Running head: Exploiting Systems

# CS3910: Assignment 7: Exploiting Systems

# Mordred Cameron

# University of Colorado Colorado Springs

In partial fulfillment of the requirements for CS3910

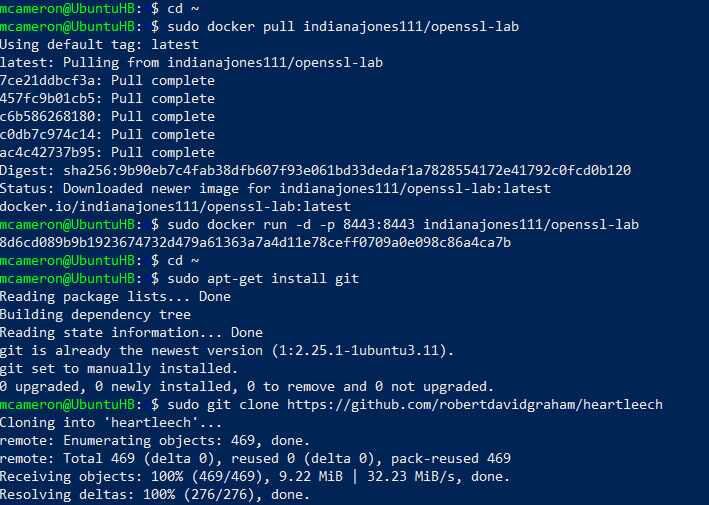
Instructor: Rhett Saunders

4/28/24

# Introduction to Exploiting Systems

In this assignment, the outcome provided insight into the Heartbleed bug through the OpenSSL security vulnerability and how to exploit it using the Heartleech code.

Assignment Results

Based on these screenshots, this is what I learnedA blue screen with white text

Description automatically generatedA blue screen with white text

Description automatically generatedA screenshot of a computer program

Description automatically generatedA screen shot of a computer program

Description automatically generatedA blue screen with white text

Description automatically generated

Heartbleed is certainly considered one of the biggest security vulnerabilities due to its expansive impact and relative simplicity. Because so many websites and services used OpenSSL, millions of these servers were vulnerable to the exploit. The exploit allowed attackers to access sensitive data through sent packets in disguise that were actually made up of much larger bytes. When the packet comes to the client as a reply “the Heartbeat Message from the server might contain only a portion of the information of these attributes mentioned. But, by repeating this several times, meaningful and confidential information can easily be obtained” (Kyatam et al., 2017). Although patches were released very quickly upon its discovery, the Heartbleed exploit stayed under the radar for an extended period of time, and continued to affect servers after it’s discovery due to lack of updating and maintenance.

Despite its widespread impact, Heartbleed has a severity impact of medium in contrast to ShellShock or Ghost which were both rated as critical. While these other exploits might have been more dangerous for big tech companies and more critical due to their execution and scope, Heartbleed caused more of a panic in the general public due to its massive impact and length of existance without discovery, and it is hard to say if it was more or less critical in comparison. Overall, each vulnerability is dangerous or impactful for different reasons, the takeaway being that security is constantly an exremely important factor to consider.

Conclusion

In summary, the Heartbleed exploit was a serious and impactful issue that continues to affect unpatched systems. We can learn from these situations to better understand and prepare for future vulnerabilities. Heartbleed was unique due to its “long exposure, ease of exploitation and attacks leaving no trace this exposure should be taken seriously” (Heartbleed, 2020). This assignment helped me learn about the severity of the exploit and how it is used to access sensitive information.

References

Kyatam, S., Alhayajneh, A., & Hayajneh, T. (2017, May). Heartbleed attacks implementation and vulnerability. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE.

Heartbleed. (2020, June 3). The heartbleed bug. Heartbleed Bug. Retrieved April 19, 2023, from <https://heartbleed.com/>