BRIDGERLAND
TECHNICAL
COLLEGE
btech.edu

Cybersecurity 2018
Course Descriptions

ITEC 1120 Penetration Testing 45 Clock Hours

This course teaches the skills and concepts of penetration testing. In penetration testing you will learn how to check if a computer, system, network, or web application has vulnerabilities that you can exploit. You will also learn the various types of penetration tests – black, grey, and white box, as well as strategies to ensure that your tests are thorough.

Objectives:

- Effectively use penetration testing tools
- Describe strategies for conducting penetration tests
- Define penetration test types
- Implement penetration test techniques

ITEC 1130 Network Traffic Analysis 60 Clock Hours

This course teaches the basics of network traffic analysis. Students will learn process of recording, reviewing and analyzing network traffic for performance, security and/or general network operations and management.

Objectives:

- Describe and appraise network utilization
- Explain download/upload speeds
- Implement network traffic analysis techniques
- Define type, size, origin and destination and content/data of packets

ITEC 1220 Kali Linux Essentials 30 Clock Hours

This course will teach students the basics of using Kali Linux. Some of the basic skills covered in this course are installing Kali Linux, customizing the OS, main features, loading components, managing packages, configuration, securing and monitoring the OS.

Objectives:

- Install and manage Kali Linux
- Learn Kali Linux basics
- Examine preinstalled cybersecurity tools

ITEC 1420 Mobile Security 30 Clock Hours

In mobile security you will learn the skills needed to understand the strengths and weaknesses in the security of Apple iOS and Android devices. Mobile devices are vital components in day-to-day business and are just as vulnerable, if not more, than traditional computing devices. This course teaches how to evaluate and test mobile security.

Objectives:

- Demonstrate proficiency with mobile application security measures
- Identify models to develop and secure Android applications
- Examine security detection and measures in iOS
- Identify trends in Mobile Device Management (MDM)

ITEC 1430 Advanced Python 45 Clock Hours

This course expands on the basics learned in the Python programming class. This class will explore more advanced topics such as object-oriented programming, system focused programming, and meta programming.

Objectives:

- Demonstrate ability to code Python using the object-oriented programming model
- Execute Python code at a system level
- Implement meta programming

ITEC 2540 Cybersecurity Concepts and Practice 90 Clock Hours

The Cyber Security Essentials - Concepts and Practices is the first half of a basic training system designed to provide a solid theoretical understanding of cyber security challenges, tools, and techniques, as well as develop the foundations of a professional cyber security skill set. This is accomplished in a progressive four-section process in Infrastructure Security, Local Host Security, Local Network Security and Cyber Security. Each area has a hands-on component to emphasize the theoretical materials.

Objectives:

- Understand critical infrastructure security systems and devices
- Implement security for local intelligent computing and controlling devices and systems
- Implement Security for Local Area Network Components and Systems
- Apply Cybersecurity measures for Users and Networks attached to the internet

ITEC 2550 Cybersecurity Environment & Testing 90 Clock Hours

The Cyber Security Essentials - Environments & Testing is the second half of a basic training system designed to provide solid theoretical understanding of cyber security challenges, tools, and techniques, as well as develop the foundations of a professional cyber security skill set. This course expands and extends from the previous four sections in Enterprise Network Security, Industrial Cyber Security Systems, Healthcare IT Security, and Introduction to Ethical Hacking. Each area has a hands-on component to emphasize the theoretical materials.

Objectives:

- Demonstrate effective use of enterprise network security
- Demonstrate effective use of industrial and utility network security
- Demonstrate effective use of medical network security
- Use common hacking tools

ITEC 2631 Digital Forensics Investigation I 60 Clock Hours

This course is the first in a two-course series designed to prepare students for the Certified Hacking Forensic Investigator (CHFI) certification. Students will learn the legal process for proper data collection, the software and methodologies used in analyzing legally collected evidence.

Objectives:

- Demonstrate proper evidence collection and chain of evidence procedures
- Use forensic software to analyze collected data
- Implement methods used to hide, erase or manipulate data
- Describe the legal process and proper evidence introduction

ITEC 2632 Digital Forensics Investigation II 60 Clock Hours

This course is the second in a two-course series designed to prepare students for the Certified Hacking Forensic Investigator (CHFI) certification. Students will be introduced to the process of collecting, analyzing and presenting evidentiary data. Students will expand on the techniques previously learned with advanced processes, mobile data collecting and processing, and white collar/corporate crime.

Objectives:

- Demonstrate advanced use of forensic software including mobile software for mobile data collection and analysis
- Describe the legal process and proper evidence introduction
- Show effective use of Stenography
- Describe the role forensics have in the corporate environment

ITEC 2641 Ethical Hacking I 75 Clock Hours

This course is the first in a two-course series designed to prepare students for the Certified Ethical Hacker (CEH) certification. Topics taught in this course include the ethics and legality of hacking, Footprinting and Social Engineering, Network Scanning and System Hacking.

Objectives:

- Define the legality of ethical hacking and its place in security
- Use Social Engineering in a security audit
- Implement procedures used in ethical and legal Network Scanning and System Hacking

ITEC 2651 Ethical Hacking II 75 Clock Hours

This course is the second in a two-course series designed to prepare students for the Certified Ethical Hacker (CEH) certification. Topics taught in this course include Trojans, Backdoors, Viruses, Worms, Sniffers, Denial of Service, Web Server vulnerabilities and SQL Injections.

Objectives:

- Describe the how Trojans, Backdoors, Viruses and Worms are used in both legal and illegal ways
- Describe network hacking and security testing including the use of Sniffers
- Describe the protection needed in securing web servers and applications and how to prevent and conduct Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Demonstrate ability to secure web and local databases against external and internal attacks

ITEC 2671 Cybersecurity First Responder 90 Clock Hours

This course provides an overview of the evolving field of cybersecurity, with an introduction to cybersecurity standards and law. Students will learn about common cyber-attacks and the techniques for identifying, detecting, and defending against cybersecurity threats. They will also gain a basic understanding of personal, physical, network, web, and wireless security, as well as a foundation for more advanced study of cybersecurity. This course prepares the student for the Cybersecurity First Responder certification.

Objectives:

- Examine common cybersecurity laws, standards and best practices
- Use basic principles of IT Security in defending against cybersecurity threats and protecting information assets
- Identify basic threats and protection mechanisms for internet, network, mobile, wireless and web security
- Demonstrate ability to mitigate cyber vulnerabilities

ITEC 2681 Cybersecurity Analysis 90 Clock Hours

This course will help students understand the fundamentals of threat and vulnerability management and employ suitable tools and methods to secure data and infrastructure as well as respond to a security incident. Besides preparing students for the CompTIA CySA+ exam, this course also serve as a foundation for advanced security credentials including the CompTIA Advanced Security Practitioner (CASP).

Objectives:

- Select and implement appropriate tools and methods to perform an environmental reconnaissance of a system or network
- Gather data and analyze the results of an environmental survey
- Describe and implement techniques and procedures to secure the organization’s information systems environment
- Classify threat data or activities to ascertain the impact of a security incident
- Manage incident response and recovery, including reporting

ITEC 2791 Wireless Security Essentials 90 Clock Hours

This course provides instruction in securing enterprise-level Wi-Fi networks from outside sources. Students will learn wireless security protocols, techniques, and models used in securing a wireless network.

Objectives:

- Define WLAN discovery, intrusion and attack techniques
- Implement Wireless Intrusion Prevention Systems (WIPS)
- Build a strong security network from the ground up
- Implement a comprehensive wireless security policy
- Plan authentication infrastructure design models

ITEC 2901 Special Applications ITEC 180 Clock Hours

A 30-hour course or courses providing competencies that meet an immediate occupational need beyond the skills available in the program's currently approved outline.