SÜLEYMAN DEMİREL ÜNİVERSİTESİ BİLGİSAYAR MÜHENDİSLİĞİ SİBER GÜVENLİK TEZSİZ YÜKSEK LİSANS PROGRAMI DERS İÇERİĞİ

Kodu / Adı:	**Siber Güvenliğe Giriş**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6

Dersin Amacı

Ülkemizde bilgi ve iletişim sistemlerinin her geçen gün daha fazla kullanılmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğimizin, hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir. Bu ders ile, bilişim sistemlerinde var olan güvenlik zafiyetlerinin/tehditlerin anlaşılabilmesi, siber saldırılara karşı alınması gereken önlemler konusunda farkındalık oluşturulması hedeflenmektedir.

Dersin İçeriği

1. Hafta: Siber güvenlik temel kavramları
2. Hafta: Siber güvenlik temel kavramları
3. Hafa: Siber Savaş
4. Hafta: Şifrelemeye Giriş
5. Hafta: Güvenlik duvarları
6. Hafta: Saldırı tanıma ve durdurma sistemleri
7. Hafta: İşletim Sistemi güvenliği
8. Hafta: İşletim Sistemi güvenliği
9. Hafta: Güvenli Yazılım Geliştirme
10. Hafta: Web Uygulamalarının Güvenliği
11. Hafta: Sızma Testleri
12. Hafta: Sızma Testleri
13. Hafta: Zararlı Yazılım Analizi
14. Hafta: Zararlı Yazılım Analizi

Kodu / Adı:	**Kriptografi**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	**6**

Dersin Amacı

Ders güvenlik protokol ve tekniklerinin temelini oluşturan kriptografik algoritma ve yöntemleri kapsayacaktır. İçerilecek konu başlıkları: klasik şifreleme teknikleri, kripto matematiği, simetrik şifreleme, açık anahtar şifreleme, anahtar yönetimi, hash ve MAC algoritmaları, kriptografik uygulamalar. Derste algoritmalara ve programlama dili kullanarak gerçeklemeye vurgu yapılacaktır.

Dersin İçeriği

1. Hafta	Ağ ve bilgisayar güvenliğinin temelleri, giriş
2. Hafta	Bilişim güvenliği kavramlar, terminoloji ve ilkeler
3. Hafta	Simetrik şifreleme yöntemi
4. Hafta	Klasik şifreleme teknikleri
5. Hafta	Blok şifreleme ve DES
6. Hafta	Finite Field'lara giriş
7. Hafta	AES
8. Hafta	Simetrik şifreleme ile ilgili diğer ayrıntılar
9. Hafta	Sayı Teorisine giriş (asal sayılar, Fermat ve Euler Teoremleri)

10. Hafta	Asal sayı test yöntemi, Chinese Remainder Teoremi, Ayrık logaritma kavramı
11. Hafta	Public Key Şifreleme Yöntemine giriş (PKE)
12. Hafta	Anahtar dağıtımı ve Diffie-Hellman algoritması
13. Hafta	RSA Şifreleme tekniği
14. Hafta	PKE'nin Kimlik ve veri bütünlüğü doğrulama uygulamaları, hash fonksiyonları

Kodu / Adı:	**Bilgisayar Ağları ve Haberleşme**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bilgisayar iletişim ve ağ kavramları. Uygulama katmanı ve yaygın uygulamalar. Taşıma katmanı ve servisleri (TCP, UDP). Ağ katmanı ve IP. Veri bağlantısı katmanı ve protokoller. Ağ oluşturma ve ağ cihazları. Kablosuz iletişim.					
Dersin İçeriği					
1. hafta:	Bilgisayar Ağlarının Sınıflandırılması ve OSI Referans Modeli				
2. hafta:	Fiziksel Katman ve Veri Bağı Katmanı Detayları				
3. hafta:	LAN Teknolojileri (Ethernet, Token Ring, Token Bus)				
4. hafta:	Omurga Teknolojileri (FDDI, ATM)				
5. hafta:	Arabağlantı Cihazları				
6. hafta:	TCP/IP Mimarisi - 1				
7. hafta:	TCP/IP Mimarisi - 2				
8. hafta:	IP Adresler, IP Yönlendirme, Alt ağ oluşturma				
9. hafta:	Router, Yönlendirme Protokolleri ve Algoritmaları				
10. hafta:	Router, Yönlendirme Protokolleri ve Algoritmaları				
11. hafta:	Kablosuz LAN Teknolojileri				
12. hafta:	Ağ güvenliği				
13. hafta:	Ağ tasarımı ve Başarımı				
14. hafta:	Ağ tasarımı ve Başarımı				

Kodu / Adı:	**Veri ve Ağ Güvenliği**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Veri ve ağ güvenliği kavramları; güvenlik sistemi tasarım süreci; güvenlik risk analizi; kriptolamanın temelleri ve uygulamaları hakkında bilgi vermek. Veri ve ağ güvenliği için analiz ve system tasarımı yapabilme becerisini kazandırmak.					
Dersin İçeriği					
1. hafta:	Veri ve Ağ Güvenliğine Giriş				
2. hafta:	Ağlar Niçin güvenli olmalıdır				
3. hafta:	Güvenlik gereksinimi ve Ne kadar güvenlik gerekir, Bilgi Güvenliği Yönetimi				
4. hafta:	Ağ Sistemlerinin Çalışması ve Topoloji Güvenlği				
5. hafta:	Yetkilendirme ve Kriptolama, Simetrik Şifreleme sistemleri				
6. hafta:	Asimetrik Simetrik Şifreleme sistemleri				
7. hafta:	Şifreleme ile Güvenlik, Sayısal İmzalar				
8. hafta:	Güvenlik Duvarları				

9. hafta:	Nüfuz Tespit Sistemleri
10. hafta:	Biyometrik Güvenlik Sistemlerine Giriş
11. hafta:	(KISA ARA SINAV)Biyometrik Güvenlik Sistemleri
12. hafta:	Sanal Özel Ağlar ile Güvenlik
13. hafta:	Yıkımdan Koruma ve Onarım
14. hafta:	Ağ Kullanım Politikaları

Kodu / Adı:	**Kablosuz Ağ Güvenliği**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Kablosuz yerel ve geniş alan ağ teknolojileri ile ilgili temel teorik bilgi ile beraber bu ağların kurulaması, yapılandırılması, güvenliği ve yönetimi ile ilgili gerekli yazılım ve donanım araçları incelenecektir.					
Dersin İçeriği					
1. hafta:	Tanışma ve Tanıtım				
2. hafta:	Ağ(Network) Genel Tekrar				
3. hafta:	Kablosuz İletişimin Tarihçesi, Gelişimi, Tanımı,				
4. hafta:	Kablosuz İletişimin Yöntem ve Teknolojileri				
5. hafta:	Kablosuz Ağların Sınıflandırılması				
6. hafta:	Kablosuz Ağ Standartları				
7. hafta:	IEEE 802.x ve Kablosuz Ağ Standartlar				
8. hafta:	Kablosuz Ağ Cihazları				
9. hafta:	Kablosuz Erişim Noktası (Access Point) Konfigürasyonu				
10. hafta:	Kablosuz Ağ Güvenliği (SSID, WEP, WPA, WPA2, TKIP, EAP, AES)				
11. hafta:	Kablosuz Ağ Saldırıları ve Korunma Tedbirleri (DoS, Spoof, Sniff)				
12. hafta:	Windows İşletim Sisteminde Kablosuz Ağ Ayarları (IPv4, IPv6)				
13. hafta:	Linux İşletim Sisteminde Kablosuz Ağ Ayarları (IPv4, IPv6)				
14. hafta:	Genel Tekrar				

Kodu / Adı:	**Veritabanı Güvenliği**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu derste, veritabanı ve sunucularını güvenliğini sağlama ve savunma algoritmaları oluşturma becerisinin kazandırılması amaçlanmaktadır.					
Dersin İçeriği					
1. hafta:	Veritabanı Sistemleri, Veri Modelleri				
2. hafta:	Varlık-ilişki modeli				
3. hafta:	İlişkisel Veri Modeli				
4. hafta:	İlişkisel Cebir				
5. hafta:	Genişletilmiş Varlık İlişki Modeli				
6. hafta:	Yapısal Sorgulama Dili (SQL)				
7. hafta:	İleri SQL				
8. hafta:	Örnek Uygulamalar				
9. hafta:	Veritabanı sistemlerinde ağ trafiğinin şifrelenmesi				
10. hafta:	Veritabanı güvenlik kontrolleri				
11. hafta:	Kimlik doğrulama				
12. hafta:	Veri sıkılaştırma ve güvenlik				

13. hafta:	Veritabanlarına yönelik saldırılar ve savunmalar
14. hafta:	Veritabanlarına yönelik saldırılar ve savunmalar

Kodu / Adı:	**Yazılım ve Web Güvenliği**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu ders ile genel yazılım güvenliği ve özellikle web uygulamalarının güvenliğinin sağlanması ve analizi ile güvenli uygulama geliştirilmesi metodolojlierinin öğretilmesi amaçlanmaktadır.					

