Defcon XII 2004

METASPLOIT

Hacking Like in the Movies

spoonm
h d moore

Introduction

- **Who are we?**
  - Independent researchers
  - Work in the security industry
- **What is this about?**
  - Exploit frameworks in general
  - New exploit technology

Exploit Frameworks

Exploit Frameworks

- **What is an exploit framework?**
  - Interface for launching exploits
  - Standardized exploit modules
  - Suite of reliable shellcode
  - Library of common routines
  - Often includes “pro” features

Exploit Frameworks

- **Why are frameworks needed?**
  - 80% of exploit code is boilerplate
  - Payloads are usually hardcoded
  - Advanced techniques rarely used
  - Most “coders” aren't programmers
  - Nobody posts code for old bugs

Exploit Frameworks

- **Public exploit frameworks**
  - Two stable commercial products
    - CORE Impact
    - Immunitysec CANVAS
  - The Metasploit Framework
  - New projects in development

Exploit Frameworks

- **CORE Impact**
  - The first real exploit framework
  - Pricey but extremely complete
  - Written in Python/C++ (Win32)
  - Pivoting through owned boxes
  - Syscall proxy payload system

Exploit Frameworks

- **Immunity CANVAS**
  - Second commercial framework
  - Supports limited syscall proxying
  - May pivot in the near future
  - Less extensive than Impact
  - Considerably less expensive

Exploit Frameworks

- **Current Capabilities**
  - Point. Click. Command shell.
  - Pivoting through owned boxes
  - Automatic payload encoding
  - Dynamic shellcode creation

```
                __.                       .__.        .__. __.
  _____   _____/  |______    ____________ |  |   ____ |__|/  |_
 /     \_/ __ \   __\__  \  /  ___/\____ \|  |  /  _ \|  \   __\
|  Y Y  \  ___/|  |  / __ \_\___ \ |  |_> >  |_(  <_> )  ||  |
|__|_|  /\___  >__| (____  /____  >|   __/|____/\____/|__||__|
      \/     \/  v2.2    \/     \/ |__|
```

Metasploit Framework

The Metasploit Framework

- **Introduction**
  - Open source exploit framework
  - Exploit development platform
  - Written in Perl scripting language
  - Runs on most modern platforms
  - Focused on improving technology

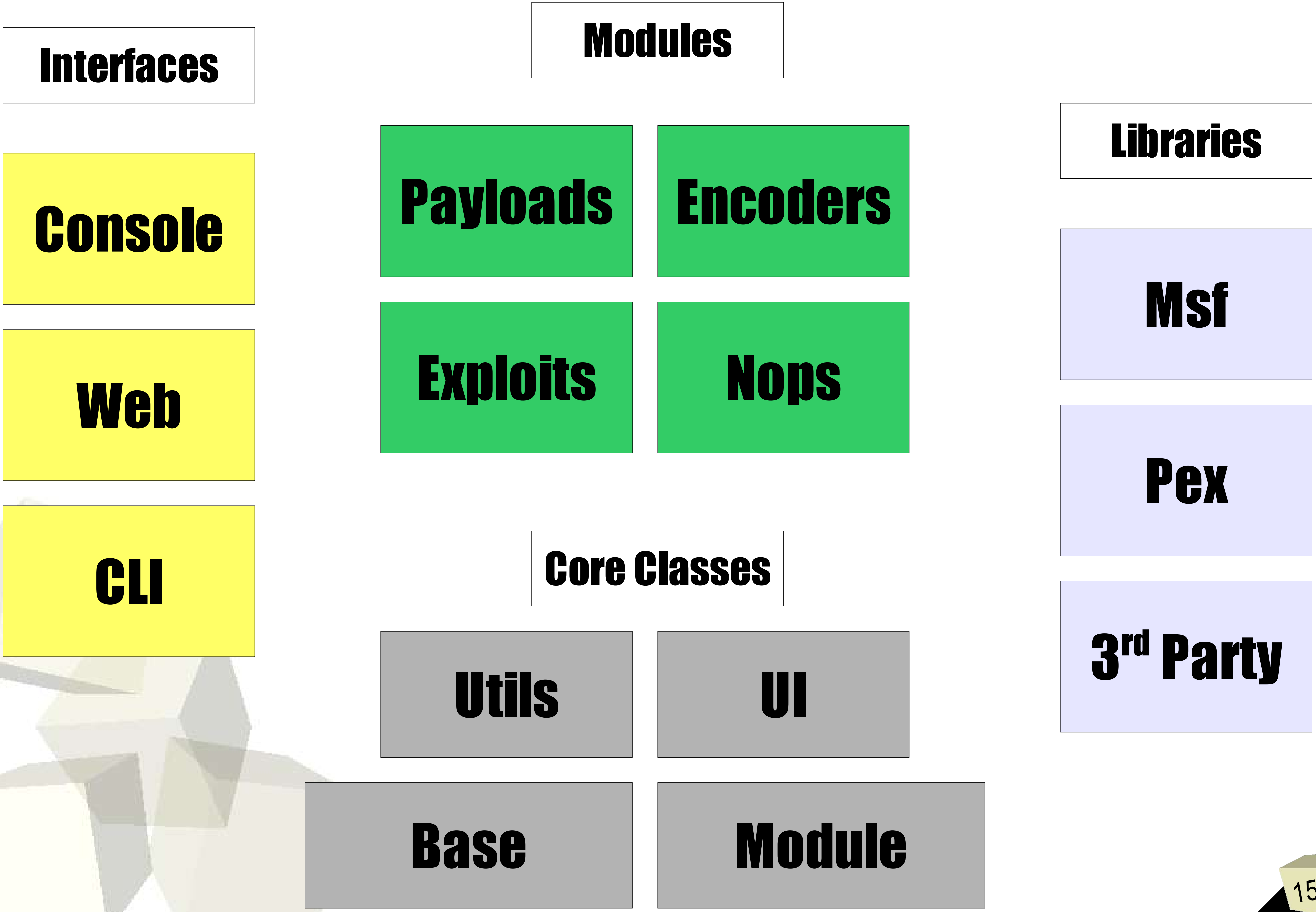
- **History**
  - Originally a network game
  - Rewritten for professional use
  - Evolved into open source project
  - Four primary developers
  - Handful of contributors

- **Development status**
  - ~35 exploits, ~40 payloads
  - Stable exploit and payload API
  - Widely used by security firms
  - Increasing use by system admins
  - MSF 2.2 first dev-friendly release

The Metasploit Framework

- **Components**
  - User interfaces
  - Exploits
  - Encoders
  - Payloads
  - Handlers
  - Nops

The Metasploit Framework



Interfaces

Console

Web

CLI

Modules

Payloads

Encoders

Exploits

Nops

Core Classes

Utils

UI

Base

Module

Libraries

Msf

Pex

3rd Party

The Metasploit Framework

- The command line interface
  - Simple scriptable interface
  - Useful for quick exploit tests

```
Usage: ./msfcli <ID> [var=val] [MODE]
Modes:
      (S)UMMARY       Show various information about the module
      (O)PTIONS       Show the available options for this module
      (A)DVANCED      Show the advanced options for this module
      (P)AYLOADS      Show available payloads for this module
      (T)ARGETS       Show available targets for this module
      (C)HECK         Determine if the target is vulnerable
      (E)XPLOIT       Attempt to exploit the target
```

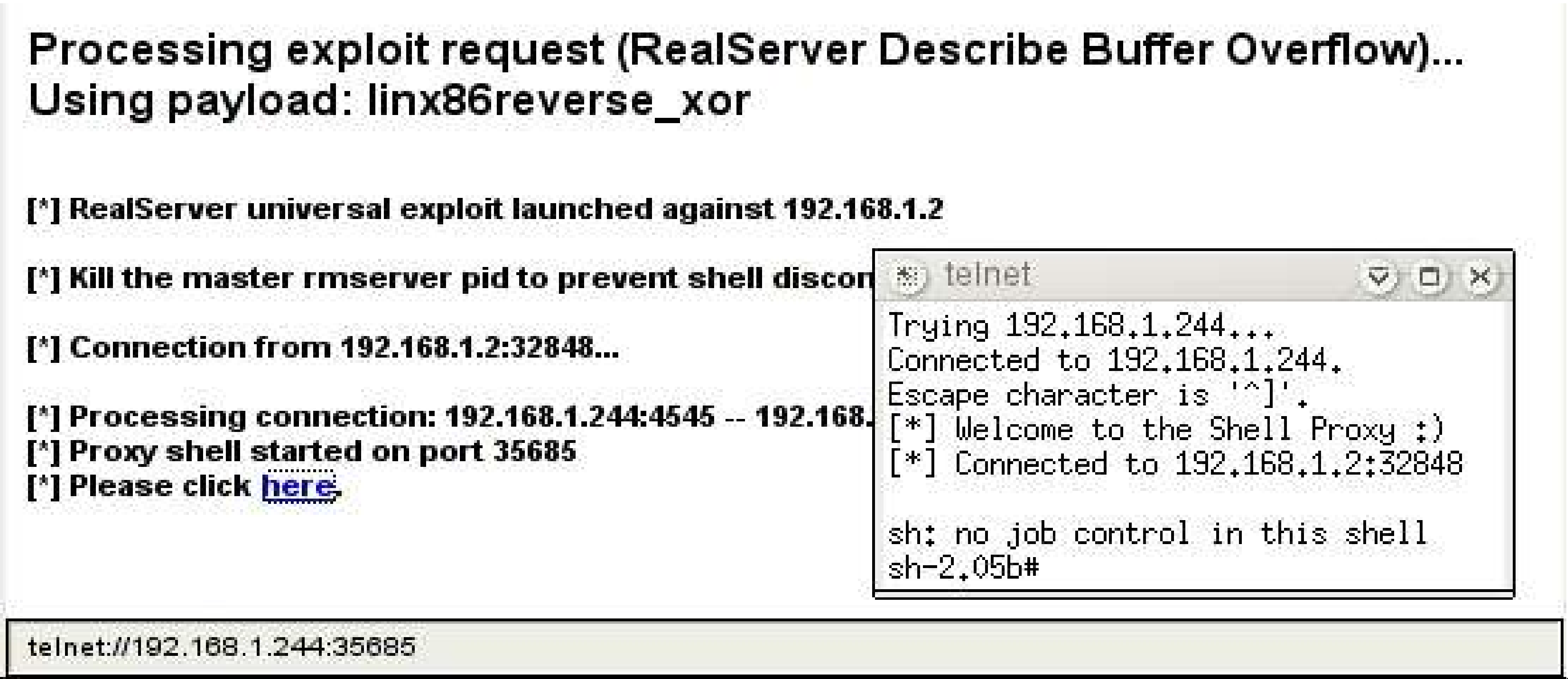
The Metasploit Framework

- The console interface
  - Tab-completion exploit shell
  - Session logging, history, environments

```
+ -- --=[ msfconsole v2.2 [35 exploits - 37 payloads]

msf > use realserver_describe_linux
msf realserver_describe_linux > set PAYLOAD linx86bind
msf realserver_describe_linux(linx86bind) > set LPORT 3456
msf realserver_describe_linux(linx86bind) > set RHOST vulnhost
msf realserver_describe_linux(linx86bind) > exploit

[*] RealServer universal exploit launched against 192.168.1.2
[*] Kill the master rmserver pid to prevent shell disconnect
[*] Connected to 192.168.1.2:3456...

bash-2.05b#
```

The Metasploit Framework

- # The web interface
  - Standalone web service
  - Proxies exploit shells



Processing exploit request (RealServer Describe Buffer Overflow)...
Using payload: linx86reverse_xor

```
[*] RealServer universal exploit launched against 192.168.1.2

[*] Kill the master rmserver pid to prevent shell discon

[*] Connection from 192.168.1.2:32848...

[*] Processing connection: 192.168.1.244:4545 -- 192.168.
[*] Proxy shell started on port 35685
[*] Please click here.
```

```
Trying 192.168.1.244...
Connected to 192.168.1.244.
Escape character is '^]'.
[*] Welcome to the Shell Proxy :)
[*] Connected to 192.168.1.2:32848

sh: no job control in this shell
sh-2.05b#
```

telnet://192.168.1.244:35685

- **Msfpescan – Return Address Fun**
  - Scans PE images for data (DLL, EXE)
  - Finds universal return addresses
  - Easy to script, easy to parse output
  - Regular expression match support
  - Can automatically disassemble code

The Metasploit Framework

- **msfpescan found good returns**
  - DCOM – NT SP6 -> XP SP1
  - Serv-U – All versions NT->2K3
  - LSASS – Autodetect Universal
  - Blackice – Mad Bruteforce Foo

The Metasploit Framework

- **Other helper utilities**
  - *msfdldebug* » Download symbols
  - *msfpayload* » Generate payloads
  - *msfpayload.cgi* » CGI payload gen
  - *msfencode* » CLI payload encoder
  - *msflogdump* » Colorized session logs
  - *msfupdate* » Online update system

The Metasploit Framework

- **Summary**
  - Stable exploit development platform
  - Designed to use with pen-tests
  - Admins use it verify scan results
  - Focused on technology (not $$$)

Exploit Technology

Exploit Technology

- **Windows Remote DLL Injection**
  - In-process DLL injection
  - Does not write files to disk
  - Written by Jarkko and Skape
  - Full access to Windows API
  - Easily convert C/C++ to payload
  - Reuse existing code (VNC)

Exploit Technology

- **Windows VNC Server Injection**
  - Injects VNC server as new thread
  - Reuses existing payload connection
  - Based on RealVNC source code
  - Adapted by Skape and HDM
  - Breaks locked desktops
  - Takes over WinLogon desktop

VNC Demo

Exploit Technology

- **Interchangeable Payloads**
  - Exploits adapt to network conditions
  - Reverse, Bind, Findsock, Exec
  - “Encrypted” xor command shells
  - Abstracted “cmd_” payloads
  - Drop in new payloads as needed
  - Integrated InlineEgg support

Payloads Demo

Exploit Technology

- **MSF Socket Class**
  - Integrated SSL support for all sockets
  - Can force connections to use proxies
  - Pivot exploit requests through proxies
  - New protocols are easy to integrate
  - Raw IP support is somewhat working

Exploit Technology

- **IDS Evasion**
  - “Polymorphic” encoders and nops
  - Avoid signatures with exploit options
  - First-exit event masking (snort 0-day)
  - Multi-staged payloads can avoid sigs
  - DCERPC request fragmentation

IDS Evasion Demo

Exploit Technology

- **Perl Protocol Libraries**
  - Perl modules for complex protocols
  - SMB stack already useful (LSASS)
  - DCERPC stack used with DCOM
  - Protocol stacks written as needed
  - Applicable outside of security testing

Exploit Technology

- **The Meterpreter**
  - Custom shell written as DLL payload
  - Connection multiplexing (channels)
  - Dynamically load extensions over net
  - Built-in cryptography support
  - Also written by Skape :)

Demonstrations

Questions?

Contact: msfdev@metasploit.com

Materials: http://metasploit.com/bh/