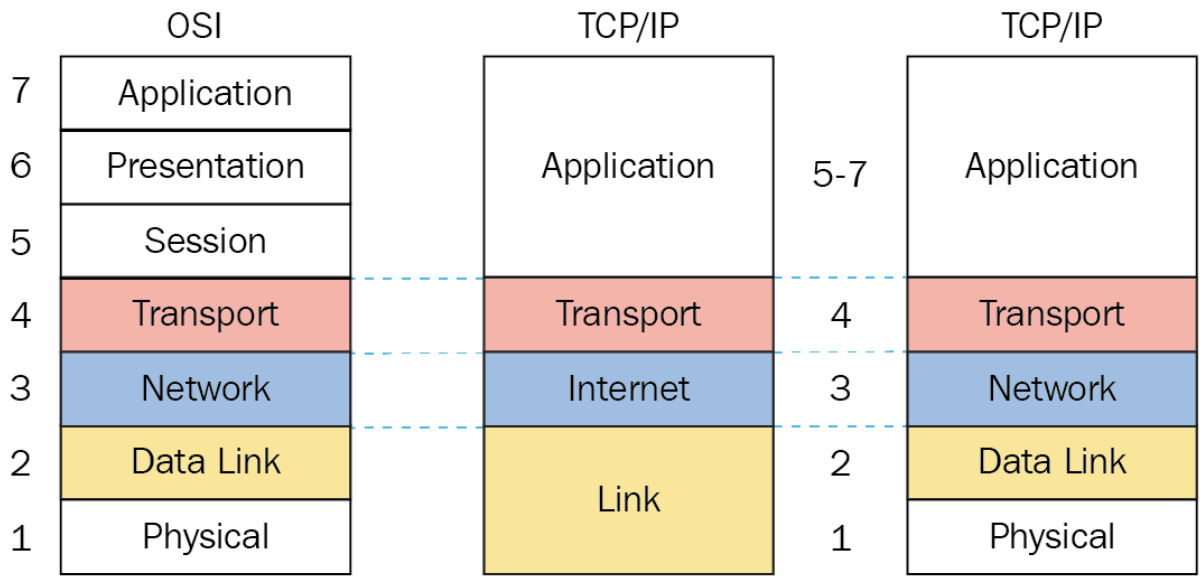
Tutorial Worksheet A

Exercise 01 (Networking) :

1. Considering the TCP/IP suite:



Completing the following table:

Protocol		Layer	Description
TCP	Transmission Control Protocol	Transport	Establish maintenance , reliable connection between applications.
UDP	User Datagram Protocol	Transport	Connectionless and fast transport layer protocol for quick data transmission, often used in real-time applications like gaming and streaming.
TLS	Transport Layer	Transport	Cryptographic protocol, ensures secure internet

	Security		communication by encrypting data between applications like web browsers and servers.
SSL	Secure Sockets Layer	Transport	Deprecated cryptographic protocol for secure communication on the internet, replaced by TLS.
HTTP	Hypertext Transfer Protocol	Application	The foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted, enabling the exchange of text, images, and other multimedia content between web browsers and servers.
HTTPS	Hypertext Transfer Protocol Secure	Transport/ Application	Secure version of HTTP, utilizing TLS encryption to safeguard data transmitted between a user's web browser and a website's server.
DNS	Domain Name System	Application	Translates user-friendly domain names into numerical IP addresses, facilitating internet communication by making websites accessible with easy-to-remember names.
DHCP	Dynamic Host Configuration Protocol	Application	Automates the assignment of IP addresses and network configurations, simplifying the process of connecting devices to a network.
ARP	Address Resolution Protocol	Network	Maps IP addresses to MAC addresses on a local network, facilitating communication between devices in the same network.
ICMP	Internet Control Message Protocol	Network	Sends error messages and operational information, essential for diagnosing network issues and supporting tools like ping.
IGMP	Internet Group Management Protocol	Network	Manages membership in multicast groups on IP networks, enabling efficient distribution of multicast traffic to interested devices.
Telnet	Telecommunication Network	Network	Allows a user to remotely access and control another device over a network, typically the internet. It transmits data in plain text, lacking encryption, and is often replaced by more secure alternatives like SSH.
SSH	Secure Shell	Network	Used for secure remote access and file transfers, ensuring the confidentiality and integrity of data.
SMTP	Simple Mail Transfer Protocol	Application	Used for sending emails between servers. It defines the rules for mail transfer, allowing email clients to

			send messages to a mail server for further distribution. SMTP is essential for the reliable transmission of emails across the internet.
IMAP	Internet Message Access Protocol	Application	Enables users to access and manage their email messages directly on a mail server. This allows for synchronization across multiple devices, providing a consistent view of the mailbox regardless of the device being used.
OSPF	Open Shortest Path First	Network	Dynamically calculates optimal data packet paths in computer networks by considering factors like network topology and link costs, ensuring efficient routing in large-scale enterprise environments.
POP3	Post Office Protocol 3	Application	An email retrieval protocol that allows users to download messages from a mail server to their local devices. Messages are usually removed from the server upon download, and POP3 is commonly used for managing emails on a single device.
Ethernet	Ethernet Protocol	Data Link	A widely used networking technology defining how data is transmitted over local area networks (LANs), commonly utilizing twisted-pair cables.
SMB	Server Message Block	Application	A network protocol for sharing files and resources between devices in a local network, enabling seamless communication and file access.
SNMP	Simple Network Management Protocol	Application	A standard protocol for managing and monitoring network devices, facilitating information collection and performance monitoring by network administrators.
RPC	Remote Procedure Call	Application	Allows programs to request services or procedures from remote servers, facilitating distributed computing by enabling communication and code execution across a network.
BGP	Border Gateway Protocol	Network	Facilitates the exchange of routing information between different autonomous systems, playing a critical role in determining efficient data paths across the global network.
RARP	Reverse Address Resolution Protocol	Data Link	Maps hardware addresses to IP addresses, providing a way for devices to discover their IP addresses

			based on their physical addresses. It has been largely replaced by more modern protocols like DHCP.
NFS	Network File System	Application	Allows files and directories to be shared seamlessly across a network, enabling remote access and collaboration as if the files were on the user's local machine.
RIP	Routing Information Protocol	Network	Helps routers share information about the best paths within a network, using a distance vector algorithm. It is suitable for smaller networks but may have limitations in larger and more complex setups.
IPv4	Internet Protocol version 4	Network	IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are addressing schemes used to identify and locate devices on a network. IPv4, the older protocol, uses 32-bit addresses, limiting the number of unique addresses to around 4.3 billion. IPv6, introduced to address the IPv4 address exhaustion issue, utilizes 128-bit addresses, providing an almost limitless number of unique addresses.
IPv6	Internet Protocol version 6	Network	
BOOTP	Bootstrap Protocol	Network	Used by devices to obtain configuration information, like IP addresses, during the bootstrap or reboot process. It is a predecessor to DHCP, offering essential network parameters for initialization.
FTP	File Transfer Protocol	Application	Used for transferring files between a client and a server. It provides a simple and efficient way to upload and download files, making it widely used for various purposes, including website management and file sharing.
TFTP	Trivial File Transfer Protocol	Application	A lightweight version of FTP used for simple and quick file transfers, particularly for tasks like booting software images on devices such as routers and switches. It operates on a connectionless basis.
UPnP	Universal Plug and Play	Network	Automatically connects devices on a local network, simplifying setup but potentially introducing security risks.

Most Communications that happen in the internet use Server/Client, the Server/Client paradigm serves for authentication. (Lasla)

2. Selecting all application-level protocols from the above list and assigning to them their corresponding communication port. Certain protocols use multiple ports.

Application-level Protocols	Port(s)
HTTP (Hypertext Transfer Protocol)	80
HTTPS (Hypertext Transfer Protocol Secure)	443
DNS (Domain Name System)	53
DHCP (Dynamic Host Configuration Protocol)	• DHCP Server (UDP): 67 • DHCP Client (UDP): 68
Telnet	23
SSH (Secure Shell)	22
SMTP (Simple Mail Transfer Protocol)	25
SMTPS (Simple Mail Transfer Protocol Secure)	465
IMAP (Internet Message Access Protocol)	143
IMAPS (Internet Message Access Protocol Secure)	993
POP3 (Post Office Protocol version 3)	110
POP3S (Post Office Protocol version 3 Secure)	995
SMB (Server Message Block)	• SMB over NetBIOS (unsecured): 139 • SMB over TCP/IP (unsecured): 445
SNMP (Simple Network Management Protocol)	• SNMP queries: 161 (UDP) • SNMP traps (asynchronous notifications): 162 (UDP)

FTP (File Transfer Protocol)	• FTP Control Connection: 21. • FTP Data Connection: 20.
TFTP (Trivial File Transfer Protocol)	69

Note: To find information about a specific internet protocol use. Type "RFC" followed by the name of the protocol.

