EMA SECURITY

Pentest Uzmanlığı Eğitimi

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Pentest Uzmanlığı Eğitimi

Eğitim Açıklaması

Pentest Uzmanlığı Eğitimi, ağ ve sistemlerdeki güvenlik açıklarını tespit etmek amacıyla penetrasyon testleri yapma becerisini kazandırır. Katılımcılar, bir hedefin zayıf noktalarını keşfetmek için kullanılan ileri düzey araç ve teknikleri öğrenirler. Bu eğitim, profesyonellere güçlü bir güvenlik altyapısı kurma ve olası saldırılara karşı savunma sağlama yeteneği kazandırır. Eğitim sonunda, katılımcılar kendi pentest raporlarını hazırlayabilecek ve şirketlerinin siber güvenliğini artırmak için etkili stratejiler geliştirebilecektir.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 5 Gün

Eğitim Seviyesi

- Orta
- İleri

Eğitim İçin Ön Gereksinimler

- Temel ağ ve sistem yönetimi bilgisi
- Programlama ve script yazma bilgisi
- Bilgisayar ağları, TCP/IP protokolleri ve firewall yapılarına hakimiyet
- Temel ethical hacking bilgisi (Etik hacking, sızma testi, açık kaynaklar, vb.)

Eğitimi Kimler Katılmalı?

- Penetrasyon testi konusunda daha derin bilgi sahibi olmak isteyenler
- Siber güvenlik uzmanları ve ağ güvenliği analistleri
- Etik hackerlar ve güvenlik test uzmanları
- Saldırı simülasyonu ve kırılma tekniklerini öğrenmek isteyen IT profesyonelleri

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, sızma testi yapmayı ve ağlarda güvenlik açıklarını tespit etmeyi öğrenir, siber güvenlik uzmanı olarak yetkinlik kazanırlar.

Eğitim İçeriği

- Penetrasyon Testi Temelleri
- Penetrasyon Testi Tanımı ve Süreçleri
- Penetrasyon testinin amacı ve kapsamı
- Test öncesi, sırası ve sonrası yapılması gerekenler
- Etik hackerlık prensipleri ve yasal yükümlülükler
- Test metodolojileri: OSSTMM, NIST 800-115, PTES, OWASP
- Test Planlaması ve Bilgi Toplama
- Müşteri ile görüşme, hedef belirleme
- Hedef sistemin profillemesi: IP/port taramaları, servis keşfi
- OSINT ve aktif bilgi toplama (Shodan, Google Dorking, DNSdumpster)
- Hedef sistemde açık kaynak araçlarıyla keşif yapma
- Ağ Penetrasyon Testi (Network Penetration Testing)
- Keşif ve Tarama
- Ağ topolojisinin çıkarılması (traceroute, pathping)
- Port ve servis taraması (Nmap, Masscan, Unicornscan)
- Versiyon tespiti ve fingerprinting
- SMB, RDP, FTP, HTTP, DNS gibi yaygın servislerin istismarı
- Kimlik Bilgisi Ele Geçirme
- Hedef ağı dinleme (Wireshark, tcpdump)
- Kimlik bilgisi toplama teknikleri (sniffing, ARP poisoning)
- SMB, FTP, Telnet ve HTTP protokollerinde parolaları kırma
- Pass-the-Hash, Pass-the-Ticket, Kerberos istismarları
- Yetki Yükseltme
- Lateral hareket ve ağdaki diğer sistemlere geçiş
- SMB, RDP, WMI, WinRM kullanarak lateral hareket
- Metasploit, Empire, Cobalt Strike kullanımı
- Erişim kazanıldıktan sonra kalıcılık sağlama yöntemleri
- Web Uygulama Penetrasyon Testi (Web Application Penetration Testing)

