

## LAN Security Threats

Kullandığımız network, yapısı itibariyle katmanlı bir mimaridir ve bu katmanların herhangi birinde sorun oluştuğunda sorunun olduğu katmandan itibaren üst katmanlar da etkilenmektedir. Bu doğrultuda güvenlik tehditlerinin de benzer şekilde L1'den başladığını söyleyebiliriz. Her katmanın kendine özgü zafiyetleri vardır. Bu zafiyetlerden kaynaklanan güvenlik tehditleriyle beraber bu tehditlere karşılık alınabilecek önlemler de bulunmaktadır.

L1 güvenliği için kabinetlerin/network cihazlarının bulunduğu oda ve kablolanın güvenliği göz önünde bulundurulmalıdır.

L2'deki güvenlik tehditleri aslında aynı network içerisinde gerçekleştirilebilecek saldırıları kapsamaktadır. Network içerisindeki L2 cihazlar switchler olduğu için tehditlerin odağı da switchlerdir. Bu tehditlere karşı alınabilecek önlemler de switchler üzerinde alınmaktadır. Bu saldırılar;

### 1- MAC/CAM Table Attacks

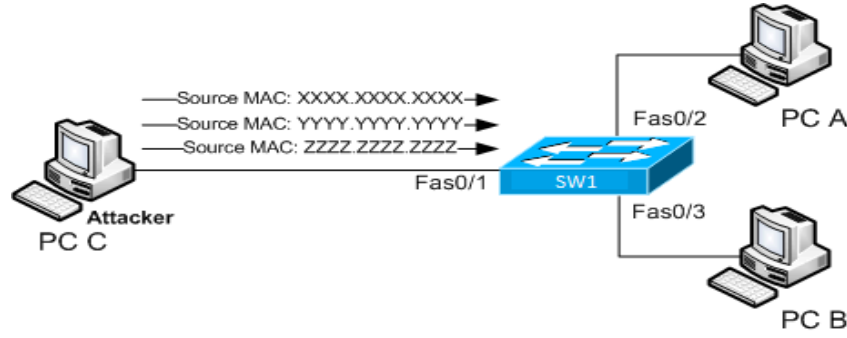
| → MAC Flooding Attack - Switchler kendilerine gönderilen framelelerin kaynak MAC adreslerini MAC/CAM Address tablosuna kaydederler. Tabloya kaydedilen adresler belirli bir süre kullanılmadığında tablodan silinir. Bu tablo sayesinde switchler, kendilerine gönderilen frameleleri hangi portlarına anahtarlama kararı verirler. Ne yazık ki bu tabloların adres kaydetme kapasitesi sınırlıdır. Bu kapasite dolduğunda, switchler kendilerine gönderilen frameleleri bütün portlarına anahtarlama (yani bir Hub gibi çalışmaya) başlar.

MAC Flood saldırısında saldırganlar switchlerdeki MAC Address tablosunu doldurarak switchin bir HUB gibi kendisine gelen frameleleri bütün portlarına anahtarlama sağlar. Bu sayede networkte oluşturulan bütün trafik saldırgan bilgisayarına da gönderilecektir. Bu durumu devam ettirebilmek için saldırganın tek yapması gereken MAC adreslerinin tabloda kayıt süreleri dolmadan yeni MAC adresine sahip frameleler göndererek tablonun dolu kalmasını sağlamaktır.

■ Burada dikkat edilmesi gereken nokta saldırı gerçekleştirilirken trafiği dinlenmek istenen istemcilerin MAC adreslerinin tabloda bulunmaması gerekiyor. Çünkü switch kendisine gelen framelelerin MAC adresini tabloda bulamadığında hedef MAC adresini öğrenebilmek için bütün portlarına anahtarlar. Gönderilen frameleden cevap döndüğünde ise framein kaynak MAC adresini MAC Address tablosuna kaydeder ki yeniden trafik oluşturulduğunda hangi porta anahtarlanacağı belli olsun. MAC Flood saldırısında MAC adres tablosu dolu olacağı için switch yeni MAC adresi kaydedemeyecektir. Bu nedenle MAC Flood saldırısı başladığı andan itibaren MAC adresi tabloda olmayan her istemcinin trafiği switchin bütün portlarına anahtarlanaacaktır.

Switchler başka bir switch ile bağlı olduğu portlarında birden fazla MAC adresi öğrenebiliyor. Bu durum istemci bağlı portlar için de geçerlidir. Zaten bu sayede frameleler farklı switchler üzerinden hedeflerine ulaştırılabilmektedir. Bir MAC Flood saldırısında da saldırgan tek bir port üzerinden farklı MAC adresine sahip frameleler gönderdiği için MAC tablosunda benzer durum gözlenecektir. Yani bir MAC Flood saldırısı olduğunda saldırının hangi switchin hangi portundan yapıldığı herhang bir switchin MAC Address tablosuna bakılarak tespit edilebilir (istemci bağlı portlardan normalde tek bir MAC adresi öğrenilmesi gerekirken birçok MAC adresi öğrenildiği görülecektir).

- Switchlerin farklı switchlere bağlı portlarından birden fazla MAC adresi öğrenebildiği gibi networkte gerçekleştirilecek bir MAC Flood saldırısında da sadece saldırının gerçekleştirildiği switchin MAC Address tablosu değil, networkteki birbirine bağlı bütün switchlerin MAC Address tablosu dolacaktır.
- Önlem olarak;
  - Switchlerde Port Security özelliği kullanılabiliyor. Bu özellik bir sonraki konuda (Switch Security) açıklanmıştır. **(Detaylı bilgi için CCNA - 2.11 - Switch Security Configuration notunu inceleyebilirsiniz).**



## 2- VLAN Attacks

| → VLAN Hoping Attack – Cisco switchlerde portlar varsayılanda DTP (Dynamic Trunking Protocol) modunda gelmektedir. VLAN Hoping saldırısı, saldırganın modu DTP bırakılan switch portuna bağlanarak portun kendini Trunk moduna alınması sağlamasıyla başlıyor. Bu sayede saldırgan bütün VLAN trafiğini dinleyebilirken aynı zamanda Trunk portlarda frame'lere eklenen 802.1q başlığına müdahale edip istediği VLAN'e trafik gönderebilir.

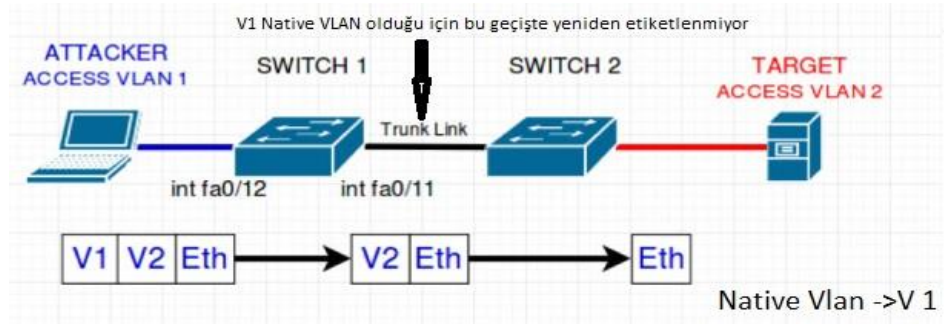
- Önlem olarak;
  - Kullanılan/kullanılmayan bütün portlar Access moduna alınmalıdır.

| → VLAN Double Tagging Attack – Switchlerde istemci bağlanan portlarda 802.1q etiketi eklenmiyor. Yinde de Access moduna alınmış porttan VLAN etiketine sahip bir frame gönderilirse switch bu frame'i alıp etiket bilgisini çıkardıktan sonra paketi ilgili portlarına anahtarlıyor. VLAN Double Tagging saldırısı için saldırganın Native VLAN'a dahil olması gerekiyor.

Saldırı için ilk olarak saldırgan gönderilecek frame içerisine göndermek istediği VLAN ve kendi bulunduğu VLAN bilgisi olmak üzere iki tane 802.1q etiketi ekliyor. Frame switch'e ulaştığında ilk etiket çıkartılarak ilgili portlara anahtarlaniyor. Burada frame farklı bir switch'e (ikinci bir switch üzerinde) anahtarlaniırken Native VLAN'a dahil olduğu için yeni etiket bilgisi eklenmeden anahtarlaniyor. Bu nedenle, frame üzerinde sadece saldırganın paketi gönderirken eklediği ikinci VLAN etiketi (frame'i ulaştırmak istediği VLAN etiketi) kaldığı için frame karşı switch'e geçtiğinde saldırganın paketi istenen VLAN'a anahtarlaniş oluyor.

- VLAN Double Tagging Attack, tek yönlü bir saldıdır. Gönderilen frame'lerden dönüş alınamaz.

- Önlem olarak;
  - Native VLAN farklı bir VLAN 'a alınmalı (Native VLAN varsayılanda VLAN 1'dir).
  - Native VLAN sadece switchler arasında kullanılmalıdır. Yani herhangi bir istemcinin bağlanacağı port Native VLAN'a alınmamalı.



### 3- DHCP Attacks

| → DHCP Starvation Attack - Saldırganın DHCP sunucusundan farklı MAC adresleriyle sürekli yeni ip istemesine dayanan bir saldırıdır. Saldırgan saldırıya ip havuzunda verilecek ip adresi kalmayınca kadar devam eder. Ip havuzunda verilecek ip adresi kalmadığında, networke yeni bağlanmak isteyen istemcilere ip bilgileri verilemeyeceği için networke bağlanamazlar.

■ Önlem olarak;

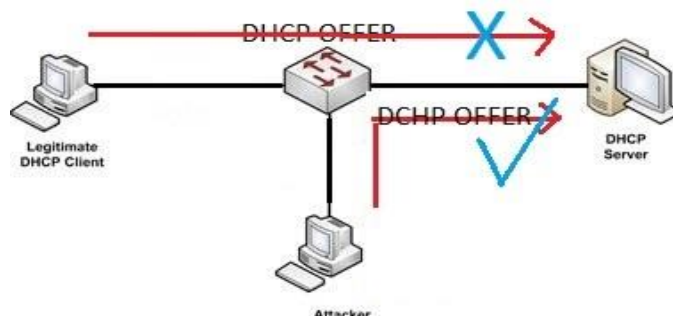
- Switchlerde Port Security özelliği kullanılabiliyor. Bu özellik bir sonraki konuda (Switch Security) açıklanmıştır. **(Detaylı bilgi için CCNA - 2.11 - Switch Security Configuration notunu inceleyebilirsiniz).**

| → DHCP Spoofing Attack / Rouge DHCP Server Attack – İstemci networke bağlandığında ip adresi alabilmek için DHCP DISCOVER paketiyle ip bilgisi alabileceği bir DHCP sunucusu arar. DHCP Spoofing Attack, saldırgan bilgisayarı üzerinde sahte bir DHCP sunucusu ayağa kaldırmasıyla başlar. İstemci DHCP DISCOVER paketi gönderdiğinde saldırgan legal DHCP sunucusundan daha hızlı DHCP OFFER paketi göndererek istemciye farklı ip bilgileri sunar. İstemci genelde ilk gelen DHCP paketini kabul ettiği için saldırganın sunduğu sahte ip bilgilerini kabul ederek kullanmaya başlayacaktır.

Saldırgan ip bilgisi olarak istemciye sahte gateway, sahte DNS veya yanlış ip adres bilgisi sunabilmektedir. Saldırgan;

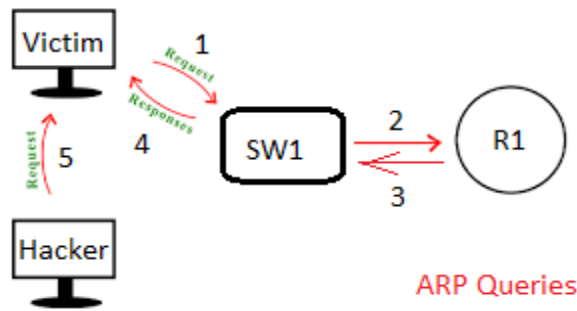
- Kurban istemciye gateway adresi olarak kendi ip adresini verip istemcinin internet trafiğinin kendi bilgisayarı üzerinden geçmesini sağlayabilir.
- Kurban istemciye sahte DNS bilgisi verip istemciyi istediği sitelere yönlendirebilir. Bu sayede fake bir siteye yönlendirilerek istemcinin parola bilgilerini çalabilir veya zararlı yazılımlar indirmek gibi çeşitli saldırılar yapabilir.
- Yanlış ip/subnet bilgileri vererek istemcinin networke bağlanmasına engel olabilir.
- Önlem olarak;

- DHCP Snooping özelliği aktive edilebiliyor. Bir sonraki konuda (Switch Security) detaylı açıklanmıştır **(Detaylı bilgi için CCNA - 2.11 - Switch Security Configuration notunu inceleyebilirsiniz).**



#### 4- ARP Attacks

|→ ARP Poisoning Attack – Farklı bir networke paket gönderileceği zaman paket öncelikle gatewaye gönderilir. Bunun için de paketi gönderecek istemcinin ARP sorgusu yaparak gatewayin MAC adresinin öğrenmesi gerekiyor. İstemcinin gönderdiği ARP Request paketine karşılık gateway ARP Reply paketiyle istemciye MAC adresini bildirir. Gateway MAC adresi öğrenildikten sonra istemci paketlerini gateway üzerinden internete çıkarmaya başlayabilir. ARP Poisoning Attack, kurban istemci gateway MAC adresini öğrendikten sonra saldırgan içinde olması gereken gateway ip adresiyle kendi MAC adresinin bulunduğu yeni bir ARP Reply paketini kurban istemciye göndererek başlar. Yeni ARP Reply paketini alan kurban istemci ARP tablosundaki gateway MAC adresini saldırganın MAC adresiyle değiştirecektir. Bu durumda kurban istemci internete çıkarmak istediği paketleri saldırgan bilgisayarına gönderecektir. Saldırgan ise istemcinin kendisine gönderdiği paketleri gatewaye yönlendirerek istemcinin internete kendi bilgisayarını üzerinden çıkmasını sağlamaktadır.



|→ IP Spoofing Attack – Saldırganın farklı ip adresleri kullanarak trafik oluşturmasıyla gerçekleştiriliyor. Bu saldırıda saldırganın kullanıldığı ip adresi farklı networke ait ip adresi olabilirken kendi networkünde farklı bir istemcinin kullandığı ip adresi de olabilir. Saldırgan bu saldırı üzerinden MITM (Man in the Middle) veya DoS (Denial of Server) gibi çeşitli saldırılar da geliştirebilmektedir.

- Benzer şekilde MAC adresi için de farklı MAC adresine sahip paketler oluşturulabiliyor. Buna MAC Spoofing Attack deniliyor.
- Önlem olarak;
  - IP Source Guard (IPSG) özelliği kullanılıyor.

#### 5- STP Attacks

|→ STP Manipulation Attack – STP protokolünde cihazlar aralarında belirli aralıklarla BPDU paketleri göndererek networkte loop olup olmadığını kontrol ediyor ve bu doğrultuda belirli portların bloklanmasını sağlıyor. STP Manipulation saldırısıyla saldırgan kendi bilgisayarında STP protokolünü ayağa kaldırarak networke bir switch gibi BPDU paketleri gönderiyor. Bu sayede networke gönderdiği BPDU paketinde oynamalar yaparak kendisini Root switch seçtirebiliyor veya kendi Priority değerini sürekli değiştirerek Root switchin sürekli değişmesini neden olabiliyor (bloklama portların sürekli değişmesine neden oluyor). Bu gibi zafiyetleri kullanarak networkte aksaklıklara neden olabiliyor.

- Arica aynı anda iki switche birden bağlanabilirse switchlerin priority değerleriyle oynayarak istediği trafiği kendi üzerine çekebilmektedir.
- Önlem olarak;
  - Switçlerde BPDU Guard koruması devreye alınıyor (Detaylar için **CCNA - 2.05 – STP notlarını inceleyebilirsin**).

## 6- CDP (Cisco Discovery Protocol) Attacks

| → CDP Reconnaissance – Cisco cihazlar bilgilerini her 30 saniyede bir bütün portlarından yayınlayarak bağlı oldukları Cisco cihazlara bildirirler. Bu sayede switch'e bağlanan bir istemci switch hakkında işletim sistemi/sürümü, ip adres, Native VLAN, Voice VLAN bilgisi gibi birçok bilgiyi elde edebiliyor.

- Bu durum open standart olan LLDP protokolü için de geçerlidir.
- Önlem olarak;
  - CDP protokolü bütün portlarda kapatılabilir veya istemci bağlı portlarda kapatılarak sadece switch bağlı portlarda kullanılabilir.

## NOT

- Macof, MAC Flood saldırısı için kullanılan yaygın araçlardan biridir.