BlackHat USA 2006 (+defcon)

Las Vegas – August 2-3, 2006

Compte rendu

Olivier Dembour, HSC

Guillaume Lehembre, HSC

Franck Veysset, France Télécom R&D

Plan

- BlackHat & Defcon
- Faits marquants

- Détail de quelques conf. choisies

BH06 – Defcon 14

- 10 ans pour BH06
  - Première conférence depuis rachat CMP
  - 3500 personnes (briefing), 15% d'étrangers, 2 jours
  - Autour de 100 conférences, 7 tracks en //
  - CISCO, Microsoft et E&Y sponsors platines…
- 14 ans pour Defcon
  - Nouvel hôtel…
  - >7000 personnes, 3 jours de conférence
  - Autour de 80 conférences, 3 tracks en //

Ambiances…

- Pro du coté de BH
  - Plus de $1300 l'inscription
  - Salon en // : cette année, tendance SIM, NAC et AVA…
- Du coté de Defcon
  - + underground
  - Nombreuses activités annexes…


BIG
BROTHER
Sprite

Black Hat Briefings

« Faits marquants 06 »

- Virtualisation Hardware et rootkit
- Attaques sur Drivers WiFi
- Contournement des équipements de sécurité (la mort des IPS/IDS ?)
- RFid…
- Encore du BlackBerry…
- Du fuzzing…
- Et Vista…

Quelques conférences…

- Device Drivers, Johnny Cache et David Maynor
- Subverting Vista Kernel For Fun And Profit, Joanna Rutkowska
- Hardware Virtualization Based Rootkits, Dino Dai Zovi
- Metasploit 3, HD Moore

Autres conférences

- Bypassing Network Access Control, Ofir Arkin
- SIP Stack fingerprinting, Hendrik Scholz
- Analysing complex systems, the BB case, FX
- Thermoptic camoulfage, HD Moore et Brian Caswell
- Nombreuses sessions Microsoft (VISTA)
  - Intro par Andrew Cushman

Du coté de Defcon

- Lockpicking, safepicking (comme d'hab…)
- Carte magnétiques
- Jericho Forum et perimetrisation
- IPv6 (limite du 30/6/08)
- Analyse de trafic et menaces sur *Privacy*
- Failles sur Windows mobile
- DNS amplification
- Phishing…

Empreinte des piles SIP (Hendrik Scholz)

- Le standard SIP
  - Nombreuses RFC
  - Nombreuses extensions
- Les implémentations réagissent différemment :
  - Entêtes (Accept, Max Forward ...)
  - Ordre des entêtes
  - Affichage du nom
  - Présence de parenthèse
  - Génération des "Call-id", "Cseq"

Empreinte des piles SIP

- Une empreinte unique
  - Système
  - Version de logiciel, du firmware
- Analyse des aléas des solutions :
  - Sipsak : bon aléa
  - Sipp : linéaire
  - Opal : Identification basée sur la MAC
  - Iswitch : adresse MAC en clair dans le call ID
  - Newport SBC : Détermination du nombre d'appels passés
- Découverte d'un 0day Cisco !

Vulnérabilité des pilotes Wifi (johnny Cache & David Maynor)

- Le protocoles 802.11 est complexe
  - Parties ambiguës
  - Libre choix de certaines réactions

  -> possibilité de prise d'empreinte
- L'implémentation semble assez anarchique
  - Nintendo ne respecte pas grand chose ... mais marche
  - Personne n'implémente de RTS/CTS

Vulnérabilité des pilotes Wifi

- Nombreuses possibilités d'empreintes
- Association redirection
  - Ignorer la réponse
  - S'associe sur la nouvelle BSSID
  - S'associe sur l'ancienne BSSID
  - Désassociation
- Durée d'émission (champ duration)
  - Dépend du débit
  - Dépend de l'état (association, data ..)

Attaques des systèmes RFID (Lukas Grunwald)

- Les puces les plus utilisée (MIFARE)
  - Pas de documentation publiques (NDA)
  - Les version Pro, sont compatibles ISO 14443-4
  - Secteurs protégés par clés
  - Brute force possible mais impensable (espace de clés = 2^6^8)
  - Test d'une clé en 25ms (driver spécifique)

Attaques des systèmes RFID

- Recherche d'information ... sur google
  - Informations extraites par un strings d'une application
  - Recherche sur google avec ces identifiants
  - Documentations, exemples
  - Découverte de clés par défaut, clés d'exemple
- -> La majorité des implémentations utilisent les clés par défaut ou les clés d'exemples

Attaques des systèmes RFID

- Analyse des passeport biométriques
  - Format MRTD (Machine Readable Travel Document)
  - Défini par l'ICAO (International Civil Aviation Organization)
  - Identifiant (UID) de chaque puce unique (pas requis par l'ICAO)
  - Vérification numérique de la signature
  - Mais pas de CRL ...

Attaques des systèmes RFID

- Contenu des passeports dépendant de l'accès
- En accès basique
  - Identité, photo, âge
- En accès étendu
  - Données biométrique
  - Pas de standard
- Démonstration de la modification du passeport
  - La signature était sûrement invalide ....

L'insécurité d'Ajax (Billy Hoffman)

- Ajax = Asynchronous JavaScript And XML
  - Utilisation conjointe de technologies
- La problématique serveur d'Ajax
  - Pas de différentiation d'une navigation "manuelle"
  - Pas d'entêtes particulière
- La problématique client d'Ajax
  - Requêtes invisibles
  - Attaques XSS plus évoluées(scanner TCP)

L'insécurité d'Ajax

- Utilisation de bridge (mashup)
  - API serveur de liaison avec d'autres sites
  - Permet l'interaction avec une partie tierce
  - Exemple : housingmaps.com
  - Attaques plus complexe pour les serveurs

Analyse de Blackberry (FX)

- Pour où commencer l'analyse de blackberry ?
  - Téléphone
  - Réseau GSM
  - Réseau RIM (inconnu), protocoles (inconnu)
  - Serveurs Blackberry (protocole inconnu sur IP)
- Choix Impact / Coût / Légalité
  - Serveurs Blackberry situés dans le LAN
- Analyse du protocole
  - Certains messages chiffrés

Analyse du blackberry

- Protocole
  - Bon chiffrement, quand utilisé
  - Possibilité d'envoi de message à tous (PIN)
- Architecture
  - SQL server (SA/NULL) contenant les clés de chiffrement
  - Codé en C++ (code propre ?, nombreuse vérifications)
  - Utilisations de nombreuses librairies (office, HTML, XML)
  - Vielles librairies (Graphics Magic 1.1.3, zlib 1.2.1)
- Bilan : Séparer les composants (DMZ)

La sécurité dans Vista (Joanna Rutkowska)

- Signature des pilotes obligatoire sous Vista
- Possibilité de contournement de la protection :
  - Utiliser (presque) toute la mémoire
  - Le système se met à paginer les processus et les pilotes
  - Le pilote est modifié directement dans le pagefile
  - La mémoire est libérée, le pilote est rechargé avec une fonction modifiée

La sécurité dans Vista

- Principe d'un rookit indétectable (Blue pill)
  - Utilisation des fonctionnalités des processeurs AMD
  - Création d'une machine virtuelle
  - Système d'exploitation déplacé dans celle-ci (par le malware)
  - L'hôte n'est pas visible, donc cheval de troie indétectable
  - Pas spécifique à Microsoft !

