**COMP 7003**

**Introduction to Information and Network Security**

*Assignment-03*

*Report*

##### Anmol Mittal A01397754

##### February 16th, 2025

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

[**Purpose** 3](#_Toc190518724)

[**Requirements** 3](#_Toc190518725)

[**Platforms** 3](#_Toc190518726)

[**Language** 3](#_Toc190518727)

[**Documents** 4](#_Toc190518728)

[**Findings** 4](#_Toc190518729)

# **Purpose**

This report aims to serve as a comprehensive resource for stakeholders, developers, and future project teams. It outlines the functional and non-functional requirements of the COMP7003-assign02 project, provides detailed descriptions of relevant project documentation—including the design document, test cases, and user guide—and offers valuable insights to inform future initiatives.

# **Requirements**

|  |  |
| --- | --- |
| **Task** | **Status** |
| Craft and send TCP SYN packets. | Fully implemented |
| Analyze network responses to identify open, closed, and filtered ports | Fully implemented |
| Accepts command-line arguments for target hosts and ports |  |
| Displays results in a structured format | Fully implemented |
| Run the scanner on localhost (127.0.0.1) for all ports | Fully implemented |
| Run the scanner on a remote host, scanning all ports | Fully implemented |
| Run the scanner on all hosts scanning a specific port (22) | Fully implemented |

# **Platforms**

The **main.py** and **packet\_parsers.py** has been tested on:

* Ubuntu 24.04.1 LTS

# **Language**

* Python 3

# **Documents**

* Design (Refer report folder, design.pdf)
* Testing (Refer report folder, testing.pdf)
* User Guide (Refer report folder, user-guide.pdf)

# **Findings**

#### Professor Provided Ips and ports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP Address | Port | Common Service | Typical Device | Security Risks |
| 192.168.0.1 | 21 | FTP (File Transfer Protocol) | Router, Network Storage, Server | Plaintext authentication, brute-force attacks, unauthorized access |
| 192.168.0.1 | 53 | DNS (Domain Name System) | Router, DNS Server | DNS poisoning, amplification attacks |
| 192.168.0.1 | 1900 | SSDP (Simple Service Discovery) | Router, Smart TV, Media Server | UPnP vulnerabilities, DDoS amplification |
| 192.168.0.1 | 8200 | Media Streaming | Router with media sharing, Smart TV, NAS | Network exposure |
| 192.168.0.1 | 20001 | IoT Device Service | IoT device, Security Camera | Potential backdoor or admin access |
| 192.168.0.2 | 23 | Telnet | Network Switch | Plain text authentication, remote access risk |
| 192.168.0.2 | 80 | HTTP (Web Server) | Router, Web Server | Web-based vulnerabilities |
| 192.168.0.2 | 443 | HTTPS (Secure Web Server) | Router, Secure Web Server | SSL/TLS misconfigurations |
| 192.168.0.2 | 40001 | (Possibly IoT or Admin Port | IoT Device, Smart Camera | Potential remote access vulnerability |
| 192.168.0.2 | 40002 | (Possibly IoT or Admin Port | IoT Device, Smart Camera | Potential remote access vulnerability |
| 192.168.0.3 | 23 | Telnet | Network Switch | Plain text authentication, remote access risk |
| 192.168.0.3 | 80 | HTTP (Web Server) | Router, Web Server | Web-based vulnerabilities |
| 192.168.0.3 | 443 | HTTPS (Secure Web Server) | Router, Secure Web Server | SSL/TLS misconfigurations |
| 192.168.0.3 | 40001 | Possibly IoT or Admin Port | IoT Device, Smart Camera | Potential remote access vulnerability |
| 192.168.0.3 | 40002 | Possibly IoT or Admin Port | IoT Device, Smart Camera | Potential remote access vulnerability |
| 192.168.0.40 | 22 | SSH (Secure Shell) | Linux Server, Router, Switch | Brute-force attacks, weak key vulnerabilities |
| 192.168.0.200 | 853 | DNS over TLS | DNS Server, Router | Man-in-the-middle attacks if improperly configured |
| 192.168.0.200 | 49152 | UPnP or Windows Dynamic Ports | Windows Device, Media Server | Network exposure |
| 192.168.0.200 | 62078 | Apple iTunes Mobile Sync Service | iPhone, macOS Device | Network exposure |
| 192.168.0.203 | 853 | DNS over TLS | DNS Server, Router | Man-in-the-middle attacks if improperly configured |
| 192.168.0.203 | 5000 | Web Services / UPnP | IoT Device, NAS, Media Server | Remote access vulnerabilities |
| 192.168.0.203 | 7000 | Possibly IoT Service | IoT Device, Smart Camera | Potential remote access risk |
| 192.168.0.203 | 7100 | Possibly IoT Service | IoT Device, Smart Camera | Potential remote access risk |
| 192.168.0.203 | 49152 | UPnP or Windows Dynamic Ports | Windows Device, Media Server | Network exposure |
| 192.168.0.203 | 49159 | Possibly IoT Service | IoT Device, Smart Camera | Potential remote access risk |
| 192.168.0.203 | 61029 | Possibly IoT Service | IoT Device, Smart Camera | Potential remote access risk |
| 192.168.0.203 | 62078 | Apple iTunes Mobile Sync Service | iPhone, macOS Device | Network exposure |

#### Hosts Guesses

* 192.168.0.1 → Router or Network Gateway
* 192.168.0.2 & 192.168.0.3 → Router, Switch, or IoT Device
* 192.168.0.40 → Linux Server or Firewall
* 192.168.0.200 → iPhone or macOS Device, or Windows PC
* 192.168.0.203 → iPhone, macOS, or Windows PC

#### Open ports on Localhost

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Port | Common Service | Security Risks |
| 127.0.0.1 | 22 | SSH (Secure Shell) | Plaintext authentication, brute-force attacks, unauthorized access |
| 127.0.0.1 | 631 | Internet Printing Protocol (IPP) | Unauthenticated access to print jobs, potential DoS attacks, exposure of sensitive data |
| 127.0.0.1 | 7070 | RealServer (Streaming Media) | Unauthorized access to media streams, buffer overflow vulnerabilities |
| 127.0.0.1 | 6463 | Discord RPC (Rich Presence) | Possible data leakage |
| 127.0.0.1 | 39330 | Dynamic or Ephemeral Port (Unknown) | Could be used by a custom app, temporary communication for software |
| 127.0.0.1 | 39697 | Dynamic or Ephemeral Port (Unknown) | Could be used by a custom app, temporary communication for software |

A screenshot of a computer

AI-generated content may be incorrect.