David Cruz - 3/10/2017 - CIS4930 Practical CyberSecurity - Assignment #3

How To Execute From Command Line:

```
python exploit_infrastructure.py | nc 10.247.49.156 8888
```

Port Number For Shell:
9856

Exploit Results:
My exploit works locally and in the infrastructure.

How I Developed My Exploit:

I developed my exploit by first developing an exploit that works in RedHat 8. I generated the shellcode in Metasploit (in python). After I generated the shellcode, I added nopsled before and after shellcode (but before EIP). It took me several attempts to get it to work and I ran into a few issues. From examining the core dump files, I noticed that everything seemed to be correct (correct eip), but I was not getting a shell. I used cc (breakpoint/trap) to verify that my shellcode was being reached, and it was. Eventually, I realized that vms were not on the same subnet. I switched both to host-only, regenerated shellcode, and it worked!

After this I moved on to testing on RedHat 9 (after setting it up), I used the same exploit to make sure it crashed. It didn't. I had to set up ulimit and do all the configs. I also remembered that the structure was different. So I searched for the shared library on RedHat 9 and copied it to Kali. I found the list of jump codes using the msfelfscan command and providing the file path and esp arguments. From there, I got a list of jump codes and chose the one that we saw in the lecture slides from that list (just to be safe), even though another one may have worked. After that, I reformatted my nops and my jump code to follow: nops,jmp,nops,shell. Also, I set up netcat in order to make sure I could chat between both vms. After verifying that all that worked, I crashed nweb and examined the contents of the core file. For some reason, it was crashing at the end of my shell code. This made me realize that my nop sled was too small. So I had to adjust. I ended up having a really large nop sled before eip and a much smaller nop sled after. I verified that it trapped (cc). Once everything checked out and I examined the core file using gdb, I replaced cc with the original characters and it worked!

After this, I regenerated shell code with the attack machine's ip address. I connected to the vpn (class infrastructure) and ssh'd into the attack machine. I set up nc listener on the port I used (9856). From a different terminal window, I sent the exploit and it returned a shell. It worked!