SL-IPTE – Advanced Infrastructure Penetration Testing Expert

Course Syllabus (Final Version)

Course Overview

This course provides advanced training in **Infrastructure Penetration Testing**, covering **Windows, Linux, and Active Directory environments** with real-world red team methodologies.
It aligns with **PTES**, **OSSTMM**, and **NIST SP800-115** frameworks, while integrating **TryHackMe modules**, **custom Sec-Llama labs**, and adversary emulation.
Graduates will be prepared to conduct full-scope red team engagements at an **OSCP+ equivalent level**.

Structure

- **Total Meetings**: 16 (+ final capstone exam)
- **Format**: Instructor-led deep dives, guided labs (THM + Sec-Llama custom labs), class missions, home missions, and self-investigate tasks.
- **Final Exam**: 48-hour OSCP-style engagement with reporting & oral defense.

Meetings Breakdown

Stage 0 – Orientation (1 Meeting)

Meet 0 – Course Introduction

- Course expectations & outcomes
- Penetration testing methodologies: PTES, OSSTMM, NIST SP800-115
- Rules of Engagement (ROE), ethics & legal scope
- Lab setup: Windows AD, Linux servers, VPN, TryHackMe + Sec-Llama labs

---

Stage 1 – Core Infrastructure Hacking Foundations (4 Meetings)

Meet 1 – Offensive Pentesting Foundations

- Offensive methodology & kill chain mapping
- Recon basics (active vs passive)
- THM Module: *Introduction to Offensive Pentesting*

Meet 2 – Red Team Fundamentals

- Threat intelligence & OPSEC
- Adversary emulation & engagement planning (CONOPS, resource, remediation plans)
- THM Module: *Red Team Fundamentals*

Meet 3 – Networking & OS Basics

- TCP/IP, VLANs, routing, firewalls
- SMB, RDP, SSH, SNMP, SMTP deep dive
- THM Modules: *Linux Fundamentals* + *Windows Fundamentals*

Meet 4 – Enumeration Mastery

- Service enumeration (Nmap NSE, SMB, LDAP, Kerberos, RPC, WinRM)
- Automation & custom recon scripts

Stage 2 – Initial Access & Exploitation (4 Meetings)

Meet 5 – Red Team Initial Access

- Attack surfaces: public services, misconfigurations, weak creds
- Exploitation frameworks (Metasploit + manual exploitation)
- Web → Infra pivoting
- THM Module: *Red Team Initial Access*

Meet 6 – Linux Exploitation

- Exploiting Linux services & misconfigs
- Weak SSH/FTP/NFS access
- Reverse shells, web shells, pivots

Meet 7 – Windows Exploitation

- Windows service exploits, RDP attacks
- Weaponizing weak AD accounts for footholds
- Living-off-the-land techniques

Meet 8 – Active Directory Hacking (Phase I)

- AD fundamentals: LDAP, domain enumeration, GPOs
- BloodHound & SharpHound mapping
- THM Room: *Attacktive Directory (Intro Labs)*

Stage 3 – Post-Exploitation & Red Team Ops (5 Meetings)

Meet 9 – Post-Compromise Tradecraft

- Credential dumping & lateral movement basics
- Persistence techniques
- THM Module: *Post-Compromise*

Meet 10 – Privilege Escalation (Linux)

- Kernel exploits, SUID abuse, Docker escape
- Automation with LinPEAS & custom scripts
- THM Module: *Linux Privilege Escalation*

Meet 11 – Privilege Escalation (Windows)

- UAC bypass, token manipulation, misconfigs
- Tools: WinPEAS, Mimikatz, Rubeus
- THM Module: *Windows Privilege Escalation*

Meet 12 – Evasion Techniques

- Host evasion: AMSI bypass, AV/EDR evasion
- Network evasion: segmentation bypass, IDS/IPS evasion
- THM Modules: *Host Evasions* + *Network Security Evasion*

Meet 13 – Active Directory Hacking (Phase II)

- Advanced AD exploitation: Kerberoasting, golden/silver tickets
- Cross-domain & forest pivoting
- Red Team persistence & stealth in AD

Stage 4 – Full-Scope Engagement (3 Meetings)

Meet 14 – Planning & Scoping

- Defining objectives & attack paths
- OPSEC & stealth considerations
- Students prepare full red team engagement plans

Meet 15 – End-to-End Attack (Execution Phase)

- Students execute full kill chain: recon → exploitation → escalation → persistence → exfiltration
- Focus on stealth, chaining attacks, and adversary simulation

Meet 16 – Reporting & Defense

- Professional reporting: executive vs technical reports
- Final presentation & defense (students questioned under “CISO-style” review)

Stage 5 – Capstone Exam (OSCP+ Style)

- **48-hour exam lab**: Mixed Linux, Windows, and AD targets
- **Requirements**: exploitation → post-exploitation → persistence → reporting
- **Deliverables**: Professional PT report + oral defense session

---

Certification Granted

SL-IPTE – Certified Infrastructure Penetration Testing Expert

---