CYB552 – BANNER GRABBING

Target ip – 192.168.100.5

Start ports used – 20,100

End ports used – 25,1000

Output :

Status of ports – closed with banner grabbing

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

a.) Identifies Services and Versions: Determining the services that are operating on a host and their version numbers aid in the vulnerability assessment process.   
Collects Configuration Information: Vulnerabilities can be discovered by looking at the configuration of a service.

b.) sock.Up to 1024 bytes can be read from the opposite end of the connection using recv (1024). It is essential for banner grabbing as it records the service's first response (banner) once the connection has been made. This offer helpful details about the service.

c.) Examples of Banner Information:

* HTTP: "HTTP/1.1 200 OK" (indicating the status and version).
* FTP: "220 Welcome to FTP service" (service greeting message).
* SSH: "SSH-2.0-OpenSSH\_7.4" (indicates the SSH version).

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated