

# VIGILANDO LAS REDES: ATAQUE



Campus Tecnológico-Deportivo  
para Jóvenes  
Universidad de Oviedo



**JOSÉ MANUEL REDONDO LÓPEZ**

PROYECTO “F-83 ‘NUMANCIA’” v1.0



Organiza:  
 Escuela de  
Ingeniería  
Informática  
Universidad de Oviedo

Colaboran:

Colegio Oficial de Graduados  
en Ingeniería Informática e  
Ingenieros Técnicos en Informática  
Principado de Asturias

Colegio Oficial de  
Ingenieros en Informática  
Principado de Asturias

CÁTEDRA CAPGEMINI  
PARA LA TRANSFORMACIÓN  
DIGITAL SOSTENIBLE

# ¿QUÉ ES ESTA PRESENTACIÓN?

- Una aproximación “amable” al mundo de las redes y su análisis ofensivo
  - Para cualquier persona con conocimientos técnicos básicos mínimos
  - Explica el direccionamiento de red y el uso de nmap, con una nueva forma dialogada de explicar
- Antes de seguir leyendo, si eres un experto/a esto no te va a aportar nada
  - Y quiero que sepas **que me he tomado licencias** para que se entendiera mejor
  - Sí, me he dejado cosas en el tintero **a propósito**
  - Sí, he recortado contenidos a propósito
  - Sí, no he explicado en profundidad y me he tomado licencias en algunas cosas
    - *¿A qué no sabes qué?* ¡A propósito!
  - Sí, el humor está puesto...ja propósito!
- Si esta presentación te decepciona porque no aprendes nada nuevo...
  - Lo siento mucho...pero **no eres el target de este curso**
  - ¡Pero espero que al menos te haya sacado una sonrisa! ☺
  - O ayudado a explicar estos conceptos a alguien...



La iniciativa  
“Cobra Kali” por  
José Manuel  
Redondo López



### Investigar Redes Sociales

Técnicas de investigación para RRSS

F-31 “Descubierta”



### Virtualización Básica

Creación y uso de máquinas virtuales

R-11 “Príncipe de Asturias”

Rango 1  
(Marinero)



### Investigación de Webs

Detección de webs problemáticas

S-64 “Narval”



### Entendiendo la Mente del Crimen

Mentes criminales y engaño

M-31 “Segura”



### Ataques contra Personas

Ciberacoso

P-74 “Atalaya”

Rango 2  
(Marinero de Primera)



### Ciberseguridad General

Ciberseguridad general para el día a día

F-74 “Asturias”



### Crime-spotting

Ejemplos de fraudes reales para concienciación

“Nautilus”



### Vigilancia de Redes

Entendiendo cómo funcionan las redes modernas

F-83 “Numancia”

Rango 3  
(Cabo)



Y si el cuerpo te pide marcha... ☺



La iniciativa  
"Cobra Kali" por  
José Manuel Redondo  
López



## Introducción a la Ciberdefensa Personal

Técnicas generales contra ciberataques (Niveles A1, A2)  
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



## Ciberdefensa Personal Avanzada

Técnicas avanzadas contra ciberataques (Niveles B1, B2)  
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



## Seguridad de Redes

Threat hunting  
TBA. L-52 "Castilla"

## Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas  
OCW (parcialmente). "A-21 Poseidón"



## Administración Segura de SO

Infrastructure as Code  
MUINGWEB, OCW. L-62 "Princesa de Asturias"



## Seguridad de Sistemas Informáticos

Capacitación técnica general en ciberseguridad  
Grado en Ing. del Software, OCW. S-81 "Isaac Peral"



## Defensa contra el Cibercrimen

Identificación y lucha contra el  
cibercrimen

Divulgación pública, cursos. P-45 Audaz"



Rango 1  
(Sargento)



Rango 2  
(Suboficial Mayor)



Rango 3  
(Capitán de Fragata)



Rango 4  
(Almirante)



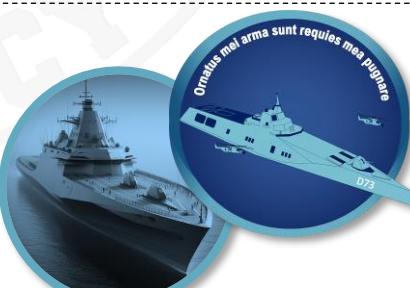
## Innovación e Investigación en Ciberdefensa

Avances e innovación en  
ciberdefensa (Nivel C2)  
Proyecto UNIDIGITAL. "BPM P-51  
'Asturias'"



## Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva: Post-  
Explotación  
TBA. K-329 "Belgorod"



## Protección de Servidores y Aplicaciones Web

CISOs de perfil técnico  
MUINGWEB, Guías INCIBE,  
Microcredenciales. D-73 y C-  
33 "Blas de Lezo"



## Desarrollo Seguro de Software

Platform engineering seguro  
Guías INCIBE. F-113 "Menéndez de Avilés"



# ÍNDICE

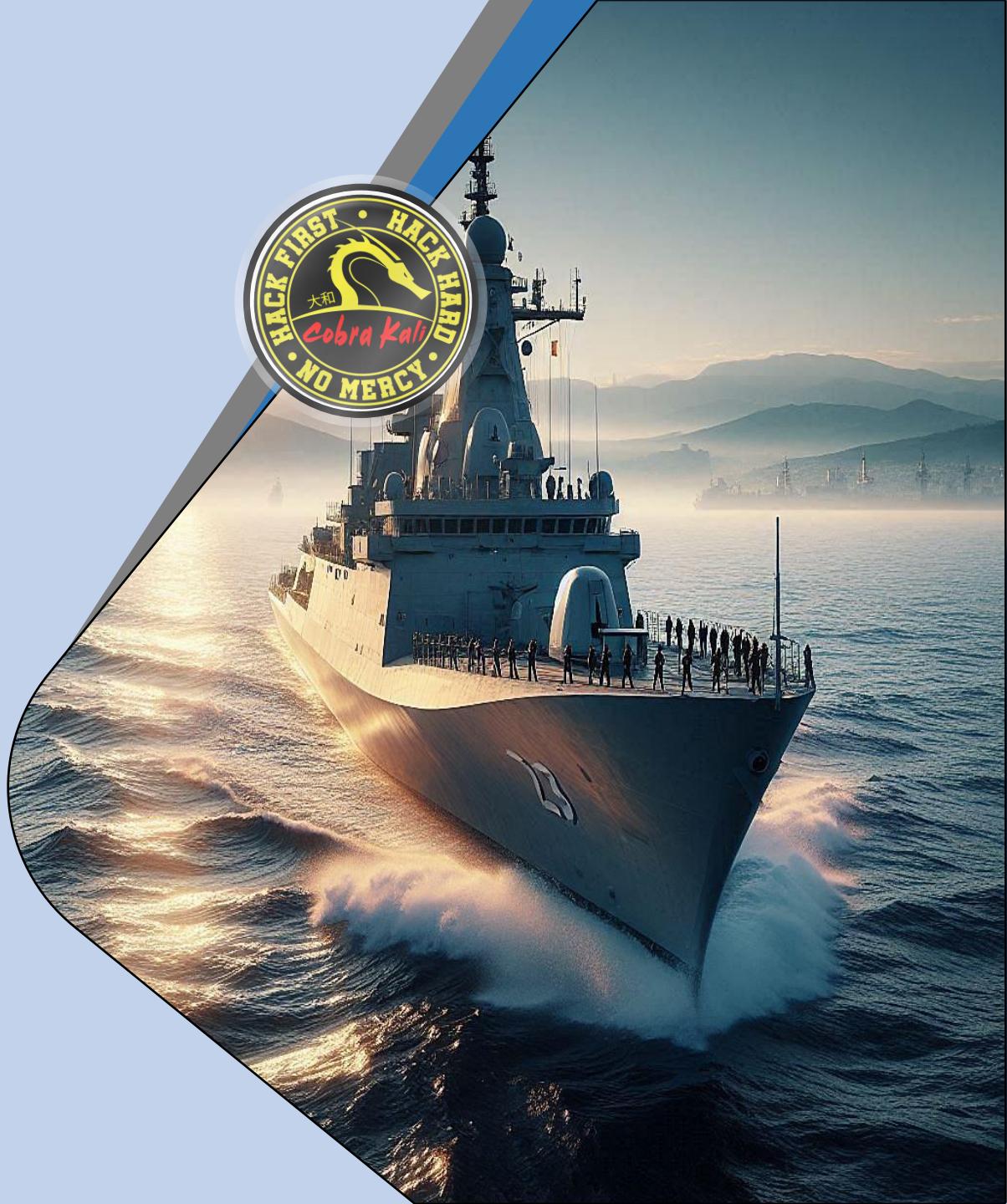


- [Un poco de teoría “light” de redes](#)
  - [Las direcciones IP](#)
  - [El DNS](#)
  - [Redes locales o LANs](#)
  - [Puertos y servicios](#)
  - [NAT y DHCP](#)
- [Nmap, el detective de la red](#)
  - [Los CVE](#)
  - [“Serious” Nmap ☺](#)
- [Shodan go on!](#)
- [Escanear vulnerabilidades](#)



# UN POCO DE TEORÍA “LIGHT” DE REDES

En serio, solo un poco ¿eh? De verdad ☺



# ¿QUÉ VAS A APRENDER EN ESTE BLOQUE?

- Entenderás cómo funciona las conexiones a Internet sin necesidad de tener demasiados conocimientos técnicos
- Sabrás lo que es exactamente la IP, o lo que es lo mismo, el “nombre” que tiene tu máquina una vez que se conecta a la red
- También sabrás qué es el DNS que, aunque no te lo creas, es lo que te permite navegar por internet sin “volverte loco”
- Entenderás la diferencia entre Internet y la red que tienes en tu casa, que no deja de ser un tipo de red especial llamada LAN
- Entenderás cómo funciona la asignación de IPs a redes de ordenadores en general
  - ¡Y todos los mecanismos que forman parte del sistema que te permite navegar por internet todos los días!



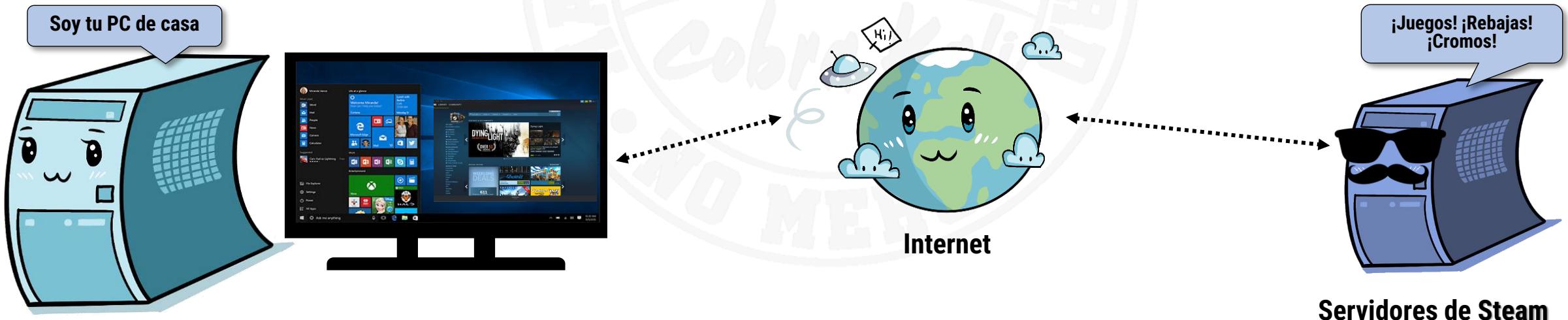
# ¿PUEDES EXPLICÁRMETO COMO SI NO TUVIERA NI IDEA?

- ¡Hola! Éste es un ordenador, como tú ordenador o el de cualquiera...
- Y, como tal, hace todo lo que sus usuarios le dicen...
  - Y lo que le ordenan los programas que usas
  - Puedes ver cada programa como un **conjunto de órdenes que le dicen a un ordenador cómo hacer ciertas tareas**
    - Escribir emails, documentos...¡todo lo que haces en tu día a día!



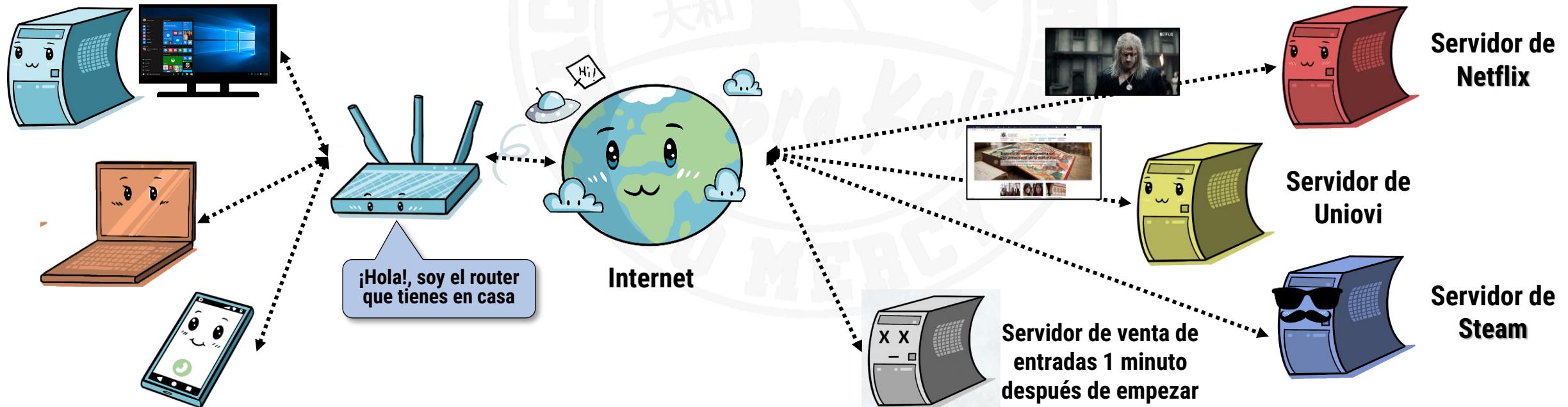
# LA “MAGIA” DE INTERNET

- Pero los ordenadores no están pensados para dar (solo) servicios a los usuarios que se sientan delante suyo...
- Algunos incluso dan servicio a usuarios que están lejos: **los servidores** 
  - Es decir, a ti, sentado en tu propio ordenador, aunque la máquina esté en la otra punta del mundo...
- Es decir, casi nadie se sienta delante de un servidor para hacer cosas “normales”
  - Te conectas a ellos desde casa, les pides cosas...y ellos te las sirven (son servidores ☺)



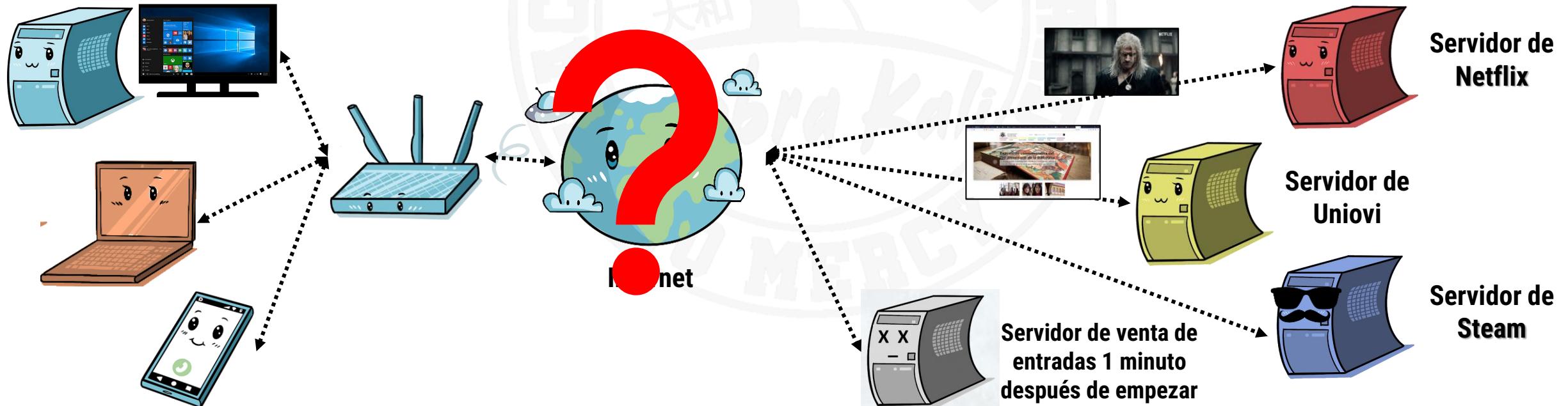
# LA "MAGIA" DE INTERNET

- ¿Cómo es eso posible?
  - Por la "magia" de las **redes de comunicaciones** 
- Principalmente por la más conocida, ¡Internet!



# LA “MAGIA” DE INTERNET

- Así que Internet es lo que permite que tu ordenador se conecte con ordenadores de todo el mundo...
- La cosa es, ¿*Nunca te has preguntado cómo funciona todo esto?* 
  - ¡Yo te lo puedo explicar para que lo entiendas! 





1  
2  
3  
4

# Las direcciones IP

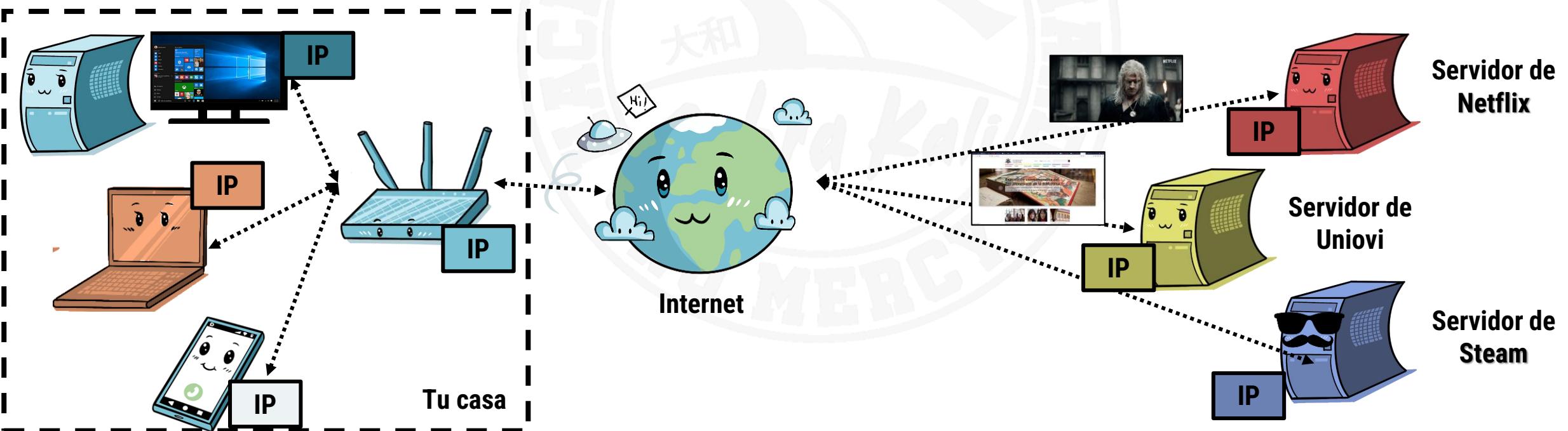
El “DNI” de los ordenadores en una red



# LA “MAGIA” DE INTERNET

- Internet funciona porque todos los equipos del mundo conectados a ella tienen una dirección única que los identifica, **su dirección IP**

- ¿Es como la MAC que nos inyectan en las vacunas del coronavirus para que el NWO nos identifique a todos desde cualquier parte?
- Más o menos...pero relajando el nivel de conspiración... 😊



# LA “MAGIA” DE INTERNET: DIRECCIONES IP

## ● Entonces... ¿Qué es una dirección IP? ¿Es como el DNI?

- ¡Parecido! Es un conjunto de 4 números separados por puntos
  - Siempre entre 0 y 255 (si en una película has visto otra cosa, la película te miente... todas lo hacen 😅)
  - Eso sería la **versión 4 (IPv4)**; también está la versión 6 (IPv6) (te hablaré de ella después)

## ● Sea la versión que sea, cada “cosa” conectada directamente a Internet es obligatorio **que tenga una IP distinta a las demás** y única, mira

- La IP de cada “cosa” conectada a Internet es “su tessssoro”

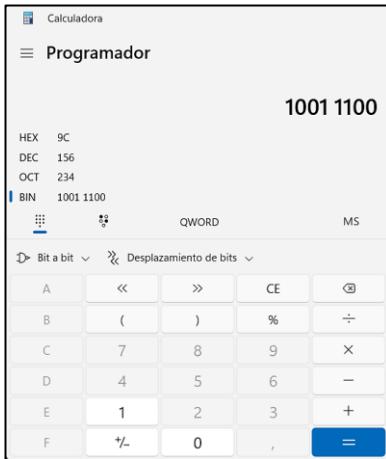


# LA “MAGIA” DE INTERNET: DIRECCIONES IP

## ● Redondo, ya vamos mal ¿¿Qué es eso???

- ¡Tranquilo/a!, eso solo **es una dirección IP en forma binaria** (1s y 0s, ya sabes) 
- Igual te suena más si uso la calculadora de Windows para convertirlo a "números de toda la vida"
- A partir de ahora las pondré con números "normales" 
  - Pero lo de ponerla en binario es una herramienta secreta que nos servirá para más adelante... 

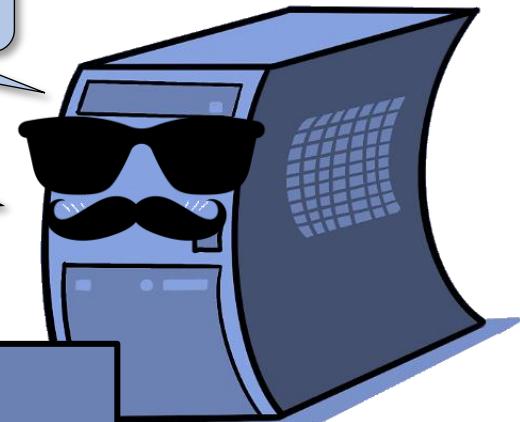
10011100.00100011.01011110.00001010



IP  
156.35.94.10

Este es el formato de IP que seguramente ya hayas visto alguna vez

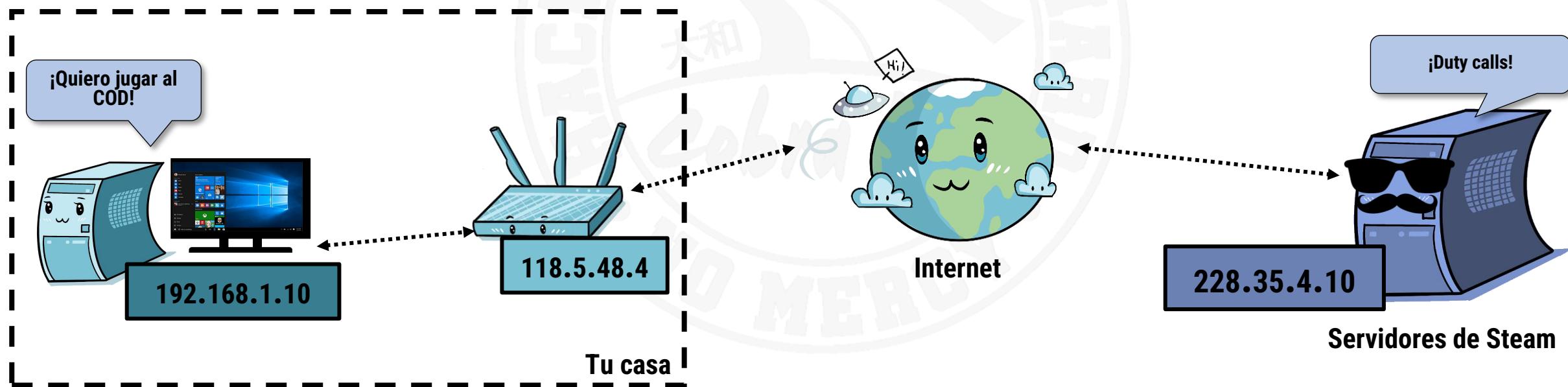
Que sí, que en alguna peli sale fijo, créeme...



# LA “MAGIA” DE INTERNET: DIRECCIONES IP

- Entonces mi máquina tiene una dirección IP (4 números), un servidor de Steam tiene una dirección IP (otros 4 números)...y así con todo

- Cuando arrancas tu Steam, se conecta a la IP del servidor de Steam, le pide tu información, y la envía a la IP de tu máquina, y todo funciona perfectamente....
- O bien te levantas por la mañana, abres Twitter en el navegador, pones la IP de un servidor de Twitter y empiezas a leer hate y gente diciéndote lo que tienes que hacer para triunfar en la vida...
  - Lo normal, vamos 😅



# LA “MAGIA” DE INTERNET: LOS DNS

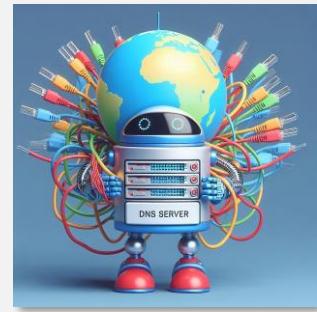
- Redondo, pero yo no pongo la IP de Twitter, yo pongo la dirección, "www.twitter.com" campeón, artista, tiranosaurio...

- ¡Je, je! Ya lo sé... 😎
- Eso es porque hay una cosa que aún no te he dicho: que Internet necesita otra cosa “en medio” para funcionar, ¡los DNS! ↔  
ON!
- ¡Vamos a ir descubriendo cosas poco a poco!

