INSA CVL
STI
2SU-5A
Sokhna Mai FALL

M.KAUFFMANN

TD1 : BINWALK

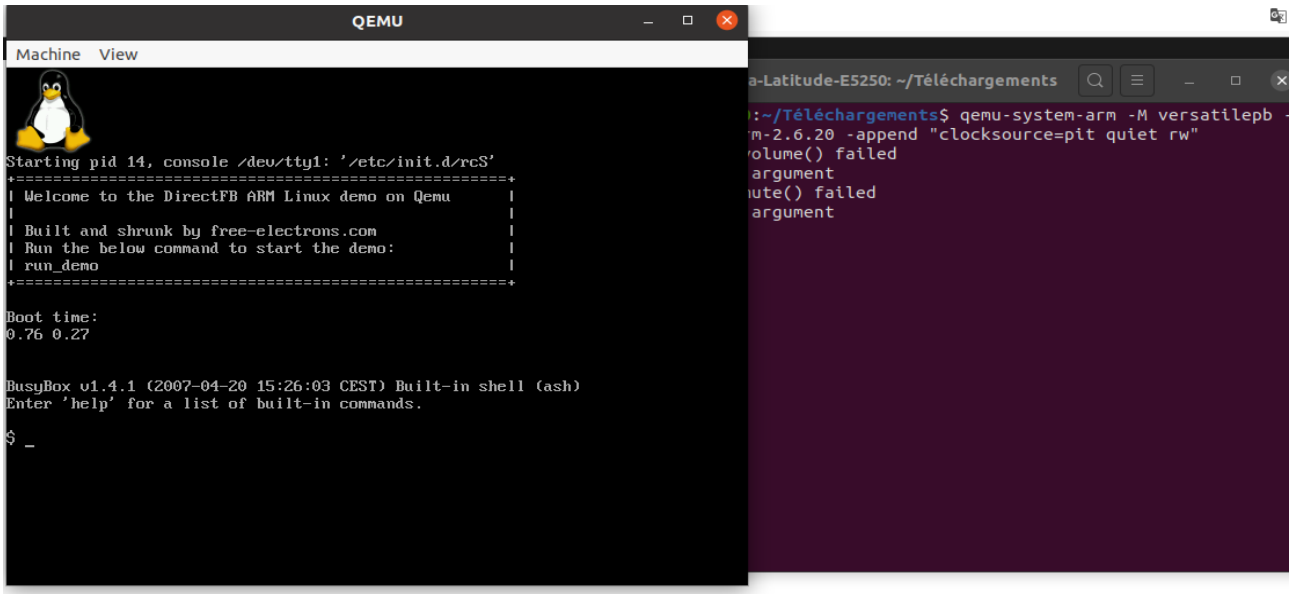
- Installation Binwalk

```
okhna@sokhna-Latitude-E5250:~/Téléchargements/beautifulsoup4-4.1.3$ sudo python
 setup.py install
unning install
unning build
unning build_py
reating build
reating build/lib
reating build/lib/bs4
opying bs4/__init__.py -> build/lib/bs4
opying bs4/testing.py -> build/lib/bs4
opying bs4/dammit.py -> build/lib/bs4
opying bs4/element.py -> build/lib/bs4
reating build/lib/bs4/builder
opying bs4/builder/__init__.py -> build/lib/bs4/builder
opying bs4/builder/_html5lib.py -> build/lib/bs4/builder
opying bs4/builder/_lxml.py -> build/lib/bs4/builder
opying bs4/builder/_htmlparser.py -> build/lib/bs4/builder
reating build/lib/bs4/tests
opying bs4/tests/test_builder_registry.py -> build/lib/bs4/tests
opying bs4/tests/__init__.py -> build/lib/bs4/tests
opying bs4/tests/test_soup.py -> build/lib/bs4/tests
opying bs4/tests/test_lxml.py -> build/lib/bs4/tests
opying bs4/tests/test_docs.py -> build/lib/bs4/tests
opying bs4/tests/test_htmlparser.py -> build/lib/bs4/tests
```

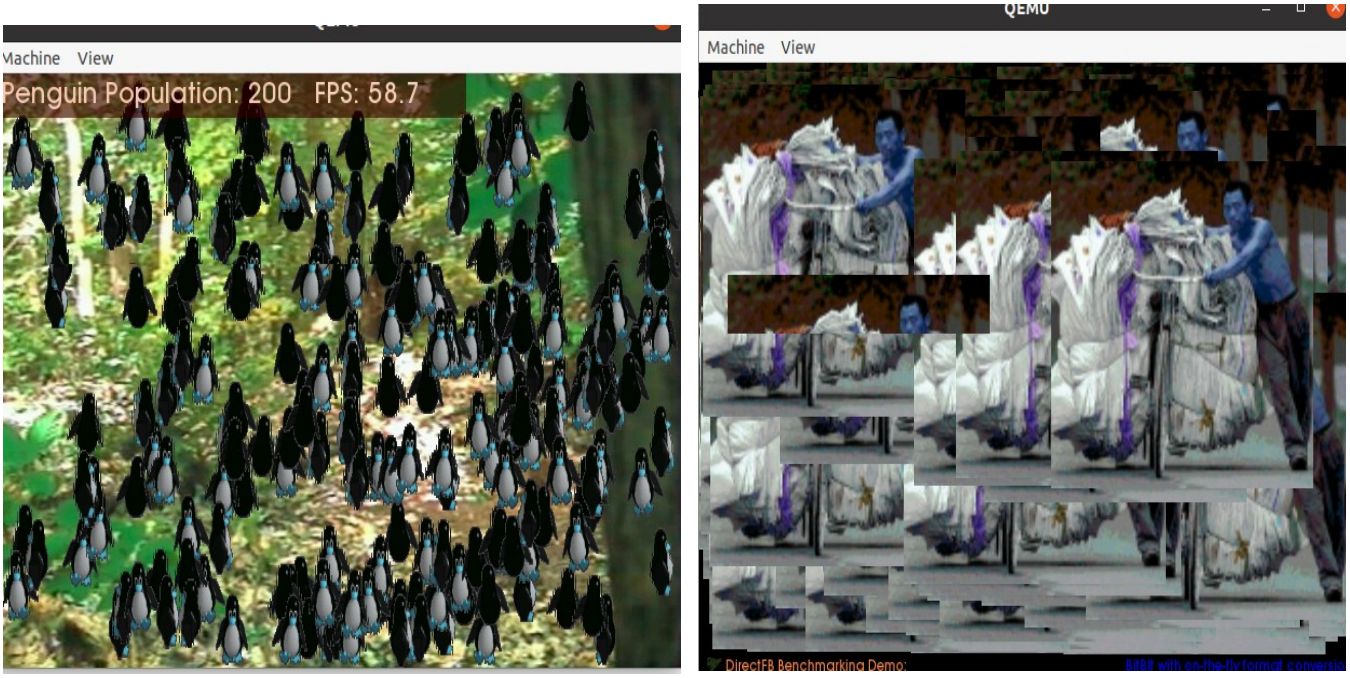
```
sokhna@sokhna-Latitude-E5250:~$ sudo apt install binwalk
[sudo] Mot de passe de sokhna :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  linux-headers-5.8.0-41-generic linux-hwe-5.8-headers-5.8.0-41
  linux-image-5.8.0-41-generic linux-modules-5.8.0-41-generic
  linux-modules-extra-5.8.0-41-generic
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  arj cramfsswap fonts-lyx freeglut3 javascript-common libafflib0v5 libblas3
  libdate-manip-perl libdouble-conversion3 libewf2 libgfortran5 libjs-jquery
  libjs-jquery-ui liblapack3 liblbfgsb0 libpcre2-16-0 libqt5core5a libqt5dbus5
  libqt5designer5 libqt5gui5 libqt5help5 libqt5network5 libqt5opengl5
  libqt5printsupport5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5
  libqt5widgets5 libqt5xml5 libtsk13 libxcb-xinerama0 libxcb-xinput0 mtd-utils
  ncompress p7zip p7zip-full python-matplotlib-data python3-binwalk
  python3-cycler python3-decorator python3-kiwisolver python3-matplotlib
  python3-numpy python3-opengl python3-pyparsing python3-pyqt5
  python3-pyqt5.qtopengl python3-pyqtgraph python3-scipy python3-sip
  python3-tk qt5-gtk-platformtheme qttranslations5-l10n sleuthkit
```

- Run the démo

Exécution :



Lancer le démo :



- Emplacement de l'image
  - Emplacement de tous les fichiers

```
sokhna@sokhna-Latitude-E5250:~/Téléchargements$ binwalk -C output_folder -M -e v
mlinuz-qemu-arm-2.6.20

Scan Time:     2022-02-03 21:51:49
Target File:   /home/sokhna/Téléchargements/vmlinuz-qemu-arm-2.6.20
MD5 Checksum:  5c8a1c2f291db79915eb2fb0eda1ebbe
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Linux kernel ARM boot executable zImage (little-en
dian)
12720         0x31B0          gzip compressed data, maximum compression, from Un
ix, last modified: 2007-05-09 06:03:48


Scan Time:     2022-02-03 21:51:49
Target File:   /home/sokhna/Téléchargements/output_folder/_vmlinuz-qemu-arm-2.6.
20.extracted/31B0
MD5 Checksum:  00f36d76c384709b0a6ca5cb93e25c0e
Signatures:    391

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```

- Emplacement de l’image (pingouin)

```
sokhna@sokhna-Latitude-E5250:~/Téléchargements$ binwalk -C output_folder -M -e
vmlinuz-qemu-arm-2.6.20 | grep tux
2984412       0x2D89DC        ASCII cpio archive (SVR4 with no CRC), file name:
 "/usr/local/share/directfb-examples/tux.png", file name length: "0x0000002B",
file size: "0x00006050"
sokhna@sokhna-Latitude-E5250:~/Téléchargements$
```

- Suppression du fichier
  - Avec binwalk

```
sokhna@sokhna-Latitude-E5250:~/Téléchargements$ binwalk -r /usr/local/share/di
rectfb-examples/tux.png vmlinuz-qemu-arm-2.6.20

General Error: Cannot open file /usr/local/share/directfb-examples/tux.png (CW
```

Remarque : On n’a pas le droit d’accéder de fichier.

- Avec dd

```
sokhna@sokhna-Latitude-E5250:~/Téléchargements$ dd of=vmlinuz-qemu-arm-2.6.20 bs=16384 seek=2984412 count=1 conv=notrunc
^C0+0 enregistrements lus
0+0 enregistrements écrits
0 octet copié, 340,618 s, 0,0 kB/s
```

- Test

Remarque :On remarque que la modification de notre fichier avec dd n'a pas fonctionné ce qui peut être du à des droits limités pour la modification des fichiers directs du système.

Questions :

- Trouvez et modifiez le pingouin. Qu'est ce qui empêche de modifier le pingouin directement?

Au niveau de la partie emplacement et suppression, on a trouvé et modifié (supprimé) l'image du pingouin.

Ce qui nous empêche de modifier le pingouin directement est qu'on n'a pas le droit de modifier le fichier.

•Qu'est ce que je peux faire pour contourner cette protection?

On peut contourner en modifiant la politique de sécurité de ce système avec AppArmor sur Ubuntu et Debian et Selinux sur Fedora ou Centos.

•Quelle propriété de sécurité est garantie?

Ici la propriété de sécurité garantie est l'intégrité car des limites ont été défini pour éviter la modification du système par n'importe qui.

Bonus: Quelle propriété de sécurité n'est pas garantie? Que peut on faire pour obtenir cette garantie?

Je dirai la confidentialité car on a accès à des images de systèmes qui devaient être secret.

On peut le résoudre en modifiant la politique de sécurité du système lui disant de ne pas donner accès aux fichiers du système.