İKTİSADİ, İDARİ VE SOSYAL BİLİMLER FAKÜLTESİ

YÖNETİM BİLİŞİM SİSTEMLERİ

DÖNEM PROJESİ

İKİNCİ KATMAN SALDIRILARI VE GÜVENLİK ÇÖZÜMLERİ

HAZIRLAYAN

Hüseyin PALA

DANIŞMAN ÖĞRETİM ÜYESİ

Doç. Dr. Recep BENZER

2026

ETİK İLKELERE UYGUNLUK BEYANI

Dönem proje yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Adı Soyadı

Hüseyin Pala

İKİNCİ KATMAN SALDIRILARI VE GÜVENLİK ÇÖZÜMLERİ

Hüseyin PALA

ANKARA MEDİPOL ÜNİVERSİTESİ

YÖNETİM BİLİŞİM SİSTEMLERİ

2026

ÖZET

Bu çalışma, OSI referans modelinin ikinci katmanında (Layer 2 / veri bağlantı katmanı) gerçekleştirilen başlıca saldırı türlerini ve bu saldırılara karşı Cisco platformunda geliştirilen güvenlik çözümlerini kapsamlı biçimde incelemektedir. Çalışma kapsamında MAC Flooding, DHCP Starvation/Spoofing, ARP Spoofing, VLAN Hopping, STP Manipülasyonu, VTP saldırısı, CDP/LLDP keşif saldırısı, IPv6 Komşu Keşfi (NDP) sahteciliği, 802.1X/MAC Authentication Bypass atlatma girişimleri ve yayın (broadcast) fırtınası saldırıları olmak üzere dokuz farklı Layer 2 tehdit vektörü; çalışma mekanizmaları, ağ üzerindeki etkileri ve önleme yöntemleri bakımından ele alınmıştır. GNS3 ve Cisco Packet Tracer simülasyon ortamlarında gerçekleştirilen uygulamalı senaryolarla; Port Security, DHCP Snooping, Dynamic ARP Inspection, BPDU Guard/Root Guard, VTP Password/Transparent Mode, CDP/LLDP devre dışı bırakma, RA Guard ve Storm Control gibi Cisco IOS güvenlik mekanizmalarının etkinliği gösterilmiştir. Bulgular, veri bağlantı katmanı güvenliğinin bütünsel bir savunma derinliği (defense-in-depth) yaklaşımıyla ele alınması gerektiğini ortaya koymaktadır. Çalışma, ağ yöneticilerine ve güvenlik uzmanlarına yönelik uygulanabilir bir yapılandırma rehberi sunmayı amaçlamaktadır.

Anahtar Kelimeler: Veri Bağlantı Katmanı, Layer 2 Güvenliği, Cisco IOS, ARP Spoofing, VLAN Hopping, Ağ Güvenliği

Danışman: Doç. Dr. Recep BENZER

LAYER 2 ATTACKS AND SECURITY SOLUTIONS

Hüseyin PALA

ANKARA MEDİPOL UNIVERSITY

MANAGEMENT INFORMATION SYSTEMS

2026

ABSTRACT

This study presents a comprehensive examination of the principal attack types carried out at Layer 2 (the data link layer) of the OSI reference model, together with the security solutions developed against them on the Cisco platform. Nine distinct Layer 2 threat vectors are addressed in terms of their working mechanisms, network impact, and mitigation methods: MAC flooding, DHCP starvation/spoofing, ARP spoofing, VLAN hopping, STP manipulation, VTP attacks, CDP/LLDP reconnaissance, IPv6 Neighbor Discovery Protocol (NDP) spoofing, attempts to bypass 802.1X/MAC Authentication Bypass, and broadcast storm attacks. Through hands-on scenarios implemented in GNS3 and Cisco Packet Tracer simulation environments, the effectiveness of Cisco IOS security mechanisms such as Port Security, DHCP Snooping, Dynamic ARP Inspection, BPDU Guard/Root Guard, VTP password/transparent mode, CDP/LLDP disabling, RA Guard, and Storm Control is demonstrated. The findings indicate that data link layer security must be addressed through a holistic defense-in-depth approach. The study aims to provide network administrators and security professionals with a practical configuration guide.

Keywords: Data Link Layer, Layer 2 Security, Cisco IOS, ARP Spoofing, VLAN Hopping, Network Security

Advisor: Assoc.Prof.Dr Recep BENZER

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

SİMGELER VE KISALTMALAR

ARP – Address Resolution Protocol (Adres Çözümleme Protokolü)

BPDU – Bridge Protocol Data Unit

CAM – Content Addressable Memory

CDP – Cisco Discovery Protocol

DAI – Dynamic ARP Inspection

DHCP – Dynamic Host Configuration Protocol

DoS – Denial-of-Service (Hizmet Reddi)

DORA – Discover, Offer, Request, Acknowledge

DTP – Dynamic Trunking Protocol

GNS3 – Graphical Network Simulator-3

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IOS – Internetwork Operating System

IP – Internet Protocol

IPSec – Internet Protocol Security

LAN – Local Area Network

LLDP – Link Layer Discovery Protocol

MAB – MAC Authentication Bypass

MAC – Media Access Control

MitM – Man-in-the-Middle

NA – Neighbor Advertisement

NDP – Neighbor Discovery Protocol

NS – Neighbor Solicitation

OSI – Open Systems Interconnection

RA – Router Advertisement

RFC – Request for Comments

SNMP – Simple Network Management Protocol

SSL – Secure Sockets Layer

STP – Spanning Tree Protocol

TLS – Transport Layer Security

TTL – Time to Live

VLAN – Virtual Local Area Network

VTP – VLAN Trunking Protocol

BÖLÜM I
GİRİŞ

Bilgisayar ağları, birden fazla cihazın veri alışverişi gerçekleştirmesini sağlayan yapılar olup günümüz bilgi toplumunun temel iletişim altyapısını oluşturmaktadır. Forouzan, B. A. (2013). İnternetin yaygınlaşması, mobil teknolojilerin gelişimi ve bulut bilişim sistemlerinin artan kullanımıyla birlikte bilgisayar ağlarının önemi giderek artmıştır. Bu gelişmeler, ağ sistemlerinin yalnızca veri iletimi açısından değil, aynı zamanda güvenlik açısından da kritik bir rol üstlenmesine neden olmuştur (Tanenbaum & Wetherall, 2011).

Ağ iletişiminin standartlaştırılması amacıyla geliştirilen OSI (Open Systems Interconnection) referans modeli, iletişim sürecini yedi katmanda ele alarak her katmanın belirli görevleri yerine getirmesini sağlamaktadır. (Memon, 2015) Bu katmanlar sırasıyla fiziksel katman, veri bağlantı katmanı, ağ katmanı, taşıma katmanı, oturum katmanı, sunum katmanı ve uygulama katmanıdır. (Sütçü, 1994)OSI modeli, ağ sistemlerinin tasarımı ve analizinde temel bir çerçeve sunmakta olup günümüzde IoT ve modern ağ mimarilerinde de referans model olarak kullanılmaya devam etmektedir (Bora et al., 2014; Yavuzer Aslan & Aslan, 2023).

Siber güvenlik alanında yapılan çalışmaların büyük bir bölümü uygulama ve ağ katmanı tehditlerine odaklanırken, veri bağlantı katmanı (Layer 2) çoğu zaman göz ardı edilmektedir. Oysa veri bağlantı katmanı; MAC adresleme, çerçeveleme ve aynı yerel ağ üzerindeki cihazlar arasındaki veri iletiminden sorumlu olması nedeniyle ağın temel yapı taşlarından biridir. (Memon, 2015) Bu katmanda çalışan Ethernet anahtarları, köprüler ve kablosuz erişim noktaları, ağ trafiğinin yönlendirilmesinde kritik rol oynamaktadır (Seifert & Edwards, 2008).

Veri bağlantı katmanında kullanılan ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) ve STP (Spanning Tree Protocol) gibi protokoller, tasarım aşamasında güvenlikten ziyade işlevsellik ve performans odaklı geliştirilmiştir. (Jha & Bhardwaj, 2014) Bu nedenle söz konusu protokoller kimlik doğrulama ve yetkilendirme mekanizmalarından yoksundur. Bu durum, saldırganların ağ trafiğini manipüle etmesine, dinlemesine veya kesintiye uğratmasına olanak tanımaktadır (Bhardwaj et al., 2021).

Layer 2 seviyesinde gerçekleştirilen saldırılar arasında ARP sahteciliği (ARP Spoofing), MAC adres taşması (MAC Flooding), DHCP açlığı (DHCP Starvation), VLAN atlama

(VLAN Hopping) ve STP manipülasyonu yer almaktadır. Bu saldırılar, ortadaki adam (Man-in-the-Middle) saldırılarına zemin hazzırlamakta ve üst katmanlardaki güvenlik mekanizmalarını etkisiz hale getirebilmektedir (Nam et al., 2012). Bu nedenle veri bağlantı katmanı güvenliği, bütünsel bir ağ güvenliği yaklaşımının ayrılmaz bir parçası olarak değerlendirilmelidir.

1.1. Problem

Bilgisayar ağlarının giderek karmaşıklaşması ve siber saldırıların artmasıyla birlikte, ağ güvenliğine yönelik tehditler de çeşitlenmiş ve derinleşmiştir. (Sütçü, 1994) Siber güvenlik literatüründe uygulama ve ağ katmanı saldırıları kapsamlı biçimde ele alınmış olsa da, OSI referans modelinin ikinci katmanı olan veri bağlantı katmanı (Layer 2) güvenlik açısından yeterince incelenmemiştir (Bhardwaj et al., 2021). Bu katmanda çalışan ARP, DHCP ve STP gibi protokoller, orijinal tasarımlarında güvenlik mekanizmaları içermemektedir. Bu eksiklik; ARP Spoofing, DHCP Starvation, VLAN Hopping ve STP Manipülasyonu gibi saldırıların gerçekleştirilmesine zemin hazırlamakta, ağ trafiğinin dinlenmesine, manipüle edilmesine veya kesintiye uğratılmasına neden olmaktadır (Neminath & Tripathi, 2016). Bu çalışmanın temel problemi, Layer 2 düzeyindeki saldırı vektörlerinin teknik mekanizmalarının ve bu saldırılara karşı geliştirilen güvenlik çözümlerinin sistematik biçimde ortaya konulmamasıdır.

1.2. Araştırmanın Amacı

Bu çalışmanın temel amacı, OSI referans modelinin ikinci katmanında (Layer 2) gerçekleştirilen başlıca saldırı türlerini teknik mekanizmaları, etki alanları ve önleme yöntemleri bakımından kapsamlı biçimde incelemektir. Bu amaç doğrultusunda çalışmada şu hedefler belirlenmiştir: (1) ARP Spoofing, DHCP Starvation, VLAN Hopping ve STP Manipülasyonu saldırılarının çalışma mekanizmalarını ortaya koymak; (2) söz konusu saldırılara karşı geliştirilmiş güvenlik çözümlerini (Dynamic ARP Inspection, DHCP Snooping, BPDU Guard vb.) değerlendirmek; (3) simülasyon ortamında (GNS3/Cisco IOS) bu saldırıları ve karşı tedbirleri uygulamalı olarak göstermek. Böylece ağ yöneticilerine ve güvenlik uzmanlarına veri bağlantı katmanı güvenliğini güçlendirmeye yönelik pratik bir rehber sunulması hedeflenmektedir (Bhardwaj et al., 2021; Hijazi et al., 2019).

1.3. Araştırmanın Önemi

Kurumsal ağlarda yaşanan güvenlik ihlallerinin önemli bir bölümü, şirket güvenlik duvarı (firewall) gibi dış güvenlik mekanizmalarını aşmak yerine iç ağ üzerinden gerçekleştirilmektedir (Bhardwaj et al., 2021). Layer 2 saldırıları, üst katman güvenlik önlemlerini (SSL, TLS, IPSec vb.) devre dışı bırakabildiğinden ve ağ içinden kolaylıkla uygulanabildiğinden son derece tehlikeli bir saldırı sınıfı oluşturmaktadır. Nitekim ARP tabanlı saldırıların önlenmediği durumlarda kurumsal veri sızıntılarının kaçınılmaz hâle geldiğini vurgulamaktadır. Bu çalışma; günümüzde sıklıkla göz ardı edilen veri bağlantı katmanı güvenliğine odaklanarak hem akademik literatürdeki boşluğu doldurmakta hem de uygulamaya dönük bilgi birikimi sunmaktadır Morsy ve Nashat (2022), Özellikle Türkiye'de bu konudaki Türkçe kaynak sayısının sınırlı olması, araştırmanın özgün değerini artırmaktadır.

