TÜBİTAK ULAKBİM

IPv6 ve Güvenlik Duvarı

IPv6 Geçiş Eğitimi

İÇERİK

1. Güvenlik ve Tehditler
2. Güvenlik Çözümleri
   - Paket Filtreleme / Erişim Kontrol Listeleri
   - Durum Denetimli Filtreleme
   - Limitleme / Trafik şekillendirme
   - L7 Çözümler
3. Genel Güvenlik Uygulamaları
   - Hangi IPv6 Adresleri, Uzantı Başlıkları Filtrelenmeli
   - UYGULAMA 4.1: Sahte Yönlendirici Koruması
   - ICMP Mesajlarının Filtrelenmesi
   - UYGULAMA 4.2: Windows Sunucu
4. Örnek Güvenlik Duvarı Kuralları
   - UYGULAMA 4.3: Linux Sunucu
   - UYGULAMA 4.4: BSD Yönlendirici / Güvenlik Duvarı

1. GÜVENLİK ve TEHDİTLER

- Genel Tehditler
- Uygulama tabanlı saldırılar
  - Uygulama açıkları, Sql Enjeksiyon
  - Şifresiz iletişim / bilgi kaybı
- Ağ saldırıları
  - DDoS
  - Sahte IP - IP Spoofing
  - Sahte Yönlendirme
- Virüs/Trojan, MitM, vb..

GÜVENLİK ve TEHDİTLER

Yeni Tehditler

- Sahte Yönlendirici (Fake Router)
- IPv6 özelliklerini kullanarak yapılan Keşif Çalışmaları
- NS/NA Mesaj Kandırmacası (Spoofing)
- IPv6 özellikleri ile Servis Dışı Bırakma Saldırısı
  - Komşu Keşfi (Neighbor Discovery) DoS
  - Yönlendirici İlanı (RA) DoS
  - Duplicate Address Detection DoS Attack
- Başarısız Komşu Erişilemezlik Denetimi (Neighbor Unreachability Detection (NUD) failure)
- Ağ Parametreleri Kandırmacası (Parameter Spoofing)

GÜVENLİK ve TEHDİTLER

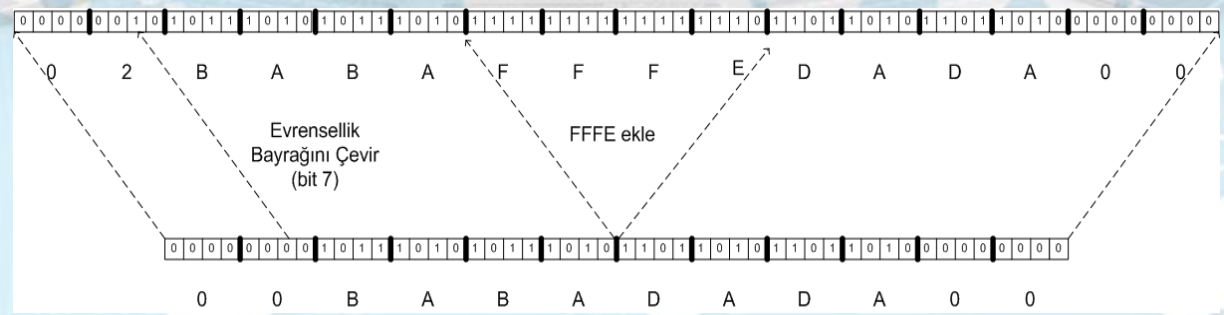
Yasal Yükümlülükler

- **5651 Sayılı Kanun**

  İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

  Uygulama Yönetmelikleri

- **Log (GET/POST) (Yer Sağlayıcı, İçerik Sağlayıcı)**
- **Adres Dağıtımı (Yer Sağlayıcı, İnternet Toplu Kullanım Sağlayıcı)**
  - **Statik**
  - **Otomatik – Durum Denetimsiz (EUI-64 kullanıldığı durumlarda)**



  - **“netsh interface ipv6 set global randomizeidentifiers=disabled”**
  - **Otomatik – Durum Denetimli (DHCPv6)**

GÜVENLİK ve TEHDİTLER

IPSec

- **IPv6 tasarımı içerisinde desteği var.**
  - **ESP ve AH kullanımı ile, IP seviyesinde şifreli iletişim!.**
- **Kullanımı zorunlu değil.**
- **Destekleyen uygulama az.**
  - **VPN**

