LEFEVRE Alexandre
GILLES Timothy
TONGRES Cyril
Groupe 2TL2-7

Rapport sécurité Final

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 chiffrée 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 : envoie d'une réponse contenant l'ip falsifiée du site).

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).
   L'identité est volée en se faisant passer pour l'adresse IP de quelqu'un d'autre.
3) Ecoute (eavesdropping) (données et signalisation).
   Surveillance non autorisée de la ligne.
4) Injection de paquet (DTMF).
5) Abus d'utilisation (theft of service).
6) DoS (signaling).
   Empêchement de l'utilité du service VOIP.
7) Spam.
   Appel téléphonique non sollicité et composé automatiquement.

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.

LEFEVRE Alexandre
GILLES Timothy
TONGRES Cyril

serveur voip :

1) Sécurisation : encryption.
2) A chaque saut : IPSECVPN, SIP over TLS (délai).
3) S/MIME pour la signalisation.
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.

2) Mise en place du protocole DNSSEC pour la sécurisation de notre DNS. Nous permettant ainsi de pouvoir gérer la protection des données et des enregistrements DNS.

3) Pour la sécurisation du Mail, nous avons mis en place SPF et DKIM.
   SPF : Cela permet de limiter l'usurpation d'identité en publiant dans les DNS votre nom de domaine la liste des serveurs ou des adresses IP, qui peuvent envoyer du courrier avec ce domaine.
   DKIM : nous permet de vérifier que le message transmis n'a pas a été modifié durant le transport de celui-ci et aussi de vérifier que le nom de domaine n'ait pas été usurpé.

   Nous avons également mis en place des certificats STARTLS, SSL/TLS. Cela nous a permis et nous a surtout été d'une grand utilité dans la sécurisation, la fiabilisation de nos échanges, vérification de l'identité du serveur. STARTLS est un protocole nous ayant permis d'améliorer une connexion classique pour une connexion sécurisée grâce à TLS.

4) Pour VOIP n'avons pas mis en place d'autres choses de plus que dans les autres secteur étant donné que les différents outils utilisés précédemment rentraient en compte pour la sécurité VOIP notamment fail2ban.