Penetrasyon Testlerinde Düşülebilecek Hatalar

Sertan Kolat

Ajanda

- Kişisel Hazırlık/Yeterlilik
- Test Yapılan Ortamlardaki Problemler
- Denetimin Planlanması
- Metodoloji
-  Bilgi Toplama/Keşif
- Zaafiyet Tespiti ve Penetrasyon
- Şifre Tahmini – Kelime Listeleri
- Raporlama

id

- Sertan Kolat
- Kıdemli Güvenlik Danışmanı
- Avanteg – Yönetilen Servisler & Denetim Birimi Yöneticisi
- Penetration Tester
- CISSP, CISA, OSCP
- Blogger
  - SertanKolat.com
  - AutomatedScanning.blogspot.com

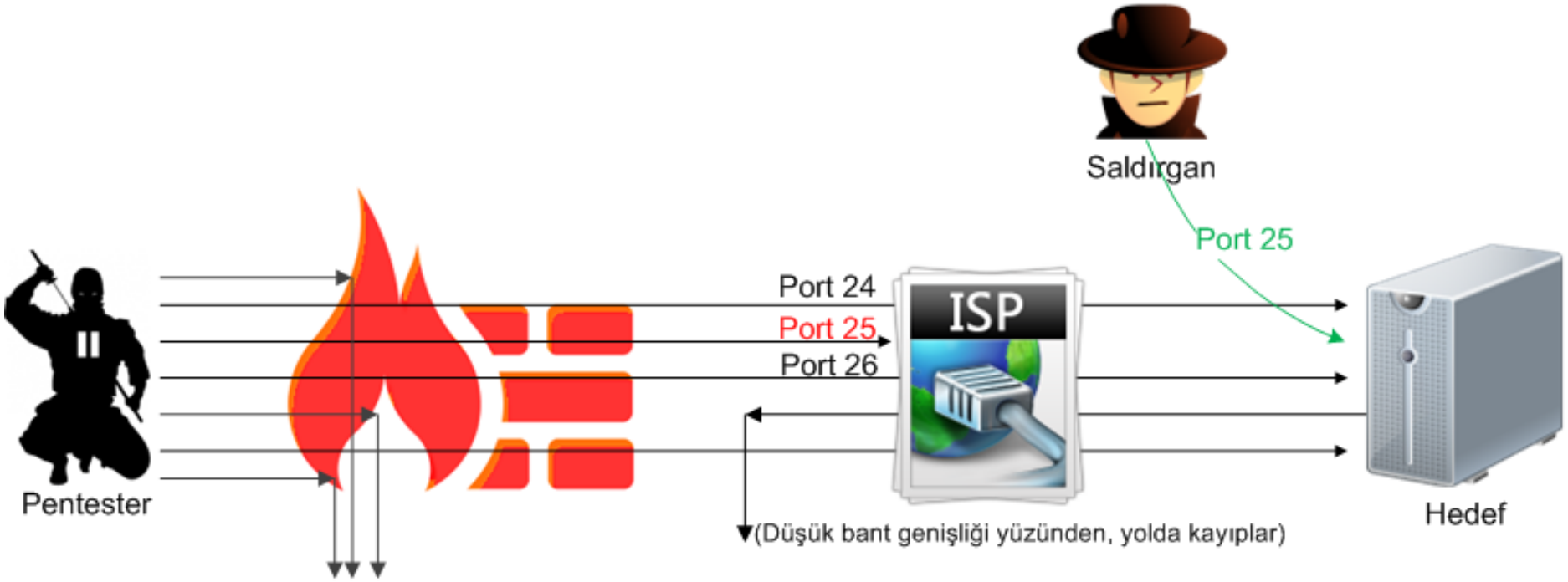
Kişisel Hazırlık/Yeterlilik

- Temel bilgi eksikliği
  - Temel TCP/IP bilgisi
  - Temel protokol/servis bilgisi
  - Kullanılan ticari uygulamalar hakkında bilgi
- Yetersiz pratik (ev ödevini yapmama)
- Kullanılan araçlar
  - Kullanılan araçlara yeterince hakim olmama
  - Araçların test ortamında önceden denenmemesi
  - Kullanılan araçları derinlemesine bilin. Neleri yapabilir? Neleri yapamaz? Yapamadıklarını nasıl telafi ederim?
  - Penetrasyon testi, yazılıma hedefi ver sonucu al değil!
- Önceki denetimlerde kazanılan deneyimlerin paylaşılmaması, kaydedilmemesi (knowledgebase vb)

Test Ortamındaki Problemler (1)

