CSC630

Practice Final

May 24, 2019

Please note: the following exercises are meant to be performed in front of your instructor. Each can be completed in 30 minutes. As you work through any of the following exercises, be sure to explain to your instructor what you're doing at each step.

1 Getting Online

You will be given a "Live USB" drive with the common Ubuntu 18.04 operating system on it, as well as a working computer with a blank hard drive.

1. Turn on the computer and boot into the Ubuntu operating system. Because you might not have ever done this before, it's fine to ask your instructor for help!
2. Connect to the PA wireless network using your own credentials. Be sure not to save your credentials to the disk, but it's not the end of the world if you do. (After all, everything will be deleted when you turn the computer off.)
3. Download an image of John Palfrey from the Web, and save it to the computer. (Keeping it in temporary storage is fine.)
4. Create an ad-hoc WiFi network on the computer (this can be done using a GUI interface in Ubuntu/GNOME's built-in settings, where it is called a WiFi hotspot).
5. Serve the image of Mr. Palfrey using a temporary HTTP server. An easy way to launch a simple HTTP server is by using the Python command python −m SimpleHTTPServer 8000 from the directory you'd like to serve (where 8000 is the host port). Rename the photo of Mr. Palfrey to important.jpg and place it in the root of the directory.
6. Connect to the ad-hoc WiFi network on your phone or another device.
7. Figure out the IP of the host computer running Ubuntu on the ad-hoc network (hint: if you don't know it off the top of your head, you can Google the answer!).
8. Load the image of Mr. Palfrey on your other device (the one connected to, but not serving, the ad-hoc WiFi network), and load the image of Mr. Palfrey by requesting it from the host computer.

2 Cybersecurity Consultant

Imagine that you are a "cybersecurity consultant"—that is, people hire you to help them secure themselves digitally. Your clients generally don't have technical backgrounds, so part of your job is explaining complicated technical ideas in ways that are accessible to even the most tech-illiterate client.

Today, you are meeting for the first time with a client to do a brief consultation. The flow of your meeting might look something like this:

1. First half: ask questions about the client's tech "setup." Evaluate their potential attack surface and work to establish a reasonable threat model.
2. Second half: give security recommendations to the client, and ask/answer any follow-up questions as necessary.

For the purpose of this practice exam, you know the following about your client:

1. They have an iPhone XS, use a MacBook Air as their primary computer, and have a home WiFi network that is password-secured.
2. Their cell carrier is Verizon.
3. Their primary online accounts are Google, Bank of America, Charles Schwab, Verizon, Todoist, employer NetID, Spotify, Amazon, and American Express.
4. They do not have any "smart home" devices.
5. They work as a linguist for the CIA and have a "Top Secret" security clearance.

3 Do It With Telnet

In this exercise, you will need to use Telnet and OpenSSL. To ensure that all students are working in the same environment, you should perform these tasks from an Ubuntu VPS.

Telnet is a protocol for simple, text-based communication between computers and was often used between 1968 and 1980 for remote terminal connections. Though built on top of TCP and being relatively robust, it offers no protections in the way of security in privacy.

You can think of a telnet connection as a TCP "pipe" through which you send data by typing and receive data as output to your terminal. It's that simple.

What this also means is that it's possible to "simulate" other TCP-based protocols, such as HTTP, using Telnet.

To connect to Google via Telnet, for example, run the following command:

```
telnet www.google.com 80
```

Then, to send data, just type and press enter twice. For example, to make an HTTP GET request to the root, type:

```
GET / HTTP/1.1
```

Maybe you'll get a page redirect to Google HTTPS website, or maybe you'll run into Phillips Academy's web filter.

Given your familiarity with HTTPS, now try to use the OpenSSL tool (the command is simply *openssl*) to connect to various websites via HTTPS. Explain any and all output you see to your teacher.