Ağ Cihazlarının Güvenliğinin Sağlanma Yöntemleri

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

ÖZET

Birçok kurum, bir güvenlik duvarı (*firewall*) aldığında güvenlik sorunlarının çoğunu çözdüğünü sanmakta ve diğer önlemleri önemsemektedir. Oysa güvenlik yönetimi ağ (*network*) üzerinde çalışan bütün elemanların güvenliğini içerir ve sürekli devam eden bir süreç olarak ele alınmaldır. Bu bildiride, ağ trafiğinin üzerinden aktığı ağ cihazlarında alınması gereken temel güvenlik önlemleri ele alınmış ve bazı ipuçları verilmiştir.

Ağ cihazlarında kurulum sırasında oluşan varsayılan (*default*) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir. Bu bildiride bütün TCP/IP ağları için geçerli ve firmadan bağımsız ayarlar hakkında bazı ipuçları verilmektedir. Uygulamalar Cisco cihazları üzerinde yapılmış ve doğru çalıştığı gözlenmiştir.

1. AĞ CİHAZLARI

Bilgisayar sistemlerinin birbirleriyle iletişim kurabilmeleri için veri sinyallerini kablo ile veya kablosuz (*wireless*) olarak iletmeleri gerekmektedir. Kablo ile veri iletilirken her bilgisayarın bağlantı kuracağı diğer bilgisayarlara ayrı ayrı kablolarla bağlanması, çok özel sistemler dışında efektif bir yöntem değildir. Yerel ağlarda birbirine yakın bilgisayarlar ortak bir cihaza bağlanmakta ve bu cihaz genelde hub veya switch olarak adlandırılmaktadır. Bu cihazların oluşturduğu ağ (*network*) ise internet'e bağlanmak için yönlendirici (*router*) cihazına gerek duymaktadır. Cihazlar OSI katmanının hangi seviyesinde çalıştıklarına göre L1 (1. Katman), L2, L3 veya yeni nesil (L1–L7) cihazlar olarak sınıflandırılmaktadır. Ağ cihazlarına diğer cihazların bağlandığı arabirimlere *port* denmektedir.

Ağ cihazları yönetim açısından, yönetilebilir (*managable*) veya yönetilemez (*unmanagable*) cihazlar olarak ikiye ayrılmaktadır. Bu bildiride yönetilebilir cihazların güvenlik ayarlarına değinilecektir. Yönetilebilir cihazların kendilerine özgü bir işletim sistemi ve konfigürasyonu bulunmaktadır. Cisco cihazlarda IOS ve CatOS, Alcatel XEON'larda XOS, Avaya cihazlarında Unixware, Juniper'de Free BSD örnek olarak verilebilir. Diğer cihazlarda da genelde UNIX tabanlı işletim sistemleri bulunmaktadır. Ağ cihazlarının ayarlanması, yönetimi ve kontrolü aşağıdaki şekillerde sağlanabilmektedir:

- HTTP protokolü ile,
- Telnet veya SSH ile,
- SNMP protokolü ile,
- TFTP veya FTP ile,
- Konsol portuyla.

Konsol portu aracılığıyla erişimde fiziksel güvenlik ön plana çıkmaktadır. Diğer erişim türlerinde ise TCP/IP protokolü kullanılacağından bu protokolün zayıflıklarına karşı önlem alınması gerekecektir.

Cihazların ayarları menüler aracılığıyla, komut (*command*) yazarak veya grafik arayüzlerle yapılabilmektedir. Cihazlarda kurulum sırasında oluşan varsayılan (default) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir.

2. FİZİKSEL GÜVENLİK

Cihaza fiziksel olarak erişebilen saldırganın konsol portu aracılığıyla cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya tap (özel ekipmanla kabloya erişim) ederek hattı dinleyebilir veya hatta trafik gönderebilir [1]. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir kıymeti bulunmamaktadır. Bazı fiziksel güvenlik önlemleri aşağıda verilmiştir:

- Cihazlar sadece ağ yöneticisinin veya onun yardımcısının açabileceği kilitli odalarda tutulmalıdır. Oda ayırmanın mümkün olmadığı yerlerde özel kilitli dolaplar (kabinetler) içine konmalıdır.
- Cihazlara fiziksel olarak kimin ve ne zaman eriştiğini belirten erişim listeleri tutulmalı (*access auditing*) ve bu listeler sık sık güncellenmelidir [2].
- Kablolar tek tek etiketlenmeli ve kayıtları tutulmalıdır. Kullanılmayan kablolar devre dışı bırakılmalıdır [3].
- Cihazların yakınına güvenlik bilgileri (şifre, IP adresi) gibi bilgiler yapıştırılmamalı ve gizli tutulmalıdır [3].
- Cihazlara fiziksel erişim mümkün ise kullanılmayan portlar disable edilmelidir [4].
- Aktif cihazların elektriği aldığı güç kaynaklarının yeri belirlenmeli ve saldırganın bu güç kaynaklarını kesmesi engellenmelidir. Devamlı güç kaynaklarına (ups) yatırım yapılmalıdır [2].
- Aktif cihazların fiziksel erişime açık olduğu yerlerde saldırganın güç kablosunu çıkartmasını engellemek için cihazın üstünde çeşitli aparatlar kullanmalı, güç kablosunu gözden ırak tutmalı, mümkünse uzakta ve fiziksel güvenliği sağlanan bir prize bağlanmalıdır [2].
- Her ne kadar aktif cihazların çalınması pek olası olmasa da bu tür olayları engellemek için mümkünse çeşitli kilit ve alarm mekanizmaları kullanılmalıdır [2].

3. ŞİFRE YÖNETİMİ

Şifreler cihazlara her türlü izinsiz erişim de hesaba katılarak iyi seçilmelidir. İyi şifrelerin özellikleri aşağıdaki gibidir [5]:

- Büyük ve küçük harf içerirler,
- Noktalama işaretleri ve rakamlar içerirler,
- Bazı kontrol karakterleri ve/veya boşluklar içerirler,

- Kolaylıkla hatırlanabilirler ve bu nedenle bir yere not edilme ihtiyacı duymazlar,
- En az yedi veya sekiz karakter uzunluğundadırlar,
- Kolay ve hızlı yazılırlar; ve böylece etraftan bakan birisi ne yazdığını anlayamaz.

Şifre yönetmenin en iyi yolu LDAP, TACACS+[1] veya RADIUS doğrulama (*authentication*) sunucuları aracılığıyla onay mekanizmasını kullanmaktır. Bu sistem kullanılsa bile yetkili (*privileged*) haklar için o cihaza yerel (*local*) tanımlı bir şifre, konfigürasyon dosyasında bulunmalıdır [6]. Birçok yönetilebilir cihaz, kullanıcı (user) modu ve yetkili (enable) mod gibi iki ayrı login mekanizmasına sahiptir. Kullanıcı modunda sadece arayüzler (interface) incelenebilirken yetkili modda ek olarak cihaz konfigürasyonu da yapılabilmektedir. Cisco cihazlarında girilen kullanıcı ve parolaların konfigürasyon dosyasında gözükmemesi için "*service password-encryption*" komutu girilmiş olmalıdır. Zayıf şifreleme algoritması kullanan "*enable password*" komutu yerine MD5-tabanlı algoritmayla şifreyi koruyan "*enable secret*" komutu kullanılmalıdır. "*no enable pass*word" komutu kullanılarak enable password'ler silinmeli yerine "*enable secret yeni_şifreniz* " ile yeniden şifreler girilmelidir.

4. CİHAZ ERİŞİM PROTOKOLERİNE DAİR AYARLAR

Ağ cihazlarının ayarlanması, yönetimi ve kontrolünde kullanılan HTTP, Telnet, SSH, SNMP, TFTP ve FTP; TCP/IP protokolünün alt elemanları olduklarından, bu protokolün zayıflıklarına karşı önlem alınması gerekmektedir. Bu türden erişimlerde denetim, bu cihazların ve dolayısıyla ağ trafiğinin güvenliği için çok gereklidir.