Eğitim İçeriği

- Web Uygulama Saldırıları
- SQL Injection, XSS, CSRF, RCE (Remote Code Execution)
- API saldırıları: JWT, OAuth token manipülasyonu
- File Upload, Path Traversal, XML External Entity (XXE) Injection
- Insecure Deserialization, Command Injection
- Subdomain enumeration ve DNS Hijacking
- Web Uygulama Güvenlik Testleri
- Burp Suite, OWASP ZAP kullanarak web uygulaması taraması
- SQLi ve XSS zafiyetlerinin elle tespiti
- Web servislerinin test edilmesi: SOAP, REST API
- Session hijacking ve Session Fixation
- Web uygulaması güvenlik duvarlarının (WAF) atlatılması
- Sistem Penetrasyon Testi (System Penetration Testing)
- Linux ve Windows Sistemlerinde Zafiyetler
- Linux sistemlerinde: Sudo, su, setuid zafiyetleri
- Windows sistemlerinde: SMBv1, EternalBlue, PowerShell exploitation
- Sistem konfigürasyon hataları ve yama yönetimi
- Privilege escalation teknikleri (Kernel Exploits, Local Exploits)
- Malware analysis ve post-exploitation
- Scripting ve Otomasyon
- Python, Bash ve PowerShell ile exploit geliştirme
- Metasploit Framework kullanarak saldırı senaryoları
- Exploit kodlarını inceleme ve hedefe özel yazılım geliştirme
- Saldırıların otomatikleştirilmesi: Veil-Evasion, Cobalt Strike
- Kablosuz Ağ Penetrasyon Testi (Wireless Penetration Testing)
- Kablosuz Ağ Analizi
- Wi-Fi ağlarının keşfi: Kapsama alanı, kanal analizi

Eğitim İçeriği

- WPA2/WPA3 parolası kırma (Wordlist ve Dictionary-based)
- WPS güvenlik açıkları ve saldırılar
- Evil Twin saldırıları, Rogue AP saldırıları
- Man-in-the-Middle (MITM) saldırıları (Wireshark, Aircrack-ng)
- Bulut Penetrasyon Testi (Cloud Penetration Testing)
- Bulut Altyapılarında Güvenlik Testleri
- AWS, Azure, GCP üzerinde güvenlik zafiyetleri
- IAM (Identity and Access Management) hataları
- S3 bucket misconfigurations ve veri sızdırma
- API anahtarları, JWT token güvenlik açıkları
- AWS Lambda, EC2 instance ve Cloud Functions güvenlik testleri
- Sosyal Mühendislik ve Phishing Testleri (Social Engineering and Phishing)
- Sosyal Mühendislik Saldırıları
- Phishing saldırıları: E-posta, SMS, sosyal medya
- CEO fraud, Business Email Compromise (BEC)
- Spear phishing ve credential harvesting
- Telefonla sosyal mühendislik saldırıları
- E-posta ve Web Sayfası Phishing Testleri
- E-posta spoofing ve kimlik avı
- Fake login sayfaları, URL masking
- E-posta spam tespiti ve analiz teknikleri
- Raporlama ve Sonuçların Sunulması
- Penetrasyon Testi Raporunun Yazılması
- Test planı, kullanılan araçlar ve metodolojiler
- Zafiyetlerin tanımlanması, etkilerinin değerlendirilmesi
- Çözüm önerileri ve önceliklendirilmiş düzeltme işlemleri
- Risk değerlendirme (CVE sistemine göre)
- İletişim ve Sunum
- Güvenlik raporunun üst yönetime sunulması
- Teknik detayların anlaşılır bir şekilde sunulması
- Güvenlik boşluklarının iyileştirilmesi için öneriler

Sıkça Sorulan Sorular

Pentest uzmanlığı eğitimi hangi seviyelerdeki katılımcılar için uygundur?

- Eğitim, temel ağ güvenliği ve sistem bilgisine sahip olan katılımcılar için uygundur. Eğer bu alanlarda temel bilginiz varsa, eğitimden verimli sonuç alabilirsiniz.

Pentest yaparken dikkat edilmesi gereken en önemli etik kurallar nelerdir?

- Pentest sırasında yasal izinler alınmalı, müşteri bilgileri gizli tutulmalı ve yalnızca belirlenen sınırlar içinde testler yapılmalıdır.

Pentest uzmanı olarak hangi iş fırsatlarını değerlendirebilirim?

- Pentest uzmanları, bağımsız danışmanlık yapabilir veya büyük güvenlik firmalarında, devlet kurumlarında, özel sektörde güvenlik analisti olarak çalışabilir.