

BİLGİSAYAR AĞLARI

ARA SINAV RAPORU

Bilgisayar Mühendisliği

Karamanoğlu Mehmetbey Üniversitesi

By
TUĞRAN DEMİREL
KASIM 2020

İÇİNDEKİLER

GİRİŞ.....	1
1 AĞ CİHAZLARININ GÜVENLİĞİNİ SAĞLAMA.....	2
2 AĞ CİHAZLARININ YAZILIMSAL GÜVENLİĞİ.....	2
2.1 Şifre Yönetimi.....	3
2.2 Güvenlik Duvarı(Firewall).....	3
2.3 IDS(Saldırı Tespit Sistemleri).....	4
2.4 Web Filtreleme Çözümleri(URL Filtering).....	5
3 IOS ERİŞİM MODLARI VE CİHAZ ERİŞİMİNİ GÜVENLİ HALE GETİRME.....	5
4 BÖLÜM SWITCH'LERDE PORT GÜVENLİĞİ.....	11
4.1 Switch'lerde Port Güvenliği Yapılandırması.....	11
5 BÖLÜM NTP PROTOKOLÜ VE YAPILANDIRMASI.....	14
6 BÖLÜM SİSTEM MESAJ KAYITLARI(SYSLOG).....	15
6.1 Syslog Mesaj Formatı.....	15
6.2 Syslog Yapılandırması.....	16
7 BÖLÜM CİHAZ YÖNETİMİ.....	17
7.1 Router Dahili Bileşenleri.....	17
7.2 Router Açılış Sıralaması.....	18
7.3 Yapılandırma Kayıtları(CONFREG).....	18
8 BÖLÜM IOS LİSANSLAMA.....	19
8.1 Lisans Çeşitleri.....	19
8.2 Lisans Aktivasyonu, Deaktivasyonu.....	19
KAYNAKÇA.....	20

GİRİŞ

Bu rapor herhangi bir kitap amacı gütmemektedir. Bilgisayar Ağları dersinin belirli konularının, önemli görülen bilgilerinin belirli süzgeçlerden geçirilip bir araya getirilmesiyle oluşturulmuştur.

1. AĞ CİHAZLARININ GÜVENLİĞİNİ SAĞLAMA

Bir ağın güvenliği dikkat edilmesi gereken bir konudur. Güvenlik duvarları(firewall) çoğu zaman bir ağın güvenliğini sağlamak için yeterli olmaz. Güvenlik bir ağda çalışmakta olan tüm cihazlar açısından düşünülmeli ve uygulanmalıdır. Ayrıca güvenliğin sürekli olması da önemli bir husustur.

Bir ağda bulunan bilgisayarların birbirleriyle iletişim kurması için bir kablo aracılığıyla bağlanmaları veya kablosuz(wireless) olarak haberleşmeleri gerekir; ancak tüm bilgisayarları kabloyla birbirlerine bağlamak kullanışlı bir yöntem değildir ve bu yüzdendir ki pek tercih edilmez. Bunun yerine tüm bilgisayarla ortak bir cihaza (switch) bağlanır. Böylece yerel bir ağ oluşturulur. Bu yerel ağın internete erişebilmesi için bir yönlendiriciye (router) ihtiyaç vardır.

Ağ cihazlarının yazılımsal güvenliği kadar fiziksel güvenliği de önemlidir. Fiziksel tehditler dört çeşit;

- 1- **Donanım Tehditleri:** Sunucularda, anahtar ve yönlendiricilerde fiziksel hasar oluşumu veya çalınması.
- 2- **Çevresel Tehditler:** Aşırı sıcak veya aşırı nem.
- 3- **Elektriksel Tehditler:** Gerilim dalgalanmaları, düşük voltaj, elektrik kesintisi.
- 4- **Bakım Tehditleri:** Elektrik bileşenlerinin kötü kullanımı, kötü kablolama, kötü etiketleme

olarak sınıflandırılabilir.

2. AĞ CİHAZLARININ YAZILIMSAL GÜVENLİĞİ

Ağ cihazlarında yazılımsal güvenliğinden maksat, Cisco IOS komutlarını kullanarak anahtar, yönlendirici gibi ağ cihazlarına yetkisiz kişilerin erişmesini engellemektir. Bir ağ ilk kurulduğunda varsayılan olarak belirli kullanıcı adı ve parola atanır. Bunları değiştirilmesi gereklidir. Şifre yönetimin en etkili biçimde kullanılması gerekmektedir. Şifre yönetiminin yanında IDS(Saldırı Tespit Sistemleri), güvenlik duvarı(firewall), web filtreleme çözümleri(URL Filtering) gibi sistemleri de kullanabiliriz.

2.1 Şifre Yönetimi

Şifre yönetiminin en efektif yolu "**LDAP**" veya "**RADIUS**" doğrulama sunucularından faydalanarak bir onay mekanizma sistemi kullanmaktır. Böyle bir mekanizma kullanılsa bile yetkili hakların kullanımı için yerel tanıtılmış bir şifre yapılandırma dosyasında bulunmalıdır. Bir şifreyi yapılandırma dosyalarında tutarken kesinlikle şifrelenmiş(encrypted) halde tutmak gerekir. Ayrıca bir şifre belirlenirken iyi bir şifrenin özelliklerini taşımasına dikkat edilmelidir. İyi bir şifre;

- Büyük ve küçük harf içerir.
- Noktalama işareti ve rakam içerir.
- Kolaylıkla hatırlanabilir böylelikle bir yere yazılmalarına gerek kalmaz.
- En az sekiz karakter uzunluğunda olur.
- Hızlı yazılabilirler.

