

Genel Bilgiler

Dersin Amacı

Bu dersin amacı, öğrencilere bilgi güvenliği temelleri, ağ güvenliği, saldırı türleri, savunma mekanizmaları, kriptografi ve siber güvenlik politikaları hakkında teorik ve pratik bilgi kazandırmaktır. Öğrenciler, gerçek hayattaki tehdit senaryolarına karşı sistemleri koruma ve test etme yetkinliği kazanırlar.

Dersin İçeriği

Bilgi güvenliği kavramları ve temel ilkeler Siber güvenlik tehditleri ve saldırı türleri Zararlı yazılımlar ve savunma mekanizmaları Güvenli ağ mimarisi Kriptografi ve şifreleme teknikleri Kimlik doğrulama ve erişim denetimi Güvenlik duvarları ve saldırı tespit sistemleri Web güvenliği, SQL injection, XSS, CSRF Sosyal mühendislik saldırıları Güvenlik politikaları ve standartları (ISO 27001, NIST, GDPR) Siber etik ve hukuki boyutlar Güncel siber saldırı örnekleri ve vaka analizleri

Dersin Kitabı / Malzemesi / Önerilen Kaynaklar

Stallings, W. (2023). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson. Çakır, H. (2022). Siber Güvenliğe Giriş. Pusula Yayıncılık.

Planlanan Öğrenme Etkinlikleri ve Öğretme Yöntemleri

Teorik ders anlatımı

Ders İçin Önerilen Diğer Hususlar

Ağ güvenliği ile ilgili ön bilgisi olmalıdır

Dersi Veren Öğretim Elemanı Yardımcıları

Bulunmamaktadır

Dersin Verilişi

Yüz yüze

Dersi Veren Öğretim Elemanları

Öğr. Gör. Dr. Kadir Kesgin

Program Çıktısı

- Bilgi güvenliği ilkelerini ve siber tehdit türlerini açıklar.
- Kriptografi yöntemlerini uygular.
- Güvenli ağ tasarımı ve erişim kontrol mekanizmalarını değerlendirir.
- Web güvenlik açıklarını tanımlar ve savunma tekniklerini uygular.
- Etik hacker araçlarını kullanarak sistem zaafiyetlerini test eder.

Haftalık İçerikler

Sıra	Hazırlık Bilgileri	Laboratuvar	Öğretim Metodları	Teorik	Uygulama
1			Düz Anlatım	Siber güvenliğe giriş ve temel kavramlar	
2			Düz Anlatım	Tehdit türleri ve güvenlik ilkeleri	
3			Düz Anlatım	Zararlı yazılımlar: Virüs, solucan, trojan	
4			Düz Anlatım	Kriptografi temelleri ve algoritmalar	
5			Düz Anlatım	Anahtar yönetimi ve dijital imzalar	
6			Düz Anlatım	Kimlik doğrulama ve erişim denetimi	
7			Düz Anlatım	Güvenli ağ mimarileri	
8			Düz Anlatım	Ara Sınav	
9			Düz Anlatım	Güvenlik duvarları ve IDS/IPS sistemleri	
10			Düz Anlatım	Web uygulama güvenliği: SQLi, XSS, CSRF	
11			Düz Anlatım	Etik hacking ve Kali Linux kullanımı	
12			Düz Anlatım	Sosyal mühendislik ve kullanıcı farkındalığı	
13			Düz Anlatım	Güvenlik politikaları, ISO 27001, GDPR	
14			Düz Anlatım	Güvenlik politikaları, ISO 27001, GDPR	

İş Yükleri

Aktiviteler	Sayısı	Süresi (saat)
Teorik Ders Anlatım	14	3,00
Derse Katılım	14	3,00
Ara Sınav Hazırlık	8	3,00
Final Sınavı Hazırlık	8	3,00

Değerlendirme

Aktiviteler	Ağırlığı (%)
Vize	40,00
Final	60,00

	P.Ç. 1	P.Ç. 2	P.Ç. 3	P.Ç. 4	P.Ç. 5	P.Ç. 6	P.Ç. 7	P.Ç. 8	P.Ç. 9	P.Ç. 10	P.Ç. 11	P.Ç. 12	P.Ç. 13	P.Ç. 14
Ö.Ç. 1														
Ö.Ç. 2														
Ö.Ç. 3														
Ö.Ç. 4														
Ö.Ç. 5														

Tablo :

