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

OSSIR
CR BlackHat / Defcon
Las Vegas – 3 au 7 août 2011

- Mardi 13 septembre 2011 -

Benjamin Arnault <Benjamin.Arnault@hsc.fr>
Renaud Dubourguais <Renaud.Dubourguais@hsc.fr>

Plan

- Présentation des conférences
- Faits marquants
- Résumé des conférences intéressantes

BlackHat

- 15ème édition de la conférence depuis 1997 !
- Las Vegas (Caesar Palace) du 30 juillet au 4 août 2011
- Droit d'entrée élevé ($1500 pour les 2j)
- Formations et conférences
  - ~50 sessions de formation de 2 ou 4 jours
  - ~90 conférences réparties dans 9 salles en simultané
- La plus grande conférence en sécurité
- Vendor Expo
  - Panel de sociétés de sécurité

Defcon

- 19ème édition depuis 1993 !
- Las Vegas (Rio) du 5 au 7 août 2011
- Droit d'entrée raisonnable
  - $150 pour 3 jours
- ~130 conférences sur 5 salles
- Conférence « Underground », moins que le CCC :)
- De nombreuses activités et challenges
  - CTF, Ingénierie sociale, cassage d'empreintes de mot de passe
  - Crochetage de serrures, jeu en réseau, inforensique réseau
  - Espace Kids, Open CTF, hacking hardware, challenge BDD
  - Pousse de barbe, glace alcoolisée, refroidissement de boisson

Faits marquants 2011

- SCADA
  - Siemens PLC, Prison, Hôpital, Compteur à eau
- Google Chrome OS
- Ordiphones
  - Android et iOS
- Inforensique
  - Mémoire, Discrète, Oracle, Timestomping
- Sophos Antivirus
- SAP J2EE

Exploiting Siemens Simatic S7 PLCs
Dillon Beresford

- PLC = Programmable Logic Controllers
  - Équipements de contrôle d'équipements industriels (SCADA)
- Étude de la sécurité des Simatic S7-300 et S7-1200
  - Utilisation du protocole ISO-TSAP pour l'administration
    - Transport des données en clair
    - Authentification (souvent non activée)
  - Approche
    - Écoute de la communication entre l'outil d'administration et le PLC
    - Analyse des données (Wireshark)
  - Découvertes
    - Identifiant, mot de passe, commandes
    - Si l'authentification est réussie alors le PLC active l'accès en lecture/écriture/exécution à sa mémoire

Exploiting Siemens Simatic S7 PLCs
Dillon Beresford

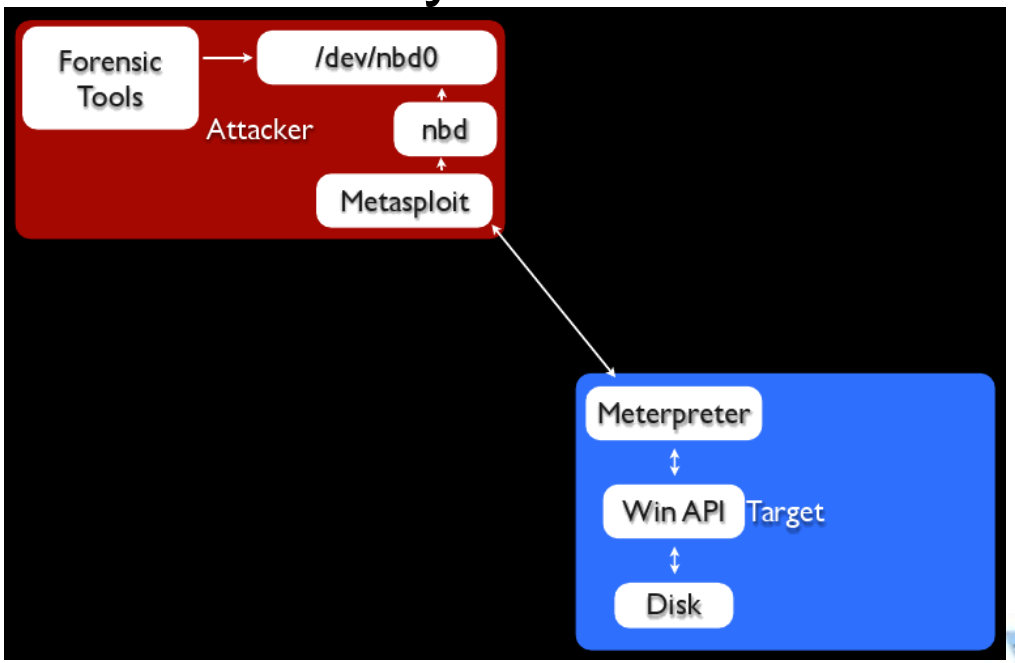
- Attaques
  - Rejeu TCP sur ISO-TSAP avec Metasploit
  - Contournement de l'authentification S7
    - Capture et rejeu de paquet d'authentification
    - Envoi de paquets forgés
    - Note : Aucune expiration de session et réutilisation possible sur un autre PLC
  - Arrêt et démarrage du CPU
    - Arrêt = PLC mis dans un état d'erreur perpétuelle (possible sans authentification)
  - Dump, lecture et écriture en mémoire
    - Modification de la configuration ou de la logique, récupération de fichier projet
  - Obtention d'une invite de commande sur le PLC
    - PLC = linux x86 + processus root !

Physical Memory for cache
Jaime Butler & Justin Murdock

- Étude inforensique = analyse des disques et de la mémoire
- Approche actuelle d'étude des processus en fonctionnement
  - Étude de la mémoire seule
- Nouvelle approche
  - En plus de la mémoire, analyser le cache
  - Pour reconstruire complétement les processus
  - Pour récupérer des clés de registre et des fichiers
- Faciliter le triage avec des listes blanches
  - Créer des empreintes MemD5 des processus de confiance
  - Exclure les processus reconnus et s'intéresser aux autres
  - Outil : Memoryze 2.0

Covert post-exploitation forensics w msf
Robert McGrew

- Objectif : réaliser une étude inforensique sans que le possesseur de l'équipement en soit averti
  - Dans le cadre d'un test d'intrusion
  - Lorsque la localisation physique de l'équipement est impossible
  - Pour espionner
- Modules meterpreter pour accéder au système de fichiers
  - Utilise Railgun
  - Permet de
    - Lister les FS
    - Réaliser une image
    - Monter le FS
  - iSCSI pour y accéder depuis Windows



What time are you anyway ?
Michael Robinson

- Timestomping = modification des temps MAC d'un fichier
- Outils classiques modifient les 4 temps (MACB) de $STANDARD_INFORMATION
- Ce n'est pas suffisant, des temps sont aussi présents ici :
  - $FILE_INFO (4)
  - Fichier de prefetch (1+8=9)
  - Fichier .lnk dans le dossier Recent (8)
  - Fichier .lnk dans le dossier Office Recent (8)
  - Clé de registre 'Recent' de l'application dans la ruche HK_USERS (?)
- Difficile de changer tous ces temps (33+) !
- Alors, comment faire ?
  - Modifier suffisamment de données pour passer inaperçu :)

Battery Firmware Hacking
Charlie Miller

- Smart Battery : permet l'interaction batterie <> OS et chargeur
  - lecture des t° et modification des paramètres de charge/décharge
- Équipent les ordinateurs portables Apple
- Démarche
  - Étude du Apple Battery Updater et du pilote associé
  - Découverte du matériel : puce Texas Instruments
  - Utiliser le module noyau AppleSmartBatteryManager pour écrire sur le bus SMBus (développement d'une API pour simplifier)
  - Beaucoup de valeurs accessibles en écriture
    - Mais les changer n'a pas modifié le comportement de la batterie
  - En réalité, il existe plusieurs modes de fonctionnement
    - Scellé, non scellé, accès complet, configuration et Boot ROM

