**BTS SERVICES INFORMATIQUES AUX ORGANISATIONS**

**SESSION 2025**

**ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)**

**Épreuve E6 - Administration des systèmes et des réseaux (option SISR)**

|  |  |  |
| --- | --- | --- |
| **DESCRIPTION D’UNE RÉALISATION PROFESSIONNELLE** | | **N° réalisation :** |
| **Nom, prénom : MD ABDUL Fahim** | **N° candidat :** | |
| **Épreuve ponctuelle Contrôle en cours de formation** | **Date :**19 / 03 / 2025 | |
| **Organisation support de la réalisation professionnelle** | | |
| **Intitulé de la réalisation professionnelle** | | |
| **Période de réalisation :** .Mars 2025....... **Lieu :** Paris..................................................................  **Modalité : Seul(e) En équipe** | | |
| **Compétences travaillées**  Concevoir une solution d’infrastructure réseau  Installer, tester et déployer une solution d’infrastructure réseau Exploiter, dépanner et superviser une solution d’infrastructure réseau | | |
| **Conditions de réalisation1 (ressources fournies, résultats attendus)**  **résultats attendus**  -Installation et configuration de Fail2Ban  -Surveillance des logs et détection des tentatives d’attaques  -Mise en place de règles de bannissement automatique ----Vérification des blocages et tests d’efficacité  **ressources fournies**  -Un serveur Debian 10.18 installé    -Accès root ou utilisateur  -Fichiers de logs (auth.log, apache logs, syslog) | | |
| **Description des ressources documentaires, matérielles et logicielles utilisées2**  Logiciels  - Vmware  Matériel  - Un serveur Debian (physique ou virtuel)  - Poste client pour tester l’accès SSH et web | | |
| **Modalités d’accès aux productions3 et à leur documentation4** | | |

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**

**ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)**

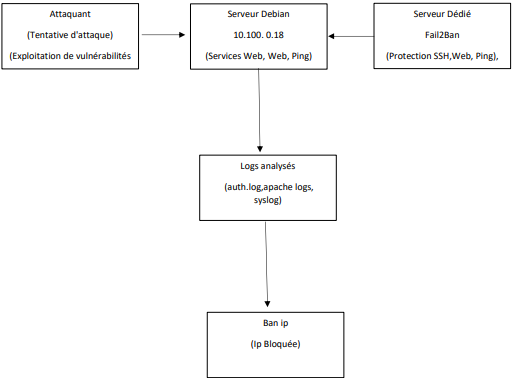
**Épreuve E6 - Administration des systèmes et des réseaux (option SISR)**

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

Un serveur connecté à Internet peut être attaqué par des pirates informatiques. Ils essaient souvent d’accéder au serveur en testant plusieurs mots de passe (attaques sur **SSH**), en exploitant des failles sur un site web (**Apache/Nginx**) ou en effectuant des tests (**ICMP/Ping**)**.**

L’objectif de cette réalisation est d’installer et configurer **Fail2Ban** sur un serveur **Debian 10.18**. **Fail2Ban** surveille les tentatives de connexion et bloque automatiquement les adresses IP suspectes après plusieurs échecs.

1.**Un pirate** tente d’attaquer le serveur en testant plusieurs mots de passe ou en exploitant des failles web.  
2.l**e serveur** enregistre ces tentatives dans des fichiers de logs.  
3️. F**ail2Ban analyse ces logs** et détecte les tentatives répétées.  
4️.L**’adresse IP de l’attaquant est bloquée** automatiquement, empêchant toute nouvelle connexion.



Grâce à cette configuration, le serveur est mieux protégé contre les attaques courantes.

**Fail2Ban** empêche les intrusions en bloquant les attaquants avant qu’ils ne puissent causer des dégâts.