yaptığı konusunda ayrıntılı bilgi sağlar. Bu da olay sonrası analizlerde kullanılabilir.
3. **Performans Optimizasyonu**: İzleme sayesinde, sistemdeki performans sorunları hızla tespit edilip düzeltilir. Bu, özellikle aşırı kaynak kullanımı veya dar boğazların belirlenmesinde faydalıdır.
4. **Yasal Uyumluluk**: Özellikle belirli sektörlerde (finans, sağlık vb.) loglama, yasal düzenlemelere uyumluluğu sağlamak için gereklidir. Log kayıtları, denetimlerde kanıt olarak sunulabilir.

Dezavantajlar:

1. **Veri Depolama ve Yönetim Zorluğu**: Büyük miktarda log verisi üretilebilir ve bu verilerin saklanması, işlenmesi ve analiz edilmesi ciddi bir altyapı gerektirir. Özellikle yüksek trafikli sunucularda bu durum bir sorun haline gelebilir.
2. **Yanlış Pozitif Uyarılar**: İzleme sistemleri, zaman zaman yanlış uyarılar verebilir. Bu da yöneticilerin zamanını alır ve gerçek tehditlerin gözden kaçmasına neden olabilir.
3. **Sistem Performansına Ek Yük**: Sürekli izleme ve loglama, sunucu kaynaklarını tüketebilir. Özellikle düşük kapasiteli sunucularda, izleme faaliyetleri sistem performansını olumsuz etkileyebilir.
4. **Yetersiz Analiz**: Loglama ve izleme sistemlerinin varlığı, etkin bir analiz yapılmadıkça yeterli değildir. Toplanan verilerin düzenli ve dikkatli bir şekilde incelenmemesi, güvenlik ihlallerinin fark edilmeden geçmesine neden olabilir.

İzinsiz Giriş Tespit ve Önleme Sistemleri (IDS/IPS)

Sunucu güvenliğinde **İzinsiz Giriş Tespit Sistemleri (IDS)** ve **İzinsiz Giriş Önleme Sistemleri (IPS)**, ağ ve sunuculara yapılan saldırıların tespit edilmesi ve önlenmesi için kritik bir rol oynar. Bu sistemler, yetkisiz erişimleri ve saldırı girişimlerini algılayarak, gerekli önlemleri alır.

IDS ve IPS Nedir?

- **IDS (İzinsiz Giriş Tespit Sistemi)**: Sunucu veya ağ üzerinde gerçekleşen şüpheli aktiviteleri ve tehditleri tespit eden bir sistemdir. IDS, yalnızca tehditleri tanımlar ve güvenlik yöneticisine bildirimde bulunur, ancak bu tehditlere müdahale etmez.
    - **Çalışma Prensibi**: IDS sistemleri, ağ trafiğini ve sunucuya gelen istekleri inceleyerek normal dışı veya kötü niyetli hareketleri belirler. Anomali tespiti yaparak, yetkisiz giriş denemeleri, zararlı yazılım faaliyetleri veya DDoS saldırıları gibi tehditleri raporlar.
- **IPS (İzinsiz Giriş Önleme Sistemi)**: IDS sistemine ek olarak, tehditleri tespit ettiğinde bunları otomatik olarak engelleyen bir güvenlik sistemidir. IPS, IDS'nin aksine aktif olarak saldırıları durdurur.
    - **Çalışma Prensibi**: IPS, ağ trafiğini analiz ettikten sonra anormal bir durum tespit ederse, bu trafiği anında durdurur ya da bloke eder. Böylece sunucuya yönelik tehditlere anında müdahale edilir.

IDS ve IPS Sistemlerinin Çeşitleri:

1. **Ağ Tabanlı IDS/IPS (NIDS/NIPS)**:
   - Ağ trafiğini izleyerek saldırıları tespit eder. Genellikle ağ geçitlerine veya güvenlik duvarlarına entegre edilmiştir.
2. **Host Tabanlı IDS/IPS (HIDS/HIPS)**:
   - Bir sunucu veya bilgisayardaki sistem aktivitelerini izler. Sistem dosyalarında yapılan yetkisiz değişiklikleri ve kötü niyetli faaliyetleri tespit eder.

