sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXX No 3 2024

MODELING SCENARIOS COMBINING CYBER INTELLIGENCE PROCEDURES, METHODS, TECHNOLOGIES AND TECHNIQUES

Atanas ATANASOV*, Veselina GAGAMOVA*, Ivan HRISTOZOV*, Elitsa PAVLOVA**

***Rakovski National Defence College, Sofia, Bulgaria**
****University of National and World Economy/UNWE/, Sofia, Bulgaria**
a.atanasov@rndc.bg, v.gagamova@rndc.bg, ihristoz@rndc.bg, epavlova@unwe.bg

Abstract: *This paper presents the capabilities of specialized simulation software to develop a visual model that represents a cyber intelligence scenario. The architecture development method is applied to create an operational view for the tactics to conduct an intelligence attack by a team in the Computer Security Incident Response Centre in the structures related to crisis management and response. For this purpose, a prognostic scenario for reconnaissance attack tactics was developed using the toolkit of the simulation software, in which the Gather information about the victim's network techniques are applied.*

Keywords: Cyber Intelligence, Simulation Modelling, Scenario Architectural Approach intelligence Tactics

1. Introduction

For the design and construction of scenarios combining procedures, methods, technologies and techniques for cyberintelligence, the use of the architectural approach [1] is proposed, as well as simulation software for describing a scenario for intelligence attack tactics. This scenario is presented as an operational view. A cyber intelligence system's architecture operational view can be expressed through various frameworks. There are a number of specialized applications for modelling communication and information infrastructures and processes, including modelling cyber intelligence procedures, methods, technologies and techniques.

This paper proposes a technology using the simulation software toolkit to develop a scenario model for an intelligence attack such as gather information about the victim's network. The model is part of an architectural model of a cyber-intelligence system that includes the Computer Security Incident Response Centres (CSIRCs) in various organizational structures participating in the system.

For the development of the simulation model, the architectural approach is used, applying an architectural framework.

The model development is after an analysis of potential software applications and use the capabilities of a specialized environment for designing and building systems Sparx System Enterprise Architect [3]. The proposed architectural approach and software product for the development of the intelligence attack scenario model could be successfully applied to solving analogous tasks for the development of procedures, methods, technologies and techniques for cyber intelligence, as well as in solving the challenges of system

DOI: 10.2478/kbo-2024-0078

development in structures related to crisis management and response.

2. Capabilities for Developing Cyber Intelligence Scenario Modelling

The Enterprise Architect application presents a wide range of capabilities for modeling scenarios in the realm of cyber intelligence. It offers a diverse array of functionalities for modeling scenarios within the domain of cybersecurity as well as for designing and managing complex systems and architectures, including grouping, systematizing and analyzing cyber threats in cyberspace. Its purpose is to support various aspects of enterprise architecture, software engineering, and system modelling.

Its wide range of capabilities designed specifically for the modeling of scenarios makes it a valuable tool for software architects, systems engineers, business analysts and enterprise architects working on complex projects. In its latest versions, the tool has built-in functionality aimed at cybersecurity, and more specifically at analyzing and modelling threats in cyberspace. These new functionalities include:

- Creation of trust diagrams by scenarios; Identify and analyze potential threats using a threat modeling tool [2].
- Tracking threats and vulnerabilities to a given model;
- Create reports and reports using built-in functions for the purpose. Making recommendations on threat suppression measures;
- Sharing the threat model for collaboration;
- Validation of threat models and countermeasures, etc.

3. Model of Intelligence Scenario Where Gather Victim Network Information Techniques Are Applied

The Tactical Intelligence Scenario Model can be developed as an Operational View - OV-1 of the Cyber Intelligence System Architecture. Operational view (OV) encompasses a collection of interconnected components delineating the objectives, processes, personnel, and transmission and exchange of data necessary to facilitate intelligence attacks.

The operational view contains a description (often in graphic form) data flows necessary for the full implementation or maintenance of a given architecture.

In accordance with an architectural framework, an operational view as part of the operational architecture involves illustrating an intelligence scenario model.

The receipt or creation of the scenario is related to the provision of a graphic image of operations in terms of the following elements: missions (tasks), functions, activities, structural elements, organization and distribution of funds for strategic, operational and tactical level.

In Figure 1 a variant of Operational View OV-1 is presented, which shows the operational concept for the Reconnaissance tactic implemented by Gather Victim Network Information techniques. It was developed with Sparx Systems Enterprise Architect, a specialized system design and construction environment [4]. The operational view OV-1 is developed as a Use Case Diagram in the UML language.

According to the Use Case Diagram definition, the scenario model contains the main functions and activities of the Reconnaissance mission, together with the use case diagrams for the Gather Victim Network Information sub-technique through which it is implemented [5].

The main notations of the use case model are:

- The use case notation that represents a functionality or task, a procedure name,
- Actors – in this case, these are the expertise from the cyber intelligence team (white hats)
- Connectors – generally represent the connections and information flows between functions and officials.

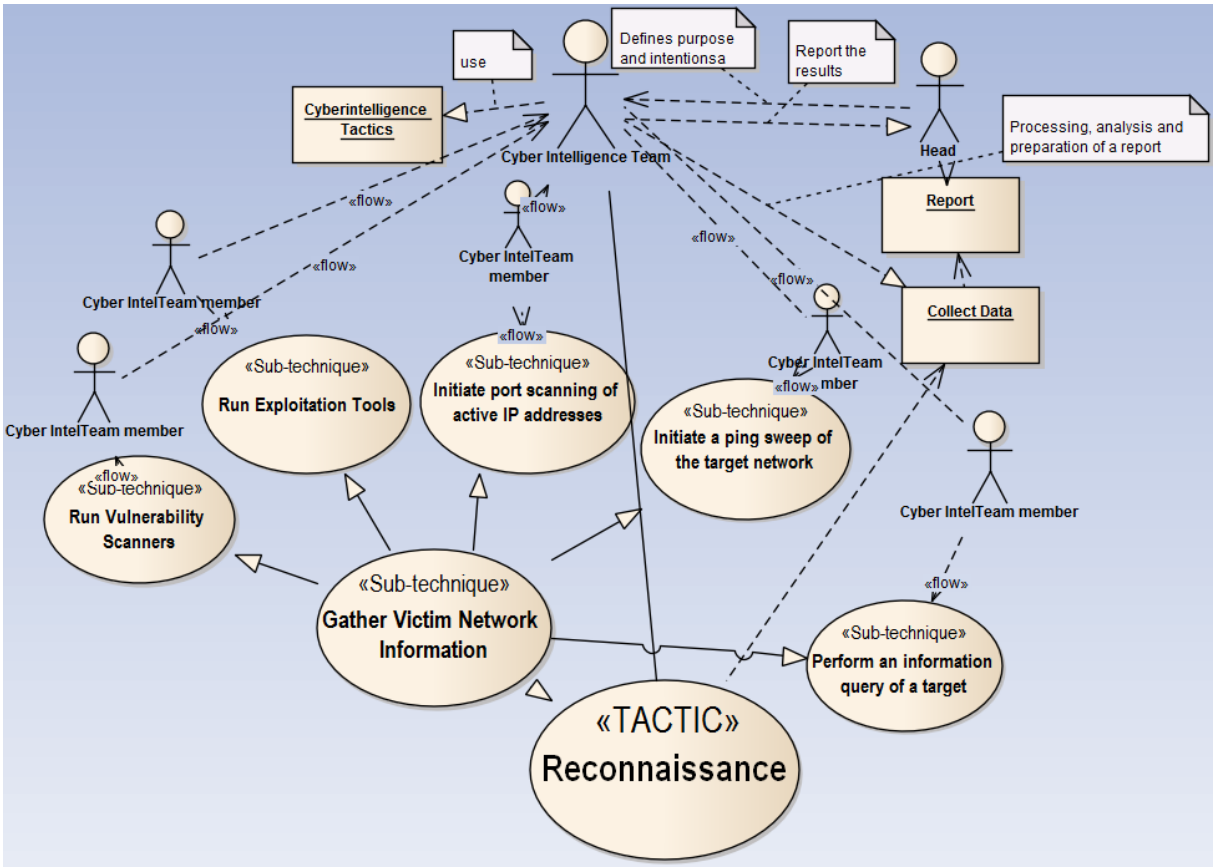

Figure 1: Operational View OV-1 Use Case "Reconnaissance" tactic implemented through Gather Victim Network Information techniques

In the developed reconnaissance scenario model, the use case Reconnaissance and use cases for the victim network information gathering techniques are developed.

Intelligence is generally about gathering information. As an association of the Reconnaissance tactic, we can imagine the tactic of a burglar in the homes of a residential neighbourhood. The thief will first look around the neighbourhood well, going from house to house in order to search homes that are for example, uninhabited, homes without video control, or a doorman.

One of the subtechniques of the Reconnaissance tactic is Gather Victim Network Information. Information about networks can include various details, including administrative data such as domain properties; DNS; different devices, their operations etc.

Techniques used for reconnaissance attacks are presented as use case notations that realize use case "Reconnaissance".

Sub-techniques Gather Victim Network Information performing reconnaissance attacks are the following:

- Search for preliminary data concerning a victim. This process may involve utilizing diverse software programs.
- Detect the IP address of the victim's network.
- Identify accessible ports or services.
- After finding the available ports, revealing the operating system and corresponding applications that are implemented on the device, as well as details for them.
- Run tools to detect exploitable vulnerable services. A port scan can be performed on the detected active IP addresses using Nmap.

4. Conclusions

In conclusion, from the conducted research it can be summarized that Enterprise Architect provides the necessary functionality for scenario modeling combining cyber intelligence procedures, methods, technologies and techniques. This proves and validates the applicability of DoDAF as a comprehensive organizational research tool.

It is concluded that the discussed frameworks and methodologies for cyber threat analysis can be applied through the Enterprise Architect software system in order to describe cyber intelligence procedures and develop scenarios for cyber threats in cyberspace. The application of threat modeling tools and cyber-intelligence processes, which are also used in NATO, is a prerequisite for the successful development of cyber-intelligence procedures interoperable with those of NATO member countries.

As a direction for future research, the development of specialized customized models for organizations, or adapting existing ones in order to meet specific cyber security requirements, can be indicated.

It can be summarized that the methods of simulation modeling and Architectural approach could be successfully used in the planning and development of cyberintelligence system.

Acknowledgements

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of October 21, 2021.

References List

[1] Popov P., Smilenova D., Vasileva V., Architectural Approach Usage in the Public Sector and Personal Data Protection, In: Proceedings of the 9th ICAICTSEE – 2019, Sofia, Bulgaria, pp. 125-135, ISSN 2367-7635

[2] Microsoft, 2022. Microsoft Threat Modeling Tool. [Online] Available on: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

[3] Sparx Systems, 2007. Using UML part one – Structural Modeling Diagrams. [Online] Available at: www.sparxsystems.com Sparx Systems, 2007.

[4] Sparx Systems, 2007. Using UML part two – Behavioral Modeling Diagrams. [Online] Available at: www.sparxsystems.com

[5] MITRE ATT&CK, Available on: https://attack.mitre.org/techniques/T1590