**Additional Resources**

As you begin your Cybersecurity journey you may wonder, "how do I take what I've learned and apply it?" The answer is rather simple. In order to be effective and efficient in this field you have to practice. You have to be careful in how you practice in this field. Because some actions you take have real world consequences. Meaning you may think you're doing a harmless Nmap scan on a random network but then 3 letter agencies decided to pay you a visit. Where is the best place to practice? That is an honest question I had to ask myself a few years ago. What I ended up doing was purchasing a physical server so I could be more familiar with all the components I would encounter on a daily basis. This solution isn't for everyone. There however, alternatives to purchasing physical equipment called Capture the Flag (CTF) events. Through CTFs you have the ability to test offensive and defensive techniques in environments designed for the sole purpose of being attacked. You are allowed to "hack" their systems legally and gain a better understanding of your chosen profession. You might think to yourself, "why would I need to understand what an offensive attacker does." Offense informs the defense, that principle fits perfectly. If you understand just what an offensive operator is going to do, you can then establish a defensive game plan or framework to defend against said attack.

The below list are some websites I've gathered over the years that have a bunch of great content as well as locations where you can practice. GCU and I in no way profit from these resources. This is simply a way for you to begin the technical journey required to be proficient in this field. The links I'm providing are open source websites. If you feel more comfortable using Google to search for them, please do. Use at your own risk. I've used them in the past myself with zero issues. In fact I checked every link prior to posting this to ensure the websites were still accessible. If you are new to this line of work, I highly recommend checking out the overthewire.org Bandit CTF first. You need to grasp Linux to be effective. Happy Hunting.

Ranges:  
Wargames  
<https://overthewire.org/wargames/>    Start with the Bandit challenge  
<http://github.com/RhinoSecurityLabs/cloudgoat><http://www.ctftime.org/><http://www.wechall.net/><http://smashthestack.org/><http://holidayhackchallenge.com/>[https://picoctf.com](https://picoctf.com/)<https://www.amanhardikar.com/mindmaps/Practice.html>[https://www.root-me.org](https://www.root-me.org/)[https://cryptopals.com](https://cryptopals.com/)[https://websec.fr](https://websec.fr/)[https://chall.stypr.com](https://chall.stypr.com/)[https://pwnable.kr](https://pwnable.kr/)[https://pwnable.tw](https://pwnable.tw/)opentoallctf.github.io  
<https://gitlab.com/r00k/ctf-resources>reddit.com/r/securityctf  
SANS Holdiay Hack Challenges  
<https://counterhack.com/h2matrix><https://cyberdefenders.org/><https://dfirdiva.com/>

Jim Browning Scammer Take Down <https://www.youtube.com/watch?v=le71yVPh4uk&list=PLBNmQJqxpaMaxqghShRiOnHUjO00ZCsor>