2.2 Güvenlik Duvarı(Firewall)

Güvenlik duvarı veya ateş duvarı, güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemi şeklinde ifade edilebilir. Bir başka deyiş ile firewall'lar, yerel ağıyla dış ağ arasındaki güvenlik kontrol yazılımları/cihazlarıdır. Firewall ilk kurulduğunda bu nokta üzerindeki bütün geçişleri durdurur. Daha önceden belirlenen politikalar dahilinde hangi data paketinin geçip geçmeyeceği, hangi geçişlerde parola doğrulaması yapılacağı gibi bilgiler firewall kural tablolarına eklenir. Bu sayede sisteme ulaşan kişi ve bilgi trafiği kontrol altına alınmış olur. İçerideki/dışarıdaki sistemlere kimlerin girip giremeyeceğine, giren kişilerin hangi bilgisayarları ve hangi servisleri kullanabileceğini firewall üzerindeki kurallar belirler.

Firewall yazılımı, adresler arası dönüştürme-maskeleye(NAT) sayesinde LAN(Local Area Network)'deki cihazların IP adreslerini gizleyerek tek bir IP ile dış ağlara erişimini sağlar. Adres saklama ve adres yönlendirme işlemleri firewall üzerinden yapılabilir. Böylece dış dünyadaki kullanıcılar yerel ağdaki kritik topoloji yapısını ve IP bilgisini edinemezler. Firewall yazılımı kendi üzerinde belirtilmiş şüpheli durumlarda sorumluları uyarabilir(e-mail, SNMP, vb.).

Gelişmiş firewall yazılımları üzerinden geçen bütün etkinlikleri daha sonradan incelenebilmesi için kaydedirler. Ek bir lisans yada modül ile birlikte VPN(Virtual Private Network) denilen yerel ağa gidip gelen bilgilerin şifrelenmesi ile uzak ofislerden yada evden internet üzerinden güvenli bir şekilde şirket bilgilerine ulaşmak mail vb.

servisleri kullanmak mümkün olmaktadır. Bu şekilde daha pahalı çözümler yerine(lised line yada frame relay) internet kullanılabilir. Yalnız uzaktaki kullanıcıların güvenliği burada ön plana çıkmaktadır. Dışarıdan bağlanan kişinin gerçekten sizin belirlediğiniz yetkili kişi olup olmadığı önemlidir. Bu kişilerin şifresini ele geçirenler sisteminize o kişilerin haklarıyla ulaşabilirler. Bu noktada kişisel firewall ve dinamik şifre üreten tokenlar devrede olmalıdır.

Günümüzdeki gelişmiş firewall sistemleri içerik denetleme işlemi yapmamakta bu tip hizmetleri firewall sistemleriyle entegre çalışan diğer güvenlik sistemlerine yönlendirmektedir. Bu sayede güvenlik firmaları sadece odaklandıkları ve profesyonel oldukları konularda hizmet vermekte, kullanıcı da bu ayrık sistemlerden kendisi için uygun olan çözümleri tercih etmektedir. Örneğin gelen bilgilerin içerisinde virüs olup olmadığı yada atak yapıp yapılmadığı firewall tarafından kontrol edilmez. Kurallarda belirtilmişse kendisi ile entegre çalışan sisteme data paketini yönlendirir. Tarama işlemi diğer makinada yapıldıktan sonra paket tekrar firewall'a geri döner.

Firewall yazılımının yönetim konsolu merkezi yönetim amaçlı olarak ayrı makinelere yüklenebilir. Yönetim ile ilgili kurallar, trafik ile ilgili kayıtlar(log) ayrı sistemlerde tutulabilir. Kullanıcı grafik arayüzü ile uzak makinelerden kolayca yönetim yapılabilir ve mevcut kullanıcı bilgileri (LDAP) uygulamalarından alınabilir. Aktif bağlantılar görüntülenip gerektiğinde ana güvenlik politikalarına engel olmadan bağlantılara müdahale edilebilir. Bant genişliği yönetimi sağlayan sistemlerle entegre olabilir.

Firewall yazılımları/cihazları güvenliğin yapı taşları olup sistem içerisindeki diğer güvenlik yazılım/cihazları ile uyumlu çalışmakta ve gelecekteki güvenlik teknolojilerine taban teşkil etmektedirler. Firewall yazılımı kesinlikle şart olmasına rağmen güvenlik için tek başına yeterli değildir.

2.3 IDS(Saldırı Tespit Sistemleri)

Saldırı Tespit Sistemleri, tüm dünyada kullanılan web trafiğinin artması ve de web sayfalarının popüler hale gelmesi ile birlikte kişisel ya da tüzel sayfalara yapılan saldırılar sonucu ihtiyaç duyulan en önemli konulardan biri haline gelmiştir. Bununla birlikte kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttıkları mail, dns, database gibi sunucularının benzeri saldırılara maruz kalabilecekleri ihtimali yine Saldırı Tespit Sistemlerini internet güvenliği alanının vazgeçilmez bir parçası haline getirmiştir. Kurumların sahip oldukları çalışan sayısı ve bu çalışanların kendi kurumlarındaki kritik değer taşıyan yapılara saldırabilme ihtimalleri de iç ağın ya da tek tek kritik sunucuların kontrol altında tutulma gerekliliğini beraberinde getirir.

IDS(Saldırı Tespit Sistemleri) genel olarak iki tip olarak karşımıza çıkar; Sunucu tabanlı IDS ve Ağ tabanlı IDS.

Ağ tabanlı IDS'in görevi, bir kurum yada kuruluşun sahip olduğu ağ yada ağlara yönelmiş olan tüm trafiği algılayarak, bu ağa doğru geçen her bir data paketinin içeriğini sorgulamak, bir atak olup olmadığına karar vererek kaydını alabilmek, kendisi ya da konfigüre edebildiği başka bir aktif cihaz tarafından atakları kesmek, sistem yöneticisini bilgilendirmek ve ilgili raporlar oluşturabilmektir. IDS bir data paketinin atak olup olmadığını, kendi atak veritabanında bulunan atak tipleriyle karşılaştırarak anlar ve karar verir. Sonuç olarak bir IDS'in en önemli bileşeni bu atak veritabanıdır. Söz konusu Atak veritabanının içeriği, ne kadar sıklıkla ve doğrulukla güncellendiği ve kimin tarafından oluşturulduğu/güncellendiği en önemli noktadır. Bu sebeple doğru üretici firma ve ekip seçimi çok önemlidir.

