ITMS 443 SYLLABUS

ITMS 443 Vulnerability Analysis and Control

Hours: 3 credit hours / 45 contact hours

Instructor: Kevin Vaccaro

Textbook, title, author, and year: *Mastering Kali Linux for Advanced Penetration Testing*, Vijay Kumar Velu, 2017

Specific course information

a. **Catalog description:** This course addresses hands-on ethical hacking, penetration testing, and detection of malicious probes and their prevention. It provides students with in-depth theoretical and practical knowledge of the vulnerabilities of networks of computers including the networks themselves, operating systems, and important applications. Integrated with the lectures are laboratories focusing on the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate, and hack other networks. It is recommended, but not required, that students also take ITMS 448 prior to or in parallel with this course.
b. **Prerequisites:** None
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each student will be able to explain the professional hacker's methodology for attacking a network and differentiate between different methods of attacks and countermeasures.
b. **Course student outcomes:**
At the conclusion of this course, each student should be able to:
- Explain the professional hacker's methodology for attacking a network.
- Explain the script kiddie's methodology for attacking network.
- Explain Network Security vulnerabilities.
- Explain Hackers, hacker techniques, tools and methodologies
- Describe hacker motivation, perform network reconnaissance and network scanning methods
- Describe and perform covering tracks after gaining access to a network.
- Describe the general symptoms of a virus attack
- Define and describe the two basic approaches to antivirus software.
- Describe how to defend against a worm and virus attack.
- Describe the steps in planning for a computer incident.
- Identify the difficulty is establishing who has jurisdiction over a computer crime.
- Understand the legal issues with regard to preserving digital evidence.
- Identify and describe the incident response goals and priorities.
- Describe the factors involved in identifying a computer incident.
- Describe and use the various tools associated with identifying an intruder.
- Describe how to handle and evaluate a computer incident.
- Recognize the role of law enforcement and rule of particularity in executing a search warrant.
- Describe the role the network security specialist would play in assisting the law enforcement and prosecution effort.
- Describe the difficulties in prosecuting a computer crime incident.
- Differentiate between competitive intelligence, economic intelligence, and industrial espionage

Topics to be covered

a. Goal Based Penetration Testing
b. Kali / Using Linux /Basic Scripting
c. Open Source Intelligence and Passive Reconnaissance
d. Active Reconnaissance of External and Internal Networks
e. Vulnerability Assessment
f. Physical Security and Social Engineering
g. Reconnaissance and Exploitation of Web-Based Applications
h. Attacking Remote Access
i. Client-Side-Exploitation
j. Bypassing Security Controls
k. Exploitation
l. Action on Objective
m. Privilege Escalation
n. Command and Control