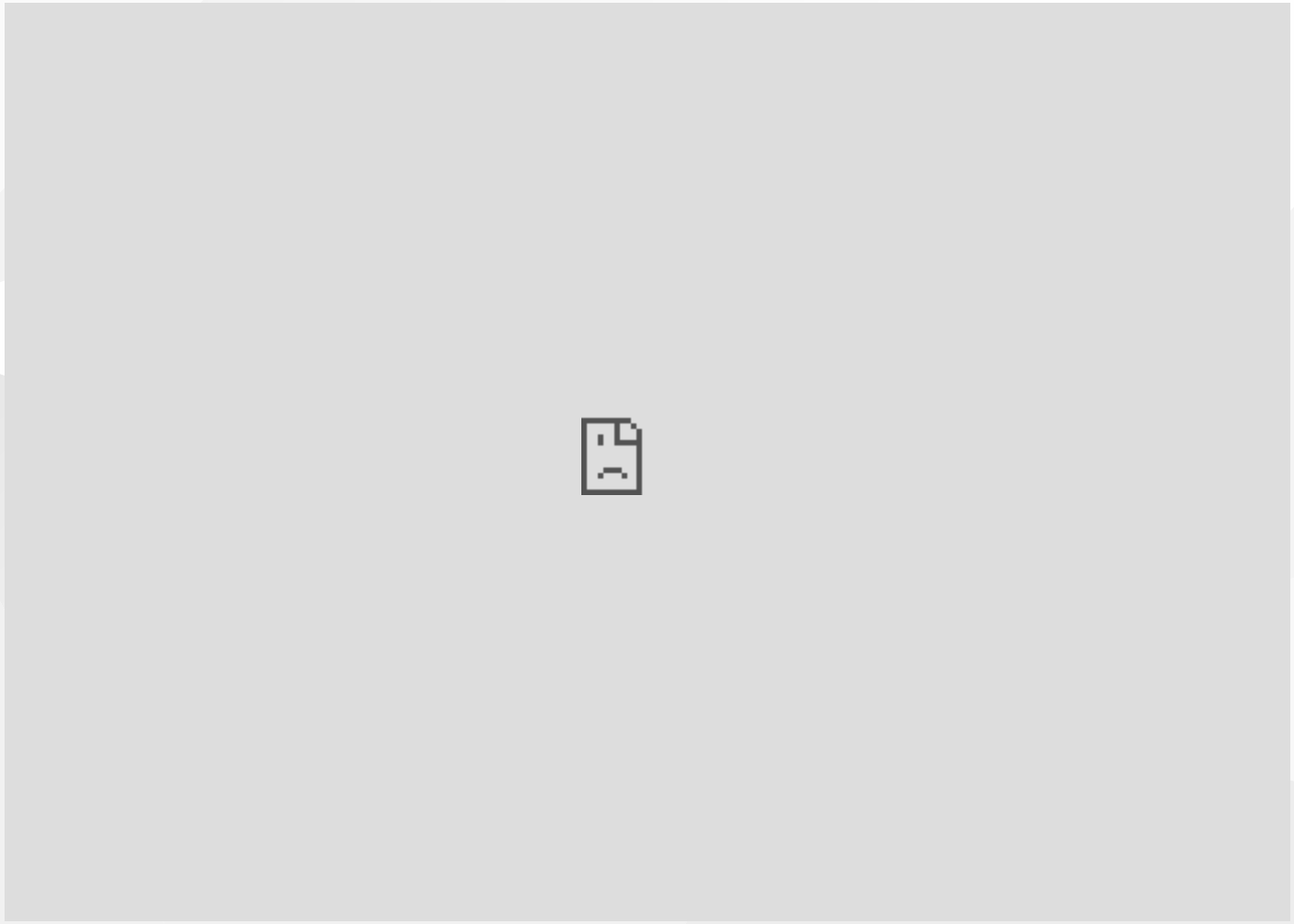
CEN429 Güvenli Programlama

Hafta-11

Güvenlik Sertifikaları ve Penetrasyon Testi Planları

İndir

- PDF
- DOC
- SLIDE
- PPTX



Outline

- Güvenlik Sertifikalarının Önemi
- Penetrasyon Testi Planları ve Araçları
- Sertifikasyon Süreçleri ve İlişkiler

Hafta-11: Güvenlik Sertifikaları ve Penetrasyon Testi Planları

Bu haftanın amacı, güvenlik sertifikasyonlarının önemini, kullanılan standartları ve sızma testi (Penetrasyon Testi) süreçlerinin nasıl planlandığını öğrenmektir. Güvenlik sertifikaları, yazılım ve donanımın güvenliğinin uluslararası standartlara uygunluğunu gösterirken, penetrasyon testleri sistemin güvenlik açıklarını belirleyip olası tehditleri analiz etmemizi sağlar.

