PROJET DE DURCISSEMENT (HARDENING) D'UN POSTE DE TRAVAIL

BTS SIO – Lycée Turgot – Année scolaire 2025–2026

Sommaire

1. PRÉSENTATION GÉNÉRALE DU PROJET

Dans le cadre de notre formation en BTS Services Informatiques aux Organisations (SIO) au lycée Turgot, situé au 69 rue de Turbigo à Paris (3e arrondissement), nous avons réalisé un projet de durcissement (hardening) d'un poste de travail.

Ce projet s'inscrit dans une démarche pédagogique visant à nous confronter à des problématiques concrètes de cybersécurité, proches de celles rencontrées en entreprise ou dans une administration publique.

Le projet a été proposé par un ancien étudiant de BTS SIO, aujourd'hui professionnel de la cybersécurité, afin de nous permettre d'appliquer nos compétences techniques dans un contexte réaliste et structuré. L'objectif n'est pas seulement d'appliquer des mesures de sécurité, mais aussi de **documenter, justifier et auditer chaque action réalisée**.

2. CONTEXTE ET MISE EN SITUATION

La mise en situation retenue est celle d'un **poste informatique utilisé par des fonctionnaires de la mairie du 3e arrondissement de Paris**.
Le poste doit répondre à des exigences élevées en matière de sécurité, de stabilité et de conformité, tout en restant utilisable au quotidien par des agents non techniques.

L'ensemble du projet est réalisé dans un **environnement de test**, à l'aide de machines virtuelles, afin d'éviter tout impact sur des postes réels.
Cette approche permet de reproduire fidèlement un environnement professionnel tout en respectant les contraintes de sécurité.

Les mesures de durcissement appliquées s'appuient exclusivement sur les **recommandations officielles de l'ANSSI**, garantissant ainsi une base fiable, reconnue et conforme aux standards français de cybersécurité.

3. OBJECTIFS DU PROJET

L'objectif principal du projet est de **sécuriser un poste de travail Linux (Ubuntu)** en appliquant des mesures de durcissement pertinentes et adaptées à l'environnement cible.

Les objectifs détaillés sont les suivants :

- Mettre en œuvre **au minimum 10 mesures concrètes de durcissement**
- Identifier les failles de sécurité avant et après durcissement
- Garantir la confidentialité, l'intégrité et la disponibilité du système
- Documenter l'ensemble des actions réalisées de manière claire et traçable
- Créer un **site web local** permettant de suivre l'application des mesures
- Comparer l'état du poste avant et après sécurisation à l'aide d'audits

Ce projet vise également à développer notre **rigueur méthodologique**, essentielle dans les métiers de l'informatique et de la cybersécurité.

4. PRÉSENTATION DU CLIENT

Le client du projet est **Maël Chatelu**, ancien étudiant en BTS SIO.
Il occupe aujourd'hui le poste d'**ingénieur en cybersécurité**, avec une spécialisation en tant qu'analyste SOC (Security Operations Center).

Dans son activité professionnelle, il est chargé de :

- Surveiller la sécurité de plusieurs systèmes d'information
- Analyser les incidents de sécurité
- Générer des rapports d'audit à l'aide de scripts automatisés

Grâce à son parcours en BTS SIO, il connaît précisément le niveau technique et méthodologique attendu d'un étudiant.
Cela lui a permis de proposer un projet **réaliste, professionnalisant et adapté** à notre formation.

5. ORGANISATION DE L'ÉQUIPE PROJET

Le projet est réalisé par une équipe de **trois étudiants**, avec une répartition claire des rôles afin d'assurer une bonne organisation et un suivi efficace.

Titouan Bouché – Chef de projet

Il est responsable de :

- La rédaction de la documentation interne
- La répartition et le suivi des tâches
- Le contrôle de l'avancement du projet
- La vérification de la qualité des livrables

Son rôle est essentiel pour garantir la cohérence globale du projet et le respect des objectifs fixés.

Raphaël Samarakoon – Recherche et développement

Ses missions principales sont :

- La réalisation de tests techniques
- La participation aux audits de sécurité
- La recherche et l'analyse des recommandations de l'ANSSI
- La création du site web de suivi du projet

Waya Chemla – Technicien et moteur du projet

Il est chargé de :

- La réalisation des audits de sécurité
- La rédaction des documentations techniques et procédures
- La mise en œuvre concrète des mesures de durcissement
- Le suivi régulier avec le client
- La publication de l'avancement du projet
- La gestion et la sauvegarde de l'espace de travail collaboratif

6. PARTENAIRES ET CONTRIBUTIONS EXTERNES

Des partenaires, jouant un rôle de consultants, ont contribué au projet en réalisant des **procédures détaillées basées sur les recommandations de l'ANSSI**.

- **Zakariya Fellah** : protection des mots de passe stockés
- **Matthieu Merlen** : chiffrement des données
- **Thomas Merlen** : gestion des comptes et des droits utilisateurs

Ces procédures sont archivées sur le cloud du projet et intégrées dans le plan de durcissement.

7. RESSOURCES UTILISÉES

- **Matérielles** : salle E09, postes Windows, réseau local limité, ordinateur personnel, disque dur externe.
- **Immatérielles** : Google Drive/Docs/Sheets, GanttProject, Lynis, Ubuntu, VirtualBox, Cisco Packet Tracer, Visual Studio Code, guides ANSSI.

8. TRAVAIL À RÉALISER – VUE D'ENSEMBLE

Le projet de durcissement s'articule autour d'un **ensemble de tâches structurées**, définies dans le cahier des charges fourni par le client.
Ces tâches couvrent l'intégralité du cycle de sécurisation d'un poste de travail, depuis l'analyse initiale jusqu'à la remise des livrables finaux.

L'approche retenue repose sur une logique progressive :

- Comprendre les recommandations de sécurité
- Créer un environnement de travail représentatif
- Auditer l'existant
- Appliquer des mesures de durcissement adaptées
- Vérifier l'efficacité des actions menées
- Documenter l'ensemble du projet

Cette structuration garantit une **méthode claire, reproductible et professionnelle**.

8.1 Planification du projet – Diagramme de Gantt

Afin d'assurer une organisation rigoureuse du projet et un suivi précis de l'avancement des travaux, un **diagramme de Gantt** a été réalisé à l'aide de l'outil **GanttProject**.

Ce diagramme présente :

- les différentes phases du projet ;
- les tâches et sous-tâches associées ;
- les dates de début et de fin ;
- la répartition du travail au sein de l'équipe.

Il permet de visualiser clairement la progression du projet et de vérifier le respect du planning établi.

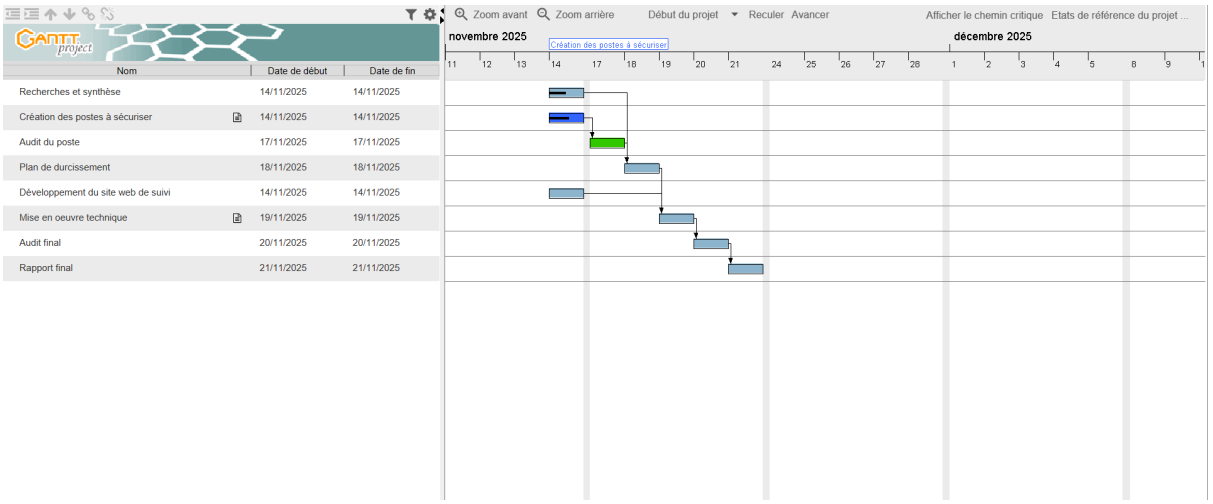


Figure 1 – Diagramme de Gantt du projet de durcissement (Source : GanttProject)

9. PLAN DE DURCISSEMENT

Le plan de durcissement est structuré en étapes claires, pour **assurer la sécurité du poste tout en permettant à un novice de suivre les actions**.

9.1 Méthodologie

1. Identifier les mesures ANSSI pertinentes.
2. Analyser leur pertinence via l'audit initial.
3. Éliminer les mesures peu utiles ou complexes.
4. Classer les mesures par priorité.
5. Justifier chaque mesure (risque couvert, impact potentiel).
6. Détail des étapes de mise en œuvre.
7. Intégration dans le site de suivi.

9.2 Axes de sécurité

9.2.1 Maîtrise du système

- Inventaire SI : postes, logiciels, utilisateurs
- Procédures et bonnes pratiques documentées
- Sensibilisation utilisateurs (charte, avertissement à la connexion)

9.2.2 Réduction de la surface d'attaque

- Pare-feu restrictif
- Logiciels sécurisés (KeePass, LibreWolf)
- Désactivation fonctionnalités inutiles

9.2.3 Gestion des identités et droits

Gestion des comptes utilisateurs

- Inventaire : `cat /etc/passwd`
- Désactivation : `sudo usermod -L <user>`
- Suppression : `sudo userdel -r <user>`
- Désactivation compte invité
- Comptes système : `/usr/sbin/nologin` ou `/bin/false`
- Expiration comptes inactifs >30 jours : `sudo useradd -D -f 30`

Groupes et privilèges

- Principe du moindre privilège
- Révision groupes sensibles : `cat /etc/group`
- Contrôle groupe sudo : `getent group sudo`
- Permissions sudo limitées et journalisées via visudo
- `Defaults logfile="/var/log/sudo.log"`
- `Defaults timestamp_timeout=0`

9.2.4 Politique des mots de passe

- Longueur min : 12 caractères
- Expiration : 90 jours
- Avertissement : 14 jours
- PAM (`/etc/security/pwquality.conf`) : minlen=12, dcredit=-1, ucredit=-1, lcredit=-1, ocredit=-1
- Verrouillage après 5 échecs : `auth required pam_tally2.so deny=5 unlock_time=900 even_deny_root`

9.2.5 Droits d'accès aux fichiers

- Audit SUID/SGID : `find / -perm /6000 -type f`
- Umask : 027 (`/etc/profile`)
- Permissions fichiers sensibles :
Fichier	Permission	Propriétaire
/etc/shadow	640	root:shadow
/etc/passwd	644	root:root
/boot	700	root:root

9.2.6 Journalisation

- Audit SELinux/AppArmor ou auditd
- Logs sudo obligatoires
- Rotation sécurisée avec logrotate

9.2.7 SSH

- PermitRootLogin no
- PasswordAuthentication no
- AllowUsers <admins>
- MaxAuthTries 3

9.2.8 Maintien du niveau de sécurité

- Automatisation mises à jour
- Audit régulier (apt-show-versions, debsums, rkhunter)

9.2.9 Cloisonnement réseau

- Connexions RDP sécurisées

9.3 Exemples détaillés de mesures

Mesure	Description	Risque couvert	Impact potentiel
libpam-tmpdir	Isoler les répertoires temporaires utilisateurs	Accès aux fichiers temporaires d'autres utilisateurs	Atteinte à confidentialité et intégrité
apt-listbugs	Avertissement des bugs critiques avant installation	Installation de paquets vulnérables	Compromission ou instabilité du système
apt-listchanges	Affiche changements importants lors des mises à jour	Modifications inattendues	Dysfonctionnement ou faille involontaire
needrestart	Indique services à redémarrer après mise à jour	Services utilisant des bibliothèques vulnérables	Failles non corrigées
fail2ban	Bloque les IP après tentatives répétées de connexion	Attaques par force brute	Compromission de comptes

9.4 Plan d'action priorisé

Les mesures sont classées par **importance** :

1. Renforcement des mots de passe
2. Configuration des droits et permissions
3. Sécurisation des connexions RDP
4. Mise en place du pare-feu restrictif
5. Avertissement et charte à la connexion
6. Gestionnaire de mots de passe sécurisé
7. Renouvellement et désactivation des comptes inactifs
8. Automatisation des mises à jour
9. Audit régulier des logiciels et intégrité

Ce classement permet une **mise en œuvre progressive et mesurable**, adaptée aux ressources disponibles et aux risques identifiés.

9.5 Protection des mots de passe stockés

La sécurité des mots de passe est un élément central du durcissement du poste. Les mesures suivantes s'appuient sur les recommandations de l'ANSSI et les bonnes pratiques PAM.

9.5.1 Sécurisation du stockage des mots de passe

Vérification des fichiers `/etc/passwd` et `/etc/shadow`

- Aucun hash ne doit apparaître dans `/etc/passwd` :

```
awk -F: '($2!="x") {print}' /etc/passwd
```

- Permissions recommandées :

Fichier	Permission	Propriétaire
/etc/shadow	-rw-------	root:shadow
/etc/passwd	-rw-r--r--	root:root

Utilisation d'algorithmes de hash robustes

- Argon2id (idéal)
- yescrypt (par défaut sur Debian 12 / Ubuntu 24+)
- SHA-512 si les deux précédents ne sont pas disponibles

Exemple de configuration PAM (`/etc/pam.d/common-password`) :

```
password required pam_unix.so sha512 shadow rounds=50000
```

9.5.2 Renforcement de la politique d'authentification (PAM)

Politique de complexité

```
password requisite pam_pwquality.so retry=3 minlen=12 ucredit=-1
lcredit=-1 dcredit=-1 ocredit=-1
```

Historique des mots de passe

```
password required pam_pwhistory.so remember=10 enforce_for_root
```

Protection contre le brute-force local

Dans `/etc/security/faillock.conf` :

```
deny=5
unlock_time=900
fail_interval=600
```

9.5.3 Gestion sécurisée des comptes utilisateurs

Désactivation des comptes sans mot de passe

- Détection :

```
awk -F: '($2=="") {print $1}' /etc/shadow
```

- Verrouillage :

```
passwd -l <utilisateur>
```

Expiration automatique des comptes inactifs :

```
useradd -D -f 30   # comptes inactifs depuis 30 jours
```

9.5.4 Protection des secrets utilisés par les services

Recherche des mots de passe stockés en clair

Emplacements sensibles : `/etc/**`, fichiers `.env`, scripts `.sh`

Commande :

```
grep -R "password\|pass\|pwd" /etc
```

Recommandations

- Utiliser des coffres à secrets : Hashicorp Vault, KeePass, `pass`…
- Appliquer des permissions strictes sur les fichiers sensibles

10. CRÉATION DU POSTE À SÉCURISER (MACHINE VIRTUELLE)

Le poste à sécuriser est créé sous forme de machine virtuelle, conformément aux contraintes imposées par le client.
Les actions réalisées sont :

- Installation d'un système d'exploitation Linux (Ubuntu)
- Création de comptes utilisateurs représentant les fonctionnaires de la mairie
- Installation des logiciels nécessaires à un usage bureautique et administratif

Cette étape permet d'obtenir un poste fonctionnel mais non durci, servant de base à l'audit initial.

10.1 Installation et préparation de l'outil d'audit Lynis

L'outil **Lynis** est utilisé pour auditer le système avant l'application des mesures de durcissement.

- **Installation** :

```
sudo apt-get install lynis -y
```

- **Vérification** :

```
sudo lynis
```

- **Premier audit** :

```
sudo lynis audit system
```

Les résultats de cet audit sont consignés dans un fichier log, qui servira de base pour identifier les faiblesses et prioriser les mesures de durcissement.

10.2 Gestion des utilisateurs

10.2.1 Liste des utilisateurs existants

Commande :

```
compgen -u
```

Cette commande permet de visualiser tous les comptes présents par défaut sur le système.

10.2.2 Création des nouveaux utilisateurs

Afin de respecter le cahier des charges, cinq comptes utilisateurs supplémentaires sont créés :

Nom Complet	**Identifiant**
Emiliya Hiditrut	ehiditrut
Waleed Signe	wsigne
Manola Heirani	mheirani
Zebadiah Carlitos	zcarlitos
Rosa Agni	ragni

Commande de création :

```
sudo adduser identifiant
```

Mot de passe temporaire : `88888888` (sera renforcé ensuite selon le plan de durcissement)

10.2.3 Vérification des utilisateurs créés

Commande :

```
compgen -u
```

Cette vérification confirme que les cinq comptes ont bien été créés et ajoutés aux groupes nécessaires.

11. AUDIT INITIAL DU POSTE DE TRAVAIL

Une fois le poste créé, un **audit de sécurité initial** est réalisé afin d'évaluer son état avant toute mesure de durcissement.

Cet audit comprend :

- Un inventaire matériel
- Un inventaire logiciel détaillé
- Une analyse des services et configurations actives
- La recherche de failles de sécurité à l'aide de l'outil open-source **Lynis**

Les résultats sont synthétisés dans un document permettant d'identifier clairement les **points faibles et axes d'amélioration**.

11.1 Cahier de tests

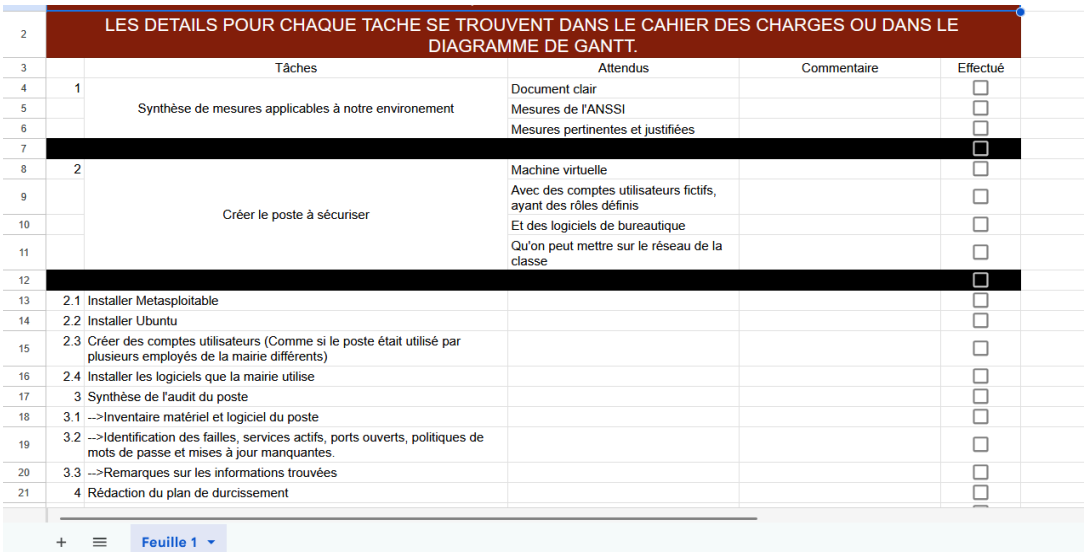
Un **cahier de tests** a été élaboré afin de vérifier l'état du système avant et après l'application des mesures de durcissement.

Il permet de :

- valider le bon fonctionnement du poste ;
- vérifier l'efficacité des mesures de sécurité mises en œuvre ;
- identifier d'éventuels dysfonctionnements ;
- assurer la conformité du poste aux exigences définies dans le cahier des charges.

Chaque test est décrit avec :

- un identifiant ;
- un objectif ;
- les prérequis ;
- les actions à effectuer ;
- le résultat attendu ;
- le résultat obtenu.



		Tâches	Attendus	Commentaire	Effectué
2	LES DETAILS POUR CHAQUE TACHE SE TROUVENT DANS LE CAHIER DES CHARGES OU DANS LE DIAGRAMME DE GANTT.				
4	1	Synthèse de mesures applicables à notre environement	Document clair		☐
5			Mesures de l'ANSSI		☐
6			Mesures pertinentes et justifiées		☐
7					☐
8	2	Créer le poste à sécuriser	Machine virtuelle		☐
9			Avec des comptes utilisateurs fictifs, ayant des rôles définis		☐
10			Et des logiciels de bureautique		☐
11			Qu'on peut mettre sur le réseau de la classe		☐
12					☐
13	2.1	Installer Metasploitable			☐
14	2.2	Installer Ubuntu			☐
15	2.3	Créer des comptes utilisateurs (Comme si le poste était utilisé par plusieurs employés de la mairie différents)			☐
16	2.4	Installer les logiciels que la mairie utilise			☐
17	3	Synthèse de l'audit du poste			☐
18	3.1	-->Inventaire matériel et logiciel du poste			☐
19	3.2	-->Identification des failles, services actifs, ports ouverts, politiques de mots de passe et mises à jour manquantes.			☐
20	3.3	-->Remarques sur les informations trouvées			☐
21	4	Rédaction du plan de durcissement			☐

Feuille 1

Figure 2 – Extrait du cahier de tests

12. RÉDACTION DU PLAN DE DURCISSEMENT

À partir de l'audit initial et des recommandations de l'ANSSI, un **plan de durcissement détaillé** est rédigé.