Sunucu Tabanlı IDS'in görevi ise kurulu bulunduğu sunucuya doğru yönelmiş bulunan trafiği yine üzerinde bulunan atak veritabanı(İşletim Sistemine göre özelleştirilmiş) baz alınarak dinlemesi ve atakları sezerek cevap vermesidir.

Genel olarak IDS iki veya daha fazla makineden oluşan bir yapıdır. Performans artırımı sebebiyle Merkezi Kontrol ve Kayıt mekanizmasının bir makinede, Trafiği dinleyen ağ tabanlı modül veya Sunucu tabanlı modül ayrı makinelerde tutulur.

IDS'ler, dinlediği trafiğin kaydını tutarak, gerektiğinde bu kayıtları baz alarak istenilen şekilde raporlar çıkartabilmektedir. Atak sezdiklerinde atakları önleyebilir, yöneticilerine mail yada benzeri yollarla haber verebilirler, önceden oluşturulmuş bir program çalıştırabilir ve telnet benzeri bağlantıları kayıt ederek sonrasında izlenmesini sağlayabilirler. Tüm bu özellikleriyle IDS ler sistemin güvenli bir şekilde işlemesine yardımcı olur ve Sistem Yöneticilerinin Sistemi güçlü bir şekilde izlemesine yardımcı olmaktadır.

2.4 Web Filtreleme Çözümleri(URL Filtering)

Bugün çalışanların çoğunun internete erişim hakkı vardır. Fakat bunların hangi sayfalara gittikleri, oralarda ne kadar zaman geçirdikleri bunların ne kadarının işle ilgili olduğu gibi soruların yanıtlanması gerekiyor. Son zamanlarda yapılan bir çok araştırma iş günü içerisinde yapılan web sayfası ziyaretlerinin çoğunun işle alakalı olmadığı, sakıncalı sayfa ziyaretlerinin sistemlere virüs/trojan bulaşmasına, gereksiz bant genişliği harcanmasına ve yasal olmayan sitelerden indirilen programların sistemlere sahte lisanslarla kurulmasına(ki bu programların lisanssız yada sahte lisanslarla kurulmasından sistem yöneticileri ve şirket sahipleri BSA'ya karşı sorumlular) sebep olmaktadır.

Bütün bunları engelleyebilmek için URL filtering denilen yazılımlar kullanılmakta. Bu yazılımların her gün güncellenen veri tabanları sayesinde dünyadaki çoğu web sayfaları sınıflandırılmış durumda. Bu yazılımlar kişi, grup, IP adres aralıklarına kural

tanımlamamızı sağlamaktadır. Bu sayede daha önceden tanımladığımız kişilere hangi zaman aralıklarında nerelere girebileceklerini belirlenebilir.

Engellenen sayfalarla ilgili olarak kullanıcı karşısına bilgilendirici bir ekran çıkar ve neden engellendiği yada hangi zaman aralıklarında geçerli olduğu belirtilir. Burada daha önceden belirlenmiş bir sayfaya yönlendirmekte mümkündür. Bu tür yazılımlarının raporlama modülleri sayesinde kimlerin nerelere gittikleri oralarda ne kadar süre boyunca kaldıkları gibi ayrıntılı bilgilere ulaşmak mümkündür.

3. IOS ERİŞİM MODLARINI VE CİHAZI ERİŞİMİNİ GÜVENLİ HALE GETİRME

Ağ altyapısı aygıtları (yönlendiriciler, anahtarlar, yük dengeleyiciler, güvenlik duvarları, vb.), güvenlik konusunda önemli bir rol oynayan ve dolayısıyla buna göre korunmaları ve yapılandırılması gereken bir kuruluşun varlıkları arasındadır.

Örneğin bir siber korsan tarafından ele geçirilmiş bir yönlendirici, verilere erişim sağlamak, diğer hedeflere giden trafiği yönlendirmek için yeniden yapılandırılmak, diğer ağlara saldırı başlatmak, diğer iç kaynaklara erişim sağlamak için kullanılarak işletmenin tüm güvenliğine zarar verebilir. Bu nedenle, ağ cihazlarının sıkılaştırması (hardening), işletmenin bütün güvenliğini arttırmak için esastır.

Cisco, bir ağ cihazını “düzlem” adı verilen 3 işlevsel elemanda ayırır:

- **Yönetim Düzlemi:** Bu bir ağ cihazının yönetimi ile ilgilidir. Yönetim düzlemi, bir ağ cihazına erişmek, yapılandırmak, yönetmek ve izlemek için kullanılır. Bu makalede yönetim düzleminin güvenliği ele alınmıştır.
- **Kontrol Düzlemi:** Kontrol düzlemi, verileri kaynaktan hedefe taşımak için ağ cihazları arasında iletişim kuran protokoller ve süreçlerden oluşur. Buna BGP, OSPF, sinyal protokolleri vb. yönlendirme protokolleri dahildir.
- **Veri Düzlemi:** Veri düzlemi, veriyi kaynaktan hedefe taşımaktan sorumludur. Çoğu veri paketinin ağ cihazında aktığı yer burasıdır (genellikle donanım tarafından hızlandırılmıştır).

Anahtar veya yönlendiricilerde konsol veya telnet erişiminde ve kullanıcı modundan ayrıcalıklı moda geçişte parola sorulmasını sağlayabiliriz.

