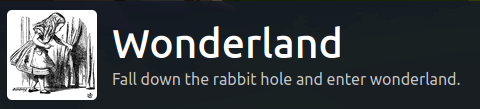
**Wonderland**

**TryHackMe**



Para começar a exploração da máquina, vamos realizar um nmap e descobrir as portas abertas.

Texto

Descrição gerada automaticamente

Descobrimos que nele existem as portas 22 e 80 abertas. Como se trata de uma aplicação web, podemos começar a explorar manualmente.

Texto

Descrição gerada automaticamente

Entrando na porta 80, descobrimos a página inicial do site, nela tem uma mensagem para nós seguirmos o coelho. Analisando um pouco o código fonte, descobrimos o diretório /img/, na qual está a nossa imagem. Podemos ver de existe directory listening e tentar descobrir outros arquivos.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Aqui é possível descobrir algo um pouco suspeito, pois existem 2 imagens da alice\_door, uma com jpg e outra com png. Talvez tenha algo aí.

Continuando a exploração, vamos fazer uma enumeração de diretórios e tentar descobrir coisas escondidas.

Texto

Descrição gerada automaticamente

Com isso, foi possível encontrar 2 diretórios que podem ser importantes, o primeiro é o /r e outro é o /poem.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Nesse indica que há algo a mais para se descobrir, podemos tentar vasculhar diretórios dentro dele.

Texto, Carta

Descrição gerada automaticamente

Nessa mostra um poema que pode ser útil em algum momento.

Depois de pensar um pouco, conseguimos descobrir os diretórios por trás do /r, ele forma a paralva “rabbit”.

Texto

Descrição gerada automaticamente

Com isso, descobrimos uma mini historinha que está sendo contata em cada página. No final dela, ou seja, na última página, podemos ver o código fonte e ver possíveis credenciais de acesso.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

- alice:HowDothTheLittleCrocodileImproveHisShiningTail

Podemos tentar essas credenciais para nos conectar no ssh.

Texto

Descrição gerada automaticamente

Com isso nos conectamos com sucesso, agora somos o usuário Alice.

Quando entramos com a aline, vimos que no diretório dela existe um arquivo chamado root.txt, que só é acessível pelo root e, um arquivo python do root, mas que temos permissão de leitura.

Texto

Descrição gerada automaticamente

Além disso, descobrimos que existem outros 3 usuários no sistema, além da alice.

Texto

Descrição gerada automaticamente

Lendo o script em python, vimos que ele mostra um poema e gera 10 linhas aleatórias para serem mostradas na tela.

Texto

Descrição gerada automaticamente

Dando o comando sudo -l, vimos que podemos executar o python3.6 como usuário rabbit. Podemos tentar usar isso para nos movermos lateralmente para o rabbit. Para isso, podemos tentar infectar o script random em python, que está sendo importado logo no início do programa.

Com isso, criamos um arquivo chamado random.py com um script que nos dá shell.

Texto

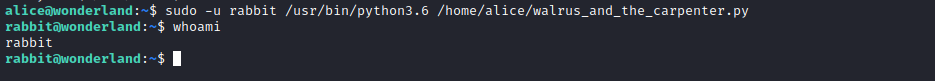
Descrição gerada automaticamente

Texto

Descrição gerada automaticamente com confiança média

Com isso, executamos o programa como usuário rabbit, pois temos permissão e, nos tornamos ele.

- sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus\_and\_the\_carpenter.py



Agora navegando para o diretório do rabbit, descobrimos que existe um binário que pode ser executado com SUID do root.

Uma imagem contendo Calendário

Descrição gerada automaticamente

Executando esse binário, vimos que ele informa a data atual e nos fala para perguntar algo.

Primeiramente, podemos tentar supor que esse binário chama a função “date” do Linux sem passar seu caminho completo. Caso isso não dê certo, pode ser que tenhamos que fazer um buffer overflow desse binário.

Podemos então para isso criar um arquivo infectado chamado date em /tmp, dar permissão para ele e colocar o diretório tmp em primeiro no PATH.

Texto

Descrição gerada automaticamente

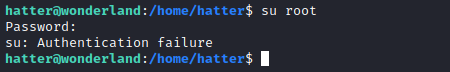
Com isso nos tornamos o usuário “hatter”. Indo no diretório dela, vimos que existe um arquivo interessante chamado password.txt

Texto

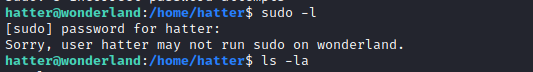
Descrição gerada automaticamente

Nesse arquivo tem um texto que muito provavelmente pode ser a senha do root, vamos tentar então.

- WhyIsARavenLikeAWritingDesk?



Não conseguimos nos autenticar como root, podemos então tentar outra coisa, essa senha pode ser a da própria hatter e podemos ter alguma coisa interessante no sudo -l.



Fazendo isso, vimos que não é isso também, porém sabemos que essa é a senha da hatter.

Continuando a exploração, descobrimos que a hatter pode executar comandos de setuid.

Texto

Descrição gerada automaticamente

Podemos explorar isso para tentar nos tornar root.

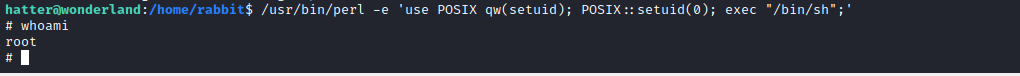
Tentando explorar isso pegando um script do gtfobins, porém, descobrimos que nosso usuário não está com gid da hatter, mas sim do rabbit, com isso não está dando permissão no perl.

Texto

Descrição gerada automaticamente

Para isso, tivemos que usar a senha da hatter e virar ela com o comando “su”, com isso conseguimos executar o comando que irá nos tornar root.

- /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'



Com isso nos tornamos root e terminamos a o CTF.