

Exceptional service in the national interest



TracerFIRE



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. SAND2016-4414 PE

Cyber Tracer Program

- 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)

- 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

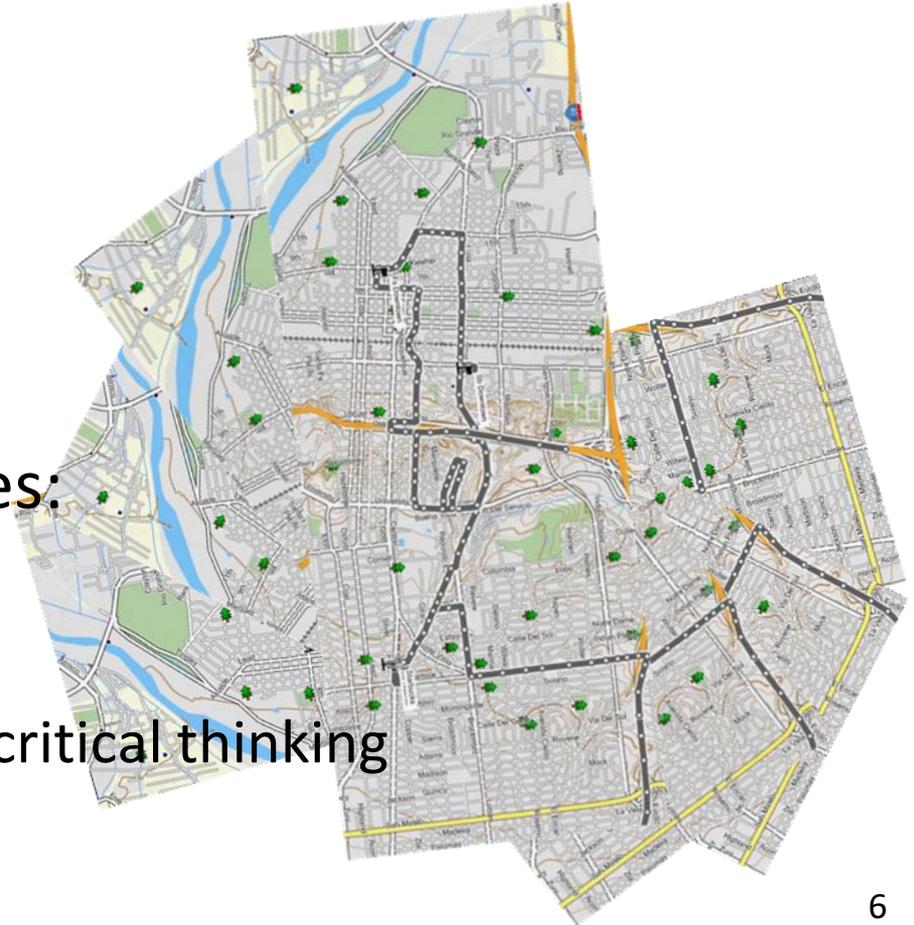
- TF5 Scenario was created with the concept of narrative based learning:
- Enables participants to enhance their understanding of cyber related problems and their solutions in contextually-meaningful ways
- Similar to medical education where students spend time in residency before qualification as a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



ShmuxBux Coffee Company Under Attack

Incident Responders Learning

- 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 Outcomes

- 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

Previous Scenario Showcase

TracerFIRE 6 Scenario: “Canuckistan”

- Students are incident responders for Canuckistan Power Company.

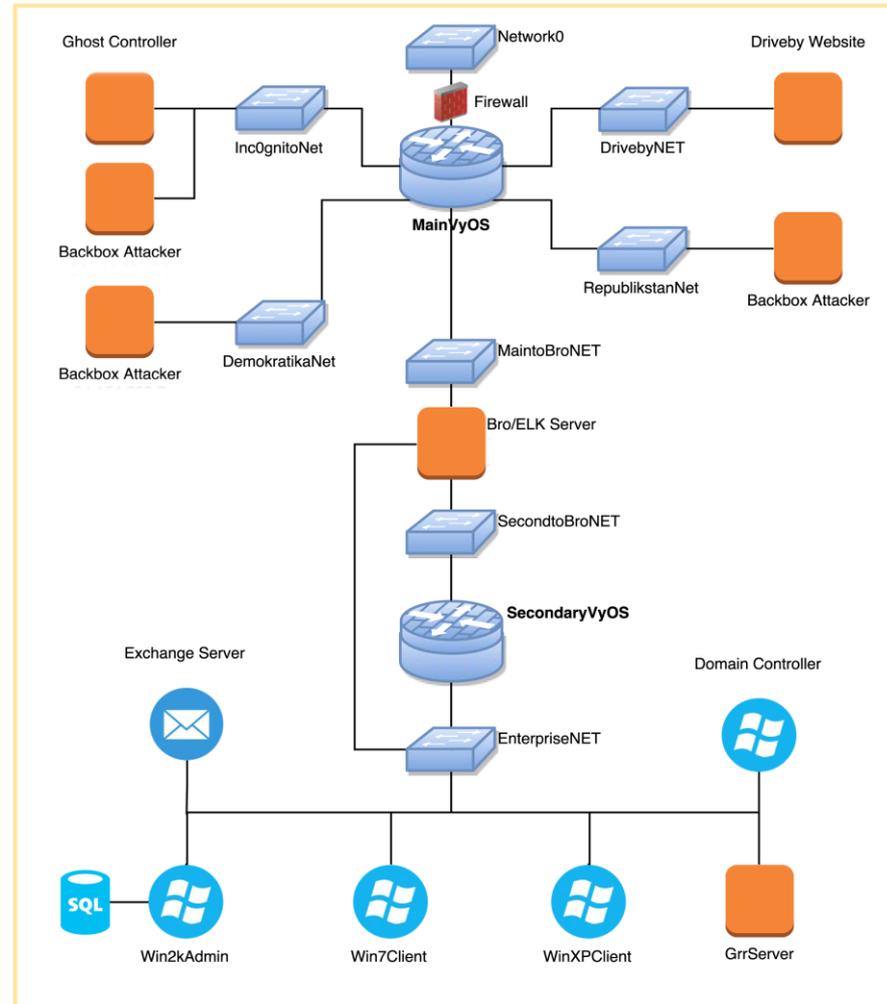


Diagram of Scenario Network Design

Canuckistan: Threat Actors

- Environmental Hacktivist Group called nCOGnito
- 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



nCOGnito 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

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



The screenshot displays a web browser window with the URL <https://10.10.10.23/article/2>. The page title is "TNN - The History of Republika...". The main content area features a map of the United States divided into three regions: "CANUCKISTAN" (green, northern), "DEMOKRATIKA" (blue, western), and "REPUBLICKSTAN" (red, eastern). A "Canuckistan Power" logo is visible in the top left of the map. Below the map is a "STORY SUMMARY" section with the following text:

STORY SUMMARY
The country of Republika split into two separate countries after many years of unrest that ended with full blown civil war. Although the war was "officially" over, there has never been a real resolution between the two new countries, Demokratika and Republikstan. Cyber attacks on the two countries are common, and border skirmishes take place regularly – though the two maintain an uneasy peace on the surface. The tenuous peace spills over to the country Canuckistan, which lies just north of Republikstan. Canuckistan Power conveniently provides power to both Demokratika and Republikstan through their energy company, Canuckistan Power.

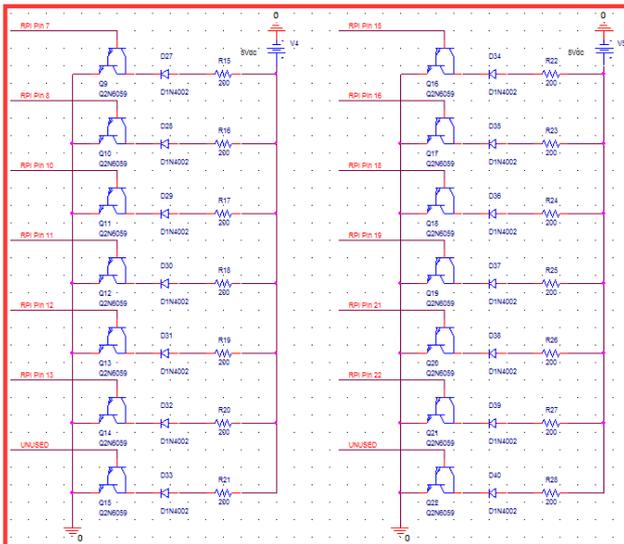
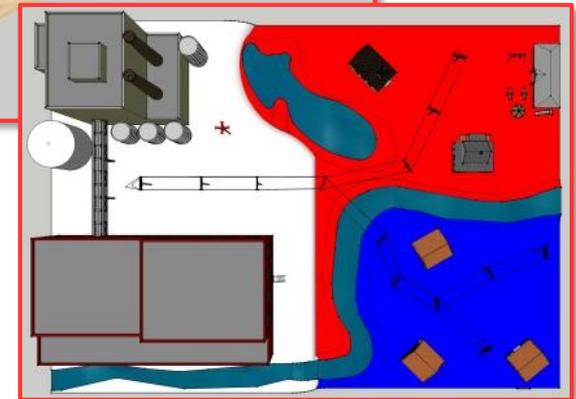
The right sidebar contains a "Latest News" section with the following headlines:

- The History of Republika (TNN)
- Presidents of Demokratika Webpage Hacked (TNN)
- Mrs. Sherlock Hudson Has Been Appointed the 42nd Attorney General for Canuckistan (TNN)
- Watch Your Step For Poison Ivy (TNN)
- Attacks on Global Oil, Gas And Petrochemical Companies Prove Common (TNN)
- SQL Injections Hurt Really Bad (TNN)
- IRC Channels Are Melting Pots For Suspicious And Illegal Activity (TNN)
- Canuckistan Power Co. Smells (TNN)
- Demokratika Official News Source Hacked Through Twitter (TNN)
- Major Chain Department Store SpotOn Requires Employees to Take Finishing Safety Course (TNN)
- High Levels of Toxic Lead

Canuckistan: SCADA Model

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

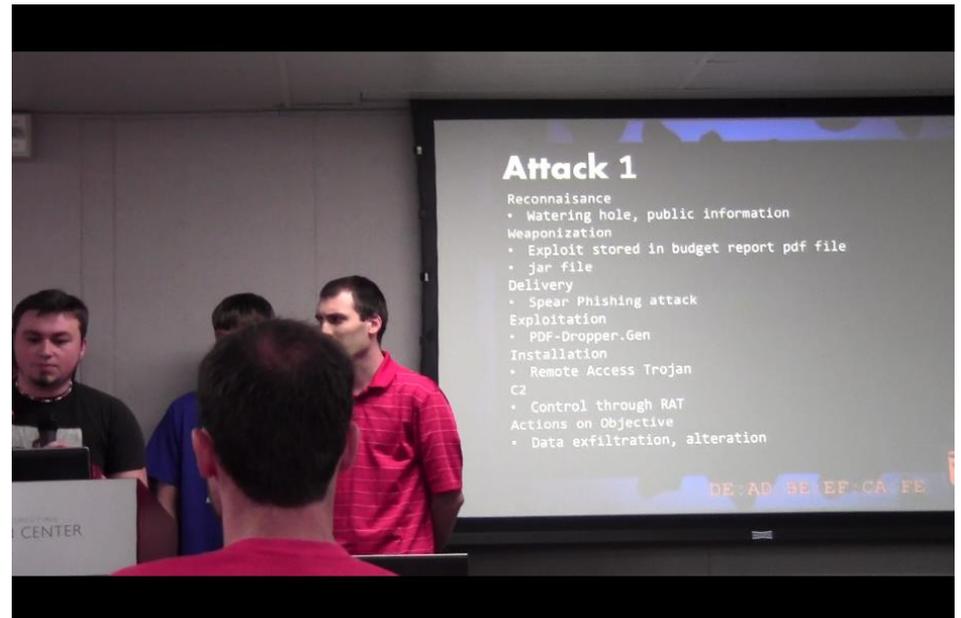


Jeremy Gin (University of Arizona), Matthew Letter (UNM) and Marcos Torres (UNM), and Rain Dartt (Rose-Hulman Institute)

Event Debrief

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



Team DeadBeef Cafe Briefing at ENDEX