Network security

Control & audit

Antoine Puissant

Enseignant : M. Rey

2014 - 2015

Résumé

Ceci est le résumé

Table des matières

1 titre

La norme 802.1X (c.f. [**8021X**]) permet de ne pas accéder au réseau si l'utilisateur ne s'est pas authentifié (même câblé).
Le contrôle et le pentest font partie de l'audit.

Pentest Pour un pentest, on se place en mode boite noire : on a la place de l'attaquant, on ne connaît pas l'architecture interne d'un réseau. De manière générale, un pentest est assez ciblé. Il n'y a souvent que peu de machines cibles.

Audit L'audit se place à l'intérieur d'un réseau, on prend la position du défenseur. C'est un étude qui est très grande. On va, par exemple, évaluer le réseau entier de l'entreprise. On va pouvoir faire du pentest sur quelques machines (les machines critiques) au sein du réseau.
Le référentiel de l'audit est l'état de l'art.
Ainsi, le résultat d'un audit est composé de préconisation.

Contrôle Pour un contrôle, on se positionne dans une entreprise mûre en sécurité. Le RSSI a alors une politique de sécurité. Ainsi, pour un contrôle, on va vérifier que la politique de sécurité est bien appliquée.
Le résultat est composé d'ordres à faire appliquer aux salariés et de conseils d'améliorations de la politique de sécurité du RSSI.

Les normes ISO27000X ($0 < X < 40$) (c.f. [**ISO27**]) vont permettre de réaliser une politique de sécurité en fonction de normes prédéfinies.
Pour les entreprises de la finance (banques, bourses, etc...), il existe une norme obligatoire en Europe : PCI-DSS.
Les OIV [1] doit se faire auditer la maîtrise de la continuité : des exercices sont fait tous les ans afin de vérifier comment l'entreprise réagit en cas d'interruption, ce qu'elle fait pour redémarrer sa production.
Lors d'un audit, tout le technique est pris en compte. Cela comprend son environnement physique, technique tout en se basant sur la référence.

1.1 L'audit

Il se compose de trois phases.

1.1.1 La prise de contact, phase préparatoire

Le client fait une demande d'audit. Pour cela, on passe par les commerciaux afin de réaliser les négociations.
On réalise une visite préparatoire. On va alors chez le commanditaire. Le commanditaire n'est pas obligatoirement le client, cela peut-être une entité supérieure (ANSSI pour les OIV).
On va ensuite chez le client pour se présenter. On va alors convier à cette journée de réunion le RSSI, les administrateurs réseau (ou l'entreprise qui gère l'infogérance). Cette réunion préparatoire va permettre de définir le périmètre mutuel d'audit.
On va ensuite signer la charte de confidentialité des données de l'entreprise (NDA). On va alors assurer de la manière dont les données seront sauvegardées,

1. Organisme d'Importance Vitale

effacées, détruites, etc...
On signe ensuite une charte d'audit, un protocole et un contrat.

Une fois cette réunion finie, il peut passer un peu de temps. Durant cette période on va planifier les interviews que l'on va réaliser avec le personnel de client.

1.1.2 L'audit

On va alors faire de l'investigation organisationnelle, vérifier comment l'organisation de l'entreprise est faite. On investigue aussi l'informationnelle. Cela permet de connaître l'e-réputation de l'entreprise. On va trouver cela en sources ouvertes.
On va pouvoir, dans le cas où il y a plusieurs auditeurs, faire des comptes-rendus chaque soirs pour se tenir au courant.
En fin d'audit, il est courant de faire un compte-rendu à chaud.
On peut aussi faire une séance de sensibilisation du personnel.

1.1.3 Le compte-rendu, le livrable

Il faut prendre le temps pour pouvoir ordonner toutes les données récupérer, tout analyser. Il faut se laisser le temps de l'analyse afin de pouvoir analyser correctement et réaliser les bonnes recommandations.

2 Rendez-vous de présentation

I Présentation des auditeurs, de qui on est.

II Méthodologie. C'est ce qu'on compte faire, comment.

III Commanditaire et ses valeurs. On défini avec eux ce qu'il faut sécuriser, ce qui est primordial.

IV Périmètre de l'audit. Ça peut-être les machines de l'entreprise, les accès sur des serveurs externes.

V Modalités.

3 Retour d'expérience – RETEX

- Pas d'analyse de risque
- Pas de cloisonnement des données
- Pas de notion de secret, beaucoup de gens donnent trop d'informationnelle
- Pas de marquage sur les documents (niveau de confidentialité)
- Pas d'étude des pannes, de snapshots, de backup, etc...
- Pas d'organisation du travail
- Pas de délimitation de l'inclusion des tiers (SSII)
- Personnel non sensibilisé
- Problème d'employé malveillant
- Il faut interdire de pouvoir s'authentifier à deux endroits différents en simultané

4 Droits de devoirs des administrateurs

Il est interdit de lire les messages comprenant la notion de « personnel » ou avec des noms et prénoms.
Il est possible d'accéder aux fichiers professionnels. L'accès fortuit aux données personnelles (scan de dossiers, etc...), cela n'est pas puni si l'accès au documents n'est pas fait.Il ne faut surtout pas faire fuiter l'information personnelle sur laquelle on est tombé.
Dans le cas d'un audit, il est autoriser d'investiguer et de tomber sur des documents personnels. On est mandaté pour cela. Il faut rester discret. La discrétion est le maître mot en cas de découverte de documents particuliers.
En cas de problème détecté, un administrateur peut accéder aux documents professionnels et personnel pour analyse. Il n'a cependant pas le droit de modifier les contenus. Si le problème est lié à la sécurité, on peut supprimer la donnée virolée dans le cadre de la politique de sécurité.
Si aucun problème n'est rencontré, aucune investigation n'est autorisée.
En cas d'intervention sur un poste, on essaye d'être avec la personne. On n'ouvre pas les données personnelles et on peut détruire les données personnelles avec son accord.

5 Scan de vulnérabilités

Commencer par lire le document sur les généralités des vulnérabilités (donne la culture des vulnérabilités).
Ensuite, lire le document *exploitation*. Cela s'appuie sur un seul scanner de vulnérabilités et montre son fonctionnement.

5.1 Question TP

Mode *credential* : on rentre dans la machine directement pour faire l'audit. Pour les machines *linux-like*, on utilise SSH. On crée aussi un compte pour OpenVAS afin de lui permettre de rentrer avec certains droits. On le configure en *credential* afin qu'il puisse avoir accès aux vulnérabilités applicatives.
Pour Windows, on va utiliser smb/spc pour faire du contrôle à distance. Dans OpenVAS on va trouver un module MSRPC.
L'objectif de ce LAB est de scanner deux machines virtuelles : une sous Linux et une sous Windows. Il faut prouver que l'on soit rentré en mode *credentials*.
Prendre la machine, à neuf, scan. On met à jour, on re-scan.
On peut aussi comparer avec une titan.