SAND2016-4414PE

Exceptional service in the national interest

Sandia National Laboratories

TracerFIRE

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Sand2016-????

Cyber Tracer Program

Sandia National Laboratories

- Our mission is to conduct research and develop techniques to:
  - Create a community of cyber defenders sharing expertise, skills, and competencies that raises the standards of individuals and the overall community of defenders
  - Attract, inspire, and grow the next generation of expert cyber defenders for the US
  - Support educational institutions to create educational capabilities and infrastructure to foster the development of future cyber defenders

TracerFIRE (Forensic Incident Response Exercise)

Sandia National Laboratories

- Focus is on Incident Response Training
- Real World Exercise Requires Student to Put the Pieces of the Incident Together or What is Referred to as the Cyber Kill Chain
  - Who is the adversary?
  - How did they get in?
  - What did they want and did they acquire it?
  - How to prevent recurring incidents?
- Students Investigate an APT (Advanced Persistent Threat) Style Adversary Throughout the Event
- TracerFIRE Team Provides the Expertise, Infrastructure, & Network for the Exercise

Goal of TracerFIRE

Allow students to achieve this state of “Flow” in Cyber Incident Response

Flow

“ is the mental state of operation in which a person in an activity is fully immersed in a feeling of energized focus, full involvement, and success in the process of the activity.”

Mihaly Csikszentmihalyi

Scenario Driven Learning

- TF5 Scenario was created with the concept of narrative based learning:
- Enables participants to enhance their understanding of cyber related problems and their solutions in contextually-meaningful ways
- Similar to medical education where students spend time in residency before qualification as a doctor.

ShmuxBux Coffee Company Under Attack

Incident Responders Learning

Sandia National Laboratories

- How to recognize adversarial tactics within the context of the kill chain:
  - Reconnaissance
  - Attack vector
  - Exploitation
  - Exfiltration
- Implicit Learning objectives:
  - Look beyond the clues
  - Infer adversarial intention!
  - Overall goal is to promote critical thinking

TracerFIRE

Sandia National Laboratories

Self Select Teams

Team 1

Team 2

Team 3

Day 1

Concept & Tool Training

Incident Response Exercise

Day 2

Concept & Tool Training

Incident Response Exercise

• • •

Last Day

Incident Response Exercise

Debriefing

TracerFIRE Options

- TracerFIRE event can be 2 days, 3 days, or a full week
- Previously Developed Events are Available
- Concept and Tool Training Can be Customized for Customer Needs
- Incident Response Exercise Can be Customized to Customer Needs by Creating Scenarios that Match your systems and networks i.e., power plant scenario for power plant operators

TracerFIRE Outcomes

Sandia National Laboratories

- Promotes Critical Thinking & Problem Solving
- Provides Training on Tools & Capabilities to Perform Incident Response
- Provides Students with a Better Understanding of the Cyber Kill Chain & Why it is Important in Incident Response
- Allows Students to Interact with Live Malware Without Compromising Their Own Systems
- Promotes Collaboration Between Team Members
  - Co-workers
  - Colleagues from other institutions
- Strengthens Relationships Between Co-Workers
- RECOIL Capabilities Can Be Added to TracerFIRE Platform
  - Identifying student level of expertise
  - Human factors research
  - Case study analysis of adversary techniques & exploit methods

Previous Scenario Showcase

TracerFIRE 6 Scenario:
“Canuckistan”

- Students are incident responders for Canuckistan Power Company.

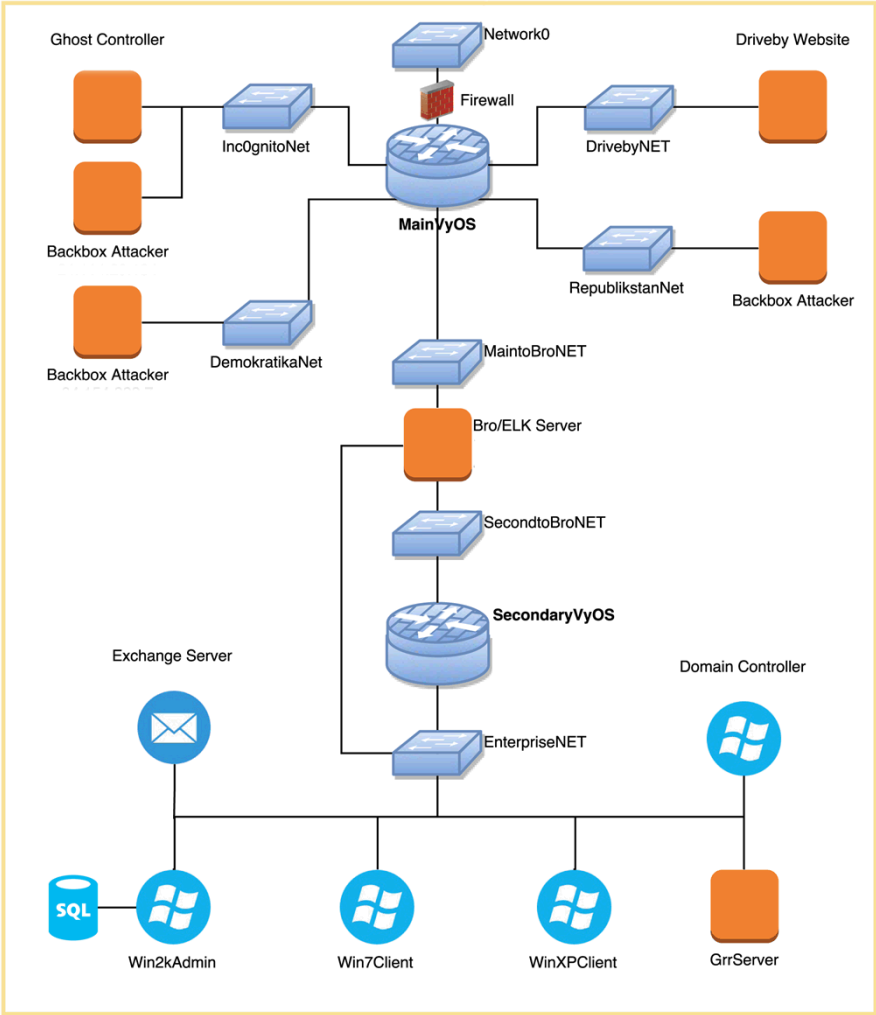
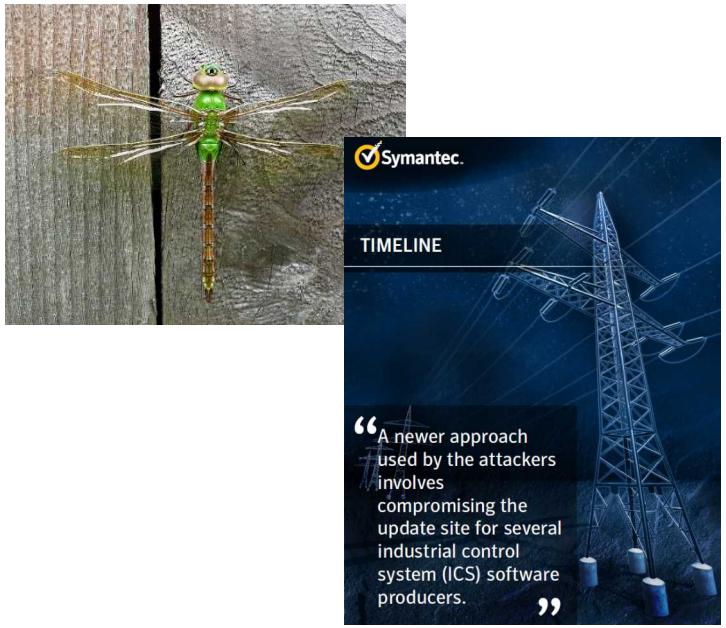


Diagram of Scenario Network Design

Canuckistan: Threat Actors

- Environmental Hacktivist Group called nC0Gnito
- Demands that Canuckistan Power shut down and convert to clean energy such as wind and solar or face a complete take over of their power generation facility



nC0Gnito video and threat narrative based on Dragonfly Campaign

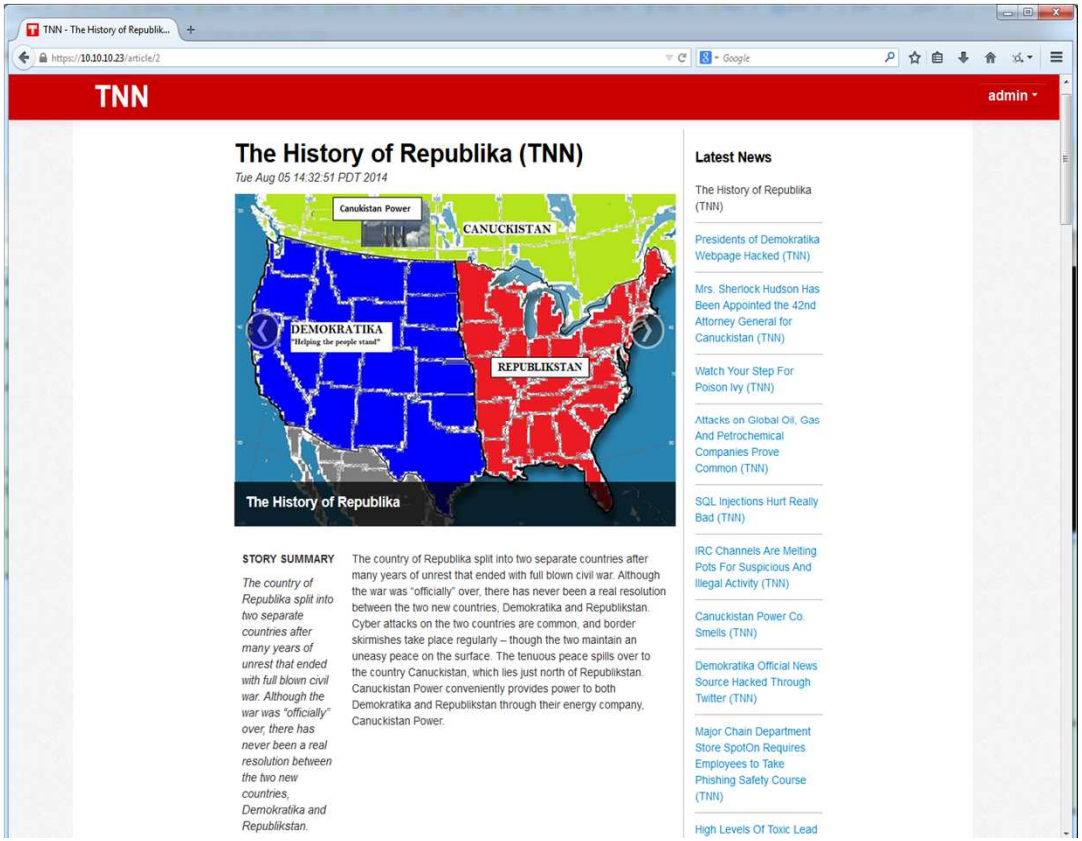
Created by Lauren Lockett (UNM), Kelly Cole, Susan Fowler (Purdue) and Rebecca Hart (Ohio State)

Canuckistan: Tracer News Network

Sandia National Laboratories

Content Management System

- Injects the relevant and irrelevant news and information into scenario and requires teams to comprehend narrative and research
- Provides researchers ability to measure situational understanding and awareness of teams while they participate in exercise
- Motivates teams to perform intelligence analysis as they progress through exercise

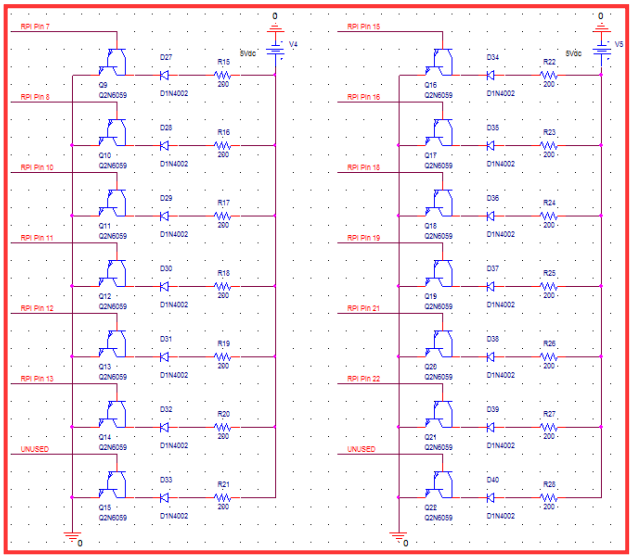


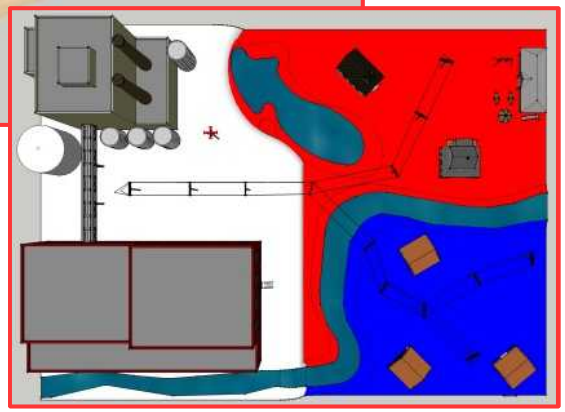
Canuckistan: SCADA Model

Sandia National Laboratories

Power Generation Simulation

- Design implemented Raspberry Pi's to simulate a SCADA system for power generation
- Portable system that can be taken to TracerFIRE events on the road
- Realistic HMI display that emulates power plant SCADA systems and power grids to educate cybersecurity experts on how to respond to energy crisis scenarios like blackouts from cyber attacks





Jeremy Gin (University of Arizona), Matthew Letter (UNM) and Marcos Torres (UNM), and Rain Dartt (Rose-Hulman Institute)

THE UNIVERSITY OF ARIZONA.

UNM

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Event Debrief & Research Efforts

Sandia National Laboratories

Event Debrief

- Teams are asked to make sense of their analysis that they performed during the week and tell a complete story of what the **adversary did and their possible motives and intentions**
- Provides teams **opportunity to reflect** on what they did and observed during the week

Research Efforts

- Teams have agreed to be videotaped and research is underway to analyze team and individual performance aspects
- Sandia's cognitive team has designed agent software to monitor students **workflow and application usage**
- Sandia is exploring research methods that include measurement of participants **eye tracking and EEG**
- Objective is to gain a **fundamental understanding of cognitive skills** of individuals and teams while they perform under stress during a simulated cyber attack

Team DeadBeef Cafe Briefing at ENDEX

Questions

Sandia National Laboratories