# 📑 Capture The Flag Report

\*\*Plataforma:\*\* HTB

\*\*Máquina:\*\* Meow

\*\*IP:\*\* 10.129.34.76

\*\*Data:\*\* 07/09/2025

---

## 🔎 Reconhecimento

- Ferramentas utilizadas:

- [x] ping

- [x] nmap

- [x] telnet

\*\*Notas:\*\*

ping 10.129.34.76  
Host respondeu com 0% packet loss

sudo nmap -sV 10.129.34.76  
23/tcp open telnet Linux telnetd

---

## ⚔️ Exploração

- Serviço vulnerável: Porta 23/tcp (Telnet)

- Método de acesso: Login como `root` com senha em branco

---

## 📂 Pós-exploração

- Diretório/Arquivo de flag: `/root/flag.txt`

---

- Comando usado:

cat /root/flag.txt

---

\*\*Flag:\*\*

b40abdfe23665f766f9c61ecba8a4c19

---

## ✅ Conclusão

- Vulnerabilidade explorada: Telnet configurado sem senha para root

- Impacto: Acesso root e controle total do sistema

- Mitigação: Desabilitar Telnet, usar SSH e implementar autenticação forte