Hazte a la idea de que soy como un enorme listín de teléfonos o, en términos modernos, la lista de seguidores de Ibai 😊

Conozco las URL de todas las IPs de Internet (y si no las sé yo directamente, se a quien preguntarle). ¡Nada se me escapa!





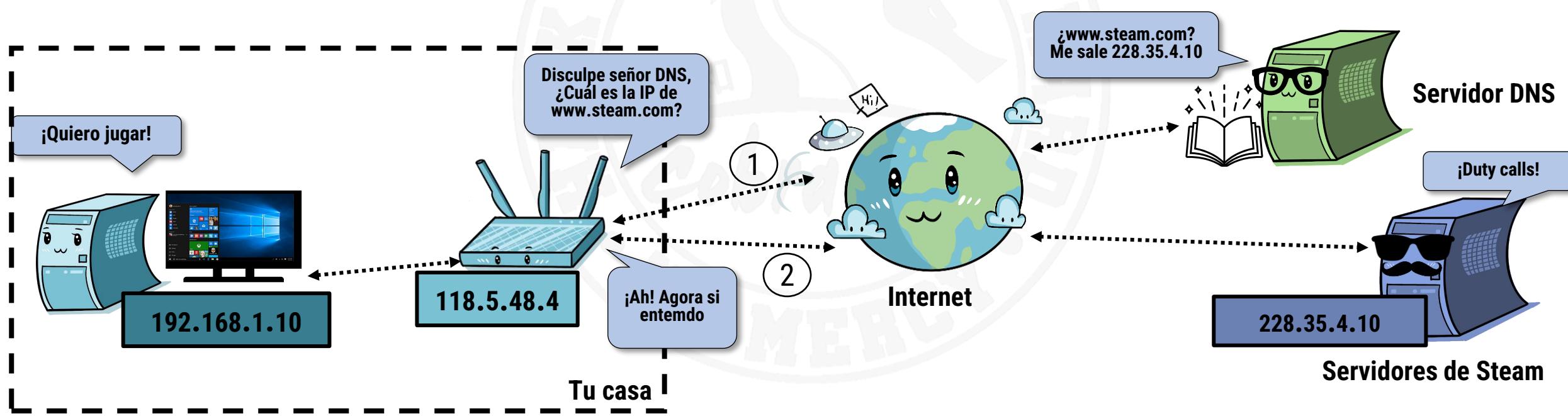
## El DNS

El “diccionario” que nos permite usar Internet



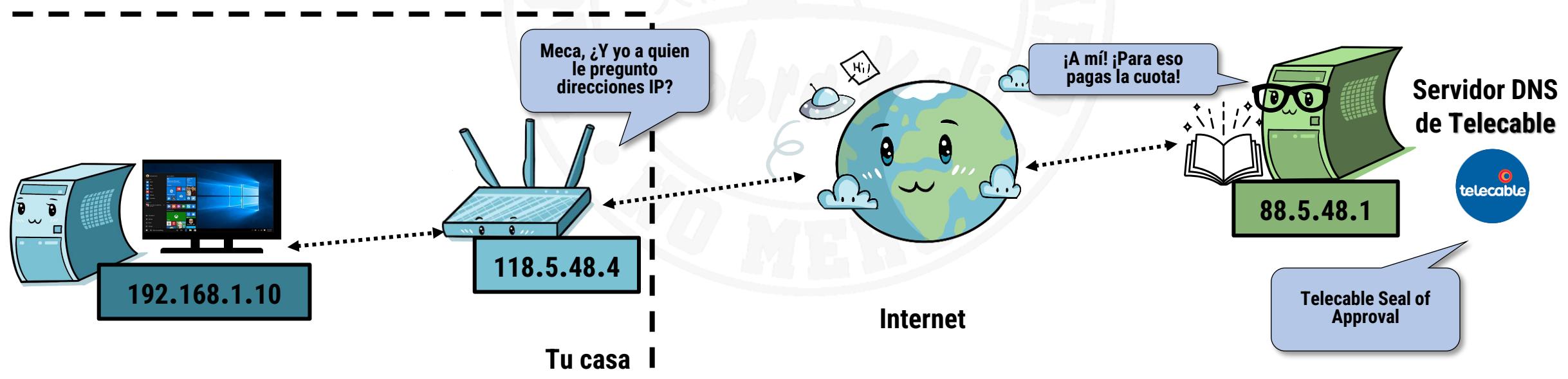
# LA “MAGIA” DE INTERNET: LOS DNS

- Sin meternos demasiado en tecnicismos, un DNS es un servicio (que está en un servidor) al que le preguntas *¿Cuál es la IP de esta URL que te paso?*
  - ¡Y te la dice!
- Pero se le pregunta automáticamente, tú no ves nada
  - Es todo **transparente y automático**, y pasa muchas veces mientras navegas 😊



# LA “MAGIA” DE INTERNET: LOS DNS

- *¿O sea que hay una “cosa” que se encarga de que cada vez que pongo una dirección en el navegador se obtenga su IP sin que yo haga nada más?*
  - ¡Exacto! ¡Todo es automático! Es la “magia” de Internet 
- *¿Y quién pone esa “cosa” ahí? ¿Cómo sabe el navegador la IP de esa máquina-diccionario de IPs tan importante?*
  - ¡Normalmente tu proveedor de Internet le da a tu router la IP de un DNS que puedes usar!
  - ¡O tú mismo le puedes decir IPs donde buscar uno! (**los hay públicos**)

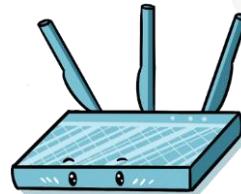


# LA “MAGIA” DE INTERNET

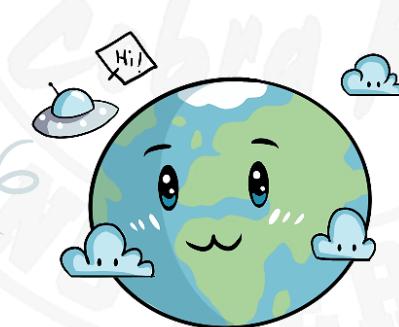
- **¿Y todo es siempre así?**
  - Mientras estás en Internet, sí
- **Si lo que tienes es una “red local” (también llamada **LAN**), entonces seguramente no haya DNS**
  - Y los dispositivos se localicen entre sí por IP directamente
  - *¿Red local? ¿Ostras y esa movida? ¡Me dejas loco/a!*
  - Tranqui, que es lo siguiente que se viene ☺ ¡poco a poco!



Tus dispositivos



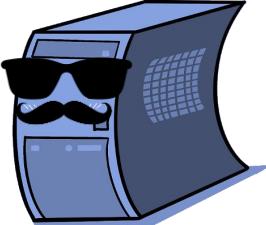
Tu router de casa



Internet



Servidor DNS



Servidores de los  
distintos servicios a los  
que accedes

¡Todos somos actores principales en esta obra! ☺

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Has entendido lo que es una dirección IP, y que dos máquinas en la misma red no deben tener la misma porque si no, no funcionaría?*
- *A consecuencia de lo anterior ¿Entiendes que dos máquinas en distintas redes que nunca se van a ver pueden tener la misma IP y no pasaría nada?*
  - Es parecido al hecho de que haya personas que se llamen igual que tú en otras provincias ☺
- *¿Entiendes que, gracias al DNS, puedes navegar como lo haces ahora, poniendo nombres de páginas en lugar de “numeritos” (las IPs, vamos) de esas páginas?*
- *¿Te ha quedado claro que todo esto es automático?*



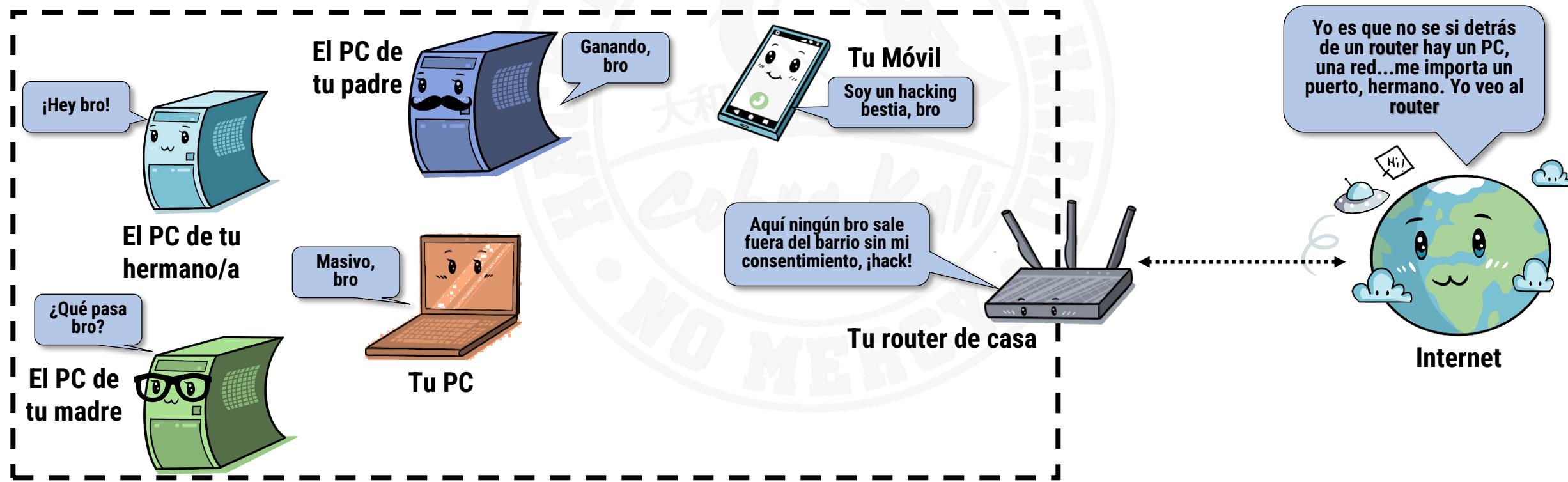
# Redes locales o LANs

Redes “de proximidad” (como la de tu casa)



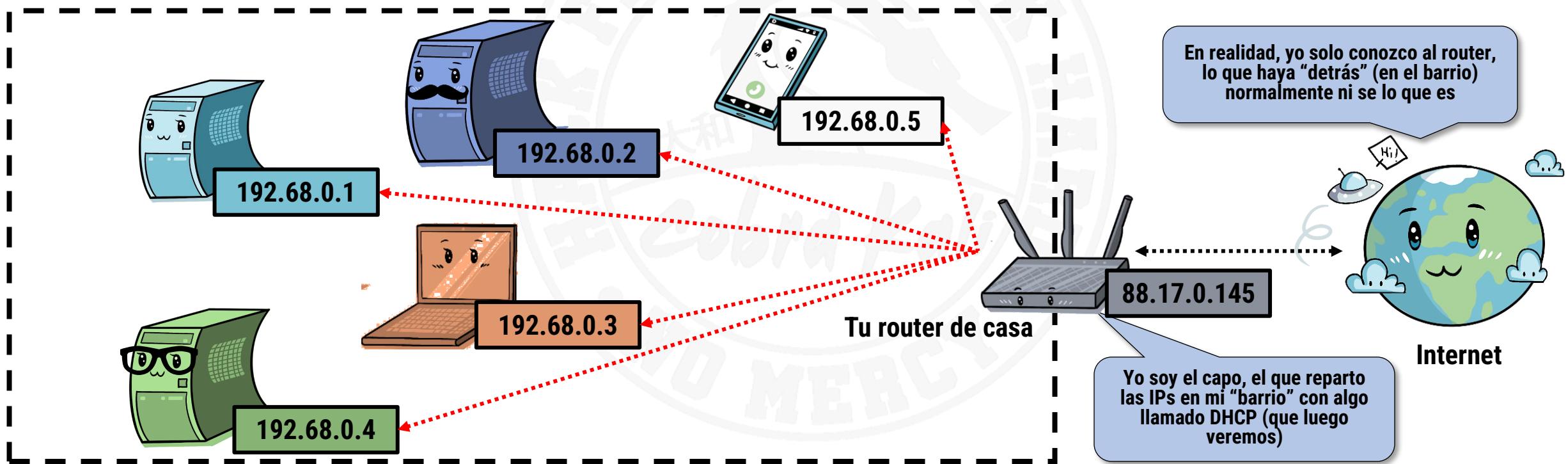
# LA “MAGIA” DE INTERNET: REDES LOCALES

- Meca, meca, ¿*Red local?* ¿¿Qué es eso?? Pues como un “barrio” 😊
- Un montón de ordenadores conectados entre sí, pero que al no haber DNS se comunican directamente por IP
  - O, normalmente, lo que hay “detrás” de tu **router** (en tu casa, vamos)



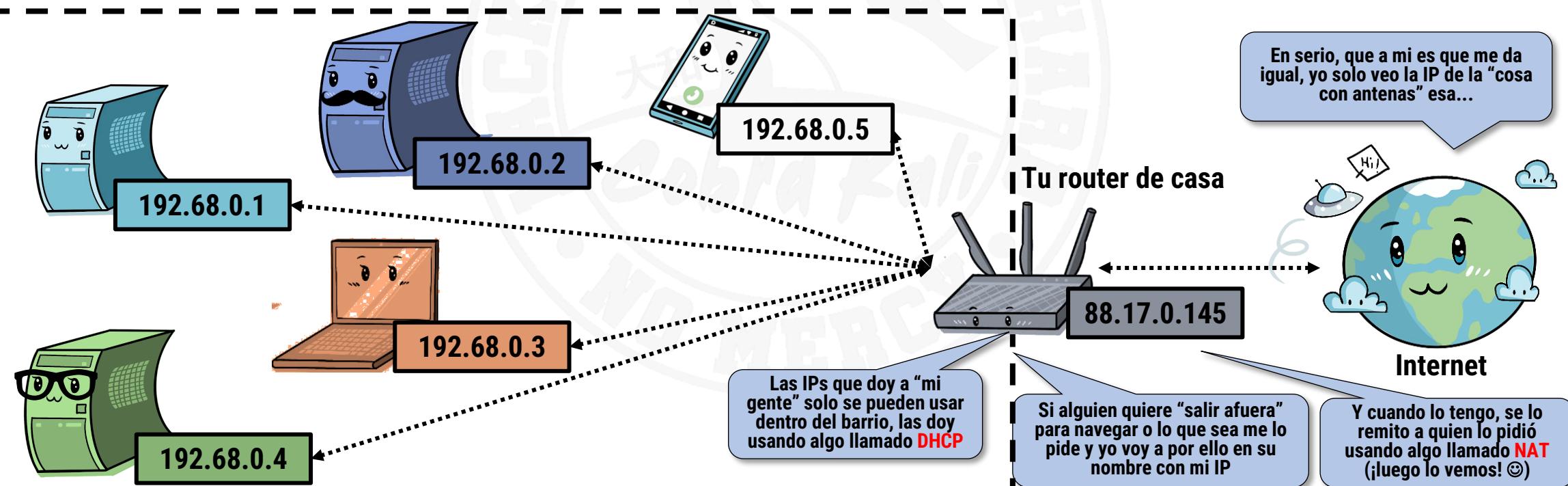
# LA “MAGIA” DE INTERNET: REDES LOCALES

- Ostras, y si no hay nadie a quien preguntarle dónde está cada uno... ¿Cómo se entienden entre ellos?
- Porque el aparato que los comunica sabe los que son del mismo “barrio”
  - ¿Aparato? ¿Qué aparato? ¡Pues tu router de casa es el que hace eso!



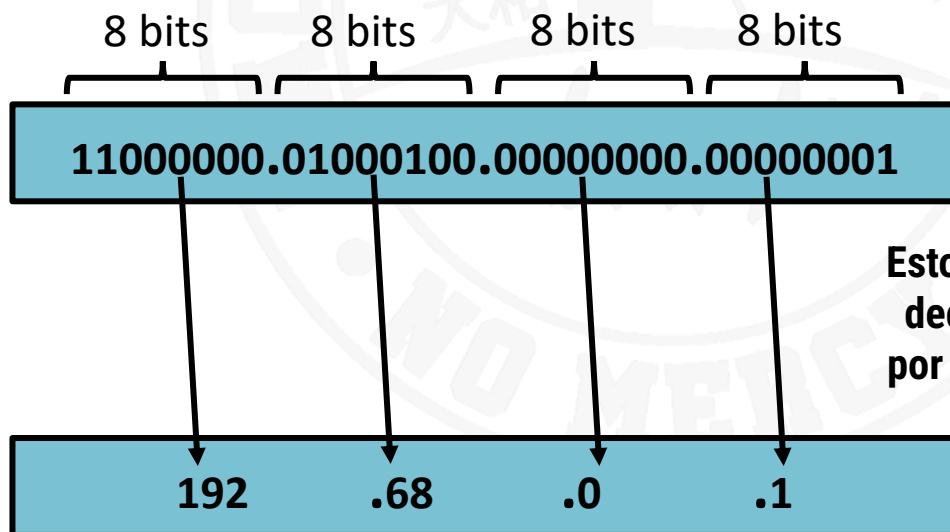
# LA “MAGIA” DE INTERNET: REDES LOCALES

- ¿Y cómo saben las máquinas a qué “barrio” pertenecen? ¡Por su dirección IP!
  - Pertenecen al mismo barrio todas las máquinas que tienen **IP compatibles**
- Me pierdo... ¿Me lo puedes explicar de forma sencilla por favor? 😞
  - ¡Cuenta con ello! ¡“José” es mi nombre y “explícalo sencillo” mi tercer apellido! 😊



# LA “MAGIA” DE INTERNET: REDES LOCALES

- Una IP es compatible con otra **si empiezan por los mismos N bits**, siendo N un número establecido por la definición de lo que es el “barrio” (red)
  - Quizá pienses “No me lo estás haciendo más fácil de entender...”
- ¡Espera! Mira esta IP y su “traducción” a nºs decimales
  - Ahora entenderás porque antes empecé poniendo 1s y 0s cuando puse la primera IP 😊

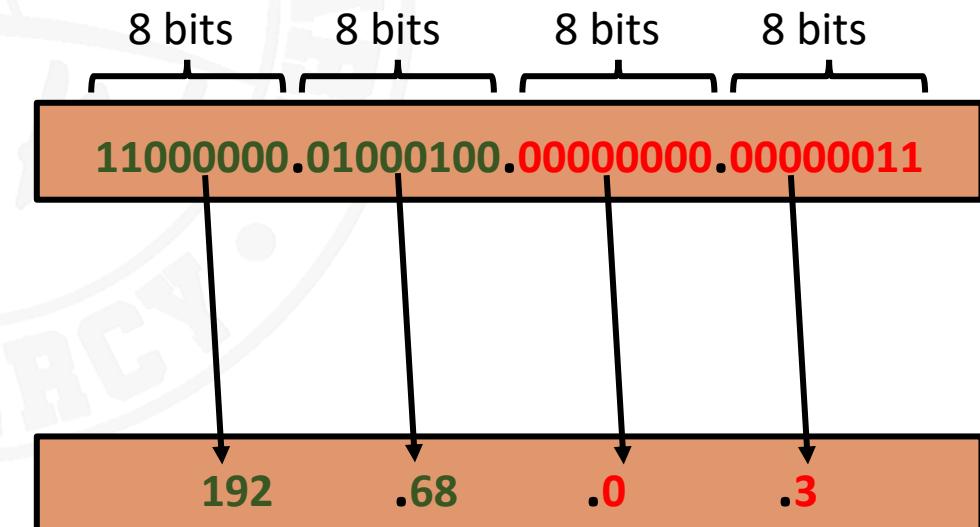
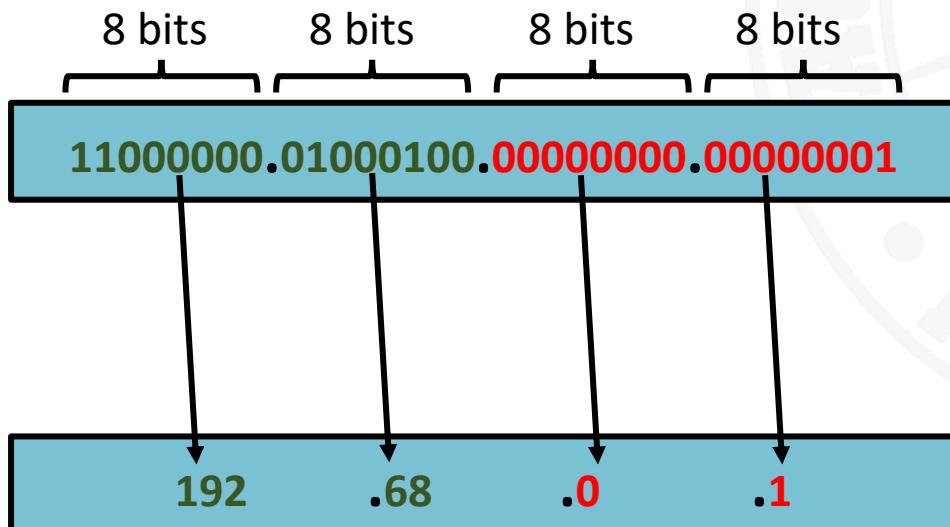


Esto es una traducción de nºs binaries a su equivalente en decimal. No tienes ni que entenderla ni que preocuparte por eso ahora. Si te resulta curioso, lo hace la calculadora de Windows fácil, como vimos antes 😊

# LA “MAGIA” DE INTERNET: REDES LOCALES

- Ahora imagina que te digo que dos IPs son compatibles si tienen los primeros 16 bits iguales

- ¿Estas dos serían compatibles? ¡SI!
- Es como los grupos sanguíneos compatibles...¡pero más fácil! :D



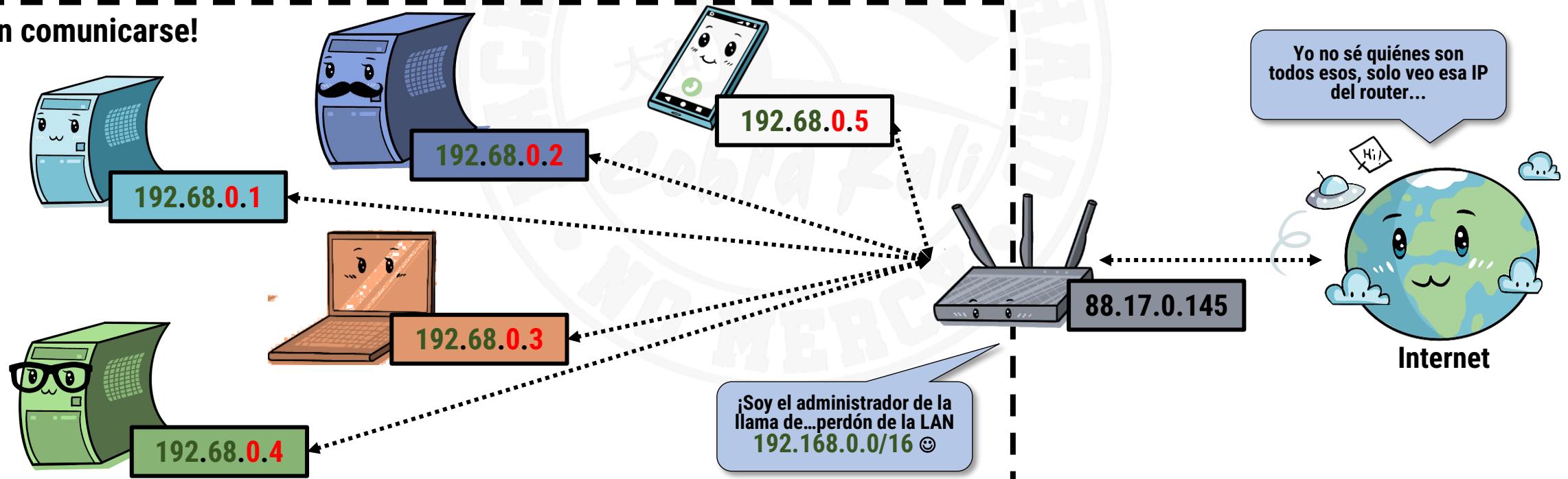
# LA “MAGIA” DE INTERNET: REDES LOCALES

- Así puedo decir que todas las IPs que empiecen por 192.168 (8+8 = 16 bits)...
  - ...son del mismo “barrio”, no me importa que números tengan detrás

- ¿Y cómo se escriben todas las IPs que pertenecen a un “barrio” dado?

- Así, por ejemplo: **192.168.0.0/16**
- N es 16, y ¡“192.168.0.0/16” es como se definiría esa red local o “barrio”!
- ¿Y eso tiene un nombre “chulo” para basilah a la peña? ¡Sí! **“Máscara CIDR”** (Cider, como Sidra :P)

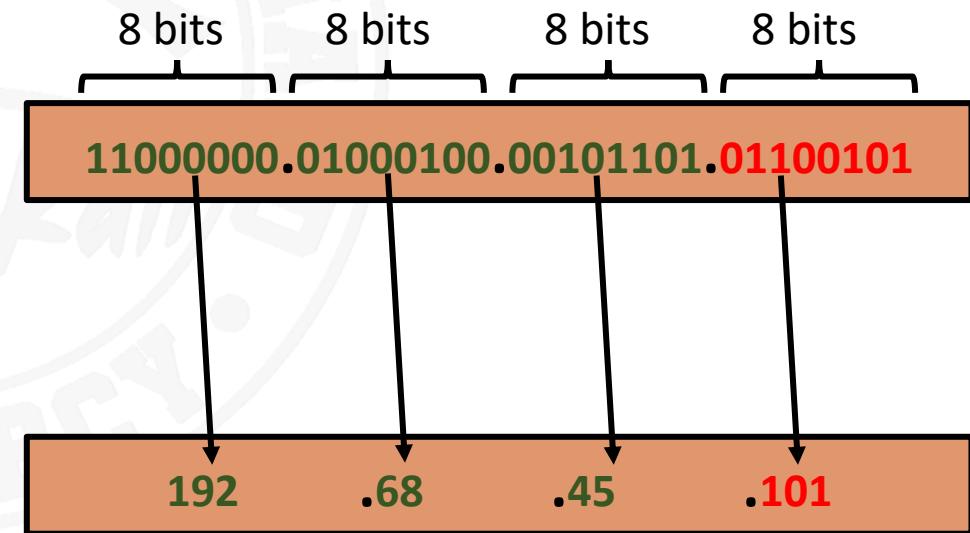
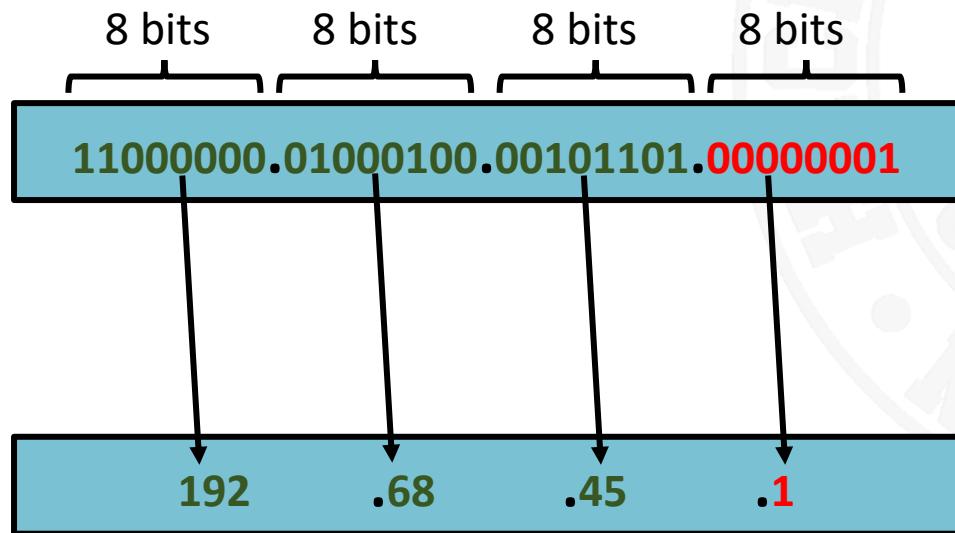
¡Pueden comunicarse!



# LA “MAGIA” DE INTERNET: REDES LOCALES

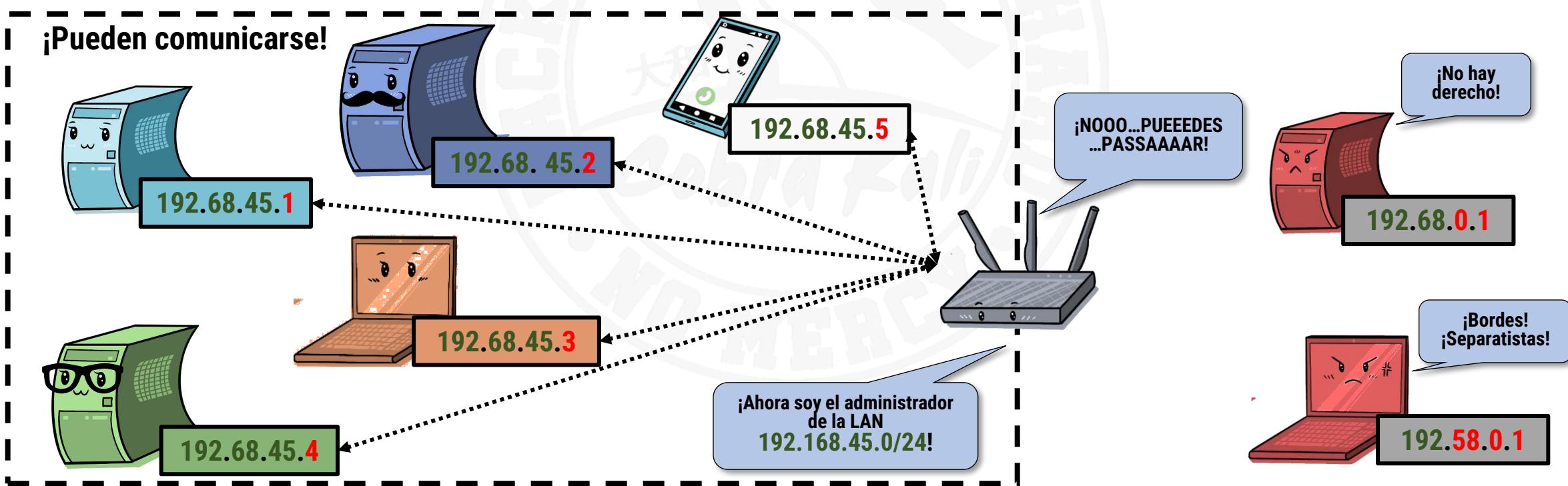
## • ¿Crees que estas a punto de pillarlo?... Pues te pongo otro ejemplo

- Si ahora te digo que la red es 192.168.45.0/24, mira lo que pasa
- ¡Las IPs son compatibles si tienen los tres primeros números iguales! ( $8+8+8 = 24$  bits)



# LA “MAGIA” DE INTERNET: REDES LOCALES

- Al final, el truco está en entender que /8 es que el primer número queda fijo
  - /16 el primero y el segundo, y /24 los tres primeros
- Se pueden poner otros números, pero es más complicado
  - No queda tan “redondo”, y no hace falta que nos metamos en más “fregaos” ahora mismo 😊
  - ¡De todas formas, /8, /16, /24 son los que más se usan a nivel mundial! ;)



# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Eres capaz de distinguir la entre una LAN e internet?*
- *¿Crees que ahora eres capaz de saber lo que es una máscara CIDR si la ves escrita en alguna parte?*
- *¿Crees que ahora sabrías decir cuándo una dirección IP pertenece o no pertenece a una red?*
- *¿Entiendes que, en el fondo, la mayoría de las IPs de las redes de casa dejan los tres primeros nºs iguales y cambia solo el último?*
  - Por lo que si sabes la IP de una de tus máquinas, la probabilidad de que la siguiente sea justo la misma, pero sumando uno al último nº es alta 😊
  - ¿Para qué complicarse la vida? 😊



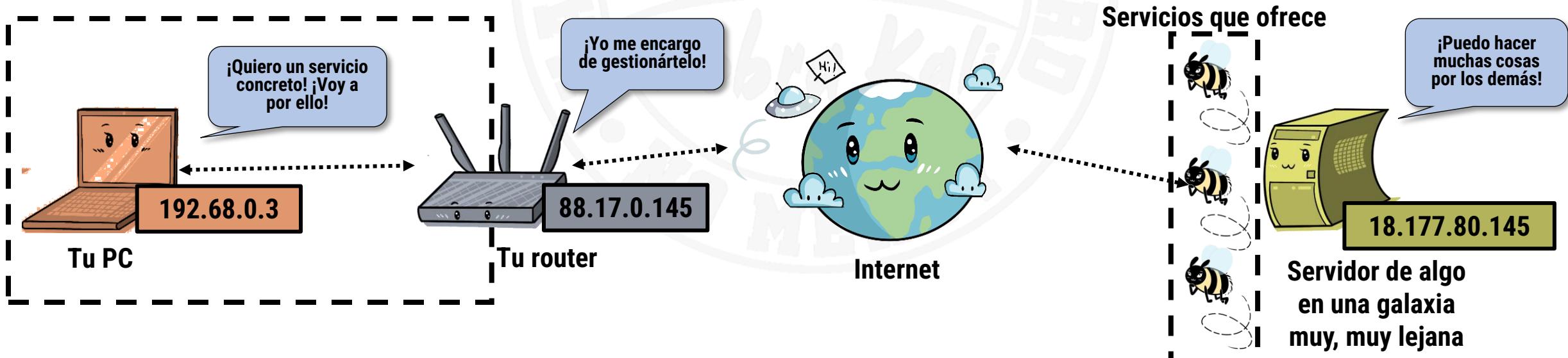
# Puertos y servicios

No creas que una máquina solo sirve para una sola cosa 😊



# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

- Vale, vale, oye, ahora puedo “llegar” a una máquina porque sé su IP...pero
  - ¿Cómo sé qué “cosas” tiene funcionando? ¿Qué servicios me ofrece?
- Y así se llaman, **servicios** que dan a los demás, e Internet está **PETADO** de ellos
  - Ver y trabajar en páginas web (estas máquinas se llaman **servidores web**)
  - Trabajar desde casa en ella (el famoso escritorio remoto)
  - Descargarse ficheros... (**servidores de descargas**)
  - Ver un streaming de video (**servidores de streaming: Netflix, HBO Max...**)
  - Ver un gameplay de algún juego (o jugar a él en red) (**servidores del LoL, Valorant...**)



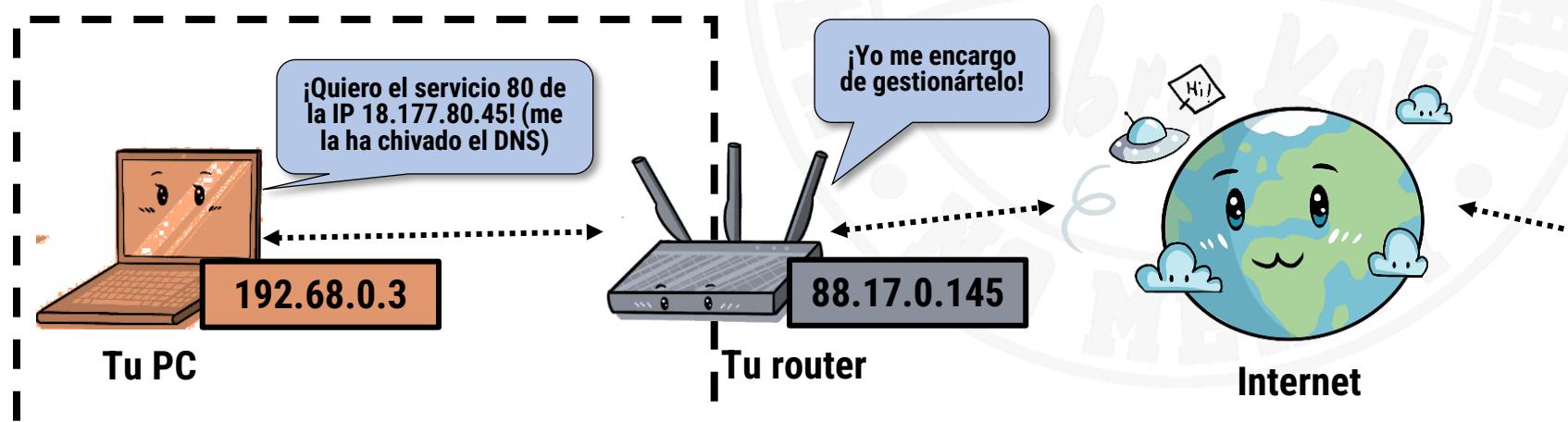
# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

## ● ¡No has contestado a mi pregunta!

- Ya, ya, te iba a decir que cada uno de esos servicios está en un “sitio” de la máquina conocido
- A esos sitios se les llama **Puertos**

## ● Y dirás...¿*Puertos*?

- Sí, como las puertas de un aeropuerto (de hecho, **son números**)



Servicios que ofrece,  
con sus nºs de puerto



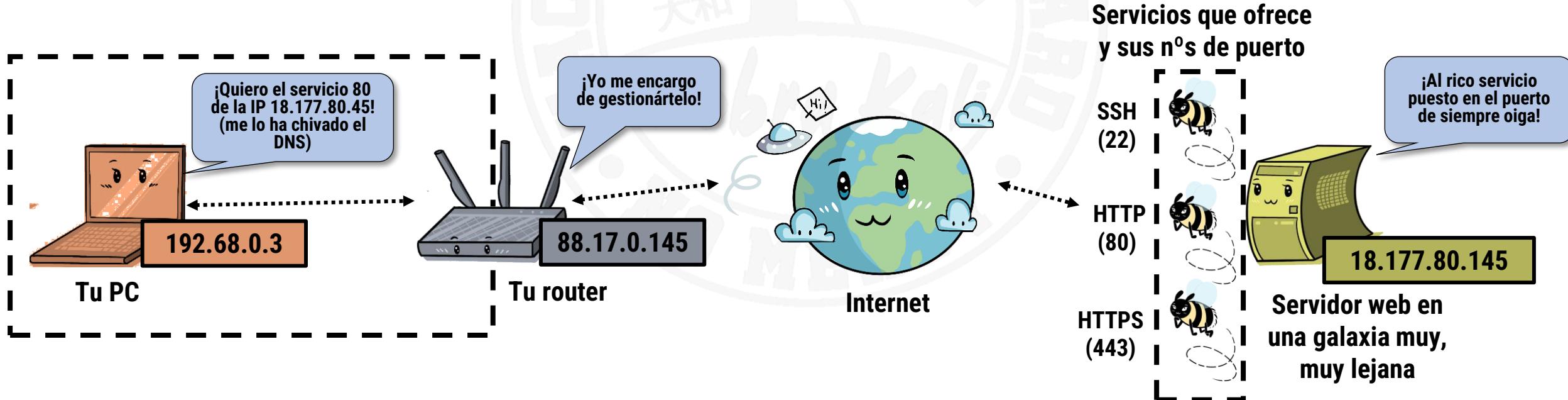
# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

## ● ¿Y cómo sabes a qué puerto vas?

- ¡Ah, amigo!, es que **para servicios típicos** normalmente se sabe el puerto al que ir siempre...
- Porque, por convenio, ¡**normalmente están siempre en el mismo!**

## ● O sea, que ¿Si yo sé que una máquina sirve una web, sé a qué puerto ir?

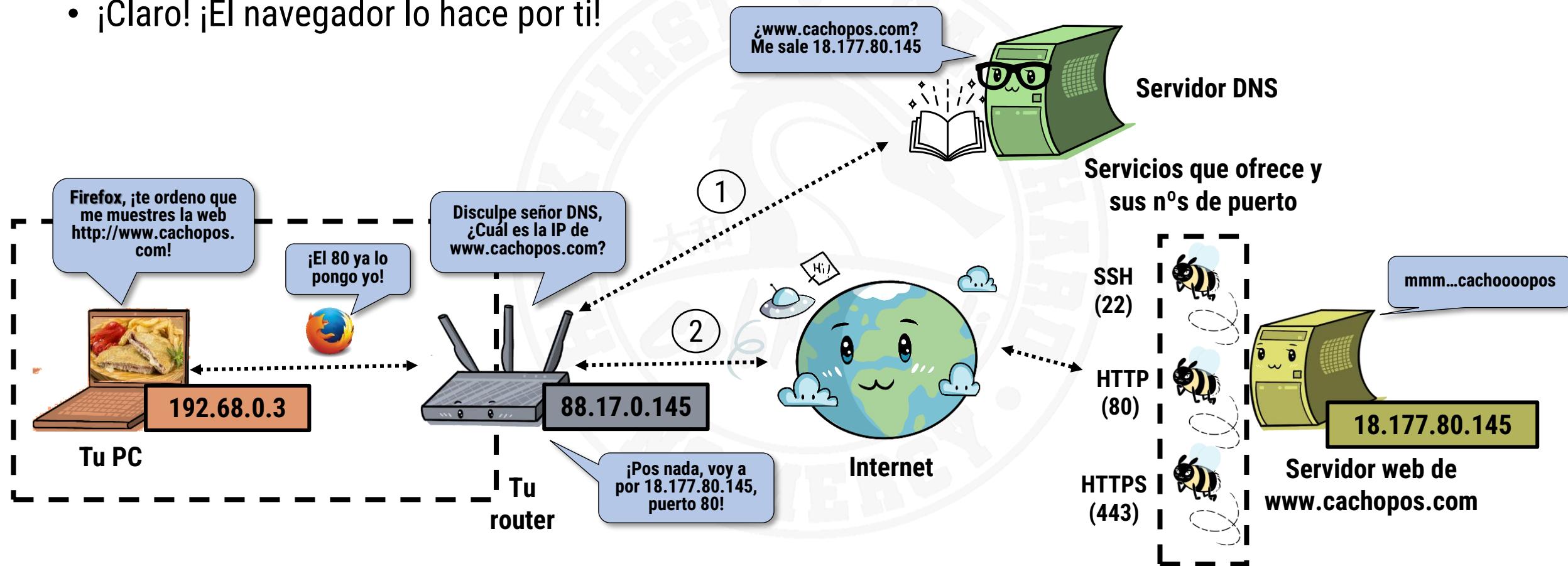
- ¡Sí! Siempre es el 80 (**http**)
- O el 443 (**https**, si la web va con candado, es decir, la transmisión no se puede “cotillear”)



# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

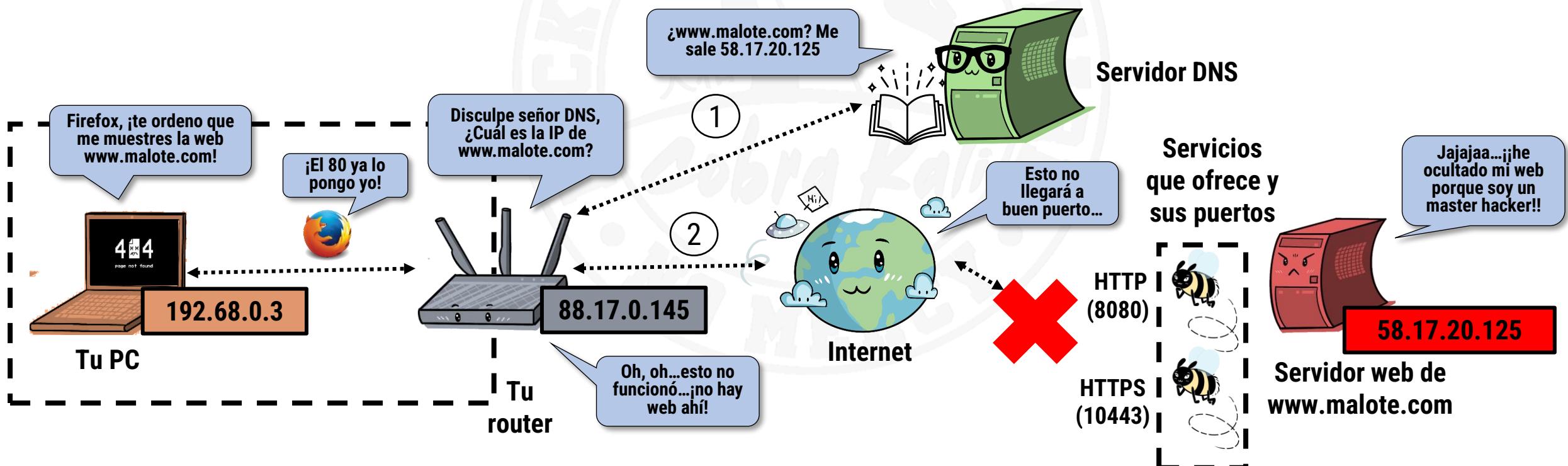
- ¡Pero yo nunca pongo puertos de nada en el navegador!

- ¡Claro! ¡El navegador lo hace por ti!



# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

- Oye, ¿Y si algún listo le da por colocar un servicio de esos en un puerto que casi nadie usa para él? ¿Qué pasa? ¿Está prohibido?
  - ¡No! Es su problema...la gente “normal” no podrá usarlo
- Pero eso no significa que no podamos descubrirlo...de hecho, ¡acabas de descubrir la principal utilidad de nmap! 💀





# PUERTOS CONOCIDOS

- Y no estaba de broma, de verdad hay un montón de puertos (nºs) donde habitualmente hay un servicio conocido

- ¡Especialmente si el número de puerto es menor de 1000!

- Esos son más bien fijos
- Los mayores de 1000 pues...bueeeeeno ☺

## COMMON PORTS

COMMON PORTS		TCP/UDP Port Numbers	
7	Echo	554	RTSP
19	Chargen	546-547	DHCPv6
20-21	FTP	560	rmonitor
22	SSH/SCP	563	NNTP over SSL
23	Telnet	587	SMTP
25	SMTP	591	FileMaker
42	WINS Replication	593	Microsoft DCOM
43	WHOIS	631	Internet Printing
49	TACACS	636	LDAP over SSL
53	DNS	639	MSDP (PIM)
67-68	DHCP/BOOTP	646	LDP (MPLS)
69	TFTP	691	MS Exchange
70	Gopher	860	iSCSI
79	Finger	873	rsync
80	HTTP	902	VMware Server
88	Kerberos	989-990	FTP over SSL
102	MS Exchange	993	IMAP4 over SSL
110	POP3	995	POP3 over SSL
113	Ident	1025	Microsoft RPC
119	NNTP (Usenet)	1026-1029	Windows Messenger
123	NTP	1080	SOCKS Proxy
135	Microsoft RPC	1194	OpenVPN
137-139	NetBIOS	1214	Kazaa
143	IMAP4	1241	Nessus
161-162	SNMP	1311	Dell OpenManage
177	XDMCP	1337	WASTE
179	BGP	1433-1434	Microsoft SQL
201	AppleTalk	1512	WINS
264	BGMP	1589	Cisco VQP
318	TSP	1701	L2TP
381-383	HP Openview	1723	MS PPTP
389	LDAP	1725	Steam
411-412	Direct Connect	1741	CiscoWorks 2000
443	HTTP over SSL	1755	MS Media Server
445	Microsoft DS	1812-1813	RADIUS
464	Kerberos	1863	MSN
465	SMTP over SSL	1985	Cisco HSRP
497	Retrospect	2000	Cisco SCCP
500	ISAKMP	2002	Cisco ACS
512	rexec	2049	NFS
513	rlogin	2082-2083	cPanel
514	syslog	2100	Oracle XDB
515	LPD/LPR	2222	DirectAdmin
520	RIP	2302	Halo
521	RIPng (IPv6)	2483-2484	Oracle DB
540	UUCP	2488-2489	MySQL
		2745	Bagle.H
		2967	Symantec AV
		3050	Interbase DB
		3074	XBOX Live
		3124	HTTP Proxy
		3127	MyDoom
		3128	HTTP Proxy
		3222	GLBP
		3260	iSCSI Target
		3306	MySQL
		3389	Terminal Server
		3689	iTunes
		3690	Subversion
		3724	World of Warcraft
		3784-3785	VentriLO
		4333	mSQL
		4444	Blaster
		4664	Google Desktop
		4672	eMule
		4899	Radmind
		5000	UPnP
		5001	Slingbox
		5001	iperf
		5004-5005	RTP
		5050	Yahoo! Messenger
		5060	SIP
		5190	AIM/ICQ
		5222-5223	XMPP/Jabber
		5432	PostgreSQL
		5500	VNC Server
		5554	Sasser
		5631-5632	pcAnywhere
		5800	VNC over HTTP
		5900+	VNC Server
		6000-6001	X11
		6112	Battle.net
		6129	DameWare
		6257	WinMX
		6346-6347	Gnutella
		6500	GameSpy Arcade
		6566	SANE
		6588	AnalogX
		6665-6669	IRC
		6679/6697	IRC over SSL
		6699	Napster
		6881-6999	BitTorrent

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

by Jeremy Stretch

v1.1

- Legend**
- Chat
  - Encrypted
  - Gaming
  - Malicious
  - Peer to Peer
  - Streaming

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *¿Has entendido lo que es un servicio?*
- *¿Y lo que es un puerto?*
- *¿Y la relación entre ambos?*
- *¿Comprendes entonces que cada vez que navegas lo que estás haciendo es acceder a un servicio (un servidor web) que te da una máquina que está en una IP remota?*
- *¿Y que tu navegador se conecta al puerto adecuado donde está ese servicio en la máquina remota, todo ello automáticamente?*
- *¿Te das cuenta de que casi todo Internet es automático?*



## NAT y DHCP

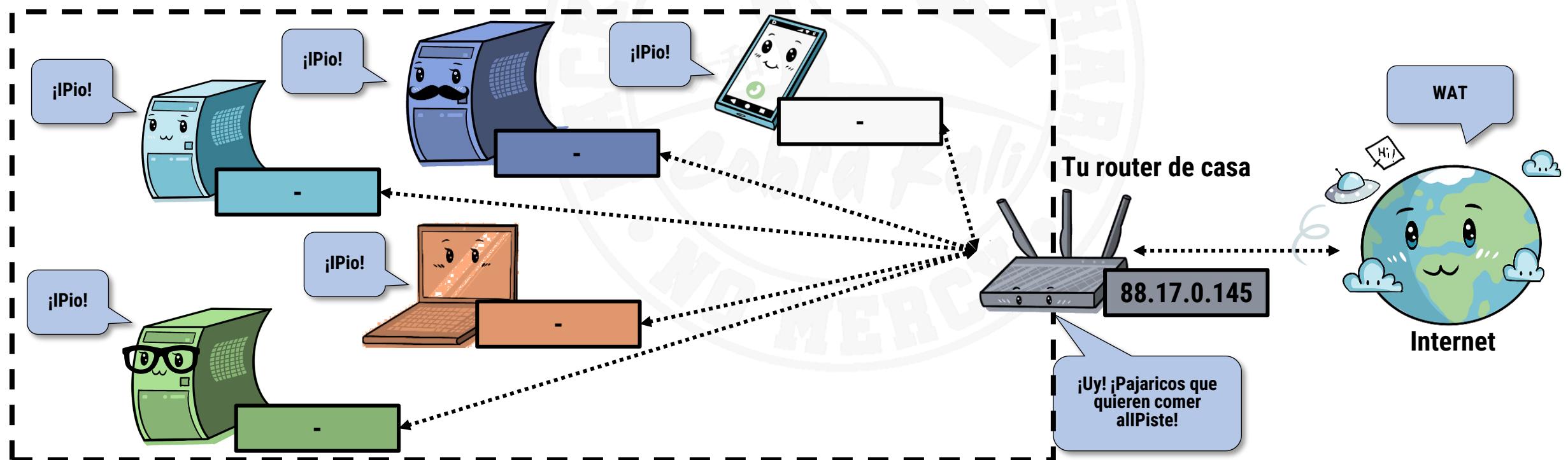
¡Los últimos elementos para entender todo!



# ¿DHCP? ¿MÁS ACRÓNIMOS?

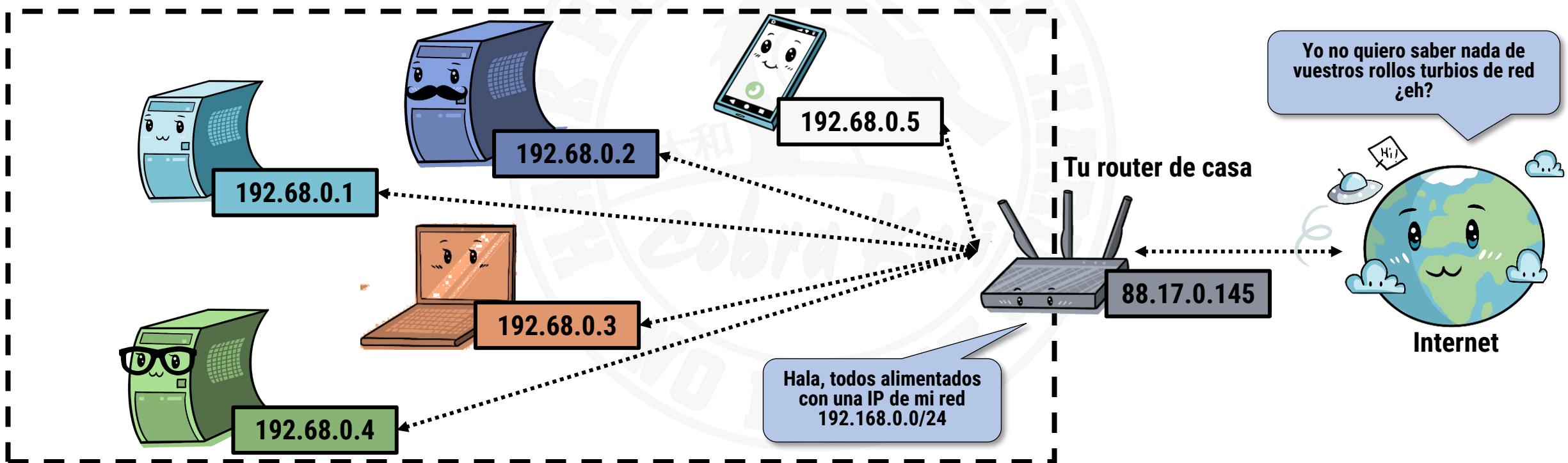
- Antes mencionamos de pasada dos acrónimos, NAT y DHCP, que son parte de la “magia” que hace funcionar todo esto

- DHCP es lo que hace que todo lo que se conecta a tu router y pone la clave de la Wifi bien (o lo hace por cable) tenga **automáticamente** una IP
- **El dispositivo conectado pide una IP y el router** se la da
- Sin más historia que merezca la pena contar aquí ☺



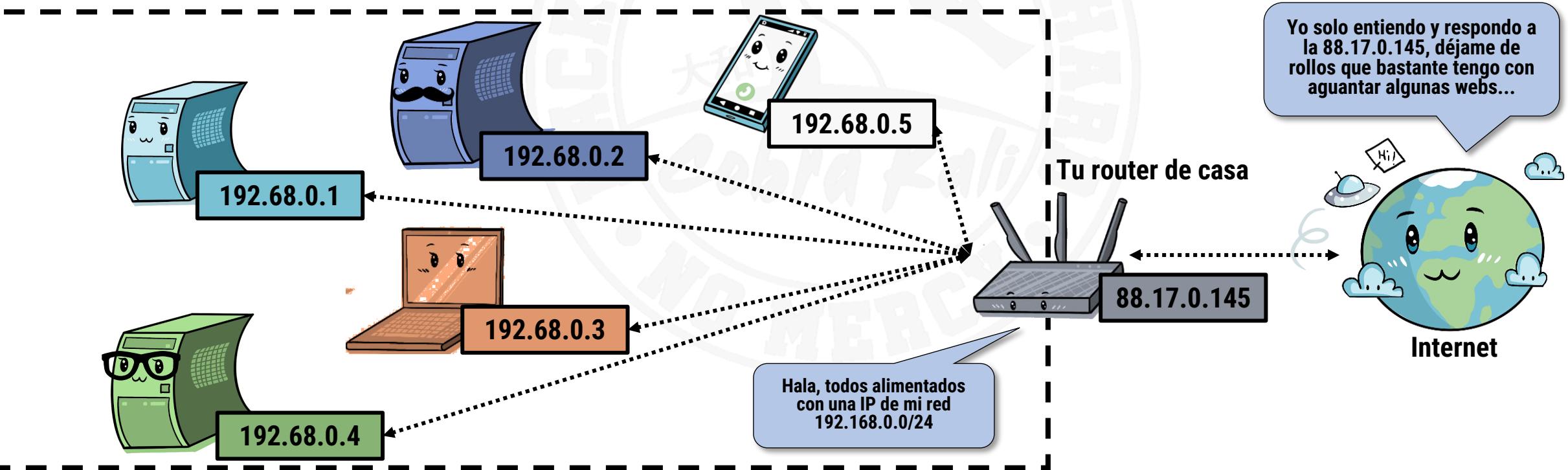
# DHCP

- Y así, cada vez que conectas algo al router todo funciona automágicamente
  - ¡Gracias a DHCP conectarse a una red es muy muy sencillo para nosotros!
- Por debajo pasan “cosas netsys” pero...francamente queridos/as, no nos importa



# IPs PRIVADAS

- Mmmm...pero yo he oído que las IPs se acaban, ahora entiendo por qué
  - Bueno, es verdad, pero en realidad los routers hacen “trampa” para que se agoten más despacio...
- ¡Tus dispositivos tienen IPs privadas!
  - Es decir, IPs que solo valen para comunicarse **sólo con otras “cosas” conectadas al mismo router**
  - Las de tu casa, vamos....



# IPs PRIVADAS

• **¿Me estás diciendo que mi router me da IPs que NO SIRVEN para ir a Internet? SÍ**

- **Solo tu router está directamente conectado a Internet** (y no siempre como veremos luego...)
  - Así tu proveedor ahorra mucho dinero (las IPs conectadas a Internet cuestan mucha pasta)
  - Y tú pues...no te enteras ☺
- **¿Ves los rangos de IPs de la segunda columna de esta tabla? Está prohibido usarlos en Internet**
- **“Detrás” de distintos routers puede haber dispositivos con la misma IP privada**
  - ¡Da lo mismo! Nadie va a verlas fuera del router, ¡no hay colisión posible!

Nombre	Rango de direcciones IP	Cantidad de IPs	N.º de Redes	Cantidad de IP por Red	Mayor bloque CIDR
Bloque de 24 bits	10.0.0.0 – 10.255.255.255	16.777.214	1	16.777.214	10.0.0.0/8 (255.0.0.0)
Bloque de 20 bits	172.16.0.0 – 172.31.255.255	1.048.576	16	65.534	172.16.0.0/12 (255.240.0.0)
Bloque de 16 bits	192.168.0.0 – 192.168.255.255	65.534	256	254	192.168.0.0/16 (255.255.0.0)
Bloque de 16 bits	169.254.0.0 – 169.254.255.255	65.534	1	65.534	169.254.0.0/16 (255.255.0.0)



Tu router de casa

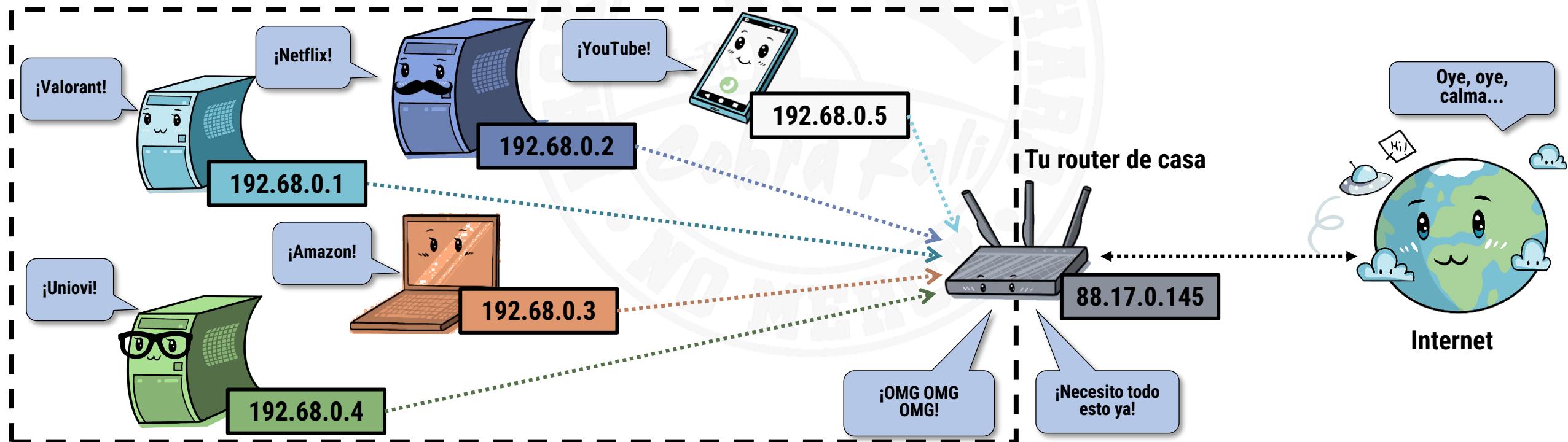
# NAT

- Pero... ¿*Como es posible?* ¡Si yo navego a donde quiero sin problema!

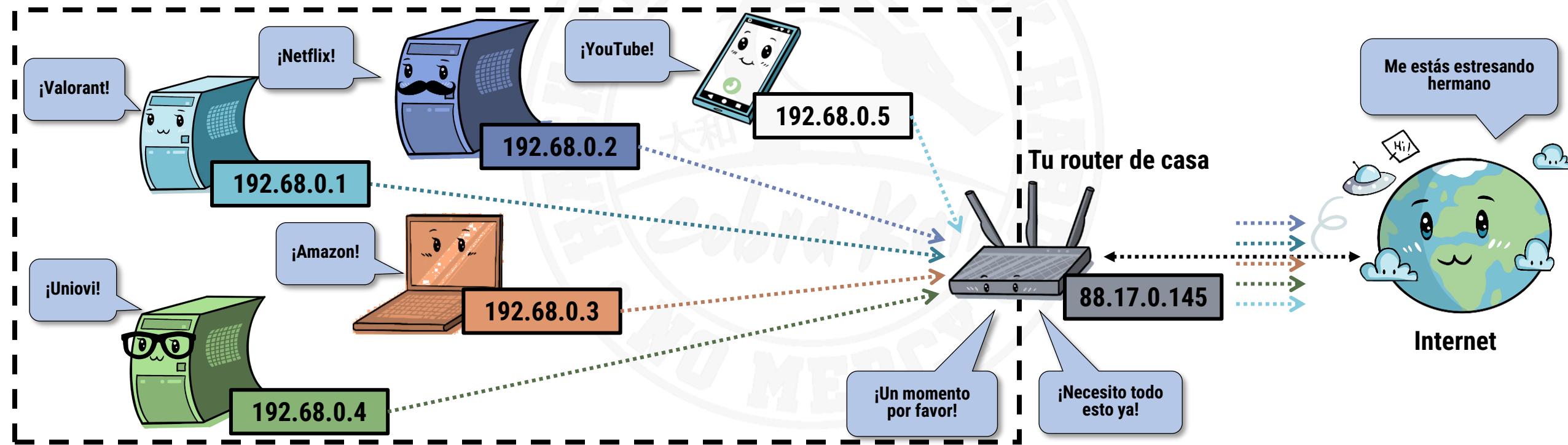
- ¡Ay, amigo! Porque nos falta la última pieza del puzzle: NAT

- **Grosso modo, tu router es un repartidor de pedidos MUY ocupado**

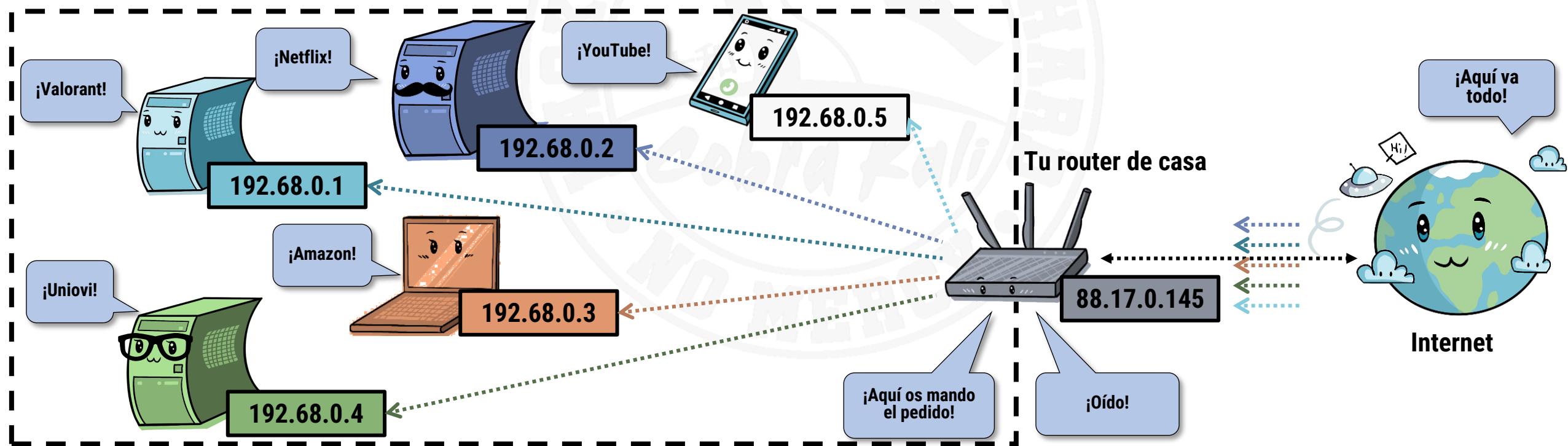
- *¿Quién pide?* Tú (bueno, el PC, móvil, TV, “cosa conectada” que estés usando...)
- *¿Qué y a quien lo pide?* Lo que sea que necesites de Internet (Valorant, Netflix, webs...) a su servidor



- Y es que, al final, tu router “da la cara” en Internet por todas las máquinas conectadas a él que le pidan algo
  - “Envuelve” todo lo que le piden, “lo hace suyo” y **lo pide a Internet en su nombre**



- Y el router devuelve a cada máquina conectada a él lo que ha pedido como respuesta, sin confundirse 😊
  - No, tus padres no van a ver de repente por donde navegas porque el router se confunda, tranqui 🤪
- Y este proceso de “poner la cara” por ti se le llama NAT



# NAT ¿ME LO RESUMES?

## • Como sé que esto es difícil de entender, vamos a hacer un resumen

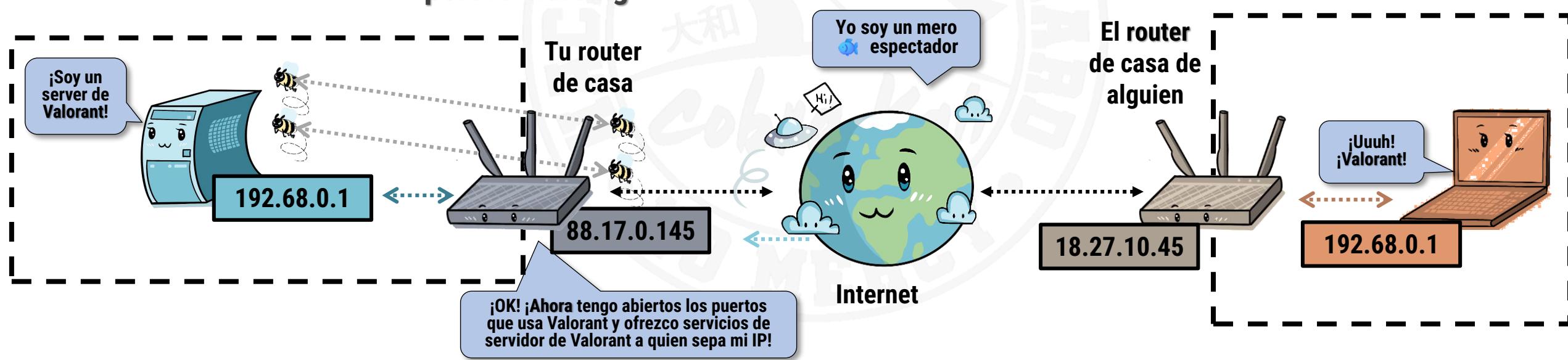
- Todos tus dispositivos tienen una IP... **pero privada**
  - Que solo vale en la red de tu router
  - Wifi, cable...da igual, es así
- Y tu **router tiene la única IP pública**, que sí vale para ir a Internet
- Pero todos tus dispositivos quieren salir a Internet, así que...
- **Tu router “pone la cara” por cualquier dispositivo** que tengas y pide lo que necesites
  - Es decir, “**traduce**” de la IP privada de cada aparato a la pública que tiene
- Cuando llega la respuesta, la “**destraduce**” ☺
  - Y devuelve a cada uno lo que ha pedido exactamente, sin opción a error
- Por eso NAT significa **Network Address Translation**
  - Traducción de direcciones de red
  - ¡Todo esto ocurre **MUCHAS veces por segundo!** (el router es MUY rápido ☺)
  - ¡La “magia” de Internet!



Es magia,  
**NATuralmente** ☺

# OYE, ¿Y SI ALGUNA DE MIS MÁQUINAS QUIERE OFRECER ALGO EN INTERNET?

- Entonces, como vimos antes, tienes que abrir un puerto y ofrecerlo
  - Por ejemplo, un servidor privado de WoW, Valorant, Doom, Counter...
- Ya tío, pero ¿Cómo “pone la cara” el router por mí en ese caso?
  - Igual: Lo que pasa es que tienes que “abrir” el puerto en el router en su programa de configuración
    - Hablaremos de como configurar un router en el **Módulo Defensa**
  - Y decir que todo lo que se conecte a ese puerto del router va para una máquina concreta de tu casa
    - A esto se le llama “**port forwarding**”



# LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

- Estoy pensando... ¿Y para que me cuentas esta movida de cómo hacen unas máquinas para **localizar** a otras, los **servicios** que ofrecen a las demás y lo de los **puertos**?
  - ¡¡¡Porque usar **nmap** necesita que entiendas primero precisamente eso!!!
  - ¡Ahora estás preparado para **subir de nivel**!



Nmap

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Comprendes que, sin DHCP, navegar por internet sería mucho más complicado por las cosas que es capaz de hacer automáticamente?*
- *¿Entiendes que el router también es el encargado de asignar las IP automáticamente por DHCP cada vez que te conectas a él?*
- *¿Entiendes para qué sirven las IPs privadas y la diferencia con las públicas?*
  - *¿Y que es imposible encontrarse una IP privada en Internet?*
- *¿Entiendes que gracias a NAT tu router hace de intermediario de cualquier cosa que tengas en tu casa, y así todos pueden salir a internet con una sola IP que te da tu proveedor?*
- *¿Entiendes también que así tu proveedor ahorra mucho dinero, porque solo te da una IP, aunque tengas 20 cosas saliendo a Internet?*
- *¿Entiendes ahora lo que significa el mapeo de puertos, y como puedes ofrecer servicios desde tu casa a otras personas?*



# NMAP, EL DETECTIVE DE LA RED

¡El Sherlock Holmes de las ondas!



# ¿QUÉ VAS A APRENDER EN ESTE BLOQUE?

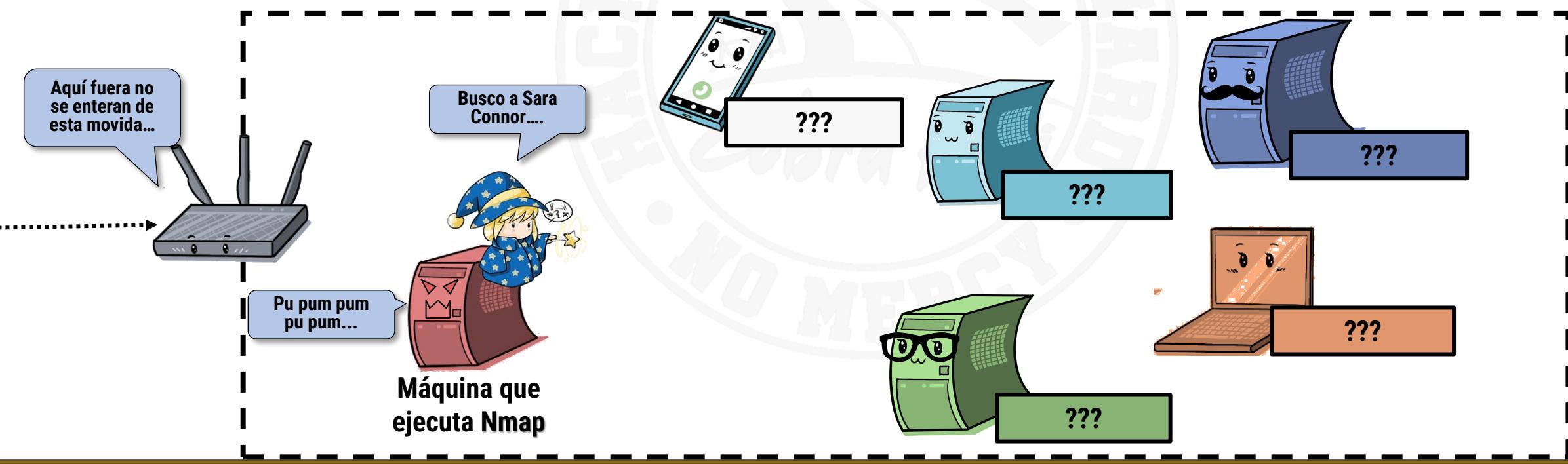
- Entenderás para qué sirve la herramienta **nmap** a la hora de descubrir máquinas puertos y servicios
- Verás como, gracias a **nmap**, puedes ver con tus propios ojos todos los conceptos que hemos explicado en la primera parte de esta presentación
  - Y que forman parte de cualquier conexión que establezcas a internet
- Te enseñaré a interpretar los resultados de un escaneo **nmap**, y la importancia que tienen de cara a la seguridad
- También te enseñaré a identificar vulnerabilidades de lo que escanees
  - La importancia que tienen y por qué es importante eliminarlas lo antes posible
- Te enseñaré también las funciones avanzadas de **nmap**, que te permiten dar mucha más potencia a sus escaneos
- Y con todo ello entenderás un poco mejor cómo se estructuran las conexiones a Internet en tu día a día...



# NMAP POWER: LA ESPÍA QUE ME MAPEO

- Nmap es una herramienta que se usa fundamentalmente para preguntar 

- Aunque tiene muchos otros usos 
- Y dirás... ¿Para preguntar el qué?
- Si otras **máquinas** están ahí, qué **servicios** están ejecutando y los **puertos** en los que están disponibles, por ejemplo
- Es decir, para preguntar todo lo que vimos en la primera parte de la presentación



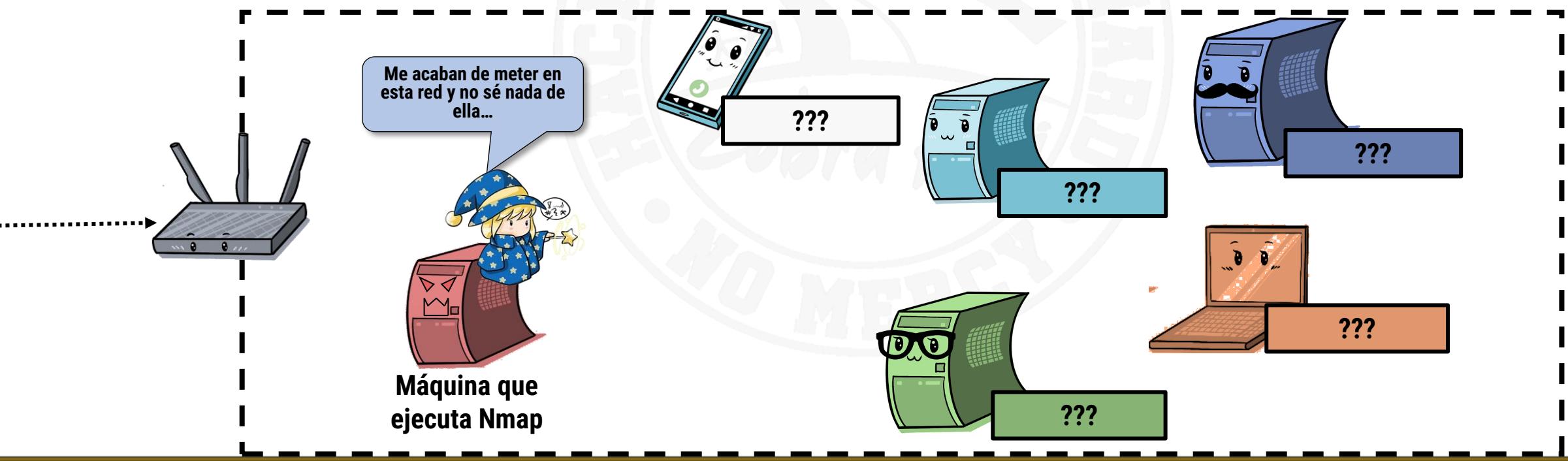
# NMAP POWER: LA ESPÍA QUE ME MAPEO

## • ¿Pero eso no lo sé de antemano?

- ¡Muchas veces no! ¡Y ahí está su principal utilidad!

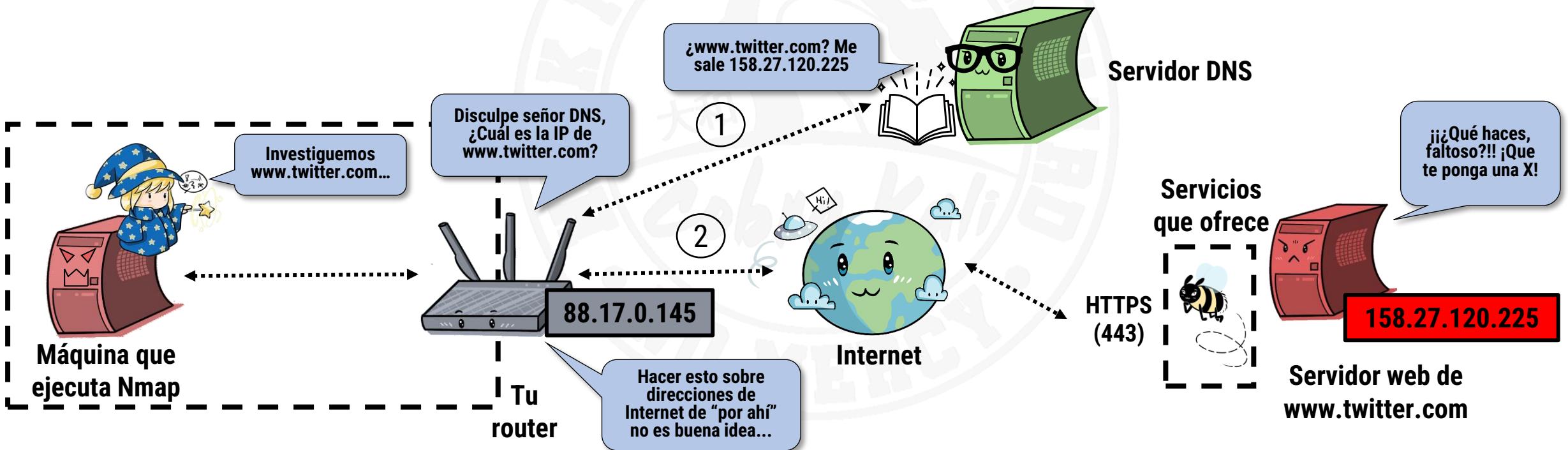
## • Voy a enseñarte varios usos de nmap que llevan parámetros

- Pero no voy a meterme en lo que significan exactamente
- Haz un acto de fe 😊 ¡Trust me I'm an engineer! 😊



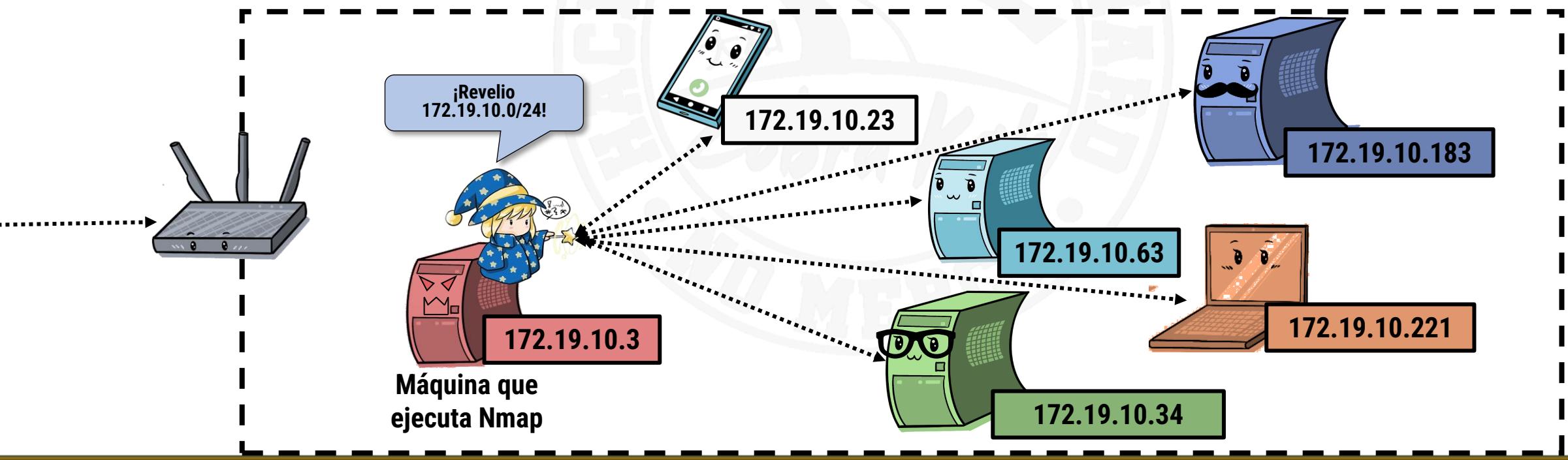
# NMAP POWER: LA ESPÍA QUE ME MAPEO

- Lo 1º es saber encontrar a tus "vecinos" u "objetivos" para preguntarles cosas
- En Internet basta con saber la URL del destino
  - ¡Pero no lo hagas salvo que el destino lo sepa y te deje hacerlo! ¡puedes meterte en un lío!
  - No se debe hacer NUNCA sin autorización de la otra parte
  - Para probar puedes intentarlo sobre **scanme.nmap.org** (es una máquina pensada para pruebas)



# NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿QUIÉN ESTÁ AHÍ?

- Pero también se puede usar en un "barrio", o red local
  - Poniendo lo que antes definimos como máscara CIDR de la red
- Vamos a probar un tipo de escaneo que solo "localiza vecinos vivos"
  - Es decir, máquinas (o cualquier "cosa") funcionando en tu red
  - Teléfonos, PCs, TVs, cualquier cosa "inteligente" (microondas, Roombas...)
  - Piensa: ¿Qué pasa si localizas algo que no sabes lo que es? 😱



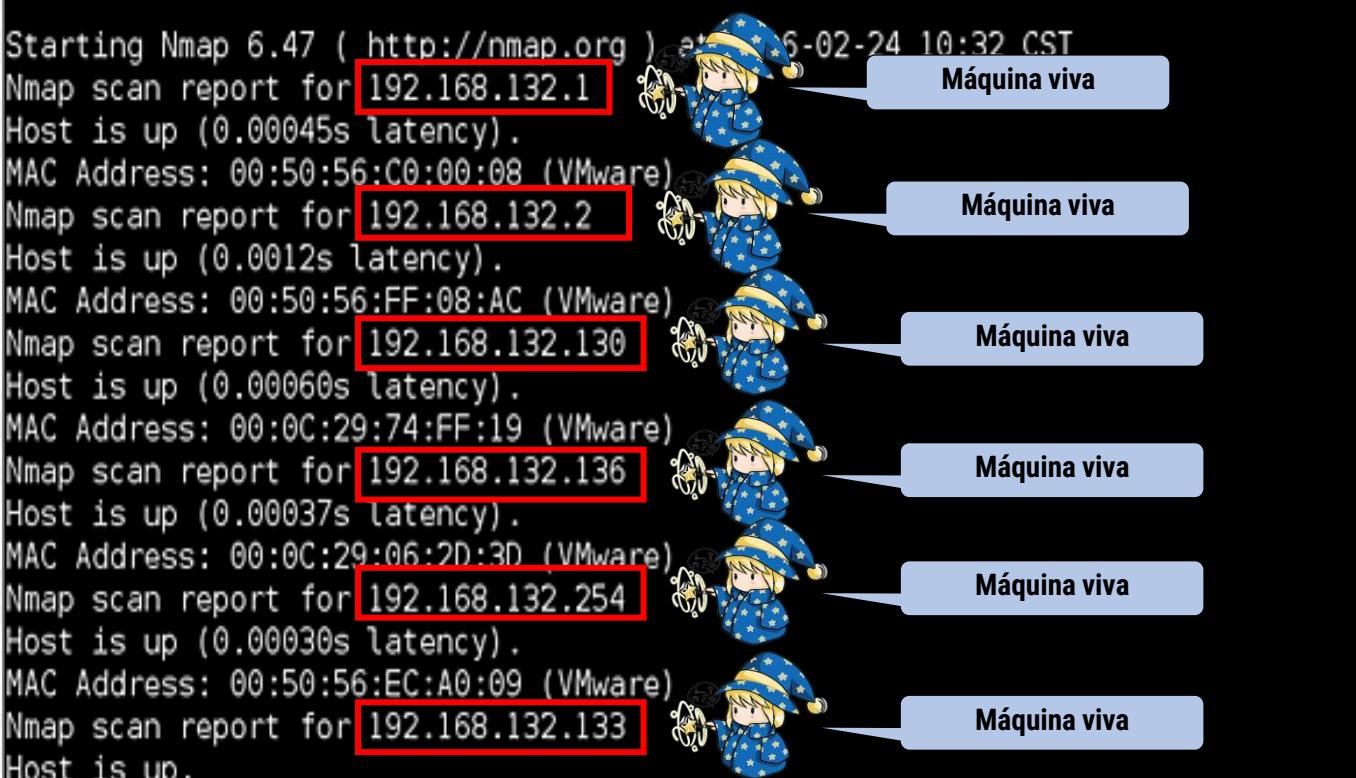
# NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿QUIÉN ESTÁ AHÍ?

- Haz **nmap -sP <IP de red>** y cada IP que te aparezca implica que hay una máquina “viva” ahí
  - Haciendo algo...
  - Vamos, ofreciendo servicios en alguno de sus puertos
- **¿El qué exactamente?**
  - ¡Ese es el siguiente paso!

```
root@attackserver:~# nmap -sP 192.168.132.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2016-02-24 10:32 CST
Nmap scan report for 192.168.132.1
Host is up (0.00045s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.132.2
Host is up (0.0012s latency).
MAC Address: 00:50:56:FF:08:AC (VMware)
Nmap scan report for 192.168.132.130
Host is up (0.00060s latency).
MAC Address: 00:0C:29:74:FF:19 (VMware)
Nmap scan report for 192.168.132.136
Host is up (0.00037s latency).
MAC Address: 00:0C:29:06:2D:3D (VMware)
Nmap scan report for 192.168.132.254
Host is up (0.00030s latency).
MAC Address: 00:50:56:EC:A0:09 (VMware)
Nmap scan report for 192.168.132.133
Host is up.

Nmap done: 256 IP addresses (6 hosts up) scanned in 4.14 seconds
```



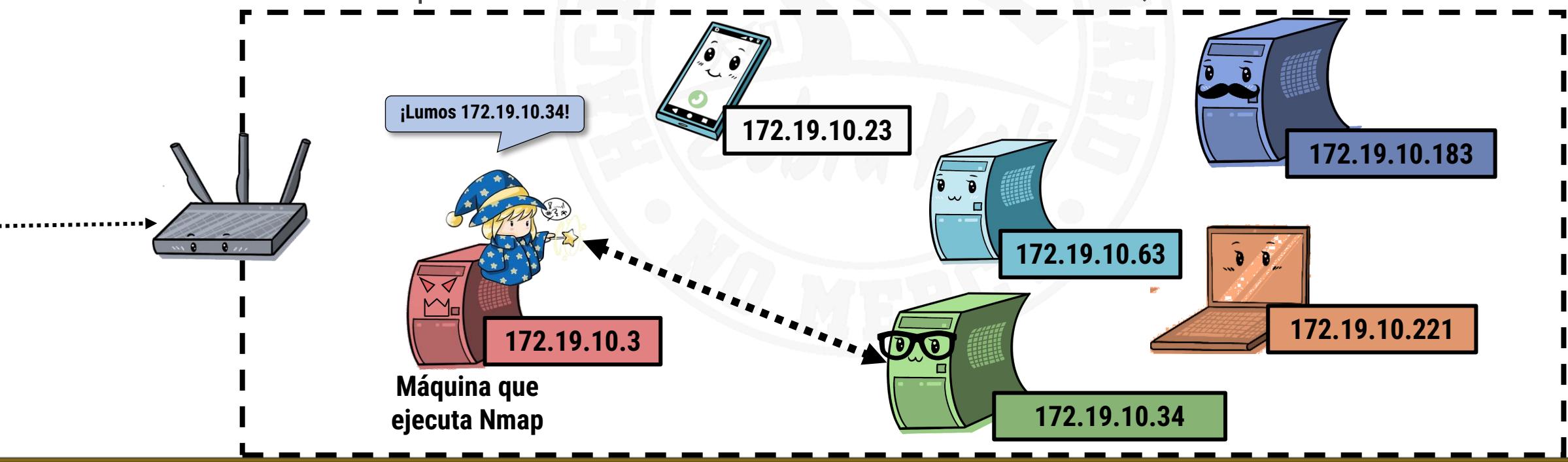
# NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿TÚ QUÉ “VENDES”?

- Con esto no obtenemos casi nada de información...

- ¡Pero sabemos que IPs están en uso!
- Y ahora podemos **estudiar cada una de ellas**

- Para un estudio inicial, elige una de esas IPs (para ir de una en una con calma 😊)

- Y haz esto para ejecutar un "escaneo rápido": **nmap --top-ports 20 --open <IP objetivo>**
- Esto me cuenta **qué ve en la máquina** que le hemos dicho
  - En los 20 nºs de puerto estadísticamente más usados a nivel mundial, si estuvieran abiertos



# NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿TU QUÉ “VENDES”?

## ● *¿Cómo interpretar esto?*

- Este objetivo solo tiene **abiertos** 6 puertos de los 20 más usados mundialmente
- Concretamente los 21, 22, 23, 80, 139 y 445

## ● *Como ves, muchos no aparecen*

- Eso es que ahí, para esta máquina, no hay un servicio esperando por nadie en ese puerto
- Vamos, que están **cerrados**

```
root@kali:~# nmap --top-ports 20 --open 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:10 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00066s latency).
Not shown: 14 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

Servicios que se ejecutan en la máquina de destino: cada uno puede ser una oportunidad para adquirir más información

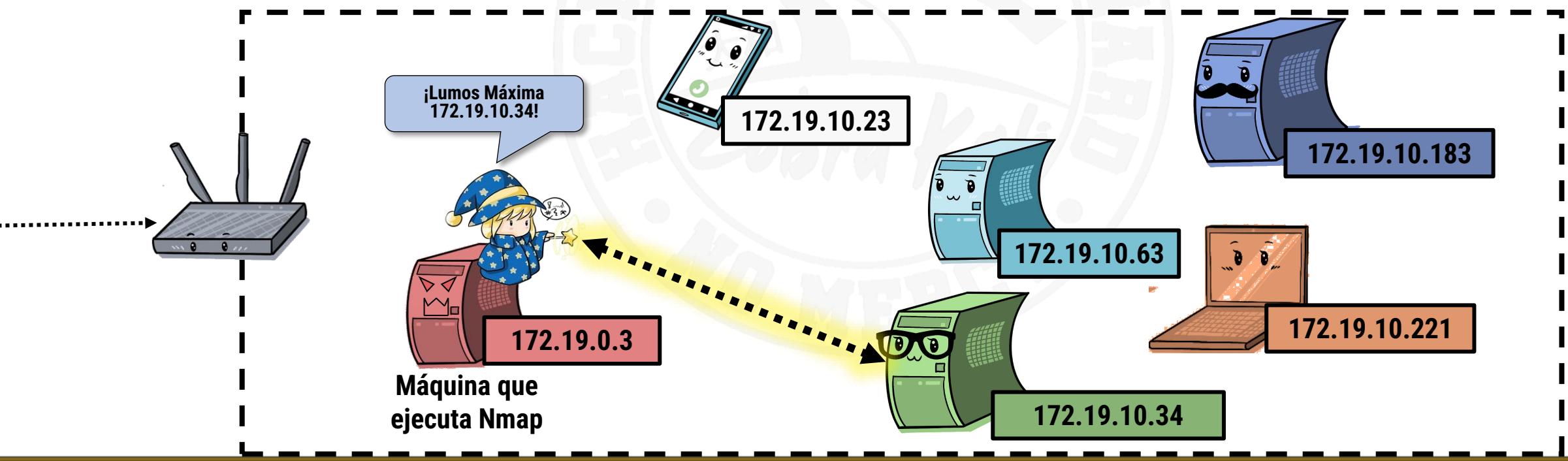
# NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿TU QUÉ “VENDES”?

- ¡¡Wow!! Que útil...

- ¡Menos sarcasmo ho! Estamos solo empezando

- Ahora sabemos que hay algo vivo ahí y que tiene servicios

- Podemos estudiarlos más a fondo con **nmap -A -T4 <IP del objetivo>**
- Y así podemos repetir el proceso con "to lo vivo" que encontramos antes





# INTERPRETANDO LOS RESULTADOS DE NMAP: EJEMPLO DE LINUX

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|   256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: server1804; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER1804, NetBIOS user: <unknown>, NetBIOS MAC: <unkno
wn> (unknown)
smb-os-discovery:
| OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
| Computer name: server1804
| NetBIOS computer name: SERVER1804\x00
| Domain name: \x00
| FQDN: server1804
| System time: 2019-10-02T11:12:04+00:00
smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

Software específico (y su versión) que proporciona unos servicios llamados FTP y SSH. No te preocupes si no sabes qué son, no nos importa ahora mismo

Servidor web / telnet y su versión: igual que los servicios anteriores

Servicio SAMBA (protocolo SMB para compartir archivos entre máquinas)

PC estándar (no un teléfono, impresora, dispositivo IoT...) con un Linux en la misma subred que el nuestro (1 salto implica que no hay "salto" entre redes)

Versión de Ubuntu claramente visible.

# INTERPRETANDO LOS RESULTADOS DE NMAP: EJEMPLO DE WINDOWS

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.22
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-03 15:04 CEST
Nmap scan report for 192.168.14.22
Host is up (0.00066s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp   open  msrpc  Microsoft Windows RPC
443/tcp   open  ssl/http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
ssl-cert: Subject: commonName=WIN-5MPQE2ICEC8
Not valid before: 2019-10-01T12:21:17
Not valid after:  2020-04-01T12:21:17
ssl-date: 2019-10-03T13:06:56+00:00; 0s from scanner time.
tls-alpn:
  h2
  http/1.1
5985/tcp  open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 08:00:27:A8:85:4F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1  0.66 ms  192.168.14.22

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 124.86 seconds
```

Servidor Web IIS, versión 10

Microsoft Remote Procedure Calls (servicio típico de Windows) y servidor web con HTTPS

Servicio WinRM (Windows Remote Management)

Tipo y versión del sistema operativo en ejecución

# NMAP POWER: LA ESPÍA QUE ME MAPEO

- Probablemente ahora pensarás: “Sigo sin verle utilidad a esto tío...”
- *¿Te das cuenta de la diferencia respecto al anterior?*
  - ¡Ahora me sale el **nombre del programa que da el servicio y su versión!**
  - ¡Y es muy importante! ¿Quieres que te cuente por qué? ¡Hablemos de CVEs!

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
|_ 2.0) 2019-07-01T19:10:00+00:00
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|_ 256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
```



# ✗ Los CVE

La “ficha policial” de un problema conocido



# NMAP POWER: LOS CVE

- Resulta que existen páginas en Internet que legalmente **listan todas las vulnerabilidades** (“movidas” de seguridad)

- Para cada programa o servicio conocido, separadas por versión
- ¿Entiendes porque es importante saber qué programa es exactamente el que está prestando un servicio en un puerto?

```
root@kali:~# nmap -sS -A -sV -O -p - 192.16
Starting Nmap 7.80 ( https://nmap.org ) at
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          OpenBSD ftnd 6.4
22/tcp    open  ssh          OpenSSH 7.6p1 Ubu
l 2.0)livos
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d
|   256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.4.
```

**CVE Details**  
The ultimate security vulnerability datasource

Log In Register What's the CVSS score of your company?

Switch to https://  
Home Browse : Vendors Products Vulnerabilities By Date Vulnerabilities By Type Reports : CVSS Score Report CVSS Score Distribution Search : Vendor Search Product Search Version Search Vulnerability Search By Microsoft References Top 5 : Vendors Vendor Cvss Scores Products Product Cvss Scores Versions Other : Microsoft Bulletins Bugtrag Entries CWE Definitions About & Contact Feedback CVE Help FAQ Articles External Links : NVD Website

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)  Search

OpenSSH

iAparecium! (Esto es así con cualquier programa que encuentres, ¿sabes?)

Vulnerability Feeds & Widgets [New](#) [www.itsecdb.com](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.	
1	<a href="#">CVE-2000-0525</a>			Exec Code	2000-06-08	2017-10-10	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
2	<a href="#">CVE-2000-0999</a>			+Priv	2000-12-11	2008-09-05	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
3	<a href="#">CVE-2001-0144</a>			Exec Code Overflow	2001-03-12	2018-05-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
4	<a href="#">CVE-2002-0083</a>	<a href="#">189</a>		+Priv	2002-03-15	2016-10-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
5	<a href="#">CVE-2002-0639</a>			Exec Code Overflow	2002-07-03	2016-10-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
6	<a href="#">CVE-2002-0640</a>			Exec Code Overflow	2002-07-03	2016-10-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
7	<a href="#">CVE-2003-0693</a>			Exec Code	2003-09-22	2018-05-03	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
8	<a href="#">CVE-2003-0786</a>			+Priv	2003-11-17	2008-09-10	10.0	None	Remote	Low	Not required	Complete	Complete	Complete	
				The SSH1 PAM challenge response authentication in OpenSSH 3.7.1 and 3.7.1p1, when Privilege Separation is disabled, does not check the result of the authentication attempt, which can allow remote attackers to gain privileges.											
				o <a href="#">CVE-2006-5051</a>	362	DoS Exec Code	2006-09-27	2017-10-11	10.0	None	Remote	Medium	Not required	Complete	Complete

# NMAP POWER: LOS CVE

- ¿Me quieres decir que ahora puedo tener una idea de los posibles problemas de seguridad que tiene una máquina sabiendo nombre y versión de sus servicios?
  - ¡Sí! ¡Exacto!
  - Si usas el nombre y la versión con esas páginas, puedes tener una idea de cómo de segura es...
- Y esto es legal, si no...¡no te lo enseñaría! ☺

```
root@kali:~# nmap -sS -A -sV -O -p - 192.16
Starting Nmap 7.80 ( https://nmap.org ) at
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          OpenBSD  ftpd 6.4
22/tcp    open  ssh          OpenSSH 7.6p1 Ubu
l 2.0)anivos
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d
|   256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56
23/tcp    open  telnet       Linux telnetd
80/tcp    open  http         Apache httpd 2.4.
```

[Openbsd » Openssh : All Versions](#)

Sort Results By : Version Descending Version Ascending Number of Vulnerabilities Descending Number

Total number of versions found = 270 Page : 1 (This Page) [2](#) [3](#) [4](#) [5](#) [6](#)

Version	Language	Update	Edition	Number of Vulnerabilities	
8.6	*	-	*	1	<a href="#">Version Details Vulnerabilities</a>
8.5	*	-	*	1	<a href="#">Version Details Vulnerabilities</a>
8.4	*	-	*	1	<a href="#">Version Details Vulnerabilities</a>
8.3	*	-	*	1	<a href="#">Version Details Vulnerabilities</a>
8.3	*	P1	*	1	<a href="#">Version Details Vulnerabilities</a>
8.2	*	*	*		
7.9					
7.7		P1			
7.7					
7.6		P1			
7.5					

¡Revelio! Habitualmente se miran las vulnerabilidades de la versión encontrada y las posteriores, ya que es muy posible que los problemas de una versión concreta estén también en las versiones anteriores



Fíjate que dice que afecta a todas las versiones hasta esta

## Vulnerability Details : CVE-2020-15778

\*\* DISPUTED \*\* scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Publish Date : 2020-07-24 Last Update Date : 2021-06-22

Collapse All Expand All Select Select&Copy  
Search Twitter Search YouTube Search Google

▼ Scroll To ▼ Comments ▼ External Links

### - CVSS Scores & Vulnerability Types

CVSS Score

6.8

Confidentiality Impact

Partial (There is a moderate informational disclosure.)

Integrity Impact

Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact

Partial (There is reduced performance or interruptions in resource availability.)

Access Complexity

Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)

Authentication

Not required (Authentication is not required to exploit the vulnerability.)

Gained Access

None

Vulnerability Type(s)

78

Puntuación y efectos de la vulnerabilidad. Si tiene un 10, ¡la máquina está en un gravísimo problema! (el color te da una pista de lo grave que es, no te preocupes ☺)

CWE ID



### - Products Affected By CVE-2020-15778

#	Product Type	Vendor	Product	Version	Update	Edition	Language	Version Details	Vulnerabilities
1	OS	<a href="#">Broadcom</a>	<a href="#">Fabric Operating System</a>	-	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>
2	Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	*	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>
3	Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>
4	Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>
5	Hardware	<a href="#">Netapp</a>	<a href="#">Hci Storage Node</a>	-	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>
6	Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	*	*	*	<a href="#">Version Details</a>	<a href="#">Vulnerabilities</a>

Otros productos afectados porque usan el que estamos mirando ahora para algo



# NMAP POWER: LOS CVE

## ● ¿Y ya está?

- ¡No! Puedes hacer lo mismo con el sistema operativo

[Microsoft » Windows Server 2003 : Vulnerability Statistics](#)

Vulnerabilities (412) CVSS Scores Report Browse all Versions Patch History OVAL Definitions Related OVAL Definitions Vulnerabilities (414) Patches (198) Directory Definitions (3) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2004	4	1	3	1							1				
2005	1		1	1											
2006	2		2	1											
2007	3	1	1	2											
2008	15	6	4	5	1							5			
2009	40	4	14	5	1					2	1	12			2
2010	61	11	25	15	4		1			2	1	22			5
2011	94	13	20	13	11		3			2		63			3
2012	37	2	11	4						1	1	22			
2013	75	10	18	15	8			1			2	50			3
2014	25	5	8	3	2					4	4	9			2
2015	49	8	10	6	2					14	14	18			
2017	3		3	1											
2019	1		1												
2020	2		2												
Total	412	63	121	72	29		4	1		25	24	201			15
% Of All		15.3	29.4	17.5	7.0	0.0	1.0	0.2	0.0	6.1	5.8	48.8	0.0	0.0	

Podrías preguntarte quién va a tener un Windows 2003 a día de hoy. Te sorprenderías...

Tipo de vulnerabilidad según sus efectos. Las de *Code Execution* son terribles

¡Mira todas las que ha ido acumulando con el tiempo! :O



# EXPLOIT-DB

- ¿Y qué puedes hacer con un código CVE, aparte de buscar lo grave que es “el roto” de un programa?
  - ¡Cosas muy muy chungas! 😷
- Te puedes ir a una web llamada exploit-db
  - <https://www.exploit-db.com/>
  - Y saber si **alguien ha hecho un programa que se aprovecha de esa vulnerabilidad** para hacer alguna maldad (esos programas se llaman **exploits**, aunque seguro que te lo imaginabas por el nombre 😅)
  - Dale a Filters – Advanced y busca directamente el nº de CVE
  - Verás un ejemplo en la siguiente hoja
- De esta manera no solo sabes que tienes vulnerabilidades...
  - Sino que encima hay un programa disponible para que cualquiera pueda usarlo para hacer el mal
  - **Moraleja:** Más te vale que actualices el sistema y te tomes la seguridad en serio, si no te atacan en estos casos es de milagro

EXPLOIT DATABASE

Type Platform Author Port Tag Advanced

Verified Has App

Show 15 Date D A V Title

Date	D	A	V	Title	Type	Platform	Author	Port	Tag
2024-07-16	⬇️	✖️	✖️	Bonjour Se					
2024-07-01	⬇️	✖️	✖️	Xhibiter NF					
2024-07-01	⬇️	✖️	✖️	Azon Dom					
2024-07-01	⬇️	✖️	✖️	Microweb					
2024-07-01	⬇️	✖️	✖️	Customer					
2024-06-26	⬇️	✖️	✖️	Automad 2.0.0-alpha.4 - Stored Cross-Site Scripting (XSS)					WebApps
2024-06-26	⬇️	✖️	✖️	SolarWinds Platform 2024.1 SR1 - Race Condition					WebApps
2024-06-26	⬇️	✖️	✖️	Flatboard 3.2 - Stored Cross-Site Scripting (XSS) (Authenticated)					WebApps
2024-06-26	⬇️	✖️	✖️	Poultry Farm Management System v1.0 - Remote Code Execution (RCE)					WebApps
2024-06-14	⬇️	✖️	✖️	Boelter Blue System Management 1.3 - SOL Injection					WebApps

Search The Exploit Database

CVE

2020-15778

Filters Reset All

El nº de CVE es uno que salió en una hoja anterior ¿eh? De inventármelo nada... A veces salen exploits, y a veces no...

Windows bios

PHP Sohel Yousef

PHP Buğra Enis Dönmez

PHP tmrswrr

PHP Geraldo Alcantara

PHP Jerry Thomas

Multiple Elhussain Fathy

PHP tmrswrr

PHP Jerry Thomas

CBKB

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes que nmap puede usarse para saber si tienes dispositivos activos en una IP de tu red de casa?*
- *¿Entiendes también que se puede usar para saber qué puertos están activos y qué servicios hay detrás de ellos?*
- Yendo un poco más allá, *¿Entiendes que también puedes sacar servicios y versiones, y con ello CVEs y posibles exploits asociados?*
- Por tanto *¿Entiendes la importancia de esta herramienta de cara a mirar la ciberseguridad de las cosas que tienes en casa y, en general, de cualquier cosa remota?*
- *¿Te ha quedado claro que NUNCA debes hacer un escaneo de este estilo contra un objetivo cuyo dueño no te autorice a hacerlo, puesto que podría ser considerado un delito?*



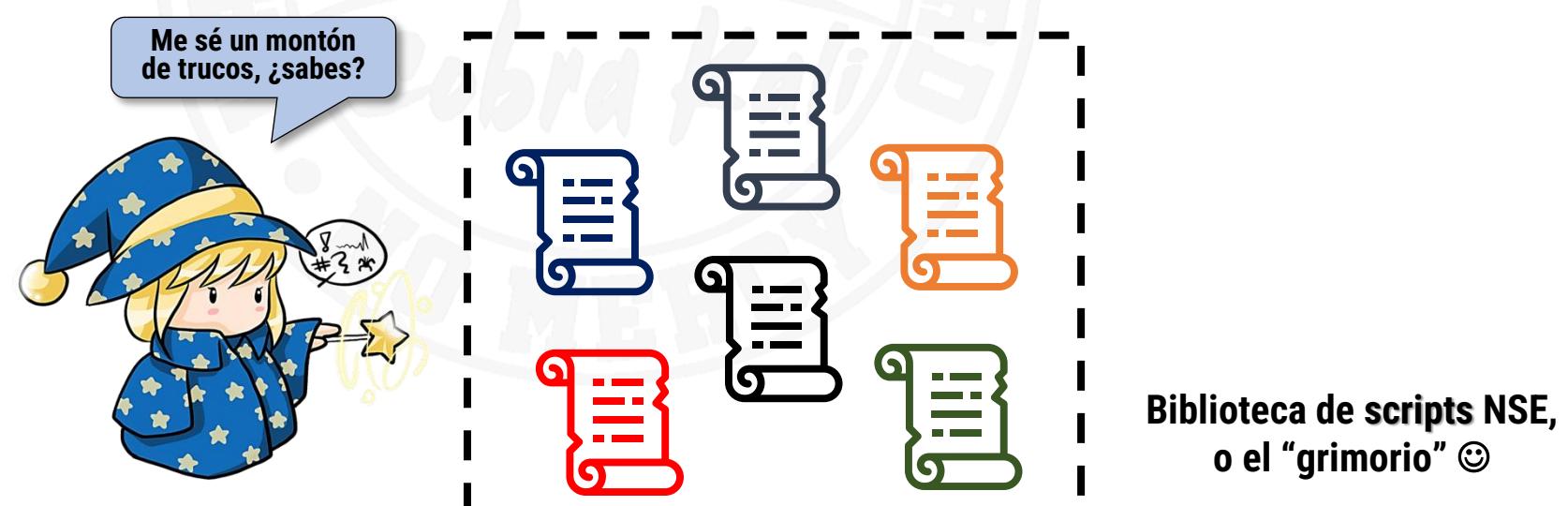
  “Serious” Nmap 😊

Usando Nmap de forma más “seria”



# NMAPSTER CHEF: COCINANDO CON SCRIPTS

- La funcionalidad de Nmap se puede extender gracias a los más de 600 “trucos” que conoce
  - Se llaman scripts NSE: <https://nmap.org/nsedoc/>
- Estos “trucos” son instrucciones para que la herramienta haga cosas distintas a la “investigación” que hemos visto
  - Con ellos, nmap es **muy flexible**
  - Y tiene acciones especiales para trabajar con casi cualquier servicio que nos encontremos
  - ¡Y hacer MUCHAS cosas con ellos! (más cuanta más experiencia “de mago” acumules ☺)



# NMAPSTER CHEF: COCINANDO CON SCRIPTS

- Para usarlos, siempre hay que hacer lo mismo
  - **nmap --script <nombre del script> --script-args <argumentos de ese script en particular>**
- Oye, ¿Y yo cómo sé su nombre y qué argumentos usan, si hay 600 de estos y encima...¡todos usan argumentos distintos!?
  - ¡Porque está todo documentado en la página anterior!
  - Busca, entra a su ficha y lee ☺



https://nmap.org/nsedoc/scripts/smb-brute.html

Script Arguments

smblockout

This argument will force the script to continue if it locks out an account or thinks it will lock out an account.

canaries

Sets the number of tests to do to attempt to lock out the first account. This will lock out the first account without locking out the rest of the accounts. The default is 3, which will only trigger strict lockouts, but will also bump the canary account up far enough to detect a lockout well before other accounts are hit.

brutelimit

Limits the number of usernames checked in the script. In some domains, it's possible to end up with 10,000+ usernames on each server. By default, this will be 5000, which should be higher than most servers and also prevent infinite loops or other weird things. This will only affect the user list pulled from the server, not the username list.

passdb, unpwdb.passlimit, unpwdb.timelimit, unpwdb.usermodel, userdb

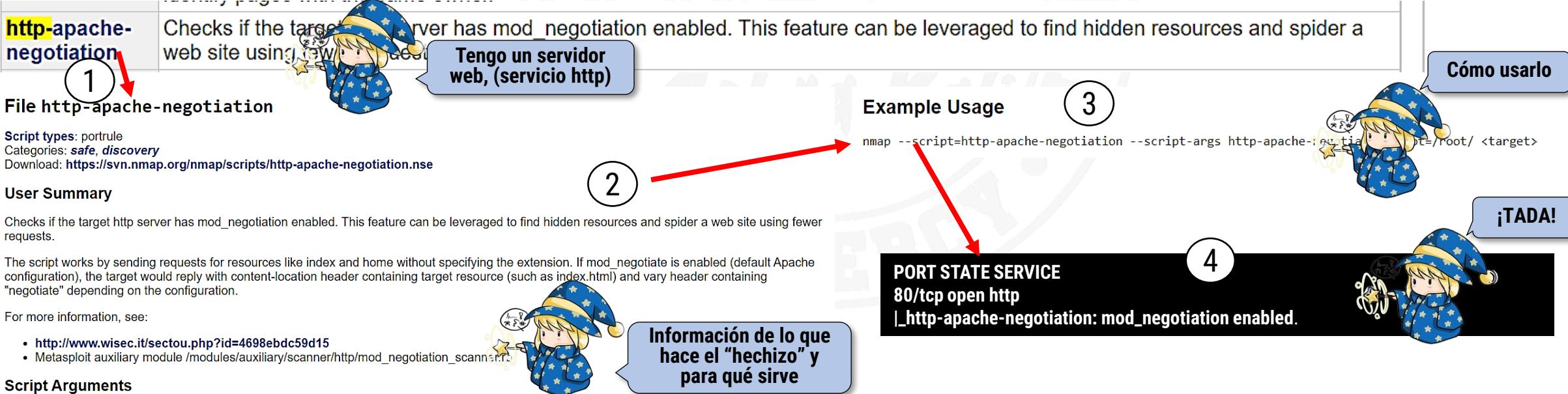
See the documentation for the unpwdb library.

randomseed, smbbasic, smbport, smbsign

See the documentation for the smb library.

# NMAPSTER CHEF: COCINANDO CON SCRIPTS

- *¿Y cómo se cuál necesito, con todos los que hay?*
- *¿Tienes ya el nombre del servicio de un escaneo?*
  - Busca en esa web los que lo llevan, entra en los que te llamen la atención y...lee ☺
- *A lo mejor piensas: “¡Buah, que movida tío!”*
  - Pero ¡tranqui! Con la práctica uno aprende a pillarle el truco ☺



**File http-apache-negotiation** 1

Script types: portrule  
Categories: safe, discovery  
Download: <https://svn.nmap.org/nmap/scripts/http-apache-negotiation.nse>

**User Summary**

Checks if the target http server has mod\_negotiation enabled. This feature can be leveraged to find hidden resources and spider a web site using fewer requests.

The script works by sending requests for resources like index and home without specifying the extension. If mod\_negotiate is enabled (default Apache configuration), the target would reply with content-location header containing target resource (such as index.html) and vary header containing "negotiate" depending on the configuration.

For more information, see:

- <http://www.wisec.it/sectou.php?id=4698ebdc59d15>
- Metasploit auxiliary module /modules/auxiliary/scanner/http/mod\_negotiation\_scanner.ruby

**Script Arguments**

Checks if the target http server has mod\_negotiation enabled. This feature can be leveraged to find hidden resources and spider a web site using fewer requests.

The script works by sending requests for resources like index and home without specifying the extension. If mod\_negotiate is enabled (default Apache configuration), the target would reply with content-location header containing target resource (such as index.html) and vary header containing "negotiate" depending on the configuration.

For more information, see:

- <http://www.wisec.it/sectou.php?id=4698ebdc59d15>
- Metasploit auxiliary module /modules/auxiliary/scanner/http/mod\_negotiation\_scanner.ruby

**Tengo un servidor web, (servicio http)** 2

**Cómo usarlo** 3

**Example Usage**

```
nmap --script=http-apache-negotiation --script-args http-apache-negotiation.tgt=/root/ <target>
```

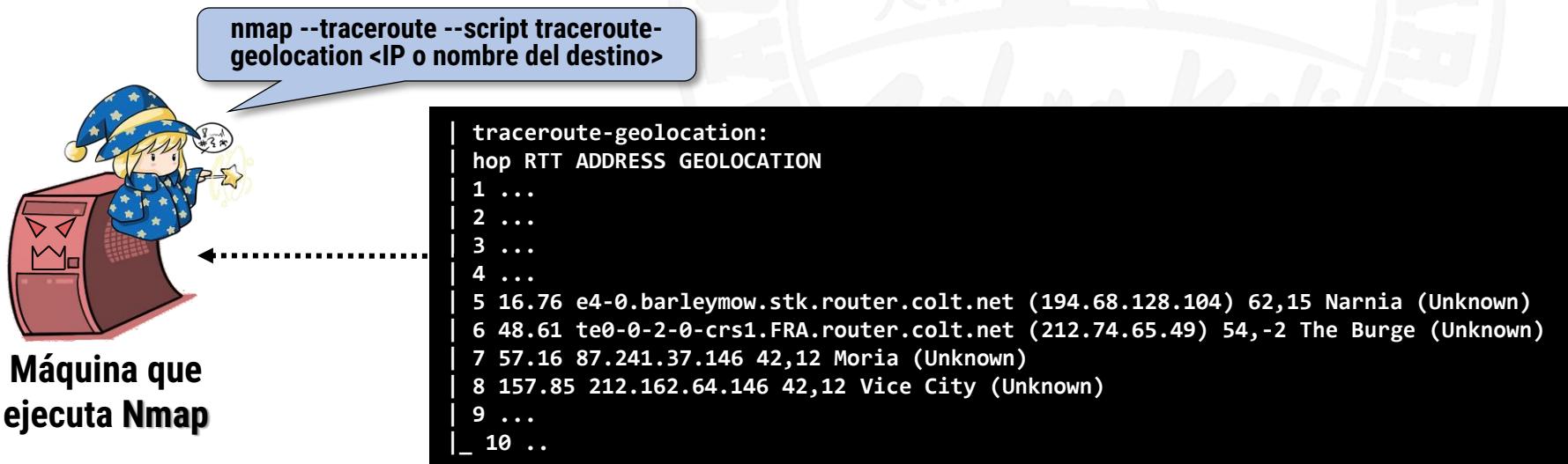
**¡TADA!** 4

**PORT STATE SERVICE**  
**80/tcp open http**  
**|\_http-apache-negotiation: mod\_negotiation enabled.**

**Información de lo que hace el "hechizo" y para qué sirve**

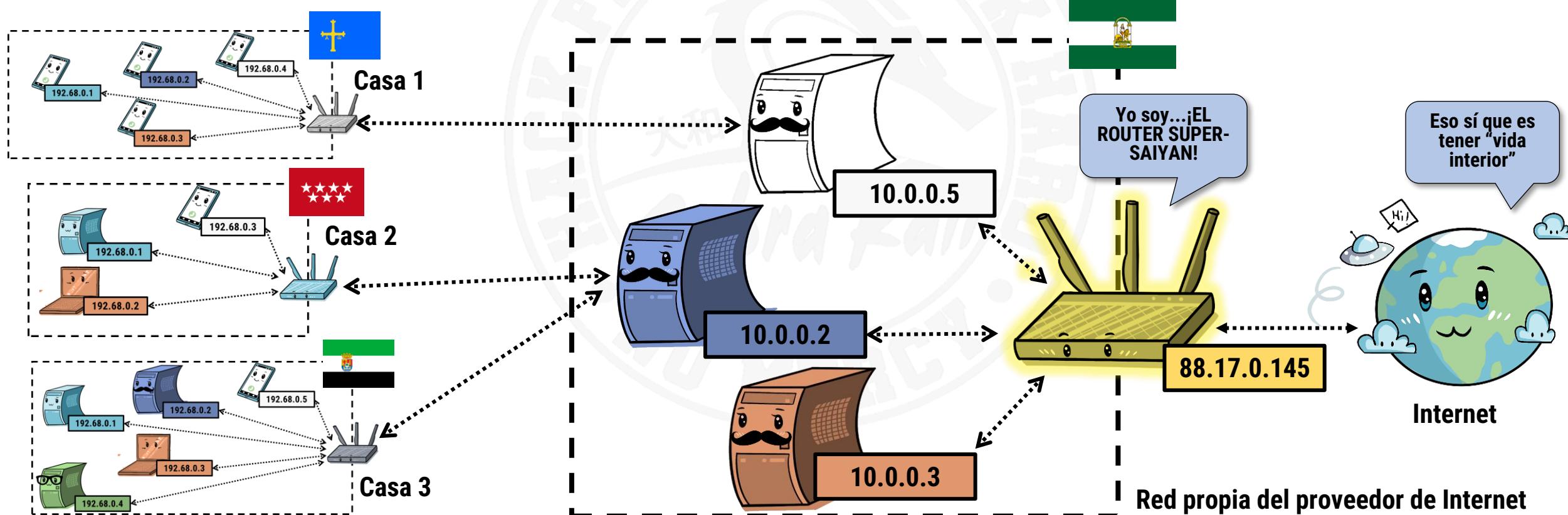
# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

- El script **traceroute-geolocation** te deja ver por dónde pasa tu tráfico de red desde tu ordenador al destino
- *¿Tu pa que quieres saber eso? Jaja saludos*
  - Hombre, aparte de para saber por qué partes del mundo va tu información...
  - A lo mejor te encuentras algo que no debería estar ahí “interceptando” tu conexión...
  - O que tu proveedor está usando **CG-NAT** contigo...*¿Quieres saber qué es?* Pasa a la siguiente hoja ☺



# CG-NAT

- ¿Sabes que, a lo mejor, tu proveedor no te conecta el router directamente a internet?
- Sino que te conecta a una red propia suya
  - Que es la que te da salida realmente internet...
  - A este “doble salto” se le llama **CG-NAT** (Carrier-Grade NAT)

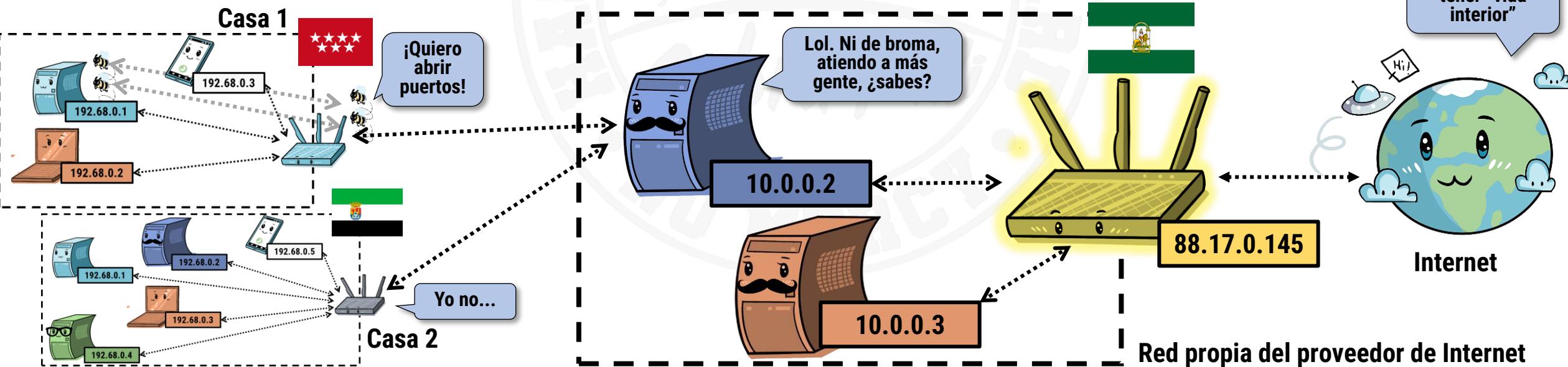


## ● ¿Por qué lo hacen?

- Ahoran dinero: con menos IP válidas en internet (caras) pueden dar servicio a muchos usuarios

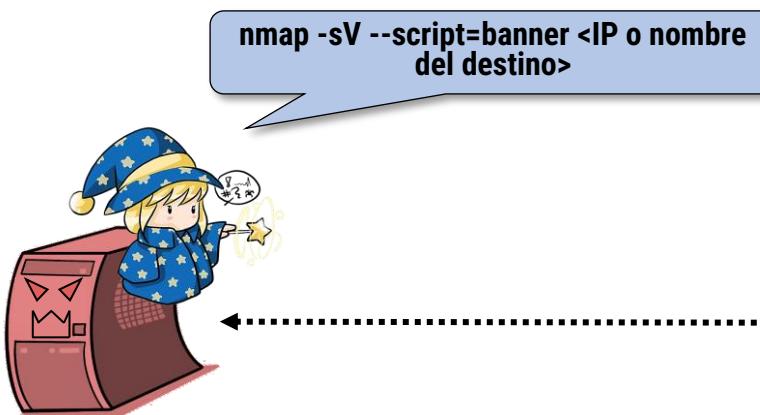
## ● ¿Y tú notas la diferencia? Pues en muchos casos no, salvo que...

- ...saber tu **localización** sea importante, porque puedes aparecer como localizado en Andalucía cuando estás en Asturias por ejemplo (depende de por dónde "salgas")
- ...necesites una **latencia** de conexiones muy baja (el famoso ping de los videojuegos)
  - Esto la afecta...el tráfico de red pega más "saltos"
- ...**necesites abrir un puerto** para hacer un servicio: Si estás bajo CG-NAT...**¡no funciona!**



# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

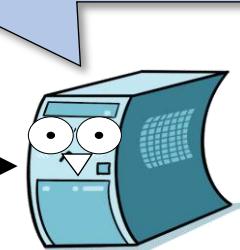
- El script **banner** pregunta a un servicio la información que da inicialmente a cualquiera que se conecte a él
- ¿Y eso para qué se hace?
  - ¡Porque muchas veces esa información es el **nombre del programa y su versión!**!
  - Y ya sabes lo peligroso que es...



Máquina que ejecuta Nmap

```
...  
21/tcp open ftp  
|_ banner: 220 Hell FTP version 666  
...
```

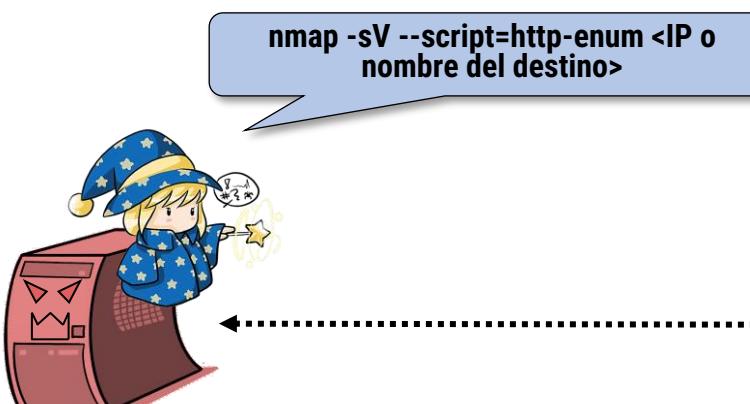
He protegido mis servicios para que no se sepa cuáles son... y resulta que al final son ellos mismos los que lo “cantan”!



Víctima

# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

- El script **http-enum** tiene una lista de rutas comunes que suele haber en cualquier web (/admin, /login...) y las prueba todas
- Meca, ¿Y eso para qué?
  - Porque si alguna de ellas es una dirección “oculta” (no hay un enlace que va hacia ella) ¡la descubrirá!
  - Mucha gente cree que si no enlaza algo nadie lo descubrirá...¡y es un error enorme!



Máquina que ejecuta Nmap

