Master M2 SeCReTS 2021-2022

Sécurité applicative (HTTP - DNS - Messagerie)

NOM, Prénom : .....

Pour chaque question, il y a ***une seule bonne réponse*** *; cette dernière rapporte un point et une mauvaise réponse* ***fait perdre 0.5 point****, ne vous précipitez pas et prenez bien le temps de répondre.*

Question 1 Pour recevoir des mails, un domaine de messagerie :

- ☐ peut posséder **plusieurs** enregistrements `MX` **mais** avec des priorités différentes.
- ☐ doit posséder **au moins un** enregistrement de type `MX`.
- ☐ doit **obligatoirement** avoir un enregistrement de type `A`.
- ☐ aucune des trois autres réponses n'est valide.

Question 2 En cas d'erreur lors de la livraison d'un mail (par exemple la boîte aux lettres de l'utilisateur est pleine), que se passe-t-il ?

- ☐ Le message est ignoré silencieusement.
- ☐ Le `MTA` prend l'adresse de l'expéditeur dans le champ "`From:`" du message et lui envoie un mail d'erreur.
- ☐ Le `MTA` envoie un message d'erreur à l'adresse du "`MAIL FROM`" de la session `SMTP`.
- ☐ Le `MTA` recherche le *reverse DNS* de l'adresse `IP` qui est en train de lui livrer le message, et envoie son message d'erreur au domaine trouvé.

Question 3 Les enregistrements `DNS` de type `NS` sont utilisés pour :

- ☐ indiquer les serveurs primaires ou secondaires en fonction de la priorité.
- ☐ aucune des trois autres réponses n'est valide.
- ☐ faire le transfert de zone entres les serveurs primaires et secondaires.
- ☐ indiquer aux clients quels sont les serveurs cache qu'ils doivent utiliser.

Question 4 Lorsqu'un un serveur cache DNS (appelé également *forwarder*) répond aux requêtes de ses clients (avec l'information présente dans son cache ou bien avec l'information récoltée à la suite du mécanisme de résolution itératif), sa réponse est :

- ☐ encapsulée dans un paquet `UDP` ou `TCP` avec le port source 53.
- ☐ encapsulée dans un paquet `UDP` avec le port source 53.
- ☐ encapsulée dans un paquet `UDP` ou `TCP` avec le port destination 53.
- ☐ encapsulée dans un paquet `UDP` avec le port destination 53.

Question 5 Un enregistrement `DNS` de type `CNAME` :

- ☐ ne peut pas être mis en cache.
- ☐ permet de stocker une adresse `IP`.
- ☐ permet de stocker un nom de domaine type `FQDN`.
- ☐ permet de stocker un nom de domaine dans `.in-addr.arpa`.

Question 6 Les `RBLDNS` (*Real Time Black-lists DNS*) permettent de maintenir en ligne une base de données des adresses `IP` utilisées par les spammeurs. Comment les `MTA` utilisent-ils cette base de données ?

- ☐ À partir de la commande `MAIL FROM`, le MTA récupère le nom de domaine de l'expéditeur, cherche un enregistrement `A` pour ce nom de domaine, et interroge les `RBLDNS` avec cette adresse IP.
- ☐ En utilisant un champ spécial dans les entêtes du message (de la forme `X-DNSBL: <IP>`).

- [ ] À partir de la commande `HELO` (ou `EHLO`), le MTA récupère le nom de domaine en paramètre de cette commande, puis cherche les adresses `IP` rattachées à ce domaine, et enfin interroge les `RBLDNS` avec ces adresses `IP`.
- [ ] Lors de la session `SMTP`, le MTA interroge les `RBLDNS` en utilisant l'adresse `IP` source de la connexion.

Question 7 Lorsqu'un serveur `DNS` primaire ou secondaire répond à une requête, que se passe-t-il si la taille de la réponse est trop grande pour être contenue dans dans un paquet `DNS` standard ?

- [ ] La fragmentation `IP` se produit et induit des latences réseaux.
- [ ] Le serveur ignore la requête.
- [ ] Seul le premier enregistrement est transmis.
- [ ] Le serveur signale au client que la réponse est tronquée.

Question 8 Dans la norme du protocole HTTP, la méthode `GET` est considérée comme une méthode "sûre" parce que :

- [ ] elle ne peut être utilisée que si le serveur web est en HTTPS.
- [ ] on ne peut pas passer d'arguments dans l'URL (*query string*).
- [ ] elle n'a pas d'effets de bord, on peut l'appeler autant de fois qu'on le souhaite.
- [ ] elle n'est accessible qu'après une authentification.

Question 9 Une adresse de messagerie est : `bob@example.net`. Le nom `DNS` `example.net` est un `CNAME` vers `example.com`. Que va faire le `MTA` pour envoyer un message à *Bob* ?

- [ ] chercher un enregistrement de type `A` pour `example.net`.
- [ ] chercher les enregistrements de type `MX` pour `example.net`.
- [ ] rien du tout car on ne peut pas utiliser un `CNAME` pour un domaine de messagerie.
- [ ] chercher les enregistrements de type `MX` pour `example.com`.

Question 10 Est-il possible d'avoir une seule adresse IP publique et d'héberger deux sites web qui doivent être accessibles avec des noms de domaines différents, par exemple `example.net` et `example.org` ?

- [ ] il suffit de mettre la même adresse `IP` dans les enregistrements `A` de chacun des noms de domaine et les clients n'auront qu'à utiliser l'entête `Host:` dans les requêtes pour différencier les deux sites.
- [ ] ce n'est pas possible à moins de faire écouter le serveur web sur deux ports TCP distincts, par exemple `TCP/80` et `TCP/8080`.
- [ ] ce n'est pas possible, car au niveau du `DNS`, les deux noms de domaine ne peuvent pas avoir un enregistrement de type `A` qui pointe vers la même adresse IP.
- [ ] aucune des autres réponses n'est correcte.

Question 11 Parmi tous les noms de domaines listés ci-dessous, un seul d'entre-eux est un `FQDN` (*Fully Qualified Domain Name*), lequel ?

- [ ] `arpa`
- [ ] `www`
- [ ] `com.`
- [ ] `www.example.net`

Question 12 Le mécanisme DKIM permet de signer une partie des entêtes d'un message. Pour vérifier si la signature est correcte, on a besoin de connaître la clé publique associée. Cette clé est stockée dans le `DNS` : à quel endroit ?

- [ ] dans la zone correspondant au nom de domaine de l'adresse mail transmise en argument de la commande SMTP `"MAIL FROM"`.
- [ ] dans un sous-domaine appartenant à une zone réservée `.dkim.net`.
- [ ] dans la zone correspondant au nom de domaine de l'adresse mail stockée dans l'entête `"From:"` du message.

☐ peu importe l'endroit où est stockée la clé publique dans le DNS, il suffit juste que cela soit paramétré au niveau du MTA qui reçoit le message pour qu'il puisse faire la vérification.

Question 13 La commande ci-dessous a été exécutée dans un terminal sur une station de travail Linux disposant d'une connexion à Internet tout à fait fonctionnelle (par exemple, l'utilisateur peut *surfer* sur le web sans aucun problème).

```
$ host www.example.net
;; connection timed out; no servers could be reached
```

Quelle est la cause probable du message d'erreur ?

☐ Les serveurs de cache ne sont pas joignables.
☐ Le domaine `www.example.net` ne contient pas d'enregistrement.
☐ Les serveurs racines ne sont pas joignables.
☐ Les serveurs autoritaires pour le domaine `example.net` ne sont pas joignables.

Question 14 Parmi les différentes commandes listées ci-dessous, laquelle peut permettre de trouver le nom DNS associé à l'adresse IP `5.120.0.211` ?

☐ `$ host -t a 5.120.0.211.in-addr.arpa.`
☐ `$ host -t ptr 211.0.120.5.in-addr.arpa.`
☐ `$ host -t ptr 5.120.0.211.in-addr.arpa.`
☐ `$ host -t cname 211.0.120.5.in-addr.arpa.`

Question 15 À quoi sert le TTL dans enregistrement DNS ?

☐ à indiquer aux *forwarders* DNS combien de temps un enregistrement peut être caché.
☐ à se protéger contre les tentatives d'injection de trafic DNS.
☐ à limiter la durée de vie des paquets UDP sur le réseau.
☐ à l'expiration du TTL (exprimée en secondes), un nouveau transfert de zone (AXFR) doit être demandé auprès des serveurs primaires.

Question 16 Qu'est-ce qui permet de communiquer de manière confidentielle et de bout en bout (*End-to-End Encryption*) avec la messagerie traditionnelle ?

☐ aucune des trois autres réponses.
☐ l'activation de SSL/TLS au niveau du MTA qui gère le domaine de messagerie.
☐ l'utilisation de DKIM.
☐ l'utilisation de Tor.