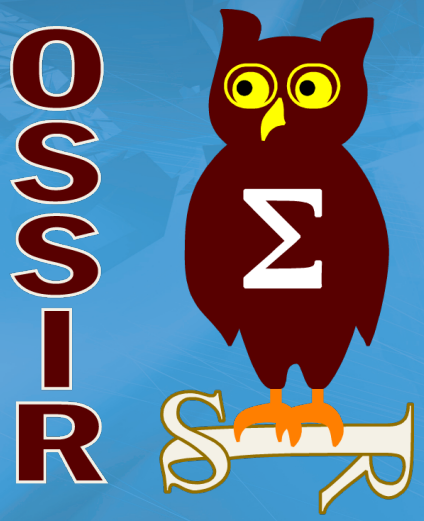
TOP 10 DES VULNÉRABILITÉS : RETOUR SUR 5 ANS DE PENTEST



10 Décembre 2013

Julien Lavesque – j.lavesque@itrust.fr

ITrust
IT Security Services

IKare©
My Business Monitoring in Real Time

$ WHOAMI

- Julien Lavesque
  - ✓ Directeur technique ITrust
  - ✓ Consultant Sécurité depuis 10 ans
  - ✓ Spécialisé en sécurité embarqué et environnement Cloud Computing

- ITrust
  - ✓ Société toulousaine
  - ✓ Expertise en sécurité informatique

- Activités
  - ✓ Service en sécurité (pentest / forensic / formation…)
  - ✓ Editeur de la solution de gestion de vulnérabilités et de supervision de sécurité IKare.

CONSTAT

75%

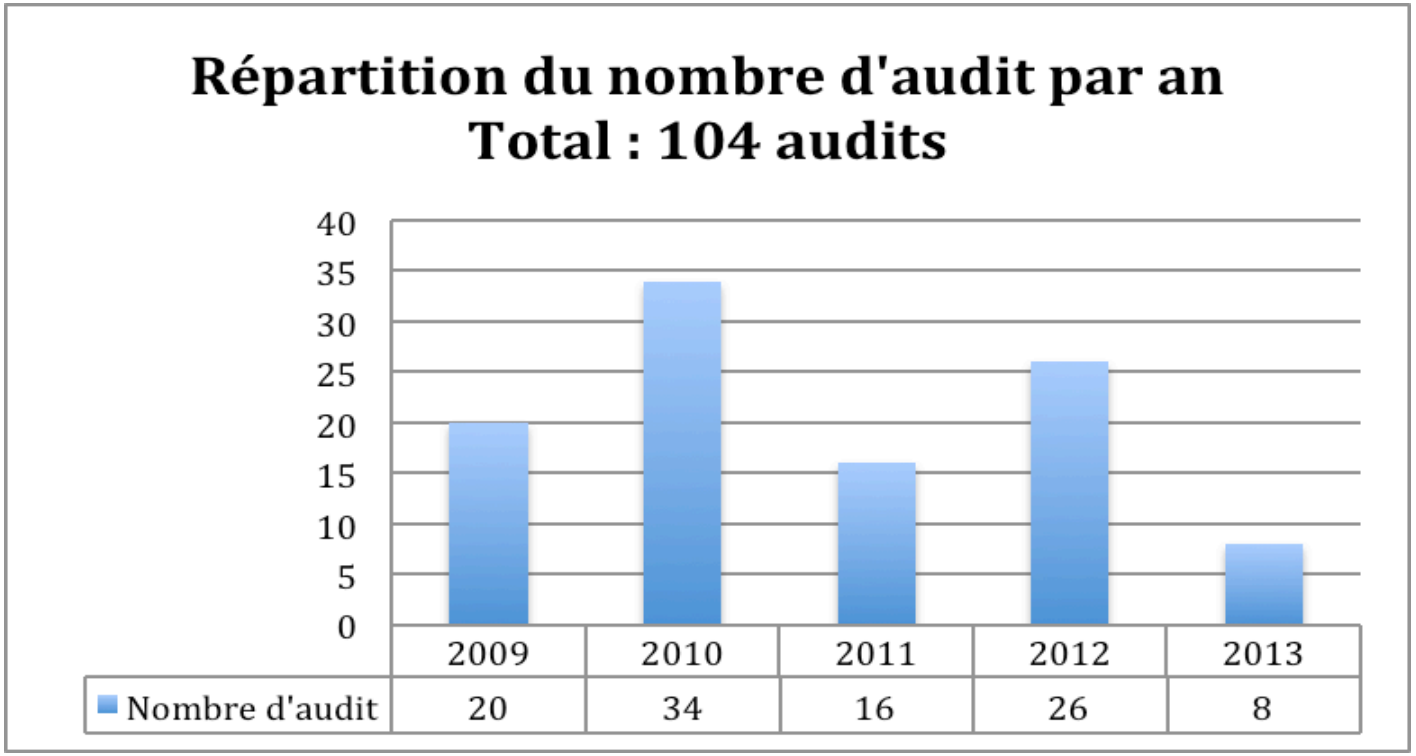
C’est le taux d’entreprises piratées au cours des 2 dernières années (Source étude Cenzic).

