2025 Yılı İçin ARP Spoofing Saldırılarının Tespiti ve Otomatik Analizinde En Son ve En Etkili Teknikler ve Trendler

1. Giriş: ARP Spoofing Tehdidi ve Otomatik Tespitin Önemi

Adres Çözümleme Protokolü (ARP) zehirlenmesi olarak da bilinen ARP spoofing saldırıları, yerel alan ağlarında (LAN) ciddi güvenlik riskleri oluşturan siber saldırılardır. Bu saldırılar, ağ iletişiminin temel bir bileşeni olan Adres Çözümleme Protokolü'nün (ARP) doğasında bulunan güvenlik zafiyetlerinden faydalanır. ARP, bir ağdaki cihazların IP adreslerini fiziksel (MAC) adreslerine dönüştürmesini sağlayan önemli bir protokoldür.[1] Ancak, ARP'nin durum bilgisi olmayan ve kimlik doğrulama mekanizmasından yoksun yapısı, onu kötü niyetli manipülasyonlara karşı savunmasız hale getirir.[2] Bu temel tasarım kusuru, gelişmiş tespit ve önleme çabalarının sürekli olarak geliştirilmesini tetikleyen birincil faktördür. Eğer ARP doğası gereği güvenli olsaydı, bu kadar çok karmaşık savunma tekniğine ihtiyaç duyulmazdı. Bu içsel eksiklik, mevcut ve gelecekteki güvenlik çözümlerinin ARP'nin güvenlik eksikliğini telafi etmesini veya onu daha güvenli alternatiflerle değiştirmesini gerektirmektedir.

Bir ARP spoofing saldırısında, saldırgan ağdaki cihazlara (genellikle hedef cihaz ve ağ geçidi) sahte ARP mesajları göndererek kendi MAC adresini meşru bir IP adresiyle ilişkilendirir.[2] Bu manipülasyon, ağ trafiğinin saldırgan üzerinden yönlendirilmesine neden olur, böylece saldırgan iletişim akışını gizlice dinleyebilir, değiştirebilir veya kesintiye uğratabilir. Bu tür saldırıların ağ üzerindeki etkileri geniş kapsamlı ve yıkıcı olabilir.

ARP Spoofing Saldırılarının Ağ Üzerindeki Etkileri

ARP spoofing, çeşitli siber tehditler için bir başlangıç noktası olarak işlev görebilir:

- **Ortadaki Adam (MITM) Saldırıları:** Saldırgan, iki iletişim kuran cihaz arasına

girerek verileri gizlice dinleyebilir (eavesdropping), değiştirebilir (data modification) veya kötü amaçlı kod enjekte edebilir.[2] Bu durum, oturum kimlik bilgileri, giriş kimlik bilgileri gibi hassas bilgilerin çalınmasına yol açabilir.[7]

- **Hizmet Reddi (DoS) Saldırıları:** Saldırganlar, ağdaki cihazların ARP önbelleklerini sahte ARP yanıtlarıyla aşırı yükleyerek veya trafiği yanlış hedeflere yönlendirerek normal ağ iletişimini kesintiye uğratabilir.[4] Bu durum, üretkenlik kaybına, hizmet kesintilerine ve iş operasyonlarında aksaklıklara neden olabilir.[4]
- **Diğer Yan Etkiler:** ARP spoofing, fikri mülkiyet sızıntısı [10], kötü amaçlı yazılım yayılımı [7], oturum ele geçirme [5] ve finansal riskler gibi ciddi güvenlik sonuçları doğurabilir.

Otomatik Tespitin Önemi ve Proje Bağlamı

ARP spoofing, diğer ağ saldırılarının aksine (örn. trafik artışları) belirgin ağ anormallikleri göstermeyen düşük seviyeli bir saldırı olduğundan, genellikle büyük bir ağ sorununa dönüşene kadar tespit edilemeyebilir.[1] Bu durum, gerçek zamanlı, proaktif ve otomatik tespit sistemlerinin geliştirilmesini zorunlu kılmaktadır. Otomatik sistemler, insan müdahalesini azaltarak daha hızlı ve ölçeklenebilir yanıtlar sağlar.[1]

Saldırganların sürekli olarak daha sofistike hale gelmesi, basit eşik tabanlı tespitleri atlatmak için kötü niyetli trafiği meşru trafikle harmanlaması, proaktif ve adaptif savunma mekanizmalarına olan ihtiyacı artırmaktadır.[9] 2025 yılına yönelik raporlar, "daha sofistike ve hedefe yönelik saldırılar" ve "gelişmiş kaçınma teknikleri" gibi tehditlerin artışına işaret etmektedir.[14] Bu artan sofistikasyon, özellikle yapay zeka ve makine öğrenimi kullanan adaptif ve proaktif savunma mekanizmalarına olan kritik ihtiyacı doğrudan tetiklemektedir.

Bu bağlamda, Wireshark aracı ile ağdaki ARP paketlerini derinlemesine analiz ederek, ARP spoofing saldırılarının ağ trafiğindeki etkilerini gözlemlemeyi amaçlayan bu proje, ağ trafiği analizinde uzmanlaşmayı ve gerçek zamanlı siber saldırıların tespiti için etkin bir yöntem sunmayı hedeflemektedir. Python ve Pyshark kütüphanesi entegrasyonuyla geliştirilecek otomatik analiz betiği, '.pcap' uzantılı ağ kayıt dosyalarını inceleyerek aynı IP adresine birden fazla farklı MAC adresinin atanması gibi kritik anormallikleri tespit edecektir. Bu yaklaşım, saldırıların hızlı ve doğru bir şekilde saptanmasını sağlayarak ağ güvenliğine önemli bir katkı sunmaktadır. Projenin "otomatik tespit" ve "gerçek zamanlı" yetenekleri hedeflemesi, gelişen saldırı kalıplarına karşı adaptif, proaktif

çözümlere olan bu kritik ihtiyaçla mükemmel bir şekilde uyum sağlamaktadır.

2. 2025 Yılı İçin En Son ve En Etkili ARP Spoofing Tespit Teknikleri ve Trendleri

ARP spoofing saldırılarının sürekli evrimi, tespit ve önleme mekanizmalarında yenilikçi yaklaşımları zorunlu kılmaktadır. 2025 yılı ve sonrası için öne çıkan en etkili teknikler ve trendler aşağıda detaylandırılmıştır.

