Ağ Çevresini Yönetmek: 2025 Yılı İçin En İyi 10 Güvenlik Duvarı ve WAF Atlama Tekniği ve Trendi

Yönetici Özeti

2025 yılı siber güvenlik ortamı, geleneksel çevre savunmalarını (güvenlik duvarları ve Web Uygulama Güvenlik Duvarları - WAF'lar) zorlayan karmaşık, adaptif atlatma teknikleriyle karakterize edilen hızlanan bir siber silahlanma yarışına sahne olmaktadır. Bu dönem, yapay zekanın sadece savunmada değil, aynı zamanda saldırı stratejilerinde de yaygın etkisini taşımaktadır. Sıfır gün istismarlarının ve gelişmiş uygulama katmanı atlatma yöntemlerinin devam eden tehdidi, güvenlik profesyonelleri için önemli bir zorluk teşkil etmektedir.

Geleneksel imza tabanlı atlatma yöntemlerinden, güvenlik kontrollerinin doğrudan istismarına ve karmaşık davranışsal taklitlere doğru belirgin bir kayma gözlemlenmektedir. Bu durum, statik güvenlik çözümlerinin yetersiz kaldığını ve sürekli adaptasyonun kritik önem taşıdığını göstermektedir. Bu bağlamda, Nmap gibi araçlar, gelişmiş paket manipülasyonu ve genişletilebilir betik motoru sayesinde, güvenlik duvarı ve saldırı tespit sistemlerini (IDS) atlatma tekniklerini test etmek ve uygulamak için vazgeçilmez bir rol oynamaya devam etmektedir. Bu rapor, 2025 yılı için en etkili 10 güvenlik duvarı ve WAF atlatma tekniğini ve trendini derinlemesine inceleyerek, bu dinamik ortamda etkili savunma ve test stratejileri geliştirmek için temel bir çerçeve sunmaktadır.

Güvenlik duvarı ve WAF atlatma tekniklerindeki ilerlemeler, yapay zekanın hem saldırganlar hem de savunmacılar tarafından kullanılmasıyla yeni bir boyut kazanmıştır. Saldırganlar, yapay zekayı kullanarak daha önce görülmemiş saldırı vektörleri oluştururken, savunmacılar da yapay zekayı kötü niyetli davranışları tespit etmek ve bunlara karşı koymak için kullanmaktadır. Bu durum, siber güvenlik alanında sürekli bir "silahlanma yarışı" yaratmaktadır; burada atlatma teknikleri yapay zeka destekli savunmalara uyum sağlamalı, savunmalar da yapay zeka destekli saldırılara karşı koymalıdır. Bu temel değişim, güvenlik stratejilerinin statik kural setlerinden dinamik, adaptif ve istihbarat odaklı yaklaşımlara geçişini zorunlu kılmaktadır. Atlatmanın doğası, artık sadece bir kuralı atlatmaktan ziyade, akıllı bir sistemi alt etmeye dönüşmektedir.

Giriş: Ağ Çevresi Güvenliğinin Değişen Dinamikleri

Günümüzün giderek artan bağlantılı dijital dünyasında, güvenlik duvarları ve WAF'lar, ağ çevresi güvenliğinin temel taşları olmaya devam etmektedir. Bu sistemler, ağlara

giren ve çıkan trafiği kontrol eden birincil kapı bekçileri olarak hizmet vermektedir. Ancak, siber tehdit ortamının sürekli evrimi, bu savunma mekanizmalarını sürekli olarak yeni ve daha sofistike atlatma teknikleriyle karşı karşıya bırakmaktadır.

2025 yılına gelindiğinde, siber suçların küresel düzeyde 10,5 trilyon dolara ulaşması beklenen zararlarıyla [1], tehdit ortamının ciddiyeti artmaktadır. Hibrit çalışma modellerine geçiş, bulut hizmetlerinin yaygınlaşması ve Nesnelerin İnterneti (IoT) cihazlarının patlaması, saldırı yüzeyini önemli ölçüde genişletmiştir.[2] 2025 yılına kadar kurumsal IoT bağlantılarının 29 milyarı aşması beklenmektedir [3], bu da her bir kurumsal cihazın korunması gereken ortalama 26,9 GB veri üretmesi anlamına gelmektedir. Bu genişleme, geleneksel çevre odaklı güvenlik modelini temelden sarsmaktadır. Daha fazla cihaz ve uzaktan erişim noktası, daha fazla giriş noktası anlamına gelmektedir. Bu durum, yalnızca güçlü bir çevre güvenlik duvarına güvenmenin yetersiz kalmasına yol açmaktadır. Sonuç olarak, atlatma teknikleri, çevreyi aşmaktan ziyade, iç ağlardaki yanal hareketlere, uç nokta güvenliğine ve bulut tabanlı kontrollere odaklanmaktadır. Bu, "güvenlik duvarı atlatma" kavramının basit ağ çevrelerinin ötesine geçtiği anlamına gelmektedir.

Saldırganlar, güvenlik kontrollerini aşmak için sürekli olarak yeni yöntemler geliştirmekte ve bu durum, savunma mekanizmalarının hızla adapte olmasını gerektiren bir "silahlanma yarışı" dinamiği yaratmaktadır.[4] Geleneksel imza tabanlı tespit yöntemleri, yeni ve gelişen tehditlere karşı yetersiz kalmaktadır.[2] Bu ortamda, Nmap (Network Mapper) gibi araçlar, ağ keşfi, güvenlik açığı değerlendirmesi ve özellikle güvenlik duvarı ile IDS atlatma tekniklerini test etmek ve göstermek için temel bir rol oynamaya devam etmektedir.[9] Nmap'in paket manipülasyonu ve betikleme yetenekleri, gelişmiş atlatma stratejilerinin uygulanmasında anahtar bir bileşen olarak öne çıkmaktadır.

2025 Yılı İçin En İyi 10 Güvenlik Duvarı ve WAF Atlatma Tekniğinin Özeti

Aşağıdaki tablo, 2025 yılı için en etkili güvenlik duvarı ve WAF atlatma tekniklerini ve trendlerini özetlemektedir. Bu özet, her bir tekniğin temel özelliklerini, birincil etkilerini ve ilgili güvenilir kaynakları sunarak, okuyuculara kapsamlı rapora dalmadan önce hızlı bir genel bakış sağlamaktadır. Bu tablo, bir siber güvenlik aracı geliştiricisi için hızlı bir kontrol listesi sunarak, araçlarının bu önde gelen atlatma vektörlerine karşı yeteneklerini değerlendirmelerine olanak tanımaktadır.

