

DHCP Servisine Yeni Bir Bakış

Gökhan Akın

İstanbul Teknik Üniversitesi / BİDB, ULAK / CSIRT

gokhan.akin@itu.edu.tr

Özet: DHCP sunucusunun güvenliği değişen ağ kullanım ihtiyaçları paralelinde önem kazanmıştır. DHCP servisinin güvenliğinin artırılması için kullanılacak tekniklerin avantaj ve dezavantajları kısaca incelenmiştir. Ayrıca güvenlik sağlayan tekniklerden biri olan DHCP Snooping (DHCP Araştırmacı) 'ın yerel alan ağlarında kullanıcı takibini kolaylaştırması avantajını değerlendirebilecek bir DHCP servisinin nasıl olabileceği tarif edilmiştir.

Abstract: Security of the DHCP server has gained its importance in parallel with the changing network usage needs. The advantages and the disadvantages of the techniques that can be used to increase the security of the DHCP services has been discussed briefly. Additionally, it is described that, how a new DHCP server design can be helpful, by using DHCP Snooping feature, on the subject of user's follow-up.

Anahtar Kelimeler: DHCP, Otomatik, IP, Option 82, Snooping, Seçenek

1. Giriş

DHCP servisi IP bazlı çalışan istemcilerin IP adresleri, alt ağ maskeleri gibi tanımlanması gereken ayarların otomatik olarak bir sunucu tarafından ayarlanmasını sağlar. Bu servis ağ yöneticilerinin yükünü bir bakıma azaltmaktadır. Ancak bu durumda istemcilerin hangi IP adresini aldıklarının takibi önem kazanmaktadır.

Ayrıca DHCP ile IP dağıtılan bir ağda DHCP servisi ile ilgili oluşacak bir sorun istemcilerin IP'siz kalmalarına ve erişlerini kaybetmelerine sebep olacaktır. Bu kadar önemli bir servis olmasına rağmen DHCP servisi güvenliği çoğu zaman göz ardı edilmektedir ve çeşitli saldırılara karşı korumasızdır.

2. DHCP Servisi'nin Güvelik Sorunları

DHCP servisi ile ilgili oluşabilen sorunlar şu şekilde özetlenebilir.

A. DHCP Sunucusunun

IP Havuzunun Boşaltılması:

Saldırmanın kaynak MAC adresini değiştirerek

DHCP sunucusunun otomatik ataması için tanımlanmış bütün IP'leri kendisine alması ile gerçekleştirilen saldırdır. Sunucu diğer istemcilere elinde IP adresi kalmadığı için servis vermez hale gelir. Bunun sonucunda istemciler IP adresi alamazlar ve erişim dışı kalırlar.

B. Yetkisiz DHCP Sunucusu Kurulumu ile İstemcilere Yanlış Adreslerin Atanması:

Yetkisiz DHCP sunucusu hizmeti verilerek son kullanıcı yanlış ağ geçidi veya yanlış DNS sunucusuna yönlendirilebilir. Yanlış ağ geçidi bilgilendirmesi ile istemcinin bütün trafiği gerçek ağ geçidine ulaşmadan saldırganın bilgisayarından geçirilebilir ve ağı dinleyen bir yazılımla birlikte bu trafik dinlenebilir. Aradaki adam saldırısı (man in the middle) olarak da isimlendirilen bu atakla şifreli olarak gerçekleştirilen SSL gibi haberleşme trafiği saldırgan tarafından algılanamaz.

İstemcinin sahte DNS sunucusu ile bilgilendirmesi daha tehlikelidir. Bu sayede kullanıcı bankacılık siteleri gibi kritik olan sitelerin sahtelerine yönlendirilebilir. Bu gibi durumlarda sertifika bazlı koruma son kullanıcıyı sahte siteye karşı

uyarabilecektir. Ancak sahte bankacılık sitesinin https yerine http olarak sunulması durumunda böyle bir uyarı da olmayacaktır. Bir sitenin https mi yoksa http mi olduğuna dikkat edecek son kullanıcı sayısı tartışmaya açık bir noktadır.

Yetkisiz DHCP Servisi verilmesi saldırı amaçlı olmayıp özellikle son kullanıcının temin ettiği kablosuz erişim cihazları gibi cihazlardan da kaynaklanabilmektedir. Bu cihazlar çoğunlukla varsayılan olarak DHCP servisi açık olarak satılmakta ve bu durumda ağda kullanılmayan bir IP aralığından adres dağıtılması söz konusu olmaktadır. Bu da istemcilere yanlış IP adresi atanmasına ve ağ erişimlerinin devre dışı kalmasına sebep olur.

3. İkinci Katman Ataklarında Değişen Şartlar

DHCP servisi 1997 yılında çıkmış RFC2131[1] ile tarif edilmiştir. Bu servis bu ataklara o dönemden beri açıktır.

Ancak bu saldırının yapılabilmesi için saldırgan ve istemcinin aynı genel yayın alanında (broadcast domain'de) bulunması gerekmektedir. Aynı kurum içerisinde kablo alt yapısının kurumun kendi personeli tarafından kullanıldığı düşünülerek bu uygulamanın büyük bir tehdit oluşturmadığı düşünülüyordu. Ancak günümüzde değişen şartlar sonucunda bu gibi ataklar ciddi tehditler oluşturmaya başlamıştır. Bu şartlar şu şekilde özetlenebilir.

A. Zararlı yazılımlardan kaynaklı saldırılar
Bilgisayarına DHCP sunucusu barındıran bir virus/worm vs. gibi zararlı yazılım bulaşan bir bilgisayar kullanıcısı farkında olmadan bulunduğu ağ bu türden ataklar ile tehdit altında tutulmaktadır. İstanbul Teknik Üniversitesi akademik ağında Ekim 2008'de bu şekilde bir worm tespit edilmiştir. İlgili zararlı yazılımın DHCP sunucusu bulunduğu genel yayın alanındaki PC'lere Ukrayna'da bulunan bir DNS sunucusunu öğrettiği tespit edilmiştir.[2]

B. Kullanıcıların Değişmesi

Yurt, otel vb mekanlarda kurumun kendi personeli dışındaki misafir olarak adlandırılabilir kullanıcılar kablolulu veya kablosuz internet erişimi sağlanması yaygın hale gelmiştir. Bu da bu türden atakların gerçekleşme ihtimalini arttırmaktadır. Bu gibi kullanımlarda aynı genel yayın alanında birbirini hiç tanımayan kullanıcıların bulunmalarını sağlamaktadır.

4.DHCP Servisine Yönelik Güvenlik Çözümleri

“DHCP mesajları için kimlik denetimi” başlığı ile 2001 yılında çıkan RFC 3118[3] yetkisiz DHCP istemcilerinin ve DHCP sunucularının bu şekilde atak yapmalarını engellemek amacıyla yazılmıştır. Ancak bu şekilde kimlik denetimi yapılabilmesi için sunucunun ve istemcinin bunu desteklemesi gerekmektedir. Şu anda yaygın olarak kullanılan DHCP istemcilerinde bu destek pek bulunmamaktadır. Belki aynı kurum içerisindeki bütün istemcilere ve sunuculara bu şekilde koruma yapabilen bir DHCP yazılımı kurulabilir. Ama misafir kullanıcısı diye adlandırılan kullanıcı grubuna bu şekilde bir kurulum yapılması pek mümkün değildir.

802.1X kimlik denetim sistemi ile dışarıdan ağa dahil olmak bir saldırgan kimlik denetimini geçemeyeceği için yerel alan ağına dahil olamayacaktır. Bu durumda DHCP servisine yönelik bir saldırı gerçekleştirilemeyeceğinden bir çözüm olarak düşünülmektedir. Ancak yetkili bir kullanıcı bilerek ya da bilmeyerek diğer kullanıcılara bu şekilde bir saldırıda bulunabilir. Ayrıca misafir diye belirtilen kullanıcı grubuna kimlik denetimi yapılması da pek mümkün değildir.

