CYBERSECURITY FOR IT PROFESSIONALS CERTIFICATE

Total Credits: 18
Catalog Edition: 2023-2024

Program Description

Intended for those already employed in computing or who have a computing background, the certificate emphasizes computer security and information assurance concepts augmented with current industry standard techniques. This career curriculum prepares students for entry-level careers in cybersecurity. Topics cover threats and vulnerabilities, prevention at the technical (hardware and software) and human levels, detection, response, and management aspects of security. This program of study is built upon the National Security Telecommunications and Systems Security Instruction (NSTISSI) 4011 and 4013. Each course in this certificate prepares the students in part to sit for the respective professional certifications. Range of occupations applicable to this certificate are: network analyst, network administrator, IT manager, internet security specialist, IT compliant specialist. Before registering, students must contact a program advisor.

Program Outcomes

Upon completion of this program, a student will be able to:

- Describe: security threats, integrity, confidentiality, and availability in security information.
- Describe security ramifications, technology weaknesses, configuration weaknesses, policy weaknesses, and human errors.
- Describe authentication, understand password issues, Kerberos assumptions, challenge handshake authentication protocol, security tokens, and biometrics.
- Define common Internet components, and identify techniques used in web hacking, attacks and malicious code, IP fragmentation attacks, spoofing, man in the middle, and TCP session hijacking.
- Investigate advanced concepts and procedures related to the transmission control protocol/internet protocol (TCP/IP).
- Secure version of internet protocol (IP) and internet protocol security (IPSec).
- Describe Web security, SSL and TLS, HTTPS vulnerabilities, javascript, activex, and buffer overflows.
- Secure workstations and servers running current Windows OS software and test the effectiveness of various security measures.
- Investigate measures that can help ensure business continuity in the event of a disaster, such as contingency planning and power and backup issues.
- Identify the basic components of a layered structure for network defense architecture, describe access control objectives, and auditing concepts.
- Analyze network operations risks; conduct network penetration tests; implement network countermeasures.

CYBERSECURITY FOR IT PROFESSIONALS CERTIFICATE

Program Requirements

A suggested course sequence for full-time students follows. All students should review this advising guide and consult an advisor.

Program Requirements

NWIT 173 - Network Security *3 semester hours*

NWIT 245 - Defending the Network *3 semester hours*

NWIT 246 - Attacker Tools and Techniques *3 semester hours*

NWIT 263 - Introduction to Digital Forensics *3 semester hours*

NWIT 275 - Wireless Security *3 semester hours*

NWIT 290 - Information Security Capstone *3 semester hours*

Total Credit Hours: 18