Güvenlik Amaçlı SNMP Walk ile Merkezi Loglama Yazılımı

Gökhan Akın[1], Uğur Sezer[2]

[1] İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, İstanbul

[2] İstanbul Teknik Üniversitesi, Telekomünikasyon Mühendisliği Bölümü, İstanbul

gokhan.akin@itu.edu.tr, ug.sezer@gmail.com

Özet: SNMP destekleyen cihazlardan istenen aralıklar ile log alınmasını sağlamak amacı ile geliştirilmiş olan "WalkBee" isimli yazılımın detayları anlatılmaktadır. Bu yazılım ile özellikle merkezi üçüncü katman anahtarlama cihazının ARP tabloları kayıt altına alınıp 5651 yasasının gereği daha rahat sağlanabilinmektedir.

Anahtar Sözcükler: ARP, SNMP, walk, IP, MAC, Ağ, Güvenlik, WalkBee.

Abstract: The details of software that receives log from the equipments that supports SNMP, developed with the name of "WalkBee" in a desired interval are explained. With this software, especially the central layer 3 switching device's ARP table can be easily recorded. This would help to provide the 5651 law requirement.

1. Giriş

Günümüzde yasal sorumluklardan dolayı ağ yöneticilerine, belirli tarihte bir IP adresini kimin kullandığı sorusu sık sık sorulmaya başlanmıştır.[1] Bu sebeple ağ yöneticileri çeşitli teknikler kullanarak ağ ile ilgili bilgileri kayıt altında tutmak durumundadır.

2. Kullanıcı Denetimi

Kullanıcı denetimini iki farklı teknik ile ele alabiliriz. Bunlardan ilki kullanıcı adı bazlı tespit teknikleridir. 802.1x [2] protokolü ve Proxy/Captive Portal uygulamaları bu amaçla günümüzde kullanılabilen tekniklerdir.

Kimlik denetimi amaçlı diğer teknikler de ise konum belirlemesini MAC adresi güvenliği ve IP adresi güvenliği teknikleri sağlamaktadır. Yaygın kullanılan MAC adresi güvenliği ve 802.1x kimlik denetim teknikleri incelendiğinde tek başlarına yetersiz kaldıkları gözlenmektedir.

3. 802.1x Ağ Kimlik Denetimi Protokolü

802.1x ağ kimlik denetimi protokolü ile kullanıcı ağa dahil olmadan kimlik denetimine tabi tutulmaktadır.

Bu sayede ağa sadece yetkili kullanıcıların erişmesi sağlanmaktadır. Kullanıcı denetimi dışında hangi kullanıcının hangi adres ile ağa eriştiği de kayıt altında tutulmaktadır. Buda ilerde oluşan bir sorgulamada ağ kaynaklarına erişen kullanıcının belirlenmesini sağlar.

Ancak 802.1x kimlik denetimi protokolü OSI'ye göre ikinci katman protokolüdür ve kimlik denetimi sırasında oluşan logda sadece MAC adresi bilgisi bulunur ve kaynak MAC adresi bilgisi başka bir ağa ulaşılması durumunda taşınmaz.

Zaten ağ yöneticilerine gelen sorgulamalar IP adresi bazlıdır. Buda 802.1x protokolünün tek başına yetersiz kaldığını göstermektedir.

4. MAC Adresi Bazlı Güvenlik

MAC adresi bazlı güvenlik uygulaması kullanıcı takibinde uzun zamandır kullanılan ve yaygın olan bir tekniktir. Bu sistemde kullanıcıların MAC adresleri kullanılan anahtarlama cihazına sabitlenmektedir. Günümüzde MAC adresleri kolaylıkla değiştirilebilmektedir. Buda ilgi anahtar cihazı portundan başka bir kullanıcının da ağa dahil olabilmesine olanak vermektedir. Ancak en azından kullanıcının bağlantı yaptığı fiziksel konum belli olacağından yapılacak incelemeler sonrasında yinede sonuca gidilebilir.

Burada sorun MAC adresinin değiştirilebilir olmasından çok IP adresinin değiştirilebilmesidir. Kullanıcı MAC adresini değiştirmeyip IP adresini başkasına tahsis edilmiş olan bir IP adresi ile değiştirebilir. Sistem buna karşı bir çözüm getirmemektedir. 802.1x sistemindeki gibi, burada sadece ikinci katman adresine göre yapılan güvenlik ile kullanıcının konumunu belirlemek mümkün olmamaktadır.