Avantajları:

1. **Erken Tespit ve Müdahale**:
   - IDS/IPS sistemleri, saldırıları erken aşamada tespit ederek sistem yöneticilerini bilgilendirir veya saldırıları otomatik olarak engeller. Bu, özellikle DDoS, brute-force ve zararlı yazılım saldırılarını etkisiz hale getirmek açısından son derece faydalıdır.
2. **Ağ Trafiğinin Sürekli İzlenmesi**:
   - Bu sistemler, ağ trafiğini sürekli izler ve normalin dışına çıkan her türlü etkinliği belirler. Bu, sistemdeki güvenlik açıklarının veya yanlış yapılandırmaların fark edilmesini sağlar.
3. **Yasal Uyumluluk ve Denetimler**:
   - IDS/IPS sistemleri, yasal düzenlemelere uyumluluğun sağlanması için güvenlik logları ve raporlar sunar. Örneğin, finans veya sağlık sektörlerinde zorunlu olan güvenlik standartlarına uyum sağlamak için kullanılabilir.
4. **Kapsamlı Güvenlik Kapsaması**:
   - Hem ağ hem de host tabanlı izleme yaparak sistemdeki farklı güvenlik tehditlerine karşı geniş bir koruma sağlar. Bu sayede, dış tehditlerin yanı sıra iç tehditler de izlenebilir.

Dezavantajları:

1. **Yanlış Pozitifler (False Positives)**:
   - IDS/IPS sistemleri, zaman zaman normal davranışları da saldırı olarak algılayabilir. Bu yanlış pozitif uyarılar, yöneticilerin gereksiz zaman kaybetmesine ve kaynakların yanlış yönlendirilmesine neden olabilir.
2. **Yüksek Kaynak Tüketimi**:
   - Özellikle yüksek trafikli ağlarda IDS/IPS sistemleri, ağ trafiğini analiz ederken yüksek miktarda CPU ve bellek kullanabilir. Bu da sistem performansını olumsuz etkileyebilir.
3. **Manuel Müdahale Gerekmesi (IDS için)**:
   - IDS sistemleri, sadece tehditleri tespit eder ve yöneticiyi uyarır. Saldırılara karşı otomatik bir müdahalede bulunmaz. Bu nedenle yöneticinin saldırıyı fark etmesi ve hızlı bir şekilde yanıt vermesi gerekir.
4. **Yetersiz Konfigürasyon Riski**:
   - IDS/IPS sistemlerinin yanlış yapılandırılması durumunda, ciddi güvenlik açıkları oluşabilir. Yanlış ayarlar, tehditlerin tespit edilememesine veya gereksiz yere engellenmesine yol açabilir.

Düzenli Güvenlik Testleri (Pentest)

Pentest Nedir?

Pentest, bir sunucunun, ağın veya uygulamanın güvenlik açıklarını tespit etmek amacıyla simüle edilmiş bir saldırıdır. Bu testler, gerçek saldırganlar tarafından kullanılabilecek güvenlik açıklarını belirleyerek, sistem yöneticilerinin bu zafiyetleri düzeltmelerine olanak tanır. Pentest, genellikle aşağıdaki adımlardan oluşur:

1. **Keşif (Reconnaissance)**:
    - Sistem hakkında bilgi toplama sürecidir. Saldırganlar genellikle bu aşamada hangi hizmetlerin ve portların açık olduğunu öğrenir.
2. **Tarama (Scanning)**:
    - Toplanan bilgilere dayanarak sunucu üzerindeki güvenlik açıkları taranır. Zayıf noktalar, açık portlar, yanlış yapılandırmalar ve eski yazılım sürümleri tespit edilir.
3. **Saldırı (Exploitation)**:
    - Tespit edilen güvenlik açıkları üzerinde deneme saldırıları gerçekleştirilir. Bu aşama, gerçek bir saldırının nasıl yapılabileceğini gösterir ve sistemin saldırılara karşı dayanıklılığı test edilir.
4. **Raporlama (Reporting)**:
    - Güvenlik testlerinin sonuçları, tespit edilen zafiyetler ve bu zafiyetlerin nasıl giderileceği ile ilgili detaylı bir rapor hazırlanır.