1. Güvenlik Sertifikalarının Önemi

Teorik Açıklama: Güvenlik sertifikaları, bir sistemin veya ürünün belirli güvenlik standartlarına uyduğunu gösterir. Sertifikalar, genellikle bir ürünün kullanıcılara güven verdiğini ve güvenlik açısından belirli testlerden geçtiğini belirtir.

- **Neden Önemli?**
  - Güvenilirlik sağlar.
  - Uluslararası standartlara uygunluğu gösterir.
  - Regülasyon ve yasal uyum gereksinimlerini karşılar.
  - Ürünlerin güvenlik seviyesini artırır.
  - Kullanıcılar ve müşterilere güven verir.

Uygulama Örnekleri:

1. Bir sistemin neden güvenlik sertifikasına ihtiyaç duyduğuna dair bir analiz yapma.
2. Güvenlik sertifikalarının ticari ürünler üzerindeki etkilerini inceleme.

2. Yaygın Güvenlik Sertifikaları ve Standartlar

Teorik Açıklama: Birçok güvenlik standardı ve sertifikasyon, donanım ve yazılım ürünlerinin güvenliğini sağlamak için kullanılır. Bu standartlar, ürünlerin nasıl test edilmesi ve sertifikalandırılması gerektiğine dair rehberlik eder.

- **ETSI (European Telecommunications Standards Institute):** Telekomünikasyon ve ağ güvenliği standartlarını belirler.
- **EMV (Europay, MasterCard, Visa):** Kart tabanlı ödeme sistemlerinin güvenliğini sağlamak için kullanılan standart.
- **GSMA:** Mobil cihazlar ve ağlar için güvenlik standartları.
- **ISO/IEC 27001:** Bilgi güvenliği yönetim sistemleri standardı.
- **PCI DSS (Payment Card Industry Data Security Standard):** Ödeme kartı bilgilerinin güvenliğini sağlamak için kullanılan standart.

Uygulama Örnekleri:

1. ETSI standartlarına göre bir ağ güvenliği planı oluşturma.
2. PCI DSS uyumluluğunun bir ödeme sistemi için nasıl sağlanacağını inceleme

3. EAL (Evaluation Assurance Level) Sertifikasyonu

Teorik Açıklama: EAL (Değerlendirme Güvencesi Seviyesi), bir ürünün belirli güvenlik gereksinimlerini karşılama düzeyini gösterir. Farklı seviyelerde (EAL1'den EAL7'ye kadar) güvenlik güvencesi sağlar.

- **EAL Seviyeleri:**
  - **EAL1:** Fonksiyonel olarak test edilmiş.
  - **EAL2:** Yapısal olarak test edilmiş.
  - **EAL3:** Metodolojik olarak test edilmiş ve denetlenmiş.
  - **EAL4:** Tasarım bazında gözden geçirilmiş, metodolojik olarak test edilmiş.
  - **EAL5:** Yüksek güvence sağlayan, semantik olarak analiz edilmiş.
  - **EAL6 ve EAL7:** Son derece yüksek güvenlik seviyesi, matematiksel olarak kanıtlanmış.

Uygulama Örnekleri:

1. EAL sertifikasyon sürecinin nasıl işlediğini araştırma.
2. EAL seviyelerine göre bir sistemin güvenliğini değerlendirme

- **Neden Penetrasyon Testi Yapılır?**
  - Güvenlik açıklarını tespit etmek.
  - Gerçek dünya saldırılarına karşı sistemi test etmek.
  - Zayıf noktaları belirleyerek savunma mekanizmalarını güçlendirmek.
  - Sistem güvenliğini proaktif bir şekilde artırmak.

