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"
6 DICEMBRE 2018 ROMA

Consortium GARR

Roma, 06/12/2018

Borsisti Day

Contesto e Contributo

- *Network Security*
- *Ambienti virtualizzati*

- *Piattaforma per lo studio della network security*
  - *approccio sperimentale*
  - *basata su container Docker*

Studiare la sicurezza di rete

Di fondamentale importanza per:

- sviluppatori
- amministratori di sistemi
- penetration tester

Approccio "hands-on" tradizionale

- infrastrutture di rete reali
  - ...e Kevin "Condor" Mitnick?!

Ethical Hacking

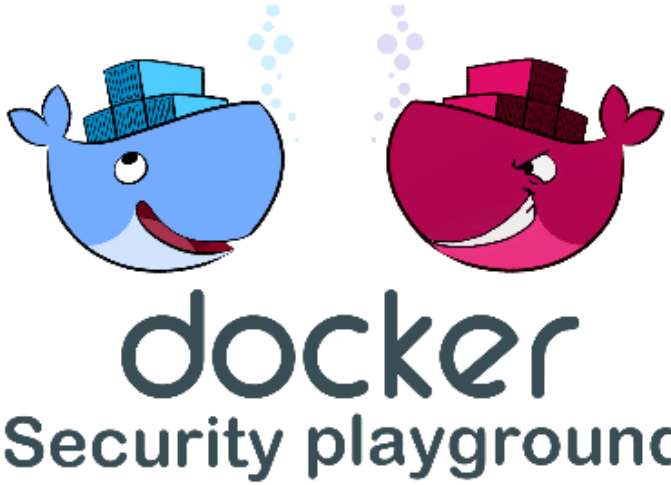
Infrastrutture di ispirazione reale

- emulate grazie a moderne tecniche di virtualizzazione

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

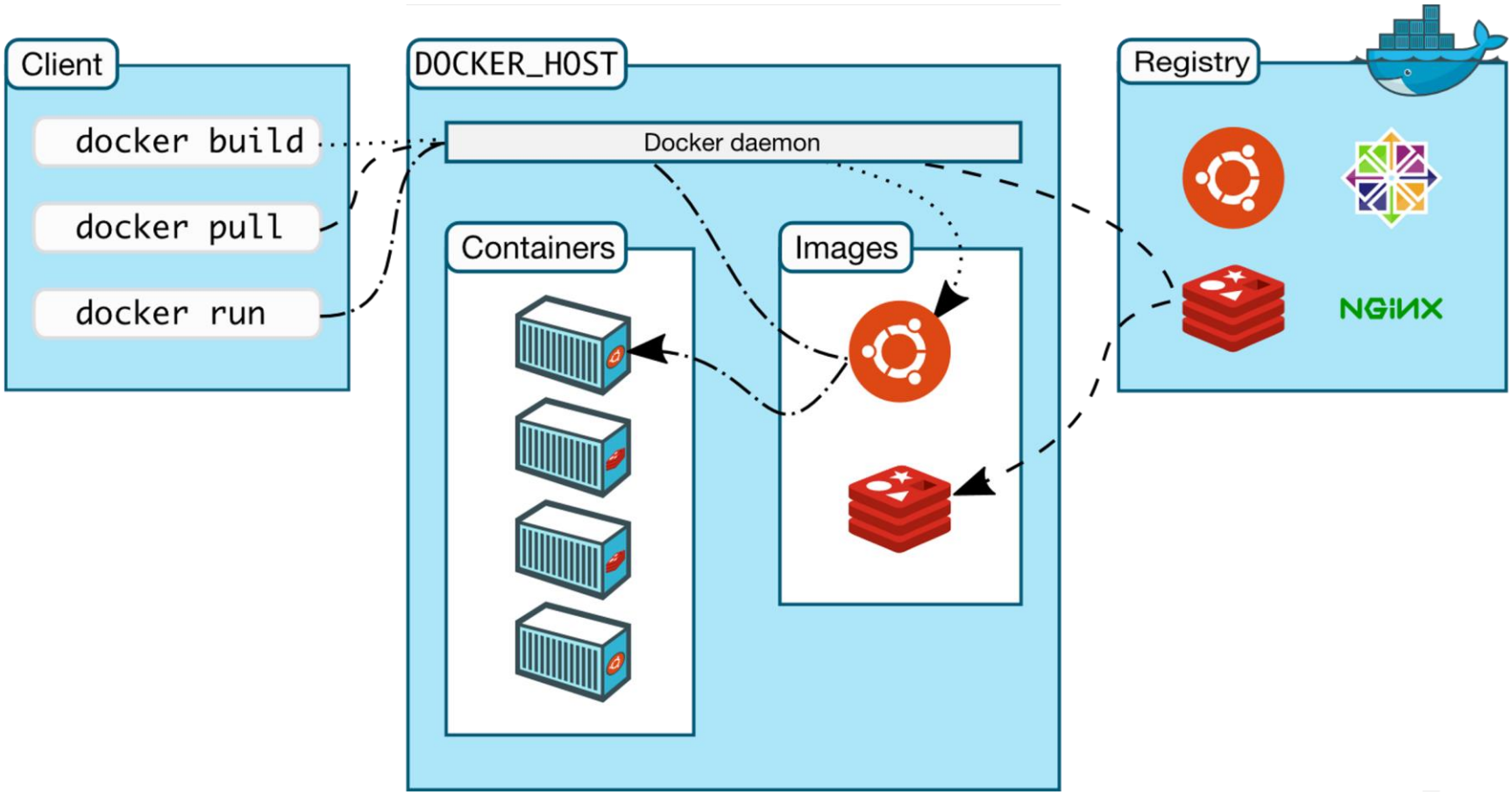
Docker Security Playground

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

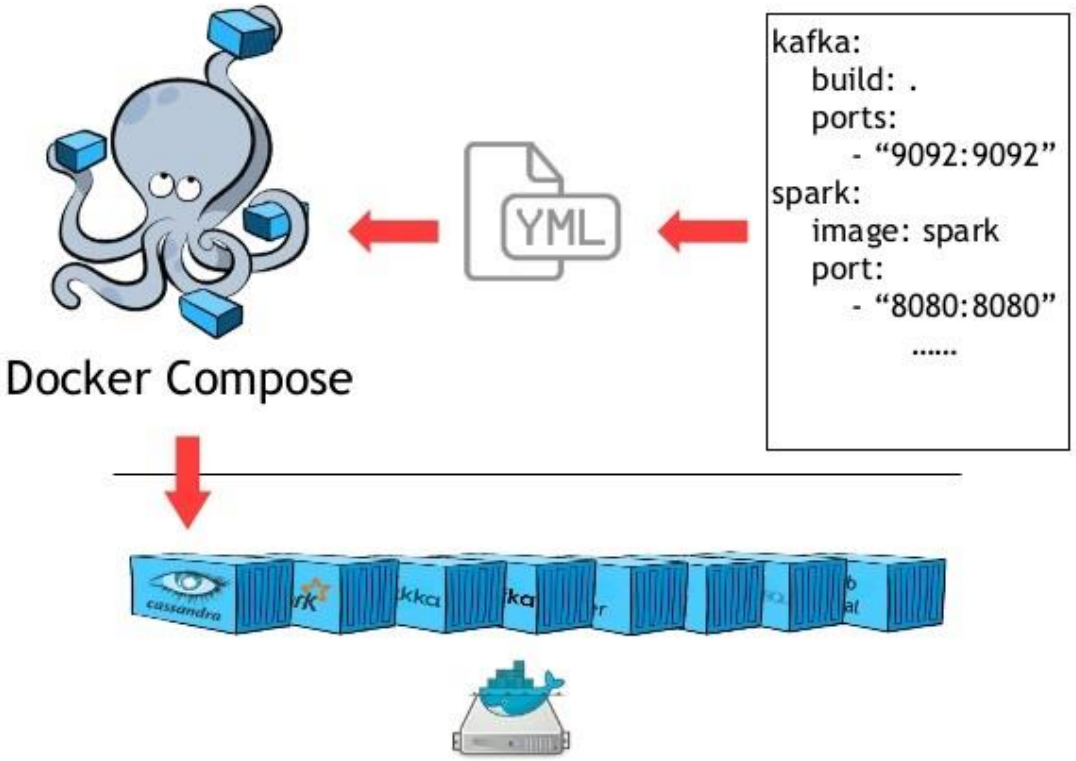


- …su misura per lo studio della sicurezza di rete

Docker


Client
docker build
docker pull
docker run
DOCKER_HOST
Docker daemon
Containers
Images
Registry
NGINX

Docker-Compose



DSP "bricks"

docker
Security playground

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

DSP labs

docker
Security playground

- Ciascuno approfondisce una tematica di sicurezza;
- Disponibili su repository pubbliche;
- Riproducibili e modificabili;
- Accompagnati da descrizione di una possibile soluzione;
- Il docker-compose file descrive l'infrastruttura del laboratorio.

DSP #NSUnina labs

docker
Security playground

DNS Enumeration	Practice your DNS Enumeration skills.	Enumeration
IPsec Crack	Get a psk-key from a non well configured open swan server	Protocols Cracking
Netcat the Almighty	Learn the basics of the "hackers' Swiss army knife"	Tools
SMTP Enumeration	Learn how to enumerate host or network users using SMTP verbs	Enumeration
SSH Local Port Forwarding	Learn how to create an SSH tunnel with Local Port Forwarding	Tools Protocols
SSH Reverse Port Forwarding	Learn how to create an SSH tunnel with Remote Port Forwarding	Protocols Tools
TCP-dump Lab	A fun TCP recap with a hands-on hacker approach.	Sniffing MITM
Wireshark Lab HTTP	Sniff and analyze HTTP traffic using Wireshark	Sniffing

DSP #BlackHat2018 lab: Capture The Flag

docker
Security playground

- Tre macchine da "hackerare"…
- …accompagnate da rispettivi "Hack Tools"

DSP configuration

docker
Security playground

- Ogni rete è composta da **container** e **sottoreti**
- L'utente usa **un editor grafico** per disegnare la rete
- Ad ogni container viene associata **un'immagine Docker**
- Se il container usa **Docker Image Wrapper**, alcune azioni sono esposte all'esterno
- Tali operazioni vengono tradotte in comandi docker all'atto dell'avviamento del laboratorio