Il inclut :

- Une liste des mesures applicables
- L'élimination des mesures non pertinentes, avec justification
- Un classement des mesures par priorité
- Le détail précis des étapes de mise en œuvre
- Un document unique regroupant l'ensemble des mesures retenues

Ce plan constitue la **feuille de route technique** du projet.

13. CRÉATION DU SITE DE SUIVI DES MESURES

Un **site web local** est développé afin de suivre l'application des mesures de durcissement.

Il permet :

- D'afficher les mesures issues du plan de durcissement
- De suivre leur état d'application via des cases à cocher
- De visualiser le niveau de conformité du poste
- De générer un compte rendu au format HTML ou PDF

14. MISE EN ŒUVRE DES MESURES DE DURCISSEMENT

Les mesures définies dans le plan sont ensuite **appliquées sur le poste**.

Pour chaque mesure :

- Les étapes de mise en œuvre sont respectées
- Les configurations sont vérifiées
- Les résultats sont documentés
- Un compte rendu est rédigé

Cette phase représente le **cœur opérationnel du projet**.

15. AUDIT FINAL DU POSTE SÉCURISÉ

Après l'application de toutes les mesures, un **audit final** est réalisé.

Il comprend :

- La vérification de l'application des mesures
- Un nouvel inventaire matériel et logiciel
- Une nouvelle analyse avec Lynis
- Une comparaison avec l'audit initial

Cette comparaison permet de mesurer **objectivement l'amélioration du niveau de sécurité**.

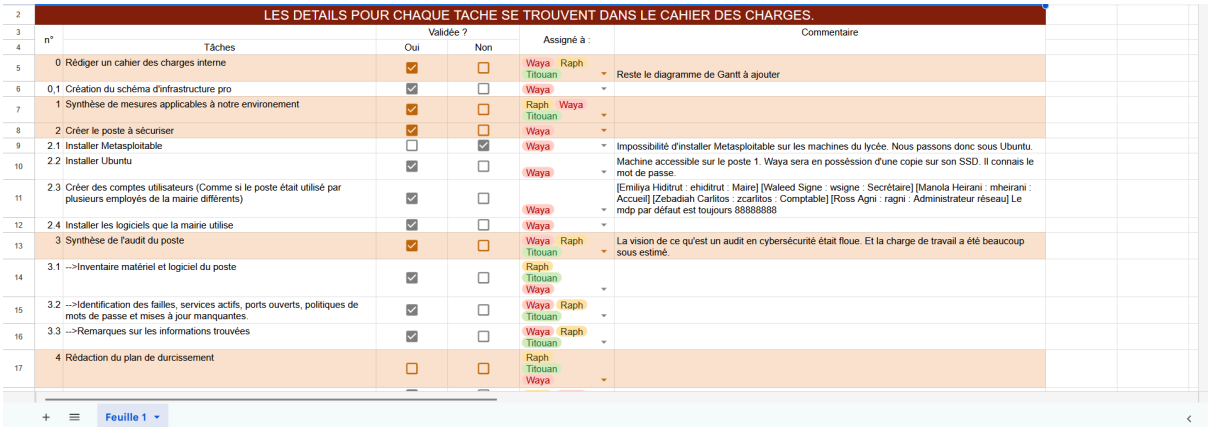
15.1 Cahier de recettes

À l'issue de la mise en œuvre des mesures de durcissement et de l'audit final, un **cahier de recettes** a été réalisé.

Ce document permet de :

- valider officiellement la conformité du poste sécurisé ;
- confirmer que les exigences du client ont été respectées ;
- attester du bon fonctionnement global du système durci.

Le cahier de recettes s'appuie sur les tests définis précédemment et formalise leur validation finale.



