YEREL ALAN AĞLARINDA PAKET ANALİZİ İLE GÜVENLİK TARAMASI

Dr. Ertuğrul Akbaş
CBR Yazılım ve Danışmanlık Ltd. Şti.
Ertugrul.akbas@cbr.com.tr

ABSTRACT

In this paper we discuss local area based network security scanner with packet analyzing and a tool for investigating high level network events, Monitoring network activity has been a critical task for administrators. This project attempts to address visualizing and centralizing packet analyzing techniques with local based resources like the owner of the process etc.. by using information visualization techniques to display packet trace data. Dynamic filtering allows the scope of data being displayed to be modified in real time, enabling the visualization to scale to large data sets..

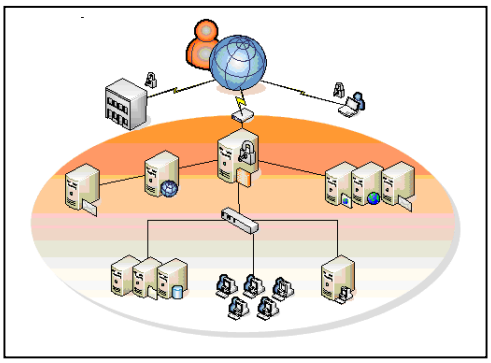
Key words: Network Security Scanner, Packet Analyzing, Sniffer, Data Visualization, SNMP

1. GİRİŞ

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. Ayrıca bu konuda pek çok akademik çalışma da mevcuttur [5,6,7,8,9,10]. Ayrıca paket analizi de bu anlamda en çok kullanılan yöntemlerden biridir [6,7,8,9,10]
Bu çalışmada dağıtık paket analizi ile merkezi değerlendirme ünitesi temelli bir güvenlik analizi yöntemi açıklanacak ve bu yöntem kullanılarak JAVA ile ürün gerçeklemesi anlatılacaktır.

2. PAKET ANALİZİ ALTYAPISI

Temel paket analizi araçlarında bile paketin kaynak adresi, kaynak portu, hedef adresi, hedef portu, protokolü, session ID, time frame gibi değerleri okunabiliyor. Ayrıca gelişmiş olanları flow diagram çıkarmak ve her türlü istatistikleri hesaplayabilmekteler. Bu çalışmada bu paket analizi yöntemleri dağıtık ortamda etmen temelli (Agent Based) bir yapı oluşturularak merkezi bir veri analizi ünitesinde analiz edilecektir (Şekil 1).



Şekil 1. Dağıtık Mimari

Burada etmenlerden toplanan paket bilgilerine ek olarak her paketle ilgili olarak merkezi ünitenin kullanacağı:

- Paketi oluşturan uygulama (Process)
- Uygulamanın sahibi (Owner)

Bu bilgiler ile birlikte

- Kaynak adresi
- Kaynak portu
- Hedef adresi
- Hedef portu
- Session ID
- Kaynak Mac Adresi
- Hedef Mac Adresi

Bilgileri de merkezi üniteye aktarılır. Bu bilgileri yerel ağlar için toplaması için CBR yazılım da Dr. Ertuğrul Akbaş ve ekibi tarafından geliştirilen Netjini [11] motorunun geliştirilmiş bir versiyonu kullanılmıştır.

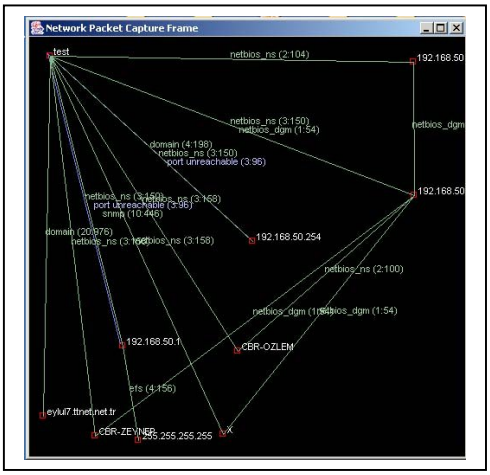
Paket uygulama ilişkisini almak Windows işletim sistemlerinde netstat –b komut satırıyla alınmakla birlikte platform bağımsız olması için bir java kod geliştirilmiştir. Ayrıca etmenlerdeki paket analizörleri iki farklı şekilde kullanılabilir.

