Challenge-SecuriTech 2004

Concours de sécurité - Retour d'expérience

Pierre BETOUIN <betouin@challenge-securitech.com>

ESIEA

Présentation et cadre du projet

- *ESIEA* : École supérieure d'informatique, d'électronique et d'automatique
- Les *TPFH* : TP de formation humaine
- Contraintes scolaires & organisationnelles
- Seconde édition du challenge
- Moyennement accueilli au début… et finalement très bien à la fin !

Équipe

- 7 étudiants de 3e année
  - Tâches spécifiques au sein du groupe
  - Domaines très variés et souvent peu connus
  - Organisation parfois complexe
- Suiveur de projet *ESIEA* (S. Duval)
- Intervenants extérieurs
  - N. Brulez - *Armadillo*
  - K. Kortchinsky - *CERT Renater*
  - R. Erra - *ESIEA*

Organisation

- Plusieurs *mailing-lists*
- *FTP* commun
- Différents scripts (*PHP*) de monitoring: stats, inscriptions, etc.
- Réunions régulières
- Comptes-rendus d'avancement pour l'*ESIEA*

Sponsors


club
internet


MISC


www.miscMAG.com
Multi-System & Internet Security Cookbook
Le site web de M.I.S.C. le mag de la sécurité informatique !


T'nB
INTELLIGENT
ACCESSORIES


Renater


SecuObs.com
L'observatoire de la sécurité internet


LE FIGARO
étudiant
www.lefigaro.fr/etudiant

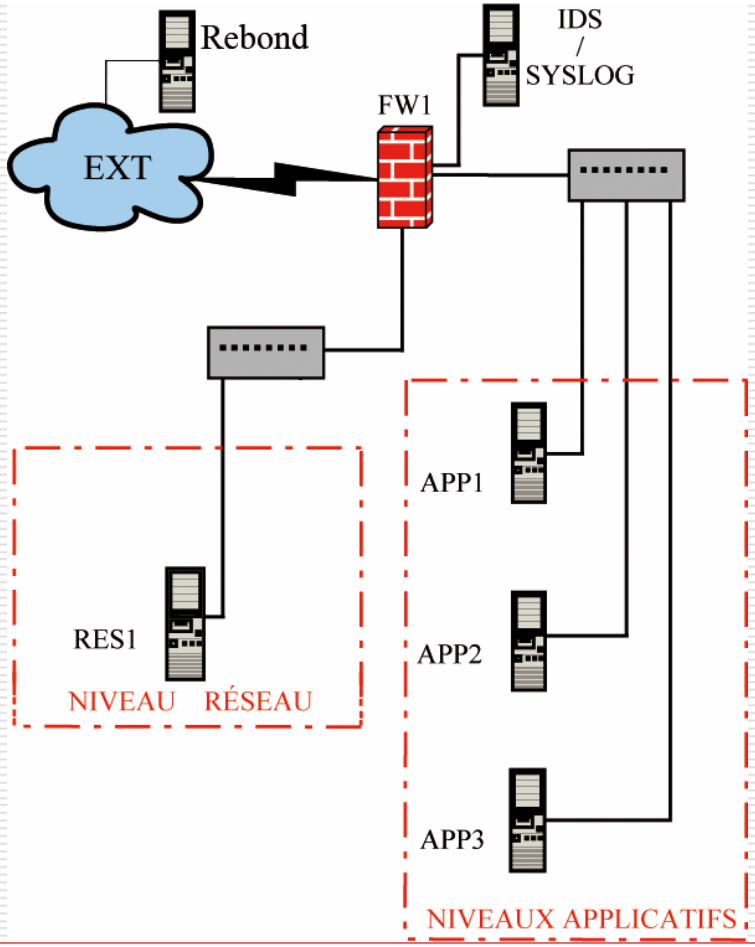

PRESENCE PC

Matériel et logistique

- Moyens modestes : 6 machines dédiées de 350MHz à 1,8GHz, *RAM* < 512MO
- Distributions *Mandrake* et *Debian* très différentes des versions initiales
- 1 machine virtuelle *Windows* (*VMWare*)
- Scripts de déploiement (Kernel, GrSec, Firewall, etc.)
- Moyens personnels et prêts des sponsors

