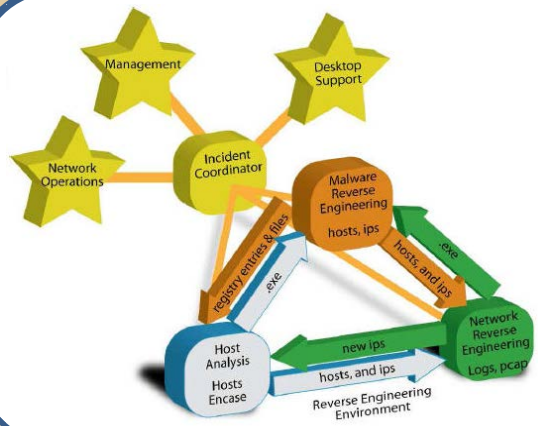
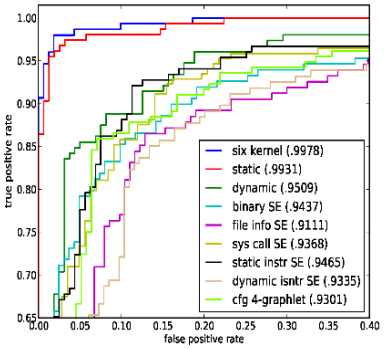
Cyber Defense Training for Nuclear Security Practitioners

Los Alamos NATIONAL LABORATORY EST. 1943

Course Description

- Course adapted from hands-on computer security training and exercises for cyber defenders in DOE, other government agencies, government contractors, and related critical infrastructure.
- The course consists of 2½ days of intensive, hands-on training, followed by a 1½-day exercise designed to reinforce the training and introduce more new concepts.
- Training focuses on:
  - Network Archaeology
  - Host Forensics
  - Malware Analysis
  - Incident Coordination
- Exercise categories include:
  - Forensic Analysis
  - Malware reverse engineering
  - Sequence Analysis
- Content drawn from contemporary intrusion sets.
- Currently used to train incident responders in DOE, DOD, DOJ. Recommended also for nuclear security practitioners.
- Course Length: 4 days





Training Tracks

Entry Point
- Introduce fundamental concepts in the four elements of incident response.
- These elements are listed below.

Network Archaeology
- Inspect network traffic and log files to find evidence, malware, or behavior.
- Reverse engineer unknown binary protocols.

Host Forensics
- Investigate and retrieve malicious software artifacts from Windows systems.
- Find the trail of breadcrumbs that might be lost in noise or history.

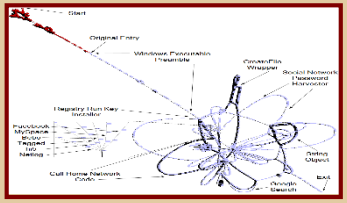
Malware Analysis
- Analyze malware using static and dynamic analysis techniques.
- Monitor the actions of executing malware and extract indicators of compromise.
- Reverse engineer malware.

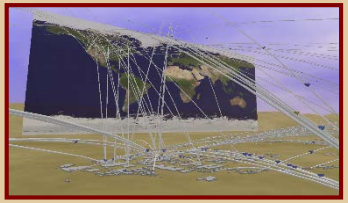
Incident Coordination
- Coordinate a large-scale incident.
- Tie together analysts, management, IT, and other parties.

Cyber Defense Training for Nuclear Security Practitioners

Puzzle-Based Exercises

- Participants self-organize into teams. The teams then work on a free-form set of challenges spanning multiple categories. Teammates collaborate to solve puzzles, sharing tips and making new professional contacts.
- In addition to puzzles developed to test techniques taught in the previous days' tracks, participants can unlock hidden puzzle categories to further develop their skills in new areas through learn-as-you-play exercises.

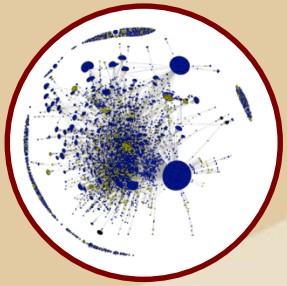


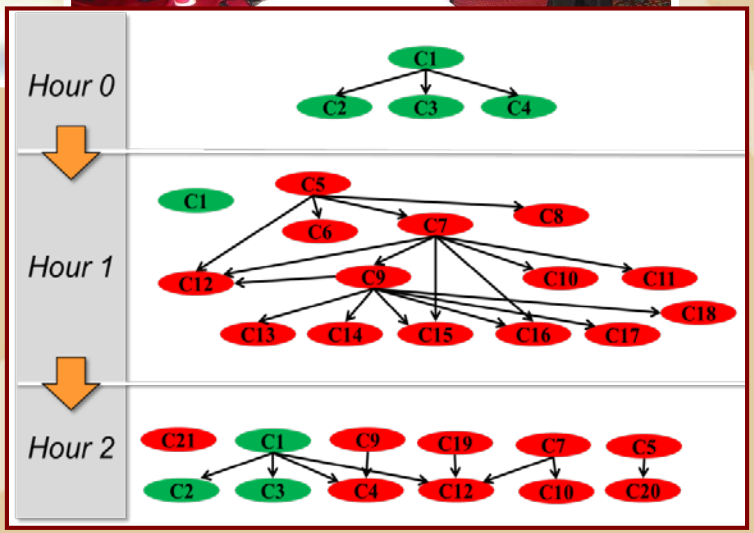


Exercise Categories

- Forensic analysis
- Javascript deobfuscation
- Network archaeology
- Malware reverse engineering
- Sequence analysis
- Binary file reverse engineering
- Snort® mastery
- Splunk® mastery

Exercise categories are designed to both reinforce the topics presented in the training phase and also introduce new concepts to enhance trainees skills





Credential compromise time evolution

LA-UR-16-25604