[redacted]

[redacted] nmap [redacted]

[redacted]

[redacted]

nmap [redacted]

[redacted]

اگر nmap روی سامانه نصب نیست، فرمان زیر به شما اجازه میدهد nmap را روی توزیع اوبونتو نصب کنید .

```
sudo apt-get install nmap
```

برای نصب nmap روی توزیع فدورا از فرمان زیر استفاده کنید :

```
sudo dnf install nmap
```

فرمان فوق nmap را روی Manjaro نصب میکند.

```
sudo pacman -Syu nmap
```

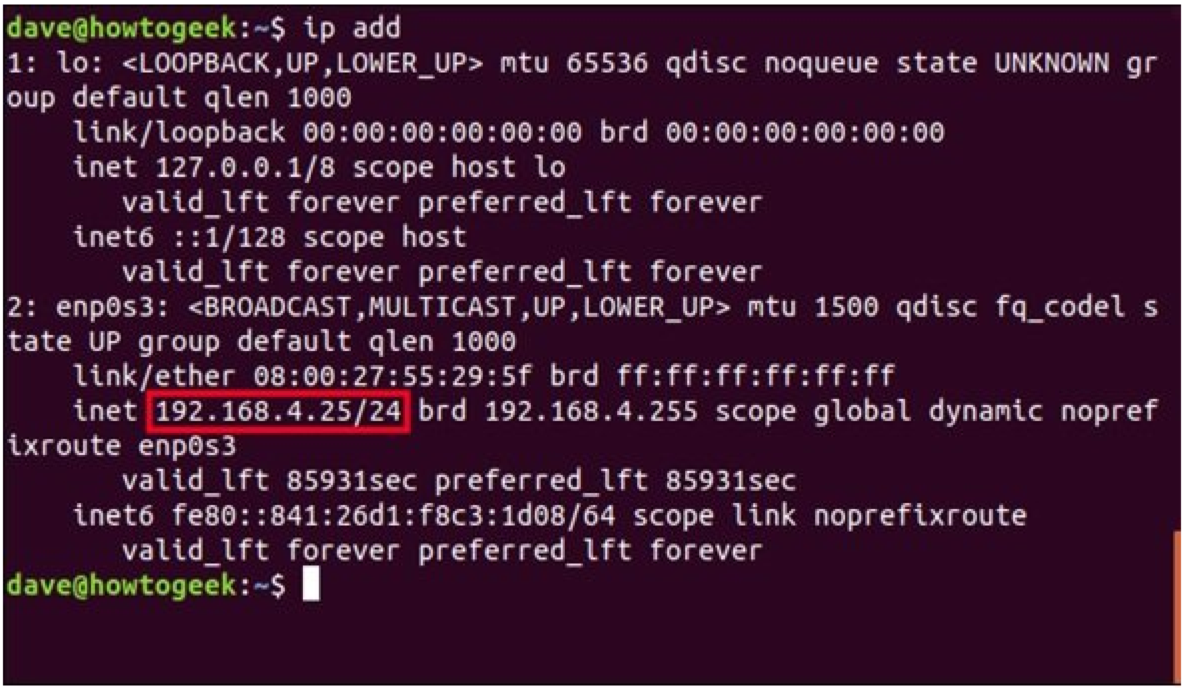
شما میتوانید nmap را روی سایر توزیعهای لینوکسی با استفاده از ابزار مدیریت بستهها نصب کنید .

پیدا کردن آدرس آیپی خودتان

در اولین گام باید آدرس آیپی کامپیوتر لینوکسی خودتان را پیدا کنید . در اینجا یک آدرس آیپی کمینه و بیشنه وجود دارد که کامپیوتر شما از آن استفاده میکند . در اینجا محدودهای از آدرسهای آیپی را مشاهده میکنید که شبکه برای مدیریت دستگاهها از آنها استفاده میکند . ما در اینجا باید آدرسهای آیپی یا محدودهای از آدرسهای آیپی را برای nmap مشخص کنیم، به همین دلیل ابتدا باید این مقدار را پیدا کنیم . لینوکس یک فرمان دمدستی به نام ip دارد که فرمان فوق گزینهای به نام addr دارد . برای استفاده از فرمان فوق ip را تایپ کرده، با کلید spacebar یک فاصله ایجاد کرده، addr را نوشته و کلید اینتر را فشار دهید .

```
ip addr
```

در انتهای فرمان فوق شما آدرس آیپی خودتان را مشاهده میکنید . آدرس فوق با برچسب inet مشخص شده است.



