



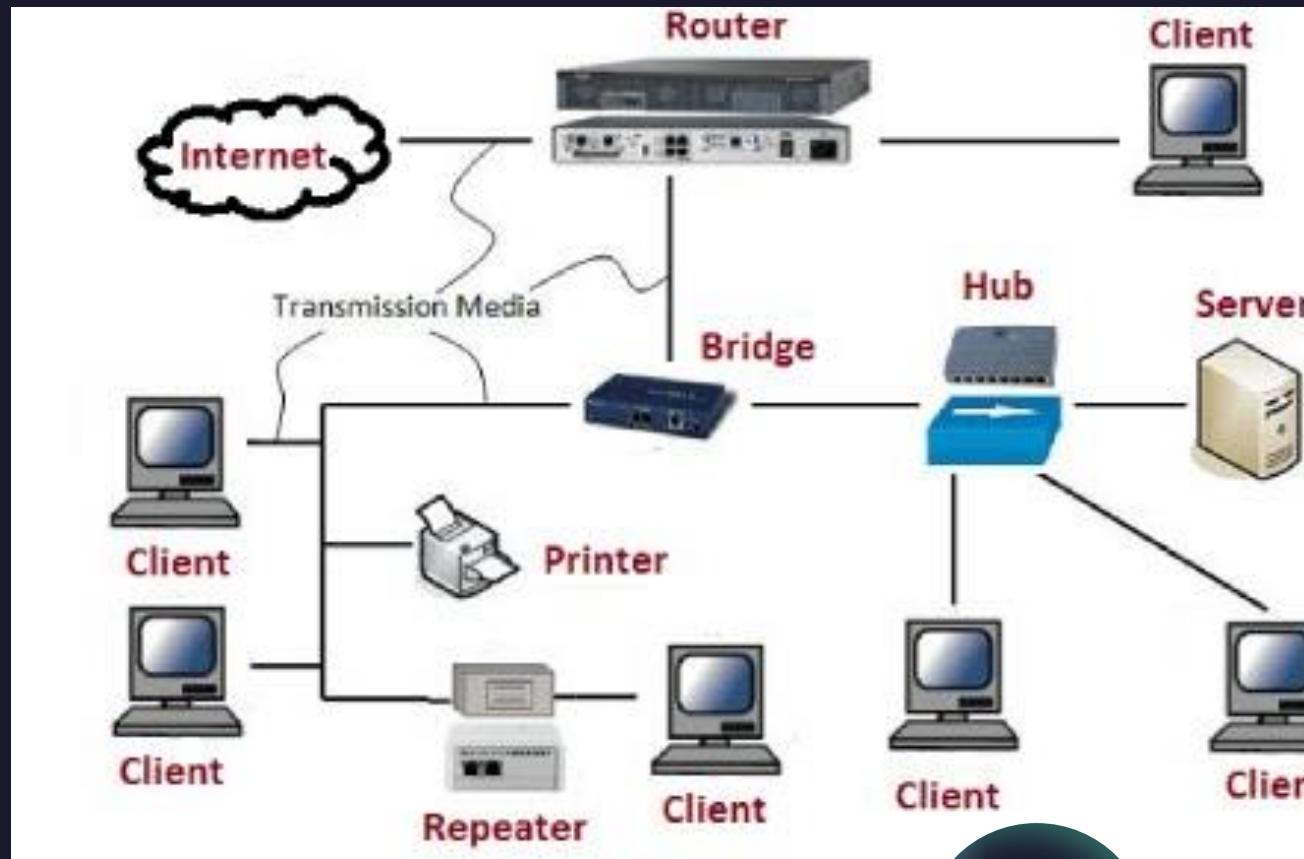
Layer 2 Attacks and Their Mitigation && Demo

- İsmet Arslan
- Cyber Securtiy Researcher
- President at KMU Cyber Security Community
- Mail : arslanismet@protonmail.com
- Linkedin : [arslanismet](https://www.linkedin.com/in/arslanismet/)

\$ls

- 1. Bilgisayar Ağı Nedir ?
- 2. OSI Nedir ?
- 3. Layer 2
- 4. Neden Layer 2 ?
- 5. Layer 2 Atakları
- 6. Alınabilecek Önlemler
- 7. Demo

1. Bilgisayar Ağrı Nedir ?



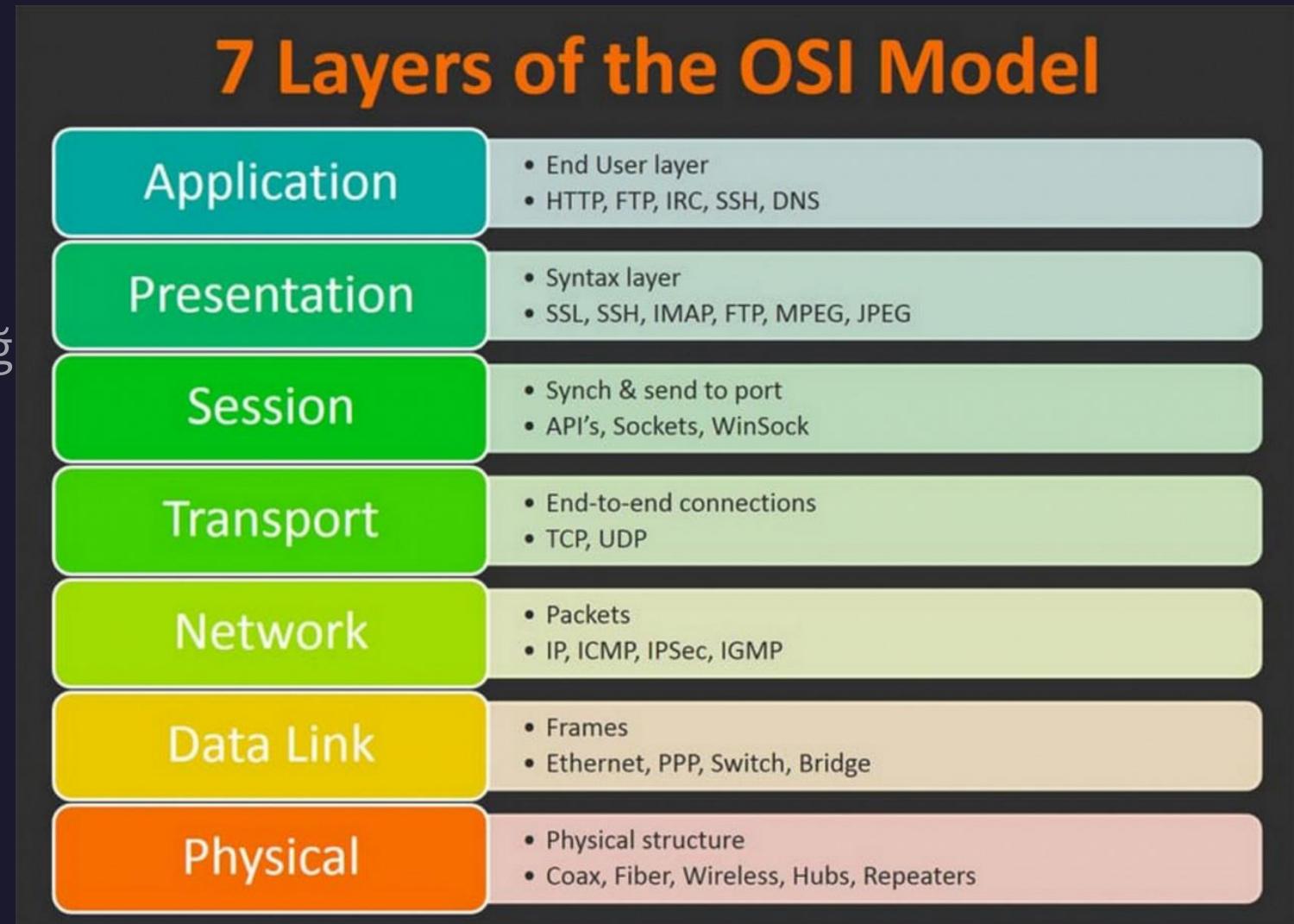
- Ağ en temelde iki veya daha fazla bilgisayarın birbirleriyle haberleştiği yapılara verilen isimdir.

2. OSI Referans Modeli Nedir ?

- TCP/IP protokol kümesi duyurulana ve tüm dünya üzerinde bir standart olarak kabul görmeden önce ağ kartı üreten firmalar ürünlerini kendi standartlarına göre üretiyordu. Bu durum ortak biçimde kullanılabilen ağ yapılarının ortayamasına büyük bir engel teşkil ediyordu. Ayrıca geliştiriciler için de durum karmaşık bir hal almış durumdaydı. Birden fazla protokol kümesi olduğu için her firma kendi kullandığı yapıda geliştirmeler yapıyordu. Bu karmaşıklığın giderilmesi için 1978 yılında ISO (International Standard Organization) tarafından OSI referans modeli duyurulmuştur.

2. OSI Referans Modeli Nedir ?

- Bu süreç kadar geliştirilmiş olan standartlardan farklı olarak, OSI ağ yapısına ve donanıma bağlı kalmadan bir modelleme sistemi ortaya koymuştur.
- Hatta günümüzde kullanılan "internet 7 katmanlı" gibi cümlelerin kaynağı da bu modeldir.



