21/07/2023 – TryHackMe – Brooklyn Nine Nine

Link: <https://tryhackme.com/room/brooklynninenine>

1. Fazendo um port scanning usando nmap:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Verificando que o usuário “anonymous” está habilitado no serviço FTP:

Texto

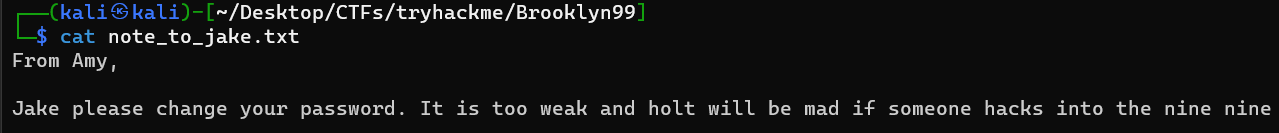
Descrição gerada automaticamente

1. Verificando os arquivos presentes:

Texto

Descrição gerada automaticamente

1. Lendo o arquivo resgatado:



1. Supondo que tal usuário possui username “jake” no serviço SSH, utilizar o Hydra para atacar com bruteforce a fim de encontrar a senha do alvo:

Texto branco sobre fundo preto

Descrição gerada automaticamente

1. Utilizar a senha encontrada para entrar no servidor pelo serviço SSH:

Texto

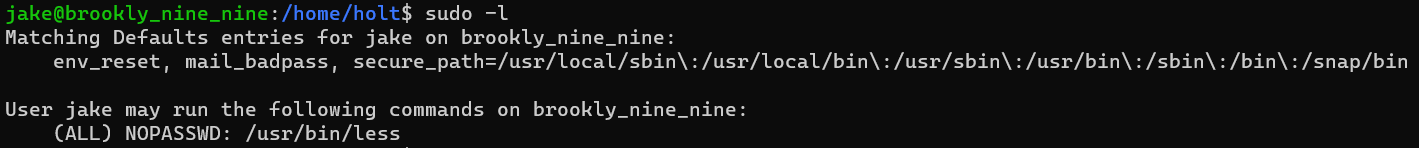
Descrição gerada automaticamente

1. Explorando os diretórios, é possível encontrar a primeira flag:

Texto

Descrição gerada automaticamente

1. Verificando binários que podem utilizar sudo sem necessidade de senha:



1. Pesquisando no site <https://gtfobins.github.io/gtfobins> sobre possíveis formas de escalação de privilégio com o binário less, pode se encontrar o seguinte:

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

1. Utilizando no alvo:



Texto

Descrição gerada automaticamente

1. Encontrando a última flag no diretório /root:

Texto

Descrição gerada automaticamente