Experiment-10

Aim: To Implement Network discovery using discovery tool

(Nmap)

Nmap, also known as network mapper, is a free and open-source security tool

widely known for its powerful network discovery, enumeration and security

auditing abilities. Network administrators utilize Nmap to establish a network

map and get more information about what’s going on inside the network: which

hosts are online, what ports are open, which services are offered, and more.

Installation

The quickest way to get up and running is by installing Nmap through the APT package

manager:

sudo apt install nmap

Target specification

Before we jump into network scanning, it’s important to define and understand the methods that

can be used to specify which targets to scan. The simplest way is specifying only one host,

without any additional parameters:

nmap scanme.nmap.org

Multiple hosts can be specified in subnet or IP range, either

from the command line or a file:

nmap 192.168.1.0/24 # Scan a whole

subnet nmap 192.168.2.100-200 # Scan

IP range

nmap 192.168.1.0/24 192.168.2.100-200 # Same as both of the

above nmap -iL targets.txt # Scan all IP addresses in text

file

It’s also possible to exclude IP addresses from the scan:

nmap --exclude 192.168.6.1.1 192.168.1.0/24 # Can also be subnet or IP

range nmap --excludefile targets.txt 192.168.1.0/24 # Exclude hosts

present

Host discovery

Nmap optimizes port scan speed by first checking if the target is online before attempting to

scan any ports. This is called host discovery or ping scanning and is enabled in every scan by

default.

Running a host-discovery-only scan is possible in case we

only want to see which hosts are online: