CPE457/557 Software Reverse Engineering

**12 - Basic Static Analysis**

# Finding Hashes & Strings

**Lab Description:** The goal of this lab is to provide an application of the basic static analysis techniques and tools discussed in the lecture. Basic static analysis allows you to identify malicious files, begin to understand it’s behavior and share threat information.

**Lab Environment:** It’s recommended that a safe VM environment from be used. In addition, the REMnux Linux distribution (<https://remnux.org/>) may also be used, this Linux distribution comes pre-configured with many of the tools needed for this lab.

**Lab Files that are Needed:** The files required will be provided in the accompanying archive, 02\_BasicStaticAnalysis.zip. The archive is password protected with the password: *infected*

### **Lab Exercise 1:**

Using the following sample, “keylogger.exe”, answer these questions. Each question should include a screenshot, and brief explanation of it.

1. Using a strings utility such as strings from a command line or the strings window in IDA Pro; what strings can you find that you think are relevant?
2. Using a hashing utility, create an MD5 hash of the program, what is the hash value? Use this hash to find additional information about the sample on VirusTotal, what are the results?
3. Now create a SHA256 and SHA512 hash, what are they?

### **LAB EXERCISE 2:**

This exercise will utilize the REMnux VM found at <https://remnux.org> and require you to create custom Clam-AV signatures.

1. Create an ASCII-based signature based off of a custom program that you create. Show the results of scanning your custom program with Clam-AV from a terminal, the results should clearly demonstrate that Clam-AV identifies your sample program as malicious.

## What to submit

Submit a Microsoft Word document or PDF that includes answers to the questions posed along with screenshots supporting your answers.