**Netdiscover Nedir?**

Netdiscover, aktif veya pasif olarak ağdaki cihazları tespit etmek için kullanılan hafif ve hızlı bir ağ keşif aracıdır. Özellikle DHCP sunucularının olduğu ortamlarda, IP-mac eşleşmelerini ve aktif istemcileri tespit etmek için kullanılır. Saldırganlar veya sızma testi uzmanları, bir ağdaki varlıkları hızlıca listelemek istediklerinde bu aracı tercih ederler.

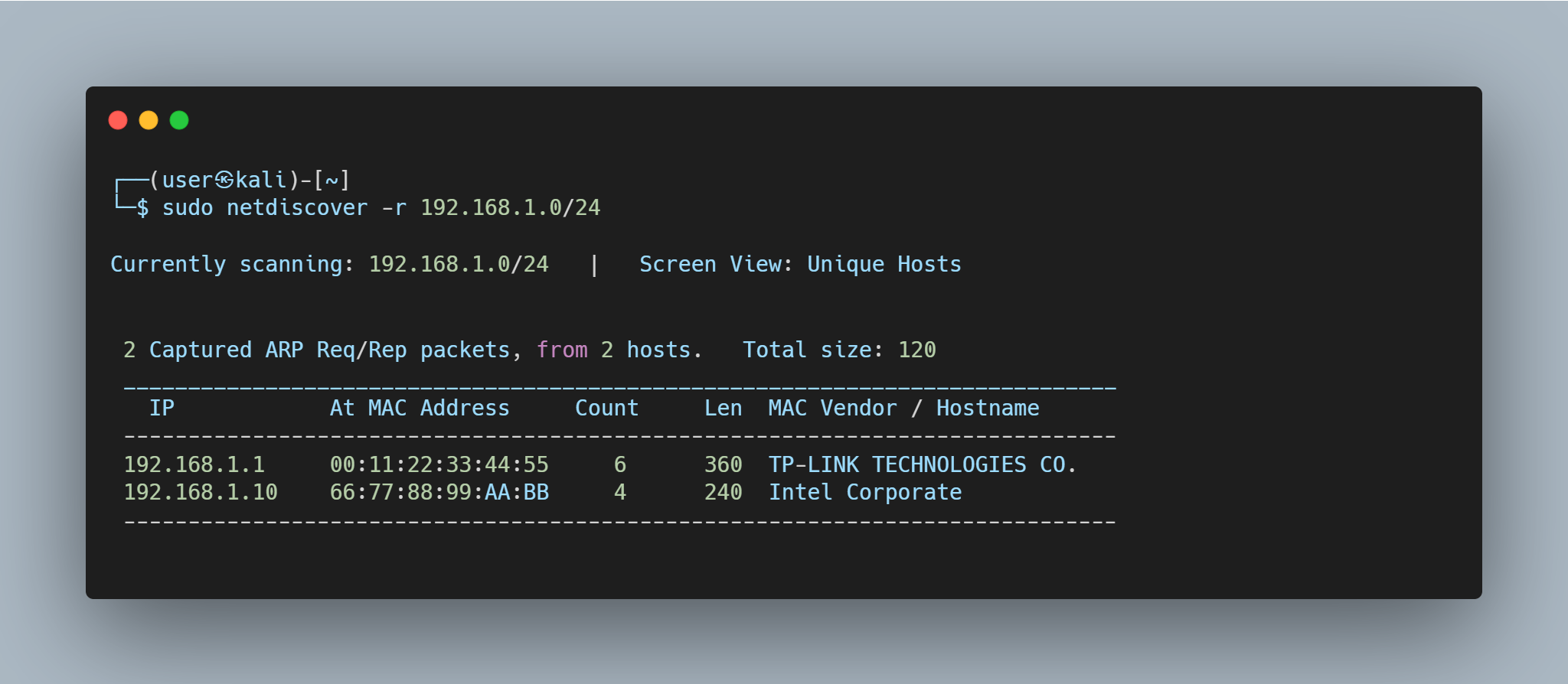
Netdiscover, ARP (Address Resolution Protocol) paketlerini kullanarak ağda kimlerin bulunduğunu belirler. Bu sayede ağ üzerinde bağlı olan bilgisayar, yazıcı, kamera veya IoT cihazlarını görebilirsiniz.

