



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
© Ammarah Khaleeq 2021

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 were 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 where 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.

AMMARAHA KHALEEQ

Bahria University, Islamabad

January, 2021

Contents

Abstract	i
Chapter 1	1
1. Introduction	1
1.1 Cyber Range:	3
1.2 Offensive and defensive Threat Modeling	3
1.3 Cyber Warfare Simulator /Cyber Range	3
1.4 Objectives of Cyber Warfare Simulator	4
1.5 Output of the project	4
1.6 Problem Description Limitation in the existing system	4
1.7 Proposed System (Project Outcome):	5
Chapter 2	6
2. Literature Review.....	6
2.1 History of Cyber Security, Cyber Crime and Cyber Range	6
2.2 Cyber Security and Why it is important:.....	7
2.3 Cyber Ranges:	8
2.4 Related Work:	8
Chapter 3	10
3. Requirement Specifications	10
3.2 Existing System	10
3.3 Problem Description Limitation in the existing system	12
3.4 Proposed System (Project Outcome):	12
3.5 Requirement Specifications	12
3.6 Use Cases	13
Chapter 4	17
4. Design	17
4.2 Data Flow Diagram Developed Cyber warfare Simulator	18
4.3 Activity Diagram	19
4.4 Sequence Diagram	19
4.5 GUI Design.....	20
Chapter 5	26

5. System Implementation	26
5.1 Introduction	26
5.2 System Architecture	26
5.3 User Interface	27
5.4 Middleware/ Backend	27
5.5 Components	28
5.6 Tools and Technologies Used	28
Chapter 6	30
6. System Testing and Evaluation	30
6.1 Introduction	30
6.2 Importance of testing	30
6.3 What are Test Cases and their importance	30
6.4 Testing Cyber warfare simulator	31
Chapter 7	33
7. Conclusions	33
7.1 Final Conclusion.....	33
7.2 Future Enhancement	33
References.....	34

List of Figures

Figure 1 Cyber Attacks Globally	1
Figure 2 Architectural Diagram Of the existing system	11
Figure 3 Use Case Diagram	14
Figure 4 Architectural Diagram	18
Figure 5 Data Flow Diagram	18
Figure 6 Activity Diagram	19
Figure 7 Sequence Diagram Admin.....	20
Figure 8 Sequence Diagram User	20
Figure 9 Sign Up.....	21
Figure 10 Sign Up.....	21
Figure 11 Sign In User.....	22
Figure 12 Sign In User.....	22
Figure 13 Sign In Admin	23
Figure 14 User Panel Dashboard	23
Figure 15 User Panel Leader Board.....	24
Figure 16 User Panel Leader Board.....	24
Figure 17 Admin Panel Dashboard.....	25
Figure 18 Admin Panel Create Scenarios	25
Figure 19 Architectural Diagram	27
Figure 20 Docker	28
Figure 21 VS Code.....	29

List of Tables

Table 1 Related Work	8
Table 2 Login Use Case	14
Table 3 Registration Use Case	15
Table 4 Play Scenarios.....	15
Table 5 Admin Create Scenarios	15
Table 6 Sign Up	31
Table 7 Login with correct credentials	31
Table 8 Login with incorrect credentials	32
Table 9 Create Scenario	32
Table 10 Start Drill	32

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