[illegible] 192.168.4.25 [illegible]. /24 [illegible] 1 [illegible]. 3x8=24

[illegible]:

```
11111111.11111111.11111111.00000000
```

[illegible] 255.255.255.0 [illegible].

[illegible] 8 [illegible] 255 [illegible] 192.168.4.0 [illegible] 192.168.4.255 [illegible]. /24 [illegible]. nmap [illegible] nmap [illegible].

nmap [illegible]

Nmap [illegible]. nmap [illegible] nmap [illegible]. -sn [illegible] nmap [illegible]. 192.168.4.0/24 [illegible] nmap [illegible] 192.168.4.0 [illegible] 192.168.4.255 [illegible]. sudo [illegible].

```
sudo nmap -sn 192.168.4.0/24
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-06-28 10:57 EDT
Nmap scan report for Vigor.router (192.168.4.1)
Host is up (0.00039s latency).
MAC Address: 00:1D:AA:B8:60:B0 (DrayTek)
Nmap scan report for 192.168.4.10
Host is up (0.00058s latency).
MAC Address: B8:27:EB:D3:98:2D (Raspberry Pi Foundation)
Nmap scan report for 192.168.4.11
Host is up (0.074s latency).
MAC Address: E4:F0:42:58:FF:98 (Unknown)
Nmap scan report for 192.168.4.12
Host is up (0.10s latency).
MAC Address: D8:50:E6:7F:7F:A7 (Asustek Computer)
Nmap scan report for 192.168.4.13
Host is up (-0.10s latency).
MAC Address: B4:B0:17:99:23:1C (Avaya)
Nmap scan report for 192.168.4.15
Host is up (-0.10s latency).
MAC Address: 44:6D:57:6E:5F:56 (Liteon Technology)
Nmap scan report for 192.168.4.17
```

```
Host is up (0.010s latency).
MAC Address: 34:D2:70:64:FB:42 (Amazon Technologies)
Nmap scan report for 192.168.4.22
Host is up (0.00063s latency).
MAC Address: 00:15:99:7F:63:CB (Samsung Electronics)
Nmap scan report for 192.168.4.23
Host is up (0.00044s latency).
MAC Address: EC:F4:BB:07:AB:C3 (Dell)
Nmap scan report for 192.168.4.24
Host is up (0.16s latency).
MAC Address: 14:D1:69:12:5A:FB (Unknown)
Nmap scan report for 192.168.4.30
Host is up (0.00050s latency).
MAC Address: 90:B1:1C:5E:8A:86 (Dell)
Nmap scan report for 192.168.4.31
Host is up (0.0046s latency).
MAC Address: C0:3F:D5:69:26:24 (Elitegroup Computer Systems)
Nmap scan report for howtogeek (192.168.4.25)
Host is up.
Nmap done: 256 IP addresses (15 hosts up) scanned in 6.76 seconds
dave@howtogeek:~$
```

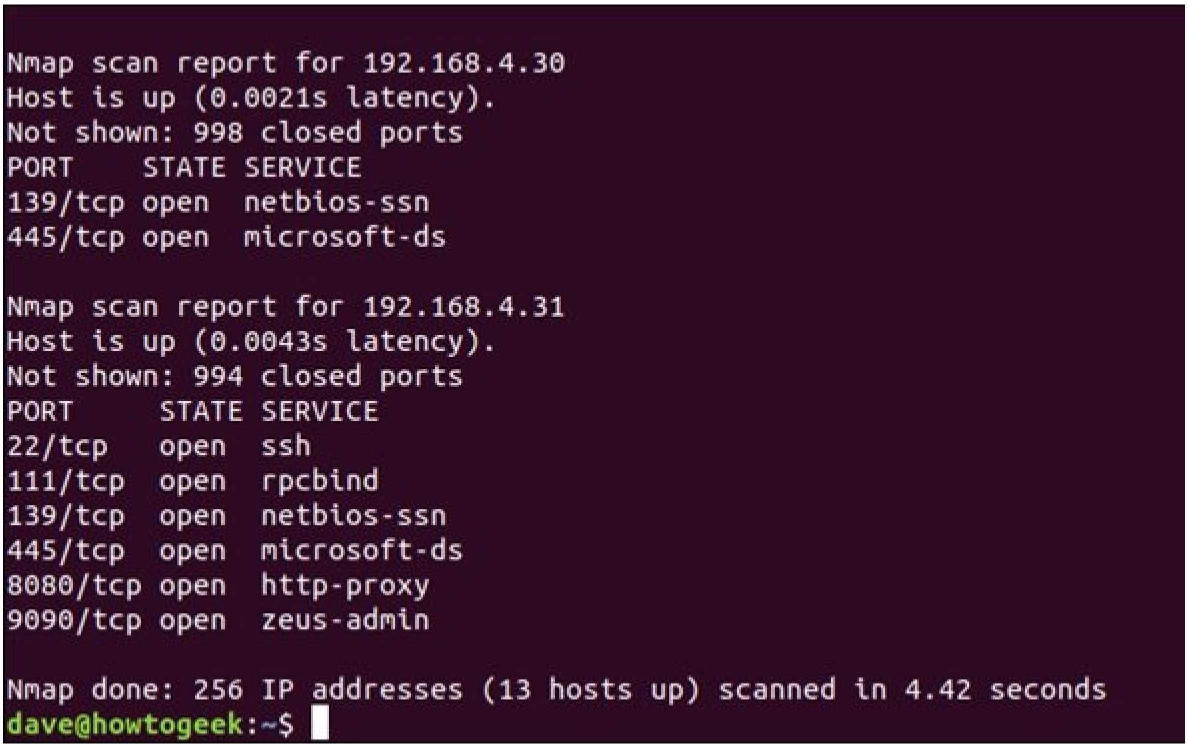
به روشنی قابل تشخیص است، اما برای برخی از دستگاهها باید کار بیشتری انجام دهید .

انجام یک پویش عمیقتر

اگر گزینه -sn را از فرمان nmap حذف کنیم، nmap پورتهای دستگاهها را نیز بررسی میکند . هر برنامه یا سرویس درون یک دستگاه یک شماره پورت دارد. ترافیک شبکه به یک آدرس آیپی و یک پورت و نه فقط به یک آدرس آیپی تحویل داده میشود . برخی از شماره پورتها از پیش تعیین شده یا رزرو شدهاند . آنها همیشه برای انتقال ترافیک شبکه برای انجام کار خاصی استفاده میشوند . بهطور مثال، پورت 22 برای اتصالات SSH محفوظ است و پورت 80 برای ترافیک وب HTTP محفوظ است. ما قصد داریم از nmap برای اسکن کردن پورت هر دستگاه استفاده کنیم تا ببینیم کدامیک از آنها باز هستند . برای این منظور فرمان زیر را اجرا میکنیم .

```
nmap 192.168.4.0/24
```

این مرتبه جزییات دقیقتری در ارتباط با هر دستگاه به دست خواهیم آورد . خروجی فرمان زیر همانند شکل زیر است.



```
Nmap scan report for 192.168.4.30
Host is up (0.0021s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.4.31
Host is up (0.0043s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
9090/tcp open  zeus-admin

Nmap done: 256 IP addresses (13 hosts up) scanned in 4.42 seconds
dave@howtogeek:~$
```

با تو .جه به اینکه خروجی این فرمان شامل اطلاعات زیادی میشود، شما میتوانید خروجی را به درون یک فایل متنی انتقال دهید . دستور زیر چنین کاری را انجام میدهد .

```
nmap 192.168.4.0/24 > nmap-list.txt
```

فرمان nmap قابلیتهای دیگر نیز دارد که پیشنهاد میکنم کمی وقت صرف کرده و همه آن قابلیتها را کشف کنید .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
ترفند شبکه
تاریخ انتشار :

□□□□□
https://www.shabakeh-mag.com/tricks/network-tricks/15721/%DA%86%DA%AF%D9%88%D9%:□□□□
86%D9%87-%D8%A7%D8%B2-%D9%81%D8%B1%D9%85%D8%A7%D9%86-nmap-
%D8%AF%D8%B1-%D9%84%DB%8C%D9%86%D9%88%DA%A9%D8%B3-
%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%B4%D8%A7%D9%87%D8%AF%D9%87-
%D8%AF%D8%B3%D8%AA%DA%AF%D8%A7%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-
%D9%85%D8%AA%D8%B5%D9%84-%D8%A8%D9%87-%D8%B4%D8%A8%DA%A9%D9%87