2025 Yılı İçin Gelişmiş Host Tarama Teknikleri ve Eğilimleri Raporu

I. Yönetici Özeti

Bu rapor, 2025 yılı için ağ keşfi ve güvenlik açığı değerlendirmesindeki en son ve en etkili teknikleri ve eğilimleri derinlemesine incelemektedir. Host tarama, hem saldırı hem de savunma siber güvenlik operasyonlarının temel adımı olarak stratejik önemini korurken, yapay zeka (YZ) destekli siber saldırılar, Sıfır Güven (Zero Trust) mimarilerinin yükselişi ve bulut, Nesnelerin İnterneti (IoT) ve sunucusuz (serverless) ortamlar gibi genişleyen saldırı yüzeyleri nedeniyle metodolojilerinde sürekli bir evrim geçirmektedir. Bu rapor, sürekli, YZ odaklı ve özelleşmiş taramanın önemini vurgulayarak, kuruluşların giderek karmaşıklaşan tehdit ortamında sağlam bir siber güvenlik duruşu sürdürmeleri için stratejik çıkarımları özetlemektedir.

II. Giriş: 2025 Yılında Ağ Keşfinin Gelişen Manzarası

Ağ keşfi, siber güvenlik operasyonlarının temelini oluşturan kritik bir süreçtir. Bu süreç, bir ağdaki aktif sistemleri tespit etmeyi, açık portları ve çalışan hizmetleri belirlemeyi içerir ve derinlemesine sızma testleri veya güvenlik açığı analizlerinden önce atılan ilk adımdır.[1] Ağ keşif araçları, yönlendiriciler, anahtarlar, sunucular, uç noktalar ve IoT cihazları dahil olmak üzere tüm bağlı varlıklar hakkında veri toplayarak güvenlik denetimleri, uyumluluk, sorun giderme ve ağ yönetimi için hayati önem taşıyan gerçek zamanlı görünürlük sağlar.[4] 2025 yılına girerken, siber güvenlik ortamı, host tarama metodolojilerinin sürekli evrimini zorunlu kılan önemli eğilimlerle şekillenmektedir.

2025'i Şekillendiren Temel Siber Güvenlik Eğilimleri

Yapay Zeka Destekli Siber Saldırılar ve Savunma Zorunluluğu: Yapay zeka (YZ), siber güvenliği her iki tarafta da hızla dönüştürmektedir. Siber suçlular, geleneksel savunmaları aşan uyarlanabilir kötü amaçlı yazılımlar, aşırı kişiselleştirilmiş kimlik avı dolandırıcılıkları ve deepfake'ler oluşturmak için YZ'yi silahlandırmaktadır.[5] YZ destekli siber saldırıların giderek daha sofistike hale gelmesi ve geleneksel güvenlik önlemleri için önemli zorluklar oluşturması beklenmektedir.[6] YZ, güvenlik açığı ifşasından çalışan bir istismara kadar geçen süreyi günlerden veya haftalardan saatlere indirerek istismar geliştirmeyi çarpıcı biçimde hızlandırmaktadır. Örneğin, CVE-2025-32433 gibi kritik bir güvenlik açığı için, GPT-4 ve Claude Sonnet 3.7 gibi üretken YZ modelleri, bulanıklaştırma ortamları kurmak, temel nedenleri belirlemek ve kavram kanıtı istismarları taslağını oluşturmak için kullanılmıştır.[8]

Bu hızlı istismar geliştirme, güvenlik açığının kamuya açıklanması ile silahlandırılması

arasındaki savunma penceresinin dramatik bir şekilde daraldığı anlamına gelmektedir. Geleneksel, daha yavaş, insan odaklı host tarama ve güvenlik açığı değerlendirme yöntemleri, YZ'nin hızına ayak uydurmakta yetersiz kalmaktadır. Bu nedenle, saldırganların YZ ile güvenlik açıklarını saatler içinde silahlandırabileceği bir ortamda, kuruluşların tehditleri etkili bir şekilde tespit edebilmesi için host tarama araçlarının ve tekniklerinin YZ ve makine öğrenimini entegre etmesi, daha hızlı, daha doğru ve daha uyarlanabilir tespit sağlaması zorunlu hale gelmiştir. Bu durum, siber güvenlikte YZ'nin bir tarafın diğerini YZ kullanmaya zorladığı doğrudan bir silahlanma yarışı olduğunu göstermektedir.

Sıfır Güven Mimarisi Yeni Standart Olarak: Geleneksel ağ çevresi ortadan kalkmakta, saldırganların eski güvenlik modellerini atlamasını kolaylaştırmaktadır. Buna yanıt olarak, Sıfır Güven ağ erişimi, ağ güvenliğinde en hızlı büyüyen segment haline gelmiştir; kurumsal uzaktan erişim dağıtımlarının %70'inin VPN'lerden Sıfır Güven mimarilerine geçmesi beklenmektedir.[5] "Asla güvenme, her zaman doğrula" ilkesine dayanan Sıfır Güven çerçevesi, sürekli kimlik doğrulamayı, katı erişim kontrollerini ve gerçek zamanlı tehdit tespitini zorunlu kılarak yetkisiz erişim riskini önemli ölçüde azaltmaktadır.[5] Cihaz parmak izi (device fingerprinting), Sıfır Güven modelinde cihaz bütünlüğüne sürekli güveni sürdürmek için temel bir sinyal haline gelmekte, sürekli cihaz puanlaması ve tam zamanında kimlik doğrulama sağlamaktadır.[9]

Sıfır Güven'in yeni standart olarak benimsenmesi, ağ içinde zımni güvenin terk edildiği anlamına gelmektedir. Bu değişim, güvenliğin artık sadece çevre savunmalarına dayanamayacağı anlamına gelmektedir. Bunun yerine, her cihaz ve kullanıcının, içeride veya dışarıda olsun, sürekli olarak doğrulanması gerekmektedir. Bu durum, host tarama ve cihaz parmak izi oluşturma yeteneklerinin sürekli ve ayrıntılı olmasını zorunlu kılmaktadır. Böylece, yalnızca yetkili ve uyumlu varlıkların kaynaklara eriştiğinden emin olunabilir. Bu durum, host taramanın periyodik bir ağ sınırı denetiminden, bağlı her uç noktanın bütünlüğünü ve duruşunu doğrulayan sürekli, yaygın bir sürece dönüşmesini ifade etmekte ve Sıfır Güven uygulamasının vazgeçilmez bir sütunu haline gelmektedir.

Genişleyen Saldırı Yüzeyleri: Bulut, IoT ve 5G: 5G ağlarının devam eden yayılımı bağlantıyı dönüştürecek ancak aynı zamanda siber güvenlik zorluklarını da beraberinde getirecektir. Daha yüksek hızlar ve daha düşük gecikme süresi ile 5G, daha fazla cihaz ve sistemin bağlanmasını sağlayarak siber suçlular için saldırı yüzeyini genişletmektedir.[6] Hem işletmelerde hem de evlerde IoT cihazlarının patlaması, benzeri görülmemiş bir kolaylık getirmekte ancak aynı zamanda önemli güvenlik zorlukları da yaratmaktadır, zira birçok IoT cihazı sağlam yerleşik güvenlikten yoksundur.[6] Bulut altyapıları temel olarak API'ler üzerine kuruludur ve bulut ortamlarındaki çoğu saldırı geneldir, API istismarı ve yanlış yapılandırmalara odaklanmaktadır.[10] Sunucusuz

mimariler, altyapı yönetimini basitleştirirken, geleneksel araçların genellikle tespit edemediği özel saldırı vektörleri ve benzersiz güvenlik kör noktaları ortaya çıkarmaktadır.[11]

Bu çeşitli ve dinamik ortamlar, geleneksel IP tabanlı taramaların yetersiz kaldığı anlamına gelmektedir. Bu nedenle, 2025'teki host tarama, API keşfi, kapsayıcı görüntü taraması ve sunucusuz işlev analizi gibi özel teknikleri içerecek şekilde çeşitlenmelidir. Bu, her bulut yerel iş yükünün benzersiz özelliklerine uyum sağlamayı gerektirmekte ve "host tarama"nın kapsamı ve doğasında önemli bir evrimi temsil etmektedir.

III. 2025 Yılı İçin En İyi 10 Gelişmiş Host Tarama Tekniği ve Eğilimi

Bu bölüm, 2025 yılı için host taramasında en etkili ve en son teknolojiye sahip on tekniği ve eğilimi, netlik ve derinlik için kategorize edilmiş olarak detaylandırmaktadır.

A. Yeni Nesil Port Tarama ve Hizmet Keşfi

1. YZ Destekli ve Sürekli Güvenlik Açığı Tarama
   Yeni Nesil Güvenlik Açığı Yönetimi (NGVM), geleneksel, periyodik taramadan sürekli, dinamik bir sürece geçişi temsil etmektedir. Bu yaklaşım, YZ tabanlı risk değerlendirmesi, gerçek zamanlı tehdit istihbaratı ve otomatik yama orkestrasyonunu kullanarak güvenlik açıklarını haftalar yerine saatler içinde tespit etmeyi ve gidermeyi amaçlamaktadır.13
   Temel Özellikler ve Mekanizmalar:
   - **Sürekli Varlık Keşfi:** Modern NGVM çözümleri, CI/CD (Sürekli Entegrasyon/Sürekli Teslimat) işlem hatları veya bulut API'leri ile entegre olarak yeni veya değişen varlıkları gerçek zamanlı olarak tanımlar. Bu, geçici kapsayıcıların ve dinamik bulut örneklerinin tespit edilmesini sağlayarak taranması gereken uç noktaların sürekli güncel bir listesini sunar.[13]
   - **YZ ile Risk Tabanlı Puanlama:** Geleneksel CVSS puanlarının ötesine geçerek, yeni nesil çözümler tehdit istihbaratını, varlık kritikliğini ve kullanım kalıplarını birleştirir. Bu sayede, istismar olasılığı ve iş etkisi dikkate alınarak yama uygulama daha stratejik hale gelir.[13]
   - **Gerçek Zamanlı Tehdit İstihbaratı Entegrasyonu:** NGVM sistemleri, yeni keşfedilen güvenlik açıklarını (sıfır gün saldırıları veya yeni kötü amaçlı yazılım kampanyaları dahil) hızlı bir şekilde güncellemek ve gidermek için tehdit beslemelerini ve kullanıcı topluluklarını sürekli olarak izler. Makine öğrenimi ile birleştiğinde, sistemin tespit kuralları her döngüde iyileşerek doğruluk artar ve gelişmiş kalıcı tehditler etkili bir şekilde savuşturulur.[13]
   - **Otomatik Yama Orkestrasyonu:** Yerleşik veya entegre yama yönetimi, kritik güvenlik açıklarını kararlı ortamlarda otomatik olarak ele alır veya geliştiricilerin

incelemesi için kısmi güncellemeleri teşvik eder, böylece manuel yükü azaltır.[13]

