ITMS 458 SYLLABUS

ITMS 458 Operating System Security

Hours: 3 credit hours / 60 contact hours

Instructor: Philip Matuszak

Textbook, title, author, and year:

a. *Mastering Windows Security and Hardening, 2nd Edition*, Dunkerley, Mark and Tumbarello, Matt, 2022
b. *Mastering Linux Security and Hardening, 3rd Edition*, Tevault, Donald A. 2020

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 in this course will be become familiar with identifying and applying core security concepts such as defense in depth, least privilege, and vendor best practices to common contemporary operating systems.
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
    - Describe and discuss current trends in information security by experiencing a variety of applications and software packages
    - Identify threats to popular operating systems
    - Propose controls and practices to protect against threats
    - Develop a high level plan to deploy a multilayered approach towards OS securiity

Topics to be covered

a. Introduction to Course and OS Security
b. Security Definitions and Players
c. OS Installations and Best Practices
d. OS Users and groups | Permissions
e. OS Controls Encryption
f. OS Controls Network Access
g. OS Controls Device Access
h. Security Certifications and Providers
i. Securing Servers Vs End user Devices
j. Tools For Auditing and Testing
k. Monitoring and Keeping Systems Up to Date
l. Cloud Based and VDI Security Concepts
m. Student Presentations and Final Review