TCP/IP Protokolü ve Zayıflıkları

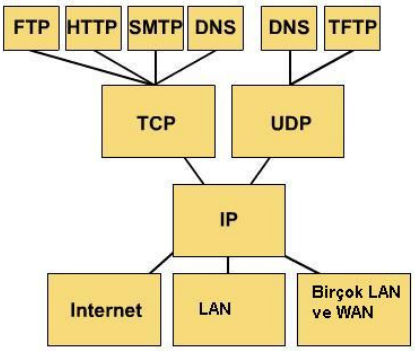
Ar. Gör. Enis Karaarslan, enis.karaarslan@ege.edu.tr
Ege Üniversitesi Kampüs Network Yöneticisi

Şu an yaşamakta olduğumuz ağ güvenliği problemlerinin çoğu TCP/IP protokolünün güvenlik açıklarından kaynaklanmaktadır. Önlemler alabilmek için öncelikle IP protokolünü ve var olan sorunları anlamak gereklidir.

TCP/IP Protokolü Nedir?

TCP/IP, her geçen gün değişen, gelişen ve içinde birçok ağlararası iletişim (internetworking) protokolleri barındıran bir protokol yığıtıdır. Amerikan Savunma Bakanlığı tarafından nükleer savaş durumunda bile çalışabilecek bir sistem olarak tasarlanmıştır. Daha çok akademik ortamlarda geliştirilen bu protokol, firmalardan bağımsız olduğu için dünya çapında farklı sistemler arasında iletişim için (yani Internet'te) en yaygın kullanılan protokoldür. TCP/IP, Internet'i yaratan protokoldür dersek yanlış olmaz. TCP/IP Protokol yığıtı, OSI modelin 7 katmanına karşılık gelen 4 katmandan oluşmaktadır:

- **Uygulama:** OSI'nin son üç katmanlarına (5-6-7) karşılık gelir
- **Transport:** Güvenilirlik, akış (flow) kontrolü ve hata düzeltme gibi servis kalitesini belirleyen parametrelerle uğraşır. Bağlantılı (TCP) ve bağlantısız (UDP) servisleri içerir.
- **Internet:** Amaç izlenen yollardan ve ağlardan bağımsız olarak hedef cihaza veri iletiminin sağlanmasıdır. Yol (path) belirleme ve veriyi o yola yönlendirmek (routing) için paket anahtarlama bu seviyede yapılır. IP protokolü kullanılır.
- **Network Access:** OSI'nin ilk iki katmanına (1-2) karşılık gelir.



TCP/IP'de yaygın olarak kullanılan protokoller yandaki protokol grafiğinde verilmiştir. Uygulama seviyesinde bir ağ ortamında sıkça rastlayacağımız protokoller aşağıda belirtilmiştir:

- *FTP* - File Transfer Protocol
- *HTTP* - Hypertext Transfer Protocol
- *SMTP* - Simple Mail Transfer Protocol
- *DNS* - Domain Name System
- *TFTP* - Trivial File Transfer Protocol

TCP/IP modelinin Internet'i yaratan bir standart olması ve birçok protokolü bünyesinde bulundurması onu daha popüler yapmaktadır. OSI modelin özellikle ağ temellerinin eğitiminde bir rehber olduğu unutulmamalıdır. TCP/IP protokolü hakkında detaylı bilgi http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/ adresinden edinilebilir.

IP Protokolü ve IP Adresleme

Internet Protokolü (IP) bir ağda uçtan uca (end-to-end) veri yönlendirmesi için kullanılır. IP tanımlamaları 1982 yılında RFC 791'de yapılmıştır. Bu tanımlamalar IP adreslerinin yapısını da içerir. Şu an dünyada yaygın olarak IPv4 (IP version - sürüm 4) kullanılmaktadır. Bu yapı Internet üzerindeki herhangi bir cihaza (makina veya yönlendirici arayüzüne) 32 bit mantıksal adres sağlar.

Avrupa Bölgesi (region) için IP adreslerinin düzenlemeleri RIPE NNC (http://www.ripe.net) tarafından sağlanmaktadır. Azalan IP adresi aralığı yüzünden özel IP'lerin kullanımı artmakta ve IPv6'ya geçiş planları yapılmaktadır.
Özel adresler, Internet'e bağlanmayan, NAT (Network Address Translation) veya proxy sunucusu aracılığı ile Internet'e bağlanan cihazlarda kullanım için ayrılmıştır. Bu adresler (10.0.0.0/8, 172.16.0.0/16, 192.168.0.0 /16)dır.

