School of Informatics & IT

Diploma in Cybersecurity & Digital Forensics

Ethical Hacking and Intrusion Prevention

Lab x – Privilege escalation with MITRE CALDERA

# Learning Outcomes

By the end of this exercise, the student should be able to demonstrate the following items:

* Set up MITRE CALDERA and deploy an agent onto a target machine
* Create an adversary profile and run it in an operation
* Gain root access from a low privilege machine using MITRE CALDERA

## Overview

## In the realm of ethical hacking, staying one step ahead of potential adversaries is crucial to ensure the security of computer networks and systems. Privilege escalation is a technique used by ethical hackers to gain unauthorized access and elevate their privileges within a target system. MITRE CALDERA is a powerful and widely acclaimed open-source framework that empowers ethical hackers to simulate, analyze, and respond to advanced cyber threats, with a specific focus on privilege escalation.

# Tasks

## 2.1 Environment Setup

### Pre-Requisite

* Kindly ensure that you have downloaded the KALI-LINUX Virtual Machine and the TARGET-MACHINE Virtual Machine, which is in POLITEMall.

### Instructions

Launch your KALI-LINUX and TARGET-MACHINE Virtual Machines.

In the TARGET-MACHINE VM, login using the following credential.

* Username: root
* Password: P@ssw0rd

In this lab, a custom Docker image will only be used to establish a remote network server that you will need to use for your caldera escelation challenge. This is to prevent any accidental modifications on the configuration settings of the KALI-LINUX Virtual Machine.

Launch the Terminal application in TARGET-MACHINE VM, and type in the following commands:

cd Documents/ProjectCaldera

docker-compose up

Leave the terminal in the background.

Launch the Terminal application in KALI-LINUX, and type in the following commands:

ip route add 172.20.0.0/16 via 192.168.100.7

## 2.2 Installing Mitre Caldera

Run the following commands in your Kali-LINUX :

git clone https://github.com/mitre/caldera.git --recursive

cd caldera

pip3 install -r requirements.txt

Once done, run the following command to launch the server inside caldera folder

python3 server.py --insecure

A screen shot of a computer screen

Description automatically generated

Open your web browser and type into the searchbar <http://localhost:8888> and click enter.

The login details is as follows:

Username: red

Password: admin

## 2.3 Caldera Escalation Challenge

### Pre-Requisite

**ALL FOLLOWING STEPS ARE DONE IN KALI-LINUX.**

Before starting the challenge, connect to the target host via SSH

ssh bob@172.20.0.2

password: P@ssword

Once you have gained access to the target machine, you can begin the lab.

### Instructions

In Mitre Caldera, navigate to “agents” and create a new agent with the following parameters:

* Sandcat agent
* Linux Platform
* app.contact.http = http://<your KALI-LINUX ip address>:8888

A screenshot of a computer

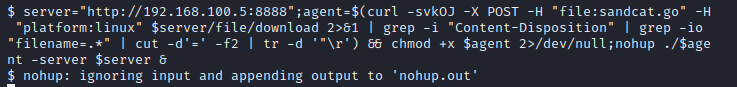
Description automatically generated

scroll down to “Download with a random name and start as a background process” and copy the command.

A screenshot of a computer program

Description automatically generated

Paste the copied code into the terminal of the target machine.



You should see the following in your MITRE CALDERA except with a different id(paw) and pid.

A screenshot of a computer

Description automatically generated

Now that you have an agent deployed on the target machine, lets do some reconnaissance to see what we are dealing with.

cat /etc/passwd

This shows that we aren’t able to read the passwd file due to low privilege access.

However, a simple sudo placed in front allows us to read the file no problem. Hence we can conclude that the user bob is in the sudoers file.

Lets see how we can exploit this 😊.

In Caldera, navigate to “adversaries”. Create a new adversary profile with the following details.

* Profile Name: IAMINYOURWALLS
* Description: System persistence, creates a user with uid and gid of root

A picture containing screenshot, text, software

Description automatically generated

Create the profile and then +Add ability with the following details:

* Tactic: persistence
* Technique: T1136.001 | Create Account: Local Account
* Ability: Create a new user in Linux with ‘root’ UID and GID

A screenshot of a computer

Description automatically generated with medium confidence

Under Payload, select ‘sandcat.go-linux’

A picture containing text, software, multimedia software, font

Description automatically generated

The following default command will not work so we will have to edit it abit :)

sudo bash -c 'useradd -ou 0 -g 0 -M -d /root -s /bin/bash butter; if [ $(cat /etc/os-release | grep -i "Name=\"ubuntu\"") ]; then echo "butter:BetterWithButter" | sudo chpasswd; else echo "butter:BetterWithButter" | sudo chpasswd; fi;'

Command Breakdown:

sudo bash -c 'useradd -ou 0 -g 0 -M -d /root -s /bin/bash butter;

**Creates user butter with uid 0 and gid 0, sets /root as home directory and sets login shell to /bin/bash**

if [ $(cat /etc/os-release | grep -i "Name=\"ubuntu\"") ]; then echo "butter:BetterWithButter" | sudo chpasswd;

**Sets password to “BetterWithButter” if OS is ubuntu**

else echo "butter:BetterWithButter" | sudo chpasswd; fi;'

**Sets password to “BetterWithButter” if OS is not ubuntu**

Under Cleanup, delete the existing command and leave it empty as we want the change to stay.



Click Save & Add

Navigate to Operation and create a new operation with the following details:

* Name: Lab1
* Adversary: IAMINYOURWALLS
* Fact source: basic

Click on ADVANCED and select “ceasar cipher” under obfuscation. This is to cover your tracks and for defence evasion in the future.

A screenshot of a computer

Description automatically generated

Click start.

The previously deployed caldera agent will proceed to do the work for you. You can see the status of the operation from the dashboard. Feel free to explore the features during this time. Once the operation is done, it will look something like this.

A black background with white text

Description automatically generated

Navigate over to the target machine terminal and run the following command to check for changes.

sudo cat /etc/passwd

Notice that a new user Butter has been added with UID 0 and GID 0.

A screenshot of a computer screen

Description automatically generated

Run the following command to log into the new user butter. The password is the previously set “BetterWithButter”

su butter

Then check your privilege with the following commands:

whoami

id

A screen shot of a computer code

Description automatically generated

Congratulations, you have successfully gained root access with MITRE CALDERA, wasn’t too hard was it?.

Retrieve the flag in /root

***Insert flag here***

**BONUS CHALLENGE:**

For this next part, we will explore how to breakout of this docker container and into the host machine that is running the container, this is equivalent to breaking out of a website to access the server itself. First, exit back into the user bob as even bob can do it!

Run the following command:

ls -la /

We see a lot of directories but one that interests us is the directory ‘host’ , upon further inspection, we can assume that this is a shared folder from the host machine to share files with the container.

A screenshot of a computer program

Description automatically generated

Since we have sudo privileges, we can run the command “chroot” on the folder and put us in through a bash interface.

sudo chroot /host bash

And just like that, We Have successfully broken out of the container due to a shared host folder that the user has forgotten to remove after he is done. This shows how badly misconfiguration can affect your system as even a low privilege user can do so.

Navigate to /root/Documents to retrieve the flag.

***Insert flag here***

## 2.4 Cleanup

Once you are done with the lab, On TARGET-MACHINE close the entire Terminal application and relaunch a new one. Type in Ctl+C to kill the docker container.

A screen shot of a computer code

Description automatically generated

**Mitigation:**

Part 1: Ensure that only users who need to use sudo are in the sudoers file. This will ensure that low-privilege users will not be able to run unauthorized commands. In this case, remove bob from the sudoers file.

Part 2: Ensure that after you are done with the docker container, remove any shared folders as they open up a vulnerability for container users to exploit to gain access to your host machine.