PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

May 2019: FINAL EXAM

M.TECH. 2nd SEMESTER CSE

UE18CS543 : Cyber Forensics and IoT Security

Time: 120 Mins Answer All Questions Max Marks:60

Note : Pls keep answers short and relevant. 1 Mark question – 2 or 3 words, 2 Marks question – max 1 Line, 3,4 Marks question – max 2-3 lines. Long Answers bring out non-clarity of thought process.

Q1 (12 Marks,3,2,3,2,2)

a. A disk image submitted for evidence, is altered by someone during the investigation process. Do you think this could be detected. How? (1,2)
b. Two disk images of the same disk are created using ProDiscover tool. One image is in Raw Format and another Proprietary. What do you think would be the difference in both the images? (2)
c. While capturing disk image using FTK Imager, following steps are suggested : Boot to Windows, Start FTK Imager, Create Disk Image using Physical Drive option. Do you agree with the suggested steps? If not what additional step would you suggest, why? (1,2)
d. When do you use a Sparse data copy of a disk? (2)
e. A forensic tool is able to load the image but unable to read the metadata of filesystem due to corruption. You want to know if a particular file exists in the image. What would you do? (2)

Q2 (12 Marks, 2,2,2,2,4)

a. What's the actual size of 1 byte file on disk? (2)
b. If you want to know number of free blocks in a disk, where would you get this information in windows file system? (2)
c. If you want to know Metadata of a file, where would you get this information in Linux file system? (2)
d. How does any tool get to know the type of partition (file system) in a disk? (2)
e. Increasing the complexity of a password always increases the effectiveness of the password. Do you agree with this statement? Justify your answer by bringing out what factors are important while evaluating the strength of a password scheme. (4)

Q3 (12 Marks, 3,3,4,2)

a. Meera sends an electronic request to the Bank, to Transfer Rs 10K to a Dealer's account. The request is signed with her Private key. An attacker sniffs the request on the Wire and resend's the same request three times to the Bank with some time interval in between the requests (Man in the Middle Attack). Would the bank be able to identify the Repeat Requests? If yes why do you think so? If not what would you recommend so that Bank can identify the same. (1, 2)
b. If you are downloading an executable from internet, in what way you can surely identify if the download is genuine and not infected. Why do you claim so? (3)
c. How does adding salt increase protection of password? You can store the salt in plaintext without any form of obfuscation or encryption. Do you support/ not support with reason. (2,2)
d. Retina based Biometrics Authentication is stronger than Fingerprints based Authentication. Under what condition could this statement might not turn out to be true? (2)

Q4 (12 Marks, 4,4,2,2)

a. What is the Primary reason for an XSS attack (1 line)? What solution would you suggest for the same? (2,2)
b. Give an example of Reflected and Stored XSS attack each. Suggest prevention for your example. (2,2)
c. Does my choice of DBMS have a role in protection against XSS attacks? Justify your answer. (2)
d. Explicit Error Descriptions can help in SQL Injection Attacks? Do you agree with this statement? Why? (2)

Q5 (12 Marks, 2,2,4,4)

a. I decide to re-use an open source code within my IoT application code. Suggest any two security issues which could arise from the same. (2)
b. Why do we need to look at an Attack Surface of a system (1 line)? (2)
c. Lack of Security update mechanism is considered as one of the top vulnerabilities for an IoT System. While building an IoT system, I make sure that it has security update mechanism in place. Provide any three suggestion so that security update mechanism is not vulnerable. (4)
d. List any three vulnerabilities I should take care of in IoT Device firmware. (4)