HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

BÀI THỰC HÀNH SỐ 06

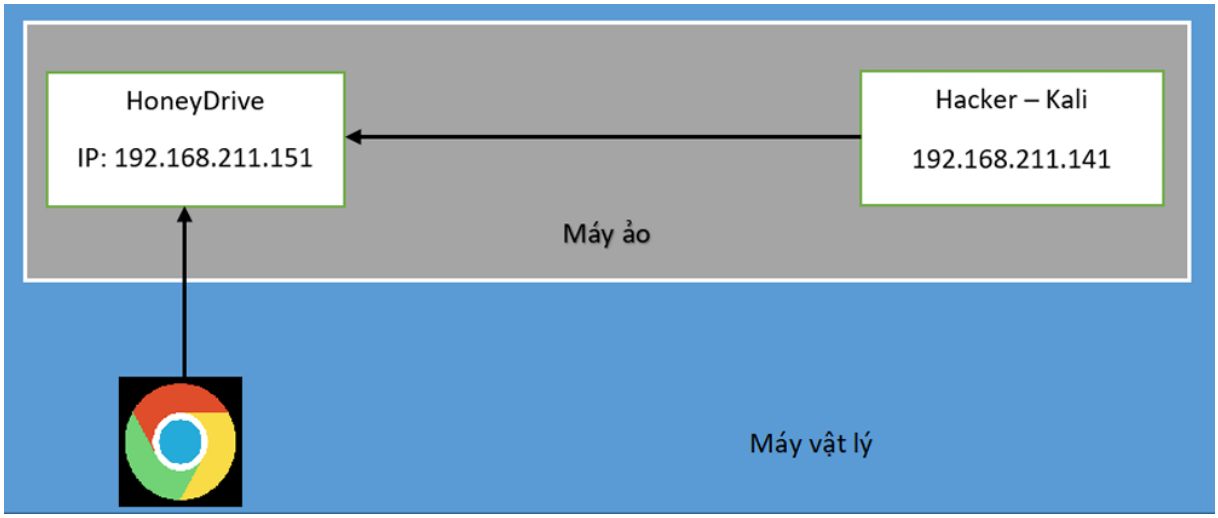
TRIỂN KHAI HONEYPOT SỬ DỤNG HONEYDRIVE

Sinh viên thực hiện: **Nguyễn Hữu Văn – AT190157**

Hà Nội, 2025

Mục Lục

I. Mô hình cài đặt



II. 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:

Kiểm tra IP

```
honeydrive@honeydrive:~/Desktop$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:68:a8:1b
          inet addr:192.168.211.151  Bcast:192.168.211.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe68:a81b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:386 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:83176 (83.1 KB)  TX bytes:56351 (56.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19790 (19.7 KB)  TX bytes:19790 (19.7 KB)

honeydrive@honeydrive:~/Desktop$
```

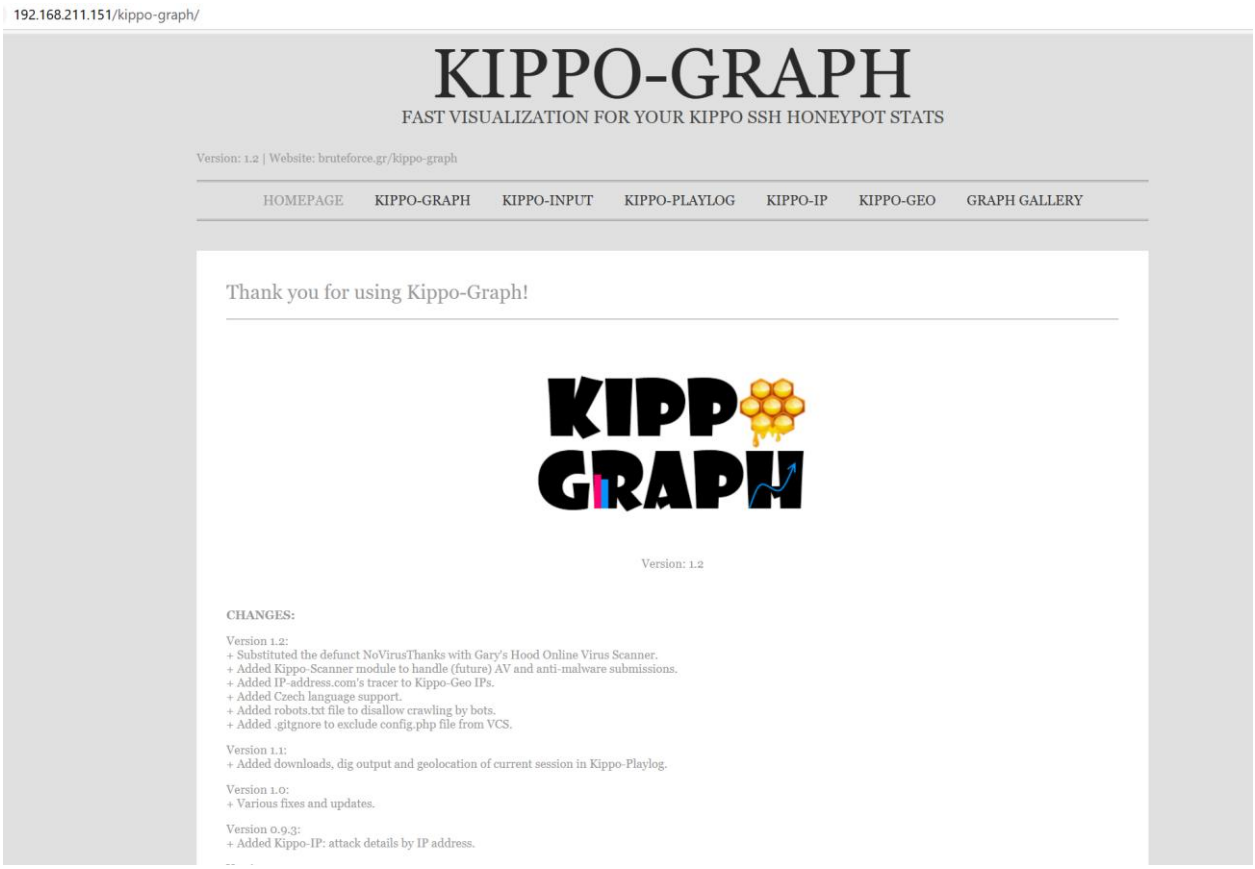
Bước 2: Chạy chương trình Honeypot kippo

```
honeydrive@honeydrive:~/Desktop$ /honeydrive/kippo/start.sh
Starting kippo in the background...

Loading dblog engine: mysql
honeydrive@honeydrive:~/Desktop$
```

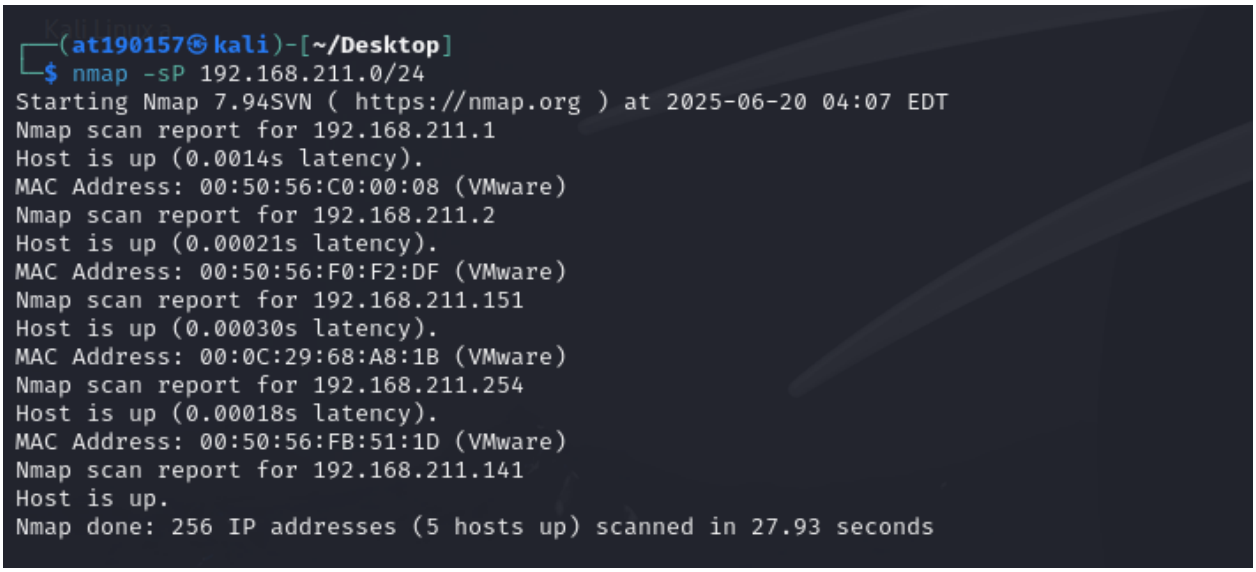
Bước 3: Quản lý Honeypot Kippo

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



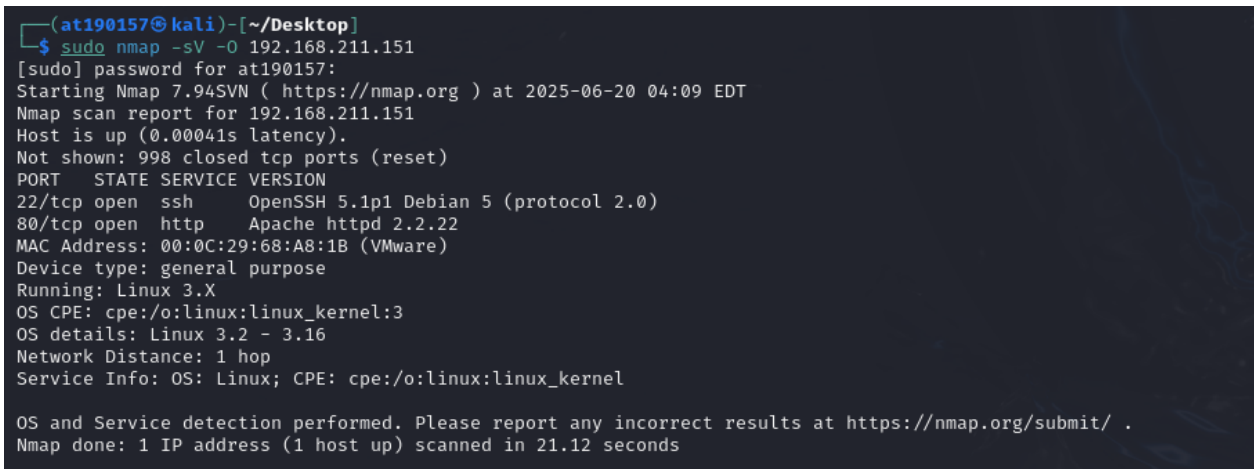
Bước 4: Kịch bản tấn công dò quét IP và dịch vụ

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



Phát hiện một số máy tính đang chạy với IP.

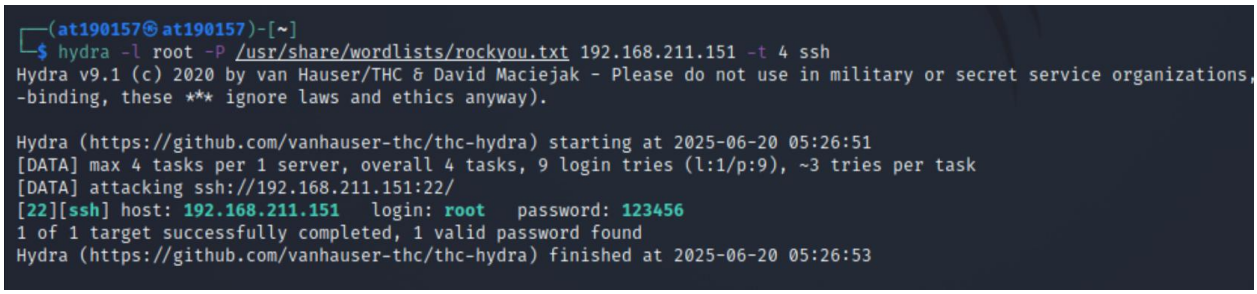
Thực hiện dò quét dịch vụ và hệ điều hành trên máy 192.168.211.151



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 Hydra trên Linux tấn công từ điển vào mật dịch vụ SSH



Kết quả thành công lấy được mật khẩu 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:

```
┌──(at190157㉿at190157)-[~]
└─$ ssh -o KexAlgorithms=+diffie-hellman-group1-sha1 root@192.168.211.151
The authenticity of host '192.168.211.151 (192.168.211.151)' can't be established.
RSA key fingerprint is SHA256:OfedJtU1A4ScTPb/7hzg+GggtLH/56BZskrD/iw0KYk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.211.151' (RSA) to the list of known hosts.
(root@192.168.211.151) Password:
root@svr03:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)
root@svr03:~#
```

Truy cập thành công

Bước 7: Thực hiện một số lệnh trên máy chủ:

```
root@svr03:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
richard:x:1000:1000:Richard Texas,,,:/home/richard:/bin/bash
root@svr03:~#
```

```
root@svr03:~# passwd richard
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

