Topolojik Bağımlı Otomatik Sistem Güvenliği Tarama Yöntemi

Ertugrul Akbas

Özet— **Bu çalışma önemi gittikçe artan ve ister ev kullanıcısı ister kurumsal kullanıcı olsun herkesin ihtiyacı durumuna gelen ve bilinen sistemlerin adresleyip çözümleyemediği tasarım problemleri (genişleme,yeni özellikler ekleme vs..) ve kolay kullanım gibi problemlere çözüm üreten otomatik güvenlik açığı tarayıcı sistem tasarım ve gerçeklemesini açıklamaktadır.Otomatik Güvenlik Tarayıcısı (OGT) yukarıda özetlenen tüm özelliklere sahiptir.**

Anahtar Kelimeler— **Ağ Güvenliği, Güvenlik Değerlendirmesi, Güvenlik Taraması, Otomatik Topolojik Haritaların Oluşturulması, SNMP**

I. Otomatik Güvenlik Tarayıcı

Otomatik güvenlik tarayıcıları ticari veya açık kaynak kodlu olarak zaten mevcuttur. Ticari olarak en bilinenleri ISS [1] ve RETINA [2] açık kaynak kodlu olanlara ise COPS[3] ve Nessus [4] dur.

Tasarlanan sistemin (OGT) en önemli ihtiyacı modüler olmasıdır. Sistem 3 katmandan oluşmaktadır. İlk katman yönetim katmanıdır ve güvenlik denetimi için gereken ortamı hazırlar ve diğer modülleri kontrol eder ve yönetir ayrıca bu katman sisteme eklenecek yeni katmanların yönetilmesi işlemlerini de sağlar. 2. katman aktif güvenlik taramalarının yapıldığı modüldür. Bu parça ayrıca plugin yapısı ile çalışan yeni güvenlik tarama yeteneklerinin eklemesi çıkarılması gibi yönetsel işlemleri de yönetir. 3 katman yapılan taramalardan kullanıcının kolay anlayabileceği raporları üretecek modüldür.

Tasarlanan sistem modüler olmasının yanı sıra her çeşit güvenlik açığını tarayabiliyor olmalı (cihaz temelli ve ağ temelli) (host based, network based vs.), yeni katmanların eklenebilmesi ve tabi sistem ve bilgisayar yöneticilerinin uzun zamanlar harcayarak edindiği tecrübeleri sisteme kolayca aktarabilecekleri bir ortam (java, MS Visual Basic ve Phyton) ve altyapı ile birlikte bu tekrar eden faaliyetleri otomatikleştirilmesi.

Dr. Ertugrul Akbas, CBR YAZILIM, Hacı HalilMah Yazı Cad. No 33, 41400, Gebze, TURKEY, ertugrul.akbas@cbr.com.tr

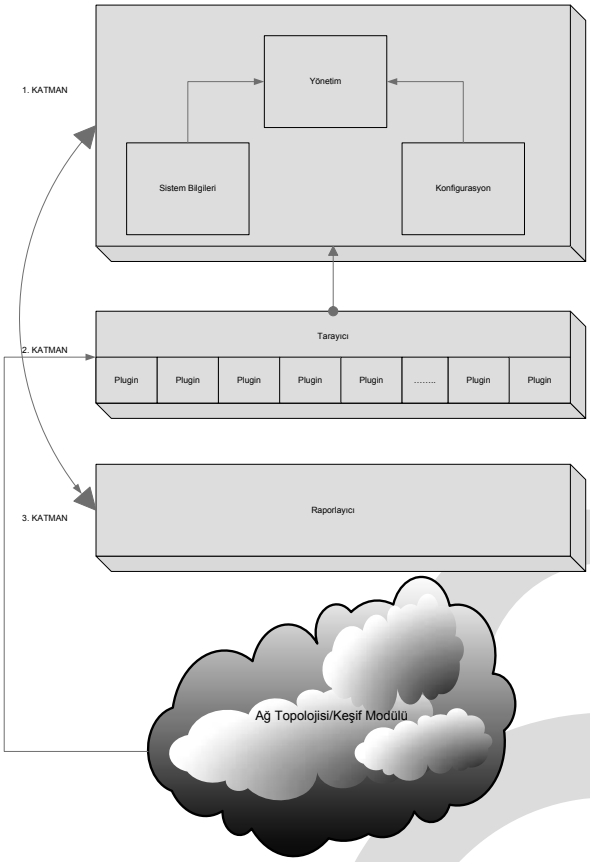
Sistem diğer sistemlerin düştüğü hatalardan biri olan, aranacak sistemle ilgili işlemlerin mesela sistemin işletim sistemi, yüklü servisler, korunma yöntemler, topolojileri vs dikkat etmeden deneme yanılma ile yapılan testler ve gereksiz zaman kaybına (bu kayıp büyük ağlarda günlerce olmakta) düşmemek için otomatik topoloji ve keşif yapabilmektedir. Otomatik keşif ve topolojinin sağladığı avantajlar:

1- Sistem yöneticisine tarama yapılacak sistem ile ilgili genel ve tam bir bakış açısı sağlaması
2- Tarama sırasında işletim sistemi ve servisler de tespit edildiği için hangi makine için hangi testler kullanılacağının tespiti
3- Topoloji ile ilgili testlerin yapılması. Mesela bir router in routing tablosu okunabilir ve değiştirilebilirse yapılması gereken diğer testler de tespit edilebilir. Parent-Child ilişkisi
4- Aktif tarama (trafik analizi ile)

II. OGT Altyapısı

Tasarlanan sistem araştırıcılar ve sistem yöneticileri için bir güvenlik tarama altyapısı (Security Scanning Framework) olmakla birlikte, benzer ticari ve açık kaynak kodlu sistemlerin genelde maruz kaldığı;

- 1-Hızlı Tarayamama
- 2-Taranılan sisteme göre pluginleri yönetememe
- 3-Her seviyede tarama yapamama (Host based ve Network based)
- 4-Sistem yöneticileri ve araştırıcıların rutin ve manüel yaptığı bir sürü görevi üzerlerinden alamama ve vakit kaybına sebep olma
- 5-Esnek bir geliştirme diline sahip olmama
- Sistem topolojisi ve envanter veritabanı ile ilişkisel bağın olmaması gibi problemleri çözmektedir



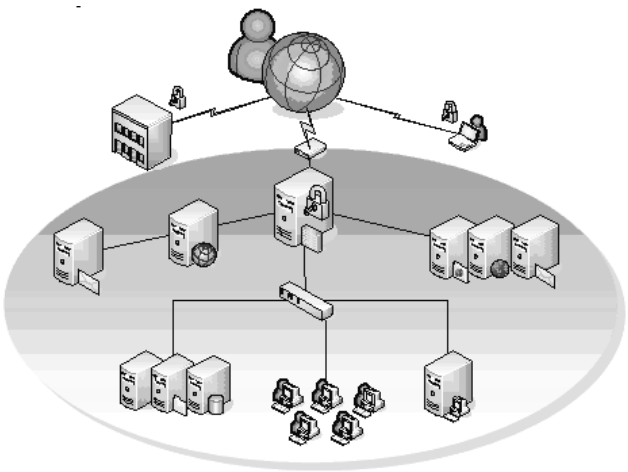
Şekil 1. OGT Altyapısı

Şekil 1. gösterilen OGT altyapısını açıklarsak:

1. Katman: Bu katman sistem için gerekli konfigürasyon parametrelerinin ayarlanması, kullanıcıdan yada API vasıtası ile diğer kaynaklardan girdileri okumak, kullanılacak plugin listeleri ve bunların yönetimi ve diğer modüllerin yönetimini yapar.
2. Katman: İkinci katman pluginlerin işletilmesi ve keşif/topoloji modülü ile entegrasyonu sağlar. Testlerin en kısa zamanda bitirilmesi, doğru testlerin uygulanması ve testlerin debug işlemlerini yönetir. Ayrıca kullanıcı tarafından girilin scriptlerin analizi ve yürütülmesi de yine bu katmanda olur. Bu katman topoloji modülü ile ilgili yönetimi de sağlar. Topoloji çıkarmak ve sistemleri marka, model tanımak ayrıca zor ve uzmanlık gerektiren bir iştir [5]. Doğru topolojiler pek çok ve yararlı bilgiler içerir. Topoloji modülü sistemi SNMP, WMI, TELNET, Servis Bannerları ile tarar ve tanır.

Topoloji modülü sayesinde sistem onbinlerce gereksiz plugini çalıştırmaktan kurtulur. Bunun ağ trafiği ve işlem gücü faturasın da ayrıca üzerinde çalışılabilecek kadar önemlidir. Sistem yöneticisi onbinlerce plugin seçmiş olsa bile bu katman topoloji modülü ile entegre olarak gereksiz testleri işletmez. Tabi ki saldırgan tarama durumunda bu işlemler yapılabilir ama ağ işletimi ve güvenliğinde optimizasyon temeldir. Birde güvenlik testlerinin çok sık yapılması gerekliliği (bazı durumlarda günde birkaç kere) göz önüne alınırsa topoloji katmanın önemi daha da anlaşılır.

Bu katman ayrıca sistem yöneticilerine politika tanıma imkânı tanır. Sistem yöneticileri sadece işletim seviyesi, sadece uygulama servisleri veya sadece güvenlik sistemlerini de taramadan geçirebilirler.



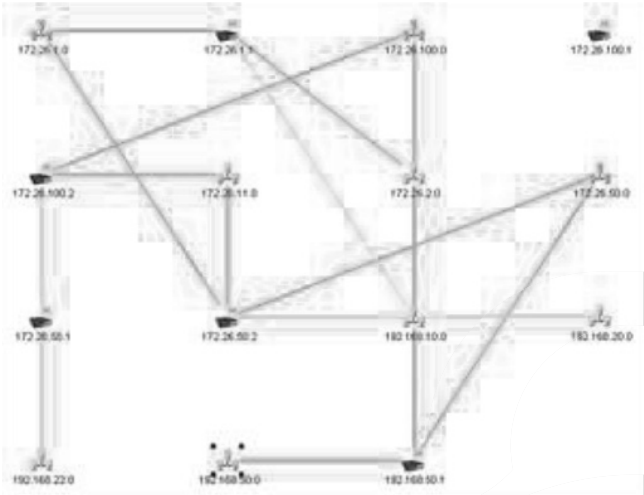
Şekil 2. Topoloji tabanlı güvenlik politikası kuralları tanımlama şablonu.

Şekil 2 topoloji ve keşif modülü tarafından ortaya çıkarılan sistemin lojik yapısıdır .Bu yapıda firewallar, antivirüsler, içerik tarayıcılar, serverlar, clientlar keşfedilip doğru bağlantı şekilleri ile bağlandığı için yukarıdaki politikalar uygulanabilir. Ayrıca her plugin eğer mümkünse tespit ettiği açıklığı yamamak üzere tasarlanmıştır. Mesela Windows işletim sistemin üretici firma Microsoft tarafından rapor edilen "Page File vulnerability" açığı otomatik olarak düzeltilmeye çalışılır, eğer bu otomatik yapılmazsa sistem yöneticilerine manüel yapılmak üzere çok fazla iş bırakır.
3. Katman: Bu katman test sonuçlarının kullanıcıya anlaşılabilir olarak raporlandığı katmandır. Bu katmanda çeşitli politikalar ve değerlendirme kriterlerine göre sonuçlar değerlendirilir, gerekirse her bir sonuç bir ağırlık olarak ele alınır toplan değerlendirme kullanıcıya değişik formatlarda sunulur. Bura verilerin analizi önemlidir. Bu katman raporları CSV, HTML, PDF veya TXT formatlarında üretilmekle birlikte bu sonuçlar bir veritabanına da kaydedilebilir.

III. OGT AVANTAJLARI

Sistem tasarlanırken pluginler guruplara ayrılarak tasarlandı. Bu guruplar depolama (storage), Güvenlik politikalar (security policies), Windows domain ayarları(domain settings), lokal ayarlar (local settings) ve şifrelerin kırılabilir olup olmamasını bakan grup. Bununla birlikte baştan beri tasarlanırken göz önünde tutulan modüler yapı ve plugin mantığı sayesinde yeni keşfedilen güvenlik problemleri için yeni pluginlerin hemen eklenmesi sağlanır. Ayrıca sistem yöneticilerinin kendi özel

ihtiyaçları için plugin yapısını kullanması da mümkün. Örnek vermek gerekirse regisrty yi düzenlemek için bir plugin yazmaları yeterli. Böylece binlerce makinede birden bu işlem otomatik olarak yapılacaktır. Sistem ayıca Keşif ve topoloji haritaları/sonuçları (Bkz. Şekil 3) ile politikaların entegrasyonunu sağlar.



Şekil 3. Örnek bir topoloji ve Keşif Haritası

IV. SONUÇ

Bu çalışmada otomatik güvenlik açığı tarama sistemi ile ağ yönetim kavramının en önemli konsepti olan ağ keşfi ve topoloji kavram ve uygulamaları birleştirilerek Güvenlik tarama ve analiz konsepti ile ağ yönetiminin sinerjik entegrasyonu sağlanmıştır. Bu çalışma ile ilgili prototip çalışmalar CBR yazılım [8] da yürütülmektedir.

KAYNAKLAR

[1] http://www.iss.net/products_services/enterprise_protection/vulnerability _assessment/ scanner_internet .php.
[2] http://www.eeye.com/html/Products/Retina/index.html.
[3] D. Farmer and E. H. Spafford, The COPS Security Checker System, in Proc. Summer Usenix Conference, Berkeley, CA, USA, pp. 165-170, 1990.
[4] Nessus, http://www.nessus.org.
[5] Ertuğrul Akbaş , Özlem Sak, "Hata Yönetimi için Zeki Keşif ve Topoloji Oluşturma Yöntemi ", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, pp 157-163, 9-11 Haziran,2005, Istanbul, Turkiye.
[6] http://www.winguides.com/tweak/.
[7] http://www.microsoft.com/technet/security/tools/mbsahome.mspx.
[8] http://www.cbr.com.tr