INET-TR 2009 BİLGİ ÜNİVERSİTESİ / İSTANBUL

Güvenlik Amaçlı SNMP Walk ile Merkezi Loglama Yazılımı

Gökhan AKIN
İTÜ/BİDB Ağ Grubu Başkanı - ULAK/CSIRT

Uğur SEZER
İTÜ Telekomünikasyon Mühendisliği

İTÜ/BİDB
Bilgi İşlem Daire Başkanlığı

Giriş

Günümüzde yasal sorumluklardan dolayı ağ yöneticilerine belirli tarihte bir IP adresini kimin kullandığı sorusu sık sık sorulmaya başlanmıştır.
Örnek: 10.0.0.1 adresini kim kullandı?
(Acil Cevap)

(Alıntı: Kampüs Ağlarında Aranan Kullanıcıların Tespiti
Akademik Bilişim 2009
Gökhan AKIN/Sınmaz KETENCİ)

Kullanıcı Denetimi

1- Kullanıcı adı bazlı tespit -

-**802.1x kimlik denetimi****

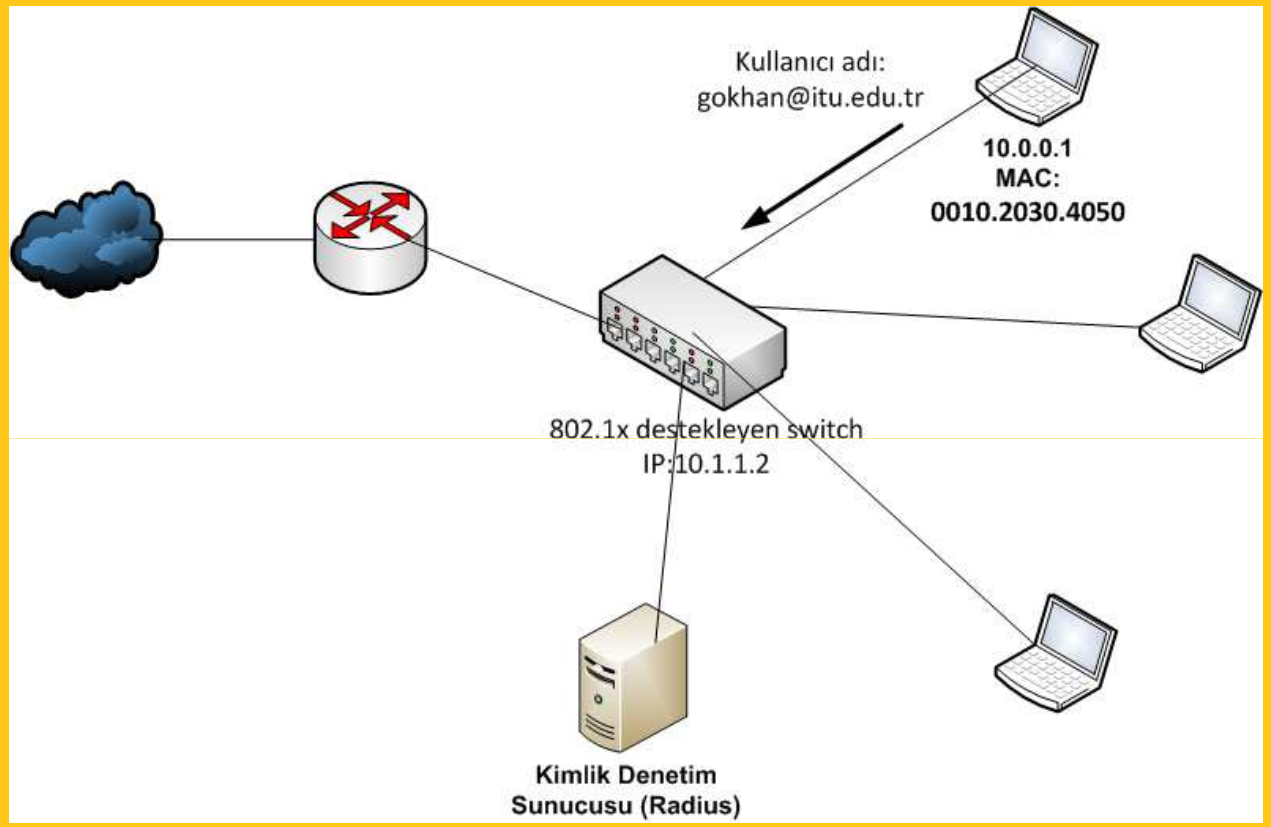
-Proxy-Captive Portal Uygulamaları

2- Kullanıcının ağa dahil olduğu yerin belirlenmesi ile tespiti

- MAC Güvenliği**

- IP Güvenliği

802.1x Kimlik Denetimi



Kullanıcı ağa geçerli kullanıcı adı ve şifresi ile dahil olur.