**Netdiscover Ne İşe Yarar?**

* İç ağdaki IP adreslerini, MAC adreslerini ve üretici bilgilerini bulur.
* Hedef ağı belirlemeden önce keşif (reconnaissance) yapmanıza olanak sağlar.
* Pasif modda çalıştırıldığında ağ trafiğini dinleyerek istemcileri tespit eder.
* Özellikle DHCP ağlarında güvenlik analizlerinde ilk adım olarak kullanılır.

Temel Kullanımı: **sudo netdiscover**

Ya da belirli bir IP bloğunda tarama yapmak için: **sudo netdiscover -r 192.168.1.0/24**



* sudo netdiscover -r 192.168.1.0/24: Belirtilen IP bloğu içinde aktif cihazları ARP yoluyla tarar.
* “At MAC Address” sütununda hedef cihazların MAC adresleri yer alır.
* “MAC Vendor” kısmı cihazın üreticisini belirtir.

**Hangi Durumlarda Kullanılır?**

Netdiscover, özellikle bilinmeyen ya da belgelememiş bir ağa sızıldığında kullanılır. Penetrasyon testlerinde ilk aşama olan bilgi toplama (reconnaissance) evresinde, hedef ağda hangi cihazların aktif olduğunu görmek için ideal bir araçtır.  
Şirket içi ağlarda, BT ekipleri de zaman zaman bu aracı ağ envanterini hızlıca görmek için kullanır.

**Çalışma Prensibi**

Netdiscover, ARP istekleri (ARP request) göndererek IP adreslerine karşılık gelen MAC adreslerini bulur. Ardından bu MAC adreslerinin üreticilerini de (vendor) veritabanından tanımlar. Bu sayede ağda tanımlanamayan bir cihaz varsa, MAC adresi ve üreticisine bakarak ne tür bir cihaz olduğunu tahmin edebilirsiniz.

Pasif modda çalıştırıldığında, Netdiscover kendi paket göndermek yerine ağı dinleyerek trafiği analiz eder. Bu yöntem, daha gizli çalışmak isteyenler için tercih edilir.

**Kullanım Parametreleri**

| **Parametre** | **Açıklama** |
| --- | --- |
| -r | Belirli bir IP aralığını tarar. (örn: -r 192.168.1.0/24) |
| -i | Belirli bir ağ arayüzünü seçer. (örn: -i eth0) |
| -p | Pasif modda çalışır, sadece ağı dinler. |
| -s | Tarama hızını belirler (yavaş/hızlı). |
| -f | Eski verileri temizleyip yeni bir tarama başlatır. |

**Güvenlik Testlerinde Kullanım Senaryosu**

Örneğin, bir sızma testinde dışardan erişim sağlandıysa ve iç ağa geçiş yapıldıysa, ilk yapılması gereken iç ağda kimlerin olduğunu belirlemektir. Bu noktada Netdiscover devreye girer. IP aralığı bilinmiyor olabilir; DHCP'den alınan bir IP üzerinden /24 ağı taranarak tüm istemciler hızlıca listelenir.

Bu bilgiler ışığında;

* Potansiyel hedef cihazlar seçilebilir,
* Aynı MAC adresine sahip klonlanmış sistemler ayırt edilebilir,
* Güvensiz veya bilinmeyen cihazların (örneğin kişisel cep telefonları, rogue cihazlar) varlığı tespit edilebilir.

**Avantajları**

* Hafif ve hızlıdır; düşük donanımda dahi rahatça çalışır.
* GUI gerektirmez, tamamen terminal tabanlıdır.
* ARP tabanlı çalıştığı için firewall’ların çoğu tarafından engellenmez.
* Ağda çok sayıda cihaz olsa bile saniyeler içinde sonuç verir.