ScanMatrix için 2025 Host Tarama Teknikleri ve Eğilimleri

I. Yönetici Özeti

Bu rapor, 2025 yılı için ağ keşfi ve güvenlik açığı değerlendirmesindeki en son teknikleri ve eğilimleri, **ScanMatrix**'in vizyonu doğrultusunda incelemektedir. ScanMatrix, Python tabanlı bir ağ güvenliği aracı olarak, açık port tarama, banner grabbing, sistem/versiyon bilgisi toplama, CVE veritabanı taraması ve Grafana tarzı görselleştirme gibi özellikler sunar.

2025'te, yapay zeka (YZ) destekli siber saldırılar, sıfır güven mimarilerinin yükselişi ve bulut, IoT ve sunucusuz ortamların genişlemesi, ağ tarama tekniklerini dönüştürmektedir. Bu rapor, ScanMatrix'in bu trendleri nasıl entegre edebileceğini ve modern tehditlere karşı nasıl daha etkili bir araç haline gelebileceğini özetlemektedir.

II. Giriş: ScanMatrix ve 2025 Ağ Keşfi Manzarası

ScanMatrix, ağ güvenliği analizini otomatikleştiren kullanıcı dostu bir araçtır. Host keşfi, port tarama, hizmet/OS tespiti, güvenlik açığı tarama ve firewall bypass gibi özellikleriyle, ağ güvenliği profesyonellerine kapsamlı bir çözüm sunar.

2025'i Şekillendiren Temel Eğilimler

- **YZ Destekli Siber Saldırılar**: YZ, kötü amaçlı yazılım geliştirmeyi ve istismarı hızlandırır.
- **Sıfır Güven Mimarisi**: "Asla güvenme, her zaman doğrula" ilkesiyle sürekli tarama gereklidir.
- **Genişleyen Saldırı Yüzeyleri**: Bulut, IoT ve 5G, daha karmaşık tarama gereksinimleri oluşturur.

III. ScanMatrix için 2025'in En İyi 10 Host Tarama Tekniği ve Eğilimi

A. Yeni Nesil Port Tarama ve Hizmet Keşfi

1. YZ Destekli ve Sürekli Güvenlik Açığı Tarama

- **Açıklama**: Gerçek zamanlı tehdit istihbaratıyla sürekli CVE taraması.
- **Neden Önemli**: YZ istismarı hızlandırır, proaktif savunma gerektirir.
- **Entegrasyon**: Nessus gibi araçlardan alınan YZ puanlama sistemiyle ScanMatrix'e entegre edilebilir.
- **2025 Etkisi**: Sürekli tarama kurumsal standart haline gelecek.

2. Gelişmiş Gizli ve Kaçınmaya Dirençli TCP/UDP Tarama

- **Açıklama**: Yem, yavaş tarama, parçalama gibi stealth teknikleri.
- **Neden Önemli**: IDS/IPS sistemlerini atlatmak kritik hale geliyor.
- **Entegrasyon**: Nmap benzeri tekniklerle stealth modu geliştirilebilir.

3. API Odaklı ve Bağlama Duyarlı Güvenlik Açığı Testi

- **Açıklama**: API'lerin güvenlik açıkları ve gölge API tespiti.
- **Neden Önemli**: Bulut güvenliği için kritik alan.
- **Entegrasyon**: Pynt gibi araçlardan ilhamla API tarama modülü eklenebilir.

B. Gelişmiş Güvenlik Duvarı Tespiti ve Atlatma

4. Yeni Nesil Güvenlik Duvarı (NGFW) Tanımlama ve Politika Analizi

- **Açıklama**: Derin paket denetimi ve politika analizine odaklı tarama.
- **Entegrasyon**: ScanMatrix, NGFW politikalarını analiz edecek modül ekleyebilir.

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

- **Açıklama**: TLS el sıkışma hash'leri ile IDS/IPS sistemlerini tespit etme.
- **Entegrasyon**: JA3/JA4 analiz modülü ile TLS üzerinden gizli keşif.

6. Otomatik Güvenlik Duvarı Kuralı Numaralandırma

- **Açıklama**: Yanlış yapılandırmaları tespit etmek için otomatik kural çıkarımı.
- **Entegrasyon**: Tufin gibi araçlardan ilham alınabilir.

C. Dinamik MAC Adresi ve Cihaz Parmak İzi

7. YZ Destekli Cihaz Parmak İzi ve MAC Sahtekarlığı Tespiti

- **Açıklama**: Davranışsal analizle sahte MAC adreslerini tespit etme.
- **Entegrasyon**: YZ destekli MAC profil analizi modülü ile genişletilebilir.

8. Davranışsal İşletim Sistemi Parmak İzi

- **Açıklama**: Geleneksel OS tespiti yerine davranış analizine dayalı tespit.
- **Entegrasyon**: OS fingerprint modülü davranışsal izleme ile zenginleştirilebilir.

D. Ortaya Çıkan Saldırı Yüzeyi ve Özelleşmiş Tarama

9. Bulut, Kapsayıcı ve Sunucusuz Ortam Taraması

- **Açıklama**: Kapsayıcılar ve FaaS sistemlerine özgü güvenlik açığı tespiti.
- **Entegrasyon**: SentinelOne gibi araçlardan alınan ilhamla modüller geliştirilebilir.

10. Hizmet Sürümü Tespiti Obfuskasyonu ve De-obfuskasyon

- **Açıklama**: Gizlenmiş hizmet sürümlerini ortaya çıkaran YZ analizleri.
- **Entegrasyon**: Bellek analizi ve tersine mühendislik teknikleriyle entegre edilebilir.

IV. ScanMatrix'in Kullanabileceği Temel Teknolojiler ve Araçlar

Araç/Platform	Sağlayıcı	Temel Özellikler	YZ Entegrasyonu	ScanMatrix'e Katkı
Nmap	Açık Kaynak	Port tarama, OS tespiti	Sınırlı	Gizli tarama teknikleri
Nessus	Tenable	Güvenlik açığı tarama	YZ risk puanlama	Sürekli tarama modeli
Pynt	Pynt.io	API güvenliği	Bağlama duyarlı	API tarama modülü
SentinelOne	SentinelOne	Bulut/kapsayıcı güvenliği	Tehdit analizi	Bulut tarama yetenekleri
Tufin	Tufin	Güvenlik duvarı politika analizi	Otomasyon	Otomatik kural çıkarımı

V. ScanMatrix için Stratejik Öneriler

- **YZ Entegrasyonu**: Anomali tespiti, otomatik risk puanlama modülleri entegre edilmelidir.
- **Bulut ve API Taraması**: Kapsayıcı ve sunucusuz mimariler için özel modüller geliştirilebilir.
- **Otomatik Kural Analizi**: Güvenlik duvarı yapılandırmaları için otomatik analiz motoru.
- **Sürekli Tarama**: Zaman bazlı periyodik değil, olay-tetikli sürekli tarama modeli uygulanmalıdır.
- **Kullanıcı Dostu Arayüz**: Grafana benzeri görselleştirme ve daha kapsamlı kullanıcı belgeleri.

VI. Sonuç

ScanMatrix, 2025'te ağ güvenliği analizinde lider bir araç olma potansiyeline sahiptir. YZ destekli tarama, gizli teknikler, bulut odaklı çözümler ve sıfır güven entegrasyonu, ScanMatrix'in modern tehditlere karşı daha etkili olmasını sağlayabilir. Bu trendlerin benimsenmesi, aracı hem profesyonel hem de eğitimsel kullanıcılar için vazgeçilmez kılacaktır.

Alıntılanan Çalışmalar

1. Nmap: Bypass Firewalls and IDS
2. Nmap: Host Discovery
3. Nmap: Firewall Subversion (man)
4. Nmap: Firewall Subversion
5. LinuxSecurity: Effective Nmap Firewall Evasion Techniques
6. Tenable: Using Nessus to Scan Hosts Behind a Firewall
7. Tenable: 4 Ways to Improve Nessus Scans Through Firewalls
8. Tenable: Configuring Nessus to Scan Through Firewalls
9. Hack The Box: 15 Must-Know Nmap Commands

10. Palo Alto: Network Security Trends 2025
11. Pynt: 10 Vulnerability Scanning Tools to Know in 2025
12. CloudEagle: Top Vulnerability Scanning Tools
13. AI Multiple: Vulnerability Scanning Tools
14. Medium: Rise of AI-Powered Vulnerability Scanners
15. Qualysec: Vulnerability Scanning Tools
16. CodeAnt: Security Vulnerability Scanning Tools
17. AI Multiple: Open-Source Vulnerability Scanning Tools
18. FireMon: Vulnerability Scanning
19. The CTO Club: Best Vulnerability Scanning Tools
20. The Cyphere: Vulnerability Scanning Tools 2025
21. YesWeHack: Recon, Port Scanning, Attack Vectors
22. Akto: API Discovery Tools
23. Nomios: Top 5 NGFW Solutions 2025
24. Cloudflare: JA3 & JA4 Fingerprinting
25. Atrity: Top 15 Firewall Management Tools in 2025
26. Google Patents: US20250112952A1
27. BitSight: Digital Fingerprinting
28. SentinelOne: Container Vulnerability Scanning Tools
29. Ostorlab: Bypassing Obfuscation – Dalvik FLIRT
30. Fortinet: Port Scan
31. InfoSec Institute: Nmap Evade Firewall and Scripting
32. Pentest Lab: Nmap Techniques for Avoiding Firewalls
33. DZone: Firewall Bypassing with Nmap & Hping3
34. Medium: Mastering Nmap Firewall Evasion (Rishav Anand)
35. Medium: Firewall Evasion with Nmap (Muhanad Israiwi)
36. SANS Whitepapers: Scanning
37. OWASP Web Security Testing Guide
38. Cisco: Firewalls Overview
39. Check Point: Quantum Security Gateway
40. CrowdStrike: Network Security
41. Microsoft Azure Security Center
42. Rapid7: InsightVM
43. Qualys: Cloud Security
44. Tufin: Security Policy Management
45. Zscaler: Zero Trust Security
46. FortiGuard Labs
47. Metasploit Framework
48. Wireshark Network Analyzer
49. Burp Suite by PortSwigger
50. Kali Linux