School of Informatics & IT

Diploma in Cybersecurity and Digital Forensics

Incident Response and Management (ICRM)

Lab x – Security Incident Response Management II

# Learning Outcomes

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

* Deploy Caldera agent to automate attacks on a target machine to simulate a live attack
* Customise the Wireshark GUI to display required information needed during the analysis.
* Apply search filters to only display what is required during the analysis.

# Tasks

## Background / Scenario

Wireshark is a free protocol analyzer that can record and display packet captures (PCAPs) of network traffic. This tool is used by IT professionals to investigate a wide range of network issues, and as a security analyst, Wireshark is often used to review traffic generated from security incidents.

Note: These trainings are a subset of the Unit42 Palo Alto Network Wireshark Training Guides (https://unit42.paloaltonetworks.com/tag/wireshark/)

MITRE CALDERA is a powerful and widely acclaimed open-source framework that empowers ethical hackers to simulate, analyze, and respond to advanced cyber threats.

## Environment Setup

### Pre-Requisite

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

### Instructions

Launch your KALI-LINUX and TARGET-MACHINE VMs.

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

* Username: root
* Password: P@ssw0rd

Launch WireShark from your desktop.

A screenshot of a computer

Description automatically generated

Select interface eth0 to begin.

A screenshot of a computer

Description automatically generated

**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

<insert learning material here>

## WireShark x Caldera

### Instructions

**Agent Deployment**

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

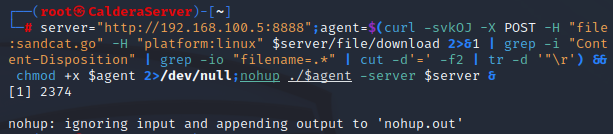
Description automatically generated

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

**Attack Deployment**

Now navigate over to operations and create an operation with the following parameters:

* Name: Lab2
* Adversary: Noisy Neighbor
* Fact source: basic

And click run.

Switch over to your REBLU.VM and see the interactions being captured.

Click on the interaction and rather information about the simulated attack

|  |  |
| --- | --- |
| **Requirement** | **Information gathered** |
| Attacker IP address |  |
| Attacker source port |  |
| Destination port |  |
| User-Agent  Hint: Follow TCP String |  |

Answers:

192.168.100.5

8888

54248

Go-http-client/1.1