



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT,
DE L'ÉNERGIE ET DE LA MER

MINISTÈRE DU LOGEMENT,
ET DE L'HABITAT DURABLE

Examen professionnel de vérification d'aptitude aux fonctions de programmeur système d'exploitation

- Session 2016 -

Épreuve écrite n°1 INFORMATIQUE

Composition sur un sujet relatif aux principes généraux du logiciel

Durée : 2 heures

Coefficient : 2

Notation : sur 20

Nombre de pages du sujet : 4 (y compris cette page)

Matériel :

Aucun matériel autorisé.

Documents :

Aucun document autorisé.

Observations :

Il sera tenu compte de la lisibilité et de la propreté des copies, ainsi que de la qualité de l'expression écrite.

Remarques générales :

- Le sujet comporte quatre parties traitant des thématiques suivantes :
 - les systèmes d'exploitation
 - acronymes à définir
 - réseau
 - sécurité

Examen professionnel de vérification d'aptitude aux fonctions de PSE			Session 2016
Épreuve écrite : Informatique	Durée : 2 h	Coefficient : 2	Page 1/4

1- Systèmes d'Exploitation (4 points)

A. Virtualisation, émulation et conteneurisation

Décrire les principes de virtualisation, d'émulation et de conteneurisation.

Préciser le contexte d'application de ces techniques.

B. Systèmes de fichiers et volumes de stockage

Pour un système de fichiers identifié, énumérer les métadonnées associées.

Proposer des catégories de métadonnées en précisant le type d'objets auxquels elles sont associées.

2- Définitions (4 points)

Définissez les acronymes suivants (quelques lignes par acronyme) :

- IOMMU
- SSH
- SCTP
- IoT
- UEFI
- LTO
- Lifi
- SIP
- PaaS
- IMAPS
- SHA-512
- RADIUS
- ITIL
- RFC
- UTF
- CRC

3- Réseau (6 points)

Le protocole *ICMP* est très utile pour les administrateurs réseaux. Pourquoi ?

La commande `ping` utilise ce protocole. Lorsqu'elle est utilisée vers une machine dont on connaît l'adresse *IP*, on peut avoir en retour ces types de message :

1. « *ICMP Network Unreachable* »
2. « *ICMP Host Unreachable* »
3. aucune réponse

Pour chacun de ces cas, préciser ce que l'on peut en conclure et qui a répondu.

Avec un analyseur réseau, nous avons capturé ces deux trames lors d'un échange *ECHO-REQUEST* entre deux machines :

```
0000  3a ca da cc 82 64 3a ca da cc 4b 36 08 00 45 00
0010  00 3c 32 87 00 00 30 01 d2 3e ac 14 0a 02 25 eb
0020  59 fa 08 00 4c f8 00 01 00 63 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67 68 69
```

```
0000  3a ca da cc 4b 36 3a ca da cc 82 64 08 00 45 00
0010  00 3c a0 e3 00 00 34 01 af e2 25 eb 59 fa ac 14
0020  0a 02 00 00 54 f8 00 01 00 63 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67 68 69
```

1. Que signifie pour vous le fait que le champ *TTL* (encadré) a changé de valeur ?
2. En décodant ces deux trames pouvez-vous donner l'adresse *IP* de la machine source et de destination ainsi que leur classe réseau respective ?

4- Sécurité (6 points)

A. Vulnérabilité

Expliquer l'importance du temps dans une architecture de sécurisée.

Décrire les principes d'attaques basées sur le temps et leurs conséquences.

B. Qu'est ce que l'ASLR ?

C. Traçabilité

Quelles preuves peuvent être exploitées sur un système en cas de compromission pour une analyse *post-mortem* ?

Préciser les contraintes techniques et juridiques s'appliquant aux traces d'exécution.

D. Mots de passe

8c6976e5b5410415bde908bd4dee15kdfb167a9c873fc4bb8a81f6f2ab448a918

Ce condensat a été volé lors du détournement d'une session sur une application critique, des erreurs ont pu survenir lors de l'interception. Aucune tentative de *crack* n'a abouti jusque-là ; cependant, vous savez par un autre canal d'information que le condensat est de type *SHA-2*.

En analysant le condensat, que pouvez-vous dire sur l'erreur survenue lors de l'interception ?

Quelles méthodes pouvez-vous employer pour retrouver la chaîne de caractères originale ?

Dans le cas où ce condensat représente un mot de passe, quelles solutions proposez-vous pour améliorer la sécurité de cette application critique ?