Battery Firmware Hacking
Charlie Miller

- Démarche (suite)
  - Étude plus poussée avec un kit Texas Instruments
    - Découverte du fonctionnement (ingénierie inverse et écoute du SMBus)
- Attaques possibles
  - « Briquage » de la batterie
  - Retirer les protections et permettre l'explosion
  - Déni de service persistant sur l'OS
  - Porte dérobée persistante sur l'OS
  - Espionnage du TPM ou du BIOS

Hacking your victims over power lines
Dave Kennedy & Rob Simon

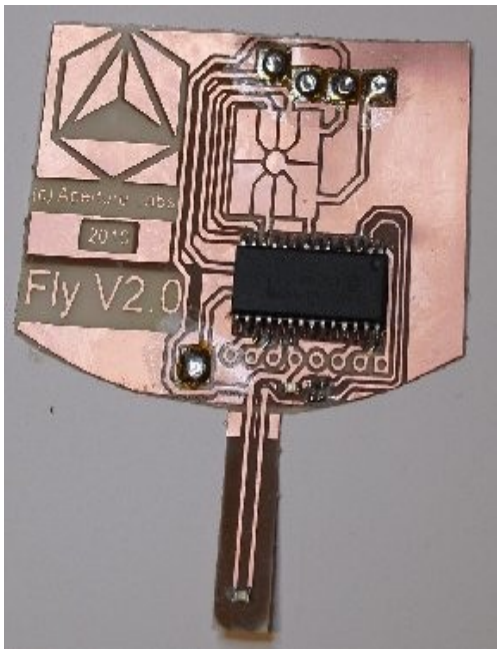
- Objectif : s'insérer dans un réseau domotique via le CPL
  - Connexion d'un dispositif sur une simple prise de courant
- Protocole X10
  - Protocole de communication sur courant porteur
  - Utilisé entre les différents systèmes
  - Chiffrement de la communication extrêmement rare
- X10 Black Out
  - Perturbe très fortement les communications au sein du réseau
  - Caméras, portes, systèmes de sécurité, etc.
- X10 Sniffer
  - Détection des systèmes connectés au réseau
  - Cartographie très précise des systèmes de sécurité d'un bâtiment

Chip & PIN are definitely broken
A. Barisani, A. Lauri, Z. Franken, D. Bianco

- État de l'art des attaques par « skimming »
  - Ajout de lecteur de bande magnétique : lecture de la carte
  - Ajout d'une caméra : récupération du code PIN
  - Dissimulés mais détectables

Chip & PIN are definitely broken
A. Barisani, A. Lauri, Z. Franken, D. Bianco

- Présentation d'une nouvelle attaque
  - Lecture directe de la puce par MITM entre le DAB et la carte
    - Insertion d'un dispositif dans le lecteur de carte → invisible
  - Par défaut, vérification du PIN de manière chiffrée
    - Défini par le standard EMV → liste CVM
    - Supporte aussi la transmission en clair
      - Le skimmer fournit une CVM ne contenant que cette méthode
      - Attaque par « CVM downgrade »
      - PIN circule en clair entre le DAB et la carte



iOS Kernel Exploitation
Stephan Esser

- Déboggage noyau
  - Pas d'API de déboggage dans la SDK iOS
  - Utilisation de KDP situé dans le noyau iOS
    - Doit être activé et ne peut être utilisé que via Ethernet ou port Série
    - Utilisation de l'outil redsn0w 0.9.8b4 (ou un noyau « personnalisé »)
  - Utilisation du iPhone Dock Connector
    - PIN 12 et 13 = Série
    - PIN 23, 25, 27 = USB
  - Construction d'un périphérique de déboggage (20 €) permettant :
    - Connexion SSH sur USB
    - Déboggage noyau via la ligne Série
  - Utilisation de GDB avec le support KDP

iOS Kernel Exploitation
Stephan Esser

- Exploitation noyaux
  - Présentation de 2 failles utilisées pour le Jailbreak
    - Dépassement de tampon dans la pile dans HFS Legacy Volume Name
      - Pod2g
      - IOS 4.2.1 – 4.2.8
    - Dépassement de tampon dans le tas dans ndrv_setspec()
      - Stephan Esser
      - IOS 4.3.1 – 4.3.3
  - Code d'exploitation en ROP

Cellular Privacy: A Forensic Analysis of Android Network Traffic Eric Fulton

- Beaucoup d'informations présentes sur un ordiphone
  - Conversations, historique des appels, messages, identifiants, mots de passe, localisation, clés privées ...
- « Evil apps are evil. Ok ! » Quid des autres ?
  - Zynga, Facebook, google.com
- Démarche
  - Mise en place d'une plateforme de test matérielle
  - Utilisation de wireshark et SSLstrip
- Résultats
  - Contact avec beaucoup de sites tiers
  - Envoi d'informations : opérateur, type de téléphone, version OS, langue, résolution d'écran, points d'accès Wi-Fi alentour, adresses IP, adresses MAC ...

Seven Ways to Hang Yourself with Google Android
Yekaterina Tsipenyuk O'Neil & Erika Chin

- Étude de mauvaises pratiques de développement Android
  - Sept erreurs
    - Spoofing d'intent (message)
      - Envoi d'intent implicite à un composant n'exigeant pas de privilège élevé
    - Injection de chaînes de caractères
      - Utilisation de données d'entrée non vérifiées pour une requête SQLite
    - Réception non autorisée d'intent
      - Interception d'intent par une application malfaisante
    - Messages persistants : sticky broadcasts
      - Messages envoyés à tout destinataire prévu, accessibles après envoi
    - Stockage non sécurisé sur carte SD
    - Communications non sécurisées (HTTP)
    - Applications disposant de privilèges élevés

Sophail : a critical analysis of Sophos AV
Tavis Ormandy

- Résultats
  - Méthode de détection basée sur des signatures statiques : faible
    - S'appuient sur CRC32
    - Souvent identifient du code mort ou non malveillant
  - Protection contre les débordements de tampon : faible ou inopérante
    - « A vouloir réinventer la roue, on ne la fait pas tout à fait ronde »
  - Protection contre les retours en libc : faible
    - Liste d'appels à surveiller, secrets mal protégés, utilisation de liste blanche
  - Chiffrement et offuscation avec SPMAA : faible
    - Chiffrement symétrique dont la clé est dans le produit
  - Analyse pré-exécution :
    - émulation x86 simpliste, packers anciens ou obsolètes (souvent inutiles sur les systèmes d'aujourd'hui)

A crushing blow at the heart of SAP J2EE Engine
Alexander Polyakov

- Interface d'administration web SAP
  - Obtention d'infos possible (version, noyau, utilisateur, journaux ...)
    - Modulo les mises à jour installées
  - Vulnérabilités déjà découvertes
    - XSS, CSRF, Relais SMB et accès direct aux servlets
  - Protocole SPML
    - Manipulation d'objets
    - Peut être utilisé au sein d'un XSS
  - Utilisation du Verb Tampering
    - Exécution de requêtes avec le verbe HEAD au lieu de GET
    - Permet le déni de service, la création d'un relais SMB ou d'un utilisateur
    - Deux requêtes suffisent pour prendre la main sur un serveur

Hacking and Securing DB2 LWU Databases
Alexander Kornbrust

- Trois versions majeures : 9.1, 9.5 et 9.7
- Vulnérabilités de la base
  - Unsecure Random, débordement de tas, divers dénis de service
  - Changement de propriétaire avec db2licm
- Fix Packs (correctifs de sécurité) fournis avec
  - Exemple de code exploitant la vulnérabilité
  - Bonne documentation (permettant de trouver d'autres vulnérabilités)
- Vulnérabilités du code
  - Injection SQL dans le code SQL/PL et PL/SQL (9.7)
- Accéder à l'OS depuis la base
  - Fichiers, réseau

Hacking and forensicating Oracle
David Litchfield

- Retour sur les techniques classiques d'exploitation Oracle
  - Injections SQL
  - Élévations de privilège (PL /SQL, Java, …)
- Oracle : facile à pirater mais inforensique difficile
  - Journaux très disparates
  - Formats différents et difficiles à exploiter
- Présentation de la suite inforensique Oracle : V3rity
  - Exploite et uniformise les journaux Oracle
  - Permet de filtrer et rechercher des événements
- Disponible que sous Windows pour Oracle 9i, 10g et 11g
  - http://www.v3rity.com/v3rity.php

Virtunoid: Breaking out of KVM
Nelson Elhage

- Présentation d'un code d'exploitation de la CVE-2011-1751
  - Vulnérabilité de type « use-after-free » dans l'émulateur PIIX4
  - Élévation de privilège : VM → machine hôte
  - Technique présentée « très » avancée
    - Détermination d'adresses de référence via le mécanisme d'allocation mémoire des VM
    - Pas de ROP : utilisation des routines internes de KVM pour enchaîner des appels à des fonctions arbitraires
      - « I'm not that good at ROP :) »
    - Utilisation de paquets ICMP pour réaliser un « heap spray »
  - Compilation d'un noyau Linux embarquant le code d'exploitation
    - Démarrage de la VM → Obtention d'un shell root sur l'hôte

ARM Exploitation ROPmap
Long Le & Thanh Nguyen

- Aucun outil de génération de charges utiles ROP pour ARM
- Implémentation d'une extension à RopeMe
  - Définition d'un méta-langage
  - Interprétation de ce méta-langage pour rechercher les gadgets
  - Construction d'une charge utile conforme au méta-langage
- Simplifie grandement l'exploitation en ROP sous ARM
  - L'attaquant n'a plus qu'à connaître le méta-langage
  - La charge utile est générée automatiquement

Attacking NoSQL and Node.js
Bryan Sullivan

- SSJS : Server-Side JavaScript
  - Serveurs web (Node.js)
  - Bases de données (MongoDB, CouchDB)
- Javascript n'apporte pas plus de sécurité
  - Exécution de code JS arbitraire (XSS)
  - Exécution de commandes système (Child Processes sous Node.js)
  - Récupération de fichiers arbitraires (File System sous Node.js)
- Vulnérabilités liées au JS maintenant côté serveur !
- Détour vers les bases NoSQL
  - Toutes aussi vulnérables à des injections (plus complexes à exploiter)
  - Peu de sécurité (services REST non authentifiés, etc.)

Hacking Google Chrome OS
Matt Johansen & Kyle Osborn

- Chrome OS = Navigateur web
- Possibilité d'installer des extensions
  - Demande de permissions à l'installation
  - Utilisables dans un ou plusieurs onglets
- Pas de cloisonnement entre les onglets
  - Fort impact en cas de XSS
  - Peu de contraintes pour les extensions malveillantes
  - Démonstration : récupération des mots de passe stockées dans LastPass

Aerial Cyber Apocalypse: If we can do it... they can too
Richard Perkins & Mike Tassey

- Idée : construire un drone et lui ajouter des outils d'intrusion
- Drone FMQ-117B modifié (moteur, trains et queue mobile)
- Embarque un PC
  - Backtrack 5, carte Wi-Fi, USRP, clé USB 4G ...
- Base de contrôle : ARM Cortex A8 et écran LCD
- Système de support : Pentium 4, GTX 470 et Backtrack 4
- Communication par openvpn
- Coût : $6,200
- Autonomie 1h

Aerial Cyber Apocalypse: If we can do it... they can too
Richard Perkins & Mike Tassey

Conclusion

- Conférences très intéressantes
  - Comme d'habitude,
    - Des conférences très intéressantes
    - Des outils publiés
    - Des sujets survolés
- Bonne ambiance
- Présentations, documents, enregistrements (audio et vidéo)
  - https://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html
  - https://www.defcon.org/html/links/dc-archives/dc-19-archive.html