

FRANCESCO CATURANO



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

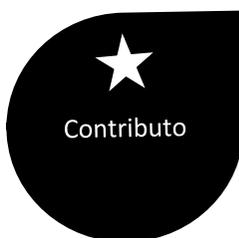


AGENDA

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



Cyber range

VS.



Playground



Hacker gets a whole lot of 14 years in prison for running Scan4You service

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



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

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

SSH Remote Port Forwarding

Download All

nsunina/alpine-ssh-client:latest	Download ⬇
nsunina/linode_lamp:v1.0	Download ⬇
nsunina/firefox-ssh-server:latest	Download ⬇



2. Drag'n'Drop Interface



The screenshot shows the Docker Security Playground v 3.0.0 interface. The browser address bar shows localhost:8080/labs. The main navigation bar includes 'New Lab', 'Labs', 'Labels', 'Images', and 'Repositories'. The 'LABS' section is active, displaying a list of labs under the 'efrcatu' category. The labs are:

Lab Name	Description	Category
DNS Enumeration	Practice your DNS Enumeration skills.	Enumeration
IPsec Crack	Get a psk-key from a non well configured open swan server	Protocols, Cracking
Mirai DDoS Mitigation	Use a distributed defense infrastructure to monitor and redirect a DDoS attack	DDoS
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 Remote Port Forwarding	Learn how to create an SSH tunnel with Remote Port Forwarding	Protocols, Tools
Wireshark Lab HTTP	Sniff and analyze HTTP traffic using Wireshark	Sniffing
TCP-dump Lab	A fun TCP recap with a hands-on hacker approach.	Sniffing, MITM



2.1 One Line Hack Tools



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

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



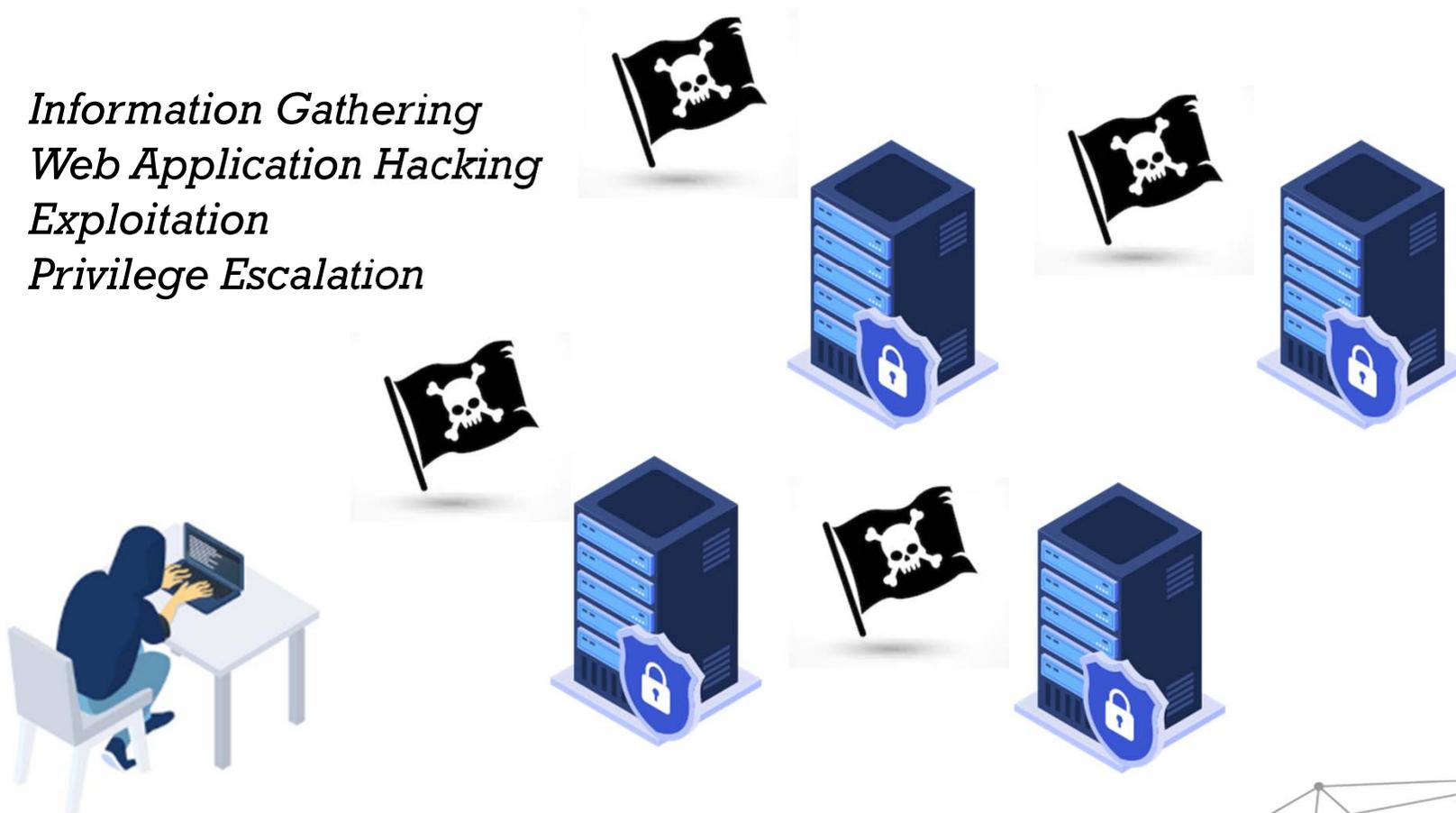
- Laboratori didattici del corso di Network Security
 - **protocolli** per la sicurezza, **tecniche** di Penetration Testing, **strategie** di difesa
- Scenari di Hacking avanzati
 - DSP tool ufficiale **BlackHat Las Vegas 2018**
 - **Hackaton** in stile Capture The Flag



DSP #Hack.gov lab: Capture The Flag



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





Sviluppi Futuri (1/2)



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)



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

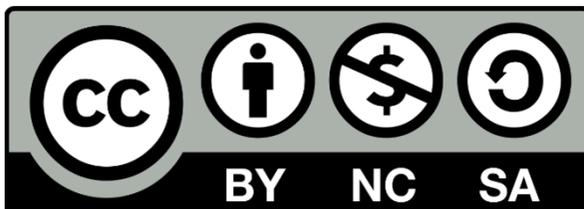


GIORNATA DI INCONTRO BORSE DI STUDIO GARR "ORIO CARLINI"
GIOVEDI' 27 GIUGNO 2019 - ROMA

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