Lab 7

Docker Containers for Malware Analysis

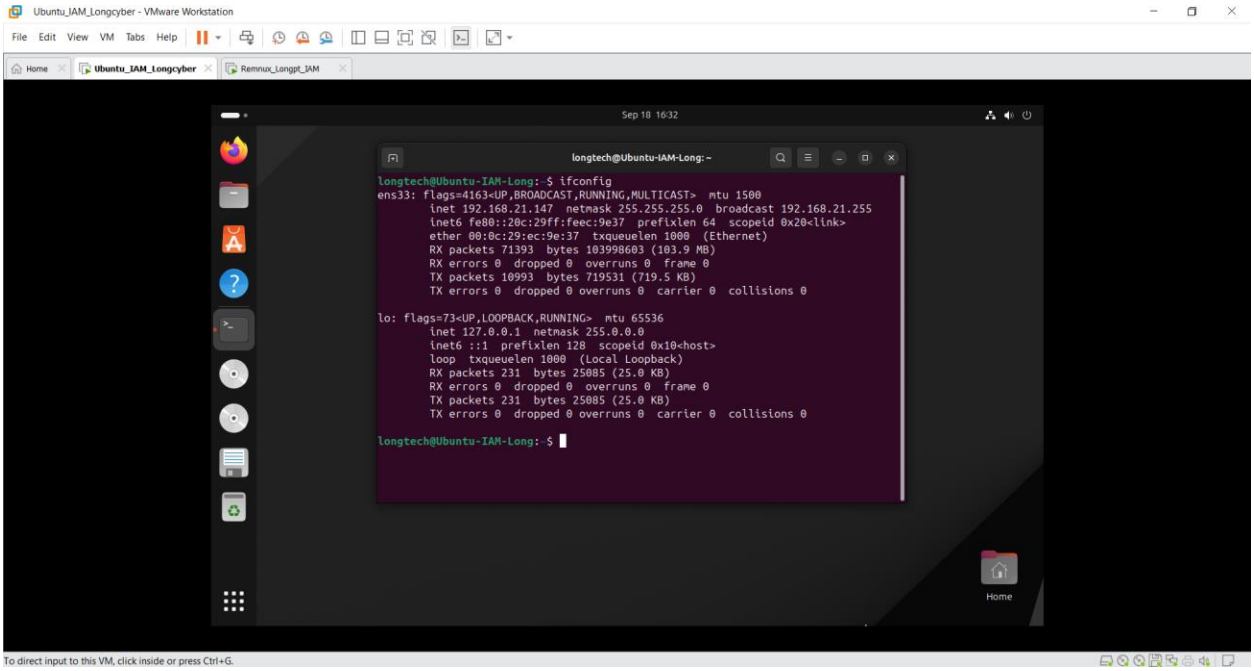
Course Name: IAM302

Student Name: Phạm Thành Long

Instructor Name: Mai Hoàng Đỉnh

Lab Due Date: 27/09/2024

ssh:



```
longtech@Ubuntu-IAM-Long:

Microsoft Windows [Version 10.0.22621.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 192.168.21.147

Pinging 192.168.21.147 with 32 bytes of data:
Reply from 192.168.21.147: bytes=32 time<1ms TTL=64
Reply from 192.168.21.147: bytes=32 time<1ms TTL=64
Reply from 192.168.21.147: bytes=32 time<1ms TTL=64
Reply from 192.168.21.147: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.21.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin>

C:\Users\admin>ssh longtech@192.168.21.147
longtech@192.168.21.147's password:
Welcome to Ubuntu 23.10 (GNU/Linux 6.5.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

0 updates can be applied immediately.

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

longtech@Ubuntu-IAM-Long:~$
```

```
longtech@Ubuntu-IAM-Long:

longtech@Ubuntu-IAM-Long:~$ sudo apt-get install docker.io
[sudo] password for longtech:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd git git-man liberror-perl pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools btrfs-progs cgroupfs-mount | cgroup-lite debootstrap docker-buildx docker-compose-v2 docker-doc rinse zfs-fuse | zfsutils
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  bridge-utils containerd docker.io git git-man liberror-perl pigz runc ubuntu-fan
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 79.5 MB of archives.
After this operation, 307 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu mantic/universe amd64 pigz amd64 2.6-1 [63.6 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu mantic/main amd64 bridge-utils amd64 1.7.1-1ubuntu1 [34.9 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu mantic-updates/main amd64 runc amd64 1.1.12-0ubuntu2~23.10.1 [8,343 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu mantic-updates/main amd64 containerd amd64 1.7.12-0ubuntu2~23.10.1 [37.6 MB]
Get:5 http://vn.archive.ubuntu.com/ubuntu mantic-updates/universe amd64 docker.io amd64 24.0.7-0ubuntu2~23.10.1 [28.8 MB]
Get:6 http://vn.archive.ubuntu.com/ubuntu mantic/main amd64 liberror-perl all 0.17029-2 [25.6 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu mantic-updates/main amd64 git-man all 1:2.40.1-1ubuntu1.1 [1,085 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu mantic-updates/main amd64 git amd64 1:2.40.1-1ubuntu1.1 [3,607 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu mantic/universe amd64 ubuntu-fan all 0.12.16 [35.2 kB]
Fetched 79.5 MB in 1min 17s (1,036 kB/s)
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 153210 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.6-1_amd64.deb ...
Unpacking pigz (2.6-1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.7.1-1ubuntu1_amd64.deb ...
Unpacking bridge-utils (1.7.1-1ubuntu1) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.1.12-0ubuntu2~23.10.1_amd64.deb ...
Unpacking runc (1.1.12-0ubuntu2~23.10.1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../3-containerd_1.7.12-0ubuntu2~23.10.1_amd64.deb ...
Unpacking containerd (1.7.12-0ubuntu2~23.10.1) ...
Selecting previously unselected package docker.io.
```

```
longtech@Ubuntu-IAM-Long:
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.7.1-1ubuntu1_amd64.deb ...
Unpacking bridge-utils (1.7.1-1ubuntu1) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.1.12-0ubuntu2~23.10.1_amd64.deb ...
Unpacking runc (1.1.12-0ubuntu2~23.10.1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../3-containerd_1.7.12-0ubuntu2~23.10.1_amd64.deb ...
Unpacking containerd (1.7.12-0ubuntu2~23.10.1) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../4-docker.io_24.0.7-0ubuntu2~23.10.1_amd64.deb ...
Unpacking docker.io (24.0.7-0ubuntu2~23.10.1) ...
Selecting previously unselected package liberror-perl.
Preparing to unpack .../5-liberror-perl_0.17029-2_all.deb ...
Unpacking liberror-perl (0.17029-2) ...
Selecting previously unselected package git-man.
Preparing to unpack .../6-git-man_1%3a2.40.1-1ubuntu1.1_all.deb ...
Unpacking git-man (1:2.40.1-1ubuntu1.1) ...
Selecting previously unselected package git.
Preparing to unpack .../7-git_1%3a2.40.1-1ubuntu1.1_amd64.deb ...
Unpacking git (1:2.40.1-1ubuntu1.1) ...
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../8-ubuntu-fan_0.12.16_all.deb ...
Unpacking ubuntu-fan (0.12.16) ...
Setting up runc (1.1.12-0ubuntu2~23.10.1) ...
Setting up liberror-perl (0.17029-2) ...
Setting up bridge-utils (1.7.1-1ubuntu1) ...
Setting up pigz (2.6-1) ...
Setting up git-man (1:2.40.1-1ubuntu1.1) ...
Setting up containerd (1.7.12-0ubuntu2~23.10.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.
Setting up ubuntu-fan (0.12.16) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ubuntu-fan.service → /lib/systemd/system/ubuntu-fan.service.
Setting up docker.io (24.0.7-0ubuntu2~23.10.1) ...
info: Selecting GID from range 100 to 999 ...
info: Adding group `docker' (GID 131) ...
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.
Setting up git (1:2.40.1-1ubuntu1.1) ...
Processing triggers for man-db (2.11.2-3) ...
longtech@Ubuntu-IAM-Long:~$
```

```
longtech@Ubuntu-IAM-Long:
longtech@Ubuntu-IAM-Long:~$ sudo docker run --rm -it ubuntu bash
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
dafa2b0c44d2: Pull complete
Digest: sha256:dfc10878be8d8fc9c61cbff33166cb1d1fe44391539243703c72766894fa834a
Status: Downloaded newer image for ubuntu:latest
root@1dd51a334917:/# hostname
1dd51a334917
root@1dd51a334917:/# exit
exit
longtech@Ubuntu-IAM-Long:~$
```

