**Module 5** : **vulnerability**

* VAPT : Vulnerability Assesment & Penetration Testing .
* **CWE (Common weakness Enumeration site):**

Link: [ <https://cwe.mitre.org/> ]

* **CVE (Common Vulnerability and Exprosures):**

Link: [ <https://cve.mitre.org/> ]

* **NVD ( National Vulnerability Database):**

Link: [ <https://nvd.nist.gov/> ]

* **Exploit Database by Rapid 7 (IMPORTANT)**

Link: [ <https://www.exploit-db.com/> ]

* **Vulnerability Analysis in Linux: (Important)**
* OpenVas-GVM tool
* to detect security problems in remote systems.
* Using gvm tool <step by step>:
* To install: Sudo apt Install openvas
* To Update gvm database: sudo gvm-feed-update
* To Start tool: sudo gvm-start
* To open GUI Interface, browse: <https://127.0.0.1:9392>
* Login Credientials: username - admin, password – admin
* **For Immediate Scan: (Important)**

Select Scan tab > goto left panel and select star> select task wizard > set target ip > scan

* **For manual Scan: (Important)**

1. **Define target:**

**Steps:** Configuration tab> targets >on left side corner- click on new target> input name> input comment> input Host/target Ip > Port list(default) > Alive test (default)> Save

1. **Define Scan:**

**Steps:** scan tab > task> new task > input name> input comment> scan target> select target > scan

* **Vulnerability Analysis in Windows: (Important)**
* **Nessus Tool:**
* Install Nessustool & browse: <https://localhost:8834>
* Username: admin , Password: Pa$$w0rd

1. **Define Scan Policy first:**
2. Click on policies (left Side panel) > Create new policy > select Advance Scan > input Policy name> input Description > select
3. Click on Discovery > port scanning > check all port enumeration.
4. Click on Advance> assign value to max number of concurrent tcp session per host and per scan too (value: Maximum , for both per host and per scan)
5. Click on Credientials> select category> host> windows> add username and password
6. Goto plugins> save
7. For Scan: create a new scan > user-defined > Assign target > Start scan