**Relatório de Pentest – HTB (*Meow*)**

**Autor:** Gh0styHunter  
**Data:** 07/09/2025  
**Alvo:** Máquina *Meow* – Hack The Box  
**Objetivo:** Obter a flag

**1. Reconhecimento**

Foi realizado um teste de conectividade para verificar se o host estava ativo:

ping 10.129.34.76

O alvo respondeu a todas as solicitações ICMP, confirmando disponibilidade.

**2. Varredura**

Foi utilizado o **Nmap** para identificar serviços expostos:

sudo nmap -sV 10.129.34.76

**Resultado:**

* Porta **23/tcp** aberta
* Serviço: **Telnet** (Linux telnetd)

**3. Exploração**

Com base na descoberta, foi realizada conexão via Telnet:

telnet 10.129.34.76

Ao tentar o login como root com senha em branco, o acesso foi concedido.

**4. Pós-exploração**

Já dentro do sistema como **root**, foi listado o diretório /root:

ls

Arquivo encontrado: flag.txt

Leitura da flag:

cat flag.txt

**Flag obtida:**

b40abdfe23665f766f9c61ecba8a4c19

**5. Conclusão**

O alvo estava vulnerável a uma configuração insegura de **Telnet**, permitindo login remoto como **root** sem senha.  
Isso possibilitou o comprometimento completo do sistema e a captura da flag.

**Lições aprendidas:**

* Nunca habilitar Telnet em produção (usar SSH).
* Senhas em branco ou fracas são extremamente perigosas.
* Sempre aplicar o princípio do menor privilégio e autenticação forte.