Vulnerability Testing using OpenVAS

By,

Harshil Tarun Kanakia

Vulnerability Testing

Vulnerability testing (also called vulnerability assessment) is the **process of identifying, analyzing, and evaluating security weaknesses** in a computer system, network, application, or other IT environment.

In simple terms, It’s like doing a health check for your digital systems to find out where they’re weak and could be attacked.

Why to perform?

- Prevent hackers from exploiting weaknesses
- Protect sensitive data (personal, financial, business)
- Stay compliant with regulations (e.g., GDPR, HIPAA, PCI-DSS)
- Reduce risks and downtime

Reasons for Vulnerability?

- Outdated software
- Misconfigurations (like open ports)
- Missing security patches
- Weak passwords
- Known vulnerabilities (based on CVEs – Common Vulnerabilities and Exposures)

Common Tools used

- OpenVAS / GVM
- Nessus
- Qualys
- Nmap (basic scanning)
- Burp Suite (for web apps)

Output of Vulnerability Testing

- A report that lists:

1) Each vulnerability found
2) Severity level (Low, Medium, High, Critical)
3) Description of the issue
4) Possible fixes or recommendations

Vulnerability Testing using OpenVAS

Vulnerability testing using OpenVAS (now known as Greenbone Vulnerability Management – GVM) is a process of scanning systems to identify security weaknesses. OpenVAS is a powerful open-source vulnerability scanner maintained by Greenbone Networks.

Requirements

- A Linux system (Kali, Ubuntu, or Debian are preferred)
- Internet access
- OpenVAS / GVM installed

Installing OpenVAS via Docker

- **Install Docker**

  sudo apt update

  sudo apt install docker.io -y
- **Run the Greenbone Community Container**

  docker run -d -p 9392:9392 --name gvm greenbone/gvm
- **Access the web interface**

  https://localhost:9392

  Defaulter user name and password = admin

Demonstration

https://www.youtube.com/watch?v=leOPbzgg7oA