**CAIO LUAN ~~ NoxRoot**

**Red Team Operative | Exploit Developer | Offensive Security Specialist**

**Especialista em segurança ofensiva com performance comprovada em ambientes extremos, dominando laboratórios de dificuldade INSANE e CTFs militares de elite — incluindo desafios utilizados pela Marinha dos EUA e pela NSA. Atuo com maestria em exploração de vulnerabilidades, escalonamento de privilégios, evasão de defesas e simulações táticas reais.**

**Domino tanto a exploração de vulnerabilidades, escalonamento de privilégios e evasão de defesas, quanto a construção de sistemas completos com múltiplas linguagens de programação. Possuo profundo conhecimento prático em:**

- **Python, C, C#, JavaScript, Rust, Bash, PHP, Node.js**
- **Desenvolvimento com ReactJS, HTML5, CSS3, Express.js e MongoDB/MySQL**


📧 **E-mail: caio.luansilva12@gmail.com**

📞 **Telefone: (79) 99921-4501**

🔗 **GitHub: github.com/cai0luan**

🔗 **LinkedIn: linkedin.com/in/caio-~noxroot-👾💀-950a3a248**


## 🎯 OBJETIVO

**Atuar como Pentester Profissional, Programador do mais alto nível, Operador Red Team ou Analista de Segurança Ofensiva, contribuindo com expertise avançada em ambientes críticos, hardening, simulações adversárias e exploração realista de vulnerabilidades.**

## 💼 EXPERIÊNCIA PROFISSIONAL

**Técnico de Suporte e Sistemas – ÁGAPE SISTEMAS**
*(2023 – 2024)*

- Suporte e diagnóstico para órgãos públicos
- Manutenção de sistemas sensíveis como folha de pagamento e eSocial
- Relatórios técnicos, identificação de falhas críticas e contato direto com infraestrutura e segurança

## 🧠 FORMAÇÃO ACADÊMICA

**Tecnologia em Defesa Cibernética**
Estácio de Sá – Aracaju (2025 – Atual)

## 📚 CERTIFICAÇÕES & CURSOS AVANÇADOS

- **Pentest Profissional Híbrido** – *CYSOURCE*
- **Analista de SOC Híbrido** – *CYSOURCE*
- **Pentest do Zero ao Profissional (SYCP)** – *SOLYD Offensive Security*
- **Análise Forense de Sistemas** – *CLAVIS Segurança da Informação*
- **Pentest e Análise Profunda** – *PATO Academy*

## Desenvolvimento & Exploit Dev

- **C# Completo**
- **Python Avançado**

- **JavaScript Avançado**
- **Banco de Dados (MySQL & PHP)**
- **Formação MERN Stack (MongoDB, Express, React, Node.js)**
- **ReactJS / HTML / CSS / UX Design**
- **Edição Avançada com After Effects e Photoshop**

## 🛠️ STACK DE ATAQUE E FERRAMENTAS

- **OSINT e Recon: Amass, SpiderFoot, Shodan, Nuclei**
- **Exploitation: Metasploit, SQLMap, Exploit Dev em C, Python, Bash**
- **Web Pentest: Burp Suite, ZAP, OWASP Top 10, SSRF, RCE, LFI**
- **Privilégio & Persistence: LinPEAS, WinPEAS, PowerShell, Cradle, Pivoting**
- **Análise Forense: Autopsy, FTK Imager, strings, Volatility**
- **C2 & Evasão: Sliver, Covenant, Obfuscation, Payload crafting**
- **SOC / Blue Team: Wireshark, Suricata, SIEM, Threat Hunting básico**
- **Ambientes: Kali Linux, Parrot, Windows Server, Docker, VirtualBox**

## 🌐 IDIOMAS

- **Inglês: Avançado (Leitura técnica + comunicação profissional)**
- **Francês: Básico**

## 🏆 CONQUISTAS CTF E MISSÕES OFFENSIVAS

### 🔓 CCT2019 – U.S. TENTH FLEET / MARINHA DOS EUA

📡 Desafio real utilizado em treinamentos da Marinha dos EUA e da NSA
🧠 Dificuldade: **INSANE**
⚔️ Apenas **10 pessoas no mundo** completaram esse desafio
📜 Resultado: Domínio absoluto. Quebrei um ambiente de guerra cibernética real

### 🪲 Exploração de Bypass Lógico no `configuration.apple.com`

📍 Site alvo: `configuration.apple.com` (Apple Configuration Profile)
🐛 Vulnerabilidade: **bypass de verificação de email/oauth**
🔧 Técnica: manipulação da resposta JSON em `email_verified`, via requisições HTTP interceptadas (proxy/guardar cabeçalhos), injetando `email_verified=true` mesmo sem posse do domínio válido — o que permite:

- Criação de contas com email falsificado, mas verificado
- Contorno de fluxos de autenticação
- Potencial acesso via SSO/OAuth, elevação de privilégios e uso em campanhas de APT

### 🕳️ TryHackMe – You're in a cave [INSANE LEVEL]

💣 Ambiente sem mapa, sem luz e sem espaço para erro
🎯 Domínio completo do lab e streak ativa de CTFs extremos
⚙️ Resultado: Hack concluído com exploit próprio, controle total do sistema

---

### 💀 TryHackMe – Insane Labs (Diversos)

🧩 Desafios extremos de priv esc, exploração de buffer overflows, shell reverso e evasão
📶 Foco em ambientes "no map zone" simulando Red Team militar
💼 Todos concluídos como Operador: ***NoxRoot***