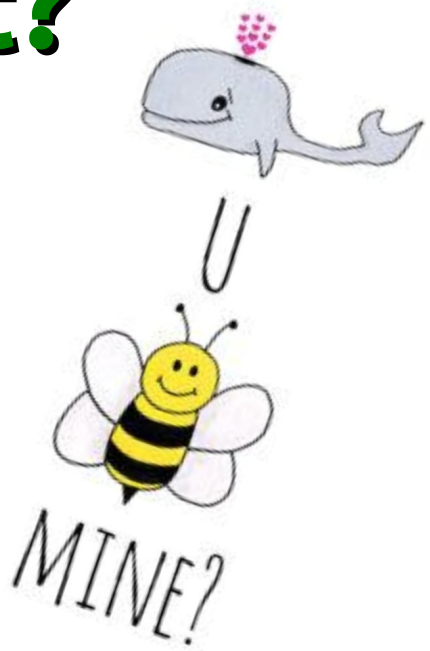
Docker e HoneyPot? Por que não?



Erick dos Santos Alves

TIC / UFRJ
2019

Roteiro

- Só vi vantagens!
- Estrutura de uma VM Docker para HoneyPot
- Docker Compose para facilitar as coisas
- Gerenciamento facilitado com o Portainer
- Envio de logs para armazenamento
- ***Extra:*** *Cowrie e Kippo-Graph*

HoneyPot

Ferramenta que simula serviços e falhas de segurança para coleta de informações e comportamentos do invasor.

- São divididos em 3 tipos:
  - Baixa Interatividade
  - Média Interatividade
  - Alta Interatividade

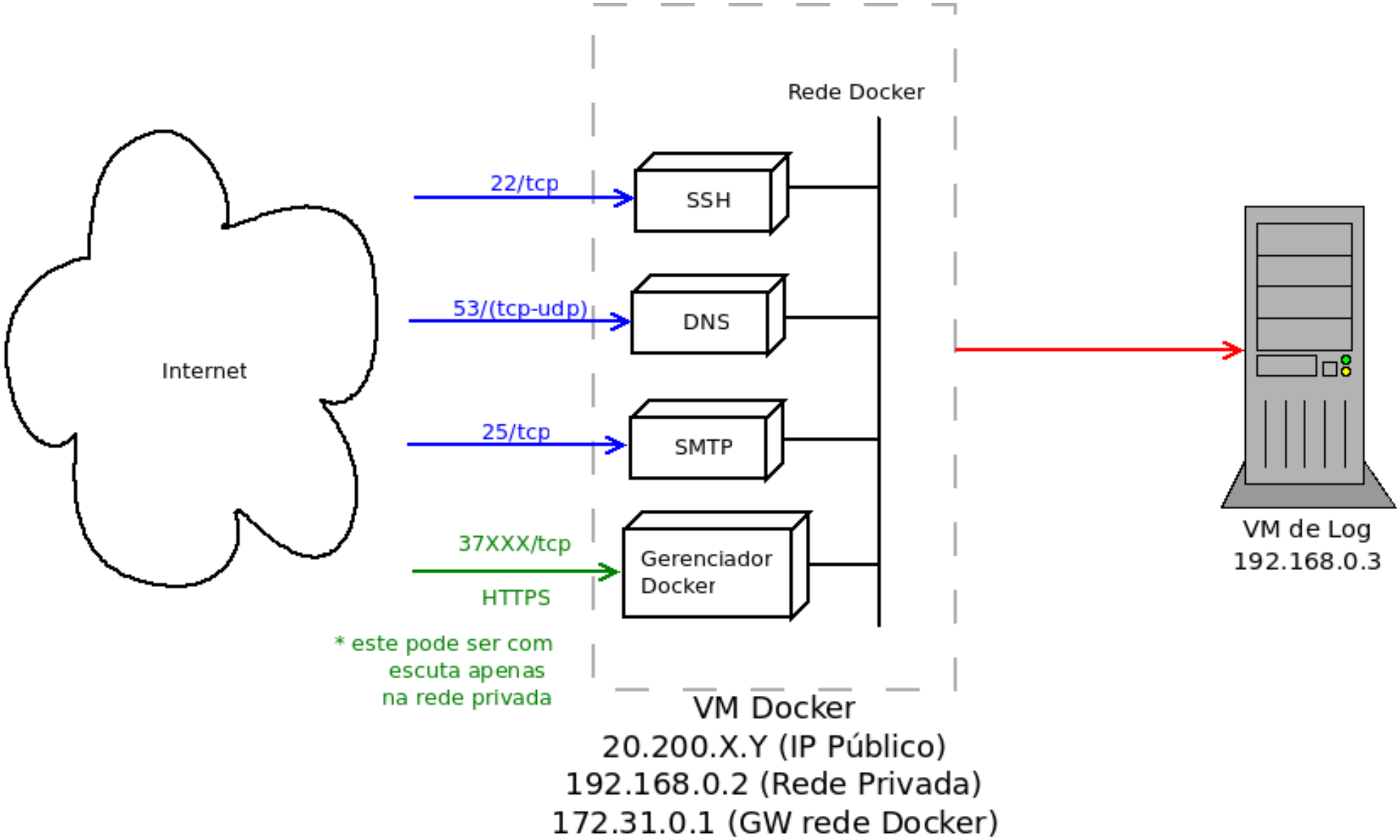
Só vi vantagens!

- Facilidade em levantar e refazer ativos para ataques
- … inclusive de hosts de alta interatividade
- Facilita diversificar serviços
- Envio de logs de forma trivial
- Maior controle na liberação de portas e redes para ataque
- Isolamento dos contêineres impede danos à VM

Docker para HoneyPot (1)

- **Algumas observações:**
  - Portas padrão ficam para interação
  - Para contêineres de gerência utilizar portas não-padrão ou subir em outros endereços IP
  - Servidor de log em contêiner separado ou, se possível, em outra VM
  - Se utilizar IP público no contêiner, não precisa publicar porta
    - *A exposição de porta já é suficiente*
    - *Necessária a criação de uma rede docker do tipo* ***macvlan***

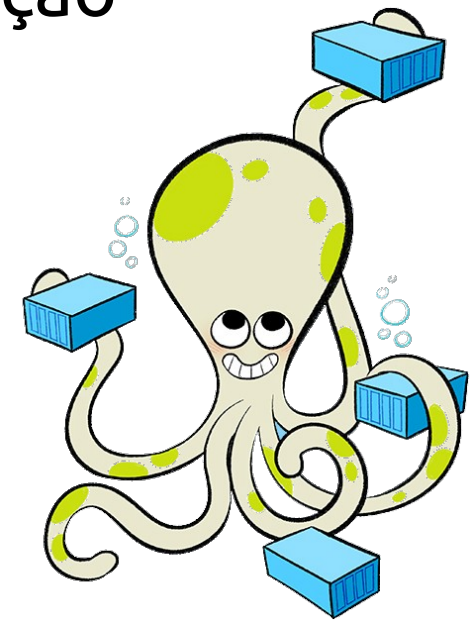
Docker para HoneyPot (2)



Docker Compose (1)

- Arquivo no formato YAML que contém as especificações do **contêiner** ou **stack***

- Deixa as configurações mais claras, facilitando a criação e a manutenção



Docker Compose (2)

```
version: '2.4'
networks:
   default:
       external:
           name: rede_docker

services:
   ssh-honey:
       container_name: ssh-honey
       hostname: ssh-honey
       image: txt3rob/docker-ssh-honey
       ports:
           - "22:22"
       volumes:
           - /etc/localtime:/etc/localtime:ro
```

Docker Compose (3)

Com IP público:

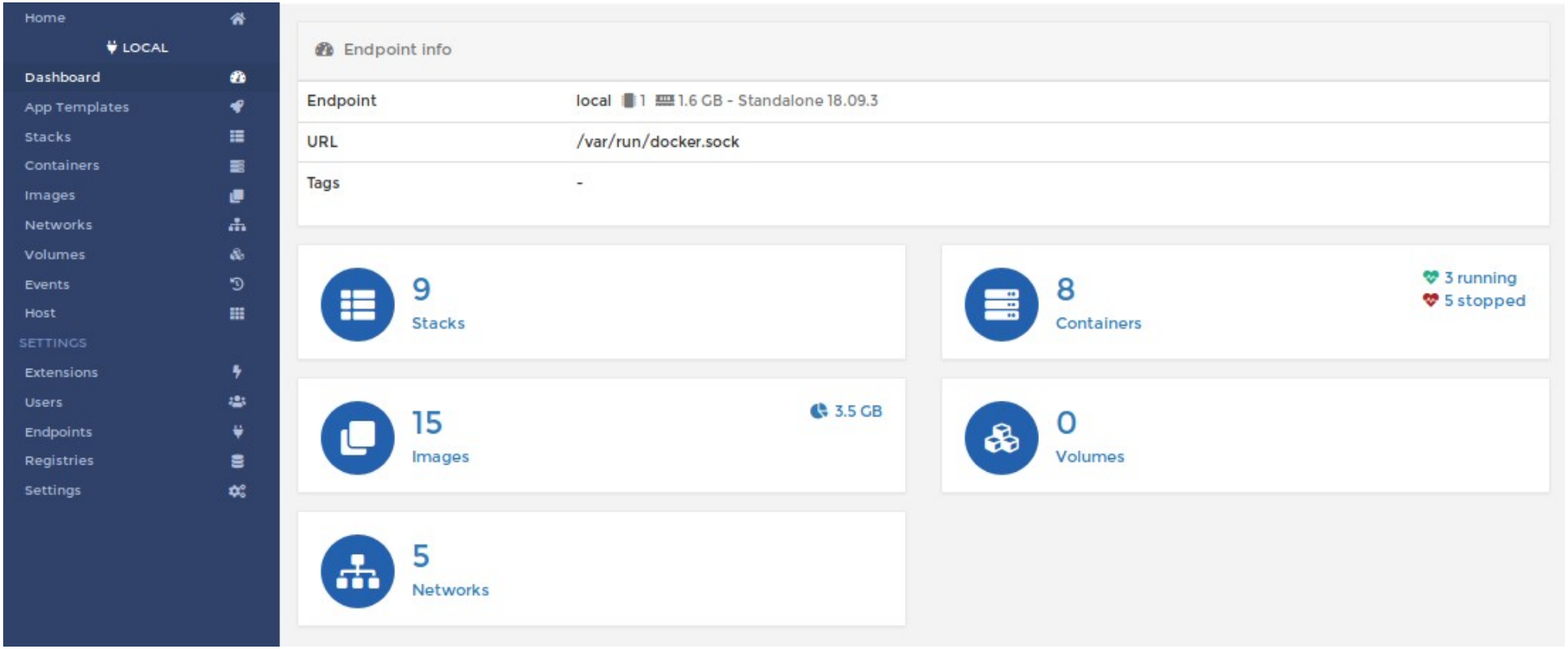
```
version: '2.4'
networks:
   default:
       external:
           name: rede_publica

services:
   ssh-honey:
       container_name: ssh-honey
       hostname: ssh-honey
       image: txt3rob/docker-ssh-honey
       expose:
           - 22
       default:
           ipv4_address: 20.200.A.B
       volumes:
           - /etc/localtime:/etc/localtime:ro
```

Portainer

- Interface web para gerência de Docker
- Versão **1.22.0**
- Facilita operações básicas de **(re)iniciar**, **desligar** e **reconstruir** contêineres.
- Interface amigável com gráficos de CPU, memória, processos e “logs”.
- Possui ACL para garantir controle de acesso aos **contêineres**, **stacks** e **endpoints**.

Portainer (Dashboard)



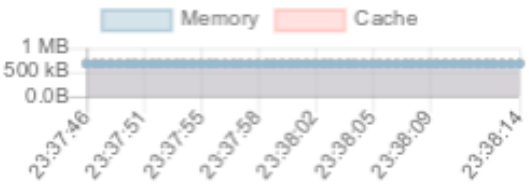
Portainer (Stats)

About statistics

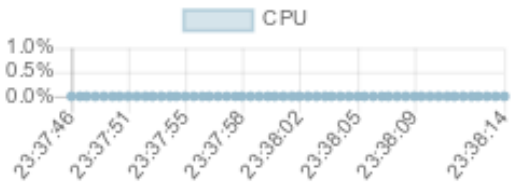
This view displays real-time statistics about the container **ssh-honey** as well as a list of the running processes inside this container.

Refresh rate 1s

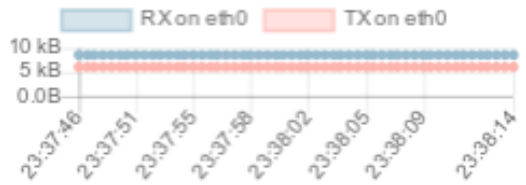
Memory usage



CPU usage



Network usage

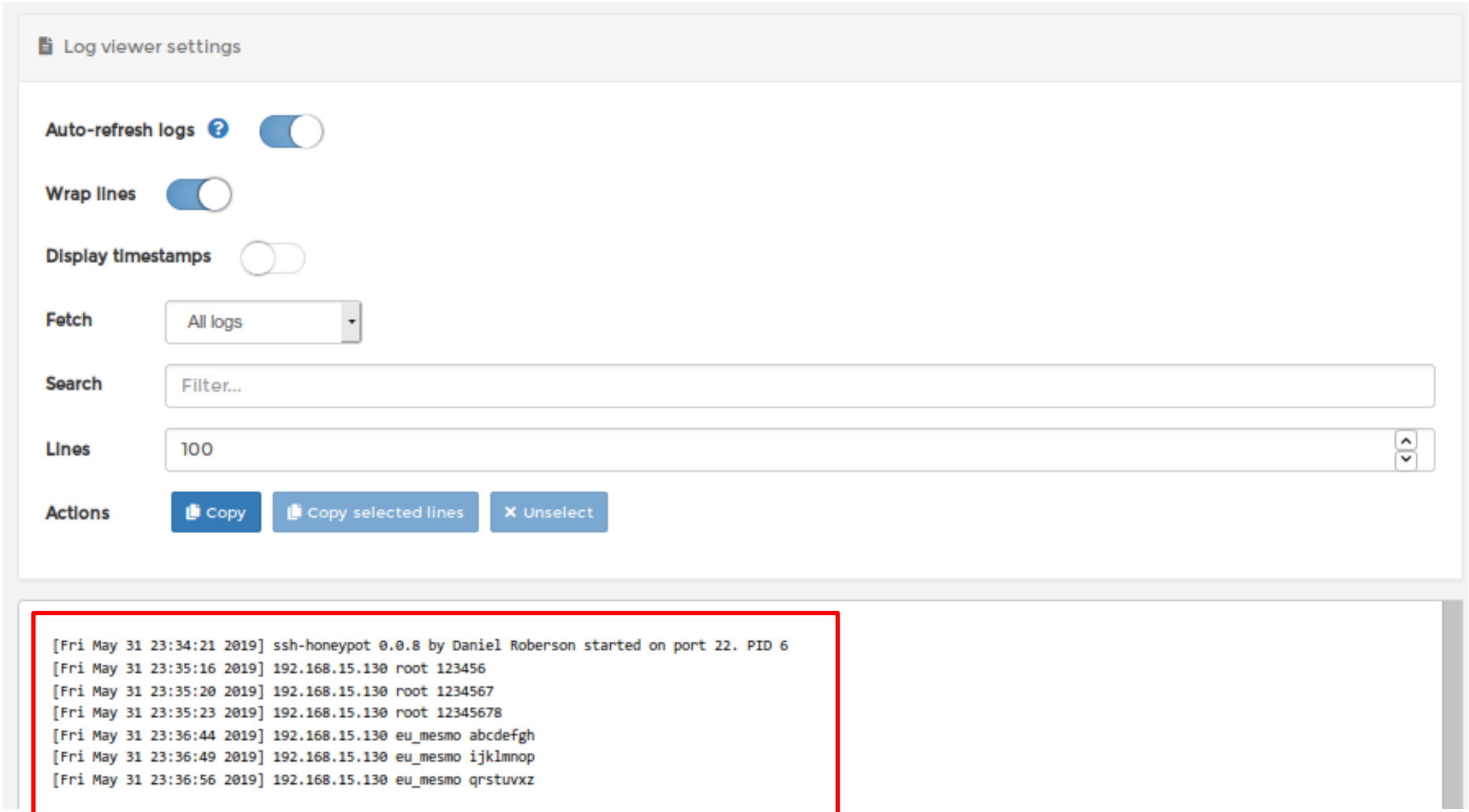


Processes

Search...

UID	PID	PPID	C	STIME	TTY	TIME	CMD
root	1963	1947	0	23:34	?	00:00:00	/bin/ash /entrypoint.sh
nobody	2017	1963	0	23:34	?	00:00:00	ssh-honeypot -r /ssh-honeypot/ssh-honeypot.rsa -p 22 -u nobody

Portainer (Logs)



Envio de Logs (1)

- Diretiva **logging** no Docker Compose
- Suporte a diversos formatos:
  - *local, json-file, syslog, journald, gelf, fluentd, awslogs, splunk, etwlogs, gcplogs, logentries*

IMPORTANTE:

Quando a saída de log de um contêiner é desviada para um servidor de log perde-se a saída de log pelo Portainer.

Envio de Logs (2)

```
logging:
  driver: syslog
  options:
    syslog-address: "tcp://192.168.0.3:5140"
```

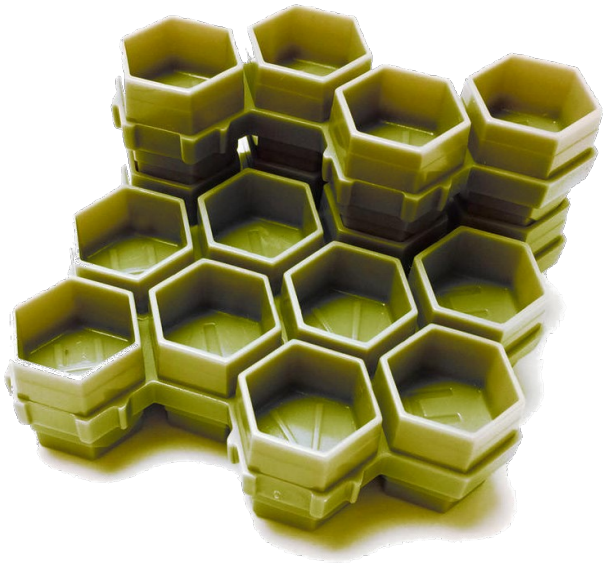
```
logging:
  driver: gelf
  options:
    gelf-address: "udp://192.168.0.3:12201"
```

Envio de Logs (3)

```
version: '2.4'
networks:
    (...)
services:
    ssh-honey:
       container_name: ssh-honey
       hostname: ssh-honey
       image: txt3rob/docker-ssh-honey
       ports:
           - "22:22"
       logging:
           driver: syslog
           options:
               syslog-address: “tcp://192.168.0.3:5140”
       volumes:
           - /etc/localtime:/etc/localtime:ro
```

Algumas imagens Docker para HoneyPot

- **txt3rob/docker-ssh-honey**
- **txt3rob/docker-telnet-logger**
  - *Baixa interatividade*



- **cowrie/cowrie**
  - *Monitora Telnet e SSH, inclusive os comandos informados*
  - *Média interatividade*

- **wonderfall/kippo-graph**
  - *Dashboard trivial para o Cowrie*

Cowrie e Kippo-Graph (1)

Algumas considerações:

- Cowrie = Contêineres de interação
  Kippo-Graph = Dashboard

- Necessário um banco **MariaDB** ou **MySQL**
  → *Este banco é comum aos "cowries" e ao kippo-graph*
  → *Cowries geram os dados e kippo-graph os lê*

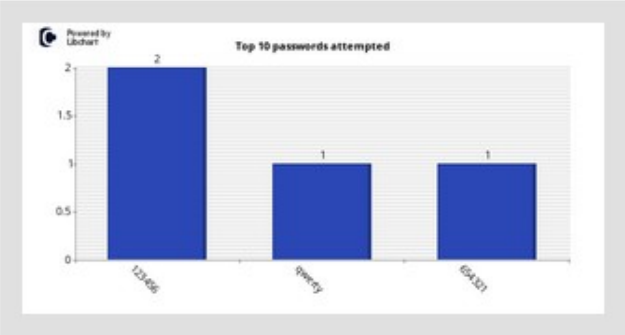
- Na imagem do Cowrie é necessário instalar o pacote **default-libmysqlclient-dev**
  → *Pode-se fazer derivando da imagem original*

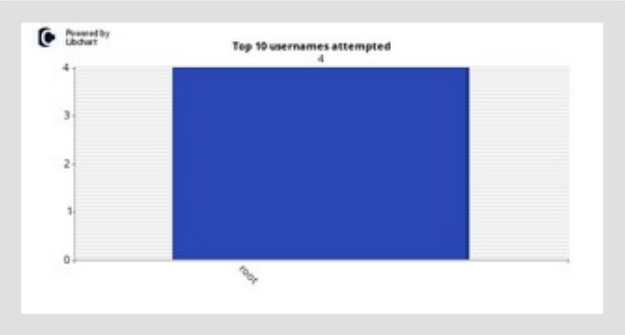
- Diversas formas de visualização dos dados coletados, mas sem filtros e customizações.

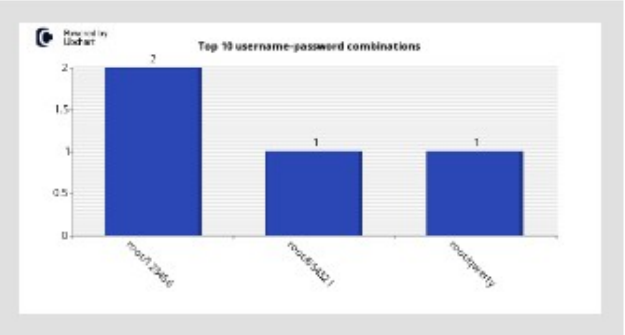
Cowrie e Kippo-Graph (2)

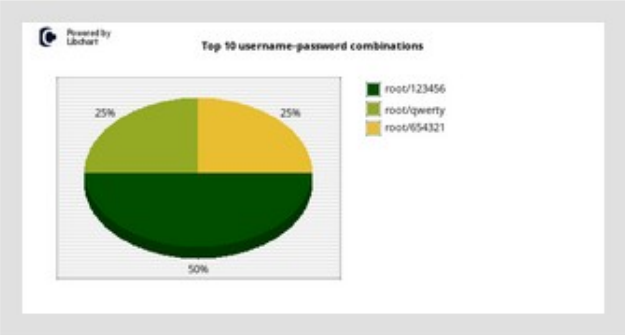
Graph Gallery

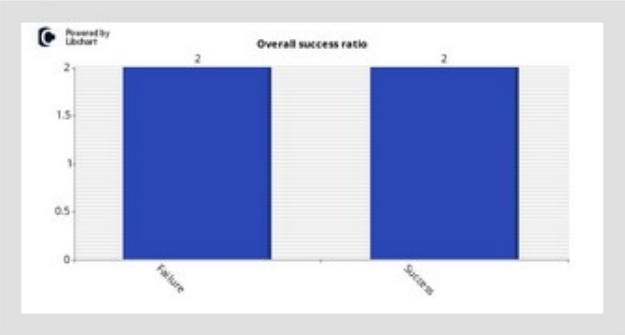
Provided you have visited all the other pages (Overview & Input), for the graphs to be generated, you can see all the images in this single page.

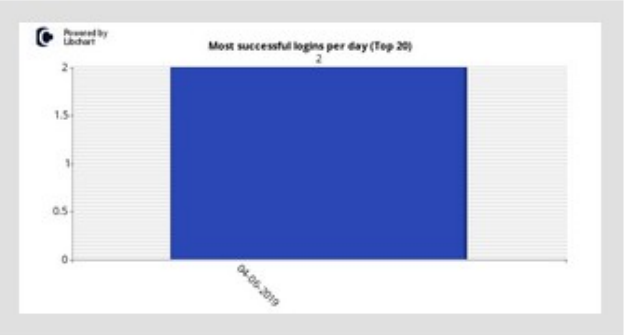












Cowrie e Kippo-Graph (3)

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	kill -9 1	1
2	poweroff	1
3	shutdown -h now	1
4	rm -Rf /	1
5	cd /	1
6	rm -R var	1
7	touch 0day.sh	1
8	ls -lah	1
9	useradd pirate	1

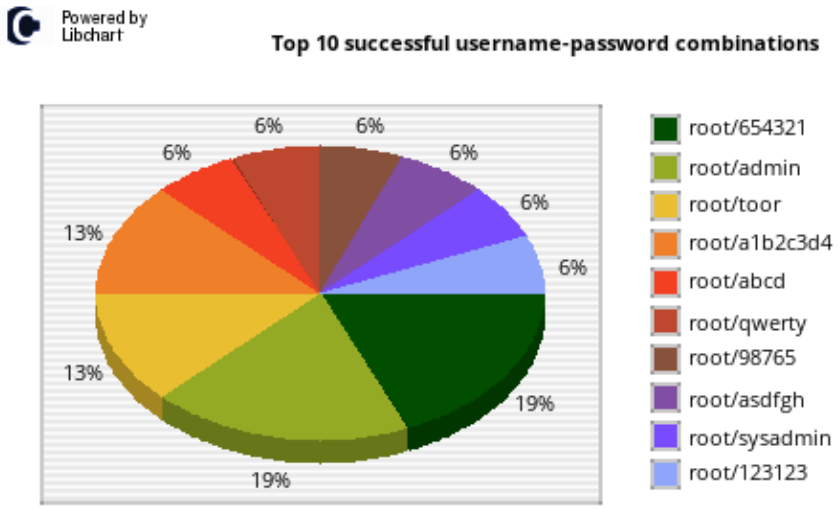
Cowrie e Kippo-Graph (4)

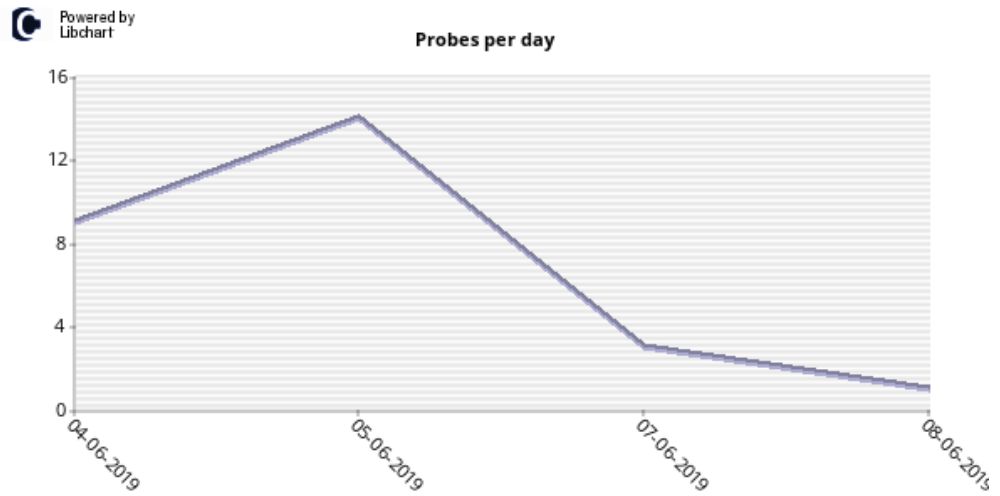
wget Commands

The following table displays the latest "wget" commands entered by attackers in the honeypot system.

CSV of all "wget" commands

Total inputs: 1					
ID	**Timestamp**	**Input**	**File link**	**Play Log**	**Kippo-Scanner**
1	2019-06-07 19:57:43	wget https://github.com/vrana/adminer/releases/download/v4.7.1/adminer-4.7.1.php	http://anonym.to/?https://github.com/vrana/adminer/releases/download/v4.7.1/adminer-4.7.1.php	Play	Scan File





Cowrie e Kippo-Graph (5)

TTY log

IP: **192.168.15.130** on 2019-06-05 23:05:45

Playing session: **c26b0c871bf9**

```
ld.so.cache               magic                     passwd-                   ho
sts                      discover-modprobe.conf
services                  host.conf                 securetty                 ho
sts.deny                 apt
wgetrc                    hosts.allow               cron.monthly              re
solv.conf                console-setup
deluser.conf              dpkg                      networks                  fs
tab.d                    ld.so.conf
groff                     inputrc                   login.defs                os
-release                 kernel
root@minerva-01:~#
nanorc        nsswitch.conf network       nologin       networks
root@minerva-01:~# cd /etc/network/
root@minerva-01:/etc/network# ll
-bash: ll: command not found
root@minerva-01:/etc/network# ls -lah
drwxr-xr-x 1 root root 4096 2013-04-05 08:52 .
drwxr-xr-x 1 root root 4096 2013-04-05 08:52 ..
drwxr-xr-x 1 root root 4096 2013-04-05 08:52 if-down.d
drwxr-xr-x 1 root root 4096 2013-04-05 08:52 if-post-down.d
drwxr-xr-x 1 root root 4096 2013-04-05 08:52 if-pre-up.d
drwxr-xr-x 1 root root 4096 2013-04-05 09:02 if-up.d
-rw-r--r-- 1 root root  277 2013-04-05 09:03 interfaces
lrwxrwxrwx 1 root root   12 2013-04-05 08:52 run -> /run/network
root@minerva-01:/etc/network# rm -f
```

Obrigado !

Erick dos Santos Alves

erick_sa@ufrj.br