



# IntroSec

Ciclo de charlas Introducción a la  
ciberseguridad – DUOC Citt

## Taller 01



# Agenda de hoy

## Introducción y herramientas de seguridad

**1.- Conceptos de redes, sistemas y conectividades**

**2.- Etapas de un Pentesting y herramientas**

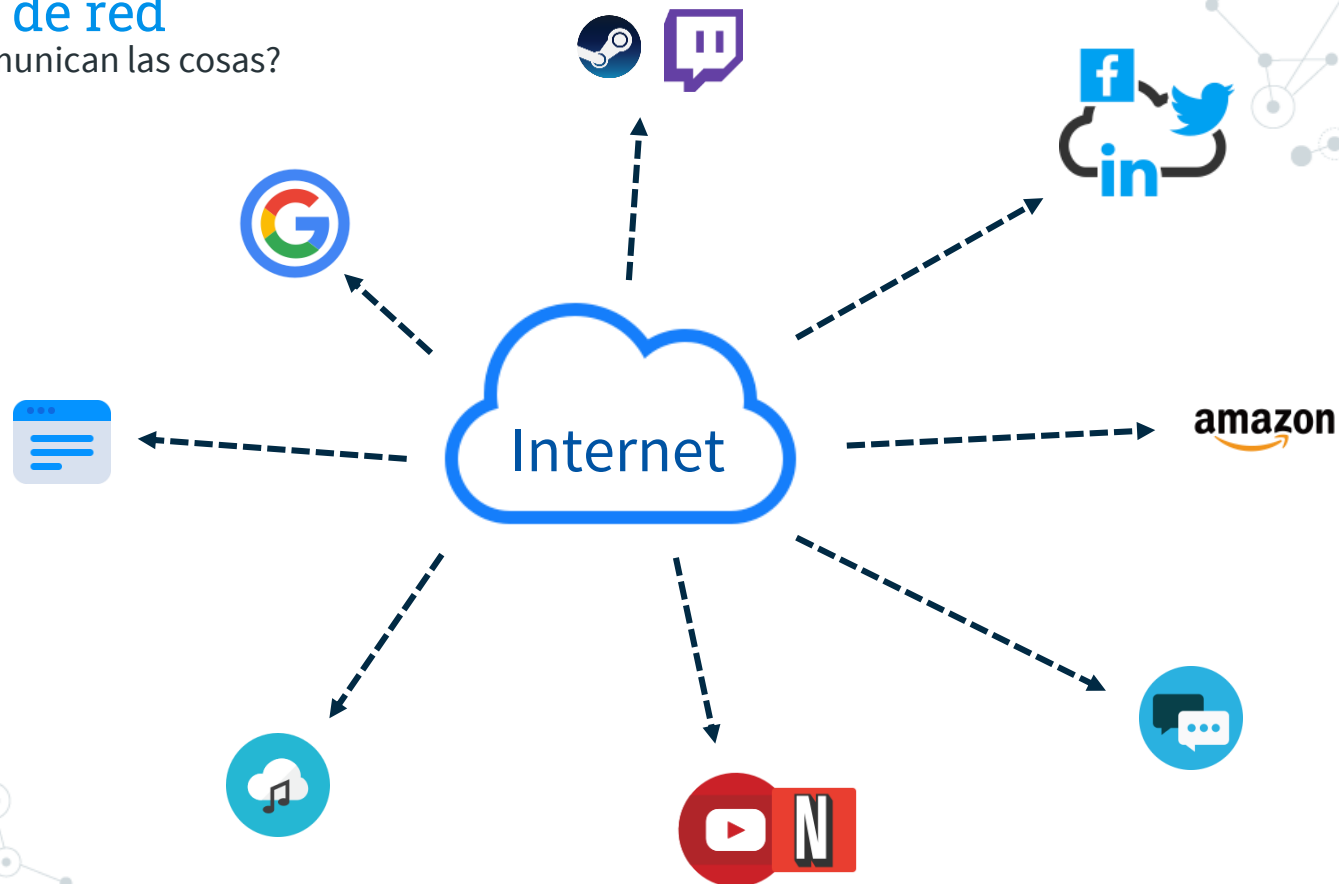
**3.- Taller práctico con Metasploitable**

**1.**

# **Conceptos de redes, sistemas y conectividades**

# Conceptos de red

¿Cómo se comunican las cosas?





