EADS

PacSec 2007
Compte-rendu

Nicolas RUFF / EADS-IW SE/CS

nicolas.ruff [à] eads.net

Généralités sur PacSec'07

- Même organisation que les conférences CanSecWest et EuSec
- 5ème édition en 2007
- 29 et 30 novembre 2007 à Tokyo
- http://pacsec.jp/

Conférences (jour 1)

- Cyber Attacks Against Japan - Hiroshi Kawaguchi, LAC
  - Retour d'expérience sur l'activité du Japan Security Operation Center (JSOC)
  - 700 sondes (commerciales) déployées chez 300 clients
  - Résultats conformes aux analyses générales
  - Faits marquants pour 2007 :
    - Botnets
    - Sites Web malveillants (légitimes ou non)
    - Exploitation de failles clients
    - Criminalisation des activités
    - 90% des attaques viennent de la Chine

Conférences (jour 1)

- Deploying and operating a Global Distributed Honeynet - David Watson, Honeynet Project
  - Initiative du « UK HoneyNet Project »
  - Distribution d'un DVD bootable
    - Base Fedora Core 6
    - Honeypots « basse interaction » : outils du projet HoneyNet
    - Honeypots « moyenne interaction » : Nepenthes
    - Honeypots « haute interaction » : VMWare Server
    - Remontée automatique des incidents
    - Les participants ont accès aux données
  - Analyse de plusieurs cas d'intrusion
  - Travaux futurs : améliorer la finesse des analyses

Conférences (jour 1)

- Office 0days and the people who love them - Takumi Onodera, Microsoft
  - Démonstration (vidéo) d'intrusion grâce à une faille PowerPoint 2003 sur Windows XP SP2
    - Analyse très fine grâce aux outils ProcMon et ProcExp
  - Effet des contre-mesures
    - Fonction UAC de Windows Vista
    - Outil MOICE pour Office 2003
    - Compte non administrateur sous Windows XP
  - Sécurité du format XML « Office 2007 »

Conférences (jour 1)

- Windows Localization: Owning Asian Windows Versions - Kostya Kortchinsky, Immunity
  - Présentation de techniques de fiabilisation des codes d'exploitation
    - Conférence déjà jouée à BH Europe
  - Problèmes courants :
    - Niveau de Service Pack
    - Langue du système d'exploitation
  - Développement de plusieurs techniques de *fingerprinting* utilisant le même port que la vulnérabilité exploitée
  - Les techniques développées ont été intégrées à l'outil Immunity Canvas

Conférences (jour 1)

- Enter Sandman (why you should never go to sleep) - Nicolas Ruff & Matthieu Suiche, EADS
  - Analyse complète du fichier d'hibernation Windows
    - Fonction « mettre en veille prolongée »
    - Fichier « hiberfil.sys »
  - Exemples d'utilisation
    - Détection de *rootkit*
    - *Forensics* tout en mémoire
    - Récupération de données sensibles (ex. clés de chiffrement)
    - Injection de code

Conférences (jour 1)

- TOMOYO Linux: A Practical Method to Understand and Protect Your Own Linux Box - Toshiharu Harada, NTT DATA CORPORATION
  - *Mandatory Access Control* (MAC) pour Linux
  - Différences avec SELinux
    - Plus simple à configurer grâce à l'auto-apprentissage
    - Décisions basées sur l'enchainement des processus et non un label de fichier
    - Activable par processus et non globalement
  - http://tomoyo.sourceforge.jp/

Conférences (jour 1)

- Agent-oriented SQL Abuse - Fernando Russ & Diego Tiscornia, Core
  - Ajout d'un framework d'injection SQL dans le produit Core Impact
  - A rapprocher de l'annonce Web Beam/SPI Dynamics ?

Lightning Talks

- Effacer ses empreintes digitales pour échapper au contrôle de l'immigration Japonais
- Sécuriser les *mashups* avec des IFRAMEs (IBM)
- Comment auditer des logiciels (Core)
  - 70 bogues ont été trouvés en 10 ans lors des campagnes d'audit de cette société
- Cryptographie malicieuse (Core)
  - Et si un virus chiffrait tous les disques durs avec la clé publique de Microsoft ?
- Sécurité des mots de passe, 10 ans après
  - Rien n'a changé …

Conférences (jour 2)

- Fuzzing Frameworks, Fuzzing Languages!? - Stephen Ridley & Colin Delaney, McAfee
  - Nouvel outil de fuzzing
  - Avantages
    - Basé sur un langage de description (pas de programmation requise)
    - Simple à installer (pas de dépendances)
    - Simple à utiliser
    - Moteur en Python, extensible
  - http://ruxxer.org/

Conférences (jour 2)

- Developing Fuzzers with Peach - Michael Eddington, Leviathan Security
  - Le *fuzzer* Peach est sorti en version 2.0
  - Nouveautés
    - GUI intuitive
    - Fichier de description XML
    - Sources de corrélation externes (ex. WireShark)
    - *Roadmap* agressive
  - http://peachfuzz.sourceforge.net/

Conférences (jour 2)

- Programmed I/O accesses: a threat to virtual machine monitors? - Loic Duflot
  - Résultats d'une thèse
    - Contournement des sécurités logicielles par le matériel
  - Mécanismes exploités
    - SMM (2006)
    - Table AGP/GART
    - Chipset USB/UHCI
  - Nécessite un accès à certains ports I/O
    - Mais l'accès physique au matériel n'est pas requis
  - Cas d'application
    - Modification du « securelevel » sous OpenBSD par l'utilisateur « root »
    - Evasion de VM

Conférences (jour 2)

- Automated JavaScript Deobfuscation - Alex Rice & Stephan Chenette, Websense Security Labs
  - Présentation de l'outil propriétaire « ThreatSeeker »
    - Catégorisation automatique de pages Web malicieuses
  - Deux étapes imbriquées
    - Dé-obfuscation JavaScript
    - Analyse comportementale
  - Détails d'implémentation intéressants
    - Il est nécessaire d'analyser toutes les étapes (et pas seulement la forme finale de la page)
  - Limites
    - La clé peut être récupérée dynamiquement (XMLHttpRequest())
  - Projet Open Source similaire
    - http://www.secureworks.com/research/tools/caffeinemonkey.html

Conférences (jour 2)

- Heap exploits are dead. Heap exploits remain dead. And we have killed them - Nicolas Waisman, Immunity
  - Les « heap overflow » ne sont plus exploitables de manière « traditionnelle » (Write4) sous Windows et Linux
  - De nouvelles techniques sont nécessaires
    - Récupération à distance du *layout* du tas
    - Contrôle de l'allocation
    - Ecrasement de données applicatives
  - Présentation de la gestion du « heap » sous Vista
  - Utilisation de l'outil « Immunity Debugger »
  - Un « heap overflow » fiable nécessite 3 semaines de travail sous Windows XP SP2, deux fois plus avec Vista

Conférences (jour 2)

- Bad Ideas: Using a JVM/CLR for Intellectual Property Protection - Marc Schoenefeld, University of Bamberg
  - Les protections logicielles sont inutiles dans les environnements « managés » (Java/.NET)
  - Plusieurs raisons
    - L'attaquant a le contrôle complet de la machine virtuelle
    - Le *bytecode* est facilement analysable/modifiable
  - Toutes les protections commerciales analysées ont été contournées

Extras

- Aspect social important
  - Un évènement tous les soirs grâce aux sponsors
- La communication Orient/Occident n'est pas facile
  - Langue
  - Culture
- Organisation de dernière minute
  - A nui aux formations (*dojos*) et aux inscriptions