

# South Dakota OWASP Adversary Emulation with MITRE's Caldera

Michael Klosterman, MBA, CISSP, CSSLP, CISA, GCIH, GNFA, GPEN

```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/10.10.10.1/10.10.10.1/g' /etc/passwd
vi /etc/selinux
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
```

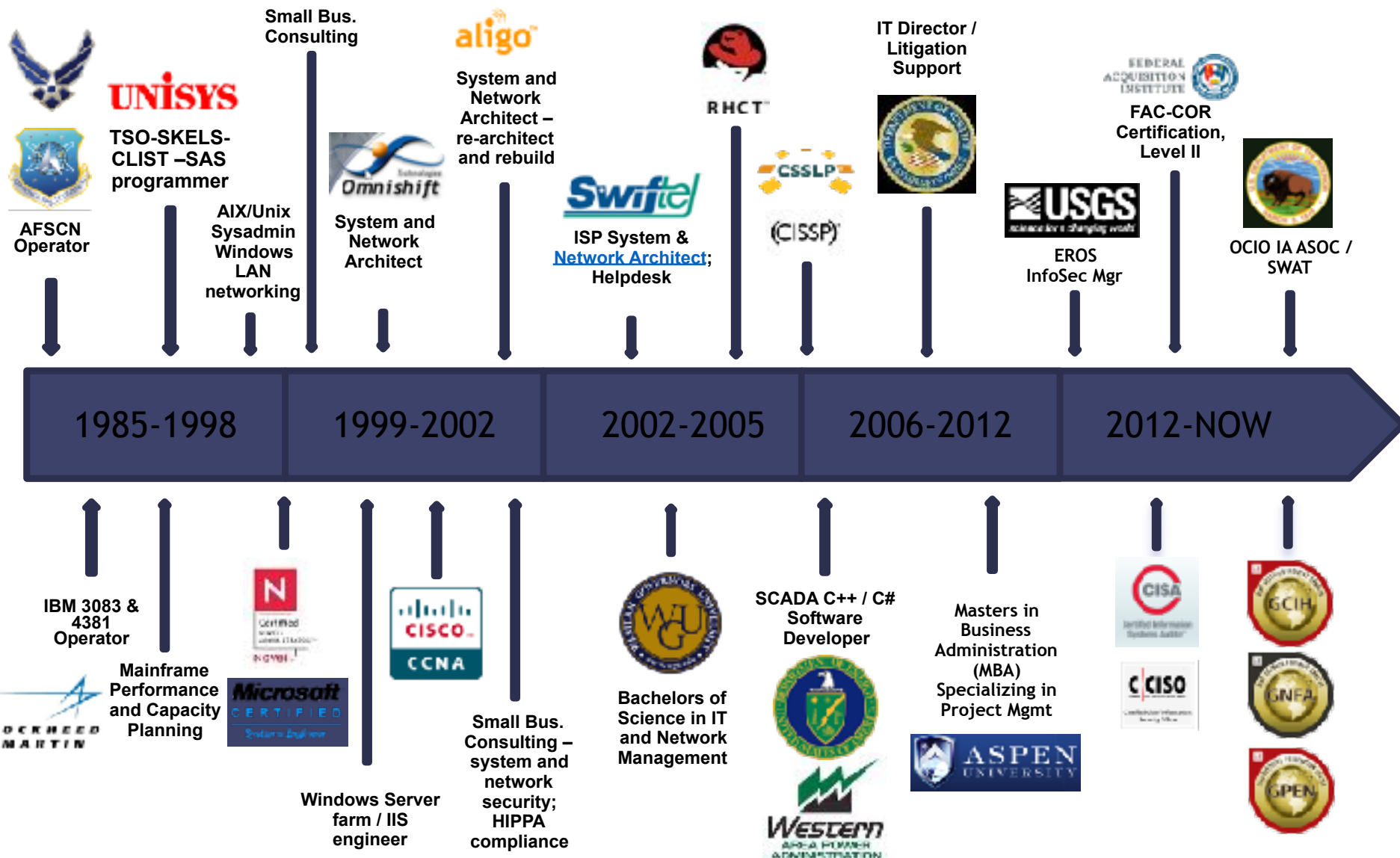
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# whoami



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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# 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

```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/log
touch /var/log
tail -f /var/log
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELinux/selinux/'
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```


caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# Caldera – What is it?

cal·de·ra

/kal'derə,kôl'derə,kal'dirə/ 

*noun*

a large volcanic crater, especially one formed by a major eruption leading to the collapse of the mouth of the volcano.



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.

[<Citation Link>](#)

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# 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>](#)

```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/log
touch /var/log
tail -f /var/log
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connect
nmcli con add
ifconfig
nmcli con mod
nmcli con rel
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i s/0/1/g
vi /etc/selinux
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# Caldera – Who Made It?



[<Citation Link>](#)



Andy Applebaum, PhD.  
Lead Cybersecurity Engineer  
MITRE

## Type

Founded

Headquarters

Key people

Revenue

Number of  
employees

Website

## Not-for-profit corporation

1958; 61 years ago

[Bedford,](#)  
[Massachusetts](#) and  
[McLean, Virginia,](#)  
United States

[Jason Providakes](#)  
[President](#) and [CEO](#)

[US\\$ 1.484 billion](#)<sup>[1]</sup>

8,425<sup>[2]</sup>

[www.mitre.org](http://www.mitre.org)

```
yum -y install
yum -y install
vi /etc/sysctl.d
sudo systemctl
vi /etc/passwd
tail -f /var/log
touch /var/log
tail -f /var/log
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl --
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/0/1/g'
vi /etc/selinux
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```



# Caldera – Where Can We .....



- .....Run This?
  - Only in Development environments, unless you are authorized!
- .....Get This?
  - [Download from github.com](https://github.com)
- .....See How to Install and Run This?
  - We'll be showing you the installation and use

```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/l
touch /var/log
tail -f /var/l
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rel
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sedit
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# Caldera – Server Installation.....

<https://github.com/mitre/caldera>

## Requirements

- Python 3.5.3+
- Google Chrome is our only supported/tested browser

## Installation

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

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

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

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

Then start the server.

```
python server.py
```



```
yum -y install
yum -y install
vi /etc/sysctl.d
sudo systemctl
vi /etc/passwd
tail -f /var/log
touch /var/log
tail -f /var/log
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELinux/SELinux/'
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```



# Caldera – Server Installation.....

## 7. Procedure

### a. Install CentOS 7.x

- i Use CentOS-7-x86\_64-Minimal-1611 iso
- ii Update to current:

```
yum -y update && yum -y upgrade
```

- iii. Install basic packages:

```
yum -y install mlocate bind-utils traceroute ntp wget curl iotop man man-pages make  
tcpdump mailx lynx sysstat net tools firewallfd bzip2 zip unzip epel-release jq whois iftop
```

- iv Install python3.6 and other prerequisites

```
yum -y install python3.6 x86_64 python3.6-devel x86_64 python3.6-pip noarch  
gcc x86_64 openssl-devel x86_64
```



```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rel  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl st  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i s/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# 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 \*\*)

```
sestatus
```

### i. Disable SELinux from starting

1. vi /etc/selinux/config

```
SELINUX=disabled
```

### ii. Reboot

```
reboot
```



```
yum -y install  
yum -y install  
vi /etc/sysctl.d  
sudo sysctl -p  
vi /etc/passwd  
tail -f /var/log  
touch /var/log  
tail -f /var/log  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connect  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con reload  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl vi  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sestatus  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# 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/mitre/caldera.git --recursive
```

## g. Install the requirements

```
cd /opt/caldera  
python3.6 -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
```



```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl st  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i s/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Server Installation.....

## i. Start the Caldera Server

```
cd /opt/caldera
python3.6 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



```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
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@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py
caldera.py -d | --debug
caldera.py -h | --help
```



# Caldera – Server Installation.....



```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rell
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELinux/selinux/'
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

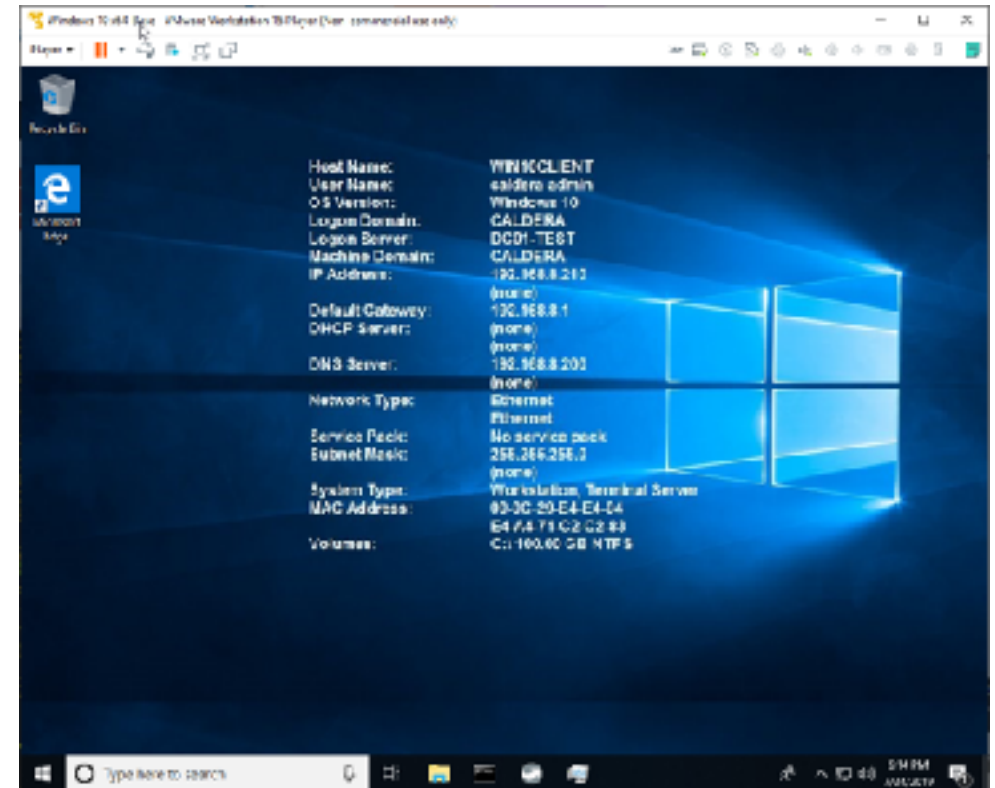
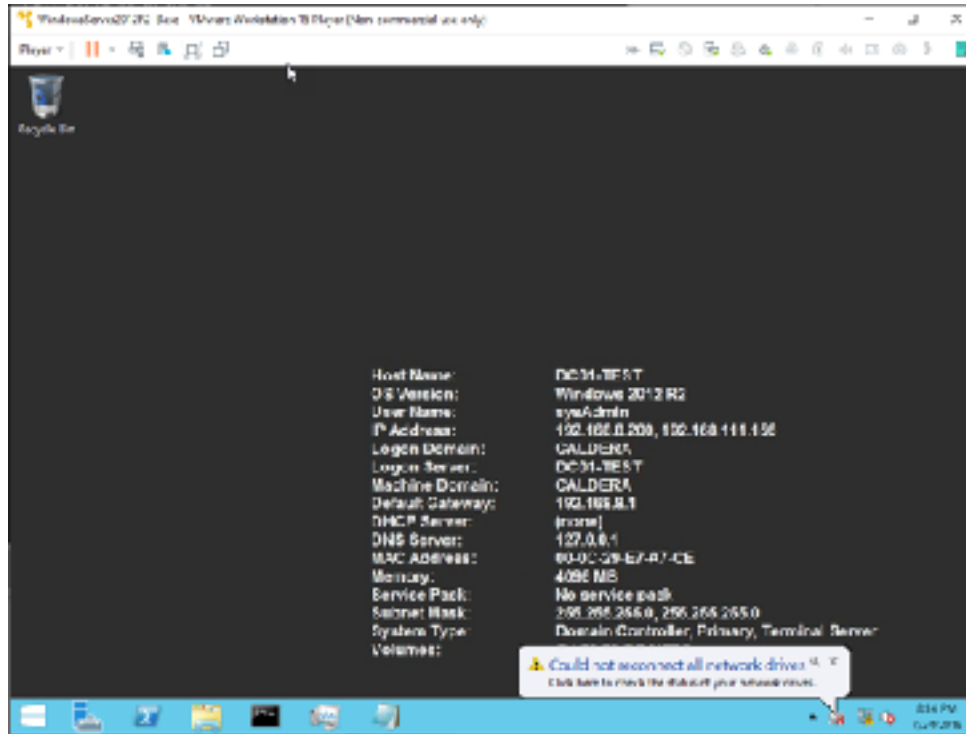
caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```



# Caldera – Windows AD and AD Client.....



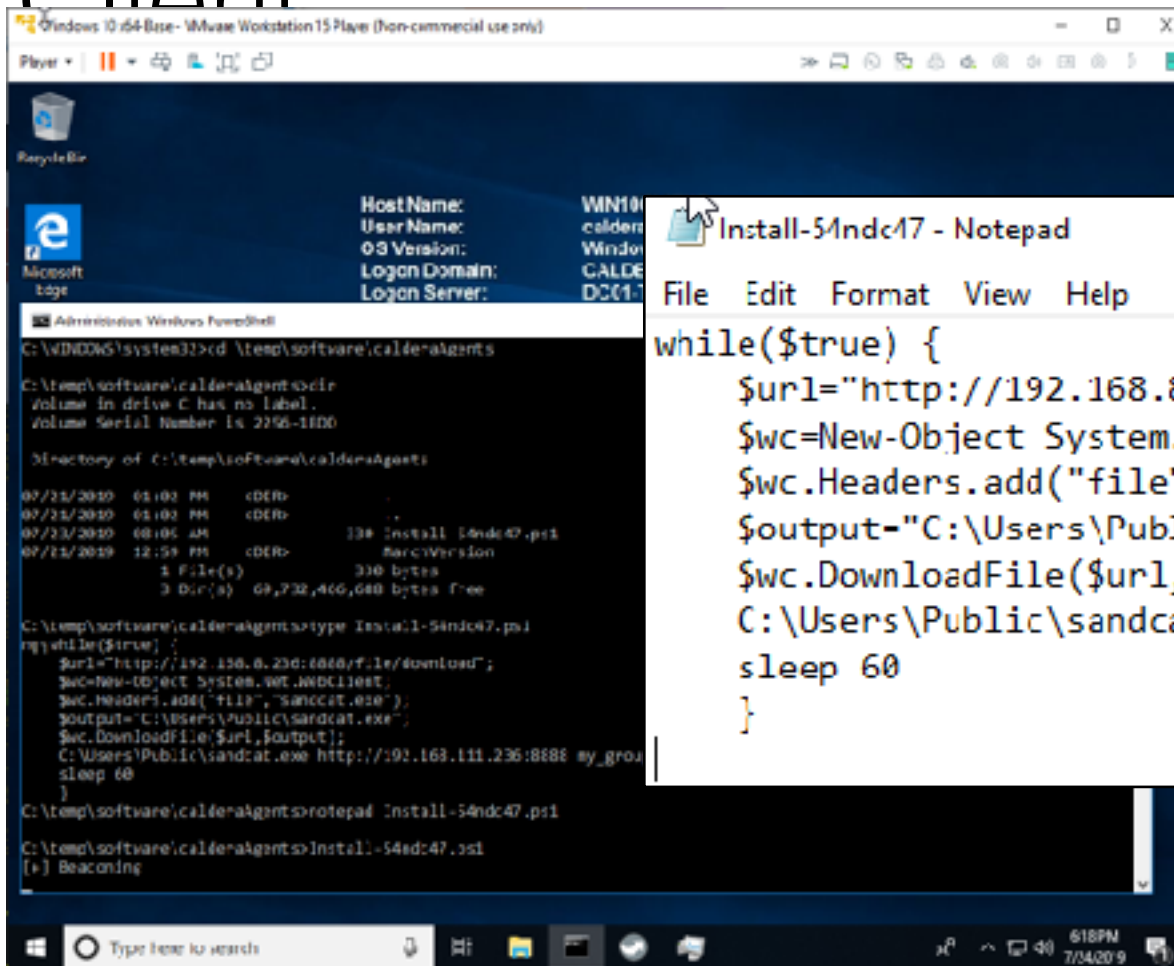
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Windows AD and AD Client



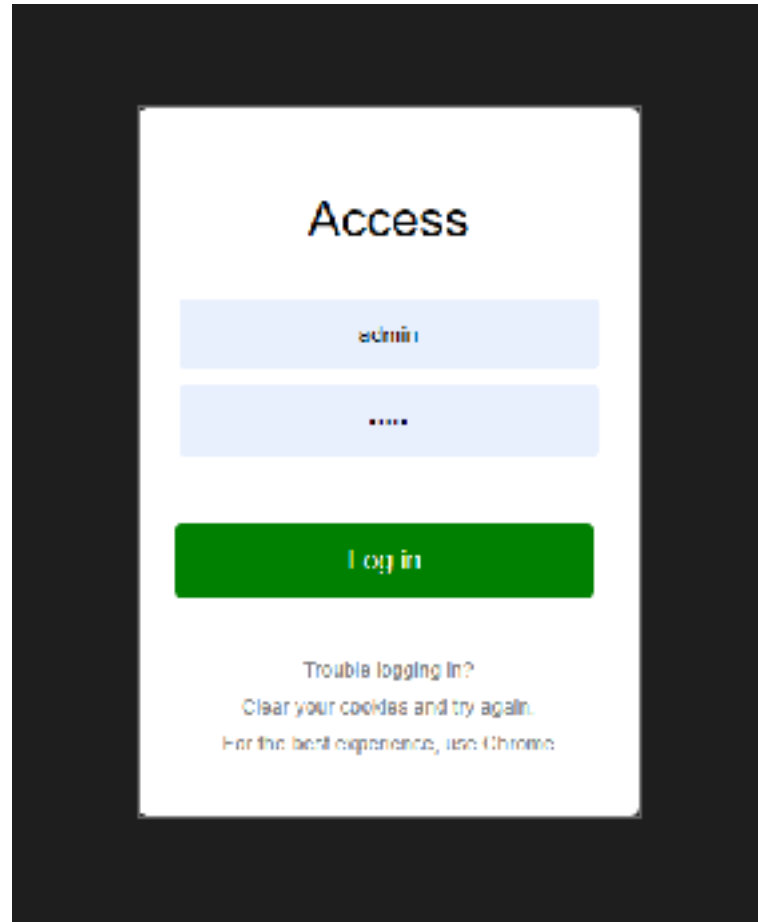
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



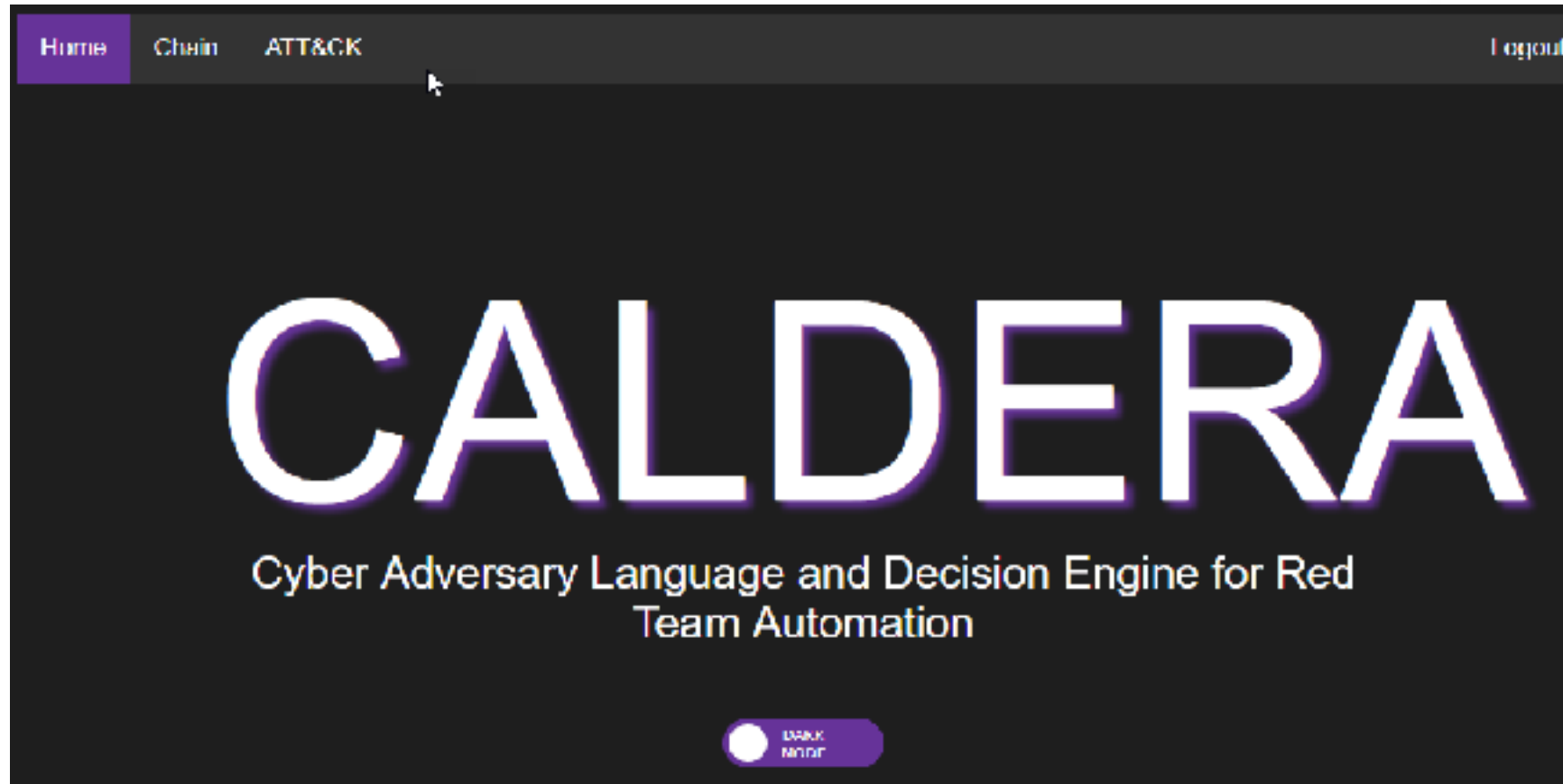
```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl st  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i 's/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd  
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl vi  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i 's/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

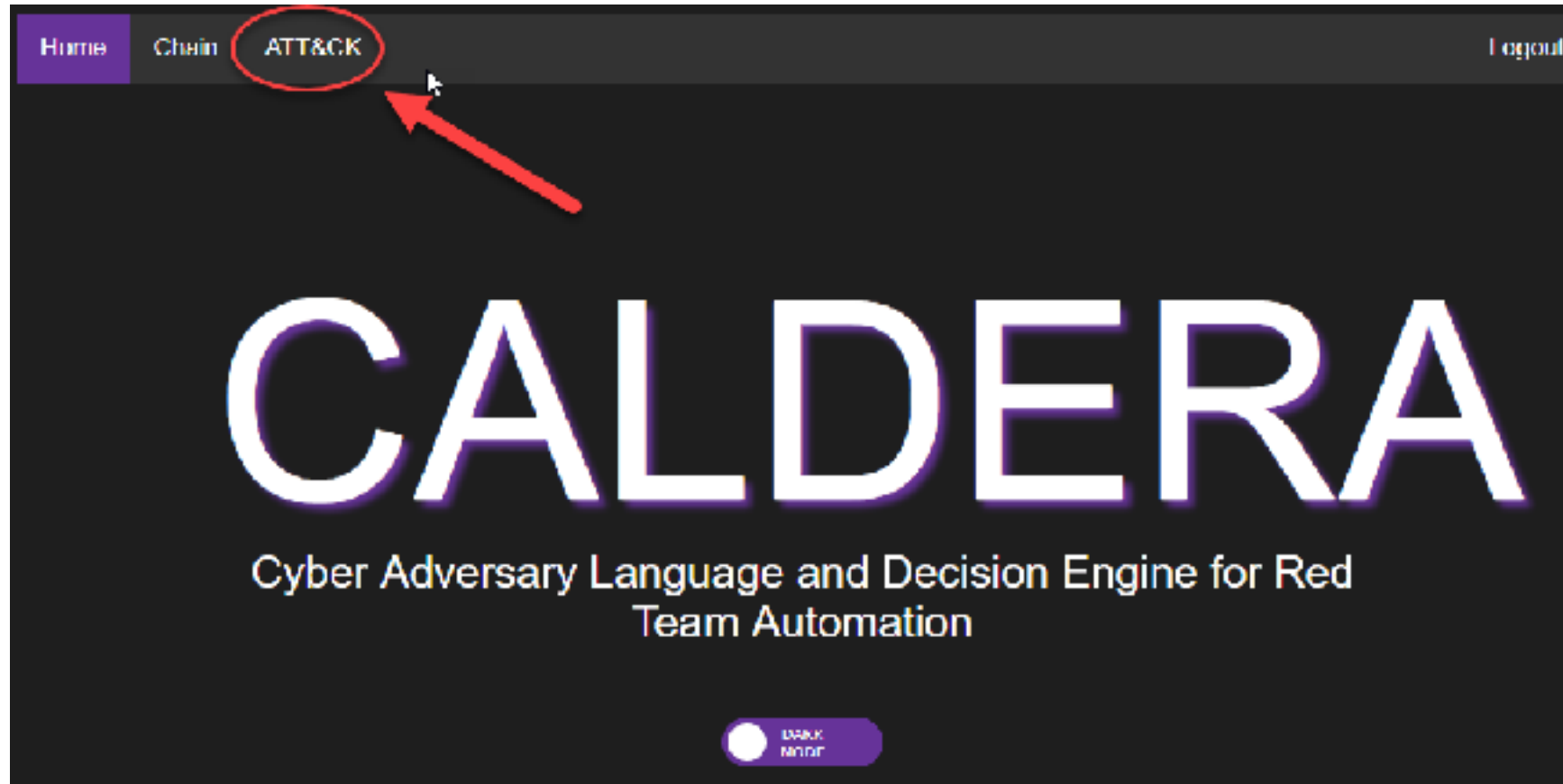
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Server Overview....



```
yum -y install  
yum -y install  
vi /etc/syslog  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl vi  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i 's/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```



# 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, in 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.

## ATT&CK™

[Get Started »](#) [Contribute »](#)

[Check out our Blog »](#)

**Tweets by @MITREattack**

ATT&CK Retweeted

**Frank Duff**  
@FrankDuff  
The @MITREAttack Evaluations Round 2 Call for Participation closes July 31, 2019. If you are interested in participating and have not signed up, now is the time. For more information visit [attack.mitre.org/methodology/](https://attack.mitre.org/methodology/)

Jul 22, 2019

ATT&CK Retweeted

**Johnny Curran**  
@JN\_JohnnyC  
Here's the #SecurityUpdate for tonight's

Embed [View on Twitter](#)

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

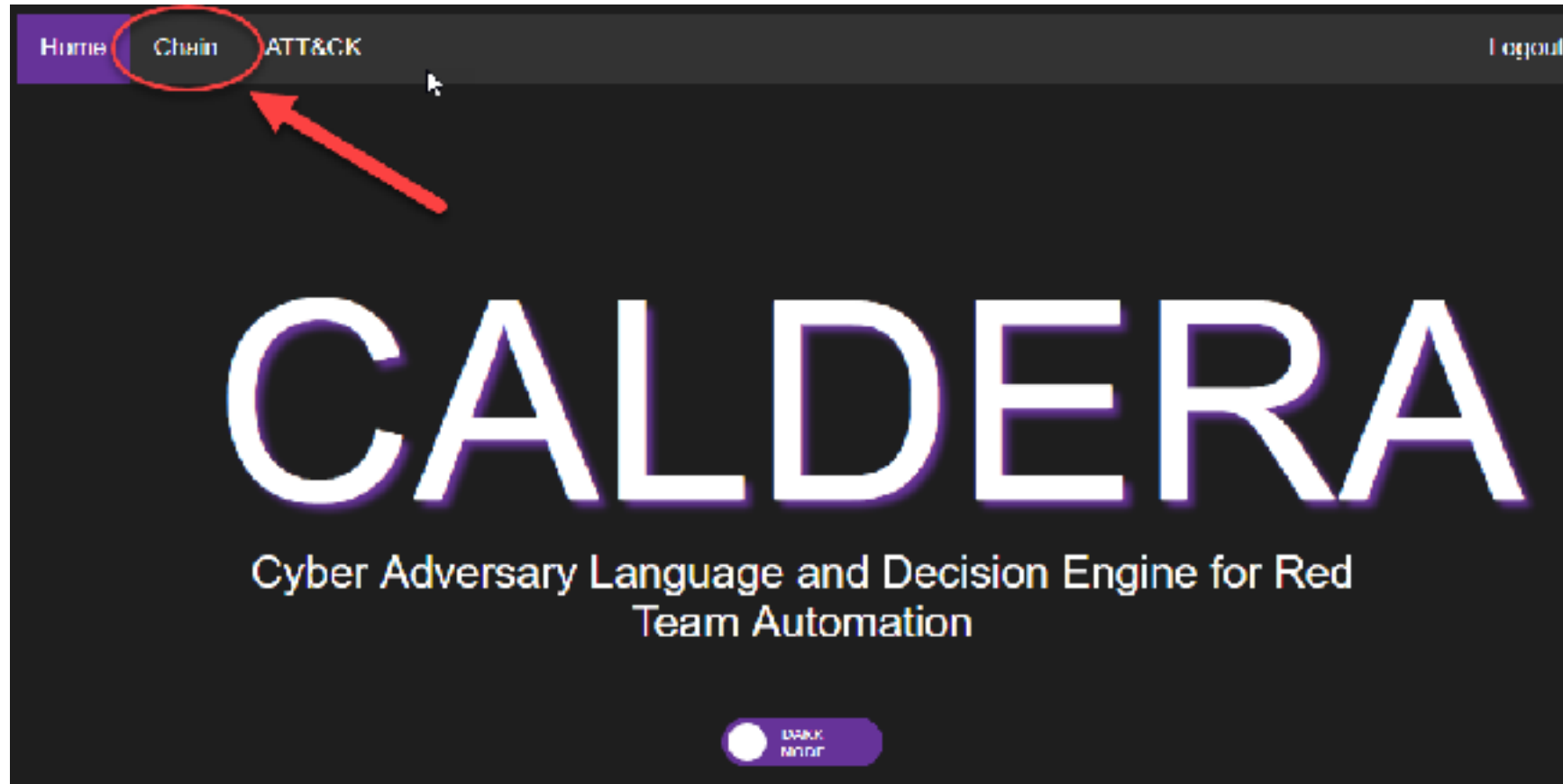
caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```



# Caldera – Server Overview....



```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl vi  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i s/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Server Overview....



Home | **Groups** | Alerts | Profile | Add new | Dispositions | Login

Manage groups

No hosts? Deploy an agent

**Add**

Enter name

**Add group**

Show 10 entries

Host	Checks	Groups	Platform	Last seen	Delete
Win10Client\$CALDERA\caldera-admin	1	my_group	windows	2019-07-25 01:27:59.04/097	X

Showing 1 to 1 of 1 entries

Previous 1 Next

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

# Caldera – Server Overview....



**Manage groups**  
No hosts? Deploy an agent

**Win10Group**

**Add group**

**Show**  
10 entries

**Search**

Host	Checks	Groups	Platform	Last seen	Delete
Win10Client\$CALDERA\caldera admin	3	my group	windows	2019-07-25 01:29:59	X

Showing 1 to 1 of 1 entries 1 row selected

Previous 1 Next

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



Clear

Groups

Abilities

Facts

Adversaries

Operations

Manage abilities

View available techniques

Select ATT&CK t

Select ATT&CK tactic

exfiltration

defense evasion

lateral-movement

command-and-control

persistence

defensive-evasion

collection

privilege-escalation

credential access

execution

discovery

ABILITY ID:

ATT&CK TACTIC:

ATT&CK TECHNIQUE ID:

ATT&CK TECHNIQUE NAME:

NAME:

DESCRIPTION:

PLATFORM:

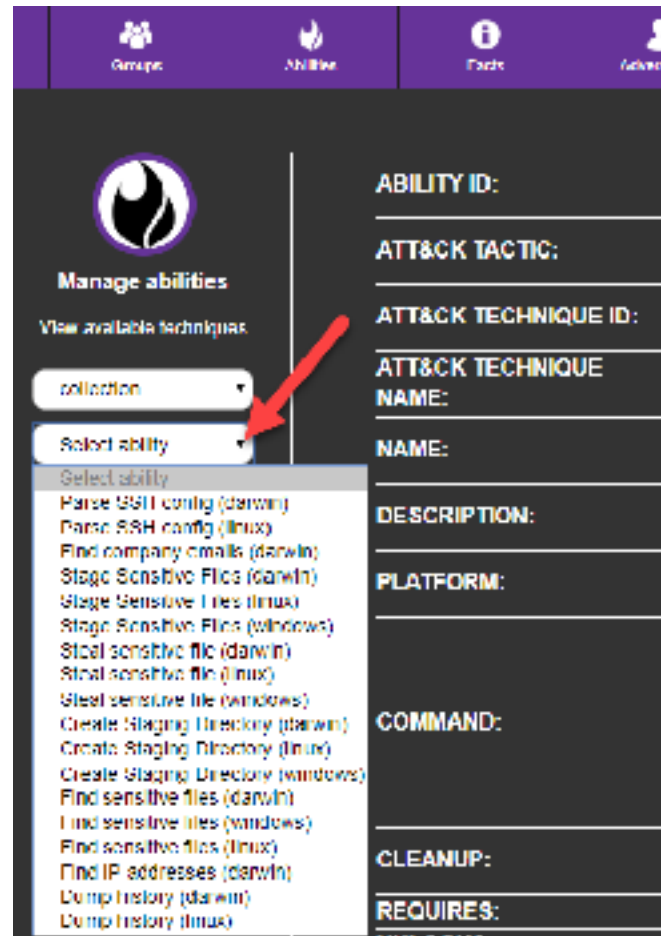
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py
caldera.py -d | --debug
caldera.py -h | --help
```

# Caldera – Server Overview....



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

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Server Overview....



The screenshot displays the Caldera web interface. At the top, there is a navigation bar with icons for Groups, Abilities, Facts, Adversaries, and Operations. The main content area is titled 'Manage abilities' and shows details for the 'collection' tactic. The details include:

- ABILITY ID:** 5d199f58-690a-41ff-8ac9-bb7b0506adcb
- ATT&CK TACTIC:** collection
- ATT&CK TECHNIQUE ID:** T1005
- ATT&CK TECHNIQUE NAME:** Data from Local System
- NAME:** Steal sensitive file
- DESCRIPTION:** Grab contents of every sensitive file
- PLATFORM:** windows
- COMMAND:** get-content -#(host.file.sensitive)
- CLEANUP:**
- REQUIRES:** host file sensitive
- UNLOCKS:**

```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```



# Caldera – Server Overview....



Property	Value	Source	Score	Blacklist	Del
file.sensitive.extension	txt	extensions	1	no	>
file.sensitive.extension	yml	extensions	1	no	>
host.user.name	Administrator	common credentials	1	no	>
host.user.name	Administrator	test lab	1	no	>
host.user.password	!@qssword123	common credentials	1	no	>
host.user.password	!@qssw0rd	test lab	1	no	>
remote.host.name	work001-testdomain	test lab	1	no	>

```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl st  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i 's/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd
```

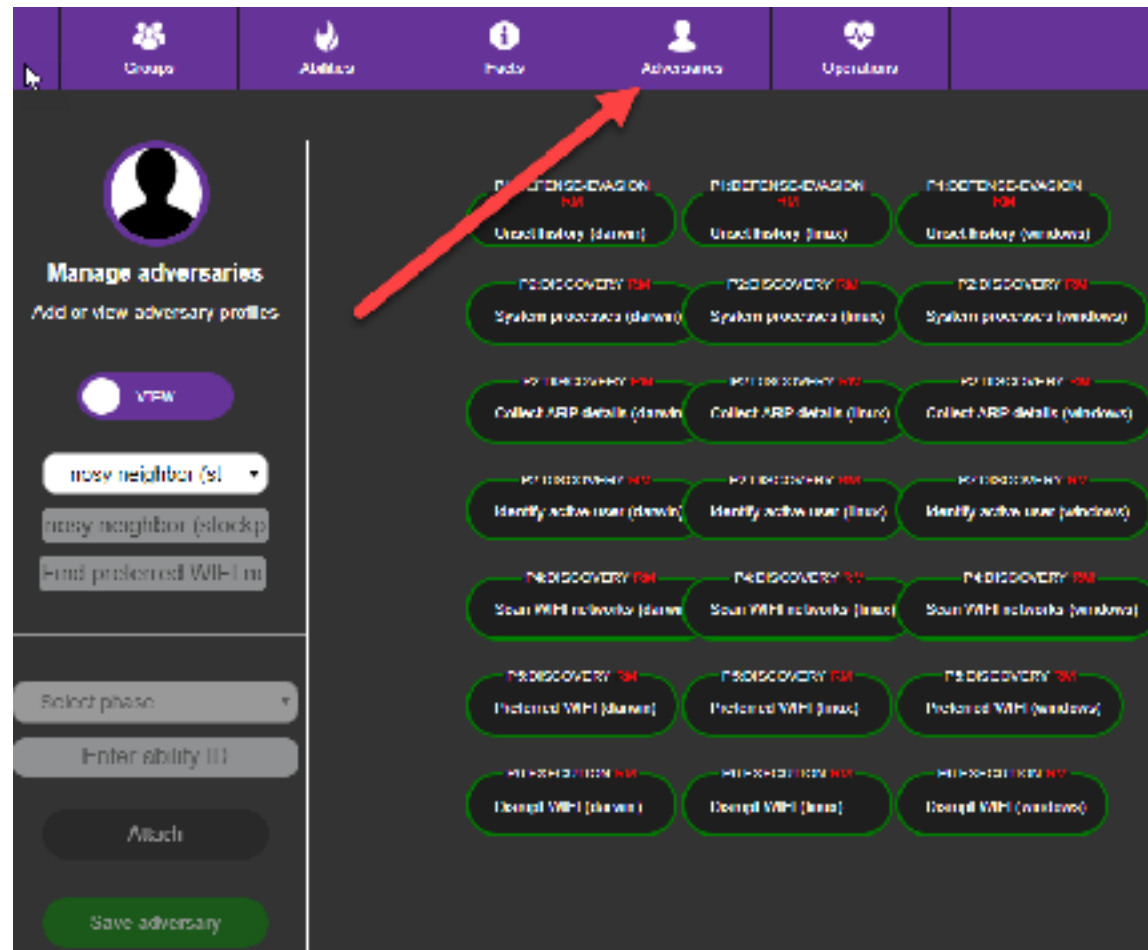
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



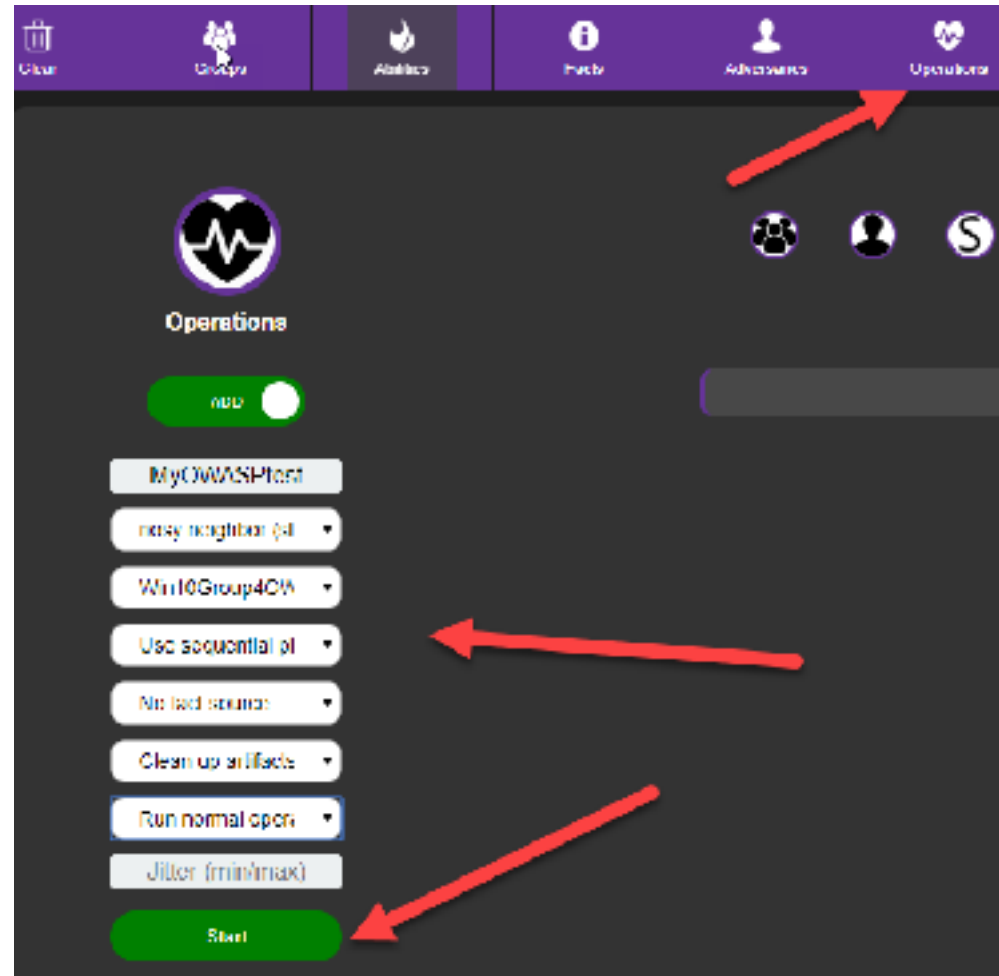
```
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```

# Caldera – Server Overview....



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

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



Group	User	Status	Created	Updated
WIN10G0RCLIP40WASP	NISBY MFICHROR (STOCKPILE)	S	2019-07-25 01:45:10	2019-07-25 01:45:10

Created	Task	Action
2019-07-25 01:45:10	Host #2... Unset history	★↓
2019-07-25 01:46:10	Host #2... Identify active user	★↓
2019-07-25 01:46:10	Host #2... Collect ARP details	★↓
2019-07-25 01:46:10	Host #2... System processes	★↓
2019-07-25 01:46:10	Host #2... Scan WIFI networks	★↓
2019-07-25 01:46:10	Host #2... Preferred WIFI	★↓
2019-07-25 01:46:10	Host #2... Disrupt WIFI	★↓

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

caldera

Usage:

```
caldera.py  
caldera.py -d | --debug  
caldera.py -h | --help
```

# Caldera – Server Overview....



```
yum -y install
yum -y install
vi /etc/sysst
sudo systemctl
vi /etc/passw
tail -f /var/
touch /var/log
tail -f /var/
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rel
hostnamectl] st
hostnamectl] se
hostnamectl] st
hostnamectl] re
hostnamectl] --
hostnamectl] vi
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
systemd
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

Windows 10 x64-BASE - VMware Workstation 15 Player (Non-co

192.168.111.236 KTTY

Caldera Server Log

Host Name  
User Name  
OS Version  
Logon  
Logon S

54ndc47 Log

Administrator: Windows PowerShell

```
[i] Running instruction
[i] Running instruction
[i] Running instruction
[i] Running instruction
[i] Running instruction
[i] Running instruction
[i] Running instruction
[i] Beaconing
[i] Cleanup: C:\Users\CALDER~1\AppData\Local
```

DEBUG:operation\_svc:Operation 5 phase 1: started
DEBUG:planning\_svc:Created 1 links for WinIOClient\CALDERA\caldera admin
DEBUG:operation\_svc:Operation 5 phase 1: started
DEBUG:planning\_svc:Created 5 links for WinIOClient\CALDERA\caldera admin
DEBUG:operation\_svc:Operation 5 phase 1: completed
DEBUG:operation\_svc:Operation 5 phase 5: started
DEBUG:planning\_svc:Created 6 links for WinIOClient\CALDERA\caldera admin
DEBUG:operation\_svc:Operation 5 phase 5: completed
DEBUG:operation\_svc:Operation 5 phase 6: started
DEBUG:planning\_svc:Created 7 links for WinIOClient\CALDERA\caldera admin
DEBUG:operation\_svc:Operation 5 phase 6: completed
DEBUG:operation\_svc:Operation complete: 5
DEBUG:sandcat:Beacon (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:file\_svc:downloading wifi.ps1...
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:[AGENT] posting results (WinIOClient\CALDERA\caldera admin)
DEBUG:sandcat:Beacon (WinIOClient\CALDERA\caldera admin)

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```



# Caldera – Server Overview....



```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rena
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl --
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELIN
vi /etc/selini
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/calder
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --dehug
caldera.py -h | --help
```

2019-07-25 01:46:10	Host #2	Unsat history	*↓
2019-07-25 01:46:10	Host #2	Identify active users	*↓
2019-07-25 01:46:10	Host #2	Collect ARP details	*↓
		Description:	Locate all active IP and FQDNs on the network
		Technique:	T1010
		Collected:	
		Finished:	
		Command:	arp -a
2019-07-25 01:46:10	Host #2...	System processes	*↓
2019-07-25 01:46:10	Host #2	Scan WIFI networks	*↓
2019-07-25 01:46:10	Host #2...	Preferred WIFI	*↓
2019-07-25 01:46:10	Host #2	Disrupt WIFI	*↓



# Caldera – Server Overview....



```
yum -y install
yum -y install
vi /etc/sysctl
sudo systemctl
vi /etc/passwd
tail -f /var/lo
touch /var/lo
tail -f /var/lo
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connecti
nmcli con add
ifconfig
nmcli con mod
nmcli con rel
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i 's/SELinux/SELinux/g' /etc/selinux
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
```

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

caldera

Usage:

```
caldera.py
caldera.py -d | --debug
caldera.py -h | --help
```

2019-07-25 01:45:10 Host #2 Unset history ★↓

arp -a

Interface: 192.168.8.210 --- 8c/

Internet Address	Physical Address	Type
192.168.8.200	00:0c:29:8d:e5:29	dynamic
192.168.8.206	00:0c:29:8d:e5:29	dynamic
192.168.8.255	ff:ff:ff:ff:ff:ff	static
192.168.111.1	e4-95-5e-45-15-e7	dynamic
192.168.111.26	51-e1-ad-cd-d1-d1	dynamic
192.168.111.45	00:0c:29:8d:e5:29	dynamic
192.168.111.200	00:0c:29:8d:e5:29	dynamic
192.168.111.236	00:0c:29:8d:e5:29	dynamic
224.0.0.22	01-00-5e-00-00-10	static
224.0.0.251	01-00-5e-00-00-1b	static
224.0.0.252	01-00-5e-00-00-fc	static
259.255.255.255	01-00-5e-7f-ff-fa	static

2019-07-25 01:45:10

Host #2... System processes

★↓

2019-07-25 01:45:10

Host #2... Scan WIFI networks

★↓

2019-07-25 01:45:10

Host #2... Preferred WIFI

★↓

2019-07-25 01:45:10

Host #2... Disrupt WIFI

★↓

# Caldera – Review



- Can I Run This at Work?
  - Only in Development environments, unless you are authorized!
- How Do Get This?
  - [Download from github.com](https://github.com)
- Can You Install and Run This?
  - Easily! (though you'll need a few systems or a VM than can host them)

```
yum -y install
yum -y install
vi /etc/sysctl.d
sudo systemctl
vi /etc/passwd
tail -f /var/log
touch /var/log
tail -f /var/log
ip addr
shutdown now &
yum -y update
shutdown now
visudo
nmcli connect
nmcli con add
ifconfig
nmcli con mod
nmcli con reload
hostnamectl st
hostnamectl se
hostnamectl st
hostnamectl re
hostnamectl --
hostnamectl st
ifconfig
nmcli
ifconfig
ping yahoo.com
yum update &&
systemctl stop
systemctl stop
yum list | gre
htop -d 50
top
man dracut
top
yum list | gre
yum -y install
sed -i s/0/1/g
vi /etc/selinux
setenforce 0
sestatus
reboot
netstat -an |
netstat -an |
cd /opt/caldera
find . | grep
ls -al
find .
find . | grep
pwd
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py
caldera.py -d | --debug
caldera.py -h | --help
```

# Adversary Emulation with MITRE's Caldera

Questions?



```
yum -y install  
yum -y install  
vi /etc/sysctl  
sudo systemctl  
vi /etc/passwd  
tail -f /var/  
touch /var/log  
tail -f /var/  
ip addr  
shutdown now &  
yum -y update  
shutdown now  
visudo  
nmcli connecti  
nmcli con add  
ifconfig  
nmcli con mod  
nmcli con rell  
hostnamectl st  
hostnamectl se  
hostnamectl st  
hostnamectl re  
hostnamectl --  
hostnamectl st  
ifconfig  
nmcli  
ifconfig  
ping yahoo.com  
yum update &&  
systemctl stop  
systemctl stop  
yum list | gre  
htop -d 50  
top  
man dracut  
top  
yum list | gre  
yum -y install  
sed -i s/  
vi /etc/selini  
setenforce 0  
sestatus  
reboot  
netstat -an |  
netstat -an |  
cd /opt/calder  
find . | grep  
ls -al  
find .  
find . | grep  
pwd  
[root@calderaserver mklosterman]# cat /opt/caldera/caldera/caldera.py
```

caldera

Usage:

```
caldera.py  
caldera.py -d | --dehug  
caldera.py -h | --help
```