L2 Güvenlik Tehditleri

Kullanılan network yapısı katmanlı mimaridir ve bu katmanların herhangi birinde sorun oluştuğunda sorunun oluştuğu katmandan itibaren üst katmanları da etkileyecektir. Bu nedenle güvenlik tehditlerinin L1'den başladığını söyleyebiliriz. Her katmanın kendisine özgü güvenlik tehtidi ve bu tehtidlere karşılık alınabilecek önlemleri vardır.

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

L2'deki güvenlik tehditleri aslında aynı network içerisinde gerçekleştirilebilecek saldırıları kapsamaktadır. Network içerisindeki L2 cihazlar switchler olduğu için saldırılar da önlemleri de switchler üzerinden getirilmektedir. Bu saldırılar;

- MAC/CAM Table Attacks
  |→ MAC Flooding Attack - Switchler kendilerine gönderilen framlelerin kaynak MAC adreslerini MAC/CAM Address tablosuna kaydederler. Tabloya kaydedilen adresler belirli bir süre kullanılmadığında tablodan silinir. Bu tablo sayesinde switchler kendilerine gönderilen frameleri hangi portlarına anahtarlayacağına karar verirler. Ne yazık ki bu tabloların adres kaydetme kapasitesi sınırlıdır. Bu kapasite dolduğunda switch bir HUB gibi çalışmaya başlar ve kendisine gönderilen frameleri bütün portlarına anahtarlamaya başlar.

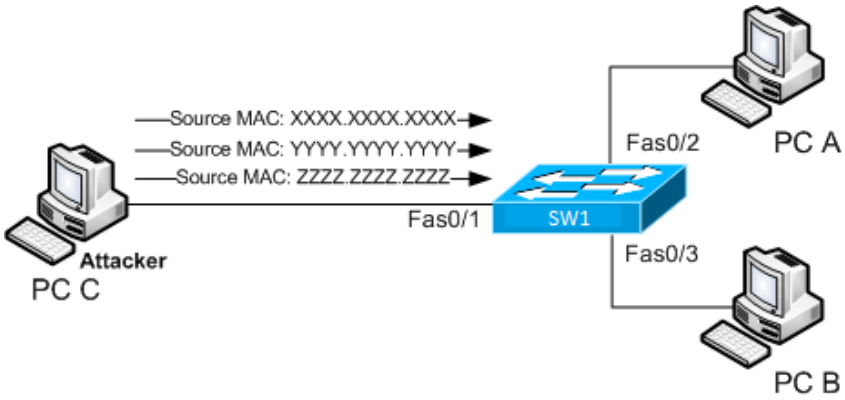
  MAC Flood saldırısında da saldırganlar switchlerdeki MAC adres tablosunu doldurarak switchin bir HUB gibi kendisine gelen frameleri bütün portlarına anahtarlamasını sağlar. Bu sayede networkte oluşturulan bütün trafik saldırgan bilgisayarına da gönderilecektir. Bu durumu devam ettirebilmek için saldırganın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

  - Burada dikkat etmesi gereken nokta saldırı gerçekleştirilirlken trafiğini dinlenmek istenen istemcilerin MAC adreslerinin tabloda bulunmaması gerekiyor. Çünkü switch kendisine gelen framelerin MAC adresini tabloda bulamadığında hedef MAC adresini öğrenebilmek için bütün portlarına anahtarlar. Gönderilen frameden cevap döndüğünde ise framein kaynak MAC adresini MAC Address tablosuna kaydeder ki yeniden trafik oluşturuldupunda hangi porta anahtarlanacağı belli olsun. MAC Flood saldırısında MAC adress tablosu dolu olacağı için switch yeni MAC adresi kaydedemeyecektir. Bu nedenle MAC Flood saldırısı başladığı andan ihtibaren MAC adresi tabloda olmayan her istemcinin trafiği switchin bütün portlarına anahtarlanacaktır.

  Switchler başka bir switch ile bağlı olduğu portlarında birden fazla MAC adresi öğrenebiliyor. Bu durum istemci bağlı portları için de geçerlidir. Zaten bu sayede frameler farklı switchler üzerinden hedeflerine ulaştırılabilmektedir. Bir MAC Flood saldırısında da saldırgan tek bir port üzerinden farklı MAC adresine sahip frameler gönderdiği için MAC tablosunda benzer durum gözlenecektir. Yani bir MAC Flood saldırısı olduğunda bunu herhang bir switchin MAC Adress tablosuna bakarak saldırının yapıldığı swtich ve port bilgileri tespit edilebilir.