“

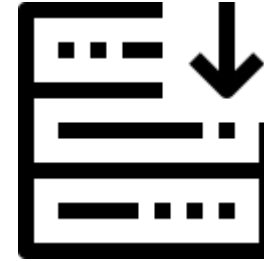
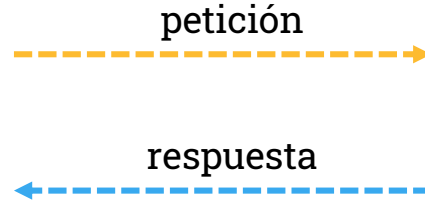
Finalmente, el internet es un  
***conjunto de dispositivos  
conectadas entre sí,***  
intercambiando información



## Una comunicación básica



Consume un  
servicio



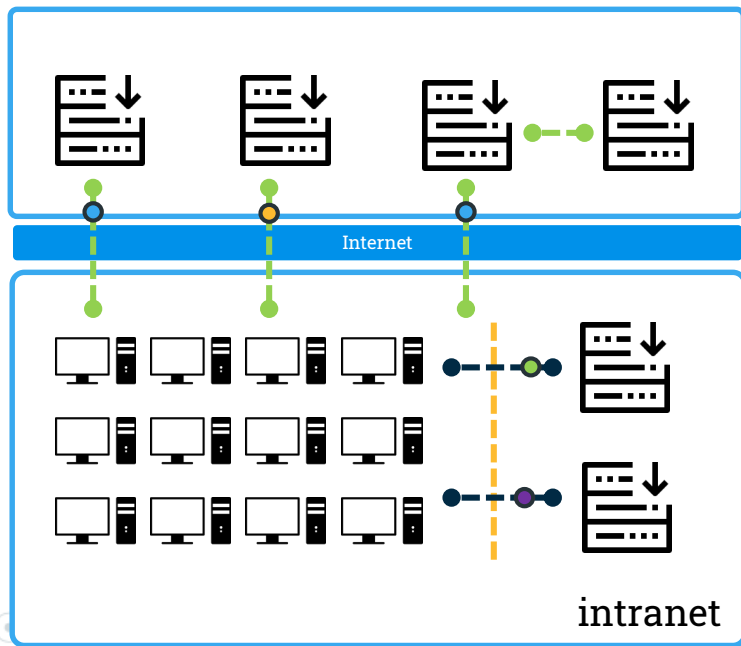
Expone un  
servicio



procesamiento



## Esquemas de red

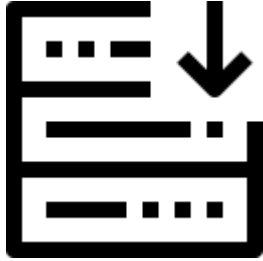


### La conectividad

Esta conectividad se da a todos niveles, vía internet, intranets, conexiones VPNs, ¡etcétera!



## Concepto 01: Dirección IP



Los servidores están ubicados en alguna parte que deben ser identificados, es como la dirección de dónde viven: a eso llamaremos **dirección IP**.

XXX.YYY.ZZZ.AAA (IPv4)

2001:db8:1234:0000:0000:0000:0000:0000 (IPv6)

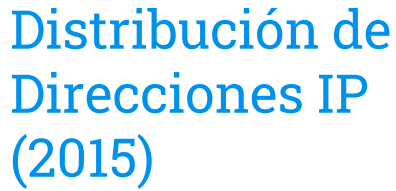
### Direcciones IP Locales

10.0.0.0 – 10.255.255.255  
172.16.0.0 – 172.31.255.255  
192.168.0.0 – 192.168.255.255

### Direcciones IP Globales

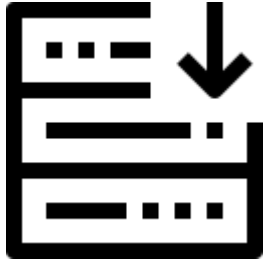
[el resto]







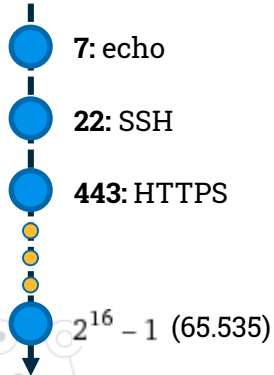
## Concepto 02: Puerto y Servicio



Cada servidor vive en una dirección en una red internet o conectado a internet (IP), sin embargo, un servidor por si solo no hace nada, ¡tiene que proveer un servicio!

Este servicio se expone por una ventanilla llamada **Puerto**, y tiene dos modalidades: **UDP** y **TCP**

< 10.0.30.5 >



Cada uno de estos servicios realiza una acción de **bind** en un determinado puerto, por lo tanto, dos servicios no pueden usar el mismo puerto.

Detrás de cada servicio existe un programa (software) recibiendo y transmitiendo datos.

216-1

[https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros\\_de\\_puertos\\_de\\_red](https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puertos_de_red)



## Concepto 02: Puertos más conocidos

Si bien puedes colocar cualquier servicio en cualquier puerto, existen algunas convenciones internacionales.

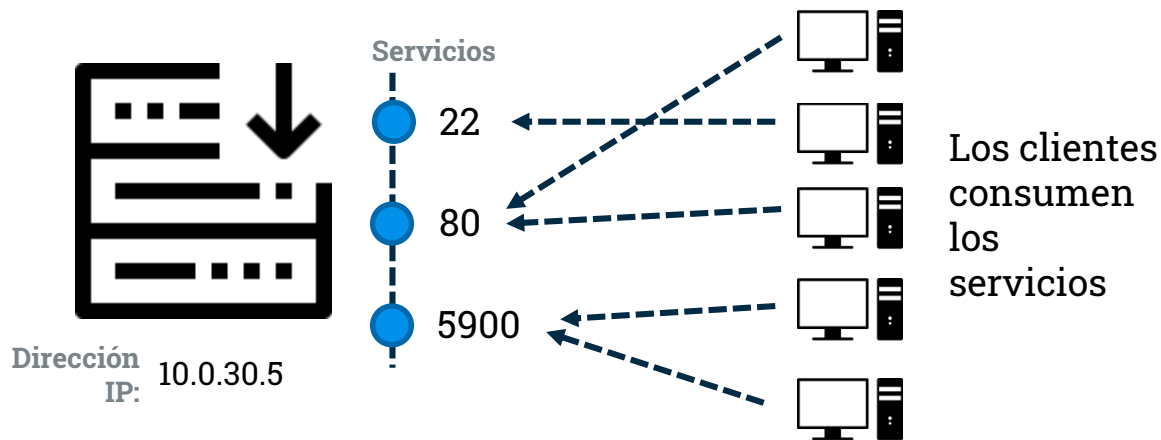
- **21:** ftp
- **22:** ssh
- **23:** telnet
- **25:** smtp
- **53:** domain name system
- **80:** http
- **110:** pop3
- **111:** rpcbind
- **135:** msrpc
- **139:** netbios-ssn
- **143:** imap
- **443:** https
- **445:** microsoft-ds
- **993:** imaps
- **995:** pop3s
- **1723:** pptp
- **3306:** mysql
- **3389:** ms-wbt-server
- **5900:** vnc
- **8080:** http-proxy





## Agrupemos lo aprendido

- Las máquinas se **comunican vía redes de computadores**.
- Utilizan **direcciones IPs** para ubicarse en esta red.
- Cada máquina puede **publicar servicios a través de un puerto**.
- **Un servicio es un programa** ejecutándose en la máquina.



