CIS6395: Homework 3

University of Central Florida
Cliff C. Zou
Assigned: Oct. 27th, 2016; Due: midnight Nov. 6th, 2016

Question 1 (15 points): Please use Internet information gathering method we introduced in class to find out for the domain name "nba.com":

(1). What is the domain's registrar name?

(2). Provide the list of authoritative DNS name servers (provide their names would be fine, no need for IP addresses)?

(3). What is the domain's admin name and, address and phone number?

Please explain how you find the above answers, and show the screenshot images.

Question 2 (20 points): Use google hacking techniques introduced in class to do information gathering about the domain "ist.ucf.edu":

(1). The list of word files (with file type of .doc) you can find in IST that contain keyword "phone". Please show the Google search phrase you have used to get your answer.

(2). Find the PDF files in IST that contains "security" in the PDF title (note: not file name). List these PDF files' title. Please show the Google search phrase you have used to get your answer.

Please show the screenshot images of your Google search result webpages.

Question 3 (20 points): In your Kali Linux VM, run 'strace' program to find out what system calls have been used by the command 'mkdir temp'. Make sure that this 'mkdir temp' can be successful. (if your Kali does not have strace, you need to install it by yourself)

(1). If you save the strace output into a text file, how many lines exist in this output file? Use screenshot image to show how you get this value.

(2). How many times the 'access()' system call has been called by mkdir command? Use screenshot image to show how you get this value.

(3). Show the complete 'execve(…)' system call executed by the mkdir command.

Question 4 (45 points): I have made a very simple 32-bit Windows executable program called 'password.exe', which can be downloaded from webCourse. The code can run on 32-bit or 64-bit Win7 or above Windows. When executed, the program asks for you to input a password. If your input password matches with the program's hardcoded password, then you are successful; otherwise it prints out that you input a wrong password. The execution is like this (the real password is blanked out):

Please use the free OllyDbg software to find out what is the correct password by dynamically analyzing this binary code. Provide the screenshot image to show your successful execution of this 'password.exe' code. In addition, use words and screenshot images to show how you find out this correct password.