Learning Guide Unit 2

Site: University of the People
Course: CS 3340-01 Systems and Application Security - AY2025-T1
Book: Learning Guide Unit 2

Printed by: Mejbaul Mubin
Date: Thursday, 5 September 2024, 2:36 PM

Description

Learning Guide Unit 2

Table of contents

Overview

UNIT 2: Cybersecurity Attacks and Countermeasures

Topics

- Introduction
- Cyber-security attacks and countermeasures
- Social engineering – attacks and countermeasure
- Wireless Attacks and Countermeasures

Learning Objectives

By the end of this Unit, you will be able to:

1. Explain cyber-security attacks and countermeasures based on research.
2. Evaluate cyber threats, their level of destruction, and recovery possibilities.
3. Create a scenario about a cyberattack on a QR code user.

Tasks

- Peer assess Unit 1 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz

Introduction

It is very hard to design a “perfect computer system” that is resilient to any cyber threats. Thomas (2020, September 9) points that “The common types of vulnerabilities are errors in the design or configuration of network infrastructure, protocols, communication media, operating systems, web-based applications and services, databases, etc.”

Understanding how to discover cyber threats that target specific vulnerabilities of computer systems is crucial to the business sustainability and availability of network resources and services to the users. It is important to understand the differences between “exploits” and “attacks”. Exploits use the computer system’s vulnerabilities to damage the system and/or get access to a piece of valuable confidential information. Attacks can be physical or nonphysical. The cybersecurity domain focuses on nonphysical attacks that are delivered via computer networks and web applications.

In this unit, students will discuss and explore various types of cyber-security vulnerabilities and attacks, as well as countermeasures recommended by industry professionals.

Reference:

Thomas, C., Fraga-Lamas, P., Fernandez-Carames, T. M. (2020). *Introductory chapter: computer security threats*. Intechopen.com. https://www.intechopen.com/chapters/72730

Cybersecurity attacks and countermeasures

A cyber-attack is a coordinated action conducted by cybercriminals using one or more digital devices (i.e. computers, smartphones, etc.) against other digital devices (i.e. computers, smartphones, etc.) and/or computer networks. A cyber-attack can be used to damage computer systems, digital devices, steal data, and/or have other malicious goals.

Cybersecurity countermeasures are designed to prevent and detect cyberattacks and mitigate the damage resulting from cyber-attacks.

Malware is software (a computer program) that has been designed for malicious intentions. The malicious intention includes, but is not limited to corrupting a computer's operating system, stealing data, demanding ransom, spy on users, businesses, and governments.

The most common types of malware are worms, viruses, botnets (bots), Trojans, spyware, adware, rootkits, key loggers, and ransomware.

Reading Assignments:

Read:

- Top 10 Most Common Types of Cyber Attacks
- The 11 most common types of malware

Watch:

- 8 Most Common Cybersecurity Threats | Types of Cyber Attacks | Cybersecurity for Beginners
- Malware: Difference Between Computer Viruses, Worms and Trojans .

Resources:

Barker, K. (2021, August 19). *The 11 most common types of malware*. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Edureka! (2018, July 18). *8 Most common cybersecurity threats | types of cyber attacks | cybersecurity for beginners | edureka* [Video]. YouTube. https://www.youtube.com/watch?v=Dk-ZqQ-bfy4

Kaspersky. (2016, March 21). *Malware: Difference between computer viruses, worms and Trojans* [Video]. YouTube. https://www.youtube.com/watch?v=n8mbzU0X2nQ

Melnick, J. (2021, May 18). *Top 10 most common types of cyber attacks* [Blog]. Netwrix. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

MalwareFox. (2020, February 25). *Different types of malware explained | how does anti-malware detects them?* [Video]. YouTube. https://www.youtube.com/watch?v=JZOLa7_LShk

Social engineering - attacks and countermeasure A

A social engineering attack is a course of deceptive actions aimed at a person to obtain access to valuable data (i.e. personal data) and/or resources, and/or run a fraud.

