



Yapısal Testler

Can Bican



Askeri Müze ve Kültür Sitesi
Komutanlığı
Harbiye, İstanbul

25 Mayıs 2011

•Yapısal Testler,

- Test edilen sistemin iç yapısına tam erişime sahip olarak yapılan,
- Sistemin işlevinden çok yapılandırılmasıyla ilgilenen testlerdir.
- Kullanım:
 - Sistemin güvenlik politikalarıyla uyumluluğunu denetlemek,
 - Fiziksel ya da uzaktan saldırılara karşı sistemi test etmek.

- İleride olması muhtemel açıklıklarla sistem tehdit altına girdiğinde zararın ne kadar az ya da çok olacağını hakkında bilgi verir.
- Kara kutu testlerine girdi sağlayarak başka türlü erişilemeyecek yapılandırma bilgilerini sunar
- Uzak saldırganların bilgi elde etmesini zorlaştırmak için gereken yöntemleri gösterir.
- Güvenlik önlemleri yetersiz kalıp saldırı başarıya ulaştığında, olayın etkilerini en aza indirmeye yardımcı olur.

- Hassas veri işleyen sistemlerde, verinin güvenliđi ve gizliliđi esastır.
- Bu yüzden ađ üzerinden iletilen bilgi, en uygun şekilde şifrelenmelidir.
- Sabit disk, CD, kaset gibi kalıcı ortamlarda saklanan veriler, mümkün olduđu durumlarda şifreli tutulmalıdır.
 - Aynı durum geçici ortamlar için de geçerlidir, fakat bu tür ortamlarda şifreleme ya imkansız ya da çok maliyetli olmaktadır. Bu nedenle geçici ortamların erişimi kısıtlanmalıdır.

- Sisteme eklenen her özellik aynı zamanda saldırı olasılıklarını artırır.
- Güncellemelerinin gözden geçirilmesi ve güvenlik açıklıklarına zamanında tepki verilmesi vb. etkinlikler maliyetleri artırır.
- Sadece yazılımın kurulu bile bulunması riskleri artırır.
- Sistemdeki yazılımların sadece gereklilerle sınırlandırılması, sisteme erişim noktalarının en aza indirgenmesi, açıklık olasılıklarını azaltarak, güvenliği sağlamanın maliyet ve risklerini düşürür.

- Hizmetlerin mantıksal olarak farklı sistemlere ayrılması, ayrı hizmetlerin güvenli bir şekilde birbirine erişiminin düzenlenmesini olanaklı kılar.
- Örneğin FTP sunucusunun ele geçirilmesi, e-posta hizmetlerini de dolaysız bir tehlikeye sokmaz.
- Bu prensip, diğer kaynaklara da uygulanabilir:
 - Topoloji tasarlanırken ağların benzer görevleri olan bilgisayarlara dağıtılması,
 - Birden fazla rol ya da yetkiye sahip olan kullanıcı bulundurulmaması
 - ...

- Çoğu işletim sistemi, güvenliğe yönelik araç ve uygulamalarla gelmektedir.
- Masaüstüne yönelik işletim sistemlerinde bile standart bir güvenlik duvarı bulunmaktadır.
- Aynı zamanda virüs tarayıcı, içeri kontrolcüsü gibi uygulamalar da kolay erişilebilir ve yapılandırılabilir durumdadır.
- Üretici tarafından sunulan ve güvenlik için önerilen çözümler atlanmamalı, varsayılan yapılandırmadaki güvenlik ayarları asgari seviye olarak belirlenmelidir.

- Güvenlik seviyesi için belirlenecek asgari seviyede, tüm hizmetlerin kaynaklara erişimi sınırlandırılmalıdır.
- Özellikler açıldıkça ihtiyaca göre erişim izinleri ayarlanabilir.
- Böylece gereksiz erişimlerin yok edilmesi sağlanabileceği gibi, sisteme erişen kullanıcıların ya da diğer sistemlerin hassas bilgilere hatalı yapılandırma sonucu erişimleri de engellenebilir.

- Sistemin mimarisinin incelenmesinin asıl amacı, sonraki çalışmalar için yol haritasını çıkartmaktır.
- Mimari çözümlemenin hedefleri:
 - Güvenlik politikasının çözümlenmesi,
 - Sistem bileşenlerinin belirlenmesi,
 - Saklanan verinin kullanımının araştırılması,
 - Sistemin dış sistemlerle etkileşiminin incelenmesi.
- Mimari çözümlemenin amaçları:
 - DDOS gibi standart saldırılara tasarım olarak dayanıklılığı
 - Kullanıcı gereksinimlerine uygunluğu
 - ...

- Sistemin ve içinde çalışan uygulamaların, verilen hizmetlerin yapılandırılması, sistem güvenliğinde çoğu ölçütün kaynağıdır.
- Yapılandırma çözümlenirken:
 - Sistemde nelerin varolduğu (işletim sistemi, çalışan süreçler, donanım özellikleri v.b.),
 - Nasıl ayarlandıkları (aynı sunucu üzerinde çalışan hizmetler, kaynakların nasıl yönetildiği v.b.),
 - Hangi kişilerin sisteme nasıl eriştikleri gözönüne alınır.

- İşlevsel çözümlemede, sistemin kaynak kodu incelenir.
- Tam bir kaynak kodu incelenmesi her zaman mümkün olmamaktadır.
- Uygulamanın nasıl çalıştığını incelenir, kritik uygulama bileşenleri belirlenir ve açıklığa sebep olabilecek noktalar ortaya çıkartılır.
 - Girdi doğrulaması
 - Çıktı düzeltilmesi
 - Veritabanı ile etkileşim
 - Dış yetkilendirme sistemleriyle iletişim

- Standart kurulum
- Güvenlik
- Özelleştirme
- Belgelendirme
- Felaket önlemleri ve felaket sonrası
- Yeni özelliklerin eklenmesi
- Güncellemelerin uygulanması
- Hata giderilmesi

- Testlerin düzenli uygulan(a)maması
 - Vaktinde önlem alınamaması
- Testlerin döngüye dahil edilmemesi
 - Düzeltmelerin hiç yapılmaması
- Diğer gereksinimlerden dolayı düzeltmelerin yapılmaması

- Otomasyon: Geç düzeltmenin ya da hiç düzeltmemenin en güçlü ilacı.
 - Otomasyon için çeşitli ürünler mevcuttur.
 - Çoğu zaman otomasyon için evde geliştirilmiş çözümler kullanılır.
 - Tek araçla her amaca yönelik çözüm bulunamayabilir.
 - Hızlı çözümler ya da Internet'ten alınan tavsiyeler kullanılan araca yönelik olmayabilir.

- Puppet, sistem yapılandırmasının otomasyonunda kullanılan bir araçtır.
- Unix benzeri ve Windows sistemlerin yapılandırmasını yönetir.
- Programlama bilgisine gerek olmadan tüm sistem otomasyonunu sağlayabilir.
- Yapılandırma testlerinin Puppet kuralları kullanarak otomasyonu, karşılaşılan sorunları azaltabilir.

- Yapısal güvenlik testleri, sistemin çeşitli güvenlik açıklıklarına, özellikle bilinmeyen güvenlik açıklıklarına karşı sıkılaştırılmasına yardımcı olur.
- Yapısal testler yapılandırma döngüsüyle bütünleştirilmelidir.
- Puppet ile tekrarlanabilir ve taşınabilir test ve sıkılaştırma çözümleri mümkündür.



TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

bican@uekae.tubitak.gov.tr

0 312 4277366 - 110