JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELORS IN BUSINESS INFORMATION SYSTEMS

2ND YEAR 2ND SEMESTER 2020/2021 ACADEMIC YEAR

MAIN CAMPUS

(SUPPLEMENTARY/SPECIAL EXAMINATION)

COURSE CODE: IIT 3225

COURSE TITLE: ETHICAL HACKING AND PENETRATION TESTIN

EXAM VENUE: **STREAM: FORENSIC**

DATE: **EXAM SESSION:**

TIME: 2.00 HOURS

INSTRUCTIONS:

a) **Answer Question 1 (Compulsory) and ANY other two questions**
b) **Candidates are advised not to write on the question paper**
c) **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1 (30 MARKS)

The excerpt below appeared in an article titled **"SECOND 'FAPPENING' HACKER PLEADS GUILTY; FACING UP TO 5 YEARS IN PRISON"** authored bySwati Khandelwal in the website **http://thehackernews.com/** on Monday, July 04, 2016 **.**

"A second man has pleaded guilty for his role in 'The Happening' breach of 2014, in which the Internet was flooded with thousands of nude photographs of popular celebrities, including Jennifer Lawrence, Kim Kardashian, Kate Upton and Kirsten Dunst. Edward Majerczyk (28) of Chicago, Illinois agreed to plead guilty last Friday to hacking into the Apple iCloud and Gmail accounts of more than 300 victims, including 30 celebrities, between November 2013 and August 2014, federal prosecutors said. Like Ryan Collins, Majerczyk used phishing scheme to trick celebrities into entering their account credentials into bogus 'security' sites and then accessed private and nude photographs and videos of celebrities.

The hackers then leaked hundreds of thousands of explicit photos of Hollywood actresses on the Internet in September 2014 that later known as The Fappening (or 'Celebgate') breach.

> 'This defendant not only hacked into email accounts — he hacked into his victims' private lives, causing embarrassment and lasting harm," FBI's Deirdre Fike said in a statement. "As most of us use devices containing private information, cases like this remind us to protect our data.'"

Using this case, answer the questions below.

a) Enumerate six fundamental factors that may have driven Edward to perform this act of hacking. (6 marks)

b) List the two main differences between this act that Edward performed and what a pentester would actually be doing. (2 marks)

c) There are two attack types that may have been used by Edward in carrying out "The Fappening" breach.

   i) Explain the two attack types clearly. (4 marks)

   ii) Which of the two is the most likely attack type that was used? Explain your answer based on the scenario above clearly. (4 marks)

d) Just as in the case of a controlled attack, some amount of knowledge is required in order to carry out a real hack such as is the case for "The Fappening" breach.

   i) Explain clearly the three kinds of required knowledge that a hack may be exposed to. (6 marks)

   ii) What are the three possible source points of knowledge for Edward? (3 marks)

e) While Edward was carrying out his act, there are five key points that he had ignored while bypassing the security of his victims that every pentester would have considered carefully. Enumerate them. (5 marks)

QUESTION 2 (20 MARKS)

a) Security consultants come in many forms with different abilities and conclusions about security. Much of this is based on their exposure and experience in the security industry and where they have realized successes and failures. Nevertheless, the skill of security consultants can be categorized in two fundamental camps. List these categories and explain them. (4 marks)

b) Social engineering is the oldest form of attack to obtain data. It practices coercion and misdirection to obtain information. Social engineering can take many forms. However, there are five major elements associated with social engineering. List and clearly discuss them. (10 marks)

c) Discuss the three main steps you would follow in developing an effective security awareness program. (6 marks)

QUESTION 3 (20 MARKS)

a) Explain the difference between inherent and imposed limitations when carrying out a pentest. (4 marks)

b) Integration of the pentest results comes in four phases and these phases can exist in their entirety or partially in remedial, tactical, or strategic planning, but must appear in some form within each characteristic of security. The one step common to each of the four areas is planning. Once the planning is

complete and a clear roadmap to recovery is established, the four areas can be addressed. Enumerate and explain these four areas. (8 marks)

c) While preparing and planning for the pentest, generating status reports by the attacking team would be very essential. What are two essential reasons for having these reports? (2 marks)

d) All the work from the engagement - materials collected, communications, tasks performed, results from tools, vulnerabilities, and any information about the target - culminates in a final document. Arguably, the company is effectively paying for the deliverable. The deliverable must accomplish two challenges. Explain these challenges. (4 marks)

e) What is a rootkit and for what purpose is it used for? (2 marks)

QUESTION 4 (20 MARKS)

a) There are several types of hackers.

i) Explain the three types of hacker categories based of their activities. (6 marks)

ii) Explain the three types of hacker categories based of their knowledge. (6 marks)

b) There are many characteristics that can be used to rate any attack as a success. Given the scenario above what would be the possible ways of looking at the attack as a success? (3 marks)

c) What is meant by the term framework? (1 mark)

d) Explain the two types of limitations while carrying out a controlled attack. (4 marks)

QUESTION 5 (20 MARKS)

The movie *Sneakers* was one of the first mainstream films that demonstrated the controlled attack. The film begins very late in the evening with Robert Redford and a small team breaking into a bank. After some very technical maneuvering, they successfully escaped with millions of dollars in loot. The next morning Robert walks into the bank and slams a suitcase full of the money on the senior staff's meeting table. It was not until this point that you realize he was not a thief, but rather a security expert proving the vulnerabilities of the bank's security systems by exploiting them.

a) Assuming that this was not a controlled attack and therefore the Robert Redford team was actually performing a real hack on the bank, explain clearly four areas that such an attack would have an impact. (8 marks)

b) It is most likely that this attack team built a model attacking system prior to the actual attack. There are generally four attributes to building such an attack system. Enumerate and explain each clearly. (8 marks)

c) Integration of the results that the team gave to the bank usually comes in four phases and these phases can exist in their entirety or partially in remedial, tactical, or strategic planning, but must appear in some form within each characteristic of security. The one step common to each of the four areas is planning. Once the planning is complete and a clear roadmap to recovery is established, the four areas can be addressed. Enumerate and explain these four areas (4 marks)