Penetration Testing with Kali Linux (PWK) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Kali ile Penetrasyon Testi (PWK), profesyonel penetrasyon testi dünyasına ciddi ve anlamlı bir adım atmak isteyen ağ yöneticileri ve güvenlik profesyonelleri için tasarlanmış bir penetrasyon testi eğitimidir. Bu benzersiz penetrasyon testi eğitimi, katılımcılara eğitim materyallerini uygulamak için uzaktan, sanal penetrasyon testi laboratuvarları dahil olmak üzere en son etik hackleme araçlarını ve tekniklerini tanıtır. Kali Linux ile Penetrasyon Testi, katılımcıları hedef açısından zengin, çeşitli ve savunmasız bir ağ ortamına enjekte ederek baştan sona tam bir penetrasyon testini simüle eder.

Lütfen bu eğitim almış katılımcılar için isteğe bağlı 24 saatlik laboratuvar tabanlı bir sertifika sınavının mevcut olduğunu unutmayın. Bu sınav, Offensive Security Certified Professional (OSCP) sertifikasına götürür ve doğrudan Offensive Security ile rezerve edilmelidir.

Prerequisites

Kali Linux ile Penetrasyon Testi temel bir eğitimdir, ancak yine de katılımcılar çevrim içi derse katılmadan önce belirli bilgilere sahip olmasını gerektirir. TCP/IP, ağ ve makul Linux becerileri hakkında sağlam bir anlayış gereklidir. Temel Perl veya Python ile birlikte Bash betikleme konusunda bilgi sahibi olmak bir artı olarak kabul edilir.

What You Will Learn

- Kali Linux ile Penetrasyon Testi
- Penetrasyon Testi: Bilmeniz Gerekenler
- Kali Linux ile Rahat Etmek
- Temel Araçlar
- Pasif Bilgi Toplama
- Aktif Bilgi Toplama
- Güvenlik Açığı Tarama
- Arabellek Taşmaları
- Win32 Arabellek Taşması İstismarı
- Linux Arabellek Taşması İstismarı
- İstismarlarla Çalışma
- Dosya Transferleri
- Ayrıcalık Yükseltme
- İstemci Tarafı Saldırıları
- Web Uygulaması Saldırıları
- Parola Saldırıları
- Port Yönlendirme ve Tünelleme
- Metasploit Çerçevesi
- Antivirüs Yazılımını Atlatma
- Parçaları Birleştirme: Penetrasyon Testi Ayrıntıları

Penetration Testing with Kali Linux (PWK) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

0 Penetrasyon Testi: Bilmeniz Gerekenler

- 0.1 Kali Linux Hakkında
- 0.2 Penetrasyon Testi Hakkında
- 0.3 Yasal
- 0.4 megacorpone.com Alanı
- 0.5 Offensive Security Labs
- 0.5.1 VPN Labs Genel Bakış
- 0.5.2 Lab Kontrol Paneli
- 0.5.3 Raporlama

1. Kali Linux ile Rahatlamak

- 1.1 Kali'de Yolunuzu Bulmak
- 1.1.1 Kali Linux'u Başlatmak
- 1.1.2 Kali Menüsü
- 1.1.3 Bul, Bul ve Hangisi
- 1.1.4 Alıştırmalar
- 1.2 Kali Linux Hizmetlerini Yönetmek
- 1.2.1 Varsayılan kök Parolası
- 1.2.2 SSH Hizmeti
- 1.2.3 HTTP Hizmeti
- 1.2.4 Alıştırmalar
- 1.3 Bash Ortamı
- 1.4 Bash Komut Dosyası Yazmaya Giriş
- 1.4.1 Pratik Bash Kullanımı – Örnek 1
- 1.4.2 Pratik Bash Kullanımı – Örnek 2
- 1.4.3 Alıştırmalar

