CE407 Güvenli Programlama Hafta-11

Güvenlik Sertifikaları ve Penetrasyon Testi Planları

Yazar: Dr. UÄŸur CORUH

İçindekiler

1	l CE407 G Λ^4 venli Programlama		
	1.1	Hafta-	11
		1.1.1	Outline
		1.1.2	Hafta-11: Güvenlik Sertifikaları ve Penetrasyon Testi Planları 1
		1.1.3	Sonuç

Şekil Listesi

Tablo Listesi

1 CE407 GÃ¹/₄venli Programlama

1.1 Hafta-11

1.1.0.1 Gývenlik Sertifikaları ve Penetrasyon Testi Planları İndir PDF¹, DOCX², SLIDE³, PPTX⁴

1.1.1 Outline

- Gývenlik Sertifikalarının Ã-nemi
- Penetrasyon Testi Planları ve Araçları
- Sertifikasyon Süreçleri ve İliÅŸkiler

1.1.2 Hafta-11: GÃ¹/₄venlik Sertifikaları ve Penetrasyon Testi Planları

Bu haftanÄ \pm n amacÄ \pm , gÃ 4 venlik sertifikasyonlarÄ \pm nÄ \pm n önemini, kullanÄ \pm lan standartlarÄ \pm ve sÄ \pm zma testi (Penetrasyon Testi) sÃ 4 vençlerinin nasÄ \pm l planlandÄ \pm ÄŸÄ \pm nÄ \pm öÄŸrenmektir. GÃ 4 venlik sertifikalarÄ \pm , yazÄ \pm lÄ \pm m ve donanÄ \pm mÄ \pm n gÃ 4 venlikÄŸinin uluslararasÄ \pm standartlara uygunluğunu gösterirken, penetrasyon testleri sistemin gÃ 4 venlik açÄ \pm klarÄ \pm nÄ \pm belirleyip olasÄ \pm tehditleri analiz etmemizi saÄŸlar.

1.1.2.1 1. Güvenlik SertifikalarınñnÖnemi Teorik Açıklama: Güvenlik sertifikaları, bir sistemin veya ürünün belirli güvenlik standartlarına uyduÄŸunu gösterir. Sertifikalar, genellikle bir ürünün kullanıcılara güven verdiÄŸini ve güvenlik açısından belirli testlerden geçtiÄŸini belirtir.

• Neden Ã-nemli?

-G
Ã 1 4venilirlik sa Ä Ÿlar.

 $^{^{1}\}mathrm{ce}407\text{-}\mathrm{week-}11.\mathrm{tr}\underline{}\mathrm{doc.pdf}$

 $^{^2{\}rm ce}407{\rm -week\text{-}}11.{\rm tr_word.docx}$

 $^{^3}$ ce407-week-11.tr_slide.pdf

⁴ce⁴07-week-11.tr slide.pptx

- Uluslararası standartlara uygunluÄŸu gösterir.
- Regülasyon ve yasal uyum gereksinimlerini karşılar.
- \tilde{A} er \tilde{A} ¹/4nlerin g \tilde{A} ¹/4venlik seviyesini art $\ddot{A}\pm r\ddot{A}\pm r$.
- Kullanıcılar ve müÅŸterilere güven verir.

Uygulama Ã-rnekleri:

- 1. Bir sistemin neden gývenlik sertifikasına ihtiyaç duyduÄŸuna dair bir analiz yapma.
- 2. Güvenlik sertifikalarının ticari ürünler üzerindeki etkilerini inceleme.
- 1.1.2.2 2. Yayg $\ddot{A}\pm n$ G \tilde{A}^{1} /venlik Sertifikalar $\ddot{A}\pm$ ve Standartlar Teorik A \tilde{A} § $\ddot{A}\pm$ klama: Bir \tilde{A} §ok g \tilde{A}^{1} /venlik standard $\ddot{A}\pm$ ve sertifikasyon, donan $\ddot{A}\pm m$ ve yaz $\ddot{A}\pm l\ddot{A}\pm m$ \tilde{A}^{1} /4r \tilde{A}^{1} /vnlerinin g \tilde{A}^{1} /venli \ddot{A} Vini sa \ddot{A} Vilamak i \tilde{A} §in kullan $\ddot{A}\pm l\ddot{A}\pm r$. Bu standartlar, \tilde{A}^{1} /4r \tilde{A}^{1} /vnlerin nas $\ddot{A}\pm l$ test edilmesi ve sertifikaland $\ddot{A}\pm r\ddot{A}\pm l$ mas $\ddot{A}\pm g$ erekti \ddot{A} Vine dair rehberlik eder.
 - ETSI (European Telecommunications Standards Institute): Telekomünikasyon ve aÄŸ güvenliÄŸi standartlarını belirler.
 - EMV (Europay, MasterCard, Visa): Kart tabanlı ödeme sistemlerinin güvenliÄŸini saÄŸ-lamak için kullanılan standart.
 - **GSMA:** Mobil cihazlar ve ağlar için gù⁄4venlik standartları.
 - ISO/IEC 27001: Bilgi güvenliÄŸi yönetim sistemleri standardı.
 - PCI DSS (Payment Card Industry Data Security Standard): Ã-deme kartı bilgilerinin güvenliÄŸini saÄŸlamak için kullanılan standart.

Uygulama Ã-rnekleri:

- 1. ETSI standartlarına göre bir aÄŸ güvenliÄŸi planı oluÅŸturma.
- 2. PCI DSS uyumlulu ÄYunun bir $\tilde{A}\P$ deme sistemi i \tilde{A} §in nas Ä \pm l sa ÄYlanaca ÄYÄ \pm n Ä \pm inceleme.
- **1.1.2.3 3. EAL (Evaluation Assurance Level) Sertifikasyonu Teorik Açıklama:** EAL (Değerlendirme Gù¼vencesi Seviyesi), bir ù¼rù¼nù¼n belirli gù¼venlik gereksinimlerini karşılama dù¼zeyini gösterir. Farklı seviyelerde (EAL1'den EAL7'ye kadar) gù¼venlik gù¼vencesi saÄŸlar.
 - EAL Seviyeleri:
 - EAL1: Fonksiyonel olarak test edilmiÅŸ.
 - EAL2: Yapısal olarak test edilmiÅŸ.
 - EAL3: Metodolojik olarak test edilmiÅŸ ve denetlenmiÅŸ.
 - EAL4: Tasarım bazında gözden geçirilmiÅŸ, metodolojik olarak test edilmiÅŸ.
 - EAL5: Yüksek güvence saÄŸlayan, semantik olarak analiz edilmiÅŸ.
 - EAL6 ve EAL7: Son derece yüksek güvenlik seviyesi, matematiksel olarak kanıtlanmıÅŸ.

Uygulama Ã-rnekleri:

- 1. EAL sertifikasyon sürecinin nasıl iÅŸlediÄŸini araÅŸtırma.
- 2. EAL seviyelerine göre bir sistemin güvenliÄŸini deÄŸerlendirme.
- 1.1.2.4 4. Penetrasyon Testi (PenTest) Planlar \ddot{A} Teorik $A\tilde{A}$ \ddot{A} \pm klama: Penetrasyon testi, bir sistemin zay \ddot{A} \pm f noktalar \ddot{A} \pm n \ddot{A} \pm ve g \tilde{A} \pm 4venlik a \tilde{A} \pm 8 \ddot{A} \pm 4klar \ddot{A} \pm 8 belirlemek i \tilde{A} \pm 8 in ger \tilde{A} \pm 8 kler \ddot{A} \pm 9 test edilecek alanlar \ddot{A} \pm 4, metodolojiyi, hedefleri ve s \tilde{A} \pm 4reci i \tilde{A} \pm 9 reir.
 - Neden Penetrasyon Testi Yapılır?
 - Güvenlik açıklarını tespit etmek.
 - Gerçek dünya saldırılarına karşı sistemi test etmek.
 - $Zay\ddot{A}\pm f$ noktalar $\ddot{A}\pm$ belirleyerek savunma mekanizmalar $\ddot{A}\pm n\ddot{A}\pm g\tilde{A}^{1/4}\tilde{A}$ §lendirmek.
 - Sistem güvenliÄŸini proaktif bir ÅŸekilde artırmak.

PenTest SÃ¹/₄reç Adımları:

- 1. **KeÅŸif (Reconnaissance):** Sistem hakkında bilgi toplama.
- 2. Tarama (Scanning): Aªık portlar, hizmetler ve zayıflıklar tespit edilir.

- 3. **Sistem İstismarı (Exploitation):** Tespit edilen zayıflıklardan yararlanarak sisteme sızma.
- 4. Avantaj Sağlama (Privilege Escalation): Sistemde yönetici haklarına eriÅŸim saÄŸlama.
- 5. Erişimi Koruma (Maintaining Access): Sızmanın kalıcı hale getirilmesi.
- 6. Kanıt Toplama (Evidence Collection): Bulunan gù4venlik açıklarının belgelenmesi.

