

SEBASTIÁN LATORRE MUÑOZ

Penetration Tester | Web • Active Directory • AI/LLM Security | OSCP+

Santiago, Chile

LinkedIn: [linkedin.com/in/sebastian-latorre-munoz](https://www.linkedin.com/in/sebastian-latorre-munoz) | GitHub: github.com/iphobiuss | Knowledge base: iphobiuss.github.io

Hack The Box: [perfil público verificable](#)

PERFIL PROFESIONAL

Penetration tester OSCP+ y estudiante de Ingeniería en Ciberseguridad (UNAB), enfocado en aplicaciones web, Active Directory y seguridad ofensiva de LLM. Mi práctica viene de exámenes de certificación y laboratorios: cadenas de ataque completas hasta Domain/Enterprise Admin, documentadas bajo PTES y OWASP con CVSS 3.1 y CWE, y remediación priorizada por riesgo para el negocio. Mantengo report-gen, un generador de informes de pentest open source, y una knowledge base pública en iphobiuss.github.io. Busco mi primer cargo en pentesting; disponibilidad para jornada completa.

CERTIFICACIONES

- **OSCP+ • OffSec Certified Professional** | OffSec | Ago. 2026 • Vigente hasta Ago. 2029 | [Verificar](#)
- **HTB CAPE • Certified Active Directory Pentesting Expert** | Hack The Box | Jun. 2026 | [Verificar](#)
- **eCPPT • Certified Professional Penetration Tester** | INE Security | May. 2026 | [Verificar](#)
- **HTB COAE • Certified Offensive AI Expert** | Hack The Box | Abr. 2026 | [Verificar](#)
- **HTB CWES • Certified Web Exploitation Specialist** | Hack The Box | Abr. 2026 | [Verificar](#)
- **HTB CPTS • Certified Penetration Testing Specialist** | Hack The Box | Abr. 2026 | [Verificar](#)
- **eWPTX • Web Application Penetration Tester eXtreme** | INE Security | Mar. 2026 | [Verificar](#)

PROYECTOS

report-gen • Generador de informes de pentest

Python, Flask, Jinja2, WeasyPrint • Código abierto (MIT) • v0.31.2 • github.com/iphobiuss/report-gen

- Herramienta propia para llevar un pentest del hallazgo al informe (PDF, DOCX y Markdown), construida como alternativa a SysReptor: gestión de hallazgos con CVSS y CWE, evidencias con anotaciones y censura en los píxeles, remediación y retest. Catálogo completo de funciones en el repositorio.
- Motor CVSS 3.1 y 4.0 validado contra recursos de referencia de FIRST y la implementación RedHatProductSecurity/cvss sobre 20.087 vectores de prueba, sin divergencias.
- Hardening propio (CSP estricta, CSRF, validación de Origin, saneado HTML, fetcher anti-SSRF), tests y CI en GitHub Actions.

iphobiuss.github.io • Knowledge base de pentesting

Sitio estático con sistema de build propio en Python • 2025 – Presente • iphobiuss.github.io

- 52 técnicas, 36 herramientas y 6 guías de máquinas de HTB (web, Active Directory e IA/LLM), con certificaciones enlazadas a su verificación oficial.
- Incluye SENTINEL, un mini-CTF de prompt injection sobre un asistente LLM simulado.

EXPERIENCIA PRÁCTICA EN SEGURIDAD OFENSIVA

Exámenes prácticos de certificación y entornos de laboratorio controlados

Penetration Test End-to-End (red + Active Directory)

OSCP+ • OffSec • Ago. 2026

- Examen práctico de 24 horas sobre una red corporativa simulada: enumeración y explotación manual, escalamiento de privilegios en Windows y Linux, pivoting y compromiso de un dominio Active Directory. Informe técnico con evidencia reproducible entregado en las 24 horas siguientes; contenido bajo NDA de OffSec.

Penetration Test Active Directory Multi-Forest

HTB CAPE • Jun. 2026

- Compromiso de 3 forests con relaciones de confianza inter-forest, desde acceso inicial hasta Enterprise/Domain Admin: RBCD y constrained delegation, abuso de ADCS (ESC), Shadow Credentials, DCSync, ataques de trust inter-forest, C2 y pivoting anidado.
- Impacto demostrado de relaciones de confianza mal configuradas (pérdida de la segregación administrativa). Reporte en SysReptor bajo PTES, con CVSS 3.1, CWE y remediación priorizada.

Network Penetration Test Multi-Dominio

HTB CPTS · Abr. 2026

- Compromiso total de una infraestructura de 2 dominios y 7 hosts desde acceso sin credenciales: Kerberoasting, DCSync, abuso de ACLs, movimiento lateral y exfiltración de credenciales entre segmentos de red, identificando dónde un control básico habría cortado la cadena. Reporte en SysReptor bajo PTES.

Penetration Test de Aplicaciones Web (5 aplicaciones)

HTB CWES · Abr. 2026

- Ejecución remota de código (RCE) en 5 aplicaciones web empresariales mediante encadenamiento de SQLi, XSS, SSRF, XXE, IDOR y Command Injection.
- 13 hallazgos (4 críticos, 8 altos, 1 medio) bajo OWASP Testing Guide, con pruebas de concepto reproducibles y remediación priorizada por horizonte temporal.

AI Red Team Assessment sobre LLM y servidor MCP

HTB COAE · Abr. 2026

- Prompt injection directa e indirecta, ataques adversariales (C&W, JSMA, label-flipping), evasión de clasificadores e inyección de comandos en servidor MCP (JSON-RPC).
- 7 hallazgos alineados a OWASP Top 10 for LLM Applications, con CVSS 3.1, CWE y recomendaciones de remediación.

COMPETENCIAS TÉCNICAS

- **Penetration Testing & Seguridad Ofensiva:** pentesting de red, web y Active Directory; ethical hacking, explotación de vulnerabilidades, post-explotación, movimiento lateral, escalamiento de privilegios, Command & Control (C2), pivoting.
- **Web Exploitation:** SQLi, XSS, SSRF, XXE, IDOR, RCE, CSRF, File Upload, Insecure Deserialization, Command Injection, OWASP Top 10.
- **API Security:** REST, GraphQL, OWASP API Security Top 10, bypass de autenticación y autorización.
- **Active Directory:** Kerberoasting, AS-REP Roasting, DCSync, Pass-the-Hash, ACL Abuse, Constrained/RBCD Delegation, ADCS (ESC), Shadow Credentials, AD Trust Attacks, BloodHound.
- **AI / LLM Security:** LLM exploitation, prompt injection (directa e indirecta), model evasion, adversarial attacks, OWASP Top 10 for LLM Applications, seguridad de servidores MCP.
- **Herramientas:** Burp Suite Pro, BloodHound, Impacket, NetExec/CrackMapExec, Metasploit, Rubeus, Mimikatz, SQLMap, Nmap, ffuf, Hashcat, Certipy, SysReptor.
- **Lenguajes y scripting:** Python, Bash, PowerShell.
- **Metodología y reportería:** PTES y OWASP Testing Guide; clasificación con CVSS 3.1 y CWE/CVE; trabajo dentro del alcance y las reglas de enfrentamiento, con autorización previa y manejo confidencial de la evidencia; informes técnicos y ejecutivos en SysReptor y report-gen.

EDUCACIÓN

- **Ingeniería en Ciberseguridad** | Universidad Andrés Bello (UNAB), Santiago | 2026 – En curso · Egreso estimado: 2028
- **Diplomado y Bootcamp en Ciberseguridad** | Universidad del Desarrollo (UDD) | 2024
- **Ingeniería en Ejecución Eléctrica** | Universidad de Atacama (UDA) | 2021 – 2024 (estudios no finalizados)
- **Tecnólogo en Electricidad** | Universidad de Atacama (UDA) | 2018 – 2021 · Titulado

IDIOMAS

- **Español** · Nativo
- **Inglés** · Lectura y escritura técnica fluidas (documentación e informes) · Conversación básica