# IT 6823 LM 8. Vulnerability Analysis and Penetration Testing

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

The module introduces the basics of vulnerability analysis and penetration testing which have the same objective: evaluate the system to identify any security weak points. A vulnerability analysis is usually an automated high-level test searching for potential vulnerability in the system. Penetration testing on the other hand, is more targeted and hands-on process testing and exploit weakness in the system.

Vulnerability analysis and penetration testing is covered in details in IT 6843 Ethical Hacking: Network Security and Penetration.

Vulnerability analysis and penetration testing is a part of Detect phase in the NITS security framework.

## Student Learning Outcomes

* **Describe what is vulnerability assessment and its main benefits.** 
  + Definition – “A network vulnerability assessment is a process of identifying security vulnerabilities in systems, quantifying and analyzing them, and remediating those vulnerabilities based on predefined risks”
  + Benefits:

Closing down security gaps

Getting compliant

Maintaining strong security

* + Source: <https://purplesec.us/perform-successful-network-vulnerability-assessment/>
* **Explain the steps in the vulnerability assessment process**

For what each step does, and tools used.

Text

Description automatically generated

* Source: <https://purplesec.us/perform-successful-network-vulnerability-assessment/>
* CVSS (Common vulnerability scoring system)

Be able to know what is CVSS and rating table.

Source: <https://nvd.nist.gov/vuln-metrics/cvss>

* **Discuss why penetration testing is needed.**
* Definition – “A penetration test is a simulated attack to exploit weaknesses and vulnerabilities on a system, network, application, website, wireless network, or employees”.
* Benefits:
  + Determining weakness in the hardware, software, or human assets of an organization in order to develop controls.
  + Maintaining the 3 triads of cyber security – Confidentiality, Integrity, and Availability.
  + Ensuring that controls which have been implemented are adequate.
  + Providing intelligence and insight of an organization’s security measures by understanding how it could be and likely will be attacked and what steps should be taken to secure the organization.
  + Improving the overall security posture of an organization
* Source: <https://purplesec.us/penetration-test/>
* **Explain the approaches and types of penetration testing**
* 3 approaches - Focus on the characters of each type and its advantages.
  + Black Box
  + White Box
  + Gray Box

Source: <https://purplesec.us/types-penetration-testing#Involve>

* 5 types pen testing – focus what each type does and main benefits.
  + Network Services
  + Web Application
  + Client Side
  + Wireless
  + Social Engineering
  + Physical Penetration Testing

Source: <https://purplesec.us/types-penetration-testing/#Types>

* **Compare and contrast vulnerability scan and penetration testing**

The table below provides a good summary. Need to know the benefits and limitations of each types of testing.

| **Items** | **Vulnerability scan** | **Penetration Cost** |
| --- | --- | --- |
| Objectives | Identify and report potential vulnerabilities in the system | Simulated attacks to detect and exploit weakness in the system |
| Process | Often automated, high level test | Hands-on by a real person |
| Results | Less accurate and less details | More accurate and thorough |
| Cost | Generally, very affordable | More costly |
| Time to complete | Quick to complete | Take more time (1 day to weeks) |
| Frequency | Weekly/monthly/quarterly | Annually or after significant change |

Source: <https://www.securitymetrics.com/blog/pentesting-vs-vulnerability-scanning-whats-difference>