Auditoría sistemas operativos Microsoft Windows: winpeas

ESCENARIO

Máquina virtual ou física:

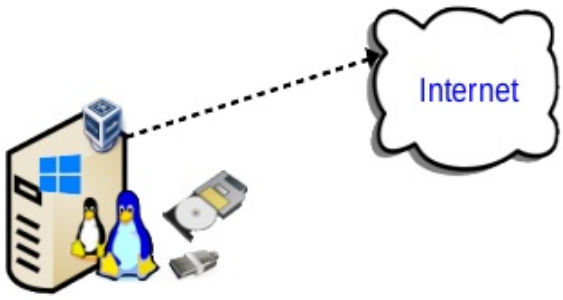
RAM ≥ 4096MB CPU ≥ 2 PAE/NX habilitado

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

REDE: DHCP (NAT)

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

Disco duro: Microsoft Windows



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:

- **Instalación por defecto**: A instalación do sistema operativo Microsoft Windows realizouse por defecto, é dicir, seguindo os pasos do instalador,
- **Apagado normal do sistema operativo**: Para un correcto funcionamento da práctica o sistema operativo Microsoft Windows debe ser apagado sen inconsistencias evitando problemas no sistema de ficheiros NTFS.
- **[1] WinPEAS - Windows Privilege Escalation Awesome Scripts**
- **[2] HackTricks - Windows Local Privilege Escalation**
- **[3] winpeas - releases**
- **[4] .NET**
- **[5] Descargar .NET**
- **[6] Práctica BRS Funcións Resumo (Funcións Hash)**

WinPEAS é unha ferramenta que busca posibles rutas para escalar privilexios en hosts Microsoft Windows. As comprobacións explícanse en **book.hacktricks.xyz**.

Consulte a lista de verificación de Escalada de privilexios de Windows local en **book.hacktricks.xyz**

Existen 2 proxectos(programas) winpeas: **winpeas.bat** e **winpeas.exe**. Se traballamos co executable (winpeas.exe), teremos como prerrequisito ter instalado .Net (>= 4.5.2), e se traballamos co arquivo por lotes (winpeas.bat) na saída da execución non teremos cores, os cales amosan o nivel de escalada de privilexios.

