SAND2020-7292D

The Center for Cyber Defenders

Expanding computer security knowledge

MOSAICS

Red Teaming to Improve Security of Industrial Control Systems

Callie Aboaf, Cornell University
Derek Dervishian, Purdue University

Project Mentor: Tim Schulz, Org. 5689

Problem Statement

Industrial Control Systems (ICS) are systems used to control industrial processes. These processes usually involve the operating of heavy machinery that keeps them running smoothly day and night.

These systems are increasingly connected to the internet. While this can improve convenience and functionality, systems connected to the internet are vulnerable to cyberattacks. It can be very costly if industrial control systems, like dams or power grids, are compromised. As such, the Department of Homeland Security has deemed this a critical infrastructure sector.

Currently, many of these systems have inadequate security infrastructure. The MOSAICS project seeks to improve their security.

Objectives and Approach

More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capabilities Technology Demonstration (JCTD) is a Department of Defense (DOD) effort to develop and demonstrate an operational capability for enhanced situational awareness and defense of industrial control systems associated with task critical assets from non-kinetic attacks.

MITRE's CALDERA is an open-source red teaming tool that is used to simulate adversary behaviors using the MITRE ATT&CK framework. As red teamers, our goals are to emulate adversary behaviors and identify security weaknesses. CALDERA helps us reach our goals by enabling us to test specific aspects of a network's security. CALDERA's capabilities can be expanded even further by adding additional features specifically for ICS security testing.

Results

We evaluated MITRE's CALDERA tool to determine whether its capabilities meet the testing needs of the project.

We added functionality to CALDERA by designing and implementing custom plugins to fill testing gaps.

- We created a plugin that allows us to create new adversaries to emulate.
- We created a plugin that enables us to scan and pull device information from ICS devices within a network.

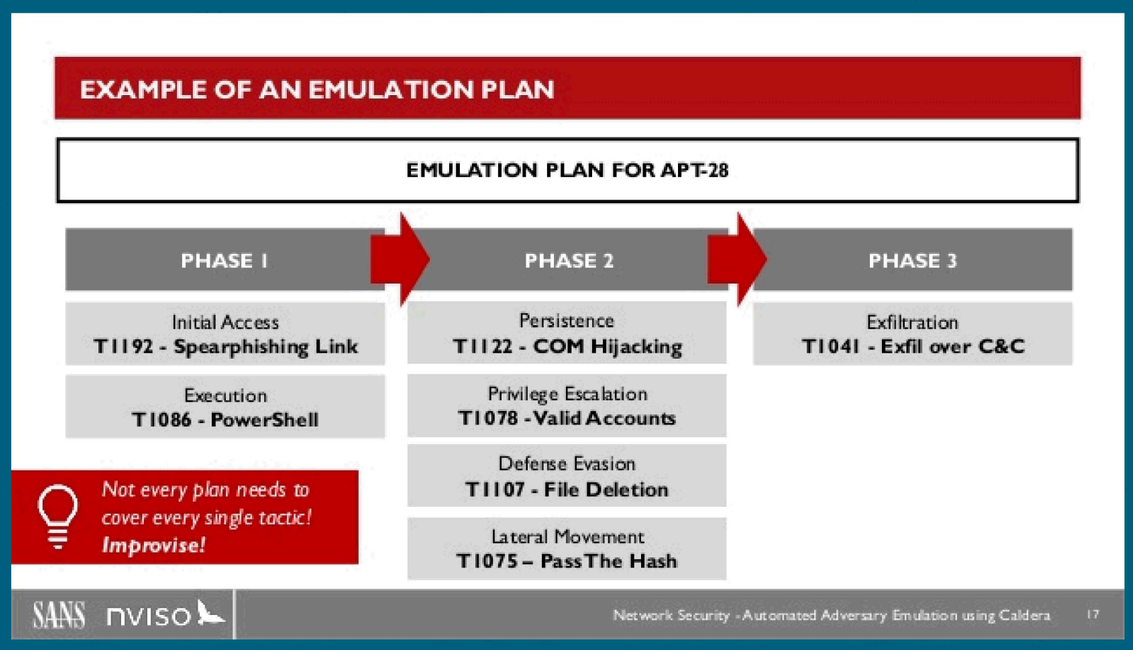
These additional features make CALDERA a much more powerful tool and tailor it to our security testing.

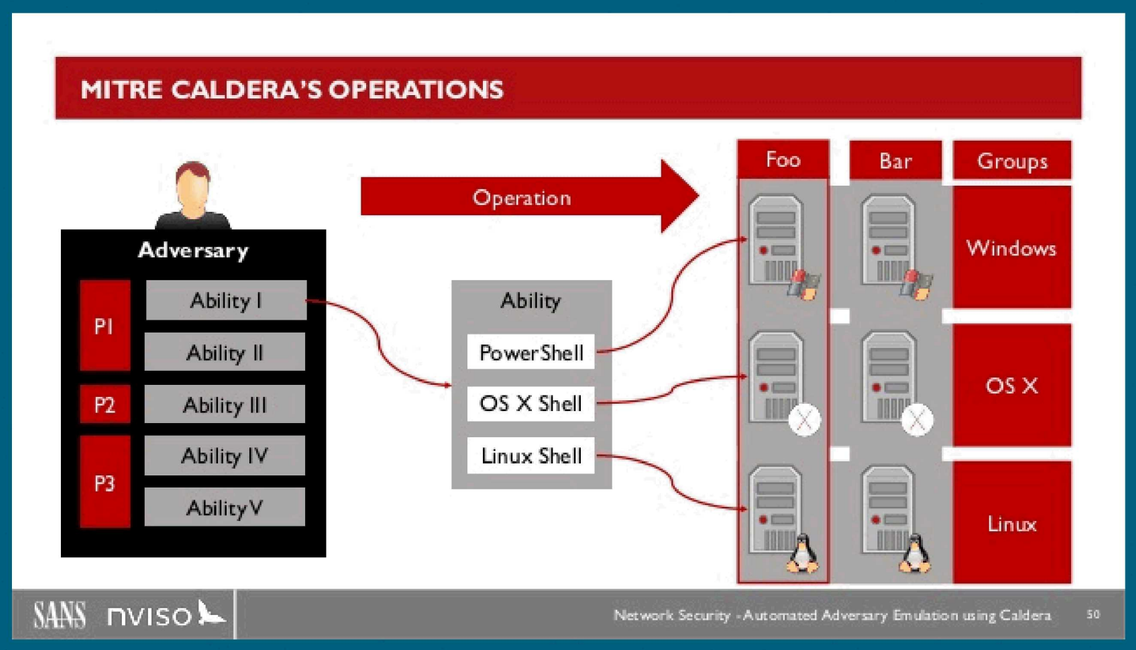
Impact and Benefits

Robust testing benefits system architects in validating and verifying defensive cyber security capabilities. Our use of CALDERA to simulate adversarial behavior enables defenders to train in identifying and mitigating attacks.

Our tests reference the ATT&CK framework, a knowledge base of adversary tactics and techniques based on real-world data built to help defenders. This enables us to communicate with the blue team using a "common language" and emulate particular adversaries with which we are concerned.

The CALDERA application is modular so we can add ICS specific functionality for testing. By creating custom features we can better test the security of the network and keep it safe from new and evolving threats.





Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-XXXX X.