

# Challenge: Pickle Rick

## Processo de Exploração

### 1. Coleta de informações iniciais

- No primeiro momento, buscamos o máximo de informação possível sobre o sistema alvo.
  - Ping / conectividade.  
-> ping IP
  - Varredura de portas e serviços com Nmap:  
-> nmap IP -T4
  - Mapeamento de diretórios com Gobuster:..  
-> gobuster dir -u IP -w wordlist
  - Inspecionar HTML/JS/CSS/Assets por dicas  
-> Verificamos o código-fonte e identificamos o nome do usuário, que armazenamos para uso posterior..

### 2. Descoberta de diretórios e login

Durante a exploração do Gobuster, encontramos possíveis diretórios. A wordlist inicial não mapeou o diretório login.php, mas após testar manualmente, encontramos a página de login.

- Tínhamos o nome de usuário, mas não a senha.
- Analisando arquivo por arquivo, não obtivemos informações relevantes.
- Ao verificar o robots.txt, encontramos uma informação útil que permitiu acessar o portal.

### 2. Painel do Portal

Dentro do portal, exploramos algumas abas. No painel de comando:

- Executamos ls e outros comandos, alguns funcionaram, outros não.
- Inicialmente tivemos dificuldade com o comando GET, não conseguimos visualizar o conteúdo. Após uma hora tentando, pesquisamos no YouTube e aprendemos a usar:

-> less <arquivo>

### 3. Flags Obtidas:

#### 1. Primeira flag:

Encontrada no arquivo lido com less:

-> mr. meeseek hair

#### 2. Segunda flag:

Dentro de clue.txt havia uma dica, mas ficamos travados. Após pesquisa, percebemos que a flag estava associada ao usuário rick:

-> jerry tear

#### 3. Terceira flag:

Explorando o diretório raiz, encontramos a terceira flag, completando a sequência de ingredientes do desafio.

-> fleeb juice

### 4. Dificuldades

- Esquecimento de comandos básicos de Linux: tivemos dificuldade em lembrar comandos essenciais para explorar o sistema.
- Tentativas longas sem sucesso: passamos mais de 1h horas tentando abordagens diferentes antes de perceber a necessidade de pesquisar.