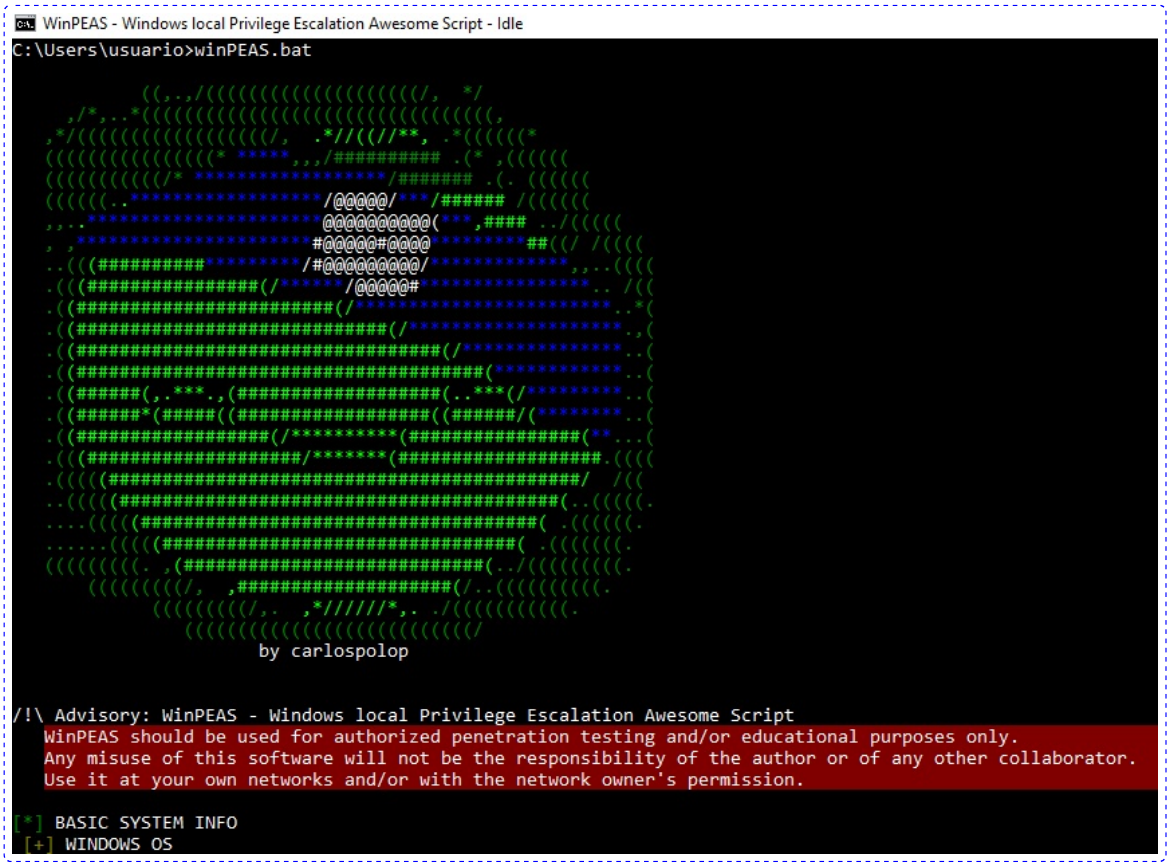
Máquina virtual Microsoft Windows

1. **winpeas.bat (Auditar o sistema operativo)**
   A. Arrancar a máquina virtual coa ISO Kali Live amd64 e 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/download/20221211/winPEAS.bat -o /tmp/winPEAS.bat #Descargar winPEAS.bat a /tmp dende github mediante curl. **NOTA: Verificar a ligazón de descarga en [3]**
      kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
         root@kali:~# fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.
         root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
         root@kali:~# mount -t auto /dev/sda2 /mnt #Montar a partición 2 do disco duro /dev/sda no directorio da live /mnt. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe. Poderiamos tamén empregar o comando **ntfs-3g /dev/sda2 /mnt** , o cal xa traballa directamente co sistema de ficheiros NTFS..
         root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali. Neste caso verificamos que a última liña refírese ao punto de montaxe /mnt onde podemos traballar coa partición /dev/sda2.
         root@kali:~# cp -pv /tmp/winPEAS.bat /mnt/Windows/System32/spool/drivers/color/ #Copiar winPEAS.bat nunha ruta dentro do sistema operativo Microsoft Windows
         root@kali:~# umount /mnt #Desmontar (deixar de facer uso) a partición primaria /dev/sda2 que estaba montada en /mnt
         root@kali:~# init 0 #Apagar a máquina enviando o sinal de apagado mediante o runlevel 0

   B. Acceder á configuración da máquina virtual e poñer como primeira opción de arranque o disco duro, para que arranque o sistema operativo Microsoft Windows. Unha vez arrancado o sistema operativo:
      1. Acceder cun usuario sen permisos de administrador.
      2. Abrir unha consola de comandos **cmd** e executar:

```
> cd C:\Windows\System32\spool\drivers\color
> winPEAS.bat
```



Máquina virtual Microsoft Windows

2. **winpeas.exe (Auditar o sistema operativo)**
   A. Arrancar a máquina virtual coa ISO Kali Live amd64 e 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/download/20221211/winPEASx64.exe -o /tmp/winpeas.exe #Descargar winPEASx64.exe a /tmp/winpeas.exe dende github mediante curl. NOTA: Verificar a ligazón de descarga en [3]
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
root@kali:~# fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.
root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
root@kali:~# mount -t auto /dev/sda2 /mnt #Montar a partición 2 do disco duro /dev/sda no directorio da live /mnt. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe. Poderiamos tamén empregar o comando ntfs-3g /dev/sda2 /mnt , o cal xa traballa directamente co sistema de ficheiros NTFS..
root@kali:~# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali. Neste caso verificamos que a última liña refírese ao punto de montaxe /mnt onde podemos traballar coa partición /dev/sda2.
root@kali:~# cp -pv /tmp/winpeas.exe /mnt/Windows/System32/spool/drivers/color/ #Copiar winpeas.exe nunha ruta dentro do sistema operativo Microsoft Windows
root@kali:~# umount /mnt #Desmontar (deixar de facer uso) a partición primaria /dev/sda2 que estaba montada en /mnt
root@kali:~# init 0 #Apagar a máquina enviando o sinal de apagado mediante o runlevel 0
```

   B. Acceder á configuración da máquina virtual e poñer como primeira opción de arranque o disco duro, para que arranque o sistema operativo Microsoft Windows. Unha vez arrancado o sistema operativo:
      1. Descargar[5] e instalar .NET (Lembrar que é un prerrequisito para que se poida executar winPEAS.exe)

Fig A. Descargar .NET

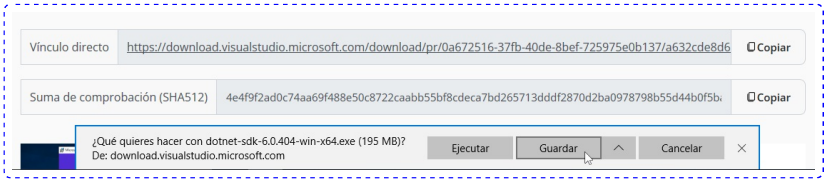


Fig B. Guardar

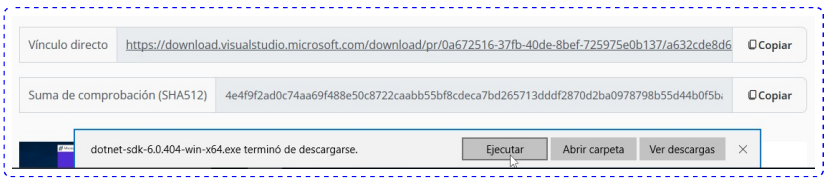


Fig C. Ejecutar

Comprobar hash SHA512 [6]:

```
> certutil -hashfile dotnet-sdk-6.0.404-win-x64.exe SHA512
```

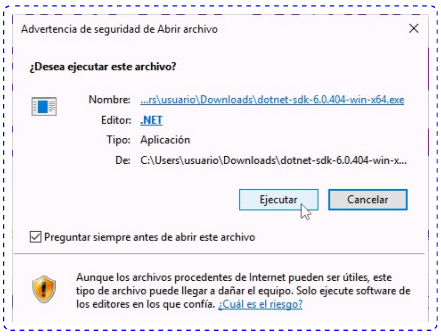


Fig D. Ejecutar

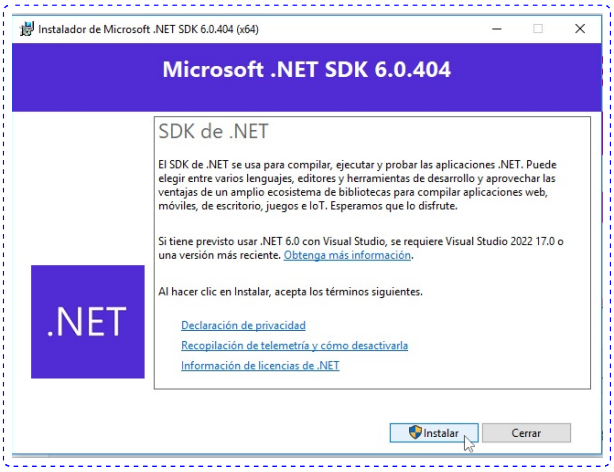


Fig E. Instalar

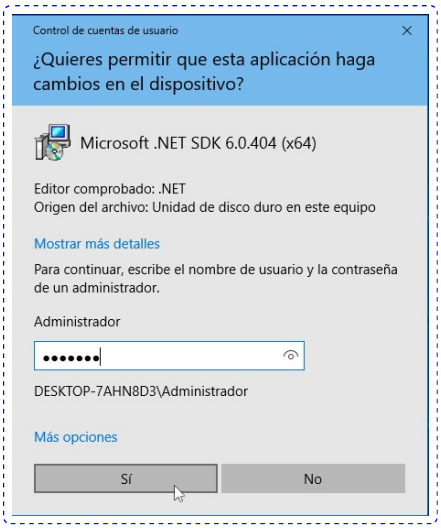


Fig F. Sí

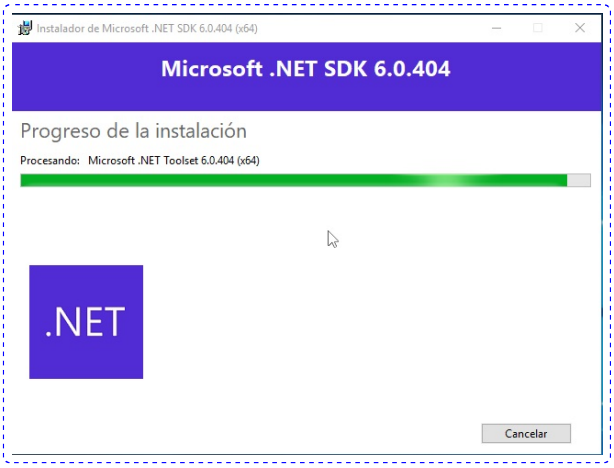


Fig G. Progreso de la instalación

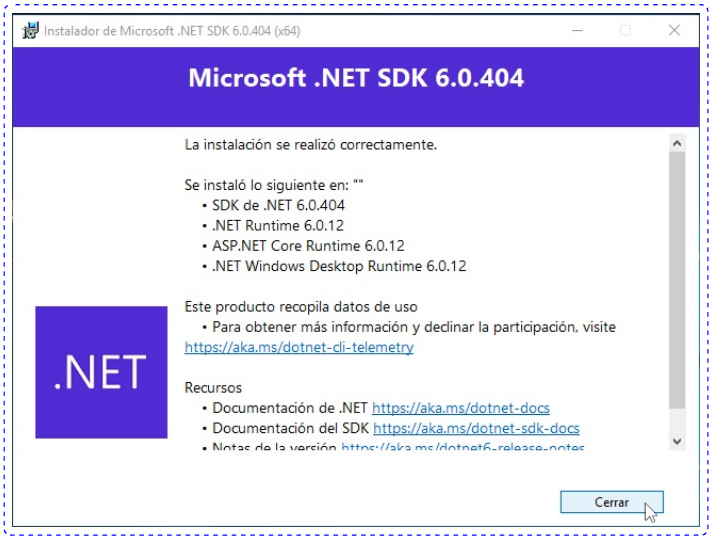


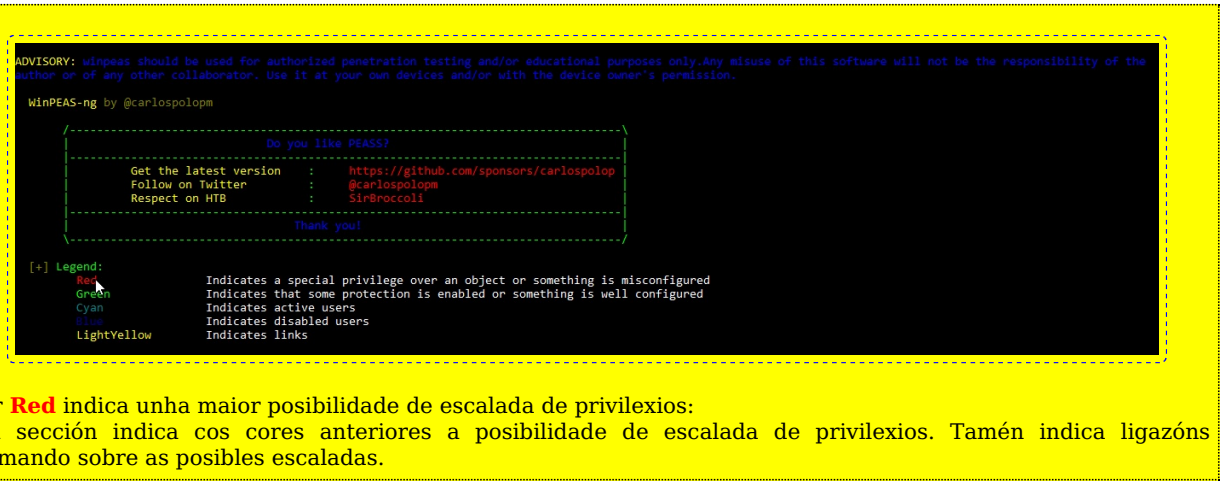
Fig H. Cerrar

2. Acceder cun usuario sen permisos de administrador.
3. Abrir unha consola de comandos **cmd** e executar:

```
> REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1
> exit
```

4. Abrir unha nova consola de comandos **cmd** e executar:

```
> cd C:\Windows\System32\spool\drivers\color
> winpeas.exe
```



A cor **Red** indica unha maior posibilidade de escalada de privilexios:
Cada sección indica cos cores anteriores a posibilidade de escalada de privilexios. Tamén indica ligazóns informando sobre as posibles escaladas.

3. **Razoa e contesta brevemente:**

   Se se realizan de novo os apartados anteriores 1 e 2, pero:

   a. Descargando os executables winPEAS.bat e winPEASx64.exe dende o propio sistema operativo Microsoft Windows.
   b. Executando os programas descargados dende a propia contorna gráfica.

   Bloquease a súa execución

Ricardo Feijoo Costa