Lucas Souza

https://www.linkedin.com/in/olucassouza/ | https://lucassouza.io

Tecnologia da Informação | Cibersegurança | Red Team

Resumo Profissional

Profissional com mais de 10 anos de experiência em TI, atuando nos últimos anos em Cibersegurança e Infraestrutura, com foco na identificação e exploração de vulnerabilidades, análise de riscos cibernéticos e avaliação da resiliência de aplicações e infraestruturas corporativas. Domínio de frameworks como PTES, MITRE ATT&CK, OWASP, NIST CSF, CIS Control e Cyber Kill Chain em execução de projetos de testes de intrusão, engenharia de ataques e modelagem de ameaças.

Experiência Profissional

Under Protection – Curitiba/PR

- **Analista Sênior em Cibersegurança | 2021 – 2025**

• Planejamento e execução de testes de intrusão avançados em aplicações, redes internas e externas.
• Validação técnica de vulnerabilidades, exploração controlada e análise de impacto.
• Utilização de frameworks de ataque (MITRE ATT&CK, PTES) para modelar cadeias de exploração e pivotagem.
• Elaboração de relatórios técnicos detalhados, com evidências, criticidade e recomendações práticas.
• Participação em red team exercises, simulando ataques direcionados e avaliando a resposta defensiva (blue team).
• Apoio a equipes de defesa na correção e mitigação de falhas exploradas.
Carta Recomendação:
http://web.docsales.com/approval/6a34b47e-0020-4d27-a89a-8ac3c612acde

- **Consultor em Segurança e Infraestrutura de TI | Freelance | 2020 – 2023**

• Execução de pentests externos, internos e web, com foco em identificação de vulnerabilidades críticas.
• Exploração manual de falhas de injeção, escalonamento de privilégios, bypass de autenticação e exploração de lógica de aplicação.
• Produção de relatórios técnicos e executivos, traduzindo riscos técnicos em contexto de negócio.

• Assessoria a equipes de desenvolvimento e infraestrutura para adoção de práticas seguras.
• Uso extensivo de ferramentas como Burp Suite, Metasploit, Nmap, BloodHound, Mimikatz, Impacket e Python.

Agropecuária Masutti – Vilhena/RO

- **Analista Sênior de Infraestrutura de TI | 2016 – 2021**

• Administração e hardening de servidores Windows e Linux, redes corporativas e sistemas críticos.
• Suporte na implementação de controles de segurança, segmentação de rede e backup.
• Gerenciamento e suporte às operações de infraestrutura de TI, monitoramento de disponibilidade de serviços e eventos de segurança.
• Implementação de políticas de segurança e melhoria contínua dos processos de TI.

Formação Acadêmica

Pós-graduação em Computação Forense e Segurança da Informação – IPOG – 2022–2023
Graduação em Análise e Desenvolvimento de Sistemas – UNOPAR – 2018–2020
Técnico em Manutenção e Suporte em Informática – SENAI – 2014–2016

Certificações

C-APIPen – Certified API Pentester - The SecOps Group - 2025
eJPT – Junior Penetration Tester - INE Security - 2025
CRTA – Certified Red Team Analyst - CyberWarFare Labs - 2025
CNSP – Certified Network Security Practitioner - The SecOps Group - 2025
CRT-ID – Certified Red Team Infra Dev - CyberWarFare Labs - 2025
CRT-COI – Certified Red Team CredOps Infiltrator - CyberWarFare Labs - 2025
DCPT – Desec Certified Penetration Tester - Desec Security - 2022

Projetos e Pesquisas de Destaque

CVE-2020–29134 – Totvs Fluig Platform
Identificação de vulnerabilidade crítica de Path Traversal em versões do Fluig, documentada na NVD.
• https://nvd.nist.gov/vuln/detail/CVE-2020-29134

ThreatTrack – Ferramenta de Consulta e Análise de Superfície de Ataque
Desenvolvimento de solução em Python para análise de IPs e domínios, integrando dados da NVD, ExploitDB e GitHub.
• https://github.com/Ls4ss/ThreatTrack

Competências Principais

• **Segurança Ofensiva:** Pentest, Red Team, Exploração, Engenharia Social, Pós-Exploitation.
• **Metodologias:** PTES, OSSTMM, OWASP, NIST CSF, MITRE ATT&CK, Cyber Kill Chain.
• **Programação e Automação:** Python, Bash, PowerShell, Git.
• **Infraestrutura:** Redes, Active Directory, Windows/Linux Hardening, Cloud Recon.
• **Ferramentas:** Nmap, Burp Suite, Metasploit, BloodHound, Mimikatz, Impacket, SQLmap, Cobalt Strike (Emulação).