Intro to Offensive Security

Task 1 What is Offensive Security? (Saldırgan Güvenlik Nedir?)

Kısacası, saldırgan güvenlik, bilgisayar sistemlerine girme, yazılım hatalarından yararlanma ve uygulamalarda boşluklar bularak bunlara yetkisiz erişim sağlama sürecidir.

Bir hacker'ı yenmek için, bu odada yapacağınız gibi, bir hacker gibi davranmanız, güvenlik açıklarını bulmanız ve bir siber suçludan önce yamalar önermeniz gerekir!

Diğer taraftan, potansiyel dijital tehditleri analiz ederek ve güvence altına alarak bir kuruluşun ağını ve bilgisayar sistemlerini koruma süreci olan savunma güvenliği de vardır; dijital adli tıp odasında daha fazla bilgi edinin.

Savunmacı bir siber rolde, nasıl saldırıya uğradığını anlamak için virüs bulaşmış bilgisayarları veya cihazları araştırabilir, siber suçluları takip edebilir veya kötü niyetli faaliyetler için altyapıyı izleyebilirsiniz.

soru ⇒

Aşağıdaki seçeneklerden hangisi bir sistemdeki güvenlik açıklarını bulmak için bir bilgisayar korsanının eylemlerini simüle ettiğiniz süreci daha iyi temsil eder?

Offensive Security (Saldırgan Güvenlik)

Defensive Security (Savunma Amaçlı Güvenlik)

cevap ⇒ **Offensive Security**

task 2 Hacking your first machine (İlk makinenizi hacklemek)

Siber güvenlik kariyerlerine ve saldırgan güvenliğin ne olduğuna geçmeden önce, sizi bilgisayar korsanlığına alıştıralım (ve evet, yasal, tüm egzersizler sahte simülasyonlardır)

İlk hack'iniz

Bu görevi bir masaüstünde ilk açtığınızda, ekranınız otomatik olarak görevin sanal makinesini başlatacak ve bölünmüş bir ekranda görüntüleyecektir. Bunu FakeBank adlı sahte bir banka uygulamasını hacklemek için kullanacaksınız. Bir mobil cihazdan dağıtmak için Makineyi Başlat düğmesine de tıklayabilirsiniz. Ekranınız bölünmezse, bu sayfanın sol üst köşesindeki mavi Bölünmüş Görünümü Göster düğmesini kullanın.

Gizli dizinleri ve sayfaları bulmak için FakeBank'ın web sitesini kaba kuvvetle zorlamak için "GoBuster" adlı bir komut satırı uygulaması kullanacağız. GoBuster, potansiyel sayfa veya dizin adlarının bir listesini alır ve her biriyle bir web sitesine erişmeyi dener; sayfa varsa, size söyler.

Adım 1) Bir terminal açın

Komut satırı olarak da bilinen terminal, grafiksel bir kullanıcı arayüzü kullanmadan bilgisayarla etkileşime girmemizi sağlar. Makinede, Terminal simgesini kullanarak terminali açın:

Adım 2) Gizli web sitesi sayfalarını bulun

Çoğu şirket, personeline günlük işlemler için temel yönetici kontrollerine erişim sağlayan bir yönetici portalı sayfasına sahip olacaktır. Bir banka için, bir çalışanın müşteri hesaplarına ve hesaplarından para aktarması gerekebilir. Genellikle bu sayfalar özel hale getirilmez ve saldırganların yönetici kontrollerini veya hassas verileri gösteren veya bunlara erişim sağlayan gizli sayfaları bulmasına olanak tanır.

GoBuster'ı (bir komut satırı güvenlik uygulaması) kullanarak FakeBank'ın web sitesindeki potansiyel olarak gizli sayfaları bulmak için aşağıdaki komutu terminale yazın.

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```

Yukarıdaki komutta, -u taradığımız web sitesini belirtmek için kullanılır, -w gizli sayfaları bulmak için yinelenecek bir kelime listesi alır.

GoBuster'ın listedeki her kelimeyle web sitesini taradığını ve sitede var olan sayfaları bulduğunu göreceksiniz. GoBuster bulduğu sayfaları sayfa/dizin adları listesinde size bildirecektir (Durum: 200 ile gösterilir).

Adım 3) Bankayı hackleyin

Bankadaki hesaplar arasında para transferi yapmanızı sağlayan gizli bir banka transferi sayfası bulmuş olmalısınız (/bank-transfer). Gizli sayfayı makinedeki FakeBank web sitesine yazın.

Bu sayfa bir saldırganın herhangi bir banka hesabından para çalmasına olanak tanır ki bu da banka için kritik bir risktir. Etik bir hacker olarak, (izin alarak) uygulamalarındaki güvenlik açıklarını bulur ve bir hacker bunları istismar etmeden önce düzeltmeleri için bankaya bildirirsiniz.

2276 numaralı banka hesabından hesabınıza (hesap numarası 8881) 2000$ transfer edin.

Transferiniz başarılı olduysa, şimdi yeni bakiyenizin hesap sayfanıza yansıdığını görebilmeniz gerekir. Şimdi oraya gidin ve parayı aldığınızı onaylayın! (Değişikliklerin görünmesi için Yenile düğmesine basmanız gerekebilir)

soru ⇒

Hesap bakiyenizin üzerinde, şimdi bu sorunun cevabını belirten bir mesaj görmelisiniz. İhtiyacınız olan cevabı bulabiliyor musunuz(ipucu= Yeni bakiyenizin pozitif bir sayı olduğundan emin olun. Bakiyeniz hala negatif bir değer gösteriyorsa (sayfayı yeniledikten sonra bile), daha fazla para aktarmanız gerekebilir.)?

cevap ⇒ **BANK-HACKED**

Eğer bir sızma testi uzmanı veya güvenlik danışmanı olsaydınız, bu, şirketlerin web uygulamalarındaki güvenlik açıklarını test etmeleri için gerçekleştireceğiniz bir alıştırmadır; güvenlik açıklarını araştırmak için gizli sayfalar bulun.

cevap gerekmemektedir.

Sayfanın üst kısmındaki kırmızı "Terminate" (Sonlandır) düğmesine tıklayarak makineyi sonlandırın.

cevap gerekmemektedir.

Task 3 Careers in cyber security (Siber güvenlik alanında kariyer)

Öğrenmeye nasıl başlayabilirim?

İnsanlar genellikle başkalarının nasıl bilgisayar korsanı (güvenlik danışmanı) veya savunmacı (siber suçlarla mücadele eden güvenlik analisti) olduğunu merak eder ve cevap basittir. İşi parçalara ayırın, ilgilendiğiniz bir siber güvenlik alanını öğrenin ve uygulamalı alıştırmaları kullanarak düzenli olarak pratik yapın. TryHackMe'de her gün biraz öğrenme alışkanlığı edinirseniz, sektördeki ilk işinize girecek bilgiyi edinmiş olursunuz.

Bize güvenin; bunu yapabilirsiniz! İlk güvenlik işlerini almak için TryHackMe'yi kullanan bazı insanlara bir göz atın:

Paul inşaat işçisiyken güvenlik mühendisi oldu. Daha fazlasını okuyun.

Kassandra müzik öğretmenliğinden güvenlik uzmanlığına geçti. Daha fazlasını okuyun.

Brandon siber alandaki ilk işini almak için okuldayken TryHackMe'yi kullandı. Daha fazlasını okuyun.

Hangi kariyerler var?

Siber kariyer odası, siber alandaki farklı kariyerler hakkında daha derinlemesine bilgi vermektedir. Ancak, burada birkaç saldırgan güvenlik rolünün kısa bir açıklaması bulunmaktadır:

Sızma Test Uzmanı - İstismar edilebilir güvenlik açıklarını bulmak için teknoloji ürünlerini test etmekten sorumludur.

Red Teamer - Düşman rolünü oynar, bir kuruluşa saldırır ve düşmanın bakış açısından geri bildirim sağlar.

Güvenlik Mühendisi - Siber saldırıları önlemeye yardımcı olmak için güvenlik kontrollerini, ağları ve sistemleri tasarlar, izler ve bakımını yapar.

Yukarıdakileri okuyun ve bir sonraki odayla devam edin!

cevap gerekmemektedir.