



7. Exploatarea vulnerabilităților



Exploit-uri de securitate

- **Program special conceput pentru a exploata vulnerabilitățile de securitate existente pe sistemele de calcul cu scopul compromiterii securității acestora**
 - obținerea accesului în sistem, escaladarea privilegiilor, blocarea funcționării, etc
- **Remote vs local exploits**
- **Public vs private exploits**
 - underground world
- **Dezvoltarea de exploit-uri necesită cunoștințe avansate de programare**
 - C/C++, perl, python

Exploit-uri de securitate (cont.)

- **EXPLOIT = VULNERABILITY + PAYLOAD**
- **Payload - codul ce se dorește a se executa pe calculatorul țintă la activarea vulnerabilității**
 - scris în limbaj de asamblare (ASM)
- **Funcționează, de regulă, numai pentru un anumit tip de platforma (Win32 , Linux)**
- **Tipuri diferite de payload-uri:**
 - **exec** → Execute a command or program on the remote system
 - **download_exec** → Download a file from a URL and execute
 - **upload_exec** → Upload a local file and execute
 - **adduser** → Add user to system accounts
 - **shell** → Provide an interactive shell
 - bind shell
 - reverse shell
- **Exemplu: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (CVE-2008-4250)**

Site-uri ce conțin exploit-uri

- SecurityFocus (<http://www.securityfocus.com>)
- Exploits Database (www.exploit-db.com)
- Milw0rm (<http://www.milw0rm.com>) – closed!
 - inj3ct0r.com
- Packet Storm (<http://packetstormsecurity.org>)

- BackTrack
 - folderul /pentest/exploits

SecurityFocus

SecurityFocus - Windows Internet Explorer

http://www.securityfocus.com/vulnerabilities

SecurityFocus

Find: MS08-067 Previous Next Options

SecurityFocus™

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

Vulnerabilities (Page 1 of 1376) 1 2 3

Vendor: Select Vendor

Title: Select Title

Version: Select Version

Search by CVE

CVE:

Submit

Mono 'loader.c' Library Loading Local Privilege Escalation Vulnerability
2010-11-12
<http://www.securityfocus.com/bid/44810>

Visual MP3 Splitter & Joiner Multiple Buffer Overflow Vulnerabilities
2010-11-12
<http://www.securityfocus.com/bid/42317>

Adersoft VbsEdit '.vbs' File Denial Of Service Vulnerability
2010-11-12
<http://www.securityfocus.com/bid/42525>

Internet 125%

Exploit frameworks

- Metasploit Framework (<http://www.metasploit.com>)
- LibExploit (<http://nixbit.com>)
- Inguma (<http://inguma.sourceforge.net/>)
- Attack Tool Kit (<http://www.computec.ch/projekte/atkl/>)

- CORE IMPACT (<http://www.coresecurity.com>)
- Immunity CANVAS (<http://www.immunitysec.com>)
- SAINT (<http://www.saintcorporation.com/>)

- Specifice unei categorii de aplicații:
 - Orasploit (Oracle)
 - BeEF (Browser Exploitation Framework)
 - W3af (Web Application Exploit Framework)

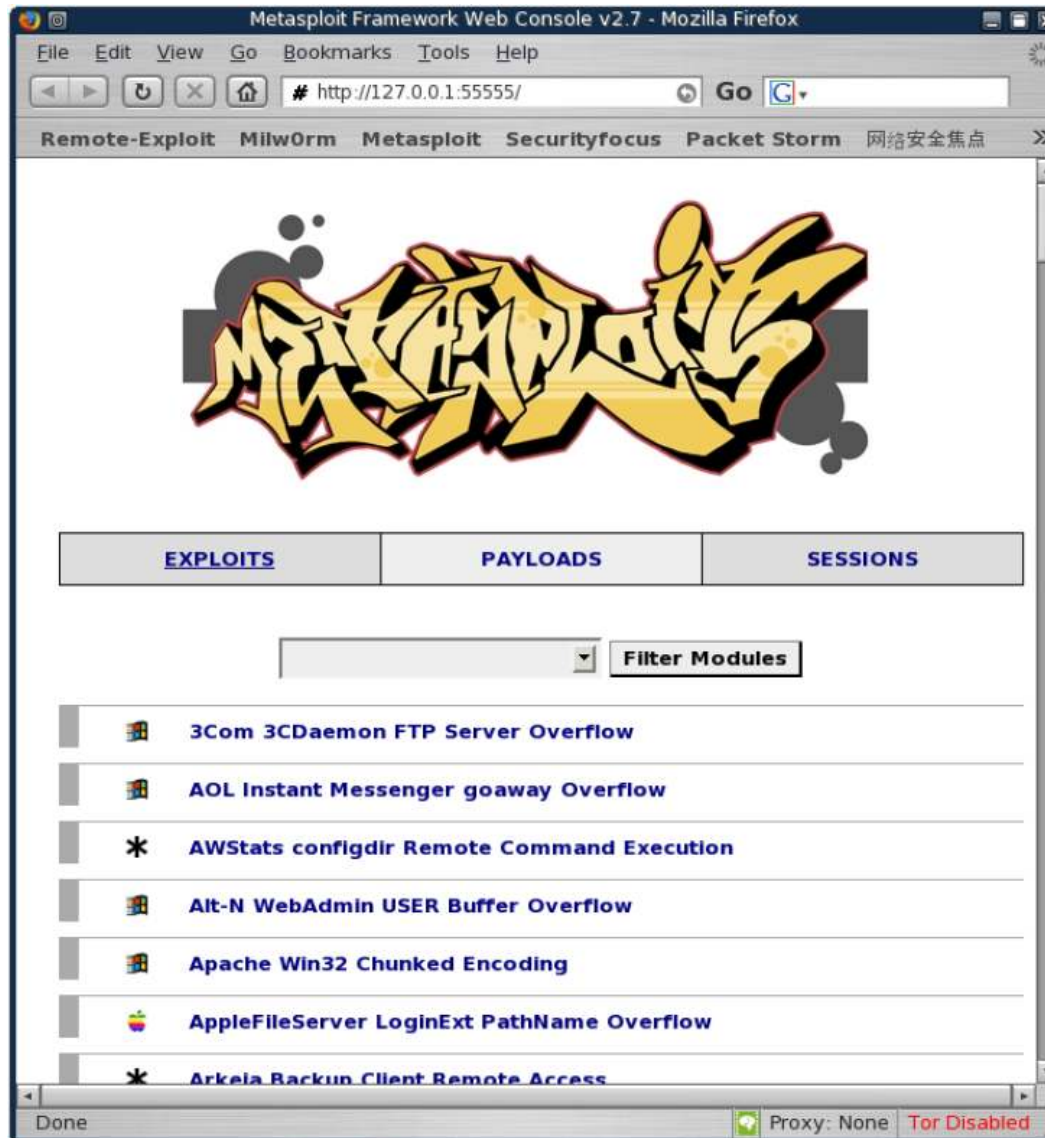
Metasploit Framework

- **Proiect open-source**
- **Scopul proiectului:**
 - platformă pentru dezvoltarea, testarea și utilizarea exploit-urilor de securitate
 - folosit pentru efectuarea de teste de penetrare sau pentru studierea vulnerabilităților
- **Creat de HD Moore în 2003 folosind Perl**
- **Rescris ulterior în Ruby (OOP, sintaxă inspirată din Perl și funcționalități similare cu Smalltalk)**
- **Disponibil pentru Linux și Windows (Cygwin)**
- **Achiziționat de către firma Rapid7, în 2009 (<http://www.rapid7.com>)**
 - versiuni comerciale Metasploit Express și Metasploit Pro
- **Modular și extensibil**
 - crearea de noi exploit-uri
- **Versiunea curentă: 3.5.0**

Metasploit Framework (cont.)

- **Metasploit Command Line Interface (MSFCLI)**
- **Metasploit Console (MSFCONSOLE)**
- **Metasploit Web Interface (MSFWEB)**
- **Etape:**
 - selectare exploit (pe baza rapoartelor obținute în urma scanării vulnerabilităților)
 - identificare opțiuni specifice (adresa IP țintă, port, etc)
 - selectare tip payload (exec, adduser, shell, etc)
 - lansare exploit

Metasploit Web Interface (MSFWEB)



Metasploit Framework – Autopwn

- **Exploatarea automată a vulnerabilităților**
- **Necesită o bază de date pentru stocarea informațiilor**
 - MySQL, SQLite, Postgres
- **Posibilitatea de a importa date din alte programe**
 - fișiere Nessus NBE, nmap XML
- **Posibilitatea de a rula nmap din cadrul programului și de a stoca rezultatele în baza de date**
- **Lansează exploit-uri pe baza porturilor, serviciilor și vulnerabilităților descoperite**

Metasploit Framework – Module Auxiliare

- **Meterpreter (Meta-Interpreter)**
 - crearea de module ce pot fi încărcate pe sistemul compromis
 - operează în interiorul procesului țintă (nu poate di detectat)
 - configurație client-server
- **PassiveX**
 - încărcare ActiveX-uri în interiorul procesului țintă
 - <http://www.uninformed.org/?v=1&a=3&t=pdf>
- **Win32 UploadExec**
- **Win32 DLL Injection**
- **VNC Server DLL Injection**

CORE IMPACT

- Unealtă foarte puternică
- Produs stabil (peste 2 ani vechime), dezvoltat de către o echipă de profesioniști
- Număr foarte mare de exploit-uri pentru:
 - Sisteme
 - Utilizatori
 - Aplicații Web
 - Wireless
- Prețul: peste 15,000 USD



CORE IMPACT (cont.)

The screenshot displays the CORE IMPACT interface during a penetration test. The main window is titled "Sample Penetration Test - CORE IMPACT".

Entity View: Shows a tree structure starting with "localhost". Under "localhost", there is a sub-entry "localagent". Below "localagent", several IP addresses are listed: 192.168.36.0, 192.168.36.1, 192.168.36.20, 192.168.36.23, 192.168.36.28, and 192.168.36.55.

Executed Modules: A table showing the execution history of modules.

Name	Started	Fin
Information Gathering Hel...	5/19/2004 11:05:26 AM	5/19/20...
Information Gathering Hel...	5/19/2004 11:05:27 AM	5/19/20...
Information Gathering Hel...	5/19/2004 11:05:27 AM	5/19/20...
Information Gathering Hel...	5/19/2004 11:05:27 AM	5/19/20...
Information Gathering Hel...	5/19/2004 11:05:28 AM	5/19/20...
Attack and Penetration	5/19/2004 11:24:42 AM	

Executed Module Info: Shows the details of the currently selected module.

```
Running: Apache - OpenSSL SSLv2 exploit

Exploiting host: 192.168.36.23 - mode: Explo...
```

WinZip 8.0 MIME Archive File Name exploit: A detailed view of the selected module.

Brief: This module exploits a stack buffer overflow in WinZip 8.0 to install a level0 agent.

Exploits Vulnerability: NOCVE-2004-7068

Category: Exploits/Client Side

Author: CORE Security Technologies

Version: 1.3.2.1

Description: This module sends a mail with a malformed MIME archive attached. Due to the nature of the exploit its success depends on an unpredictable value, that value could be 0,1,2 or 3 and is specified in the ATTACK_VARIANT parameter, the default selection for that parameter is "Multiple", which means that four different files are sent to the victim in the same mail. It would be better to send the files in...

