Une journée d'audit ordinaire

Céline et Laurent Estieux
SGDN/DCSSI/Bureau Inspections en SSI

SSTIC, 3 juin 2005

Plan de l'exposé

Réunion de préparation

Objectifs :

- bien cerner les origines de la demande d'audit ;
- définir le périmètre ;
- définir les actions à mener ;
- identifier les points de contact ;
- proposer un planning.

Tests d'intrusion externes

- Interaction avec le client :
  - identifier la cible ;
  - point de contact pour la prestation.
- Résultats :
  - souvent peu probants via une attaque directe ;
  - $\Rightarrow$ utilisation d'un cheval de Troie avec l'accord de l'audité ;
  - réalisation d'un premier bilan avec le client.

Audit dans les locaux

- prise en compte de la sécurité physique ;
- réalisation d'entretiens ;
- réalisation de relevés techniques voire de tests d'intrusion internes.

Sécurité physique

- accès au bâtiment ;
- accès à la salle serveur, aux locaux techniques ;
- sécurité incendie, dégâts des eaux, . . . ;
- restauration (sauvegardes, procédures, . . .).

Déroulement des entretiens

- rencontre de plusieurs personnes à différents niveaux (stratégique, pilotage et technique) ;
- différents sujets abordés :
  - stratégie de SSI (PSSI, SDSSI, organisation, ...)
  - administration quotidienne axée SSI (gestion comptes, mots de passe, mises à jour, . . .)
  - paramétrages techniques (règles de pare-feu, fichiers de configuration de serveurs, . . .)

Tests d'intrusions internes

- définition du périmètre ;
- objectif :
  - sensibilisation forte des équipes,
  - $\Rightarrow$ devenir administrateur de domaine/root le plus rapidement possible, accéder à des données (dépend de l'objectif).

Conclusion

- les vulnérabilités les plus récurrentes sont présentes dans les actes,
- l'expérience de l'auditeur apprend vite à ne pas se fier aux apparences. . .

Coordonnées

Céline et Laurent Estieux

- SGDN/DCSSI/SDO/Bureau Inspections en SSI
- celine.estieux@sgdn.pm.gouv.fr
- laurent.estieux@sgdn.pm.gouv.fr