Cihaz Güvenliği ve Temel Sıkılaştırma (Device Security)

Ağ güvenliği sadece dışarıdan gelen hacker'ları (hacker) engellemek değil, içerideki kötü niyetli veya dikkatsiz kullanıcılardan ağ cihazlarını korumaktır. En güçlü güvenlik duvarını (Firewall) kursanız bile, yönlendiricinizin (Router) veya anahtarınızın (Switch) parolası "12345" ise tüm ağınız tehlikededir.

1. Fiziksel ve Çevresel Tehditler

Bir cihazın fiziksel güvenliğini sağlayamazsanız, yazılımsal güvenliğinin hiçbir anlamı kalmaz. Cihazın yanına gidebilen bir saldırgan parolaları sıfırlayabilir (Password Recovery) veya ağa sızabilir.

- **Donanım Tehditleri:** Cihaza fiziksel zarar verilmesi veya çalınması. *Önlem: Kilitli sistem odaları (Kabinet kilitleri, biyometrik/kartlı geçiş sistemleri, güvenlik kameraları).*
- **Çevresel Tehditler:** İklimsel olaylar. *Önlem: İklimlendirme cihazları (Klima), ısı ve nem sensörleri.*
- **Elektriksel Tehditler:** Gerilim yükselmesi, voltaj dalgalanması veya elektrik kesintisi. *Önlem: Kesintisiz Güç Kaynakları (UPS) ve yedek jeneratörler.*
- **Bakım Tehditleri:** Kötü kablolama, eksik etiketleme veya kalitesiz donanım kullanımı. *Önlem: Düzenli kablo yönetimi ve standartlara uygun altyapı.*

2. Temel Parola Güvenliği ve Şifreleme

Cihazın ayrıcalıklı (Privileged EXEC) moduna geçişi korumak en önemli adımdır.

- `enable password [parola]` : Parolayı düz metin (Clear-text) olarak kaydeder. `show running-config` yazan herkes parolayı okuyabilir. **Kullanılmamalıdır.**
- `enable secret [parola]` : Parolayı MD5 (veya daha güncel cihazlarda SHA-256) algoritmalarıyla şifreleyerek kaydeder. Güvenlidir. *(Not: Her ikisi de ayarlıysa, cihaz her zaman `secret` parolasını geçerli sayar).*

Router(config)# enable secret Cisco123!

! Çalışan yapılandırmadaki (Running-Config) eski Düz Metin parolaları
! Type 7 (Zayıf şifreleme) ile gizlemek için kullanılır. Omuz sörfüne karşı korur.
Router(config)# service password-encryption

! Parola Politikası: Tüm yeni parolaların en az 10 karakter olmasını zorunlu kılma
Router(config)# security passwords min-length 10

3. Konsol ve VTY Hatlarının Güvenliği

Cihaza fiziksel konsol kablosuyla veya ağ üzerinden bağlananları kontrol altına almalıyız.

```
! Konsol (Fiziksel) Bağlantı Güvenliği
Router(config)# line console 0
Router(config-line)# password KonsolPass
Router(config-line)# login              ! (Bağlanırken parolayı sor demek)
Router(config-line)# exec-timeout 5 0    ! (Cihaz 5 dakika 0 saniye boş kalırsa oturumu otomatik kapat)
Router(config-line)# exit

! Brute-Force (Kaba Kuvvet) Saldırılarına Karşı Koruma (Çok Kritik!)
! Kural: 60 saniye içinde 3 kez yanlış şifre girilirse, IP adresini 180 saniye boyunca engelle (banla).
Router(config)# login block-for 180 attempts 3 within 60
```

4. SSHv2 (Secure Shell) Yapılandırması

Telnet, verileri ve parolaları ağ üzerinde düz metin (Clear-text) olarak gönderir. Ağı dinleyen biri (Örn: Wireshark ile) parolalarınızı kolayca çalabilir. Bu nedenle uzak bağlantılar için veriyi kriptolayan **SSH (Secure Shell)** kullanılmalıdır.

Cisco cihazlarda SSH'ı aktif hale getirmek için 5 adımlı bir süreç izlenir:

```
! 1. Cihaza bir isim (Hostname) ve Alan Adı (Domain Name) verilir.
! (Bu ikisi birleşerek kriptografik anahtarın adını oluşturur, örn: R1.sirket.local)
Router(config)# hostname R1
R1(config)# ip domain-name sirket.local

! 2. RSA Kriptolama Anahtarı Üretilir (SSH bu anahtarı kullanarak trafiği şifreler)
! Komutu girince size anahtar uzunluğunu soracaktır, güncel güvenlik için en az 1024 veya 2048 seçilmelidir.
R1(config)# crypto key generate rsa

! 3. Güvenlik için SSH Versiyon 2'ye zorlanır (SSHv1'de güvenlik açıkları vardır)
R1(config)# ip ssh version 2

! 4. Cihazın kendi veritabanında (Lokal) bir kullanıcı adı ve parola oluşturulur
R1(config)# username admin privilege 15 secret AdminParola123!

! 5. VTY (Sanal Terminal) Hatlarına Girilir ve Sadece SSH'a İzin Verilir
R1(config)# line vty 0 4
R1(config-line)# login local          ! (Yerel veritabanındaki kullanıcı/parolayı kullan)
R1(config-line)# transport input ssh ! (Telnet'i yasakla, SADECE SSH bağlantılarını kabul et)
R1(config-line)# exit
```

Doğrulama Komutları:

- `show ip ssh` : SSH'ın versiyonunu ve kimlik doğrulama sürelerini gösterir.
- `show users` : O an cihaza konsoldan veya SSH/Telnet üzerinden bağlı olan kullanıcıları listeler.

5. Uyarı Mesajları (Banner MOTD)

Cihaza bağlanan kişilere hukuki olarak "Yetkisiz erişim yasaktır" uyarısı yapmak için kullanılır. Uyarı mesajı başlatıcı ve bitirici bir karakter (genellikle `#` veya `"`) arasına yazılır.

R1(config)# banner motd "DİKKAT: Sadece Yetkili Personel Girebilir. Tum islemler loglanmaktadir."

Merkezi Kimlik Doğrulama: AAA ve RADIUS

Kurumsal ve büyük ölçekli ağlarda cihaz güvenliğini yönetmek için yerel veritabanları (cihazın kendi içindeki `username/password` kayıtları) yeterli ve güvenli değildir. Bunun yerine cihazlar, kimlik doğrulama işlemini merkezi bir sunucuya (Örn: Cisco ISE, Windows NPS) devrederler. Bu mimari yapıya **AAA** denir.

1. AAA Çerçevesi (Framework) Nedir?

AAA, ağ güvenliğinin üç temel ayağını oluşturur:

1. **Authentication (Kimlik Doğrulama):** "Sen kimsin?" Cihaza bağlanmak isteyen kullanıcının gerçekten iddia ettiği kişi olup olmadığını doğrular (Parola, Sertifika veya Biyometrik verilerle).
2. **Authorization (Yetkilendirme):** "Neler yapabilirsin?" Kimliği doğrulanan kullanıcının cihaz üzerinde hangi komutları çalıştırmaya yetkisi olduğunu belirler (Örn: Sadece `show` komutlarını çalıştırabilen Privilege 1 kullanıcısı veya tam yetkili Privilege 15 kullanıcısı).
3. **Accounting (Hesap Verilebilirlik / Kayıt Tutma):** "Neler yaptın?" Kullanıcının sisteme ne zaman girdiğini, ne kadar kaldığını ve hangi komutları çalıştırdığını kayıt altına alarak loglar. Olası bir hatada sorumluyu bulmak için hayatidir.

2. RADIUS ve TACACS+ Karşılaştırması

AAA mimarisini uygulamak için cihazlar ile sunucu arasında konuşulan iki ana protokol vardır: RADIUS ve TACACS+. (CCNA sınavında aralarındaki farklar çok sık sorulur).

Özellik	RADIUS	TACACS+
Standardı	Açık Standart (IETF)	Cisco'ya Özgü (Cisco Proprietary)
Taşıma Protokolü	**UDP** (Port 1812, 1813)	**TCP** (Port 49)
Şifreleme (Encryption)	Sadece **Parolayı** şifreler. (Kullanıcı adı düz metin gider).	Tüm paketi (Payload) **tamamen şifreler**.
Kimlik Doğrulama / Yetki	Authentication ve Authorization işlemlerini **birleşik** yapar.	Authentication ve Authorization işlemlerini **ayrı ayrı** yapar.

Özetle: TACACS+ cihaz yönetimi için daha güvenli ve esnektir, RADIUS ise daha çok son kullanıcıların ağa erişimi (Örn: 802.1X Wi-Fi doğrulaması) için tercih edilir.

3. Yönlendirici (Router) Üzerinde RADIUS Yapılandırması

Bir cihazı AAA sunucusuna (RADIUS) bağlamak için sırasıyla AAA modelini açmalı, sunucuyu tanıtmalı ve bu doğrulama yöntemini uzak bağlantı (VTY) hatlarına uygulamalıyız.