2. Temel Araçlar

- 2.1 Netcat
- 2.1.1 TCP/UDP Portuna Bağlanma
- 2.1.2 TCP/UDP Portunda Dinleme
- 2.1.3 Netcat ile Dosya Aktarımı
- 2.1.4 Netcat ile Uzaktan Yönetim
- 2.1.5 Alıştırmalar
- 2.2 Ncat
- 2.2.1 Alıştırmalar
- 2.3 Wireshark
- 2.3.1 Wireshark Temelleri
- 2.3.2 Ağ Dökümlerini Anlama
- 2.3.3 Yakalama ve Görüntüleme Filtreleri
- 2.3.4 TCP Akışlarını Takip Etme
- 2.3.5 Alıştırmalar
- 2.4 Tcpdump
- 2.4.1 Trafiği Filtreleme
- 2.4.2 Gelişmiş Başlık Filtreleme
- 2.4.3 Alıştırmalar

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

3. Pasif Bilgi Toplama

- 3.1 Açık Web Bilgi Toplama
- 3.1.1 Google
- 3.1.2 Google Hackleme
- 3.1.3 Alıştırmalar
- 3.2 E-posta Hasat
- 3.2.1 Alıştırma
- 3.3 Ek Kaynaklar
- 3.3.1 Netcraft
- 3.3.2 Whois Sayımı
- 3.3.3 Alıştırma
- 3.4 Yeniden Yapılandırma

4. Etkin Bilgi Toplama

- 4.1 DNS
- 4.1.1 Bir DNS Sunucusuyla Etkileşim
- 4.1.2 Aramaları Otomatikleştirme
- 4.1.3 İleri Arama Kaba Kuvvet
- 4.1.4 Ters Arama Kaba Kuvvet
- 4.1.5 DNS Bölge Transferleri
- 4.1.6 Kali Linux'taki İlgili Araçlar
- 4.1.7 Alıştırmalar
- 4.2 Port Tarama
- 4.2.1 TCP CONNECT / SYN Tarama
- 4.2.2 UDP Tarama
- 4.2.3 Yaygın Port Tarama Tuzakları
- 4.2.4 Nmap ile Port Tarama
- 4.2.5 İşletim Sistemi Parmak İzi
- 4.2.6 Banner Yakalama/Hizmet Sayımı
- 4.2.7 Nmap Komut Dosyası Motoru (NSE)
- 4.2.8 Alıştırmalar
- 4.3 SMB Sayımı
- 4.3.1 NetBIOS Hizmeti İçin Tarama
- 4.3.2 Boş Oturum Sayımı
- 4.3.3 Nmap SMB NSE Komut Dosyaları
- 4.3.4 Alıştırmalar
- 4.4 SMTP Sayımı
- 4.4.1 Alıştırma
- 4.5 SNMP Sayımı
- 4.5.1 MIB Ağacı
- 4.5.2 SNMP için Tarama
- 4.5.3 Windows SNMP Sayımı Örneği
- 4.5.4 Alıştırmalar

5. Güvenlik Açığı Taraması

- 5.1 Nmap ile Güvenlik Açığı Taraması
- 5.2 OpenVAS Güvenlik Açığı Tarayıcısı
- 5.2.1 OpenVAS İlk Kurulumu
- 5.2.2 Alıştırmalar

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

6. Arabellek Taşmaları

- 6.1 Bulanıklaştırma
- 6.1.1 Güvenlik Açığı Geçmişi
- 6.1.2 DEP ve ASLR
- 6.1.3 POP3 Protokolüyle Etkileşim
- 6.1.4 Alıştırmalar

7. Win32 Arabellek Taşması İstismarı

- 7.1 Çökmeyi Tekrarlama
- 7.2 EIP'yi Kontrol Etme
- 7.2.1 İkili Ağaç Analizi
- 7.2.2 Benzersiz Bir Dize Gönderme
- 7.2.3 Alıştırmalar
- 7.3 Kabuk Kodunuz İçin Alan Bulma
- 7.4 Kötü Karakterleri Kontrol Etme
- 7.4.1 Alıştırmalar
- 7.5 Yürütme Akışını Yeniden Yönlendirme
- 7.5.1 Bir Dönüş Adresi Bulma
- 7.5.2 Alıştırmalar
- 7.6 Metasploit ile Shellcode Oluşturma
- 7.7 Bir Shell Elde Etme
- 7.7.1 Alıştırmalar
- 7.8 Exploit'i İyileştirme
- 7.8.1 Alıştırmalar