- **DevOps Entegrasyonu:** Güvenlik süreçleri, geliştirme yaşam döngüsüne (shift-left) erken entegre edilir. Eklentiler ve API'ler aracılığıyla tarama, derleme süreçlerine dahil edilir ve yeni kod yüksek önem dereceli güvenlik açıkları içeriyorsa birleştirme istekleri engellenebilir.[13]

Önde Gelen Araçlar ve Platformlar:

- **Pynt:** API güvenlik açıklarını tarayan YZ destekli bir API Güvenliği çözümüdür. Geleneksel, modern ve LLM API'leri için otomatik, CI/CD entegre, bağlama duyarlı testler sunar. Ayrıca gölge ve belgelenmemiş API'ler için API Keşfi de sağlar.[15]
- **Nessus:** Çeşitli BT ortamlarındaki güvenlik açıklarını belirlemeye yardımcı olan yaygın olarak kullanılan bir güvenlik açığı tarayıcısıdır. Yanlış yapılandırmaları, eksik yamaları ve uyumluluk ihlallerini tespit etmek için hem kimlik bilgileriyle hem de kimlik doğrulaması yapılmamış taramayı destekler.[2]
- **OpenVAS:** Greenbone Networks tarafından geliştirilen açık kaynaklı bir güvenlik açığı tarayıcısıdır. Ağlar, sistemler ve uygulamalardaki güvenlik zayıflıklarını belirlemek için tasarlanmıştır ve düzenli olarak güncellenen beslemeler sunar.[15]
- **Rapid7 InsightVM, Tenable (Nessus, Vulnerability Management, Security Center), Qualys VMDR, Arctic Wolf Managed Risk, CrowdStrike Falcon Spotlight:** Bu önde gelen ticari çözümler, genellikle YZ destekli platformları kullanarak kapsamlı güvenlik açığı değerlendirmesi ve maruziyet yönetimi sunar.[16]
- **SentinelOne Singularity™:** Kapsayıcı görüntü katmanlarına, orkestratörlere ve çalışma zamanı durumlarına taramayı genişleten birleşik bir platformdur. Gerçek zamanlı yanıt ve otomatik çözümler için gelişmiş analitik ve yerel YZ motorlarını kullanır.[13]

YZ'nin istismar geliştirmeyi çarpıcı biçimde hızlandırması ve güvenlik açığı ifşasından kamuya silahlandırılmasına kadar geçen süreyi günlerden saatlere indirmesi, savunma penceresinin kritik bir şekilde daraldığı anlamına gelmektedir. Bu durum, geleneksel haftalık veya aylık güvenlik açığı taramalarının hızla eskimesine ve kuruluşların savunmasız kalmasına yol açmaktadır. Bu nedenle, sürekli, YZ destekli güvenlik açığı taraması, yalnızca bir iyileştirme değil, 2025 yılında yaygın istismardan önce düzeltmeyi sağlamak için bir zorunluluk haline gelmiştir. Bu proaktif yaklaşım, ortaya çıkan YZ destekli tehditlerin önünde kalmak için hayati önem taşımaktadır.

2. Gelişmiş Gizli ve Kaçınmaya Dirençli TCP/UDP Tarama

   Modern host tarama, güvenlik duvarları, Saldırı Tespit Sistemleri (IDS) ve Saldırı Önleme Sistemleri (IPS) tarafından tespit edilmekten kaçınırken, hedefin saldırı

yüzeyini doğru bir şekilde haritalandırmak için sofistike teknikler kullanır. Bu, kısmi bağlantı taramalarını, paket manipülasyonunu ve aracı hostların kullanımını içerir.
Temel Teknikler ve Mekanizmalar:

- **TCP SYN Taraması (-sS Nmap'te):** Tam bir TCP bağlantısı kurmadan bir SYN paketi gönderen ve bir SYN-ACK yanıtı bekleyen popüler ve gizli bir aktif port tarama yöntemidir. Bu kısmi el sıkışma, hedef sistem tarafından günlüğe kaydedilme olasılığını azaltır.[18]
- **UDP Taraması (-sU Nmap'te):** UDP üzerinden çalışan hizmetleri (örneğin, DNS, SNMP) belirlemek için kullanışlıdır. Bağlantısız olduğu için, TCP taramalarına göre tespit edilmesi doğası gereği daha zordur. Güvenilirliği, hız sınırlaması ve yeniden denemelerle artırılabilir.[18]
- **Kaçınma Teknikleri:**
  - **Yem Kullanımı (-D Nmap'te):** Gerçek taramanın yanı sıra sahte IP adreslerinden sahte tarama trafiği gönderir, bu da tespit sistemlerinin gerçek kaynağı belirlemesini zorlaştırır.[18]
  - **Taramaları Yavaşlatma (--scan-delay Nmap'te):** Problar arasına gecikmeler eklemek, eşik tabanlı IDS kurallarının tetiklenmesini önlemeye yardımcı olur ve normal ağ trafiğini taklit eder.[18]
  - **Paketleri Parçalama (-f Nmap'te):** TCP paketlerini daha küçük parçalara böler, bu da paketleri düzgün bir şekilde yeniden birleştirmeyen basit IDS/IPS sistemlerini atlayabilir.[18]
  - **IP Boşta Tarama (-sI Nmap'te):** Boşta bir "zombi" hostu aracı olarak kullanır. Zombinin IP Kimliğindeki değişiklikleri gözlemleyerek, tarayıcı, saldırganın IP'sinden doğrudan etkileşim olmadan hedef portun durumunu çıkarabilir.[19]
  - **ACK Taraması (-sA Nmap'te):** Durumlu ve durumsuz güvenlik duvarlarını ayırt etmek için yalnızca ACK paketleri gönderir. Durumsuz güvenlik duvarları bunları geçirebilirken, durumlu olanlar ilişkili bir bağlantı olup olmadığını kontrol eder.[19]
  - **IPv6 Taraması:** Güvenlik duvarı yapılandırmalarındaki potansiyel gözden kaçmaları istismar eder, zira IPv6, IPv4'ten daha az sıkı bir şekilde izlenebilir.[19]

Araçlar:

- **Nmap:** Host keşfi, port taraması, hizmet tespiti ve işletim sistemi parmak izi için temel, tam özellikli bir araç olmaya devam etmektedir. Esnek betik yetenekleri sunar.[2]
- **Masscan:** En hızlı internet port tarayıcısı olarak tanımlanır ve büyük IP aralıklarını hızlı bir şekilde taramak için eşzamansız TCP paketleri gönderebilir, hızlı ilk değerlendirmeler için uygundur.[18]

- **Naabu:** Canlı hostları hızlı bir şekilde belirlemek için tasarlanmış hafif bir port tarayıcısıdır, ilk keşif ve diğer araçlarla entegrasyon için uygundur.[18]

[18] ve [18], saldırganlar tarafından IDS/IPS'den kaçınmak için kullanılan çeşitli kaçınma tekniklerini (yemler, parçalanma, taramaları yavaşlatma) detaylandırmaktadır. [19], güvenlik duvarı atlatma için Nmap'in IP Boşta ve ACK taramalarını daha da açıklamaktadır. Bu teknikler sadece saldırı amaçlı değildir. Siber güvenlik uzmanları için, bu gelişmiş kaçınma yöntemlerini sızma testleri sırasında anlamak ve simüle etmek [1], kendi ağ savunmalarının dayanıklılığını doğrulamak için kritik öneme sahiptir. Bir kuruluşun IDS/IPS'si veya güvenlik duvarı bu tekniklerle atlatılabiliyorsa, bu, ele alınması gereken önemli bir güvenlik açığına işaret eder. Bu durum, kaçınmayı saf bir saldırı taktiğinden, hayati bir savunma testi stratejisine dönüştürmektedir.

3. API Odaklı ve Bağlama Duyarlı Güvenlik Açığı Testi

   Bulut hizmetlerinin ve mikro hizmet mimarilerinin yaygınlaşmasıyla API'ler birincil saldırı yüzeyi haline gelmiştir. 2025'teki gelişmiş host tarama, gizli veya belgelenmemiş uç noktaları ve yanlış yapılandırmaları belirlemek için üretken YZ uygulamalarına güç verenler de dahil olmak üzere API'lerin özelleşmiş, bağlama duyarlı güvenlik açığı testini kapsar.

   Temel Özellikler ve Mekanizmalar:

   - **API Merkezli Tarama:** Bulut altyapıları temel olarak API'ler üzerine kuruludur ve çoğu bulut saldırısı API istismarı ve yanlış yapılandırmalara odaklanır.[10]
   - **Otomatik API Güvenlik Açığı Testi:** Çözümler, API güvenlik açıklarını sürekli olarak taramak için CI/CD işlem hatlarına entegre olur, manuel testlerin yerini alır ve geliştirme yaşam döngüsünün başlarında doğrulanmış kusurları tespit eder.[15]
   - **YZ Destekli ve Bağlama Duyarlı Analiz:** Araçlar, modern ve LLM API'lerini hedefleyenler de dahil olmak üzere sofistike, gerçek dünya saldırı senaryolarını simüle etmek için API mantığını anlar.[15]
   - **API Keşfi:** Bulut ortamlarında gölge ve belgelenmemiş API'ler de dahil olmak üzere tüm API'leri keşfetmek ve sınıflandırmak için çok önemlidir, geliştirme sürecinde kaçırılan API'lerin olasılığını en aza indirir.[15]
   - **Üretken YZ API Güvenliği:** Üretken YZ uygulamalarının hızlı yükselişi, artan saldırı yüzeyi, API çağrılarından veri sızıntısı ve hassas verilere yetkisiz erişim dahil olmak üzere yeni API güvenlik riskleri ortaya çıkarmaktadır.[21]

   Önde Gelen Araçlar:

   - **Pynt:** YZ destekli, bağlama duyarlı API güvenliği, otomatik API güvenlik açığı testi ve API Keşfi sunar.[15]
   - **Akto:** Özellikle mikro hizmetler ve bulut ortamları için gerçek zamanlı API envanteri ve güvenlik platformu sağlar, sürekli API envanteri ve gerçek zamanlı güvenlik açığı testi sunarak API güvenliğine odaklanır.[20]

- **Cloudflare API Keşfi:** Gerçek zamanlı API izleme ve güvenlik sunar, API kullanımını kaydeder ve güvenlik açıklarını tespit etmek için CI/CD işlem hatlarına entegre olur.[20]

[10], bulut altyapılarının API'ler üzerine kurulu olduğunu ve onları temel hale getirdiğini belirtmektedir. [21], kuruluşların %57'sinin API ile ilgili veri ihlalleri yaşadığını ve üretken YZ'nin API güvenliği için "ciddi ila aşırı risk" oluşturduğunu ortaya koymaktadır. Bu gerçekler, API'lerin artık sadece dahili bir bileşen olmadığını, bulut yerel ortamlarda kritik, açık bir "ağ çevresi" haline geldiğini göstermektedir. Geleneksel host tarama araçları, IP adresleri ve portlara odaklandığı için API'lerin güvenlik duruşunu tam olarak değerlendirmekte yetersiz kalmaktadır. Bu durum, 2025'teki etkili host taramanın, API mantığını anlayan, geliştirme iş akışlarına entegre olan ve YZ tarafından yönlendirilenler de dahil olmak üzere API etkileşimlerine özgü riskleri belirleyebilen özel API keşif ve güvenlik açığı test araçlarını içermesi gerektiğini göstermektedir. Bu, "host tarama" çabalarının yoğunlaşması gereken yerde temel bir kaymayı temsil etmektedir.

B. Gelişmiş Güvenlik Duvarı Tespiti ve Atlatma

4. Yeni Nesil Güvenlik Duvarı (NGFW) Tanımlama ve Politika Analizi
   2025 yılında güvenlik duvarları, temel paket filtrelemeden sofistike Yeni Nesil Güvenlik Duvarlarına (NGFW) doğru evrilmektedir. Gelişmiş host tarama teknikleri artık NGFW yeteneklerini tanımlamalı ve derin paket denetimi, saldırı önleme ve gerçek zamanlı tehdit istihbaratı gibi karmaşık politikalarını analiz etmelidir. Bu yetenekler genellikle YZ/ML tarafından desteklenmektedir.
   Temel Özellikler ve Mekanizmalar:
   - **Gelişmiş Yetenekler:** NGFW'ler, derin paket denetimi (DPI), saldırı önleme sistemleri (IPS), uygulama kontrolü ve gerçek zamanlı tehdit istihbaratı sunarak, yalnızca temel kriterlere göre veri bloklayan veya izin veren geleneksel güvenlik duvarlarının ötesine geçer.[22]
   - **YZ/ML Entegrasyonu:** YZ ve Makine Öğrenimi, NGFW yeteneklerini yeniden şekillendirerek sıfır gün tehditlerinin hassas bir şekilde tespit edilmesini ve engellenmesini, trafik analizinin ve anomali tespitinin otomatikleştirilmesini sağlar.[23]
   - **Kullanıcı Varlık Davranış Analizi (UEBA):** NGFW'ler, davranış kalıplarını analiz ederek ve anormallikleri işaretleyerek içeriden gelen tehditleri ve şüpheli etkinlikleri tespit etmek için UEBA ile yeteneklerini artırmaktadır.[23]
   - **Politika En İyi Uygulamaları:** Etkili NGFW uygulaması, açık, rol tabanlı erişim kurallarının tanımlanmasını, "tümünü reddet, istisnaları izin ver" yaklaşımının kullanılmasını, politikaların düzenli olarak gözden geçirilmesini ve güncellenmesini, ayrıca günlük kaydı ve izlemenin uygulanmasını içerir.[22]
   - **Çok Katmanlı Güvenlik:** NGFW'ler, uç nokta koruması, saldırı tespiti ve antivirüs çözümleriyle entegre edilir ve ağ segmentasyonu ile Sıfır Güven

ilkelerini destekler.[22]

Önde Gelen Araçlar:

- **Cisco Firepower Yönetim Merkezi, Fortinet FortiManager, Palo Alto Networks Panorama, Check Point Güvenlik Yönetimi, Juniper Networks Security Director, Sophos Central, Barracuda CloudGen Güvenlik Duvarı Kontrol Merkezi, McAfee ePolicy Orchestrator (ePO), SonicWall Global Yönetim Sistemi (GMS), WatchGuard Firebox Sistem Yöneticisi (WSM):** Bunlar, merkezi yönetim, gelişmiş tehdit önleme ve politika otomasyonu sunan önde gelen ticari NGFW çözümleridir.[28]
- **IBM QRadar Güvenlik İstihbarat Platformu, Tufin Orkestrasyon Paketi, FireMon Security Manager, AlgoSec Güvenlik Yönetim Paketi:** Bu araçlar, karmaşık güvenlik duvarı ortamları için gelişmiş güvenlik istihbaratı, otomatik güvenlik politikası yönetimi, uyumluluk denetimi ve ağ topolojisi görselleştirmesi sağlar.[28]

NGFW'lerin derin paket denetimi, IPS, uygulama kontrolü ve YZ/ML destekli sıfır gün tehdit tespiti gibi gelişmiş özellikler entegre ettiği göz önüne alındığında, 2025'teki bir host taraması için sadece bir güvenlik duvarının varlığını veya bir portun açık olup olmadığını belirlemek yetersiz kalmaktadır. Daha derin bir analiz, host tarama tekniklerinin NGFW'nin politika uygulama sofistikasyonunu ve gerçek zamanlı tehdit istihbarat yeteneklerini değerlendirecek şekilde evrilmesi gerektiğini göstermektedir. Bu, temel port taramasının ötesine geçerek, uygulama kontrollerini atlatma girişimlerini, SSL denetimini test etmeyi ve NGFW'nin YZ/ML bileşenlerinin bilinen kaçınma kalıplarına nasıl tepki verdiğini analiz etmeyi içermektedir. Bu durum, temel güvenlik duvarı *tanımlamasından* ayrıntılı güvenlik duvarı *duruş değerlendirmesine* doğru bir geçişi işaret etmektedir.

5. TLS Parmak İzi (JA3/JA4) ile Gizli Güvenlik Duvarı Tespiti ve Kaçınma

TLS parmak izi, özellikle JA3 ve JA4 hash'leri kullanılarak, bir istemcinin TLS el sıkışmasının benzersiz özelliklerini tanımlayan sofistike bir tekniktir. Güvenlik duvarları bu parmak izlerini kötü amaçlı trafiği (örn. botnetler, DDoS saldırıları) tespit etmek ve kısıtlamak için kullanırken, gelişmiş tarama araçları tespit edilmekten kaçınmak için meşru istemci profillerini taklit etmek için bunları kullanabilir.

Temel Özellikler ve Mekanizmalar:

- **Benzersiz İstemci Tanımlama:** JA3 ve JA4, bir TLS istemci hello paketinin (TLS sürümü, desteklenen şifreleme paketleri, dahil edilen uzantılar) ayrıntılarını benzersiz bir hash'e dönüştürür. Bu hash, erişimi izlemek ve kısıtlamak için bir parmak izi görevi görür.[30]
- **Güvenlik Duvarı Uygulaması:** Vercel gibi güvenlik duvarları, bu TLS parmak izlerini, birden fazla IP'ye veya kullanıcı aracısına yayılmış DDoS saldırıları gibi sofistike saldırıları tanımlamak ve engellemek veya bot trafiğini önlemek için

kullanır.[30]

- **Ayrıntılı Ağ Parmak İzi:** JA4, JA4+ paketinin bir parçası olarak, ağ parmak izi için daha ayrıntılı ve esnek bir yaklaşım sunar, kötü amaçlı trafiğin ve bot etkinliğinin daha iyi azaltılmasına yardımcı olur. Sunucu tarafı şifreli ağ trafiğini tanımlayabilir, izleyebilir ve kategorize edebilir.[30]
- **İstek Başlıkları:** Bu parmak izleri, işlevler veya uygulamalar tarafından istek başlıklarından (örn. x-vercel-ja4-digest) okunabilir, bu da istemcinin TLS profiline göre gerçek zamanlı işlem ve yanıt sağlar.[30]

[30] ve [30], güvenlik duvarlarının (Vercel'inki gibi) JA3/JA4 TLS parmak izlerini kullanarak botnetler ve DDoS saldırıları dahil olmak üzere kötü amaçlı trafiği nasıl tespit edip engellediğini, TLS istemci hello paketlerinden benzersiz hash'ler oluşturarak sürekli olarak açıklamaktadır. Aynı zamanda, [35], TCP/IP yığını parmak izinin (TLS parmak izini de içerir) güvenlik ekipleri tarafından yetkisiz cihazları tespit etmek için kullanıldığını belirtmektedir. Bu durum, kritik bir "çift kullanımlı" dinamik olduğunu göstermektedir. Daha derin bir anlayış, savunmacılar TLS parmak izini sofistike tespit için kullanırken, gelişmiş saldırganların (ve dolayısıyla gelişmiş tarama araçlarının) bu savunmaları atlatmak için meşru TLS parmak izlerini analiz etme ve taklit etme yeteneğine sahip olması gerektiğidir. Bu, host taramayı temel ağ problarının ötesine, kriptografik el sıkışma analizinin bir katmanına yükseltmekte ve hem gizli operasyonlar hem de sağlam savunma için bu parmak izlerini oluşturma ve analiz etme yeteneğinin anahtar olduğunu vurgulamaktadır.

6. Otomatik Güvenlik Duvarı Kuralı Numaralandırma ve Çıkarım Teknikleri
   Karmaşık, dinamik ağlar için güvenlik duvarı kurallarının manuel denetimi artık ölçeklenebilir veya etkili değildir. 2025'teki gelişmiş host tarama, güvenlik duvarı politikalarını numaralandırmak, analiz etmek ve çıkarmak için otomatik araçlar ve teknikler kullanır; yanlış yapılandırmaları, yedekli kuralları ve istismar edilebilecek potansiyel atlatmaları belirler.
   Temel Özellikler ve Mekanizmalar:
   - **Politika Yönetimi En İyi Uygulamaları:** Varsayılan olarak tüm trafiği engelleyerek ve yalnızca gerekli bağlantılara izin vererek En Az Ayrıcalık İlkesi'ni (PoLP) uygulamayı, kritik hizmetlere erişimi kısıtlamayı ve güvenlik duvarı yapılandırmalarına yönetici erişimini sınırlamayı vurgular.[27]
   - **Yapılandırılmış Kural Kümeleri:** Daha kolay anlama, denetim ve değişiklik için kuralların açık kategorilere (İzin Ver, Reddet, Günlük Kaydı, Geçici) ayrılmasını ve uygun şekilde belgelenmesini savunur.[27]
   - **Düzenli Denetimler ve Güncellemeler:** Eskimiş veya yedekli kuralları kaldırmak ve politikaları değişen iş ihtiyaçları ve ortaya çıkan tehditlerle uyumlu hale getirmek için periyodik incelemelerin (örn. üç ayda bir) gerekliliğini vurgular.[22]

- **Optimizasyon için Otomatik Araçlar:** Otomatik güvenlik duvarı yönetimi araçları, denetim sürecini kolaylaştırır, yedekli kuralları belirler, optimizasyonlar önerir ve performansı artırır, böylece manuel hataları azaltır ve daha güvenli bir kurulum sağlar.[22]
- **Trafik Günlüğü Analizi:** Ağ trafik günlüklerini incelemek ve güvenlik analitiği kullanmak, hangi kuralların aktif olarak kullanıldığını belirlemeye yardımcı olur ve güvenlik duvarı politikalarındaki zayıf noktaları vurgular.[22]
- **Kural Sırası Önceliklendirmesi:** Güvenlik duvarları kuralları yukarıdan aşağıya doğru sırayla işler. Bu nedenle, kasıtsız trafik akışını önlemek için doğru önceliklendirme (daha geniş kurallardan önce belirli izin verme kuralları, reddetme kurallarının stratejik yerleşimi) çok önemlidir.[27]
- **Durum Denetimi:** Modern güvenlik duvarları, aktif bağlantıların durumunu izlemek ve yalnızca meşru trafiğe izin vermek için durum denetimi kullanır, bu da analizde dikkate alınmalıdır.[24]

Araçlar:

- **Tufin Orkestrasyon Paketi, FireMon Security Manager, AlgoSec Security Management Suite:** Bu araçlar, karmaşık ağlarda güvenlik politikası değişikliklerini otomatikleştirmek, sürekli politika izleme, uyumluluk denetimi ve güvenlik duvarı kuralı optimizasyonunda uzmanlaşmıştır.[28]
- Şüpheli etkinliklere dayalı gerçek zamanlı uyarılar için otomatik araçlar ve merkezi günlük yönetimi için SIEM sistemleriyle entegrasyon da kritik öneme sahiptir.[22]

[22] ve [22], "düzenli güvenlik duvarı denetimleri ve kural temizliği" ile "otomatik güvenlik duvarı yönetimi araçlarının" kritik ihtiyacını vurgulamaktadır. Ayrıca, kural kümelerinin karmaşıklığını, en az ayrıcalık ilkesini ve trafik günlüklerinin önemini de belirtmektedirler. Daha derin bir anlayış, ağların dinamik doğası ve NGFW politikalarının artan karmaşıklığı göz önüne alındığında, manuel güvenlik duvarı kural incelemesinin eskimeye başladığıdır. Bunun yerine, 2025'teki gelişmiş host tarama teknikleri, güvenlik duvarı kurallarının ve politikalarının *otomatik çıkarımına* doğru kaymalıdır. Bu, ağ davranışını [26], trafik kalıplarını ve günlük verilerini analiz ederek aktif kuralları dinamik olarak haritalandırmayı, yanlış yapılandırmaları belirlemeyi ve hatta potansiyel atlatmaları tahmin etmeyi içermekte ve "bu port açık mı?" gibi reaktif bir yaklaşımdan "bu güvenlik duvarı nasıl davranıyor ve doğal zayıflıkları nelerdir?" gibi proaktif bir yaklaşıma geçişi sağlamaktadır.

C. Dinamik MAC Adresi ve Cihaz Parmak İzi

7. YZ Destekli Cihaz Parmak İzi ve MAC Sahtekarlığı Tespiti
   IoT cihazlarının yaygınlaşması ve MAC sahtekarlığı saldırılarının artan karmaşıklığı ile 2025'teki gelişmiş host tarama, basit MAC adresi tespitinin ötesine geçmektedir. Bu, ağ trafiğini izleyen, zengin bir cihaz özellik kümesi toplayan ve

MAC sahtekarlığını doğru bir şekilde tespit etmek ve cihaz türlerini ve rollerini belirlemek için güven puanlaması kullanan YZ destekli cihaz parmak izini içerir.
Temel Özellikler ve Mekanizmalar:

- **Cihaz Parmak İzi Verisi Üretimi:** Ağ trafiğini izleyerek MAC adresleri ve bir dizi özellik içeren cihaz parmak izi verileri oluşturmayı içerir. Bu, pasif taramalar (normal çalışma sırasında mesaj başlıklarından veri türetme) veya aktif taramalar (belirli yanıtları tetiklemek için mesaj iletme) yoluyla yapılabilir.[31]
- **MAC Sahtekarlığı Tespiti:** Sistem, bu parmak izi verilerine dayanarak iki veya daha fazla cihazın ortak bir MAC adresi kullanıp kullanmadığını belirler. Ayrıca, yazılım güncellemeleri veya MAC adresi yeniden atamaları nedeniyle tek bir cihazın birden fazla kaydı olabileceği durumları da dikkate alır ve yanlış pozitifleri azaltmak için MAC adresi kullanım istatistiklerini (kullanım zamanları, kullanım ağı) kullanır.[31]
- **Özellik Türetme:** DHCP mesajları (Seçenekler 55, 60, host adı) ve HTTP kullanıcı ajanları, işletim sistemi, sürüm, yazılım, eklentiler ve cihaz modeli gibi cihaz özelliklerini belirlemek için işlenir.[31]
- **Güven Puanlaması:** Bir güven puanı, MAC sahtekarlığı olasılığını gösterir ve önceden belirlenmiş eylemler (örn. iletişimi engelleme, uyarı oluşturma) yalnızca bu puan bir eşiği aşarsa tetiklenir. Her kayıt, veri miktarı, mesaj sayısı ve çıkarım yöntemine göre bir "parmak izi güven puanına" da sahip olabilir.[31]
- **Cihaz Tanımlama:** Ağ keşif araçları tipik olarak ping taramaları veya ARP istekleri kullanarak IP aralıklarını tarayarak başlar. Bir cihaz yanıt verdiğinde, SNMP, NetBIOS gibi protokoller kullanarak MAC adresi, host adı, işletim sistemi ve donanım türü gibi öznitelikleri sorgulayarak onu sınıflandırmaya çalışır.[4]
- **Rol Çıkarımı:** Parmak izi teknikleri, cihaz türlerini ve rollerini (örn. yazıcı, yönlendirici, cep telefonu) çıkarır, bu da yetkisiz veya kötü niyetli uç noktaların belirlenmesine yardımcı olur.[4]

[31] ve [31], YZ destekli cihaz parmak izi kullanarak MAC sahtekarlığı tespitine yönelik bir patenti detaylandırmakta olup, bu patent sadece MAC adresinin ötesinde çeşitli cihaz özelliklerini (OS, yazılım, donanım) toplamakta ve güven puanlaması uygulamaktadır. [4] ve [4], ağ keşif araçlarının bu özelliklerden cihaz türlerini ve rollerini nasıl çıkardığını açıklamaktadır. IoT cihazlarının hızla yayılması [6] ve saldırganların artan sofistikasyonu göz önüne alındığında, statik bir MAC adresi aramasının güvenlik için yetersiz olduğu anlaşılmaktadır. Bunun yerine, 2025'teki host tarama, sadece MAC sahtekarlığı tespitini değil, aynı zamanda ayrıntılı erişim kontrolünü, davranışsal anomali tespitini ve Sıfır Güven ilkelerinin uygulanmasını sağlayan *dinamik, zengin cihaz profilleri* oluşturmak için YZ'yi kullanmalıdır. Bu, basit cihaz tanımlamasından, çeşitli ve potansiyel olarak güvenilmeyen uç noktaları yönetmek için kritik olan sürekli, akıllı cihaz duruş değerlendirmesine doğru bir geçişi ifade etmektedir.

8. Davranışsal İşletim Sistemi Parmak İzi ve Kaçınmaya Dirençli Tespit
   Geleneksel işletim sistemi parmak izi yöntemleri kaçınma tekniklerine (örn. paket rastgeleleştirmesi, tarayıcı sahtekarlığı) karşı savunmasız hale geldikçe, odak noktası davranışsal işletim sistemi parmak izine kaymaktadır. Bu, sürekli kimlik doğrulama ve dolandırıcılık tespiti için daha sağlam, kaçınmaya dirençli cihaz profilleri oluşturmak amacıyla dinamik kullanıcı ve sistem davranışlarını YZ/ML ile birleştirerek analiz etmeyi içerir.
   Temel Özellikler ve Mekanizmalar:
   - **Geleneksel İşletim Sistemi Parmak İzi:** Farklı işletim sistemlerinin ağ protokollerini (TCP/IP yığını) nasıl uyguladığına dair nüanslara dayanarak işletim sistemini tanımlar; TTL, TCP seçenekleri ve Parçalamama (DF) bitleri gibi özellikleri analiz eder. Bu, aktif (hazırlanmış paketler, örn. Nmap) veya pasif (mevcut trafiği gözlemleme, örn. p0f) olabilir.[17]
   - **Kaçınma Zorlukları:** Tespit sistemleri, botlara özgü kalıpları tanımak için makine öğrenimi modelleri kullanır ve kullanıcı aracılarını veya proxy'leri döndürmek gibi temel hileleri yetersiz kılar. Saldırganlar, tarayıcı parmak izi sahtekarlığı (Canvas, WebGL, ses parmak izi), WebRTC sızıntıları, DNS sızıntıları ve paket yapılarını rastgeleleştiren işletim sistemi düzeyindeki araçlar gibi teknikler kullanır.[33]
   - **Davranışsal Biyometri:** Sürekli kimlik doğrulama için ideal olan, kullanıcının kimliğini arka planda sürekli olarak doğrulamak için yazma ritmi, fare hareketi ve yürüyüş gibi kalıpları analiz eder.[9]
   - **Yüksek Entropili Davranışsal Parmak İzleri:** Davranışsal girdiler, benzer donanımlarda bile kullanıcılar arasında çakışma olasılığı daha düşük olan ve sahtekarlığa karşı daha sağlam parmak izleri oluşturur.[9]
   - **ML Destekli Analiz:** Makine öğrenimi algoritmaları, organik varyasyonu şüpheli etkinlikten daha doğru bir şekilde ayırt etmek, yanlış pozitifleri azaltmak ve yeni dolandırıcılık taktiklerine uyum sağlamak için parmak izi verileri üzerinde eğitilmiştir.[37]
   - **Uyarlanabilir Güvenlik Önlemleri:** Bir cihaz veya kullanıcıyla ilişkili risk seviyesine göre güvenlik protokolleri dinamik olarak ayarlanabilir.[37]

[32], statik TCP/IP yığını özelliklerine dayalı geleneksel işletim sistemi parmak izini tanımlamaktadır. Ancak, [33] ve [35], bu statik yöntemleri güvenilmez kılan çok sayıda kaçınma tekniğini (örn. tarayıcı parmak izi, WebRTC sızıntıları, paket rastgeleleştirmesi) detaylandırmaktadır. [36] ve [9], "cihaz zekasının bir sonraki sınırı" olarak "davranışsal biyometri" ve "davranışsal parmak izi"ni tanıtmakta olup, bunlar daha sağlam, kaçınmaya dirençli profiller oluşturmak için dinamik kullanıcı etkileşimlerini (yazma ritmi, fare hareketi) analiz etmektedir. [37] ve [38], dolandırıcılık tespitinde ve yanlış pozitiflerin azaltılmasında ML'nin rolünü daha da vurgulamaktadır. Bu durum, saldırganlar statik işletim sistemi imzaları için daha sofistike kaçınma teknikleri

geliştirdikçe, savunmacıların doğru ve kaçınmaya dirençli cihaz tanımlamasını sürdürmek için dinamik, davranışsal analize, genellikle YZ/ML destekli analize geçmesi gerektiğini göstermektedir. Bu, host taramayı sadece işletim sistemini tanımlamaktan, işletim sisteminin ve kullanıcısının *davranışsal bütünlüğünü* sürekli olarak doğrulamaya doğru kaydırmaktadır.

D. Ortaya Çıkan Saldırı Yüzeyi ve Özelleşmiş Tarama

9. Bulut, Kapsayıcı ve Sunucusuz Ortam Taraması
   Bulut yerel ortamların (IaaS, PaaS, SaaS, kapsayıcılar, sunucusuz işlevler) dinamik, geçici ve dağıtık doğası, geleneksel host tarama yöntemlerini yetersiz kılmaktadır. 2025'te, özelleşmiş tarama teknikleri, API tabanlı varlık keşfine, kapsayıcı görüntü bütünlüğüne ve sunucusuz işlevlerin çalışma zamanı analizine odaklanarak güvenliği CI/CD işlem hattına entegre etmektedir.
   Temel Özellikler ve Mekanizmalar:
   - **Bulut Varlık Keşfi:** Gölge BT'yi tespit etmek ve güvenlik politikalarını uygulamak için ağ trafiğini analiz eden Bulut Erişim Güvenliği Aracılarından (CASB'ler) SaaS keşfi için yararlanır. API bağlayıcıları da merkezi görünürlük için çeşitli SaaS satıcı portallarından veri toplar.[39]
   - **Aracısız/Aracı Tabanlı Keşif:** Modern BT varlık keşif araçları, ağ protokollerini (SNMP, SSH, WMI) kullanarak BT varlıklarını tarar veya şirket içi, bulut ve IoT ortamlarında yapılandırma ve durum bilgisi toplamak için yazılım aracıları dağıtır.[4]
   - **Kapsayıcı Güvenlik Açığı Taraması:** Dockerfile'ları, temel işletim sistemi katmanlarını inceleyerek ve kod bağımlılıklarını CVE veritabanlarıyla karşılaştırarak kapsayıcı görüntülerindeki ve bağımlılıklarındaki (eskimiş/kötü amaçlı paketler, yanlış yapılandırmalar) güvenlik risklerini belirlemeye odaklanır.[14]
   - **Gerçek Zamanlı Kapsayıcı İzleme:** Araçlar, CVE beslemelerini gerçek zamanlı olarak izler, geliştiricilere otomatik geri bildirim ve otomatik oluşturulmuş düzeltmeler (örn. temel görüntü yükseltmeleri) sağlar ve taramayı geliştirme süreçlerine entegre eder.[14]
   - **Sunucusuz Güvenlik Taraması:** Kısa ömürlü işlevlerin benzersiz zorluklarını ele alır. Odak noktası, ağ denetiminden kod korumasına, aşırı ayrıcalıklı IAM rollerini, zehirlenmiş bağımlılıkları, düz metin sırlarını ve kilitsiz API ağ geçitlerini yönetmeye kayar.[11]
   - **Sunucusuz En İyi Uygulamalar:** Asgari izinler (en az ayrıcalık) verilmesini, tüm girdilerin doğrulanmasını, özel sır yönetimi hizmetlerinin kullanılmasını, hız sınırlaması uygulanmasını ve izleme, günlük kaydı ve izlemenin önceliklendirilmesini vurgular.[11]

- **Sunucusuz için Aracısız Tarama:** Doğrudan host erişimi olmadan bile sunucusuz kapsayıcı süreçlerine ve çalışma zamanı ortamlarına tam görünürlük elde etmek için hayati öneme sahiptir.[43]

Önde Gelen Araçlar:

- SaaS ve bulut varlık keşfi için CASB platformları (örn. Zluri, Lansweeper, Invgate).[39]
- Kapsayıcı tarama araçları: SentinelOne Singularity™ Cloud Security, Snyk Container, Aqua Trivy, Anchore, Prisma Cloud (Palo Alto Networks), Tenable.io Container Security, Clair, Aikido.[14]
- Sunucusuz ortamlar için bağımlılık taraması için bulut yerel güvenlik çözümleri (örn. AWS CodeGuru, GitHub Advanced Security, Defender for Cloud, Google Artifact Analysis).[11]

[10] ve [43], bulut, kapsayıcı ve sunucusuz ortamların geçicilik, dağıtıklık ve API odaklı etkileşimlerle karakterize edildiğini topluca göstermektedir. Geleneksel "host" kavramları (sabit bir IP, kalıcı bir işletim sistemi) burada büyük ölçüde geçerliliğini yitirmiştir. Daha derin bir anlayış, 2025'teki host taramanın artık sadece IP aralıklarını taramakla ilgili olmadığı, aynı zamanda geçici kapsayıcıları, sunucusuz işlevleri ve API'leri içerecek şekilde "host" kavramının temelden yeniden tanımlanması gerektiğidir. Bu, sadece ağ düzeyindeki problardan ziyade kod bütünlüğü, yapılandırma (IAM rolleri, sırlar), API davranışı ve çalışma zamanı analizine odaklanan özel tarama yöntemlerini gerektirmektedir. Bu durum, modern BT altyapılarında "host keşfi"nin nasıl kavramsallaştırıldığı ve yürütüldüğünde bir paradigma kaymasını ifade etmektedir.

10. Hizmet Sürümü Tespiti Obfuskasyonu ve De-obfuskasyon Teknikleri
Saldırganlar, kötü amaçlı hizmetleri gizlemek, sürümlerini belirsizleştirmek ve tespitten kaçınmak için giderek daha sofistike obfuskasyon teknikleri (örn. kod dönüşümü, bellek içi implantlar, AMSI atlatmaları) kullanmaktadır. 2025'teki gelişmiş host tarama, bu gizli tehditleri ortaya çıkarmak ve tehlikeye atılmış hizmetleri doğru bir şekilde tanımlamak için de-obfuskasyon tekniklerini (genellikle YZ destekli) ve bellek tabanlı tespiti içermektedir.
Temel Özellikler ve Mekanizmalar:
    - **Kod Obfuskasyonu:** Program anlamayı engellemek ve fikri mülkiyeti korumak için kontrol akışı düzleştirme, karma Boolean-Aritmetik ve sanal makineler gibi teknikler kullanılır, bu da tersine mühendisliği zorlaştırır.[44]
    - **AMSI Atlatma:** Saldırganlar, imzaları önlemek için kodu değiştirerek, DLL işlevselliğini bozarak veya DLL yüklemesini engelleyerek Antimalware Scan Interface (AMSI) sistemini atlatır. Bu genellikle dize obfuskasyonu/şifrelemesi, anti-emülasyon ve anti-sandbox tekniklerini içerir; tespit, atlatma kodu imzalarına veya çalışma zamanı tespitlerine (kullanıcı alanı kancaları, ETWti, bellek taramaları) dayanır.[45]

    - **Bellek İçi İmplantlar:** Dosyasız kötü amaçlı yazılımlar (örn. TRAILBLAZE, BRUSHFIRE) yalnızca geçici bellekte bulunur, geleneksel disk tabanlı tespit mekanizmalarını atlar ve minimum iz bırakır.[46]
    - **YZ/ML ile De-obfuskasyon:** Öncü yaklaşımlar, sofistike obfuskasyonu atlatmak için imza tabanlı eşleştirmeyi (örn. Android uygulamaları için DalvikFLIRT) LLM destekli kod dönüşümü ile birleştirir, bu da daha önce aşılamayan kodun otomatik güvenlik analizini sağlar.[47]
    - **Bellek Tabanlı Tespit:** Yetkisiz süreç enjeksiyonları, DLL yan yüklemeleri veya düzensiz API çağrıları gibi şüpheli etkinlikler için RAM'i izleyen araçlar, dosyasız saldırıları tespit etmek için kritik öneme sahiptir.[49]

[45] ve [44], saldırganların kötü amaçlı hizmetleri ve sürümlerini gizlemek, onları geleneksel host tarama yöntemlerine [18] "görünmez" kılmak için giderek daha sofistike obfuskasyon, bellek içi implantlar ve atlatma teknikleri (AMSI atlatma gibi) kullandığını topluca göstermektedir. Bu eğilim, host taramanın yüzeysel ağ düzeyindeki problardan derin kod ve bellek analizine kaymasını zorunlu kılmaktadır. Araçlar, gizli hizmetleri ortaya çıkarmak, gerçek sürümlerini belirlemek ve tespitten aktif olarak kaçınmaya çalışan kötü amaçlı kodu tespit etmek için gelişmiş de-obfuskasyon tekniklerini [47] ve bellek adli tıpını içermelidir. Bu durum, 2025'teki "host tarama"nın, geleneksel yöntemlerle tespit edilemeyecek şekilde tasarlanmış tehditleri bulmak için tersine mühendislik ve çalışma zamanı analizi alanına uzandığı anlamına gelmektedir.

IV. 2025 Host Taramasını Yönlendiren Temel Teknolojiler ve Araçlar

Bu bölüm, 2025 yılında host tarama ve güvenlik açığı değerlendirmesinde öncü olan lider ticari ve açık kaynaklı araçlara genel bir bakış sunmaktadır. YZ ve Makine Öğrenimi platformlarının bu yetenekleri geliştirmedeki dönüştürücü rolü vurgulanacaktır.

