Nmap Basic Tutorial

tutorial

CKjones EVILCORP -CEO Aug '22

Hello everyone, in this tutorial we will explore the basic use of the port scanner Nmap. I hope that you find this useful and can apply this in some way. Let's get started!

LISTING PORTS ON AN OPEN TARGET
Now, to launch a normal scan the bare minimum Nmap needs is an IP (Internet Protocol) address. To run a scan input this command in the Linux terminal: `Nmap TARGET IP` The scan results will display all host information obtained, such as IPv4 (and IPv6, if available) addresses, reverse DNS, and important port and service names.

The default Nmap scan returns a list of ports. In addition, it returns a service name from a database distributed with Nmap and the port state for each of the listed ports.

- **Open:** Open indicates that a service is listening for connections on this port.
- **Closed:** Closed indicates that the probes were received, but it was concluded that there was no service running on this port.
- **Filtered:** Filtered indicates that there were no signs that the probes were received and the state could not be established. This could indicate that the probes are being dropped by some kind of filtering.
- **Unfiltered:** Unfiltered indicates that the probes were received but a state could not be established.
- **Open/Filtered:** This indicates that the port was filtered or open, but the state could not be established.
- **Closed/Filtered:** This indicates that the port was filtered or closed but the state could not be established.

SCANNING SPECIFIC PORT RANGES

Setting port ranges correctly during your scans is a task you often need to do when running Nmap scans. There are several ways of using the Nmap -p option:

- Port list separated by commas: $ Nmap -p80,443 localhost
- Port range denoted with hyphens: $ Nmap -p1-100 localhost
- Alias for all ports from 1 to 65535: # nmap -p- localhost
- Specific ports by protocol: # nmap -pT:25,U:53
- Service name: # nmap -p SMTP
- Service name with wildcards: # nmap -p SMTP*
- Only ports registered in the Nmap services database: # nmap -p[1-65535]

I hope that you find this helpful!

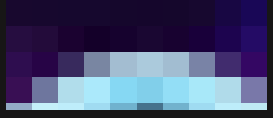
-CKjones

hoek Sep '22

Cool.
In the past I wrote some article about nmap, at the end you can find some cheatsheet

Skip to main content

A little bit about Nmap



Nmap is powerful tool. Mostly used for network discovery and security auditing. If you want to know more about what assets are in your network and what services they are running, Nmap is best choice.