CYBER TEST BEDS FOR THE SIMULATION AND MODELING OF CYBER WAR GAMES

By

Marium Khalid

A thesis submitted to the Faculty of Information Security Department, Military College of Signals, National University of Science and Technology, Pakistan in partial fulfillment of the requirements for the degree of Master of Science in Information Security

May 2016

ABSTRACT

Cyber space is considered as the fifth domain of warfare. Recently cyber space has evolved in to a war zone worldwide due to which it has become an important aspect for the military and government. As a matter of fact these days more and more data is present online and the conventional ways of maintaining records and storing data have been ruled out. Due to enormous data present online all the countries worldwide are taking measures to secure their data uploaded on internet. Besides, every country is preparing its own cyber army with specialized skills to defend their cyber borders.

This thesis tends to investigate the methods used to train cyber army. Cyber war games as one of the most important training method have been highlighted. The thesis focuses on the simulation of war games using cyber test beds as an important platform. Since various methods are used by attackers we will consider the latest technique of attacking enemy cyber space with malwares. We will focus on how to train the army on malware defense/ reverse engineering rather than attacking. Malware Reverse engineering is an important area in information security to know the mechanics and working of malwares to detect, prevent and analyze the malware attacks. We have build a prototype for developing war games by proposing our own methodology that will help in future for simulation the of more advanced war games.

In order to propose the methodology for developing war games the first step is to identify different elements of war games. The relationship between the war games and test beds have been well developed in this thesis and test beds have been considered as a basic building block for creating a war game. Moreover we have proposed model for war games. The model has been developed according to the latest trends of malware reverse engineering. The game architecture and functioning is decided for the purpose of teaching the malware reverse engineering techniques in the academia and research and to provide better ways of training on malware defense with

best utilization of resources. It is found that the proposed game model is helpful in many ways with the respect to war games and malware analysis. Finally in the end the framework has been proposed for the design of cyber test beds on malware defense.

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

DEDICATION

I dedicate this thesis to my parents, who supported in every walk of life and also to my siblings, family members and all friends.

ACKNOWLEDGMENT

In the name of Allah, the Most Gracious and the Most Merciful

All praises to Allah for the strengths and His blessing in completing this thesis. I would like to convey my gratitude to my supervisor, Dr. Mehreen Afzal for her supervision and constant support. Her full devotion and dedication towards students research, constructive comments and suggestions throughout the experimental analysis and thesis works are major contributions for the success of this research. Also, I would thank my committee members; Dr. Babar Aslam, Dr. Imran Rashid and Lecturer Mian Mohammad Waseem Iqbal for their support and knowledge regarding this topic.

I would also thank system administration team of MIS Cell of Military College of Signals, for providing me with the required MCS network related data. Also, I would like to thank IPC for providing me a good research environment with their supporting staff.

Last, but not the least, I am highly thankful to my parents (Khalid Masood and Jamila Khalid), siblings (Huma, Nida, Nimra, Sonu) and friends (Tania, Raeesa, Mahvish, Faiza, Sadia). They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them all for their care, love and support through my times of stress and excitement.

In the end special thanks to Lipton Yellow Label.

TABLE OF CONTENTS

LIST OF FIGURES

LSIT OF TABLES

Chapter 1

INTRODUCTION

1.1 Introduction

This chapter is about introducing the concept of cyber war games in the field of information and communication technology. The chapter gives the overview of research in the area of war games. Further we describe our contribution in this field by discussing the aims and objectives of the research.

1.2 Overview Of Thesis

Today, the conventional warfare has been taken over by the cyber warfare due to tremendously increasing reliability on cyber space. Conventional warfare involves physically targeting the enemy whereas cyber warfare involves remote exploitation through internet that poses some serious threats to the critical cyber infrastructure of a state. To win war for a country specialized training is being conducted to train personnel to fight enemy in conventional warfare. Since now a days cyber warfare is used as a weapon to win conventional warfare therefore there is a dire need to conduct specialized trainings on cyber warfare as well. For this purpose the concept of cyber war games have been introduced to conduct trainings for cyber soldiers. Cyber war games provide the best platform for a state to develop offensive and defensive capabilities in cyber space for the security and protection of their cyber borders. The armed forces have conducted war games to test capabilities, surface gaps in plans and build their leaders abilities to make decisions in real

time. The cyber games help the state to respond realistic simulated cyber crisis.

However cyber warfare is a very broad domain that involves two competitors fighting each other by launching attacks and defending their own network for cyber espionage. The competitors could be two states, two organizations and the cyber criminals/ terrorists attacking for retrieving secret information. Similarly cyber war games can be used in academia to train students to master the design and defense systems by practically doing it in an adversarial environment.

1.3 Motivation

Probability of occurrence of cyber attack incidents is rising with time and causing damage to individuals, websites, servers and network daily. The cyber space has been used by hackers, hacktivists and cyber-terrorists frequently. Highly sophisticated and deceptive cyber attacks can bypass the security mechanisms easily. The rapidly growing cyber security threats/ challenges pose a serious threat to the states military and government sectors. The online information need to be in safe hands. Therefore we need to have a training platform for cyber specialists to provide them with closely related real world scenarios to prepare them for cyber warfare.

The latest technique used by hackers these days to capture enemy information is the use of malware attacks. We need to address malware attack and defense scenarios through war games to include them as a necessary training element. By using war games we need to prepare ourselves for the best defense by considering the simplest situation of virus attack to the most sophisticated APT attack.

1.4 Problem Statement

Cyber war games are meant for strengthening offensive and defensive capabilities in cyber space. Many simulation/ emulation platforms exist, some are free and open source while others are

closed source. The relation between cyber test beds and cyber war games is not well established. Limitations of the existing test beds in respect of cyber war game for different scenarios especially malware detection is yet to be explored. Attack and response scenario developed for malware detection through some existing open source/ online simulation/ emulation environment, with the objective of training the response team to combat enemy during cyber crisis, is not available in existing researches in this field.

1.5 Aims and Objectives

The main aim of our research is to:

a. Provide a proof of concept of cyber war gaming and cyber war test beds.

b. How can we relate cyber war games with cyber test bed and how cyber test beds can be helpful in developing cyber war games.

c. Build a simulation/ emulation environment for campus using one of the existing test beds.

d. Propose a game model for test bed environment and develop various exercises for it on malware defense.

e. Propose a framework for malware analysis test bed that could be implemented on our network to analyze advanced malwares in future by using techniques of cyber war games.

1.6 Research Methodolgy

This research has two key elements. The first step is to provide a proof of concept of cyber war games and test beds by developing a war game. The second line of research focuses on using the simulation/ emulation platform in a war game to address several areas within the domain of cyber security by building some exercises on the test bed. The main pupose of the research will be to train persons on malware defense. The research is categorized in to few major steps. The first

step involves the exploration of existing war games and discuss various findings about war games. The war games are build for various purposes in a different way. The next step includes the study of war games for one particular domain. The study of war games further leads to proposing the basics steps for building war game for malware analysis. In the last the game model is developed to merge the reverse engineering techniques of malwares in a war game to achieve the results.

1.7 Thesis Contributions

The major contributions of thesis are explained as follows:

a. During the literature review phase we discussed various cyber war games developed for different purpose [1]. We have tried to extract the taxonomy of war games by categorizing them according to the outcomes of a war game. The taxonomy of war game in terms of its output is important to define because that will define the scope of the game and the purpose the game for which it is built.

b. While investigating various techniques for creating the games we explored test benches that are really helpful in building the war games [2] and [3]. We have put effort to establish the relationship between war games and cyber test beds as a useful technology for building war games.

c. The research thesis proposes certain steps to develop war games after exploring the existing games and the methods/ techniques for creating the war games. These steps are used as a prototype for war gaming.

d. To the best of our knowledge, the game model for malware analysis has been proposed for the first time to understand the malware scripts.

e. This thesis contributes towards the design and a proof-of-concept implementation of developing cyber war games techniques for malware analysis using cyber test benches. The proposed technique is an extension of the previous research conducted in this direction and has helped to

extend the work of war games described in old schemes [4] and [5].

f. The proposed technique is evaluated in the perspective of war games and malware analysis to present a framework for malware analysis test bed to be used in cyber war games. In order to analyze the war games under study effectively, different test benches have been explored that are using real systems and virtualization technology. The main goal behind focusing on test benches is using them to analyze the effect of using the test-beds in the performance of the war games due to their automation approach and proper utilization of resources.

1.8 Thesis Organization

The rest of the thesis work is described as follows:

Chapter 2 describes the complete taxonomy of war games by identifying major elements of war games. These elements are discussed one by one in detail.

In Chapter 3, the proposed solution is given to establish the relationship between war games and test beds and test beds have been declared as a basic building block for creating war games. The steps for malware analysis as a war game are outlined.

In Chapter 4, based on the proposed solution a game model is presented by keeping in mind the limitations of existing test benches and existing plans for malware containment and analysis. These plans have been merged and given the shape of a war game model. The implementation of war game model has also been discussed in this chapter in detail.

Finally, Chapter 5 presents some snapshots of experimental analysis for the proposed model. Experiments show the practical feasibility for the implementation of the proposed game model.

In Chapter 6, concluding remarks have been given. The achieved objectives have been explained in detail. Besides, the limitation and future directions have been discussed.

1.9 Conclusion

In this chapter we have discussed in detail about cyber warfare and its training elements. This chapter tends to provide a brief introduction on war games used to train the cyber response specialists. The main objectives, motivation, problem statement and scope of the thesis are underlined. In the end the complete organization of the rest of the thesis is briefly described.

Chapter 2

A SURVEY OF CYBER WAR GAMES

2.1 Introduction

In this chapter we give an overview of the existing cyber war games and their techniques. We present a complete taxonomy that characterizes the war games based on their outputs. We have performed a survey on the related literature, placing each work with described categories and briefly describe them in order to provide the reader with a basic idea of the proposed work. In this way the reader can realize the current research developments in this area and identify the outstanding issues. We also discuss about the malware reverse engineering and its relation with war games.

2.2 Cyber War Games

The cyber war has become inevitable and relentless due to the increasing cyber conflicts on internet. The war games in particular focus on the highly stylized representation of cyber conflicts in a simulation model. War games are built for military, academic and private sectors. The study summarizes recently existing war games and describe their purpose and functionality. We are interested in knowing the outcomes of a war game for which they are developed. It highlights the latest trends for which war games have been developed recently. Several game models have been designed for different purpose including information security and information assurance education, training and awareness, for the detailed examination and testing of security related

network algorithms, detection units and frameworks and for the understanding of malwares and attack scripts and their counter measures [4]. So far, different cyber games have been developed to simulate diverse aspects of building and managing information systems and defense exercise models have been presented that can be used to train cyber response specialists to respond to real time cyber crisis. The games are available in the form of simulation tool, emulation environment and laboratories as well [1] [6] and [4]. These include SECUSIM, Cyber Ciege, RADICL, Deter lab, Planet lab, RINSE, Net Warrior, Cyber Protect, SANS Net wars, Capture the Flag and MAADNET etc. We consider the following metrics for discussing war games.

1. War games in the form of simulation, emulation, test bed platform, real time laboratory are dicussed and test beds war games are highlighted as in [7].

2. The over view of war games, their purpose and functioning.

3. Any capabilities or features from malware analysis perspective will be highlighted in the games discussed below.

2.2.1 SECUSIM:

It is a simulation tool based on advanced modeling and simulation concepts implemented on Visual C++ to simulate various attacks on multiple network components. It covers simulation of almost 20 attack scenarios against hundred network components. It has five operating modes basic mode, intermediate, advanced, professional and application mode. This tool is a good example for the training and awareness of basic network concepts and their functioning [8].

2.2.2 CYBER CIEGE:

Cyber Ciege is an innovative computer based network security simulation tool packaged as a video game to teach information assurance concepts. In this game the players construct and

defend computer networks and find the flaws and loop holes in their configuration of network components. The first objective of Cyber Ciege is to create a tool for the simulation of a large number of scenarios. It has a unique simulations engine with scenario definition language and scenario definition tool to allow the students to create their own advanced scenarios. It is available with no cost educational license [9].

2.2.3 CAPTURE THE FLAG:

The CTF exercises are designed for students to teach few concepts of cyber security. These exercises are different from previous tools because they engage team of students with various scenarios of attack and defense. One team of students is responsible for attacking and the other puts effort to protect the network and data depending upon the scenario. These exercises are built on test bed environment known as Deter lab. The test bed environment is very helpful for the deployment of cyber war games and in this thesis we will further discuss about test bed platforms and their features [1]. There are few instances of CTF.

2.2.3.1 DEFCON

This competition is arranged yearly based on hackers convention. It has multile qualifying rounds and knock out stages in the competition. It is based on teaming concepts. This particular event has been running since 1993 [10].

2.2.3.2 International Capture The Flag

iCTF is limited to academia hosted by the university of california, Sant Barbara. This competition also involves teams with each team running an identical parallel version of the game. It has a virual competition environment. This has been running since 2004 [11] and [7].

2.2.3.3 Collegiate Cyber Defence Competition

CCDC is also an academia based competition. The main purpose of this competition is to inculcate the techniques of defending network against outside attacks in the players by creating network defense scenarios.The CCDC 2006 competition had multiple teams on the same network to play for a set of real world business scenarios. The teams had to meet tough deadlines for task completion. However the game focused on task completion with some considerations given to detectective problem solving [11].

2.2.3.4 Cyber Defense Exercise

CDX is an annual competition that takes place ina very sophisticated environment limited to military and government officials only. The CDX locked shield 2014 competition involved various forensic tasks for the competitors that include investigating a large captured network traffic, NTFS file system, encryption, malware identification, remote response and registry and remp file etc [7].

2.2.4 RADICL:

It is a real time laboratory built by students with a large number of physical resources/ hardware, network components and softwares. The purpose of this lab is to provide the war gaming environment by equipping the lab with necessary resources. It provides a good environment for students to perform exercises like CTF, DOS attacks malware analysis and network discovery. The RADICL reconfigurability feature allows more than one student at a time to use multiple resources without interference. This lab is built with maximum resources and features [2].

2.2.5 NET WARIOR:

artment of Defense that provides the user opportunity to configure network components features to run them against real world network security attacks. It also provides a good performance review of user as well. But this tool is now quite old. It was developed in 1999 and it has not been updated since then [12].

2.2.6 MAADNET:

It is a tool based on client server architecture using object oriented design with java applet. The user on the client side builds a network using a network builder and then creates a scenario using scenario generator that is then submitted to the server side to simulate the scenario using a simulation engine [13].

2.2.7 RINSE:

It is more advanced network simulator that serves the same purpo It is developed by Department of Defense. It is also an advanced network simulator designed for simulating network attacks [4].

2.2.8 CYBER PROTECT:

Cyber Protect is another effective network simulation tool developed by Depse as other network simulator tools do to simulate network attacks. This simulator is designed differently to perform more effectively [14].

2.2.9 NETENGINE:

It is more advanced network simulator that serves the same purpose as other network simulator tools do to simulate network attacks. This simulator is designed differently to perform more

effectively [14].

2.2.10 EMULAB:

Emulab is a project of university of Utah. This software is used for over twenty other testbeds worldwide. This facility is mainly used in the area of networking, security and distributed systems. Emulab is developed using support of tools generating background network traffic and tools for simulating network links. It also supports automation of experiment setup and tear down including the installation of operating systems, creating network topologies and reservation of resources [15].

2.2.11 DETERLAB:

Deterlab is an exclusive all in all package to be used for developing a war game for malware analysis. This platform is a shared internet accessible platform and is available on internet to be remotely accessible by the academic and research users to initiate project by requesting the Deter operational staff. One of the main characteristic of Deter is that all experiments are isolated from each other and only allowed to access when the project leader acknowledges the request. The experiments are also isolated from internet also and no traffic is allowed to connect to the internet to prevent any mal traffic from coming in and out of the test bed. So, in conclusion when it comes to sharing of material and experiments deter community have the rights to allow and deny other users to see and run their project depending on the criticality of the project. On the other hand when it comes to isolation the experiment itself could be isolated from other experiments as well as the platform is also made isolated from the external world to provide safe and sound experimentation of malwares limiting only the remote users who can easily access the test bed [6] and [16].

Cyber War Games	Use Test bed technology	Malware Analysis Capability
SECUSIM	NO	YES
Cyber Ciege	YES	NO
Capture The Flag	YES	NO
RADICL	YES	NO
Netwarior	YES	NO
Cyber Protect	YES	NO
MAADNET	YES	NO
RINSE	NO	YES
NETENGINE	NO	YES
PLANETLAB	YES	NO
EMULAB	YES	YES
DETER	YES	YES

Table 2.1: Cyber War Games capability of Test bed and Malware Detection

2.2.12 PLANETLAB:

Planet lab is a great remote online facility like Deterlab that serves the same purpose but slightly with a different technique and approach.

2.3 CYBER WAR GAMES TAXONOMY

The compiled information on war games assist us to propose a taxonomy. We have explored the various components of cyber war game taxonomy. War games produce various types of outcomes that are categorized in to two basic elements which are further divided in to sub categories. This taxonomy supports a profound improvement in developing/ creating a cyber war game for

particular purpose. The war game taxonomy incorporates various elements that are useful in classification of the existing war games on the basis of proposed techniques for delivering particular results/ output. Taxonomy will also provide a systematic listing enabling a user to select appropriate technique for war game on the basis of outcomes of war games. Such taxonomy will become standard framework that provides guidance, helping users learn and explore what they need to know about war game. The output could be tangible or intangible depending on the purpose for which they are build. Figure 2.1 gives the proposed taxonomy of war games.

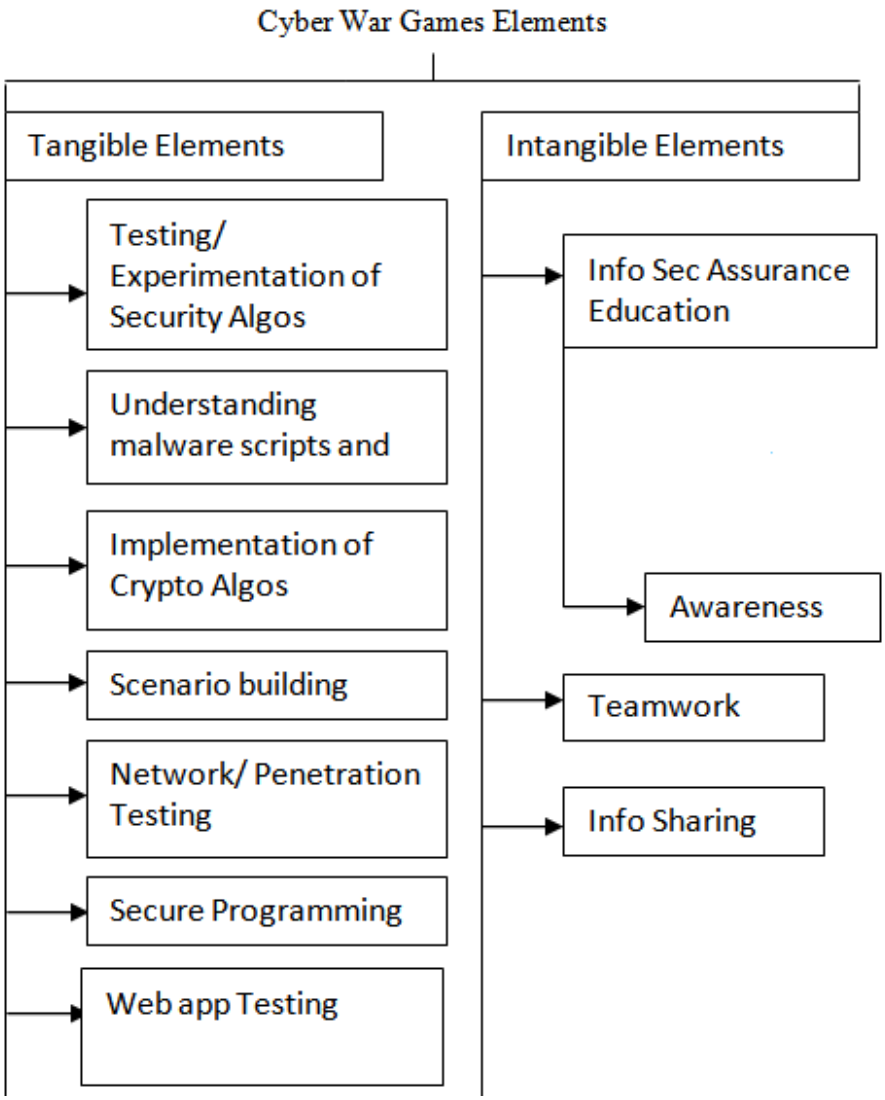

Figure 2.1: Cyber War Games Taxonomy

2.3.1 INTANGIBLE ELEMENTS

Possible intangible outputs that exist are education/ awareness/ information assurance and training. Table 1 show possible techniques/ methodology include a simulation platform to represent various security issues by building small exercises with the help of any suitable tool/ development engine on a standalone system with no other physical resources required. After deep study, we analyze war games for such purpose do not need teaming and scoring phenomenon. They also do not require a test bed environment for experimentation and testing because simulation tends to represent more intangible elements of actual operation and reduce reality to a much more detailed model.

2.3.1.1 INFO ASSURANCE EDUCATION/ TRAINING

A primary objective of developing war games has been improvement of information assurance education and training for cyber response specialists [17]. The game design depends upon the learning objectives of the game. The educational games are mostly designed for training of the body of knowledge. Games developed for professional training of cyber response specialists has more complex design. Such trainings must also address the needs and security policies of a particular organization. According to [18] a number of techniques exist in the past for cyber security training which includes web based sessions, teleconferencing sessions, instructor led sessions, seminars, workshops, email alerts, periodic newsletters but all of them have shortcomings that are addressed with the use of war games that has set the momentum for cyber security training in this modern era. One such highly interactive and flexible training tool is available online that supports training objectives by engaging users in security related adventures [19].

2.3.1.2 AWARENESS

The best approach to secure information is to provide general awareness on information assurance concepts through the use of effective tools. This will help improve the reactions of any person when security is attempted to be compromised. For the general awareness of end users small scale simulations are of great help since they allow user interaction and hands on experience [19].

2.3.1.3 TEAM WORK

The large scale war games are often build with team work based approach in which agents of various teams takes part in a competitive environment to show their best of the security knowledge. In this sort of platform agents of same team cooperate with each other to complete the end task and agents of different teams compete with each other with different approach. For example the different agents in one team may split their roles and tasks on the basis of their need and the team members which are called agents achieve their tasks for reaching the common long time goal [20]. War game with multi agent systems is also an active area of research these days.

2.3.1.4 INFO SHARING

The modern form of war game has also taken in to consideration the importance of information sharing as well. This is done by the online availability of game and customization of games for various scenarios where anyone can customize according to the situation needed and share it with others to help them use in future [2] and [3].

2.3.2 TANGIBLE ELEMENTS

On the other side when we talk about war games that deliver results closer to reality for training the experts and professionals the criteria is somehow different. The simulations tools in collaboration

with some virtualization may be needed to emulate large networks on a cyber test bed [2] and [3]. A management platform may also be needed to perform scenario development for emulating various networks. This may also be needed to manage the teams and auto scoring phenomenon for fair competition. The physical resources may also be required depending on the complexity of scenario. Operating system customization in such cases will help to create experiments on test bed with diversity and versatility. A network topology simulator will also help in this case. At last the study of war games is not only limited to simulation/ emulation platforms but building real time laboratories for war games and modelling real time scenarios is the biggest achievement so far [7]. But a lot of processing and physical resources in combination with simulation/ emulation techniques is required. For creating such laboratories the focus is more shifted towards defining the specifications and configurations of hardware needed in the laboratory. The scenario building in such case may take time even longer than expected due to limited resources in the lab and managing the resources manually. Defining teams and auto scoring mechanism will make the game show interesting. The hardware and software requirements may differ depending on the tools and techniques used by the teams. The complexity of scenario will be judged according to the hardware and software needed by the attacking and defending team. There must also be a neutral team that is passively involved in the competition and is responsible for keeping track of both the teams, awarding points on the basis of performance and may also give penalties on any foul actions by the competitor teams.

2.3.2.1 TESTING/ EXPERIMENTATION OF SECURITY ALGOS

Mostly network security Algos involve monitoring of traffic/ data on particular network. Testing the network security algorithms properly to test their performance is a very time consuming and difficult process. For security related Algos mostly the output is known before the software is

deployed. This is true in case of detection of security related events such as generating alarms in case of any intrusion on host or network. Cyber war games are also used to deal with such scenarios of testing network security Algos. According to [21] an emulation platform has been built to take advantage of the captured traffic and using the DETER network to generate closely realistic network traffic according to interest.

2.3.2.2 IMPLEMENTATION OF CRYPTO ALGORITHMS

The researchers design and implement several cryptographic Algos for exchange of information. The strength of these cryptographic Algos is tested through various experiments [1].

2.3.2.3 REAL TIME SCENARIO BUILDING

This is true that we cannot encounter all real world scenarios so we think of simulating those scenarios as if we are dealing real world networks. Imitating real world scenarios is not an easy task. Simulation models are the extended representation of real world scenarios. Emulation platforms are somewhat closer to a realistic representation a real world phenomenon. Such type of simulation and emulation platforms does exist with certain limitations [2] and [3]. The most efficient platform for such purpose will not require task to be done from scratch each the new scenario is being build. They must have flexibility to cater for various scenarios in different environments.

2.3.2.4 NETWORK/ PENETRATION TESTING

It is really very important to secure our government and military networks and websites. For the testing of network and websites pen testing methods are used to find loop holes and vulnerabilities in the network and website. There are several standard ways for pen testing. The method used for

network pen testing is somehow different from website pen testing. But these methods use some tools to check the vulnerabilities and loop holes. The pen testing scenarios could be created in a test bed environment and we can merge this field of pen testing as well with a cyber war game.

2.3.2.5 SECURE PROGRAMMING

The flaws in programming could leave loop holes in the source code that is the greatest security threat and these vulnerabilities are then exploited by a hacker. The programmer must be aware of the security requirements to make the source code secure. Therefore the source code written by a programmer is tested later on the security team to identify the weaknesses in the code that a typical programmer is unaware of.

2.3.2.6 DIGITAL FORENSICS

Digital forensic is used to recover data from any digital device e:g computers, laptop, mobile phone, SD cards, tablets etc. The recovery tools are used for retrieving the present and deleted data from the device. These tools are openly and commercially available. The tools of forensics in collaboration with the test bed that supports these tools can be used for building small exercises to practice the art of digital forensics.

2.3.2.7 WEB APPLICATION TESTING

The cyber war games are also utilized to develop expertise in web application testing. The methods pf web application testing techniques and methods are merged in a war game to open new ways of learning the pen testing.

2.3.2.8 UNDERSTANDING MALWARE SCRIPTS AND REVERSE ENGINEERING TECHNIQUES

The modern malware are designed to communicate with outside world across the internet. In todays prevention techniques containment is one such good practice in which a malware is refrained from communicating to the outer world by developing an isolated platform. In this way malwares could be evaluated under controlled environment with development of some containment policies. Such techniques are used to prevent malware from harming others while ensuring that it still exhibits its inheritance behaviour. The Deterlab [22] has allowed the safe experimentation of such risky malware in a Deterlab test bed. The malwares attacks are mostly used because of their capability of remote exploitation. The severity of attacks differs depending upon the damage they cause. To understand the functioning and mechanics of malwares the reverse engineering of malwares is done. The malware analysts use reverse engineering techniques to know the mechanics of malwares to measure the damage caused by the malware and detect them in future and take further preventive measures. The two most common techniques used by analysts for understanding malware scripts are, Static analysis and Dynamic analysis. Static analysis is done by using tools and techniques to uncover the malware code to understand its behaviour. In dynamic analysis the malware is run in a safe/ virtual/ sandboxed environment, and then methods are used to understand the functioning of malware by detecting the changes done on the victim system after the malware is run. Even now a days malwares are designed to detect the virtualized environment and are instructed to behave differently on virtual environment from their normal functioning. To detect and understand such malwares functioning more advanced techniques are used in cyber war games to help in the understanding of malware scripts as well. The reverse engineering tools are integrated in the game to detect and analyze malwares.

Cyber War Games	**Category**
SECUSIM	Intangible
Cyber Ciege	Intangible
Capture The Flag	Tangible
RADICL	Tangible
Netwarior	Tangible
Cyber Protect	Tangible
MAADNET	Tangible
RINSE	Tangible
NETENGINE	Tangible
PLANETLAB	Tangible and Intangible
EMULAB	Tangible and Intangible
DETER	Tangible and Intangible

Table 2.2: Existing Solutions in Taxonomy

2.4 Conclusion

In this chapter the well-known cyber war games have been identified and the purpose of creating these games. The development tools and simulation/ emulation techniques used for development of war games are also highlighted. The purpose of devloping war games is also briefly discussed. Then, types of malware attacks have been discussed and the methods of reverse engineering of malware attacks have been explained.

Chapter 3

A NOVEL APPROACH FOR DEVELOPING CYBER WAR GAMES

3.1 Introduction

Cyber war games in particular focus on the highly stylized representation of cyber conflicts in a simulation model. This chapter focuses on the development of cyber war games. We propose the way to radically increase the usefulness and scope of test bed based cyber war games. It represents the main idea for the development of a prototype for building war games particularly for malware analysis.

3.2 AN OVERVIEW FOR THE DEVELOPMENT OF WAR GAMES

War games have been recognized as a critical area in the field of cyber security. Due to the recent cyber attacks, cyber warfare has become a very hot topic. The incidents of cyber attacks in Estonia in May 2007, the most famous APT attack stuxnet on Irans nuclear plant at Natanz in 2009 and the recent DDOS attacks defacing the Israeli websites have been under debate for a long time [12]. This chapter attempts to provide a solution for carrying out war games to help counter these cyber attacks. This chapter helps us to think of war games in perspective of malwares which has been the most prominent and deadly method used by an attacker these days. Numerous innovative technologies have been introduced for the development and implementation of war games. Cyber test beds facilitates in the implementation/ deployment of war games by offering the integration of various tools and techniques on a single platform. We propose the steps to create war games

for malware analysis. The malwares is the most dangerous weapon of an enemy in cyber space and we tend to create small exercises to carry out simulation of war games. On the other hand more and more versatile malwares are evolving these days to be used as an important weapon for a war game. Intelligent competitors are working to merge the field of malware analysis and war games to produce results by offering the best defensive mechanism. The advantage of merging both fields will provide a novel and interesting way of educating and training the students in the field of malware analysis.The tools and techniques to be used for malware analysis is integrated with war games to build a training platform for malware analysis.

3.3 PROPOSED SOLUTION

The basic approach for developing war game for malware analysis require various factors including the study of war games and their development in correlation with the study of malware reverse engineering. So far we discussed cyber war games in our previous chapter highlighting the usefulness of game and describing the basic purpose and functionality of the games. There are many cyber war games/ cyber drills/ cyber exercises that have been developed nation wide. Few exercises are built on international level that involves participation of teams from countries. But these are not accessible openly on internet. Therefore we propose steps for creating war games using the resources that are openly available on internet. Since cyber test beds are openly available to the academia and research community so we present a test bed based approach for cyber war games to be used for malware analysis.

3.4 REQUIREMENTS FOR DECIDING TEST BED

The cyber testbeds are considered to be the best platform for developing a war game but it is really very important to decide suitable test bed that could nearly meet our requirements. So deciding

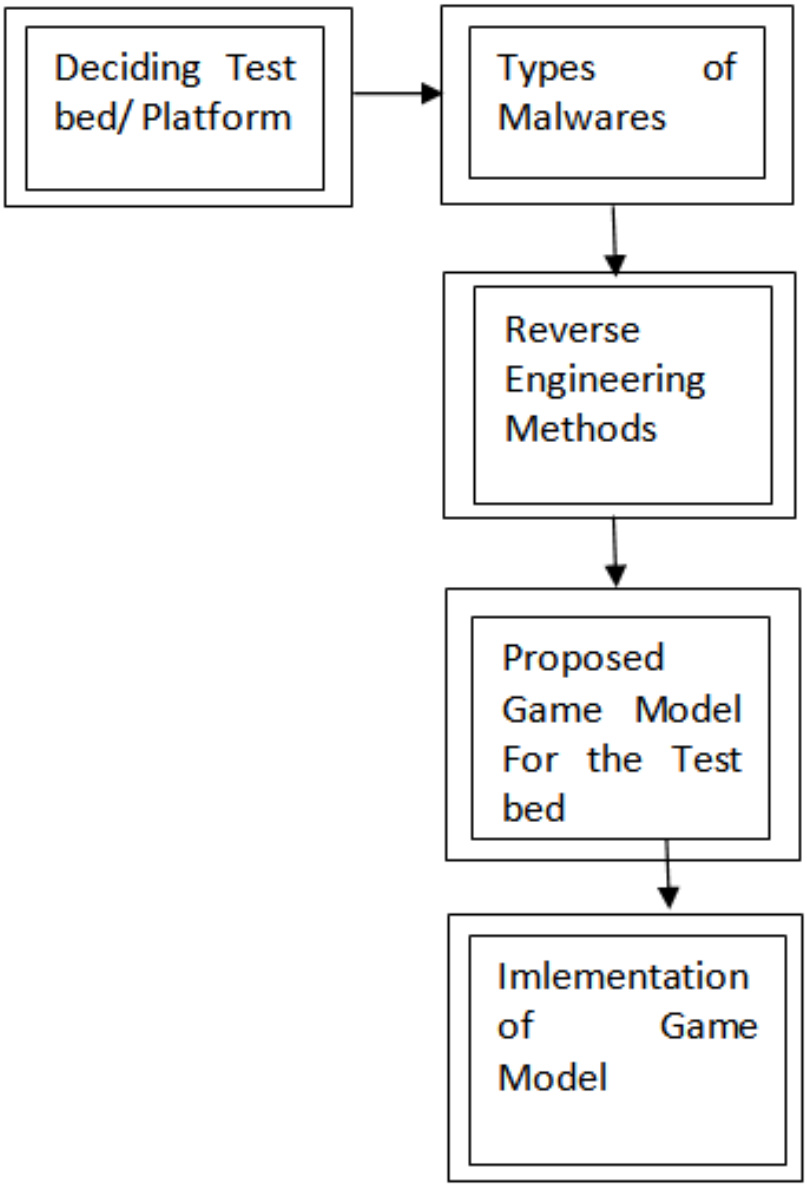

Figure 3.1: Cyber War Games Taxonomy

a suitable test bed for our game is one of the critical tasks in developing cyber games.These days more and more versatile malwares are quickly evolving and so the attacking techniques also vary. Therefore it is important to choose the complexity level of game by deciding the types of malwares: [ostrenga]. As malwares are quickly evolving therefore the detection techniques and reverse engineering methods also vary. It is important to decide the method that we are going to use for detection of malware in our game depending on the types of malwares. All above in view,

the proposed methodolgy is presented with focus on types of malwares, detection techniques and limitation of platform. The game model can be implemented and tested on any testbed. The steps to develop war games for cyber attacks/ malwares are given below in Figure-2. The first and most important step of the proposed methodology is to choose the relevant and best platform/ test bed by critically analyzing them according to our needs. The requirements on the basis of which platform is chosen are highlighted in this chapter. Having a cyber test bed provides an edge to organizations to pay attention to filter DNS traffic and avoid data exfiltration attacks on their network. Test bed would help bringing those tools on one platform to be used to detect in order to mitigate data exfiltration and C and C traffic [23].

3.4.1 Malware Analysis

The platforms available for testing and experimentation deals in different areas. Some platforms can handle more than one domain but some are specifically build for dealing with only one domain. The advantage of dealing with one domain is obvious that the platform is more focused and is build with free of limitations in other areas. More details could be inserted in to the platform and it is build with each major and minor details. In chapter 2 we have discussed all the domains that are important for war games. The domains are the elements of war games. All the offensive and defensive techniques that are used in war game need to be addressed in our simulated war games. Similarly in our case we have pointed out the major weapon of a war game that is very common and advanced technique these days to win a cyber war. The enemy always wants to compromise its competitor network and systems to retrieve the critical data that could be used against the competitor. The most advanced method of compromising competitor network and equipments today is by sending a malware that can harm the competitor with logic and time bombs to the highest level of intrusion in which the critical data is stolen from the competitors machine and the attacker

takes hold of machine completely starting to operate it remotely and making it worthless for the competitor. But obviously other aspects of transporting the malware and detecting and analyzing the malware on competitors end are also important. It is necessary to run malware in safe environment to provide containment and isolation. The platform on which malware is run should be an isolated environment and its architecture should restrain the malwares to effect the platform itself. Another important factor is remote access instead of physical access: [6].

In our research we have chosen the best available test bed for dealing in malware domain. The reason why we are choosing malwares as an important factor in our war game is already described above.

3.4.2 Types of Malwares

When deciding for the test bed for malware analysis it is very important to decide what kind of malwares you are trying to analyze on the test bed and decide the complication level of cyber game. Once the malwares are decided game model will be build on the basis of complexity level of game. The complexity of game is dependent on the type of malwares we are going to use as a sample for our experimentation in a cyber game.

1. There are signature based malwares that are easily detected by antivirus because their signatures are known. These malwares are also easy to be detected by malware analysts. So, a game based approach be used to consider such kind of malwares [24].

2. Some malwares are known to vary signatures spontaneously but each time they are decrypted to resent a known signature that could be easily detected [10].

3. Metamorphic malwares are known to be dangerous because their signatures are not known. So, more advanced techniques be used for detecting and analyzing such types of malwares [25].

4. More advanced malwares include hardware based Trojans that are already inserted in the hard-

ware and could not be detected using common methods of malware analysis.

5. Zero day attacks may also be taken in to consideration but no technique yet has been identified to detect such types of malwares.

6. Today malwares are even more versatile and developed intelligently to detect virtual environment which is the most common and known method for malware analysts to run malware in a virtual environment and know all the mechanics of malware. But malwares today are designed in such a fashion that before executing they differentiate between a real and virtual environment. Such typesz1 of malwares could be bypassed also and their detection and analysis process is discussed in detail in [26].

If we study all the malwares and the methods used by attackers the common and advanced malwares today behave in such a way that they a command and control server and on execution they try to connect to that server to receive instruction from the master and behave according to the way.

There are number of malware types but the most common and advanced malwares today behave in such a way that they are bound to connect to a remote server to receive instructions form the master and behave accordingly.

3.5 Reverse Engineering Techniques

After having decided the type of malwares, it is very important to decide the reverse engineering technique used in the game. The malwares attacks are mostly used because of their capability of remote exploitation. The severity of attacks differs depending upon the damage they cause. To understand the functioning and mechanics of malwares the reverse engineering of malwares is done. The malware analysts use reverse engineering techniques to know the mechanics of malwares to measure the damage caused by the malware and detect them in future and take further

preventive measures. The owner and player must use the same reverse engineering technique in order to match results. Different techniques may be used by the player for reverse engineering but it may cause to vary the results and in the end the player might not earn the points. Generally there are two methods for reverse engineering, static analysis and dynamic analysis. In static analysis the analyst seems to be more interested in code of the malware to know the mechanics of malware. But in dynamic analysis the analyst wants to run the malware in order to see the behaviour of malware that will help him identify the nature of malware and it will also cause the malware to fully function and connect to its command and control server to receive instructions. In our technique we are exactly using the same technique of revere engineering by running the malware in a fully controlled environment. Cyber war games are helpful in understanding the malware scripts as well. The reverse engineering tools are integrated in the game to detect and analyze malwares to provide awareness on reverse engineering methods. This helps analysts to perform self assessment and enhance their skills. Even scenarios can be made where one team will attack with malwares and the other team has to detect and analyze the malwares.

3.6 Scenerio Management

Scenarios are basically closely related real world situations. To develop a cyber game on test bed, test bed needs to have capability for dealing with multiple scenarios. This will help us to develop playable scenarios that a student can run in a lab environment. Different scenarios will provide the student more exposure about the real cyber war. As we are focusing on malware analysis so, in a scenario where player will confront more advanced malwares they will be driven by the will to analyze the malware and know the mechanics of malwares. As we are approaching and developing a game that can handle more risky malwares there will be more probability in future that we get skilled malware analysts and produce better results in a real cyber war. It is also done

so that custom scenarios and sets of scenarios could be developed to facilitate teaching specific concepts.

Scenario management will help on demand creation of experimental scenarios for representation of real world attacks. The management engine has the capability to deal with multiple scenarios simultaneously. Unlike other techniques, test bed doesnt start from scratch each time a new scenario is being created [27].

3.7 Key Features of Test Bench

It is demonstrated in [28] and [3] that test bed provides different sort of gaming environment for building cyber war games. Using test bed reduces the amount of work done in building a war game. Depending upon the scenario the test bed is designed to be open, part of internet and isolated. The test bed has following characteristics. The auto management capability of cyber test beds proves their usability for war games. They are capable of defining network topology on the fly through a set of network management tools and later make changes according to the user demand. This is the reason why more and more complex networks can be build within no time for experimentation. The resources of experiments are shared according to the need and desire. Experiments not utilizing resources at any time dedicate resource to another experiment for better utilization and work load. Different scenarios and experiments demands versatility of operating systems. So, test bed has a repository of OS images that are to be used for quickly loading them on remote nodes and we may alter them later. The software/ packages repository helps in quick installation of softwares needed instead of going through a cumbersome process of searching and gathering them from internet. The remote node and virtualization concept has helped the community to research in this area inspite of limited resources. Due to availability of cyber test beds we do not need a plenty of physical resources, instead we use remote nodes that are already

configured for us to use them. For experiments it is difficult to create a much traffic equivalent to the internet for the experiments. So, the concept of dummy traffic has helped a lot in the recent past where experimenters create a dummy traffic for testing purpose. The laboratory is build to be used from anywhere. So physical access is not necessary and researchers could use resources by sitting remotely. The virtualization on a standalone system is itself a cumbersome and time consuming process but it has been made easy in testbeds by auto management of virtualization. The remote node communication is not done simply; rather it is being done securely using SSH communication to avoid any security lapse. Multiple network configuration features of test beds provides an ease to test the configurations of a network on the fly and provides the flexibility to test experiment for different topologies of network for the attack and defense scenarios in a systematic way.

3.8 Conclusion

This chapter focuses on development of cyber war games.We propose the way to radically increase the usefulness and scope of testbed based cyber war games. The main agenda of this chapter is to discuss various resources needed to build a war game. Later thechapter proceeds with development of a prototype for building war games from malware detection perspective.

Chapter 4

A GAME MODEL FOR CYBER ATTACKS

4.1 Introduction

This chapter collectively offers the study of testbed and building game models. The major element in the simulation is the modelling of war games from malware detection perspective that result either in the successful analysis of malwares or compromising the assets by not knowing the mechanic of malwares.

4.2 The Overview of Cyber War Game Model

The concept of war games started in the field of information and communication technology with rise of cyber attacks. We need to understand the phenomenon of cyber attacks to evolve new techniques of detection and prevention. The cyber attackers think of new advanced ways to deteriorate the enemy. The war games provide a channel to understand the anatomy of cyber attacks. The war games are capable of dealing with the simplest virus attack to the most sophisticated malware advanced persistent threat (APT) attack. After exploring existing war games and their techniques, limitation and flaws, this paper attempts to merge the cyber attacks in a war game by presenting a unique game model for cyber attacks and discussing the implementation and practical limitations of a model. This paper proposes a prototype model for developing war games for cyber attacks simulation. The practical implementation and complexities of the model has been discussed in detail in this paper. Due to the recent cyber attacks, cyber warfare has become a very

hot topic. The incidents of cyber attacks in Estonia in May 2007, the most famous APT attack stuxnet on Irans nuclear plant at Natanz in 2009 and the recent DDOS attacks defacing the Israeli websites have been under debate for a long time. The concept of cyber war games is not new but using war games for malware attacks is a novel technique for understanding the mechanics/ anatomy of malwares. The malware attacks in a cyber war are considered to be the most alarming threat today, because every time the victim is attacked with a highly sophisticated malware that is unique in its behaviour and technique making it difficult for the defending party to detect and prevent the attack. The war game developed for malware attacks provides a continuous learning channel to prepare for the future attacks. Therefore, we need a comprehensive game model for cyber attacks. The existing war games, techniques, malware attacks, reverse engineering techniques, role of malwares in war games, everything to the best of knowledge has to be considered in building such a game model. All the existing war games we have studied so far are unique from the perspective for which they have been designed [4].

The cyber war game model helps to understand the importance of war games in the modern day world and the ongoing problems with the malwares. It simulates a large number of attacks to see the behaviour of advanced malwares and will definitely be helpful for cyber attack analysts to analyze the trends of latest malware attackers. The game model helps us to understand the architechture and function of a game. So, the first and most important step in creating game of any sort is to build a model that fulfils all the needs and is able to provide the best possible outcomes needed using the desired resource. The game model consists of various elements. It is necessary to identify those elements before building a game model. The important element in developing a model is to identify the hardware resources needed. The hardware resources are the building block of a game model and it tells us the basic hardware requirements needed to build a specific game. After identifying he hardware resources and their use, the software requirements are to be

defined. The software include the tools, virtual machines, simulators and emulators. The scripting languages and different flavours of operating systems must also be identified. Another important element is the modules. It becomes comparatively an easier task to divide the model in to different modules. Each module has its own own functioning depending upon the input and output of the module. The modules are inter related and the relationship between modules is also established for the proper working of a game. The inter connectivity of modules is also an important element of the game.

4.2.1 The Elements of a Game Model

In this paper, we propose a unique malware detection game model by identifying the important elements of a war game with respect to malwares.

4.2.1.1 Hardware Requirement

The proposed model need some hardware resources but due to the invention of test bed technology the resources are reduced. Rather than utilizing the real hardware we prefer to use the advance technique of test beds that provide virtual resources that behaves almsot in a similar way to real environment with some limitations. With use of test beds the games are speedy and less costly. So, the basic hardware requirement for our game model are the physical machine for the administrator and the player.

4.2.1.2 Software Requirements

The software we need for our game are the Windows based operating system, Linux based operating system and Honeynet project. The emulation platform is the Deterlab to access remote machines and configure them for experimentation. The virtual machine technology is also used.

The tools for reverse engineering of malwares are also used for our game for the player/ analysts. The C sharp wpf application is used to build the interface of a game and provide an efficient user friendly environment.

4.2.1.3 Modules

The game is divided in to various modules. The integration of modules is done after each module is configured and tested. The module 1 of our game consists of Deter lab platform. All the configurations needed to run experiment on this platform is a part of module 1 which is discussed later in Section 5. The module 2 consists of configuration of each node whether it is a part of Deter platform or an external machine. The node configurations has also been described in Section 5. Finally the module 3 consists of an interactive interface for a game. All the three modules are run and tested separately after which the integration of modules is performed. The integration of modules is an important element done by the interconnectivity of modules.

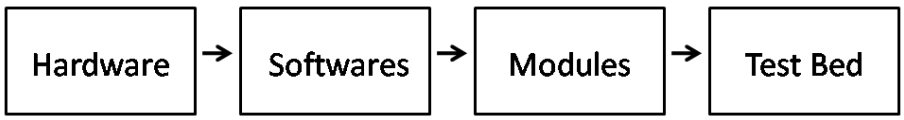

Figure 4.1: Game Model Blocks

4.2.2 Purpose of the Game Model

Then proposed model serves following goals.

2. To provide a real or seemingly real malware communication with external world.

3. Automated decisions without human intervention.

4. Incorporating malware detection techniques.

5. Automating remote learning.

6. Free of cost training.

7. Investigating latest trends of malwares.

8. Investigating the frequent malwares communication with the external world.

4.2.3 Features of a Game Model

1. Updation of game to incorporate new malwares.

2. Behavioural categorization of malwares.

3. Huge extendible database of malwares.

4. Game logs at each step of analyst and experimental history to be saved.

5. The internal network has virtual machines to run the malware in a safe environment. The real machines are used to run the advanced emulation resistant malwares [29].

6. Support of different operating systems.

4.3 MAIN ALGORITHM OF THE GAME

4.3.1 Overview

The game follows basic algorithm as described below and works according to the description. The game algorithm is build keep

4.3.2 Level 1

The player logins on the first node and the level 1 task given to the player is to detect which node in the internal network is infected. The first step to analyze malwares is to identify if the victim is infected or not. We often encounter problems in IT where we have to analyze the systems if they are infected or not or even we have to analyze the whole network being infected or not. So, we have considered level 1 of the game as follows:

4.3.2.1 Identifying the Victim Node:

In level 1 the identification of victim node is very important for the player to proceed to the next level. If the player is failed to identify the potentially infected node then he will not be able to conquer level 2 stage and further. On the admin side we already know which node is infected and the node that is infected is marked with some flag to be matched later. Once the player has finished its investigations on finding out the infected node he is going to mark every node as infected or not infected. By doing that the player answer is saved in a db which is matched with the db on the administrator side. If the data base files are all same then player has successfully passed the Level 1.

4.3.3 Level 2

Once the stage 1 is cleared. Player is given more access rights to the node. The player is granted more permission to the node marked infected and he can use the file sharing center of the testbed to install the tool from there on the node and get the level 2 continue. The level 2 has now a different challenge for the player. The player has to find out the type of malware that has infected the victim node. The malware could be a conventional virus, worm, spyware, Trojan, root kit etc. The definition of all these malwares are described in the help file of the game. After analyzing the

node for the type of malware with the best available tools the player will mark the answer with his own choice. It is to be mentioned here that the admin of the game has already done analysis of all the malwares present in the malware archive node. The analysis results are saved in a db file. The answer of the player is matched with the db file of the admin. If the malware type is matched player has successfully completed the level 2 also.

4.3.4 Level 3

We discussed earlier that we are going to have all the malwares that communicates to the outside network with their command and control servers. So, in this category of malwares it is very important to identify the location/ ip address of the command and control server to which the malware connects and received instructions to carry out further damage to the victim. The ip addresses are saved in a data base to be matched with the findings of the player. If the answer is matched then the player has successfully passed the initial test for malware analyst by playing a simple game.

4.3.5 Level 4

Finally the last level of game is about finding the signatures for malware. The signature of the malwares is something that an analyst has to identify for further preventive actions. In our case as we have a condition as well that the malwares that we are considering not only communicates outside the network but also makes some hidden file in the system. The hash of these files is signatures of the malware which are saved on the admin side in the database. If the player identifies the correct file and calculate hash of that file. The hash will be matched with saved hash in our data base. If it matches the player has successfully completed the last level of our game which is the most advanced level.Figure 3 shows the working of game.

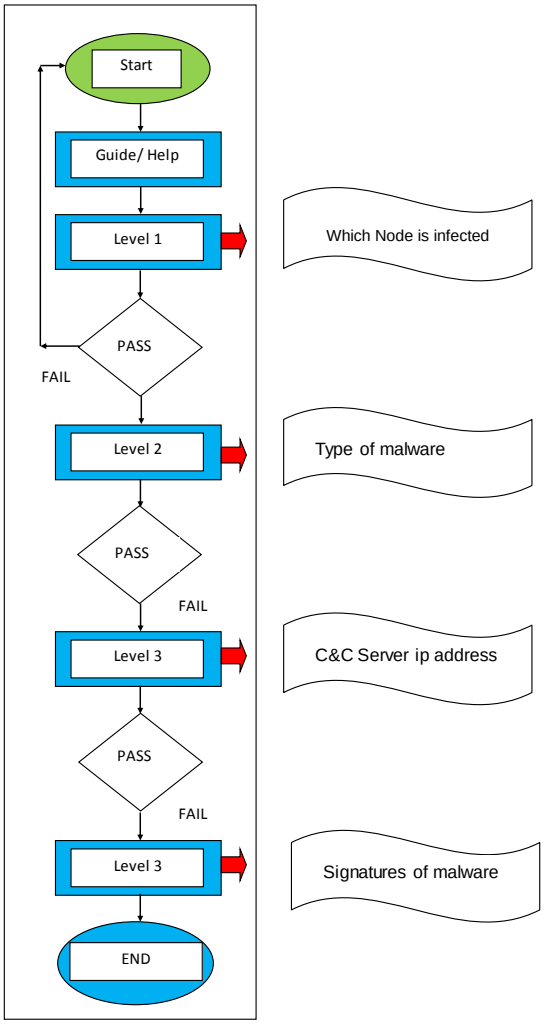

Figure 4.2: Game Algorithm

4.4 Implementation of a model

4.4.1 Initial Configurations

Initial configuration of our model follows that of [6]. However our model is of a game, whereas they have used it for malware containment. Initially in a game model the malware archive node is assigned and controlled by the operation staff of Deter lab. This node is a part of our experiment

and is accessible and controlled by the administrator of the game. A firewall is to be configured as a part of our network that blocks certain IPs and blocks the traffic from going out of the test bed. The functions of firewall are described as follows:

a. The firewall will continue its conventional functioning by blocking the traffic from going in an out of the test bed. But allowing the user to establish a secure session with testbed experiment.

b. We add an advance feature to firewall by making it to function more intelligently to accept the traffic, reject the traffic or redirect the traffic since it is gateway between in and out of the test bed. The firewall accept the traffic by forwarding it as it is in and out if the network if the traffic is found harmless. The firewall drops the packets that we are doubted to make the test bed malfunction and contaminated. The third case is to redirect the traffic using a smart impersonator feature in firewall. This impersonator with a honey net technology where we all the fake servers are configured. The web server is configured to acknowledge the malware with the expected reply it wants from the original server. In that case when malware will begin the http request instead of forwarding that request to the original server we are going to use our fake web server that will send the malware with a reply that malware expects to get from the original server. In this case there is a limitation that those malwares that can differentiate between the fake and original server will not behave accordingly and will die. So we are not able to analyze those malwares since we cannot forward them to the original server to avoid contaminating our test bed. Then we have a smtp server to deal with those malwares that communicate through emails. Further a ftp server is configured so that malware can proceed and upload the files stolen from the victim on the ftp server and we can analyze how malware behaves and what type of files it uploads on its server.

The second phase for our game model consists of insertion of malware in to one of the node in the internal network. The malware node will have a certain database of malwares and every time it will randomly pick one malware from the database and it will run pass that malware to one of the

nodes in the internal network. The transport procedure to the node could be manual or automated. The third phase for our game model is the execution phase. The preliminary analysis of malware is done by the admin of the game and the useful extracted information be saved in a db file in the malware archive node. Once the malware is loaded in to the victim node its analysis file is activated.

On the player/ user end when player starts the game, a guideline will appear for the player how to analyze malwares and also the tools that are used to analyze malwares. The player will read the manual before starting the game. Once the game is started. The player is given login rights to the inyernal network of the experiment. The player will login to every node and will examine all the nodes using his/her own to skills to find out the infected node. The player will be given access to the file sharing center in the test bed from where he can install tools.

4.4.2 Module 1 - Realization of Game in Deterlab

The internal network corresponds to the nodes and their connection built on Deterlab. In Deterlab it is the responsibility of a user to determine the number of nodes that will be used for experiment and also the connection of node with each other is necessary to specify to define topology of a network. The internal network is going to have both virtual machines and real bare metal machines activated. The purpose of having both the type of machines will be described later. The advantage of having internal network on Deterlab is that it is accessible online and we do not need any extra hardware for large experiments but we are just using the remote machines that are provided by the laboratory. It is also easy to add or remove any node from the experiment. Since we are dealing with malware experimentation it is very important to define a safe and secure network design for our game so that malware does not affect the test bed itself. The use of remote technology is also important. The player does not need to be present physically on the situation

but he/she can access game online by just providing credentials of the user. The in house network could be as large as possible keeping in mind the limitations of bandwidth. The internal network is easily modifiable and the software on nodes and operating system can be changed within no time by just providing an image of the OS. The possibility that is any machine is infected it could be separated from the network within no time. Also the use of virtual switches and routers makes it easy to make a network of any type. We can virtualize everything when we are using this platform we do not need to worry about extra hardware and cost.

Each registered user can access its own configured experimental nodes using SSH. A programmable backplane of Ethernet provides network connection to the experimental nodes. Each node is connected to the switch through VLANS, which are used to create desired network topology for the respective experiments. Besides, each node has at least a 100Mbs port for downloading various software and controlling the experiment. No node has any connection with external internet. For guidance, full documentation including DETER lab usage policy and many tutorials on setting DETER lab nodes and NS files has been provided to its users.

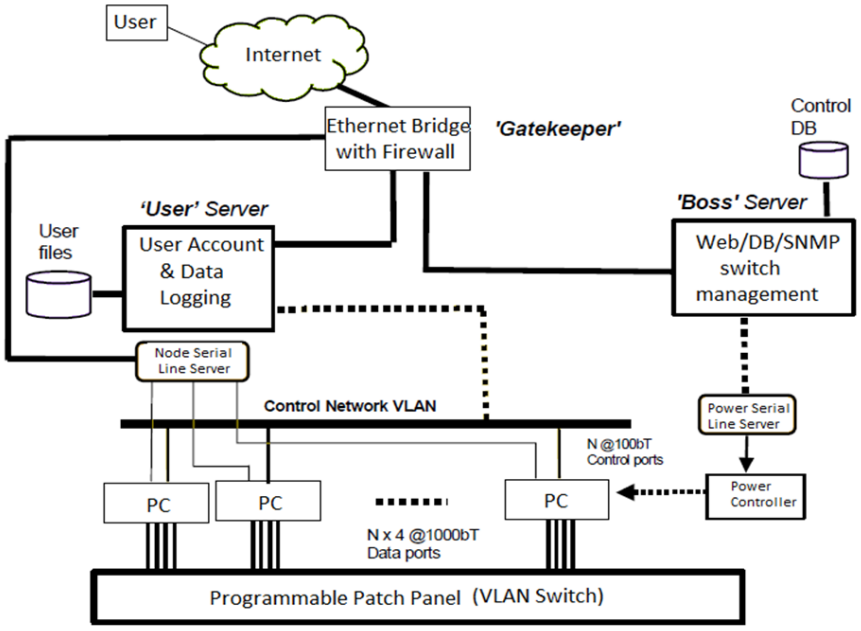

Figure 4.3: Deter Architechturel

4.4.3 Module 2 - Nodes Functioning

The nodes 1 to 5 define the internal network of a game. Windows Xp/ 7 is installed on all the systems in the internal network/ LAN.

4.4.4 Monitoring Node

There is a monitoring node which is also the gateway of the internal network. The gateway is a Linux based system. All the traffic of the network is redirected to the internal gateway which consists of firewall as well to filter the traffic. The wire shark is used at monitoring node to monitor the IPs in and out of the network. The burp suite proxy is also used either to allow the traffic, deny or redirect the traffic to the internal servers. Another famous tool inetsim is used to record further parameters of network traffic and to create the DNS, smtp, ftp servers to trick the attacker.

Machines	Operating Systems
Node A	Windows XP
Node B	Windows XP
Node C	Windows XP
Node D	Windows XP
Malware Archive Node	Windows XP
Monitoring Node	Honey Net
Switch	Cisco Catalyst2960 Switch (48) 10/100 Ethernet Ports (90)

This node also contains the data base of anlayzed malwares to match the player entries with the admin results. Ever time the malware is added to the malware archive node the analysis of malware is done and save din the data base in monitoring node. The data base records the nodes infected in a network. It also records the type of malware, ip addresses and hash of the malware. It is necessary to update this list in order to match the results of a player.

4.4.5 Malware Archive Node

The malware archive node has the updated list of similar malwares to analyze.

4.4.6 Module 3 - Game Interface

An interactive interface has been built for our game using C sharp wpf application shown in Fig 7.

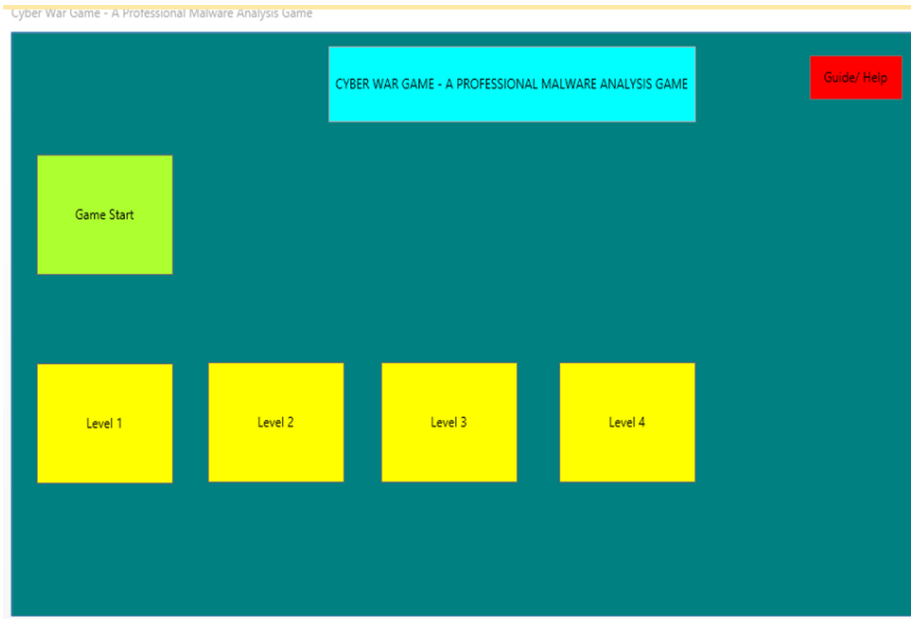

Figure 4.4: Game Interface

4.5 Modes of a Game

Our game consists of three modes:

4.5.1 Basic Mode

If the player starts the game in basic mode the player is guided how to investigate the malware attack. The tool is provided to the player to for each level of a game.

4.5.2 Intermediate Mode

In intermediate mode the player is given the permission to use the set of tools without guiding the player with the tools. The player can initiate request to download its own tools to investigate the attack. The permission is given to the player to download the tools on the gateway server of test bed and access it from the internal network.

4.5.3 Expert Mode

In expert mode the player is allowed to use minimum set of tools and the player has to use manual expertise to investigate the malware attack.

4.6 Criteria for Passing the Level

The level 1 is about the detection of victim. We have the authority of infecting more than one system in our in house network. So, when initially the player logins to each node to detect the infected node it could be more than one. In case the player is not being able to detect at least one victim node he/she is not allowed to proceed to next level. This is the criteria for our game level 1. On second level the player has to identify the type of malware the node is infected with. There may be a case where different malwares are processed at one time on different nodes. So, he has

to detect the type of malware for all the victim nodes and the types may also differ depending which malware has infected which node. This is multi dimensional aspect in our game. So, we can process more than one malwares at a time on more than one node. When player identifies a true victim node then he is given more permissions/ rights to access the softwares on the test bed network to install on the node for further analysis. Finally the player identifies the signatures of malware to be added to match with our own signature data base.

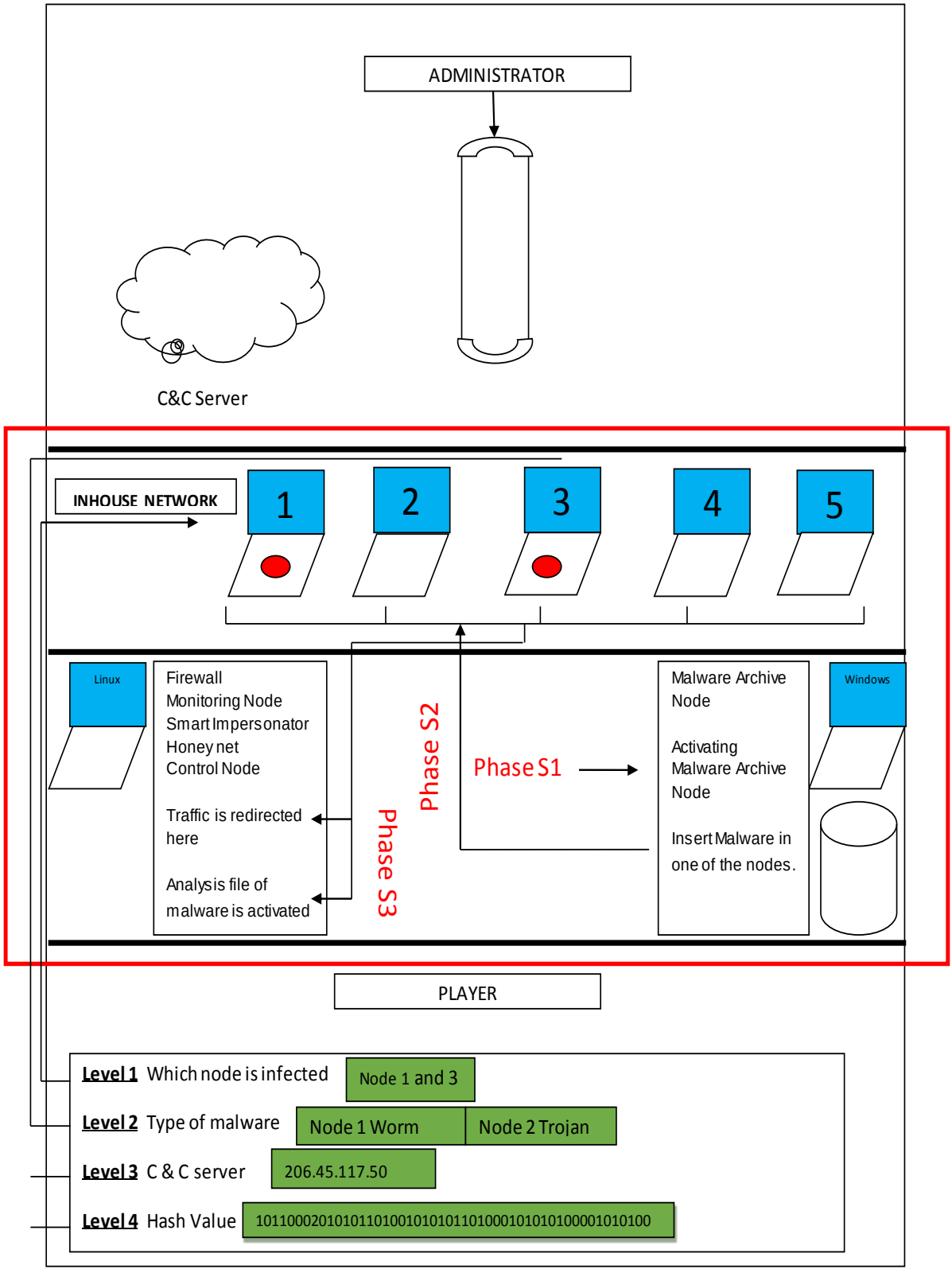

Figure 4.5: Game Model

Chapter 5

EXPERIMENTATION RESULTS

5.1 Experimentation Results

5.1.1 Module 1

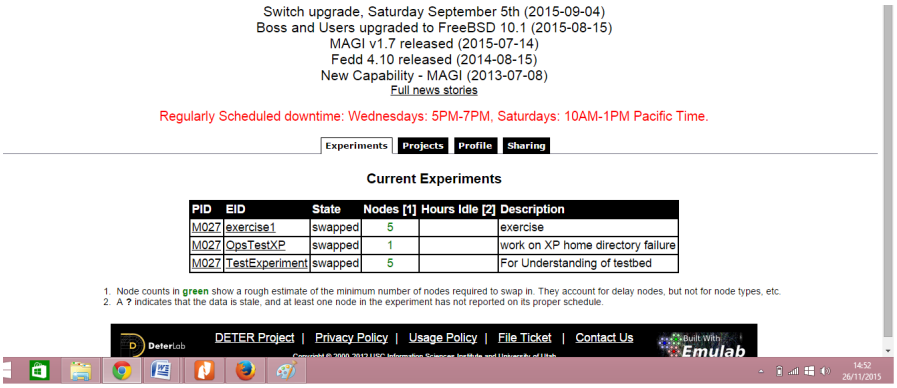

Figure 5.1: Test Bed

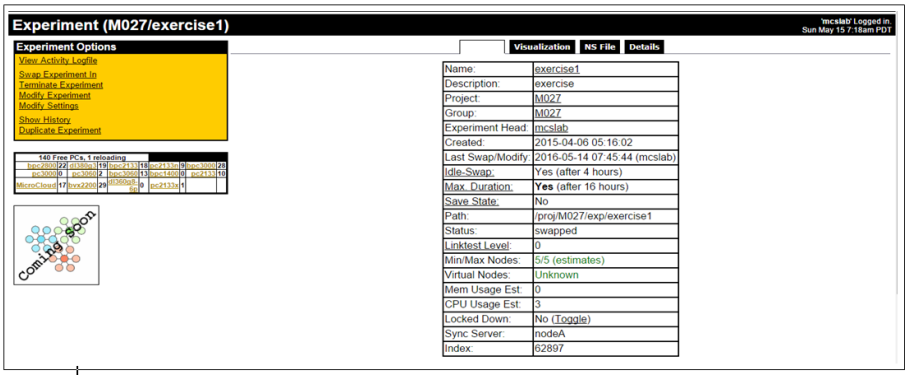

Figure 5.2: Experiment Details

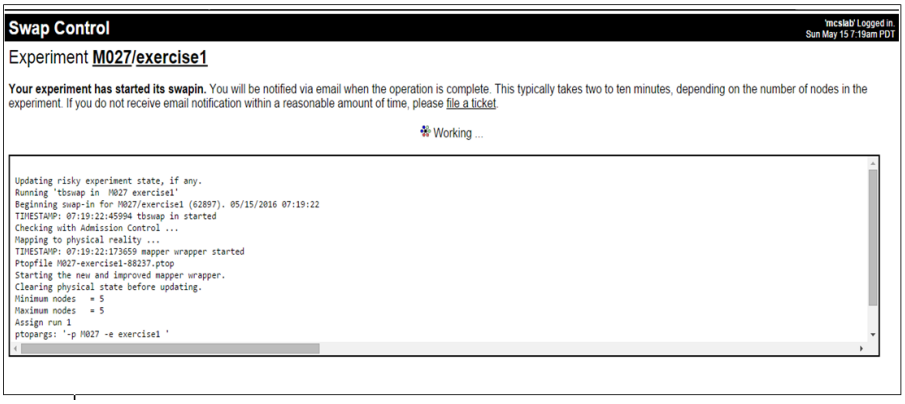

Figure 5.3: Swapin

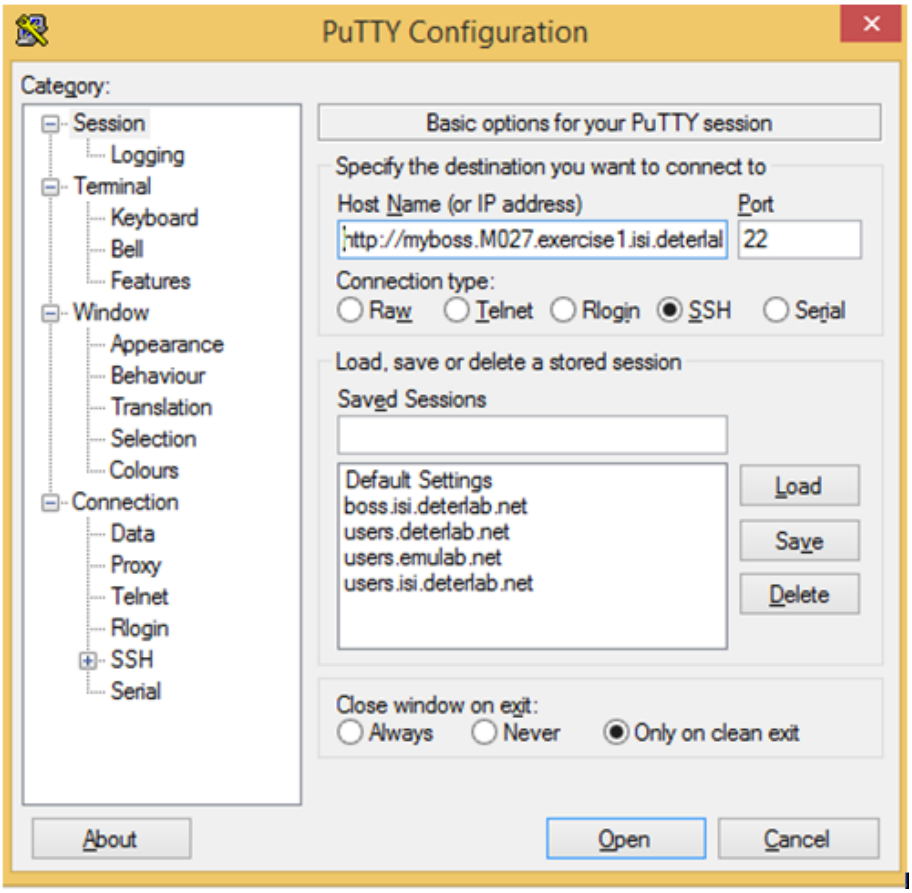

Figure 5.4: Putty

5.1.2 Module 3

The results for the experimental game model are presented in this chapter. We executed the malware on the internal network as described in the previous chapter to show the propoer functioning of the game. Initially the game interface looks like as shown in Fig 8.

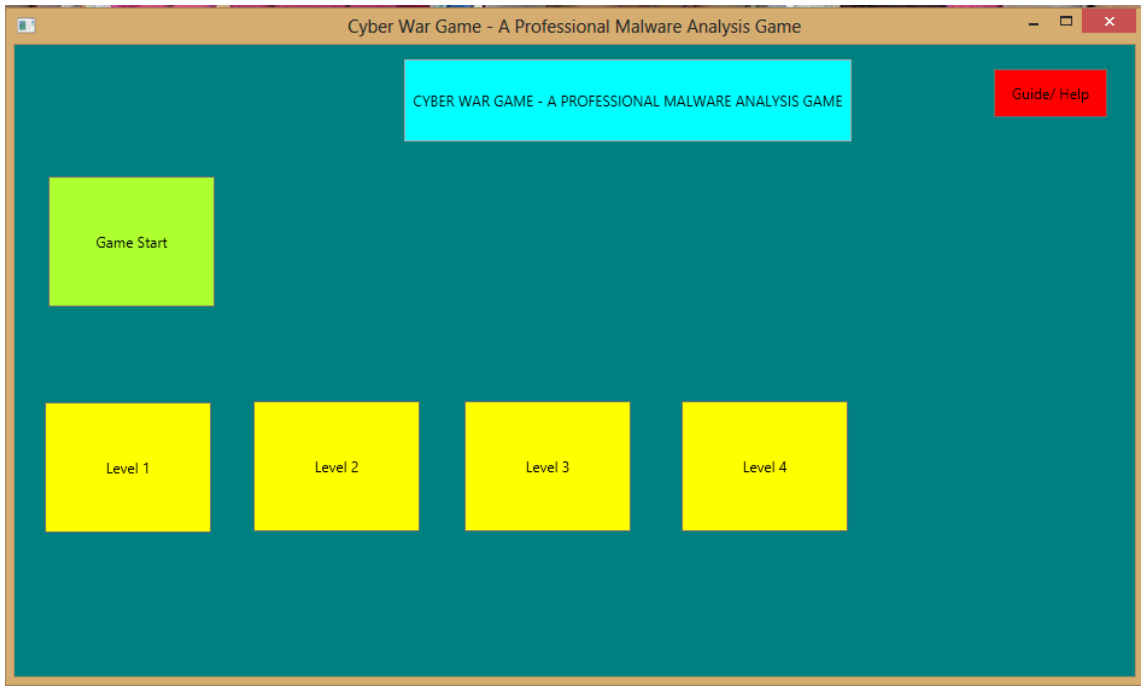

Figure 5.5: Game Interface

According to the game model the node which is marked as malware archive node is activated and the malware from the database is loaded in to one of the nodes in the internal network. As soon as the player press the button game start the malware is connected to the platform and malware is loaded in to the network.

The player proceeds to the Level 1 and is given access to all the nodes in the internal network.

The player examines all the nodes by logging in to the each system. I this case Node 2 is infected and the player finds Node 2 infected through vaiours mehtods like checking the processes and

Figure 5.6: Game Start

Figure 5.7: Level 1

services running at the start of the system and some hidden/ temp files that are created upon the execution of malware. As soon as the player successfully pass the Level 1, it proceeds to the Level 2.

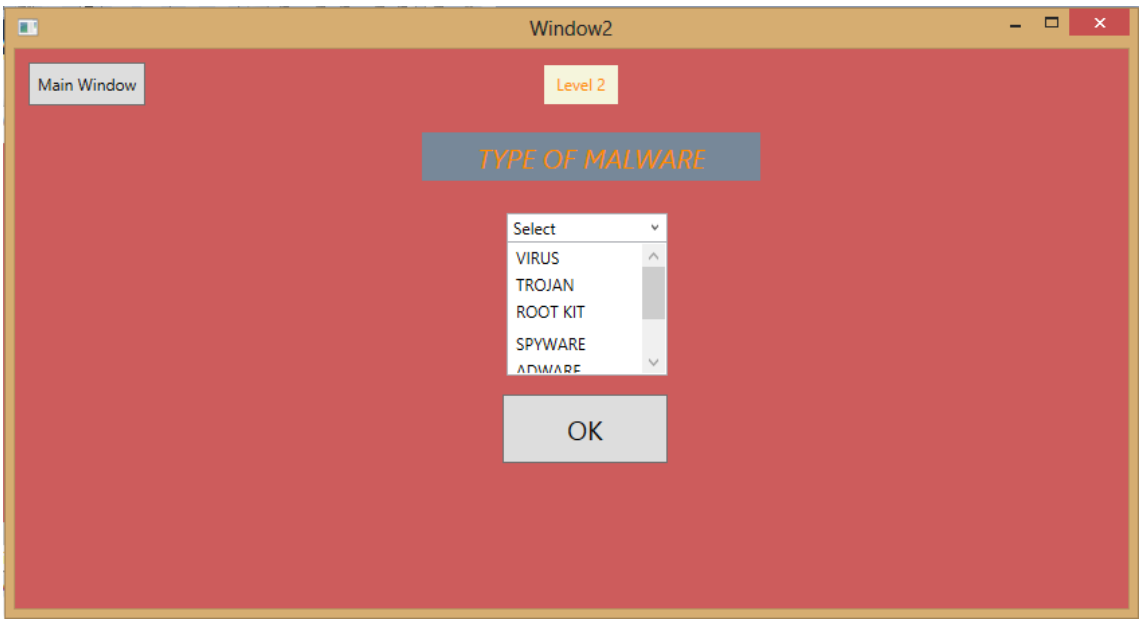

Figure 5.8: Level 2

The player further investigates to check the behaviour of malware tht is found to be Trojan. Next, the Level 3 details are as under.

Figure 5.9: Level 3

The C and C server ip address is checked through the wireshark by the player. The Level 4 details

are:

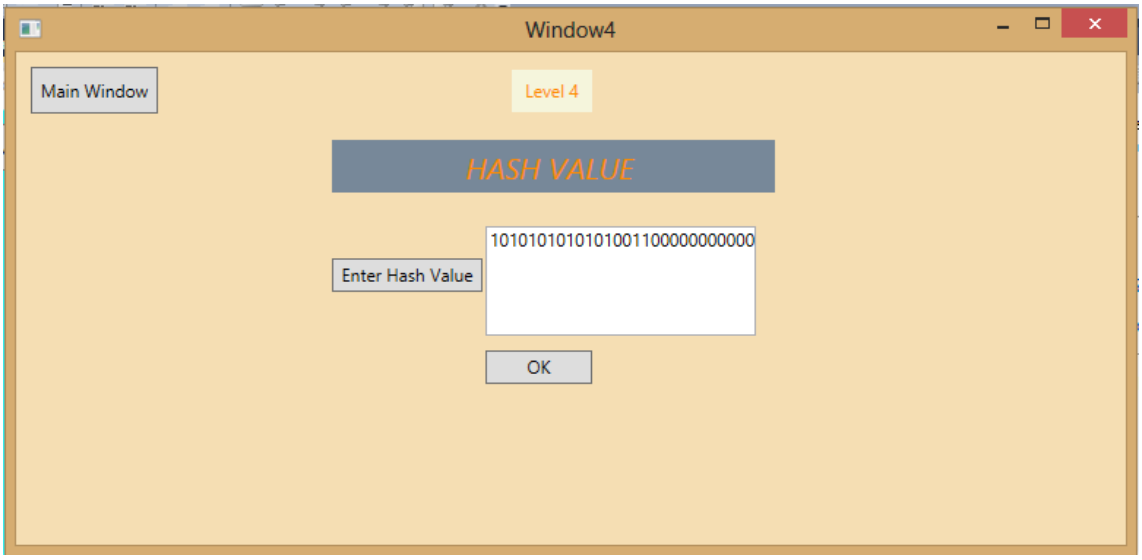

Figure 5.10: Level 4

AT the end the hash value of the hidden file/ temp file created by the malware is being entered by the player to match with the admin answer. The player has found that correct and successfully completed all the levels in basic mode.

Chapter 6

CONCLUSION

6.1 Conclusion

This thesis serves as a foundation for the upcoming war games in malwares perspective. The study of war games itself is a broad domain and so is the study of malwares. This thesis put efforts to merge the field of war games and malware detection by using war games to train in malware detection. The study of test beds opens news ways to develop war games and minimize the resources by utilizing the test bed laboratories. We need to understand the phenomenon of cyber attacks to evolve new techniques of detection and prevention. The cyber attacker think of new advanced ways to deteriorate the enemy. After exploring existing war games and their techniques, limitations and flaws, this thesis attempts to merge the cyber attacks in a war game by presenting a unique game model for malware detection. The war games provide a channel to understand the anatomy of attacks.

6.2 Future Work

The war games is an important weapon for future cyber war drills. The cyber war drills are openly available for academia and research communities. It is evident that war games provide a good way for students hands on learning and problem solving skills for malware reverse engineering.
However much more work is needed in this area to incorporate latest techniques of cyber attacks in a war game. The games will help academia, research and IT industry to grow in a better way in

a competitive environment. In future we propose the work to be done in integrating all the three modules and more and more games can be developed using this war game model as a prototype to make advancements in the field of war games and malwares. The malwares of different types could be dealt in future in war games. The more advanced techniques of reverse engineering and malware detection be integrated with the war game to enhance the difficulty level of the game and to update with the technology and methods of malware detection. Then game interface could be improved and the game model itself with further refinements can be used for the campus to serve the purpose of training.

BIBLIOGRAPHY

[1] A. Alwabel, H. Shi, G. Bartlett, and J. Mirkovic, "Safe and Automated Live Malware Experimentation on Public Testbeds," In *Proceedings of the 7th USENIX Conference on Cyber Security Experimentation and Test*, CSET'14 pp. 2–2 (USENIX Association, Berkeley, CA, USA, 2014).

[2] K. King, D. Manz, P. Ortman, D. Shikashio, and P. Oman, "A Rapidly Reconfigurable Computer Lab for Software Engineering Security Experiments and Exercises," In *Software Engineering Education and Training Workshops, 2006. CSEETW '06. 19th Conference on*, pp. 24–24 (2006).

[3] A. Conklin, "The use of a collegiate cyber defense competition in information security education," In *Proceedings of the 2nd annual conference on Information security curriculum development*, pp. 16–18 (2005).

[4] J. Mirkovic and P. A. H. Peterson, "Class Capture-the-Flag Exercises," In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, (USENIX Association, San Diego, CA, 2014).

[5] N. Idika and A. P. Mathur, "A survey of malware detection techniques," Purdue University 48 (2007).

[6] R. Ostrenga, S. Schwab, and R. Braden, "A Plan for Malware Containment in the DETER Testbed," In *Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007*, DETER pp. 10–10 (USENIX Association, Berkeley, CA, USA, 2007).

[7] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds," Technical report, DTIC Document (2013) .

[8] J. S. Park, J.-S. Lee, H. K. Kim, J.-R. Jeong, D.-B. Yeom, and S.-D. Chi, in *Information and Communications Security: Third International Conference, ICICS 2001 Xian, China, November 13–16, 2001 Proceedings*, S. Qing, T. Okamoto, and J. Zhou, eds., (Springer Berlin Heidelberg, Berlin, Heidelberg, 2001), Chap. SECUSIM: A Tool for the Cyber-Attack Simulation, pp. 471–475.

[9] M. F. Thompson and C. E. Irvine, "CyberCIEGE Scenario Design and Implementation," In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, (USENIX Association, San Diego, CA, 2014).

[10] C. Cowan, "Defcon capture the flag: Defending vulnerable code from intense attack," In *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, **2,** 71–72 (2003).

[11] B.-T. Chu, G.-J. Ahn, S. Blanchard, J. Deese, R. Kelly, H. Yu, and A. Young, "Collegiate Cyber Game Design Criteria and Participation," In *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on*, pp. 1036–1041 (2007).

[12] D. Kushner, "The real story of stuxnet," Spectrum, IEEE **50,** 48–53 (2013).

[13] E. Alomari, S. Manickam, B. Gupta, P. Singh, and M. Anbar, "Design, Deployment and use of HTTP-based Botnet (HBB) Testbed," In *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, pp. 1265–1269 (2014).

[14] H. Shi, A. Alwabel, and J. Mirkovic, "Cardinal pill testing of system virtual machines," In *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 271–285 (2014).

[15] C. Siaterlis, A. P. Garcia, and B. Genge, "On the use of Emulab testbeds for scientifically rigorous experiments," Communications Surveys & Tutorials, IEEE **15,** 929–942 (2013).

[16] J. Mirkovic, T. Benzel, T. Faber, R. Braden, J. Wroclawski, and S. Schwab, "The DETER project: Advancing the science of cyber security experimentation and test," In *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, pp. 1–7 (2010).

[17] K. E. Heckman, M. J. Walsh, F. J. Stech, T. A. O'boyle, S. R. DiCato, and A. F. Herber, "Active cyber defense with denial and deception: a cyber-wargame experiment," Computers & Security **37,** 72–77 (2013).

[18] T. Benzel, "The Science of Cyber Security Experimentation: The DETER Project," In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11 pp. 137–148 (ACM, New York, NY, USA, 2011).

[19] D. P. Masterson, "Creating reusable virtual machines to simulate networks for cyber challenges," (2014).

[20] T. Bailey, J. Kaplan, and A. Weinberg, "Playing war games to prepare for a cyberattack," McKinsey Quarterly pp. 1–6 (2012).

[21] K. Kosina, *Wargames in the fifth domain* (Diplomatische Akademie, 2012).

[22] L. Spitzner, "The honeynet project: Trapping the hackers," IEEE Security & Privacy pp. 15–23 (2003).

[23] I. Kotenko, "Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet," In *19th European Simulation Multiconference Simulation in wider Europe*, (2005).

[24] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*, pp. 256–262 (2012).

[25] D. Gritzalis and S. Papageorgiou, "PANOPTES: The Greek National Cyber Defence Exercise," (2016).

[26] D. Masterson, "CREATING REUSABLE VIRTUAL MACHINES TO SIMULATE NETWORKS FOR CYBER CHALLENGES," (2014).

[27] M. F. Thompson and C. E. Irvine, "CyberCIEGE Scenario Design and Implementation," In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, (2014).

[28] D. Watson and J. Riden, "The honeynet project: Data collection tools, infrastructure, archives and analysis," In *WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, pp. 24–30 (2008).

[29] M. G. Kang, H. Yin, S. Hanna, S. McCamant, and D. Song, "Emulating emulation-resistant malware," In *Proceedings of the 1st ACM workshop on Virtual machine security*, pp. 11–22 (2009).