HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Groupe OSSIR

Compte Rendu BlackHat/Defcon

Louis Nyffenegger
<Louis.Nyffenegger@hsc.fr>

Jérôme Poggi
<Jerome.Poggi@hsc.fr>

BlackHat : Introduction

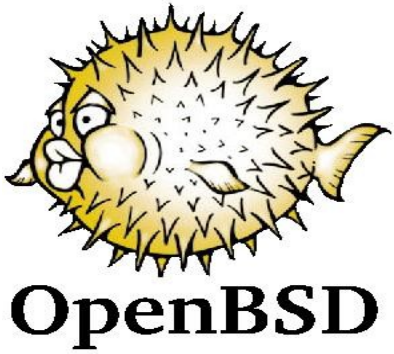
- Date :
  - Training : 28-29 et 30-31 juillet
  - Briefing : 1-2 août

- Casino Caesars Palace

- 8 conférences en parallèle dans les salles de bal du Caesars Palace

OpenBSD Remote Exploit

- Alfredo Ortega (Core Security)
- « Only **2** remote holes in the default install »
- 2 paquets ICMPv6
- Gestion de l'exploitation malgré toutes les protections OpenBSD
- Peut-être une 3ème vulnérabilité ...



"Hacking Intranet Websites from the outside"

- Jeremiah Grossman & Robert Hansen
- Rappels sur l'historique de ce type d'attaque
- Attaques CSRF/XSS :
  - vols d'historiques
  - scans réseau
  - CUPS hacking sur MacOSX (http://127.0.0.1:631/)
- Pas de grandes nouveautés...

Attacking Web Service Security...

- Brad Hill (iSEC Partners)
- Complexité et sécurité
- Multiples avantages de SSL
- Attaques sur XML Signature :
  - Sun Java JRE/JDK Processing of XSLT Stylesheets in XML Signatures Vulnerability
  - CVE-2007-3716

Tactical Exploitation (Part 2)

- HD Moore & Valsmith
- Première partie décevante :(
- Comment faire un TI interne sans utiliser d'exploits ?
- Attaque avec SMB/WPAD : MITM

"IsGameOver(), anyone ?"

- Joanna Rutkowska &

  Alexander Tereshkin

- Chargement de modules ?
  - l'an dernier : Page File attacks
  - utilisation d'un pilote vulnérable
    - (ATI ou NVIDIA)
  - Certificat à 250$
- Malware utilisant la virtualisation (Bluepill) ?
  - ils n'ont pas encore trouvé de solution pour parer à la méthode présentée à Syscan 2007 par Barbosa 2 semaines plus tôt.

Injecting RDS-TMC Traffic Information Signals

- Andrea Barisani & Daniele Bianco
- « Owning a car, priceless... »
- Montage simple : carte TV/ Démodulateur, PIC 16F84...
- Pas de chiffrement ni d'authentification des signaux
- L'antenne le **« sterilizer »**
- Attaque « Keep your parents from reaching home »
- Exemples de messages possibles :
  - Bull fight
  - Air raid
  - Bomb alert
- http://dev.inversepath.com/rds/

Blind Security Testing
An Evolutionary Approach

- Scott Tender
- Complexité de la recherche de vulnérabilités dans une application (trop de possibilités)
- Utilisation d'algorithmes évolutifs : sélection de la meilleure chaîne par vulnérabilité.
- Recherche de :
  - XSS
  - injections SQL
  - ...
- Récupération des messages d'erreurs (wapiti ?)
- Dommage, l'outil n'est pas encore développé

Fuzzing Sucks! (or Fuzz it Like you Mean it!)

- Pedram Amini & Aaron Portnoy
- Sulley : Framework d'écriture de Fuzzer
- Gestion de l'API VMware
- Gestion de suite d'événements : Fuzzer à états
- Développé en Python
- Interface Web

Oracle Forensic

- David Litchfield (NGS Software) et auteur du site http://www.databasesecurity.com
- Peu d'outils existent, voire aucun pour cette science
  - Oracle très souvent ciblé, très souvent vulnérable
  - Oracle très rarement mis à jour en production
    - Problèmes de contraintes, de régressions ...
    - Très souvent vulnérables
- Nécessité de connaître la structure des
  - Fichier des bases de données, des journaux, zones mémoires ...
- F.E.D.S.(Forensic Examiners Database Scalpel)
  - un outil d'aide à la recherche d'information après incident.

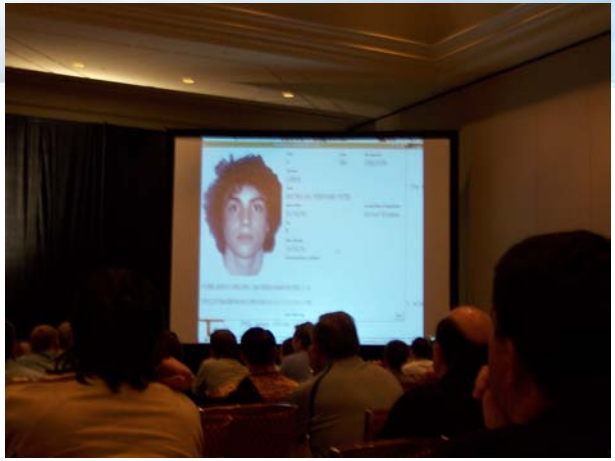
MS-SQL Forensic

- Kevvie Fowler, d'Emergis
- Même constat que D. Litchfield :
  - Peu d'outils, structures de données compliquées, informations répartie
  - Journaux multiples, beaucoup d'informations en mémoire ...
- Nécessité d'obtenir une copie de la mémoire du système
  - Avant interventions
- Analyse plus aisée en live
  - Possible avec la distribution HELIX

Black Out : What happened ?

- Jamie Butler et Kris Kendall, MANDIANT
- Détails important sur comment injecter du code sous Windows
  - Plusieurs méthodes, facile a faire, intégré dans Windows ...
  - Privilège « SE_DEBUG » très dangereux
- Nécessité d'avoir une DLL
  - Détection par le forensic
- Utilisation de Metasploit
  - Tout en mémoire
- Conférence assez technique, mais trop « blackhat » et commerciale

RFIDIOT



- Adam Laurie - http://rfidiot.org/
- Présentation peu changée depuis le début
- Toujours des démonstrations en direct
  - Les pays sont responsables de la sécurité de leurs passeports
    - Implémentation différentes pour chaque pays
    - Contenu des passeports différent
  - ID du RFID aléatoire
    - Australie jamais ^08
  - Clonage possible suivant les pays
    - Mais signé, donc pas modifiable
  - Données pouvant provoquer des débordement de pile/tampons ?
    - Réalisable, mais les données ne seront pas signées correctement
      - Autorité de certification vérifiée ? :-)

Breaking Forensics Software: Weaknesses in Critical Evidence Collection

- Chris Palmer, Tim Newsham, Alex Stamos, Chris Ridder
- Coup de pied dans la fourmilière !
  - SleuthKit et Encase victimes de débordement de pile/tampons et déni de service
  - Compromission du poste de l'enquêteur !
  - Dissimulation et/ou altération d'information
- Le produit EEE (Encase Enterprise Edition)
  - Ne garantit pas l'intégrité et l'identité du disque étudié à distance
    - Nécessité d'authentification manuelle et visuelle

Conclusion

- Beaucoup de conférences en même temps
  - Difficile de tout suivre
    - Même à deux
- Sujets peu nouveaux
  - Excepté quelques uns (heureusement)
- Conférence devenant trop commerciale
  - Beaucoup sont là pour vendre leurs produits plutôt qu'innover
- Contenu des présentations pas toujours à la hauteur avec le titre

Defcon : Introduction

- Hotel Riviera
- du 3 au 5 août 2007
- Moins commercial que BH
- Quelques conférences déjà présentes à Blackhat

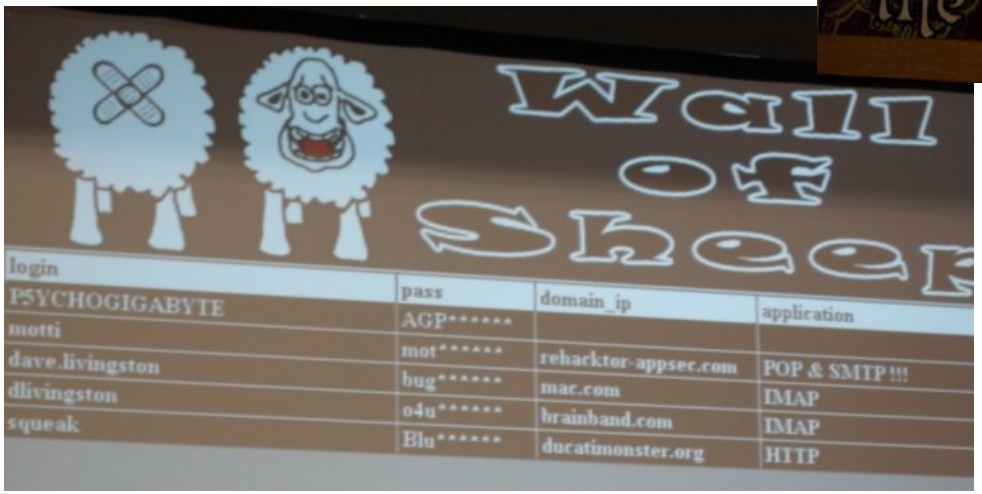
Defcon : Contests

- Lock-picking Contest

- Spot the Fed -> Spot the undercover

- Capture The Flag (une équipe française)

- Guitar Hero II Contest



- Defcon bots

Defcon : la boutique

- Tee-shirts, stickers ...
- Vente de matériels informatique
  - Historique
  - Actuel
- Kit de lockpicking, sniffer USB et PS/2
- Matériel Wi-Fi
- Livres ...

SQL injection and out-of-band channeling

- Patrick Karisson

- Cas de l'injection SQL aveugle.

- Envoi des données par d'autres tunnels :
  - HTTP : peu probable
  - TCP : encore moins probable
  - DNS : quasiment toujours vrai

- Démonstration sur Oracle/Récupération de table

When Tapes Go Missing

- Robert Stoudt
- Aux US, la perte de données est soumise à déclaration obligatoire
- Besoins étendus
  - Structure de données différente,
  - Structure de base différente,
  - Nécessite un équipement très hétérogène
- Très peu d'outils pour récupérer des données
  - TAPECAT : http://freshmeat.net/projects/tapecat/
  - ADSMTAPE pour TSM : http://sourceforge.net/projects/adsmtape
  - DD non utilisable, du fait des données après un EOD (End Of Data)

How smart is Intelligent fuzzing or how stupid is dump fuzzing

- Charlie Miller
- Rappels sur ce qu'est le « *Fuzzing* »
- Le fuzzing sans intelligence :
  - Simple, rapide, pas besoin d'intelligence, ni de connaissance
- Le fuzzing intelligent :
  - Départ de la RFC, et fuzzing à tous les niveaux
  - Ajout d'analyse statistique pour améliorer le nombre de réussites
- Exemple donné avec libpng
  - Le « dump fuzzing » trouve moins de cas que le « smart fuzzing »
  - Beaucoup plus de code généré, pour un résultat moindre

Interstate : A stateful protocol fuzzer for SIP

- Ian G. Harris

- Protos et Snooze n'ont pas été testés
- L'UAS (User Agent Server) de Interstate a été testé
  - Permet de tester les téléphones
  - Utilise un automate a état pour ne pas le suivre
  - Seulement 2 téléphones ont été testés
    - Aucun nom n'a été donné

One token to rule them all

- Luke Jennings

- Peu de recherche sur les tokens Microsoft
  - Possibilité d'imposture / imitation
  - Les tokens sont encore disponible même après « logoff »
- Utilisation de « Incognito » pour faire de l'imposture / imitation
  - Disponible sur :
    - https://www.defcon.org/images/defcon-15/dc15-presentations/Jennings/Extras.zip

No-Tech Hacking

- Johnny Long – http://johnny.ihackstuff.com/

- Même conférence qu'à BlackHat
- Une des conférences les plus plébiscitées
  - Salle comble, normes de sécurité largement dépassées...
  - http://johnny.ihackstuff.com/
- Conférence intéressante et ludique

Pentesting Wi-Fi

- Aaron Peterson

- Présentation de Wi-Crawl :
  - Outils d'intrusion automatique de réseaux sans fil
    - Paquet tout en un
    - Fournit tous les outils nécessaires
    - Permet d'automatiser tout le processus :
      - Découverte
      - Cassage WEP/WPA
      - Connexion
  - http://midnightresearch.com/projects/wicrawl/

Creating Unreliable Systems, Attacking the Systems that Attack You

- Sysmin et Marklar

- Utilisation de TOR
- Recherche google anonyme
- « Qui je suis ? » vs « Ce que je suis ? »
- Comment corriger une erreur ?
- Statistiques sur les mots recherchés par pays (« Sheep sex »)

- False life project : http://falselife.hackerpimps.com/

Hacking your Access Control Reader

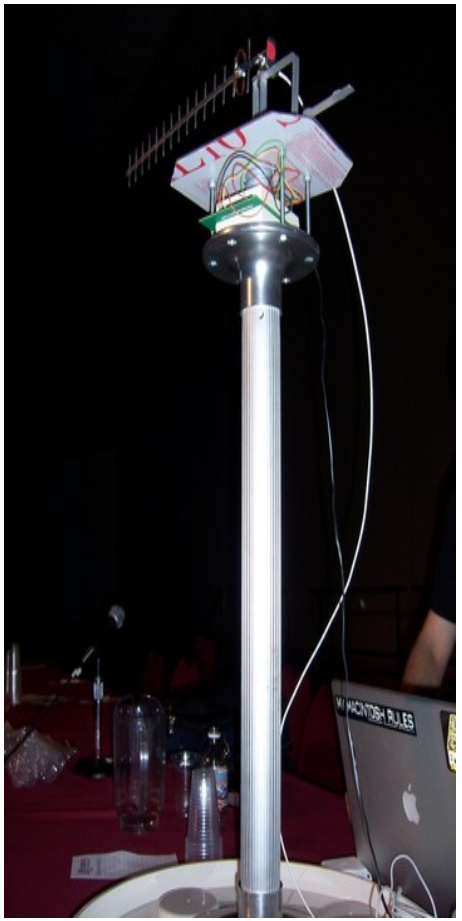
- Zac Franken
- Détails, avantages et inconvénients des contrôles d'accès
- Rappel que le plus gros problème est la révocation d'un accès
- Création d'un « dongle » pour lecteur de contrôle d'accès
  - Démonstration impressionnante pour un prototype
  - Une carte pour :
    - Rejouer une identification
    - Enregistrer une identification
    - Activer / Désactiver le contrôle d'accès
  - Les futures évolutions :
    - lecture par led, carte binaire, bluetooth, gsm ...

GeoLocation of Wireless Access Points and "Wireless GeoCaching"

- Ricky Hill

- Géolocalisation de points d'accès Wifi

- Fonctionnement :
  - Une équipe cache un AP
  - Balade en bateau pour le géolocaliser
  - Si l'autre équipe le trouve, ils ont gagné



The Emperor Has No Cloak - WEP Cloaking Exposed

- Vivek Ramachandran
- Wep Cloaking : envoi de données pour biaiser les outils de cassage de clé.
- Plusieurs techniques :
  - Envoi de faux IVs faibles
  - Envoi de trames de taille fixe
  - Envoi de trames de taille variable
  - ...
- Toutes les techniques actuelles sont facilement cassables à l'aide d'un pré-filtrage sur les paquets

High insecurity : Locks, lies and Liability

- Marc Tobias et Matt fiddler

- Dénonciation des constructeurs de serrures
  - Pas assez sérieux
  - Sécurité par l'obscurité
  - Utilisation d'oeillères
  - Utilisation de vielles techniques, peu d'innovations réelles
- Très critique sur les constructeurs
  - Exemple de « bumping » d'une Medeco M3 par une jeune fille de 12 ans
- http://www.security.org/ Et http://in.security.org/

Questions ?

Références et divers

- Google video, Youtube
  - LayerOne 2007
  - DefCon 15
  - BlackHat 2007

Slides disponibles sur
http://www.hsc.fr/

- http://www.blackhat.com/html/bh-multimedia-archives-index.html
- https://www.defcon.org/html/links/defcon-media-archives.html