



metasploit

PRIME

H D Moore <hdm [at] metasploit.com>

metasploit

Project lead

BreakingPoint Systems

Director of BreakingPoint Labs

egypt <egypt [at] metasploit.com>

metasploit

Core developer

< censored >

...

The Metasploit Project

- **Exploits and tools since 2003**
 - Focus on sharing information
 - Driven by the community
 - Destroyers of FUD
- **Project promotion and support**
 - Make new research accessible
 - Hosting, SVN, code sharing

The Metasploit Framework

- **An exploit development platform**
 - Designed for research and testing
 - Also useful for penetration testing
- **Tons of exploit modules**
 - Windows, Linux, BSD, Solaris, AIX, IRIX
- **Free to use, but restricted***

* EULA-like license, anti-commercial, prevent sales

Metasploit 3.1

- **Released in January 2008**
 - METASM, MSFGUI, Lorcon, Scruby
 - Kernel Payloads, WiFi Exploits
 - 450 modules (265 exploits)
 - 150,000~ lines of Ruby

Metasploit 3.2

- **Officially an open-source project**
 - Released under 3-clause BSD license
 - Wide open license (sell, rename, fork)
- **New development team**
 - egypt, mc, hdm
 - ramon, patrickw, l)ruid, et, pusscat
 - -skape -spoonm

Metasploit 3.2

- **Massive amount of new code**
 - 577 modules (300+ exploits)
 - 300,000 lines of Ruby
- **Consolidates 10 months of work**
 - DNS Spoofing, Byakugan WinDBG Ext
 - Context-map payload encoding
 - Tons of bug fixes and new options

Module Format

- **Simplified module structure**
 - Not backwards compatible
 - Faster to load and cache
 - Location agnostic
- **Minor, few-line change**
 - Scripted with `tools/convert31.rb`

Meterpreter Updates

- **Luke Jennings's Incognito**
 - Token stealing and impersonation
 - Escalate privileges (system->domain)
 - Hijack misplaced tokens
- **API updates and bugfixes**
 - More reliable, better tested

Raw Packet Tools

- **Updated PcapRub library**
- **Scrubby improvements**
 - Dot11 patches from Robin Wood
 - Bugfixes and usability changes
- **Tod Beardsley's PacketFu**
 - Fast and simple to TCP/IP library

METASM Updates

- **Support for the MIPS platform**
 - New MIPS payloads
 - New MIPS encoders
- **Compile C directly to shellcode**
 - Write payloads and encoders in C
 - Compile at runtime

Better NX Support

- **NX stagers are now default**
 - Bigger, but more reliable
- **Generated EXEs support NX**
 - Useful for remote access / social eng.
- **Meterpreter updated for NX**
 - Less breakage on 2003 / Vista

EXE Template

- **WinMain written in assembler**
 - ~1500 byte executable
- **Stores payload in .rdata segment**
 - VirtualProtects it to RWX at runtime
- **Avoids all those annoying AVs**
 - We love VirusTotal.com

Javascript Obfuscation

- **Strings**

- “hello”

- “\x68\x65\x6c\x6c\x6f”

- unescape(“%68%65%6c%6c%6f”)

- String.fromCharCode(...)

- **Better handling of spaces**

Javascript OS Detection

- **Jerome Athias**
- **Uses IE's ScriptMajorVersion and ScriptMinorVersion**
- **Reliably detects browser, OS, and service pack**
 - Even if the UA is spoofed

Javascript OS Detection (cont)

- Falls back to browser parsing bugs
 - This should be familiar to web developers
- If that doesn't work, use the UA

Browser Autopwn

- Fires up a ton of browser exploits and SMBRelay
- OS detection in javascript
- Falls back to server-side UA string

Metasploit-in-the-Middle

- **Used with existing MITM techniques**
 - ARP, WPAD, Wireless, DNS
- **Suite of protocol capture services**
 - SMB, HTTP, IMAP, POP3, SMTP, FTP
- **Abuse the HTTP security model**
 - Steal cookies and saved form data

Karmetasploit

- **Evil Wireless Access Point**
 - Hijacks all WiFi clients in range
 - Re-beaconing of probe requests
- **Airbase-NG + Metasploit 3.2**
 - Any WiFi card that supports injection
 - Combines all of the MITM services
 - Effective on planes, hotels, cafes

Reflective DLL Injection

- **Stephen Fewer's new system**
 - Harmony Security
- **Re-implements PE loader in C**
 - Skape/JT's patches existing loader
 - Reflective re-implements it
- **Prepended to DLL as a stub**

Full IPv6 Support

- **Rex::Socket reimplemented**
 - RangeWalker, CIDR, nto*() ato*()
- **Use IPv6 with any Exploit / Auxiliary**
- **New IPv6 stagers for Windows**
 - Meterpreter
 - VNCInject

WMAP

- **Efrain Torres's new project**
 - Web assessment as auxiliary modules
 - Run modules by hand or automated
- **Still early stages**
 - Expect a big announcement soon!

PHP

- **Payloads for bypassing disabled_functions**
- **Encoders for bypassing magic_quotes_gpc**
- **New findsock for PHP / Apache**

Summary

- **Metasploit 3.2 is Awesome!**
- **Release in 1-2 weeks**
- **Early access in SVN tree**
 - <http://metasploit.com/svn/framework3/trunk/>

QUESTIONS ?