DEEP SEC VIENA

OPEN SOURCE NETWORK MONITORING

PAULA DE LA HOZ

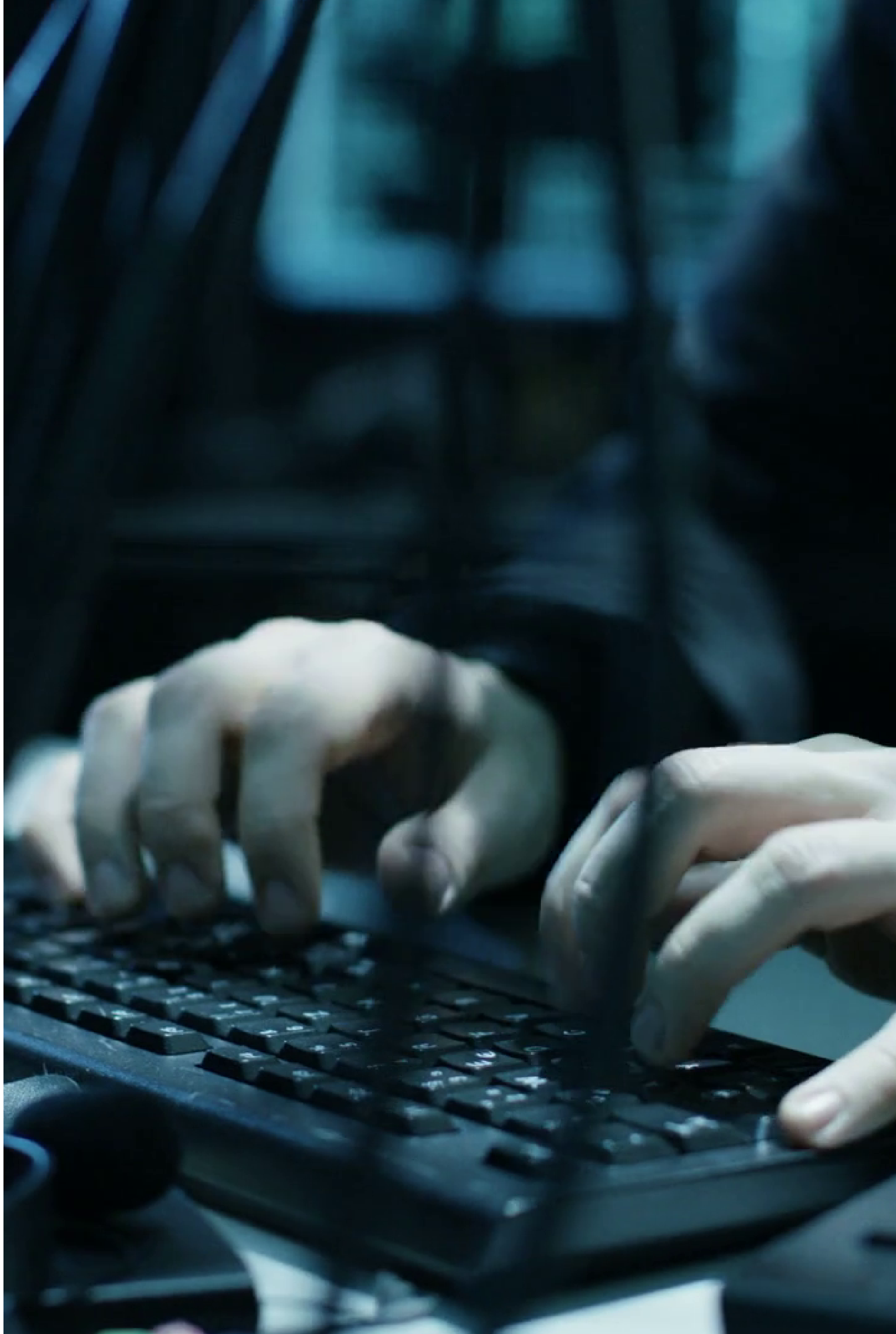
PAULA DE LA HOZ GARRIDO

- SECURITY AUDITOR
- COMPUTER ENGINEERING
- JOURNALISM
- INTERFERENCIAS

@TERCERANEXUS6

OUTLINE

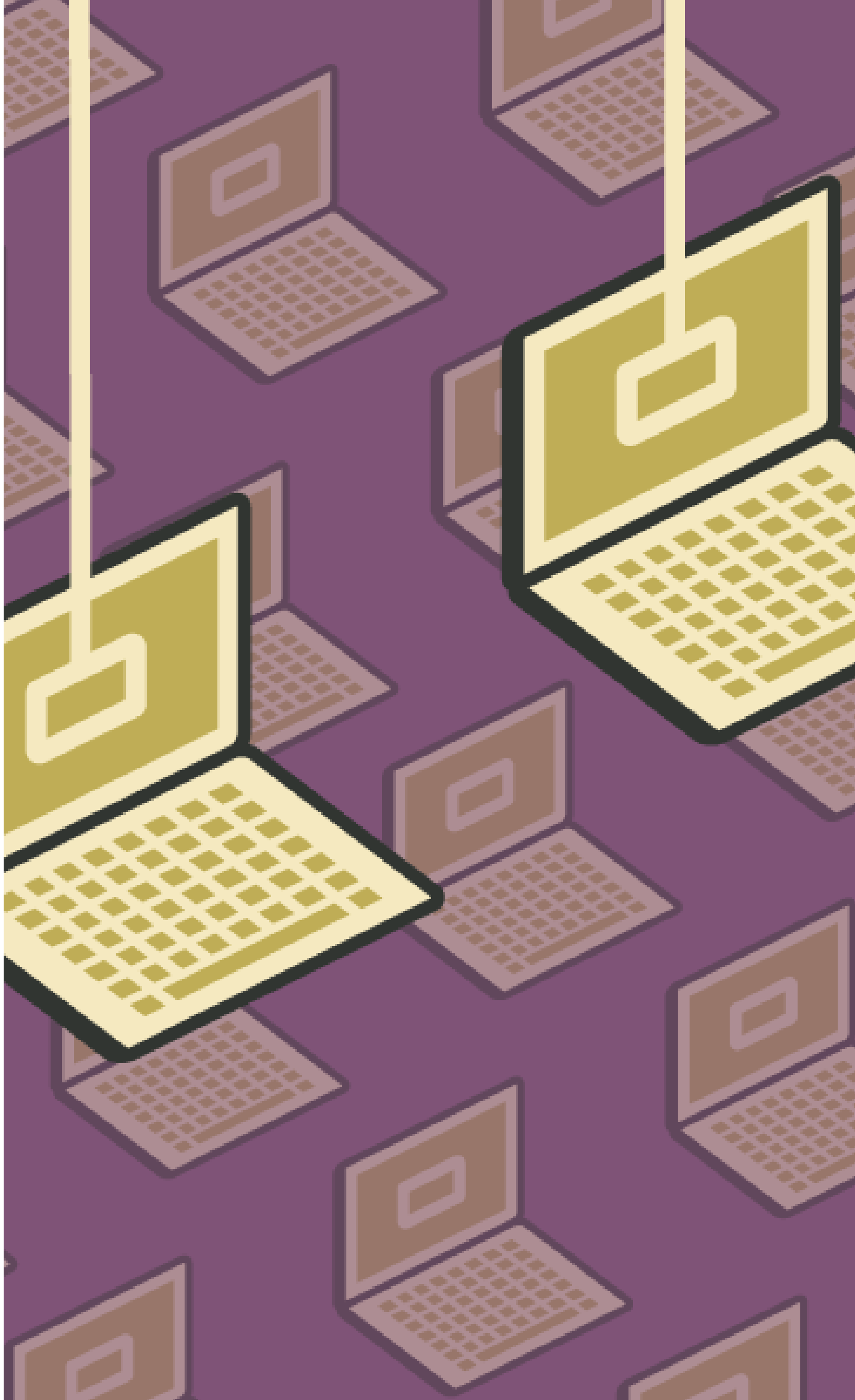
- INTRO: WHY OPEN?
- NETWORK MONITORING
- DISAGGREGATED HARDWARE
