**15/04/2024 – EASYCTF**

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

1. Escaneamento com Nmap
   1. anonymous no FTP

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Escaneamento com Gobuster
   1. presença do robots.txt

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. FTP com anonymous

Texto

Descrição gerada automaticamente

1. SQLi no site
   1. fazendo uma pesquisa encontra-se que o CMS Made Simple tem exploit de SQLi
   2. usando: <https://gist.github.com/kriss-u/321f0418778697e2ec919f04664ceb4>b

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. SSH com dados obtidos

Texto

Descrição gerada automaticamente

1. Privesc
   1. investigando sudo -l (vim)

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

