



Labris™ Saldırı Tespit ve Önleme Sistemi (IDS/IPS)

Saldırı tespit sistemleri ağınıza yada makineniz üzerine yapılan saldırıları tespit eder
Saldırıları karşı gerekli önlemleri alabilmeniz için size yardımcı olur

İnternetin 1990'lı yıllarda hızla gelişmeye başlamasıyla Internet üzerine açılan servislerin sayısı gittikçe artmıştır. Ancak bu servisleri vermek için kullanılan sistemlerin veya uygulamaların üzerinde varolan yada çıkabilecek zayıflıkları sürekli olarak izlemek gittikçe imkansız hale gelmektedir.

İşte STS'ler bu tip zayıflıkları kullanarak sistemlere zarar vermeye çalışanları tespit ederek buna önlem alabilmeye yardımcı olurlar. Hatta yeteneğine bağlı olarak saldırı yapan yerleri güvenlik duvarı yazılımları ile ortak çalışarak engelleyebilir.

Eğer kural tabanında yer alıyorsa, Internet üzerine bağlı tüm cihazlara yapılabilecek saldırıları tespit edebilir. Farklı tipte saldırıları tespit edebilmeniz için sizin kural tabanına ekleme yapabilmenize olanak sağlar.

Saldırı Tespit Sistemi Nasıl Çalışır?

Saldırı tespit sistemleri değişik şekillerde çalışabilir. Bunlardan en fazla kullanılan sunucu ve ağ saldırı tespiti şeklindedir. Sunucu modu çalışmada Saldırı Tespit Sistemi sunucu üzerine kurularak sadece bu sunucu üzerine yapılan saldırılar tespit edilir. Diğer çalışmada ise Saldırı Tespit Sistemi ağ üzerinde konumlandırılarak ağ üzerindeki sunuculara veya istemcilere yada Internet üzerinden yerel ağa yapılan saldırıların tespit edilmesi mümkündür.

Bu saldırı tespit işlemi Saldırı Tespit Sisteminin kural tabanları üzerinden yapılmaktadır. Bu kural tabanları sürekli olarak güncellendiğinden yeni tip saldırıların tespitleri çok kolay bir biçimde yapılabilmektedir. Ayrıca bu kural tabanlarına istenirse yönetici tarafından yeni kurallar eklenebilmektedir.

Raporlama konusunda gerçek zamanlı raporlama yeteneğinin yanında SNMP, SMB , Syslog gibi uygulamalara da raporlama yapabilmektedir.

Kimin için?

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



Labris™ Saldırı Tespit ve Önleme Sistemi (IDS/IPS)

Bir Bakışta...

- ⊕ Kolay kurulum
- ⊕ Labris multi-platform kurulum programı (Labris Installer)
- ⊕ Birden fazla CPU platformu yada İşletim Sistemi üzerinde çalışabilme yeteneği
- ⊕ IP Ağları üzerinde saldırı tespit yada paket izleme yeteneği
- ⊕ Paket izleme yaparken değişik formlarda kayıt imkanı
- ⊕ Protokol analizi, içerik arama ve denetleme ayrıca birçok saldırı şeklini tespit edebilme yeteneği
- ⊕ Stateful izleme yeteneği
- ⊕ Portscan tespit kabiliyeti
- ⊕ Gerçek zamanlı saldırı tespitini gösterebilme yeteneği
- ⊕ Raporlama'yı farklı uygulamalar üzerine yapabilme özelliği
- ⊕ Sürekli olarak güncellenen kural tabanı
- ⊕ 3000'den fazla saldırı imzası
- ⊕ Kural tabanı üzerine ekleme yapabilme esnekliği
- ⊕ İmza tabanlı çalışma yapısına ek olarak davranış analizi ve protokol anormallik tespiti yöntemleri desteği
- ⊕ Sınırsız kullanıcı ve süre ile lisanslama
- ⊕ Üçüncü parti ürünler ile entegrasyon (firewall vb.)
- ⊕ 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 IDS cihazı arasında güvenli LMCCP protokolü ile erişim
- ⊕ Tek ekrandan ağdaki birden fazla yakın ve uzak Labris IDS 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.)
- ⊕ SFTP ve LMCCP ile uzaktan güncelleme
- ⊕ *SSH ile gelişmiş konsol yönetimi*
- ⊕ *Türkçe yönetim arabirimleri*

Kayıt-Raporlama...

- ⊕ Saldırıları gerçek zamanlı olarak gösterebilme
- ⊕ Saldırıları gerçek zamanlı olarak ;
 - SNMP
 - SMB
 - Syslog
 - Unixsock
 - XML
 - Tcpdump
 - Veri tabanlarına yazabilme yeteneği