Questionnaire Candidat

Bachelors 3 pour Système Réseaux et cybersécurité

Ce questionnaire contient 2 parties. Une première partie avec des questions sur vos connaissances générales en système, réseau et sécurité.
La deuxième partie est un projet à réaliser.

Système

Question 1

Dans un terminal (BASH), vous tapez la commande: ***ps -ef | grep ssh*** pour:

- Lister les fichiers de votre répertoire HOME?
- Connaître les utilisateurs connectés à votre session
- Lister les processus actifs puis filtrer la recherche
- Avoir un état de lieux de l'utilisation mémoire

Quelle autre commande pourriez-vous utiliser sous Debian/Ubuntu pour avoir plus d'informations?

ps -aux | grep ssh

Question 2

Comment passer un ou plusieurs arguments à un script BASH?
Passer des arguments à un script BASH se fait directement via la ligne de commande lorsqu' on exécute le script. On peut accéder à ces arguments dans le script en utilisant des variables positionnelles comme $1, $2, etc., et $@ pour accéder à tous les arguments.
Donnez des exemples de redirection des E/S standard pour passer un argument à un script.
Script BASH (argument.sh)

```
 GNU nano 7.2                          argument.sh *
#!/bin/bash

echo "Le premier argument est : $1"
echo "Le deuxième argument est : $2"
echo "Tous les arguments sont : $@"
```

Exécution du script avec des arguments:

bash argument.sh arg1 arg2

Redirection des E/S standard pour passer un argument à un script:

1)Redirection de l'entrée standard (stdin):

```
#!/bin/bash

while read line; do
    echo "Ligne lue : $line"
done
```

exécution du script avec redirection de l'entrée:
bash lecture.sh < entree.txt

Redirection de la sortie standard (stdout):

```
#!/bin/bash

echo "Ceci est un message"
```

Exécution du script avec redirection de la sortie:

bash message.sh > sortie.txt

Question 3

Dans quel environnement est exécuté un script inscrit dans la crontab de l'utilisateur */home/debianUser* ?

/home/debianUser

Question 4

Citez et décrivez brièvement les 4 états des processus dans un environnement Unix/Linux.

Dans un environnement Unix/Linux, un processus peut être dans l'un des quatre principaux états qui représentent différentes phases de l'exécution et de la gestion des processus par le système d'exploitation.
ces états sont les suivants:

1)running:Un processus est dans l'état "Running" lorsqu'il est actuellement en train d'être exécuté par le processeur.

2)sleeping:Un processus est dans l'état "Sleeping" lorsqu'il est en attente de la disponibilité d'une ressource ou d'un événement spécifique.

3)stopped:Un processus est dans l'état "Stopped" lorsqu'il a été interrompu ou suspendu par un signal. Cela peut se produire pour plusieurs raisons, telles que le débogage ou une pause explicite par l'utilisateur.

4)zombie:Un processus est dans l'état "Zombie" lorsqu'il a terminé son exécution, mais son entrée dans la table des processus n'a pas encore été supprimée par son processus parent. Un processus zombi conserve son PID (Process Identifier) et des informations minimales sur son exécution passée.

Réseau

Question 1

Sur un réseau Ethernet, que fera un host ou un équipement qui reçoit une trame contenant une adresse MAC unicast qui ne correspond pas à sa propre adresse MAC ?

- Il rejette la trame
- Il transmet la trame à l'hôte suivant.
- Il retire la trame
- Il de-encapsule la trame pour trouver l'adress IP dans le paquet

Question 2

Sur quelle couche du modèle OSI va travailler

- Un commutateur (switch)?:couche 2(couche liaison des données)
- Un router ?:couche 3(couche réseau)
- Le protocole TCP ?:couche 4(couche transport)
- HTTP?: couche 7(couche application)

Question 3

On vous donne une trame réseau en hexadécimal. Quel outil/logiciel pouvez vous utiliser pour l'interpréter?
-Tcpdump ou Wireshark

Question 4

Quels champs appartiennent à un paquet TCP ? Sélectionnez tous les champs possibles.

- Adress IP source
- Adresse MAC destination
- Adresse MAC source
- Data
- MIT
- FCS
- TTL
- Header Checksum
- Window Size
- Ack Number
- Adresse IP destination
- Control Bits
- Application Layer data

Question 5

Quel est le but d'une attaque d'ARP spoofing?

- Inonder le réseau avec des réponses aux ARP Broadcasts
- Remplir la table des adresse MAC du commutateur avec des adresses erronées
- Associer une adresse IP avec un adresse MAC erronée
- Inonder le réseau avec des requêtes ARP

Sécurité

Question 1

Existe-t-il une norme pour la sécurité informatique?

=> Oui, il existe plusieurs normes pour la sécurité informatique tels que :ISO/IEC 27001,ISO/IEC 27002, ISO 27701,NIST,PCI DSS,NIS2,etc

Question 2

Concernant la sécurité, quelles institutions/agences pouvez-vous citer pour la France?

Institutions/Agences pour la Sécurité en France:

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information):l'autorité nationale en matière de sécurité et de défense des systèmes d'information en France
- CNIL (Commission Nationale de l'Informatique et des Libertés):l'autorité française chargée de veiller à la protection des données personnelles.

A l'international?

- NIST (National Institute of Standards and Technology):Une agence du Département du Commerce des États-Unis qui développe des normes et des directives en matière de cybersécurité.
- OWASP (Open Web Application Security Project):une organisation mondiale à but non lucratif dédiée à la sécurité des applications web.

Question 4

Avec votre usage habituel du numérique (PC, tablette, téléphone), quels sont les moments où vous êtes vulnérables ?
Quels pourraient en être les conséquences?
Qui d'autre pourrait être impacté d'une faille de sécurité chez vous (ou dans votre entreprise)?

On est vulnérable lors de:

- Connexion à des réseaux Wi-Fi publics :les réseaux publics non sécurisés peuvent être des cibles pour certaines attaques informatiques qui ont comme consequences:Vol de données sensibles, mots de passe ou des informations

bancaires.Les autres qui peuvent être impactés sont:les contacts ou les entreprises si des informations professionnelles sont compromises.

- Téléchargement et installation de logiciels/applications :le téléchargement de logiciels malveillants ou de fichiers compromis.
  Conséquences : Infections par des virus, ransomwares, ou autres malwares.
  Les autres qui peuvent êtres impactés sont:les applications professionnelles installées dans mon portables.

- Ouverture d'e-mails et de pièces jointes malveillantes avec comme conséquences:Compromission de comptes, vol d'identité, propagation de malwares. Les autres qui peuvent être impactés sont:les contacts de messagerie, entreprise si le compte professionnel est compromis.