Uygulama Ã-rnekleri:

- 1. Bir web uygulamas $\ddot{A}\pm i\tilde{A}$ şin penetrasyon testi plan $\ddot{A}\pm$ olu \ddot{A} Ÿturma.
- 2. Gerħek dünya saldırılarını simüle ederek bir sistemin güvenlik açıklarını analiz etme.
- **1.1.2.5 5. Penetrasyon Testi Yà ¶ntemleri Teorik Aà §Ä±klama:** Penetrasyon testi yà ¶ntemleri, test edilecek sistemin tà ¼rà ¼ne ve saldırı hedeflerine gà ¶re deÄŸiÅŸiklik gà ¶sterir. Bazı yaygın test yà ¶ntemleri ÅŸunlardır:
 - Beyaz Kutu (Whitebox) Testi: Test eden kiÅŸi, sistemin iç yapısını ve kaynak kodunu bilir.
 - Kara Kutu (Blackbox) Testi: Test eden kiÅŸi, sistem hakkında hiçbir bilgiye sahip deÄŸildir. Saldırılar dıÅŸarıdan gerçekleÅŸtirilir.
 - Gri Kutu (Graybox) Testi: Test eden kiÅŸi, sistemin bazı bölümleri hakkında bilgi sahibidir. Ã-rneÄŸin, uygulama yapısına veya kullanıcı rollerine dair bilgiye sahiptir.

Uygulama Ã-rnekleri:

- 1. Beyaz kutu ve kara kutu testi arasındaki farkları analiz etme.
- 2. Bir sistem Ź/4zerinde gri kutu testi ger§ekleÄŸtirerek sonu§ları raporlama.
- 1.1.2.6 6. Penetrasyon Testi Ara \tilde{A} şlar \ddot{A} \pm Teorik A \tilde{A} ş \ddot{A} \pm klama: Penetrasyon testleri s \ddot{A} \pm ras \ddot{A} \pm nda \tilde{A} şe \dot{A} \ddot{Y} itli ara \tilde{A} şlar kullan \ddot{A} \pm larak sistemin zay \ddot{A} \pm f noktalar \ddot{A} \pm analiz edilir. Bu ara \tilde{A} şlar, testin kapsam \ddot{A} \pm na ve hedeflerine g \tilde{A} ¶re se \tilde{A} şlir.
 - Nessus: Zayıf nokta taraması için kullanılan popüler bir araçtır.
 - Metasploit: Güvenlik açıklarının istismar edilmesi ve zayıflıkların test edilmesi için kullanılan bir çerçeve.
 - Wireshark: $A\ddot{A}\ddot{Y}$ trafi $\ddot{A}\ddot{Y}$ ini izlemek ve analiz etmek i \ddot{A} §in kullan $\ddot{A}\pm l\ddot{A}\pm r$.
 - 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 Ã-rnekleri:

- 1. **Nessus** kullanarak bir sistemin güvenlik açıklarını tarama.
- 2. **Metasploit** kullanarak bir güvenlik açığından yararlanma ve sonuçlarını analiz etme.
- 1.1.2.7 7. Penetrasyon Testi ve Sertifikasyon İliÅŸkisi Teorik AçÄ \pm klama: Penetrasyon testi sonuçlarÄ \pm , bir sistemin güvenlik sertifikasyonu sürecinde önemli bir rol oynar. Sertifikasyon saÄŸlayÄ \pm cÄ \pm larÄ \pm , bir sistemin güvenliÄŸini doÄŸrulamak için genellikle penetrasyon testi sonuçlarÄ \pm nÄ \pm göz önünde bulundurur.
 - Nasıl İliÅŸkilidir?
 - PenTest sonuħları, sertifikasyon sürecine eklenir ve güvenlik seviyesi kanıtlanır.
 - Güvenlik sertifikası almak için belirli testlerin baÅŸarıyla geçilmesi gerekir.
 - Penetrasyon testleri, sertifika uyumluluÄŸunu saÄŸlamak için dÃ⅓zenli olarak yapılır.

Uygulama Ã-rnekleri:

- 1. Penetrasyon testi sonu Ã \S lar
Ä \pm nÄ \pm sertifikasyon sÃ 1 4recine nasÄ \pm l entegre edebilece Ä Ÿimizi analiz etme.
- 2. Sertifikasyon gereksinimlerine uygun bir güvenlik testi planı hazırlama.

1.1.3 Sonuç

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

11. Hafta-Sonu