Belirli IP'lerin Cihaza Erişimine İzin Vermek

Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu da access-list yazılarak sağlanır. Örneğin Cisco IOS'de sadece 200.100.17.2 ve 200.100.17.3 IP'lerin erişimine izin verilmesi ve diğer ip'lerin engellenmesi aşağıdaki access-list ile sağlanmaktadır.

```
access-list 7 permit 200.100.17.2
access-list 7 permit 200.100.17.3
access-list 7 deny any log
```

Örnekte verilen 7 numaralı access-list belirtilen IP'lere izin vermekte (permit), diğer IP'leri kabul etmemektedir (deny). Bu access-list'in devreye girmesi için herhangi bir arayüzde etkin hale getirilmesi gerekmektedir. Telnet (veya ssh) için uygulanması da aşağıdaki gibi olmaktadır:

```
line vty 0 4
access-class 7 in
```

Http erişimi için kısıtlanması da aşağıdaki gibi olmaktadır:

```
ip http access-class 7
```

SNMP erişimine belirtilen IP'lerin izin verilmesi ise aşağıdaki gibi olmaktadır:

[1] TACACS+: Terminal Access Controller Access Control System Plus

snmp-server host 200.100.17.2 snmp_şifresi
snmp-server host 200.100.17.3 snmp_şifresi

HTTP Erişimi

HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir. Daha önceden de belirtildiği gibi HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IP'lere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir. Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

HTTP protokolünde doğrulama mekanizması ağda şifrenin düz metin şeklinde gönderimi ile sağlandığı için efektif değildir ama farklı üreticilerin değişik çözümleri bulunmaktadır. Doğrulama mekanizması, onay sunucuları (Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması "*ip http authentication*" komutuyla sağlanmaktadır.

Telnet ve Secure Shell (SSH) Erişimi

Telnet ile erişimlerde saldırganın ağ üzerinden dinlenme (sniff) yoluyla iletilen bilgiyi elde etmesi mümkün olduğundan, iletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmaldır. SSH şu anda bütün cihazlar ve cihaz işletim sistemleri tarafından desteklenmemektedir. Bu konuda üretici firmanın cihaz dökümantasyonu incelenmelidir.

SNMP Erişimi

Simple Network Management Protokol (SNMP), cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Trafik istatistiklerinden bellek ve CPU kullanımına kadar bir cihaz hakkında çok detaylı bilgiler edinilebilmektedir. Bir veya daha fazla Ağ Yönetim İstasyonu, üzerlerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan (server) bu istatistikleri toparlayacak (poll) şekilde ayarlanmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Router Traffic Grapher (MRTG) gibi programlar bulunmaktadır [7].

SNMP protokolünün, özellikle SNMP Version 1'in birçok uygulamasında zayıflık (vulnerability) olduğu CERT[2] 'in raporlarında belirtilmiştir [8]. Birçok cihaz üretecisi bu konuda yama (patch) çıkartmış ve önerilerde bulunmuştur [9] [10] [11]. SNMP Version 1, düz metin (clear text) doğrulama dizileri (string) kullandığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz

[2] CERT: Computer Emergency Response Team – http://www.cert.org

(*digest*) doğrulama şeması kullanan ve çeşitli yönetim verilerine kısıtlı erişim sağlayan SNMP Version 2'nin kullanılması gerekmektedir. Mümkünse her cihaz için ayrı bir MD5 gizli (*secret*) değeri kullanılmalıdır [1]. Daha detaylı bilgi için [12] incelenebilir.

Öneriler:

- Sadece Oku (*Read only*) ve Oku-Yaz (*Read-Write*) erişimleri için kullanılan varsayılan SNMP şifre (*community*) adları değiştirilmeli ve bu iki parametre birbirinden farklı olmalıdır.
- SNMP şifrelerine kritik bir UNIX makinasındaki root şifresi gibi davranılmaldır [4].
- SNMP erişimi hakkı sadece belirli güvenilir (*trusted*) IP'lere (Ağ Yönetim istasyonlarına) sağlanmalıdır.
- Ağ Yönetim İstasyonu tarafından SNMP erişimi yapılırken "Sadece Oku" parametresi kullanılmalıdır. Mümkünse cihazlarda "Oku-Yaz" parametresi iptal edilmelidir [4].
- Ağ Yönetimi için ayrı bir subnet, mümkünse VLAN[3] yaratılmalıdır. Access-list ve Ateş Duvarı (*firewall*) kullanılarak bu ağa dış ağlardan gelen trafik kısıtlanmalıdır.

