

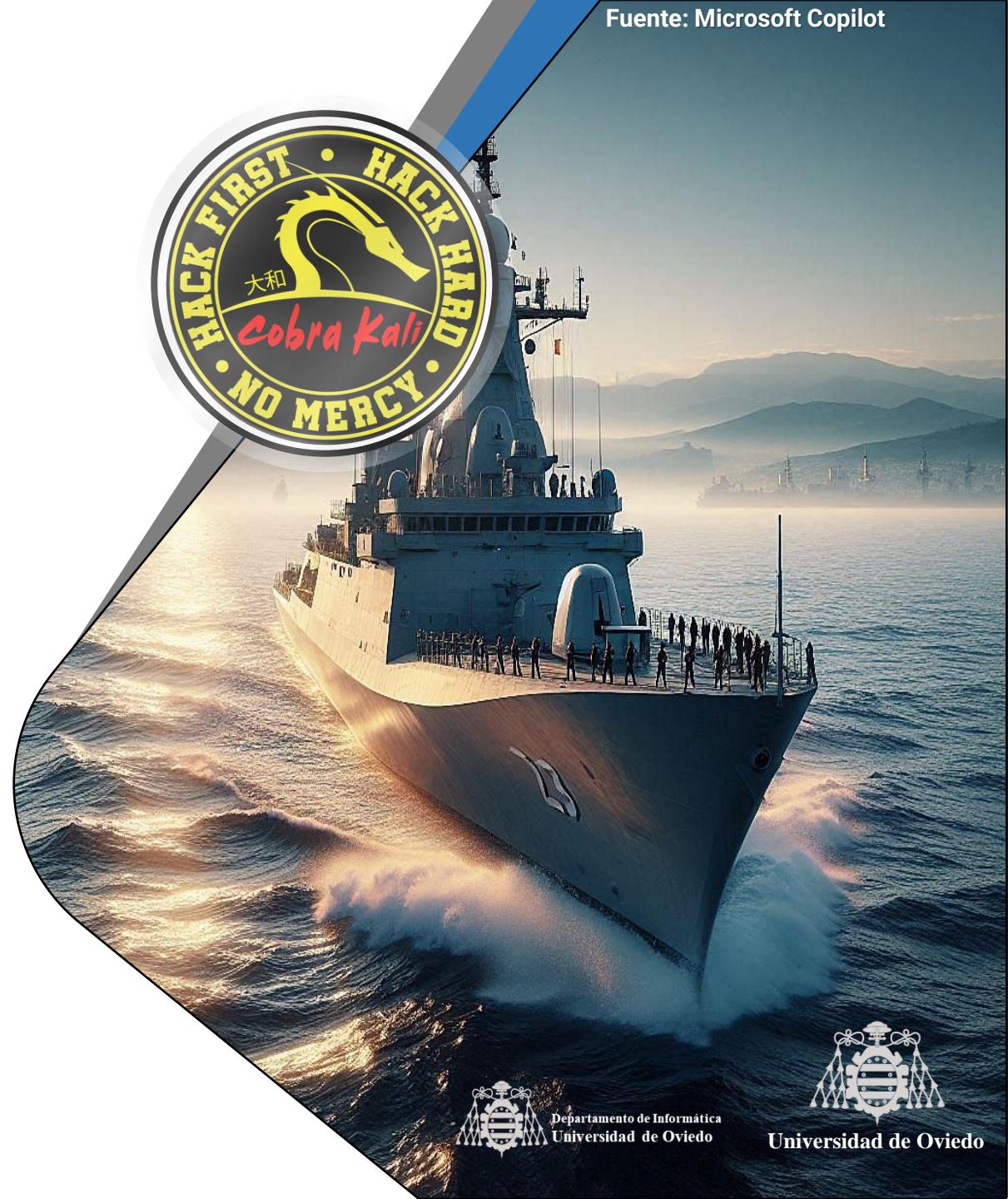
VIGILANDO LAS REDES: ATAQUE

Entendiendo cómo funciona todo el mundo conectado



JOSÉ MANUEL REDONDO LÓPEZ

PROYECTO "F-83 'NUMANCIA' " V1.0 BETA



¿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!
 - Si, el humor está puesto...¡a 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"

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-
Exploitación
TBA. K-329 "Belgorod"

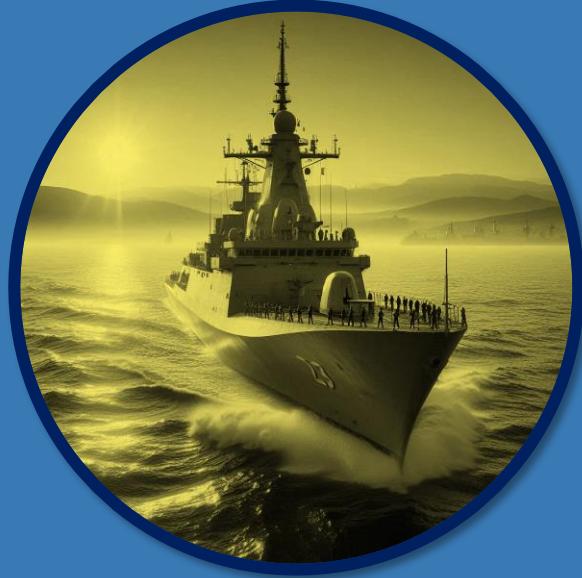


Protección de Servidores y Aplicaciones Web

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



ÍNDICE



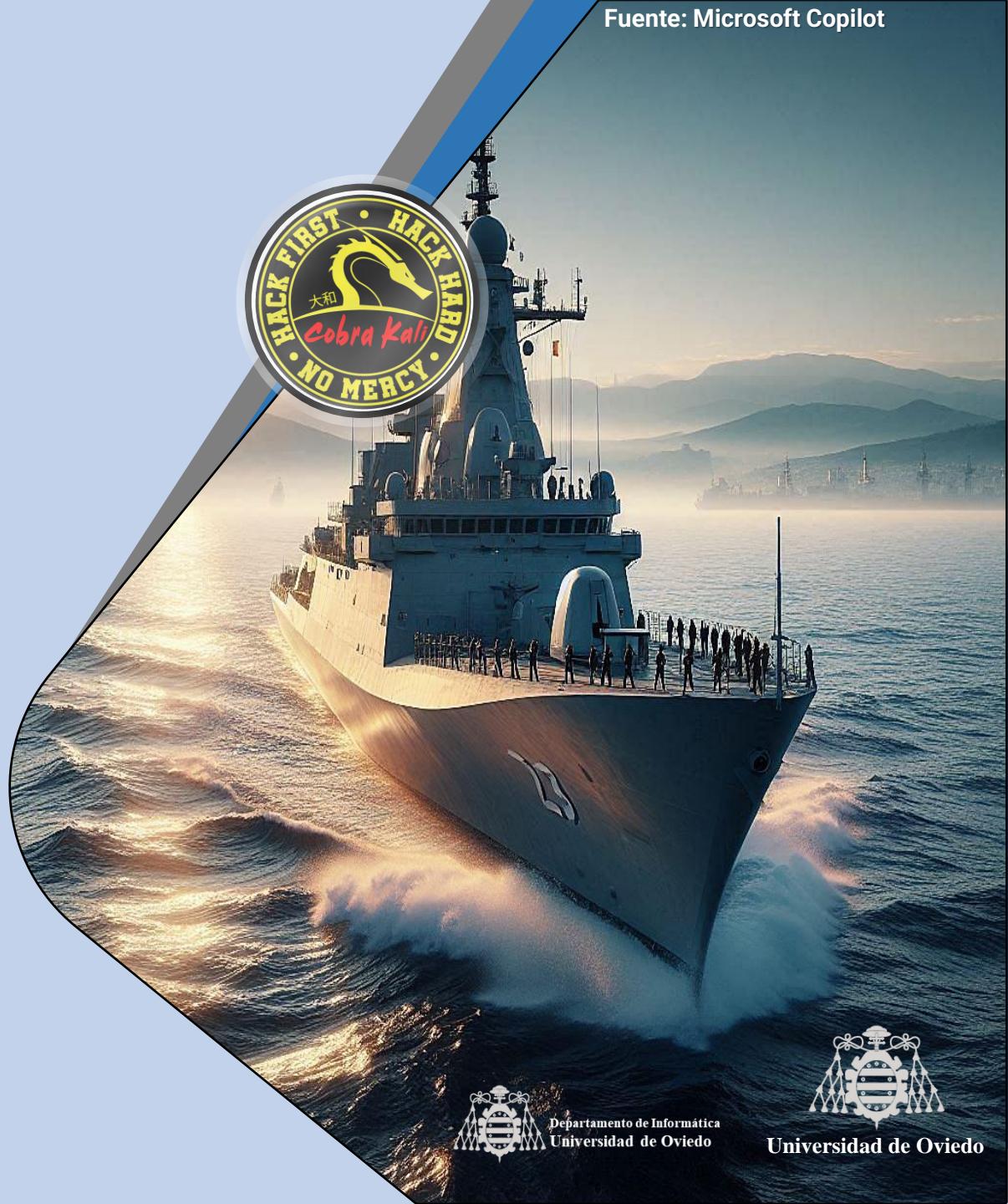
- [Un poco de teoría “light” de redes](#)
 - [Las direcciones IP](#)
 - [El DNS](#)
 - [Redes locales o LANs](#)
 - [Puertos y servicios](#)
 - [NAT y DHCP](#)
- [Nmap, el detective de la red](#)
 - [Los CVE](#)
 - [“Serious” Nmap 😊](#)
- [Shodan go on!](#)
- [Escaneadores automáticos de vulnerabilidades](#)

< Ir al Índice



UN POCO DE TEORÍA “LIGHT” DE REDES

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



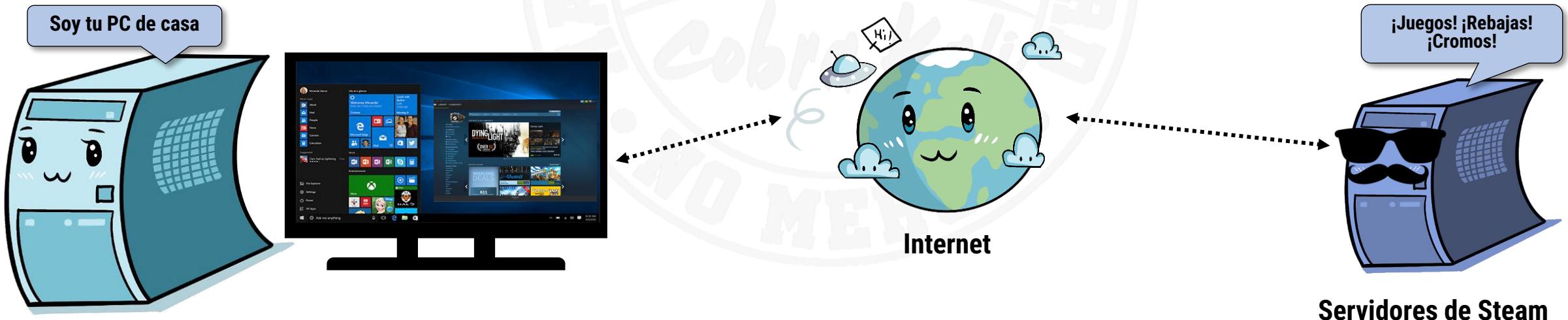
¿PUEDES EXPLICÁRMELO COMO SI NO TUVIERA NI IDEA?

- ¡Hola! Este 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 como hacer ciertas tareas** (escribir emails, documentos...)



