

Examen : module “ Administration Système Unix / Linux ” IATIC5 2022/2023

(Date : mardi 6 décembre 2022 – 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 (6.5 points)

La boutique de marque Grand Frère (™) propose une machine à mouvement perpétuel qui se branche sur le secteur (5000 watts). En temps de crise énergétique, le dispositif est proposé avec une option Wifi afin de permettre l'extinction à distance de cette machine.

Ylone Meusk est une collectionneuse écolo passionnée par les objets connectés et la domotique. Elle est vivement intéressée par ce produit. Afin de gérer l'ensemble de sa collection, elle souhaite organiser son réseau selon l'architecture suivante:

Trois sous-réseaux locaux:

- Réseau primaire (réseau wifi “ChezYlone”)
- Réseau domotique dédié aux objets connectés (essuie-glaces connectés avec caméras Grand Frère (™), pacemaker avec ping ...) (réseau wifi “YloneOfThings”)
- Réseau sécurisé (zone démilitarisée pour serveur web, serveur minecraft, vers l'extérieur “Ylonely”).

L'adresse principale du réseau est 198.63.22.0

Question 1 – 0.5 point(s) Quelle est la classe du réseau? Justifier.

Question 2 – 1 point(s) Proposer un masque du sous-réseau qui répond aux besoins tout en maximisant le nombre de machines possibles par sous-réseau.

Question 3 – 1 point(s) De combien d'objets connectés maximum Ylone peut-elle disposer dans sa collection ?

Question 4 – 0.5 point(s) Donner une adresse IP possible pour l'ordinateur portable d'Ylone. Justifier.

Question 5 – 0.5 point(s) Quelle est l'adresse de diffusion (broadcast) de ce sous-réseau ? Justifier.

Question 6 – 1 point(s) Configurer l'interface réseau des essuie-glaces connectés de manière persistante: fournir la commande complète ou les fichiers à éditer ainsi que leurs contenus, avec une IP réaliste, en supposant qu'il n'y a pas de serveur DHCP disponible.

Question 7 – 1 point(s) Indiquer la table de routage nécessaire à la communication des essuie-glaces avec l'ordinateur portable d'Ylone.

Question 8 – 1 point(s) Dans quelle couche du modèle OSI une adresse logique est-elle ajoutée pendant l'encapsulation ?

Partie II : Pilotes (9.5 points)

L'entreprise Grand Frère (TM) a des pratiques disruptives concernant la conception de ses objets; officieusement l'entreprise espionne ses clients dans le but de collecter des données sensibles, puis les revend au plus offrant.

Question 9 – 1 point(s) Tout le système de fichiers du disque dur (UUID=deadbeef1337) de la machine à mouvement perpétuel est en lecture seule. Donner le nom du fichier ainsi que la ligne à ajouter qui a permis de réaliser cette tâche.

Question 10 – 1.5 point(s) Quel est l'intérêt de configurer ce système de fichiers en lecture seule ? (Donner 3 avantages)

Question 11 – 1 point(s) Lorsque l'appareil démarre, il télécharge un pilote en mémoire dans /tmp (en RAM) qui donne un accès facile aux paquets bruts du réseau à des fins d'espionnage, via un fichier spécial. De quel type de pilote s'agit-il ? Justifier et donner la procédure pour son chargement.

Question 12 – 0.5 point(s) A quoi sert un numéro majeur et un numéro mineur ?

Question 13 – 1 point(s) Donner la configuration nécessaire complète (commandes, fichiers, etc ...) afin que le téléchargement s'exécute au démarrage de l'appareil. Préciser les dépendances entre services, s'il y en a.

Question 14 – 0.5 point(s) Jean-Eudes de la Prunellière, concepteur de la machine à mouvement perpétuel, a écrit un script bash "powerful_sniffer.sh" qui capture l'ensemble des paquets circulant sur l'interface réseau via le pilote précédemment téléchargé. Comment ce script peut-il s'assurer que le pilote est bien chargé ?

Question 15 – 1 point(s) Comment ce script peut-il facilement interagir avec le pilote ? Donner un exemple.

Question 16 – 1 point(s) Le script doit être exécuté toutes les 5 minutes. Comment Jean-Eudes peut-il réaliser cette tâche ? Fournir les commandes ou contenus de fichiers requis.

Question 17 – 1 *point(s)* Tous les paquets circulant sur le réseau sont effectivement consultables. Quel équipement réseau peut être responsable de cela ?

Question 18 – 1 *point(s)* Dans un objectif de parfaire la sécurité de la machine (et peut-être aussi pour ne pas se faire repérer ...), Jean-Eudes souhaite transférer les données vers les serveurs de son entreprise de façon totalement chiffrée. Proposer 2 solutions pour accomplir cette tâche.

Partie III : Sécurité (2 points)

Ylone s'aperçoit que ses WC connectés se déclenchent toutes les 5 minutes depuis 3 semaines, ainsi que le lave-linge, provoquant la perte de milliers de litres d'eau. Le bruit empêche Ylone, soucieuse d'économie énergétique, de se concentrer sur le tri de ses emails. Les dysfonctionnements coïncident avec la mise en marche de l'appareil à mouvement perpétuel.

Elle découvre un port série caché sur la machine et décide de s'y connecter à l'aide d'un terminal. Une invite de commande s'ouvre.

Question 19 – 2 *point(s)* Elle souhaite comprendre pourquoi sa maison est devenue hors de contrôle. Décrire l'ensemble de sa démarche d'investigation (commandes, fichiers, ...) afin de détecter une activité suspecte. On supposera que toutes les commandes de bases sont disponibles (système Linux).

Partie IV : Question pour un champion (2 points)

Pour assurer la maintenance, Jean-Eude souhaite maintenir son accès SSH aux différentes machines, une fois celles-ci vendues. Cependant, il n'a aucun contrôle sur les réseaux de ses clients.

Question 20 – 2 *point(s)* Comment peut-il initier une connexion si la machine est derrière un NAT / pare-feu ? On suppose que Jean-Eude ne veut pas utiliser le VPN, mais que les pare-feux des clients autorisent toutes les connexions sortantes.