University of Sussex Autumn 2019

Introduction to Computer Security – G6077

**Weighting:** 50% of marks for the module

**Released:**

**Submission deadline:** Thursday 12th of December by 16:00 as an e-submission to Canvas

*You must work on this assignment on your own. The standard Informatics*

*rules for collusion, plagiarism and lateness apply. Any cases of potential*

*misconduct discovered will be reported and investigated.*

***Key points:***

*1) All questions must be answered. There are no optional questions.*

*2) You must have a main file as a doc file. This file will list all the tasks and reference to any associated files.*

*3) You must provide associated files. You will lose marks if full evidence is not provided for any of the tasks.*

*4) If you do not have any associated files, you must submit only the main file. If you have associated files, you must provide all the files in a folder and submit it as a compress folder. The compress folder must be named after your student number.*

*5) To ensure anonymous marking, you must NOT mention your name in the coursework, only your student number.*

*6) This coursework for the students whose surname starts from any of the characters from A to K. If a student submits a wrong coursework, it will not be accepted.*

# Part A: Principles, User authentication, Malware [20 marks]

## **Task 1**

Provide a brief but concrete explanation about the suitability or unsuitability of the following passwords.

a) cr@zyp@ss b) qwerty c ) \*laptop\_admin# d) KVK919

## **Task2**

You will need to use the DVDSwap application for this task, which is available on Canvas. There are a number of files and folders in the project.

You will need to find the part, which is required to complete the task. You are not required to fix errors to make the application run.

In the module, you have studied different issues and challenges about protecting passwords. As a junior expert in cyber security, describe and analyse the password policy used in the DVDSwap application. Suggest improvements based on your analysis. Implementation of these suggestions is not required.

Keep the answer to the point. Use bullet points to answer the question.

# Part B: Digital Forensics [20 marks]

## **Task 3**

Suppose you are working as a member of Cyber Crime, UK Police force. You received a password protected PDF file from your manager who asked you to find the password for the PDF file. He also asked that you must create your own password dictionary. Your manager have solid information that it is protected by four digits password.

PDF file is provided on Canvas. It is named as PasswordProtectedFile [A to K].

# Part C: Encryption [35 marks]

## **Task 4 [20 marks]**

Decrypt as many letters and words as you can in the cipher text listed below. You don’t need to explain, only bullet list the steps in the order that you take to decrypt this cipher-text.

Suppose you work as a junior cyber security expert in a security organisation. Your manager has forwarded you the encrypted message below and has asked you to carry out an analysis.

|  |
| --- |
| *EQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTO*  *ZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFE*  *VWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQ*  *HFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVA* |

## **Task 5 [15 marks]**

Perform the encryption and decryption using the RSA algorithm:

a) p=13; q=31, e=19; m=2

# Part D: Challenge

## **Task 6 [5 marks]**

Consider Smart Solutions Brighton Ltd is a local company, which provides IT solutions. They hired you as a cyber-security consultant. The company wants you to develop an attack tree. Smart Solutions is housed in two buildings on the same property: one building is headquarters; the other building contains network and computer services. A fence around the perimeter physically protects the property. The only entrance to the property is through a guarded front gate. The local networks are split between Headquarters’ LAN and the Network Services’ LAN. Internet users connect to the Web Server through a firewall. Dial-up users get access to a particular server on the Network Services’ LAN. Develop an attack tree in which the root node represents disclosure of proprietary secrets. Include physical, social engineering, and technical attacks. The tree may contain both AND and OR nodes. Develop a tree that has 15 leaf nodes.

## **Task 7 [14 marks]**

Develop a simple web application, which will have three features: user registration, user login and submission of CV. (4 marks)

System will allow users to create an account. Students should identify different suitable fields for registration. Users must be able to log back into the system using their passwords. The system must store passwords in the form of hash values. (3 marks)

The system must allow registered users to submit their PDF or MS Word format CV only. The system must be safe to use and must not be exploited. (7 marks)

## **Task 8 [6 marks]**

Write an NSE script that turns on/off the firewall on the Windows OS. (3 marks)

Install a Windows OS on AWS or use an already OS if it is available to you. Apart from script, you will need to provide a screen recording evidence (video) with commentary. If the evidence is not 100% clear that you have recorded it and have not done it yourself, you will not get marks for this part of the task. (3 marks)