Ce taux atteint 90% sur les statistiques de nos audits.

La plupart du temps les entreprises ne savent même pas qu’elles sont piratées.

STATISTIQUES DU TOP 10

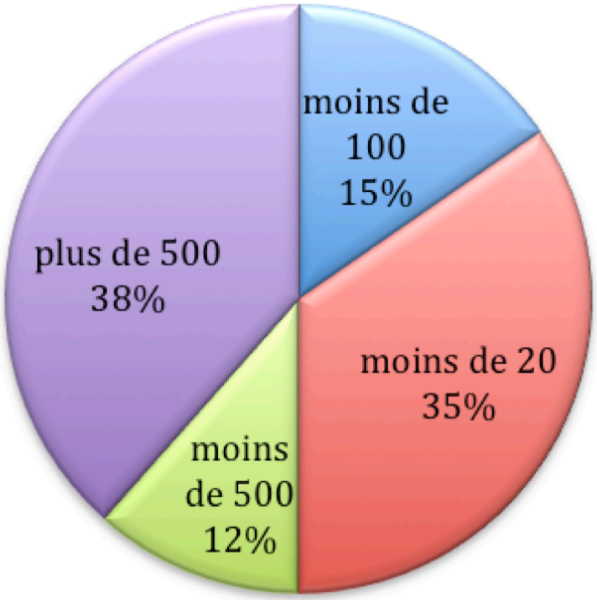
- Etude basée sur les 5 dernières années de tests d'intrusion.



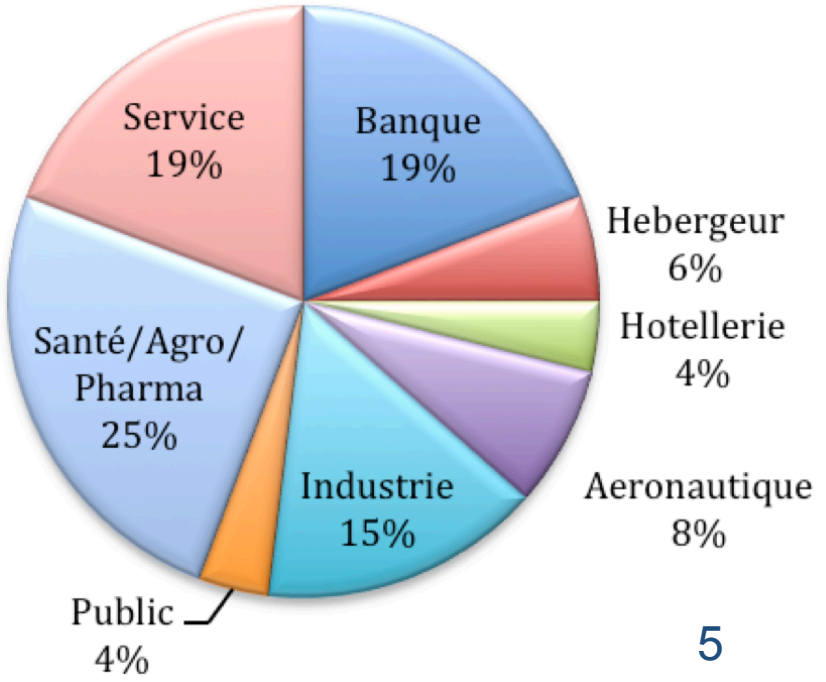
STATISTIQUES DU TOP 10

- Quelques chiffres sur la répartition des audits :

Répartition des clients par nombre d'employés



Répartition des clients par domaine d'activité



ITrust
IT Security Services

TOP 10
DES VULNÉRABILITÉS

10 - SYSTÈMES TROP VERBEUX

Le salon de thé des réseaux :

- Etape initiale d'un test d'intrusion
  - ✓ Pas de compromission
  - ✓ Informations importantes sur les cibles potentielles
- Serveur de nom DNS
  - ✓ Accès à toutes les zones par transfert
  - ✓ Avec les sous-zones (par responsabilité / département…)
  - ✓ Zones intéressantes : Compta / R&D…
- Contrôleur de domaine
  - ✓ Informations accessibles par LDAP, Samba ou RPC
  - ✓ Obtention d'informations sur le domaine ou le système d'exploitation
  - ✓ Obtention d'informations sur les utilisateurs

10 - SYSTÈMES TROP VERBEUX

- Exemple : utilisateurs d'un domaine

```
~$ rpcclient 192.168.0.1 -p 139 -U% -c enumdomusers
user:[Administrateur] rid:[0x1f4]
user:[Invité] rid:[0x1f5]
user:[Wheel] rid:[0x476]

~$ rpcclient 192.168.0.1 -p 139 -U% -c enumdomgroups
group:[Admins du domaine] rid:[0x200]
group:[Utilisa. du domaine] rid:[0x201]
group:[Invités du domaine] rid:[0x202]

~$ rpcclient 192.168.0.1 -p 139 -U% -c 'querygroupmem 0x200'
rid:[0x1f4] attr:[0x7]
rid:[0x476] attr:[0x7]

~$ rpcclient 192.168.0.1 -p 139 -U% -c getdompwinfo
min_password_length: 0
password_properties: 0x00000000

~$ rpcclient 192.168.0.1 -p 139 -U% -c querydispinfo
index: 0x11ee RID: 0x1f4 acb: 0x00000210 Account: Administrateur    Name: (null)      Desc: Compte d'utilisateur d'administration
index: 0x11f4 RID: 0x476 acb: 0x00000210 Account: Wheel    Name: (null)      Desc: 5AB4Gy4
```

Propagation de la compromission

- Environnement Unix
  - ✓ Terminaux à distance non protégés (rsh et rlogin)

  De moins en moins autorisés par les politique de sécurité

  Compromission en chaine (.rhosts et host.equiv)
  - ✓ SSH

  Manque de protection de clés et utilisées sur plusieurs serveurs

  Fichier know_hosts pour savoir ou aller.

- Environnement Windows
  - ✓ Relations de confiance entre domaine : propagation de la faiblesse

- Nouvelle menace : le navigateur

08 – GESTION DES DROITS

- Besoin d'en connaitre
  - ✓ Classification de l'information absente
  - ✓ Gestion des droits laxiste

- Exemple : le test du stagiaire
  - ✓ Le stagiaire est ajouté dans les groupes AD de son (ses) maitre de stage

  - ✓ Test du stagiaire :
    - Un gestionnaire de fichiers
    - Un stagiaire avec son compte « stagiaire »
    - Et du temps

  - ✓ > Obtention de compte et d'informations en quelques jours

07 – PROTOCOLES D'ADMINISTRATION

Le diable est dans les détails

- Equipement souvent oubliés
  - ✓ Eléments actifs du réseaux (switch, routeur…)
  - ✓ Imprimantes
  - ✓ Onduleurs
- Configuration par défaut
  - ✓ Mots de passe par défaut
  - ✓ Protocoles en clair (telnet, FTP)
- Exemple : arrêt de la production
  - ✓ Compte par défaut sur l'administration web d'un onduleur.

Exemple : Audit d'un boitier VPN

- Boitier VPN d'une agence utilisé comme routeur Internet
- Le service SNMP est ouvert et permet la lecture et surtout l'écriture de la MIB
- Le scénario mis en place consiste à rediriger les requêtes DNS sur un de nos serveurs et étudier les statistiques des requêtes.
- le trafic mail et web est redirigé vers notre serveur et l'accès au compte de messagerie ainsi que l'intégralité des messages transitant est recueillie par nos soins.

- Cibles de choix
  - ✓ Informations confidentielles ou utilisables
  - ✓ Compte utilisateur

- Configuration non durcie
  - ✓ Verbosité : listage des bases Oracle
  - ✓ Mots de passes évidents : Oracle « changeoninstall »
  - ✓ Mots de passes basés sur le nom du serveur.

- Obtention de compte
  - ✓ Dump des bases utilisateurs
  - ✓ Cassage des mots de passe

- Exemple : ERP de la société

05 – PARTAGE DE FICHIERS

- Partages sans restriction
  - ✓ NFS : restriction seulement par adresse IP
  - ✓ FTP : accès anonymes. Attention aux uploads
  - ✓ Samba : accès anonymes sans restriction

- Récupération beaucoup d'informations confidentielles
- Malveillance interne plus problématique en cas de suppression.

- Exemple : imprimante de la direction
  - ✓ Imprimante / scan / fax avec un partage par défaut
  - ✓ Accès aux documents en cours d'envoi ou d'impression
  - ✓ Fichiers temporaires non supprimés.

04 – SERVEURS DE TEST OU A L'ABANDON

- Peu d'inventaire matériel et logiciel
  - ✓ Découverte de serveurs à l'abandon lors des audits
  - ✓ Pas de connaissance sur ces serveurs.

- Serveurs non stratégiques

- Serveurs facilement exploitables
  - ✓ Contient des comptes dupliqués sur les serveurs en production
  - ✓ Permet de faire des rebonds sur des cibles plus intéressantes
  - ✓ Contient des informations partiellement valides

- Sujet très bien décrit dans le top 10 OWASP

- Les vulnérabilités rencontrées se divisent en 2 phases:
- Phase 1 : les points d'entrée
  - ✓ Les applications pas à jour
  - ✓ Les attaques XSS
  - ✓ Les injections SQL
  - ✓ La gestion des sessions

- Exemple : le presque pire du cookie

  Set-Cookie: site[user]=j.lavesque%40itrust.fr; expires=…
  Set-Cookie: site[passwd]=5ceab7e78cf7dd140d7fc9bad1de3585; expires=…

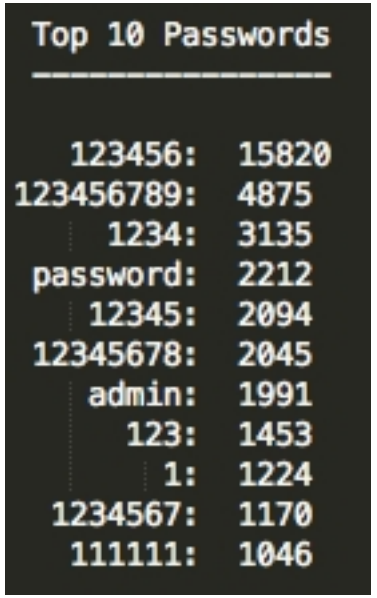
- Exemple : vidéo surveillance
  - ✓ Accessible sur internet
  - ✓ Cookie de session rejouable et format devinable
  - ✓ Mot de passe faible
  - ✓ Parfait pour organiser des cambriolages

- Phase 2 : exploitation
  - ✓ L'exposition de données sensibles
  - ✓ L'absence de configuration sécurisée
  - ✓ Le manque de restriction de privilèges.

- Exemple : fonction PHP non protégé
  - ✓ Une fonction d'upload de contenu est disponible
  - ✓ Le format des fichiers uploadé n'est pas vérifié
  - ✓ Possibilité d'uploader un webshell
  - ✓ Le fichier de mot de passe est récupéré
  - ✓ Rebond possible sur le backoffice

02 – MOTS DE PASSES

- Dans 96% des audits réalisés un mot de passe par défaut ou trivial permet d'accéder à des ressources confidentielles.
- Sujet pour lequel les utilisateurs sont le plus sensibilisés
- Reste le vecteur d'attaque le plus simple à exploiter
- Exemple d'une base de mots de passe exploitée par un botnet [Source Spiderlabs]
- Le retour ITrust : top 3 des mots de passe:
  - ✓ Pas de mot de passe
  - ✓ Mot de passe = login
  - ✓ Mot de passe = générique lors de la création



- Exemple : Serveur Blackberry

- Mot de passe par défaut pour le compte admin de la base MSSQL
- Accès à toutes les tables

- Fonction xp_cmdshell activé
  - ✓ Création d'un compte admin sur le serveur
  - ✓ Connexion au partage administratif C$
  - ✓ Inspection de l'arborescence

- Vulnérabilité du serveur Blackberry
  - ✓ Les pièces jointes par Blackberry sont stockés dans un répertoire Temp
  - ✓ Plusieurs giga de données confidentielles.

01 – VULNÉRABILITÉS HISTORIQUES

- Vulnérabilités connues et publiées par les CERT
- Quasiment 100% de présence lors de nos audits
- Problématique la plus facile à exploiter et à automatiser
- Il suffit de mettre à jour les systèmes et applications pour s'en prémunir.
- Responsables de la plupart des exploitations dans l'actualité
- Exemple du Playstation Network.

CONCLUSION

9 fois sur 10 nous pénétrons un système au cours d'un audit – à partir d'une vulnérabilité de ce top 10.

75%

C'est le taux d'entreprises piratées au cours des 2 dernières années.

97%

Des attaques auraient pu être évitées par des contrôles simples ou intermédiaires (Source Verizon).

Un outil de détection de services et de vulnérabilités automatisé permet d'identifier la majeure partie de ces menaces.

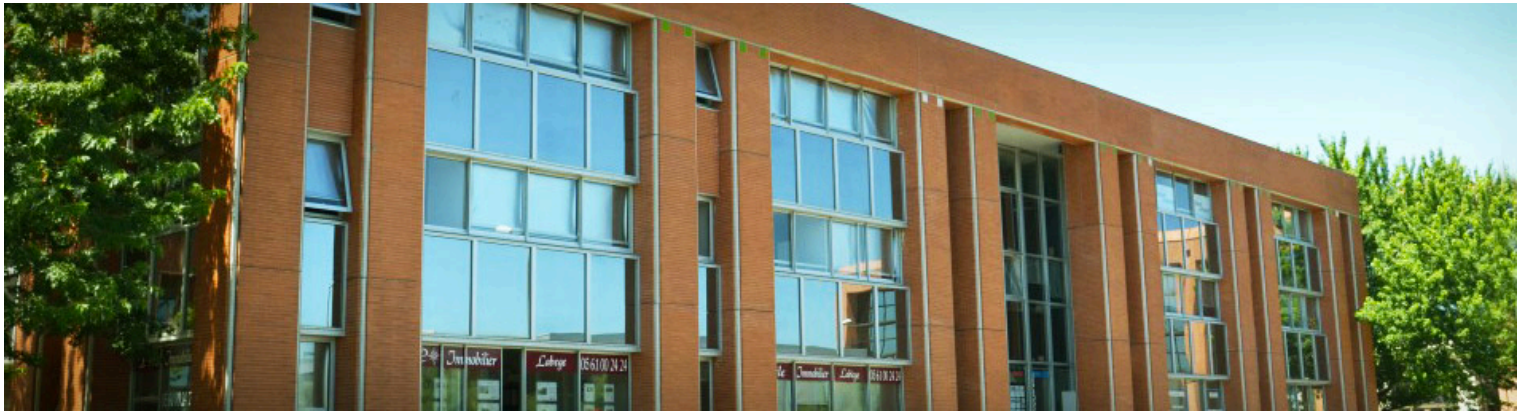
QUE FAIT LA POLICE ?

- Souvent le salut vient de la réglementation.

- Ces contrôles seront mis en place de manière systématique que s'ils sont obligatoires

- C'est une tendance forte dans les normes et guides
  - ✓ Guide d'hygiène sur la sécurité de l'ANSSI
  - ✓ 20 contrôles de sécurité du SANS
  - ✓ Norme santé HDS
  - ✓ ISO 27001…

QUESTIONS ?



ITrust - Siège Social
55 Avenue l'Occitane,
BP 67303
31673 Labège Cedex

+33 (0)5.67.34.67.80
contact@itrust.fr
www.itrust.fr
www.ikare-monitoring.com