**Module 05: Vulnerability Analysis**

**Vulnerability Research**

* The process of analyzing protocols, services, and configurations to discover vulnerabilities and design flaws that will expose an OS and its applications to exploit, attack, or miuse.
* Classfied based on severity level and exploit range (local, remote)

**Vulnerabilities Assessment**

* An in-depth examination of the ability of a system or application, including current security procedures and cointrols, to withstand the exploitation.
* Recognize, measure, and classfy security vulnerabilities in a computer system, network, and communication channels.

**Vulnerability Scoring System and Databases**

* **CVSS**: Common Vulnerability Scoring System, provide an open framework for communicating the characteristics and impacts of IT vulnerabilities.
* **CVE**: Common Vulnerabilities and Exposures, a publicly available and free-to-use list od dic of standardized identifiers for common…
* **NVD**: National Vulnerability Database, a **US government repository** of standards-based vulnerability management data represented using the **SCAP (Security Content Automation Protocol)**
* **CWE:** Common Weakness Enumeration, **a category system** for software vulnerabilities and weaknesses.

**Vulnerability Assessment Life-Cycle**

* Identifies assets and create a baseline
* vulnetability scan
* risk assessment
* remediation
* verification
* monitor

**Vulnerability Classfication**

* Misconfiguration
* Default Installation
* Buffer Overflow
* Unpatched Servers
* Design Flaws
* OS Flaws
* Application Flaws
* Open Services
* Default Passwords

**Types of Vulnerability Assessment**

* **Active Assessments** : actively sending requests to the live network and examining the the responses. It requires probing the target host.
* **Passive Assessments** : includes packet sniffing to discover vulnerabilities, running services, open ports, and others. It is a process without interfering the target host.
* **External Assessment** : find out vulnerabilities and exploit them from outside.
* **Internal Assessment** : find and exploit vulnerabilities in the internal network.
* **Host-based Assessment…**
* **Network-based Assessment…**
* **Application Assessment…**
* **Database Assessment…**
* **Wireless Network Assessment…**
* **Distributed Assessment…**
* **Credentialed Assessment…**
* **Non-credentialed Assessment…**
* **Manual Assessment…**
* **Automated Asssessment…**

**Vulnerability Assessment Solutions**

**Product based solution vs Service based solution**

* **Product based solutions** are deployed within the network. Usually dedicated for internal network.
* **Service based solutions** are third-party solutions which offers security and auditing. This can be host either inside or outside the network. This can be a security risk of being compromised.

**Tree-based Assessment vs Inference-based Assessment**

* **Tree-based Assessment** is the approach in which auditor follows different strategies for each component of an environment
* **Inference-based Assessment** is the approach to assist depending on the inventory of protocols in an environment

**Vulnerability Assessment Tools**

* **Qualys Vulnerability Management:** A cloud-based service that offers…
* **Nessus Professional:** An assessment solution for identifying the…
* **GFI LanGuard:** Scan, detect, assesses and retifies security vulnerabilities…
* **OpenVAS:** A framework of several services and tools offering…
* **Nikto:** Web server assessment tool that examines a web server to discover…