Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 3105 NETWORK SECURITY

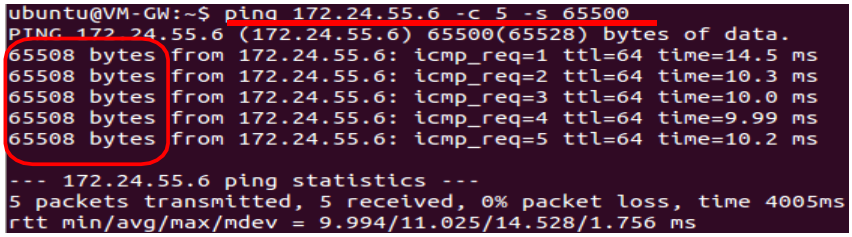
DATE: 26th July 2024 Time: 13:00-15:00 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE (THIRTY MARKS)

a) The figure below depicts network layer attack. Examine it carefully and respond to the following questions:



i) Describe the attack and highlight its threat to the network. **(2 marks)**

ii) Apart from the above attack, describe two other network layer attacks and explain how a network administrator can defend against them. **(4 marks)**

b) Discuss the various types of attacks that can occur at the MAC layer. Provide examples to illustrate these attacks. (**6 Marks**)

c) Explain the principles of packet sniffing and spoofing, and discuss the potential security risks associated with these techniques. (**6 Marks**)

d) Compare and contrast TCP and UDP in terms of their vulnerability to network attacks. Provide examples of specific attacks targeting each protocol. (**6 Marks**)

e) Explain what is meant by the term ***firewall*** in network security **and** discuss how it is used in network architectures. (**6 Marks**)

QUESTION TWO (15 MARKS)

a) An anti-spam company called Blue Security Inc. used a vigilante approach to fighting spam. Blue Security customers reported their spam to Blue Security, which analyzed it and sent back a set of instructions to a Blue Frog client running on the customer's machine. The client software used these instructions to visit the websites advertised by the spam messages and leave complaints on those websites. For each spam a user received, the Blue Frog client would leave one generic complaint. Blue Security operated on the assumption that as the community grew, the flow of complaints from hundreds of thousands of computers would apply enough pressure on spammers and their clients to convince them to stop spamming. A similar idea is the basis of an open-source P2P system called Okopipi.

On May 1st 2006, Blue Security's web site came under a massive DDoS attack using a variety of techniques including *DNS amplification*. Subsequently, the company shut down.

b) How does a DNS amplification DDoS attack work? (**3 Marks**)

c) What are some solutions to DNS amplification? (**3 marks**)

d) Suppose Blue Security was still in business. Can the Blue Security service itself be used to mount a DoS attack? If so, explain how. (**2 Marks**)

e) Explain the Heartbleed bug, how it was exploited, and the lessons learned for network security. (**3 Marks**)

f) Discuss the implementation and security benefits of DNSSEC. How does it help in preventing DNS spoofing attacks? (**4 Marks**)

QUESTION THREE (15 MARKS)

a) James and Alexander are having debate about computer and network security. James says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with James? You should explain your answer with SIX (6) reasons. (**7 marks**)

b) Describe how the Border Gateway Protocol (BGP) works and the types of attacks that can target BGP. How can these attacks be prevented? (**4 Marks**)

c) What is a reverse shell, and how can it be used in network attacks? Provide a scenario where a reverse shell might be utilized by an attacker. (**4 Marks**)

QUESTION FOUR (15 MARKS)

a) Name three types of Network vulnerability; give an example for each and a brief description of how each could be exploited. [**6 marks**]

b) Alice wants to attack Bob's computer via the Internet, by sending IP packets to it, directly from her own computer. She does not want Bob to find out the IP address of her computer.

   (i) Is this easier to achieve for Alice with TCP or UDP based application protocols? Explain why. [**2 marks**]

   (ii) For the more difficult protocol, explain one technique that Alice could try to overcome this obstacle and one countermeasure that Bob could implement in his computer. [**2 marks**]

   (iii) Name three functions that Alice's Internet service provider could implement to make it more difficult for Alice to achieve her goal? [**3 marks**]

c) In what way are TCP/UDP port numbers below 1024 special? [**2 marks**]

QUESTION FIVE (15 MARKS)

a) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these FIVE (5) requirements. (**5 marks**)

b) There are several methods of achieving secure remote access. One important method is to use a VPN. Explain if/ how a VPN achieves each of the requirements in part (a) (**5 marks**)

c) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. (**3 marks**)

d) Can a stateless firewall block TCP connection initiation requests from an external location to any local host, but at the same time allow returning traffic from connections initiated by local hosts? Why or why not? (**2 Marks**)