Kobe Coleman

Professor Duvall

CYSE 368

7/1/2024

Reflection Paper 2

For these 50 Hours I did a lot of self-training. While waiting to be assigned a system to test I decided to gain better knowledge that I would start doing hack the box courses during the downtime at work. The hack the box course I did included pen testing process, network enumeration, information gathering, vulnerability assessment, and shells & payloads. These course on hack the box got me more comfortable with being on Linux. With these course I was hoping to utilize what I had learned to help with the tests that I may be assigned too and too make sure I don't slow down my fellow testers as much.

My team and I have weekly team meetings. With me taking the hack the box courses I was able to gain a better understanding of the high level talk my coworkers were having when talking about the systems they are testing. While I was also waiting I was getting familiar with some of the Linux tools I may use like Nmap and Metasploit. These are two essential tools a person must know to be able to do this kind of job. Nmap is used to scan IPs to see what ports are open and what version those IPs are running. Metasploit is essential since that is the main tool pen testers and hackers use to do their job. Metasploit contains a large number of tools and payloads that help pen tetsers to carry out attacks, evade detection, and search for vulnerabilities related to a version number or even application.