Pentest Türleri:

1. **Beyaz Kutu Testi (White-box Testing)**:
    - Test yapan kişiye sistem hakkında kapsamlı bilgi sağlanır. Kaynak kodlarına, yapılandırma dosyalarına ve ağ yapısına erişim sağlanarak sistem detaylı bir şekilde analiz edilir.
2. **Siyah Kutu Testi (Black-box Testing)**:
    - Test yapan kişi, sistem hakkında hiçbir bilgiye sahip değildir. Bir saldırganın dışarıdan sisteme nasıl erişmeye çalışacağını simüle eder. Sadece dışardan erişim yolları incelenir.
3. **Gri Kutu Testi (Gray-box Testing)**:
    - Test yapan kişiye sistem hakkında sınırlı bilgi verilir. Hem içeriden hem de dışarıdan saldırı senaryoları test edilir. Bu test türü, gerçek hayattaki tehdit senaryolarını simüle etmek açısından oldukça etkilidir.

Avantajları:

1. **Güvenlik Açıklarının Erken Tespiti**:
    - Pentest, sistemde var olan güvenlik açıklarının siber saldırganlar tarafından keşfedilmeden önce tespit edilmesini sağlar. Bu da potansiyel saldırıların önlenmesine yardımcı olur.
2. **Güvenlik Stratejisinin Güçlendirilmesi**:
    - Pentest raporları, sistemdeki zayıf noktaların giderilmesi için yol gösterici olur. Bu sayede, sunucuya yönelik saldırılara karşı savunma stratejileri güncellenir ve iyileştirilir.
    -

3. **Yasal Uyumluluk**:
    - Özellikle belirli sektörlerde (finans, sağlık vb.) güvenlik testleri yasal bir zorunluluk haline gelmiştir. Düzenli pentestler, işletmelerin yasal düzenlemelere uyum sağlamasına yardımcı olur ve olası denetimlerde güvenlik açıklarını kapatır.
4. **Gerçekçi Saldırı Simülasyonu**:
    - Pentest, gerçek saldırı yöntemlerini simüle ettiği için sistemin gerçek dünyadaki saldırılara ne kadar dayanıklı olduğunu test etme imkânı sunar. Bu, sadece teorik bir test değil, pratikteki saldırıların nasıl olacağını anlamaya yardımcı olur.
5. **İtibarın Korunması**:
    - Olası bir siber saldırının tespit edilmemesi durumunda, müşteri bilgilerinin çalınması veya sistemin devre dışı kalması, bir şirketin itibarına büyük zarar verebilir. Pentest, bu tür durumların önlenmesi için alınacak tedbirleri önceden belirler.

Dezavantajları:

1. **Yüksek Maliyet**:
    - Profesyonel pentest hizmetleri maliyetli olabilir. Özellikle büyük ölçekli sistemlerde kapsamlı testler yapılması gerektiğinde, test maliyetleri artabilir.
2. **Test Süresi ve Kaynak Kullanımı**:
    - Pentest süreci, sunucu kaynaklarını etkileyebilir ve test sırasında sistemin performansında düşüşlere neden olabilir. Bu nedenle testlerin planlı bir şekilde yapılması önemlidir.
3. **Yanlış Pozitifler**:
    - Pentest sırasında bazen yanlış pozitif sonuçlar elde edilebilir. Yani, sistemde gerçekte var olmayan güvenlik açıkları tespit edilebilir. Bu durum, gereksiz zaman ve kaynak harcanmasına yol açabilir.
4. **Zafiyetlerin Yeniden Ortaya Çıkması**:
    - Pentest sırasında tespit edilen güvenlik açıkları kapatılsa bile, ilerleyen süreçte yeni yazılım güncellemeleri veya yapılandırma değişiklikleri nedeniyle yeni zafiyetler ortaya çıkabilir. Bu nedenle, pentest sadece belirli bir zaman dilimindeki güvenliği garanti eder.

