Training & Exercises

TECHNICAL TRAINING COURSES

In collaboration with UT San Antonio, the Cybersecurity Monitor launched a series of three (3) continuing education courses centered on cybersecurity defense. Each course ran for one hour and included a supplemental lab exercise on a cyber range to test knowledge and reinforce learned principles. The offered courses were:

1. **Wireshark Fundamentals**
    - How to see Network Traffic
    - Capturing Traffic
    - Viewing and Filtering

2. **Port Scanning**
    - Nmap's role in network scanning
    - Basic scans overview (e.g., Ping, Half-Open Stealth, UDP)
    - Conducting a network scan and analyzing the results

3. **Data Leakage Search**
    - Defining what data leakage is and how it differs from a Data Breach?
    - Illustrate Use Case examples of Data Leak
    - Utilize Spider Foot, an OSINT (Open-Source Intelligence) tool for collecting public information and scanning for exposed private data in order to identify organizational data leakage

Each course ran for one hour and included an extended period for supplemental lab exercises performed on a cyber range to test knowledge and reinforce learned principles.

TABLETOP EXERCISES

Exercises are intended to be a cybersecurity-focused incident response (IR) training opportunity, designed to simulate a realistic scenario that focuses on a utility's capability to detect, identify, protect, respond, and recover from an attack.

PURPOSE

- Provide a forum for participants to test their incident response plan
- Provide an opportunity for utilities to work with one another on a simulated attack scenario
- Obtain documented exercise feedback that can be easily digestible across the organization

BENEFITS

- Identifies potential issues with IR strategy without causing any disruption to production systems
- Enables staff to better understand their individual roles and responsibilities
- Facilitate better coordination
- Help to inform decision-making

VIRTUAL

- In April and June of 2022, we ran two exercises in collaboration with NUARI
- Participants played via the DECIDE platform which utilized email and chat functions to drive the scenario and injects
- Post-Exercise, participants were given an After-Action Report which emphasized observations at the group level and offered recommendations

RED AND BLUE TEAM (2024 SUMMIT)

- Red Team exercise to test how hackers break into systems and allow participants to experiment with security tools that may be “too risky” for production networks.
- Blue Team exercise is to test or expand incident response and forensics skills. Participants were challenged to find out how the systems were compromised,where the attacks came from, and what sensitive or proprietary information was taken. Tasks included finding and removing malware, backdoors, and persistence mechanisms left by the intruders.
- For both, participants received immediate feedback when they’ve solved part of the puzzle or completed a required step to track their individual progress.

INCIDENT RESPONSE TRAINING

During the Cybersecurity Summit, non-technical participants engaged in a Community Cybersecurity Preparedness Simulation course (MTG-301).

Developed by National Cybersecurity Preparedness Consortium, the course utilizes a gamified approach to augmenting Incidence Response where participants strategize with a diverse group of stakeholders to plan for and respond to a cybersecurity incident that could have cascading effects across a community.

The course is designed to assist leaders and managers with cybersecurity preparedness.