UDACITY

Cybersecurity Foundations

Securing a Computer System

Securing a Computer System

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
2	Adobe Reader XI
3	Candy Crush Friends
4	Farm Heroes Saga
5	Google Chrome

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*
JoesAuto	JoesAccount	Administrator
AUser	A User	Standard
Frank	Frank	Standard
Hacker	A Hacker	Administrator
Notadmin	Do Not Use	Standard
JaneS	Jane Smith	Administrator

Security Services

Document the PC's security settings status listed below.

	Security Feature	*Status*
	Firewall product and status--Private network	Off
	Firewall product and status--Public network	On
	Virus protection product and status	Working + Updated to the latest
	Internet Security messages	N/A
	Network firewall messages	Bad (Firewall is OFF for Private networks & Domain Network)
	Virus protection messages	OK
	User Account Control Setting	Never Notify

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. *I suggest setting a PIN, Strong Password, 2FA and the other Factor would be better if it is a Facial Recognition, or a fingerprint scanner And an Encrypted USB used for Logging-in purposes for securing the PC.*

System and Security: Firewall

Please answer the following question.

1 It would Protect the Operating system (OS), and the data belonged to the user in the OS from unallowed access.

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	*It would provide a Great protection from malware, Crack Software, Keygen Tools, Viruses, And Backs up data automatically in OneDrive so you can restore it in case of a ransomware.*

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?	*They Should authenticate their identity using Fingerprints, ID Cards, Voice Recognition, USB encrypted flash drive (by a password) used for authentication, Facial Recognition.*	*They have to authenticate with those mentioned recommendations, so no one can steal the other's identity, as well as preventing impersonation.*
What Access Rights/Permissions should Joe have?	*He should have administrator Permissions.*	*As he is the owner of Joe's Garage, he should have the full rights. He should have the full access to the PC*
What Access Rights/Permissions should Jane have?	*She Should have Standard Privileges.*	*Because she is working For Joe, and some suspicious things may happen, so only least privileges apply to her.*

Users- Part 3

Please answer the following two questions.	
1	*It is important because if your remove the unneeded accounts your reduce the chances of being breached, and to manage the accessibility of accounts into PC/Apps, this also free some storage and improve the PC/App performance.*
2	*1.Reducing the Security of PC.* *2. Increase Chances of being Hacked/getting infected by a malware/ransomware.* *3.Instability of the OS.* *4.Difficulity in tracking changes made to the PC.* *5. Every single app will be installed for all users, not for a specific user.*

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.Spotify 3.Farm Heroes Saga
2	*Name three vulnerabilities, threats, or risks to having unnecessary applications.* 1.7zip 2.MusicBee 3.NpCap

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	Skype
2	Google Chrome

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 bookkeeper :* He should have the privileges to get access to e-bills (invoices), billing infos, track payments, and the money received, and access to Customer info for billing purposes. He should authenticate his identity by using password, and 2FA/MFA.

2 *For the Head Mechanic (H.M) :* He should have access to diagnostic software and repair manuals so he can fix the Cars of the customers. He also should have the permissions to order Parts and supplies online, and access customer records for service history. He should authenticate his identity by username and password, 2FA/MFA, PIN, and Biometric + Facial authentication.

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 There are a lot of threats that may happen, such as :

- unauthorized access
- Data gets stolen
- The possible spread of malware by sending emails that contains that malware
- Impersonation.

Possible Risks :

- Reputation damage
- Financial Loss

Possible Vulnerabilities :

- Weak Passwords
- Phishing Attacks

What to do :

- Change email’s password, lock with MFA
- Investigate the incident and check logs
- Update antivirus and viruses detection databases.
- Train employees on avoiding phishing + scam emails.