Tablo 1: 2025 Yılı İçin Öne Çıkan ARP Spoofing Tespit Teknikleri ve Trendleri Özeti

Teknik/Trend Başlığı	Temel Mekanizma	Neden Önemli	2025 Potansiyel Etkisi	Ana Kaynak
Makine Öğrenimi (ML) ve Derin Öğrenme (DL) Tabanlı Anomali Tespiti	Ağ trafiğindeki normal ARP davranış kalıplarını öğrenerek anormal IP-MAC eşleşmelerini ve trafik sapmalarını tespit eder.	Statik kuralların kaçırdığı karmaşık ve gizli saldırı desenlerini yakalar, sıfırıncı gün saldırılarına karşı etkilidir.	Büyük ve dinamik ağlarda (IoT, SDN) standart haline gelecek, gerçek zamanlı tespit sağlayacak.	10
Derin Paket İncelemesi (DPI) ve Gerçek Zamanlı Trafik Analizi	ARP paket başlıklarını ve yüklerini derinlemesine inceleyerek anormal desenleri (yanlış IP-MAC, tekrarlayan yanıtlar) gerçek zamanlı olarak tespit eder.	Yüksek doğrulukla hızlı tespit ve müdahale sağlar, ağ hızını minimum düzeyde etkiler.	Ağ kenarında ve kritik ağ geçitlerinde anlık denetim için vazgeçilmez olacak.	19
Dinamik ARP Denetimi (DAI)	Yönetilen anahtarlar	Saldırıları ağa girmeden	Kurumsal ağlarda ve	6

ve Ağ Anahtarı Güvenliği	üzerinde ARP paketlerini güvenilir IP-MAC bağlama veritabanına göre doğrulayarak kötü niyetli paketleri engeller.	proaktif olarak önler, temel bir güvenlik katmanı sağlar.	anahtar tabanlı altyapılarda temel bir güvenlik katmanı olmaya devam edecek.	
Yazılım Tanımlı Ağlar (SDN) Tabanlı Tespit ve Azaltma	Merkezi kontrolörler aracılığıyla ağ trafiğini ve ARP tablolarını küresel olarak izler, ML modelleriyle saldırıları tespit eder ve dinamik olarak ağ yapılandırmaları nı yeniden düzenler.	Büyük ölçekli ve dinamik ağlarda (veri merkezleri, bulut) ARP spoofing'e karşı ölçeklenebilir ve verimli çözümler sunar.	Veri merkezleri ve bulut ortamlarında ARP spoofing'e karşı dayanıklılığı artıracak.	12
Davranışsal Analiz ve Anomali Tespiti	Normal ağ davranışının bir profilini oluşturarak, bu profilden sapmaları (örn. anormal ARP istek/yanıt kalıpları) tespit eder.	Geleneksel imza tabanlı yöntemlerin yetersiz kaldığı yeni veya karmaşık saldırı vektörlerini yakalar.	IoT cihazları ve dinamik bulut ortamları gibi heterojen ağlarda kritik öneme sahip olacak.	15
Kriptografik ARP Kimlik Doğrulaması ve Güvenli Protokoller	ARP paketlerinin gerçekliğini kriptografik anahtarlarla imzalayarak veya IPv6'daki NDP gibi daha güvenli alternatif protokoller kullanarak	ARP protokolünün temel kimlik doğrulama eksikliğini giderir, sıfır yanlış pozitif/negatif olasılığı sunar.	Yüksek güvenlik gerektiren sektörlerde (finans, kritik altyapı) daha sağlam bir savunma sağlayacak.	2

	doğrular.			
Gelişmiş Honeypot'lar ve Tuzak Sistemleri	Temel ağ hizmetlerini taklit ederek saldırganları çeker, yakalanan trafiği analiz ederek spoofing saldırılarını tespit eder ve tehdit istihbaratı toplar.	Maliyet etkin bir güvenlik katmanı sunar, saldırgan davranışlarını öğrenmek ve yeni saldırı vektörlerini keşfetmek için değerli istihbarat sağlar.	Küçük ve orta ölçekli kuruluşlar için erken uyarı ve tehdit istihbaratı kaynağı olacak.	20
XDR (Genişletilmiş Tespit ve Yanıt) Çözümleri	Uç noktalar, ağ, bulut ve e-posta gibi birden fazla güvenlik katmanından tehdit verilerini birleştirerek saldırıları daha geniş bir bağlamda tespit eder ve otomatik yanıt sağlar.	Karmaşık ve çok vektörlü saldırılara karşı kurumsal savunmanın temel taşı olacak, kapsamlı yanıt sağlar.	Kurumsal savunmada merkezi rol oynayacak, ARP spoofing'in büyük saldırı zincirlerinin parçası olduğu senaryolarda hızlı yanıt verecek.	22
SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı) Platformları	Güvenlik araçlarını ve süreçlerini tek bir merkezde birleştirerek olay yanıtını otomatikleştiren ve orkestrasyonunu sağlar.	Güvenlik operasyon merkezlerinin (SOC) verimliliğini artırır, insan müdahalesini azaltır ve yanıt süresini hızlandırır.	Güvenlik operasyonlarında otomasyonu artıracak, tekrarlayan olaylara yanıt süresini önemli ölçüde hızlandıracak.	24
Birleşik Siber Güvenlik Platformları (Unified Security Platforms)	SIEM, NDR, EDR, UEBA ve SOAR gibi birden fazla güvenlik işlevini tek bir mimaride birleştirir.	Güvenlik operasyonlarını basitleştirir, maliyetleri düşürür ve tehditlere karşı yanıt hızını artırır.	Güvenlik operasyonlarında karmaşıklığı azaltacak, entegre görünürlük ve otomasyon sağlayacak.	26