Dersin İçeriği	
1. hafta:	Bilgi ve yazılım güvenliği temelleri
2. hafta:	Yazılım güvenliği ihlal teknikleri
3. hafta:	Temel kriptografi,SSL protokolü
4. hafta:	Sayısal ödeme sistemleri ve SET protokolü
5. hafta:	Tarayıcı güvenliği
6. hafta:	Kötücül HTML kodu ve Web saldırıları
7. hafta:	Çerez yazılımlar, web kötücül kodları ve casus yazılımlar
8. hafta:	Windows sistemleri ve Internet tarayıcı güvenliği
9. hafta:	UNIX/LINUX güvenliği
10. hafta:	Apache web sunumcu
11. hafta:	(KISA ARA SINAV) Değişik erişim denetimleri
12. hafta:	Yazılım güvenlik risklerinin yönetimi
13. hafta:	Güvenli uygulama yazılımı geliştirme
14. hafta:	Paket filtreleme tabanlı Güvenlik duvarları ve Web Güvenlik duvarı

Kodu / Adı:	**Mobil Güvenlik**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu ders ile genel mobil cihaz güvenliği ve özellikle mobil uygulamalarının güvenliğinin sağlanması ve analizi ile güvenli uygulama geliştirilmesi metodolojlierinin öğretilmesi amaçlanmaktadır.					

Dersin İçeriği	
1. hafta:	Mobil güvenlik temelleri
2. hafta:	Temel güvenlik ve kriptografi teknikleri
3. hafta:	Android İşletim Sistemi ve Güvenliği
4. hafta:	iOS İşletim Sistemi ve Güvenliği
5. hafta:	Windows Mobile İşletim Sistemi ve Güvenliği
6. hafta:	Mobil Uygulamalar ve Yapıları
7. hafta:	Mobil Kötücül Yazılımlar
8. hafta:	Kötücül Yazılım Analiz Araçları
9. hafta:	Mobil Web Güvenliği
10. hafta:	GSM Ağ Güvenliği
11. hafta:	LTE Güvenliği
12. hafta:	Wifi ve Bluetooth Güvenliği
13. hafta:	Mobil VoIP Güvenliği
14. hafta:	Mobil Güvenlikte Trendler

Kodu / Adı:	Bilgi Yönetimi ve Güvenliği				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bilgi güvenliği yönetimi teknik ve standartları ile uygulamada yapılacak risk analizinin ve yönetiminin öğretilmesi amaçlanmaktadır.					
Dersin İçeriği					
1. hafta:	Temel kavramlar: Veri güvenliği temel ilkelerinin tanıtımı, Bilgi güvenliği yönetiminin temelleri				
2. hafta:	Bilgi güvenliği yönetimi bileşenleri ve standartlar,				
3. hafta:	Bilgi sisteminde tutulacak olan verilen güvenlik açısından sınıflandırılması				
4. hafta:	Bilgi sistemini kullanma hakkı olanların yetkilerinin güvenlik açısından sınıflandırılması				
5. hafta:	Kullanıcı ve veri güvenlik sınıflandırmasına uygun olarak erişimlerin izlenmesi, denetlenmesi ve raporlanması;				
6. hafta:	Bilgi güvenliği yönetimi strateji ve politikaları				
7. hafta:	Bilgi güvenliği yönetişimi,;				
8. hafta:	Risk Analizi yöntemleri				
9. hafta:	Bilgi güvenliği yönetim politikaları.				
10. hafta:	Bilgi güvenliği yönetim standartları(ISO 2700x).				
11. hafta:	Bilgi güvenliği yönetim standartları(COBIT) -Vize Sınavı				
12. hafta:	Bilgi Güvenliği yönetim sistemi tasarımı;.				
13. hafta:	Bilgi Güvenliği yönetim sistemi tasarımı, uygulama adımları				
14. hafta:	Öğrenci dönem projesi sunumları				