:

2. GÜVENLİK ÇÖZÜMLERİ

- Paket Filtreleme / Erişim Kontrol Listeleri
- Durum Denetimli Filtreleme
- Limitleme / Trafik şekillendirme
- L7 Çözümler

:

Paket Filtreleme

- En basit güvenlik duvarı
- Giriş veya çıkış yönünde, bir protokolün belirli bir portunun belirli IP adresleri için engellenmesi
- Örnek 1: TCP ve UDP protokollerinin 137-139 portları
- Örnek 2: Web sunucusunun, 80 (http) ve 443 (https) portlarına izin verilip diğer servis portlarının engellenmesi

Durum Denetimli Filtreleme

- İletişimin kim tarafından başlatılacağının belirlenmesi
- Port engellemek ağı kısıtlar
- NAT ile gelen alışkanlıkların yerine geçer

:

Limitleme

- Engelleme ama limitle!
  - ICMP

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-request -m limit --limit
900/min -j ACCEPT

ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-reply -m limit --limit
900/min -j ACCEPT
```

- DDoS'tan korun
  - İstemci başına SYN bağlantı limiti

L7 ÇÖZÜMLER

- Durum korumalı GD: İstemci – Sunucu mimarisi
- İstemci-İstemci mimarisi:
  - Aktif FTP, Torrent, SIP, RTSP vb.
- Geniş Adres/port aralıklarına izin verilmeli.
- GÜVENLİK ZAAFİYETİ!.
  - Trafiği izle, içeriği kontrol et
  - Kötü trafiği işaretle, düşür, iletişimi kes.
  - DPI, IPS, L7 FW

L7 ÇÖZÜMLER

- Snort-inline (IPS)
- ALG (Application Layer Gateway)
  - Windows Firewall
    - Windows 2008 Server / Win7 / Vista
    - Uygulamanın, içeri veya dışarı doğru, tercih edilen ağdan trafik oluşturmasına izin ver/ engelle

:

3. GENEL GÜVENLİK UYGULAMALARI

- Korunacak olan ağın, istemcinin veya sunucunun ihtiyaçları göz önüne alınarak, sadece kullanılan servislere ait protokole ve portlara izin verilmeli, geri kalan her şey engellenmelidir.
- Güvenlik duvarı bir istemci veya sunucu üzerinde ise yönlendirici paketleri engellenmelidir.
- Yönlendiriciler üzerinde ise, yönlendirilecek ağın haricinde çıkışa ve girişe izin verilmemelidir.

3. GENEL GÜVENLİK UYGULAMALARI

- İstemciler arası kullanılan protokollere izin verilecek ise DPI (L7) uygulamaları kurulmalı, uygulama seviyesinde paket incelemesi ile filtreleme yapılmalıdır.
- Güvenlik, iletişim zincirinde yer alan tüm öğelerde ele alınmalıdır.

  İstemcilerde ve sunucularda Güncel İşletim Sistemi ve ihtiyaca uygun güvenlik duvarı ve virüs/trojan programı uygulanmalıdır.

  Ağ Cihazlarında yönetim ağı kurulmalıdır. Ayrıca;

  Telnet -> ssh

  Rsh, ftp -> ssh, sftp, scp

  SNMPv2c -> SNMPv3

  Yetkilendirilmiş yönlendirme protokolleri (acl, md5, sha)

3. GENEL GÜVENLİK UYGULAMALARI

- Yeni tehditlere yeni önlemler alınmalıdır:
  - ICMPv6
  - Sahte Yönlendirici
  - Çoklu Gönderim
  - Uzantı Başlıkları
    - Yönlendirme Başlığı (RH) Tip0
  - Yarın?

ICMPv6

- ICMPv6 paketlerinin tamamını filtrelemek IPv6 protokolünün sağlıklı çalışmasını engeller.

Mesaj Tipi	Mesaj Adı
1	Hedef Erişilemez
2	Paket Çok Büyük
3	Zaman Aşımı
4	Parametre Problemi
133	Yönlendirici Talebi
134	Yönlendirici İlanı
135	Komşu Talebi
136	Komşu İlanı

- Ağda verilmeyen servislere ait ICMPv6 mesaj tiplerinin ağa girmesine izin verilmesi güvenlik açıklarına neden olacaktır.
- Bazı tipler iç ağa izin verilebilir, dışarıdan erişim engellenebilir.

ICMPv6 Filtre Önerisi

ICMPv6 Tipi		İçeriye	Dışarıya	Açıklama
1	Hedef Erişilemez	İzin ver	Engelle	Ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. Dışarıya doğru sadece güvenilir ağlara izin verilmelidir.
2	Paket Çok Büyük	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
3	Zaman Aşımı	İzin ver	Engelle	İzin verilmesi gerektiği önerilse de, ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. Dışarıya doğru sadece güvenilir ağlara izin verilmelidir.