3. Listing the set of protocols that are used within your local network when you open a terminal on your PC and execute the command **$ping www.ensia.edu.dz**, for the very first time.

DNS in TCP/UDP in IP in Ethernet to resolve the domain name into an IPv4 address.

ICMP in IP in Ethernet to send/receive ping requests/responses to/from ensia web server.

4. Describing how NAT operates when the two computers simultaneously send ping requests to a same destination, e.g., www.ensia.edu.dz.

When both computers send their ping requests message, their gateway runs NAT to replace the private ip address source with the public one and since there is no port, the gateway records identification number + sequence number of the ICMP request. When the response is received, the gateway

will use the recorded information (identification number + sequence number) to determine to which computer the response should be given to after replacing the public address with the corresponding private addresses.

Note: We need both identification number and sequence number with NAT for pings because:

> **ID:** Distinguishes entire ping exchanges, even if from the same device (ideal scenario).
> **Sequence number:** Differentiates multiple pings within a single exchange, especially when the same device sends multiple pings quickly (ID might be reused accidentally).

5. Explaining how routers, which typically operate on Layer 3, perform natting (NAT), a process that requires access to communication port fields in TCP and UDP segments (Layer 4).

While routers traditionally operate at Layer 3 (network layer), they can perform NAT (Network Address Translation) by examining information from Layer 4 (transport layer). This is achieved through a process called cross-layer interaction.

6. Listing the set of protocols that are used within your local network when you open a web browser on your PC and type https://www.ensia.edu.dz , for the very first time.

https -> http in TLS in TCP in IP in Ethernet.

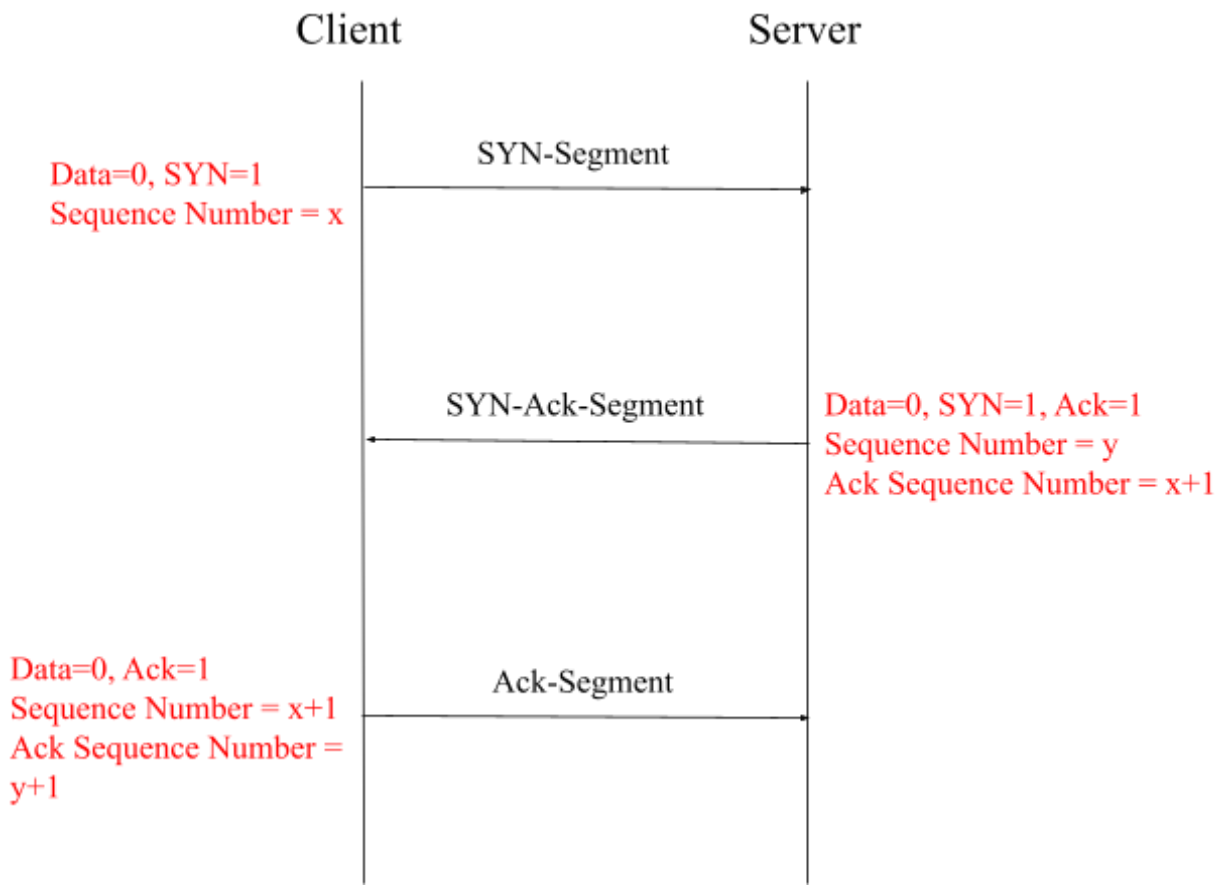
> **Ethernet:** Transfers data over the physical network cable.
> **IP:** Routes data packets between devices using their IP addresses.

TCP: Ensures reliable data delivery by breaking it into packets and reassembling them.
TLS (over HTTP): Encrypts communication for secure data exchange.
HTTP: Requests and receives web content from the server.

7. Application protocols that send their data in plaintext:

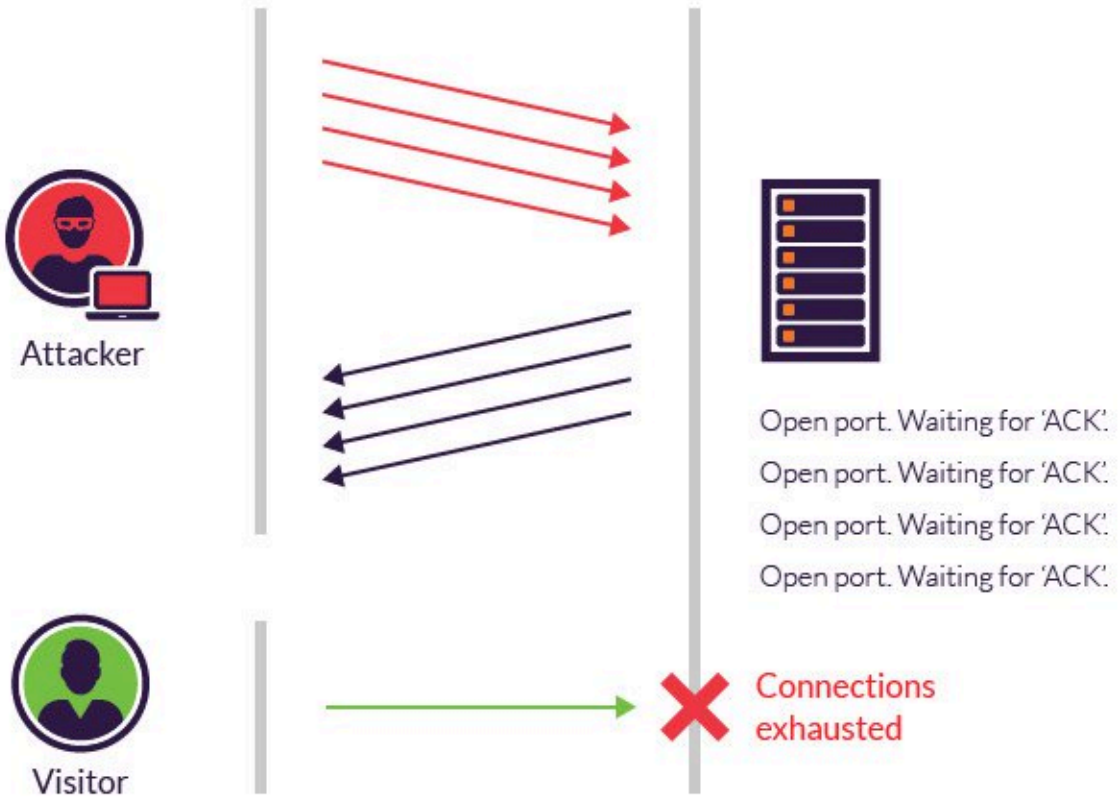
HTTP, DLS, DHCP, TELNET, SMTP, IMAP, POP3, FTP, TFTP, SMB before V3, SNMP before V3, UPnP, RPC (Depends on implementation), NFS before V3, BOOTP.

8. TCP three-way handshake process:



9. Exploitation of the TCP three-way-handshake:

TCP flooding attack or SYN flood attack, the client initiates the attack by sending a TCP segment to the server. Upon receiving the first segment, the server allocates a certain amount of memory (which depends on the operating system) to handle the connection. However, if the client quickly changes ports and sends TCP SYN packets on various ports simultaneously, and either not responding to the server's SYN-ACK packets or spoofing the source IP address, the server's memory resources may become exhausted. As a result, the server becomes unable to handle connection requests from other clients, leading to a denial of service as you deny the service from other clients.



10. Describing what happens when a user sends a ping request with an ICMP’s data field carrying around 65,900 bytes of data:

In the standard specifications an IP datagram can have a maximum size of 65535 bytes (2^16 - 1) , with 20 bytes reserved for the header and 65515 bytes for the data. Since the ICMP packet is encapsulated within an IP packet, the maximum size of the ICMP data is further reduced to 65509 bytes (65515 - 8 bytes for the ICMP header).

In this case, the ping request with ICMP’s data field carrying around 65,900 bytes of data would result in a datagram size of 65928 bytes when combined with the ICMP header (8 Bytes) and IP header (20 Bytes). This exceeds the allowed maximum size, and therefore the datagram would be fragmented into smaller IP packets for transmission. However, it is important to note that most modern operating systems and network devices do not allow such large ICMP packets to be sent, as it can lead to vulnerabilities.

In the past, older operating systems like MAdos, Microsoft Windows 95, Windows NT, Windows 3.11, MACOS7, Sun Solaris (X-95 2.4 and 2.5), and Linux versions prior to 2.0.23 were vulnerable to a specific type of attack known as "ping of death." In this attack, the attacker would send a ping with a payload larger than what the target operating system is capable of handling. When the fragmented packets were reassembled at the destination, it could cause buffer overflow in internal variables, leading to the crashing of the entire operating system, often resulting in the infamous "blue screen of death" error.

Ping of death -> buffer overflow -> Blue screen of death

Exercise 02 (Password-based Authentication) :

1. Five different approaches to defeat password-based authentication:

Offline Password Guessing: The attacker performs guessing without interaction with the authentication server, meaning cracking users password given its hash stored in **etc/shadow**. We have mainly two cases:

Dictionary based attack: The attacker uses a huge list of possible passwords (Most common + leaked passwords from the internet).

Bruteforce based attack: The attacker tries all possible combinations. Brute force is 100% reliable but takes infinitely time.

During an offline attack there is no risk that the password may be changed by the user during the cracking process.

Online Password Guessing: The attacker interacts with the authentication server by trying several passwords.
The server may limit the number of attempts per time unit or per network bandwidth or based on the server computational power (how many requests can the server handle).

Social engineering: The attacker uses different techniques, he tries to deceive the users to reveal their passwords using:

Shoulder Surfing: Spying on someone entering sensitive information by looking over their shoulder, typically to obtain passwords or PINs.

Dumpster Diving: Searching through discarded materials, like trash, to find information for malicious purposes, such as identity theft, often involving personal documents.

Eye sneaking: Secretly observing or spying on someone without their awareness or permission.

Phishing: Cyber attack where attackers deceive individuals into revealing sensitive information, like usernames and passwords, by posing as a trustworthy entity in electronic communication.

Where victims are deceived to input their passwords in a form they believe is secure, where actually it is managed by the attacker.

2. An algorithm that exploits the file **p_hash** to crack the password of arbitrary registered users (i.e., trawling).

Step One: Construct a long list of candidates denoted as $w_1, w_2, \ldots, w_n$.

Step Two: For each password w_j compute h_j (h_j = Hashing(w_j)) and store them in a table T (Rain-Bow Table) of pairs (h_j , w_j) sorted based on h_j in ascending order. This table allows for faster hash lookups during the cracking process.

Step Three: Steal the password file **p_hash** containing all the usernames and their corresponding passwords' SHA512-hashes P_i sorted in ascending order.

Step Four: Compare the two sorted tables T and **p_hash** and look for a matching hash values (H(P_i), H(w_j)). This may yield many matching pairs. The corresponding password candidate w_j from T can be used as a potential user password for the password P_i .

One of the most known software tools that implement this algorithm is **John The Ripper**.

3. Solutions (countermeasures) to make the above system more secure and immune to classical password-cracking attacks than it currently is.

-Using passphrases are generally longer and more complex than traditional passwords, making them resistant to brute-force attacks..

-Implementing slow hashing techniques such as iterated hashing or Lamport hash chains not only increases the time it takes to generate hash values during password creation (hashing time) but also significantly extends the time required for attackers to crack passwords (cracking time).

-Using salting hashing where a random seed is concatenated to the password hashing. If we have a seed of n-bits, complexity will increase by 2^n for attackers trying to crack passwords. But if the seed becomes known, the attackers could construct tables (Rainbow Tables) based on the seed,

-Using pepper hashing (secret salt) is similar to salt hashing, but the attacker cannot deduce the secret value.

Note: In salt hashing, the salt is considered public information and is stored alongside the hashed password in the database. In pepper hashing, the pepper is kept confidential and is not stored with the hashed passwords.

4. Discuss attack scenarios where explaining that the term “strong” is not always strong (misleading term).

The word strong in indeed misleading because the passwords can be found using:
-Social engineering.
-Reverse social engineering (a form of manipulation that involves an attacker

convincing a targeted individual to take actions or divulge sensitive information by posing as someone who needs help or assistance).

5. Dealing with passphrases instead of passwords.

Passphrases, when properly implemented, can provide a higher level of security compared to traditional passwords, but still no authentication method is completely immune to all possible attacks.

6. Considering a system that implements a password recovery mechanism where the user is asked to answer some security questions, input a confirmation code (received on the mobile-phone), and respond to a CAPTCHA challenge.
Proposing a malicious scenario, where an attacker misleads a legitimate user to unawarely answer all those password reset questions and manage to reset the password, locking the legitimate user out.

Interleaving attack: a security threat in which an attacker strategically inserts their malicious actions within the normal operations of a system or user, aiming to compromise security measures or gain unauthorized access. This involves weaving malicious actions into the sequence of legitimate events, making detection and prevention challenging.

User Initiates Password Recovery:

- Legitimate User (LU) starts the password recovery process.
- The system generates a set of security questions.

Attacker Intercepts Security Questions:

- Attacker (A) intercepts the security questions sent to LU.

Attacker Impersonates System:

- A sends fake security questions to LU, pretending to be the legitimate system.
- LU unknowingly answers the fake security questions.

System Sends Confirmation Code:

- Legitimate system sends a confirmation code to LU's mobile phone.

Attacker Intercepts Confirmation Code:

- A intercepts the confirmation code sent to LU.

Attacker Tricks LU to Enter Confirmation Code:

- A sends a fake message to LU, claiming to be the legitimate system.
- LU unknowingly enters the confirmation code into the fake system.

LU Responds to CAPTCHA Challenge:

- Legitimate system presents a CAPTCHA challenge to ensure human interaction.
- LU responds to the CAPTCHA challenge.

Attacker Simulates CAPTCHA Challenge:

- A simulates a fake CAPTCHA challenge and tricks LU into *responding.*

Attacker Gathers Information:

- A has now gathered security question answers, confirmation code, and CAPTCHA response.

Attacker Initiates Password Reset:

- A, armed with all the gathered information, initiates the password reset process on the legitimate system.

System Resets Password:

- The legitimate system, perceiving A as the legitimate user, resets the password.

Legitimate User Locked Out:

- LU, unaware of the attack, is now locked out of their account.

7. Password managers and Master Password.

Password managers are tools designed to help users securely store and manage their passwords for various online accounts. The primary purpose of a password manager is to generate strong, unique passwords for each of your accounts and store them in an encrypted vault. Instead of having to remember multiple complex passwords, users only need to remember a single strong password, often referred to as the master password to unlock the password manager and access their stored credentials.

Password managers employ two main approaches:

password wallet (vault): Securely stores and manages actual user credentials (username and password) in an encrypted database, requiring users to remember only a single master password for access.

Derived passwords: Generates unique passwords for each service or website based on a combination of factors, often including the master password and the website's domain, without storing the actual passwords, providing dynamic and secure access.

- *Explaining how some password managers provide a certain resistance against phishing:*
  Certain password managers provide extra protection against phishing attacks. When you log in to a website, the password manager remembers that your password is associated with that specific site. If someone tries to trick you with a fake website, the password manager detects that your password doesn't match the fake site and alerts you. this extra check helps you spot and avoid entering your login details on fake websites, giving you better protection against phishing attacks.
- *Analyzing password managers' security to show that it delivers fewer security advan-tages (usability, efficiency, ...) than expected (they are password "concentrators"):*
  Password managers, acting as password "concentrators," store multiple

passwords under one master password. If the master password is compromised, all other passwords become vulnerable and if the master password is leaked there is no way to recover it. Moreover the master password, often user-chosen, is susceptible to offline and online guessing attacks.

- *Among web-based password managers, there is PwdHash from Stanford university:*
  PwdHash uses the derived passwords approach, it is not as widely used today because other alternative solutions have flooded the market such built-in browser password managers (They store and autofill the actual passwords that users enter or save during their online activities e.g., Google Chrome, Mozilla Firefox, Safari, Microsoft Edge).

8. Five disadvantages related to the graphical-password schemes:

1. People with certain disabilities may face challenges when using graphical passwords due to factors such as limited mobility, impaired vision, or cognitive difficulties.
2. Graphical passwords are mainly made for touchscreens on smartphones, tablets, and new computers. They might not work well on older devices.
3. Many people choose easy patterns, making it easier for others to guess their passwords.
4. Smurf attacks, like detecting traces left on the screen.
5. Some graphical-password systems may have limitations in the complexity and diversity of images or patterns users can choose, potentially reducing the overall security of the authentication method.

9. Three possible attack scenarios where an attacker may bypass CAPTCHA authentication using a malicious program.

- Using Machine Learning algorithms to solve CAPTCHAs.
- Recruit some human specialists in solving CAPTCHAs.
- OCR (Optical Character Recognition).

Exercise 03 (Security Services) :

1. The five fundamental security services:

Authentication: Prove your identity: What you know/have/are and where you are.
Confidentiality: Protect information from being disclosed to unauthorized parties.
Integrity: Protect information from being modified while being stored or transferred or processed.
Availability: Guarantee that information system resources are available at all times.
Non-repudiation: Nobody denies having done (i.e., executed, sent, received, deleted, created, logged on/out, modified, ...) something in the system.

2. Providing two examples of mechanisms that are used in real-life to provide and guarantee a certain level of each fundamental service.

Authentication:

Passwords: Users must provide a unique combination of characters to access a system or account. The system verifies the entered password against a stored version.

Fingerprints: Biometric authentication uses unique physical attributes, such as fingerprints. Devices like smartphones and biometric scanners use fingerprints for user identification.

Confidentiality:

Encryption: Data is transformed into unreadable ciphertext using algorithms and keys. Only authorized parties with the correct decryption key can revert the data to its original form.

Access Control: Restricts access to data or resources based on user permissions. Users are granted specific privileges, and access is limited to what is necessary for their roles.

Integrity:

Hash Functions: Generate fixed-size hash values (digests) for data. Even a small change in the data results in a significantly different hash, allowing detection of alterations.

Physical Protection: Secure physical environments, such as data centers or server rooms, prevent unauthorized access and potential tampering with hardware.

Availability:

Resource Duplication: Utilizing redundant systems or resources to ensure continuous availability. For example, having multiple servers that can take over if one fails.

Physical Control: Implementing measures like fire suppression systems, climate control, and backup power supplies to protect against physical threats and ensure continuous operation.

Non-repudiation:

Digital Signature: Cryptographic techniques to sign digital messages or documents, providing a way to verify the sender's identity and ensuring that the sender cannot deny sending the message.

Trusted Third Parties: In transactions, a trusted third party (like a certificate authority) can validate the identities of involved parties and provide evidence in case of a dispute. This enhances non-repudiation by establishing trust in the transaction.

3. Proposing a ranking for those security services (i.e., from the most important to the least important) and provide arguments (examples) to support your proposition.

1. Authentication and non-repudiation (generally come first).
2. Availability.
3. Integrity.
4. Confidentiality.

4. Listing five other “non-fundamental” security services and explaining their function.

Authorization:
Definition: Authorization is the process of determining what actions authenticated users can perform within a system or network based on their roles or privileges.

Example: In a network, a user with a regular employee role might have read-only access to certain files, while an administrator might have full control and editing permissions.

Accountability:
Definition: Accountability involves tracking and recording user activities or system events to attribute actions to responsible parties.
Example: Logging systems record who accessed a particular file, when the access occurred, and what actions were taken. This information can be crucial for auditing, forensic analysis, and ensuring accountability.

Trust and Trustworthiness:
Definition: Trust and trustworthiness involve establishing confidence in the reliability and integrity of entities, such as systems, applications, or individuals.
Example: Users trust a secure and regularly updated software application because it demonstrates a commitment to addressing vulnerabilities and maintaining a trustworthy environment.

Privacy:
Definition: Privacy is the protection of an individual's personal information from unauthorized access or disclosure.
Example: Data encryption, access controls, and policies that limit data sharing are measures taken to ensure privacy. This is particularly important in handling sensitive information like personal details, financial records, or medical data.

Anonymity:
Definition: Anonymity allows individuals to conceal their identities when interacting online.
Example: Some online forums or communication platforms may allow users to participate without revealing their real names. This can provide a level of privacy and protection, but it also raises considerations about accountability and potential misuse.

5. Security services that may get compromised when a computer is infected by malware?

Malware: Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Authentication:

Malware can perform actions on behalf of the user, which may lead to compromised authentication. For example, it might capture login credentials, manipulate authentication processes, or conduct unauthorized activities using legitimate user accounts.

Confidentiality and Privacy:

Malware may read confidential information when accessed by authorized users. This compromises the confidentiality of sensitive data, as the malware can exfiltrate or expose private information. The unauthorized access to personal or sensitive data by malware also compromises the privacy of users, as their personal information may be stolen or misused.

Availability:

Malware can block access to resources for users, limiting the availability of services or data. For instance, a denial-of-service (DoS) attack caused by malware can overwhelm a system or network, making it inaccessible to legitimate users. Malware can also crash the system or the hard disk drive (HDD), leading to a loss of availability. This can render the affected system or data temporarily or permanently inaccessible.

Integrity:

Malware may change the content of system files, applications, or data,

compromising their integrity. This alteration can lead to the execution of unauthorized commands, modification of critical files, or corruption of data, impacting the overall integrity of the system.

6. Security serviced enforced by digital-watermarking:
Digital watermarking is a technique to embed a unique identifier, or "watermark," into digital content like images or documents. It serves purposes such as protecting copyright, verifying integrity, authenticating origin, tracing distribution, and creating content fingerprints. The watermark is typically imperceptible and helps identify and track digital content, providing security and authenticity.

Example: The use of security thread and certain watermarks on money bills to prevent counterfeiting and impersonation.

Exercise 04 (Security Policy) :

Aspects (Key Components)	Description	Related risks and threats
Scope and Purpose	The policy is set to make explicit rules, meaning what is allowed and what is supposed to be not allowed, and procedures to the employees and visitors, within the company.	If no such policy is present, then there are no legally-bound documents that would protect your company in case of damage.
Roles and Responsibilities	Explicitly and without Ambiguity defines who should do what, on which, and where. It specifies the responsibility of the users (who is legally responsible if an incident happens +	Without defining roles and responsibilities, there is nobody to blame if things go Wrong and security incidents occur. Also users do not know to whom they should turn to when incidents happen (e.g.,

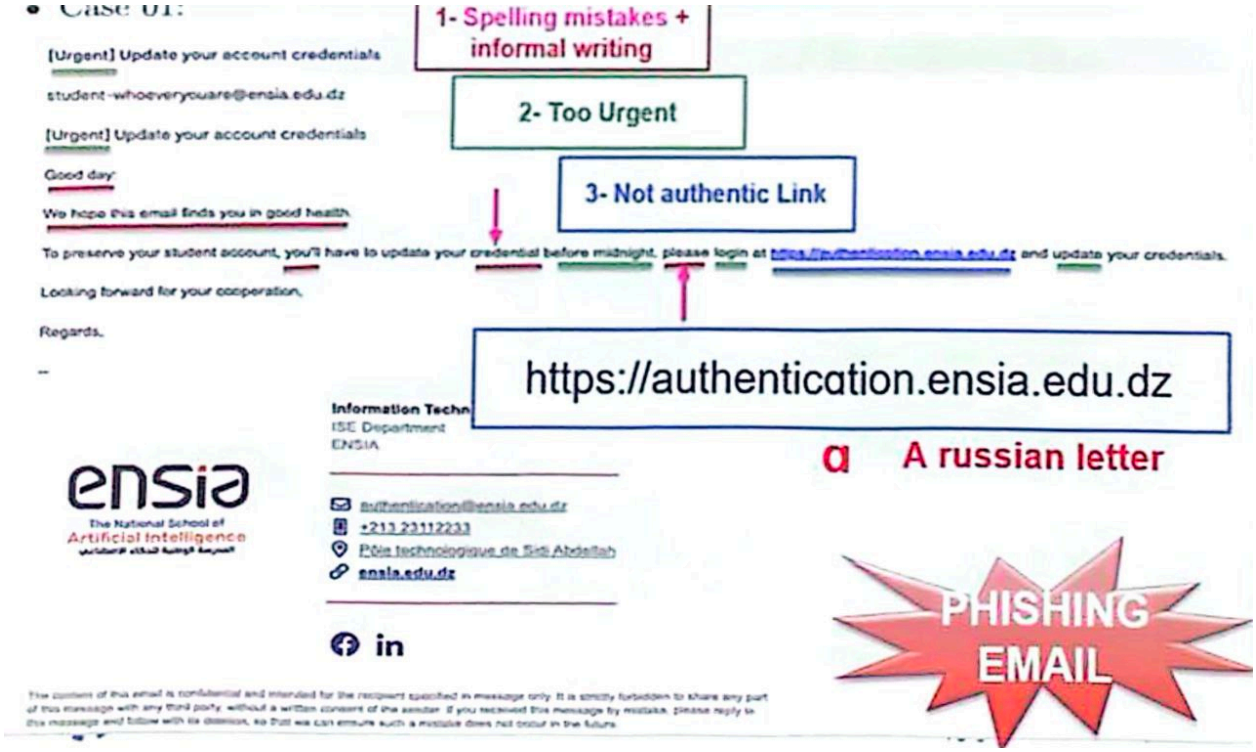
	consequences).	when detecting malicious activity).
Access Controls	Define who is allowed to access what, where and when. There are various mechanisms including physical security, access rights, etc.	Authenticated users are people who are assumed to be authorized to be part of the IT system, but there should be rules to hierarchically organize the users and assign to them different privileges on various resources of the IT system.
Data Classification	The data that is being manipulated within the company should be classified (Top secret, secret, confidential, internal, public,..).	If data is not classified, then data leakage will happen. Some people will access data that is not supposed to be accessible to them. There might be privacy violations as well.
Acceptable Use	Define how the company's IT resources should be used and how they should not be used.	If such rules are not defined, employees would use the IT infrastructure in an inappropriate manner, exposing the IT resources to security threats and possible physical damage.
Password Management	Define rules and procedures as per how passwords should be made and managed when used in the company's IT system.	If there are no such rules, employees may stick password notes On their monitors, Or use guessable passwords (e.g- 1234567 Or qwerty, and azerty).
Incident Response	There should be an explicit and unambiguous plan to follow when incidents happen.	If such a plan is missing, then when an incident happens things go in different directions, causing extra problems (e.g. from an attack to an intrusion).
Network Security	Define how the network components are secured (physical security + logical security - security protocols,	If the components of the network are not secured, then various attacks could take place, varying from cutting

