

GamaLAN Yerel ağ güvenlik denetimi, kurumsal yerel ağ verimliliğinin ve sağladığı güvenlik seviyesinin ölçülmesi için hazırlanmış özel kontroller içermektedir. Güvenlik denetimi süresince yerel ağ zaafiyet analizi ve ağ elemanlarının yapılandırma analizi yapılmakta, saptanan güvenlik açıklarının kullanımı sonucu elde edilen haklar ve işlemler, çözüm raporu ile beraber sunulmaktadır. Saptanan zaafiyetlerin giderilmesini takiben yapılan doğrulama testi hizmete dahildir.

Kazanımlarınız

- Olacakları bilmek: Sisteminize yerel ağdan gelecek gerçek bir saldırı durumunda başınıza gelecek kayıpları zarar görmeden tecrübe etmek
- Mevcudu onaylamak: Mevcut güvenlik mekanizmalarınızı, saldırı tespit ve cevap sistemlerinizi deneyimli **GamaSEC** güvenlik uzmanlarına karşı sınavdan geçirmek ve güvenilirliğini onaylamak
- Düşmanı tanımak: Sisteminizin yerel ağdan nasıl görüldüğünü ve düşmanın neler yapabileceğini görmek, gerçekte yaşayacağınız zararı yaşamadan düşmanınızı tanımak
- Farkındalık: Organizasyonun tüm seviyelerinde farkındalık yaratarak şirket güvenlik politikasının gelişimine katkı sağlamak

GamaLAN - Denetim Metodolojisi

- Erişilebilirlik Analizi
- Ağ Haritası Oluşturulması
- Aktif Cihazların Keşfedilmesi ve Analizi
- Yardımcı Ağ Cihazlarının Analizi
- Güvenlik Teknolojilerinin Analizi
- Otomatize Güvenlik Açığı Taraması
- Yayınlanmış Güvenlik Açığı Taraması
- Yayınlanmamış Güvenlik Açığı Taraması
- Saptanan Güvenlik Açıklarının Değerlendirilmesi
- Çözüm Geliştirme ve Rapor Hazırlığı

Erişilebilirlik Analizi

Bu aşamada kuruluşunuzun yerel ağ üzerindeki varlığı ve alınabilen temel bilgiler gözden geçirilerek bilgisayar ağınıza ait, herhangi bir saldırıda kullanılacak temel bilgileri toplanmaktadır. Genel Bilgi Toplama, Ağ Altyapısı Analizi, Ağ Haritalama ve WINS/DNS sorgulama aşamalarından oluşmaktadır. Hedef ağ doğru biçimde yapılandırılmış ise, ideal durumda ağ ile ilgili istenmeyen bilgi saptanmayacaktır.

Ağ Haritası Oluşturulması

Kuruma ait ağ üzerinde etkin durumda olan sistemlerin saptanması, servisleri, işletim sistemi ve uygulamaların belirlenmesi ile sistemlerin bağlantı biçimleri analizini içermektedir. Yapılan analiz sonucunda sunucuların işletim sistemi, uygulamaları, servisleri, güvenlik teknolojileri ve sistemlerin bağlantı biçimleri elde edilebilmektedir.

Aktif Cihazların Keşfedilmesi ve Analizi

Kurum tarafından kullanılan IP adresleri aralığı üzerinde, belirli bir dzi TCP, UDP ve ICMP paketleri gönderilerek aktif durumdaki cihazların tespit edilmesi bu adımda gerçekleştirilir. GamaSEC danışmanları, switch ve hub gibi katmanda çalışan cihazların yapılandırılmalarının analizini yapacaktır.

Yardımcı Ağ Cihazlarının Analizi

Ağda bulunan ve sistemlere yardımcı olma amaçlı kullanılan güç kaynağı, ağ temelli yazıcı ve tarayıcı gibi cihazların yönetim zaafiyetleri denetlenecektir. Bu cihazların zaafiyetleri ağına veya sunucuların devre dışı bırakılmasına sebep olabileceği gibi içindeki bilgilerin dışarı sızmasına da sebebiyet verebilmektedir.

Güvenlik Teknolojilerinin Analizi

Hedef ağı korumakta olan güvenlik teknolojileri yol izleme, etkin sistem saptama, bilgi sızmaları ve özel yöntemler kullanılarak saptanmaktadır. Saptanan güvenlik teknolojileri TCP/IP yapıları, tepkileri ve mimarileri analiz edilerek güvenlik açıklarına karşı denetlenmektedir.

Otomatize Güvenlik Açığı Taraması

Denetim süresince saptanan tüm sistemlere otomatize yazılımlar aracılığıyla güvenlik açığı denetimi yapılmaktadır. Çok sayıda farklı yazılım aracılığıyla saptanamayan birçok güvenlik açığı saptanabilmektedir. Kullanılmakta olan güvenlik açığı tarama yazılımları ticari lisanslara sahip veya açık kaynak kodlu ve ücretsizdir.

