Metasploit

BONDUE Emeric
LECOQ Simon

Un bref historique

2003
Création par H. D. Moore

2007
Perl → Ruby

ruby

2009
Acquisition par Rapid7

RAPID7

A quoi sert Metasploit ?

Aider les experts des technologies de l'information à :

Identifier
Les failles et vulnérabilités

Evaluer
Les risques liés

Renforcer
La sécurité de l'infrastructure

Que peut faire Metasploit ?

Liste non exhaustive :

- Scans
- Exploitation
- Social engineering
- Bruteforce
- Audits de sécurité
- Moultes autres fonctionnalités...

Metasploit en chiffres

1800+
Exploits

540+
Payloads

580+
Contributeurs

Exploits sur de nombreuses plateformes :

AIX, Android, BSD, BSDi, Cisco, Firefox, FreeBSD, HPUX, Irix, Java, JavaScript, Linux, mainframe, multi (applicable to multiple platforms), NetBSD, NetWare, nodejs, OpenBSD, OSX, PHP, Python, R, Ruby, Solaris, Unix, and Windows

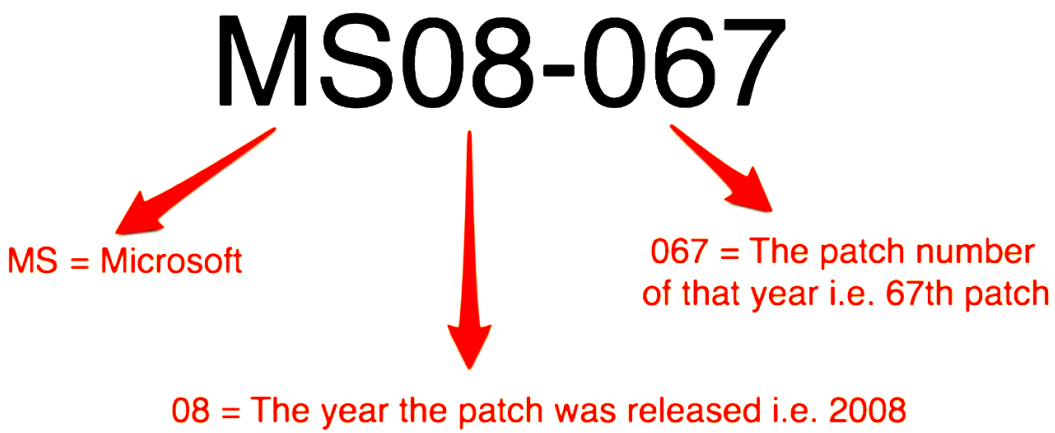
Petit récapitulatif

- La “boîte à outils” du pen-testeur
- Une immense bibliothèque d’exploits, de payloads, de modules auxiliaires etc…
- Un ensemble de fonctionnalités réunies en un seul framework
- Permet de combiner différents modules très rapidement

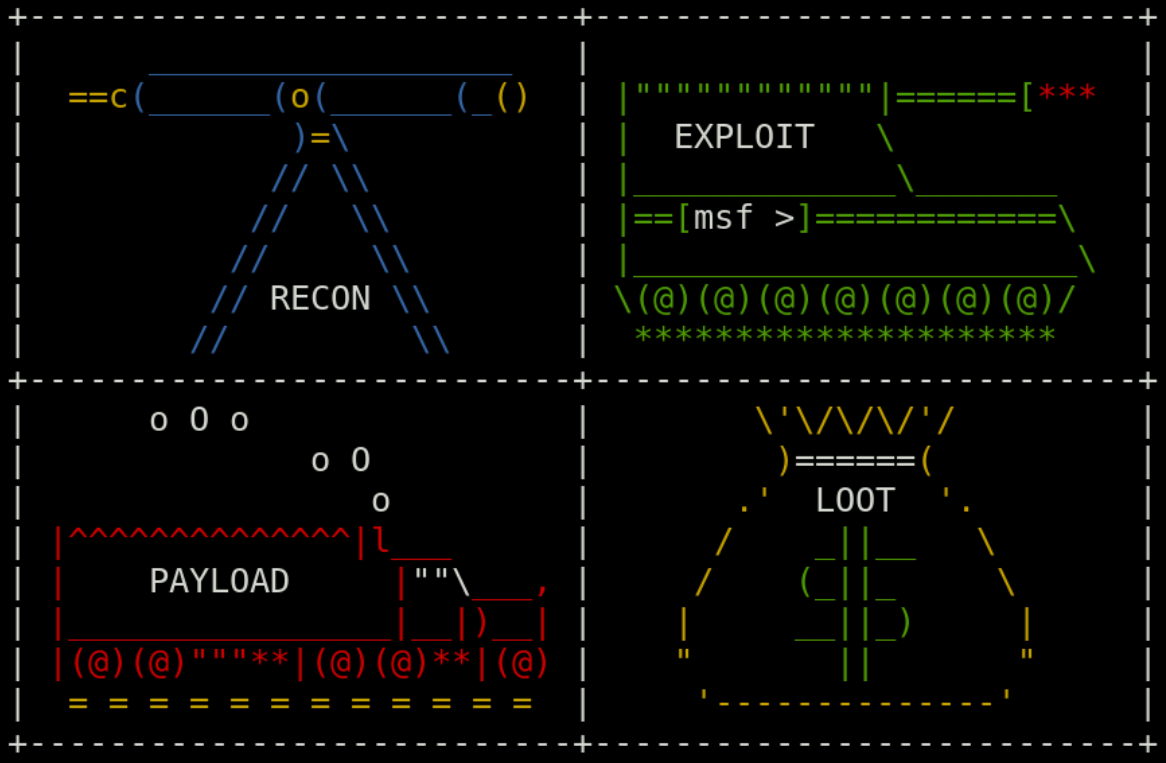
Common Vulnerabilities and Exposures (CVE)

Dictionnaire des informations publiques relatives aux vulnérabilités de sécurité

Système de notation universel : CVE-AAAA-NNNN (Ex : CVE-2008-4250)



Quelques définitions



Étapes basiques pour exploiter un système

1. Choisir et configurer un exploit
2. Vérifier si la cible est vulnérable à l'exploit
3. Choisir et configurer un payload
4. Encoder le payload
5. Exécuter l'exploit

Les outils additionnels

- Scan de ports : Nmap / Zenmap
- Scan de vulnérabilités : Nessus / OpenVas / Nexpose
- Social Engineering : SEToolkit / Maltego
- Décryptage de mot de passe : John The Ripper / Crackstation
- Sniffing : Wireshark / Ettercap

Démonstration