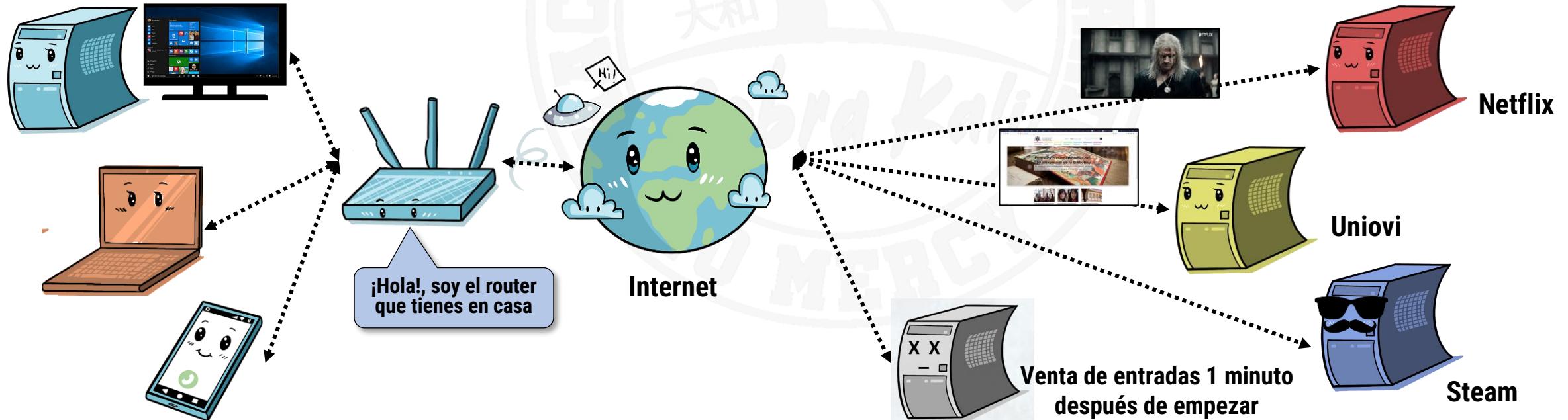
LA “MAGIA” DE INTERNET

- 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** 
 - Sentados en su propio ordenador
- Es decir, casi nadie se sienta delante de ellos para hacer cosas “normales”
 - Te conectas a ellos desde casa y les pides cosas...y ellos te las sirven ☺



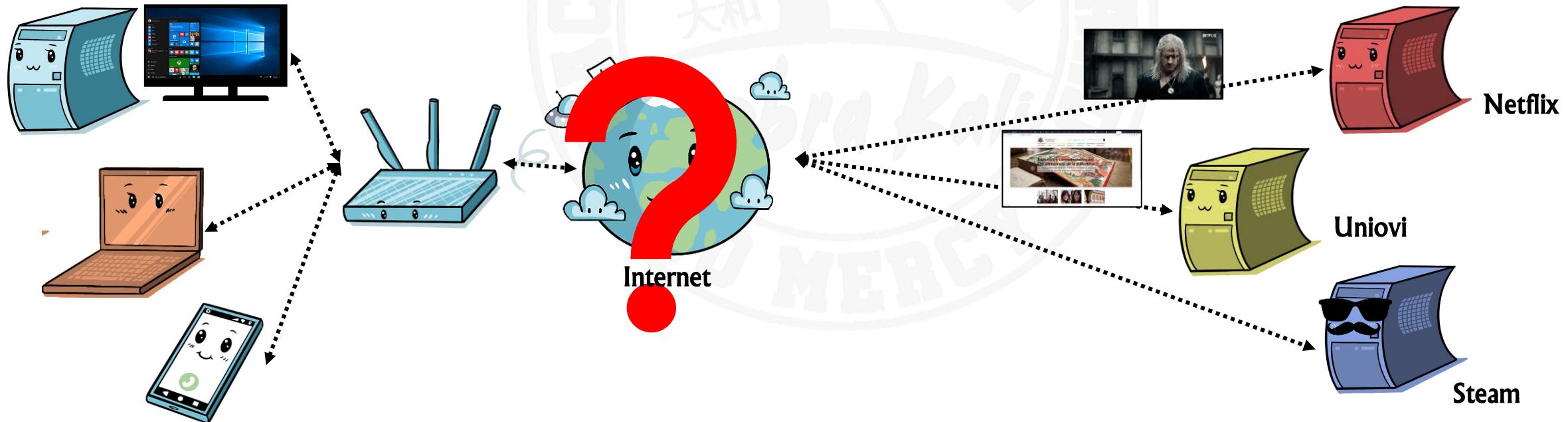
LA "MAGIA" DE INTERNET

- ¿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 mi 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

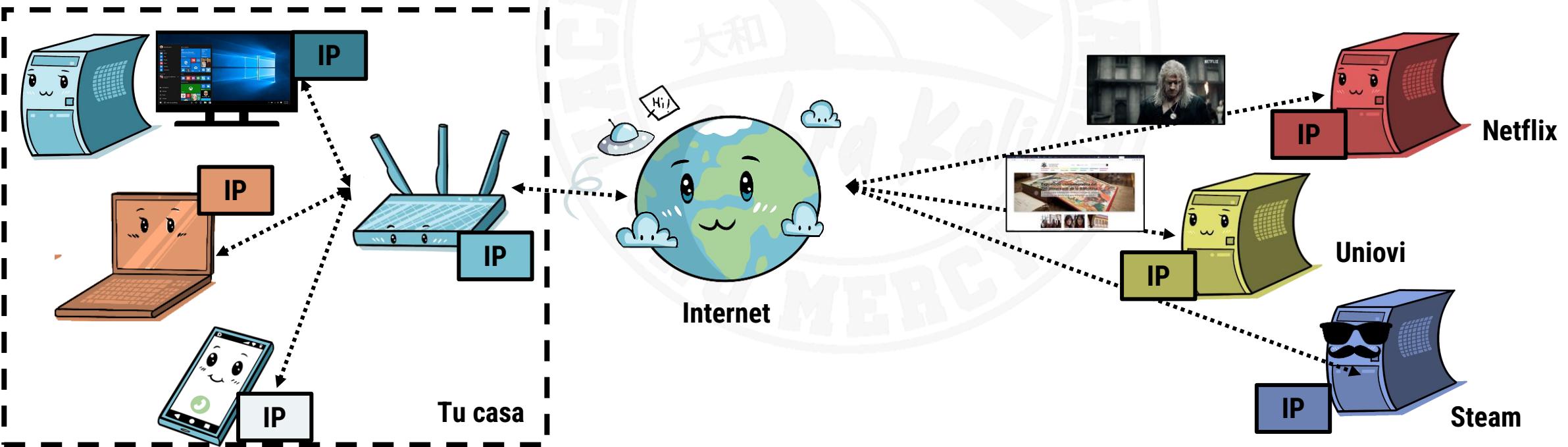
El "DNI" de los ordenadores en una red



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?
- ¡Sí! 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 bloques (números entre 0 y 255) separados por puntos
- Eso sería la **versión 4 (IPv4)**; también está la versión 6 (IPv6)
 - Que son 8 bloques de 4 n°s y letras de la A a la F, pero eso mejor lo dejamos por ahora
- De momento **solo vamos a hablar de versión clásica**, la 4

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

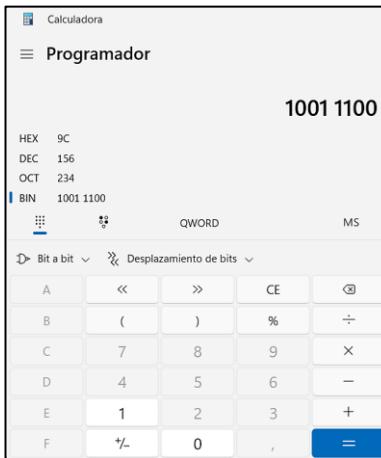


LA “MAGIA” DE INTERNET: DIRECCIONES IP

● 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

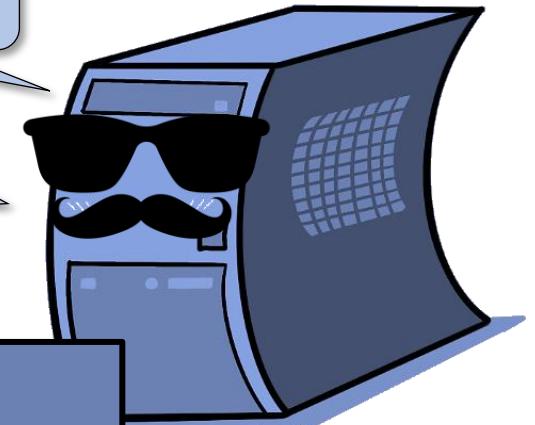


Este es el formato de IP que seguramente ya hayas visto alguna vez

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

IP

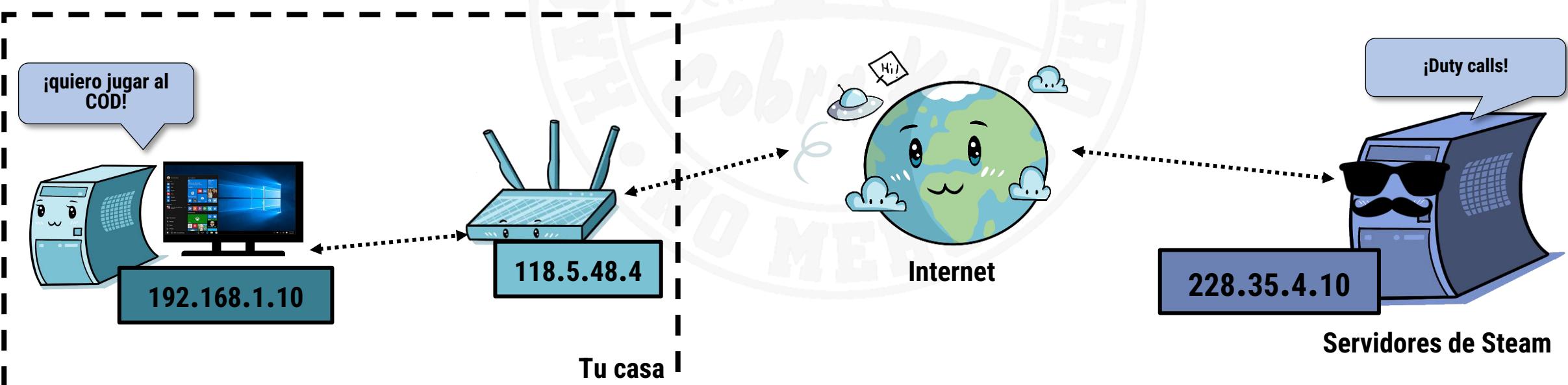
156.35.94.10



LA “MAGIA” DE INTERNET: DIRECCIONES IP

- Entonces tu 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 ☺

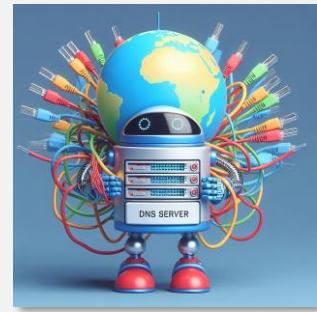


LA “MAGIA” DE INTERNET: LOS DNS

- 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!





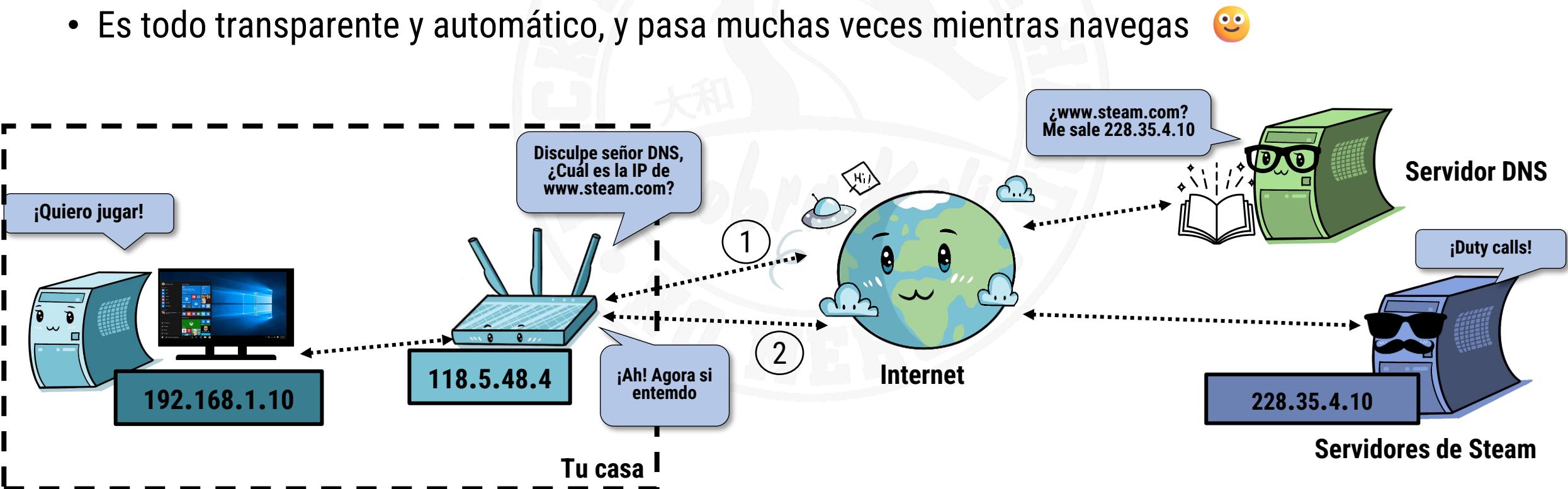
El DNS

El “diccionario” que nos permite usar Internet



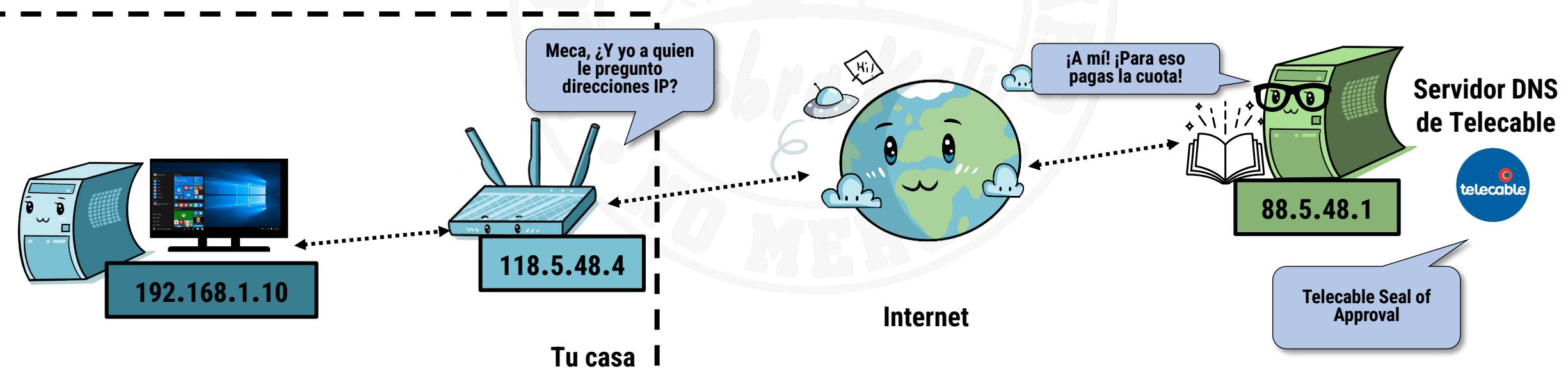
LA “MAGIA” DE INTERNET: LOS DNS

- Sin meternos demasiado en tecnicismos, un DNS es un servicio 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”? ¿Cómo sabe el navegador la IP de esa máquina-diccionario de IPs?*
 - ¡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**)

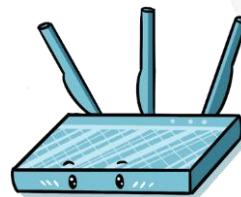


LA “MAGIA” DE INTERNET

- **¿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 por IP directamente
 - *¿Red local? ¿Ostras y esa movida? Me dejas loco/a*
 - Tranqui, que es lo siguiente que viene ☺