¿Y cuando  
comienza el  
hackeo?





## Concepto 03: Una vulnerabilidad

Los programas tienen vulnerabilidades, principalmente por culpa de diseño o configuraciones.

¡Estas vulnerabilidades se pueden aprovechar para tomar control de los sistemas o conseguir información!

Problemas de diseño

Configuración insegura

Vulnerabilidades en la comunicación

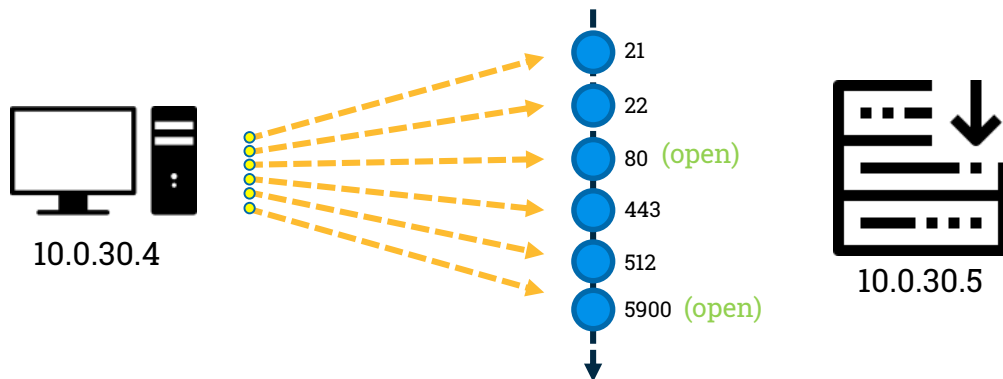
## Concepto 04: Un exploit

Un exploit es una forma automática o manual de cómo utilizar una vulnerabilidad para realizar algo.

Una vulnerabilidad puede tener o no un **exploit**.

## Concepto 05: Escanear puertos abiertos

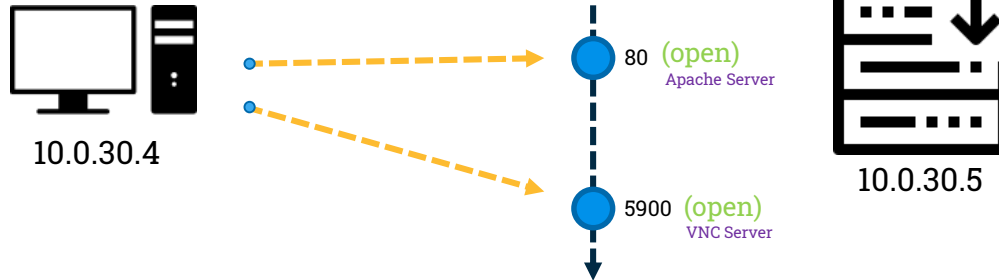
Cuando queremos saber que servicios son vulnerables, primero tenemos que visualizar que puertos hay abiertos.



(Three-way handshake – TCP)

## Concepto 06: Reconocer el servicio

Una vez identificando que puerto está abierto, se establece una conexión. Dependiendo de los datos transmitidos se puede identificar el servicio que está en ese puerto.





