Assignment 1
Due date: 13th of Feb, 2023
At 11:55am

(Group of 3)

I. PART I : IDENTIFY VULNERABILITIES, THREATS, IMPACTS (35 points)

IDONTCARE is a popular company doing e-commerce. They are located in a country where government is strict in protecting personal information's. Any company which neglects its obligations of protection personal information pays a large fine which represents 30% of the turnover. System architecture is described through the figure 1.

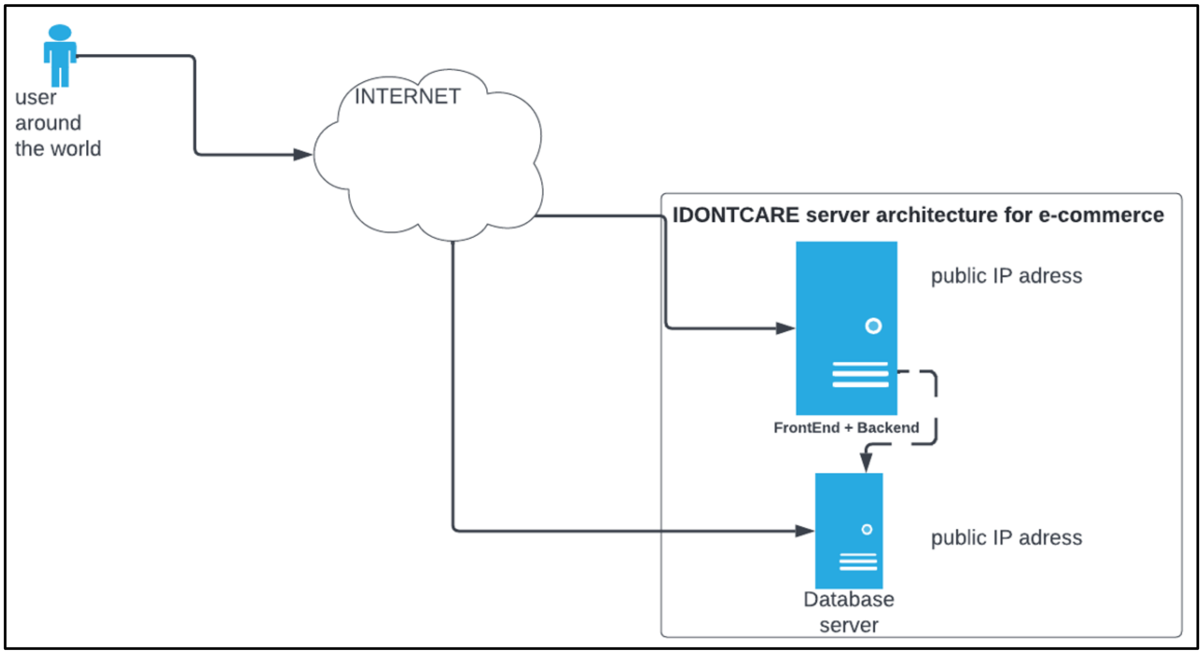

Figure 1 : IDONTCARE system architecture for e-commerce

The backend server use following:

- Operating system Redhat 6
- Backend uses Apache Struts 2.3.10 as framework

Database server is a mysql 5

Please answer the questions below:

1. **Question 1**: identify at least 4 vulnerabilities for IDONTCARE systems (2 for architectural view and 2 for non architectural view). You must explain and provide CVEs if applicable. (10 points)
2. **Question 2**: Identify 2 threats. You must explain and provide references to justify your point of view (10 points)
3. **Question 3**: Provide 2 business impact for the company concerned? (10 points)
4. **Question 4**: Provide two countermeasures to mitigate businesses impacts and threats (5 points)

II. PART II : CRYPOGRAPHY

1. Hash (30 points)

Consider the file **hashefile.txt** for the Hash exercise. For this exercise, we suggest to use **certutil**[1] tool if you are using windows or **md5sum** and **sha1sum**, **sha256sum** in Linux. You can use other tools if you desire.

For all your response, you must provide commands used and the output.

a. **Question 1**

- Provide the md5 hash of the file. (3 points)

b. **Question 2**

- Modify the file content and add just one character and provide a new md5 hash of the modified file.
- Do the output changed? Why? (3 points)

c. **Question 3**

- Provide the SHA1 of the modified file. (3 points)
- The hash is the same as which obtained in the previous question (question2) ? Why? (3 points)
- What you can conclude about the security of sha1 compared to md5? (3 points)

d. **Question 4**

- With the same modified file, provide sha256 hash. (4 points)
- Is the new hash longer or sorter ? Why? (4 points)
- What you can conclude about the security of sha256 compared to sha1? (2 points)

e. **Question 5 (5 points)**

Find 2 protocols where hashing algorithms are used and explain how algorithms are applied to secure the protocol.

2. RSA (35 points)

a. **Question 1 (10 points)**

If we choose p as 19 and q as 17, what would be the n, e and d? Show all your calculations.

b. **Question 2 (20 points)**

If we choose RSA to encrypt a message ("CMIS")

[1] https://portal.nutanix.com/page/documents/kbs/details?targetId=kA07V000000LWYqSAO

- clearly show how the message will be encrypted by using the public key (n,e) and how the decryption will work by using the private key (n,d). You need to show all the steps for encryption and decryption. (15 points)
- You need also to provide the ciphertext obtained. (5 points)

Message = CMIS
E(Message) = CypherText
D (CypherText) = Message

c. Question 3 (5 points)

Explain clearly and briefly, how RSA can defeat "man in the middle" attack. You can use the following scenario: Imagine a sender S wants to share a secret key K to the receiver R. What exactly the sender S has to send to the receiver R?