7. Exploatarea vulnerabilităţilor

Exploit-uri de securitate

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

Exploit-uri de securitate (cont.)

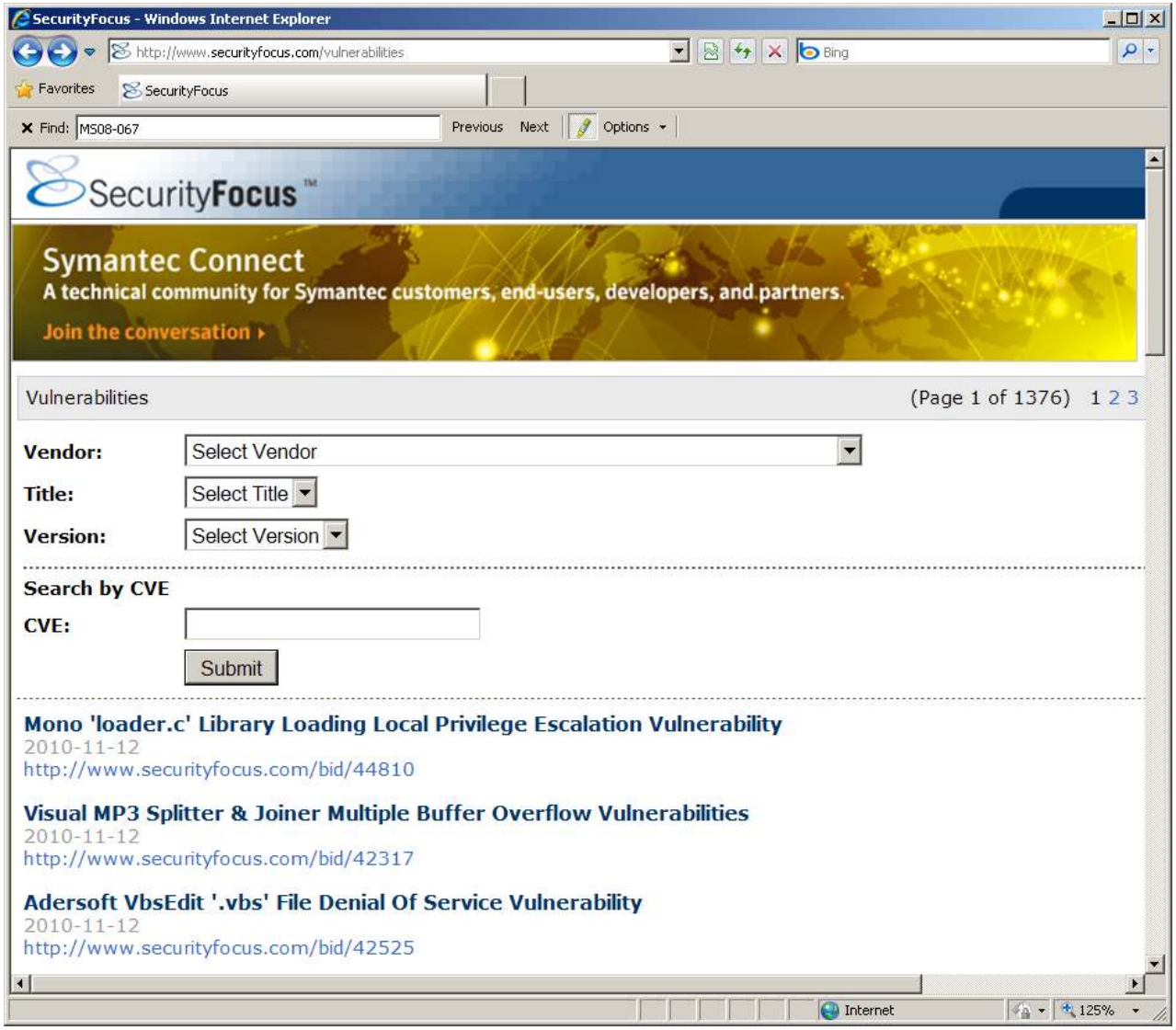
- EXPLOIT = VULNERABILITY + PAYLOAD
- Payload - codul ce se doreşte a se executa pe calculatorul ţintă la activarea vulnerabilităţii
  - scris în limbaj de asamblare (ASM)
- Funcţionează, de regulă, numai pentru un anumit tip de platforma (Win32 , Linux)
- Tipuri diferite de payload-uri:
  - exec → Execute 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 conţin 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



