Network Security Fundamentals 1A: Introduction

Have you seen news headlines about cyber data breaches or hacks? With so many businesses working hard to ensure that their data and their customers' information stay safe and secure, it's no wonder that careers in cybersecurity are in high demand. Learn what information security is, hackers, viruses, spyware, network systems, identifying potential vulnerabilities, protecting against attacks, and creating a disaster and response plan if breaches do occur. Could you be the security specialist that stops the next cyberattack?

Unit 1: Security (and What Threatens It)

Sometimes, it seems like you can't go a day without hearing news about a data breach, computer intrusion, or some technology that a friend promises will change your life. Technology and connected devices definitely make society and our lives more productive and interesting! And yet, along with the good of every tool comes unintended consequences. Have you ever stopped to think about how all of our connected devices work? Have you ever thought about how much of your personal data has been recorded and where that information is stored? Over the duration of the course, we will dive into all of these issues and, most importantly, discuss how they function. Providing cybersecurity for modern-day networks is a challenge and a critical skill that will form the focus of our study in this course.

What will you learn in this unit?

- Define and gain an understanding of information security
- Examine threats, vulnerabilities, and exploits and how they can be used by attackers
- Explain how to build a layered defense for an organization
- Investigate the types of controls used in the implementation of a security strategy
- Discuss how data breaches occur and what their impacts are on organizations, organizational partners, and customers

Unit 2: Fundamental Concepts of Cybersecurity

Without a solid foundation, a building will not stand for long or withstand significant weather events. Cybersecurity is very similar—without a solid foundation, our cybersecurity fails. A failure of either foundation could lead to a catastrophic event. Solid foundations result in an understanding of fundamental concepts, research, planning, implementation, and review. Throughout this unit, we will examine fundamental cybersecurity concepts and learn about frameworks that help us build the foundation required to secure our networks. We will also examine the federal agencies that help guide frameworks and policies for cybersecurity. This unit will open your mind to other aspects of cybersecurity that you may want to research as you continue through the course.

What will you learn in this unit?

- Identify agencies that provide advice about cybersecurity policy and frameworks
- Provide a detailed explanation of the CIA triad
- Explain the differences between disaster planning and incident response planning
- Assess the major goals of a network disaster recovery plan and an incident response plan

Unit 3: Building a Network

Now that we have gained some insight into security goals and the terminology used to describe them, we can turn our attention to understanding the infrastructure that powers a business and connects it to the internet. You will come across many new terms and standards in this unit. Returning here as you proceed through the course

will help you clarify other terms and concepts that you encounter. And, after studying this unit, don't be surprised if you feel encouraged to conduct further research into networking components. Networks are complicated things; if they were easy, cybersecurity wouldn't be a challenge. This unit's introduction to networking equipment builds the foundation upon which we'll add security later in the course.

What will you learn in this unit?

- Describe differences among the internet, intranets, and extranets
- Understand the components of basic network equipment and their functions
- Explain various network topologies
- Compare different types of firewalls and how they protect networks
- Identify the type of NetFlow data that can assist in improving a network

Unit 4: Protocols, Services, and Data Transfer

Everything you have learned so far has set the stage for us to talk about how the Transmission Control Protocol/Internet Protocol (TCP/IP) moves data around a network. At times, this protocol may seem like a complicated maze of protocols, ports, subnets, and services. In this unit, we will introduce firewall rules and troubleshooting commands. We have a full menu of items to get through. Do you remember the OSI model? It will surely remain our guiding light and will be referred to many times in this unit. Don't feel discouraged if you need to read through the content a few times for it to come together for you. It is difficult material, so the troubleshooting tools, tips, and tricks in this unit are designed to help you gain some hands-on experience with the content. If you love acronyms, this is the unit for you!

What will you learn in this unit?

- Explain the difference between IPv4 and IPv6 address spaces and why they both exist
- Distinguish the IPv4 subnet classifications
- Understand the common ports as defined by IANA
- Describe the different types of NAT and when to apply them
- Demonstrate the use of client-based network troubleshooting tools
- Identify the correct network tools to use in Windows and Linux

Network Security Fundamentals 1a Midterm Exam

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from the first half of the course (Note: You will be able to open this exam only one time.)

Unit 5: Building Our Defenses

We connect our devices to different networks every day, and often, these are wireless networks. Do we take for granted that these networks are secure and confidential? By the end of this unit, you will be able to recognize and identify the type and strength of the security that a network provides. You will be able to recognize various types of network attacks and, hopefully, how to prevent them from ever happening. This unit will also give you an opportunity to walk through a real-life cyberattack and put you on the front line to provide you with a sense of what network security professionals encounter on a daily basis.

What will you learn in this unit?

- Define the basic network elements to secure

- Describe various wireless protection measures
- Recognize various network attack types
- Identify the steps that can be taken to mitigate network attacks

Unit 6: When the Intruders Are at the Door

Networks are under attack every day. Sometimes, defenders know they are under attack, but an attack can also be silent. In this unit, you will see who the key players are in the struggle to keep networks secure and data safe. You will also learn about defensive measures that should be deployed as part of effective security strategy. Along the way, we will discuss the legal environment in which this all plays out as well as the responsibility that comes with being a security professional!

What will you learn in this unit?

- Identify three types of hackers
- Differentiate between active and passive cyberattacks
- Understand the differences between intrusion detection systems and intrusion prevention systems as well as when to deploy them
- Explain how defense tactics and countermeasures differ
- Judge whether network penetration testing is legal or illegal

Unit 7: A Closer Look at Malware

In your online experience, you've likely seen pop-up advertisements and spam emails or landed on a website that looked questionable to you. Pretty much all homes and organizations have devices connected to their networks, and these represent just a part of the total attack surface. In this unit, we will focus on the systems that you connect to networks as well as the types of malware and viruses that target, infect, and cripple those systems. We will also examine ways to mitigate the overall dangers that malicious software poses to systems. Lastly, we will consider the motivations of those who create malware and look at a few infamous examples from recent history.

What will you learn in this unit?

- Explain what malware is
- Identify differences between malware and viruses
- Understand how malicious software spreads
- Compare measures taken to defend against malware
- Assess the impact of past malware attacks

Unit 8: Security Design Principles

At this stage, it should be clear that many aspects of network security involve technical expertise, but in addition to the technical skills required to secure your data, there is a set of complementary guiding principles that you will learn to apply. These principles inform the design of an information security plan and will prove instructive to you in the application of all aspects of information security. We will also examine policies that have been published by government agencies with the goal of providing a framework for all organizations to build their own robust information security plans.

What will you learn in this unit?

- Identify and define security design principles

- Describe controls that should be part of a security design plan
- Explain various authentication methods
- Understand the balance between the need for strong security and user access

Network Security Fundamentals 1a Exam

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from the second half of the course (Note: You will be able to open this exam only one time.)