COMP 7003
Introduction to Information and Network Security

Assignment-03

Report

Anmol Mittal
A01397754

February 16th, 2025

Course Reference Number (CRN): 91662

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
If the host responds with TCP SYN/ACK, then send a TCP RST packet.	Fully implemented
Analyze network responses to identify open, closed, and filtered ports	Fully implemented
Accepts command-line arguments for target hosts and ports	Fully implemented
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

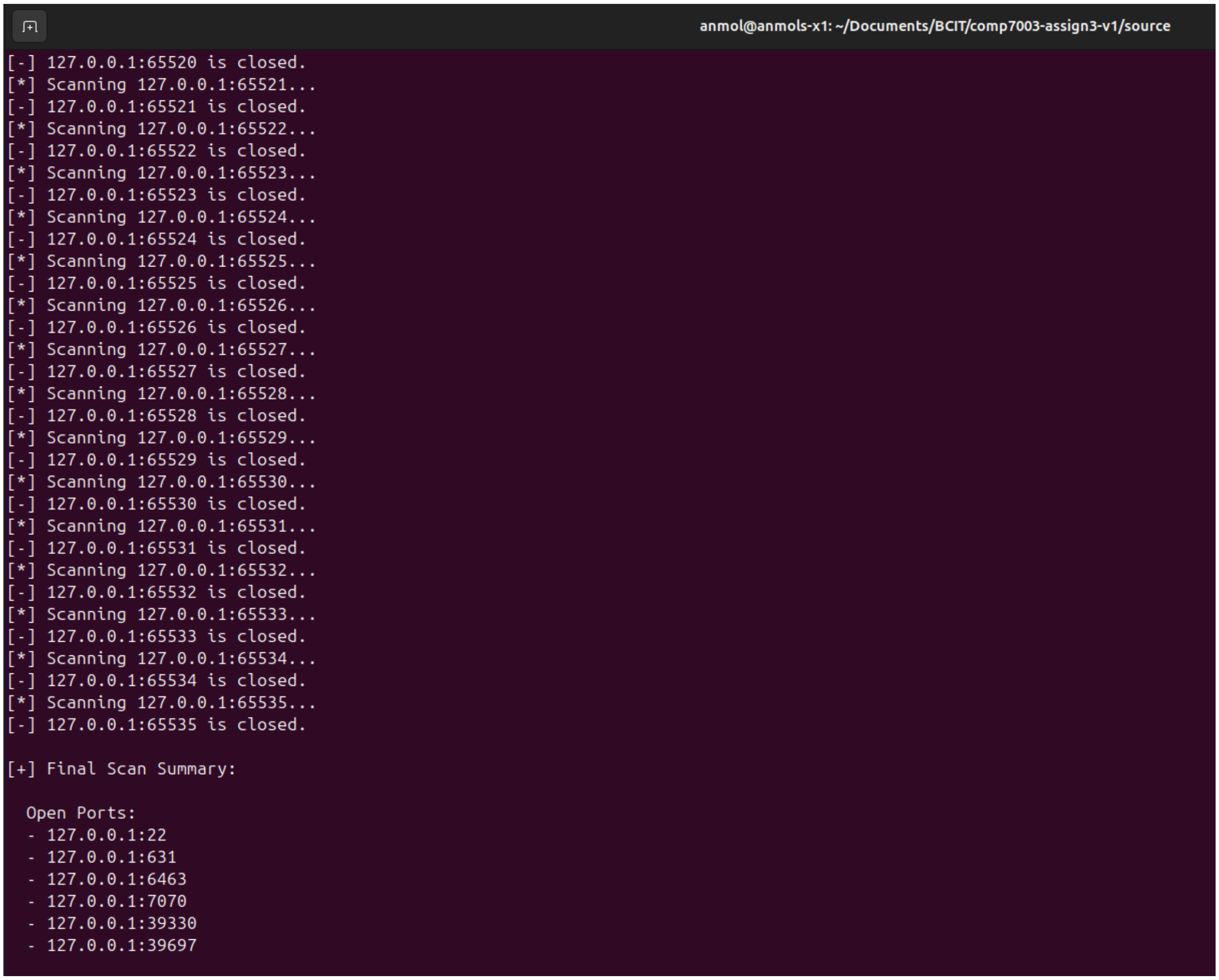
IP Address	Port	Common Service	Typical Device	Security Risks
192.168.0.1	21	FTP (File Transfer Protocol)	Router, Network Storage, Server	Plaintext authentication, brute-force attacks, unauthorized access
192.168.0.1	53	DNS (Domain Name System)	Router, DNS Server	DNS poisoning, amplification attacks
192.168.0.1	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

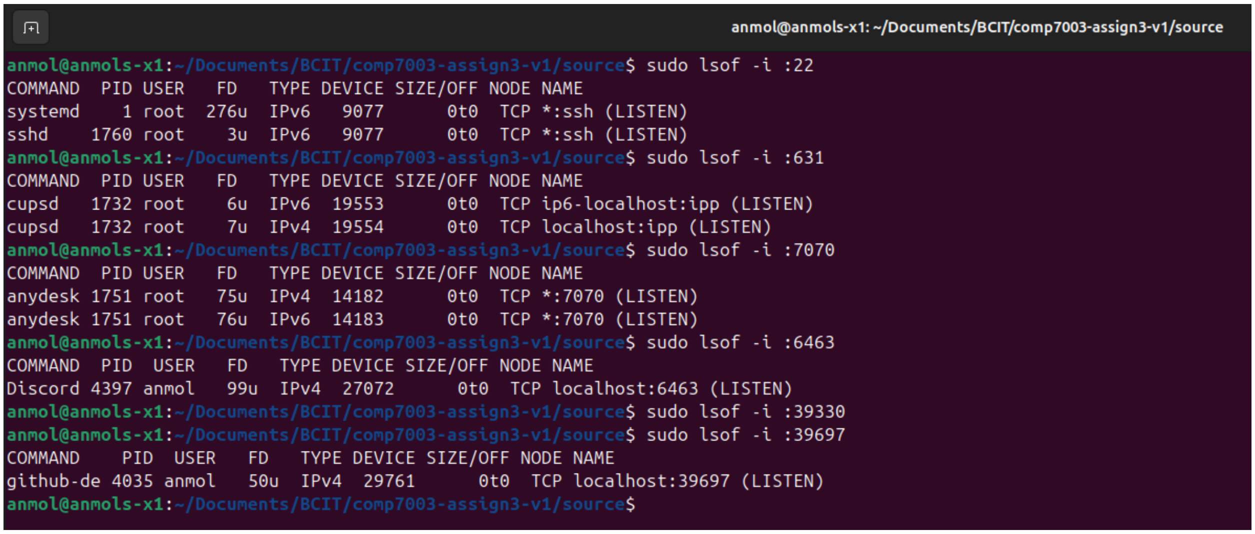

anmol@anmols-x1: ~/Documents/BCIT/comp7003-assign3-v1/source

```
[-] 127.0.0.1:65520 is closed.
[*] Scanning 127.0.0.1:65521...
[-] 127.0.0.1:65521 is closed.
[*] Scanning 127.0.0.1:65522...
[-] 127.0.0.1:65522 is closed.
[*] Scanning 127.0.0.1:65523...
[-] 127.0.0.1:65523 is closed.
[*] Scanning 127.0.0.1:65524...
[-] 127.0.0.1:65524 is closed.
[*] Scanning 127.0.0.1:65525...
[-] 127.0.0.1:65525 is closed.
[*] Scanning 127.0.0.1:65526...
[-] 127.0.0.1:65526 is closed.
[*] Scanning 127.0.0.1:65527...
[-] 127.0.0.1:65527 is closed.
[*] Scanning 127.0.0.1:65528...
[-] 127.0.0.1:65528 is closed.
[*] Scanning 127.0.0.1:65529...
[-] 127.0.0.1:65529 is closed.
[*] Scanning 127.0.0.1:65530...
[-] 127.0.0.1:65530 is closed.
[*] Scanning 127.0.0.1:65531...
[-] 127.0.0.1:65531 is closed.
[*] Scanning 127.0.0.1:65532...
[-] 127.0.0.1:65532 is closed.
[*] Scanning 127.0.0.1:65533...
[-] 127.0.0.1:65533 is closed.
[*] Scanning 127.0.0.1:65534...
[-] 127.0.0.1:65534 is closed.
[*] Scanning 127.0.0.1:65535...
[-] 127.0.0.1:65535 is closed.

[+] Final Scan Summary:

  Open Ports:
  - 127.0.0.1:22
  - 127.0.0.1:631
  - 127.0.0.1:6463
  - 127.0.0.1:7070
  - 127.0.0.1:39330
  - 127.0.0.1:39697
```

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) (Anydesk)	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


anmol@anmols-x1: ~/Documents/BCIT/comp7003-assign3-v1/source

```
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :22
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd    1 root  276u  IPv6   9077      0t0  TCP *:ssh (LISTEN)
sshd    1760 root    3u  IPv6   9077      0t0  TCP *:ssh (LISTEN)
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :631
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
cupsd   1732 root    6u  IPv6  19553      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd   1732 root    7u  IPv4  19554      0t0  TCP localhost:ipp (LISTEN)
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :7070
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
anydesk 1751 root   75u  IPv4  14182      0t0  TCP *:7070 (LISTEN)
anydesk 1751 root   76u  IPv6  14183      0t0  TCP *:7070 (LISTEN)
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :6463
COMMAND  PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
Discord 4397 anmol   99u  IPv4  27072      0t0  TCP localhost:6463 (LISTEN)
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :39330
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$ sudo lsof -i :39697
COMMAND    PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
github-de 4035 anmol   50u  IPv4  29761      0t0  TCP localhost:39697 (LISTEN)
anmol@anmols-x1:~/Documents/BCIT/comp7003-assign3-v1/source$
```