Auditoría sistemas operativos GNU/Linux, UNIX: linpeas

ESCENARIO

Máquina virtual ou física:

RAM ≥ 4096MB CPU ≥ 2 PAE/NX habilitado

ISO/CD/DVD/USB: kali-linux amd64

REDE: DHCP (NAT)

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **[1] LinPEAS - Linux Privilege Escalation Awesome Script**
- **[2] HackTricks - Linux Privilege Escalation**
- **[3] GNU/Linux Hardening básico**
- **[4] sudo/visudo → Xestión de usuarios (páx. 34)**

Máquina virtual Kali amd64

1. **linpeas (Auditar o sistema operativo)**

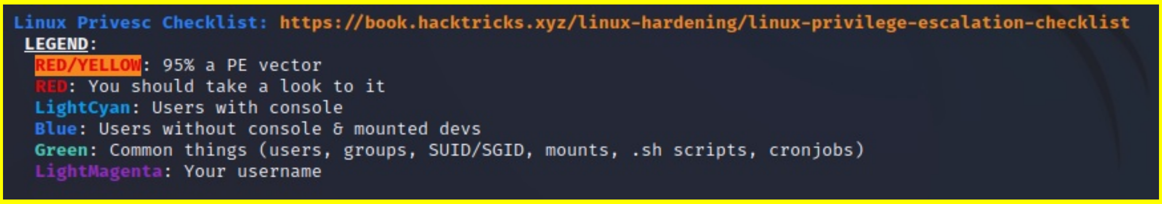
Na contorna gráfica abrir un terminal e executar:

kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
kali@kali:~$ curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
#Descargar linpeas dende github mediante curl. Unha vez descargado executar o script linpeas mediante a shell sh.

LinPEAS é un script que busca posibles rutas para escalar privilexios en hosts Linux/Unix*/MacOS. As comprobacións explícanse en **book.hacktricks.xyz**.

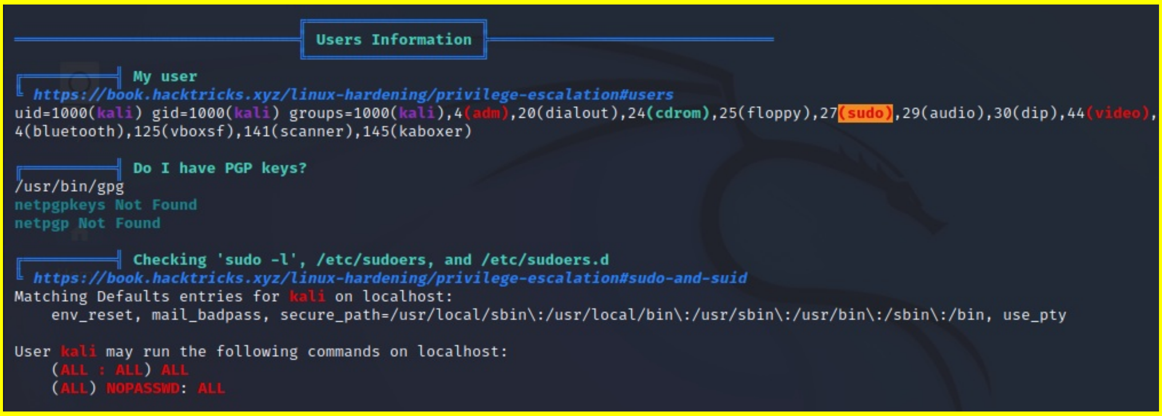
Consulte a lista de verificación de Escalada de privilexios de Linux local desde **book.hacktricks.xyz**

Na execución amosa en cores o nivel de escalada de privilexios. A maior posibilidade de escalada de privilexios posúe o fondo RED/YELLOW:



```
Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username
```

Cada sección indica cos cores anteriores a posilibidade de escalada de privilexios. Tamén indica ligazóns informando sobre as posibles escaladas.



```
Users Information

My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),
4(bluetooth),125(vboxsf),141(scanner),145(kaboxer)

Do I have PGP keys?
/usr/bin/gpg
netpgpkeys Not Found
netpgp Not Found

Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for kali on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
```

2. **Explotar a escalada de privilexios atopada na sección Checking 'sudo -l'**

kali@kali:~$ sudo -l #Listar os comandos permitidos e prohibidos a través de sudo do usuario que executa o comando, neste caso o usuario *kali*

```
...
User kali may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
```

Podemos indicar o listado dos comandos sudo dun usuario en cuestión empregando a opción -U. Así, por exemplo:
kali@kali:~$ sudo -l -U ana #Listar os comandos permitidos e prohibidos a través de sudo do usuario *ana*

Entón, como podemos comprobar en **[4]** o usuario kali pode executar calquera comando a través do propio comando **sudo** sen que se lle solicite un contrasinal. Así, executando o comando: ***sudo su -*** , o usuario **kali** pode acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

root@kali:~#