**06/05/2024 - BOUNTY HACKER**

<https://tryhackme.com/r/room/cowboyhacker>

1. Exploração com Nmap
   1. login anonymous disponível

Texto

Descrição gerada automaticamente

1. Conexão FTP
   1. arquivos para pegar via ftp

Texto

Descrição gerada automaticamente

1. Bruteforce ssh
   1. RedDr4gonSynd1cat3

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Conexão ssh
   1. aquisição da primeira key no desktop

Texto

Descrição gerada automaticamente

1. Busca por prevesc
   1. sudo -l – indica comandos sudo que o usuário pode fazer
   2. comando permitido: tar
   3. uso do GTFOBins para encontrar privesc (https://gtfobins.github.io/gtfobins/tar/)

Uma imagem contendo Texto

Descrição gerada automaticamente

1. Encontrando root.txt
   1. find . -name “nome” – procurando arquivo pelo nome

Texto

Descrição gerada automaticamente