Abbès Laghrour University – Khenchela
Faculty of Science and Technology.
Department of Computer Science

Module: Security techniques
2nd Year Master Computer Science SI
Duration: 1 hour and 30 minutes

Academic Year: 2025/2026, Semester 3 Exam for normal Cycle

NAME:

Question 1: Le **Single Sign-On (SSO)**
A. Repose sur un système central d'authentification qui délivre un ticket ou un jeton de confiance.
B. Oblige l'utilisateur à saisir ses identifiants à chaque application.
C. Améliore la sécurité en réduisant la réutilisation des mots de passe.
D. Fonctionne uniquement sans serveur d'authentification central. **Réponse correcte : A et C 2pts**

Question 2: **Active Directory (AD)** est principalement utilisé pour :
A. Centraliser et organiser les informations sur les utilisateurs, ordinateurs et autres ressources du réseau dans une structure logique.
B. Assurer uniquement le chiffrement des données échangées sur le réseau.
C. Remplacer les systèmes d'exploitation des serveurs.
D. Gérer exclusivement les bases de données locales d'un seul ordinateur. **Réponse correcte : A 1pt**

Question 3: Concernant le protocole d'authentification **Kerberos**, quelle affirmation est **FAUSSE** ? **Corrigez la faute dans la proposition incorrecte.**

A. Kerberos empêche la transmission des mots de passe en clair sur le réseau en utilisant des tickets chiffrés.
B. B. Kerberos repose sur un tiers de confiance centralisé permettant une authentification mutuelle entre le client et le service.
C. C. Kerberos échange directement les clés de chiffrement symétriques entre le client et le service afin d'établir la session sécurisée**.** **Réponse correcte : C 1pt**

1 pts:La correction est :Kerberos **n'échange pas directement** les clés de chiffrement symétriques entre le client et le service ;les clés sont distribuées de manière sécurisée par le **KDC (Key Distribution Center)** à l'aide de **tickets**.

Question 4: Quelle affirmation décrit correctement la différence de transport entre les trois mécanismes DNS ?

A. Le DNS classique, DoT et DoH utilisent tous UDP sur le port 53.
B. Le DNS classique utilise UDP 53 sans chiffrement, DoT utilise TCP 853 avec TLS, et DoH utilise HTTPS sur le port 443.
C. DoH utilise TCP 853 tandis que DoT utilise HTTPS sur le port 443.
D. DoT utilise HTTPS sur le port 443 tandis que DoH utilise TCP sur le port 853. **Réponse correcte : B 1pt**

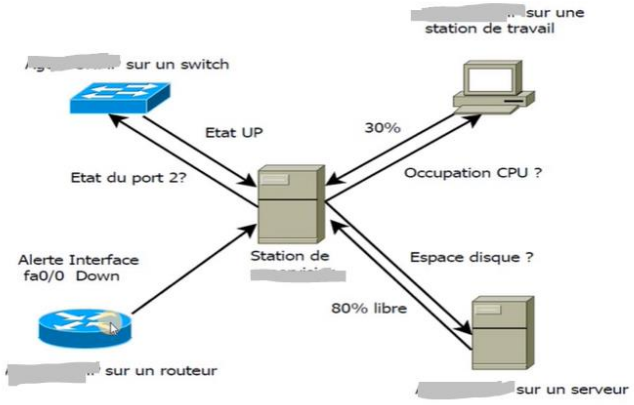
Question 5: Dans quel mécanisme **le navigateur envoie directement la requête DNS chiffrée**, sans passer par le résolveur DNS du système ?

A. DNS classique
B. DoT
C. DoH
D. Tous les mécanismes fonctionnent de la même manière **Réponse correcte : C 1pt**

Question 6: Pourquoi le **DoH** est-il plus difficile à détecter ou filtrer par les équipements réseau traditionnels ?

…… **Parce qu'il encapsule les requêtes DNS dans du trafic HTTPS standard sur le port 443**. **3pts**

Question 7: Observez attentivement l'image ci-dessous. Certaines informations ont été volontairement masquées. Écrivez les mots ou expressions cachés dans l'image. Les reponses **Agent SNMP** sur et Station de **supervision 2pts**

	Question 8: Quelle est la principale différence entre **TRAP** et **INFORM**. A. Un TRAP est **confirmé** par le gestionnaire, tandis qu'un INFORM n'est **pas confirmé**. B. Un TRAP est envoyé **sans accusé de réception**, tandis qu'un INFORM est **confirmé par le gestionnaire**. C. Un TRAP utilise toujours TCP, tandis qu'un INFORM utilise UDP. **Réponse correcte :B 1pt**
Question 9: Concernant les protocoles de messagerie **POP3** et **IMAP**, laquelle des affirmations suivantes est correcte ? A. POP3 permet une **synchronisation totale** entre plusieurs appareils. B. IMAP permet d'accéder aux emails **hors ligne uniquement sur un seul appareil**. C. POP3 télécharge les emails **localement et ne synchronise pas** avec le serveur. D. IMAP fonctionne **indépendamment d'Internet**, comme POP3. **Réponse correcte : C 1pt**	Question 11: Quelle affirmation décrit **correctement la différence** entre SMTP et S/MIME ? A. SMTP est un protocole de transport d'emails, tandis que S/MIME chiffre et/ou signe le contenu des emails. B. SMTP chiffre automatiquement le contenu des emails, S/MIME ne fait que transporter les messages. C. S/MIME remplace SMTP pour envoyer les emails de manière sécurisée. D. SMTP ne peut transporter que des emails HTML et S/MIME uniquement du texte brut **Réponse correcte :A 1pt**
Question 12: Lors d'une analyse PCAP d'un email envoyé via SMTPS avec S/MIME, quelle affirmation est correcte ? A. Le contenu du message est visible en clair dans le PCAP car S/MIME ne chiffre rien. B. Le message est chiffré par S/MIME avant SMTP, et SMTPS ajoute un chiffrement TLS sur le port 465 ou 587. C. SMTP et S/MIME utilisent le même protocole et port, il est impossible de distinguer le chiffrement. **Réponse correcte :B 1pt**	Question 13: Quelle affirmation décrit correctement la différence entre un **proxy forward** et un **proxy inverse** ? A. Un **proxy forward** agit pour les clients en les aidant à accéder à Internet, tandis qu'un **proxy inverse** agit pour les serveurs en filtrant et sécurisant les requêtes entrantes. B. Un proxy forward est utilisé pour protéger les serveurs, tandis qu'un proxy inverse est utilisé pour protéger les clients. C. Les deux types de proxy utilisent toujours le même port et la même configuration. **Réponse correcte :A 1pt**
Question 14: Dans TLS, le **Master Secret** est utilisé pour : A. Chiffrer directement les données envoyées entre le client et le serveur. B. Générer les clés de session symétriques pour le chiffrement et l'intégrité des communications. C. Authentifier le serveur uniquement. **Réponse correcte :B 1pt**	Question 15: Le Master Secret et les clés dérivées dans TLS assurent : A. Le chiffrement des données, l'intégrité (MAC) et parfois l'authentification des messages. B. La seule vérification que le serveur est bien en ligne. C. La création de certificats X.509 pour le serveur. **Réponse correcte :A 1pt**

Question 16: Comment le **Master Secret** est-il créé lors d'un handshake TLS ?

A. Il est dérivé à partir du **Pre-Master Secret** échangé via **RSA** ou Diffie-Hellman
B. Il est dérivé à partir du Pre-Master Secret et d'un random côté client et serveur.
C. Il est choisi aléatoirement par le client ou le serveur.

Réponse correcte :B 1pt