چگونه از فرمان nmap در لینوکس برای مشاهده دستگاه‌های متصل به شبکه استفاده کنیم؟

به این موضوع فکر می‌کنید که چه دستگاه‌هایی به شبکه خانگی شما متصل شده‌اند؟ ممکن است از دستگاه‌هایی که بدون اطلاع شما به شبکه خانگی متصل شده‌اند، شگفت زده شوید، اما چگونه این دستگاه‌ها را شناسایی کنیم؟ در این مقاله با نحوه استفاده از فرمان nmap در لینوکس برای شناسایی همه دستگاه‌های متصل به شبکه آشنا خواهید شد.

برخی از مردم تصور می‌کنند شبکه خانگی یک موجودیت کاملا ساده است که هیچ‌گونه نکته پنهان خاصی در ارتباط با آن وجود ندارد و نیازی نیست دانش خود در خصوص این شبکه‌ها را افزایش دهند. شاید دیدگاه فوق در گذشته درست بود، اما با گسترش دستگاه‌های اینترنت اشیا، دستگاه‌های همراه مانند گوشی‌های هوشمند و تبلت‌ها، انقلاب خانه‌های هوشمند در کنار دستگاه‌های معمولی همچون روترهای باند پهن، لپ‌تاپ‌ها و کامپیوترهای رومیزی چشمان شما باید کاملا باز باشند. کاربرانی که سیستم‌عامل ویندوز 10 روی سامانه‌های آن‌ها نصب شده است، به راحتی قادر به شناسایی این مسئله هستند، اما چگونه در لینوکس دستگاه‌های فوق را شناسایی کنیم؟ پاسخ در واژه‌ای به نام Nmap نهفته است.

اولین گام نصب nmap

در این مقاله قصد داریم از فرنام Nmap برای شناسایی دستگاه‌های متصل به شبکه استفاده کنیم. بسته به پکیج نرم‌افزاری که روی سامانه خود نصب کرده‌اید، ممکن است به مجبور شوید nmap را روی سامانه خود نصب کنید.

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
```

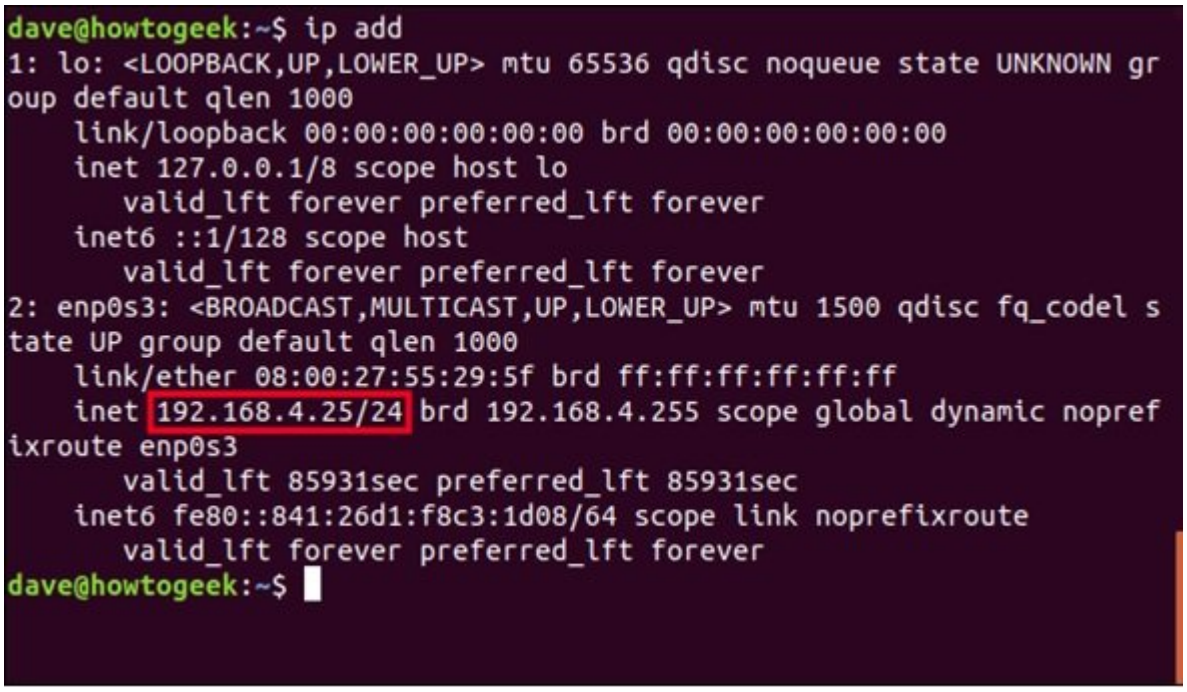
شما می‌توانید nmap را روی سایر توزیع‌های لینوکسی با استفاده از ابزار مدیریت بسته‌ها نصب کنید.

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.



آدرس آی‌پی در تصویر بالا برابر با 192.168.4.25 است. /24 به معنای آن است که سه مجموعه متوالی از هشت 1 در ماسک زیر شبکه وجود دارد. 3x8=24

در سیستم باینری، ماسک زیر شبکه برابر با مقدار زیر است:

```
11111111.11111111.11111111.00000000
```

در سیستم دهدهی این مقدار برابر با 255.255.255.0 است.

ماسک زیرشبکه و آدرس آی‌پی برای نشان دادن این‌که کدام قسمت از آدرس آی‌پی برای شناسایی شبکه و کدام قسمت برای شناسایی دستگاه‌ها است استفاده می‌شوند. این ماسک زیر شبکه به سخت‌افزار اطلاع می‌دهد که سه

شماره اول آدرس آی‌پی شبکه را شناسایی می‌کند و بخش چهارم آدرس آی‌پی است که برای شناسایی دستگاه‌های منحصر به فرد از آن استفاده می‌شود. از آنجایی که بزرگ‌ترین مقداری که شما می‌توانید نگه‌داری کنید یک مقدار 8 بیتی باینری و برابر با 255 است، آدرس آی‌پی برای این شبکه در محدوده 192.168.4.0 تا 192.168.4.255 است. همه این موارد در /24 درج شده است. خوشبختانه، nmap با این علامت کار می‌کند، بنابراین کاری که ما باید انجام دهیم به‌کارگیری nmap است.

شروع به‌کارگیری nmap

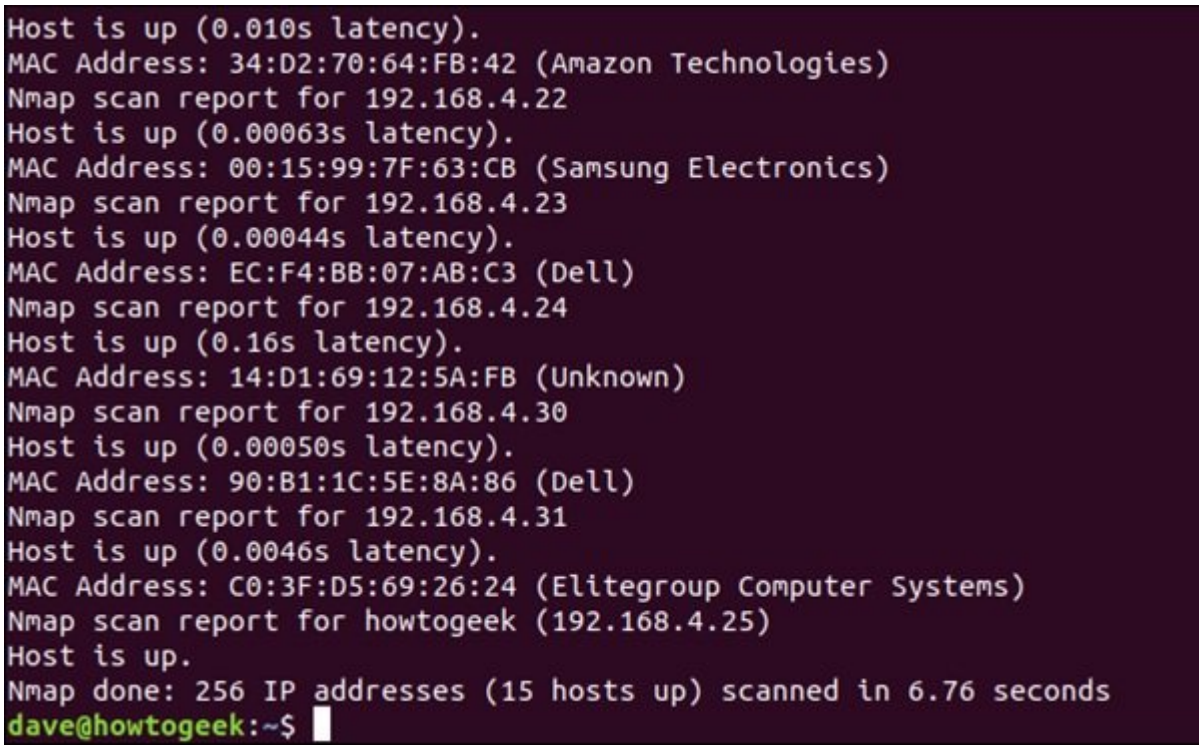
Nmap یک ابزار نگاشت شبکه است. nmap با ارسال پیام‌های مختلف شبکه مختلف به آدرس‌های آی‌پی در محدوده‌ای که ما برای آن مشخص می‌کنیم کار می‌کند. بیایید یک اسکن ساده با nmap را انجام دهیم. ما قصد داریم از گزینه -sn (پویش بدون پورت) استفاده کنیم. این گزینه به nmap می‌گوید در حال حاضر نیازی نیست وضعیت پورت‌های روی دستگاه‌ها را بررسی کند. در نتیجه یک اسکن سبک و سریع را انجام خواهد داد. دقت کنید هرچه تعداد دستگاه‌های درون یک شبکه زیاد باشند، به همان نسبت انجام کار نیز زمان‌بر خواهد بود. آدرس آی‌پی که ما قصد استفاده از آن‌را داریم آدرسی است که از اجرای فرمان قبل به دست آوردیم. در این‌جا پارامتر 192.168.4.0/24 برای nmap بع معادل آدرس آی‌پی برای شروع برابر با 192.168.4.0 است ترجمه شده و همه آدرس‌های آی‌پی تا محدوده 192.168.4.255 را شامل می‌شود. دقت کنید ما از sudo به شرح زیر استفاده می‌کنیم.

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

پس از یک انتظار کوتاه، خروجی فرمان فوق در پنجره ترمینال نوشته می‌شود. شما می‌توانید این اسکن را بدون استفاده از sudo اجرا کنید، اما استفاده از sudo تضمین می‌کند که اطلاعات تا حد امکان استخراج خواهند شد. به‌طور مثال، بدون sudo این پویش اطلاعات تولید کننده را باز نمی‌گرداند.