Kodu / Adı:	Bilgi Sistemleri Güvenliği				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu ders, bilgi sistemleri güvenliği konusunun temel prensiplerini içerir.					
Dersin İçeriği					
1. hafta:	Giriş Tanımlar, güvenlik tarihi, günümüzdeki çalışmalar, BS güvenlik ortakları ve BS güvenliğinin etkileri.				
2. hafta:	BS Güvenliğinin Yönetimi BS güvenlik yönetiminin prensiplerine, BS güvenliğinin işlevlerine ve güvenlik yöntemlerine giriş				
3. hafta:	Risk Analizi ve Yönetimi Önemli ilkeler, yönetimin işlevi, standartlar, Risk Yönetimi Yazılımına giriş				
4. hafta:	Acil Durum ve Süreklilik Planlaması Önemli kavramlar, yıkımdan geri kazanma ve faaliyet süreklilik planlarının geliştirilmesi, risk değerlendirmesi, faaliyet etki değerlendirmesi, geri kazanım stratejileri ve ortak tuzaklar				
5. hafta:	Mantıksal ve Fiziksel Güvenlik mantıksal ve fiziksel veri güvenliği kriterleri, girdi kontrolleri, veritabanı kontrolleri, güvenlik kuralları ve mekanizmaları, fiziksel güvenlik kriterleri, erişim kontrolleri, önleyici, tespit edici ve düzeltici ölçüler.				
6. hafta:	İnternet Güvenliği Açıklıklar ve tehditler, saldırılara ve sisteme sızmalara yaklaşımlar (alan ismi ve hat analizi), suistimal, örnek olay incelemesi ve gösterim, akımlar.				
7. hafta:	Şifreleme, Umumi-Anahtar Altyapısı (PKI), Dijital İmzalar, Geçit Güvenliği Terimleri, saldırı çeşitleri, saldırılara karşı korunma, doğrulama yöntemleri, güvenlik politikası, teknik çözümler (güvenlik duvarı, şifreleme).				

8. hafta:	E-Ticaret (B2B) Güvenliği e-ticaret türleri, SET, PKI, dijital sertifikalar, Doğrulama (NCSA, HTML, kullanıcı çerezleri, SSL, dijital sertifikalar, iki faktörü ve biyostatistik), e-ticaret için gerekli güvenlik altyapılarının oluşturulması.
9. hafta:	İşletim sistemleri Güvenliği İşletim sistemlerine genel bakış, İşletim sistemleri güvenliği için yöntemler, İşletim sistemi güvenliğinin evrimi, UNIX ve Microsoft NT nin karşılaştırılması.
10. hafta:	Veritabanı Güvenliği Veritabanlarına genel bakış, erişim kontrolü, yetkilendirme, bütünlük, güvenlik mekanizmaları
11. hafta:	Kanuni Konular Bilgisayarlardaki değerlerin korunması, telif hakkı, bilgisayarı kötüye kullanma, gizliliğin hukuki yönleri, hukuki anlaşmalar, bilgisayardaki bir kanıtın mahkemedeki geçerliliği, bilgisayarlarla ilgili hususları düzenleyen kanunlar, ihmalkarlık ve yönetime etkileri.
12. hafta:	Etik Sorunlar Özel yaşam ve gözetleme ve bilgi sistemleri güvenliğine olan etkileri, bilgi sistemlerindeki mesleki yükümlülükler
13. hafta:	Yeni ortaya çıkan eğilimler: Biyostatistik Önemli kavramlar, türleri ve kullanımları, işleyiş ve örnekler, kullanımla ilgili kilit konular (kabul, kabul edilebilirlik, kesinlik, maliyet ve etik)
14. hafta:	Genel tekrar.

Kodu / Adı:	**Siber Savaş, Savunma ve Güvenlik**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin İçeriği					
1. hafta:	Bilgi güvenliği alanındaki savaşlar, bilgi harbi				
2. hafta:	Güvenlik birimleri ve süreçleri				
3. hafta:	Bilişim uzayının temel özellikleri				
4. hafta:	Kritik alt yapı ve sistemleri				
5. hafta:	Stratejik ve işlevsel savaşlar				
6. hafta:	Saldırı kaynakları, Saldırı türleri, Savunma sistemleri				
7. hafta:	Gelişmiş siber silahların saptanması ve önlenmesi, Savunma mimarisi				
8. hafta:	Şifreleme uygulamaları, Elektronik Güvenlik				
9. hafta:	Bilgi güvenliği standartları				
10. hafta:	Casusluk ve istihbarat yöntemleri, ulus-devlet düzeyinde siber savaşın işlevsel gereksinimleri,				
11. hafta:	(KISA ARA SINAV) Savaş sistemleri, kavramları, yönetimi				
12. hafta:	Savaş varlıklarının entegrasyonu kontrolü ve etkin kullanımı				
13. hafta:	Savunma yaklaşımları				
14. hafta:	İleri Savunma stratejileri				

Kodu / Adı:	Adli Bilişim				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu ders, Adli Bilişim tekniklerinin anlatılacağı bir ders olacaktır. Ders boyunca Linux ve Windows tabanlı sistemlerde adli bilişim incelemelerinin nasıl yapıldığı üzerine teknikler anlatılacaktır. Adli Bilişim incelemesi esnasındaki süreç, adli bilişim ile ilgili inceleme için toplanacak olan elektronik bilginin nasıl toplanacağının anlatılmasıyla başlayıp toplanan bu bilgilerin nasıl analiz edileceği ile devam edip, analiz sonrası elde edilen delillerin sunulmasıyla son bulan bir şekilde incelenecektir. Derste, elektronik ortamda birçok değişik teknik ile delil bulma ve bu delillere bağlı olarak hukuki sürecin sağlıklı işleyebilmesi için delillerin geçerliliğinin sağlanabilmesinin yöntemlerine de değinilecektir.					
Dersin İçeriği					
1. hafta:	Adli Bilişime giriş				
2. hafta:	Adli Bilişim araştırma süreci				
3. hafta:	Adli Bilişim ofis ve laboratuvarları				
4. hafta:	Bilgi toplama araç ve yöntemleri				
5. hafta:	Suç ve olay yeri inceleme				
6. hafta:	Dijital delil kontrolü				
7. hafta:	Windows ve Linux Sistemlerinde Adli Bilişim				
8. hafta:	Veri elde etme				
9. hafta:	Bilgi analizi				
10. hafta:	Veri kurtarma				
11. hafta:	E-posta araştırmaları				
12. hafta:	Araştırma raporlama				
13. hafta:	Tekrar				
14. hafta:	Dönem değerlendirmesi				

Kodu / Adı:	Bilgi Güvenliği Hukuku				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bilgi Güvenliği Hukuku Dersi'nde, bilgi güvenliği uygulamalarının hukuksal boyutu işlenecek olup, farklı sektör ve ihlal çeşitleri doğrultusunda ortaya çıkabilecek senaryolarda alınması gereken hukuki aksiyonlar, bu ihlaller öncesinde oluşturulması gereken politikalar ve prosedürler kapsamında hukuksal bağlayıcılığın ve hukuksal uyumun sağlanması, delil oluşturma süreçlerinin belirlenmesi gibi konular Türk Hukuku ve ülkemizdeki pratik uygulamalar dikkate alınarak incelenecekti. Ayrıca ülkemizde yürürlüğe girmiş ve taslak halinde bulunan bilgi güvenliği ile ilgili kanuni düzenlemeler de ders kapsamında tartışılacaktır.					
Dersin İçeriği					
1. hafta:	Bilgi güvenliğine giriş				
2. hafta:	Bilgi güvenliği temelleri				
3. hafta:	Bilgi güvenliği hukuki boyutları				
4. hafta:	Bilgi güvenliği hukuki boyutları				
5. hafta:	Bilgi güvenliği ihlalleri				
6. hafta:	Bilgi güvenliği ihlalleri				
7. hafta:	Sektörel ihlaller				
8. hafta:	Sektörel ihlaller				
9. hafta:	Örnek senaryo incelemeleri				
10. hafta:	Örnek senaryo incelemeleri				

11. hafta:	Delil oluşturma süreçleri
12. hafta:	Bilgi güvenliği ile ilgili kanuni düzenlemeler
13. hafta:	Bilgi güvenliği ile ilgili kanuni düzenlemeler
14. hafta:	Dönem değerlendirmesi

