# Network Vulnerability Test with OpenVAS in TryHackme

Agasthya P – CH.EN.U4CYS22004

OpenVAS (Open Vulnerability Assessment Scanner) is a comprehensive open-source tool designed to identify vulnerabilities in networked systems. It's a key component of the Greenbone Vulnerability Management (GVM) framework, which offers a suite of tools for effective vulnerability assessment and management.

**GVM Framework Architecture:**

The GVM framework comprises several components:

* **Front-End:** Includes the Greenbone Security Assistant (GSA) and other web interfaces that users interact with.
* **Back-End:** Consists of the OpenVAS scanner, which performs the actual vulnerability assessments, and the Greenbone Vulnerability Manager (GVM), acting as an intermediary between the scanner and the user interfaces.
* **Vulnerability/Information Feed:** Contains Network Vulnerability Tests (NVTs), Security Content Automation Protocol (SCAP) data, and user-provided information, forming the basis for system assessments.

### Scanning:

1. **Configure a Target:**
   1. Navigate to the "Configuration" section.
   2. Select "Targets" and create a new target by specifying the IP address or hostname of the system you wish to scan.
2. **Create a Scan Task:**
   1. Go to the "Scans" section and select "Tasks."
   2. Create a new task, linking it to the previously configured target.
3. **Execute the Scan:**
   1. Start the task and monitor its progress.
   2. Upon completion, review the results to identify detected vulnerabilities.

**Reporting and Continuous Monitoring:**

OpenVAS provides detailed reports highlighting identified vulnerabilities, their severity, and potential remediation steps. Regular scans and continuous monitoring are essential to maintain network security and promptly address new vulnerabilities.

**Practical Vulnerability Management:**

Effective vulnerability management involves:

* **Identification:** Detecting vulnerabilities through regular scans.
* **Evaluation:** Assessing the severity and potential impact of identified vulnerabilities.
* **Remediation:** Implementing fixes or mitigations to address vulnerabilities.
* **Documentation:** Maintaining records of identified vulnerabilities and the actions taken.
* **Review:** Regularly reassessing systems to ensure vulnerabilities have been effectively addressed.