- Yerel Alan Ağı temelli
- Etmen Temelli

Birinci yöntemde bütün ağı bir noktadan analizi yapılabilirken ikinci yöntemde filtreler kullanılarak bütün etmenlerde çalıştırılır ve makine bazlı paketler toplanır. Bu toplanan paketler daha sonra merkezi ünitede değerlendirilir.

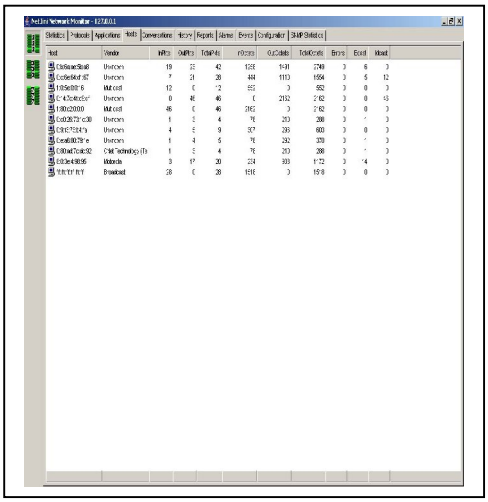
Analizdeki temel amaç: aynı uygulama ve/veya uygulamanın sahibinin ağda pek çok makineden aynı paketleri üretip üretmediğini analiz etmek. Bu

analizin dayandığı temel; aynı uygulamanın dağıtık bir şekilde her makineden aynı paketleri yayınlama ihtimallerine dayanmaktadır. Tabii ki network karakteristiği ile ilgili geçmiş bilgileri (History) temelli bir analiz söz konusudur. Şekil 2. de ki gibi network flow diagramları da ayrıca bu analizin önemli bir parçasıdır.



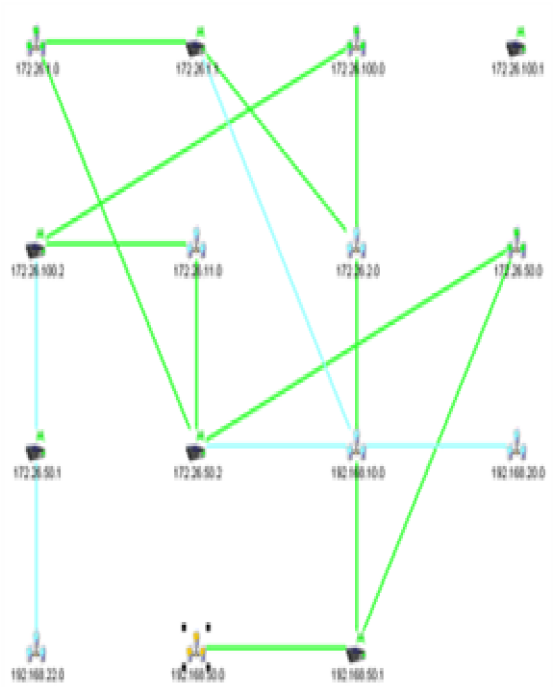
Şekil 2. Paket Haritası (IP seviyesi)

Etmenlerden toplanan bilgiler OSI katmanı 2,3,7 olarak ayrılmış bir şekilde merkeze iletilmekte Şekil 3.



Şekil 3. Paket Analizi (OSI katmanları)

Flow analizi yapıldıktan sonra güvenlik tehdidi analizi için kullanılacak diğer bir veri de topoloji bilgisidir. Sistem ayıca Keşif ve topoloji haritaları (Şekil 4) ile trafik akış diagramlarının birlikte analizini yapmak için sistem yöneticisine grafik ortamda bu haritaları oluşturup sunar. Bu haritaların



Şekil 4. Örnek bir topoloji ve Keşif Haritası

Oluşturulması ile ilgili literatürde pek çok çalışma mevcuttur. [5]

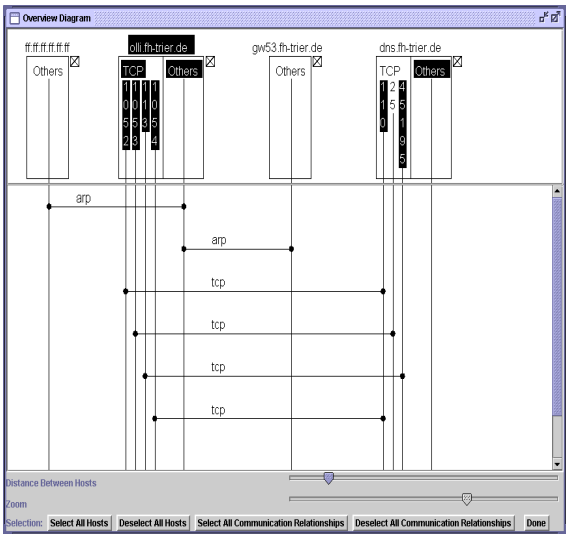
Topolojik haritaların güvenlik analizinde kullanılması ile ilgili de yapılan çalışmalar vardır[12]. Benzer algoritmalarla paket analizi temelli bir algoritmanın birleştirilmesi bu çalışmaya özgüdür.

Bu çalışmada kullanılan yöntem hem yeni hem de entegrasyon ve genişlemeye uygun olarak tasarlanmıştır.Böylece AR-GE altyapısını teknolojik gereksinimleri adreslemekte hem de araştırıcılara plugin olarak bu çalışmada kullanılan sniffer temelli algoritma yerine CISCO Netflow,JUNIPER J/FLOW ve benzeri pakat analizi algoritmalarını plugin olarak ekleyerek araştırma yapma ve teknoloji ihtiyaçlarına cevap verme şansı vermektedir.

Sistem bir resim bin kelimeye bedeldir felsefesini temel alarak flow analizi yapmakta ve bu analizi

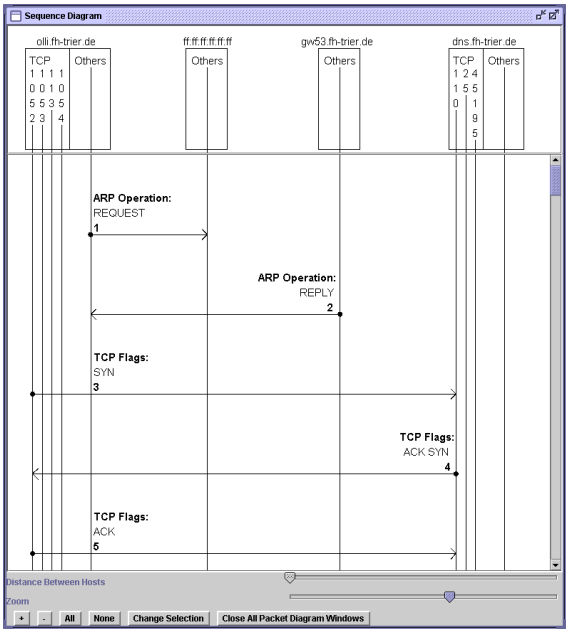
- Kaynak adresi
- Kaynak portu
- Hedef adresi
- Hedef portu
- Session ID
- Kaynak Mac Adresi
- Hedef Mac Adresi

görsel (Visual) olarak yapabilmekte Şekil [5]



Şekil 5. Paket Trafik Görselleştirme.

Bu görselleştirmenin esas amacı paket trafiğinde lokal analizler için okunabilir veriler resimler elde etmektir.Bu görselleştirmede en önemli görevi sequence diyagramları oynamaktadır şekil [6].



Şekil 6. Sequence Görselleştirme.

Paket analizi yorumlama merkezinde yapıldığı ve bilginin dağıtık bir altyapı ile toplanabildiği için trafik toplama ve analiz altyapısında NETFLOW ve SYSLOG protokolleri de kullanılabilir. Bu çalışmada kendi tasarladığımız ve geliştirdiğimiz motor kullanılmış olmakla birlikte veri işleme merkezi diğer kaynaklardan veri kabul edebilmesi mümkündür.

3. GERÇEKLEME

Paket analizi ile güvenlik taraması Dr. Ertuğrul Akbaş ve ekibi tarafından geliştirilen paket yakalama ve analiz motoru kullanılarak gerçeklenmiştir. Sistem Windows,Linux,Hp-Unix,Solaris,MAC gibi değişik işletim sistemlerinde veri toplayabilmek adına JAVA ile geliştirilmiş olup etmenler merkezi üniteye SQL bağlantısı kurarak verileri aktarmaktalar. Ayrıca dağıtık (highly distributed) bir yapı sağlamak amacı ile bütün etmenlere RMI tabanlı bir ara yüz ile uzak bağlantı kurulabilmekte ve ayrıca bütün etmenler de kendi aralarında bu ara yüz ile konuşabilmekteler.

Sistem gereksinimleri iki farklı kurulum (implementation) senaryosuna göre değişmektedir.