Teknik/Trend	Kısa Açıklama	Birincil Etki	Güvenilir Kaynak
1. Yapay Zeka Destekli Polimorfik Kötü Amaçlı Yazılımlar ve Saldırı Zincirleri	Yapay zeka kullanılarak sürekli değişen, imza tabanlı tespitleri atlatan kötü amaçlı kodlar ve saldırı süreçlerinin otomasyonu.	Geleneksel güvenlik duvarlarını ve antivirüsleri etkisiz hale getirir; saldırı tespit süresini kısaltır.	[2]
2. Sıfır Gün İstismarı (Doğrudan Güvenlik Duvarı/WAF Güvenliğinin Aşılması)	Güvenlik duvarı, WAF veya kritik uygulamalardaki bilinmeyen güvenlik açıklarının doğrudan istismarı.	Tüm güvenlik politikalarını atlatır, sisteme tam erişim sağlar; güvenlik cihazının kendisini saldırı platformuna dönüştürür.	[12]
3. Adversary Yapay Zeka ve Yapay Zeka Model Manipülasyonu	Yapay zeka destekli güvenlik sistemlerini (örneğin, WAF'lar) yanıltmak, manipüle etmek veya alt etmek için yapay zeka modellerine karşı saldırılar.	Yapay zeka destekli savunmaların temel işlevselliğini bozar, geleneksel uyarıları tetiklemeden atlatma sağlar.	[14]
4. Uygulama Katmanı Ayrıştırma Tutarsızlıkları (RFC/ABNF Kötüye Kullanımı)	WAF ile arka uç uygulama arasındaki HTTP protokolü ayrıştırma farklılıklarını istismar ederek WAF'ı atlatma.	WAF'ın kötü amaçlı trafiği iyi niyetli olarak yanlış yorumlamasına neden olur, saldırganın arka uca ulaşmasını sağlar.	[16]
5. HTTP Başlık ve Protokol Manipülasyonu (HTTP/2 Hızlı Sıfırlama ve Next.js Bypass Dahil)	HTTP başlıklarının manipülasyonu ve protokol nuanslarının istismarı (örn. HTTP/2 Hızlı Sıfırlama ile WAF'ları aşırı yükleme, Next.js'deki iç başlıkları kullanma).	Uygulama katmanı kontrollerini atlatır, WAF'ları aşırı yükler veya yanıltır; yüksek hacimli DDoS'a yol açabilir.	[17]
6. Gelişmiş İstemci	WAF'lar ve NAC'lar	Anomali tabanlı	[19]

Parmak İzi Taklidi ve Davranışsal Atlatma	tarafından kullanılan gelişmiş istemci parmak izi (TLS, JavaScript, HTTP) ve davranışsal analizi atlatmak için otomatik araçların meşru kullanıcıları taklit etmesi.	tespitleri atlatır, otomatik araçların insan trafiği gibi görünmesini sağlar; tespit süresini uzatır.	
7. Aldatma Teknolojisi Atlatma (Honeypot/Decoy Tespiti ve Kaçınma)	Saldırganların honeypot'ları, honeytoken'ları ve tuzak sistemlerini tespit etme ve bunlardan kaçınma stratejileri.	Saldırganların tespit edilmeden daha uzun süre faaliyet göstermesine olanak tanır, istihbarat toplama yeteneğini azaltır.	21
8. Dağıtık Saldırılar ve IP İtibarını Aşma (Konut/Mobil Proxy'ler, Büyük Botnet'ler, Tuzak IP'ler)	Kötü amaçlı trafiği çok sayıda farklı IP adresine (konut/mobil proxy'ler, büyük botnet'ler) yayarak hız sınırlamalarını ve IP tabanlı engellemeyi atlatma.	IP tabanlı engelleme ve hız sınırlamalarını etkisiz hale getirir; saldırganın gerçek kaynağını gizler.	23
9. Gelişmiş Ağ Paketi Manipülasyonu ve Protokol Kötüye Kullanımı (TCP Parçalanması, Hatalı Sağlama Toplamları, Katmanlar Arası Saldırılar Dahil)	Ağ protokolü uygulamalarındaki ince kusurları veya tek tek paketleri manipüle etmeyi içeren düşük seviyeli atlatma teknikleri.	Güvenlik duvarlarının derin paket denetimini atlatır, protokol yığınındaki zayıflıkları istismar eder.	25
10. Nmap Betik Motoru (NSE) ile Hedefli Atlatma ve Güvenlik Açığı Keşfi	Nmap Betik Motoru'nu kullanarak belirli güvenlik duvarı davranışlarına veya uygulama protokollerine göre uyarlanmış karmaşık ve akıllı atlatma girişimleri	Genel taramaların ötesine geçerek hedefe özel atlatma ve güvenlik açığı tespiti sağlar; Nmap'in adaptasyon yeteneğini artırır.	27

	gerçekleştirme.		

2025 Yılı İçin En İyi 10 Güvenlik Duvarı ve WAF Atlatma Tekniği ve Trendi

1. Yapay Zeka Destekli Polimorfik Kötü Amaçlı Yazılımlar ve Saldırı Zincirleri

Bu teknik, saldırganların yapay zeka (YZ) ve makine öğrenimi (ML) yeteneklerini kullanarak sürekli değişen ve adaptif kötü amaçlı kodlar (polimorfizm/metamorfizm) üretmelerini içermektedir. Bu kodlar, imzalarını sürekli değiştirerek geleneksel, imza tabanlı güvenlik duvarları ve antivirüs çözümleri tarafından tespit edilmelerini son derece zorlaştırmaktadır.[2] Tek tek kötü amaçlı yazılımların ötesinde, yapay zeka artık ilk keşiften yük dağıtımına kadar tüm saldırı yaşam döngülerini otomatikleştirmek ve hızlandırmak için kullanılmakta, bu da savunmacıların tepki sürelerini kısaltan "YZ destekli saldırı zincirleri" oluşturmaktadır.[4]

YZ algoritmaları, savunma kalıplarını analiz ederek gerçek zamanlı olarak yeni, daha önce görülmemiş kötü amaçlı kod varyantları üreterek statik tespit mekanizmalarını atlatmaktadır.[2] Bu, gelişmiş gizleme tekniklerini ve bağlam duyarlı hedeflemeyi içermekte, böylece kötü amaçlı yazılımların normal ağ etkinliğiyle harmanlanmasını sağlamaktadır.[8] YZ ayrıca, güvenlik açığı taraması, istismar dağıtımı ve istismar sonrası faaliyetler gibi görevleri otomatikleştirerek çok aşamalı kampanyaları koordine etmekte, bu da saldırıları daha hızlı ve daha ölçeklenebilir hale getirmektedir.[4]

Bu tekniğin önemi, geleneksel güvenlik duvarlarının statik kural setlerine ve bilinen imzalara bağımlı olmaları nedeniyle bu dinamik tehditlere karşı etkisiz kalmasından kaynaklanmaktadır.[6] YZ destekli saldırıların hızı ve ölçeği, savunmacılar için "bekleme süresini" önemli ölçüde azaltmakta, bu da otomatik ve adaptif yanıtları zorunlu kılmaktadır.[4] YZ destekli polimorfik kötü amaçlı yazılımların yükselişi, geleneksel güvenlik duvarları için önemli bir tespit boşluğu yaratmaktadır. Statik imza tabanlı güvenlik duvarlarının bu tür dinamik tehditlere ayak uyduramaması, davranışsal analize ve YZ destekli WAF'lara doğru temel bir kaymayı zorlamaktadır. Bu, güvenlik duvarı atlatma ve tespitte sürekli bir geri bildirim döngüsü oluşturmaktadır. Kullanıcının aracı için bu trend, gelişmiş davranışsal anomali tespiti ve potansiyel olarak YZ destekli Nmap taraması [9] gibi yeteneklerin geliştirilmesi gerektiğini ima etmektedir. Sızma testi ekipleri, bu tür saldırıları simüle etmek ve savunmaların dayanıklılığını test etmek için YZ'yi kullanarak daha güçlü ve tespit edilemez yükler geliştirecektir.

