**Module 1 Threats, Attacks & Vulnerabilities**

**1.5 Vulnerability Scanning Concepts**

**Vulnerability Scanning/Assessment**

* Vulnerability

1. Flaw in system that can leave it open to attack
2. Can also refer to any type of weaknesses in computer system itself/in set of procedures/anything that leaves information security exposed to threats

* Vulnerability Scanning

1. Inspection of potential points of exploit on computer/network to identify security holes
2. Detects & classifies system weaknesses in computers, networks & communications equipment & predicts effectiveness of countermeasures

* Goal is to identify

1. System, network or app weaknesses
2. Unpatched/not-updated systems/apps
3. Common misconfigurations
4. Lack of security controls

**Vulnerability Scanning/Assessment Process**

* Passively test security controls – does not exploit vulnerabilities
* Identify vulnerability/system flaws/unpatched code
* Identify lack of security controls
* Identify common misconfigurations by reviewing system settings/policies/rule sets

**Vulnerability Scanning/Assessment Types**

* Intrusive vs. Non-Intrusive – see passive vs. active reconnaissance

1. Intrusive – directly engaging on target system to identify weaknesses that can be used to launch attack
2. Non-Intrusive – gain vulnerability information about target computer/network w/o actively engaging with systems (Eg. Qualys SSL Labs)

* Credentialed vs. Non-Credentialed

1. Whether authentication credentials (user-ids & passwords) used in scanning
2. Credentialed has lesser risks & may provide more information, but isn’t realistic

* False Positive – occurs when scan mistakenly identifies vulnerability when it’s not