JARAMOGI OGINGA ODINGA UNIVERSITY FOR SCIENCE & TECHNOLOGY

School of Informatics and Innovative Systems

Department of Computer Science and Software Engineering

KISUMU LEARNING CENTER

BSc Computer Security & Forensics

IIT 3125 EMERGING THREATS, ATTACKS AND DEFENSES

TIME: 2HRS

Instructions

1. This paper contains FIVE questions
2. Answer Question One (Compulsory) and ANY OTHER TWO questions
3. Answer each question on a new page

QUESTION ONE (COMPULSORY) [30 MARKS]

(a) For each of the following, identify ONE emerging security threats, attacks and defenses. Give reasons to support your answer. [6 Marks]

(i) IP telephony

(ii) Social Networking Sites

(b) The following statements might be TRUE or FALSE. For each case, provide reasons in support of your choice. [4 Marks]

(i) Online Social Networks are at a crossroads between being monolithic proprietary applications and open applications in the federated identity management space.

(ii) A malicious user can sniff the encrypted data to obtain network information.

(c) Define the following terms and concepts as applies to computer security [8 Marks]

(i) Vulnerabilities

(ii) Online Extortion

(iii) Drive-by-pharming

(iv) Cyber Stalking

(d) Name and explain ANY TWO; [8 Marks]

(i) Security threats and respective defenses applicable for Wireless Networks

(ii) Emerging cyber attacks and defenses in the current Internet World

(e) "Regulatory approaches supplements management of cyberspace security" Do you agree? Explain. [4 Marks]

QUESTION TWO **[20 MARKS]**

(a) What is *VOIP Security*? How is it different from the general network security? [4 Marks]

(b) Name FOUR security measures that apply to VOIP security. [4 Marks]

(c) When Emmanuela was asked by her lecturer why there is increase in cyber intelligence, her response was "open source network compromises disclosures". What is your view on Emmanuela's response? Was she right? Support your answer. [4 Marks]

(d) Explain emerging defenses that are applied in Windows Vista security. [4 Marks]

(e) What is a *mobile worm*? Name any TWO examples of mobile worms. [4 Marks]

QUESTION THREE **[20 MARKS]**

(a) What are the key drivers of security problems that affect web transactions? [6 Marks]

(b) In your own opinion, is adoption of E-commerce Security Strategy critical to financial organization? Explain. [4 Marks]

(c) Consider yourself as an Information Security expert that has been hired to develop a strong E-Commerce Security Plan for Jamii Corporate Limited that has witness serious cyber attacks. The company has multiple points of presence across its region and manages sensitive customer database that is subjected to concurrent transactional

activities. The database has modules that support both online functions and integration of mobile services. You are expected to come up with a deployable security framework for the enterprise-wide network. [10 Marks]

QUESTION FOUR [20 MARKS]

Below is a newspaper extract from Kenya's Standard on Saturday of March 23, 2013. Read it and use it to answer the questions that follow.

South Korean investigators said on Friday they mistakenly identified a Chinese Internet address as the source of a cyber-attack that paralyzed tens of thousands of computers at banks and broadcasters earlier this week. But they said they still believe the attack originated from abroad.

The error by South Korean regulators raised questions about their ability to track down the source of an attack that hit 32,000 computers at six companies on Wednesday and exposed South Korea's Internet security and vulnerabilities to hackers.

South Korean investigators said on Thursday that a malicious code that spread through the server of one target, Nongyup Bank, was traced to an Internet Protocol address in China. Even then it was clear that the attack could have originated somewhere else, because such data can easily be manipulated by hackers. Experts suspect North Korea was behind the attack.

The state-run Korean Communications Commission said on Friday that the IP address actually belonged to a computer at the bank. The IP address was used only for the company's internal network and was identical to a public Chinese address.

(a) Considering the above case, explain the possible network tools the South Korean investigators might have relied upon to trace an Internet Protocol (IP) Address in China were used to launch the cyber-attack. [4 Marks]

(b) What are the possible reasons that might have necessitated the error by South Korean regulators when trying to track down the source of their attack? [2 Marks]

(c) Using a suitable example, expand how a malicious code might have been used in launching a successful attack to target Nonghyup Bank server. [4 Marks]

(d) Consider yourself as hired by the South Korean authorities to beef up their cyber security, what technical measures are you likely to employ to avoid future attack on their servers? [4 Marks]

(e) Explain any two techno-economic impacts of cyber terrorism to a developing economy like the case of Kenya. [4 Marks]

(f) Presenting admissible evidence in a court of law has been one major challenge towards effective prosecution of cyber crime cases. What are the two techno-legal issues that have stood in the way of justice when it comes to handling cyber crime cases? [2 Marks]

QUESTION FIVE **[20 MARKS]**

Below is an excerpt of an article which was published in the November 2009 issue of Texas Banking. Read it carefully and use it to answer the questions provided below.

"In August 2009, Israeli hacker Ehud Tenenbaum, aka "The Analyzer", plead guilty to a single count of bank card fraud for his role in a sophisticated computer-hacking scheme that scored over $10 million from U.S. banks, some reportedly from Texas. Attacks on U.S. banks, such as this example, seem to occur more and more frequently. These increases in attacks coupled with economic strains that cause many banks to cut security budgets have many skeptics predicting 2010 could be a worse year for security breaches"

(i) While referring to above excerpt, explain FOUR vulnerabilities that attackers may exploit when launching these successful attacks. [8 Marks]

(ii) Name ANY FOUR emerging information security threats banks faces not only in the US but also in Kenya. [4 Marks]

(iii) Propose respective defenses against listed information security threats mentioned in (ii) above that the banks can resort to. [8 Marks]

- END -