Fundamentals of Cybersecurity (CS 4222/6222)
Exam 1 Solutions

Instructor: Olusesi Balogun
Department of Computer Science
Georgia State University
Fall 2025

October 10, 2025

Name: _____

Panthers ID: _____

INSTRUCTION

This is a closed-book exam. There are three parts in the exam, (a) multiple choice, (b) short answers, and (c) problem solving. Please, read each question carefully and try to answer each question on the provided page. If you need extra space, let the examiner know. Please write legibly and show all your working clearly. Please note that you are permitted to use an A4 size cheat sheet.

Section	**Points**	**Grade**
Multiple Choice		40
Short Answers		20
Problem Solving		40
Bonus		5
Total		100 (+5)

PART A: Multiple Choice (2 points)

Table 1: PART A MCQS ANSWERS

1		2		3		4		5		6		7		8		9		10	
11		12		13		14		15		16		17		18		19		20	

In question 1 - 3, with respect to CIA goals, state the risk(s) posed by the following.

1. Maria, an employee at an online examination center, discovers that she can repeatedly refresh the results portal and send hundreds of simultaneous requests. Her repeated actions cause the web server to slow down significantly, preventing other students from accessing their test results during peak hours. Which fundamental security property is being violated in this scenario?

   (a) Confidentiality
   (b) **Availability**
   (c) Integrity

2. After being reprimanded by her department head, Alex, a systems analyst at a large university, exploits her administrative credentials to secretly access the institution's academic database and manipulate students' grades—subtly inflating and deflating records to discredit her supervisor

   (a) Confidentiality
   (b) Availability
   (c) **Integrity**

3. James is sitting in a coffee shop using public Wi-Fi to log in to his online shopping account. The system transmits his password in plain text. An attacker using packet-sniffing tools on the same network captures James's credentials without his knowledge.

   (a) **Confidentiality**
   (b) Availability
   (c) Integrity

4. Robert, a student at Georgia State University, wants to trick the machine learning system that decides who gets access to certain university resources. He doesn't have access to the training data, and he also doesn't know how the model works internally or what parameters it uses. However, he tries to guess and test the system's responses by sending many different inputs to observe how it behaves. What type of attack does this Robert attempts to carry out?

   (a) White Box
   (b) Grey Box
   (c) **Black Box**

5. According to the Work Factor Principle, the cost of security mechanism should:

   (a) Be as expensive as possible
   (b) Cost more than the system it protects
   (c) **Be proportional to the resources of potential attackers**
   (d) Require no computational overhead

6. At DataRag Company, a part-time worker in the IT department was given administrative access to several staff accounts so he could help reset passwords. Instead of limiting his access to only the tools needed for that specific task, his account was allowed to view and modify all user data in the system. Later, a security audit revealed that this broad access could have been easily abused. Which fundamental security design principle was violated in this situation?

(a) **Least Privilege Principle**

(b) Work factor

(c) Partial Mediation

(d) Closed Design

7. What is the major advantage of packet switching over circuit switching?

   (a) Guaranteed bandwidth for each connection

   (b) No header information required

   (c) **More efficient bandwidth usage and flexibility under congestion**

   (d) Complex routing tables

In question 8 - 9, what types of attacks are being launched by each scenarios.

8. An attacker manages to intercept an online funds transfer request as it travels from a customer's device to the bank's server. During this interception, the attacker alters the message by changing the destination account number to their own account before forwarding the modified message to the bank. The transfer is successfully processed, and the funds are diverted without immediately triggering any alarms.

   (a) **Alteration**

   (b) Masquerading

   (c) Eavesdropping

   (d) Denial-of-service

9. After a large-scale ransomware incident, investigators use global honeypots, blockchain transaction tracing, and ISP logs to map the attack infrastructure back to a specific threat actor group operating in Eastern Europe.

   (a) **Traceback**

   (b) Denial-of-service

   (c) Aletration

   (d) Eavesdropping

10. In the Internet Protocol (IP) stack, every Network Interface Card (NIC) in a computer or device is assigned a unique 48-bit hardware address that is permanently burned into the card during manufacturing. This identifier is used for identifying devices within the same local network segment. At which layer of the Internet Protocol stack does this 48-bit unique identifier primarily operate?

    (a) Application Layer

    (b) Transport Layer

    (c) Network Layer

    (d) **Link Layer**

    (e) Physical Layer

11. When a laptop at home tries to visit www.gsu.edu, it must first obtain the IP address of that hostname. The DNS server's IP address was already provided earlier by DHCP. What is the first step the laptop takes when sending its DNS query on a LAN?

    (a) It contacts the default gateway directly.

    (b) It sends the query to the browser cache.

    (c) **It broadcasts an ARP request to find the DNS server's MAC address.**

    (d) It creates a TCP connection with port 80.

12. A student plugs two laptops into the same classroom LAN, both manually configured with IP 192.168.5.10. Moments later, neither laptop can reach the internet and both show an "IP address conflict" warning. Which network concept best explains why communication fails?

    (a) **ARP replies from both devices confuse the switch, breaking the MAC → IP mapping.**

(b) DHCP has assigned duplicate leases.

(c) The default gateway has blocked the subnet.

(d) DNS caching caused duplicate names.

13. A client initiates a TCP connection by sending a segment with Seq = 1000. The server responds with SYN-ACK, Seq = 5000, Ack = 1001. What acknowledgment number will the client send back to complete the handshake?

    (a) 5005

    (b) **5001**

    (c) 1000

    (d) 1003

14. A system administrator notices that two users who selected the same password have identical hash values stored in the password file regardless of the hashing algorithm. Which of the following mechanisms would best prevent this issue and make offline dictionary attacks more difficult

    (a) Using a longer hash algorithm like SHA-512 instead of SHA-1

    (b) Encrypting the password file with a symmetric key

    (c) **Adding a random unique salt to each user's password before hashing**

    (d) Compressing the password file to reduce visibility of repeated patterns

15. Consider a Normal ARP Request such that a Host of IP: 192.168.1.102 wants to ping 192.168.1.101. It doesn't know the MAC, so it sends an ARP request. However, the cable loop on the switch, frame circulates endlessly. This circumstance is known as:

    (a) **Broadcast Storm**

    (b) IP Spoofing

    (c) ICMP Attacks

    (d) DNS Hijacking

16. Which of the following mechanism ensures that the connecting medium is not overwhelmed with packets during packet transmission?

    (a) Flow Control

    (b) **Congestion Control**

    (c) Connection Control

    (d) Retransmission Control

17. The Application Layer is where apps and services interact with the network. It's responsible for what you see and use such as websites, email, file sharing. Which of the following protocols does not operate in this layer?

    (a) HTTPS

    (b) SMTP

    (c) **UDP**

    (d) FTP

18. The purpose of Network Address Translation (NAT) is to:

    (a) **Change private internal IP addresses into a single external public IP address**

    (b) Encrypt private IP addresses

    (c) Assign new IP addresses to all internal hosts

    (d) Prevent routing of any private packets

19. In a stack overflow, a type of buffer overflow, what is typically overwritten when too much data is input?

    (a) Data segment variables

    (b) **Return address and frame pointer**

(c) I/O buffer

(d) Heap Segment

20. What does the StackGuard defense mechanism use to detect stack corruption?

(a) Return address masking

(b) Heap reallocation check

(c) **Random canary value**

(d) Static code analysis

PART B: Short Answers (5 points each)

1. Briefly explain the difference between Firewall and Intrusion Detection System?

   A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. A Firewall is a preventive security mechanism that filters incoming and outgoing traffic based on predefined rules, blocking or allowing packets, to protect a network perimeter.

   An Intrusion Detection System (IDS) is a detection mechanism that monitors network or system activity for malicious behavior and sends an alert when suspicious activity occurs.

2. Briefly explain what Virus, Trojan, and Worm are.

   Virus: A computer virus is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication. It attaches itself to legitimate files or programs and spreads when the host file is executed. So, it needs user action to propagate.

   Trojan Horse: A Trojan horse (or Trojan) is a malware program that appears to perform some useful task, but which also does something with negative consequences (e.g., launches a keylogger).

   Worm: A computer worm is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction. It self-replicates and spreads automatically across networks without user intervention or attaching to other files.

3. Differentiate between White-list and Black-list Firewall.

   White-list Firewall: Only allows explicitly approved traffic; all else is blocked by default. That is, it is a default-deny policy, in which packets are dropped or rejected unless they are specifically allowed by the firewall.

   Black-list Firewall: It uses a default-allow policy. In other words, all packets are allowed through except those that fit the rules defined specifically in a blacklist. It allow all other traffic by default and blocks known malicious or disallowed traffic that fit into the rule.

4. Consider the following security scenarios. Indicate if each of them is a penetration test or security test.

Table 2: Security Activities: Penetration Test (P) vs. Security Test (S)

#	**Activity**	**P**	**S**
i	Breaking into a computer system without authorization.	X	
ii	Proposing a new procedure which implementation may help improve systems security.		X
iii	Finding out that 1/3 of the security procedures are not actually implemented.		X
iv	Scanning a network in order to gather IP addresses of potential targets.	X	
v	Performing a denial-of-service attack.	X	

PART C: (10 points each)

1. The University Research Data System (URDS) hosts files and resources used by a Computer Science research lab. There are three users, three key resources or data files, and three permissions as shown below.

   - Subjects (Users): Dr. James, Dr. Alex, and Dr. John
   - Objects (Data): Grades, Projects, and Research
   - Permissions: Read (R), Write (W), Execute (X)

   Given the policy rules:

   - James has full administrative control on all files (R, W, X)
   - Alex have (1) Read and Write permission to Grades File, (2) No access at all to Projects File, (3) Read and Write permission to Research File.
   - John have (1) Read permission to Grades File, (2) Execute permission on Projects File (3) No access at all to Research File.

   (a) Prepare an Access Control matrix for the University.