A Docker image of an app contains the software and its dependencies.

For example, you can easily launch the Thug honeyclient container. Docker automatically downloads the image.

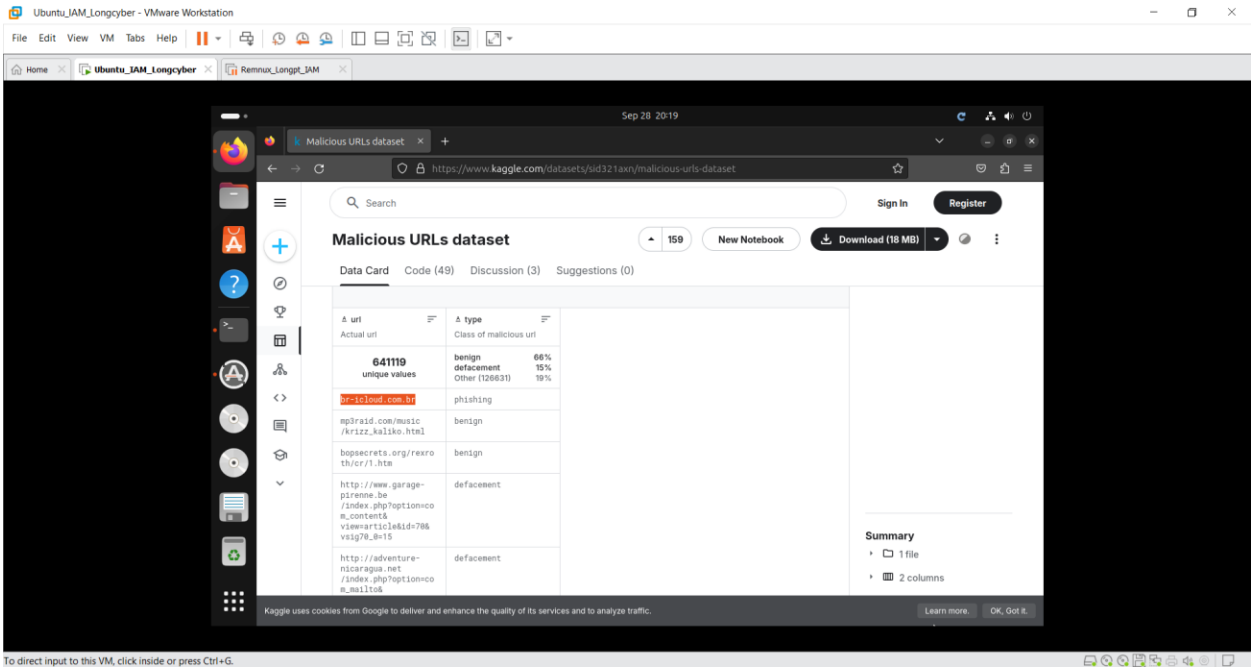
```
longtech@Ubuntu-IAM-Long:~$ sudo docker run --rm -it ubuntu bash
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
dafa2b0c44d2: Pull complete
Digest: sha256:dfc10878be8d8fc9c61cbff33166cb1d1fe44391539243703c72766894fa834a
Status: Downloaded newer image for ubuntu:latest
root@1dd51a334917:/# hostname
1dd51a334917
root@1dd51a334917:/# exit
exit
longtech@Ubuntu-IAM-Long:~$ sudo docker run --rm -it remnux/thug bash
[sudo] password for longtech:
Unable to find image 'remnux/thug:latest' locally
latest: Pulling from remnux/thug
3f701d9643d3: Pull complete
50597f06a896: Pull complete
5fea02d83833: Pull complete
4f4fb700ef54: Pull complete
d79e75a06114: Pull complete
4a7be60f63db: Pull complete
a27996c289d6: Pull complete
85ce5ebd4b5c: Pull complete
Digest: sha256:d1b96f9f40e01ef8c534476c1388ea2839fe8b6f253497de1e78af2eb86387d4
Status: Downloaded newer image for remnux/thug:latest
[2024-09-28 09:10:40] [window open redirection] about:blank -> http://bash
[2024-09-28 09:10:42] [HTTPSession] HTTPConnectionPool(host='bash', port=80): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.conne
ction.HTTPConnection object at 0x7d794f43dc60>: Failed to establish a new connection: [Errno -2] Name or service not known'))
longtech@Ubuntu-IAM-Long:~$
```

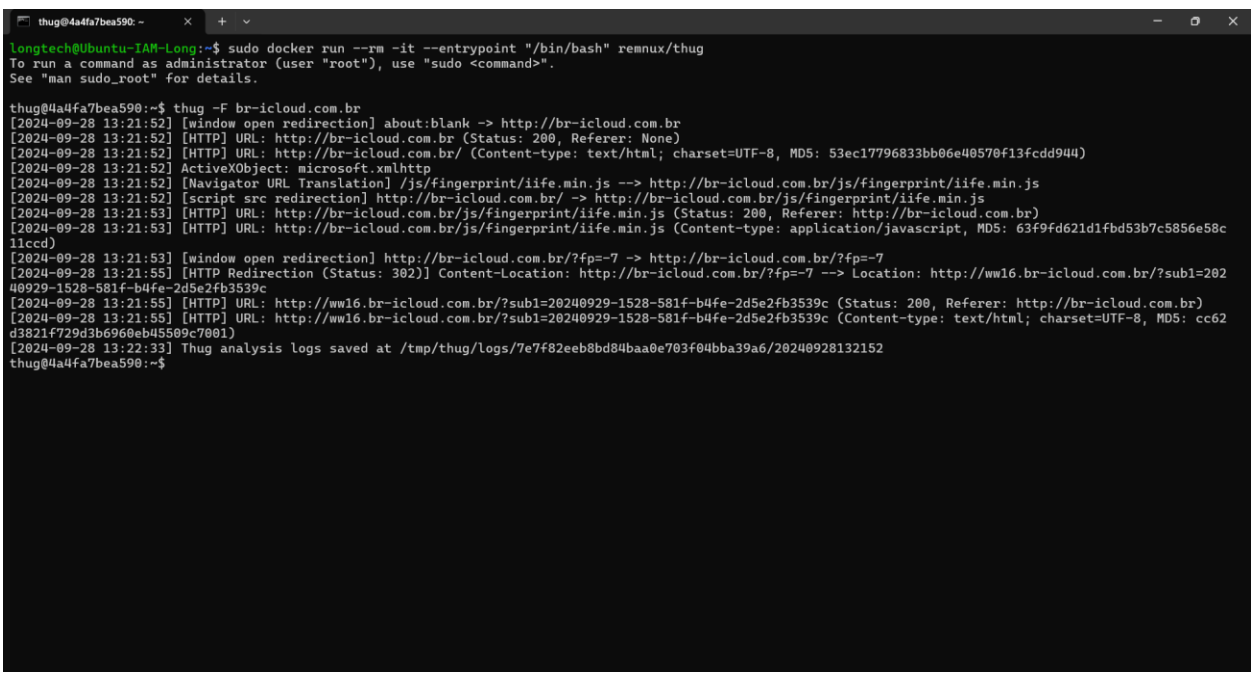
```
dafa2b0c44d2: Pull complete
Digest: sha256:dfc10878be8d8fc9c61cbff33166cb1d1fe44391539243703c72766894fa834a
Status: Downloaded newer image for ubuntu:latest
root@1dd51a334917:/# hostname
1dd51a334917
root@1dd51a334917:/# exit
exit
longtech@Ubuntu-IAM-Long:~$ sudo docker run --rm -it remnux/thug bash
[sudo] password for longtech:
Unable to find image 'remnux/thug:latest' locally
latest: Pulling from remnux/thug
3f701d9643d3: Pull complete
50597f06a896: Pull complete
5fea02d83833: Pull complete
4f4fb700ef54: Pull complete
d79e75a06114: Pull complete
4a7be60f63db: Pull complete
a27996c289d6: Pull complete
85ce5ebd4b5c: Pull complete
Digest: sha256:d1b96f9f40e01ef8c534476c1388ea2839fe8b6f253497de1e78af2eb86387d4
Status: Downloaded newer image for remnux/thug:latest
[2024-09-28 09:10:40] [window open redirection] about:blank -> http://bash
[2024-09-28 09:10:42] [HTTPSession] HTTPConnectionPool(host='bash', port=80): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.conne
ction.HTTPConnection object at 0x7d794f43dc60>: Failed to establish a new connection: [Errno -2] Name or service not known'))
longtech@Ubuntu-IAM-Long:~$ sudo docker run --rm -it --entrypoint "/bin/bash" remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@cf501efd8869:~$
```

A container gets its own file system, process listing and network stack.

However, containers share the OS kernel with each other and the underlying host.

thug -F <malicious URL>



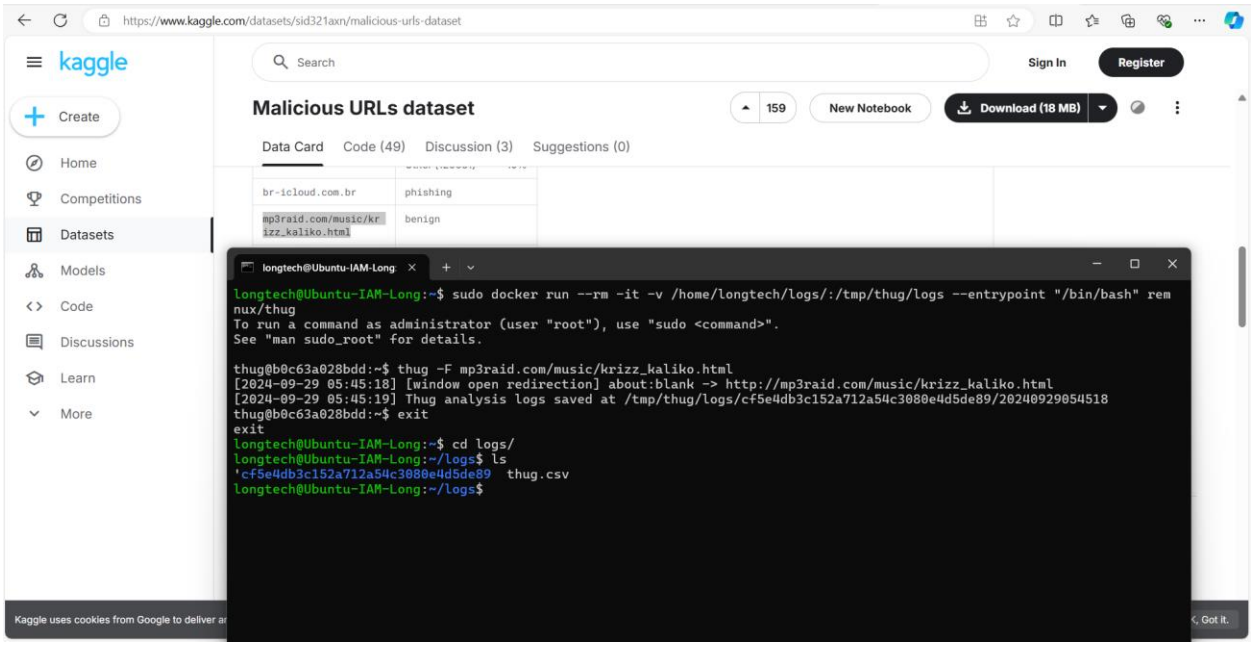


Use “-v” to map the host’s directory into the container.

First create the directory on the underlying host and make it world-accessible.

```
longtech@Ubuntu-IAM-Long:
thug@cf501efd8869:/$ exit
exit
longtech@Ubuntu-IAM-Long:~$ mkdir logs
longtech@Ubuntu-IAM-Long:~$ ls -l
total 17176
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Desktop
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Documents
drwxr-xr-x  5 longtech longtech     4096 Sep 16 17:08 Downloads
drwxrwxr-x  2 longtech longtech     4096 Sep 28 16:21 logs
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Music
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Pictures
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Public
drwxr-xr-x 18 longtech longtech     4096 Sep 16 16:32 Python-2.7.18
-rw-rw-r--  1 longtech longtech 17539408 Apr 20  2020 Python-2.7.18.tgz
drwx------  5 longtech longtech     4096 Sep 16 14:24 snap
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Templates
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Videos
longtech@Ubuntu-IAM-Long:~$ chmod a+xwr logs
longtech@Ubuntu-IAM-Long:~$ ls -l
total 17176
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Desktop
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Documents
drwxr-xr-x  5 longtech longtech     4096 Sep 16 17:08 Downloads
drwxrwxrwx  2 longtech longtech     4096 Sep 28 16:21 logs
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Music
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Pictures
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Public
drwxr-xr-x 18 longtech longtech     4096 Sep 16 16:32 Python-2.7.18
-rw-rw-r--  1 longtech longtech 17539408 Apr 20  2020 Python-2.7.18.tgz
drwx------  5 longtech longtech     4096 Sep 16 14:24 snap
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Templates
drwxr-xr-x  2 longtech longtech     4096 Sep 16 11:41 Videos
longtech@Ubuntu-IAM-Long:~$
```

sudo docker run --rm -it -v <local folder>:/home/thug/logs --entrypoint "/bin/bash" remnux/thug



The use of containers encourages separating “code” from “data”.

Store data on your underlying host while running apps in transient environments.

```
nonroot@c81949ee92d1: ~/w
longtech@Ubuntu-IAM-Long:~$ mkdir samples
longtech@Ubuntu-IAM-Long:~$ chmod a+xwr samples/
longtech@Ubuntu-IAM-Long:~$ cd samples/
longtech@Ubuntu-IAM-Long:~/samples$ wget -q https://zeltser.com/media/archive/gootkit.zip
longtech@Ubuntu-IAM-Long:~/samples$ ls
gootkit.zip
longtech@Ubuntu-IAM-Long:~/samples$ unzip gootkit.zip
Archive:  gootkit.zip
[gootkit.zip] about.txt password:
  inflating: about.txt
  inflating: agressive.exe
  inflating: grabber.exe
  inflating: gtk1.exe
  inflating: jhg26ff.sys
longtech@Ubuntu-IAM-Long:~/samples$ sudo docker run --rm -it -v /home/longtech/samples/:/home/nonroot/workdir remnux/viper bash
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

nonroot@c81949ee92d1:~/workdir$
```

Start viper by use ‘viper’ command. Then import all PE32 type files from the

../workdir directory into the Viper database:

store --folder ../workdir --file-type PE32

```
nonroot@c81949ee92d1: ~/w
nonroot@c81949ee92d1:~/workdir$ viper
        _
       (_)
  _  _ _ ____ _____ ____
 | | | | |  _ \| ___ |/ ___)
  \ V /| | | |_| | ____| |
   \_/ |_|  __/|_____)_| v2.0-rc11
        |_|

You have 0 files in your default repository.
You have 41 modules installed.
viper > store --folder ../workdir --file-type PE32
[+] Stored file "ritaglio_unpack.dll" to /home/nonroot/.viper/binaries/9/d/a/0/9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8
[*] Session opened on /home/nonroot/.viper/binaries/9/d/a/0/9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8
[*] Running command "yara scan -t"
[*] Scanning ritaglio_unpack.dll (9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8)
[*] Running command "triage"
[*] ritaglio_unpack.dll is a DLL
[+] Stored file "grabber.exe" to /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Running command "yara scan -t"
[*] Scanning grabber.exe (08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f)
[*] Running command "triage"
[+] Stored file "jhg26ff.sys" to /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Session opened on /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Running command "yara scan -t"
[*] Scanning jhg26ff.sys (20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05)
[*] Running command "triage"
[*] jhg26ff.sys is a Windows driver
[+] Stored file "agressive.exe" to /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Session opened on /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Running command "yara scan -t"
[*] Scanning agressive.exe (1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a)
[*] Running command "triage"
[+] Stored file "gtk1.exe" to /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Session opened on /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Running command "yara scan -t"
[*] Scanning gtk1.exe (e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787)
[*] Running command "triage"
viper >
```

When you run the ‘find all’ command, Viper will search and list all existing

malware samples in its database.

```
nonroot@c81949ee92d1: ~/w
You have 0 files in your default repository.
You have 41 modules installed.
viper > store --folder ../workdir --file-type PE32
[+] Stored file "ritaglio_unpack.dll" to /home/nonroot/.viper/binaries/9/d/a/0/9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8
[*] Session opened on /home/nonroot/.viper/binaries/9/d/a/0/9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8
[*] Running command "yara scan -t"
[*] Scanning ritaglio_unpack.dll (9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1af94de8bbb6667d8)
[*] Running command "triage"
[*] ritaglio_unpack.dll is a DLL
[+] Stored file "grabber.exe" to /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Running command "yara scan -t"
[*] Scanning grabber.exe (08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f)
[*] Running command "triage"
[+] Stored file "jhg26ff.sys" to /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Session opened on /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Running command "yara scan -t"
[*] Scanning jhg26ff.sys (20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05)
[*] Running command "triage"
[*] jhg26ff.sys is a Windows driver
[+] Stored file "agressive.exe" to /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Session opened on /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Running command "yara scan -t"
[*] Scanning agressive.exe (1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a)
[*] Running command "triage"
[+] Stored file "gtk1.exe" to /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Session opened on /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Running command "yara scan -t"
[*] Scanning gtk1.exe (e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787)
[*] Running command "triage"
viper > find all
+---+--------------------+-------------------------------------+--------------------------------+--------+
| # | Name               | Mime                                | MD5                            | Tags   |
+---+--------------------+-------------------------------------+--------------------------------+--------+
| 1 | ritaglio_unpack.dll | application/x-dosexec; charset=binary | ca438d4b536ef02ad0abe2860ff789c5 | dll    |
| 2 | grabber.exe        | application/x-dosexec; charset=binary | ca39d7cd301e61f0a01bda488af8f5fb |        |
| 3 | jhg26ff.sys        | application/x-dosexec; charset=binary | cd58eb1e49a088854b0d463d6b6a957b | driver |
| 4 | agressive.exe      | application/x-dosexec; charset=binary | 3315287968320a0dc4d045d3dae935b4 |        |
| 5 | gtk1.exe           | application/x-dosexec; charset=binary | 639819ee45daaa30e53d066938cb72ad |        |
+---+--------------------+-------------------------------------+--------------------------------+--------+
viper >
```

After that, we can open a session by the MD5 hashed value of the file and analysis on virustotal (this may requires the Private API key of Virustotal- which is received by login VirusTotal > Account > API Key)

open <hash of file> : open a file to analysis

virustotal : analysis by using VirusTotal

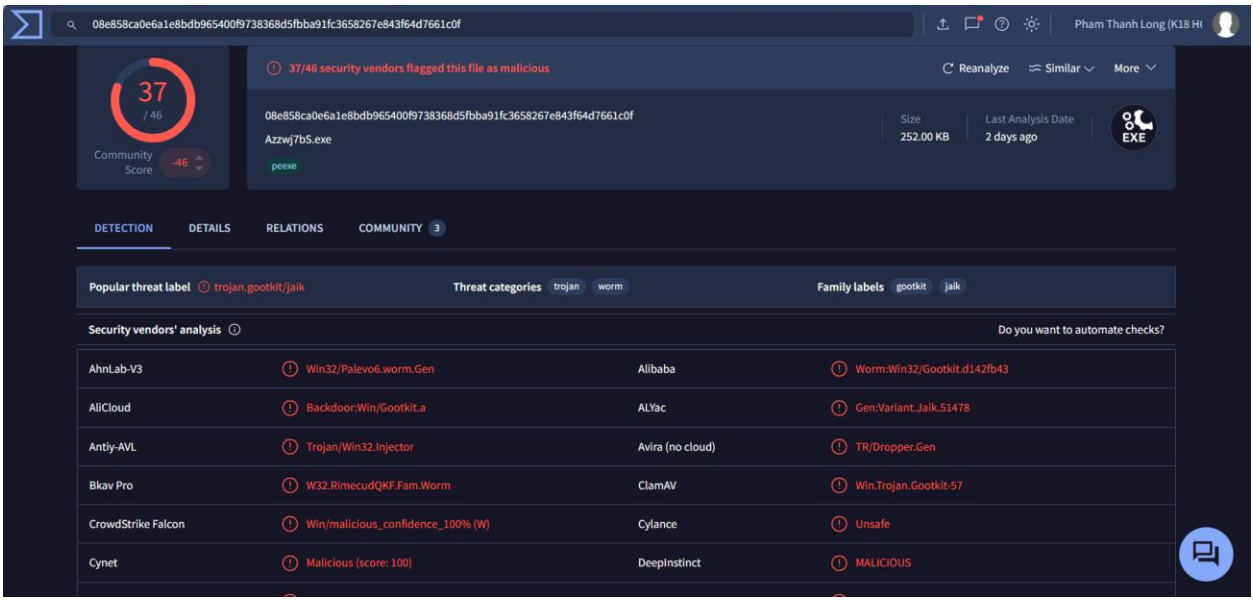
```
nonroot@127062b14644: ~/w
[+] Stored file "grabber.exe" to /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
[*] Running command "yara scan -t"
[*] Scanning grabber.exe (08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f)
[*] Running command "triage"
[+] Stored file "jhg26ff.sys" to /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Session opened on /home/nonroot/.viper/binaries/2/0/7/8/20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05
[*] Running command "yara scan -t"
[*] Scanning jhg26ff.sys (20789eadfd97e38238579419e05a42ffdb55ec71c3966303a3e4858048a30f05)
[*] Running command "triage"
[*] jhg26ff.sys is a Windows driver
[+] Stored file "agressive.exe" to /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Session opened on /home/nonroot/.viper/binaries/1/2/6/8/1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a
[*] Running command "yara scan -t"
[*] Scanning agressive.exe (1268d1f0b4fcdeb8953b1d3e7e9b4350660e442ca24f56ee5d2bc1a2e9e3741a)
[*] Running command "triage"
[+] Stored file "gtk1.exe" to /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Session opened on /home/nonroot/.viper/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787
[*] Running command "yara scan -t"
[*] Scanning gtk1.exe (e8fcd05758a8e1a4bf945f4913e10557b80120f25e329f06d8642017dd353787)
[*] Running command "triage"
viper > find all
+---+--------------------+-------------------------------------+--------------------------------+--------+
| # | Name               | Mime                                | MD5                            | Tags   |
+---+--------------------+-------------------------------------+--------------------------------+--------+
| 1 | ritaglio_unpack.dll | application/x-dosexec; charset=binary | ca438d4b536ef02ad0abe2860ff789c5 | dll    |
| 2 | grabber.exe        | application/x-dosexec; charset=binary | ca39d7cd301e61f0a01bda488af8f5fb |        |
| 3 | jhg26ff.sys        | application/x-dosexec; charset=binary | cd58eb1e49a088854b0d463d6b6a957b | driver |
| 4 | agressive.exe      | application/x-dosexec; charset=binary | 3315287968320a0dc4d045d3dae935b4 |        |
| 5 | gtk1.exe           | application/x-dosexec; charset=binary | 639819ee45daaa30e53d066938cb72ad |        |
+---+--------------------+-------------------------------------+--------------------------------+--------+
viper > open ca39d7cd301e61f0a01bda488af8f5fb
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
viper grabber.exe > virustotal
[!] You tried to perform calls to functions for which you require a Private API key.
viper grabber.exe >
```

```
nonroot@c81949ee92d1: ~/w
+---+--------------------+-----------------------------------+-------------------------------+--------+
viper > open ca39d7cd301e61f0a01bda488af8f5fb
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
viper grabber.exe > virustotal
[!] You tried to perform calls to functions for which you require a Private API key.
viper grabber.exe > about
+---------------+-----------------------------------------------+
| About         |                                               |
+---------------+-----------------------------------------------+
| Viper Version | 2.0-rc11                                      |
| Python Version | 3.8.10                                       |
| Homepage      | https://viper.li                              |
| Issue Tracker | https://github.com/viper-framework/viper/issues |
+---------------+-----------------------------------------------+
+-------------------+--------------------------------------+
| Configuration     |                                      |
+-------------------+--------------------------------------+
| Configuration File | /home/nonroot/.viper/viper.conf      |
| Active Project    | default                              |
| Storage Path      | /home/nonroot/.viper                 |
| Module Path       | /home/nonroot/.viper/modules         |
| Database Path     | sqlite:////home/nonroot/.viper/viper.db |
+-------------------+--------------------------------------+
viper grabber.exe > exit
nonroot@c81949ee92d1:~/workdir$ nano /home/nonroot/.viper/viper.conf
bash: nano: command not found
nonroot@c81949ee92d1:~/workdir$ sudo apt update
[sudo] password for nonroot:
Get:1 http://archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [4036 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [177 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/restricted amd64 Packages [33.4 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 Packages [1275 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [11.3 MB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [30.9 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [4024 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [33.5 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1560 kB]
```

```
nonroot@c81949ee92d1: ~/w
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [4024 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [33.5 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1560 kB]
Get:14 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [4188 kB]
Get:15 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [4488 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [1273 kB]
Get:17 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [55.2 kB]
Get:18 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [28.6 kB]
Fetched 33.2 MB in 6s (5531 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
161 packages can be upgraded. Run 'apt list --upgradable' to see them.
nonroot@c81949ee92d1:~/workdir$ sudo apt install nano
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  hunspell
The following NEW packages will be installed:
  nano
0 upgraded, 1 newly installed, 0 to remove and 161 not upgraded.
Need to get 269 kB of archives.
After this operation, 868 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 nano amd64 4.8-1ubuntu1 [269 kB]
Fetched 269 kB in 2s (151 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package nano.
(Reading database ... 20163 files and directories currently installed.)
Preparing to unpack .../nano_4.8-1ubuntu1_amd64.deb ...
Unpacking nano (4.8-1ubuntu1) ...
Setting up nano (4.8-1ubuntu1) ...
update-alternatives: using /bin/nano to provide /usr/bin/editor (editor) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/editor.1.gz because associated file /usr/share/man/man1/nano.1.gz (of link group editor)
doesn't exist
update-alternatives: using /bin/nano to provide /usr/bin/pico (pico) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/pico.1.gz because associated file /usr/share/man/man1/nano.1.gz (of link group pico) does
n't exist
nonroot@c81949ee92d1:~/workdir$
```

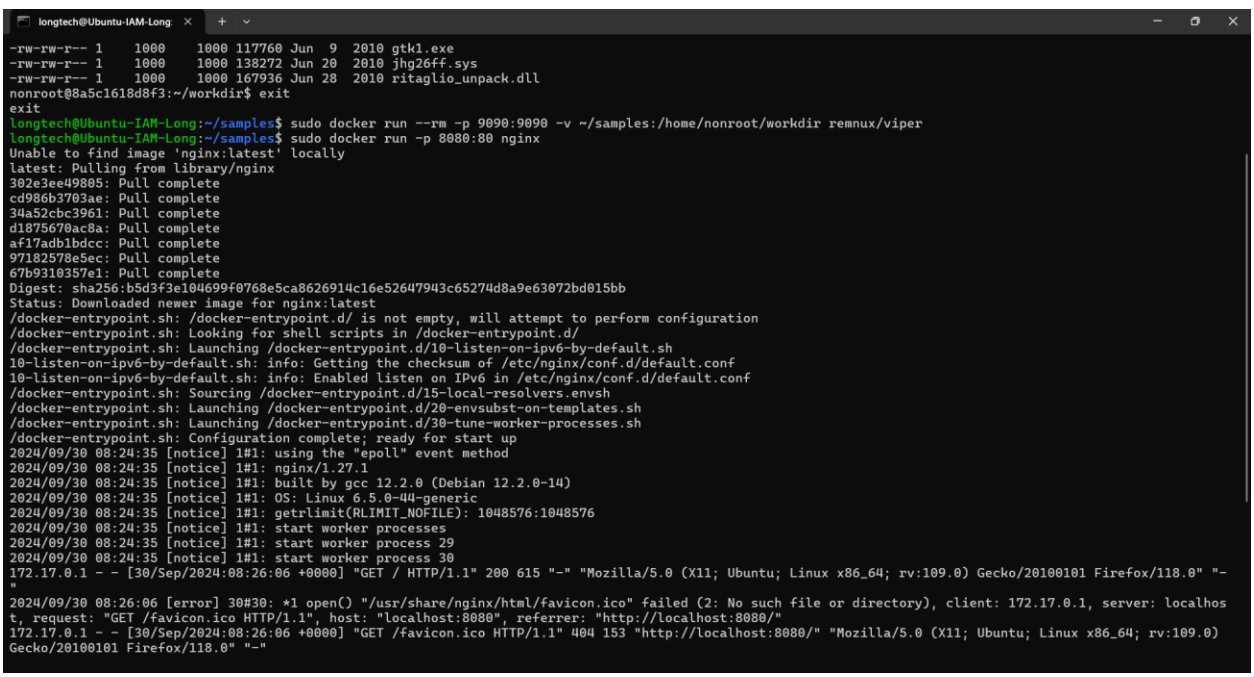
```
nonroot@c81949ee92d1: ~/w
  GNU nano 4.8                    /home/nonroot/.viper/viper.conf                    Modified

[autorun]
enabled = True

# Verbose True will print the output of each command.
# False will tell you a command has been run but not display the output
verbose = False

# Enter a comma separated list of command lines, As you would enter them in the CLI. You can use ; to chain commands.
# Commands are run in sequence and the output of MODULES is stored if store_output is set to True.
# commands = yara scan -t, fuzzy, pe compiletime
commands = yara scan -t, triage


##
# Modules
##

[virustotal]
virustotal_has_private_key = False
virustotal_has_intel_key = False
virustotal_key = 97678962701d38ac431d8b7724028e42ca11a884f7093a6fe404aadae18887c6

[cuckoo]
cuckoo_modified = False
cuckoo_host = http://localhost:8090
cuckoo_web = http://localhost:8000
auth_token =

[joesandbox]
apiurl = https://jbxcloud.joesecurity.org/api
#apiurl = http://localhost/joesandbox/api
apikey =
# https://jbxcloud.joesecurity.org/download/termsandconditions.pdf (Cloud only)
accept_tac = False

# Submission parameters, refer to the API documentation for a description.

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was
```

```
nonroot@c81949ee92d1: ~/w
(Reading database ... 20163 files and directories currently installed.)
Preparing to unpack .../nano_4.8-1ubuntu1_amd64.deb ...
Unpacking nano (4.8-1ubuntu1) ...
Setting up nano (4.8-1ubuntu1) ...
update-alternatives: using /bin/nano to provide /usr/bin/editor (editor) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/editor.1.gz because associated file /usr/share/man/man1/nano.1.gz (of link group editor)
doesn't exist
update-alternatives: using /bin/nano to provide /usr/bin/pico (pico) in auto mode
update-alternatives: warning: skip creation of /usr/share/man/man1/pico.1.gz because associated file /usr/share/man/man1/nano.1.gz (of link group pico) does
n't exist
nonroot@c81949ee92d1:~/workdir$ nano /home/nonroot/.viper/viper.conf
nonroot@c81949ee92d1:~/workdir$ nano /home/nonroot/.viper/viper.conf
nonroot@c81949ee92d1:~/workdir$ viper

        _
       (_)
  _  _ _ ____ _____ ____
 | | | | |  _ \| ___ |/ ___)
  \ V /| | |_| | ____| |
   \_/ |_|  __/|_____)_| v2.0-rc11
         |_|

You have 5 files in your default repository.
You have 41 modules installed.
viper > find all
+---+--------------------+-----------------------------------+--------------------------------+--------+
| # | Name               | Mime                              | MD5                            | Tags   |
+---+--------------------+-----------------------------------+--------------------------------+--------+
| 1 | ritaglio_unpack.dll | application/x-dosexec; charset=binary | ca438d4b536ef02ad0abe2860ff789c5 | dll    |
| 2 | grabber.exe        | application/x-dosexec; charset=binary | ca39d7cd301e61f0a01bda488af8f5fb |        |
| 3 | jhg26ff.sys        | application/x-dosexec; charset=binary | cd58eb1e49a088854b0d463d6b6a957b | driver |
| 4 | agressive.exe      | application/x-dosexec; charset=binary | 3315287968320a0dc4d045d3dae935b4 |        |
| 5 | gtk1.exe           | application/x-dosexec; charset=binary | 639819ee45daaa30e53d066938cb72ad |        |
+---+--------------------+-----------------------------------+--------------------------------+--------+
viper > open ca39d7cd301e61f0a01bda488af8f5fb
[*] Session opened on /home/nonroot/.viper/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f
viper grabber.exe > virustotal
[*] 37 out of 46 antivirus detected ca39d7cd301e61f0a01bda488af8f5fb as malicious.
[*] https://www.virustotal.com/gui/file/08e858ca0e6a1e8bdb965400f9738368d5fbba91fc3658267e843f64d7661c0f/detection/f-08e858ca0e6a1e8bdb965400f9738368d5fbba9
1fc3658267e843f64d7661c0f-1727432999

viper grabber.exe >
```

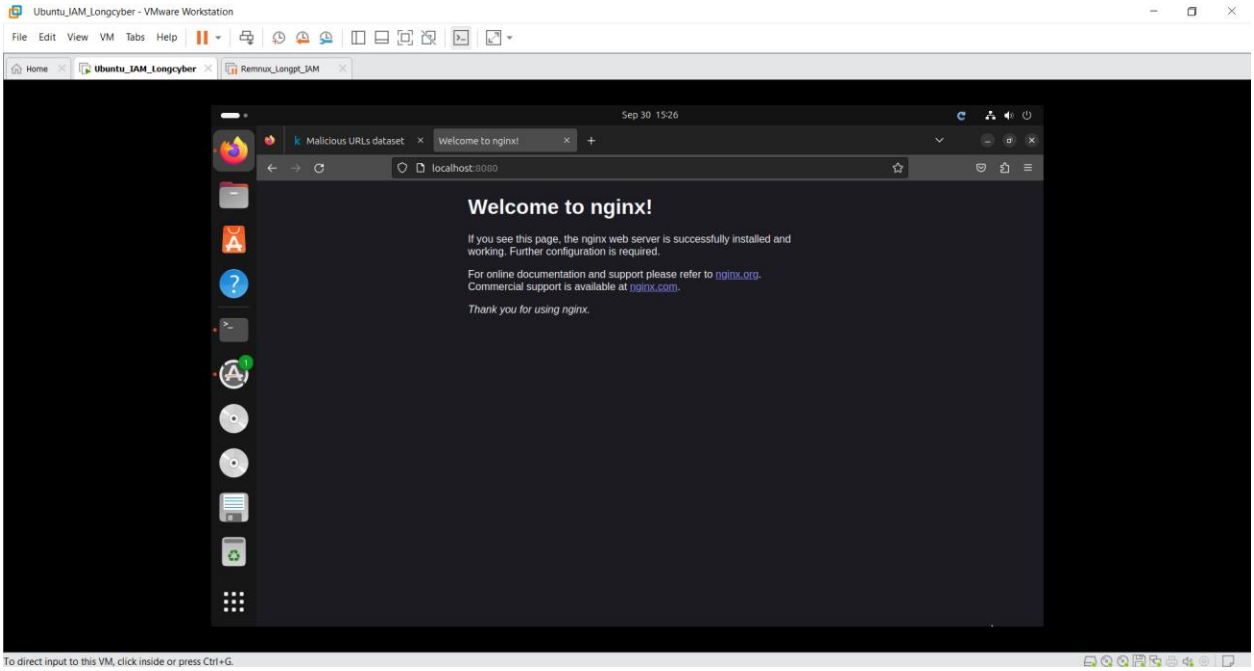


Use “-p” to access network ports within a container.

Expose map port 8080 on the Docker host to TCP port 80 in the container.

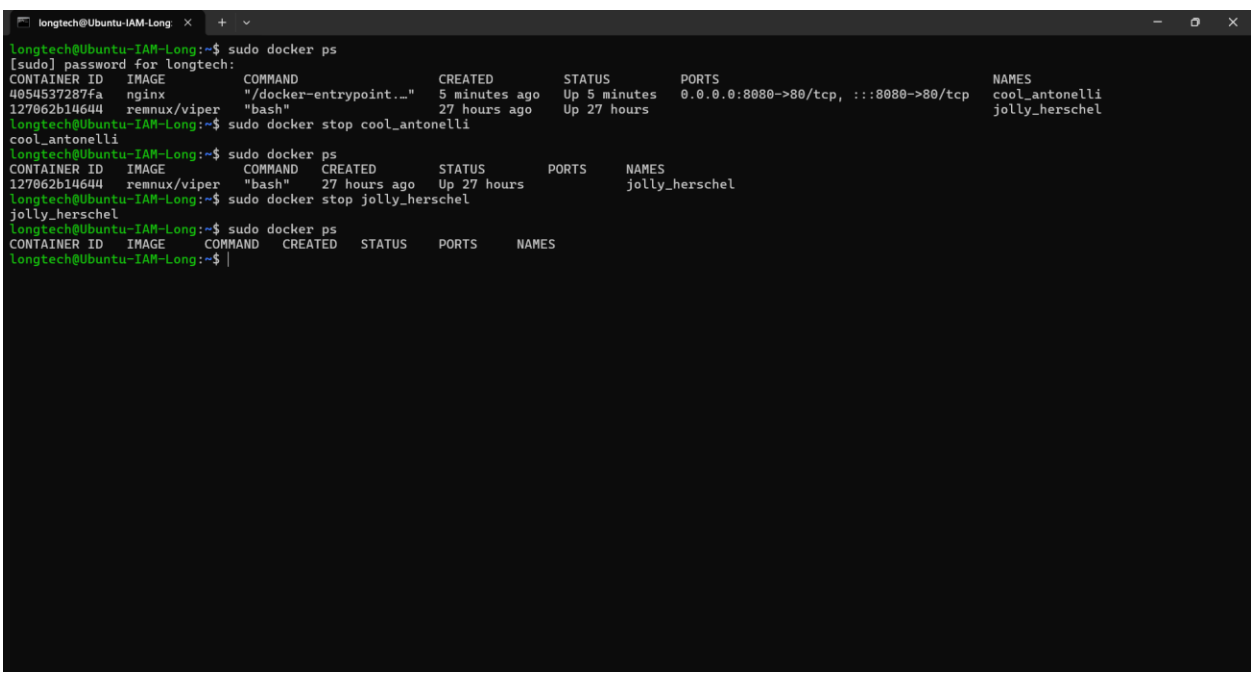


```
longtech@Ubuntu-IAM-Long
-rw-rw-r-- 1    1000    1000 117760 Jun  9  2010 gtk1.exe
-rw-rw-r-- 1    1000    1000 138272 Jun 20  2010 jhg26ff.sys
-rw-rw-r-- 1    1000    1000 167936 Jun 28  2010 ritaglio_unpack.dll
nonroot@8a5c1618d8f3:~/workdir$ exit
exit
longtech@Ubuntu-IAM-Long:~/samples$ sudo docker run --rm -p 9090:9090 -v ~/samples:/home/nonroot/workdir remnux/viper
longtech@Ubuntu-IAM-Long:~/samples$ sudo docker run -p 8080:80 nginx
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
302e3ee49805: Pull complete
cd986b3703ae: Pull complete
34a52cbc3961: Pull complete
d1875670ac8a: Pull complete
af17adb1bdcc: Pull complete
97182578e5ec: Pull complete
67b9310357e1: Pull complete
Digest: sha256:b5d3f3e104699f0768e5ca8626914c16e52647943c65274d8a9e63072bd015bb
Status: Downloaded newer image for nginx:latest
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
/docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Configuration complete; ready for start up
2024/09/30 08:24:35 [notice] 1#1: using the "epoll" event method
2024/09/30 08:24:35 [notice] 1#1: nginx/1.27.1
2024/09/30 08:24:35 [notice] 1#1: built by gcc 12.2.0 (Debian 12.2.0-14)
2024/09/30 08:24:35 [notice] 1#1: OS: Linux 6.5.0-44-generic
2024/09/30 08:24:35 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2024/09/30 08:24:35 [notice] 1#1: start worker processes
2024/09/30 08:24:35 [notice] 1#1: start worker process 29
2024/09/30 08:24:35 [notice] 1#1: start worker process 30
172.17.0.1 - - [30/Sep/2024:08:26:06 +0000] "GET / HTTP/1.1" 200 615 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0" "-
"
2024/09/30 08:26:06 [error] 30#30: *1 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such file or directory), client: 172.17.0.1, server: localhos
t, request: "GET /favicon.ico HTTP/1.1", host: "localhost:8080", referrer: "http://localhost:8080/"
172.17.0.1 - - [30/Sep/2024:08:26:06 +0000] "GET /favicon.ico HTTP/1.1" 404 153 "http://localhost:8080/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/118.0" "-"
```



