ICS 487 : Cyber Incident Response and Handling

A. Course Description

Credits: 4

Prerequisites:

ICS 382 Computer Security
OR
MATH 215 Discrete Mathematics

Lab Hours/ Weeks:

Corequisites: None

Lecture Hours/ Week :

MnTC Goals: None

As cyber breaches and intrusions continue to increase, enterprises are now looking to hire professionals who can identify and respond to breaches and incidents before they have adverse impacts on information systems and data networks. This course provides an in-depth coverage of applying Digital Forensics and Incident Response methodologies and frameworks to address and manage the aftermath of security breaches or incidents with the goal of limiting the damages and reducing the recovery time and costs. The student will be able to identify, contain, eradicate and recover from an attack in an enterprise network. Topics include identifying threat actors and security breaches, analyzing artifacts and logs, restoring back the system, performing postmortem analysis, and implementing and/or modifying mitigating techniques.

B. Course Effective Dates: 05/07/2019 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Identify and analyze the attacker's Tactics, Techniques, and Procedures (TTPs) to evaluate the modus operandi of cyber adversaries, target the resulting investigation and incident response, and anticipate and mitigate future activity.
2. Demonstrate a practical understanding of various methodologies for analyzing artifacts left on a compromised system.
3. Apply Incident Handling methodology based on the National Institute of Standards and Technology (NIST), the US-CERT, and other frameworks.
4. Use various available digital forensic and security tools in an efficient and effective manner to aid in investigation.
5. Validate the current stage of a cyber-attack based on the Lockheed Cyber Kill Chain model.
6. Produce quality reports and communicate the technical contents to a variety of audiences.

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.