Unit 6 - Design Doc vs Unit 11 - Exec Summary Outcomes

The major difference between our design document and our executive summary was the difference in the types of information gathered throughout. Our design document focused heavily on information gathering and reconnaissance with an emphasis on tools such as *whois, dig, NMap*, etc. Many of these tools may have ended up being used in our final analysis during the executive summary, but were left out as the information they garnered wasn't sufficiently useful to be reported or was incorporated into a more thorough vulnerability scan. An example would be using SSLScan to check the presence of transport layer security (TLS) or secure socket layer (SSL) encryption on traffic. This tool failed to find anything making an inelegant conclusion that SSL was not present. In the executive summary we scrapped this in favor of the results of more comprehensive scans by Nessus, which found and rated the lack of any traffic encryption to be the highest severity vulnerability.

Another difference between these two documents was the "what" of what was found vs the "why" where the design document tended to emphasize a plan of finding "what" information might be available, with less emphasis on the relevance of what the information might be useful for in future exploits. This is excusable by the length and scope limitations of this document, while the executive summary had more room for explanation and implication. This is where the executive summary was able to tie in the relationship between the scan results and a more detailed account of industry regulation and best practice. Ultimately, this showed growth in understanding and execution throughout the module, where we were able to better put together a more polished, professional analysis of a website, using more comprehensive and advanced scans to check for vulnerabilities.