> **Kritik Güvenlik Notu (Fallback/Yedek Mekanizması):** Sadece RADIUS sunucusuna güvenirsek ve sunucu çökerse (veya aradaki kablo koparsa) cihaza biz de giremeyiz. Bu yüzden yöntem listesinde her zaman RADIUS'un yanına yedek olarak "local" (cihazın kendi veritabanı) eklenir.

! 1. AAA Modelini Küresel Olarak Aktif Hale Getirme

```
Router(config)# aaa new-model

! 2. RADIUS Sunucusunun IP Adresini ve Ortak Şifreyi (Key) Tanımlama
! (Key, sunucu ile router'ın birbirine güvenmesi için kullanılan kapı şifresidir)
Router(config)# radius-server host 192.168.1.100 key CiscoGizliSifre123

! (Güncel IOS Sürümlerinde bu komut şu şekilde de yazılabilir:)
! Router(config)# radius server MERKEZ_RADIUS
! Router(config-radius-server)# address ipv4 192.168.1.100
! Router(config-radius-server)# key CiscoGizliSifre123

! 3. Kimlik Doğrulama Yöntem Listesi (Method List) Oluşturma
! Kural Oku: Giriş (login) için varsayılan (default) olarak önce RADIUS grubuna sor,
! Eğer RADIUS sunucusuna hiç ulaşılamıyorsa cihazın KENDİ YEREL (local) veritabanına bak.
Router(config)# aaa authentication login default group radius local

! (Yerel veritabanında mutlaka bir acil durum hesabı olmalıdır)
Router(config)# username admin privilege 15 secret YedekSifre123!

! 4. Oluşturulan Listeyi VTY (Telnet/SSH) Hatlarına Uygulama
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# end
```

4. RADIUS Sunucusu Tarafında Yapılması Gerekenler

Router tarafındaki ayarlar tek başına yeterli değildir. AAA sunucusu (Örneğin Windows Server NPS veya Packet Tracer içindeki Server cihazı) üzerinde şu üç ayarın yapılması zorunludur:

1. **Client Name (İstemci Adı):** Yönlendiricinizin adı (Örn: `R1_Ankara`).
2. **Client IP Address (İstemci IP Adresi):** Yönlendiricinin sunucuyla konuşacağı IP adresi.
3. **Secret (Ortak Anahtar):** Router'da `key` komutuyla girdiğimiz parolanın (`CiscoGizliSifre123`) aynısı sunucuya da girilmelidir. Aksi takdirde sunucu, router'dan gelen istekleri reddeder.
4. Sunucu üzerinde, cihaza bağlanacak ağ yöneticileri için (Örn: `Ahmet`, `Mehmet`) kullanıcı adları ve parolalar oluşturulur.

Erişim Kontrol Listeleri (ACL) - Bölüm 1: Temeller ve Standart ACL

ACL (Access Control List), bir yönlendirici (Router) üzerinden geçen paketleri belirli kriterlere göre (Kaynak IP, Hedef IP, Port vb.) inceleyen ve bu paketlere **Permit (İzin Ver)** veya **Deny (Engelle)** aksiyonu uygulayan bir kurallar dizisidir.

1. ACL Çalışma Mantığı ve Altın Kurallar

ACL'ler yukarıdan aşağıya doğru sırayla okunur. Bir paket bir kurala uyarsa (Match), o kural uygulanır ve listenin geri kalanına bakılmaz.

- **Sıralama Önemlidir:** En spesifik kurallar her zaman en üstte, en genel kurallar en altta olmalıdır.
- **Gizli Engelleme (Implicit Deny):** Her ACL'nin en sonunda görünmez bir `deny any` (her şeyi engelle) kuralı vardır. Eğer paket hiçbir kurala uymazsa otomatik olarak engellenir. Bu yüzden en az bir `permit` kuralı yazılmalıdır.
- **Yön Kavramı (Inbound vs Outbound):** * **In (Gelen):** Paket yönlendiricinin içine girmeden, yönlendirme kararı verilmeden önce kontrol edilir.
    - **Out (Giden):** Yönlendirme kararı verilmiş, çıkış kapısına yönelmiş paketler kontrol edilir.

2. Wildcard Mask (Joker Maskesi) Hesaplama

ACL yazarken Alt Ağ Maskesi (Subnet Mask) yerine **Wildcard Mask** kullanılır. Wildcard Mask'ta `0` bitleri "tam eşleşme lazım", `1` bitleri ise "fark etmez/serbest" anlamına gelir.

Hesaplama Formülü: `255.255.255.255 - Subnet Mask = Wildcard Mask`

Subnet Mask	Wildcard Mask	Açıklama
255.255.255.255	0.0.0.0	Sadece tek bir IP adresi (**host**)
255.255.255.0	0.0.0.255	Tüm bir C sınıfı ağı

255.255.255.192	0.0.0.63	64'lük bir blok aralığı
0.0.0.0	255.255.255.255	Tüm IP adresleri (**any**)

3. Standart ACL (Numaralı: 1-99)

Standart ACL'ler sadece **Kaynak (Source) IP** adresine bakarlar. Paketin nereye gittiği veya hangi protokolü (HTTP, FTP vb.) kullandığı ile ilgilenmezler.

- **Kural:** Standart ACL'ler her zaman **Hedefe en yakın** noktaya uygulanmalıdır.

Senaryo ve Yapılandırma

Senaryo: `192.168.10.0/24` ağındaki bilgisayarların, `172.16.1.100` IP'li sunucuya erişmesini engelleyelim, geri kalan herkes her yere gidebilsin.

```
! 1. ACL Kuralını Oluşturma (Numara: 10)
Router(config)# access-list 10 deny 192.168.10.0 0.0.0.255  ! Bu ağı engelle
Router(config)# access-list 10 permit any                    ! Geri kalan herkese izin ver (Implicit deny'ı aşmak için)

! 2. ACL'yi Arayüze Uygulama
! Kural hedefe yakın uygulanacağı için sunucunun bağlı olduğu Router bacağına gidiyoruz.
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip access-group 10 out                    ! Kapıdan çıkarken kontrol et
Router(config-if)# exit
```

4. VTY (SSH/Telnet) Hatları için ACL (access-class)

ACL'ler sadece arayüzlerden geçen trafiği değil, cihazın kendisine yapılan bağlantıları da kısıtlayabilir. Örneğin, sadece Bilgi İşlem (IT) bilgisayarının yönlendiriciye SSH yapmasına izin verebiliriz.

```
! 1. Sadece 192.168.1.3 IP'li host'a izin veren ACL

Router(config)# access-list 50 permit host 192.168.1.3
```

! 2. VTY hatlarına girip ACL'yi uygulama (access-group yerine access-class kullanılır)

Router(config)# line vty 0 4

Router(config-line)# access-class 50 in

Router(config-line)# end

Erişim Kontrol Listeleri (ACL) - Bölüm 2: Extended ve Named ACL

Standart ACL'ler sadece kaynağa bakarken, **Extended ACL**'ler; Kaynak IP, Hedef IP, Protokol (TCP/UDP/ICMP) ve Port numarasına göre çok daha detaylı filtreleme yapar.

1. Extended ACL (Numaralı: 100-199)

Extended ACL'ler, trafiği kaynağa mümkün olduğunca **en yakın** noktada engellemek için kullanılır. Böylece gereksiz trafik ağın içinde boşuna seyahat etmemiş olur.

Komut Yapısı: `access-list [no] [permit/deny] [protokol] [kaynak_ip] [kaynak_wildcard] [hedef_ip] [hedef_wildcard] [operatör] [port]`

Temel Yapılandırma Örnekleri:

! Senaryo 1: 192.168.20.0 ağındaki herkesin, 172.16.10.100 IP'li Web Sunucusuna (Port 80) erişmesine izin ver.

Router(config)# access-list 105 permit tcp 192.168.20.0 0.0.0.255 host 172.16.10.100 eq 80

! Senaryo 2: Aynı ağdaki hiç kimse sunucuya Ping (ICMP) atamasın.

Router(config)# access-list 105 deny icmp 192.168.20.0 0.0.0.255 host 172.16.10.100

! Senaryo 3: Geri kalan tüm trafiğe izin ver (Implicit deny'ı aşmak için).

Router(config)# access-list 105 permit ip any any

! ACL'yi Arayüze Uygulama (Kaynağa en yakın port)

Router(config)# interface gigabitEthernet 0/0

Router(config-if)# ip access-group 105 in

Operatörler:

- `eq` (Equal): Belirli bir porta eşitse (Örn: `eq 80`).
- `gt` (Greater than): Belirli bir porttan büyükse.
- `lt` (Less than): Belirli bir porttan küçükse.
- `range`: Belirli bir port aralığındaysa (Örn: `range 20 21` FTP için).

