Nmap QuickStart Guide

insecure.org

What is Nmap?

Nmap is the world's most popular port scanner which has additional capabilities added over time. Created by Gordon "Fyodor" Lyon in 1997, Nmap runs on most operating systems. A GUI version named Zenmap is also available.

You can find Nmap at insecure.org.

WARNING

Port scanning can have unintended consequences in network environments, particularly in ICS/OT networks. Ensure you have authorization and understand the potential ramifications of scanning a particular network before doing so.

Finding Hosts

Ping Sweep – Find hosts with ICMP responses
Example: **nmap -sP 192.168.1.0/24**

ARP Scan – Find hosts with ARP broadcasts
Example: **nmap -PR 192.168.1.0/24**

DNS Lookup – Lookup hostnames by IP
Example: **nmap -sL 192.168.1.0/24**

Performance Settings

Nmap allows for performance tuning using the -T switch. The speed at which Nmap scans targets can be adjusted. The faster the scan, the more you risk bringing down a network or being discovered with network security monitoring.

-T0 (Paranoid)
-T1 (Sneaky)
-T2 (Polite)
-T3 (Normal / Default)
-T4 (Aggressive)
-T5 (Insane)

Port Scanning

Scan a Single Host – Default TCP Ports
Example: **nmap 192.168.1.5**

Scan a Single Host – Default UDP Ports
Example: **nmap -sU 192.168.1.5**

Scan a Single Host – All TCP ports
Example: **nmap 192.168.1.5 -p-**

Scan a TCP Specific Port on a Single Host
Example: **nmap 192.168.1.5 -p 80**

Scan a UDP Specific Port on a Single Host
Example: **nmap -sU 192.168.1.5 -p 161**

Default TCP Port Scan On All Hosts on Subnet
Example: **nmap 192.168.1.0/24**

Display Only Open Ports (No Closed/Filtered)
Example: **nmap 192.168.1.0/24 -p 80 --open**

Exclude Hosts from a Network Scan
Example: **nmap 192.168.1.0/24 --exclude 192.168.1.132**

OS Fingerprinting
Example: **nmap -O 192.168.1.5**

Scan a Host List from Text File
Example: **nmap -iL hosts.txt**

Nmap "Does it All" (e.g., port, service and script scans, OS fingerprinting and traceroute)
Example: **nmap -A 192.168.1.5**

Service Scans

Service scans can be used to determine the actual service/application running on an open port. Returned information can be used for determining the potential existence of vulnerabilities.

Conduct a Service Scan on Default TCP Ports
Ex: nmap -sV 192.168.1.5

The Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) provides additional capabilities beyond port scanning and service detection. Scripts can be written in LUA and stored in the Nmap /scripts folder.

Conduct a Script Scan with Default Scripts
Ex: nmap -sV -sC 192.168.1.5

Conduct a Script Scan with Only a Specific Script
Ex: nmap 192.168.1.5 -p 21 --script ftp-anon

Conduct a Script Scan with All Related Scripts
Ex: nmap 192.168.1.5 -p 21 --script "ftp*"

Nmap Output

Nmap can save its output in several formats.

-oN: Normal text format
-oX: XML format
-oG: Grepable format
-oA: All three of the above at one time
-oS: s|<rIpt kIddi3 format

Ex: nmap 192.168.1.0/24 -oN results.txt

Special thanks to Gordon "Fyodor" Lyon for an incredible tool over the last 25 years!

linkedin.com/in/mikeholcomb