LES DETAILS POUR CHAQUE TACHE SE TROUVENT DANS LE CAHIER DES CHARGES.

n°	Tâches	Validée ? Oui	Validée ? Non	Assigné à :	Commentaire
0	Rédiger un cahier des charges interne	☑	☐	Waya Raph Titouan	Reste le diagramme de Gantt à ajouter
0,1	Création du schéma d'infrastructure pro	☑	☐	Waya	
1	Synthèse de mesures applicables à notre environement	☑	☐	Raph Waya Titouan	
2	Créer le poste à sécuriser	☑	☐	Waya	
2.1	Installer Metasploitable	☐	☑	Waya	Impossibilité d'installer Metasploitable sur les machines du lycée. Nous passons donc sous Ubuntu.
2.2	Installer Ubuntu	☑	☐	Waya	Machine accessible sur le poste 1. Waya sera en posséssion d'une copie sur son SSD. Il connais le mot de passe.
2.3	Créer des comptes utilisateurs (Comme si le poste était utilisé par plusieurs employés de la mairie différents)	☑	☐	Waya	[Emiliya Hiditrut : ehiditrut : Maire] [Waleed Signe : wsigne : Secrétaire] [Manola Heirani : mheirani : Accueil] [Zebadiah Carlitos : zcarlitos : Comptable] [Ross Agni : ragni : Administrateur réseau] Le mdp par défaut est toujours 88888888
2.4	Installer les logiciels que la mairie utilise	☑	☐	Waya	
3	Synthèse de l'audit du poste	☑	☐	Waya Raph Titouan	La vision de ce qu'est un audit en cybersécurité était floue. Et la charge de travail a été beaucoup sous estimé.
3.1	-->Inventaire matériel et logiciel du poste	☑	☐	Raph Titouan Waya	
3.2	-->Identification des failles, services actifs, ports ouverts, politiques de mots de passe et mises à jour manquantes.	☑	☐	Waya Raph Titouan	
3.3	-->Remarques sur les informations trouvées	☑	☐	Waya Raph Titouan	
4	Rédaction du plan de durcissement	☐	☐	Raph Titouan Waya	

Feuille 1

Figure 3 – Extrait du cahier de recettes

16. RÉDACTION DU RAPPORT FINAL

Un **rapport final complet** est rédigé afin de clôturer le projet.
Il présente :

- La méthode de travail adoptée
- Le détail de la réalisation avec captures d'écran
- Les résultats obtenus
- Les limites, remarques et conclusions
- L'ensemble des livrables fournis

17. CONTRAINTES IMPOSÉES PAR LE CLIENT

Le client impose les contraintes suivantes :

- Utilisation exclusive d'outils **open-source**
- Déploiement uniquement sur des **machines virtuelles**
- Respect strict des **guides de l'ANSSI**
- Documentation claire, complète et traçable

18. LIVRABLES FOURNIS

Les livrables du projet sont :

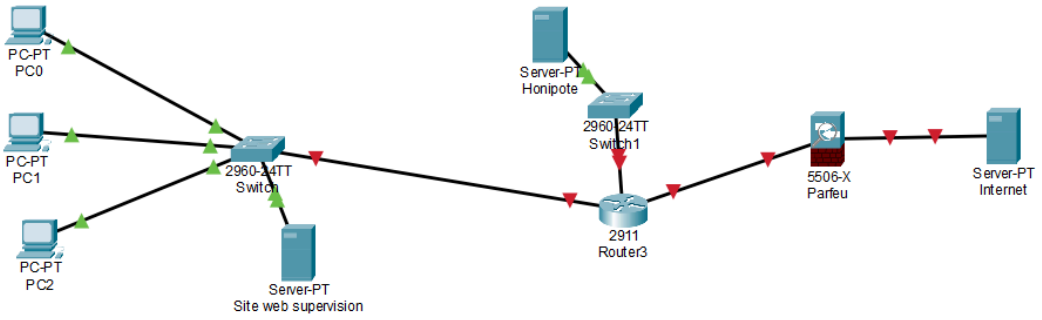
- Un cahier de tests
- Un cahier de recettes
- Un diagramme de Gantt détaillé (GanttProject, tâches et sous-tâches)
- Une synthèse de l'audit initial
- Un plan de durcissement
- Une synthèse de l'audit final
- Un site web local
- Un rapport final complet

19. SCHÉMA D'INFRASTRUCTURE

Un **schéma d'infrastructure** a été réalisé afin de représenter visuellement :

- La machine virtuelle
- Le poste à sécuriser
- L'environnement réseau de test
- Les outils utilisés

Ce schéma facilite la **compréhension globale de l'architecture du projet**.



Capture d'écran du Schéma d'infrastructure

Waya CHEMLA

Signature numérique de Waya CHEMLA
Date : 2026.01.09 10:16:16 +01'00'