Kobe Coleman

Professor Duvall

CYSE 368

7/5/2024

Reflection Paper 5

The following 50 hours were spent on study and attempting to obtain access or exploit the system. After I receive my scans and eyewitness screenshots, we begin the study process. This is when we try to use all of the information we've gathered to hunt for exploits or strategies we can use to gain access to and/or manipulate the system. This step focuses on searching Google for CVEs and exploits that can be exploited on the machine. My coworkers and I also looked for old tests that pervious Pen Testers did on the same system. After completing this stage, we return to test the system using the information we gathered from the internet. We attempted Brute Force Login, which is "An SSH brute force attack is a hacking technique in which the attacker repeatedly tries different username and password combinations until gaining access to the remote server." The attacker employs automated tools capable of testing thousands of login and password combinations in a matter of seconds, making it a quick and effective method of compromising a server" (TrendMirco) utilizing credentials previously discovered by the old Pen Tester that did not work. We also attempted to do a SQL injection on the web pages, which “This injection works by manipulating any flaw in software where user input is required to access database information. Simply by injecting malicious characters, attackers could alter the workflow of the SQL statement, causing a remote code execution to steal user data and/or otherwise harm the targeted company” (Aqua-cloud) which failed to exploit the web-page. It was a great thing that most of the exploits and vulnerabilities were patched or failed since it means that our systems were really secured.

Work Cited

"What Is SSH Brute Force Attack and How to Deal with It." *Trend Micro Help Center*, helpcenter.trendmicro.com/en-us/article/tmka-19689. Accessed 5 July 2024.

Zhydkova, Tania. "Top 6 Most Common Vulnerabilities Found during Penetration Testing: Aqua Cloud." *Aqua Cloud - Best Software for Testing*, 2 Jan. 2024, aqua-cloud.io/6-most-common-vulnerabilities-found-during-penetration-testing/.