Ağ Yönetim İstasyonları, ağdaki cihazlara ait SNMP şifre dizileri gibi doğrulama bilgileri bulundurdukları için doğal bir saldırı hedefi durumuna gelmektedir. Bu yüzden bu makinaların fiziksel, yazılımsal ve ağ güvenlikleri sağlanmalıdır.

Auxiliary Port

Yönlendiricilerde acil durumlarda telefon hatları üzerinden modem kullanılarak erişimin sağlanması için "Auxiliary port" bulunmaktadır. Bu tür bir erişim için PPP'de (Point to Point Protocol) PAP (Password Authentication Protocol) yerine CHAP (Challenge Handshake Authentication Protocol) doğrulama methodu kullanılmalıdır. CHAP, dial-up ve noktadan noktaya (point to point) bağlantılarda uç noktayı engelleyerek izinsiz erişimleri engellemektedir [13].

TFTP- FTP ile Erişim

Cihazlara yeni işletim sistemleri veya konfigürasyonları TFTP veya FTP gibi protokollerle yüklenebilmekte veya Ağ Yönetim İstasyonu'na yedek amaçlı alınabilmektedir. Özellikle TFTP protokolü, UDP kullanması ve kullanıcı-cihaz doğrulama sistemleri kullanmamasından dolayı bilinen bazı güvenlik açıklarına sahiptir [13]. Bu yüzden bu protokoller cihazlarda access-list ile kontrol altına alınmalı ve dosya transferi belirli IP'lerle sınırlandırılmalıdır. TFTP sunucu olarak kullanılan Ağ Yönetim İstasyonu'nda da bu protokolü kullanırken uygulayacağı ek güvenlik ayarları yapılmalı, mümkünse bu servis bu makinda sadece kullanılacağı zaman açılmalıdır. Cihaz FTP'yi destekliyorsa bu protokolün kullanılması tercih edilmelidir.

[3] VLAN: Virtual Local Area Network

5. KAYITLAMA (LOGGING) AYARLARI

Ağ cihazları çeşitli hadiseler (*event*) hakkında kayıtlama özelliğine sahiptir. Bu kayıtlar, güvenlik hadiselerinin belirlenmesinden ve önlem alınmasında kritik önem taşıyabilmektedir. Arayüzlerin durum değişikliği, sistem konfigürasyon değişikliği, access-list'lere takılan (*match*) bağlantılar gibi güvenlik açısından önemli olan bilgilerin kayıdı tutulabilmektedir. Cihazda kayıtlama aşağıdaki şekillerde yapılabilmektedir:

- SNMP Trap Logging: Sistem durumunda (*status*) karakteristik (*significant*) değişikliklerde Ağ Yönetim İstasyonuna uyarı (*notification*) göndermektedir.
- Sistem Kayıtlaması: Sistem konfigürasyonuna bağlı olarak hadiselerin kayıdını tutmaktadır. Sistem kayıtlaması farklı yerlere yapılabilmektedir:
    - Sistem konsoluna bağlı ekrana "*logging console*" komutuyla,
    - Üzerinde UNIX'in syslog protokolü çalışan ağdaki bir sunucuya "*logging ip-address*", "*logging trap*" komutlarıyla,
      Ör: *logging 200.100.17.2*
    - Telnet veya benzeri protokolle açılan VTY remote oturumlara (session) "*logging monitor*", "*terminal monitor*" komutlarıyla,
    - Yerel buffer olan RAM'ine "*logging buffered*" komutuyla yapılabilmektedir.

Kayıtlar düzenli olarak takip edilmeli ve sistemin düzgün çalışıp çalışmadığı kontrol edilmeldir. Farklı cihazlardan Ağ Yönetim İstasyonu'na gönderilen mesajların zamana göre senkronize olması için cihazlarda Network Time Protokol (NTP) çalıştırılmalıdır [4].

