DERS BİLGİ FORMU

<table>
<tr><td>DERSİN ADI</td><td colspan="4">MEDYADA SİBER GÜVENLİK</td></tr>
<tr><td>DERSİN SINIFI</td><td colspan="4">10. Sınıf</td></tr>
<tr><td>DERSİN SÜRESİ</td><td colspan="4">Haftalık 2 Ders Saati</td></tr>
<tr><td>DERSİN AMACI</td><td colspan="4">Bu derste öğrenciye; siber güvenlik alanında bilgi toplama teknikleri, ağ güvenliğini sağlama ve güvenlik yöntemlerini uygulama ile ilgili bilgi ve becerilerin kazandırılması amaçlanmaktadır.</td></tr>
<tr><td>DERSİN ÖĞRENME KAZANIMLARI</td><td colspan="4">1. Siber güvenlik araçlarını kullanarak işletim sistemi üzerinde işlemler yapar.
2. İşletim sistemi ve online araçlarını kullanarak bilgi toplar.
3. Sniffing tekniklerini bilir ve sniffing saldırılarının tespitini yapar.
4. İstenilen ihtiyaca uygun şifreleme algoritmalarını kullanır.</td></tr>
<tr><td>EĞİTİM-ÖĞRETİM ORTAM VE DONANIMI</td><td colspan="4">Ortam: Bilişim Teknolojileri laboratuvarı,

Donanım: Akıllı tahta/projeksiyon, bilgisayar, yazıcı/tarayıcı</td></tr>
<tr><td>ÖLÇME VE DEĞERLENDİRME</td><td colspan="4">Bu derste; öğrenci performansı belirlemeye yönelik çalışmalar değerlendirilirken gözlem formu, derecelendirme ölçeği ve dereceli puanlama anahtarı gibi ölçme araçlarından uygun olanlar seçilerek kullanılabilir.
Bunun yanında öz değerlendirme ve akran değerlendirme formları kullanılarak öğrencilerin, öğretimin süreç boyutuna katılmaları sağlanabilir.</td></tr>
<tr><td rowspan="5">KAZANIM SAYISI VE SÜRE TABLOSU</td><td>ÖĞRENME BİRİMİ</td><td>KAZANIM SAYISI</td><td>DERS SAATİ</td><td>ORAN (%)</td></tr>
<tr><td>Siber Güvenliğe Giriş</td><td>3</td><td>16</td><td>22</td></tr>
<tr><td>Bilgi Toplama Teknikleri</td><td>2</td><td>20</td><td>28</td></tr>
<tr><td>Sniffing Yöntem ve Uygulamaları</td><td>2</td><td>18</td><td>25</td></tr>
<tr><td>Şifreleme Teknikleri</td><td>3</td><td>18</td><td>25</td></tr>
<tr><td colspan="2">TOPLAM</td><td>10</td><td>72</td><td>100</td></tr>
</table>

ÖĞRENME BİRİMİ	KONULAR	ÖĞRENME BİRİMİ KAZANIMLARI ve KAZANIM AÇIKLAMALARI
Siber Güvenliğe Giriş	• Hacker ve Hacking Kavramları • Etik ve Güvenlik • Ağ Güvenliği Temelleri	**1. Hacker (Bilgisayar Korsanı) kimliğini ve hacking işlemini açıklar.** • Hacker özellikleri açıklanır. • Siyah Şapkalı, Beyaz şapkalı ve Gri Şapkalı Hacker özellikleri açıklanır. • Arka kapı ve kötü amaçlı yazılım özellikleri açıklanır. **2. Bilişimde etik kavramını ve siber güvenlik kavramını açıklar.** • Bilgi güvenliği uzmanlarının ahlaki sorumlulukları açıklanır. • Bilgi Gizliliği ve Etik kavramları açıklanır. • İnternet gizliliği ve önemi açıklanır. • Bilgi güvenliği uygulamasıyla ilgili yasal problemler ve telif hakları açıklanır. • Güncel tehditler ve saldırılar, dijital medyaya yönelik siber tehditler açıklanır. • Dijital adli bilişim tekniklerinin sahte haber ve bilgi manipülasyonunu tespit etmede kullanımı açıklanır. **3. Ağ güvenliğinin önemini dikkate alarak ağ saldırılarını algılama ve önleme kavramlarını açıklar.** • Ağ güvenliğinin önemi açıklanır. • Ağ güvenlik planın oluşturulması gereken adımlar açıklanır. • Ağ saldırılarını algılama ve önleme teknikleri açıklanır. • Ağ trafiğinin kontrol altına alınması teknikleri açıklanır. • Yetkisiz erişimin engellenmesi için alınması gereken teknikler açıklanır.
Bilgi Toplama Teknikleri	• Pasif bilgi toplama yöntemleri uygulamaları • Aktif bilgi toplama yöntemleri uygulamaları	**1. Bilgi toplama adımlarına dikkat ederek pasif bilgi toplama işlemlerini uygular**. • IP adresleri üzerinden bilgi toplama işlemlerini yaptırır. • Domainler üzerinden bilgi toplama işlemlerini yaptırır. • Web sayfalarından bilgi toplama işlemlerini yaptırır. **2. Bilgi toplama adımlarına dikkat ederek aktif bilgi toplama işlemlerini uygular.** • Ağ haritalama uygulamalarını kullanarak ağ haritası çıkarma açıklanır. • Ağ haritalama uygulamalarını kullanarak açık sistemleri tespit ettirir. • Ağ haritalama uygulamalarının parametrelerini kullandırır. • IP tarama tekniklerini kullandırarak, tarama

