# SİBER GÜÇ KAMPI EĞİTİM İÇERİĞİ

## BİLİŞİM GÜVENLİĞİ SIZMA TESTİ EĞİTİMİ (5 Gün – Uygulamalı)

TEMEL SIZMA TESTİ METODU

SALDIRI (GİRDİ) NOKTALARI

METOD VE ARAÇLAR(Uygulamalı Giriş)

SİSTEM ELE GEÇİRME SENARYOLARI

KALI LINUX'A GİRİŞ

- Kali Linux Nedir?
- Linux Shell Ortamı
- Linux Dosya Sistemi İşlemleri
- Linux Dosya Bulma İşlemleri
- Linux Shell Scripting
- Linux Kullanıcı Yönetimi
- Linux Ağ Trafiği İzleme
- Kali Linux Servis Yönetimi
- Linux Uygulama Kurulumu
- Editörler ve Dosya İzleme Araçları

BİLGİ TOPLAMA

- Hedef IP Aralığı Tespiti
- Canlı Sunucu Tespiti
- Port Tarama
- Servis ve İşletim Sistemi Tespiti
- Kullanıcı Tespiti

METASPLOIT VE METERPRETER

- Metasploit Kullanımı
- Meterpreter Kullanımı
- Post Exploitation ve Yetki Yükseltme
- Handler Modülü
- Hashdump

BELLEK TAŞMA AÇIKLIKLARI

- Stack Tabanlı Bellek Taşması
- Kullanılacak Araçlar
- Uygulamanın Fuzz Edilmesi

- Python Script
- EIP Register Kontrolü
- Stack Alanı
- Bad Char
- Return Address – JMP ESP
- Shellcode
- Metasploit Exploit Ekleme Adımları

WEB UYGULAMA AÇIKLIKLARI

- Web Uygulama Açıklıklarının Önemi
- Sistem Ele Geçirmeye Yol Açabilecek Web Uygulama Açıklıkları
- Sistem Ele Geçirme Saldırı Ağacı
- SQL Injection Senaryosu
- Dizin Aşım Senaryosu
- Dosya Yükleme Senaryosu
- Web Saldırılarına Etki Eden Faktörler
- SQLMAP Aracının Etkinliği

PAROLA KIRMA SALDIRILARI

- Parola Saldırı Türleri
- Hashing Algoritması
- Salt Yöntemi
- Rainbow Tables & Online Crackers
- Linux Hash Kırma
- Windows Hash Kırma
- MySQL Hash Kırma
- Çevrimiçi (Online) Parola Kırma

İSTEMCİ TARAFLI SALDIRILAR

PORT YÖNLENDİRME

YETKİ YÜKSELTME

- Linux Bilgi Toplama
- Linux Root Erişim Yöntemleri
- Windows Bilgi Toplama
- Windows System Erişim Yöntemleri