FIT1047 Applied Session Week 12

VULNERABILITIES AND ATTACKS

OBJECTIVES

The purpose of this applied session is to introduce two resources:
(i) The NSA Network Infrastructure Security Guidance report
(ii) The NIST NICE Framework.

INSTRUCTIONS

- You may work in a small group.

Activity 1: The NSA Network Infrastructure Security Guidance report

Read the NSA Network Infrastructure Security Guidance report and answer the following questions:

a. What does NSA recommend with respect to frequently changing passwords?

b. What is the minimum required cryptography policy for VPNs using IPSec?

c. What should a DMZ be used for?

d. What are "discovery protocols" and why does the NSA recommend disabling them?

Sample Solution:

a. Article 5.8
b. Article 2.6
c. Article 2.1
d. Article 7.10

Activity 2: The NIST NICE Framework

Read the NSA Network Infrastructure Security Guidance report and answer the following questions:

a. How many speciality areas and work roles are defined for cybersecurity jobs?

b. List speciality areas and work roles that need the following skills:

(i) [K0059] - Knowledge of new and emerging information technology (IT) and cybersecurity technologies.

(ii) [K0068] - Knowledge of programming language structures and logic.

(iii) [K0170] - Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.

(iv) [K0342] - Knowledge of penetration testing principles, tools, and techniques.

c. List the high level role description and the detailed tasks of the following roles:

(i) Vulnerability Assessment Analyst
(ii) Cyber Defense Incident Responder
(iii) Exploitation Analyst
(iv) Cyber Ops Planner

Sample Solution:

a. Areas: 33 Roles: 52
b.
   - [K0059] - Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
     i. Authorizing Official/Designating Representative
     ii. Security Control Assessor
   - [K0068] - Knowledge of programming language structures and logic.
     i. Software Developer
   - [K0170] - Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
     i. Enterprise Architect
   - [K0342] - Knowledge of penetration testing principles, tools, and techniques.
     i. Authorizing Official
c. The high level role description and the detailed tasks of the following roles:
   (i) Vulnerability Assessment Analyst
   (ii) Cyber Defense Incident Responder
   (iii) Exploitation Analyst
   (iv) Cyber Ops Planner
   can be found in the work role table of contents.