Etik Hackleme ve Sızma Testi Nedir?

Çalışma Kağıdı

Etik hackleme, sistem sahibinin izniyle güvenlik açıklarını bulmak için yapılan faaliyetlerdir. Sızma testi ise bu faaliyetlerin daha yapılandırılmış ve hedefe yönelik bir halidir.

Sorular

1. Etik hackleme faaliyetleri için en önemli ön koşul nedir?

A) En yeni hackleme araçlarına sahip olmak
B) Sistem sahibinden yazılı izin almak
C) Saldırıları gizli tutmak
D) Sadece açık kaynak kodlu sistemleri hedeflemek

2. Aşağıdakilerden hangisi sızma testinin temel amaçlarından biri DEĞİLDİR?

A) Sistemdeki kritik zafiyetleri belirlemek
B) Saldırı sonrası kurtarma planlarını test etmek
C) Kötü niyetli saldırganlardan önce güvenlik açıklarını kapatmak
D) Sistemin mevcut güvenlik duruşunu değerlendirmek

3. Bir sızma testinde 'pasif istihbarat toplama' ne anlama gelir?

A) Hedef sisteme doğrudan erişim sağlamak
B) Hedefle doğrudan etkileşime girmeden bilgi toplamak
C) Sistemin kaynaklarını tüketmek
D) Saldırı vektörlerini aktif olarak denemek

4. Bir şirketin web sitesindeki SQL Injection zafiyetini tespit etmek için sızma testi nasıl yapılır?

5. Bir kurumun iç ağındaki zayıf parolaları bulmak için etik hackleme faaliyeti nasıl yürütülür?

6. Bir mobil uygulamanın güvenliğini test etmek için hangi adımlar izlenir?

7. Tanımla: Etik Hackleme Nedir?

8. Tanımla: Sızma Testi (Penetration Test) Nedir?

9. Tanımla: Kırmızı Takım (Red Team) Nedir?

Cevap Anahtarı

1. B) Sistem sahibinden yazılı izin almak — Etik hackleme, yasalara uygun ve sistem sahibinin bilgisi ve izni dahilinde yapılmalıdır. Bu, en önemli yasal ve etik gerekliliktir.

2. B) Saldırı sonrası kurtarma planlarını test etmek — Saldırı sonrası kurtarma planlarının test edilmesi genellikle felaket kurtarma (disaster recovery) veya iş sürekliliği (business continuity) testlerinin bir parçasıdır, sızma testinin doğrudan ana amacı değildir.

3. B) Hedefle doğrudan etkileşime girmeden bilgi toplamak — Pasif istihbarat toplama, hedef sistemin farkında olmadan veya onunla doğrudan etkileşim kurmadan (örn. OSINT - Açık Kaynak İstihbaratı) bilgi toplama yöntemleridir.

4. 1. Hedef web sitesi belirlenir. 2. Web uygulaması tarama araçları (örn. OWASP ZAP, Burp Suite) kullanılarak olası giriş noktaları (parametreler, form alanları) tespit edilir. 3. SQL Injection payload'ları denenerek veritabanına yetkisiz erişim sağlanıp sağlanamayacağı kontrol edilir. 4. Tespit edilen zafiyet raporlanır ve iyileştirme önerileri sunulur.

5. 1. Kurumdan gerekli izinler alınır. 2. Ağ tarama araçları (örn. Nmap) ile aktif cihazlar ve servisler belirlenir. 3. Kırılabilir parolalara sahip olabilecek servisler (örn. SMB, FTP) tespit edilir. 4. Yaygın parola listeleri veya kaba kuvvet (brute-force) yöntemleri kullanılarak zayıf parolalar denenir. 5. Tespit edilen zayıf parolalar ve etkileri raporlanır.

6. 1. Uygulamanın statik analizi yapılır (kod incelemesi). 2. Dinamik analiz ile uygulama çalışırken ağ trafiği izlenir ve hassas verilerin iletimi kontrol edilir. 3. Yetkilendirme ve kimlik doğrulama mekanizmaları test edilir. 4. Veri depolama güvenliği (örn. yerel depolama, keychain) incelenir. 5. Bulunan güvenlik açıkları raporlanır.

7. Sistem sahibinin izniyle gerçekleştirilen, güvenlik açıklarını bulmaya yönelik yasal faaliyet.

8. Belirli bir hedef sistemin güvenlik açıklarını, gerçek bir saldırgan gibi kullanarak tespit etme süreci.

9. Saldırı simülasyonu yapan ve sistemin savunmasını test eden ekip.