		işlemini yaptırır. • Port tarama tekniklerini kullandırarak, tarama işlemini yaptırır. • Portlarda servis tarama tekniklerini kullandırarak, tarama işlemini yaptırır. • Web üzerinden online port tarama tekniklerini kullandırarak, tarama işlemini yaptırır.
Sniffing Yöntem ve Uygulamaları	• Sniffer araçlarını kullanma • Sniffing saldırılarının tespiti	**1. Ağın analizini ve ağda oluşan problemleri çözmek için Sniffer araçlarını kullanır.** • Ağ ara yüzüne ulaşan paketleri incelemek için uygulama yaptırır. • Ağa yapılabilecek izinsiz girişleri yakalamak için uygulama yaptırır. • Çalışan uygulamaların ağa etkisini araştırmak için uygulama yaptırır. • Ağ geçidi ile bilgisayarların arasına girilmesi uygulamasını yaptırır. **2. Yapılan işleme göre belirlenen sniffing türüne göre araç kullanır**. • Mac Flooding sniffing tespitine karşı tedbirleri uygulatır. • Arp Poisoning siniffing tespitine karşı tedbirleri uygulatır.
Şifreleme Yöntemleri	• Simetrik Şifreleme yöntemleri • Asimetrik Şifreleme • Steganografi yöntemi	**1. Şifreleme adımlarına uygun olarak gizli anahtarlı-simetrik- şifreleme yöntemleri kullanır.** • DES (Data Encryption Standart) Veri Şifreleme Standartı uygulaması yaptırır. • Dijital kaynak koruma yöntemleri (Hash Fonksiyonları) uygulaması yaptırır. • Güvenli dosya alma ve gönderme uygulaması yaptırır. **2. Şifreleme adımlarına uygun olarak asimetrik şifreleme yöntemleri kullanır.** • Anahtar ikilisi ile şifreleme uygulaması yaptırır. **3. Şifreleme adımlarına uygun olarak steganografi şifreleme yöntemlerini kullanır.** • Resim içine resim koyarak şifreleme işlemini yaptırır. • Resim içine text-metin- gizleyerek şifreleme işlemini yaptırır.
UYGULAMA FAALİYETLERİ/TEMRİNLER		
Uygulama faaliyeti/temrinler; ders kazanımına uygun olarak okulun fiziki kapasitesi ve donatımı, öğrenci sayısı göz önünde bulundurularak en fazla uygulama faaliyeti/temrini yaptıracak şekilde meslek, alan zümre öğretmenler kurulu tarafından seçilir. Meslek, alan zümre öğretmenleri tarafından aşağıda yer alan temrinlerden farklı temrinlerin uygulanmasına karar verilebilir**.**		

Siber Güvenliğe Giriş	1. Ağ güvenlik planı oluşturmak 2. Siber olay sırasında süreç raporu hazırlamak 3. Siber olay sonrası süreç raporu hazırlamak
Bilgi Toplama Teknikleri	1. IP adresi bilinen noktaya ait bilgi toplama uygulaması yapmak 2. Domain adresi verilen bir web sitesine ait bilgilerinin toplanması uygulamasını yapmak 3. Web sayfalarından bilgi toplayan uygulama yapmak 4. Ağ haritasını çıkartma uygulaması yapmak 5. Ağ haritasındaki cihazların açıklarını tespit eden uygulama yapmak 6. Araçlar üzerinden port taraması uygulamaları yapmak 7. Online araçlar üzerinden port taraması uygulaması yapmak
Sniffing Yöntem ve Uygulamaları	1. Ağ ara yüzüne ulaşan paketleri inceleme uygulaması yapmak 2. Ağa yapılabilecek izinsiz girişleri yakalayan uygulama yapmak 3. Çalışan uygulamaların ağa etkisini inceleyen uygulamayı yapmak 4. Ağ geçidi ile bilgisayarların arasına girilmesi uygulamasını yapmak 5. Mac Flooding tekniği uygulamasını yapmak 6. Arp Poisoning siniffing tekniği uygulamasını yapmak
Şifreleme Teknikleri	1. Data Encryption Standart) Veri Şifreleme Standartı uygulaması yapmak 2. Hash Fonksiyonları kullanarak şifreleme uygulaması yapmak 3. Sezar şifreleme tekniği uygulaması yapmak 4. Gizli, anahtarlama şifreleme tekniği uygulaması yapmak 5. Anahtar ikilisi ile şifreleme uygulaması yapmak 6. Resim içine resim gizleyerek şifreleme uygulaması yapmak 7. Resim içine metin gizleyerek şifreleme uygulaması yapmak

DERSİN UYGULANMASINA İLİŞKİN AÇIKLAMALAR

1. Bu derste, verilen görevi yapma değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir.
2. Her öğrencinin uygulama yapması için ortam oluşturulmalıdır.
3. Uygulama faaliyetlerinde İş sağlığı ve güvenliğine ilişkin risk ve tehlike oluşturacak her türlü duruma karşı tedbirler alınmalıdır.
4. Bu dersin işlenişi sırasında yasalara uyma, çevre temizliği, emeğe saygı, özgüven, kendini ifade edebilme, emanete sahip çıkma, hedef belirleme, işbirliği, vb. değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir.
5. Bu etkinliklerde beyin fırtınası, grup tartışması, düz anlatım, soru cevap, örnek olay incelemesi gibi yöntem ve teknikler kullanılabilir.
6. Uygulama faaliyetleri ve temrinler örnek olup, örnekler çoğaltılmalıdır.