1.4. Sayıltılar

Bu çalışmada aşağıdaki sayıltılardan hareket edilmiştir: (1) Simülasyon ortamında (GNS3 ve Cisco IOS) gerçekleştirilen saldırı ve savunma senaryolarının gerçek ağ ortamlarındaki davranışları yeterince temsil ettiği varsayılmaktadır. (2) Çalışmada ele alınan Layer 2 protokollerinin (ARP, DHCP, STP, 802.1Q) standart IEEE ve IETF spesifikasyonlarına uygun biçimde uygulandığı kabul edilmektedir. (3) Kullanılan akademik kaynakların yöntemsel açıdan güvenilir olduğu ve bilimsel denetimden geçtiği varsayılmaktadır.

1.5. Sınırlılıklar

Bu çalışma aşağıdaki sınırlılıklar çerçevesinde yürütülmüştür: (1) Araştırma kapsamı OSI modelinin yalnızca ikinci katmanında (veri bağlantı katmanı) gerçekleştirilen saldırılarla sınırlı tutulmuş; ağ (Layer 3) ve üzeri katmanlardaki saldırılar kapsam dışında bırakılmıştır. (2) Simülasyon ortamı olarak GNS3 ve Cisco Packet Tracer kullanılmış; deneyler fiziksel donanım üzerinde değil, sanal ortamda gerçekleştirilmiştir. (3) Kullanılan Cisco IOS sürümü ve donanım simülasyonları, tüm üretici ve platform kombinasyonlarını temsil etmeyebilir. (4) Çalışma, kablolu (Ethernet) yerel alan ağları üzerine odaklanmış olup kablosuz ağlara (Wi-Fi) özgü Layer 2 saldırıları inceleme dışında bırakılmıştır.

1.6. Tanımlar

Layer 2 (Veri Bağlantı Katmanı): OSI referans modelinin ikinci katmanıdır. MAC adresleme, çerçeveleme (framing) ve aynı yerel ağ (LAN) segmentindeki cihazlar arasında veri iletiminden sorumludur. Forouzan, B. A. (2013).

ARP (Address Resolution Protocol): Bir IP adresine karşılık gelen MAC adresini bulmak için kullanılan protokoldür. Kimlik doğrulama mekanizmasından yoksun olması nedeniyle sahtekârlık (spoofing) saldırılarına açıktır (Hijazi et al., 2019).

DHCP (Dynamic Host Configuration Protocol): Ağa bağlanan istemcilere otomatik olarak IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS adresi atayan protokoldür. Kimlik doğrulama yapısı olmadığından DHCP Starvation ve DHCP Spoofing saldırılarına karşı savunmasızdır (Tripathi & Hubballi, 2018).

VLAN (Virtual Local Area Network): Fiziksel olarak aynı anahtar üzerinde bulunmalarına karşın mantıksal olarak birbirinden izole edilmiş ağ segmentleridir. IEEE 802.1Q standardıyla tanımlanmaktadır.

STP (Spanning Tree Protocol): IEEE 802.1D standardıyla tanımlanan ve anahtarlar arasındaki döngüleri (loop) önlemek amacıyla kullanılan protokoldür. BPDU mesajları aracılığıyla kök köprü (root bridge) seçimi gerçekleştirilir; bu sürecin kimlik doğrulamadan yoksun olması STP Manipülasyonu saldırılarına yol açmaktadır (Bhardwaj et al., 2021).

Man-in-the-Middle (MitM) Saldırısı: Saldırganın iki taraf arasındaki iletişime gizlice müdahale ettiği saldırı türüdür. Layer 2 saldırıları bu tür saldırılar için zemin hazırlamaktadır (Nam et al., 2012).

CAM Tablosu (Content Addressable Memory Table): Anahtarların (switch) MAC adreslerini ve bu adreslerin bağlı olduğu port numaralarını eşleştiren dinamik tablodur. MAC Flooding saldırısında bu tablo sahte adreslerle doldurularak anahtarın hub moduna geçmesi sağlanır (Gajo, 2025).

BÖLÜM II
KAVRAMSAL ÇERÇEVE

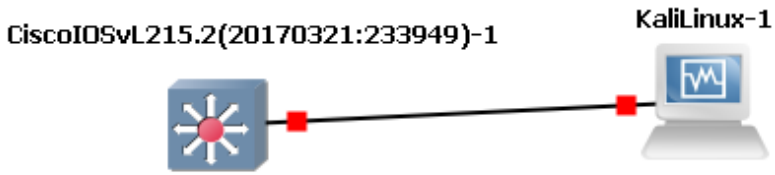
Bu bölümde, OSI referans modelinin ikinci katmanında gerçekleştirilen başlıca saldırı türlerine ve bu saldırılara karşı geliştirilen güvenlik çözümleri ele alınmaktadır. Her bir saldırı türü; çalışma mekanizması, ağ üzerindeki etkileri ve önleme yöntemleri bakımından ayrı ayrı incelenmektedir.

2.1. MAC Flooding (CAM Overflow) Saldırısı

2.1.1 CAM Tablosu ve Switchin Çalışma Mantığı

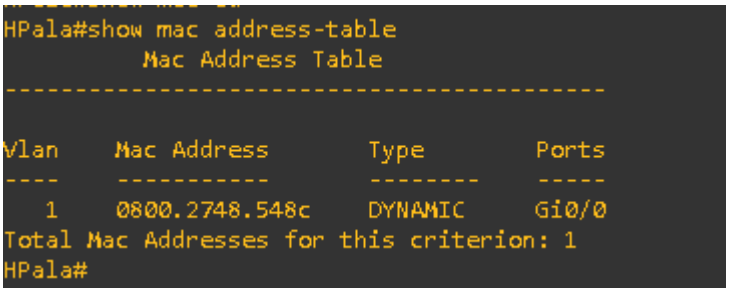
Anahtarlar (switch), bağlı olduğu cihazların MAC adreslerini ve bu adreslere karşılık gelen port numaralarını CAM (Content Addressable Memory) tablosunda saklarlar. Bu tablo sayesinde anahtarlar, gelen bir veri çerçevesini yalnızca hedef MAC adresinin bulunduğu porta iletir; böylece gereksiz ağ trafiği en aza indirilmiş olur. Anahtarın CAM tablosunu oluşturma süreci şu adımları izler: (Demirkol & Demirkol, t.y.) Gelen çerçevenin kaynak MAC adresi ve geldiği port kaydedilir. Hedef MAC adresi tabloda bulunmuyorsa çerçeve tüm portlara iletilir (flooding). Hedef cihaz yanıt verdiğinde bu cihaızn MAC adresi ve bulunduğu port da tabloya eklenir. (Gajo, 2025).

Anahtarların CAM tablosu sınırsız değildir; cihaza göre değişmekle birlikte belirli bir maksimum kapasite içermektedir. Tablodaki kayıtlar varsayılan olarak yaklaşık 300 saniye boyunca tutulur; bu süre içinde ilgili porttan trafik gelmezse kayıt silinir. Yerel alan ağları (LAN) bu tablo mekanizmasına bağımlı olduğundan, söz konusu yapıdaki açıklar çeşitli saldırılara zemin hazırlamaktadır. (Gajo, 2025).



Şekil 2.1. Saldırı simülasyonu için kullanılan ağ topolojisiGNS-3 (Cisco Switch – Kali Linux)

Şekil 2.1'de görüldüğü üzere simülasyon ortamı, bir Cisco anahtarı ile Kali Linux işletim sisteminin kurulu olduğu bir saldırgan makineden oluşmaktadır. Saldırı öncesinde anahtarın MAC adres tablosunda yalnızca Kali Linux cihazına ait tek bir kayıt bulunmaktadır.

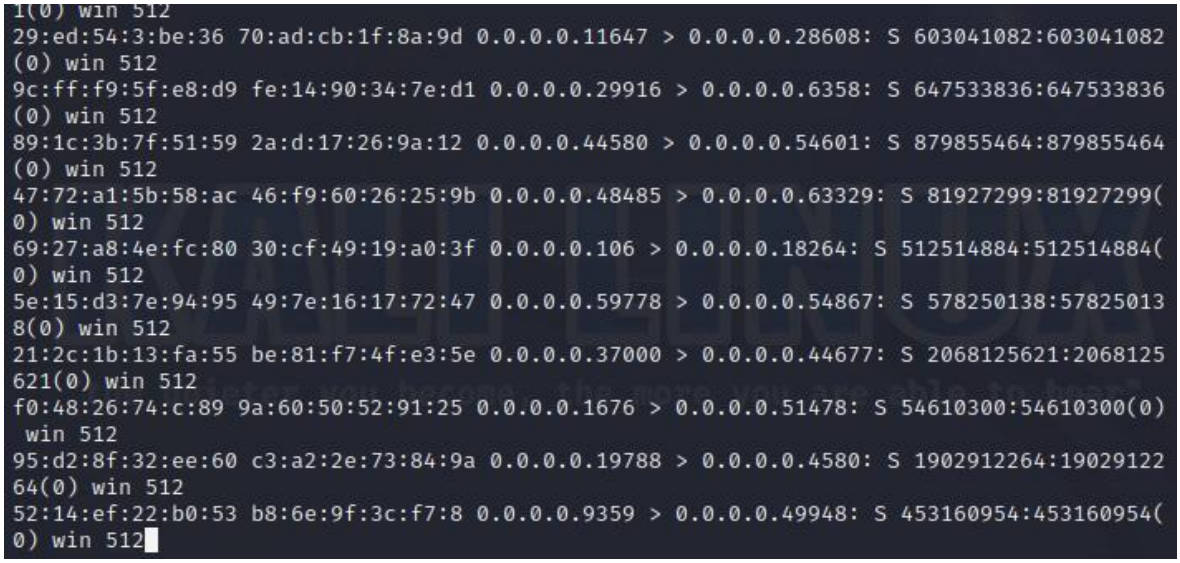


Şekil 2.2. Saldırı öncesi CAM tablosu

2.1.2 Saldırının Mekanizması

MAC Flooding saldırısı, saldırganın ağa bağlandığı anahtarın CAM tablosunu sahte MAC adresleriyle doldurmayı hedefler. Kali Linux üzerinde çalışan macof aracı kullanılarak büyük miktarda sahte MAC çerçevesi hedefe gönderilebilmektedir (Gajo, 2025). Saldırıyı başlatmak için aşağıdaki komut çalıştırılır:

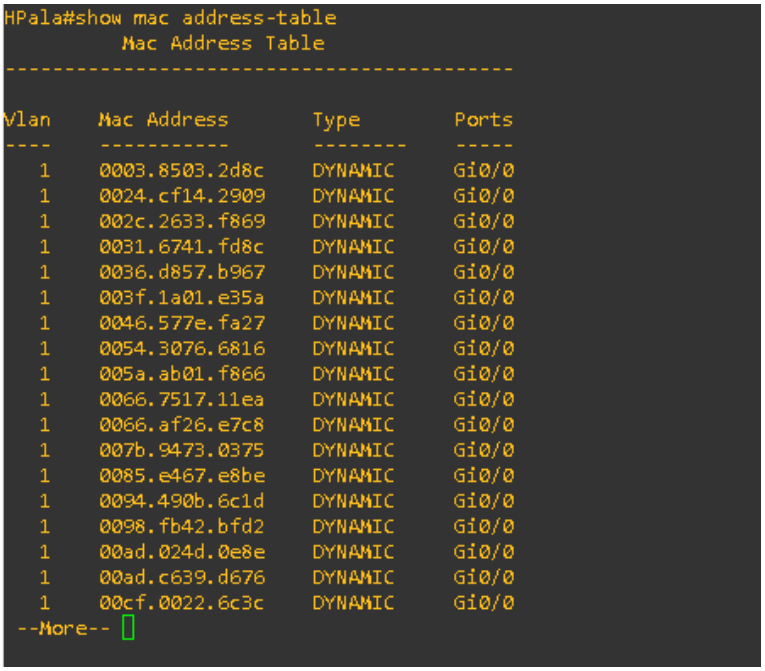
Şekil 2.3. Kali Linux üzerinde macof aracının çalıştırılması



Şekil 2.4. macof aracıyla üretilen sahte MAC adresleri

Şekil 2.4'te görüldüğü üzere saldırı başlatıldığında anahtar, çok sayıda farklı kaynak MAC adresinden gelen çerçevelerle karşı karşıya kalmaktadır. Bu çerçeveler anahtarın CAM tablosunu kısa sürede doldurur. Tablo dolduğunda anahtar iki farklı tepki verebilir: Fail-open modunda hub benzeri bir davranış sergileyerek tüm trafiği tüm portlara yayınlamaya başlar; bu durum ağdaki hassas verilerin yetkisiz cihazlar tarafından ele geçirilmesi riskini doğurur. Fail-closed modunda ise anahtar tepkisiz hale gelir ve MAC adres tablosu temizlenene kadar trafik iletimini durdurur (Gajo, 2025).

Bu açıdan değerlendirildiğinde MAC Flooding saldırısı, aynı zamanda bir Hizmet Reddi (Denial-of-Service, DoS) saldırısı niteliği de taşımaktadır (Gajo, 2025). Alcaraz (2017), bu saldırıların erişim katmanı anahtarlarının fiziksel güvenliğinin yeterince sağlanamadığı ofis ortamları, ortak çalışma alanları ve eğitim kurumlarında özellikle yaygın olduğunu vurgulamaktadır.