Reading Assignments:

Read: Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model

Watch: Watch Out! 5 Most Common Social Engineering Attacks

Resources:

Airehrour, D., Nair, N.V., & Madanian, S. (2018, May 3). *Social engineering attacks and countermeasures in the new zealand banking system: advancing a user-reflective mitigation model*. MDPI. https://www.mdpi.com/2078-2489/9/5/110

Demakis Technologies. (2021, March 6). *Watch out! 5 most common social engineering attacks* [Video]. YouTube. https://www.youtube.com/watch?v=j5j6c05Btfc

MalwareFox. (2020, October 20). *What is social engineering in cyber security? Explained* [Video]. YouTube. https://www.youtube.com/watch?v=v7VTJhkJUUY

Wireless attacks and countermeasures

The use of wireless devices is increasing both for personal needs and business. Thus, it is imperative to be aware of cybersecurity risks associated with wireless attacks.

Some of the countermeasures are using VPN at all times, turning OFF the Bluetooth feature when not using it, and being careful when you use clicks as a confirmation of any unsolicited requests.

Cyber-attacks can be delivered to both devices connected to the computer network using network communication cables or wirelessly. Wireless connection is provided via wireless networks such as cellular phones, wireless sensor networks, satellite communication, radio waves, and microwave networks. Cyberattacks delivered via wireless networks are called wireless attacks.

The most commonly known wireless attacks include but are not limited to the rogue access point, jamming of legitimate wireless signals, evil tween, bluejacking, and/or bluesnarfing.

Reading Assignments:

Read: Wireless attacks and its types

Resources:

Alpine Security. (2017, December 3). *Wireless attacks explained* [Video]. YouTube. https://www.youtube.com/watch?v=D4RStq3wcNI

Wireless attacks and its types. (n.d.). ExamCollection. https://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html

Reading Assignment

1. Airehrour, D., Nair, N.V., & Madanian, S. (2018, May 3). *Social engineering attacks and countermeasures in the new zealand banking system: advancing a user-reflective mitigation model*. MDPI. **https://www.mdpi.com/2078-2489/9/5/110**
2. Barker, K. (2021, August 19). *The 11 most common types of malware*. **https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/**
3. Melnick, J. (2021, May 18). *Top 10 most common types of cyber attacks* [Blog]. Netwrix. **https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/**
4. Thomas, C., Fraga-Lamas, P., Fernandez-Carames, T. M. (2020). *Introductory chapter: computer security threats*. Intechopen.com. **https://www.intechopen.com/chapters/72730**
5. *Wireless attacks and its types.* (n.d.). ExamCollection. **https://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html**

Video Resources

1. Alpine Security. (2017, December 3). *Wireless attacks explained* [Video]. YouTube. **https://www.youtube.com/watch?v=D4RStq3wcNI**
2. Demakis Technologies. (2021, March 6). *Watch out! 5 most common social engineering attacks* [Video]. YouTube. **https://www.youtube.com/watch?v=j5j6c05Btfc**
3. Edureka! (2018, July 18). *8 Most common cybersecurity threats | types of cyber attacks | cybersecurity for beginners | edureka* [Video]. YouTube. **https://www.youtube.com/watch?v=Dk-ZqQ-bfy4**
4. Kaspersky. (2016, March 21). *Malware: Difference between computer viruses, worms and Trojans* [Video]. YouTube. **https://www.youtube.com/watch?v=n8mbzU0X2nQ**
5. MalwareFox. (2020, February 25). *Different types of malware explained | how does anti-malware detects them?* [Video]. YouTube. **https://www.youtube.com/watch?v=JZOLa7_LShk**
6. MalwareFox. (2020, October 20). *What is social engineering in cyber security? Explained* [Video]. YouTube. **https://www.youtube.com/watch?v=v7VTJhkJUUY**

Discussion Assignment

For this discussion, select a type of vulnerability. Conduct research on vulnerability and respond to the following:

- Discuss how vulnerability impacts computer systems.
- Describe the reasons behind that vulnerability.
- Explain the countermeasures that can be effectively used to mitigate or prevent major damages caused by that vulnerability.

