## **horizontal line**

**Vulnerability Assesment**

**Vulnerability analysis is a part of the scanning phase. In the Hacking cycle.**

**vulnerability analysis is a major and important part. In this module, we will discuss the concept**

**of vulnerability assessment, Vulnerability Assessment phases, types of assessment, tools and other important aspects.**

**This is a fundamental task for a penetration tester to discover the vulnerabilities in an environment.**

**Vulnerability assessment includes discovering weakness is an environment, design flaws and other security concerns which can cause an operating system, application or website to be misused.**

**Basically, In vulnerability assessment we will check Vulnerability Impact and Vulnerability Ranking**

**What type of vulnerabilities included :**

**- Misconfiguration**

**- Default Configuration**

**- Design flaws**

**- Buffer Overflow**

**- Operating System Flaws**

**- SQL Injection**

**- XSS Attack etc.**

**Vulnerability Divides in Four categories**

**1. Low**

**2. Medium**

**3. High**

**4. Critical**

**Types of Vulnerability Assessment**

**• Active Assessment - Direct interaction**

**• Passive assessment - Indirect Interaction**

**• External Assessment - Outside Org**

**• Internal Assessment - Inside Org**

**• Host Based Assessment - On a Pc**

**• Network Assessment - On a Network**

**• Application Assessment - Web, Mobile etc.**

**• Wireless Network Assessment - WIFI**

**Vulnerability Management Life Cycle**

**1. Creating Baseline**

**2. Vulnerability Assessment**

**3. Risk Assessment**

**4. Remediation**

**5. Verification**

**6. Monitor**

**Vulnerability Scoring Systems**

**1: Common Vulnerability Scoring System (CVSS)**

**Security Base Score Rating**

**None 0.0**

**Low 0.1 - 3.9**

**Medium 4.0 - 6.9**

**High 7.0 - 8.9**

**Critical 9.0 - 10.0**

**2: Common Vulnerabilities and Exposure (CVE) - http://cve.mitre.org - https://www.exploit-db.com/**

**3: National Vulnerability Database (NVD) - https://nvd.nist.gov**

**Vulnerability Assessment Tools**

**Nikto**

**Legion**

**NMAP**

**OWASP ZAP**

**Nessus**

**BURPSUITE**

**Nexpose/InsightVm**

**Acunetix**