Vulnerability and Threat Analysis

RIS430 NAA

Assignment 5

Reflection Report

Prepared By Group 10,

Khondoker Ishmum Muhammad (155895212)

Aryan Santosh Saindane (136235215)

Ananthu Krishna Vadakkeppatt (154290217)

Syed Mujahid Hamid Ali (161202213)

Reflection Report

What have you studied?

We learnt a lot about different tools and how they can be applied in different situations so as to acquire a quick understanding of the security status of a system. Throughout this assignment we learnt about new tools suchs wfuzz, ffuf, skipfish, nikto and ZAP. New tools introduced new ways of going about looking for vulnerabilities.

We conducted an assessment of a host machine and discovered vulnerabilities that needed to be addressed. This led us to study various aspects of system hardening, which involves securing the system by configuring settings to specific values and implementing complex configurations. Additionally, we gained insights into the significance of firewalls in the context of system hardening. We also learned the importance of not leaving ports open to prevent potential security risks.

We have learned to make sure that sour systems, software, and the overall network infrastructure should always be kept up to date as vendors consistently provide system or software updates to the security to make sure that the vulnerabilities are mitigated.

What was Successful?

We were quite successful in getting a good overview of all the vulnerabilities that were affecting each operating system. Moreover, we were able to do a commendable job in trying to patch most of the vulnerabilities that were encountered across this assignment.

Additionally we were also able to have a good understanding of how tools such as wfuzz and ffuf worked on the basis of the fuzzing technique.

As a group we were able to learn a lot about the concept of system hardening throughout this assignment. This assignment gave us a really good opportunity to understand different system hardening practices, security vulnerabilities and risk management.

What was not Successful?

All of us did our best when we looked back at our progress throughout this assignment. However, some of the areas that we would like to improve would be implementing challenging configurations, testing the changes made to ensure that they do not produce any new threats and properly documenting measures taken to secure a system.

Despite these shortcomings, we should acknowledge that system hardening is a complex process that should be handled with extreme care and dedication. The group's efforts in analyzing as well as identifying various vulnerabilities, learning about different operating systems and patching different issues have shown the understanding that we have acquired of different security best practices.

Steps for improvement?

Based on our assessment and learning experiences, we can take the following steps to improve the security and hardening of the host machine or any future systems:

- Perform Regular Vulnerability Assessments: Regularly examine the system for vulnerabilities to find any potential flaws that need immediate attention.
- Implement recommended system hardening practices: Use industry best practices for system hardening, from straightforward configuration adjustments to more intricate security measures.

- Update and patch: To mitigate known vulnerabilities, make sure that the host machine's software, operating system, and apps are current with the most recent security updates.
- Close Unnecessary Ports: Close any open ports that are not required for the system's functionality to reduce the attack surface and limit potential entry points for attackers.