4	Parametre Sorunu	İzin ver	İzin ver / Engelle	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
128	Yankı İsteği	Engelle	İzin ver	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
129	Yankı cevabı	İzin ver	Engelle	İç ağın haritasını çıkarmak ve tespit etmek için kullanılabilir. İstemciler için engellenmelidir, ağ cihazları için açılabilir.
130-132	MLD	Engelle	İzin ver	İç ağda ihtiyaç duyulur, dışarıya engellenebilir.
135-136	ND	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
133-134	RD	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
135	Redirect	İzin ver	İzin ver	Ağın sağlıklı çalışması için gereklidir.
139-140	Düğüm Bilgisi Sorgusu	Engelle	Engelle	Uygulamada henüz kullanım alanı az olduğundan, kapatılabilir.
141-142	Ters komşu keşfi	Engelle	Engelle	Uygulamada henüz kullanım alanı az olduğundan, kapatılabilir.
144-147	Dolaşılabilirlik başlıkları	Engelle	Engelle	Dolaşılabilirlik desteği vermedi iseniz, kapatılmalıdır.

Sahte Yönlendirici

- Bir saldırganın yerel ağda kendini düğümlere bir yönlendirici olarak tanıtabilmesi durumunda birçok yeniden yönlendirme, ortadaki adam (MitM) ve DoS atağı yapabilir.
- Sahte yönlendirici olmak isteyen bir saldırgan, ağdaki bütün düğümlere ya da -bir düğümden gelen yönlendirici talebine karşılık- tek düğüme "yönlendirici ilan" mesajı gönderir.
- SEND (Secure Neighbour Discovery)

Sahte Yönlendirici – RD Mesajları

- Sahte Yönlendirici İlanı Mesajlarını engellemek için
  - ICMPv6 134, sadece resmi yönlendiriciden gelsin.
    - 2. seviyede destekleyen anahtarlar var.
  - Sahte ilanlar için (L2 de kapatılamıyorsa)
    - İstemcilerde güvenlik duvarı kuralı girilebilir.
      - (RA adresi / aralığı tanımlanabilir)
    - Ağa talep (133) göndererek, cevap verenler dinlenir.

      Sahte ilan yayınlayanlar tespit edilir, engellenir.
- IPv6 kullanmadığınız bilgisayarlarda, desteğini de kapatın.

Sahte Yönlendirici

UYGULAMA 4.1: İSTEMCİ GÜVENLİĞİ

Topolojilerinizde ***Yalın IPv6 ağında*** bulunan ve otomatik adres yapılandırması ile adres alan ***6 numaralı Windows 7 bilgisayarında,*** sahte yönlendirici ilanlarından korunmak için:

1. Resmi yönlendiricinin ilan yaptığı adresi bulun.
2. 6 numaralı bilgisayarın güvenlik duvarındaki ilgili kuralı değiştirerek, ***"sadece yönlendiriciden gelen RA mesajlarını kabul eden"*** güvenlik duvarı kuralı girin.

Uygulama kağıdına bakmadan yapmaya çalışın, takıldığınız yerde kontrol edin.

KONTROL: 6'daki arayüzü *disable-enable* yapın, IPv6 aldığını görün.

UZANTI BAŞLIKLARI

- Dolaşılabilirlik başlığı, eğer iç ağda dolaşılabilirlik desteği verilmiyor ise engellenebilir.
- Yönlendirme başlığı RH için, Tip 0 kullanımında tespit edilmiş güvenlik açıkları bulunmaktadır.
  - Tip 0 kaynağın yolladığı paketin rotasını tanımlamasını sağlar.
  - Tip 1 kullanım dışı olarak tanımlanmış,
  - Tip 2 ise Dolaşılabilirlik uygulaması için Tip 0 filtrelemesi amacıyla tanımlanmıştır.

UZANTI BAŞLIKLARI - RH Tip 0

- Tip 0 işlenmemelidir (kernel).
- Ağ cihazlarında düşürülmelidir.

İşletim Sistemi	Yöntem
Cisco IOS	no ipv6 source-route
Linux	Kernel 2.6 dan itibaren kaldırılmıştır. Yönlendirici olması durumunda paketleri engellemek için, kural listesinin başına aşağıdaki kurallar eklenir: **ip6tables -A INPUT -m rt--rt-type 0 -j DROP** **ip6tables -A FORWARD -m rt--rt-type 0 -j DROP** **ip6tables -A OUTPUT -m rt--rt-type 0 -j DROP**
FreeBSD	Kernel 6.2'den itibaren kaldırılmıştır. Eski çekirdekler için yama: http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet6/route6.c.diff?r1=1.12&r2=1.13 Kapatmak için: **sysctl net.inet6.ip6.rthdr0_allowed=0**
