EMA SECURITY

Ağ Saldırı ve Savunma 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

Ağ Saldırı ve Savunma Eğitimi

Eğitim Açıklaması

Ağ Saldırı ve Savunma Eğitimi, ağ güvenliği konusunda derinlemesine bilgi edinmek isteyen profesyonellere yönelik bir programdır. Katılımcılar, ağ saldırıları, bu saldırılara karşı etkili savunma yöntemleri ve güvenlik duvarı yapılandırmalarını öğrenirler. Eğitimde, ağdaki güvenlik açıkları, izinsiz erişim tespit teknikleri ve saldırılara karşı savunma stratejileri ele alınacaktır. Katılımcılar, ağları izinsiz girişlere karşı koruma becerisi kazanacaklardır.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 3 Gün

Eğitim Seviyesi

- Orta
- İleri

Eğitim İçin Ön Gereksinimler

- Temel ağ yapıları ve protokolleri bilgisi
- Güvenlik duvarları ve yönlendirici yapılarına hakimiyet
- Ağ saldırılarını tanıma ve savunma stratejileri

Eğitimi Kimler Katılmalı?

- Ağ güvenliği alanında uzmanlaşmak isteyenler
- Güvenlik uzmanları, ağ yöneticileri ve sistem analistleri
- Siber saldırı simülasyonları ve ağ savunması ile ilgilenen profesyoneller

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, ağ üzerindeki saldırı tekniklerini ve savunma stratejilerini öğrenir, ağ güvenliğini sağlama becerisi kazanırlar.

Ağ Saldırı ve Savunma Eğitimi

Eğitim İçeriği

- Keşif ve Bilgi Toplama
- Pasif Bilgi Toplama
- OSINT teknikleri: Shodan, Censys, Google Dorking
- DNS ve WHOIS analizleri
- Netflow ve Metadata analizi
- Aktif Bilgi Toplama
- Port tarama ve servis tespiti (Nmap, Masscan)
- Versiyon tanımlama ve fingerprinting (WhatWeb, Banner Grabbing)
- Ağ topolojisi çıkarımı (traceroute, path MTU discovery)
- Ağ Katmanlı Saldırılar (Layer 2-4)
- Katman 2 (Data Link) Saldırıları
- ARP Spoofing & Poisoning (Bettercap, Ettercap)
- STP manipülasyonu ve BPDU spoofing
- DHCP Starvation & Rogue Server
- MAC Flooding ve CAM table saldırıları
- Katman 3-4 Saldırıları
- IP Spoofing, ICMP redirect saldırıları
- TCP Hijacking & Session Prediction
- DNS Cache Poisoning
- SYN Flood, UDP Flood, ICMP Flood
- Ağ Hizmetlerine Yönelik Saldırılar
- DNS hizmetlerine saldırılar (Zone Transfer, DNS tunneling, NXDOMAIN flood)
- SMTP & Mail sunuculara yönelik istismarlar (open relay, spoofing)
- FTP/TFTP zafiyetleri ve credential sniffing
- SNMP abuse (default community strings, information disclosure)
- NFS, SMB, RDP gibi protokollerin abuse edilmesi
- VPN tünelleri ve kimlik doğrulama atlatma (Split tunneling abuse)
- Erişim Sağlama ve Lateral Movement

Ağ Saldırı ve Savunma Eğitimi

Eğitim İçeriği

- Exploit kullanarak sistemlere sızma (Metasploit, CVE uygulamaları)
- Credential harvesting (cleartext protocols, hash sniffing)
- SSH key hijacking ve reuse
- ProxyChains, Dynamic Port Forwarding, VPN pivoting
- Network pivoting ve çapraz VLAN geçiş senaryoları
- Ağ Güvenliğini Sertleştirme ve Segmentasyon
- Network segmentation ve Zero Trust mimarisi
- NAC sistemleri (802.1X, RADIUS tabanlı kontrol)
- VLAN yapılandırmaları ve segmentasyon hataları
- ACL, Firewall ve Router üzerinde kural seti oluşturma
- IoT ve OT cihazlarda network izolasyonu
- IDS/IPS Sistemleri ve Anomali Tespiti
- Saldırı tespit sistemleri: Suricata, Snort, Zeek
- Signature-based vs. anomaly-based tespit farkları
- Port scan, beaconing, DoH trafiği tespiti
- Custom rule yazımı (Snort, Suricata)
- Netflow, PCAP ve full-packet capture analizi
- Loglama ve Olay İzleme
- Syslog, Rsyslog ve journald logları merkezi toplama
- Log konsolidasyon (SIEM sistemleri: Wazuh, ELK, Splunk)
- IDS/IPS logları, NetFlow/PCAP kayıtları analizi
- Ağ saldırılarına yönelik özel log korelasyon senaryoları
- Zararlı Trafik ve Komuta Kontrol (C2) Tespiti
- DNS tabanlı C2 iletişimi analizi (beaconing pattern)
- HTTP/S C2 protokolleri ve anormal User-Agent tespiti
- Tor, I2P, VPN ve Tunneling trafiği anomali analizi

Ağ Saldırı ve Savunma Eğitimi

Eğitim İçeriği

- Cobalt Strike ve Empire beacon davranışlarının ayırt edilmesi
- Uygulamalı Saldırı ve Savunma Senaryoları
- Ağ taraması → Kimlik bilgisi ele geçirme → Erişim → Lateral movement
- ARP spoofing ile MITM → FTP parolası çalma → Shell erişimi
- DNS tunneling ile veri dışarı sızdırma → Zeek ile tespit
- DHCP spoofing → rogue gateway → trafik yönlendirme
- IDS logları ve firewall event'leri üzerinden korelasyon ve alarm senaryoları

Sıkça Sorulan Sorular

Ağ saldırılarını önlemek için hangi güvenlik önlemleri alınmalıdır?

- Güçlü şifreleme, IDS/IPS sistemleri, VPN kullanımı, güvenlik duvarı yapılandırmaları ve ağ segmentasyonu gibi yöntemlerle ağları koruyabilirsiniz.

Bu eğitimde hangi saldırı türleri üzerinde çalışılacak?

- Eğitimde, DoS/DDoS saldırıları, ARP spoofing, MITM (Man-in-the-Middle) saldırıları, DNS spoofing gibi ağ tabanlı saldırılar ele alınacaktır.

Ağ savunma stratejileri nelerdir?

- Ağ savunmasında, güvenlik duvarları, saldırı tespit ve önleme sistemleri (IDS/IPS), VPN'ler ve ağ segmentasyonu gibi yöntemler kullanılır.

Eğitim sonunda hangi beceriler kazanılacak?

- Katılımcılar, ağ saldırılarını analiz etme, tespit etme ve savunma stratejileri geliştirme becerisi kazanacaklar.