GamaSEC Denetim Hizmetleri

- GamaNET İnternet Güvenlik Denetimi
- GamaAPP Web Uygulama Güvenlik Denetimi
- GamaLAN Yerel Ağ Güvenlik Denetimi
- GamaAUDIT Bilişim Sistemleri Denetimi
- GamaWIRELESS Kablosuz Ağ Güvenlik Denetimi
- GamaSCAN Otomatize Güvenlik Denetimi
- GamaVPN Sanal Özel Ağ Güvenlik Denetimi
- GamaDMZ DMZ Ağı Güvenlik Denetimi

GamaSEC Danışmanlık Hizmetleri

- GamaPOLICY Güvenlik Politikası Danışmanlığı
- GamaCON Bilgi Güvenliği Danışmanlığı

GamaSEC Tecrübesi

➤ **GamaSEC** danışmanları, kurumsal güvenlik ihtiyacınızın belirlenmesi, bilgi güvenliği yatırımınızın verimliliğinin ölçülmesi, bilgi varlıklarınıza yönelik güvenlik tehditlerinin belirlenmesi, kurumsal risk analizinizin yapılması hizmetlerini sunabilmek amacıyla en yeni teknolojileri, kendi geliştirmiş oldukları yöntemleri ve araçları kullanmaktadır.

➤ **GamaSEC** danışmanları, güvenlik denetimi ağa/sunucuya sızma sürecinde kullanmak üzere **GamaSEC** Exploit Framework yazılımını geliştirmiş, kendi geliştirmiş olduğu teknik ve araçları yazılıma entegre etmiştir. GamaSEC Exploit Framework yazılımı ile çok sayıda yayınlanmış veya ekipçe geliştirilmiş exploit merkezi yapıya sokulmuş, ağa/sunucuya sızma süreci daha verimli hale getirilmiştir.

➤ **GamaSEC** danışmanlarınca geliştirilen bir diğer ortam olan **GamaSEC** Audit Framework ile de ticari yazılımlar, açık kaynaklı yazılımlar ve **GamaSEC** Exploit Framework arası entegrasyon sağlanmış, raporlama süreçleri iyileştirilmiş ve güvenlik denetim süreçleri yönetilebilir hale getirilmiştir.

Yayınlanmış Güvenlik Açıkları Özel Taraması

Otomatize güvenlik açığı tarama yazılımları, güvenlik açıklarının uygulamaya özel olması, özel doğrulama yöntemi gereksinimi, farklı sistem türlerinde çalışması veya ağ üzerinden erişilebilir olmaması nedeniyle başarılı sonuçlar üretememektedir. Bu nedenle otomatize tarama araçlarının yetersiz kaldığı göz önünde tutularak, denetim boyunca saptanan tüm sistem ve uygulamalar özel denetimler aracılığıyla denetlenmektedir. Özel denetim aşamasında, saptanmış olan her uygulamanın yayınlanmış ve doğrulanmış olan güvenlik açıkları sırayla denetlenmekte, yayınlanmış güvenlik açığı sonuçları farklı açılardan yaklaşılarak analiz edilmekte, alternatif yöntemler kullanılarak sonuçlar incelenmektedir.

Yayınlanmamış Güvenlik Açıkları Özel Taraması

Hatalı uygulama geliştirme, yapılandırma veya ağ yerleşiminden kaynaklanan ancak henüz yayınlanmamış olası güvenlik açıklarının analizini içermektedir. Web temelli veya ağ temelli uygulamalar ile ağ yapısı üzerinde var olan veya oluşabilecek güvenlik açıkları aranmaktadır. Söz konusu güvenlik açığı olabilecek nokta saptandığında oluşan risk analiz edilmekte, arka planda bulunan yapının güvenlik açığından etkilenme oranı hesaplanmakta ve çözüm geliştirilmektedir.

Saptanan Güvenlik Açıklarının Değerlendirilmesi

Erişilebilen tüm sunucu, yönlendirici, güvenlik teknolojileri ve istemcilerin üzerinde bulunabilecek güvenlik açıkları tespit edilir. Bu son aşamada, önceki aşamalarda elde edilmiş tüm bilgiler toplanarak sınıflandırılır ve haritalandırılır. Çeşitli zayıflıklar, riski ve tahmin edilen saldırı yolları göz önüne alınarak önem derecelerine göre sıralanır. Tespit edilen güvenlik açıkları, taşıdıkları riskler değerlendirilir ve önemine göre sıralanır.

Çözüm Geliştirme ve Rapor Hazırlığı

Yukarıdaki tüm işlemler tamamlandıktan sonra, güvenlik uzmanlarımız tespit edilen bulgular ve güvenlik açıklarından hareketle her bir güvenlik açığı için çözüm önerileri oluşturur ve raporlar. Denetim Raporu, yönetici özeti, güvenlik açıklarının istatistiksel dağılımı, grafikleri, her bir açığın açıklaması ve çözüm önerilerini içermektedir. Bu rapor sayesinde güvenlik taramasına dahil edilen sistemlerin güçlü ve zayıf olduğu noktalar değerlendirilebilecektir.