**02/06/2024 – CHOCOLATE FACTORY**

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

1. Mapeamento com Nmap
   1. utilizando -p- para descobrir as portas abertas e os serviços

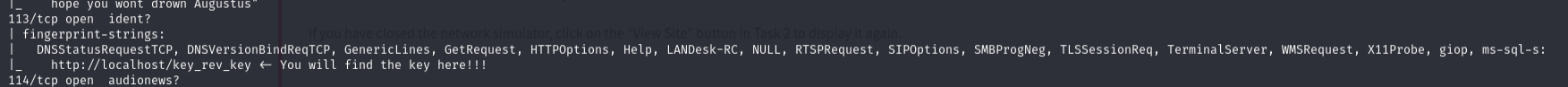
Texto

Descrição gerada automaticamente com confiança média

* 1. o mapeamento detalhado das portas abertas mostrou informações importantes.
  2. FTP com login anonymous.
  3. A sequência de portas 100 – 125 mostrou mensagens com mensagens para procurar em outro lugar, com exceção da porta 113 que indicou o caminho da chave.

Linha do tempo

Descrição gerada automaticamente com confiança média



1. Conexão FTP com usuário anonymous­­­
   1. imagem gum\_room.jpg disponível

Texto

Descrição gerada automaticamente

1. Estenografia com a imagem
   1. usando ferramenta stegseek
   2. arquivo de texto criptografado em base64 injetado na imagem

Texto

Descrição gerada automaticamente

* 1. extraindo o arquivo com stegseek, sem uso de senha

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. decriptografando usando decoder online (<https://www.base64decode.org/>)
  2. arquivo do /etc/shadow

Uma imagem contendo Texto

Descrição gerada automaticamente

* 1. descriptografando usando john chega-se a senha do charlie

Texto

Descrição gerada automaticamente

1. Explorando diretório indicado
   1. acessando /key\_rev\_key, o navegador baixa um arquivo key\_rev\_key
   2. executando nano /key\_rev\_key para ler o arquivo encontra-se a chave



1. Fazendo login com o usuário charlie no navegador
   1. input permite realizar comandos bash
   2. procurando arquivos no diretório



* 1. usuário charlie na pasta /home
  2. chaves RSA privada e pública

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente com confiança média

1. Conexão com chave RSA
   1. usuário charlie

Texto

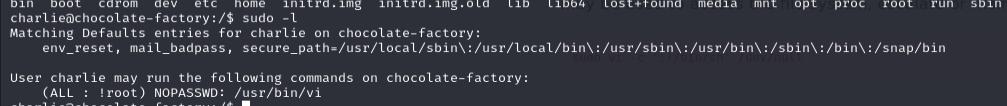
Descrição gerada automaticamente

1. Flag user.txt na pasta /home/charlie

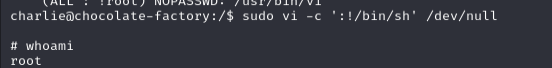
Texto

Descrição gerada automaticamente

1. Privesc
   1. procurando através de comandos sudo



* 1. privesc através do sudo vi (<https://gtfobins.github.io/gtfobins/vi/#sudo>)



1. Encontrando flag do root
   1. dentro da pasta /root há um arquivo python (root.py), ao rodar ele pede a chave obtida no ínicio

Forma

Descrição gerada automaticamente com confiança média

Texto

Descrição gerada automaticamente