**THIẾT LẬP VÀ CẤU HÌNH HONEYDRIVE**

* 1. **Mô tả**

HoneyDrive là môi trường đã được cài đặt sẵn một số Honeypot để thu hút tấn công của tin tặc, giúp người quản trị xây dựng môi trường thử nghiệm. Bản thân HoneyDrive được tích hợp một số công cụ sau:

- Kippo SSH honeypot

- Dionaea and Amun malware honeypots

- Honeyd low-interaction honeypot

- Glastopf web honeypot and Wordpot

- Conpot SCADA/ICS honeypot

- Thug and PhoneyC honeyclients

- Kippo-Graph, Honeyd-Viz, DionaeaFR, an ELK stack

Trong bài thực hành này hướng dẫn sinh viên sử dụng Kippo SSH Honeypot.

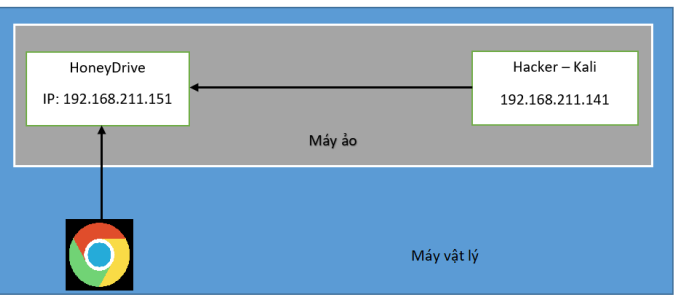
**1.2. Chuẩn bị**

− 01 máy ảo hệ điều hành Kali linux

− 01 máy ảo hệ điều hành HoneyDrive.

− Trình duyệt trên máy vật lý

**1.3. Mô hình cài đặt**

****

**1.4. Các bước cài đặt**

- Download phần mềm:

<https://sourceforge.net/projects/honeydrive/>

- Tải phần mềm dưới dạng máy ảo đã cài sẵn:

HoneyDrive\_3\_Royal\_Jelly.ova

Sử dụng phần mềm máy ảo để bung tệp tin ova này thành máy ảo HoneyDrive.

- Sử dụng máy Kali linux để thực hiện tấn công vào Honeypot SSH kippo

- Sử dụng trình duyệt trên máy vật lý truy cập vào Kippo-graph trên máy HoneyDrive để phân tích.

**1.5. Thực hiện**

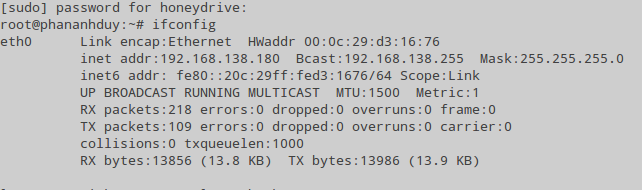
**Bước 1. Chạy máy ảo HoneyDrive**

Sau khi bung nén máy ảo HoneyDrive, khởi chạy máy ảo thành công có giao diện như sau:

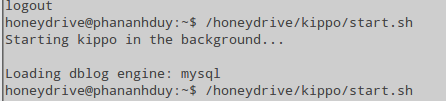


Tiếp theo cần xác địch địa chỉ IP của máy:

Chạy terminal trên Desktop và sử dụng lệnh ifconfig để xem:

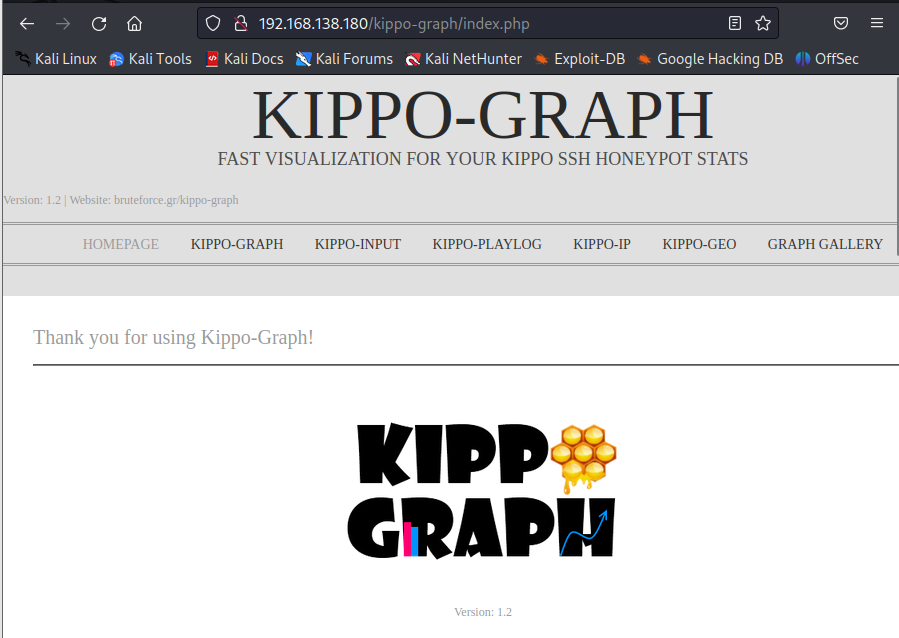


**Bước 2. Chạy chương trình Honeypot kippo**



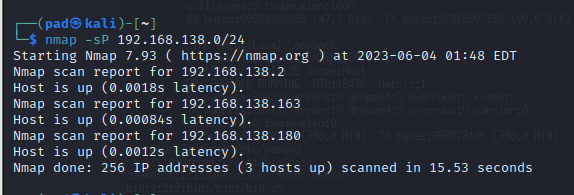
**Bước 3. Quản lý Honeypot Kippo**

Trên máy vật lý sử dụng trình duyệt web truy cập vào máy ảo HoneyDrive theo địa chỉ đã xem ở trên và theo đường dẫn sau: <http://192.168.138.180/kippo-graph/>



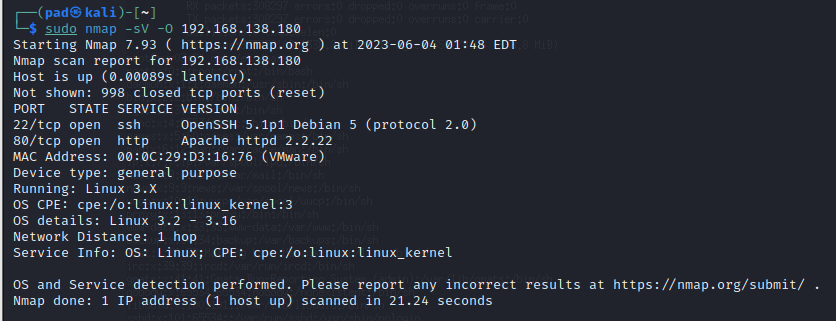
**Bước 4: Kịch bản tấn công dò quét IP và dịch vụ**

- Sử dụng Nmap trên Kali tấn công thăm dò mạng nội bộ:



Phát hiện một số máy tính đang chạy với IP.

- Thực hiện dò quét dịch vụ và hệ điều hành trên máy 192.168.138.180

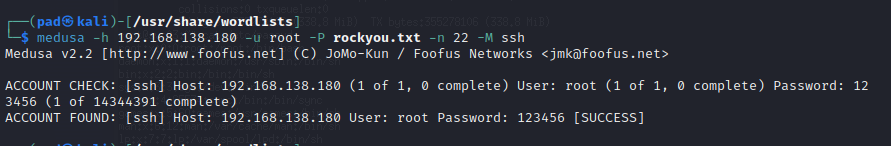


Kết quả phát hiện dịch vụ SSH và web đang chạy trên cổng 22, 80. Hệ điều hành máy đích là Linux => khả năng đây là máy chủ web.

Kẻ tấn công thực hiện các bước mà không phát hiện ra họ đang tấn công vào dịch vụ của Honeypot.

**Bước 5. Kịch bản tấn công mật khẩu dịch vụ SSH**

Sử dụng medusa trên Linux tấn công từ điển vào mật dịch vụ SSH



Kết quả thành công, thu được mật khẩu của tài khoản root.

**Bước 6. Truy cập vào máy chủ thông qua dịch vụ SSH**

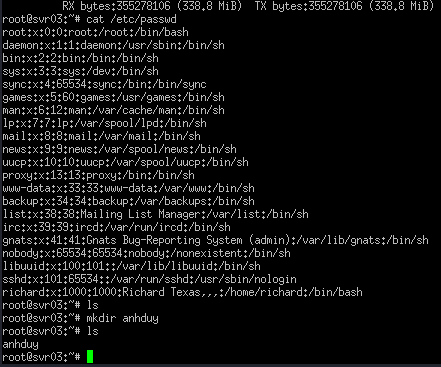
Với tài khoản và mật khẩu đã có, kẻ tấn công thực hiện lệnh kết nối tới máy chủ:





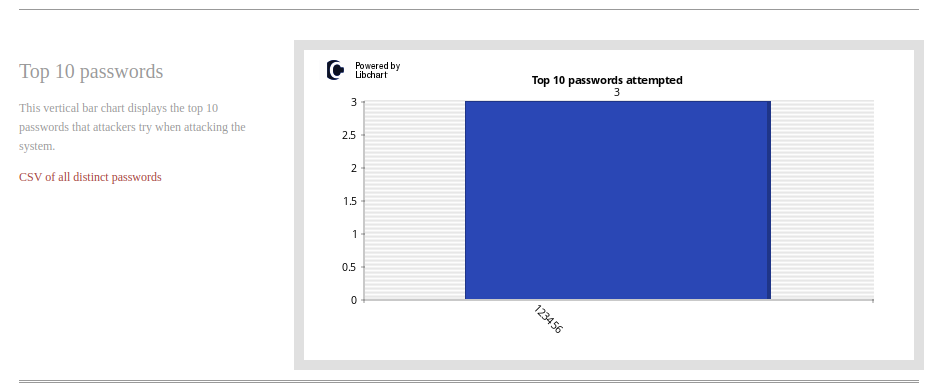
Truy cập thành công

**Bước 7. Thực hiện một số lệnh trên máy chủ**

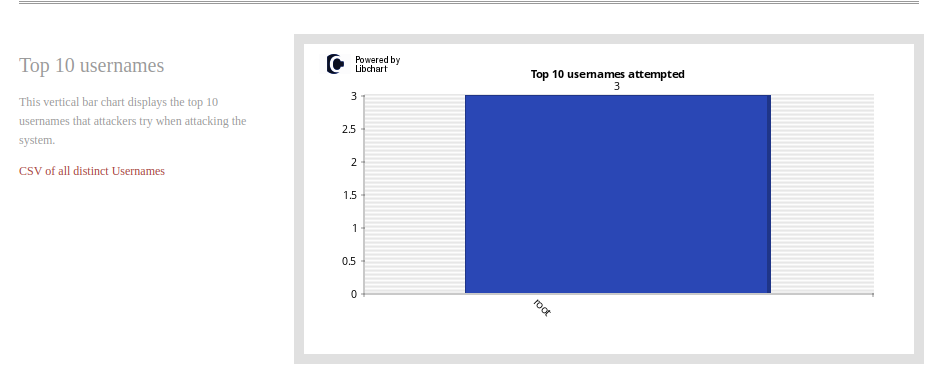


**Bước 8. Phân tích hành vi**

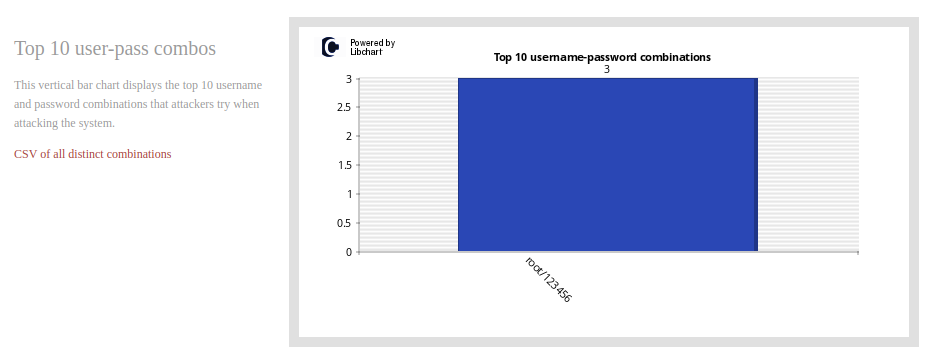
Tại trình duyệt Kippo đã bật trong bước 3. Refresh lại trình duyệt thì kết quả như sau:



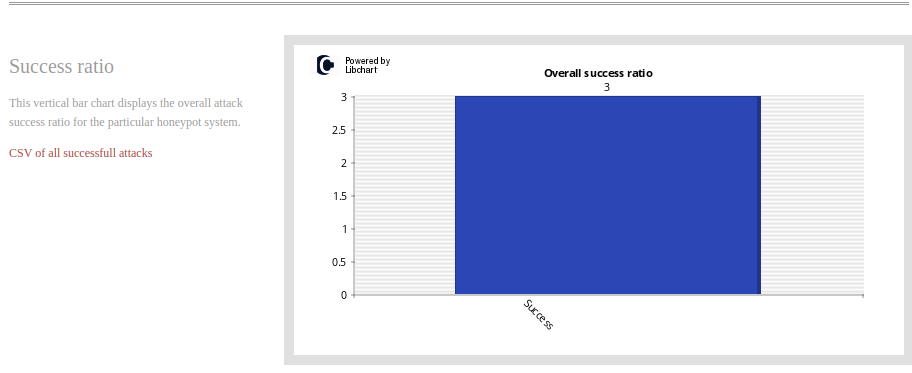
Giao diện này cho biết mật khẩu và số lượng tin tặc đã sử dụng.

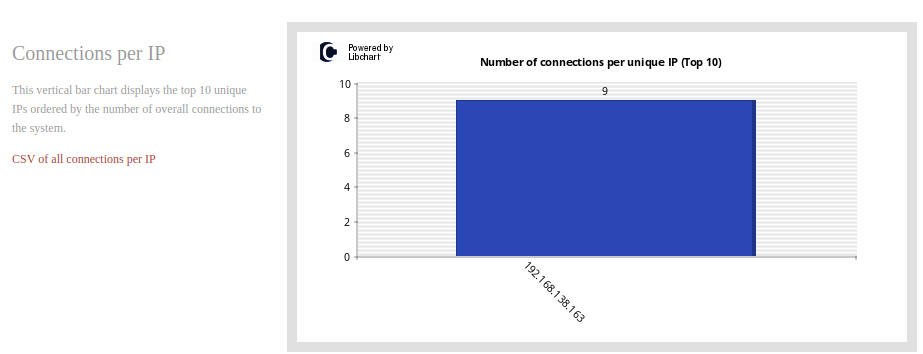


Giao diện này cho biết tài khoản và số lần đăng nhập.



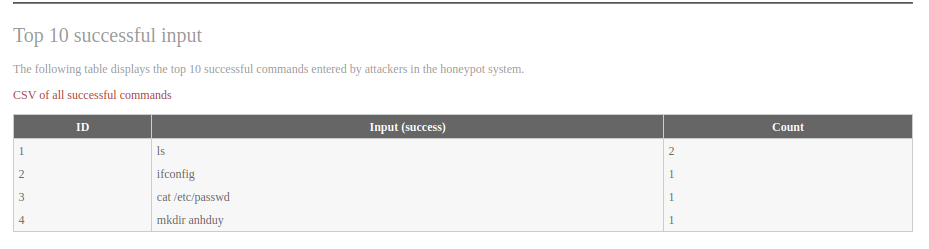
Giao diện này cho biết tài khoản được đăng nhập bởi mật khẩu tương ứng.

Giao diện này cho biết số lần đăng nhập đúng và sai.



Giao diện này cho biết IP của tin tặc đã sử dụng để xâm nhập vào máy chủ Honeypot.

Chuyển sang Tab Kippo-Input để phân tích một số lệnh tin tặc đã sử dụng



**Kết luận:**

Với HoneyDrive người quản trị có thể sử dụng để thực hiện một số Honeypot để thu hút tấn công của tin tặc. Từ đó biết được cách thức tấn công, dịch vụ bị tấn công. Vì vậy mà người quản trị có thể đưa ra các giải pháp ngăn chặn cho hệ thống thực.