Kampüs Ağlarında Aranan Kullanıcıların Tespiti V1.1

Gökhan AKIN, Sınmaz KETENCİ
İstanbul Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, Ayazağa/İstanbul – ULAK-CSIRT, Ankara

Özet: Günümüzde yasal sorumluluklardan dolayı ağ yöneticilerine belirli bir tarihte aranan bir IP adresinin kimin tarafından kullanıldığı sık sık sorulmaya başlanmıştır. Ortamda gerçek IP adresi bile kullanılsa IP ve MAC adresleri kolaylıkla değiştirilebilmekte ve zarar verici bir teşebbüste bulunan kullanıcıların tespiti imkansız bir hal almaktadır. Kaldı ki birçok kampüs ağında gerçek IP adresi kullanılmamakta ve bu da tespiti daha da zorlaştırmaktadır. Bu çalışmada yukarıda bahsedilen durumlarda bile kullanıcıların takibini sağlayacak ağ çözümleri bir araya getirilmiştir.

1- Giriş

Çeşitli sebeplerden belirli bir IP'nin ilgili zaman aralığında kimin tarafından kullanıldığının tespiti gerekebilmektedir. Ağ alt yapısına bağlı olarak bu tespit işlemi farklı teknikler ile gerçekleştirilebilir.

2- Tespit Teknikleri

Tespit işlemini gerektiren olaylarda, Kampus ağı sorumlusuna gerçek IP adresi belirtilerek tespit çalışması yapılması istenecektir. Ancak NAT yapılan ağlarda bu adres tek başına hiçbir şey ifade etmeyecektir. Bu nedenle NAT uygulaması kullanan ağlarda NAT loglarının tutulması için ekstra bir emek harcanması gerekir.

Kurum gerçek IP adresi ile istemcilerini Internet'e eriştirse bile IP adresi kolaylıkla değişebildiği için yine de kullanıcı takibi için çeşitli yöntemler uygulamak durumundadır. Bu durumda kullanılabilecek tekniklerin en başında kimlik denetim sistemlerinin kullanılması yani 802.1x veya Proxy/Captive Portal bazlı uygulamalar gelmektedir. Ancak kimlik denetiminin kullanılamadığı durumlar da söz konusudur. Bu durumda MAC bazlı veya IP bazlı güvenlik teknikleri ile kullanıcının kimliğinin veya yerinin tespiti yapılabilinir. [1,2]

Ancak kesin olan bir şey var ki, yazı dahilinde bahsedilen IP bazlı güvenlik tekniği hariç, hangi teknik kullanılırsa kullanılsın kullanıcının ilgili zaman aralığında sadece IP adresinin bilinmesi yetersiz kalmakta ve aynı zaman aralığında kullandığı MAC adresinin de bilinmesi gerekmektedir. Bunun içinde DHCP Sunucusu logu veya Üçüncü katman cihazı ARP tablosu kayıt altına alınmalıdır.

3- NAT Kullanan Ağlar İçin Gereken Takip Yöntemleri

NAT kullanılan ağlarda, ağ kontrol yapısı ne şekilde yapılandırılırsa yapılandırılsın, söz konusu ağda 802.1x kimlik denetimi yapılıyorsa bile mutlaka NAT tercüme (translation) tablolarının loglanması gerekmektedir. Aksi takdirde kullanıcının izinin sürülmesi imkansız hale gelmektedir. Bu sebepten NAT tercüme tablolarının çıkış yönlendiricisinden zaman bilgileri ile alınıp saklanmaları gerekmektedir.

Iptables ile NAT logunu tutmak için gereken konfigurasyon:

```
#LOG komutu önce yürütülmelidir. Aksi taktirde NAT sonrası LOG oluşmaz.
iptables -t nat -A POSTROUTING -s 192.168.1.0/255.255.255.0 -o eth1 -j LOG
iptables -t nat -A POSTROUTING -s 192.168.1.0/255.255.255.0 -o eth1 -j MASQUERADE
```

Harici bir SYSLOG sunucusuna NAT logunun yollanması için gereken konfigurasyon:

```
vim /etc/syslog.conf
#NAT logları kern.warn tipindedir. Tüm logların uzak istemciye gönderilmesi istenirse log tipi *.* seçilebilir.
kern.warn          @192.168.2.2
```

Tutulan NAT logunun örneği:

```
Feb 9 15:44:24 linux-box kernel: IN= OUT=eth1 SRC=160.75.218.174 DST=208.67.222.222 LEN=52
TOS=0x00 PREC=0x00 TTL=127 ID=8783 DF PROTO=TCP SPT=49725 DPT=80 WINDOW=8192
RES=0x00 SYN URGP=0
```

```
Feb 9 15:44:24 linux-box kernel: IN= OUT=eth1 SRC=160.75.218.133 DST=208.67.222.222 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=7046 DF PROTO=TCP SPT=4582 DPT=25406 WINDOW=65535 RES=0x00 SYN URGP=0
```