802.1x Kimlik Denetimi Sorunu

Free Radius Logu:

Fri Jan 9 00:27:17 2009

Packet-Type = Access-Request

User-Name = “gokhan@itu.edu.tr"

Framed-MTU = 1400

Called-Station-Id = "001f.2232.0050"

Calling-Station-Id = **"0010.2030.4050"**

Service-Type = Login-User

Message-Authenticator = 0xc18b0072d5e598015fbf9b8563db1ed9

EAP-Message =

0x0201001d01616e6f6e796d6f757340756c616b62696d2e676f762e7472

NAS-Port-Type = Wireless-802.11

NAS-Port = 2237

NAS-IP-Address = 10.1.1.2 **<- SADECE SWITCH’IN IP ADRESİ**

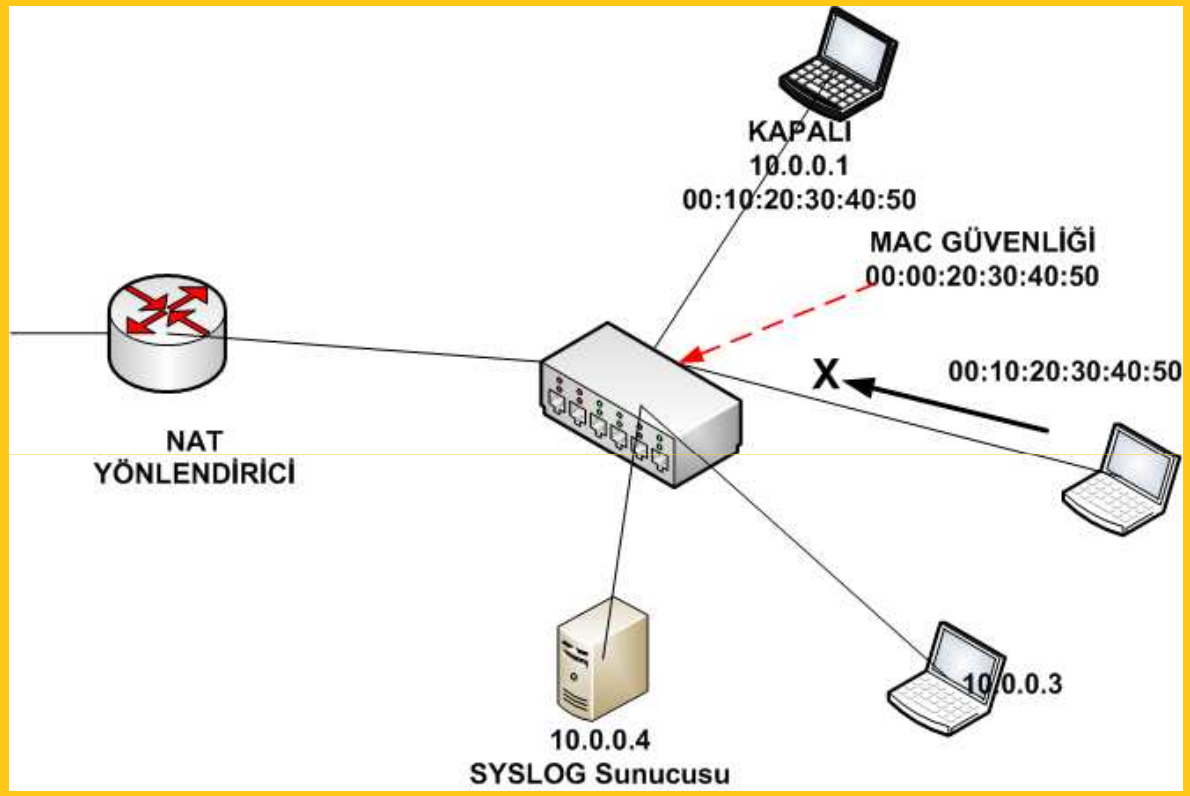
NAS-Identifier = “BOCEK"

