Comp715 Problem Set 5 (Summer ’19) due 7/24/19

Instructions: Type your answers and hand in a printed copy (please associate question number with each answer). Add a separate cover sheet with the assignment number and your name. Please be concise, complete with answers…describe/explain generally means several paragraphs.

Research questions: *[4 points total]*

1) *[1 points]* Go to YouTube.com and type in the phrase *“how to crack a WEP key”* (or you can try WPA, though it’s a bit harder but some students have done it).
   a. Watch a few videos and find one that reveals the actual key and write down the URL.
   b. Now follow the steps and write them down as you do them.
   c. Were you successful? If no what happened?

2) *[1 points]* `nmap` is a scanning utility and although it works on many platforms, it’s best to work with it on unix.
   a. You’ve been given access to linus.unh.edu (userid: comp715, passwd: comp715)
   b. What can `nmap` do for you? Discuss in detail.
   c. Show some commands you’ve discovered and what results they give you.
      i. Note you’ll have to do some online research on using `nmap`.

3) *[2 points]* Go into your Windows (or Mac) firewall (use lab laptops if you don’t own one).
   a. Under menu choices, select **Allow a program through Windows Firewall**, and list all exceptions you have checked
      i. Create hierarchical list, some exceptions have multiple items (edit details)
      ii. Now, for each try and write Firewall rules as we discussed in class. i.e.

         General syntax:

         ```
         <action><protocol> from <source_address><source_port>
         to <destination_address><destination_port>
         ```

         Where fields are:

         - action: either keyword **deny** or **allow**
         - protocol: either keyword **tcp**, **udp**, or **icmp**
         - source/destination_addr: ip addr, ip addr range or keyword **any**
         - source/destination_port, port number or keyword **any**
      iii. Note if you have more than 10, do the first 10 only.
   b. Under **Advanced settings**, repeat for Inbound, Outbound and Connection Security Rules

4) *[2 points]* Explore Fiddler *(COMP 815 students only)*
   a. Download and install on your machine (available for Windows and Mac OS)
   b. Give a detailed description of what it does and its capabilities
      i. Somewhat open-ended but I recommend being detailed and spent some time exploring the tool so you can be a bit exhaustive (to a point)
   c. Use it to explore some specific element on your computer
      i. Setup an experiment using Fiddler and document what you did and what information you were able to capture.

Lab questions: *[4 points total]*

The Great Summer Secret Key Hunt

Summary: In lab on July 3rd and 10th we worked with a shorter sequence, 16 bit random number generator. Though worse than the 32 bit version we used prior, the point was to allow us the opportunity to do some brute force attacks in JavaScript. For this homework assignment, you will download **final_6.html** which has a text field of **150** encrypted strings of which there are **12** hidden secret strings. I'm not telling you how I encrypted them but will tell you that all take on the form of recognizable dictionary words, albeit some use pretty good password naming techniques. It is your job to find as many of these as you can. *(Hint, I may have used all the encryption techniques we did in lab and homework).*

Discussion: *[1 points]* In general terms (i.e. don't talk about JavaScript) discuss in detail:

a) What steps you would take to find most of these secret strings.
b) What obstacles besides good password naming techniques are you likely to encounter.

Implementation: *[3 points]* Now try and implement your techniques in code to crack as many of the **12** strings as you can. You will have trouble finding all **12** (I think).

Let the games begin…