# ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
## TEKNİK BİLİMLER MESLEK YÜKSEK OKULU
## DİJİTAL DÖNÜŞÜM ELEKTRONİĞİ PROGRAMI

| Ders Adı: SCADA Sistemlerinde Siber Güvenlik<br>Ders Adi(İng): Cybersecurity in SCADA Systems | | | | | | Program : Dijital Dönüşüm Elektroniği | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dönem** | **Sınıfı** | **Ders Kodu** | **Teori** | **Uyg.** | **Lab.** | **Toplam** | **AKTS** | **Dili** | **Dersin Türü** |
| 1 | 2 | DDE207 | 2 | 1 | 0 | 3 | 5 | Türkçe | Seçmeli |

| | | |
|---|---|---|
| **Dersin Önkoşulu** | Yok | |
| **Dersin Koordinatörü** | | **e-mail :**<br>**Web :** |
| **Kurs Asistanı** | | **Mail :**<br>**Web :** |
| **Dersin Veriliş Şekli** | Yüz yüze | |
| **Dersin Amacı** | Bu dersin amacı, SCADA (Supervisory Control and Data Acquisition) sistemlerinin yapısını ve bu sistemlere yönelik olası siber tehditleri tanıtmak, SCADA altyapısında bilgi güvenliği sağlamak için gerekli önlemleri ve savunma tekniklerini öğretmektir. Öğrenciler, gerçek vakalar ve laboratuvar senaryoları üzerinden güvenlik açıklarını tespit etmeyi ve güvenli SCADA sistemleri kurmayı öğrenirler. | |

**Dersin Öğrenme Kazanımları**

| | |
|---|---|
| 1 | SCADA sistemlerinin mimarisini ve ağ yapılarını analiz eder |
| 2 | SCADA sistemlerine yönelik tehdit türlerini (malware, DoS, MITM) tanımlar |
| 3 | Endüstriyel kontrol sistemlerine yönelik uluslararası güvenlik standartlarını açıklar (ISA/IEC 62443, NIST SP800-82) |
| 4 | Güvenlik açığı tarama, izleme ve olay yanıt süreçlerini uygular. |
| 5 | Firewall, VPN, segmentasyon ve erişim kontrolü gibi savunma tekniklerini uygular |
| | |
| | |
| | |

| | |
|---|---|
| **Ders Kitabı, Referanslar ve/veya Diğer Kaynaklar** | Ders notları |

| | | | |
|---|---|---|---|
| | | | |
| **Değerlendirme** | | **Sayısı** | **(%) Katkı oranı** |
| | **Vize** | **1** | **40** |
| | **Ödev** | | |
| | **Sunum** | | |
| | **Final Sınavı** | **1** | **60** |

**Ders Planı**

| Hafta | Konular |
|---|---|
| 1 | SCADA sistemlerine giriş, mimari yapısı ve bileşenler |
| 2 | SCADA iletişim protokolleri (Modbus, DNP3, OPC, IEC 104) |
| 3 | SCADA sistemlerinin zafiyetleri ve tipik saldırı yüzeyleri |
| 4 | Siber tehdit türleri: Virüs, trojan, DoS, spoofing, sniffing |
| 5 | Siber saldırı örnekleri: Stuxnet, BlackEnergy, TRITON |
| 6 | Güvenlik politikaları, rol tabanlı erişim kontrolü |
| 7 | Ağ segmentasyonu ve firewall yapılandırmaları |
| 8 | Arasınav |
| 9 | Güvenli uzaktan erişim: VPN, SSH, şifreleme teknikleri |
| 10 | Olay izleme ve loglama sistemleri (SIEM, Syslog, IDS/IPS) |
| 11 | SCADA ağlarında güvenlik testi ve zafiyet tarama (Wireshark, Shodan vb.) |
| 12 | IEC 62443 ve NIST SP800-82 standartlarının temel ilkeleri |
| 13 | Siber olaylara müdahale ve kriz yönetimi |
| 14 | Final proje senaryosu geliştirme ve simülasyon |
| 15 | Final Sınavı |

| AKTS / İŞ YÜKÜ TABLOSU | | | |
|---|---|---|---|
| **Etkinlik** | **SAYISI** | **Süresi [Saat]** | **Toplam İş Yükü [Saat]** |
| **Teorik Dersler** | 14 | 2 | 28 |
| **Uygulamalı Dersler** | 14 | 1 | 14 |
| **Sınıf Dışı Ders Çalışma Süresi (Ön çalışma, pekiştirme)** | 14 | 1 | 14 |
| **Ödevler** | 10 | 2 | 20 |
| **Projeler** | 2 | 20 | 40 |
| **Arazi Çalışmaları** | 0 | 0 | 0 |
| **Arasınavlar** | 1 | 2 | 2 |
| **Diğer** | 2 | 8 | 16 |
| **Yarıyıl Sonu Sınavları** | 1 | 2 | 2 |
| **Toplam İş Yükü** | | | 136 |
| **Toplam İş Yükü / 30 saat** | | | 5 |