- NETWORK VIRTUALIZATION
- COLLABORATIVE HACKING
- QUESTIONS



01

WHY OPEN?

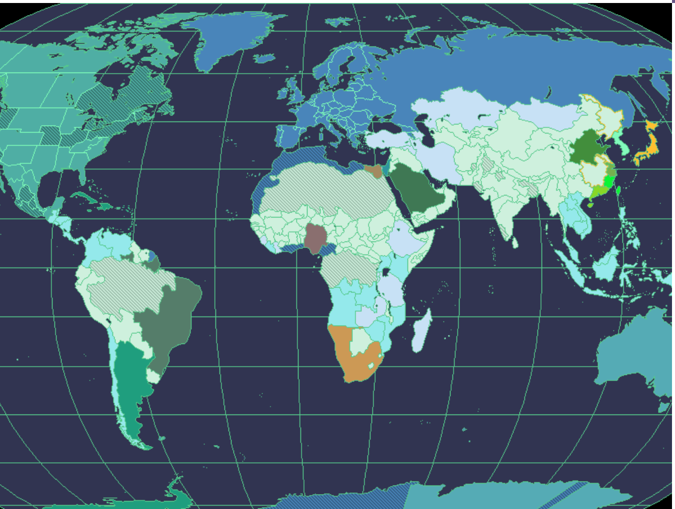
FREEDOM OF THE SOFTWARE, HARDWARE AND MEANS



COLLABORATION CREATE BETTER PROJECTS, ALSO IN SECURITY.

RESPONSIBILITY OF THE COMMUNITY, UNDERSTANDING OF THE TECH.

ACCESSIBLE TECHNOLOGY, FOR EVERYONE.

