SAND2019-9511C

Automation of Red Team Assessment activities

Russel Waymire, IDART Vulnerability Assessments

8/13/2019

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

Project Overview

- Sandia's Red Teams work to provide vulnerability assessments on various private and government sector systems. Sandia's unique approach to vulnerability assessments by taking a defense-in-depth look at systems, their intended use, and unforeseen avenues of exploitation is the focus of the IDART methodology. Sandia leverages this capability to help harden systems of National Security importance.
- Current efforts involve looking at system data (including system documentation and configuration data) before performing an on-site assessment of target system .
- Final artifacts of the effort are usually an assessment report with findings, justification, and recommendations.
- Key resources are expert assessors, time, and system access.

The Problem

- Time and availability of Subject Matter Experts (SMEs) is the most pressing issue.
- Consistency between various Red Teams in their findings, mappings, and pedigree of supporting data.
- Large data sets from various sources create constraints on ability to look closely at the data and understand the entire picture in a manageable way.

Possible Solution

- Use Machine Learning and/or Natural Language Processing along with scripted processes to:
  - Ingest source system documentation and configuration data with the intent to map it to sets of security controls or findings in an assessment report.

Difficulties to Overcome

- Identifying inferences in system documentation
- Generating a generic capability to map from source to target over different systems with different forms of documentation, security controls, and configuration data.
- We do not anticipate that we will ever be able to completely automate Red Team analyst abilities but are looking to filter system data and results in a way that can improve efficiency and reduce the workload of the analyst.