**14/05/2024 – Pickle Rick**

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

1. Escaneamento com Nmap

Texto

Descrição gerada automaticamente

1. Enumeração com Gosbuter

Texto

Descrição gerada automaticamente

1. Exploração web
   1. usuário no código fonte da página

Texto

Descrição gerada automaticamente

1. Acessando robots.txt
   1. senha está no arquivo

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Painel de comandos
   1. comando cat desativado – visualizar arquivos pela url
   2. cd .. && cd .. && cd .. && cd home && cd rick && ls -ld

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Privesc
   1. comando sudo liberado para todos os comandos
   2. usando sudo para setar /root como 777

Tabela

Descrição gerada automaticamente