EVILTEAM COURSE

PREMIUM V2 • Advanced Social Engineering & Phishing Awareness

Section 1: Introduction

What is this: Foundation of ethical hacking and phishing awareness.

How it works: Explains legal boundaries, mindset, and attack structure concepts.

Tools Covered: N/A

Section 2: Browser Exploitation Concepts

What is this: Understanding how browsers can be targeted.

How it works: User interaction with crafted pages can expose sessions and trust.

Tools Covered: BeEF Framework

Section 3: Hosting & Infrastructure

What is this: Backend setup used in phishing simulations.

How it works: Deploy realistic websites and domains to mimic trusted services.

Tools Covered: Apache, Hosting Platforms

Section 4: Tool Integration

What is this: Combining tools for advanced workflows.

How it works: Multiple systems are chained to simulate real-world scenarios.

Tools Covered: BeEF, Metasploit

Section 5: Phishing Campaigns

What is this: How phishing campaigns are designed and executed.

How it works: Targets receive crafted messages leading to controlled environments.

Tools Covered: GoPhish

Section 6: Session Attacks

What is this: Focus on session tokens instead of passwords.

How it works: Capturing active sessions allows access without credentials.

Tools Covered: Evilginx

Section 7: Multi-Stage Attacks

What is this: Layered attack techniques.

How it works: Multiple steps increase success rate and bypass simple protections.

Tools Covered: Evilginx + GoPhish

Section 8: Custom Templates

What is this: Tailoring phishing pages.

How it works: Templates are modified to resemble specific brands or services.

Tools Covered: Phishlets

Section 9: URL Engineering

What is this: Manipulating URLs to appear legitimate.

How it works: Users trust familiar-looking links without verifying details.

Tools Covered: Custom Domains

Section 10: Real-Time Alerts

What is this: Monitoring campaign activity.

How it works: Systems notify when interaction occurs.

Tools Covered: Telegram Bot

Section 11: Email Concepts

What is this: Email-based social engineering.

How it works: Spoofed messages trick users into trusting fake sources.

Tools Covered: GoPhish

Section 12: Advanced Techniques

What is this: Modern phishing approaches.

How it works: Fake browser windows/interfaces simulate trusted environments.

Tools Covered: Browser Techniques

Section 13: Automation

What is this: Scaling attacks through automation.

How it works: Processes are automated to target large audiences efficiently.

Tools Covered: Scripts

Section 14: Interaction Techniques

What is this: Real-time victim guidance.

How it works: Dynamic interaction increases trust and completion rates.

Tools Covered: Web Tools

Section 15: Security Awareness

What is this: Understanding protections.

How it works: Explains how systems like DMARC protect users.

Tools Covered: Email Security Concepts

Section 16: Domains & SSL

What is this: Trust indicators online.

How it works: HTTPS shows encryption, not legitimacy.

Tools Covered: Apache, SSL

Section 17: Modern Phishing

What is this: New evolving threats.

How it works: Mobile and app-based attacks are increasing rapidly.

Tools Covered: Web APIs

Section 18: Remote Access Concepts

What is this: Unauthorized access awareness.

How it works: Attackers attempt remote control via deceptive methods.

Tools Covered: EvilVNC

Section 19: Voice Attacks

What is this: Phone-based scams.

How it works: Automated systems trick users into sharing information.

Tools Covered: IVR Systems

Section 20: Homograph Attacks

What is this: Lookalike domain tricks.

How it works: Characters are replaced to mimic trusted websites.

Tools Covered: Domain Tools

Section 21: Defense & Awareness

What is this: Protection strategies.

How it works: Users learn to identify and avoid attacks.

Tools Covered: Security Practices

Section 22: N8N Automation Setup

What is this: Building automated phishing email workflows.

How it works: N8N is configured to automate mail delivery, trigger logic, and campaign actions.

Tools Covered: N8N

Section 23: Email Spoofing Automation

What is this: Sending realistic spoof-style emails.

How it works: Automated workflows generate sender masks and improve delivery realism.

Tools Covered: N8N Workflow

Section 24: Cloud VPS Deployment

What is this: Hosting phishing infrastructure on cloud server.

How it works: Full backend is deployed on VPS for stable campaign handling.

Tools Covered: Cloud VPS, PhishingClub

Section 25: Campaign Testing Basics

What is this: Initial campaign creation and inbox testing.

How it works: Landing pages, mail sending, and result tracking are verified before launch.

Tools Covered: PhishingClub

Section 26: Domain Integration

What is this: Connecting custom domain names.

How it works: DNS records are mapped with infrastructure for branded URLs.

Tools Covered: Domain Panel, PhishingClub

Section 27: Domain Campaign Deployment

What is this: Full campaign launch using custom domain.

How it works: Mail sender, page host, SSL, and tracking linked under one domain.

Tools Covered: Custom Domain, PhishingClub

Section 28: Custom Page Injection

What is this: Adding branded phishing pages manually.

How it works: Custom HTML templates are inserted to increase realism.

Tools Covered: PhishingClub Templates

Section 29: AI Evilginx Automation

What is this: Speed creation of Evilginx phishlets.

How it works: AI-assisted logic helps generate and customize phishlets.

Tools Covered: Evilginx, AI Automation