Minnesota State College Southeast

NWAT 2693: Website and Applications Security

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 3

Lab Hours/Week: *.*

OJT Hours/Week: *.*

Prerequisites:
This course requires all three of these prerequisite categories
1. One of these two groups
    1. NWAT 1608 - MS Workstation
    Or
    2. Both of these
        NWAT 1601 - MS Workstation I
        NWAT 1602 - MS Workstation II
    And
2. NWAT 1641 - Networking Fundamentals
    And
3. NWAT 2681 - Fundamentals of Security

Corequisites: None

MnTC Goals: None

Website and application security prepares the student for a role as a security officer, auditor, security professional, or site administrator. It also empowers a website and/or application developer with the knowledge necessary to create and maintain secure applications. The course studies how various vulnerabilities in server architecture, web/application development, and database structure expose these systems to attack. Students learn how these vulnerabilities are exploited and develop the skills to effectively protect these systems against attack. Students will gain an understanding of the tools hackers use to exploit these issues. They also learn to effectively utilize tools to detect attack and set up appropriate countermeasures to defend against attacks and intrusion. (Prerequisites: NWAT1641, NWAT1649, NWAT2681 and NWAT2689) (3 credits: 3 lecture/0 lab)

B. COURSE EFFECTIVE DATES: 04/15/2015 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. Session Hijacking
2. Web Server/Application Vulnerabilities
3. Web-Based Password Cracking
4. Hacking Web Browsers
5. SQL Injection/Database Server Hacking

D. LEARNING OUTCOMES (General)

1. Explain what happens when a session is hijacked
2. Identify TCP/IP hijacking and session hijacking tools
3. List common Web server and IIS server vulnerabilities
4. List and user countermeasures
5. Understand the anatomy of an attack
6. Understand Web application threats
7. Use Web application hacking tools
8. Define authentication and list authentication mechanisms
9. Understand Web browsers
10. Hack popular user browsers
11. Understand browser security and privacy features
12. Understand SQL injection and describe SQL injection techniques
13. Understand blind SQL injection
14. Take countermeasures against SQL injection
15. Understand hacking database servers
16. Break into an Oracle database
17. Hack a SQL server
18. Secure a SQL server using security tools

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted