

## Seguridad

la seguridad son aquellas medidas que se toman para evitar que algo que se hackea en segundos les lleve más tiempo.

- Defensa en capas (físico, SO, Datos, Aplicación,.....)
- Mínimos servicios. Únicamente los necesarios para su cometido
- Mínimos privilegios

## Guías para bastionar

[http://www.nsa.gov/ia/mitigation\\_guidance/security\\_configuration\\_guides/operating\\_systems.shtml](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml)

## Contención

### Segmentar la red

- Uso de VLANs y DMZ
- bastionar los servidores

### Instalación de HoneyPots

- Deception tool kit (DTK )
- honeyd
- spetcher
- honeynet project

## Monitorización

### Varios

- <http://www.criptored.upm.es/paginas/docencia.htm>
- <https://underc0de.org/>
- <https://underc0de.org/foro/talleres-underc0de-213/listado-de-talleres-underc0de/?PHPSESSID=e98087b16b7950fb4f217e24c8c833dc>

From:  
<http://wiki.intrusos.info/> - LCWIKI

Permanent link:  
<http://wiki.intrusos.info/doku.php?id=seguridad>

Last update: **2023/01/18 13:49**