Fri Jan 9 00:27:17 2009

Packet-Type = Access-Accept

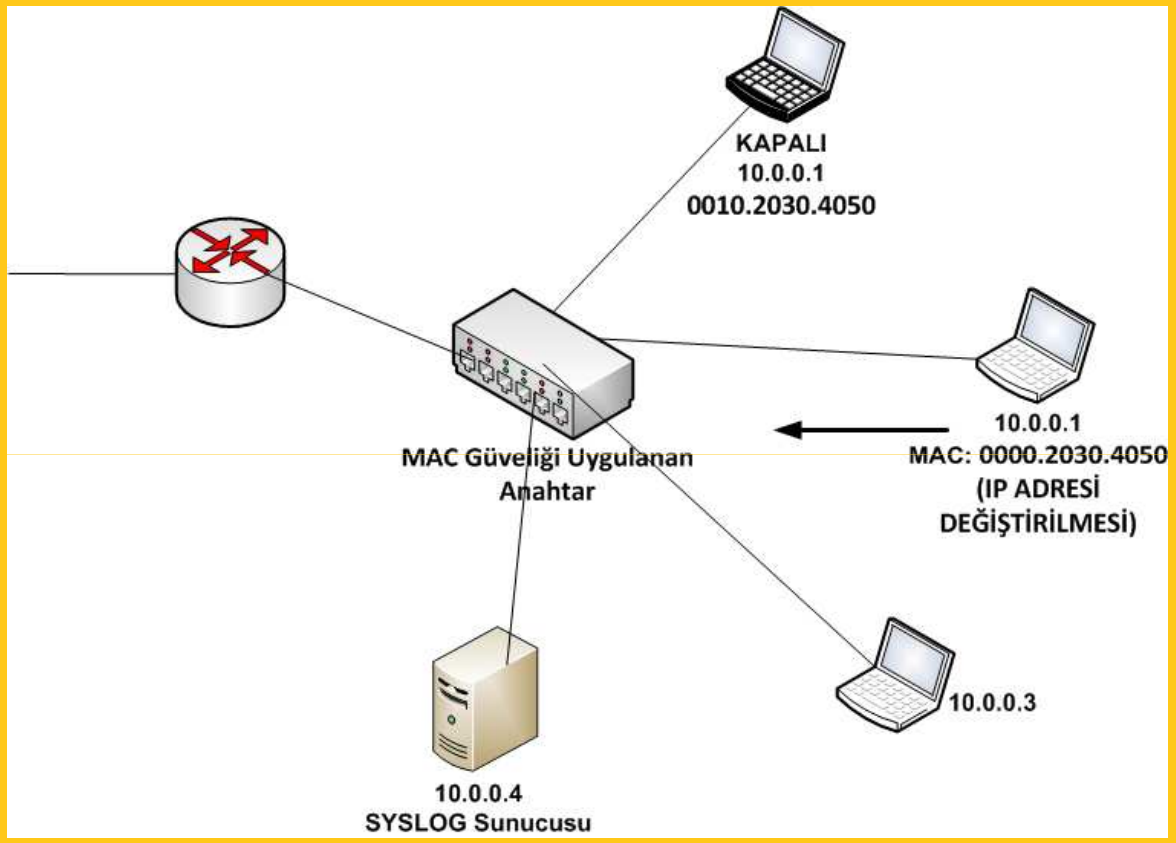
Reply-Message = "Hello, %u"

MAC Adresi Güvenliği



Kenar anahtar cihazında ağ erişimi yapabilecek MAC adresleri sabitlenir.

MAC Adresi Güvenliği Sorunları



Kullanıcı MAC adresini değiştirmese de IP adresini değiştirebilir.

Çözümler

İlgili IP adresinin o zaman aralığında hangi MAC adresini kullandığının takip edilmesidir.

Bunun için çözüm:

1- DHCP logunun incelenmesi

2- Merkez 3. katman anahtarların ARP tablosunun loglanması

Çözüm 1: DHCP Logu

Linux ISC-DHCP ile Tutulan DHCP logunun örneği:

 # DHCP logu /var/log/messages dosyasınında tutulmaktadır.

tail -f /var/log/messages | grep dhcpd | grep 10.0.0.1

Feb 1 20:19:13 linux-box dhcpd: DHCPDISCOVER from 00:10:20:30:40:50 via eth0

Feb 1 20:19:14 linux-box dhcpd: DHCPOFFER on 10.0.0.1 to 00:10:20:30:40:50 (yuce) via eth0

Feb 1 20:19:14 linux-box dhcpd: DHCPREQUEST for 10.0.0.1 (10.0.0.50) from 00:10:20:30:40:50 (yuce) via eth0

Feb 1 20:19:14 linux-box dhcpd: ***DHCPACK*** *on* ***10.0.0.1*** *to* ***00:10:20:30:40:50*** *(yuce) via eth0*

Çözüm 1: DHCP Logu Sorunları

Kullanıcı sabit IP adresi kullanırsa DHCP logundan takip edilemez.

DHCP Snooping ve Source Guard ile kullanıcının DHCP dışında IP adresi verilmesi engellenebilir.

Sorun:

1- Pahalı Switch

2- Kullanıcıların DHCP'den IP adresi alması mecburi

Çözüm 2: Merkez Yönlendirici ARP Tablosunun Loglanması

Başka bir ağa giden her istemcinin IP ve MAC adresinden oluşan ARP kayıdı Merkez yönlendiricide oluşur.

Bu kayıt loglanarak istenen IP ve MAC adresi eşleşmesi elde edilebilir.

Çözüm 2: Merkez Yönlendirici ARP Tablosunun Loglanması

Yönlendiricilerden ARP logunu almak için SNMP Protokolü kullanılabilir.

