# **Lab 10 Report**

1. Name: Student ID:
2. Analyze the Lab09-01.exe

How can you get this malware to install itself?

What are the command-line options for this program? What is the password requirement?

How can you use OllyDbg to permanently patch this malware, so that it doesn’t require the special command-line password?

What are the host-based indicators of this malware?

What are the different actions this malware can be instructed to take via the network?

Are there any useful network-based signatures for this malware?

1. Analyze the Lab09-02.exe

What strings do you see statically in the binary?

What happens when you run this binary?

How can you get this sample to run its malicious payload?

What is happening at 0x00401133?

What arguments are being passed to subroutine 0x00401089?

What domain name does this malware use?

What encoding routine is being used to obfuscate the domain name?

What is the significance of the CreateProcessA call at 0x0040106E?