2. Sıfır Gün İstismarı (Doğrudan Güvenlik Duvarı/WAF Güvenliğinin Aşılması)

Bu teknik, güvenlik duvarı, WAF, VPN cihazları veya korudukları kritik uygulamalar

içindeki daha önce bilinmeyen güvenlik açıklarının (sıfır günler) istismar edilmesini içermektedir. Bu, saldırganların yapılandırılmış tüm güvenlik politikalarını atlatmalarına ve yetkisiz erişim elde etmelerine olanak tanımaktadır.[2] Bu tür istismarlar son derece değerli olup, kimlik doğrulaması yapılmamış uzaktan kod yürütme (RCE) veya cihaz üzerinde tam kontrol sağlayabilmektedir.[12]

Saldırganlar, güvenlik cihazlarının (örneğin Fortinet, Ivanti, SonicWall) veya kritik uygulamaların (örneğin Next.js, Windows CLFS sürücüsü) yazılım veya donanım yazılımındaki sıfır gün güvenlik açıklarını keşfetmekte veya satın almaktadır. Daha sonra, genellikle bellek bozulmasına (arabellek taşmaları, serbest bırakma sonrası kullanım) veya komut enjeksiyonuna yol açan belirli yükler oluşturarak RCE veya ayrıcalık yükseltme ile sonuçlanmaktadır.[12] Bu istismarlar, daha derin bir uzlaşma için diğer güvenlik açıklarıyla zincirlenebilmektedir.[34]

Sıfır gün istismarları, güvenlik açığı savunmacılar tarafından bilinmediği için en gelişmiş, güncel güvenlik sistemlerini bile atlatmaktadır.[5] Etkileri şiddetli olup, tam sistem uzlaşmasına, veri hırsızlığına ve kalıcı erişime yol açabilmektedir.[12] 2025'in Ocak ayında 4.000'den fazla yeni CVE'nin (Ortak Güvenlik Açıkları ve Açıklıkları) yayınlanması [33], bu tür fırsatların sürekli akışını göstermektedir. Güvenlik duvarları ve WAF'lar artık sadece aşılması gereken engeller değil, giderek sıfır gün istismarı için doğrudan hedefler haline gelmektedir. Bu durum, bir savunma önlemini bir saldırı platformuna dönüştürmektedir. Güvenlik duvarlarının artan karmaşıklığı (Yeni Nesil Güvenlik Duvarları - NGFW'ler, YZ destekli) doğal olarak daha fazla potansiyel güvenlik açığı yaratmaktadır. Bu güvenlik açıklarının istismar edilmesi, amaçlanan güvenlik işlevinin tamamen atlatılmasına yol açmakta ve hatta güvenlik duvarının daha fazla saldırı için bir dayanak noktası olarak kullanılmasına olanak tanımaktadır. Bu durum, kuruluşların yalnızca güvenlik duvarlarının kendilerini korumasına güvenemeyecekleri, aynı zamanda güvenlik duvarlarının kendilerini de titizlikle yamalamaları ve güvence altına almaları gerektiği anlamına gelmektedir. Kullanıcının aracı için bu, savunmasız güvenlik duvarı sürümlerini tanımlama ve potansiyel olarak bunlara karşı bilinen istismarları test etme yeteneklerine ihtiyaç duyulduğunu ima etmektedir.

3. Adversary Yapay Zeka ve Yapay Zeka Model Manipülasyonu

Yapay zeka ve makine öğrenimi, gelişmiş tehdit tespiti için yeni nesil WAF'lara ve güvenlik sistemlerine entegre edildikçe [3], saldırganlar bu YZ modellerini karıştırmak, manipüle etmek veya alt etmek için "Adversary Yapay Zeka" teknikleri geliştirmektedir.[14] Bu, kötü amaçlı trafiği meşru olarak yanlış sınıflandırmak için tasarlanmış "adversary girdiler" oluşturmayı veya YZ'nin eğitim verilerini bozmak için "veri zehirlenmesi" yapmayı içermektedir.[14]

Saldırganlar, insan algılamasına kapalı olan ancak bir YZ modelinin yanlış kararlar almasına neden olan kötü amaçlı yüklerde ince bozulmalar yaratmaktadır.[14] Bu, içerik filtrelerini atlayabilir veya dolandırıcılık tespit araçlarını devre dışı bırakabilir. "Veri zehirlenmesi", YZ'nin eğitim veri setlerine kötü amaçlı veriler enjekte ederek zamanla arka kapılar oluşturmaya, yanlış sınıflandırmalara neden olmaya veya doğruluğu azaltmaya yönelik bir yöntemdir.[14] "Prompt enjeksiyonu" ise, üretken YZ sistemlerine (örneğin, büyük dil modelleri - LLM'ler) karşı, çıktılarını manipüle etmek veya veri sızdırmak için kullanılan belirli bir tekniktir.[14]

Bu, saldırganların gelişmiş güvenlik sistemlerinin "beyinlerini" doğrudan hedef aldığı yeni bir atlatma sınırını temsil etmektedir. Başarılı olursa, YZ destekli savunmaların temel işlevselliğini baltalamakta, geleneksel uyarıları tetiklemeden onları etkisiz hale getirmektedir.[14] "YZ silahlanma yarışı", hem saldırının hem de savunmanın YZ'yi kullandığı anlamına gelmekte ve karmaşık YZ'ye karşı YZ savaşlarına yol açmaktadır.[4] YZ'nin güvenlik sistemlerine entegrasyonu, YZ modellerinin kendilerinin manipülasyon için hedef haline geldiği yeni bir saldırı yüzeyi yaratmaktadır. Bu, güvenlik çözümlerinin yalnızca YZ destekli değil, aynı zamanda YZ'ye karşı güçlendirilmiş olması gerektiği anlamına gelmektedir. Kuruluşlar, YZ güvenlik açıklarını proaktif olarak test etmek için adversary ML'yi kırmızı takım tatbikatlarına entegre etmektedir.[15] Kullanıcının aracı için bu, YZ destekli WAF'ları test etmek üzere adversary girdileri simüle etme ve potansiyel olarak YZ destekli Nmap taraması [9] kullanarak YZ destekli WAF'ların gözden kaçırabileceği yeni atlatma kalıpları oluşturma ihtiyacını ima etmektedir. Bu aynı zamanda YZ destekli honeypot'ları atlatma [21] yeteneğini de kapsamaktadır.

