Backman, Nathan. “Facilitating a Battle Between Hackers.” *Proceedings of the 47th ACM*

*Technical Symposium on Computing Science Education - SIGCSE '16*, 2016, pp. 603–608., doi:10.1145/2839509.2844648.

This is an analysis about capture the flag events. There are two types of capture the flag events: Jeopardy and Attack and Defend. Challenges for the CTFs include: 1) provisioning a computer (typically a virtual machine) for each team; 2) managing services, flags, and infrastructure support code on all computers; and 3) the need to incentivize teams to keep their services online and functional. People attain points for capturing flags, keeping (securing) flags, and keeping services running. Flags may be stored in different services or formats, but all you have to really do is read them.

Bui, Thahn. “Analysis of Docker Security.” 2014.

Although containers are more lightweight than VMs, they present some security concerns. This paper discusses two areas of docker security, its internal security and how it interacts with the Linux kernel security features, and how these security concerns may be mitigated. The paper explains different approaches to virtualization, gives an overview of dockers, and then details the different aspects of the security of dockers, such as device, network, filesystem, and IPC isolation and docker and kernel security systems. The paper concludes by stating that the security concerns found in dockers can be generally mitigated if the proper procedures are implemented.

Goodger, David. “Docstring Conventions.” Python Developer's Guide, 29 May 2001,

www.python.org/dev/peps/pep-0257/.

This article guides the conventions in making docstrings. Docstrings will be an important aspect of creating documentation of the code in order to make our code readable by other users. Docstrings will also assist with the API development.

Seitz, Justin. Black Hat Python: Python Programming for Hackers and Pentesters. No Starch

Press, 2015.

This book is a fairly comprehensive guide on creating a network attack platform in Python. As such, it will be useful for the attack and defense aspects of our project, since it will give a guide on how to build a network launcher to be controlled by the launcher itself. Moreover, chapters like the packet sniffing segment will be useful for recon and analysis, which is the third module planned. Functionally, this is a guide to the non-automated aspects of our project.

Sweigart, Al. Automate the Boring Stuff with Python: Practical Programming for Total

Beginners. 2015.

This books is a fairly introductory guide to automation using python. Chapter 15 will be useful as it specifically deals with the proper implementation of scheduling multiple tasks and launching other programs python, which should be useful for launcher. Additionally, chapter 16 goes over automating network flows, which can be used for the network output module. Functionally, this will be used as a sanity check and as a way of preventing overthinking, since this book is predominantly intended for new programmers and consequently gives a springboard for this project.

Yam, Wye, and Kede Jerel. “Theses and Dissertations.” *Strategies Used in Capture-the-Flag*

*Events Contributing to Team Performance,* Mar. 2016.

This is an analysis of the strategies that are utilized within capture the flag events. Strategies include: Reusing Exploits, Detecting exploits, Detect Outgoing Flags, Obfuscating exploits, Obfuscating ex-filtration, Mangling flags, Attacking Clients, Collusion, Leverage on External Resources. Tools include: Disassemblers and Debuggers, Exploitation Frameworks, Scripting Languages, Network Traffic Analysis Tools, Network Visualization Tools