AES (Advanced Encryption Standard):

AES (Gelişmiş Şifreleme Standardı), günümüzde yaygın olarak kullanılan güçlü bir simetrik şifreleme algoritmasıdır. 2001 yılında ABD hükümeti tarafından resmi olarak kabul edilen AES, yüksek hız ve güvenlik sunarak birçok uygulamada ve sunucu ortamında standart haline gelmiştir.

- **Çalışma Prensibi**: AES, verileri sabit boyutlu 128 bitlik bloklar halinde şifreler. 128, 192 ve 256 bit olmak üzere üç farklı anahtar uzunluğu ile kullanılabilir. AES'in simetrik bir algoritma olması, hem şifreleme hem de çözme işlemi için aynı anahtarın kullanıldığı anlamına gelir.

- **Kullanım Alanları**:
    - AES, dosya şifrelemeden, veri tabanı şifrelemeye kadar birçok alanda kullanılır. Özellikle sunucu ortamlarında, depolanan verilerin ve hassas bilgilerin korunması için tercih edilir. AES, **Veri Tabanı Şifreleme**, **Disk Şifreleme** ve **Dosya Transfer Güvenliği** gibi kritik güvenlik alanlarında yaygın olarak kullanılır.
- **Avantajları**:
    - **Güvenlik**: AES, günümüzde kırılması zor olan en güvenli algoritmalardan biridir.
    - **Performans**: AES, hem yazılım hem de donanım tabanlı uygulamalarda yüksek hızda çalışabilir, bu da büyük veri setlerinin bile hızlı bir şekilde şifrelenmesine olanak tanır.
    - **Kapsamlı Kullanım**: AES, neredeyse tüm modern güvenlik protokollerinde yer alır.
- **Dezavantajları**:
    - **Anahtar Yönetimi**: Simetrik şifrelemenin temel dezavantajı, güvenli anahtar yönetiminin zor olmasıdır. Şifreleme ve çözme işlemleri için aynı anahtarın kullanılması, bu anahtarın güvenli bir şekilde iletilmesini ve saklanmasını zorlaştırabilir.

HTTPS (Hypertext Transfer Protocol Secure):

HTTPS, sunucular arasında veri transferi yapılırken güvenliğin sağlanması amacıyla kullanılan bir protokoldür. HTTPS, SSL (Secure Sockets Layer) veya TLS (Transport Layer Security) protokolleri ile verilerin şifrelenmesini sağlar. Web tabanlı uygulamalarda, istemci ve sunucu arasında gerçekleşen veri iletişimlerini güvenli hale getirmek için vazgeçilmez bir yöntemdir.