2.1. Makine Öğrenimi (ML) ve Derin Öğrenme (DL) Tabanlı Anomali Tespiti

Makine Öğrenimi (ML) ve Derin Öğrenme (DL) modelleri, ağ trafiğindeki normal ARP davranış kalıplarını öğrenerek, IP-MAC adresi çakışmaları, anormal ARP istek/yanıt oranları veya beklenmedik MAC adresi değişiklikleri gibi sapmaları tespit eder.[3] Bu yöntemler, statik kurallara dayalı sistemlerin kaçırabileceği karmaşık ve gizli saldırı desenlerini yakalamada üstündür. Çeşitli algoritmalar, örneğin Random Forest, Long Short-Term Memory (LSTM) Ağları, Evrişimsel Sinir Ağları (CNN'ler), Destek Vektör Makineleri (SVM) ve Gated Recurrent Unit (GRU), yüksek doğruluk oranlarıyla test edilmiştir.[10] Özellikle Random Forest'ın %94'e varan doğruluk oranına sahip olduğu belirtilirken [10], GRU modelinin simülasyon ortamında %98.94 gibi etkileyici bir doğruluk sergilediği gözlemlenmiştir.[16]

Geleneksel tespit yöntemleri genellikle "yavaş ve ölçeklenebilir değil" [19] ve "yeni saldırı kalıplarına uyum sağlamakta zorlanıyor".[12] Buna karşılık, ML ve DL tabanlı yaklaşımlar, "analiz edilen geçmiş örneklere dayanarak yeni ve mevcut tehditlere uyum sağlama kapasitesine" sahiptir [11] ve "daha önce görülmemiş saldırıları, genellikle sıfırıncı gün saldırılarını" tespit etmek için daha uygundur.[17] Bu durum, imza tabanlı, reaktif tespitten adaptif, proaktif anomali tespitine doğru belirgin bir kaymayı işaret etmektedir. Bu modellerin etkinliği, yüksek doğruluk oranları ile kanıtlanmıştır.

2025'te, ML/DL tabanlı sistemler, özellikle büyük ve dinamik ağlarda, örneğin Nesnelerin İnterneti (IoT) ve Yazılım Tanımlı Ağ (SDN) ortamlarında, ARP spoofing tespitinde standart haline gelecektir.[10] Gerçek zamanlı trafik analizi ve geleneksel yöntemlerle tespit edilemeyen sıfırıncı gün saldırılarının tespiti için kritik öneme sahiptirler. Bu sistemlerin performansı için özellik mühendisliği büyük önem taşır. Protokol başlıklarından (ARP, ICMP, IPv4, IPv6, TCP, UDP, DNS ve HTTP) 128'e kadar özellik çıkarılması [15], ya da uzman görüşleri ve literatüre dayalı olarak seçilen ve PCA aracılığıyla optimize edilen 6 özellik dahil 12 özellikli gerçek zamanlı veri kümelerinin kullanılması [12], model doğruluğu için kritik faktörlerdir. Chi-kare gibi istatistiksel yöntemlerle en iyi özelliklerin seçilmesi, yüksek performans elde etmek için önemlidir.[18] Yanlış özellik seçimi "yüksek hata değerlerine" yol açabilir.[11]

2.2. Derin Paket İncelemesi (DPI) ve Gerçek Zamanlı Trafik Analizi

Derin Paket İncelemesi (DPI), ağ paketlerinin başlıklarını ve yüklerini derinlemesine inceleyerek anormal ARP desenlerini, yanlış IP-MAC eşleşmelerini veya tekrarlayan ARP yanıtlarını tespit eden güçlü bir tekniktir.[19] Bettercap gibi araçlarla entegre edildiğinde, gerçek zamanlı izleme ve hızlı müdahale sağlayarak ağ trafiğindeki olağandışı aktiviteyi dikkatlice kontrol eder.[19] Bettercap, ARP trafiğini gerçek zamanlı olarak izlerken, DPI modülü paketleri ayrıntılı olarak inceler, IP-MAC eşleşmelerindeki tutarsızlıkları veya tek bir IP adresinden gelen birden fazla ARP yanıtı gibi şüpheli aktiviteleri arar.[19]

Bu yaklaşımın temel faydası, gelişmiş gerçek zamanlı tespit için araçların sinerjisidir. Bettercap ve DPI'ın birleştirilmesi, ağ hızını yavaşlatmadan gerçek zamanlı tespit sunarak daha iyi bir denge sağlar.[19] Bettercap gerçek zamanlı yakalama ve izlemeyi yönetirken, DPI ayrıntılı incelemeyi sağlar. Bu iş bölümü, hem verimlilik hem de analiz derinliği sağlar. Bu sinerjinin etkinliği, %98'lik bir tespit doğruluğu ve 0.5 saniyelik düşük bir yanıt süresi ile kanıtlanmıştır.[19]

2025'te, DPI, özellikle Bettercap gibi araçlarla birleşerek, ağ kenarında (edge) ve kritik ağ geçitlerinde ARP trafiğini anlık olarak denetlemek için vazgeçilmez olacaktır.[19] Bu birleşik yaklaşım, ağ hızını minimum düzeyde etkileyerek yüksek doğrulukta tespit sunar.

2.3. Dinamik ARP Denetimi (DAI) ve Ağ Anahtarı Güvenliği

Dinamik ARP Denetimi (DAI), yönetilen anahtarlar üzerinde çalışan, ARP paketlerini güvenilir IP-MAC bağlama veritabanına göre doğrulayan önemli bir güvenlik özelliğidir.[6] Bu özellik, kötü niyetli ARP paketlerinin ağa girmesini engelleyerek ARP spoofing saldırılarını proaktif olarak önler. DAI, ağ erişim katmanında önleyici bir önlem olarak işlev görür, böylece saldırıları bir dayanak noktası oluşturmadan önce durdurur.