Şekil 2.5. Saldırı sonrası CAM tablosunun durumu

Şekil 2.5'te saldırı sonrasında anahtarın CAM tablosunun tamamının sahte MAC adresleriyle dolduğu görülmektedir. Tüm kayıtlar aynı fiziksel porta (Gi0/0) atanmış durumdadır; bu durum saldırının tek bir port üzerinden gerçekleştirildiğini açıkça ortaya koymaktadır.

2.1.3. Güvenlik Çözümü: Port Security

MAC Flooding saldırısına karşı en etkili ve yaygın çözüm, anahtarlar üzerinde Port Security özelliğinin etkinleştirilmesidir. Port Security, her porta bağlanabilecek maksimum MAC adresi sayısını sınırlandırarak CAM tablosunun sahte adreslerle doldurulmasını engeller. Gajo (2025) tarafından gerçekleştirilen Packet Tracer simülasyonunda, port başına yalnızca bir MAC adresine izin verecek şekilde yapılandırılan anahtarın MAC Flooding saldırısına karşı başarıyla korunduğu gösterilmiştir. Bu yapılandırmada yetkisiz bir cihaz porta bağlandığında port otomatik olarak kapatılmış ve bağlantı kesilmiştir.

Port Security yapılandırması aşağıdaki adımlarla uygulanmaktadır.

Switch# clear mac address-table dynamic

Switch# configure terminal

Switch(config)# interface gigabitEthernet 0/0

Switch(config-if)# switchport mode access

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security violation shutdown
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery interval 30
```

Port Security kapsamında MAC adresi öğrenme yöntemi iki şekilde yapılandırılabilir. Sticky yönteminde, porta dinamik olarak bağlanan ilk cihazın MAC adresi kalıcı olarak kaydedilir ve bu adres dışındaki cihazlara erişim izni verilmez. Statik yöntemde ise ağ yöneticisi izin verilen MAC adresini doğrudan yapılandırma üzerinden tanımlar (Gajo, 2025). Alcaraz (2017) ise sticky MAC öğrenmenin sabit cihazların bulunduğu ortamlarda güçlü bir kimlik tabanlı erişim denetimi sağladığını; ancak cihaz değişiminin sık yaşandığı BYOD (Bring Your Own Device) ortamlarında dikkatli yönetilmesi gerektiğini belirtmektedir. (Siddiqui, 2014)

İhlal (violation) durumunda anahtarın vereceği tepki de Port Security kapsamında yapılandırılabilmektedir. Üç farklı ihlal modu bulunmaktadır:

- Shutdown modu: İhlal gerçekleştiğinde ilgili port tamamen kapatılarak Error-Disabled durumuna getirilir. SNMP trap ve syslog mesajı gönderilir. En katı güvenlik yaklaşımını temsil eder ve ortalama 3 saniyede tehdidi kontrol altına alır (Alcaraz, 2017).
- Restrict modu: Port kapatılmaz; ancak kurala aykırı paketler düşürülür ve SNMP üzerinden ağ yöneticisine TRAP mesajı iletilir. Bu mod, güvenlik ile kullanılabilirlik arasında denge kurduğundan kurumsal ortamlar için önerilen varsayılan yapılandırma olarak değerlendirilmektedir (Alcaraz, 2017).
- Protect modu: Paketler düşürülür; ancak herhangi bir uyarı veya kayıt oluşturulmaz. Görünürlüğün kritik olduğu ortamlarda bu modun tek başına kullanılması önerilmemektedir (Alcaraz, 2017; Gajo, 2025).

Kapatılan portun otomatik olarak yeniden devreye alınması da yapılandırılabilmektedir. Bu amaçla errdisable recovery cause psecure-violation komutu kullanılarak portun belirli bir

süre sonunda (örneğin 30 saniye) normal çalışma durumuna dönmesi sağlanabilir. Bu süre zarfında saldırı devam ediyorsa ihlal işlemi yeniden uygulanır (Gajo, 2025).

2.2. DHCP Starvation ve DHCP Spoofing Saldırıları

2.2.1. DHCP Protokolü ve Çalışma Mantığı

DHCP (Dynamic Host Configuration Protocol), ağ üzerindeki istemcilere otomatik olarak IP adresi, alt ağ maskesi (subnet mask), varsayılan ağ geçidi (default gateway) ve DNS sunucusu gibi yapılandırma bilgilerini sağlayan bir uygulama katmanı protokolüdür. DHCP, istemci ve sunucu arasında gerçekleşen "Discover, Offer, Request, Acknowledge (DORA)" süreci ile çalışmaktadır (Droms, 1997).

2.2.2. Saldırının Mekanizması: DHCP Spoofing ve DHCP Starvation

DHCP protokolü, ağ yönetimini kolaylaştırmakla birlikte, tasarımında kimlik doğrulama mekanizmalarının bulunmaması nedeniyle çeşitli güvenlik açıklarına sahiptir. Bu açıkların başında DHCP Spoofing saldırısı gelmektedir. (Kumar & Singh, 2022) Bu saldırıda, ağ içerisine sızan bir tehdit aktörü yetkisiz bir DHCP sunucusu kurarak istemcilerin gönderdiği DHCP Discover mesajlarına sahte DHCP Offer yanıtları verir. İstemciler genellikle ilk aldıkları DHCP Offer mesajını kabul ettiklerinden dolayı, saldırgan tarafından sağlanan hatalı ağ yapılandırma bilgilerini kullanabilirler (Tripathi & Hubballi, 2018).

DHCP Spoofing saldırıları sonucunda istemciler, sahte DNS sunucularına veya kötü niyetli ağ geçitlerine yönlendirilebilir. Bu durum, kullanıcıların sahte web sitelerine yönlendirilmesi ve kimlik bilgilerinin ele geçirilmesi gibi sonuçlar doğurabilir. Ayrıca saldırgan, kendisini varsayılan ağ geçidi gibi göstererek ortadaki adam (Man-in-the-Middle) saldırıları gerçekleştirebilir ve ağ trafiğini izleyebilir veya manipüle edebilir (Griffin & Schneider, 2007).

DHCP tabanlı bir diğer önemli saldırı türü DHCP Starvation saldırısıdır. Bu saldırıda tehdit aktörü, farklı MAC adresleri kullanarak çok sayıda DHCP Discover mesajı gönderir ve DHCP sunucusundaki IP adres havuzunu tüketir. Sonuç olarak, ağa bağlanmak isteyen meşru istemciler IP adresi alamaz ve ağ hizmetlerinde kesinti meydana gelir (Mishra & Singh, 2012).

Bu tür saldırılar yalnızca kötü niyetli kullanıcılar tarafından değil, aynı zamanda bilinçsiz kullanıcı davranışları sonucunda da ortaya çıkabilir. Örneğin, kurumsal bir ağa bağlanan ev tipi modem veya yönlendirici cihazlar, varsayılan olarak aktif gelen DHCP sunucu özellikleri nedeniyle ağda yetkisiz DHCP hizmeti sağlayabilir ve benzer güvenlik sorunlarına yol açabilir.

2.2.3. Güvenlik Çözümü: DHCP Snooping

DHCP tabanlı saldırıların önlenmesinde en yaygın yöntemlerden biri DHCP Snooping mekanizmasıdır. DHCP Snooping, anahtar (switch) üzerinde çalışan bir güvenlik özelliği olup, yalnızca güvenilir (trusted) portlardan gelen DHCP sunucu mesajlarına izin verirken, diğer portları güvenilmez (untrusted) olarak işaretler. Bu sayede yetkisiz DHCP sunucularının ağa müdahale etmesi engellenir (Cisco Systems, 2012).

Ayrıca DHCP Snooping, port başına DHCP paket oranını sınırlayarak DHCP Starvation saldırılarını da önleyebilmektedir. Bu mekanizma sayesinde, belirli bir zaman diliminde gönderilebilecek DHCP paket sayısı sınırlandırılır ve anormal trafik davranışları engellenir. Bununla birlikte, DHCP Snooping tarafından oluşturulan bağlama tablosu (binding table), ağ yöneticilerine hangi IP adresinin hangi MAC adresi ve port ile eşleştiğini izleme imkânı sunarak ağ güvenliğinin artırılmasına katkı sağlar.

Sonuç olarak, DHCP protokolünün doğasında bulunan güvenlik zafiyetleri, özellikle veri bağlantı katmanında ciddi tehditler oluşturabilmektedir. Bu nedenle DHCP Snooping gibi güvenlik mekanizmalarının kullanılması, kurumsal ağların bütünlüğü ve sürekliliği açısından kritik öneme sahiptir.

```
HuseyinPala(config)# ip dhcp snooping

HuseyinPala(config)# interface fastEthernet 0/1

HuseyinPala(config-if)# ip dhcp snooping trust

HuseyinPala(config-if)# exit

HuseyinPala(config)# interface range fastEthernet 0/5-24

HuseyinPala(config-if-range)# ip dhcp snooping limit rate 6
```

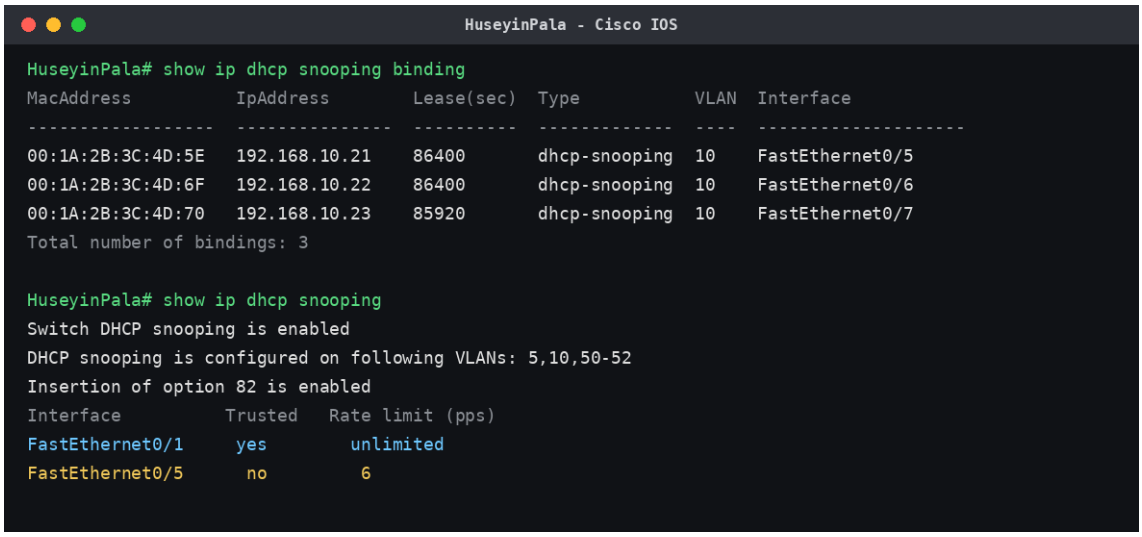
HuseyinPala(config-if-range)# exit

HuseyinPala(config)# ip dhcp snooping vlan 5,10,50-52

HuseyinPala(config)# exit

HuseyinPala# show ip dhcp snooping

HuseyinPala# show ip dhcp snooping binding (EN İYİ KONTROL KOMUTU)



Şekil 2.6. Cisco IOS üzerinde DHCP Snooping bağlama (binding) tablosu ve port güven (trust) durumu

2.3. ARP Spoofing (ARP Zehirlenmesi) Saldırısı

2.3.1. ARP Protokolü ve Çalışma Mantığı

ARP (Address Resolution Protocol), yerel ağ (LAN) üzerinde bir IP adresine karşılık gelen MAC adresini bulmak için kullanılan bir protokoldür. Bir cihaz, iletişim kurmak istediği hedef cihazın MAC adresini bilmediğinde ağa "Bu IP adresinin sahibi kim?" diye bir ARP isteği (ARP Request) yayınlar. (Whalen, 2001) Hedef cihaz MAC adresini içeren bir ARP yanıtı (ARP Reply) göndererek kendini tanıtır ve bu eşleşme, istek sahibi cihazın ARP önbelleğine (ARP cache) kaydedilir. (Whalen, 2001) ARP, 1982 yılında RFC 826 ile tanımlanmış olup tasarımı sırasında güvenlik değil işlevsellik ön planda tutulmuştur; bu nedenle protokol kimlik doğrulama mekanizmasından tamamen yoksundur (Hijazi et al., 2019).

ARP'nin kritik bir güvenlik zafiyeti, Gratuitous ARP (GARP) mekanizmasından kaynaklanmaktadır. GARP, bir cihazın isteğe bağlı olarak kendi IP-MAC eşleşmesini ağa duyurmasına olanak tanır. Ağdaki diğer cihazlar bu duyuruyu doğrulamaksızın kabul ederek ARP önbelleklerini günceller. Bu durum, saldırganların sahte ARP yanıtları göndererek kurbanların ARP tablolarını zehirlemesine (ARP poisoning) zemin hazırlamaktadır (Bhardwaj et al., 2021).

2.3.2. Saldırının Mekanizması

ARP Spoofing saldırısında saldırgan, ağda birden fazla cihaza sahte ARP yanıtları göndererek kurbanların ARP önbelleklerini kendi MAC adresiyle zehirler. Örneğin A istemcisi ile ağ geçidi (gateway) arasındaki iletişimi ele geçirmek isteyen saldırgan (S), hem A cihazına "Ben gateway'im, MAC adresim S'dir" hem de gateway'e "Ben A'yım, MAC adresim S'dir" mesajı gönderir. Bu işlemin ardından A ile gateway arasındaki tüm trafik saldırgan üzerinden geçmeye başlar; bu durum klasik bir Ortadaki Adam (Man-in-the-Middle, MitM) saldırısını oluşturmaktadır (Nam et al., 2012).

Saldırı Kali Linux platformunda arpspoof veya ettercap araçlarıyla kolaylıkla gerçekleştirilebilmektedir. Aşağıda Cisco IOS komut arayüzünde, saldırı öncesinde ve sonrasında gerçekleştirilen ARP tablo kontrolü gösterilmektedir:

Router# show arp

Protocol Address Age(min) Hardware Addr Type Interface

Internet 192.168.1.10 5 aabb.cc00.0100 ARPA Gi0/0

! -- Saldırı sonrası: 192.168.1.10 artık saldırganın MAC adresini gösteriyor --

Internet 192.168.1.10 2 dead.beef.1337 ARPA Gi0/0 <-- SAHTE!

Şekil 2.7. Cisco IOS üzerinde show arp komutu: Saldırı öncesi (normal) ve sonrası (zehirlenmiş) ARP tablosu

2.3.3. Güvenlik Çözümü: Dynamic ARP Inspection (DAI)

ARP Spoofing saldırısına karşı en etkili savunma mekanizması Dynamic ARP Inspection (DAI)'dır. DAI, anahtarlar üzerinde çalışan bir güvenlik özelliği olup gelen ARP paketlerini DHCP Snooping bağlama tablosuyla (binding table) karşılaştırarak yalnızca meşru IP-MAC eşleşmelerine izin verir; sahte ARP yanıtlarını düşürür. Bu sayede ARP önbelleği zehirlenmesi ve dolayısıyla MitM saldırıları önlenmektedir (Morsy & Nashat, 2022;

Bhardwaj et al., 2021). Cisco IOS üzerinde DAI yapılandırması şu şekilde gerçekleştirilmektedir:

```
Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 10

Switch(config)# ip arp inspection vlan 10

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# ip dhcp snooping trust

Switch(config-if)# ip arp inspection trust

Switch# show ip arp inspection vlan 10
```

Şekil 2.8. Cisco IOS üzerinde Dynamic ARP Inspection (DAI) yapılandırması

2.4. VLAN Hopping (VLAN Atlama) Saldırısı

2.4.1. VLAN ve Trunk Bağlantısının Çalışma Mantığı

VLAN (Virtual Local Area Network), tek bir fiziksel anahtar üzerinde birden fazla mantıksal ağ segmenti oluşturulmasına olanak tanıyan IEEE 802.1Q standardına dayalı bir teknolojidir. Forouzan, B. A. (2013). VLAN'lar sayesinde farklı departmanlar veya güvenlik bölgeleri birbirinden izole edilmekte, yayın trafiği (broadcast) sınırlandırılmakta ve ağ yönetimi kolaylaşmaktadır. Anahtarlar arasında birden fazla VLAN trafiğini taşıyan bağlantılar trunk port olarak adlandırılır; bu portlar 802.1Q çerçeveleme ile VLAN etiketlerini (tag) iletir (Bhardwaj et al., 2021).

Cisco anahtarlarında port modu, DTP (Dynamic Trunking Protocol) aracılığıyla otomatik olarak müzakere edilebilmektedir. Varsayılan olarak birçok Cisco anahtarı portu "dynamic auto" veya "dynamic desirable" modunda çalışır; bu durum portun karşı tarafla trunk bağlantısı kurmasına izin verir. Bu yapılandırma zafiyeti, VLAN Hopping saldırısının temel sömürü noktasını oluşturmaktadır (Bhardwaj et al., 2021).

2.4.2. Saldırının Mekanizması

VLAN Hopping saldırısı iki farklı teknikle gerçekleştirilebilir. Birincisi Switch Spoofing saldırısıdır: Saldırgan, bağlı olduğu anahtarın portuna DTP mesajları göndererek trunk bağlantısı müzakeresi başlatır. Port "dynamic" modda olduğundan trunk moduna geçer ve saldırgan tüm VLAN trafiğine erişim kazanır. İkincisi Double Tagging (Çift Etiketleme)

saldırısıdır: Saldırgan, paketlerine iki katmanlı 802.1Q etiketi ekler. Dıştaki etiket anahtarın kendi VLAN'ı(genellikle native VLAN, VLAN 1) ile eşleşir ve anahtar bu etiketi kaldırarak paketi iletir. İkinci etiket ise hedef VLAN'ı tanımlar ve paket farklı bir VLAN segmentine ulaşır (Neminath & Tripathi, 2016).

Aşağıda Cisco IOS üzerinde saldırı tespiti ve VLAN güvenlik durumunun kontrol edilmesine yönelik komutlar gösterilmektedir:

```
Switch# show interfaces trunk

Port      Mode        Encapsulation  Status        Native vlan

Gi0/0     on          802.1q         trunking      1
```

Şekil 2.9. Cisco IOS üzerinde show interfaces trunk komutu: Native VLAN 1 olarak görünen trunk port (VLAN Hopping riski taşır)

2.4.3. Güvenlik Çözümü: DTP Devre Dışı Bırakma ve Native VLAN Yalıtımı

VLAN Hopping saldırılarının önlenmesinde temel strateji, DTP'yi devre dışı bırakmak ve tüm kullanıcı portlarını statik olarak access moduna almaktır. Ayrıca native VLAN, kullanıcı trafiği taşımayan ayrı bir VLAN ID'ye atanmalı; kullanılmayan portlar kapatılarak izole bir VLAN'a taşınmalıdır (Bhardwaj et al., 2021). Cisco IOS üzerindeki yapılandırma şu şekilde gerçekleştirilir:

```
Switch(config)# interface range fa0/1 - 24

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

Switch(config-if-range)# switchport nonegotiate

! -- Trunk portlarda native VLAN'i özel bir VLAN'a al --

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk native vlan 999

Switch(config-if)# switchport nonegotiate
```

Şekil 2.10. Cisco IOS üzerinde VLAN Hopping karşı önlemleri: DTP devre dışı bırakma ve native VLAN 999 ataması

2.5. STP Manipülasyonu Saldırısı

2.5.1. STP'nin Çalışma Mantığı

STP (Spanning Tree Protocol), IEEE 802.1D standardıyla tanımlanan ve anahtarlı ağlarda (switched networks) döngüleri (loop) önlemek amacıyla geliştirilmiş bir Layer 2 protokolüdür. Anahtarlar arasında birden fazla fiziksel yol bulunduğunda STP, kök köprü (root bridge) seçimi yaparak ağın döngüsüz ve mantıksal olarak ağaç topolojisinde çalışmasını sağlar. Bu süreçte anahtarlar, BPDU (Bridge Protocol Data Unit) mesajlarını periyodik olarak birbirlerine gönderir. En düşük bridge priority değerine sahip anahtar kök köprü olarak seçilir; bağ (tie) durumunda en düşük MAC adresine bakılır. STP'nin herhangi bir kimlik doğrulama mekanizması içermemesi, saldırganların BPDU mesajlarını taklit ederek ağ topolojisini manipüle etmesine olanak tanımaktadır (Bhardwaj et al., 2021).

2.5.2. Saldırının Mekanizması

STP Manipülasyonu saldırısında saldırgan, ağa özel olarak hazırlanmış BPDU mesajları göndererek kendisini kök köprü olarak tanıtmayı hedefler. Kali Linux üzerinde çalışan Yersinia aracı, bu tür saldırıları otomatik olarak gerçekleştirebilmektedir. Saldırgan, ağa "bridge priority = 0" gibi son derece düşük bir öncelik değeri içeren BPDU mesajları yayarak kök köprü seçimi sürecini yeniden tetikler. Anahtarlar, bu mesajları doğrulama yapamadan işler ve saldırganı kök köprü olarak kabul ederek tüm ağ trafiğini saldırganın üzerinden yönlendirmeye başlar. Bu durum hem ağ trafiğinin dinlenmesine (pasif MitM) hem de yeni kök köprü seçimi süreçleri nedeniyle ağda 30-50 saniyelik kesintilere yol açabilir (Bhardwaj et al., 2021).

Aşağıda Cisco IOS üzerinde mevcut STP topolojisinin görüntülenmesi ve saldırı öncesi/sonrası kök köprü değişiminin tespitine yönelik komutlar gösterilmektedir:

```
Switch# show spanning-tree vlan 10

VLAN0010

  Spanning tree enabled protocol ieee

  Root ID    Priority    0      <-- SALDIRGAN root secildi!

             Address     dead.beef.4444
```

Şekil 2.11. Cisco IOS üzerinde show spanning-tree çıktısı: STP Manipülasyonu saldırısı sonrası saldırganın root bridge seçilmesi

2.5.3. Güvenlik Çözümü: BPDU Guard ve Root Guard

STP Manipülasyonu saldırılarına karşı Cisco IOS'ta iki temel güvenlik mekanizması kullanılmaktadır. BPDU Guard, son kullanıcı portlarında (access ports) PortFast ile birlikte etkinleştirilerek bu portlara BPDU mesajı geldiğinde portu otomatik olarak err-disabled durumuna getirir; böylece saldırganın BPDU göndermesi engellenir. Root Guard ise anahtar üzerinde kök köprü olmaya aday olmayacak portlarda etkinleştirilerek bu portlardan gelen üstün BPDU mesajlarının ağ topolojisini etkilemesini önler (Bhardwaj et al., 2021). Yapılandırma şu şekilde gerçekleştirilir:

```
Switch(config)# spanning-tree portfast bpduguard default

Switch(config)# interface gigabitEthernet 0/2

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

Switch# show spanning-tree inconsistentports
```

Şekil 2.12. Cisco IOS üzerinde BPDU Guard ve Root Guard yapılandırması

2.6. VLAN Trunking Protokolü (VTP) Saldırısı

2.6.1. VTP Protokolünün Çalışma Mantığı

VLAN Trunking Protokolü (VTP), Cisco'ya özgü bir Layer 2 protokolü olup birden fazla anahtarın bulunduğu bir ağda VLAN veritabanının merkezi olarak yönetilmesini ve trunk bağlantılar üzerinden tüm anahtarlara otomatik olarak dağıtılmasını sağlamaktadır. Bir VTP etki alanındaki (domain) sunucu (server) modundaki bir anahtarda yapılan VLAN ekleme, silme veya yeniden adlandırma işlemleri, VTP Advertisement adı verilen mesajlarla diğer anahtarlara iletilmektedir (Abbasi Rad, 2024). Her VTP mesajı, VLAN veritabanındaki değişiklikleri izlemek amacıyla kullanılan bir yapılandırma revizyon numarası (configuration revision number) içermektedir; bir anahtar, kendisinden daha yüksek revizyon numarasına sahip bir VTP mesajı aldığında, kendi VLAN veritabanını gelen veriyle eş zamanlı olarak günceller.

VTP, sunucu, istemci, şeffaf (transparent) ve kapalı (off) olmak üzere dört farklı modda çalışabilmektedir. Sunucu modundaki anahtarlar VLAN değişikliği yapabilir ve bu değişiklikleri ağa duyurabilirken; istemci modundaki anahtarlar yalnızca gelen güncellemeleri kabul etmektedir. Bu mimarinin temel güvenlik zafiyeti, VTP'nin varsayılan olarak kimlik doğrulamadan yoksun olmasıdır; bir parola tanımlanmadığı sürece ağa

bağlanan herhangi bir anahtar, VTP etki alanı adını öğrenip uygun revizyon numarasına sahip sahte bir VTP mesajı göndererek tüm VLAN veritabanını değiştirebilmektedir (Abbasi Rad, 2024; Bhardwaj et al., 2021).

2.6.2. Saldırının Mekanizması

VTP saldırısında tehdit aktörü, ağa daha önce kullanılmış ve yüksek bir yapılandırma revizyon numarasına sahip bir anahtarı -ya da bu numarayı taklit eden sahte bir VTP mesajını- trunk bağlantı üzerinden ağa dahil eder. Saldırının gerçekleşebilmesi için saldırganın bağlı olduğu portun trunk moduna geçmesi (bkz. VLAN Hopping/Switch Spoofing, Bölüm 2.4) ve VTP etki alanı adını bilmesi gerekmektedir; etki alanı adı genellikle CDP/LLDP keşif saldırısı (Bölüm 2.7) ya da pasif VTP trafiği dinlemesi yoluyla elde edilmektedir. Saldırgan, mevcut en yüksek revizyon numarasından daha büyük bir değer taşıyan boş ya da değiştirilmiş bir VLAN veritabanı yayınladığında, etki alanındaki tüm sunucu ve istemci modundaki anahtarlar kendi VLAN veritabanlarını bu sahte veriyle günceller; bu durum mevcut VLAN'ların tamamen silinmesine yol açabilmektedir (Abbasi Rad, 2024).

Bu saldırının başlıca sonucu bir Hizmet Reddi (DoS) durumudur: VLAN veritabanı silindiğinde, ilgili VLAN'lara atanmış tüm portlar artık tanımlı olmayan bir VLAN'a ait olduğundan iletişim kurulamaz hale gelmekte ve kurumsal ağın tamamı kısa sürede kullanılamaz duruma gelebilmektedir. Yersinia gibi araçlar, sahte VTP paketlerinin (VLAN ekleme, silme veya özel paket gönderme) otomatik olarak üretilmesine imkân tanımaktadır.

Şekil 2.13. VTP saldırısı: yüksek revizyon numaralı sahte VTP mesajı sonucu VLAN veritabanının silinmesi

2.6.3. Güvenlik Çözümü: VTP Password, Transparent Mod ve Versiyon 3

VTP saldırılarına karşı en temel önlem, VTP etki alanında bir VTP parolası (vtp password) tanımlanmasıdır; bu sayede daha yüksek revizyon numarasına sahip bir anahtar dahi, doğru parolayı sağlamadığı sürece etki alanına dahil olamamaktadır (Abbasi Rad, 2024). Kurumsal ağlarda VLAN değişikliklerinin sık yapılmadığı durumlarda, anahtarların VTP Transparent moda alınması önerilmektedir; bu modda anahtar, VLAN veritabanını yalnızca yerel olarak tutar ve aldığı VTP mesajlarını işlemeden yalnızca iletir, böylece saldırının etkisi o anahtarla sınırlı kalır.

VTP'nin üçüncü sürümü (VTP Version 3), birincil sunucu (primary server) mekanizmasıyla VLAN değişikliklerinin yalnızca tek bir yetkili anahtar üzerinden yapılmasına imkân tanıyarak güvenliği önemli ölçüde artırmaktadır; bu sürümde ayrıca MD5 tabanlı daha güçlü bir kimlik doğrulama mekanizması da bulunmaktadır. Trunk olmayan portlarda switchport nonegotiate komutunun kullanılması ve kullanılmayan portların kapatılması, saldırganın trunk bağlantısı kurmasını engelleyerek VTP saldırısının ön koşulunu ortadan kaldırmaktadır (Abbasi Rad, 2024).

```
Switch - Cisco IOS (VTP Guvenlik)
Switch(config)# vtp domain MEDIPOL
Switch(config)# vtp password K4r4nl1k$VLAN!
Switch(config)# vtp version 3
Switch(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)# interface range fa0/1 - 24
Switch(config-if-range)# switchport nonegotiate
Switch(config-if-range)# exit
Switch# show vtp password
VTP Password: K4r4nl1k$VLAN!
Switch# show vtp status
VTP Operating Mode                : Transparent
VTP Domain Name                   : MEDIPOL
Configuration Revision            : 0
```

Şekil 2.14. Cisco IOS üzerinde VTP parolası, sürüm 3 ve Transparent mod yapılandırması

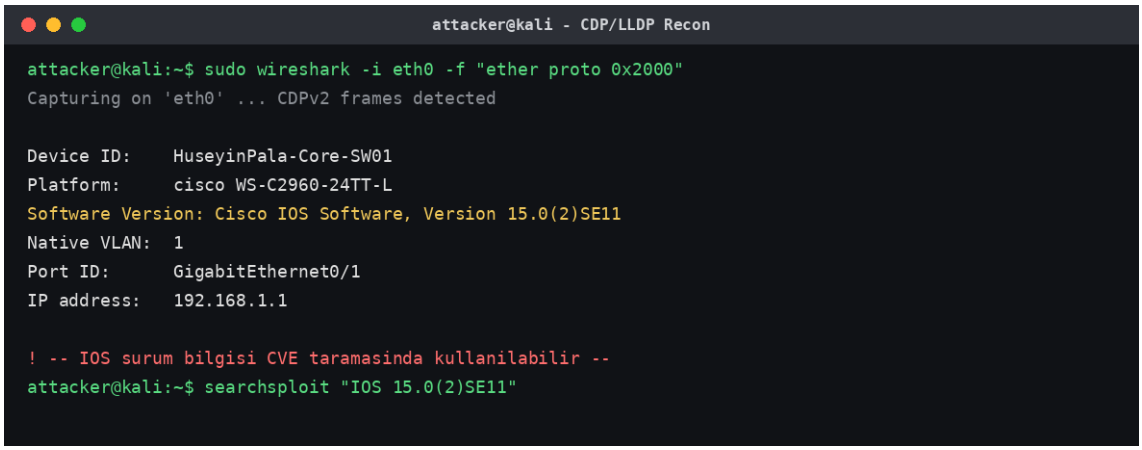
2.7. CDP/LLDP Keşif (Reconnaissance) Saldırısı

2.7.1. CDP ve LLDP Protokollerinin Çalışma Mantığı

Cisco Discovery Protocol (CDP), Cisco cihazlarının doğrudan bağlı komşularını -cihaz modeli, IOS sürümü, IP adresi, native VLAN ve port bilgileri dahil olmak üzere- otomatik olarak tanımasını sağlayan, Cisco'ya özgü ve varsayılan olarak etkin gelen bir Layer 2 keşif protokolüdür. IEEE 802.1AB ile standartlaştırılan Link Layer Discovery Protocol (LLDP) ise aynı işlevi vendor-bağımsız biçimde yerine getirmektedir. Her iki protokol de kimlik doğrulama veya şifreleme mekanizması içermeden, belirli aralıklarla multicast çerçeveler hâlinde cihaz bilgilerini ağa yaymaktadır (Gao et al., 2020).

2.7.2. Saldırının Mekanizması

CDP/LLDP keşif saldırısında tehdit aktörü, ağa fiziksel veya mantıksal olarak erişim sağladıktan sonra Wireshark gibi bir paket analiz aracıyla CDP/LLDP çerçevelerini pasif biçimde dinleyerek; hedef anahtarın model numarasını, çalıştırdığı IOS yazılım sürümünü, IP adresini ve native VLAN bilgisini elde edebilmektedir. Bu bilgiler doğrudan saldırı niteliği taşımamakla birlikte, saldırganın hedef cihaza özgü bilinen güvenlik açıklarını (CVE) araştırmasına ve sonraki aşamalardaki saldırılarını (VLAN Hopping, VTP saldırısı vb.) daha isabetli biçimde planlamasına imkân tanıyan kritik bir keşif (reconnaissance) adımı oluşturmaktadır (Sweeney, 2006). Ayrıca her iki protokol de kimlik doğrulamadan yoksun olduğundan, saldırgan sahte CDP/LLDP çerçeveleri enjekte ederek komşu cihazların topoloji tablolarını da bozabilmektedir.

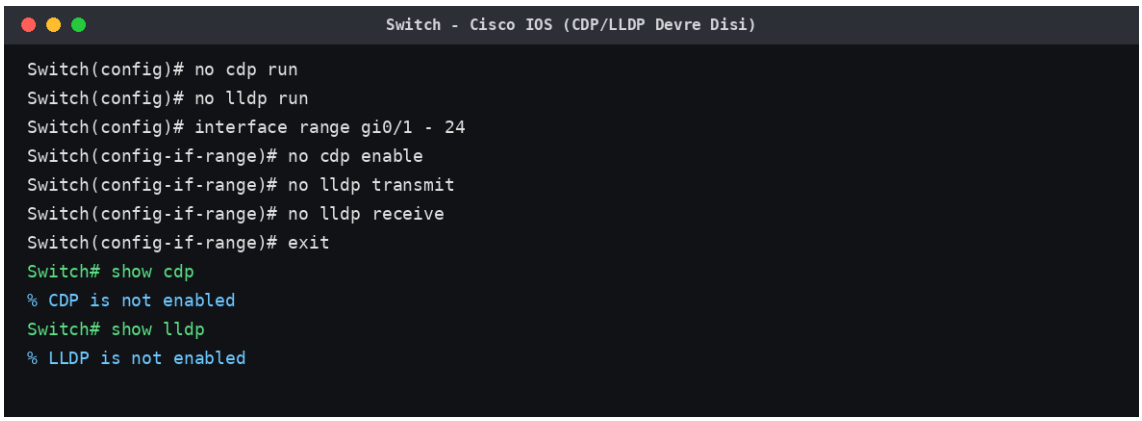


Şekil 2.15. Kali Linux üzerinde Wireshark ile CDP trafiğinin dinlenmesi ve IOS sürüm bilgisinin elde edilmesi

2.7.3. Güvenlik Çözümü: Protokollerin Devre Dışı Bırakılması

CDP/LLDP kaynaklı bilgi sızıntısının önlenmesinde en etkili yöntem, bu protokollerin yönetim amacıyla gerçekten ihtiyaç duyulmadığı arayüzlerde -özellikle son kullanıcı erişim

portlarında ve güvenilmeyen ağ sınırlarında- devre dışı bırakılmasıdır. Global olarak no cdp run ve no lldp run komutları ile protokoller tüm cihaz genelinde kapatılabileceği gibi, arayüz bazında no cdp enable ve no lldp transmit / no lldp receive komutlarıyla yalnızca belirli portlarda devre dışı bırakılabilmektedir. IP telefonu gibi CDP/LLDP bilgisine ihtiyaç duyan cihazların bağlı olduğu portlarda protokollerin etkin bırakılması, ancak bu portların port security ve DHCP snooping ile ayrıca korunması önerilmektedir (Gao et al., 2020).



Şekil 2.16. Cisco IOS üzerinde CDP ve LLDP protokollerinin global ve arayüz bazında devre dışı bırakılması

2.8. IPv6 Komşu Keşfi Protokolü (NDP) Sahteciliği ve RA Guard

2.8.1. NDP'nin Çalışma Mantığı ve ARP ile Karşılaştırılması

IPv6 ağlarında Komşu Keşfi Protokolü (Neighbor Discovery Protocol, NDP), IPv4 ortamında ARP'nin üstlendiği IP-MAC adres çözümleme işlevinin yanı sıra yönlendirici keşfi (router discovery), durumsuz otomatik adresleme (SLAAC) ve yinelenen adres tespiti (DAD) gibi işlevleri de yerine getirmektedir. NDP, ICMPv6 mesajları (Router Solicitation/Advertisement, Neighbor Solicitation/Advertisement) üzerinden çalışmakta olup, tıpkı ARP gibi yerel bağlantıdaki tüm düğümlerin güvenilir olduğu varsayımına dayanmaktadır ve varsayılan olarak herhangi bir kimlik doğrulama mekanizması içermemektedir (Barbhuiya et al., 2013).

2.8.2. Saldırının Mekanizması: Sahte Router Advertisement (RA) ve NS/NA Sahteciliği

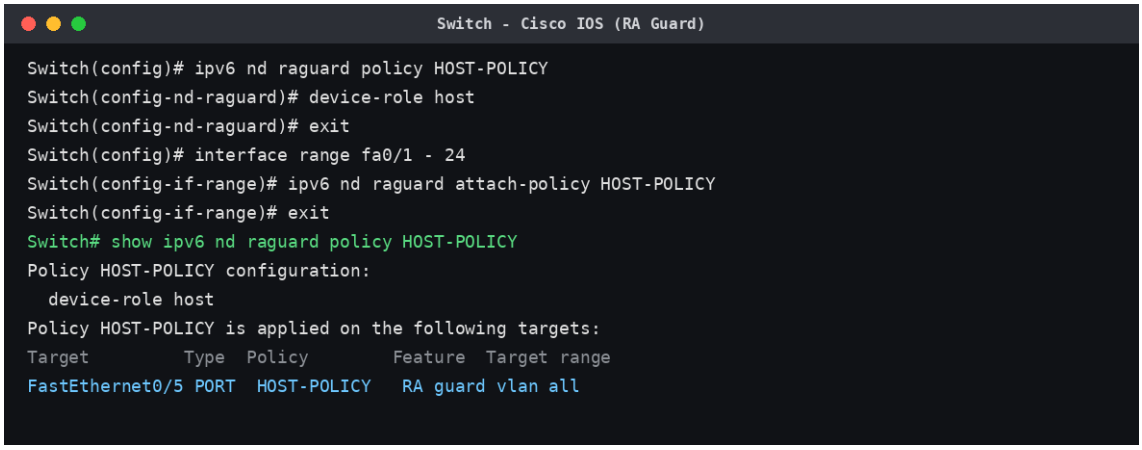
NDP sahteciliği saldırısında tehdit aktörü, ağa sahte Router Advertisement (RA) mesajları göndererek kendisini meşru bir IPv6 yönlendiricisi olarak tanıtabilmektedir; bu durumda yerel ağdaki istemciler varsayılan ağ geçidi bilgilerini saldırganın yayınladığı (genellikle

geçersiz veya saldırgana ait) adresle güncelleyerek tüm IPv6 trafiğini saldırgan üzerinden yönlendirmeye başlamaktadır (Anbar et al., 2016). Benzer şekilde, Neighbor Solicitation (NS) ve Neighbor Advertisement (NA) mesajlarının sahtecilik yoluyla taklit edilmesi, ARP Spoofing'e benzer bir Ortadaki Adam (MitM) saldırısına zemin hazırlamaktadır. fake_router6 ve parasite6 gibi araçlar, bu tür saldırıların otomatik olarak gerçekleştirilmesine imkân tanımaktadır. Söz konusu zafiyet, IPv6'nın IPv4'ün yerini almasıyla giderek artan bir önem kazanmaktadır (Mönnich et al., 2021).

Şekil 2.17. Kali Linux üzerinde sahte Router Advertisement (RA) yayını ile varsayılan ağ geçidinin ele geçirilmesi

2.8.3. Güvenlik Çözümü: RA Guard ve DHCPv6 Snooping

IPv6 NDP tabanlı saldırılara karşı geliştirilen temel Cisco IOS güvenlik mekanizması, RFC 6105 ile standartlaştırılan Router Advertisement Guard (RA Guard) özelliğidir. RA Guard, anahtar portlarını host (güvenilmez) veya router (güvenilir) rolleri ile sınıflandırarak, yalnızca yetkili portlardan gelen RA mesajlarının ağa iletilmesine izin vermekte ve host rolündeki portlardan gelen RA mesajlarını doğrudan düşürmektedir (Mönnich et al., 2021). ARP için DHCP Snooping ve Dynamic ARP Inspection ne ifade ediyorsa, IPv6 ortamında da DHCPv6 Guard ve IPv6 Snooping/ND Inspection benzer bir işlevi üstlenmekte; bağlama tablosu (binding table) üzerinden meşru IPv6-MAC eşleşmelerinin doğrulanmasını sağlamaktadır.



Şekil 2.18. Cisco IOS üzerinde IPv6 RA Guard politikasının tanımlanması ve arayüze uygulanması

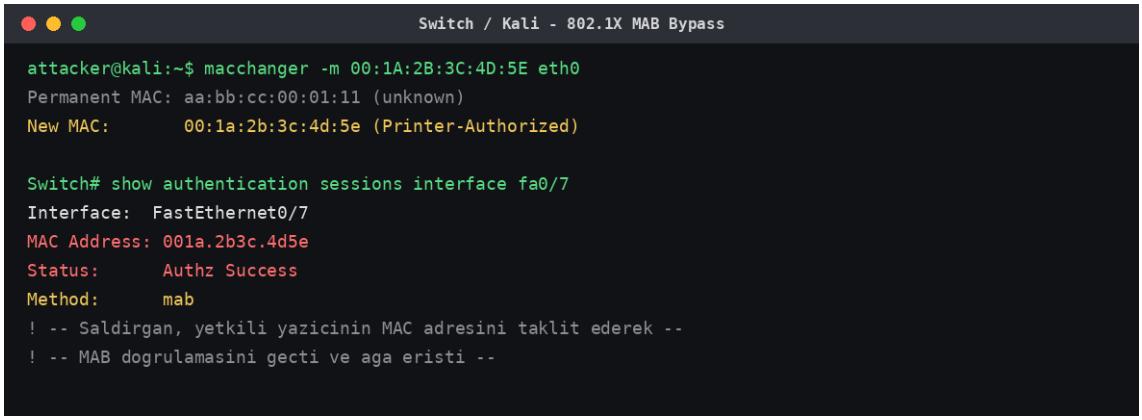
2.9. IEEE 802.1X / MAC Authentication Bypass (MAB) Atlatma Saldırısı

2.9.1. Port Tabanlı Erişim Kontrolünün Çalışma Mantığı

IEEE 802.1X standardı, bir LAN portuna bağlanan cihazların ağa erişebilmesi için kimlik doğrulamadan geçmesini zorunlu kılan port tabanlı bir ağ erişim kontrolü (Port-Based Network Access Control) çerçevesi tanımlamaktadır (IEEE, 2020). Bu mimaride istemci (supplicant), anahtar (authenticator) ve bir RADIUS sunucusu (authentication server) arasında EAP/EAPOL protokolü üzerinden kimlik doğrulama gerçekleştirilmektedir. Yazıcı, IP kamera veya IoT sensörü gibi 802.1X istemci yazılımını (supplicant) desteklemeyen cihazların ağa dahil edilebilmesi için Cisco anahtarlarında MAC Authentication Bypass (MAB) adı verilen alternatif bir mekanizma sunulmaktadır; bu yöntemde cihazın kimliği, kullanıcı adı/parola yerine yalnızca kaynak MAC adresine bakılarak RADIUS sunucusundaki yetkili liste üzerinden doğrulanmaktadır.

2.9.2. Saldırının Mekanizması: MAC Adresi Sahteciliği ile MAB Atlatma

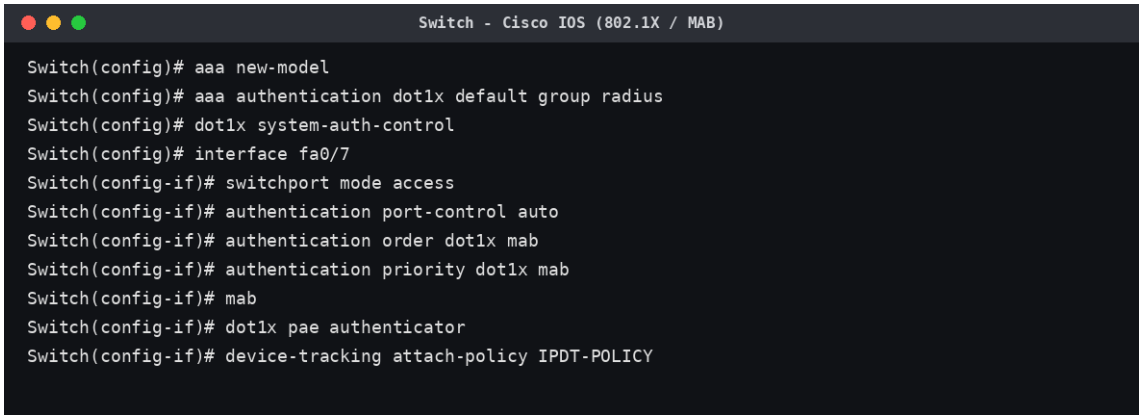
MAB, tasarımı gereği MAC adreslerinin değiştirilemez ve güvenilir bir kimlik bilgisi olduğu varsayımına dayanmaktadır; ancak MAC adresleri yazılımsal olarak kolaylıkla değiştirilebilmektedir. Saldırgan, ağı pasif biçimde dinleyerek yetkili bir cihazın (örneğin ağ yazıcısının) MAC adresini tespit ettikten sonra kendi ağ arabirimini macchanger gibi bir araçla bu adresi taklit edecek şekilde yeniden yapılandırabilmekte ve böylece RADIUS sunucusundaki yetkili MAC listesini atlatarak ağa yetkisiz erişim sağlayabilmektedir. Bu saldırı, MAB'nin yalnızca cihaz kimliğini doğruladığı, kullanıcı kimliğini doğrulamadığı için sınırlı bir güvence sunduğunu ortaya koymaktadır.



Şekil 2.19. Kali Linux üzerinde MAC adresi sahteciliği ile MAC Authentication Bypass (MAB) atlatma denemesi

2.9.3. Güvenlik Çözümü: 802.1X Önceliklendirme ve Cihaz İzleme

MAB atlatma riskinin azaltılmasında temel strateji, mümkün olduğunca 802.1X kimlik doğrulamasının MAB'ye tercih edilmesi ve yalnızca 802.1X'i desteklemeyen cihazlarda MAB'nin yedek (fallback) yöntem olarak kullanılmasıdır; bu, authentication order dot1x mab ve authentication priority dot1x mab komutlarıyla yapılandırılmaktadır. Ayrıca cihaz izleme (IP Device Tracking) özelliğinin etkinleştirilmesi, MAC-IP eşleşmelerinin sürekli izlenmesini sağlayarak anormal davranışların (örneğin aynı MAC adresinin farklı portlarda art arda görünmesi) tespit edilmesine katkı sunmaktadır. RADIUS sunucusu üzerinde MAB için ayrı ve kısıtlı yetkilere sahip dinamik VLAN/ACL atamalarının yapılması da olası bir MAB atlatma durumunda saldırganın erişimini sınırlandırmaktadır.



Şekil 2.20. Cisco IOS üzerinde 802.1X ve MAB öncelik sıralı port tabanlı erişim kontrolü yapılandırması

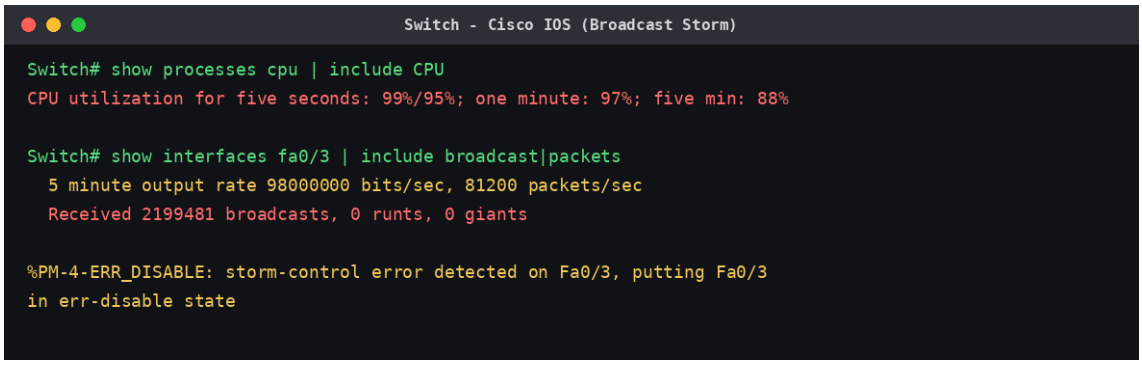
2.10. Yayın (Broadcast) Fırtınası Saldırısı ve Storm Control

2.10.1. Yayın Fırtınasının Oluşma Mekanizması

Bir yayın (broadcast) çerçevesinin, Ethernet çerçevelerinde bulunmayan bir yaşam süresi (Time-To-Live) alanı nedeniyle döngülü bir Layer 2 topolojide sınırsız biçimde çoğalarak ağdaki tüm kullanılabilir bant genişliğini tüketmesi durumuna yayın fırtınası (broadcast storm) adı verilmektedir. STP'nin devre dışı bırakıldığı, yanlış yapılandırıldığı veya çok satıcılı (multi-vendor) ortamlarda uyumsuzluk yaşandığı durumlarda fiziksel döngüler oluşabilmekte ve bu döngüler hızla bir yayın fırtınasına dönüşebilmektedir (Nair, Shubhamangala & Vaidehi, 2011).

2.10.2. (DoS)

DoS yalnızca kablolama hataları veya yanlış yapılandırmalardan değil, kasıtlı saldırılardan da kaynaklanabilmektedir. Saldırgan, ağa yüksek hacimli sahte ARP istekleri, yayın adresine yönlendirilmiş ICMP Echo istekleri (Smurf saldırısı) veya bilinçli olarak oluşturulmuş bir Layer 2 döngüsü göndererek anahtarların CPU ve bant genişliği kapasitesini tüketebilmekte; bu durum bir Hizmet Reddi (DoS) saldırısına dönüşmektedir (Nair, Shubhamangala & Vaidehi, 2011). Bu tür saldırılar genellikle anahtar CPU kullanımında ani bir yükselme ve ilgili arayüzlerde anormal yayın paketi oranlarıyla kendini göstermektedir.

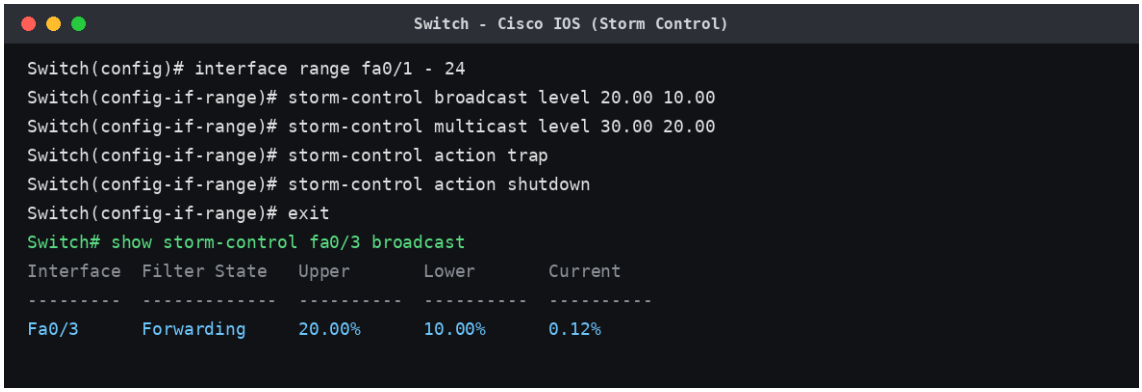


Şekil 2.21. Yayın fırtınası sırasında anahtar CPU kullanımının %99'a yükselmesi ve arayüz hata durumuna geçişi

2.10.3. Güvenlik Çözümü: Storm Control Yapılandırması

Cisco IOS'ta yayın fırtınalarına karşı temel savunma mekanizması Storm Control özelliğidir. Bu özellik, bir arayüzde belirli bir zaman aralığında alınan yayın, çoklu yayın (multicast) veya bilinmeyen tekli yayın (unknown unicast) trafiğinin bağlantı bant genişliğine oranını sürekli izleyerek, bu oran önceden tanımlanmış bir eşik (rising threshold) değerini aştığında ilgili trafiği sınırlandırmakta veya tamamen düşürmektedir. Eşik aşıldığında alınacak aksiyon (trap, shutdown) ayrıca yapılandırılabilmekte; shutdown seçeneği, portu otomatik

olarak err-disabled duruma getirerek olası bir saldırının ya da döngünün etkisini izole etmektedir. Storm Control, STP gibi topolojik döngü önleme mekanizmalarının tamamlayıcısı olup, kasıtlı trafik tabanlı DoS saldırılarına karşı ek bir savunma katmanı sunmaktadır.



Şekil 2.22. Cisco IOS üzerinde Storm Control (broadcast/multicast) eşik değerleri ve ihlal aksiyonu yapılandırması

2.11. Cisco Çapında Bütünsel Layer 2 Güvenlik Mimarisi (Defense-in-Depth)

Önceki alt bölümlerde ayrı ayrı ele alınan saldırı türleri ve karşı önlemler incelendiğinde, veri bağlantı katmanı güvenliğinin tek bir özellik veya komutla sağlanamayacağı, aksine birbirini tamamlayan birden fazla Cisco IOS mekanizmasının katmanlı biçimde (defense-in-depth) bir arada uygulanması gerektiği görülmektedir (Seifert & Edwards, 2008; Gao et al., 2020). Tablo 2.1, bu çalışma kapsamında incelenen dokuz Layer 2 saldırı türünü, sömürdükleri temel protokol zafiyetini ve önerilen Cisco IOS güvenlik çözümünü özetlemektedir.

Saldırı Türü	**Sömürülen Zafiyet**	**Cisco IOS Güvenlik Çözümü**
MAC Flooding	CAM tablosunun sınırlı kapasitesi	Port Security (maksimum MAC sınırı + violation shutdown)
DHCP Starvation / Spoofing	DHCP'de kimlik doğrulama eksikliği	DHCP Snooping (trusted port + rate-limit)
ARP Spoofing	ARP'de kimlik doğrulama eksikliği (Gratuitous ARP)	Dynamic ARP Inspection (DAI)

VLAN Hopping	DTP otomatik trunk müzakeresi, double tagging	DTP devre dışı, native VLAN izolasyonu
STP Manipülasyonu	BPDU'da kimlik doğrulama eksikliği	BPDU Guard ve Root Guard
VTP Saldırısı	VTP revizyon numarası kontrolünün parolasız işlemesi	VTP Password, Transparent mod, VTP v3
CDP/LLDP Keşfi	Kimlik doğrulamasız cihaz bilgisi yayını	no cdp run / no lldp run, port bazlı devre dışı bırakma
IPv6 NDP Sahteciliği	NDP'de kimlik doğrulama eksikliği (rogue RA)	RA Guard, DHCPv6 Guard
802.1X / MAB Atlatma	MAC adresinin sahtecilik yoluyla taklit edilebilmesi	802.1X > MAB önceliklendirme, IP Device Tracking
Broadcast Fırtınası	Ethernet çerçevesinde TTL bulunmaması	Storm Control (rising/falling threshold + err-disable)

Tablo 2.1 de özetlenen önlemlerin tek başına yeterli olmadığı, bunların birbirini tamamlayan bir bütün olarak ele alınması gerektiği vurgulanmalıdır. Örneğin DAI'nin etkin biçimde çalışabilmesi DHCP Snooping bağlama tablosuna; RA Guard'ın IPv6 ortamındaki etkinliği ise benzer biçimde port güven sınıflandırmasına bağımlıdır. Bu nedenle Cisco, erişim katmanı anahtarlarında aşağıdaki temel yapılandırma ilkelerinin bir bütün hâlinde, ağ genelinde tutarlı bir politika olarak uygulanmasını önermektedir (Cisco Systems, 2012; Bhardwaj et al., 2021):

- Kullanılmayan tüm portların access modunda ve shutdown durumunda tutulması; native VLAN'ın kullanıcı trafiği taşımayan ayrı bir VLAN'a atanması.
- Port Security, DHCP Snooping ve Dynamic ARP Inspection üçlüsünün birlikte ve aynı VLAN'larda etkinleştirilmesi.
- BPDU Guard ve Root Guard'ın tüm erişim katmanı portlarında varsayılan olarak etkinleştirilmesi.

- VTP'nin parola korumalı veya gereksiz olduğu durumlarda Transparent/Off modda çalıştırılması.
- CDP/LLDP'nin yalnızca gerçekten ihtiyaç duyulan portlarda (örneğin IP telefon bağlantıları) etkin bırakılması.
- Mümkün olan tüm uç noktalarda 802.1X kimlik doğrulamasının, desteklenmeyen cihazlarda ise sıkı izlenen MAB'nin kullanılması.
- IPv6 dağıtımı yapılan ağlarda RA Guard ve DHCPv6 Guard'ın IPv4 eşdeğerleriyle birlikte standart yapılandırmaya dahil edilmesi.
- Tüm erişim portlarında Storm Control eşiklerinin tanımlanarak hem kazara döngülere hem de kasıtlı DoS saldırılarına karşı bir güvenlik ağı oluşturulması.

Sonuç olarak, Layer 2 güvenliği; tek bir komutla değil, yukarıda sıralanan mekanizmaların ağ mimarisinin tasarım aşamasından itibaren bütünleşik bir güvenlik politikası çerçevesinde uygulanmasıyla sağlanabilmektedir. Bu yaklaşım, hem bilinen saldırı türlerine karşı doğrudan koruma sağlamakta hem de üst katman güvenlik mekanizmalarının (TLS, IPSec vb.) işlevselliğini koruyan sağlam bir temel oluşturmaktadır (Tanenbaum & Wetherall, 2011).

BÖLÜM III
YÖNTEM

3.1. Araştırmanın Modeli

Bu çalışma, nitel araştırma yaklaşımlarından doküman analizi ile teknik bir uygulama/durum çalışmasının (case study) bir arada kullanıldığı karma bir desende yürütülmüştür. Çalışmanın ilk aşamasında, Layer 2 saldırı türleri ve güvenlik çözümlerine ilişkin akademik literatür sistematik biçimde taranarak betimsel bir doküman analizi gerçekleştirilmiştir. İkinci aşamada ise literatürde tanımlanan saldırı senaryoları, GNS3 ve Cisco Packet Tracer simülasyon ortamlarında Cisco IOS anahtarlar ve Kali Linux saldırgan makinesi kullanılarak uygulamalı biçimde yeniden üretilmiş ve önerilen karşı önlemlerin etkinliği gözlemsel olarak test edilmiştir. Bu bakımdan araştırma modeli, betimsel doküman analizi ile deneysel/uygulamalı simülasyon yönteminin birleştirildiği bir teknik durum çalışması niteliği taşımaktadır.

3.2. Evren ve Örneklem

Araştırmanın evrenini, veri bağlantı katmanı (Layer 2) güvenliği konusunda yayımlanmış ulusal ve uluslararası akademik makaleler, konferans bildirileri, standart dokümanları (RFC, IEEE) ve Cisco teknik dokümantasyonu oluşturmaktadır. Örneklem, amaçlı örnekleme (purposive sampling) yöntemiyle belirlenmiş olup; Google Scholar, IEEE Xplore, ScienceDirect, SpringerLink ve ACM Digital Library veritabanlarında 'Layer 2 attacks', 'ARP spoofing', 'VLAN hopping', 'DHCP snooping', 'STP security', 'VTP attack', 'IPv6 neighbor discovery security' gibi anahtar kelimelerle yapılan taramalar sonucunda erişilen, konuyla doğrudan ilişkili ve hakemli yayınlardan oluşmaktadır. Simülasyon boyutunda örneklem, çalışmanın kapsamı dahilinde belirlenen dokuz Layer 2 saldırı senaryosu (MAC Flooding, DHCP Starvation/Spoofing, ARP Spoofing, VLAN Hopping, STP Manipülasyonu, VTP saldırısı, CDP/LLDP keşfi, IPv6 NDP sahteciliği, 802.1X/MAB atlatma) ile sınırlandırılmıştır.

3.3. Veri Toplama Araçları

Çalışmada iki tür veri toplama aracı kullanılmıştır. Birincisi, literatür taramasında kullanılan akademik veritabanları ve arama motorlarıdır (Google Scholar, IEEE Xplore, ScienceDirect,

ResearchGate,Cisco Official Documents). İkincisi ise simülasyon ortamında saldırı ve savunma senaryolarının uygulanmasında kullanılan yazılım ve donanım araçlarıdır. Ağ simülasyonu için GNS3 ve Cisco Packet Tracer; saldırı senaryolarının üretilmesi için Kali Linux işletim sistemi üzerinde çalışan macof (MAC Flooding), ettercap ve arpspoof (ARP Spoofing), Yersinia (STP/VTP/DTP saldırıları), fake_router6 ve parasite6 (IPv6 NDP saldırıları) ile macchanger (MAC adresi sahteciliği) araçları kullanılmıştır. Trafik analizi ve protokol doğrulaması için Wireshark paket analiz aracından yararlanılmış; Cisco tarafındaki yapılandırma ve doğrulama işlemleri için Cisco IOS komut satırı arayüzü (CLI) kullanılmıştır.

3.4. Verilerin Toplanması

Veri toplama süreci iki paralel aşamada yürütülmüştür. Doküman analizi aşamasında, belirlenen anahtar kelimelerle taranan yayınlar; saldırı mekanizması, etki alanı ve önerilen çözüm bakımından sınıflandırılarak bir kaynak matrisi oluşturulmuştur. Simülasyon aşamasında ise her bir saldırı türü için ayrı bir GNS3/Packet Tracer topolojisi kurulmuş; saldırı öncesi durum (örneğin CAM tablosu, ARP tablosu, VLAN veritabanı, VTP revizyon numarası) kayıt altına alınmış, ardından ilgili saldırı senaryosu Kali Linux üzerinden çalıştırılarak saldırı sonrası durum gözlemlenmiş ve son olarak önerilen Cisco IOS güvenlik önlemi uygulanarak savunma sonrası durum yeniden kayıt altına alınmıştır. Bu üç aşamalı (öncesi/saldırı/sonrası) kayıt yöntemi, her saldırı-çözüm çifti için tutarlı bir karşılaştırma zemini sağlamıştır.

3.5. Verilerin Analizi

Doküman analizinden elde edilen veriler, betimsel içerik analizi yöntemiyle değerlendirilmiş; literatürde tekrarlayan saldırı mekanizmaları ve önerilen çözümler arasındaki ortak temalar belirlenerek Bölüm II'deki kavramsal çerçevenin oluşturulmasında kullanılmıştır. Simülasyon verileri ise karşılaştırmalı (before-after) analiz yöntemiyle değerlendirilmiştir; her saldırı senaryosunda, güvenlik önlemi uygulanmadan önceki ve sonraki sistem durumları (CAM/ARP tablosu içeriği, VLAN veritabanı bütünlüğü, kimlik doğrulama sonucu, CPU kullanımı vb.) karşılaştırılarak ilgili Cisco IOS mekanizmasının saldırıyı engelleme etkinliği değerlendirilmiştir. Elde edilen bulgular Bölüm IV'te araştırma soruları temelinde sunulmuştur.

BÖLÜM IV
BULGULAR VE YORUM

4.1. Birinci araştırma sorusuna(alt problem) ilişkin bulgular.

Araştırmanın birinci alt problemi, Layer 2 düzeyinde gerçekleştirilen başlıca saldırı türlerinin teknik çalışma mekanizmalarının neler olduğudur. Bölüm II'de ayrıntılı biçimde incelenen dokuz saldırı türü (MAC Flooding, DHCP Starvation/Spoofing, ARP Spoofing, VLAN Hopping, STP Manipülasyonu, VTP saldırısı, CDP/LLDP keşfi, IPv6 NDP sahteciliği ve 802.1X/MAB atlatma) incelendiğinde, bu saldırıların ortak paydasının veri bağlantı katmanı protokollerinin (ARP, DHCP, STP, VTP, CDP/LLDP, NDP) tasarımlarında kimlik doğrulama mekanizmalarının bulunmaması olduğu görülmüştür (Bhardwaj et al., 2021; Hijazi et al., 2019). Simülasyon ortamında elde edilen bulgular, bu protokollerin varsayılan yapılandırmalarının saldırılara karşı savunmasız olduğunu; örneğin yalnızca birkaç saniye içinde macof aracıyla CAM tablosunun doldurulabildiğini veya Yersinia ile gönderilen tek bir sahte BPDU mesajının ağın kök köprüsünü değiştirebildiğini doğrulamaktadır.

4.2. İkinci araştırma sorusuna(alt problem) ilişkin bulgular.

Araştırmanın ikinci alt problemi, bu saldırılara karşı geliştirilen Cisco IOS güvenlik çözümlerinin etkinliğinin ne olduğudur. Simülasyon bulguları, incelenen tüm güvenlik mekanizmalarının (Port Security, DHCP Snooping, Dynamic ARP Inspection, BPDU Guard/Root Guard, VTP Password, CDP/LLDP devre dışı bırakma, RA Guard, 802.1X/MAB önceliklendirme ve Storm Control) ilgili saldırı senaryosunu başarıyla engellediğini veya etkisini önemli ölçüde sınırlandırdığını göstermektedir. Öte yandan bulgular, bu çözümlerin birbirinden bağımsız değil, karşılıklı bağımlı (interdependent) olduğunu da ortaya koymaktadır; örneğin Dynamic ARP Inspection'ın doğru çalışabilmesi DHCP Snooping bağlama tablosunun önceden oluşturulmuş olmasına bağlıdır. Bu bulgu, Bölüm 2.11'de sunulan bütünsel savunma derinliği (defense-in-depth) yaklaşımının gerekliliğini doğrulamaktadır (Seifert & Edwards, 2008).

4.3. Üçüncü araştırma sorusuna (alt problem) ilişkin bulgular.

Araştırmanın üçüncü alt problemi, GNS3/Cisco Packet Tracer simülasyon ortamında gerçekleştirilen uygulamalı senaryoların bulgularının neler olduğudur. Şekil 2.1-2.22 arasında sunulan ekran görüntüleri ve komut çıktıları, her bir saldırı-çözüm çiftinin öncesi/sonrası karşılaştırmasını somut biçimde belgelemektedir. Örneğin Şekil 2.4 ve 2.5'te MAC Flooding saldırısı sonucunda CAM tablosunun saldırgan tarafından üretilen sahte adreslerle dolduğu; Şekil 2.13'te ise VTP saldırısı sonucunda VLAN veritabanının tamamen silindiği gösterilmektedir. Buna karşılık, ilgili güvenlik önleminin (Port Security, VTP Password vb.) uygulanmasının ardından aynı saldırı senaryoları tekrarlandığında, saldırının ya tamamen engellendiği ya da ilgili portun otomatik olarak err-disabled duruma getirilerek izole edildiği gözlemlenmiştir. Bu sonuçlar, literatürde raporlanan bulgularla (Gajo, 2025; Morsy & Nashat, 2022; Abbasi Rad, 2024) tutarlılık göstermektedir.

BÖLÜM V
SONUÇ, TARTIŞMA VE ÖNERİLER

5.1. Sonuç

Bu çalışmada, OSI referans modelinin ikinci katmanında (Layer 2) gerçekleştirilen dokuz farklı saldırı türü; çalışma mekanizmaları, ağ üzerindeki etkileri ve Cisco IOS tabanlı güvenlik çözümleri bakımından kapsamlı biçimde incelenmiştir. Elde edilen bulgular, veri bağlantı katmanı protokollerinin (ARP, DHCP, STP, VTP, CDP/LLDP, NDP) tasarım aşamasında kimlik doğrulamadan ziyade işlevsellik ve performans odaklı geliştirildiğini ve bu durumun ciddi güvenlik açıklarına yol açtığını doğrulamaktadır. GNS3 ve Cisco Packet Tracer ortamlarında gerçekleştirilen simülasyonlar, incelenen tüm Cisco IOS güvenlik mekanizmalarının (Port Security, DHCP Snooping, Dynamic ARP Inspection, BPDU Guard/Root Guard, VTP Password, CDP/LLDP devre dışı bırakma, RA Guard, 802.1X/MAB ve Storm Control) ilgili saldırıyı etkili biçimde engellediğini göstermiştir.

