

DERS TANITIM ve UYGULAMA BİLGİLERİ

Dersin Adı	Kodu	Yarıyıl	T+U+L (saat/hafta)	Türü (Z / S)	Yerel Kredi	AKTS
Etik Siber Saldırı	MIS 328	Güz	03+00+00	Seçmeli	3	5
Akademik Birim:	Yönetim Bilişim Sistemleri					
Öğrenim Türü:	Örgün Eğitim					
Ön Koşullar	-					
Öğrenim Dili:	İngilizce					
Dersin Düzeyi:	Lisans					
Dersin Koordinatörü:	- -					
Dersin Amacı:	Bu ders, öğrencilere Etik Hackerlığın temel ilkelerini, metodolojilerini ve araçlarını tanıtır. Öğrenciler, gerçek dünyadaki saldırgan güvenlik tekniklerini kontrollü, yasal ve etik bir şekilde uygulayacaklardır. Ders, keşif ve zafiyet analizinden, istismar, istismar sonrası, web güvenliği, kablosuz saldırılar, sosyal mühendislik ve kurumsal güvenlik önlemlerine kadar uzanır. Öğrenciler, özel sızma testi platformları ve endüstri standardı araçlarla kapsamlı bir şekilde çalışacaklardır.					
Dersin İçeriği:	1. 1. Etik hackerlığı yöneten temel siber güvenlik kavramlarını, etik ilkeleri ve yasal çerçeveleri anlayın. 2. 2. OSINT, keşif, ağ taraması ve güvenlik açığı tespiti gerçekleştirin. 3. 3. Yerleşik sızma testi metodolojilerini kullanarak sistem ve ağ güvenlik açıklarından yararlanın. 4. 4. OWASP Top 10 dahil olmak üzere yaygın web uygulaması güvenlik açıklarını analiz edin, kullanın ve azaltın. 5. 5. Kablosuz güvenlik testi ve sosyal mühendislik tekniklerinde yetkinlik gösterin. 6. 6. Karşı önlemler ve savunma stratejileri uygulayın ve profesyonel sızma testi raporları hazırlayın.					
Dersin Öğrenme Çıktıları (ÖÇ):	• 1- Etik hackerlığı yöneten temel siber güvenlik ilkelerini, etik yönergeleri ve yasal çerçeveleri anlamak. • 2- OSINT, ağ taraması ve güvenlik açığı tespiti dahil olmak üzere pasif ve aktif keşif gerçekleştirmek. • 3- Endüstri standardı araçlar ve metodolojiler kullanarak sistem ve ağ istismarını yürütmek. • 4- OWASP En Önemli 10 güvenlik açığı da dahil olmak üzere web uygulaması güvenlik açıklarını analiz etmek, istismar etmek ve azaltmak. • 5- Kontrollü ortamlarda kablosuz güvenlik değerlendirmeleri ve sosyal mühendislik simülasyonları gerçekleştirmek. • 6- Metodoloji, uygulama, dokümantasyon ve raporlama dahil olmak üzere eksiksiz bir profesyonel sızma testi çalışması hazırlamak.					
Dersin Öğrenme Yöntem ve Teknikleri	Ders içi anlatımlar, ara sınav ve final sınavı.					

HAFTALIK PROGRAM

Hafta	Konular	Ön Hazırlık
1	Etik Hackerlığa Giriş • Bilgi Güvenliği Kavramları: CIA Üçlüsü, Tehditler, Riskler • Hacker Türleri • Saldırı Vektörleri, İstismar Yüzeyleri	• Siber güvenlik temelleri hakkındaki giriş bölümlerini okuyun • VirtualBox / VMware'i yükleyin
2	Etik, Yasal Çerçeve ve Metodoloji • Siber Yasalar, Sorumlu Bilgilendirme • Kapsam ve Katılım Kuralları • Penetrasyon Testi Metodolojileri	• Yerel siber yasaları inceleyin • Penetrasyon testi kapsam şablonu oluşturun
3	Laboratuvar Kurulumu ve Araç Tanıtımı • Kali Linux / Parrot OS Kurulumu • Linux terminal temelleri • Giriş: Nmap, Burp Suite, Wireshark	• Kali araçlarını güncelleyin ve yapılandırın • Temel Linux komutlarını uygulayın
4	OSINT ve Pasif Keşif • OSINT Yöntemleri:	• WHOIS ve DNS aramaları gerçekleştirin

	WHOIS, DNS, meta veri • Araçlar: theHarvester, Recon-ng, Maltego • Alan adı keşfi: Sublist3r, Amass	• Sahte bir hedef için OSINT profili oluşturun
5	Aktif Keşif ve Tarama • Ağ Keşfi: Nmap, Zenmap • Port ve Servis Numaralandırma • Güvenlik Duvarı Algılama, Banner Yakalama	• Örnek Nmap taramaları çalıştırın • Açık portları ve hizmetleri belgeleyin
6	Güvenlik Açığı Tarama ve Haritalama • Nikto, OpenVAS Tarama • Güvenlik Açığı Sınıflandırması • Topoloji Haritalama ve Saldırı Yüzeyi Analizi	• Bir laboratuvar sanal makinesinde güvenlik açığı taraması gerçekleştirin • Keşif/Güvenlik Açığı Raporu hazırlayın
7	Sömürü Temelleri • CVE'leri ve Sömürü Veritabanlarını Anlama • Yükler ve Kabuklar • Metasploit Temelleri	• Exploit-db ve CVE veritabanlarını keşfedin • Metasploit temel modüllerini uygulayın
8	Sistem İstismarı • Windows ve Linux istismarı • İlk Erişimi Elde Etme • İstismar İş Akışı	• Metasploitable üzerinde istismar laboratuvarları çalıştırın • Güvenlik açığı bulunan hizmetleri belirleyin
9	İstismar Sonrası ve Ayrıcalık Yükseltme • Ayrıcalık Yükseltme Yöntemleri • Kimlik Bilgisi Toplama • Kalıcılık, İzleri Kapatma	• Uygulamalı ayrıcalık yükseltme alıştırımları • İstismar sonrası adımları belgeleyin
10	Web Uygulaması Güvenlik Temelleri • HTTP, Oturumlar, Çerezler • DVWA, OWASP Juice Shop Kurulumu • Giriş Doğrulaması ve Yaygın Zayıflıklar	• DVWA güvenlik seviyelerini yapılandırın • Burp Suite'te pratik oturum analizi yapın
11	OWASP İlk 10 (Bölüm 1) • SQL Enjeksiyonu (manuel ve SQLMap) • XSS (Yansıyan ve Depolanan) • Burp Suite Web Testi	• DVWA'da SQLi laboratuvarlarını çalıştırın • XSS yüklerini uygulayın
12	OWASP İlk 10 (Bölüm 2) ve API Güvenliği • CSRF, Bozuk Kimlik Doğrulama • Dosya Yükleme Saldırıları • API Keşfi ve Testi • NoSQL Enjeksiyonu	• Analyze vulnerable API endpoints • Explore Burp Suite extensions
13	Kablosuz Güvenlik ve Sosyal Mühendislik • Wi-Fi Standartları ve Zayıflıkları (WPA/WPA2/WPS) • Aircrack-ng, Kismet, Evil Twin Kurulumu • Sosyal Mühendislik, Kimlik Avı Simülasyonu	• WPA el sıkışmasını yakalayın • Bir kimlik avı şablonu tasarlayın
14	Karşı Önlemler ve Nihai Raporlama • IDS/IPS, Güvenlik Duvarları, Uç Nokta Güçlendirme • Yama Yönetimi ve Temel Hatlar • Profesyonel Bir Penetrasyon Testi Raporu Yazma	• Tam nihai penetrasyon testi raporunun hazırlanması • Savunma güvenlik sistemlerinin incelenmesi

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

ZORUNLU ve ÖNERİLEN OKUMALAR

- Sertifikalı Etik Hacker (CEH) v12 Resmi Eğitim Malzemesi – EC-Council
- “Web Uygulaması Hacker'ı El Kitabı (2. Baskı)” – Dafydd Stuttard ve Marcus Pinto
- “Sızma Testi: Hacker'lığa Uygulamalı Giriş” – Georgia Weidman

DİĞER KAYNAKLAR

İlan Edilecek

DEĞERLENDİRME SİSTEMİ

Yarıyıl İçi Çalışmaları	Sayı	Katkı Payı (%)
Proje	1	30
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	1	30
Final Sınavı	1	40
Total:	3	100

İŞ YÜKÜ HESAPLAMASI

Etkinlikler	Sayısı	Süresi (saat)	Toplam İş Yüğü (saat)
Ders Saati	14	3	42
Proje	1	35	35
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	1	21	21
Final Sınavı	1	27	27
Toplam İş Yüğü (saat):			125

1 AKTS = 25 saatlik iş yüğü

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

#	PY1	PY2	PY3	PY4	PY5	PY6	PY7	PY8	PY9	PY10	PY11
OC1											
OC2											
OC3											
OC4											
OC5											
OC6											

Katkı Düzeyi: 1 Düşük, 2 Orta, 3 Yüksek