Nmap QuickStart Guide for ICS/OT

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.

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 (Safest to Least Safest)

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

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

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

Performance Settings

Controlling how fast Nmap sends packets on the network can help to reduce the risk of negatively impacting an ICS/OT network or asset.

- Use the –scan-delay option to force a limit on how often network probes are sent.
- Set --max-parallelism to 1 to ensure only one packet is sent at a time.

Example: **nmap 192.168.1.0/24 --scan-delay 5s --max-parallelism 1**

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-**

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

Scan for Most Common ICS/OT TCP Protocols
Example: **nmap 192.168.1.5 -p 102,502,789,1911,1962,2455,5007,9600,18245, 20000,20547,44818**

Scan for Most Common ICS/OT UDP Protocols
Example: **nmap 192.168.1.5 -p 5006,5094, 44818,47808**

Common ICS/OT Protocols & Ports

There are several common ICS/OT protocols that run on default ports to be familiar with.

Modbus	TCP 502	**GE-STRP**	TCP 18245
S7	TCP 102	**Hart**	UDP 5094
DNP3	TCP 20000	**PCWorx**	TCP 1962
BACnet	UDP 47808	**Omron**	TCP 9600
CODESYS	TCP 2455	**Red Lion**	TCP 789
Tridium	TCP 1911	**ProConOS**	TCP 20547
EthernetIP	TCP 44818	**MELSEC-Q**	TCP 5007
EthernetIP	UDP 44818	**MELSEC-Q**	UDP 5006

Service Scans

Service scans can be used to determine the actual service/application running on an open port.

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 502 --script modbus-discover

Other included ICS/OT protocol enumeration scripts include **bacnet-info, enip-info,fox-info, iec-identify, modbus-discover, omron-info, pcworx-info and s7info.nse.**

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