A. Connaissances Générales

1. Système

Question 1:
La commande `ps -ef | grep ssh` permet de lister les processus actifs puis filtrer la recherche. On pourrait utiliser les commandes `top` (se rafraîchit toutes les 3 secondes) ou `htop` pour visualiser les processus actifs en temps réel. La commande `top` permet notamment de voir l'utilisation des ressources de l'ordinateur (processeur, mémoire) et bien d'autres mesures.

Question 2:
La syntaxe pour passer un ou plusieurs arguments à un script est `./script.sh arg1 arg2`. On sépare les arguments par des espaces et on utilise `$1, $2` pour récupérer leurs valeurs dans le script (car `$0` correspond au nom du script).

Exemples de redirection pour passer un argument à un script:

1. **En entrée:** `./script.sh < fichier.txt` (stdin est utilisée).
2. **En sortie:** `./script.sh | head -n 15` (aussi appelé tube).

On peut également utiliser la substitution de commande: `./script.sh $(cat fichier.txt)`.

Question 3:
Un script exécuté via la Crontab de `/home/debianuser` s'exécute dans un environnement dit "minimal" de l'utilisateur, car certaines variables accessibles via le terminal ne sont pas chargées sauf si définies manuellement dans Crontab. (Exemple: `PATH=/usr/bin:/bin` au lieu de la valeur actuelle dans le terminal).

Question 4:
Les 4 états des processus dans un environnement Unix/Linux sont:

1. **Running (R):** En cours d'exécution.
2. **Sleeping (S):** En attente d'une ressource (ex: `cat` sans argument fourni).
3. **Stopped (T):** Suspendu ou mis en pause (ex: `ping google.com` puis `CTRL+Z`).
4. **Zombie:** Terminé, mais non libéré par le processus parent.

2. Réseau

Question 1:
Si un appareil reçoit une trame contenant une adresse MAC unicast ne correspondant pas à la sienne, il rejette la trame (ignore).

Question 2:

1. **Un commutateur (Switch):** La couche 2 (liaison de données).
2. **Un routeur:** La couche 3 (réseau qui traite les adresses IP).
3. **Un protocole TCP:** La couche 4 (transport de données).
4. **HTTP:** La couche 7 (application).

Question 3:
Pour interpréter une trame hexadécimale, on peut utiliser **Wireshark** (application bureau) ou **tcpdump** (accessible en ligne de commande terminal).

Question 4:
Les champs qui appartiennent à un paquet TCP sont:

- Data
- Window size
- Ack Number
- Control bits
- Application Layer Data

Question 5:
Le but d'une attaque ARP est d'associer une adresse IP à une adresse MAC erronée.

3. Sécurité

Question 1:
Oui, il existe plusieurs normes qui régissent la sécurité informatique, telles que:

- **ISO/IEC 27001:** Norme internationale établissant les exigences pour mettre en œuvre et maintenir un système de management de la sécurité informatique.
- **Le NIST Cybersecurity Framework:** Développé par le National Security Institute of Standards, il fournit des lignes directrices afin de gérer les risques liés à la cybersécurité.
- **PCI DSS:** S'adresse aux organisations traitant des données de cartes bancaires.

Question 2:
Institutions/Agences:

- **En France:**
    - **L'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Informations) fournit des directives, des certifications et intervient en cas de cyberattaques majeures.
    - **La CNIL** (Commission Nationale de l'Informatique et des Libertés) veille à la protection des données personnelles et la vie privée.
- **À l'international:**
    - **ENISA** (European Union Agency for Cybersecurity) est l'agence européenne chargée de renforcer la cybersécurité dans les États membres.
    - **CERTs** (Computer Emergency Response Team) sont des équipes de réponse aux incidents de sécurité informatique présentes dans de nombreux pays.
    - **NIST** cité plus haut.

Question 3:
Les moments où l'on est le plus vulnérable incluent:

- L'utilisation de réseaux Wi-Fi publics.
- Le téléchargement de fichiers ou d'applications.
- L'utilisation de mots de passe faibles.

- L'ouverture de pièces jointes ou de liens suspects.

Les conséquences peuvent inclure:

- Le vol de données.
- Des pertes financières.
- Une atteinte à la réputation.

En cas de faille de sécurité, d'autres personnes comme la famille, les amis, ou les collègues, ainsi que les clients ou partenaires de l'entreprise, pourraient également être impactés.

B. Projet VPN

J'ai créé configuré une machine virtuelle locale (Ubuntu 24.04) en utilisant **VirtualBox**.