```
...
Interesting ports on matrix.breathtaking.org (208.81.2.52):
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack
| http-enum:
| /icons/: Icons and images
| /images/: Icons and images
| /robots.txt: Robots file
| /sw/auth/login.aspx: SEPE Login portal
| /images/outlook.jpg: Outlook Web Access
| /tarjetas_black/:
...
...
```

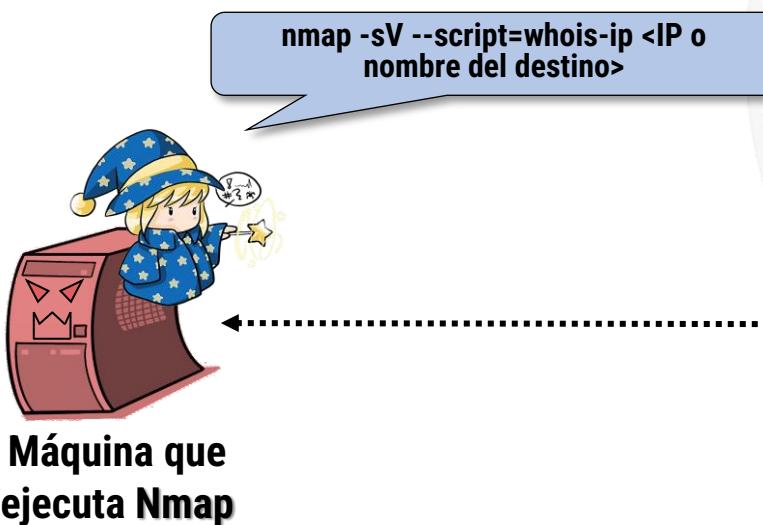
¡Tenía una web /tarjetas\_black y me la han descubierto!



Víctima

# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

- El script **whois-ip** averigua quién ha registrado una determinada web y, por tanto, quién figura como su dueño
- ¡Eh! ¡¿Pero cómo sabe eso?!
  - Porque al crear una web pública, **tienes que dar esa información**
  - Aunque a lo mejor el proveedor de hosting **da la suya por el dueño**, y por ahí no puedes saber nada...
    - Pero por probar...

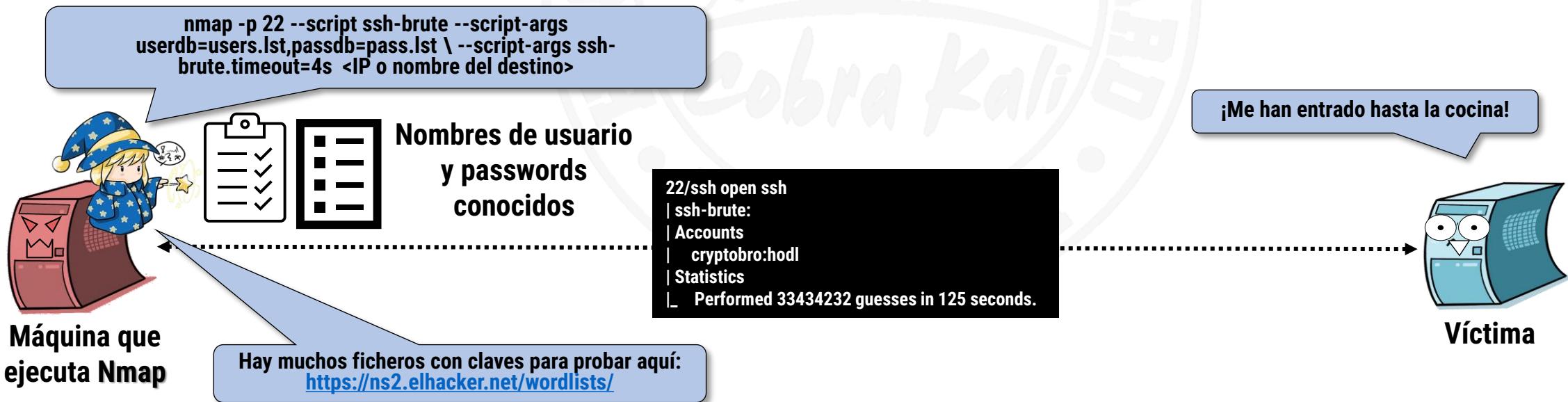


```
Host script results:  
| whois-ip: Record found at whois.arin.net  
| netrange: 64.13.134.0 - 64.13.134.63  
| netname: NET-64-13-143-0-26  
| orgname: Rude Gotenks Networks  
| orgid: WREX  
| _country: US stateprov: CA
```



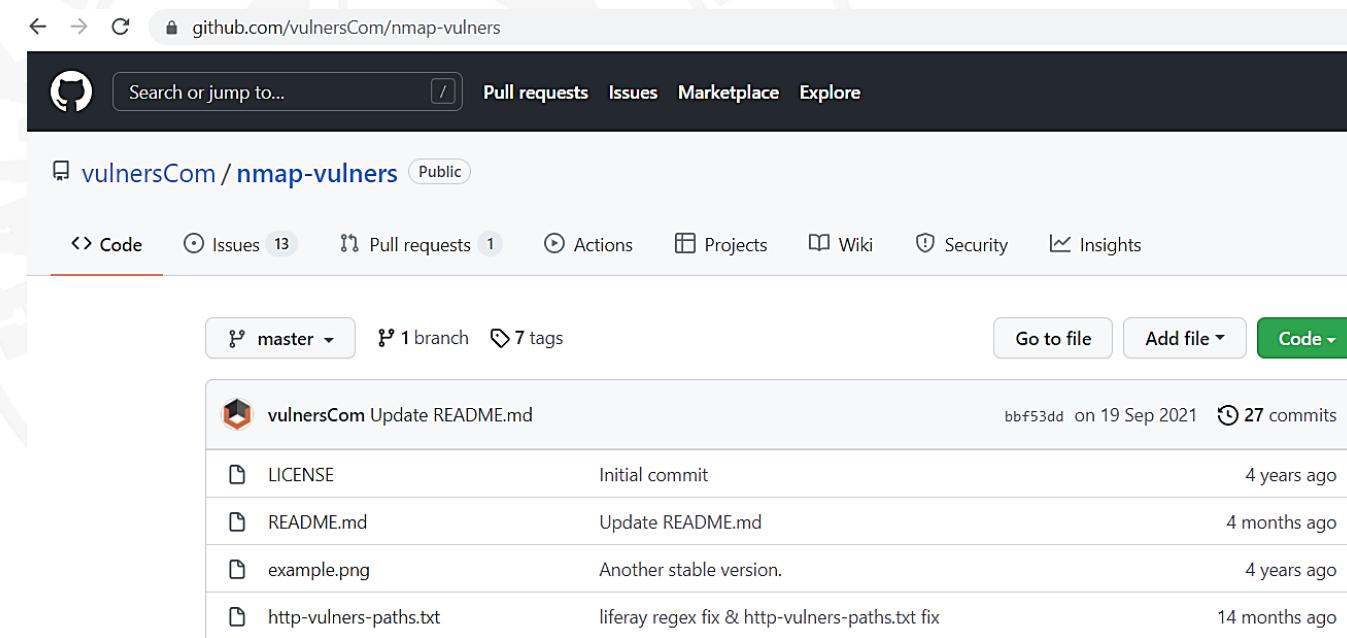
# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

- El script **ssh-brute** puede averiguar la clave de un usuario de una máquina si la clave es común y si se usa el servicio ssh (acceso remoto)
- *¿Cómo los hackers de Hollywood?!*
  - Bueno, en realidad **prueba todas las contraseñas y nombres de usuario que le pases** en dos ficheros (uno para cada cosa), a ver si hay suerte...
  - Obviamente, hacer esto sin autorización del propietario **ES DELITO**



# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

- *¿Y si te digo que hay un script que te saca automáticamente todos los CVE asociados a los servicios que localiza?*
- *¿Cómo? ¿Qué te hace todo el trabajo solo?*
  - ¡Exacto!, se llama **nmap-vulners** (<https://github.com/vulnersCom/nmap-vulners>)
  - Pero hay que instalarlo aparte, como dice en su web...



Commit	Author	Date	Commits
vulnersCom Update README.md	bbf53dd on 19 Sep 2021	27 commits	
LICENSE	Initial commit	4 years ago	
README.md	Update README.md	4 months ago	
example.png	Another stable version.	4 years ago	
http-vulners-paths.txt	liferay regex fix & http-vulners-paths.txt fix	14 months ago	



José Manuel  
Redondo López

# NMAPSTER CHEF: “RECETAS” DE EJEMPLO

```
redondo@lab8_kali:/usr/share/nmap/scripts$ sudo nmap -sV --script=nmap-vulners/ 172.8.0.13
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-09 17:12 UTC
Nmap scan report for lab8_obsolete.lab8_lab8_net (172.8.0.13)
Host is up (0.000030s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
vulners:
cpe:/a:openbsd:openssh:6.6.1p1:
  CVE-2015-5600  8.5  https://vulners.com/cve/CVE-2015-5600
  MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/  6.9  https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/  *EXPLOIT*
  CVE-2015-6564  6.9  https://vulners.com/cve/CVE-2015-6564
  CVE-2018-15919 5.0  https://vulners.com/cve/CVE-2018-15919
  CVE-2021-41617 4.4  https://vulners.com/cve/CVE-2021-41617
  MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/  4.3  https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/  4.3  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/  4.3  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/  4.3  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/  *EXPLOIT*
  MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/  4.3  https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/  *EXPLOIT*
  CVE-2020-14145 4.3  https://vulners.com/cve/CVE-2020-14145
  CVE-2015-5352 4.3  https://vulners.com/cve/CVE-2015-5352
  MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/ 1.9  https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/  *EXPLOIT*
  CVE-2015-6563 1.9  https://vulners.com/cve/CVE-2015-6563
23/tcp    open  telnet  Linux telnetd
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
vulners:
cpe:/a:apache:http_server:2.4.7:
  CVE-2021-39275 7.5  https://vulners.com/cve/CVE-2021-39275
  CVE-2021-26691 7.5  https://vulners.com/cve/CVE-2021-26691
  CVE-2017-7679 7.5  https://vulners.com/cve/CVE-2017-7679
  CVE-2017-3167 7.5  https://vulners.com/cve/CVE-2017-3167
  PACKETSTORM:127546 6.8  https://vulners.com/packetstorm/PACKETSTORM:127546  *EXPLOIT*
  MSF:ILITIES/UBUNTU-CVE-2018-1312/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1312/  *EXPLOIT*
  MSF:ILITIES/UBUNTU-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/SUSE-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/  *EXPLOIT*
  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/  *EXPLOIT*
```

¡Avada kedavra!



¡Sectumsempra!



# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

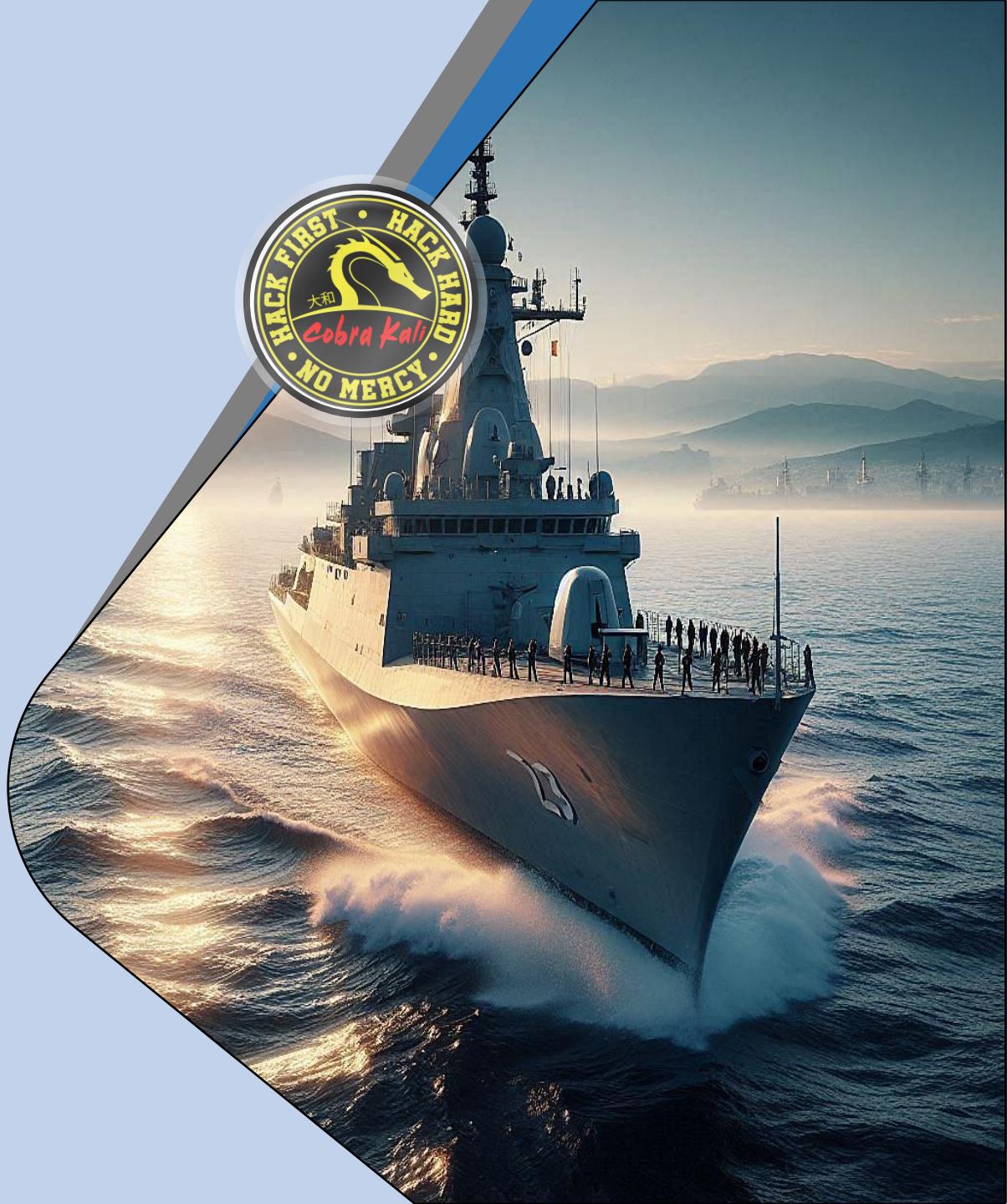


- *¿Entiendes que la librería de scripts de nmap le da una enorme versatilidad para hacer muchas cosas, que de otra manera la herramienta no podría?*
- *¿Te ha quedado claro que, a pesar de que solo hemos visto una pequeña parte de las cosas que hace nmap, la cantidad de información que puede sacar de un servicio remoto es enorme?*
- *¿Te das cuenta de que ahora mismo tienes en tu mano una herramienta de análisis muy potente y que, si te interesa seguir en el camino de la seguridad, ya tendrás una base buena para seguir investigando?*
- *¿Entiendes que gracias a las funcionalidades de nmap puedes averiguar si tu proveedor te ha metido en una red CG-NAT y tú no lo sabes?*
  - *¿Y entiendes que si tienes que ofrecer un servicio en tu casa debes pedir que te lo quiten?*
- *¿Te das cuenta de que usando nmap puedes sacarle los CVEs cualquier dispositivo de tu casa con un solo comando?*



# SHODAN GO ON!

El buscador de máquinas de todo tipo por Internet



# ¿QUÉ VAS A APRENDER EN ESTE BLOQUE?



- Entenderás cómo existen buscadores de máquinas conectadas a internet y lo que te permiten encontrar
- También te darás cuenta de que poco a poco nos vamos moviendo a un modelo donde las direcciones IP son más complejas
  - Pero siguen funcionando como ya te explicamos en el módulo anterior
- Entenderás que conectado a internet puede haber prácticamente cualquier cosa, y que todo eso se llama Internet of Things
- Y que, con un buscador de máquinas, puedes localizar lo que quieras en la zona geográfica que quieras...
  - Y restringir la búsqueda todo lo que necesites para que no se te escape nada

# BUSCAR COSAS POR INTERNET DA MUCHO JUEGO...

- Estamos acostumbrados a buscar o pedirle a una IA información
  - Ya sea que esté indexada o que nos la cree en función de nuestras necesidades
- ¿Qué pasa si, en lugar de eso, buscamos máquinas conectadas?

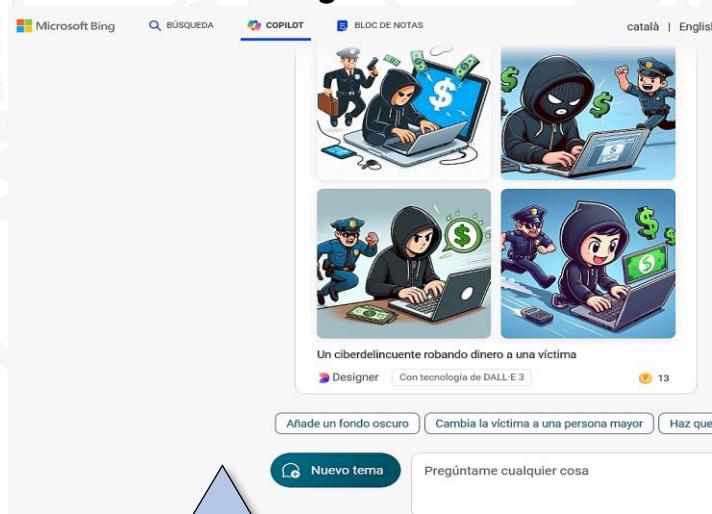


Buscador “de siempre”



Yo busco páginas

IA generativa



Yo creo textos o imágenes

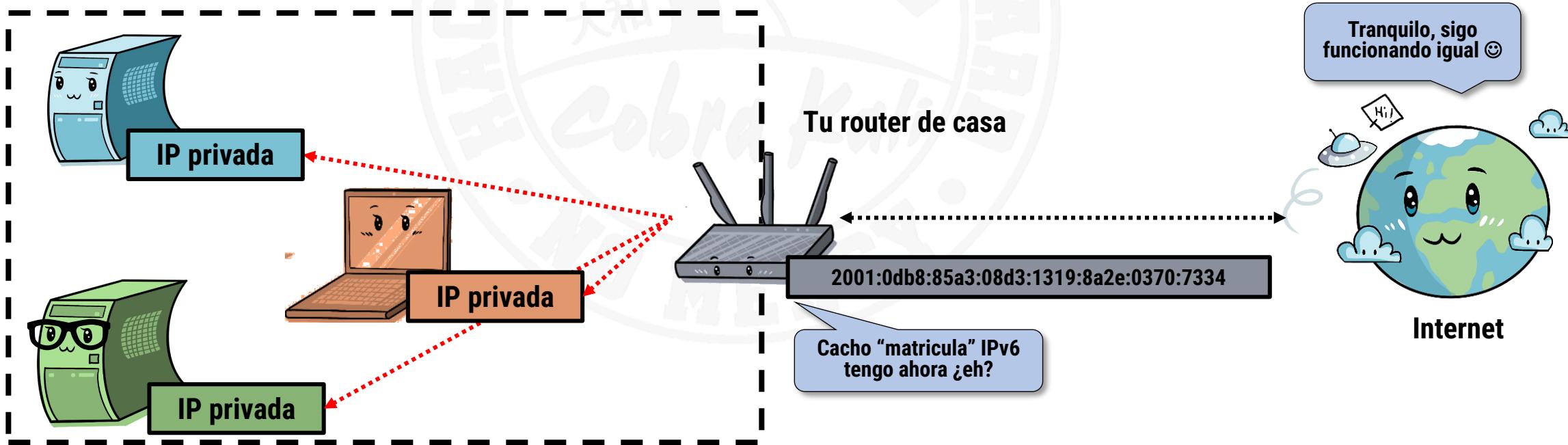
Buscador de máquinas



Yo encuentro las máquinas donde  
están los otros dos... ¡o cualquier  
cosa conectada a Internet!

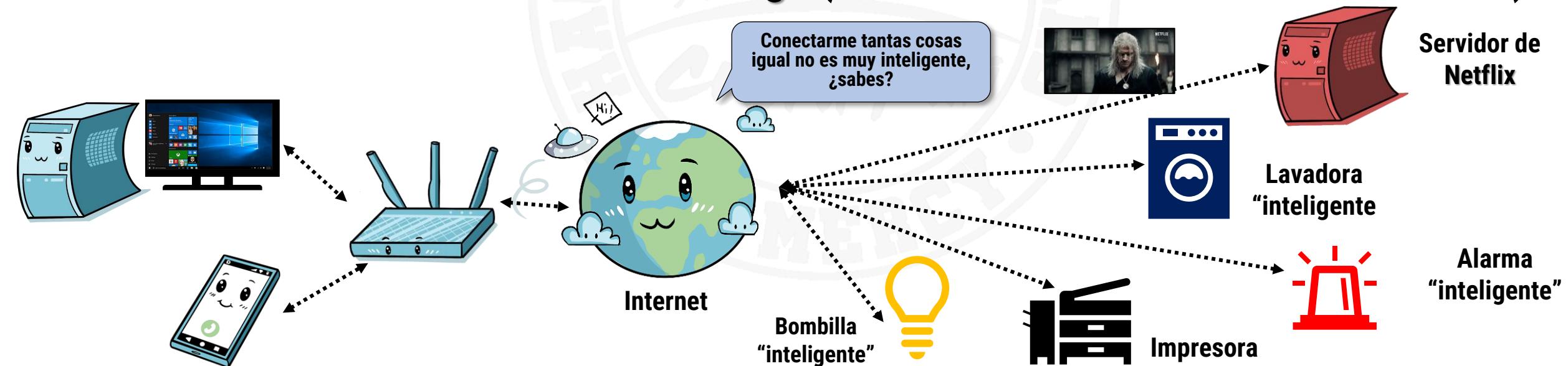
# IPv6

- Antes de seguir, tienes que saber te encontrarás con IPs en un formato nuevo (v6)
- Significa lo mismo que hemos visto, solo que ahora los nombres que le damos a los dispositivos son más “feos” 😊
  - ¡Y no es por capricho! Esta nueva versión nos permite acabar con el problema de la escasez de IPs
- Pero no te preocupes, no deja de ser lo mismo, pero con otro formato 😊
  - Que son **8 bloques** de **4 nºs** y **letras** de la A a la F



# IoT (INTERNET OF THINGS)

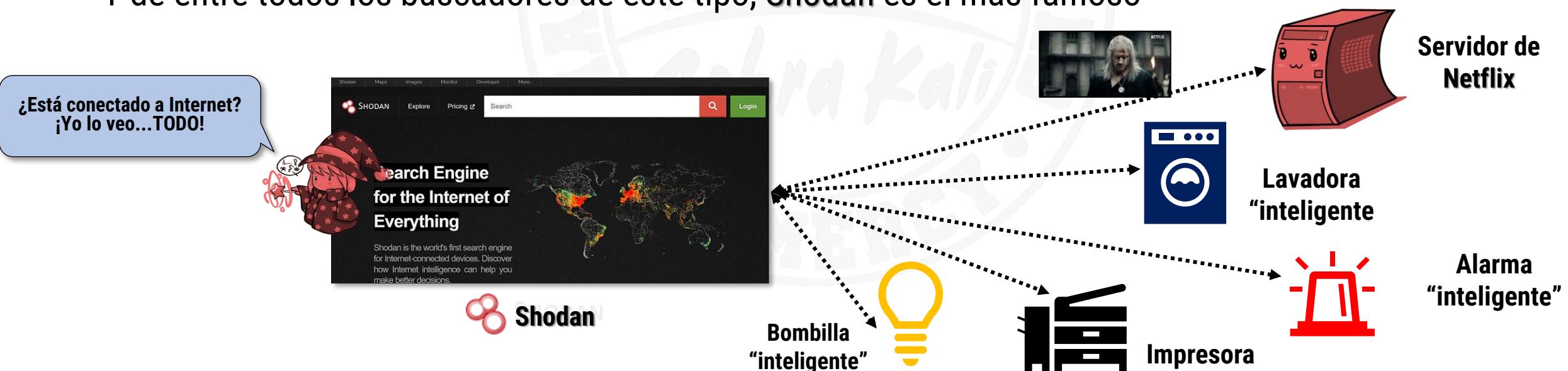
- También tienes que tener en cuenta que hoy en día **casi todo puede estar conectado a internet**
  - ¿Crees que solo son PCs, móviles, tablets o televisiones?
  - ¡Para nada! hay un montón de “cacharros” que se pueden conectar a internet para diferentes cosas
    - Pulseras, relojes, aparatos para casa de diferentes tipos (hasta electrodomésticos convencionales), bombillas, cerraduras electrónicas...
    - Cualquier cosa que se pueda controlar remotamente desde tu móvil está conectada
- A todo ello se le llama **Internet of Things (“cosas” con una IP válida en Internet)**



# BUSCADORES DE MÁQUINAS O “COSAS”

- Y como hay un montón de tipos de dispositivos conectados a Internet...

- También hay **buscadores para esos dispositivos**
  - Si los sabes buscar te dicen **lo que son, dónde están, los puertos y servicios** que tienen abiertos...y muchas veces sus **vulnerabilidades conocidas**
  - Sí, te dicen los **CVEs** que tienen...¿Y ya sabes *lo que te puede pasar después no?*
- Y encima es un buscador: **él busca por ti**
  - ¡La máquina de la que “saca las vergüenzas” nunca sabrá que has sido tu quien las ha consultado!
- Y de entre todos los buscadores de este tipo, Shodan es el más famoso



## ● Recuerda: Es un motor de búsqueda de máquinas (no webs)

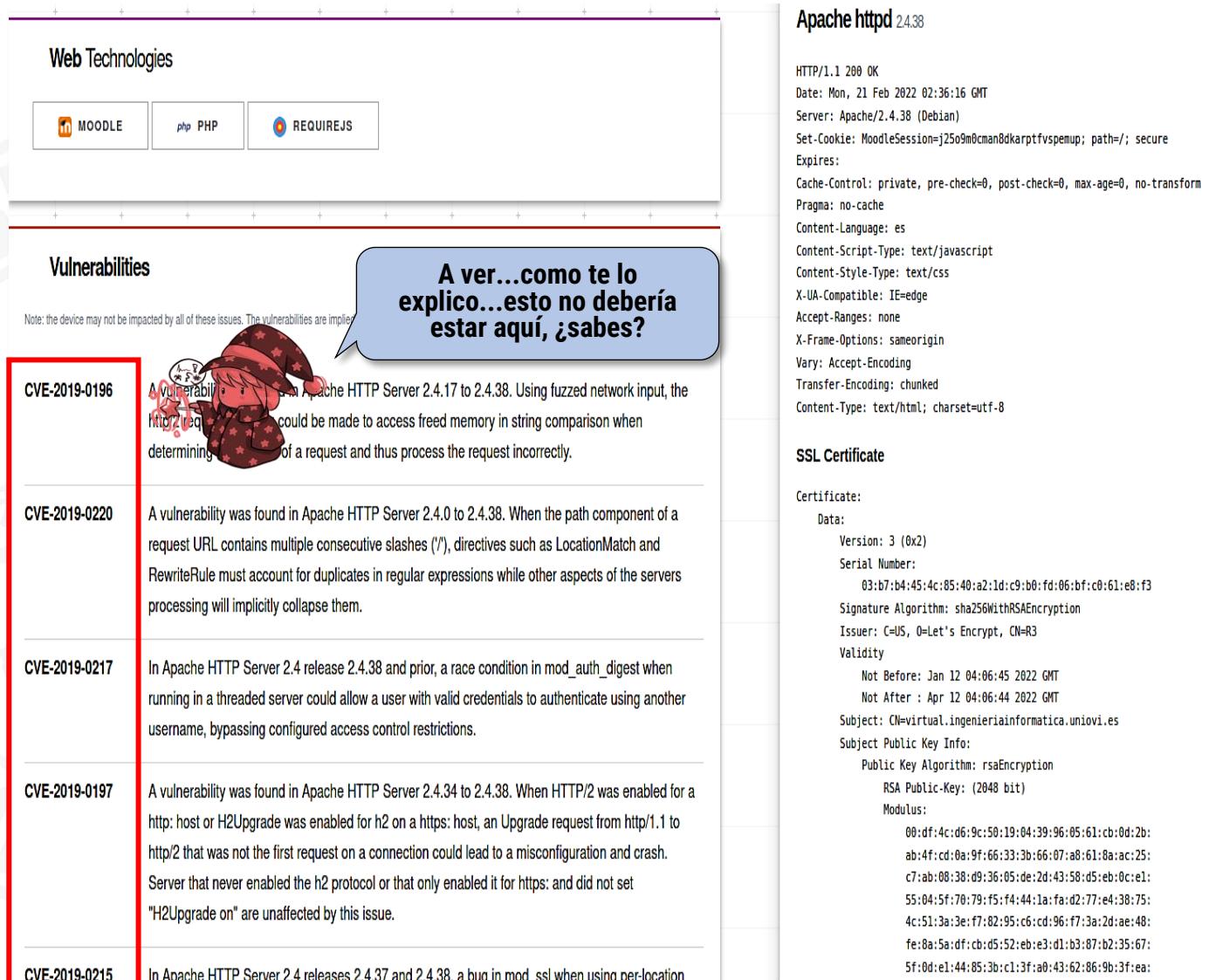
- Routers, servidores, cámaras... (IoT)
- Informa del tipo de servicio encontrado, versión, etc.

## ● Busca hasta 10 dispositivos

- El registro (gratuito) puedes hacer más cosas y usar operadores
- Úsalo para ver dispositivos expuestos a internet y si representan un peligro
  - Ej.: Tienen software de gestión al que acceder y por tanto atacar

## ● Tutoriales

- <https://danielmiessler.com/study/shodan/>
- <https://hacking-etico.com/2016/02/12/4979/>



The screenshot shows a Shodan search result for "Apache httpd 2.4.38". The top section displays "Web Technologies" with icons for Moodle, PHP, and REQUIREJS. Below this is a "Vulnerabilities" section containing five entries, each with a red border:

- CVE-2019-0196**: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the `Http2Request` could be made to access freed memory in string comparison when determining the type of a request and thus process the request incorrectly.
- CVE-2019-0220**: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as `LocationMatch` and `RewriteRule` must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- CVE-2019-0217**: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in `mod_auth_digest` when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- CVE-2019-0197**: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When `HTTP/2` was enabled for a `http: host` or `H2Upgrade` was enabled for `h2` on a `https: host`, an `Upgrade` request from `http/1.1` to `http/2` that was not the first request on a connection could lead to a misconfiguration and crash. Servers that never enabled the `h2` protocol or that only enabled it for `https:` and did not set "`H2Upgrade on`" are unaffected by this issue.
- CVE-2019-0215**: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in `mod_ssl` when using `per-location`

A blue speech bubble on the right side of the vulnerabilities section says: "A ver... como te lo explico... esto no debería estar aquí, ¿sabes?" (Aver... how do I explain this... this shouldn't be here, do you know?).

On the right side of the screenshot, there is a detailed list of HTTP headers for the Apache server:

- HTTP/1.1 200 OK
- Date: Mon, 21 Feb 2022 02:36:16 GMT
- Server: Apache/2.4.38 (Debian)
- Set-Cookie: MoodleSession=j25o9m0cman8dkarptfvspemup; path=/; secure; Expires:
- Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
- Pragma: no-cache
- Content-Language: es
- Content-Script-Type: text/javascript
- Content-Style-Type: text/css
- X-UA-Compatible: IE=edge
- Accept-Ranges: none
- X-Frame-Options: sameorigin
- Vary: Accept-Encoding
- Transfer-Encoding: chunked
- Content-Type: text/html; charset=utf-8

Below the headers is a "SSL Certificate" section with details about the certificate:

- Certificate:
- Data:
  - Version: 3 (0x2)
  - Serial Number: 03:b7:b4:45:4c:85:40:a2:1d:c9:b0:fd:06:bf:c0:61:e8:f3
  - Signature Algorithm: sha256WithRSAEncryption
  - Issuer: C=US, O=Let's Encrypt, CN=R3
  - Validity
    - Not Before: Jan 12 04:06:45 2022 GMT
    - Not After : Apr 12 04:06:44 2022 GMT
  - Subject: CN=virtual.ingenieriainformatica.uniovi.es
  - Subject Public Key Info:
    - Public Key Algorithm: rsaEncryption
    - RSA Public-Key: (2048 bit)
    - Modulus:  
00:df:4c:d6:9c:50:19:04:39:96:05:61:cb:0d:2b:  
ab:4f:cd:0a:9f:66:33:3b:66:07:a8:61:8a:ac:25:  
c7:ab:08:38:d9:36:05:de:2d:43:58:ds:eb:0c:el:  
55:04:5f:70:79:f5:f1:44:1a:fa:d2:77:e7:43:87:5:  
4c:51:3a:3e:f7:82:95:c6:cd:96:f7:3a:2d:ae:48:  
fe:8a:5a:df:cb:d5:52:eb:e3:d1:b3:87:b2:35:67:  
5f:0d:el:44:85:3b:c1:3f:a0:43:62:86:9b:3f:ea

The search engine for Webcams

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.

**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.

**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!

56% of Fortune 100

Shodan is used around the world by researchers, security pros

iMi "primo" nmap es un aficionado a mi lado!

**TOP COUNTRIES**

Country	Count
United States	4,765,632
Mexico	1,234,983
China	1,051,604
Germany	1,044,601
Japon	896,419

**TOP SERVICES**

Service	Count
HTTP	7,055,184
HTTPS	5,376,265
HTTP (8080)	620,781
8081	203,495
HTTP (81)	174,230

**72.29.75.120**

72.29.75.120 static.hostdime.com  
HostDime.com  
Added on 2017-12-04 15:19:36 GMT  
United States, Orlando  
Details

