Epreuve E4 conception et maintenance de solutions informatiques

BTS Services informatiques aux organisations **Session 2020**
E4 – Conception et maintenance de solutions informatiques **Coefficient 4**
DESCRIPTION D'UNE SITUATION PROFESSIONNELLE
Épreuve ponctuelle **Contrôle en cours de formation**
PARCOURS SISR **PARCOURS SLAM**
NOM et prénom du candidat : JUNDT Philippe **N° candidat :**
Contexte de la situation professionnelle Une entreprise spécialisée dans la gestion de données bancaires souhaite sécuriser les équipements informatiques de son siège social. Elle dispose déjà d'équipements d'identification des utilisateurs et de supervision du parc informatique. Pour assurer un niveau efficace de sécurisation de ses infrastructure l'entreprise souhaite également sécuriser les installations physiques, pour se prémunir contre les intrusions et la captation d'information.
Intitulé de la situation professionnelle Mise en place de Secure Shell (SSH) pour la sécurisation locale et distante des accès aux équipements réseaux.
Période de réalisation : 2ème semestre 2020 Lieu : Strasbourg **Modalité :** Individuelle
Conditions de réalisation (ressources fournies, résultats attendus) Assurer l'accessibilité aux équipement réseaux pour les administrateurs et pour un parc informatique hétérogène. Mise en place de SSH pour faciliter le télétravail des administrateurs systèmes et réseaux. Cahier des charges : Proposer des procédures d'installation sur les équipements en local Permettre un accès distant à un équipement réseau Proposer des solutions pour sécuriser les équipements face à des tentative d'intrusion.
Productions associées Documentation technique fournie par le constructeur des protocoles utilisés et des instructions de configuration des équipements.
Modalités d'accès aux productions Présentation sur le portfolio https://pjundt.fr/E4.html Fiche et Documentation

Description de la situation

Contexte :

Une entreprise spécialisée dans la gestion de transactions bancaires souhaite sécuriser ses infrastructures. L'entreprise a récemment étendu son réseau et a ajouté des équipements pour assurer des redondances de ses équipements. Elle souhaite conserver un haut niveau de sécurité pour ses équipements et s'informe sur les solutions d'authentification et les solutions de chiffrement.

L'entreprise a mis en place des moyens de défense actifs et passifs pour identifier les hackers ou les auteurs d'activités illicites. Elle assure un contrôle des identités sur son réseau interne avec un annuaires des utilisateurs, un ADDS pour les services Microsoft, un Honeypot.

Besoin :

Les différents moyens de défense actifs et passifs de l'entreprise sont efficaces. Elles ont déjà pu détecter des individus qui souhaiter s'introduire sur les réseaux. De récentes tentatives ont mis en lumière que les attaquent ne visent les données et s'orientent vers les équipements réseaux, dans le but de paralyser certains de ses services par DDoS.

Solutions informatiques :

Un moyen pour sécuriser des équipements ou des applications est de réaliser des procédures d'authentification. La majorité des équipements fonctionnent sous des OS qui intègrent certains types de services qui ne sont pas installés de base :

- Ajouter un mot de passe
- Mettre en place un certificat SSH sur le router pour un accès distant
- Etudier la faisabilité d'intégrer ACL pour authentifier les admins ou des user

Cela permet de réduire les risques de captation de données sensibles sur les équipements lorsque les administrateurs interviennent à distance pour un dépannage ou une modification du réseau.

Le fait de chiffrer les données a un coût en terme de sollicitation des ressources CPU ou RAM des équipements, mais il semble être acceptable au regard des besoins de l'entreprise à sécuriser ses équipements.