LEFEVRE Alexandre
GILLES Timothy
TONGRES Cyril

Groupe 2TL2-7

Rapport sécurité Mission 3

Risques encourus par le VPS

risque de perte du vps

- usurpation d'identité du serveur.
- attaque sur le mdp du client.

Les mesures mises en place contre les risques :

Fail2Ban : logiciel qui permet de bloquer les adresses IP qui tenteraient d'accéder à notre VPS sans succès.
Nous l'avons configuré de sorte qu'il bannisse les adresses IP qui tentent de se connecter plusieurs fois sur nos vps sans succès.

Sur les vps : nous avons désactivé les identifications par compte root ainsi que l'authentification par mot de passe. La connexion se fera dès lors par clé asymétrique que nous aurons généré.

fichier a modifier : /etc/ssh/sshd_config

Mise en place de ssh :

- création de l'utilisateur.
- générer la clé chiffrées pour l'accès à votre compte.
- déplacer la clé publique sur le serveur distant.
- modifier les permissions.

Risques encourus par les services mis en place

serveur DNS :

1) *Interception des paquets : message unique non authentifié*

Attaque de type Man in the Middle.
Réponse falsifiée (fishing : envois d'une réponse contenant l'ip du site falsifiée).

2) *Corruption des données du serveur*

Cache poisoning.
Mise en avant d'un service commercial.
Blocage de certains sites web (Pirate Bay).

3) *Déni de service : surcharge du serveur l'empêchant de répondre aux requêtes.*

Site web intranet : afin que les employés uniquement puissent accéder à ce site, nous allons réaliser des access-list tel que vu dans le cours d'infrastructure réseau.

LEFEVRE Alexandre
GILLES Timothy
TONGRES Cyril

serveur MAIL :

1) *Confidentialité (POP,IMAP et SMTP en clair)*
2) *Intégrité (usurpation d'identité à l'envoi ou durant le transit)*
3) *Spam*

impact au niveau de la bande passante, de la mémoire des serveurs et mailboxes et de la productivité.

4) *Phishing*

serveur VOIP :

1) Sécurité des données.
2) Usurpation d'identité (spoofing).
3) Ecoute (eavesdropping) (données et signalisation).
4) Injection de paquet (DTMF).
5) Abus d'utilisation (theft of service).
6) DoS (signaling).
7) Spam.

Contre mesure

serveur dns :

1) *DNSSec : Signature cryptographique des enregistrements DNS.*
2) *Différentier DNS interne et externe (architecture dns sécurisée).*
3) *Création d'accès-list pour que les ip des employés puissent accéder au site intranet.*

serveur mail :

1) *Filtre anti-spam*

Basé sur le format et sur le contenu du message

2) *S/MIME : fourni la possibilité de signer et ou de chiffrer des messages emails.*
3) *PGP : logiciel de cryptographie permettant de garantir la confidentialité et l'authentification des données.*
4) *Utilisation de Proxies mail pour isoler les serveurs mail d'internet en DMZ.*

serveur voip :

1) Sécurisation : encryption.
2) A chaque saut : IPSECVPN, SIP over TLS (délai).

3) S/MIME for signalling.
4) SRTP pour les données media (échange de clé dans SDP).
5) Authentification client serveur (clé).

Contre mesure mise en place

1) Mise en place du protocole HTTPS pour la sécurisation de notre serveur web, nous avons configuré le certificat SSL. Les sites B2B et www sont sécurisés en https. Nous n'avons pas sécurisé l'intranet en https étant donné qu'il ne sera accessible uniquement en local par les employés