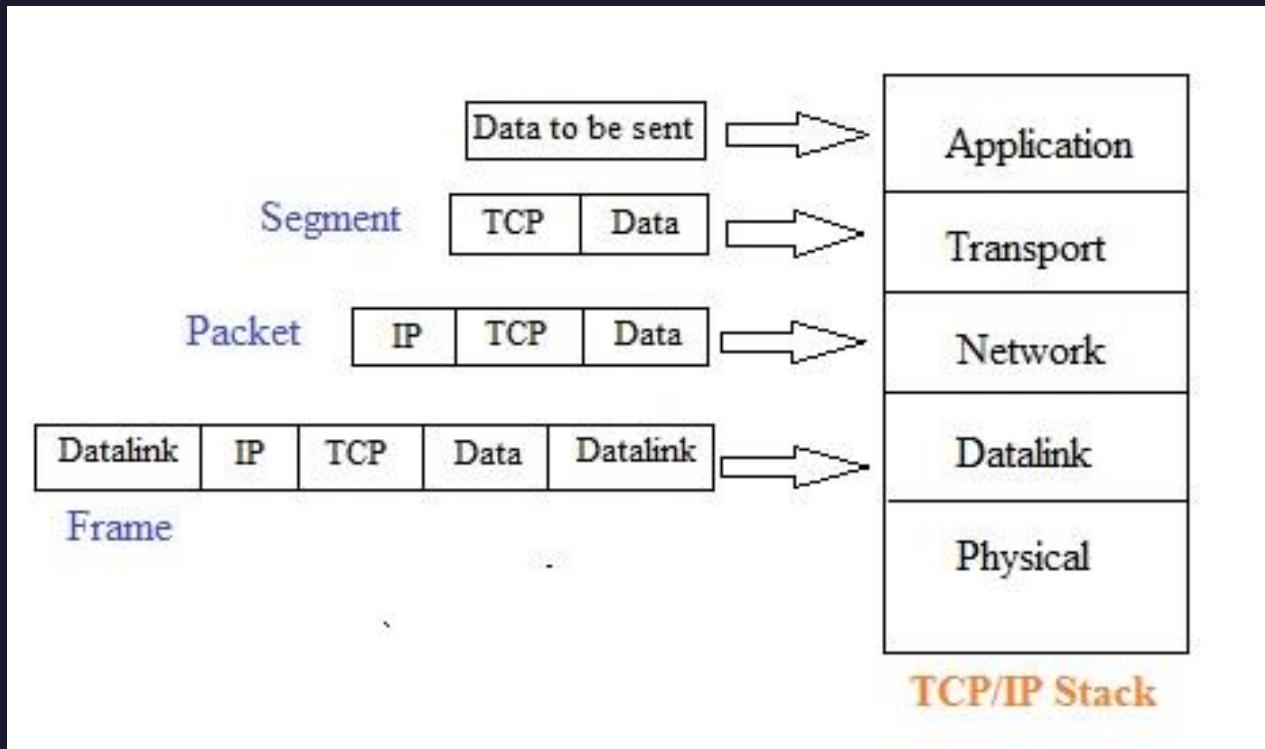
3. Layer 2

Layer 2

OSI modelinin Data-Link ya da 2. katmanı olarak isimlendirilen katmanda ;

Veri paketlerinin encapsulation işlemine tabii tutulması ,
Frame Senkronizasyonu ,
MAC adresleme ,
LLC ile hata ve akış denetimi sağlama ,
Pakcet switching veya LAN switching ,
VLAN (Virtual Local Area – Sanal Yerel Ağ Alanı)





4. Neden
Layer 2 ?



Neden Layer 2 ?



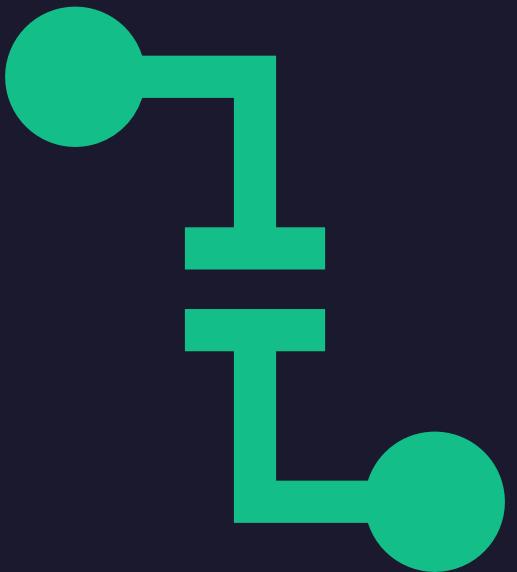
- Günümüzde NG (Next-Generation) Firewall gibi ürünler ile birçok güvenlik zafiyetinizi kontrol edebilir ve önlemlerimizi içeren dışarıya ya da dışarıdan içeriye akan trafik içerisinde alabilmek mümkün hale gelmiştir.
- Firewall cihazının genel olarak yaptığı şey ana internet çıkışları ile iç ağ arasında konumlanarak, ağ trafiğinin denetimini ve kontrolünü sağlamaktır. (Network Management cihazı olarak düşünülebilir)

Peki firewall ardında kalan alan ?



- Çoğu kurum ve kuruluşun saldırılarının yalnızca dışarıdan gelebileceği gibi yanlış bir düşüncesi var. FBI'nın 2004 yılında yaptığı bilgisayar suçları ve güvenlik anketine göre memnun olmayan çalışanlar tarafından içерiden saldırı yapılabilmeye ihtimali %56 olarak belirlenmiştir.
-
- Geçtiğimiz haftalarda Ubiquiti firmasının içерiden saldırıya uğramış olması en yakınlardaki örneklerden birisidir
- Bununla birlikte yerel ağa sızan bir saldırganın pivoting yöntemiyle diğer cihazlara geçiş yapması veya ele geçirdiği cihaz üzerinden MITM gibi LAN saldırılarında bulunması göz ardı edilebilecek tehlikeler değildir.

Yaklaşım ?



- Günümüz teknolojisine baktığımızda, sahada kullanılan Layer 2 switch lere artık Layer 3 yeteneklerinin de eklendiğini gözlemliyoruz.
- Öncelikle ağ mimarinizin ve konumlandırılan switcherin konfigürasyonunun doğru biçimde yapılması önem arz ediyor.
- Güvenlik uygulamalarını sağlamadan önce mutlak bir erişim yapısına sahip olmanız gerekmektedir.
- VLAN lar arası trafiğiniz ya da ZONE lar arası erişimleriniz ve içерiden dışarıya giden client-sunucu trafiğinizde herhangi bir sorun var mı?
- Varsa öncelik bu sorunların çözümü olmalıdır.

5. Layer 2 Atakları



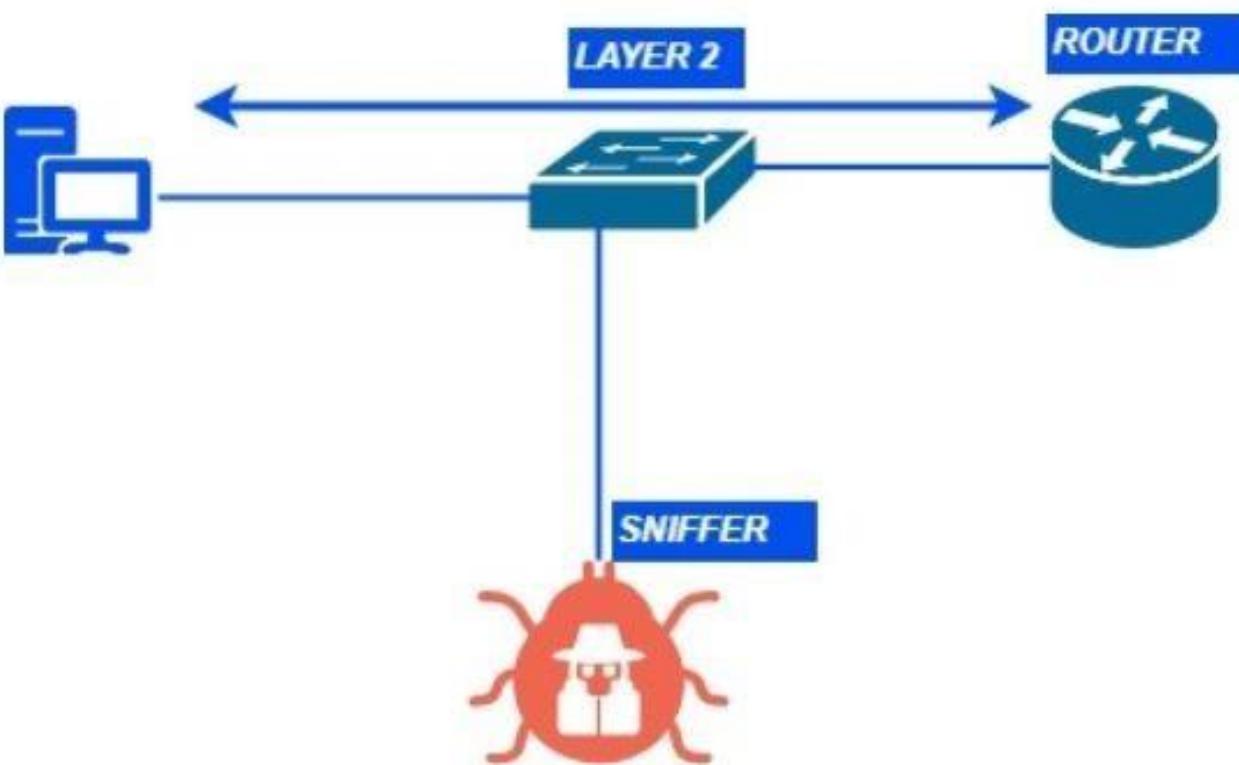


1- ARP
Spoofing/ARP
Poisoning

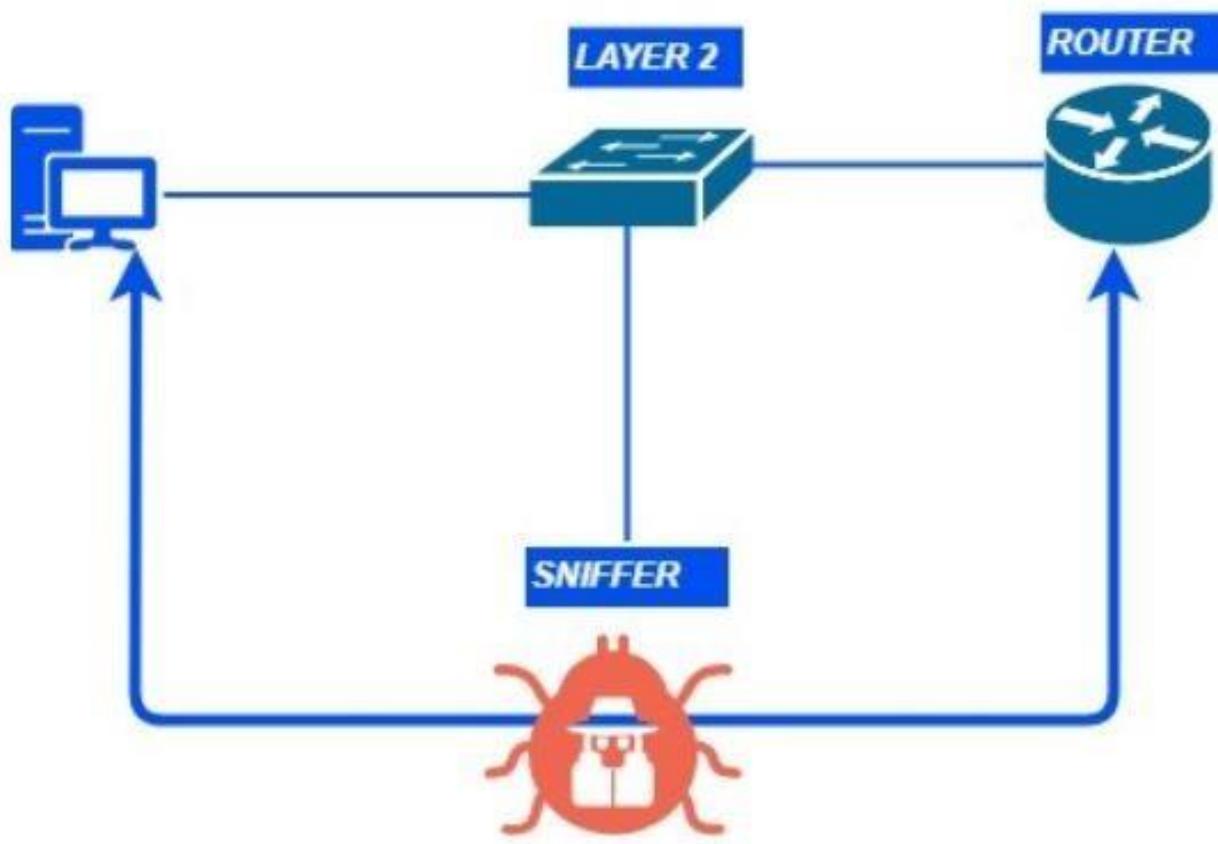
ARP Spoofing / ARP Poisoning

- ARP local ağda bir MAC adresine karşı bir IP adresinin atanmasını takip eden ve eşlestiren protokoldür. Çalışma prensibi kısaca özetlersek; switche bağlı bir PC başka bir PC ye bir paket göndereceği zaman bilgisayarın MAC adresini öğrenmek için switch bir ARP Request Packet (istek paketi) gönderir. Buna karşın sadece paketin gönderileceği hedef makine bu ARP isteğine cevap vermektedir. Paketi gönderen PC ise IP-MAC tablosunda bu eşleşmeyi tutmaktadır.
- Sahte ARP ataklarında ise saldırıcı, paketin gönderileceği yerin cevap vermesini bekleyen kendisini cevap veren olarak göstererek, paket trafiğini kendi üzerine alabilmektedir. Bu kısımda gönderen PC nin IP-MAC tablosunda da saldırıcının PC sine ait IP-MAC bilgileri yer alacaktır. ORNEK-1 ve ORNEK-2 de bu işlemin kısa bir topolojisini sizler için tanımladım. ORNEK-1 de trafik normal devam ederken ORNEK-2 de saldırıcı atağını gerçekleştirerek içereniden dışarıya giden ve dışarıdan içeriye gelen trafiği tamamen kendi üzerine alarak trafiğin analizini sağlamaktadır.





ORNEK-1



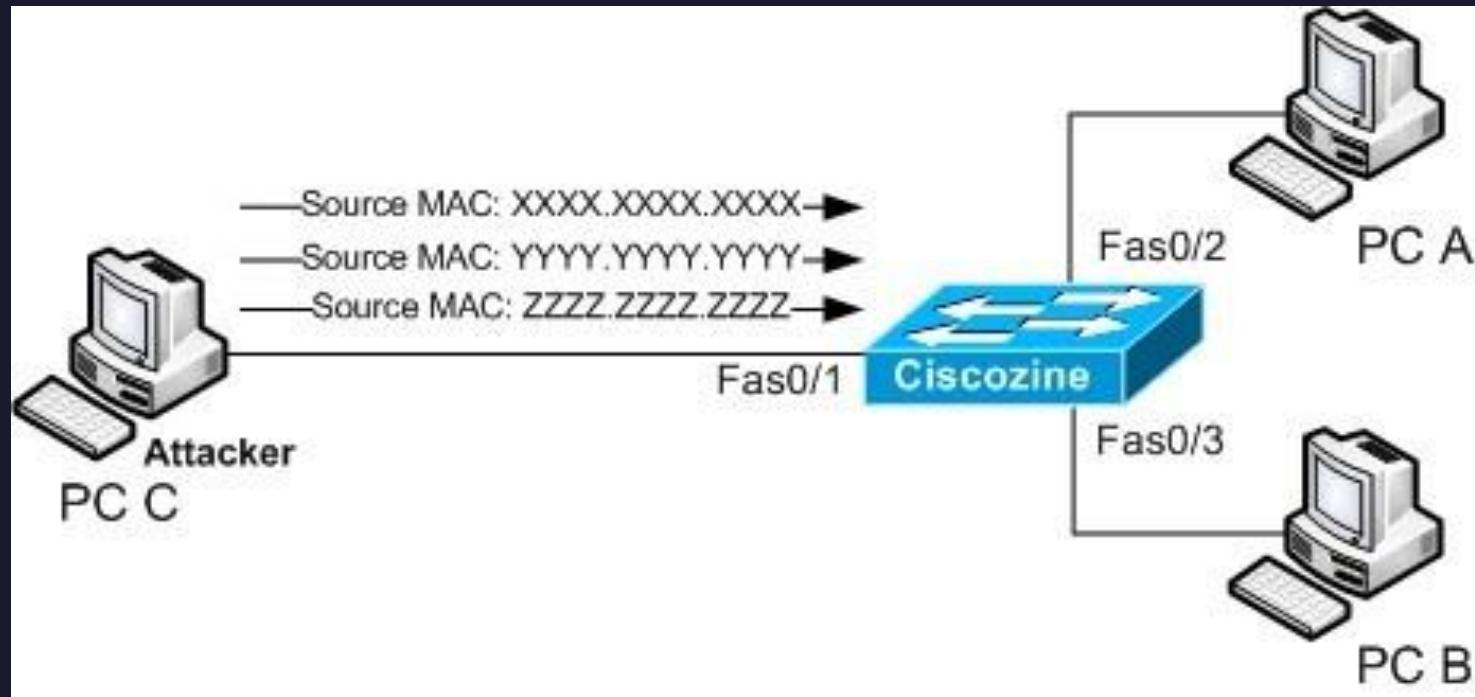
ORNEK-2



2- MAC Flooding

2- MAC Flooding

- Saldırgan bu saldırı tipinde karşısında yer alan switch e binlerce MAC adresi gönderir ve switch'in MAC tablosunu doldurarak switch I hub durumuna getirebilir. Böylelikle ağı aktif olarak dinleme pozisyonuna geçebilir. Bu noktada clear-text olarak içerde yaptığınız haberleşmelerdeki detayların tamamını gözlemleyebilir.



ORNEK-3

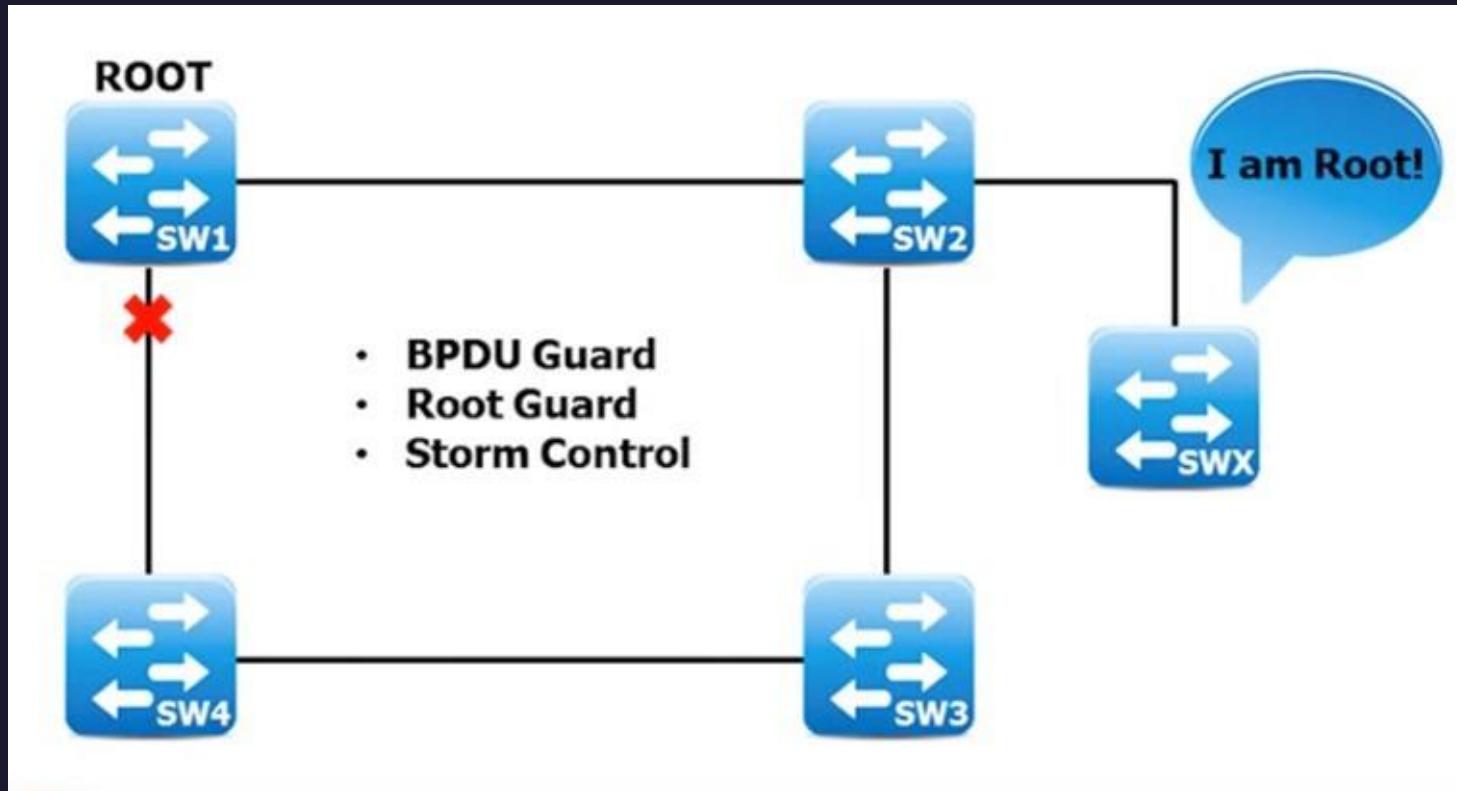
A black and white aerial photograph showing a large agricultural area. The land is divided into numerous circular plots, likely created by center pivot irrigation systems. The fields appear to be in various stages of cultivation, with some showing dark, tilled soil and others appearing more yellowish or green. The overall pattern is a dense grid of circles.

3- STP
Atakları

3- STP Atakları

Genel anlamda switch üzerinde oluşabilecek döngülerin önüne geçilmesi amacıyla kullanılan protokoldür. Saldırganlar switch üzerinde “portfast” modunda olan portları kullanarak döngüler oluşturup ağ içerisinde paket iletimini olumsuz etkileyerek ve hizmetlerin çalışmasını etkileyerek saldırıarda bulunabilmektedir. Saldırgan kendisini switch gibi göstererek “**root bridge**” bilgisini değiştirmeye çalışabilir.

BPDU switchler arası haberleşme sağlayan pakettir. Kullanıcı networküne bağlı porttan gelmemesi gerekmektedir. Bu yüzden kullanıcı networküne/ağına ait porta gereken bpduguard önlemini almanız gerekmektedir.



ORNEK-4



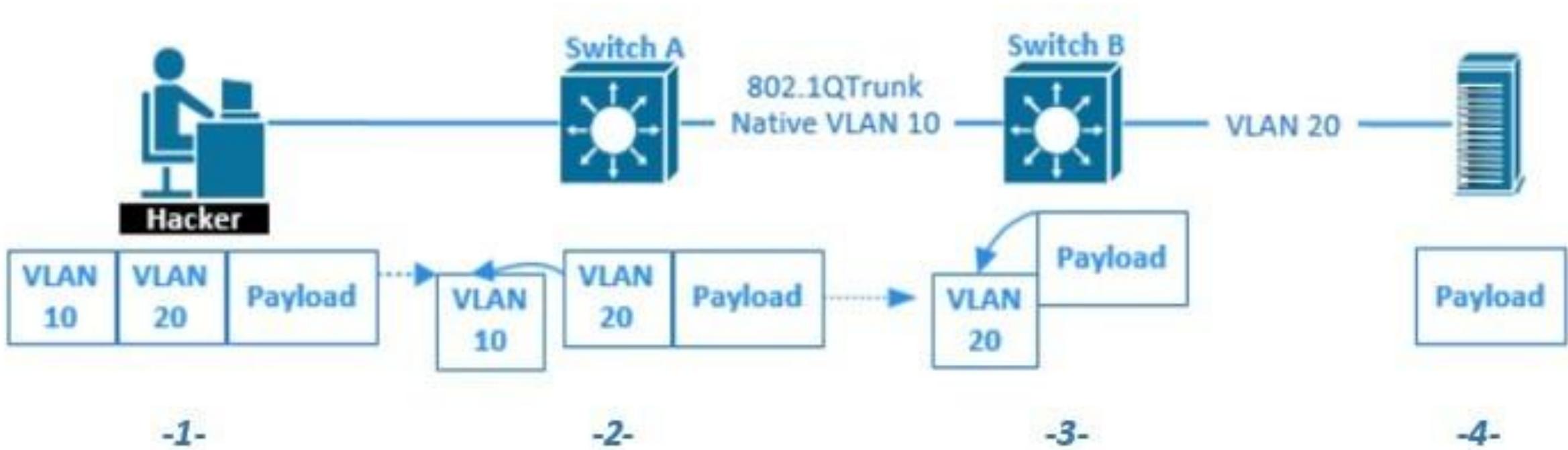
4- VLAN Hopping

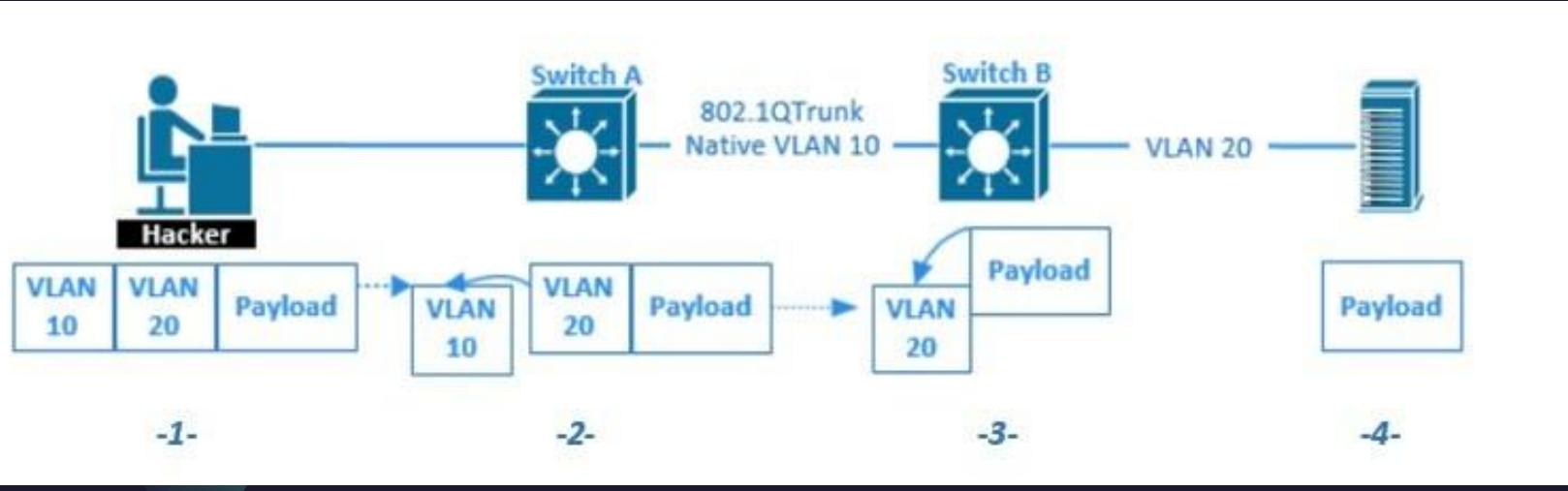
4-VLAN Hooping:

Saldırganın bulunduğu bir VLAN dan diğer VLAN lara ulaşmasını Sağlayan atak tipidir. İki çeşit byline VLAN Hopping atağı vardır:

- a. Double Tagging: Bu atakta, paketin istenen VLANe erişebilmesi için porta giren çerçevelere (frame) iki adet IEEE 802.1q başlığı (header) eklenir. Çerçeveyi ilk alan anahtar birinci başlığı (header) çıkarır. Çerçeveyi alan ikinci anahtar, çerçeve içerisindeki ikinci başlığının VLAN bilgisi okuyarak paketi, gitmesini istediği hedef VLANe gönderir.

