CEN429 GÃ¼venli Programlama Hafta-11

GÃ¼venlik SertifikalarÄ± ve Penetrasyon Testi PlanlarÄ±

Yazar: Dr. UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-11

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

- PDF[1]
- DOC[2]
- SLIDE[3]
- PPTX[4]

1.1.1 Outline

- GÃ¼venlik SertifikalarÄ±nÄ±n Ã–nemi
- Penetrasyon Testi PlanlarÄ± ve AraÃ§larÄ±
- Sertifikasyon SÃ¼reÃ§leri ve Ä°liÅŸkiler

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

Bu haftanÄ±n amacÄ±, gÃ¼venlik sertifikasyonlarÄ±nÄ±n Ã¶nemini, kullanÄ±lan standartlarÄ± ve sÄ±zma testi (Penetrasyon Testi) sÃ¼reÃ§lerinin nasÄ±l planlandÄ±ÄŸÄ±nÄ± Ã¶ÄŸrenmektir. GÃ¼venlik sertifikalarÄ±, yazÄ±lÄ±m ve donanÄ±mÄ±n gÃ¼venliÄŸinin uluslararasÄ± standartlara uygunluÄŸunu gÃ¶sterirken, penetrasyon testleri sistemin gÃ¼venlik aÃ§Ä±klarÄ±nÄ± belirleyip olasÄ± tehditleri analiz etmemizi saÄŸlar.

[1] pandoc_cen429-week-11.tr_doc.pdf
[2] pandoc_cen429-week-11.tr_word.docx
[3] cen429-week-11.tr_slide.pdf
[4] cen429-week-11.tr_slide.pptx

1.1.2.1 1. GÃ¼venlik SertifikalarÄ±nÄ±n Ã–nemi Teorik AÃ§Ä±klama: GÃ¼venlik sertifikalarÄ±, bir sistemin veya Ã¼rÃ¼nÃ¼n belirli gÃ¼venlik standartlarÄ±na uyduÄŸunu gÃ¶sterir. Sertifikalar, genellikle bir Ã¼rÃ¼nÃ¼n kullanÄ±cÄ±lara gÃ¼ven verdiÄŸini ve gÃ¼venlik aÃ§Ä±sÄ±ndan belirli testlerden geÃ§tiÄŸini belirtir.

- **Neden Ã–nemli?**
  - GÃ¼venilirlik saÄŸlar.
  - UluslararasÄ± standartlara uygunluÄŸu gÃ¶sterir.
  - RegÃ¼lasyon ve yasal uyum gereksinimlerini karÅŸÄ±lar.
  - ÃœrÃ¼nlerin gÃ¼venlik seviyesini artÄ±rÄ±r.
  - KullanÄ±cÄ±lar ve mÃ¼ÅŸterilere gÃ¼ven verir.

Uygulama Ã–rnekleri:

1. Bir sistemin neden gÃ¼venlik sertifikasÄ±na ihtiyaÃ§ duyduÄŸuna dair bir analiz yapma.
2. GÃ¼venlik sertifikalarÄ±nÄ±n ticari Ã¼rÃ¼nler Ã¼zerindeki etkilerini inceleme.

1.1.2.2 2. YaygÄ±n GÃ¼venlik SertifikalarÄ± ve Standartlar Teorik AÃ§Ä±klama: BirÃ§ok gÃ¼venlik standardÄ± ve sertifikasyon, donanÄ±m ve yazÄ±lÄ±m Ã¼rÃ¼nlerinin gÃ¼venliÄŸini saÄŸlamak iÃ§in kullanÄ±lÄ±r. Bu standartlar, Ã¼rÃ¼nlerin nasÄ±l test edilmesi ve sertifikalandÄ±rÄ±lmasÄ± gerektiÄŸine dair rehberlik eder.

- **ETSI (European Telecommunications Standards Institute):** TelekomÃ¼nikasyon ve aÄŸ gÃ¼venliÄŸi standartlarÄ±nÄ± belirler.
- **EMV (Europay, MasterCard, Visa):** Kart tabanlÄ± Ã¶deme sistemlerinin gÃ¼venliÄŸini saÄŸlamak iÃ§in kullanÄ±lan standart.
- **GSMA:** Mobil cihazlar ve aÄŸlar iÃ§in gÃ¼venlik standartlarÄ±.
- **ISO/IEC 27001:** Bilgi gÃ¼venliÄŸi yÃ¶netim sistemleri standardÄ±.
- **PCI DSS (Payment Card Industry Data Security Standard):** Ã–deme kartÄ± bilgilerinin gÃ¼venliÄŸini saÄŸlamak iÃ§in kullanÄ±lan standart.

Uygulama Ã–rnekleri:

1. ETSI standartlarÄ±na gÃ¶re bir aÄŸ gÃ¼venliÄŸi planÄ± oluÅŸturma.
2. PCI DSS uyumluluÄŸunun bir Ã¶deme sistemi iÃ§in nasÄ±l saÄŸlanacaÄŸÄ±nÄ± inceleme.

1.1.2.3 3. EAL (Evaluation Assurance Level) Sertifikasyonu Teorik AÃ§Ä±klama: EAL (DeÄŸerlendirme GÃ¼vencesi Seviyesi), bir Ã¼rÃ¼nÃ¼n belirli gÃ¼venlik gereksinimlerini karÅŸÄ±lama dÃ¼zeyini gÃ¶sterir. FarklÄ± seviyelerde (EAL1'den EAL7'ye kadar) gÃ¼venlik gÃ¼vencesi saÄŸlar.

- **EAL Seviyeleri:**
  - **EAL1:** Fonksiyonel olarak test edilmiÅŸ.
  - **EAL2:** YapÄ±sal olarak test edilmiÅŸ.
  - **EAL3:** Metodolojik olarak test edilmiÅŸ ve denetlenmiÅŸ.
  - **EAL4:** TasarÄ±m bazÄ±nda gÃ¶zden geÃ§irilmiÅŸ, metodolojik olarak test edilmiÅŸ.
  - **EAL5:** YÃ¼ksek gÃ¼vence saÄŸlayan, semantik olarak analiz edilmiÅŸ.
  - **EAL6 ve EAL7:** Son derece yÃ¼ksek gÃ¼venlik seviyesi, matematiksel olarak kanÄ±tlanmÄ±ÅŸ.

Uygulama Ã–rnekleri:

1. EAL sertifikasyon sÃ¼recinin nasÄ±l iÅŸlediÄŸini araÅŸtÄ±rma.
2. EAL seviyelerine gÃ¶re bir sistemin gÃ¼venliÄŸini deÄŸerlendirme.

1.1.2.4 4. Penetrasyon Testi (PenTest) PlanlarÄ± Teorik AÃ§Ä±klama: Penetrasyon testi, bir sistemin zayÄ±f noktalarÄ±nÄ± ve gÃ¼venlik aÃ§Ä±klarÄ±nÄ± belirlemek iÃ§in gerÃ§ekleÅŸtirilen saldÄ±rÄ± simÃ¼lasyonlarÄ±dÄ±r. Penetrasyon testi planlarÄ±, test edilecek alanlarÄ±, metodolojiyi, hedefleri ve sÃ¼reci iÃ§erir.

- **Neden Penetrasyon Testi YapÄ±lÄ±r?**
  - GÃ¼venlik aÃ§Ä±klarÄ±nÄ± tespit etmek.
  - GerÃ§ek dÃ¼nya saldÄ±rÄ±larÄ±na karÅŸÄ± sistemi test etmek.

- ZayÄ±f noktalarÄ± belirleyerek savunma mekanizmalarÄ±nÄ± gÃ¼Ã§lendirmek.
- Sistem gÃ¼venliÄŸini proaktif bir ÅŸekilde artÄ±rmak.

PenTest SÃ¼reÃ§ AdÄ±mlarÄ±:

1. **KeÅŸif (Reconnaissance):** Sistem hakkÄ±nda bilgi toplama.
2. **Tarama (Scanning):** AÃ§Ä±k portlar, hizmetler ve zayÄ±flÄ±klar tespit edilir.
3. **Sistem Ä°stismarÄ± (Exploitation):** Tespit edilen zayÄ±flÄ±klardan yararlanarak sisteme sÄ±zma.
4. **Avantaj SaÄŸlama (Privilege Escalation):** Sistemde yÃ¶netici haklarÄ±na eriÅŸim saÄŸlama.
5. **EriÅŸimi Koruma (Maintaining Access):** SÄ±zmanÄ±n kalÄ±cÄ± hale getirilmesi.
6. **KanÄ±t Toplama (Evidence Collection):** Bulunan gÃ¼venlik aÃ§Ä±klarÄ±nÄ±n belgelenmesi.

Uygulama Ã–rnekleri:

1. Bir web uygulamasÄ± iÃ§in penetrasyon testi planÄ± oluÅŸturma.
2. GerÃ§ek dÃ¼nya saldÄ±rÄ±larÄ±nÄ± simÃ¼le ederek bir sistemin gÃ¼venlik aÃ§Ä±klarÄ±nÄ± analiz etme.

1.1.2.5 5. Penetrasyon Testi YÃ¶ntemleri Teorik AÃ§Ä±klama: Penetrasyon testi yÃ¶ntemleri, test edilecek sistemin tÃ¼rÃ¼ne ve saldÄ±rÄ± hedeflerine gÃ¶re deÄŸiÅŸiklik gÃ¶sterir. BazÄ± yaygÄ±n test yÃ¶ntemleri ÅŸunlardÄ±r:

- **Beyaz Kutu (Whitebox) Testi:** Test eden kiÅŸi, sistemin iÃ§ yapÄ±sÄ±nÄ± ve kaynak kodunu bilir.
- **Kara Kutu (Blackbox) Testi:** Test eden kiÅŸi, sistem hakkÄ±nda hiÃ§bir bilgiye sahip deÄŸildir. SaldÄ±rÄ±lar dÄ±ÅŸarÄ±dan gerÃ§ekleÅŸtirilir.
- **Gri Kutu (Graybox) Testi:** Test eden kiÅŸi, sistemin bazÄ± bÃ¶lÃ¼mleri hakkÄ±nda bilgi sahibidir. Ã–rneÄŸin, uygulama yapÄ±sÄ±na veya kullanÄ±cÄ± rollerine dair bilgiye sahiptir.

Uygulama Ã–rnekleri:

1. Beyaz kutu ve kara kutu testi arasÄ±ndaki farklarÄ± analiz etme.
2. Bir sistem Ã¼zerinde gri kutu testi gerÃ§ekleÅŸtirerek sonuÃ§larÄ± raporlama.

1.1.2.6 6. Penetrasyon Testi AraÃ§larÄ± Teorik AÃ§Ä±klama: Penetrasyon testleri sÄ±rasÄ±nda Ã§eÅŸitli araÃ§lar kullanÄ±larak sistemin zayÄ±f noktalarÄ± analiz edilir. Bu araÃ§lar, testin kapsamÄ±na ve hedeflerine gÃ¶re seÃ§ilir.

- **Nessus:** ZayÄ±f nokta taramasÄ± iÃ§in kullanÄ±lan popÃ¼ler bir araÃ§tÄ±r.
- **Metasploit:** GÃ¼venlik aÃ§Ä±klarÄ±nÄ±n istismar edilmesi ve zayÄ±flÄ±klarÄ±n test edilmesi iÃ§in kullanÄ±lan bir Ã§erÃ§eve.
- **Wireshark:** AÄŸ trafiÄŸini izlemek ve analiz etmek iÃ§in kullanÄ±lÄ±r.
- **Burp Suite:** Web uygulamalarÄ±nda gÃ¼venlik testi yapmak iÃ§in kullanÄ±lan bir araÃ§tÄ±r.
- **OWASP ZAP:** Web uygulamalarÄ±nda gÃ¼venlik aÃ§Ä±klarÄ±nÄ± tespit etmek iÃ§in kullanÄ±lan aÃ§Ä±k kaynak bir araÃ§.

Uygulama Ã–rnekleri:

1. **Nessus** kullanarak bir sistemin gÃ¼venlik aÃ§Ä±klarÄ±nÄ± tarama.
2. **Metasploit** kullanarak bir gÃ¼venlik aÃ§Ä±ÄŸÄ±ndan yararlanma ve sonuÃ§larÄ±nÄ± analiz etme.

1.1.2.7 7. Penetrasyon Testi ve Sertifikasyon Ä°liÅŸkisi Teorik AÃ§Ä±klama: Penetrasyon testi sonuÃ§larÄ±, bir sistemin gÃ¼venlik sertifikasyonu sÃ¼recinde Ã¶nemli bir rol oynar. Sertifikasyon saÄŸlayÄ±cÄ±larÄ±, bir sistemin gÃ¼venliÄŸini doÄŸrulamak iÃ§in genellikle penetrasyon testi sonuÃ§larÄ±nÄ± gÃ¶z Ã¶nÃ¼nde bulundurur.

- **NasÄ±l Ä°liÅŸkilidir?**
  - PenTest sonuÃ§larÄ±, sertifikasyon sÃ¼recine eklenir ve gÃ¼venlik seviyesi kanÄ±tlanÄ±r.
  - GÃ¼venlik sertifikasÄ± almak iÃ§in belirli testlerin baÅŸarÄ±yla geÃ§ilmesi gerekir.

– Penetrasyon testleri, sertifika uyumluluÄŸunu saÄŸlamak iÃ§in dÃ¼zenli olarak yapÄ±lÄ±r.

Uygulama Ã–rnekleri:

1. Penetrasyon testi sonuÃ§larÄ±nÄ± sertifikasyon sÃ¼recine nasÄ±l entegre edebileceÄŸimizi analiz etme.
2. Sertifikasyon gereksinimlerine uygun bir gÃ¼venlik testi planÄ± hazÄ±rlama.

1.1.3 SonuÃ§

Bu hafta, gÃ¼venlik sertifikasyonlarÄ±nÄ±n ve penetrasyon testlerinin sistem gÃ¼venliÄŸi Ã¼zerindeki etkilerini inceledik. GÃ¼venlik sertifikalarÄ±, uluslararasÄ± standartlara uyumluluÄŸu gÃ¶sterirken, penetrasyon testleri bir sistemin zayÄ±f noktalarÄ±nÄ± ortaya Ã§Ä±kararak gÃ¼venliÄŸini artÄ±rÄ±r. Bu iki sÃ¼reÃ§, yazÄ±lÄ±m ve donanÄ±m Ã¼rÃ¼nlerinin gÃ¼venlik seviyesini artÄ±rmak iÃ§in birlikte Ã§alÄ±ÅŸÄ±r.

$11. Hafta - Sonu$