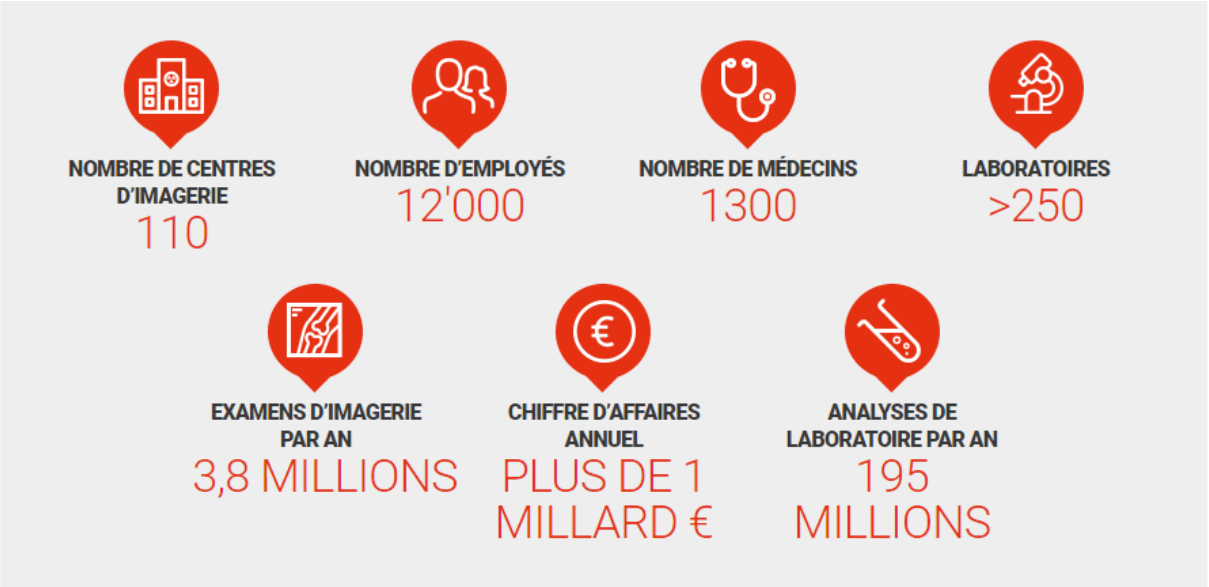
Présentation du projet réseau

MICKAËL HONVAULT

L’entreprise EPSIMedilab en quelques mots

- Leader européen sur les prélèvements médicaux pour les particulier.

- L’entreprise réalise des diagnostics variés (imagerie médicale, médecine reproductive et génétique, services de développement de médicaments …)



Problématique de l’entreprise

L’entreprise souhaite revoir l’architecture de son système d’information.

- Améliorer l’évolutivité de son système d’authentification. (forêt désorganisée tous dans une seule OU).
- Implémenter des éléments de sécurité et améliorer la disponibilité de son site web afin de permettre plus de connexion.
- Sécuriser l’accès au réseau de l’entreprise.
- Obtenir davantage de visibilité sur la disponibilité et les systèmes de sauvegarde de son système d’information.

Architecture Web

L’entreprise rencontre des difficultés :

- Des attaques sur son site web actuellement hébergé en DMZ (en mode lamp), sans chiffrement ni éléments de sécurité).
  - Attaques sur le service de base de données (brute de force sur l’authentification), les assaillants ont réussi à accéder aux données directement depuis le serveur.
  - Attaque sur le service web (déni de service HTTP, capture du trafic, HTTP, vol de cookie …), modification des pages web.
  - Attaque sur le service SSH (brute force distribués sur l’authentification)

