

Examen : module “ Administration Système Unix / Linux ” IATIC5 2021/2022

(Date : vendredi 7 décembre 2021 – 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 (9.5 points)

Vous conseillez Jean-Eudes de la Prunellière, jeune diplômé de l'EESTEA (Eminente Ecole de Surveillance, Traque, Espionnage et beaux Arts), recruté en tant qu'expert système pour l'entreprise Grand Frère™ qui vend des accessoires et décorations de luxe (couvertures, oreillers, peintures, etc) pour clients fortunés. Officieusement, l'entreprise espionne ses clients pour collecter des données bancaires et personnelles afin de les revendre. Chaque objet dispose d'un Raspberry Pi connecté au réseau de l'entreprise.

Question 1 – 1 point(s) Un sous-réseau est dédié à l'infrastructure back-end de Jean-Eudes afin de surveiller les nœuds du réseau. D'autres sous-réseaux sont dédiés aux objets connectés. Afin de vérifier le bon fonctionnement de son infrastructure de surveillance, Jean-Eudes a besoin d'une commande **unique** permettant de vérifier la connectivité de **tous** ses serveurs de surveillance. Quelle commande devrait-il utiliser ?

Question 2 – 1 point(s) Quel est le protocole de niveau trois (modèle OSI) utilisé dans ce mécanisme ?

Question 3 – 2 point(s) Grand Frère™ décide de mettre en place un réseau VPN sur lequel les objets vont se connecter. Pour cela, Jean-Eudes souhaite utiliser l'IPv4 10.5.0.0 pour l'adressage des objets, avec un sous-réseau par type de produits. Il y a 12 123 types de produits. Quel masque de sous-réseau Jean-Eudes devrait-il utiliser ? Combien de produits peut-il connecter par sous-réseau ?

Question 4 – 1 point(s) Proposer une adresse d'un sous-réseau et une adresse d'un objet de ce sous-réseau.

Question 5 – 0.5 point(s) Pourquoi l'utilisation d'IPv4 est-elle une mauvaise idée ?

Question 6 – 2 point(s) Suite au renvoi d'un oreiller auto-chauffant en SAV pour maintenance, Jean-Eudes se rend compte que la connexion n'a pas lieu. Donner les différentes étapes de diagnostic et les causes potentielles du problème.

Question 7 – 1 point(s) Décrire le principe de la connexion initiale au serveur DHCP.

Question 8 – 1 point(s) L'oreiller ayant des ressources limitées, le service SSH installé dans le Raspberry Pi doit s'exécuter à la demande (il ne doit pas fonctionner en permanence). Donner le nom du mécanisme à utiliser et son fichier de configuration associé.

Partie II : Sauvegarde (6.5 points)

Des serveurs dans l'infrastructure sont dédiés à la collecte et au traitement des données envoyées par les objets connectés. Ces informations doivent ensuite être stockées sur un NAS.

Question 9 – 1.5 point(s) Quels services peuvent être utilisés pour envoyer les fichiers sur le NAS ? Citer 3 solutions.

Question 10 – 1 point(s) Le NAS est configuré avec 2 disques en RAID 0 (volume agrégé par bande) avec partition ext2. Choqué par les pratiques de son employeur, Jean-Eudes décide d'améliorer la résilience des données confidentielles enregistrées. On souhaite entre autres s'assurer qu'il n'y ait pas de corruptions silencieuses des données. Quel(s) système(s) de fichiers préconisez-vous pour le NAS ?

Question 11 – 1 point(s) Comment Jean-Eudes doit-il procéder afin d'installer ce nouveau système de fichiers ?

Question 12 – 1 point(s) Quels sont les quatre composants essentiels de tout système de fichiers Linux ?

Question 13 – 2 point(s) On souhaite faire face à divers scénarios catastrophes tels que: incendie, inondation, perquisition, tremblement de terre. Quelle stratégie Jean-Eudes doit-il adopter pour garantir la pérennité des données? Fournir la ou les approches avec les commandes et scripts associés.

Partie III : Sécurité (2.5 points)

Compte-tenu des activités discutables de la société, un lanceur d'alerte pourrait dénoncer Grand Frère™ à la CNIL.

Question 14 – 0.5 point(s) Quelle pratique recommanderiez-vous à Jean-Eudes afin de s'assurer qu'une saisie du matériel informatique ne puisse pas compromettre les activités de la société ?

Question 15 – 1 point(s) La connexion SSH aux objets connectés ne doit pouvoir se faire que depuis les serveurs de surveillance. Proposer une solution afin de respecter cette contrainte.

Question 16 – 1 point(s) Jean-Eudes souhaite réduire au maximum tout risque de fuite de données sur internet. Citer 2 attaques possibles et des solutions de protection.

Partie IV : Question pour un champion (1.5 points)

Jean-Eudes tape la commande suivante:

```
$ ls -lah
total 4,0K
drwxr-xr-x 19 root root          3,6K 15 nov. 08:56 .
drwxr-xr-x 19 root root          4,0K  5 juin 23:15 ..
crw-----  1 root root          10,   59 15 nov. 08:56 acpi_thermal_rel
crw-r--r--  1 root root          10,  235 15 nov. 08:56 autofs
drwxr-xr-x  2 root root          320 15 nov.  2021 block
crw-----  1 root root          10,  234 15 nov. 08:56 btrfs-control
drwxr-xr-x  3 root root           60 15 nov.  2021 bus
drwxr-xr-x  2 root root          4,0K 15 nov. 08:56 char
crw--w----  1 root tty           5,    1 15 nov. 08:56 console
lrwxrwxrwx  1 root root           11 15 nov. 08:56 core -> /proc/kcore
drwxr-xr-x 14 root root          280 15 nov. 08:56 cpu
crw-----  1 root root          10,   62 15 nov. 08:56 cpu_dma_latency
crw-----  1 root root          10,  203 15 nov. 08:56 cuse
drwxr-xr-x  8 root root          160 15 nov.  2021 disk
[...]
brw-rw----  1 root disk        259,    9 15 nov. 08:56 nvme0n1p10
brw-rw----  1 root disk        259,    2 15 nov. 08:56 nvme0n1p2
brw-rw----  1 root disk        259,    3 15 nov. 08:56 nvme0n1p3
brw-rw----  1 root disk        259,    4 15 nov. 08:56 nvme0n1p4
brw-rw----  1 root disk        259,    5 15 nov. 08:56 nvme0n1p5
brw-rw----  1 root disk        259,    6 15 nov. 08:56 nvme0n1p6
brw-rw----  1 root disk        259,    7 15 nov. 08:56 nvme0n1p8
brw-rw----  1 root disk        259,    8 15 nov. 08:56 nvme0n1p9
crw-----  1 root root        249,    1 15 nov. 08:56 nvme1
brw-rw----  1 root disk        259,   10 15 nov. 08:56 nvme1n1
brw-rw----  1 root disk        259,   11 15 nov. 08:56 nvme1n1p1
brw-rw----  1 root disk        259,   12 15 nov. 08:56 nvme1n1p2
brw-rw----  1 root disk        259,   13 15 nov. 08:56 nvme1n1p3
crw-----  1 root root          10,  144 15 nov. 08:56 nvram
crw-r----- 1 root kmem         1,    4 15 nov. 08:56 port
crw-----  1 root root        108,    0 15 nov. 08:56 ppp
crw-----  1 root root          10,    1 15 nov. 08:56 psaux
crw-rw-rw-  1 root tty          5,    2 15 nov. 09:40 ptmx
[...]
```

Question 17 – 1.5 point(s) Dans quel répertoire a-t-il tapé cette commande ? Que signifie les lettres "b" et "c" au début de certaines lignes ?