Temel ve Gelişen Araçlar

- **Nmap (Network Mapper):** Ağ keşfi, güvenlik denetimi, host keşfi, port taraması, hizmet tespiti ve işletim sistemi parmak izi için temel, ücretsiz ve açık kaynaklı bir araç olmaya devam etmektedir. Büyük ölçekli taramayı destekler, Nmap Betik Motoru (NSE) aracılığıyla esnektir ve TCP/IP yığını parmak izi sunar.[1]
- **Wireshark:** Derin paket denetimi, anormalliklerin belirlenmesi, ağ sorunlarının giderilmesi ve kötü amaçlı etkinliklerin tespiti için paha biçilmez bir ağ protokol analizcisidir.[2]
- **Masscan ve Naabu:** Nmap'i hızlı, büyük ölçekli port taraması için tamamlar, ilk keşif için hızı önceliklendirir.[18]

Yeni Nesil Güvenlik Açığı Tarayıcıları

- **Nessus:** Tenable'dan güçlü bir tescilli güvenlik açığı tarayıcısıdır. Çeşitli sistemler ve ağlardaki güvenlik risklerini belirlemek için yaygın olarak kullanılır ve derinlemesine tarama, uyumluluk denetimi ve tehdit tespiti sunar.[2]
- **OpenVAS:** Ağlar, sistemler ve uygulamalardaki güvenlik zayıflıklarını belirlemek için tasarlanmış açık kaynaklı bir güvenlik açığı tarayıcısıdır (Greenbone Güvenlik Yönetimi'nin bir parçasıdır) ve düzenli olarak güncellenen beslemeler ve CVE kapsamı sunar.[15]
- **Pynt:** Otomatik, bağlama duyarlı API güvenlik açığı testi ve keşfi için proaktif bir YZ destekli API Güvenliği çözümüdür.[15]
- **Qualys VMDR, Rapid7 InsightVM, Tenable Vulnerability Management/Security Center:** Kapsamlı güvenlik açığı değerlendirmesi, maruziyet yönetimi ve saldırı yüzeylerini azaltmak ve tehditleri ortadan kaldırmak için YZ destekli analizler sunan önde gelen ticari platformlardır.[16]

Ağ Keşfi ve Topoloji Haritalama Araçları

- **Auvik Ağ Yönetimi:** Gerçek zamanlı ağ haritalama ve keşif yetenekleri sunar. SNMP, ICMP, CDP ve LLDP kullanarak ağ topolojisinin port düzeyine kadar etkileşimli, görsel haritalarını otomatik olarak oluşturur. Topolojiyi gerçek zamanlı olarak sürekli tarar ve günceller.[50]
- **LiveAction LiveNX:** Gerçek zamanlı ağ topolojisi haritalama ve güvenlik görselleştirmesi sağlar. Otomatik cihaz keşfini sürekli izleme ile birleştirerek yönlendirme, trafik kalıpları veya cihaz kullanılabilirliğindeki değişiklikleri hızlı bir şekilde belirler.[53]
- **ManageEngine OpManager, Paessler PRTG, Site24x7, JDisc Discovery, NetBrain, Faddom:** Performans grafikleri, eşik uyarıları ve dinamik ağ haritaları gibi özelliklerle uçtan uca ağ izleme, BT varlık yönetimi ve keşfi sunar.[4]

YZ ve Makine Öğrenimi Platformlarının Dönüştürücü Rolü

YZ ve ML, tehdit tespiti, yanıt süreleri ve gelecekteki ihlalleri tahmin etme ve önleme yeteneğini artırmaktadır.[5]

- **Tahmine Dayalı Tehdit Tespiti:** YZ, büyük veri kümelerini gerçek zamanlı olarak analiz ederek, potansiyel tehditleri ortaya çıkmadan önce tahmin etmek için kalıpları ve anormallikleri belirler.[6]
- **Otomatik Olay Yanıtı:** YZ sistemleri, tespit edilen tehditlere (örn. sistemleri izole etme, IP'leri engelleme) otomatik olarak yanıt başlatır ve yanıt sürelerini önemli ölçüde azaltır.[5]
- **Gerçek Zamanlı Ağ Analizi ve Anomali Tespiti:** Ağ etkinliklerinin sürekli

izlenmesi, olağandışı davranışların hızlı bir şekilde tespit edilmesini sağlar, şüpheli oturum açma girişimlerini veya beklenmedik dosya transferlerini işaretler.[6]
- **YZ Destekli Anomali Tespiti:** Ağ trafiğini ve kullanıcı davranışını izleyerek, YZ normal etkinlik kalıplarından sapmaları tespit eder, yetkisiz erişim veya kötü amaçlı yazılım sızmasına işaret eder.[55]

Önde Gelen YZ Destekli Güvenlik Platformları:

- **SentinelOne (Purple AI, Singularity Hyperautomation, AI-SIEM, Singularity Data Lake, Singularity VM, Singularity Cloud Security):** Uç nokta, bulut, XDR ve sanal makine için birleşik mimari sunar; gerçek zamanlı yanıt, otomatik önleme ve tespit sağlar.[13]
- **Vectra AI Platform, Darktrace / NETWORK, ExtraHop RevealX, Gatewatcher NDR Platform, Stellar Cyber Open XDR Platform, ThreatBook Threat Detection Platform, Cisco Secure Network Analytics:** Bunlar, hibrit saldırı tespiti, soruşturma ve çeşitli ortamlarda yanıt için YZ'den yararlanan önde gelen Ağ Tespiti ve Yanıtı (NDR) ve Genişletilmiş Tespit ve Yanıtı (XDR) platformlarıdır.[56]
- **Google Chronicle Security Operations, Microsoft Defender XDR, Palo Alto Cortex XDR:** Anomali tespiti ve uç noktalar, ağlar ve bulut genelinde proaktif tehdit tespiti için YZ'yi entegre eden bulut tabanlı SIEM ve XDR çözümleridir.[57]

YZ destekli tehditlerin hacmi ve hızı, güvenliği ayrı araçlarla yönetmeyi pratik olmaktan çıkarmaktadır. Bu durum, host tarama verileri de dahil olmak üzere çeşitli kaynaklardan gelen verileri ilişkilendirebilen, bütünsel bir görünüm sağlayabilen ve otomatik, gerçek zamanlı tehdit tespiti ve yanıtı sağlayabilen YZ destekli, entegre platformlara doğru bir pazar konsolidasyonunu tetiklemektedir. Bu, tek tek araçların önemli olmaya devam etse de, değerlerinin giderek bu daha geniş, YZ odaklı güvenlik ekosistemlerine entegrasyonları aracılığıyla gerçekleştiği anlamına gelmektedir.

Tablo 2: Önde Gelen Host Tarama ve Güvenlik Açığı Değerlendirme Araçlarının Karşılaştırmalı Analizi (2025)

Araç Adı / Platform	Sağlayıcı	Temel Özellikler	YZ/ML Entegrasyonu	Hedef Ortam(lar)	Dikkat Çeken Yetenekler
Nmap	Açık Kaynak	Host keşfi, port taraması, hizmet/OS tespiti, betiklenebilir	Sınırlı (NSE betikleri aracılığıyla)	Şirket içi, Ağ	Ağ keşfi için temel, yüksek düzeyde özelleştirilebi

		(NSE), esnek çıktı.			lir.
Nessus	Tenable	Güvenlik açığı taraması (OS, ağ, web uygulamaları, bulut), kimlik bilgileriyle/kimlik doğrulaması yapılmamış taramalar, uyumluluk denetimi.	YZ destekli maruziyet yönetimi (Tenable platformu)	Şirket içi, Bulut, Web Uygulamaları	Kapsamlı güvenlik açığı değerlendirmesi, güçlü uyumluluk özellikleri.
Pynt	Pynt.io	Otomatik API güvenlik açığı testi, DAST, API Keşfi, CI/CD entegre.	YZ Destekli ve bağlama duyarlı	API (Geleneksel, Modern, LLM)	API güvenliği için özelleşmiş, gölge API'leri tanımlar.
Auvik Ağ Yönetimi	Auvik Networks	Gerçek zamanlı ağ haritalama, otomatik Katman 2 keşfi, sürekli taramalar, çoklu satıcı desteği, ayrıntılı cihaz envanteri.	Snippet'lerde açıkça belirtilmemiş	Şirket içi, Ağ, IoT	Dinamik topoloji görselleştirmesi, hızlı sorun giderme.
LiveAction LiveNX	LiveAction	Gerçek zamanlı ağ topolojisi haritalama, otomatik cihaz keşfi, trafik kalıbı izleme,	Snippet'lerde açıkça belirtilmemiş	Şirket içi, Ağ	Güvenlik olayı yanıtını iyileştirir, sürekli güncel harita.

		güvenlik görselleştirmesi.			
SentinelOne Singularity™	SentinelOne	Uç nokta, bulut, XDR, VM için birleşik mimari; gerçek zamanlı yanıt, otomatik önleme/tespit.	Purple AI, AI-SIEM, yerel YZ motorları	Uç nokta, Bulut, Kapsayıcı, OS	Çeşitli iş yüklerinde otonom önleme, tespit ve yanıt.
Qualys VMDR	Qualys	Bulut tabanlı güvenlik, sürekli güvenlik açığı tespiti, uyumluluk, BT çözümleri, tek ajan.	Otomatik güvenlik açığı tespiti	Şirket içi, Bulut, Uç noktalar, Sunucular, Web Uygulamaları	Kolaylaştırılmış güvenlik ve uyumluluk, geniş platform kapsamı.
Darktrace / NETWORK	Darktrace	YZ odaklı hibrit saldırı tespiti, soruşturma ve yanıt, gerçek zamanlı tehdit istihbaratı.	Benzersiz YZ teknolojisi	Ağ, Hibrit Bulut	Otonom yanıt, bilinmeyen tehditleri tanımlar.
ExtraHop RevealX	ExtraHop	Ağ Tespiti ve Yanıtı (NDR), tehditlere, güvenlik açıklarına, performans sorunlarına görünürlük.	YZ odaklı	Şirket içi, Bulut	Fidye yazılımı, tedarik zinciri, Sıfır Güven, yanal hareket odaklı.

Aikido	Aikido.dev	Koddan buluta güvenlik, kapsayıcı görüntü taraması, OS paketi CVE'leri, kitaplık kusurları, yanlış yapılandırmalar.	AI AutoFix, YZ destekli önceliklendirme	Kod, Bağımlılıklar, Kapsayıcılar, IaC, Bulut	Geliştirici odaklı, otomatik düzeltmeler üretir, gürültüyü azaltır.

V. 2025'te Proaktif Güvenlik İçin Stratejik Öneriler

Bu bölüm, kuruluşların gelişmiş host tarama tekniklerini daha geniş güvenlik stratejilerine entegre ederek siber güvenlik duruşlarını proaktif olarak geliştirmeleri için eyleme geçirilebilir öneriler sunmaktadır.

Sürekli Güvenlik Açığı Yönetimi ve Sızma Testi Döngülerine Gelişmiş Taramanın Entegre Edilmesi

Kuruluşlar, sürekli varlık keşfi, YZ ile risk tabanlı puanlama ve gerçek zamanlı tehdit istihbaratı entegrasyonu sunan Yeni Nesil Güvenlik Açığı Yönetimi (NGVM) çözümlerini benimsemelidir.[13] Güvenlik duvarı denetimleri (üç ayda bir) ve kural temizliği düzenli olarak yapılmalı, yedekli veya çakışan kuralları belirlemek ve trafik günlükleri ve güvenlik analitiği kullanarak verimliliği doğrulamak için otomatik araçlardan yararlanılmalıdır.[22] İhlal ve Saldırı Simülasyonu (BAS) ve kırmızı takım tatbikatları, savunmaları gerçek dünya saldırı senaryolarına karşı sürekli test etmek, güvenlik açıklarını ortaya çıkarmak ve tehdit tespit yeteneklerini iyileştirmek için standart güvenlik uygulamaları haline gelmelidir.[57] Gelişmiş gizli ve kaçınma teknikleri (örn. Nmap yemleri, parçalanma, boşta taramalar) dahili sızma testlerinde proaktif olarak kullanılmalı ve IDS/IPS ile güvenlik duvarı kurallarının sofistike saldırılara karşı etkinliği değerlendirilmelidir.[18]

Erken Kusur Tespiti İçin DevSecOps ile "Sola Kaydırma" Güvenlik Yaklaşımının Benimsenmesi

Güvenlik süreçleri, geliştirme yaşam döngüsüne erken entegre edilmeli, tarama derleme süreçlerine dahil edilmeli ve yeni kod yüksek önem dereceli güvenlik açıkları içeriyorsa birleştirme istekleri engellenmelidir.[13] Bulut, kapsayıcı ve sunucusuz ortamlar

için her kod taahhüdü ve çekme isteğinde güvenlik taramaları otomatikleştirilmelidir.[14] Geliştirme ekipleri, güvenli kodlama standartları ve yaygın güvenlik açığı kalıpları konusunda eğitilmeli, işbirlikçi bir güvenlik kültürü teşvik edilmelidir.[58] Sunucusuz ortamlar için, otomatik bağımlılık taraması (örn. AWS CodeGuru, GitHub Advanced Security) uygulanmalı ve bağımlılık ayak izi en aza indirilmelidir.[11]

Tahmine Dayalı Tehdit İstihbaratı ve Otomatik Olay Yanıtı İçin YZ'den Yararlanma

Tahmine dayalı tehdit tespiti yapabilen YZ destekli savunma sistemleri benimsenmelidir. Bu sistemler, gelecekteki saldırıları tahmin etmek için geçmiş verileri ve ortaya çıkan kalıpları analiz eder.[5] Saldırıları anında analiz edebilen, tehlikeye atılmış sistemleri izole edebilen ve tehditleri insan müdahalesi olmadan etkisiz hale getirebilen otomatik olay yanıt sistemleri uygulanmalıdır.[5] YZ motorlarını beslemek için günlükler ve telemetri merkezi bir veri gölünde birleştirilmeli, analistlerin model çıktılarını en son tehdit istihbaratına göre iyileştirdiği geri bildirim döngüleri oluşturulmalıdır.[58] Ağ etkinliklerini ve kullanıcı davranışını sürekli olarak izleyerek potansiyel ihlallere veya içeriden gelen tehditlere işaret eden olağandışı kalıpları işaretlemek için gerçek zamanlı ağ analizi ve davranışsal analitik için YZ kullanılmalıdır.[7]

Gerçek Zamanlı Host ve Ağ Bilgileriyle Desteklenen Sıfır Güven İlkelerinin Uygulanması

Geleneksel VPN'lerden Sıfır Güven mimarilerine geçiş yapılmalı, "asla güvenme, her zaman doğrula" ilkesine dayalı sürekli kimlik doğrulaması ve katı erişim kontrolleri uygulanmalıdır.[5] YZ destekli cihaz parmak izi ve davranışsal işletim sistemi parmak izi, sürekli cihaz puanlaması ve tam zamanında kimlik doğrulama için entegre edilmeli, bir cihaz yeni, tutarsız veya riskli göründüğünde dinamik olarak çok faktörlü kimlik doğrulama (MFA) veya "adım adım kimlik doğrulama" gerektirilmelidir.[9] Kritik sistemleri izole etmek ve yanal hareketi sınırlamak için ağ segmentasyonu ve mikro segmentasyon uygulanmalı, her paketin denetlenmesi ve doğrulanması sağlanmalıdır.[22]

Sürekli İzleme, Tehdit Avcılığı ve Uyarlanabilir Savunma Mekanizmalarının Teşvik Edilmesi

Tüm ortamlar için, özellikle sunucusuz işlevler için izleme, günlük kaydı ve izleme önceliklendirilmelidir, böylece bir olay sırasında neyin yanlış gittiği hızlı bir şekilde keşfedilebilir.[11] Tehdit avcılığı ekipleri ve gelişmiş analitik araçlar kullanılarak sistemler genelinde potansiyel güvenlik açıkları ve anormallikler aktif olarak aranmalıdır.[6] Saldırganları şaşırtmak, ilerlemelerini geciktirmek ve teknikleri ve yükleri hakkında değerli istihbarat toplamak için aldatma teknolojileri (örn. bal küpleri, sahte kimlik bilgileri) konuşlandırılmalıdır.[49] Dosyasız saldırılar için bellek tabanlı tespit araçlarına yatırım yapılmalı, yetkisiz süreç enjeksiyonları veya düzensiz API çağrıları gibi şüpheli

etkinlikler için RAM izlenmelidir.[49] Parmak izi teknikleri sürekli olarak güncellenmeli ve geliştirilmeli, yeni tespit yöntemleri (WebGL, ses, davranışsal) dahil edilmeli ve uyarlanabilir dolandırıcılık tespiti için makine öğrenimi kullanılmalıdır.[35]

Bu öneriler, 2025'te proaktif güvenlik için yeni bir paradigma oluşturan yakınlaşan stratejilerdir. YZ destekli tehditlerin artan hızı ve sofistikasyonu, host taramanın artık bağımsız bir faaliyet olmaktan çıkıp, daha büyük, uyarlanabilir bir savunma stratejisinin ayrılmaz, otomatik ve sürekli bir bileşeni olmasını gerektirmektedir. Bu, tarama verilerinin doğrudan YZ odaklı analitiklere beslenmesi, Sıfır Güven modelinde dinamik politika uygulamasını bilgilendirmesi ve geliştirme yaşam döngülerine entegre edilmesi anlamına gelmekte, böylece bütünsel ve dayanıklı bir güvenlik ekosistemi oluşturulmaktadır.

VI. Sonuç

2025 yılına girerken, ağ keşfi ve güvenlik açığı değerlendirmesi, siber güvenlik duruşunun temel bir bileşeni olmaya devam etmektedir. Yapay zeka destekli siber saldırıların artan sofistikasyonu, Sıfır Güven mimarilerinin yaygınlaşması ve bulut, kapsayıcı ve sunucusuz ortamların genişleyen saldırı yüzeyleri, host tarama tekniklerinin ve eğilimlerinin önemli ölçüde evrilmesini zorunlu kılmaktadır.

Bu rapor, YZ destekli sürekli güvenlik açığı taraması, gelişmiş gizli ve kaçınmaya dirençli TCP/UDP taraması, API odaklı ve bağlama duyarlı güvenlik açığı testi, yeni nesil güvenlik duvarı tanımlama ve politika analizi, TLS parmak izi (JA3/JA4) kullanımı, otomatik güvenlik duvarı kuralı çıkarımı, YZ destekli cihaz parmak izi ve MAC sahtekarlığı tespiti, davranışsal işletim sistemi parmak izi, bulut, kapsayıcı ve sunucusuz ortam taraması ile hizmet sürümü tespiti obfuskasyonu ve de-obfuskasyon teknikleri gibi en son 10 tekniği detaylandırmıştır. Bu teknikler, geleneksel yöntemlerin yetersiz kaldığı alanlarda derinlemesine görünürlük ve proaktif savunma sağlamaktadır.

Özellikle, YZ'nin istismar geliştirmeyi hızlandırması, savunma penceresini daraltmış ve sürekli, YZ odaklı taramayı zorunlu kılmıştır. Sıfır Güven modelleri, her cihazın ve kullanıcının sürekli doğrulanmasını gerektirerek, host taramanın ağ çevresi denetiminden her uç noktanın bütünlüğünü doğrulayan yaygın bir sürece dönüşmesini sağlamıştır. Ayrıca, bulut yerel ortamların dinamik doğası, host kavramının yeniden tanımlanmasını ve kod bütünlüğü, yapılandırma ve API davranışı gibi alanlara odaklanan özelleşmiş tarama yöntemlerini gerektirmiştir. Son olarak, saldırganların obfuskasyon tekniklerindeki gelişimi, host taramanın yüzeysel ağ problarından derin kod ve bellek analizine kaymasını zorunlu kılmıştır.

Geleceğe bakıldığında, ağ keşfi ve güvenlik açığı değerlendirmesi alanındaki sürekli

adaptasyon ve inovasyon hayati önem taşımaktadır. YZ'nin güvenlik açıklarını daha hızlı silahlandırma yeteneği, savunmacıların da YZ'yi daha hızlı ve daha akıllı tespit ve yanıt için kullanmasını gerektirecektir. Bu, YZ destekli analitiklerin daha da geliştirilmesi, davranışsal parmak izi teknolojilerinin olgunlaştırılması ve bulut yerel ortamlar için entegre güvenlik çözümlerinin genişletilmesi gibi alanlarda sürekli araştırmaya ve geliştirmeye olan ihtiyacı vurgulamaktadır. Kuruluşlar, siber tehditlerin sürekli gelişen doğasına karşı dayanıklı kalabilmek için bu eğilimleri yakından takip etmeli ve güvenlik stratejilerini buna göre uyarlamalıdır.

Alıntılanan çalışmalar

1. Cybersecurity Reconnaissance - Cymulate, erişim tarihi Haziran 12, 2025, https://cymulate.com/cybersecurity-glossary/cyber-reconnaissance/
2. Top 10 Reconnaissance And Enumeration Tools In Cybersecurity For 2025 - ITU Online, erişim tarihi Haziran 12, 2025, https://www.ituonline.com/blogs/top-10-reconnaissance-and-enumeration-tools-in-cybersecurity-for-2025/
3. Host Discovery Techniques in Ethical Hacking | ARP, ICMP, TCP, UDP, and IP Protocol Scans Explained with Nmap Commands and Real-Time Use Cases - Web Asha Technologies, erişim tarihi Haziran 12, 2025, https://www.webasha.com/blog/host-discovery-techniques-in-ethical-hacking-arp-icmp-tcp-udp-and-ip-protocol-scans-explained-with-nmap-commands-and-real-time-use-cases
4. Best Network Discovery Tools: Top 10 Tools to Know in 2025 - Faddom, erişim tarihi Haziran 12, 2025, https://faddom.com/best-network-discovery-tools-top-10-tools-to-know-in-2025/
5. Top 10 cybersecurity trends for 2025 | Insights | Elliott Davis, erişim tarihi Haziran 12, 2025, https://www.elliottdavis.com/insights/top-10-cybersecurity-trends-2025
6. Top 12 Cyber Security Trends And Predictions For 2025 - Splashtop, erişim tarihi Haziran 12, 2025, https://www.splashtop.com/blog/cybersecurity-trends-2025
7. AI-Driven Cybersecurity Threats in 2025 | Netrix Global - Netrix, LLC, erişim tarihi Haziran 12, 2025, https://netrixglobal.com/blog/cybersecurity/ai-driven-cyber-threats-what-to-expect-in-2025/
8. AI Drastically Accelerates Exploit Development for CVE-2025-32433 ..., erişim tarihi Haziran 12, 2025, https://www.netizen.net/news/post/6259/ai-drastically-accelerates-exploit-development-for-cve-2025-32433
9. Beyond the basics: Why device fingerprinting is mission-critical in 2025 - WorkOS, erişim tarihi Haziran 12, 2025, https://workos.com/blog/beyond-the-basics-why-device-fingerprinting-is-mission-critical-in-2025
10. Black Hat USA 2025 | Trainings Schedule, erişim tarihi Haziran 12, 2025,

https://www.blackhat.com/us-25/training/schedule/
11. Serverless Security Pitfalls: A 2025 Checklist | sanj.dev, erişim tarihi Haziran 12, 2025, https://sanj.dev/post/serverless-security-pitfalls-2025
12. 4 AWS Serverless Security Traps in 2025 (And How to Fix Them) - Tamnoon, erişim tarihi Haziran 12, 2025, https://tamnoon.io/blog/4-aws-serverless-security-traps-in-2025-and-how-to-fix-them/
13. What is Next Generation Vulnerability Management? - SentinelOne, erişim tarihi Haziran 12, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/next-generation-vulnerability-management/
14. 10 Container Vulnerability Scanning Tools in 2025 - SentinelOne, erişim tarihi Haziran 12, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/container-vulnerability-scanning-tools/
15. 10 Vulnerability Scanning Tools to Know in 2025 - Pynt, erişim tarihi Haziran 12, 2025, https://www.pynt.io/learning-hub/application-security/10-vulnerability-scanning-tools-to-know-in-2025
16. Best Vulnerability Assessment Reviews 2025 | Gartner Peer Insights, erişim tarihi Haziran 12, 2025, https://www.gartner.com/reviews/market/vulnerability-assessment
17. The Most Popular Penetration Testing Tools in 2025: 30 Products to Support Your Pentesting Efforts This Year - PlexTrac, erişim tarihi Haziran 12, 2025, https://plextrac.com/the-most-popular-penetration-testing-tools-in-2025-30-products-to-support-your-pentesting-efforts-this-year/
18. Recon #4: Port scanning and revealing hidden services – YesWeHack, erişim tarihi Haziran 12, 2025, https://www.yeswehack.com/learn-bug-bounty/recon-port-scanning-attack-vectors
19. Nmap, the Tool for Mapping and Assessing Network Security, erişim tarihi Haziran 12, 2025, https://www.vaadata.com/blog/nmap-the-tool-for-mapping-and-assessing-network-security/
20. Top 10 API Discovery Tools & Vendors in 2025 - Akto, erişim tarihi Haziran 12, 2025, https://www.akto.io/learn/api-discovery-tools
21. 2025 State of API Security Report - Traceable AI, erişim tarihi Haziran 12, 2025, https://www.traceable.ai/2025-state-of-api-security
22. 7 Firewall Management Best Practices in 2025 - Infraon, erişim tarihi Haziran 12, 2025, https://infraon.io/blog/7-firewall-management-best-practices/
23. Top 5 NGFW solutions for 2025 | Nomios Group, erişim tarihi Haziran 12, 2025, https://www.nomios.com/news-blog/top-5-solutions-ngfw-2025/
24. Firewall Assessment in 2025: 5-step Methodology - Research AIMultiple, erişim tarihi Haziran 12, 2025, https://research.aimultiple.com/firewall-assessment/
25. Firewall Best Practices in 2025: Fortifying Your First Line of Defense - Network

Pedia LLC, erişim tarihi Haziran 12, 2025, https://networkpedia.com/firewall-best-practices-in-2025-fortifying-your-first-line-of-defense/
26. Essential Steps for Effective Firewall Setup - The Complete 2025 Guide - MoldStud, erişim tarihi Haziran 12, 2025, https://moldstud.com/articles/p-essential-steps-for-effective-firewall-setup-the-complete-2025-guide
27. Best Practices for Configuring Firewall Rules in 2025 - SecureMyOrg, erişim tarihi Haziran 12, 2025, https://securemyorg.com/best-practices-for-configuring-firewall-rules/
28. Top 15 Firewall Management Tools in 2025 - Atrity, erişim tarihi Haziran 12, 2025, https://www.atrity.com/top-15-firewall-management-tools-in-2025/
29. Top 15 Firewall Management Tools in 2025, erişim tarihi Haziran 12, 2025, https://hackedalert.com/top-15-firewall-management-tools-in-2025/
30. Firewall Concepts - Vercel, erişim tarihi Haziran 12, 2025, https://vercel.com/docs/vercel-firewall/firewall-concepts
31. US20250112952A1 - Detection of mac spoofing - Google Patents, erişim tarihi Haziran 12, 2025, https://patents.google.com/patent/US20250112952A1/en
32. Digital Fingerprinting in Cybersecurity: OS, Nmap, & More - Bitsight, erişim tarihi Haziran 12, 2025, https://www.bitsight.com/learn/cti/digital-fingerprinting
33. 7 best tools for browser fingerprint evasion in web scraping for 2025 - SOAX, erişim tarihi Haziran 12, 2025, https://soax.com/blog/prevent-browser-fingerprinting
34. The 8 best fingerprint detection tools for web scrapers in 2025 - SOAX, erişim tarihi Haziran 12, 2025, https://soax.com/blog/best-browser-checking-tools
35. Top 9 Browser Fingerprinting Techniques Explained - Bureau, erişim tarihi Haziran 12, 2025, https://www.bureau.id/blog/browser-fingerprinting-techniques
36. Advancements in Biometric Security: What to Expect in 2025, erişim tarihi Haziran 12, 2025, https://securityforcenow.com/advancements-in-biometric-security-what-to-expect-in-2025/
37. What is Device Fingerprinting? How Does It Fight Fraud? - FOCAL, erişim tarihi Haziran 12, 2025, https://www.getfocal.ai/knowledgebase/what-is-device-fingerprinting
38. The role of AI and machine learning in fraud detection and financial security - | World Journal of Advanced Research and Reviews, erişim tarihi Haziran 12, 2025, https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-1450.pdf
39. Top 8 SaaS Discovery Methods In 2025 | Zluri, erişim tarihi Haziran 12, 2025, https://www.zluri.com/blog/saas-discovery-methods
40. Top 13 IT Asset Discovery Tools in 2025 - Workwize, erişim tarihi Haziran 12, 2025, https://www.goworkwize.com/blog/it-asset-discovery-tools
41. Top Container Scanning Tools in 2025 - Aikido, erişim tarihi Haziran 12, 2025, https://www.aikido.dev/blog/top-container-scanning-tools
42. Serverless Computing in 2025: Complete Guide & Best Practices - BuzzClan, erişim tarihi Haziran 12, 2025, https://buzzclan.com/cloud/serverless-computing/

43. What is Serverless Security? | Wiz, erişim tarihi Haziran 12, 2025, https://www.wiz.io/academy/serverless-security
44. Recon Training - Software Deobfuscation Techniques by Tim Blazytko, erişim tarihi Haziran 12, 2025, https://recon.cx/2025/trainingSoftwareDeobfuscationTechniques.html
45. Blog Bypass AMSI in 2025 - r-tec IT Security GmbH, erişim tarihi Haziran 12, 2025, https://www.r-tec.net/r-tec-blog-bypass-amsi-in-2025.html
46. UNC5221's Latest Exploit: Weaponizing CVE-2025-22457 in Ivanti Connect Secure, erişim tarihi Haziran 12, 2025, https://www.picussecurity.com/resource/blog/unc5221-cve-2025-22457-ivanti-connect-secure
47. Bypassing Obfuscation in Android Apps: A Dual Approach with DalvikFLIRT and LLM-Powered Rewrites | Ostorlab, erişim tarihi Haziran 12, 2025, https://blog.ostorlab.co/bypassing-obfuscation-android-app-dalvik-flirt-llm-powered-rewrites.html
48. ScatterBrain: Unmasking the Shadow of PoisonPlug's Obfuscator | Google Cloud Blog, erişim tarihi Haziran 12, 2025, https://cloud.google.com/blog/topics/threat-intelligence/scatterbrain-unmasking-poisonplug-obfuscator
49. Advanced Ransomware Evasion Techniques in 2025 - Tripwire, erişim tarihi Haziran 12, 2025, https://www.tripwire.com/state-of-security/advanced-ransomware-evasion-techniques
50. Top Nmap Alternatives in 2025 - Slashdot, erişim tarihi Haziran 12, 2025, https://slashdot.org/software/p/Nmap/alternatives
51. Penetration Testing for IT Pros: June 10th, 2025 - Live in Salt Lake City, Utah | LMG Security, erişim tarihi Haziran 12, 2025, https://www.lmgsecurity.com/product/penetration-testing-for-it-pros-june-2025-slc/
52. Network Topology and Visualization with Auvik: Gain Insights, erişim tarihi Haziran 12, 2025, https://www.auvik.com/network-management-software/use-case/network-topology/
53. Network Topology Mapping - LiveAction, erişim tarihi Haziran 12, 2025, https://www.liveaction.com/solutions/network-performance/topology-mapping/
54. Compare Advanced IP Scanner vs. Nmap in 2025 - Slashdot, erişim tarihi Haziran 12, 2025, https://slashdot.org/software/comparison/Advanced-IP-Scanner-vs-Nmap/
55. The Future of AI Data Security: Trends to Watch in 2025 - CyberProof, erişim tarihi Haziran 12, 2025, https://www.cyberproof.com/blog/the-future-of-ai-data-security-trends-to-watch-in-2025/
56. Best Network Detection and Response Reviews 2025 | Gartner Peer Insights, erişim tarihi Haziran 12, 2025, https://www.gartner.com/reviews/market/network-detection-and-response

57. Threat Detection Solutions in 2025 You Need to Know - SISA, erişim tarihi Haziran 12, 2025, https://www.sisainfosec.com/blogs/threat-detection-solutions-in-2025-you-need-to-know/
58. 10 Security Protocols Organizations Need To Follow In 2025 - SISA, erişim tarihi Haziran 12, 2025, https://www.sisainfosec.com/blogs/10-security-protocols-organizations-need-to-follow-in-2025/
59. JA3/JA4 fingerprint · Cloudflare bot solutions docs, erişim tarihi Haziran 12, 2025, https://developers.cloudflare.com/bots/additional-configurations/ja3-ja4-fingerprint/