LIVE FREE OR HACK HARD

METASPLOIT 2007

CANSECWEST 2007

who am i ?

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

metasploit project

Core developer and project lead

BreakingPoint Systems

Director of Security Research

why listen ?

- Fun with Metasploit 3
- Tools for pen-testers
- Tools for bug hunters
- API for developers

metasploit framework

- An exploit development platform
  - Security researchers
  - Penetration testers
  - Security vendors
  - Script kiddies

metasploit coverage

- In the last few weeks
  - Windows .ANI (unpatched)
  - Windows DNS RPC (unpatched)
  - Handful of ActiveX exploits
  - Fun new DCERPC tools

metasploit history

- **1.0** (2003-2004) PERL
  - 15 exploits, curses UI
- **2.7** (2003-2006) PERL
  - 150+ exploits, 3 UIs
- **3.0** (2007+) RUBY

metasploit 3.0

- 100,000 lines of Ruby
- 53,000 lines of C/C++
- 8,000 lines of ASM
- 360 unique modules
- 2 years to develop

3.0 release

- Announced March 27th 2007
- 20,000 IPs downloaded
- 4,000 IPs updated
- RoR == 100+ load avg.

compatibility

- Linux, BSD, Win32, Mac OS X
- Native Windows support
- Runs on embedded Linux/BSD
    - Nokia 770, Nokia N800
    - Zaurus (multiple models)

extensibility

- New Auxiliary module format
- Event hooking framework
- Plugins can hook and extend
- Ruby shell available at any time

scalability

- Modules split into directories
- Modules are cached
- Namespace is enforced
- Supports thousands of modules

concurrency

- Use Ruby's built-in threading
- Multiple users per interface
- Persistent exploit modules
- Handle multiple shells at once

802.11

- Ruby-Lorcon (injection)
- Ruby-PcapX (sniffing)
- Rewrites of common tools
- 802.11 driver exploits

kernel-mode

- Support win32 kernel payloads
- Stage any userland payload
- Opens the door...

client-side

- Web server for browser exploits
- SMTP delivery of file-format bugs
- Inject any payload as an EXE
- Deep evasion features

meterpreter

- The super-payload for Windows
- Merged functions into “stdapi”
  - ls, rm, upload, download
  - ps, kill, execute, open
  - route, ifconfig, portfwd
  - eventlog, registry, threads

meterpreter

- The Meterpreter “priv” extension
  - hashdump (no-disk pwdump)
  - timestomp (f*off Encase)
  - privilege escalation...

```
meterpreter >  use priv
```

meterpreter

- Provides a rich Ruby API
- Meterpreter scripting
  - Kill all antivirus, firewalls, etc
  - Search and download files
  - Read and write process memory...

auxiliary

- Write security tools as modules
- Seperated into functional groups
  - discovery, scanning, info, dos
  - audit, brute force, fuzzing

licensing

- Metasploit Framework License
- Prevents commercial abuse
- Allows commercial modules
- Not FSF/OSU compatible

licensing

- Rex library provided under **BSD**
- Rex includes the interesting code
  - HTTP, SMB, DCERPC, SMTP

demos !

questions ?