

DERS TANITIM ve UYGULAMA BİLGİLERİ

Dersin Adı	Kodu	Yarıyıl	T+U+L (saat/hafta)	Türü (Z / S)	Yerel Kredi	AKTS
Siber Güvenlik Operasyonları	CCIP 507	Bahar	03+00+00	Zorunlu	3	7.5
Akademik Birim:	Siber Güvenlik					
Öğrenim Türü:	Örgün Eğitim					
Ön Koşullar	Yok					
Öğrenim Dili:	İngilizce					
Dersin Düzeyi:	Yüksek Lisans					
Dersin Koordinatörü:	Oğuzhan CEYLAN					
Dersin Amacı:	Bilgi sistemlerinin değerlendirilmesi amacıyla düşman davranış simülasyonları. Saldırıların adli analizi için test sistemlerinde farklı sistemlerin ve savunma tekniklerinin incelenmesi. Zayıflıkların azaltılması ve tehditlere karşı durabilmek için mühendislik çözümleri geliştirilmesi. Bilgi güvenliği amaçları bakımından farklı zayıf ve güçlü yönlerin tespit edilmesi, sızma testleri, tehdit modelleme, zafiyet analizi, kötüye kullanım ve raporlama.					
Dersin İçeriği:	Giriş. Sibergüvenlik ve Güvenlik Operasyon Merkezleri, İşletim Sistemleri: Windows İşletim Sistemi, Linux İşletim Sistemi. Ağ protokolleri ve servisleri. Ağ altyapısı. Ağ güvenliğinin prensipleri, Ağ saldırıları. Ağ koruması. Kriptografi ve Açık Anahtarlama Altyapısı. Uçnokta güvenliği ve analizi. Güvenlik izleme. Ağ güvenliği ve dijital deliller.					
Dersin Öğrenme Çıktıları (ÖÇ):	1- Sibergüvenlik operasyonlarının tanımlayan bileşenleri anlayabilmek. 2- Verimli sibergüvenlik operasyonlarını tanımlayabilmek. 3- Zayıf noktaları azaltmak ve tehlikelerle başedebilmek için çözümler geliştirebilmek.					
Dersin Öğrenme Yöntem ve Teknikleri	Sınıf dersleri, ödevler, vize ve final sınavları, Laboratuvar uygulamaları.					

HAFTALIK PROGRAM

Hafta	Konular	Ön Hazırlık
1	Giriş	
2	Sibergüvenlik ve Güvenlik Operasyon Merkezleri	
3	İşletim Sistemleri: Windows İşletim Sistemi	
4	Linux İşletim Sistemi	
5	Ağ Protokolleri ve Servisleri	
6	Ağ altyapısı	
7	Ağ güvenliği prensipleri	
8	Ağ saldırıları	
9	Ağın Korunması	
10	Kriptografi ve Açık Anahtarlama Altyapısı	
11	Uçnokta güvenliği ve analizi	
12	Güvenlik izleme	
13	Ağ güvenliği ve dijital deliller	
14	Proje Sunumları	

Kadir Has Üniversitesi'nde bir dönem 14 haftadır, 15. ve 16. hafta sınav haftalarıdır.

ZORUNLU ve ÖNERİLEN OKUMALAR

Rittinghouse, John, Hancock, William. Cybersecurity Operations Handbook, Digital Press, 2013.

DİĞER KAYNAKLAR

- Cisco Networking Academy, CCNA Cybersecurity Operations Course Booklet, Cisco Press, 2018
- Nathans, David. Designing and Building Security Operations Center, Syngress, 2014.
- Çeşitli İnternet Kaynakları.

DEĞERLENDİRME SİSTEMİ

Yarıyıl İçi Çalışmaları	Sayı	Katkı Payı (%)
Katılım	13	5
Proje	1	15
Ödev	5	15
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	5	25
Final Sınavı	1	40
Total:	25	100

İŞ YÜKÜ HESAPLAMASI

Etkinlikler	Sayısı	Süresi (saat)	Toplam İş Yüğü (saat)
Ders Saati	14	3	42
Proje	1	20	20
Ödev	5	10	50
Dersle İlgili Sınıf Dışı Etkinlikler	9	3	27
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	1	40	40
Final Sınavı	1	20	20
Toplam İş Yüğü (saat):			199

1 AKTS = 25 saatlik iş yükü

PROGRAM YETERLİLİKLERİ (PY) ve ÖĞRENME ÇIKTILARI (ÖÇ) İLİŞKİSİ

#
OC1

OC2
OC3

Katkı Düzeyi: 1 Düşük, 2 Orta, 3 Yüksek