Architecture réseau

Machines hébergées
chez *Club-Internet*



Spécifications réseau

- Ligne mise à disposition par *Club-internet*
- Bande passante de 70Mb/sec
- Salle blanche de *CI* : la garantie d'une meilleure disponibilité
- Matériel fiable (*CISCO*, onduleurs…)
- Disponibilité des personnes sur place (équipes d'astreintes)

Sécurité des serveurs

- Contraintes de sécurité au niveau de *CI* et de l'hébergeur *Amen*
- Risques de *DoS* vers l'extérieur importants en raison de la *BP*
- Machines Linux avec patches *grsecurity*
- Services chrootés (avec renforcements *grsec*)
- Difficultés pour sécuriser une machine faillible (niveaux du concours)

Monitoring

- Monitoring à distance via une machine de rebond (plage IP différente et lointaine)
- Trafic très important
- Serveur *syslog (UDP)* en cas de compromission d'une machine
- Enregistrement de l'intégralité des paquets avec *tcpdump*
- Plusieurs scripts de maintenance réguliers (compression, etc.)
- *IDS Snort* : très (trop) bavard !
- Monitoring double par *Club-internet*
- Analyse détaillée des *logs* prévue rapidement (environ 20GO compressés)

Épreuves du concours 2004…

- Nouveauté : 3 intervenants extérieurs
- Large panel de niveaux : cryptographie, stéganographie, reverse, failles applicatives, failles Web, réseau, etc.
- Calibrage de la difficulté et du temps
- Méthodes de conception des niveaux
- Quelques détails…

… En quelques chiffres

- Environ 2000 inscrits (*combien de participants effectifs ?*)
- 450 inscrits actifs (score > 0)
- Validations :
  - Niv. 5 Web le plus validé (302 pers.)
  - Niv. 3 Reverse le moins validé (2 pers.)
- Top 10 de haut niveau
- Nombreux participants motivés

Profils des participants

<u>En majorité :</u>

- Nombreux étudiants (universitaires, ingénieurs, BTS, IUT, etc.)
- Consultants
- Chercheurs
- Personnes intéressées par l'actualité du challenge (RSSI, etc.) sans les aspects techniques

Attaques constatées

- Nombreuses attaques « latérales » :
  - Une majorité de type Web
  - Tentatives d'évasions des *chroots*
- Nombreuses attaques sur le site officiel du challenge (hébergé)
- Activité générale impressionnante !

Le Bug *xinetd* en 2003 a laissé des traces dans les esprits…

Conférence de clôture

- Remise des prix
- Interventions en rapport avec des niveaux du concours
- Permet aux participants de se rencontrer et d'échanger leurs solutions
- Pot (ici encore : peu de moyens ☹)

Perspectives

- Reprise éventuelle par le mastère *SIS* (sécurité de l'information et des systèmes) de l'*ESIEA*.
  - Projet tenu par les étudiants
  - Reprise des bases existantes
- Améliorations importantes :
  - Système de points
  - Plus de personnes sur les aspects techniques

Les insolites… sans succès ! ☺

- *Bruteforce* du routeur via un *shellcode*
- *Bruteforce* du serveur *MySQL* via une injection
- *Bruteforce* d'un *MD5* de validation !
- *Shellcodes* très exotiques…
- Résolution des niveaux de cryptographie uniquement avec Excel!

Questions ?

Adresses utiles :

http://www.challenge-securitech.com
Site du concours

http://www.esiea.fr
Site de l'école *ESIEA*

http://www.secuobs.com
Plusieurs dossiers sur *SecuriTech*

staff@challenge-securitech.com
Contact mail