



Labris™ Güvenlik Tarayıcısı / Zayıflık Analiz Sistemi

Güvenlik Tarama sistemi,

**ağınız üzerine bağlı olan tüm cihazları tarar,
olası güvenlik sorunlarını raporlar**

İnterneti kullanan sistemlerin ve servislerin gittikçe yaygınlaşması sonucu bunlar üzerinde çıkacak güvenlik açıkları veya zayıflıkları tespiti servislerin sürdürülebilirliğini sağlamak açısından çok önemli olmuştur. Çünkü İnternet üzerindeki bu servislerde oluşabilecek bir kesinti kurumlar için hem prestij hem de para kaybına sebep olmaya başlamıştır.

Güvenlik Tarama Sistemlerinin kullanılarak İnternet cihazlarının raporlanmış açıklar yada zayıflıkları taşıyıp taşımadıklarını tespit etmek mümkün olabilmektedir. Buna göre güvenlik zayıflığının yada açığının bulunduğu sistem için gerekli yükseltmeler(upgrade) ya da yamalar(patch) yapılarak sistemler daha güvenli hale getirilebilir.

Güvenlik Tarama Sistemi Nasıl Çalışır?

Sistemimde açık yada zayıflık var mı acaba?

Güvenlik tarama sistemi kendi veri tabanında olan zayıflık veya açıkları karşıdaki sistem her ne olursa olsun deneyerek tespit eder.

Tespit edilen bu açıkları değişik formatlarda raporlayarak kullanıcıya esneklik sağlar. Ayrıca bu raporlarda güvenlik açığının yada zayıflığının önem katsayısı da verilerek kullanıcının buna göre hareket etmesi sağlanmış olur.

Açıklar ve zayıflıklar sürekli olarak yenilediğinden yeni çıkanlara karşı da önlem alınmış olur.

Kimin için?

Tüm ağlar için: Dışarı açık her türlü ağda, İnternet protokollerini (TCP,UDP,ICMP) kullanan tüm cihazlar için kullanılabilir.



Labris™ Güvenlik Tarayıcısı / Zayıflık Analiz Sistemi

Bir Bakışta

- ⊕ Birden fazla işlemci (CPU) platformları ve işletim sistemleri desteği
- ⊕ Cihaz tipinden bağımsız olarak tüm TCP cihazları ile çalışabilirlik
- ⊕ Plugin desteği sayesinde güvenlik testinin kullanıcı tarafından kolayca eklenebilme esnekliği
- ⊕ Kendine ait betik dili sayesinde kolayca kural eklenebilme yeteneği
- ⊕ İstemci-sunucu mimarisinde çalışma yeteneği
- ⊕ Akıllı servis tanıma yeteneği sayesinde kendi portu üzerinde çalışmayan servisleri tespit edebilme özelliği
- ⊕ Güvenlik taraması yapılacak sistem üzerindeki servisin özelliklerine göre test yapabilme kabiliyeti
- ⊕ Bütün ssl servislerini test edebilme yeteneği
- ⊕ Güvenli tarama modu ile arka plan sistemlerine zarar vermeden tarama
- ⊕ Zamanlanmış taramalar ile arka planda sistemlerin taranması
- ⊕ Raporlamayı farklı formatlar şeklinde yapabilme özelliği
- ⊕ Raporlamada risk seviyesini belirtme
- ⊕ Sürekli olarak güncellenen kural tabanı
- ⊕ 7000'den fazla açık imzası
- ⊕ Kural tabanı üzerine ekleme yapabilme esnekliği
- ⊕ Sınırsız kullanıcı ve süre ile lisanslama
- ⊕ Üçüncü parti ürünler ile entegrasyon
- ⊕ Yüksek başarımlı

Yönetim – İzleme

- ⊕ Grafik Kullanıcı Arayüzü ile Kolay Yönetim
- ⊕ Windows, Linux, Solaris ve diğer birçok platformdan, uzaktan yönetim
- ⊕ Yönetim konsollarında veri tutulmadığından tamamen mobil yönetim
- ⊕ Yönetim konsolu ve SS cihazı arasında güvenli LMCCP protokolü ile erişim
- ⊕ Tek ekrandan ağdaki birden fazla yakın ve uzak Labris SS cihazının yönetimi
- ⊕ Yönetim arabiriminden kolayca oluşturulan istemci-ağ erişimleri için son kullanıcı erişim sertifikaları
- ⊕ Yönetim platformundan belli kişilere çeşitli seviyelerde yetki dağıtımı (sadece izleme, ayar değiştirme vb.)
- ⊕ SSH ile gelişmiş uzaktan yönetim

Kayıt-Raporlama

Saldırı ve zayıflığı yapılan sistemleri ile ilgili raporları;
ASCII text
LaTeX
HTML formatlarında sunabilme yeteneği