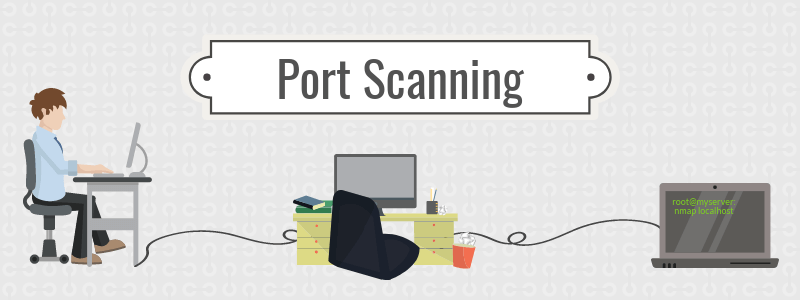
A black background with blue text

Description automatically generated

**ST5062CEM Programming and Algorithms 2**

**Topic: Port Scanning**



Submitted By:

Nishan Tamang

College ID:

230107

Coventry ID

14187399

Submitted To:

Suman Shrestha

**Acknowledgement**

It is with my most pleasure I would like to thank Mr. Suman Shrestha sir for being given the opportunity to do research and write about port scanning. And with his help I have been able to learn about port scanners.

**Abstract**

An essential tool for network administration and security is a port scanner, which searches a host or network for open ports. Understanding the services that are operating on a system and evaluating any security flaws need knowing which ports are open. While port scanning has genuine uses in network inventory, monitoring, and vulnerability assessment, hostile actors may also abuse it to find and take advantage of vulnerabilities.

Table of Contents

[Introduction 4](#_Toc169076328)

[Objective 4](#_Toc169076329)

[Literature Review 5](#_Toc169076330)

Table of Figure

[Figure 1: Port Scanner 4](#_Toc169076138)

# Introduction

A port scanner is an application which is made to probe a host or server to identify open ports. If used for malicious purposes it can lead to exploitation of vulnerabilities by finding network service running on a host. Security analysts also use this to confirm network security policies.

A network or server's open ports that are receiving information may be found by doing a port scan. It can also identify security devices like firewalls that are positioned between the sender and the destination.

## Objective

* File Transfer Protocol (FTP) for data transfer.
* Secure Shell (SSH) protocol for secure logins, FTP, and port forwarding

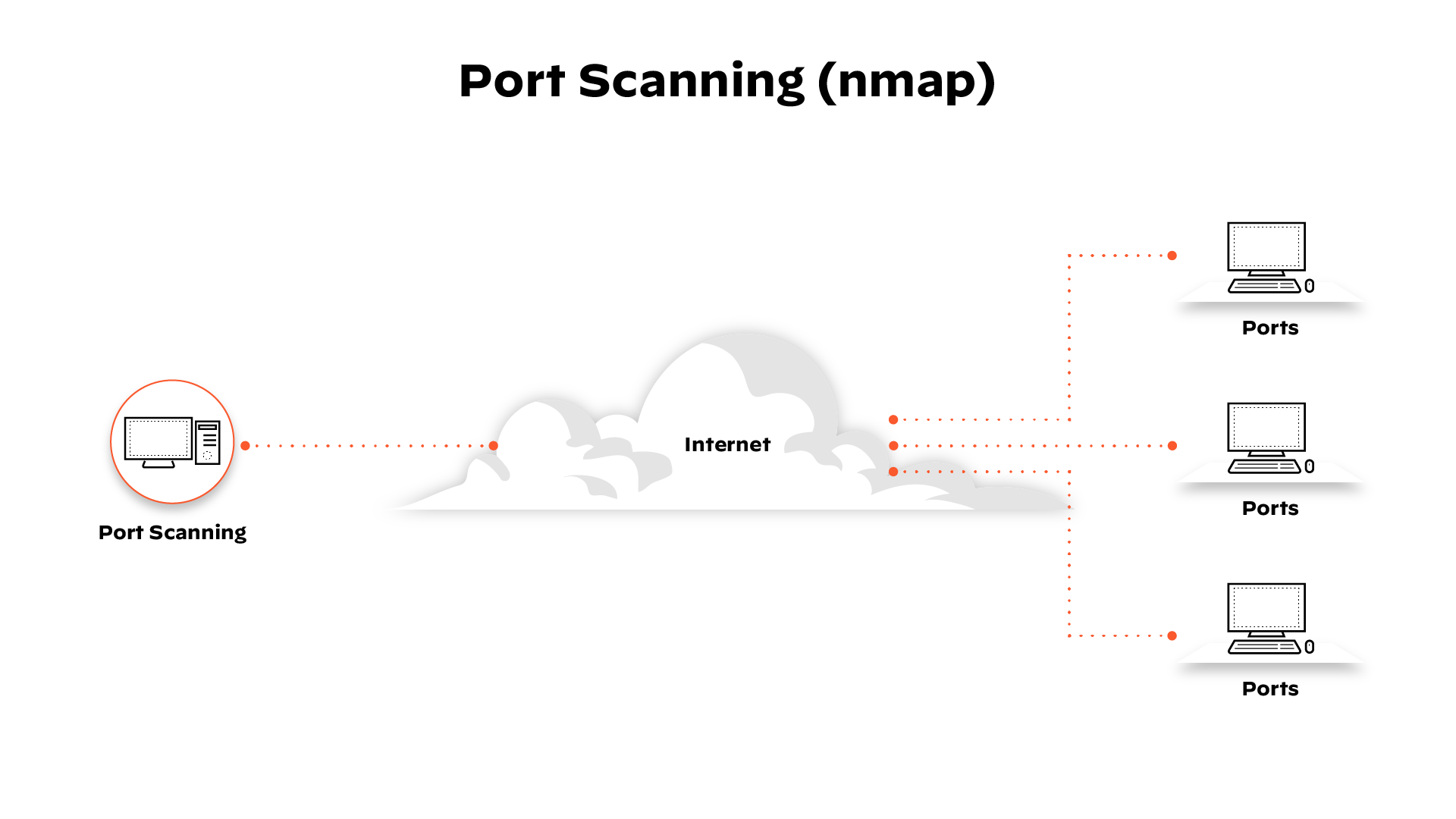


Figure 1: Port Scanning

# Literature Review

Many important publications have advanced the technique of port scanning, which is crucial to network security. Gordon "Fyodor" Lyon's 2009 book "Nmap Network Scanning" provides a thorough introduction to utilizing Nmap, a potent port scanner, covering everything from fundamental network discovery to sophisticated security scanning. Like this, Chris McNab's "Network Security Assessment: Know Your Network" (2017) emphasizes port scanning as a means of finding vulnerabilities and provides useful insights on network security.  
  
Important scientific publications have also influenced the field. Nmap uses TCP/IP stack fingerprinting, a method first described in Fyodor's "Remote OS Detection via TCP/IP Stack Fingerprinting" (2001) to identify target host operating systems. An empirical examination of port scan reliability is given in "An Empirical Study of the Reliability of Port Scans" by Paul Barford et al. (2002), emphasizing the accuracy and limitations of various scanning methods.

Robert Graham's (2013) "Masscan: Mass IP port scanner" is one of his notable creations. It is well-known for its efficiency and speed and can scan the whole Internet in less than six minutes. Together, these efforts advance our knowledge of port scanning technologies and their advancement, which is vital for network security and vulnerability analysis.