2. Named (İsimli) ACL ve Düzenleme İşlemleri

Numaralı ACL'lerin en büyük dezavantajı, tek bir kuralı değiştirmek istediğinizde tüm listeyi silip baştan yazmanız gerekmesidir. **Named ACL** ise hem isimlendirme kolaylığı sağlar hem de satır numaraları (Sequence Numbers) ile esnek düzenleme imkanı sunar.

Named ACL Oluşturma (Standart veya Extended)

! İsimli Standart ACL

Router(config)# ip access-list standard YONETICI_ERISIM

Router(config-std-nacl)# permit host 192.168.1.5

Router(config-std-nacl)# deny any

! İsimli Extended ACL

Router(config)# ip access-list extended PING_KORUMA

Router(config-ext-nacl)# deny icmp any any

Router(config-ext-nacl)# permit ip any any

ACL Düzenleme: Araya Kural Ekleme ve Silme

Varsayılan olarak kurallar 10, 20, 30... gibi 10'ar 10'ar artan numaralarla kaydedilir. Bu, araya kural eklememize olanak tanır.

Örnek Senaryo: Mevcut bir ACL'de 10. ve 20. kurallar arasına yeni bir izin ekleyelim.

! 1. Mevcut ACL'yi ve satır numaralarını gör

Router# show access-lists PING_KORUMA

! Çıktı:

! 10 deny icmp any any

! 20 permit ip any any

! 2. Düzenleme moduna gir

Router(config)# ip access-list extended PING_KORUMA

! 3. 15 numaralı satıra (10 ile 20 arasına) yeni bir izin ekle

Router(config-ext-nacl)# 15 permit icmp host 192.168.1.10 any

! 4. Mevcut bir kuralı satır numarasıyla sil

Router(config-ext-nacl)# no 10

Router(config-ext-nacl)# end

! Yeni Durumu Kontrol Et

Router# show access-lists

3. ACL İçin Kritik İpuçları ve Doğrulama

- **Wildcard Hesaplama Özeti:**
  - Tek bir IP için: `host 192.168.1.1` (veya `192.168.1.1 0.0.0.0`)
  - Herkes için: `any` (veya `0.0.0.0 255.255.255.255`)
- **ACL Yerleşimi:**
  - **Standart ACL:** Hedefe (Destination) en yakın noktaya.
  - **Extended ACL:** Kaynağa (Source) en yakın noktaya.

Doğrulama Komutları (Troubleshooting)

! Tüm ACL'leri ve paket eşleşme (match) sayılarını gösterir

Router# show access-lists

! Belirli bir arayüzdeki ACL uygulamasını gösterir

Router# show ip interface gigabitEthernet 0/0

! Yapılandırma dosyasındaki ACL satırlarını gösterir

Router# show running-config | include access-list

Önemli Not: ACL'ler Router'ın işlemcisini (CPU) yorar. Çok uzun listeler oluşturmak ağ performansını etkileyebilir. Mümkün olduğunca kısa ve öz tutulmalıdır.

1. Katman 2 Tehdit Modelleri ve Saldırı Türleri

Katman 2, cihazların aynı yerel ağ (LAN) içinde birbirlerini tanıdığı ve güvendiği katmandır. Buradaki protokoller (ARP, DHCP, STP) genellikle "güven" esasına dayanır ve kimlik doğrulama yapmazlar. Saldırganlar bu güveni suistimal ederek ağın kontrolünü ele geçirirler.

A. MAC Adres Tablosu Taşırma (MAC Flooding)

Switchler, hangi MAC adresinin hangi portta olduğunu **CAM (Content Addressable Memory)** adı verilen bir tabloda tutar. Bu tablonun fiziksel bir hafıza sınırı vardır.

- **Saldırı Mekanizması:** Saldırgan, `macof` gibi araçlar kullanarak Switch'e saniyeler içinde binlerce farklı ve sahte kaynak MAC adresine sahip çerçeve (frame) gönderir.
- **Sonuç:** Switch'in CAM tablosu tamamen dolar. Yeni ve gerçek bir cihaz ağa bağlandığında, Switch onu kaydedecek yer bulamaz. Bu durumda Switch, güvenli moddan çıkarak **"Fail-Open"** durumuna geçer. Yani, gelen her paketi (Unicast olsa bile) tüm portlara yaymaya (Flood) başlar.
- **Tehlike:** Switch artık bir **Hub** gibi davranmaktadır. Saldırgan, Wireshark açarak kendisine ait olmayan tüm trafiği (şifreler, özel yazışmalar) izleyebilir.

B. DHCP Saldırıları (Starvation ve Spoofing)

DHCP, ağdaki cihazlara otomatik IP dağıtan sistemdir ve saldırganlar için iki büyük kapı açar:

1. DHCP Starvation (DHCP Açlığı)

- **Saldırı:** Saldırgan, sürekli değişen sahte MAC adresleri kullanarak binlerce `DHCP Discovery` paketi yollar.
- **Sonuç:** DHCP sunucusu tüm bu isteklere IP ayırır ve kısa sürede elindeki IP havuzu (Pool) tükenir.
- **Etki:** Gerçek bir kullanıcı ağa bağlandığında IP alamaz. Bu bir **DoS (Denial of Service)** saldırısıdır.

2. DHCP Spoofing (Sahte DHCP Sunucusu)

- **Saldırı:** Saldırgan ağa kendi "Rogue DHCP" sunucusunu kurar. Starvation ile gerçek sunucuyu devre dışı bıraktıktan sonra, IP isteyen kullanıcılara kendi sahte paketlerini yollar.
- **Tehlike:** Saldırgan, kullanıcılara IP verirken **Default Gateway** (Varsayılan Ağ Geçidi) olarak kendi IP'sini verir. Kullanıcı internete çıktığını sanırken tüm trafiği saldırganın bilgisayarı üzerinden geçer (**Man-in-the-Middle**).

C. ARP Spoofing ve ARP Zehirlenmesi (ARP Poisoning)

ARP protokolü, "Bu IP kimin?" sorusuna "Benim, MAC adresim de bu" cevabını veren bir sistemdir. Ancak kimse bu cevabın doğruluğunu sorgulamaz.

- **Saldırı:** Saldırgan, ağdaki hedef bilgisayara ve yönlendiriciye (Router) sürekli **Gratuitous ARP** (istemsiz yanıt) mesajları yollar. Bilgisayara "Ben ağ geçidiyim", ağ geçidine ise "Ben o bilgisayarım" der.
- **Sonuç:** Cihazların ARP tabloları zehirlenir. Bilgisayar internete paket yolladığında paket Switch tarafından saldırganın MAC adresine yönlendirilir.
- **Araçlar:** `Ettercap`, `Bettercap` veya `arpspoof`.

D. VLAN Atlaması (VLAN Hopping)

VLAN'lar arasındaki izolasyonu aşmak için kullanılan iki yöntem vardır:

1. Switch Spoofing (DTP İstismarı)

Cisco portları varsayılan olarak `dynamic desirable` modundadır. Saldırgan, bilgisayarını bir Switch gibi gösterip **DTP (Dynamic Trunking Protocol)** mesajları yollar. Portu "Trunk" moduna geçirirse, tüm VLAN'ların trafiği o porta akmaya başlar.

2. Double Tagging (Çift Etiketleme)

Saldırgan paketine iki adet 802.1Q etiketi ekler.

1. Dış etiket, Switch'in **Native VLAN**'ı ile aynıdır.
2. İç etiket ise ulaşmak istediği hedef VLAN'dır. Switch paketi aldığında dış etiketi (Native VLAN olduğu için) söker ve diğer switch'e iletir. Diğer switch içteki etiketi görünce paketi o gizli VLAN'a teslim eder. Bu saldırı genellikle tek yönlüdür.

2. Savunma Teknikleri ve Yapılandırma (Kısım A)

Saldırıları bilmek bizi tetikte tutar, ancak doğru yapılandırma ağın "bağışıklık sistemini" oluşturur. Cisco anahtarlarda (Switch) bu özellikleri aktif hale getirirken dikkat edilmesi gereken kritik detaylar şunlardır:

A. Port Security (MAC Adres Güvenliği)

Amacı: MAC Flooding saldırılarını engellemek ve bir porta sadece bizim belirlediğimiz cihazların (veya belirli sayıda cihazın) takılmasını sağlamaktır.

Detaylı Yapılandırma Adımları:

Port Security sadece **Access** portlarında çalışır; Trunk portlarında etkinleştirilemez.

! 1. İlgili arayüz aralığına giriyoruz

Switch(config)# interface range fastEthernet 0/1-24

! 2. Portu zorunlu olarak access moduna çekiyoruz (Güvenlik gereği)

Switch(config-if-range)# switchport mode access

! 3. Port Security özelliğini aktif hale getiriyoruz

Switch(config-if-range)# switchport port-security

! 4. Maksimum izin verilen MAC adresi sayısını belirliyoruz

! (Örn: Bir kullanıcı portuna sadece 1 cihaz takılabilsin)

Switch(config-if-range)# switchport port-security maximum 1

! 5. MAC Adresi Öğrenme Yöntemi (Sticky):

! Cihaz takıldığı an MAC adresini öğrenir ve "running-config"e yazar.

