POINTFUL EDUCATION

Cybersecurity

Syllabus

» Course Overview

In the Cybersecurity course, students will learn about the practice of protecting networks, systems, and programs from digital attacks. They will better understand the aim of these attacks, such as destroying information, extorting money and resources, or disrupting business operations. They will learn about the challenges and opportunities that implementing cybersecurity measures can present. As attackers become more innovative, it is more important than ever to have effective cybersecurity channels in place to counter them. Students will learn about countermeasures and role recovery and their integral function in the cybersecurity realm. Additionally, students will learn what makes certain networks and systems more vulnerable to attacks. They will become adept at identifying potential viruses, worms, threats, and malware. The Cybersecurity course acts as a foundation on which to build extensive knowledge about threats to digital security.

» Course Outline by Module

Module 1	Introduction to Cybersecurity	**Module 5**	Intrusion and Intrusion Detection Systems Part II
Module 2	The Basics of Cybersecurity Part I	**Module 6**	Intrusion Prevention
Module 3	The Basics of Cybersecurity Part II	**Module 7**	Social Engineering and Fundamental Security Design Principles
Module 4	Intrusion and Intrusion Detection Systems Part I	**Module 8**	Careers in Cybersecurity

» Module Overview and Learning Objectives

Module 1. Introduction to Cybersecurity

In this module, we'll get a glimpse into how cybersecurity has evolved over the years. Students will learn about the importance of computer security and the potential consequences of data breaches. They will get an introduction to defense mechanisms, tools, and technologies used in such attacks.

***Learning Objectives*:** In this module, students will:

- Explain the various elements that make up the security taxonomy used by the U.S. Computer Emergency Readiness Team (CERT) and describe the challenges associated with achieving and maintaining computer security.
- Discuss the range of potential consequences of various forms of security breaches and describe various defense mechanisms, techniques, and methodologies.
- Compare and contrast mechanisms employed in passive and active cyber-attacks and describe the difference between an inside and an outside attack.
- Describe vulnerabilities associated with each element of the CIA Triad and explain the differences between hardware, software, data, and network assets susceptible to cyber-attack.
- Describe the tools and technologies used in cybersecurity and define intrusion detection and discuss its role in cybersecurity.
- Explain what is meant by the term countermeasures and describe the role recovery plays in cybersecurity.

Module 2. The Basics of Cybersecurity Part I

This module will introduce you to the various vulnerabilities associated with cybersecurity. You will learn how hackers use footprinting and port scanning to exploit these vulnerabilities. You will also learn about the importance of a strong password. Finally, you'll learn about different types of cyberattacks like DoS attacks, spoofing, malware, viruses, worms, botnets, and rootkits, and also how and when they are used.

***Learning Objectives*:** In this module, students will:

- Describe the basic categories of vulnerabilities associated with cybersecurity (i.e., hardware, software, network, human, physical, and organizational) and how social networks such as Facebook are cybersecurity targets.
- Describe footprinting and explain how it is used to reveal system vulnerabilities and explain why default values and technical controls are points of vulnerability and describe the hardening efforts being taken by government and industry.
- Describe the process of port scanning and explain why it is so prevalent in cybersecurity.
- Describe what is meant by password strength and explain its relationship to vulnerability, distinguish between a weak and a strong password and describe how intruders can cover their tracks.
- Describe the circumstances under which a computer system is vulnerable to a denial-of-service attack and spoofing as an attack mechanism and discuss its consequences and common motivating factors for its use.
- Describe the introduction of malware, spyware, and grayware as an attack mechanism and discuss its consequences and common motivating factors for its use.
- Describe the use of computer viruses or worms and Logic Bombs as an attack mechanism and discuss its consequences and common motivating factors for its use.
- Describe botnet, rootkit, and Trojan Horse as an attack mechanism and discuss its consequences and common motivating factors for its use.

Module 3. The Basics of Cybersecurity Part II

We will start this module by learning about some more attack mechanisms like DNS poisoning, buffer overflow, and other network and wireless attacks. Next, we will learn about cryptography and steganography, and different security systems that are available to encrypt and protect confidential information.

***Learning Objectives*:** In this module, students will:

- Describe DNS poisoning as an attack mechanism and discuss its consequences and common motivating factors for its use as well as buffer overflow as an attack mechanism and discuss its consequences and common motivating factors for its use.
- Describe wired/media-agnostic network attacks including but not limited to Man-in the middle/Arp spoofing, and DHCP.
- Examine safe wireless configuration options and dealing with wireless issues as an added attack surface.
- Describe Cryptographic Algorithms including Hashing Functions, Symmetric Keys, Asymmetric Keys, and Kerberos.
- Describe steganographic techniques including network steganographic methods (e.g., VOIP, WLAN), digital steganographic methods (e.g., image encryption, audio, mimic functions, video, packet manipulation), and steganographic techniques.
- Understand how cryptography and digital signatures address security concepts including confidentiality, integrity, authentication, non-repudiation, and access control.
- Define PKI (Public Key Infrastructure) including certificates (e.g., policies, practice statements), revocation, and trust models.

Module 4. Intrusion and Intrusion Detection Systems Part I

Computing systems around the world have many different types of security measures in place to deal with the threat of cyberattacks. In this module, you will learn about different types of digital certificates. We'll discover how they help network systems validate entities as trusted entities and keep out potential malicious users. You will also learn about the different types of intruders and hackers and understand the logic behind how intrusions occur. You will learn the basics of intrusion detection systems and how they work behind the scenes to detect and stop intrusions.

***Learning Objectives*:** In this module, students will:

- Describe the role of a Certificate Authority (CA) as well as Registration Authority (RA) and its relevance to security certificates.
- Describe the events that make up the lifecycle of a certificate and how root certificate distribution works.
- Compare and contrast SSL/TSL X.509-compliant certificates with PGP-compliant certificates.
- Define intrusion and describe the classes of intruders (i.e., masquerader, misfeasor, clandestine user).
- Describe what is meant by a hacker and discuss their role in cybersecurity as well as compare and contrast the "black hat" and "white hat" hacker cultures (i.e., computer criminal versus computer security expert).
- Describe intrusion and user behavior, the three logical components that comprise an IDS (i.e., sensors, analyzers, user interface), and describe the essential requirements for any IDS.
- Describe anomaly detection, specifically threshold and profile-based approaches as well as the types of audit records employed in intrusion detection (i.e., native, detection-specific).

Module 5. Intrusion and Intrusion Detection Systems Part II

In this module, you will learn all about different types of intrusion detection and prevention systems. You will learn how IDS sensors are placed strategically in network systems. You will also learn about the key differences between an IDS and IPS and learn about some of the most widely-used intrusion detection systems on the market.

***Learning Objectives*:** In this module, students will:

- Describe signature detection, specifically rule-based anomaly, and penetration identification approaches.
- Describe the primary approach for network-based intrusion detection.

- Compare and contrast inline and passive sensors and discuss typical placement of sensors in a network-based IDS environment as well as describe the operation, typical activities, and outputs of an intrusion detection system.
- Describe some of the limitations of intrusion detection systems and differentiate between an intrusion detection system (passive) and an intrusion prevention (reactive) system.
- Compare and contrast several of the intrusion detection systems available on the current market.

Module 6. Intrusion Prevention

In the last few modules, you learned all about intrusion detection systems and how they are used to detect network intrusions. In this module, we'll look at intrusion prevention systems (IPS) and how they are used to monitor and detect port scans. You'll learn about how firewalls and honeypots are used as techniques to prevent intrusions. You will also learn about ACLs and virtual operating systems.

***Learning Objectives*:** In this module, students will:

- Describe the process of monitoring/detecting port scanning attacks and associated patterns and explain how the monitoring and analysis of network traffic can be used to detect intrusion.
- Describe the purpose and limitations of firewalls and the four types of firewalls (i.e., packet filtering, stateful inspection, application-level gateway, circuit-level gateway) as well as VLAN and other basic network isolation techniques.
- Describe the use of honeypots as an intrusion prevention technique and explain how security policies are used to prevent intruders.
- Explain how Access Control Lists (ACLs) are used to prevent intrusion and describe the limitations of traffic monitoring within virtual networks.
- Discuss the primary vulnerability of virtual operating systems and describe the "hypervisor" and explain its role in securing a virtual environment.

Module 7. Social Engineering and Fundamental Security Design Principles

Social engineering is a fast-growing cause for concern in the world of cybercrime. In this module, you will learn about social engineering and how it exploits the human element. You will also learn about some of the fundamental security design principles. These principles are the basis for the development of all of the security solutions that are available in the market today.

***Learning Objectives*:** In this module, students will:

- Define social engineering and describe its role in cybersecurity and discuss common mechanisms that constitute social engineering (e.g., phishing, baiting, quid pro quo, pretexting)
- Describe the variety of attacks targeting the human element and countermeasures that can be used to counter social engineering attacks as well as discuss the three over-arching security design principles (i.e., only necessary, simple, ease of use).
- Describe the following principles.
    - principle of least privilege as it relates to computer security.
    - principle of separation of duties as it relates to computer security.
    - principle of defense-in-depth as it relates to computer security.
    - principle of fail-secure or fail-safe as it relates to computer security.
    - principle of economy of mechanism as it relates to computer security.
    - principle of complete mediation as it relates to computer security.
- Describe the following principles.
    - principle of open design as it relates to computer security.
    - principle of least common mechanism as it relates to computer security.
    - principle of psychological acceptability as it relates to computer security.
    - principle of leveraging existing components as it relates to computer security.
    - principle of weakest link as it relates to computer security.
    - principle of a single point of failure as it relates to computer security.

Module 8. Careers in Cybersecurity

In this module, we will discuss how the concepts of cybersecurity are applied to create safety rules and regulations in organizations. You will learn about tangible action you can take in case of cyber attack incidents. You will also learn about the different hats and teams that are created as part of defensive security teams. Finally, we will discuss the career opportunities available in various cybersecurity avenues like penetration testing, DFIR, and more.

***Learning Objectives*:** In this module, students will:

- Describe personal and jobsite safety rules and regulations that maintain safe and healthy work environments.
- Explain emergency procedures to follow in response to workplace accidents.
- Understand Hats and Teams terminology as it relates to careers in cybersecurity.
- Explain Blue Team – day-to-day defensive security and DFIR – Blue Team's First Responders as it relates to careers in cybersecurity.
- Understand Penetration Testing – hacking for security as it relates to careers in cybersecurity.
- Compare and contrast social engineering, creating a good security policy as it relates to careers in cybersecurity.