

Masscan

MASSCAN is a TCP port scanner that sends SYN packets asynchronously and delivers results similar to the most well-known port scanner, Nmap. It was originally created for scanning the entire internet as fast as possible.

Installation:

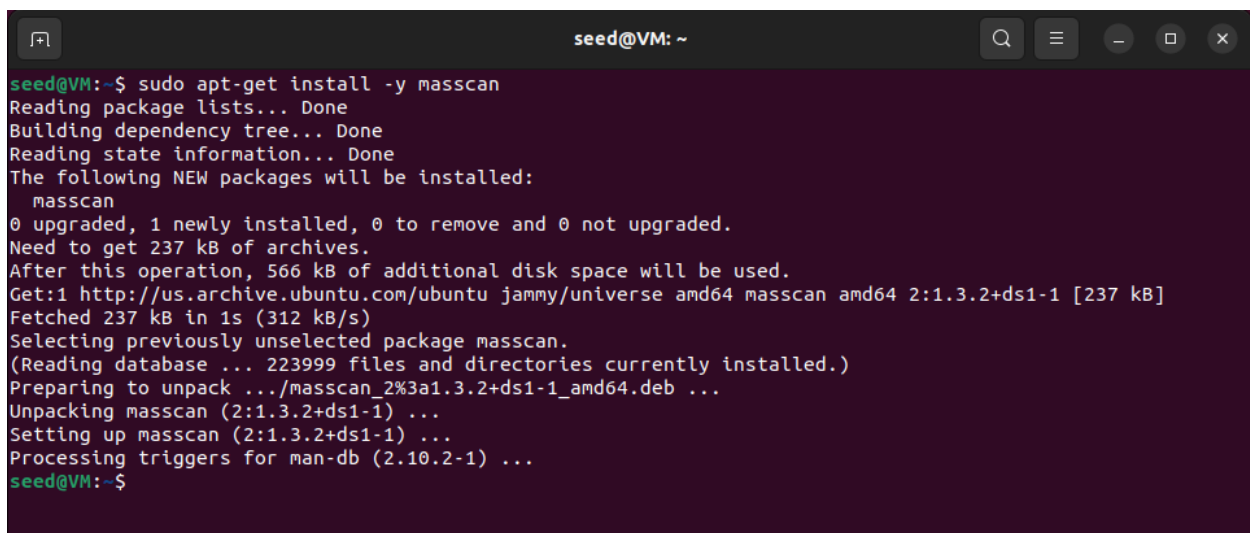
For the purpose of this guide Masscan will be installed on Ubuntu 20.04 and appropriate commands with respect to Linux distro will be used.

Step 1: All the package lists will be updated using following command:

- `sudo apt-get update -y`

Step 2: After updating and verifying all the package, next Masscan will be installed using following command:

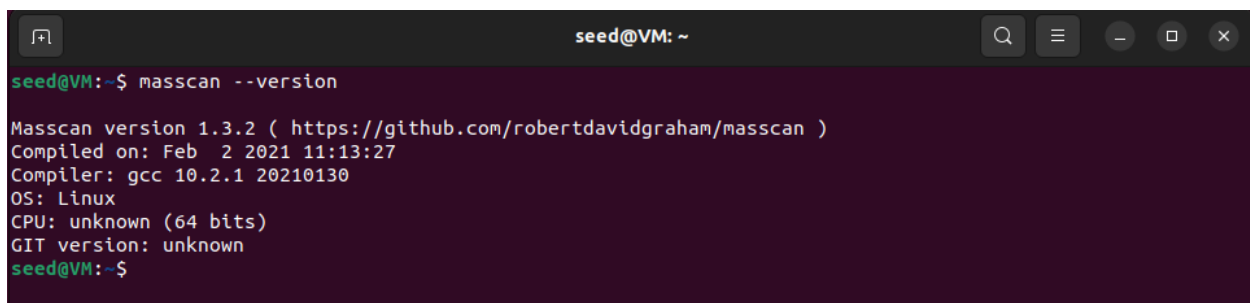
- `sudo apt-get install -y masscan`

A terminal window titled 'seed@VM: ~' showing the command 'sudo apt-get install -y masscan' and its output. The output indicates that the package lists are updated, dependencies are resolved, and the package 'masscan' is installed. It shows the disk space requirements and the source of the package (us.archive.ubuntu.com).

```
seed@VM:~$ sudo apt-get install -y masscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  masscan
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 237 kB of archives.
After this operation, 566 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 masscan amd64 2:1.3.2+ds1-1 [237 kB]
Fetched 237 kB in 1s (312 kB/s)
Selecting previously unselected package masscan.
(Reading database ... 223999 files and directories currently installed.)
Preparing to unpack .../masscan_2%3a1.3.2+ds1-1_amd64.deb ...
Unpacking masscan (2:1.3.2+ds1-1) ...
Setting up masscan (2:1.3.2+ds1-1) ...
Processing triggers for man-db (2.10.2-1) ...
seed@VM:~$
```

Step 3: The successful installation of Masscan can be verified using following command:

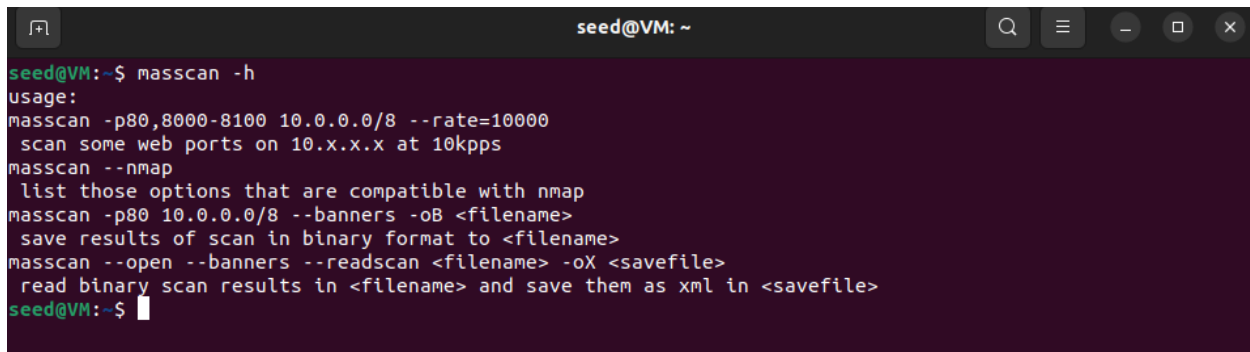
- `masscan --version`

A terminal window titled 'seed@VM: ~' showing the command 'masscan --version' and its output. The output displays the version number (1.3.2), the source URL (https://github.com/robertdavidgraham/masscan), the compilation date and time, the compiler used (gcc 10.2.1), the operating system (Linux), the CPU architecture (unknown 64 bits), and the Git version (unknown).

```
seed@VM:~$ masscan --version
Masscan version 1.3.2 ( https://github.com/robertdavidgraham/masscan )
Compiled on: Feb  2 2021 11:13:27
Compiler: gcc 10.2.1 20210130
OS: Linux
CPU: unknown (64 bits)
GIT version: unknown
seed@VM:~$
```

Step 4: The usage of Masscan can be seen using below command:

- masscan --version

A terminal window titled 'seed@VM: ~' with a dark purple background. The user has entered the command 'masscan -h'. The output shows the usage of masscan, including options for specifying ports, rate, banners, and saving results. The terminal text is as follows:

```
seed@VM:~$ masscan -h
usage:
masscan -p80,8000-8100 10.0.0.0/8 --rate=10000
  scan some web ports on 10.x.x.x at 10kpps
masscan --nmap
  list those options that are compatible with nmap
masscan -p80 10.0.0.0/8 --banners -oB <filename>
  save results of scan in binary format to <filename>
masscan --open --banners --readscan <filename> -oX <savefile>
  read binary scan results in <filename> and save them as xml in <savefile>
seed@VM:~$
```

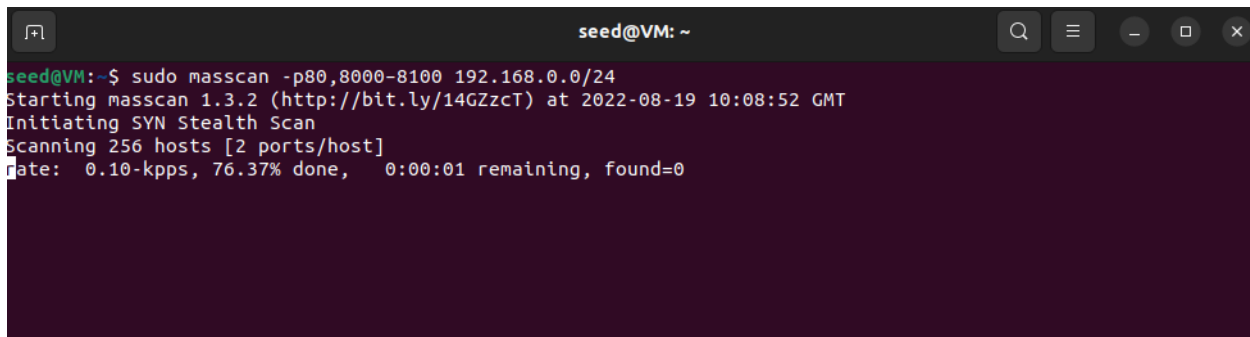
Execution:

Masscan works similar to Nmap however unlike Nmap which scans all ports by default, for Masscan user need to specify ports to scan using -p <ports> option. Also, it only supports targets hosts as IP address/subnet ranges.

By default, Masscan scans 2 million packets/second but this limit can be expanded with 10-gbps ethernet adapter and special driver known as “PF_RING DNA”.

Below sample command will show how Masscan scans a network segment for some ports:

- masscan -p80,8000–8100 192.168.0.0/24

A terminal window titled 'seed@VM: ~' with a dark purple background. The user has entered the command 'sudo masscan -p80,8000-8100 192.168.0.0/24'. The output shows the scan progress, including the number of hosts scanned and the rate. The terminal text is as follows:

```
seed@VM:~$ sudo masscan -p80,8000-8100 192.168.0.0/24
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-19 10:08:52 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [2 ports/host]
Rate: 0.10-kpps, 76.37% done, 0:00:01 remaining, found=0
```

As seen from the screenshot, the scans are performed really quickly. This tool can be used for scanning big target scopes such as organizations entire network for live IP addresses or ranges and can be really handy in ethical penetration tests.