IPsec

IPsec protokolü, hem IPv4 için hem de IPv6 için doğrulama (authentication), bütünlük (integrity) ve gizlilik (confidentiality) servisleri sağlamak için tasarımlanmıştır. Transport seviyesinde çalıştığı için uygulamalarda ek bir ayarlama yapmaya gerek yoktur (transparent). IPv4 ağlarına IPSEC eklemek için bu görevi üstlenecek bir ağ cihazı (router, VPN concentrator ... vb) veya ağ güvenlik duvarı kullanmak gerekmektedir. Kullanıcı da VPN client yazılımını makinasına kurmalıdır.
IPSEC'de güvenlik 2 mekanizma ile sağlanmaktadır:

- Authentication Header (AH): Veri doğrulama,veri bütünlüğü sağlamak için
- Encapsulated Security Payload (ESP): Veri gizliliği sağlamak, şifreleme için

Bu iki mekanizma tek başlarına kullanılabilecekleri gibi birlikte de kullanılabilir.

Var olan TCP/IP Zayıflıkları ve Çözümleri

Şu an kullanılan IPv4 protokolü tasarlanırken güvenlik dikkate alınmamıştır. Bunun sonucunda yaşanan zayıflıklar ve çözümler olarak aşağıdakileri belirtmek mümkündür:

Hedefe ulaşan veri, IP paketlerinden oluşmaktadır. Bu paketlerde:

- ***Gizlilik (Confidentiality):*** Paketin seyrettiği yol boyunca içeriği okunmuş olabilir. ***Önlem:*** İçeriğin şifrelenmesi. – Uygulama: IPsec
- ***Paket Doğrulama (Authentication):*** Paketin kaynak adresi değiştirilmiş olabilir. (Örn:spoof saldırıları) ***Önlem:*** Daha kuvvetli doğrulama yöntemlerinin kullanılması. – Uygulama: IPsec- AH
- ***İçerik bütünlüğü (integrity):*** Paketin içeriği değiştirilmiş olabilir. ***Önlem:*** Daha gelişmiş data bütünlüğü kontrollerinin yapılması. – Uygulama: IPsec - AH

IP protokolünün zayıflıkları kullanılarak servislere yönelik saldırılar yapılabilir:

- ***Flood Saldırıları:*** Protokolde trafik önceliğinin (priority) olmaması yüzünden ağa yönelik sel (flood) saldırıları. ***Önlem:*** Servis kalitesi(QOS), aktif cihazlarda ve güvenlik duvarlarında önlemler almak.
- ***DOS-DDOS Saldırıları:*** Sistemleri ve servisleri devre dışı bırakmak için yapılan saldırılar. ***Önlem:*** Güvenlik duvarı kullanmak, sistemlerde gerekli güncellemeleri düzenli olarak yapmak ve ilave güvenlik önlemleri almak, protokollerin yeni ve daha güvenli versiyonlarını kullanmaya başlamak.

IPv6

IPv6'nın tanımlamaları da tamamlanmak üzeredir. IPv6, daha büyük bir adres uzayı (128 bit adres), yönlendirme esnekliği, entegre servis kalitesi (QOS), otomatik konfigürasyon, mobil computing, "data multicasting" ve gelişmiş güvenlik özelliklerine sahiptir.
IPv6 'da IPSEC desteği bütünleşik olarak gelmektedir. Bu tür bir entegrasyon bu servislerin daha sorunsuz ve etkin çalışmasını sağlayacaktır. Örneğin ağ seviyesinde doğrulama ile paketin belirtilen kaynak adresinden gelip gelmediği tespit edilebilmektedir.
Detaylı bilgi http://www.ipv6.org adresinden elde edilebilir.

IPv6 Kullanımında Türkiye

Türkiye'deki üniversiteler arası ağ olan Ulakbim bünyesinde yapılan çalışmalarda IPv6 denemeleri yapılmış ve şu anda çalışan servislerin IPv6 üzerinde de çalışması sağlanmıştır. Ulakbim ağ yöneticilerinden Onur Bektaş'a bu konuda birkaç soru yönelttik.

- IPv6'ya tümden geçişin Ulakbim bünyesinde ne kadar süreceği düşünülmektedir? Dünyadaki diğer IPv4 ağlarıyla iletişim için dönüştürme nasıl yapılacaktır?

UlakNet bünyesinde IPv6'ya geçiş çalışmaları 2003 yılı başında, Bölgesel Internet Tahsis Kurumu olan RIPE organizasyonundan UlakNet için 2001:A98::/32 IPv6 adres aralığı alınmasıyla başlamıştır. 2004 yılının başında, bu adres aralığı kullanılarak UlakNet'e bağlı uçlara talepleri doğrultusunda IPv6 adresleri dağıtılmaya başlanmıştır. UlakNet'in global internetle IPv6 bağlantısı BGP4+ yönlendirme protokolü ile 1.5 senedir Avrupa Akademik Ağı GEANT üzerinden mevcuttur, şu anda Ulakbim'deki http, ftp, rsync, dns, web önbellekleme servisleri IPv4 yanında IPv6 olarak da kullanıcılara sunulmaktadır. IPv6'ya geçiş aşamasında önümüzdeki 3-4 sene boyunca omurganın ve uçlardaki birimlerin ikili-yığın (dual-stack) olarak çalıştırılması planlanmaktadır. Üniversitelere önerilerimiz IPv6'ya geçiş çalışmalarını ilk olarak sunucu sistemlerden başlayıp mevcut IPv4 ile verilen hizmetlerin IPv6 destekler hale getirildikten sonra son kullanıcı seviyesinde IPv6 desteği için uğraşmaları. IPv6'ya tümden geçişin işletim sistemi ve programların IPv6 desteğinin artmasıyla beraber kendiliğinden yavaş yavaş olabilecek bir konu olduğunu düşünüyorum. Tamamen IPv6'ya geçmek IPv4'den vazgeçilmesi anlamına geleceği için, bu konunun ne zaman olabileceği UlakNet yanında Türk Telekom ve diğer internet servis sağlayıcıların IPv6'ya geçiş planlarının ne olduğu ve ne kadar zamanda IPv6 destekler hale geleceklerine de bağlıdır. Bu nedenle zaman konusunda tahmin yapmak şu aşamada çok zor.

IPv6 ağlarının IPv4 ile konuşması için 6to4 ve 4to6 IP tünelleri kullanmak veya "6to4 relay router" gibi çözümler kullanılması gerekecektir.

- IPv6'da IPsec uygulamaları dışında, özellikle DOS-DDOS saldırılarını önlemeye yönelik ne tür düzenlemeler vardır?

IPv6 her ne kadar yapısında güvenlik konusunda bir çok yenilik getirse de Ulakbim bünyesinde IPv6'ya geçiş çalışmalarında gördüğümüz kadarıyla IPv6'ya geçiş aşamasında güvenliğin sağlanması konusu pratikte IPv6 kodlarının çoğunun deneysel olması, güvenlik duvarlarının protokolün tüm özelliklerini desteklememeleri vb sorunlar nedeniyle teoride olduğu kadar iyi çalışmamakta ve ekstra güvenlik riskleri doğurabilmektedir.

DOS-DDOS saldırıları açısından IPv4 ve IPv6'yı karşılaştırırken bu tip saldırıların yapılmasında temel teşkil eden smurf ve spoof saldırılarına yeni versiyon IP'deki durumları açısından bakmak gerekiyor. Her ne kadar RFC 2827'de spoof saldırılarından korunmak için önerilen ingress filtreleme tekniği IPv4'de mümkünse de, IPv6 adres yapısının çok kolay şekilde özetlenebilmesi filtrelemeleri çok daha kolay hale getirecek, örneğin UlakNet'in tüm IP'lerini temsil için 3 tane /16 adress yazmak yerine bir tane /32 adres yazmak yeterli olacaktır.

Smurf saldırıları açısından bakacak olursak RFC 2463'e göre ICMPv6'ya cevap mesajlarının hedef adresi IPv6 multicast, data-link seviye multicast ve broadcast adresi olamayacağı için smurf saldırılarının IPv6 dünyasında karşılıkları olmadığını söyleyebiliriz.

Bence pratikte DOS-DDOS saldırılarını önlemede IPv6'ya geçmenin en büyük avantajı, yeni kurbanlarını genelde mevcut adres aralığını tarayarak arayan saldırganların, yeni bilgisayar IP'lerini bulmakta karşılaşacakları zorluklardır. IPv6'da

pratikte kullanılan en küçük subnet /64 olduğu için bu subnette saldırılan bir bilgisayardan diğer bilgisayarları bulmak için 2^{64} olasılık olduğu anlamına geliyor ki bu saniyede 1.000.000 host tarasanız bile subnetteki tüm bilgisayarları bulmanızın 28.000 yıl alacağı anlamına geliyor. IPv4'de bu sayı genelde subnetler /24 olduğu için 2^8 yani 256 idi. Bu durumda saldırganların yeni yöntemler geliştirmeleri gerekecektir.

SONUÇ

- Kurum ağlarında mutlaka ağ güvenlik duvarı (firewall) kullanılmalı, saldırı tespit sistemleri gibi mekanizmalarla ağ sürekli olarak takip edilmelidir.
- IPsec veya IPv6 kullanılarak birçok zayıflıklardan korunmak mümkündür. IPv6'ya geçiş için işletim sistemleri ve telekominikasyon ağlarının olgunlaşmasını beklemek gerekecektir.
- Internet üzerindeki kaynaklardan yeni oluşabilecek zayıflıklar takip edilmeli ve önerilen çözüm yöntemleri kullanılmalıdır.
- TCP/IP üzerinde çalışan snmp gibi uygulama seviyesindeki protokollerin mümkün olduğunca en son sürümleri kullanılmalıdır.
- Telnet, SNMP'nin eski sürümleri gibi paketleri şifrelemeden gönderen protokollerin şifreleme destekleyen türevleri ssh, SNMPv3 kullanılmaya başlanmalıdır.