SL-JPT – Junior Penetration Testing

Course Syllabus

Course Overview

This course introduces students to the core foundations of offensive cybersecurity and penetration testing.
It covers operating systems, networks, Active Directory, Linux/Windows internals, scripting (Bash & Python), web and mobile testing basics, and social engineering fundamentals.

The syllabus is aligned with PTES, MITRE ATT&CK, and OWASP, combining theory, hands-on labs, and real-world simulations.
By the end of the course, students will execute a complete penetration test covering recon, exploitation, reporting, and presentation.

Structure

- **Total Meetings:** 36 (~12 weeks)
- **Format:** Instructor-led theory, guided demos, live labs, class missions, and real-world case studies.
- **Final Project:** Scoped penetration test including recon → exploitation → reporting → defense presentation.

Meetings Breakdown

Stage 1 – Introduction to Offensive Cyber (3 Meetings)

Meet 1 – Course Kickoff & Offensive Cyber Overview

- Offensive cybersecurity roles (Pentester, Red Team, Bug Bounty)
- Legal, ethical, and strategic goals
- Real-world case studies

Meet 2 – Red Team vs Blue vs Purple

- Threat actors and adversary simulation
- MITRE ATT&CK TTPs overview
- Frameworks: PTES, NIST, MITRE

Meet 3 – Engagement Rules & Tools Overview

- Rules of Engagement (ROE), scoping, authorization
- Lab setup: Kali Linux + Windows VM
- Tool overview: Burp Suite, Wireshark, Nmap, MobSF

Stage 2 – Computer Basics (3 Meetings)

Meet 4 – OS Concepts & Filesystems

- OS architecture basics
- NTFS, ext4, file navigation
- File permissions (r/w/x)

Meet 5 – Processes, Users, and System Navigation

- Processes & task management
- Users, groups, privilege levels
- System info gathering

Meet 6 – Command-Line Skills (CMD, PowerShell, Bash)

- CMD: ipconfig, dir, tasklist
- PowerShell: Get-Process, Get-Service
- Bash: ls, cat, grep, find, history

Stage 3 – Computer Networks (3 Meetings)

Meet 7 – TCP/IP, Ports & Protocols

- OSI vs TCP/IP models
- TCP, UDP, DNS, HTTP, SMB
- Common service ports

Meet 8 – DNS, DHCP, NAT, Firewalls

- DNS resolution & DHCP flow
- NAT and routing
- Host & network firewalls

Meet 9 – Packet Analysis & Scanning Tools

- Wireshark intro & filtering
- Nmap basics & flags
- Masscan vs Nmap

Stage 4 – Windows Server & Active Directory (3 Meetings)

Meet 10 – Intro to Active Directory

- Domains, forests, OUs
- Domain Controllers & GPOs
- Trust relationships

Meet 11 – LDAP, Groups, and Enumeration

- LDAP concepts & tools
- AD Explorer demo
- Basic enumeration (whoami, net user/domain)

Meet 12 – Password Policies & Misconfigurations

- Default groups & privileges
- GPO analysis
- Password policy enforcement & bypass cases

Stage 5 – Linux for Hackers (3 Meetings)

Meet 13 – User Management & Permissions

- /etc/passwd, /etc/shadow
- File ownership, chmod, chown
- Sudo basics

Meet 14 – Services, Cron Jobs, and SSH

- systemctl, cron, service management
- SSH keys & passwordless access
- Common services: apache2, sshd

Meet 15 – Bash Scripting & Automation

- Variables, loops, functions
- Pipes and redirection
- Writing automation scripts

Stage 6 – Python for Hackers (3 Meetings)

Meet 16 – Python Basics + OS Interaction

- Variables, conditions, loops
- File read/write
- OS & subprocess modules

Meet 17 – Networking & Web Automation

- socket basics – client/server
- requests & HTTP automation
- Simple GET/POST

Meet 18 – Parsing and Tool Building

- BeautifulSoup for HTML parsing
- Web scraping basics
- Brute-forcing loop example

Stage 7 – Cyber Kill Chain (3 Meetings)

Meet 19 – The 7 Stages Explained

- Reconnaissance → Action on Objectives
- Real-world examples

Meet 20 – Attacker Methodologies

- MITRE ATT&CK Matrix overview
- Tactics, Techniques, Procedures (TTPs)
- Kill Chain vs Pentesting

Meet 21 – Threat Simulation Design

- Target selection
- Pretext, infrastructure, payload design
- Red team vs pentest mindset

Stage 8 – Infrastructure PT (3 Meetings)

Meet 22 – Reconnaissance & Enumeration

- Passive vs active recon
- WHOIS, DNS, subdomains (amass, sublist3r)
- Port/service scanning

Meet 23 – SMB, SNMP, Shares & Internal Services

- SMB enumeration (enum4linux)
- SNMP queries
- Open share discovery

Meet 24 – Vulnerability Discovery

- Banner grabbing
- CVE search (NVD, Vulners)
- Nessus & Nuclei basics

Stage 9 – Web PT (3 Meetings)

Meet 25 – HTTP Basics and Recon

- Requests, responses, headers, cookies
- Burp Suite setup & proxy

Meet 26 – Auth Flaws, XSS, SQLi Basics

- Login bypass & username enumeration
- Reflected/stored XSS
- SQLi introduction

Meet 27 – Fuzzing and Enumeration

- Dirb & ffuf for endpoint discovery
- Parameter tampering
- WAF detection

Stage 10 – Mobile PT (3 Meetings)

Meet 28 – Android & iOS Architecture

- APK vs IPA
- AndroidManifest, components, permissions
- iOS sandbox & signing

Meet 29 – Static & Dynamic Analysis

- MobSF usage
- Extracting credentials/base64 keys
- ADB interaction

Meet 30 – Mobile Threat Models

- OWASP Mobile Top 10
- Common app flaws
- Data leakage cases

Stage 11 – HUMINT (OSINT, Phishing, Physical) (3 Meetings)

Meet 31 – OSINT Techniques and Tools

- Google Dorking, email harvesting
- theHarvester, recon-ng
- Sock puppets

Meet 32 – Phishing Infrastructure and Payloads

- Email/SMS/voice phishing
- Tools: GoPhish, Evilginx (intro)
- Payload tradecraft

Meet 33 – Physical Intrusion Planning

- Badge cloning, tailgating, pretexting
- Tools: Flipper Zero, RFID reader (demo)
- Story building for engagements

Stage 12 – PT Report Writing + Final Project (3 Meetings)

Meet 34 – Penetration Testing Report Writing

- Executive vs technical reporting
- CVSS scoring & OWASP mapping
- PoC evidence

Meet 35 – Final Project – Practical Simulation

- Full pentest execution: recon → exploitation
- Team-based simulation with instructor oversight

Meet 36 – Final Presentation & Debrief

- Students present findings & methodology
- Report submission & defense
- Feedback and course wrap-up

Evaluation

- **Class Missions:** Hands-on labs each meeting
- **Final Project:** Scoped penetration test simulation
- **Reporting:** Final technical + executive report, live defense presentation

---

Certification Granted

SL-JPT – Certified Junior Penetration Testing