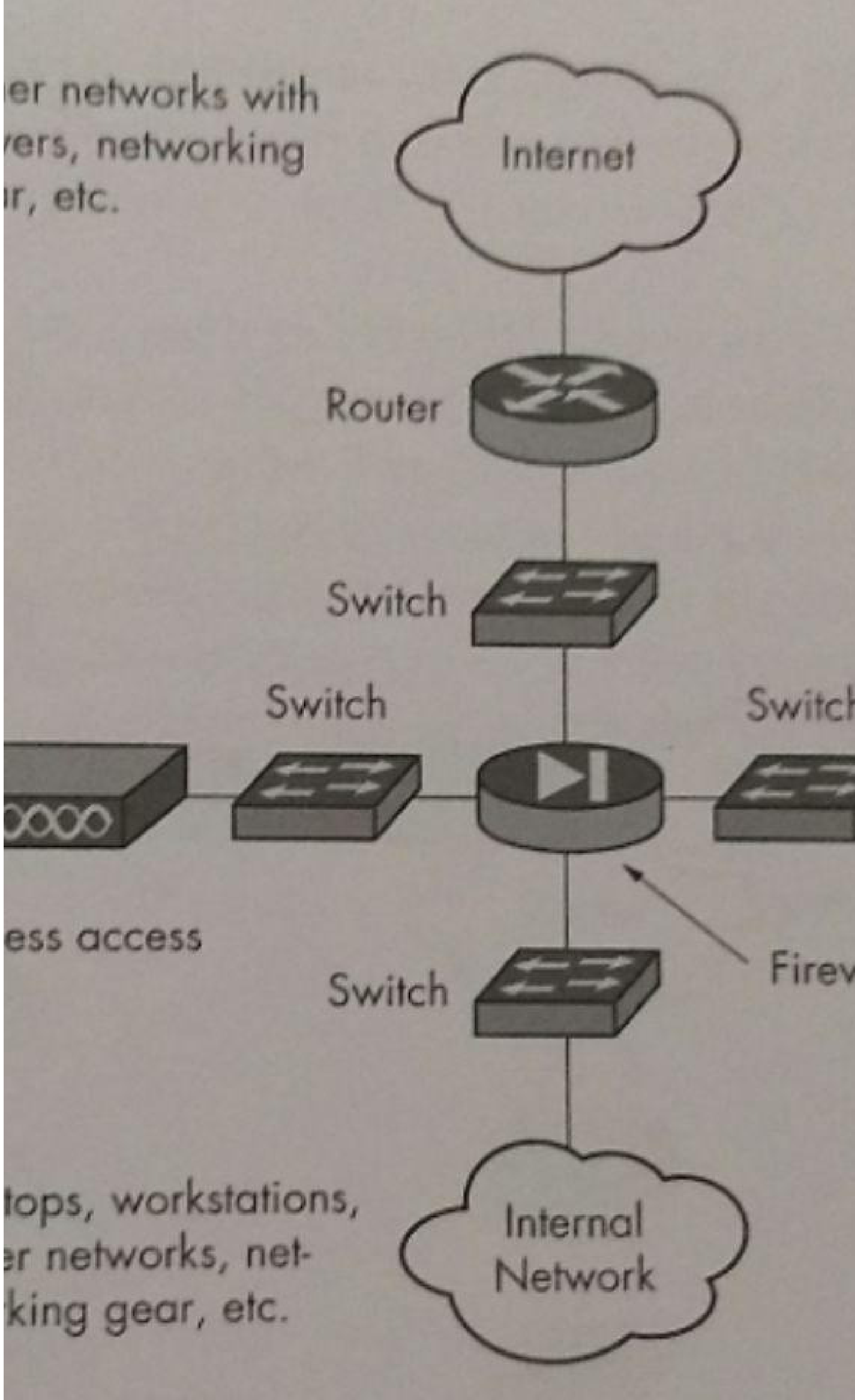


OBFUSCATION IS NOT SECURITY.

02

NETWORK MONITORING

CONTROL, PREVENTION AND ACTIONS



TOOLS AND RESOURCES

GETTING THE FILES

Wireshark, ettercap, tcpdump + Bro

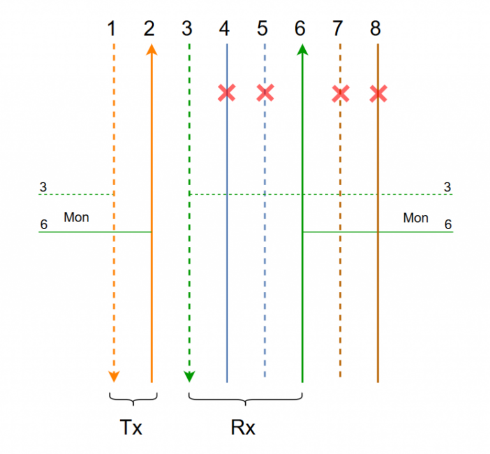
HARDWARE?

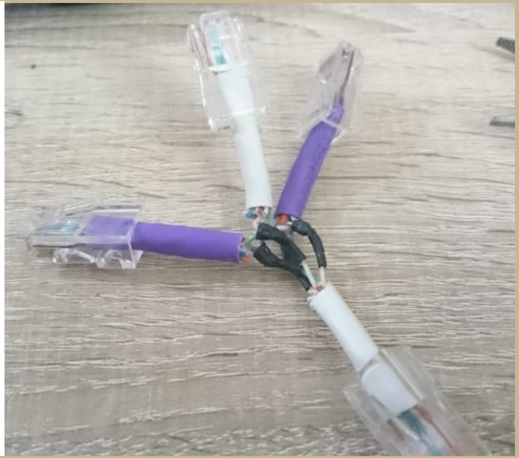
network tap, RPI station, Pineapple, Honeypot...

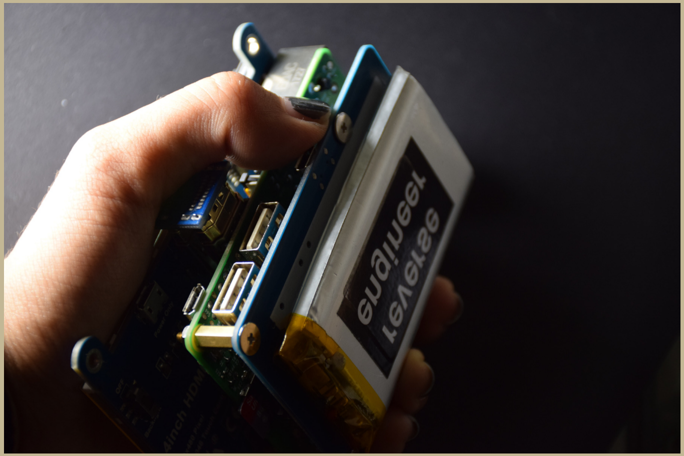
WHAT TO SNIFF?

- context (partial/complete)
- session data
- transaction data
- statistics
- metadata

Depending on what we want we perform different monitoring, and techniques







03

DISAGGREGATED HARDWARE

NEW HORIZONS, FREEDOM OF THE NETWORK

DISAGREGGATED HARDWARE

CHOICE

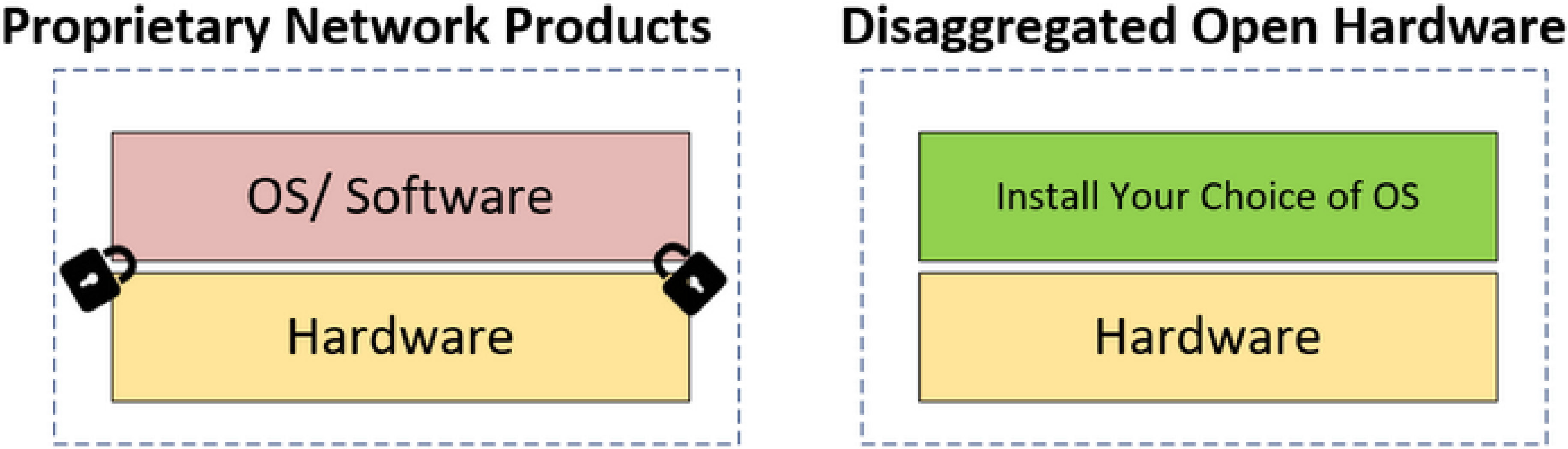
a disaggregated network device allows you to install your choice of operating system.

AN INCIPIENT REVOLUTION

OCP, TIP

EXAMPLES

- Edge-Core AS5712
- Mellanox SN2700
- Alpha Networks SNX-60x0-486F
- Inventec DCS7032Q28