Cisco ile NAT logunu tutmak için gereken konfigurasyon

```
! SYSLOG Sunucusunun IP adresi belirtilir
logging 10.0.0.4
! NAT Tercume tablolarının Syslog Sunucusuna yollaması için gereken komut
ip nat log translations syslog
```

Tutulan NAT logunun örneği:

```
*Feb 1 20:14:22.126: %IPNAT-6-CREATED: tcp 10.0.0.4:1882 85.102.185.159:1882 192.168.10.68:80 192.168.10.68:80
*Feb 1 20:15:05.842: %IPNAT-6-DELETED: udp 10.0.0.4:58416 85.102.185.159:58416 192.168.10.1:53 192.16
```

4- Aranan IP Adresinin MAC adresi Kaydının Tutulması

İlgili IP adresinin o zaman aralığında hangi MAC adresi tarafından kullanıldığının belirlenmesi araştırmayı bir adım ileriye götürecektir. Söz konusu ağda otomatik IP adresi dağıtma sistemi kullanılıyorsa MAC adresi bilgisi DHCP[3] sunucusu logundan tespit edilebilir. Aşağıda Linux ISC-DHCP ve Cisco Yönlendiricilerin DHCP sunucusu için örnek konfigürasyon ve alınabilecek log çıktısı bulunmaktadır.

Harici bir SYSLOG sunucusuna DHCP logunun yollanması için gereken konfigurasyon:

```
#syslog ile uzak bir istemciye loglari göndermek için syslog.conf dosyasında log tipi ve uzak istemci ip adresi eklenmelidir.
vim /etc/syslog.conf
deamon.info @160.75.200.2
```

Tutulan DHCP logunun örneği:

```
# DHCP logu /var/log/messages dosyasınında tutulmaktadır. Grep komudu ile aranan IP'nin bilgilerine ulaşılabilir.
tail -f /var/log/messages | grep dhcpd | grep 160.75.200.254
Feb 9 20:19:13 linux-box dhcpd: DHCPDISCOVER from 00:10:20:30:40:50 via eth0
Feb 9 20:19:14 linux-box dhcpd: DHCPOFFER on 160.75.200.254 to 00:10:20:30:40:50 (yuce) via eth0
Feb 9 20:19:14 linux-box dhcpd: DHCPREQUEST for 160.75.200.254 (160.75.200.1) from 00:10:20:30:40:50 (yuce) via eth0
Feb 9 20:19:14 linux-box dhcpd: DHCPACK on 160.75.200.254 to 00:10:20:30:40:50 (yuce) via eth0
```

Cisco yönlendiricilerde DHCP Kiralama tablosunun loglanması için konfigürasyon

```
ip dhcp database ftp://dhcp:dhcp123@10.0.0.4/router-dhcp write-delay 120
ip dhcp database tftp://10.0.0.4/dhcp_log write-delay 60
```

Ancak kullanıcıların elle sabit IP vermeleri durumunda MAC adresi verisine bu yöntemle ulaşılamaz. Gerek otomatik IP, gerekse sabit IP kullanılması durumu için MAC adresi bilgisine ulaşmanın en güzel yöntemi merkez üçüncü katman yönlendiricinin ARP tablosunun bir kopyasını periyodik olarak loglamaktır. Kutu yönlendirici çözümlerinde ilgili markaya göre değişen SNMP MIB değerleri ile ARP tablosu kopyalanabilmektedir. Linux yönlendirici çözümü için yapılabilecek örnek konfigürasyon aşağıdadır.

Linux tabanlı yönlendiricileride ARP logunun tutulmasını sağlayacak betik:

```
#!/bin/sh
# arp tablosunun logunun alinmasi
# Scripti calistirmadan once mkdir /var/log/arplog/ komudu ile klasorunu olusturunız.
# Crontab ile bu script belirlediğiniz sıklıkta çalıştırılabilir.
DIR=/var/log/arplog/
FILE=arptablosu.`date +"%d-%m-%Y-%H:%M"`
cd $DIR
arp -a > $FILE
```

Tutulan ARP logunun örneği:

```
? (160.75.200.78) at 00:16:D4:00:00:D0 [ether] on eth0
? (160.75.200.206) at 00:1E:00:00:00:D5 [ether] on eth0
? (160.75.200.171) at 00:1B:38:00:00:6F [ether] on eth1
```

