Yurak Clark Quispe Espinal

Huancayo, Junín, Perú • 7clarkespinal@gmail.com • +51 947 787 816
clarkportafolio.vercel.app • github.com/espinalclark • linkedin.com/in/espinalclark

Perfil Profesional

Estudiante de Ingeniería en Ciberseguridad con formación práctica en pentesting y seguridad defensiva. Certificado eJPT. He realizado un pentest externo black-box sobre infraestructura en producción y construyo labs propios para practicar AD, cloud y hardening. Vengo del desarrollo backend, lo que me da contexto para analizar aplicaciones desde adentro.

Educación

SENATI — Servicio Nacional de Adiestramiento en Trabajo Industrial Huancayo, Perú
Ingeniería en Ciberseguridad Feb 2023 – Presente

Certificaciones:

- eJPT — Junior Penetration Tester, INE Security
- INE Certified Cloud Associate (ICCA), INE Security
- Hacker Ético, Cisco Networking Academy
- Programming Essentials in Python, Cisco Networking Academy
- Networking Essentials, Cisco Networking Academy

Experiencia

Plataforma IoT GPS (Freelance) Remoto
Penetration Tester — External Black-box Jun 2026

- Ejecuté pentest externo black-box sobre 3 hosts en producción sin credenciales previas: 19 hallazgos (3 críticos, 5 altos, 5 medios, 4 bajos, 2 informativos).
- Obtuve acceso administrativo completo a Grafana mediante credenciales por defecto.
- Expuse arquitectura interna vía instancia pública de Wiki.js sin autenticación.
- Verifiqué ausencia de rate limiting en SSH con más de 2000 intentos sin bloqueo (Hydra).
- Documenté hallazgos bajo CVSS, CWE y MITRE ATT&CK con recomendaciones priorizadas.

VafTec Perú Remoto
Programador Backend Jr Sep 2025 – Dic 2025

- Desarrollé y mantuve funcionalidades backend con soporte y corrección de errores en aplicaciones web.
- Realicé pruebas de APIs desde perspectiva funcional y de seguridad.
- Detecté e implementé corrección de Clickjacking mediante cabeceras HTTP (X-Frame-Options / CSP).

Proyectos

ad-attack-lab reporte
Laboratorio de Active Directory con cadena de ataque completa: LLMNR poisoning, AS-REP Roasting, Kerberoasting, pivoting con Ligolo-ng, ACL abuse, ADCS ESC1 y DCSync.

aws-misconfig-lab reporte
Infraestructura AWS/Terraform intencionalmente vulnerable: enumeración S3, IAM privesc, SSRF → robo de credenciales IMDSv1, RCE en Lambda, secretos en ECR y persistencia vía backdoor IAM.

aws-server-hardening reporte
Hardening automatizado de EC2 en AWS en 6 fases: kernel sysctl + AIDE, SSH post-quantum, WireGuard VPN, nftables default-drop, AppArmor enforce y auditd. Marco: CIS Benchmark L2 + MITRE ATT&CK v14.

TryHackMe & HackTheBox write-up
Más de 10 máquinas resueltas y documentadas. Técnicas: SMB enum, file upload bypass, PATH hijacking, EternalBlue, PrintSpoofer.

Habilidades

Pentesting: Metasploit, SQLMap, Hydra, Medusa, Netcat, Nikto, Feroxbuster
Reconocimiento: Nmap, Amass, Enum4linux, Masscan, Gobuster, Tcpdump, Responder
Scripting: Python, Bash, PowerShell
Sistemas: Kali Linux, Arch Linux, Ubuntu Server
Cloud: AWS, Terraform, Docker
Cracking: Hashcat, John the Ripper

Idiomas: Español (nativo), Inglés (técnico, lectura/escritura)