1. OSWP SERTİFİKASI NEDİR?

Offensive Security tarafından verilen (http://www.offensive-security.com) ve açılımı "Offensive Security Wireless Professional" olan OSWP sertifikası, kablosuz ağ güvenliği ile uğraşan, sızma testleri yapan veya ilgi duyanlar için hazırlanmış bir sertifika programıdır. Bu sertifikanın alınması için öncelikle "Offensive Security Wireless Attacks", eğitiminin alınması gerekmektedir. Eğitimin başlıkları hakkında ayrıntılı bilgi offsec web sitesinde bulunmaktadır. Eğitim sonunda 4 saatlik sınava girme hakkı tanınır. Sınav online olarak yapılır ve Offsec tarafından özel olarak hazırlanan ortam üzerindeki makinalara ssh ile bağlanılarak oluşturulan kablosuz ağ ortamı üzerinden sağlanır. Online olmasından dolayı diğer kablosuz ağ güvenliği ile ilgili sertifikalardan ayrı tutmak yerinde olacaktır. Sınav OSCP gibi zor bir sınav değil. Sınav odaklı değil öğrenme odaklı olursanız sertifika sınavında başarılı olmamanız için hiçbir neden yok. Yine her sertifikasında olduğu gibi burada da "try harder sloganı" geçerli.

2. EĞİTİM HAKKINDA

Öncelikle eğitime başladığınızda size eğitim dokümanlarını indirme imkanı tanınır (doküman + video). Bu materyaller sadece size aittir ve sizin isminiz ve adresinizle arka plan doldurulmuştur. Bu sebepten paylaşmamanız sizin yararınıza olacaktır.

Sağlanan dokümanlar ve videolar son derece yararlıdır. Eğitimde OSCP'den farklı olarak bir laboratuvar ortamı yoktur. Laboratuvar ortamının hazırlanması size aittir. Laboratuvarınızın nasıl oluşturulacağını aşağıda tek tek anlatıyor olacağım .

3. ADIM ADIM LAB ORTAMI HAZIRLAMA ve EĞİTİM

- ✓ Öncelikle eğitim için sizin almanız gereken ve daha sonra da pentestlerde kullanabileceğiniz ekipmanlar var.
  - Önerilen Access Pointler
    - D-Link DIR-601
    - Netgear WNR1000v2
  - Önerilen Kablosuz ağ adaptörleri
    - Netgear WN111v2 USB
    - ALFA Networks AWUS036H USB 500mW (Ben aynı model 1000mW lığını aldım)
- ✓ Buradaki hardwareler sadece öneri, favori bir kartınız varsa onla da yapabilirsiniz ama alfa card aldım ben ve çok memnunum. Aynı model olması çok önemli linux rt8187 driverı ile görüyor. Farklı daha ileri bir model alırsanız aircrack ile problem yaşayabilirsiniz. Bu card 1 watt çıkışlı ve gerçekten süper.
- ✓ Access point almadım çünkü elimde 2 adet wireless özelliği olan eski ADSL modem vardı fakat bu modemlerle bazı atakları yapamadım örneğin WEP PSK çünkü desteklemiyorlardı. Bununla birlikte diğerlerini test edebildim.
- ✓ Lab ortamını oluşturduktan sonra indirmiş olduğunuz dokümanları ve videoları dikkatli bir şekilde inceleyin
- ✓ Eğitim dokümanları üzerindeki tüm egzersizleri yapın.
- ✓ Eğitim konuları özet olarak şöyle sıralanabilir:
  - Wireless ağlar hakkında genel bilgi.
  - Wireless paket incelemeleri detaylı bir şekilde yer almaktadır.
  - Wireless ağ adaptörlerinin linux sistemlerine tanıtılması
  - Linux komutları (iw, iwconfig, aircrack-ng, airodump-ng,vb)
  - Aircrack-ng suite kullanımı
  - WEP cracking
    - DeAuthentication Attack
    - Fake Authentication Attack
    - ARP attack
    - Interactive packet replay (Natural & Modified)
    - Fragmantation attack
    - ChopChop Attack
    - WEP PSK attack
  - WPA cracking
    - Aircrack-ng ve Airolib-ng
    - coWPAtty
    - pyrit
  - Wireless Reconnasainance
  - Rogue Access Point yapılandırması ve kullanımı

- ✓ Eksik Olan konular ise
  - WEP cracking Hirte attack
  - WPS cracking
  - WPA Enterprise cracking
- ✓ Eksik konular için SecurityTube Wireless Megaprimer serisini şiddetle tavsiye ederim. Vivek Ramachandran tarafından hazırlanmış video serisi çok güzel. İsterseniz Torrentlerden tüm içeriği indirip offline izeleyebiliyorsunuz.
- ✓ Eğitimde WEP ağırlık verilmiş olsada size wireless networking temellerini veriyor. Zaten WPA de dictionary attack yapmaktan başka bir çareniz olmamasından dolayı da WPA tarafında pek bişey yok. Sadece işlemi hızlandırmak için yöntemler mevcut.
- ✓ Bol bol pratik yapın. Ben tüm atakları içeren bir script yazdım çok da işime yarıyor.

4. ADIM ADIM FINAL SINAVI (CHALLANGE)

Gelelim sınava…

- ✓ Sınav 4 saat.
- ✓ Gelen email ile başlıyor.
- ✓ Email de tüm kurallar yazıyor. Kurallara uymanız önemli, uymazsanız sınavınız iptal edilebiliyor.
- ✓ Eğer iyi hazırlandıysanız ve egzersizleri hakkıyla yaptıysanız geçersiniz.
- ✓ Ben sınavı raporlama dahil 50 dakikada bitirdim.
- ✓ Sınav hakkında fazla bilgi veremiyorum. Dediğim gibi sınav önemli değil siz öğrenmeye odaklanın.
- ✓ Sınav esnasında sadece 3 adet access point veriliyor. Bunların herbiri farklı senaryolarda.
- ✓ Tavsiyem birine odaklanın ve yazdığınız ilgili olan her komutu ve çıktısını bir dokümana kaydedin. Sonra bu sizin raporunuz olacak.
- ✓ OSCP deki gibi ayrıntılı bir rapor beklenmiyor. Sadece ilgili access pointi ele geçirirken hangi komutları yazdınız ve ekran çıktılarını vermeniz yeterli.
- ✓ Ben sınavı bitirdiğimde raporum da hazırdı. Ufak tefek format değişiklikleri sonucunda da raporu hemen gönderdim.

5. Diğer SERTiFiKALARLA KIYASLAMA

Offensive security sertifikaları diğer sertifikalarla kıyaslandığında ortaya çıkan sonuç şudur:

- ✓ Ticari amaç güdmemektedir. Diğerleri devam ettirmek için ayrıca para istemektedirler.
- ✓ Eğitimi alanın gerçekten öğrendiğini tesciller. Diğerleri çoktan seçmelidir. Braindumplardan soruları bulabilmeniz işten bile değil.

Özet olarak OSWP wireless konusunda alınması gereken bir eğitim.

6. SONUÇ

TRY HARDER ☺