CIS6395: Homework 4

University of Central Florida
Cliff C. Zou

Question 1 (20 points): Please use Internet information gathering method we introduced in class to find out for the domain name "**spectrum.com**" (hint: introduced in 'reconnaissance.ppt' slides):

(1). What is the domain's 'Registrant Organization' and 'Registrant Email'?
(2). Provide the list of authoritative DNS name servers for this domain (provide their domain names would be fine, no need for IP addresses)?

Besides provide the direct answers to the above questions using text, please also 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 "cise.ufl.edu":

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

(2). Find the PDF files in the website that contains "scanning" 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 (25 points): In your Kali Linux VM, use Fierce reverse DNS lookup to find out the DNS domain assignments around a webserver.

(1). In Kali terminal, use command to find out what is the IP address of webserver 'www.cise.ufl.edu'? Besides the text answer, please also provide screenshot image.

(2). Use Fierce reverse DNS lookup to find out, within the /24 subnet that contains the above webserver's IP address, the list of IP addresses that have assigned with corresponding domain names. Please provide the text answer of the list of IP addresses and their domain names, and also the screenshot image to show the Fierce command and the initial part of the command result.

Question 4 (35 points): I have made a very simple 32-bit Windows executable program called 'password.exe', which can be downloaded from the course website associated with this assignment. 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.