interniaDiscover & interniaMap — Kullanım Kılavuzu

Bu kılavuz, **interniaDiscover.py** (canlı host keşfi) ve **interniaMap.py** (port tarama + servis/versiyon + opsiyonel CVE eşlemesi) araçlarının kurulumu ve kullanımını adım adım açıklar.

> **Önemli:** Her iki araç da **Nmap** komut satırı aracını kullanır. Nmap'in sisteminizde kurulu ve `PATH` üzerinde erişilebilir olduğundan emin olun.

---

1) Kurulum

Gereksinimler

- **Python**: 3.8 veya üzeri
- **Nmap**: https://nmap.org/download.html
- **Python paketleri**: `colorama`, `requests`

Kurulum Adımları

```
# 1) Sanal ortam (opsiyonel ama tavsiye edilir)
python -m venv .venv
# Windows
.venv\Scripts\activate
# Linux/macOS
source .venv/bin/activate

# 2) Bağımlılıklar
pip install -r requirements.txt
```

> **Windows ipucu:** Nmap kurulumundan sonra Terminal'i kapatıp yeniden açın ki `nmap.exe` PATH'e eklensin.

---

2) interniaDiscover.py — Canlı Host Keşfi

Amaç: Ağda **canlı cihazları** tespit eder. Farklı ping yöntemlerini kullanır (ICMP, TCP SYN/ACK, UDP, ARP, IP Protocol).

Temel Kullanım

```
python interniaDiscover.py 192.168.1.0/24
python interniaDiscover.py 192.168.1.65 --vv --packet-trace --live
python interniaDiscover.py targets.txt --methods PS,PA --json out.json
python interniaDiscover.py 203.0.113.0/24 --preset stealth
```

Önemli Argümanlar

- **Hedef girdisi (`target`)**: CIDR (`192.168.1.0/24`), tek IP, aralık, *veya* `targets.txt` dosyası.
- **—methods** : `all` veya virgülle ayırarak: `PE,PP,PM,PS,PA,PU,PR,PO`
  - `PE` : ICMP Echo Ping (klasik ping)
  - `PP` : ICMP Timestamp
  - `PM` : ICMP Address Mask
  - `PS` : TCP SYN Ping (örn. `--ps-ports 22,80,443,3389`)
  - `PA` : TCP ACK Ping (örn. `--pa-ports 80,443`)
  - `PU` : UDP Ping (örn. `--pu-ports 53,123`)
  - `PR` : ARP Ping (aynı subnet'te çok güvenilir)
  - `PO` : IP Protocol Ping (örn. `--po-protos 1,6,17,47`)
- **—preset {fast|stealth|thorough}**
  - `fast` : `PE,PS,PR` + `-T3` + `--max-rate 200`
  - `stealth` : `PS,PA,PU` + `-T1` + `--scan-delay 200ms` + `--max-rate 30` + `--fragment`
  - `thorough` : `all` + `-T2` + `--scan-delay 100ms` + `--max-rate 80`
- **Görünürlük/Takip**: `--vv` , `--packet-trace` , `--live` , `--stats-every 2s`
- **Evasion/Timing**: `-T0…-T5` , `--scan-delay 200ms` , `--max-rate 50` , `--decoy <decoys>` , `--spoof-mac 0` , `--src-ip <IP>` , `--iface <iface>` , `--fragment` , `--mtu 8` , `--proxies` , `--defeat-rst-ratelimit`
- **Çıktı**: `--json out.json` , `--csv out.csv`
- **Diğer**: `--explain` (seçilen yöntemleri tarama öncesi açıklar), `--dry-run` , `--quiet`

Örnek Senaryolar

- **LAN'da hızlı keşif (ARP + SYN)**:

```
python interniaDiscover.py 192.168.1.0/24 --methods PR,PS --ps-ports
```

- **FW arkasında yaşıyor mu? (ACK ping)**:

```
python interniaDiscover.py 10.10.0.0/16 --methods PA --pa-ports 443,8
```

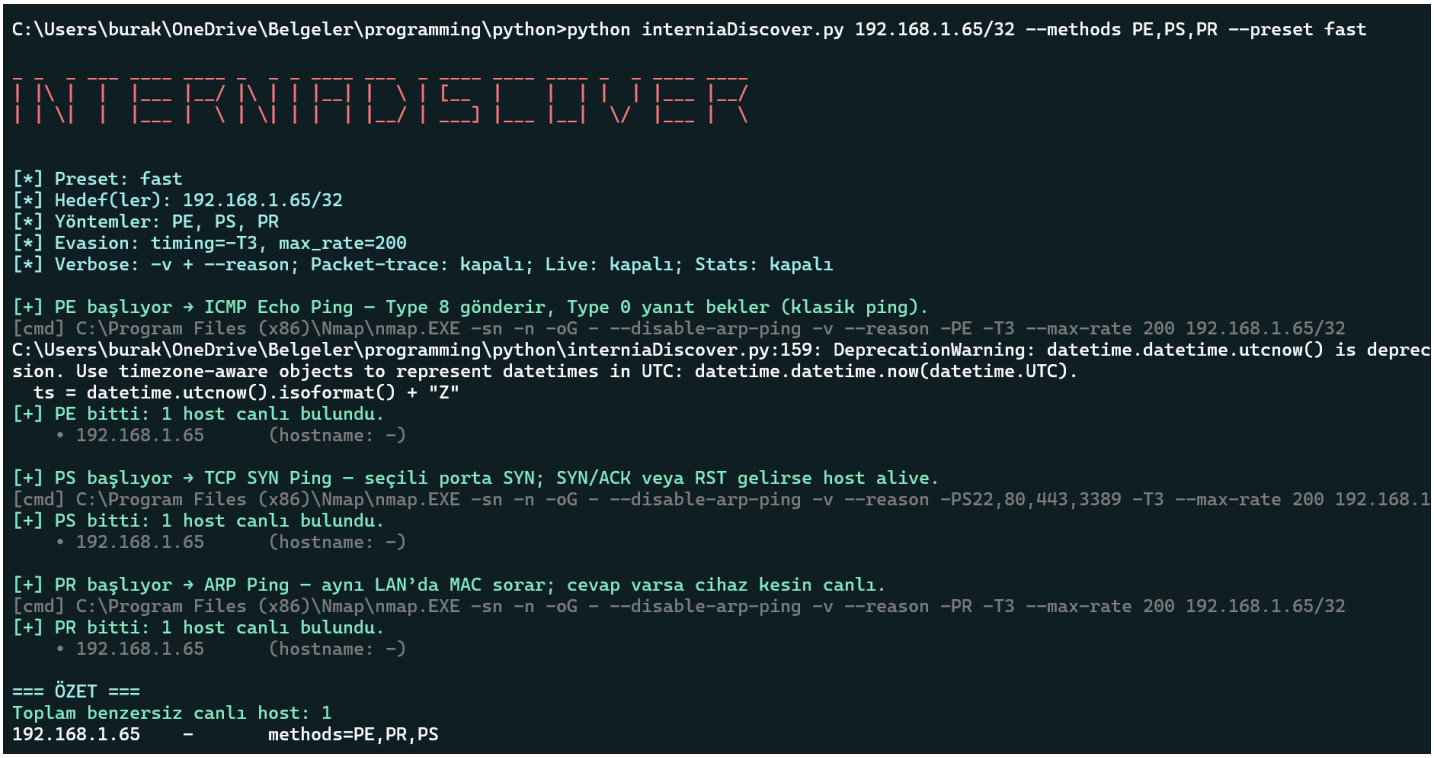
- **Sonuçları kaydetme**:

```
python interniaDiscover.py targets.txt --methods all --json discover.
```

Çıktı Örneği (özet)

```
=== ÖZET ===
Toplam benzersiz canlı host: 5
10.0.0.5        -       methods=PA,PS,PR
10.0.0.10       web-1   methods=PE,PS
...
```

ÖRNERK GÖRSEL



---

3) interniaMap.py — Port Tarama & Servis/Versiyon & CVE

Amaç: Seçilen hedef(ler)de port taraması yapar; servis/versiyon tespiti (`-sV`) ve opsiyonel **NVD** tabanlı **CVE** araması yapabilir.