- P.Ç. 1 :** Öğrenciler temel bilgisayar bilimi kavramlarını anlar, bilgisayar donanımı ve yazılımı hakkında bilgi sahibi olur ve temel ağ teknolojileri ile iletişim protokollerini kavrayarak bu alanlarda yetkinlik kazanır.
- P.Ç. 2 :** Bilgi güvenliği tehditlerini tanıma ve risk değerlendirme becerisi kazandırılan öğrenciler, güvenlik politikaları ve standartlarına uygun önlemler almayı öğrenir ve kritik altyapıların korunması ile sızma testi tekniklerini uygular.
- P.Ç. 3 :** Veritabanı tasarlama, uygulama ve yönetim becerileri geliştiren öğrenciler, ilişkisel veritabanı yönetim sistemlerini etkin bir şekilde kullanmayı öğrenir ve veri modelleme tekniklerini anlama ve uygulama yetkinliği kazanır.
- P.Ç. 4 :** Programlama dillerini ve teknolojilerini kullanarak yazılım geliştirme becerisi kazanan öğrenciler, yazılım yaşam döngüsü süreçlerini anlamayı ve uygulamayı öğrenir ve yazılım kalitesi ile test süreçlerini kavrar.
- P.Ç. 5 :** İngilizce iletişim araçlarını etkin bir şekilde kullanan öğrenciler, yönetim, bilişim ve organizasyon alanlarında profesyonel düzeyde iletişim kurar.
- P.Ç. 6 :** Veri analitiği ve veri madenciliği tekniklerini öğrenen öğrenciler, veri teknolojilerini kullanarak analiz ve keşif yapar, iş zekası araçlarını etkin bir şekilde kullanarak veri odaklı kararlar alır ve uzman sistemleri kavrayarak tasarlayabilir.
- P.Ç. 7 :** Öğrenciler bilgi ve sonuçları yazılı ve sözlü olarak etkili bir şekilde sunmayı öğrenir, bilgi teknolojileri çözümlerini teknik ve teknik olmayan kitlelere iletme becerisi geliştirir ve karar alıcılarla etkili bir iletişim kurar.
- P.Ç. 8 :** Proje yönetimi prensiplerini anlama ve uygulama becerisi kazanan öğrenciler, iş süreçlerini analiz ederek iyileştirme tekniklerini uygular ve proje ekiplerini yöneterek iletişim becerilerini geliştirir.
- P.Ç. 9 :** Liderlik ve yönetim becerileri kazanan öğrenciler, işletme fonksiyonları ile ilgili bilgi sahibi olur, ekip içi iletişim ve işbirliği yeteneklerini geliştirir ve karar verme süreçlerini etkili bir şekilde yönetir.
- P.Ç. 10 :** Girişimcilik ve inovasyon konularında bilgi sahibi olan öğrenciler, yeni iş fikirleri geliştirerek bilgi teknolojileri alanında yenilikçi projeler ortaya koyar ve girişimcilik ekosistemine katkıda bulunur.
- P.Ç. 11 :** Bilgi teknolojilerinin etik kullanımına yönelik farkındalık kazanan öğrenciler, sosyal sorumluluk bilinciyle hareket eder ve bilişim sistemlerinde etik karar alma süreçlerine katkı sağlar.
- P.Ç. 12 :** Sürekli öğrenme yaklaşımını benimseyen öğrenciler, bilişim ve yönetim alanındaki yeni trendleri ve teknolojileri takip eder ve bu yenilikleri uygulamaya geçirir.
- P.Ç. 13 :** Küresel ve yerel iş dinamiklerini analiz eden öğrenciler, rekabetçi ve yenilikçi stratejiler geliştirerek bulunduğu organizasyonda fark yaratır.
- P.Ç. 14 :** E-ticaret platformlarının tasarımı, geliştirilmesi ve yönetimi konularında bilgi sahibi olan öğrenciler, dijital iş modellerini etkin bir şekilde uygular.
- Ö.Ç. 1 :** Bilgi güvenliği ilkelerini ve siber tehdit türlerini açıklar.
- Ö.Ç. 2 :** Kriptografi yöntemlerini uygular.
- Ö.Ç. 3 :** Güvenli ağ tasarımı ve erişim kontrol mekanizmalarını değerlendirir.
- Ö.Ç. 4 :** Web güvenlik açıklarını tanımlar ve savunma tekniklerini uygular.
- Ö.Ç. 5 :** Etik hacker araçlarını kullanarak sistem zaafiyetlerini test eder.