## Concepto 06: Encontrar vulnerabilidades

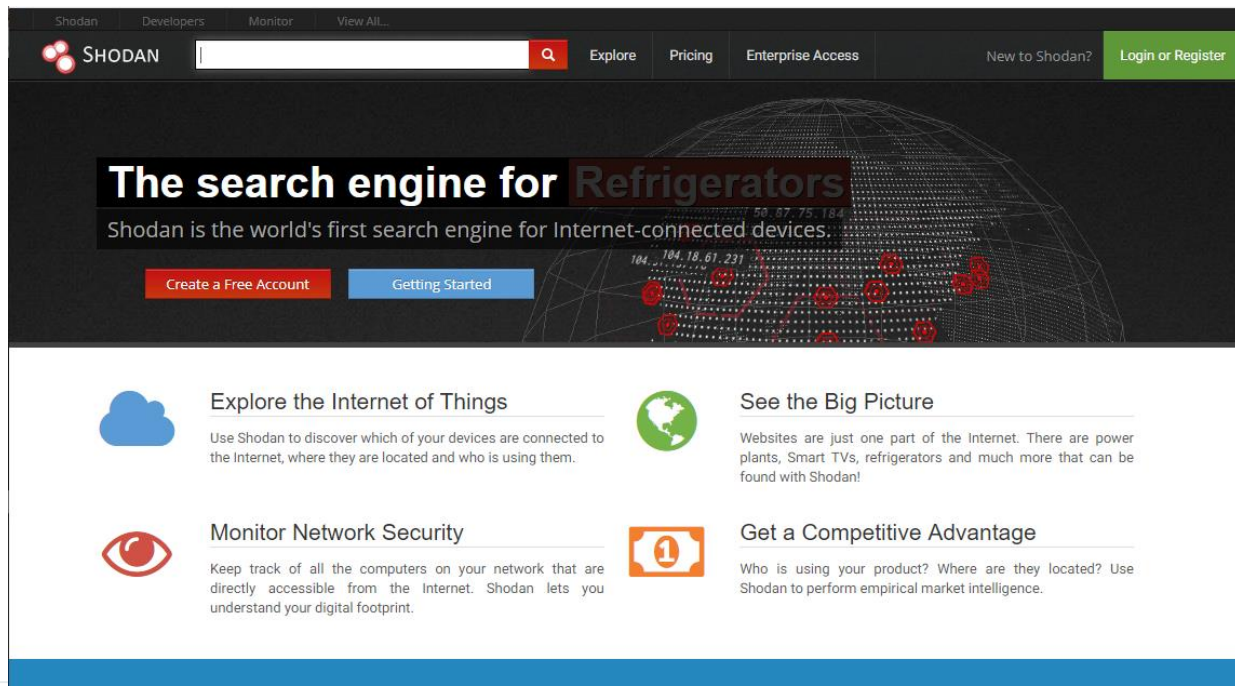
Una vez identificando que puerto está abierto, se establece una conexión. Dependiendo de los datos transmitidos se puede identificar el servicio que está en ese puerto.



80	(open)	Apache Server	<versión>
5900	(open)	VNC Server	<versión>

Utilizando el **nombre del servicio** y **su versión** es posible encontrar vulnerabilidades y sus exploits en internet.

## Veamos un ejemplo de escaneos masivos



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for Shodan, Developers, Monitor, and View All. A search bar is prominently displayed with a magnifying glass icon. To the right of the search bar are links for Explore, Pricing, Enterprise Access, and a green button for Login or Register. The main banner features the text "The search engine for Refrigerators" in a large, bold font, with "Refrigerators" highlighted in a dark red box. Below this, it states "Shodan is the world's first search engine for Internet-connected devices." and provides buttons for "Create a Free Account" and "Getting Started". The background of the banner shows a globe with red location markers and IP addresses like "104.18.61.231". Below the banner, there are four sections with icons and text: "Explore the Internet of Things" (cloud icon), "See the Big Picture" (globe icon), "Monitor Network Security" (eye icon), and "Get a Competitive Advantage" (dollar bill icon).

Shodan Developers Monitor View All


SHODAN

Explore Pricing Enterprise Access New to Shodan? Login or Register


### The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.


Create a Free Account Getting Started

 Explore the Internet of Things


Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

 See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

 Monitor Network Security


Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

 Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



## Las Herramientas



Muchos de estos procesos están automatizados en herramientas que hacen prácticamente todo el trabajo pesado por nosotros.