Dépôt Github

Étape 1: Installation d'OpenVPN

1. Mettre à jour le système :

```
sudo apt update && sudo apt upgrade -y
```

2. Installer OpenVpn et easy-rsa (pour générer les certificats et les clés):

```
sudo apt install openvpn easy-rsa -y
```

Etape 2: Génération des clés et certificats

1. Création d'un répertoire pour easy-rsa:

```
mkdir ~/easy-rsa
ln -s /usr/share/easy-rsa/* ~/easy-rsa/
chmod 700 ~/easy-rsa
cd ~/easy-rsa
```

2. Créer un PKI (Public Key Infrastructure):

```
./easy-rsa init-pki
```

La commande crée le répertoire pki qui contiendra les certificats et clés.

3. Générer le certificat de l'autorité de certification (CA) utilisée pour signer les certificats:

```
./easy-rsa build-ca
```

Cette commande génère les fichiers ca.crt et ca.key.

4. Générer les certificats pour le serveur et les clients (dans le cas d'une configuration manuelle du client):

```
./easyrsa gen-req server nopass
./easyrsa sign-req server server
./easyrsa gen-req client1 nopass
./easyrsa sign-req client client1
```

5. Générer une clé Diffie-Hellman (pour l'échange de clés):

```
./easyrsa gen-dh
```

6. Générer une clé HMAC:

```
openvpn --genkey --secret ta.key
```

Renforce la sécurité des communications.

Étape 3: Configuration du serveur OpenVPN

1. Créer un fichier de configuration:

```
sudo nano /etc/openvpn/server.conf
```

2. Démarrer le serveur OpenVPN avec:

```
sudo openvpn --config /etc/openvpn/server.conf
```

Étape 4: Ajout du serveur OpenVPN à systemd (pour un démarrage automatique)

```
sudo systemctl start openvpn@server.service
sudo systemctl enable openvpn@server.service
```

Étape 5: Configuration d'un pare-feu avec UFW

```
sudo apt update && sudo apt upgrade
sudo apt install ufw -y
sudo ufw allow 1194/udp
sudo ufw enable
```

Étape 6: Configuration l'authentification à deux facteurs

A. Installation de Google Authenticator

1. Installation Google Authenticator:

```
sudo apt install libpam-google-authenticator -y
```

2. Configuration manuelle Google Authenticator pour un client:

```
google-authenticator
```

B. Configuration de OpenVPN pour utiliser 2FA

1. Ajout au fichier de configuration OpenVPN: `plugin /usr/lib/x86_64-linux-gnu/openvpn/plugins/openvpn-plugin-auth-pam.so openvpn`
2. Création un fichier PAM `/etc/pam.d/openvpn` sur le serveur et ajouter `auth required pam_google_authenticator.so`.

Modifications apportées à la configuration 2FA

Pour l'authentification à deux facteurs, j'ai utilisé un script shell provenant de ce dépôt GitHub: outil openvpn_2fa utilisé.

J'ai modifié le fichier **manage.sh** pour automatiser:

1. La génération de certificats et de clés.
2. La génération de fichiers de configuration clients (.ovpn).
3. La configuration de Google Authenticator pour le client.

Problèmes rencontrés lors de l'implémentation du projet VPN

1. **Problème de connexion à Internet via le VPN**
   Lors de la connexion au serveur VPN, bien que la connexion au serveur soit réussie, il était impossible d'accéder à Internet (par exemple, les commandes comme `ping google.com` échouaient). Après avoir analysé les erreurs avec **systemctl**, j'ai découvert que le problème venait de la redirection IP. Le trafic entre le client VPN et Internet n'était pas correctement acheminé. J'ai résolu ce problème en

activant la redirection IP en modifiant la valeur de `net.ipv4.ip_forward=1` (de 0 à 1) dans le fichier `/etc/sysctl.conf` et en enregistrant les modifications avec:

```
sudo sysctl -p
```

2. **Problème de configuration du pare-feu**
   Un problème similaire s'est produit lors de la configuration du **pare-feu**. Pour le résoudre, j'ai dû configurer les règles NAT en ajoutant la ligne suivante au fichier `/etc/ufw/before.rules` :

   ```
   -A POSTROUTING -s 10.9.0.0/24 -o enp0s3 -j MASQUERADE
   ```

   Ensuite, j'ai rendu ces règles persistantes pour qu'elles soient appliquées automatiquement au redémarrage du serveur en exécutant la commande :

   ```
   sudo netfilter-persistent save
   ```