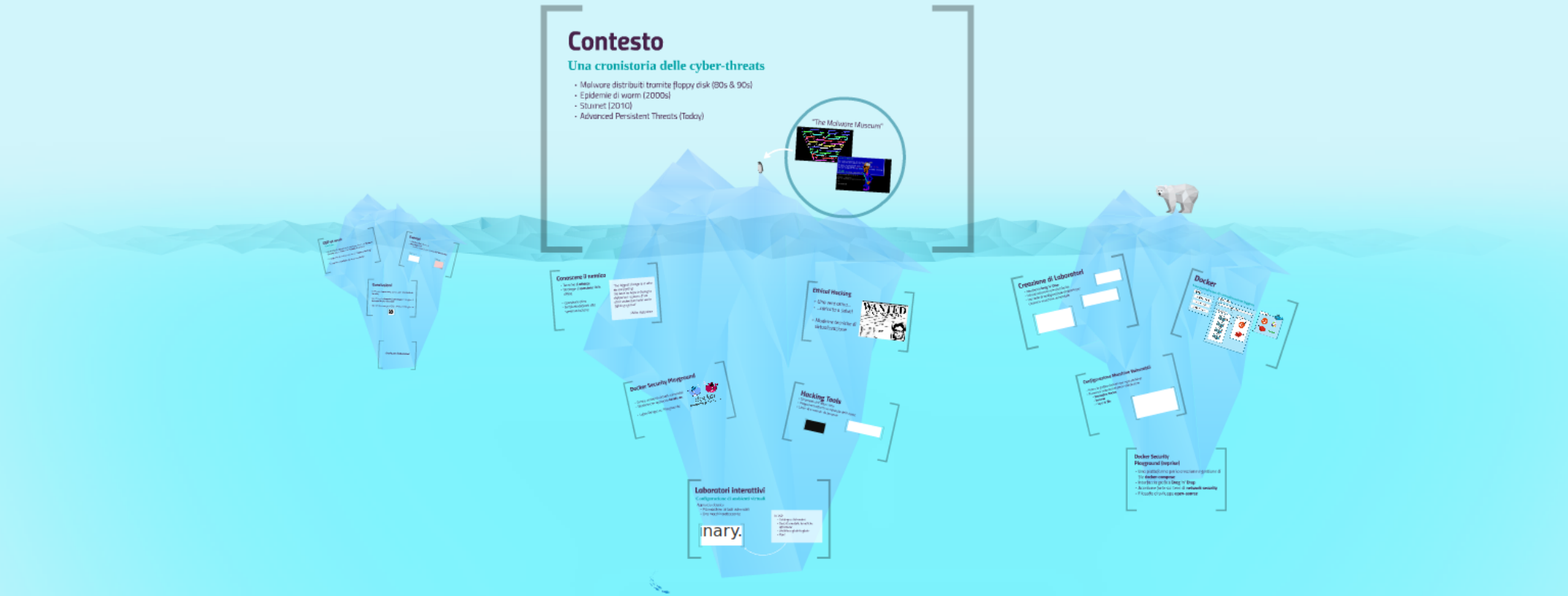
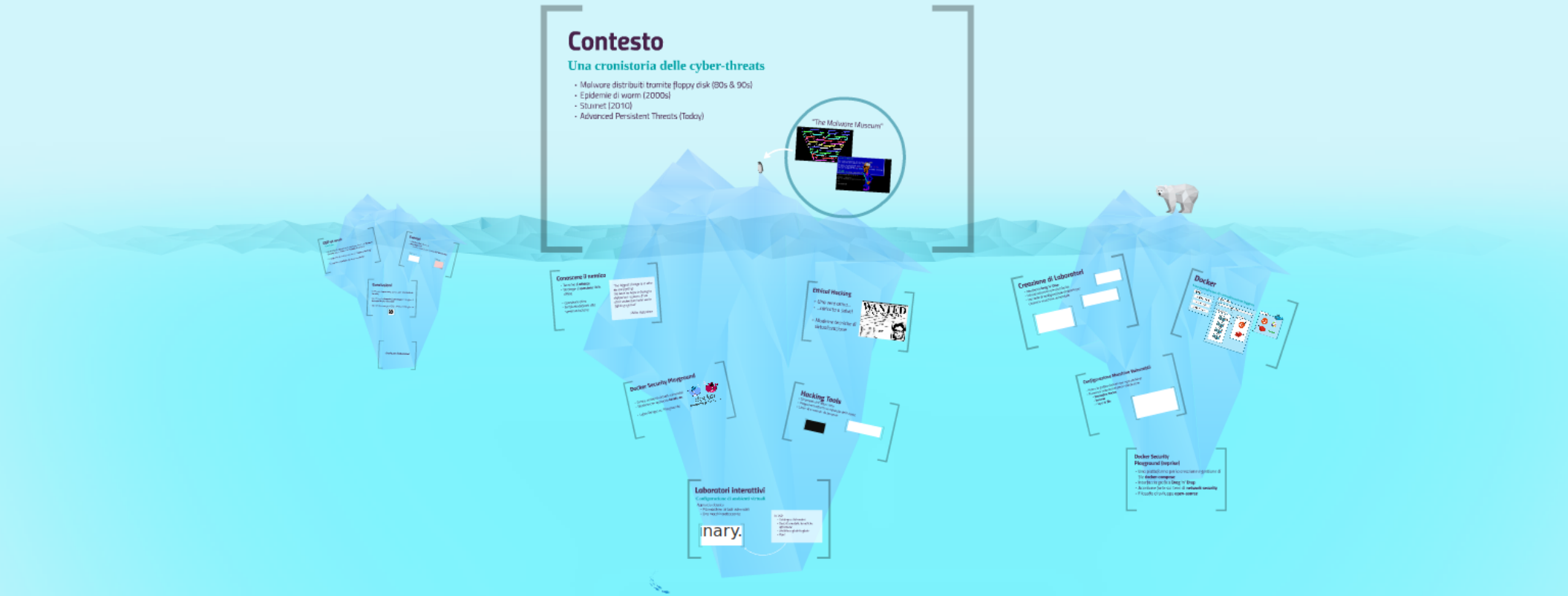


Docker Security Playground

Un framework a microservizi per la realizzazione di scenari di attacco su infrastrutture di rete virtualizzate

Francesco Caturano, Borsista GARR
francesco.caturano@unina.it



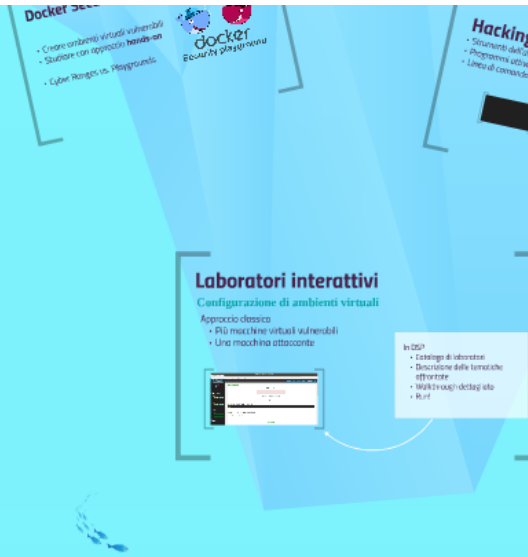
Docker Security Playground

Un framework a microservizi per la realizzazione di scenari di attacco su infrastrutture di rete virtualizzate

Francesco Caturano, Borsista GARR
francesco.caturano@unina.it

Francesco Caturano, Borsista GARR

francesco.caturano@unina.it



docker
Security playground

Docker Security Playground

Un framework a microservizi per la realizzazione di scenari di attacco su infrastrutture di rete virtualizzate

Contesto

Una cronistoria delle cyber-threats

- Malware distribuiti tramite floppy disk (80s & 90s)
- Epidemie di worm (2000s)
- Stuxnet (2010)
- Advanced Persistent Threats (Today)