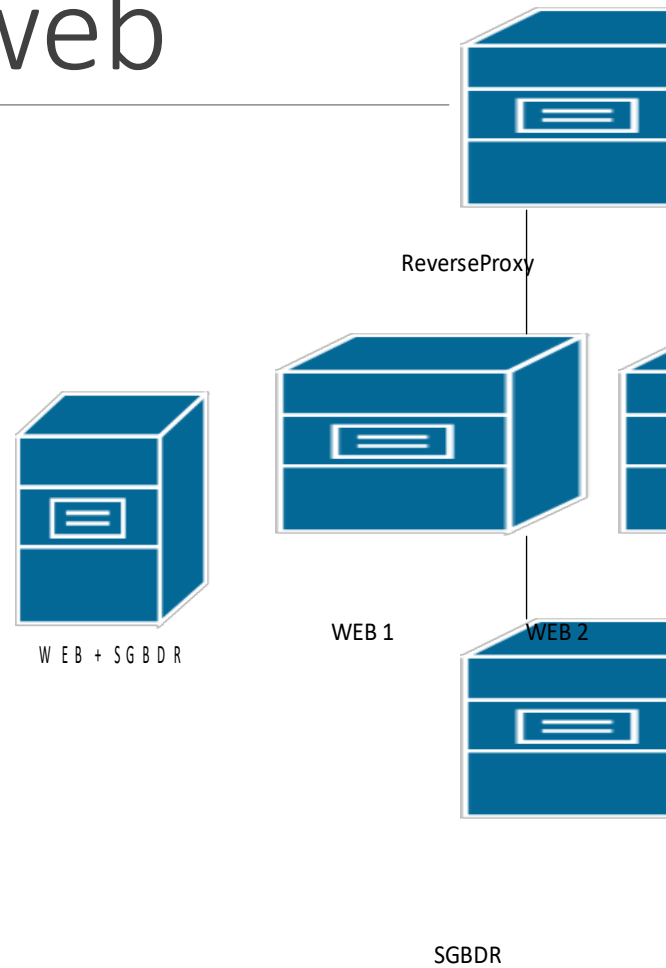
Evolution à réaliser sur la partie web

1) Répartir l'architecture web en 3 tiers (ReverseProxy, Web et SGBDR)

2) BDD : Mettre en place les sécurités de connexion (*ex : **mysql_secure**, filtre les connexions (**firewall + listen/bind**), système de **blocage des brutes forces** sur le service ssh et mariadb, …)*

3) Web : Remplacer le service apache2, et sécuriser le service (*mettre en place un **certificat** (auto sign ou github educ), mettre en place un système de blocage des **brutes forces ssh/authentification**, des tentatives de **fuzzing**, alerter les **modifications de fichier** de configuration ou du code de l'application …).*

4) ReverseProxy : Répartir la charge sur plusieurs serveurs web



Système d'authentification

L'entreprise rencontre des difficultés :

- L'ensemble des utilisateurs de l'organisation sont dans une seule unité d'organisation OU il est ainsi difficile de définir des politiques de sécurité.
- La création des comptes utilisateurs est considérée comme une tâche ingrate par les équipements système.

Les évolutions :

- Prévoir **différentes unités d'organisation** et mettre en place des groupes de sécurité selon une arborescence hiérarchique.
- **Automatiser la création des utilisateurs** ainsi que leur **affectation dans les groupes** à l'aide d'un script. Le script exploitera notamment la **notion d'objet**, de **fonction** et réalisera les critères de **contrôles** (présence de l'utilisateur, du groupe …) à l'aide de condition et de try catch. *Éventuellement l'intégration de logs dans le* ***gestionnaire d'événement Windows*** *serait un plus.*

Exemple de fichier d'imports et de matrice de partage de fichier

	Service (OU)	Prenom	Nom	DateIn	Tel	DateOut
1	Laboratoire	Zenaida	Tucker	03/12/2023	03 09 02 60 20	03/07/2025
2	Comptabilité	Camille	Cameron	13/12/2023	06 17 07 66 84	03/07/2025
3	Informatique	Chaney	Molina	26/01/2024	06 78 60 70 46	03/07/2025
4	Juridique	Hamish	Singleton	23/02/2024	04 80 52 33 14	01/06/2025
5	RH	Camden	Norman	08/01/2024	06 61 92 74 53	02/02/2025
6	Direction	Deanna	Ratliff	25/02/2024	06 04 21 68 06	02/02/2025
7	R&D	Zorita	Morgan	25/03/2024	02 08 61 80 83	01/06/2025
8	R&D	Yardley	Gill	14/01/2024	04 37 90 07 82	01/06/2025
9	Informatique	Elijah	Joyce	16/02/2024	04 26 50 66 80	01/06/2025
10	Informatique	Shannon	Sharp	20/04/2024	02 26 04 85 33	02/02/2025

Identifiant de type pnom, exemple : ztucker et adresse mail ztucker@epsimedilab.fr

Service	CE	Laboratoire	Comptabilité	Informatique	Juridique	RH	Direction	R&D
Laboratoire	r	rw						
Comptabilité	r		rw					
Informatique	r			rw				
Juridique	r				rw			
RH	rw					rw		
Direction	rw	r	r	r	r	r	rw	r
R&D	r	r						rw

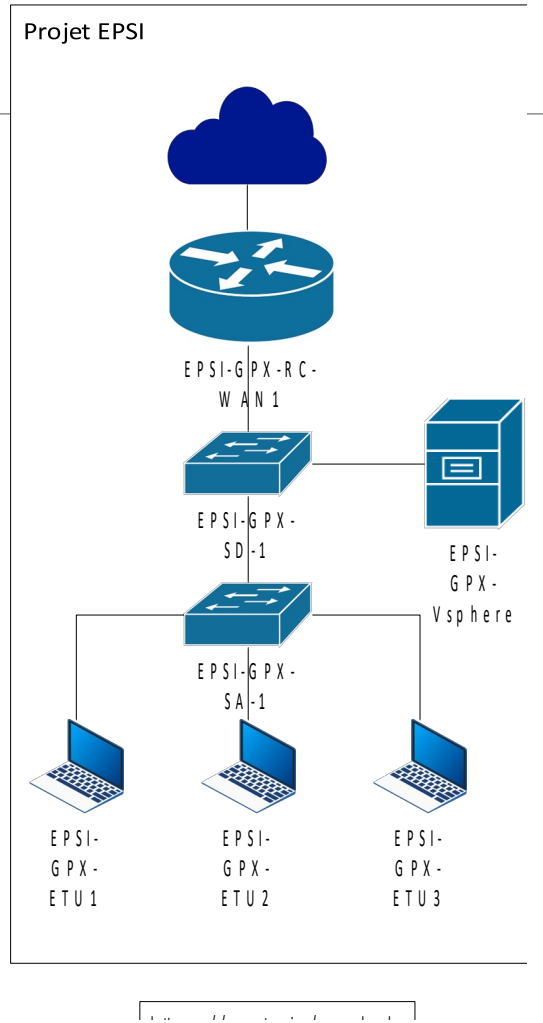
Architecture réseau

L’entreprise possède l’architecture réseau suivante.

Il est arrivé que des personnes malveillantes débrancher les ordinateurs pour y brancher un système KaliLinux et réaliser des attaques *(arp spoofing, dhcp spoofing/snooping, rogue dhcp, dtp negociation, vtp destruction, cdp, …).*

Evolution :

Reproduisez l’architecture avec les différents vlan et ajouter des éléments de sécurité pour bloquer les connexions d’équipements sauvages.



Architecture réseau

Liste des vlan : *(Adressage réseau IPv4 et IPv6 libre)*

Informatique

Compta

RH

Serveurs

Laboratoire

Supervision

Actuellement l'organisation n'a aucune visibilité sur l'état de son système d'information.

Evolution :

Implémenter une solution de supervision afin de monitorer l'hardware des équipements (cpu, ram, hdd, network) et des services applicatifs tels que (check_ldap, check_http, check_bdd) et réaliser des tests de performance ou de parcours clients sur le site web.

Un alerting basé sur des solutions telles que discord/teams ou encore la création automatique de tickets GLPI serait un plus.

Rendu

L’évaluation se basera sur un document rendu exposant les mises en > réaliser et les tests réalisés.

Le document évoquera notamment des captures d’écrans des installations *(avec l’heure sur la machine sur lequel vous êtes afin d’éviter le vol de capture d’écran sauvage)*

Le document présentera également les commandes écrites pour la configuration des services Linux, le script powershell ainsi que les configurations des équipements réseau.