Cisco cihazlarda SNMP ile alınmış olan ARP logu görüntüsü:

ipNetToMediaPhysAddress.99.10.0.0.1 = STRING: ***0:00:20:30:40:50***

ipNetToMediaPhysAddress.99.10.0.0.2 = STRING: *0:1E:0:0:0:D5*

ipNetToMediaPhysAddress.99.10.0.0.4 = STRING: 0:1.20:44:60:ee

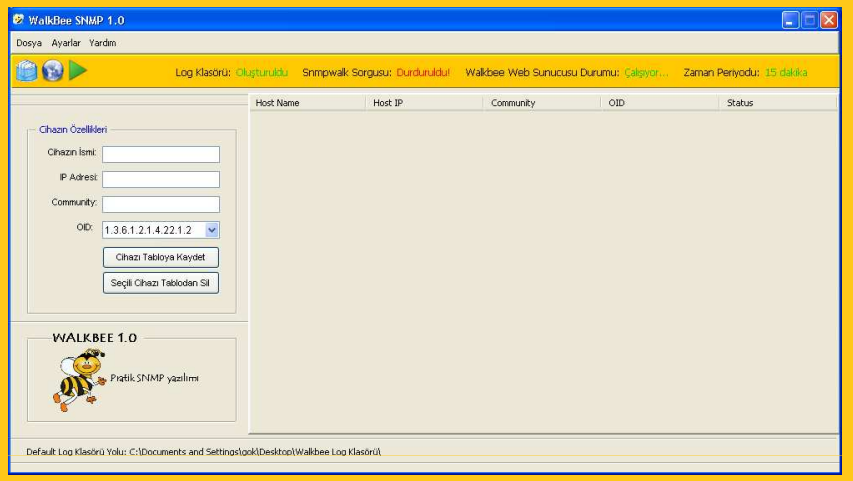
Çözüm 2: Merkez Yönlendirici ARP Tablosu Loglama Sorunu

Bunun için İ.T.Ü.'de kullanılan sistem:

1- PHP, SNMP, Web sunucusu kurulmuş bir Linux sunucu.
2- SNMP logunun alınabilmesi için PHP ile yazılmış bir betik.
3- Belirli zamanlarda logu arşivleyen başka bir betik.
4- Log'lara kolay erişebilmesi için Web sunucusu yapılandırması.
5- Log'lamanın ve arşivlemenin yapılabilmesi için Crontab'da gereken yapılandırma.

Özetle uygulanması zor bir sistem.

Merkez Yönlendirici ARP Tablosu Çözümü: WalkBee

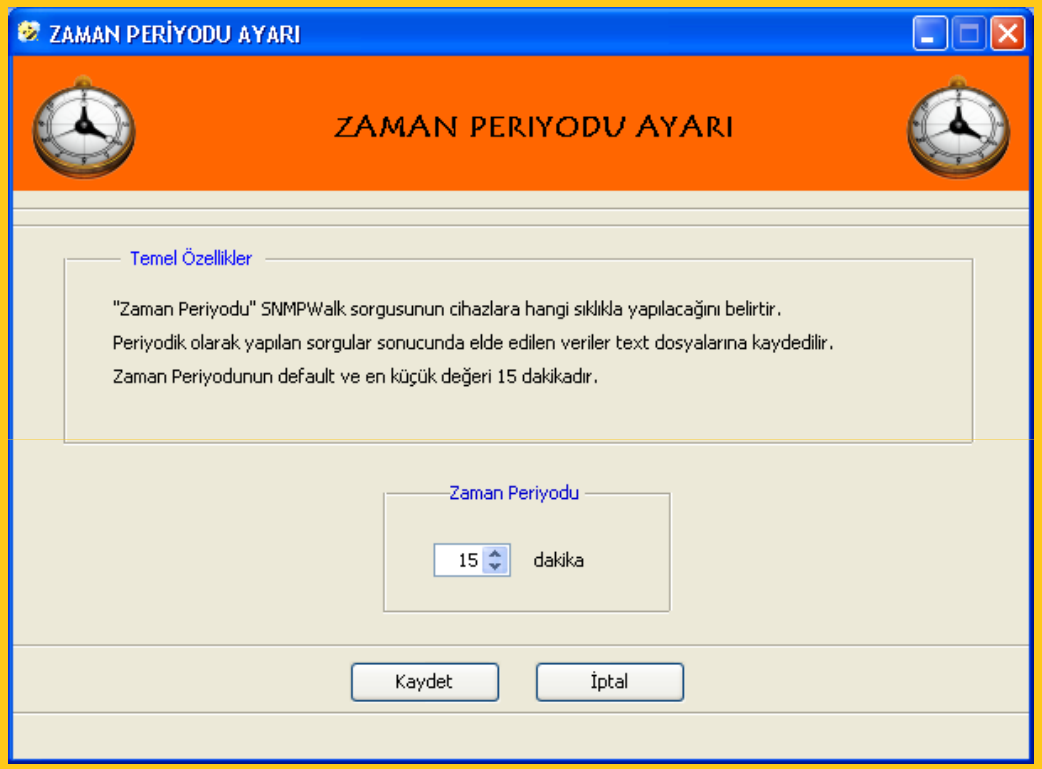


Bu amaçla geliştirdiğimiz SNMP Walk loglama yazılımı "WalkBee" Java programlama dili ile geliştirilmiş bir yazılımdır ve işletim sistemlerinden bağımsızdır.

Programın geliştirme aşamasında, GPL lisanslı 'AdventNet SNMP' kütüphanesinden yararlanılmıştır.

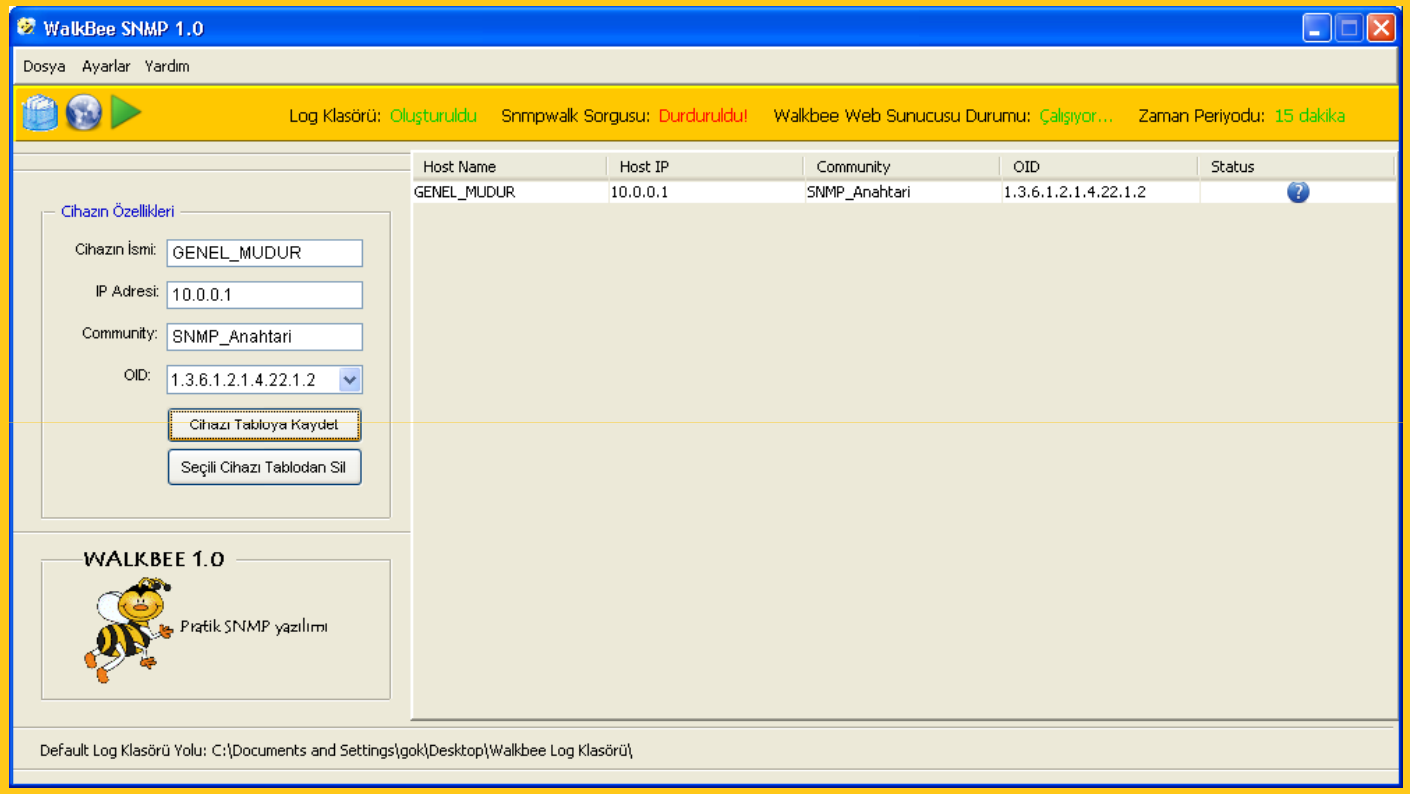
İTÜ/BİDB Bilgi İşlem Daire Başkanlığı

Zaman Periyodu Ayarı



Varsayılan olarak 15 dakika aralıklarla SNMP sorgusu ile veri toplayabilmektedir ve bu süre değiştirilebilir.

Cihazların Tanıtımı (1)

