BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

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

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 02**
Nom, prénom : BAZIN Maxime	**N° candidat : 01948338680**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :**

Contexte de la réalisation professionnelle

Amélioration de l'infrastructure du client « Belletable » pour apporter plus de fonctionnalités et de sécurité dans une infrastructure déjà fonctionnelle mais non optimisée.

Intitulé de la réalisation professionnelle

Afin de surveiller et sécurisé l'infrastructure de Belletable nous avons installé et déployer un HIDS tel que Wazuh pour une gestion efficace des informations de sécurité et gestion des événements de sécurité pour fournir des alertes en temps réel. De plus nous ajoutons un proxy sur PfSense pour filtrer les accès vers internet des utilisateurs.

Période de réalisation : Lieu :

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 réalisation [1] (ressources fournies, résultats attendus)

- Présentation du client (Belletable) et du prestataire (InfoServices) et un extrait d'audit.
- Une plateforme de laboratoire avec ferme de serveurs, baie de brassage, matériels d'interconnexion
- Délais : environ 3 mois (découpés en plusieurs séances à raison d'une par semaine environ)

Ressources fournies :

La réalisation professionnelle est réalisée avec le matériel du CFA Cerfal Campus Montsouris et avec des logiciels open source en respectant le cahier de charge de Infoservices.

Logiciels :

- Mise en place d'une solution de détection d'intrusions qui est Wazuh dans l'infrastructure réseau de Belletable en privilégiant les réseaux locaux
- Mise en place d'un proxy PfSense pour filtrer les accès des utilisateurs vers internet

Résultats attendus :

- Serveur Wazuh fonctionnel capable de remonter des informations en cas d'attaque et des diagnostiques/scan du trafic réseau
- Serveur proxy PFsense capable de filtrer les accès des utilisateurs sur internet

Description des ressources documentaires, matérielles et logicielles utilisées [2]

- Présentation du client (Belletable) et du prestataire (InfoServices) et un extrait d'audit.
- Une plateforme de laboratoire avec ferme de serveurs, baie de brassage, matériels d'interconnexion
- Documentation Wazuh : https://documentation.wazuh.com/current/deployment-options/elastic-stack/all-in-one-deployment/index.html
- Documentation Squid : http://www.squid-cache.org/

Modalités d'accès aux productions [3] et à leur documentation [4]
Portfolio : portfolio-dsm-f.fr Drive google : Fiche Wazuh / Règle Brute Force / PfSense Squid / Filtrage Proxy
https://urlz.fr/lpvb / https://urlz.fr/lpvd / https://urlz.fr/lpvf / https://urlz.fr/lpvg

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023**

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

Épreuve E5 - Administration des systèmes et des réseaux (option SISR) - Coefficient 4

Descriptif de la réalisation professionnelle, y compris les productions réalisées (établir une liste / tableau) et schémas explicatifs

Mission Wazuh HIDS – PfSense Proxy

Le proxy sera mis entre le WAN et le LAN. SRV-Wazuh dans le VLAN 1.

Infoservices à juger judicieux d'installer un serveur HIDS pour surveiller le réseau de belletable et ses machines. Les machines à surveiller sont : SRV-DC, SRV-Fichiers, SRV-WEB
Serveur Wazuh installé dans le réseau Belletable dans le VLAN1 sur une machine virtuelle installer sur VMware ESXi sous les conseils de Infoservices.

Wazuh est installé avec la suite **Elastick Stack** (solution open-source de monitoring et de gestion des logs) en All-in-one déploiement sur Debian 11.6

Mission : Installation d'un HIDS Wazuh avec la suite Elastic Stack

Une fois tout installer et configurer on peut se connecter à l'interface web de notre serveur.

Une fois dans l'interface web on peut commencer à déployer les agents sur les instances à surveiller.

De plus on peut ajouter des règles pour rendre Wazuh plus efficace en cas d'attaque.

Afin d'être alerter même si on n'est pas sur l'interface web on configure une alerte par mail.

A cela nous ajoutons un proxy sur PfSense pour filtrer les accès des utilisateurs vers internet.

Pour infoservices le proxy offre de nombreuses possibilités en matière de sécurisation, d'économie de données, restrictions et de navigation anonyme sur le web.

Pour ce faire il va falloir installer et configurer Squid sur PfSense.

Installation de Squid Guard pour effectuer du filtrage web basé sur des catégories via une blacklist
Règles : Blocage des sites illégaux, téléchargements, sites de streaming et de vidéo à la demande.

Et enfin on va ajouter un filtrage du trafic HTTPS pour une meilleure sécurité surtout contre les attaques "Man in the middle".

Productions réalisées :

Procédure :

- Installation et configuration de Wazuh
- Déploiement des agents
- Ajout règle anti brute force
- Installation et configuration de Squid et Squid Guard
- Ajout de filtrage par catégories