! Cihazı kaydederseniz (write), bir sonraki açılışta sadece o cihaz çalışır.

Switch(config-if-range)# switchport port-security mac-address sticky

! 6. İhlal Durumunda Alınacak Aksiyon (Violation Mode):

! shutdown: Portu kapatır (err-disable yapar), yönetici açmalıdır (Varsayılan).

! restrict: Trafiği engeller, log üretir ve ihlal sayacını artırır.

! protect: Sadece trafiği engeller, hiçbir kayıt tutmaz (Önerilmez).

Switch(config-if-range)# switchport port-security violation shutdown

Doğrulama ve İzleme:

- `show port-security interface fa0/1` : İlgili portun güvenlik durumunu ve kaç ihlal (violation) yaşandığını gösterir.
- `show port-security address` : Kayıtlı (Sticky) MAC adreslerini listeler.

B. DHCP Snooping (DHCP Güvenliği)

Amacı: Sahte (Rogue) DHCP sunucularını engellemek ve DHCP Starvation (Açlık) saldırılarını durdurmaktır.

Çalışma Mantığı:

Switch üzerindeki portları ikiye ayırır:

1. **Trusted (Güvenilir):** DHCP sunucusunun veya diğer switchlerin bağlı olduğu portlardır. Buradan gelen `DHCP Offer` ve `ACK` paketlerine (sunucu paketleri) izin verilir.
2. **Untrusted (Güvenilmez):** Son kullanıcıların bağlı olduğu portlardır. Buradan sadece `DHCP Discover` (istemci paketi) gelebilir. Eğer bir kullanıcı bu porttan sahte sunucu paketi yollarsa Switch portu anında bloklar.

Detaylı Yapılandırma Adımları:

! 1. DHCP Snooping özelliğini global olarak açıyoruz

Switch(config)# ip dhcp snooping

! 2. Hangi VLAN'larda aktif olacağını belirtiyoruz (Çok Önemli!)

Switch(config)# ip dhcp snooping vlan 10,20,30

! 3. Güvenilir Portu Belirleme (Uplink/Server Portu):

! Eğer bu portu "trust" yapmazsanız, hiçbir kullanıcı IP alamaz!

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# ip dhcp snooping trust

Switch(config-if)# exit

! 4. Starvation (Açlık) Koruması (Rate Limiting):

! Kullanıcı portlarından saniyede gelebilecek DHCP paketi sayısını sınırlarız.

! Saldırgan saniyede binlerce sahte istek atamaz.

Switch(config)# interface range fastEthernet 0/1-24

Switch(config-if-range)# ip dhcp snooping limit rate 10

DHCP Snooping Binding Table:

DHCP Snooping sadece güvenliği sağlamaz, aynı zamanda bir **veritabanı** oluşturur. Hangi MAC adresi hangi IP'yi hangi porttan almış, bunu kaydeder. Bu veritabanı, bir sonraki aşamada anlatacağımız **DAI (Dynamic ARP Inspection)** için temel teşkil edecektir.

Doğrulama Komutları:

- `show ip dhcp snooping` : Genel ayarları ve hangi VLAN'ların korunduğunu gösterir.
- `show ip dhcp snooping binding` : Kimin hangi IP'yi kiraladığını gösteren o meşhur tabloyu listeler.

C. Dynamic ARP Inspection (DAI)

Amacı: ARP Zehirlenmesi (ARP Poisoning) ve Ortadaki Adam (MitM) saldırılarını engellemektir.

Çalışma Mantığı:

DAI, switch üzerinden geçen her ARP paketini yakalar. Paketin içindeki IP ve MAC adresi eşleşmesini, daha önce oluşturulan **DHCP Snooping Binding Table** ile karşılaştırır.

- Eğer bir saldırgan "Ben Gateway'im" diye sahte bir ARP cevabı yollarsa, DAI bu MAC adresinin o IP ile eşleşmediğini (veritabanında olmadığını) görür ve paketi anında çöpe atar (drop).

Detaylı Yapılandırma Adımları:

! 1. DHCP Snooping'in açık ve veritabanının oluşmuş olması şarttır!