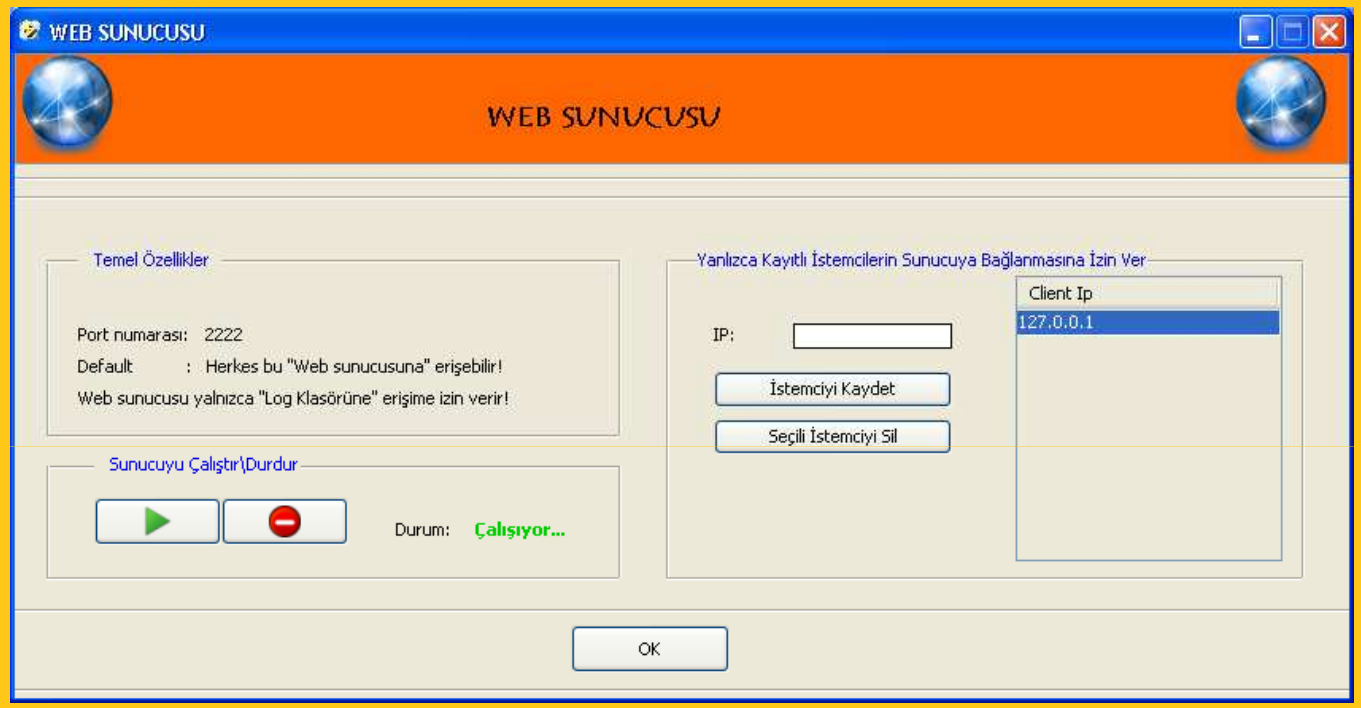


Cihazın adı, IP adresi ve SNMP anahtar kelimesi, OID Sorgulanacak SNMP bilgisini yazılıma belirtilir.

Cihazların Tanıtımı (2)

Birden fazla yönlendiricinin bilgileri programa girilebilir.

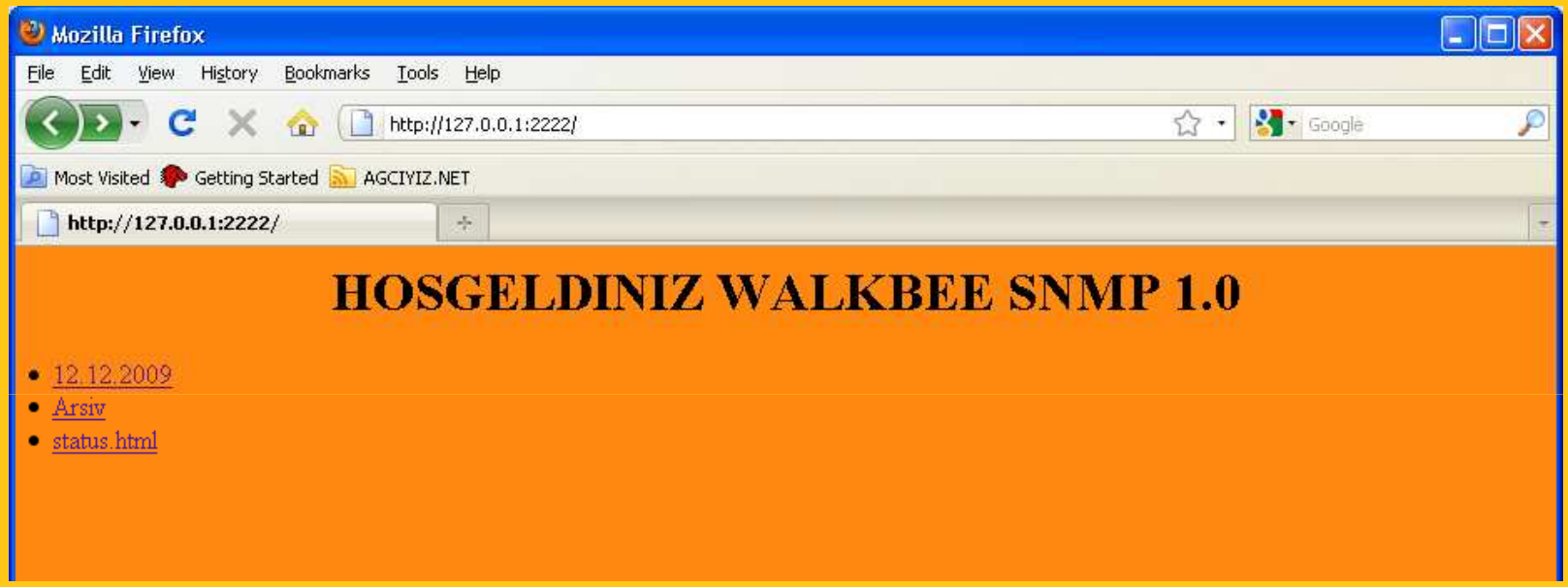
Web Sunucusu Ayarları



Programın içinde 2222. port'tan hizmet veren bir web sunucusu bulunmaktadır.

