LOGIX ACADEMY

Lab: Port Scanning Using Nmap

Purpose

In this lab, we are going to use Nmap to perform network discovery and port scans including scanning a range of IPs, specific ports, fingerprinting Operating Systems and discovering IPs.

Common Nmap Commands

Purpose	Command
Scan 1000 common ports for a single IP	nmap 192.168.1.1
Scan 1000 common ports for subnet	nmap 192.168.1.1/24
Scan ALL ports for a single IP	nmap -p- 192.168.1.1
Scan ALL ports for a range of IPs	nmap -p- 192.168.1.1-99
Scan a range of ports for a single IP	nmap -p 80-100 192.168.1.1
Scan a single port for a single IP	nmap -p 80 192.168.1.1
Fingerprint the OS for a single IP	nmap -O 192.168.1.1
Discover all IPs (hosts) in a subnet	nmap -sP 192.168.1.1

Scan 1000 Common Ports of Your Own System

nmap localhost

Scan ALL Ports

nmap -p- localhost

Scan Port 80

nmap -p 80 localhost

Fingerprint the Operating System

nmap -O localhost

Fingerprint the Operating System

First, you need to find out the IP address of the Ethernet Card that the VMWare machine is using, so issue the following command: **ifconfig**

```
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:94:8b:38
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
```

nmap -sP 10.0.2.15

Task:

- Scan the port range 60 – 120 for your local machine
- Investigate if Telnet is running on your local machine (assume that you scan only a SINGLE port)

(Solution on Next Page)

LOGIX ACADEMY

Solution:

- **Issue the command to scan port range 60 – 120 for your local machine**

  nmap -p 60-120 localhost

- **Issue the command to find if Telnet is running on your local machine (scan only a SINGLE port)**

  nmap -p 23 localhost