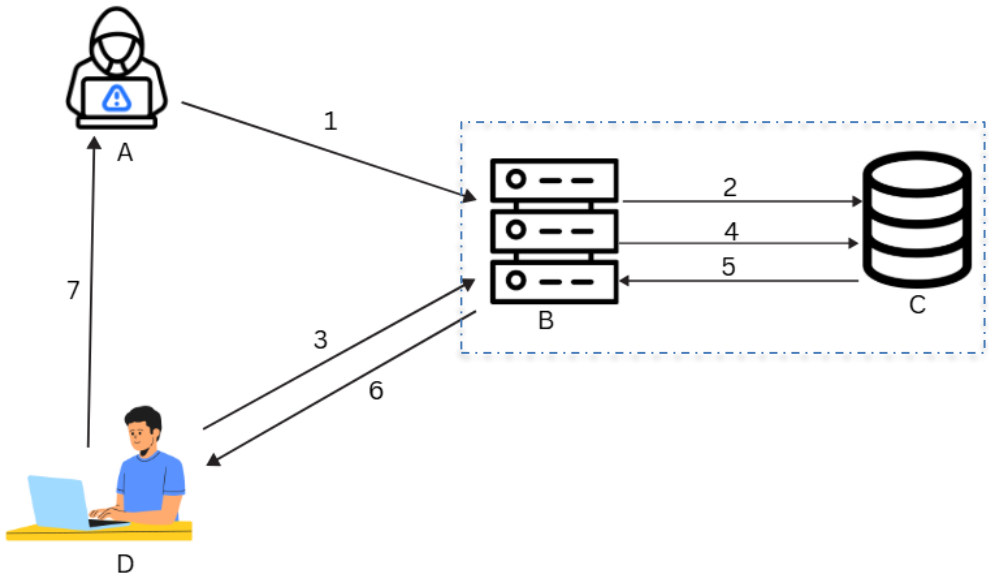
University of Echahid Hamma Lakhdar
Faculty of Exact sciences
Level: 1st year IoT&Cyber Security Master degree

Module: Computer Security.
Date: 17-01- 2026.
Duration: 1 hr, 30 mins.

Final Exam

Exercise 1 (4.5 pts)

The following diagram illustrates a Cross-Site Scripting (XSS) attack flow.



1- Label the objects: A, B, C (database), and D as well as the message content: 1, 2, 3, 4, 5, and 6 in the diagram above.
2- Is this a Reflected XSS or a Persistent XSS attack? Justify your answer.
3- Propose a specific security measure that could prevent or mitigate this type of XSS attack.

Exercise 2: (3.5 pts)

The following protected packet is captured during network analysis:

(New IP Header – ESP Header – Original IP Header – Data – ESP Trailer – Authentication Data)

a) Identify the IPsec mode and the protocol used.
b) Specify precisely which parts are encrypted and which are authenticated.
c) Explain how anti-replay protection is achieved in this configuration.

Exercise 3: **(4.5 pts)**

1. Define Multi-Factor Authentication (MFA) and explain why it is more secure than single-factor authentication.
2. Given the following authentication factors in MFA: Password, Smart card, Fingerprint scan, Security token (e.g., RSA token), Voice recognition, PIN code, Facial recognition, Security question (your preferred hobby), SMS.
   Classify them as: Something you know, Something you have, Something you are.
3. Describe a real world scenario where MFA could prevent an attack that single-factor authentication would not.

Exercise 4: **(04 pts)**

An employee receives a spoofed email appearing to be from the CEO, urgently requesting confidential files be sent to an external address. The employee complies via unencrypted email, allowing the files to be intercepted and leaked to a competitor. The employee later denies wrongdoing, claiming they believed the instructions were legitimate.

1. Identify the human risk and technical threat categories involved.
2. Which security services failed?
3. What mechanisms could have prevented or detected this?

Exercise 5: (3.5 pts)

1. Describe the normal TCP 3-way handshake between the victim and the gateway.
2. Explain how the attacker predicted the TCP sequence number.
3. Why did the attacker flood the gateway with UDP packets during the attack?

تمرين 1: يُظهر الرسم التوضيحي التالي سير هجوم (Cross-Site Scripting (XSS.

1. قم بتسمية الكائنات والرسائل في الرسم التوضيحي.
2. هل هذا الهجوم يُعتبرReflected XSS أم Persistent XSS أشرح سبب اختيارك.
3. اقترح إجراءً أمنيًا واحدًا محددًا يمكن أن يُسهم في **منع أو تخفيف** هذا النوع من هجمات.

تمرين 2: تم التقاط الحزمة المحمية التالي خلال تحليل حركة مرور الشبكة:

1. حدد the IPsec mode and the protocol المستخدم.
2. حدد بدقة أي الأجزاء encrypted وأيها Authenticated.
3. اشرح كيف يمكن لهذا الشكل حماية الشبكة من هجوم Reply.

تمرين 3:

1. عرف المصادقة متعددة العوامل واشرح لماذا هي أكثر أمانا من المصادقة بعامل واحد.
2. صنّف عوامل المصادقة المذكورة لثلاث أصناف: شيء تعرفه، شيء تملكه، شيء يميّزك أنت.
3. بّين بمثال من الواقع كيف لنظام بمصادقة متعددة منع هجوم لا يتمكن اعتماد مصادقة بعامل واحد من منعه.

تمرين 4:

يتلقى موظف بريدًا إلكترونيًا مزيفًا يبدو وكأنه مرسل من المدير التنفيذي (CEO)، يطلب فيه نقل ملفات سرية بشكل عاجل إلى عنوان بريد إلكتروني خارجي. يقوم الموظف بالاستجابة للطلب عبر إرسال البريد الإلكتروني دون تشفير، مما يسمح باعتراض الملفات وتسريبها إلى أحد المنافسين. ينكر الموظف لاحقًا أي مخالفة، مدعيًا أنه اعتقد أن التعليمات كانت شرعية.

1. حدد فئات التهديدات البشرية والتقنية المرتبطة بهذا الهجوم.
2. حدد security services التي تم كسرها.
3. اقترح security mechanismsالتي تمكن من منع أو اكتشاف الهجوم

تمرين 5:

1. صف خطوات TCP 3-way handshake الطبيعية التي تحدث بين victime وGateway.
2. اشرح كيف يستطيع المُهاجم توقع Sequence Number لـ TCP.
3. لماذا قام hacker بإغراق Gatewayبحزم UDP أثناء تنفيذ الهجوم ip spoofing؟

Exam Correction

Exercise 1: (4.5 pts)

1- Objects: **A** = Attacker, **B** = Web Server, **C** = Database, **D** = Victim

Flows:

1. Submits script via form
2. Saves to database
3. Requests vulnerable page
4. Fetches data from database
5. Returns page with injected script
6. Executes script / attack performed

2- Type of XSS: Persistent (Stored) XSS

Justification: The malicious script is stored in the database (step 2) and later served to multiple victims (steps 3–5), rather than being reflected in a single request/response cycle.

3- Preventive Measures:

Input Validation & Sanitization: Strip or encode HTML/JavaScript from user inputs before storing in the database.

Exercise 2: (3.5 pts)

1. IPsec Mode and Protocol Used

Mode: Tunnel Mode

Justification: The original IP header is preserved inside the encapsulated payload, indicating that the entire original IP packet (header + data) is protected, which is characteristic of Tunnel Mode. In Transport Mode, only the payload (TCP header + data) is protected, and the original IP header remains outside.

Protocol: ESP (Encapsulating Security Payload)

Justification: The packet explicitly contains an ESP Header and ESP Trailer, which are unique to the ESP protocol. AH (Authentication Header) does not use an ESP Trailer.

2. Encryption and Authentication Scope

Encrypted Parts: Original IP Header, TCP Header, Data,ESP Trailer

Authenticated Parts: New IP Header – ESP Header – Original IP Header – Data – ESP Trailer – Authentication Data

3. Anti-Replay Protection Mechanism

Anti-replay protection in IPsec (ESP) is achieved using:

Sequence Number Field: A 32-bit sequence number is included in the ESP Header. This number increments with each packet sent in the same Security Association (SA).

Sliding Window Mechanism: The receiver maintains a fixed-size window (default size = 64 packets) of valid sequence numbers.

Packets with sequence numbers: Behind the window → Rejected (replayed packet).

Within the window but not yet received → Accepted and marked.

head of the window → Advance the window and accept.

Cryptographic Validation: The sequence number is included in the authenticated data, preventing tampering.

If a replayed packet is detected, it is discarded before decryption or further processing.

Exercise 3: (4.5 pts)

MFA requires ≥2 factors; reduces risk of single point of failure.
Know: Password, PIN code, Security question.
Have: Smart card, Token, SMS.
Are: Fingerprint, Voice, Face recognition.

Example: Phishing steals password, but attacker lacks token → MFA blocks access.

Exercise 4: (04 pts)

1. Identify the human risk and technical threat categories involved.

- **Human Risk:** Social engineering, lack of security awareness, failure to verify the legitimacy of the request.
- **Technical Threat:** Email spoofing, unencrypted data transmission, interception (eavesdropping), and unauthorized data exfiltration.

2. Which security services failed?

- **Confidentiality:** The files were sent unencrypted and intercepted.
- **Integrity:** The email's origin was falsified, and the files were leaked without authorization.
- **Authentication:** The email sender was not properly verified.
- **Non-repudiation:** The employee later denied sending the files intentionally.

3. What integrity mechanisms could have prevented or detected this?

- **Email authentication protocols** such as SPF, DKIM, and DMARC could have detected the spoofed header.
- **End-to-end email encryption** (e.g., S/MIME, PGP) would have protected the content in transit.
- **Digital signatures** on internal emails from executives would have verified authenticity.
- **Data Loss Prevention (DLP)** tools could have blocked the sending of confidential files to external addresses.

4. How could authentication services (e.g., digital signatures) have helped?

- **Digital signatures** would have allowed the employee to verify that the email truly came from the CEO and had not been altered.
- **Email signing with S/MIME** would provide cryptographic proof of the sender's identity, preventing spoofing.
- **Two-factor authentication (2FA)** or **MFA for email access** would add a layer of verification before sending sensitive data.
- **Secure email gateways** could flag or block unsigned or suspicious emails from impersonating executives.

Exercise 5: (3.5 pts)

Normal TCP 3-way handshake:

Step 1 (SYN): The victim (10.0.0.102) sends a SYN packet to the gateway (10.0.0.1) to initiate a connection.

Step 2 (SYN-ACK): The gateway replies with a SYN-ACK packet, acknowledging the request and sending its own sequence number.

Step 3 (ACK): The victim sends an ACK packet to confirm, completing the handshake. Both sides enter the ESTABLISHED state.

Sequence number prediction: The attacker sniffed the ongoing TCP session between the victim and gateway using a network monitoring tool. By analyzing captured packets, the attacker observed the current sequence numbers and their incremental pattern, allowing them to predict the next expected sequence number in the exchange.

UDP flood purpose: The attacker flooded the gateway with UDP packets to slow down or temporarily incapacitate it (a DoS effect). This ensured that the attacker's spoofed packet would reach the victim before the legitimate gateway response, increasing the chance of session hijacking.