Tus dispositivos



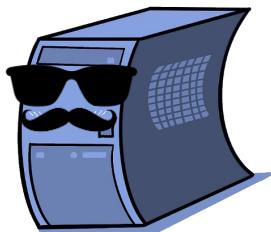
Tu router de casa



Internet



Servidor DNS



Servidores de los
distintos servicios a los
que accedes

¡Todos somos actores principales en esta obra! ☺



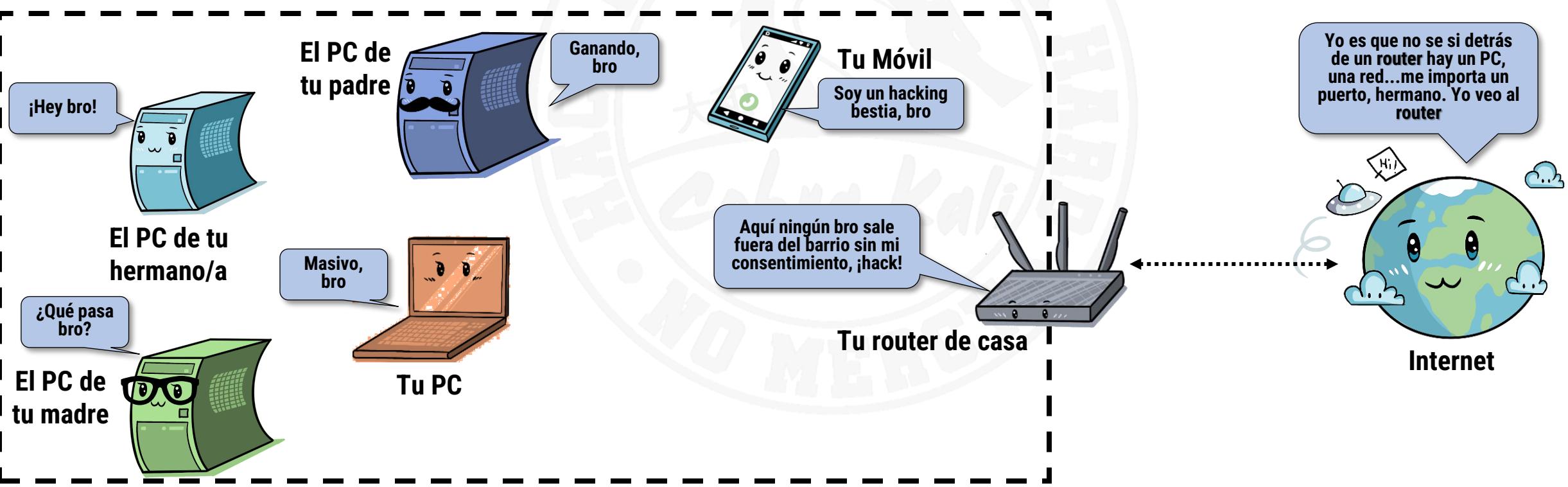
Redes locales o LANs

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



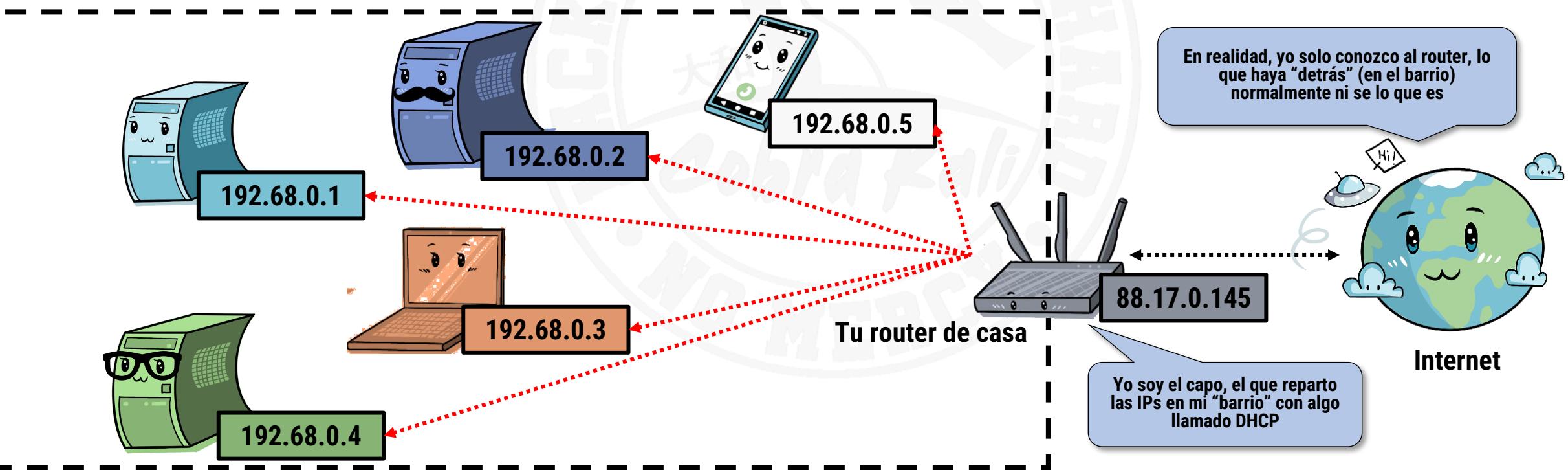
LA “MAGIA” DE INTERNET: REDES LOCALES

- 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



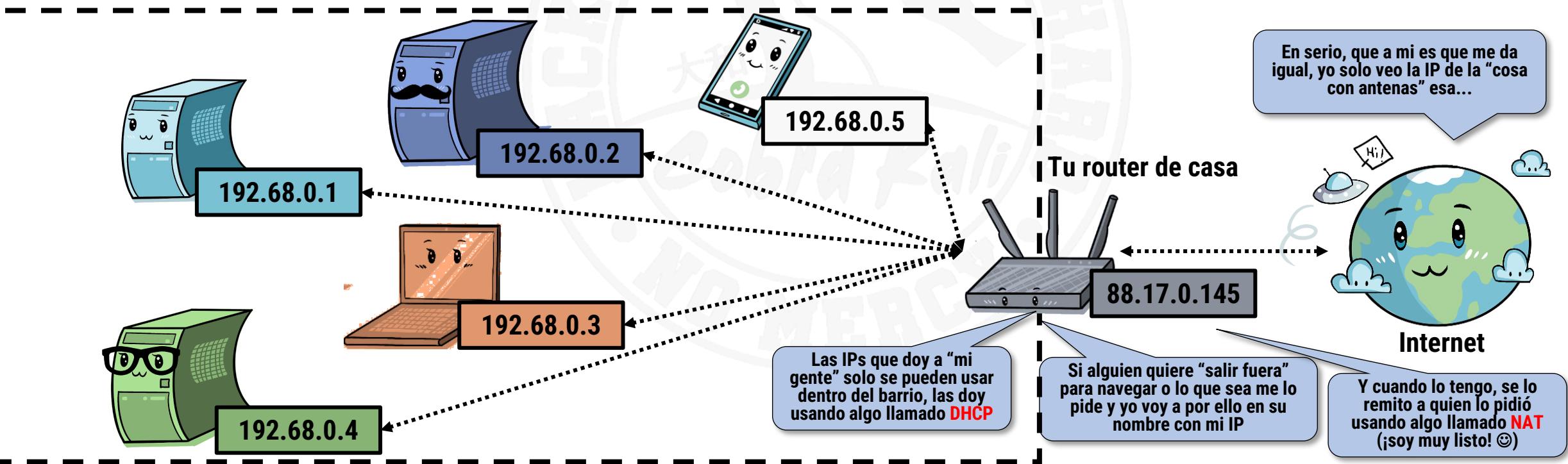
LA “MAGIA” DE INTERNET: REDES LOCALES

- 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 hace eso!



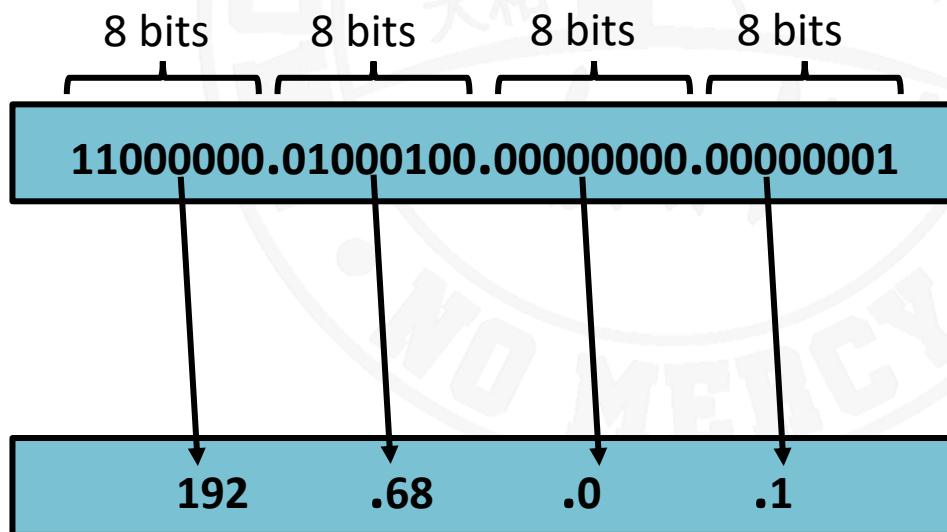
LA “MAGIA” DE INTERNET: REDES LOCALES

- ¿Y cómo sabe a qué “barrio” pertenece cada uno? ¡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! :D



LA “MAGIA” DE INTERNET: REDES LOCALES

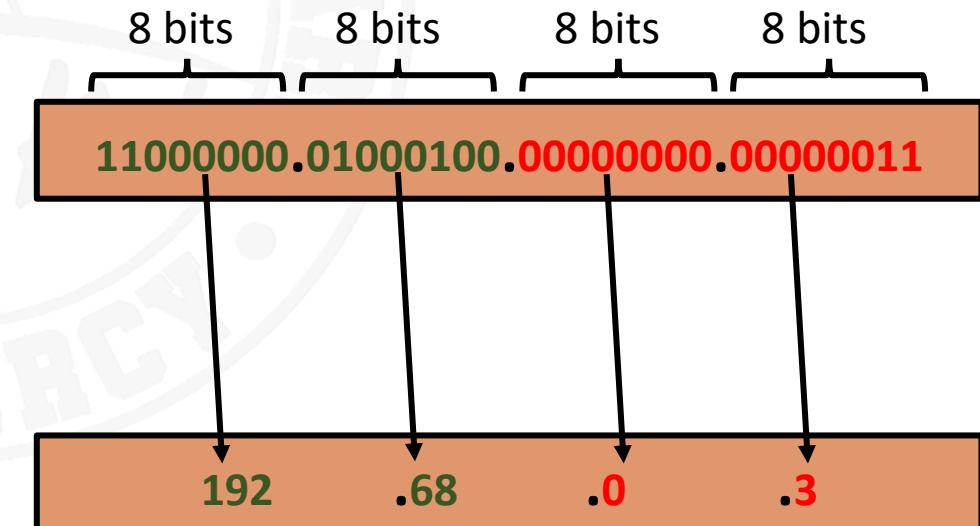
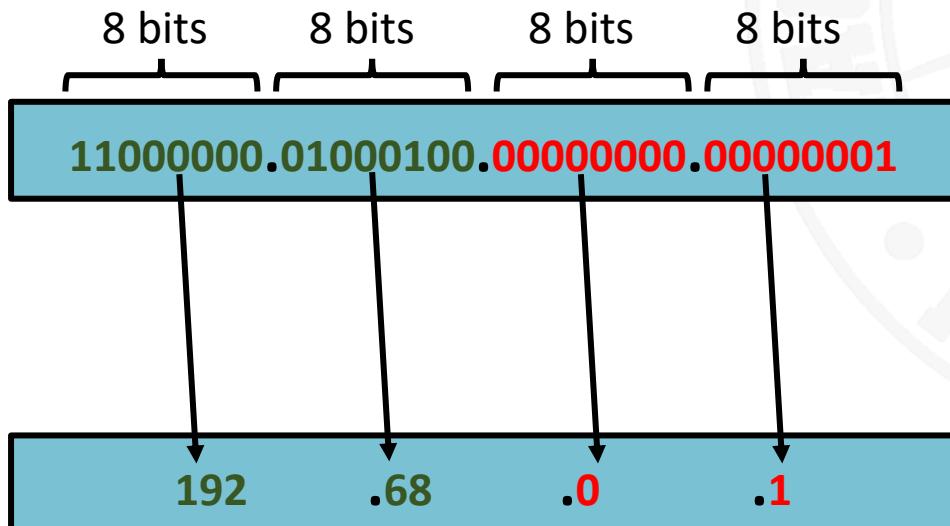
- Una IP es compatible con otra si empiezan por los mismos N bits, siendo N un número establecido por la definición de lo que es el “barrio” (red)
 - Quizá pienses “No me lo estás haciendo más fácil de entender...”
- ¡Espera! Mira esta IP y su “traducción” a nºs decimales
 - (Ahora entenderás porque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