Anahtarlama cihazlarının MAC adresi tablolarının kontrol edilmesi ile ilgili kişinin yeri ancak aranan kullanıcı o anda ağda barınmakta ise tespit edilebilir. Ayrıca MAC adresi kolaylıkla değiştirilebilir ve aranan MAC adresini tespit sırasında kullanan istemci ile olayın sorumlusu kullanıcının aynı kullanıcılar olduğu yargısına varılamaz. Bu sebepten çözüm olarak yukarda anlatılan loglama işlemlerine ek olarak aşağıdaki çözümler de kullanılmalıdır. Kullanıcı Adı Bazlı Tespit - 802.1x Kimlik Denetimi
Kampüs ağı yöneticisinin kullanıcı kimliğinin tespitine olanak sağlayan en güvenilir çözüm 802.1x ağ kimlik denetimi teknikleridir. Kablosuz ağlarda popüler olarak kullanılmaktadır. Ancak kablolu ağlarda kampüs ağlarındaki istemci çeşitliliği kimlik denetim sistemlerinin kullanılmasını zorlaştırmaktadır. Kimlik denetimi kullanılması durumunda ilgili zaman aralığındaki Radius sunucusunun logunun incelenmesi kullanıcının tesbiti için yeterli olacaktır.

5- Kullanıcının Ağa Dahil Olduğu Yerin Belirlenmesi İle Tespiti

5.1- MAC adresinin takibi ile yerinin tespiti

5.1.1- Option 82 bilgisi ile yerin belirlenmesi

Option (Seçenek) 82 DHCP paketleri içine eklenen bir özelliktir.[4] Aslen RFC3046[5] ile belirlenmiştir ve "DHCP Relay Agent" bilgisinin DHCP sunucusuna taşınması için geliştirilmiştir. Bu bilgi kısmında IP adresini isteyen istemcinin bağlı olduğu anahtarlama cihazının MAC adresi ve bağlı olduğu port numarası loglanabilmektedir. Bu sayede kullanıcın bağlandığı yer tam olarak tespit edilebilmektedir. Ancak bunun için kenar anahtarlama cihazlarının bunu desteklemesi ve tüm kullanıcıların otomatik IP adresi alması gerekmektedir. Kullanıcılar sabit IP kullanmaları durumunda takip dışında kalmaktadırlar ve bu da tek başına "Option 82" özelliğinin kullanılmasını yetersiz kılmaktadır. Cisco anahtarlama cihazlarında "Option 82" bilgisinin devreye alınması için gereken bilgilendirme aşağıdadır. [6]

```
! Snooping'i devreye alma komutu
ip dhcp snooping
ip dhcp snooping vlan <vlan no>
!
! option 82bilgisinin taşınmasının devreye alınması için gereken komut
ip dhcp snooping information option
!
interface <int adı> <int.no>
description Istemci bilgisayar portu – Bir konfigurasyon yapmaya gerek yoktur.
!
interface <int adı> <int.no>
description DHCP sunucusunun portu veya Uplink portu
ip dhcp snooping trust
```

Sabit IP adresi kullanılmasını engellemek için "Source Guard" isimli bir çözüm bulunmaktadır. Ancak günümüzde bu özellik henüz üçüncü katman anahtarlar ile sağlanabilmekte ve bu da biraz daha masraflı bir çözüm olarak karşımıza çıkmaktadır. Daha fazla bilgi için [BENIM DHCP SUNUMU] incelenebilir.

5.1.2- MAC Adresi Güvenliği ile Yerin Belirlenmesi

Kenar anahtarlama cihazlarında ağ erişimi yapabilecek MAC adresleri sabitlenebilir. Bu çözümde kullanıcılar MAC adreslerini değiştiremeyeceklerinden aranan MAC adresinin bağlandığı port kolaylıkla tespit edilebilir. Ancak böyle bir işleme gidebilmek için önce bütün kullanıcıların MAC adresleri toplanmalı ve bu bilgiler sürekli güncel tutulmalıdır. Bu sebepten port bazında MAC adresi güvenliği uygulaması zor bir çözümdür. Ayrıca kullanılan kenar anahtarların da buna destek vermesi gerekmektedir. Cisco anahtarlama cihazlarında MAC adresi bazlı güvenliğin devreye alınması için gereken konfigürasyon aşağıdadır. [X]

```
İnterface <int adı> <int.no>
!MAC guvenligini açar
```

```
switchport port-security
!O portan bağlantı kurabilecek maximum  mac adresini belirler
switchport port-security maximum <toplam PC sayısı>
!Kural dışı bir işlem yapılırsa uygulanacak yaptırım
switchport port-security violation <protect | restrict | shutdown>
!İstemcinin MAC adresinin belirtildiği kısım
switchport port-security mac-address <PC'nin MAC adresi>
```

5.1.3- MAC Adresi Tablosu Değişikliği Logu ile Takip

Bu amaç için kullanılan başka bir teknik de, kenar anahtarlama cihazının desteklemesi durumunda MAC adresi tablosuna eklenen ve silinen adreslerin loglanmasıdır. Bu da aranan MAC adresinin ilgili zamanda bağlı olduğu anahtarlama cihazının ve portunun tespitini sağlar. Biraz fazla log oluşturması dışında çok geçerli bir çözümdür. Cisco marka cihazlarda MAC adresi değişikliği logları "SNMP Trap" tekniği ile log sunucusuna yollanmaktadır ve örnek konfigürasyon aşağıdaki gibidir.

```
!SNMP Trapleri Dinleyecek Sunucunun tanimlanması
snmp-server host 160.75.100.100 anahtar_kelime
!
!MAC adresi değişikliklerinin loglanması devreye alır
mac-address-table notification
snmp-server enable traps config
!
!Loglananın yapılacağı interface'in belirtilmesi
interface <int adı> <int.no>
description Istemci bilgisayar portu
snmp trap mac-notification added
snmp trap mac-notification removed
```

5.2- IP Adresi Erişim Kontrol Listesi ile Takip

Diğer çözümlere nazaran daha yeni bir çözüm sayılabilecek bir çözüm olan IP adresi bazlı port güvenliği, kullanıcıların bağlı olduğu kenar switch'lerde IP bazlı erişim kontrol listesi yazılmasıdır. Bu sayede ilgili IP adresi sadece o porttan erişim yapabilmekte ve bir log tutulması gereği ortadan kalmaktadır. Bu çözüm kullanıcıların sabit IP adresi kullanmasına daha uygundur. Ancak MAC adresi rezervasyonu yapılması durumunda otomatik IP adresi kullanılması mümkündür. Cisco marka cihazlar için örnek konfigürasyon aşağıdaki gibidir.

```
! IP ACL'lerin belirtilmesi
access-list 1 permit 160.75.99.1
access-list 2 permit 160.75.99.2
...
! Interface'e uygulanması
interface FastEthernet0/1
 description oda_no 1 Priz_no 1
 switchport mode access
 ip access-group 1 in
```

6- Sonuç

5651 sayılı kanun getirdiği sorumluluklar çerçevesinde ağ yöneticilerinin ağ kullanıcılarının takibi zorunlu hale gelmiştir. Bu sebepten ağ yöneticileri kendi ağ mimarilerine en uygun olan tekniği belirleyerek uygulamalıdır.

Bildiride de belirtildiği gibi NAT kullanan kampüs ağlarında NAT tercüme (translation) tablolarının loglanması yapılmıyorsa kampus ağı dışına hedefli hiçbir olayın kaynağı tespit edilemez. Kullanıcı takibi için en güvenilir çözüm kimlik denetimi (802.1x) teknikleridir. Ancak kampüs ağlarındaki istemci çeşitliliği kimlik denetim sistemlerinin kullanılmasını zorlaştırmaktadır.

Bildiride incelediğimiz bir diğer teknik de kullanıcının ağa dahil olduğu yerin belirlenmesidir. Uygulanabilecek en kolay tekniklerden biri IP bazlı erişim kontrol listesi tekniğidir. Kenar anahtarlama cihazı bu tekniği

desteklemiyor ise veya dinamik IP adresi kullanılıyorsa MAC adresi takibi önem kazanır. IP adresinin ilgili zaman aralığında hangi MAC adresi tarafında kullanıldığının kayıt altında tutulmasının en kesin yöntemi yönlendirici cihazının arp tablosunun loglanmasıdır. MAC adresi değiştirilmesi olasılığına karşı MAC adresini tablosu değişiminin loglanması veya MAC adresi bazlı güvenliğin uygulanması gerekmektedir.

Son olarak yönetilemeyen kenar anahtarlama cihazı kullanılması durumunda kullanıcı takibi pek mümkün olmamaktadır.

Referanslar

[1] Karaarslan,E., Akın G., "Kurumsal Ağlarda Zararlı Yazılımla Savaş", Akademik Bilişim 2008, Çanakkale
[2] Karaarslan,E., Akın G., "Kurumsal Ağlarda Zararlı Yazılımla Mücadele Kılavuzu", Ulaknet Çalıştayı 2008, Konya
[3] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, IETF, Mart 1997.
[4] Akın G., "DHCP Servisine Yeni Bir Bakış", INET-TR 2008, Ankara
[5] M. Patrick, "DHCP Relay Agent Information Option", RFC 3046, IEFT, Ocak 2001
[6] Ken Coley, "Recommended Operation for Switches Running Relay Agent and Option 82", EtherNet/IP Implementor Workshops, 2004