Tarih: 23 Mart 2026 15:41

Yıl

Yönetim Bilişim Sistemleri Bölümü / Yönetim Bilişim Sistemleri Bölümü / Yönetim Bilişim Sistemleri

Ders Kodu	Ders Adı	Teorik	Uygulama	Laboratuvar	Yerel Kredi	AKTS
YBS3152	Siber Güvenlik	3,00	0,00	0,00	3,00	4,00

Ders Detayı

Dersin Dili	:	Türkçe
Dersin Seviyesi	:	Lisans
Dersin Tipi	:	Seçmeli
Ön Koşullar	:	Yok
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 Elemanları	:	Arş. Gör. Cemal Yüksel
Dersi Veren Öğretim Elemanı Yardımcıları	:	Bulunmamaktadır
Dersin Verilişi	:	Yüz yüze
En Son Güncelleme Tarihi	:	17.11.2025 20:08:34
Dosya İndirilme Tarihi	:	23.03.2026

Ders Öğrenme Çıktıları

Bu dersi tamamladığında öğrenci :

1 Bilgi güvenliği ilkelerini ve siber tehdit türlerini açıklar.

2 Kriptografi yöntemlerini uygular.

3 Güvenli ağ tasarımı ve erişim kontrol mekanizmalarını değerlendirir.

4 Web güvenlik açıklarını tanımlar ve savunma tekniklerini uygular.

5 Etik hacker araçlarını kullanarak sistem zaafiyetlerini test eder.

Ön / Yan Koşullar

Ders Kodu	Ders Adı	Koşul	Teorik	Uygulama	Laboratuvar	Yerel Kredi	AKTS

Haftalık Konular ve Hazırlıklar

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

Değerlendirme Sistemi %

1 Vize : 40,000

2 Final : 60,000

AKTS İş Yükü

Aktiviteler	Sayı	Süresi(Saat)	Toplam İş Yükü
Teorik Ders Anlatım	14	3,00	42,00
Derse Katılım	14	3,00	42,00
Ara Sınav Hazırlık	8	3,00	24,00
Final Sınavı Hazırlık	8	3,00	24,00
		Toplam :	132,00
		Toplam İş Yükü / 30 (Saat) :	4
		AKTS :	4,00

Program Öğrenme Çıktısı İlişkisi

	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
	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	3	3	2	2	2	2	2	1	0	2	2	3	3	2
Ö.Ç. 2	3	3	2	2	2	2	2	1	0	2	2	3	3	2
Ö.Ç. 3	3	3	2	2	2	2	2	1	0	2	2	3	3	2
Ö.Ç. 4	3	3	2	2	2	2	2	1	0	0	2	3	3	2
Ö.Ç. 5	3	3	2	2	2	2	2	1	0	0	2	3	3	2
Ortalama	3,60	3,60	2,60	2,40	2,40	2,40	2,40	1,40	0,20	1,20	2,40	3,60	3,60	2,40

Ders/Program Çıktıları İlişkisi

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
3	3	3	2	2	2	2	2	1	0	2	3	3	2