Web erişimi için IP bazlı güvenlik yapabilmektedir.

Web Arayüzü: Ana Sayfa

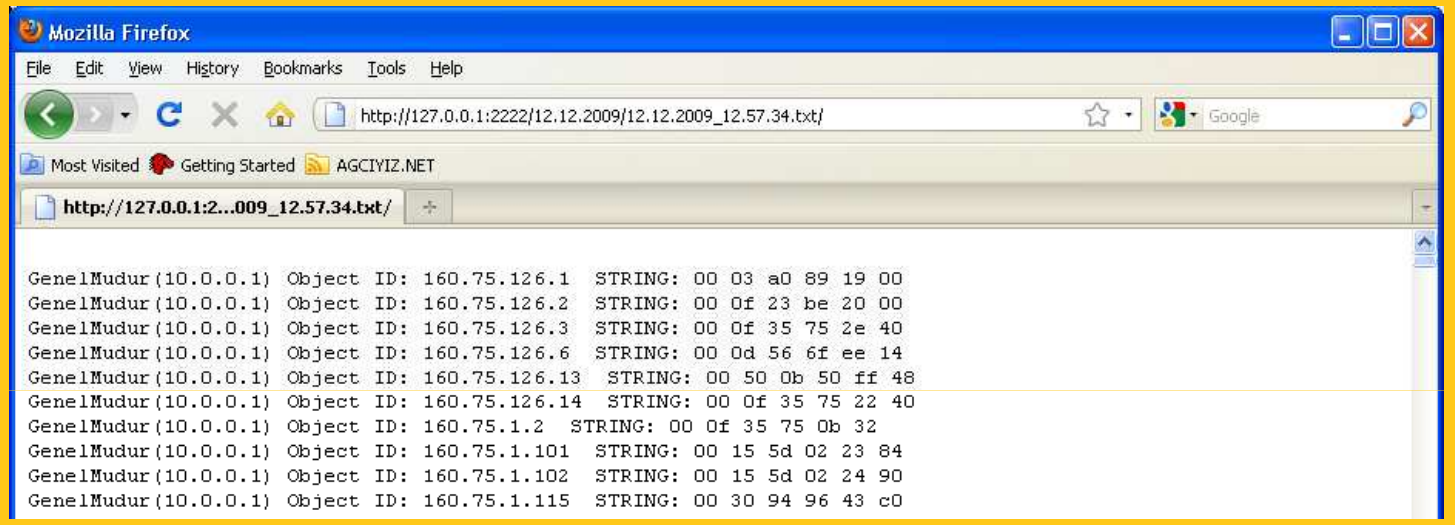


Kayıtların uzaktan kontrolü için WalkBee'nin web arayüzü kullanılabilir.

Web Arayüzü: Günlük Kayıtları

Günlük kayıtların görüntüsü…

Web Arayüzü: ARP Tablosu

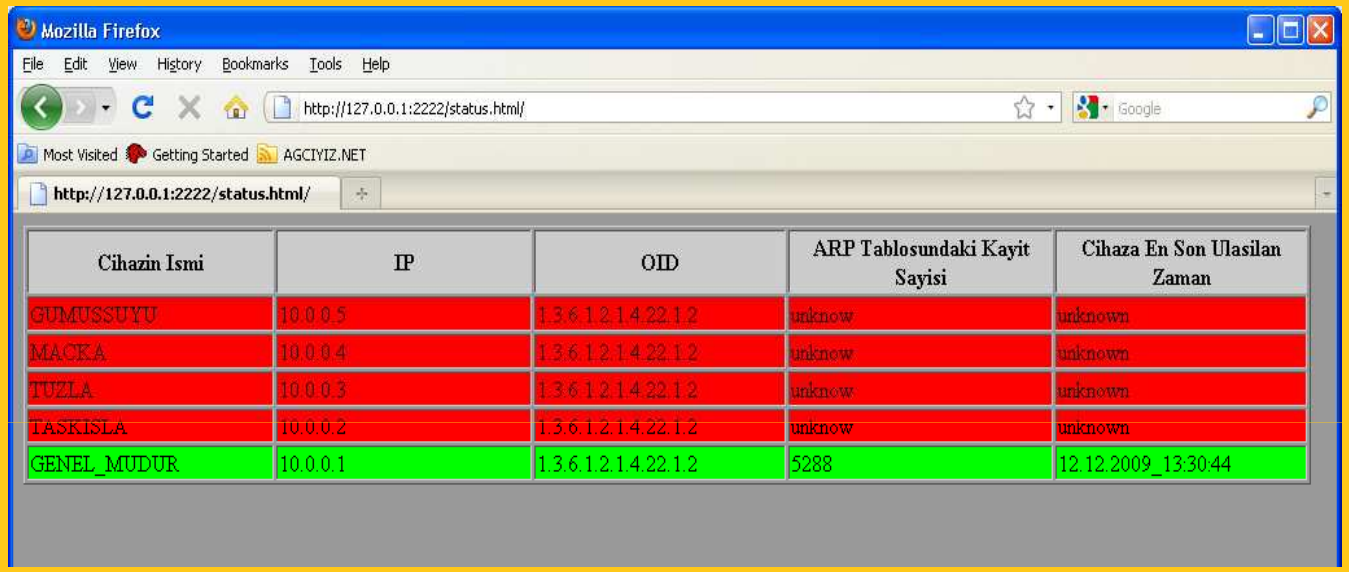


SNMP logu Web arayüzü üzerinde incelenebilir.