- Denetim yapan sistemin, Firewall veya NAT yapan cihaz arkasında bulunması
- Düşük bant genişliği
- ISP tarafından getirilen kısıtlamalar
  - Örneğin 25, 139, 445, 1434 ISP tarafından filtreleniyor, ama hedef sistemde açık!
- Denetim yapan sistemin bağlı bulunduğu switch cihazının kalitesiz olması
  - Yoğun paketleri kaldıramayabilir
- Denetim yapan sistem sanal sunucuysa, ağ ayarı "Bridged Network" olmalıdır
  - Host only veya NAT olduğu durumlarda bulgularda farklar, eksiklikler

Test Ortamındaki Problemler (1)



- Çok fazla paket, NAT tablosu doldu,
- Tam izin verildiği halde engellenen port'lar,
- Spoofed paketler,
- Fragmente paketler,
- Özel oluşturulmuş paketler

Test Ortamındaki Problemler (2)

- Denetim sunucularının güvenliği
  - Antivirus yok/devre dışı
  - Firewall yok/devre dışı
  - Ek paket filtreleme özellikleri devre dışı (özel denetim paketlerini engellemek istemeyiz)
  - Bazı güvenlik güncellemeleri –belki özellikle– eksik
  - Dışarıya açık servis varsa, default route tanımı kaldırılıp, sadece denetlenen hedef ağ için route eklenebilir
- Denetim sonrası atıl dosyalar silinmelidir (wipe)

Denetimin Planlanması (1)

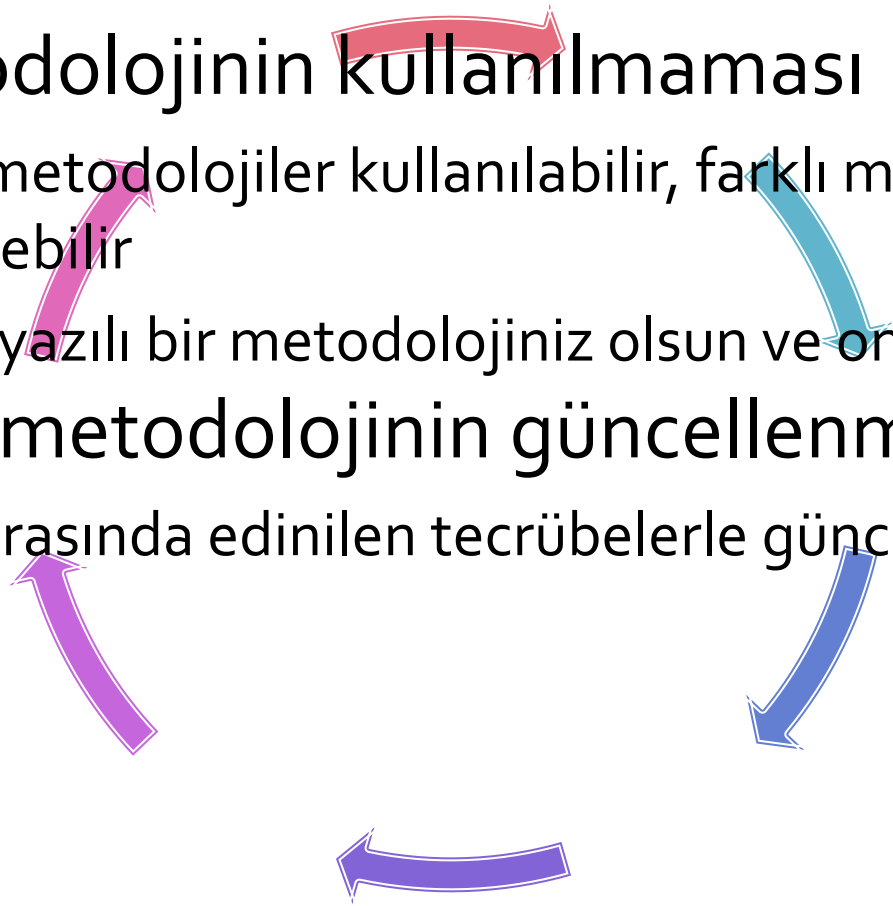
- Terminolojide netleşme. Ne isteniliyor? (pentest vs assessment)
- Kısıtlamalar
  - Bütçe
  - Zaman
- Kapsam belirleme
  - Kesin, net bir kapsam belirlenmeli
  - En büyük korkunuz/endişeniz nedir?
    - Kapsam belli değilse, öncelikli endişeler kapsamı odaklamak için kullanılabilir
    - Kolay hedefler öncelikli denetlenebilir
  - Nasıl bir test yapılacak?
  - Neler denetime dahil edilmeli?
  - Neler gerçekten kapsam dışı bırakılmalı?

