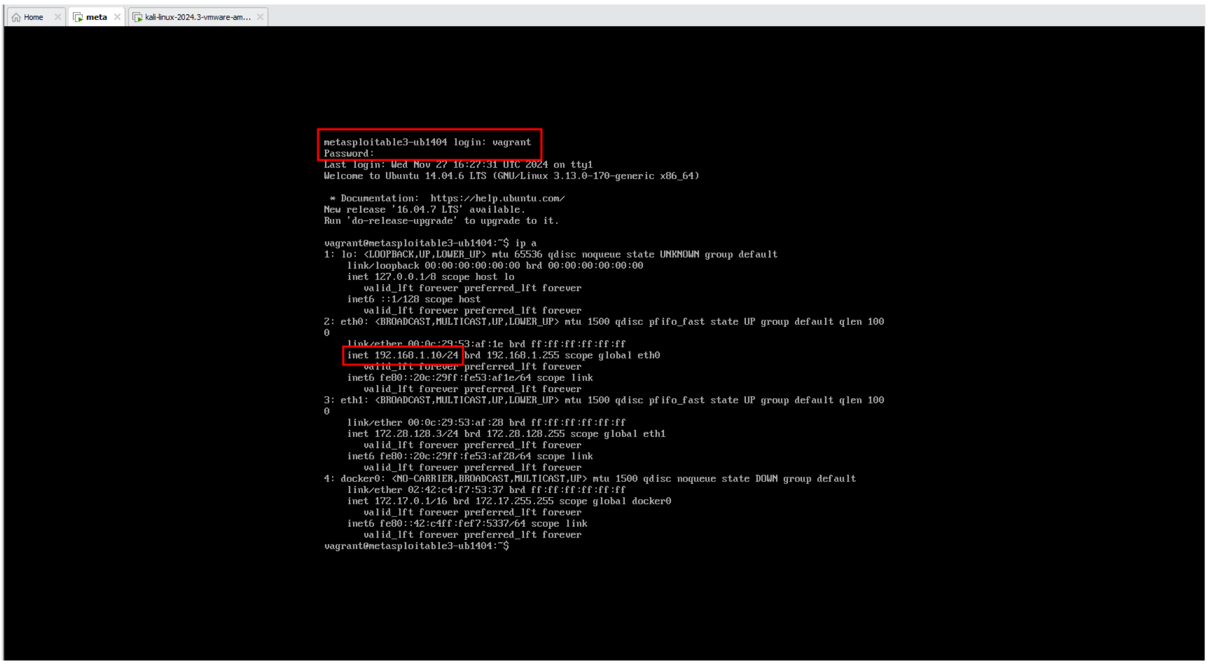
## Nmap scan:

1. Metasploitable-2 :

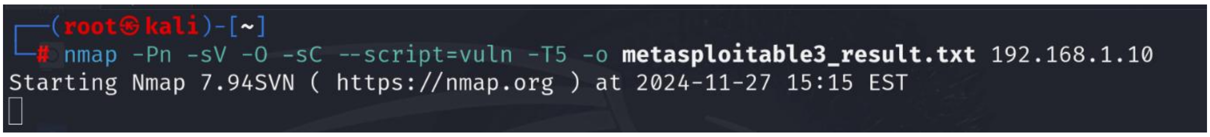


```
metasploitable3-ub1404 login: vagrant
Password:
Last login: Wed Nov 27 16:27:31 UTC 2024 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

vagrant@metasploitable3-ub1404:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 00:0c:29:53:af:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe53:af1e/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 00:0c:29:53:af:28 brd ff:ff:ff:ff:ff:ff
    inet 172.28.128.3/24 brd 172.28.128.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe53:af28/64 scope link
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:c4:f7:53:37 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:c4ff:fef7:5337/64 scope link
       valid_lft forever preferred_lft forever
vagrant@metasploitable3-ub1404:~$
```

2. nmap command to scan the target machine:



```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sV -O -sC --script=vuln -T5 -o metasploitable3_result.txt 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 15:15 EST
```

**-Pn** → Disable host discovery. Port scan only**.**

**-sV** → Attempts to determine the version of the service running on port

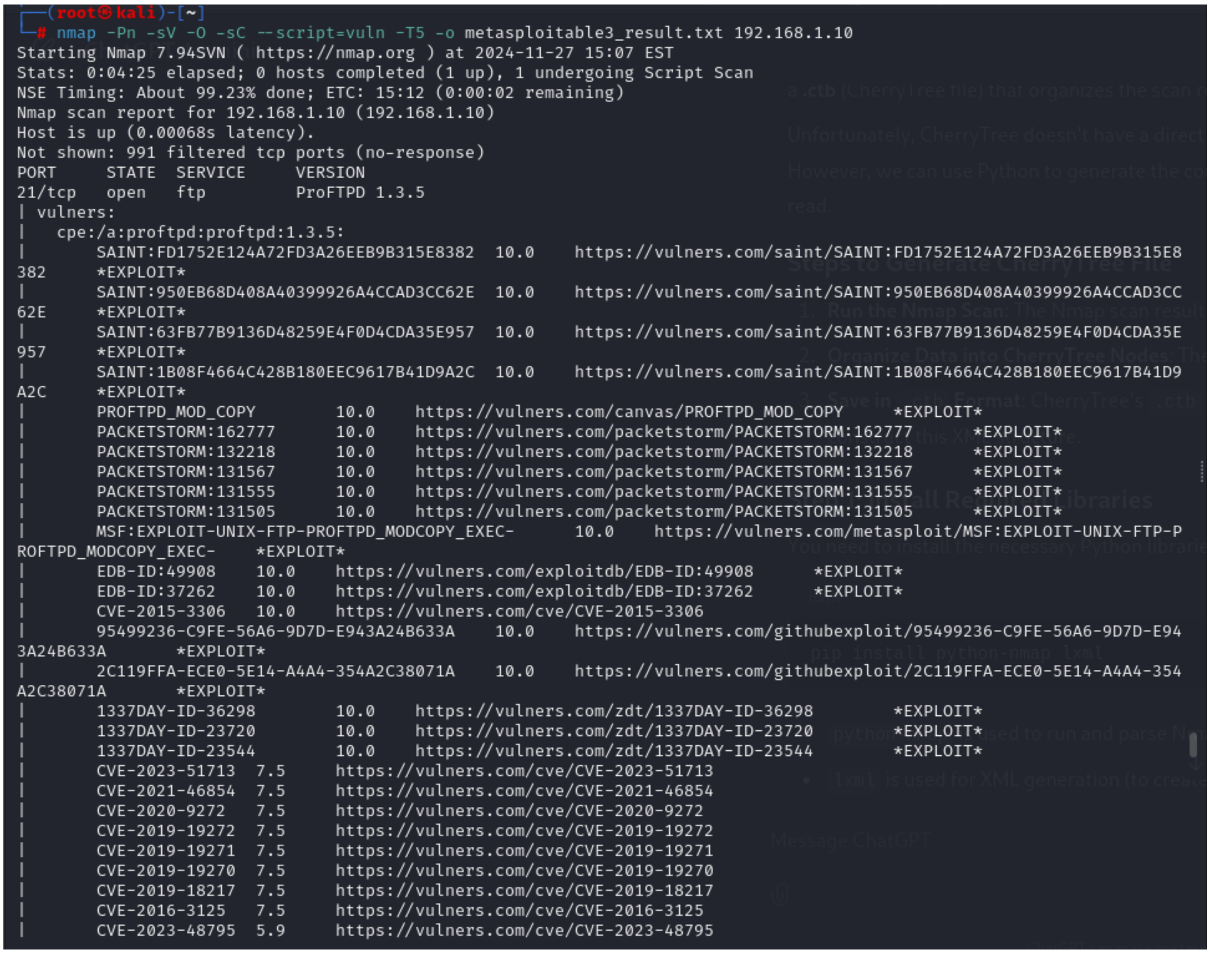
**-sC** → Scan with default NSE scripts. Considered useful for discovery and safe

**--script==vuln** → Vulnerability Scanning (NSE)

**-T5** → Time and performance - Insane (5) speeds scan; assumes you are on an extraordinarily fast network

**-o <filename>** → Output to

### 3. Nmap scan report with open ports, service versions, os, vulnerabilities:



```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sV -O -sC --script=vuln -T5 -o metasploitable3_result.txt 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 15:07 EST
Stats: 0:04:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.23% done; ETC: 15:12 (0:00:02 remaining)
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.00068s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.5:
|       SAINT:FD1752E124A72FD3A26EEB9B315E8382  10.0    https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8
382     *EXPLOIT*
|       SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0    https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC
62E     *EXPLOIT*
|       SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0    https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E
957     *EXPLOIT*
|       SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9
A2C     *EXPLOIT*
|       PROFTPD_MOD_COPY        10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|       PACKETSTORM:162777      10.0    https://vulners.com/packetstorm/PACKETSTORM:162777      *EXPLOIT*
|       PACKETSTORM:132218      10.0    https://vulners.com/packetstorm/PACKETSTORM:132218      *EXPLOIT*
|       PACKETSTORM:131567      10.0    https://vulners.com/packetstorm/PACKETSTORM:131567      *EXPLOIT*
|       PACKETSTORM:131555      10.0    https://vulners.com/packetstorm/PACKETSTORM:131555      *EXPLOIT*
|       PACKETSTORM:131505      10.0    https://vulners.com/packetstorm/PACKETSTORM:131505      *EXPLOIT*
|       MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-      10.0    https://vulners.com/metasploit/MSF:EXPLOIT-UNIX-FTP-P
ROFTPD_MODCOPY_EXEC-    *EXPLOIT*
|       EDB-ID:49908    10.0    https://vulners.com/exploitdb/EDB-ID:49908      *EXPLOIT*
|       EDB-ID:37262    10.0    https://vulners.com/exploitdb/EDB-ID:37262      *EXPLOIT*
|       CVE-2015-3306   10.0    https://vulners.com/cve/CVE-2015-3306
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E94
3A24B633A       *EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354
A2C38071A       *EXPLOIT*
|       1337DAY-ID-36298        10.0    https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|       1337DAY-ID-23720        10.0    https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
|       1337DAY-ID-23544        10.0    https://vulners.com/zdt/1337DAY-ID-23544        *EXPLOIT*
|       CVE-2023-51713  7.5     https://vulners.com/cve/CVE-2023-51713
|       CVE-2021-46854  7.5     https://vulners.com/cve/CVE-2021-46854
|       CVE-2020-9272   7.5     https://vulners.com/cve/CVE-2020-9272
|       CVE-2019-19272  7.5     https://vulners.com/cve/CVE-2019-19272
|       CVE-2019-19271  7.5     https://vulners.com/cve/CVE-2019-19271
|       CVE-2019-19270  7.5     https://vulners.com/cve/CVE-2019-19270
|       CVE-2019-18217  7.5     https://vulners.com/cve/CVE-2019-18217
|       CVE-2016-3125   7.5     https://vulners.com/cve/CVE-2016-3125
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
```