NMAP: TRY AND LEARN

NMap is a valuable tool for identifying attackers and testing for vulnerabilities within a network. In cybersecurity, understanding your packet traffic is crucial for preparing against attacks. Regularly scanning your network is essential to stay ready for potential threats.

Install First… Practice Second

Before we get to how to use NMap, we're going to look at how to install it. Windows, Linux and MacOS users can download Nmap here. https://nmap.org/download.html

Now unpack, compile and install. Use the standard configure and make commands when building software from source.

- tar jxvf nmap-5.61TEST5.tar.bz2
- cd nmap-5.61TEST5/
- ./configure
- make
- make install

NMap's main uses include:
- port scanning,
- ping sweeps,
- OS detection, and
- version detection.

- **ARP ping scan Command:** # nmap -sP -PR 192.168.1.1/24

- **NMap Use Cases**
  You can use Nmap to:
  - Identify live hosts on network
  - Identify open ports on network
  - Identify the operating system of services on network
  - Address vulnerabilities in network infrastructure

- **Port Scanning Techniques**
  - sS TCP SYN scan
  - sT TCP connect scan
  - sU UDP scans
  - sY SCTP INIT scan
  - sN TCP NULL.

How

- Fire up your command line or GUI

- Type scanme.nmap.org to perforr default scan for open ports on domain.

Scan Yourself-

- **TCP SYN Scan:** sS TCP SYN Scan
- **TCP Connect Scan:** sT TCP Connect Scan
- **UDP Scan:** sU UDP Scan
- **SCTP INIT port scan:** sY SCTP INIT Scan
- **TCP NULL Scan:** sN TCP NULL Scan
- **Host Scanning:** nmap -sP <target IP range>
- **Identify Hostnames:** nmap -sL 192.100.0.0/24
- **OS Scanning:** nmap -O 192.168.5.102
- **Version Detection:** #nmap -sV 192.168.1.1