ORNEK-5





- 1.Adım: Saldırgan Access iletişiminde yer alan porta double tag içeren bir paket göndermektedir.
- 2.Adım: Switch paketi aldıktan sonra Trunk portuna iletir. İlk tag Native VLAN ile aynı olduğundan paketten çıkarılır.
- 3.Adım: Switch B tarafından ikinci etiketli/Tag li paket alınır. Kaynak VLAN 20 olarak tanımlanır.
- 4.Adım: Paketin orijinali VLAN 10 dan VLAN 20 ye gönderilmiş oldu.

4-VLAN Hopping:

- b. Switch Spoofing: Saldırgan kendisine switch davranışını atamaktadır ve saldırısı yapacağı VLAN'ı etkileyebilmek için kendisi switch gibi gösteren bir port a sahiptir. Saldırganın kendisini bu port ile switch gibi gösterebilmesi ile tüm VLAN'lara üye olmasını erişimini sağlamaktadır.

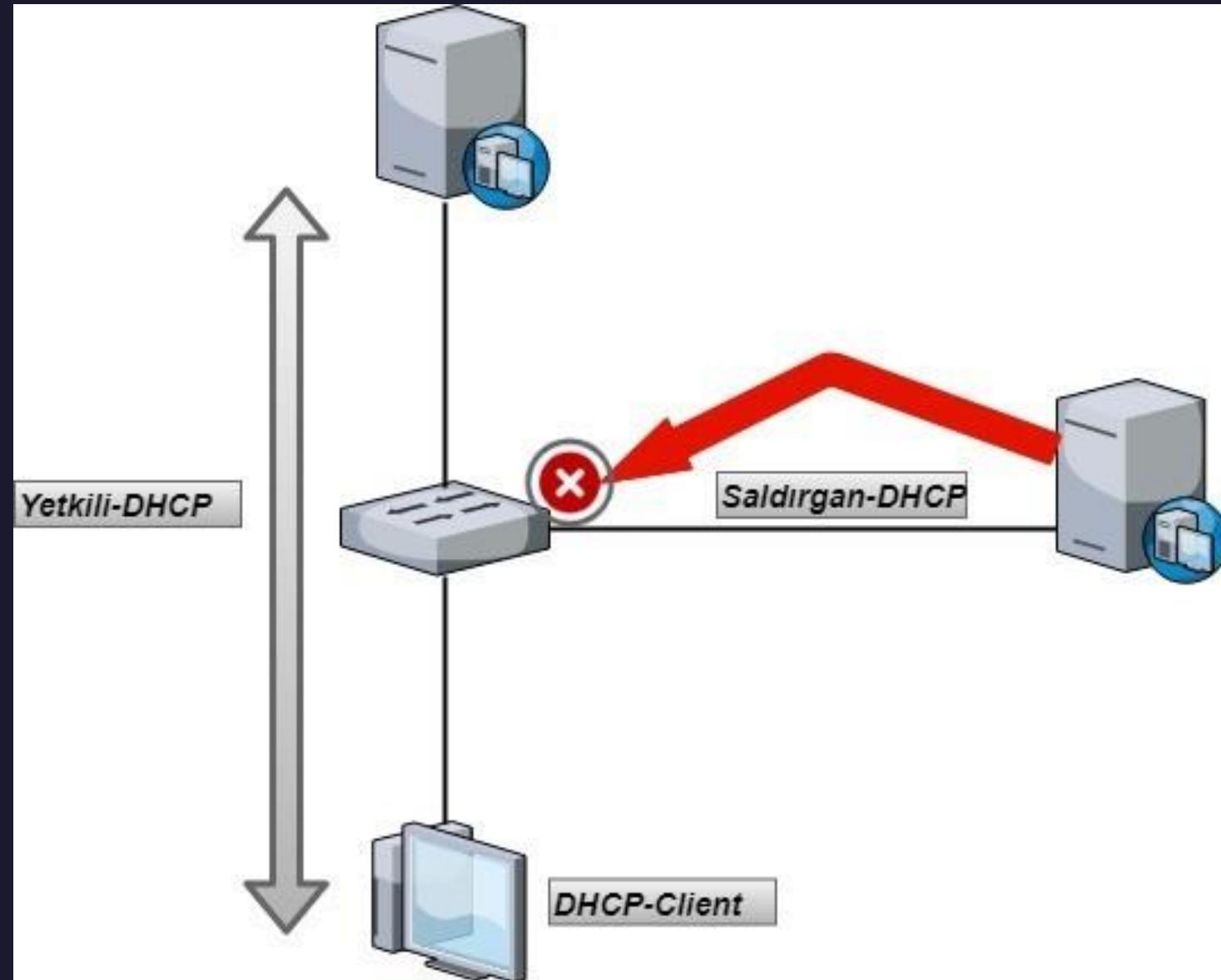


5- DHCP Snooping/Rogue

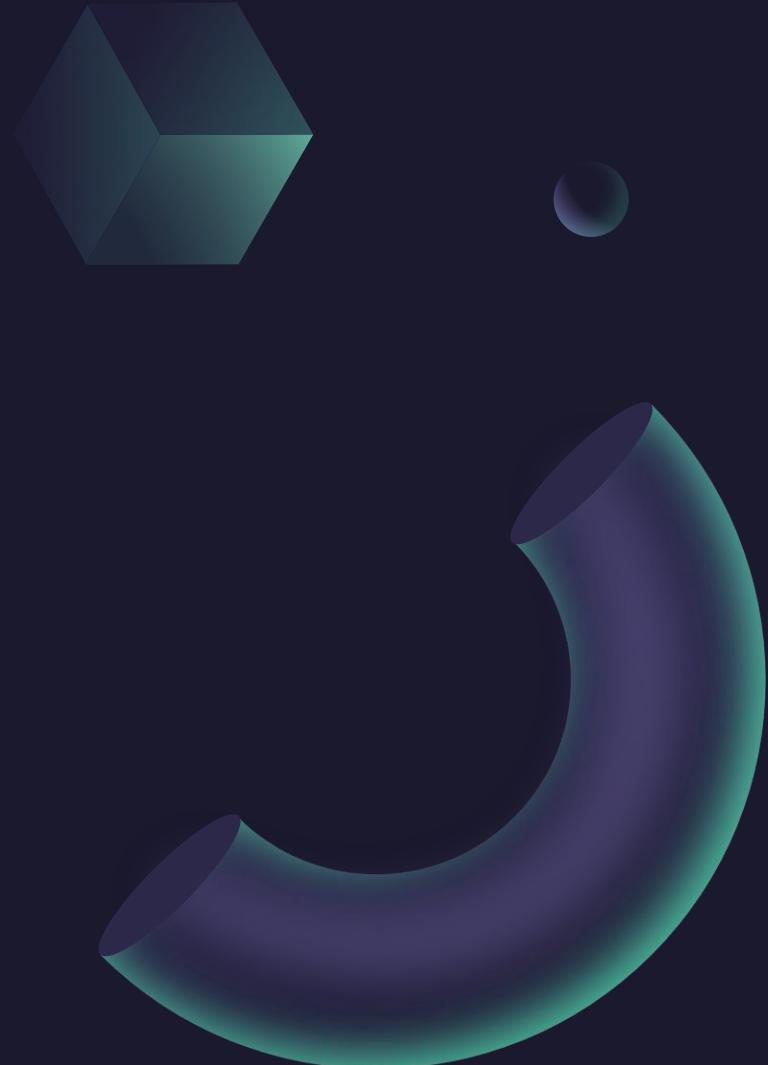


5- DHCP Snooping/Rogue:

- Saldırgan kendisini DHCP server olarak göstererek switch üzerindeki IP MAC tablosunda ki gateway eşleşmesinin güncellenmesini sağlar. Ağa bağlanan cihazlara DHCP offer paketi ile yanıt sağlayarak kullanıcının ağ bilgileri içerisindeki gateway adresini kendi adresi olarak güncellettirebilmektedir. Kullancı saldırmanın gönderdiği bilgileri onaylayıp DHCP request paketi gönderir ve sonrasında saldırında ACK bilgisini kullanıcıya göndererek işlemlerini tamamlar. Kullanıcının gateway i artık saldırın olur.



ORNEK-6

A dark blue background featuring abstract 3D-rendered geometric shapes. In the upper left, there's a dark teal hexagonal prism. Below it, a large, translucent purple cylinder curves from the bottom left towards the center. A small, semi-transparent teal sphere is positioned above the cylinder. The overall aesthetic is minimalist and modern.

6- DHCP Starvation

6- DHCP Starvation:

- Switch e bağlı olan saldırıcı switch üzerinden gateway e sürekli olarak DHCP discover paketi gönderebilir ve bir süre sonrasında ise gateway in DHCP havuzu dolarak cevap veremez hale gelebilmektedir. Farklı sahte MAC adreslerinden bu istekler gönderilmektedir. Bu işlem sonrası cevap veremeyen DHCP sunucu yerine saldırıcı kendi oluşturduğu DHCP sunucusunu entegre ederse işlem tamamlanır. Genel de çok basit uygulamalarla bunu profesyonel olmayan kişilerde sağlayabilir.

7- CPU Atakları



7- CPU Atakları:

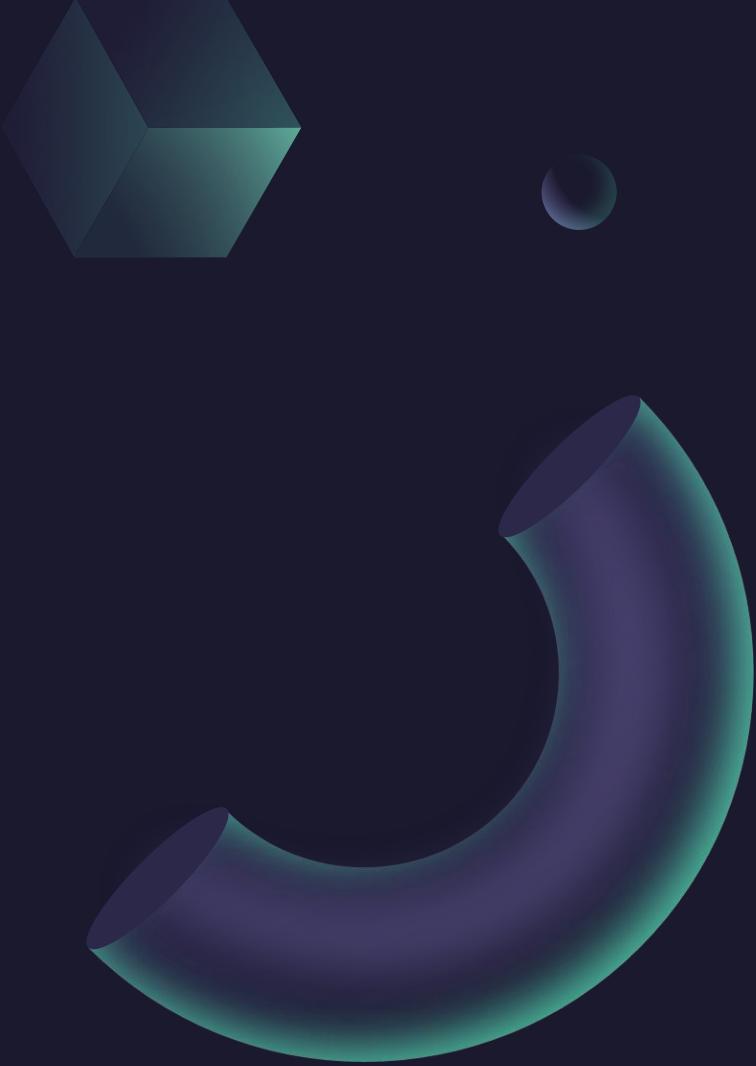
- Switch CPUları üreticiler tarafından yüksek miktarda gelen paket trafigini sorunsuz işlemek için tasarlanmaktadır. Ancak, saldırganlar bu durumu gözönüne alarak yüksek miktarda paket trafigi üretecek switch üzerine atak yapabilirler ki böyle durumlarda switch anlık servis kesintileri yaşayabilir hatta gelen paket trafigini işleyemez hale gelerek üzerinde bağlı kullanıcılarla erişim sorunu yaşatabilmektedir. ARP, DHCP veya OSPF ve benzeri protokollerin yarattığı ve kullandığı paketler bu saldırınlarda kullanılmaktadır.

The image shows a collection of brown cardboard boxes of different sizes and orientations. Some boxes are stacked, while others are placed individually. They are set against a solid brown background. The lighting creates soft shadows, emphasizing the three-dimensional nature of the boxes.

8- Diğer
Paket Bazlı
Ataklar

8- Diğer Paket Bazlı Ataklar

IP Flood Atakları,
IGMP Atakları,
LAND Atakları, (Local Area Network Denial)
SMURF Atakları,
TCP Flag Atakları,
Excess-Fragmanted Atakları,
Excess-Offset Atakları,
Repeated Packet Fragment Atakları,
Tear Drop Atakları,
Syndrop Atakları,
NewTear Atakları,
Bonk Atakları,
Nesta, Rose,Fawx, Ping of Death ve Jolt Atakları,
TCP, SYN, ICMP Atakları



9- Storm Control

9- Storm Control:

- Standart çalışma düzenine sahip bir ağda beklenmedik bir şekilde broadcast, multicast ve unicast trafiginin artması ile cihazın artık isteklere karşı cevap veremeyecek kadar sistemsel durmasına neden olan saldırısı tipidir. Aslında denial-of-service (DOS) atak ile benzer bir atak tipidir. Switch Loopları, Sunucu-DHCP ya da farklı bir switch cihazının ağa bağlanması vb gibi durumlarda meydana gelen saldırılardır.

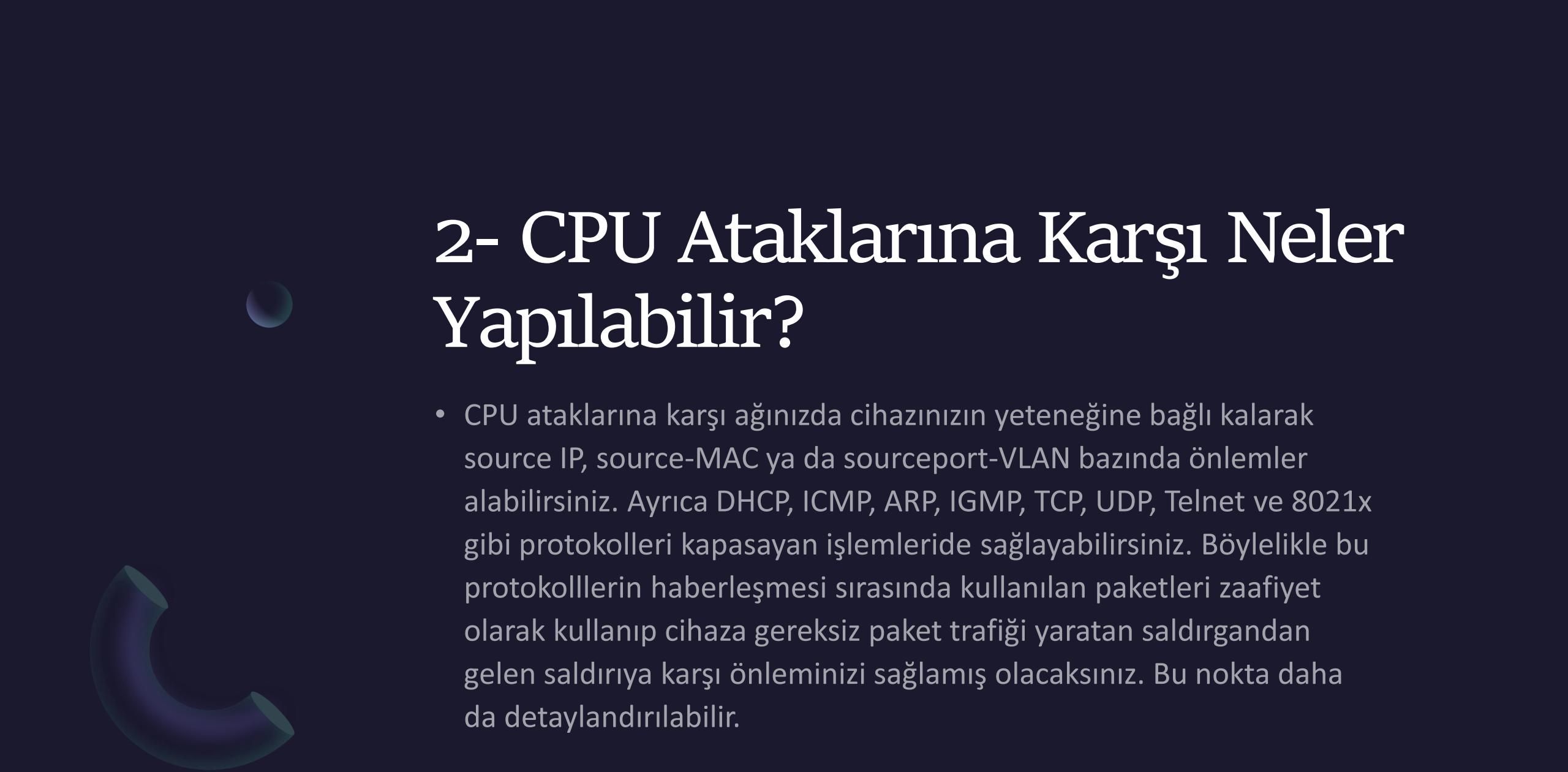
6.Mitigation



1- ACL (Access Control List- Erişim Kontro Listesi)

Rule-based (Kural-Tabanlı) çalışan bir yapıya sahip olan ACL ile kaynak-hedef arasında ki erişimleri switchiniz üzerinden tanımladığınız permit-deny(izin ver-engelle) işlemleri ile sağlanmanız mümkündür. Bilindiği üzere aynı switch üzerine bağlı olan kullanıcılar yapınızda gateway olsa dahi gateway inize çıkmadan switch üzerinden haberleşmektedir ya da VLAN yapınız varsa farklı vlanlarınızın birbir arasında erişim planınız var oalbilir. Bu noktada ACL ile hem VLAN lar arası trafiginizi hem de kullanıcı bazında kullanıcılarınız arasında ki trafigi genel anlamda yönetmeniz mümkündür. Böylelikle hem yetkisiz kullanıcı erişimlerini ya da voice network ü gibi farklı networklerinizi birbirinden bağımsız ve birbiri arasında kontrollü-akışkan bir trafik yaratabilirsiniz. Enterprise Network ler de yoğunlukla ACL yapısı işlenmekte ve tercih edilmektedir.

