

ADVANCED ETHICAL HACKING - COMP 4077

AEH Group Assignment

CALDERA™ is a cyber security platform designed to easily automate adversary emulation, assist manual red-teams, and automate incident response. It is built on the MITRE ATT&CK™ framework and is an active research project at MITRE.

The task for your group is to research and implement this tool in your environment and show values to the team. Please do the following

1. Research on Caldera, explain in your own word, what is it? How can you install it? What benefit can the tool brings on to your company? How do you use it? (5 marks)

Installation of caldera on Linux.

Group Members

Samuel Adeshina. 101501091

Alina Josekutty 101509790

Mohamad Almasri 101167438

Omar Farooq 101486546

Akinbode Oluwademilade 101431512

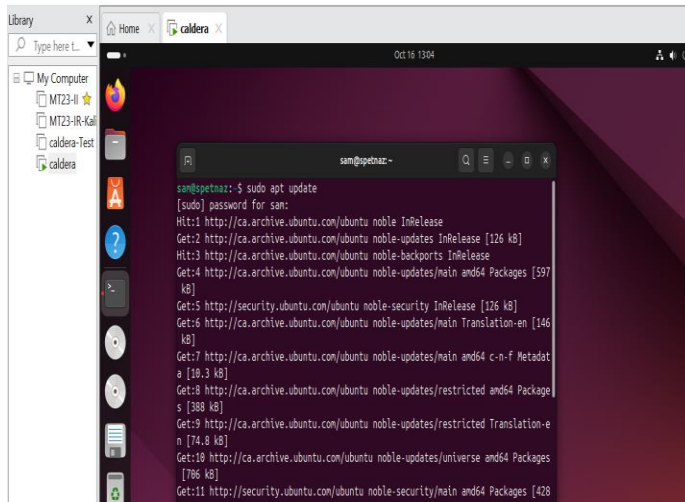
CALDERA

CALDERA is an open-source cybersecurity tool by MITRE that automates adversary emulation to test defenses based on the MITRE ATT&CK framework. For realistic attack tests, agents are loaded onto target machines to conduct the simulated attack; therefore, an organization may test and improve its security posture. Prebuilt and customizable attack profiles provided with CALDERA can assist in locating weaknesses, test detection, and refine response capabilities.

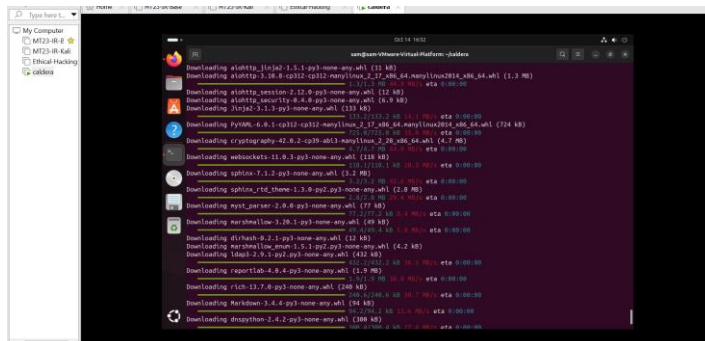
INSTALLATION PROCESS

- I. Sudo apt update to update your system with necessary requirements.

ADVANCED ETHICAL HACKING - COMP 4077

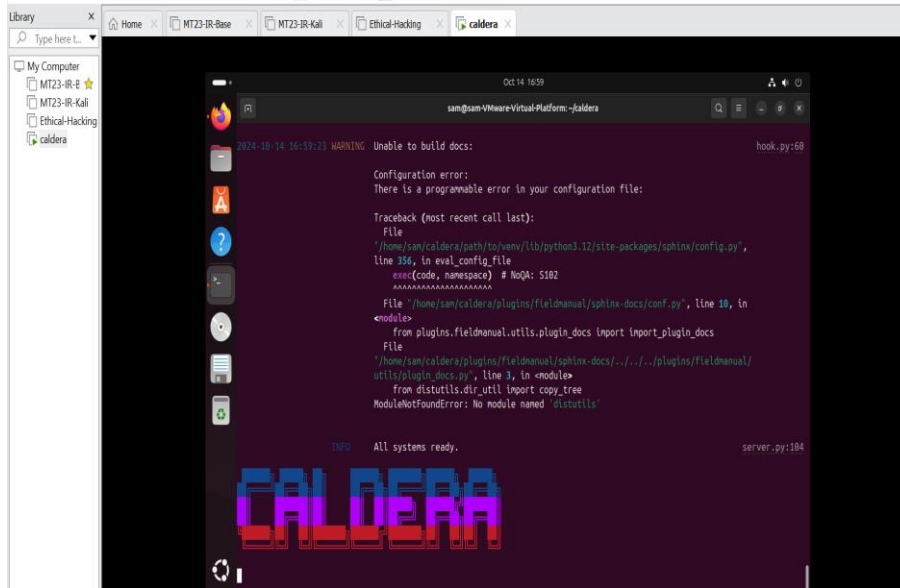


II. Install Required Dependencies and Clone the Caldera Repository

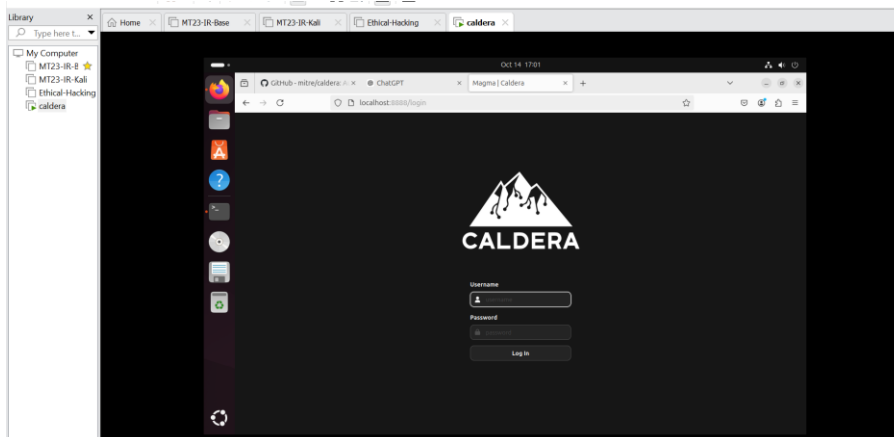


III. Run the server

ADVANCED ETHICAL HACKING - COMP 4077



IV. Go to browser and access it



2. Add few test machines (preferably VMs) in your network and find them using Caldera and try out at least 2 TTPs (tactics, techniques, and procedures) on them and note down the results. You must take step by step screenshots **with explanations** about what are you doing **and** what are you achieving by performing that step (5 marks)

TACTICS, TECHNIQUE AND PROCEDURES

Adversarial Tactics, Techniques, and Procedures are applied to a real-life cyber attack with the use of the MITRE ATT&CK

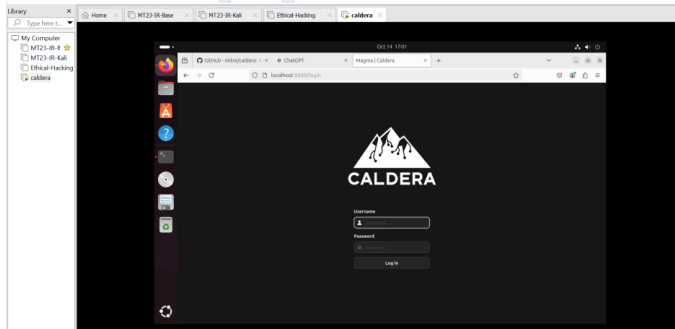
ADVANCED ETHICAL HACKING - COMP 4077

framework. Included are adversary profiles, but these can also be created with custom TTPs through YAML files.

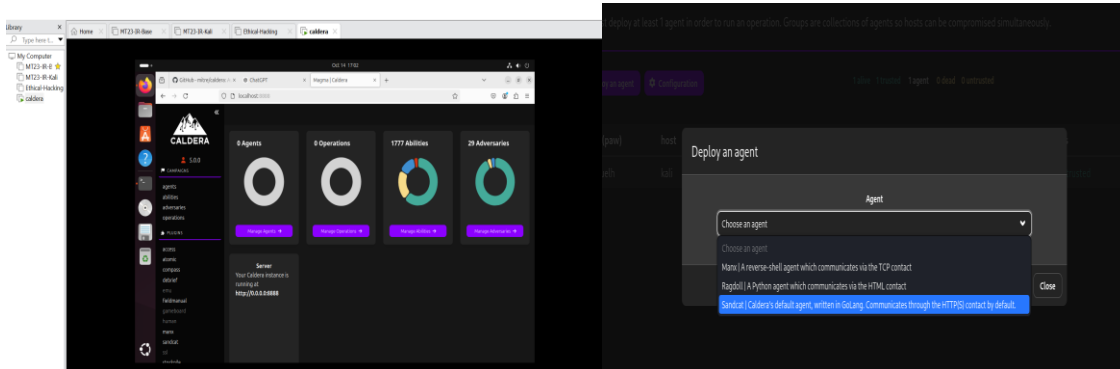
The agents of CALDERA will then execute such TTPs on the target system for the organization to test detection, analyze security gaps, and thus strengthen defenses via realistic simulations with detailed results.

INSTALLATION OF AGENTS

- Log into the browser

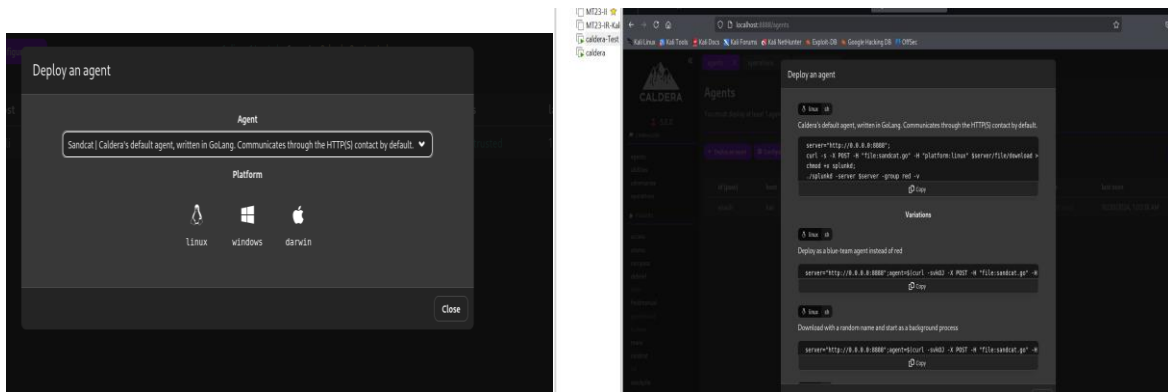


- Go to agent and click deploy an agent (I chose sandcat)

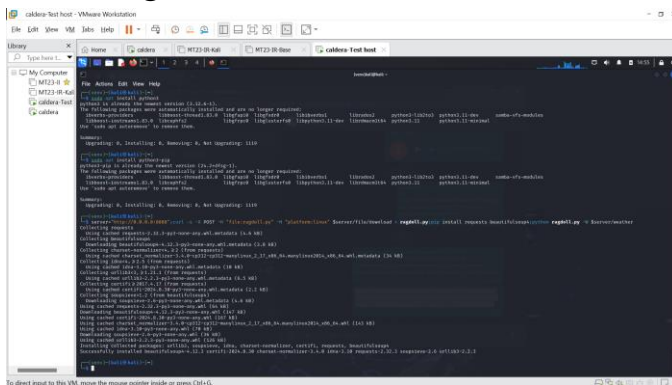


- Select the OS of the vm you want to deploy the agent. Copy payload and run on the agent.

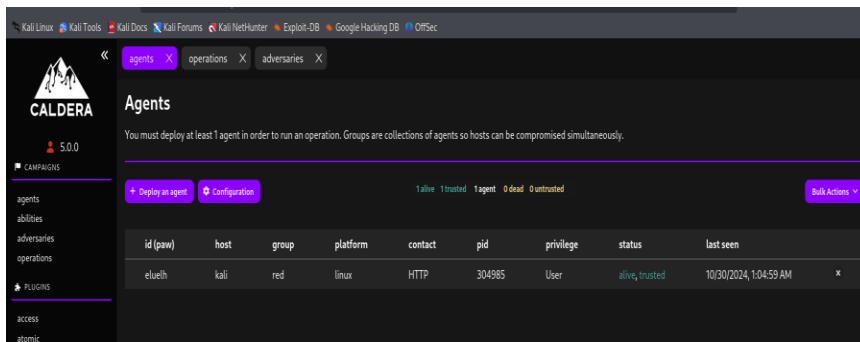
ADVANCED ETHICAL HACKING - COMP 4077



- Run agent on Vm's



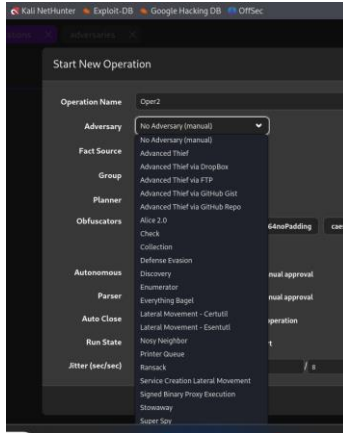
- Confirm agent has been deployed on the GUI



ADVANCED ETHICAL HACKING - COMP 4077

Techniques, Tactics and Procedure

Two major TTP's used in this lab are **Discovery** and **Defense evasion**. They're so many others included in caldera.



Discovery

The discovery techniques enable an attacker to gather information about the target system, network, and defenses. Some of the important techniques include:

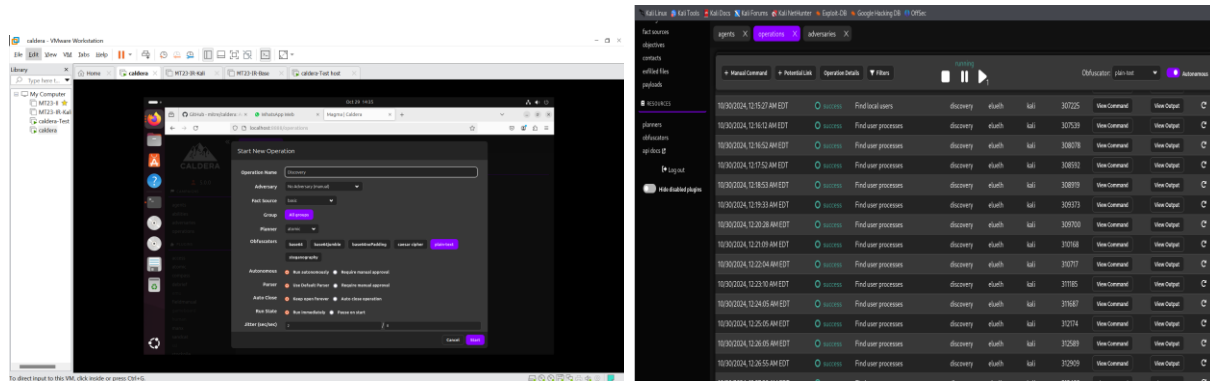
- **System Information Discovery:** Information gathering includes OS, user accounts, and installed software.
- **Network discovery** is very much about finding out all the devices, open ports, and network structure.
- **Credential Dumping:** It is a technique of extracting stored credentials to escalate privileges.

These techniques provide attackers with critical insights for further steps, like privilege escalation and lateral movement, often used with defense evasion to stay undetected and progress toward their objectives.

USAGE ON CALDERA

- Go to the operation tab and name operation. Select discovery on adversaries

ADVANCED ETHICAL HACKING - COMP 4077



Defence evasion

Defense Evasion are Techniques that aim to bypass security mechanisms for evading detection or avoiding defense include the following:

- **Disable Security Tools:** The attackers may disable antivirus software, firewall rules, or logging processes.
- **Obfuscation:** It means hiding or encoding code to evade detection. It includes examples like packing or encrypting the malicious payload.
- **Masquerading:** Renaming files or changing their paths to disguise them as valid processes, such as renaming malware to seem like system files.

Techniques described here allow attackers to remain persistence in systems without being detected by security teams, oftentimes enabling long-term access.

USAGE ON CALDERA

- Go to the operation tab and name operation. Select discovery on adversaries

ADVANCED ETHICAL HACKING - COMP 4077

The image displays two screenshots from a Kali Linux desktop environment. The left screenshot shows the 'Start New Operation' dialog box, and the right screenshot shows the 'Operation Details' window.

Start New Operation Dialog:

- Operation Name: op2
- Adversary: Defense Evasion
- Fact Source: basic
- Group: All groups, red
- Planner: atomic
- Obfuscators: base64, base64jumble, base64noPadding, caesar cipher, plain-text, steganography
- Autonomous: Run autonomously, Require manual approval
- Parser: Use Default Parser, Require manual approval
- Auto Close: Keep open forever, Auto close operation
- Run State: Run immediately, Pause on start
- Jitter (sec/sec): 2 / 8

Operation Details Window:

The window shows a list of operations with columns: Time, Status, Ability Name, Task, Agent, Host, PID, Link Command, and Link Output.

Time	Status	Ability Name	Task	Agent	Host	PID	Link Command	Link Output
10/30/2024, 12:29:45 AM EDT	Success	Avoid logs	defense-evasion	elath	kali	34281	View Command	No output
10/30/2024, 12:30:20 AM EDT	Success	Identify active user	discovery	elath	kali	314781	View Command	No output
10/30/2024, 12:31:15 AM EDT	Success	Collect API details	discovery	elath	kali	315230	View Command	No output
10/30/2024, 12:32:10 AM EDT	Success	System processes	discovery	elath	kali	315814	View Command	No output
10/30/2024, 12:33:20 AM EDT	Failed	Scan WiFi networks	discovery	elath	kali	316378	View Command	No output
10/30/2024, 12:34:31 AM EDT	Success	Preferred WiFi	discovery	elath	kali	316871	View Command	No output
10/30/2024, 12:35:31 AM EDT	Success	Disrupt WiFi	Impact	elath	kali	317252	View Command	No output