6. VLAN UYGULAMALARI

Virtual Lan (VLAN - sanal ağlar) kullanılarak kullanıcıları fiziksel lokasyonundan bağımsız olarak gruplamak, farklı subnetlerde toplamak mümkündür. VLAN'a almak tek başına bir güvenlik önlemi sayılmamakla beraber bir güvenlik artışı olmaktadır. Ağ Yönetimi için ayrı bir VLAN yaratılmalıdır. Bölgeler VLAN trafiklerine göre prunning yapılarak ayrılmalı, sadece o bölgede kullanılan VLAN'lar iletilmelidir.

VLAN bilgilerini ve bütün ağ trafiğini aktif cihazlar arasında taşımak için kullanılan cihaz port'ları "trunk" olarak tanımlanmaktadır. Trunk olmayacak port'ların trunk olarak tanımlanması o port'a bağlı cihazın bütün ağ trafiğini almasını sağlayacağından bu tür yanlış tanımlamalar mutlaka düzeltilmelidir [4].

Cihazların kullanılmayan portlarını L3 (OSI 3.katman) bağlantısı verilmemiş bir VLAN'a atamalı veya portlar "disable" edilmelidir [4]. Böylece saldırganın cihazın boş portuna girip ağa ulaşması engellenmiş olmaktadır.

Switch'in port numarasına, cihazın MAC[4] adresine veya kullanılan protokole göre dinamik VLAN ataması uygulanarak cihazların VLAN ve IP bilgileri tek noktadan

[4] MAC Adresi: Media Access Control Adresi, ethernet ağlarında ethernet kart adresi

kontrol edilebilmekte ve daha güvenilir ağ yapısı oluşturulmaktadır. Böylelikle sadece kayıtlı MAC adreslerine sahip cihazlar izin verilen ağlara ulaşabilmektedir.

VLAN kullanılan ağlarda ne tür zayıflıklar olabileceği SANS Enstitüsü tarafından incelenmiştir. Detaylı bilgi için bakınız [14].

7. ÇÖZÜM ve SONUÇLAR

Ağ güvenliği sadece bir güvenlik duvarı (*firewall*) alınarak sağlanamaz. Ağ Güvenliği Yönetimi'nin her zaman devam eden bir süreç olduğu unutulmamaldır. Ağa bağlı her elemanın güvenliği belirli seviyerlerde sağlanmalı ve sistem devamlı kontrol altında tutulmalıdır. Bu bildiride ağ trafiğinin üzerinden aktığı ağ cihazlarında alınması gereken temel güvenlik önlemleri ele alınmış ve ipuçları verilmiştir. Ağ Güvenliği konusundaki çalışmalarımız Ege Üniversitesi Güvenlik Grubu'nun web sayfasından (http://security.ege.edu.tr) takip edilebilir.

KAYNAKLAR

[1] Increasing security on IP Networks
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

[2] Why Is Physical Security Important?,Aron Hsiao, 2001, http://www.informit.com

[3] Pc Security Products, Physical Security
http://www.utoronto.ca/security/pcsecphy.htm

[4] SAFE: A *Security* Blueprint for *Enterprise* Networks, Sean Convery , Bernie Trudel, 2000,
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

[5] Şifre Seçimi, Ege Üniversitesi Network Güvenlik Grubu,
http://security.ege.edu.tr/dokumanlar.php

[6] Improving Security on Cisco Routers,
http://www.cisco.com/warp/public/707/21.html

[7] Multi Router Traffic Grapher,
http://people.ee.ethz.ch/~oetiker/webtools/mrtg

[8] CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP),
http://www.cert.org/advisories/CA-2002-03.html

[9] Avaya Security Advisories on SNMP Vunerability,
http://support.avaya.com/security/2002-1/index.jhtml

[10] Cisco Advisory on SNMP Vulnerability,
http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

[11] Alcatel's response to SNMP Security Vulnerability,
http://www.ind.alcatel.com/service_support/CERT_Bulletin_031101_00.pdf

[12] Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQ), http://www.cert.org/tech_tips/snmp_faq.html

[13] Talisker's Intrusion Detection List,
www.networkintrusion.co.uk/Cisco.htm

[14] Are there Vulnerabilites in VLAN Implementations?, VLAN Security Test Report, David Taylor, 2000
http://www.sans.org/newlook/resources/IDFAQ/vlan.htm