

Forum:[Hack Forums](#)

Thread: [Open Port Scanning and OS Detection with Nmap in Kali Linux](#)

Sphynx - February 2, 2021, 1:55 am

Nmap stands for Network Mapper and is an open-source tool for network exploration and security auditing which comes standard with Kali Linux but is also available for Windows, OSX, and many other UNIX platforms. Nmap also has a graphical user interface called Zenmap.

Please be careful using the more aggressive functions of Nmap against hosts you do not own or do not have permission to scan. It may be against your ISP's terms to use some Nmap features.

Open Port Scanning and OS Detection

Firstly, I will be using [ip address] versus an actual or fake IP please use common sense and put an IP and not [ip address] if you do not do this and come here to ask for help or why it's not working 99% chance I will make fun of you and even possibly shit talk you.

Let's start with a ping scan on an IP range to determine live hosts using the following command:

Code `nmap -sP [ip address]-100`

Next we will start a SYN scan with OS detection on one of the live hosts using the following command:

Code `nmap -sS [ip address]-O`

Now we will start an open port scan with version detection using the following command:

Code `nmap -sV [ip address] -A`

When we add -v to the command we can increase the verbosity:

Code `nmap -sV [ip address] -A -v`

-lamu- - February 6, 2021, 9:48 am

Thank you soo much. I am relearning everything! :D