Bu teknik, çok katmanlı savunma stratejilerinde temel bir proaktif katman olarak kabul edilir. ML/DL tabanlı sistemler gelişmiş tespit sunarken, DAI ağ erişim katmanında saldırıları önleyici bir rol oynar. DAI'nin etkinliği, saldırıları bir dayanak noktası oluşturmadan önce durdurmasındadır.[6] DAI, ağ erişim kontrolü (NAC) ile iyi entegre olur ve katmanlı bir güvenlik yaklaşımının önemli bir parçasıdır.[8]

2025'te, DAI, kurumsal ağlarda ve özellikle anahtar tabanlı altyapılarda temel bir

güvenlik katmanı olmaya devam edecektir.[6] Ağ Erişim Kontrolü (NAC) ile entegrasyonu, yetkisiz cihazların ağa erişimini ve ARP manipülasyonunu daha da kısıtlayacaktır.[8]

2.4. Yazılım Tanımlı Ağlar (SDN) Tabanlı Tespit ve Azaltma

Yazılım Tanımlı Ağlar (SDN) mimarisi, merkezi kontrolörler aracılığıyla ağ trafiğini ve ARP tablolarını küresel olarak izleme ve yönetme yeteneği sunar.[12] Bu, ARP spoofing saldırılarını tespit etmek, etkilenen anahtarların ARP önbelleklerini temizlemek ve ağ yapılandırmalarını dinamik olarak yeniden yapılandırmak için makine öğrenimi modellerini kullanır.[12] SDN'nin temel faydası, merkezi kontrol ve programlanabilirlik yeteneğidir. Kontrolörler, gelen tüm ARP paketlerini yakalayabilir, analiz edebilir, adres eşlemelerini öğrenebilir ve bunları uygulamanın belleğinde saklayabilir; böylece devam eden ARP önbellek karşılaştırmaları için bir temel oluştururken aynı zamanda küresel bir önbelleği sürdürebilirler.[12] Bu, geleneksel dağıtılmış ARP yönetimine göre önemli bir mimari avantajdır.

SDN, özellikle büyük ölçekli ve dinamik ağlarda (veri merkezleri, bulut ortamları) ARP spoofing'e karşı dayanıklılığı artıracaktır.[12] Performans darboğazlarını ve tek hata noktası (SPOF) sorunlarını ele alarak daha ölçeklenebilir ve verimli çözümler sunar.[12] Yapay Sinir Ağları (ANN), Evrişimsel Sinir Ağları (CNN), Uzun Kısa Süreli Bellek (LSTM) ve Gated Recurrent Unit (GRU) gibi ML modellerinin SDN içinde tespit için uygulanması, yüksek doğruluk elde etmiştir.[16]

2.5. Davranışsal Analiz ve Anomali Tespiti

Bu teknik, normal ağ davranışının (örn. ARP istek/yanıt kalıpları, IP-MAC eşleşme sıklığı, trafik hacmi) bir profilini oluşturur.[15] Bu profilden sapmalar, ARP spoofing veya diğer MITM saldırıları gibi anormal faaliyetleri işaret eder.[15] Yapay zeka ve makine öğrenimi bu profilleri oluşturmak ve anormallikleri tespit etmek için kullanılır.[15] Buradaki temel düşünce, bilinen kötü imzaları aramak yerine, normalden sapmaları aramaktır. Bu yaklaşım, "daha önce görülmemiş saldırıları, genellikle sıfırıncı gün saldırılarını tespit etmek için daha uygun" olarak kabul edilir.[17] Saldırganlar sürekli geliştiği için, eğer "normal" iyi tanımlanmışsa, herhangi bir önemli sapma, bilinen bir saldırı imzasıyla

eşleşip eşleşmediğine bakılmaksızın şüpheli kabul edilir.

2025'te, davranışsal analiz, özellikle IoT cihazları ve dinamik bulut ortamları gibi heterojen ağlarda ARP spoofing'in tespiti için kritik olacaktır.[15] Geleneksel imza tabanlı yöntemlerin yetersiz kaldığı yeni veya karmaşık saldırı vektörlerini yakalamada etkilidir.[15]

2.6. Kriptografik ARP Kimlik Doğrulaması ve Güvenli Protokoller

ARP protokolünün kimlik doğrulama mekanizmasından yoksun olması, ARP spoofing'in temel nedenidir.[2] Kriptografik anahtarlarla imzalanmış ARP paketleri (örn. D-ARP şeması) veya daha güvenli alternatif protokoller (örn. IPv6'daki Komşu Keşif Protokolü - NDP) kullanarak ARP paketlerinin gerçekliğini doğrulamak, saldırıları önlemede etkilidir.[2] Bu yaklaşımlar, ARP'nin güvensizliğinin belirtilerini tespit etmek veya önlemek yerine, doğrudan temel nedeni ele alır. D-ARP gibi şemalar, "anahtarla imzalanmış" ARP paketleri göndererek ve istekler ile yanıtlar arasında bir korelasyon kurarak "sıfır yanlış pozitif ve sıfır yanlış negatif olasılığı" elde etmeyi amaçlamaktadır.[21] Bu, belirtisel değil, temel bir çözümdür.

2025'te, mevcut IPv4 ağlarında D-ARP gibi şemaların benimsenmesi veya yeni ağ altyapılarında IPv6'ya geçişin hızlanmasıyla, ARP spoofing'e karşı daha sağlam bir savunma sağlanacaktır.[5] Bu, özellikle yüksek güvenlik gerektiren finans ve kritik altyapı sektörlerinde önem kazanacaktır.

2.7. Gelişmiş Honeypot'lar ve Tuzak Sistemleri

Gelişmiş düşük etkileşimli honeypot'lar, temel ağ hizmetlerini taklit ederek saldırganları çeker.[20] Tshark gibi araçlarla ağ trafiğini yakalayıp Python betikleriyle (örn. IP/MAC whitelist kontrolü) analiz ederek spoofing saldırılarını tespit edebilir ve saldırgan hakkında bilgi toplayabilirler.[20] Honeypot'lar öncelikle üretim sistemlerindeki bir saldırıyı önlemekten ziyade, kontrollü bir ortama saldırganları çekerek "kötü niyetli aktörler ve nasıl çalıştıkları hakkında ayrıntılı bilgi edinmek" [20] içindir. Bu, değerli tehdit istihbaratı sağlar. Tshark ve Python betikleriyle geliştirilmesi, özellikle spoofing'i tespit etmelerine ve daha sonra analiz için trafik yakalamalarına olanak tanıyarak bir erken uyarı sistemi görevi görmelerini sağlar.[20] Bu, tamamen savunmacı yaklaşımdan

istihbarat odaklı savunmaya doğru bir kaymadır.

2025'te, honeypot'lar, özellikle küçük ve orta ölçekli kuruluşlar için maliyet etkin bir güvenlik katmanı sunacak, saldırgan davranışlarını öğrenmek ve yeni saldırı vektörlerini keşfetmek için değerli istihbarat sağlayacaktır.

2.8. XDR (Genişletilmiş Tespit ve Yanıt) Çözümleri

Genişletilmiş Tespit ve Yanıt (XDR), uç noktalar, ağ, bulut iş yükleri, e-posta ve kimlik sağlayıcılar gibi birden fazla güvenlik katmanından tehdit verilerini birleştiren kapsamlı bir siber güvenlik çözümüdür.[22] Gelişmiş analitik ve makine öğrenimi kullanarak ARP spoofing gibi saldırıları daha geniş bir bağlamda tespit eder ve otomatik yanıt iş akışları sağlar.[22] Bu, daha verimli ve hızlı tehdit araştırması, avcılığı ve yanıtı mümkün kılar.

XDR'nin temel ayırt edici özelliği, "daha önce izole edilmiş güvenlik araçlarından tehdit verilerini birleştirmesidir".[23] Bu, bir ARP spoofing uyarısının sadece izole bir olay olmadığı; uç nokta günlükleri, kimlik verileri ve bulut etkinliği ile ilişkilendirildiği anlamına gelir. Bu "saldırının tutarlı anlatımı" [23], güvenlik ekiplerinin basit bir ARP spoofing'in izole bir olay mı yoksa daha büyük, daha sofistike bir saldırı zincirinin (örn. fidye yazılımı, APT) bir parçası mı olduğunu anlamalarını sağlar. Bu bağlam, etkili yanıt için kritik öneme sahiptir.

2025'te XDR, karmaşık ve çok vektörlü saldırılara karşı kurumsal savunmanın temel taşı olacaktır.[23] ARP spoofing'in daha büyük bir saldırı zincirinin parçası olduğu senaryolarda hızlı tespit ve kapsamlı yanıt sağlayacaktır.

2.9. SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı) Platformları

Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformları, güvenlik araçlarını ve süreçlerini tek bir merkezde birleştirerek, olay yanıtını otomatikleştiren ve orkestrasyonunu sağlayan teknolojilerdir.[24] ARP spoofing tespit edildiğinde, SOAR önceden tanımlanmış "playbook"ları (örn. şüpheli MAC adresini engelleme, ARP önbelleğini temizleme, uyarı gönderme) otomatik olarak tetikleyebilir.[24]

SOAR'ın temel faydası otomasyondur; "tekrarlayan görevleri otomatikleştirme" ve "olaylara yanıtı hızlandırma".[25] SOAR, "uyarı yorgunluğunu azaltarak SOC analistlerinin analiz ve daha derin insan müdahalesi gerektiren görevlere odaklanmasını sağladığını" belirtmektedir.[24] Siber tehditlerin hacmi arttıkça bu çok önemlidir. ARP spoofing için hızlı, otomatik bir yanıt (örn. bir bağlantı noktasını engelleme, bir ARP önbelleğini düzeltme) zararı en aza indirebilir. "Playbooklar"dan bahsedilmesi, bu otomatik yanıtların yapılandırılmış, önceden tanımlanmış doğasını vurgulamaktadır.[24]

2025'te SOAR, güvenlik operasyon merkezlerinin (SOC'ler) verimliliğini artıracak, insan müdahalesini azaltacak ve ARP spoofing gibi tekrarlayan olaylara yanıt süresini önemli ölçüde hızlandıracaktır.[24] Bu, özellikle büyük ölçekli ve dinamik ağlarda kritik öneme sahiptir.

2.10. Birleşik Siber Güvenlik Platformları (Unified Security Platforms)

Geleneksel "en iyi çözüm" (best-of-breed) yaklaşımının aksine, birleşik platformlar (örn. aiXDR360), SIEM (Güvenlik Bilgileri ve Olay Yönetimi), NDR (Ağ Tespit ve Yanıt), EDR (Uç Nokta Tespit ve Yanıt), UEBA (Kullanıcı ve Varlık Davranışı Analizi) ve SOAR gibi birden fazla güvenlik işlevini tek bir mimaride birleştirir.[26] Bu, ARP spoofing'in tespiti ve yanıtı için entegre görünürlük, analitik ve otomasyon sağlar.

2025 yılı RSAC konferansında, "parçalanmış 'en iyi çözüm' güvenlik yığınının artık yeterli olmadığı" ve "farklı satıcılardan on veya daha fazla aracı bir araya getirme çağının sona erdiği" açıkça belirtilmiştir.[26] Bu, büyük bir endüstri trendidir. Farklı araçları yönetmenin karmaşıklığı, maliyeti ve gecikmesi tolere edilemez hale gelmektedir. Birleşik platformlar bunu, "tespit, yanıt, analitik, uyumluluk ve otomasyonu tek bir mimaride birleştirerek" çözmektedir.[26] Bu platformlar, güvenlik operasyonlarını basitleştirecek, maliyetleri düşürecek ve tehditlere karşı yanıt hızını artıracaktır. ARP spoofing gibi temel ağ saldırılarının, daha geniş bir tehdit bağlamında daha etkin bir şekilde yönetilmesini sağlayacaktır.[26]

3. Bütünleşik Siber Güvenlik Çözümleri ve Proaktif Savunma Yaklaşımları

ARP spoofing'e karşı etkili bir savunma, tekil tespit tekniklerinin ötesine geçerek, bütünleşik siber güvenlik çözümlerini ve proaktif savunma yaklaşımlarını benimsemeyi gerektirir. Siber güvenlik alanındaki eğilimler, reaktif nokta çözümlerinden proaktif, entegre ekosistemlere doğru belirgin bir geçişi göstermektedir. Bu ilerleme, temel tespit araçlarından (Wireshark, ARPWatch [6]) başlayarak, daha otomatik tespit ve önleme için Saldırı Tespit Sistemleri (IDS) ve Saldırı Önleme Sistemleri (IPS) [4] kavramına doğru bir evrimi içermektedir. Ağ Erişim Kontrolü (NAC) sistemleri ise erişim kontrolü katmanı ekleyerek savunmayı güçlendirir.

Güvenlik Araçlarının Yakınsaması

Geleneksel olarak ayrı çalışan güvenlik duvarları, Saldırı Tespit Sistemleri (IDS), Saldırı Önleme Sistemleri (IPS) ve Ağ Erişim Kontrolü (NAC) gibi araçlar, ARP spoofing gibi ağ katmanı saldırılarına karşı daha güçlü bir savunma sağlamak için giderek daha fazla entegre edilmektedir.

- **IDS/IPS Sistemleri:** Bu sistemler, gelişmiş kural setleri ve trafik analizi ile ARP spoofing'i gerçek zamanlı olarak tanımlayabilir ve engelleyebilirler.[2] IDS, şüpheli trafik kalıplarını bayraklandırarak analiz sürecini kolaylaştırırken, IPS kötü niyetli etkinliği doğrudan engelleyebilir.[4]
- **NAC (Network Access Control):** NAC, cihazların ağa bağlanmadan önce kimlik doğrulaması yapmasını zorunlu kılarak yetkisiz cihazların (saldırganların kullandığı dahil) erişimini engeller.[5] NAC, ARP spoofing'e karşı koruma sağlamak için Dinamik ARP Denetimi (DAI) ile iyi entegre olur, böylece yalnızca güvenilir IP-MAC bağlamalarına sahip meşru ARP paketlerinin ağa girmesine izin verilir.[8]

Holistik Savunma için Entegrasyon

Siber güvenlik alanında, tehditlerin karmaşıklığı arttıkça, güvenlik çözümlerinin entegrasyonu hayati önem taşımaktadır. ARP spoofing tespitinin sadece izole bir olay olarak ele alınmasından, daha geniş bir güvenlik bağlamında anlaşılmasına ve hızla yanıt verilmesine doğru bir değişim gözlemlenmektedir.

- **XDR ve SOAR'ın Rolü:** Genişletilmiş Tespit ve Yanıt (XDR) çözümleri, uç nokta, ağ, bulut ve kimlik gibi çeşitli kaynaklardan gelen tehdit verilerini birleştirerek ARP spoofing'in daha büyük bir saldırı zincirinin (örn. fidye yazılımı veya Gelişmiş Kalıcı Tehditler - APT) parçası olup olmadığını ortaya çıkarır.[22] Bu, güvenlik ekiplerinin bir ARP spoofing olayının tüm ağdaki bağlamını anlamalarını sağlar. Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR) platformları ise tespit edilen olaylara otomatik yanıtlar (örn. şüpheli MAC adresini engelleme, ARP önbelleğini temizleme) tetikleyerek yanıt süresini önemli ölçüde kısaltır.[24]
- **Birleşik Platformlar:** Geleceğin siber güvenliği, parçalı "en iyi çözüm" araçları yerine, tüm güvenlik işlevlerini (SIEM, NDR, EDR, UEBA, SOAR) tek bir mimaride birleştiren birleşik platformlara doğru ilerlemektedir.[26] Bu platformlar, güvenlik operasyonlarını basitleştirir, maliyetleri düşürür ve tehditlere karşı yanıt hızını artırır. ARP spoofing gibi temel ağ saldırılarının, daha geniş bir tehdit bağlamında daha etkin bir şekilde yönetilmesini sağlar.

Proaktif Önlemlerin Temel Rolü

Etkili tespit, "normal" veya "güvenilir" olanın neye benzediğini bilmeye dayanır. Güvenilir bir temel çizgi olmadan, anormallikleri tespit etmek zordur ve yüksek yanlış pozitiflere yol açabilir.[27] Bu nedenle, ARP spoofing'e karşı proaktif önlemler, savunma stratejisinin ayrılmaz bir parçasıdır.

- **Statik ARP Girişleri:** Kritik cihazlar (örn. yönlendiriciler) için IP-MAC eşlemelerini manuel olarak sabitlemek, dinamik ve sahtekarlığa açık ARP güncellemelerine olan bağımlılığı ortadan kaldırır.[5] Bu, temel bir güvenilir temel çizgi oluşturur.
- **Ağ Segmentasyonu (VLAN'lar):** Hassas cihazları izole ederek ve ağı daha küçük, yalıtılmış segmentlere bölerek, ARP spoofing saldırılarının ağın geneline yayılmasını sınırlar.[6] Bu, bir saldırının etkisini kısıtlar.
- **Paket Filtreleme:** Güvenlik duvarları ve anahtarlar, kötü amaçlı ARP paketlerini, çakışan kaynak bilgileri içerenleri tespit ederek cihazlara ulaşmadan durduracak şekilde yapılandırılabilir.[5] Bu, ağ giriş noktasında bir savunma katmanı sağlar.
- **Şifreli İletişim Protokolleri (HTTPS, SSH, VPN):** Veriler ele geçirilse bile, şifreleme sayesinde saldırganlar tarafından okunamaz veya değiştirilemez.[2] Bu, ARP spoofing'in bir MITM saldırısı olarak kullanılması durumunda bile veri gizliliğini korur.

Bu önlemlerin sürekli doğrulanması gerekmektedir. "Referansları sürekli güncelleme ve

kaynak IP ve MAC adreslerini doğrulama" [12] ve ARP önbellek izlemesi için "periyodik ağ taraması" [1] gibi kavramlar, bu temel çizginin sürekli olarak güncel ve doğru kalması ihtiyacını pekiştirmektedir.

4. Gelecek Perspektifi ve Proje İçin Öneriler

ARP spoofing tespiti ve otomatik analizi alanı, siber güvenlik tehditlerinin evrimiyle birlikte sürekli bir değişim içindedir. Gelecek, daha akıllı, daha entegre ve daha proaktif savunma mekanizmalarını gerektirecektir.