Gizli Parolayı Etkinleştirme: IOS aygıtına ayrıcalıklı yönetim erişimi sağlamak için güçlü bir “Enable Secret” parolası oluşturulmalıdır. Parola oluşturulurken Şifre

Yönetimine dikkat edilmelidir ve güçlü bir şifreleme ile parola oluşturan enable secret komutunu da kullanmayı unutmamalıyız.

```
Router# config terminal
Router(config)#enable password strpassword
Router(config)#enable secret strongpassword
```

Enabled password komutunu kullanarak şifremizi *strpassword* olarak belirledik. Daha sonra enable secret komutunu kullanarak şifremizi *strongpassword* olarak belirttik. İkisi arasındaki temel fark enable password ile vermiş olduğumuz şifre kullanıcı modundan ayrıcalıklı moda geçişte kullanılırken enable secret ile vermiş olduğumuz şifre ise daha güvenlidir.

Parolaları Cihazda Şifreleme: Cisco aygıtında yapılandırılan tüm parolalar (“enable secret” hariç) yapılandırma dosyasında açık metin olarak gösterilir. “show running-config | include enable” komutu ile çalışan yapılandırma dosyası görüntülenir. | işareti ve include ile sadece enable kısmını dahil edilir.

```
Router#show running-config | include enable
enable secret 5 $1$mERt$kTYfdh95shecs$adsdha78AET
enable password strpassword
```

Yukarıda da görüldüğü gibi enable secret ile oluşturulan şifre MD5 ile şifrelendiği için açıkça görülmez iken enable password ile şifrelenen şifre görülmektedir.

Açık metin parolalarını şifrelemek ve yapılandırma dosyasında görünmesini engellemek için, “service password-encryption” global komutunu kullanmalıyız.

```
Router(config)# service password-encryption
```

Tekrardan “show running-config | include enable” ile çalışan yapılandırma dosyalarını görüntülediğimizde;

```
Router#show running-config | include enable
enable secret 5 $1$mERt$kTYfdh95shecs$adsdha78AET
```

```
enable password 7 02896ADSA418S
```

enable password ile verdiğimiz parola type 7 ile şifrelendi.

Kullanıcı Kimlik Doğrulaması İçin Harici Bir AAA Sunucu Kullanımı: Her cihazda yönetici erişimi için yerel kullanıcı hesaplarını kullanmak yerine, kullanıcıların aygıtlara erişimini Kimlik Doğrulama, Yetkilendirme ve Hesaplama işlemlerini yürütmek için harici bir AAA sunucusunu (TACACS + veya RADIUS) kullanması çok daha güvenli, esnek ve ölçeklenebilir. Merkezi bir AAA sunucusu ile hesap şifrelerini kolayca değiştirebilir, etkinleştirebilir, devre dışı bırakabilir, güçlü şifre politikaları uygulayabilir, hesap kullanımını ve kullanıcı erişimini izleyebilirsiniz.

TACACS+

```
Router# config terminal
Router(config)# enable secret K6dn!#scfw35 (İlk önce bir
"etkinleştirme" şifresi oluşturulur.)
Router(config)# aaa new-model (AAA hizmetini etkinleştirilir.)
Router(config)# aaa authentication login default group tacacs+
enable ("enable" şifresiyle kimlik doğrulama için TACACS + '1
kullanılır.)
Router(config)# tacacs-server host 192.168.1.10 (Dahili AAA
sunucusunu ataması.)
Router(config)# tacacs-server key 'secret-key' (AAA sunucusunda
yapılandırılmış gizli anahtarı)
Router(config)# line vty 0 4
Router(config-line)# login authentication default (VTY satırlarına
(Telnet, SSH vb.) AAA kimlik doğrulaması uygulanır.)
Router(config-line)# exit
Router(config)# line con 0 (Konsol bağlantı noktasına AAA kimlik
doğrulaması uygulanır.)
Router(config-line)# login authentication default
```

RADIUS

```
Router# config terminalRouter(config)# enable secret K6dn!#scfw35
Router(config)# aaa new-model
Router(config)# aaa authentication login default group radius
enable
Router(config)# radius-server host 192.168.1.10
Router(config)# radius-server key 'secret-key'
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# line con 0
Router(config-line)# login authentication default
```

Kullanıcı Kimlik Doğrulaması İçin Ayrı Yerel Hesaplar Oluşturulması: Harici bir AAA sunucusu kurulamıyor ve kullanılamıyorsa, cihazlarınıza erişim vereceğiniz herkes için ayrı bir yerel hesap oluşturulmalıdır. IOS versiyon 12.2 (8) T ve sonrasında cihaz üzerinde oluşturulan yerel hesaplar MD5 hash ile şifrelenir.

```
Router# config terminal
Router(config)# username tugran-admin secret Lms!a2eZSf*%
Router(config)# username ismet-admin secret d4N3$6&%sf
Router(config)# username ramazan-admin secret 54sxSFT*&(zsd
```

Yukarıdaki hesaplar oluşturulurken IOS versiyonu 12.2 (8) T ve sonrası baz alınmıştır.

Maksimum Başarısız Kimlik Doğrulama Denemelerinin Yapılandırılması: Cihazlara kaba kuvvet şifre saldırılarını önlemek için, bir kullanıcı bu eşikten sonra kilitlenecek şekilde başarısız giriş denemesi sayısını yapılandırabilir. Bu, cihazlardaki yerel kullanıcı hesapları için çalışır.

```
Router# config terminal
Router(config)# username tugram-admin secret Lms!a2eZSf*%
Router(config)# aaa new-model
Router(config)# aaa local authentication attempts max-fail 5
maksimum 5 başarısız giriş denemesi.
Router(config)# aaa authentication login default local
```

Aygıtlara Yalnızca Belirli IP’lerden Yönetim Erişimine İzin Verme: Bu yöntem, Cisco ağ cihazlarında muhtemelen en önemli güvenlik yapılandırmalarından biridir. IP adreslerini cihazlarınız için Telnet veya SSH’yi erişimi için sınırlandırmanız gerekir. Bu, yöneticilerin ağı yönetmek için kullanacakları birkaç yönetim sistemi ile sınırlandırılmalıdır.

Ağ Zaman Protokolünün(NTP) Etkinleştirilmesi: Bu yöntem için günlük(syslog) tutulmalıdır. Günlük verilerinin doğru zaman ve saat dilimi ile damgalanması için tüm ağ cihazlarında doğru ve düzgün saat ayarlarına sahip olmanız gerekir. Dahili veya harici bir NTP sunucusu yapılandırılabilir ve kullanılacak bir çok ortak NTP sunucusu vardır.

```
Router# config terminal
Router(config)# ntp server 1.1.1.1
Router(config)# ntp server 2.2.2.2
```

Güvenli Yönetim Protokollerini Kullanılması: Telnet, Cisco cihazlarına Komut Satırı erişimi için varsayılan yönetim protokolüdür. Ancak, tüm yönetim trafiği Telnet ile açık metin olarak gönderilir. Güvenlik nedeniyle, Telnet yerine yönetim için SSH'yi tercih edilmesi daha doğru olur.

İlk olarak yönlendiriciye hostname ve domain name yapılandırılması gerekir. Çünkü bu domain name ve hostname kullanılarak SSH anahtarı oluşturulacak.

Cisco cihaza SSH erişimi yapılandırılması:

```
Router# config terminal
Router(config)# hostname London
London(config)# ip domain-name mydomain.com
London(config)# ip ssh version 2
London(config)# crypto key generate rsa modulus 2048
London(config)# username tugran-admin password strpassword
London(config)# ip ssh time-out 60
London(config)# ip ssh authentication-retries 3
London(config)# line vty 0 15
London(config-line)# login local      (login local komutu ile
yönlendirici localinde oluşturmuş olduğumuz kullanıcı adı ve
şifre ile oturum açılmasını sağlıyoruz.)
London(config-line)# transport input ssh (SSH yapılandırılması
sağlandı.)
```

SNMP Erişimini Kısıtla ve Güvenli Hale Getirilmesi: Basit Ağ Yönetimi Protokolü (SNMP) ağ cihazlarından bilgi toplamak için çok yararlı olabilir, ancak uygun şekilde yapılandırılmadıysa da bir güvenlik riski oluşturabilir. SNMP protokolü, cihazdaki SNMP verilerine erişimi kısıtlamak için şifre (Şifre Okuyucu veya Okuma / Yazma) olarak kullanılan bir "Topluluk Dizesi" kullanır. Güçlü bir Topluluk Dizesi yapılandırmaya ek olarak, yalnızca birkaç yönetim iş istasyonundan SNMP erişimine izin vermek için IP filtrelemesi de uygulanmalıdır.

4- SWITCH’LERDE PORT GÜVENLİĞİ

Anahtarlarda, şirket BT kullanım politikalarına göre belirli güvenlik yapılandırmaları gerçekleştirilebilir. Bunların başında ise port güvenliği gelmektedir. Böylelikle bir anahtar portuna bağlanacak MAC adres sayısını sınırlandırarak, kullanıcıların şahsi bilgisayarlarını şirket ağına bağlayarak ağ güvenliğini tehlikeye atmalarını önlemiş oluruz ve bunu da genel güvenlik olarak nitelendirebiliriz. Port güvenliği sayesinde hangi MAC adresinin hangi porta erişebileceğini de belirleyebiliriz ve bu durumu da artırılmış güvenlik olarak nitelendirebiliriz.

Portlar static olarak belirlendiğinde her biri için static olarak elle girilmiş bir MAC adresi olur. Dinamik, kalıcı(sticky) olarak belirlendiğinde ise verilen sayıda ilk takılanlara izin verilir ve sticky MAC adresi “switchport port-security mac-address sticky” komutu ile yapılandırılır.

Port güvenlik politikası çöğendiğinde ise üç çeşit cevap vardır. Protect, restrict, shutdownur. Shutdown default tercihtir(moddur).

4.1 Switch’lerde Port Güvenliği Yapılandırması

Port güvenliğini sağlanması için gereken adımlar:

Switch’e Cihazların Bağlanması:

Cihazları port 1 ve port 2’ye takıyoruz. Portların aktif hale gelmesi 30 saniye alır. Önce koyu sarı yanarlar bu STP kontrolünün yapıldığı anlamına gelir. Yeşil olduklarında port aktiftir.

Cihazlara IP adresi Verilmesi ve Devamlı Ping Atılması:

İlk önce cihazlara IP adresi verilir ve pingler devamlı her iki cihazdan birbirine olacak şekilde etkinleştirilir.

Cihazların IP adresi:

```
10.1.2.50  
10.1.2.51
```

```
ping 10.1.2.51 -t  
ping 10.1.2.52 -t
```

Switch’de MAC Adresi Tablosunun Görüntülenmesi:

“show mac address-table” komutu ile MAC adresi tablosu görüntülenir. Default statik MAC adreslerinin altında portlara atanmış adresleri görebiliyoruz.

0011.43fe.5425	DYNAMIC	Fa0/2
f8b1.56fe.9da9	DYNAMIC	Fa0/1

Bilgisayarlar üzerinden MAC adresleri kontrol edildiklerinde uyuyorsa birbirlerine herhangi bir sıkıntı yoktur demektir.

Switch’de Port Security’nin Aktif Hale Getirilmesi:

İlk olarak portların port security’i kabul etmeleri için “access port” olmaları gerekmektedir.

```
interface range fastEthernet 0/1-2
switchport mode access
```

Fakat trunk portlar üzerinde port security aslında yapılabilir. Fakat bu genellikle yapılan bir şey değildir çünkü oradan başka ne geleceğini bilemeyiz. Bir porta başka bir switch bağladıysak o porttan bir sürü MAC adresi gelebilir. Dinamik bir portta kesinlikle yapılamaz. “Command Rejected” hatası verecektir.

```
interface fastEthernet 0/1
switchport port-security ?
```

? işareti ile opsiyonları görüntülediğimizde,

- aging: mac adreslerinin ne kadar süre ile hatırlanacağı.
- mac-address: spesifik bir mac adresi veya sticky mac adresi kullanabiliriz.
- maximum: Kaç tane maksimum adrese izin verdiğimiz.
- violation: Kural aşıldığında ne yapacağı, protect, restrict ve shutdown modları vardı.

```
Interface fastEthernet 0/1
switchport port-security
```

Bu komutlar sayesinde port security’i aktif hale getirmiş oluyoruz.

Birden Fazla MAC Adresinden Trafik Oluştur:

Scapy gibi bir uygulamadan yapılabileceği gibi bir daha az fonksiyonel bir dummy switch bağlayarak da yapılabilir.

Scapy ile “ab:cd:ef:ab:cd:ef” kaynak MAC adresinden “00:50:79:66:68:00” hedef MAC adresine bir frame yollanması:

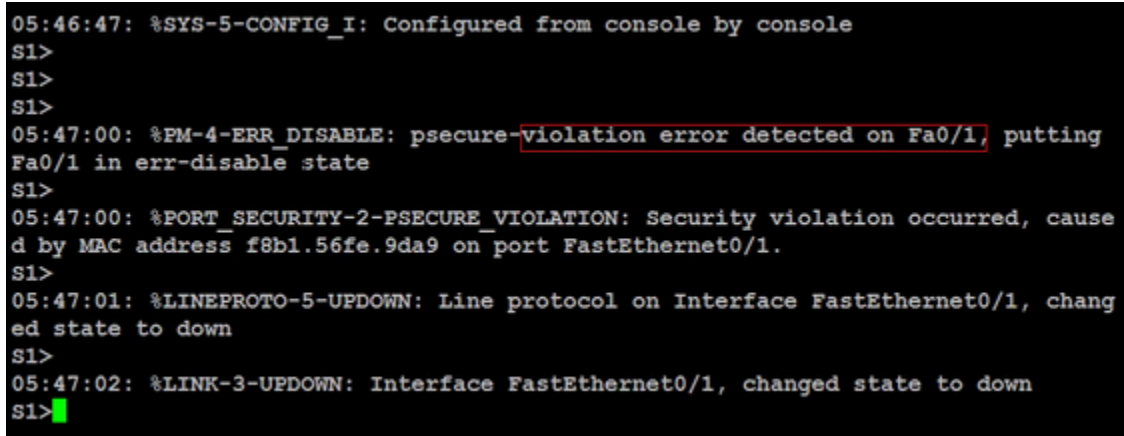
İlk olarak bilgisayarlardaki interfaceler öğrenilir.

```
netsh interface show interface
```

Ardından scapy içerisinde girerek aşağıda belirtilmiş olan MAC adresinden frame yollayabiliriz.

```
sendp(Ether(src="ab:cd:ef:ab:cd:ef", dst="00:50:79:66:68:00"),  
iface="VMware Network Adapter VMnet8")
```

Şu ana kadarki gerekli adımlar doğru yapıldıysa switch’de port security’nin etkin hale gelerek violation detect ettiği görülecektir.



```
05:46:47: %SYS-5-CONFIG_I: Configured from console by console  
S1>  
S1>  
S1>  
05:47:00: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting  
Fa0/1 in err-disable state  
S1>  
05:47:00: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, cause  
d by MAC address f8b1.56fe.9da9 on port FastEthernet0/1.  
S1>  
05:47:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, chang  
ed state to down  
S1>  
05:47:02: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down  
S1>
```

Son bağlanan cihaz iletişim kurmayı denediğinde(muhtemelen bir IP adresine ihtiyacım var gibi bir DHCP isteği göndererek) 1 MAC adresi kısıtlamasını geçmiş oluyor. Portun port security bilgilerini görüntülediğimizde,

```
show port-security interface fa0/1
```

Port Security: Enable, Port-Status: Secure-Shutdown olarak görülür. Bu da portun kapatıldığı anlamına geliyor(default violation mode). Aynı zamanda Last Source Address olarak son MAC adresini kayıt altına almış ve Violation counter ile saydığını görüyoruz. Restrict bu counter’ı arttırıyor. Sonuç olarak portun gittiğini ışığının söndüğünü görüyoruz. Basitçe “no shutdown” diyerek aktif hale getiremeyiz.

```
show interfaces fa0/1
```

komutun çıktısında gördüğümüz üzere error-disabled pozisyonunda. Bu bir yönetici tarafından kapatılmadığı bir hatadan dolayı kapatıldığı anlamına geliyor.

5. NTP PROTOKOLÜ VE YAPILANDIRMASI

NTP(Ağ Zaman Protokolü), packet-switched, variable-latency veri ağları üzerinden bilgisayar sistemleri arasında saat senkronizasyonu için bir ağ protokolüdür. Başka bir deyişle NTP, fazlalık kapasitesi olan bir sıralı zaman dağıtım sistemidir. Ağdaki ve de hedef makinedeki algoritmaları, gecikmeleri ölçer. Bu teknikleri kullanarak saatleri saliselere kadar senkronize edebilir. NTP ayarları hangi dağıtımın kullanıldığına bağlı olarak ya `/etc/ntp.conf` ya da `/etc/xntp.conf` dosyasından yapılır. NTP sunucu olarak yerel ağdaki bir NTP sunucu kullanabileceği gibi internet üzerindeki NTP sunucularını da kullanabilir.

NTP gerçek zaman bilgisini(doğru olan), cihaz üzerindeki yerel ana saat, internetteki ana saat, atomik saat veya GPS üzerinden alabilir.

Çoğu temel yapılandırılmalı `ntp.conf` dosyasında iki sunucu ismi mevcuttur. Birisi, saat ayarının yapılması istenen sunucunun adı ve diğeri de sahte bir IP adresidir. Sahte IP adresi ağ problemleri olması durumunda veya NTP sunucusunun kapalı olması-çökmesi durumunda kullanılır. Sistemdeki NTP uygulaması, uzak NTP sunucusu ayağa kalkınca, sistem saatini tekrar ona göre ayarlayacaktır. Bu iki sunucudan birincisi asıl sunucu olarak işlem yapar, ikincisi ise yedek amaçlıdır. Ayrıca bu hedef dosyanın yeri de belirtilmelidir. NTP zamanla, sistem saatindeki hata oranını "öğrenecek" ve kendini buna göre ayarlayacaktır.

NTP konfigürasyon dosyalarında(`/etc/ntp.conf`, `xntpd`) başlıca;

- Olası senkronizasyon sunucularının listesi
- Hangi kriterlere göre senkronizasyon sunucunun seçileceği
- Sunucunun ana makineye bağlanırken içerdiği kısıtlamalar
- NTP paketlerinin ağda yayınlanıp yayınlanmayacağı
- Broadcast (tüm gönderim) NTP paketlerinin dinlenip dinlenmeyeceği
- Multicast (çoğa gönderim) NTP paketlerinin dinlenip dinlenmeyeceği
- Driftfile dosyasının yeri
- NTP bağlantılarının görüntülenip görüntülenmeyeceği
- Ana makineye konfigürasyon yenileme izninin verilip verilmeyeceği

bilgilerini de içerir. Konfigürasyon dosyası istenilen formatta yazılabilir. İstemci modunda sunucu diğer sunuculara o anki zamanı almak için kontrol eder. Tüm sunucular kontrol edildikten sonra ana makine hangi sunucuya senkronize edileceğini seçer. Sunucuyu istemci modda yapılandırmak için NTP konfigürasyonunda kontrol edilecek sunucuların adının ve IP adresinin bulunduğu bir sunucu cümlesi olmalıdır.

Sistem xntp daemon'u ve istemci modu, broadcast ya da multicast istemci modu, simetrik aktif modları da kullanarak diğer sunucularla senkronize edilebilir.

6. SİSTEM MESAJ KAYITLARI(SYSLOG)

Log kelimesi günlük manasına gelir. System Log'u ise system günlükleri olarak çevirebiliriz. Peki bu system günlükleri ne işimize yarar? Örneğin, bir port açılıp kapatıldığında ya da port güvenliği ihlali gerçekleştiğinde ağ cihazları yöneticisine detaylı bilgi vermemizi sağlar. Ağ yönetici isterse bu syslog kayıtlarını depolar, isterse de görüntüler. Kısacası ağ cihazlarının gönderdiği mesajları okumak için Syslog protokolü kullanılır.

6.1 Syslog Mesaj Formatı

Syslog protokolü tarafından üretilen her mesajın bir önem düzeyi ve facility(mesaj kaynağını gösteren etiket) bölümü vardır. Syslog mesajlarının iki format vardır. RFC3164 a.k.a(eski)Formatı ve RFC5424 a.k.a.(yeni) Formatıdır.

RFC3164 a.k.a(eski) Formatı: Bir örnek ile /dev/log içeriisinde bulunan yapıyı inceleyelim.

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

<34> öncelik sayıdır. 8 ile çarpılan facility yerini kolaylıkla gösterir. Facility otomatik değer olarak 4 alır.

Oct 11 22:14:15 yaygın olarak kullanılan zaman stilidir. Salise dışındaki diğer zaman bilgilerini verir. Saniye, dakika, saat, gün, ay gibi. Bundan dolayı rsyslog ISO-8601 ile RFC3164 formatından ayırır.

Mymachine mesajın yazıldığı hostname'dir.

su: Etikettir.

su: etiketinden sonra gelen bütün her şey mesaj olarak nitelendirilir.

RFC5424 a.k.a(yeni) Formatı: RFC3164'ün problemlerinden kaynaklı olarak oluşturulmuş bir standatdır.

1K'dan daha fazla syslog mesajları gönderilmiyor. Çünkü bir UDP paketinin maksimum değerinde. RFC5424 tercih edilme sebebi UDP'nin yanında başka

protokolleri de desteklemesidir. RFC3164'e ek olarak zaman stilinde saliseleri de tutuyor. Herhangi bir konumunun olmasına gerek yok. Json formatında da mesajlar tutulabilir.

Örneğin:

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - - - 'su
root' failed for lonvick on /dev/pts/8
```

6.2 Syslog Yapılandırması

Varsayılan olarak Cisco IOS Syslog mesajlarını konsola gönderir. Ayrıca bu mesajlar tampon bellekte saklanır. Syslog mesajlarını konsola göndermek için “logging con-sole”, Syslog mesajlarını tampon bellekte saklamak için “logging buffered” komutları kullanılır.