Rootkit & virtualisation

- Harware Virtualization rootkits, Dino Dai Zovi
  - Présentation semblable à « BluePill »
- Utilisation de processeurs Intel
  - Techno VT « Vanderpool »
  - Cette fois, sur Apple OS-X
  - Rootkit « Vitriol »

Metasploit 3

- Compression de 40% avec l'utilisation de Ruby
- Multi-tâche; suspension et résumé de session
- Mixins : écritures d'exploits simplifié (HTTP, RPC, FTP, SMB ...)
- Evasion plus poussée, module anti-IPS !
- Meterpreter amélioré
  - bloque souris, clavier
  - Migration des processus

Vulnérabilités RSS (Robert Auger)

- Danger des flux RSS ou Atom malveillants à cause des injections de code utilisateurs possibles (Javascript)
- Les XSS et CSRF deviennent utiles ...
- Mauvais filtrage des Javascript ouvrant des possibilités de :
  - scan du réseau interne (Cf présentation J. Grossman)
  - capture des frappes clavier
  - vols d'informations dans le contexte du site accédé

Breaking Crypto (Chris Eng)

- Analyse des données chiffrées / encodés dans les applications Web (Cookies, etc.) afin de les compromettre sans connaître la clé ou l'algorithme utilisé
- Deux points clés pour y arriver :
  - la structuration des données (longueur fixe, séparateurs)
  - observation attentive (entropie, répétition des blocs chiffrés, longueur caractéristique, début de bloc caractéristique, corrélation des sorties en fonction des données entrées)

Breaking Crypto

- Quelques recommandations :
  - Utiliser un chiffrement par bloc en mode CBC (et non ECB)
  - Corréler des données du cookie avec celle de l'utilisateur au niveau du serveur
  - Ne pas réutiliser de suite chiffrante (« *keystream* »)
  - Utiliser des fonctions d'intégrité indexées par des clés (type HMAC)
  - Ne pas chercher à faire de la sécurité par l'obscurité

Thermoptic Camouflage (H.D Moore & Brian Caswell)

- Présentation de multiples méthodes d'évasion IDS / IPS et en particulier sur les protocoles complexes DCERPC, SMB
- La fragmentation est toujours un problème ... surtout quand elle est faite à de multiples niveaux : IP, TCP, SMB, DCERPC (en même temps ! = Game Over !)
- L'encodage des caractères est une vrai plaie
  - ex : 125 manières d'encoder un 'A' en UTF-8 !

Thermoptic Camouflage

- Les vendeurs d'IDS / IPS commerciaux ne prennent pas tous le soin de chiffrer leur base de signature ... et ça facilite grandement la tâche pour les évasions !
- Le chiffrement des transmissions reste encore la meilleure méthode pour évader les sondes
- Quid d'un WMF dans un flux transmis par un relai applicatif HTTPS (fsurf.com ou proxify.com) ?

Le Wi-Fi dans Vista

- Nouvelle pile pour le Wi-Fi dans Vista
- Microsoft s'est (enfin) décidé à corriger les failles relatives au Wi-Fi dans Win2K et WinXP:
  - « Probe Request » émies uniquement pour les réseaux cachés et plus sur tous les SSID des « réseaux favoris »
  - Plus de fuite mémoire dans les SSID des Probe Request sous WinXP
  - Plus d'association à des réseaux ayant le même SSID mais un niveau de sécurité différents
  - Intégration automatique de filtres lors de l'association sur des connexions non authentifiées

Bypassing NAC

- Présentation de Ofir Arkin
  - Session « zero day! »
- En fait, intro sur les technos de NAC
- Et illustration de problèmes
  - Détection d'un « nouvel arrivant »
  - Gestion des exceptions
  - Contournement des mécanismes
  - Dangers de la zone de quarantaine
  - …
- Bonne intro sur le sujet

Panel « traffic analysis »

- Dirigé par le CTO de PGP (John Callas)
- Idée : après le chiffrement, il faut maintenant prendre en compte les risques liés à l’analyse de trafic
- Exemple : timing attaques sur SSH (obsolète)

- Débat intéressant…

Jericho Forum

- Keynote en 2004
- Panel Defcon en 2006
- Toujours le même thème : *mort aux firewall* ☺
  - 70% des attaques traversent les firewalls. (source : gartner)
- Idée : lancement d'un concours…
  - Résultats à BH07 / Defcon 07

Présentations « Françaises »

- Talks
  - Renaud Bidou, IPS Shortcomings
  - Nicolas Fischbach, Carrier VoIP Security
- Turbo talk
  - Franck Veysset , Wi-Fi Advanced Stealth

Questions ?