Module D5: PATCHING BINARIES

# patching BINARIES

**Lab Description:** The objective of this lab is to allow you to gain experience patching binaries.

**Lab Environment:** This is intended to be an interactive lab with the instructor providing guidance to extend student demonstrations of very basic static analysis skills. The exercise should be run in a protected environment as it may deal with malware. It can be run in the SRE class virtual environment, which would contain the crackme files and tools for static analysis. It would also allow instructors to view/step-in to the student environment even when not co-located.

**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**

* Patch each of the 7 binaries in the 0711\_modify\_for\_students directory so that they display the "Access allowed!" message. The binaries are all already on your 64-bit Linux VMs in the lab environment, and in the attached tar file.
* 1 and 2 were covered in the module lecture, so they should be an easy review. Examples 3-7 are new. Some notes on these:
* In binary 5, you are looking for the specific string "Access allowed!" to be printed (you'll be able to use the same solution as for 4 to get a slightly different string to be printed, but that's not sufficient)
* In binary 6, it's acceptable for the binary to print either "Access allowed!" or "Access granted", but it should not print "Access denied"
* In all cases the programs should terminate normally (i.e., they should not segfault)
* You can use whatever patching method you want, but you're not allowed to just use the debugger to manually modify registers (i.e., you actually have to patch instructions).
* In each case your submission should clearly show what you changed, how you changed it, and that the change had the intended effect.

# What to submit

Students should present their results to the class.

Instructor Notes:

Results will be greatly varied as student select difference file and approach the RE process and documenting the RE process differently. Prompts you might use during presentations include:

* Why did you choose that method?
* What would you do to prevent the method you chose from being successful (or similarly, what conditions in the binary allowed your chosen method to be successful).

**Options –**

Instructors can assign different binaries to each student.