

## LIN3 - KERBEROS - FORMATIVE

Points: 3/20

**✗ Incorrect** 0/1 Points

1. Comment nomme-t-on le domaine d'autorité d'un serveur Kerberos ?

\* 

Un realm

Bonnes réponses : Realm

**✗ Incorrect** 0/1 Points

2. Qu'est-ce qu'un principal ?

\* 

Une identité unique

Bonnes réponses : L'identifiant unique Interagissant avec Kerberos représentant un utilisateur  
ou un service**✗ Incorrect** 0/1 Points

3. Qu'est-ce qu'un service pour Kerberos ?

\* 

Une ressource que on met a disposition de l'utilisateur

Bonnes réponses : Un système, une ressource, une application

à des utilisateurs, ou d'autres systèmes.

pour lequel Kerberos doit gérer l'accès

✗ **Incorrect** 0/1 Points

4. KDC ? Signification et rôle au sein de Kerberos.

\* 

Key Distribution Center, le coeur de Kerberos

Bonnes réponses :

Key Distribution Center

C'est le coeur de Kerberos

Livre des tickets

Livre des sessions temporaires offrant l'accès à des services.

Il centralise toutes les données sensibles concernant les utilisateurs et les services.

✗ **Incorrect** 0/1 Points

5. Quels sont les différents contenus échangés dans les messages (aucune distinction entre ce qui est crypté ou non) ?

\* 

Username ID, Servicename ID, IP, Timestamp

Bonnes réponses :

authenticator -> permet d'être authentifié par le service

ticket -> contient les infos de résultat du processus d'authentification)

✓ **Bonnes réponses** 1/1 Points

6. Reproduire la séquence

\* 

- 1 L'utilisateur fait une demande au KDC, en clair
- 2 Le KDC livre un TGT encrypté
- 3 L'utilisateur lit le TGT
- 4 L'utilisateur fait une demande au TGS
- 5 Le TGS génère et livre le ST (service ticket) à l'utilisateur

- 6 L'utilisateur demande accès au service
- 7 Le service confirme l'accès à l'utilisateur

✓ **Bonnes réponses** 1/1 Points

7. Lorsque l'utilisateur reçoit son TGT de la part du KDC, de quoi doit-il disposer pour pouvoir lire ce TGT ?

Aide : calculé à l'aide du nom d'utilisateur, d'un sel, ainsi que d'une fonction de hashage

\* 

Client Secret Key

✗ **Incorrect** 0/1 Points

8. Quels sont les deux types de contenus que l'utilisateur doit livrer au service pour demander (et obtenir) l'accès ?

\* 

Le Service Ticket et son User Authenticator

Bonnes réponses :

✗ **Incorrect** 0/1 Points

9. Quels sont les deux services composants de KDC ? (acronyme et noms complets)

\* 

AS et TGS, Authentication Server et Ticket Granting Server

Bonnes réponses :

✓ **Bonnes réponses** 1/1 Points

10. Voici le "contrat" que Kerberos fait avec vous, si vous le mettez en place correctement.

(Cochez si juste)

\* 

- ☐ Les mots de passes ne sont transmis qu'une seule fois en claire à travers le réseau
- ☒ Tous les acteurs de Kerberos peuvent identifier avec qui ils communiquent.
- ☐ Il est rarement attaqué car c'est un protocole qui est très peu utilisé.

✗ **Incorrect** 0/1 Points

11. Dans quel type de message transite la durée de la session (time to live) ?

\* 

Le Timestamp

Bonnes réponses : Tickets

✗ **Incorrect** 0/1 Points

12. La première étape du processus d'authentification, est-il en clair ou encrypté ? Qui sont les acteurs impliqués ?

Note : ne répondez pas le KDC mais précisez bien quel(s) serveur(s)

\* 

En clair, entre l'user et l'AS

Bonnes réponses : AS - authentication server Client Oui, en clair !

✗ **Incorrect** 0/1 Points

13. Quels sont les attributs obligatoires que le client envoie lors de sa demande (initiale) d'authentification ? Et à qui ?

\* 

User Name/ID, Service Name/ID

Bonnes réponses : Envoie à l'AS User Name / ID Service Name / ID User Ip Adress

Requested lifetime for TGT

✗ **Incorrect** 0/1 Points

14. L'attribut "User IP address" envoyé lors de l'authentification initiale, que peut-il contenir comme information ?

\* 

Une IP, plusieurs, ou rien

Bonnes réponses :

1 adresse ip

x adresses ip

aucune adresse ip

✗ **Incorrect** 0/1 Points

15. A quel moment l'AS génère-t-il, l'identifiant unique représentant le "principal" (Client Secret Key) ?

\* 

Il va checker dans sa DB

Bonnes réponses :

Lors de l'inscription de l'utilisateur/du service dans le KDC

✗ **Incorrect** 0/1 Points

16. Quels sont les attributs présents dans le TGT, et qui n'ont pas été transmis lors de la demande initial à l'AS ?

\* 

TGS Name/ID, Timestamp, TGS Session Key

Bonnes réponses :

TGS Name/ID

Timestamp

✗ **Incorrect** 0/1 Points

17. Que pouvez-vous dire à un collègue qui prétend qu'un système basé sur des clés symétriques n'est pas utilisé dans Kerberos ?

\* 

C'est faux car des clés symétriques sont utilisés tels que les TGS Session Key et Service Session

Bonnes réponses :

TGS Session Key est une clé symétrique

Produite par l'AS

Livrée à l'utilisateur

Livrée au service

Afin qu'ils puissent (utilisateur et service)  
s'authentifier mutuellement

✗ **Incorrect** 0/1 Points

18. L'utilisateur, en utilisant son pwd, va pouvoir décrypter la TGS Session Key.

Pourquoi ne peut-il pas également décrypter le TGT ?

Et qui le pourra ?

Mais pourquoi le reçoit-il s'il ne peut de toutes manières par le lire ?

\* 

Car il a été chiffré avec la TGT Secret Key, que l'user n'a pas. Le TGS pourra le déchiffrer avec sa

Bonnes réponses :

Le client a besoin de disposer de sa "client secret key", qu'il obtient en saisissant son pwd dans le client Kerberos (qui va générer sa clé privée)

Le TGT ne pourra être lu que par le service qui est concerné par ce même TGT.

L'utilisateur en a besoin pour s'adresser sa demande d'accès au service ciblé.

✗ **Incorrect** 0/1 Points

19. Quels sont les éléments (attributs) qui sont envoyés en clair entre le client et le service ciblé ?

\* 

Service Name/ID et le timestamp

Bonnes réponses :

Le service name / id

Le time stamp

Le reste est encrypté. Le service pourra l'ouvrir avec sa propre clé privée (TGS Secret key)

✗ **Incorrect** 0/1 Points

20. Comment le TGS se protège contre les "replay attack" ?



Il garde en cache les user qui ont fait des demandes récentes

Bonnes réponses :

Il dispose d'un cache

Maintenant ainsi la liste des demandes réalisées récemment

Une seule entrée étant possible par "client".

Conservez les informations avec vous en enregistrant la réponse.

[Enregistrer ma réponse](#)



Ce contenu est créé par le propriétaire du formulaire. Les données que vous soumettez sont envoyées au propriétaire du formulaire. Microsoft n'est pas responsable des pratiques de confidentialité ou de sécurité de ses clients, y compris celles de ce propriétaire de formulaire. Ne donnez jamais votre mot de passe.

Microsoft Forms | Enquêtes, questionnaires et sondages basés sur l'intelligence artificielle [Créer mon propre formulaire](#)  
[Confidentialité et cookies](#) | [Conditions d'utilisation](#) | [Accessibilité](#)