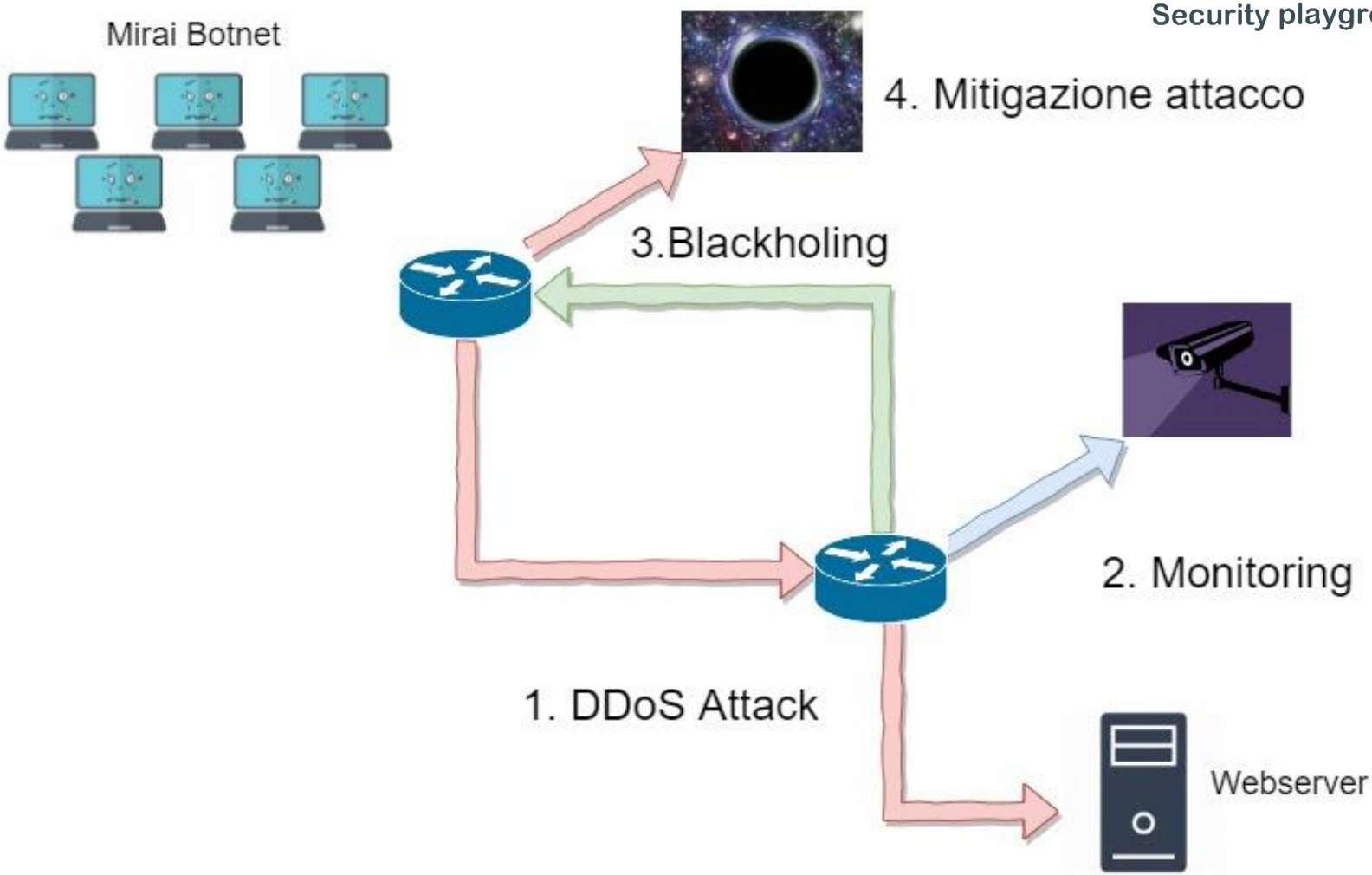
MIRAI DDoS

docker
Security playground

1. Infezione
2. Connessione
3. Controllo
4. Riproduzione

DSP: MIRAI mitigation (1/3)

docker
Security playground



DSP: MIRAI mitigation (2/3)

docker
Security playground

1. SYN ATTACK

```
root@botnet# syn 172.20.0.3 360
```

2. Fastnetmon DETECTION

```
IPs ordered by: packets
Incoming traffic          105634 pps     48 mbps  96872 flows
172.20.0.3                105672 pps     48 mbps 105654 flows
```

DSP: MIRAI mitigation (3/3)

docker
Security playground

3. BGP BLACKHOLING

```
static {
    route 10.10.10.1/32 next-hop 172.21.0.3 community 65001:666;
}
```

4. HOST UNREACHABLE

```
PING 172.20.0.3 (172.20.0.3) 56(84) bytes of data.
From 172.22.0.2: icmp_seq=4 Redirect Host(New nexthop: 172.22.0.2)
From 172.22.0.2 icmp_seq=2 Destination Host Unreachable
```

Riferimenti

- Repository Github DSP
  - https://github.com/giper45/DockerSecurityPlayground
- DSP per studenti Unina
  - https://gitlab.com/ns-unina/dsp-for-students
- 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