

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±nemi, 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.

¹pandoc_cen429-week-11.pdf

²pandoc_cen429-week-11.docx

³cen429-week-11.pdf

⁴cen429-week-11.pptx

1.1.2.1 1. GÃ¼venlik SertifikalarÄ±nÄ±n Ä±nemli Teorik AÄŒÄ±klama: GÃ¼venlik sertifikalarÄ±, bir sistemin veya Ä±rÄ±nÄ±n belirli gÃ¼venlik standartlarÄ±na uyduÄ±yunu gÃ¼sterir. Sertifikalar, genellikle bir Ä±rÄ±nÄ±n kullanÄ±cÄ±lara gÃ¼ven verdiÄ±yini ve gÃ¼venlik aÄŒÄ±sÄ±ndan belirli testlerden geÄŒtiÄ±yini belirtir.

- **Neden Ä±nemli?**
 - GÃ¼venilirlik saÄ±ylar.
 - Uluslararası standartlara uygunluÄ±yü gÃ¼sterir.
 - RegÃ¼lasyon ve yasal uyum gereksinimlerini karÄ±yÄ±lar.
 - ÄcerÄ±nlerin gÃ¼venlik seviyesini artÄ±rÄ±r.
 - KullanÄ±cÄ±lar ve mÄ±Ä±terilere gÃ¼ven verir.

Uygulama Ä±rneklere:

1. Bir sistemin neden gÃ¼venlik sertifikasÄ±na ihtiyaÄŒ duyduÄ±yuna dair bir analiz yapma.
2. GÃ¼venlik sertifikalarÄ±nÄ±n ticari Ä±rÄ±nler Ä±zerindeki etkilerini inceleme.

1.1.2.2 2. YaygÄ±n GÃ¼venlik SertifikalarÄ± ve Standartlar Teorik AÄŒÄ±klama: BirÄŒok gÃ¼venlik standardÄ± ve sertifikasyon, donanÄ±m ve yazÄ±lÄ±m Ä±rÄ±nlerinin gÃ¼venliÄ±yini saÄ±lamak iÄŒin kullanÄ±lan standart. Bu standartlar, Ä±rÄ±nlerin nasÄ±l test edilmesi ve sertifikalandÄ±rÄ±lmasÄ± gerektiÄ±yine dair rehberlik eder.

- **ETSI (European Telecommunications Standards Institute):** TelekomÄ±nikasyon ve aÄ±y gÃ¼venliÄ±yini standartlarÄ±nÄ± belirler.
- **EMV (Europay, MasterCard, Visa):** Kart tabanlı Ä±deme sistemlerinin gÃ¼venliÄ±yini saÄ±lamak iÄŒin kullanÄ±lan standart.
- **GSMA:** Mobil cihazlar ve aÄ±lar iÄŒin gÃ¼venlik standartlarÄ±.
- **ISO/IEC 27001:** Bilgi gÃ¼venliÄ±yini yÄ±netim sistemleri standardÄ±.
- **PCI DSS (Payment Card Industry Data Security Standard):** Ä±deme kartÄ± bilgilerinin gÃ¼venliÄ±yini saÄ±lamak iÄŒin kullanÄ±lan standart.

Uygulama Ä±rneklere:

1. ETSI standartlarÄ±na gÃ¼re bir aÄ±y gÃ¼venliÄ±yini planÄ± oluÄ±turma.
2. PCI DSS uyumluluÄ±yunun bir Ä±deme sistemi iÄŒin nasÄ±l saÄ±lanacaÄ±yÄ±nÄ± inceleme.

1.1.2.3 3. EAL (Evaluation Assurance Level) Sertifikasyonu Teorik AÄŒÄ±klama: EAL (DeÄ±ylerlendirme GÃ¼vencesi Seviyesi), bir Ä±rÄ±nÄ±n belirli gÃ¼venlik gereksinimlerini karÄ±yÄ±lama dÄ±zeyini gÃ¼sterir. Farklı seviyelerde (EAL1'den EAL7'ye kadar) gÃ¼venlik gÃ¼vencesi saÄ±ylar.

- **EAL Seviyeleri:**
 - **EAL1:** Fonksiyonel olarak test edilmiÄ±y.
 - **EAL2:** YapÄ±sal olarak test edilmiÄ±y.
 - **EAL3:** Metodolojik olarak test edilmiÄ±y ve denetlenmiÄ±y.
 - **EAL4:** TasarÄ±m bazÄ±nda gÃ¼zden geÄŒirilmÄ±y, metodolojik olarak test edilmiÄ±y.
 - **EAL5:** YÄ±ksek gÃ¼vence saÄ±layan, semantik olarak analiz edilmiÄ±y.
 - **EAL6 ve EAL7:** Son derece yÄ±ksek gÃ¼venlik seviyesi, matematiksel olarak kanÄ±tlanmÄ±Ä±y.

