

**OWASP Latam Tour
Venezuela 2015**

Conociendo al Enemigo **HONEYPOTS**



OWASP

The Open Web Application Security Project



root@honeypot:~# cat josmell



Josmell Chavarri Velásquez

- ✓ Ingeniero en Comunicaciones y Electrónica.
- ✓ Especialista en Seguridad de la Información.
- ✓ Miembro OWASP Capitulo Venezuela.
- ✓ Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT)



OWASP
★★★★★★★★
Venezuela Chapter



OWASP

The Open Web Application Security Project

Acciones Defensivas



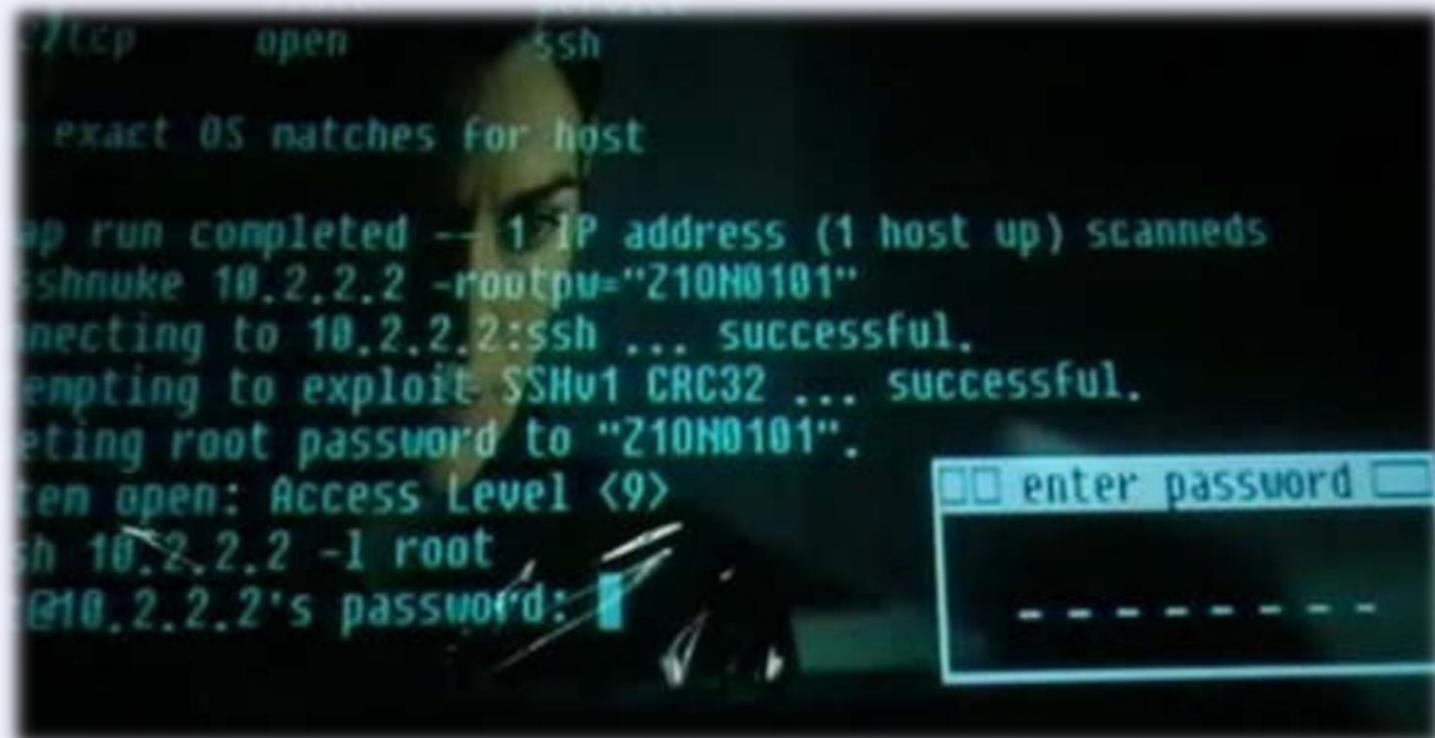


OWASP

The Open Web Application Security Project

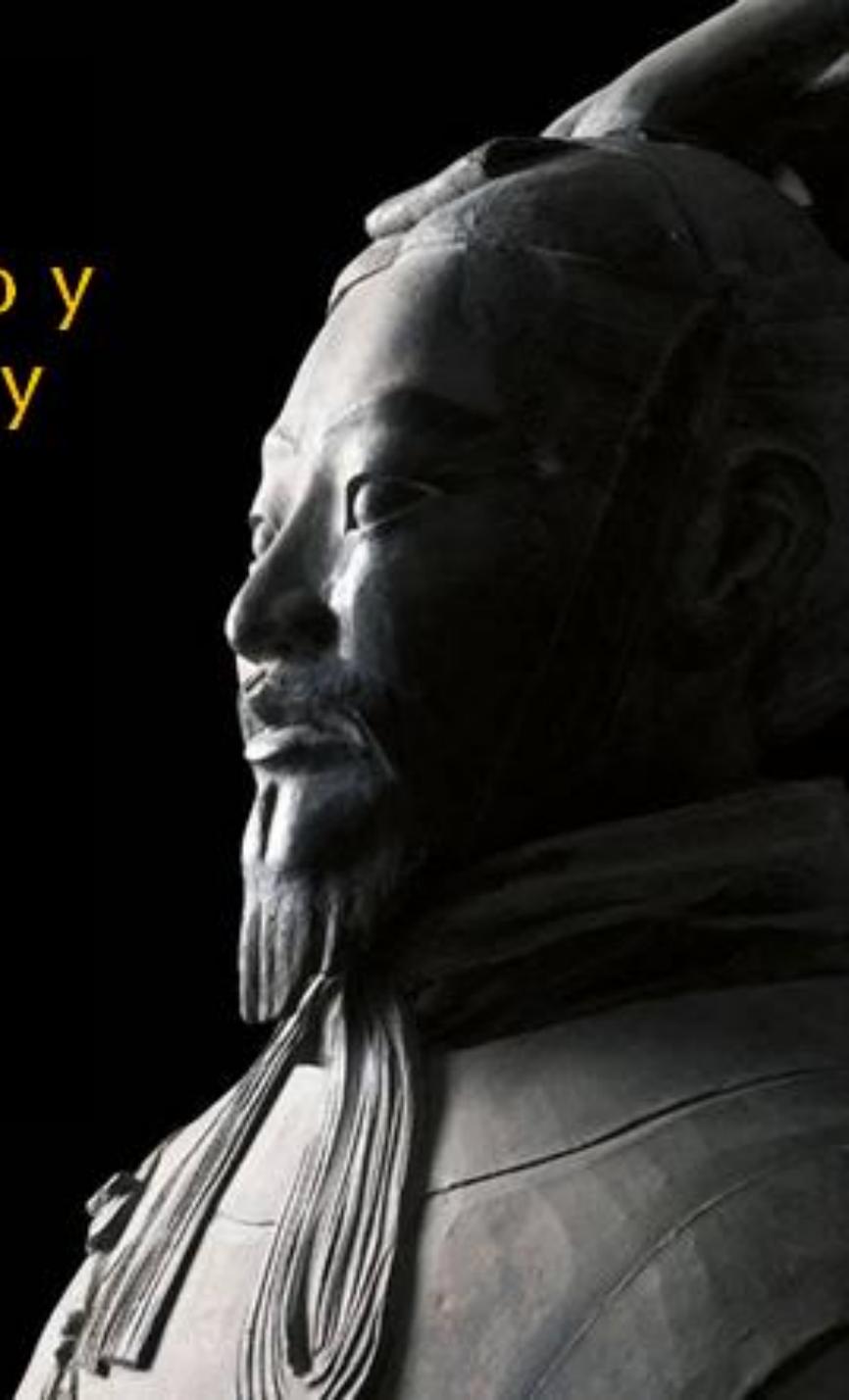
¿Cómo defendernos contra un enemigo, cuando no sabemos quien es el enemigo?

```
tcp open ssh
exact OS matches for host
scan run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="210N0101"
connecting to 10.2.2.2:ssh ... successful.
attempting to exploit SSHv1 CRC32 ... successful.
entering root password to "210N0101".
ssh 10.2.2.2 -l root
@10.2.2.2's password: [REDACTED]
```



“Conoce a tu enemigo y
conócete a ti mismo, y
saldrás triunfador en
mil batallas”

— *Sun Tzu, "El Arte de la Guerra"*





OWASP

The Open Web Application Security Project



Honeypots



HONEYPOTS



Según su traducción: Tarro de Miel

Objetivos



OWASP

The Open Web Application Security Project



- ✓ Obtener información de ataques.
- ✓ Mejorar el conocimiento.
- ✓ Distraer al atacante.
- ✓ Detectar ataques de forma temprana.

