Network Security Fundamentals 1B: Forensics and Permissions

As the world becomes increasingly more interconnected by technology, computer and mobile-based crimes are becoming more prevalent. Explore cyber forensics, encryption, cryptography and cryptology, user and password management to mitigate large data breaches, and other threats, vulnerabilities, and security issues. Discover what it takes to enter this high-demand career field. As a cybersecurity specialist, you'll never get bored with trying to keep individuals and organizations safe!

Companion courses are listed at the bottom.

Unit 1: Computer and Digital Forensics

Computer and digital forensics is an exciting and emerging field in forensic science. As the world becomes more digitally dependent, it's only natural there would be an increase in computer-based crimes and a corresponding need to solve them because individuals and organizations alike are negatively impacted by computer crimes. As a result, law enforcement has become modernized by adding digital forensic experts or partnering with them to aid in the collection of evidence in hopes of identifying those responsible for computer crimes.

What will you learn in this unit?

1. Define computer and digital forensics
2. Summarize the four steps involved in the forensics process
3. Identify when a computer forensics investigation is needed
4. Explain forensics procedures for the collection of digital evidence
5. Describe open-source digital forensic tools

Unit 2: Cryptology and Cryptography

This unit will dive into the complexities of how data and communications are encrypted. There is a long history of employing creative methodologies to keep communications safe. From 400 BCE until today, significant advances have been made in breaking codes to gain access to information. So, while this is a complicated topic, it is critically important to the profession and the overall strategy for network security.

What will you learn in this unit?

1. Define cryptography and cryptology
2. Understand storage and transport encryption
3. Recognize digital certificates and signatures
4. Describe hashing and encryption algorithms
5. Determine what protocols and methodologies are deployed on your system

Unit 3: Operating System Administration

Every device that is connected to a network or the internet runs an operating system (OS). The OS provides the interface between the human operator and the computing hardware. Operating system administration requires talented individuals who understand OS software, hardware, the network, and human operators in order to make the overall network function smoothly. Each OS has its own personality, requirements, benefits, and frustrations. In this unit, we will explore the role of systems administrators and their challenges as well as the best practices that should be followed while managing different operating systems and devices.

What will you learn in this unit?

1. Explain basic principles of operating system administration
2. Understand the role of a systems administrator
3. Recognize the differences between services and applications
4. Identify log files and their significance
5. Contrast the benefits and risks of virtualization

Unit 4: Managing Users and Permissions

In this unit, we will examine how to deploy the first line of defense for our users and systems: passwords. They sound simple, but there is more to them than meets the eye, and vulnerabilities lurk everywhere. We will also examine and develop a process to manage a network's users and discuss how to grant the permissions they need in order to complete their jobs. Through a process of continuous monitoring, the sysadmin team will be on the lookout for anomalies in the network to detect any compromises of user accounts that could lead to a larger data breach. We will cover all aspects of managing users to keep our systems secure.

What will you learn in this unit?

1. Create best practices for password policies
2. Understand share and file permissions
3. Demonstrate how inheritance works in file systems
4. Identify different types of password attacks
5. Explain how the principle of least privilege helps systems administration

Unit 5: Application Security

The application layer (layer 7) of the OSI is where users spend much of their time completing daily tasks and using different application (software) packages. Those tasks could include anything from running monthly payroll to ordering lunch online. Because of this, each application in your environment needs to be understood and evaluated for possible vulnerabilities. In this unit, we will take a deep dive into how to accomplish that analysis. And, of course, when talking about application security, we cannot ignore the users. It sounds accusatory, but they are the weakest link in our security framework. Users like to click on things before thinking, so do not forget to provide frequent security awareness training to your users!

What will you learn in this unit?

1. Explain why application security is critical to an overall security strategy
2. Identify and describe various types of application security attacks
3. Understand the guiding principles of social engineering
4. Recognize web application attacks
5. Defend against attacks targeting the application layer

Unit 6: Mobile Threats and Security

Mobile devices play vital roles in our everyday lives and allow us to access the internet. Some of us would become very anxious if we had to give up our smart devices even for a few hours. We use them to shop, work, entertain ourselves, communicate, and create. Because of this and the other ways we interact with our devices, they contain tremendous amounts of information about us and our lives. Being treasure troves of personal information, mobile devices have naturally become prime targets for hackers. In this unit, we will examine

some common mobile device threats and vulnerabilities as well as mitigation strategies we can employ to keep our data safe. After completing this unit, you will be able to secure your mobile device against common threats.

What will you learn in this unit?

1. Define mobile security and its importance
2. Identify common mobile security settings
3. Understand mobile app threats
4. Explain mobile threat mitigation strategies

Unit 7: Current Events in Cybersecurity

If you ever meet someone who says they know everything there is to know about cybersecurity, you can rest assured that they're wrong. With each new day, there are so many new events, laws, regulations, threats, applications, or solutions released that there is no possible way to be aware of everything that is happening. In this unit, we will explore several areas of cybersecurity that are undergoing tremendous change. Some areas may be uncomfortable to think about and challenge your personal beliefs. While you won't be aware of every current event when you complete this unit, you will be equipped with trusted sources of information that will aid you in attempting to keep up with the changes.

What will you learn in this unit?

1. Identify trusted sources of information for current events
2. Understand challenges in achieving and maintaining computer security
3. Recognize the benefits and dangers of social media platforms
4. Describe critical infrastructure that needs to be protected from cyberattacks
5. Explain ethical and privacy issues in cybersecurity

Unit 8: Careers and Education in Cybersecurity

"What do you want to be when you grow up?" At this point in your life, you may well be tired of answering this question. Maybe you responded in the past by saying you wanted to be a doctor, lawyer, journalist, or professional athlete, but after this lesson, perhaps your response will be cyber professional! The world is changing, after all. High schools and colleges are ramping up their offerings for technology education in response to the emerging needs of the workforce. At the same time, large companies are sponsoring cyber competitions to train youth and search for qualified professionals in the cyber field. The cybersecurity industry has a global shortage of four million qualified professionals. In short, we need you. Now is the time to start thinking about your career plan and the steps that you can take to position yourself for a rewarding career that will always challenge you—and that you will never find boring!

What will you learn in this unit?

1. Understand the reasons for the cyber talent shortage
2. Recognize viable career paths
3. Identify available educational opportunities
4. Describe items to include on your resume and in your portfolio
5. Establish a plan to pursue a career in the cyber field

Companion courses:

Cybersecurity

Intro to Networking

Principles of Networking Technology