**06/06/2024 - BIOHAZARD**

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

1. Mapeamento das portas com Nmap
   1. busca por todas as portas com -p-

Texto

Descrição gerada automaticamente

* 1. busca profunda pelas portas encontradas

Texto

Descrição gerada automaticamente

1. Exploração Web
   1. na tela inicial é possível ver o nome da equipe e também um redirecionamento para a próxima página



* 1. na página Main hall descobre-se o caminho para a próxima sala pelo código HTML

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. na página Dining room encontra-se o link para a flag do emblema



* 1. o caminho para próxima página está no comentário do HTML novamente, porém dessa vez encriptado com base64 (https://www.base64decode.org/)

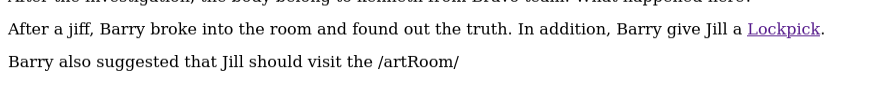
Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. na página Tea room há um redirecionamento para a flag do lockpick e uma indicação da próxima página



* 1. na página Art room há um redirecionamento para um mapa da casa



* 1. o mapa apresenta uma série de caminhos para seguir

Uma imagem contendo Padrão do plano de fundo

Descrição gerada automaticamente

* 1. na página Bar room ele pede a senha do lockpick encontrado anteriormente que redireciona para outra página

Texto

Descrição gerada automaticamente

* 1. na página Bar room aberta ele pede a flag do piano e expõe uma nota encontrada

Texto

Descrição gerada automaticamente

* 1. a nota exibe notas musicais que parece ser um texto criptografado



* 1. usando o cipher-identifier encontramos que o texto está criptografado em base32

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

* 1. inserindo a flag no campo do piano somos redirecionados para a página Secret bar room
  2. na página Secret bar room tem um link que redireciona para a flag do emblema de ouro

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente com confiança média

* 1. na página da flag ele também da a dica para dar um refresh na página anterior

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. ao dar refresh na página do Secrer bar room ele abre um campo parar colocar a flag do emblema do início, redirecionando para outra página

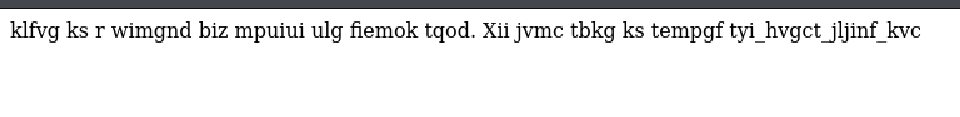
Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. a página redirecionada exibe apenas o nome rebecca



* 1. ao colocar a flag do gold emblem no input da dining Room redireciona para um texto criptografado



* 1. o texto é um vigenere que a chave usada é “rebecca”

Texto

Descrição gerada automaticamente

* 1. acessando a página do escudo dentro da dinning room (/the\_great\_shield\_key.html) obtém-se a flag shield

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. na página Dining room 2F há uma mensagem codificada com cifra de césar (<https://site112.com/cifra-de-cesar-codificar-descodificar>)



Interface gráfica do usuário, Texto, Aplicativo, Word, chat ou mensagem de texto

Descrição gerada automaticamente

* 1. acessando a página pela url /diningRoom/saphire.html obtém-se a flag blue gem

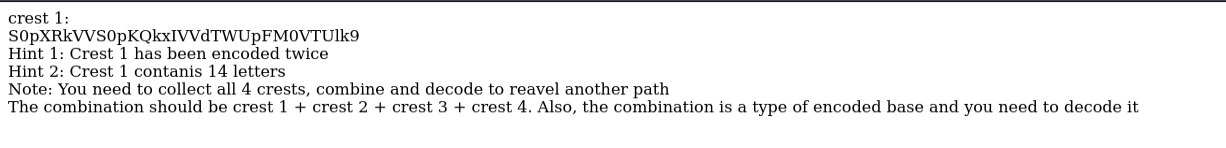
Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

* 1. na página Tiger status room há um input para colocar a flag da blue gem que redireciona para uma página com algumas informações encontra-se a primeira crista, agora é necessário encontras as outras 4

Interface gráfica do usuário, Texto, Aplicativo

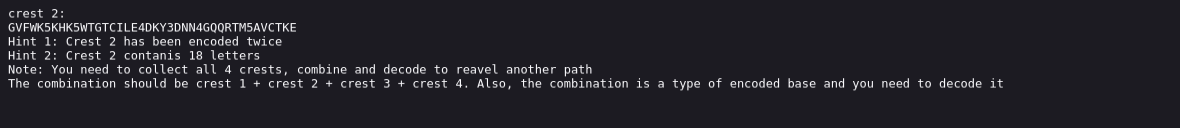
Descrição gerada automaticamente



* 1. Na página Gallery room há um redirecionamento para uma nota que possui a segunda crista

Texto

Descrição gerada automaticamente



* 1. Na página Armor room há um input para colocar a flag shield que redireciona para uma outra parte da sala com uma nota

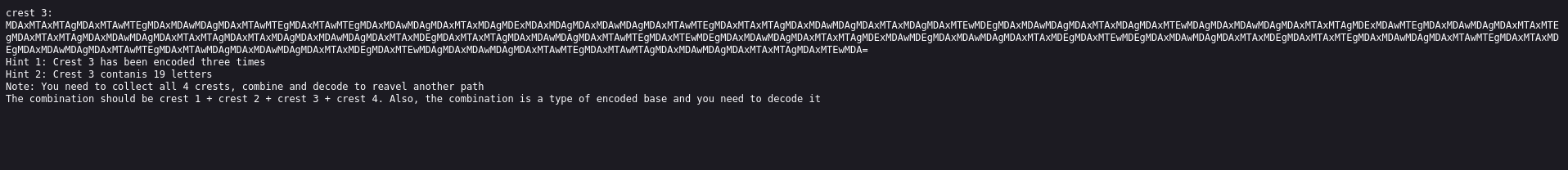
Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Uma imagem contendo foto, homem, mesa, display

Descrição gerada automaticamente

* 1. ao visualizar a nota é redirecionado para uma página com a terceira crista



* 1. acessando a página attic há novamente um input para colocar a flag shield que redireciona para uma outra parte da sala com uma nota

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Site

Descrição gerada automaticamente

* 1. ao visualizar a nota é redirecionado para uma página com a quarta crista

Texto

Descrição gerada automaticamente

* 1. descriptografando crista 1, primeiro com base64 e depois com base 32 (usando cyberchef)

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

* 1. decriptografando a crista 2, primeiro com base32 e depois com base 58 (usando cyberchef)

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Texto, Aplicativo, Tabela

Descrição gerada automaticamente

* 1. decriptografando a crista 3, primeiro com base64, depois com binário e depois com hexadecimal (usando cyberchef)

Tabela

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente com confiança baixa

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. decriptografando a crista 4, primeiro com base58 e depois com hexadecimal (usando cyberchef)

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. a senha obtida no final foi RlRQIHVzZXI6IGh1bnRlciwgRlRQIHBhc3M6IHlvdV9jYW50X2hpZGVfZm9yZXZlcg== e pode ser decriptografada com base64 (usando cyberchef), assim encontra-se o usuário e senha FTP.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Exploração via protocolo FTP
   1. Fazendo conexão com dados encontrados

Texto

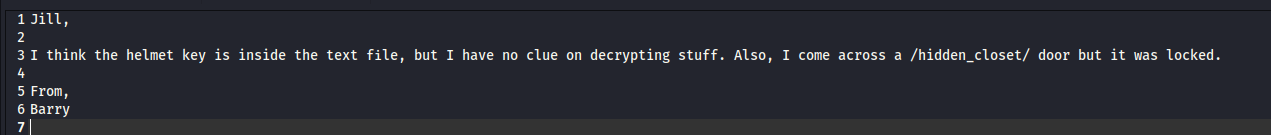
Descrição gerada automaticamente

* 1. no diretório atual, encontra-se três imagens com rótulo de key, a chave do helmet criptografada com gpg e um arquivo importante.txt

Texto

Descrição gerada automaticamente

* 1. no arquivo important.txt há uma confirmação que a key do helmet está dentro do arquivo gpg e uma direção para um outro path web



* 1. extraindo a senha criptografada da imagem 001 usando stegseek

Texto

Descrição gerada automaticamente

* 1. extraindo a senha escondida na imagem 002 nas strings da imagem

Texto

Descrição gerada automaticamente

* 1. extraindo a senha escondida na imagem 003 utilizando binwalk

Texto

Descrição gerada automaticamente

* 1. unindo os textos forma a senha cGxhbnQ0Ml9jYW5fYmVfZGVzdHJveV93aXRoX3Zqb2x0 que ao ser decriptografada por base 64 da a senha do arquivo gpg

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. decriptografando o arquivo gpg com a senha e obtendo a key helmet

Texto

Descrição gerada automaticamente

* 1. acessando o path que ele indicou no início há um campo para inserir a key obtida

Interface gráfica do usuário

Descrição gerada automaticamente

* 1. ao inserir a key do helmet redireciona para a página Closet room, com um redirecionamento para um disco magnético e um para uma medalha de lobo

Interface gráfica do usuário

Descrição gerada automaticamente

* 1. ao acessar o disco magnético há um texto criptografado

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

* 1. decriptografando a senha com vigenere (auto decode do <https://www.boxentriq.com/code-breaking/vigenere-cipher>), a senha do weasker é stars\_members\_are\_my\_guinea\_pig

Interface gráfica do usuário, Aplicativo

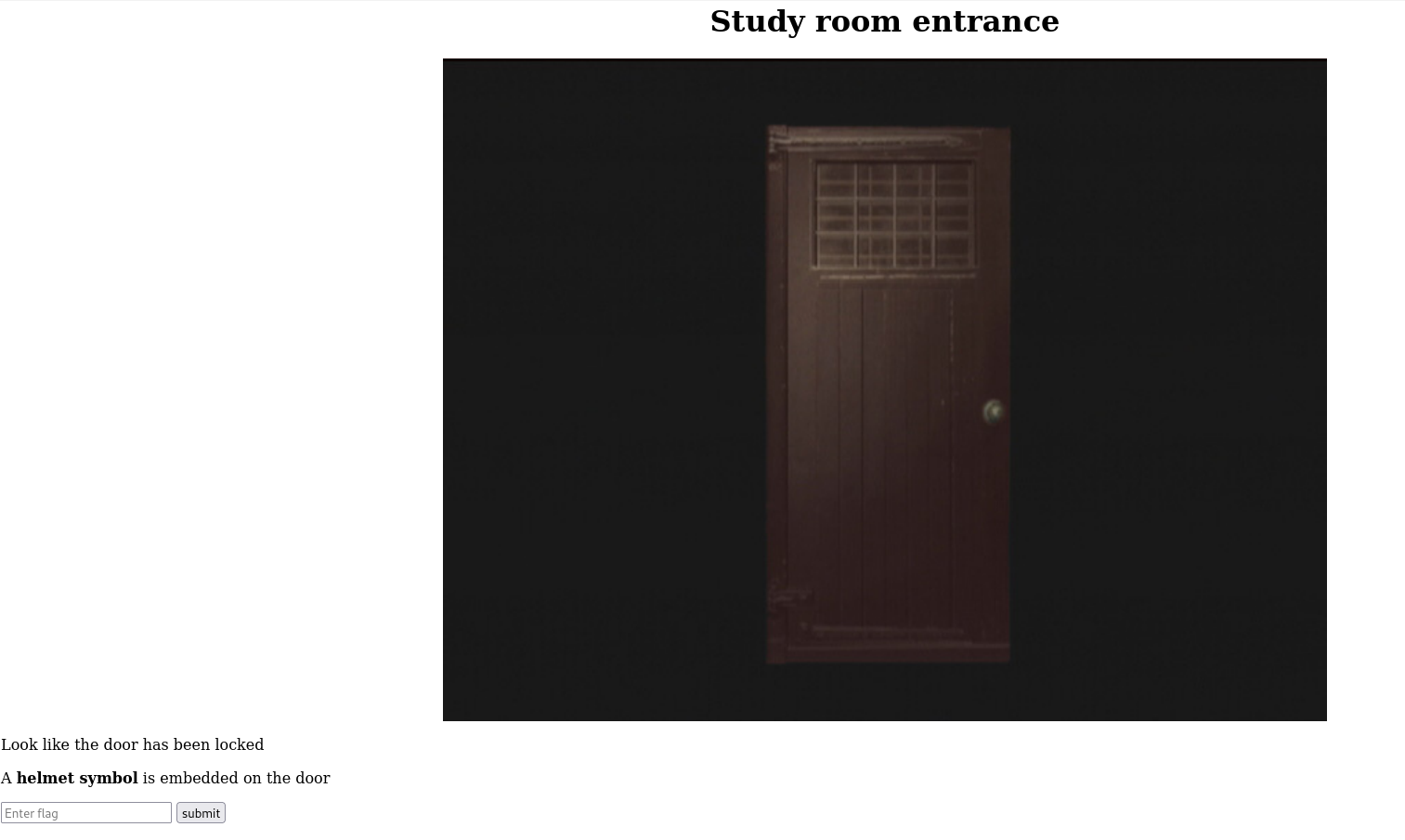
Descrição gerada automaticamente

* 1. na página da medalha de lobo há a senha de acesso ssh

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. na página Study room há um input para colocar a key do helmet também



* 1. ao inserir a key redireciona para uma página que contém um livro para ser examinado

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. ao acessar a página do livro, um arquivo.tar.gz é baixado
  2. descompactando o arquivo, obtém-se um arquivo com o usuário ssh

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente com confiança média

1. Exploração via protocolo SSH
   1. conectando via ssh com o usuário e senha

Texto

Descrição gerada automaticamente

* 1. ao procurar diretórios e arquivos ocultos encontra-se um diretório .jailcell com um arquivo chris.txt, onde há o código do disco 2

Texto

Descrição gerada automaticamente

* 1. entrando no diretório do usuário weasker encontra-se uma nota que indica que ele é o traidor

Texto

Descrição gerada automaticamente

* 1. entrando no usuário weasker com o login e senha, descobre-se que ele tem acesso à todos os comandos sudo

Texto

Descrição gerada automaticamente

* 1. entrando no privilégio de root encontra-se a flag root.txt no diretório root, com a flag e o nome da forma final

Texto

Descrição gerada automaticamente