Automated Penetration Testing with the Metasploit Framework

NEO Information Security Forum

March 19, 2008

Topics

- What makes a good penetration testing framework?

- Frameworks available

- What is the Metasploit Framework?

- How does it work?

- Features

- Metasploit autopwn

- Limitations

- Live demonstration
  - Basic Metasploit exploit
  - Exploit multiple hosts with autopwn

What makes a good penetration testing framework?

- Platform independent
  - Install on Windows, Mac, Linux
- Good exploit collection w/regular updates
- A intuitive, robust GUI
- Ability to add new exploits
- Open source or ability to customize
- Good reporting tools

What frameworks are available?

- Metasploit Framework
- Inguma
- SecurityForest
- Attack Tool Kit
- SAINT ($)
- Immunity Canvas ($)
- CORE IMPACT ($)

Some are application or web specific…
- Orasploit (Oracle)
- PIRANA (email content filtering framework)
- BeEF (Browser Exploitation Framework)
- W3af (Web Application Exploit Framework)

What is the Metasploit Framework?

- Tool for developing and executing exploit code against a remote target machine
- Runs on Linux, Mac OS X, BSD, Windows
- Version 3.x written in Ruby. 2.x Perl
- Remote/Local exploits
  - browser exploits with self contained web server
- Ability to create exploits
- Written by HD Moore
  - Version 3.1 HD Moore, spoonm, skape

How does it work?

- Allows a user to configure exploit modules and launch them against target systems

- Choose and configure a **exploit** then select and configure a **payload**

  Payload: code that is executed on the target system if the exploit is successful (bind/reverse shell, VNC server, etc...)

- **Basic Example**
  If the exploit is successful...a payload is executed and the user is able to interact with a command shell

- **Automated Example**
  Collect host information and exploit multiple hosts (autopwn)

  – Nmap Scan, Nessus import

Features

- Choose from 269 exploits. 118 payloads. (as of the latest update)

- Web, command line, GUI interfaces, multiple sessions

- Auxiliary modules

  - Lorcon (802.11 packet injection), fuzzing, various scanners, DoS tools

- Injection into running processes (meterpreter payload)

  - Executed into memory, never touches the disk

- Create packaged executable payloads (runme.exe)

- Pivoting

  - Use compromised host to attack hosts on internal network

- IDS/IPS evasion options

Metasploit autopwn

- Automated exploit module
- Requires a database
    - MySQL, Sqlite, Postgres
- Some pre-configuration required
    - RubyGems, active record (part of ruby on rails)
    - Database configuration
- Ability to import vulnerability data
    - Nessus NBE files, Nmap XML output
- Run Nmap from the module and puts results in the database
- Launches exploits based on ports, services or vulnerabilities from imported data

Limitations of Metasploit

- Majority of exploits are for Windows

- Logging not robust, debug modes only

- Local exploits only start the web server locally
  - Need to send email on your own

- autopwn may be difficult to configure correctly

- No automated reporting in autopwn
  - Database can be queried for vulnerability data

- Basic "bind shell" only option for payload in autopwn

- Large amounts of import data slows exploits
  - Module needs tuning...hopefully fixed in future versions

More Information

- **Metasploit Web Site**
  http://metasploit.com
- **Metasploit Toolkit Book**
- **autopwn Overview**
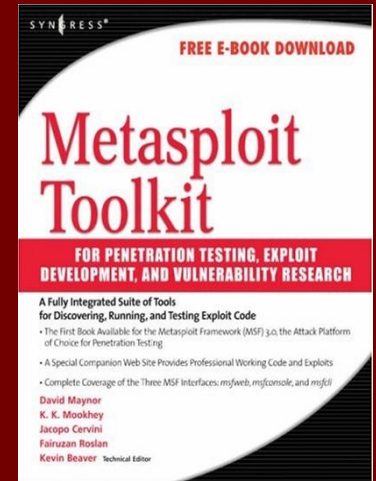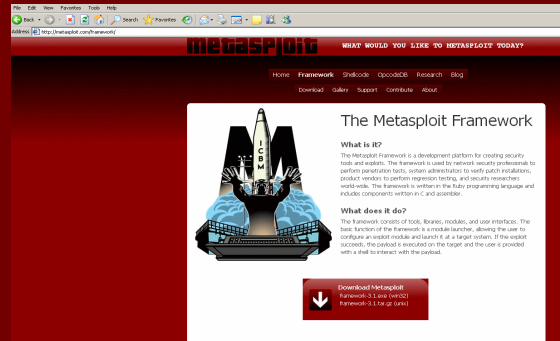 http://blog.metasploit.com/2006/09/metasploit-30-automated-exploitation.
- Want to test autopwn in a lab?

  Backtrack 2 has it working and installed (ninja script)
  Backtrack 3 beta requires fast-track.py run first...

Questions

tom@spylogic.net

Presentation posted at:

http://spylogic.net

Live Demonstration

- Lab Setup
  - VMware Workstation
  - 3 Windows Systems
    - 1 Windows 2000 Srv, 2 Windows XP Pro

- Basic Metasploit exploit
  - Show basic commands

- Exploit multiple hosts with autopwn
  - Using Nessus vulnerability data