Temel Kullanım

```
python interniaMap.py 192.168.1.65
python interniaMap.py 192.168.1.0/24 --udp
python interniaMap.py 192.168.1.65 -p 80,443,5173 --service-version
python interniaMap.py targets.txt --os --cve --json out.json
python interniaMap.py 192.168.1.65 --preset stealth
```

Önemli Argümanlar

- **Hedef girdisi (`target`)**: tek IP/host, CIDR (`192.168.1.0/24`) veya `targets.txt`
- **Port kapsamı** (birini seçin):
  - `-p 80,443,5173` (veya `1-65535`)
  - `--top-ports 2000`
  - `--popular web|remote|iot|mixed` (gömülü setler)
- **Tarama Teknikleri**:
  - TCP: `--connect` (varsayılan), `--syn` , `--ack` , `--fin` , `--null` , `--xmas` , `--maimon` , `--window`
  - UDP: `--udp`
- **Derinlik**:
  - `-sV, --service-version` (servis/versiyon)
  - `--os` (OS tespiti)
  - `-A, --aggressive` (küme: OS + script + traceroute vb.)
- **Verbosity/Trace**: `--vv` , `--packet-trace` , `--live` , `--stats-every 2s`
- **Evasion/Timing**: `-T0…-T5` , `--scan-delay` , `--max-rate` , `--min-rate` , `--spoof-mac` , `--src-ip` , `--iface` , `--fragment` , `--mtu` , `--proxies` , `--defeat-rst-ratelimit`
- **Çıktı**: `--json out.json` , `--csv out.csv`
  - **CVE eşleme (NVD)**: `--cve` (opsiyonel), `--cve-max 5`

CVE Eşleme Nasıl Çalışır?

- `--cve` kullanıldığında, **tüm açık portlar** için servis/bannerdan **ürün** ve **versiyon** bilgisi toplanır (ör. `nginx 1.18.0`).
- Bu metin ile **NVD** API'de arama yapılır ve ilk sonuçlardan kısa bir özet eklenir.

- **Öneri:** Doğruluk için `-sV` ile birlikte kullanın.

```
python interniaMap.py 192.168.1.65 -p 80,443 -sV --cve --cve-max 3 --jsor
```

Presetler

- `fast`: `--top-ports 200` + `-T4` + `--max-rate 1000`
- `stealth`: `-T1` + `--scan-delay 200ms` + `--max-rate 50` + `--fragment` (SYN ile uyum notu: Connect taramada fragment etkisizdir)
- `thorough`: `-sV` + `--top-ports 2000` + `-T2` + `--scan-delay 100ms` + `--max-rate 200`

Çıktı Örneği (özet)

```
=== SONUÇ ===
[+] 192.168.1.65 (hostname: -) — 2 açık port
    • tcp/80   http — nginx 1.18.0
        ↳ CVE-2021-23017: ...
    • tcp/443  https — nginx 1.18.0 (TLS1.2)
        ↳ CVE-2021-...: ...
```

