The week of 1/19/18

All knowledge is good knowledge.

I spent much of my time this week behind a book rather than a monitor. Chapter one is, in my humble opinion the perfect explanation of hacking. The second chapter of Hacking the Art of Exploitation is a technical and in-depth review of C programing and lower level processes.

“Most people associate hacking with breaking the law and assume that everyone who engages in hacking actives is a criminal” (Erickson p1). In my mind hacking is not about the law, hacking is an attitude. Hacking is trying to figure out a clever solution to a complex problem, often via trial and error. The solutions that come out of this method can be used for good or bad.

In chapter two, I found much value in the section regarding the x86 processor. The x86 processor is used by all Windows machines and many of the new Macintosh computers. The x86 chip was developed and manufactured by Intel. Intel, up until recently, has been one of the most widely used and reputable chips on the market.

The recent hardware vulnerability, “Meltdown”, may or may not change their standings among the computer science community. I doubt society at large will notice the hit in computational power after the software workaround to the hardware bug has been implemented. I took up a bit of an interest in x86 because I believed in the longevity of Intel’s chips. After a vulnerability such as this, doubt sets in.

For next weeks blog post, I want to do a review of Pico CTF. I will go through some of the level one challenges and explain the one’s I liked or the one’s that stumped me. If you have a specific request for a challenge you want me to attempt, let me know via the “contact me” tab.

Week of 1/26/18

The difference between find and grep

“Leaf of the Tree” is a large file system that uses many directories to make it difficult to find your flag. The idea is to use tab to auto complete the directory name. The file names are very long with a random string of characters tagged on the end. It would be very inefficient to type them out in their entirety.

“Leaf of the Forest” is file system many magnitudes larger than the “Leaf of a Tree” puzzle. In this challenge the effective way to find the flag is to use the “find” Linux command. Find can be used to find things. Weird, I know. To find a file by name we must use a flag.

find -name “flag”

If we wanted a list of all txt files in the directory then we could use the \*.

find -name “\*.txt”

We are not limited to our current directory by the find command. We can change the directory search by specifying before the name. If I wanted to see a list of all the html files on my desktop then the following command should do the trick.

find /Users/Victoria/Desktop -name “\*.html”

There are many cool flags other than -name. Suppose I have been inconsistent in my naming conventions. CamelCase or modifiedCamelCase? Who remembers. The flag -iname is just like the name tag however it ignores text case.

The flag -mtime stands for modify time. If I wanted to see the .txt files modified in the last seven days then the following command would do nicely.

find -mtime 7 -name “\*.txt”

Grep is an entirely different beast. I learned about grep a semester ago and it has become a great tool in my arsenal. Grep searches for a string of plain text inside files. If I forgot my social security number but I knew I had it written somewhere on my computer, I could use grep. If we run this command from the root, we will be waiting an awful long time. The -R stands for recursive. The -R will ensure that a pointer will sift through every file on my computer looking for the text string I provided.

grep “Social Security Number:” -R

Hopefully I would have remembered where I saved this sensitive data. I could save myself time by narrowing down the search field. The following command will complete in a much shorter time.

grep /User/Victoria/Documents/mySensitiveData “Social Security Number:” -R

As a side note, please don’t save your sensitive data in a folder labeled mySensitiveData. It’s just not safe there.

This week’s independent research time was dedicated to getting back on the horse. The challenges on picoctf.com enabled me to brush up on my terminal commands. I am researching ways to set up my vulnerability testing environment. Using virtual box, I obtained a version of Kali Linux. Kali Linux was recommended to me by members of UF’s Security InfoSec Team (SIT). Next week I want to start practicing on Metasploit. Metasploit is a virtual machine with network-layer vulnerabilities. <http://resources.infosecinstitute.com/hacking-lab/>.

Week of 2/02/19

Ifconfig

Nmap

https://www.youtube.com/watch?v=LI4v7UDxxto