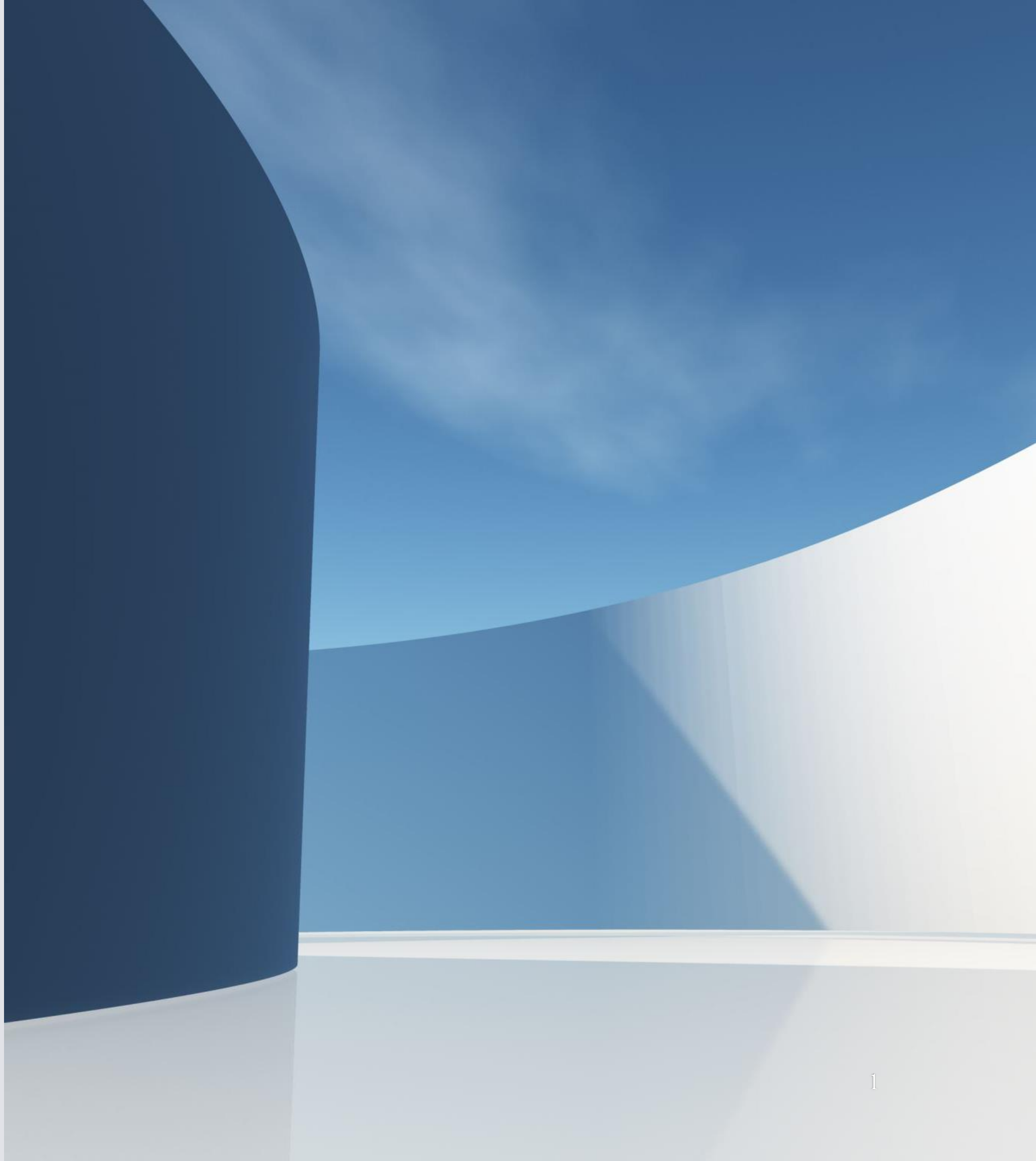
NOVEMBER 8TH UPDATE

GRID-SIEM
Group 29



SECURITY ONION IMPLEMENTATION & GRAVWELL UPDATES

- Demo: November 14th
- Attempted to set up the manager node on sensor 3 as opposed to the manager but was failing the verification.
- Setting up a manager node is adjusting the firewall rules.
- Can ping from the manager node to sensors, but sensors cannot ping master nodes.
- Troubleshooting led to people online declaring it was an issue with the NAT or networking.
- Exploring ways around this configuration or possibly implementing manager search nodes instead.
- https://iowastate-my.sharepoint.com/:w:/r/personal/docompo_iastate_edu/_layouts/15/Doc.aspx?sourcedoc=%7B534B0AA9-BBC6-4E17-897D-AAD267BD09F8%7D&file=Security%20Onion%20Installation%20Guide.docx&action=default&mobileredirect=true

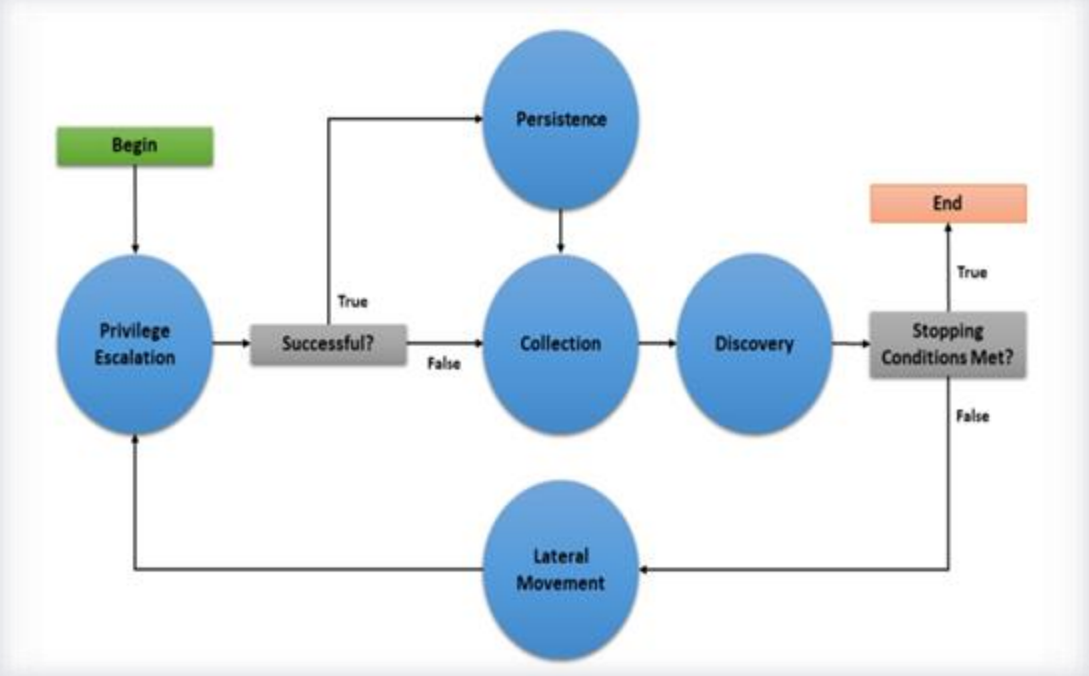
MITRE CALDERA AUTONOMOUS VS. MANUAL RED-TEAM ENGAGEMENTS

- Base option - Autonomous
  - Can use the framework to build specific adversary profile to launch against the grid
  - The process involves:
    - Logging in as a 'red' user
    - Deploying an agent
      - Choosing the victim operating system
    - Selecting an adversary
      - Has stockpile options to choose from
    - Running the operation & viewing the results
- Additional option - Manual
  - Caldera provides the ability to build your own custom plugins and agents
  - Useful when you want to remain undetected from existing defense capabilities
  - Utilizes the Manx agent to deploy manual attacks
  - Simply allows you to run custom attacks not covered in Caldera

  - https://github.com/mitre/stockpile/tree/master

AUTONOMOUS OPTIONS & IMPLEMENTATIONS

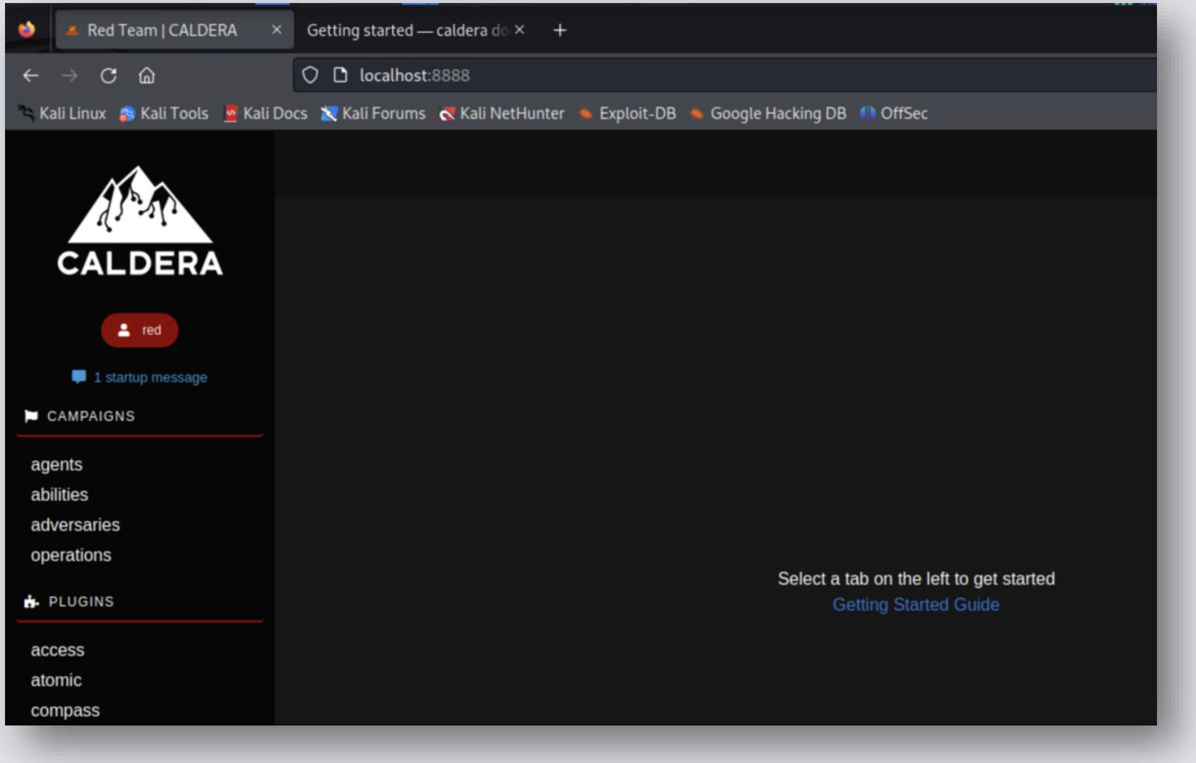
- Enables us to build and launch custom adversary profiles. Emulating a specific APT attack style.
- Procedure: Launch Caldera server, deploy an agent in the web app console select an adversary profile and run the operation, review and oversee the running operation, export the operation results.
- Plugins: Numerous plugins available that allow us to add simulated agents, work with reverse shells, autonomous incident response capabilities, etc.
- Debrief plugin: especially useful to display an overview of a campaign.



Example of a planner.

MANUAL OPTIONS & IMPLEMENTATIONS

- Done using a Manx agent. (Plugin installed)
- Mitre Caldera on Kali VM (Installed).
- Caldera for OT – Optional plugins are available to attack OT systems. The Modbus plugin leverages the pyModbus Library to expose native functionality of the Modbus protocol to Caldera. (Pluggin Installed).
- Tutorial: To learn how to use Caldera, navigate to the Training plugin and complete the capture-the-flag style course.



Select a tab on the left to get started
Getting Started Guide