

metasploit

6 years later

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

metasploit

Project lead

BreakingPoint Systems

Director of Security Research

Beginnings

Metasploit started in June of 2003

- Initial resource was the Opcode Database
- Releasing a few of exploits (dcom, sadmin)
- Launched the Metasploit Framework (1.0)

A fight against anti-disclosure

- Share exploit knowledge with everyone
- Prevent OIS from killing public code
- Turn exploits into standard security tools

Early Days

Metasploit Framework Alpha

- A MUD-like ncurses video game in Perl
- The game you could play anywhere

Metasploit Framework 1.0

- Only 11 exploits and a few payloads
- Still a ncurses-based console
- Generated a lot of criticism

Getting Started

Metasploit 2.0

- A complete rewrite of the original Perl
- Spoonm joined the development team
- Created something actually useful

Metasploit 2.2

- Introduction of advanced payloads (meterpreter)
- Skape joined the development team
- Major ramp on development speed

Transition

Metasploit 2.7

- The last stable release of the Perl version
- Still useful today for a couple modules
- About 44,000 lines of code

Metasploit 3.0

- Complete, from-scratch, rewrite in Ruby
- Created Metasploit LLC to own the rights
- Released under mostly-free license

Expansion

Metasploit 3.1

- Spoonm and Skape no longer active
- Released under the BSD license
- About 150,00 lines of code (450 modules)

Metasploit 3.2

- New core developers (egypt, mc) (+5 more)
- About 300,000 lines of code (577 modules)
- Major updates for IPv6, NX, Vista, PHP, etc

Today

Metasploit is now a “big” project

- Mentioned in 210+ books and 16,000+ blogs
- Almost 419,000 lines of code (796 modules)
- 73,000+ unique IPs updated via SVN (2009)
- 650,000+ unique IPs hit the web site (2009)
- Largest Ruby project in the world
 - <http://ohloh.net/p/metasploit>

Purpose

Changing focus from exploits to tools

- Exploits are still strongly supported
- More auxiliary modules (175+ now)
- Focus on MITM, WiFi, Fuzzing, Web Apps

A vehicle for distributing research

- Integrate the latest security research
- Instantly distribute this to 50,000+ people
- Make it understandable and maintainable

Tomorrow

Developers tend to be niche-focused

- Only a couple folks looking at the core
- I do less development, more integration
- Tons of projects running in parallel...

Database Exploitation

Extensive set of Oracle exploits

- SQL injection flaws, priv escalation, overflows
- Support for Metasploit payloads via Oracle
- Headed up by MC and Chris Gates
- Much more about this at Defcon
- MC's personal site has more
 - <http://metasploit.com/users/mc/>

Web Applications

WMAP is starting to come together

- A modular web app assessment system
- Launch modules individually or automatically
- Headed up by Efrain Torres
- Even more about this at Defcon
- Integrates with SQLMap and Nikto
- Support for recent attacks
 - WebDAV + Unicode
 - Automated SQL injection

Client-Side Exploitation

Browser AutoPWN

- Automatically exploit any web browser
- Headed up by Egypt (more at Defcon)
- Handles obfuscation and no-script

File format exploitation

- PDF is well supported, working on Office docs
- Extensive evasion capabilities

Reflective DLL Injection

Alternate in-memory DLL loading

- Added by Stephen Fewer of Harmony Security
- Reimplementation of the Win32 DLL loader
- Less fragile and easier to “stage”

Tested for the last 8 months

- Only a few minor issues left to solve
- Switching all DLL injection payloads
 - Metepreter, VNC, etc

Meterpreter

Expanded automation capabilities

- Improved the API and example scripts
- Carlos Perez has added dozens
 - Grab data, install RDP, browser credentials

Meterpreter core getting an overhaul

- New keyboard, video, audio sniffing features
- Adding a multi-threaded socket engine
- Adding a remote Ruby interpreter

Meterpreter Everywhere

Mac OS X “machterpreter”

- Written by Charlie Miller and Dino Dai Zovi
- Should be integrated “soonish”

Meterpretux for Linux/POSIX

- In the works for almost 3 years

Meterpreter for PHP

- Developed by Egypt, more at Defcon

Support for Ruby 1.9.1

Huge speed improvements

- 3.2 took ~15 seconds to initialize
- 3.3-dev is down to ~8 seconds
- Ruby 1.9.1 brings this down to ~4
- Still room for code optimization

Looking at alternate interpreters

- IronRuby on Microsoft .NET (Silverlight)
- JRuby on Java (Applets)

Executable Hackery

Created scrambled Win32 EXEs

- Important for AV bypass with exploits
- Ties in with “persistent” shellcode
- Client-side exploits require these

Embedding shellcode into EXEs

- Standard viral “infection” of executables
- Powerful when done via MITM (Karmetasploit)
- Working on “signed” changeable EXEs

Windows 7

Changed the module list in PEB

- Breaks all current Metasploit shellcode
- Requires a minor fix to be integrated

Security model support

- Updating Meterpreter and VNC to work
- Fixes apply to Vista too in some cases
- Signed executables will be necessary
- Signed SMB communication as well

Product Integration

Working with third-party products

- Using Metasploit to verify assessment data
- Using Metasploit to inject remote agents
- Both open source and proprietary
- Announcements soon!

Working with third-party developers

- Opening the door to “commercial” modules
- Metasploit as a standard exploit platform

More Product Integration

Maltego transforms for data mining

- Run Metasploit modules from Maltego
- Leverage the output to build models
- Ex. Dump a remote user list from a server

Netifera agents as payloads

- Use Metasploit to inject a remote Java agent
- Leverage Netifera to explore the network
- Relay Metasploit through Netifera

Task-based Interfaces

Metasploit is currently module focused

- Basically just a gigantic bag of tools
- Advanced uses require scripting

Custom web consoles for tasks

- Create and control client-side campaigns
- Monitor and control Karmetasploit
- Intelligence gathering and network sniffing
- Manage large numbers of shells

Other Wireless Technology

DECT

- Used by portable telephones and other gear
- Complete Metasploit integration soon
- Everything done but call recording

Zigbee

- Used by smart grid and other utility devices
- Lorcon support happening right now
- Integration with Metasploit this year

Remote XMLRPC Daemon

Interact with remote Metasploit nodes

- Support for SSL and authentication
- Extensive API allows for almost anything
- Even better with Java/.NET/Ruby 1.9

Launch attacks from other networks

- Really powerful with Metasploit-in-an-Applet
- Use browsers as attack sources

OpenVAS Server Mode

OpenVAS (forked Nessus 2)

- Use Metasploit as an OpenVAS server
- Existing OpenVAS client can “scan” for shells
- Leverage the OpenVAS reporting system
- Export Metasploit data in OpenVAS formats

File View Task Scope Report Help



Name High Medium Low

Global Settings

Global Settings

Comments Options Report

General

Plugins

Credentials

Microsoft DNS RPC Service extractQuote

Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)

This module is Copyright (C) 2009 Metasploit LLC

Family: Exploits: Windows

Category: infos

OpenVAS NVT OID: metasploit.exploits.windows.dcerpc.msdns_zonename

Plugin Version: 6479

Plugin description:

This module exploits a stack overflow in the RPC interface of the Microsoft DNS service. The vulnerability is triggered when a long zone name parameter is supplied that contains escaped octal strings. This module is capable of bypassing NX/DEP protection on Windows 2003 SP1/SP2.

Signatures:

NVT is not signed.

Set plugin timeout...

Show dependencies

 Close

Plugin selection

Name	Warning
Mercury/32 <= 4.01b LOGIN Buffer Overflow	
Mercury/32 <= v4.01b PH Server Module Buffer Overflow	
Mercury/32 v4.01a IMAP RENAME Buffer Overflow	
Microsoft ASN.1 Library Bitstring Heap Overflow	
Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)	
Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)	
Microsoft DirectX DirectShow SAMI Buffer Overflow	
Microsoft IIS 4.0 .HTR Path Overflow	

381 plugins; 381 enabled

No filter active

Filter...

Enable all

Disable all

Expand all

Collapse all

Dependencies: Enable at runtime Silent Automatically enable new plugins

Connection: root@127.0.0.1

Analog Telephony

Wardialing with Metasploit

- Full-blown dialer already in the SVN tree
- Works with a real modem using ATA/Analog
- Nudge strings, banner detection, etc
- Can be distributed using a shared DB
- More on this by I)ruid at Defcon

Digital Telephony

Wardialing with WarVOX (warvox.org)

- A mostly-unrelated side project of Metasploit
- Dials using VoIP and records the audio
- Post-processes the audio to detect things
- Dialed over 10,000+ numbers in 3 hours

A new spin on telephone audits

- Detects insecure PBXs, voicemail lines, tones
- Great detection for modems, faxes, etc

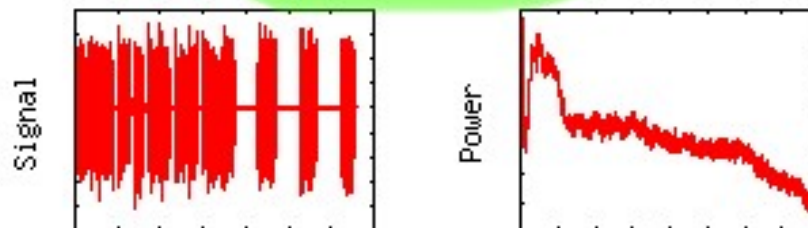
Number



CallerID: [REDACTED]
Provider: Vitely
Audio: 66 Seconds
Ringer: 33 Seconds

Signal

VOICEMAIL-OPEN



Seconds

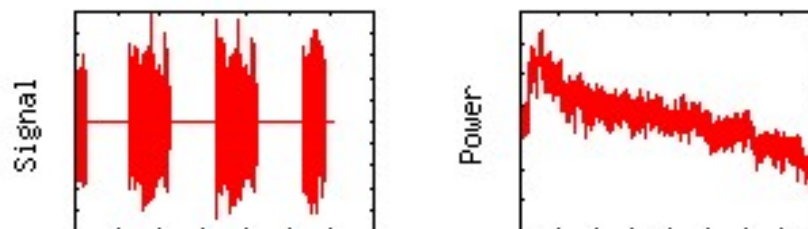
Frequency

AT&T Voicemail Deleted Messages (6002@28)
AT&T Voicemail Deleted Messages (6003@27)
AT&T Voicemail Deleted Messages (6001@22)
AT&T Call Has Been Forwarded (4005@22)
AT&T Voicemail Access (6009@17)
AT&T Voicemail Access (6015@16)
AT&T Voicemail (4027@15)
Invalid Number (1001@15)



