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 <IP_Address>
Scan ALL ports for a single IP	nmap -p- <IP_Address>
Scan ALL ports for a range of IPs	nmap -p- <start IP_Address- End IP_Address>
Scan a range of ports (80-100) for single IP	nmap -p 80-100 <IP_Address>
Scan a single port for a single IP	nmap -p <IP_Address>
Fingerprint the OS for a single IP	nmap -O <IP_Address>
Discover all IPs (hosts) in a subnet	nmap -sP <IP_Address>

Tasks

Pre-Requisite:

Before you can start the lab, you need to run the lab script which will setup everything. Open the **Labs** folder on Desktop then right-click and "Open Terminal Here". Or open a terminal and cd to Desktop/Labs folder, then issue the command:

```
sudo ./main_script.sh
```

Select **Nmap Scanning Lab** option from the lab menu.

1. Scan the 1000 most common ports of your local system
2. Scan only port 22 specifically
3. Fingerprint the OS and find the Linux kernel version
4. There is a secret service running on an uncommon port, you must find which port, but the challenge is that you **cannot** scan ALL ports, but you are allowed to scan the port range between 40,000 – 60,000, so issue one command which scans that range.

Solution discussed in next lecture

https://t.me/learningnets