4. Uygulama Katmanı Ayrıştırma Tutarsızlıkları (RFC/ABNF Kötüye Kullanımı)

Bu teknik, WAF'lar ile arka uç uygulamaları arasındaki HTTP standartlarını (RFC'ler, ABNF gramer kuralları) yorumlamadaki ince farklılıkları istismar etmeyi içermektedir.[16] Bu, kötü amaçlı isteklerin WAF filtrelemesini atlamasına ancak sunucu tarafından doğru şekilde yorumlanmasına olanak tanımaktadır.

Saldırganlar, WAF'ın iyi niyetli olarak yanlış yorumladığı, ancak arka ucun kötü niyetli olarak işlediği alışılmadık sözdizimi, içerik türleri (örneğin, multipart/form-data, XML mutasyonları) veya HTTP başlıklarını manipüle ederek istekler oluşturmaktadır.[16] Bu, WAF'lar ve arka uç uygulamaları arasındaki "içerik ayrıştırma tutarsızlıklarını" kullanmaktadır.[16]

Bu tekniğin önemi, WAF'ın güçlü imza tespiti olsa bile, protokol düzeyinde sofistike bir atlatma sağlamasından kaynaklanmaktadır. Bu, atlatmayı "yükü gizlemekten" "WAF'ın yükü yanlış yorumlamasını sağlamaya" kaydırmaktadır.[16] Bazı tutarsızlıklara karşı web sitelerinin %90'ından fazlasının savunmasız olması [16] yaygın uygulanabilirliğini

göstermektedir. WAF'lar ayrıştırma vekil sunucuları olarak işlev görmektedir ve ayrıştırma mantıklarındaki herhangi bir sapma, arka uç uygulamasının mantığından farklıysa, kritik bir atlatma güvenlik açığı yaratmaktadır. Bu, WAF'ların arka uç uygulama ayrıştırma mantığıyla mükemmel bir senkronizasyon içinde olması gerektiği anlamına gelmektedir. Kullanıcının aracı, hedef WAF'larda bu tür tutarsızlıkları tespit etmek için fuzzing tekniklerini dahil edebilmektedir. Bu, karmaşık web ortamlarında WAF dağıtımlarının sağlamlığını test etmek için kritik öneme sahiptir.

5. HTTP Başlık ve Protokol Manipülasyonu (HTTP/2 Hızlı Sıfırlama ve Next.js Bypass Dahil)

Bu teknik, HTTP başlıklarını manipüle etmeyi ve WAF'lar ile diğer Katman 7 güvenlik kontrollerini atlatmak için belirli protokol nuanslarını istismar etmeyi içermektedir. Örnekler arasında, WAF'ları aşırı istek hacimleriyle boğan HTTP/2 Hızlı Sıfırlama tekniği [17] ve Next.js gibi çerçevelerdeki uygulama ara yazılımlarını (genellikle WAF benzeri işlevleri yerine getiren) atlatmak için x-middleware-subrequest gibi belirli dahili başlıkları istismar etme yer almaktadır.[18]

HTTP/2 Hızlı Sıfırlama, protokolün çoklama yeteneklerini kullanarak çok sayıda akışı gönderip hemen iptal etmekte, bu da sunucu kaynaklarını etkili bir şekilde tüketmekte ve geleneksel HTTP/1.1 bağlantıları için tasarlanmış hız sınırlamalarını aşmaktadır.[17] Başlık manipülasyonu, WAF'ı veya uygulama mantığını güvenlik kontrollerini atlamaya ikna eden belirli, genellikle dahili veya hatalı biçimlendirilmiş HTTP başlıklarıyla istekler oluşturmayı içermektedir.[18]

Bu teknikler, uygulama katmanını doğrudan hedefleyerek geleneksel ağ katmanı güvenlik duvarlarını atlatmakta ve WAF'ları aşırı yüklemekte veya karıştırmaktadır. İnce protokol tasarım kusurlarını veya uygulama çerçevelerindeki yanlış yapılandırmaları istismar etme yetenekleri nedeniyle son derece etkilidirler. HTTP/2 Hızlı Sıfırlama saldırısı, 2025'in ilk çeyreğinde benzeri görülmemiş paket oranları (saniyede 4,8 milyar paket) sergilemiştir.[17] Modern web protokollerinin (HTTP/2) ve uygulama çerçevelerinin (Next.js ara yazılımı) artan karmaşıklığı, saldırganların yüksek etkili Katman 7 atlatma için istismar edebileceği ince güvenlik açıkları yaratmaktadır. Bu, güvenlik çözümlerinin protokol belirtimlerini derinlemesine anlaması ve doğru bir şekilde uygulaması gerektiği anlamına gelmektedir. Bu teknikler, web uygulamalarının ve API'lerin dayanıklılığını test etmek için kritik öneme sahiptir. Kullanıcının aracı, WAF ve uygulama ara yazılımı sağlamlığını değerlendirmek için bu teknikleri uygulayabilmektedir. Bu, WAF'ların gelişmiş protokol denetimini desteklemesi ve geliştiricilerin çerçeveye özgü atlatma yöntemlerinin farkında olması gerektiğini vurgulamaktadır.

6. Gelişmiş İstemci Parmak İzi Taklidi ve Davranışsal Atlatma

WAF'lar ve Ağ Erişim Kontrolü (NAC) sistemleri, botları ve kötü amaçlı etkinliği tespit etmek için giderek artan bir şekilde sofistike istemci parmak izi (TLS, JavaScript, HTTP detayları) ve davranışsal analize güvenmektedir.[19] Saldırganlar, otomatik araçlarının meşru insan kullanıcılar veya yetkili cihazlardan ayırt edilemez görünmesini sağlamak için gelişmiş taklit teknikleri kullanmaktadır.[19]

Saldırganlar, otomasyon belirtilerini gizleyen güçlendirilmiş başsız tarayıcılar kullanmaktadır.[19] HTTP başlık değerlerini ve sıralamasını titizlikle eşleştirmekte, doğru HTTP/2 kullanımını sağlamakta ve meşru TLS parmak izlerini taklit etmektedir.[19] Teknik parmak izlerinin ötesinde, rastgele aralıklar, istekler arasındaki gecikmeler ve değişen kullanım kalıpları gibi insan benzeri davranışsal kalıpları simüle etmekte ve hatta orijinal cihazın özelliklerini kopyalarken MAC adreslerini taklit etmektedir.[20]

Bu teknik, basit imza veya IP tabanlı engellemenin ötesine geçerek istemci davranışındaki ve cihaz özelliklerindeki anormallikleri tespit eden yeni nesil WAF'ları ve NAC'ları atlatmak için kritik öneme sahiptir.[5] Davranışsal analizin güvenlikte artan benimsenmesine doğrudan bir karşı önlemdir.[30] WAF'larda ve NAC'larda davranışsal analiz ve istemci parmak izi kullanımına doğru kayma, saldırganları son derece sofistike taklit ve davranışsal atlatma teknikleri benimsemeye zorlamaktadır. Bu, savaşın "bilinen kötü" yerine "normal"den ince sapmaları tespit etmeye kaydığı anlamına gelmektedir. Bu teknik, büyük ölçekli web kazıma, kimlik bilgisi doldurma ve tespit edilmeden kalması gereken her türlü otomatik kötü amaçlı faaliyet için hayati önem taşımaktadır. Kullanıcının aracı, gelişmiş parmak izi ve davranışsal taklit yeteneklerini entegre edebilmektedir. Sızma testi uzmanları, davranışsal güvenlik kontrollerinin etkinliğini doğru bir şekilde değerlendirmek için bu teknikleri dahil etme ihtiyacı duyacaktır.

