ICS 482 : Vulnerability Assessment and Penetration Testing

A. Course Description

Credits: 4

Prerequisites: ICS 382 Computer Security OR instructor permission.

Lab Hours/ Weeks: Corequisites: None

Lecture Hours/ Week :

MnTC Goals: None

To properly secure any organization’s information infrastructure and assets, a periodic assessment of its security posture at various levels of the organization is essential. One key area is the direct assessment of vulnerabilities in the IT infrastructure, systems and applications, followed by targeting and exploitation of the same. This course covers the theoretical bases for cyber threats and vulnerabilities, and delves into selection and application of penetration testing methodologies ranging from reconnaissance to the exploitation of vulnerabilities by probing infrastructure, services and applications. The course places a strong emphasis on the use of these methodologies to demonstrate, document, report on, and provide a clear roadmap for remediation of exposed security issues.

B. Course Effective Dates: 08/20/2016 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Theoretical Learning Outcomes: o Understand applicable theories connecting cybersecurity to human behavior. o Critique the purpose and goals of vulnerability assessments and penetration testing. o Interpret and differentiate cyber threats and exploits in a penetration testing context. o Describe and distinguish key phases of ethical hacking: reconnaissance, scanning, gaining access, maintaining access, and covering the tracks.

2. Practical Learning Outcomes: o Perform protocol analysis using packet captures and analysis data using a sniffer (e.g. Wireshark). o Investigate and uncover network devices, operating systems, ports, and services (e.g. Nmap). o Discover network security issues using an intrusion detection tool (e.g. Snort). Implement and leverage penetration testing suite of applications (e.g. Metasploit) to:

3. o Recognize information targets across operating systems and services. o Implement scripts and tools to assist in penetration testing. o Deploy and test exploits targeting operating systems and services. o Conduct remote and client side attacks. o Identify and exploit various vulnerabilities in web applications. o Deploy tunneling techniques to bypass firewalls.

4. Apply testing methodologies using tools such as Wireshark, Nmap, Snort, Metasploit and related applications and platforms.

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information
Note: Students are responsible to both be aware of and abide by prerequisites for ICS courses for which they enroll, and will be administratively dropped from a course if they have not met prerequisites.