FRANCESCO CATURANO

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Docker Security Playground

Un framework a microservizi per l'implementazione di scenari di attacco in infrastrutture di rete virtualizzate

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
27 GIUGNO 2019 ROMA

Consortium GARR

Roma, 27/06/2019

Borsisti Day

AGENDA

1. *Contesto e Contributo*
2. *Obiettivi preposti*
3. *Risultati raggiunti*
4. *Sviluppi futuri*
5. *Q&A*

Contesto e Contributo

- *Network Security*
- *Ambienti virtualizzati*

- *Piattaforma per lo studio della network security*
  - *approccio «hands-on»*
  - *basata su container Docker*

Studiare la sicurezza di rete

Due tipologie di utenti:

- Studenti alle prime armi
- Esperti alla ricerca di nuove soluzioni da sperimentare

VS.

Cyber range

Playground

[illegible]king

Infrastrutture di ispirazione reale

- emulate grazie a moderne tecniche di virtualizzazione

- Una vera arma…
  - …ma caricata a salve!

DSP "bricks"

- Piattaforma di gestione di file **Docker-Compose**;
- **Web GUI** per la creazione di nuovi laboratori;
- **Repository** di laboratori disponibile pubblicamente;
- Immagini Docker Vulnerabili e "**Hack Tools**" per creare nuovi laboratori.

Obiettivi Preposti

docker
Security playground

1. Gestione unificata delle **Immagini Docker**

2. Interfaccia **Drag’n’Drop** per la realizzazione di nuovi laboratori

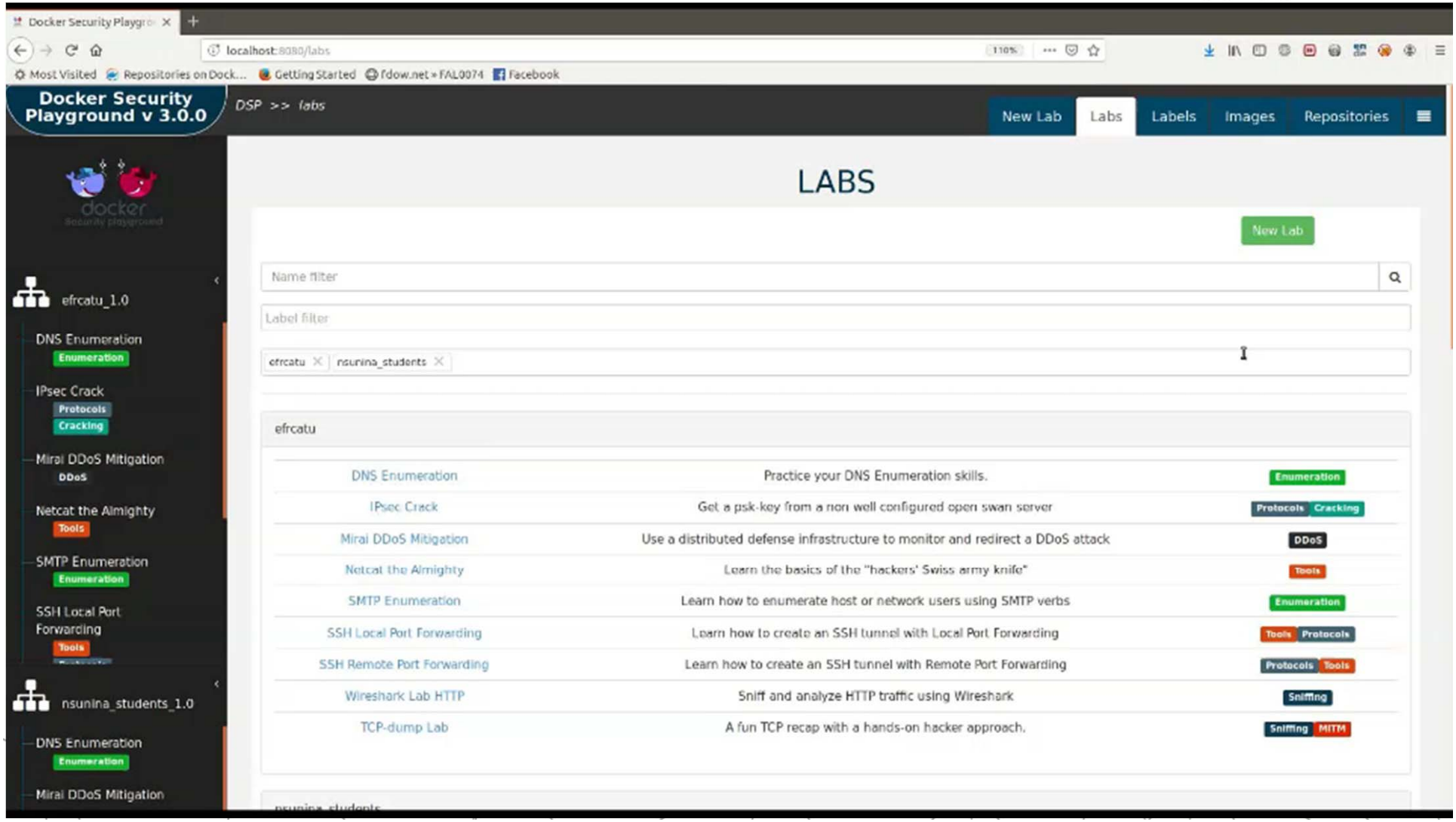
3. Librerie di scenari per lo studio delle tematiche di **Network Security**

1. Gestore Immagini Docker

docker
Security playground

- Catalogo di laboratori
- L’utente effettua il download delle immagini per il laboratorio di interesse

2. Drag’n’Drop Interface



2.1 One Line Hack Tools

docker
Security playground

1. Arsenale di '**strumenti dell'Hacker**'

2. Singoli comandi **mascherati** da container Docker
   - *docker run --rm «nome-immagine» «comando»*

3. «***Everything is a container***»

2.2 One Line Hack Tools

- ***Nmap 193.21.1.2*** -> Run Command

docker
Security playground

Hack Tools

```
  Starting Nmap 7.60 ( https://nmap.org ) at 2019-06-20 10:02 GMT

  Nmap scan report for c0a0321a74f1.smtpenumeration_public_network (193.21.1.2)

  Host is up (0.000035s 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:C1:15:01:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds

anon@\:>
```

3. DSP labs

docker
Security playground

- Laboratori didattici del corso di Network Security
  - **protocolli** per la sicurezza, **tecniche** di Penetration Testing, **strategie** di difesa

- Scenari di Hacking avanzati
  - DSP tool ufficiale **BlackHat Las Vegas 2018**
  - **Hackaton** in stile Capture The Flag

DSP #Hack.gov lab: Capture The Flag

docker
Security playground

- *Information Gathering*
- *Web Application Hacking*
- *Exploitation*
- *Privilege Escalation*

Sviluppi Futuri (1/2)

docker
Security playground

1. *Everything is a container … is it, really?*
   - **Integrazione** con diverse tecnologie di virtualizzazione
   - DSP cuore di una **piattaforma estesa**

2. Parametrizzazione delle strategie di Hacking
   - Velocizza la fase di design degli scenari
   - **Beyond** the Docker Image Wrapper

Sviluppi Futuri (2/2)

docker
Security playground

3. DSP designer di esperimenti
   - **Testbed** su larga scala in collaborazione con GARR
   - Costruzione di **dataset** degli attacchi
     - DDoS, Remote to Local, User to Root

Esempi applicativi:
   - Applicazione di modelli generativi dell'IA per la costruzione di adversarial examples test set

Riferimenti

- Repository Github DSP
  - https://github.com/giper45/DockerSecurityPlayground
- DSP Vagrant box
  - https://github.com/giper45/DSP_Vagrant
- DSP #BlackhatLab 2018
  - https://gitlab.com/dsp_blackhat/dsp_blackhat_vagrant
- Indirizzo E-mail
  - francesco.caturano@unina.it

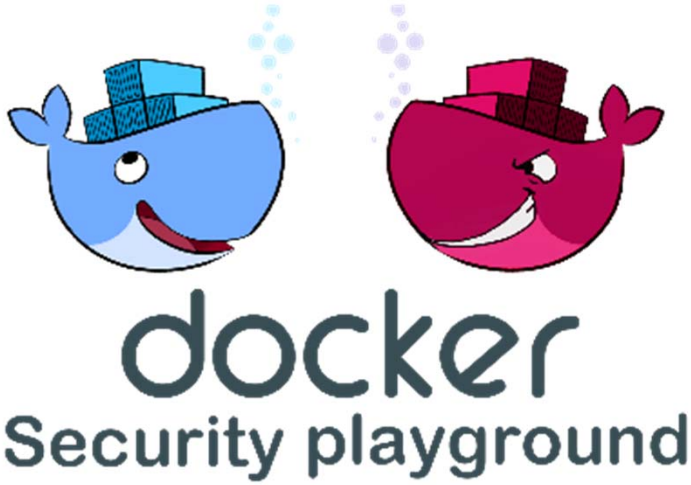
Docker Security Playground

docker
Security playground

Grazie per l’attenzione

Backup: Docker Security Playground

- Un sistema per costruire e gestire infrastrutture di rete virtuali…



- …su misura per lo studio della sicurezza di rete