考生
序号____

苏州城市学院 信息安全 课程期末试卷

Suzhou City University

CS 336 Final Examination (Spring 2022)

Name：_____

Student ID：_____

1. (14 pts - 2pts each) **Circle** the correct answer for each of the following.

(1) Which protocol of the TCP/IP suite addresses reliable data transport?
A. Transmission Control Protocol
B. User Datagram Protocol
C. Internet Protocol
D. Internet Control Message Protocol

(2) Which of the following is **NOT** a characteristic of a good intrusion detection system?
A. Need constant monitoring
B. Run continually
C. Be fault tolerant
D. Observe deviations

(3) Common availability challenges do **NOT** include which of the following?
A. Rapid spread of viruses
B. Denial of service
C. Equipment failure
D. Loss of information system due to natural disaster or human action

(4) Which of the following is **NOT** a characteristic of common commercial cryptosystems?
A. Algorithms made readily available to the public
B. A key is used to encrypt messages
C. Keys and algorithms are published
D. A key is used to decrypt messages

(5) Cryptographic keys are used to do all of the following **except**:
A. Maintain the receiver's privacy
B. Authenticate the sender
C. Test the integrity of messages
D. Keep messages private

(6) Which of the following advantages does a VPN offer?
A. A VPN reduces the need for dedicated network connections and reduces the costs associated with network maintenance.
B. A VPN is generally more secure than shared network services.
C. A VPN allows employees and business partners access to the organization's network in a secure manner.
D. All of the above.

(7) Which of the following is most affected by denial-of-service attacks?
A. Confidentiality
B. Integrity
C. Accountability
D. Availability

2. (20 points) Fill in the blank (2 points each)

(i) Two different strings that have the same hash value is called _____.

(ii) Designed to protect the distribution and reproduction rights of the owner, _____ protection is a category of intellectual property law.

(iii) TCP uses _____ to establish connection.

(iv) One method cryptographer uses to disguise messages is _____ where letters are rearranged into a different order.

(v) _____ is a computer network administration software utility. It requests a destination to return a reply, intended to show that the destination system is reachable and functioning.

(vi) The _____ describes physical objects/devices that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices over the internet.

(vii) Verification of one's identification credential is done with the _____.

(viii) A/An _____ is a puzzle that supposedly only a human can solve, so a server application can distinguish between a human who makes a request and an automated program generating the same request repeatedly.

(ix) Two evaluation criteria are the orange book and _____.

(x) _____ is the right to control who knows certain aspects about you, your communications, and your activities.

3. (15 points) Provide a brief description of each of the following: (3 points each)

(1) Honeypot

(2) Botnets

(3) Demilitarized zone (DMZ)

(4) Port scanning

(5) Worm

4. (8 points) Distinguish between symmetric and asymmetric encryption. What are the pros and cons of symmetric encryption? What are the pros and cons of asymmetric encryption?

5. (9 points) The secure design principles, documented by Jerome Saltzer and Michael Schroeder, include:

a. Ease of use: The protection mechanism should be easy to use.
b. Permission based: The default condition should be denial of access.
c. Open design
d. Complete mediation
e. Least privilege
f. Separation of privilege
g. Least common mechanism
h. Economy of mechanism

Pick **THREE** from *c* to *h* and explain them (3 points each).

6. (12 points) Denial-of-service attack (DoS).

a. (3 points) Define a denial-of-service attack.
b. (3 points) Why do many DoS attacks use packets with spoofed source address?
c. (3 points) What is a DDoS attack?
d. (3 points) What is the primary defense against many DoS attacks?

7. (6 points) OS implements some security functions for general objects, such as access control, audit, and virtualization. What is audit? What is the purpose of it? How can we use audit to help protect the system?

8. (6 points) Assume there is a data center located in a room. To prevent the data center from being accessed by unauthorized people, you will implement physical controls. List one example of deterrent control, one example of detective control, and one example of preventive control.

9. (10 points) SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

(3 points) a. Define firewalls.

(3 points) b. Describe the effect of rules A, B and E.

(4 points) c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Will the attack succeed? Which rules in the rule set will be applied? Give details.