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 – du 25 au 29 juillet 2012

Johann Broudin <Johann.Broudin@hsc.fr>
Thibaut Leveslin <Thibaut.Leveslin@hsc.fr>

BlackHat USA 2012

- 16e édition de BlackHat USA
- Briefings
  - 6500 participants
  - 2 jours (25 et 26 juillet)
  - 8 présentations en parallèle
  - Environ 80 conférences
- Hôtel du Caesar's Palace à Las Vegas

Defcon 20

- Possibilité de suivre plus de conférences qu'à BlackHat
  - 5 présentations en parallèle
  - > 110 conférences
- 4 jours (26 – 29 juillet)
- Hôtel Rio

- Beaucoup de participants (accès aux conférences parfois difficile)
- Des activités et stands
  - CTF (> 30 personnes pour l'équipe gagnante)
  - Challenges (inforensique réseau, badge Defcon)
  - Wall of Sheep, Spot the Fed, etc.

Defcon 20

- Les stands présents :
  - Matériel (*hardware hacking*) ;
  - Crochetage de serrure ;
  - Ingénierie sociale.
- Sur place :
  - Une très bonne ambiance ;
  - Beaucoup d'entre-aides pour s'améliorer sur ces sujets, beaucoup de conseils ;
  - Des conférences spécifiques pendant 3 jours sur le thème du stand ;
  - Du matériel mis à disposition.

Defcon 20

- La salle des concours :
  - Rétro-ingénierie de code / ingénierie sociale ;
  - Inforensique réseau ;
  - Des stands de dessin ;
  - Un stand pour tondre les cheveux ;
  - Un stand Team Fortress 2 ;
  - Un concours de crochetage ;
  - Un concours de tir aux pigeons sur un simulateur.
- L'exposition des vendeurs :
  - Vente de t-shirts et goodies ;
  - Vente de matériel d'occasion de tout type ;
  - Kit de crochetage ;
  - Vente de livres.

BH et Defcon, c'est aussi...

- La remise du BlueHat Prize de Microsoft
- Pwnie Awards
- Defcon Kids II

« DRONES! »
Chris Anderson

- Une conférence sur le modèle économique d'une société fabriquant des drones
  - Vente du matériel à quelques centaines de dollars (les moins chers du marché)
  - Toute la partie logicielle et programmation des drones est Open Source et pilotée par la communauté
  - Système de récompense des développeurs les plus actifs
    - Envoi de t-shirts
    - Réductions
    - Envoi de matériel gratuit
    - Etc.

« Safes and Containers – Insecurity Design Excellence »
Marc Weber Toblas, Matt Fiddler, Tobias Bluzmanis

- Une présentation sur les coffres permettant de ranger des armes à feu aux États-Unis
  - Soumis à une réglementation et certifiés par le département de la justice de Californie
  - Certification inadaptée
- Présentation de multiples vulnérabilités de ces coffres
  - Soulever un coffre et le laisser tomber suffit à l'ouvrir
  - Accès à des trous dans le coffre qui permettent d'activer les mécanismes internes
  - Un lecteur d'empreintes digitales peut être poussé pour accéder à l'intérieur du coffre
- Ces techniques ont été mise en œuvre dans une vidéo par un enfant de 3 ans

« Advanced Chrome Extension »
Kyle Osborn & Krzysztof Kotowicz

- Workshop de 2h sur les extensions Chrome
- Première partie : conférence
  - Les extensions souffrent des mêmes vulnérabilités que les applications HTML 5
    - XSS
    - CSRF
  - De nombreuses extensions vulnérables
  - Présentation d'un outil facilitant l'exploitation de ces vulnérabilités (XSS Chef)
- Deuxième partie : workshop
  - Exploitation pratique de vulnérabilités
  - Utilisation de l'outil

« Ruby for pentesters »
Cory Scott & Michael Tracy & Timur Duehr

- Workshop de 3h sur l'utilisation de Ruby en test d'intrusion
- Utilisation de bibliothèques telles que
  - Buby (burp ruby) ;
  - Protocol (scapy en ruby) ;
  - Ragweed (debugger) ;
  - Utilisation de curb (curl rb) ;
  - Jruby.

« AMF testing made easy »
Luca Carettoni

- AMF est un protocole utilisé par les applications Flash pour communiquer avec un serveur Adobe Flex
- Présentation d'un outil pour aider aux tests d'intrusion des applications utilisant le protocole AMF
- La conférence présente un plugin Burp
  - Permet la découverte des méthodes disponibles
  - Facilite les tests automatiques

« Reversing and breaking the diag protocol » Martin Gallo

- Description du protocole Diag utilisé dans SAP
- Présentation d'un dissecteur Wireshark
- Présentation d'un module Scapy
- Découverte de vulnérabilités par fuzzing
  - Dénis de service
  - Exploitation d'une vulnérabilité distante (*reverse shell*)

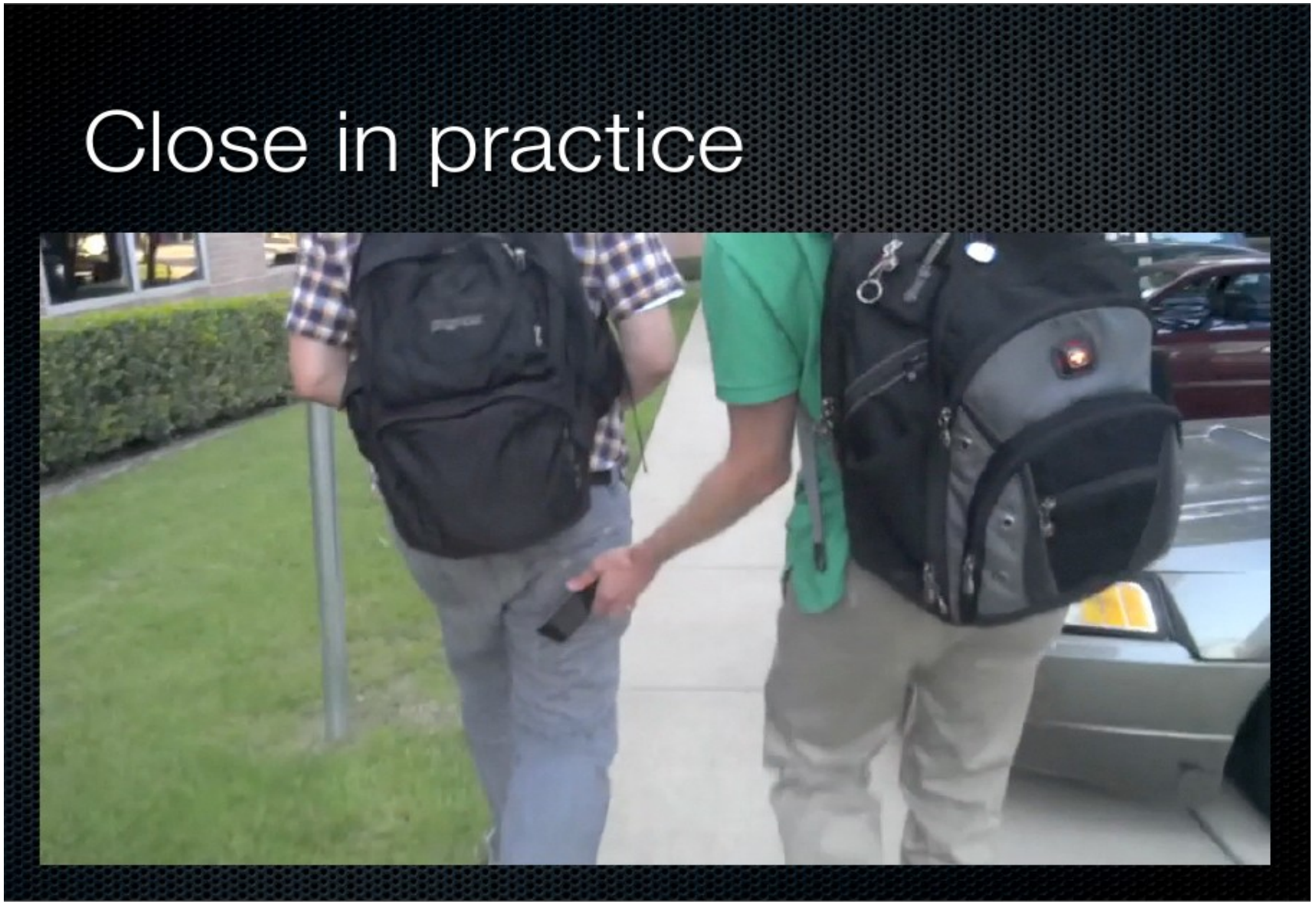
« Metadata weird machine »
Rebecca Shapiro & Sergey Bratus

