AMMARAH KHALEEQ
01-235172-012

Cyber warfare simulator offensive and defensive threat modeling and evaluation.

Bachelor of Science in Information Technology

Supervisor: Prof. Dr. Faisal Bashir

Department of Computer Science
Bahria University, Islamabad

June 2020

Abstract

Cyber threats are on the rise and with each passing year significant increase is observed internationally. Despite numerous anti-malware measures, cybercriminals and hackers aren't ones to give up easily, especially not as long as there's money to be made in malware. Although, some traditionally-popular forms of malware appear to be losing ground in recent years, as hackers and cybercriminals are changing their tactics to attack new or underutilized vulnerabilities [1].

Information Systems Audit and Control Association (ISACA), in its latest 2020 annual report, highlighted that 62% of cybersecurity professionals believe their organization's cybersecurity team is understaffed. Understaffing among organizations, including business and government, could create a strain on existing staff and lead to an increased risk from malware threats. The demand for cyber security professionals is increasing year-over-year. Industry has always raised concern over the readiness and skill set of new employees especially in the offensive & defensive domains of cyber security. It is of utmost importance that offensive security skillset should be developed in students and cyber security professionals that should be comparable to expertise of cyber criminals.

A cyber range is a safe environment for training and learning about the execution of cyberattacks. If an organization wants to train and keeping the main systems unaffected cyber range is the best approach. Cyber ranges are the exact mirror of the real systems. It is a simulation and has complete resources to learn without impacting the real system. Previously the cyber ranges where in the fixed places and locality. Now a day's cyber ranges are shifting to the cloud for flexibility. Cyber warfare simulators are advanced cyber ranges were multiple user can launch and defend against cyberattacks in a virtual environment. Besides Cyber range used as a trainer platform, it is also used as a training purpose in securing the system. Network and infrastructure security are widely ignored due to less awareness. For such reasons, the proposed project is to give knowledge and training to people by learning about networking infrastructure and its vulnerabilities by applying different practices like security hacking, malware analysis, phishing, etc.

In this Final Year Project (FYP), a cyber warfare simulator is developed with focus on a user friendly digital-end for generating simulations. The cyber warfare platform is created using advanced and latest technologies for better performance. The front end is designed in React JS and in the backend Docker, Django and Node JS is used allowing the user to have an interactive interface to learn and train themselves, with a user friendly environment. The threat base or vulnerable software/machines are built using containers use Docker technology. It allows resource friendly virtualization upon same operating system kernel, as compared to dedicated virtual machines used in many other similar products. The drawback containers have is that it only supports Unix based programs and software packages but its efficient resource usage is enough to prove its worth. The developed cyber warfare simulator provides an excellent opportunity for expansion by increasing new Docker images of advance vulnerabilities. The developed product can be used to train both students and professionals in the domain of penetration testing.

Acknowledgments

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, all commendations to Allah for the qualities and His approval in finishing this undertaking. Foremost, I would like to express my sincere gratitude to my advisor Prof. Dr. Faisal Bashir for the continuous support of my final year project and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis and Final year project. I could not have imagined having a better advisor and mentor for my FYP. He puts his additional knowledge and efforts for my help and was always there for our guidance.

AMMARAH KHALEEQ

Bahria University, Islamabad

January, 2021

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

DSA	Data Structure and Algorithms
OOP	Object Oriented Programming
PF	Programming Fundamentals
SE	Software Engineering
SQL	Structured Query Language
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICODE	Unique, Universal, and Uniform Character encoding
XML	Extensible Markup Language