Ağ Güvenliği ve SSL/TLS Nedir?

Çalışma Kağıdı

Ağ güvenliği, bilgisayar ağlarını ve ağ üzerindeki verileri yetkisiz erişim, kötüye kullanım veya zarar görmeden koruma uygulamalarıdır. SSL/TLS (Secure Sockets Layer/Transport Layer Security), web siteleri ve tarayıcılar arasındaki iletişimi şifreleyerek bu güvenliği sağlayan kriptografik protokollerdir.

Sorular

1. Aşağıdakilerden hangisi ağ güvenliğinin temel amaçlarından biri DEĞİLDİR?

A) Veri gizliliğini sağlamak
B) Ağ performansını artırmak
C) Veri bütünlüğünü korumak
D) Yetkisiz erişimi engellemek

2. SSL/TLS protokolü hangi katmanda çalışır?

A) Uygulama Katmanı
B) Taşıma Katmanı
C) Oturum Katmanı
D) Ağ Katmanı

3. Bir web sitesinde 'https://' kullanılması ne anlama gelir?

A) Siteye erişim ücretsizdir.
B) Site mobil uyumludur.
C) Site ile tarayıcı arasındaki iletişim şifrelidir.
D) Site yavaş yükleniyor demektir.

4. Bir e-ticaret sitesinde SSL/TLS nasıl çalışır?

5. SSL/TLS neden önemlidir?

6. Tanımla: SSL/TLS'nin açılımı nedir?

7. Tanımla: SSL/TLS'nin temel amacı nedir?

8. Tanımla: Bir web sitesinde SSL/TLS kullanıldığını nasıl anlarız?

Cevap Anahtarı

1. B) Ağ performansını artırmak — Ağ güvenliğinin temel amacı iletişimin güvenliğini sağlamaktır; performans artırmak doğrudan bir amacı değildir, ancak güvenli bir ağ dolaylı olarak performansı etkileyebilir.

2. B) Taşıma Katmanı — SSL/TLS, OSI modelinin Taşıma Katmanı'nda veya TCP/IP modelinde Taşıma ve Uygulama Katmanı arasında yer alır ve güvenliği sağlar.

3. C) Site ile tarayıcı arasındaki iletişim şifrelidir. — 'https://' protokolü, HTTP'nin güvenli versiyonudur ve SSL/TLS kullanılarak iletişimin şifrelendiğini gösterir.

4. Müşteri tarayıcısı siteye bağlanır.,Sunucu, SSL/TLS sertifikasını ve genel anahtarını gönderir.,Tarayıcı, sertifikanın geçerliliğini doğrular ve oturum anahtarını şifreler.,Şifrelenmiş oturum anahtarı sunucuya gönderilir.,Sunucu, özel anahtarını kullanarak oturum anahtarını çözer.,Artık tarayıcı ve sunucu arasındaki tüm veri alışverişi bu oturum anahtarıyla şifrelenir.

5. Veri Gizliliği: İletilen bilgilerin (kredi kartı numaraları, şifreler vb.) okunmasını engeller.,Veri Bütünlüğü: Verilerin iletim sırasında değiştirilmediğini garanti eder.,Kimlik Doğrulama: Kullanıcının gerçekten doğru web sitesiyle iletişim kurduğunu doğrular.,Güven Oluşturma: Kullanıcılara dijital işlemlerde güven verir.

6. Secure Sockets Layer / Transport Layer Security

7. İnternet üzerindeki iletişimi şifreleyerek güvenliğini sağlamak.

8. Tarayıcı adres çubuğunda kilit simgesi ve 'https://' öneki ile.