- **Çalışma Prensibi**: HTTPS, HTTP'nin güvenli bir versiyonudur. Veri iletimi sırasında, istemci (tarayıcı) ve sunucu arasında SSL/TLS protokolleri ile bir bağlantı kurulur. Bu bağlantı şifrelenir, böylece üçüncü şahısların veri transferi sırasında bilgilere erişmesi engellenir. HTTPS, kimlik doğrulama ve veri bütünlüğü sağlar, böylece sadece yetkili taraflar arasında veri iletişimi gerçekleşir.
- **Kullanım Alanları**:
    - Web sitelerindeki oturum açma formları, ödeme sistemleri, banka işlemleri gibi hassas veri iletimlerinin gerçekleştiği her alanda HTTPS kullanılır. Ayrıca, veri bütünlüğünü ve gizliliğini sağlamak amacıyla, web sunucuları HTTPS ile korunmalıdır.
- **Avantajları**:
    - **Veri Güvenliği**: HTTPS, verilerin güvenli bir şekilde iletilmesini sağlar ve üçüncü şahıslar tarafından ele geçirilmesini zorlaştırır.
    - **Kimlik Doğrulama**: HTTPS, sunucuların kimliğini doğrulayarak kullanıcıların sahte sitelere yönlendirilmesini engeller.
    - **Yasal Uyumluluk**: Birçok sektör, özellikle finans ve sağlık gibi hassas verilerin kullanıldığı sektörlerde, HTTPS kullanımını zorunlu tutar.
- **Dezavantajları**:
    - **Sertifika Yönetimi**: HTTPS bağlantısı için SSL/TLS sertifikaları gerekir ve bu sertifikaların yönetimi zaman alabilir. Sertifikaların düzenli olarak yenilenmesi ve doğruluğunun sağlanması, ek maliyet ve bakım gerektirebilir.

    - **Performans Maliyeti**: Şifreleme ve şifre çözme işlemleri sunucuya ek yük bindirebilir ve performansı olumsuz yönde etkileyebilir. Ancak modern donanımlarla bu dezavantaj minimize edilebilir.

Depolama ve Transfer Güvenliği:

Sunucu ortamlarında sadece verilerin transferi değil, aynı zamanda verilerin depolanması da büyük bir güvenlik konusu oluşturur. Verilerin hem sunucu üzerinde depolanırken hem de transfer edilirken şifrelenmesi gerekir. Bu bağlamda, **SFTP (Secure File Transfer Protocol)** gibi şifreleme destekli protokoller, veri güvenliğini sağlamak için önemli bir rol oynar.

- **Depolama Güvenliği**: Sunucularda depolanan verilerin güvenliği, AES gibi güçlü şifreleme algoritmaları ile sağlanabilir. Özellikle hassas veriler, diskte veya veri tabanında şifrelenerek yetkisiz erişimlere karşı korunur. Bu, veri ihlallerini önlemede kritik bir önlemdir.
- **Transfer Güvenliği**:
    - Verilerin sunucular arasında veya istemci-sunucu arasında taşınması sırasında SFTP, HTTPS gibi şifreleme protokolleri kullanılmalıdır. SFTP, FTP'nin güvenli bir versiyonudur ve veri transferi sırasında şifreleme sağlar. Özellikle dosya transferleri sırasında kullanılması gereken bir yöntemdir.
    - **Veritabanı İletişimi**: Sunucu ile veritabanı arasındaki iletişim sırasında da şifreleme yöntemleri kullanılmalıdır. Bu, hem veri tabanındaki bilgilerin korunmasını sağlar hem de veri tabanı sunucusu ile uygulama sunucusu arasındaki veri transferini güvence altına alır.
- **Avantajları**:
    - **Güvenlik**: Depolama ve transfer sırasında verilerin şifrelenmesi, veri ihlallerine karşı önemli bir güvenlik katmanı ekler. Özellikle sunucular arası dosya transferlerinde bu güvenlik katmanı kritik rol oynar.
    - **Bütünlük**: Şifrelenmiş verilerin transferi sırasında verilerin bozulması veya değiştirilmesi daha zor hale gelir, bu da veri bütünlüğünü korur.
- **Dezavantajları**:
    - **Performans Etkisi**: Şifreleme ve şifre çözme işlemleri, işlemci ve bellek üzerinde ek bir yük oluşturabilir ve transfer hızı üzerinde olumsuz etki yaratabilir. Ancak bu, modern donanımlarla en aza indirgenebilir.
    - **Yönetim Zorluğu**: Şifreleme anahtarlarının yönetimi ve güvenli bir şekilde saklanması zor olabilir. Bu süreçlerde yapılan hatalar, veri kayıplarına veya güvenlik ihlallerine neden olabilir.