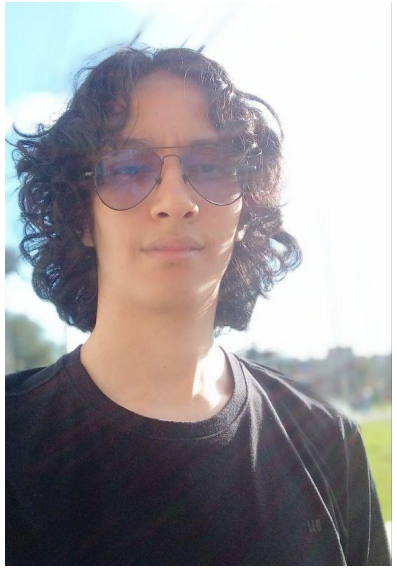
Analyzing capacities and drawbacks of Breach Attack Simulation (BAS) solutions

Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación

BSIDES Cybersecurity conference
Medellín, Colombia, April 27th ,2024



Nicolas David Rogers

Cybersecurity researcher. Professional in Applied Mathematics and Computer Science (c), School of Engineering, Science and Technology
Universidad del Rosario

nicolas.rogers@urosario.edu.co

Juan Daniel Casanova

Ethical Hacker. Professional in Applied Mathematics and Computer Science (c), School of Engineering, Science and Technology
Universidad del Rosario

juan.casanova@urosario.edu.co

Daniel Díaz, PhD

Cybersecurity researcher.
School of Engineering, Science and Technology
Universidad del Rosario

danielo.diaz@urosario.edu.co

Carlos Castañeda, PhD

Cybersecurity Entrepreneur
Serval Networks

carlos.castanneda@gmail.com

Agenda

1. What is BAS?
2. Most popular BAS Platforms
3. 10 Comparison Criteria and Results
4. Attacking with Caldera
5. Attacking with Keysight
6. Some thoughts

I. What is Breach and Attack Simulation (BAS)?

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Offensive security method

Integrate automated security tools + human intervention

Automate TTPs

TTPs (Tactics, Techniques and Procedures) included in MITRE and NVD

Execute different type of attacks

Web, data exfiltration, email-based, abuse, lateral movement, etc

Test security at different layers

Apps, network, cloud, containers, endpoints

Discover fails in security controls

Vulnerability scanners, malicious traffic detectors (IPS/IDS), IAM engines, data protectors, correlators (SIEM)

I. What is BAS?

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

	BAS	Pentesting
Type of test	**Automated** procedures	**Manual** procedures
Continuity	May be **continuous**	Every 3 or 6 months (?) **Frequency** depends on contract
Exposition window	Automation of technique may **take a time** to be incorporated in a BAS' attack database	**Almost immediate** manual validation of new techniques
Scope	**L1:** Capacity to analyze security of the virtual machine, server or PC where the agent is installed	Capacity to: ● Analyze security of **virtual machines, servers, PC's, perimeter security devices**. ● Generate **external/(internal?) attacks** ● Provide overview of **input vectors**
	L2: L1 + Capacity to generate internal attacks [MITRE]	
	L3: L2 + Capacity to generate external attacks [MITRE]	
	L4: L3 + Capacity to provide overview of input vectors	
Precission	May have **false positives**	May have **false negatives**

II. Most popular BAS Platforms

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

ATTACKIQ

- **Ease of use and deployment:**
  On cloud or On Premise
- **Real-World Attack Simulation**
  Yes, but limited to EDR (Endpoint)
- **Remediation and Recommendations**
  Basic recommendations*
- **Threat Intelligence**
  Yes, 3 sources: MITRE, CrowdStrike and Red Canary
- **Price & Packaging**
  $5,000 per Test Point Engine

SafeBreach

- **Ease of Use and Deployment:** external adversaries and a virtual appliances. On-cloud and on-premise
- **Real-World Attack Simulation:** Uses packet replay for network-based attacks.
  Supports kill-chain simulations with NDR and EDR techniques.
- **Remediation and Recommendations:** Basic remediations for EDR security controls.
- **Threat Intelligence:** Database of TI with 5+ years of security research
- **Price & Packaging:**
  $70K for 3 endpoints,
  $5K for additional endpoints each

II. Most popular BAS Platforms

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Cymulate

Breach & Attack Simulation

- **Ease of Use and Deployment: Fast and easy deployment**, delivering insights within minutes after the setup is completed.
- **Real-World Attack Simulation:** Supports **agent-less attack simulation** and has a well-diversified library of attack vectors and techniques, including **NDR, EDR, and email. WAF attacks** are conducted agentless and are targeted directly.
- **Remediation and Recommendations:** Remediations are considered **basic** relative to competitors, with limited EDR support.
- **Threat Intelligence:** Founded in 2016, its leadership includes individuals with IDF backgrounds, and the team actively looks for **new vulnerabilities** while also monitoring **emerging threats.**
- **Price & Packaging:** Prices start at $40,000 and scale based on company size, the number of attack vectors, and the number of assessments per year.

PICUS

- **Ease of Use and Deployment:** Requires a longer **setup time** (hours), but once operational, provides immediate insights.
- **Real-World Attack Simulation:** Offers realistic **simulations** focused on **NDR** but is **limited to HTTP/HTTPS protocols** and also validates EDR and email security controls.
- **Remediation and Recommendations:** Delivers a subset of the recommendations that other tools like Threat Simulator provide.
- **Threat Intelligence: Uses third-party** threat intelligence feeds. The company keeps the location of their main development and research center private.
- **Price & Packaging:** Pricing begins at $50,000 for two endpoints

II. Most popular BAS Platforms

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

KEYSIGHT TECHNOLOGIES | THREAT SIMULATOR

- **Ease of Use and Deployment:** Operates as a **SaaS platform** for quick scenario deployment and rapid insights.
- **Real-World Attack Simulation:** Specializes in **simulating NDR security** scenarios and is developing capabilities for **EDR and email.**
- **Remediation and Recommendations:** Offers **recommendations** across **security controls** and best practices.
- **Threat Intelligence:** managing a database that catalogs **known and emerging threats.**
- **Price & Packaging:** Available from $60,000 annually for a package of five agents, with scalable options.

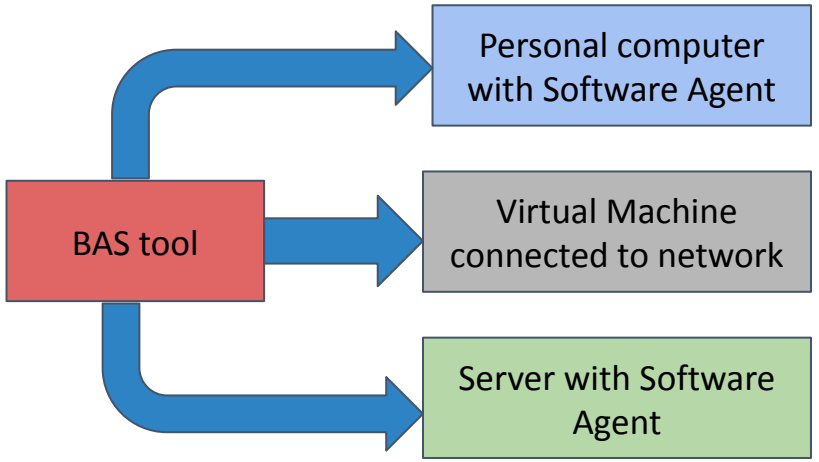
CALDERA

- **Ease of Use and Deployment:** CALDERA is designed for straightforward deployment, suitable for **various operational environments** due to its **open-source** nature.
- **Real-World Attack Simulation:** The tool focuses on emulating **adversary behaviors** using the MITRE ATT&CK framework to inform its simulation strategies.
- **Remediation and Recommendations:** Provides f**eedback on security posture**, suggesting improvements based on simulation outcomes.
- **Threat Intelligence:** Utilizes the extensive **ATT&CK framework** which is regularly updated with the latest threat intelligence by the cybersecurity community.
- **Price & Packaging:** As an open-source tool, it is available without direct cost, fostering accessibility for a wide range of users and organizations.

III. 10 Comparison Criteria and Results

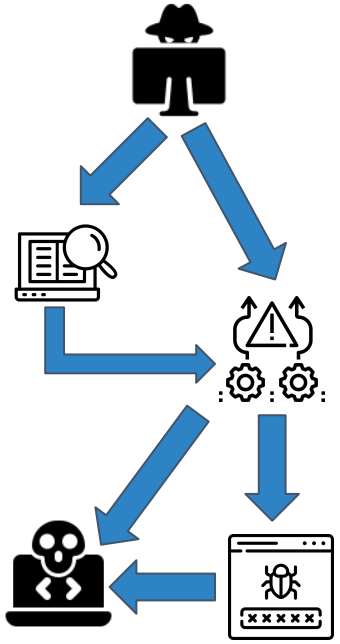
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

1. Mechanism used in the simulation.



Simulate

Emulate

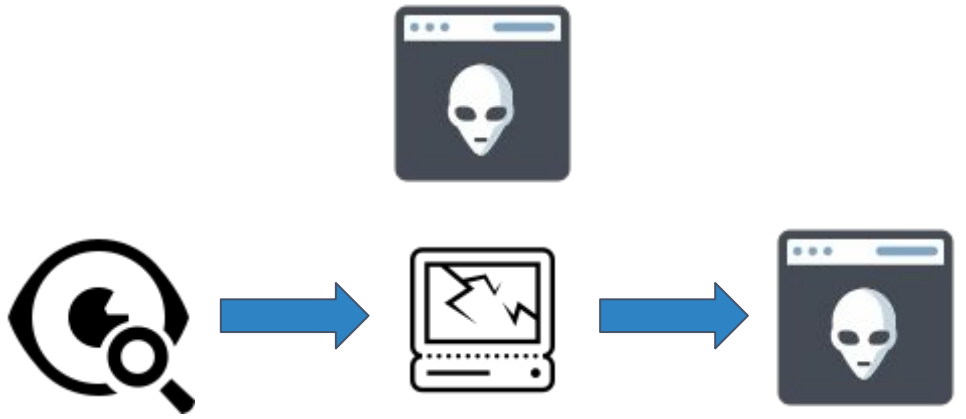


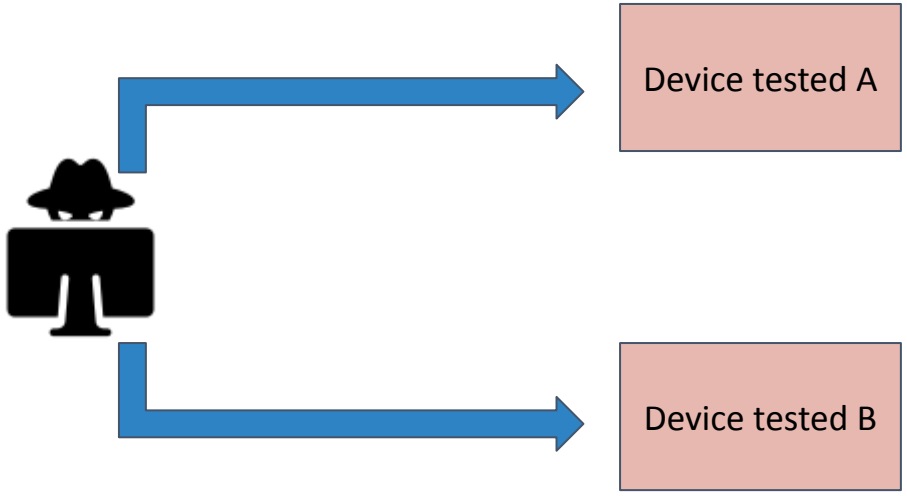
2. Simulate or emulate adversary campaigns

III. 10 Comparison Criteria and Results

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

3. Single or multi stage attacks

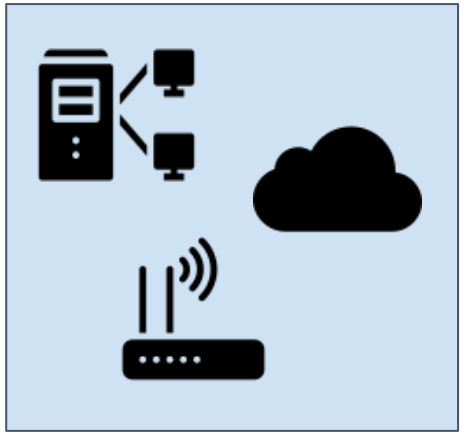


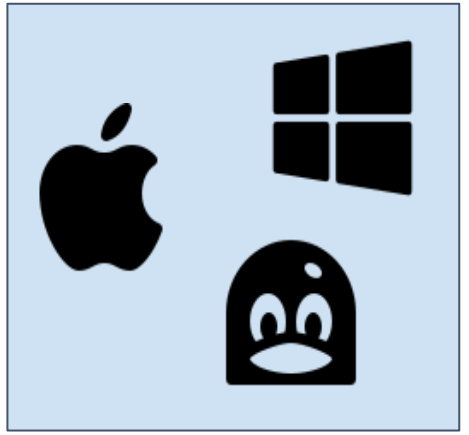


4. Concurrent attacks

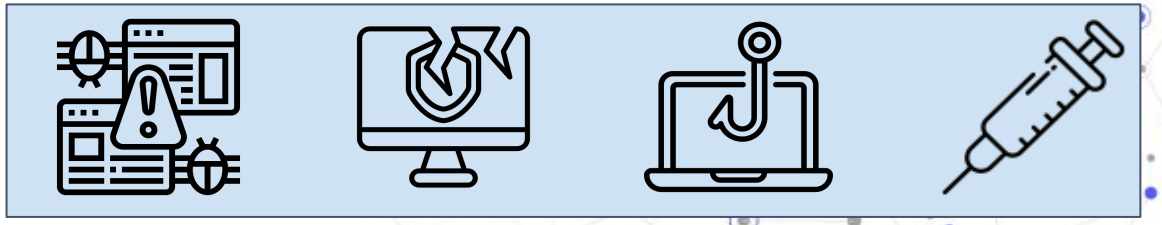
III. 10 Comparison Criteria and Results

5. Implemented MITRE TTPs





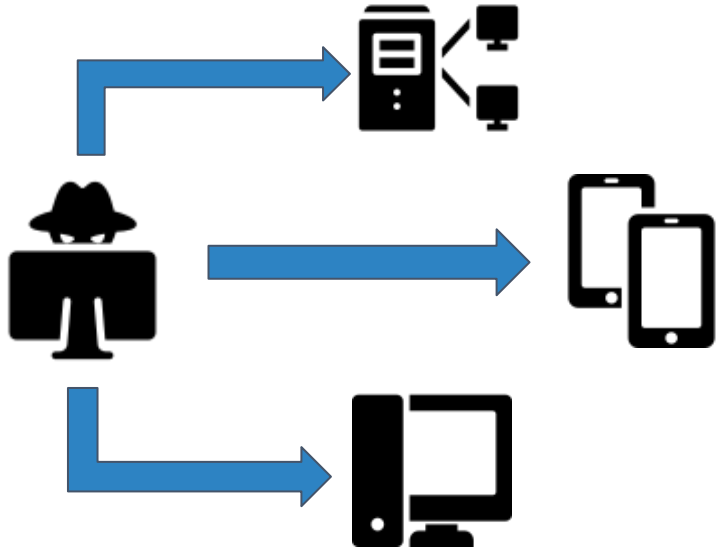
6.Kind of supported attacks



III. 10 Comparison Criteria and Results

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

7. Kind of assets supported to be tested



8. Quality of the report

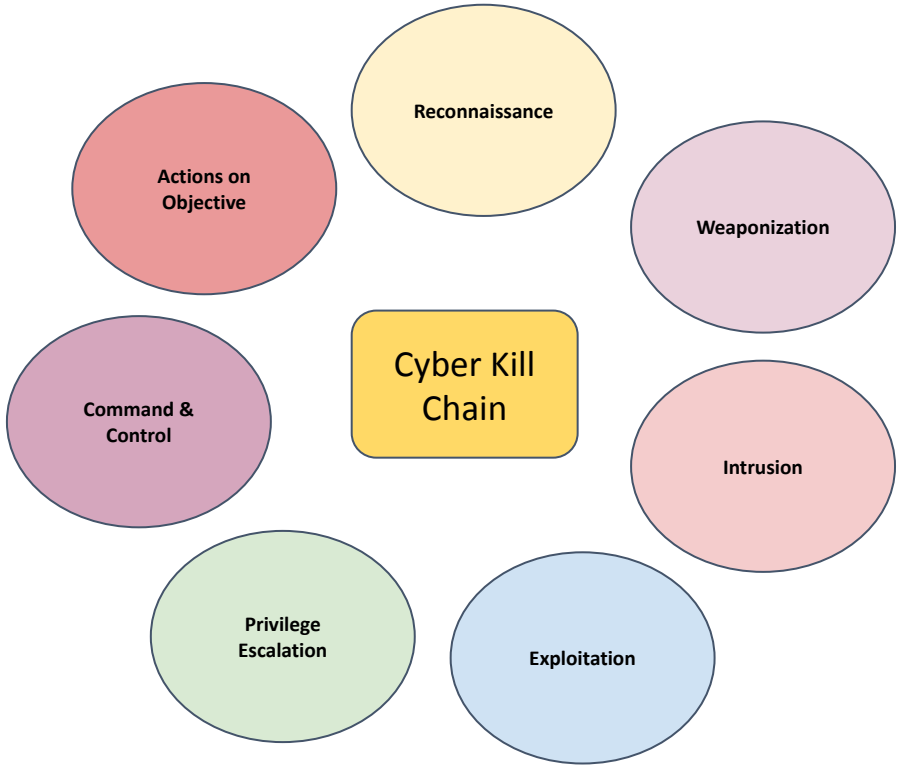
III. 10 Comparison Criteria and Results

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

9. Metrics for vulnerabilities

10.0 - 9.0	Critical
8.9 - 7.0	High
6.9 - 4.0	Medium
3.9 - 0.1	Low
0	None

CVSS
CVE
VPR



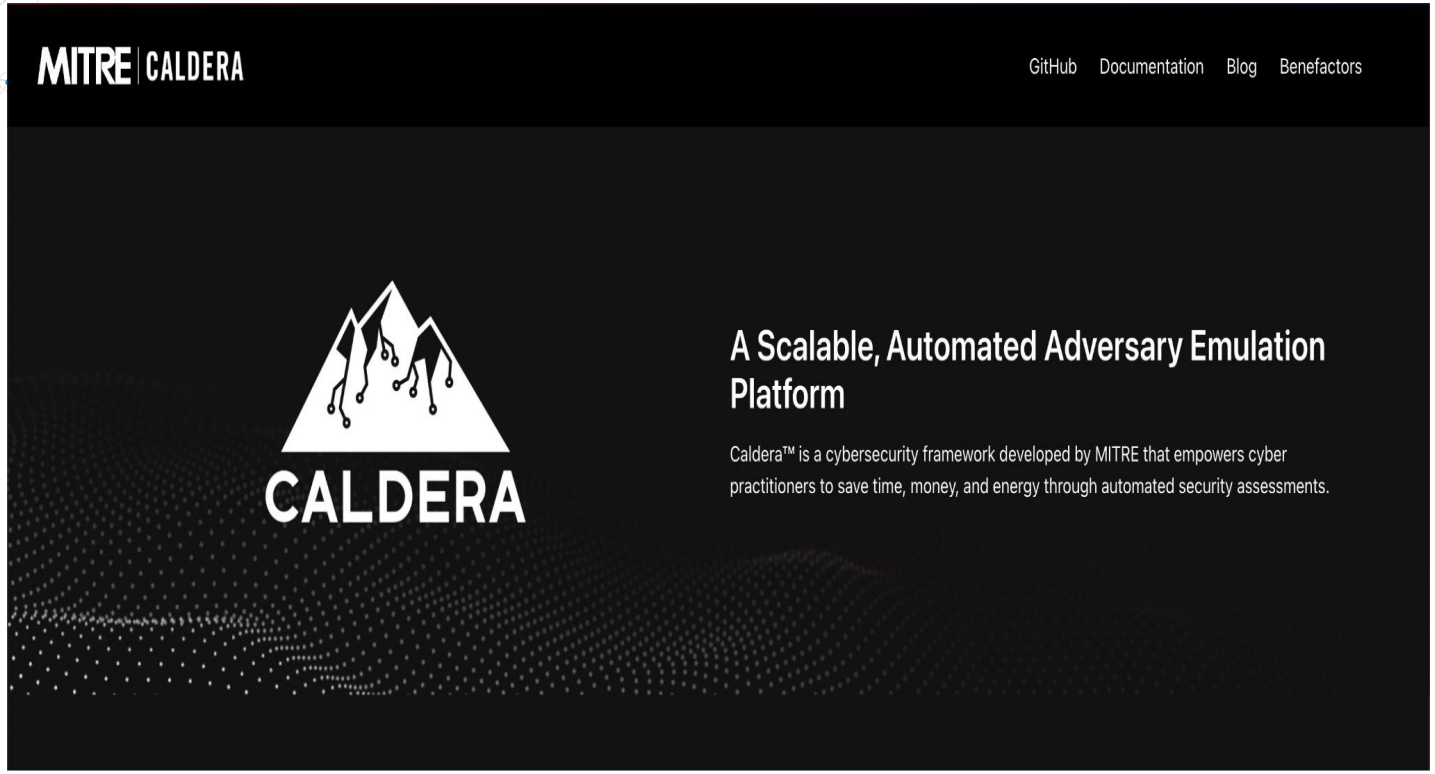
10. Attack Cycle

III. 10 Comparison Criteria and Results

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

	Caldera	Keysight
Mechanism used in the simulation	**Software Agent**. **Virtual Machines.**	**Software Agent.** **Virtual Machines.**
Simulate or emulate adversary campaigns	**Emulate.**	**Simulate.**
Single or multi stage attacks	**Single stage attack.** **Multi stage attacks.**	**Single stage attack.** **Multi stage attacks.**
Concurrent attacks	**Single attack**.	**Single attack.** **Multiple attacks: The platform can launch until 100 simultaneous attacks.**
Implemented MITRE TTPs	**Implement all the MITRE TTPs**	**Implemente all the MITRE TTPs**
Kind of supported attacks	**Network attack.** **OS attack.** **Cloud attack.**	**Network attack.** **OS attack.** **Email Assessments.** **Web Attack.**
Kind of assets supported to be tested	**Network devices.** **Servers.** **Personal Computers.**	**Network devices.** **Servers.** **Personal Computers.**
Quality of the report	**Overall detection, vulnerability, prevention and audits percentage.** **Recommendations for prevent each vulnerability detected.** **Details about the vulnerabilities found.**	**Overall detection, vulnerability, prevention and audits percentage.** **Recommendations for prevent each vulnerability detected.** **Details about the vulnerabilities found.**
Metrics for vulnerabilities	**Use metrics MITRE CVE.**	**Use metrics CVE.** **App use its own judgment.**
Attack Cycle	**Implement all the Cyber Kill Chain.**	**Implement all the Cyber Kill Chain.**

Attacking with Caldera



https://caldera.mitre.org/

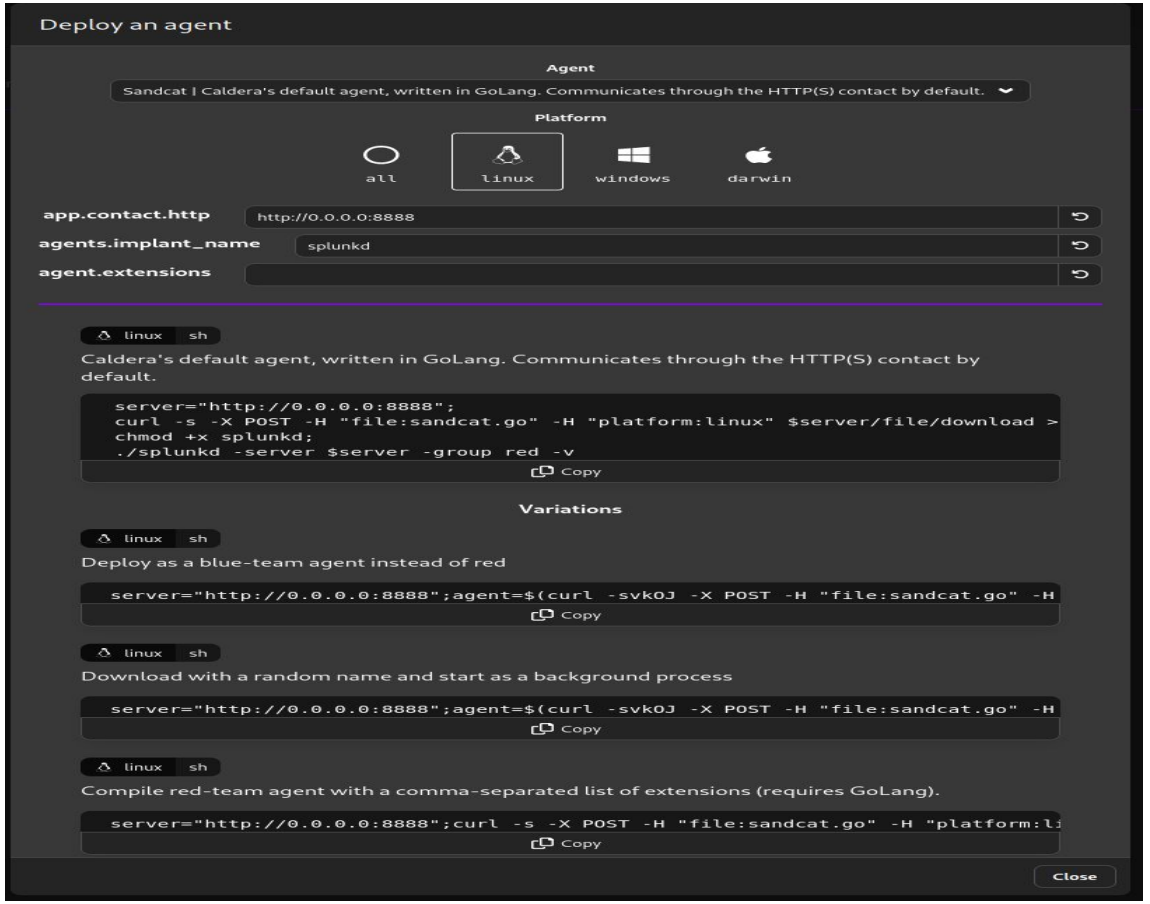
- CALDERA is an **open-source** tool for automating adversary emulation.
- It allows organizations to **assess** and improve their defenses against cyber threats.
- leverages the **MITRE ATT&CK framework** to simulate **real-world cyber attacks**, providing a dynamic testing environment.
- The primary goal is to identify **vulnerabilities and defensive gaps** in network security before an actual cyber attack occurs.

AGENTS

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Agents are deployed on target systems to execute actions as directed by the server. These agents simulate the steps an attacker would take in a real-world scenario.
there are 3 kind of agents:

- Sandcat : https
- Ragdoll : python
- manx : tcp



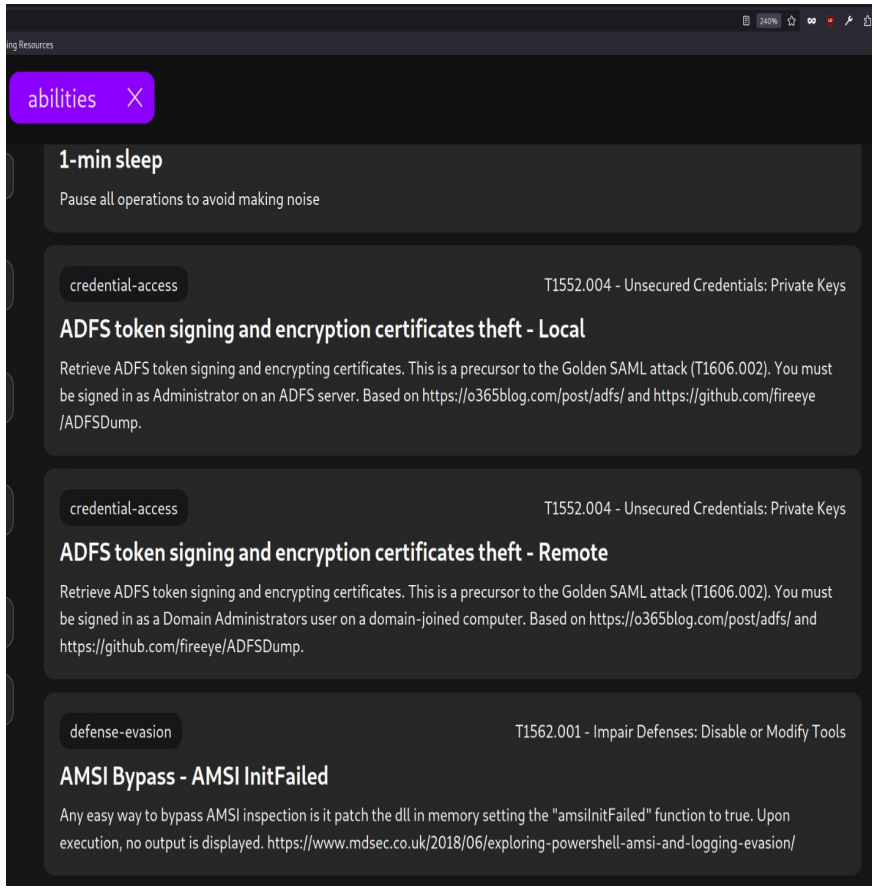
id (paw)	host	group	platform	contact	pid	privilege	status	last seen	
xoikzr	parrot	red	linux	HTTP	36473	User	alive, trusted	4/26/2024, 5:11:12 AM	×
pltlhf	parrot	red	linux	html	36506	User	alive, trusted	4/26/2024, 5:11:01 AM	×

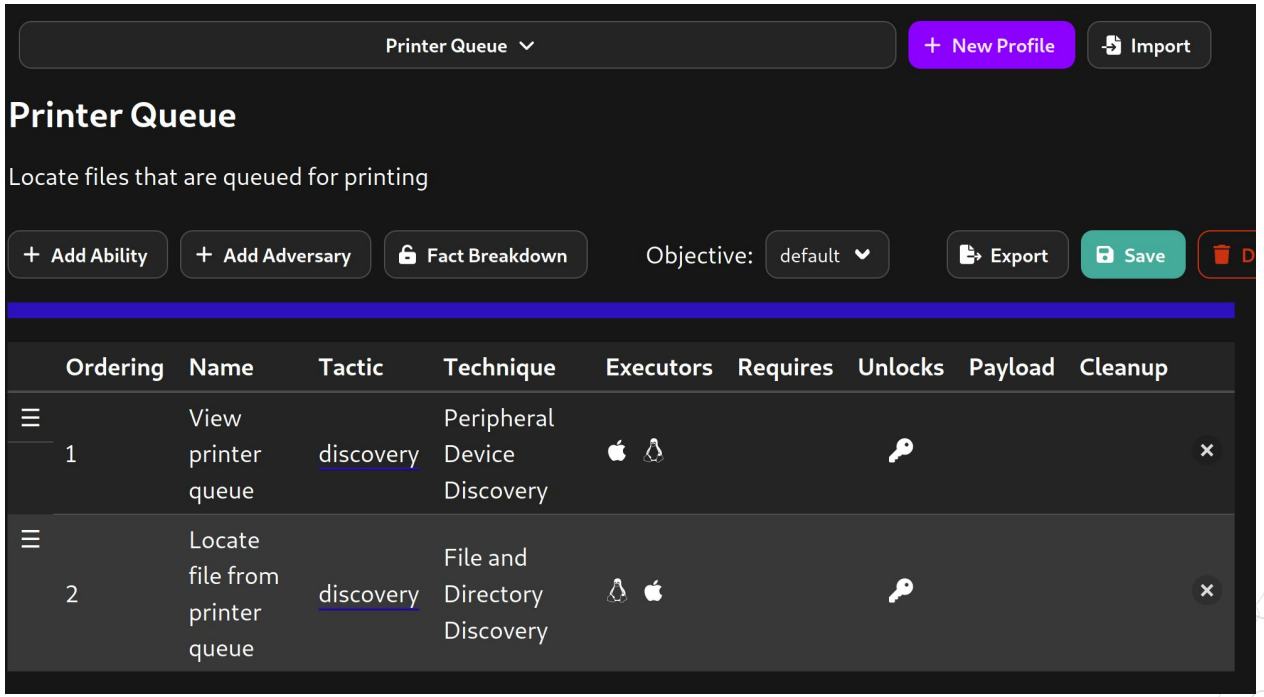
ADVERSARIES

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Abilities are specific actions that adversaries can perform during an emulation.

Adversaries are defined as profiles that specify certain types of attack behaviors.





Planning and Configuration

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

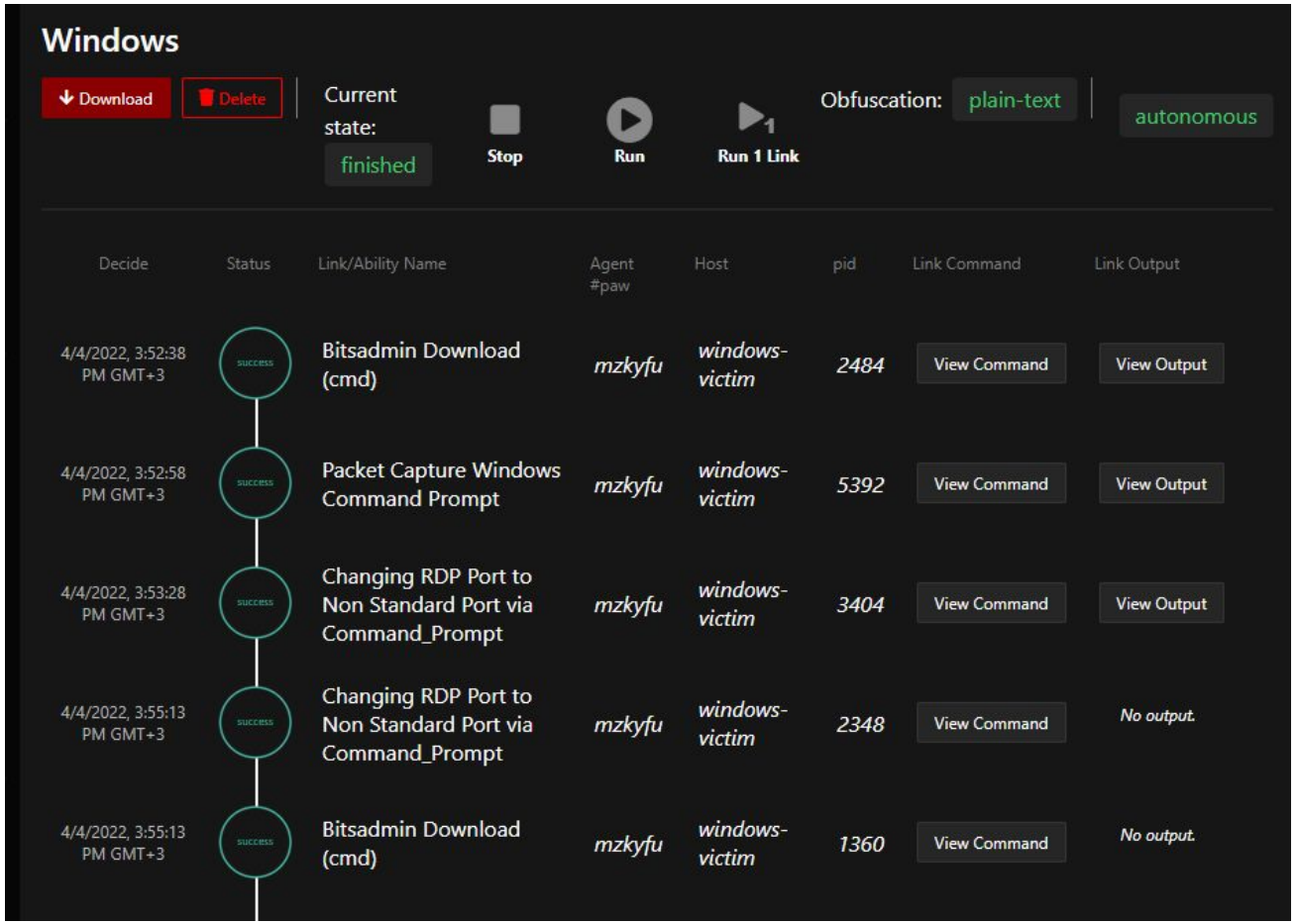
Users start by defining the objectives and scope of the emulation, selecting specific adversary behaviors from the MITRE ATT&CK matrix to simulate.

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
4/26/2024, 5:17:44 AM UTC	success	Identify active user	discovery	xoikzr	parrot	36575	View Command	View Output
4/26/2024, 5:17:44 AM UTC	success	Identify active user	discovery	jayucy	parrot	36572	View Command	View Output
4/26/2024, 5:17:59 AM UTC	success	Find local users	discovery	xoikzr	parrot	36618	View Command	View Output
4/26/2024, 5:17:59 AM UTC	success	Find local users	discovery	jayucy	parrot	36614	View Command	View Output
4/26/2024, 5:18:54 AM UTC	collect	Find user processes	discovery	xoikzr	parrot	N/A	View Command	No output
4/26/2024, 5:18:54 AM UTC	collect	Find user processes	discovery	jayucy	parrot	N/A	View Command	No output

Execution of Attack Scenarios

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

CALDERA executes the planned attack paths using its agents to carry out actions that mimic those of an actual attacker, testing the effectiveness of network defenses.



DEMO TEST CASE

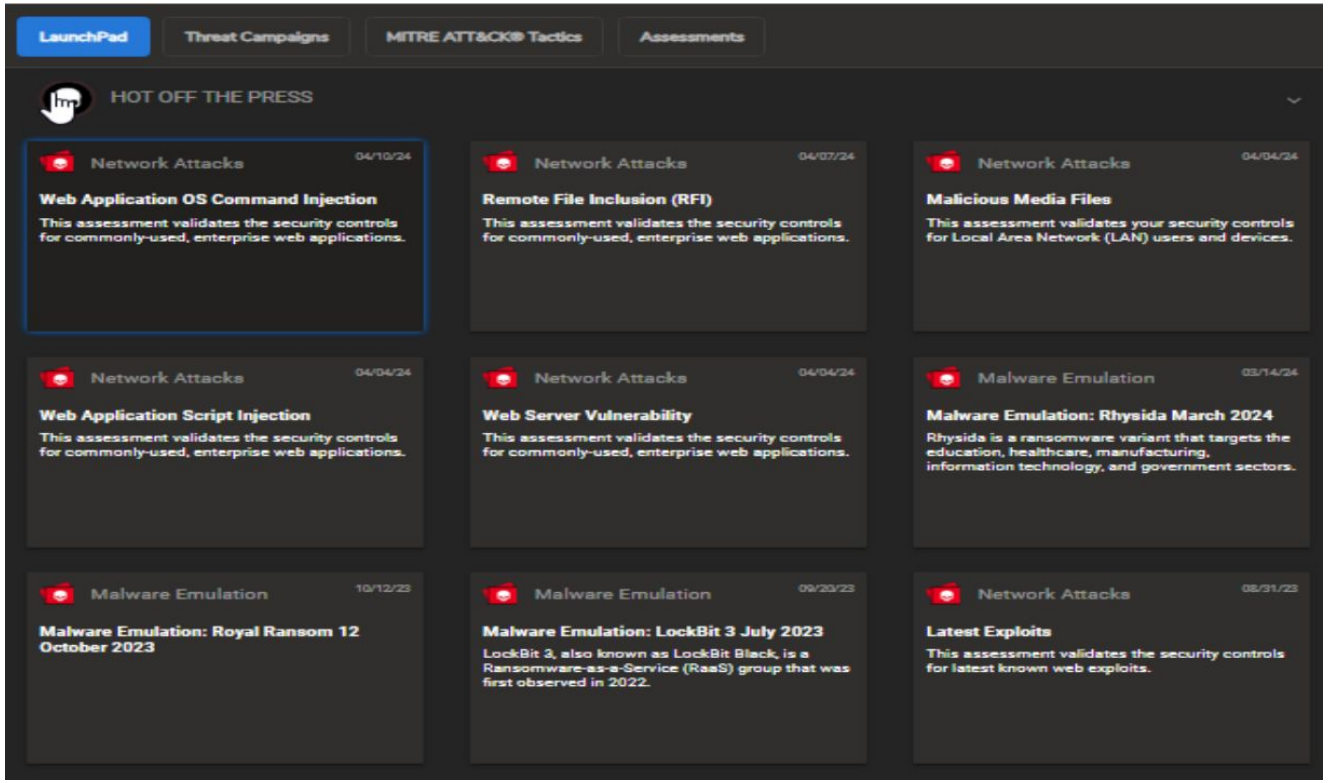
https://www.youtube.com/watch?v=ygSnh_OAPbg

Attacking with Keysight

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

KEYSIGHT

- KEYSIGHT provides multiple self-designed tests.
- Offers vulnerability testing based on real attacks and how they were carried out.
- The tool allows you to generate your own TTPs based on the MITRE table.

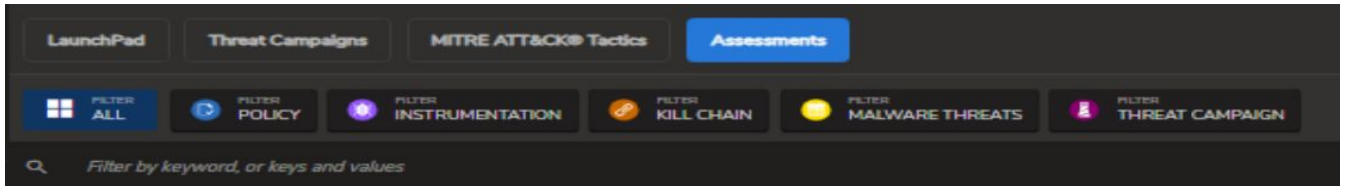


https://threatsimulator.cloud/security/assessments/launchpad

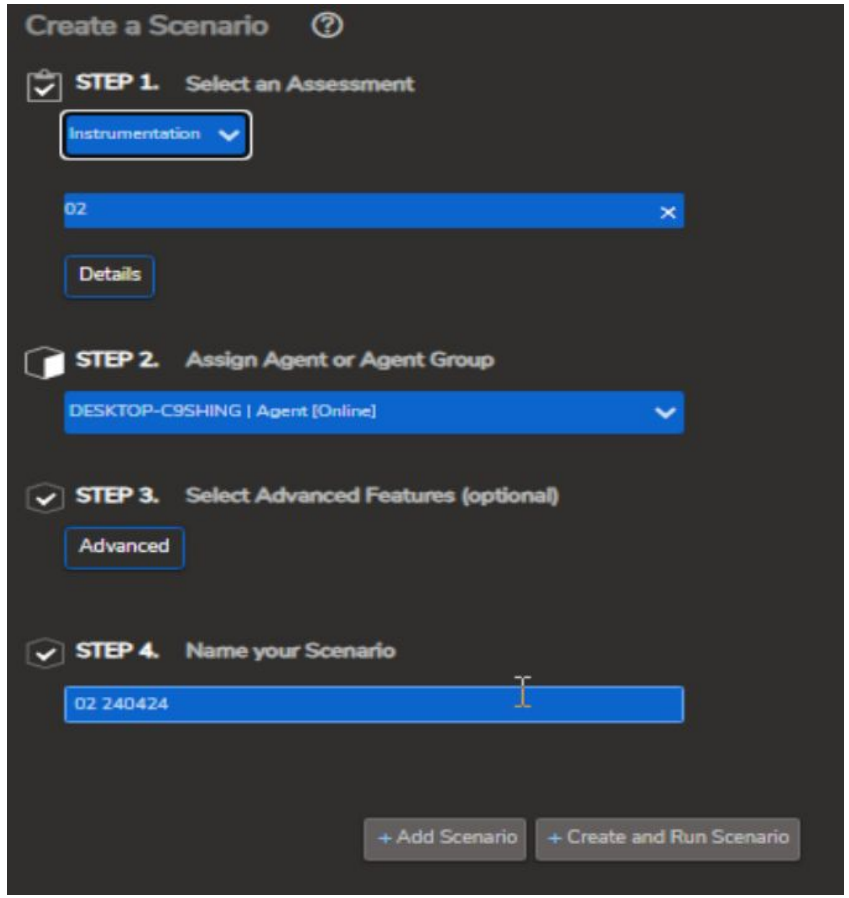
Attacking with Keysight

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- In the scenarios section, the techniques and techniques allowed by the platform are implemented.
- Assessments are the vulnerability campaigns implemented by the user or by the platform.



https://threatsimulator.cloud/security/assessments/assessments-profiles



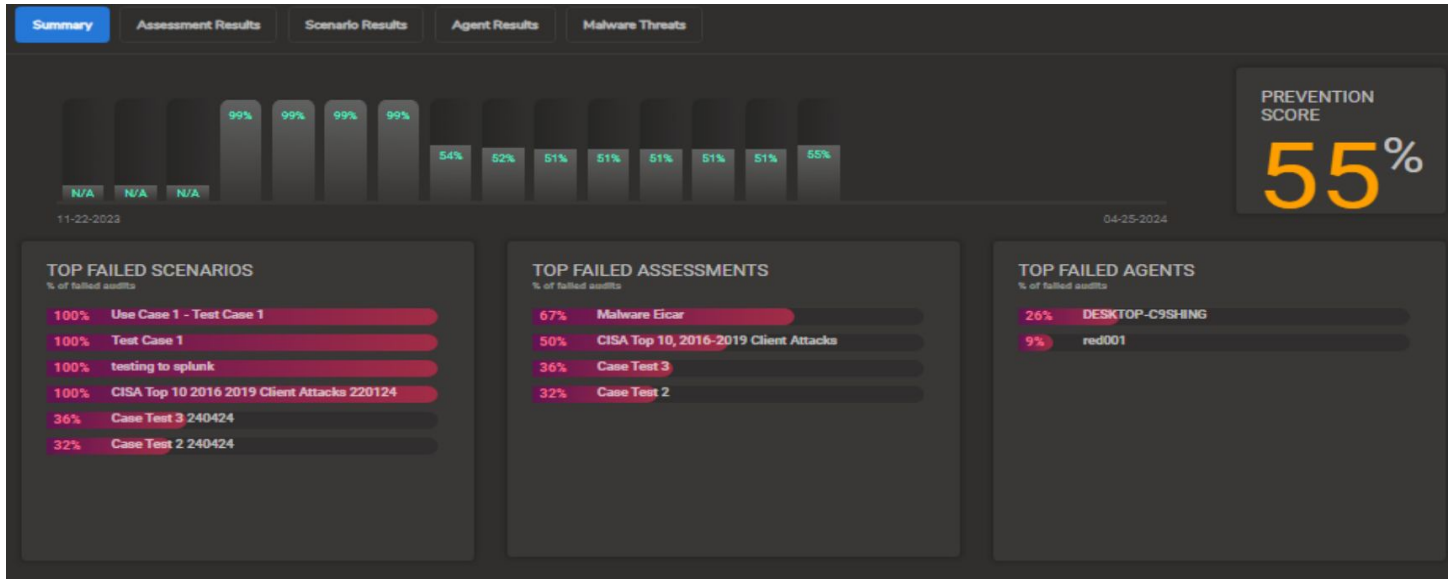
https://threatsimulator.cloud/security/scenarios

Attacking with Keysight

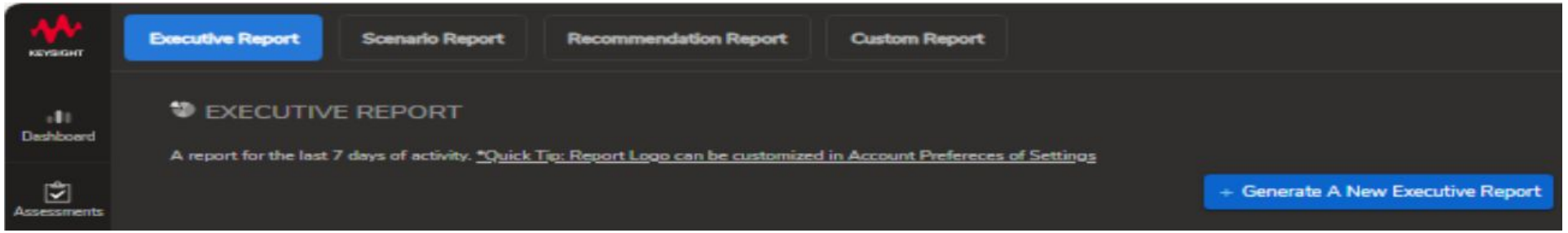
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- The tool allows you to generate different types of reports in which it offers details about the four types of reports (Executive, Scenario, Recommendation and Custom).

- The platform gives a general summary of the results obtained in all the tests carried out. Also, give the results from each scenario executed.



https://threatsimulator.cloud/security/dashboard



https://threatsimulator.cloud/security/reports

DEMO TEST CASE

https://youtu.be/MRhPaT8lHJU

Some thoughts

Diversity	The wide diversity in deepness/scope/quality between BAS platforms makes us think twice before choosing one
Mitigation	As in the traditional pentesting, it is quite important to breach as to mitigate, so a BAS method has to be “followed” by a proper mitigation strategy
Duo	A combination of automated + manual testing may allow to identification of already-known breaches and newborn security breaches
First Approach	Caldera is a quite efficient entry-level BAS platform, which additionally is open source, allowing more SMEs may adopt a BAS-supported security strategy

Questions?