JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF SCIENCE

COMPUTER SECURITY & FORENSICS

1ST YEAR 2ND SEMESTER 2013/2014 ACADEMIC YEAR

CENTRE: MAIN

COURSE CODE: IIT 3125

COURSE TITLE: EMRGING THREATS, ATTACKS AND DEFENSES

EXAM VENUE: LR 2 **STREAM: BSc. Computer Security & Forensics**

DATE: 18/12/2013 **EXAM SESSION: 11.30 – 1.30 PM**

TIME: 2 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 questions.**
2. **Candidates are advised not to write on the question paper.**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room.**

QUESTION ONE (COMPULSORY) **[30 MARKS]**

(a) Differentiate between the following as applies to computer security [8 Marks]

(i) Hacking and Cracking

(ii) Phishing and Vishing

(iii) Vulnerabilities and Threats

(iv) Bluesnarfing and Bluebugging

(b) The following statements might be TRUE or FALSE. For each case, use a suitable example to support your choice [6 Marks]

(i) Network stack fingerprinting is a common technique for identifying hosts on a network.

(ii) MObile SEcurity processing System (MOSES) secures boot and run-time memory protection.

(iii) Criminal activities involving the perpetration of a fraud through the use of the computer or the internet can take many different forms.

(c) Identify TWO current threats by mobile malware. [2 Marks]

(d) What is *Domain Name System (DNS) poisoning*? Is it the same as cache poisoning? Use an example to support your answer. [4 Marks]

(e) Briefly explain TWO key drivers of web transactions security problems. [4 Marks]

(f) "When Bluetooth is enabled on a device, it's essentially broadcasting the fact that "*I'm here, and I'm able to connect*" to any other Bluetooth-based devices within range".

(i) Do you agree with the above statement? Support your answer. [2 Marks]

(ii) Explain the four categories of Bluetooth hacks. [4 Marks]

QUESTION TWO

(a) Network security attacks can be classified into *passive* and *active* attacks. Using appropriate examples, distinguish between the two classifications. [4 Marks]

(b) With examples, explain any TWO network security goals violations that can be experienced in Mobile Ad Hoc Wireless Network (MANETs). [4 Marks]

(c) For each of the cases below, identify the possible threats, common attacks and effective respective defenses [12 Marks]

(i) Web browsers

(ii) Social Networking Sites

(iii) Virtual Local Area Networks (VLANs)

(iv) Operating Systems

QUESTION THREE

(a) "Cyber threats can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet."

(i) How true is the above statement? Explain [2 Marks]

(ii) Name any TWO types of cyber threats you know. For each, identify the technical motivation and the methods used for actualizing the attacks. [8 Marks]

(b) Read the extract below and use it to answer the questions (i - iv) that follows

The Ugandan government has warned its citizens to be cautious over rising cases of internet fraud by ensuring their privacy when they use web services. Speaking at the first East African Information Securities Conference, John Nasasira, information and communications technology minister, said the rise in internet fraud and hacking of websites has become a top priority for national governments and businesses worldwide.

(i) What is an internet fraud? [2 Marks]

(ii) How do these criminals succeed in their mission as indicated above? [4 Marks]

(iii) Give TWO countermeasures that can be used to address internet fraud. [2 Marks]

(iv) What are the jurisdictional challenges that affect effective litigation against these internet fraud cases? [2 Marks]

QUESTION FOUR

(a) Identify a security threat that prevents secure communication in MIPv6 based nodes. Propose security solution for the mentioned threat. [2 Marks]

(b) Use a well labeled diagram to explain how the following security attacks are carried out in a network. For each case, propose an effective countermeasure. [12 Marks]

(i) Smurf DOS Attacks

(ii) IP Spoofing Attacks

(iii) Packet Sniffing

(c) "A Virtual Machine can be used to steal the cryptographic keys that are in place to keep data secure from another running on the same physical hardware".

(i) Briefly explain how true the above statement is. [3 Marks]

(ii) Explain any countermeasure that can be used to address any security compromise that involves virtual machines. [3 Marks]

QUESTION FIVE

(a) Read the extract below and use it to answer questions that follows

Last week, a company got a KES 100,000 phone bill. It turns out some enterprising types have been bouncing their calls off the voice network. This allowed them to make numerous calls to a foreign country using the equipment. And it looks like they are stuck with the bill. The problem is that the voice over IP (VoIP) network is set up to receive incoming call requests from the general public. This is the normal way these phone calls work. They use the SIP protocol, which is designed to accept voice connections from anywhere.

(i) Explain any TWO vulnerabilities that are likely to be exploited here. [4 Marks]

(ii) Propose TWO respective security mechanisms that can used to correct mentioned vulnerabilities in Qn 5 (a) (i) above. [4 Marks]

(iii) Identify the possible legal challenge that VOIP related security issues like this faces. [2 Marks]

(b) "Though the bulk of mobile threats are in the form of malicious or high-risk apps, mobile devices are also troubled with other threats."

(i) Identify THREE other vulnerabilities being referred to in the above case. [3 Marks]

(ii) Give respective defense mechanisms for mentioned vulnerabilities in Qn 5 (b) (i) above. [3 Marks]

(c) What are the security improvements that make Microsoft Vista security better than the earlier versions? How do you compare Windows Vista security with Ubuntu Linux? [4 Marks]