5. IP Adresinin Kayıt Altına Alınması İçin Kullanılabilecek Teknikler

Gerek 802.1x gerekse MAC adresi güvenliği tekniklerini kullanıcı takibinde etkin kılabilmek için ağ yöneticisinin ilgili IP adresinin sorgulanan zaman aralığında hangi MAC adresi tarafından kullanıldığını belirlenmesi gerekmektedir.[3] Bunun için iki farklı teknik kullanılabilir.

a- DHCP logunun incelenmesi
b- Merkez yönlendircinin (3. Katman anahtarın) ARP tablosunun loglanması

a- DHCP Logunun İncelenmesi

İstemcilere otomatik IP adresi verilmesini sağlayan DHCP[4] servisi, logunda hangi IP adresinin hangi MAC adresine atandığı bilgisini de barındırmaktadır. Bu logun yardımı ile istenen IP adresi bilgisine ulaşma imkanı bulunmaktadır. Ancak kullanıcı DHCP sunucusundan IP adresi almak yerine kendisi IP adresi atayabilir. Bu durumda kullanıcın takibi mümkün olamayacaktır.

Buna çözüm olarak güncel anahtarlama cihazlarında "DHCP Snooping" ve "Source Guard"[5] özellikleri ile kullanıcının sabit IP adresi ataması engellenebilir. Ancak bu özellikleri ağdaki bütün anahtarlama cihazlarının desteklemesi gerekir. Ayrıca ağ yöneticisi çeşitli durumlarda otomatik IP adresi sistemini kullanmakta istemeyebilir. Buda loglamayı engelleyecektir.

b- Yönlendiricinin ARP Tablosunun Loglanması

Diğer çözüm ise merkez 3.katman cihazının ARP tablosunun belirli sıklıklarda kayıt altına alınmasıdır. Başka bir ağa ulaşmak isteyen bütün kullanıcıların IP ve MAC adreslerinden oluşan ARP kayıtları bu cihazda oluşur. Bu çözümde otomatik veya sabit IP adresi kullanan bütün kullanıcıların bilgileri loglanmış olur.

Güncel yönlendiricilerin hepsi SNMP (Simple Network Management Protocol) [6] protokolünü desteklemektedir. ARP tablosu birden fazla satırdan oluşacağı için SNMP sorgusunda SNMPWalk uygulaması kullanılır. Bu uygulama kullanılarak herhangi bir betik dili (PHP,Perl..vs) ile gereken loglamayı yapabilecek bir program geliştirilebilir. İstanbul Teknik Üniversitesi dahilinde PHP dili ile geliştirilirmiş bir betik ile uzun bir süredir bu loglama yapılmaktadır.

İTÜ dahilde kullanılan sistemde yazılan betiğin çalışması için SNMP Kütüphanesi ve PHP yapılandırılması yapılmış bir sunucu kullanılmaktadır. Sunucuda istenen aralıkta betiğin çalışması için Crontab uygulaması devreye alınmıştır. Başka bir betik ile de kayıt altına alınan logların daha az yer kaplaması için sıkıştırılarak arşivleme işlemi yaptırılmaktadır.

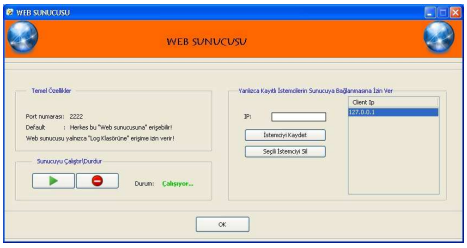
Bunun yanı sıra kayıt altına alınmış ARP kayıtlarının ihtiyaç halinde kolayca incelenebilmesi için bir web sunucusu yapılandırılmış, yetkili kullanıcılar uzaktan bu verilere ulaşabilir hale gelmişlerdir. Yapılan çalışma dahilinde bütün bu yapılandırmaya gerek kalmadan aynı işlemleri gerçekleştirebilecek bir uygulama geliştirilmiştir.

6. Geliştirilmiş olan SNMP Walk kullanan Merkezi Loglama Yazılımı

WalkBee[7] adı ile geliştirilmiş olan yazılım Java programlama dili ile geliştirilmiştir ve işletim sistemlerinden bağımsızdır. Programın geliştirme aşamasında, ücretsiz olan 'AdventNet SNMP' kütüphanesinden yararlanılmıştır. Geliştirme ortamı olarak Eclipse ve grafik arayüzü tasarımı için NetBeans IDE kullanılmıştır. Program SNMP versiyon 2[8] ile istenen MIB değeri için SNMP Walk sorugusu yapabilmektedir.

