Metasploit

Pour tous ou presque ...

Présentation pour le groupe SUR

12/12/2006

Saâd Kadhi et Guillaume Arcas

Agenda

- ★ Attaque vs. Défense
- ★ Metasploit 101
- ★ Démonstration
- ★ Conclusion, Références

Attaque vs. Défense

Un Brin d'Histoire

★ La qualité des exploits varie

- Certains sont hautement fiables
- D'autres compilent à peine

★ Pas de consistance, peu de réutilisation de code

★ Désordre innommable

Frameworks

★ Pour résoudre ce désordre, des développeurs très talentueux ont crée des frameworks d'exploits

- Pour le développement et l'utilisation d'exploits modulaires

Chaînes de Montage

★ Ces frameworks peuvent être assimilées à des chaînes de montage

- Pour la création massive (industrielle) d'exploits
- Henry Ford n'a pas inventé l'automobile

Bienvenue dans l'Ere Industrielle

★ Framework d'exploits ~ 75% du travail

- Automatisation partielle de la production

★ Le développeur n'a plus qu'à se concentrer sur l'essentiel

Frameworks et Scanners

★ Ne pas confondre framework et scanner de vulnérabilité

★ Un scanner de vulnérabilité tente de déterminer si une cible est vulnérable

★ Un framework pénètre la cible et confirme la vulnérabilité

Avantages pour les Attaquants

★ Les frameworks offrent des avantages indéniables pour les attaquants

- Pour ceux qui créent leurs propres exploits ciblés
- Pour les script kiddies

Frameworks et Exploits Ciblés

★ Réduction du temps nécessaire pour créer un nouvel exploit

★ Facilité accrue

★ Meilleure qualité

- On ne parle pas de PoC

Vous Avez Dit Correctif ?

★ A l'ère des frameworks et de la rétro-conception binaire, les exploits sont crées de plus en plus rapidement

★ Où en êtes vous dans votre campagne de correctifs ? 6, 3 ... 1 mois ?

Doux Rêveurs , Réveillez-Vous !

★ "J'ai des applications métier"

- Et bien entendu, vous avez tout développé "from scratch" selon des principes de développement sécurisé

★ "J'ai un IDS/IPS"

- Et ?

Bénéfices pour les Défenseurs ?

★ Vérification des vulnérabilités remontées par des scanners

★ Tests de vos IDS/IPS

- "Ils sont à jour !" ... euh

★ Vérification du bon suivi de la campagne de correctifs

Mais encore !

★ Amélioration de vos tests d'intrusion

★ Vous développez des exploits en interne ? Soyez plus productif !

★ Prise de conscience

- " Monsieur le directeur ... votre mâchoire ... elle se décroche"

Attention !

★ Certains exploits peuvent causer des dysfonctionnements

★ Prise de ~~conscience~~ la porte

- "Tiens c'est bizarre... la base de données transactionnelle ne répond plus..."

Exemples de Frameworks

★ CANVAS d'Immunity : $$$

★ IMPACT de Core Security Technologies : $$$

★ Metasploit : libre pour des utilisations non-commerciales

Metasploit îOî

Et Metasploit Fût

★ En 2003, H.D. Moore et spoonm ont crée Metasploit

- http://www.Metasploit.com/

★ Le meilleur framework d'exploits "libre"

★ 2 versions : 2.7 , 3.0

Tableau Comparatif

Version	Langage	Licence	+/-
2.7	Perl	GPLv2, Artistic	Stable, une certaine lenteur, problèmes d'automatisation et de portabilité, bonne documentation utilisateur
3.0	Ruby	Metasploit Framework License	Bêta, guide de développement, évasion d'IDS, docs API, sessions, exécution simultanée de plusieurs exploits avec de multiples shellcodes

Architecture MetaSploit 3.0

- msfapi
- msfconsole
- msfcli
- msfweb
- msfwx

Interfaces

- plugins personnalisés
- outils protocolaires

- framework-base
- framework-core
- rex
- librairies

Modules

- auxiliaires
- encodeurs
- NOPs
- charges utiles
- exploits

- anti-filtres
- anti-détection
- injection de charges utiles
- manipulation mémoire

Atelier de l'attaquant

Rex

★ Rex::Arch -> Génération d'instructions Assembleur à la volée

★ Rex::Encoding -> Encodeurs XOR

★ Rex::Exploitation -> Manipulation mémoire, SEH overflow

framework-core

★ Interface pour les modules et les plugins

★ Stockage de valeurs contrôlées par l'utilisateur

★ Gestion d'événements

framework-base

- ★ Facilite l'interaction avec le framework
- ★ Gestion de configuration, debugging, sérialisation de données sur les modules, sessions

Exploits

★ 116 exploits (3.0 bêta 3)

★ Différentes plates-formes/ applications

- Linux, Windows, Mac OS X, Solaris
- IIS, Solaris, Exchange, Snort ...

Charges Utiles

★ 99 charges utiles (3.0 bêta 3)

- Shell, Reverse Shell, Téléchargement/Exécution, Meterpreter...

★ Différentes plates-formes

- Linux, Windows, *BSD, Solaris ...