Arşivlenmiş Kayıtlara Ulaşım

Saat 24:00'de günlük dosyalar sıkıştırılıp arşiv klasörüne kaldırılır.

Web Arayüzü: Durum Tablosu



Cihazin Ismi	IP	OID	ARP Tablosundaki Kayit Sayisi	Cihaza En Son Ulasilan Zaman
GUMUSSUYU	10.0.0.5	1.3.6.1.2.1.4.22.1.2	unknow	unknown
MACKA	10.0.0.4	1.3.6.1.2.1.4.22.1.2	unknow	unknown
TUZLA	10.0.0.3	1.3.6.1.2.1.4.22.1.2	unknow	unknown
TASKISLA	10.0.0.2	1.3.6.1.2.1.4.22.1.2	unknow	unknown
GENEL_MUDUR	10.0.0.1	1.3.6.1.2.1.4.22.1.2	5288	12.12.2009_13:30:44

Erişilen cihazlar ve durum raporları anlık olarak gözlenebilir.

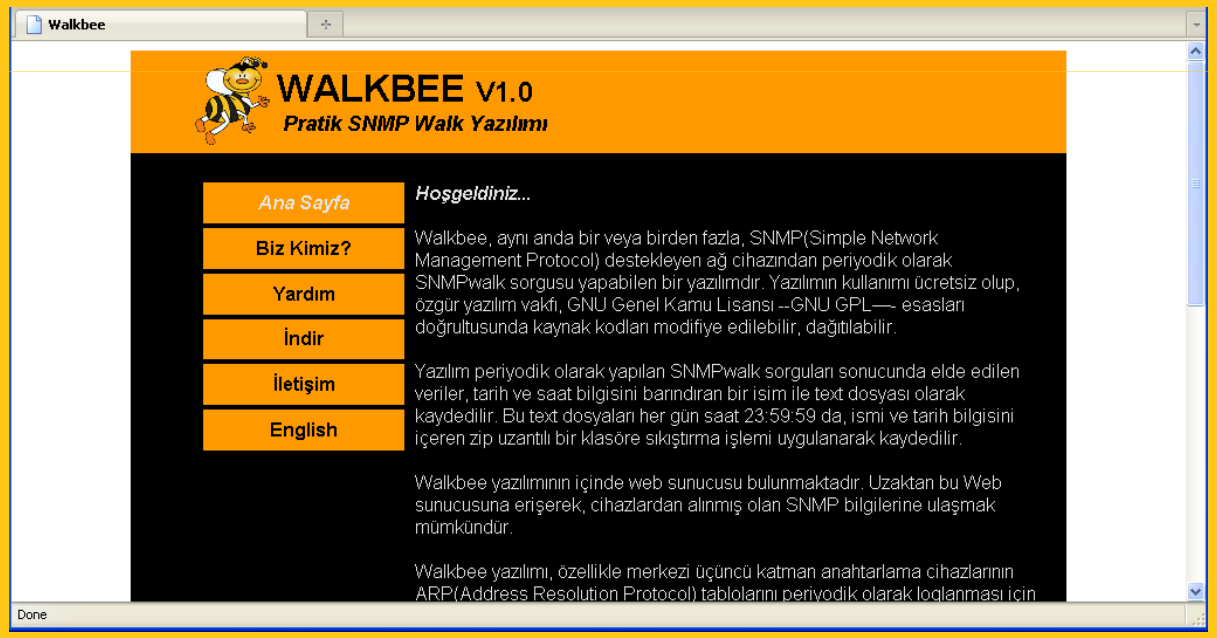
İTÜ/BİDB Bilgi İşlem Daire Başkanlığı

Yazılım Web Adresi

Yazılımı indirmek ve daha fazla detay için:

http://www.walkbee.net

(http://www.walkbee.com)



İTÜ/BİDB Bilgi İşlem Daire Başkanlığı

Sonuç

Ağ yöneticilerinin kontrolü ellerinde tutabilmeleri için gün geçtikçe daha fazla araç kullanmaları gerekmektedir.

Bu amaçla “WalkBee” ve benzeri yazılımlar kullanıcı takibi için önem kazanmaktadır.

Sorular

Teşekkürler

Sunum ve Bildiri için:

http://www2.itu.edu.tr/~akingok

(http://www.gokhanakin.net)

Yazılımın web sayfaları:

http://www.walkbee.net

(http://www.agciyiz.net/walkbee)