Top 10 des failles internes
« Améliorer sa sécurité en se piratant »

23 mars 2010

<d.ducamp@itrust.fr>

Immeuble ACTYS/1
Avenue l'Occitane BP 67303
31673 LABEGE CEDEX
contact@itrust.fr
Tel: 09.80.08.36.12
Fax: 09.80.08.37.23

http://www.itrust.fr

Ikare : an ITrust Innovative Solution for Real Time Analysis

Ikare : La Solution d'aide à la décision informatique et la réduction des coûts informatiques

· Une supervision bout en bout du SI
· Analyse de la performance réseau, infrastructure, application ,securite et perception utilisateur
· Business activity monitoring : Performance et disponibilité
· Gestion des services métiers
· Une cartographie de SI, découverte automatique
· Un scanner non intrusif en mode SAAS (interne ou externe)
· Un moteur de services experts
· Un algorithme de corrélation proactif
· Gestion de la disponibilité et performance des SLA (Service level agreement)
· Consolidation intelligente et corrélation d'événements et de logs
· Évaluation de conformité

Ikare redéfinit la nouvelle génération des outils de supervision (SIM, SIEM)

TOP 10 (1/2)

- Domaine bureautique
  - Gestionnaires de domaines trop verbeux : MS, ldap...
  - Mots de passe évidents
  - Partages : droit et besoin d'en connaître
- Relations de confiance : propagation de la compromission
- Serveurs de bases de données
- Serveurs DNS trop verbeux pour les domaines internes

TOP 10 (2/2)

- Systèmes non sécurisés :
  - Partages de fichiers,
  - Protocoles d'administration,
  - Serveurs à l'abandon ou de validation et de développement
  - Failles historiques
- Ex : photocopieurs, routeurs, switches...

3 exemples réels...

- Routeur VPN d'une agence distante
- Serveur BlackBerry
- « Photocopieurs »

Gestionnaires de domaines trop verbeux : MS, ldap...

- Serveurs acceptant de lister les utilisateurs
  - Via SMB
    - Liste complète ou un par un...
  - et LDAP
    - Avec une connexion anonyme.
- Postes clients acceptant de donner le nom de son utilisateur

Mots de passe évidents

- Pas de mot de passe
- Mot de passe = login
- Mot de passe par défaut lors de la création
- Prénom
- Dictionnaire : langue natale, spécialisé (métier...)

Partages : droit et besoin d'en connaître

- Chaque utilisateur appartiennent à un groupe
  - Le groupe se voit octroyer un droit d'accès à un partage quand un utilisateur en a besoin
  - Chaque stagiaire est mis dans le(s) groupe(s) de son(ses) maître(s) de stage
- Test du stagiaire :
  - Un gestionnaire de fichiers
  - Un stagiaire et son compte « stagiaire »
  - Et du temps...
  - => Obtention des comptes / mots de passe d'administration en quelques jours

Relations de confiance : propagation de la compromission

- Unix
  - hosts.equiv et .rhosts : rlogin, rsh
  - shosts.equiv et .shosts : ssh
    - Mais aussi les clés privées non protégées par mot de passe et autorisées sur d'autres serveurs...
    - et known_hosts pour savoir où aller tester...
- Windows
  - Relation de confiance entre domaines
  - Le compte test d'un domaine contamine l'autre...

Serveurs de bases de données

- Trop verbeux
  - Listage des bases Oracle
- Avec des mots de passe évidents
  - Oracle : system/manager, sys/changeoninstall
  - MSSQL : admin/admin
  - MySQL : root/
- Si accès administrateur alors dump des bases d'utilisateurs et cassage avec john (+jumbo)
  - Sinon dump des droits des tables => liste de logins
- « schémas » : noms de bases, utilisateurs et mots de passe basés sur le nom du serveur

Serveurs DNS trop verbeux pour les domaines internes

- Accès à toutes les zones par transferts
  - IP -> machines
  - Machines -> IP
  - Avec les sous-zones
    - Par responsabilité
    - Par département : R&D, comptabilité...
- Permet de trouver rapidement les cibles les plus intéressantes

Partages de fichiers

- Partages sans restrictions :
  - NFS : restreint seulement par IP et par défaut pour root
    - Si je suis root sur le client alors je peux avoir l'identité que je souhaite sur le serveur...
- FTP anonyme : normalement « chrooté »
  - Attention également aux uploads...
- Et sur les « imprimantes/fax/photocopieurs » ?
  - Données en cours d'impression, de scan, d'envoi par fax/mail...
  - Données temporaires non effacées
  - Quid de l'effacement contre l'accès direct au disque ?
  - De plus en plus de systèmes Windows/Solaris non à jour et non sécurisés

Protocoles d'administration

- SNMP
  - Accès en lecture (public) = confidentialité
  - Accès en écriture (private) = administration
  - MIB propriétaires, mais publiques...
- telnet, rsh, ssh, HTTP
  - Voir toutes les listes publiques de login et mots de passe par défaut pour chaque matériel
- Logiciels propriétaires
  - Téléchargeables librement sur le site de l'éditeur
  - Puis à utiliser avec les mots de passe par défaut
- Notamment sur les routeurs, switches...

Serveurs à l'abandon et serveurs de val. & de dév.

- Avec des données « obsolètes » ou de « test »
- Mais avec :
  - Du durcissement système et applicatif non effectué
    - Dont des patches de sécurité non passés
  - Des mots de passe évidents
    - Dont les comptes de validation ou de développement
- Cause : serveurs non stratégiques
  - Mais les serveurs de production peuvent avoir gardé les comptes de validation ou de développement
    - Ou ne pas avoir été mis à jour...
  - Les anciens serveurs peuvent avoir des données toujours partiellement valides

Failles historiques

- tftp : get /etc/passwd
- rsh/telnet : -l -froot

Routeur VPN d'une agence distante

- Utilisé comme switch et routeur Internet
- SNMP RO & RW ouverts sur Internet
  - Lecture et écriture de la MIB standard, par exemples :
    - Version du firmware : présence d'une faille connue
    - Statistiques d'utilisation des interfaces
    - Désactivation des interfaces
  - Présence d'une MIB propriétaire
    - Serveurs DNS => modifiés pour interroger notre serveur
      - Analyse des requêtes effectuées durant une journée : journaux bind
      - Mise en place de traduction d'adresse, d'un relais inverse et d'un tcpdump
        - flux pop3, smtp, web : mots de passe en clair
        - flux HTTPS (avec la clé privée du relais inverse): copie mail via webmail
- Cause : les utilisateurs n'identifient pas les serveurs

Serveur BlackBerry

- Mot de passe par défaut pour le compte admin de la base MSSQL
  - Accès à toutes les tables
- Et fonction xp_cmdshell activée
  - Création d'un utilisateur, mis dans le groupe admins
  - Montage des partages administratifs (SMB)
  - Scans des arborescences...
  - Et récupération de données très sensibles dans TEMP
    - Fichiers temporaires non effacés : +ieurs Go en qlqs années
- Cause : non durcissement du serveur MSSQL

ITrust

« Photocopieurs »

- Partages FTP, SMB et NFS présents...
  - En plus de tous les services d'un Solaris par défaut...
- Montage du partage NFS non restreint
  - Scans des arborescences...
  - Et récupération de données très sensibles
    - Fichiers temporaires non effacés : +ieurs Go en quelques semaines
- Cause : serveur à part entière, mais non sécurisé

Vos questions ?

- Merci de votre attention

Intégrité – Excellence – Innovation - Confidentialité