Kodu / Adı:	**Sızma Tespiti ve Önleme**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu ders ile kurumsal yapıların genel güvenlik yapısının parçası olan sızma tespit sistemlerinin analizi ve tasarımı ile pratik kavramların öğretilmesi amaçlanmaktadır.					
Dersin İçeriği					
1. hafta:	Bilgi sistemlerine yönelik saldırı türleri				
2. hafta:	Saldırılara karşı geliştirilen yöntemler ve teknikler				
3. hafta:	Saldırı türüne özel karşı önlemler,Sezgisel önlemler				
4. hafta:	Sızma tespitinin tarihçesi				
5. hafta:	Anormallik ve kötüye kullanım yöntemleri				
6. hafta:	Anormallik ve kötüye kullanım tabanlı sızma tespiti				
7. hafta:	Ağ ve sunucu tabanlı sızma tespiti				
8. hafta:	Hata yüzdeleri ve ROC eğrilerinin kullanımı				
9. hafta:	Taban değer yanılgısı(Base rate fallacy) problemi				
10. hafta:	Potansiyel sızmalara karşı önlemler				
11. hafta:	(KISA ARA SINAV) Güvenlik duvarı kuralları ve STS				
12. hafta:	Bal kabı(honey pot) yöntem ile sızma özniteliklerinin analizi				
13. hafta:	Pratik konular				
14. hafta:	Tekrar				

Kodu / Adı:	**Risk Yönetimi**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Risk yönetimi kavram ve yöntemlerinin öğretimi.					
Dersin İçeriği					
1. hafta:	Risk kavramı ve riskin analitik olarak tanımlaması				
2. hafta:	Risk kavramı ve riskin analitik olarak tanımlaması				
3. hafta:	Risk yönetimi alanları ve özellikleri				
4. hafta:	Risk yönetimi alanları ve özellikleri				
5. hafta:	Risk değerlendirme teknikleri, yöntemleri değerlendirme araçları				
6. hafta:	Risk değerlendirme teknikleri, yöntemleri değerlendirme araçları				
7. hafta:	Klasik, Bayesian, bulanık mantık ve diğer risk yönetimi karar modellerinin tanıtımı				
8. hafta:	Klasik, Bayesian, bulanık mantık ve diğer risk yönetimi karar modellerinin tanıtımı				
9. hafta:	Klasik, Bayesian, bulanık mantık ve diğer risk yönetimi karar modellerinin tanıtımı				
10. hafta:	Hedef, zamanlama, maliyet, fırsat maliyeti riskleri bakımından karmaşık karar verme yöntemleri				
11. hafta:	Hedef, zamanlama, maliyet, fırsat maliyeti riskleri bakımından karmaşık karar verme yöntemleri				

12. hafta:	Güvenlik alanında stratejik risk yönetimi teknikleri
13. hafta:	Güvenlik alanında stratejik risk yönetimi teknikleri
14. hafta:	Tekrar

Kodu / Adı:	**Siber Güvenlik için Veri Madenciliği**		
Türü	Seçmeli	**Programın Adı**	Bilgisayar Müh. ABD.
Dersin Amacı			
Bu ders, siber güvenlik bağlamında veri madenciliği araçlarının teorisini ve pratiğini kapsayacaktır. Bu tekniklerin siber güvenlik problemlerinin çözümünde kullanılmasının öğretilmesi amaçlanmıştır.			
Dersin İçeriği			
1. hafta:	Giriş: bilgi güvenliğine, mevcut güvenliğin durumuna, güvenlik veri madenciliğine genel bakış		
2. hafta:	Botnet tespiti		
3. hafta:	İç saldırı tespiti		
4. hafta:	Davranışsal Biyometrikler		
5. hafta:	Sahtecilik tespiti		
6. hafta:	Ağ ve bilgisayar tabanlı saldırı tespiti		
7. hafta:	Web tehdit tespiti		
8. hafta:	Çoklu sınıflayıcı sistemler ve Çekişmeli makine öğrenmesi		
9. hafta:	Derin paket denetleme- Vize Sınavı		
10. hafta:	Güvenlik için makine öğrenmesi		
11. hafta:	Elektronik imza teknolojileri		
12. hafta:	Polimorfizim		
13. hafta:	Oltalama tespiti		
14. hafta:	Otomatik uyarı ilişkisi		

