Module C1: FILE HANDLING TECHNIQUES

# Analyzing honeypot piles

**Lab Description:** The objective of this lab is to allow you to use the Honeypot instance you created in class to acquire and investigate real malware samples in the wild. It also provides an opportunity to deploy additional honeypots.

**Lab Environment:** This lab uses an EC2 (or similar) Honeypot instance created in class, to include Dionaea and Cowrie honeypots. This honeypot should be exposed to the live internet in order to observe exploitation efforts.

**LAB EXERCISE/STEP 1**

The instructor needs to clearly express the following warning:

WARNING: This lab may expose you to malware. Malware needs to be handled carefully. Malware may trigger Anti-Virus or other similar security tools. DO NOT EXECUTE THESE BINARIES ON ANY SYSTEM. The safest approach is to examine this within the environment you have been provided.

**LAB EXERCISE/STEP 2**

Monitor your Cowrie/Dionaea hosts over the week and write a description of a Cowrie event and a Dionaea event for presentation to the class.

**LAB EXERCISE/STEP 3 (OPTIONAL)**

Deploy at least one more honeypot on the EC2 host (or somewhere else provided that you have permission – careful!). Describe the honeypot you selected and at least one event from that honeypot.

# What to submit

Students should present their results to the class. Results will be greatly varied as they are dependent on the interactions with their individual honeypots. In addition, repeating this exercise over time will yield difference results as the attack vectors change significantly over a very short time period.

**Options –**

Instructors can assign determine if the optional assignment is required/optional/requested, etc.