**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS** **SESSION 2025**

**Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**

**ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)**

| **DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE** | **N° réalisation : 1** |
|---|---|
| **Nom, prénom : Belloum Nedjmeddine** | **N° candidat :** |
| **Épreuve ponctuelle** ☐ **Contrôle en cours de formation** ☒ | **Date :** 31 / 10 / 2025 |
| **Organisation support de la réalisation professionnelle** | |
| **Intitulé de la réalisation professionnelle : Serveur Mediaschool** | |
| **Période de réalisation :** 09/10/2025 au 31/10/2025 **Lieu :** Mediaschool – IRIS Nice ..... **Modalité :** ☐ **Seul(e)** ☒ **En équipe** | |
| **Compétences travaillées**<br>☒ Concevoir une solution d'infrastructure réseau<br>☒ Installer, tester et déployer une solution d'infrastructure réseau<br>☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau | |
| **Conditions de réalisation[1] (ressources fournies, résultats attendus)**<br><br>**Ressources :** Une machine virtuelle Linux (Debian). VirtualBox pour la virtualisation. Accès Internet pour installer paquets et outils de sécurité. Accès au réseau NAT pour la connexion SSH.<br><br>**Résultats attendus :** Un serveur Linux sécurisé, durci, et conforme aux bonnes pratiques. | |
| **Description des ressources documentaires, matérielles et logicielles utilisées[2]**<br><br>**Ressources documentaires** : Documentation officielle Debian/Ubuntu (security, SSH, PAM, rsyslog). Documentation Fail2Ban.<br>Assistance IA ponctuelle : ChatGPT / Copilot pour résoudre des erreurs ou optimiser des configurations.<br><br>**Matérielles et logicielles utilisées :** Visual Studio Code, Machine virtuelle Linux (Debian). VirtualBox (virtualisation). SSH + clés publiques. Fail2Ban pour la sécurité. L'outils Vagrant. | |
| **Modalités d'accès aux productions[3] et à leur documentation[4]**<br><br>Lien du repositories contenant le README et le projet : Documentation | |

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS** **SESSION 2025**

**Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**

**ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)**

**Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**

1. Configuration de la sécurité système
   - Mise à jour complète du système (apt update / upgrade).
   - Mise en place d'un pare-feu via UFW (ports autorisés, politiques par défaut).
   - Désactivation des services inutiles et vérification des services actifs (systemctl).
2. Sécurisation de SSH
   - Modification du port SSH pour réduire le risque de scans.
   - Désactivation de l'accès root en SSH.
   - Mise en place de l'authentification par clé publique (RSA/ED25519).
   - Activation du mécanisme de bannissement avec Fail2Ban.
3. Gestion des utilisateurs et authentification
   - Création et gestion d'utilisateurs locaux avec permissions limitées.
   - Ajout au groupe sudo selon la politique de sécurité.
   - Mise en place d'un mot de passe robuste (politiques PAM).
   - Vérification des droits via ACL selon les besoins des répertoires.
4. Mise en place et configuration des logs
   - Analyse et configuration de rsyslog pour centraliser et organiser les journaux.
   - Activation des logs d'authentification détaillés (/var/log/auth.log).
   - Mise en place d'audits via auditd :
     - suivi des connexions,
     - suivi des élévations de privilèges,
     - suivi des actions système sensibles.
5. Surveillance & détection d'intrusions
   - Installation et configuration de Fail2Ban :
     - seuils de tentatives,
   - Mise en place de scripts de monitoring (vérification régulière des logs).
   - Configuration des alertes mail en cas de tentative d'intrusion.
6. Tests & validation
   - Test de connexion SSH avec clé publique → succès.
   - Tentatives d'authentification incorrectes → détectées dans les logs + bannissement Fail2Ban.
   - Vérification du bon fonctionnement d'auditd (suivi des commandes sudo).
   - Vérification de la rotation des logs et de leur lisibilité.

**Compétences mobilisées :**

- **Administration et suivis.**
- **Automatisation des tâches systèmes.**
- **Documentation technique.**