Fundamentals of Cybersecurity (CS 4222/6222)
Final Examination Practice Questions

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

Note: Your Final Exam will have fewer questions. The essence of the questions is to have enough questions to practice with. Please answer ALL the questions.

PART A – Multiple-Choice Questions

Instructions: For each question, select the **single best** answer (A–D). Where a short scenario is given, base your answer only on the information presented in the scenario and your understanding of course concepts.

1. A regional hospital experiences a ransomware attack. All patient records on the central server are encrypted, and for 12 hours doctors cannot view laboratory results or prior diagnoses, although the data has not been modified or leaked (yet). Which CIA security goal is *primarily* impacted in this scenario?

   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Authenticity

2. A software vendor discovers that a malicious insider modified the source code of their accounting system so that all transactions above $5,000 are secretly rounded down by $5. As a result, financial reports no longer match the real amounts. Which CIA goal has been violated?

   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Non-repudiation

3. A company deploys full-disk encryption on all employee laptops. If a laptop is stolen from a car, the thief cannot access any file contents without the decryption key. Which CIA goal is *directly* supported by this control?

   (a) Availability
   (b) Confidentiality
   (c) Integrity
   (d) Accountability

4. A bank configures its systems to log every login, transaction, and configuration change, along with the user identity and timestamp, and regularly reviews these logs for fraud. Within the AAA framework, this log collection and review primarily support:

   (a) Authentication
   (b) Authorization
   (c) Accounting
   (d) Anonymization

5. When a user accesses a VPN portal, she first enters her username and password, then is granted access only to resources she is permitted to use according to a policy. In this scenario, the *identity verification* step is referred to as:

   (a) Authorization
   (b) Authentication

(c) Accounting

(d) Auditing

6. An employee in the finance department, angry about a denied promotion, uses his legitimate credentials to log into the payroll server after hours and deletes several salary records. He did not bypass technical controls; he simply abused his legitimate access. This is best classified as:

    (a) External attack

    (b) Insider misuse

    (c) Social engineering

    (d) Physical attack

7. A group of attackers rent a large botnet and repeatedly send bogus HTTP requests to an e-commerce site's front-end server, exhausting its CPU and bandwidth so that legitimate users' requests time out. What type of attack is this?

    (a) Man-in-the-middle (MITM)

    (b) Denial-of-Service (DoS) / DDoS

    (c) Replay attack

    (d) Phishing

8. A fake "IT support" caller phones employees, claims there is an urgent system issue, and persuades them to reveal their passwords over the phone by pretending to be from the internal help desk. This is best described as:

    (a) SQL injection

    (b) Social engineering

    (c) DNS poisoning

    (d) Cross-site scripting

9. During a penetration test, the tester is given complete access to documentation, network diagrams, and source code before beginning the assessment. This type of test is usually referred to as:

(a) Black-box testing

(b) Grey-box testing

(c) White-box testing

(d) Blind testing

10. A company hires a security consultant to perform a broad evaluation that includes policy review, configuration auditing, staff interviews, and a limited number of technical checks, with the goal of measuring the organization's overall security posture. Compared to penetration testing, this activity is best described as:

    (a) Red teaming

    (b) Security testing / security assessment

    (c) Vulnerability scanning only

    (d) Incident response

11. The principle of **least privilege** can be summarized as:

    (a) Give every user access to all data.

    (b) Give each user only the access they need to perform their tasks.

    (c) Allow users to inherit all of their manager's permissions.

    (d) Deny all access by default, even to administrators.

12. A file server checks a user's permissions only when the file is first opened. If the administrator later revokes access while the file remains open, the user can continue reading it until they close the file. The violated security design principle here is:

    (a) Open design

    (b) Complete mediation

    (c) Economy of mechanism

    (d) Psychological acceptability

13. A vendor claims that their proprietary encryption system is secure *because nobody knows how it works.* No external experts have reviewed the design. This argument is an example of:

(a) Open design

(b) Security by obscurity

(c) Separation of duty

(d) Defense in depth

14. In a Role-Based Access Control (RBAC) system for a hospital, permissions such as *"view lab results"* and *"order medications"* are bound to roles like *Doctor*, *Nurse*, and *Pharmacist*, rather than to individual users directly. One main advantage of this approach is that it:

    (a) Eliminates the need for authentication

    (b) Scales better for large organizations with many users

    (c) Makes auditing impossible

    (d) Eliminates the risk of insider attacks

15. Consider the following description: "Permissions are bundled with each object, listing which subjects may access it and how." This most closely describes:

    (a) Access Control Matrix

    (b) Access Control List (ACL)

    (c) Capability List

    (d) RBAC Policy

16. A student chooses a 6-character password consisting only of lowercase letters. Another student chooses a 14-character password with lowercase, uppercase, digits, and special characters. From a password strength and entropy perspective, the second password is stronger primarily because:

    (a) It is easier to remember

    (b) It uses a larger character set and longer length

    (c) It looks more "random"

    (d) It contains dictionary words

17. An attacker pre-computes a large table of hash values for many possible passwords and stores them in a file, so that when they obtain a hashed password from a system, they can quickly look up the corresponding plaintext. This type of attack is best known as:

    (a) Dictionary attack
    (b) Rainbow table attack
    (c) Brute-force attack
    (d) Phishing attack

18. Adding a long, random **salt** to each password before hashing it significantly increases security because:

    (a) It makes the hash algorithm faster.
    (b) It prevents two users with the same password from having identical hashes and breaks precomputed tables.
    (c) It encrypts the password instead of hashing it.
    (d) It eliminates the need for strong passwords.

19. In C, a function reads user input into a fixed-size character array using `gets(buf)`. If the user inputs more data than the buffer can hold, the extra data may overwrite adjacent memory, including a saved return address. This vulnerability is known as:

    (a) Integer underflow
    (b) Format-string bug
    (c) Buffer overflow
    (d) Race condition

20. Which class of malware typically requires *user action* (such as opening an infected attachment) to spread between systems?

    (a) Worm
    (b) Virus
    (c) Rootkit
    (d) Logic bomb

21. A self-replicating program autonomously scans the Internet and exploits a known vulnerability in a network service to copy itself to other machines without user interaction. This is an example of:

    (a) Trojan
    (b) Worm
    (c) Spyware
    (d) Adware

22. 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

23. 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

24. 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

25. 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) Simpler routing tables

26. A workstation broadcasts a request like "Who has IP 10.0.0.5? Tell 10.0.0.3." on its local network. The protocol used to resolve the IP address to a MAC address in this scenario is:

(a) DNS
(b) ARP
(c) ICMP
(d) HTTP

27. When a user types `www.example.com` in the browser, the system needs to resolve this domain name into an IP address before establishing a TCP connection. This resolution is primarily performed by:

(a) ARP
(b) DNS
(c) DHCP
(d) SMTP

28. In the TCP/IP layered architecture, logical routing decisions (deciding the next-hop IP address) are made primarily at the:

(a) Application layer
(b) Transport layer

(c) Network layer

(d) Link layer

29. Ethernet networks that use CSMA/CD detect that a collision has occurred on the medium and then:

    (a) Permanently shut down the interface

    (b) Immediately resend the frame with higher power

    (c) Jam the medium and then back off for a random time before retransmission

    (d) Drop all frames silently

30. In the TCP three-way handshake, the correct *sequence* of control flags exchanged between client and server when establishing a new connection is:

    (a) SYN, ACK, FIN

    (b) SYN, SYN+ACK, ACK

    (c) ACK, SYN, SYN+ACK

    (d) FIN, ACK, FIN+ACK

31. In TCP congestion control, the *slow start* phase is best described as:

    (a) Immediately sending at maximum bandwidth

    (b) Increasing the congestion window exponentially from a small value

    (c) Decreasing the congestion window linearly on success

    (d) Dropping all packets on loss

32. A network device that inspects packet headers and maintains state about active connections, allowing or denying packets based on both rules and connection state, is best described as a:

    (a) Stateless packet filter

    (b) Stateful firewall

    (c) Hub

    (d) Switch

33. A company deploys a Virtual Private Network (VPN) for remote employees. The primary security benefit of the VPN is that it:

    (a) Compresses all traffic
    (b) Provides an encrypted tunnel over an untrusted network
    (c) Replaces the need for firewalls
    (d) Eliminates the need for authentication

34. 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

35. 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.

36. 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.

37. 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

38. 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 used. 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

39. 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

40. 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

41. 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

42. 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

43. 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

44. 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

45. An Intrusion Detection System (IDS) has a low false negative rate but a relatively high false positive rate. Over time, administrators begin to ignore many alerts because "they are probably nothing." This phenomenon is most closely related to:

    (a) Base rate fallacy

    (b) Encryption overhead

    (c) TCP slow start

    (d) Subnetting

46. In web security, the Same-Origin Policy (SOP) primarily restricts:

    (a) A script from one origin reading or modifying data from a different origin in the browser

    (b) Servers from communicating with each other

    (c) Users from opening multiple tabs

    (d) Cookies from being set over HTTPS

47. A malicious script is injected into a vulnerable web forum so that when other users view the page, the script executes in their browsers and steals their session cookies. This attack is best classified as:

    (a) Cross-Site Request Forgery (CSRF)

    (b) Cross-Site Scripting (XSS)

    (c) SQL Injection

(d) Command Injection

48. A logged-in user visits a malicious site while also authenticated to their online banking site in another tab. The malicious site causes the browser to send a forged transfer request to the bank using the user’s existing session cookie. This is an example of:

    (a) Cross-Site Request Forgery (CSRF)
    (b) Cross-Site Scripting (XSS)
    (c) DNS poisoning
    (d) Phishing

49. A web application constructs SQL queries by concatenating unvalidated user input directly into the query string. An attacker is able to submit input such as `’ OR 1=1 -` to bypass authentication. This vulnerability is:

    (a) SQL Injection
    (b) XSS
    (c) CSRF
    (d) Path Traversal

50. In the context of web attacks, which of the following is *primarily* a **client-side** attack affecting the browser?

    (a) SQL Injection into the database
    (b) Stored XSS that runs in the victim’s browser
    (c) OS command injection on the server
    (d) Misconfigured firewall rule

51. The Euclidean Algorithm for computing $\gcd(a, b)$ works by repeatedly:

    (a) Dividing both numbers by 2
    (b) Subtracting the smaller from the larger until they are equal
    (c) Replacing (a, b) with $(b, a \bmod b)$ until the remainder is 0
    (d) Factoring both numbers into primes directly

52. Two integers are said to be **relatively prime** (coprime) if:

    (a) They are both prime

    (b) Their greatest common divisor is 1

    (c) Their product is odd

    (d) One divides the other

53. In RSA, the public key is typically composed of:

    (a) (p, q) where p, q are primes

    (b) (n, e) where $n = pq$ and e is the public exponent

    (c) (n, d) where d is the private exponent

    (d) The hash algorithm and block size

54. A digital signature generated with a user's *private key* allows anyone with the corresponding public key to:

    (a) Recover the original plaintext message

    (b) Verify that the message originated from the claimed signer and was not altered

    (c) Regenerate the user's private key

    (d) Decrypt any ciphertext for that user

55. In a medical dataset, attributes like **ZIP code**, **Age**, and **Gender** are not directly identifying on their own, but in combination they may uniquely identify individuals. Such attributes are referred to as:

    (a) Sensitive attributes

    (b) Quasi-identifiers

    (c) Noise attributes

    (d) Public attributes

56. A data publisher wants to ensure that every released record in an anonymized table is indistinguishable from at least $k - 1$ other records with respect to the quasi-identifiers. This privacy property is known as:

(a) k-anonymity

(b) l-diversity

(c) T-closeness

(d) Differential privacy

57. T-closeness extends k-anonymity by additionally requiring that:

(a) All records in a group share the same sensitive value

(b) The distribution of sensitive values in each group is close to the distribution in the overall table

(c) Each record has at least t quasi-identifiers

(d) Only numeric attributes are used

58. In digital forensics, creating a **bit-by-bit** copy of an entire disk (including slack space and unallocated space) for analysis is called:

(a) Logical backup

(b) Forensic imaging

(c) Incremental backup

(d) RAID mirroring

59. A write-blocker is used when acquiring forensic evidence from a storage device in order to:

(a) Speed up data transfer

(b) Prevent any modifications to the original evidence

(c) Compress the disk image

(d) Encrypt the disk on the fly

60. A social engineer leaves several USB flash drives labeled “Salary Data 2025 (Confidential)” in the company cafeteria. Curious employees plug them into their work computers, unknowingly executing malware. This technique is best described as:

(a) Tailgating

(b) Baiting

(c) Pretexting

(d) Shoulder surfing

61. An attacker sends a convincing email that appears to come from the university registrar's office, instructing students to "confirm their login credentials" on a fake portal. This is an example of:

    (a) Spear phishing

    (b) Tailgating

    (c) Dumpster diving

    (d) Shoulder surfing

62. In adversarial machine learning, an **adversarial example** is best described as:

    (a) A model trained on malicious data

    (b) A carefully perturbed input that appears normal to humans but causes a model to misclassify

    (c) Any input that the model misclassifies due to noise

    (d) A dataset used for red-teaming models

63. A facial recognition system deployed for access control consistently misidentifies people from a particular demographic group while performing well on others. This security and ethics concern is primarily related to:

    (a) Availability

    (b) Fairness and bias in AI

    (c) Confidentiality

    (d) Hash collisions

64. One motivation for **explainable AI (XAI)** in security-sensitive applications (such as loan approval or recidivism prediction) is that:

    (a) It guarantees the model has no bugs

    (b) It allows stakeholders to understand and challenge decisions, improving trust and accountability

(c) It always increases accuracy

(d) It eliminates the need for testing

65. In a security context, combining encryption, access control, logging, and human training together to protect an asset is an example of:

    (a) Security by obscurity

    (b) Defense in depth

    (c) Open design

    (d) Single point of failure

PART B – Problem-Solving and Short-Answer Questions

Instructions: Answer all questions. Show your work for any calculations and clearly justify your reasoning for conceptual questions. Where appropriate, you may use diagrams, tables, pseudocode, or equations.

1. **CIA Goals in Context** For each of the following brief scenarios, identify *which CIA goal(s)* (Confidentiality, Integrity, Availability) are at risk, and explain *in one or two sentences* why.

   a) A university transcript database is misconfigured so that anyone on the campus network can browse students' grades without logging in.

   b) An attacker tampers with a software update server and replaces a legitimate patch with a malicious one that installs spyware.

   c) A cloud-based learning management system (LMS) crashes during final exams week and remains unavailable for 6 hours.

2. **Threat Types and Attack Classification** Given the attack categories {*eavesdropping, alteration, denial-of-service, masquerading, repudiation, correlation, traceback*}, classify the primary attack type in each case and justify briefly:

   a) An ISP intentionally drops 30% of VoIP packets for a competitor's traffic, making their service unusable.

   b) An intruder logs into a CEO's account using stolen credentials and sends fraudulent emails to staff.

   c) A government agency monitors timing and volume of encrypted messages to link accounts across different messaging platforms, even though it cannot see message contents.

3. **Access Control Matrix, ACL, and RBAC Design**

   A small company has three subjects: *Alice (Manager)*, *Bob (Engineer)*, *Eve (Intern)* and three objects: *HR_Records*, *Source_Code*, *Public_Docs*. Possible rights are **read (R)**, **write (W)**, and **execute (X)**.

a) Propose a reasonable Access Control Matrix that captures typical permissions for each subject on each object.

b) Convert your matrix into an **Access Control List (ACL)** representation (list the ACL for each object).

c) Propose at least two RBAC roles (e.g., Manager, Engineer, Intern) and show how your matrix could be implemented by assigning users to roles.

4. **Password Space and Entropy**

   Assume passwords are chosen uniformly at random from a given character set.

   a) Suppose passwords are exactly 10 characters long using 26 lowercase letters and 10 digits (total 36 symbols). Compute the total number of possible passwords and the entropy in bits.

   b) Explain in 2–3 sentences why increasing both password length and character set size increases resistance to brute-force attacks.

5. **Password Vulnerabilities and Salting**

   a) Briefly describe two common password vulnerabilities (e.g., reuse, weak composition, password sharing) and give a concrete example of each.

   b) Explain, step by step, how adding a unique random salt to each password before hashing mitigates rainbow-table attacks, and why two users with the same password no longer produce identical hashes.

6. **Buffer Overflow Root Cause and Mitigation**

   Consider the following C code:

```
void process() {
    char buffer[16];
    char input[64];
    strcpy(buffer, input); // unsafe
}
```

a) Explain precisely how this function can lead to a buffer overflow and what parts of memory may be overwritten.

b) Rewrite the critical part of the code using a safer C library function and a length check to prevent the overflow.

c) List one compile-time defense and one run-time defense against buffer overflow (e.g., stack canaries, ASLR) and briefly explain how each helps.

