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

Las Vegas 2010

Compte-rendu Black Hat et Defon

Jean-Baptiste Aviat et Yves Le Provost
<Jean-Baptiste.Aviat@hsc.fr> <Yves.Le-Provost@hsc.fr>

Hervé Schauer Consultants

- Présentation ?

Return Oriented Programming

- Sujet de quatre conférences !
- Principe pour exploiter un buffer overflow:
  - Ret-into-libc : on pousse sur la pile (non exécutable) :
    - @'/bin/sh'
    - @exec()
  - Problème dans les cas suivants :
    - Les adresses de exec() ou la chaine '/bin/sh' contiennent des bytes nulls (ASCII Armored) ;
    - Les bibliothèques contenant des fonctions « sensibles » sont chargées en mémoire à des adresses aléatoires (ASLR)...
  - Solution potentielle : le ROP, Return Oriented Programming :)

Pour une librairie sans ASLR

- On veut exécuter A, B, C
- Chercher les instructions suivies d'un RET (« gadgets ») :

```
gadget 1 : 0x080480f0 A
           0x080480f2 RET
gadget 2 : 0x080482f0 B
           0x080482f2 RET
gadget 3 : 0x080485e0 C
           0x080485e2 RET
```

- Il suffit de pousser ceci sur la pile :

```
0x080480f0 (@ gadget 1)
0x080482f0 (@ gadget 2)
0x080485e0 (@ gadget 3)
```

- A s'exécute ;
- RET s'exécute...
- ...et place dans EIP l'adresse de B.

Return-Oriented Exploitation

- Dino Dai Zavi
- Présentation d'un outil de construction de ROP
  - Création d'un dictionnaire par analyse de binaire
  - Outil non public
- Démonstration de l'exploitation de MS10-002
  - Windows 7 avec le DEP

• Payload Already Inside

- **Data Re-Use for ROP exploits**, Long Le, VNSecurity
- But : outrepasser l'ASLR
  - Construire une pile « fixe »
  - Section « data » des exécutables
    - Peut être écrite
    - Adresse fixe et connue
  - Libc avec ASLR
    - Intervalle entre deux adresses de fonctions est constant !
    - Calcul à l'aide de la GOT
- Stage 1 :
  - Résolution des adresses, ordonnancement des adresses
- Stage 0 :
  - Stabilise la pile
  - Y transfère Stage 1

• Payload Already Inside

- Outil ROPEME
  - Génère les « gadgets » pour un binaire
  - Cherche des « gadgets » particuliers
  - Génération de payload stage-1 et stage-0 d'exemple
- De telles fonctionnalités vont voir le jour dans Metasploit

Everybody be cool this is a roppery !

- Tim Kornau, Vincenzo Iozzo, Ralf-Philipp Weinmann
  - Zynamics

Everybody be cool this is a roppery !

- ROP sur ARM
- Construction intelligente de charges utiles
  - Le langage REIL est un méta-langage assembleur
  - Traduire les gadgets en REIL
    - Les gadgets équivalents peuvent être éliminés
- Écriture d'un compilateur pour ces gadgets
  - Génération automatisée de n'importe quel code
    - Sous réserve d'une bibliothèque assez grande !
- Travail très académique
  - Au résultat très concret

ROP in PHP Application Exploits

- Stefan Esser
- But : réutiliser le code de l'application
- ROP inexploitable en PHP
  - La pile d'appels est séparée entre le tas, la pile, le data segment
  - Bytecode PHP situé à des positions inconnues
- POP : Property Oriented Programming
  - Unserialize() exécute wakeup() sur les classes sérialisées

Jackpotting Automated Teller...

- Pas grand chose à dire de plus :

Blue Screen of the Death is dead

- Matthieu Suiche
  - Moonsols

Blue Screen of the Death is dead

- Moonsols Windows memory toolkit
- Peut convertir au format Microsoft crash dump (Windbg) :
  - Full memory dumps Windows
  - Fichiers d'hibernation
  - Possibilité de convertir
    - les fichiers d'hibernation de toute version
    - dumps « raw »
      - Périphérique \Device\PhysicalMemory
      - Fichiers vmem (VMWare), pour des machines démarrées

There's a party at Ring0 (and you're invited)

- Julien Tinnes et Tavis Ormandy
  - Google

There's a party at Ring0 (and you're invited)

- Retour sur de nombreuses failles noyau
  - « The kernel as a target »
- Chroot(), jails, MAC
  - laissent le noyau complètement accessible
- Windows : TTF parsing → Ring0
  - @font-face sous IE (même code depuis NT4)
  - Nombreuses implémentations vulnérables... mais peu en Ring0
- NULL deref
  - sock_sendpage()
    - noyaux 2.4 & 2.6
  - udp_sendmsg()
- #GP Trap Handler bug
  - Windows à partir de 1993

Exploiting Timing Attacks...

- ...in widespread systems
- Nate Lawson

- Timing attacks sur des applications Web
- Taux de réussite intéressant
  - Particulièrement dans les applications Java
  - Peu d'informations disponibles actuellement

- Fonction de comparaison de mot de passe
  - Temps constant ?

Exploiting Timing Attacks...

- Utilisation d'une machine dédiée
  - Faible préemption
- Implémentation d'un client HTTP
  - Pour des mesures de temps précises
  - À l'aide des raw sockets
    - Pour scinder l'envoi de la requête

Virt-ICE : next generation debugger...

- ...for malware analysis
- Quynh Nguyen Anh et Kuniyasu Suzaki
- Programme à déboguer
  - Placé dans une machine virtuelle
  - Disposant d'un driver
- Déboggueur
  - Placé dans l'hôte
- Avantages du procédé
  - Déboggeur Invisible
  - Peut examiner les malwares Ring0

Virt-ICE : next generation debugger...

- Utilise qemu
  - KVM ou Xen utilisent une exécution physique
  - Exécution logicielle des binaires virtualisés
    - Ajout de fonctions simple
    - Pas de problème particulier de performance

```
# From Qemu's monitor, load Virt-ICE module into Qemu
monitor> kmodule load /opt/kobuta/virt-ice.km
# From the host, run Virt-ICE client to connect to Virt-ICE module
%> virt-ice
# In Virt-ICE client, list all the running processes inside the Windows VM
vice> ps
# List all kernel modules currently loaded in the Windows VM
vice> kmodules
# List all DLL files open by process with pid 134
vice> dlls -p 134
# List all registries open by process with pid 134
vice> registry -p 134
# Stop the VM when malware.exe is loaded into memory, before it is executed
vice> db -S -p malware.exe
# Set breakpoint at WriteProcessMemory() function
vice> db -p malware.exe -s WriteProcessMemory
```

SMB NTLM Weak Nonce vulnerability

- Hernan Ochoa, Agustin Azubel

SMB NTLM Weak Nonce vulnerability

- MS10-12
- NTMLv1
  - Le serveur génère un nonce
  - Le client le renvoi chiffré par le mot de passe
- Plusieurs attaques :
  - Par écoute et rejeu jusqu'à duplication d'un nonce
  - De même, en collectionnant activement les nonces (phishing)
  - Via le PRNG faible : les nonces peuvent être prédits

Surviving the mobile application explosion

- Étude des applications mobiles
  - Téléchargement systématique depuis les « stores »
    - Apple Store
    - Google Market
- Comment est utilisée l'API ?
- Lecture « illégale » des contacts
  - 14% sur iPhone
  - 8% sur Android
- Accès « illégal » à la géolocalisation
  - 33% sur iPhone
  - 30% sur Android

This is not the droid you're looking for

- Android
  - Système d'exploitation basé sous Linux
- Il existe des backdoors sous Linux
  - Sous Android aussi !
  - Hook de l'IDT
- exécution de commandes lors d'un appel
- Pas de méthode pour sortir de la VM

Getting in Bed With Robin Sage

- Via les réseaux sociaux
- En se faisant passer pour...
  - Une jolie femme
  - Intelligente
  - CV fourni
- On peut obtenir bien des choses des hommes !
  - Acteurs du monde de la sécurité informatique

My life as a spyware developer

- Garry Pejski, ancien « lead developper » de spyware
- Entreprise canadienne
- Développement d'un spyware « conventionnel »
- Pour le client :
  - Hook du navigateur
    - Publicités en fonction des recherches
    - Ajout d'icones, de moteur de recherche
  - Dissimulation de fichiers dans les Alternate Data Streams
  - Exécution de code arbitraire
- Pour le serveur :
  - Gestion de campagnes marketing
  - C&C

Questions ?