PenTest Süreç Adımları:

1. **Keşif (Reconnaissance):** Sistem hakkında bilgi toplama.
2. **Tarama (Scanning):** Açık portlar, hizmetler ve zayıflıklar tespit edilir.
3. **Sistem İstismarı (Exploitation):** Tespit edilen zayıflıklardan yararlanarak sisteme sızma.
4. **Avantaj Sağlama (Privilege Escalation):** Sistemde yönetici haklarına erişim sağlama.
5. **Erişimi Koruma (Maintaining Access):** Sızmanın kalıcı hale getirilmesi.
6. **Kanıt Toplama (Evidence Collection):** Bulunan güvenlik açıklarının belgelenmesi.

5. Penetrasyon Testi Yöntemleri

Teorik Açıklama: Penetrasyon testi yöntemleri, test edilecek sistemin türüne ve saldırı hedeflerine göre değişiklik gösterir. Bazı yaygın test yöntemleri şunlardır:

- **Beyaz Kutu (Whitebox) Testi:** Test eden kişi, sistemin iç yapısını ve kaynak kodunu bilir.
- **Kara Kutu (Blackbox) Testi:** Test eden kişi, sistem hakkında hiçbir bilgiye sahip değildir. Saldırılar dışarıdan gerçekleştirilir.
- **Gri Kutu (Graybox) Testi:** Test eden kişi, sistemin bazı bölümleri hakkında bilgi sahibidir. Örneğin, uygulama yapısına veya kullanıcı rollerine dair bilgiye sahiptir.

Uygulama Örnekleri:

1. Beyaz kutu ve kara kutu testi arasındaki farkları analiz etme.
2. Bir sistem üzerinde gri kutu testi gerçekleştirerek sonuçları raporlama.

6. Penetrasyon Testi Araçları

Teorik Açıklama: Penetrasyon testleri sırasında çeşitli araçlar kullanılarak sistemin zayıf noktaları analiz edilir. Bu araçlar, testin kapsamına ve hedeflerine göre seçilir.

- **Nessus:** Zayıf nokta taraması için kullanılan popüler bir araçtır.
- **Metasploit:** Güvenlik açıklarının istismar edilmesi ve zayıflıkların test edilmesi için kullanılan bir çerçeve.
- **Wireshark:** Ağ trafiğini izlemek ve analiz etmek için kullanılır.
- **Burp Suite:** Web uygulamalarında güvenlik testi yapmak için kullanılan bir araçtır.
- **OWASP ZAP:** Web uygulamalarında güvenlik açıklarını tespit etmek için kullanılan açık kaynak bir araç.

Uygulama Örnekleri:

1. **Nessus** kullanarak bir sistemin güvenlik açıklarını tarama.
2. **Metasploit** kullanarak bir güvenlik açığından yararlanma ve sonuçlarını analiz etme.

7. Penetrasyon Testi ve Sertifikasyon İlişkisi

Teorik Açıklama: Penetrasyon testi sonuçları, bir sistemin güvenlik sertifikasyonu sürecinde önemli bir rol oynar. Sertifikasyon sağlayıcıları, bir sistemin güvenliğini doğrulamak için genellikle penetrasyon testi sonuçlarını göz önünde bulundurur.

- **Nasıl İlişkilidir?**
  - PenTest sonuçları, sertifikasyon sürecine eklenir ve güvenlik seviyesi kanıtlanır.
  - Güvenlik sertifikası almak için belirli testlerin başarıyla geçilmesi gerekir.
  - Penetrasyon testleri, sertifika uyumluluğunu sağlamak için düzenli olarak yapılır.

Uygulama Örnekleri:

1. Penetrasyon testi sonuçlarını sertifikasyon sürecine nasıl entegre edebileceğimizi analiz etme.
2. Sertifikasyon gereksinimlerine uygun bir güvenlik testi planı hazırlama.

Sonuç

Bu hafta, güvenlik sertifikasyonlarının ve penetrasyon testlerinin sistem güvenliği üzerindeki etkilerini inceledik. Güvenlik sertifikaları, uluslararası standartlara uyumluluğu gösterirken, penetrasyon testleri bir sistemin zayıf noktalarını ortaya çıkararak güvenliğini artırır. Bu iki süreç, yazılım ve donanım ürünlerinin güvenlik seviyesini artırmak için birlikte çalışır.

$11. Hafta - Sonu$