```
root@svr03:~# mkdir /virus
root@svr03:~# touch virus.sh /virus/
root@svr03:~#
```

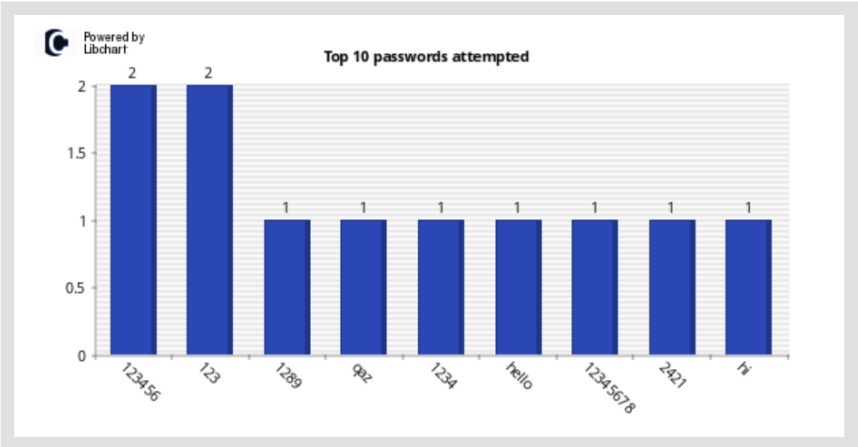
Bước 8: Phân tích hành vi

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

Top 10 passwords

This vertical bar chart displays the top 10 passwords that attackers try when attacking the system.

CSV of all distinct passwords

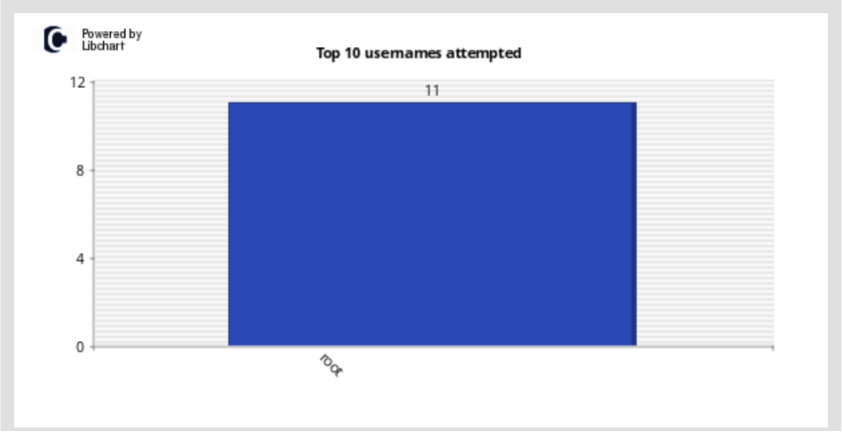


Giao diện này cho biết mật khẩu và số lượng tin tặc đã sử dụng.

Top 10 usernames

This vertical bar chart displays the top 10 usernames that attackers try when attacking the system.

CSV of all distinct Usernames

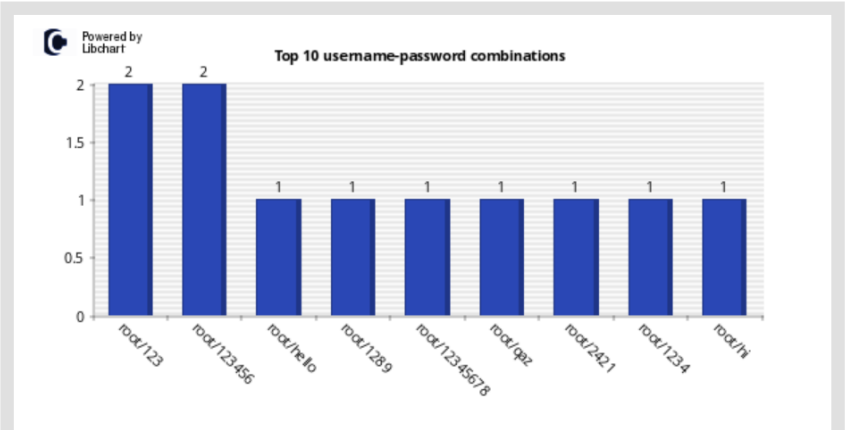


Giao diện này cho biết tài khoản và số lần đăng nhập.

Top 10 user-pass combos

This vertical bar chart displays the top 10 username and password combinations that attackers try when attacking the system.

CSV of all distinct combinations

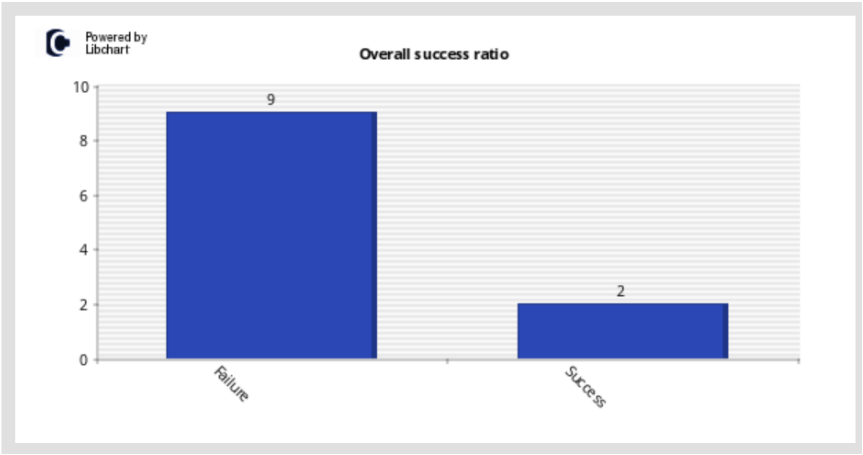


Giao diện này cho biết tài khoản được đăng nhập bởi mật khẩu tương ứng

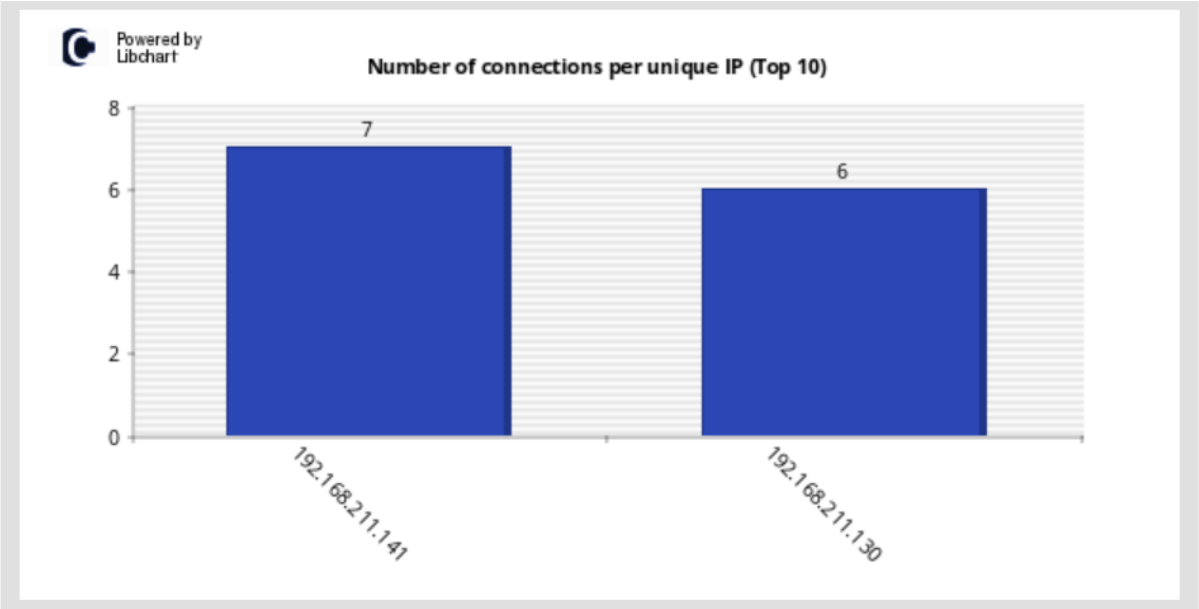
Success ratio

This vertical bar chart displays the overall attack success ratio for the particular honeypot system.

CSV of all successfull attacks



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

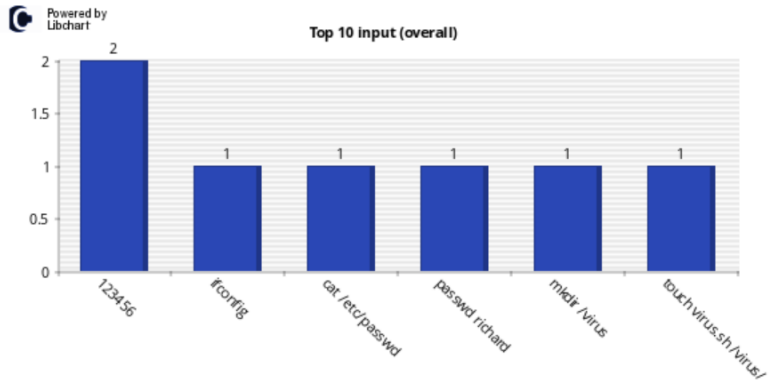
Top 10 input (overall)

The following table displays the top 10 commands (overall) entered by attackers in the honeypot system.

CSV of all input commands

ID	Input	Count
1	123456	2
2	ifconfig	1
3	cat /etc/passwd	1
4	passwd richard	1
5	mkdir /virus	1
6	touch virus.sh /virus/	1

This vertical bar chart visualizes the top 10 commands (overall) entered by attackers in the honeypot system.



III. 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.