ITMS 458 SYLLABUS

ITMS 458 Operating System Security

Hours: 3 credit hours / 60 contact hours

Instructor: Sean Hughes-Durkin

Textbook, title, author, and year: Online materials will be assigned for reading

Specific course information

a. **Catalog description:** This course will address theoretical concepts of operating system security, security architectures of current operating systems, and details of security implementation using best practices to configure operating systems to industry security standards. Server configuration, system-level firewalls, file system security, logging, anti-virus and anti-spyware measures and other operating system security strategies will be examined.
b. **Prerequisites: ITMO 356.**
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will be able to describe the different types of malicious threats targeted to an operating system. The student will be able to explain ways to mitigate these threats, correct vulnerable configurations, and use best practices to harden systems. This course and the concepts described in the class cover topics included on the Certified Information Systems Security Professional (CISSP). The GIAC Security Essentials (GSEC) certification is another recognized security certification that covers the concepts the student will learn throughout this course.
b. **Course student outcomes:**
   Students completing this course will be able to:
   - Describe potential system attacks and the actors that might perform them
   - Describe appropriate measures to be taken should a system compromise occur
   - Describe characteristics of malware and identify different malware
   - Apply tools and techniques for identifying vulnerabilities
   - Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications
   - Securely install a given OS, remove or shut down unnecessary components and services, close unnecessary ports, ensure that all patches and updates are applied
   - Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)

Topics to be covered

a. Malicious Software/Attacks (2 parts)
b. Incident Handling
c. User Authentication & Access Control Cryptographic Tool
d. Host Firewalls
e. Host Based Intrusion Detection (2 parts)
f. General OS Hardening
g. Linux Hardening
h. Windows Hardening
i. Post OS Hardening Testing