You can use the following cybersecurity website to search for reported vulnerabilities and countermeasures:

Latest cybersecurity vulnerability news. (2021). *The Daily Swig*. Retrieved January 06, 2022, from https://portswigger.net/daily-swig/vulnerabilities

Your Discussion should be a minimum of 200 words in length and not more than 500 words. Please include a word count. Following the APA standard, use references and in-text citations for the textbook and any other sources.

Written Assignment

Submit a paper that is 2-3 pages in length exclusive of the reference page, double-spaced using 12-point Times New Roman font. The paper must cite at least two (2) outside sources in APA format and be well-written. Check all content for grammar, spelling and be sure that you have correctly cited all resources (in APA format) used. Refer to the UoPeople APA Tutorials in the LRC for help with APA citations.

A QR code is an image-type barcode that can be read by a digital device. It allows access to the product and service information. Some mobile devices and smartphones have a built-in capability to read and interpret QR codes. QR codes are very popular because they enable a lot of different remote tasks and data access.

For this assignment, it is recommended you conduct independent, online research on QR code attacks. In case you are not sure where to start, try to review the following online articles:

- Qrlijacking
- How attackers exploit QR codes and how to mitigate the risk

1. Describe a scenario where the attacker abuses the bar code to commit a cybercrime, such as stealing a bank account.
2. Identify a vulnerability that enabled this attack, explain its mechanism.
3. Provide a solution to defeat such an attack.
4. Support your scenario analysis and solution proposal with external references (appropriate research).
5. Use APA style for a list of references and in-text citations.

References

OWASAP Foundation. (2021). *Qrlijacking*. https://owasp.org/www-community/attacks/Qrljacking#

Violino, B. (2020, October 19). *How attackers exploit QR codes and how to mitigate the risk*. CSO India. https://www.csoonline.com/article/3584773/how-attackers-exploit-qr-codes-and-how-to-mitigate-the-risk.html

Written Assignment Peer Assessment

In the unit following the submission of your written assignment, you will peer assess three (3) of your classmates' assignments according to the instructions found in the Assessment Form. During this peer assessment period, you are expected to provide details in the feedback section of the Assessment Form, indicating why you awarded the grade that you did to your peer. The written assignment grade is comprised of a combination of your submission (90%) and your peer assessments (10%).

Written Assignment Peer Assessment Rubric

Learning Journal

The Learning Journal is a tool for self-reflection on the learning process. In addition to completing directed tasks, you should use the Learning Journal to document your activities, record problems you may have encountered, and draft answers for Discussion Forums and Assignments. The Learning Journal should be updated regularly (weekly), as your instructor will assess the learning journals as part of your Final Grade.

In this unit, we learned about various types of cyber threats and how to mitigate or prevent them from damaging your computer networks and data. To reflect on what you have learned, answer each of the following questions:

- Describe what was the most interesting topic you learned about in this unit. Think about reasons why you noticed this topic, your impression, your plans for further exploration of that topic.
- Describe a cyberattack experience that happened to you, someone you know, or a business you are familiar with. Describe the type of cybersecurity issue, the way it was discovered, and steps taken to recover and/or prevent this cybersecurity issue from happening again.

The Learning Journal entry should be a minimum of 500 words and not more than 750 words. Use APA citations and references if you use ideas from the readings or other sources

Refer Learning Journal Rubrics

Self-Quiz

The Self-Quiz gives you an opportunity to self-assess your knowledge of what you have learned so far.

The results of the Self-Quiz do not count towards your final grade. However,the quiz is an important part of the University's learning process and it is expected that you will take it to ensure understanding of the materials presented. Reviewing and analyzing your results will help you perform better on future Graded Quizzes and the Final Exam.

Please access the Self-Quiz on the main course homepage; it is listed inside the Unit.

Checklist

- Peer assess Unit 1 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz