

GamaNET Internet güvenlik denetimi, kurumsal ağ altyapınızın verimliliğinin ve sağladığı güvenlik seviyesinin ölçülmesi için hazırlanmış özel kontroller içermektedir. Güvenlik denetimi süresince tam ağa sızma denetimi yapılmakta, saptanan güvenlik açıklarının kullanımı sonucu elde edilen haklar ve işlemler, çözüm raporu ile beraber sunulmaktadır. Güvenlik probleminin tarafınızdan giderilmesini takiben, açıkların kapandığını doğrulamak amacıyla yapılan doğrulama testi hizmete dahildir.

Kazanımlarınız

- Olacakları bilmek: Sisteminize internet üzerinden 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 dışarıdan 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

GamaNET - Denetim Metodolojisi

- Erişilebilir Bilgi Taraması
- Ağ Haritalama
- Güvenlik Teknolojilerinin Analizi
- Otomatize Güvenlik Açığı Taraması
- Yayınlanmış Güvenlik Açığı Taraması
- Yayınlanmamış Güvenlik Açığı Taraması
- Güvenlik Açığı Kullanılarak Sisteme Sızılması
- Saptanan Güvenlik Açıklarının Değerlendirilmesi
- Çözüm Geliştirme ve Rapor Hazırlığı

Erişilebilir Bilgi Taraması

Bu aşamada kuruluşunuzun Internet üzerindeki varlığı ve alınabilen temel bilgiler gözden geçirilerek bilgisayar ağınızın herhangi bir saldırıda kullanılabilir temel bilgileri toplanmaktadır. Genel Bilgi Toplama, yapılan bir grup sorgulama sonucu hedef organizasyon yada yerel ağ hakkında elde edilebilecek bilgileri ortaya çıkarmaya dayanır.

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.

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 sahiptir veya açık kaynak kodlu ve ücretsizdir.

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 üretmemektedir. 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.

GamaSEC Denetim Hizmetleri

- GamaNET Internet 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.

Yayınlanmamış Güvenlik Açıkları Özel Taraması

Hatalı uygulama geliştirme, yapılandırma veya ağ yerleşiminden kaynaklanan ancak henüz yayınlanmamış olası güvenlik açıklarının analizi 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.

Güvenlik Açıkları Kullanılarak Sisteme Sızılması

Sistemlerde saptanmış olan güvenlik açıkları kullanılarak açığı barındıran sistemlere veya ağa sızılmaya çalışılmaktadır. Yayınlanmış güvenlik açıklarının bir kısmının içeriği de açıklanmış ve "exploit" olarak bilinen kullanım yöntemleri yayınlanmıştır. Bir kısmının ise içeriği açıklanmamış veya açıklanmasına rağmen açığın kullanım yöntemleri belirlenememiştir. Bu sebeple saptanan bazı güvenlik açıklarının kullanılması mümkün olamamaktadır.

Bu sorunlara çözüm olarak GamaSEC danışmanları GamaSEC Exploit Framework yazılımını geliştirmiş, çok sayıda "exploit"i özelleştirmiş ve "exploit"i yazılmamış birçok açık için "exploit" geliştirerek tek bir yazılım altında birleştirmiştir.

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.