SOCIAL ENGINEERING TESTING (SET) FRAMEWORK

Tactical Assessment & Resilience Blueprint

by Kai Aizen
GenAI Security Researcher | SnailSploit

snailsploit.com

TABLE OF CONTENTS

1. INTRODUCTION

Social engineering attacks continue to rank as some of the most effective and insidious tactics used by adversaries in today's digital landscape. With the emergence of AI-driven phishing, deepfake impersonations, and the increasing adoption of IoT devices, attackers now have access to a broader array of tools to exploit human vulnerabilities.

To mitigate these threats, organizations must adopt a holistic approach to assessing and improving their defenses, with a particular emphasis on human factors. The Social Engineering Testing (SET) Framework is designed to simulate, test, and improve the resilience of employees and organizations against a wide range of social engineering tactics.

Through automated attack simulations, real-time feedback, and continuous improvement cycles, organizations can enhance their preparedness and security awareness, ultimately fostering a culture of resilience.

2. OVERVIEW OF THE SET FRAMEWORK

What is the SET Framework?

The SET Framework is a strategic methodology for assessing and addressing human vulnerabilities through simulated social engineering attacks. These attacks mimic real-world adversarial tactics, such as phishing, vishing, impersonation, and more recent threats driven by AI, such as deepfake-based impersonations and AI-generated phishing campaigns.

Core Components

• **Scope Definition & Objective Setting:** Define simulation scope including departments, roles, and attack vectors to be tested.

• **Scenario Development & Customization:** Design attack scenarios based on organizational risk profile and real-world threats.

• **Automated Execution with AI Integration:** Employ AI tools to automate and scale various social engineering attacks.

• **Data Collection & Analysis:** Collect detailed metrics on employee interactions with simulated attacks.

• **Continuous Feedback & Improvement:** Provide real-time feedback and generate regular reports for iterative refinement.

Key Goals

Goal	Description
Enhancing Employee Resilience	Train employees to recognize and respond effectively to attacks
Quantifying Vulnerabilities	Measure reactions using metrics like click-through rates
Continuous Improvement	Use data-driven insights to refine awareness programs

3. SET TACTICS AND SUB-TACTICS

SET-001: Pretexting

Creating elaborate, fabricated scenarios to trick victims into divulging sensitive information.

ID	Sub-Tactic	Description
SET-001-01	Impersonating Authority Figures	Pretending to be executives or law enforcement
SET-001-02	Creating Urgent Scenarios	Scenarios creating a sense of emergency
SET-001-03	Gaining Trust Through Familiarity	Referencing mutual contacts or past projects

SET-002: Baiting

Enticing targets with promises of rewards, exploiting curiosity or desire for benefit.

ID	Sub-Tactic	Description
SET-002-01	Physical Media Drops	Leaving infected USB drives in visible locations
SET-002-02	Online Baiting	Fake download links promising valuable rewards
SET-002-03	Scareware	Fake security alerts urging software downloads

SET-003: Tailgating/Piggybacking

Gaining physical access by exploiting the courtesy of authorized personnel.

ID	Sub-Tactic	Description
SET-003-01	Following Authorized Personnel	Following employees through secure doors
SET-003-02	Using Large Objects as Props	Carrying boxes to avoid questioning
SET-003-03	Pretending to Be an Employee	Using badges or uniforms to avoid suspicion

SET-004: Impersonation

Pretending to be someone trusted by the target.

ID	Sub-Tactic	Description
SET-004-01	Phone Impersonation	Calling as executives or support personnel
SET-004-02	In-Person Impersonation	Entering premises as contractor or IT staff
SET-004-03	Email Impersonation	Business Email Compromise (BEC) attacks

SET-005: Quid Pro Quo

Offering something valuable in exchange for sensitive information.

ID	Sub-Tactic	Description
SET-005-01	Offering Free Services	Offering tech support in exchange for access
SET-005-02	Offering Rewards	Promising gift cards for personal information
SET-005-03	Exploiting Curiosity	Offering information for seemingly harmless details

SET-006: Phishing

Using deceptive emails to trick targets into revealing sensitive information.

ID	Sub-Tactic	Description
SET-006-01	Generic Email Phishing	Mass emails with general content
SET-006-02	Spear Phishing	Targeted, personalized phishing attacks
SET-006-03	Clone Phishing	Copying legitimate emails with altered links

SET-007: Vishing (Voice Phishing)

Using phone calls or voice messages to deceive individuals.

ID	Sub-Tactic	Description
SET-007-01	Phone Calls from Fake Authorities	Impersonating bank reps or executives
SET-007-02	Automated Voice Messages	Automated messages claiming urgent issues

SET-008: Smishing (SMS Phishing)

Using SMS text messages to deceive targets.

ID	Sub-Tactic	Description
SET-008-01	Text Messages with Malicious Links	Fraudulent texts with phishing links
SET-008-02	Fake Alerts and Notifications	Claiming accounts are locked

SET-009: Dumpster Diving

Retrieving sensitive information from discarded materials.

ID	Sub-Tactic	Description
SET-009-01	Searching for Discarded Information	Searching trash for sensitive documents
SET-009-02	Recovering Discarded Devices	Recovering unwiped electronic devices

SET-010: Shoulder Surfing

Physically observing individuals entering sensitive information.

ID	Sub-Tactic	Description
SET-010-01	Observing Password Entry	Watching credentials being entered

SET-011: Advanced Tactics

Sophisticated tactics exploiting new technologies.

ID	Sub-Tactic	Description
SET-011-01	Watering Hole Attacks	Compromising frequently visited websites
SET-011-02	Business Email Compromise	Gaining access to legitimate business emails
SET-011-03	Physical Surveillance	Observing behavior to identify weaknesses
SET-011-04	Fake Job Offers	Creating fake job offers to lure individuals

4. AI-ERA TACTICS (2025+)

SET-015: Deepfake Impersonation

Using AI to create highly convincing audio and video impersonations.

ID	Sub-Tactic	Description
SET-015-01	Deepfake Video Calls	Impersonating executives in video calls
SET-015-02	Deepfake Voice Messages	Creating convincing voice messages

SET-016: AI-Powered Phishing

Using machine learning to craft personalized and adaptive phishing.

ID	Sub-Tactic	Description
SET-016-01	AI-Generated Spear Phishing	AI gathering info for personalized emails
SET-016-02	AI-Adaptive Campaigns	AI adjusting approach based on behavior

SET-017: Social Media Engineering 2.0

Exploiting social platforms to gather intelligence or manipulate.

ID	Sub-Tactic	Description
SET-017-01	LinkedIn Impersonation	Fake profiles posing as executives
SET-017-02	Influencer Targeting	Targeting influencers to manipulate followers

SET-018: IoT-Based Social Engineering

Exploiting vulnerabilities in connected devices.

ID	Sub-Tactic	Description
SET-018-01	Smart Device Impersonation	Impersonating virtual assistants
SET-018-02	Connected Device Hacking	Compromising IoT for physical access

5. SOCIAL ENGINEERING THREAT MATRIX

The Threat Matrix provides a structured overview mapping tactics against attack vectors, targets, likelihood, impact, success rates, and mitigations.

Tactic	Vector	Target	Likelihood	Impact	Success	Frequency
SET-001: Pretexting	Email/Phone	Exec/HR/IT	High	High	70%	Quarterly
SET-002: Baiting	Physical/Online	General	Medium	Medium	60%	Semi-Annual
SET-003: Tailgating	Physical	Security	Low	High	50%	Quarterly
SET-004: Impersonation	Phone/Email	HR/Finance	High	High	65%	Quarterly
SET-006: Phishing	Email	All	Very High	High	75%	Monthly
SET-007: Vishing	Phone	Exec/HR	Medium	High	60%	Semi-Annual
SET-015: Deepfake	Video/Audio	Exec/HR	Medium	High	60%	Quarterly
SET-016: AI Phishing	Email	All	Very High	Medium	75%	Monthly
SET-017: Social Media	Social	Exec/Mktg	Medium	Medium	65%	Semi-Annual
SET-018: IoT	IoT Devices	IT/Facilities	Medium	High	55%	Semi-Annual

6. ASSESSMENT METHODOLOGY & METRICS

Real-Time Vulnerability Assessment Metrics

Metric	Description	Target
Click-Through Rate (CTR)	Percentage who clicked phishing links	**< 5%**
Credential Submission Rate	Employees who entered sensitive info	**< 2%**
Time-to-Report (TTR)	Speed of reporting suspicious activity	**< 5 min**
Challenge Rate	Employees who challenge unauthorized individuals	**> 90%**

Role-Based Assessment Metrics

Metric	Description
Role-Specific Attack Success Rate	Success of simulated attacks targeted at specific roles
Challenge Rate by Role	How often high-risk roles challenge suspicious requests
Role-Specific TTR	Time taken by specific roles to recognize and report attempts

7. CONTINUOUS FEEDBACK & IMPROVEMENT

AI-Generated Insights

Metric	Description
Behavioral Risk Score (BRS)	AI-generated score based on past simulation behavior
Anomaly Detection Rate (ADR)	Percentage of anomalous behaviors detected
Vulnerability Prediction Rate (VPR)	Predicts which employees are most at risk
Adaptive Learning Progress (ALP)	Tracks improvement in recognizing attacks

Continuous Feedback Loops

Immediate Post-Test Feedback: Employees receive instant feedback including identification of mistakes, tailored learning materials, and positive reinforcement for successful identification.

Real-Time Reporting Encouragement: Implement automated phishing reporting buttons, vishing response protocols, and immediate response alerts to security teams.

Benchmarking Goals: Phishing CTR target < 5%, Time-to-Report target < 5 minutes, Role-specific response rates should exceed averages.

8. ADVANCED METRICS

Testing Effectiveness Metrics

Metric	Description
Attack Success Rate (ASR)	Percentage of successful attacks during simulations
Training Impact Rate (TIR)	Performance comparison before and after training
Reporting Rate (RR)	Percentage who successfully report attempts
Attack Progression Interruption Rate	Rate at which employees interrupt attack progression

Assessment Frequency Guidelines

Target Group	Risk Level	Recommended Frequency
Executives, Finance, IT	High	Monthly
HR, Legal, Operations	Medium	Quarterly
General Staff	Standard	Semi-Annual
Physical Security	Variable	Semi-Annual

9. CONCLUSION

Why the SET Framework is Essential

• **Growing Threat Landscape:** AI-powered attacks, deepfake impersonations, and adaptive phishing require structured simulation and assessment.

• **Human Error as Primary Attack Vector:** Despite technological advancements, human error remains the leading cause of data breaches.

• **Compliance and Risk Mitigation:** Many industries have stringent compliance requirements for security awareness testing.

Key Advantages

Advantage	Description
Comprehensive Simulations	Wide range from traditional phishing to deepfake impersonation
AI-Powered Insights	Track behavior in detail with personalized training recommendations
Continuous Improvement	Real-time feedback creates proactive security culture
Customization	Fully customizable based on industry-specific threats
Quantifiable Metrics	Clear metrics for tracking progress
Future-Proof Security	Designed with emerging threats in mind

As social engineering continues to be the primary entry point for cyberattacks, the SET Framework provides the essential tools, insights, and strategies needed to protect an organization's most vulnerable assets—its people.