Scanning for Open Ports with nmap

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the purpose and function of the *nmap* utility.
2. Use *nmap* to scan servers for open ports.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Scanning for Open Ports with *nmap*
    - Why scan for ports
    - An introduction to *nmap*
    - Performing network discovery
- Performing network scans
    - Identifies unauthorized systems and services
    - Tests firewall configurations
    - Verify compliance with policy
- Introduction to *nmap*
    - Open source network scanner
    - The name is short for Network Mapper
    - Automated tool that establishes connections to systems on the network
    - Provides easy to interpret output
    - https://nmap.org
    - `sudo apt install nmap`
- Performing a quick scan
    - Default scan
        - Scans 1000 well known ports
        - `nmap 10.222.0.51`
    - Disable ping probe
        - `-Pn`
            - Treat all hosts as online
            - Useful when firewalls block ICMP
        - `nmap -Pn 10.222.0.51`
    - Fast scan
        - Scans 100 well known ports
        - `nmap -F 10.222.0.51`
- Scanning all ports
    - `-p`
        - Port ranges
        - `-p 1-1023`
        - `-p-` includes everything
    - `nmap -p- 10.222.0.51`
- Scanning multiple systems
    - IP List
        - `nmap 10.222.0.9 10.222.0.13 10.222.0.55`
        - `nmap 10.222.0.9,13,55,210`
        - `nmap 10.222.0.50-60`

    - Subnet
        - `nmap 10.222.0.*`
- Learn more about services
    - Internet Assigned Numbers Authority (IANA) Database
        - https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
    - Examine the port to determine service details
    - `-sV` - Service/Version Detection
    - `nmap -Pn -sV 10.222.0.51`