5.2. Tartışma

Çalışmanın bulguları, literatürdeki mevcut çalışmalarla büyük ölçüde örtüşmektedir; Bhardwaj ve diğerleri (2021) ile Gajo (2025) tarafından da vurgulandığı gibi, Layer 2 saldırılarının üst katman güvenlik mekanizmalarını (SSL/TLS, IPSec) etkisiz hâle getirebilme potansiyeli, bu katmanın bütünsel ağ güvenliği stratejilerinde merkezi bir yer tutması gerektiğini ortaya koymaktadır. Bununla birlikte, bu çalışmanın sınırlılıkları bölümünde (1.5) belirtildiği üzere bulgular yalnızca simüle edilmiş kablolu Ethernet ortamlarına dayanmaktadır; gerçek üretim ağlarında donanım performansı, çok satıcılı (multi-vendor) ortam etkileşimleri ve trafik yoğunluğu gibi etkenlerin güvenlik mekanizmalarının performansını farklılaştırabileceği göz önünde bulundurulmalıdır. Ayrıca incelenen çözümlerin etkinliğinin, doğru ve tutarlı bir yapılandırma politikasının uygulanmasına sıkı sıkıya bağlı olduğu; tek bir yanlış yapılandırmanın (örneğin native VLAN'ın değiştirilmemesi) dahi savunma zincirinde zayıf bir halka oluşturabileceği tartışılmalıdır.

5.3. Öneriler

Bu çalışmanın bulguları doğrultusunda ağ yöneticilerine ve gelecekteki araştırmacılara yönelik şu öneriler sunulmaktadır: (1) Kurumsal ağlarda erişim katmanı anahtarlarında Bölüm 2.11'de özetlenen Cisco IOS güvenlik mekanizmalarının tamamının, birbirini tamamlayan bütünsel bir politika çerçevesinde standart yapılandırmaya dahil edilmesi önerilmektedir. (2) Ağ yöneticilerinin, yeni nesil tehdit vektörlerine (özellikle IPv6'nın yaygınlaşmasıyla artan NDP tabanlı saldırılara) karşı düzenli farkındalık eğitimi alması önerilmektedir. (3) Gelecekteki çalışmalarda, bu araştırmada simülasyon ortamında değerlendirilen senaryoların gerçek donanım üzerinde ve farklı satıcı (vendor) ortamlarında tekrarlanması; ayrıca makine öğrenmesi tabanlı anomali tespit sistemlerinin Layer 2 saldırı tespitindeki etkinliğinin araştırılması önerilmektedir. (4) Kablosuz ağlara özgü Layer 2 saldırılarının (örneğin sahte erişim noktası saldırıları) bu çalışmanın kapsamı dışında bırakıldığı göz önünde bulundurularak, ileride yapılacak çalışmaların bu alanı da kapsayacak şekilde genişletilmesi önerilmektedir.

KAYNAKÇA

Alcaraz, C. (2017). Switch port security mechanisms in Cisco networks: Configuration and performance evaluation. International Journal of Technology Management & Humanities (IJTMH), 3(1), 9–16.

Gajo, S. I. (2025). Mitigating MAC flooding attacks using port security techniques. Proceedings of the Nigerian Society of Physical Sciences, 2, 162. https://doi.org/10.61298/pnspsc.2025.2.162

Bhardwaj, J., Yadav, V. K., Trivedi, M. C., & Sen, A. K. (2021). ARP cache poisoning: Detection, mitigation and prevention schemes. *International Journal of Computational Vision and Robotics*, 11(4), 357–373.

Bora, G., Bora, S., Singh, S., & Arsalan, S. M. (2014). OSI reference model: An overview. *International Journal of Computer Trends and Technology*, 7(4), 214–218.

Forouzan, B. A. (2013). *Data communications and networking* (5th ed.). McGraw-Hill.

Nam, S. Y., Jurayev, S., Kim, S.-S., & Choi, G. S. (2012). Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN. *EURASIP Journal on Wireless Communications and Networking*, 2012(1), 89.

Seifert, R., & Edwards, J. (2008). *The all-new switch book: The complete guide to LAN switching technology* (2nd ed.). Wiley.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.

Yavuzer Aslan, F., & Aslan, B. (2023). Comparison of IoT protocols with OSI and TCP/IP architecture. *International Journal of Engineering Research and Development*, 15(1), 333–343. https://doi.org/10.29137/umagd.1063036

Droms, R. (1997). Dynamic Host Configuration Protocol. *RFC 2131*.

Tripathi, N., & Hubballi, N. (2018). Exploiting DHCP vulnerabilities in network security. *Journal of Network and Computer Applications*, 120, 1–14.

Griffin, T., & Schneider, F. B. (2007). A framework for analyzing network security protocols. *IEEE Symposium on Security and Privacy*.

Mishra, P., & Singh, V. (2012). Detection and prevention of DHCP starvation attack in network. *International Journal of Computer Applications*, 41(21), 1–5.

Cisco Systems. (2012). DHCP snooping configuration guide. Cisco Press.

Hijazi, A., Zaiter, M., & Rawashdeh, M. (2019). Address resolution protocol spoofing attacks and security approaches: A survey. *Security and Privacy*, *2*(1), e49. https://doi.org/10.1002/spy2.49

Morsy, S. M., & Nashat, D. (2022). D-ARP: An efficient scheme to detect and prevent ARP spoofing. *IEEE Access*, *10*, 49142–49153. https://doi.org/10.1109/ACCESS.2022.3173006

Neminath, H., & Tripathi, N. (2016). A closer look into DHCP starvation attack in wireless networks. *Computers & Security*, *65*, 115–128. https://doi.org/10.1016/j.cose.2016.09.008

Gao, N., Zhao, L., & Yin, J. (2020). Network security issues of data link layer: An overview. In *Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1–6). IEEE. https://doi.org/10.1109/iCoMET48670.2020.9073825

Sweeney, B. (2006). Understanding and preventing attacks at layer 2 of the OSI reference model. In *Proceedings of the IEEE WESCANEX 2006* (pp. 1–6). IEEE. https://doi.org/10.1109/WESCANEX.2006.1628088

Abbasi Rad, M. (2024). Examining the VTP protocol, identifying the risks of its use and providing risk reduction solutions in the computer networks of offices and large organizations. International Journal of Modern Achievement in Science, Engineering and Technology (IJSET), 1(4), 113–123. https://doi.org/10.63053/ijset.52

Barbhuiya, F. A., Bansal, G., Kumar, N., Biswas, S., & Nandi, S. (2013). Detection of neighbor discovery protocol based attacks in IPv6 network. Networking Science, 2(3–4), 91–113. https://doi.org/10.1007/s13119-013-0018-2

Anbar, M., Abdullah, R., Saad, R. M. A., Alomari, E., & Alsaleem, S. (2016). Review of security vulnerabilities in the IPv6 neighbor discovery protocol. In Information

Science and Applications (ICISA) 2016 (Lecture Notes in Electrical Engineering, Vol. 376, pp. 603–612). Springer. https://doi.org/10.1007/978-981-10-0557-2_59

Mönnich, M., Sertbaş Bülbül, N., Ergenç, D., & Fischer, M. (2021). Mitigation of IPv6 router spoofing attacks with P4. In Proceedings of the Symposium on Architectures for Networking and Communications Systems (ANCS '21) (pp. 1–7). ACM. https://doi.org/10.1145/3493425.3502765

Nair, T. R. G., Shubhamangala, B. R., & Vaidehi, M. (2011). A novel agent based approach for controlling network storms. arXiv preprint arXiv:1107.1954.

IEEE. (2020). IEEE standard for local and metropolitan area networks—Port-based network access control (IEEE Std 802.1X-2020). IEEE. https://doi.org/10.1109/IEEESTD.2020.9018454

Memon, M. (2015). *The OSI Model: Overview on the Seven Layers*. International Journal of Computer Science and Information Technology Research, 3(2), 461–466.

Jha, A., & Bhardwaj, A. (2014). *OSI Reference Model: An Overview*. International Journal of Computer Trends and Technology, 7(1), 1–4.

Siddiqui, R. A. (2014). *Bring your own device (BYOD) in higher education: Opportunities and challenges*. International Journal of Emerging Trends & Technology in Computer Science, 3(1), 233–236.

Kumar, S., & Singh, R. (2022). *The DHCP snooping and DHCP alert method for network security*. International Journal of Computer Applications.

Whalen, S. (2001). *An introduction to ARP spoofing*. 2600: The Hacker Quarterly

Sütçü, C. S. (1994). *Bilgisayar ve bilgisayar adları*. Marmara İletişim Dergisi, 5, 145–156.

Demirkol, Ö. E., & Demirkol, A. (t.y.). *Dijkstra ve Bellman-Ford en kısa yol algoritmalarının karşılaştırılması*.