```
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
```

مزیت استفاده از گزینه -sn در اسکن سریع و سبک خلاصه شده است که فهرستی روشن از آدرس‌های جاری را ارائه می‌کند. به عبارت دیگر، ما فهرستی از دستگاه‌های متصل به شبکه را همراه با آدرس آی‌پی آن‌ها در اختیار داشته و در صورت امکان، nmap اطلاعات تولیدکننده دستگاه را نیز ارائه می‌کند. در تصویر زیر فهرست ارائه شده را همراه با مشخصات تولیدکنندگان مشاهده می‌کنید.



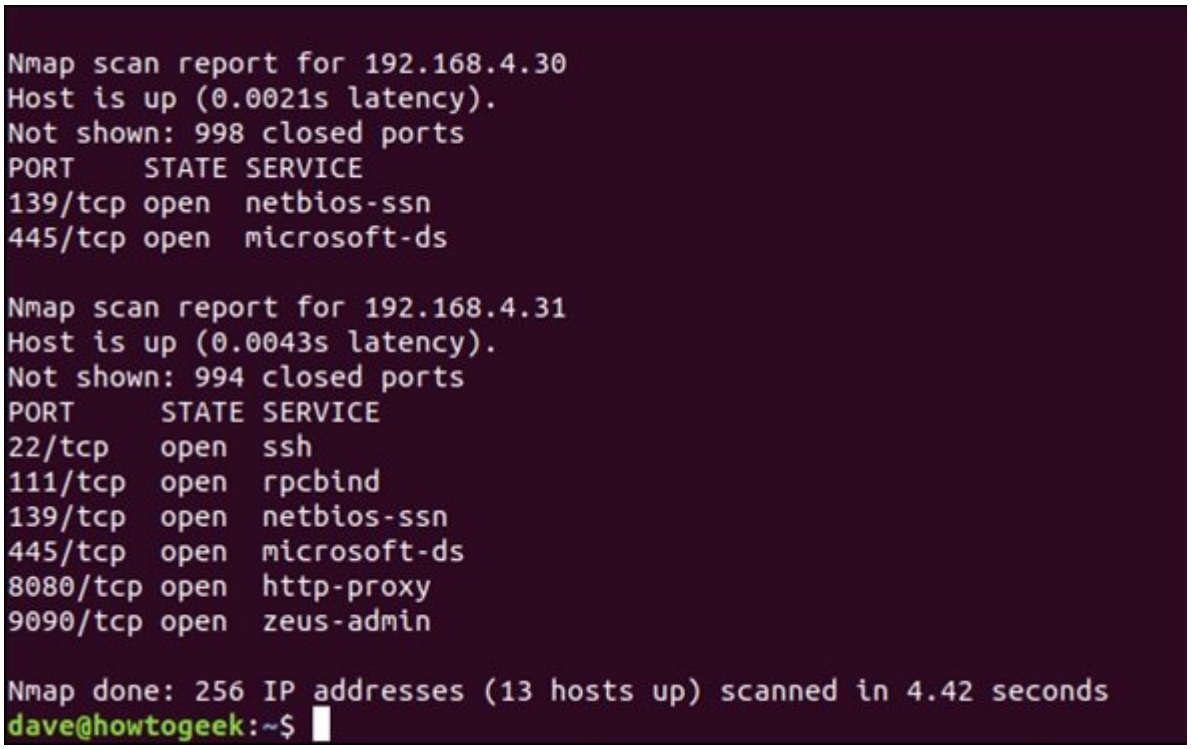
ما اکنون فهرستی از دستگاه‌های متصل به شبکه در اختیار داریم، بنابراین می‌دانیم چه تعداد دستگاه به شبکه متصل شده‌اند. در تصویر بالا 15 دستگاه روشن و متصل به شبکه وجود دارد. ما نام برخی تولیدکنندگان دستگاه‌ها را نیز می‌دانیم. به احتمال زیاد مشخصات برخی از دستگاه‌ها همچون رزبری پای به روشنی قابل تشخیص است، 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.



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.

تاریخ انتشار:

28 مرداد 1398

نشانی منبع:
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