## **Nmap Service Detection**

Once Nmap discovers you, you can probe the available port to detect the running service. Further investigation of open ports is essential is learning what if any vulnerabilities can be identified of the services running.

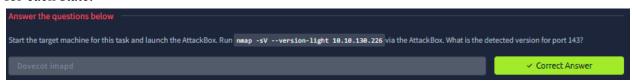
Adding -sV to the Nmap command will collect and determine the service and version information for the open ports. The intensity can be controlled with --version-intensity LEVEL level being specified on a scale 0-9 being the least intensive and most intensive. I's important to note -sS stealth SYN is not possible when stealth Version -sV has been activated.

-sV leads to a new column in the output showing each version for each detected service. Eg. TCP port 22 being open instead of 22/TCP open ssh we obtain 22/tcp open ssh OpenSSH 6.7p1 Debian S+deb8u8 (protocol 2.0).

```
Pentester Terminal
pentester@TryHackMe$ sudo nmap -sV 10.10.130.226
Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for 10.10.130.226
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.6.2
110/tcp open pop3 Dovecot pop3d
111/tcp open rpcbind 2-4 (RPC #100000)
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Service Info: Host: debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.40 seconds
ote that many Nmap options require root privileges. Unless you are running Nmap as root, you need to use sudo as in the example above.
art the VM. Once it is ready, open the terminal on the AttackBox to answer the following questions
```

```
oot@ip-10-10-12-161:-# nmap -sV --version-light 10.10.130.226
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 10:44 BST
Nmap scan report for ip-10-10-130-226.eu-west-1.compute.internal (10.10.130.226)
Host is up (0.0071s latency).
Not shown: 992 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh
25/tcp open smtp
80/tcp open http
                        OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
                         Postfix smtpd
                        nginx 1.22.1
110/tcp open pop3
                         Dovecot pop3d
111/tcp open rpcbind
143/tcp open imap
                         Dovecot imapd
993/tcp open ssl/imap Dovecot imapd
995/tcp open ssl/pop3 Dovecot pop3d
MAC Address: 02:A3:77:F1:03:EB (Unknown)
Service Info: Host: debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
root@ip-10-10-12-161:-# []
```

Our example shows the context learnt in the first section of this document. Showing the versions for each state.



As the question asks what is detected for version for port 143, we can see from the above example it is Dovecot imapd.



Rpcbind did not have a detected version, as shown in the same above example.