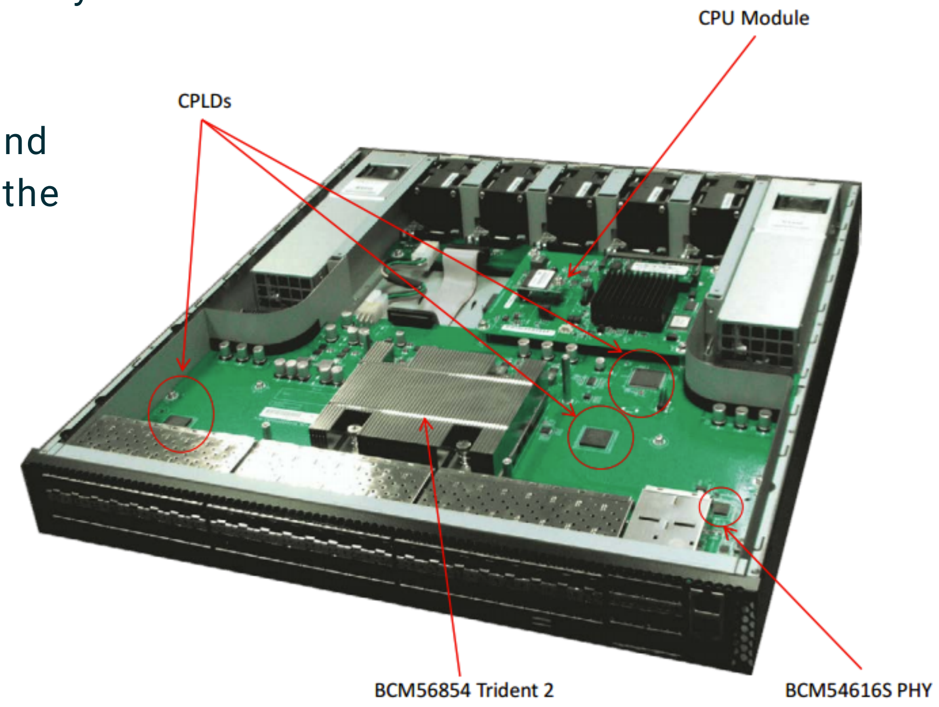

Proprietary Network Products
OS/ Software
Hardware
Disaggregated Open Hardware
Install Your Choice of OS
Hardware

HOW ETHERNET SWITCHES ARE BUILT

there are very few companies worldwide producing merchant Ethernet switch chipset (Silicon). A merchant silicon is a chipset that is already designed, tested and built by a chipset manufacturer, which can be bought by anyone looking to build an Ethernet switch.

An Ethernet switch hardware has a simple design and components. In simple terms, a switch consists of the following components:

- Chassis
- Power supplies
- Fans
- To control fans, system management.
- CPU PCBA
- Switch main board PCBA



04

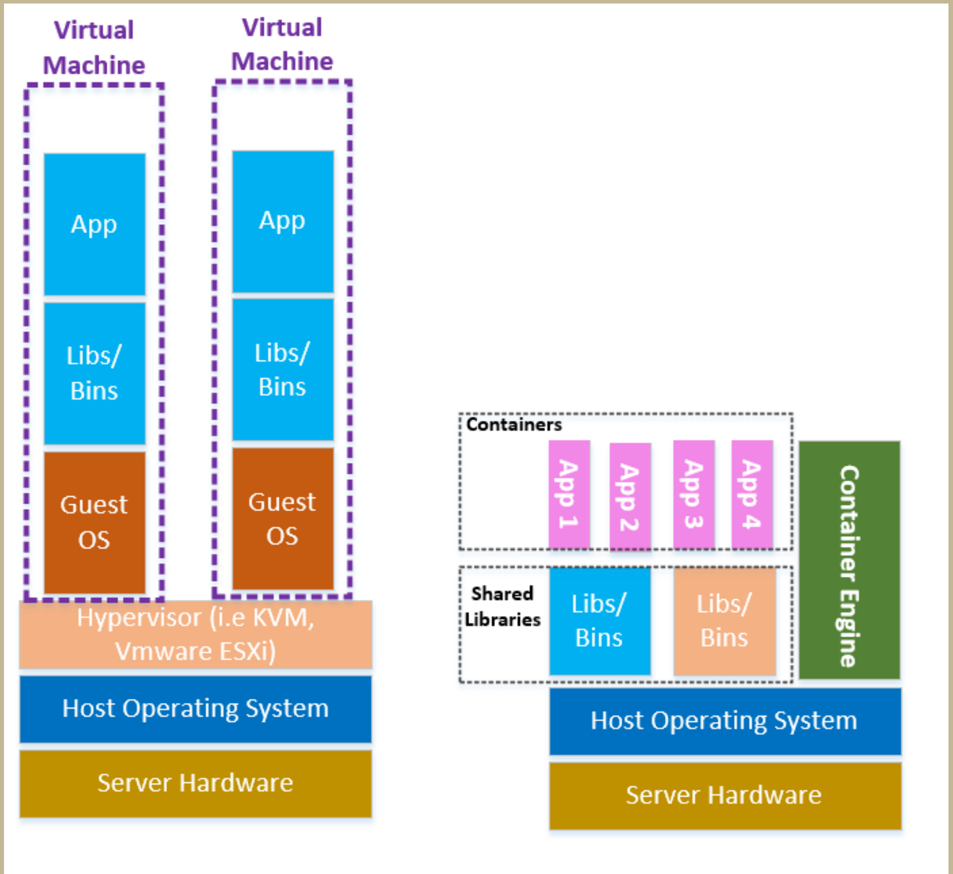
NETWORK VIRTUALIZATION

COMMUNICATION BETWEEN VIRTUAL MACHINES OR CONTAINERS WITHIN A COMPUTE HOST.

MAKE IT VIRTUAL!

LINUX

Network virtualization includes virtual networks that only exist within a host , as well as technologies that allow communication between Linux bridges of multiple hosts.



