# Write-ip SIMOC

Enumeração de serviços trás SSH e WEB (80)

Enumeração de diretórios web, achou js/main.js [**FLAG**!]

js indica a existência de detalhes.php, além de um código comentado de faz a descompactação de zlib

pagina detalhes não da pra deduzir muita coisa, porém é possível descobrir que ela gera um cookie. este cookie está encriptado com zlib, ao decriptar consegue uma senha do usuário king:SenhaSecretadoSimoc

é possível logar com o usuário king e a senha descoberta via ssh, no home dele existe uma flag [**FLAG**!]

existe um processo redis rodando, com a porta 6379 aberta com bind para localhost

acessando o redis-cli, e listando as chaves, encontramos somente uma, prince

o valor dessa chave é prince@@prince que é a senha do user prince, subindo com su de king para prince conseguimos acesso e na home dele consta outra flag [**FLAG**!]

no bash_history do usuário prince existe algumas tentativas de subir como queen, com erros de digitação e posterior digitação da senha OreiMaximo@@

ao descobrir as credenciais de queen, no home dela existe outra flag [**FLAG**!]

no home de queen, existe a estrutura de diretórios ./program/bin/interpreter, este software é uma cópia do binário perl. Ele está com a cap setuid habilitada, existe uma chamada de perl que vc ganha um shell como root (./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";')

no /root consta a ultima flag [**FLAG**!]