
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, I)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 Jenning'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**
- **Scruby 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/

Exploiting IPv6

- The Internet is running out of addresses
  - Specifically ASIA
- Government mandate for IPv6 support
  - June 30, 2008. IPv6 on backbones
- Networking vendors supporting IPv6
  - Slower, buggier, incomplete (IPSEC).
- Consumer operating systems
  - Default: Vista, OS X, Ubuntu
  - Supported: XP, Linux, BSD

- Nobody actually cares*
  - Very little market demand
  - A “checkbox” feature
  - Few real endpoints

* Except Asia, US Government, Internet2

- IPv6 is already here, sorta.
  - IPv6 is deployed at the backbone level
  - IPv6 is deployed at the consumer level
  - ISPs are the only missing link
  - Tunnel services bridge this

Hacking IPv6

- Finding “public” IPv6 systems
  - Network sweeping is infeasible (64 bit subnets)
  - Discovery depends on DNS, known addresses
  - Look for AAAA records for known sites
  - Otherwise you are SOL...

Hacking IPv6

- Port scanning “public” IPv6 systems
  - No raw IPv6 port scanners (Nmap works OK)
  - Nmap depends on native IPv6 stack
  - UDP probes... just Nmap.
  - Other IPv6 tools
    - ping6 (ping, just plain ping)
    - netcat6 (fork of the old netcat tool)
    - ncat (nmap's netcat replacement)
    - socat (supports ipv6 and tons more)

Hacking IPv6

- Exploiting “public” IPv6 systems
  - Exploits can be ported or relayed
    - xinetd, socat, ncat, proxies, etc
  - Shellcode just kinda sucks
    - Bind, Reverse code needs to be ported
    - Reverse needs to support link-local

Hacking IPv6

- Firewalls and IPv6
  - Some firewall products work
    - Windows Firewall
    - Norton Internet Security 2009 Beta
  - Some firewall products don't
    - ZoneAlarm
    - IPTables (without specific IPv6 rules)
  - IPS products a mixed bag
    - Support for some sigs, some transports
    - 6in4, Toredo, tunnel services, etc

Practicality

- What would you pen-test?
  - Few orgs run IPv6 servers
  - Host discovery is hard
- Firewalls and public servers
  - Do they firewall IPv6 correctly?
  - Look for AAAA DNS records
- OK, now what...
  - This might be useful someday
  - But who cares now?

Local IPv6 Networks

- IPv6 and Modern Operating Systems
  - Vista, Mac OS X, Ubuntu, Solaris
    - Link-local and Site-local addresses
  - Linux distros

    ```
    # modprobe "ipv6"
    ```
  - Windows XP

    ```
    C:\> ipv6 install
    ```
- Tons of networking gear
  - Cisco switches, routers
  - NAS storage devices

Link-Local and Auto-Configuration

- IPv6 interfaces have default addresses
  - **FE80**:0000:0000:0000:**XXXX**:**XX**FF:FE**XX**:**XXXX**
  - **2000**:0000:0000:0000:**XXXX**:**XX**FF:FE**XX**:**XXXX**
- Link-local prefix is FE80::EUI-64
- Site-local prefix is 2000::EUI-64
  - EUI64: Ethernet MAC address + 2 bytes
- Magic broadcast addresses
  - FF02::1 is link-local all nodes (FF02::2 is routers)
  - FF05::1 is site-local all nodes

IPv6 Local Discovery

- ARP is replaced by Neighbor Discovery
  - ICMPv6 with special broadcast addresses
  - **`# ping6 -I eth0 FF02::1`**
- THC Attack Toolkit's “alive6”
  - Send 3 probes to detect local IPv6
  - **`# alive6 eth0`**
- Work network, we don't use IPv6...
  - Over 30 active IPv6 hosts
  - One active IPv6 router

IPv6 Broadcast + UDP

- IPv4 UDP Services
  - Most listen on 0.0.0.0::PORT
  - Handle all unicast requests
- IPv6 UDP Services
  - Most listen on :::PORT (::0 or 0::0)
  - Handle all unicast requests
  - Handle local broadcast requests!
- Using “broadcast” BIND DNS

```
$ dig www.domain.com @FF02::1
```

Local IPv6 Exploitation

- Cut through crappy firewalls
  - Portscan with Nmap and Metasploit (aux)
  - Exploit systems with standard modules
- Confuse your system administrators
  - Exploit attempt from ***what*** source address?
- Probe all IPv6 UDP services at once
  - Send packets to FF02::1
  - Easy reconnaisance

More to come...

- Abusing IPv4 compatibility addresses
  - ::A.B.C.D, ::FFFF:A.B.C.D
- IPv6 and web browsers
  - http://[2000::XXXX:XXFF:FEXX:XXXX]/
- MITM fun with THC-IPv6

questions ?