



## 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?

**top ou htop**

#### Question 2

Comment passer un ou plusieurs arguments à un script BASH?

**./exemple.sh argument1 argument2**

Donnez des exemples de redirection des E/S standard pour passer un argument à un script.

**Entrée : ./exemple.sh < inputfile**

**Sortie : ./exemple.sh > outputfile**

### Question 3

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

**Dans l'environnement de l'utilisateur spécifié.**

### Question 4

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

**Running (R) :** Le processus est en cours d'exécution ou prêt à être exécuté.

**Sleeping (S) :** Le processus attend un événement ou une ressource.

**Stopped (T) :** Le processus est arrêté par un signal ou un débogueur.

**Zombie (Z) :** Le processus est terminé, mais son entrée dans la table des processus n'a pas été nettoyée.

## 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)? **2**
- Un router ? **3**
- Le protocole TCP ? **4**
- HTTP? **7**

### Question 3

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

**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, ISO/IEC27001.**

## Question 2

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

A l'international?

**En France : ANSSI**

**À l'international : NIST**

## Question 4

Avec votre usage habituel du numérique (PC, tablette, téléphone), quels sont les moments où vous êtes vulnérables ?

**Réseaux publics, downloads et social engineering.**

Quels pourraient en être les conséquences ?

**Vol de données et piratage de comptes.**

Qui d'autre pourrait être impacté d'une faille de sécurité chez vous (ou dans votre entreprise)?

**La famille et les amis, les collègues de travail, et l'entreprise.**

# Projet VPN

---

Sur un environnement Linux Debian virtualisé, vous allez installer un VPN et le sécuriser.

## Partie 1

Vous pouvez utiliser l'outil `easy-rsa` qui est fourni avec OpenVPN pour le faire. Suivez les instructions pour générer les clés et les certificats.

Ensuite, vous devrez configurer le serveur OpenVPN: créez un fichier de configuration pour le serveur et spécifiez les paramètres nécessaires pour permettre à deux utilisateurs de se connecter.

Pour sécuriser le VPN, vous devrez activer un cryptage fort. OpenVPN supporte plusieurs algorithmes de cryptage, tels que AES et Blowfish. Choisissez un algorithme de cryptage considéré comme sûr.

Enfin, lancez le serveur OpenVPN en exécutant la commande appropriée. Vous devriez maintenant être en mesure de vous connecter au VPN à partir d'autres appareils.

## Partie 2

Ajoutez le service VPN au `systemd` afin qu'il se lance automatiquement au démarrage du serveur..

Configurez un firewall afin que seules les connexions HTTP soient permises aux utilisateurs se connectant au VPN.

## Partie 3

Vous pouvez également sécuriser le VPN en activant l'authentification à deux facteurs. Cela exige que les utilisateurs fournissent une forme supplémentaire d'authentification, comme un code envoyé sur leur téléphone, avant de pouvoir se connecter au VPN.

Pour activer l'authentification à deux facteurs, vous devrez utiliser un logiciel tel que Google Authenticator ou Duo. Suivez les instructions pour le configurer.

## Rendu

Sur un repository github, envoyez vos fichiers de configuration du serveur, et les scripts/configurations utilisés pour créer les utilisateurs .

Dans un fichier PDF, vous devrez vous présenter en quelques lignes et parler de votre intérêt pour la cybersécurité.

Vous devrez également copier le lien vers votre repository github où se trouve le travail demandé ci-dessus.