8. Linux Arabellek Taşması İstismarı

- 8.1 Ortamı Kurma
- 8.2 Crossfire'ı Çökertmek
- 8.2.1 Alıştırma
- 8.3 EIP'yi Kontrol Etmek
- 8.4 Kabuk Kodumuz İçin Alan Bulmak
- 8.5 İstismar Güvenilirliğini Geliştirmek
- 8.6 Kötü Karakterleri Keşfetmek
- 8.6.1 Alıştırmalar
- 8.7 Bir Geri Dönüş Adresi Bulmak
- 8.8 Bir Kabuk Almak
- 8.8.1 Alıştırma

9. İstismarlarla Çalışmak

- 9.1 İstismarları Aramak
- 9.1.1 Kali Linux'ta İstismarları Bulmak
- 9.1.2 Web'de İstismarları Bulmak
- 9.2 İstismarları Özelleştirmek ve Düzeltmek
- 9.2.1 Bir Geliştirme Ortamı Kurmak
- 9.2.2 Çeşitli İstismar Kod Dilleriyle Başa Çıkmak
- 9.2.3 Alıştırmalar

10. Dosya Aktarımları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 10.1 Anti-Virüs Yazılımı
- 10.2 Dosya Aktarım Yöntemleri
- 10.2.1 Etkileşimli Olmayan Kabuk
- 10.2.2 Dosya Yükleme
- 10.2.3 Alıştırmalar

11. Ayrıcalık Yükseltme

- 11.1 Ayrıcalık Yükseltme Saldırıları
- 11.1.1 Linux'ta Yerel Ayrıcalık Yükseltme Saldırısı Örneği
- 11.1.2 Windows'ta Yerel Ayrıcalık Yükseltme Saldırısı Örneği
- 11.2 Yapılandırma Sorunları
- 11.2.1 Yanlış Dosya ve Hizmet İzinleri
- 11.2.2 Bir Ağ Yöneticisi Gibi Düşünün
- 11.2.3 Alıştırmalar

12. İstemci Tarafı Saldırıları

- 12.1 Hedefinizi Tanıyın
- 12.1.1 Pasif İstemci Bilgi Toplama
- 12.1.2 Aktif İstemci Bilgi Toplama
- 12.1.3 Sosyal Mühendislik ve İstemci Tarafı Saldırıları
- 12.1.4 Alıştırmalar
- 12.2 MS12-037 Internet Explorer 8
- 12.2.1 İstemci Tarafı Saldırısını Kurma
- 12.2.2 Kabuk Kodunu Değiştirme
- 12.2.3 Alıştırmalar
- 12.3 Java İmzalı Applet Saldırısı
- 12.3.1 Alıştırmalar

13. Web Uygulaması Saldırıları

- 13.1 Temel Iceweasel Eklentileri
- 13.2 Siteler Arası Komut Dosyası (XSS)
- 13.2.1 Tarayıcı Yönlendirmesi ve IFRAME Enjeksiyonu
- 13.2.2 Çerezleri ve Oturum Bilgilerini Çalma
- 13.2.3 Alıştırmalar
- 13.3 Dosya Dahil Etme Güvenlik Açıkları
- 13.3.1 Yerel Dosya Dahil Etme
- 13.3.2 Uzaktan Dosya Dahil Etme
- 13.4 MySQL SQL Enjeksiyonu
- 13.4.1 Kimlik Doğrulama Baypası
- 13.4.2 Veritabanını Numaralandırma
- 13.4.3 Sütun Numarası Numaralandırması
- 13.4.4 Çıktının Düzenini Anlama
- 13.4.5 Veritabanından Veri Çıkarma
- 13.4.6 Kod Yürütme İçin SQL Enjeksiyonundan Yararlanma
- 13.5 Web Uygulaması Vekilleri
- 13.5.1 Alıştırmalar
- 13.6 Otomatik SQL Enjeksiyon Araçları
- 13.6.1 Alıştırmalar

