



ÜRÜN TANITIMI · V0.1.1

parsDedector

Ağ Keşif ve Envanter Platformu

Bakım anlaşması teklifi öncesinde kurum ağının envanterini çıkaran, cihazları sınıflandıran, risk bulgularını listeleyen ve müşteriye sunulabilir PDF rapor üreten saha aracı.

Teknisyen ağa bağlanır, kapsamı seçer, taramayı başlatır. Birkaç dakika sonra elinde hem teknik envanter hem de müşteriye bırakılabilecek bir rapor vardır. Kurulum gerektirmeden çalışır; kurulan her bileşen taramayı bir seviye derinleştirir.

Taşınabilir

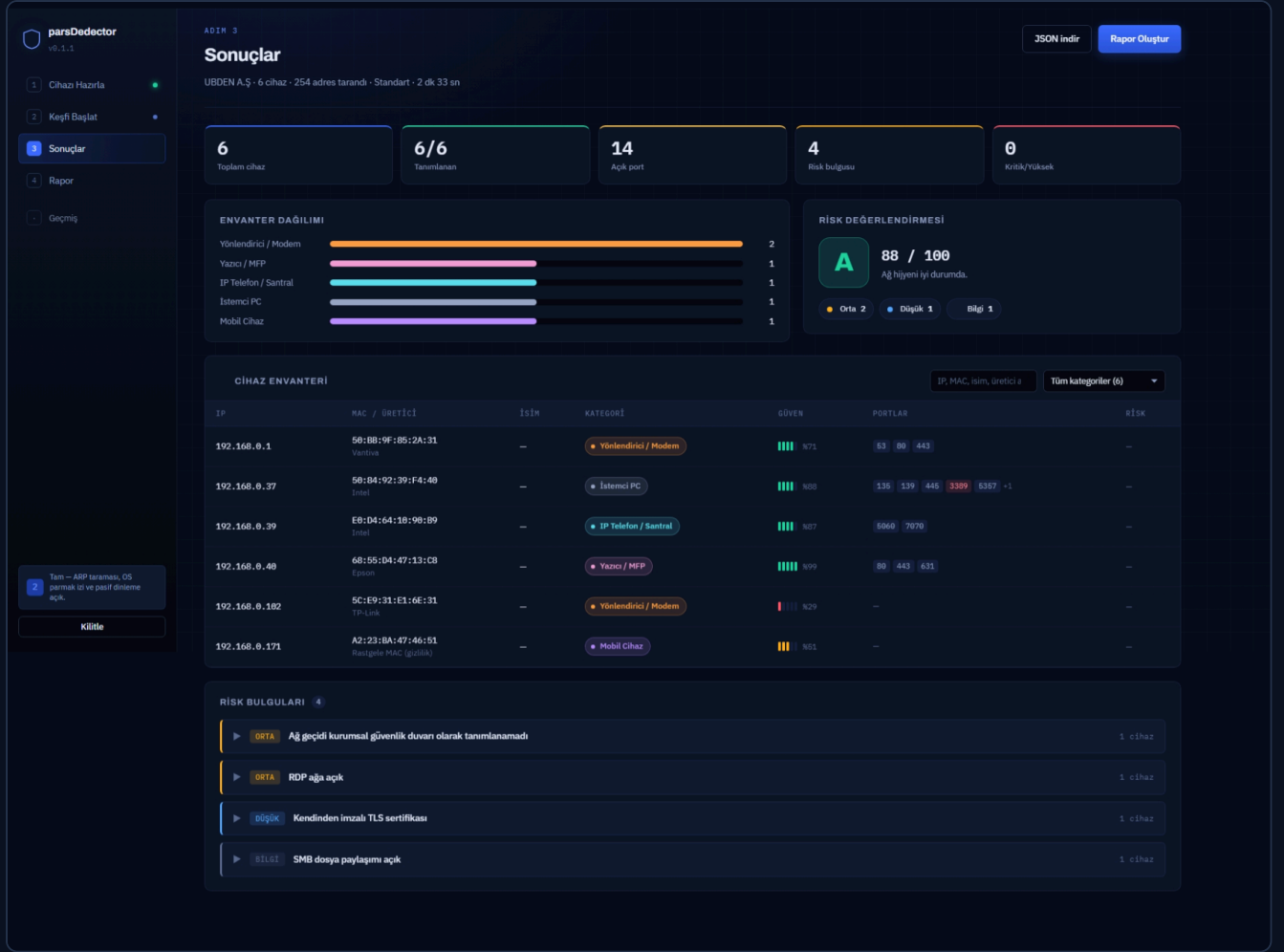
Tek dosya, kurulum yok. Nmap veya Npcap yoksa temel keşif yine çalışır.

Gerekçeli

Her sınıflandırma kararının kanıtı saklanır ve arayüzde gösterilir; teknisyen düzeltebilir.

Sunulabilir

Yönetici özeti, envanter, port matrisi ve risk bulguları içeren hazır PDF rapor.



Sonuç ekranı – envanter dağılımı, risk skoru, cihaz tablosu ve bulgular tek görünümde.

Saha akışı

Uygulama dört adımdan oluşur. Her adım bir öncekinin çıktısını doğrular; hiçbir aşama sessizce atlanmaz.

ADIM 1

Cihazı Hazırla

Yetki, bağımlılık ve harici araç kontrolü; eksikler tek tuşla kurulur.

ADIM 2

Keşfi Başlat

Kapsam, tarama profili, ek modüller ve yetkilendirme kaydı.

ADIM 3

Sonuçlar

Cihaz envanteri, güven skorları, açık portlar ve risk bulguları.

ADIM 4

Rapor

Bölümleri seçilebilir, müşteriye sunulabilir PDF çıktısı.



paraDedector

v0.1.1

1

Cihazı Hazırla

2

Keşfi Başlat

3

Sonuçlar

4

Rapor

5

Geçmiş

2

Tam — ARP taraması, OS parmak izi ve pasif dinleme sağ.

Kilitli

ADIM 2

Keşfi Başlat

Taranacak ağları seçin. VPN tüelleri, sanal switch'ler ve boşta kalmış adaptörler gerekçeleriyle birlikte otomatik olarak işaretli gelir — istemeden kapsam dışı bir ağa dokunmayın diye.

TARANACAK AĞLAR

☒

192.168.8.0/24 **FİZİKSEL**

254 adres

Wi-Fi: Intel(R) Wi-Fi 6 AX201 160MHz · gw 192.168.0.1 · 1.2 Gbps

Varolan ağ geçidini bulunduğu ağ — birinci kurum ağı.

☐

169.254.8.0/16 **APIPA**

65.534 adres

OpenVPN TAP-Windows6 · TAP-Windows Adapter V9 · 1 Gbps

APIPA (169.254.x) — adaptör DHCP alamamış, arkasında ağ yok.

☐

169.254.255.253/32 **APIPA**

1 adres

CatoNetworks · Cato Networks Tunnel · 100 Gbps

APIPA (169.254.x) — adaptör DHCP alamamış, arkasında ağ yok.

☐

172.17.0.0/20 **SANAL**

4.094 adres

vEthernet (Default Switch) · Hyper-V Virtual Ethernet Adapter · 10 Gbps

Sanallaştırma switch'i (Hyper-V/Virtualware/Docker) — host makinenin kendi iç ağı. Sanal sunucuları taramak istiyorsanız işaretleyin.

Elle hedef ekle

10.0.0.0/24, 192.168.1.50-99, 172.16.4.10

CIDR, tek adres veya aralık. Virgülle ayırın.

TARAMA PROFİLİ

Hızlı 24 port

En yaygın 24 port. Ağda ne olduğunu birkaç dakikada görmek için — ilk keşif turu veya zaman darısa.

Standart 159 port

+200 port + servis banner'ı + HTTP/TLS/SNMP/SMB parmak izi. Bakım anılaması keşif için önerilen denge.

Derin 1027 port

Geniş port aralığı + işletim sistemi parmak izi + pasif dinleme. En doğru envanter, büyük ağlarda uzun sürer.

EK MODÜLLER

☐ **Pasif dinleme**

LLDP/CDP ile switch/AP model ve port bilgisi, DHCP sunucusu ve istemci adları, mDNS isimleri. Paket gönderilmez.

☐ **Kimlik bilgili envanter**

WMF/SSH ile CPU, RAM, disk doluluk, OS build, uptime, kurulu yazılım. Bakım tekiri için en değerli veri.

☐ **Active Directory envanteri**

Domain'deki bilgisayarı hesapları, pasif hesaplar, OU yapısı. Kapalı cihazları da ortaya çıkarır.

☐ **Kablolu ortam taraması**

Görünür SSID'ler, girişleme izi, kanal çıkışması, rogue AP tespiti.

KAPSAM VE YETKİLENDİRME KAYDI

Adım 2 — kapsam seçimi, tarama profili ve ek modüller.

Kademeli tarama modeli

Yönetici yetkisi zorunlu olduğu için değişken olan tek şey harici araçlardır. Kurulum izni çıkmayan bir sahada bile temel keşif çalışır. Arayüzün sol altındaki rozet hangi seviyede olduğunuzu gösterir.

SEVİYE	KOŞUL	KAZANILAN YETENEK
0 — Taşınabilir	Harici araç yok	ICMP + TCP + ARP keşfi, port taraması, ters DNS, NetBIOS, HTTP/TLS parmak izi, mDNS/UPnP/SNMP kimlik tespiti
1 — Nmap	Nmap kurulu	Servis versiyonu tespiti, NSE scriptleri, daha doğru keşif
2 — Tam	Npcap kurulu	ARP taraması, işletim sistemi parmak izi, LLDP/CDP pasif dinleme

Seviye 0 ile Seviye 1 arasındaki fark hız/derinlik dengesidir: nmap servis versiyonu verir ama -sV taramayı belirgin şekilde yavaşlatır. Bu yüzden **Hızlı profilde nmap servis tespiti kapalıdır** — profilin adı sözünü tutmalıdır.

paraDedector
v0.1.1

1 Cihazı Hazırla

2 Keşfi Başlat

3 Sonuçlar

4 Rapor

Geçmiş

Tam — ARP taraması, OS parmak izi ve pasif dinleme sık.

Kilit

ADIM 1

Cihazı Hazırla

Tarama motorunun ihtiyaç duyduğu bileşenler kontrol edilir ve eksikler kurulur.
paraDedector hiçbir şey kurulmadan da çalışır — kurulan her bileşen taramayı bir seviye derinleştirir.

0 Tasınabilir
Kurulum gerekmez - ping, TCP, ARP, NetBIOS, HTTP

1 Nmap
Servis versiyonu - NSE scriptleri

2 Tam
ARP taraması - OS parmak izi - pasif dinleme

SİSTEM

Yönetici yetkisi
Uygulama yükseltilmiş yetkiyle çalışıyor.

Çalışma ortamı
Paketlenmiş sürüm (gömülü Python 3.13.0)

Veri klasörü
D:\paraDedector\data yazılabilir (542.7 GB boş).

PYTHON BAĞIMLILIKLARI

Python bağımlılıkları
11 modülün tamamı pakete gömüldü.

SNMP sorgulama
pysnmp 7.1.29 kurulu.

HARİCİ ARAÇLAR

Nmap
Nmap version 7.98 (https://nmap.org)

Npcap sürücüsü
Kurulu (sürüm 1.10.5).

TARAMA YETENEKLERİ

ICMP yoklama
Çalışıyor (geri döngü testi başarılı, TTL=128).

Scapy (ham paket)
Scapy 2.7.0 — ham paket erişimi hazır.

VERİ KAYNAKLARI

MAC üretici veritabanı
IEEE veritabanı yükü — 53.747 kayıt.

İnternet erişimi
Diğ ağa erişim var.

RAPORLAMA

Adım 1 — bileşen kontrolü; eksik olan her şey nedeniyle birlikte listelenir.

Nasıl çalışır

Cihaz keşfi

Keşif üç bağımsız kanalla yapılır, çünkü hiçbirisi tek başına yeterli değildir.

- **ICMP** — Windows'un IcmpSendEcho API'si üzerinden. Ham soket yerine bu API kullanıldığı için yönetici yetkisi gerekmez. Yanıt TTL'i işletim sistemi ailesi hakkında bedava ipucu verir.
- **TCP** — ICMP'yi engelleyen hostlar için. "Bağlantı reddedildi" (RST) yanıtı da değerlidir: port kapalı olsa bile hostun ayakta olduğunu kanıtlar.
- **ARP tablosu** — Tarama sonrası tablo yeniden okunur. Hem MAC adreslerini tamamlar hem de hiçbir şeye yanıt vermeyen sessiz cihazları (bazı yazıcılar, IoT cihazları) ortaya çıkarır.

Cihaz kimliği

Kimlik yalnızca MAC üreticisine bırakılmaz. MAC iki durumda yetersizdir: modern telefonlar gizlilik için MAC'i rastgeleleştirir, ve "TP-Link" bilgisi cihazın mesh ünitesi mi akıllı priz mi olduğunu söylemez. Bu yüzden cihazların kendi kimlik beyanları toplanır.

© ParsDX A.Ş.

www.parsdx.com

KANAL	NE VERİR
mDNS / Bonjour	Cihazın ilan ettiği ad ve model (EPSON ET-2950 Series, Deco X50) ve servis tipi (_ipp = yazıcı, _googlecast = medya)
UPnP / SSDP	Üretici, model adı ve numarası — router, TV, NAS ve mesh üniteleri
SNMP	sysDescr ile switch/AP/firewall model ve firmware; yazıcılarda sayfa sayacı
LLDP / CDP	Switch ve AP'lerin model, firmware ve bağlı olunan port numarası
DHCP	Ana bilgisayar adı ve satıcı sınıfı (android-dhcp-14) — rastgele MAC'li cihazları bile tanımlar

mDNS servis tipleri sabit listeden değil, `_services._dns-sd._udp` meta sorgusuyla ağda ne varsa keşfedilir; böylece tescilli servisler elle eklenmeden bulunur.

Sınıflandırma

Ağırlıklı kanıt toplama ile yapılır. Yukarıdaki kanalların tamamı, port imzaları, HTTP/TLS parmak izleri ve TTL değerleri puanlanır; en yüksek puanlı kategori kazanır. Her kararın gerekçesi saklanır ve arayüzde gösterilir — motor yanılabilir, teknisyen kategoriyi elle düzeltebilir ve düzeltme rapora yansır.

Üretici adı normalizasyonu

IEEE kayıtları tutarsızdır; aynı marka üç farklı biçimde geçebilir. Envanterin okunabilir kalması için adlar tek biçime indirgenir:

```
Beijing Xiaomi Electronics Co.,Ltd → Xiaomi
Seiko Epson Corporation → Epson
TP-LINK TECHNOLOGIES CO.,LTD. → TP-Link
```

Kapsam seçimi

APIPA adresleri, VPN tünelleri ve sanallaştırma switch'leri gerekçeleriyle birlikte otomatik olarak işaretli gelir. Tipik bir kurumsal dizüstünde 10+ arayüz vardır; hepsini taramak saatler sürer ve kapsam dışı sistemlere dokunur.

Modüller

Temel tarama her zaman çalışır. Aşağıdaki modüller keşif ekranından seçilir; seçilmeyen veya çalışamayan modül sessizce atlanmaz — nedeni tarama günlüğünde ve faz listesinde açıkça yazar.

MODÜL	NE YAPAR	GEREKSİNİM
Cihaz kimliği	mDNS + UPnP + SNMP ile marka/model tespiti	— (her zaman çalışır)
Pasif dinleme	LLDP/CDP komşuları, DHCP istemci adları, mDNS/NBNS yayınları	Npcap + yönetici
Kimlik bilgili envanter	WMI (Windows) ve SSH (Linux) ile CPU/RAM/disk/OS/uptime/yazılım	Hedefte yerel yönetici / SSH kullanıcısı
Active Directory	Bilgisayar ve kullanıcı hesapları, pasif kayıtlar, OS dağılımı, ağda görünmeyenler	Domain okuma yetkisi
Kablosuz ortam	SSID'ler, şifreleme, kanal yoğunluğu, rogue AP şüphesi	Kablosuz arayüz

Kimlik bilgileri yalnızca tarama boyunca bellekte tutulur. Tarama sonucu diske yazılırken kimlik bilgisi nesnesi bilerek dışarıda bırakılır; parolalar SQLite'a, JSON dışı aktarımına veya PDF'e düşmez.

Rapor çıktısı

Yönetici özeti

Ağ genel görünümü

Cihaz envanteri

Açık port ve servis matrisi

Ekler ve metodoloji

Kablosuz ortam

Active Directory envanteri

Pasif dinleme bulguları

Risk bulguları

Bakım anlaşması öneri maddeleri

parsDedector

v0.1.1

1

Cihazı Hazırla

2

Keşfi Başlat

3

Sonuçlar

4

Rapor

5

Geçmiş

Tam – ARP taraması, OS parmak izi ve pasif dinleme açık.

Kilitli

ADIM 4

Rapor

Müşteriye sunulabilir PDF raporu. Yönetici özeti ve teknik ekler ayrı bölümler halinde; istemediğiniz bölümü çıkarabilirsiniz.

RAPOR BÖLÜMLERİ

Yönetici Özeti

Envanter dağılımı, risk skoru, en kritik bulgular ve bakım anlaşması öneri maddeleri.

Ağ genel görünümü

Alt ağ tablosu, ağ geçidi/DNS bilgisi ve segmentasyon değerlendirilmesi.

Cihaz envanteri

Kategori bazlı tam cihaz listesi: IP, MAC, üretici, tem, güven skoru.

Açık port ve servis matrisi

Cihaz başına açık portlar, servis adları ve sızım bilgileri.

Kablosuz ortam

Görünen SSID'ler, şifreleme tipi, kanal dağılımı ve yoğunluk analizi. Yalnızca kablosuz modülü çalıştıysa rapora girer.

Active Directory envanteri

Bilgisayar ve kullanıcı hesapları, işletim sistemi dağılımı, pasif hesaplar ve ağla görünmeyen kayıtlar.

Pasif dinleme bulguları

LLDP/CDP kompu cihazları (switch/AP model ve port bilgisi) ile DHCP istemci adları ve statü sınıfları.

Risk bulguları

Önemli derecesine göre gruplu bulgular; her biri açıklama ve öneriyle.

Ekler ve metodoloji

Tarama parametreleri, kapsam kaydı, yöntem açıklaması ve yasal not.

RAPOR KÜNYESİ

Kurum

UBDEN A.Ş.

Yetkili

CAN KURT

Not

—

Tarih

31.08.2026 20:26

Kapsam

192.168.0.0/24

Profil

Standart

Tarama seviyesi

2 – Tam – ARP taraması, OS parmak izi ve pasif dinleme açık.

Bulunan cihaz

6

Risk skoru

88/100 (A)

Bulgu sayısı

4

Adım 4 – rapor bölümleri ve künye; çıktı doğrudan PDF olarak üretilir.

Bilinen sınırlar

Ürünün bilerek yapmadığı şeyler de en az yaptıkları kadar önemlidir.

- **SSH host anahtarı doğrulanmaz.** Keşif aracıyız; doğrulayacak bir bilgi tabanımız yok. Çalıştırılan tüm komutlar salt okunurdur.
- **LLDP/CDP duyuruları 30-60 saniyede bir yapılır.** Kısa dinleme süresinde switch yakalanmayabilir; varsayılan 90 saniyedir.
- **DHCP yakalamak zaman alır.** İstemciler yalnızca kira yenilerken konuşur.

© ParsDX A.Ş.

www.parsdx.com

Kapsam ve sınırlar

parsDedector bir **envanter aracıdır**; sızma testi veya zafiyet tarayıcısı değildir. Hiçbir sisteme giriş denemesi, parola denemesi veya açık sömürüsü yapmaz. Bulgular yalnızca ağ üzerinden gözlemlenebilen bilgilere (açık portlar, servis banner'ları, sertifika alanları) dayanır.

Tarama, yalnızca ağ sahibinin izniyle yapıldığında meşrudur. Uygulama her taramadan önce yetkilendirme onayı ister ve bunu rapora kaydeder.



parsDedector

Ağ Keşif ve Envanter Yazılımı · © ParsDX A.Ş.

Bilgi ve demo talepleri · info@parsdx.com