Anahtar Trendlerin Özeti

- **Yapay Zeka/Makine Öğrenimi Hakimiyeti:** ML/DL, ağ trafiğindeki karmaşık anormallikleri tespit etme yetenekleri sayesinde ARP spoofing tespitinde baskın bir güç olmaya devam edecektir.[10]
- **Otomasyon ve Entegrasyon:** SOAR ve XDR gibi platformlar aracılığıyla otomatik yanıt ve farklı güvenlik katmanları arasında entegrasyon, olay yanıt sürelerini hızlandıracak ve güvenlik operasyonlarının verimliliğini artıracaktır.[22]
- **Proaktif ve Davranışsal Analize Geçiş:** Statik kural tabanlı sistemlerden, normal ağ davranışının profillenmesine ve sapmaların tespitine dayalı davranışsal analize doğru bir kayma gözlemlenmektedir.[15]
- **Birleşik Güvenlik Platformları:** Güvenlik araçlarının tek bir mimaride birleştirilmesi, karmaşıklığı azaltacak ve bütünsel görünürlük sağlayacaktır.[26]

Gelecekteki Zorluklar

Siber güvenlikte sürekli bir "silah yarışı" dinamiği bulunmaktadır; savunma yapay zekası, saldırı yapay zekasına sürekli uyum sağlamak zorundadır. ML/DL tespit için güçlü olsa da [10], saldırganlar da yapay zekayı kullanarak daha sofistike teknikler geliştirmektedir. Yapay zeka tarafından üretilen derin sahtekarlıklar (deepfakes) [28] ve gelişmiş kaçınma yöntemleri [14], mevcut ML modellerinin etkinliğini zorlayabilir, zira

normal trafik kalıplarını daha ikna edici bir şekilde taklit edebilirler.

Diğer önemli zorluklar arasında kaynak kısıtlı cihazlar için (örn. IoT cihazları) kenar ağlarda (edge networks) ARP spoofing tespiti için hafif ve hesaplama açısından verimli modellerin geliştirilmesi [17] ve büyük ve dinamik ağlarda milyonlarca paketi gerçek zamanlı olarak analiz etmek ve yönetmek için ölçeklenebilirlik yer almaktadır.

Proje İçin Öneriler

Mevcut projenin ARP spoofing saldırılarının tespitine yönelik hedefleri doğrultusunda, aşağıdaki öneriler gelecekteki geliştirmeler ve daha geniş bir etki alanı için yol gösterebilir:

- **ML/DL Modelleri İçin Özellik Setini Genişletme:** Mevcut IP-MAC çakışması kuralının ötesine geçerek, ARP paket başlıklarından (opcode, gönderen/hedef IP/MAC, paket boyutu, frekans) ve diğer protokollerden (ICMP, IP, TCP, UDP) daha zengin özellik setleri çıkararak ML modellerinin doğruluğunu artırın.[12] Bu, projenin mevcut "aynı IP adresine birden fazla farklı MAC adresinin atanması" kuralının ötesine geçerek davranışsal örüntü tanıma ile önemli bir iyileşme sağlayacaktır.
- **Gerçek Zamanlı Yakalama ve Hat İçi Analizi Keşfetme:** Projenin .pcap dosyalarını analiz etme yeteneğini, Bettercap gibi araçlara benzer şekilde gerçek zamanlı paket yakalama ve hat içi analiz yetenekleriyle genişletmeyi düşünün.[19] Bu, saldırılara daha hızlı yanıt verilmesini sağlar ve proaktif, hat içi tespit yeteneği kazandırır.
- **Geniş Güvenlik Çerçeveleriyle Entegrasyon Potansiyeli:** Geliştirilen tespit sisteminin çıktısının (örn. tespit edilen kötü amaçlı IP/MAC çiftleri, uyarılar), SOAR veya XDR gibi daha büyük güvenlik platformları tarafından kolayca tüketilebilecek şekilde tasarlanması önemlidir.[22] Bu, standartlaştırılmış günlük kaydı formatları veya API entegrasyonları aracılığıyla sağlanabilir. Bağımsız bir araç entegrasyon sorunlarıyla karşılaşabilir, bu nedenle birlikte çalışabilirlik kritik öneme sahiptir.
- **Davranışsal Profilleme ve Anomali Tespitini Araştırma:** Ağdaki normal ARP davranışının bir temelini oluşturmak ve bu temelden sapmaları tespit etmek için ML (örn. otomatik kodlayıcılar) kullanmayı düşünün.[15] Bu, sıfırıncı gün saldırılarını ve daha sofistike kaçınma tekniklerini yakalamak için daha nüanslı bir yaklaşım sunar. Bu, geçmiş
  .pcap verilerini toplayarak ve normal kalıpları öğrenmek için ML tekniklerini kullanarak gerçekleştirilebilir.

- **Honeypot Entegrasyonu Potansiyeli:** Proje için tehdit istihbaratı toplamak ve çeşitli saldırı kalıpları üzerinde ML modellerini eğitmek için honeypot'lardan (özellikle gelişmiş düşük etkileşimli olanlar) yararlanmayı değerlendirin.[20] Honeypot'lar, kontrollü bir ortamda test veri setleri oluşturmak için değerli bir kaynak olabilir.
- **Geleceğe Hazırlık: IPv6'nın NDP Protokolü:** Uzun vadeli bir perspektifte, IPv6'nın ARP'ye kıyasla daha güvenli olan Komşu Keşif Protokolü (NDP) kullanımını göz önünde bulundurun.[5] Ağ altyapıları IPv6'ya geçtikçe, tespit stratejilerinin de buna uyum sağlaması gerekecektir.

ARP spoofing bir ağ katmanı saldırısı olsa da, siber güvenlikte ağ merkezli güvenlikten kimlik merkezli güvenliğe doğru daha geniş bir eğilim bulunmaktadır.[28] Bir kimlik sahtekarlığı yapılırsa, ağ düzeyindeki kontroller atlatılabilir. Bu nedenle, projenin ek bir bağlam katmanı eklemek için kimlik yönetimi sistemleriyle entegrasyonu düşünmesi faydalı olabilir. Örneğin, bir IP-MAC anormalliği tespit edilirse, ilişkili kullanıcı/cihaz kimliğini doğrulamak, olay yanıtı için kritik bağlam sağlayabilir. Bu uzun vadeli bir vizyon olsa da, ARP spoofing tespitinin gelecekteki rolünü anlamak için önemlidir.

Alıntılanan çalışmalar

1. Detecting ARP spoofing with OpUtils - ManageEngine, erişim tarihi Haziran 20, 2025, https://www.manageengine.com/products/oputils/how-to-detect-arp-spoofing.html
2. ARP Poisoning - 1Kosmos, erişim tarihi Haziran 20, 2025, https://www.1kosmos.com/security-glossary/arp-poisoning/
3. Machine Learning-Based Detection of ARP Spoofing Attacks Using ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/392689907_Machine_Learning-Based_Detection_of_ARP_Spoofing_Attacks_Using_Behavioral_Analysis
4. What is ARP Spoofing? Risks, Detection, and Prevention, erişim tarihi Haziran 20, 2025, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/arp-spoofing/
5. What is ARP Spoofing | ARP Cache Poisoning Attack Explained - Imperva, erişim tarihi Haziran 20, 2025, https://www.imperva.com/learn/application-security/arp-spoofing/
6. What Is ARP Spoofing? - JumpCloud, erişim tarihi Haziran 20, 2025, https://jumpcloud.com/it-index/what-is-arp-spoofing
7. ARP Poisoning: How to Prevent ARP Spoofing Attacks - Trustifi, erişim tarihi Haziran 20, 2025, https://trustifi.com/blog/what-is-arp-poisoning-and-how-to-prevent-it/
8. What is Address Resolution Protocol (ARP)? - Portnox, erişim tarihi Haziran 20, 2025,

https://www.portnox.com/cybersecurity-101/what-is-address-resolution-protocol/
9. ARP Spoofing in Action: An Ethical Approach to Network Security - ResearchGate, erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/391339315_ARP_Spoofing_in_Action_An_Ethical_Approach_to_Network_Security
10. Detecting and Preventing ARP Spoofing Attacks Using Real-Time ..., erişim tarihi Haziran 20, 2025, https://www.ijircst.org/view_abstract.php?title=Detecting-and-Preventing-ARP-Spoofing-Attacks-Using-Real-Time-Data-Analysis-and-Machine-Learning&year=2024&vol=12&primary=QVJULTEzMDk=
11. (PDF) Detecting and Preventing ARP Spoofing Attacks Using Real- Time Data Analysis and Machine Learning - ResearchGate, erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/384296277_Detecting_and_Preventing_ARP_Spoofing_Attacks_Using_Real-_Time_Data_Analysis_and_Machine_Learning/download
12. ARP spoofing detection using machine learning classifiers: an ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/384668138_ARP_spoofing_detection_using_machine_learning_classifiers_an_experimental_study
13. Implementation of Dynamic ARP Inspection for Enhanced Network Security, erişim tarihi Haziran 20, 2025, https://indjcst.com/archiver/archives/implementation_of_dynamic_arp_inspection_for_enhanced_network_security.pdf
14. The Cyberthreat Report: April 2025 - Trellix, erişim tarihi Haziran 20, 2025, https://www.trellix.com/advanced-research-center/threat-reports/april-2025/
15. Behavioral profiling of abnormal network traffic in security - SPIE Digital Library, erişim tarihi Haziran 20, 2025, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/13562/1356248/Behavioral-profiling-of-abnormal-network-traffic-in-security/10.1117/12.3060427.full
16. Using different machine learning models for address resolution ..., erişim tarihi Haziran 20, 2025, https://discovery.researcher.life/article/using-different-machine-learning-models-for-address-resolution-protocol-spoofing-attack-detection-in-software-defined-network-architecture/2ae8227002823c9ca007a390d172f805
17. Anomaly detection on edge networks - Lund University Publications, erişim tarihi Haziran 20, 2025, https://lup.lub.lu.se/student-papers/record/9188366/file/9188367.pdf
18. Detection of ARP Spoofing with Optimized False Alarm Using Deep ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/386400938_Detection_of_ARP_Spoofing_with_Optimized_False_Alarm_Using_Deep_Learning_Based_Absolute_Thresholding
19. ARP Spoofing in Action: An Ethical Approach to Network ... - IRJIET, erişim tarihi

Haziran 20, 2025, https://irjiet.com/common_src/article_file/IRJIET-INSPIRE250391745457582.pdf
20. An approach to enhance low -interaction honeypots by enabling ..., erişim tarihi Haziran 20, 2025, https://norma.ncirl.ie/4489/1/rheabonnerji.pdf
21. D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing ..., erişim tarihi Haziran 20, 2025, https://www.researchgate.net/publication/360362946_D-ARP_An_Efficient_Scheme_to_Detect_and_Prevent_ARP_Spoofing
22. eXtended Detection and Response (XDR) - Bitdefender, erişim tarihi Haziran 20, 2025, https://www.bitdefender.com/business/support/en/77209-376320-xdr.html
23. What Is Extended Detection and Response (XDR)? XDR Security Guide - Cynet, erişim tarihi Haziran 20, 2025, https://www.cynet.com/xdr-security/understanding-xdr-security-concepts-features-and-use-cases/
24. View of STREAMLINING THREAT RESPONSE AND AUTOMATING CRITICAL USE CASES WITH SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR) | Journal of Digital Security and Forensics, erişim tarihi Haziran 20, 2025, https://www.digitalsecurityforensics.org/digisecforensics/article/view/45/22
25. Top 9 SOAR Platforms and Vendors - BlinkOps, erişim tarihi Haziran 20, 2025, https://www.blinkops.com/blog/soar-platforms
26. RSAC 2025 Recap: Why the Future of Cybersecurity Belongs to Unified Platforms - Seceon, erişim tarihi Haziran 20, 2025, https://seceon.com/rsac-2025-recap-why-the-future-of-cybersecurity-belongs-to-unified-platforms/
27. ARP Poisoning: Definition, Techniques, Defense & Prevention - Okta, erişim tarihi Haziran 20, 2025, https://www.okta.com/en-au/identity-101/arp-poisoning/
28. AI-based Identity Fraud Detection: A Systematic Review - arXiv, erişim tarihi Haziran 20, 2025, https://arxiv.org/html/2501.09239v1
29. 5 Cyber-Security and Authentication Trends to Keep an Eye on in 2025 - Blog - Wultra, erişim tarihi Haziran 20, 2025, https://www.wultra.com/blog/5-cyber-security-and-authentication-trends-to-keep-an-eye-on-in-2025
30. Designing a Zero Trust Architecture: 20 open-source tools to secure every layer | Cerbos, erişim tarihi Haziran 20, 2025, https://www.cerbos.dev/blog/20-open-source-tools-for-zero-trust-architecture