



SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF COMPUTER NETWORKS AND CYBER
SECURITY
CNS3105: NETWORK SECURITY
END OF SEMESTER EXAMINATION

DATE: 3rd August 2022

Time: 2 Hours

Instructions

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

Question One [30 Marks]

Part A – Short Answer Questions

- a. What is exploit in network security? [1 Mark]
- b. In an ICMP address mask request, what is the attacker looking for? [1 Mark]
- c. Which feature on a network switch can be used to prevent rogue DHCP servers? [1 Mark]
- d. Name one secure network protocol which can be used instead of telnet to manage a router? [1 Mark]
- e. Can an IP address be traced after it has been changed? Explain. [2 Marks]
- f. Briefly describe the two types of IPsec VTI interfaces. [2 Marks]
- g. Briefly describe any two means of user authentication which can be used in organization or in a network. [2 Marks]

Part B - Case study (Dyn DDoS Attack)

- a. Discuss how the DDoS attack on Dyn has led some security analysts to question the long-term viability of the Internet itself. [10 Marks]
- b. Explain 5 ways that would have been used by Dyn to avoid the DDOS attack. [10 Marks]

Question Two [15 Marks]

- a. What is CAM flooding attacks on a network switch? Which feature on a network switch can be used to protect against CAM flooding attacks? Explain the feature. [4 Marks]
- b. Briefly describe some considerations on when to use, select, deploy and maintain a VPN.

[6 Marks]

- c. Why does active file transfer protocol (FTP) not work with network firewalls? Mention a solution to this challenge. [5 Marks]

Question Three [15 Marks]

- a. Describe how a man-in-the-middle attack may be performed on a Wi-Fi network and the consequences of such an attack. [9 Marks]
- b. How can the mentioned attack on a Wi-Fi network be defeated? Explain. [4 Marks]
- c. What is an ip grabber? [2 Marks]

Question Four [15 Marks]

- a. Explain using a sequence of activities how secure sockets layer (SSL)/ Transport Layer Security (TLS) works? [6 Marks]
- b. How should organizations monitor for trojans and back doors? [4 Marks]
- c. How can brute force attack on a windows login page be prevented? [2 Marks]
- d. How can phishing emails be stopped with email security? [3 Marks]

Question Five [15 Marks]

Figure 1 illustrates the layered defense in depth model use to secure resources and the network in an information technology organization. Use the figure to answer the questions i-iii.

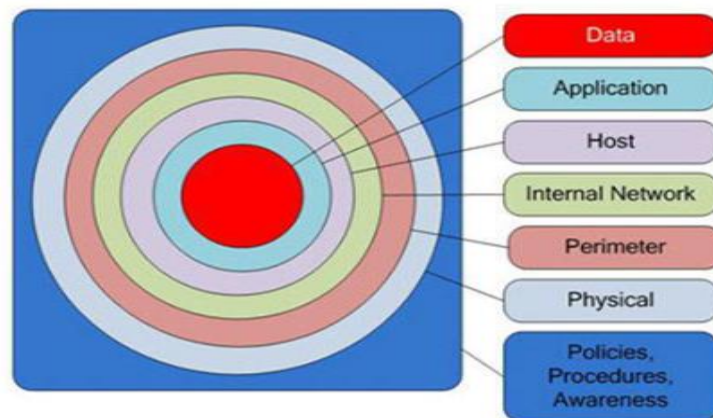


Figure 1: Security in Depth

- i. Using the control classification of resources: physical controls, technical controls, and administrative controls, explain the security requirements in each layer with the aim of achieving confidentiality, integrity, and availability in the network. [Hint: *resources and the types of network security tools*]. [9 Marks]
- ii. What security measures should be put in place by a technical manager for in-house developed applications? [4 Marks]
- iii. Briefly describe any two factors that affect the performance of the network? [2 Marks]