**COMP 7003**

**Introduction to Information and Network Security**

*Assignment-03*

*User Guide*

##### Anmol Mittal A01397754

##### February 16th, 2025

##### Course Reference Number (CRN): 91662

Contents

[**Purpose** 3](#_Toc190533712)

[**Installation** 3](#_Toc190533713)

[Requirements 3](#_Toc190533714)

[Building 3](#_Toc190533715)

[Running 3](#_Toc190533716)

[**Command Line Arguments** 3](#_Toc190533717)

[**Examples** 4](#_Toc190533718)

# **Purpose**

The purpose of the program is to perform network reconnaissance using a SYN scan, a technique where it sends SYN packets to target ports and interprets responses to determine their state. It is useful for:

* Identifying active hosts on a network.
* Detecting open/closed/filtered ports on those hosts.
* Scanning a local subnet or a specified target range.
* Customizing scans using command-line arguments.

# **Installation**

Navigate to [https://learn.bcit.ca](https://learn.bcit.ca/). Download COMP7003-assign03-v1.zip and Extract the contents.

## Requirements

Need Scapy installed.

## Building

No building required

## Running

sudo python3 main.py -t <target> -p <ports> --show <filter>

# **Command Line Arguments**

The following configuration values can be set:

|  |  |
| --- | --- |
| **Variable** | **Purpose** |
| -t <target> | specifies the target(s) to scan |
| -p <ports> | specific ports or port ranges to scan |
| --show <filter> | Filters the final output based on port states (open, closed, filtered) |

# **Examples**

A screenshot of a computer program

AI-generated content may be incorrect.