  - Switchlerin farklı swtichlere bağlı portlarından birden fazla MAC adresi öğrenebildiği gibi networkte gerçekleştirilecek bir MAC Flood saldırısında da sadece saldırının yapıldığı switchin MAC Adres tablosunu değil aynı zamanda networkteki birbirine bağlı bütün switchlerin MAC adres tablıosunu dolduracaktır.

- Önlem olarak;
    - Switchlerde PortSecurity özelliği kullanılabiliyor. Bu özellik bir sonraki konuda (Swithch Security) açıklanamıştır.



- VLAN Attacks

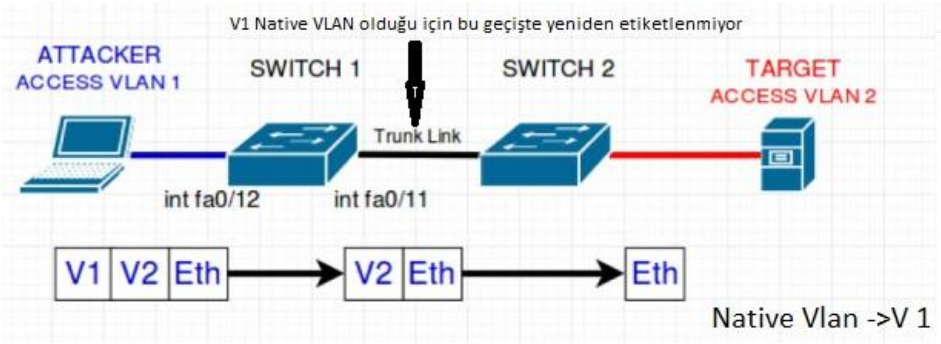
|→ VLAN Hoping Attack – Cisco swihclerde portlar varsayılanda DTP (Dynamic Trunking Protocol) modundan gelmektedir. VLAN Hoping saldırısı, saldırganın modu DTP bırakılan porta bağlanarak portun kendini Trunk moduna çekilmesiyle gerçekleştiriliyor. Bu sayede saldırgan bütün VLAN trafiğini dinleyebilirken aynı zamanda Trunk portlarda framelere eklenen 802.1q başlığına müdahale edip istediği VLAN'de trafik oluşturabiliyor

- Bu durum sadece switchler arasında trafiğine izin verilen VLAN'lar için geçerlidir. Yani saldırganın bağlı olduğu switche gelen VLAN'ların trafiğini dileyebilir veya trafik oluşturabilir.
- Önelm 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 bunu framei 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 switche ulaştığında ilk etiket çıkartılarak ilgili portlara anahtarlanıyor. Burada frame farklı bir switche anahtarlanıtken Native VLAN'a dahil olduğu için yeni etiket bilgisi eklenmmeden anahtarlanıyor. Bu nedenle frame üzerinde sadece saldırganın paketi gönderirken eklediği ikinci VLAN etiketi (framei ulaştırmak istediği VLAN etiketi) kaldığı için frame karşı switche geçtiğinde saldırganın istedği VLAN'a anahtarlanmış oluyor. Bu sayede frame istenilen VLAN'a ulaşmış oluyor.

- VLAN Double Tagging Attack, tek yönlü bir saldırıdır. Gönderilen framelerden dönüş alınamaz.
- Önelm olarak;
    - Native Vlan farklı bir VLAN 'a alınmalı (Native VLAN varsayılanda VLAN 1'dir).
    - Native VLAN sadece switchler arasında kullanılmalı. Yani herhangi bir istemcinin bağlanacağı port Native VLAN'a alınmamalı.



- DHCP Attacks

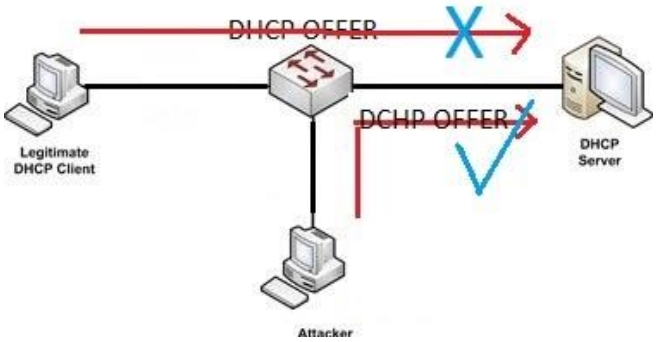
|→ DHCP Starvation Attack - Saldırganın DHCP sunucusundan farklı MAC adresleriyle sürekli yeni ip istemesine dayanan bir saldırıdır. Saldırı ip havuzunda verilecek ip adresi kalmayıncaya kadar devam eder. Ip havuzunda verilecek ip adresi kalmadığında, networke yeni bağlanmak isteyen istemcilere ip bilgileri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

- Önlem olarak;
  - Switchlerde PortSecurity özelliği kullanılabiliyor. Bu özellik bir sonraki konuda (Swithch Security) açıklanamıştır.

|→ 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 bilgilerii kabul ederek kullanmaya başlayacaktır.

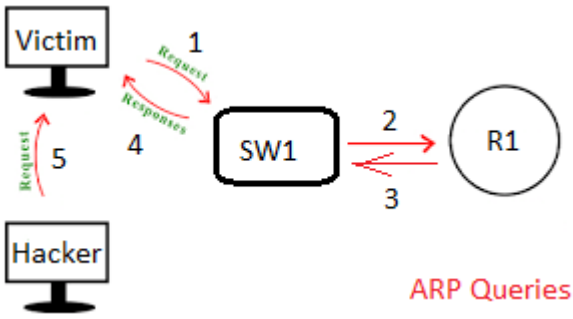
Saldırgan ip bilgisi olarak istemciye sahte gateway, sahte DNS veya yanlış ip adres bilgisi sunabilmektedir.

- Gateway adresi olarak kendi ip adresini verip istemcinin internet trafiğinin kendi bilgisayarı üzerinden geçmesini sağlayabilir.
- Sahte DNS bilgisi verip istemciyi istediği sitelere yönlendirebilir. Bu sayede fake bir siteye yönlendirerek istemcinin parola bilgilerini çalabilir veya zararlı yazılımlar indirtmek gibi çeşitli saldırılar yapabilir.
- Yanlış ip/subnet bilgileri vererek sitemcinin networke bağlanmasına engel olabilir.
- Önlem olarak;
  - DHCP Snooping özelliği aktive edilebiliyor. Bir sonraki konuda (Switch Security) detaylı açıklanmıştır.



- ARP Attacks

  |→ARP Poisining 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 ve istemci paketlerini gateway üzerinden internete çıkarmaya başlayabilir.
  ARP Poisining Attack, istemci gateway MAC adresini öğrendikten sonra içinde olması gereken gateway ip adresiyle kendi MAC adresinin bulunduğu yeni bir ARP Reply paketini istemciye göndererek başlar. Yeni ARP Reply paketini alan istemci ARP tablosundaki gateway MAC adresini saldırgan MAC adresiyle değiştirecektir. Bu sayede istemci internete çıkarmak istediği paketleri saldırgan bilgisayarına gönderecektir. Saldırgan ise istemcinin kendisine gönderdiği paketleri gatewaye yönlendirerek istemcinin internete kendi bilgisayarı üzerinden çıkmasını sağlamaktadır.



  |→ IP Spoofing Attack – Saldırganın farklı ip adresleriyle trafik oluşturmasıyla gerçekleştiriliyor. Bu saldırıda saldırganın kullanılandığı 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 adrei için de farklı MAC adresine sahip paketler oluşturulabiliyor. Buna MAC Spoofing Attack deniliyor.
  - Önlem olarak;
    - IP Source Guard (IPSG) özelliği kullanılıyor.

- STP Attacks

  |→ STP Manipulation Attack – STP protokolünde cihazlar aralarında belirli aralıklarla BPDU paketleri göndererek networkte loop oluşup oluşmadığını kontrol ediyor ve belirli portların bloklanmasını sağlıyordu. 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. Bu durumda kendi priority değerini sürekli değiştirerek Root switchin sürekli değişmesini sağlayarak bloklana portların sürekli değişmesine neden olabilir. Bu sayede network trafiğinde aksamalar olacaktır.

  - Arıca aynı anda iki switche birden bağlanabilirse swtichlerin priority değerleriyle oynayarak istediği trafiği kendi üzerine çekebilmektedir.
  - Önlem olarak;
    - Swwitchlerde BPDU Guard koruması devreye alınıyor.

- CDP (Cisco Discovery Protocol) Attacks
  |→ CDP Reconnaissance – Cisco cihazlar bilgilerini her 30 saniyede bir bütün portlarından yayınlayarak bağlı oldukları Cisco cihazlara bildirirler. Bu satede switche 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.

NOTLAR

- Macof, MAC Flood saldırısı için kullanlan yaygın araçlar arasındadır.