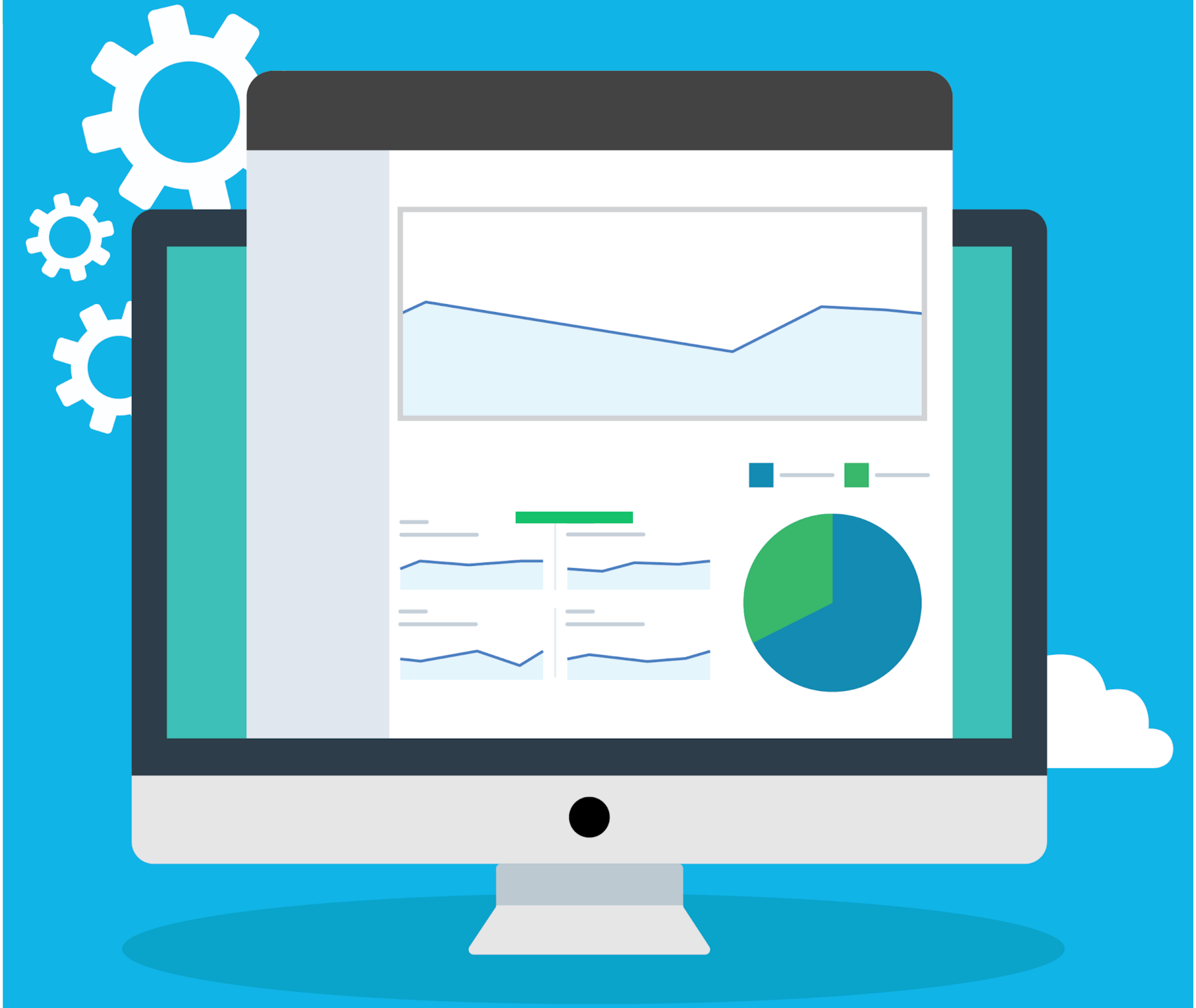
UDACITY

Cybersecurity Foundations



Securing a Computer System

Securing a Computer System

أشبال مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Congratulations!

You have been hired to audit the security for the PC used at your friend’s business: Joe's Auto Body. Joe provides car repair services throughout the tri-state area. He's had previous employees use it for activities unrelated to work (e.g., web browsing, personal email, social media, games, etc.), and he now uses it to store his critical business information. He suspects that others may have broken into it and could be using it to transfer files across the internet. He has asked that you secure it for him according to industry best practices so that it can again be used as a standard PC.

In this project, you have been given a “broken” Windows 10 PC and asked to figure out what’s wrong with it and then make changes to fix and secure it. The process of analyzing and applying security happens in workplaces around the globe and is exactly what cybersecurity professionals do daily. This project allows you to apply what you’ve learned in the course by investigating a Windows 10 PC. The same skills you use on one PC can be applied to thousands.

You do not need to do anything on this slide.

Part 1: Reconnaissance

Hardware

The first step in securing any system is to know what it is, what’s on it, what it’s used for, and who uses it. That’s the concept of systems reconnaissance and asset inventory. In this step, you’ll document the hardware, software, user access, system and security services on the PC. Complete each section below.

1	*Device Name*	JoesGaragePC
2	*Processor*	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz 2.59 GHz
3	*Install RAM*	4.00 GB
4	*System Type*	64-bit operating system, x64-based processor
5	*Windows Edition*	Windows 10 Pro
6	*Version*	22H2
7	*Installed on*	11/23/2021
8	*OS build*	19045.2486

Software

Another common early step in securing is taking an inventory of software or applications installed on a computer system. These are programs outside of the standard operating system. Please list five applications running on this PC.

