5ta Jornada de Ciberseguridad de la Universidad Nacional de Colombia

EVALUATING A BREACH ATTACK SIMULATION PLATFORM (BAS) THROUGH A FUNCTIONAL AND INDUSTRY-BASED APPROACH

Abstract

This project evaluates the MITRE Caldera tool as a cybersecurity attack simulation solution, using Red and Blue agents along with various plugins to emulate tactical techniques and attack procedures included in the MITRE ATT&CK framework. Strengths were identified, such as the visualization of the attacker's capability through the aforementioned framework with the use of the Compass plugin and the integration of agents with Metasploit framework attacks through the Access plugin. Additionally, a review was made of the criteria seen in the article "Picus-ten criteria for choosing the right BAS solution" defined by the manufacturer Picus, where it was found that Caldera does not meet those criteria related to: simulation of initial access attacks, constant update of attacks, validation and customization of detection rules, customization of threats and reports and mitigation perspectives.Finally, a set of improvement opportunities that could be applicable to Caldera is proposed.

Introduction

In the global landscape cybersecurity is a critical priority for organizations that need to proactively assess their defenses against cyber threats, this because every day there are new cyber attacks using new tactics and techniques, this leads us to the BAS that we mentioned earlier allows us to be constantly evaluating the architecture to test new attacks that are discovered in the market to see if your infrastructure is vulnerable or not.

Background

Breach Attack Simulators (BAS), such as Mitre Caldera, offer an advantage by emulating real cyber attack tactics to continuously assess the security of organizations. Based on MITRE's ATT&CK framework, these simulators allow mapping Techniques, Tactics and Procedures (TTP) of real adversaries, helping to identify existing vulnerabilities in an enterprise environment in advance.

Unlike traditional solutions, BAS detect advanced threats in real time, adapt to infrastructure changes and provide actionable data to strengthen the security posture against emerging attacks. Because BASs are very new platforms in the cybersecurity landscape, there are still not enough evaluation mechanisms suitable for this type of platform.

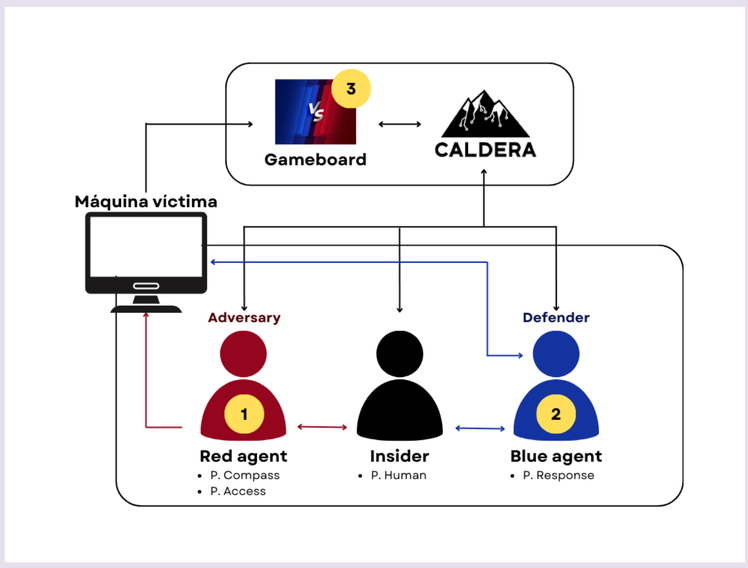
Proposal

It is proposed to perform attack simulations using the BAS Mitre Caldera platform, through which its capabilities, functionalities and limitations will be evaluated. A detailed analysis of plugins available for Caldera such as Mock, Human, GameBoard and Response is also carried out. Finally, Caldera is evaluated according to the picus-ten criteria for choosing the right BAS solution, including: coverage of Mitre's ATT&CK framework, integration with existing security systems, quality of reports, ease of implementation and scalability, to determine its usefulness in enterprise environments.

Picus-ten Criteria	
Criterion	**Description**
Criterion 1	Threat simulation throughout the attack lifecycle
Criterion 2	Update on current and emerging threats
Criterion 3	Validation of the company's security controls
Criterion 4	Continuous and automated simulation
Criterion 5	Validation of detection rules
Criterion 6	Threat customization
Criterion 7	Actionable and direct mitigation insights
Criterion 8	Customizable and real-time reports
Criterion 9	Mapping to MITRE ATT&CK and other frameworks
Criterion 10	Ease of use

Experiments

Evaluation of functionalities:



Agent / Element	Description
Red Agent	Use the Compass and Access plugins to execute attacks.
Blue Agent	Use the Response plugin to defend and mitigate attacks.
Human Agent	Simulate activities of a legitimate user, generating noise and complicating detection.
Gameboard	Manage the interaction between agents and evaluate their effectiveness in a controlled attack and defense environment.
Plugins	They provide functions such as: - Visualization of the MITRE ATT&CK matrix (Compass). - Integration with Metasploit (Access). - Incident response (Response). - Noise simulation (Human).

Evaluation of criteria:

Picus-ten Criteria	
Criterion	**Description**
Criterion 1	Focused on post-compromise attacks (requires an agent to be installed)
Criterion 2	Limited to the libraries created and uploaded by MITRE
Criterion 3	It does not have this feature
Criterion 4	It focuses on that
Criterion 5	It does not have this feature
Criterion 6	It does not have this feature
Criterion 7	It does not have this feature
Criterion 8	Creates a generalized report
Criterion 9	It has a dedicated plugin (COMPASS)
Criterion 10	Usable but presents difficulty in extending or customizing due to documentation issues

Conclusions

Mitre Caldera offers valuable functionality as an open source BAS solution, which makes it attractive, especially for SME-type organizations that need a basic and flexible tool to simulate attacks and evaluate their security posture. However, its limited documentation makes it difficult to take full advantage of its capabilities, as is the case with the Gameboard plugin, which could not be used in the experiment due to lack of documentation. On the other hand, Mitre Caldera does not meet 4 of the criteria established by Picus and other 4 criteria are partially met, which may cause it to lag behind other more advanced solutions in the market. Finally, the following improvement opportunities are identified for Mitre Caldera: i) generation of customized reports adapted to the different roles within a company, ii) integration of a cybersecurity controls recommendation system, which allows mitigating the vulnerabilities detected, facilitating informed decision making.

References

1. BBVA: La ia, en los dos lados de la ciberseguridad: aliada y amenaza en el mundo digital (2024)
2. Desplanques, B., Thienpondt, J., Demuynck, K.: ECAPA-TDNN: emphasized channel attention, propagation and aggregation in TDNN based speaker verification.(2020)
3. Kaspersky: Investigación de kaspersky confirma que tales violaciones son casi tan comunes como las brechas de ciberseguridad (2023)

Autor(es)

Juan Contreras, Laura Salazar, Daniel Díaz-López
Matemáticas Aplicadas y Ciencias de la Computación (MACC)
Escuela de Ingeniería, Ciencia y Tecnología (EICT)
Universidad del Rosario

Organiza

Universidad Nacional de Colombia
Grupo de investigación UNsecureLab
Semillero de investigación Uqbar
Grupo de investigacion Tlön

UNIVERSIDAD NACIONAL DE COLOMBIA