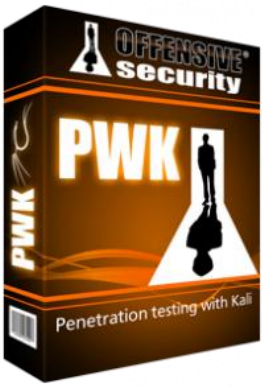
1. OSCP SERTİFİKASI NEDİR?

Offensive Security tarafından verilen (http://www.offensive-security.com) ve açılımı "Offensive Security Certified Professional" olan OSCP sertifikası, sızma testleri yapan veya ilgi duyanlar için hazırlanmış bir sertifika programıdır. Bu sertifikanın alınması için

öncelikle "Pentesting With Kali", PWK (eski adıyla Pentesting With Backtrack, PWB) eğitiminin alınması gerekmektedir. (Bu arada Backtrack öldü yaşasın Kali☺). PWK 01.01.2014 de verilmeye başladığından ben PWB aldım. Eğitimin başlıkları hakkında ayrıntılı bilgi offsec web sitesinde bulunmaktadır. Eğitim sonunda 90 gün içerisinde sınava girme hakkı tanınır. Sınav bildiğiniz sınavlardan çok farklıdır ve 24 saat süresi vardır. Sınav online olarak yapılır ve Offsec tarafından özel olarak hazırlanan ortam üzerindeki makinalara yetkili erişim yapma esasına dayanır. O zamana kadar hiç görmediğiniz ve kullanmadığınız metodları kullanmanız gerekecek. Bu sebepten dolayı OSCP sertifikasını diğer sertifikalardan ayrı tutmak yerinde olacaktır. Gerçekten zor bir o kadar da eğlenceli bir eğitim. Zaten Offsec'in mottosu "TRY HARDER" ☺

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 sizin belirleyeceğiniz süreler zarfında (30,60,90 gün) online olarak vpn ile lab ortamına erişim sağlayarak öğrendiklerinizi uygulama imkanınız bulunmaktadır. Çalışmamdan dolayı ben 90 gün aldım. Lab

ortamında 4 tane ağ bulunuyor. Bu ağların sizin de dahil olduğunuzda yaklaşık 30-40 tane sunucu/pc bulunuyor. Bunların bazıları gateway olarak konumlandırılmış ve diğer ağlara sızma olanağı sunuyor. Diğerlerinde de az sayıda sunucu var. Tüm hepsini ele geçirmeniz bekleniyor fakat bazıları gerçekten zor makinalar ve bazıları da dikkat gerektiriyor.

Diğer eğitimlerden farklıdır!! Kesinlikle size git şu makinada şu zafiyet var git şu exploit ile patlat diyen diğer eğitimlerdeki adım adım yol gösteren lab egzersizleri yok. Tamamıyla kendi başınasınız. IRC kanalından bir ortam bulunmakta, buradan da adminlerle konuşabiliyorsunuz. Fakat adminlerden bir ipucu alabilmek neredeyse imkansız. Büyük olasılıkla alacağınız cevap "Try harder", "more enumeration" olacaktır. Bununla birlikte eğer bir makine üzerinde çok uğraştınız birçok şey elde ettiniz, işte o zaman adminler dolaylı yoldan ipucu verebiliyor ama bu seferde ipucunun olayla ilgisini anlamak için kafa patlatıyorsunuz. Yanlış girdiğiniz her yol size yeni bir şey öğretiyor. Bu sebepten yanlış yollara girmeye korkmayın. Aşağıda hem eğitim sırasında hem de final sınavında ne yapmanız ne yapmamanız kendi yaşadıklarım doğrultusunda anlatmaya çalıştım…

3. ADIM ADIM LAB PENTEST

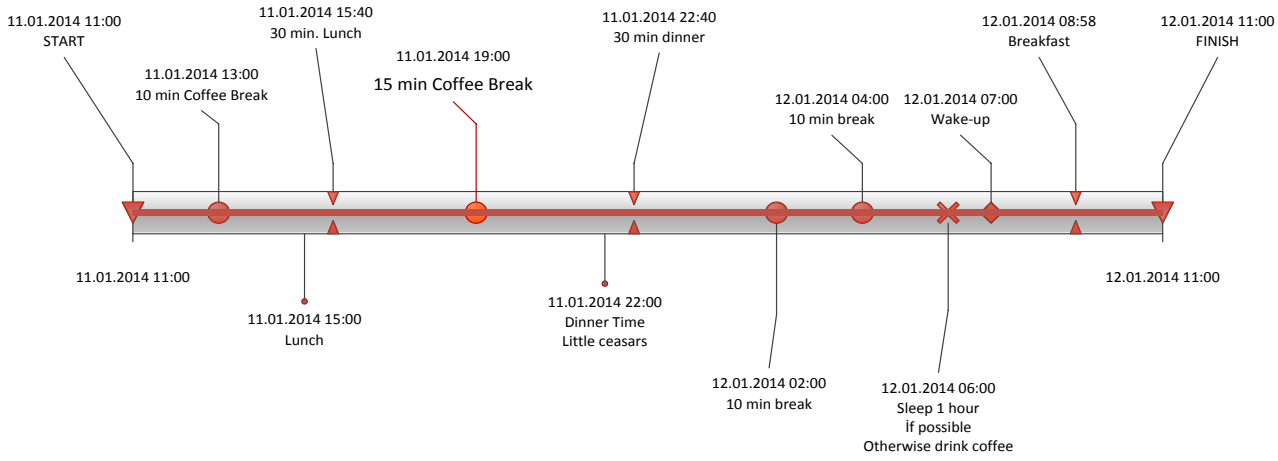
- ✓ Öncelikle iş ve ev durumunuzu göz önünde tutarak lab zamanına karar verin. Ben evli, çocuklu ve çalışan biri olduğumdan 90 gün aldım. Son zamanlarda bayram tatili geldi, fakat o zamana kadar bitiremeyeceğimi ön göremediğimden dolayı bayram tatilim zehir oldu diyebilirim ☺
- ✓ Lab ortamı için indirmiş olduğunuz dokümanları ve videoları dikkatli bir şekilde inceleyin.
- ✓ Eğitim materyalleri içerindeki tüm egzersizleri ve ekstra egzersizleri yapın. Egzersizler lab ortamı hakkında size bilgi verecektir. Bazı egzersizleri lab zamanınız bittikten sonra yapmayı düşünebilirsiniz çünkü inanın lab zamanınız çok çabuk tükeniyor hele bir de çalışıyorsanız, evli ve çocukluysanız ☺
- ✓ Sadece materyale bağlı kalmayın. Konu ile ilgili birçok kaynaktan yararlanmalısınız.
- ✓ Egzersizleri yaparken yaptığınız enumeration işlemlerini otomatikleştirmek için mutlaka script yazın. Bu scriptler size zaman kazandıracaktır. Script dili fark etmez ama en kolayı bash'dir. Eğer daha advanced scriptler yazmak istiyorsanız python tavsiye ederim.
- ✓ Bir sistemi ele geçirmenin sadece bir yolu yok. En basiti ile ele geçirmek önemli değil. Önemli olan makinayı diğer yöntemlerle de ele geçirmek. Bu sebepten çalışan her servise dikkatli bir şekilde bakılmalı. Karşınıza daha önce hiç karşılaşmadığınız ama yapınca mutlu olduğunuz yöntemler çıkıyor.
- ✓ Zamanınızı iyi kullanın, çok çabuk tükeniyor. Ben bazı günler sabah 9'dan gece 12:00-01:00'e kadar uğraştığımı bilirim. Bazı günler sabahladığımı.
- ✓ Ele geçirdiğiniz her makinayı dokümante edin. Ben keepnote kullandım, güzel bir not tutma aracı. Ayrıca freemind kullandım, hiyerarşik bilgileri organize etmek için böylelikle bir pentest bilgi ağacı oluşturdum ve çok faydalı oldu.
- ✓ Bir çok script yazdım işimi kolaylaştırmak için. Şiddetle tavsiye ederim.
- ✓ Bir makinaya konsantre olun ve ilerleyin. Makinadan makinaya atlarsanız zaman kaybedersiniz.

- ✓ Ayrıca IRC kanaldan !<hostname> yazarsanız o host ile ilgili ipucu vermektedir. Ben bunu çok geç fark ettim. Tabi öncelikle uğraştığınız makinanın hostname'ini bilmeniz gerekiyor.
- ✓ Offsec forum'u kullanın, bazı durumlar için ipucu bulabilirsiniz. Tabi açık bir şekilde değil…
- ✓ Bir makine için her işlemi kaydedin. Makinayı o an ele geçiremeyebilirsiniz. Daha sonra geri döndüğünüzde yaptığınız işlemleri tekrar yapmamanız için bu gerekli.
- ✓ Ben 3 hostu ele geçiremedim zaman problemimden dolayı.
- ✓ Lab zamanı bittikten sonra biraz dinlenmek şart, hemen sınavı ayarlamayın.
- ✓ Lab rapor şablonunuzu oluşturun ve yavaş yavaş yazmaya başlayın. 90 gününüz var iyi değerlendirin inanın bu zaman da çabuk geçiyor.
- ✓ Lab ortamı için söyleyeceklerim bu kadar.

4. ADIM ADIM FINAL SINAVI (CHALLANGE)

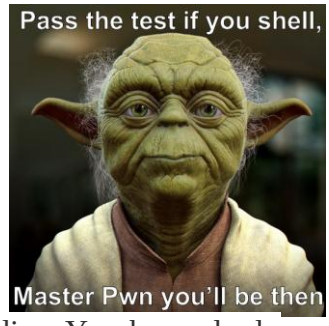
Gelelim sınava…

- ✓ Sınav 24 saat.
- ✓ Çok iyi planlamak şart, yoksa başarısız olmanız işten bile değil.
- ✓ Uyguladığım plan aşağıda. Bu plana sadık kaldım. Sadece 1 saat değil 2 saat uyudum mükafat olarak çünkü yeterli puanı almıştım fakat tüm herşeyi ele geçirememiştim☺



- ✓ 2 saatte bir ara vermeniz size başka bir açıdan düşünmeyi sağlıyor. Kahve araları hayat kurtarıyor ve kahve gerçekten zihninizi açıyor.
- ✓ Ayrıca 2 saatte bir host ile uğraşın, eğer ele geçiremediyseniz yaptığınız herşeyi dokümante edip diğer hoşta geçin.
- ✓ İlk 2 saat hiçbir makinayı ele geçiremedim. Hatta en basit hostu bile. Moralim bozuldu haliyle. Ama sonra 25 puanlık hostu 10 dk içinde ele geçirdim ve bu moralle diğer hostta unprivilege erişim sağladım. Daha sonra 7-8 saat içinde toplam 50 puanım vardı. Gece 2 de ise artık 70 puanlık limiti geçmiştim, geriye artık tatmin

kalmıştı ve Pazar 09:00 da tüm hostları ele geçirdim ve 100 puanı toplamıştım. Daha bitmedi tabi. Bu sefer de 24 saat içinde raporu yazıp göndermeniz gerekiyor.



- ✓ Sınavda 5 host var ve inanın labda gördüğünüz senaryolarla alakası yok. Bu sebepten dolayı farklı düşünme becerisine sahip olmanız gerekiyor. Burada bu zafiyet yoktur demek sizi yanlış yönlendirecektir.
- ✓ Metasploit kullanımı kısıtlı sadece belirli sayıda hostta exploit kullanabiliyorsunuz (sınavdan sınava da değişiyor olabilir!!). Msfpayload, auxuliary, msfencode kullanmak serbest. Bazı hostlarda kesinlikle kullanımı yasak olarak belirtilmektedir. Yasak yerlerde kullanmanız 0 puan anlamına geliyor.
- ✓ Sınav, size sınav hakkında bir emailin gönderilmesiyle başlıyor. Emailde kurallar ve her bir makina için açıklamalar var. Bunları dikkatlice okuduktan sonra sınava başlayın
- ✓ Ben en düşük puanlıdan başladım ve hüsrana uğradım. En düşük puan demek en kolayı anlamına gelmiyor ☺
- ✓ Hazırladığınız programa uygun davranın.
- ✓ Saatler ilerledikçe ve herhangi bir makine ele geçiremediyseniz stress artıyor. Stressi dağıtmanın en iyi yolu kahve içmek… İçerken de yaptığınız işlemleri düşünebilirsiniz.
- ✓ Buffor Overflow da uzmanlaşın ☺ Direkt overwrite, SEH based, vb.
- ✓ Sınav bittikten sonra dinlenin ve raporunuzu yazın.
- ✓ Eğer sınavda yeterinde puan toplayamayıp sınırda olduğunuza inanıyorsanız yine de raporunuzu yazın ve lab raporuyla birlikte kullanın. Örneğin 60-65 puandaysanız yine de raporunuzu gönderin. Bir ümit kazanabilirsiniz.

5. DiğER SERTiFiKALARLA KIYASLAMA

Kıyaslama götürmez bence. GIAC GPEN, EC/COUNCIL CEH, LPT vb [1] sertifikalarla kıyaslandığında çok yukarılarda olan bir sertifika. Diğerlerinin sınavının çoktan seçmeli olması (bilgi ölçmede yetersiz), lablarının tamamıyla senaryo bazlı olması ve size bir rehber sunması(yaratıcılığı öldürüyor), devam ettirmek için yıllık ücret talep etmeleri (ticari) ve sınav ücretlerinin pahalı olması (ticari) gerçekten OSCP'nin değerini göstermektedir. OSCP sertifikalı bir kişinin ne aşamalardan geçerek sertifikayı aldığını bildiğiniz zaman, sertifikaya sahip olanın en azından penetrasyon tekniklerine hakim olduğunu biliyor oluyorsunuz.

6. SONUÇ

TRY HARDER ☺ [2] [3]

EK KAYNAKLAR

[1] http://pwndizzle.blogspot.com.tr/2012/09/ceh-vs-oscp-vs-gpen.html

[2] http://www.en-lightn.com/?p=941

[3] http://chris-huey.com/index.php/my-oscp-tips