Audit d'un système d'information

Table des matières

1. Définition

L'**audit de sécurité** d'un système d'information (SI) est une vue à un instant *T* de tout ou partie du SI, permettant de comparer l'état du SI à un référentiel.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes.

2. Introduction

Ce document n'a pas la prétention de présenter toutes les attaques possibles, mais juste faire une présentation de certaines d'entres elle qui constitue de points d'entrée fréquents des attaques.

Un système d'information doit être protégé. Cependant toutes les entreprises n'ont pas besoin du même niveau de sécurité. Le contrat doit donc mentionner les secteurs à tester. Il se peut, par exemple, que l'entreprise ne soit pas intéressée par un audit utilisant le Social engineering.

De même, certaines phases comme la collecte d'informations dépendent directement du type d'audit réalisé.

Nous allons voir, dans les prochaines étapes de cette documentation, un certain nombre de techniques d'intrusion. La liste n'est pas exhaustive bien entendu, les possibilités n'ayant de limite que l'imagination, ou presque.

Nous ne parlerons pas ici de furtivité ou de suppressions de nos traces sur le réseau.

3. Procédure

La première étape consiste à prendre connaissance de manière extrêmement fine les attentes du client. Il convient de bien comprendre ses besoins et de les reformuler.

Cette première étape est particulièrement importante dans la mesure où elle plante le contexte précis dans lequel l´audit va être mené : autant d´informations qui seront incluses dans le rapport d´audit afin d´en faciliter l´interprétation, même plusieurs années après sa réalisation.

Ensuite, une lettre de mission sera rédigée. En plus de définir la procédure à venir, elle a deux objectifs principaux :

- elle est le contrat qui lie l´entreprise et l´auditeur ;
- elle permettra d´informer les différentes personnes impliquées de l´arrivée d´un audit dans l´entreprise. Elle est dans le même temps, auprès des salariés, une légitimation de cet audit par la direction.

Troisième phase : le recueil de toutes les informations nécessaires pour préparer la mission. Il s´agit de récolter les éléments relatifs à la culture de l´entreprise, au contexte général toujours en corrélation avec le système d´information. Des rendez-vous sont donc organisés avec les personnes concernées.

La quatrième phase est la réalisation de la mission, l'audition du système d'information de l'entreprise peu commencé.

Enfin, une réunion de synthèse est organisée entre l´auditeur et les personnes intéressées. Il s´agit de s´assurer ensemble :

- que les questions de l´auditeur ont été bien comprises ;
- que les réponses ont été bien interprétées.

Le rapport est ensuite rédigé, de plusieurs manières (concis et plus complet), car il s´adresse en général à plusieurs types de publics.

Le rapport détaillé expliquera les attentes de départ, le contexte, les limites, les faiblesses constatées, leur importance relative et les solutions.

Un rapport d´audit doit être clair et didactique. En aucun cas il ne doit être technique.

4. Les techniques d'audit

A. L'audit dit "boite blanche"

La méthode dite « *white box* » consistant à tenter de s'introduire dans le système en ayant connaissance de l'ensemble du système, afin d'éprouver au maximum la sécurité du réseau.

a) Audit de code

Il existe des bases de vulnérabilités très fiables pour les applications répandues. Néanmoins, pour des applications moins utilisées, ou codées par l'entreprise elle-même, il peut être nécessaire d'analyser leur sécurité. Si les sources de l'application sont disponibles, il faut lire et comprendre le code source, pour déceler les problèmes qui peuvent exister. Notamment, les débordements de tampon (Buffer Overflow), les bugs de format, ou pour une application web, les vulnérabilités menant à des injections SQL...

