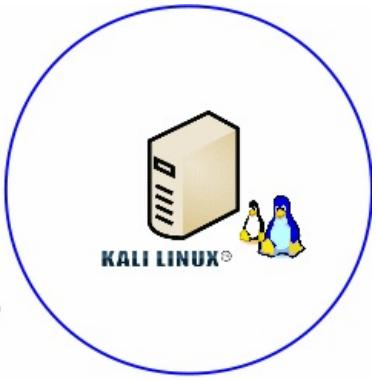
Práctica Seguridade Informática: Esteganografía

ESCENARIO

Máquina Kali Linux:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
ISO: Kali Live amd64

"KALI LINUX ™ é unha marca comercial de Offensive Security"



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:

- **Comandos: cat, file, strings, dd, xxd**
- **magic number or file signatures**
- **binwalk**
- **foremost**
- **steghide**
- **Imaxe PNG empregada → kempachitux**

Práctica SI Esteganografía

Máquina Kali amd64

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

Exemplo 1

2. Concatenar ficheiros:
   kali@kali:~$ wget https://openclipart.org/image/2000px/133561 -O kempachitux.png #Descargar imaxe kempachitux.png
   kali@kali:~$ echo 'Kali GNU/Linux - 1234567890' > file.txt #Xerar o ficheiro file.txt
   kali@kali:~$ cat kempachitux.png file.txt > file.png #Concatenar os ficheiros kempachitux.png e file.txt en file.png, obtendo así un ficheiro imaxe de resultado
   kali@kali:~$ file file.png #Determinar que tipo de ficheiro é o ficheiro file.png. Neste caso: tipo imaxe PNG image data

   ```
   file.png: PNG image data, 1990 x 2000, 8-bit/color RGBA, non-interlaced
   ```

   kali@kali:~$ ls -l kempachitux.png file.png #Listar de forma extendida os ficheiros kempachitux.png e file.png. Ambos amosan a mesma imaxe pero posúen distinto tamaño. Iso é debido a que file.png tamén contén oculto un arquivo de texto (file.txt)

   ```
   -rw-r--r-- 1 kali kali 647631 nov 10 13:32 file.png
   -rw-r--r-- 1 kali kali 647603 nov 10 13:31 kempachitux.png
   ```

3. A. Esteganografía (binwalk): Ver arquivos ocultos na imaxe file.png:
   kali@kali:~$ binwalk --dd='.*' -e file.png #Extraer se é o caso contido oculto no cartafol _file.png.extracted

   ```
   DECIMAL       HEXADECIMAL     DESCRIPTION
   --------------------------------------------------------------------------------
   0             0x0             PNG image, 1990 x 2000, 8-bit/color RGBA, non-interlaced
   477           0x1DD           Zlib compressed data, best compression
   ```

   kali@kali:~$ ls _file.png.extracted #Listar o contido do cartafol _file.png.extracted

   ```
   total 16820
   -rw-r--r-- 1 kali kali   647631 nov 10 13:32 0
   -rw-r--r-- 1 kali kali 15922000 nov 10 13:32 1DD
   -rw-r--r-- 1 kali kali   647154 nov 10 13:32 1DD.zlib
   ```

   kali@kali:~$ file _file.png.extracted/* #Determinar os tipos de ficheiros existentes no cartafol _file.png.extracted

   ```
   _file.png.extracted/0:        PNG image data, 1990 x 2000, 8-bit/color RGBA, non-interlaced
   _file.png.extracted/1DD:      data
   _file.png.extracted/1DD.zlib: zlib compressed data
   ```

   kali@kali:~$ cat _file.png.extracted/1DD.zlib #Ver o contido do ficheiro. Fixarse na última liña → contido de file.txt que estaba oculto na imaxe file.png

   ```
   ...
   ...
   ...
   ?[illegible]Z[illegible]i[illegible]X3[illegible]J[illegible]V%[illegible]i[illegible]F[illegible]J[illegible]D[illegible]^[illegible] *V[illegible]v[illegible]v[illegible]+![illegible]![illegible]{K[illegible]IEND[illegible]B`[illegible]Kali GNU/Linux - 1234567890
   ```

   B. Esteganografía - Outro método (strings): Ver arquivos ocultos na imaxe file.png:
   kali@kali:~$ strings -n 22 file.png #Ver cadeas de texto con lonxitude mínima de 22 caracteres

   ```
   this tux is inspired by zaraki kempachi from the manga "bleach"S
   https://openclipart.org/detail/133561/kempachi-tux-by-zafx
   CC0 Public Domain Dedication http://creativecommons.org/publicdomain/zero/1.0/
   Kali GNU/Linux - 1234567890
   ```

Exemplo 2

4. Concatenar ficheiros:

kali@kali:~$ wget https://openclipart.org/image/2000px/133561 -O kempachitux.png #Descargar imaxe kempachitux.png

kali@kali:~$ echo 'Kali GNU/Linux - 1234567890' > file.txt #Xerar o ficheiro file.txt

kali@kali:~$ tar cvjf file.tar.bz2 file.txt #Empaquetar e comprimir o ficheiro file.txt en file.tar.bz2

kali@kali:~$ cat kempachitux.png file.tar.bz2 > file2.png #Concatenar os ficheiros kempachitux.png e file.tar.bz2 en file2.png, obtendo así un ficheiro imaxe de resultado

kali@kali:~$ file file2.png #Determinar que tipo de ficheiro é o ficheiro file2.png. Neste caso: tipo imaxe PNG image data

```
file.png: PNG image data, 1990 x 2000, 8-bit/color RGBA, non-interlaced
```

kali@kali:~$ ls -l kempachitux.png file2.png #Listar de forma extendida os ficheiros kempachitux.png e file.png. Ambos amosan a mesma imaxe pero posúen distinto tamaño. Iso é debido a que file.png tamén contén oculto un arquivo comprimido (file.tar.bz2)

```
-rw-r--r-- 1 kali kali 647758 nov 10 13:42 file2.png
-rw-r--r-- 1 kali kali 647603 nov 10 13:31 kempachitux.png
```

5. A. Esteganografía (binwalk): Ver arquivos ocultos na imaxe file2.png:

kali@kali:~$ binwalk --dd='.*' -e file2.png #Extraer se é o caso contido oculto no cartafol _file2.png.extracted

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1990 x 2000, 8-bit/color RGBA, non-interlaced
477           0x1DD           Zlib compressed data, best compression
647603        0x9E1B3         bzip2 compressed data, block size = 900k
```

kali@kali:~$ ls _file2.png.extracted #Listar o contido do cartafol _file2.png.extracted

```
total 16836
-rw-r--r-- 1 kali kali   647758 nov 10 13:42 0
-rw-r--r-- 1 kali kali 15922000 nov 10 13:42 1DD
-rw-r--r-- 1 kali kali   647281 nov 10 13:42 1DD.zlib
-rw-r--r-- 1 kali kali    10240 nov 10 13:42 9E1B3
```

kali@kali:~$ file _file2.png.extracted/* #Determinar os tipos de ficheiros existentes no cartafol _file2.png.extracted

```
_file2.png.extracted/0:        PNG image data, 1990 x 2000, 8-bit/color RGBA, non-interlaced
_file2.png.extracted/1DD:      data
_file2.png.extracted/1DD.zlib: zlib compressed data
_file2.png.extracted/9E1B3:    POSIX tar archive (GNU)
```

kali@kali:~$ tar tvf _file2.png.extracted/9E1B3 #Amosar o contido empaquetado no ficheiro 9E1B3

```
-rw-r--r-- kali/kali  28 2021-11-10 13:44 file.txt
```

kali@kali:~$ tar xvf _file2.png.extracted/9E1B3 -C _file2.png.extracted #Extraer o contido empaquetado no ficheiro 9E1B3 no cartafol _file2.png.extracted.

```
file.txt
```

kali@kali:~$ cat _file2.png.extracted/file.txt #Ver o contido do ficheiro file.txt que estaba oculto na imaxe file2.png

```
Kali GNU/Linux - 1234567890
```

B. Esteganografía - Outro método (binwalk + dd): Ver arquivos ocultos na imaxe file2.png:

kali@kali:~$ binwalk file2.png #Extraer se é o caso contido oculto no cartafol _file2.png.extracted

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1990 x 2000, 8-bit/color RGBA, non-interlaced
477           0x1DD           Zlib compressed data, best compression
647603        0x9E1B3         bzip2 compressed data, block size = 900k
```

kali@kali:~$ dd if=file2.png of=hide bs=1 skip=647603 #Recuperación dos bloques que conteñen o ficheiro oculto file.txt mediante o comando dd. Recuperamos do ficheiro file2.png o ficheiro hide. Para iso ao comando dd pasámolle como argumentos o valor do bloque (bs=1) e dende que bloque comezar a recuperar (skip).

```
155+0 registros leídos
155+0 registros escritos
155 bytes copied, 0,000843733 s, 184 kB/s
```

kali@kali:~$ file hide #Determinar o tipo de ficheiro hide

kali@kali:~$ tar tvfj hide #Amosar o contido empaquetado e comprimido no ficheiro hide

```
hide: bzip2 compressed data, block size = 900k
```

kali@kali:~$ tar xvfj hide #Extraer o contido empaquetado e comprimido no ficheiro hide.

```
file.txt
```

kali@kali:~$ cat file.txt #Ver o contido do ficheiro file.txt que estaba oculto na imaxe file2.png

```
Kali GNU/Linux - 1234567890
```

Exemplo 3

6. **Magic Number / File Signature:**

kali@kali:~$ xxd kempachitux.png | head -1 #Ver o contido hexadecimal do ficheiro kempachitux.png e filtrar a saída para quedarse soamente coa primeira liña, na cal observamos que o ficheiro comeza por **8950 4e47 0d0a 1a0a** o que significa que é un ficheiro PNG

```
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
```

kali@kali:~$ xxd file.png | head -1 #Ver o contido hexadecimal do ficheiro file.png e filtrar a saída para quedarse soamente coa primeira liña, na cal observamos que o ficheiro comeza por **8950 4e47 0d0a 1a0a** o que significa que é un ficheiro PNG

```
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
```

kali@kali:~$ xxd file2.png | head -1 #Ver o contido hexadecimal do ficheiro file2.png e filtrar a saída para quedarse soamente coa primeira liña, na cal observamos que o ficheiro comeza por **8950 4e47 0d0a 1a0a** o que significa que é un ficheiro PNG

```
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
```

kali@kali:~$ xxd file2.png | grep BZh #Ver o contido hexadecimal do ficheiro file2.png e filtrar a saída co patrón de búsqueda BZh, na cal observamos que no ficheiro file2.png existe o magic number **BZh (equivalente ao hexadecimal 42 5a 68, sendo neste caso 42 5a68 na dirección 0x9e1b0)** o que significa que é un ficheiro Bzip2

```
0009e1b0: 4260 8242 5a68 3931 4159 2653 598d c3a7  B`.BZh91AY&SY...
```

Cuestións. Razoa as respostas:

7. Como poderiamos verificar que un ficheiro descargado é orixinal? Hashes? Sinatura electrónica? Magic number?

8. Como poderiamos verificar que un ficheiro descargado non posúe "contido oculto"? Hashes? Sinatura electrónica? Magic number?

Ricardo Feijoo Costa