HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH

AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 06

TRIỂN KHAI HONEYPOT SỬ DỤNG HONEYDRIVE

Người xây dựng bài thực hành:

Th.S Cao Minh Tuấn

HÀ NỘI, 2021

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Triển khai Honeypot sử dụng HoneyDrive.

Học phần: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

Máy tính vật lý có cấu hình tối thiểu: RAM 4GB, 50 HDD

- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

THIẾT LẬP VÀ CẤU HÌNH HONEYDRIVE

1.1. 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.

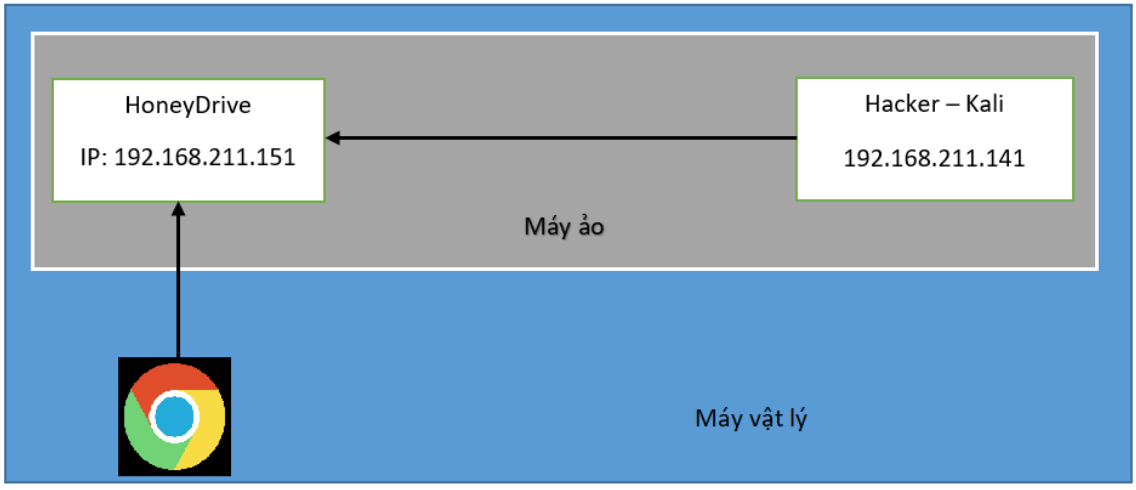
1.2. Chuẩn bị

– 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 định địa chỉ IP của máy:

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

```
honeydrive@honeydrive:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ea:45:d8
          inet addr:192.168.211.151  Bcast:192.168.211.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feea:45d8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6269 (6.2 KB)  TX bytes:10587 (10.5 KB)
```

Bước 2. Chạy chương trình Honeypot kippo

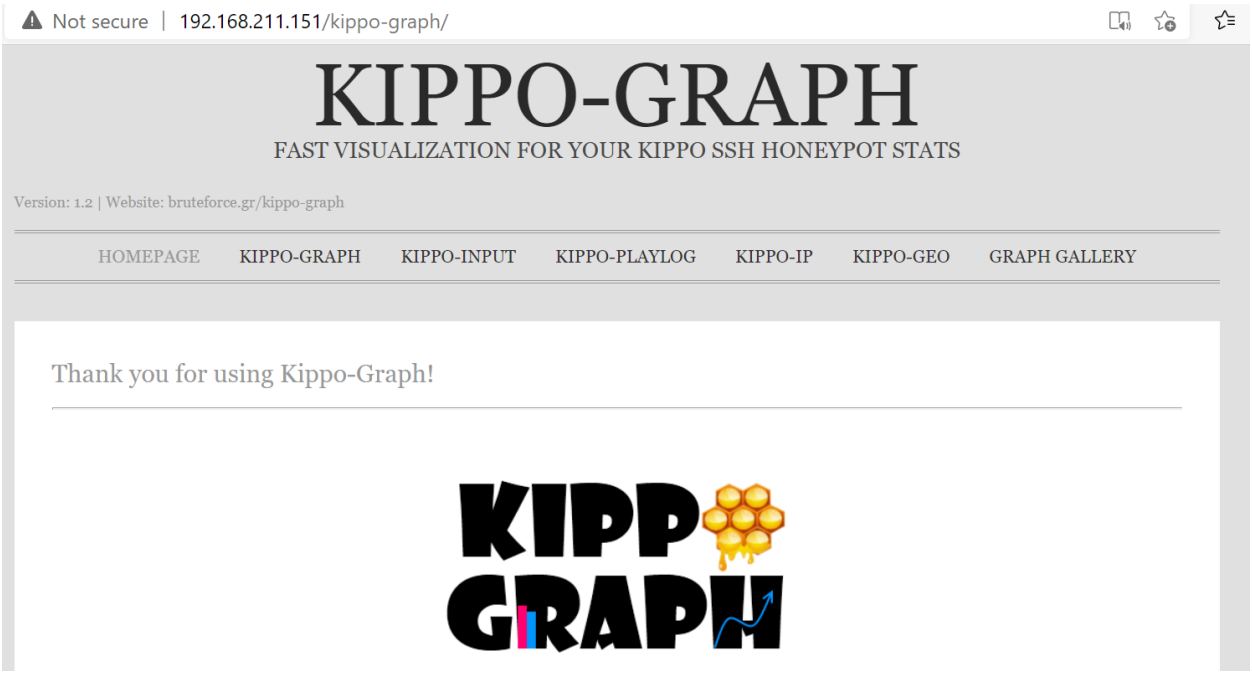
```
honeydrive@honeydrive:~$ /honeydrive/kippo/start.sh
Starting kippo in the background...

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

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://192.168.211.151/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:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.211.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 03:41 EST
Nmap scan report for 192.168.211.2
Host is up (0.0019s latency).
Nmap scan report for 192.168.211.129
Host is up (0.00066s latency).
Nmap scan report for 192.168.211.141
Host is up (0.0040s latency).
Nmap scan report for 192.168.211.151
Host is up (0.0027s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.56 seconds
```

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.211.151
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 03:44 EST
Nmap scan report for 192.168.211.151
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22
MAC Address: 00:0C:29:EA:45:D8 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

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

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.211.151 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-01 03:48:08
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://192.168.211.151:22/
[22][ssh] host: 192.168.211.151   login: root   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-01 03:48:12
```

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:

```
┌──(kali㉿kali)-[~]
└─$ ssh -o KexAlgorithms=+diffie-hellman-group1-sha1 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)
```

Truy cập thành công.

Bước 7. Thực hiện một số lệnh trên máy chủ

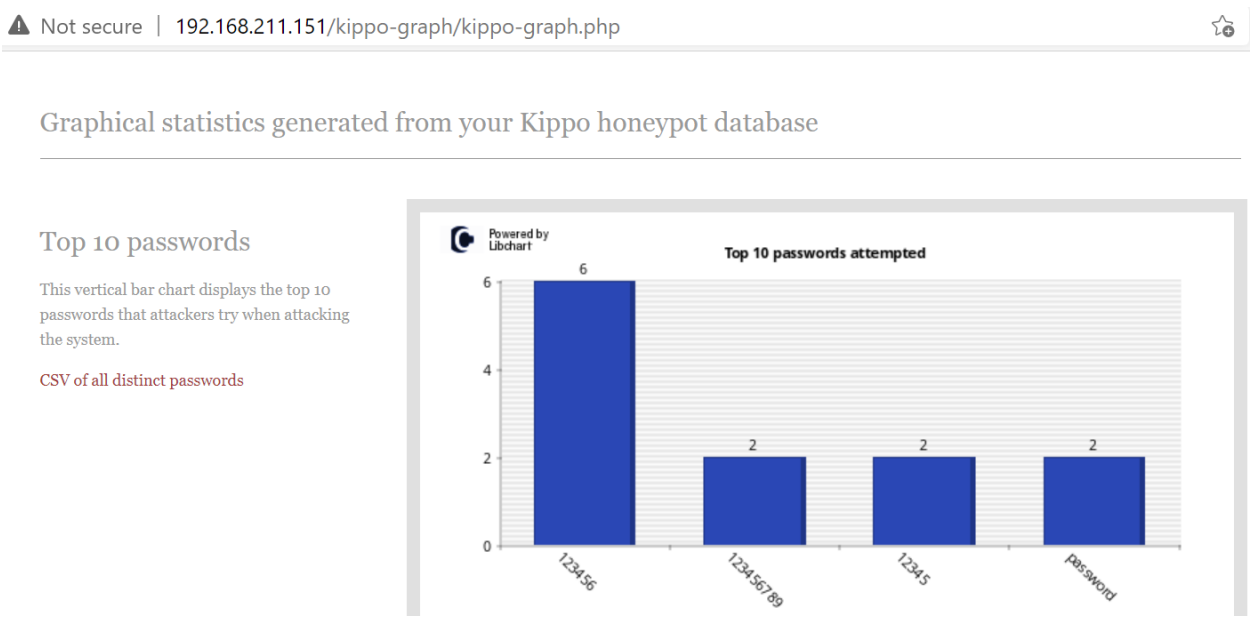
```
root@svr03:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
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:~#
```