Kodu / Adı:	**Siber Güvenlik için Makine Öğrenmesi**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bu dersin amacı, öğrencilere makine öğrenme kavramını ve farklı öğrenme metodlarını öğretmektir. Bu dersin sonucunda, öğrenci kendisine verilen gerçek hayattaki bir problemi en uygun hangi makine öğrenme metodunu uygulayacığını ve bu metodun hata ve karmaşıklık açısından nasıl analiz edeceğini öğrenecektir.					
Dersin İçeriği					
1. hafta:	Giriş				
2. hafta:	Gözetimli öğrenme				
3. hafta:	Bayesian karar teorisi				
4. hafta:	Parametrik metodlar				
5. hafta:	Çok-değişkenli metodlar				
6. hafta:	Boyut azaltma				
7. hafta:	Parametrik olmayan metodlar				
8. hafta:	Ara Sınav				
9. hafta:	Karar Ağaçları				
10. hafta:	Doğrusal ayırım				
11. hafta:	Çok-katmanlı algılayıcılar				
12. hafta:	Gizli Markov modelleri				

13. hafta:	Destek vektör makine
14. hafta:	Denetimsiz ve takviyeli öğrenim

Kodu / Adı:	**İşletim Sistemleri Güvenliği**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
İşletim sistemlerinin BT sistemleri güvenliğine etkisi, özellikleri ve açıklıkları ile güvenli işletim sistemi analiz/tasarımı kavramının öğretilmesi amaçlanmaktadır					
Dersin İçeriği					
1. hafta:	İşletim sistemi Güvenliğine Giriş				
2. hafta:	İşletim Sistemi ve yaygın kullanılan işletim sistemlerinin (Unix, Linux, Windows, Pardus, Android, iOS) temel özellikleri				
3. hafta:	İşletim Sistemi ve yaygın kullanılan işletim sistemlerinin (Unix, Linux, Windows, Pardus, Android, iOS) temel özellikleri				
4. hafta:	İşletim Sistemi ve yaygın kullanılan işletim sistemlerinin (Unix, Linux, Windows, Pardus, Android, iOS) temel özellikleri				
5. hafta:	Unix/Linux İşletim sisteminin sağladığı güvenlik olanakları,				
6. hafta:	Unix/Linux İşletim sisteminin sağladığı güvenlik olanakları,				
7. hafta:	Windows İşletim sisteminin sağladığı güvenlik olanakları,				
8. hafta:	Windows İşletim sisteminin sağladığı güvenlik olanaklar				
9. hafta:	İşletim sisteminden kaynaklanan güvenlik açıkları				
10. hafta:	Süreç güvenliği, Erişim güvenliği				
11. hafta:	(KISA ARA SINAV) Kullanıcıların tanımlanması, Yetkilendirme,				
12. hafta:	Yetkilerin izlenmesi ve denetimi				
13. hafta:	Kullanım kayıtlarının tutulması				
14. hafta:	Güvenlik modelleri				

Kodu / Adı:	**Etik Güvenlik Kırma**				
Türü	Seçmeli	**Kredi**	3	**AKTS**	6
Dersin Amacı					
Bilgi güvenliği ihlallerinin ana unsuru olan güvenliği kırma(hack) yöntemleri ve pratik uygulamaları hakkında bilgi vermek, etik hacking yapılması yöntemlerinin öğretilmesi amaçlanmaktadır.					
Dersin İçeriği					
1. hafta:	Güvenlik kırmanın kısa tarihçesi				
2. hafta:	Modern bilişim sistemlerinin özelliği ve zayıflıkları				
3. hafta:	Güvenliği aşma metodolojileri				
4. hafta:	Keşif ve bilgi toplama				
5. hafta:	Sosyal Mühendislik				
6. hafta:	Tarama yöntemleri				
7. hafta:	Ağ istismarcılığı				
8. hafta:	Web istismarcılığı				
9. hafta:	İşletim sistemleri güvenliği				
10. hafta:	Yığıt parçalama				
11. hafta:	(KISA ARA SINAV) Kabuk komutlarıyla derin giriş				
12. hafta:	Erişim ve engellerin korunması13.				

13. hafta:	Sızma testi raporu geliştirme
14. hafta:	Vaka çalışmaları