Subject	**Grades**	**Projects**	**Research**
Dr. James	R, W, X	R, W, X	R, W, X
Dr. Alex	R, W	–	R, W
Dr. John	R	X	–

   (b) Design an Access Control List for the University

   - **Grades:** James (R,W,X); Alex (R,W); John (R)
   - **Projects:** James (R,W,X); John (X)
   - **Research:** James (R,W,X); Alex (R,W)

2. (a) Consider two nodes in a network, given the following ARP states:

```
Node 1:
IP: 192.168.4.102
MAC: 00:11:22:33:44:03

Node 2:
IP: 192.168.4.6
MAC: 00:11:22:33:44:04

Attacker:
IP: 192.168.4.103
MAC: 00:11:22:33:44:07
```

   i. What is the state of ARP tables of Node 1 and Node 2 after ARP poisoning?

   - Node 1: 192.168.4.6 → 00:11:22:33:44:07 (attacker's MAC)
   - Node 2: 192.168.4.102 → 00:11:22:33:44:07 (attacker's MAC)

   ii. List two distinct mitigation strategies to prevent the ARP poisoning in this subnet.

   Any two is okay. OR Any correct list given by the students.

   - Implement **Dynamic ARP Inspection**
   - Use **Static ARP entries** for critical systems.
   - Employ **Port Security** and ARP monitoring tools.

3. Given that Delta Airlines allows their clients to create their password with at least 4 characters and at most 6 characters from the character set with lowercase letters a-z, uppercase letters A-Z and digits 0-9. Characters can be repeated.

   a) Calculate the total number of possible passwords using at least one digit which can be created from it?

   Given: Characters = 26 lowercase + 26 uppercase + 10 digits = 62 total.
   Password length = 4 to 6 characters; must contain at least one digit.

$$N = (62^4 + 62^5 + 62^6) - (52^4 + 52^5 + 52^6)$$

$$N = 37{,}573{,}019{,}440$$

$$\boxed{37{,}573{,}019{,}440}$$

   b) If an attacker have the capacity of cracking 1.2 million passwords/second. How long would it take an attacker to guess such a password with an accuracy of 80%?

$$Time = \frac{37{,}573{,}019{,}440}{1.2 \times 10^6} * \frac{80}{100} \tag{1}$$

$$= 25048 \text{ seconds}$$

$$\approx 417.48 \text{ minutes}$$

$$\boxed{6.96 \text{ hours}}$$

4. If a network has an IP address of 198.168.7.120/25.

   (a) What is the subnet mask of the network

   Subnet Mask: 255.255.255.128

   (b) What is the number of usable hosts in the network? (3 points)

   (c) **Usable Hosts:** $2^{(32-25)} - 2 = 126$

   (d) What is the range of the network host IPs

   198.168.7.1 – 198.168.7.126

   Explanations: Since the CIDR (Classless Inter-Domain Routing) prefix length is 25. It means that 25 bits are meant for the network and 7 bits for the host.

   (1) To get the Subnet Mask, we turn all the network bits to 1s and all the host bit to 0s. So, in a 32-bit IP address, the subnet masks will be:

   11111111.11111111.11111111.10000000

   = 255.255.255.128

   (2) The Usable Hosts = $2^{(HostBits)} - 2 = 126$

   Note: The 2 that we subtracted are the Network and Broadcast which are special IPs.

   $= 2^7 - 2 = 126$

To get the Hosts range, we will need to get the Network IP address which is obtained with all hosts bits set to be 0s and the Broadcast Address which is obtained with all hosts bits set to be 1s.

First, let us convert the IP address to bits (not necessary, but for clarity), we have:

198.168.7.120 = 11000110.10101000.00000111.01111000

Then, we need to focus on the last 7 bits which is the host part: 1111000

The Network Address then becomes 11000110.10101000.00000111.0000000 = 198.168.7.0

Similarly, the broadcast address is 11000110.10101000.00000111.01111111 = 198.168.7.127

(3) The other hosts is our host range, which is from the IP after the network and to the IP before the broadcast: 198.168.7.1 - 198.168.7.126

Bonus (5 points)

Consider the given buffer overflow vulnerable code:

```
#include <stdio.h>

void vulnerable() {
    char buf[16];
    printf("Enter input: ");
    gets(buf); // unsafe
    printf("You entered: %s\n", buf);
}

int main() { vulnerable(); return 0; }
```

The function `gets()` reads an arbitrarily long line from `stdin` into `buf` without checking the buffer size. If an attacker supplies more than 15 characters (plus the terminating `'\0'`), the extra bytes will overflow the 16-byte array and overwrite adjacent stack data such as frame pointer, return address, saved registers, etc. This is a stack-based buffer overflow.

Correct Code: Use a bounded input function such as `fgets()`

```
#include <stdio.h>
#include <string.h>

int main(void) {
    char buf[16];

    printf("Enter input: ");
    if (fgets(buf, sizeof(buf), stdin) != NULL) {
        /* remove trailing newline, if present */
        size_t len = strlen(buf);
        if (len > 0 && buf[len - 1] == '\n') {
            buf[len - 1] = '\0';
        }
        printf("You entered: %s\n", buf);
    } else {
        /* handle error / EOF */
        fprintf(stderr, "Input error or EOF\n");
        return 1;
    }

    return 0;
}
```