CALDERA Update 1

Information Security Inc.

Contents

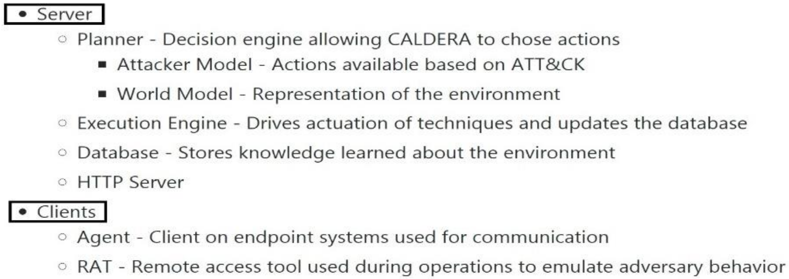
- About CALDERA
- Architecture
- Requirements
- Testing Setup
- Creating a CALDERA Network
- Running an Operation on the created Network
- References

About CALDERA

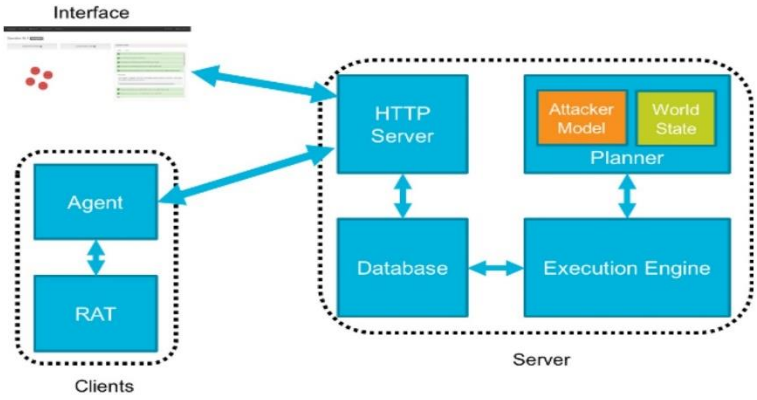
- CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks

- Blueteam => what can you detect and how fast can you handle it

Architecture



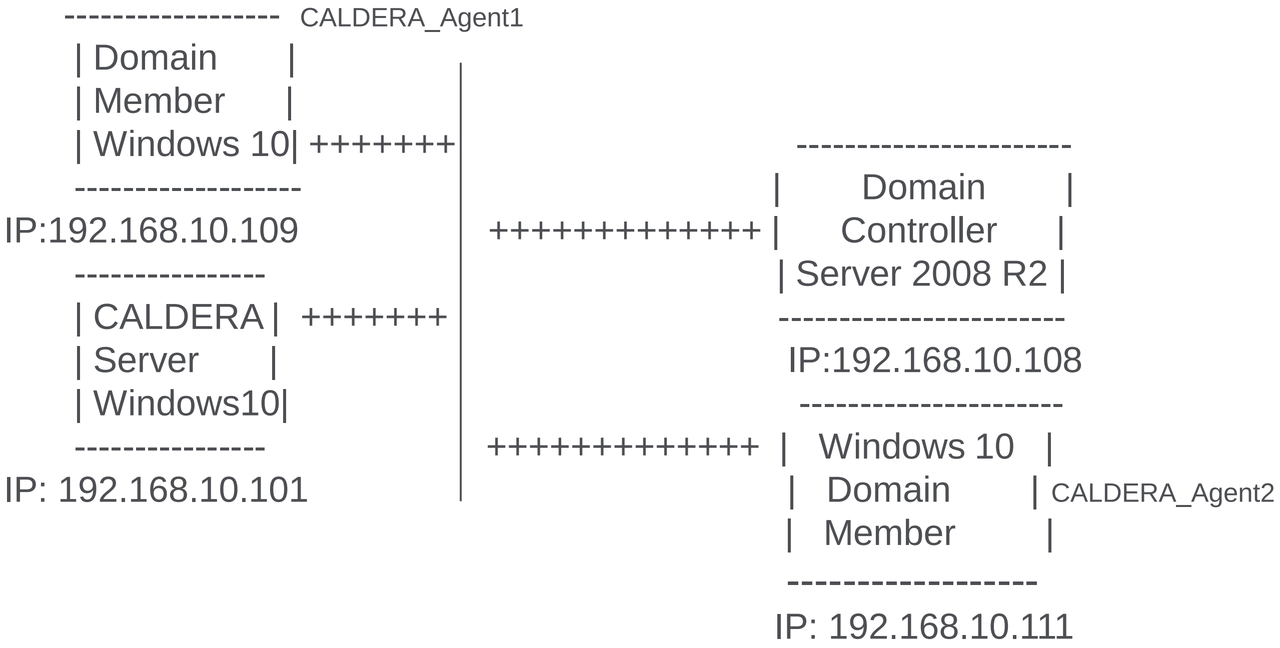
- Server
  - Planner - Decision engine allowing CALDERA to chose actions
    - Attacker Model - Actions available based on ATT&CK
    - World Model - Representation of the environment
  - Execution Engine - Drives actuation of techniques and updates the database
  - Database - Stores knowledge learned 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



CALDERA_Agent1

Domain Member Windows 10

IP:192.168.10.109

CALDERA Server Windows10

IP: 192.168.10.101

Domain Controller Server 2008 R2

IP:192.168.10.108

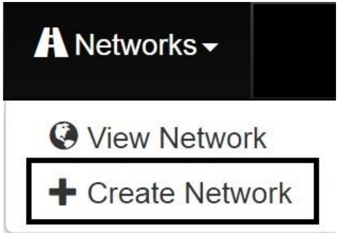
Windows 10 Domain Member

CALDERA_Agent2

IP: 192.168.10.111

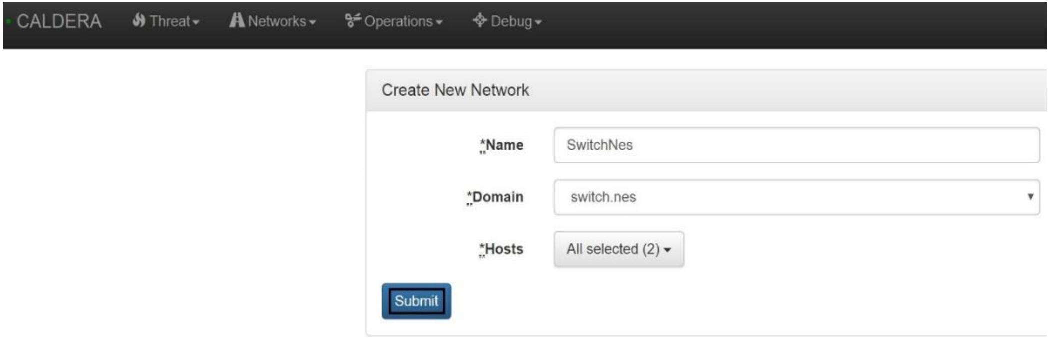
Creating a CALDERA Network

- Creating a CALDERA Network



Creating a CALDERA Network

- Creating a CALDERA Network, Networks are just collections of host, a simple way for CALDERA to organize and group together computers



Create New Network

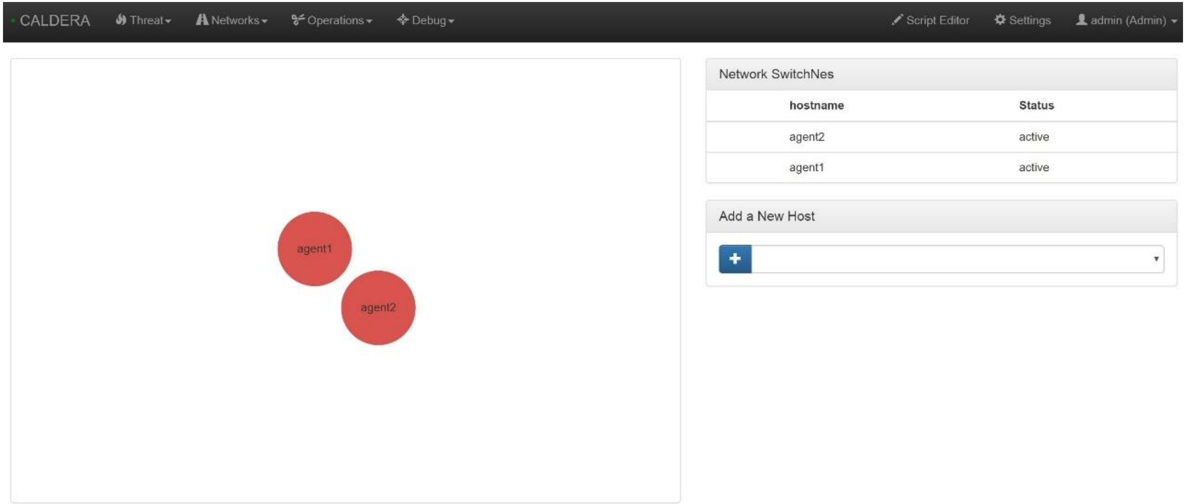
*Name SwitchNes

*Domain switch.nes

*Hosts All selected (2)

Creating a CALDERA Network

- Creating a CALDERA Network



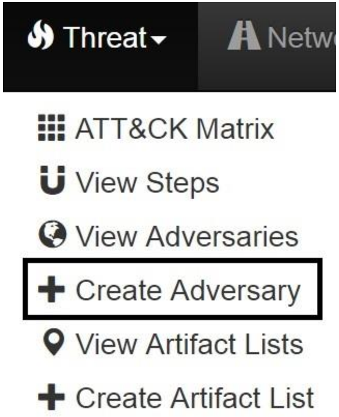
Network SwitchNes

hostname	Status
agent2	active
agent1	active

Add a New Host

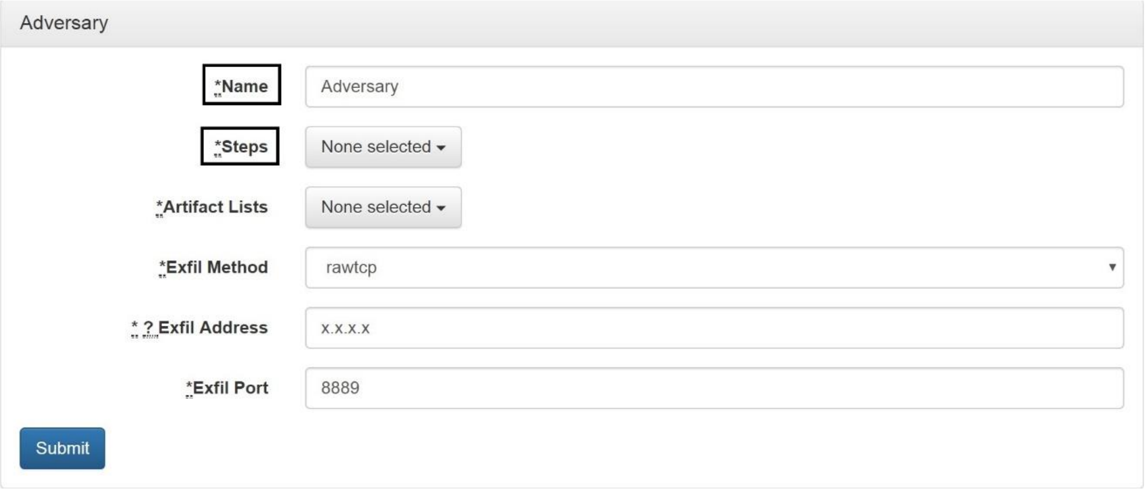
Running an Operation on the created Network

- Creating Adversary



Running an Operation on the created Network

- Creating Adversary

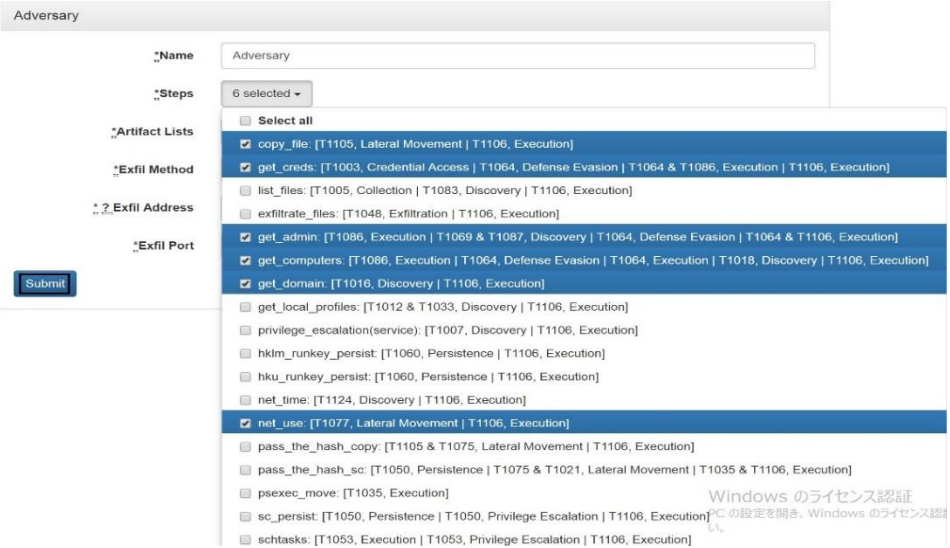


Adversary

*Name	Adversary
*Steps	None selected ▾
*Artifact Lists	None selected ▾
*Exfil Method	rawtcp ▾
* ? Exfil Address	x.x.x.x
*Exfil Port	8889

Running an Operation on the created Network

- Creating Adversary



Adversary

*Name: Adversary

*Steps: 6 selected ▾

- □ **Select all**
- ☑ copy_file: [T1105, Lateral Movement | T1106, Execution]
- ☑ get_creds: [T1003, Credential Access | T1064, Defense Evasion | T1064 & T1086, Execution | T1106, Execution]
- □ list_files: [T1005, Collection | T1083, Discovery | T1106, Execution]
- □ exfiltrate_files: [T1048, Exfiltration | T1106, Execution]
- ☑ get_admin: [T1086, Execution | T1069 & T1087, Discovery | T1064, Defense Evasion | T1064 & T1106, Execution]
- ☑ get_computers: [T1086, Execution | T1064, Defense Evasion | T1064, Execution | T1018, Discovery | T1106, Execution]
- ☑ get_domain: [T1016, Discovery | T1106, Execution]
- □ get_local_profiles: [T1012 & T1033, Discovery | T1106, Execution]
- □ privilege_escalation(service): [T1007, Discovery | T1106, Execution]
- □ hklm_runkey_persist: [T1060, Persistence | T1106, Execution]
- □ hku_runkey_persist: [T1060, Persistence | T1106, Execution]
- □ net_time: [T1124, Discovery | T1106, Execution]
- ☑ net_use: [T1077, Lateral Movement | T1106, Execution]
- □ pass_the_hash_copy: [T1105 & T1075, Lateral Movement | T1106, Execution]
- □ pass_the_hash_sc: [T1050, Persistence | T1075 & T1021, Lateral Movement | T1035 & T1106, Execution]
- □ psexec_move: [T1035, Execution]
- □ sc_persist: [T1050, Persistence | T1050, Privilege Escalation | T1106, Execution]
- □ schtasks: [T1053, Execution | T1053, Privilege Escalation | T1106, Execution]

*Artifact Lists

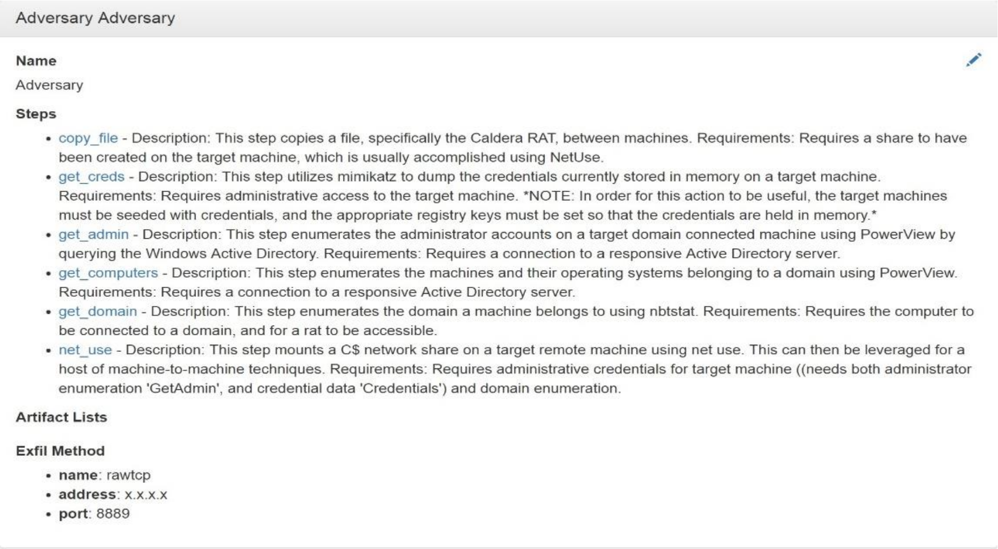
*Exfil Method

* ? Exfil Address

*Exfil Port

Running an Operation on the created Network

- Creating Adversary



Adversary Adversary

Name

Adversary

Steps

- copy_file - Description: This step copies a file, specifically the Caldera RAT, between machines. Requirements: Requires a share to have been created on the target machine, which is usually accomplished using NetUse.
- get_creds - Description: This step utilizes mimikatz to dump the credentials currently stored in memory on a target machine. Requirements: Requires administrative access to the target machine. *NOTE: In order for this action to be useful, the target machines must be seeded with credentials, and the appropriate registry keys must be set so that the credentials are held in memory.*
- get_admin - Description: This step enumerates the administrator accounts on a target domain connected machine using PowerView by querying the Windows Active Directory. Requirements: Requires a connection to a responsive Active Directory server.
- get_computers - Description: This step enumerates the machines and their operating systems belonging to a domain using PowerView. Requirements: Requires a connection to a responsive Active Directory server.
- get_domain - Description: This step enumerates the domain a machine belongs to using nbtstat. Requirements: Requires the computer to be connected to a domain, and for a rat to be accessible.
- net_use - Description: This step mounts a C$ network share on a target remote machine using net use. This can then be leveraged for a host of machine-to-machine techniques. Requirements: Requires administrative credentials for target machine ((needs both administrator enumeration 'GetAdmin', and credential data 'Credentials') and domain enumeration.

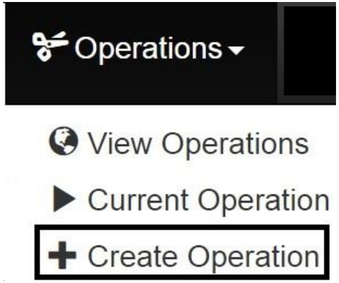
Artifact Lists

Exfil Method

- **name**: rawtcp
- **address**: x.x.x.x
- **port**: 8889

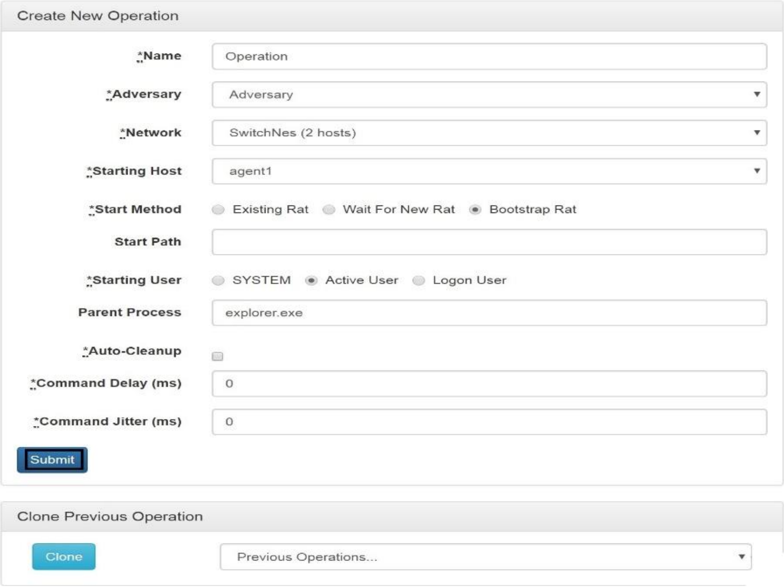
Running an Operation on the created Network

- Running the Adversary on the created Network



Running an Operation on the created Network

- Running the Adversary on the created Network



Create New Operation

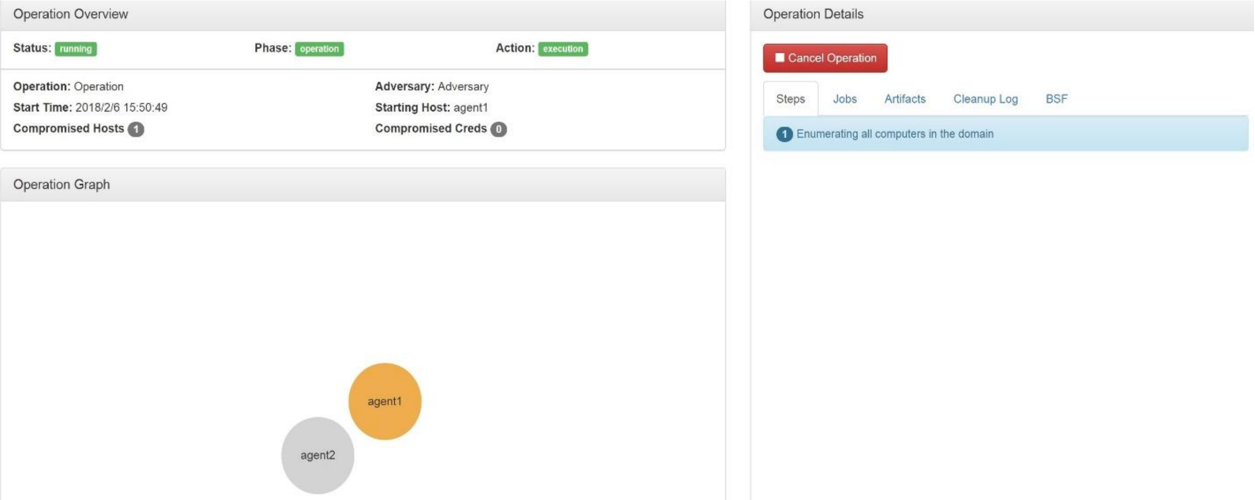
*Name	Operation
*Adversary	Adversary ▾
*Network	SwitchNes (2 hosts) ▾
*Starting Host	agent1 ▾
*Start Method	○ Existing Rat ○ Wait For New Rat ● Bootstrap Rat
Start Path	
*Starting User	○ SYSTEM ● Active User ○ Logon User
Parent Process	explorer.exe
*Auto-Cleanup	□
*Command Delay (ms)	0
*Command Jitter (ms)	0

Clone Previous Operation

Previous Operations... ▾

Running an Operation on the created Network

- Running the Adversary on the created Network



Operation Overview

Status: running **Phase:** operation **Action:** execution

Operation: Operation
Start Time: 2018/2/6 15:50:49
Compromised Hosts 1

Adversary: Adversary
Starting Host: agent1
Compromised Creds 0

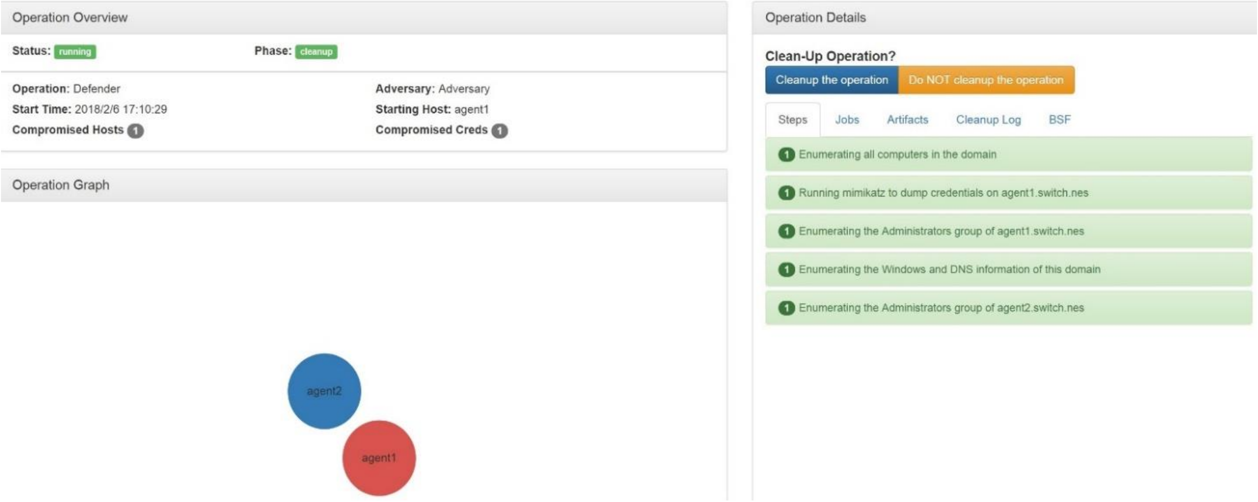
Operation Graph

Operation Details

1 Enumerating all computers in the domain

Running an Operation on the created Network

- Running the Adversary on the created Network



Operation Overview

Status: running **Phase:** cleanup

Operation: Defender
Start Time: 2018/2/6 17:10:29
Compromised Hosts 1

Adversary: Adversary
Starting Host: agent1
Compromised Creds 1

Operation Graph

Operation Details

Clean-Up Operation?

1 Enumerating all computers in the domain

1 Running mimikatz to dump credentials on agent1.switch.nes

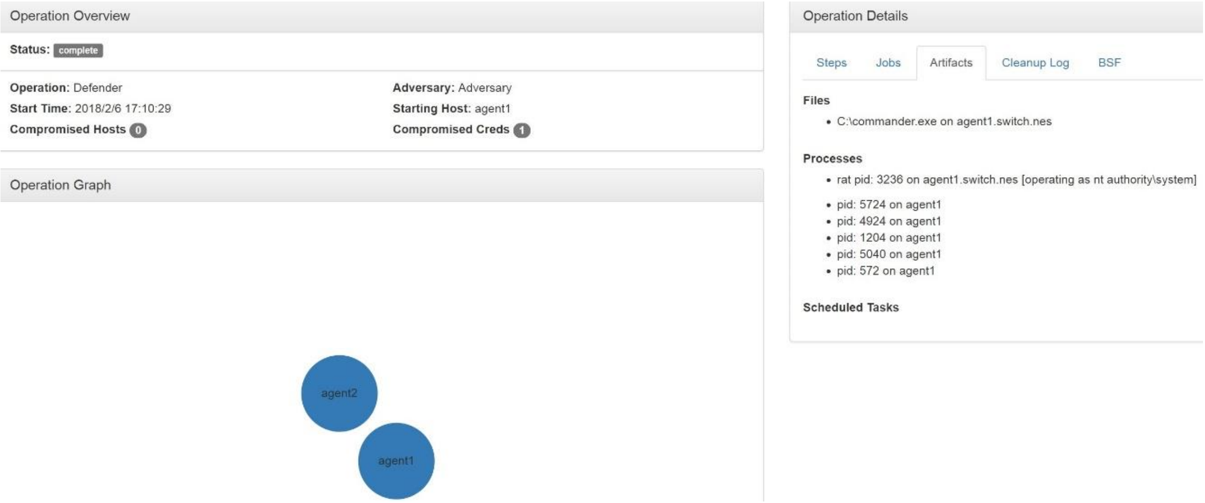
1 Enumerating the Administrators group of agent1.switch.nes

1 Enumerating the Windows and DNS information of this domain

1 Enumerating the Administrators group of agent2.switch.nes

Running an Operation on the created Network

- Running the Adversary on the created Network



Operation Overview

Status: complete

Operation: Defender
Start Time: 2018/2/6 17:10:29
Compromised Hosts 0

Adversary: Adversary
Starting Host: agent1
Compromised Creds 1

Operation Graph

Operation Details

Files

- C:\commander.exe on agent1.switch.nes

Processes

- rat pid: 3236 on agent1.switch.nes [operating as nt authority\system]
- pid: 5724 on agent1
- pid: 4924 on agent1
- pid: 1204 on agent1
- pid: 5040 on agent1
- pid: 572 on agent1

Scheduled Tasks

References

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

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