ANSSI Agence nationale de la sécurité des systèmes d'information

Compte-rendu de la conférence Cansecwest 2010

Loïc Duflot
Agence Nationale de la
Sécurité des Systèmes d'Information

SGDSN/ANSSI 51 boulevard de la Tour Maubourg 75007 Paris

loic.duflot@ssi.gouv.fr

ANSSI Agence nationale de la sécurité des systèmes d'information

Introduction

- Cette présentation est un compte-rendu de la conférence Cansecwest 2010 qui s'est déroulée à Vancouver du 24 au 26 mars 2010.
  - La conférence est organisée par la société Dragostech également en charge de l'organisation des conférences BACon, Pacsec et EUSecwest.
  - Les planches de la plupart des présentations sont disponibles au lien suivant http://dragos.com/csw10.
- 18 présentations ont été effectuées plus quelques « lightning talks ». Plusieurs « dojos » (sessions de formations payantes sur des thèmes divers) ont également été organisés en marge de la conférence.
- Le résumé des présentations se veut factuel et ne reflète pas l'opinion de l'ANSSI sur lesdites présentations ou leur contenu.

Internet Nails

- Markus Ranum (Tenable Security).
- Présentation d'introduction relativement courte (25 minutes).
- Markus Ranum présente la complexification progressive des différentes couches protocolaires (FTP, TCP, HTTP, Technologies Web).
- Il présente pourquoi cette complexification qui aurait initialement pu être évitée facilement est aujourd'hui la source de la plupart des problèmes de sécurité rencontrés, en ce concentrant sur le problème du suivi d'état des protocoles.

ANSSI | Agence nationale de la sécurité des systèmes d'information

Under the kimono of Office Security Engineering

- T. Gallagher, D. Conger (Microsoft).
- Présentation des principes de sécurité de la suite Office 2010.
- La sécurisation est une opération complexe: plus de 300 parseurs sont mis en œuvre par Office.
- Les grands principes sont les suivants:
  - Analyse a priori (fuzzing notamment, retrait des parseurs obsolètes).
  - Contrôle de format dynamique (Gatekeeper).
  - « Sandboxing » en cas de provenance douteuse ou de problème dans le format.
- Info: près de 2000 bogues corrigés par Microsoft dans Office 2007 suite à son initiative SDL et autant dans Office 2010.

Automated SQL Ownage Techniques

- Fernando Federico Russ (Core technologies).
- Les injections SQL classiques sont (relativement) bien connues.
- Ici, l'idée est d'utiliser des techniques de fingerprinting pour déterminer à quel endroit dans une requête est utilisé un champs vulnérable, quel est le type du champs, etc.
- La détermination de la nature de la base considérée (MySQL, SQL server) est également possible.
- La technique nécessite de nombreuses injections successives, et les impacts de ces requêtes sur la base de donnée sont pour l'instant mal mesurés.

ANSSI | Agence nationale de la sécurité des systèmes d'information

Can you still trust your network card?

- Yves-Alexis Perez, Loïc Duflot (ANSSI).
- Les cartes réseau sont des objets très exposés à la menace informatique.
- La présentation visait à démontrer, preuve de concept et démonstration à l'appui sur un cas réel, qu'il était possible pour un attaquant de prendre le contrôle à distance d'une carte réseau.
- En l'absence d'IOMMU, il est ensuite possible de prendre le contrôle de la machine hôte, quel que soit le système d'exploitation.
- Le problème utilisé pour la preuve de concept a été remonté au vendeur concerné et un correctif est disponible.
- http://www.ssi.gouv.fr/site_article187.html

SEH overwrite and its exploitability

- Shuichiro Suzuki (FourteenForty).
- La compromission des Structured Exception Handler est une technique d'exploitation classique en environnement Windows.
- La présentation discutait de l'utilité des différents mécanismes de sécurité Windows pour empêcher ce type d'attaque:
  - /GS non utile.
  - SEHOP contournable quand les adresses sont connues.
  - SafeSEH contournable quand l'exécutable cible est lié avec des bibliothèques qui ne sont pas protégées (pour simplifier).
  - DEP contournable avec des techniques de type « ret2libc » en l'absence de randomisation.
  - ASLR est le mécanisme le plus efficace.

ANSSI | Agence nationale de la sécurité des systèmes d'information

There's a party at ring 0 and you're invited

- Tavis Ormandy et Julien Tinnes (Google).
- La présentation détaillait les différentes failles noyaux mises en évidence par les auteurs au cours de l'année écoulée (NetBSD, Linux, Windows).
- De plus en plus d'applications s'exécutent dans un environnement non privilégié (virtualisation, sandboxing, etc.). L'exploitation de faille noyau permet potentiellement de contourner le cloisonnement. La surface d'attaque exposée par le noyau est souvent très importante. De nombreuses fonctions sont obsolètes.
- Mention de l'utilisation probable de SECCOMP en environnement Linux dans une future version du navigateur Chrome.

Babysitting an army of monkeys: fuzzing with 5 lines of Python

- Charlie Miller.
- Fuzzing de Adobe Reader, Preview, Office PPT, Openoffice impress.
- La technique retenue est de télécharger un maximum de documents PDF et PPT sur Internet, de les modifier à la marge, de tenter de les ouvrir avec chaque application et de retenir les crashs reproductibles.
- Classification des crashs avec des outils classiques (Valgrind, Microsoft !exploitable).
- Les bogues trouvés ont été rapportés aux industriels concernés mais n'ont pas été présentés.
- Les vendeurs sont selon l'orateur souvent assez lents à corriger les vulnérabilités (difficulté à reproduire les bogues?).
- http://securityevaluators.com.

ShaREing is caring

- Sebastian Probst, Halvar Flake (Zynamics).
- Présentation de BinCrowd permettant le partage d'information pour les analystes de programmes.
- Les participants peuvent soumettre des applications à une base de données après analyse et rechercher des programmes similaires dans la base.
- Lorsque des programmes similaires sont détectés, il est alors possible de bénéficier du travail déjà effectué lors de la première analyse.
- Sur le plan technique, nécessité de disposer d'une fonction de hachage pour les graphes de contrôle de flot, et une méthode de calcul permettant de quantifier la ressemblance entre deux graphes.
- bincrowd.zynamics.com

Cisco IOS exploitation with IODIDE

- Andy Davis (KPMG).
- IODIDE est un débogueur pour IOS. Il semble qu'IOS permette facilement la connexion d'un débogueur gdb.
- Environnement PowerPC.
- IODIDE peut être exécuté localement où à distance.
- Démonstration d'exploitation d'une faille (ancienne et corrigée) sur IOS et utilisation de cette exploitation pour brancher le débogueur à distance.
- Une version d'IODIDE devrait être publiée prochainement.

ANSSI | Agence nationale de la sécurité des systèmes d'information

Random tales from a mobile phone hacker

- Collin Mulliner (Université de Berlin).
- Analyse des informations qui fuient par les headers HTTP lorsque les internautes se connectent à un site depuis un « smartphone » (à partir des journaux de son propre site).
- Les informations (numéro de téléphone, numéro d'abonné, localisation), ajoutées par les passerelles avec le réseau Internet, dépendent des opérateurs.
- Mise en place d'un site permettant aux internautes de s'assurer de l'absence d'information dans leurs headers (pas de journalisation).
- mulliner.org/blog

Legal perspectives of hardware hacking

- Jennifer Granick (Electronic Frontier Foundation).
- La présentation se voulait une analyse juridique détaillant dans quel cadre il était possible d'effectuer des analyses inverses (reverse engineering) de produits matériels sans tomber sous le coup des lois américaines.
- Les points suivants sont à retenir:
  - Valider l'EULA (Licence d'utilisation) créée un contrat entre l'analyste et le propriétaire des droits.
  - Si l'on doit mettre en œuvre une analyse inverse à des fins d'interopérabilité, il vaut toujours mieux avoir recours à deux équipes différentes (une pour l'analyse, l'autre pour la réalisation du nouveau produit).

Stuff we don't want on our phones

- Jimmy Shah, McAfee, Inc.
- L'orateur a présenté une liste de logiciels malveillants, de logiciels espions ou d'« adware » pouvant être utilisés pour compromettre un « smartphone » et que l'on peut trouver dans la nature.
- Liste réalisée à partir d'exemples publics (articles de presse).

Practical exploitation of modern wireless devices

- Thorsten Schroeder (Dreamlab Technologies).
- Analyse de la sécurité des claviers sans fil (protocole propriétaire mis en œuvre par les composants Nordic Semiconductor utilisés dans certains claviers, mais pas tous).
- La cryptographie mise en œuvre est basique.
- Il est possible d'intercepter les frappes à distance (soi-disant plusieurs dizaines de mètres), et d'injecter des frappes.
- Les auteurs ont réalisé avec succès une démonstration d'injection de frappes.
- Le design de la carte utilisée pour l'interception est Opensource.
- Projet KeyKeriki.

RFID hacking at home

- Melanie Rieback
- Présentation de « RFID Guardian », un émulateur programmable d'étiquette RFID pouvant également jouer le rôle de lecteur RFID.
- Permet selon l'auteur de réaliser un « pare-feu pour RFID ».
- Permet également de mettre en œuvre les attaques classiques par spoofing ou par relai.
- Le projet est « open source », mais des exemplaires du « RFID Guardian » devraient être également commercialisées à bas pris.
- www.rfidguardian.org

ANSSI | Agence nationale de la sécurité des systèmes d'information

Advanced MAC OS X physical memory analysis

- Matthieu Suiche (MoonSols).
- Présentation d'un utilitaire d'analyse post mortem de la mémoire des machines MAC OS X.
- Reconstitution automatique de l'arbre des processus:
  - Informations sur les processus (threads, mémoire, descripteurs de fichiers…).
  - Accès aux structures bas-niveau (tables de page notamment).
- Détection d'attaques classiques (notamment « hooks » dans la table des appels systèmes).
- Démonstration en séance.
- http://www.moonsols.com/talks/CSW2010.pdf

Full process analysis and reconstitution of a virtual machine from the host

- Jamie Butler (MANDIANT).
- Analyse de la mémoire d'une machine virtuelle depuis le système d'exploitation de la machine hôte.
- L'analyse peut être dynamique (pendant le fonctionnement de la machine virtuelle).
- Fonctionne uniquement pour les machines virtuelles sous Windows.
- Machines virtuelles supportées Xen et VMWare.

ANSSI Agence nationale de la sécurité des systèmes d'information

Through the looking glass: an investigation of malware trends and response activity

- Jeff Williams (Microsoft)
- Répartition géographique des machines compromises et participant à différents botnets.
- Indications sur le fait que le botnet Waledac a été démantelé grâce à une coordination internationale.

ANSSI | Agence nationale de la sécurité des systèmes d'information

The jedi packet trick takes over the deathstar: taking NIC backdoors to the next level

- Arrigo Triulzi, Sevenseas (via Skype).
- Présentation d'un rootkit pour carte réseau avancé permettant par exemple de contourner des politiques de filtrage sur un pare-feu.
- Réalisé sur des cartes anciennes qui ne sont plus commercialisées.
- Communication entre deux cartes compromises via le bus PCI.
- Soutien de la carte graphique comme coprocesseur pour accélérer les traitements.
- Quelques idées pour assurer la pérennité d'un tel rootkit: compromission du microcode du CPU, piège d'EFI.

ANSSI | Agence nationale de la sécurité des systèmes d'information

« Lightning talks »

- Uniquement 5 lightning talks ont été effectués cette année (contre plus d'une dizaine l'an dernier).

- Firefox: lutte contre les attaques de type XSS.
- Démantèlement du botnet Waledac.
- Utilisation des « URL shorteners » (par exemple bits.ly) à des fins malveillantes.
- Et pour mémoire:
  - « Sons à 2600 Hz »
  - « Patch Tuesday »

Références

http://www.cansecwest.com