



YAŞAR UNIVERSITY
GRADUATE SCHOOL

MASTER OF SCIENCE THESIS

**INJECTION DEVELOPMENT FOR CYBER WARFARE
EXERCISES**

CAN BERK HAYRETDAG

THESIS ADVISOR: ASSOC. PROF.(PHD) AHMET KOLTUKSUZ

COMPUTER ENGINEERING

PRESENTATION DATE: 06.06.2022

BORNOVA / İZMİR
JUNE 2022

We certify that, as the jury, 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. (PhD) Ahmet H. Koltuksuz
Yaşar University

.....

Prof. (PhD) M. Cudi Okur
Yaşar University

.....

Assist. Prof. (PhD) İbrahim Zincir
İzmir University of Economics

.....



Prof. (PhD) Yücel Öztürkoğlu
Director of the Graduate School

ABSTRACT

INJECTION DEVELOPMENT FOR CYBER WARFARE EXERCISES

Hayretdağ, Can Berk

MSc of Science, Computer Engineering

Advisor: Assoc. Prof. (PhD) Ahmet Koltuksuz

June 2022

In the last years, with the development of computer systems, there has been an incredible increase in cyber attacks. For this reason, countries and organizations began to feel the need to prepare themselves for this new war front. This study focuses on preparing cyber warfare exercises, the best way to compose an organization for a cyber attack. Furthermore, the thesis contributes to the standardization of injection scenarios, one of the essential components, with a case study.

keywords: cyber security, cyber warfare, cyber warfare exercise, information security, red teaming

ÖZ

SİBER SAVAŞ EGZERSİZLERİ İÇİN ENJEKSİYON GELİŞTİRİLMESİ

Hayretdağ, Can Berk

Yüksek Lisans Tezi, Bilgisayar Mühendisliği

Danışman: Doç. Dr. Ahmet Koltuksuz

Haziran 2022


Son yıllarda bilgisayar sistemlerinin gelişmesiyle birlikte siber saldırıların sayısında inanılmaz bir artış oldu. Bu sebeple ülkeler ve kurumlar kendini bu yeni savaş cephesine hazırlama ihtiyacı duymaya başladılar. Bu çalışma bir kurumu siber saldırıya hazırlamanın en iyi yolu olan siber savaş egzersizlerinin nasıl hazırlanması gerektiğine yoğunlaşır. Bunu yaparken, tez, en önemli yapılardan biri olan enjeksiyon senaryolarının standartlaştırılmasına örnek bir çalışma ile katkıda bulunur.

Anahtar Kelimeler: siber güvenlik, siber savaş, siber savaş egzersizi, bilgi güvenliği, kırmızı takım

ACKNOWLEDGEMENTS

I would like to acknowledge and give my warmest thanks to my supervisor Assoc.Prof. (PhD) Ahmet Koltuksuz who made this work possible. His guidance and advice carried me through all the stages of writing my project. I would also like to thank my committee members for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

I would also like to give special thanks to my family as a whole for their continuous support and understanding when undertaking my research and writing my project.



Can Berk Hayretdağ
İzmir, 2022

TEXT OF OATH

I declare and honestly confirm that my study, titled “INJECTION DEVELOPMENT FOR CYBER WARFARE EXERCISES” and presented as a Master’s Thesis, has been written without applying 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.

Can Berk Hayretdağ

June 06th, 2022



TABLE OF CONTENTS

ABSTRACT.....	V
ÖZ	VII
ACKNOWLEDGEMENTS	IX
TEXT OF OATH	XI
TABLE OF CONTENTS.....	XIII
LIST OF FIGURES	XV
LIST OF TABLES	XVI
CHAPTER 1 INTRODUCTION	1
1.1. Scope.....	2
1.2. Motivation and Aim.....	2
1.3. This Work's Novelty	3
CHAPTER 2 LITERATURE SURVEY.....	5
2.1. Information Security & Cyber Warfare.....	5
2.2. Cyber Threat Intelligence	7
2.3. Red Team Methodology	8
2.4. Cyber Kill Chain.....	13
2.5. Vulnerabilities & Threats	14
CHAPTER 3 CYBER WARFARE EXERCISES	23
3.1. Definition.....	24
3.2. Types.....	25
3.2.1 Table-Top	25
3.2.2. Hybrid	25
3.2.3. Full Live.....	26
3.3. Development Steps	26
3.3.1 Exercise Planning	26
3.3.1.1. Objectives	26
3.3.1.2. Exercise Type	27
3.3.1.3. Teams.....	27
3.3.1.4. Scenarios.....	28

3.3.1.5. Outcomes.....	28
3.3.1.6. Other Components: Location, Resources, Scoring	29
3.3.2. Exercise Execution	29
3.3.2.1. Information Management	29
3.3.2.2. Daily Review.....	30
3.3.3. Post Exercise	30
3.4. Examples from Around the World: NATO, USA, and Europe.....	31
3.4.1. Locked Shields: NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)	31
3.4.2. Cyber Storm: Department of Homeland Security, USA	32
3.4.3. Cyber Europe: ENISA	33
CHAPTER 4 DEVELOPING SCENARIOS & INJECTIONS.....	35
4.1. Definition.....	35
4.2. Developing Injections: Scenarios & Attack Techniques.....	35
4.3. Example Injections	36
4.3.1. MITRE Perspective.....	37
4.3.2. Locked Shields.....	37
CHAPTER 5 SAMPLE CYBER EXERCISE.....	39
5.1. Background Information	39
5.2. Exercise Target Group.....	40
5.3. Exercise Objectives	40
5.4. Exercise Expected Outcomes	41
5.5. Exercise Events: Master Event list (MEL).....	41
5.6. Exercise Injections – Master Injection List (MIL).....	42
5.7. MEL-MIL-Objective-Outcome Matrix	43
5.8. Master Scenario Event List (MSEL) Table.....	44
5.9. Exercise Hybrid Network Topology	46
5.10. Software Tools to be Utilized.....	47
5.11. Exercise Environment	47
CHAPTER 6 DISCUSSION, CONCLUSION AND FUTURE WORK	49
6.1. Discussion	49
6.2. Conclusion.....	49
6.3. Future Work	50
REFERENCES	51

LIST OF FIGURES

Figure 3.1. Exercise Information Flow	30
Figure 4.1. Cyber Kill Chain Model	38
Figure 5.1. Cyber Exercise Topology	46
Figure 5.2. The Teams layout	48



LIST OF TABLES

Table 5.1. Objectives of the Cyber Exercise..... 40

Table 5.2. The Expected Outcomes of the Cyber Exercise 41

Table 5.3. The Event List of the Cyber Exercise 42

Table 5.4. MEL-MIL-Objective-Outcome Matrix..... 43

Table 5.5. MSEL Table of the Cyber Exercise - Day-1 45

Table 5.6. MSEL Table of the Cyber Exercise – Day-2 45

Table 5.7. The Software Tools..... 47





CHAPTER 1

INTRODUCTION

In the last years, with the born of the term "Cyber Terrorism," the cyber world has become a warfare area because of the competition between nations, organizations, and threat groups. This competition's destructive power is constantly increasing because threat groups rapidly improve their capabilities daily, so cyber attacks have become more complicated to understand for security engineers and researchers. Therefore nations and organizations need to prepare and enhance the skills and awareness of their security researchers against current cyber threats and trends. Although there are many resources on cyberspace to research, practice is as critical as research, especially for an area such as cyber security. Capture The Flag (CTF), and similar events are the most popular ways to practice and evaluate security researchers' knowledge. However, these competitions are not reciprocal, so they are not enough to simulate realistic cyberwarfare scenarios with perspective attack and defense. Therefore these events are not enough when compared with real-world scenarios. One of the most realistic and important ones is cyber warfare exercises that show participants a cyber warfare simulation with real attack scenarios. The different cyber warfare exercises can be chosen according to the organization's objectives.

There are vital critical points for preparing cyber warfare exercises, such as objectives, outcomes, and injections. Each of these points must be crafted carefully to maintain practical activities and learn from the exercise. The organization may determine objectives according to its expectation from the exercise. These objectives also determine the course of the exercise. Outcomes are another critical point for evaluating an organization's security posture and researchers' awareness. Injections are more technical and related to attack scenarios that participants should apply correctly. However, because the preparation of injections needs technical skills, exercise planners could make some mistakes during the development process. Therefore, if there is a reference to help planners prepare an injection list, they would develop the

injections more accurately.

This thesis aims to research injections that may be called technical attack scenarios according to the story of exercise. Many organizations organized cyber warfare exercises to educate security researchers to simulate realistic cyber incidents. Many different kinds of attack scenarios are used and applied in these exercises. However, there is no standardization work about the preparation of injections when those exercises are investigated. Therefore, this thesis proposes a development model to standardize cyber warfare injections with a sample fictitious scenario-based case study.

1.1. Scope

Investigation of the first part of this research covers a literature review of some security-related topics such as Information Security, Cyber Warfare, Cyber Threat Intelligence, Red Team Methodology, Cyber Kill Chain, Vulnerabilities, and Threats. In today's technology, all these topics are critical to understanding for any organization that wants to build a conscious and robust security posture against current threats.

In the second part of the study, we discussed some points about cyberwarfare exercises, such as the definition of cyber warfare exercises, their types, how to develop an exercise step by step to reach objectives successfully, and we will see different types of examples (Table-Top, Hybrid, and Full Live) based on EUROPA, and the USA with examples from organizations around the world such as Locked Shields (NATO CCDCOE), Cyber Storm (Dept. of Homeland Security, USA), and Cyber Europe (ENISA).

We discussed injections such as definition, injection scenario that contains explanation about writing scenarios, and implementation of attack techniques to these scenarios based on objectives, some example injections proposed by different organizations and used in exercises in the last and central parts of the study. Finally, we present the proposed standard and structure of the model with examples.

1.2. Motivation and Aim

These days, many organizations form their cyber security teams for attack and defense

because most of them are somehow affected by cyber threats. These cyber-attacks teach the importance of the pre-attack phase to organizations. At this point, red team operations come into play to identify weaknesses in the organization's computer systems before they are affected by cyber-attacks. If organizations develop red team operations correctly according to their systems and expectations, they may save themselves from being a piece of cake for threat groups.

This thesis aims to improve a standard model for developing cyber warfare injections to manage red team operations more effectively in cyber exercises. This model quickly implements injections between different kinds of cyber warfare exercises according to their objectives.

1.3. This Work's Novelty

In the last years, researchers and organizations have made many attempts to make some processes measurable and standard in cybersecurity-related areas such as threat enumerations (e.g., CVE, CWE), languages (e.g., OVAL, CVSS), repositories, etc. Most of these attempts were based on threat classification and managing vulnerabilities. However, the novelty of this work is contributing to managing and standardizing red team operations in cyber exercises. Therefore, while organizations prepare their cyber exercises, they can focus on their objectives and outcomes instead of thinking about designing injections.

Organizations in the same work area can also use this standard injection model to create an injection database for their exercises with similar attack scenarios.

CHAPTER 2

LITERATURE SURVEY

2.1. Information Security & Cyber Warfare

2.1.1. On Cyber Warfare

In a digital world, new security considerations appeared for states and organizations with the transfer of information. Therefore, Cyber Security is getting more and more popular every day. Some cases, such as cyber-attacks against Estonia that appeared in the last years, showed that cyber-attacks have become international (Cornish et al., 2010). This situation revealed the terms such as "Cyber War" and "Cyber Warfare." The wars in the virtual world (cyberspace) are different from than traditional world (Cornish et al., 2010). Attackers or threats are not physically there, so they are unidentifiable. There are various types of hazards, such as Direct military threats, Indirect and non-military threats, Terrorism and extremism, Cyber espionage, Economic cyber crime, and Psychological cyber warfare (Cornish et al., 2010). The digital world is developing so fast; therefore, the internet is bigger and more complex than all countries or companies (Cornish et al., 2010). That's why each state must manage its offensive and defensive operations against threats from the internet. These operations may be divided into different fields, such as political and economic (Cornish et al., 2010). Therefore, each state should have a national strategy framework against cyber warfare and fully understand it for national security (Cornish et al., 2010).

2.1.2. Cyberattacks and Cyberterrorism

Cyberattack is one of the most popular terms in information technology. Especially, Stuxnet proved how a cyber attack could be devastating (Theohary & Rollins, 2015). Cyberattacks can be initiated globally as long as there is a connection to the internet. Therefore, the term "Cyber Terrorism," which aims to devastate systems on computer networks with the objectives such as ideological or political, has become popular. According to the goals, there are many types of threat actors, such as Cyberterrorists,

Cyberspies, Cyberthieves, Cyberwarriors, and Cyberactivists in this ecosystem (Theohary & Rollins, 2015). Nevertheless, there are no exact definitions to determine whether a cyber activity is a crime or not (Theohary & Rollins, 2015). And along with that, the uncertainties in descriptions puzzle everybody about whether the strategies against cyberattack & cyberterrorism are effective against cyber threat actors or not.

2.1.3. Cyber Warfare: Issues and Challenges

In the past, there was competition between nations in physical ways. However, today, the battlefield changed to cyberspace. These developments have revealed new terms such as Information Warfare, Cyber Warfare, and Cyber War. The actor and intent definition model provides this methodology (Robinson et al., 2015) to solve definition problems in cyber warfare definitions. In this model, some essential descriptions are cyber attack, intent, actor, cyber event, cyber warfare, and cyberwar (Robinson et al., 2015). Cyber Warfare is a vast and complex topic (Robinson et al., 2015). Thus, to understand it better, the work divides it into nine different research challenges: Early Warning Systems, Ethics of Cyber Warfare, Applying Existing laws to Cyber Warfare, Conducting Cyber Warfare, Cyber Weapons, Attribution Problems, Cyber Defense and Deterrence, Conceptualising Cyber Warfare, Nation's Perspectives (Robinson et al., 2015). These different research areas show that considerations and issues about cyber warfare can not be solved with only one perspective of a research area (Robinson et al., 2015).

2.1.4. Developing a Strategy for Cyber Warfare

With the development of information and communications systems in the last several decades, information security has become a crucial issue for states, especially their armies (Colarik & Janczewski, 2011). Any threat group can damage huge organizations with the possibilities of today's technology. Therefore, states should be ready for cyber wars and criminal activities (Colarik & Janczewski, 2011). According to this paper, each country should have its own Cyber War Doctrine (CWD) (Colarik & Janczewski, 2011). The doctrine is accepted or supported by some principles (Colarik & Janczewski, 2011). CWD is a set of rules which are managed by states able to survive in cyberspace (Colarik & Janczewski, 2011). For establishing CWD, some critical issues and decisions such as Determining the difference between conventional and cyber war, Battle-space determination, Aggression versus response, Victory

conditions, Required assets, and Moderating responses should be made clear (Colarik & Janczewski, 2011). Constructing an effective CWD is not easy, so establishing CWD should be a collaborative and discussion framework managed by government and business professionals (Colarik & Janczewski, 2011).

2.2. CYBER THREAT INTELLIGENCE

2.2.1. Cyber Threat Intelligence: Issues and Challenges

In recent years, preventing cyber-attacks has become difficult because of fast-developing technology and attackers' capabilities, such as sophisticated techniques and tools. Therefore, it is vital to understand cyber threat intelligence; however, there is no standard definition. Before defining cyber threat intelligence, the community should realize cyber-threats are malicious activity (Sahrom Abu et al., 2018). Another point community should know about is intelligence which is information collected from cyber operations. So the definition of cyber threat intelligence is formed by relevance, timeliness, and actionable coming together (Sahrom Abu et al., 2018). An organization can use internal and external sources for threat intelligence (Sahrom Abu et al., 2018). There are also different standards and tools such as STIX, TAXII, CPE, and CCE to share information and provide intelligence between organizations (Sahrom Abu et al., 2018). Organizations can use these tools and standards according to their requirements and objectives. Finally, it is essential to note that organizations need to be careful about Data Overload, Data Quality, Legal Issues, and Interoperability in cyber threat intelligence (Sahrom Abu et al., 2018).

2.2.2. Threat Intelligence: Collecting, Analyzing, and Evaluating

Threat intelligence is a new topic in the information security field, and there are other researches and definitions for it. Threat intelligence is information that helps response teams to understand threats and prevent threats. We can divide threat intelligence into four different parts (i) Strategic (better understand current threats and risks for helping strategists), (ii) Tactical (investigate how hackers attack the organization and which tactics they used), (iii) Operational (operational is essential for mitigation of attacks with actionable information), and (iv) Technical (this part is interested with technical details of attackers used such as tools and technologies) (Chismon & Ruks, 2015). The threat intelligence cycle is a good guide for dividing the process into sophisticated

pieces and following these steps to maintain a successful threat intelligence program (Chismon & Ruks, 2015). In cyber security, attackers do not target just a single organization, so sharing communities is one of the most critical parts of effective threat intelligence programs (Chismon & Ruks, 2015).

2.2.3. Cyber Threat Intelligence Model

Nowadays, organizations are at risk in the cyber world because of cyber threats. At that point, the incident response team of organizations should identify threats at the time of the attack. Threat intelligence is crucial to identify and know dangers, and its sharing standards are also necessary. There are different types of models used by response teams against threats.

DML (Detection Maturity Level) is a model that can understand threats and act according to this information (Mavroeidis & Bromander, 2017). Modified DML consists of four levels: Attacker Identity, Attacker Goals, Attack Execution Plan, and Methods and Traces of Attack Execution (Mavroeidis & Bromander, 2017). Another model is cyber threat intelligence used for sharing standards and taxonomies (Mavroeidis & Bromander, 2017). Taxonomies and sharing standards can be divided into three entities: Enumerations (NVD, CVE, etc.) Scoring Systems (CVSS, CWSS) and Sharing Standards (STIX, MAEC) (Mavroeidis & Bromander, 2017).

2.3. Red Team Methodology

2.3.1. Cyber Red Team

The red team is becoming increasingly popular, especially in cyber exercises and games. The blue team should be tested first to test the defense of computer and network systems, and that's why a red team is essential for cyber security. To conduct and construct a red teaming framework, firstly, the definition of the red team should be understood by the organization then activities should be transparent. Three attributes are critical such as design, development, and execution.

To provide efficiency in red teaming, the question should be, "how the system fails". Testing network systems only are not enough, and in addition to network and application, the human factor should also be tested by the red team. The cyber red team provides a better understanding of adversaries and their methodologies. While applying red team operations, another important consideration is legal implications

(Brangetto et al., 2015). Therefore red teaming framework should be constructed based on national laws (Brangetto et al., 2015).

2.3.2. A Guide to Red Teaming

There are various definitions of red teaming. Red teaming is a function or tool with many purposes, such as identifying weaknesses and threats (Development, Concepts and Doctrine Centre, 2010). It also provides alternative perspectives to commanders or leaders with outputs (Development, Concepts and Doctrine Centre, 2010). There are four steps for using a red team in defense: set red team objectives, plan outputs usage, identify red team problems, and choose the right red team (Development, Concepts and Doctrine Centre, 2010). The fundamental principles are learning culture, commanders' engagement, independence, output-oriented, interaction, timeliness, and staff to construct an effective red teaming (Development, Concepts and Doctrine Centre, 2010).

Red teaming input is also crucial to effectively plan (Development, Concepts and Doctrine Centre, 2010). Red team members must be selected for sophisticated areas and objectives. The main aim of the red team should be clear to provide practical outputs. Each point in red teaming is too critical to the defense of any government or organization to find vulnerabilities in the system before attackers find them.

2.3.3. Information Security Testing and Assessment

In information security, determining how secure an object is is called assessment consisting of three method types: testing, examination, and interviewing (Scarfone et al., 2008). These methods can consist of three steps: planning, execution, and post-execution (Scarfone et al., 2008). Different types of techniques can be used for assessment, such as review (documentation review, log review, network sniffing, etc.), target identification and analysis (wireless scanning, network discovery, etc.), target vulnerability validation (password cracking, social engineering, etc.). Still, there are also non-technical techniques (Scarfone et al., 2008). These assessments may apply with a different perspective as black-box (external, internal) or white-box (Scarfone et al., 2008). To conduct these assessments, entities, planning effectively, and policy are essential, and they should be repeatable and precise (Scarfone et al., 2008). After all of these, organizations need to analyze the result and report them for mitigation (Scarfone et al., 2008).

2.3.4. Penetration Testing Tools and Approaches

With the rapid development of Information technology, systems have become more critical for organizations. These developments arise many doors for adversaries to attack the organizations. At that point, penetration testing comes into play to determine how secure the system is. There are different types of penetration testing, such as network penetration testing, application penetration testing, and physical penetration testing (Chiem, 2014). As a model, two types of model exist, such as flaw hypothesis and attack tree (Chiem, 2014). There are also different types of methodologies based on the environment. In addition, there are various types of tools, many of which are open-source tools, such as *Nmap* and *Metasploit*. There are two phases of penetration testing: Selecting and utilizing pre-selected penetration testing tools and deployment of attacks. Organizations should apply penetration tests periodically to find security flaws and patch them before adversaries attack their systems.

2.3.5. A Threat-Driven Approach to Cyber Security

In cyber security, combating threats is the main focus of most organizations with some frameworks or policies, such as Kill Chain Intelligence Driven Defense, but there are some limitations (Muckin & Fitch, 2015). Another methodology or framework is the threat-driven approach that guides organizations (Muckin & Fitch, 2015). The architecture-engineering and operating-managing sections are fully isolated in traditional frameworks (Muckin & Fitch, 2015). However, in a threat-driven approach, they are integrated and a combination of methodologies: IDDIL and Intelligence Driven Defense (Muckin & Fitch, 2015).

There are different tools for maintaining this model effectively, such as Threat Categorization table, Functional Controls Hierarchy, Controls Effectiveness Matrix and Scorecard, Intelligence Management System, Architectural Renderings (Muckin & Fitch, 2015). In addition, this architecture helps the information security practices for risk management and lifecycle (Muckin & Fitch, 2015).

2.3.6. Network Security: Attacks, Tools, and Techniques

One of the most critical issues for security engineers is network security because tons of information is transferred through these networks. The primary purpose of protection is to guarantee information's integrity, confidentiality, and availability. To

be able to provide this security, organizations should have a methodology. There are different network attacks such as security threats, virus attacks, unauthorized access, information theft and cryptography attacks, unauthorized application installations, and application-level attacks (Ritu Sindhu, 2015).

Protecting the network is not easy, so the network should be scanned periodically to detect any suspicious situations, such as unnecessary ports or user shares. There are also some tips to increase network security, such as turning off ping service, closing unused ports, binding IP to MAC address, use intrusion detection systems (Ritu Sindhu, 2015).

2.3.7. Network Attacks: Taxonomy, Tools, and Systems

Since most of the work done is over computer networks, tons of network attacks happen each day in today's technology. These attacks can be in different forms, such as trojan and DDoS, and consist of four-step such as information gathering, assessing vulnerability, launching an attack, and cleaning up (Hoque et al., 2014). Each step also has many techniques and tools (Hoque et al., 2014).

The threats should be understood clearly, and the system should be monitored constantly to detect the attacks. However, it is hard to detect and prevent high-level and complex attacks. At that point, there are many network tools for both red teams and blue teams to provide detection and monitoring networks. These tools can be divided into three attack launching (Trojans, DDoS, Packet Forging, Application Layer Attack, Fingerprinting, User Attack, Others), information gathering (Sniffing, Network Mapping), network monitoring (Visualization and Analysis) (Hoque et al., 2014). Each tool has different features from others; therefore, this tool taxonomy helps security teams to choose tools and combine them (Hoque et al., 2014).

2.3.8. Remote Exploit Development for Cyber Red Team

Cyberattacks that have been seen in the last years showed that traditional borders are not crucial as in old times. These complex and sophisticated attacks proved that physical limitations are just numbers now. One of the critical infrastructure systems in industrial control systems is a vital target for cyber attacks. Different attacks can be applied to SCADA systems; therefore, the red team should simulate these attacks like adversaries. Red team's scenarios should be as complicated as APTs and be realistic in cyber exercises. There are many examples of these attack scenarios, such as

PROFINET IO RT Command Injection Attack, IEC-104 Command Injection Attack, TELEM-GW6/GWM Control Takeover (Blumbergs, 2019). There are many points to be careful of protection from attacks: secure VPN connections, software updates, firewalls, and password policy are some of them. The red team operations should be applied periodically to check these points (Blumbergs, 2019).

2.3.9. Stuxnet and Strategy

Stuxnet was one of the most sophisticated and devastating cyber attacks in the current century. It was a computer worm created by the USA to disrupt the nuclear infrastructure of Iran on Windows computers and Siemens devices. Attack also affected computers in others countries and cost tons of money. It also increased the security considerations of other countries for their critical infrastructures.

In today's cold war, cyberwar, cyber power is an effective tool and can be used for information gathering, affecting morale, cyber attack, and disrupting an enemy's infrastructure (Milevski, 2011). Although it has strategic limitations, with the use of zero-days, hid and attacked by itself (Milevski, 2011). Stuxnet was utterly different from traditional cyberattacks, whether successful or not. However, adversaries show adversaries how sophisticated and advanced attacks can be created. Therefore, nations and organizations need to learn new lessons from Stuxnet to minimize their security considerations.

2.3.10. Double Dragon APT41 Report

APT41 is a hacker group from China, and they are popular with sophisticated espionage operations. They are targeting a different types of sectors such as video games (studios and distributors in East and Southeast Asia), media, healthcare (medical device companies and pharmaceuticals), and telecoms from different countries for stealing sensitive information and espionage (FireEye, 2020). Another thing observed about APT41 is consistent with China's national strategies and benefits (FireEye, 2020). APT41's attack life-cycle steps are Initial Compromise, Establish Foothold, Escalate Privilege, Maintain Presence, Internal Reconnaissance, Move Laterally, Complete Mission (FireEye, 2020).

When their tactics are examined from MITRE ATT&CK's perspective, the group uses many techniques in each tactic. They also use any malware for Linux and Windows operating systems.

2.4. Cyber Kill Chain

2.4.1. Technical Aspects of Cyber Kill Chain

Nowadays, with the unbelievable development of the Cyber world, the number of threats and hackers has also increased. Therefore, Cyber attacks and tools have become more complicated.

Cyber Kill Chain is a model based on phases of cyberattacks. It provides Cyber Security Analysts to model and breaks down cyber attacks into small steps for better understanding and analysis (Yadav & Rao, 2015).

The Cyber Kill Chain has seven phases: Reconnaissance, Weaponize, Delivery, Exploitation, Installation, Command & Control, and Act on Objective (Lockheed Martin). Reconnaissance is the first step in collecting information about the target. This step can be divided into two types Passive and Active. In the Weaponize step, the attacker creates some tools for remote access and makes a plan to penetrate the system. One of the essential steps is Delivery. In this step, the attacker interacts with the target to deliver their weapon to the target system. The next step is Exploitation which runs the malicious payload of the attacker. The installation step is another step which is installing a backdoor to the target system for persistence. The next step is Command and Control, which provides the attacker to execute instructions remotely. The final step is to Act on the Objective, and the attacker applies their primary objectives. It may be stealing credentials, DDOS, or data exfiltration.

2.4.2. Intelligence-Driven Computer Network Defense

As computer networks expand, threats against networks also increase. Unfortunately, in recent years, traditional methods to prevent network threats can not be successful against more sophisticated attacks such as Advanced Persistent Threats (APT).

Intelligence-driven Computer Network Defense is based on an indicator that is any information about intrusions (Hutchins et al., 2010). These indicators are analyzed according to their corresponding indicator states in the indicator life cycle (Hutchins et al., 2010). This paper handles the kill chain based on intrusions with the Intrusion Kill Chain (Hutchins et al., 2010). The Courses of Action Matrix is utilized to understand the adversary (Hutchins et al., 2010). In this matrix, each kill chain phase is analyzed based on actions such as Detect, Deny, Disrupt, Degrade, Deceive and

Destroy (Hutchins et al., 2010). Another essential point is intrusion reconstruction which provides defenders to see if the adversary was successful and how the attack would continue (Hutchins et al., 2010). Defenders should collect information from adversaries about the later phases of the kill chain (Hutchins et al., 2010). Analyzing many intrusions, defenders can determine common indicators and intents of adversaries with Campaign Analysis (Hutchins et al., 2010). Furthermore, with campaign analysis, defenders can improve their capabilities according to attack patterns and behaviors of adversaries (Hutchins et al., 2010).

2.5. Vulnerabilities & Threats

2.5.1. Analysis of Network Security Threats and Vulnerabilities

With the unpredictable growth of computer networks, threats have increased with this rate. This development revealed the security considerations about information that is transported on networks. There is no exact definition of network threat, but it protects networks from unauthorized access. There are different types of network attacks, such as interruption, interception, modification, and fabrication; however, they can also be divided into functional (data changes) and passive attacks (there is not any data change) (Ahmad & Habib, 2010).

To protect the network, network administrators need to follow security trends and current vulnerabilities in their technologies. There are also key points to be considered, such as cryptography, application-layer security (Authentication Level, Email Level, IP Level, Web Level), and system-level solutions (IDS, IPS, Antivirus, Firewalls) (Ahmad & Habib, 2010). Finally, reports and attack simulations are essential for seeing the effects of cyber attacks.

2.5.2. The Phishing Attack Techniques

Phishing is one of the oldest terms in information security. Attackers send an email to victims with malicious intent, such as stealing sensitive information such as SSN, address, passwords, or bank transactions without the victim's intention. Phishing can be divided into social engineering and technical subterfuge (Chawla & Chouhan, 2014). Basically, in phishing attacks, there are four steps firstly, the attacker creates a fake website that looks realistic; the second step is sending an email to the victim. In the third step, the victim clicks the link, opens the website, and enters the required

information. The final step is stealing the information of the victim. There are three entities in the life cycle of phishing email transfer: Message Transfer Agent, Message Delivery Agents, and Mail User Agent (Chawla & Chouhan, 2014). Some detection methods should be used to protect users from phishing, such as filtering.

2.5.3. An Example for an Attack and Defense: Linux Privilege Escalation Technique

Privilege escalation is a vulnerability that provides attackers reach access more than regular users. It is also a step in attacker methodology in models such as cyber kill chain. Especially, Linux privilege escalation is significant for the infrastructure of organizations such as web servers and databases.

Different privilege escalation attacks are used: kernel exploits, weak services, and physical access attacks (Long, 2016). Kernel bugs provide to attackers run malicious codes in the system, and the attacker can get access to the root (Long, 2016). Another method is weak services, and the attacker can find an inadequate Linux service in the system and exploit them (Long, 2016). Finally, physical access is a critical attack, and an attacker can easily disrupt the system. Although the Linux community develops kernels periodically, sometimes bugs exist in the kernel. Therefore, to protect systems against privilege escalations, system administrators need to follow new Linux patches and periodically check users in the system.

2.5.4. Command & Control

In recent years, specific and complex cyber-attacks have increased, such as APT attacks. In these intricate and sophisticated attacks, the command and control step is one of the essential steps for stealing sensitive information and bridging the attacker and victim's system. There are two types of communication such as centralized and decentralized (for scalability) architectures about the structure of the channel. Attack surface mostly depends on the attacker's motivations, targeted attacks, and evasions. In the last years, C2 architectures developed fastly to detect threats (Gardiner, 2014). Their security primarily relies on the monitoring of network traffic and detection algorithms. Many detection algorithms and techniques include honeynets/malware traps, spam detection, server detection, and host detection (Gardiner, 2014). According to expectations, attackers will use decentralized malware in the coming years, and

anonymity services will be increased against detection systems (Gardiner, 2014).

2.5.5. Common Cyber Attacks: Reducing The Impact

Information systems of organizations may be exposed to cyber-attacks; therefore, organizations think about these potential risks. Surfaces of attacks depend on both organizations and attackers. Some parts of attacks surfaces can be given by weaknesses in the organization's system or depending on the attacker's skills and objectives. Organizations can be targeted with two different possibilities such as un-targeted and targeted attacks (National Cyber Security Centre, 2016). Targeted attacks are more dangerous because it means the attacker chooses the organization specifically, and they may consist of phishing, DDoS, and subverting the supply chain (National Cyber Security Centre, 2016). However, note that each organization is a potential victim of cyberattacks.

Understanding cyber groups' vulnerabilities and attack patterns are crucial to preventing attackers. Security controls (firewalls, malware protection, password policy, etc.) should be ready for attacks. There are also many ways to mitigate attacks, such as user training and awareness.

2.5.6. An Example Threat Landscape Report by ENISA in 2018

This report of ENISA collects from cyber threat intelligence services with experiences (ENISA, 2019). Cyber threat intelligence services provide organizations with information about threats to help with risk management. First and most common threat in 2018 is malware, and 79% of malware was created for Windows (ENISA, 2019). Another threat is web-based attacks such as injections, browser attacks, redirection, and CMS exploitation (ENISA, 2019). The common threats are web application attacks such as SQL injection, cross-site scripting, and local file inclusion (ENISA, 2019). Another attack is phishing, based on social engineering, and is mainly used to send malware to the victim (ENISA, 2019). The next attack is Denial of Service (DoS) attacks that make network systems unavailable (ENISA, 2019). Another threat in 2018 is spam which is popular with email and messages to flood victims (ENISA, 2019). The next threat is a botnet, the attacker hacks and controls the victims' computers and attacks these computers (ENISA, 2019). It is also primarily used in DDoS. Another threat type is a data breach that allows attackers to reach sensitive information about the organization or other users (ENISA, 2019). Another threat is insider threat

stemming from employees or partners (ENISA, 2019). The tenth threat is physical damage or manipulation provided to attacker ATM fraud or POS attacks (ENISA, 2019). There are also five more but less prevalent threats such as information leakage, identity theft, cryptojacking, ransomware, and cyber espionage (ENISA, 2019).

2.5.7. Study of Race Condition: A Privilege Escalation Vulnerability

In today's programming concepts, parallel programming is too popular and helpful for many purposes. One of the critical principles of parallel programming is shared memory (Farah & Shelim, 2018). However, this situation may cause vulnerability, such as race conditions, if implemented wrong. In race condition attacks, the attacker manipulates the checking time of the critical section part by sending multiple requests simultaneously (Farah & Shelim, 2018).

In the past years, attackers found many critical race condition vulnerabilities in essential and popular products such as Firefox, Windows, Internet Explorer, and Linux Kernel (Farah & Shelim, 2018). Semaphore solves this problem by synchronizing the locks (Farah & Shelim, 2018). In addition, semaphore provides working of threads synchronously and communication between them to solve the race conditions. The deadlock issue is also an essential detail in implementing parallel programming that needs attention.

2.5.8. Attacks on Databases and Database Security Techniques

Data is one of the most critical components for any organization in today's technology (Kulkarni & Urolagin, 2012). These data are stored in database systems with structured and relational forms. However, this stored information may be critical for the organization and its users, making security important. Many attackers can apply a type of attack against database systems such as inference, active and passive attacks, SQL injection (Kulkarni & Urolagin, 2012). Inference attacks mainly depend on queries, and the attacker can reach sensitive data from non-sensitive (Kulkarni & Urolagin, 2012). Passive attacks do not change or disrupt the data however can be read and observed. Inactive attacks, an attacker can change data value with some methods such as spoofing and splicing. The last type of attack is SQL injection, the most dangerous attack on databases. An attacker can fingerprint the database, change information, bypass authentication, and more with SQL injection. The organizations need security techniques such as access control mechanisms (checking and controlling user rights to

access some resources), SQL injection fighting techniques (syntax aware evaluation, string evaluation, etc.), data encryption, data scrambling and various techniques (poly instantiation) to prevent database attacks (Kulkarni & Urolagin, 2012).

2.5.9. Session Hijacking and Prevention Technique

One of the most critical topics is cyber security because of the rapidly growing cyber world. Users apply sensitive operations such as bank transactions or online paying on different platforms. That's why these platforms are under attack by attackers. There are many types of attacks, and one of them is session hijacking which provides to attacker steal sensitive information of users. There are three types of session hijacking: active, passive, and hybrid (Baitha & Vinod, 2018). In active type, the attacker tries to steal a live session between user and server. In the passive style, the attacker shows himself to the victim as a server, so the user sends their information to the attacker without noticing. A hybrid attack combines active and passive attack types and can be divided into blind spoofing and non-blind spoofing. There are different countermeasures against session hijacking, such as secure socket layer, secure shell use, HTTPS, strong session ID, random session ID, and session ID generated by server (Baitha & Vinod, 2018).

2.5.10. Documented Examples of Vulnerability and Threat Trends

The number of vulnerabilities that exist is increasing day by day rapidly. In 2018, most of the vulnerabilities live in internet&mobile category (Skybox Security, 2018). Some of the most vulnerable products of 2018 are Google Android, Microsoft Windows, Google Chrome, Apple MacOS (Skybox Security, 2018). Compared with server-side and client-side vulnerabilities, 80 percent of vulnerabilities are server-side (Skybox Security, 2018). Browser vulnerabilities still exist, and many. According to previous years, the number of vulnerabilities in all browsers increased many, and the most vulnerable browser of 2018 was Microsoft Edge (Skybox Security, 2018).

There were also many malware attacks in 2018, such as Cisco Smart Install Flaw, Drupalgeddon2, and VPNFilter (Skybox Security, 2018). In Google's market, Google Play, the number of malware increased much more than IOS because of google development environment is more accessible and easy for attackers (Skybox Security, 2018). Threat intelligence services of organizations need to follow these trends and understand current existing threats.

2.5.11. Top 25 Most Dangerous Programming Errors

The top 25 list of SANS/CWE explains most dangerous programming errors may cause serious effects such as stealing information, account takeover, and code executions (MITRE & SANS, 2009). These errors can be divided into three categories: insecure interaction between components, risky resource management, and porous defenses (MITRE & SANS, 2009). The vulnerabilities in the first category are improper input validation, wrong encoding or escaping of output, SQL injection, cross-site scripting, OS command injection, the clear-text transmission of sensitive information, cross-site request forgery, race condition, and error message information leak (MITRE & SANS, 2009). These type of vulnerabilities occurs when inputs are not sanitized between components. The vulnerabilities that are in the second category are memory overflows, external control of critical state data, external control of file name or path, untrusted search path, code injection, download of code without integrity check, improper resource shutdown or Release, improper initialization, incorrect calculation (MITRE & SANS, 2009). These types of errors mostly come from resource misconfigurations. The vulnerabilities in the last category are authorization, broken or risky cryptographic algorithms, hard-coded passwords, incorrect permission assignment for critical resources, use of insufficiently random values, client-side enforcement of server-side security (MITRE & SANS, 2009). These vulnerabilities occur when security techniques are implemented wrong. The primary purpose of this report is to provide an awareness to programmers about software security (MITRE & SANS, 2009).

2.5.12. Trends In Cyber-Attack Vectors

Organizations need to understand current attack vectors to prevent them from cyber-attacks and threats. The best way to do this is to divide the attack into steps and investigate each step precisely. Before starting to attack, the threat group researches the organization in detail. This operation may take a long time the success. With the information collected in the previous step, an attacker can fake mails with fake domains and apply phishing. After reaching the system, the next step is to control the endpoint in the network (Wood, 2018). After the attacker has access to the endpoint, it is time to explore all networks for any exciting information, such as users in the system or devices. After all these steps, an attacker can take control and execute instructions

on the system and leave the backdoor. From now on, the following steps depend on attacker objectives. An attacker needs to find essential data for him and his purposes in the next step. Finally, after reaching the aimed data, the attacker steals these data over a channel or some trick such as file transfer services.

2.5.13. Windows Privilege Escalations

There are four core stages in the privilege escalation cycle: information gathering, planning, testing, and exploitation (Haboob, n.d.). In Windows privilege escalations, to provide privilege, there are some points: kernel, services, registry, credential dumping, scheduled tasks, hot potato, startup application (Haboob, n.d.). The kernel can be exploited by an attacker's code execution (Haboob, n.d.). There are different methods to attack services, such as DLL hijacking, binPath, unquoted path, registry, and named pipes (Haboob, n.d.). The registry is a critical database consisting of essential information for Windows (Haboob, n.d.). There are two components that the attacker can exploit for registry attacks, such as Autorun and AlwaysInstallElevated (Haboob, n.d.). Password dumping is another method in Windows to privilege escalation by stealing some login and password credentials (Haboob, n.d.). There are four components to investigate for attackers: memory, registry, configuration files, and rdp files (Haboob, n.d.). Another Windows component is scheduled tasks, and the attacker can use this when executing their codes instead of non-protected folders (Haboob, n.d.). There are three ways to privilege in hot potato: local NBNS spoofer, fake WPAD proxy server, and HTTP to SMB NTLM relay (Haboob, n.d.). According to these privilege escalation methods, there are different types of mitigation techniques that administrators should check.

2.5.14. Denial of Service Attacks

DoS attacks are one of the most critical network attacks. DoS attacks can be applied with distributed hosts, called DDoS. Different techniques can be used for DoS from a network perspective, such as TCP SYN flooding, ICMP smurf flooding, and UDP flooding (Gu & Liu, 2007). The success behind DoS/DDoS attacks is the internet's architecture because of its end-to-end structure (Gu & Liu, 2007).

There are also different types of perspectives to classify these attacks. The main categories are Scanning, Spoofing, targeting, and impact. Scanning can be divided into random scanning, hitlist scanning, signpost scanning, and permutation scanning (Gu

& Liu, 2007). Spoofing approaches are random spoofing, subnet spoofing, and fixed spoofing (Gu & Liu, 2007). DoS attacks may target server applications, network access, and infrastructure according to their target. They are disruptive and degrading types (Gu & Liu, 2007). There are also many prevention surfaces against DoS, such as deployment defense, attacker side defense, victim side defense, defense in transit networks, and defense using overlay networks to prevent DoS attacks (Gu & Liu, 2007).

2.5.15. Malware (Malicious Codes)

There are many malware definitions; however, the basic description is malicious software created with harmful intent. There are many types of malware, such as viruses, trojan horses, worms, and spyware. A worm is a type of malware that can copy itself and thus spread quickly. A botnet consists of bots called zombie computers managed by attackers for malicious activities such as DDoS attacks. The virus is another type of malware similar to a worm, but there is a difference. A virus victim needs to trigger to execute it, and thus the virus creates a copy of itself; however, the worm makes it automatically by itself. A rootkit is different from other malware because it consists of tools for various purposes, such as leaving a backdoor and information gathering (Zeidanloo et al., 2010). A trojan horse is like a virus, but it does not spread. Trojans also can be controlled by an attacker remotely. The backdoor is too similar to a trojan horse, but it also can be managed on the internet. It can steal information and/or shut down the system. Other types of malware are also less popular, such as logic bombs, rabbits, and spyware (Zeidanloo et al., 2010).

2.5.16. OWASP Top 10: The Ten Most Critical Web Application Security Risks

Application security risks provide attackers with different ways of a disrupt organization or their users. Some years ago, OWASP (Open Web Application Security Project) released the top ten web application vulnerabilities. In 2017, top web application risks were injection, broken authentication, sensitive data exposure, XML external entities, broken access control, security misconfiguration, cross-site scripting, insecure deserialization, using components with known vulnerabilities, insufficient logging and monitoring (OWASP, 2017). In injection attacks, the attacker manipulates

input to execute arbitrary commands or queries in SQL, OS, LDAP (OWASP, 2017). Broken authentication is about wrong implementations of authentication and session mechanisms and allows attackers to reach other users' keys or passwords (OWASP, 2017). Sensitive data exposure arises when an application does not protect sensitive information such as API keys (OWASP, 2017). XXE is an attack that provides the attackers with internal port scanning, code execution, and more if an attacker can interfere with application process XML data (OWASP, 2017). Broken access controls are risks that provide attackers with access to some restricted resources (OWASP, 2017). Security misconfiguration occurs when some technical details are implemented wrong (OWASP, 2017). XSS occurs when inputs are not sanitized before javascript processes it (OWASP, 2017). Insecure deserialization occurs when an application changes language object to JSON or vice versa. Using components with known vulnerabilities are existing flaws in some unpatched products (OWASP, 2017). Insufficient logging and monitoring is wrong integration which provides to attackers manipulate logs (OWASP, 2017).

2.5.17. OWASP Top 10: The Ten Most Critical API Security Risks

APIs play critical roles in web applications because they interact with databases and server-side in today's web technologies. According to OWASP, the most vital ten API risks are as follows. The first risk is Broken Object Level Authorization, which provides the attacker to reach an object that does not belong to him (OWASP, 2019). The second risk is Broken User Authentication, which lets attackers gain tokens or other users' identities (OWASP, 2019). Authorization mechanisms are complex structures and hard to implement safely, so generally, attackers find some vulnerabilities in them. Excessive Data Exposure is another risk that allows attackers to reach sensitive information about the system or organization, such as API keys (OWASP, 2019). The subsequent risk is the lack of Resources & Rate Limiting that attackers apply brute force or DoS because there is no restriction (OWASP, 2019). Broken Function Level Authorization is another type of vulnerability that provides attackers access to other users or admin resources (OWASP, 2019). Mass Assignment allows attackers to change some objects that should be forbidden (OWASP, 2019). Security Misconfiguration arises because of wrong implementations of technical details such as CORS or HTTP (OWASP, 2019). Injections are the most dangerous vulnerabilities that allow attackers to fingerprint databases and arbitrary code

execution on a server (OWASP, 2019). Improper Assets Management means an attacker can reach old documentation or versions of API (OWASP, 2019). Insufficient Logging & Monitoring consists of the wrong implementation of monitoring systems and provides attackers with some access to extract data (OWASP, 2019).



CHAPTER 3

CYBER WARFARE EXERCISES

3.1. Definition

Until the 21st century, when there was no concept like cyber warfare yet, there were four battlefield areas: land, sea, air, and space. However, with the rapid development of computer systems, people who use these technologies unwantedly started to think about how to disturb these systems. Therefore, as computer systems become more complex, many attack methods and computer viruses appear. Much earlier, “this idea was first discussed in a series of lectures by mathematician John von Neumann in the late 1940s and a paper published in 1966, Theory of Self-Reproducing Automata” (Kaspersky, n.d.). However, this issue has not been fully understood because the studies carried out at that time were far from contemporary hardware & software architectures.

These attack methods have become much more specific, serious, and devastating for any nation or organization. The world has seen how severe and destructive cyberattacks could have been over the Stuxnet incident. Therefore, cyberspace has become the fifth battlefield area with the born of the term cyber warfare. Furthermore, If we look at cybercrime statistics, each person that uses digital devices and connects to the Internet is also a part of this battlefield. According to the Internet Crime Complaint Center (IC3) report, in 2019, hackers inflicted “more than \$ 3.5 billion in losses on individual and business victims” (FBI, 2020; IC3, 2019). When all of these are considered, nations and organizations have begun to investigate how to protect themselves and be prepared for cyber warfare. There are many ways to prevent cyberattacks, such as security audits, educating employees, password policies, and using some products such as firewalls and honeypots. Although many organizations use these products, APT groups find and attack the new targets, “which are carefully chosen and researched, typically including large enterprises or governmental networks” (Imperva, n.d.). These specific attacks “are vast and include intellectual property theft, compromised sensitive information, sabotaging critical organizational infrastructures, and total site takeovers” (Imperva, n.d.). Most of the time, security products cannot fully provide security themselves, so organizations need experienced and aware

security teams that use these tools effectively to deal with threat groups. Therefore, organizations should prepare security researchers practically and realistically to assist them in awareness of an incident. One of the most robust ways to provide this is cyber warfare exercises that “assess or evaluate an organization focusing on the information assurance program” (Kick, 2014). “Cyber exercise provides a simulation environment for information security students and personnel to practice their skills in a controlled environment” (Ahmad et al., 2015). This environment offers integrated learning for vulnerability assessment, cyber attack, forensic, and incident handling (Augustine & Dodge, 2017).

3.2. Types

There are three main types of cyber warfare exercises: Table-Top, Hybrid, and Full Live. This section explains these types of exercises and the main differences between them. Then, according to their expectations from the exercise, the organization may choose one of them for better results.

3.2.1 Table-Top

“Table-top exercises received their name because, in most cases, the planners and players of the exercise sit down at one table and execute the exercise” (Kick, 2014). “Participants are encouraged to problem-solve together through in-depth discussion” (Federal Emergency Management Agency, n.d.). Communication between participants is critical to maintaining table-top exercise, and they all should stick to the plan. According to MITRE, this type of exercise can be planned (1-2 months) and executed quickly (1-3 days), depending on the number of organizations involved (Kick, 2014). Therefore, table-top exercises need fewer people and fewer resources than the other types of exercises. This type of exercise is discussion-based, so participants do not gain any practical experience but focus on solving the security considerations of organizations that apply exercises.

3.2.2. Hybrid

As the name suggests, hybrid exercises combine both Table-Top and Full Live exercise types to take positive aspects of each type. Hybrid-based exercises are table-top exercises with realistic actions to show participants real-world scenarios. According to MITRE, they are coordinating and planning a hybrid exercise requires more than

Table-Top like, approximately 3–6 months (Kick, 2014).

3.2.3. Full Live

Full live exercises are the most realistic type of exercises that show participants in a practical way how cyber incidents occur in the real world. In this type of exercise, planners build a dynamic environment running on live systems that provide interactive warfare for both offensive and defensive perspectives. This environment may contain different designs according to the organization's expectations – web application, cloud, and networks. Therefore, this format enables an organization to test its equipment, hardware, software, and communications skill-sets more clearly when seeing their teams' shortcomings with the scoring system.

3.3. Development Steps

This section clearly explains the development process of exercises in three main steps: planning, execution, and post-exercise. Exercise development is a long process, so every step must be carefully designed.

3.3.1 Exercise Planning

The first step of planning a cyber exercise consists of many components such as identifying objectives, choosing an exercise type, teams, scenarios, and injections. This section describes these components except injections since they are held explicitly in the following chapters.

3.3.1.1. Objectives

When an organization begins to devise a cyber exercise, there are many vital points: concept, timeline, participants, environment, and scoring. However, the first thing to consider is the objectives of the exercise that determine the course of the exercise. “Having clear objectives set from the start will ensure your approach remains focused” (National Cyber Security Centre, 2020). “A group of exercise planners focused on the objectives selects the best means to reach those objectives and develops a complete exercise plan known as the master scenario event list (MSEL)” (Kick, 2014). These objectives may change depending on some organization entities and their culture. Each organization has a different environment, security posture, background of participants,

network systems, and applications. Therefore, planners should evaluate these criteria and establish the most effective objectives.

3.3.1.2. Exercise Type

The next step is selecting the most appropriate and effective exercise type according to defined objectives after the aims of the exercise have been clearly defined. As aforementioned, according to National Cyber Security Centre (2020), there are different types of exercises, so the organization needs to consider some factors when selecting the exercise type, such as;

- Objectives that are defined.
- Resources that are available to the organization.
- The time available to both plan and execute the exercise.
- The availability of crucial teams involved in cyber incident response.

3.3.1.3. Teams

Red Team

A red team is “a team that is formed to subject an organization's plans, programs, ideas, and assumptions to rigorous analysis and challenge” (Ministry of Defence, 2013). “The aims of pen-testing and red teaming, in general, can be viewed as the same, as they are both focused on uncovering an organization's vulnerabilities” (Brangetto et al., 2015). As expected, in cyber exercises, the red team plays a part in realizing cyber attack scenarios defined by planners. “Successful attacks by the red team lead to a negative score for the blue teams” (Seker & Ozbenli, 2018).

Blue Team

Unlike the red team, protect the organization's network and be ready for attacks. The blue team is also responsible for improving the detection and response of cyber incidents. In cyber warfare exercises, the blue team represents the organization's security team that protects the system against external threats. Therefore, the blue team must know environments such as Windows and Linux and how to protect these systems. They also need to monitor all network traffic and able to detect anomalies. Application security is also essential in understanding and detecting web application attacks and payloads.

Green Team

The green team mainly focuses on vulnerabilities, misconfigurations, and research on solving them. “In some exercises, the Green Team represents normal network traffic and background noise. Some exercises use it as a technical team responsible for preparing and maintaining the cyber range technical infrastructure” (Greis, 2016).

Yellow Team

Usually, the yellow team deals with software products solutions within cyber security. However, cyber exercises and software solutions may respond by providing information about the exercise course to the white team during the exercise.

White Team

The white team, the central control team, determines the fundamentals of exercises. “The white team also acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission” (National Institute of Standards and Technology, 2019).

3.3.1.4. Scenarios

Scenarios are another essential components to consider by exercise planners. “The cyber exercise scenario is the story or case-study through which a hypothetical cyber incident is introduced to exercise participants” (Victorian Government, 2019).

Exercise scenarios need to have;

- Clear enough to understand.
- Include relevant and popular threat types.
- Suitable for the technical infrastructure of the organization.
- Similar to real-life examples.

3.3.1.5. Outcomes

Outcomes are specific expected results based on the objectives of the exercise. According to the objectives and goals, each exercise needs to have outcomes. Predetermining expected outcomes provides a more efficient course of exercise. Also, in this way, deficiencies and setbacks in the course of the exercise can be detected more easily. However, the fact that the expected outcomes are realistic and feasible

plays a vital role in ensuring that the exercise takes a suitable course for its purpose.

3.3.1.6. Other Components: Location, Resources, Scoring

Depending on the desired exercise course, the organization may need various tools, resources, etc. Exercise planners and control teams may forbid some automated tools and vulnerability scanners to encourage the participants to develop their skill-sets. The control team can also define a specific list of devices that participants are expected to improve with these tools. Organizations may also need different types of resources according to their exercise plan. Therefore, planners need to notify the organization to get the resources required. Scoring is another component to planners and control teams identify it clearly to handle execution. For example, the scoring of the red team depends on the fulfill the attack scenario and injection successfully. There are also many other components to consider, such as location, logistics, participants, and expectations from the exercise.

3.3.2. Exercise Execution

According to chosen exercise type, exercise execution may take hours or days. Before starting the exercise, the control team may make a session to describe the detailed exercise plan to the teams. As detailed below, there are some critical points for which the control teams are responsible during the exercise.

3.3.2.1. Information Management

Information management is part of the execution for maintaining more reliable exercise. During the execution, the control team needs to take notes about pitfalls, scoring, etc. While scenarios are being played, they should monitor the environment and investigate each team's moves. “Monitoring and logging is the basis for the scoring system, and it helps to identify and respond to incidents during the exercise at an early stage” (Seker & Ozbenli, 2018). Information sharing is another important concept in cyber exercises because of the needs between participants or teams in interactions. In the Cyber Exercise Playbook of MITRE, the information flow of exercise is given in the following Figure 3.1.

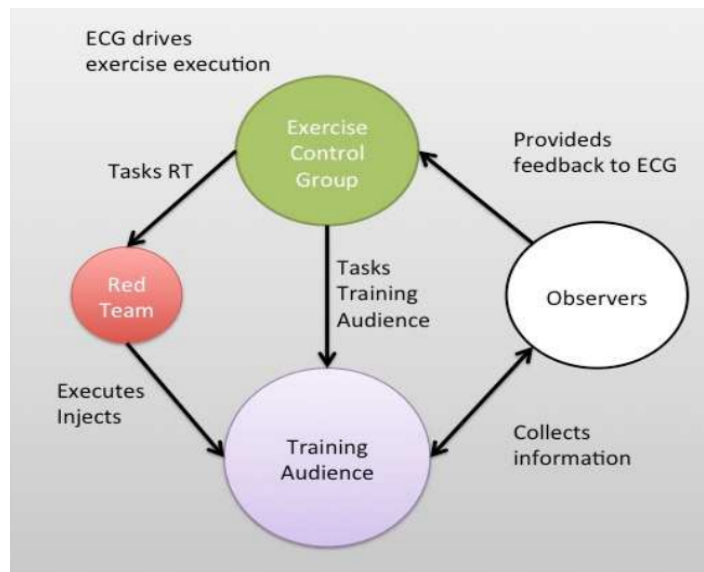


Figure 3.1. Exercise Information Flow (MITRE)

Kick, J. (2014, November). *Cyber Exercise Playbook*. MITRE.

3.3.2.2. Daily Review

At the end of each exercise day, the control team summarizes the day's events, reviews, and how many attacks were covered and how many remain (Department of Defense Office, 2018). In addition, the control team also may share privately with every team their daily notes and reports about performance, weaknesses, and recommendations about each team. These reviews not only prevent participants from breaking away from exercise, but also keep them motivated constantly.

3.3.3. Post Exercise

The after-action report (AAR), prepared after the exercise is completed, plays a critical role in evaluating exercise. Each team can see their detailed performance for specific scenarios or injections in this report. In addition to that, “the exercise purpose, participants, scoring, technical infrastructure, red team attacks (client-side, web, network), defenses made by the blue team, defects in these defenses, general mistakes made, observations from all teams and sub-teams, recommendations and evaluations are also covered” (Seker & Ozbenli, 2018). In the end, feedback, in the form of a questionnaire, should be obtained from the participants. Thus, the shortcomings of the exercise should be determined to evaluate the exercise and the overall performance of the planners. Apart from the questionnaire, a piece of advice can always be obtained from the participants about eliminating the deficiencies of the exercise.

3.4. Examples from Around the World: NATO, USA, and Europe

This section briefly explains the most famous and international-scale (Locked Shields, Cyber Storm, and Cyber Europe) exercises. In addition, objectives, scenarios, and information about participants of these exercises are provided below.

3.4.1. Locked Shields: NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)

“This annual exercise, organized by CCDCOE since 2010, enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks” (NATO Cooperative Cyber Defence Center of Excellence, 2021). “The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects.” (NATO Cooperative Cyber Defence Centre of Excellence, 2021).

Participants: More than 1500 participants from 30 nations played the exercise in Locked Shields 2019.

Objectives: According to After Action Report of Locked Shields of 2013, some of the objectives used in the exercise focus on testing the skills of the blue team and the red team;

- Learning the network (Blue Team).
- System administration and prevention of attacks (Blue Team).
- Monitoring networks, detecting and responding to attacks (Blue Team).
- Handling cyber incidents (Blue Team).
- Teamwork: delegation, dividing and assigning roles, leadership (Blue Team).
- National and international cooperation. Information sharing (Blue Team).
- Reporting (Blue Team).
- Ability to convey the big picture (Blue Team).
- Crisis communication (Blue Team).
- Deface with BIT message and point to malware for distraction (Red Team).
- Delete content & destroy the host as much as possible to keep BT busy in Aid_DMZ (Red Team).
- Compromise and steal volunteer database (Red Team).

- Spread inside AID_INT to other hosts and set beacons (Red Team).
- Compromise mail server in Aid_DMZ and steal specific e-mails (Red Team).
- Conduct routing attack against MIL_DMZ (Red Team).

Scenario: Aid organizations report cyber attacks against their systems in the country and ask for coalition assistance until crisis response teams fly in.

3.4.2. Cyber Storm: Department of Homeland Security, USA

“Cyber Storm, the Department of Homeland Security's (DHS) biennial exercise series, provides the framework for the most extensive government-sponsored cyber security exercise of its kind” (Cybersecurity and Infrastructure Security Agency, n.d.). According to the After Action Report of Cyber Storm V, the exercise strengthens cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure.

Participants: In Cyber Storm V, more than 1,200 participants represented entities from the public and private sectors within the United States and abroad.

Objectives: Some of the exercise objectives taken from the report are as follows:

- Continue to exercise coordination mechanisms, information sharing efforts, development of shared situational awareness, and decision-making procedures of the cyber incident response community during a cyber event.
- Evaluate relevant policy, statutory, and fiscal issues that govern cyber incident response authorities and resource prioritization.
- Provide a forum for exercise participants to exercise, evaluate, and improve the processes, procedures, interactions, and information sharing mechanisms within their organization or community of interest.
- Assess the role, functions, and capabilities of DHS and other government entities in a cyber event.

Scenario: According to the Department of Homeland Security of USA, After Action Report July 2016, the scenario of the exercise is given as the following excerpt:

"Scenario of Cyber Storm V is designed based on cyber events that are common in today's conditions such as corporate and government systems, medical devices, and payment systems with leveraged weaknesses in common protocols and services used

on the Internet. The scenario included impacts to routing methodology, the Domain Name System (DNS) used to map hostnames to Internet Protocol (IP) addresses, and Public Key Infrastructure (PKI) used to provide authentication and confidentiality."

3.4.3. Cyber Europe: ENISA

“Cyber Europe is a series of EU-level cyber incidents and crisis management exercises for the public and private sectors from the EU and EFTA Member States” (European Union Agency for Cybersecurity, n.d.).

Participants: Cyber Europe 2018 included around 900 participants, from the public authorities and private companies, mainly in the Aviation sector, from all 28 EU Member States and two European Free Trade Association (EFTA) countries, Norway and Switzerland.

Objectives: are listed below:

- Assess the quality of information sharing.
- Monitor occurrences of cooperation activities.
- Provide opportunities to Participants to test their intra-organizational procedures, if they exist.
- Provide opportunities to Participants to test cross-organizational cooperation processes, if any.
- Provide opportunities to train a wide variety of cybersecurity-related skills.
- Provide learning opportunities.

Scenario: Following scenario taken from the After Action Report of Cyber Europe 2018.

"The scenario was set around the concept of the worldwide rise of extremism. This 'virtually invisible' phenomenon has turned into an open and widespread one with several different facets, from religion to political beliefs, engaging thousands of followers and millions of supporters. The number of radical websites has increased exponentially since 2013, and extremists are utilizing social media to recruit and organize.

The increase of the followers of this extremism leads to their engagement in cyber-attacks. Radical groups could use advanced or less advanced techniques to strike at any time as they revealed the Internet to be a hotbed of radicalization; 'Now on the internet, radicalization can occur instantly and anonymously within significantly

larger and more geographically distributed groups'. A new radicalistic movement without a central organization has a powerful arsenal of cyber-attack techniques with capabilities, such as exfiltration, traffic capturing and logging, keylogging, ransomware, hybrid attacks with drones, IoT infectors, worms, etc. "



CHAPTER 4

DEVELOPING SCENARIOS & INJECTIONS

4.1. Definition

In the previous section, general information about cyberwarfare exercises and the components in these exercises was given. This chapter aims to understand more clearly what the injections mean in terms of these exercises and their connection with other components such as objectives and outcomes. In this section, firstly, the definition of injection is given. Secondly, how an injection should be written and be standardized is explained. Finally, at the end of the chapter, injections created by different organizations are examined.

An injection is defined as "A specific activity executed as part of a master scenario event list (MSEL)." according to the MITRE's guideline (Kick, 2014; Joint Chiefs of Staff, 2012). Moreover, to define it more clearly and simply following the content of this study, an injection can be defined as "An event or process that is informative instruction for participants to achieve goals, scenarios, and objectives while adhering to the course of the exercise."

4.2. Developing Injections: Scenarios & Attack Techniques

When cyberattacks are examined, although different techniques are used in all of them, the attack stages go in a specific order. In particular, most of the attacks made by APT groups, which have become extremely widespread today, operate in this way. "Targeted attacks and advanced persistent threats (APTs) are organized, focused efforts that are custom-created to penetrate enterprises and government agencies for access to internal systems, data, and other assets" (Trend Micro, n.d.). "Each attack is customized to its target, but follows a consistent life cycle to infiltrate and operate inside an organization" (Trend Micro, n.d.). For this reason, some models show the operation of complex cyber attacks, and the most popular of them is Cyber Kill Chain. Suppose the main scenario used in the exercise is based on a model such as the cyber kill chain. In that case, the participants will be given the opportunity to see in advance

how modern and complex cyber attacks work or what they will encounter in case of any cyber attack.

In Figure 4.1 below, every stage of modern attacks is clearly seen and can be summarized as, “the attacker performs reconnaissance, intrusion of the security perimeter, exploitation of vulnerabilities, gains and escalates privileges, moves laterally to gain access to more valuable targets, attempts to obfuscate their activity, and finally, exfiltrates data from the organization” (Cassetto, 2020).

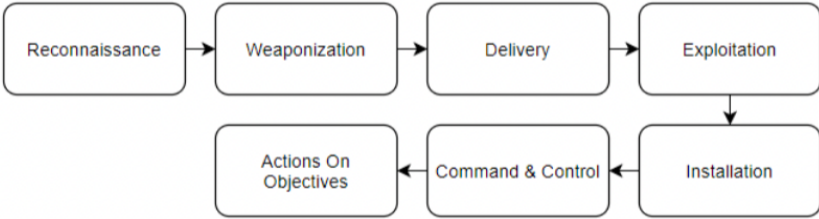


Figure 4.1. Cyber Kill Chain Model

Lockheed Martin. (n.d.). The Cyber Kill Chain. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

There are many factors to write and apply injections in a cyber warfare exercise effectively. One of the most important of these factors is the scenario that is where the injection take place. An injection scenario is a scenario that is technically suitable for current attack scenarios used by today's threat groups and includes many injections.

Therefore, two critical metrics must be considered when writing an injection. The first of these is the scenario of the injection itself. The most crucial point to be considered while writing the injection scenario is that it should follow the integrity of the main scenario and the path followed by an attack applied according to the mentioned model above.

The second metric is the attack techniques within the injection scenario. Again, people with technical knowledge and experience should create them. However, before these attack techniques are developed, the team that will write these techniques should examine and analyze the organization's infrastructure. In this way, they can determine the types of attacks suitable for the organization's infrastructure and may encounter them in real life.

4.3. Example Injections

This section briefly underlines the injections and scenarios utilized in some of the most widespread cyber warfare exercises.

4.3.1. MITRE Perspective

MITRE, a not-for-profit organization, has one of the most comprehensive guides written on the cyber warfare exercise (Kick, 2014). MITRE's Cyber Exercise Playbook provides a table about cyber injections. There is a unique ID value for each injection, and each injection has a title and detailed explanation. Moreover, the injection descriptions explain what is expected from the red team. A list of the objectives and outcomes linked with each injection is also included in the table. Associating each injection with the objectives and outcomes is extremely important to maintain the exercise's integrity and flow according to the already defined purpose.

4.3.2. Locked Shields

Locked Shields is an annual Red team vs. Blue Team exercise, “organized by CCDCOE since 2010, enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks” (CCDCOE, n.d.). “Locked Shields is the largest and most complex international live-fire cyber exercise in the World” (Mochinaga, 2021). The After Action Report (AAR) of Cyber Defence Exercise Locked Shields 2013 shows that three sets of injections were utilized in the exercise: scenario injects, media injects, and legal injects (NATO CCDCOE, 2013). It is crucial to underline that media and legal injects, apart from the technical details of a real cyber-attack, show the participants' environmental and psychological effects or the situation they may encounter.

According to the AAR, there are scored scenario injections in the report. In addition, each injection has a description section that provides information about the injection scenario, injection time, injection method, and injection feedback (CCDCOE, 2013). The scoring is the second part of injections, and it explains scoring criteria and some best practice usage for bonus points (CCDCOE, 2013). The last point of each injection is the responses from the blue team. It is also clear that the injections were prepared with a defensive perspective that suggests the blue team as the root of the injections.



CHAPTER 5

A SAMPLE CYBER EXERCISE

5.1. Background Information

- **Location:** A fictitious country name, i.e., Victimia
- **Victim:** The Central Bank of Victimia
- **Scenario:**

One of the largest private banking companies in the VICTIMIA is the *Central Bank of Victimia*. The cybercriminals plan to steal sensitive information, disturb financial transactions, and steal some money, if possible.

Firstly, cybercriminals are planning to hijack the admin page of the bank's web application. Therefore, they try many ways to reach their goals, such as fuzzing techniques, injection attacks, and wifi attacks. In the fuzzing phase of the attack, they explore some sensitive admin pages and use these pages to try to hijack the admin panel with a brute force attack. The next try of cybercriminals is one of the most popular injection attacks known as the SQL injection. This time they are trying to bypass the login page to enter the panel with an injection attack. If they cannot access the admin page with these methods, the cybercriminals will use their last shot with a robust sniffing network cyber attack. They start sniffing the network and listen to all traffic while trying to capture the credentials of the admin page.

The next aim of cybercriminals is to infiltrate the system from any point and make the information inside inaccessible by deleting or encrypting. To do these, attackers first send a phishing email with a keylogger. With this malicious software sent, attackers wait for the victim to enter the database password to enter the database. As an alternative way, the cybercriminals review the web application and detect XSS vulnerability. With this vulnerability, they try to reach their goals by making changes to the page content and obtaining the cookie information of the already logged-in users. The final social engineering attack by the attackers begins when they discover that one of the subdomains of the target application can be taken. They utilize this vulnerability to create a fake login page and send it to blue teams. So that the panel will be hijacked, if the victim enters their login information while on that page

In the third attack stage, the cybercriminals should get a remote connection to the system, so they need to find the remote code execution vulnerability. Firstly, they scan

the network to find a Windows machine. They attack SMB services and exploit them as soon as it is found. An alternative way, maybe they can use this way to attack Windows machine: They found a vulnerability exists in this machine's version and exploit it with reverse powershell. Another remote code execution that founded by the cybercriminals is about PHP parameter. They saw a url parameter and use injection attacks and execute system commands.

In the final stage of the scenario, the cybercriminals use different attacks. First, they attack Windows RPC to infiltrate the victim's machine. Then, capture the Admin hash values stored in Windows to get credentials. Another attack type is DOS. They apply DOS attack to the bank's web application to collapse the system. Finally, the cybercriminals found another vulnerability in the bank's web application. They decode used weak hash algorithm then solve the cookies' pattern to log in as admin.

- **Exercise Duration:** Two and a half days. Two days for the execution of the exercise and half a day for the preparation of After Action Report (AAR)

5.2. Exercise Target Group

It is of utmost importance to define the target group getting the training by the exercise. In this example, the fintech staff of the banking company is being described as the target group.

5.3. Exercise Objectives

The objectives of the cyber exercise are given here in the table format.

Table 5.1. Objectives of the Cyber Exercise

#ID	Objective
1	Assess the ability of teams to explore infrastructure.
2	Assess the ability of the blue team to detect and react against red team activities.
3	Assess the ability to develop methodologies.
4	Test the intelligence-sharing procedures during response responding to cyber incidents.
5	Evaluate the cyber incident response team's resource prioritization.
6	Provide opportunities to Participants to train their cybersecurity-related skills.
7	Understand the security vulnerabilities and adversary perspective.
8	Provide opportunities for participants to assess themselves.

5.4. Exercise Expected Outcomes

The outcomes, again, are provided in the form of a table.

Table 5.2. The Expected Outcomes of the Cyber Exercise

#ID	Outcome	Activity	Category
1	Strengthen team's cyber response preparedness.	Participants will see how they must be prepared against cyber risks.	Training
2	Reduce cyber-attack impact on data, systems, and critical infrastructure.	Participants will understand the severe impacts of cyber-attacks.	Training
3	Ensured cyber awareness about finance technologies.	Participants will see various types of attacks that they may encounter in the finance sector.	Execution
4	Ensured awareness about the potential risk of cyber-attacks with realistic scenarios.	Participants will see scenarios based on real examples.	Execution
5	Ensured maintenance services during cyber-attack by system administrators.	System engineers will be trained in about maintenance of systems during attacks such as DOS	Execution
6	Provided ability to use different kind of tools for each team.	Participants will be trained usage of different types of tools for both attack and defense.	Validation
7	Reviewed and discussed how correctly applied performed injections.	After exercise, participants will see their scores and can evaluate themselves.	Validation
8	Identified and reported gaps in exercise.	Lastly, the overall functioning of the exercise will be evaluated.	Validation

5.5. Exercise Events: Master Event list (MEL)

This sample cyber exercise has four events, and each event has three injections.

- **Broken Admin:** The red team tries to infiltrate the demo application's admin panel with different injection scenarios and attack techniques.
- **Social Engineering:** The red team tries to move through the system by infiltrating the computer of anyone in the blue team with different social engineering scenarios.
- **Remote code execution:** The red team tries to find the Remote Code Execution

vulnerability, one of the system's most destructive attack types. They try to reach their goals with the discovered vulnerability by running the code remotely in the system.

- **The other various attacks:** The red team applies multiple attacks and techniques to reach their goals. They use Windows RPC to get a reverse shell, encrypt all files, apply DOS attacks to collapse the server, and decode the weak hash to act as an admin user.

5.6. Exercise Injections - Master Injection List (MIL)

Table 5.3. The Event List of the Cyber Exercise

Tech. Num.	Injection	CAPEC Number	Description	Relating to the Exercise Objectives Numbered	Relating to the Exercise Outcomes Numbered
T1110	Broken Admin: Fuzzing CWE-79	CAPEC-28 CAPEC-112	The adversary applies to fuzz to hidden directories such as PHPMyAdmin; admin then cracks the admin credentials with brute force.	3, 5, 6, 7, 8	1, 2, 3, 4, 6, 7, 8
T1190	Broken Admin: SQL Injection CWE-89	CAPEC-66	The adversary exploits SQL Injection vulnerability to bypass authentication of demo bank application.	2, 4, 6, 7, 8	1, 3, 4, 7, 8
T1557	Broken Admin: ARP Poisoning CWE-290	CAPEC-157	The adversary sniffs the network packets with ARP Poisoning.	1, 3, 6, 7, 8	2, 4, 6, 7, 8
T1010	Social Engineering: Key Logger	CAPEC-568	The adversary puts a keylogger on the system and steals the information.	2, 4, 5, 7, 8	3, 4, 7, 8

Table 5.3. The Event List of the Cyber Exercise (continued)

T1059	Social Engineering: XSS CWE-79	CAPEC-63	The adversary exploits the XSS vulnerability to steal session cookies.	3, 6, 7, 8	1, 4, 7, 8
T1584	Social Engineering: Subdomain Takeover CWE-16	CAPEC-148	The adversary takeovers a subdomain of the demo bank application to create a phishing page.	2, 3, 6, 7, 8	1, 4, 6, 7, 8
T1055	Remote Code Execution: SMB Delivery CWE-553	CAPEC-253	The adversary exploits a vulnerability with an old SMB service. They generate malicious dll file to get into the system.	1, 2, 3, 5, 6, 7, 8	1, 2, 4, 5, 6, 7, 8
T1059	Remote Code Execution: PowerShell CWE-553	CAPEC-253	The adversary copies a malicious bat file to the system written in Powershell.	1, 2, 3, 6, 7, 8	1, 2, 4, 5, 6, 7, 8
T1059	Remote Code Execution: PHP Bypass CWE-94	CAPEC-248	The adversary exploits remote code execution vulnerability by PHP parameter to escalate their privileges with the server.	3, 6, 7, 8	1, 4, 5, 6, 7, 8
T1205	Various Attacks: Windows RPC CWE-553	CAPEC-122	The adversary infiltrates the system with the vulnerability in the Windows RPC service and encrypts all the files.	1, 2, 3, 7, 8	1, 3, 4, 6, 7, 8
T1499	Various Attacks: DOS CWE-400	CAPEC-482	The adversary attempts to apply a DOS attack to an endpoint in the web demo application for collapsing server.	1, 2, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 7, 8
T1600	Various Attacks: Weak Hash CWE-328	CAPEC-461	The adversary decodes the weak hash session tokens to masquerade as an admin.	3, 6, 7, 8	1, 4, 6, 7, 8

5.7. MEL-MIL-Objective-Outcome Matrix

It always helps to see the MEL & MIL with the related exercise objectives and expected outcomes in a table.

Table 5.4. MEL-MIL-Objective-Outcome Matrix

Master Event List (MEL)	Master Injection List (MIL)	Relating to the Exercise Objectives	Relating to the Exercise Expected Outcomes
1. Broken Admin	1.1. Using fuzzing and brute	3, 5, 6, 7, 8	1, 2, 3, 4, 6, 7, 8

	force techniques		
	1.2 Bypassing authentication with injection attack	2, 4, 6, 7, 8	1, 3, 4, 7, 8
	1.3 Sniffing the network and collect credentials.	1, 3, 6, 7, 8	2, 4, 6, 7, 8
2. Social Engineering	2.1 Sending phishing mail and using keylogger	2, 4, 5, 7, 8	3, 4, 7, 8
	2.2 Exploiting XSS vulnerability to steal cookies	3, 6, 7, 8	1, 4, 7, 8
	2.3 Applying social engineering with exploiting subdomain takeover	2, 3, 6, 7, 8	1, 4, 6, 7, 8
3. Remote Code Execution	3.1 Exploiting SMB delivery vulnerability with using Metasploit Framework	1, 2, 3, 5, 6, 7, 8	1, 2, 4, 5, 6, 7, 8
	3.2 Using bat file to get reverse shell connection	1, 2, 3, 6, 7, 8	1, 2, 4, 5, 6, 7, 8
	3.3 Attacking unsanitized PHP parameter and execute remote codes	3, 6, 7, 8	1, 4, 5, 6, 7, 8
3. Various Attacks	4.1 Using port knocking and exploit Windows RPC for get reverse shell	1, 2, 3, 7, 8	1, 3, 4, 6, 7, 8
	4.2 Applying DOS attack for collapse the server	1, 2, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 7, 8
	4.3 Decoding weak hashed values to act as an admin	3, 6, 7, 8	1, 4, 6, 7, 8

5.8. Master Scenario Event List (MSEL) Table

It is a table that contains information such as the duration and time of the events and injections expected to occur during the msel exercise in cyber warfare exercises, which team will be applied, and location (FEMA, n.d.).

Day-1

Table 5.5. MSEL Table of the Cyber Exercise – Day-1

Time	Event Logs	Expected Action	From
9:00	Presentation about exercise	-	-
10:00	Informative mail send	Exercise start	White Team
10:05	Red Team scan network	Blue team detect scan and block	Red Team
10:25	Fuzzing directories	Check broken access	Red Team
10:50	Brute forcing	Check passwords	Red Team
12:00 – 13:00	Lunch (No Action)	-	-
13:15	Red Team sends malicious mail	Check if the mail is fake or not	-
14:30	Red team subdomain enumeration	-	Red Team
16:00 – 17:00	Daily Hotwash	-	All participants

Day-2

Table 5.6. MSEL Table of the Cyber Exercise – Day-2

Time	Event Logs	Expected Action	From
9:00	Presentation about exercise	-	-
10:00	Informative mail send	Exercise start	White Team
10:05	Red Team scan network	Blue team detect scan and block	Red Team
10:30	SMB works	Disable the connection	Red Team
10:40	Automotive scanner works	Detect noise and block	Red Team

Table 5.6. MSEL Table of the Cyber Exercise – Day-2 (continued)

12:00 – 13:00	Lunch (No Action)	-	-
13:15	Fuzzing port 135	Disable the port	-
14:45	DOS attack starts	Detect DOS and disconnect attackers	Red Team
16:00 – 17:00	Daily Hotwash	-	All participants
17:00 – 19:00	Preparing the report	-	All participants

5.9. Exercise Hybrid Network Topology

As in Figure 5.1 below, each team is connected to the main router with a switch on the single bus topology. In addition, each team has computers with different operating systems according to their technical needs. Apart from these, there are also two firewalls, one of which is positioned to monitor internet traffic and the other to monitor the traffic of the demo application.

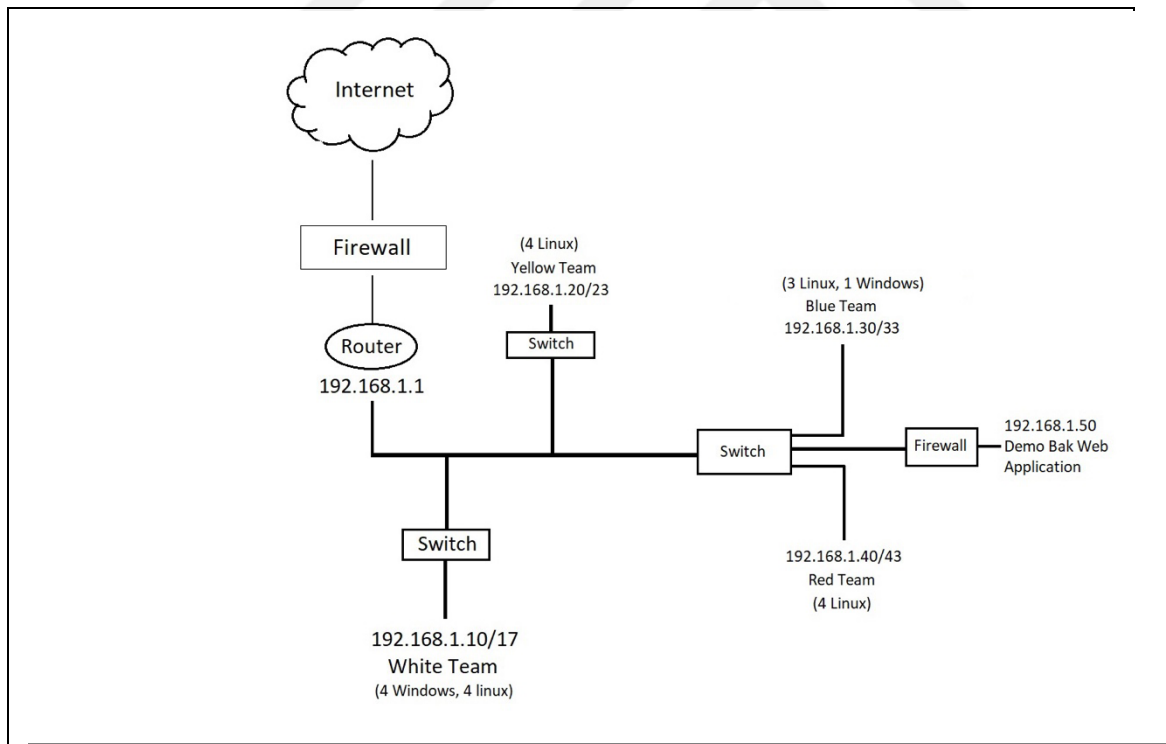


Figure 5.1. Cyber Exercise Topology.

Notes:

- The mail addresses that will be utilized for communication between teams or administrators will be as follows:
 - Red team mail pattern is rt01@exercise.com, rt02@ exercise.com etc.
 - Blue team mail pattern is bt01@ exercise.com, bt02@ exercise.com etc.
 - Yellow team mail pattern is yt01@ exercise.com, yt02@ exercise.com etc.
 - White team mail pattern is wt01@ exercise.com, wt02@ exercise.com etc.

5.10. Software Tools to be Utilized

The software necessary for the red team to accomplish the results through the injections is given as a list.

Table 5.7. The Software Tools

Injection ID	Tools
1	Nmap, FFUF, Burp Suite, OpenVAS
2	Nmap, OpenVAS, SQLMap, Robots.txt, Wappalyzer (Browser Extension)
3	Nmap, OpenVAS, Ettercap, WireShark
4	Nmap, OpenVAS, Mail Server, Apache, MySQL, Python Script, Malicious PDF, AES-512
5	Nikto, Javascript Code (XSS), CHM, Browser
6	KnockPy (Subdomain Enumeration), GitHub, HTML, Javascript
7	Nmap, Windows, Rundll32.exe, Metasploit, Firewall, SMB Delivery, WireShark, Reverse Connection
8	Netcat, PowerShell, Bat, Msfvenom, Windows, Firewall, WireShark
9	Wappalyzer, PHP7, Nikto, WAF (Firewall), Arjun (hidden parameter finder)
10	Nmap, Netcat, Windows, Metasploit, Firewall, Ransomware, WireShark, Reverse Shell TCP/IP, FFUF
11	Nmap, WireShark, Firewall, LOIC (DOS Tool)
12	WAF, WireShark, MD5, Burp Suite

5.11. Exercise Environment

The rooms for the teams should be separated due to their color, and there must be absolutely no physical contact, especially between the blue and the read teams. A

conceptual layout might be something like that of the given picture below.

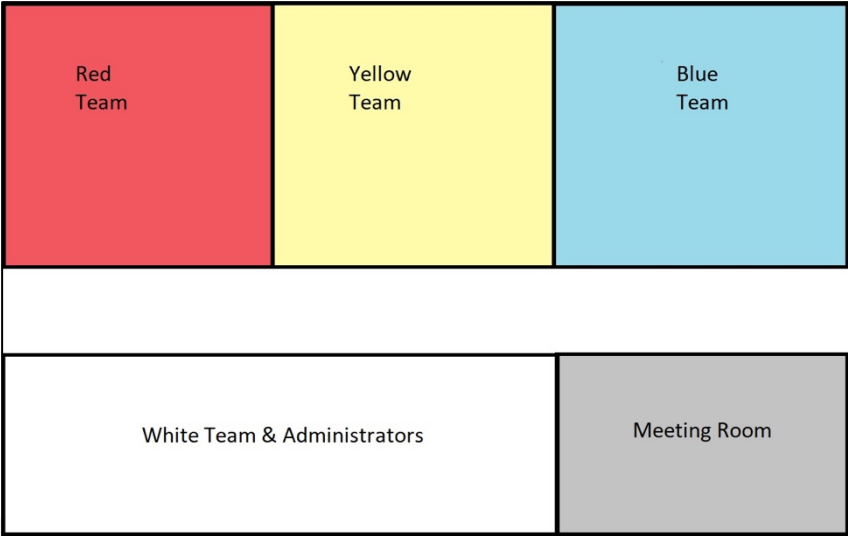


Figure 5.2. The Teams layout

CHAPTER 6

DISCUSSION, CONCLUSION, AND A FUTURE WORK

6.1. Discussion

it is mentioned in the first chapter that more technical skills and experience are required to develop injections in preparing a cyber warfare exercise. Therefore, certain standards must be employed while designing them. When injections are insufficient in some cases and are incompatible with the scenario in some other cases, the whole cyber-attack scenario can easily be disrupted. When the sample injections in the previous chapter are examined, it may be seen that none of them were randomly selected and placed on the timeline. While preparing the injections, attention was paid to the technical order so that participants could quickly grasp the realization stages of a complex cyber attack. In addition, each injection is associated with standardized MITRE database CAPEC numbers. Moreover, since the injections were created according to an order, it should be sufficient for all participants to search the internet to find the injection technique or other similar techniques. This study clearly shows the importance of the systematic approach to injection development. A detailed example is provided in chapter five of how injections should be created for institutions and individuals who want to plan a cyber warfare exercise.

6.2. Conclusion

After providing necessary theoretical background information about cyberwarfare exercises, the real cyber warfare exercises implemented by different organizations and nations were studied. As a result of this research, it has been discovered that there is no standard action plan for red team operations in cyber warfare exercises. This study aims to solve this problem by helping to create a completely realistic attack scenario since it is built on the APT attack steps as defined in the cyber kill-chain methodology. With this study, organizations can realistically prepare their own red team scenarios and injections. Furthermore, this work offers the ability to implement injections used in cyber warfare exercises created by different organizations. In this way, organizations can create an injection database among themselves and take the injections suitable for the scenario they apply from this database and manage a rapid exercise preparation

process.

Moreover, organizations should pay attention to the techniques introduced in this study when developing injections as the cyber attack steps. It is necessary to ensure that these selected techniques are suitable for the organization's technological infrastructure. In this way, the staff responsible for preparing the cyber warfare exercise will understand the attack methods that can be planned against the technical infrastructure of their organizations, hence being ready for a remedial action when and if the actual cyber attack occurs.

6.3. Future Work

Developing an extensive injection database categorized according to different and various other technological infrastructures and targets is one of the future works of this study. Thus, research that creates injection scenarios according to the technological components determined with the help of artificial intelligence will be a continuation of the current study. Therefore, when this is accomplished, the institutions will be able to add their injections to this open-source database or create injection scenarios for themselves easily when they need it. So, institutions can conduct these exercises at more frequent intervals and prepare themselves for cyber attacks by automating injection development, one of the most challenging and complex points in cyber warfare exercises.

REFERENCES

- Ahmad, A., Johnson, C., & Storer, T. (2015). *A Cyber Exercise Post Assessment: Adoption of the Kirkpatrick Model*. *Advances in Information Sciences and Service Sciences*, 7(2), 1.
- Ahmad, N. & Habib, M.. (2010). *Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution*. <http://www.bth.se/fou/cuppsats.nsf>. I. 93.
- Augustine T., Dodge, R. C., (2007). *Cyber Defense Exercise: Meeting Learning Objectives thru Competition*. *IEEE Security and Privacy*, 5(5).
- Baitha, A.K., & Vinod, S. (2018). Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology*, 7(2.6), 193. <https://doi.org/10.14419/ijet.v7i2.6.10566>
- Blumbergs, B. (2019). Remote Exploit Development for Cyber Red Team Computer Network Operations Targeting Industrial Control Systems. *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. <https://doi.org/10.5220/0007310300880099>
- Brangetto, P., Çalişkan, E., & Rõigas, H. (2015). *Cyber Red Teaming*. CCDCOE.
- Cassetto, O. (2020, February 13). *Cyber Kill Chain: Understanding and Mitigating Advanced Persistent Threats*. Exabeam. Retrieved March 5, 2022, from <https://www.exabeam.com/information-security/cyber-kill-chain/>
- CCDCOE. (2013). *Cyber Defence Exercise Locked Shields 2013: After Action Report*.
- CCDCOE. (n.d.). *Locked Shields*. Retrieved March 7, 2022, from <https://ccdcoe.org/exercises/locked-shields/>
- Chawla, M., & Singh Chouhan, S. (2014). A Survey of Phishing Attack Techniques. *International Journal of Computer Applications*, 93(3), 32–35. <https://doi.org/10.5120/16197-5460>
- Chiem, T.P. (2014). A study of penetration testing tools and approaches.
- Chismon, D., & Ruks, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating*. MWR InfoSecurity.
- Colarik, A. M., & Janczewski, L. J. (2011). Developing a grand strategy for Cyber War. *2011 7th International Conference on Information Assurance and Security (IAS)*. <https://doi.org/10.1109/isias.2011.6122794>
- Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010, November). *On Cyber*

- Warfare*. Chatham House.
https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf
- Cybersecurity and Infrastructure Security Agency. (n.d.). *CYBER STORM: SECURING CYBER SPACE*. Cisa. Retrieved March 14, 2021, from <https://www.cisa.gov/cyber-storm-securing-cyber-space>
- Department of Defense Office. (2018, July). *The Department of Defense Cyber Table Top Guidebook*.
- Development, Concepts and Doctrine Centre. (2010, February). *A GUIDE TO RED TEAMING*.
- European Union Agency for Cybersecurity. (n.d.). *Cyber Europe*. Europa. Retrieved March 14, 2021, from <https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme>
- Farah, T., & Shelim, R. (2018). Study of Race Condition : A Privilege Escalation Vulnerability.
- FBI. (2020, February 11). *2019 Internet Crime Report Released*. Retrieved February 7, 2021, from <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>
- Federal Emergency Management Agency. (n.d.). Discussion-based Exercises - Types, Goals, and Conduct. Fema. Retrieved February 17, 2021, from https://emilms.fema.gov/is_0120c/groups/41.html
- FEMA. (n.d.). *Master Scenario Events List (MSEL)*. Retrieved March 13, 2022, from https://emilms.fema.gov/is_0130a/groups/25.html
- FireEye. (2020). *DOUBLE DRAGON: APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION*.
- Gardiner, J., Cova, M., & Nagaraja, S. (2014). Command & Control: Understanding, Denying and Detecting - A review of malware C2 techniques, detection and defences. *arXiv: Cryptography and Security*.
- Greis, J. (2016, May). *Cyber Security Exercise Modeling & Tracking*. JAMK University of Applied Sciences.
- Gu, Q., & Liu, P. (2007). Denial of Service Attacks. *Handbook of Computer Networks*, 454–468. <https://doi.org/10.1002/9781118256107.ch29>
- Haboob, "Windows Privilege Escalations", (accessed 29 July 2020). [Online]. Available: <https://www.exploit-db.com/docs/english/46131-windows->

privilege-escalations.pdf

- Hoque, N., Bhuyan, M. H., Baishya, R., Bhattacharyya, D., & Kalita, J. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40, 307–324. <https://doi.org/10.1016/j.jnca.2013.08.001>
- Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.
- Internet Crime Complaint Center (IC3). (2019). *2019 INTERNET CRIME REPORT*.
- Imperva. (n.d.). *Advanced persistent threat (APT)*. Retrieved February 13, 2021, from <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>
- Joint Chiefs of Staff. (2012, August). *CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL*.
- Kaspersky. (n.d.). *A Brief History of Computer Viruses & What the Future Holds*. Retrieved February 3, 2021, from <https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>
- Kick, J. (2014, November). *Cyber Exercise Playbook*. MITRE.
- Kulkarni, S., & Urolagin, S. (2012). Review of Attacks on Databases and Database Security Techniques. *International Journal of Emerging Technology and Advanced Engineering*, 2(11).
- Lockheed Martin. (n.d.). *The Cyber Kill Chain*. Retrieved May 6, 2021, from <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- Long, M. C. (2016). *Attack and Defend: Linux Privilege Escalation Techniques of 2016*. SANS Institute.
- Mavroeidis, V., & Bromander, S. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. *2017 European Intelligence and Security Informatics Conference (EISIC)*. <https://doi.org/10.1109/eisic.2017.20>
- Milevski, L. (2011). STUXNET AND STRATEGY A Special Operation in Cyberspace?. *Joint Force Quarterly*. 63.
- Ministry of Defence. (2021, June). *Red Teaming Handbook*. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/>

attachment_data/file/1027158/20210625-Red_Teaming_Handbook.pdf

MITRE & SANS. (2009, October). *2009 CWE/SANS Top 25 Most Dangerous Programming Errors*. MITRE Corporation.
https://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top_25.pdf

MITRE. (n.d.-a). *ATT&CK for Industrial Control Systems*. Retrieved March 21, 2022, from https://collaborate.mitre.org/attackics/index.php/Main_Page

MITRE. (n.d.-a). *CAPEC List Version 3.7*. Retrieved March 21, 2022, from <https://capec.mitre.org/data/index.html>

MITRE. (n.d.-a). *CAPEC VIEW: Domains of Attack*. Retrieved March 13, 2022, from <https://capec.mitre.org/data/definitions/3000.html>

MITRE. (2021, June 22). *CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses*. Retrieved March 13, 2022, from <https://cwe.mitre.org/data/definitions/1337.html>

MITRE. (n.d.-e). *Enterprise Techniques*. Retrieved March 21, 2022, from <https://attack.mitre.org/techniques/enterprise/>

Muckin, M., & Fitch, S. C. (2015). *A Threat-Driven Approach to Cyber Security Methodologies , Practices and Tools to Enable a Functionally Integrated Cyber Security Organization*. Lockheed Martin Corporation.

MITRE. (n.d.). *Corporate Overview*. Mitre. Retrieved March 7, 2022, from <https://www.mitre.org/about/corporate-overview>

Mochinaga, D. (2021, May 18). *JPCERT/CC participated in the Locked Shields 2021*. Jpcert. Retrieved March 7, 2022, from <https://blogs.jpCERT.or.jp/en/2021/05/locked-shields-2021.html>

National Cyber Security Centre. (2016). *Common Cyber Attacks: Reducing The Impact*.

National Cyber Security Centre. (2020, February 3). *Effective Steps to Cyber Exercise Creation*. Ncsc. Retrieved February 28, 2021, from <https://www.ncsc.gov.uk/guidance/effective-steps-to-cyber-exercise-creation>

National Institute of Standards and Technology. (2009, July 10). *White Team*. NIST. Retrieved March 5, 2021, from https://csrc.nist.gov/glossary/term/White_Team

NATO Cooperative Cyber Defence Centre of Excellence. (2021). *Locked Shields*. Ccdcoe. Retrieved March 14, 2021, from <https://ccdcoe.org/exercises/locked-shields/>

- OWASP. (2019). *OWASP API Security Top 10 2019 The Ten Most Critical API Security Risks*.
- OWASP. (2017). *OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks*.
- Ritu Sindhu, V. (2015). Network Security: Attacks, Tools and Techniques. *International Journal of Scientific Research and Management*, 3(5). Retrieved from <https://ijsrm.in/index.php/ijsrm/article/view/1020>
- Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70–94. <https://doi.org/10.1016/j.cose.2014.11.007>
- Sahrom Abu, M., Rahayu Selamat, S., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371. <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>
- Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September). *Technical Guide to Information Security Testing and Assessment* (No. 800–115). National Institute of Standards and Technology.
- Seker, E., & Ozbenli, H. H. (2018). *The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation*. 2018 *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. <https://doi.org/10.1109/cybersecpods.2018.8560673>
- Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). *ENISA Threat Landscape Report 2018*. ENISA.
- Skybox Security. (2018). *VULNERABILITY AND THREAT TRENDS: 2018 Mid-Year Update*.
- Theohary, C. A., & Rollins, J. W. (2015, March). *Cyberwarfare and Cyberterrorism: In Brief*. Congressional Research Service.
- Trend Micro. (n.d.). *APT Attack Sequence*. Retrieved March 8, 2022, from https://docs.trendmicro.com/all/ent/ddi/v5.1/en-us/ddi_5.1_olh/APT-Attack-Sequence.html
- Victoria State Government. (2019). *A Guide To Cyber Exercises*. <https://www.vic.gov.au/sites/default/files/2019-08/Vic-Gov-Cyber-Exercise-guide.pdf>
- Victorian Government. (2019). *A guide to cyber exercises*.

- Wood, P. (2018). Trends in Cyber Attack Vectors. *ITNOW*, 60(2), 40–41.
<https://doi.org/10.1093/itnow/bwy049>
- Yadav, T., & Rao, A. M. (2015). Technical Aspects of Cyber Kill Chain. *Communications in Computer and Information Science*, 438–452.
https://doi.org/10.1007/978-3-319-22915-7_40
- Zeidanloo, H.R., Tabatabaei, F., Amoli, P.V., & Tajpour, A. (2010). All About Malwares (Malicious Codes). *Security and Management*.



