#1 and 2 use 10/12 and 10/17 lecture recordings

#3 use 10/24 lecture recording

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'?

Using whois.com and querying “spectrum.com”, we get the following:

Email: hostmaster@charter.com

Organization: Charter Communications Operating, LLC

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

ns1.charter.com

ns2.charter.com

ns3.charter.com

ns4.charter.com

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.

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

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

(1). The list of word file names (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.

cyber filetype:doc site:cs.ucf.edu

(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.

intitle:scanning filetype:pdf site:cs.ucf.edu

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

Text

Description automatically generated

A screenshot of a video game

Description automatically generated

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.ece.umass.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, how many IP addresses having been assigned with domain names within this /24 subnet? Please provide the text answer of this number value, 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 this windows executable file here password.exe Download password.exe. The code can run on 32-bit or 64-bit Win7 or above Windows (you can run it in your Windows VM if you are using Mac or Linux). 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):

Text

Description automatically generated

Please use the free OllyDbg software we introduced in class 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.