Introduction to Metasploit Post Exploitation Modules

Stephen Haywood

@averagesecguy

www.averagesecurityguy.info


YOU
FAILED

Shout Out

dc423.org

Don't Take Notes

These slides and a detailed how to document are available at averagesecurityguy.info

Why are We Here?

What is Post-Exploitation

How To Build PE Modules

How to Contribute PE Modules to Metasploit

What is Post-Exploitation?

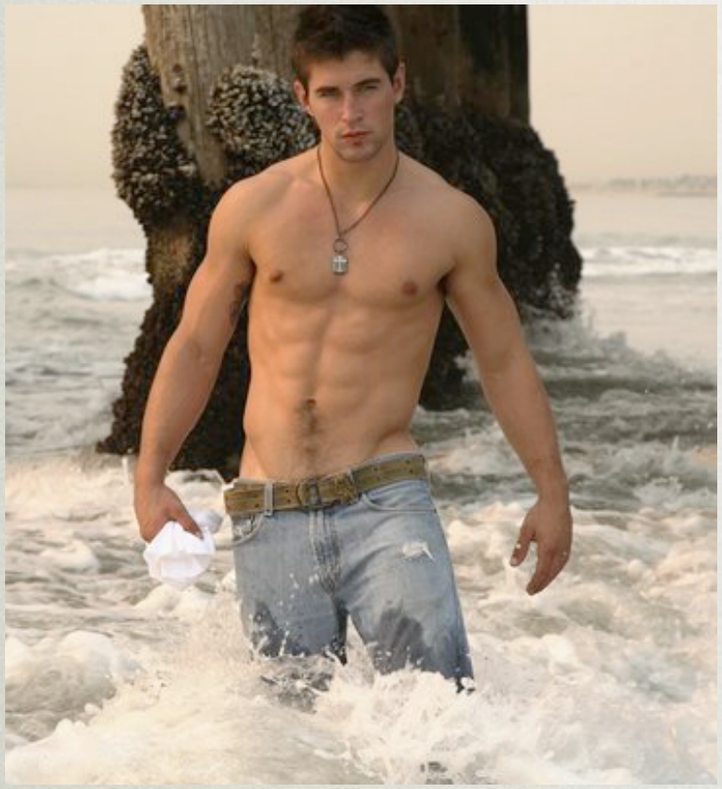
Identify

and

Capture

Sensitive Data

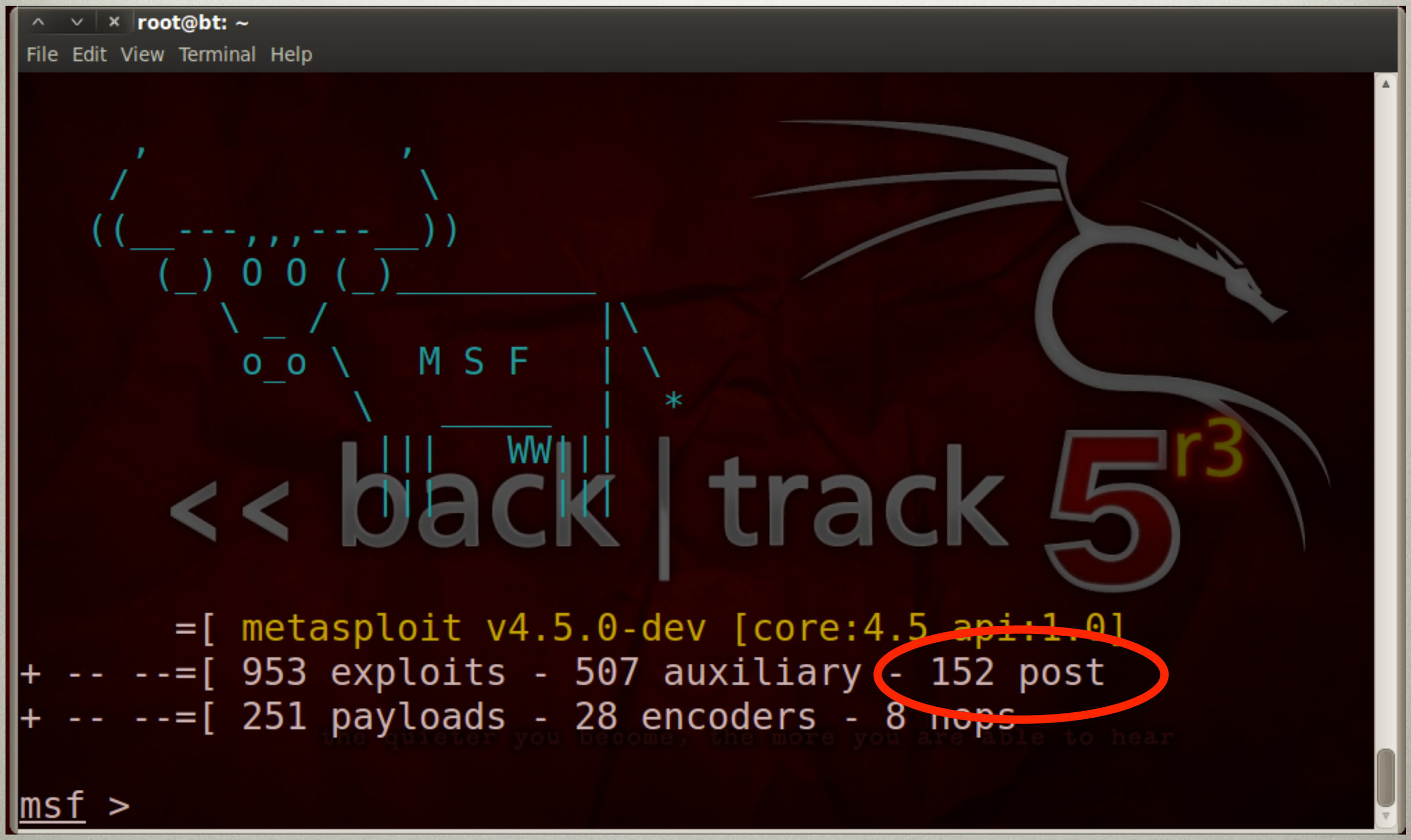
So, While Exploitation May Be Sexy...*



* I am an equal opportunity sexist.

Post-Exploitation Has The Bling

Post-Exploitation With Metasploit



Post-Exploitation With Metasploit

root@bt: /opt/metasploit/msf3/modules/post/windows/gather

File Edit View Terminal Help

```
root@bt:/opt/metasploit/msf3/modules/post# ls
aix  cisco  linux  multi  osx  solaris  windows
root@bt:/opt/metasploit/msf3/modules/post# cd windows
root@bt:/opt/metasploit/msf3/modules/post/windows# ls
capture  escalate  gather  manage  recon  wlan
root@bt:/opt/metasploit/msf3/modules/post/windows# cd gather
root@bt:/opt/metasploit/msf3/modules/post/windows/gather# ls
arp_scanner.rb                  enum_ms_product_keys.rb
bitcoin_jacker.rb               enum_powershell_env.rb
cachedump.rb                    enum_services.rb
checkvm.rb                      enum_shares.rb
credentials                     enum_snmp.rb
dumplinks.rb                    enum_termserv.rb
enum_applications.rb            enum_tokens.rb
enum_artifacts.rb               enum_unattend.rb
enum_chrome.rb                  forensics
enum_computers.rb               hashdump.rb
```

What is Post-Exploitation

How To Build PE Modules

How to Contribute PE Modules to Metasploit

How To Build Post-Exploitation Modules

Basic Structure

Using the Post Libraries

Providing Feedback

Store the Loot

Basic Structure

Initialize

Register Options

Build the Run Method

Initialize

```
def initialize(info={})
    super(update_info(info,
        'Name'           => 'Windows Gather Windows Host File Enumeration',
        'Description'    => %q{
                This module returns a list of entries in the target system's
hosts file.
            },
            'License'        => BSD_LICENSE,
            'Author'         => [ 'vt <nick.freeman[at]security-assessment.com>'],
            'Version'        => '$Revision: 14774 $',
            'Platform'       => [ 'windows' ],
            'SessionTypes'   => [ 'meterpreter', 'shell' ]
        ))
    end
```

Register Options

Option Name

Is the option required?

Description

Default value

```
register_options(
    [
        OptString.new('GROUP', [true, 'Domain Group to enumerate', nil])
    ], self.class)
```

```
register_options(
    [
        OptEnum.new('CMD', [true, 'Specify the autoroute command', 'add',
['add','print','delete']])
    ], self.class)
```

Array of possible values.

Register Advanced Options

Option Name

Is the option required?

Description

Default value

```
register_advanced_options(
    [
        # Set as an advanced option since it is only useful in shell sessions.
        OptInt.new('TIMEOUT', [true ,'Timeout in seconds.', 90]),
    ], self.class)
```

Options are stored in the datastore hash.

```
print_status("Found users in #{datastore['GROUP']}")
```

Valid Option Types

Option	Description
OptString	A multi-byte character string
OptBool	A boolean indicator (true or false)
OptPort	A TCP or UDP service port
OptAddress	An IP address or hostname
OptPath	Path name on disk or an Object ID
OptInt	An integer value
OptEnum	Select from a set of valid values
OptAddressRange	A subnet or range of addresses

Build The Run Method

```
# Run Method for when run command is issued
def run
    print_status("Running module against #{sysinfo['Computer']}")
    arp_scan(datastore['RHOSTS'], datastore['THREADS'])
end


def arp_scan(cidr,threads)
    print_status("ARP Scanning #{cidr}")
    ws = client.railgun.ws2_32
    iphlp = client.railgun.iphlpapi
    a = []
    iplst,found = [],""
    ipadd = Rex::Socket::RangeWalker.new(cidr)
```

How To Build Post-Exploitation Modules

Basic Structure

Using the Post Libraries

Providing Feedback

Store the Loot

Use The Post Libraries

```
root@bt:/opt/metasploit/msf3/lib/msf/core/post# ls
common.rb  file.rb  linux  osx  solaris  unix.rb  windows
root@bt:/opt/metasploit/msf3/lib/msf/core/post# ls *
common.rb  file.rb  unix.rb

linux:
priv.rb  system.rb

osx:
system.rb

solaris:
priv.rb  system.rb

windows:
accounts.rb    powershell.rb  registry.rb          shadowcopy.rb
cli_parse.rb   priv.rb        registry.rb.ut.rb    user_profiles.rb
eventlog.rb    railgun.rb     services.rb          user_profiles.rb.ut.rb
root@bt:/opt/metasploit/msf3/lib/msf/core/post#
```

Use The Post Libraries

```
require 'rex'
require 'msf/core'
require 'msf/core/post/file'
require 'msf/core/post/windows/registry'
require 'yaml'

class Metasploit3 < Msf::Post

    include Msf::Auxiliary::Report
    include Msf::Post::File
    include Msf::Post::Windows::Registry
```

Use The Post Libraries

Building Post-Exploitation Modules

Basic Structure

Using the Post Libraries

Providing Feedback

Store the Loot

Providing Feedback

Command	Result
print_line(text)	Print the text with no decoration
print_status(text)	Print the text preceded by a blue [*]
print_good(text)	Print the text preceded by a green [+]
print_error(text)	Print the text preceded by a red [-]
vprint_status(text)	Call print_status() if datastore['VERBOSE'] is true.
vprint_good(text)	Call print_good() if datastore['VERBOSE'] is true.
vprint_error(text)	Call print_error() if datastore['VERBOSE'] is true.

Providing Feedback

```
        # reset user pass if setpass is true
        if datastore["SETPASS"]
            print_status("Setting user password")
            if !reset_pass(user,pass)
                print_error("Error resetting password")
                return 0
            end
        end
```

Building Post-Exploitation Modules

Basic Structure

Using the Post Libraries

Providing Feedback

Store the Loot

Store The Loot

```
path = store_loot(ltype, ctype, session,
                  data, filename, info)
```

```
# Store the original hosts file
p = store_loot(
    'hosts.confige',
    'text/plain',
    session,
    buf,
    'hosts_file.txt',
    'Windows Hosts File'
)
```

Short string to describe the loot type

MIME type of the data being stored

Data to write to the loot file

Name of the file you are writing

DB description of the loot data.

Side Note

Editing Modules

What is Post-Exploitation

How To Build PE Modules

How to Contribute PE Modules to Metasploit

Contributing Modules to The Framework

Read the Guidelines

Fork the Framework

Add Your Code

Submit a Pull Request

Read the Guidelines

Acceptance Guidelines

Style Tips

Metasploit Development Environment

Fork the Framework

Login to GitHub and fork the Rapid7/metasploit-framework repository.

Clone the new repo to your development environment.

Add Your Code

Place your code in the appropriate folder under modules/post

Commit your Code

Push Your Code

Submit a Pull Request

Go back to GitHub and submit a pull request at Rapid7/metasploit-framework

Watch the request to see if you are asked to make any changes.

What Did We Learn?

What is Post-Exploitation

How To Build PE Modules

How to Contribute PE Modules to Metasploit

Remember

These slides and a detailed how to document are available at averagesecurityguy.info

?

Introduction to Metasploit Post Exploitation Modules