

## Portfólio de Pentest – Gh0styHunter

 **Apelido:** Jackson / Gh0styHunter

 **E-mail:** [jacksonfelixbertolb@gmail.com](mailto:jacksonfelixbertolb@gmail.com) / [gh0styhunter.bugbounter@gmail.com](mailto:gh0styhunter.bugbounter@gmail.com)




 **LinkedIn:** [ [linkedin.com/in/gh0styhunter](https://linkedin.com/in/gh0styhunter) ]

 **GitHub:** [ [github.com/gh0styhunter](https://github.com/gh0styhunter) ]

## Experiência em CTFs / Labs

 Plataforma	 Máquina / Laboratório	 Dados	 Ferramentas	 Bandeira	 Aprendizado
HTB	Miau	07/09/2025	ping, Nmap, Telnet	b40abdf23665f766f9c61ecba8a4c19	Recon de rede, exploração Telnet sem senha, documentação de pentest
TryHackMe	Banco Falso	10/09/2025	Gobuster	BANCO HACKEADO	Descoberta de diretórios ocultos, exploração de página administrativa, mitigação ética

## Ferramentas Principais

 Categoria	 Ferramenta	 Nível
Recon / Subdomínios	Acumular, Sublocalizador	Intermediário
Recon / Rede	Nmap, Wireshark	Intermediário / Básico
Web / APIs	FFUF, Suíte Burp, Gobuster	Intermediário / Básico
Força bruta	Hidra	Intermediário / Básico

## ⚠ Vulnerabilidades Estudadas

- 🔒 Telnet sem senha (HTB Meow) – Acesso root
- 🏠 Página administrativa sem restrição (FakeBank) – Transferência não autorizada

## 📄 Certificados

🔔 Todas as certificações Cisco abaixo possuem selo oficial

- Associado Cisco CyberOps – Cisco – 2025
- Fundamentos de Python – Cisco – 2024
- Conceitos Básicos de Redes – Cisco – 2024
- CCNA – Cisco – 2024
- Introdução ao Pentest – Desecc/Solyd – 2025

## 🔗 Como usar este repositório

- Abra CTFs/para ver cada laboratório com notes.md, flag.txt e report.md.
- Coloque Certificados/os PDFs para referência (opcional: links públicos).
- Em Ferramentas/há guias rápidos e comandos de uso.
- Em Vulnerabilidades/há documentação padrão por vulnerabilidade (descrição, PoC em alto nível, evidências e mitigações).
- Use Portfolio-PDF/para ter uma versão em PDF pronta para envio.

## 📄 Observações Profissionais

- 🧑‍💻 Experiência prática em **CTFs e laboratórios virtuais seguros**
- 📄 Relatórios documentados com **flags, comandos e instruções**, simulando workflow de pentest profissional
- 🚀 Motivado para crescer em **mobile pentest, web scan avançado e documentação de pentest**
- ⚙ Conhecimento aplicado em **ferramentas de reconhecimento, fuzzing, brute-force e web/mobile pentest**