	e.g., TLS, RADIUS Configuring Remote Authentication Dial-in User Service, MFA Multi-Factor Authentication...), as well as how their security is managed, and who should be involved and held responsible.	cables and spray-painting the cameras, to hacking into the servers and locking users out.
Physical Security	Define and implement security mechanisms and procedures to physically protect the company's IT system, covering physical, logical, and social resources.	If physical security is underestimated, the cables will be destroyed, the walls will be filled up with graffiti, and strangers will be walking around your company's corridors, and maybe your employees will be assaulted. Think about the tax-offices or their administrative offices: they use glass/acrylic separators between the agents and the citizens, why?
Security Awareness and Training	Employed individuals must be trained, sensitized, and have a sense of responsibility. They should be trained, and frequently “surprisingly tested to verify their incident response reaction”.	If the employees are not aware about the danger of cyber attacks and the consequences of taking things easy, the company may go through hard times and go bankrupt_ a spoiled reputation.
Compliance with Regulations	The company must check that the rules and procedures they would like to enforce are compliant with the local governmental regulations.	If no such verification, the procedures and rules may violate the privacy of others, which would result in lawsuit and juridic issues.

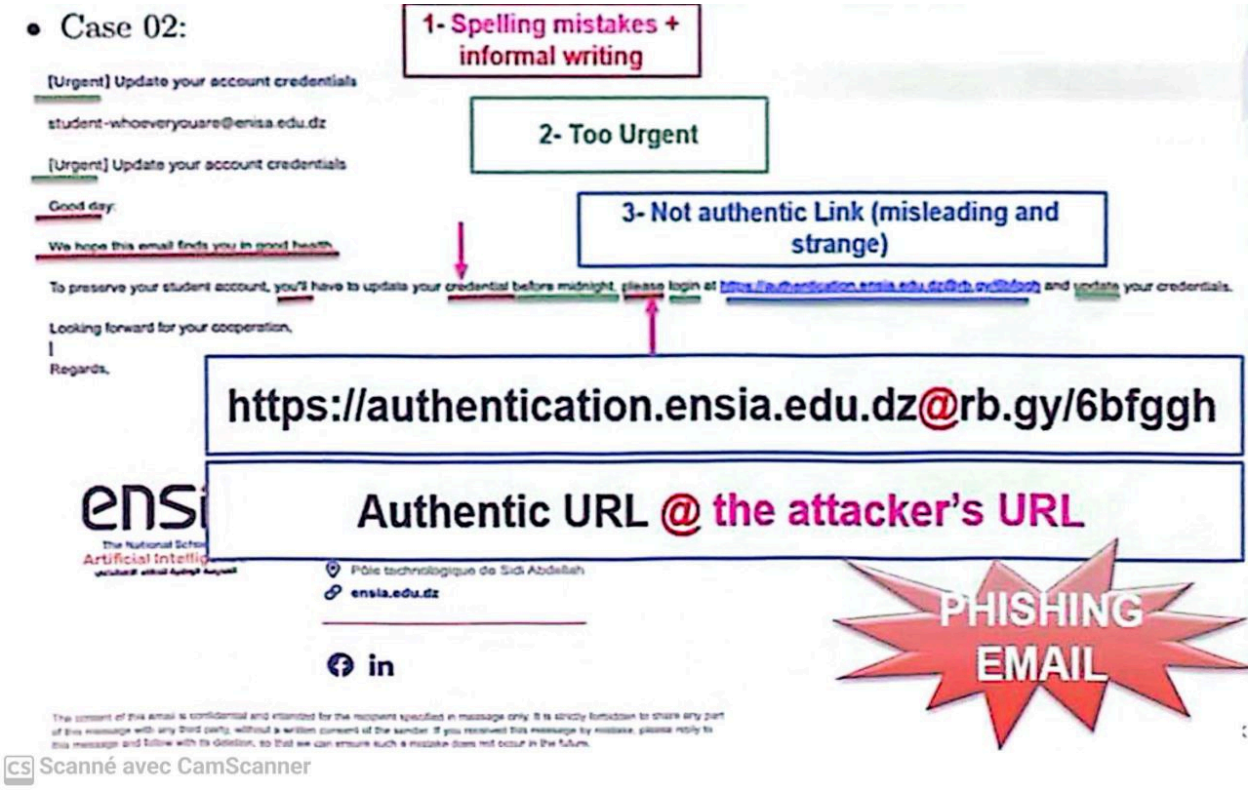
Exercise 5 (Phishing):

1. Determining phishing patterns that would classify each scenario as phishing attempts instead of legitimate communications.

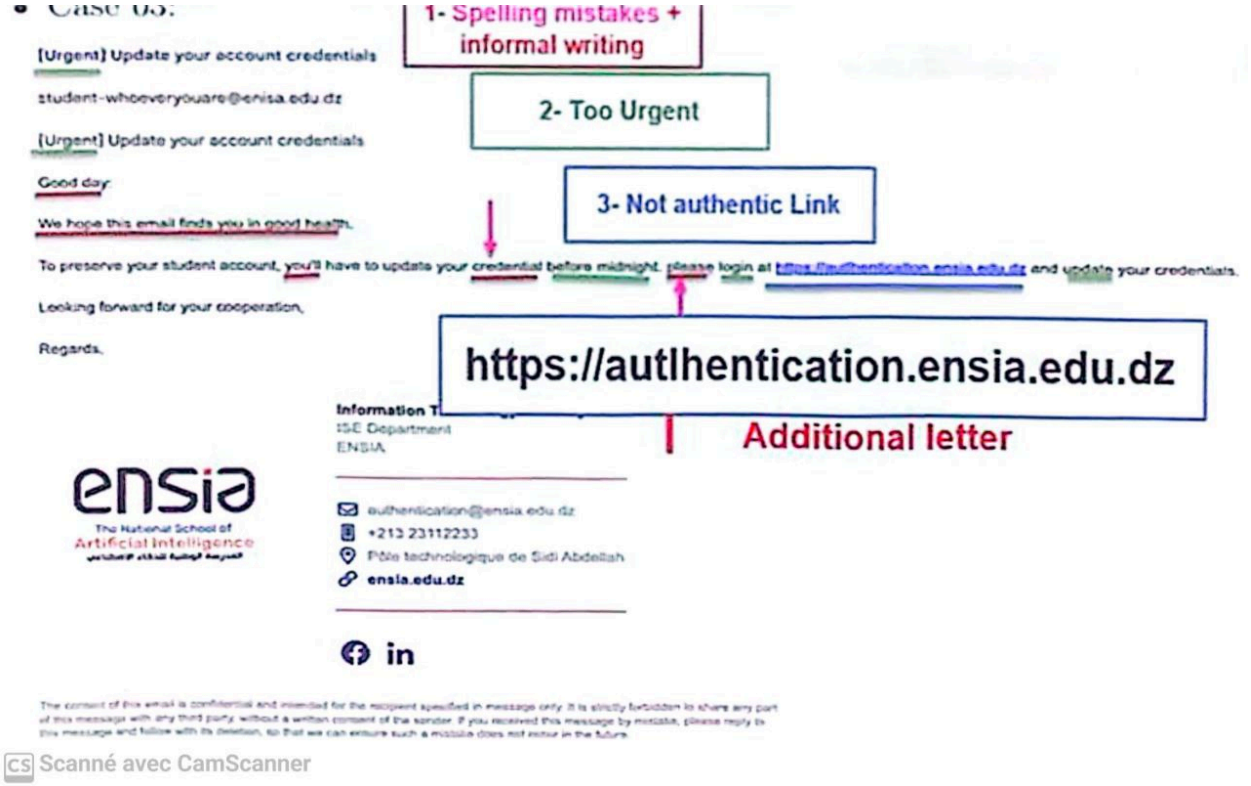
Case 01:



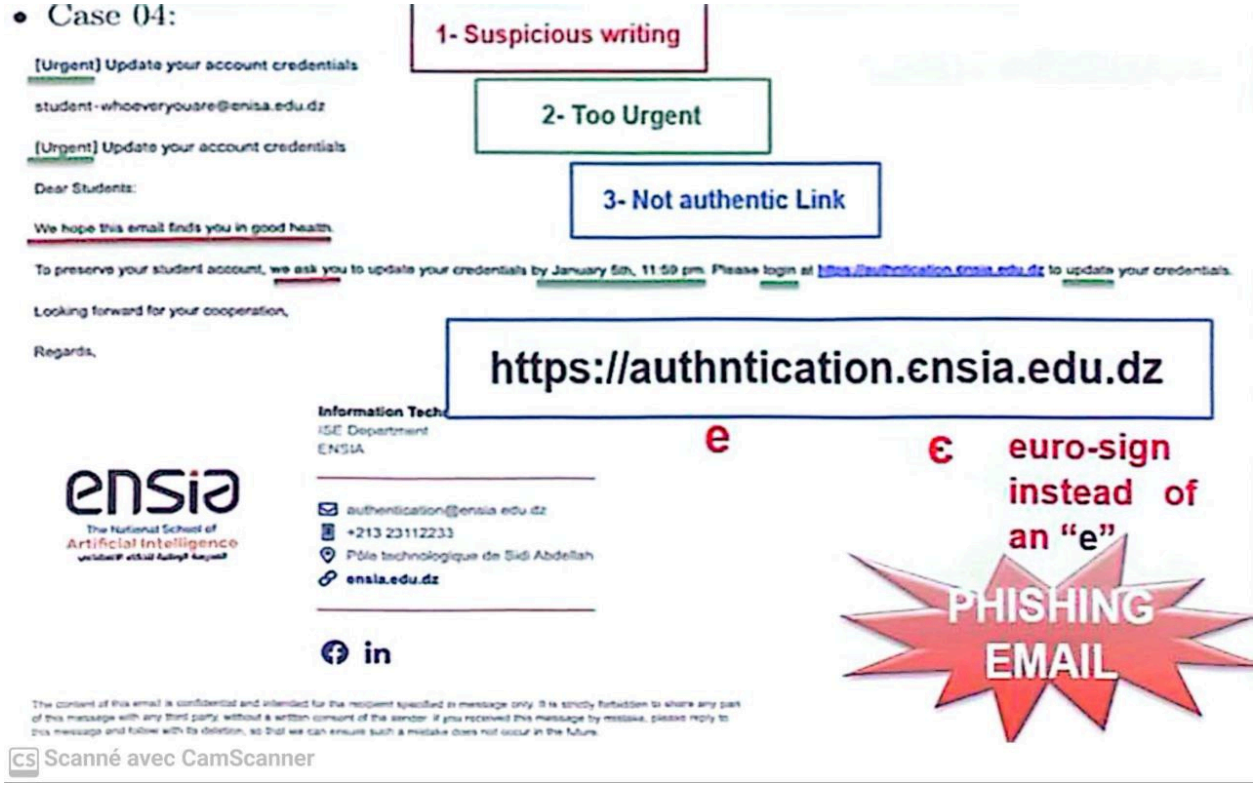
Case 02:



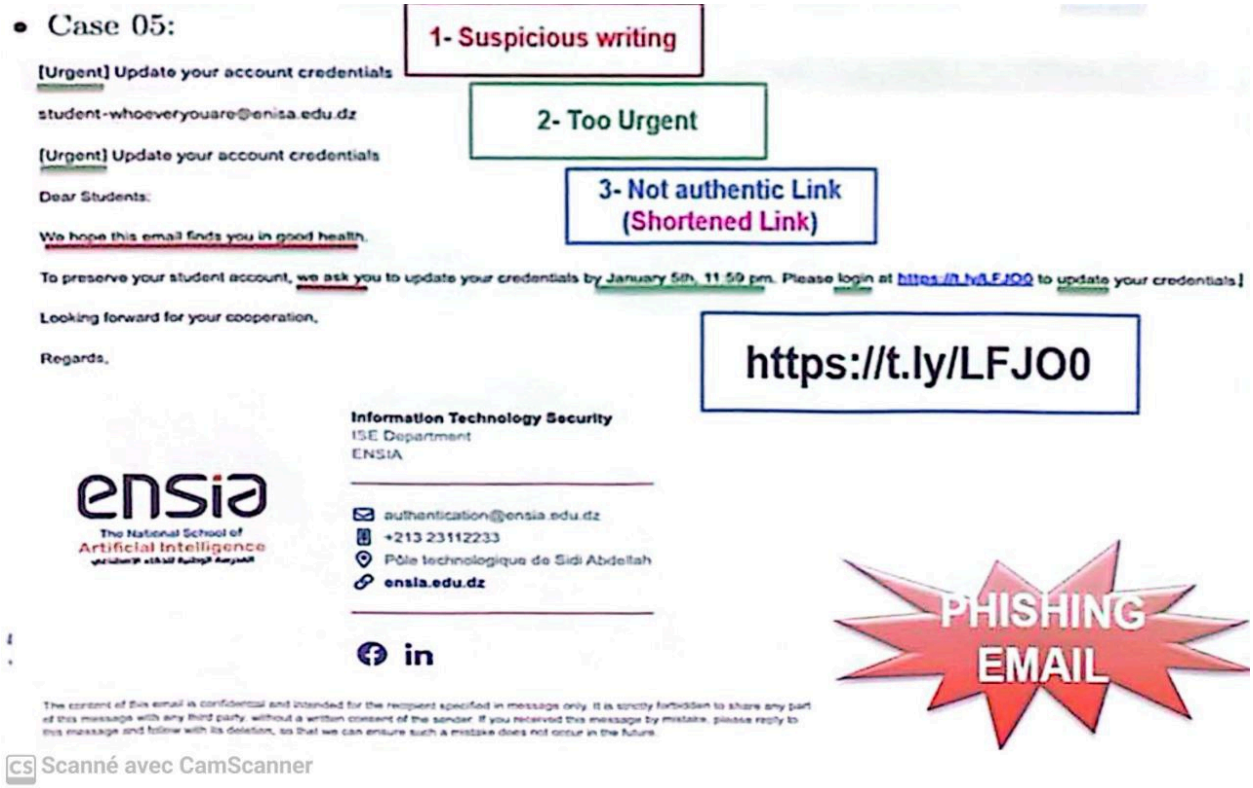
Case 03:



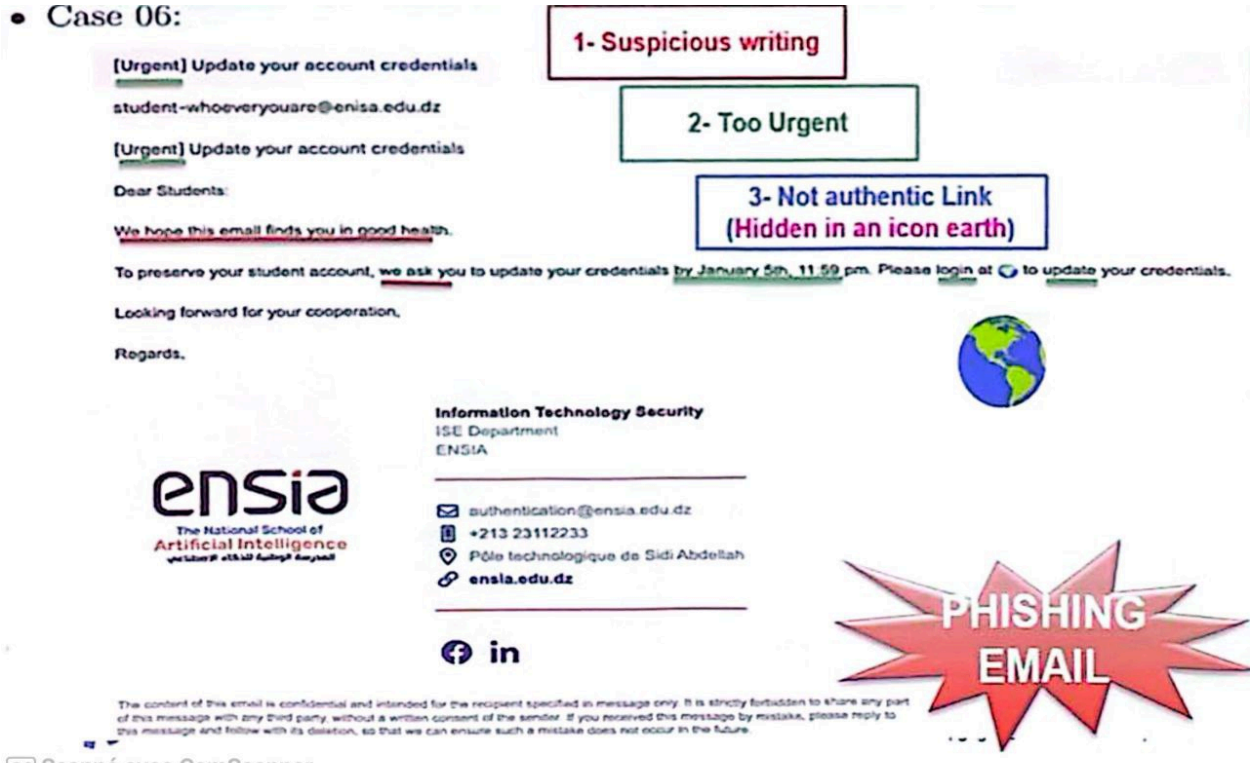
Case 04:



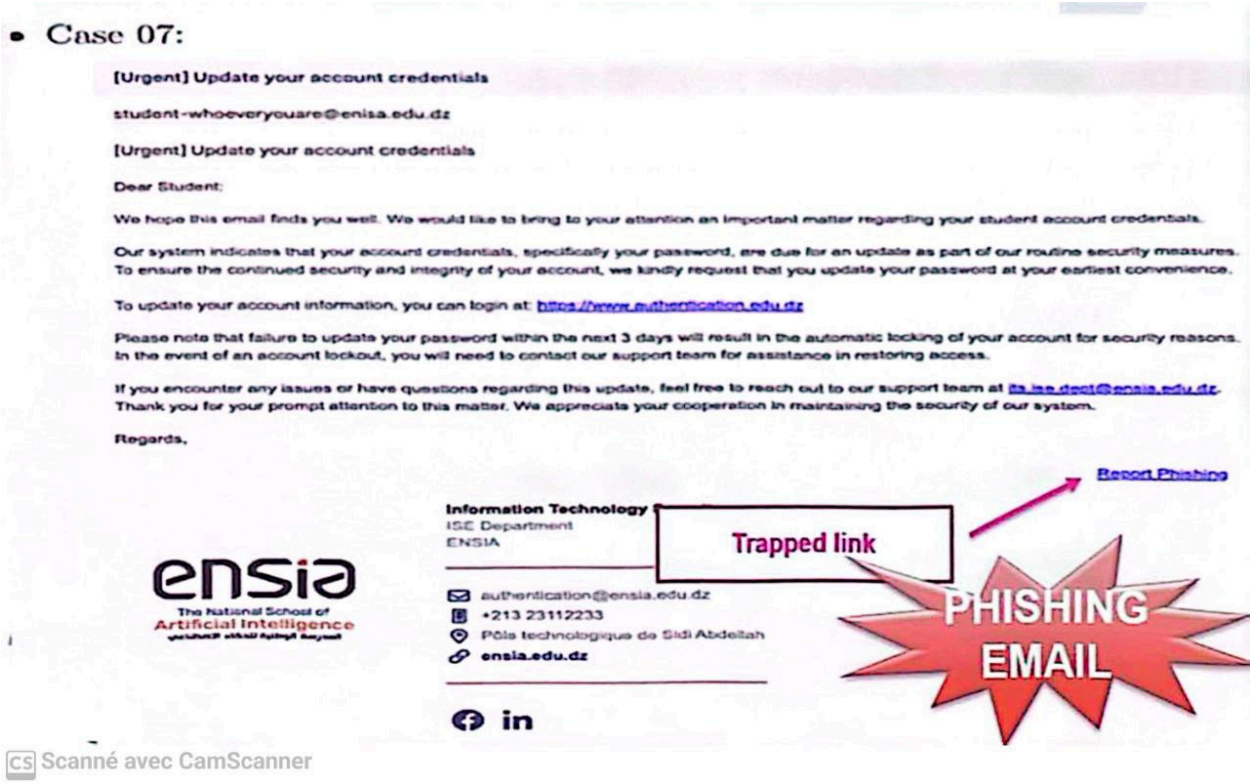
Case 05:



Case 06:



Case 07:



2. You are a Windows user (e.g., Microsoft Windows 11) and receive an email, from Microsoft, that contains an attached file, claiming an important security update. Explain what should you do:

Software companies and big tech companies will never send you an update by email. Delete the email and forget about it.

Exercise 06 (Security Aspects):

Physical	Social	Network	Application	Operating System
CCTV cameras	shredding machines	firewall	Trap doors	Trap doors
lighting projectors	cybersecurity training	HTTPS	free software	anti-malware
smart locks	tossed USBs in parking lots	disallow rogue devices	backdoors	firewall
fire extinguishers				backdoors
smoke detectors				running services
back-up power system				regular system update
HVAC system				
Shredding machines				
Thorny bushes				

Exercise 07 (Attack Classification) :

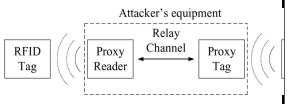
Attack	Explanation	vulnerability	Compromised security services	Countermeasures
Ping of death	A cyber attack where an attacker sends an unusually large and malformed Internet Control Message Protocol (ICMP) ping packet to a target computer or network. This oversized packet is designed to exceed the maximum allowed size, exploiting vulnerabilities in the target's network stack or operating system.	The improper handling of fragmented packets during the reassembly process by the target system.	Availability	**Patch Systems:** Keep software and systems up-to-date. **Firewall Configuration:** Block oversized or malformed packets. **Network Policies:** Enforce policies to restrict unnecessary ICMP traffic. **Packet Filtering:** Discard suspicious packets at the network perimeter.
Buffer overflow on the stack	A cyber attack where a program writes more data to a stack-based memory buffer than it can hold. This can overwrite adjacent memory, potentially leading to the execution of malicious code and compromising the program's security or stability.	A software bug in a program, exploiting the lack of proper input validation.	Various security services	Input validation Memory boundaries
Replayinga	A cyber attack	The lack of packet	Authentification	**Timestamps:** Include

n old packet	where an attacker intercepts a network packet transmitted between two parties and later resends or "replays" it to the network.	uniqueness or the absence of proper measures to prevent replay incidents.		time-related information in data packets. **Tokens:** Assign and verify tokens to enhance security and prevent unauthorized access.
Spray Paint on CCTV camera	A form of vandalism where individuals intentionally apply spray paint or other substances to cover or obscure the lens of a closed-circuit television (CCTV) camera.	The placement of the CCTV camera in accessible locations where attackers can physically reach and tamper with it.	Availability	**Secure Mounting:** Install cameras in hard-to-reach locations. **Redundant Cameras:** Install overlapping cameras for continuous coverage.
Cracking password	A cyber attack where unauthorized individuals attempt to gain access to a system by systematically guessing or decrypting the password, often using methods like brute force attacks or dictionary attacks.	The vulnerability lies in the use of weak or reused passwords and the absence of password complexity rules.	Primary authentication, it could escalate to other services	**Using Passphrases:** Encourage long, unique passphrases, avoid common phrases. **Changing Passwords:** Prioritize risk-based changes, implement multi-factor authentication.
ICMP smurf attack	A cyber attack where an attacker spoofs the victim's IP address and sends ICMP echo requests (ping) to the broadcast address of a network. As a result, all devices on the network respond to the victim's IP address, overwhelming it with a flood of responses and	The lack of authentication within the ICMP protocol.	Availability	**Disable IP Directed Broadcast:** Prevents broadcast **amplification.** **Ingress Filtering:** Blocks traffic with spoofed addresses. **Firewall Rules:** Restricts ICMP to broadcast addresses.

	causing a Denial of Service (DoS) due to the excessive volume of incoming ICMP packets			
Generating spoofed IP datagrams	A cyber attack where an attacker uses a different IP address to impersonate another computer. This technique allows the attacker to manipulate or deceive systems by presenting a false source IP address in the datagrams.	The absence of authentication in the IP protocol.	Authentication	I**ngress Filtering:** Block packets with spoofed source IP addresses at network borders. **Anti-Spoofing Policies:** Enforce strict policies against accepting packets with illegitimate source addresses. **Rate Limiting:** Control incoming packet rates from a single source to mitigate the impact of spoofed IP datagram attacks.
TCP flooding	A cyber attack where an attacker overwhelms a target system by inundating it with a high volume of malicious or unnecessary Transmission Control Protocol (TCP) connection requests.	The server's inability to differentiate between legitimate connection requests and malicious ones during the initial stage of communication.	Availability	**SYN Cookies:** Use SYN cookies to mitigate SYN flood impact. **Firewall Rate Limiting:** Set limits on incoming TCP connection requests. **Intrusion Prevention Systems (IPS):** Employ IPS for real-time protection against TCP flooding.
Packet Sniffing	A cyber attack where unauthorized interception and capture of data packets on a network occur, allowing analysis	The absence of encryption for transmitted packets.	Confidentiality	**Secure Protocols:** Use encryption (e.g., HTTPS) to secure data. **VPN (Virtual Private Network):** Implement encrypted communication tunnels. **Network Segmentation:**

	and potential extraction of sensitive information.			Restrict access, enhancing security.
Smashing server's room door	A physical security attack where an unauthorized individual forcefully breaks into a server room, potentially gaining access to critical infrastructure, servers, and sensitive information housed within the secured space.	Insufficient attention to physical security for the server room, creating a risk of unauthorized access.	Physical integrity	**Access Controls:** Use keycard or biometric systems. **Surveillance Cameras:** Monitor with cameras for deterrence. **Intrusion Detection Systems (IDS):** Detect and alert on unauthorized access.
Cloning RFID access cards.	A cyber attack where an unauthorized individual duplicates the information stored on a legitimate RFID access card to create a copy, allowing them to gain unauthorized entry to secured areas or systems.	The lack of security measures in certain RFID technologies, making them susceptible to cloning.	Authentication	**Encryption:** Secure RFID transmissions. **Secure Enclosures:** Protect cards from unauthorized scanning. **Authentication Protocols:** Use strong authentication to prevent cloning.
Integer overflow Attack	A cyber attack where an attacker manipulates numeric values in a way that exceeds the	Bugs in implementation, leading to potential integer overflow exploits.	Various security services	**Data Input Checks:** Validate input to prevent overflow. **Use Unsigned Integers:** Choose unsigned integers to expand representable values.

	allocated memory, potentially leading to unexpected behavior, crashes, or security vulnerabilities in a program or system.			
Cut accessible Ethernet cables	A physical attack where an individual intentionally cuts network cables. This leads to the disconnection of devices from the network, rendering them inaccessible and disrupting communication.	Lack of physical security. Visible and easily accessible Ethernet cables.	Physical integrity	**Secure Cable Management:** Conceal or secure cables. **Physical Access Controls:** Restrict unauthorized access.
Zip bombing attack	A malicious technique where a small compressed file expands into an extremely large one upon decompression, overwhelming system resources.	The system inability to check compressed file size during decompression.	Availability	**Content Filtering:** Use filters to check compressed files for unusual compression ratios. **Decompression Limits:** Set strict limits on decompression to prevent files from expanding excessively. **Security Software:** Use updated security software that can detect and block zip bombing attacks.
RFID Relay attack	A technique where an attacker uses a skimmer near an RFID card to capture signals and a repeater near the RFID reader to	The system's inability to verify the physical distance between the RFID card and the RFID reader.	Authentification	**Cryptographic Protocols:** Authenticate devices and secure key exchange. **Distance Limitations:** Restrict RFID range to prevent relay attacks.

	transmit those signals, creating a false impression that the card is physically present, even from a distance. 			**Biometric Verification:** Use biometrics for enhanced user authentication in RFID systems.
Wi-Fi wardriving.	The act of driving around to find unsecured wifi networks for unauthorized access	The broadcast nature of signals in all directions, making them susceptible to interception. The use of weak encryption in some Wi-Fi setups.	Confidentiality	**Strong Encryption:** Use robust encryption (e.g., WPA3) for Wi-Fi security. **Connection Limitations:** Restrict the number of simultaneous connections for Wi-Fi security. **Intrusion Detection Systems (IDS):** Deploy IDS to monitor and detect unauthorized access.
HTTP Cookie Hijacking	A security attack where an attacker intercepts and steals the session cookie, containing user information, compromising the user's session on a website.	Lack of knowledge.	Authentication	**Education and Training:** Regular cybersecurity education. **Information Sharing:** Collaborate and share threat information. **Security Policies:** Implement and enforce comprehensive security policies.
SQL Injection	A cyber attack where an attacker inserts malicious	Lack of SQL input validation.	Various services	**Parameterized Queries:** Use parameterized queries or prepared

	SQL code into input fields of a web application, manipulating the application's database and potentially gaining unauthorized access, extracting, or modifying sensitive information.			statements. **Input Validation:** Implement rigorous input validation. **Web Application Firewall (WAF):** Deploy a WAF for real-time monitoring and filtering.
Shoulder sniffing at // attack	An attack where an individual observes or eavesdrops on someone entering their PIN (Personal Identification Number) at an ATM or other devices with PIN entry, aiming to gain unauthorized access to the victim's account or sensitive information.	Lack of privacy protection during PIN entry at ATMs.	Confidentiality	**Privacy Screens:** Install screens to protect PIN entry. **User Awareness:** Educate users on shielding their PIN. **Camouflage Keypad Layouts:** Use randomized layouts to confuse observers.
Drawing nasty graffiti on the company's wall.	A destructive act involving the unauthorized creation of offensive images or messages on the company's property.	Lack of physical security measures.	Physical Integrity	**Surveillance Cameras:** Install to monitor and deter vandals. **Fencing or Barriers:** Implement physical barriers to restrict access.
Corrupt Linux kernel files.	The act of intentionally damaging critical files in the operating system's core, leading to system instability and security risks.	Insufficient controls enable unauthorized manipulation of critical Linux kernel files.	Integrity	**File Integrity Monitoring:** Regularly check for unauthorized changes. **Access Controls:** Apply strict permissions. **Updates and Backups:** Keep the system updated and maintain backups.

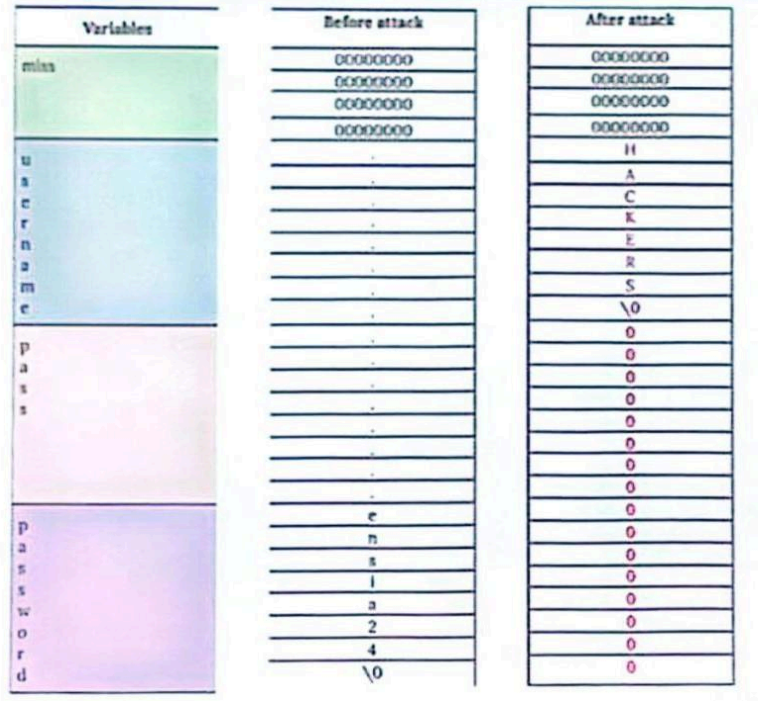
Exercise 8 (Vulnerability Identification):

1.

A malicious user, who has knowledge about how the code is implemented, can perform an integer overflow attack. They can insert a large value e.g 9999999999999999 (16 digits), the variable user_input_value will overflow and contain a value that if multiplied by 100, will remain less than 1000 e.g negative, positive number, greater than 1050. This vulnerability can be fixed by declaring the integer values as unsigned values.

2.

Following the declaration of the variables password then pass then username then miss all with 8 characters then the user can enter a pass with 16 characters where each 8 char represent a word and the word will be duplicated and by that he can decide the new password to use to pass the authentication because of overwriting the password.



3.

This time the order is username , miss, pass and password , the user can override the value of miss to get infinite chance to bruteforce the password this is by entering the 12 digits in in the pass and get a new value for the miss which will never reach 3 because it is already bigger(like 1111) use fget() instead of get to control user input.