

Netdiscover

Netdiscover是一个主动/被动的ARP侦查工具。该工具在不使用DHCP的无线网络上非常有用。使用Netdiscover工具可以在网络上扫描IP地址，ARP侦查工具Netdiscover检查在线主机或搜索为它们发送的ARP请求。

1.主动

```
netdiscover -i eth0 -r 192.168.79.131/24
```

使用netdiscover通过网卡来搜索192.168.79.131主机下的局域网内所有主机。

```
C:\root> netdiscover -i eth0 -r 192.168.79.131/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
```

```
76 Captured ARP Req/Rep packets, from 4 hosts. Total size: 4560
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.79.1	00:50:56:c0:00:08	64	3840	VMware, Inc.
192.168.79.2	00:50:56:f8:39:77	6	360	VMware, Inc.
192.168.79.131	00:0c:29:c0:6c:ab	4	240	VMware, Inc.
192.168.79.254	00:50:56:f9:e2:42	2	120	VMware, Inc.

2.被动

```
netdiscover -p
```

获取经过“我”的arp流量/主机

```
C:\root> netdiscover -p
```

```
Currently scanning: (passive) | Screen View: Unique Hosts
```

```
22 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1320
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.79.1	00:50:56:c0:00:08	16	960	VMware, Inc.
192.168.79.2	00:50:56:f8:39:77	4	240	VMware, Inc.
192.168.79.131	00:0c:29:c0:6c:ab	2	120	VMware, Inc.