Lesson Plan

LESSON TITLE: **Module 9: Vulnerability Assessment/System Hardening**

SUMMARY:

Securing any information system requires circumspect planning on both ends of the development life cycle. First, software developers must build applications with a "security-first" mindset. Second, end users must be aware of common vulnerabilities and take care to avoid them. To use the analogy of a car, the developer's job is to produce a safe vehicle. This may mean sacrificing speed, increasing cost, and other tradeoffs. On the other side of the coin, an end user must be a "defensive driver" who avoids accidents by compensating for others' mistakes.

As such, erecting defenses against these dangers must necessarily be two-pronged: 1) responsible development and 2) attack surface reduction with trustworthy software and circumspect protocols. Responsible end users of every stripe should know how to assess the vulnerabilities of their system(s), then implement appropriate defense modifications.

GRADE BAND:

☐ K-2 ☐ 6-8

☐ 3-5 ☒ High School

Time Required:

180 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- Understand system vulnerability assessment;
- Perform penetration testing of systems;
- Recommend remedial actions for system hardening.

Materials List:

- Lecture Presentation
- KaliTools, OpenVAS, Armitage
- VirtualBox

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

- Delivery method - participatory lecture
- Formative assessment (web-based student response system and "Fist-to-Five")
- Gamification (periodic quizzes, leaderboard)
- Group discussion after activity
- Cooperative active learning

This lesson includes:

☒ Mapping to Cyber Security First Principles
☒ Learning Objectives
☒ Assessments

Mapping to Cyber Security First Principles:

☒ Domain Separation
☐ Abstraction
☐ Process Isolation
☒ Data Hiding
☒ Resource Encapsulation
☐ Layering
☒ Modularity
☐ Simplicity
☐ Least Privilege
☐ Minimization

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Other Choose an item. Choose an item. Choose an item. Choose an item.	Participants will use Armitage to perform a cyber-attack on a virtual system. Next, they will perform a hands-on assessment using KaliTools and OpenVAS. After analyzing the reports, participants will identify actions to minimize attack surfaces.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Reference YouTube videos will include annotation and/or closed captioning as appropriate.

Description of Extension Activity(ies):

Vulnerability Assessment and Penetration Testing

Participants will use Armitage to perform a cyber-attack on a virtual system, highlighting the multiple significant dangers inherent in an older, un-patched system. Next, they will perform a hands-on assessment using KaliTools and OpenVAS. After analyzing the reports, participants will identify actions to minimize attack surfaces. Afterwards, they can verify their new defenses by repeating their previously successful cyber-attacks.

Acknowledgements: