Vulnerability Report – Task 3
Performed Using OpenVAS (Greenbone Vulnerability Manager)

Overview:

A vulnerability scan was performed on the local system (127.0.0.1) using OpenVAS (GVM). The scan successfully completed and detected 1 Medium-severity vulnerability.

Target Information:

- Target IP: 127.0.0.1
- Scan Type: Full & Fast
- Scanner: OpenVAS (GVM Community Edition)

Detected Vulnerability:

1. Apache server-status Information Disclosure

Severity: Medium
Port: 80/tcp
CVE: CVE-2020-25073

Description:

Apache exposes the /server-status page which leaks sensitive system information.

Impact:

Attackers can analyze load, modules, config, and plan targeted attacks.

Fix:

- Disable mod_status or restrict access to localhost.

See task3.pdf and screenshots folder for evidence.