LEARNING COMMONS

FRANKLIN UNIVERSITY PROFICIENCY EXAM (FUPE)
STUDY GUIDE

Course Title: CYSC 200: Cybersecurity Fundamentals

Recommended Textbook(s): https://www.franklin.edu/current-students/academic-resources/textbooks

Number & Type of Questions: **50 –** Multiple Choice

Permitted Materials: No materials permitted

Time Limit: 120 minutes (2 hours)

Minimum Passing Score: 75%

Format varies

Outline of the Topics Covered:

Course Description

The Internet has changed dramatically; so have the activities that are dependent on it in some shape or form. Understanding the need for security, it's influence on people, businesses and society, as well as business drivers is critical. The course also covers malicious attacks, threats and vulnerabilities common to the world of security, as well as access controls, and methods to assess and respond to risks. Hands-on labs accompany the various concepts that are taught.

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Explain the concepts of information systems security (ISS) as applied to an IT infrastructure and the way people and businesses communicate
2. Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure, and the methods attackers use to compromise systems, networks, and the defenses used by organizations
3. Explain the role of access controls, operations and administration in implementing an effective security policy
4. Explain how businesses apply cryptography in maintaining information security
5. Analyze the importance of network principles and architecture to security operations

Course Content

1. Introduction to Security
    a. Basic principles of information security.
    b. Hacker’s mindset.
    c. Types and attributes of various threat actors
    d. Malicious software threats.
    e. How malware finds its way in to computer systems.
    f. How to defend against malware threats in a proactive way.
    g. How to fix problems that do occur with malware manifested.
2. Computer Systems Security
    a. How to select, install, and configure security applications
    b. Security tools and selection criteria for different situations
    c. How to protect a computer's hardware
    d. How to protect mobile devices and the data they contain
3. OS Hardening and Virtualization
    a. How to make your operating system strong by using patches and hotfixes.
    b. Reducing the attack surface by disabling unnecessary services and uninstalling extraneous programs.

    c. Virtual machines and their implementations to real world scenarios.
4. Application Security
    a. How to secure a browser.
    b. How to make common applications such as Microsoft Office safe.
    c. Specify concepts to use in programming to make your code secure such as system testing, code reviewing, and fuzzing.
5. Network Design Elements
    a. Various network design elements.
    b. Network address translation, private versus public IP addresses, and the private IP ranges. c. Intranets and extranets.
    d. Protect networks from attacks.
    e. Vulnerabilities and hazards associated with moving server and network resources to the cloud.
    f. Cloud-based threats and how to combat them effectively.
6. Networking Protocols and Threats
    a. Ports and protocols and securing the ports.
    b. How to make decisions on locking down various ports in your configuration.
    c. Basics of network attacks and how to defend against them.
7. Network Perimeter Security, Securing Network Media and Devices
    a. Fundamentals of firewalls.
    b. Various network security concepts such as packet filtering, access control lists, proxy servers, and honeypots.
    c. Characteristics, advantages, disadvantages and differences of network intrusion detection systems and network intrusion prevention systems.
    d. How to reduce the risk of attack to your wired networks and connecting devices.
    e. Security for common network devices such as SOHO routers and firewalls.
    f. How to secure twisted pair, fiber-optic, and coaxial cables.
    g. How to secure wireless access points and protect against intruders.
    h. Wi-Fi security, Bluetooth security, and security of other technologies.
8. Physical Security
    a. Door access, biometric readers, access logs, and video surveillance.
    b. Various fire suppression methods for servers and other company assets.
    c. Proper management and security of facilities to help protect company assets and employees.
9. Authentication Models, Access Control Methods and Models
    a. Various methods and models to authenticate a person who wants access to computers and networks.
    b. Local and remote authentication types.
    c. Various access control models and methodologies.
    d. How to develop a plan of action and access control model to be used in organizations.
    e. Users, groups, permissions, rights, and policies that can be created on a computer network.
    f. Measures to ease administration and security at the same time.
    g. How to implement security templates to make it easier to implement a secure set of policies.

10. Vulnerability and Risk Assessment

a. Concepts of risk management and risk assessment and how they differ.
b. Differences between qualitative and quantitative risk analysis.
c. Vulnerability management methodologies.
d. How to perform penetration tests.
e. How to use common network security tools to measure the vulnerability of computer systems and network devices.

11. Monitoring and Auditing,
    a. Importance of monitoring the network.
    b. Various monitoring methodologies that application solutions use.
    c. Various performance analysis tools and protocol analysis tools.
    d. How to configure logging for your networks.
    e. How to conduct successful and meaningful audits.
12. Encryption and Hashing Protocols/Concepts, PKI Systems
    a. Understand the basic terminology of cryptography.
    b. Differentiate between various encryption algorithms.
    c. Investigate hashing as the most common way to verify the integrity of files.
    d. Fundamentals of public key infrastructure
    e. VPN-related protocols.
13. Redundancy and Disaster Recovery
    a. Setting up redundancy planning.to ensure network and servers are fault tolerant
    b. Disaster recovery plan and procedures.
    c. How to protect against potential failures and recover from would-be disasters.
14. Social Engineering and User Education
    a. Methods and techniques to gain access to buildings and systems and obtain company data and personal information.
    b. How to defeat social engineers.
    c. How to train your users on the basics of security.
15. Policies and Procedures
    a. Ways to classify data.
    b. Laws that protect privacy.
    c. Personnel security policies.
    d. Safe disposal of computers.
    e. Processes and procedures involved in computer security incident management.
    f. Basics of security frameworks and how they can help to organize IT processes and procedures.

Sample Questions

1. You have been tasked with hardening an operating system to prevent hacker attacks. What should you do? (Select the two best answers.)
    a. Install patches
    b. Install a network based IDS
    c. Disable unused services
    d. Install a SSH server
    e. Restart operating system

2. Which law protects personal health records?
    a. FISMA
    b. HIPAA
    c. SOX
    d. GLBA
3. What is fundamental difference between a DoS and DDoS attack?
    a. There is no difference between them
    b. DoS attack is a real type of attack; DDoS is a simulation
    c. DoS may cause privilege escalation; DDoS does not
    d. In DDoS, multiple computers attack to a single server; DoS attack is done from a single computer