Ethical Hacking   2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 225 - Ethical Hacking

PREREQUISITES: CSIA 105 - Introduction to Cyber Security/Information Assurance and SVAD 111 - Linux and Virtualization Tech
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 2
LAB HOURS MIN: 2
DATE OF LAST REVISION: Fall, 2020

Students will learn threats and defense mechanisms; web applications and data servers; Linux, Macintosh and mobile systems; and secure network infrastructures. Hands-on practical application will be included.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Demonstrate use of resources to perform system footprinting and enumeration.
2. Discuss the characteristics of Trojans, Viruses and worms.
3. Use sniffing tools to glean information about a network and demonstrate how social engineering and phishing work.
4. Defend against denial of service attacks and vulnerabilities associated with buffer overflows.
5. Hack Web servers and database servers and use password-cracking techniques.
6. Identify and protect against Web application vulnerabilities.
7. Hack Linux, Macintosh, routers, cable modems, firewalls, mobile devices, Bluetooth devices, RFID and USB devices.
8. Determine security policies for Linux, Macintosh, routers, cable modems, firewalls, mobile devices, Bluetooth devices, RFID and USB devices
9. Hack wireless networks and discuss physical security.
10. Evade IDS and Firewalls and detect the existence of honey pots.
11. Apply data security and controls and use basic cryptography for secure communications.

COURSE CONTENT: Topical areas of study include -

- Footprinting
- Enumeration
- Threats and defense mechanisms
- Web applications
- Data servers
- Linux, Macintosh and mobile systems
- Secure network infrastructure

Course Addendum - Syllabus (Click to expand)