La Plateforme

Questionnaire Candidat

Bachelors 2 pour Système Réseaux et cybersécurité

Première partie : questions de connaissances générales en système, réseau et sécurité.

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 commande pourriez-vous utiliser sous Debian/Ubuntu pour avoir plus d'informations?
On pourrait utiliser la commande ***ps aux | grep ssh*** pour obtenir davantage d'informations sur les processus actifs liés à SSH. Les options ***aux*** permettent d'afficher les processus actifs de tous les utilisateurs (***a***), les informations utilisateurs (***u***), sans terminal associé (***x***).

Question 2

Quelle commande utiliser pour connaître l'état de vos interfaces réseaux?
La commande ***ip a***.

Question 3

Donnez des cas d'application des différents types d'hyperviseurs.
Les hyperviseurs de type 1 prennent la place de l'OS (comme Proxmox, qui permet de virtualiser un serveur) et les hyperviseurs de type 2 s'installent par dessus la couche de l'OS (comme VirtualBox, qui permet de créer des VM sur un ordinateur).

Réseau

Question 1

Quels protocoles connaissez-vous? HTTP, HTTPS, SSH, TCP/UDP, IP, FTP, SFTP, SMTP, TLS
Pouvez-vous les classer par types et dire lesquels représentent un enjeu de sécurité?
On peut les classer selon le modèle OSI :
7 - Application : HTTP, HTTPS, SMTP, SSH, FTP, SFTP
5 - Session : TLS
4 - Transport : TCP/UDP
3 - Réseau : IP
Tous les protocoles mentionnés représentent un enjeu de sécurité.

Question 2

Sur quelle couche du modèle OSI va travailler

- Un commutateur (switch)? couche 2 - Liaison
- Un router ? couche 3 - Réseau
- Le protocole TCP ? couche 4 - Transport
- HTTP? couche 7 - Application

Question 3

Quel de ces types va utiliser le serveur DNS donner l'adresse d'un serveur ?

- A record
- NS record
- MX record
- AAAA record

Question 4

Pendant le handshake de connexion TCP, quels messages sont envoyés?

- ACK et FIN
- FIN et RESET
- RESET et SYN
- SYN et ACK

Sécurité

Question 1

Existe-t-il une norme pour la sécurité informatique?
Il existe plusieurs ‘normes’ : la norme ISO 27001, le RGPD, l’HIPAA, le NIST.

Question 2

Concernant la sécurité, quelles institutions/agences pouvez-vous citer pour la France? A l'international?
L’ANSSI et la CNIL en France, le NIST à l’international.

Question 3

Avec votre usage habituel du numérique (PC, tablette, téléphone), quels sont les moments où vous êtes vulnérables ? Lorsque mon matériel est déverrouillé, en utilisant des mots de passe pas suffisamment sécurisés, en naviguant sur des sites non sécurisés, en ouvrant des pièces jointes malveillantes, etc.
Quels pourraient en être les conséquences? Perte ou vol de données.
Qui d'autre pourrait être impacté d'une faille de sécurité chez vous (ou dans votre entreprise)? Tout ce qui est connecté au réseau (par exemple, dans une entreprise : le matériel informatique des collaborateurs, les serveurs, les équipements réseaux, etc).