# caldera介绍

1、概述

cadera是一个自动的攻击者仿真工具，模拟攻击者在windows企业网络中占据了一个立足点之后的行为。

caldera工作原理是利用其内置的语义模型来描述Windows企业域的结构，描述攻击者目标和行为的攻击者模型，以及决定要执行哪些操作的人工智能规划器。caldera通过生成一系列攻击计划，到window主机实现这些计划，以便生成真实且相同的数据；caldera远程访问工具(RAT)，能在受感染的主机上执行攻击者操作，通过网络复制自身。

2、功能

作为一个完全自动化的工具，防御者可以使用CALDERA来验证防御是否有效，并作为测试防御工具。另外，CALDERA的模块化设计允许用户定制每个单独的操作，以便用户可以将自己的技术融入CALDERA的自动评估中。

3、流程

(1)、caldera将RAT传感器装在域网络中的每台window主机，用于主机和caldera服务器通信。

(2)、caldera通过用户配置的攻击步骤在caldera引擎中生成计划列表 。

(3)、依次执行列表中的攻击步骤，然后将步骤传入RAT传感器，使得window主机执行相应的指令，并将成功与否的结果传回给caldera服务器。

(4)、如果当前步骤执行成功，重新生成计划执行。如果当前步骤失败，执行计划中的下个步骤。

(5)、直到没有计划执行，结束操作。

3、参考资料

与caldera相关论文

(1)、ANALYSIS OF AUTOMATED ADVERSARY EMULATION TECHNIQUES

(2)、Intelligent, Automated Red Team Emulation

与caldera相关网站

(1)、<https://github.com/mitre/caldera/>

Caldera工具地址

(2)、<https://attack.mitre.org/>

ATT&CK知识库地址

(3)、<https://github.com/redcanaryco/atomic-red-team/tree/master/atomics>

每个技术能否执行的测试