JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

MAIN CAMPUS (BONDO)

END SEMESTER EXAMINATION

BSC IN COMPUTER SECURITY AND FORENSICS

GROUP: YEAR 1 SEM 2

PAPER: IIT 3125 EMERGING THREATS, ATTACK AND DEFENSES

INSTRUCTIONS

1. This paper contains FIVE questions. Question One is 30 Marks and the rest are 20 Marks each.
2. Answer question one which is COMPULSORY and ANY OTHER TWO
3. Be precise and clear in your answers.

QUESTION ONE [30 MARKS]

(a) For each of the following, identify the possible vulnerabilities cases. [4 Marks]

(i) Online Social Networking sites

(ii) Mobile IPv6

(iii) Wireless Networks

(iv) Web browsers

(b) The following statements might be TRUE or FALSE. For each case, provide reasons in support of your choice. [8 Marks]

(i) Not a single virus is reportedly specific to infecting the VOIP packets.

(ii) "Air-poison" is proof of concept tool that sniff air for HTTP Javascript requests and prepends a cacheable malicious payload to the victim.

(iii) Identity server adapts established privacy and security technologies to provide novel solutions to problems within the context of mobile social network systems.

(iv) Trojans are capable of operating camera and sending contents over the Internet.

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

(i) Vulnerabilities and Threats

(ii) White Hacker and Black Hacker

(iii) DNS Cache Poisoning and ARP Poisoning

(iv) VOIP Vishing and Voice SPAM

(d) Name and explain ANY TWO; [6 Marks]

(i) Security threats and respective defenses applicable for Mobile Social Networks

(ii) New frightening types of cyber threats in the current Internet World

(e) "K-Anonymity does not provide a simple and efficient approach to protect private individual information". Do you agree with the statement? Discuss. [4 Marks]

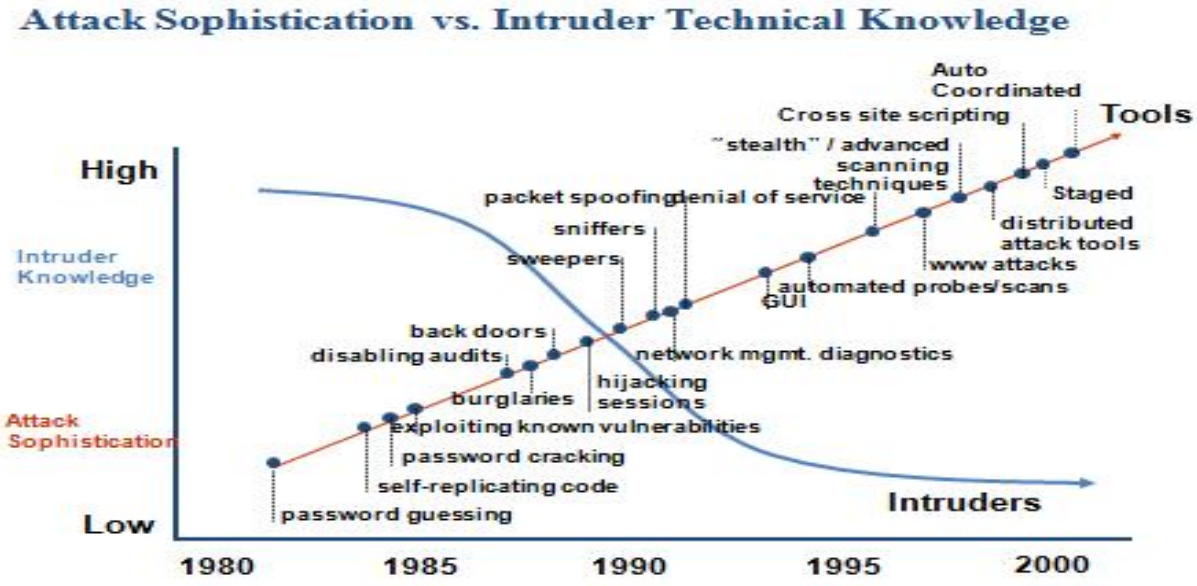
QUESTION TWO [20 MARKS]

(a) Name and explain THREE emerging threats to server security. [6 Marks]

(b) Using OSI Network Model, discuss threats, attacks and defenses that applies for each network layer. Use diagram where necessary. [14 Marks]

QUESTION THREE [20 MARKS]

The graph provided below shows advancement in attacks strategies vis-a-vis intruder's technical knowledge as studied over time. Use it to answer the question below.



(a) In brief sentences, expand on your understanding of the above figure. [2 Marks]

(b) From the above figure, compare the technical motivations for employing in *cross-site scripting* and *session hijacking* in organizational network that support transactional activities. [4 Marks]

(c) Below is a summary table showing some of the techniques from the above figure. Fill in the gaps corresponding targets, motivations and appropriate defenses. [12 Marks]

No.	Techniques	Targets	Motivations	Defenses
(i)	WWW Attacks			
(ii)	Automated Probes			
(iii)	Advanced Scanning			
(iv)	Disabling Audits			

(d) Name any TWO emergent attacks in Mobile Social Networking. [2 Marks]

QUESTION FOUR [20 MARKS]

(a) Using supporting practical examples, name ten most devastating database security threats used by attackers today. [10 Marks]

(b) "It is important to understand basic approaches used by attackers targeting some specific web application". Discuss the basic steps in attacker methodology applicable in web security. [10 Marks]

QUESTION FIVE [20 MARKS]

(a) Explain your understanding of *economics of information security*. [2 marks]

(b) Explain the following security features that applies to Windows Vista [8 Marks]

(i) Windows Defender

(ii) Windows Firewall

(iii) Bitblocker Drive Encryption

(iv) Security Center

(c) "In cyber threat landscape, one needs to be aware of the trending attack techniques and the profile of the attacker to identify the subtle changes that may indicate an emerging threat". Support this statement. [2 Marks]

(d) "Cyber attacks have become much more sophisticated and are now easily bypassing traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways, compromising the majority of enterprise networks".

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

(ii) What positive impacts do *dynamic threat intelligence clouds* has on fight against cyber attacks? [4 Marks]

(iii) What are the techno-legal issues that complicate the case of cyber attacks? [2 Marks]

- END -