7. Aldatma Teknolojisi Atlatma (Honeypot/Decoy Tespiti ve Kaçınma)

Kuruluşlar, saldırganları tespit etmek, geciktirmek ve onlar hakkında istihbarat toplamak için aldatma teknolojilerini (honeypot'lar, honeytoken'lar, tuzak sistemleri) giderek daha fazla kullandıkça [22], saldırganlar bu tuzakları tespit etme ve bunlardan kaçınma stratejileri geliştirmektedir. Başarılı atlatma, saldırganın uyarıları tetiklemeden veya taktiklerini ifşa etmeden hedeflerine devam edebilmesi anlamına gelmektedir.[39]

Saldırganlar, tuzak sistemleri içindeki "açık tuzakları", varsayılan yapılandırmaları, gerçekçi olmayan güvenlik açıklarını veya gerçekçi olmayan verileri aramaktadır.[21] Ağ trafiği kalıplarını, sistem yanıtlarını veya dosya içeriklerini analiz ederek meşru varlıklar ile tuzaklar arasındaki farkı ayırt edebilmektedirler.[21] YZ destekli adaptif honeypot'ların yükselişiyle birlikte [21], saldırganlar bu daha sofistike tuzakları tespit etmek için de

YZ'den faydalanabilmektedir.

Aldatma teknolojisi, kritik bir erken uyarı sistemi ve istihbarat toplama aracıdır.[22] Bu teknolojiyi atlatmak, saldırganların daha uzun süre tespit edilmeden faaliyet göstermesine olanak tanımakta, bekleme süresini ve potansiyel zararı artırmaktadır. Aldatma teknolojisi pazarının hızla büyümesi, 2025'te yaygın olarak benimseneceğini göstermektedir.[41] Aldatma teknolojisi güçlü bir savunma aracı olsa da, artan karmaşıklığı (YZ destekli, adaptif) saldırganlardan eşit derecede gelişmiş atlatma tekniklerini gerektirmekte, bu da gerçekçilik ve tespit konusunda bir silahlanma yarışına yol açmaktadır. Bu, saldırganların bu tuzakları nasıl tespit edip kaçınacakları konusunda istihbarat geliştirmeleri gerektiği anlamına gelmektedir. Bu teknik, aldatma platformlarının etkinliğini test etmek için kırmızı takım angajmanları için kritik öneme sahiptir. Kullanıcının aracı, yaygın honeypot özelliklerini tanımlama veya bilinen tuzak imzalarına ilişkin tehdit istihbarat akışlarıyla entegre olma yeteneklerini içerebilmektedir. Bu, honeypot'ların son derece gerçekçi ve adaptif olması gerektiğini vurgulamaktadır.

8. Dağıtık Saldırılar ve IP İtibarını Aşma (Konut/Mobil Proxy'ler, Büyük Botnet'ler, Tuzak IP'ler)

Bu teknik, kötü amaçlı trafiği çok sayıda farklı IP adresine yaymayı içermektedir. Bu, genellikle konut veya mobil proxy'ler ya da büyük botnet'ler kullanılarak gerçekleştirilmektedir.[19] Amaç, hız sınırlamalarını, IP tabanlı engellemeyi ve tek veya sınırlı bir IP adresi kümesinden gelen şüpheli etkinliği işaretleyen davranışsal analizleri atlatmaktır.[23] Nmap, bir taramanın gerçek kaynağını gizlemek için "tuzak IP" seçeneklerini kullanabilmektedir.[24]

Saldırganlar, trafiklerini meşru konut veya mobil cihaz ağları üzerinden yönlendirerek, isteklerin farklı coğrafi konumlardaki gerçek kullanıcılardan geliyormuş gibi görünmesini sağlamaktadır.[19] Bu, bilinen veri merkezi IP'lerini engelleyen veya tek bir kaynaktan yüksek hacimli trafiği tespit eden WAF'ları atlatmaktadır.[19] 2025'teki büyük ölçekli kaba kuvvet saldırıları, milyonlarca IP adresini kullanmıştır.[23] Nmap'in tuzak özelliği (-D), taramaya rastgele IP adresleri ekleyerek gerçek tarayıcının tespit edilmesini zorlaştırmaktadır.[24]

Geleneksel güvenlik duvarları ve WAF'lar büyük ölçüde IP itibarına ve hız sınırlamalarına dayanmaktadır. Dağıtık saldırılar, kötü amaçlı etkinliği birçok meşru görünen kaynağa yayarak bu kontrolleri daha az etkili hale getirmektedir.[23] 2025'in ilk çeyreğinde ortaya çıkan devasa botnet'ler (1,33 milyon cihaz [42]), bu tekniği önemli bir tehdit haline getirmektedir. Dağıtık saldırıların (milyonlarca IP, devasa botnet'ler) ölçeği, geleneksel IP tabanlı ve hız sınırlamalı savunmaları aşarak, hacim ve kaynak

çeşitliliğini güçlü bir atlatma tekniği haline getirmektedir. Bu, savunmaların basit IP kara listelemenin ötesine geçerek, farklı IP'ler arasındaki davranışsal korelasyonu daha karmaşık bir şekilde analiz etmesi gerektiği anlamına gelmektedir. Bu teknik, büyük ölçekli web kazıma, kimlik bilgisi doldurma ve DDoS saldırıları için kritik öneme sahiptir. Kullanıcının aracı, güvenlik duvarı ve WAF'ın bu tür saldırılara karşı dayanıklılığını test etmek için tuzak IP'ler ve çeşitli proxy türleri kullanarak dağıtık taramaları simüle edebilmektedir. Bu, farklı IP'ler arasındaki etkinliği ilişkilendirebilen gelişmiş davranışsal analitiklere olan ihtiyacı vurgulamaktadır.