Belirli periyotlarda bir DHCP istemcisi gibi IP adresi isteğinde bulunup cevap veren DHCP sunucularını loglayan yazılımlar vardır. Bu amaçla Unix türevi işletim sistemleri için geliştirilmiş “DHCP Probe” [4] yazılımı ve Windows işletim sistemleri için geliştirilmiş

“dhecploc” [5] yazılımı kullanılabilir. Bu yazılımlar yardımı ile ağda bulunan yetkisiz bir DHCP sunucusu tespit edilebilir. Ancak yetkisiz sunucu MAC adresini ve DHCP sunucu adresini tanımlayan Option 54 (DHCP Server Id) değerini asıl sunucu ile aynı yapabilir. Bunun yanı sıra bütün genel yayın alanlarının da bu şekilde dinlenmesi gerekmektedir. Ayrıca istemcinin DHCP sunucusun bütün IP’lerini alarak DHCP sunucusunu servis dışı bırakma atağı da bu çözümle engellenemez.

Yerel alan ağ anahtarlarında (switch’lerde) bu sorunlara çözüm sağlamak amacı ile “DHCP Snooping” (DHCP Araştırmacısı) diye isimlendirilen bir özellik geliştirilmiştir. Böyle bir güvenlik için daha pahalı olan yönetilebilir anahtarlama cihazları gerekmektedir. Ancak 802.1x gibi kimlik denetimi bazlı bir çözümde de aynı sorun söz konusudur. Ayrıca günümüz donanım olanakları ile DHCP ile ilgili bir servis ileri bir sistem kaynağı ihtiyacı olmadan karşılanabildiğinden gün geçtikçe daha ekonomik olarak bu özellikler elde edilebilmektedir. Bu özelliğe sahip cihazlarda, yetkili DHCP sunucusunun bağlanacağı porta sunucu olarak paket yollama izni verilmiştir. Diğer portlardan gelecek DHCP sunucusu paketleri cihaz tarafından bloklanmakta ve bu şekilde bir teşebbüste bulunan portlar loglanmaktadır. Bu şekilde sahte DHCP sunucusu hizmeti verilmesi engellenebilir.

Bir paketin DHCP istemci paketimi sunucu paketimi olup olmadığının anlaşılması için servisin verildiği UDP port numaralarının kontrolü yeterlidir. İstemci paketi UDP 68 kaynak, UDP 67 hedef port numarası ile istekte bulunurken tam tersi şeklinde de sunucu istemciye cevap verir. Ayrıca sunucu portu dışındaki portlarda saniyede gerçekleşebilecek DHCP paketi sayısı sınırlanıp, bu sınırının üstünde DHCP paketi yollayan istemci portları kapatılabilmektedir. Bu sayede istemcilerin DHCP sunucusundaki bütün IP’lerin kısa bir sürede tüketilmesi de engellenmektedir.



Şekil.1 DHCP Snooping destekli anahtarlama cihazlarında DHCP trafiği

5. DHCP SNOOPING ile OPTION 82 Verisinin de Kullanılması

DHCP servisi istemcinin genel yayın olarak DHCP sunucusundan IP adresi istemesi ile gerçekleşir. Genel yayın paketleri üçüncü katman cihazlarından geçemeyeceği için her genel yayın alanına ayrı bir DHCP sunucusu kurulması gerekmektedir. Bu pratikte pek mümkün ve mantıklı değildir. Buna çözüm olarak “DHCP Relay Agent” olarak isimlendirilen ve RFC 3046 [6] tanımlanan bir uygulama geliştirilmiştir.

Buna göre bu özelliğe sahip yönlendirici veya ilgili genel yayın alanında kurulan başka bir sunucu istemcilerden gelen DHCP isteklerini dinlerler. Bu istekleri daha önceden de belirlenmiş olan DHCP sunucularına unicast (tekil yayın) olarak iletip DHCP sunucusu tarafından atanan IP adresini istemciye iletirler. Bunu yaparken “DHCP Relay Agent” sunucusu kendisi ile ilgili bilgiyi DHCP istek paketinin sonunda bulunan “options” (seçenekler) kısmına 82 numara ile ekleyebilmektedir.

Bu veri kablone/ADSL benzeri sistemlerde IP’yi isteyen istemcinin bağlı olduğunu cihaz bilgisi ve istemcinin devre numarası halini almıştır. Hatta günümüzde “DHCP Snooping” özelliği bulunan yerel alan ağ anahtarlama cihazları istemciden gelen paketin bir DHCP paketi olduğunu anlayıp DHCP isteğinin peşine Option 82 verisi olarak kendi MAC adresini ve istemcinin bağlı olduğu port numarasını da DHCP sunucusuna yollayabilmektedir.

6. Yerel Alan Ağlarında Takibi Kolaylaştırmak için Yeni IP Atama Mimarisi

Bilgisayar ağlarında IP adreslerinin kimin tarafından kullanıldığının belirlenmesi güvenlik anlamında çok değerli ve çoğu zaman tespiti zor olan bir bilgidir. Bir sorun olması durumunda sorunun kaynağı IP adresi ile tarif edilmektedir. İstemcilerin sürekli aynı IP adresini alması statik olarak IP'lerin verilmesi veya DHCP sunucunda MAC adresi bazlı rezervasyon ile sağlanabilmektedir. Ancak IP adresleri kolaylıkla değiştirilebilmektedir. Buda kaynak bilgisayarın tespitini zorlaştırmaktadır.

Bu duruma çözüm olması amacı ile İTÜ/BİDB kapsamında geliştirilmiş SNMP protokolü ile merkezi üçüncü katman anahtarlama cihazının arp tablosunu belirli sıklıklar ile loglamaktadır. Elde edilen log ile de saldırganın hangi MAC adresini kullandığı tespit edilebilmektedir. Ancak ilgili MAC adresine sahip bilgisayar artık ağa bağlı olmayabilir ve ikinci katman anahtarları MAC adresi tablolarını çok kısa süre tuttıkları için yerinin tespit edilmesi mümkün olmaz. Kaldı ki saldırgan başkasının MAC adresini bir süreliğine kendi bilgisayarına verip ilgili saldırıyı gerçekleştirmişte olabilir.

IP adresi atanan PC'nin option 86 verisi ile beraber loglanması sayesinde ilgili IP adresi eğer bir saldırıya adı karışır, saldırganın hangi anahtarın hangi portundan ağa eriştiği tespit edilebilir. İlgili portun hizmet verdiği oda belirlenebilir saldırganın kimliğine kadar ulaşılabilir.

Ayrıca gerek son kullanıcının istemesi gerekse monitör etmek kolaylığı açısından aynı istemciye sürekli aynı IP'nin verilmesi istenebilir. Bunun için kullanılacak teknikler şu şekildedir.

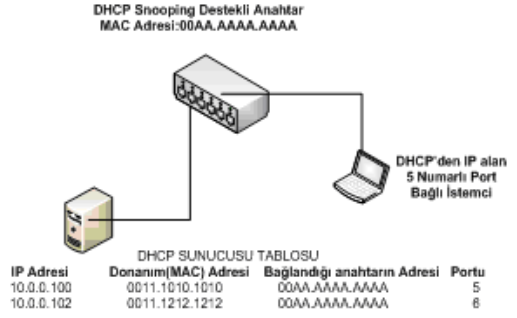
A. MAC Adresi Rezervasyonu

MAC adresi rezervasyonu tekniği ile gerçekleştirilebilir. Bu şekilde DHCP sunucusunda istemcinin MAC adresi ve IP adresi belirtile-

rek hep aynı IP'yi alması sağlanabilir. Ancak istemciler kolay bir şekilde başkasının MAC ile kendi adreslerini değiştirebilirler.

B. Option (Seçenek) 82 Bazlı Rezervasyon

Option 82 bazlı bir rezervasyon tekniği kullanılabilir. Bu durumdan istemci odasındaki prizden IP istemesi durumunda hep aynı IP adresini alabilecektir. [7]



Şekil.2 Option 82 destekli DHCP sunucusunda oluşacak DHCP tablosu

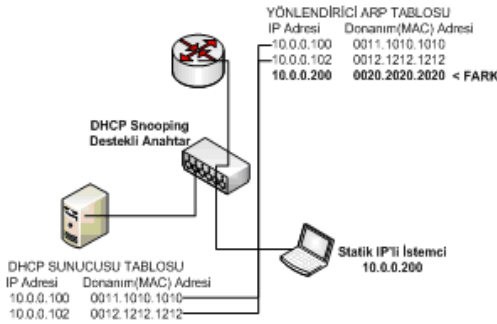
Tasarımı üzerine uğraşılan DHCP sunucusunun özellikle ikinci özelliği desteklemesi üzerinde durulmaktadır. İlk teknik ise opsiyonel olarak düşünülmektedir.