Meterpreter îOî

★ Charge utile générique pour plate-forme Windows

★ Transporte une DLL spéciale vers la cible. Peut être assimilée à un shell

★ Exécution à l'intérieur du processus vulnérable

Meterpreter l'Enchanteur

★ Pas de création de processus séparé

★ Meterpreter travaille exclusivement en mémoire

- Autopsie ? Quelle autopsie ?
- Bye-bye chroot ...

VNC

★ Vous préférez une interface graphique ?

★ Utilisez la charge utile VNC !

- Pas de création de processus séparé

NOPs

★ Les instructions NOPs (No Operation) améliorent la probabilité d'atteindre la charge utile

★ 4 types de NOPs (3.0 bêta 3)

Encodeurs

★ 17 encodeurs (3.0 bêta 3)

★ Majuscules, minuscules, mélange des deux, Unicode, substitution de variables Shell ...

Modules Auxiliaires

★ 17 modules auxiliaires (3.0 bêta 3)

★ Utilitaires MSSQL, Détection de bannière, Détection de services UDP, Suppression de fichiers via LPD sous Solaris, Attaques de réseaux sans-fil ...

Interfaces

★ Plusieurs interfaces "utilisateur"

★ Ligne de commande, mode interactif, et même un serveur Web en ERb/ Ajax

★ IDE Web disponible

Exploits | Auxiliaries | Payloads | Encoders | Nops | Sessions | Jobs | IDE | Help

Available Exploits

SEARCH Linux

Matched 8 modules for term *Linux*

Icecast (<= 2.0.1) Header Overwrite (win32)

This module exploits a buffer overflow in the header parsing of icecast, discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable). !! This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won't be decremented. This means for each time your payload exits, the counter will be left incremented, and eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.

Oracle 9i XDB FTP PASS Overflow (win32)

By passing an overly long string to the PASS command, a stack based buffer overflow occurs. David Litchfield, has illustrated multiple vulnerabilities in the Oracle 9i XML Database (XDB), during a seminar on "Variations in exploit methods between Linux and Windows" presented at the Blackhat conference.

Oracle 9i XDB FTP UNLOCK Overflow (win32)

By passing an overly long token to the UNLOCK command, a stack based buffer overflow occurs. David Litchfield, has illustrated multiple vulnerabilities in the Oracle 9i XML Database (XDB), during a seminar on "Variations in exploit methods between Linux and Windows" presented at the Blackhat conference. Oracle9i includes a number of default accounts, including dbsnmp:dbsmp, scott:tiger, system:manager, and sys:change_on_install.

Oracle 9i XDB HTTP PASS Overflow (win32)

This module exploits a stack overflow in the authorization code of the Oracle 9i HTTP XDB service. David Litchfield, has illustrated multiple vulnerabilities in the Oracle 9i XML Database (XDB), during a seminar on "Variations in exploit methods between Linux and Windows" presented at the Blackhat conference.

PeerCast <= 0.1216 URL Handling Buffer Overflow (linux)

This module exploits a stack overflow in PeerCast <= v0.1216. The vulnerability is caused due to a boundary error within the handling of URL parameters.

RealServer Describe Buffer Overflow

This module exploits a buffer overflow in RealServer 7/8/9 and was based on Johnny Cyberpunk's THCrealbad exploit. This code should reliably exploit Linux, BSD, and Windows-based servers.

Snort Back Orifice Pre-Preprocessor Remote Exploit

This module exploits a stack overflow in the Back Orifice pre-processor module included with Snort versions 2.4.0, 2.4.1, 2.4.2, and 2.4.3. This vulnerability could be used to completely compromise a Snort sensor, and would typically gain an attacker full root or administrative privileges.

Démonstration

(Et priez pour que Murphy ne soit pas dans la salle)

Conclusion, Références (et Autres Sujets)

Un Equilibre des Forces ?

★ Excellent outil d'attaque

- Création rapide d'attaques ciblées fiables

★ Bon outil de défense

- Testez votre S.I.

Indicateur pour les Défenseurs

Références

★ Counter Hack Reloaded. SKOUDIS (Ed), 2nd Edition, Prentice Hall, 2006

★ Metasploit Reloaded, MOORE (H.D.), BreakingPoint Systems, Black Hat 2006

★ Metasploit 3.0 Developer's Guide, The Metasploit Staff

Ressources

★ http://www.Metasploit.com/projects/Framework/mailinglist.html

★ http://lists.immunitysec.com/mailman/listinfo/dailydave

Remerciements

★ Jérôme Léonard (a.k.a. mitch) pour la relecture

★ Wolfgang Haffner et Mamadou Diabaté pour la musique

★ Et à toute l'assistance pour nous avoir écouté !

Intervenants

★ Saâd Kadhi, consultant sécurité, HAPSIS (http://www.hapsis.fr/)

★ Guillaume Arcas, consultant sécurité indépendant

Informations Utiles

★ Vous pouvez télécharger cette présentation en ligne

- http://saad.docisland.org/docs/

★ Questions ? Commentaires ?

- saad@docisland.org ||
  yom@retiaire.org

Licence

★ Creative Commons Attribution-NonCommercial 2.5

- http://creativecommons.org/licenses/by-nc/2.5/

★ Sauf le logo Metasploit, propriété de Metasploit LLC