```

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache
Last-Modified: Wed, 20 Jul 2016 05:39:00 GMT
ETag: "6f-5380a3e4a98500"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

<html><head><meta HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/def...

```

**SerranoArt**

66.39.58.227 serranoart.com pair Networks  
Added on 2017-12-04 15:19:36 GMT  
United States, Pittsburgh  
Technologies: Details

```

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache/2.4.29
Last-Modified: Wed, 02 Jan 2008 19:02:16 GMT
ETag: "241d-442c1ea6d5e00"
Accept-Ranges: bytes
Content-Length: 9245
Content-Type: text/html

```

## Busca estos servicios

- HTTP/HTTPS (**webs**)
- FTP (donde la gente **sube archivos**)
- SSH (donde la gente se **conecta**)
- Telnet (**terrible** si te lo encuentras)
- SNMP (**correo electrónico**)
- SIP (**telefonía IP**)
- RTSP (**streaming** de video y cámaras)
- ...



- Lo bueno de tener una cuenta en Shodan es la potencia de sus filtros de búsqueda

- ¡Es como un Google de máquinas!

- Puedes buscar máquinas por una cantidad enorme de criterios

- Incluidos aspectos avanzados de servicios HTTP y SSL

- Es decir, especialmente contra servidores web y máquinas remotamente accesibles desde Internet

## Filter Reference

### General

- all
- asn
- city
- country
- cpe
- device
- geo
- has\_ipv6
- has\_screenshot
- has\_ssl
- has\_vuln
- hash
- hostname
- ip
- isp
- link
- net
- org
- os

¿Quieres hablar  
mi idioma?



### HTTP

- http.component
- http.component\_category
- http.favicon.hash
- http.headers\_hash
- http.html
- http.html\_hash
- http.robots\_hash
- http.securitytxt
- http.status
- http.title
- http.waf

### Bitcoin

- bitcoin.ip
- bitcoin.ip\_count
- bitcoin.port
- bitcoin.version

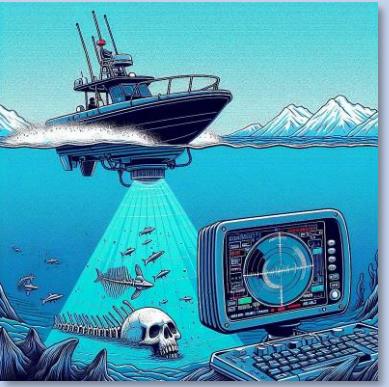
### SSL

- ssl
- sslAlpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkey.bits
- ssl.cert.pubkey.type
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain\_count
- sslcipher.bits
- sslcipher.name
- sslcipher.version
- sslJa3s
- sslJarm
- sslversion

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes que con un buscador como Shodan puedes encontrar cualquier cosa y que hoy en día eso de “cualquier cosa” puede ser literal?*
- *¿Te has parado a pensar que hay conectados a Internet cosas como cámaras de vigilancia, surtidores de gasolina, impresoras, cualquier tipo de máquina, aparatos de casa...y que muchas veces ni siquiera es necesario?*
  - *¿Qué crees que pasaría si Shodan identifica los CVEs de esos dispositivos?*
  - *¿Qué crees que pasaría si esos dispositivos tienen acceso remoto activo y no tienen una protección adecuada?*
- *Por ejemplo, la password por defecto de muchos de ellos es algo conocido porque se puede buscar por internet fácilmente...*
  - *¿Crees que todas las personas saben que tienen un dispositivo de estos conectado a internet y además habrán cambiado esa contraseña por otra cosa?*
  - *¿Entiendes por tanto la enorme peligrosidad de tener cosas expuestas en internet*
  - *¿Y cómo puedes usar Shodan para saber si tienes un problema por tener una “casa conectada”?*



## ESCANEAR VULNERABILIDADES

Buscando las vergüenzas a una máquina (si te autorizan a ello) con un click



# ¿QUÉ VAS A APRENDER EN ESTE BLOQUE?

- Que existen programas que son capaces de encontrar automáticamente vulnerabilidades en máquinas o webs que les pasemos
- Y que son capaces encontrar miles de vulnerabilidades
  - Que, para encontrarlas manualmente, necesitaríamos conocimientos que (aún) no tenemos
- Que, a pesar de no ser perfectas y no poder sustituir a un ser humano, sí que te pueden ayudar si no tienes conocimientos técnicos
- Y, por último, que tengas bien claro que estas herramientas **solamente las puedes pasar sobre máquinas o webs que sean tuyas**
  - O te autoricen a hacerlo...
  - Asumiendo que podrían alterar su funcionamiento y, por tanto, **debes hacerlo sobre una copia y con mucha precaución**
    - Lo mejor es contra una copia en una máquina virtual (**R-11 “Príncipe de Asturias”**)
  - ¡Es “fuego real”!

¡Boom! ¡Boom! jajajajaja



# ¿QUÉ SON ESTAS HERRAMIENTAS?

- Hasta ahora hemos hablado de buscar vulnerabilidades con **nmap** para máquinas
  - O con buscadores, para máquinas en internet
- Pues resulta que hay herramientas que te **automatizan esta búsqueda**
  - Y que puedes lanzar contra máquinas o webs en cualquier lugar
- Pero hay un gran problema: **hacerlo sin autorización es delito**
  - *¿Por qué te lo explico entonces? Porque tú puedes ayudar a cualquiera a saber si tiene problemas*
  - *¿Por qué no aconsejas a un familiar o amigo/a que tenga máquinas o una web que se haga estas pruebas a sí mismo/a y así evitar un disgusto?*

Somos armas cargadas para pruebas,  
pero armas, al fin y al cabo. Así que  
cuidado contra qué nos disparas, no  
vayas a tener “un disgusto legal”

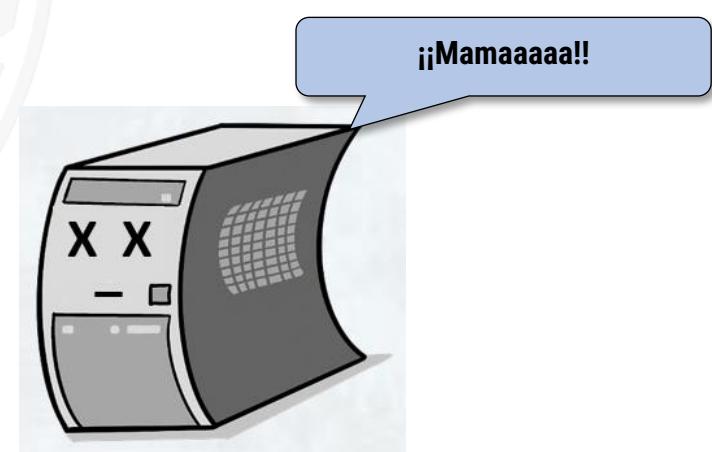


# ¿QUÉ SON ESTAS HERRAMIENTAS?

- Las herramientas automáticas de descubrimiento de vulnerabilidades son útiles para una cosa concreta

- Nos permiten obtener un esquema claro de las vulnerabilidades más evidentes que un sistema puede tener, ahorrándonos tiempo
- **Pero NO sustituyen el trabajo de una auditoria de seguridad bien hecha (la complementan)**
- No las confundas **NUNCA** con un pentesting o con el trabajo de un Red Team
  - Eso es mucho más completo, hay que contratarlo (y pagarle)
- Algunas empresas llaman a esto “pentesting”: es **ERRÓNEO (y probablemente fraudulento)**

¡Boom! ¡Boom! jajajajaja



# INTRODUCCIÓN: LA IMPORTANCIA DE ESTAS HERRAMIENTAS

- Si se solucionan todos los problemas detectados por estas herramientas, la máquina objetivo será significativamente menos vulnerable
  - Por lo tanto, son herramientas necesarias para la seguridad...
  - ... pero son “buscadores de vulnerabilidades” **no una prueba de seguridad completa**
- Cada herramienta de estas genera una cantidad grande de tráfico de red
  - Y puede consumir muchos recursos del objetivo...
  - Por lo tanto, repito, **NUNCA** tenemos que lanzarlas sin la debida autorización del propietario



Hablando en serio: Me puedes usar para el bien o para el mal. Es TU decisión. Yo solo soy una herramienta, cómo me usas es COSA TUYA

## ● Permite análisis en detalle de servidores

- Puede comprobar más de 50.000 vulnerabilidades, actualizándose diariamente
- Examinar los servidores y cualquier servicio que oferten
  - Su base de datos de vulnerabilidades es **enorme**, y cubre muchos servicios conocidos
- También requiere 4+ Gb RAM solo para la aplicación

Fuente: <https://null-byte.wonderhowto.com/how-to/perform-large-scale-network-security-audit-with-openvass-gsa-0179340/>



The screenshot shows the Greenbone Security Assistant web interface. The title bar reads "Greenbone Security Assistant". The URL in the address bar is "https://192.168.1.199:9392/omp?cmd=get\_report&report\_id=560edce2-23f1-4210-b355-4b093fd1cd34". The main content area displays a report titled "Report: Results (67 of 343)". To the right of the report title, there are details: ID: 560edce2-23f1-4210-b355-4b093fd1cd34, Modified: Wed Aug 9 16:39:33 2017, Created: Wed Aug 9 16:03:21 2017, Owner: admin. Below this, a table lists 67 vulnerabilities found across 67 hosts. The columns in the table are: Vulnerability, Severity, QoD, Host, Location, and Actions. The first few rows of the table are:

Vulnerability	Severity	QoD	Host	Location	Actions	
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.205	80/tcp		
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.1.205	1099/tcp		
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.205	1524/tcp		
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.205	8787/tcp		
OS End Of Life Detection	10.0 (High)	80%	192.168.1.205	general/tcp		
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.205	3632/tcp		
PostgreSQL weak password	9.0 (High)	99%	192.168.1.205	5432/tcp		
VNC Brute Force Login	9.0 (High)	95%	192.168.1.205	5900/tcp		
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.205	3306/tcp		
SSH Brute Force Logins With Default Credentials Reporting	9.0 (High)	95%	192.168.1.205	22/tcp		

## ● Tutoriales

- <https://blog.ehcgroup.io/index.php/2018/06/21/escaneo-de-vulnerabilidades-con-openvas-9-parte-1-instalacion-y-configuration/>
- <https://blog.ehcgroup.io/index.php/2018/06/21/escaneo-de-vulnerabilidades-con-openvas-9-parte-2-escaneo-de-vulnerabilidades/>

# 1 Result Overview

Host	High	Medium	Low	Log	False Positive
[REDACTED] uniovi.es	0	9	0	28	0
Total: 1	0	9	0	28	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Information on overrides is included in the report.

Notes are included in the report.

This report might not show details of all issues that were found.

This report contains all 37 results selected by the filtering described above. Before filtering there were 37 results.

Soy una herramienta profesional y al acabar mi trabajo te hago un informe completo de todo. Estoy en otro nivel, bro 😊



Medium (CVSS: 4.3)  
NVT: jQuery < 1.9.0 XSS Vulnerability

## Product detection result

cpe:/a:jquery:jquery:1.7.1

Detected by jQuery Detection (OID: 1.3.6.1.4.1.25623.1.0.141622)

## Summary

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The `jQuery(strInput)` function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '`<`' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '`<`' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

## Vulnerability Detection Result

Installed version: 1.7.1

Fixed version: 1.9.0

## Solution

**Solution type:** VendorFix

Update to version 1.9.0 or later.

## Affected Software/OS

jQuery prior to version 1.9.0.

## Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: jQuery < 1.9.0 XSS Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.141636

Version used: \$Revision: 12183 \$

## Product Detection Result

Product: cpe:/a:jquery:jquery:1.7.1

Method: jQuery Detection

OID: 1.3.6.1.4.1.25623.1.0.141622)

## References

CVE: CVE-2012-6708

Other:

URL: <https://bugs.jquery.com/ticket/11290>



# ZED ATTACK PROXY (ZAP)

[https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)

- Escáner de seguridad para webs

- Una de las herramientas más famosas y utilizadas para estos fines

- Incluye varios análisis de seguridad pasivos y/o activos que le permiten encontrar vulnerabilidades en las webs escaneadas

- Pero de nuevo: **NO LO LANCES CONTRA UNA WEB SIN AUTORIZACIÓN**
- Y mejor contra una copia en una máquina virtual (**R-11 “Príncipe de Asturias”**)

- Tutorial

- <https://blog.segu-info.com.ar/2015/09/tutorial-de-uso-owasp-zaproxy.html>



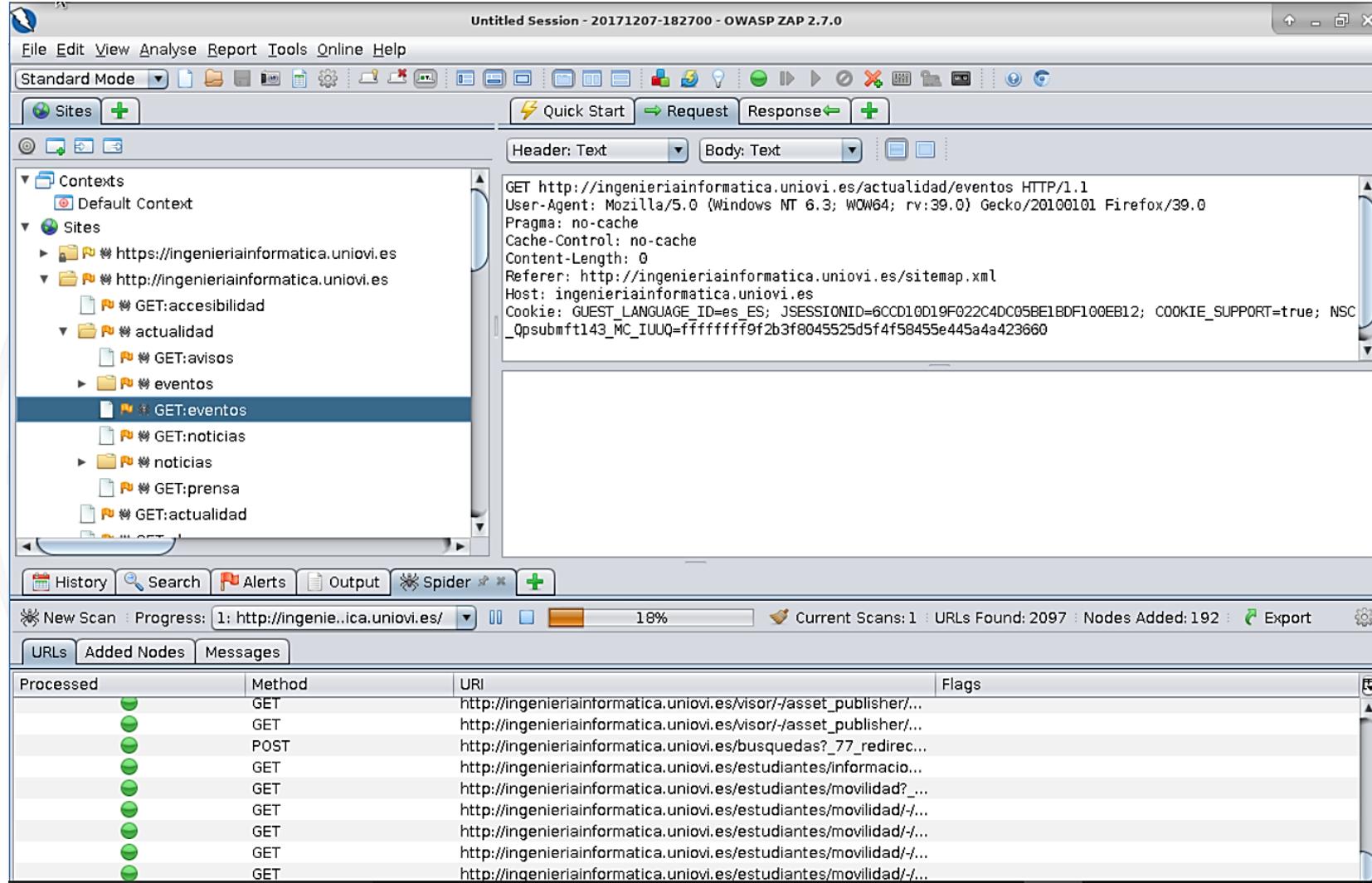
Como mi “hermana” soy “fuego real”,  
pero contra páginas web...

# ZED ATTACK PROXY (ZAP)

- Un análisis automático sigue sin ser perfecto
- Pero puede encontrar “vergüenzas” en una web
  - Cualquier delincuente puede hacer lo mismo, así que...
  - ...¡ARRÉGLALAS! ☺



¿Has pagado por una web y yo la hago “cantar”? ¿Igual contactaba con quien te la hizo eh? Muy normal no es, especialmente si le estás pagando mantenimiento...



Untitled Session - 20171207-182700 - OWASP ZAP 2.7.0

Header: Text Body: Text

GET http://ingenieriainformatica.uniovi.es/actualidad/eventos HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0  
Pragma: no-cache  
Cache-Control: no-cache  
Content-Length: 0  
Referer: http://ingenieriainformatica.uniovi.es/sitemap.xml  
Host: ingenieriainformatica.uniovi.es  
Cookie: GUEST\_LANGUAGE\_ID=es\_ES; JSESSIONID=6CCD10D19F022C4DC05BE1BDF100EB12; COOKIE\_SUPPORT=true; NSC\_Qpsubmft143\_MC\_IUUQ=ffffffff9f2b3f8045525d5f4f58455e445a4a423660

Processed	Method	URI	Flags
✓	GET	http://ingenieriainformatica.uniovi.es/visor/-/asset_publisher/...	
✓	GET	http://ingenieriainformatica.uniovi.es/visor/-/asset_publisher/...	
✓	POST	http://ingenieriainformatica.uniovi.es/busquedas?_77_redirec...	
✓	GET	http://ingenieriainformatica.uniovi.es/estudiantes/informacio...	
✓	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad?_...	
✓	GET	http://ingenieriainformatica.uniovi.es/estudiantes/movilidad/-/...	

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes que estas herramientas de búsqueda de vulnerabilidades no son más que una especie de “metralleta” para buscar problemas de seguridad, que lanza contra máquinas o contra webs?*
  - *¿Te ha quedado claro entonces por qué no se la puedes lanzar a cualquiera, ya que sería equivalente a dispararle con una ciber-metralleta?*
- *¿Entiendes que, aunque estén pensadas en principio para no destruir las máquinas o webs que examinan, la posibilidad nunca es del 0%?*
  - *¿Y que debes hacerlo con autorización sobre una copia, y con mucho cuidado?*
- *Por tanto ¿eres consciente de que ahora puedes aconsejar el uso de una de estas herramientas a alguien que tenga un negocio y que sea de tu confianza?*
  - *¿O que pueda pedir a su proveedor que lo haga por él?*
  - *¿O que te cree una copia de lo que quieras escanear para hacer pruebas sobre él?*
- *¿Entiendes como casa el concepto de máquinas virtuales con este tipo de escaneos, y cómo puedes usar ambas cosas para escanear de forma segura?*

# VIGILANDO LAS REDES: ATAQUE