9. Gelişmiş Ağ Paketi Manipülasyonu ve Protokol Kötüye Kullanımı (TCP Parçalanması, Hatalı Sağlama Toplamları, Katmanlar Arası Saldırılar Dahil)

Bu kategori, tek tek paketleri titizlikle oluşturmayı ve manipüle etmeyi veya ağ protokolü uygulamalarındaki ince kusurları istismar etmeyi içeren düşük seviyeli ağ atlatma tekniklerini kapsamaktadır. Bu, paketlerin denetimi atlatmak için daha küçük parçalara bölündüğü TCP parçalanmasını [9], "hatalı sağlama toplamları" veya yanlış sağlama toplamı işleme ile ilgili güvenlik açıklarını istismar etmeyi [32] ve TCP/IP süiti içindeki daha gelişmiş "katmanlar arası güvenlik açıkları" veya anlamsal saldırıları [26] içermektedir.

Nasıl Çalışır:

- **TCP Parçalanması:** Nmap, yalnızca ilk parçayı denetleyen veya yeniden birleştirmede zorluk çeken güvenlik duvarlarını atlatmak için paketleri parçalayabilmektedir (-f, --mtu).[9] Günümüzde yaygın olarak tespit edilse de [28], temel bir teknik olmaya devam etmektedir.
- **Hatalı Sağlama Toplamları/Yanlış İşleme:** Sistemlerin sağlama toplamlarını yanlış işlediği veya doğruladığı güvenlik açıklarını istismar etmek, arabellek taşmalarına veya RCE'ye yol açarak güvenlik kontrollerini etkili bir şekilde atlatabilmektedir.[32] Bu, kasıtlı olarak hatalı biçimlendirilmiş sağlama toplamlarına sahip paketler oluşturmayı veya sağlama toplamı hesaplama mantığındaki kusurları kullanmayı içerebilmektedir.
- **Katmanlar Arası/Anlamsal Saldırılar:** Bu saldırılar, TCP/IP yığınının farklı katmanları arasındaki ince etkileşimleri veya yanlış yorumlamaları, örneğin sahte ICMP hata mesajlarını istismar etmektedir.[26] Hping3 gibi araçlar, farklı protokoller, TOS ve parçalanma dahil olmak üzere gelişmiş ağ testi için kullanılabilmektedir.[28]

Bu teknikler, ağ iletişiminin temel yapı taşlarını hedeflemektedir. Basit parçalanma, gelişmiş IDS/IPS nedeniyle 2025'te daha az etkili olsa da [28], protokol ayrıştırma ve durum makinesi kusurlarını istismar etme temel prensibi güçlü kalmaktadır. TCP/IP'deki "ince anlamsal güvenlik açıklarının" sürekli keşfi [26], bu düşük seviyeli saldırıların devam

eden önemini vurgulamaktadır. Çekirdek ağ protokollerinin (TCP/IP) karmaşıklığı ve uzun süredir var olması, ince, anlamsal güvenlik açıklarının var olmaya devam etmesi anlamına gelmektedir. Bu da protokol ayrıştırma veya durum makinesi kusurlarını istismar ederek son derece teknik ve genellikle gizli atlatma yöntemlerine olanak tanımaktadır. Bu, "eski" protokollerin bile yeni saldırı vektörleri sağlayabileceğini vurgulamaktadır. Bu teknikler, NGFW'lerin derin paket denetim yeteneklerini ve ağ cihazı yazılımlarının sağlamlığını test etmek için kritik öneme sahiptir. Kullanıcının aracı, Nmap'in paket manipülasyon özelliklerinden yararlanabilir ve protokol düzeyinde test için hping3'ün gelişmiş yeteneklerini keşfedebilir. Bu alan, yeni protokol güvenlik açıklarını keşfetmek için YZ destekli yaklaşımlardan da faydalanmaktadır.[26]

10. Nmap Betik Motoru (NSE) ile Hedefli Atlatma ve Güvenlik Açığı Keşfi

Nmap Betik Motoru (NSE), Nmap'in yeteneklerini temel port taramasının ötesine taşıyarak, hedef hizmetlerle karmaşık, otomatik etkileşimlere olanak tanımaktadır. 2025'te NSE betikleri, genellikle belirli protokol yardımcılarını veya bilinen zayıflıkları istismar ederek, hedefe yönelik güvenlik duvarı/IDS atlatma, güvenlik açığı tespiti ve bilgi toplama için kritik öneme sahiptir.[9]

NSE betikleri çeşitli gelişmiş görevleri yerine getirebilmektedir:

- **Güvenlik Duvarı Atlama Betikleri:** Örneğin, firewall-bypass.nse betiği, dinamik olarak port açmak için yardımcıları (örneğin, FTP, SIP) kullanan güvenlik duvarlarındaki güvenlik açıklarını tespit etmektedir. Bu, güvenlik duvarını ilgili bir bağlantıyı açmaya ikna etmek için hedef sunucudan paketleri taklit ederek yapılmaktadır.[27]
- **Gizlilik ve Atlama:** NSE, taramaları IDS/IPS tarafından daha az tespit edilebilir hale getirmek için sofistike zamanlama kontrolleri (-T), paket parçalama (-f), kaynak IP taklidi (-S) ve tuzak ana bilgisayar oluşturma (-D) uygulayabilmektedir.[10]
- **Güvenlik Açığı Tespiti:** --script vuln gibi betikler, atlatma veya erişim için istismar edilebilecek bilinen güvenlik açıklarını tanımlamaktadır.[11]

NSE, Nmap'in genel taramaların ötesine geçerek belirli güvenlik duvarı davranışlarına veya uygulama protokollerine göre uyarlanmış yüksek düzeyde özelleştirilmiş ve akıllı atlatma girişimleri yapmasına olanak tanımaktadır. Yeni savunma önlemlerine uyum sağlama ve yeni atlatma yöntemleri keşfetme esnekliği sağlamaktadır.[10] Nmap'in geleceği, gelişmiş YZ destekli tarama ve daha sofistike otomasyon betikleme özelliklerini içermektedir.[9] Nmap'in genişletilebilir betik motoru (NSE), yeni güvenlik duvarı savunmalarına hızlı adaptasyon ve belirli güvenlik açıklarının keşfi/istismarı için güçlü bir mekanizma sağlamakta, böylece gelişen atlatma ortamında sürekli önemini garanti etmektedir. Bu, özelleştirilebilirlik ve otomasyonun etkili atlatma için anahtar

olduğunu göstermektedir. Bu teknik, gelişmiş sızma testi ve otomatik güvenlik denetimleri için kritik öneme sahiptir. Kullanıcının aracı, güvenlik duvarı markası tespiti ve güvenlik açığı değerlendirmesi için NSE betik işlevlerini entegre edebilir veya taklit edebilir. Betikleri çok aşamalı atlatma için zincirleme yeteneği, NSE'yi bir saldırganın araç setinde güçlü bir bileşen haline getirmektedir.