Senaryolar:

- Her etmen kurulduğu cihazın bilgilerini analiz merkezi üniteye gönderecek
- Her yerel alan ağında 1 etmen olacak ve port yönlendirme (port mirroring) ile analiz yapılacak

1. senaryoda etmen trafiği üreten uygulama ve uygulama sahibini aynı cihaz üzerinde çalıştığı için kolaylıkla tespit eder ve bu bilgileri de TAG olarak ekleyerek merkezi üniteye gönderir.

2. Seneryado etmen yerel alan ağında bir noktada çalıştığı için her cihaza ayrıca bu paketleri oluşturan uygulama ve sahibini algılamak için sorgu göndermesi gerekir.

Örnek: Domain yada LDAP ile aktif kullanıcıların sorgulanması ve uzak makşnada remote execute ile “netstat -b” çalıştırılması gibi.

Platform bağımsız paket yakalama motoru JPCAP [12] kullanılmıştır.

Topolojik haritalar için yine Java tabanlı Big:eye [13] kullanılarak oluşturulmuştur.

4. SONUÇLAR

AR-GE çalışmalarının teknolojik yenilik içermesi ve ürüne dönüşmesinin esas olduğuna inandığımızdan dolayı çalışmayı gerçeklemek ve gerçeklemenin sonunda ürün olabilecek bir altyapıya sahip olması hedeflerimizden biriydi. Bununla birlikte bu çalışmada önerilen yöntemin yeniliğiyle birlikte faydalarını özetlemek gerekirse:

- Ağ Yöneticileri için:
  - Güvenlik Analizi
    - Paletler değişti mi?
    - Aynı process birden fazla makineden aynı paketi üretiyor mu
  - Performans Analizi
  - Cevap Verme Zamanlarının Optimizasyonu
- Yazılım Geliştiriciler
  - Dağıtık Mimari Analizi
    - RMI
    - CORBA
    - DCOM
    - J2EE
- Öğreticiler ve Öğrenciler
  - Paket oluşumu ve akışı gerçek zamanlı görme ve kendileri paket oluşturup onun fotografını cekme

Bir resim bin kelimeye bedel

Bu çalışmanın devamında SYSLOG temelli pakaet analizleri de sisteme entegre edilebilir.

Sistemin plugin yapısı trafik analizinin NETFLOW ve Syslog ile trafik bilgisine almaya ve bunları işlemeye müsait biçimde tak çıkar tasarlandığı için genişlemeye ve -hibrid – bir yapıda olduğu için genişletilebilir.

Projede tasarım ve gerçekleme gerçek ortamda kullanım ve yük altında sistemin dayanıklı ve güvenilir sonuçlar üretmesini de hedeflemiştir. Bu çalışmada kullanılan netjini, jpcap ve dağıtık mimari altyapısı RMI ve SQL 92 temelli veri güncelleme sadece akademik olarak değil pek çok üründe de kullanılarak kendilerini kanıtlamıştır. Dolayısı ile altyapı ve motor üzerine plugin olarak ve iyileştirme ve yenilik olarak gelen özellikler bu altyapıyı genişletmiştir.

KAYNAKLAR

[1] http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet php

[2] http://www.eeye.com/html/Products/Retina/index.htm

[3] D. Farmer and E. H. Spafford, The COPS Security Checker System, in Proc. Summer Usenix Conference, Berkeley, CA, USA, pp. 165-170, 1990. 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] Analysis Console for Intrusion Databases (ACID). downloadable at: http://acidlab.sourceforge.net/, cited December 13, 2004.

[7] Ronald M. Baecker, William Buxton, Jonathan Grudin, and Saul Greenberg. *Readings in Human-Computer Interaction: Toward theYear 2000*. Morgan Kaufmann Publishers, second edition, 1995.

[8] Robert Ball, Glenn A. Fink, and Chris North. Home-centric visualization of network traffic for security administration. In *VizSEC/DMSEC'04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 55–64. ACM Press, 2004.

[9] R.A. Becker,W. S. Cleveland, and M. J. Shyu. The Visual Design and Control of Trellis Display. *Journal of Computational and Statistical Graphics*, 5:123–155, 1996.

[10] http://www.cs.ubc.ca/~spark343/NAV.pdf

[11] Ertuğrul Akbaş "Topolojik Bağımlı Otomatik Sistem Güvenliği Tarama Yöntemi", ISC'07 Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık,2007, Ankara, Turkiye.

[12] JPCAP-http://jpcap.sourceforge.net/

[13] www.cbr.com.tr