14. Parola Saldırıları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 14.1 Brute Force'a Hazırlık
- 14.1.1 Sözlük Dosyaları
- 14.1.2 Anahtar Alanı Brute Force'u
- 14.1.3 Pwdump ve Fgdump
- 14.1.4 Windows Kimlik Bilgisi Düzenleyicisi (WCE)
- 14.1.5 Alıştırmalar
- 14.1.6 Parola Profilleme
- 14.1.7 Parola Mutasyonu
- 14.2 Çevrimiçi Parola Saldırıları
- 14.2.1 Hydra, Medusa ve Ncrack
- 14.2.2 Doğru Protokolü Seçmek: Hız mı Ödül mü?
- 14.2.3 Alıştırmalar
- 14.3 Parola Karma Saldırıları
- 14.3.1 Parola Karmaları
- 14.3.2 Parola Kırma
- 14.3.3 John the Ripper
- 14.3.4 Rainbow Tabloları
- 14.3.5 Windows'ta Karmayı Geçirme
- 14.3.6 Alıştırmalar

15. Port Yönlendirme ve Tünelleme

- 15.1 Port Yönlendirme/Yeniden Yönlendirme
- 15.2 SSH Tünelleme
- 15.2.1 Yerel Port Yönlendirme
- 15.2.2 Uzak Port Yönlendirme
- 15.2.3 Dinamik Port Yönlendirme
- 15.3 Proxy Zincirleri
- 15.4 HTTP Tünelleme
- 15.5 Trafik Kapsülleme
- 15.5.1 Alıştırmalar

16. Metasploit Çerçevesi

- 16.1 Metasploit Kullanıcı Arayüzleri
- 16.2 Metasploit Çerçevesini Kali'de Kurma
- 16.3 Metasploit Çerçevesini Keşfetme
- 16.4 Yardımcı Modüller
- 16.4.1 MSF Sözdizimine Alışma
- 16.4.2 Metasploit Veritabanı Erişimi
- 16.4.3 Alıştırmalar
- 16.5 Exploit Modülleri
- 16.5.1 Alıştırmalar
- 16.6 Metasploit Yükleri
- 16.6.1 Aşamalı ve Aşamalı Olmayan Yükler
- 16.6.2 Meterpreter Yükleri
- 16.6.3 Meterpreter ile Deneyler
- 16.6.4 Yürütülebilir Yükler
- 16.6.5 Ters HTTPS Meterpreter
- 16.6.6 Metasploit Exploit Çoklu İşleyici
- 16.6.7 İstemci Tarafı Saldırılarını Yeniden Ziyaret Etme
- 16.6.8 Alıştırmalar
- 16.7 Kendi MSF Modülünüzü Oluşturma

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- 16.7.1 Alıştırma
- 16.8 Metasploit ile Sonradan İstismar
- 16.8.1 Meterpreter Sonradan İstismar Özellikleri
- 16.8.2 Sonradan İstismar Modülleri
- B10B7B11B12

17.Antivirüs Yazılımını Atlatma

- 17.1 Metasploit ile Yükleri Kodlama
- 17.2 Yazılım Koruyucuları ile Bilinen Kötü Amaçlı Yazılımları Şifreleme
- 17.3 Özel/Yaygın Olmayan Araçlar ve Yükler Kullanma
- 17.4 Alıştırma

18. Parçaları Birleştirme: Penetrasyon Testi Ayrıntısı

- 18.1 Aşama 0 – Senaryo Açıklaması
- 18.2 Aşama 1 – Bilgi Toplama
- 18.3 Aşama 2 – Güvenlik Açığı Belirleme ve Önceliklendirme
- 18.3.1 Parola Kırma
- 18.4 Aşama 3 – Araştırma ve Geliştirme
- 18.5 Aşama 4 – İstismar
- 18.5.1 Linux Yerel Ayrıcalık Yükseltme
- 18.6 Aşama 5 – İstismar Sonrası
- 18.6.1 Etkiyi Genişletme
- 18.6.2 Dahili Ağa Yönelik İstemci Tarafı Saldırısı
- 18.6.3 AD Aracılığıyla Ayrıcalık Yükseltme Yanlış Yapılandırmalar
- 18.6.4 Port Tünelleme
- 18.6.5 HTTP Kapsülleme ile SSH Tünelleme
- 18.6.6 Yüksek Değerli Hedefleri Arama
- 18.6.7 Alan Ayrıcalık Yükseltmesi
- 18.6.8 Öldürmeye Gitme