L'audit de code est une pratique fastidieuse et longue. De plus, elle ne permet généralement pas, en raison de la complexité, de dresser une liste exhaustive des vulnérabilités du code. Des méthodes automatiques existent, et permettent de *dégrossir* le travail, avec des outils comme RATS. Mais se reposer uniquement sur ce genre de méthodes peut nous faire passer à côté de problèmes flagrants pour un humain.

b) Audit de configuration

Les audits de configuration permettent d'expertiser l'architecture technique déployée et de mesurer la conformité des configurations des éléments qui la composent (serveurs, bases de données, équipements réseau, pare-feu, autocommutateurs privés, etc.) avec la politique de sécurité définie. Ils en exposent les points faibles de l'architecture et se concentrent sur les actions à entreprendre pour mettre en œuvre un processus de sécurisation par couche. La réalisation d'un audit de configuration est par nature non destructrice (contrairement à certaines étapes d'un test d'intrusion). Ce type d'audit est destiné à toutes les entreprises.

c) Audit de gestion des habilitations

Les audits de gestion des habilitations permettent d'analyser les accès aux ressources systèmes ou applicatives et impliquant des utilisateurs internes ou externes à l'entreprise. Ainsi, les comptes et les droits fantômes seront détectés, les actions de fraude seront rendues plus difficiles et la détection des actes malicieux sera facilitée. Ce type d'audit est destiné à toutes les entreprises.

d) Audit déclaratif

Les audits déclaratifs permettent d'obtenir des résultats reposant uniquement sur les déclarations lors d'entretiens avec les acteurs du système audité : cela introduit un biais du au contrôle volontaire/involontaire des audités sur les informations délivrées. Ce type d'audit est destiné à toutes les entreprises.

e) Audit organisationnel

Les audits organisationnels permettent de mesurer et d'identifier les risques des éléments critiques de l'entreprise (processus métier, outils de production dont le système informatique, …). Ils représentent une optique à long terme. Ils sont importants pour préserver un niveau de sécurité dans le temps. Ils sont réalisés à l'aide de méthodes formelles telles Méhari, CRAMM, COBIT. Les audits organisationnels prennent en compte la sécurité en général dans l'entreprise. Cependant, c'est une démarche lourde qui peut mobiliser une équipe de consultants spécialisés durant plusieurs semaines, et elle est de ce fait rarement appliquée à des entreprises de taille plus modeste. Ce type d'audit est donc destiné aux grandes entreprises.

B. L'audit dit "boite noire"

La méthode dite « *black box* » consistant à essayer d'infiltrer le réseau sans aucune connaissance du système, afin de réaliser un test en situation réelle.

a) Audit de vulnérabilités

Les audits de vulnérabilités permettent de détecter les éventuelles failles de sécurité du système d'information d'une entreprise tel qu'il peut être vu de l'extérieur, c'est à dire depuis Internet. L'opération est possible à l'aide de scanners de vulnérabilités. Ceux-ci lancent des attaques connues sur le réseau cible (hormis celles qui pourraient neutraliser les systèmes évalués). L'avantage de ces tests tient à leur rapidité, leur simplicité de mise en oeuvre et leur faible coût. De plus, les audits de vulnérabilités ne sont pas destructeurs. Leur inconvénient, bien sûr, est que ces tests ne détectent vraiment que les failles connues et plutôt simples à exploiter. Ce type d'audit est destiné aux PME.

b) Test d'intrusion

Les tests d'intrusion permettent de valider périodiquement le niveau de sécurité du système d'information et d'en mesurer les variations. Ils sont réalisés de manière récurrente. Ils consistent à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle à partir de l'extérieur de l'entreprise. Ils ne permettent pas de garantir la sécurité du système, dans la mesure où des vulnérabilités peuvent avoir échappé aux testeurs. Ce type d'audit est destiné à toutes les entreprises.

c) Audit technique

Les audits techniques permettent d'évaluer le niveau de sécurité par analyse interne des systèmes en place. On se place dans du court terme, pour mettre à niveau la sécurité dans l'urgence. Ils permettent d'étudier les éléments techniques en production dans l'entreprise et d'en valider le niveau de sécurité. Il s'agit d'une prestation hautement technique, dont la plupart des PME peuvent très bien se passer. Ce type d'audit est donc destiné aux grandes entreprises.

d) Le Fuzzing:

Pour les applications *boite noire*, où le code n'est pas disponible, il existe un pendant à l'analyse de code, qui est le fuzzing. Cette technique consiste à analyser le comportement d'une application en injectant en entrée des données plus ou moins aléatoires, avec des valeurs *limites*. Contrairement à l'audit de code qui est une analyse structurelle, le fuzzing est une analyse comportementale d'une application.

5. Les besoins

La première chose est de se tenir au courant des dernières vulnérabilités, ainsi, s'abonner à des mailing-list (securityfocus.com, seclists.org) et consulter fréquemment des sites de veille sont des moyens efficaces d'être informé.

Une distribution de type Backtrack permettra d'avoir un environnement muni de la plupart des outils nécessaires à un pentest, mais peuvent être remplacé par un système Unix quelconque. Une clé/carte wifi compatible injection et monitor est également recommandé.

6. La réalisation d'un audit

A. La recherche d'informations

Un test d'intrusion commence toujours par une phase de collecte d'informations. Récolter les éléments relatifs à la culture de l´entreprise, au contexte général toujours en corrélation avec le système d´information.

Qui travail dans cette entreprise, sont-ils sensibilisés aux problèmes de sécurité ? Quelles sont leurs infrastructures (sans parler de la partie logiciels), CISCO, Enterasys, CheckPoint ? Des périphériques informatiques (clé USB etc...) peuvent-ils entrer dans l'entreprise ? Les employés ramènent ils des données chez eux ? Quels sont les IP accessibles depuis l'extérieur ?

Autant de questions auxquels il faut tenter de répondre avant de commencer un test d'intrusion.

On recherche tous les domaines enregistrés par la cible grâce au Whois (Nous donne aussi noms, adresses et téléphones des administrateurs).

```
[root@Evil /root]# whois secway.com@whois.networksolutions.com
[whois.networksolutions.com]
<...>
Registrant:
Secway (SECWAY-DOM)
   25-27, rue de l'Ouest
   Paris, 75014
   FRANCE

   Domain Name: SECWAY.COM

   Administrative Contact, Technical Contact, Billing Contact:
      Nicolas, DUBEE  (DN4404)  ndubee@DF.RU
      SECWAY
      25-27, rue de l'Ouest
      paris
      75014
      FR
      +33 1 43211718

   Record last updated on 21-May-2001.
   Record expires on 07-Mar-2002.
   Record created on 07-Mar-1999.
   Database last updated on 13-Sep-2001 06:38:00 EDT.

   Domain servers in listed order:

   NS1.325I.COM              216.149.77.66
   NS3.NJD.XO.COM             216.156.2.3
```

On interroge DNS pour connaître les adresses IP des serveurs www, mail, …

```
[root@Evil /root]# host -a secway.com
Trying null domain
rcode = 0 (Success), ancount=3
The following answer is not authoritative:
The following answer is not verified as authentic by the server:
secway.com      172296 IN      NS      NS1.325I.com
secway.com      172296 IN      NS      NS3.NJD.XO.com
secway.com      172296 IN      A       194.221.6.40
For authoritative answers, see:
secway.com      172296 IN      NS      NS1.325I.com
secway.com      172296 IN      NS      NS3.NJD.XO.com
Additional information:
NS1.325I.com    172296 IN      A       216.149.77.66
NS3.NJD.XO.com  172296 IN      A       216.156.2.3
[root@Evil /root]# host -t mx secway.com
secway.com mail is handled (pri=10) by mail.secway.com
[root@Evil /root]# host -a www.secway.com
Trying null domain
rcode = 0 (Success), ancount=1
www.secway.com  3600 IN CNAME   secway.com
For authoritative answers, see:
secway.com      3600 IN NS      secway.com
Additional information:
secway.com      3600 IN A       216.149.77.66
```

Grâce à DNS, nous avons obtenu des adresses IP du réseau ciblé, nous faisons une recherche inverse avec les bases d'IP régionales, afin de connaître l'ensemble des IP allouées à la cible.

```
[root@Evil /root]# whois 216.149.77.66@whois.arin.net
[whois.arin.net]
9 Net Avenue, Inc. (NETBLK-NINENETAVE-1)
  110 Meadowland Parkway
  Secaucus, NJ 07094
  US

  Netname: NINENETAVE-1
  Netblock: 216.149.0.0 - 216.149.255.255
  Maintainer: 9NET

  Coordinator:
    Grosso, Patrick  (PG64-ARIN)  patg@9NETAVE.COM
    888-963-8283

  Domain System inverse mapping provided by:

  NS2.9NETAVE.COM          216.156.2.2
  NS3.9NETAVE.COM          216.156.2.3

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

  Record last updated on 27-Jan-2000.
  Database last updated on 10-Sep-2001 23:16:26 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
[root@Evil /root]#
```

Exemples de Nicolas Dubée

Le mail Bounce: Envoi d'un mail à une adresse invalide dans le domaine cible pour obtenir un retour.

En examinant les en-têtes dans le mail retourné nous obtenons des informations sur la structure du réseau ciblé.

Received: from relais.xxxxx.com ([123.45.67.89]) by koi.df.ru (8.9.0/8.8.8) with SMTP id QAA21414 for <ndubee@DF.RU>; Fri, 11 Aug 2000 16:20:06 +0400
Received: from **192.1.1.50** by relais.xxx.com (InterScan E-Mail VirusWall NT); Fri, 11 Aug 2000 14:24:14 +0200 (Paris, Madrid (heure d'été))
Received: by **mail.xxxxx.com(Lotus SMTP MTA SMTP v4.6 (462.2 9-3-1997))** id C1256938.0043AF89 ; Fri, 11 Aug 2000 14:19:18 +0200
X-Lotus-FromDomain: ORG
To: Nicolas Dubee ndubee@DF.RU

Received: from relais.xxxx.com ([123.45.67.89]) by koi.df.ru (8.9.0/8.8.8) with SMTP id TAA17429 for <ndubee@df.ru>; Fri, 11 Aug 2000 19:06:50 +0400
Message-Id: <200008111506.TAA17429@shell.dataforce.net>
Received: from **192.1.1.50 by relais.xxxx.com (InterScan E-Mail VirusWall NT)**; Fri, 11 Aug 2000 17:10:58 +0200 (Paris, Madrid (heure d'été))
From: POSTMASTER@mail.xxxxx.com
To: ndubee@df.ru
Date: Fri, 11 Aug 2000 17:05:54 +0200
Objet: message non distribué
X-UIDL: 3864dfdeb927e75e31fd1ea0fe9acfd9

------- Motif de l'échec --------

Utilisateur non recensé dans le Carnet d'adresses public
fdgdfgsdfg@xxxxxxxxx.com

------- Message renvoyé --------
Received: from **relais.xxxx.com ([192.168.20.1])** by mail.xxxxxxxxx.com (Lotus SMTP MTA SMTP v4.6 (462.2 9-3-1997)) with SMTP id C1256938.0052E6F3; Tue, 11 Aug 1970 17:05:30 +0200
Received: from 195.132.98.198 by relais.xxxxx.com (InterScan E-Mail VirusWall NT); Fri, 11 Aug 2000 17:09:57 +0200 (Paris, Madrid (heure d'été))

bounce test.

---
vérifié par interscan (antivirus)

Le Traceroute nous permet de déterminer de tous les intermédiaires (routeurs) entre nous et la cible.

C'est l'envoi de paquets avec un TTL (Time To Live) incrémenté qui va permettre à traceroute de connaitre la route empruntée par un paquet vers la destination. Le TTL correspond à la durée de vie d'un paquet transitant sur un réseau. Chaque passage par un équipement de routage va décrémenter le TTL de un. Une fois le TTL à zero, le routeur nous renvoie alors un message ICMP de type : 11 ICMP TTL Exceeded. Ce qui permet de récupérer l'adresse du premier routeur.

Cependant certain équipements réseaux sont configurés pour ne pas envoyer de paquet d'avertissement dans le cas où le TTL vaut 0 (Pour une question de sécurité). Cette technique présente donc des limites.

Le Firewalking est une variante de traceroute qui permet de déterminer les ACL (Access Control List) au niveau du firewall.

Il va déterminer le nombre de routeurs entre la machine source et la machine cible (située donc derrière le firewall). Ensuite, il envoie des paquets tests avec un TTL égal à (nombre de routeurs + 1). Le +1 permettra d'aller faire mourir le paquet sur la machine cible. Si le paquet est accepté par le firewall, il le traverse, et on obtient une réponse. Sinon le paquet est bloqué par l'ACL du firewall, il sera abandonné et, selon la configuration du firewall, soit aucune réponse ne sera envoyé, soit il enverra un paquet de ICMP de type 13 (filtre admin).