Denetimin Planlanması (2)

- Denetim kuralları belirlenmelidir
  - Test yöntemi, hedefler nasıl test edilecek?
  - Kimler projede yer alacak?
  - IPS devre dışı bırakılacak mı?
  - Başlangıç/bitiş günleri, test zamanları?
  - Testler sistem yöneticilerinin bilgisi dahilinde mi yapılıyor?
  - …

Metodoloji

- Bir metodolojinin kullanılmaması
  - Mevcut metodolojiler kullanılabilir, farklı metodolojiler birleştirilebilir
  - Mutlaka yazılı bir metodolojiniz olsun ve onu takip edin
- Varolan metodolojinin güncellenmemesi
  - Testler sırasında edinilen tecrübelerle güncelleyin



Bilgi Toplama/Keşif

- Testin tümünü şekillendiren, en önemli bölüm
- Penetrasyon testinin başarısı, hedefi ne kadar anlayabildiğinizle alakalıdır

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat…"
Sun Tzu

- Daha fazla bilgi = Testin başarı oranı

"If I had eight hours to chop down a tree, I'd spend six sharpening my axe"
Abraham Lincoln

Bilgi Toplama/Keşif (2)

- En az 1 gün, bütçede sorun yoksa daha fazla zaman ayırın
- Diğer tüm aşamalar bilgi toplama ve keşif bölümüne dayanıyor
  - Bu nedenle ayakları yere sağlam basan, iyi not alınmış detaylı keşif aşaması şart
  - Elde edilen bilgileri düzenli, anlaşılır ve kullanışlı bir biçimde not alın
- Hedef envanteri tutun
  - IP, host, nasıl tespit edildi, OS, açık portlar, servis/sürüm, bilinen açıklar, hesaplar, yönetici hesapları, notlar …
- Çalışan servis ve sürüm tespiti önemli

Zaafiyet Tespiti ve Penetrasyon

- Hostname yerine IP adresi kullanın
- Denetim yaparken bir sniffer ile paketleri izleyin
  - Ne geliyor / ne gidiyor?
  - Kayıt etmek önemli değil
  - tcpdump bu iş için hızlı ve efektif
- Mutlaka full port tarama yapın
  - Zaman kısıtlı ve kapsam genişse full TCP, common UDP seçilebilir
- Hazır exploit kodlarına dikkat!
  - İçerisindeki shell kodunu değiştirin
  - Kendi sistemlerinizde detaylı inceleyin
- Penetrasyon testi yazılıma hedefi göster sonucu al değil!
- Asıl eğlence shell erişimi sağladıktan sonra başlıyor
  - Shell erişimi != Terminal erişimi
    - Shell erişiminde problem çıkartan komutlar yerine benzer işi yapan alternatif komutlar kullanın (http://bit.ly/pentest-komut-kilavuzu)
  - Kısıtlı terminaller üzerinden dosya transferi
  - Kurulmadan çalışan keşif, port tarama, tünelleme yazılımları

Şifre Tahmini - Kelime Listeleri

- Şifre kırma != Şifre tahmini
- Hedefe özel kelime listeleri oluşturun
  - Varolan temel listeleri hedefe göre genişletin
- Testler sırasında bulduğunuz şifreleri kelime listenize ekleyin
  - Bir sistemde ele geçirilen şifreler, farklı yerlerde işinize yarayabilir
- Her bir şifreyi kırmak ne kadar zamanınızı alıyor?
  - Yeni işlemci özelliklerini kullandırın(MMX, SSE2, 64bit), farklı platformlar daha hızlı olabilir (CUDA, Crackstation ;)
  - Normal sunucular, sanal sunuculara göre daha hızlı şifre kırmaktadır
  - JTR yamaları, hashcat gibi alternatifler denenebilir

Kelime Listeleri (2)

- Burası Türkiye!
  - Internet'teki bir çok liste İngilizce
  - Türkçe isimler
  - Gündemdeki olaylar, tarihimiz, futbol, diziler, ünlüler…

Raporlama

- Bıraktığınız en önemli iz
- Mutlaka denetim raporu hazırlayın
- Denetim sırasında çok iyi not alın
- Raporlarınızı ekran görüntüleriyle destekleyin
- Özet zaman planı oluşturun. Risk seviyesine göre hangi bulgular daha önce kapatılmalı?
  - Raporunuzdan uzun vadede yararlanılmasını sağlar

Raporlama (2)

- Raporda mutlaka bulunması gerekenler:
  - Yönetici özeti
  - Kapsam/test edilen sistemler
  - Denetim tarihi/zamanı
  - Test sırasında kullanılan kaynak IP adresleri
  - Denetimi yapan ekipteki kişiler
  - Organizasyondan denetime katılanlar
  - Metodoloji
  - Hedef envanteri
  - Mümkünse çözüm önerilerinde alternatif yöntemler

Teşekkürler!

İletişim
Sertan Kolat
 sertan@gmail.com
 sertankolat.com
 *twitter: @warex*