! 2. İlgili VLAN'larda DAI'yi aktif hale getiriyoruz

Switch(config)# ip arp inspection vlan 10,20

! 3. Güvenilir Portu Belirleme (Uplink/Router Portu):

! Router'lar genellikle statik IP kullandığı için DHCP veritabanında olmayabilirler.

! Bu yüzden Router'a giden portu "trust" (güvenilir) yapmalıyız.

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# ip arp inspection trust

Switch(config-if)# exit

! 4. Ekstra Kontroller (Opsiyonel):

! Sadece IP/MAC değil, çerçevenin içindeki kaynak/hedef MAC uyumuna da bakabiliriz.

Switch(config)# ip arp inspection validate src-mac dst-mac ip

Doğrulama Komutları:

- `show ip arp inspection` : Hangi VLAN'larda aktif olduğunu ve kaç adet sahte ARP paketinin engellendiğini (drops) gösterir.
- `show ip arp inspection statistics vlan 10` : VLAN bazlı istatistikleri listeler.

D. IP Source Guard (IPSG)

Amacı: IP Adresi Sahteciliğini (IP Spoofing) engellemektir.

Çalışma Mantığı:

Saldırganın, kendisine atanan IP adresini manuel olarak değiştirip ağda yetkili bir bilgisayarın (Örn: Müdürün bilgisayarı) IP'sini taklit etmesini önler. Port düzeyinde bir filtre oluşturur; porttan gelen paketin kaynak IP'si DHCP tablosundaki ile tutmuyorsa trafik geçemez.

Detaylı Yapılandırma Adımları:

! 1. DHCP Snooping açık olmalıdır.

! 2. İlgili kullanıcı portuna (Access Port) giriyoruz

Switch(config)# interface range fastEthernet 0/1-24

! 3. IP Kaynak Korumasını Aktif Ediyoruz

! "ip-address" seçeneği sadece IP'yi, "mac-address" ile birlikte kullanımı ikisini birden kontrol eder.

Switch(config-if-range)# ip verify source

! (Veya hem IP hem MAC kontrolü için):

! Switch(config-if-range)# ip verify source port-security

E. STP Koruması (BPDU Guard ve Root Guard)

Amacı: Ağın topolojisini (Spanning Tree) bozmaya çalışan saldırıları veya yanlışlıkla takılan cihazların ağda loop (döngü) yaratmasını engellemektir.

1. BPDU Guard (Erişim Portları İçin)

Bilgisayar takılan bir porta yanlışlıkla bir Switch takılırsa, o porttan BPDU paketleri gelmeye başlar. BPDU Guard, bir uç porttan (PortFast açık olan port) BPDU paketi aldığı an portu **err-disable** (hata) moduna sokup kapatır.

Switch(config)# interface range fa 0/1-24

Switch(config-if-range)# spanning-tree bpduguard enable

2. Root Guard (Omurga Portları İçin)

Saldırgan, ağa çok güçlü (Priority değeri 0 olan) bir switch takıp kendini **Root Bridge** ilan etmeye çalışabilir. Root Guard etkinleştirilen bir porttan, mevcut Root Bridge'den daha üstün bir BPDU (superior BPDU) gelirse, Switch o portu "Root-Inconsistent" moduna sokup trafiği keser.

! Bu komut genellikle Core Switch'in, diğer switchlere bağlandığı portlarda kullanılır.

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# spanning-tree guard root

3. Siber Güvenlik Araç Kutusu ve Saldırı Simülasyonu (Detaylı)

Bu bölümde, siber güvenlik dünyasında yukarıdaki protokolleri test etmek (veya sömürmek) için kullanılan araçları detaylandırıyoruz:

1. **Yersinia:** Katman 2'nin "İsviçre Çakısı"dır.
    - **Ne Yapar?** Sahte STP Root Bridge olabilir, DHCP Starvation başlatabilir, sahte CDP mesajları yollayabilir.
    - **Savunma:** Port Security, DHCP Snooping, BPDU Guard.
2. **Ettercap / Bettercap:** ARP Zehirlemesi (ARP Poisoning) için en çok kullanılan araçtır.
    - **Ne Yapar?** Ağı tarar, cihazları bulur ve araya girerek (MitM) trafiği sniff eder.
    - **Savunma:** DAI (Dynamic ARP Inspection).
3. **Macof (dsniff):** CAM tablosu taşırma (MAC Flooding) saldırısı yapar.
    - **Ne Yapar?** Saniyede binlerce rastgele MAC adresi üretip Switch'e basar.
    - **Savunma:** Port Security (Maximum 1).