JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATION SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SECURITY AND FORENSIC

2ND YEAR 2ND SEMESTER 2013/2014 ACADEMIC YEAR

MAIN

COURSE CODE: IIT 3221

COURSE TITLE: COMPUTER AND NETWORK SECURITY

EXAM VENUE: CL I **STREAM: (BSc. Computer Security and Forensic)**

DATE: 14/04/14 **EXAM SESSION: 9.00 – 11.00 AM**

TIME: 2.00 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) Explain the significance of the following abbreviations to network security. [4 Marks]

(i) DMZ

(ii) IPsec

(iii) PGP

(iv) TLS

(b) Identify TWO strengths and TWO weaknesses of biometric authentication techniques. [4 Marks]

(c) In what ways do the three basic goals of information security overlap? [4 Marks]

(d) Name any TWO intelligent gathering tools that can be used in a network. [2 Marks]

(e) Explain how a targeted worm or virus can avoid detection by virus scanner. [2 Marks]

(f) "Firewalls can be used to block all distributed denial of service attacks while allowing all authorized communications".

(i) Do you disagree with the above statement? Explain your answer. [3 Marks]

(ii) Identify any THREE network threats that a firewall does not protect against. [3 Marks]

(iii) Explain <u>one</u> weakness of firewall at network perimeter in defending servers, desktop machines, and laptops against network threats. [2 Marks]

(g) In a Mandatory Access Control system, how can an insider with access to high-security file leak information to a low-security process using the virtual memory system? [2 Marks]

(h) A software house incorporates a time-clock which causes their product to stop working if it is not supplied with a suitable password every four (4) months. What risks are they running? [4 Marks]

QUESTION TWO **[20 MARKS]**

(a) What are the differences between a boot sector virus, an application virus, and a macro virus? Consider what each must do to spread and how they may be controlled. [6 Marks]

(b) Usual authentication systems verify passwords with the help of their hashes stored in protected files.

(i) What is the purpose of storing password hashes rather than the passwords themselves? [3 Marks]

(ii) Why should access to the password hashes be protected? [3 Marks]

(c) A firewall is placed at the gateway between a corporate LAN and the Internet. Explain in outline how the firewall could be configured to bar any external machine on the Internet from initiating a connection to a machine on the corporate LAN. [3 Marks]

(d) "In web security HTTP Digest Authentication is said to be a low budget security alternative to SSL".

(i) Do you agree with this statement? Explain in support of your answer. [2 Marks]

(ii) Explain how the HTTP digests offers protection against replay attack and against disclosure of the server database. [3 Marks]

QUESTION THREE **[20 MARKS]**

(a) Upon analysis on a university's site network, the following threats and attacks are identified: threats from malicious code (e.g. virus, worms and Trojan horse), port scanning, IP spoofing, and TCP SYN flood attacks. To counter these threats and attacks, an administrator in the university, Daniel, has suggested using a firewall to control the access of the site network from the Internet.

(i) Describe what Port Scanning, IP Spoofing, and TCP SYN flood attacks are, and explain how a firewall can be used to protect these attacks. [6 Marks]

(ii) There are three types of firewalls to choose from: packet filtering firewalls, stateful packet inspection firewalls, and application gateways. Describe the working mechanisms of the three types of firewalls. [6 Marks]

(b) A Sacco decides to allow electronic voting at all general meetings. Each member is given an ID which is his/her number on share register and a password which is a hash of this ID and his/her address details. Passwords are included with official notices of meetings which are sent to shareholders through the post. A special website is created to accept votes up to the time of the meeting. When a shareholder connects to the site he/she is

asked for his/her ID and password and if a correct ID/password pair is provided another screen appears through which voting may take place. As the company's auditor you are responsible for ensuring that meetings are conducted properly. In this capacity what concerns would you have about the system proposed? What additional information would you require about the electronic voting system and what checks would you make before declaring the results of the votes? [8 Marks]

QUESTION FOUR **[20 MARKS]**

(a) A rapidly-growing online crime is *phishing*, in which victims are lured by an e-mail to log on to a website that appears genuine but that actually steals their passwords. You have been hired by a bank to help them harden their online banking service against phishing attacks. Explain briefly the strengths and weaknesses of the following FOUR possible countermeasures:

(i) SSL/TLS client certificates issued to each customer [4 Marks]

(ii) a handheld password calculator issued to each customer [4 Marks]

(iii) displaying a unique picture to each customer during the login process [4 Marks]

(iv) requiring that large payments, or payments to new recipients, be authorized by telephone or SMS as well as online. [4 Marks]

(b) You are told that the budget will accommodate only two of the above options in (a) above. Which two would you recommend, and why? [4 marks]

QUESTION FIVE **[20 MARKS]**

(a) The One Laptop Per Child project aims to supply millions of rugged low-cost laptops to children in less-developed countries. The machines run Linux, have 2 GB flash rather than a hard-disk, and have a wireless LAN capability that may be used either in the conventional way or to setup ad-hoc peer-to-peer networks. You have been tasked to design the security policy for these laptops. If the project is to do, supply standard security software with each machine, what should it try to do and how? [6 marks]

(b) Describe any TWO problems that classical multilevel-secure systems suffer. A client is proposing to implement an e-mail sent internally within the company i.e. with no outside recipients should be deleted after 30 days unless a manager authorizes its retention. Which of the mentioned problems would you have to consider and why? [4 Marks]

(c) Consider yourself being approached to help in implementing a new IEEE802.11 WLAN (Wireless Local Area Network) for their county office with 150 computer users. The county has already got a wired network facility and it is required that this WLAN should be integrated with the existingwired network facility.Identify *three* security threats that are introduced as the result of this wireless network installation and integration, and outline security services that are required to address these threats. [6 Marks]

(d) Propose a Disaster Recovery Plan (DRP) that can be used to arrest any threats originating from network downtime mentioned in 5 (c) above. [4 Marks]

- END -