Sonuçlar

2025 yılı siber güvenlik ortamı, yapay zekanın hem saldırı hem de savunma stratejilerine yaygın entegrasyonuyla büyük ölçüde hızlanan bir silahlanma yarışı ile tanımlanmaktadır. Statik kurallara dayanan geleneksel güvenlik duvarı ve WAF çözümleri, dinamik, polimorfik ve bağlam duyarlı atlatma tekniklerine karşı giderek yetersiz kalmaktadır. Atlama odak noktası, sadece çevre savunmalarını aşmaktan, güvenlik cihazlarının kendilerindeki sıfır gün güvenlik açıklarını istismar etmeye, uygulama katmanı protokollerini manipüle etmeye ve gelişmiş tespit sistemlerini atlatmak için sofistike davranışsal taklitler kullanmaya doğru kaymıştır. Aldatma teknolojileri daha yaygın hale gelmekte, bu da saldırganlardan karşı atlatma stratejilerini gerektirmektedir. Nmap, gelişmiş paket manipülasyonu ve genişletilebilir betik motoru sayesinde, bu karmaşık atlatma tekniklerini hem test etmek hem de uygulamak için kritik bir araç olmaya devam etmektedir.

Bu analizden çıkarılan temel çıkarımlar ve kullanıcının aracı için öneriler aşağıdaki gibidir:

- **Adaptif İstihbarat:** Geliştirilen aracın, polimorfik saldırıları ve adversary yapay zeka tekniklerini tespit etmek ve bunlara uyum sağlamak için yapay zeka/makine öğrenimi yeteneklerini içermesi gerekmektedir. Bu, aracın yalnızca bilinen tehditleri değil, aynı zamanda sürekli evrilen ve kendini gizleyen tehditleri de tanıyabilmesini sağlayacaktır.
- **Sıfır Gün ve Güvenlik Açığı Odaklılık:** Araç, belirli güvenlik duvarı/WAF markalarındaki ve bunların altında yatan uygulamalardaki bilinen güvenlik açıklarının (CVE'ler) tanımlanmasına öncelik vermelidir. Bu, potansiyel zayıflıkların proaktif olarak tespit edilmesine ve istismar edilebilir hedeflerin belirlenmesine olanak tanıyacaktır.
- **Derin Protokol Analizi:** Gelişmiş HTTP/TCP protokol manipülasyonu ve ayrıştırma tutarsızlığı tespiti için modüller uygulanmalıdır. Bu, uygulama katmanındaki ince zayıflıkları ve protokol uyumsuzluklarını ortaya çıkararak daha sofistike WAF atlatma senaryolarının test edilmesini sağlayacaktır.
- **Davranışsal Taklit ve Tespit:** Gelişmiş istemci parmak izi (TLS, JS, HTTP) ve davranışsal simülasyon için özellikler geliştirilmelidir. Bu, WAF'ların davranışsal

analiz yeteneklerini test etmek ve aynı zamanda ağdaki anormal davranışları tespit etmek için kritik öneme sahiptir.

- **Aldatma Farkındalığı:** Honeypot'ları/tuzakları tanımlama ve bunlardan kaçınma yetenekleri araca entegre edilmelidir. Bu, sızma testleri sırasında tuzak sistemlerinden kaçınarak daha gerçekçi saldırı senaryolarının yürütülmesini sağlayacaktır.
- **Dağıtık Saldırı Simülasyonu:** Konut proxy'leri ve tuzak IP'ler ile dağıtık taramalar desteklenmelidir. Bu, güvenlik duvarlarının ve WAF'ların hız sınırlamalarına ve IP tabanlı engellemelere karşı dayanıklılığını test etmek için gereklidir.
- **Nmap Entegrasyonu ve Geliştirme:** Nmap'in NSE'si, özel atlatma betikleri ve gelişmiş tarama türleri için kullanılmalı ve geliştirilmelidir. Potansiyel olarak Nmap'in yapay zeka destekli tarama yetenekleri de artırılmalıdır. Bu, aracın esnekliğini ve adaptasyon yeteneğini önemli ölçüde artıracaktır.
- **Sürekli Güncellemeler:** Hızla gelişen tehdit ortamına ve yeni güvenlik açıklarına uyum sağlamak için aracın sürekli güncellemeler alması gerektiği vurgulanmalıdır. Bu, aracın 2025 ve sonrası için etkinliğini sürdürmesi için hayati önem taşımaktadır.

Alıntılanan çalışmalar

1. Next Generation Firewall using IPS & IDS - IJRASET, erişim tarihi Haziran 4, 2025, https://www.ijraset.com/best-journal/next-generation-firewall-using-ips-ids
2. 10 Cyber Security Trends For 2025 - SentinelOne, erişim tarihi Haziran 4, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/
3. (PDF) ADVANCED NETWORK SECURITY: EVALUATING FIREWALL AND VPN STRATEGIES FOR ROBUST PROTECTION IN MODERN TELECOMMUNICATIONS - ResearchGate, erişim tarihi Haziran 4, 2025, https://www.researchgate.net/publication/389634702_ADVANCED_NETWORK_SECURITY_EVALUATING_FIREWALL_AND_VPN_STRATEGIES_FOR_ROBUST_PROTECTION_IN_MODERN_TELECOMMUNICATIONS
4. Advanced Endpoint Threat Detection in 2025 Network Environments - Cyber Security News, erişim tarihi Haziran 4, 2025, https://cybersecuritynews.com/advanced-endpoint-threat-detection/
5. What Is WAF Evasion? | Prophaze Learning Center, erişim tarihi Haziran 4, 2025, https://prophaze.com/learn/waf/what-is-waf-evasion/
6. Threat Detection and AI - A10 Networks, erişim tarihi Haziran 4, 2025, https://www.a10networks.com/blog/threat-detection-and-ai/
7. Endpoint Security in 2025 - Cyber Defense Magazine, erişim tarihi Haziran 4, 2025, https://www.cyberdefensemagazine.com/endpoint-security-in-2025/
8. How AI-Powered Malware Is Evading Traditional Firewalls - NetworkTigers News, erişim tarihi Haziran 4, 2025, https://news.networktigers.com/cloud-chronicles/how-ai-powered-malware-is-evading-traditional-firewalls/