**¡Hoy veremos algunas de ellas en el taller!**



# 🛡️ ¿Como se puede hackear un equipo y tomar control?

## Un enfoque inicial:

1. Encontrar un objetivo (su dirección IP).
2. Analizar los servicios que tiene expuestos.
3. Analizar si esos servicios tienen vulnerabilidades conocidas.
4. Analizar si esas vulnerabilidades tienen exploits conocidos.
5. Explotar la vulnerabilidad.
6. Utilizar esa vulnerabilidad para lograr algo.

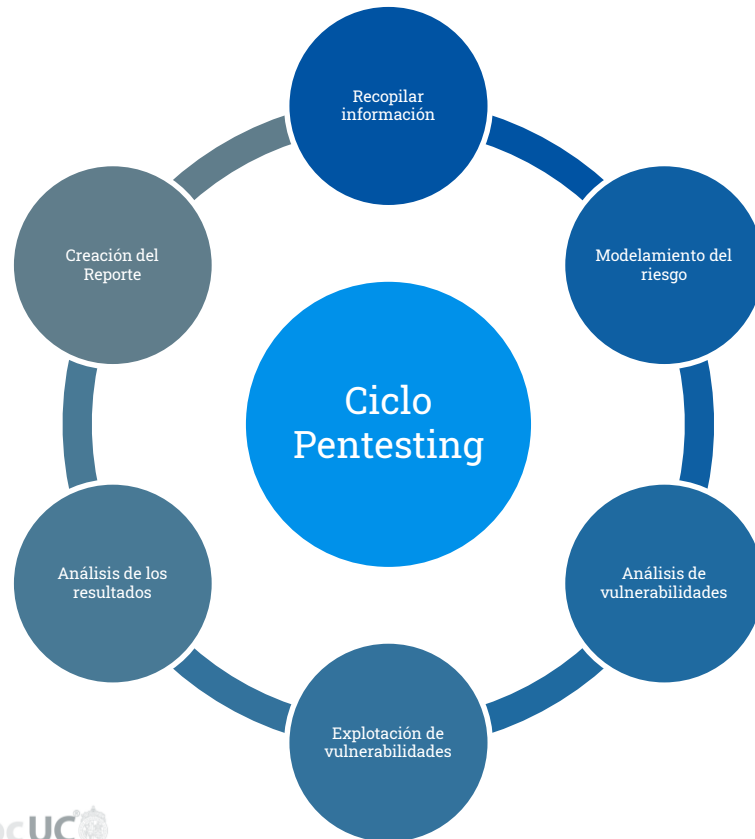
### Nota

**¿Y si no hay exploit?** Un pentester (muy) avanzado es capaz de crear sus propios exploits mediante reversing, analítica de código, mucho ingenio y experiencia.

# 2.

## **Etapas de un pentesting y herramientas**

## ↺ Los pasos para realizar un pentesting



### El proceso es importante

Durante el trabajo de un pentesting es necesario ser metodológico, anotar todo y ser extremadamente ordenado.

# Herramientas para el pentester

## Herramientas de Red

- Nmap
- Masscan
- DNSMap
- Wireshark (\*)
- BeeF
- BetterCap
- Aircrack-ng

## Herramientas Web

- Nikto
- WPscan
- SQLMap
- BurpSuite / OwaspZed
- Arachni

## Fuerza Bruta

- JohnTheRipper
- THC Hydra

## Escanear vulnerabilidades

- OpenVAS
- Acunetix (!)
- Nessus (!)
- NetSparker (!)

## Ingeniería Social

- SETtoolkit
- CUPP
- Rubber Ducky
- Piña Wifi

## Herramientas Útiles

- Shodan
- Exploit-DB

(Tan sólo algunas)



### 3. ¿Y si hackeamos un poquito?

Ya, vamos al laboratorio...







# Muchas gracias!

## **IntroSec – Taller01**

Me pueden encontrar en Telegram: @mdiazcl