Top 20 Nmap Commands (Using IP: 10.0.2.15)

## Basic Host Discovery

**Command:** *nmap 10.0.2.15*

Performs a simple scan to check if the host is up and shows open ports.

## Ping Scan (Check if Host is Alive)

**Command:** *nmap -sn 10.0.2.15*

Checks if the host is alive by sending ping requests. It does not scan for open ports.

## Service Version Detection

**Command:** *nmap -sV 10.0.2.15*

Detects the version of services running on open ports.

## OS Detection

**Command:** *nmap -O 10.0.2.15*

Attempts to identify the target's operating system.

## Aggressive Scan (All in One)

**Command:** *nmap -A 10.0.2.15*

Performs OS detection, version detection, traceroute, and default script scanning.

## TCP Connect Scan (Full)

**Command:** *nmap -sT 10.0.2.15*

Performs a full TCP connect scan when SYN scan is not possible.

## SYN Scan (Stealth Scan)

**Command:** *nmap -sS 10.0.2.15*

Performs a half-open SYN scan, which is faster and stealthier.

## UDP Scan

**Command:** *nmap -sU 10.0.2.15*

Scans for open UDP ports, which can reveal services like DNS, DHCP, SNMP.

## Fast Scan (Top 100 Ports)

**Command:** *nmap -F 10.0.2.15*

Scans only the most common 100 ports for a faster result.

## Specific Port Scan

**Command:** *nmap -p 22,80,443 10.0.2.15*

Scans only selected ports (SSH, HTTP, HTTPS).

## Port Range Scan

**Command:** *nmap -p 1-1000 10.0.2.15*

Scans ports from 1 to 1000 to find open services.

## Script Scan (Default Scripts)

**Command:** *nmap -sC 10.0.2.15*

Runs Nmap's default NSE scripts for vulnerability and info gathering.

## Intense Scan with Script + Version

**Command:** *nmap -sC -sV 10.0.2.15*

Combines default scripts with version detection for detailed information.

## Scan Without DNS Resolution

**Command:** *nmap -n 10.0.2.15*

Skips DNS resolution to make the scan faster.

## Verbose Scan

**Command:** *nmap -v 10.0.2.15*

Provides detailed information during the scan process.

## Very Verbose Scan

**Command:** *nmap -vv 10.0.2.15*

Gives even more detailed output than -v (useful for debugging).

## Traceroute + Scan

**Command:** *nmap --traceroute 10.0.2.15*

Shows the network path to the target host while scanning.

## Save Results to File

**Command:** *nmap -oN scan\_results.txt 10.0.2.15*

Saves scan output to a normal text file for future reference.

## XML Output (For Tools/Parsing)

**Command:** *nmap -oX scan\_results.xml 10.0.2.15*

Saves scan output in XML format, useful for automation or tools.

## Combine Everything (Ultimate Scan)

**Command:** *nmap -A -T4 -p- 10.0.2.15*

Performs an aggressive scan of all ports with faster timing.