1	7-Zip 19.00(x64)
2	Adobe Reader XI (11.0.01)
3	Candy Crush Friends
4	Google Chrome
5	VLC media player

Accounts

As part of your security assessment, you should know the user accounts that may access the PC. Please list the accounts, name, and access level for the accounts on this PC.

Account Name	*Full Name*	*Access Level*
Frank	Frank	Local User
Guest		Local User
Hacker	A Hacker	Administrator Remote User
JaneS	Jane Smith	Administrator Remote User
JoesAuto	Joes Account	Administrator
Notadmin	Do Not Use	Remote User

Security Services

Document the PC’s security settings status listed below.

	Security Feature	*Status*
	Firewall product and status--Private network	Disabled
	Firewall product and status--Public network	Enabled
	Virus protection product and status	Not secure from Ransomware Attacks
	Internet Security messages	Repudiation-based Protection
	Network firewall messages	Firewall is using Settings that makes the device unsafe
	Virus protection messages	No action needed except for ransomware protection
	User Account Control Setting	Set to :Never notify , not recommended

Part 2: Assessment

Authentication

Consider the 3 factors of authentication: something you KNOW, something you HAVE, and something you ARE. In 1 to 3 sentences below, suggest and explain what type of authentication would be appropriate for JoesPC.

1. Something you KNOW is like a password or a Passphrase That Joe is the only one knows it.
2. Something you HAVE is like a physical token or a mobile authenticator.
3. Something you ARE may be a fingerprint or a facial recognition integrated with the hardware of his laptop.

System and Security: Firewall

Please answer the following question.

1 *In 1 to 2 sentences, explain what protection would enabling the Windows Firewall provide.*

It Helps in controlling the Apps that can communicate over the network, and helps to prevent network attacks.

System and Security: Firewall

Scenario: You need to ensure the Windows Defender anti-virus is enabled to always protect against current threats. It should be set to continually scan the PC for malicious software automatically. Please answer the following question.

1 *In 1 to 2 sentences, explain what protection enabling the Microsoft Defender Antivirus would provide.*

By enabling the Microsoft Defender Antivirus it would provide malware detection and removal of them and and also providing real time protection.

Part 3: Securing Access

Users - Part 1

Ensuring only specific people have access to a computer is a common step in information security. It starts by understanding who should have access and the rules or policies that should be followed. Please review the following users who should have access.

- JoesAuto
- Jane Smith (Joe’s Assistant)

It is your responsibility to create suggestions for securing this computer. Use the next slide to give and explain your recommendations. The slide following your recommendations will have two questions regarding users and privileges.

Users - Part 2

Fill in this table based on the guidelines you would recommend to Joe. Recommendations do not have to be in complete sentences. Explanations must be at least one sentence.		
	Recommendation	*Explanation*
How should users authenticate their identity?	By using 2-Factor Authentication	To ensure that there is no Information disclosure and apply non-Repudiation Concept
What Access Rights/Permissions should Joe have?	Joe Should Have the Administrator Rights	As he should be Able to control the data usage for other users and control security controls
What Access Rights/Permissions should Jane have?	Organization or Normal user account	To have less access to confidential data and be able to access only data that he should and apply least privilege

Users- Part 3

Please answer the following two questions.	
1	*In 1 to 2 sentences, explain why it is important to disable or remove unneeded accounts from a PC or application.* *To apply Security controls and apply Non-Repudiation,* *And disable access for who are not intended to access the PC*
2	*Administrator privileges for too many users is a security challenge. Provide at least 3 risks associated with users having administrator rights on a PC.* *1.Unauthorized System configuration* *2.Tampering* *3.Data Breach*

Part 4: Securing Applications

Unnecessary Applications

Joe wants everyone to use the latest version of the Internet Explorer browser by default. There should be no games or non-work-related applications installed or downloaded. Joe is also concerned that there are “hacking” programs downloaded or installed on the PC that should be removed. This PC is used for standard office functions.	
1	*List three applications that violate this policy.* 1.Candy Crush Friends 2.Farm Heroes Saga 3.MusicBee
2	*Name three vulnerabilities, threats, or risks to having unnecessary applications.* 1.Attack Surface Increase 2.Application Attack Vulnerabilities 3.System Protection complexity increase

Patching and Updates

All applications should be up-to-date on patches or fixes by the manufacturer. Any old version of software should be uninstalled. List two applications on JoesPC that are out of date.	
1	Google Chrome
2	VLC media player

Standout Suggestions

Standout Suggestion 1

Joe has decided to allow least privilege access to 2 additional employees. He would like the bookkeeper and the head mechanic to have access to JoesPC. In 3 - 5 sentences total below, describe the privileges these two employees should have, and detail how they should authenticate their identities.

1 For the Mechanic should have access to the diagnostic tools on the computer and have unique password and a token to access his account, For the Bookkeeper He would access financial records and accounting data and software and will also need a unique password and a token to access his account, Computer Admin can Make a role-based access control (RBAC) to insure least privilege

Standout Suggestion 2

Joe believes one of his employee’s emails has been compromised. What are the possible threats, risks, or vulnerabilities, and how should he respond? Detail your answer in 3 to 5 sentences.	
2	That may lead to unauthorized access , Information disclosure and data tampering and also may lead to unavailability and there is a potential of malware and phishing. To fix this he will have to insure that each account gets a new password and have Multi-Factor Authentication and check the system logs and strange behaviors on the system to make sure there is no malicious attack, he can investigate with his employees to delete the compromised account and save the other accounts and data.