Güvenli E-Posta Geçidi

Gizem İSKENDEROĞLU, Halit ALPTEKİN

Öğr.Gör. Selçuk CEVHER

Giriş

Proje kapsamı içerisinde güvenli e-posta geçidi gerçekleştirilmiştir.İlgili geçit içerisinde e-posta trafiği toplanmaktadır.Toplanan e-posta trafiği daha sonradan analiz işlemine tabi tutulmaktadır.Analiz edilen ve analiz edilmeyi bekleyen e-postalar bir panel aracılığı ile kullanıcıya gösterilmektedir.Bu panel içerisinden analiz edilen e-postanın herhangi bir tehdit içerip içermediği görülebilmektedir.Aynı şekilde kullanıcının tanımlayabileceği kurallar ile de e-posta trafiğinin uyuşup uyuşmadığı görülebilmektedir.

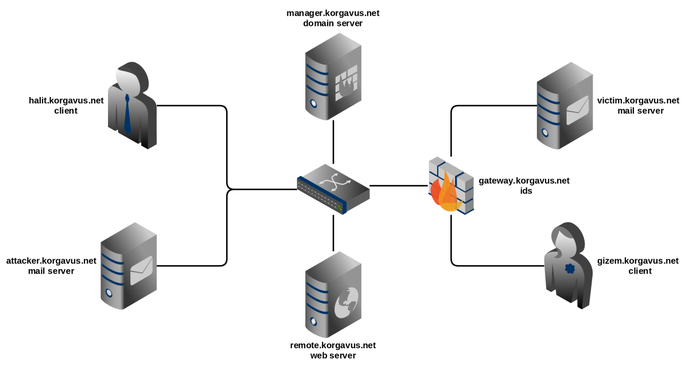
Bu sistem aracılığı ile korunmak istenen ağa gelen e-posta trafiği analiz edilip içerisinde herhangi bir siber tehdit barındırıp barındırmadığının kontrolü yapılmaktadır.Burada bahsedilen siber tehditler zararlı dosya indiren site adresleri, dünya üzerinde yer alan saldırgan IP adresleri, spam e-posta gönderen adresler olabileceği gibi henüz tespit edilmemiş açıklıkları sömüren kod parçaları olabilmektedir.Örneğin yakın bir zamanda ortaya çıkan ve e-posta sunucuları hedef alan açıklığın sömürülmesi, gerçekleştirilen sistem tarafından başarıyla tespit edilmiştir.

Kurulumlar

Sistem yapısı gereği birçok alt birimden oluşmaktadır.Bu birimler birbirlerinden tamamen bağımsız olarak geliştirilmiştir.Gerçekleştirilen sistem ağ altyapısı, ağ geçidi, paket toplayıcı, analiz aracı ve siber tehdit kaynak arayüzü alt birimlerinden oluşmaktadır.

Ağ Altyapısı

Gerçekleştirilen ağ geçidinin test edilebilmesi için uygun bir ağ ortamına ihtiyaç duyulmaktadır.Bu yüzden kurumsal bir ağ yapısı kurgulanıp proje içerisinde kullanılmıştır.



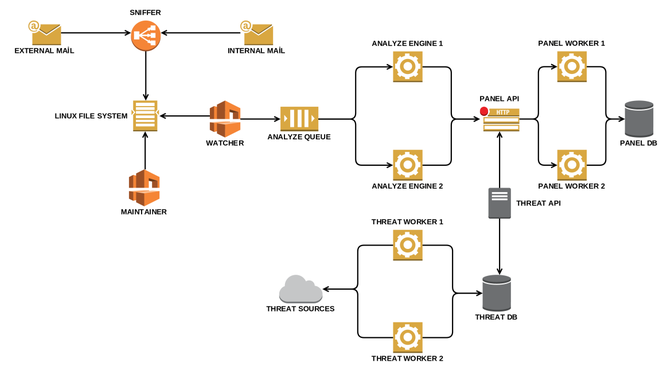
Şekil: Gerçekleştirilen ağ alt yapısı.

Ağ Geçidi

Gerçekleştirilen ağ geçidi, üzerinden geçen trafiği toplayıp analiz etme ile ilgilenmektedir.Burada toplanan trafik sadece e-posta trafiği olmaktadır.Geçidin trafiği toplayabilmesi için iki adet ağ arayüzü kullanılmıştır ve aralarında köprü bağlantısı yapılmıştır.

Paket Toplayıcı

Geçidin, üzerinden geçen trafiği köprülemesinden sonra yapılması gereken bu trafiğin toplanmasıdır.Bu amaçla paket toplayıcı yazılımı geliştirilmiştir.E-posta paketleri yapısına uygun olarak dosya sistemi içerisine kaydedilmektedir.



Şekil: E-posta akış grafiği.

Analiz Aracı

Geçit üzerinden geçen paketler birer json dosyası olarak kaydedilmektedir.Paket toplayıcı bu görevini tamamladıktan sonra ilgili e-postaların analiz edilmesi gerekmektedir.Bu analiz işlemi hem kural tabanlı hem de imza tabanlı olarak gerçekleştirilmektedir.Aynı zamanda yeni bir analiz motorunun eklenmesi yapısı gereği çok kolaydır.

Takipçi

Takipçi uygulaması dizin içerisine yeni bir paket gelip gelmediğinin kontrolünü yapmaktadır.Yeni bir paketin gelmesi durumunda dosya içeriği e-posta yapısına uygun olarak ayrıştırılmaktadır ve analiz aşamasına geçilmektedir.

Siber Tehdit Kaynak Arayüzü

Üzerinden geçen trafiğin analiz edilmesi sırasında kullanılan kural ve imza veritabanlarının güncel tutulması gerekmektedir.Bu amaçla siber tehdit kaynak arayüzü gerçekleştirilmiştir.Burada sürekli olarak siber tehditler çeşitli kaynaklardan toplanarak geçerli kurallar topluluğuna dönüştürülmektedir.

Yapılandırmalar

Sistem içerisinde yer alan tüm birimler ayrı bir şekilde yapılandırılmıştır.Bu yapılandırmalar içerisinde Raspberry Pi cihazının işlemci saat frekansını arrtırmak gibi performans ile ilgili kısımlar da vardır.Benzer şekilde güvenlik açısından önemli yapılandırmalar da gerçekleştirilmiştir.

Sonuçlar

Proje kapsamında tasarımı yapılan tüm aşamalar başarıyla tamamlanmıştır.Kurulan test ağ ortamında yer alan iki sunucunun birinden diğerine gönderilen e-postalar analiz işlemine tabi tutulabilmektedir.Analiz işlemleri sırasında elde edilen sonuçlar başarıyla panel içerisinde gösterilebilmektedir.Analiz motorlarının daha performanslı çalışması için gerekli tüm çalışmalar yapılmıştır.Bu amaçla kendisini ispat etmiş kütüphanelerden faydalanılmıştır.Haliyle ortaya çıkan sonuç başarılı olmuştur.Geliştirme sürecinin kolay geçmesi açısından yazılan harici betikler de başarıya ulaşmada büyük etken olmuştur.

Tasarım Projeleri Sergisi, 8 Ocak 2016, Trabzon