Solucion Laboratorio 1

Rodrigo Castillo

9 de agosto de 2020

enunciado :

Lab 1 - Cybersecurity Concepts
Write one essay of minimum 1 page ("Letter size", Font 11, Single line) in academic English where you address the following assignment:
An e-shop company with a national presence hosts its web servers on its own data center. The e-shop has been working fine until now, however, the growth in sales, due partially to the Free-taxes days, have motivated the company to migrate to the cloud considering the possible benefits: i) scalability (to support the most demanding days), ii) flexibility (to make fast deployments), iii) location (to reach new costumer) and iv)costs (Only pay for what is consumed without Cost-of-Ownership). You, a cybersecurity consultant, must define the Security Strategy that the company should implement to migrate to the cloud in a safe and functional way.
In the essay, you must include concepts you have learned in the 4 challenges studied in AWS Educate along this week: i) components of cloud computing, ii) multifactor authentication (MFA), iii) least privilege, iv) personal data privacy, v) encryption, vi) vpn, vii) https vs http, viii) digital certificate to validate identity, ix) password manager, x) integrity, xi) confidentiality, xii) availability, etc.
Use the free service of Grammarly to review and adjust your academic English before submitting the essay.

1. Basic Stuff

At first, the E-Shop must make physical backups of their information, so if they make any mistake making the transition they are not going to loose their Data. Second they have to browse for good alternatives to cloud services. As they are an E-Shop, thei'r data must be confidential, so they must include how much confidence are they able to put in thei'r cloud service client on the criteria of picking a cloud service. They also most include how scalability works in their cloud service because there are cloud services that are super cheap, but the scalability is expensive, and they also have to include the location of the cloud server service, because, for example, if they are in latin america and they offer a service in latin america, getting a service in other contintents can cause an slow service and thats not going to be worse for them. Also they have to check the state of the server in the cloud service. I think a good way for checking this is asking for free trials and checking them before paying for a cloud service.

Once they know which service are they going to pick, they will have to check that their service have minimum standarts of security. Check that every person who have contact with the service have the minimum priviledges so they can use the service but they cant abuse of it, there are many standarts of minimum priviledges principes so the company can pick it accordint to their necesities. Then they have to check that the comunication between the clients and the server is correctly cypher so there is not going to be intruders intercepting

the comunication between the users and the service. Then, they have to check that everyone who have access to the server have secure credentials. Based on how much money they have and how valuable is the data that they want to protect, and prioritizing the accounts that have more priviledges

Website must have proper encription algorithms and enought bits of RSA encription so they will be able to be secure at the eyes of the public. Also they have validate certificates so customers can get sure that the page is not being spoofed.

2. Credentials

They must have credentials based on 3 things:

1. Something that they have
2. Something that they are
3. Something that they know

2.1. Something that they have:

is about something physical that cannot be replicated easily, such as the cellphone number or a token.

2.2. Something that they are

is about physical characteristics that humans have such as the voice, the footpring, the eyes reticle ...etc . this is actually the most vulnerable characteristic because an attacker can artificially simulate many of those characteristics.

2.3. Something that they know

Something that they know is about clues that are supposed to be confidential for the people such as passwords or personal questions like the name of their pets, the favorite football player or the origin city. Actually private questions are quite vulnerable because an skilled attacker can guess those kind of questions by researching information about a targets, and passwords can be quite vulnerable too because an attacker can brute force it. so for making a secure password they will have to consider those items:

1. Password Lenght
2. Type of characters in the password
3. pronounceability of the password and relation with the owner

More longer is the password, more difficult is to brute force it , if the password have special characters, upper and lower case letters and numbers it also increase the number of possible passwords for an attacker, the company can check how secure is a password here : (https://tmedweb.tulane.edu/content_open/bfcalc.php) to check how much time would take to an attacker to break it using brute force it. Also, attackers uses tools like :

1. Cupp(common User Password Profiler (https://github.com/Mebus/cupp))
2. Wyd (Who's Your Daddy' : (https://www.darknet.org.uk/2006/11/wyd-automated-password-profiling-tool/))

3. Crunch : https://github.com/crunchsec/crunch

to create dictionaries for brute forcing passwords based on information that they know about the target. They also used dictionaries of vulnerable passwords. so a good practice for making good passwords is constantly attacking them based on information about the owner of then to check that he's not using personal information on them.

2.4. How to make secure credentials

By far, the most secure credentials for a system would be implementing those 3 things on every client, but this can be suffocating for users and also expensive, so based on minimum priviledges concept and how much priviledges have every account inside the system, the E-Shop administrators will have to decide which credential system to implement at each rung of their pyramid of privileges. Also. all of the clients should use trusted VPN services when they are on insecure networks to prevent attacks.