CallerID: [REDACTED]
Provider: Vitely
Audio: 30 Seconds
Ringer: 31 Seconds

VOICEMAIL



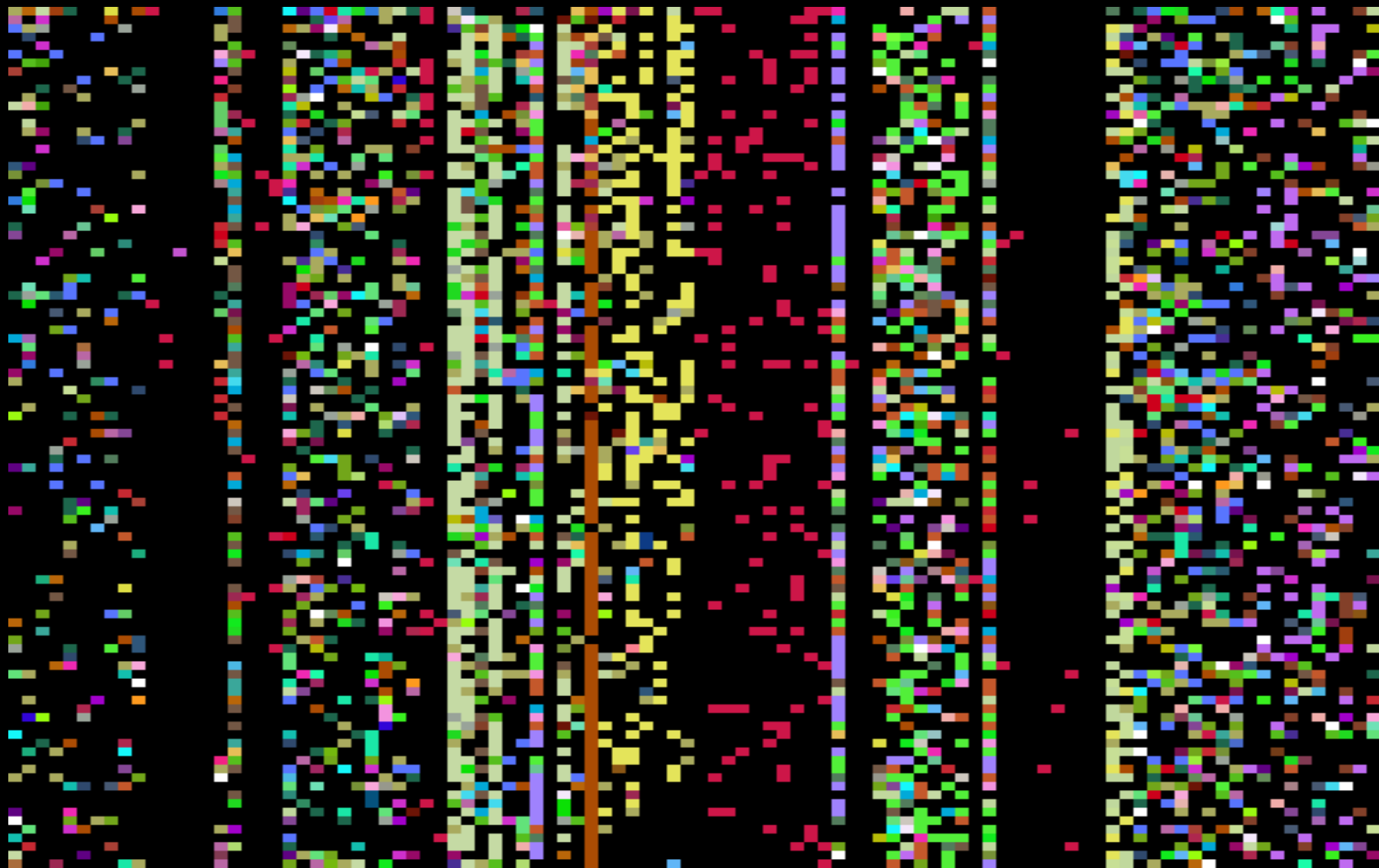
Seconds

Frequency

AT&T Voicemail Enter Password (6011@36)
AT&T Call Has Been Forwarded (4005@29)
AT&T Voicemail Enter Password (6006@21)
AT&T Voicemail Access (6009@15)

VOICEMAIL-OPEN

Grouping by Peak Frequency



QUESTIONS ?