

	MSÜ DENİZ HARP OKULU DEKANLIĞI BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜM BAŞKANLIĞI DERS TANITIM BİLGİLERİ	
---	--	---

Dersin Adı	Dersin Kodu	Sınıf / Dönem	Ders Saati (T+U+L)	Kredi	AKTS
Zararlı Yazılım Analizi (Siber Güvenlik)	BİL960	4 / Güz veya Bahar	3+0+0	3	3

Dersin Dili	:	Türkçe
Dersin Seviyesi	:	Lisans, Zorunlu
Dersin Önkoşulu	:	Herhangi bir programlama dilinde (C, C++, Java, C#, vb.) yazılım geliştirmiş olmak.
Dersin Öğretim Elemanları	:	Bilgisayar Mühendisliği Öğretim Elemanı
Dersin Amacı	:	Dersin amacı katılımcılara temel saldırı çeşitlerini ve bunlara karşı alınabilecek önlemleri öğretmektir. Bu ders katılımcılara zararlı yazılımların neler olduğunu, nasıl davranış sergilediklerini ve davranışlarına göre bu yazılımların nasıl sınıflandırıldıklarını öğretir. Ayrıca katılımcılar şüpheli bir yazılımı farklı teknikler kullanarak analiz etmeyi öğrenir. Zararlı bir yazılımı tespit etmenin yanında onunla mücadele etmeyi ve sistemden tamamen temizlemeyi öğretmek dersin amaçları arasındadır.
Dersin Öğrenme Çıktıları	:	Bu dersi başarı ile tamamlayabilen öğrenciler; 1. Zararlı yazılımın ne olduğunu ve potansiyelini bilir. 2. Zararlı yazılımın nasıl davranışlar sergileyebileceğini bilir. 3. Tespit ettiği bir zararlı yazılımın ne tür bir zararlı olduğunu bilir, sınıflandırabilir. 4. Şüpheli bir yazılımın analizini yapıp zararlı olup olmadığını anlayabilir. 5. Zararlı yazılımlara karşı ne tür önlemler alması gerektiğini bilir. 6. Enfekte olmuş bir sistemi zararlılardan nasıl temizleyeceğini bilir.
Dersin İçeriği	:	Bu derste öncelikle zararlı yazılımın ne olduğu ve yol açabileceği zararlar başlıkları üzerinde durulacaktır. Daha sonra zararlı yazılım davranışları irdelenecek olup bu davranış profili kullanılarak zararlı yazılım tespitinin nasıl yapılacağı anlatılacaktır. Bununla birlikte sistematik analiz teknikleri öğretilecek ve nasıl kullanılması gerektiği hakkında bilgiler verilecektir. Temel statik analiz, ileri statik analiz, temel dinamik analiz ve ileri dinamik analiz bu ders kapsamında üzerinde durulacak tekniklerdendir.

Ders Kitabı	:	Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software, Sikorski, M., & Hanig, No Starch Press, 2012. Some’ler İçin Ağ ve Malware Analizi, M.Alparslan AKYILDIZ, Gazi Kitabevi Yayınları, 2018.				
Diğer Kaynaklar	:	Malware Analyst’s Cookbook and DVD: Tools and techniques for fighting malicious code, Ligh, M., Harstein, B., & Adair, S., John Wiley & Sons Inc, 2010.				
Ödevler ve Projeler	:	Var				
Bilgisayar Kullanımı	:	Yok				
Diğer Uygulamalar	:	Yok				
Başarı Değerlendirme Sistemi	:	Faaliyetler		Taban Notu	Adedi	Değerlendirmedeki Katsayısı (%)
		Ara Sınav		50	1	%30
		Yarıyl Değerlendirme	Kısa Sınavlar	50	-	%10
			Ödevler	50	1	
			Projeler	50	-	
			Dönem Ödevi / Projesi	50	1	
			Laboratuvar Uygulaması	50	-	
			Diğer Uygulamalar	50	-	
			Bitirme Sınavı		50	1
		Bütünleme Sınavı / NYS		50	-	%100
		Çift Ders Sınavı		50	-	%100

PROGRAM ÇIKTILARININ DERSİN ÖĞRENME ÇIKTILARI İLE İLİŞKİSİ

Katkı Düzeyi	1	2	3	4	5
	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek

ZARARLI YAZILIM ANALİZİ															
		Program Çıktıları													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Dersin Öğrenme Çıktıları	1	5	5	3	3	3	2	2	1	1	1	1	1	1	5
	2	5	5	3	3	3	2	2	1	1	1	1	1	1	5
	3	2	5	3	3	3	3	3	2	2	1	1	1	1	5
	4	1	2	4	4	4	4	4	5	5	5	5	5	5	5
	5	1	2	4	4	4	4	4	5	5	5	5	5	5	5
	6	1	1	2	3	3	3	3	4	4	4	5	5	5	5

HAFTALIK KONULAR	
Hafta	Konular
1	Tanıtım ve Temel Kavramlar
2	Zararlı Yazılım Türleri ve Önlemleri
3	Zararlı Yazılım Analiz Türleri
4	Temel Statik Analiz
5	Temel Statik Analiz
6	Temel Dinamik Analiz
7	Temel Dinamik Analiz
8	ARA SINAV
9	İleri Statik Analiz
10	İleri Statik Analiz
11	İleri Statik Analiz
12	İleri Dinamik Analiz
13	İleri Dinamik Analiz
14	İleri Dinamik Analiz
15	Proje Sunumu

AKTS / İŞ YÜKÜ TABLOSU			
FAALİYETLER	SAYI	SÜRE	TOPLAM İŞ YÜKÜ
Teorik Ders	14	3	42
Uygulama	-	-	-
Sınıf Dışı Ders Çalışma Süresi	14	0.5	7
Ödev Hazırlama	1	6	6
Proje Hazırlama	-	-	-
Dönem Projesi Hazırlama	1	8	8
Dönem Projesi Sunumu	1	1	1
Ödev Sunumu	-	-	-
Proje Sunumu	-	-	-
Kısa Sınav	-	-	-
Ara Sınav	1	2	2
Ara Sınav İçin Bireysel Çalışma	1	10	10
Bitirme Sınavı	1	2	2
Bitirme Sınavı İçin Bireysel Çalışma	1	12	12
TOPLAM İŞ YÜKÜ	90 Saat		
DERSİN AKTS KREDİSİ	Toplam İş Yüğü / 30 = 90 / 30 = 3 Kredi		

Son Güncelleme Tarihi	:	22.03.2024
Güncelleyen Kişi	:	Musa MİLLİ