SL-HPTE – HUMINT Penetration Testing Expert

Course Syllabus

Course Overview

This course provides students with advanced, end-to-end training in **Human-Centered Penetration Testing (HPTE)** — covering **OSINT, phishing, device-assisted intrusions, and physical penetration exercises**.
The syllabus aligns with **PTES Social Engineering Guidelines** and **real-world red team methodologies**, focusing on **practical tradecraft, OPSEC, and full-process adversary simulation**.
By the end of the course, students will conduct a complete red team operation: from reconnaissance and phishing, to physical access and reporting.

Structure

- **Total Meetings**: ~17
- **Format**: Instructor-led theory, guided demos, live labs, class missions, and real-world exercises.
- **Final Project**: Full **end-to-end human PT engagement** — from tasking → recon → phishing → physical intrusion → reporting.

SL-HPTE

Meetings Breakdown

Stage 1 – OSINT Foundations (6 Meetings)

Meet 1 – Introduction to OSINT

- What is OSINT & why it matters in social engineering
- Ethics, legality & disclaimer
- Note keeping & structured intelligence documentation
- Sock puppets: creating & maintaining digital identities

Meet 2 – Search Engine & Image OSINT

- Advanced search operators
- Reverse image searching
- Metadata & EXIF analysis
- Geolocation from images

Meet 3 – People & Account OSINT

- Email harvesting & enumeration
- Breached credentials & password hunting
- Username correlation across platforms
- Phone number, DOB, resume & voter record research

Meet 4 – Social Media OSINT

- Profiling across platforms (Twitter, Facebook, Instagram, Reddit, LinkedIn, TikTok, Snapchat)
- Behavioral analysis & lifestyle indicators
- Leveraging social data for phishing/pretexting

Meet 5 – Website, Business & Wireless OSINT

- Website footprinting & hidden directories
- Business intel collection (structure, staff, suppliers)
- Wireless intelligence gathering
- Case studies & real-world scenarios

Meet 6 – OSINT Tools & Automation

- Building an OSINT lab
- Frameworks & utilities
- Automating searches & correlations
- Writing professional OSINT reports

Stage 2 – Phishing & Social Engineering (4 Meetings)

Meet 7 – The Perimeter & Phishing Fundamentals

- Enterprise defenses & bypasses (MFA, filters, whitelists)
- Domain selection & registration tradecraft
- Email infrastructure setup

Meet 8 – Phishing with GoPhish

- Server setup & configuration
- TLS certificates & mail profiles
- Campaign creation & monitoring
- Infrastructure hardening (stealth + OPSEC)

Meet 9 – Advanced Phishing Techniques

- Custom HTML for emails & landing pages
- Password reset & credential harvesting flows
- MFA bypass with Evilginx (phishlets, domain configs)
- Combining GoPhish + Evilginx

Meet 10 – Smishing & Vishing

- SMS phishing setup (EvilGoPhish, providers)
- Voice phishing strategies & call scenarios
- Combining OSINT with phishing vectors
- Reporting & defensive countermeasures

Stage 3 – Device Demonstrations (1 Meeting)

Meet 11 – Hacking Devices: Introduction & Demonstration

- USB-based attacks (Rubber Ducky, Bash Bunny)
- Wireless devices (Flipper Zero, Wi-Fi tools, RFID/NFC cloning)
- Pwnagotchi basics & Wi-Fi handshakes
- Focus: *Demonstration only — not deep technical labs*

Stage 4 – Physical Intrusion (4 Meetings)

⚠ **Content Classified** – roadmap disclosed, details withheld.

Meet 12 – Physical Intrusion Training (Content Classified)
Meet 13 – Physical Intrusion Training (Content Classified)
Meet 14 – Physical Intrusion Training (Content Classified)
Meet 15 – Physical Intrusion Training (Content Classified)

Stage 5 – Full Process Simulation (2 Meetings)

Meet 16 – End-to-End Operation (Execution Phase)

- Mission briefing & scenario handout
- OSINT → phishing → pretexting → intrusion plan
- Students execute engagement in teams

Meet 17 – Reporting & Defense

- Writing a professional Social Engineering PT report
- Presenting findings to stakeholders (“CISO-style” defense)
- Peer review & lessons learned

Evaluation

- **Class Missions**: Hands-on OSINT, phishing, and device demos
- **Home Missions**: Individual assignments after each stage
- **Final Project**: End-to-end Human Penetration Test engagement with full reporting

---

Certification Granted

SL-HPTE – Certified Human Penetration Testing Expert