B. Les techniques sans accès au SI

La première chose à faire est de scanner le réseau, nous utiliserons pour cela le logiciel Nmap.

L'utilisation de la distribution Backtrack, basé sur une Linux Ubuntu, va nous permettre d'avoir tout les outils à portée de main.

Nmap permet beaucoup de chose, et connaitre son fonctionnement est primordial: Les principes et techniques sont expliqués sur la documentation officielle de Nmap.

Nous allons commencer par nous renseigner sur les serveurs et postes accessible depuis l'extérieur. Les IDS/IPS ou Firewall peuvent bloquer les tentatives de nmap, c'est pourquoi plusieurs techniques de scan doivent être utilisées... Lors des scans effectués avec nmap pendant un audit de sécurité, il est recommandé d'utiliser un logiciel de collecte et de classement les données. L'utilitaire Dradis (compris dans le package Backtrack) pourra nous aider.

La diversité des scans de Nmap lui permette de contourner certaines protections, ainsi, les différentes alternatives doivent être choisies en fonction de la machine à scanner, c'est pourquoi une bonne connaissance de nmap et de ces techniques sont requises.

Connaitre le système d'exploitation de la cible est une bonne chose, Nmap permet cela (Flag -O). Il le détermine en créant un Fingerprint avec les paquets reçu, et le compare ensuite à sa base de donnée. Si nmap n'arrive pas à déterminer la version, il pourra certainement nous donner une liste des systèmes qui pourraient potentiellement correspondre (Flag --osscan-guess).

Si des ports sont ouverts, il faut maintenant tenter de les exploiter. Un port ssh ouvert pourra conduire à un simple bruteforce par dictionnaire, en effet, les mots de passe "commun" et donc peu sécurisé, sont encore utilisés fréquemment. Sur un protocole SSH, cela fait de l'attaque par dictionnaire un moyen simple et fiable de détecter un problème de sécurité dans un système d'information.

D'innombrables possibilités étant possible, cette documentation n'est la que pour donner des pistes.

Si aucun port n'est ouvert, d'autres techniques sont possibles.

L'envoi d'un email infecté à une personne non sensibilisé à la politique de sécurité est une voie à exploiter, de plus, cela ne nécessite que quelques minutes. Heureusement, un firewall équipé d'un antivirus de flux (VStream) ou un antivirus installé sur la machine devrait détecter cela. Cependant des techniques de dissimulations existent, même si elles ont leurs limites.

Le social engineering est une autre solution, qui consiste à utiliser les failles humaines de l'entreprise. En utilisant ses connaissances, son charisme, l'imposture ou le culot, nous pourrons souvent avoir accès à des informations confidentielles. Cela dépendra de votre imagination.

Un exemple récent d'exploitation particulièrement sournoise est l'utilisation d'une souris piégée par une société d'audit. Cette dernière l'a envoyé à un employé qui l'a branché pensant à un cadeau promotionnel. Un cheval de Troie c'est alors déployé, créant une backdoor discrète puisque l'exploit utilisait une faille zero-day de McAfee. (Une souris branché sur un port PS/2 n'aurait pu répandre un malware, d'où l'utilité d'être attentif aux ports USB...)

Des antennes et carte wifi puissante peuvent étendre considérablement la portée des signaux wifi, ainsi, nous pourrons tenter de capter le réseau wifi de l'entreprise.

Imaginons que celui ci utilise du WEP (Même si aujourd'hui cela est très rare, certaines petites entreprise pourrait encore l'utiliser, cela est bien entendu une faille énorme), nous pourrons alors le pénétrer en quelques minutes grâce à des outils spécialisés comme aireplay, airodump ou aircrack, distribués avec Backtrack.

Cependant cela reste des cas isolés. Comme le cassage d'un réseau WPA/WPA2, WPA Entreprise ou WPA-PSK est à l'heure actuelle, quasi impossible, a moins que les mots de passes choisis soit brutforcable par dictionnaire, nous allons nous concentrer sur un autre type d'attaque wifi, les rogues AP.

Le rogue AP est une solution efficace pour ce mettre en position de Man in the middle, et donc avoir accès à tout le trafic. L'utilisation d'une attaque déauth va vous permettre de déconnecter la machine ciblée du wifi. En parallèle, vous créerez un AP copiant tous les paramètres du réseau ciblé (SSID, adresse MAC...), si votre signal est plus fort que le signal réel (ce qui est possible grâce à des cartes/routeurs wifi puissants), Windows se connectera automatiquement dessus. Vous pourrez ensuite espionner et rerouter le trafic réseau.

La dernière attaque à mettre en place est le DDOS (distributed denial-of-service attack**)**, une attaque simple, mais qui peut avoir des conséquences économiques réelles pour une entreprise. Nous ne détailleront pas ici sa mise en œuvre, des logiciels spécialisés pouvant s'en occuper très facilement.

Si l'audit concerne un serveur web, ou que des identifiants peuvent être récupérer sur le site, les failles XSS ou CSRF sont des moyens pertinents pour récupérer un compte utilisateur.

L'injection SQL peut donner de bon résultat en DROPANT les tables utilisateurs. Pour automatiser la recherche de failles XSS CSRF ou SQL, certains outils peuvent être utilisés.

Encore beaucoup de failles de ce type sont présentes sur internet. Cependant, l'utilisation de Framework du type Symfony ou Zend (Réservés à des sites d'une taille importante) permette d'éviter ce genre de problème, le système de token étant implémenté plus facilement pour les CSRF, des ORM sont utilisés pour contrer les injections SQL et quelques lignes de configurations évitent les failles XSS.

C. Les techniques avec accès au SI

Disposer d'un accès à l'intérieur du réseau nous permettra d'effectuer des tests plus fins et plus en profondeur.

Connaitre la génération des mots de passes est une bonne chose, s'ils ne sont pas assez robustes, un brutforce (par dictionnaire ou non, en fonction des mots de passes) démontrera les limites d'un passe trop peu complexe.

La première chose à faire va être de cartographier le réseau, nmap le permet. Même si nous savons combien d'hôtes constitue le réseau, il est important de savoir lesquels sont accessibles.

Une fois les hôtes découverts, nous devons savoir si des ports qui ne devrait pas l'être sont ouvert, et de par ce fait, peut-être exploitable.

Dans le cas d'un audit avec accès au réseau, certains logiciels vont nous simplifier la vie, Nessus est un programme qui va tester le réseau pour nous. Nessus doit être configuré et les hôtes ajoutées à son champ d'action. Une fois ceci fait, il va se charger de détecter un bon nombre de failles à notre place.

Cependant, un logiciel comme Nessus n'est pas parfait, et il ne traitera pas tout. Il est donc primordial de compléter son analyse.

Nous pouvons tout d'abord vérifier les versions de chaque logiciel installés sur les hôtes du réseau, un logiciel faillible peut conduire à une escalade des privilèges pour un pirate. Rechercher des logiciel non mis a jour et ce renseigner sur les failles de sécurité potentielles desdits logiciels.

Le Framework Metasploit qui est intégrer à Backtrack, permet de créer des payloads personnalisés avec de nombreux shellcodes fournies (Shell reverse TCP par exemple), et des techniques d'offuscations (différents système de cryptage du payload sont disponibles). Ainsi, si certains logiciels utilisés sont faillibles (Buffer Overflow, Format String...), Metasploit nous permettra de créer et d'utiliser un exploit aisément

Nous pouvons aussi tenter d'exécuter des logiciels malicieux par les ports USB des machines.

Une attaque de type SSL Strip peut également servir à capturer des identifiants de pages sécurisés.

L'attaque ARP spoofing/cache poisonning permet quand à elle plusieurs types d'attaque, le DOS et DDOS, le Man in the midlle et le MAC Flooding.

Le MAC Flooding est particulièrement intéressant. Certains matériels réseaux actifs, lorsqu'ils sont surchargés, basculent dans un mode moins gourmand en ressources, pour sauvegarder leurs liens : ils deviennent de simples hubs et donc broadcastent tout le trafic réseau sur tous leurs ports. Ce qui permet ensuite d'écouter facilement tout ce qui transite sur le réseau.

7. Les contremesures

Tout d'abord, nous venons de voir une des plus grandes faiblesses en termes de sécurité informatique, l'humain.

Une simple souris envoyée a un employé peu compromettre la sécurité de tout un réseau. C'est pourquoi les ports USB des machines doivent être vivement contrôlé, voir désactivé s'il n'y en a pas de besoin, et surtout, l'exécution automatique des périphériques désactivée.

Mais le personnel doit également être sensibilisé à tout cela. Cette sensibilisation peut être une formation par des organismes extérieurs.

Exemple: un SSL Strip sur une page d'identification est grave, et il est presque invisible pour un utilisateur lambda, encore plus si son navigateur n'est pas a jour. Quelques bonnes pratiques peuvent éviter cela.

Tous les logiciels doivent être à jours, en particulier les navigateurs si ils sont utilisés, pour éviter toute faille connue et non patché, qui pourrait être exploitable.

Si l'entreprise utilise des logiciels développés uniquement pour elle, celle ci doit s'assuré de la qualité de l'application en terme de sécurité.

Les mots de passe constituent une énorme porte d'entré si ils ne sont pas suffisamment robuste, c'est pourquoi ils doivent être changés régulièrement et être généré aléatoirement, avec certaines règles (Caractères spéciaux obligatoire par exemple).

La sécurité nous l'avons vu, s'applique aussi et surtout à la configuration du réseau. Un IDS/IPS est une sécurité en plus concernant la prévention des attaques, il va permettre de détecté facilement d'éventuel scan et attaque, et permettra de les bloquer en amont.

Les mails sont une source d'infection importante (CF l'attaque de Bercy en 2011) c'est pourquoi un antispam/antivirus comme ProofPoint est vivement conseillé.

Il est évidemment impératif d'avoir des firewalls qui filtre toutes les communications et un antivirus sur chaque poste.

Les réseaux wifi doivent être configuré correctement, il est clair qu'un wifi en WEP ne tiendra pas longtemps. Optez pour des sécurités wifi d'entreprise.

La meilleure protection contre l'ARP Poisoning (et beaucoup d'autre attaques) est la surveillance de votre réseau, en effet, avec les outils appropriés, cette attaque ne peut pas passer inaperçue. Par exemple, il existe un outil nommé ARPwatch qui permet, en autres, d'envoyer une alerte quand des messages ARP anormaux apparaissent. Pour de tout petit réseaux, vous pouvez utiliser une méthode imparable: Utiliser des Adresses IP fixes / Tables ARP statiques. Certains switch intègrent des options « port security » (par exemple Cisco) cette option permet de définir une seule adresse MAC par ports et qui, si cette adresse change, verrouille le port.

8. Le rapport d'audit

Une fois le système informatique de l'entreprise testé, la société auditrice doit rendre un rapport.

Le rapport est rédigé de plusieurs manières (concis et plus complet), car il s´adresse en général à plusieurs types de publics.

Le rapport détaillé expliquera les attentes de départ, le contexte, les limites, les faiblesses constatées, leur importance relative et les solutions.

Un rapport d´audit doit être clair et didactique. En aucun cas il ne doit être technique.

9. Conclusion

Nous venons de voir un certains nombre de techniques d'intrusion dans un système d'information.

Comme vous l'aurez remarqué, il en existe beaucoup, et les pirates développent sans cesse de nouvelles méthodes. C'est pourquoi un réseau doit être en permanence surveillé, par des équipements mais aussi par des administrateurs. La veille est un moyen efficace de ce protégé de presque tout type d'attaque.

De plus, les mesures prise par l'entreprise doivent être en corrélation avec les sensibilités des données de son réseau. Avant un audit, une analyse des risques est donc conseillée afin de savoir ce que l'on veut protéger, et surtout, comment.

J'espère avoir donné un bon nombre de pistes qui pourront servir de "mémo" ou de pistes pour de futurs audits.