IPv6 Saldırı Araçları ve IPv6-GO Uygulamaları

Emre Yüce, Yavuz Gökırmak

***Özet*— Teknolojinin gelişmesi ile ortaya çıkan gereksinimler ve IPv4 adreslerinin hızla tükenmesi yeni nesil internet protokolü IPv6'nın kullanımını zorunlu hale getirmektedir. İnternette IPv6 kullanımının artması ile birlikte ağ yöneticilerinin IPv6 geçişi ile ilgili bilgi birikimi günden güne artmaktadır. Mevcut ağlara IPv6 desteğinin verilmesi ve ağların yönetilmesine yönelik bil-yap bilgisi edinilmesinin yanında IPv6 güvenliğine yönelik de bilgi sahibi olunmalıdır. IPv6 geçiş aşamasına ve kullanımına yönelik güvenlik önlemlerinin alınabilmesi için IPv6 protokolüne özel saldırı açlarının ve güvenlik açıklarının irdelenmesi gerekmektedir. Bu konuda yapılacak olan çalışmalar saldırganların nasıl bir strateji izleyeceklerini tahmin etmek ve gerekli önlemler almak konusunda ağ ve güvenlik yöneticilerine yardımcı olacaktır. Bu çalışmada, güvenlik açıklarının uygulanmasına örnek teşkil etmek amacıyla literatürde yer alan ve "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında geliştirilen IPv6 saldırı araçları incelenmiş ve bu araçların IPv6-GO test ağında örnek uygulamaları gerçekleştirilmiştir.**

***Anahtar Kelimeler*—Ağ güvenliği, IPv6, saldırı araçları, IPv6-GO**

I. GİRİŞ

TÜM dünyada 20 yılı aşkın süredir yaygın olarak kullanılan IPv4 [1], zaman içinde yapılan teknik iyileştirmelere rağmen, günümüz internet altyapısının ihtiyaçlarını karşılamakta yetersiz hale gelmiştir. Teknolojinin getirdiği gereksinimler doğrultusunda 90'lı yılların başlarında yeni internet protokolü için çalışmalara başlanmıştır. Bu çalışmaların sonucunda yeni nesil internet protokolü Internet Protocol Version 6 (IPv6) 1998 yılında yayımlanan RFC 2460 [2] ile tanımlanmıştır. IPv6 protokolünün günümüz ihtiyaçları göz önüne alınarak tasarlanan yapısal iyileştirmeleri aşağıdaki gibi sıralanabilir:

- 128 bitlik adres yapısı ile geniş adres uzayı
- Otomatik adres dağıtma özelliği ile kolay yönetilebilirlik
- Basitleştirilmiş paket başlığı yapısı ile hızlı yönlendirme
- Zorunlu IPsec desteği
- Genişleme başlıkları ile Servis Kalitesi (Quality of Service, QoS) , gezgin IPv6 (mobile IPv6), IPsec desteğinin kolay sağlanabilmesi
- Geliştirilmiş çoklu gönderim (multicast) desteği

İnternet altyapısındaki IPv4 kullanımı bir gecede bırakılamayacağından, her iki protokolün de kullanımı belli bir süre devam edecektir. Geçiş sürecinin kullanıcılara ve servis sağlayıcılara olan etkisini azaltmak için çeşitli geçiş yöntemleri önerilmiştir [3]-[5].

IPv6 protokolünün yayılımında yukarıda belirtilen yapısal değişikliklerin ağ ve bilgi güvenliğine etkisinin pozitif veya negatif olması önemli bir etken olacaktır. IPv4'ün yerine IPv6 kullanımının, ağ güvenliğini nasıl etkilediği çeşitli araştırmalarda incelenmiştir [6]-[7]-[8]-[9]-[10]-[11]-[12]. Bu çalışmalarda, güvenlik tehditleri IPv4 ile benzerlik gösteren saldırılar ve IPv6 protokolü ile gelen yeni saldırılar olmak üzere iki başlık altında toplanmıştır [13]. Taşırma saldırıları, SQL injection vb. uygulama seviyesi saldırıları IPv4 ile benzerlik gösteren saldırılardan birkaçıdır [14]. IPv6 protokolü ile gelen yeni veya değişim gösterecek saldırılar ise yerel ağ saldırılarını, gezgin IPv6 saldırılarını [15]-[16]-[17]-[18]-[19], keşif yöntemlerini, geçiş yöntemi temelli saldırıları [20]-[21]-[22]-[23]-[24]-[25] içermektedir. Bu saldırılara ek olarak, IPv6 kullanımı yaygınlaştığında, şu anda öngörülemeyen ilk gün saldırılarının gerçekleştirilmesi mümkündür.

Yeni nesil internet protokolü ile birlikte gelen teknolojik yeniliklerin ve kolaylıkların kullanımı esnasında güvenlikten ödün vermemek ve güvenli bir IPv6 ağı oluşturmak için mevcut güvenlik açıkları ve bu açıkları kullanan saldırılar hakkında bilgi sahibi olunmalıdır [26]-[27]. Bu çalışmada literatürde yer alan ve "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında geliştirilen IPv6 saldırı araçları araştırılmış ve bu araçların örnek uygulamaları IPv6-GO test ağında gerçekleştirilmiştir. Bildirinin devamında; ikinci bölümde örnek uygulamaların gerçekleştirildiği IPv6-GO test ağı kısaca tanıtılmış, üçüncü bölümde saldırı araçları sınıflandırılmış ve yapılan örnek uygulamalar anlatılmıştır. Son bölümde ise değerlendirmeler ve sonuçlar yer almaktadır.

II. IPV6 GELİŞTİRME ORTAMI (IPV6-GO)

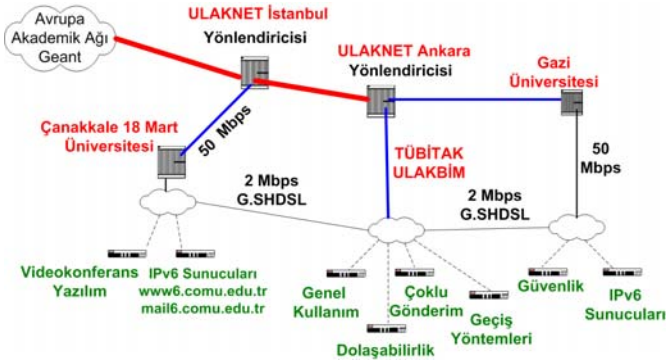
"Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi"

Çalışma 20 Mart 2010 tarihinde gönderilmiştir. Bu çalışma Türkiye çapında IPv6 altyapısı oluşturmak ve Türkiye'nin IPv6 protokolüne geçişini planlamak amacıyla TÜBİTAK – ULAKBİM'in yönetici, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi'nin yürütücü, Bilgi Teknolojileri ve İletişim Kurumu'nun müşteri kurum olarak katıldığı "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında gerçekleştirilmiştir [4]. Bu proje TÜBİTAK tarafından desteklenmektedir.

Emre Yüce, TÜBİTAK ULAKBİM bünyesinde araştırmacı olarak çalışmaktadır. Aynı zamanda ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Bölümü'nde doktora çalışmalarına devam etmektedir (Tel: 0312 298 93 92 Fax: 0312 298 93 93 E-mail: emre@ulakbim.gov.tr).

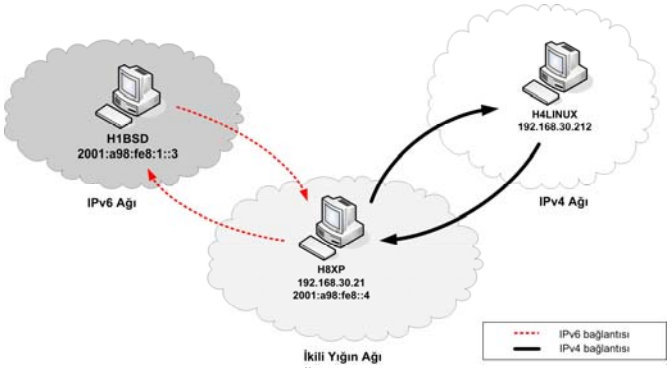
Yavuz Gökırmak, TÜBİTAK ULAKBİM bünyesinde araştırmacı olarak çalışmaktadır. (Tel: 0312 298 93 91 Fax: 0312 298 93 93 E-mail: yavuzg@ulakbim.gov.tr).

[4] kapsamında, Türkiye'de IPv6 kullanımını yaygınlaştırmak, IPv6 geçiş yöntemleri ile ilgili testler ve güvenlik analizleri yapmak ve IPv6 tabanlı uygulamaların testlerini gerçekleştirmek amacıyla TÜBİTAK ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi bünyesinde IPv6-GO test laboratuarları [28] kurulmuştur. Bu test laboratuarlarının kurulması ile oluşacak bilgi birikimi ile üniversiteler, araştırma kurumları ve sanayi kuruluşlarındaki araştırma geliştirme faaliyetlerinin desteklenmesi hedeflenmektedir. Proje kapsamında halen geçiş senaryolarının, IPv6 ileri seviye özelliklerinin ve IPv6 saldırı araçlarının test uygulamaları devam etmektedir. IPv6-GO ağ yapısı Şekil 1 'de verilmiştir.



Şekil 1. IPv6-GO Genel Bağlantı Ağ Yapısı

IPv6 saldırı araçlarının örnek uygulamalarını gerçekleştirmek amacıyla IPv6-GO ağının TÜBİTAK ULAKBİM ayağında Şekil 2 'de gösterilen test ağı oluşturulmuştur. Test ağında üç adet bilgisayar kullanılmıştır. Bu bilgisayarlar H8XP (Windows XP SP3), H1BSD (FreeBSD 7.1), H4Linux (Debian 5.0.2) olarak isimlendirilmiştir. H8XP ikili yığın ağında, H1BSD yalın IPv6 ağında, H4Linux yalın IPv4 ağında bulunmaktadır.



Şekil 2. IPv6-GO Saldırı Araçları Örnek Uygulama Ağ Yapısı

III. IPv6 Saldırı Araçları

IPv6 saldırı araçları, ağdan geçen trafiğin izlenmesi, değiştirilmesi, gizlenmesi ve ağdaki mevcut servislerin ve sunucuların hizmet veremez hale getirilmesi amacı ile yazılmış programlardan oluşmaktadır. Saldırı araçları ağa zarar vermek isteyen saldırganlar tarafından kullanılabileceği gibi ağı daha güvenli hale getirmek isteyen ağ ve sistem yöneticileri tarafından da ağda yapılacak güvenlik testlerinde kullanılabilmektedir. Bu araçların kullandığı açıkların ve saldırı yöntemlerinin bilinmesi, ağı güvenli hale getirmek için alınacak önlemlerin tespitine katkı sağlayacaktır.

IPv6 üzerinden gerçekleşecek saldırının ilk adımı ağ hakkında bilgi edinilerek potansiyel kurbanların tespit edilmesidir. Ağ üzerinde gerçekleştirilecek tarama faaliyeti ile verilen servisler ve olası güvenlik zafiyetleri hakkında bilgi edinilmesi amaçlanmaktadır. Ağda IPv4 ile birlikte veya yalın olarak IPv6 kullanımı ağ tarama ve keşif yöntemlerinde birçok farklılığa yol açacaktır. Bu farklılıklar "Ağ Tarama ve Keşif Araçları" bölümünde incelenmiştir.

Saldırgan, keşif aşamasından sonra bulduğu kurbana yaptığı saldırı sonucunda cihaz yönetimini ele geçirebilir. Bu aşamada saldırgan, kaynağının bulunmasını zorlaştırmak ve cihazın uzaktan yönetimini fark ettirmeden gerçekleştirmek amacı ile arka kapı olarak yansıtıcı uygulamalar kullanabilir. Bu tür uygulama örnekleri "Port Yansıtma Araçları" bölümünde incelenmiştir.

IPv6 üzerinden yapılabilecek diğer bir saldırı türü kurbanın sahip olduğu bant genişliği, işlemci gücü ve bellek miktarı benzeri kaynakların aşırı kullanımına neden olarak kurbanı servis veremeyecek hale getirmek olabilir. Bu servis dışı bırakma saldırı örnekleri "Servis Dışı Bırakma Saldırı Araçları" başlığı altında incelenmiştir.

Paket düzeyinde paketin içeriğini değiştirmeye ve yakalamaya yönelik saldırı araçları "Paket Düzeyinde Saldırı Araçları" bölümünde incelenmiştir.

A. Ağ Tarama ve Keşif Araçları

IPv6 adres uzayının büyüklüğü göz önüne alındığında IPv4 ağlarında gerçekleştirilebilen rastgele ağ taramasının IPv6 ağlarında mümkün olmadığı öngörülmektedir. IPv6 adres aralığı büyüklüğü nedeni ile adres uzayının tamamının taranması mümkün olmasa da çeşitli yöntemler ile taranacak adres uzayının daraltılması mümkündür [29]. 128bitlik adresin hatırlanmasının zorluğu bu yöntemlerin geçerliliğini artırmaktadır. Bu yöntemler arasında sıradan (::1, ::2 vb.) veya hatırlanması kolay kelime şeklinde (::baba,::dede, ::face) IPv6 adresleri kullanılması yer almaktadır. Benzer şekilde adres uzunluğu sebebi ile DNS sunucularının kullanımının IPv6 ağlarında artacağı öngörülmektedir. Bu artış DNS sunucularını, geçerli IPv6 adreslerini bulmak için önemli birer kaynak haline getirmektedir [30]. Geçiş yöntemlerinin bir ağda kullanılması da, bazı geçiş yöntemlerinde kullanılan adres yapısının standart olması sebebiyle, ağ keşfini ve taramasını kolaylaştırmaktadır. Örneğin 6to4 geçiş yönteminde 2002::/16 öneki kullanılmaktadır. Adresin 17–48. bitleri 6to4 yönlendiricinin IPv4 adresini içermektedir. Bir 6to4 ağı tespit edildiğinde, bu ağdaki cihazların tespiti kullanılan adres yapısı sayesinde kolaylaşmaktadır.

IPv6 protokolünün kullanılması ile kullanılan ağ keşfi yöntemleri de değişiklik göstermektedir. IPv6 protokolünde yer alan komşu keşfi (neighbourhood discovery) ve durum denetimsiz adres yapılandırması (stateless address configuration) mesajlarının fiziksel güvenliği sağlanmış

bağlantılar üzerinden iletileceği düşünülmüştür [6]. Bu sebeple yerel ağa dâhil olmayı başaran bir cihaz tüm ağ güvenliğini tehdit edebilir. Bu durum özellikle gezgin IPv6 ağlarında tehlike arz etmektedir. Yerel ağ mesajları dışında çoklu gönderim ve herhangi birine gönderim (anycast) adreslerinin de ağ keşfi amacıyla kullanılması mümkündür.

Bölümün geri kalanında ağ taraması ve keşfi amacıyla yazılmış araçların incelemelerine ve IPv6-GO test ağında yapılan örnek uygulamaların sonuçlarına yer verilmiştir.

1) Nmap

Nmap (Network MAPper) [31], ağ taramak için Windows, Linux, BSD işletim sistemlerinde kullanılabilen bir araçtır. Nmap kullanılarak belli bir adres aralığındaki cihazlar, cihazlar üzerinde çalışan servisler, açık ve filtrelenmiş port numaraları, işletim sistemleri belirlenebilmektedir.

Nmap IPv6 desteği "-6" seçeneği ile kullanılabilmektedir. IPv4 ağlarında mümkün olan ağ tarama ve işletim sistemi tespiti özellikleri IPv6 ağlarında desteklenmemektedir. Bağlantı taraması (-sT), ping taraması (-sP), liste taraması (-sL) NMap aracının IPv6 ağlarında uygulanabilen seçenekleri arasındadır. NMap, bu seçenekler ile kullanılıp çalışan bir servis ile karşılaşmadığında, istemcinin kapalı olduğunu kabul etmektedir. İstemcinin ping cevaplarına bakılmaksızın tüm servislerin kontrol edilmesi için –PN seçeneği kullanılmalıdır. Ayrıca –PS seçeneği çalışması muhtemel servis port numarası ile birlikte kullanılabilmektedir. Bu uygulamaların örneği Tablo I 'de verilmiştir.

TABLO I
IPV6 NMAP ÖRNEK UYGULAMASI

```
[root@H1BSD ~]# nmap -6 -PS 2001:a98: fe8::4

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-01 10:04 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try
-PN
Nmap done: 1 IP address (0 hosts up) scanned in 2.08 seconds
[root@H1BSD ~]# nmap -6 -PS3389 2001:a98: fe8::4

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-01 10:08 UTC
Interesting ports on 2001:a98: fe8::4:
Not shown: 999 filtered ports
PORT    STATE  SERVICE
3389/tcp closed ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
[root@H1BSD ~]# nmap -6 -PN 2001:a98:fe8::4

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-01 10:08 UTC
Interesting ports on 2001:a98: fe8::4:
Not shown: 999 filtered ports
PORT    STATE  SERVICE
3389/tcp closed ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds
```

2) ARI (Automated Record Identifier)

"Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında geliştirilen ARI [4], bir alan adı altında tanımlanan ve alan adı sunucusunda kayıtları bulunan bilgisayarların tümünü ya da bir kısmını bulmakta kullanılabilen bir araçtır. Kaba kuvvet yöntemiyle tarama yapan ARI, çok kanallı (multi thread) çalışmaktadır. ARI, iş yükünü işçi fonksiyonlara bölerek, paralel süreçlerle verimi arttırmayı hedeflemektedir.

Tablo II'deki komut yardımıyla; ulakbim.gov.tr alan adı altında bulunan, en az 2 en çok 5 harfli kelimeler sadece karakterler kullanılarak oluşturulur ve ns1.ulakbim.gov.tr alan adı sunucusuna bu alan adlarıyla ilgili sorgular gönderilir. Bütün işlemler 4 işçi kanal yardımıyla paralel olarak gerçekleştirilmektedir.

Örnek bir çalışma çıktısı Tablo II'de görülen ARI'nın bu çalışmasında ortalama bellek tüketimi 7560 kb'dir.

TABLO II
IPV6 ARI ÖRNEK UYGULAMASI

```
/ari –d ulakbim.gov.tr –s ns1.ulakbim.gov.tr –n4 -uc -l2 -
m5
ab.ulakbim.gov.tr
cd.ulakbim.gov.tr
…
Sorgu/Saniye: 3919
Sure: 52.33 dk.
Taranan alan adi sayisi: 12.356.604
```

Çok kanallı mimaride iş paylaşımının verimi uygulama performansını doğrudan etkileyen bir etkendir. ARI, aranacak kelimelerin önceden belirlenip işçilere dağıtıldığı bir tasarım üstüne şekillenmemiştir. Böyle bir mimari hem fazla kaynak tüketmektedir hem de dengeli bir iş bölümüne engel olmaktadır. ARI 'da, işçi fonksiyonlara adres alanının hangi bölümünü tarayacakları bilgisi verilir ve işçiler bu bilgiyi kullanarak tarama yaparlar.

ARI, tasarımı sayesinde, farklı bilgisayarlarda kanal sayısı sınırlaması olmadan çalışabilmektedir. Farklı bilgisayarlarda ortaklaşa çalışabilmesi, dağıtık bir DNS saldırısı yapabilme imkânı sağlamaktadır.

3) Scan6

Scan6 Windows XP/2000 işletim sistemleri için hazırlanmış, C programlama dili ile yazılmış basit bir port

TABLO III
IPV6-GO SCAN6 ÖRNEK UYGULAMASI

```
C:\Scan6>scan6 -6 2001:a98: fe8::4

----IPv4/IPv6 PortScanner for Windows 2k/XP----

By LeVante^

----Scan6----
Host/IP Address: 2001:a98: fe8::4
Start Port: 1
End Port: 65535

NOTE: If you want to check "not so big" port range
specify a startport and an endport, the scanner will go faster

----PortScanning just started. Please wait----

Port 135 OPEN

----Port Scan terminated----
```

tarama uygulamasıdır. Belirtilen IPv4/IPv6 adresinin port aralığı belirtilmemişse, 1–65536 aralığındaki portlarını taramaktadır. Uygulamaya seçenek olarak taranacak port aralığı da verilebilmektedir. IPv6-GO 'da yapılan testte, H8XP üzerinde çalıştırılan komut ile H8XP 'nin IPv6 üzerinden dinlediği açık portları listelenmiştir. Test çıktıları Tablo III 'te verilmiştir.

4) MTR

MTR [32], Linux ve BSD işletim sistemleri için hazırlanmış "traceroute" ve "ping" uygulamalarının işlevlerini birleştiren bir ağ analiz aracıdır. Uygulama, Linux işletim sistemi paket yöneticisinde ve BSD işletim sistemi port yapısında yer almaktadır.

MTR, üzerinde çalıştığı istemci ve hedef adres arasındaki ağ cihazlarına ICMP veya UDP paketleri göndererek, paketin hedefe giderken üzerinden geçtiği her bir elemanın performansını ölçmektedir. IPv6-GO 'da H1BSD üzerinde MTR uygulaması çalıştırılmıştır. Hedef olarak H8XP belirtilmiştir. Tablo IV 'te uygulama çıktısı olan iki cihaz arasındaki ağ cihazları listesi, paket kaybı yüzdesi, gönderilen paket sayısı, son RTT değeri (ms), ortalama RTT değeri (ms), en düşük/iyi RTT değeri (ms), en yüksek/kötü RTT değeri (ms) ve standart sapma değeri yer almaktadır. Bu değerlere istenirse anlık jitter değeri, ortalama jitter değeri, en kötü jitter değeri eklenebilmektedir. MTR, ağ sorunlarını tespit etmek ve çözümlemek için uygun bir araçtır. Ayrıca, saldırganlar tarafından ağ keşfi için kullanılması mümkündür.

TABLO IV
IPV6-GO MTR ÖRNEK UYGULAMASI

My traceroute [v0.75]
H1BSD (::) Thu Apr 1 14:22:14 2010
Keys: Help Display mode Restart statistics Order of fields quit

Host	Packets Loss%	Snt	Pings Last	Avg	Best	Wrst	StDev
1. 2001:a98:fe8:1::1	0.0%	2	1.1	1.4	1.1	1.7	0.5
2. 2001:a98:fe8::4	0.0%	1	0.3	0.3	0.3	0.3	0.0

B. Port Yansıtma (Bouncer) Araçları

Port yansıtma (port bouncer) araçları çalıştırıldığı istemcinin belli bir portuna gelen trafiği dinlemekte ve bu porta gelen paketleri belirlenmiş hedefe iletmektedir. Bu araçlar çalıştırıldıkları cihaz üzerindeki belirli bir portu dinlediği için bu port, erişim kontrol listesi ile kontrol edilmediği takdirde, dışarıdan yapılan bağlantılara açık olacaktır. Ayrıca saldırganların bu tip servisleri IPv4-IPv6 ağları arasında geçiş yapmak veya bir saldırının izini bulmayı zorlaştırmak için kullanmaları mümkündür.

1) Relay6

Relay6 [33]; Windows NT, 2000 ve XP işletim sistemlerinde çalışmak üzere tasarlanmış GPL lisansına sahip, çalıştırıldığı bilgisayara gelen bağlantı isteklerini hedef adrese yansıtan bir uygulamadır. Relay6 uygulaması sadece TCP bağlantılarını desteklemektedir. Uygulamanın UDP desteği bulunmamaktadır.

Relay6 uygulaması çalıştırıldığı bilgisayar üzerinde belirlenmiş bir portu dinlemektedir. Bu porta gelen IPv4/IPv6 TCP bağlantı isteklerini hedef adresin hedef portuna iletmektedir. İletimi başlık bazında yaptığı için her iki protokol arasında da, aynı protokol üzerinden de iletim yapabilmektedir. (IPv4 → IPv6, IPv6 → IPv4, IPv4 → IPv4 , IPv6 → IPv6)

Relay6 uygulamasına verilen parametreler kullanılarak uygulama ile ilgili çeşitli ayarlamalar yapılabilmektedir. "/b:", parametresi ile dinlenecek IPv4/IPv6 adresi, "/c:" parametresi ile izin verilen maksimum bağlantı sayısı belirlenebilmektedir. "/f:" parametresi kullanılarak uygulama için erişim kontrol listesi kullanılabilmektedir. Relay6 uygulaması ile aynı dizine yerleştirilecek erişim kural listesini içeren dosya ile gelen/giden bağlantı istek IP adresleri ve/veya port numaraları kısıtlanabilmektedir. Bu parametre özelliklerine ek olarak uygulama çıktısı günlük olarak kayıt altına alınabilmektedir.

Tablo V 'te gösterilen örnek komut kullanılarak H8XP 'nin 5555 numaralı portuna gelen IPv6 paketleri, H4LINUX 'un IPv4 adresinin 22 numaralı portuna iletilmektedir. Bu kurulum ile IPv6-GO test ağında yalın IPv6 istemciden (H1BSD) yalın IPv4 istemciye (H4LINUX) SSH bağlantısı gerçekleştirilmiştir.

TABLO V
IPV6 RELAY6 ÖRNEK UYGULAMASI

```
C:\relay6>relay6 5555 192.168.30.212 22 /b:::

relay6 3.0

     the tcp bouncer ipv* to ipv*
     ¯ francesco picasso <s0tp@libero.it>


----- relay6 started -----

[date 2/4/2010] [14:10:29]

[14:10:31] <unknown> [[2001:a98: fe8:1::3]:53436] is
connected
[14:10:31] Actual connections 1
```

2) 6tunnel ve NT6tunnel

6tunnel [34] ; Linux işletim sistemlerinde çalışmak üzere tasarlanmış GPL lisansına sahip, çalıştırıldığı bilgisayara gelen bağlantı isteklerini hedef adrese yansıtan bir uygulamadır. 6tunnel uygulaması sadece TCP bağlantılarını desteklemektedir. Uygulamanın UDP desteği bulunmamaktadır. 6tunnel uygulaması Linux işletim sistemine kaynak dosyası indirilerek veya paket yöneticisi aracılığı ile kurulabilmektedir.

NT6tunnel [34], 6tunnel uygulamasının Windows işletim sistemine uyarlanmış halidir. 6tunnel uygulamasında olduğu gibi komut satırından çalıştırılmaktadır. Relay6 ve 6tunnel uygulamalarına benzer şekilde NT6tunnel uygulaması da IP*

→ IP* arasında TCP paketlerinin iletimini gerçekleştirmektedir.

Her iki uygulama da aynı özellikleri barındırmaktadır. Uygulamalar varsayılan olarak IPv4 uygulamasından IPv6 uygulamasına bağlantıları desteklemektedir. Tablo VI 'da gösterilen örnek komut kullanılarak H8XP 'nin IPv4 adresinin 10001 numaralı portuna gelen paketler, H1BSD 'nin IPv6 adresinin 22 numaralı portuna iletilmektedir. Bu kurulum ile IPv6-GO test ağında yalın IPv4 istemciden (H4LINUX), yalın IPv6 istemciye (H1BSD) SSH bağlantısı gerçekleştirilmiştir.

TABLO VI
IPV6 NT6TUNNEL ÖRNEK UYGULAMASI

```
C:\NT6tunnel> NT6tunnel 10001 2001:a98:fe8:1::3 22
```

C. Servis Dışı Bırakma Saldırı Araçları

Bu bölümde bir ağ cihazına çok sayıda paket göndererek cihazın verdiği servisi devre dışı bırakmak amacıyla yazılmış araçlar incelenmiştir. Bu tarz servis dışı bırakma saldırılarının "Paket Düzeyindeki Saldırı Araçları" bölümündeki araçlar kullanılarak da gerçekleştirilebilmesi mümkündür. Servis dışı bırakma saldırılarına karşı ağ belirli bir adresten gelen bağlantı isteklerini kısıtlama veya erişim kontrol listeleri ile korunabilmektedir. Saldırı, IPv6 ağlarında, IPv4 ağlarındaki uygulamasından farklı olmamakla birlikte geçiş yöntemleri kullanımı ile oluşabilecek dar boğazlar tek noktada arıza riskini artırmakta ve ağı servis dışı bırakma saldırılarına karşı daha açık hale getirmektedir [35].

1) 6tunnelDOS

6tunnelDOS, C programlama dili ile yazılmış bir araçtır. Hedef IPv4/IPv6 adresinin belirtilen portuna kısa aralıklarla çok sayıda TCP bağlantısı gerçekleştirerek ilgili porttaki servisi, servis dışı bırakmak için kullanılmaktadır.

6tunnel veya NT6tunnel araçlarının dinlediği porta yapılacak servis dışı bırakma saldırısı yansıtma işlevinin yerine getirilmemesine yol açacaktır. IPv6-GO 'da ikili yığın ağında bulunan H8XP üzerinde çalışan NT6tunnel uygulamasının dinlediği 10001 numaralı porta 6tunnelDOS aracı ile servis dışı bırakma saldırısı uygulanmıştır. Tablo VII 'de verilen komut ile H8XP 'nin, 10001 numaralı portuna her 10 milisaniyede bir olmak üzere toplam 25000 bağlantı yapılmıştır. Saldırı süresince H8XP üzerinden verilen SSH hizmetinin servis dışı kaldığı gözlenmiştir.

TABLO VII
IPV6-GO 6TUNNELDOS ÖRNEK UYGULAMASI

```
H4LINUX:~/6tunneldos# ./6tunneldos
Usage: 6tunneldos [-6] ip4/6 [port] [delay (ms)] [times]
H4LINUX:~/6tunneldos# ./6tunneldos 192.168.30.21
10001 10 25000
Started with ipv4 flood to 192.168.30.21 on 10001 for
25000 times!
Connection no. 0
Connection no. 1
Connection no. 2
Connection no. 3
Connection no. 4
Connection no. 5
Connection no. 6
…
```

2) Imps6-tools

Imps6-tools, hedef istemci port tarama ve hedef istemciye IPv6 paketi gönderme işlevlerini gerçekleştiren iki adet C programından oluşmaktadır.

IPv6-GO bünyesinde H8XP üzerinde Relay6 uygulaması 5555 numaralı porttan hizmet verecek şekilde çalıştırılmış, H1BSD üzerinde ise Imps6-tools uygulaması çalıştırılmıştır. Imps6-tools içinde yer alan tarama uygulaması scan6 programı, hedef H1BSD, taranacak port aralığı da 1 – 10000 olacak şekilde çalıştırılmıştır. Uygulama bu parametrelerle H8XP üzerinde açık port bulamamıştır. Uygulama, hedef istemci H8XP, hedef port aralığı 5555 – 5555 olarak çalıştırıldığında 5555 numaralı portun açık olduğunu tespit edebilmiştir. Imps6-tools içinde yer alan paket gönderme uygulamasından ise sonuç alınamamıştır.

D. Paket Düzeyindeki Saldırı Araçları

Yeni nesil internet protokolü ile IP paket yapısı değişmiştir. Bu değişiklik ile birlikte genişleme başlıkları (extension headers) tanımlanmıştır. Paketin temel özellikleri (kaynak adres, hedef adres vb.) dışındaki opsiyonlar genişleme başlıkları ile belirtilmektedir. IPv6 ağlarına yönelik tehditler yönlendirme başlığı saldırısı, parçalanmış paket saldırısı, ICMPv6 keşif saldırıları ve çoklu gönderim keşif saldırılarını içermektedir [36]-[37]. Bu saldırılar istenilen özelliklerde paket üreten araçlar ile uygulanabilmektedir. Bu araçlar aynı zamanda ağın belirli bir saldırıya karşı açık olup olmadığını, güvenlik duvarı kurallarını ve saldırı tespit sistemlerini test etmek amacıyla da kullanılabilmektedir.

1) Scapy

Scapy [38]; paket göndermek, koklamak, analiz etmek amacıyla, Python programlama dili ile yazılmış bir araçtır. Uygulamanın çalışması paket gönderme ve gelen cevapları görüntüleme mantığı üzerine oturtulmuştur. Scapy kullanılarak bir paketler bütünü oluşturulur ve gönderilir. Gelen cevaplar Scapy tarafından eşleştirilir ve kullanıcıya eşleştirilen ve eşleştirilmeyen cevaplar gösterilir. Diğer saldırı araçlarından farkı, gelen cevapları olduğu gibi görüntülemesi ve yorumlamamasıdır.

IPv6-GO bünyesinde Scapy örnek uygulaması (Tablo VIII) H1BSD ve H8XP kullanılarak gerçekleştirilmiştir. Bu örnekte Scapy kullanılarak H1BSD üzerinden kaynak IPv6 adresi sahte IPv6 adresi olan bir ICMPv6 Echo Request paketi H8XP 'ye gönderilmiştir. H8XP bu paketi aldığında, sahte IPv6 adresine ICMPv6 Echo Reply paketi ile cevap vermiştir.

2) ISIC

ISIC (IP Stack Integrity Checker) [39], mevcut IP yığınını ve yığın bileşenlerini (TCP, UDP, ICMP vb.) test etmek için hazırlanmış bir araçtır. Uygulamanın 0.07 numaralı versiyonundan itibaren IPv6 desteği sunulmaktadır. ISIC ile

rastgele paket kümeleri oluşturulabilir ve bu paket kümeleri IP yığınını veya güvenlik duvarı kurallarını test etmek amacıyla kullanılabilir. ISIC uygulamasına verilen parametreler ile oluşturulacak rastgele paketlerin içeriği belirlenebilir. Paketlerin %10 'unun parçalanmış paket olması, %15 'inin geçersiz genişletilmiş başlık opsiyonu içermesi oluşturulabilecek paket içerikleri örneklerindendir.

IPv6-GO 'da ISIC uygulaması, ağa geçersiz Hop-by-Hop opsiyonu içeren paketler basılması ile örneklenmiştir. Bu uygulamada paketler H1BSD 'den, H8XP'ye gönderilmiştir. Aynı senaryo ile eğer istenirse sahte IPv6 adresi kullanımı da mümkündür. Gerçekleştirilen örnek uygulamanın çıktısı Tablo IX 'de verilmiştir. Bu örnekte kullanılan komutta yer alan –m 5 argümanı maksimum 5KBps veri gönderileceğini, -H 100 argümanı gönderilecek paketlerin %100 'ünün geçersiz Hop-by-Hop opsiyonu içereceğini, -F 0 –V 0 –P 0 argümanları ise gönderilen paketlerin hiçbirinin parçalanmış paket, geçersiz versiyon numarası veya rastgele veri içermeyeceğini belirtmektedir.

TABLO VIII
IPV6-GO SCAPY ÖRNEK UYGULAMASI

```
[root@H1BSD /usr/ports]# scapy
Welcome to Scapy (2.1.0)
>>> realsrc='2001:a98:fe8:1::3'
>>> spoofsrc='2001:a98:fe8::6'
>>> dest='2001:a98:fe8::4'
>>> spoofpkt=IPv6(src=spoofsrc,
dst=dest)/ICMPv6EchoRequest()
>>> ans,unans=sr(spoofpkt,timeout=1)
Begin emission:
…
Finished to send 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
```

3) THC IPv6 Saldırı Aracı

THC IPv6 Saldırı Aracı [40], IPv6 yerel ağ saldırılarını yapmaya yarayan bir yazılımdır. Araç, IPv6'nın yerel ağında kullanılan ve genel olarak "komşu keşfi" [41] olarak adlandırılan süreçteki açıklardan [42] faydalanmaktadır. Bu programların içerdiği saldırılardan bazıları aşağıda açıklanmıştır:

- Alive6: Yerel ağdaki IPv6 istemcilerinin keşfi için yazılmıştır. Ağa çoklu gönderim mesajı göndererek gelen cevaplara göre çalışan düğümleri tespit etmeye çalışmaktadır.
- PARSITE6: Yerel ağda, sahte komşu keşfi mesajları göndererek ortadaki adam saldırısı gerçekleştirmek mümkündür.
- FAKE_ROUTER6: Bu aracı kullanarak yerel ağda sahte yönlendirici gibi davranarak trafiği izlemek mümkündür.
- DETECT-NEW-IPv6: Yerel ağa yeni dâhil olan IPv6 istemcilerini tespit etmek için kullanılmaktadır.
- DOS-NEW-IPv6: Ağa yeni bağlanan istemcinin adres almak için gönderdiği adres tespiti mesajlarını cevaplayarak, IPv6 adresi almasını engellemek için kullanılmaktadır.

THC IPv6 saldırı aracında yer alan programlar, IPv6-GO test ağı bünyesinde uygulanmıştır. Alınan sonuçları ve sonuçlarla ilgili analizi içeren bir bildirinin ilerleyen tarihlerde yayınlanması planlanmaktadır.

TABLO IX
IPV6-GO ISIC ÖRNEK UYGULAMASI

```
[root@H1BSD /usr/ports/net-mgmt/isic]# isic6 -s
2001:a98:fe8:1::3 -d 2001:a98:fe8::4 -m 5 -H 100 -F 0 -V 0
-P 0
Compiled against Libnet 1.1.2.1
Installing Signal Handlers.
Seeding with 88675
Maximum traffic rate = 5.00 k/s
Bad IP Version  = 0%          Odd Payload Length      = 0%
Frag'd Pcnt     = 0%       Bad Hop-by-Hop Options  = 100%
 1000 @ 499.6 pkts/sec and 489.4 k/s
 2000 @ 499.5 pkts/sec and 484.0 k/s
 3000 @ 499.5 pkts/sec and 476.4 k/s
 4000 @ 499.5 pkts/sec and 479.5 k/s
 5000 @ 499.5 pkts/sec and 479.0 k/s
 6000 @ 499.5 pkts/sec and 493.3 k/s
 7000 @ 499.5 pkts/sec and 484.7 k/s
^C
Caught signal 2
Used random seed 88675
Wrote 11276 packets in 22.57s @ 499.55 pkts/s
```

IV. SONUÇ VE DEĞERLENDİRME

IPv6 desteği verilmiş ağlardaki cihazların güvenlik testleri bu çalışmada anlatılan saldırı araçları kullanılarak gerçekleştirilebilir. Örneğin güvenlik duvarı kuralları ve erişim kontrol listelerini test etmek için paket düzeyindeki saldırı araçları kullanılabilir. Bunun yanında, tek noktada arıza riski taşıyan ağ cihazlarının performansı servis dışı bırakma saldırı araçları ile ölçülebilir. Çalışmada belirtilen saldırı araçları kullanılarak gerçekleştirilen saldırılardan çıkacak sonuçlar dâhilinde ağ cihazlarında ve güvenlik donanımında gerekli iyileştirmeler yapılmalıdır.

IPv6 desteği verilmemiş yalın IPv4 ağlarında saldırganlar, IPv4 paketi içine sarmalanmış IPv6 paketi benzeri tünelleme tekniklerini ve diğer yöntemleri kullanarak IPv6 desteği olan istemcilere ulaşabilmektedirler. Bu tip saldırılara özellikle kurulumda IPv6 desteğini otomatik olarak aktive eden Windows işletim sistemi kullanan cihazlar maruz kalmaktadır. IPv6 desteğinin otomatik aktive edildiği cihazlar, ağda kullanıcının ve ağ yöneticisinin kontrolü dışında IPv6 trafiği oluşmasına yol açmaktadır. Bu sebeple IPv6 desteği olmayan bir ağ, IPv6 protokolünü kullanan saldırı araçlarına karşı güvenlidir önermesi yanlıştır.

IPv6-GO test ağında uygulanan senaryolarda görüldüğü üzere, farklı araçlar kullanıldığında, kurban ve saldırganın ağdaki pozisyonu değişmektedir. Bu durum farklı ağ yapılarının çeşitli araçlar kullanılarak saldırıya uğrayabileceğine işaret etmektedir. Bu nedenle, IPv6 protokolünü göz ardı etmek yerine, IPv6 protokolünün ağdaki varlığı kabul edilmeli ve ağın güvenliği bütün olarak sağlanmalıdır. İlk adım olarak ağdaki cihazların IPv6 desteği olup olmadığı, varsa hangi seviyede IPv6 desteği verdiği incelenmelidir.

Çalışmanın, IPv6 farkındalığı ve kullanımının arttığı dönemde, IPv6 güvenliğine dikkat çekeceği öngörülmektedir. IPv6 açıkları ve bu açıkları kullanan saldırı araçları hakkında bilgi sahibi olan ağ ve sistem yöneticileri, bu saldırılara karşı ağı daha güvenli hale getirebilir. Bu saldırılara ve saldırı araçlarına karşı alınabilecek güvenlik önlemleri gelecek çalışmalarda incelenmesi öngörülen alanlar arasında yer almaktadır.

REFERANSLAR

[1] J. Postel, "INTERNET PROTOCOL", RFC 0791, September 1981

[2] S. Deering ve R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998

[3] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000

[4] TÜBİTAK - ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi, "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi", http://www.ipv6.net.tr/

[5] Emre YÜCE, Yavuz GÖKIRMAK, Onur BEKTAŞ, Serkan ORCAN, "IPv6 Geçiş Yöntemleri Güvenlik Analizi", 3. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu, Aralık 2009, İstanbul

[6] Şeref Sağıroğlu, Onur. Bektaş, Murat Soysal, "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması", 3.Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008, Ankara, Sayfa 132-138

[7] Microsoft security bulletin ms06-064 , "Vulnerabilities in TCP/IP IPv6 could allow denial of service"

[8] Caicedo, C.E.; Joshi, J.B.D.; Tuladhar, S.R.; , "IPv6 Security Challenges", Computer , vol.42, no.2, pp.36-42, Feb. 2009

[9] Jae-Deok Lim; Young-Ho Kim; Ki-Young Kim; , "Packet Filter Algorithm to prevent the security hole of routing header in IPv6", SICE-ICASE, 2006. International Joint Conference , vol., no., pp.3924-3927, 18-21 Oct. 2006

[10] Kyeong Yoo, Ray Hunt, "Implementation of an IPv6 multicast firewall testbed", Computer Communications, Volume 29, Issue 16, More Than a Protocol for Next Generation Internet, 12 October 2006, Pages 3079-3091, ISSN 0140-3664, DOI: 10.1016/j.comcom.2005.11.009.

[11] Choudhary, A.R.; , "In-depth analysis of IPv6 security posture", Collaborative Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on , vol., no., pp.1-7, 11-14 Nov. 2009

[12] Martin, Cynthia E.; Dunn, Jeffrey H.; , "Internet Protocol Version 6 (IPv6) Protocol Security Assessment", Military Communications Conference, 2007. MILCOM 2007. IEEE , vol., no., pp.1-7, 29-31 Oct. 2007

[13] S. Convery, D. Miller, "Cisco IPv6 and IPv4 threat comparison and bestpractice evaluation (v1.0)"

[14] D. Zagar, K. Grgic, R.Snjezana, "Security aspects in IPv6 networks implementation and testing," Computers and Electrical Engineering, vol. 4, page 425-437, September 2007

[15] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004

[16] K. Elgoarany, M. Eltoweissy, "Security in mobile IPv6 a survey," Information Security Tech. Report, vol 4, sayfa 32-43, Ocak. 2007

[17] T. Aura, "Mobile IPv6 Security," Microsoft Research Ltd. http://research.microsoft.com/users/tuomaura/publications/auraprotocols02.pdf

[18] Min-Shiang Hwang, Cheng-Chi Lee, Song-Kong Chong, "An improved address ownership in mobile IPv6", Computer Communications, Volume 31, Issue 14, 5 September 2008, Pages 3250-3252

[19] Geon-Woo Kim; Jong-Wook Han; Dong-Il Seo; , "Mobile IPv6 security while traversing a NAT", Networks, 2003. ICON2003. The 11th IEEE International Conference on , vol., no., pp. 331- 335, 28 Sept.-1 Oct. 2003

[20] P. Savola, C. Patel, "Security Consideration for 6to4", RFC 3964, December 2004

[21] Sabir, M. R., Fahiem, M. A., and Mian, "An Overview of IPv4 to IPv6 Transition and Security Issues", In Proceedings of the 2009 WRI international Conference on Communications and Mobile Computing - Volume 03 (January 06 - 08, 2009). CMC. IEEE Computer Society, Washington, DC, 636-639

[22] Taib, A.H.M., Budiarto, R., "Security Mechanisms for the IPv4 to IPv6 Transition", Research and Development, 2007. SCOReD 2007. 5th Student Conference on , vol., no., pp.1-6, 12-11 Dec. 2007

[23] Koutepas, Georgios; Douitsis, Athanasios; Philippides, Demetris; Maglaris, Vasilis; , "An Approach for the Administration and Security of IPv6 Transition Mechanisms: An SNMP MIB for 6to4", Computing in the Global Information Technology, 2006. ICCGI '06. International Multi-Conference on , vol., no., pp.10-10, Aug. 2006

[24] Dunn, J.H.; Martin, C.E.; , "Notional Security Architecture for the Department of Defense (DoD) Networks Transitioning to Internet Protocol Version 6 (IPv6)", Military Communications Conference, 2006. MILCOM 2006. IEEE , vol., no., pp.1-7, 23-25 Oct. 2006

[25] Mackay, M.; Edwards, C.; Dunmore, M.; Chown, T.; Carvalho, G.; , "A scenario-based review of IPv6 transition tools," Internet Computing, IEEE , vol.7, no.3, pp. 27- 35, May-June 2003

[26] C. A. Potyraj, "NSA Firewall Design Considerations for IPv6," http://www.nsa.gov/snac/downloads_all.cfm

[27] D. Zagar, K. Grgic, "IPv6 security threats and possible solutions," World Automation Congress, 2006

[28] Onur BEKTAŞ, Emre YÜCE, Neşe Kaptan KOÇ, İlknur GÜRCAN, Serkan ORCAN, "IPv6-GO Test Ağı Kurulumu", 3. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu, Aralık 2009, İstanbul

[29] T. Chown, "IPv6 Implications for Network Scanning", RFC 5157, March 2008

[30] A. Kamra, H. Feng, V. Misra, A. Keromytis, "The effect of DNS delays on worm propagation in an IPV6 Internet", Proceedings of IEEE Infocom, Miami, 2005, 2405- 2414

[31] NMap Ağ Keşif ve Tarama Uygulaması http://nmap.org

[32] MTR ağ analiz aracı http://www.bitwizard.nl/mtr/

[33] Relay6, Windows TCP yansıtıcı, http://sourceforge.net/projects/relay6/

[34] 6tunnel, NT6tunnel port yansıtıcı, http://toxygen.net/6tunnel/

[35] Y. Xinyu, M. Ting, S.Yi, "Typical DoS/DDoS threats under IPv6", Computing in the Global Information Technology, Guadeloupe, 2007, 55-61

[36] P. Savola, "IPv6 Routing Header and Home Address Options Internet draft", http://www.6net.org/publications/standards/draft-savola-ipv6rhha-security-03.txt

[37] J. Lim, Y. Kim, "Protection algorithm against security holes of IPv6 routing header", Advanced Communication Technology , vol l3, sayfa 2004 -2007, Şubat. 2006

[38] Scapy paket oluşturma, gönderme ve analiz aracı, http://secdev.org/projects/scapy

[39] ISIC (IP Stack INtegrity Checker) http://isic.sourceforge.net/

[40] THC IPv6 Saldırı Aracı http://freeworld.thc.org/thc-ipv6/

[41] T.Narten, E.Nordmark ve W.Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998

[42] P. Nikander, J. Kempf ve E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threat", RFC3756, May 2004