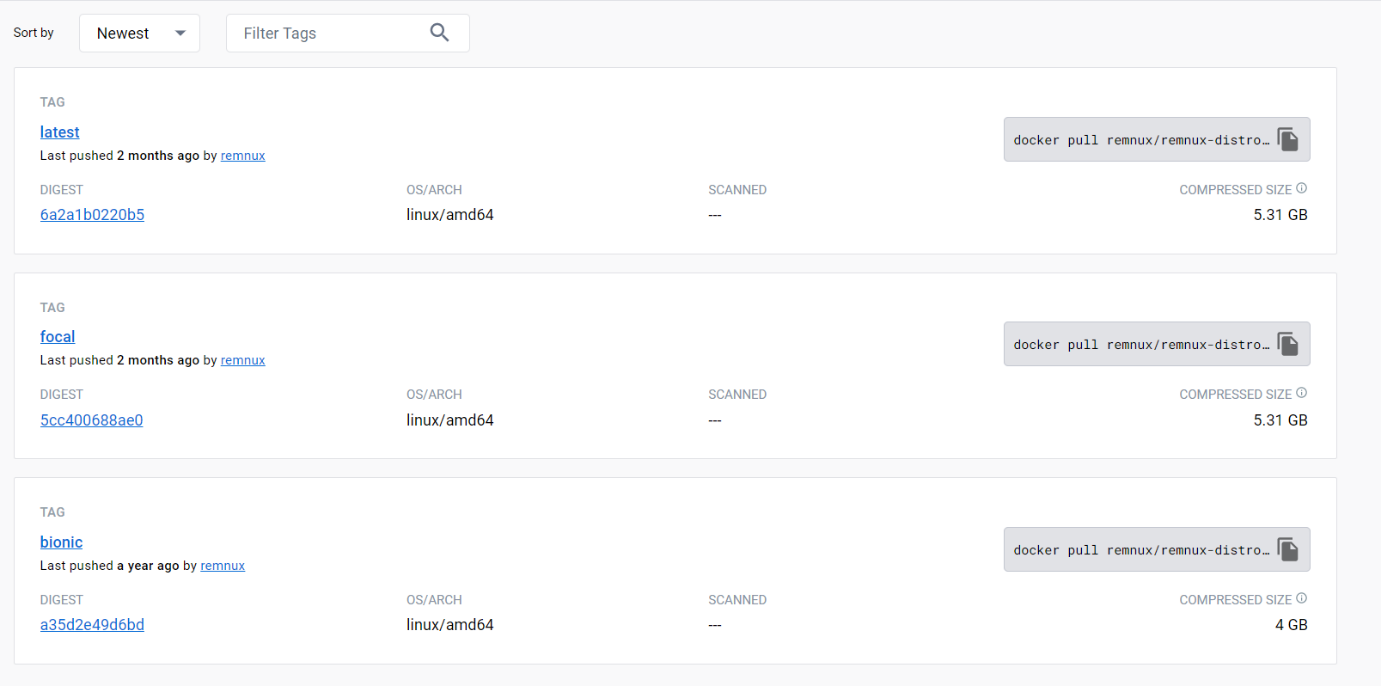
VNCER

TÌM HIỂU REMNUX

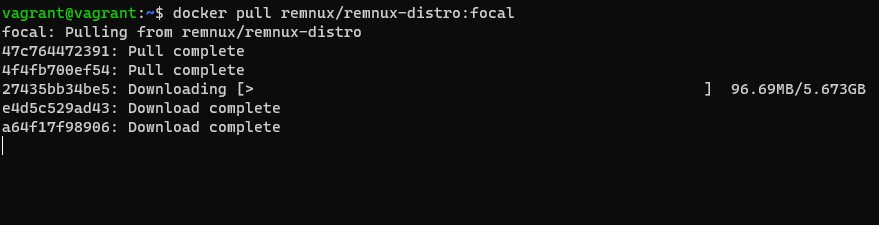
# Image All IN ONE

Đường dẫn: https://hub.docker.com/r/remnux/remnux-distro/tags



Hình 1 Docker Hub kho lưu trữ của Remnux

Tải phiên bản ubuntu20 (focal)



Hình 2 Quá trình pull remnux

“docker run --rm -it -u remnux remnux/remnux-distro:focal bash”

“docker run” là lệnh dùng để khởi chạy một container trong Docker.

“—rm” là tùy chọn để yêu cầu Docker xóa container sau khi container đã dừng.

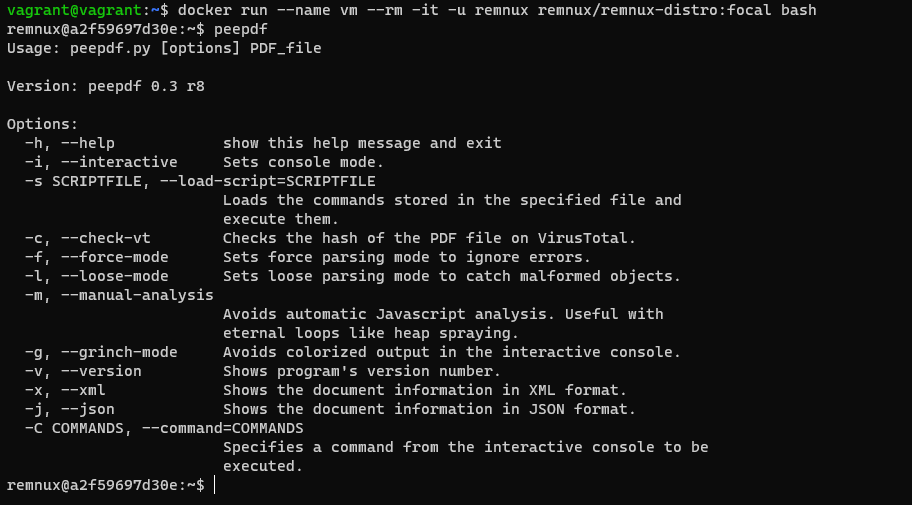
“-it” được sử dụng để kết nối container với terminal của host, cho phép người dùng tương tác với container thông qua terminal.

“-u remnux” được sử dụng để chạy container với user là "remnux".

“remnux/remnux-distro:focal” là image được sử dụng để khởi chạy container, trong trường hợp này là image "remnux-distro" phiên bản "focal" được phát triển bởi Remnux Project.

“bash” là lệnh được chạy bên trong container sau khi container được khởi chạy.

Vì vậy, khi chạy lệnh “docker run --rm -it -u remnux remnux/remnux-distro:focal bash”, Docker sẽ khởi chạy một container với user "remnux" và kết nối container với terminal của host, sử dụng image "remnux-distro" phiên bản "focal". Sau đó, container sẽ thực hiện lệnh "bash" để cho phép người dùng tương tác với container thông qua terminal. Sau khi lệnh "bash" hoàn thành, container sẽ bị xóa do tùy chọn "--rm".



Hình 3 Kết quả khi docker thực thi image thành công

# Image Bổ Sung

## Thug

Là một honeyclient tương tác thấp để kiểm tra các trang web đáng ngờ là một honeyclient tương tác thấp để kiểm tra các trang web đáng ngờ

A black screen with white text

Description automatically generated with low confidence

Hình 4 Cài đặt Thug

## Binary Refinery

Là tập hợp các tập lệnh Python thực hiện các phép biến đổi dữ liệu nhị phân như nén và mã hóa. Bạn có thể xâu chuỗi các công cụ khi cần thiết để đạt được mục tiêu của mình

A screen shot of a computer

Description automatically generated with medium confidence

Hình 5 Cài đặt Binary Refinery

## JSDetox

Là một công cụ dựa trên trình duyệt để phân tích và giải mã JavaScriptà một công cụ dựa trên trình duyệt để phân tích và giải mã JavaScript

A picture containing text, screenshot, font

Description automatically generated

Hình 6 Cài đặt JSDetox

Kết quả sau khi được cài đặt.

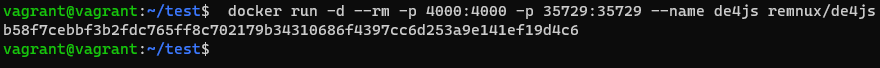
A screenshot of a computer

Description automatically generated

Hình 7 Phân tích một đoạn mã script

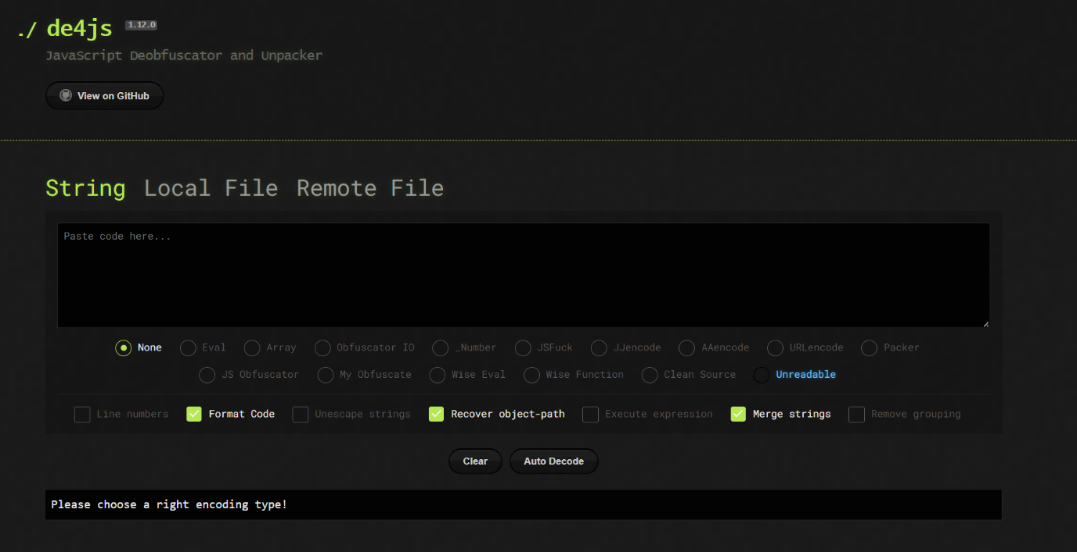
## De4js

Là một công cụ dựa trên trình duyệt để gỡ rối mã nguồn và giải nén JavaScript



Hình 8 Docker thực hiện chạy image de4js

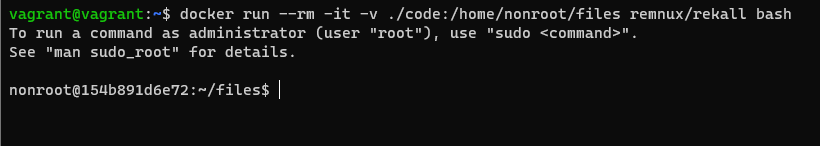
Kết quả thực thi đoạn code trong ảnh trên:



Hình 9 Giao diện website của de4js

## Rekall

Là một bộ công cụ để trích xuất các tạo phẩm kỹ thuật số từ bộ nhớ và các khía cạnh khác của hệ thống khi thực hiện ứng phó sự cố.



Hình 10 Cài đặt Rekall

## RetDec

Là trình dịch ngược hỗ trợ nhiều định dạng tệp khác nhau, bao gồm PE và ELF cũng như một số kiến ​​trúc 32 và 64 bit.

A computer screen with white text

Description automatically generated with low confidence

Hình 11 Docker cài đặt RetDec

## Rizin

Là một framework kỹ thuật đảo ngược bao gồm khả năng phân tách và phân tích cho nhiều định dạng và kiến ​​trúc có thể thực thi.

A black screen with white text

Description automatically generated with low confidence

Hình 12 Cài đặt Rizin bằng Docker

## Radare2

Là một framework kỹ thuật đảo ngược tương tự như Rizin.

A computer screen with white text

Description automatically generated with low confidence

Hình 13 Cài đặt Radare2

## Viper

Là một khuôn khổ để phân tích và quản lý bộ sưu tập các mẫu phần mềm độc hại của bạn, mật khẩu là: “nonroot”.

A screenshot of a computer program

Description automatically generated with medium confidence

Hình 14 Cài đặt và cấu hình Viper

## Ciphey

Được thiết kế để tự động nhận dạng và giải mã/giải mã các kỹ thuật mã hóa và mã hóa phổ biến.

A screenshot of a computer

Description automatically generated with medium confidence

Hình 15 Mã hóa đoạn mã base64 với Ciphey

# Ưu nhược điểm của Image

Ưu điểm: các image được cài đặt các gói có sẵn nên quá trình khởi động nhanh và ổn định

Nhược điểm: vì các image được cấu hình riêng cho các mục đích khác nhau nên có sự không liên kết, có thể khắc phục bằng docker-compose hoặc là sử dụng máy ảo do Remnnux cung cấp.

Đường dẫn tham khảo:

<https://docs.remnux.org/run-tools-in-containers/remnux-containers>

<https://docs.remnux.org/install-distro/remnux-as-a-container>