

CEN429 GÃ¼venli Programlama Hafta-11

GÃ¼venlik SertifikalarÄ± ve Penetrasyon Testi PlanlarÄ±

Yazar: Dr. UÄŸur CORUH

İçindekiler

1 CEN429 GÃ¼venli Programlama	1
1.1 Hafta-11	1
1.1.1 Outline	1
1.1.2 Hafta-11: GÃ¼venlik SertifikalarÄ± ve Penetrasyon Testi PlanlarÄ±	1
1.1.3 SonuÅŸ	4

Åekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-11

1.1.0.1 GÃ¼venlik SertifikalarÄ± ve Penetrasyon Testi PlanlarÄ± Ä±ndir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- GÃ¼venlik SertifikalarÄ±nÄ±n Ä±nemi
- Penetrasyon Testi PlanlarÄ± ve AraÅŸlarÄ±
- Sertifikasyon SÄ±reÅŸleri ve Ä°liÅŸkiler

1.1.2 Hafta-11: GÃ¼venlik SertifikalarÄ± ve Penetrasyon Testi PlanlarÄ±

Bu haftanÄ±n amacÄ±, gÃ¼venlik sertifikasyonlarÄ±nÄ±n Ä±nemini, kullanÄ±lan standartlarÄ± ve sÄ±zma testi (Penetrasyon Testi) sÄ±reÅŸlerinin nasÄ±l planlandÄ±ÄŸÄ±nÄ± Ä±ÄŸrenmektir. GÃ¼venlik sertifikalarÄ±, yazÄ±lÄ±m ve donanÄ±mÄ±n gÃ¼venliÄŸinin uluslararası standartlara uygunluÄŸunu gÄŸsterirken, penetrasyon testleri sistemin gÃ¼venlik aÅŸÄ±klarÄ±nÄ± belirleyip olasÄ± tehditleri analiz etmemizi saÄŸlar.

¹[pandoc_cen429-week-11.pdf](#)

²[pandoc_cen429-week-11.docx](#)

³[cen429-week-11.pdf](#)

⁴[cen429-week-11.pptx](#)

1.1.2.1 1. GÃ¼venlik SertifikalarÄ±nÄ±n Ä±nemli Teorik AÃŒÄ±klama: GÃ¼venlik sertifikalarÄ±, bir sistemin veya Ä±rÄ±nÄ±n belirli gÃ¼venlik standartlarÄ±na uyduÄŒunu gÃ¼sterir. Sertifikalar, genellikle bir Ä±rÄ±nÄ±n kullanÄ±cÄ±lara gÃ¼ven verdiÄŒini ve gÃ¼venlik aÃŒÄ±sÄ±ndan belirli testlerden geÃŒtiÄŒini belirtir.

- **Neden Ä±nemli?**
 - GÃ¼venilirlik saÄŒlar.
 - Uluslararası standartlara uygunluÄŒu gÃ¼sterir.
 - RegÃ¼lasyon ve yasal uyum gereksinimlerini karŒÄ±lar.
 - Ä±erÄ±nlerin gÃ¼venlik seviyesini artÄ±rÄ±r.
 - KullanÄ±cÄ±lar ve mÃ¼ÄŒterilere gÃ¼ven verir.

Uygulama Ä±rnekleri:

1. Bir sistemin neden gÃ¼venlik sertifikasÄ±na ihtiyaŒ duyduÄŒuna dair bir analiz yapma.
2. GÃ¼venlik sertifikalarÄ±nÄ±n ticari Ä±rÄ±nlar Ä±zerindeki etkilerini inceleme.

1.1.2.2 2. YaygÄ±n GÃ¼venlik SertifikalarÄ± ve Standartlar Teorik AÃŒÄ±klama: BirÄŒok gÃ¼venlik standardÄ± ve sertifikasyon, donanÄ±m ve yazÄ±lÄ±m Ä±rÄ±nlarının gÃ¼venliÄŒini saÄŒlamak iŒin kullanÄ±lÄ±r. Bu standartlar, Ä±rÄ±nların nasÄ±l test edilmesi ve sertifikalandÄ±rÄ±lmasÄ± gerektiÄŒine dair rehberlik eder.

- **ETSI (European Telecommunications Standards Institute):** TelekomÃ¼nikasyon ve aÄŒ gÃ¼venliÄŒi standartlarÄ±nÄ± belirler.
- **EMV (Europay, MasterCard, Visa):** Kart tabanlı Ä±deme sistemlerinin gÃ¼venliÄŒini saÄŒlamak iŒin kullanÄ±lan standart.
- **GSMA:** Mobil cihazlar ve aÄŒlar iŒin gÃ¼venlik standartlarÄ±.
- **ISO/IEC 27001:** Bilgi gÃ¼venliÄŒi yÄŒnetim sistemleri standardÄ±.
- **PCI DSS (Payment Card Industry Data Security Standard):** Ä±deme kartÄ± bilgilerinin gÃ¼venliÄŒini saÄŒlamak iŒin kullanÄ±lan standart.

Uygulama Ä±rnekleri:

1. ETSI standartlarÄ±na gÃ¼re bir aÄŒ gÃ¼venliÄŒi planÄ± oluŒturma.
2. PCI DSS uyumluluÄŒunun bir Ä±deme sistemi iŒin nasÄ±l saÄŒlanacaÄŒÄ±nÄ± inceleme.

1.1.2.3 3. EAL (Evaluation Assurance Level) Sertifikasyonu Teorik AÃŒÄ±klama: EAL (DeÄŒerlendirme GÃ¼vencesi Seviyesi), bir Ä±rÄ±nÄ±n belirli gÃ¼venlik gereksinimlerini karŒÄ±lama dÃ¼zeyini gÃ¼sterir. Farklı seviyelerde (EAL1'den EAL7'ye kadar) gÃ¼venlik gÃ¼vencesi saÄŒlar.

- **EAL Seviyeleri:**
 - **EAL1:** Fonksiyonel olarak test edilmiÄŒ.
 - **EAL2:** YapÄ±sal olarak test edilmiÄŒ.
 - **EAL3:** Metodolojik olarak test edilmiÄŒ ve denetlenmiÄŒ.
 - **EAL4:** TasarÄ±m bazÄ±nda gÃ¼zden geÃŒirilmÄŒ, metodolojik olarak test edilmiÄŒ.
 - **EAL5:** YÄŒksek gÃ¼vence saÄŒlayan, semantik olarak analiz edilmiÄŒ.
 - **EAL6 ve EAL7:** Son derece yÄŒksek gÃ¼venlik seviyesi, matematiksel olarak kanÄ±tlanmÄ±ÄŒ.

Uygulama Ä±rnekleri:

1. EAL sertifikasyon sÃ¼recinin nasÄ±l iÄŒlediÄŒini araŒtÄ±rma.
2. EAL seviyelerine gÃ¼re bir sistemin gÃ¼venliÄŒini deÄŒerlendirme.

1.1.2.4 4. Penetrasyon Testi (PenTest) PlanlarÄ± Teorik AÃŒÄ±klama: Penetrasyon testi, bir sistemin zayıf noktalarÄ±nÄ± ve gÃ¼venlik aÃŒÄ±klarÄ±nÄ± belirlemek iŒin gerÄŒekleŒtirilen saldÄ±rÄ± simÃ¼lasyonlarÄ±dÄ±r. Penetrasyon testi planlarÄ±, test edilecek alanlarÄ±, metodolojiyi, hedefleri ve sÃ¼reci iŒerir.

- **Neden Penetrasyon Testi YapÄ±lÄ±r?**
 - GÃ¼venlik aÃŒÄ±klarÄ±nÄ± tespit etmek.
 - GerÄŒek dÃ¼nya saldÄ±rÄ±larÄ±na karŒÄ± sistemi test etmek.