OpenBSD	OpenBSD 4.0-stable için yama: ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/012_route6.patch OpenBSD 3.9-stable için yama: ftp://ftp.openbsd.org/pub/OpenBSD/patches/4.0/common/012_route6.patch

UYGULAMA 4.2: SUNUCU GÜVENLİĞİ

GÖREV 1: Topolojinizde ***Sunucular*** ağında ***8 numaralı sunucu*** olarak yer alan, DNS ve WEB servislerinin verildiği ***Windows 2008 sunucusuna*** IPv6 eğitim sınıfındaki sadece topolojilerin IPv6 ağından ping atılabilmesini, sınıf ağından atılamamasını sağlayın.
Topolojilerin IPv6 ağı: 2001:a98:1F::/48
Sınıf Bilgisayarları ağı: 2001:a98:11::/48

Yapılacak işlem: "echo–request" ICMP tipi için, giriş yönünde, 2001:a98:1F::/48 ağından izin veren **yeni bir kural girilmesi**.

KONTROL: Görev sonunda, sınıfta yer alan tüm topolojilerden 8 numaralı sunucunuza ping atılabilir olmalı***, 2001:a98:11::/48*** ağında yer alan sınıf bilgisayarlarından ise atılamamalıdır.

UYGULAMA 4.2: SUNUCU GÜVENLİĞİ

GÖREV 2: Topolojinizde ***Sunucular*** ağında ***8 numaralı sunucu*** olarak yer alan ***Windows 2008 sunucusu*** üzerinde koşan Web servisine, sadece ***sizin topolojinizdeki yalın IPv6 ağından*** bağlanılsın, diğer ağlardan bağlanılamasın.

Yapılacak işlem: **a.** Yalın IPv6 ağ adresinizi bulun.
b. Sunucunun güvenlik duvarı üzerinde, giriş yönünde http trafiğine izin veren kuralı bulun, izin verilen aralığı, yalın IPv6 ağınıza daraltın.

KONTROL: Görev sonunda, 8 numaralı sunucudaki web servisine, sadece yalın IPv6 ağınızdan erişilebilmeli (7 numara), ikili yığın ağından erişilememelidir (5 numara).

GÜVENLİK DUVARI KURALLARI ÖNERİSİ

1. İç ağ adreslerinizi içeri kaynak yönünde engelleyin. İç ağınızdaki adreslerin dışarıdan gelmesi, sahte IP (spoofing) trafiği olarak tanımlanır, engellenmelidir.
2. İç ağ adresleriniz dışında kalan adresleri dışarı kaynak yönünde engelleyin.
3. Kullanmadığınız uzantı başlıklarını engelleyin.

- Dolaşılabilirlik uygulaması için kullanılan başlıkları dolaşılabilirlik servisini vermiyorsanız engelleyin.
- Yönlendirme başlığı tip 0 olan paketleri engelleyin.

GÜVENLİK DUVARI KURALLARI ÖNERİSİ

4. Tünelleme yapan iç ağ adresleriniz dışında kalan iç ağ aralığına, tünel adres aralıklarını engelleyin (6to4 aralığı: 2002::/16, Teredo 2001::/32).

5. Internet için ayrılan alanlar 2000::/3 ve küresel çoklu gönderim adresleri gibi, iletişimde bulunulacak IPv6 adres aralığı dışında kalan IP adreslerini engelleyin.

- **Eşsiz yerel tekil gönderim adresleri (fc00::/7).**
- **Rezerve edilmiş aralık (0::/8).**
- **Bağlantı Yerel Tekil (fe80::/10).**

GÜVENLİK DUVARI KURALLARI ÖNERİSİ

6. TCP, UDP, ICMPv6 ve ESP gibi, iç ağınıza dışarıdan erişilmesi gereken protokollere izin verin, kalan tüm protokolleri engelleyin.

7. Sunucularınızı ve servis portlarınızı tanımlayarak,

- a. Sunucular haricinde iç ağa dışarıdan iletişim başlatılmasını
- b. Sunucu servis portlarının haricindeki portlara iletişim başlatılmasını

engelleyin (durum koruması). Sunucuların servis portlarına izin verirken, DoS saldırılarından korunmak için, bağlantı limiti, servis verilen IP aralığı gibi kısıtlamalar uygulayın.

GÜVENLİK DUVARI KURALLARI ÖNERİSİ

8. Çoklu gönderim adreslerini belirleyerek, kapsam dışından gelen veya kapsam dışına çıkan paketleri engelleyin.
9. ICMPv6 başlıklarından sadece gerekli olanlarına izin verin, kalanını engelleyin.
10. İç ağdaki tüm IP adreslerinin dışarı doğru durum korumalı iletişim başlatmasına izin verin.

:

4. ÖRNEK GÜVENLİK DUVARI KURALLARI

Cisco IOS – ICMP ACL

