Lab 8

Part A

1. What Anti-disassembly techniques are used in the binary?

2. What Anti-debugging techniques used in the binary?

3. What does the sample do?

Part B

4. Patch the PE to bypass any techniques found.

   - I should be able to set a breakpoint in the malicious subroutine and let the program execute until that breakpoint without a problem.

Please Submit:

1. Answers to these questions

2. The patched and zipped binary (password: ‘infected’)

Send to : malwarefall2015+lab8@gmail.com