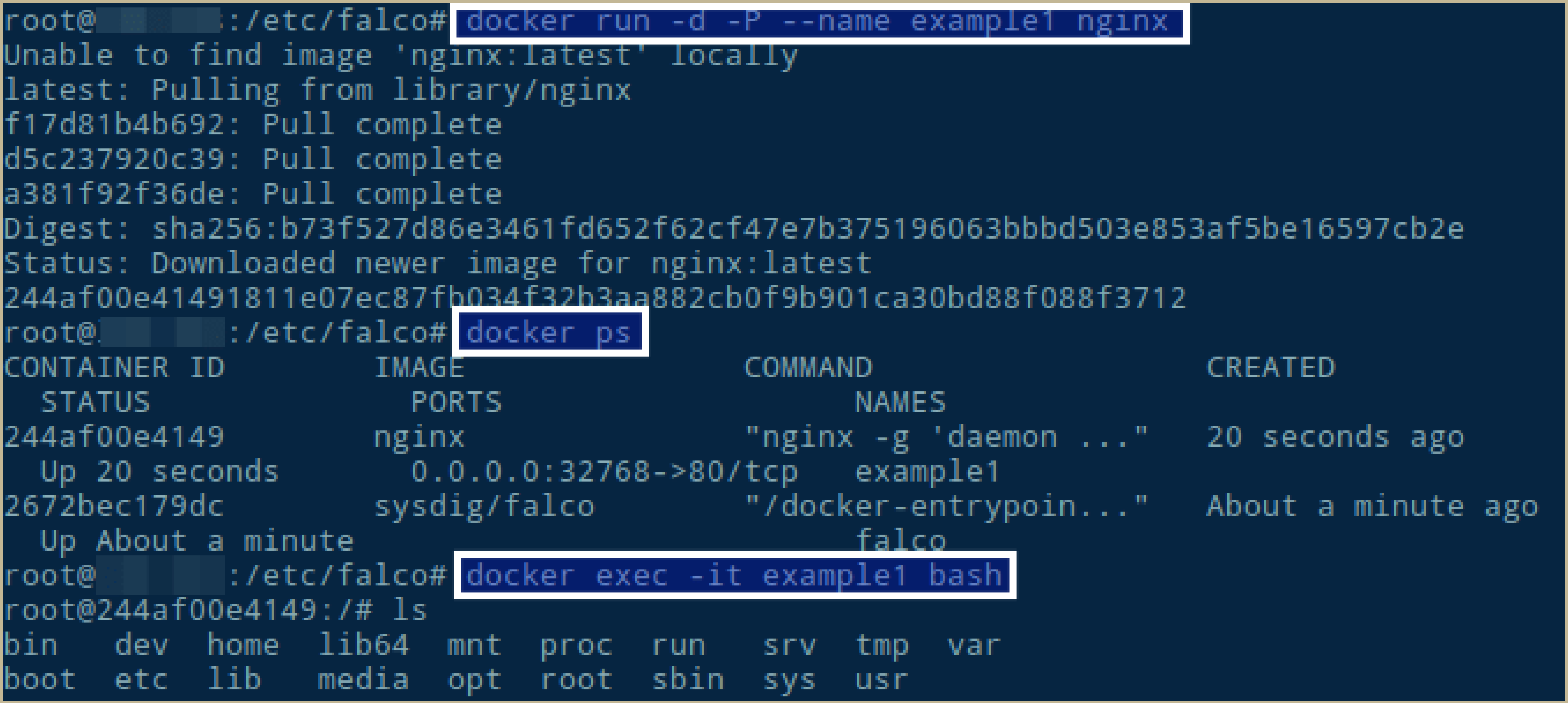
Virtual Machines VS Containers

CONTAINERS

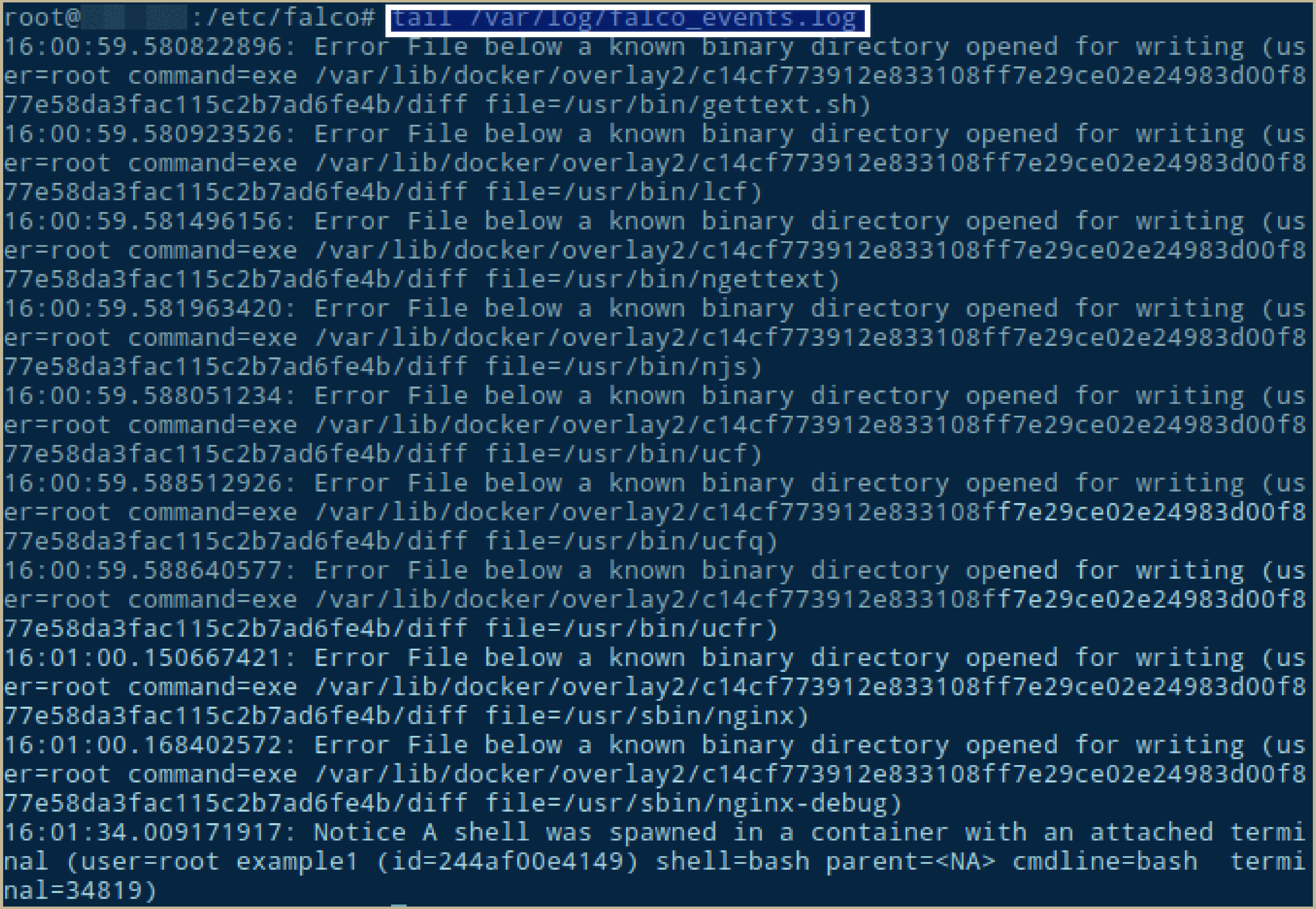
- Containerization is a method for running multiple isolated Linux systems (containers) on a control host using a single Linux kernel.

MONITORING WITH FALCO

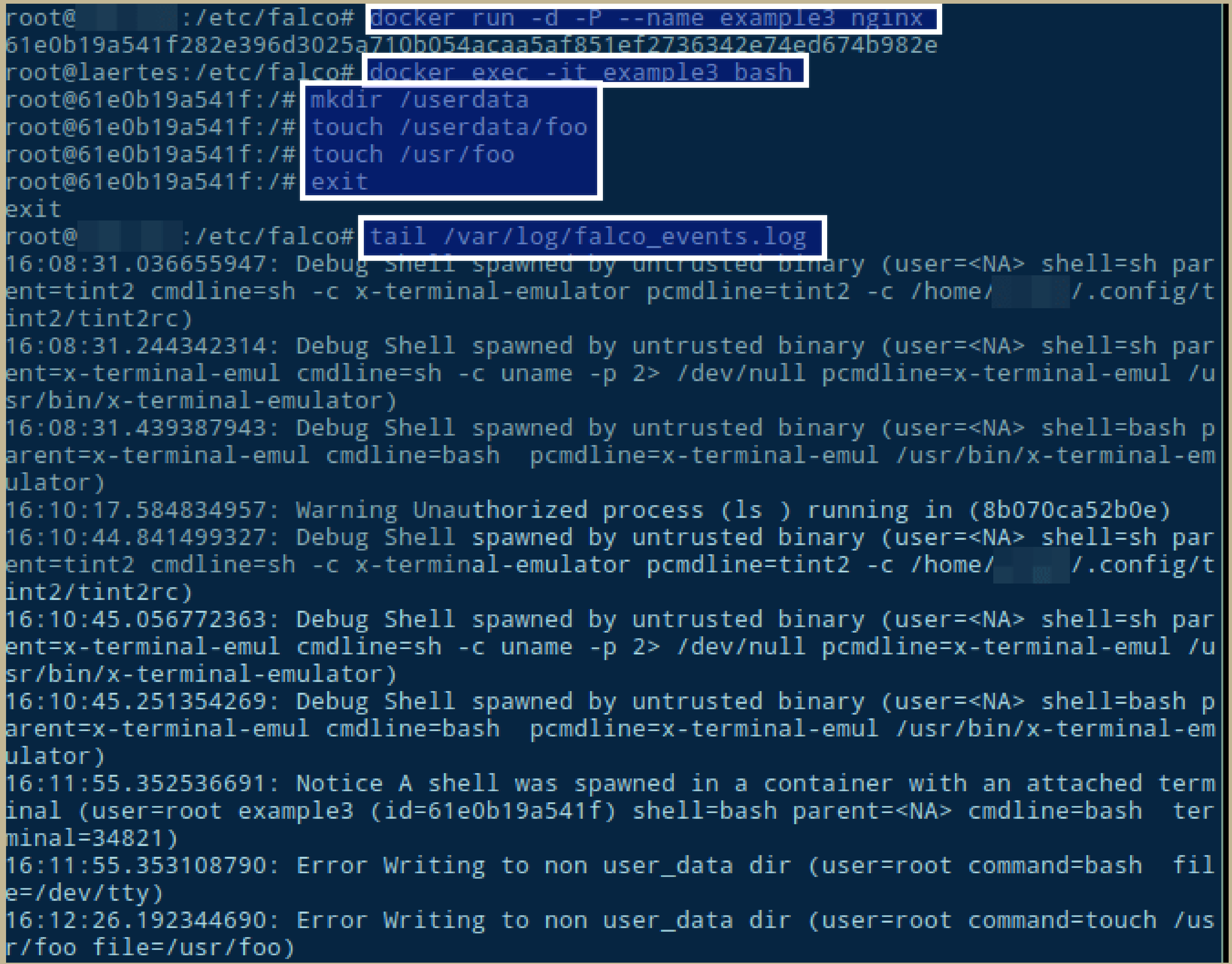
monitor behavioral activity and detect anomalous activity in applications.



```
root@[redacted]:/etc/falco# docker run -d -P --name example1 nginx
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
f17d81b4b692: Pull complete
d5c237920c39: Pull complete
a381f92f36de: Pull complete
Digest: sha256:b73f527d86e3461fd652f62cf47e7b375196063bbbd503e853af5be16597cb2e
Status: Downloaded newer image for nginx:latest
244af00e41491811e07ec87fb034f32b3aa882cb0f9b901ca30bd88f088f3712
root@[redacted]:/etc/falco# docker ps
CONTAINER ID        IMAGE                COMMAND                  CREATED
  STATUS              PORTS                     NAMES
244af00e4149        nginx                "nginx -g 'daemon ..."   20 seconds ago
  Up 20 seconds       0.0.0.0:32768->80/tcp     example1
2672bec179dc        sysdig/falco         "/docker-entrypoin..."   About a minute ago
  Up About a minute                             falco
root@[redacted]:/etc/falco# docker exec -it example1 bash
root@244af00e4149:/# ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
```



```
root@[redacted]:/etc/falco# tail /var/log/falco_events.log
16:00:59.580822896: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/gettext.sh)
16:00:59.580923526: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/lcf)
16:00:59.581496156: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/ngettext)
16:00:59.581963420: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/njs)
16:00:59.588051234: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/ucf)
16:00:59.588512926: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/ucfq)
16:00:59.588640577: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/bin/ucfr)
16:01:00.150667421: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/sbin/nginx)
16:01:00.168402572: Error File below a known binary directory opened for writing (us
er=root command=exe /var/lib/docker/overlay2/c14cf773912e833108ff7e29ce02e24983d00f8
77e58da3fac115c2b7ad6fe4b/diff file=/usr/sbin/nginx-debug)
16:01:34.009171917: Notice A shell was spawned in a container with an attached termi
nal (user=root example1 (id=244af00e4149) shell=bash parent=<NA> cmdline=bash  termi
nal=34819)
```



```
root@[redacted]:/etc/falco# docker run -d -P --name example3 nginx
61e0b19a541f282e396d3025a710b054acaa5af851ef2736342e74ed674b982e
root@laertes:/etc/falco# docker exec -it example3 bash
root@61e0b19a541f:/# mkdir /userdata
root@61e0b19a541f:/# touch /userdata/foo
root@61e0b19a541f:/# touch /usr/foo
root@61e0b19a541f:/# exit
exit
root@[redacted]:/etc/falco# tail /var/log/falco_events.log
16:08:31.036655947: Debug Shell spawned by untrusted binary (user=<NA> shell=sh par
ent=tint2 cmdline=sh -c x-terminal-emulator pcmdline=tint2 -c /home/[redacted]/.config/t
int2/tint2rc)
16:08:31.244342314: Debug Shell spawned by untrusted binary (user=<NA> shell=sh par
ent=x-terminal-emul cmdline=sh -c uname -p 2> /dev/null pcmdline=x-terminal-emul /u
sr/bin/x-terminal-emulator)
16:08:31.439387943: Debug Shell spawned by untrusted binary (user=<NA> shell=bash p
arent=x-terminal-emul cmdline=bash  pcmdline=x-terminal-emul /usr/bin/x-terminal-em
ulator)
16:10:17.584834957: Warning Unauthorized process (ls ) running in (8b070ca52b0e)
16:10:44.841499327: Debug Shell spawned by untrusted binary (user=<NA> shell=sh par
ent=tint2 cmdline=sh -c x-terminal-emulator pcmdline=tint2 -c /home/[redacted]/.config/t
int2/tint2rc)
16:10:45.056772363: Debug Shell spawned by untrusted binary (user=<NA> shell=sh par
ent=x-terminal-emul cmdline=sh -c uname -p 2> /dev/null pcmdline=x-terminal-emul /u
sr/bin/x-terminal-emulator)
16:10:45.251354269: Debug Shell spawned by untrusted binary (user=<NA> shell=bash p
arent=x-terminal-emul cmdline=bash  pcmdline=x-terminal-emul /usr/bin/x-terminal-em
ulator)
16:11:55.352536691: Notice A shell was spawned in a container with an attached term
inal (user=root example3 (id=61e0b19a541f) shell=bash parent=<NA> cmdline=bash  ter
minal=34821)
16:11:55.353108790: Error Writing to non user_data dir (user=root command=bash  fil
e=/dev/tty)
16:12:26.192344690: Error Writing to non user_data dir (user=root command=touch /us
r/foo file=/usr/foo)
```

attacking/defending

THE CONTAINER

- Scanning for vulnerabilities using CoreOS Clair
- Using seccomp for setting rules
- Hashicorp for storing "secrets"

05

COLLABORATIVE HACKING

HACKERS ARE NOT MEANT TO BE LONE WOLVES...

SECURITY OF THE USERS

THIS IS NOT ABOUT YOU,
this is about community. The name "hacker" was firstly created for those who learnt, experiment and created together in tech. Now it's all about secure the internet, secure the users. It must keep the community point.

KEEP THE REVOLUTION

Working in community, and cybersec extends to more than using open source. It's a way of standing up against the main problems.

Questions?

Thank you!