```
ipv6 access-list sinir-yonlendirici-giris
remark belirli ICMP tiplerine giris yonunde izin ver
  permit icmp any 2001:a98:60::/48 destination-unreachable
  permit icmp any 2001:a98:60::/48 packet-too-big
  permit icmp any 2001:a98:60::/48 parameter-problem
  permit icmp any 2001:a98:60::/48 echo-reply
remark uzak agdan pinglenmesine izin ver
  permit icmp 2001:a98:20::/48 2001:a98:60::/48 echo-request
remark RD Haric, ND ve MLD ICMP tiplerine izin ver
  permit icmp any any nd-na
  permit icmp any any nd-ns
  permit icmp any any mld-query
  permit icmp any any mld-reduction
remark kalan ICMPleri engelle, kalan herseyi ac
  deny icmp any any log
  permit any any
```

4. ÖRNEK GÜVENLİK DUVARI KURALLARI

UYGULAMA 4.3

GÖREV: Topolojinizde Sunucular ağında ***10 numaralı sunucu*** olarak yer alan ***Ağ Yönetim Sunucusu*** üzerinde, ağ bilgilerinizi içeren önemli bilgiler bulunmaktadır. Sunucunun üzerindeki **ip6tables** güvenlik duvarını yapılandırarak, servislere başkalarının ulaşamamasını sağla.

Sunucuya ping atabilecekler: **2001:a98:1F::/48** (Tüm sınıf topolojileri erişebilsin, sınıf bilgisayarları ve İnternet'ten erişilemesin)
Web ve ssh servisine ulaşabilecekler: **2001:a98:11::/48** (Tüm sınıf bilgisayarları erişebilsin, sınıf topolojileri ve İnternet'ten erişilemesin)
Akış bilgisi gönderecek yönlendirici: Yönlendiricinin Sunucular Ağı'na bakan arayüzündeki (em1) IPv6 adresi olan **2001:a98:1F:____::1** adresinden gelen 9995 ile 9999 arası udp portlarını aç.

4. ÖRNEK GÜVENLİK DUVARI KURALLARI

UYGULAMA 4.4

GÖREV: ***1 numaralı yönlendirici*** olarak topolojinizin merkezinde yer alan BSD sunucu üzerinde,

a. pf kural listesini görüntüle

b. /etc/pf.egitim.conf içeriğini incele ve aktive et

c. Kuralların çalıştığını kontrol et.

: