

Nmap OS Detection/Traceroute

Nmap can detect the Operation System (OS) based on its behaviour and any telltale signs in its response. OS detection can be enabled using the **-O** to achieve this and O meaning **O in the OS**.

nmap -sS -O 10.10.130.226

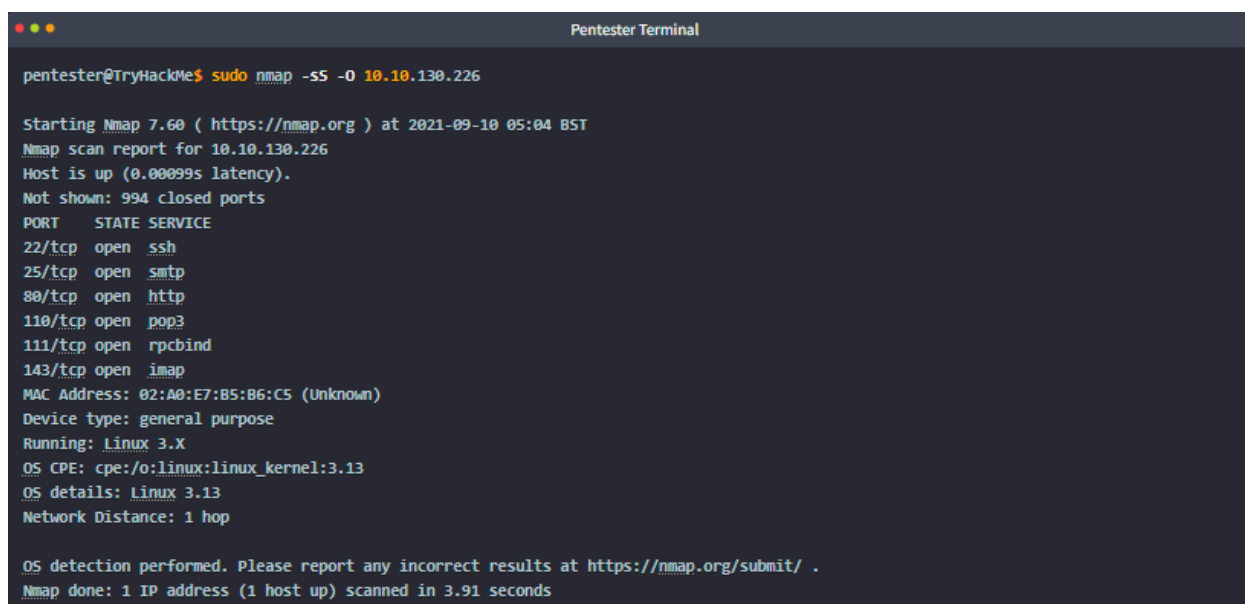
Breaking it down just for clarity:

nmap : Calling to allow the configuration to run

-sS : Stealth SYN

-O : Operating System

10.10.130.226 : IP of the target system



```
pentester@TryHackMe$ sudo nmap -sS -O 10.10.130.226

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:04 BST
Nmap scan report for 10.10.130.226
Host is up (0.00099s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.91 seconds
```

The system scanned in the above example attempted to detect the OS version running at kernel version 3.16. Nmap was able to make a close guess, but if in another case scanning Fedora Linux system with kernel 5.13.14 however Nmap detected it as Linux 2.6.x. Good news is it was guessed correctly but the kernel version was wrong.

OS detection can be convenient but **factors might affect accuracy**. For example, Nmap needs **at least one open and one closed port to make a reliable guess**. Furthermore the guest OS fingerprint might get distorted due to the rising use of virtualisation and similar technologies. Therefore always take the OS version **without relying on it too much**.

Tracer Route:

If you want Nmap to find the routers between you and the target just **--traceroute**. Maps traceroute works slightly different than the traceroute command found on Linux and macOS or tracert found on MS windows.

Traceroute starts with a packet of low TTL (Time To Live) and keeps increasing until it reaches the target. Nmap tracer route starts with high TTL (Time To Live) and keeps decreasing.

Traceroute : Low TTL - Increasing till reaches target.

Nmap Traceroute : High TTL - Decreasing till reaches target.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -sS --traceroute 10.10.130.226

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:05 BST
Nmap scan report for 10.10.130.226
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)

TRACEROUTE
HOP RTT    ADDRESS
1   1.48 ms 10.10.130.226

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

```

root@ip-10-10-12-161:~# nmap -O 10.10.130.226
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-27 10:57 BST
Nmap scan report for ip-10-10-130-226.eu-west-1.compute.internal (10.10.130.226)
Host is up (0.00069s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 02:A3:77:F1:03:EB (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/27%OT=22%CT=1%CU=39624%PV=Y%D=1%DC=0%G=Y%M=02A377%T
OS:M=6885F826%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=108%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW
OS:7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4
OS:B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=
OS:40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%
OS:0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4
OS:0%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.15 seconds

```

This is the example achieved when running the nmap -O command on the target IP address. We get a list of open ports as well as the note: **No Exact matches for host.**

It also tells us the through the TCP/IP fingerprint it is referring to Linux such as this zoomed in:

```
OS:M=6885F912%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%II=I%
```

Answer the questions below

Run **nmap** with **-O** option against **10.10.130.226** . What OS did Nmap detect?

Linux

✓ Correct Answer

Like so!