- Zayıf noktalar belirlenerek savunma mekanizmaları geliştirilerek güçlendirilmek.
- Sistem güvenliğini proaktif bir şekilde artırmak.

PenTest Sırası Adımları:

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

Uygulama Örnekleri:

1. Bir web uygulamasının penetrasyon testi planı oluşturma.
2. Gerçek dünya saldırıları ve simüle ederek bir sistemin güvenlik açıkları analiz etme.

1.1.2.5 5. Penetrasyon Testi Yöntemleri Teorik Aşakı: Penetrasyon testi yöntemleri, test edilecek sistemin türüne ve saldırı hedeflerine göre de ayrılır. Bazı yaygın test yöntemleri şunlardır:

- **Beyaz Kutu (Whitebox) Testi:** Test eden kişi, sistemin iş yapışları ve kaynak kodunu bilir.
- **Kara Kutu (Blackbox) Testi:** Test eden kişi, sistem hakkında hiçbir bilgiye sahip değildir. Saldırıları dâhil olarak gerçeğe yakındır.
- **Gri Kutu (Graybox) Testi:** Test eden kişi, sistemin bazı bileşimleri hakkında bilgi sahibidir. Örneğin, uygulama yapışları 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 gerçeğe yakındır sonuçları raporlama.

1.1.2.6 6. Penetrasyon Testi Araşları Teorik Aşakı: Penetrasyon testleri sırasında seçitli araçları kullanarak sistemin zayıf noktaları analiz edilir. Bu araçları, testin kapsamına ve hedeflerine göre seçilir.

- **Nessus:** Zayıf nokta taraması için kullanılan popüler bir araçtır.
- **Metasploit:** Güvenlik açıkları ve istismarı edilmesi ve zayıflıkları test edilmesi için kullanılan bir çerçeve.
- **Wireshark:** Ağı trafiğini izlemek ve analiz etmek için kullanılan araçtır.
- **Burp Suite:** Web uygulamalarında güvenlik testi yapmak için kullanılan bir araçtır.
- **OWASP ZAP:** Web uygulamalarında güvenlik açıkları tespit etmek için kullanılan açık kaynak bir araçtır.

Uygulama Örnekleri:

1. **Nessus** kullanarak bir sistemin güvenlik açıkları tarama.
2. **Metasploit** kullanarak bir güvenlik açıkları üzerinden yararlanma ve sonuçları analiz etme.

1.1.2.7 7. Penetrasyon Testi ve Sertifikasyon Öliki Teorik Aşakı: Penetrasyon testi sonuçları, bir sistemin güvenlik sertifikasyonu sırasında önemli bir rol oynar. Sertifikasyon sağlayıcıları, bir sistemin güvenliğini doğrulamak için genellikle penetrasyon testi sonuçları ve güvenli kaynak bir araçtır.

- **Nasıl Öliki?**
 - PenTest sonuçları, sertifikasyon sürecine eklenir ve güvenlik seviyesi kanıtlanır.
 - Güvenlik sertifikası almak için belirli testlerin başarıyla geçilmesi gerekir.

- Penetrasyon testleri, sertifika uyumluluđunu sađlamak iđiñin dđzenli olarak yapđlđr.

Uygulama Ėrnekleri:

1. Penetrasyon testi sonuđlarıñn sertifikasyon sađrecine nasđl entegre edebileceđimizi analiz etme.
2. Sertifikasyon gereksinimlerine uygun bir gđvenlik testi planđ hazırlama.

1.1.3 Sonuđ

Bu hafta, gđvenlik sertifikasyonlarđn ve penetrasyon testlerinin sistem gđvenliđi Ėzerindeki etkilerini inceledik. Gđvenlik sertifikalarđ, uluslararası standartlara uyumluluđu gđsterirken, penetrasyon testleri bir sistemin zayıf noktalarđn ortaya đđkararak gđvenliđini artırdı. Bu iki sađređ, yazđlđm ve donanđm Ėrđnlerinin gđvenlik seviyesini artırmak iđiñin birlikte đđsalđđ.

11. Hafta – Sonu