Honeypots



Resuelve fallos de seguridad

Detiene a un atacante



Clasificación



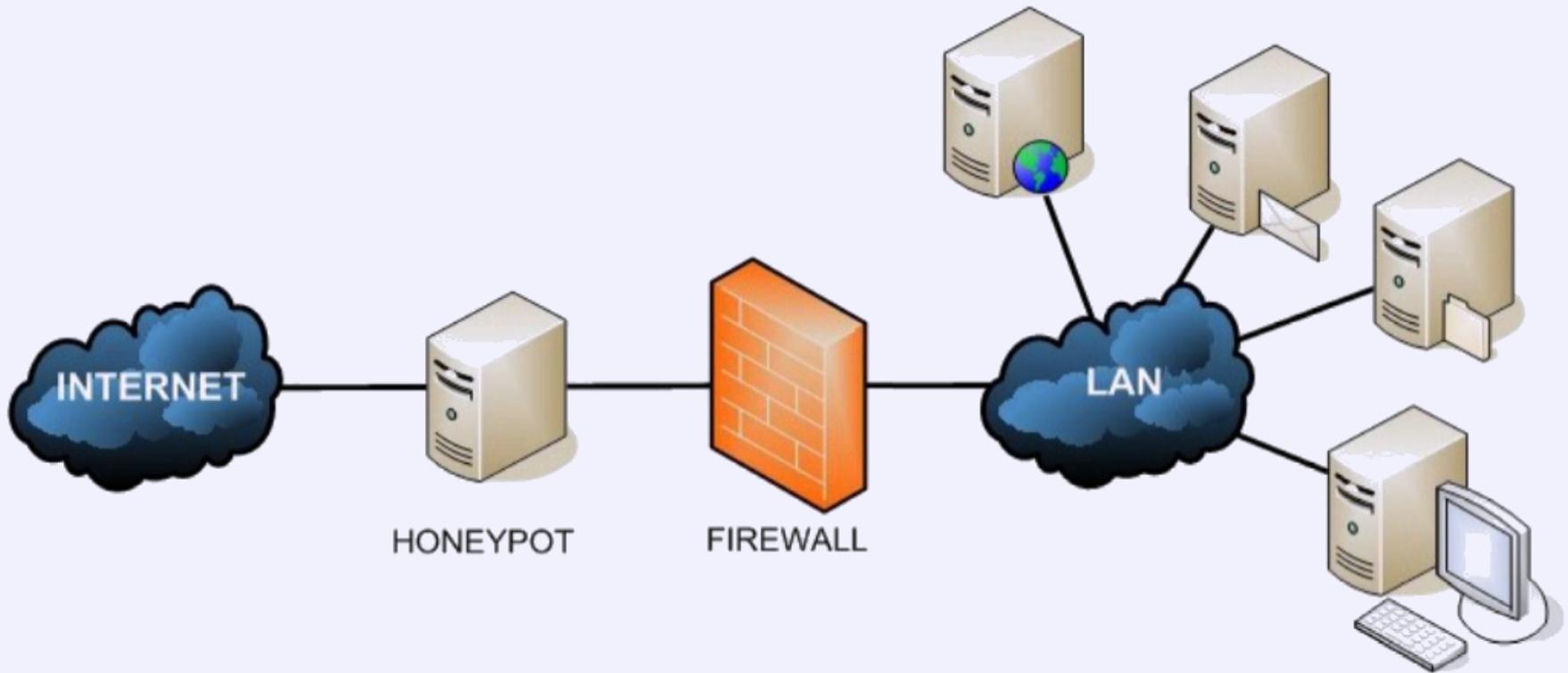
OWASP

The Open Web Application Security Project

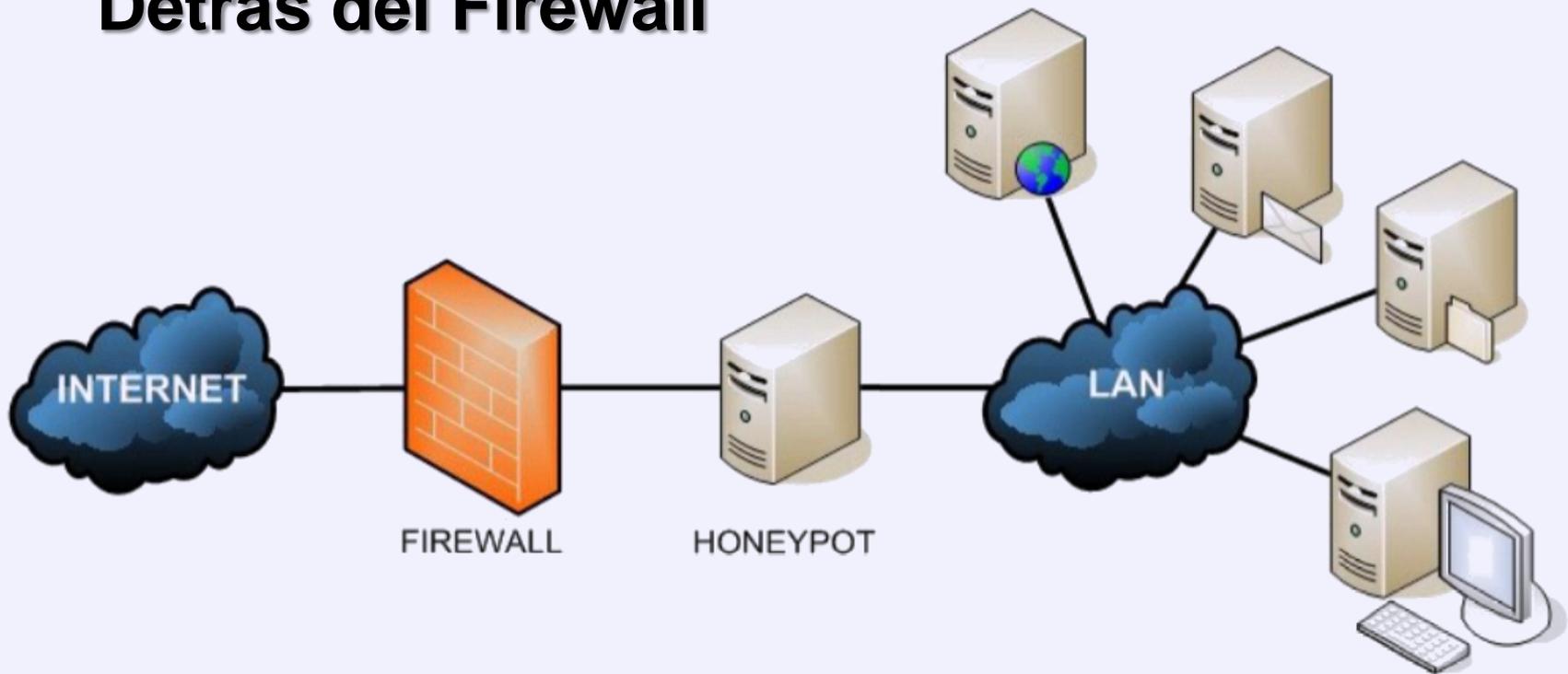




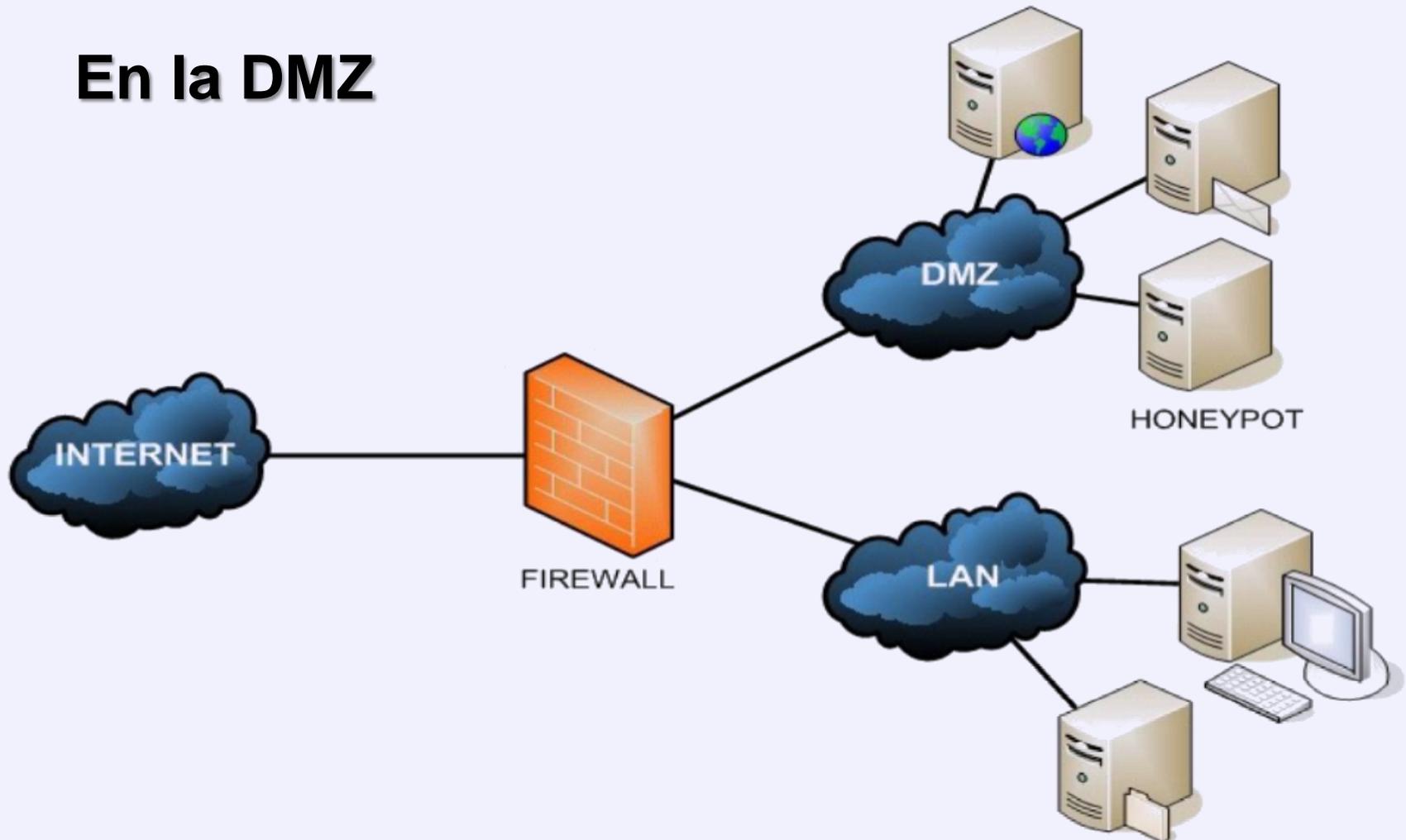
Delante del Firewall



Detrás del Firewall



En la DMZ



Proyectos



OWASP

The Open Web Application Security Project

PROJECT HONEY POT



OWASP WASC Distributed Web Honeypots Project

Main | [How to Participate](#) | [FAQs](#) | [Acknowledgements](#) | [Road Map and Getting Involved](#) | [Project About](#) [\[edit\]](#)



OWASP WASC Distributed Web Honeypots Project [\[edit\]](#)

The goal of the OWASP WASC Distributed Web Honeypots Project is to identify emerging attacks against web applications and report them to the community including automated scanning activity, probes, as well as, targeted attacks against specific web apps.

What is the OWASP WASC Distributed Web Honeypots Project? [\[edit\]](#)

The OWASP WASC Distributed Web Honeypots Project provides:

- Real-time, detailed Web

Quick Download [\[edit\]](#)

- [Link to download Honeypot VM \(ZIP\)](#) [\[edit\]](#)

News and Events [\[edit\]](#)

- [WASC Honeypot Opens Up](#)



Tipos



OWASP

The Open Web Application Security Project



Bokken 1.5
Welcome to Bokken 1.5
Select backend to use: Pyew
Select a target or enter the path manually.
Valid inputs are: PE/ELF, PDF, plain text files and URLs
Analysis options:
 Deep analysis
 Lower case disassembly

phpLiteAdmin v1.9.3
Database name: logsql.sqlite
Path to database: J:\J\logdionaea\var\dionaea\logsql.sqlite
Size of database: 92 KB
Database last modified: 3:43am on December 26, 2012
SQLite version: 3.7
SQLite extension
PHP version: 5.3.3

HONEYD-VIZ
VISUALIZATION TOOL FOR YOUR HONEYD HONEYPOT INSTANCE

KIPPO-GRAPH
FAST VISUALIZATION FOR YOUR KIPPO SSH HONEYPOT STATS





OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

Gracias por su Atención



OWASP



Venezuela Chapter

Josmell.chavarri@owasp.org