- Insertion de code dans les en-têtes de fichiers ELF
  - Insertion de portes dérobées
- Conférence très technique sur le fonctionnement du format de fichier ELF
- Mais une longue introduction qui n'apporte rien à la présentation

« Don't stand so close to me » Charlie Miller

- Analyse de la surface d'attaque « NFC »
- Pourquoi ?
  - Devient un standard sur les téléphones
    - Présent sur tous les Nokia
    - Présent sur les nouveaux téléphones Android
    - De nombreuses rumeurs pour l'iPhone 5
  - Nouveau type d'attaque « côté serveur »
- Retour sur quelques bases du NFC
  - Explication de plusieurs protocoles
  - Rappel sur les limites du NFC (utilisation à 4cm)
  - Informations techniques sur les fréquences utilisées

« Don't stand so close to me »
Charlie Miller



« Don't stand so close to me »
Charlie Miller

- Présentation de la démarche suivie
  - Présentation du matériel utilisé
  - Présentation du fuzzing et de la méthode
  - Des tests très manuels
- Découvertes de vulnérabilités dans la pile NFC
  - Un double free dans Android
    - Corrigé dans ICS 4.0.1
    - Tous les téléphones Gingerbread vulnérables
      - 92% des téléphones
  - Quelques plantages mais pas de découverte d'exploitation

« Don't stand so close to me » Charlie Miller

- Des applications gèrent ces données NFC
  - Par défaut
  - Sans interaction utilisateur
- Android
  - De nombreuses applications sur le store
  - Android Beam
    - Introduit dans ICS
    - Partage de contenu par NFC
    - Pas d'interaction utilisateur du client
    - Ce qui augmente grandement la surface d'attaque (visionneuse d'images, lecteur de documents, navigateurs, etc.)

« Don't stand so close to me » Charlie Miller

- Nokia Content Sharing
  - Comme Beam, pour Nokia
  - Permet l'exploitation de vulnérabilités clientes sans interaction utilisateur
    - libpng 1.2.42 vulnérable
    - Vulnérabilité dans les PPTs et les PDFs : koffice-2.3.3
  - Bluetooth pairing
    - Demande de confirmation désactivée par défaut
    - Même si le Bluetooth est éteint, il peut être réactivé automatiquement par NFC
  - Lecture des SMS, émission d'appel, lecture de données système, etc.

« PinPadPwn »
Nils et Rafael Domingues Vera

- Analyse de la sécurité des terminaux de paiement mobile
- Homme du milieu sur la carte à puce pour comprendre le protocole.
- Sécurité des terminaux
  - Signature des binaires
    - Mécanismes implémentés pour interdire l'exécution de logiciels malveillants et la falsification des binaires
    - Ce mécanisme, même s'il empêche la falsification des binaires exécutés sur le terminal, dans certains cas, ne vérifie pas tous les fichiers d'une application (par exemple, certains fichiers de configuration)
    - Dans certains cas, les accès obtenus au système permettait l'exécution de code
  - Les techniques de protection contre les codes d'exploitation n'étaient pas mises en place

« PinPadPwn »
Nils et Rafael Domingues Vera

- Trois cas d'étude
  - Premier cas
    - Une vulnérabilité découverte avec un accès au port Ethernet d'un terminal a permis de découvrir des informations sur le système
    - Découverte de vulnérabilité par une carte à puce
    - Présentation d'un code d'exploitation qui lance un jeu de voiture dans le terminal de paiement

      → exécution de code arbitraire, contrôle de l'interface et du ticket imprimé
  - Deuxième cas
    - Découverte d'accès par défaut permettant d'activer le service Telnet
    - Découverte d'une vulnérabilité d'injection de commande permettant d'élever ses privilèges sur l'application
    - Accès root au système

« PinPadPwn »
Nils et Rafael Domingues Vera

- Troisième cas, une exploitation pratique
  - Utilisation d'une première carte qui affiche une erreur de paiement
  - Elle ajoute une porte dérobée qui modifie le fonctionnement du terminal de paiement pour enregistrer tous les numéros de cartes avec le code pin associé
  - Une deuxième carte permet de récupérer ces informations et affiche que le paiement est accepté

« Adventures in BouncerLand »
Nicholas J. Percoco et Sean Schulte

- Analyse des applications du Google Play Store

  ➪ Système « Bouncer » (février 2012)

  Réalise une vérification lors de la publication, des MAJ et régulièrement

  Analyse comportementale

- Objectif : déterminer les facteurs d'acceptation d'une application
- Approche boîte noire
- Réalisation d'une application malfaisante
  - Chaque fonctionnalité ajoutée progressivement
  - Liste noire des plages IP Google pour désactivation des comportements malveillants
  - Chaque comportement malveillant est compensé par une fonctionnalité légitime (permissions)

« Adventures in BouncerLand »
Nicholas J. Percoco et Sean Schulte

- Utilisation de la fonctionnalité de pont JavaScript
  - MAJ des fonctionnalités sans passage par Google Play
  - Pas de vérification du bouncer
  - Serveur C&C contacté par l'application
- Non détection par le bouncer
  - Coordonnées des contacts
  - Enregistrements SMS
  - Paramètres de configuration (numéro de téléphone)
  - Fichiers multimédias
  - Historique des appels
  - Fonctionnalités « botnet »

« Windows Phone 7 Internals and Exploitability » Tsukasa Oi

- Applications utilisateur exécutées dans un bac à sable (développement en .NET)
- Conçu de manière sécurisée (contrôle d'accès, signature, etc.)
- Système « Capabilities » similaire aux permissions Android
  - ID_CAP_INTEROPSERVICES : utilisation de code natif
    - Cas étudié par l'orateur
- Bonnes pratiques non appliquées pour les pilotes tiers
- DEP : bonne implémentation
- ASLR : faible entropie (10 bits)
- Chaînes dynamiques Unicode => mémoire exécutable

« The subway line 8 - Exploitation of Windows 8 Metro Style Apps »
Sung-ting Tsai et Ming-chieh Pan

- Conception des applications Metro Style
  - Disposent de « Capabilities » (réseau, système de fichiers, périphériques, etc.)
  - Utilisation d'un bac à sable (AppContainer)
    - Accès aux ressources via les API WinRT (basé sur COM)
- Cible des attaques : RuntimeBroker
  - Processus destiné à réaliser des actions spécifiques pour une application
  - Mécanisme d'IPC pour la communication entre le Broker et les applications
    - Interfaces COM
    - Communication via des ports ALPC
- Objectif : sortir de l'environnement cloisonné

« The subway line 8 - Exploitation of Windows 8 Metro Style Apps »
Sung-ting Tsai et Ming-chieh Pan

- Vecteurs d'attaque
  - Communication ALPC
    - Hook de la fonction d'envoi et fuzzing
  - Serveur(s) COM
    - Identification des serveurs COM
      - Privilèges élevés (niveau d'intégrité > moyen)
      - Si lancement autorisé pour « ALL APPLICATION PACKAGE »
    - Spécification des interfaces et des méthodes, puis fuzzing
  - API WinRT : fuzzing des fonctions de l'API
  - Conception
    - Contournement des limitations de l'accès Internet
    - Contournement des limitations de lancement d'un programme
    - Contournement d'accès à un fichier / répertoire

« Owning One to Rule Them All »
Dave Kennedy et Dave DeSimone

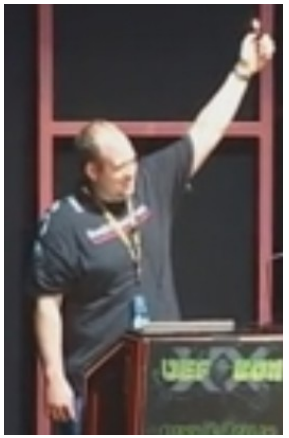
- Objectif : compromission de l'ensemble des machines de l'infrastructure SCCM
- Environnement PXE
  - Récupération des empreintes de l'administrateur local
- SCCM
  - Focalisation sur l'aspect déploiement d'applications
  - Attaque du point de gestion

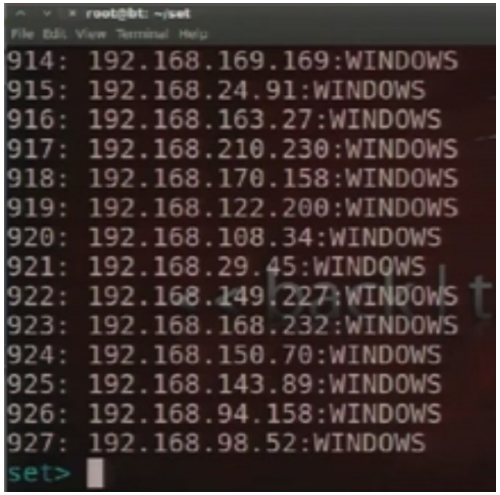
➪ ajouter une porte dérobée à un package valide

- Beaucoup d'informations disponibles depuis l'agent SCCM
  - Adresse IP du point de gestion
  - Package ID

« Owning One to Rule Them All »
Dave Kennedy et Dave DeSimone

- Ajout de la porte dérobée
  - Connexion en tant qu'administrateur sur le serveur SCCM
  - Détermination de l'emplacement des packages
  - Remplacement d'un exécutable
    - Mais vérification de la signature
      - ➪ Utilisation de la méthode WMI RefreshPkgSource()
    - SCCM 2012 SP1 : gère également Mac OS X et Linux/Unix
- Compromission des machines
- Intégré à SET (Social-Engineering Toolkit)





« Post-Exploitation Nirvana: Launching OpenDLP Agents over Meterpreter Sessions » Andrew Gavin, Michael Baucom et Charles Smith

- Pouvoir analyser chaque système après compromission
  - Déploiement d'un agent de recherche (expressions rationnelles)
  - ➪ ne nécessite pas de mot de passe / empreinte

1. Utilisation d'une session Meterpreter existante
   - Utilisation du serveur RPC de Metasploit
   - Développement d'un module de communication
     - Interaction avec les sessions
2. Module de post-exploitation dédié
   - Pour compatibilité avec Armitage

- Quelques modifications de l'interface Web de OpenDLP

« Weaponizing the Windows API with Metasploit's Railgun » - David "thelightcosine" Maloney

- Intégration de Railgun à Metasploit en juin 2010
- Conférence de rappel du fonctionnement de l'API Railgun
  - Permet l'utilisation de l'API Win32 depuis Meterpreter
    - Sélection de la DLL et fonction à appeler
    - Utilisation des fonctionnalités proposées par Windows
  - Support 64 bits
  - Implémentation basée sur LoadLibrary() et GetProcAddress()
  - Réalisation simple de modules

« Cortana: Rise of the Automated Red Team » Raphael Mudge

- Moyen simple d'automatisation de Metasploit
- Pratique pour les périmètres larges
  - Gain de temps
  - Facilite l'application de la méthodologie d'intrusion
- Langage de script pour Armitage
  - Automatisation des tâches courantes
  - Personnalisation de l'interface graphique de Armitage
- Utilisation d'un système d'agents
  - Analyse des entrées de la BDD Metasploit
- Réponse à un certain nombre d'évènements
  - Découverte d'un nouvel hôte / service / mot de passe, etc.

« Cortana: Rise of the Automated Red Team » Raphael Mudge

- Exemples
  - Import automatique de résultats de scans
    - Surveillance de la BDD
    - Ajout des résultats des balayages de ports
    - Lancement de scripts suivant le service
  - Post-exploitation : restreindre l'utilisation du navigateur Internet
    - Récupération de l'identifiant du processus et terminaison
    - Toutes les 5s
  - Ajout d'un menu dans l'interface graphique
    - Interception nom d'utilisateur / mot de passe FTP

https://github.com/rsmudge/cortana-scripts

« Fuzzing Online Games »
Elie Bursztein et Patrick Samy

- Rétro-ingénierie de jeux en ligne
  - Diablo 3 et League of Legends
- Présentation d'une démarche applicable

1. Interception du trafic
   - Hooks sur des fonctions des APIs réseaux (ex : Winsock)
     - Détectés dans une certaine mesure par le système anti-triche de Diablo 3
   - Depuis l'extérieur (hôte pour une machine virtuelle)
2. Déchiffrement du trafic
   - League of Legends : clé Blowfish en paramètre
   - Diablo 3 : procédure d'authentification chiffrée, mais pas le trafic au serveur de jeu

3. Rétro-ingénierie du protocole
   - À partir de traces réseaux
   - Plusieurs étapes
     - Identification des différents types de paquets (opcodes existants)
     - Détermination de la taille des champs et des valeurs acceptables
     - Analyse de la fréquence des opcodes
     - Ordre d'apparition des opcodes
     - Corrélation entre une action observable et la génération d'un paquet
4. Fuzzing
   - Envoi des paquets et analyse de l'impact
   - Identification des emplacements mémoire
     - Par réalisation d'opérations « atomiques »

« Hardware Backdooring is Practical »
Jonathan Brossard

- Création d'une porte dérobée difficilement détectable
  - Et persistante (réinstallation OS)

➪ Cible : BIOS

- Cas d'attaque :
  - Accès physique au matériel (ex : chaîne d'approvisionnement)
  - Après intrusion
- Conçue autour de composants Open Source
  - Coreboot (détection du matériel)
  - SeaBIOS (implémentation des interfaces typiques d'un BIOS x86)
  - iPXE (chargement d'un OS par le réseau)

➪ Portable / Piles réseaux / Composants légitimes

« Hardware Backdooring is Practical » Jonathan Brossard

- Permet l'affaiblissement de la sécurité (NX Bit, ASLR, etc.)
- Bootkit Windows : utilisation de Kon-Boot
- Non détection par les anti-virus
- Aucune trace de compromission sur le disque
  - Récupération par le réseau de la charge utile (support Wi-Fi et WiMAX), à chaque démarrage
  - Bootkit uniquement en mémoire

- Recommandations
  - Flasher le firmware du nouveau matériel
  - Vérifier l'intégrité des firmwares

« Anti-Forensics and Anti-Anti-Forensics: Attacks and Mitigating Techniques for Digital-Forensic Investigations » - Michael Perklin

- Techniques compliquant l'analyse inforensique (✭)
  - Ajouter des coûts / du temps à l'analyse
  - Méthodologie pour les limiter (➔)

- Créer une copie de travail
  - ✭ Saturation de données (problématique pour stockage également)
    - ➔ Paralléliser le processus d'acquisition / Utiliser le matériel sur place
  - ✭ Utilisation de RAID non standards, ex : paramètres personnalisés
    - ➔ Utiliser le système du suspect (Live CD)
- Traiter les données pour l'analyse
  - ✭ Modification des en-têtes des fichiers
    - ➔ Fuzzy hashing avec les autres fichiers / Analyse des fichiers récents

« Anti-Forensics and Anti-Anti-Forensics: Attacks and Mitigating Techniques for Digital-Forensic Investigations » - Michael Perklin

- Séparer le bon grain de l'ivraie
  - Filtres d'exclusion : modification des fichiers système (*12h*)
    - Utiliser une approche par liste blanche
- Analyser la pertinence des données
  - Mélange dans les temps MACE (*16h*)
    - Regarder du côté des fichiers de journalisation (séquentiel)
- Préparer le rapport des résultats
  - Utilisation de noms de fichiers réservés
    - Spécifier un nom de fichier différent lors de l'export
- Conclusion : 63h de travail supplémentaire

http://www.perklin.ca/~defcon20/perklin_antiforensics.pdf

Des questions ?

Merci à l'OSSIR pour sa participation !