

FRANCESCO CATURANO



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**

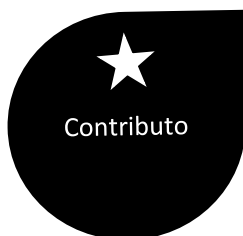
Consortium GARR

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*



Di fondamentale importanza per:

- sviluppatori
- amministratori di sistemi
- penetration tester

Approccio "hands-on" tradizionale

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

RubberSheep.com

U.S. Department of Justice
United States Marshals Service

WANTED BY U.S. MARSHALS

NOTICE TO ARRESTING OFFICE: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NCIC/ W721450021)

NAME:MIDNICK, KEVIN DAVID

AKS (S):MIDNICK, KEVIN DAVID
.....HERBILLE, BRIAN ALLLEN

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
Skin tone:LIGHT
Scars, Marks, Tattoos:NONE KNOWN
Social Security Number (s):550-39-5695
NCIC Fingerprint Classification:D0P2G0P613B1P619P609



ADDRESS AND LOCALITY: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION OF UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485)

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSD0000.

PREP RECTIONS ARE OASOLETS AND NOT TO BE USED

Form 1284a
(Rev. 3/78)



Ethical Hacking

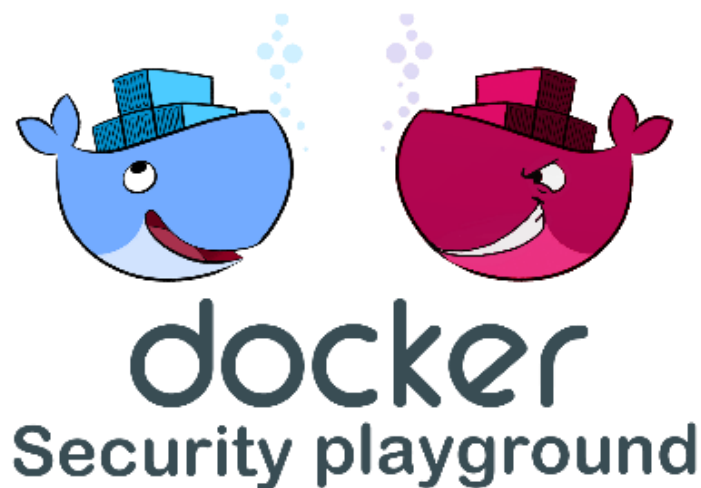
Infrastrutture di ispirazione reale

- emulate grazie a moderne tecniche di virtualizzazione
- Una vera arma...
 - ...ma caricata a salve!



Docker Security Playground

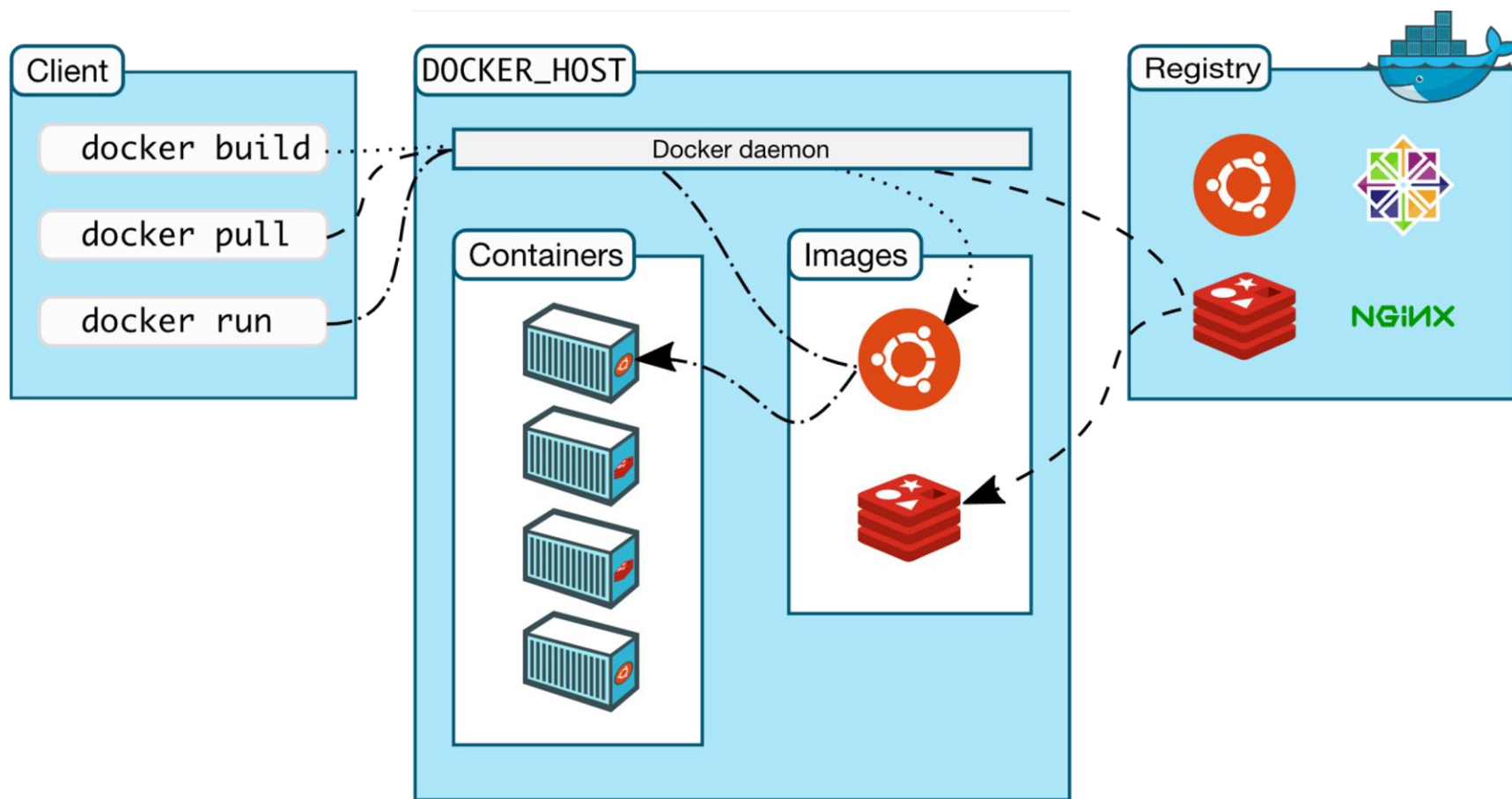
- Un sistema per costruire e gestire infrastrutture di rete virtuali...