Bu yöntemle virus bulanın bir kullanıcını tüm network ü tehlikeye atacak bir durumda bırakmasında önleyebilirsiniz. Video-Voice gibi trafiklerin ayrıştırılması ile bir nevi netwok te yaşanacak delay lerin (gecikmelerin) de önüne geçebilirsiniz.



2- CPU Ataklarına Karşı Neler Yapılabilir?

- CPU ataklarına karşı ağınızda cihazınızın yeteneğine bağlı kalarak source IP, source-MAC ya da sourceport-VLAN bazında önlemler alabilirsiniz. Ayrıca DHCP, ICMP, ARP, IGMP, TCP, UDP, Telnet ve 8021x gibi protokoller kapasayan işlemlerde sağlayabilirsiniz. Böylelikle bu protokollerin haberleşmesi sırasında kullanılan paketleri zaafiyet olarak kullanıp cihaza gereksiz paket trafigi yaratan saldırından gelen saldırıya karşı önleminizi sağlamış olacaksınız. Bu nokta daha da detaylandırılabilir.

3- MFF (MAC Forced-Forwarding/Zorla Yönlendirme)

- Bu yapı ile switchinizde Layer 2 seviyesinde kullanıcılarınızı birbirinden izole edebilirsiniz. Layer 2 de meydana gelebilecek zararlı atakların önüne geçmenize fayda sağlamaktadır. MFF ARP paketlerinin tamamını gateway e yönlendirerek aslında trafigin LAYER 3 te dönmesini zorlamaktadır. Bu işlem ile servis kalitenizi ve ağ güvenlik düzeyinizi artırmaktasınız.

4- Storm Control Defense

- Switch Interface leriniz altında alt eşik değeri veya üst eşik değeri vererek gereksiz broadcast, multi-cast ve unicast trafiklerinin önüne geçmeniz mümkün olacaktır.

5- DAI (Dynamic ARP Inspection)

- MITM (Man-in-the-middle-attack) ataklarına karşı koyabilmek için mutlaka aktif edilmelidir.

6- ARP Protokolü ile Diğer Ataklara Karşı Önlemler Nelerdir?

(Opsiyonel-Cihaz Kabiliyetine Dayalı Eklemenizde Fayda Olacaktır.)

- a. ARP Paket Limitleme,**
 - b. ARP Miss Message Limitleme,**
 - c. ARP Replay Optimizasyonunun Sağlanması,**
 - d. Strict ARP Learning**
 - e. ARP Entrying Limitleme,**
 - f. ARP Gateway Anti-Collision,**
 - g. Gratuitous ARP Packet Sending-Sahte ARP Paketi Gönderimini Engeleme,**
 - h. ARP Flood Atak Limitlerinin Belirlenmesi,**
-

7- Port Security

- Layer 2 düzeyinde bir interface altında MAC bazlı erişim denetimini sağlayabildiğimiz yapıdır. İsterseniz bir port u tek bir MAC adresine rezerve de etme imkanını size sunmaktadır. Dinamik olarak büyük networklerde tek tek MAC adresi girmemeniz içinde ayrıca size bir kolaylık sağlamaktadır(Sticky). Port Security “violation” komutu ile size 3 farklı işlem-davranış seçeneği sunmaktadır. Bunlar “protect, restrict ve shutdown” dur. Kısaca bahsetmemizde fayda olacaktır.

7- Port Security

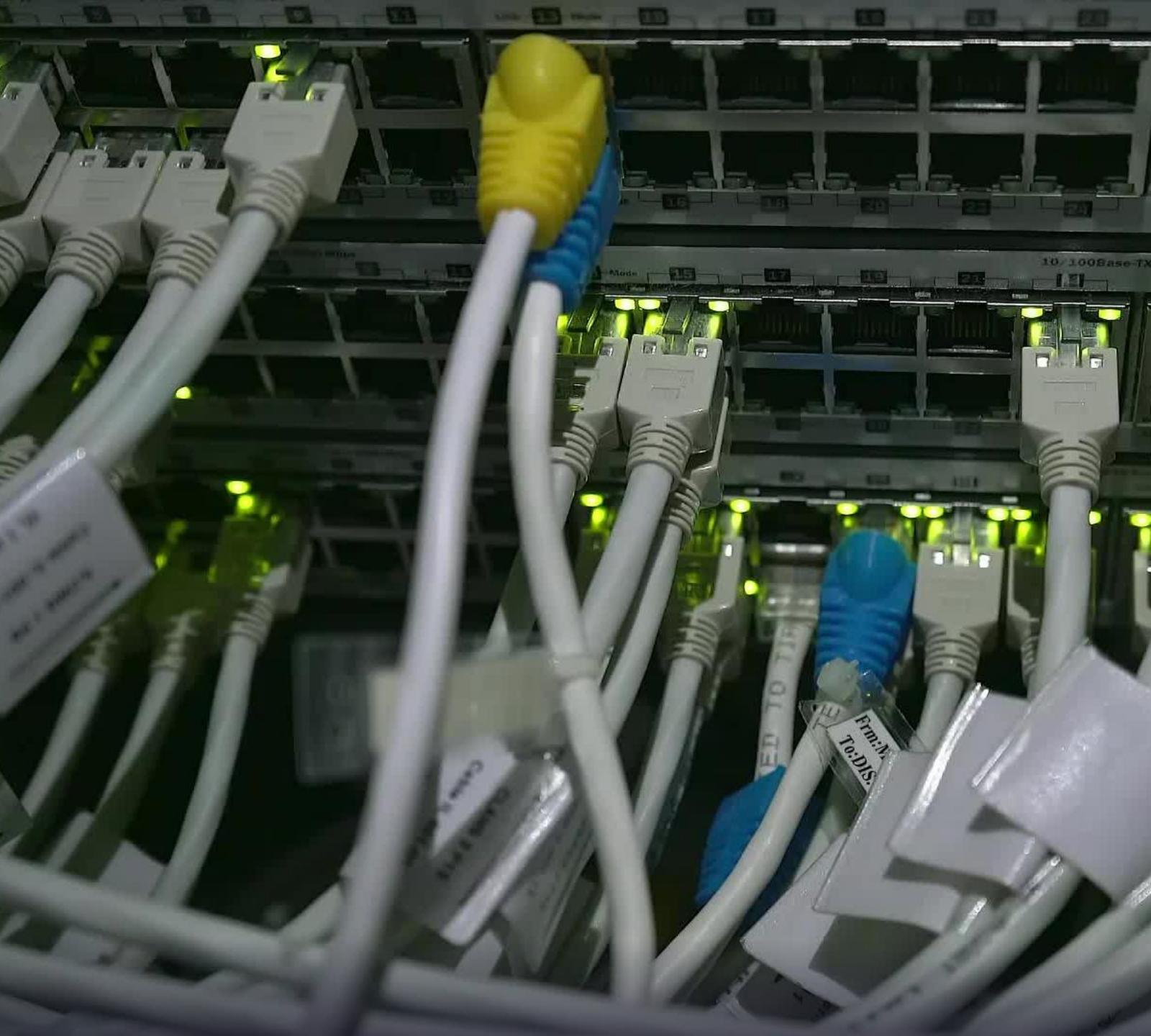
Protect: porta gelen bağlantı isteğinin iptal edilmesini ve bağlantıyı engellemesini sağlıyor,

Restrict: protect komutu ile aynı işlemi yapıyor ve bu işlemin loglarının tutulmasını sağlıyor,

Shutdown: Port'un kapatılması durumudur. Belirlediğiniz kısıtlar dışında bir durum olduğunda portu tamamen kapatır. Çok tercih edilebilir bir yapı değildir. Erişimin tamamen kesilmesinden dolayı.

8- DHCP Snooping

Saldırgan switch üzerinde bağlı olan kullanıcılarla kendisi DHCP server/gateway olarak göstermeye ve trafiği kendi üzerine almaktadır. Bundan dolayı mutlaka ağ içerisinde önlemimizi almamız gerekmektedir.





9- IPSG (IP Source-Guard)

- Layer 2 de IP paketlerini kontrol eder. Kontrolü sağlarken switch binding tablosunu kullanır. Saldırgan ağ da yer alan bir kullanıcının izinli olan IP sini kendisi kullanarak gateway e ve erişebilir diğer VLAN lara geçiş yapmayı deneyebilir. Bu yüzden switch te aktif edilmesi önem arz etmektedir. IPSG I interface lerinizde yada VLAN interface leriniz içerisinde uygulamanız gerekmektedir.

NOT: PSG, Static ARP ve ARP Spoofing Ataklarına karşı koruma sağlamaz. Bu noktayı detaylarını inceleyerek yorumlamamanızda fayda olacaktır.

