2nde BAC Pro CIEL	LINUX Securisation de base du serveur	
		 Année 2025/2026

Nom		
Prénom		
Date		
<u>Matériel</u> <u>Outillage</u> 	⇨ VM DEBIAN PROXMOX	<u>Durée</u> : 3H 
<u>Travaux à réaliser</u> 	⇨ Sécurisation du serveur	
<u>Pôle d'activité :</u> Mise en œuvre de réseaux informatiques		
<u>Activités :</u> ⇨ **R3** : Exploitation et maintien en condition opérationnelle		
<u>Compétences :</u> ⇨ **C06** : Valider la conformité d'une installation ⇨ **C09** : Installer les éléments d'un système électronique ou informatique ⇨ **C10** : Exploiter un réseau informatique		
		
Lorsque le logo  apparaît, il est indispensable d'appeler l'enseignant pour vérification.		

A. Mise en contexte

L'entreprise CyberABE Solutions commence à déployer ses premiers serveurs Debian pour héberger des services internes (web, stockage, supervision, authentification...).

Les audits internes de cybersécurité exigent que chaque serveur soit sécurisé selon des règles minimales avant d'être mis en production.

Tu fais partie de l'équipe "Exploitation & Cybersécurité", et ta mission consiste désormais à mettre en place les mesures essentielles de sécurité pour protéger le serveur contre :

- ⇨ les connexions non autorisées
- ⇨ les comptes dangereux
- ⇨ les services inutiles
- ⇨ les failles de configuration
- ⇨ les attaques réseau simples

Un premier audit automatique montre plusieurs faiblesses : compte root accessible, port SSH par défaut, services inutiles actifs, journaux non surveillés, permissions trop ouvertes...

Le responsable te demande donc de renforcer la sécurité basique du serveur avant qu'il soit intégré dans l'infrastructure finale.

B. Problématique

Comment sécuriser un serveur Debian en appliquant des mesures simples mais essentielles pour limiter les attaques, réduire les risques d'accès non autorisés et renforcer la fiabilité du système ?

C. Compétences

C01 COMMUNIQUER EN SITUATION PROFESSIONNELLE (ANGLAIS/FRANÇAIS)	
La présentation (typographie, orthographie, illustration, lisibilité) est soignée et soutient le discours avec des enchaînements cohérents	
La présentation orale (support et expression) est de qualité et claire	
L'argumentation développée lors de la présentation et de l'échange est de qualité	
L'argumentation tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit	
C03 PARTICIPER A UN PROJET	
Les rôles et tâches de chacun sont identifiés ; le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte	
Le planning prévisionnel est compris	
Le suivi du projet est respecté	
L'espace collaboratif est correctement utilisé	
C04 ANALYSER UNE STRUCTURE MATÉRIELLE ET LOGICIELLE	
Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines	
Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents	
Les informations nécessaires sont extraites des documents réglementaires et/ou constructeurs	
Les indicateurs de fonctionnement sont interprétés	
Les fiches de test ou d'intervention sont renseignées	
C06 VALIDER LA CONFORMITÉ D'UNE INSTALLATION	
Les exigences du cahier des charges sont respectées	X
Les tests sont effectués	X
Les résultats attendus sont vérifiés	X
La procédure de test est respectée	X
C07 RÉALISER DES MAQUETTES ET PROTOTYPES	
Le placement et routage sont conformes au cahier des charges	
La génération des fichiers de fabrication du PCB est conforme aux attentes	
Le PCB est réalisé, contrôlé et conforme aux IPC (tolérances mécaniques, finition de surface, propreté, ESD etc.)	
Les composants sont conformes à la nomenclature (marquage, étiquetage)	
La nomenclature des composants est respectée	
Le brasage de la carte est conforme à la nomenclature et aux IPC	
Les contraintes liées aux impacts environnementaux sont intégrées	
Le contrôle visuel de la carte assemblée est conforme au dossier de fabrication	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C08 CODER	
Les environnements de développement et de test sont mis en oeuvre en tenant compte des contraintes de fonctionnalités et de sécurité	
Le module logiciel est débogué et syntaxiquement correct	
Les composants logiciels individuels sont développés et testés conformément aux spécifications du cahier des charges et des bonnes pratiques	
La solution (logicielle et matérielle) est intégrée et testée conformément aux spécifications du cahier des charges et des bonnes pratiques	
Le code est commenté et le logiciel est documenté	

C09 INSTALLER LES ÉLÉMENTS D'UN SYSTÈME ÉLECTRONIQUE OU INFORMATIQUE	
L'ensemble des éléments pour l'installation du système est complet et vérifié par rapport au cahier des charges	X
Les éléments du système sont installés et raccordés selon une procédure	X
La configuration est réalisée	X
La mise en service est réalisée	X
L'état de l'installation est renseigné de manière écrite ou orale	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	X
C10 EXPLOITER UN RÉSEAU INFORMATIQUE	
Les alertes et problèmes rencontrés sont renseignés	X
Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés	
La mise à jour des équipements (iOS, OS, logiciel, firmware) est effectuée	
Les optimisations nécessaires sont effectuées	X
C11 MAINTENIR UN SYSTÈME ÉLECTRONIQUE OU RÉSEAU INFORMATIQUE	
L'intervention est préparée	
Le dysfonctionnement est constaté	
La maintenance ou la réparation est réalisée	
La fiche d'intervention est correctement renseignée	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	

Nature de complexité de l'activité :

Découverte	
Intermédiaire	X
Bac Pro	

D. Retrait des utilisateurs inutiles

Vérifier la liste des utilisateurs du système.

Si des utilisateurs autre que vous sont présent, **supprimer**-les ainsi que leur répertoire personnel.

Vérifier que seul votre répertoire personnel est présent dans l'environnement de travail des utilisateurs.

Si d'autres répertoire, autre que le vôtre, apparait, **supprimer** les.

E. Mot de passe

La commande `passwd` permet de changer le mot de passe du compte courant.

Proposer un mot de passe pour le compte super-utilisateur et votre compte en vous aidant de l'annexe 1.

	Nouveau mot de passe
root	
votre utilisateur	

Changer les deux mots de passe et **valider** leur bon fonctionnement.

F. Sécurité renforcé SSH

Les modifications suivantes s'opèrent dans le fichier de configuration du serveur SSH.

- ⇨ Limiter la tentative d'authentification à 3 essais (MaxAuthTries)
- ⇨ Limiter le délai d'inactivité à 60 secondes (ClientAliveInterval)

G. Permission du répertoire personnel

Vérifier que votre répertoire personnel vous appartienne et que vous êtes le seul à pouvoir y effectuer toutes les actions. Si ce n'est pas le cas, **effectuer** les opérations nécessaires.

H. Surveillance SSH

La commande suivante permet de lister les journaux (logs) du serveur SSH et de n'afficher que les 20 dernières lignes en temps réel.

```
$ journalctl -u ssh | tail -n 20
```

Entrer la commande.

Ouvrir une nouvelle fenêtre Putty et **réaliser** des tests de connexion (réussies et échec) sur votre serveur afin d'observer l'avancement du log dans la fenêtre principal (journalctl ...)

I. Installation et paramétrage de sudo

Réaliser l'installation du paquet « sudo ».

Vérifier la présence du groupe « sudo » dans le système.

Si le groupe sudo n'apparait pas, appeler l'enseignant.

Ajouter votre utilisateur dans le groupe « sudo ».

Vérifier la présence de votre utilisateur dans le groupe « sudo ».

Editer le fichier le fichier `/etc/sudoers`

Ajouter la ligne suivante :

```
username ALL = (ALL:ALL) ALL
```

Avec *username* votre nom d'utilisateur.

Cette ligne permet d'autoriser à votre utilisateur d'utiliser les commandes de super-utilisateur depuis son commande grâce à la commande sudo.

Avec votre compte utilisateur **tester** la commande `sudo -v` afin de **valider** le bon fonctionnement.

Si un problème apparait lors de l'utilisation de la commande, appeler l'enseignant.

Désormais, lorsque vous souhaitez utiliser une commande root, vous avez simplement à précéder la commande par `sudo`.

J. Désactivation de la connexion root

Maintenant que votre utilisateur peut effectuer des opérations de super-utilisateur grâce à sudo, vous allez devoir « désactiver » le compte root pour des questions de sécurité évidente.

Pour verrouiller le compte super-utilisateur, **entrer** la commande suivante :

```
$ sudo passwd -l root
```

Essayer de vous connecter.

Si vous arrivez à vous connecter en super-utilisateur, appeler l'enseignant.

Annexe 1 : Complexité d'un mot de passe

Nombre de caractères	Uniquement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Lettres minuscules et majuscules + chiffres	Lettres min. et maj. + chiffres + caractères spéciaux
4	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT
6	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	1 sec	5 sec
8	IMMÉDIAT	5 sec	22 min	1 heure	8 heures
10	IMMÉDIAT	58 min	1 mois	7 mois	5 ans
12	25 sec	3 semaines	300 ans	2 000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années
16	2 jours	34 000 ans	2 milliards d'années	37 milliards d'années	1 milliard de milliards d'années