YBS4103 - Ağ ve Sistem Güvenliği - Ömer Seyfettin Uygulamalı Bilimler Fakültesi - Yönetim Bilişim Sistemleri Bölümü

Genel Bilgiler

Dersin Amacı

Bu dersin amacı, öğrencilere ağ ve sistem güvenliğinin temel prensiplerini öğretmek, olası tehditleri ve saldırı türlerini analiz etmelerini sağlamak ve siber güvenlik önlemlerini tasarlayıp uygulama becerisi kazandırmaktır. Ders sonunda öğrenciler, güvenlik politikaları geliştirebilir ve temel sızma testleri gerçekleştirebilir.

Dersin İçeriği

Ağ güvenliğine giriş ve temel kavramlar

Siber tehditler ve saldırı türleri

Güvenlik protokolleri (SSL/TLS, IPSec, SSH)

Kimlik doğrulama ve erişim kontrolü

Güvenlik duvarları (firewall) ve saldırı tespit/önleme sistemleri (IDS/IPS)

Şifreleme teknikleri ve VPN teknolojileri

Sistem güvenliği: işletim sistemi güvenliği, yamalar, log yönetimi

Sızma testleri (penetration testing) ve etik hacking

Güvenlik politikaları, standartlar (ISO 27001, NIST) ve uyumluluk

Dersin Kitabı / Malzemesi / Önerilen Kaynaklar

Stallings, W. (2022). Network Security Essentials: Applications and Standards. Pearson.

Kaufman, C., Perlman, R., & Speciner, M. (2022). Network Security: Private Communication in a Public World. Prentice Hall.

Planlanan Öğrenme Etkinlikleri ve Öğretme Yöntemleri

Teorik ders anlatımı

Ders İçin Önerilen Diğer Hususlar

Temel ağ teknolojileri bilgisi (TCP/IP, ağ cihazları) ön koşuldur.

Dersi Veren Öğretim Elemanı Yardımcıları

Bulunmamaktadır

Dersin Verilişi

Haftada 3 saat teorik

Dersi Veren Öğretim Elemanları

Dr. Öğr. Üyesi Alican Doğan

Program Çıktısı

1. Ağ ve sistem güvenliğinin temel kavramlarını ve protokollerini açıklar.
2. Siber tehdit ve saldırı türlerini analiz eder.
3. Güvenlik duvarı, IDS/IPS ve VPN gibi güvenlik teknolojilerini uygular.
4. Temel sızma testi yöntemlerini kullanarak sistem güvenlik açıklarını değerlendirir.
5. ISO 27001 gibi güvenlik standartlarına uygun güvenlik politikaları geliştirir.

Haftalık İçerikler

Sıra	Hazırlık Bilgileri	Laboratuvar	Öğretim Metodları	Teorik	Uygulama
1				Ağ ve sistem güvenliğine giriş	
2				Siber tehditler ve saldırı türleri	
3				Güvenlik protokolleri (SSL/TLS, IPSec)	
4				Kimlik doğrulama ve erişim kontrol mekanizmaları	
5				Güvenlik duvarları (Firewall) ve IDS/IPS sistemleri	
6				Şifreleme teknikleri ve VPN teknolojileri	
7				Sistem güvenliği: işletim sistemi güvenliği, yamalar	
8				Ara Sınav Haftası	
9				Sızma testleri ve etik hacking temelleri	
10				Wireshark ve Kali Linux ile pratik uygulamalar	
11				Güncel siber saldırı vakaları analizi	
12				Güvenlik politikaları ve standartlar (ISO 27001, NIST)	
13				Grup projeleri: güvenlik yapılandırma senaryoları	
14				Grup projeleri: güvenlik yapılandırma senaryoları	

İş Yükleri

Aktiviteler	Sayısı	Süresi (saat)
Ders Öncesi Bireysel Çalışma	14	2,00
Ders Sonrası Bireysel Çalışma	14	2,00
Teorik Ders Anlatım	14	3,00
Derse Katılım	14	3,00
Ara Sınav Hazırlık	7	2,00
Final Sınavı Hazırlık	7	2,00

Değerlendirme

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

Yönetim Bilişim Sistemleri Bölümü / Yönetim Bilişim Sistemleri X 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
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 : Ağ ve sistem güvenliğinin temel kavramlarını ve protokollerini açıklar.

Ö.Ç. 2 : Siber tehdit ve saldırı türlerini analiz eder.

Ö.Ç. 3 : Güvenlik duvarı, IDS/IPS ve VPN gibi güvenlik teknolojilerini uygular.

Ö.Ç. 4 : Temel sızma testi yöntemlerini kullanarak sistem güvenlik açıklarını değerlendirir.

Ö.Ç. 5 : ISO 27001 gibi güvenlik standartlarına uygun güvenlik politikaları geliştirir.