Cyber Range Lab Assignment 10

Vulnerability Courses

Jon Mahoney

SRA 440W

# General Context

The recurring theme among the three different courses is examining vulnerabilities. The courses detail the different ways vulnerabilities are detected, the tools that are used, and the best practices in doing so. For instance, there are a wide variety of vulnerability scans that can be leveraged to detect vulnerabilities. An organization may identify the type of scan they want to employ by determining the scope or area, the available permissions, and the number of resources to be dedicated. As shown in the course videos, active scans can consume a significant amount of resources depending on the parameters or conditions. It may even be infeasible to support a wide range active scan during normal hours of operation as the scan may consume too many resources and inadvertently disrupt other business services. Some of the vulnerability scans mentioned in the course videos include the ability to detect vulnerabilities in IT governance. The vulnerability scanner, Nessus, can be used to scan for compliance failure to standards such as PCI DSS.

As for the best practices of vulnerability scanning, it is important to automate and validate scans. IT professionals should leverage automation and scripting to streamline vulnerability scans as well as to ensure they are consistent. A concept described through the course was the notion that vulnerability scans can return true or false, as well as positive or negative. Due to the possibility of these different outcomes, it is important to validate the results of scans as the scan may have returned a false negative, meaning the scan failed to raise a flag after encountering a vulnerability. While the courses mostly described vulnerability scanning, other topics such as general vulnerability detection were detailed as well. Additional information security topics such as penetration testing, reconnaissance, fingerprinting, and social engineering were briefly described as well.

# Screenshots



