

Metasploit Framework ile Penetration Test Eğitimi

Penetration Testing

Kötü amaçlı saldırganın sistemlerinize verebileceği zararı görebilmeniz ve gerekli tedbirleri alabilmeniz için yapılan saldırı simülasyonudur.

Metasploit Framework

İçerisinde yüzlerce exploit, farklı payloadlar, encoder, nop ve auxiliary barındıran bir güvenlik aracıdır.

Exploit teknikleri ile istismarları hakkında bilgi sağlayan, oluşturduğu yapı ile güvenlik denetçilerine, IDS imza geliştirme ve istismar araştırmaları yapan uzmanlara, hackerlara faydalı bilgiler vermekte ve exploit geliştiricileri için bir çatı oluşturmaktadır.

Eğitimin Amacı ?

Güvenlik dünyasında ileri seviyede yer alan nmap ve metasploit framework araçlarının detay özelliklerini öğrenmek, etkin bir şekilde kullanarak sızma testleri gerçekleştirmek.

Kimler Katılmalı ?

Bilgi sistemleri denetim uzmanları

Bilgi sistemleri denetim adayları

Ağ güvenliğini kendileri test etmek isteyen kurumlar

Kariyer alanı olarak "pentester" seçmeyi planlayanalar

IT security denetim ekipleri

Neler Katacak ?

Eğitim sonrası katılımcılar ağ haritalama ve sızma testleri alanında en iyisi sayılabilecek bu araçları tüm detayları ile birlikte nerede nasıl kullanılacağını uygulamalı olarak öğrenmiş olacaktır.

Eğitim Süresi

4 Gün (12 saat)

Temel Gereksinimler

Temel TCP/IP bilgisi

Linux ve Windows işletim sistemleri bilgisi

Eğitmen

Ozan UÇAR

ozan@cehturkiye.com

Eđitim İeriđi

1. Penetration Test Türleri

- 1.1. Siyah Kutu Testi
- 1.2. Gri Kutu Testi
- 1.3. Beyaz Kutu Testi

2. Nmap ile Port Tarama Teknikleri

- 2.1. Pratik Port Tarama Teknikleri
- 2.2. alıřan Servislerin Tespiti
- 2.3. İřletim Sisteminin Tespiti
- 2.4. Firewall, IDS/IPS Keřfi
- 2.5. Nmap Script Engine Kullanımı
- 2.6. Nmap ıktıları ve Raporlama

3. Nmap Sonularını Metasploit İinde Kullanmak

4. Exploit Nedir ?

- 4.1. Bir Exploitin Yařam Döngüsü
- 4.2. Exploit Türleri

5. Payload Nedir ?

- 5.1. Üst düzey bazı payloadlar

6. Encoder Nedir ?

- 6.1. Metasploitde bulunan encoderlar

7. NOP Nedir ?

- 7.1. NOP lar

8. Auxiliary

- 8.1. Metasploitde bulunan Auxiliary ler

9. Metasploit Kurulumu

- 9.1. Windows Platformlara kurulumu
- 9.2. Linux Sistemlere kurulumu
- 9.3. Güncelleme

10. Geliřmiř Payload ve Eklenti Modülleri

- 10.1. Meterpreter
- 10.2. VNC Inject
- 10.3. PassiveX
- 10.4. DLL Inject
- 10.5. Auxiliary Modülleri

11. Metasploit Araçlarını Anlamak

- 11.1. msfconsole
- 11.2. msfweb
- 11.3. msfcli
- 11.4. msfopcode
- 11.5. msfpayload
- 11.6. msfencode
- 11.7. msfrpcd
- 11.8. msfgui

12. Metasploit Framework ile Pen-Test

- 12.1. Bilgi Toplama
- 12.2. Dradis Framework
- 12.3. Port Tarama
- 12.4. Auxiliary Eklentileri
- 12.5. Servis Keşfi
- 12.6. Password Sniffing

13. Güvenlik Zaafiyeti Tarama

- 13.1. Güvenlik Açığı Referansına Dayalı Exploit Seçimi
- 13.2. Açık Port(lar)a Dayalı Exploit Seçimi

14. Client Side Saldırı Yöntemleri

- 14.1. Binary Payloadlar
- 14.2. Antivirüsleri Atlamak
- 14.3. Linux Binary Trojan
- 14.4. Java Uygulamalarını Bulaştırmak
- 14.5. İstemci tabanlı Saldırıları

15. Exploit Sonrası Sistemde Nasıl İlerlersin ?

- 15.1. Bilgiyi Açığa Çıkarma
- 15.2. Sistem Loglarının Yönetimi
- 15.3. Trafik Dinleme (Packet Sniffing)
- 15.4. TimeStomp
- 15.5. Ekran Görüntüsü Yakalama
- 15.6. Ses, Webcam Görüntüsünü Yakalama
- 15.7. Hedef Sistemde İçerik Arama

16. Erişimi Sürdürme Yöntemleri

- 16.1. Klavye Girişlerini Yakalama
- 16.2. Kalıcı Meterpreter Servisi

16.3. Meterpreter Backdoor

17. İleri Metasploit Kullanımı

- 17.1. PHP Meterpreter
- 17.2. Payload Derlemek (.exe , .js , .DLL, .VBA)
- 17.3. Browser Autopwn

18. Metasploit Ötesinde Hacking Araçları

- 18.1. Ratproxy
- 18.2. Wmap
- 18.3. FastTrack
- 18.4. Sosyal Mühendislik Aracı (SET)
- 18.5. Gerçek Dünyadan Senaryolar