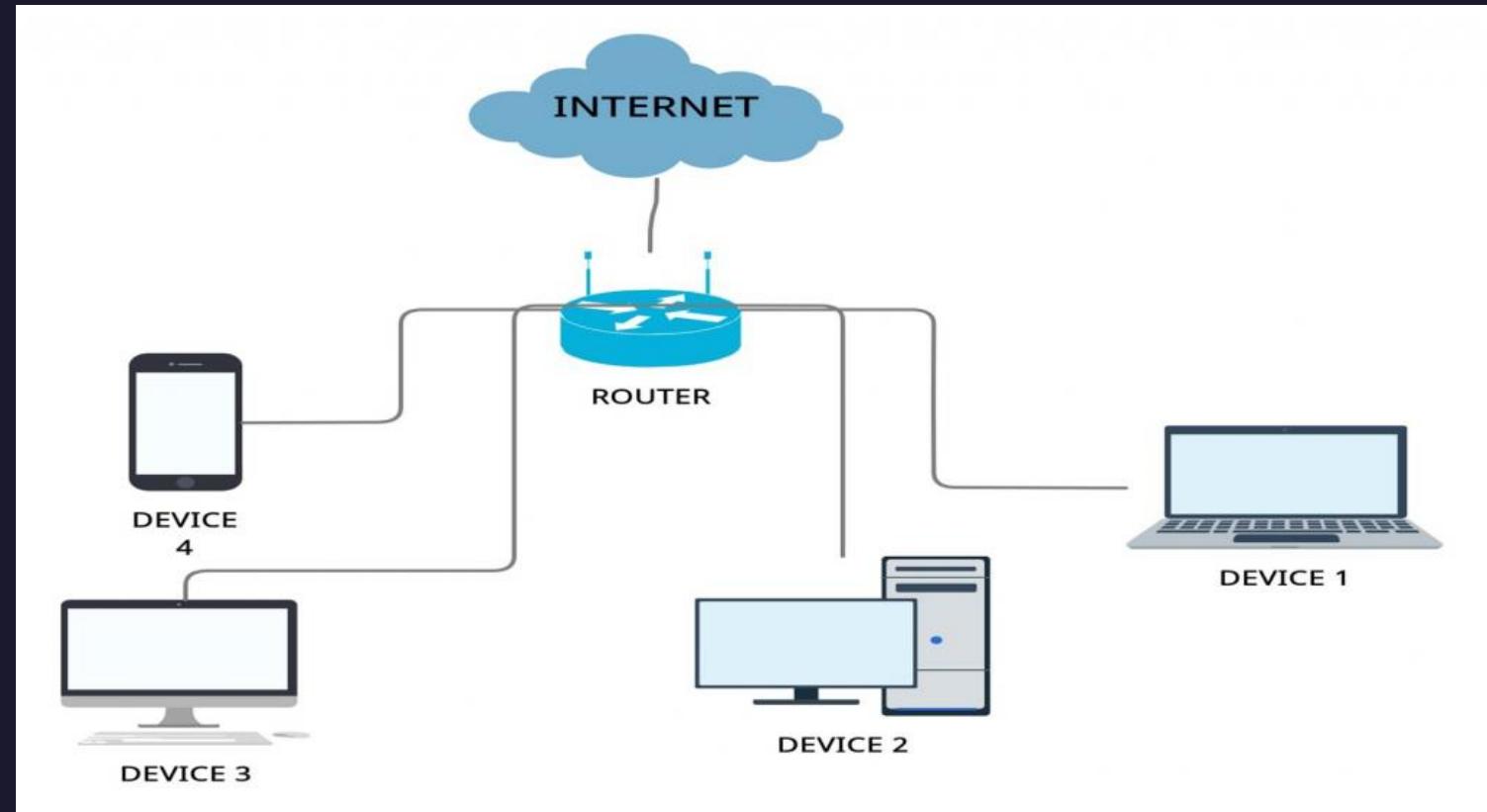
7. Demo



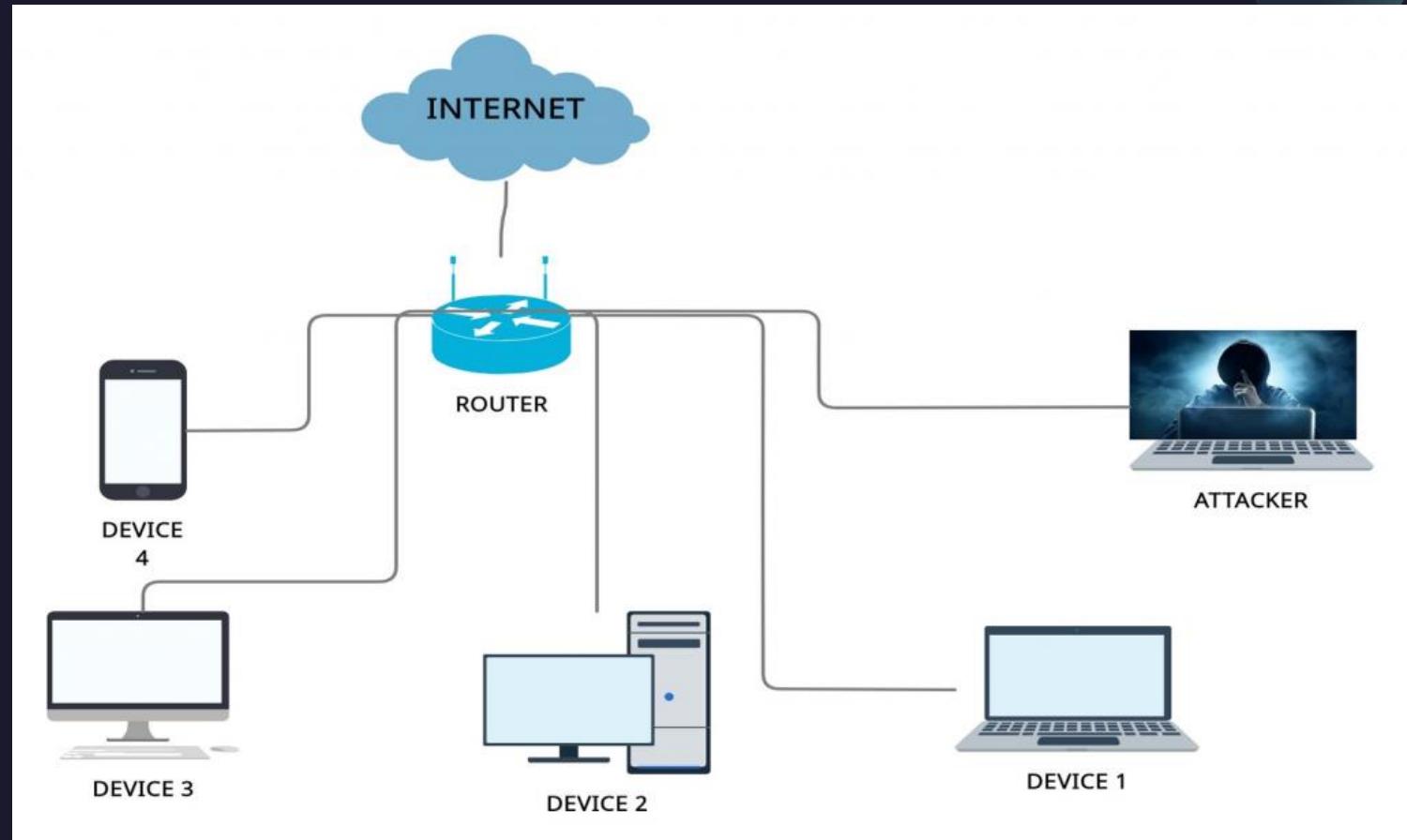
ARP Spoofing / ARP Poisoning

- ARP (Address Resolution Protocol) protokolü MAC adreslerinin çözümlenmesini sağlar. Yani IP adreslerini MAC adreslerine çevirir. Bu çevirme işlemini yapabilmek için MAC adreslerini ve IP adreslerini cahce denilen bir tabloda tutar. ARP protokolü OSI modelinin 2. katmanında (Data-Link) çalışır.
- ARP Spoofing (ARP Kandırmacası)/ARP Poisoning(ARP Zehirlenmesi) ise ARP paketlerinin kullanılarak yerel ağa bağlı olan cihazların gönderdiği paketlerin bu cihazların kandırılmasına ve kandırılmış cihazların ağ trafiğini izlenmesine ve manipüle edilmesine imkan veren saldırıdır.

- Şekildeki LAN'a bir saldırganın dahil olduğunu varsayıyalım.



- Saldırgan router'a "ben device 1'im" diye broadcast paketleri gönderir. Router ARP tablosunu belirli aralıklarla bu gelen mesajlara göre düzenlediği için bir süre sonra device 1 olarak artık saldırılan cihaz tutulmaya başlar.



Kaynakça

- [layer 2 atakları](#)
- <https://www.cemerbas.com/2019/06/23/katman-layer-2/>
- <https://fatihturgutegitim.medium.com/layer2-sald%C4%B1r%C4%B1-t%C3%BCrleri-69748387ab53>
- <https://www.siberguvenlik.web.tr/index.php/2020/02/06/ikinci-katman-layer2-ataklari-ve-onlenmesi/>
- https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/L2-security-Bootcamp-final.pdf





TEŞEKKÜRLER