9. What is Nmap? Overview, Features & Role in Network Scanning ..., erişim tarihi Haziran 4, 2025, https://www.craw.in/what-is-nmap-overview-features-role-in-network-scanning/
10. Nmap Cheat Sheet in 2025, all commands and options ..., erişim tarihi Haziran 4, 2025, https://hackyourmom.com/en/kibervijna/nmap-cheat-sheet-u-2025-roczi-usi-komandy-ta-parametry/
11. Nmap Network Scanning: A Hands-On Cybersecurity Lab (2025 Edition), erişim tarihi Haziran 4, 2025, https://www.buildingtheitguy.com/index.php/nmap-network-scanning-a-hands-on-cybersecurity-lab-2025-edition/cybersecurity/
12. UNC5221's Latest Exploit: Weaponizing CVE-2025-22457 in Ivanti Connect Secure, erişim tarihi Haziran 4, 2025, https://www.picussecurity.com/resource/blog/unc5221-cve-2025-22457-ivanti-connect-secure
13. Threat Actor Allegedly Selling Fortinet Firewall Zero-Day Exploit - SecurityWeek, erişim tarihi Haziran 4, 2025, https://www.securityweek.com/threat-actor-allegedly-selling-fortinet-firewall-zero-day-exploit/
14. Understanding the Biggest AI Security Vulnerabilities of 2025 ..., erişim tarihi Haziran 4, 2025, https://www.blackfog.com/understanding-the-biggest-ai-security-vulnerabilities-of-2025/
15. AI Security: 2025 Predictions & Recommendations - HiddenLayer, erişim tarihi Haziran 4, 2025, https://hiddenlayer.com/innovation-hub/ai-security-2025-predictions-recommendations/
16. WAFFLED: Exploiting Parsing Discrepancies to Bypass Web Application Firewalls - arXiv, erişim tarihi Haziran 4, 2025, https://arxiv.org/html/2503.10846v1
17. Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report, erişim tarihi Haziran 4, 2025, https://blog.cloudflare.com/pl-pl/ddos-threat-report-for-2025-q1/
18. CVE-2025-29927: Next.js Middleware Bypass Vulnerability Explained - Picus Security, erişim tarihi Haziran 4, 2025, https://www.picussecurity.com/resource/blog/cve-2025-29927-nextjs-middleware-bypass-vulnerability
19. How to Bypass Imperva Incapsula when Web Scraping in 2025, erişim tarihi Haziran 4, 2025, https://scrapfly.io/blog/how-to-bypass-imperva-incapsula-anti-scraping/
20. Ethical Hacking with Kali Linux: Techniques to Bypass MAC Filtering ..., erişim tarihi Haziran 4, 2025, https://www.examcollection.com/blog/ethical-hacking-with-kali-linux-techniques-to-bypass-mac-filtering/
21. Best Practices for Deploying Honeypots in 2025: A Comprehensive Guide - SecureMyOrg, erişim tarihi Haziran 4, 2025,

https://securemyorg.com/2025/03/25/best-practices-for-deploying-honeypots-in-2025/
22. Mitigating Insider Threats with Deception: A Strategy for 2025 | Fidelis Security, erişim tarihi Haziran 4, 2025, https://fidelissecurity.com/threatgeek/deception/mitigating-insider-threats-with-deception/
23. Brute Force Attacks in 2025: How They Work, What's Changed and How to Stop Them, erişim tarihi Haziran 4, 2025, https://www.blackfog.com/brute-force-attacks-in-2025-how-they-work-whats-changed-and-how-to-stop-them/
24. How to perform stealthy Nmap scans to avoid detection in Cybersecurity - LabEx, erişim tarihi Haziran 4, 2025, https://labex.io/tutorials/nmap-how-to-perform-stealthy-nmap-scans-to-avoid-detection-in-cybersecurity-415611
25. Firewall Evasion with Nmap - Pluralsight, erişim tarihi Haziran 4, 2025, https://www.pluralsight.com/labs/aws/firewall-evasion-with-nmap
26. Exploiting Cross-Layer Vulnerabilities: Off-Path Attacks on the TCP/IP Protocol Suite, erişim tarihi Haziran 4, 2025, https://cacm.acm.org/research/exploiting-cross-layer-vulnerabilities-off-path-attacks-on-the-tcp-ip-protocol-suite/
27. firewall-bypass NSE script - Nmap, erişim tarihi Haziran 4, 2025, https://nmap.org/nsedoc/scripts/firewall-bypass.html
28. Firewall Basic Bypassing Techniques With Nmap and Hping3 - Cybrary, erişim tarihi Haziran 4, 2025, https://www.cybrary.it/blog/firewall-basic-bypassing-techniques-nmap-hping3
29. Detecting and Mitigating an Authorization Bypass Vulnerability in Next.js | Akamai, erişim tarihi Haziran 4, 2025, https://www.akamai.com/blog/security-research/march-authorization-bypass-critical-nextjs-detections-mitigations
30. Emerging Trends in Cybersecurity Detection and Response 2025 - Gradient Cyber, erişim tarihi Haziran 4, 2025, https://www.gradientcyber.com/resources/emerging-trends-in-cybersecurity-detection-and-response-2025
31. Airborne: Wormable Zero-Click RCE in Apple AirPlay Puts Billions of Devices at Risk | Oligo Security, erişim tarihi Haziran 4, 2025, https://www.oligo.security/blog/airborne
32. The Bug Report - January 2025 Edition - Trellix, erişim tarihi Haziran 4, 2025, https://www.trellix.com/blogs/research/the-bug-report-january-2025-edition/
33. January 2025 Threat Report: Fortune Favors the Prepared - Greenbone, erişim tarihi Haziran 4, 2025, https://www.greenbone.net/en/blog/january-2025-threat-report-fortune-favors-the-prepared/
34. CVE-2025-29824: The Windows CLFS Zero Day Used in Ransomware Campaigns, erişim tarihi Haziran 4, 2025, https://www.ampcuscyber.com/shadowopsintel/cve-2025-29824-the-windows-cl

fs-zero-day-used-in-ransomware-campaigns/
35. Vulnerability Summary for the Week of April 14, 2025 | CISA, erişim tarihi Haziran 4, 2025, https://www.cisa.gov/news-events/bulletins/sb25-111
36. Vulnerability Summary for the Week of March 17, 2025 | CISA, erişim tarihi Haziran 4, 2025, https://www.cisa.gov/news-events/bulletins/sb25-083
37. Early 2025 DDoS Attacks Signal a Dangerous Trend in Cybersecurity - Imperva, erişim tarihi Haziran 4, 2025, https://www.imperva.com/blog/early-2025-ddos-attacks-signal-a-dangerous-trend-in-cybersecurity/
38. Advancing Cybersecurity with Honeypots and Deception Strategies - MDPI, erişim tarihi Haziran 4, 2025, https://www.mdpi.com/2227-9709/12/1/14
39. How to Bypass WAF in 2025: Challenges and Solutions - ZenRows, erişim tarihi Haziran 4, 2025, https://www.zenrows.com/blog/waf-bypass
40. Advanced Ransomware Evasion Techniques in 2025 - Tripwire, erişim tarihi Haziran 4, 2025, https://www.tripwire.com/state-of-security/advanced-ransomware-evasion-techniques
41. Deception Technology Market Outlook 2025–2034: Identifying Growth Drivers, Technology Trends, and Policy Impact - Latest Global Market Insights, erişim tarihi Haziran 4, 2025, https://blog.tbrc.info/2025/05/deception-technology-market-report-5/
42. Q1 2025 DDoS, bots and BGP incidents statistics and overview - Qrator.Blog, erişim tarihi Haziran 4, 2025, https://blog.qrator.net/en/q1-2025-ddos-bots-and-bgp-incidents-statistics-and_211/
43. HTB's 15 must-know Nmap commands in 2024, erişim tarihi Haziran 4, 2025, https://www.hackthebox.com/blog/nmap-commands