Uygulama Ä±rneklere:

1. EAL sertifikasyon saÄ±recinin nasÄ±l iÄ±lediÄ±yini araÄ±tÄ±rma.
2. EAL seviyelerine gÃ¼re bir sistemin gÃ¼venliÄ±yini deÄ±ylerlendirme.

1.1.2.4 4. Penetrasyon Testi (PenTest) PlanlarÄ± Teorik AÄŒÄ±klama: Penetrasyon testi, bir sistemin zayıf noktalarÄ±nÄ± ve gÃ¼venlik aÄŒÄ±klarÄ±nÄ± belirlemek iÄŒin gerÄŒekleÄ±tirilen saldÄ±rÄ± simÃ¼lasyonlarÄ±dÄ±r. Penetrasyon testi planlarÄ±, test edilecek alanlarÄ±, metodolojiyi, hedefleri ve saÄ±reci iÄŒerir.

- **Neden Penetrasyon Testi YapÄ±lanÄ±r?**
 - GÃ¼venlik aÄŒÄ±klarÄ±nÄ± tespit etmek.
 - GerÄŒek dÄ±nya saldÄ±rÄ±larÄ±na karÄ±yÄ± sistemi test etmek.

- Zayıf noktaları belirleyerek savunma mekanizmalarını güçlendirmek.
- Sistem güvenliğini proaktif bir şekilde artırmak.

PenTest Sırası 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 yetkili haklarına erişim sağlama.
5. **Erişimi Koruma (Maintaining Access):** Sızmanın kalıcılığı hale getirilmesi.
6. **Kanıt Toplama (Evidence Collection):** Bulunan güvenlik açıklarının belgelenmesi.

Uygulama Örnekleri:

1. Bir web uygulamasının penetrasyon testi planı oluşturma.
2. Gerçek dünyaya saldırılarının simüle edilerek bir sistemin güvenlik açıklarının analizi.

1.1.2.5 5. Penetrasyon Testi Yöntemleri Teorik Açıklama: Penetrasyon testi yöntemleri, test edilecek sistemin türüne ve saldırı hedeflerine göre deyişlik gösterir. Bazı yaygın test yöntemleri şunlardır:

- **Beyaz Kutu (Whitebox) Testi:** Test eden kişi, sistemin iş yapış tarzını ve kaynak kodunu bilir.
- **Kara Kutu (Blackbox) Testi:** Test eden kişi, sistem hakkında hiçbir bilgiye sahip değildir. Saldırılar dâğır gerçeyle yapılır.
- **Gri Kutu (Graybox) Testi:** Test eden kişi, sistemin bazı bileşenleri hakkında bilgi sahibidir. Örneğın, uygulama yapış tarzı 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 gerçeyle tirerek sonuçları raporlama.

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

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

Uygulama Örnekleri:

1. Nessus kullanarak bir sistemin güvenlik açıklarının taraması.
2. Metasploit kullanarak bir güvenlik açıklarından yararlanma ve sonuçları analiz etme.

1.1.2.7 7. Penetrasyon Testi ve Sertifikasyon Ölişikisi Teorik Açıklama: Penetrasyon testi sonuçları, bir sistemin güvenlik sertifikasyonu sürecinde önemli bir rol oynar. Sertifikasyon sağlayıcıları, bir sistemin güvenliğini doğrulamak için genellikle penetrasyon testi sonuçları gâz önünde bulundurulur.

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

– Penetrasyon testleri, sertifika uyumluluđunu sađlamak iđin dđzenli olarak yapđlđr.

Uygulama Ėrnekleri:

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

1.1.3 Sonuđ

Bu hafta, gđvenlik sertifikasyonlarđnđ ve penetrasyon testlerinin sistem gđvenliđi Ėzerindeki etkilerini inceledik. Gđvenlik sertifikalarđ, uluslararası standartlara uyumluluđu gđsterirken, penetrasyon testleri bir sistemin zayıf noktalarđnđ ortaya đđkararak gđvenliđini artđrđr. Bu iki sađređ, yazđlđm ve donanđm Ėrneklerinin gđvenlik seviyesini artđrmak iđin birlikte đđlđr.

11.Hafta – Sonu