Eğitim İçeriği

Cybersecurity Expert Camp

Tüm Siber Güvenlik Eğitimleri 19 modül

Siber Güvenlik Nedir?

Siber güvenlik, dijital sistemleri, ağları, verileri ve cihazları siber saldırılardan koruma süreçlerini kapsayan bir alandır. Amaç, bilgi güvenliğini sağlamak, izinsiz erişimleri önlemek ve tehditlere karşı proaktif önlemler almaktır. Siber güvenlik, veri şifreleme, ağ güvenliği, kullanıcı erişim kontrolü ve güvenlik duvarı gibi yöntemlerle bireylerin ve işletmelerin dijital varlıklarını korur.

Siber Güvenlik Uzmanlık Kampı

Siber Güvenlik Kampı, dijital sistemleri koruma, veri güvenliğini sağlama ve siber tehditlere karşı önlem alma süreçlerini kapsayan kapsamlı bir eğitim programıdır. Kamp boyunca ağ güvenliği, zafiyet analizi, veri şifreleme, erişim kontrolü ve saldırı önleme yöntemleri gibi konular ele alınır.

Siber Güvenlik Kampına Neden Katılmalısınız?

Bu kamp, dijital ortamdaki güvenlik seviyesini artırmak, veri ihlallerini önlemek ve işletmelerin siber saldırılara karşı dayanıklılığını güçlendirmek isteyen profesyoneller için tasarlanmıştır. Siber güvenlik bilgisi, işletmelere stratejik koruma ve operasyonel verimlilik kazandırır.

Kimler Siber Güvenlik Kampına Katılabilir?

- IT uzmanları ve sistem yöneticileri
- Veri güvenliği alanında kariyer yapmak isteyenler
- Şirketlerin dijital güvenlik süreçlerini yöneten bireyler
- Kendi sistemlerinin güvenliğini sağlamak isteyen kişiler

Bu kamp, dijital dünyada güvenlik süreçlerini etkin bir şekilde yönetmek isteyen herkes için uygundur.

Siber Güvenlik Kampının Kariyere Yararları Nelerdir?

- Temel ve ileri düzey siber güvenlik alanında uzmanlık kazandırır.
- Veri güvenliği ve sistem koruma alanlarında yetkinlik sağlar.
- Şirketlerin siber tehditlere karşı dayanıklılığını artırır.
- İş dünyasında artan siber güvenlik talebine yanıt verme fırsatı sunar.

- Daha geniş iş olanakları ve profesyonel statü elde etme imkânı sağlar.

Kamp Sonunda Hangi Beceriler Kazanılır?

- Siber tehditleri tespit etme ve analiz etme
- Güvenlik duvarları ve saldırı önleme sistemlerini yönetme
- Veri şifreleme ve güvenlik politikaları oluşturma
- Ağ güvenliğini sağlama ve güvenlik açıklarını kapatma
- Siber saldırılara karşı proaktif savunma yöntemleri geliştirme

Eğitim Programı

1. Giriş ve Temel Bilgiler

1. Giriş ve Temel Bilgiler

1.1 Siber Güvenliğe Giriş

1.1 Siber Güvenliğe Giriş

- Siber güvenliğin tanımı ve önemi.
- Siber güvenlik tehdit türleri:
- • Malware (zararlı yazılımlar).
- • DDoS saldırıları.
- • Phishing saldırıları.
- • Zero-day saldırılar.
- Siber güvenlikte yasal mevzuatlar:
- • Kişisel Verilerin Korunması Kanunu (KVKK).
- • GDPR.
- • ISO 27001 standartları.
- Siber güvenlikte kariyer yolları:
- • CEH, OSCP, CISSP gibi sertifikalar.
- • Penetrasyon test uzmanı ve SOC analisti rolleri.

1.2 Kali Linux Kurulumu

1.2 Kali Linux Kurulumu

- Kali Linux için sanallaştırma araçlarının seçimi:
- • VirtualBox veya VMware kurulumu.
- Kali ISO dosyasının indirilmesi ve kurulumu.
- Kali'nin masaüstü ortamı ve araçlarına giriş:
- • Terminal kullanımı.

- • Dosya ve dizin yönetimi (ls, cd, mkdir vb.).
- Kali Linux araçlarının kısa tanıtımı:
- • Nmap: Ağ tarama.
- • Metasploit: Exploit framework.
- • Wireshark: Paket analizi.

2. Ağ Güvenliği ve Network Temelleri

2. Ağ Güvenliği ve Network Temelleri

2.1 Network Temelleri

2.1 Network Temelleri

- Ağ türleri:
- • LAN, WAN, MAN, WLAN, VPN.
- • Peer-to-peer ve client-server ağ yapıları.
- Ağ cihazları:
- • Router, Switch, Hub, Access Point.
- • Firewall ve IDS/IPS sistemleri.
- OSI modeli:
- • 7 katmanın detaylı açıklaması (Fiziksel Katman'dan Uygulama Katmanı'na kadar).
- • TCP/IP modeline geçiş.
- Protokoller:
- • HTTP/HTTPS: Web trafiği.
- • FTP ve SSH: Dosya aktarımı ve güvenli oturum.
- • DNS: Alan adı çözümleme.
- • DHCP: IP dağıtımı.

2.2 IP Adresleme ve Subnetting

2.2 IP Adresleme ve Subnetting

- • IPv4 ve IPv6 karşılaştırması.
- • CIDR ve subnet mask hesaplama örnekleri.
- • VLSM (Variable Length Subnet Masking) ile ağ optimizasyonu.

2.3 Network Tarama ve Keşif Araçları

2.3 Network Tarama ve Keşif Araçları

- Nmap ile Port ve Servis Tarama:
- • Açık portların tespiti.
- • Hedef cihaz üzerinde servislerin analizi.

- Wireshark ile Paket Analizi:
- • Canlı trafik yakalama.
- • Filtreleme teknikleri (ör. yalnızca HTTP paketlerini izleme).
- Cisco Packet Tracer ile Ağ Topolojisi:
- • IP adresleme ve routing yapılandırması.
- • Switch ve router senaryoları.

3. Zafiyet Tarama ve Exploit Temelleri

3. Zafiyet Tarama ve Exploit Temelleri

3.1 Zafiyet Tarama Araçları

3.1 Zafiyet Tarama Araçları

- OpenVAS ve Nessus:
- • Tarama profilleri ve raporlama.
- • Kritik zafiyetlerin analizi.

3.2 Exploit Framework’ler

3.2 Exploit Framework’ler

- Metasploit Framework:
- • Exploit nedir? Exploit kullanımı ve çeşitleri.
- • Payload ve shell türleri (Reverse Shell, Bind Shell).

3.3 OpenVAS ile Zafiyet Tarama

3.3 OpenVAS ile Zafiyet Tarama

- • Tarama işlemi oluşturma ve zafiyet raporlarının analizi.

3.4 Metasploit ile Exploit Kullanımı

3.4 Metasploit ile Exploit Kullanımı

- • Sistem açığına yönelik exploit oluşturma.
- • Meterpreter oturumu ile hedef sistem kontrolü.

4. Web Uygulama Güvenliği

4. Web Uygulama Güvenliği

4.1 Web Güvenlik Temelleri

4.1 Web Güvenlik Temelleri

- • HTTP/HTTPS protokolleri.
- • Güvenli şifreleme yöntemleri (SSL/TLS).

4.2 OWASP Top 10

4.2 OWASP Top 10

- • Injection (SQL Injection, Command Injection).
- • Broken Authentication.
- • XSS (Cross-Site Scripting).
- • CSRF (Cross-Site Request Forgery).

4.3 SQL Injection Senaryoları

4.3 SQL Injection Senaryoları

- • DVWA (Damn Vulnerable Web Application) ile SQL Injection simülasyonu.

4.4 Burp Suite Kullanımı

4.4 Burp Suite Kullanımı

- • Proxy ile trafik izleme ve analiz.
- • POST isteklerini değiştirme.

4.5 Nikto ile Web Taraması

4.5 Nikto ile Web Taraması

- • Hedef sistemin güvenlik açıklarını raporlama.

5. Kablosuz Ağ Güvenliği

5. Kablosuz Ağ Güvenliği

5.1 Kablosuz Ağ Protokolleri

5.1 Kablosuz Ağ Protokolleri

- • WEP, WPA, WPA2 ve WPA3 protokolleri.
- WEP, WPA, WPA2 ve WPA3 protokolleri.
- • EAP ve PSK yöntemleri.

5.2 Kablosuz Ağ Saldırı Türleri

5.2 Kablosuz Ağ Saldırı Türleri

- • Evil Twin saldırıları.
- • Man-in-the-middle saldırıları.

5.3 Aircrack-ng ile WPA Handshake Yakalama

5.3 Aircrack-ng ile WPA Handshake Yakalama

- • Handshake yakalama ve parola kırma simülasyonu.

5.4 Fern WiFi Cracker Kullanımı

5.4 Fern WiFi Cracker Kullanımı

- • Otomatik saldırı senaryoları oluşturma.

6. Sosyal Mühendislik ve Uygulama

6. Sosyal Mühendislik ve Uygulama

6.1 Social Engineering Toolkit Kullanımı

6.1 Social Engineering Toolkit Kullanımı

- • Phishing sayfası oluşturma.
- • Kimlik bilgisi toplama senaryosu geliştirme.

7. Şifre Kırma ve Parola Güvenliği

7. Şifre Kırma ve Parola Güvenliği

7.1 Hydra ile Brute Force

7.1 Hydra ile Brute Force

7.2 John the Ripper ile Hash Kırma

7.2 John the Ripper ile Hash Kırma

8. Dosya Analizi ve Zararlı Yazılımlar

8. Dosya Analizi ve Zararlı Yazılımlar

8.1 Binwalk ve Strings ile Dosya Analizi

8.1 Binwalk ve Strings ile Dosya Analizi

8.2 Virüs Yapılarının Analizi

8.2 Virüs Yapılarının Analizi

9. Açık Kaynak Çözümlerle SOC

9. Açık Kaynak Çözümlerle SOC

9.1 Pfsense ile Firewall Yapılandırması

9.1 Pfsense ile Firewall Yapılandırması

9.2 Wazuh ile SIEM Yönetimi

9.2 Wazuh ile SIEM Yönetimi

9.3 Zabbix ile Ağ İzleme ve Alarm Yönetimi

9.3 Zabbix ile Ağ İzleme ve Alarm Yönetimi

Bu eğitimi kurumunuza özel planlayalım. İçerik, süre ve uygulama senaryoları ekiplerinizin rolüne ve seviyesine göre uyarlanabilir. www.impress.com.tr/iletisim