```
Router(config)#ntp server myip
Router(config)#logging host myip
Router(config)#logging trap 4
Router(config)#service timestamps log datetime msec
```

Öncelikle `ntp server myip` komutu ile Syslog mesajlarına doğru zaman bilgisi ile dalgalanması için NTP sunucudan doğru zaman bilgisini almalıyız. `logging host myip` komutu ile sunucu adresine giriyoruz ve log tutulması için komut veriyoruz. `logging trap 4` komutu ile Syslog sunucusuna gönderilecek mesajların seviyelerini belirtiyoruz. 4 ile 4 ve daha düşük seviye mesajların sunucuya gönderilmesini söyledik. `logging trap warning` komutuyla da aynı işi yapabiliriz. `service timestamps log datetime msec` komutu ile de Syslog mesajlarına mili saniye olarak zaman damgası ekledik. Böylelikle yapılandırmayı gerçekleştirmiş oluyoruz. Yapılandırmayı görmek için `show logging` komutunu kullanabiliriz.

7. CİHAZ YÖNETİMİ

Cisco IOS işletim sisteminin yedeklenmesi ve güncellenmesi, parolaların kurtarılması gibi cihaz yönetimi gibi işlemleri IOS komutları ve bazı protokoller(TFTP) kullanılarak gerçekleştirilir.

7.1 Router Dahili Bileşenleri

Bir yönlendirici Flash, ROM, RAM, NVRAM bellekler ve işlemi(CPU) ana bileşenlerinden oluşur.

Bellek Çeşidi	Geçici/Kalıcı	Depolama Alanı
ROM	Kalıcı	Başlatma Yönergeleri Temel Tanılama Yazılımları(POST) Sınırlı IOS(ROM Monitor)
RAM	Geçici	Çalışan IOS Çalışan Yapılandırma Dosyası(running config) Yönlendirme Tablosu(routing table) ARP Tablosu Paket Arabelleği
NVRAM	Kalıcı	Başlangıç Yapılandırma Dosyası(startup config)
Flash	Kalıcı	IOS Sistemle İlgili Dosyalar

7.2 Router Açılış Sıralaması

Bir yönlendirici açılırken 3 ana işlem yapar.

- 1- POST(Power On Self Test) işleminin gerçekleşmesi ve ön yükleme programının yüklenmesi:** Post işleminin amacı yönlendiriciyi donanımı test edip kontrol etmektir. POST işlemi ROM içerisinde bulunan bir yazılım tarafından gerçekleştirilir. Önyükleme program ROM'dan RAM'e yüklenir, görevi IOS'u bulup RAM'e yüklemektir.
- 2- Cisco IOS yazılımının bulunması ve yüklenmesi:** Cisco IOS çoğunlukla kibrit kutusu büyüklüğünde ve kare şeklindeki bir flash kart içinde bulunur ve yönlendirici üzerinde ilgili slota takılır. Öncelikle IOS dosyası flash kartta aranır ve bulunur ise sıkıştırılmış IOS dosyasını açılarak RAM'e yüklenir. IOS flash bellekte bulunamadıysa TFTP sunucundan aranır, buradan da bulunamaz ise ROM bellek içinde bulunan ve kısıtlı IOS özellikleri taşıyan ve kısaca ROM Monitör denen kısıtlı IOS RAM'e yüklenir.
- 3- Başlangıç yapılandırma dosyasının bulunması ve yüklenmesi:** Bu aşamada ön yükleme programı NVRAM'de bir başlangıç yapılandırma dosyası arar. Bulunur ise RAM'e yükler ve artık RAM'deki bu dosyanın adı çalışan yapılandırma dosyasıdır. Bulunmaz ise TFTP sunucunda arayabilir, yine bulunmaz ise Setup yani kurulum moduna girilir.

7.3 Yapılandırma Kayıtları(CONFREG)

Tüm Cisco yönlendiricilerde NVRAM'de tutulan 16 bitlik bir yapılandırma kayıt edici bulunur. Yapılandırma kayıtları bir yönlendiricinin nasıl boot edeceğini kontrol etmek için kullanılır. IOS'un flash bellekten ve başlangıç yapılandırma dosyasının NVRAM'den yüklenmesini sağlayan confreg değeri 0x2101'dir. Confreg değeri değiştirilerek yönlendirici boot sıralaması değiştirilebilir.

Yapılandırma kayıtlarında 0-3 bitlerden oluşan alan boot sıralamasını kontrol eder.

“show version” komutu ile en alt satırda geçerli yapılandırma kaydı görüntülenebilir.

8. IOS LİSANSLAMA

Cisco IOS 15. sürümünden sonra yeni bir lisans modeline geçiş yaptı. Her cihaz universal imaj ile gönderilmekte. Cisco Lisans Yöneticisi veya Cisco Lisans Portalı arayışıyla etkinleştirme yapılır. Bunun için PAK(Product Activation Key) alınmalıdır. PAK, Cisco tarafından oluşturulan 11 basamaklı alfa sayısal karakterlerdir.

8.1 Lisans Çeşitleri

- 1- **IP Tabanı(IP Base):** Bütün cihazlarla gelen temel lisanstır. BGP, OSPF, EIGRP, IS-IS, RIP, IGMP, Multicast gibi özellikleri destekler.
- 2- **Veri(Data):** Ekstra ücret ödeyerek aktif edilir. MPLS, BFD, L2VPN, IP SLA gibi özellikleri destekler.
- 3- **Tümleşik İletişim(Unified Communications-UC):** Ekstra ücret ödeyerek aktif edilir. CUBE, SRST, Voice Gateway, CUCME, DSM gibi özellikleri destekler.
- 4- **Güvenlik(Security-SEC):** Ekstra ücret ödeyerek aktif edilir. Firewall, SSL, VPN, DMVPN, IPS, IPsec gibi özellikleri destekler.

IP Tabanı lisansı bütün lisanslar için gereklidir.

8.2 Lisans Aktivasyonu, Deaktivasyonu

Lisans aldıktan sonra mail adresimize .lic uzantılı bir XML dosyası gelir. Bu lisans dosyasını “license install” komutu ile aktif edip cihazı yeniden başlatırız. Bir lisansı kaldırmadan önce devre dışı bırakmamız gerekmektedir. Devre dışı bıraktıktan sonra lisans dosyalarını siliyoruz. “license install” komutu ile de aktif ettiğimiz lisansları kaldırabiliriz.

```
Router(config)#license boot module c1900 technology-package  
securityk9 disable  
Router#license clear seck9
```

KAYNAKÇA

Cemal Taner, Ağ Yöneticiliği Temelleri

<https://www.cemaltaner.com.tr/2018/07/21/10-adimda-cisco-cihaz-sikilastirmasi/>

<http://www.sariyildiz.net/networking/switching/port-security/>

https://en.wikipedia.org/wiki/Network_Time_Protocol

[https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/06/ntp-\(network-time-protocol--a%C4%9F-zamanlama-protokol%C3%BC\)](https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/06/ntp-(network-time-protocol--a%C4%9F-zamanlama-protokol%C3%BC))

<https://sematext.com/blog/what-is-syslog-daemons-message-formats-and-protocols/>