Lucas S.

Linkedin | Portfólio

Pesquisador | Consultor em Cibersegurança | Especialista em Segurança Ofensiva (Red Team)

RESUMO PROFISSIONAL

Profissional em Cibersegurança com foco em Segurança Ofensiva (Red Team), possuo experiência sólida na identificação de vulnerabilidades, análise de riscos cibernéticos e avaliação da resiliência de ambientes e aplicações. Domínio de frameworks como NIST CSF, MITRE ATT&CK, CIS Controls e Cyber Kill Chain, com foco em testes de intrusão (pentest) e gestão de vulnerabilidades. Apaixonado por tecnologia e inovação, busco constantemente aprimorar meus conhecimentos para fortalecer a segurança de organizações, alinhando visão estratégica aos riscos operacionais e organizacionais.

EXPERIÊNCIA

Analista em Cibersegurança Sênior

Under Protection, Curitiba\PR
Dezembro de 2021 - Atualmente

- Levantamento e análise de riscos cibernéticos com base em padrões de segurança como NIST CSF, MITRE ATT&CK, CIS Controls e Cyber Kill Chain.
- Diagnóstico de brechas de segurança e recomendação de melhores práticas, controles e ferramentas para mitigação de riscos.
- Atuação em projetos de segurança ofensiva, incluindo testes de penetração e análise de superfície de ataque.

Consultor em Segurança Ofensiva

Freelance
Junho de 2020 - Janeiro de 2023

Como consultor de segurança cibernética freelancer, atuei na execução de testes de segurança ofensiva (pentest) em diversas empresas, identificando vulnerabilidades críticas e propondo soluções para fortalecer a postura de segurança dos sistemas. Minhas responsabilidades incluíam:

- Realização de testes de invasão em redes, aplicações web e infraestruturas, seguindo metodologias reconhecidas (OWASP, NIST, entre outras);
- Elaboração de relatórios detalhados com recomendações técnicas para mitigação de riscos, alinhados às necessidades dos clientes;
- Colaboração com equipes internas para implementação de correções e melhoria contínua dos processos de segurança;
- Através desse trabalho, contribui para a proteção de ativos críticos e a redução de riscos cibernéticos, garantindo conformidade com regulamentações e padrões do setor.

Analista em Infraestrutura de TI Sênior
Agropecuária Masutti, Vilhena\RO
Junho de 2016 - Junho de 2021

- Coleta e análise de informações de ambientes para mapeamento de riscos cibernéticos, documentando-os de acordo com os principais padrões de segurança.
- Suporte na implementação de controles de segurança e ferramentas de proteção.

FORMAÇÃO

Pós-graduação em Computação Forense e Segurança da Informação
IPOG – Novembro de 2022 - Dezembro de 2023

Graduação em Análise e Desenvolvimento de Sistemas
UNOPAR – Fevereiro de 2018 – Dezembro de 2020

Técnico em Manutenção e Suporte em Informática
SENAI – Março de 2014 – Abril de 2016

CERTIFICAÇÕES

Desec Security — *DCPT - Desec Certified Penetration Tester*

Março de 2022

Credencial: FNDZ-JTPJE-QGNF

CyberWarFare Labs — *CRTA - Certified Red Team Analyst*

Março de 2022

Credencial: CRTA-2011289

PROJETOS e PESQUISAS

CVE-2020–29134 Totvs Fluig Platform

- Identificação de vulnerabilidade de Path Traversal na plataforma TOTVS Fluig, afetando as versões Fluig Lake 1.7.0, Fluig 1.6.5 e Fluig 1.6.4.

Referências:

- **https://lucassouza.io/lab/pesquisa/2021/03/04/CVE-2020-29134-Totvs-Fluig-Platform.html**
- **https://nvd.nist.gov/vuln/detail/CVE-2020-29134**
- **https://www.exploit-db.com/exploits/49622**

ThreatTrack - Ferramenta de Consulta e Análise de Superfície de Ataque

- Desenvolvimento de uma ferramenta em Python para consulta e análise de segurança em IPs públicos e domínios, utilizando a API do Shodan.
- Integração com bancos de dados como NVD (National Vulnerability Database), ExploitDB e GitHub para consulta de CVEs e PoCs (Provas de Conceito).

Referências:

- **https://lucassouza.io/lab/projeto/2024/04/21/ThreatTrack-O-melhor-de-3-mundos!.html**

HABILIDADE TÉCNICAS

- Segurança Ofensiva: Testes de intrusão, Red Team, Análise de Vulnerabilidades.
- Frameworks e Metodologias: OWASP, NIST CSF, MITRE ATT&CK, CIS Controls, Cyber Kill Chain, OSSTMM, PTES, WSTG.
- Ferramentas: Nmap, Burp Suite, Metasploit, BloodHound, Mimikatz, Impacket, Python.
- Certificações: DCPT, CRTA.