COURSE TABLE OF CONTENTS

Garak

OEM: Koenig Original • Duration: 1 Day (5 hrs)

COURSE MODULES & TOPICS

Module 1: Foundations and Installation

- Scanner workflow overview
- Generators, probes, detectors, and evaluation
- Install Garak and inspect components
- Run a small test (LAB)

Module 2: Connecting a Model

- Model generators and provider configuration
- Managing credentials and scan limits
- Connect a model
- Run a focused baseline scan (LAB)

Module 3: Selecting Vulnerability Probes

- Probe families: prompt injection, jailbreaks, encoding, data leakage
- Run selected probes
- Compare probe outputs (LAB)

Module 4: Detectors and Result Validation

- Detection logic and outcome types
- Pass/fail outcomes and false positives
- Coverage limits
- Inspect flagged responses
- Confirm or reject findings (LAB)

Module 5: Reports and Configuration

- JSONL reports and hit logs
- Saved settings and reproducible evidence
- Review report records
- Repeat scan with saved settings (LAB)

Module 6: Retesting and Assessment

- Compare equivalent scan runs
- Write remediation recommendations
- Assess a training model
- Present a concise report (LAB)

© Koenig Solutions