Şekil 1. Yazılımın Ana Penceresi

Program, ana penceresinde bulunan, cihazların kayıtlı olduğu tablodaki 3. katman cihazlarına bir döngü içerisinde, en üstte yer alan cihazdan başlayarak sırayla SNMP Walk sorgusu yapmaktadır. Cihazlardan ayrı ayrı elde ettiği bu bilgileri bir text dosyası içine yazıp, döngü bittiği anda ise dosyayı kapatır. Bu aşamadan sonra program bir sonraki sorguya kadar bekleme halinde kalır.



Şekil 2. Web Sunucusu Ayarları

SNMPwalk sorgusu sonucunda elde edilen verilerin ve cihazların durumunun uzaktan izlenebilmesi amacıyla, program içerisinde 2222. porttan hizmet veren bir adet web sunucusu bulunmaktadır. Bekleme durumunda program kendi web sunucusuna gelen isteklere yanıt vermeye devam eder.

Şekil 3. Web Ayayüzü

Program, kullanıcı tarafından belirtilen aralıklarda periyodik olarak SNMPwalk sorgusu yapacak şekilde tasarlanmıştır. Program aylarca, durmadan çalışacak şekilde belirtilen periyotlarda cihazlara sorgu yapmaya devam edebilecek özelliğe sahiptir.

Şekil 4. Sorgu Periyodu Ayarı

SNMP Walk sorgusu sonucunda elde edilen verilerin sistemde daha az yer kaplaması hedeflenmiştir. Bu amaçla her 24 saatte bir, program o gün SNMP Walk sorguları sonucunda elde edilen text dosyalarını, günün tarih bilgisini içeren bir isim ile zip uzantılı olarak arşiv klasörüne sıkıştırma işlemini uygulayarak kaydeder.

7. Sonuç

5651 sayılı kanun getirdiği sorumluluklar çerçevesinde ağ yöneticileri ağ kaynaklarının kullanımını daha sıkı takip altına almak zorundadır.

Bu amaçla kullanılan 802.1x ve MAC adresi güvenliği tek başına yetersiz olan uygulamalar oldukları çok açık görülmektedir. Bu uygulamaların yeterli olabilmesi için kullanıcının IP ve MAC adreslerinin de ayrıca kayıt altına alınması gerekmektedir.

Bu amaçla kullanılabilecek DHCP sunucusu kayıtları kullanıcılar sabit IP kullanmaları durumunda yine yetersiz kalmaktadır.

Diğer çözüm olan üçüncü katman yönlendiricin ARP tablosunun kayıt altına alınması ise her tür IP dağıtım sisteminde kullanılabilmektedir. Ağ yöneticilerinin gün içinde belirli periyotlar da bir bu ARP tablolarının kayıt altına almaları ağ takibini çok kolaylaştıracaktır. Çalışma dahilde geliştirilmiş olan WalkBee yazılımı da açık kaynak kodlu olarak dağıtılmak amacı ile geliştirilmiştir. Kısaca sadece bu yazılım ile ARP tablosunun kayıt altına alınması ve daha sonra bu verilere erişilebilmesi kolaylıkla sağlanabilmektedir.

Son olarak bu yazılımda kullanılsa NAT kullanan ağlarında NAT tercüme (translation) tabloları kesinlikle ayrıca bir yazılım ile loglanmalıdır. Aksi taktirde ağ dışına hedefli hiçbir olayın kaynağı tespit edilemez.

Kaynaklar

[1] Akın G., Ketenci S., 'Kampüs Ağlarında Aranan Kullanıcıların Tespiti', Akademik Bilişim 2009, Urfa

[2] Akın G.,Yüce H., Demir H. 'FreeRADIUS - LDAP ile Kimlik Denetimi Klavuzu', Ulaknet Çalıştayı, Mayıs 2008

[3] Karaarslan,E., Akın G., 'Kurumsal Ağlarda Zararlı Yazılımla Savaş', Akademik Bilişim 2008, Çanakkale

[4] Droms R., 'Dynamic Host Configuration Protocol', RFC 2131, IETF, Mart 1997.

[5] Akın G., 'DHCP Servisine Yeni Bir Bakış', INET-TR 2008, Ankara

[6] Case J., 'Simple Network Management Protocol', RFC 1157, IETF, Mayıs 1990.

[7] Akın G., 'WalkBee Resmi Web Sayfası', Aralık 2009, http://www.walkbee.net

[8] Case J., 'Introduction to Community-based SNMPv2', RFC 1901, IETF, Ocak 1996.