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/atk/)

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

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

Metasploit Framework

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

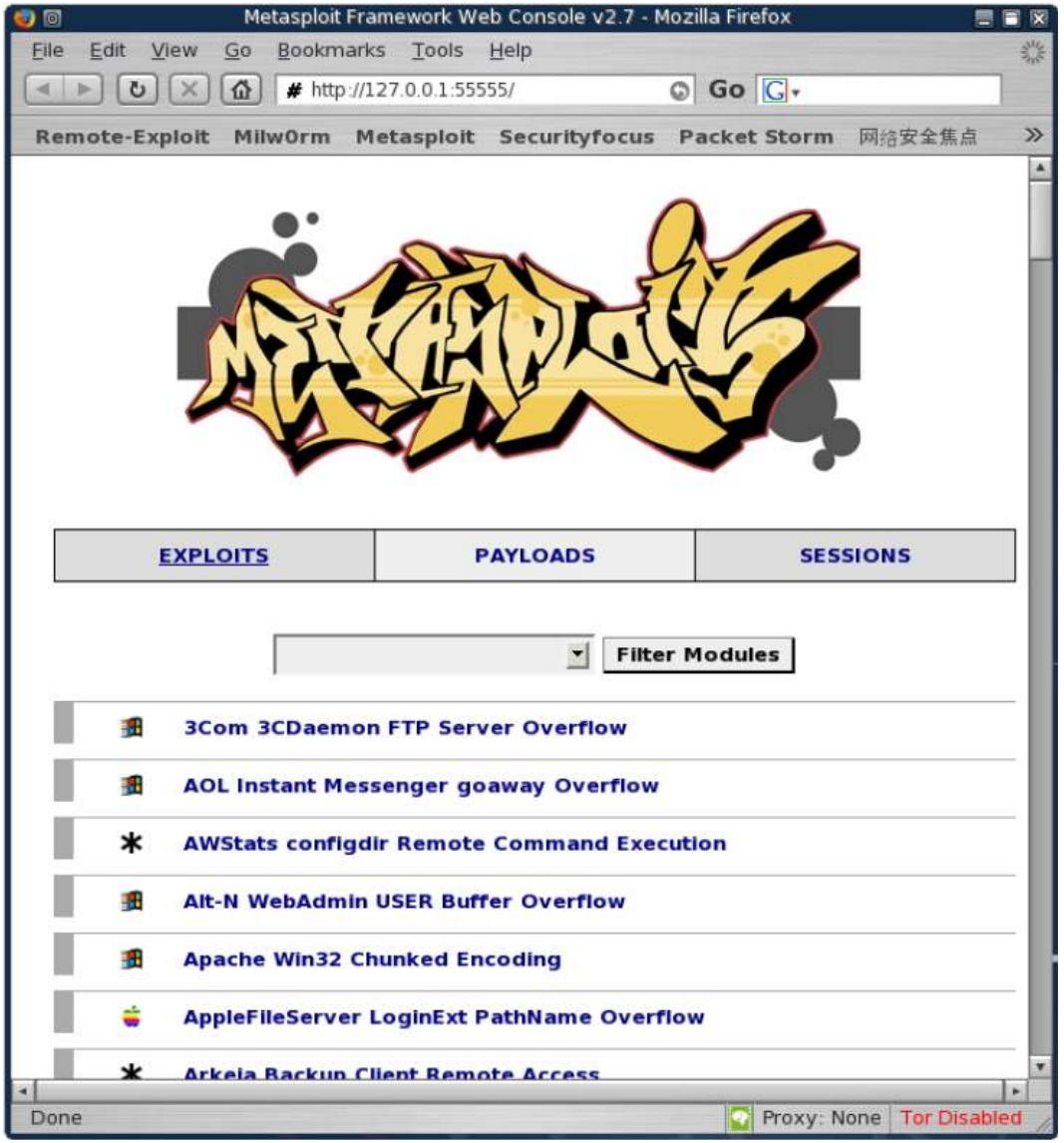
Metasploit Framework (cont.)

