

Sécurité des Protocoles Internet

Les supports de cours et autres documents **ne sont pas autorisés**.

Vous avez droit à vos notes de cours rédigées sur une feuille manuscrite recto-verso.

Chaque question est notée sur un ou deux points, et seule une réponse complète avec des explications claires et un minimum de détails (nul besoin d'écrire un roman !) se verra accorder la totalité des points.

Pour les questions de type QCM, il peut y avoir une ou plusieurs bonnes réponses.

Il est inutile de recopier le cours si on ne sait pas répondre.

1 La sécurité du DNS

1.1 Le mécanisme de résolution

▷ (2 points) Expliquez tout ce qui se passe *en arrière plan au niveau DNS* lorsque vous saisissez une URL dans la barre d'adresse de votre navigateur sous une plateforme type Unix ?

Soyez très précis sur les termes techniques que vous utilisez : indiquez ce qui se passe au niveau système et au niveau réseau en précisant à chaque stade les différentes erreurs qui peuvent survenir. Pour vous donner un indice, on peut distinguer *au moins 6 grandes étapes*.

Notez bien que cette question est notée sur 4 points et seule une réponse claire et détaillée apportera la totalité des points.

1.2 Les problèmes de pollution

▷ (1 point) Rappeler pourquoi les plages d'adresses IP privées (par exemple au sens de la RFC 1918) peuvent causer des problèmes de pollution au niveau des serveurs DNS d'infrastructure (régine, TLD).

▷ (1 point) Quelle solution technique pourrait être mise en oeuvre au niveau global pour limiter cette pollution ?

2 La messagerie

2.1 Validité des adresses mail

Au cours d'une conversation téléphonique, votre correspondant vous a donné ses coordonnées mais après avoir raccroché, vous n'êtes plus complètement sûr d'avoir noté correctement son adresse mail.

▷ (2 points) Quelles vérifications techniques pourriez-vous effectuer afin de déterminer la validité de l'adresse que vous avez notée ? Quel degré de fiabilité avez-vous sur le résultat final ? On élimine bien sûr les solutions évidentes comme rappeler son correspondant, envoyer un message de test et le rappeler pour savoir s'il l'a reçu, etc.

3 Le protocole SMTP

Les gestionnaires de liste de diffusion utilisent souvent un système appelé VErP (*Variable Envelope Return-Path*).

Ce système permet, lorsqu'on envoie un message à une liste de diffusion, de positionner le paramètre MAIL FROM de l'enveloppe SMTP à une valeur différente pour chaque adresse de la liste.

▷ (2 points) Quel est l'intérêt de ce système ? Expliquer.

3.1 Le chiffrement SSL/TLS

Beaucoup de protocoles de messagerie (SMTP, IMAP, POP) supportent la commande STARTTLS.

▷ (2 points) Rappelez ce que permet de faire cette commande ? Quel est son intérêt ? Est-ce que tous les protocoles applicatifs pourraient implémenter cette commande ?

4 Les protocoles web

▷ (1 point) Expliquer la différence entre une méthode HTTP sûre et une méthode HTTPS non sûre (ne pas confondre avec HTTTPS). Donner un exemple de méthode de chaque type.

▷ (1 point) Quelle est la différence entre HTTP et HTTPS ?

▷ (1 point) Qu'est-ce qu'un proxy ?

▷ (1 point) Expliquer la différence entre FTP actif et FTP passif

5 Kerberos

▷ (2 points) Généralités
— sur quel type d'algorithme de chiffrement se base Kerberos ?
— citez au moins 2 services qui supportent ce mode d'authentification.

▷ (1 point) Expliquez ce qu'est un ticket kerberos, ce qu'il contient et ce qu'il permet de faire

▷ (1 point) Un serveur kerberos est composé notamment d'un TGS (Ticket Granting Service) A quoi sert il ?

6 Extraction et analyse de malware

▷ (1 point) Décrivez les étapes d'une attaque de type *Drive By Download* / d'un *Exploit Kit*

▷ (1 point) De nos jours, la grande majorité des malwares sont obscurcis, à l'aide notamment d'un ou plusieurs *packers*.
— Citez deux raisons de cet obscurcissement
— Proposez une méthode d'obscurcissement

▷ (1 point) *Forensics* : Une carte SD (du type de celles utilisées dans les appareils photos) est retrouvée dans une zone sensible d'une entreprise.

- Quelles sont les précautions à prendre pour l'analyser ?
- Un dossier au nom suspectif est présent sur la carte, mais est vide. Que peut faire l'analyste pour en savoir plus ?