CRSS 434: COMPUTER SECURITY

QUESTION ONE IS COMPULSORY AND ANY OTHER TWO

QUESTION ONE: 30 MARKS

a) In access control systems, what is a capability? (2 marks)
b) Explain the four main security properties of a computing system. (4 marks)
c) Describe social engineering in relation to computer security (3 marks)
d) Discuss four layers of computer security in detail by citing relevant examples in each case (4 marks)
e) Describe the following terms:

   i) Identity theft (2 marks)

   ii). Packet sniffing (2 marks)

   iii). Port scanning (2 marks)

   iv). Non repudiation (2 marks)

f) Write three practical goals of an Intrusion Detection System (2 marks)

g) What is your understanding of an *exploitable* vulnerability? (3 marks)

h) How would you secure the Kenya from cyber-attacks which could result in lowering our standard living (such as power outages, telephone outages, etc.) or maybe even result in the loss of life? (4 marks)

QUESTION TWO: 20 MARKS

a) Explain what meant by computer security policy? Discuss different types of computer security policy in details (8 marks)
b) Discuss the two types of intrusion detection systems? Differentiate between them by writing their characteristics. (8 marks)
c) What is cyberspace crime? Give examples (4 marks)

QUESTION THREE: 20 MARKS

a) Explain how change in Technology has led to drastic approaches in handling computer security issues (6 marks)
b) Explain measures and methods that are employed to counter cyberspace crimes across the globe. (4 marks)

c) Why is Digital Crime Scene Preservation and Documentation phase very important in achieving successful digital crime investigation (4 marks)

d) China is believed to be one of the perpetrators of cyber espionage. Explain how it is using it to its advantage by citing relevant practical examples (6marks)

QUESTION FOUR: 20 MARKS

a) Why do you think many cybercrime suspects go scot-free mostly in the developing countries especially Kenya, Uganda? What should be done in your opinion to enable them face justice and be charged for the offences? (8 marks)

b) Describe the differences between cyber warfare and cyber terrorism (4 marks)

c) Explain why acquisition or imaging of exhibits very crucial in computer crime investigation process (6 marks)

d) What is data privacy? (2marks)

QUESTION FIVE: 20 MARKS

a) List the basic computer security checklist (6marks)

b) Describe some of the most common cyber-crimes in the world. (8 marks)

c) In a high security setup it's advisable to deploy multifactor authentication (MFA), explain? (4marks)

d) Define the term firewall. Explain its purpose (2 marks)