

How to Generate an Asset Inventory Using Nmap

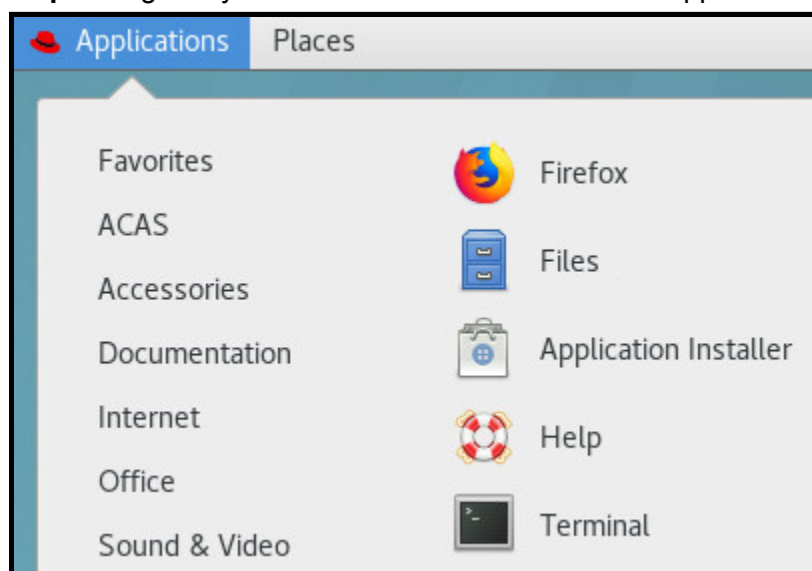
Task. Generate an asset inventory using Nmap.

Purpose. Generating and monitoring your asset inventory is the first Critical Security Control recommended by the Center for Internet Security. An asset inventory is a list of devices connected to your enterprise physically, virtually, and/or remotely. An asset inventory enables you to “accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate” (<https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/>).

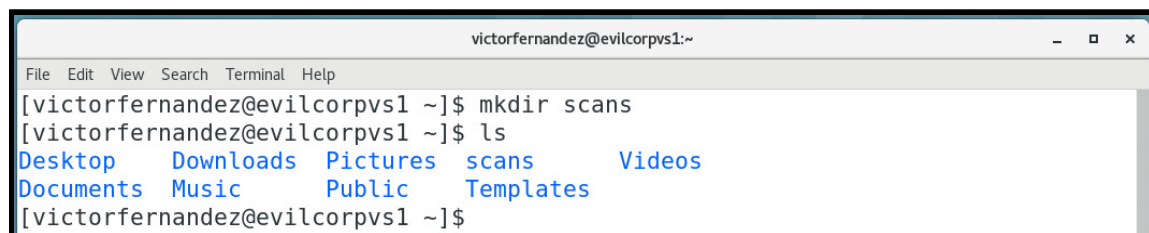
Conditions. You have knowledge of the IP address range, administrator privileges, and access to Nmap (this How-to uses the Nmap binary file that ships with Red Hat Enterprise Linux 7).

Standard. You were able to generate an asset inventory using Nmap.

Step 1. Login to your administrator account. Click “Applications” and select “Terminal.”

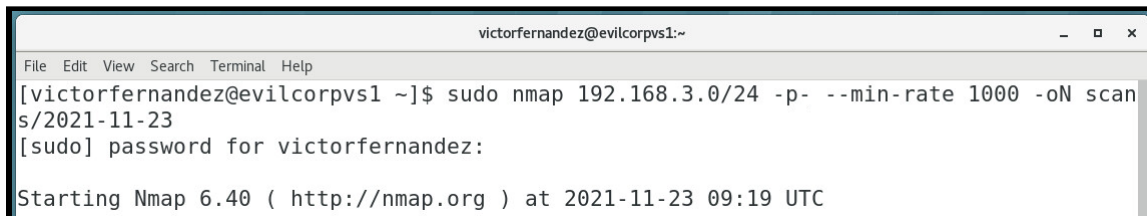


Step 2. Type “mkdir scans” to make a directory called “scans.” This directory will be used to house your Nmap scans. Type “ls” to list the contents of your current directory and confirm “scans” was created.



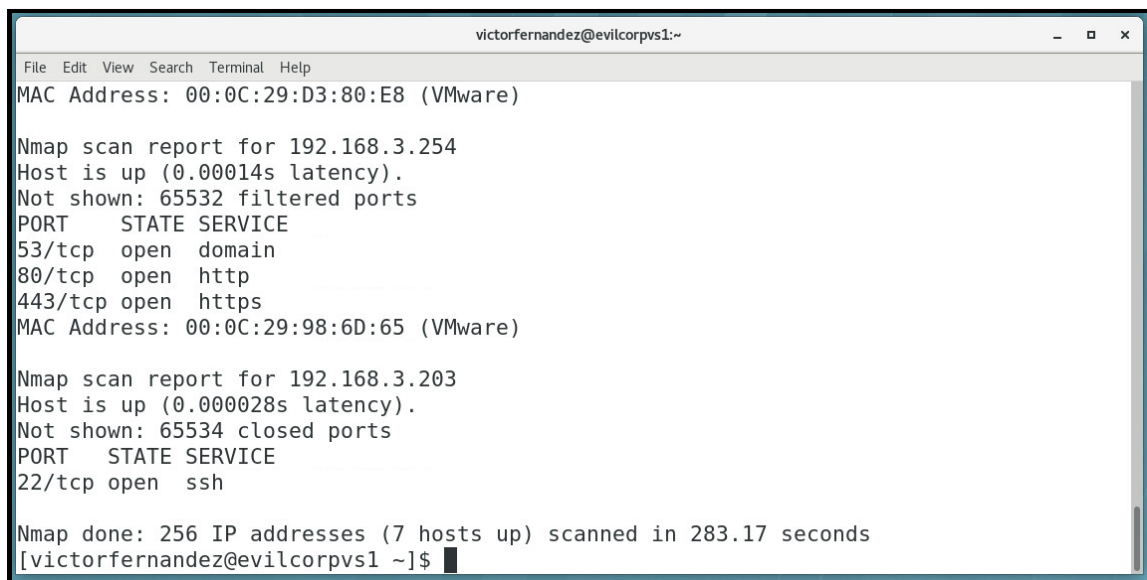
How to Generate an Asset Inventory Using Nmap

Step 3. In the next instruction, replace “192.168.3.0/24” with your IP address range and “2021-11-23” with today’s date. Type “sudo nmap 192.168.3.0/24 -p- -sS -sU --min-rate 1000 -oN scans/2021-11-23.” Type your password when prompted.

A terminal window titled 'victorfernandez@evilcorpvs1:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command '[victorfernandez@evilcorpvs1 ~]\$ sudo nmap 192.168.3.0/24 -p- --min-rate 1000 -oN scans/2021-11-23' is entered. The prompt '[sudo] password for victorfernandez:' is shown. The output is 'Starting Nmap 6.40 (http://nmap.org) at 2021-11-23 09:19 UTC'.

```
victorfernandez@evilcorpvs1:~  
File Edit View Search Terminal Help  
[victorfernandez@evilcorpvs1 ~]$ sudo nmap 192.168.3.0/24 -p- --min-rate 1000 -oN scans/2021-11-23  
[sudo] password for victorfernandez:  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-11-23 09:19 UTC
```

The command sentence above includes a number of arguments. “sudo” means “super user do,” and tells the operating system to run this command using administrator privileges. “-p-” means scan all 65,535 ports. “--min-rate 1000” tells Nmap to send at least 1,000 packets at a time instead using a dynamically determined rate. Finally, “-oN scans/2021-11-23” tells Nmap to save its output to a specific output. Other output options include “-oG” (grepable format), “-oX” (XML format), and “-oA” (all formats).

A terminal window titled 'victorfernandez@evilcorpvs1:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The output of the Nmap scan is displayed, showing MAC addresses, scan reports for 192.168.3.254 and 192.168.3.203, and a summary of 256 IP addresses scanned in 283.17 seconds.

```
victorfernandez@evilcorpvs1:~  
File Edit View Search Terminal Help  
MAC Address: 00:0C:29:D3:80:E8 (VMware)  
  
Nmap scan report for 192.168.3.254  
Host is up (0.00014s latency).  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
MAC Address: 00:0C:29:98:6D:65 (VMware)  
  
Nmap scan report for 192.168.3.203  
Host is up (0.000028s latency).  
Not shown: 65534 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 256 IP addresses (7 hosts up) scanned in 283.17 seconds  
[victorfernandez@evilcorpvs1 ~]$
```

Step 4. Review the output. Identify how many hosts were discovered online. Cross-examine the IP addresses and ports reported with information from sources like DNS, Active Directory Domain Services, etc.