```
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:

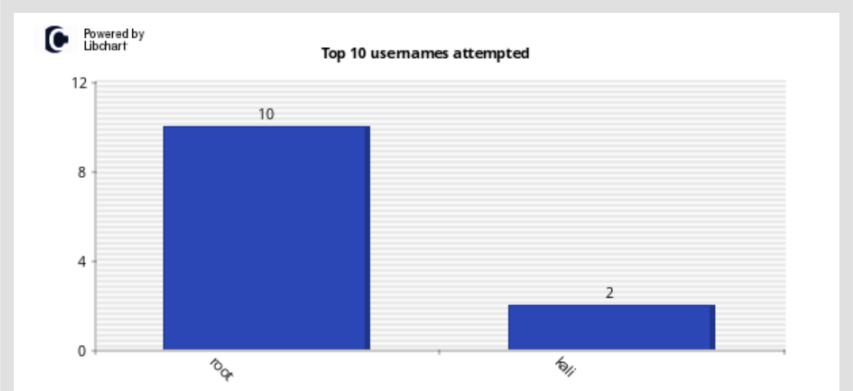


Giao diện này cho biết mật khẩu và số lượng tin tặc đã sử dụng.

Top 10 usernames

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

CSV of all distinct Usernames

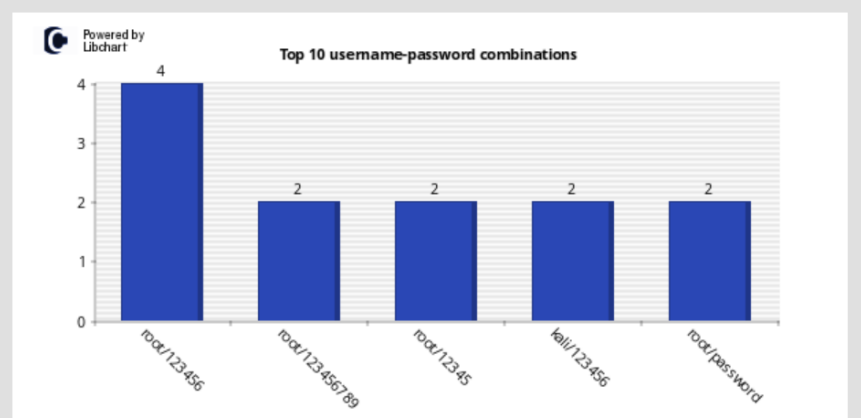


Giao diện này cho biết tài khoản và số lần đăng nhập.

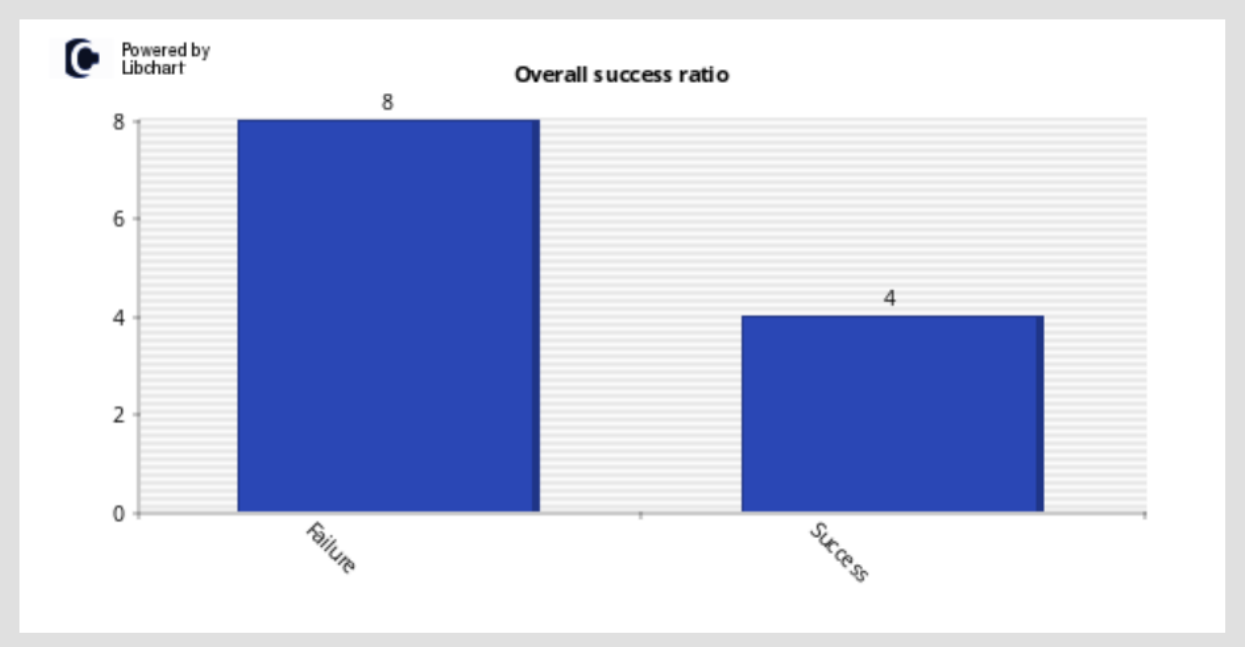
Top 10 user-pass combos

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

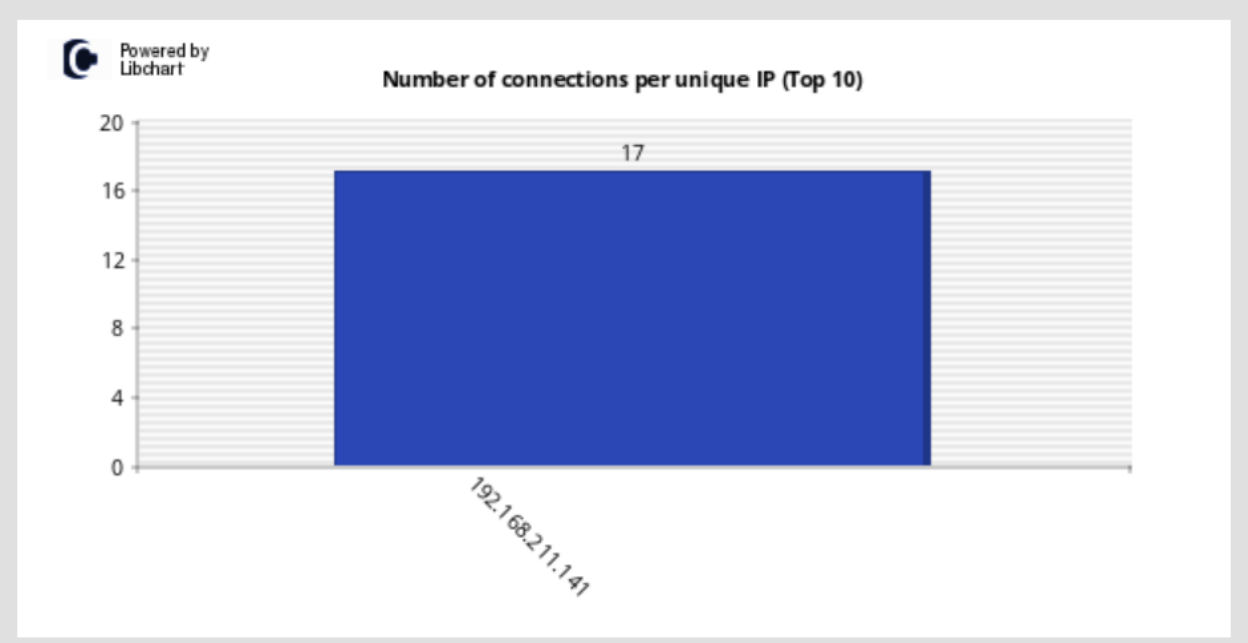
CSV of all distinct combinations



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



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

ID	Input (success)	Count
1	ls	2
2	cat /etc/passwd	2
3	exit	2
4	mkdir /adfj	1
5	mkdir /test	1
6	cd /var	1
7	cd /var/log/	1
8	cd	1
9	cat /etc/password	1
10	ifconfig	1

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.

```
//kết thúc bài thực hành.
```