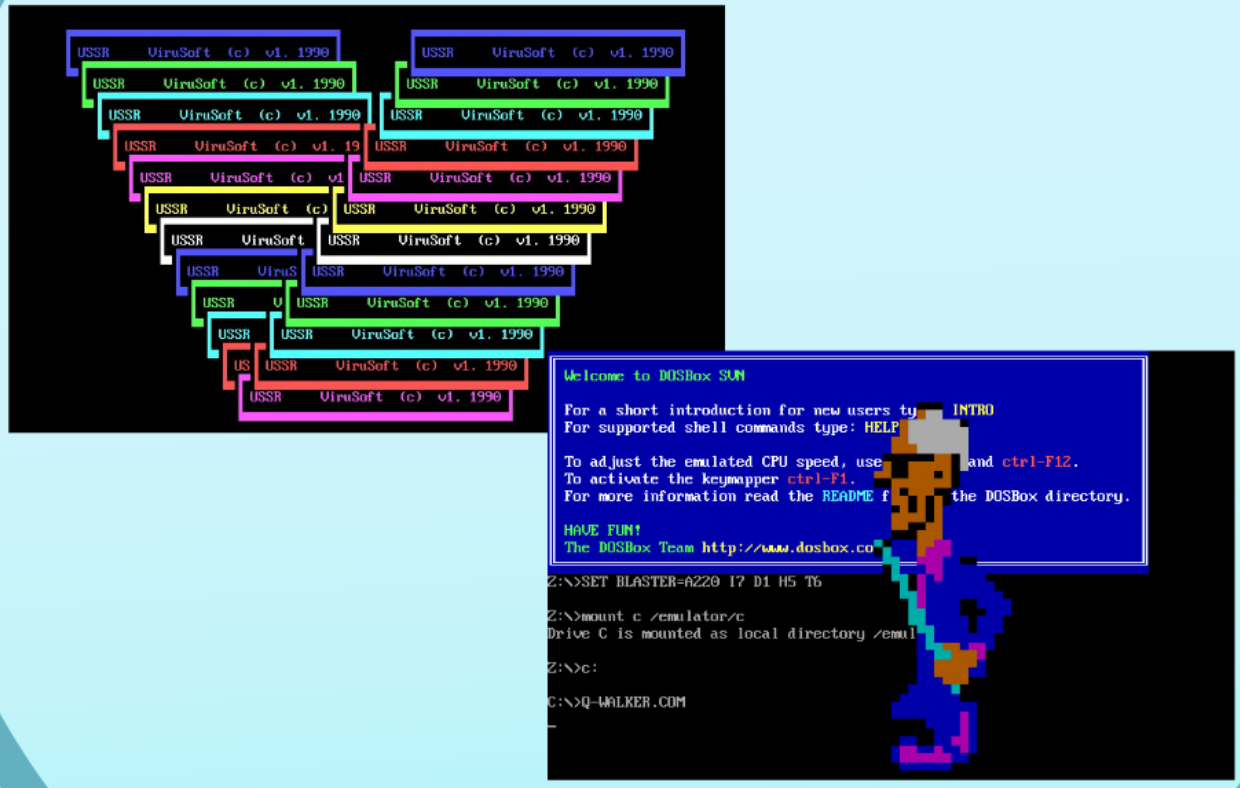
Conoscere il nemico

- Tecniche di attacco
- Strategie di **evasione** delle difese

'The biggest change is in who we are fighting.
We have no hope in trying to

Ethical Hacking

"The Malware Museum"



The Malware Museum"

Contesto

Una cronistoria delle cyber-threats

- Malware distribuiti tramite floppy disk (80s & 90s)
- Epidemie di worm (2000s)
- Stuxnet (2010)
- Advanced Persistent Threats (Today)

Conoscere il nemico

- Tecniche di **attacco**
- Strategie di **evasione** delle difese

- Questione etica
- Ambienti dedicati alla sperimentazione

'The biggest change is in who we are fighting.
We have no hope in trying to defend our systems if we don't understand who we're fighting against'

Mikko Hyppönen

Ethical Hacking

- Una vera arma...
- ...caricata a salve!

- Moderne tecniche di virtualizzazione

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W214660021).

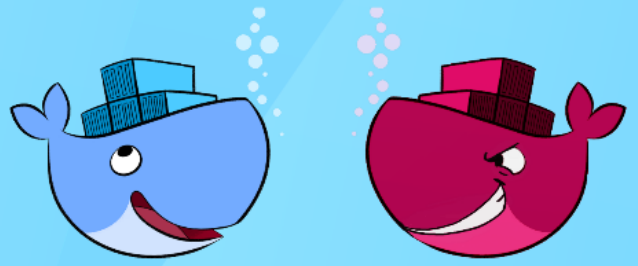
NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN

Docker Security Playground

- Creare ambienti virtuali vulnerabili
- Studiare con approccio **hands-on**

- Cyber Ranges vs. Playgrounds

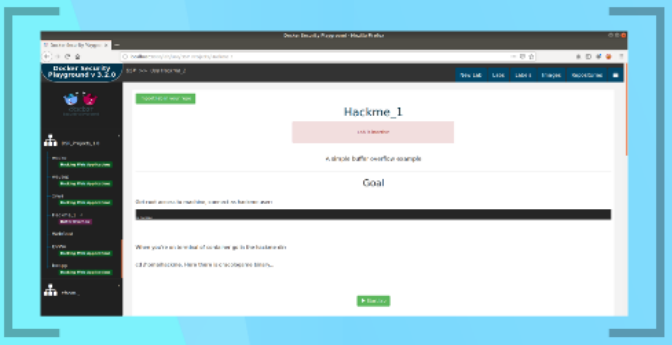


Laboratori interattivi

Configurazione di ambienti virtuali

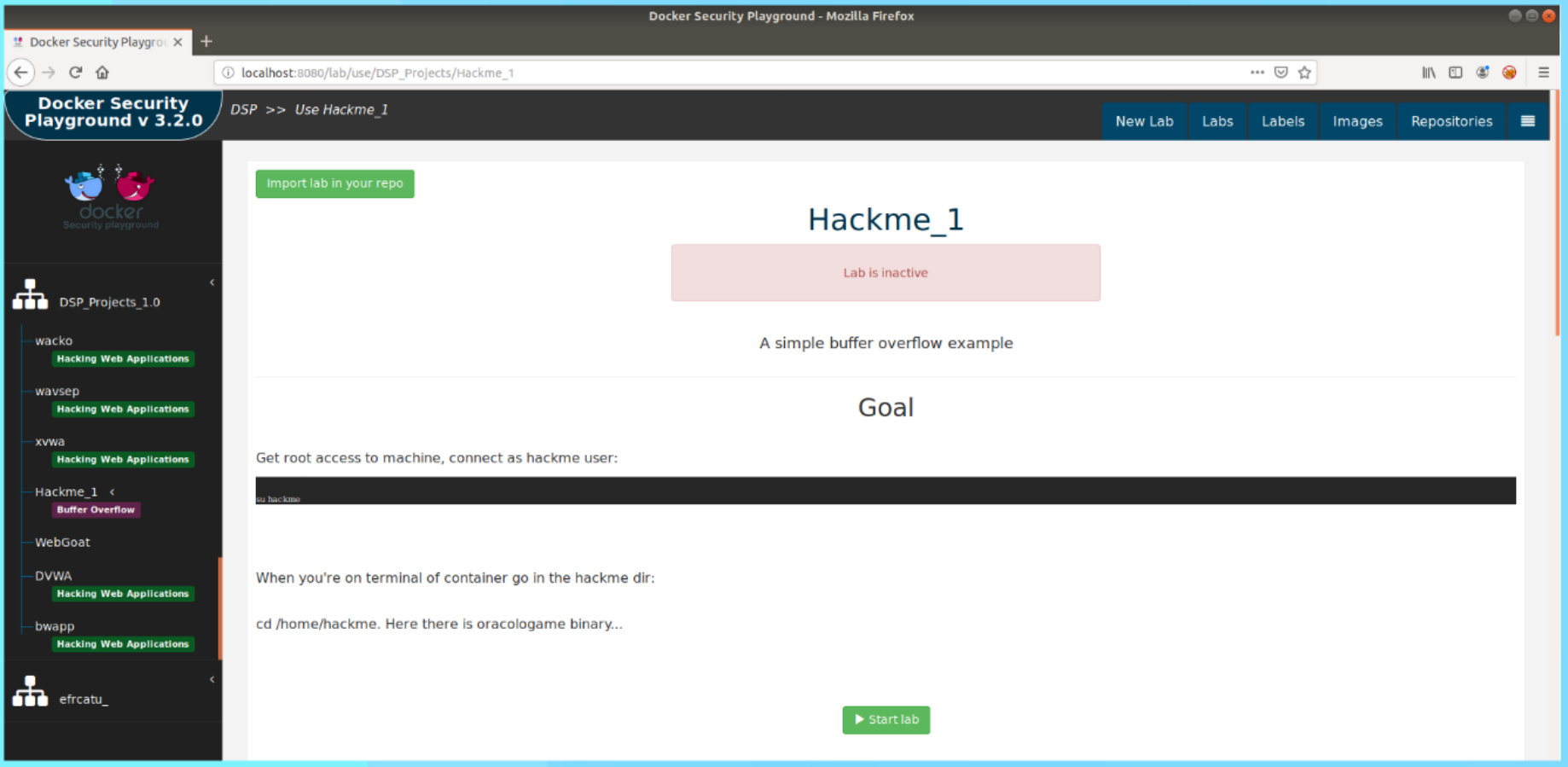
Approccio classico

- Più macchine virtuali vulnerabili
- Una macchina attaccante



In DSP

- Catalogo di laboratori
- Descrizione delle tematiche affrontate
- Walkthrough dettagliato
- Run!


Docker Security Playground - Mozilla Firefox
Docker Security Playgro
localhost:8080/lab/use/DSP_Projects/Hackme_1
Docker Security Playground v 3.2.0
DSP >> Use Hackme_1
New Lab
Labs
Labels
Images
Repositories
docker
Security playground
DSP_Projects_1.0
wacko
Hacking Web Applications
wavsep
Hacking Web Applications
xvwa
Hacking Web Applications
Hackme_1
Buffer Overflow
WebGoat
DVWA
Hacking Web Applications
bwapp
Hacking Web Applications
efrcatu_
Import lab in your repo
Hackme_1
Lab is inactive
A simple buffer overflow example
Goal
Get root access to machine, connect as hackme user:
su hackme
When you're on terminal of container go in the hackme dir:
cd /home/hackme. Here there is oracologame binary...
Start lab

DSP_Projects_1.0

- wacko
  Hacking Web Applications
- wavsep
  Hacking Web Applications
- xvwa
  Hacking Web Applications
- Hackme_1
  Buffer Overflow
- WebGoat
- DVWA
  Hacking Web Applications
- bwapp
  Hacking Web Applications

Import lab in your repo

Get root access to machine, connect as hackme user:

```
su hackme
```

When you're on terminal of container go in the hackme di

cd /home/hackme. Here there is oracologame binary...

New Lab

Hackme_1

Lab is inactive

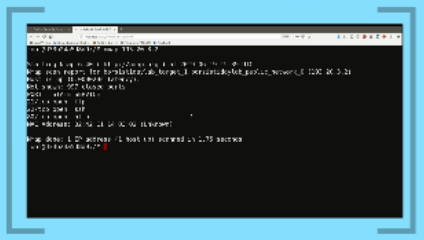
A simple buffer overflow example

Goal

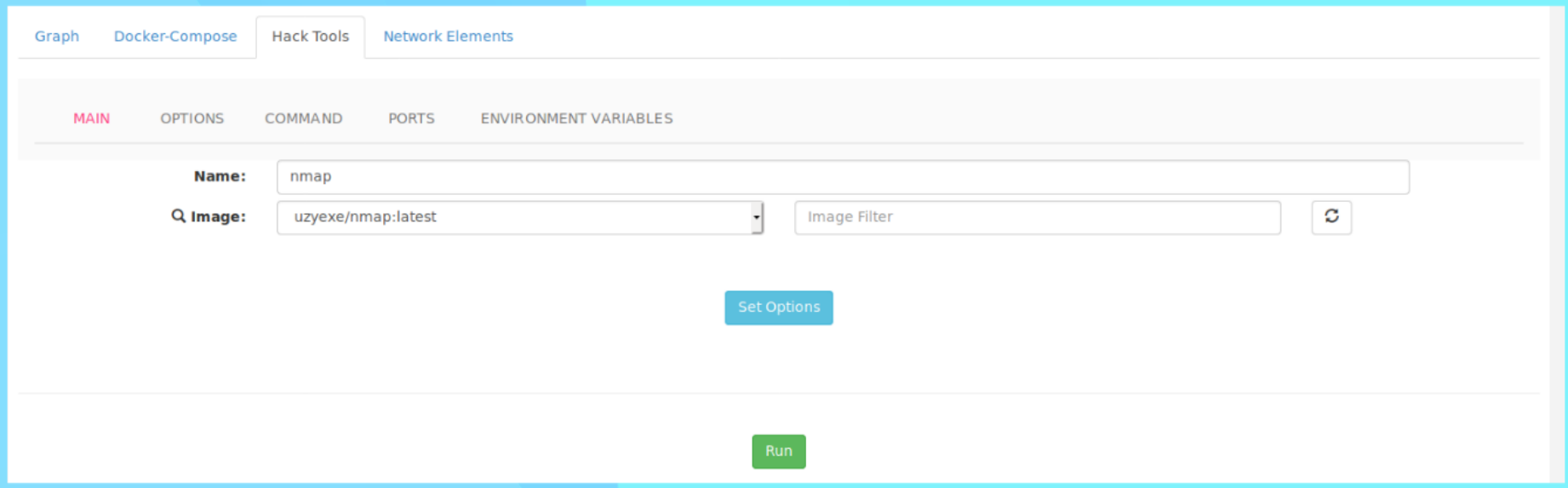
ıser:

Hacking Tools

- Strumenti dell'attaccante
- Programmi attivati su richiesta dell'utente
- Linea di comando da browser



utente



Compose | Hack Tools | Network Elements

PTIONS | COMMAND | PORTS | ENVIRONMENT VARIABLES

Name: nmap

Image: uzyexe/nmap:latest

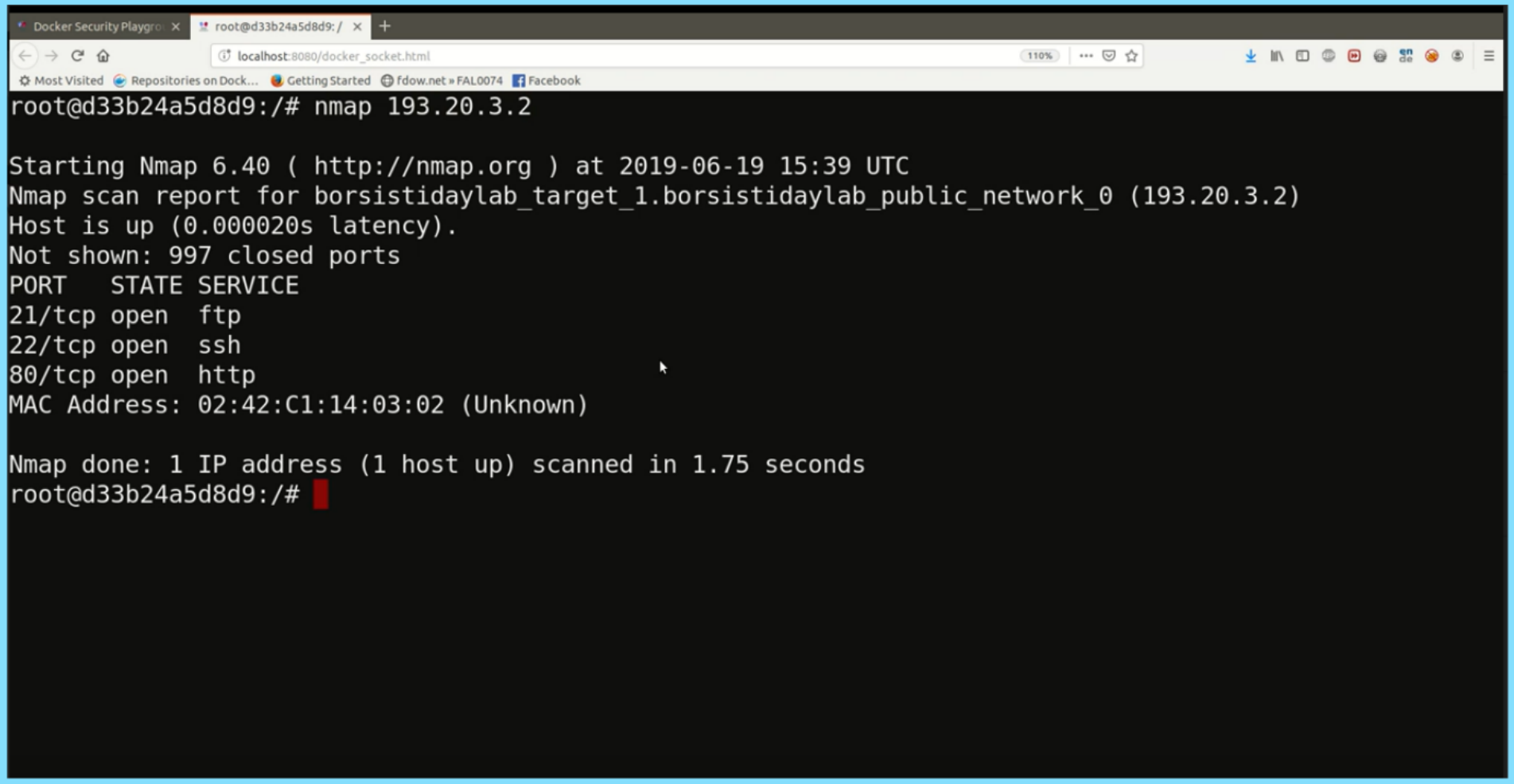
Imag

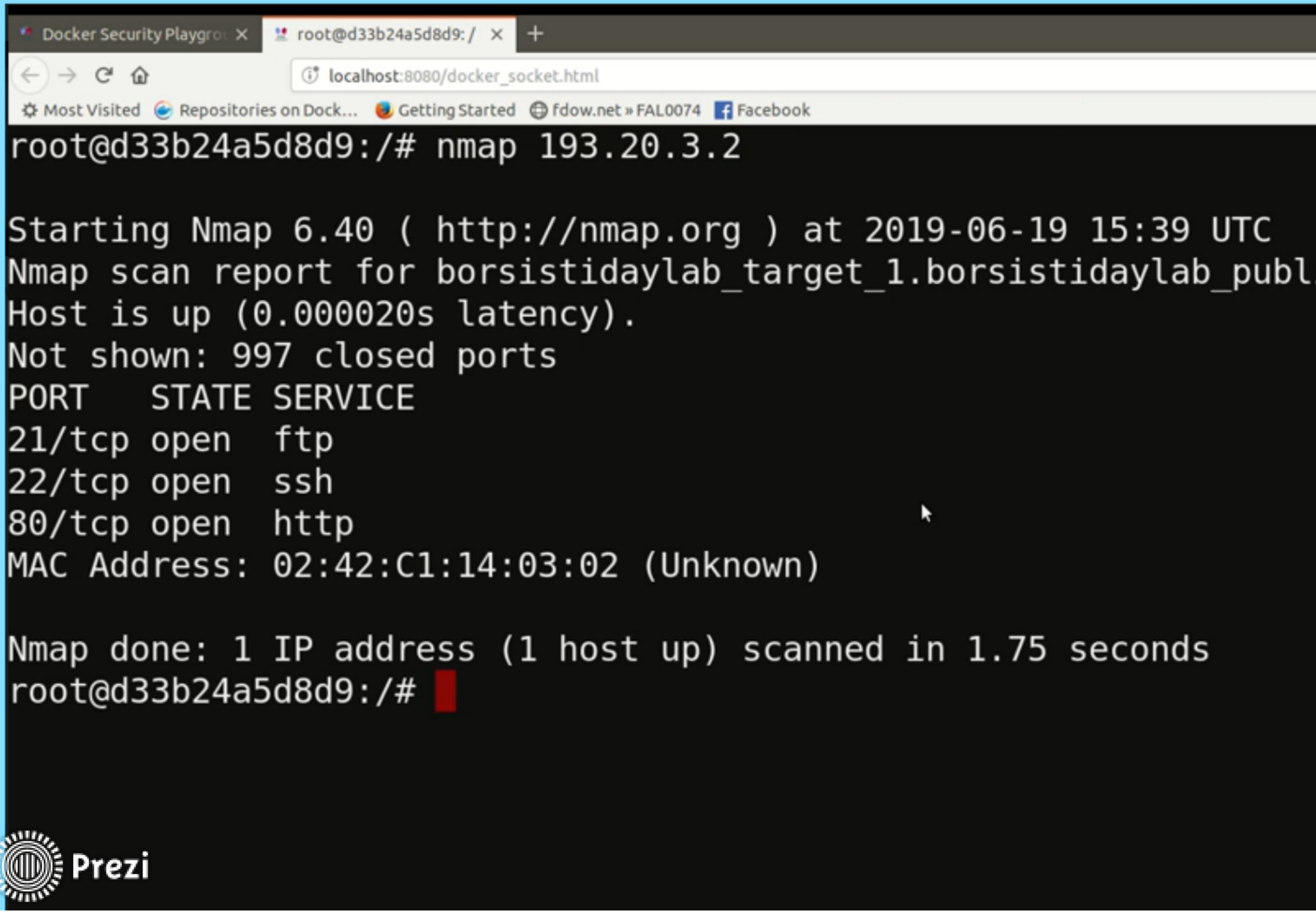
Set Options

Image Filter

Set Options

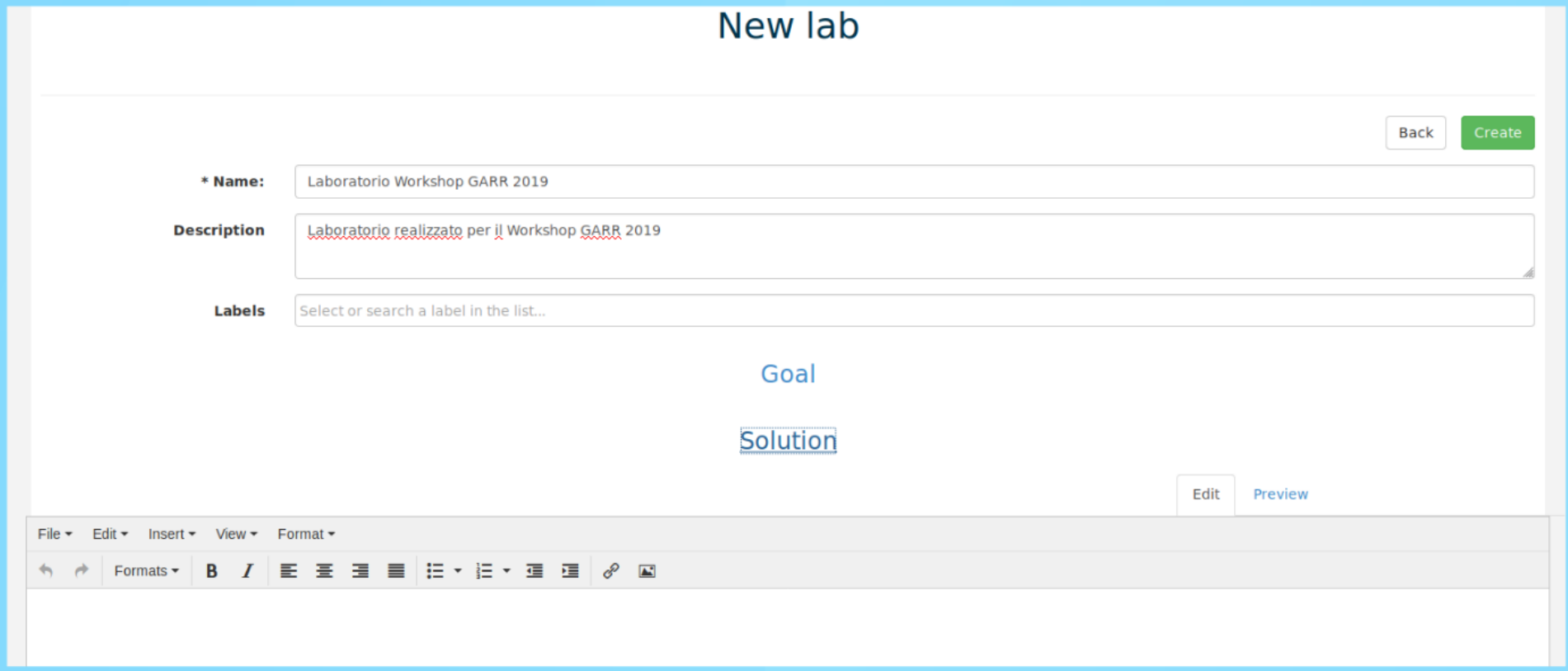
Run


Docker Security Playgro
root@d33b24a5d8d9: /
localhost:8080/docker_socket.html
110%
Most Visited
Repositories on Dock...
Getting Started
fdow.net » FAL0074
Facebook
root@d33b24a5d8d9:/# nmap 193.20.3.2
Starting Nmap 6.40 (http://nmap.org) at 2019-06-19 15:39 UTC
Nmap scan report for borsistidaylab_target_1.borsistidaylab_public_network_0 (193.20.3.2)
Host is up (0.000020s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 02:42:C1:14:03:02 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
root@d33b24a5d8d9:/#


Docker Security Playgro
root@d33b24a5d8d9: /
localhost:8080/docker_socket.html
Most Visited
Repositories on Dock...
Getting Started
fdow.net » FAL0074
Facebook
root@d33b24a5d8d9:/# nmap 193.20.3.2
Starting Nmap 6.40 (http://nmap.org) at 2019-06-19 15:39 UTC
Nmap scan report for borsistidaylab_target_1.borsistidaylab_publ
Host is up (0.000020s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 02:42:C1:14:03:02 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
root@d33b24a5d8d9:/#

Creazione di Laboratori

- Interfaccia **Drag 'n' Drop**
- Infrastruttura di rete distribuita
- Pannello di configurazione dedicato per ciascuna macchina vulnerabile


New lab
Back
Create
* Name:
Laboratorio Workshop GARR 2019
Description
Laboratorio realizzato per il Workshop GARR 2019
Labels
Select or search a label in the list...
Goal
Solution
Edit
Preview
File
Edit
Insert
View
Format
Formats

New lab

*** Name:** Laboratorio Workshop GARR 2019

Description Laboratorio realizzato per il Workshop GARR 2019

Labels Select or search a label in the list...

Goal

Solution

er


Copy
Delete Lab
Edit infos
Laboratorio Workshop
GARR 2019
Laboratorio realizzato per il Workshop GARR 2019
Goal
Create Docker Network
Clear Logs
Graph
Docker-Compose
Hack Tools
Network Elements

Edit infos

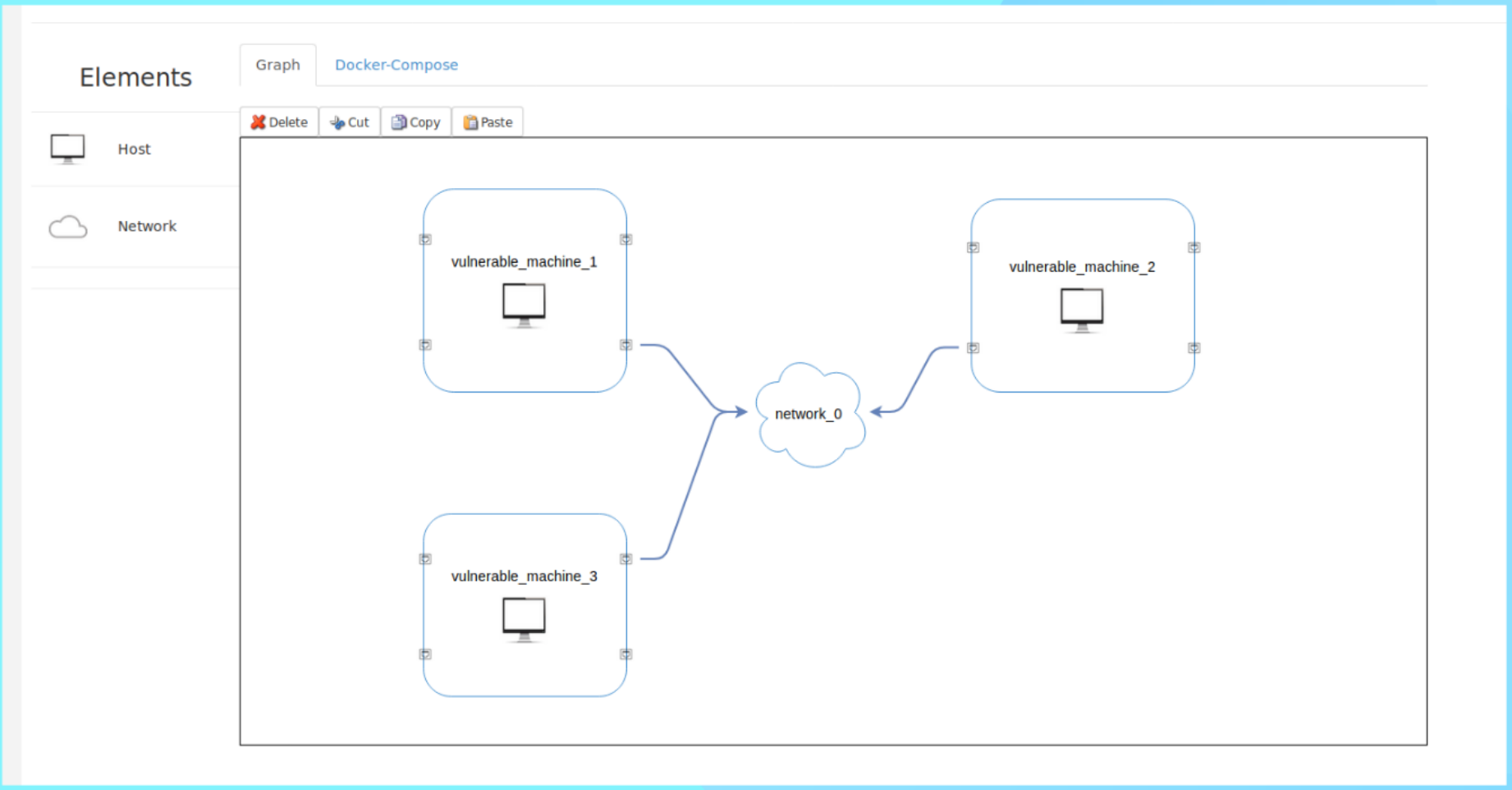
Laboratorio Workshop GARR 2019

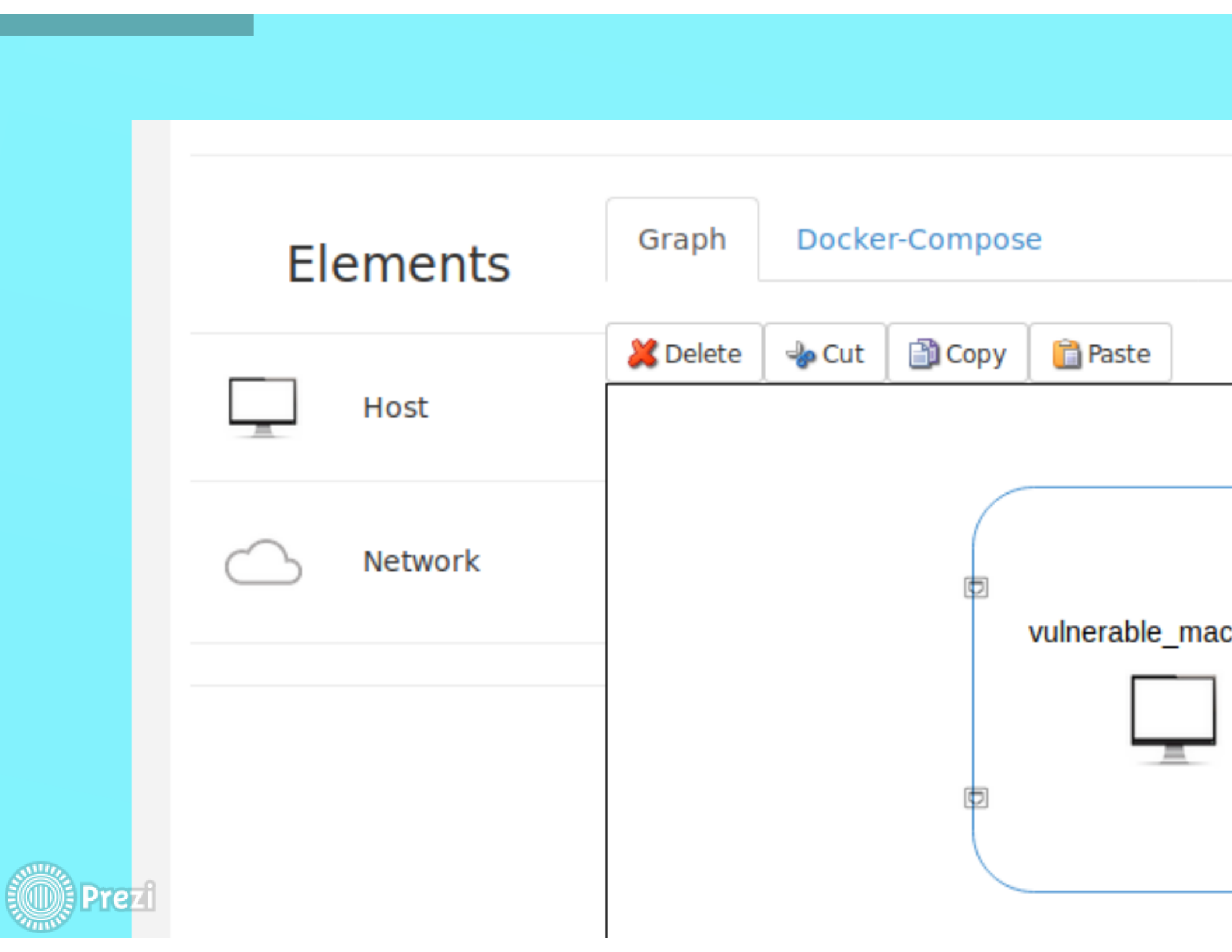
Laboratorio realizzato per il Workshop GARR 2019

Goal

Create Docker Network

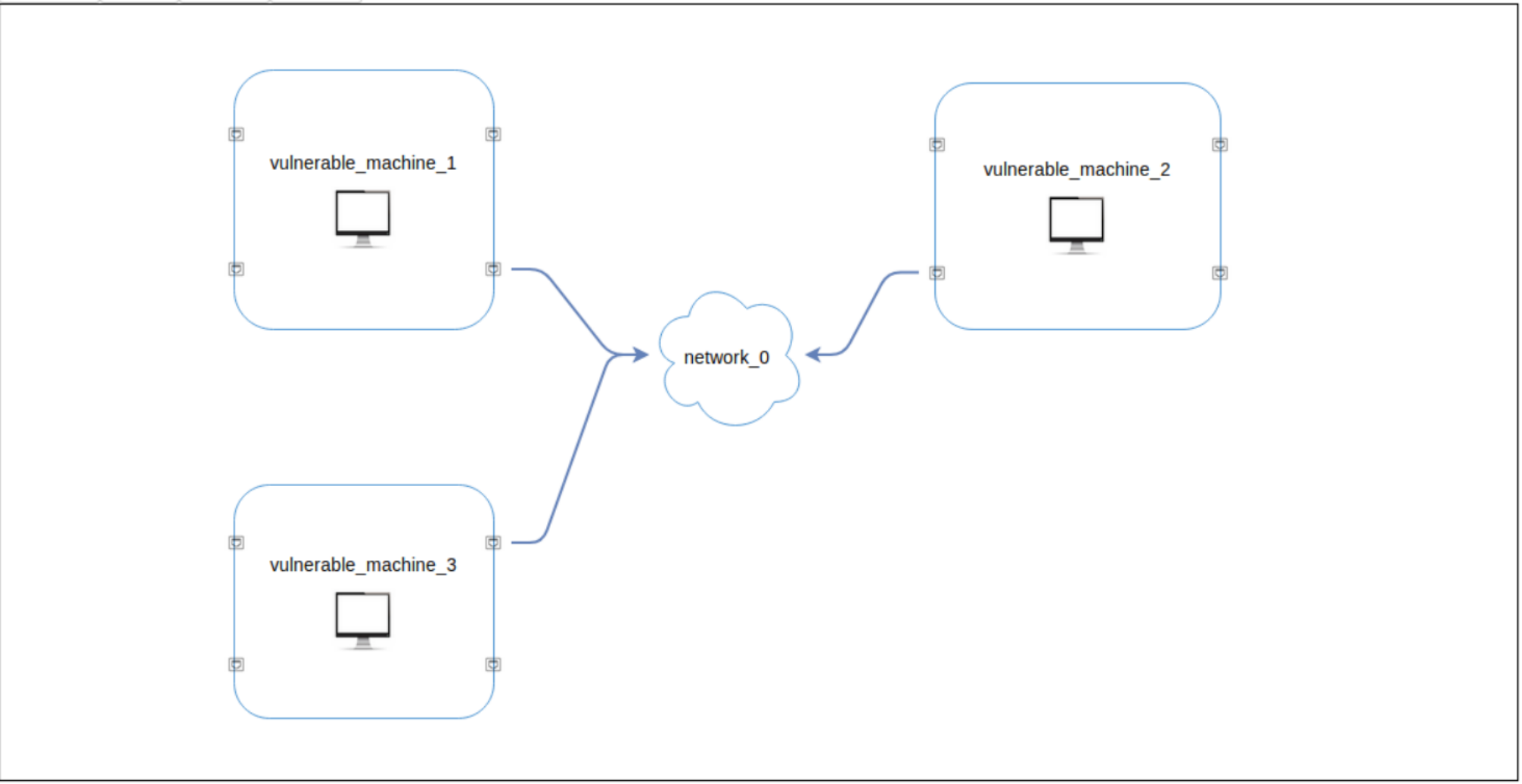
Network Elements


Elements
Graph
Docker-Compose
Delete
Cut
Copy
Paste
Host
Network
vulnerable_machine_1
vulnerable_machine_2
network_0
vulnerable_machine_3


Elements
Graph
Docker-Compose
Delete
Cut
Copy
Paste
Host
Network
vulnerable_mac
Prezi

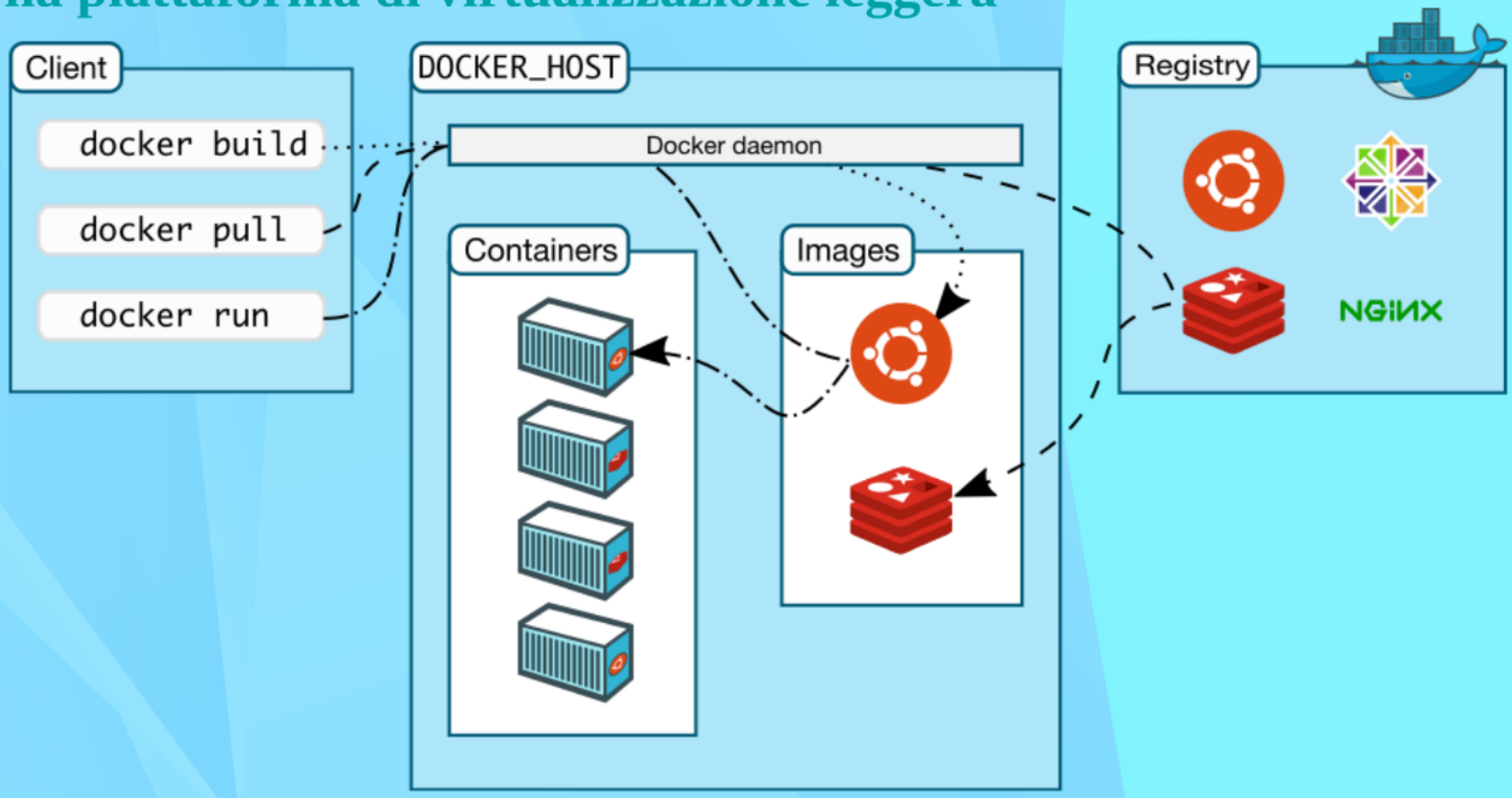
Graph | Docker-Compose

Delete | Cut | Copy | Paste



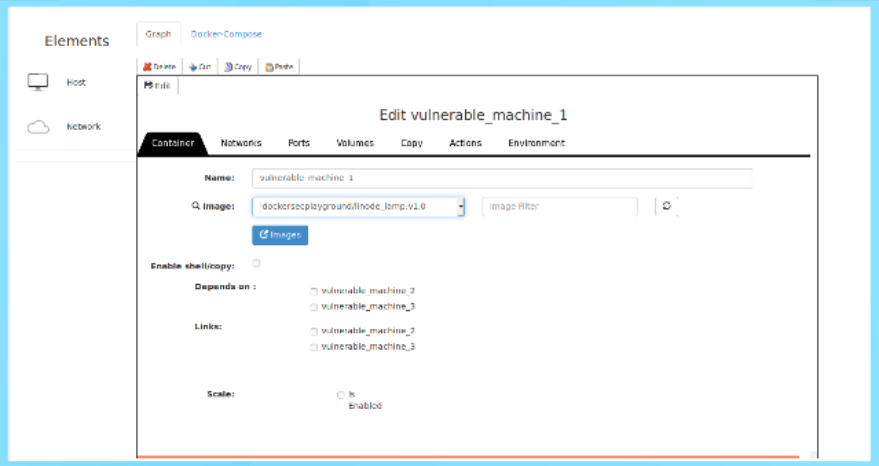
Docker

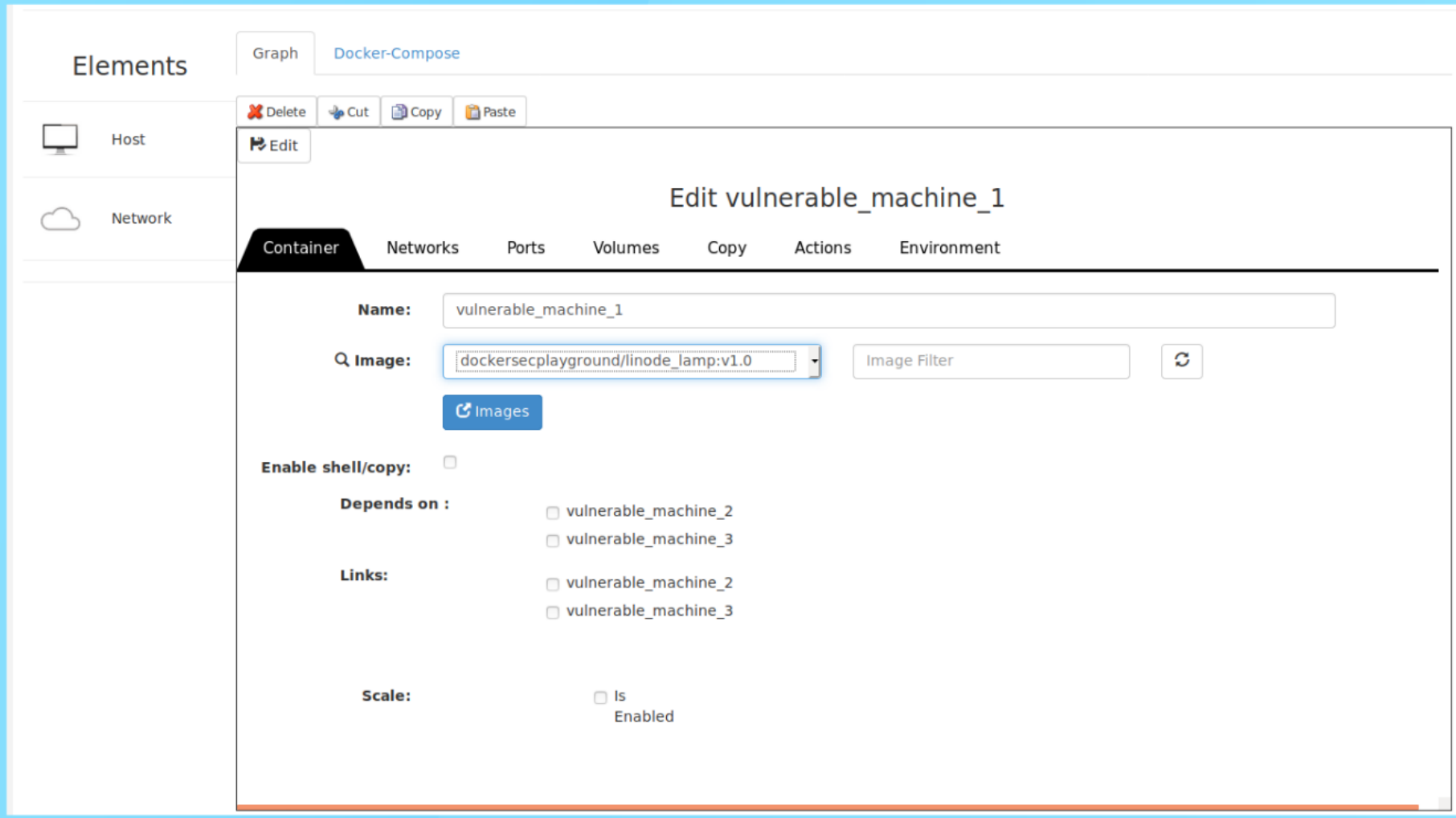
Una piattaforma di virtualizzazione leggera

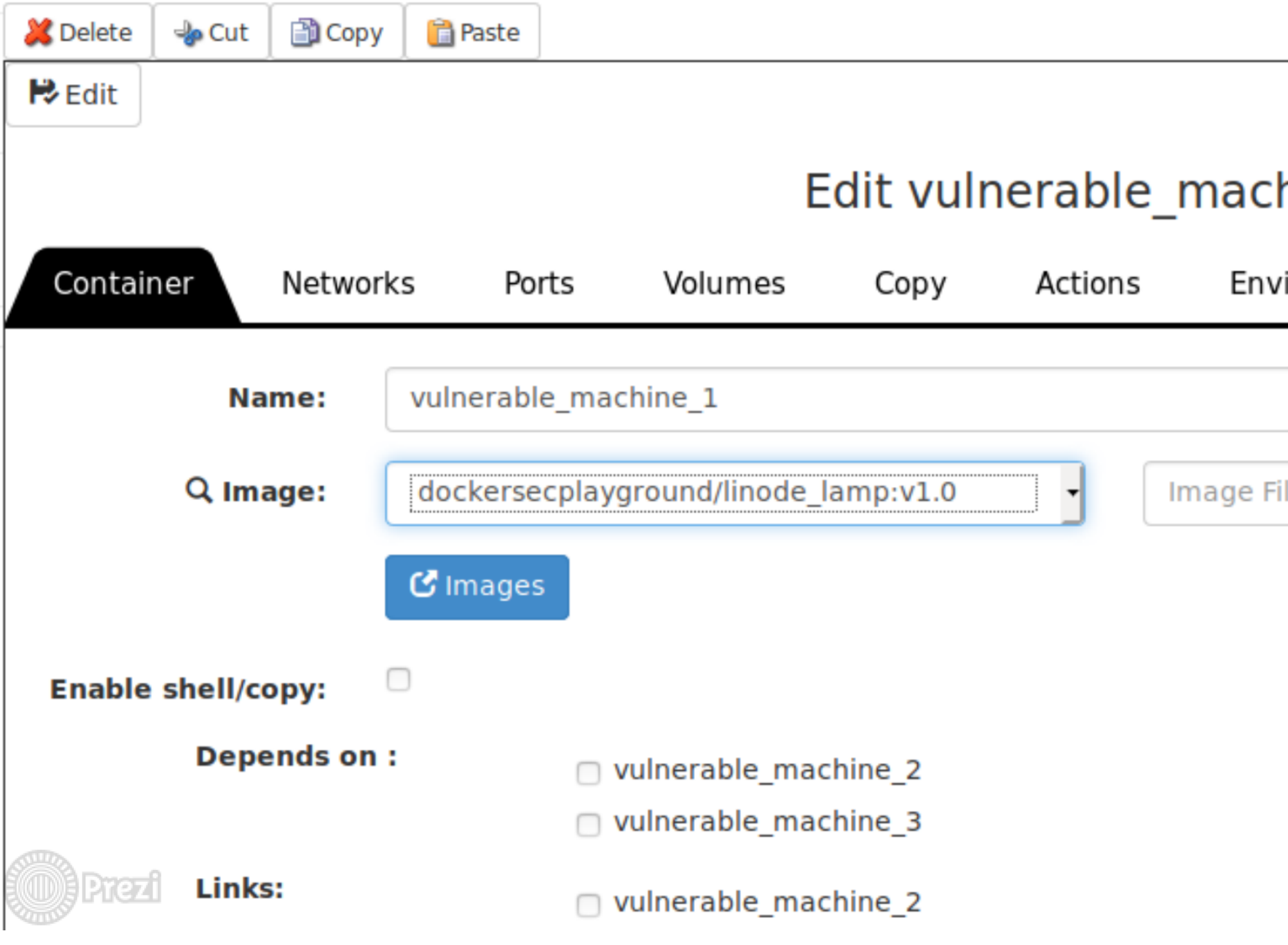


Configurazione Macchine Vulnerabili

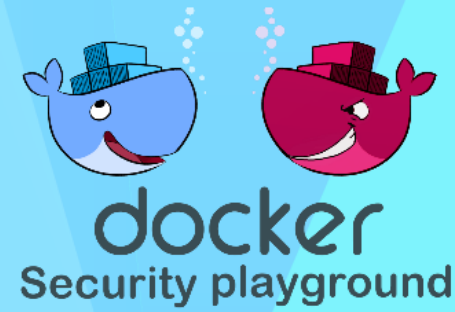
- Pannello grafico dedicato per ogni container
- Numerosi parametri di personalizzazione
  - **Immagine Docker**
  - **Volume**
  - Copia di **file**




Elements
Graph
Docker-Compose
Delete
Cut
Copy
Paste
Host
Edit
Network
Edit vulnerable_machine_1
Container
Networks
Ports
Volumes
Copy
Actions
Environment
Name:
vulnerable_machine_1
Image:
dockersecplayground/linode_lamp:v1.0
Image Filter
Images
Enable shell/copy:
Depends on :
vulnerable_machine_2
vulnerable_machine_3
Links:
vulnerable_machine_2
vulnerable_machine_3
Scale:
Is
Enabled


Delete
Cut
Copy
Paste
Edit
Edit vulnerable_mach
Container
Networks
Ports
Volumes
Copy
Actions
Envi
Name:
vulnerable_machine_1
Image:
dockersecplayground/linode_lamp:v1.0
Image Fil
Images
Enable shell/copy:
Depends on :
vulnerable_machine_2
vulnerable_machine_3
Links:
vulnerable_machine_2

Docker Security Playground (reprise)



- Una piattaforma per la creazione e gestione di file **docker-compose**
- Interfaccia grafica **Drag 'n' Drop**
- Accezione forte sui temi di **network security**
- Filosofia di sviluppo **open-source**

DSP at work

Casi d'uso

- Strumento di supporto esercitativo per il corso di **Network Security** presso l'Università **Federico II** di Napoli
- Piattaforma di creazione di scenari **"Capture The Flag"**
- Incubatore di **testbed** a scopi sperimentativi