Use “ps” to show running containers and “stop” to stop them.

You can refer to the container using its ID or its easier-to-type name.



Docker automatically removes this container after it is stopped, because we launched it with the “--rm” parameter.

Building and Your Own Docker Images

Create image

A Dockerfile contains instructions for building a new Docker image.

- Use an existing image as a starting point.
- Document instructions for downloading, compiling and configuring the application.
- Commands must work without user interaction.
- Look at other Dockerfiles to start learning.
- Test commands manually by running them in

```
sudo docker run --rm -it ubuntu:22.04 bash
```

Create an image:

```
longtech@Ubuntu-IAM-Long:~$ mkdir docker-images
longtech@Ubuntu-IAM-Long:~$ ls
Desktop  docker-images  Documents  Downloads  snap  Music  Pictures  Public  Python-2.7.18  Python-2.7.18.tgz  snap  snap  Templates  Videos
longtech@Ubuntu-IAM-Long:~$ cd docker-images/
longtech@Ubuntu-IAM-Long:~/docker-images$ nano my-image
longtech@Ubuntu-IAM-Long:~/docker-images$
```

Docker images in the REMnux collection start from ubuntu:22.04.

Start with “apt-get update”, then install only the packages required by the software.

```
  GNU nano 7.2                                   my-image *
FROM ubuntu:22.04

MAINTAINER longtech

USER root
RUN apt-get update && \
    apt-get install -y --no-install-recommends \
        python2.7 \
        python2.7-dev \
        curl \
        ssdeep \
        python-pip \
    && rm -rf /var/lib/apt/lists/*

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Docker stacks read-only file system images to form an image.

A union mount allows multiple file systems to be mounted and appear as a single file system.

Balance efficiency and readability when crafting the Dockerfile.

Chain commands into a single RUN instruction to remove files before a layer is committed.

```
longtech@Ubuntu-IAM-Long:
  GNU nano 7.2                                                my-image *
FROM ubuntu:22.04

MAINTAINER longtech

USER root
RUN apt-get update && \
    apt-get install -y --no-install-recommends \
        python2.7 \
        python2.7-dev \
        curl \
        ssdeep \
        python-pip \
    && rm -rf /var/lib/apt/lists/*

RUN pip install -q jsbeautifier \
    rarfile \
    beautifulsoup4 \
    pefile \
    six \
    html5lib

RUN groupadd -r thug && \
    useradd -r -g thug -d /home/thug -s /sbin/nologin -c "Thug User" thug

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Avoid saving files to the file system to help minimize disk space.

Don’t bother removing files after the layer has been already committed (e.g., “apt-get clean”).

Don’t run commands as “root” unless you really need to.

- That’s why we created user “thug”.
- Use “USER” to specify which user account to use for subsequent commands.
- Understand “ENV”, “WORKDIR” and “CMD” Dockerfile directives.

```
longtech@Ubuntu-IAM-Long:
  GNU nano 7.2                                                my-image *
FROM ubuntu:22.04

MAINTAINER longtech

USER root
RUN apt-get update && \
    apt-get install -y --no-install-recommends \
        python2.7 \
        python2.7-dev \
        curl \
        ssdeep \
        python-pip \
    && rm -rf /var/lib/apt/lists/*

RUN pip install -q jsbeautifier \
    rarfile \
    beautifulsoup4 \
    pefile \
    six \
    html5lib

RUN groupadd -r thug && \
    useradd -r -g thug -d /home/thug -s /sbin/nologin -c "Thug User" thug

USER thug
ENV HOME /home/thug
ENV USER thug
WORKDIR /home/thug/src

COPY ./thug/py /home/thug/src/

CMD ["python", "./thug/py"]

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

ENV HOME /home/thug: Set the HOME environment variable to /home/thug.

ENV USER thug: Similar to above, set the USER environment variable to thug. It simply sets the USER environment variable that processes can use to determine the default user.

WORKDIR /home/thug/src: Sets the default working directory inside the container.

CMD ["./thug.py"]: Specifies the default command to be executed when the container starts, which will execute the file thug.py located in the current working directory (set to /home/thug /src by WORKDIR).

Build image

Use “docker build” to build the image out of the Dockerfile.

-t=my-image:latest: set my-image as the name of the image and latest as the tag of the image.

-f my-image: specify my-image as the name of the Dockerfile.