

ISTY - Université de Versailles – St Quentin en Yvelines
 IATIC5
 Module “ Administration Système Linux ”

Franck TALBART, Vincent PALOMARES, Nicolas PETIT

Examen : module “ Administration Système Unix / Linux ” IATIC5 2023/2024

(Date : vendredi 22 décembre 2023 – Durée : 2h00 – Seul le support de cours est autorisé)

Lire attentivement et en entier les énoncés des exercices avant de les commencer, afin de bien assimiler ce qui est attendu. Faire les exercices dans l'ordre et laisser de l'espace si besoin. Justifier TOUTES les réponses en se limitant à ce qui est pertinent (une recopie du cours sur un sujet donné ne constitue pas une réponse). **Les réponses non justifiées ne rapportent pas de point.**

Partie I : Réseau (7 points)

La ferme *SuperGreen* est une start-up digitale biologique durable gérée par la militante écolo Ylone Meusk. Elle innove en contrôlant ses cultures à l'aide d'une Intelligence Artificielle (*ChatGéGéPT(c)*) déployée sur un data center exaflopique nécessitant un mini réacteur nucléaire au milieu des champs.

Chaque légume est équipé d'un capteur mesurant sa taille, sa couleur et son état. Les capteurs sont connectés en wifi. L'IA détermine lorsqu'il est nécessaire d'arroser un légume.

Gégé, fameux ingénieur Picardien au CV impressionnant (cf sujets d'examens précédents), est responsable de l'infrastructure de la ferme. Il dispose du bloc d'adresses IPv4 192.168.0.0/20 (masque de réseau non conventionnel qui ne respecte pas les classes) et souhaite créer trois sous-réseaux : un pour les carottes, un pour les betteraves, et un pour le cluster.

Question 1 – 0.5 point(s) Quel est le nombre de bits à utiliser pour l'identifiant des sous-réseaux (on suppose que les sous-réseaux sont de taille identique) ? Justifier.

Question 2 – 1 point(s) Quel type d'adresse permet d'envoyer un ping à l'ensemble des carottes ? Dans notre situation, proposer une adresse utilisable à cette fin. Justifier.

Question 3 – 0.5 point(s) Combien de carottes est-il possible de cultiver au maximum ? Justifier.

Question 4 – 1 point(s) En supprimant la contrainte sur la taille identique des sous-réseaux, comment peut-on augmenter ce nombre pour les carottes uniquement et sans impacter la taille des autres sous-réseaux ?

Question 5 – 2 point(s) Proposer un masque, et les nouvelles adresses des trois sous-réseaux si nécessaire.

Question 6 – 1 point(s) Proposer la première et la dernière adresse disponible pour les carottes dans cette nouvelle configuration.

Gégé souhaite augmenter encore davantage le nombre de carottes. Une solution conventionnelle serait de passer à IPv6, mais son pentium III overclocké tournant sur Windows 98 (seconde édition) ne le permet pas. Gégé décide de ne plus se restreindre à son bloc d'adresses.

Question 7 – 1 point(s) En supposant qu'il a à sa disposition toutes les adresses ipv4 théoriques, quel sous-réseau Gege pourrait-il allouer aux carottes pour en maximiser la taille (sans réduire la taille des autres sous-réseaux) ? Justifier.

Partie II : Logs & NFS (6 points)

Des logs sont enregistrés afin de stocker les données de chaque carotte vers un noeud du datacenter.

Question 8 – 1.5 point(s) Quel service Gégé peut-il utiliser ? Donner le nom et le contenu des fichiers de configuration, ainsi que les actions nécessaires pour répondre à ce besoin.

Question 9 – 1 point(s) L'IA contrôle un robot, Nestor, arrosant les légumes de pesticides biologiques. La régularité est essentielle afin de garantir la qualité reconnue des produits: toutes les 3 minutes, sauf la nuit. Par quel mécanisme l'ordre peut-il être donné ? Décrire le contenu du fichier de configuration associé.

Question 10 – 1 point(s) Il est nécessaire de surveiller la nappe phréatique en permanence. Pour cela, une dizaine de sondes enregistrent son état via le protocole NFS. Quelle architecture NFS Gégé peut-il utiliser pour son besoin ? Justifier à l'aide d'une explication ou d'un schéma.

Question 11 – 1 point(s) Donner les fichiers de configuration associées.

Question 12 – 1.5 point(s) Gégé s'aperçoit que son champ n'émet plus de données sur le serveur NFS depuis plusieurs mois. Décrire sa démarche d'investigation pour diagnostiquer le problème (donner cinq potentiels problèmes, la technique de diagnostic et les actions correctrices associées).

Partie III : Sécurité (5 points)

Un groupe d'utilisateurs anti-carotte du réseau social Y (anciennement *Chirper*) décide d'attaquer l'exploitation. Un pirate découvre le mot de passe SSH du datacenter en essayant des mots de passe communs.

Question 13 – 1.5 point(s) Comment se nomme cette attaque ? Comment Gégé aurait-il pu s'en prémunir ? Donner deux solutions.

Question 14 – 1.5 point(s) Le pirate n'ayant pas accès au routeur principal (protégé différemment), comment peut-il découvrir et exploiter ce qui se trouve sur le réseau (découverte ip routeur, ip carottes, services exécutés) ? Donner 3 solutions et les commandes associées.

Question 15 – 1 point(s) Il se connecte au datacenter via le compte `gege`. Il tente ensuite de se connecter au compte local de Nestor mais obtient l'erreur suivante:

```
$ su nestor
This account is currently not available
```

Que se passe-t-il ? Sous quelles conditions l'attaquant pourrait-il contourner ce problème ?

Question 16 – 0.5 point(s) Grâce aux données découvertes dans le répertoire `$HOME` de Gégé (`todo_encrypt_this.txt`), l'attaquant trouve le mot de passe du wifi. Il s'y connecte à l'aide de son ordinateur portable et souhaite effectuer une attaque *Man In the Middle* entre Nestor et le datacenter depuis sa propre machine. Il lui faut falsifier l'identité de sa machine pour détourner le trafic. Quel protocole de niveau 3 peut être empoisonné ? Justifier.

Question 17 – 0.5 point(s) Le compteur *Gégère(c)* de surveillance du réacteur s'emballe, et le bruit empêche Ylone de dormir. Elle décide d'investiguer et se rend compte de l'attaque. Elle souhaite piéger les pirates en les redirigeant vers un faux site présentant l'état des carottes (`statutcarotte.fermesupergreen.local`). Comment peut-elle s'y prendre ? Donner le contenu du fichier de configuration associé.

Partie IV : Question pour un champion (2 points)

Gégé exécute les commandes suivantes sur son terminal:

```
$ rm -rf bazar/
rm: cannot remove 'bazar/bob_leponge.txt': Permission denied
$ rm -rf bazar
$ echo $?
0
```

Question 18 – 2 point(s) Que s'est-il passé ?