İstemcinin elle IP adresi verme ihtimali de söz konusudur, bunun engellenebilmesi için yine anahtarlama cihazları bazlı çalışabilen "Source Guard" olarak isimlendirilen bir özellik vardır. Anahtarlama cihazları "DHCP Snooping" özellikleri ile otomatik IP adresi verilen port numarasını, istemcinin MAC adresini ve atanan IP adresini bir tabloda tutabilmektedir. Bu özellik devreye alındığında bu tabloda belirtilen IP, MAC ve port eşlemesine uymayan hiçbir trafik anahtar cihazından içeri alınmamaktadır. Ancak günümüzde bu henüz üçüncü katman anahtarlar ile sağlanabilmekte ve bu da çok masraflı bir çözüm olarak karşımıza çıkmaktadır.

Bir başka çözüm ise anahtarlama cihazının desteklemesi durumunda IP bazlı erişim kural listesinin yazılmasıdır. Ancak gerek tek tek bü-

tün portlara sabit IP girilmesinin zor olması gerekse “Source Guard” desteği olan anahtarlar kadar maliyetli olmasa da maliyetin fazla olmasından dolayı tercihi yine zor bir metottur.

Sabit IP verilmesini engellemek amacı ile bu iki çözüm kadar kesin olmasa da sabit IP verenlerin tespitinde kullanılacak bir yazılım geliştirilmesi planlanmaktadır. Buna göre merkez L3 anahtarlama cihazından belirli sıklıklar ile alınan ARP tablosu DHCP sunucusundaki kayıtlar ile karşılaştırılacaktır. DHCP sunucusunda kaydı bulunmayan bir ARP kaydı tespit edilirse sunucu yöneticiyi uyarabilecektir. Bu sayede yönetici sabit IP vermiş kullanıcıyı belirleyip gereken uyarıyı yapabilecektir.



Şekil.3 Option 82 destekli ve 3.katman ARP tablosu karşılaştırması ile sabit IP veren istemcinin tespiti

7. Sonuçlar

Giderek daha yaygın olarak kamuya açık yerlerde birbirlerini tanımayan istemciler aynı yerel alan ağına bağlanmaktadır. Buda ikinci katman atakları üzerine daha fazla yoğunlaşılmasını gerektirmektedir.

Ayrıca yerel alan ağı kullanıcı kayıtlarının mutlaka iyi bir kayıt sistemi ile tutulması gerekmektedir. Bu şekildeki bir kayıt sisteminin varlığı kullanıcıları ağ kullanımı sırasında daha dikkatli olmaya yönlendirecektir. Özellikle de DHCP sunucusu kayıtları titizlikle tutulmalıdır.

Değişen kullanım ihtiyaçları sonucunda DHCP sunucusu ataklarına çözüm olan “DHCP snooping” desteği ile beraber “Option 82” verisi de mutlaka değerlendirilip kayıt altına alınmalıdır. Bunun için bünyemizde geliştirilmesi üzerine çalışılan DHCP sunucusu yazılımı veya benzeri yazılımlar araştırılmalı ve mutlaka devreye alınmalıdır.

Kaynaklar

- [1] R. Droms, “Dynamic Host Configuration Protocol”, RFC 2131, IETF, Mart 1997.
- [2] Gökhan AKIN, “Ağımızda yedek DHCP sunucularınız olabilir”, Ekim 2008, <http://blog.csirt.ulakbim.gov.tr/?p=112>
- [3] R. Droms, W. Arbaugh, “Authentication for DHCP Messages”, RFC 3118, IETF, Haziran 2001.
- [4] dhcp_probe : DHCP and BootP servers Discovery Software, http://www.net.princeton.edu/software/dhcp_probe/
- [5] dhcplc : DHCP and BootP servers Discovery Software for Windows, <http://technet.microsoft.com/enus/library/cc759117.aspx>
- [6] M. Patrick, “DHCP Relay Agent Information Option”, RFC 3046, IETF, Ocak 2001
- [7] Ken Coley, “Recommended Operation for Switches Running Relay Agent and Option 82”, EtherNet/IP Implementor Workshops, 2004