JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF

BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENSICS

1ST YEAR 2ND SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1108

COURSE TITLE: EMERGING THREATS, ATTACKS AND DEFENSES

DATE: 23/4/2025
SESSION: 15.00-17.00
VENUE : LAB 7
TIME : 2HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two 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**
4. **No mobile devices (e.g., laptops, phones. etc.) are allowed into the Examination Room**

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

QUESTION ONE **[30 MARKS]**

a) Define crimeware and explain its primary objective. [2 marks]

b) What is online extortion, and provide two examples of online extortion tactics. [2 marks]

c) Differentiate between traditional pharming attacks and drive-by-pharming attacks. [2 marks]

d) Discuss any two attacks on cryptosystems and show any defense mechanism that are available [4 marks]

e) Discuss any five malware and show the defense mechanisms that are available for each. [5 marks]

f) Discuss any five threats that operating systems are facing and suggest the defense method for each [5 marks]

g) Define the following terms [2 marks]

i. Threat

ii. vulnerability

h) For each of the cases below, identify the possible threats, common attacks and effective respective defenses [6 Marks]

i Web browsers

ii Social Networking Sites

iii Virtual Local Area Networks (VLANs)

i) What is VoIP spam (SPIT), and what are its potential impacts? [2 marks]

QUESTION TWO **[20 MARKS]**

a) What is the role of threat actors in cybersecurity, and what motivates them to launch cyber-attacks? [2 marks]

b) What are some examples of emerging cyber threats that have gained prominence in recent years? [5 marks]

c) Show how session Hijacking is a threat to a web user [3 marks]

d) Most communication on the internet involves domain Name service (DNS). Discuss how an attacker can use this service to attack web users [5 marks]

e) Discuss the techniques used in perimeter security approach to deal with attacks [5 marks]

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

QUESTION THREE **[20 MARKS]**

a) With the proliferation of mobile devices, what are the evolving threats targeting mobile platforms, and how can individuals and organizations protect themselves from mobile-based attacks? [5 marks]

b) Discuss how firewall provides defense mechanism against external threats [5 marks]

c) Discuss the following types of access attacks [8 marks]

i. Password attacks

ii. Trust exploitation

iii. Port redirection

iv. Man-in-the-middle attacks

d) Discuss the concept of least privileges and how it can be used to deal with security threat [2 marks]

QUESTION FOUR **[20 MARKS]**

a) Differentiate between the following terms and concepts as applies to computer security [4 Marks]

i Vulnerabilities and Threats

ii White Hacker and Black Hacker

iii DNS Cache Poisoning and ARP Poisoning

iv VOIP Vishing and Voice SPAM

b) What are the differences between confidentiality, integrity, and availability in the context of cybersecurity? **[**6 marks**]**

c) Discuss what you understand by the term eavesdropping and show how protocol analyzer tool can help the attacker perform this act. [6 marks]

d) Explain the concept of "deepfake" technology and its potential impact on cybersecurity. How can organizations detect and mitigate the risks associated with deepfake attacks? **[**4 marks**]**

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

QUESTION FIVE **[20 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) Discuss the following threats [4Marks]

i. Trojan Horse

ii. Worm

iii. Rootkit

iv. Ransomware

c) The only way to be sure your network is secure is to actually check for vulnerabilities and flaws. Discuss any three tools that can help you in doing so. [3Marks]

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

The Kenya 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, Edward Owalo, 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? [1 Marks]

ii How do these criminals succeed in their mission as indicated above? [2 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]

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

This is the last printed page

- END –

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING