TRANCHULAS

AI-Powered Social Engineering and Deepfake Exploitation Training Course

Next-Generation Human Hacking: Master AI-Enhanced Social Engineering and Deepfake Defense

Introduction

Enter the future of cybersecurity with our intensive 3-day AI-powered social engineering program. Through accelerated hands-on training with artificial intelligence tools, deepfake technology, and advanced psychological profiling and persuasion tactics, you'll develop expertise to understand, execute, and defend against the most sophisticated human-based attacks that leverage machine learning and synthetic media to bypass traditional security controls. This comprehensive program addresses the critical evolution in threat landscape by training cybersecurity professionals to understand, simulate, and defend against next-generation attack vectors.

Accreditations

Tranchulas is a CREST Cyber Training Provider, validating the excellence and credibility of our training offerings.

Course Objectives

By the end of this course, participants will be able to:

1. Understand how artificial intelligence and machine learning are transforming social engineering attack methodologies and defense strategies.
2. Leverage AI-powered OSINT tools to conduct automated target profiling, social media analysis, and large-scale reconnaissance operations.
3. Apply natural language processing and computer vision techniques to extract psychological profiles and behavioral patterns from digital footprints.

4. Create sophisticated deepfake content including synthetic video, audio, and text for authorized security testing and awareness purposes.
5. Conduct real-time deepfake attacks using live video manipulation and voice transformation technologies in simulated scenarios.
6. Implement machine learning-based detection systems to identify deepfakes and synthetic media in organizational environments.

Course Outline

Day 1: AI-Enhanced OSINT & Automated Target Profiling

Module 1: Introduction to AI-Powered Social Engineering

- Evolution of Social Engineering in the AI Era
- Understanding AI-Enhanced Attack Vectors
- Machine Learning Fundamentals for Cybersecurity
- Neural Networks and Deep Learning Basics
- Ethical and Legal Considerations
- Red Team vs. Threat Actor Perspectives

Module 2: Traditional Social Engineering Foundations

- Psychology of Influence and Persuasion
- Cognitive Biases and Human Vulnerabilities
- Social Engineering Attack Lifecycle
- Pretexting, Phishing, and Vishing Techniques
- Trust Exploitation and Authority Manipulation
- Exercise: Conduct traditional social engineering reconnaissance

Module 3: AI-Powered OSINT and Data Collection

- Automated Social Media Scraping and Analysis
- Machine Learning for Pattern Recognition
- Large-Scale Data Aggregation Techniques
- AI-Driven Search and Discovery Tools
- Dark Web and Alternative Data Sources
- Privacy Implications and Data Protection
- Exercise: Use AI tools to build comprehensive target profiles

Module 4: Natural Language Processing for Profiling

- NLP Fundamentals and Text Analysis
- Sentiment Analysis and Emotional Profiling
- Personality Assessment through Writing Analysis
- Automated Communication Style Mimicry
- Behavioral Prediction Models
- Exercise: Analyze social media posts to create psychological profiles

Module 5: Computer Vision for Visual Intelligence

- Image Recognition and Facial Analysis
- Location Identification from Photos
- Social Network Mapping through Images
- Metadata Extraction and Analysis

- Visual Pattern Recognition for Target Selection
- Exercise: Extract intelligence from image datasets

Day 2: Deepfake Creation & Synthetic Media Exploitation

Module 6: Introduction to Deepfake Technology

- Generative Adversarial Networks (GANs) Explained
- Deepfake Evolution and Current State
- Types of Synthetic Media (Video, Audio, Images, Text)
- Deepfake Use Cases in Social Engineering
- Technical Requirements and Infrastructure
- Ethical Boundaries and Responsible Use

Module 7: Deepfake Video Creation

- Face Swapping Techniques and Tools
- DeepFaceLab and FaceSwap Platforms
- Facial Reenactment and Expression Transfer
- Video Quality Enhancement and Optimization
- Lighting and Environmental Matching
- Exercise: Create deepfake video of target executive

Module 8: Voice Cloning and Synthetic Audio

- Voice Synthesis Technology Overview
- AI-Powered Voice Cloning Platforms
- Accent and Emotion Replication
- Real-Time Voice Transformation
- Audio Quality Assessment and Enhancement
- Vishing Attack Integration
- Exercise: Clone voice samples for phone-based attacks

Module 9: AI-Generated Text and Content

- Large Language Models
- Automated Phishing Email Generation
- Personalized Message Crafting at Scale
- Writing Style Mimicry and Impersonation
- Multi-Language Content Generation
- Exercise: Generate personalized phishing campaigns using AI

Module 10: Real-Time Deepfake Applications

- Live Video Manipulation Technology
- Real-Time Face Swapping for Video Calls
- Voice Modulation in Live Conversations
- Zoom/Teams Deepfake Integration

- Technical Challenges and Limitations
- Exercise: Conduct live deepfake video call simulation

Day 3: AI Defense & Deepfake Detection Systems

Module 11: Deepfake Detection Fundamentals

- Deepfake Detection Challenges and Limitations
- Visual Artifacts and Inconsistencies
- Audio Analysis for Synthetic Speech Detection
- Metadata and Forensic Analysis
- Behavioral Anomaly Detection
- Exercise: Identify deepfakes in mixed media samples

Module 12: Machine Learning-Based Detection Systems

- AI-Powered Deepfake Detection Tools
- Training Detection Models
- Adversarial Machine Learning Concepts
- Detection Evasion Techniques
- Continuous Model Improvement
- Exercise: Implement and test detection algorithms

Module 13: Organizational Defense Strategies

- AI Security Awareness Training Programs
- Human Verification Protocols
- Multi-Factor Authentication for Identity Verification
- Communication Channel Security
- Incident Response for Deepfake Attacks
- Policy Development and Governance
- Exercise: Develop organizational AI security policy

Module 14: Technical Controls and Monitoring

- Email Security and AI-Powered Filtering
- Network Monitoring for Anomalous Behavior
- Endpoint Detection for Deepfake Tools
- Automated Response Systems
- Exercise: Configure detection and monitoring infrastructure

Module 15: Threat Intelligence and Attribution

- AI-Enhanced Threat Intelligence Gathering
- Attack Attribution Methodologies
- Tracking Deepfake Campaigns
- Adversary Profiling and TTPs

- Information Sharing and Collaboration
- Industry Threat Landscape Analysis

Module 16: Red Team Operations and Testing

- Planning AI-Enhanced Social Engineering Campaigns
- Multi-Vector Attack Coordination
- Deepfake Integration in Red Team Exercises
- Success Metrics and Effectiveness Measurement
- Reporting and Remediation Recommendations
- Exercise: Execute full-scale AI-enhanced social engineering simulation