- ...su misura per lo studio della sicurezza di rete

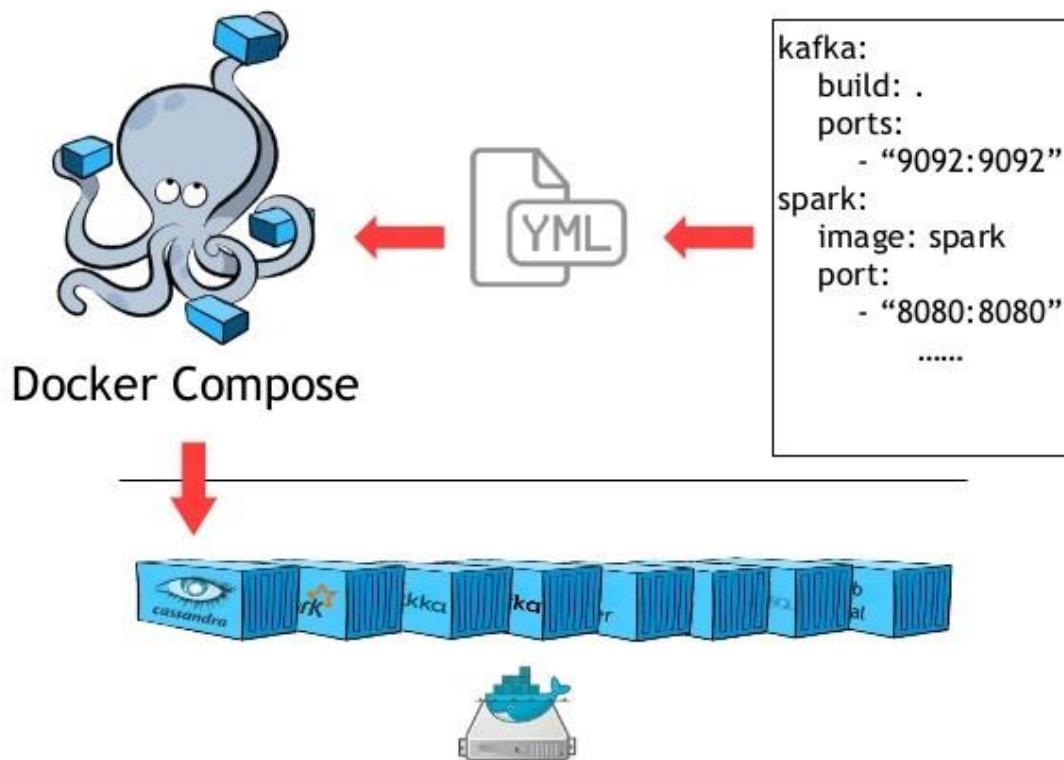


Docker



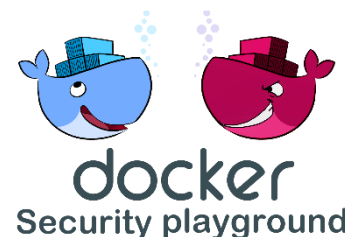


Docker-Compose





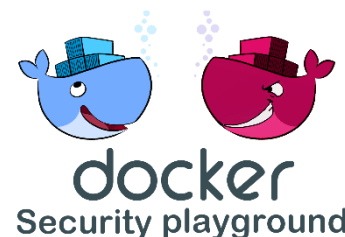
DSP "bricks"



- 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



- 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



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



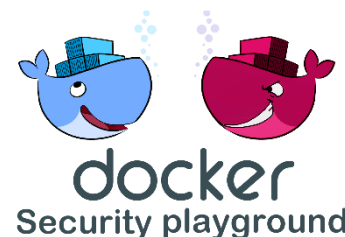
DSP #BlackHat2018 lab: Capture The Flag



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



DSP configuration



- 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

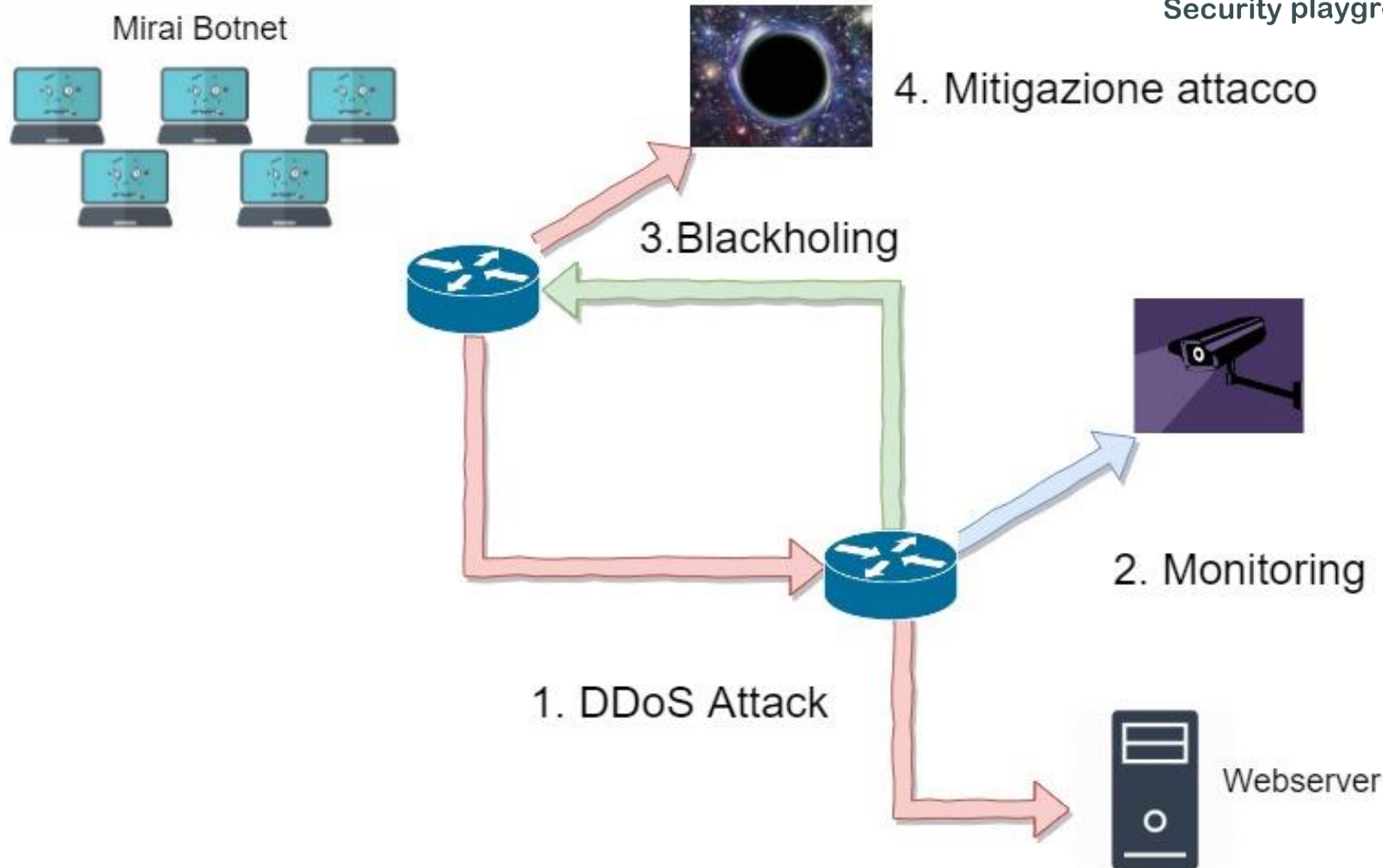


1. Infezione
2. Connessione
3. Controllo
4. Riproduzione





DSP: MIRAI mitigation (1/3)





DSP: MIRAI mitigation (2/3)



1. SYN ATTACK

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

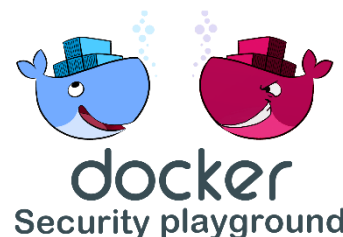
2. Fastnetmon DETECTION

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)



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



Grazie per l'attenzione