ÖRNEK GÖRSEL

```
C:\Users\burak\OneDrive\Belgeler\programming\python>python interniaMap_reviewed.py 192.168.1.65 --os --ports 8081 --vv  -sV --cve
[!] Yalnızca yetkili olduğun hedefleri tara. İzinsiz tarama hukuka aykırı olabilir.

 _ _  _ ___ ____ ____ _  _ _ ____ _  _ ____ ___
 | |\ |  |  |___ |__/ |\ | | |__| |\/| |__| |__]
 | | \|  |  |___ |  \ | \| | |  | |  | |  | |


[*] Hedef: 192.168.1.65
[*] Port kapsamı: 8081
[*] TCP modları: connect (varsayılan)
[*] UDP: kapalı; sV: açık; OS: açık; A: kapalı
[*] Evasion: yok
[*] Verbose: -vv + --reason; Packet-trace: kapalı; Live: kapalı; Stats: kapalı
[cmd] C:\Program Files (x86)\Nmap\nmap.EXE -n -oX - -vv --reason -p 8081 -sT -sV -O 192.168.1.65

=== SONUÇ ===
[+] 192.168.1.65        (hostname: -) — 1 açık port
    • tcp/8081  http — Apache httpd 2.4.25 ((Debian))
        ↳ CVE-2016-8743: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted fr
s. Accepting these different behaviors represe
    -- OS tahminleri:
      - Microsoft Windows 10 1607 - 11 23H2 (~%99)
      - Microsoft Windows 10 1511 (~%97)
      - Windows 11 21H2 (~%97)
      - Microsoft Windows 10 1703 (~%96)
      - Windows Server 2022 (~%96)
      - Microsoft Windows 10 1703 or Windows 11 21H2 (~%96)
      - Microsoft Windows 10 1703 - 11 21H2 (~%95)
      - Microsoft Windows 11 21H2 (~%95)
      - Microsoft Windows 7 or 8.1 R1 (~%94)
      - Microsoft Windows 10 1607 (~%94)
```

---

4) İleri Seçenekler ve İpuçları

- **Hedef dosyası (targets.txt)**: Her satıra bir hedef yazın (IP, CIDR veya host adı).
- **DNS'i kapatma**: Araçlar varsayılan olarak `-n` ile DNS çözümlemeyi kapatır (daha hızlı ve gürültüsüz).
- **Windows PowerShell örneği**:

```
python .\interniaMap.py 192.168.1.65 --vv --stats-every 3s --json out
python .\interniaDiscover.py 192.168.1.0/24 --methods PR,PS --ps-port
```

- **Hız / Gürültü dengesi**: `-T4/5` ve yüksek `--max-rate` hızlıdır ama tespit edilme ve paket kaybı riski artar.
- **UDP taramaları**: `--udp` + yeterli izinler/gereken firewall ayarları. UDP'de false negative olasılığı daha yüksektir.
- **Deadlock önleme**: Her iki araçta da Nmap'ın `stdout` / `stderr` birleşik okunur; `--live` ile anlık log akışı alabilirsiniz.

---

5) Hata Giderme (Troubleshooting)

- `Nmap bulunamadı` **hatası**: Nmap kurulu değil ya da PATH'te değil.
- `Permission denied` **/ Raw socket gereken işlemler**: Bazı teknikler yönetici/Root gerektirebilir. Windows'ta "Yönetici olarak çalıştır", Linux'ta `sudo` kullanın.
- `--cve` **sonuç getirmiyor**: Banner boş olabilir; doğruluk için `-sV` ekleyin. NVD oran limiti/ping'e takılmamak için bir süre sonra tekrar deneyin.
- `--packet-trace` **çok gürültülü**: Sadece hata ayıklamada kullanın.
- **Çok yavaş**: `--top-ports` sayısını düşürün veya preset `fast` deneyin. `--max-rate` ile hız artırın (kayba dikkat).

---

6) Hukuki Uyarı

Bu araçları yalnızca **yetkili olduğunuz** sistem ve ağlarda kullanın. İzinsiz tarama **yasa dışıdır** ve sorumluluk size aittir.

---

7) Sürüm Bilgisi

- Kılavuz: 2025-08-11

- Scriptler: `interniaDiscover.py` ve `interniaMap.py` (kullanım örnekleri ve argüman isimleri bu sürüme göredir)