EMA SECURITY

Beyaz Şapkalı Hacker 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

Beyaz Şapkalı Hacker Eğitimi

Eğitim Açıklaması

Beyaz Şapkalı Hacker 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

- Başlangıç
- Orta

Eğitim İçin Ön Gereksinimler

- Temel ağ ve internet bilgisi
- Linux/Unix işletim sistemlerine aşinalık
- Temel programlama bilgisi (Python, Bash, vb.)
- Temel güvenlik açıkları ve siber tehditlere dair genel bilgi

Eğitimi Kimler Katılmalı?

- Siber güvenlik alanında kariyer yapmak isteyenler
- Güvenlik araştırmacıları ve analistleri
- Penetrasyon testine ilgi duyan IT profesyonelleri
- Etik hacking yapmayı öğrenmek isteyen yazılım geliştiriciler

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, etik hacking ve sızma testleri konusunda bilgi sahibi olup, güvenlik açıklarını tespit etme ve savunma yapma becerisi kazanırlar.

Eğitim İçeriği

- Etik Hackerlık Temelleri
- Etik Hackerlık Nedir?
- Beyaz şapkalı hacker (etik hacker) tanımı
- Yasal sorumluluklar ve etik kurallar (CEH, OSCP, CISSP gibi sertifikalar)
- Hacker türleri: Beyaz, siyah ve gri şapkalılar
- Yasal ve etik hacking sınırları
- Etik Hackerlık Süreçleri
- Penetrasyon testi metodolojileri: OSSTMM, PTES, OWASP
- Penetrasyon testinin aşamaları: keşif, saldırı, raporlama
- İleri düzey testler: Güvenlik değerlendirmesi, zafiyet analizi
- Yasal uyarılar ve test sözleşmesi
- Saldırı Teknikleri ve Metodolojiler
- Keşif (Reconnaissance)
- Pasif Keşif: OSINT (Open Source Intelligence), Google Dorking, DNSdumpster
- Aktif Keşif: Port tarama (Nmap, Masscan), servis ve versiyon tespiti
- Hedef Profil Oluşturma: Hedef sistemin mimarisini çıkarma, ağ topolojisi analizi
- Zafiyet Tespiti (Vulnerability Assessment)
- Manuel ve otomatik zafiyet taraması (Nessus, OpenVAS)
- Web uygulama güvenlik testleri (OWASP Top 10: SQLi, XSS, CSRF)
- Sistem zafiyetlerinin tespiti (Misconfigurations, güvenlik yamaları)
- İstismar (Exploitation)
- Web Uygulama İstismarı: SQL Injection, XSS, Command Injection
- Ağ İstismarı: ARP Spoofing, DNS Spoofing, SMB/NTLM relay saldırıları
- Sistem İstismarı: Privilege escalation, Local Exploits (Linux, Windows)
- Kablosuz Ağ İstismarı: Wi-Fi parolası kırma (WPA/WPA2), Evil Twin saldırıları
- Yetki Yükseltme (Privilege Escalation)
- Linux ve Windows sistemlerinde yetki yükseltme teknikleri
-

Eğitim İçeriği

- Kernel ve yazılım zafiyetleri kullanarak root/admin hakları elde etme
- Credential dumping (Mimikatz, LSASS dump)
- Savunma ve Önleme Stratejileri
- Saldırı Tespiti ve İzleme
- IDS/IPS (Intrusion Detection/Prevention Systems): Suricata, Snort, Zeek
- Log Yönetimi ve Korelasyon: SIEM araçları (Splunk, ELK Stack, Security Onion)
- Anomali Tespiti: Ağ trafiği analizi, anomalilerin tespiti
- Zararlı Trafik Analizi: DNS tunneling, HTTP/S tunneling
- Güvenlik Duvarları ve Filtreleme
- Ağ güvenlik duvarı konfigürasyonları (iptables, pfSense)
- WAF (Web Application Firewall) kullanımı ve bypass teknikleri
- Proxy ve VPN ile ağ gizliliği sağlama
- Şifreleme ve Veri Güvenliği
- SSL/TLS güvenliği, SSL/TLS certifikaları ve saldırılar (BEAST, POODLE)
- Şifreleme algoritmaları (AES, RSA) ve zayıf şifreleme uygulamaları
- Anahtar yönetimi ve veri sızıntısı önleme (DLP) sistemleri
- Web Uygulama Güvenliği
- Web Uygulama Zafiyetleri
- OWASP Top 10: SQLi, XSS, CSRF, Insecure Deserialization, Command Injection
- Web uygulamalarında kullanıcı doğrulama zafiyetleri
- API güvenliği: RESTful API zafiyetleri, JWT token manipülasyonu
- Cookie güvenliği ve session hijacking
- Web Uygulama Güvenliği Araçları
- Burp Suite: Web uygulama tarama ve güvenlik testleri
- OWASP ZAP: Web uygulama güvenliği açıklarını tespit etme
- Nikto: Web sunucusu güvenlik taraması
- SQLmap: SQL Injection testleri

Eğitim İçeriği

- Ağ ve Sistem Güvenliği
- Ağ Penetrasyon Testi
- Port Taraması: Nmap, Masscan, Unicornscan
- Servis Tespiti ve Exploit: Metasploit kullanımı, zafiyetlerin istismarı
- SMB, SSH, RDP İstismarı: Brute force saldırıları, parola kırma
- MITM (Man in the Middle): ARP Spoofing, SSL Strip, DNS Spoofing
- Sosyal Mühendislik: Phishing saldırıları, manipülasyon teknikleri
- Sistem Güvenliği Testleri
- Linux: Sudo, setuid, .bashrc zafiyetleri
- Windows: EternalBlue, SMB, PowerShell exploitleri
- Network Services: SNMP, FTP, RDP, DNS istismarları
- Raporlama ve Sonuçların Sunulması
- Penetrasyon Testi Raporu Yazma
- Test planı, metodoloji ve kullanılan araçlar
- Zafiyetlerin tanımlanması, etkilerinin açıklanması
- İyileştirme ve güvenlik önlemleri önerileri
- Raporun sunulması: Teknik ve yöneticilere yönelik sunum

Sıkça Sorulan Sorular

Beyaz şapkalı hacker olmak için hangi becerilere sahip olmam gerekiyor?

- Bu eğitim, etik hacking konusunda temel bilgi ve becerileri kazandırmayı amaçlamaktadır. Programlama bilgisi, ağ güvenliği, sızma testleri gibi temel alanlarda bilgi sahibi olmanız faydalıdır.

Beyaz şapkalı hacker ile siyah şapkalı hacker arasındaki fark nedir?

- Beyaz şapkalı hackerlar, güvenliği test etmek ve güvenlik açıklarını tespit etmek için etik ve yasal olarak çalışırken, siyah şapkalı hackerlar, yasa dışı faaliyetlerde bulunurlar.

Eğitim sonunda hangi sertifikaları alabilirim?

- Eğitim sonunda katılım sertifikası verilecek olup, ayrıca global olarak tanınan CEH (Certified Ethical Hacker) gibi sertifikalara hazırlık yapabilirsiniz.