CALDERA

Information Security Inc.

iSEC
information security inc.

Contents

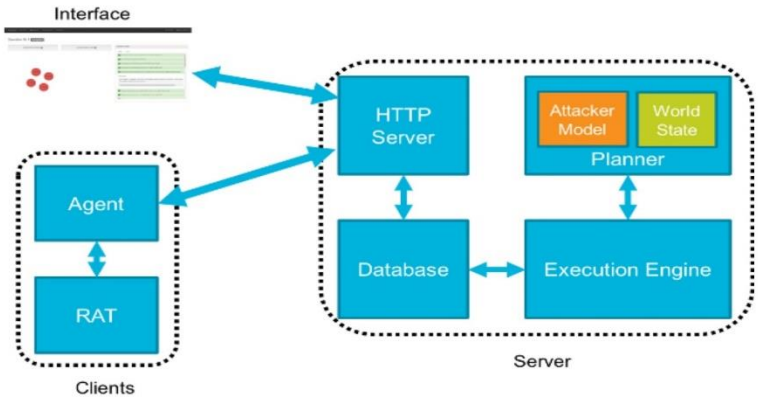
- About CALDERA
- Architecture
- Requirements
- Testing Setup
- Installing CALDERA
- Running CALDERA
- References

About CALDERA

- CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks
- Blueteam => what can you detect and how fast can you handle it

Architecture

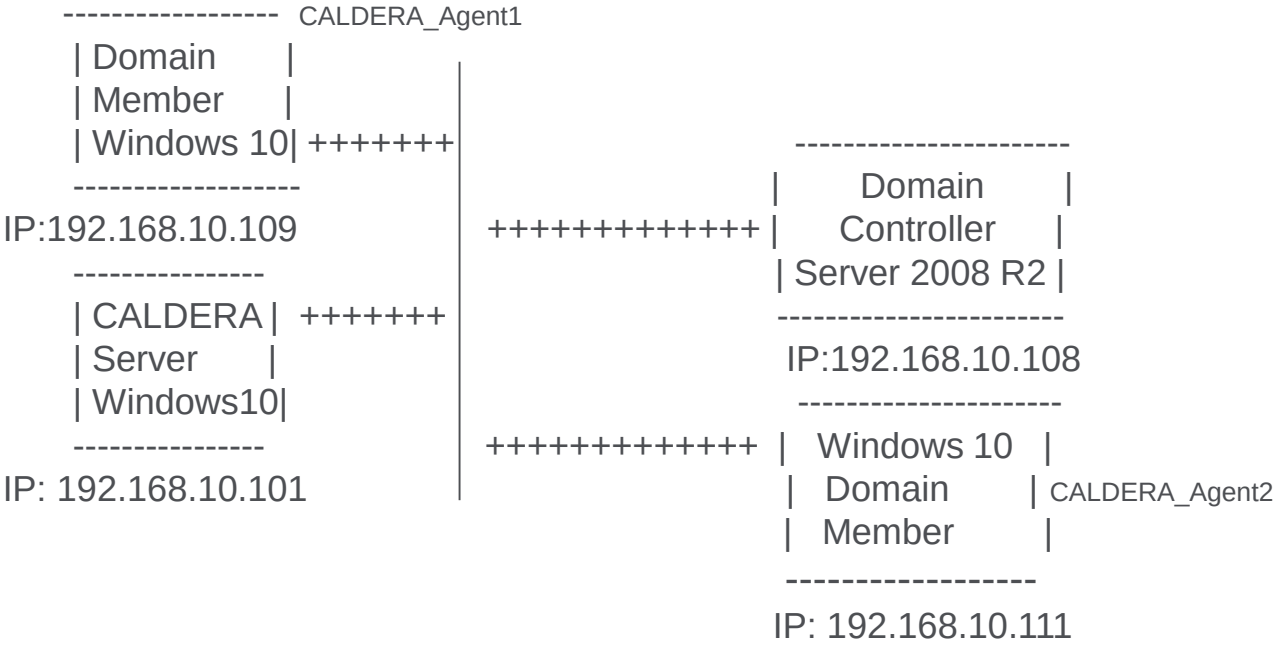
- Server
  - Planner - Decision engine allowing CALDERA to chose actions
    - Attacker Model - Actions available based on ATT&CK
    - World Model - Representation of the environment
  - Execution Engine - Drives actuation of techniques and updates the database
  - Database - Stores knowledge learned about the environment
  - HTTP Server
- Clients
  - Agent - Client on endpoint systems used for communication
  - RAT - Remote access tool used during operations to emulate adversary behavior



Requirements

- CALDERA only supports Windows Enterprise networks that are configured as a Windows Domain
- At a minimum this will contain a Domain Controller running Windows Server 2008 R2 through 2016 and two Windows Enterprise computers joined to that domain
- Because the techniques and tactics currently built into CALDERA are unique to Windows domains
- The CALDERA server can be installed on either Linux or Windows

Testing Setup

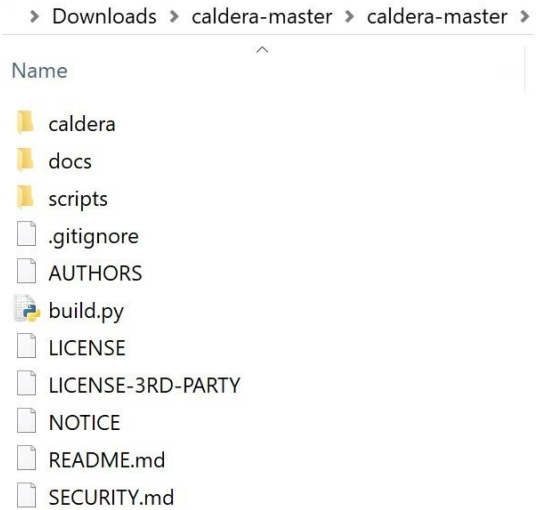


Installing CALDERA

- CALDERA Server Installation on Windows 10
- Download the zip from github and unzip it

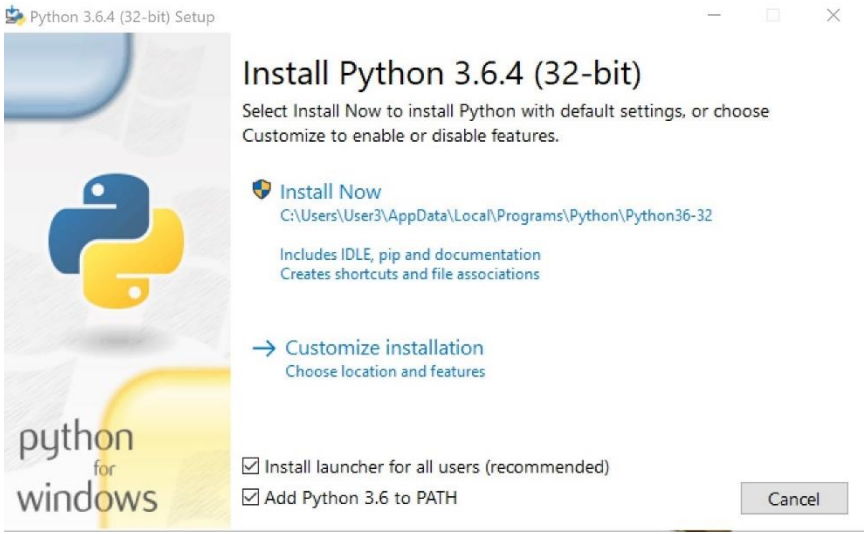
Installing CALDERA

- CALDERA Server Installation on Windows 10
- Download the zip from github and unzip it



Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install Python 3.5.4 or later



Installing CALDERA

- CALDERA Server Installation on Windows 10
- Upgrade to setuptools 24.0 or later

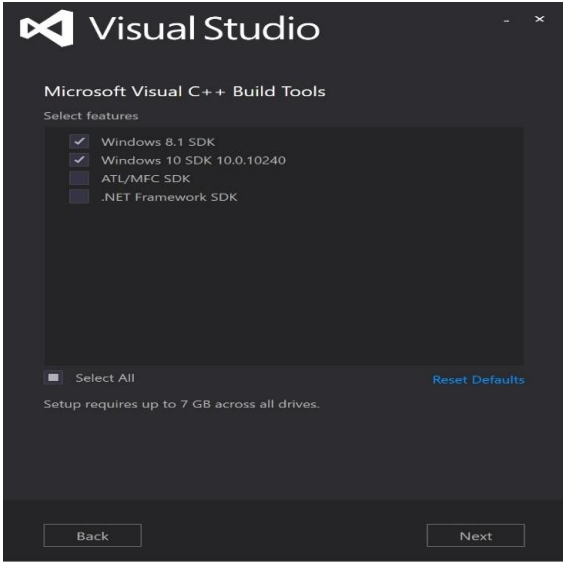
```
C:\Program Files (x86)\Python36-32\Scripts>pip3.6.exe install --upgrade setuptools
Collecting setuptools
  Downloading setuptools-38.5.0-py2.py3-none-any.whl (489kB)
    100% |████████████████████████████████| 491kB 1.6MB/s
Installing collected packages: setuptools
  Found existing installation: setuptools 28.8.0
    Uninstalling setuptools-28.8.0:
      Successfully uninstalled setuptools-28.8.0
Successfully installed setuptools-38.5.0
```

Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install Visual C++ 2015 Build Tools

Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install Visual C++ 2015 Build Tools



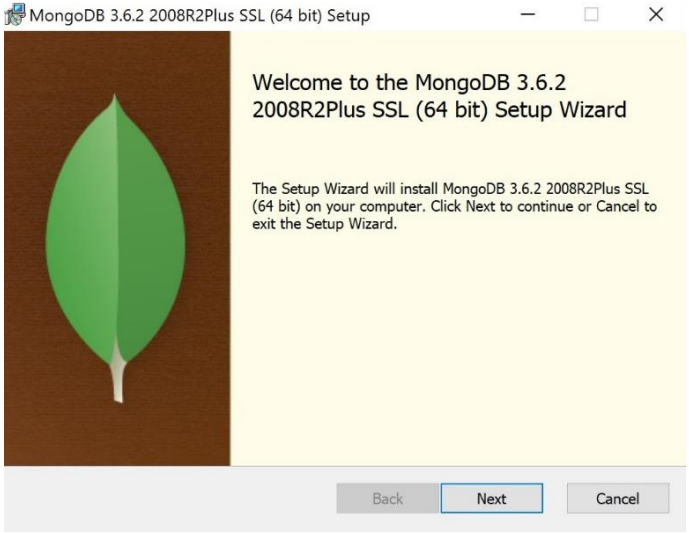
Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install Python libraries

```
C:\Users\User3\Downloads\caldera-master\caldera-master\caldera>pip3 install -r requirements.txt
Collecting aiohttp==2.3.9 (from -r requirements.txt (line 1))
  Using cached aiohttp-2.3.9-cp36-cp36m-win32.whl
Collecting aiohttp-jinja2==0.14.0 (from -r requirements.txt (line 2))
  Using cached aiohttp_jinja2-0.14.0-py3-none-any.whl
Collecting antlr4-python3-runtime==4.7 (from -r requirements.txt (line 3))
  Using cached antlr4-python3-runtime-4.7.tar.gz
Collecting asn1crypto==0.24.0 (from -r requirements.txt (line 4))
  Using cached asn1crypto-0.24.0-py2.py3-none-any.whl
Collecting async-timeout==2.0.0 (from -r requirements.txt (line 5))
  Using cached async_timeout-2.0.0-py3-none-any.whl
Collecting certifi==2017.11.5 (from -r requirements.txt (line 6))
  Using cached certifi-2017.11.5-py2.py3-none-any.whl
Collecting cffi==1.11.4 (from -r requirements.txt (line 7))
  Using cached cffi-1.11.4-cp36-cp36m-win32.whl
Collecting chardet==3.0.4 (from -r requirements.txt (line 8))
  Using cached chardet-3.0.4-py2.py3-none-any.whl
Collecting cryptography==2.1.3 (from -r requirements.txt (line 9))
  Using cached cryptography-2.1.3-cp36-cp36m-win32.whl
Collecting idna==2.6 (from -r requirements.txt (line 10))
  Using cached idna-2.6-py2.py3-none-any.whl
```

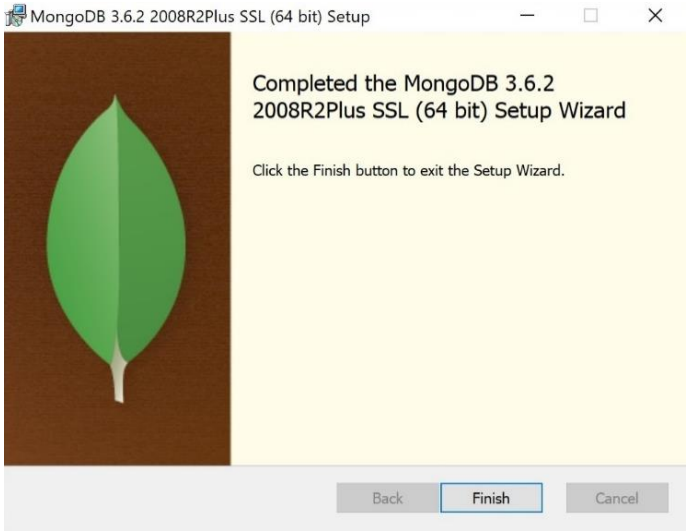
Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install MongoDB



Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install MongoDB



Installing CALDERA

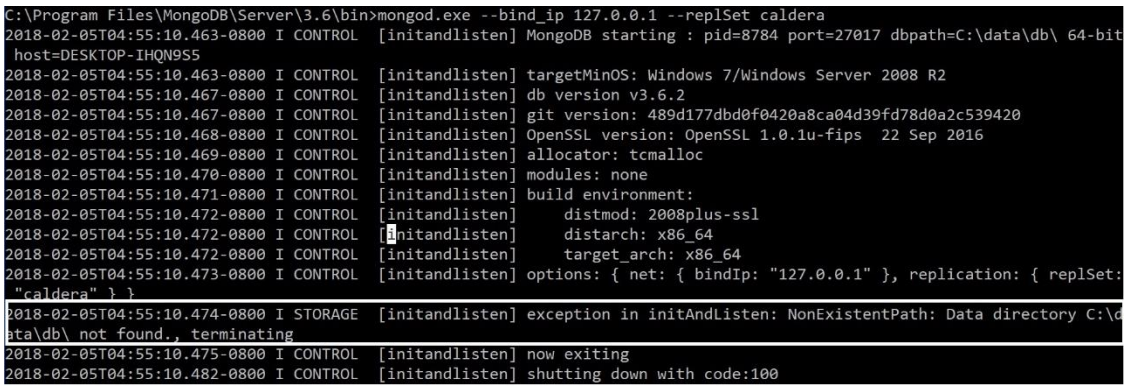
- CALDERA Server Installation on Windows 10
- Install OpenSSL (https://slproweb.com/products/Win32OpenSSL.html)

Installing CALDERA

- CALDERA Server Installation on Windows 10
- Add OpenSSL to PATH => C:¥WINDOWS¥system32>setx path "%path%;C:¥OpenSSL-Win32¥bin"

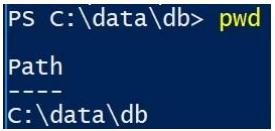
Installing CALDERA

- CALDERA Server Installation on Windows 10
- Start MongoDB => If getting the following error (NonExistentPath: Data directory C:¥data¥db¥ not found., terminating manually) create the folder



Installing CALDERA

- CALDERA Server Installation on Windows 10
- Start MongoDB => If getting the following error (NonExistentPath: Data directory C:¥data¥db¥ not found., terminating manually) create the folder



Installing CALDERA

- CALDERA Server Installation on Windows 10
- Start MongoDB

```
C:\Program Files\MongoDB\Server\3.6\bin>mongod.exe --bind_ip 127.0.0.1 --replSet caldera
2018-02-05T05:02:33.807-0800 I CONTROL  [initandlisten] MongoDB starting : pid=4024 port=27017 dbpath=C:\data\db\ 64-bit
 host=DESKTOP-IHQN9S5
2018-02-05T05:02:33.807-0800 I CONTROL  [initandlisten] targetMinOS: Windows 7/Windows Server 2008 R2
2018-02-05T05:02:33.811-0800 I CONTROL  [initandlisten] db version v3.6.2
2018-02-05T05:02:33.812-0800 I CONTROL  [initandlisten] git version: 489d177dbd0f0420a8ca04d39fd78d0a2c539420
2018-02-05T05:02:33.812-0800 I CONTROL  [initandlisten] OpenSSL version: OpenSSL 1.0.1u-fips  22 Sep 2016
2018-02-05T05:02:33.813-0800 I CONTROL  [initandlisten] allocator: tcmalloc
2018-02-05T05:02:33.814-0800 I CONTROL  [initandlisten] modules: none
2018-02-05T05:02:33.814-0800 I CONTROL  [initandlisten] build environment:
2018-02-05T05:02:33.815-0800 I CONTROL  [initandlisten]     distmod: 2008plus-ssl
2018-02-05T05:02:33.815-0800 I CONTROL  [initandlisten]     distarch: x86_64
2018-02-05T05:02:33.816-0800 I CONTROL  [initandlisten]     target_arch: x86_64
2018-02-05T05:02:33.816-0800 I CONTROL  [initandlisten] options: { net: { bindIp: "127.0.0.1" }, replication: { replSet:
 "caldera" } }
```

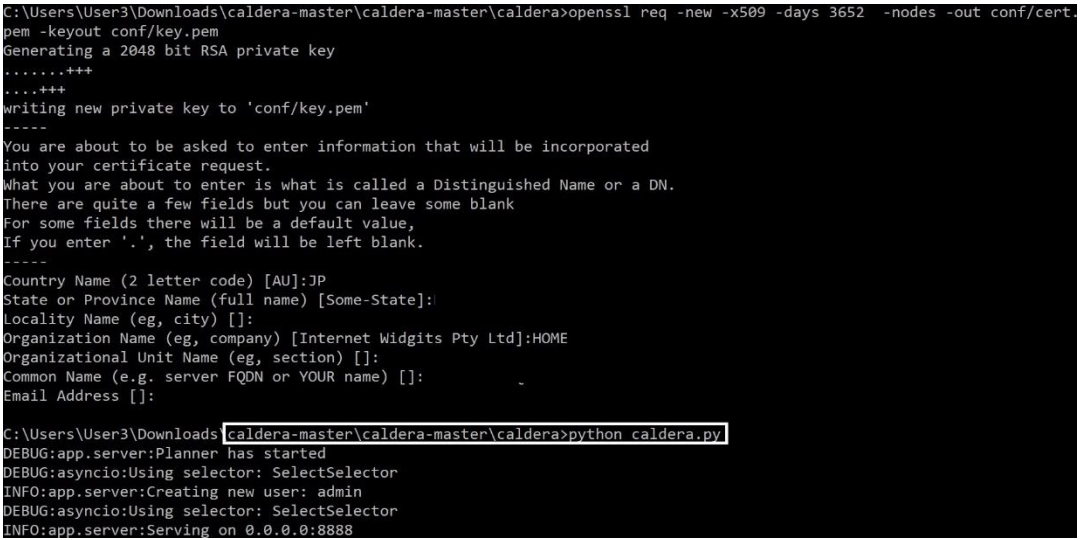
Installing CALDERA

- CALDERA Server Installation on Windows 10
- Install CraterMain.exe => It should be placed in: (C:¥Users¥User3¥Downloads¥caldera-master¥caldera-master¥dep¥crater¥crater¥CraterMain.exe) on the computer that the CALDERA server is installed on

```
PS C:\Users\User3\Downloads\caldera-master\caldera-master\dep\crater\crater> pwd

Path
----
C:\Users\User3\Downloads\caldera-master\caldera-master\dep\crater\crater


PS C:\Users\User3\Downloads\caldera-master\caldera-master\dep\crater\crater> ls


    Directory: C:\Users\User3\Downloads\caldera-master\caldera-master\dep\crater\crater


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/5/2018   5:05 AM          17920 CraterMain.exe
```

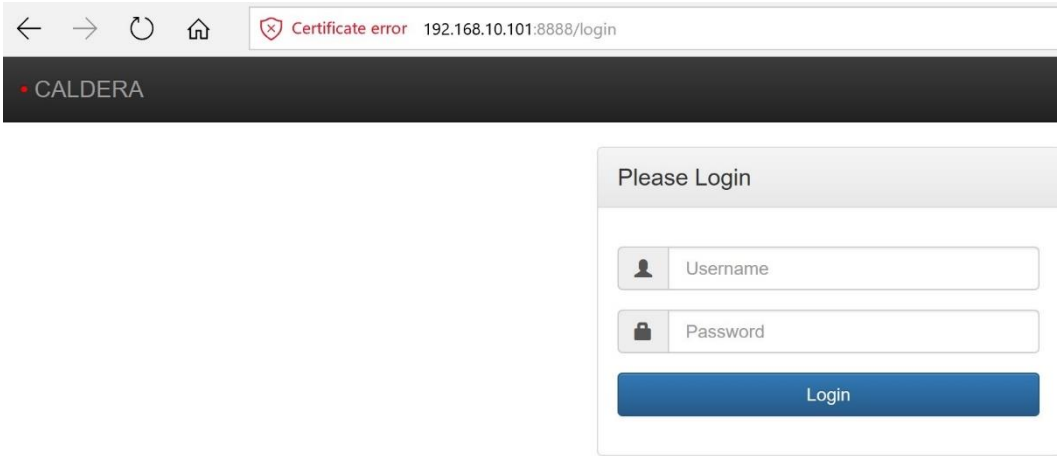
Running CALDERA

- Start the CALDERA server



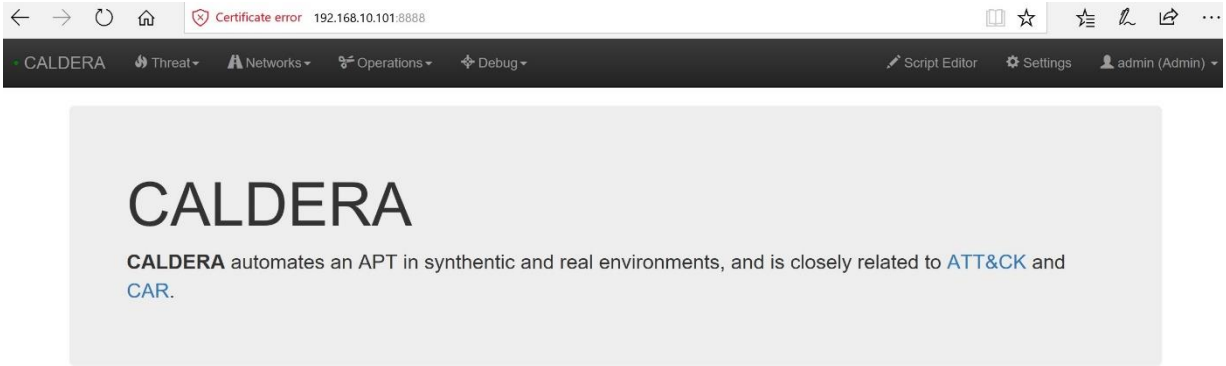
Running CALDERA

- Login to the Caldera server => username: admin
- password: caldera



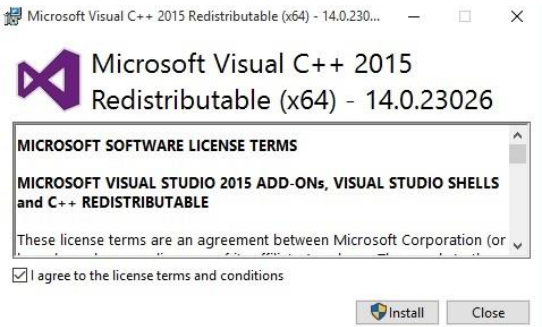
Running CALDERA

- Login to the Caldera server => username: admin
- password: caldera



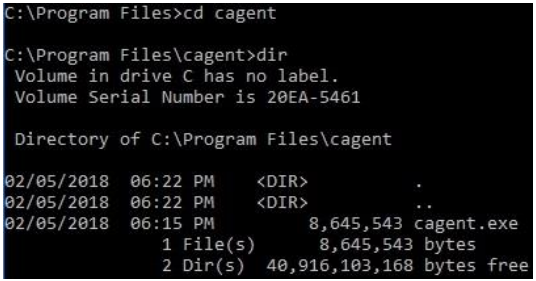
Installing CALDERA

- CALDERA Agent Installation
- The CALDERA Agent or cagent, is installed on every computer participating in the Adversary Emulation
- It should be accessible over the network to the CALDERA server
- Install the Visual C++ Redistributable for Visual Studio 2015



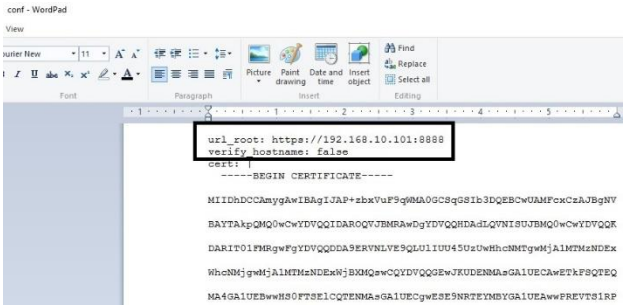
Installing CALDERA

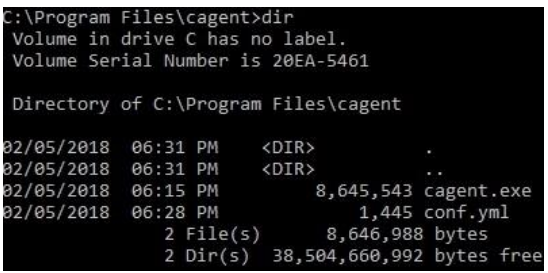
- CALDERA Agent Installation
- Download the latest release of cagent(https://github.com/mitre/caldera-agent/releases)
- Place cagent.exe in the desired installation location (the recommended location is C:¥Program Files¥cagent¥cagent.exe)



Installing CALDERA

- CALDERA Agent Installation
- In the same directory, place the conf.yml file which can be downloaded from the CALDERA server by navigating to https://192.168.10.101:8888/conf.yml





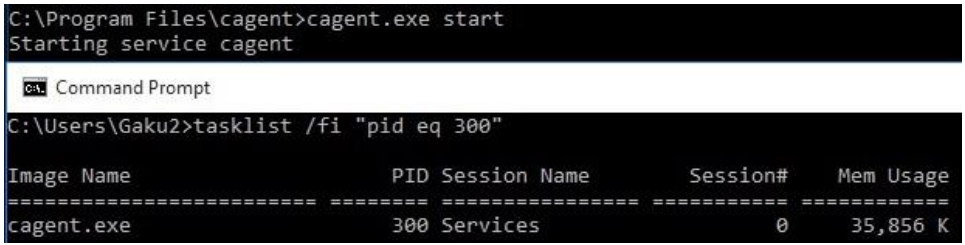
Installing CALDERA

- CALDERA Agent Installation
- In an Administrator command prompt install cagent with “cagent.exe --startup auto install”

```
C:\Program Files\cagent>cagent.exe --startup auto install
Installing service cagent
Service installed
```

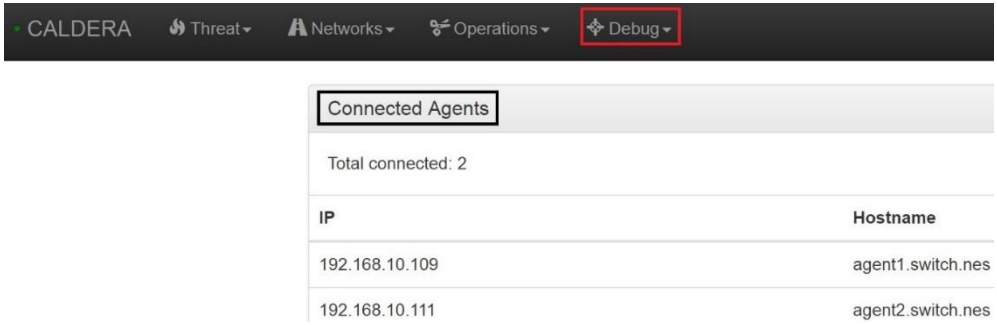
Running CALDERA

- CALDERA Agent
- In an Administrator command prompt start cagent with “cagent.exe start”



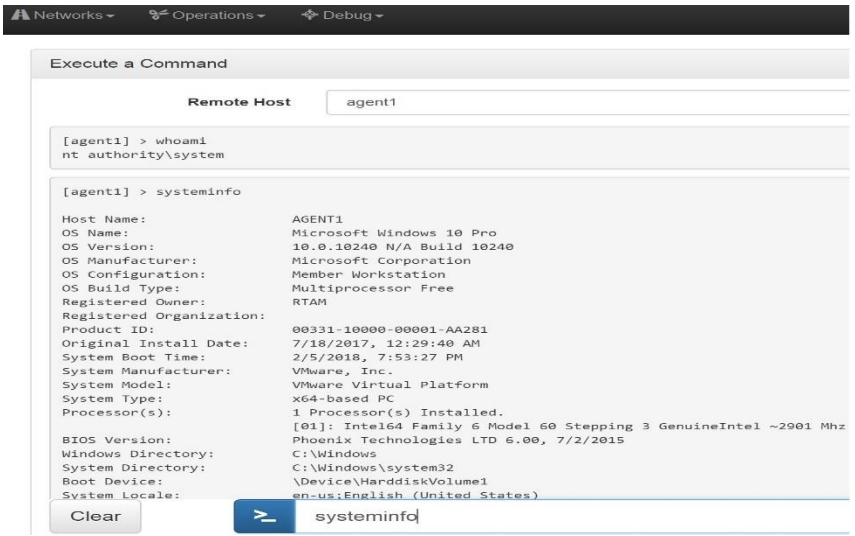
Running CALDERA

- CALDERA Agent
- Agents that are connected to the CALDERA server are visible by checking the Debug>Connected Agents tab



Installing CALDERA

- CALDERA Agent Installation
- Send remote commands to the remote host (Agent)



References

- CALDERA documentation
https://caldera.readthedocs.io/en/latest/

- MongoDB
https://www.mongodb.com/download-center#community

- OpenSSL
https://slproweb.com/products/Win32OpenSSL.html

- Caldera Crater
https://github.com/mitre/caldera-crater/releases

- Caldera Agent
https://github.com/mitre/caldera-agent/releases