**Name: Akhil Montrose**

**Course Code: TCOM3003**

**Lecturer: Wilbur Roberts**

**Document Type: Lab 1: Scanning & Reconnaissance**

# Part A

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, text, chat or text message

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

A picture containing text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

# Part B: Open Vas

## Part A: OpenVas Start

Text

Description automatically generated with medium confidence

## Part B: Openvas Target

A picture containing text, wall, green, screen

Description automatically generated

Graphical user interface, website, timeline

Description automatically generated

Graphical user interface

Description automatically generated

## Part C: OpenVas vulnerability scan

Graphical user interface

Description automatically generated

Graphical user interface, website

Description automatically generated

## Part D: The Report

Graphical user interface

Description automatically generated

Text

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, text

Description automatically generated

Description of 3 of the vulnerabilities:

* Ingreslock: It is a backdoor installed on the remote host.
* VNC Brute Force Login: It tries to login with the given passwords via VNC protocol.
* DistCC Remote Code Execution Vulnerability: DistCC 2.x as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.