7. **Malware Scenario and Botnets**

An organization notices that many of its workstations periodically connect to an unknown IP address on a non-standard port and then participate in large outbound traffic spikes that do not match normal business patterns.

a) Explain how this behavior is consistent with a **botnet** infection.

b) Describe one likely method by which the malware initially spread to these machines.

c) Propose two defensive measures (technical or procedural) the organization could take to detect or prevent future botnet infections.

8. **Intrusion Detection System and Malware**

a) Briefly explain the difference between Firewall and Intrusion Detection System.

b) Briefly explain what Virus, Trojan, and Worm are.

c) Differentiate between White-list and Black-list Firewall.

d) Consider the following cybersecurity scenarios. Indicate whether each one represents a penetration test or a security test.

Table 1: Security Activities: Penetration Test (P) vs. Security Test (S)

#	**Activity**	**P**	**S**
i	Attempting to exploit a misconfigured web server to gain unauthorized access during an authorized assessment.		
ii	Reviewing organizational password policies to determine whether they meet current security standards.		
iii	Evaluating whether the company's incident-response procedures are being followed in practice.		
iv	Conducting a controlled vulnerability scan to identify outdated software versions across the network.		
v	Simulating a phishing attack against employees to test their susceptibility to social-engineering threats.		

9. **DNS Resolution and Attack Surface**

    a) List and briefly describe the main steps in resolving `www.bank.com` from a client's perspective, starting from the browser to obtaining an IP address.

    b) Identify two different points in this process where an attacker could interfere (e.g., DNS cache poisoning, rogue DNS server) and explain the impact of each.

10. **IPv4 Subnetting**

    Consider the network `192.168.10.0/27`

a) Write the subnet mask in dotted-decimal notation.

b) Compute the number of usable host addresses in this subnet.

c) Determine the network address and broadcast address.

d) Suppose you need at least 50 usable hosts in a single subnet. Explain briefly why `/27` is insufficient and what prefix length would be required instead.

If a network has an IP address of **198.168.9.120/25**

(a) What is the subnet mask of the network (3 points)

(b) What is the number of usable hosts in the network? (3 points)
Hint: Usable Hosts = Total hosts - 2

(c) What is the range of the network host IPs? (4 points)

11. **ARP Poisoning Scenario**

On a local LAN, a malicious host wants to intercept all traffic between a victim workstation and the default gateway without physically rewiring anything.

a) Describe how ARP poisoning (ARP spoofing) can be used to achieve this man-in-the-middle position.

b) Explain the effect on the victim's ARP cache and routing behavior.

c) Suggest two concrete mitigations (e.g., dynamic ARP inspection, static ARP entries, network segmentation) and the trade-offs involved.

Consider two nodes in a network, given the following ARP states:

```
Node 1:
IP: 192.168.6.96
MAC: 00:15:24:36:41:07

Node 2:
IP: 192.168.5.98
MAC: 00:15:22:30:40:09
```

```
Attacker:
IP: 192.168.7.120
MAC: 00:15:20:48:20:10
```

(a) What is the state of ARP tables of Node 1 and Node 2 after ARP poisoning? (5 points)

(b) List two mitigation strategies to prevent the ARP poisoning. (5 points)

12. **Flow Control vs. Congestion Control**

a) Conceptually distinguish between *flow control* and *congestion control* in TCP/IP networks.

b) Give one concrete example or mechanism for each (for example, TCP sliding window for flow control and TCP congestion window with slow start/AIMD for congestion control).

13. **Base Rate Fallacy in IDS**

Suppose only 1% of network connections are actually malicious. An IDS has a true positive rate of 99% (detects 99% of real attacks) and a false positive rate of 5% (5% of benign connections are incorrectly flagged).

a) If you observe an alert, explain why it is *not* necessarily very likely that this alert corresponds to a real attack, even though the true positive rate is high.

b) In 100,000 total connections, estimate roughly how many alerts would be false positives vs. true positives, and briefly discuss the operational impact on analysts.

14. Consider the following cookies:

(a)
```
name = cookie1
value = a
domain = account.microsoft.com/
path = /
```

(b)
```
name = cookie2
value = b
domain = microsoft.com
path = /my/account
```

(c)
```
name = cookie3
value = c
domain = microsoft.com
path = /
```

Given three URLs:

(a) support.microsoft.com

(b) account.microsoft.com/my/account

(c) microsoft.com.com/my/page

(d) microsoft.com/my/home

Indicate if each cookie can be generated or run on each domain. If not. give the reason.

15. **Euclidean Algorithm and Modular Inverse**

    a) Use the Euclidean Algorithm to compute $\gcd(276, 345)$. Show each step.

    b) Using the Extended Euclidean Algorithm or otherwise, find an integer x such that $17x \equiv 1 \pmod{72}$. Clearly show your reasoning.

16. **Small RSA Example**

    Let $p = 13$, $q = 19$, and $e = 5$.

    a) Compute $N = pq$ and $\phi(N)$.

    b) Find the corresponding private exponent d such that $ed \equiv 1 \pmod{\phi(N)}$.

    c) Encrypt the message $M = 7$ to obtain ciphertext $C \equiv M^e \pmod{N}$.

    d) Show that decrypting C with d recovers the original message M.

    Let $p = 17$, $q = 29$, public exponent $e = 3$, and message $M = 100$.

(a) Compute $N = pq$ and $\phi(N)$.

(b) Find the private exponent d such that $ed \equiv 1 \pmod{\phi(N)}$.

(c) Encrypt the message: $C \equiv M^e \pmod{N}$.

(d) Decrypt the ciphertext: $M' \equiv C^d \pmod{N}$ and confirm that $M' = M$.

17. **k-Anonymity Transformation**

A hospital has the following microdata (similar to your assignment):

ZIP Code	Age	Gender	Disease
47677	29	F	Flu
47677	27	F	Cancer
47678	43	M	Flu
47602	45	M	Diabetes
47602	47	M	Cancer
47605	31	F	Flu

The quasi-identifiers (QIs) are **ZIP Code, Age, Gender**, and the sensitive attribute is **Disease**. The publisher wants to achieve **3-anonymity**.

a) Explain in your own words what it means for this table to satisfy 3-anonymity with respect to the QIs.

b) Propose one possible anonymized version of the table that satisfies 3-anonymity (using generalization and/or suppression).

c) Briefly discuss one trade-off between data *utility* and *privacy* in your anonymization.

18. **Cyber Forensics Process and Evidence Handling**

A financial company suspects that an employee copied confidential customer data to a USB drive and emailed it to an external address.

a) Outline the main phases of a typical digital forensic investigation (e.g., acquisition, preservation, analysis, reporting) and briefly describe what occurs in each phase *for this case.*

b) Explain why maintaining a proper **chain of custody** and using **hashes** (e.g., SHA-256) on acquired images are critical for admissibility in court.

19. **Social Engineering Email Analysis**

    You are given the following email (paraphrased): *"Dear Student, Our records show an urgent problem with your financial aid disbursement. If you do not confirm your bank details within 24 hours, your payment will be cancelled. Please click the link below and log in using your university credentials to avoid losing your funds. Sincerely, Financial Aid Office"* (link points to `gsu-payments.com` not `gsu.edu`).

    a) Identify at least three red flags that indicate this message may be a phishing attack.

    b) For each red flag, explain which social engineering principle or cognitive bias it exploits (e.g., urgency, authority, scarcity, fear).

    c) Suggest two technical controls and two user-awareness measures that a university can deploy to reduce the success rate of such phishing campaigns.

20. **Security of Machine Learning Applications**

    A company deploys an image classification model in a self-driving car to recognize traffic signs. Security researchers demonstrate that adding carefully crafted stickers to a stop sign causes the model to classify it as a speed-limit sign, even though humans still clearly see a stop sign.

    a) Explain why this is an example of an **adversarial example** and discuss the potential safety impact.

    b) Describe two possible defenses or robustness strategies (technical or procedural) that could reduce the risk of such attacks (e.g., adversarial training, input sanitization, model ensembles, multi-sensor fusion).

    c) Briefly discuss how fairness, accountability, and transparency (FATE) considerations might also be relevant when deploying ML models in safety-critical or high-stakes environments.