**14/05/2024 - RROTME**

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

1. Escaneamento de portas
   1. escaneando todas as portas sem o -A (mais rápido)
   2. fazendo -A nas portas que encontrou

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Escaneamento com gobuster

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Reverse shell
   1. filtro de arquivos .php – uso de .phtml (<https://github.com/pentestmonkey/php-reverse-shell>)
   2. upload em /panel
   3. acesso ao link para executar reverse shell

Texto

Descrição gerada automaticamente

1. Privesc
   1. procura por SUIDs
   2. usando python para privesc (https://gtfobins.github.io/gtfobins/python/#suid)

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente