



**BUILDING CYBER OPERATION
SCENARIOS FOR
CYBERWARFARE SIMULATIONS**

KEMAL YILDIRIM

YAŞAR UNIVERSITY

2016



YAŞAR UNIVERSITY
FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING
MASTER THESIS

**BUILDING CYBER OPERATION
SCENARIOS FOR
CYBERWARFARE SIMULATIONS**

KEMAL YILDIRIM
THESIS ADVISOR: ASSOC. PROF. KOLTUKSUZ, A., PH.D.

CYBER SECURITY PROGRAM

PRESENTATION DATE: 25.11.2016

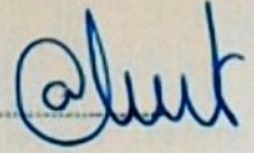
We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Jury Members:

Signature:

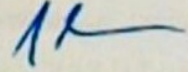
Assoc. Prof. Ahmet KOLTUKSUZ, Ph. D.

Yaşar University



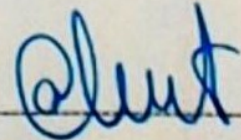
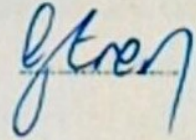
Asst.Prof. Tuğkan TUĞLULAR, Ph. D.

Izmir Institute of Technology



Asst.Prof. Ahmet Tuncay ERCAN, Ph. D.

Yaşar University



Assoc. Prof. Ahmet KOLTUKSUZ, Ph. D.
Head, Department of Computer Engineering

ABSTRACT

BUILDING CYBER OPERATION SCENARIOS FOR CYBERWARFARE SIMULATIONS

YILDIRIM, Kemal

MSc in Computer Engineering, Cyber Security

Supervisor: Assoc. Prof. Ahmet H. Koltuksuz

November 2016

This thesis describes cyberspace as a new domain and cyber operation environment. Try to develop its principles, compare with kinetic warfare and propose new principles. After describing cyber related terms, examines existing cyber security simulations and describes our simulation project, developed in Yaşar University, Information Warfare Simulator (IWSIM), and examines the structure and the building of cyber operation scenarios and their use in simulations and analysis them. In this way, the study is about how to make the cyber operation scenario database model efficiently for future designsto achieve a real working simulation. This thesis consists of 6 chapters which covering above topics.

Key Words: Cyber space, Cyberwarfare, Simulation, Cyber Security, Cyber Defense, Cyber Scenarios, Cyberwarfare principles, IWSIM, Information Warfare, Cyber Simulator, Network Attacks, Cyber Operations

ÖZET

SİBER SAVAŞ BENZETİMLERİNDE KULLANIM İÇİN SİBER HAREKÂT SENARYOLARININ OLUŞTURULMASI

Kemal YILDIRIM

Yüksek Lisans Tezi, Bilgisayar Mühendisliği Bölümü Siber Güvenlik
Bilimdalı

Tez Danışmanı: Doç. Dr. Ahmet KOLTUKSUZ

Kasım 2016

Bu tez, yeni bir etki alanı olarak siber uzayı ve siber harekât ortamı tanımlayarak siber hareket prensiplerini oluşturmak için klasik savaflara göre karşılaştırmasını yapar ve yeni prensipler teklif eder. Siber ile ilgili terimlerin tanımından sonra, var olan siber güvenlik simülatörlerini inceleyerek Yaşar Üniversitesinde geliştirdiğimiz IWSIM'i anlatır, IWSIM'in yapısını inceleyerek bu kapsamda siber hareket senaryolarının veri tabanı modelini ortaya koyar. Bu sayede gelecekte yapılacak benzer simülasyon çalışmalarında daha gerçekçi çalışan bir ortama ulaşmak için etkin bir siber hareket senaryo veri tabanı modellemesini ve nasıl olması gerektiğini araştırır. Bu tez yukarıda bahsedilen konuları kapsayan 6 bölümden oluşmuştur.

Anahtar kelimeler: siber hareket, siber savaş, siber uzay, siber savaş prensipleri, simülasyon senaryo modeli, IWSIM, siber güvenlik, siber savunma, bilgi harbi, ağ saldırıları.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Ahmet KOLTUKSUZ for his guidance and patience during this study.

I would like to express my enduring love to my family, who are always supportive, loving and caring to me in every possible way in my life.

I would like to thank, in addition, to Çağatay YÜCEL, Hüseyin YAĞCI, Bahar TİMAÇ, and Tuğçe KALKAVAN for their help on my thesis study and cooperation in IWSIM Project.

Kemal YILDIRIM

İzmir, 2016

TEXT OF OATH

I declare and honestly confirm that my study, titled “Building Cyber Operation Scenarios for Cyberwarfare Simulations” and presented as a Master’s/PhD Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.

Kemal YILDIRIM

.....
25 November 2016

TABLE OF CONTENTS

	Page
<u>ABSTRACT</u>	v
<u>ÖZET</u>	vii
<u>ACKNOWLEDGEMENTS</u>	ix
<u>TEXT OF OATH</u>	xi
<u>TABLE OF CONTENTS</u>	xiii
<u>INDEX OF FIGURES</u>	xv
<u>INDEX OF TABLES</u>	xvii
<u>CHAPTER ONE INTRODUCTION</u>	1
<u>1.1 Subject and Context of the Thesis</u>	1
<u>1.2 Problem Definition and Aims</u>	2
<u>CHAPTER TWOLITERATURE REVIEW AND PREVIOUS RESEARCH</u> ..	3
<u>2.1 Definition of CW/CO and Its Principles</u>	3
<u>2.2 Modeling of Cyberspace and Building CO Scenario Subjects</u>	6
<u>CHAPTER THREEDESCRIPTION OF THE CYBER TERMS</u>	10
<u>3.1 Cyberspace</u>	10
<u>3.2 Cyberwarfare (CW)</u>	11
<u>3.3 Cyberspace Operations (CO)</u>	12
<u>3.4 Principles of War and Cyberwarfare</u>	15
<u>3.5 Cyberspace Specific Principles</u>	17
<u>CHAPTER FOURDESCRIPTION OF CYBER SECURITY SIMULATIONS</u>	
21	
<u>4.1 Description of Cyber Security Simulations</u>	21
<u>4.2 Existing Cyber Security Simulations</u>	22
<u>4.2.1 CyberLympics</u>	22
<u>4.2.2 CyberPatriot</u>	22
<u>4.2.3 Defcon CTF</u>	23
<u>4.2.4 Siber Meydan</u>	23
<u>4.3 IWSIM</u>	23
<u>4.3.1 Environmental Settings</u>	24
<u>4.3.2 Main Modules of IWSIM</u>	26
<u>4.3.3 IWSIM Scenario Parameterization & Running</u>	29

<u>CHAPTER FIVE BUILDING CYBERWARFARE / OPERATION SCENARIOS</u>	34
<u>5.1 Properties of Cyberwarfare / Operation Scenarios Database</u>	34
<u>5.2 Modeling Cyberwarfare / Operation Scenario Database</u>	36
<u>5.3 Test Scenarios Employed in IWSIM</u>	44
<u>5.3.1 Estonian DDOS Attacks</u>	44
<u>5.3.2 Operation Aurora</u>	45
<u>5.3.3 Turkish Baku-Tbilisi-Ceyhan (BTC) Pipeline</u>	45
<u>CHAPTER SIX CONCLUSION</u>	46
<u>REFERENCES</u>	47
<u>CURRICULUM VITEA</u>	52
<u>APPENDIX 1 CO SCENARIO DB SCHEMA (ER) DIAGRAM</u>	53
<u>APPENDIX 1 CO SCENARIO DB SCHEMA (ER) DIAGRAM (cont.)</u>	54
<u>APPENDIX 2 CO SCENARIO DB SAMPLE VALUES</u>	55

INDEX OF FIGURES

Figure 1 Core Code Architecture of IWSIM.....	25
Figure 2 Sample of Red Team Screen.....	27
Figure 3 Sample of Yellow Team Screen.....	29
Figure 4 Example XML file defining the parameters of a Scenario.....	31
Figure 5 Sample of White Team Screen.....	32



INDEX OF TABLES

Table 1 Categorization of reviewed previous works.	9
Table 2 Scenario table.	37
Table 3 Scenario Types table.	38
Table 4 Scenario Actors table.	38
Table 5 Scenario Teams table.	39
Table 6 Scenario Constraints table.	40
Table 7 Scenario Objectives table.	41
Table 8 Nodes table.	41
Table 9 Network tables.	42
Table 10 Targets table.	43
Table 11 Intelligence table.	43

INDEX OF SYMBOLS AND ABBREVIATIONS

<u>Symbols</u>	<u>Explanations</u>
----------------	---------------------

C	Cycle Time (min)
---	------------------

Abbreviations

C2W	Command Control Warfare
-----	-------------------------

CW	Cyberwarfare
----	--------------

CO	Cyber Operation
----	-----------------

DCO	Defensive Cyber Operation
-----	---------------------------

DODIN	Department of Defense Information Networks
-------	--

IW	Information Warfare
----	---------------------

IWSIM	Information Warfare Simulator
-------	-------------------------------

GW	Generation Warfare
----	--------------------

LOIC	Low Orbit Ion Cannon
------	----------------------

OCO	Offensive Cyber Operation
-----	---------------------------

SDL	Simulation Definition Language
-----	--------------------------------

1 CHAPTER ONE

INTRODUCTION

We live in the 4th/5th generation warfare (4/5GW) era. 1G was the form of regular army, and then 2G was started with the faith of İstanbul with use of artillery in tactics, after WWI, use of heavy machine mechanized units, war planes and intelligence in war tactics was formed 3G warfare. Fourth generation warfare uses all available networks (political, economic, social, and military) to convince the enemy's political decision makers that their strategic goals are either unachievable or too costly for the perceived benefit [1]. 4/5GW is an evolved form of insurgency which primarily depends on technology and information so cyberspace is the master theater for this era. As the frequency of cyber-attacks rises exponentially, being ready for this kind of warfare depends more and more on one's experience in the field. On the other hand, regarding the time and bandwidth costs, implementing a real drill would be inefficient. Therefore, training requirements in this domain have created a certain need for a robust and realistic simulation environment that can be engendered by a certain group of software.

1.1 Subject and Context of the Thesis

The subject of thesis is to build cyber operation scenarios for cyberwarfare simulations. To achieve this goal, this thesis is comprised of six chapters. First, literature and previous related studies were researched and reviewed in chapter two. Secondly, to define the cyber space, Cyberwarfare, cyber operations and its principles, underline differences from those in kinetic warfare in chapter three. Chapter four gives a generic description of cyber security simulation. Existing simulations about this subject were searched and examined, then our implementation, Information Warfare Simulator (IWSIM) and its main components, design steps, and open source tools, which are used in our simulation, were determined and defined. Then, cyber operation scenarios principles were constructed from previously related studies and cyber operation scenario database were modeled and tested with three different

scenarios in chapter five. Finally, a conclusion and future works are formed in chapter six.

1.2 Problem Definition and Aims

The main problem is lack of any standard cyber operation scenario model due to the nature of this domain. Besides, this is a new type of warfare and yet doctrines and principles are not fully matured. The aim of this thesis is to build a model for using it in IWSIM as a prototype, to offer as useful model for future designs and to generate sample scenarios in its database. While performing it, make suggestions about how to build cyber operation scenarios and its principles.

2 CHAPTER TWO

LITERATURE REVIEW AND PREVIOUS RESEARCH

Definition of CW/CO and its principles, modeling of this domain and building scenario subjects are the basics of this chapter. In order to set up a model previous researches and find the related literature are the leverage for this thesis. For this reason, hundreds of papers, books, and article were scanned and most related 16 papers, books, and article were reviewed in two sections.

2.1 Definition of CW/CO and Its Principles

Firstly, the definition of CW/CO and its principles were scanned in order to drawing frame and determine the borders of the thesis. The most abundant papers have found in this part of review study because of this is the entry point of the subject.

2.1.1 Joint Publication 3-12 (R) Cyberspace Operations U.S. Department of Defense, 5 February 2013

This document [2] is the most matured and formal document about this subject. This doctrine is used for CO in the U.S. and scopes for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations. As it is a doctrine, it provides military guidance for U.S. Joint Force CO. It has four chapters. Firstly, define cyberspace in terms of three layers: physical network, logical network, and cyber-persona, integrating cyberspace operations with other types (land, maritime, air) of operations and conducted in the physical domains and the wide variety of legal issues that relate to CO and position of The Joint Force reason for cyberspace threats varies ranging from nation states to individual actors. Then second chapter guides for;

- **Military Operations in and Through Cyberspace;**

CO missions are categorized as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN based on their intent.

- **National Intelligence Operations in and Through Cyberspace;**

National level intelligence organizations, including major DOD agencies, conduct intelligence activities for national intelligence priorities. This intelligence can support a military commander's planning and preparation.

- **Department of Defense Ordinary Business Operations in and Through Cyberspace;**

Organizations support and sustain DOD functions, conduct routine uses of cyberspace, as well as DODIN operations and some internal defensive measures.

- **The Joint Functions and Cyberspace Operations;**

Joint functions common to joint operations at all levels of war fall into six basic groups: command and control (C2), intelligence, fires, movement and maneuver, protection and sustainment. This section guides for these functions.

The third chapter defines and guides for authorities, roles, responsibilities and legal considerations. The last chapter guides for the joint operation planning process and cyberspace operations, cyberspace operations planning considerations, command and control of cyberspace operations, synchronization of cyberspace operations, assessment of cyberspace operations, inter-organizational considerations, and multinational considerations.

2.1.2 Notes on Military Doctrine for Cyberspace Operations in the United States 1992-2014, August 27, 2015, Michael Warner, the Cyber Defense Review

This article [3] is related to the evolution of doctrine JP 3-12 (R) CO. The paper provides a detailed review on historical changes in the warfare doctrines since 1992 which began with the directive on information warfare and presents a path to understanding the evolution of cyber conflict as well as current military questions about the best ways of raising, organizing, training, and employing cyber forces.

2.1.3 On Cyberwarfare, DCAF Publications, 2015, Fred Schreier

This working paper [4] presents the definition and understanding of cyberwarfare and related issues, difference between information warfare and other types of warfighting domains. This paper gives us a general concept of the warfare in cyberspace and summary of major incidents of cyber conflict which can be used as a sample for related scenarios.

2.1.4 Cyberwar Thresholds and Effects

This article [5] reviews cyber-attack in armed conflicts, thresholds for considering cyber exploits as use of force, and possible cyber scenarios can be realized in the future. This paper gives some existing conflict in laws and political implications of cyber exploits and so draws its legal frames.

2.1.5 Principles of Cyberwarfare

This article [6] aims to define principles of cyberwarfare by adapting kinetic warfare principles which are rooted from Sun Tzu's thousands of years ago. That is a good starting point to determine the principles of CW/CO and so to define cyber scenarios models.

2.1.6 Applying Traditional Military Principles to Cyberwarfare

This paper [7] is also related with cyberwarfare principles. Their approach to determine the principles depends on applicable traditional military principles. The paper also explains approaches to an attack in cyber space and defines cyber conflict.

2.1.7 Cyberwar: The What, When, Why, and How

This article [8] gives a general concept of cyberwarfare and attempts to define the cyber-attack model, then gives a statistical information and methodological approach for cyber-attacks. This article can also be useful with given statistics and methodology for modeling cyber-attack scenarios.

2.2 Modeling of Cyberspace and Building CO Scenario Subjects

This section of the literature review, attempts to find previous research about modeling and simulation of Cyberspace, CO, and scenario models. This part of the review supports the main subject of the thesis.

2.2.1 Adversary Modeling and Simulation in Cyberwarfare

This paper aims [9] to utilize game theoretic techniques and uses a new probability search technique entitled Partially-Serialized Probability Cutoff Search, and demonstrates modeling time and time dependent attack techniques. This model can be useful for building a simulation engine for adversarial attack and guessing the steps of adversaries.

2.2.2 Simulating Cyber-Intrusion Using Ordered UML Model-Based Scenarios

This paper [10] presents a UML based scenario model and its network security simulator to overcome the limitation of existing simulations. The author's studies show the order steps of attack in a standard model (UML) for use in simulations. This can be a useful model for generating scenarios.

2.2.3 Modeling Active Cyber Attack for Network Vulnerability Assessment

This paper [11] proposed an active cyber-attack model to assess vulnerability in a network system. The model presents an integrated framework for active cyber-attack adapting “effect based operation”, ‘Sensor to Shooter’ and ‘OODA (Observe, Orient, Decide, Act) Loop’ concepts. The study offers a mechanism for a cyber-attack with two agents (ISR agent and Attack action agent) and two modules (Information Collection Management Module and Cyber-Attack Management Module) and an action controller and attack damage assessment analyzer. This paper can also be useful for building scenario generators in simulations.

2.2.4 Designing a Cyber Attack Information System for National Situational Awareness

This paper [12] proposed an approach to situational awareness (a recent term for intelligence analysis) and incident response cycle and a conceptual framework which is called the Cyber Attack Information System (CAIS) for the cyber-attack information center. Their concepts can be useful for the structure a systematic cyber-attack process and mechanism.

2.2.5 A Game Theoretic Engine for Cyberwarfare

This paper [13] presents an interesting theoretical game theory approach as we also sometimes consider the Cyberwarfare as a game. “The objective of a game theory engine is to identify for each player the set of feasible moves by all players from a given state, and to select the COA for a player that optimizes the sequence of future states with respect to his own assumptions at each step as the game proceeds.” This phrase is a good summary for the cyber object state variables and typical moves available to network. This study can be useful for offers a scheduler which manages checkpoint retention, saving the state of the game at specified times to build mechanism in simulation for replay, and rewind properties

2.2.6 Exploring Game Design for Cyber Security Training

In this paper [14] authors describe the state of practice by describing the gaming tool via the example of the cyber security gaming tool CyberNEXS™ (Science Applications International Corporation), which should be addressed in cyber security training and note some other approaches that might be useful for cyber security training game and simulation developments. This paper can be useful for selecting the subjects of scenarios and to disseminate a wide spectrum of cyber security topics for training issues.

2.2.7 Red Teaming of Advanced Information Assurance Concepts

In this paper [15] authors summarize the study of modeling red team development which was developed for Sandia National Laboratories Information Design Assurance Red Team (IDART) and used in five other DARPA projects. The paper explains the key elements of red team and, finally, lessons learned about the projects. This paper can be useful for modeling for red team in cyber security simulations and its scenario modules.

2.2.8 Cyber Security Kill Chain

This is a Lockheed Martin registered concept [16] to information security, using it as a method for modeling intrusions on computer networks. The model propose that threats must progress in seven stages; Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2 and Action. This concept can be useful to determine the stages of threats in the scenario model.

2.2.9 Cyber Attack Modeling and Simulation for Network Security Analysis

To efficiently simulate cyber-attack scenarios, this paper [17] presents a simulation modeling approach to represent computer networks and intrusion detection systems (IDS) and the generating IDS alert depends upon the attack

model according to phase groups. This paper can be useful to model a cyber-attack by phases.

The categorization of this chapter is shown in Table-1.

General Concepts and Cyber Terms	Cyber Principles	Cyber-Attack Modeling	CO Simulation Modeling	CO Scenario Modeling
2.1.1, 2.1.2, 2.1.3, 2.1.4	2.1.5, 2.1.6	2.1.1, 2.1.7, 2.2.3, 2.2.4, 2.2.7, 2.2.9	2.2.1, 2.2.5, 2.2.6, 2.2.9	2.2.2, 2.2.3, 2.2.4, 2.2.6, 2.2.8

Table 1 Categorization of reviewed previous works.

3 CHAPTER THREE

DESCRIPTION OF THE CYBER TERMS

3.1 Cyberspace

The first usage of cyberspace was in a science-fiction novel in 1984 *Neuromancer*, Gibson, W. [18] "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity..."

According to the U.S. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms [19]; "The notional environment in which digitized information is communicated over computer networks. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers."

OTTIS, R. [20] add time parameter and defines cyberspace; "a time-dependent set of interconnected information systems and the human users that interact with these systems."

In the US Joint Publication 3-12 (R) *Cyberspace Operations Doctrine* [2] defines; Cyberspace while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. The physical network layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual,

specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.

From the several definitions as described above, we can say cyberspace has several layers such as physical, logical, cyber-persona, time, etc., and comprises all components which data can be digitally processed, transmitted and stored such as cable, wireless, satellite, computers, disks, files, software and systems. Besides, with military perspective, it is also considered an interdependent domain within the information environment with the other four physical domains of air, land, maritime, and space.

3.2 Cyberwarfare (CW)

The first usage of cyberspace as domain for war was also in William Gibson's science-fiction novel *Neuromancer* in 1984[18]. It tells how savants hacked their rivals in the "consensual illusion" of cyberspace, and also how corporations and states fought each other in that digital realm. Subtly influencing from *Neuromancer*, several definitions have been made about CW. In my opinion the term and principles of CW has not been matured yet; the evolution process continues.

In many military documents CW has been defined as a sub war of Information Warfare (IW) and was inspired by the kinetic war definition. Initial documents describe CW as, "all actions by a nation-state to protect her computers and information systems from adversaries while take control, influence or damage of them."

Cyberwarfare has been defined by Clarke, Richard A.[21] as "actions by a nation-state to penetrate another nation's computers or networks for the

purposes of causing damage or disruption," but later definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations. Then, the term gains additional non-states meanings.

3.3 Cyberspace Operations (CO)

The US Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms [19] defines the term cyberspace operations as “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.” The US has also a joint doctrine about CO JP 3-12(R)[2] for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations. The evolution process of IW brought out firstly the term CW then IW turned into Information Operations (IO) and CW turned into CO in the US by a long term evolution process. Today, there is not any definition about IW or CW on JP 1-02 Department of Defense Dictionary of Military and Associated Terms. Michael Warner [3] summarized the 20-year period of the evolution of these terms in his article. According to his article chronically;

- JP 3-13 published as Command, Control, and Communications Countermeasures (C3CM) in 1987.
- DoDD TS 3600.1 defined information warfare that include psychological operations (PSYOP), Electronic Warfare (EW), Command and Control Warfare (C2W), military deception and physical attack/destruction after the 1991 Persian Gulf War,
- Joint Doctrine for C2W published as the first doctrinal definition in early 1996. C2W is an application of IW in military operations and is a subset of IW.
- Information Operations defined as the replacement of Information Warfare by introducing the concept of “computer network attack”

which it defined as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” in late 1996.

- Joint Doctrine for Information Operations (JP 3-13) published in October 1998.
- JP 3-13 was updated after the experiences in Afghanistan and Iraq in 2006. The document establishes the core capability of computer network operations (CNO), consisting of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE).
- Next revision of JP 3-13 published in November 2012, and the new version quietly abandoned the idea that computer network operations represented a core IO capability and CNO, CNA, CND, and CNE
- New doctrine Joint Publication 3-12, Cyberspace Operations emerged in 2013 for this subject [19]. Cyberspace and information operations are often complementary, but cyberspace operations (CO) employ capabilities “to create effects which support operations across the physical domains and cyberspace,” while information operations in contrast employ “information-related capabilities...to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.”

20-year period of the evolution of these terms is resulted with a doctrinal shift. In the past, CO have been considered a subset of IO and those operations incorporated in the terms of computer network operations, computer network attack, computer network defense, and CNE. JP 3-12 described the purposes and scope of cyberspace operations. Such operations would now perform three kinds of missions:

- Offensive (“intended to project power by the application of force in and through cyberspace”), Offensive missions are authorized like all “operations in the physical domains, via an execute order.”

- Defensive (“intended to defend DoD or other friendly cyberspace”) Defensive missions can be either passive or active (and can even create effects outside DoD networks that “rise to the level of use of force”).

- Sustaining (of DoD systems).

The commander conducts these missions using four basic kinds of cyberspace actions. Two of which—cyberspace defense and cyberspace attack. The latter two, however, are novel, and correspond to the old CNE category. They are as follows:

- Cyberspace intelligence, surveillance, and reconnaissance (ISR) includes ISR activities in cyberspace conducted to gather intelligence that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and operation of cyberspace systems, in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction, and cyberspace forces that are trained and certified to a common standard with the intelligence community (IC). ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other government departments and agencies.

- Cyberspace Operational Preparation of the Environment (OPE) consists of the nonintelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE requires cyberspace forces trained to a standard that prevents compromise of related IC operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other government departments and agencies.

Last word, because all things occurs in milliseconds, moreover never two states cyber armies will fight each other, the term cyberspace operations is more accurate meaning for the events we mention, instead using the term cyberwar. So, from this point to have a clear understanding of the thesis CO is equal meaning with CW.

3.4 Principles of War and Cyberwarfare

While our purpose is to build CO scenario DB model, which is to use in CO simulations, this subject should depend on some principles. In order to determine these principles, firstly we should look into principles of traditional (Classic) war which have been derived from thousands of years of experience as Sun Tzu, Carl von Clausewitz, Mustafa Kemal Atatürk and many others. They are known as the principles of war. We can adopt these proven principles into new domain CS. According to JP 1, Doctrine for the Armed Forces of the US [22], those principles are; Objective, Offensive, Mass, Economy of force, Maneuver, Unity of command, Security, Surprise and Simplicity. While these principles are utilized for classic wars, Raymond C. Parks and David P. Duggan [6] study these principles to use in CW and so CO;

3.4.1 Objective

Military operations should be a clearly defined, decisive, and attainable objective. This principle has also same meaning in CO.

3.4.2 Offensive

This principle means to seize, retain, and exploit the initiative. In CO moving bits is much easier than moving tanks, ships, and aircraft, so the principle of offensive can easily apply to CO.

3.4.3 Mass

The commander should concentrate the effects of combat power at the decisive place and time of combat power at a particular place and time to

achieve decisive results. In CO, using overwhelming force is naturally largely accepted tactic (e.g. denial-of-service (DOS) attacks).

3.4.4 Economy of Force

Commander should allocate minimum essential combat power to secondary efforts. Because CO is the exemplar of asymmetric warfare, economy of force for both secondary and primary efforts is essential.

3.4.5 Maneuver

Commander should plan to gain advantage and place the enemy in a disadvantageous position. This principle should also use in CO.

3.4.6 Unity of Command

To achieve the goal, all units of operation should be directed one responsible commander. Generally, this is applicable to CO in most operations, but some types of attacks have exemption for this, such as crowd-sourcing and Low Orbit Ion Cannon (LOIC), that use unwitting bystanders or loosely controlled volunteers who are not within the command of the combatant.

3.4.7 Security

Protecting our forces and outmatching the enemy to acquire an unexpected advantage is important. This principle is applicable to CO within the nature of cyberspace

3.4.8 Surprise

Strike the enemy at an unexpected time or place or in a manner. This principle may be the most applicable ones to CO, because of the man-made nature of cyberspace.

3.4.9 **Simplicity**

Commander should prepare clear, uncomplicated plans and clear, concise orders to ensure that every soldier is on the way of the same objectives. This principle is also valid in CO because friendly fire is a negative factor and should be avoided.

3.5 **Cyberspace Specific Principles**

As seen, the basic principle of war is fixed, although warfare evolves by generations. Now cyberspace is regarded as the fifth domain in theater [2,23], so we can adopt nearly the same principles for CO as mentioned above. That's a good starting point. Raymond C. Parks and David P. Duggan also proposed additional Cyberwarfare Principles in the same article [6]. These are;

3.5.1 **Lack of Physical Limitations**

Physical limitations of distance, quantity and space have not much adverse effect in CO because of the nature of cyberspace. In cyberspace, other side of the Earth or multiple copies of a cyber-weapon has almost no expense of time or materials.

3.5.2 **Kinetic Effects**

In CO as it is in 4GW, affect the minds of decision-makers is important. According to its objective, CO should have a kinetic effect in the real world. Opening of a dam spill-gate, shutdown of an electrical substation or exploding pipelines can be done with using cyber space.

3.5.3 **Stealth**

Cyberspace is created by human beings and for protecting and detecting intruders in it, hardware and software is used, so attackers cannot pass directly a firewall or IDS. For a successful attack, attacker's bits should be seen as

normal activity bits and on the other side, defenders should distinguish those bits than normal by capturing network packets and using appropriate tools.

3.5.4 Mutability and Inconsistency

As the definition of Cyberspace, time is a parameter for cyber space. There are no totally same any process which runs different time, software can fail, hardware can fail, programs can run faster than expected, temperature, buffer size, etc. can change. Because this domain is artificial, we cannot assume that it is sufficiently mutable or reliable. So in CO, attacks do not always behave the same way, environments can change at the mid-attack.

3.5.5 Identity and Privileges

The nature of cyber space, to perform any action depends on identity, privileges and access rights so an attacker's goal is to take control of privileges and identity of that entity.

3.5.6 Dual Use

In classic warfare, majority of weapons has single purpose, which is offense, defense, or sensing. However, CO's majority tools are dual use and security teams test their systems to look for weaknesses by attackers' tools. Vulnerability scanners, packet capture devices, penetration testing tools are sample for this principle.

3.5.7 Infrastructure Control

Cyber space cannot be controlled by one side (defenders or attackers). The majority part of infrastructure is controlled by commercial providers. For example, DoD directly controls only 10 percent of the communications infrastructure used for DoD traffic. This means that both attacker and defender are vulnerable to attacks on third-party infrastructure and if one side can take control of part of that infrastructure, that party gains a significant advantage.

3.5.8 Information as Operational Environment

In kinetic warfare, all information about terrain, the weather, the enemy's condition is important for Information Preparation of the Operational Environment (IPOE). Sensors are used for transform the physical reality into information. In CO, it's the information itself that constitutes IPOE. The communication connections, computer network maps, personnel rosters, websites, links, emails, postings, and every other aspect of the target is already information in cyberspace.

3.5.9 Insidious Attack

This is my first additional offer for CW principles. As cyberspace is a man-made artificial domain, everything processed in a rule and expected results. So if an attacker tries to attack directly, firewalls, IDS, and IPS can detect and defuse it. So attackers use an insidious object such as Trojan, backdoor, spyware, etc. Generally, social engineering or software deficiencies provide possible access.

3.5.10 Persistency

This is my second additional offer for CW principles. In cyberspace a new type of weapon has been created, APT's (advanced persistent threat), with the most known one is Stuxnet. There is no time limitation to gain advantage, the tricky point is a targeted attack for critical objects, so persistency is important.

Briefly, cyberwarfare is different from conventional, kinetic warfare. One of the fundamental differences between cyberwarfare and kinetic warfare is the nature of their environments. Kinetic warfare takes place in the physical world, governed by physical laws that we know and understand with respect to warfare. Cyberwarfare takes place in an artificial, man-made world that's constantly changing. Cyberwarfare can use some principles of kinetic warfare,

but others have little or no meaning in cyberspace. For these reasons, new principles of cyberwarfare should be different from those of kinetic warfare.



4 CHAPTER FOUR

DESCRIPTION OF CYBER SECURITY SIMULATIONS

4.1 Description of Cyber Security Simulations

Developed nation's prosperity and physical security mostly depends on their cyberspace facilities. However, this domain can also be used by adversaries to exploit nation's critical infrastructures. To protect these systems requires well-planned cyber security strategy, talented cyber-defender, monitor and analysis of the systems. Response time, training and technology are the most important characteristics of cyber incidents [24]. Regarding the time and bandwidth costs, implementing a real drill would be inefficient; therefore, training in this domain has created this certain need for robust and realistic simulation software. In a real-time simulation environment, data and scenarios from real incidents can be implemented and from the analysis that comes out of the simulation, nations can build more effective defense mechanisms and event-specific procedures. Therefore, Cyber security simulations have certain benefits;

- Effective training,
- Standardized skills assessment,
- Portability and scalability,
- Planning and modeling tools,
- Rewind and replay.

There is a certain need to describe standards of this new type of simulations to achieve the benefits above. Bryan K. Fite proposes an innovative way to model Cyber Operations via simulations, abstracting the fundamental elements as Objects and describing their interaction via a Simulation Definition Language (SDL) [25]. SDL helps to standardize the expressing definition of a scenario from a narrative or story into certain types of objects and to the rules that govern them. Using a standard SDL ensures consistent assessment capabilities across platforms and makes simulations available to more diverse populations, regardless of budget, access to technology or experience-level.

4.2 Existing Cyber Security Simulations

Various simulations exist which have different structures and purposes. Capture the flag (CTF) competition-based simulations are the most well-known. Capture the Flag (CTF) is a special kind of information security competitive game involving opposing teams trying to steal something of value from each other. In computer security, the flag is typically a piece of secret data, and the territory from which it is captured is a computer system controlled by the opponent. There are some popular formats for CTF games: Jeopardy-style, attack/defense, mixed form, King of the Hill and Cyber Grand Challenge (CGC) have adopted this format, challenging fully automated systems to reverse engineer unknown software, then locate and heal its weaknesses in a live network competition.

Here, only well-known simulations are listed to make comparison with our study.

4.2.1 Cyberlympics

Global Cyberlympics(<http://www.cyberlympics.org/>) is an international online cyber security competition, dedicated to finding the top computer network defense teams. This event tests the skills of information assurance professionals in teams of 4 to 6 people in the areas of ethical hacking, computer network defense and computer forensics.

4.2.2 CyberPatriot

Cyber Patriot (<http://www.uscyberpatriot.org>) is the U.S. National Youth Cyber Education Program. There are three main programs within CyberPatriot: The National Youth Cyber Defense Competition, AFA Cyber Camps and the Elementary School Cyber Education Initiative. CyberPatriot was conceived by the Air Force Association (AFA) to inspire students toward careers in cyber security or other science, technology, engineering, and mathematics (STEM) disciplines critical to the nation's future.

4.2.3 Defcon CTF

This is a CTF game at DEFCON (<https://legitbs.net/>) which is the oldest cyber security meetings and world's best known hackers' convention. Their claim is "We build innovative Capture the Flag games that pit hackers from around the world against the smartest analog adversaries and computerized challengers known."

4.2.4 Siber Meydan

This is yet another cyber security competition simulation developed by TÜBİTAK BİLGEM Cyber Security Institute (www.sibermeydan.org) and includes scenarios featuring all kinds of vulnerabilities that may be found on network components, clients, servers and corporate services. Different types of competitions such as "Capture the Flag" or "Defend Yourself and Penetrate the Enemy" maybe applied [26].

4.3 IWSIM

The IWSIM project (iwsim.yasar.edu.tr) started in 2014 at Yaşar University with the aim of providing two simulators at once; the first one is a comprehensive simulator and drill environment for cyber security teams to training on, and the second one is a cyber-incident analyzer tool for local networks, critical infrastructures, and for countrywide area networks. The main aims of this research are;

- To improve our strategies, tactics and power in cyberspace,
- To deduce outcomes from cyber incidents to strengthen our networks and secure our critical infrastructures,
- To train qualified personnel for this arena.

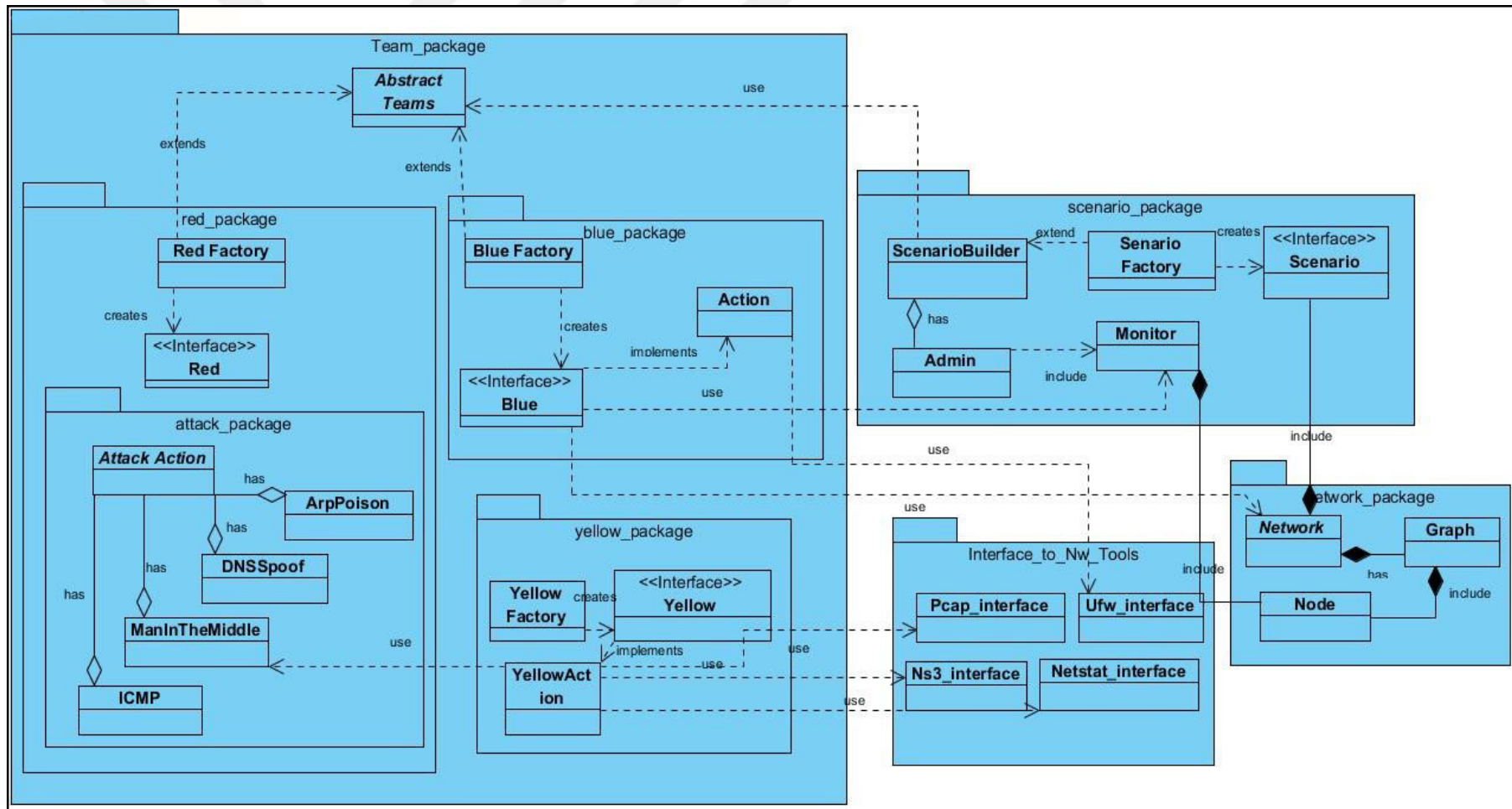
The author of this study and four other individuals with the advisor Assoc. Prof. Ahmet H. Koltuksuz maintain the IWSIM project at the Cyberspace Security lab of Yaşar University. The project has continually advanced from following three main modules;

- Network and Critical Infrastructure Modeling
- Scenario Construction, Analysis and Interfacing with Metasploit
- Attack and Malicious Code Analysis Module

4.3.1 Environmental Settings

The IWSIM environment can be set up on an arbitrary number of machines on a network where each one is called a “node”. Nodes can be real or virtual machines as well. The Ubuntu operating system was chosen as the development environment. Although IWSIM is written in JAVA for portability purposes, it bears shell scripts for open source tools such as Metasploit, NS3, Ettercap, Wireshark, Ufw, Nmap, Netcat, Inetsim, Hping3, Sshpass, Scada Honeynet Project and Scp [27]–[38].

IWSIM has approximately 7000 lines of code and the numbers of lines are increasing steadily. The project is currently 800 KB without any external open source tools packed in it. Figure-1 specifies core functions of the IWSIM. Mainly, it consists of Red, Blue, Yellow, Interface and Network Tools packages. All the teams are binded with the scenario package. A scenario is created by admin, using the xml file format. Teams are specified with ip addresses and virtual nodes on each ip.



ure 1 Core Code Architecture of IWSIM.

Fig

IWSIM, as mentioned above, can be set up as both team drill environment and scenario analyzer. In team drills, the environment may have five different teams; red for the attacker, blue for the defender, yellow for reconnaissance, white for facilitators, and green for administrative. While the Green team is dedicated to the drill scenarios, the administrative team is the referee of the drill, and customer of the analysis tool. However, when the case is to analyze a scenario, a virtual network environment is set and actions are taken in accordance with the scenario instead of building teams. The time parameter of the simulator is scaled by the constraints of a scenario.

4.3.2 Main Modules of IWSIM

In this section, the details of the main modules are given and the information flow between these modules is provided.

4.3.2.1 Network and Critical Infrastructure Module

This module is the backbone of the IWSIM. It provides implementations of network nodes and devices. Network nodes can be real or virtual; therefore, this module uses Inetsim, Scada Honeynet Project and Netcat in order to support the servers, SCADA systems and any type of virtual nodes communicating from various ports. Apart from these open source tools, IWSIM acts as an adapter for all of these to communicate on the simulated network. Network and Critical Infrastructure generations are achieved by their respective modules.

4.3.2.1.1 Network Generation Module

Given the parameters, IWSIM utilizes shell scripts running over a network to add nodes to the simulated scenario. Network nodes can be configured with either NS3, Netcat, Inetsim or native JAVA network packet generators to act as a part of the designed network topology.

4.3.2.1.2 Critical Infrastructure Generation Module

This module heavily depends on the Scada Honeynet Project to model critical infrastructure networks. Network nodes, generated either for teams or scenarios, interact with the Scada Honeynet nodes in order to simulate attacks such as Stuxnet.

4.3.2.2 Scenario Construction, Analysis and Interfacing with Metasploit

The construction of the scenarios and performing the analysis afterwards while Metasploit interfacing is taking place are done through the modules detailed below. This model is the first version of the building scenario database.

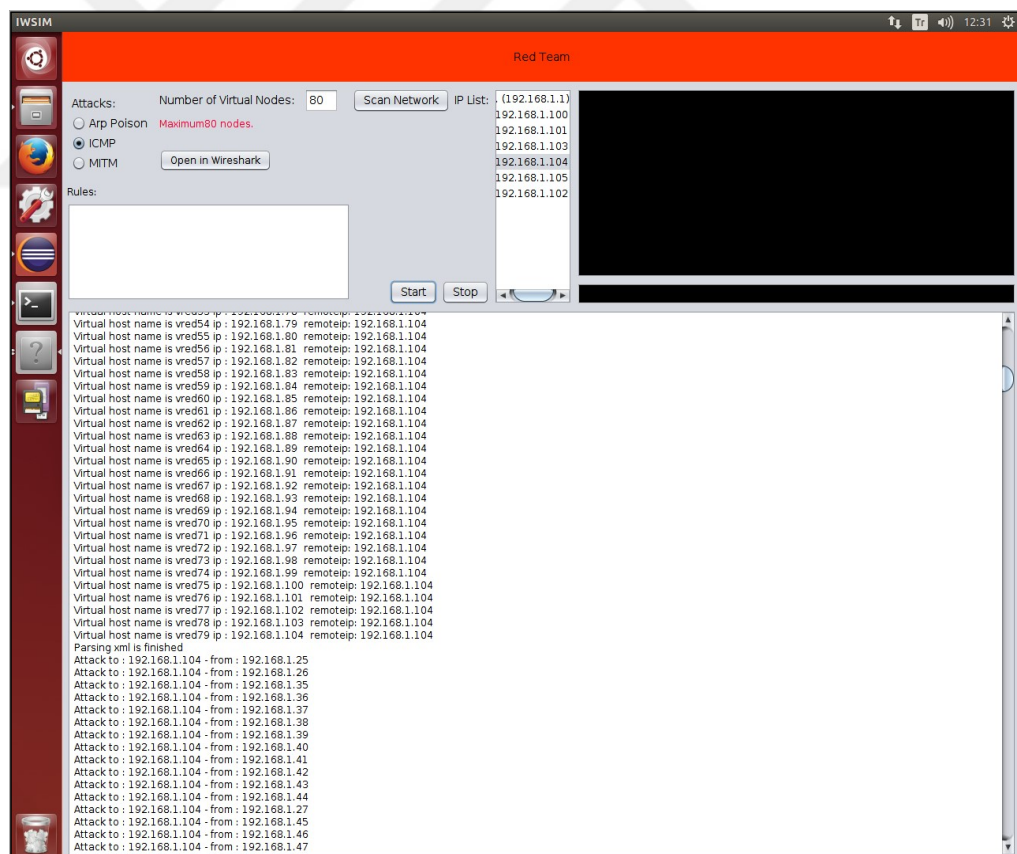


Figure 2 Sample of Red Team Screen.

4.3.2.2.1 Scenario Module

The scenario module runs on the administrator node in order to define a network topology and the roles which are based on an incident or assignment of the teams. All communications taking place between IWSIM nodes are done by XML file format. The administrator node provides a UI for generating these XML files and is responsible for sending them over the network to implement the scenario.

4.3.2.2.2 Scenario Analysis and Map Module

Time lines and charts are generated on the processes over the backbone of the scenario or the drill. At any time of the running event, the actions and locations can be tracked with this module. The locations must be provided to IWSIM with the scenario so that the nodes can be distributed over a map.

4.3.2.2.3 Metasploit Interface Module

A reduced Linux based terminal is implemented in IWSIM for integrating an instance of Metasploit Console (msfconsole). Metasploit is integrated to the project for two reasons; the first one is to check in case there are any known vulnerabilities of the simulated system, and second is to automatize post exploits for the vulnerabilities defined in the scenario.

4.3.2.3 Attack and Malicious Code Analysis Module

To understand a malicious network package, one needs to capture all of the incoming/outgoing traffic and process each package, decompile it, and check whether there is malicious content inside the package or not. This process is a highly costly operation to accomplish.

In this simulator, IWSIM has a module that implements a man-in-the-middle procedure to a simulator's router and detects if there is a spoofing in the IPs, DNS entries; anomalies in operating systems; traces of ARP

poisoning, or such anomalies occurring at any of the nodes. Therefore, detecting an attack either from one of the teams as they are in the drill or from the exploit that is used by Metasploit module is possible to achieve. Very helpful data from cyber incidents can be extracted this way.

In addition to these modules, IWSIM also has a module which functions as a reporting, logging and chatting module to be used in drills.

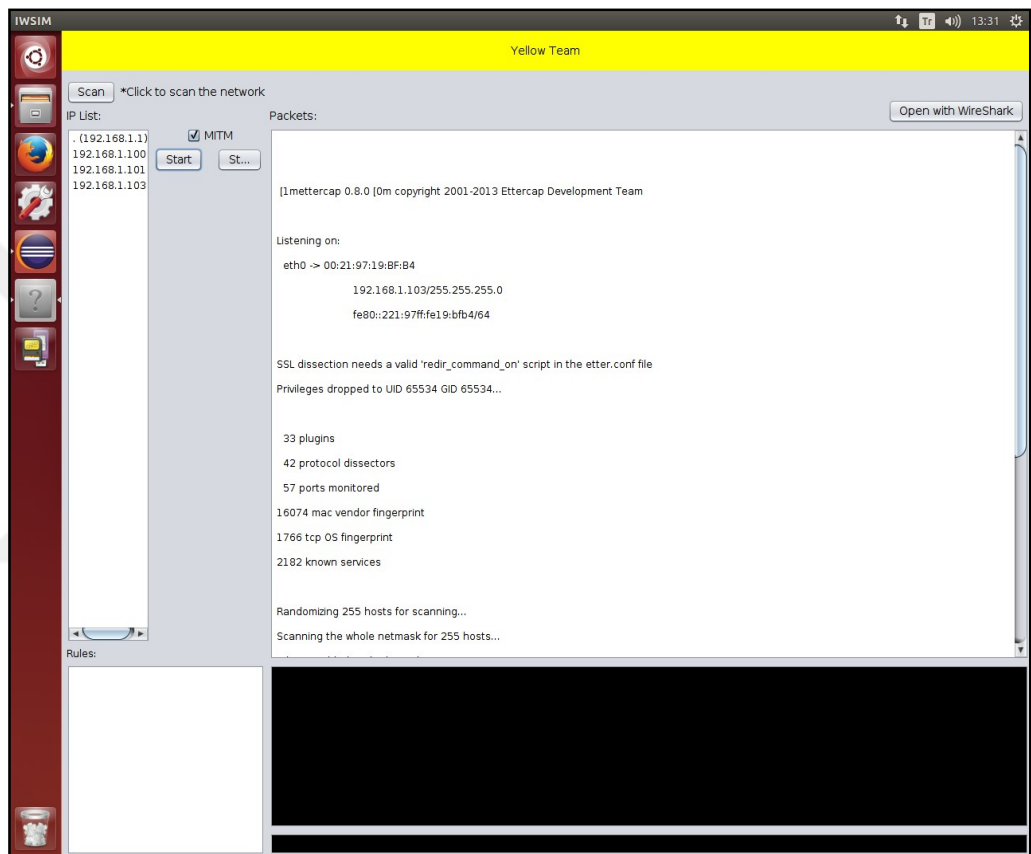


Figure 3 Sample of Yellow Team Screen.

4.3.3 IWSIM Scenario Parameterization & Running

One of the most useful aspects of IWSIM is its ability to use scenarios in a parameterized way so that any scenario can be applied in this simulator according to the needs dictated by strategies and/or tactics of the training job in hand. The scenario parameterization is introduced in the three steps below.

4.3.3.1 **Network Parameterization**

IWSIM can create servers, firewalls and arbitrary virtual nodes in order to implement a scenario. In a drill mode of IWSIM, the administrator team decides which nodes/teams have what kind of services each. As shown in Table 1, an example team can have a FTP server, a web server and a SSH server whilst having the ability of DDOS and Man-in-the-Middle attacks. Most commons server types are imported from the Inetsim tool, which is an Internet service simulation suite. It also provides a gray traffic for the simulation environment while implementing a scenario. Firewalls are created by configuring the default firewall of the Ubuntu operating system (Ufw).

4.3.3.2 **Incident Parameterization & Visualization**

Implementing a cyber-incident involves describing the attack type, attack duration, starting time with respect to the scaled time parameter of the simulator, attack IPs, node locations, firewall actions such as port blocking, and IP range blocking. Such specifications are also exemplified in Figure-4.

```

<scenario>
  <name> Example Scenario</name>
  <scenarioType> analyze </scenarioType>
  <scenarioElements>
    <server>
      <ftpServer>
        <name>ftpServer1</name>
        <protocol> ftp </protocol>
        <ip> 192.168.1.105</ip>
        <interfaceName> eth0 </interfaceName>
      </ftpServer>
      <webServer>
        <name>webServer</name>
        <protocol> http </protocol>
        <ip> 192.168.1.107</ip>
        <interfaceName> eth0 </interfaceName>
      </webServer>
      <SSHServer>
        <name>SSHServer</name>
        <protocol> ssh </protocol>
        <ip> 192.168.1.105</ip>
        <interfaceName> eth0 </interfaceName>
      </SSHServer>
    </server>
    <attack>
      <DDOS>
        <tool> hping3 </tool>
        <flag> icmp </flag>
        <flag> SYN </flag>
        <flag> ATCK </flag>
        <speed> realTime </speed>
        <time> always </time>
      </DDOS>
      <MITM>
        <tool> ettercap </tool>
        <flag> M ARP</flag>
        <targetIP> 192.168.1.1 </targetIP>
        <logFileName> mitmlog </logFileName>
        <time> 5min </time>
      </MITM>
    </attack>
  </scenarioElements>
</scenario>

```

Figure 4 Example XML file defining the parameters of a Scenario.

IWSIM Scenario Parameterization model is the first version of the building scenario database. When running a scenario, the actions that are defined on the scenario file are executed according to their order on the file by the *Scenario Factory* class. *Network* class includes the scenario file from the factory and the network and virtual nodes are created regarding this file. Network creation is done by sending the virtual host creation command to the NS3 instances on the connected ips. Each node then creates the virtual nodes and executes the partial scenario on their part. All the network tools and scripts are interfaced through *Interface_to_Nw_Tools* as well as the scripts for NS3 interface. When implementing a new attack type, necessary modules

should be implemented in this package in order to be used in scenarios and this is one of the main ramifications of this project.

The IWSIM environment has the ability to visualize attacks on a map. On this map gray traffic is ignored and at the current stage nodes are shown at their locations if they are specified by the administrator.

4.3.3.3 Team Arrangement

When the administrator module starts, it immediately scans the IWSIM main router for the connected nodes on the network. Defined by the IPs, the nodes are assigned to separate teams provided with the list of possible actions that each team can take depending on the rules of the game. In the default setting, Red Team is the attacker team, Blue Team is the defending side and Yellow Team is the reconnaissance team for both Red and Blue sides.

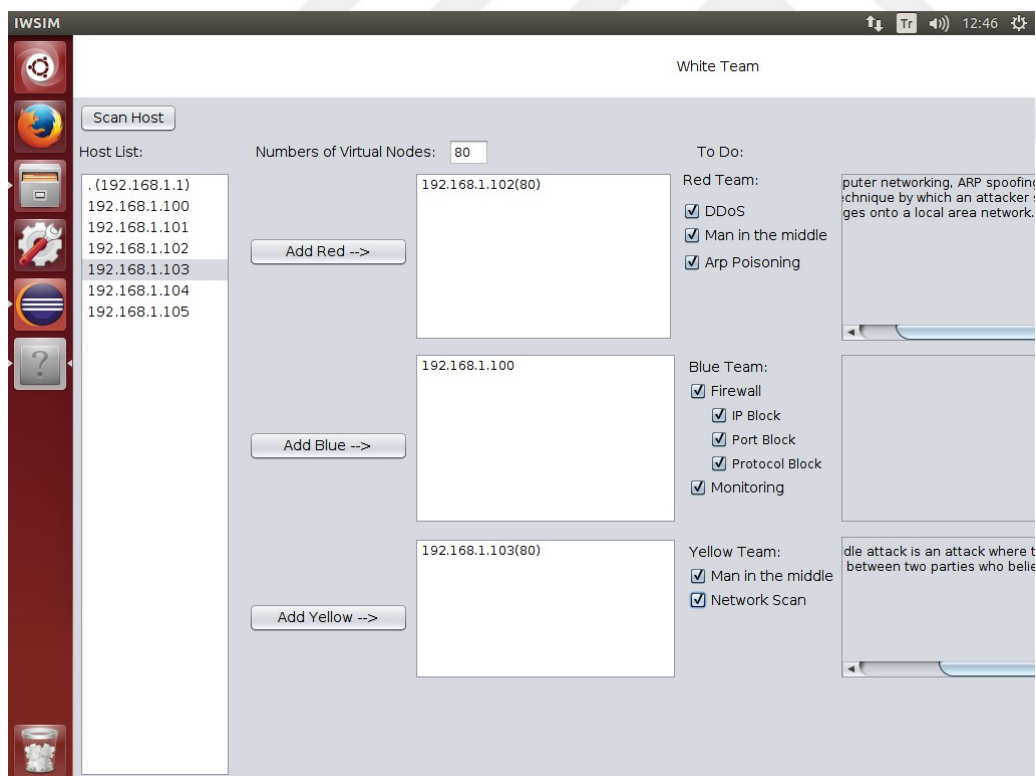


Figure 5 Sample of White Team Screen.

Red team is mainly equipped with attack tools whilst blue has the capabilities of an IT department. Currently red team has 4 different types of attacks. They are man in the middle, DNS spoofing, arp poisoning and ddos. These attacks are scripted through etherape, ettertap, tshark.

For the time being, blue team has the abilities of port blocking, IP blocking, allowing specific protocols and other management of Ubuntu's firewall and incident reporting.

For the yellow team, IWSIM has simple anomaly detection and a network sniffing tools. Yellow team has the ability of conducting MITM attacks as well as red team. However, aim of the yellow team depends on the scenario and this team has the necessary permissions for working for both teams. Depending on the scenario or the drill, this team can gather intelligence for red or blue team or both at the same time.

5 CHAPTER FIVE

BUILDING CYBERWARFARE / OPERATION SCENARIOS

Cyberwarfare simulations have many modules as we built in IWSIM. In this chapter and thesis focus on only building CO scenario model. Building CO scenario is one of the most important parts of the simulation, but if this model combines with other modules (network, analysis, mapping, visualization, management, etc.) then it became a CO simulation.

5.1 Properties of Cyberwarfare / Operation Scenarios Database

In this section concentrated on cyber operation scenarios principle depends on, as mentioned in section 2, studies on building principles of Cyberwarfare/operation. Inspired from hacker's attack paths and to think like a hacker, this model should follow pattern of an attacker's steps. According to this, a cyber-operation scenario should contain the phases occurs that are shown in below.

- Preparation Phase (Preliminary, Threat Identification, Attack planning)
- Attack Phase (Espionage, Diffusion, Management)
- Post-attack Phase (Escalation, attain targets, remove traces and preparing next step)

Details of these phases are not the subject of this thesis, but while building a scenario we should consider them and make many calculations on our plans. Old strategist Sun Tzu said about this manner, *“Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.”*

In addition to phases to achieve our objectives, cyber operation scenario should cover these basic properties;

5.1.1 **Traceable:**

Scenarios can be traced at every step. They also allow you to generate reports about status.

5.1.2 **Rewind and replay**

For training, analyzing and planning purposes, scenarios should be rewind and replay.

5.1.3 **Scalar:**

Because of the limitation of an environment, real cyber events should be modeled and fit in a simulation environment.

5.1.4 **Measurable:**

Evaluation with metrics is important for CTF based scenarios, there should be measurable events in points to establish a winner or get statistics. Some of the metrics examples [15] are:

- Number of exploits and attack scenarios,
- Number of services and protocols represented in the test network and data,
- Number of resources required to run each security system feature on a specific platform,
- Number of operating system platforms that can run successfully using a security system,
- System overhead percentages for each security feature,

- The degree to which a security system increases the applications capability and enhances the reliability and fault tolerances of a network,
- The security system does not add depreciablely to the end-to-end network delays as indicated by throughput calculations and measurements,
- Security mechanisms provided by a security system are shown not to be weak against different compromising scenarios,
- Percentage of access attempts that are effectively denied by a security system,
- Percentage of denial of service attacks that succeeded in denying critical operations,
- Percentage of attacks that succeeded in crashing the security system itself and the degree of recoverability,
- Distribution of times for response to be complete from the time that the attack was assessed,
- Distribution of times for response to be complete from the time the first event of attack was detected,
- Distribution of times to alert unauthorized access from the time the first event of attack was detected,
- Distribution of times to recover operations for valid users after a denial of service attack,
- Distribution of times to recover critical operations,
- Distribution of times to re-establish the normal operational state after a successful attack against the system.

5.2 Modeling Cyberwarfare / Operation Scenario Database

Benefiting from previous searches some of which are in section 2 and experiencing in IWSIM, a database model has developed for CO. Considering our Cyberwarfare / Operation Scenarios properties a database schema (ER)

diagram has been built in Appendix-1 with the 3rd normal form. According to principles of CO in section 3, IWSIM properties and objectives in section 4 and told by Bryan K. Fite from SANS Institute [25], the scenario database should contain some primitive and optional elements. By corporate with previous related research and literature in this section models a CO scenario database. In this model network components are assumed optional elements as it should be managed by the network module of the simulations.

In this model elements are explained below.

5.2.1 Scenario Name and Story

Every scenario should have a name and story. The story can be described as the vocal order of the commander. It should be a 50-100-word phrase, understandable by everyone and shows the intent of the commander.

senarios	
id:	INTEGER NOT NULL [PK]
name:	VARCHAR(255) NOT NULL
story:	LONGVARCHAR
notes:	LONGVARCHAR NOT NULL
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP

Table 2 Scenario table.

5.2.2 Scenario Type

Attack and defense are not sole types of operations. According to U.S. JP 3-12 (R) there are several types of CO (Intelligence Operations, Offensive Cyberspace Operations, Defensive Cyberspace Operations, Information Network Operations, Routine Uses of Cyberspace, Cyberspace Defense, Cyberspace ISR, Cyberspace Operational Preparation of the Environment, Cyberspace Attack, and Joint

Operations). These types help to categorize CO and determine other primitives.

senario_types	
id:	INTEGER NOT NULL [PK]
name:	VARCHAR(255) NOT NULL
notes:	LONGVARCHAR
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP

Table 3 Scenario Types table.

5.2.3 Scenario Actors

They are active participants in a scenario. They have several roles due to their teams. This element contains such information like id, role, team info, capability level, adversary type, email, phone number.

actors	
id:	INTEGER NOT NULL [PK]
name:	VARCHAR(100) NOT NULL
team_color:	VARCHAR(100) NOT NULL
role:	VARCHAR(255) NOT NULL
adversary_type:	VARCHAR(255)
capability:	VARCHAR(255) NOT NULL
notes:	LONGVARCHAR
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP
team_id:	INTEGER NOT NULL [FK]
phone:	CHAR(15)
email:	CHAR(100)

Table 4 Scenario Actors table.

5.2.4 Scenario Teams

For running a scenario under the simulation environment and set up rules, there should be several groups for management, attack, defense, reconnaissance, etc. These groups can be identified by the majority accepted colors (red, blue, yellow, etc.).

scenario_teams	
id:	INTEGER NOT NULL [PK]
scenario_id:	INTEGER NOT NULL [FK]
team_color:	VARCHAR(255) NOT NULL
team_name:	VARCHAR(255)
name:	VARCHAR(255)
surname:	VARCHAR(255)
email:	VARCHAR(255)
phone:	VARCHAR(255)
notes:	LONGVARCHAR
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP

Table 5 Scenario Teams table.

5.2.4.1 Blue Teams

They are defenders whose main task is to secure and protect a pre-built infrastructure against the Red Team's attacks.

5.2.4.2 Red Teams

They are attackers, their mission is to compromise or degrade the performance of the Blue Team systems.

5.2.4.3 White Teams

They are responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information

systems. They had the responsibility for preparing the scenario and controlling it during execution.

5.2.4.4 Yellow Team

Their role was to provide situational awareness about the game, mainly to the White Team but also to all other participants.

Scenario Teams element contains such information like team id, color, leader id (this id belongs to actor's id).

5.2.5 Scenario Constraints

Since scenarios run in a simulator which is modeling cyber space or an operation theater each requires some limitations which can be time or environment factors. This element contains such information like id, constraint type, unit, unit type.

scenario_constraints	
id:	INTEGER NOT NULL [PK]
const_type:	VARCHAR(255) NOT NULL
unit:	NUMERIC(3)
unit_type:	VARCHAR(255)
notes:	LONGVARCHAR
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP
scenario_id:	INTEGER NOT NULL [FK]

Table 6 Scenario Constraints table.

5.2.6 Objectives

Basically, objectives show scenario aims. This element contains such information like id, objective class, type, target_id and objective_text.

objectives	
id:	INTEGER NOT NULL [PK]
name:	VARCHAR(255) NOT NULL
o_class:	VARCHAR(255)
o_type:	VARCHAR(255)
notes:	LONGVARCHAR
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP
scenario_id:	INTEGER NOT NULL [FK]
target_id:	INTEGER NOT NULL [FK]
objective_text:	CHAR(1)

Table 7 Scenario Objectives table.

5.2.7 Nodes

Any system in a scenario related to network layers. Nodes info contains such information like id, name, flag, OS, interface addresses, mac addresses, vendor, version, purpose and other optional properties like services, listening ports, etc. Nodes table is complemented with nodes_props table for detail properties and their values of nodes.

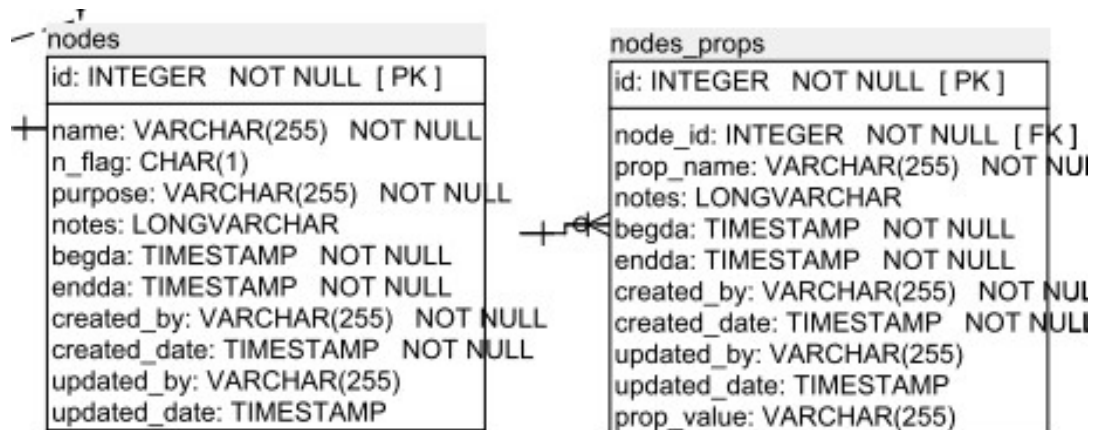


Table 8 Nodes table.

5.2.8 Network

This tables uses for define the communication path between teams, actors, and nodes. Actually this element is the basement of the simulation and should be managed in another module of the simulation. The db model should only cover the information in this network. Networks info can be describing with network properties and their values as optional info type.

- Network table contains such information like id, scenario_id, and name.
- Network_props table contains id and property columns, and such information like protocol, capacity, topology, layers, domain, mac_addresses, and switches, etc
- Network_values table contains net_prop_id and prop_value columns.

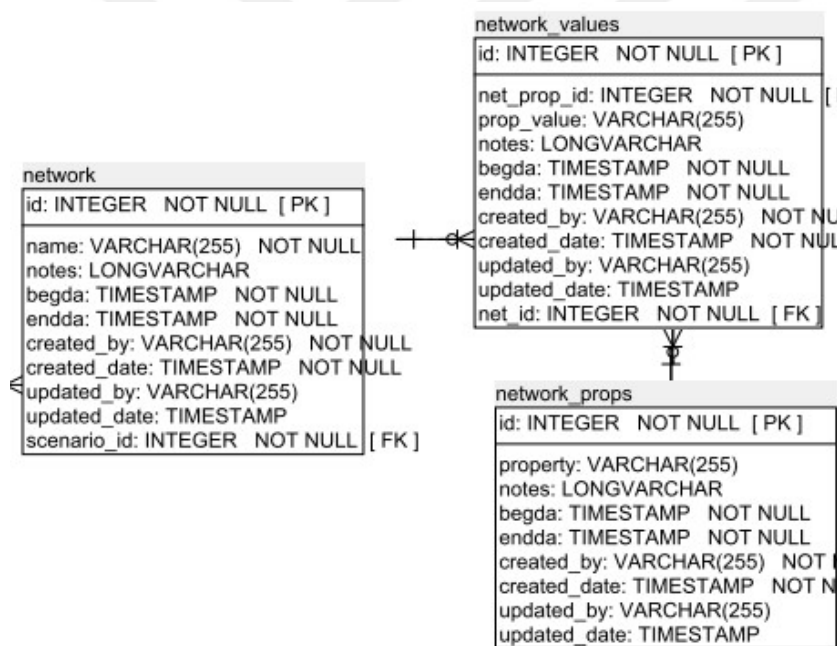


Table 9 Network tables.

5.2.9 Targets

An identified objective, asset can be referenced by nodes and defined with team dependence. This way each team has its own targets. This element contains such information like id, scenario_id, node_id, team_id, and descriptions.

targets	
id:	INTEGER NOT NULL [PK]
scenario_id:	INTEGER NOT NULL [FK]
node_id:	INTEGER NOT NULL [FK]
team_id:	INTEGER NOT NULL [FK]
short_desc:	VARCHAR(255) NOT NULL
notes:	LONGVARCHAR NOT NULL
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP

Table 10 Targets table.

5.2.10 Intelligence

Intelligence table uses for to define any knowledge, condition information of things for scenario and targets. This element contains such information like id, scenario_id, target_id and sense.

intelligence	
id:	INTEGER NOT NULL [PK]
scenario_id:	INTEGER NOT NULL [FK]
target_id:	INTEGER NOT NULL [FK]
sense:	LONGVARCHAR NOT NULL
notes:	LONGVARCHAR NOT NULL
begda:	TIMESTAMP NOT NULL
endda:	TIMESTAMP NOT NULL
created_by:	VARCHAR(255) NOT NULL
created_date:	TIMESTAMP NOT NULL
updated_by:	VARCHAR(255)
updated_date:	TIMESTAMP

Table 11 Intelligence table.

Finally, it can be said, for supporting properties 5.1.1 traceable and 5.1.2 rewind&replay, 5.1.4 measurable, in this database every table has fixed 7 columns as;

- Beginning time,

- Ending time; these columns provide a time scale for the scenarios items. Instead of deleting, changing any row, limiting it with an ending time, and a new row starts with beginning time. The last row's ending time of the default value is infinity.

- Created date,

- Created by,

- Updated date,

- Updated by; these columns provide answers for who and when question for scenarios items.

- Notes; this column provides any extra note, or definition for scenario items.

Most known data types attack type, phases, teams, etc. values are shown in Appendix-2.

5.3 Test Scenarios Employed in IWSIM

5.3.1 Estonian DDOS Attacks

The Estonia cyber war was one of the first cyberwarfare ever conducted. After some political disagreements, Estonia's e-government backbone X-Road [39] came to be under cyber-attacks. In these attacks a lot of DDOS, DOS and Spam emails which carried political messages were used [40], [41].

In our case, a reduced implementation of the X-Road system was prepared on IWSIM and DDOS attacks were carried out. This simulation was tested to discover if it was possible to maintain services that are not under attack but still connected to X-Road during the attacks. The results showed that, without any compartmentalization on X-Road, it was impossible to maintain continuation of the systems that were connected to X-Road.

5.3.2 Operation Aurora

Another incident called Operation Aurora which was conducted on Google in 2009 [42], [43], is yet another cyber-attack simulated in IWSIM. Operation Aurora can be considered as an example of an APT as it was exploiting a zero-day vulnerability of Internet Explorer as well as heavily involved with social engineering applications.

In this scenario, whether these kinds of espionage incidents could be detected during the actual attack taking place was tested. For implementation of this scenario, a Metasploit module Meterpreter was scripted and the traces of a reverse shell command and control technique were searched. The results of this scenario showed that this attack could be detected if MDSN (multi cast) packets were analyzed.

5.3.3 Turkish Baku-Tbilisi-Ceyhan (BTC) Pipeline

After the explosion of a pipeline near the town of Refahiye in Turkey on August 6th, 2008, there was some speculative news about whether this incident was a cyber-attack [44]. There were no official reports stating that it was, however, most experts believed that it was an attack which was somewhat similar to that of the Stuxnet [45]. Resources stated that the attack had been conducted on a carelessly configured IP camera system and privilege escalation had been done on XP Windows Operating System running on Industrial Control Systems (ICS) of the pipeline.

For this scenario, an ICS was implemented through IWSIM's critical infrastructure module and it was possible with Metasploit to exploit XP Windows Operating System using many of the vulnerabilities XP OS had at the time. However, as there is no official analysis made available, the simulation did not lead to any comparative results.

6 CHAPTER SIX

CONCLUSION

As we live in 4th/5th generation warfare era, need for robust simulations for cyber security is an indisputable fact. A matured scenario db model for CO simulations has not been described in a standard model yet. Academic and industrial research has been going on. In this thesis a CO scenario model is constructed, but not claimed as a fully matured one. However, the elements of the scenario database described above might be satisfied by many types of simulation models.

In this thesis; previous research and studies have been reviewed as a first step. Secondly, basic terms on cyber, cyber space, cyberwarfare, cyber operations and their principles were reviewed. Then a generalized look into existing simulation models and our simulation project IWSIM were created. Finally, information received from previous studies and experienced in IWSIM, presented as a scenario model which can be used in cyber operation simulations.

This study does not present a fully new proposal on this area, however, it combines many previous studies and experiences of IWSIM. The proposed scenario database model comprises 17 info types as primitive and 3 info type for network as optional. The future considerations for this project will be transferring the IWSIM experiences to the new project “Proactive Cyber Defense Framework” which has been established at Yaşar University and optimize this scenario model for future works.

REFERENCES

- 1 Colonel T. X. Hammes** USMC, R. Fourth generation warfare evolves, Fifth emerges Military Review; May/Jun2007, Vol. 87 Issue 3, p14
- 2 U.S. Joint Publication 3-12 (R)** Cyberspace Operations U.S. Department of Defense, 5 February 2013
- 3 Michael Warner**, The Cyber Defense Review, 27August 2015, “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014”
- 4 Fred Schreier**, On Cyberwarfare, DCAF publications, 2015
- 5 Lewis, J.** Cyberwar Thresholds and Effects IEEE Security Privacy, 2011, 9, 23-29
- 6 Parks, R. & Duggan D.**, Principles of Cyberwarfare, Security Privacy, IEEE, Vol. 9, pp. 30-35, 2011
- 7 Liles, S.; Rogers, M.; Dietz, J. & Larson, D.**, Applying traditional military principles to cyber warfare Cyber Conflict (CYCON), 2012 4th International Conference on, 2012, 1-12
- 8 Zeadally, S. & Flowers, A.**, Cyberwar: The What, When, Why, and How [Commentary] Technology and Society Magazine, IEEE, 2014, 33, 14-21
- 9 Hamilton, S. N. & Hamilton, W. L. Jajodia, S.; Samarati, P. & Cimoto, S. (Eds.)**, Adversary Modeling and Simulation in Cyber Warfare. SEC, Springer, 2008, 278, 461-475
- 10 Eung Ki Park Joo Beom Yun1, H. P. I.**, Simulating Cyber-Intrusion Using Ordered UML Model-Based Scenarios D.-K. Baik (Ed.): AsiaSim 2004, LNAI 3398, pp. 643-651, 2005., 2004

11 Eom, J.-H.; Han, Y.-J. & Chung, T.-M. Min, G.; Martino, B. D.; Yang, L. T.; Guo, M. & Runger, G. (Eds.), Modeling Active Cyber Attack for Network Vulnerability Assessment. ISPA Workshops, Springer, 2006, 4331, 971-980

12 Skopik, F.; Ma, Z.; Smith, P. & Bleier, T. Aschenbruck, N.; Martini, P.; Meier, M. & Tolle, J. (Eds.) Designing a Cyber Attack Information System for National Situational Awareness. Future Security, Springer, 2012, 318, 277-288

13 Ott, A.; Moir, A. & Rickard, J. T. Yager, R. R.; Reformat, M. Z. & Alajlan, N. (Eds.), A Game Theoretic Engine for Cyber Warfare. Intelligent Methods for Cyber Warfare, Springer, 2015, 563, 219-237

14 Nagarajan, A.; Allbeck, J.; Sood, A. & Janssen, T., Exploring game design for cybersecurity training Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on, 2012, 256-262

15 Wood, B. J. & Duggan, R. A., Red Teaming of advanced information assurance concepts DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings, 2000, 2, 112-118 vol.2

16 Cybersecurity Kill Chain <http://cyber.leidos.com/solutions/cyber-kill-chain>

17 M.E.Kuhl, M.Sudit, J.Kistner, K.Costantini, Cyber Attack Modeling and Simulation for Network Security Analysis, Winter Simulation Conference, 2007

18 Gibson, W., Neuromancer: Roman Heyne, 1984

19 U.S. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms U.S. Department of Defense, 8 November 2010 (As Amended Through 15 February 2016)

20 Ottis, R. L. P., 2010. Cyberspace: Definition and Implications. Dayton, Ohio, USA, Academic Publishing Ltd., pp. 267-270.

21 Clarke, Richard A. & Knake, R. K., Cyber war: the next threat to national security and what to do about it Ecco, 2010

22 JP 1, Doctrine for the Armed Forces of the US. 25 March 2013

23 Matthijs Veenendaal Kadri Kaska Pascal Brangetto, Cyber Policy Brief, Is NATO Ready to Cross the Rubicon on Cyber Defence? NATO CCDCOE Tallinn, June 2016

24 A. Koltuksuz, "Use of Cyberspace and Technology by Terrorists," *Technological Dimensions of Defence Against Terrorism*, vol. 115, p. 106, 2013.

25 Bryan K. Fite, Simulating Cyber Operations: A Cyber Security Training Framework, SANS Institute Reading Room, February 11, 2014

26 <http://sge.bilgem.tubitak.gov.tr/en/cozumler/cyber-security-simulation-and-competition-environment>

27 "Metasploit." [Online]. Available: <http://www.metasploit.com/>. [Accessed:30-Dec-2015].

28"NS3." [Online]. Available: <https://www.nsnam.org/>.

29Ettercap.github.io, "Ettercap Home Page," 2015. [Online]. Available: <https://ettercap.github.io/ettercap/>. [Accessed: 30-Dec-2015].

30Wireshark.org, "Wireshark," 2015. [Online]. Available: <https://www.wireshark.org/>. [Accessed: 30-Dec-2015].

31Help.ubuntu.com, “Firewall,” 2015. [Online]. Available: <https://help.ubuntu.com/12.04/serverguide/firewall.html>. [Accessed: 30-Dec-2015].

32Nmap.org, “Nmap: The Network Mapper - Free Security Scanner,” 2015. [Online]. Available: <https://nmap.org/>. [Accessed: 30-Dec-2015].

33Netcat.sourceforge.net, “The GNU Netcat -- Official homepage,” 2015. [Online]. Available: <http://netcat.sourceforge.net/>. [Accessed: 30-Dec-2015].

34Inetsim.org, “INetSim: Internet Services Simulation Suite - Project Homepage,” 2015. [Online]. Available: <http://www.inetsim.org/>. [Accessed: 30-Dec-2015].

35Hping.org, “hping security tool - man page,” 2015. [Online]. Available: <http://www.hping.org/manpage.html>. [Accessed: 30-Dec-2015].

36Linux.die.net, “sshpas(1) - Linux man page,” 2015. [Online]. Available: <http://linux.die.net/man/1/sshpas>. [Accessed: 30-Dec-2015].

37Scadahoneynet.sourceforge.net, “SCADA HoneyNet Project: Building Honeypots for Industrial Networks,” 2015. [Online]. Available: <http://scadahoneynet.sourceforge.net/>. [Accessed: 30-Dec-2015].

38 Linux.die.net, “scp(1): secure copy - Linux man page,” 2015. [Online]. Available: <http://linux.die.net/man/1/scp>. [Accessed: 30-Dec-2015].

39 CYBERNATICA, “X-Road A secure data exchange layer for building eGovernments”, Technical Whitepaper” 2014.

40J. Nazario, “DDoS Attack Evolution,” Journals Netw. Secur., vol. 2008, no. 2, pp. 7–10, 2008.

41J. Nazario, “Politically Motivated Denials of Service Attacks,” Virtual Battlef. Perspect. Cyber Warf., pp. 163–181, 2009.

42Damballa, “The Command Structure of the Aurora Botnet”, 2010.

43R. Varma, “McAfee Labs: Combating Aurora.”

44Jordan Robertson and Michael Riley, “Mysterious 2008 Turkey Pipeline Blast Opened New Cyberwar” Bloomberg.com, 2014. [Online]. Available: <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>. [Accessed: 30-Dec-2015].

45R. M. Lee, M. J. Assante, T. Conway, “Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack” SANS ICS Defense Use Case (DUC) Dec 20, 2014.



CURRICULUM VITEA

Kemal YILDIRIM

Gaziemir, İZMİR

Phone: 535-9777457

kemal.yildirim.tr@hotmail.com

Education:

OBI Course, International Computer Institute, Ege University, 2000

Electronic Eng., Air Force Academy, Yeşilyurt, İstanbul, 1994

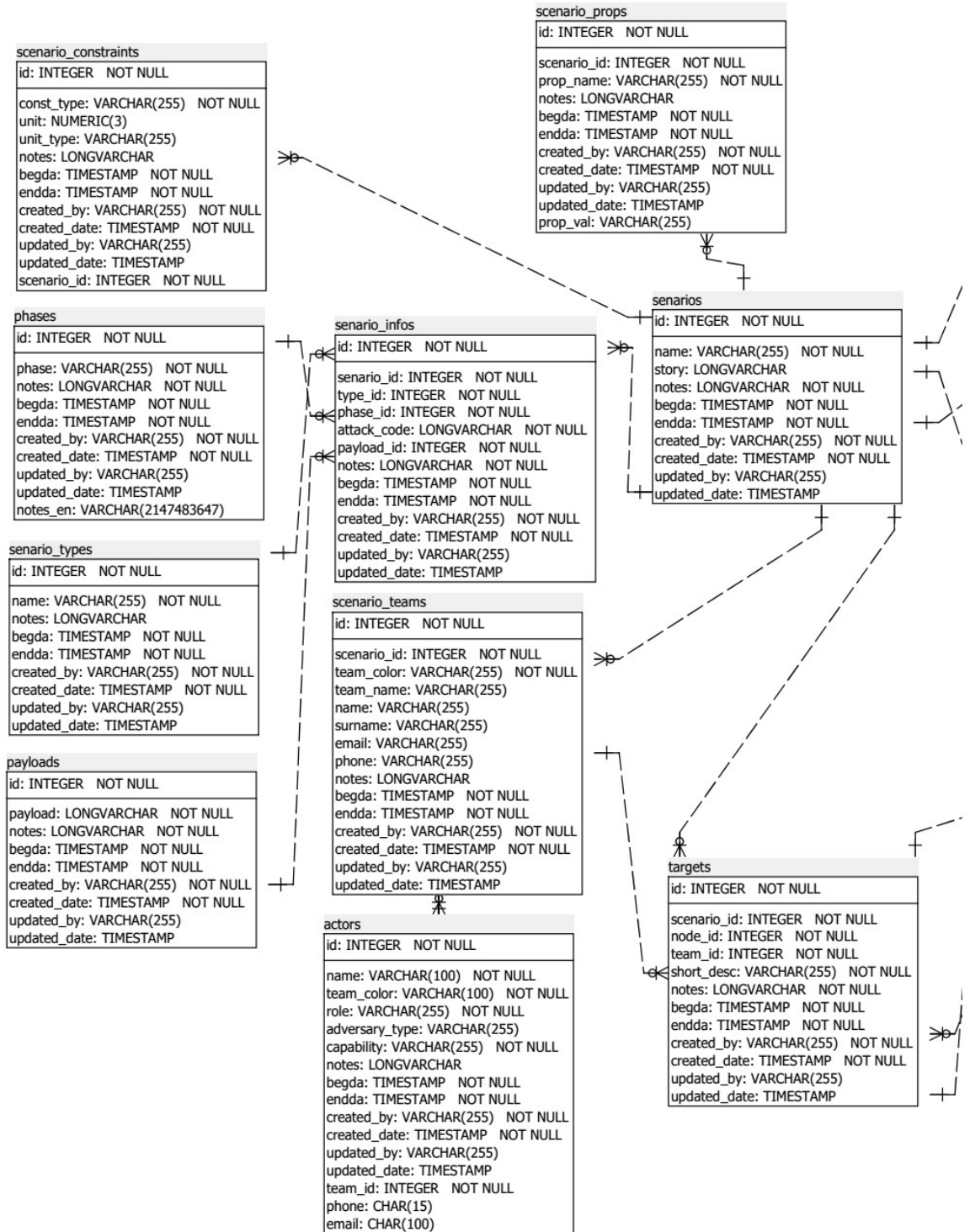
Employment History:

1994-1999 Information Systems Officer

2000-2012 Information Systems Project Officer

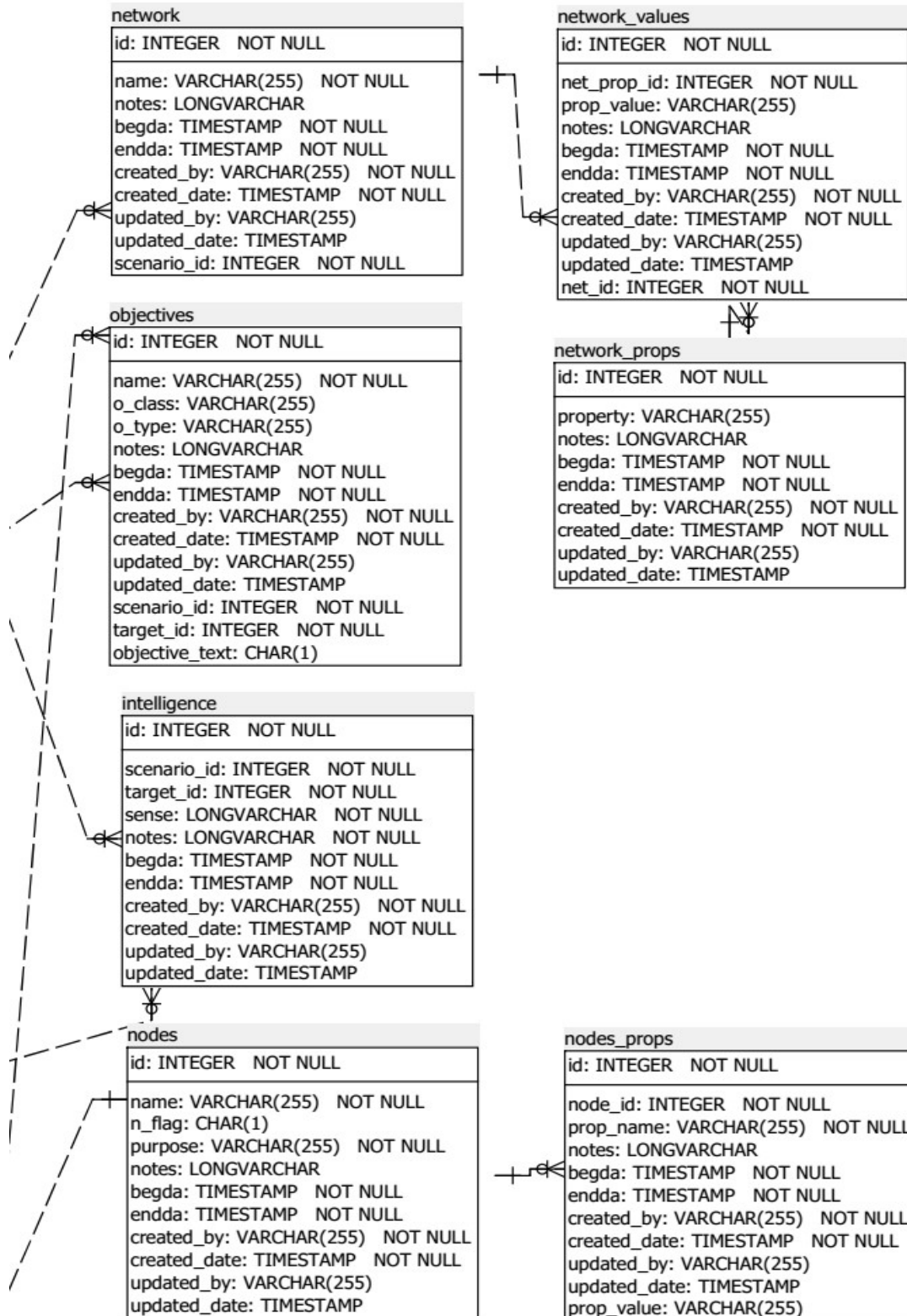
2012- Information Systems Training Supervisor

APPENDIX 1 CO SCENARIO DB SCHEMA (ER) DIAGRAM



APPENDIX 1 CO SCENARIO DB SCHEMA (ER) DIAGRAM

(cont.)



APPENDIX 2 CO SCENARIO DB SAMPLE VALUES

Table Phases

(Typical hacker actions in a cyber-attack)[17]

Phase_Id	Phase
0	Recon. Foot printing
1	Intrusion User
2	Escalation Service
3	Intrusion Root
4	Goal Denial of Service
5	Recon. Enumeration
6	Intrusion User
7	Escalation Service
8	Intrusion Root
9	Goal Pilfering

Objectives[13]

Blue player objective functions:

- Preserve availability: Adds points for each host under supervision if the host is up and working properly.
- Investigate suspicious activity: Adds points for states that provide information about a host that has gone down or is non-functional, even if it isn't fixed.
- DoS defense: Adds points for maneuvers to stop a denial of service, such as blocking IP addresses, ports, or applying patches.
- Worm defense: Adds points for applying patches; deducts points for non-critical ports being open, deducts points for each host infected
- Submit weekly report: Adds points for successfully uploading data to a database on a weekly basis
- Minimize work: Deducts points for executing moves that utilize administrator time/energy

Red player objective functions;

- Corrupt database: Adds points for modifying data on any database
- Corrupt web server: Adds points for modifying data on any web server

- Cover tracks: Adds points for removing log entries, software installations, etc. that result from an attack and could lead to being caught
- DoS host: Adds points for preventing network access to any host
- Gain server root account: Adds points for obtaining a username/password on a server
- Minimize risk: Deducts points for executing moves that have risk
- Poison DNS: Adds points for modifying host files to point to one of your own servers
- Remote reconnaissance: Adds points for mapping an opponent's network and determining what services and vulnerabilities are there
- Setup bots: Adds points for getting root privileges on remote machines
- Steal data: Adds points for exfiltration data from any host
- Steal server data: Adds points for exfiltration data from any server