This is timeline for GSoC Project “Windows Shellcode and Code Obfuscation modules” with organization OWASP ZSC.

Week 1 and Week 2

Add opcoder for windows shellcode like this one which is for linux.
Add Execute shellcode for windows.
Start work for Writing to file shellcode.

Week 3

Complete writing to file shellcode.
Add create directory shellcode.

Week 4 and Week 5

Add shellcode Download and Executing a file.
Add shellcode for creating user and adding user to admin group.
Add shellcode for creating a messagebox.

Week 6 and Week 7

Add shellcode for disabling firewall.
Add other shellcodes which will be required.
Add Documentation for all windows shellcode.

Week 8

Add Simple Reverse hex and flip bit hex obfuscation modules. Both the modules will be created in python, perl, javascript, ruby and php.

Add Simple Reverse base64 and flip bit base64 obfuscation modules. Both the modules will be created in python, perl, javascript, ruby and php.

Week 9

Research on more complex Obfuscation modules particularly Collberg’s Algorithm and Chenxi Wang’s Algorithm.

Start working on Colberg’s Algorithm at the end of the week.

Week 10

Complete Collberg’s Algorithm module.
Implement Chenxi Wang’s obfuscation Algorithm.

Week 11

Add Rot13 encoding and Binary obfuscation modules. Both of the modules will be created in the languages mentioned above.

Dummy code obfuscation modules in the languages python, ruby, php, perl and javascript.

Start adding encryption obfuscation modules in all the languages mentioned.

Week 12

Add one more complex obfuscation module on which I will be doing more research in Week 9 and Community Bonding period. If I could not come up with good plan of one more complex obfuscation method then I will add few encryption modules in all languages.

Add documentation for obfuscation modules.

Clean up the code, test all the code again and prepare for final evaluation.