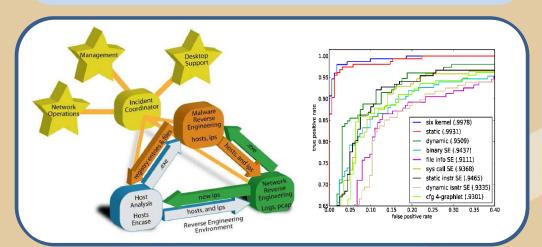
Cyber Defense Training for Nuclear Security Practitioners



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.



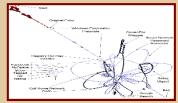
Cyber Defense Training for Nuclear Security Practitioners



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.

market Cont	apture th	e flag: s	coreboa	ırd	The Filter						4.54		i Na <u>j</u>	kis. Al	ملوي	and the		
Overall	bletchley (3150)	compaq (25950)	crypto (1938)	fireeye (33)	forensics (57780)	logger (472)	octopus (804)	printf (930)	pwnables (2133)	rlyeh (11)	round1 (187)	round2 (65)	round3 (2)	sequence (19768)	skynet (5928)	solera (66)	steg (1280)	tanks (57
dread Kendra: obie: 1.74 ufbrd: 2.35 UNM/NMT 2.58 shake	draad obie: 300 /dev/null: 500 clan of monkeys: 500 UNM/NMT:	dread obie: 1500 /dev/null: 2250 shake weight: clan of monkeys: 5350	dread pirates: 211 Kendra: 211 oble: 211 shake	/dev/null: ufbrd: 3 oble: 3 shake weight: 3 dread	obie: 4191 /dev/null: 7660 clan of monkeys: 7602 dread pirates:	dread	ufbrd: 41 /dev/null: 74 clan of monkeys: 298	shake weight: 115 clan of	Kendra: 72 UNM/NMT: 238 shake weight: 313 clan of monkeys: 678	clan of monkeys: 2	ufbrd: 14 /dev/null:	/dev/null: shake weight: 17 oble: 18	shake weight: 1	Kendra: obie: 1456 shake weight /dev/null: 4758 clan of monkeys:	clan of monkeys:	7 ufbrd: 10	dread clan of ufbrd: 130 obie: 130 shake weight: 170	shake ufbrd: 48 UNM/NM 64 /dev/null: 65 obie: 86
weight: 2.84 /dev/null: 2.94 clan of monkeys: 4.16	600 ufbrd: 1150	uft 11:	6			9		9					1					irtbags: 8 lendra: 65
W.			A TIL															
ries			ı		ı		Н	our 0					_	- \-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\-\				



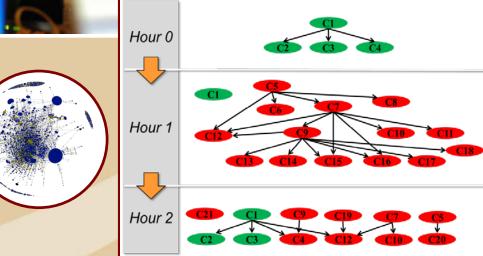




Exercise Categories

- 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