ALBSYSTEM.NET

Da Zero a eJPT in 6 Mesi — Edizione 2026

Questo piano di studio ti porta dalle basi assolute fino alla certificazione eJPT (eLearnSecurity Junior Penetration Tester). E strutturato per chi studia da autodidatta, con 8-10 ore settimanali disponibili. Ogni settimana ha obiettivi chiari, risorse gratuite e un esercizio pratico verificabile.

Cosa ti serve per iniziare

PC o laptop: Qualsiasi — useremo macchine virtuali. 8GB RAM minimo, 16GB consigliato.

VirtualBox: Gratuito su virtualbox.org. Per il lab isolato.

Connessione internet: Per TryHackMe, risorse e aggiornamenti.

Account TryHackMe: Gratuito su tryhackme.com. La piattaforma principale del corso.

Voglia di studiare: 8-10 ore a settimana. Non serve essere geni — serve costanza.

La Certificazione Target: eJPT

La **eJPT (eLearnSecurity Junior Penetration Tester)** e la prima certificazione pratica di penetration testing. Costa circa 200 dollari, dura 3 giorni, e si svolge in un ambiente di lab reale — non e un quiz a risposta multipla. Dimostra che sai fare exploitation basico, ricognizione, privilege escalation e scrivere un report.

Percorso consigliato dopo eJPT: CompTIA Security+ (teoria) → PNPT (pratica avanzata) → OSCP (il gold standard).

Panoramica del Percorso — 6 Mesi

Periodo	Fase	Focus
MESE 1-2	FONDAMENTA	Linux, rete, Python base, primo CTF
MESE 3-4	ATTACCO	Nmap, Metasploit, web hacking, SQLi, XSS
MESE 5	AVANZATO	Privilege escalation, AD intro, buffer overflow base
MESE 6	CERTIFICAZIONE	Simulazione esame, review, certificazione eJPT

Piano Settimanale Dettagliato

	Titolo	Argomenti	Risorse	Ore
W1	**Linux da Zero**	• Terminale e comandi base • Permessi e utenti • File system Linux • SSH fondamentali	TryHackMe: Pre-Security Linux Fundamentals 1-2	9h
W2	**Networking Fondamentali**	• Modello OSI e TCP/IP • IP, subnet, CIDR • DNS, HTTP, HTTPS • Wireshark intro	TryHackMe: Pre-Security Networking Fundamentals	9h
W3	**Python per Hacking**	• Variabili e tipi • Funzioni e loop • File I/O • Script di rete base	TryHackMe: Python Basics author.to/learnpython.org	10h
W4	**Setup Lab e Kali Linux**	• VirtualBox setup • Kali Linux installazione • Metasploitable2 setup • Primo scan Nmap	TryHackMe: Intro to Cybersec kali.org/get-kali	9h
W5	**Reconnaissance & OSINT**	• theHarvester • Shodan • Google Dorks • Sublist3r, amass	TryHackMe: OSINT Reconnaissancero	9h
W6	**Nmap Completo**	• Scan types: -sS -sV -sC • NSE Scripts • Output e analisi • Evasion base	TryHackMe: Nmap nmap.org/book	10h
W7	**Metasploit Framework**	• Architettura MSF • Workflow exploit • Meterpreter comandi • Sessioni multiple	TryHackMe: Metasploit Metasploitable2 lab	10h

	Titolo	Argomenti	Risorse	Ore
W8	**Web Hacking con Burp Suite**	• Setup proxy • Intercept e Repeater • Spider e scanner • DVWA su Docker	TryHackMe: Burp Suite PortSwigger Academy	10h
W9	**SQL Injection**	• SQLi teoria e tipi • Detection manuale • SQLmap automazione • DVWA SQLi • Prepared statements	TryHackMe: SQLi PortSwigger SQLi Labs	10h
W10	**XSS e CSRF**	• Reflected vs Stored • DOM-based XSS • CSRF meccanismo • Difese pratiche	TryHackMe: XSS PortSwigger XSS Labs	9h
W11	**Privilege Escalation Linux**	• Enum con LinPEAS • SUID exploitation • Sudo misconfiguration • Cron jobs • Capabilities	TryHackMe: Linux PrivEsc gtfobins.github.io	10h
W12	**Privilege Escalation Windows**	• WinPEAS enumeration • Unquoted service paths • Token impersonation • AlwaysInstallElevated	TryHackMe: Windows PrivEsc HackTheBox Windows basics	10h
W13	**Macchine Complete HackTheBox**	• Metodologia completa • Easy machine 1 • Easy machine 2 • Writeup reading	HackTheBox: Starting Point Tierl - Tier II	12h
W14	**Active Directory Intro**	• AD struttura • Enumeration con BloodHound • Kerberoasting intro • Pass-the-hash base	TryHackMe: Active Directory HackTheBox AD labs	10h

	Titolo	Argomenti	Risorse	Ore
W15	**CTF e Consolidamento**	• PicoCTF challenges • CTFtime eventi passati • Web, crypto, forensics • Report di una macchina	picoctf.org ctftime.org write-ups	12h
W16	**Report Professionale**	• Struttura report pentest • CVSS scoring • Executive summary • Remediation writing • Simulazione report eJPT	INE/eLearnSecurity templates Serpico report tool	10h
W17	**Simulazione Esame 1**	• Laboratorio simulato • Ricognizione su lab • Exploitation • Post-ex e note	INE eJPT Practice Labs Pratica su TryHackMe	12h

W18	**Simulazione Esame 2 + Review**	• Secondo tentativo simulazione • Review punti deboli • Ripasso rapido argomenti critici • Booking esame	INE eJPT Practice Labs Review personale note	**12h**
W19	**Settimana Buffer**	• Ripasso temi deboli • Macchine aggiuntive • Lettura writeup • Rest e prep mentale	Materiali precedenti HackTheBox/TryHackMe	**8h**
W20	**Preparazione Finale**	• Checklist tecnica • Test ambiente esame • Ripasso report template • Exam day prep	INE official prep material	**6h**
W21	**Esame + Post-Esame**	• Esame eJPT (3 giorni) • Post-exam review • Piano percorso futuro • Community e networking	eJPT Exam Platform AlbSystem community	**15h**

Risorse Gratuite Essenziali

Risorsa	URL	Uso
TryHackMe	`tryhackme.com`	Lab guidati browser-based. Il punto di partenza. Path: Pre-Security → Jr Penetration Tester
HackTheBox	`hackthebox.com`	Macchine piu sfidanti. Inizia da Starting Point. Gratuito per le macchine base.
PortSwigger Academy	`portswigger.net/web-security`	100% gratuito. I migliori lab di web hacking esistenti. Burp Suite incluso.
GTFOBins	`gtfobins.github.io`	Catalogo binari Unix sfruttabili per privesc. Aperto durante ogni lab.
Exploit-DB	`exploit-db.com`	Database exploit pubblici. Per trovare CVE e proof-of-concept.
OWASP Top 10	`owasp.org/Top10`	Le 10 vulnerabilita web piu critiche. Leggi prima di iniziare il web hacking.
PicoCTF	`picoctf.org`	CTF permanente per principianti. Ottimo per web, crypto e forensics.

Checklist Milestone

Mese 1

- ☐ Completo TryHackMe Pre-Security Path
- ☐ 30 ore di lab completate
- ☐ Primo script Python funzionante

Mese 2

- ☐ Lab Kali + Metasploitable operativo
- ☐ Prima macchina HackTheBox completata
- ☐ Nmap scan interpretato correttamente

Mese 3

- ☐ Burp Suite intercetta traffico HTTPS
- ☐ SQLi su DVWA Level Low, Medium, High
- ☐ XSS stored trovata su DVWA

Mese 4

- ☐ Privesc root su macchina TryHackMe

- ☐ Privesc SYSTEM su macchina Windows
- ☐ 3 macchine HackTheBox complete

Mese 5

- ☐ CTF picoCTF 5 sfide completate
- ☐ Report professionale scritto su una macchina
- ☐ AD intro completato su TryHackMe

Mese 6

- ☐ 2 simulazioni esame eJPT completate
- ☐ Punteggio simulazione >70%
- ☐ CERTIFICAZIONE eJPT OTTENUTA