Esempi

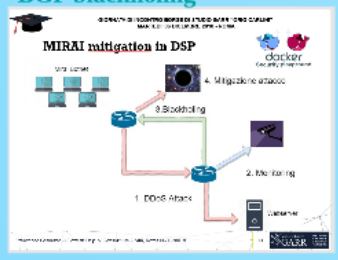
- USA **Black Hat** Lab 2018
- **Mirai-DDoS Lab**
  - tecniche di mitigazione tramite **BGP Blackholing**

Black Hat Las Vegas 2018

Capture The Flags

Mirai DDoS Lab

BGP blackholing

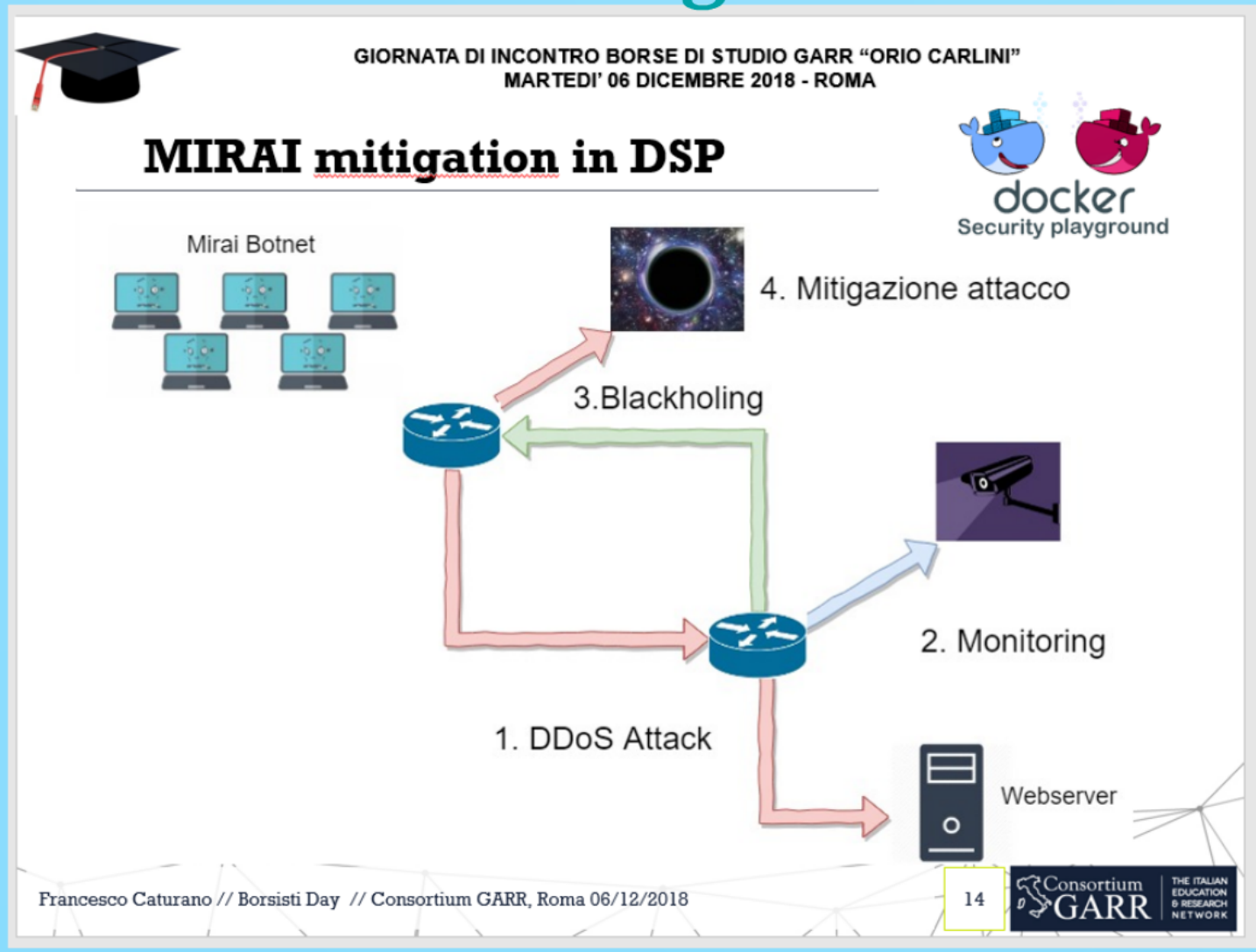


Black Hat Las Vegas 2018

Capture The Flags

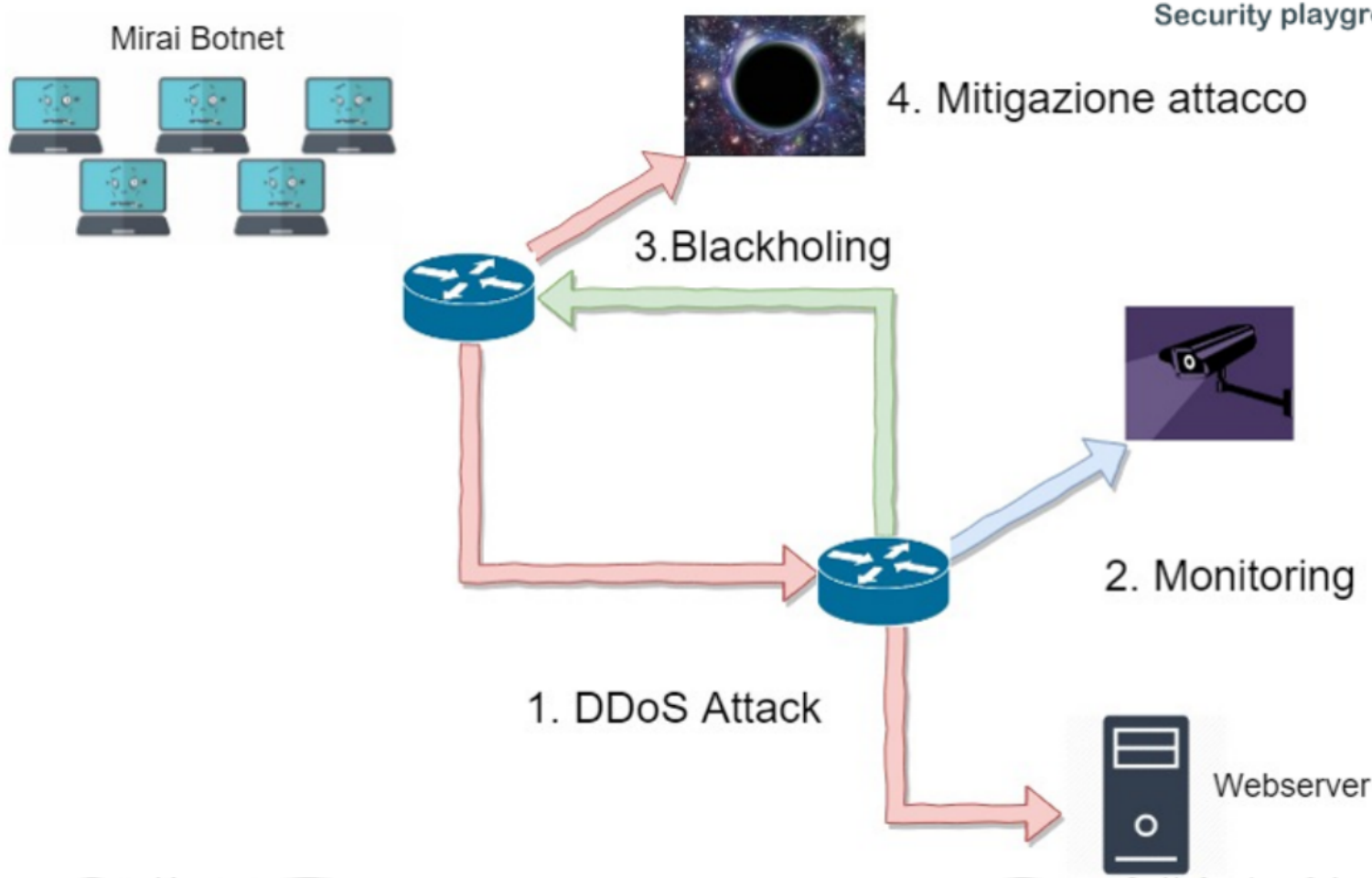
Mirai DDoS Lab

BGP blackholing

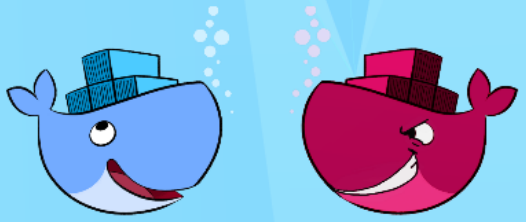


MIRAI mitigation in DSP

docker
Security playground



Conclusioni



docker
Security playground

- Piattaforma **open source** per lo studio della **Network Security**
- Contributo di **sviluppatori**, **Lab Designer** o Designer di **Immagini Docker Vulnerabili**
- https://github.com/giper45/DockerSecurityPlayground

Grazie per l'attenzione!