- Metasploit Command Line Interface (MSFCLI)
- Metasploit Console (MSFCONSOLE)
- Metasploit Web Interface (MSFWEB)
- Etape:
  - selectare exploit (pe baza rapoartelor obţinute în urma scanării vulnerabilităţilor)
  - identificare opţiuni specifice (adresa IP ţintă, port, etc)
  - selectare tip payload (exec,adduser, shell, etc)
  - lansare exploit

Metasploit Console (MSFCONSOLE)

```
bt framework2 # ./msfconsole



                  |                    |     _) |
 __ `__ \   _ \ __|  _` |  __| __ \   |  _ \   | __|
 |   |   |  __/ |   (   |\__ \ |   | | (   | | |
_|  _|  _|\___|\__|\__,_|____/ .__/ _|\___/ _|\__|
                             _|


+ -- --=[ msfconsole v2.7 [157 exploits - 76 payloads]

msf > help

Metasploit Framework Main Console Help
======================================

        ?            Show the main console help
        cd           Change working directory
        exit         Exit the console
        help         Show the main console help
        info         Display detailed exploit or payload information
        quit         Exit the console
        reload       Reload exploits and payloads
        save         Save configuration to disk
        setg         Set a global environment variable
        show         Show available exploits and payloads
        unsetg       Remove a global environment variable
        use          Select an exploit by name
        version      Show console version
```

Metasploit Web Interface (MSFWEB)



Metasploit Framework – Autopwn

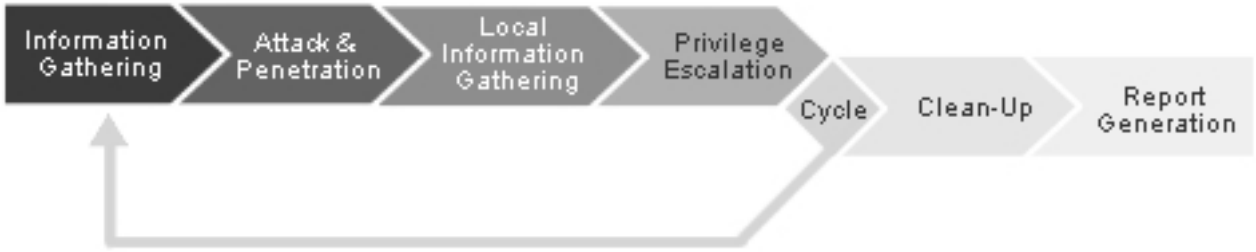
- Exploatarea automată a vulnerabilităţilor
- Necesită o bază de date pentru stocarea informaţiilor
  - MySQL, SQLite, Postgres
- Posibilitatea de a importa date din alte programe
  - fişiere Nessus NBE, nmap XML
- Posibilitatea de a rula nmap din cadrul programului şi de a stoca rezultatele în baza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

Metasploit Framework – Module Auxiliare

- Meterpreter (Meta-Interpreter)
  - crearea de module ce pot fi încărcate pe sistemul compromis
  - operează în interiorul procesului ţintă (nu poate di detectat)
  - configuraţie client-server
- PassiveX
  - încărcare ActiveX-uri în interiorul procesului ţintă
  - 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 profesionişti
- Număr foarte mare de exploit-uri pentru:
  - Sisteme
  - Utilizatori
  - Aplicaţii Web
  - Wireless
- Preţul: peste 15,000 USD



CORE IMPACT (cont.)