LA “MAGIA” DE INTERNET: REDES LOCALES

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

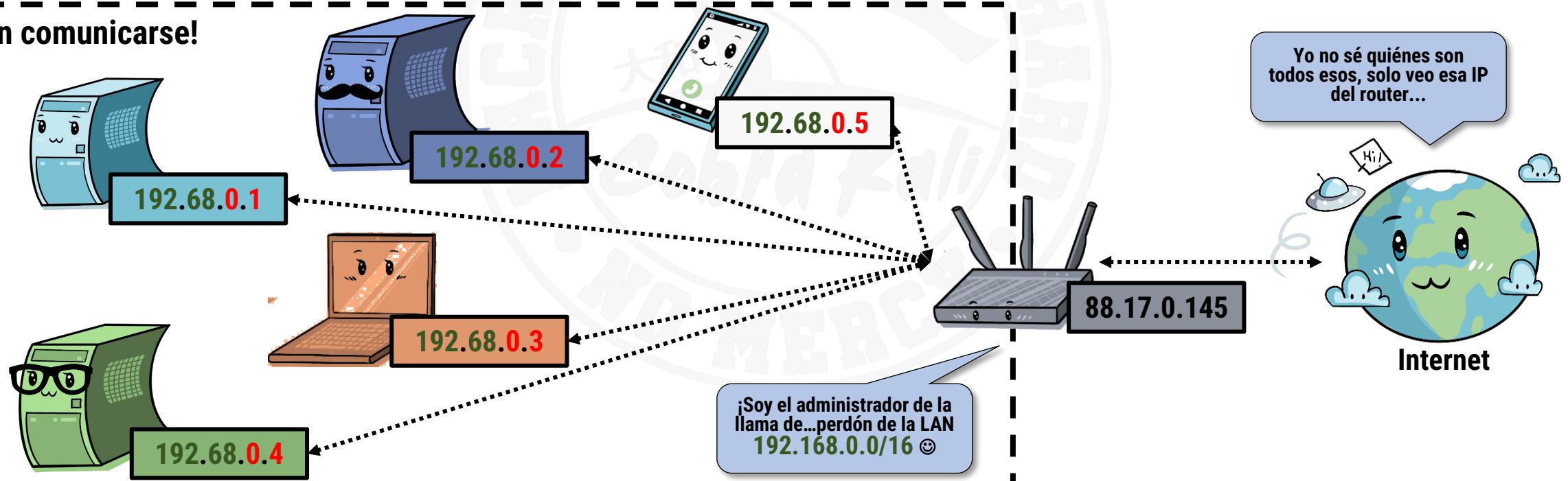
- ¿Estas dos serían compatibles? ¡SI!
- Es como los grupos sanguíneos compatibles...¡pero más fácil! :D



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 eso cómo se escribe para que la gente lo entienda?
 - 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)

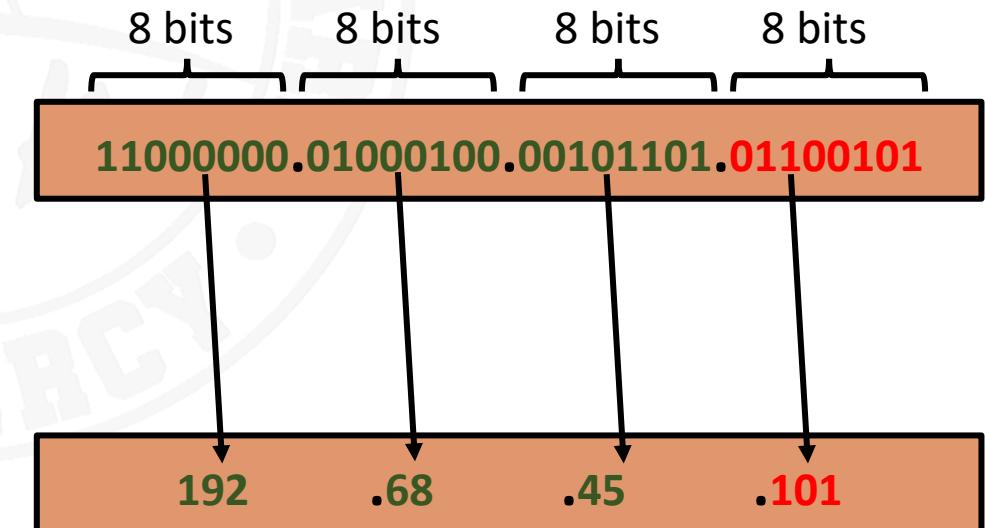
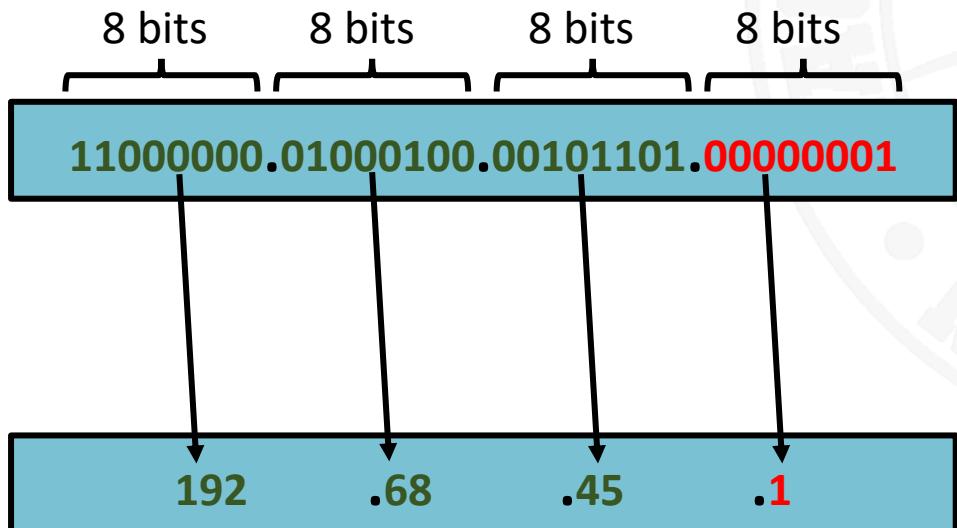
¡Pueden comunicarse!



LA “MAGIA” DE INTERNET: REDES LOCALES

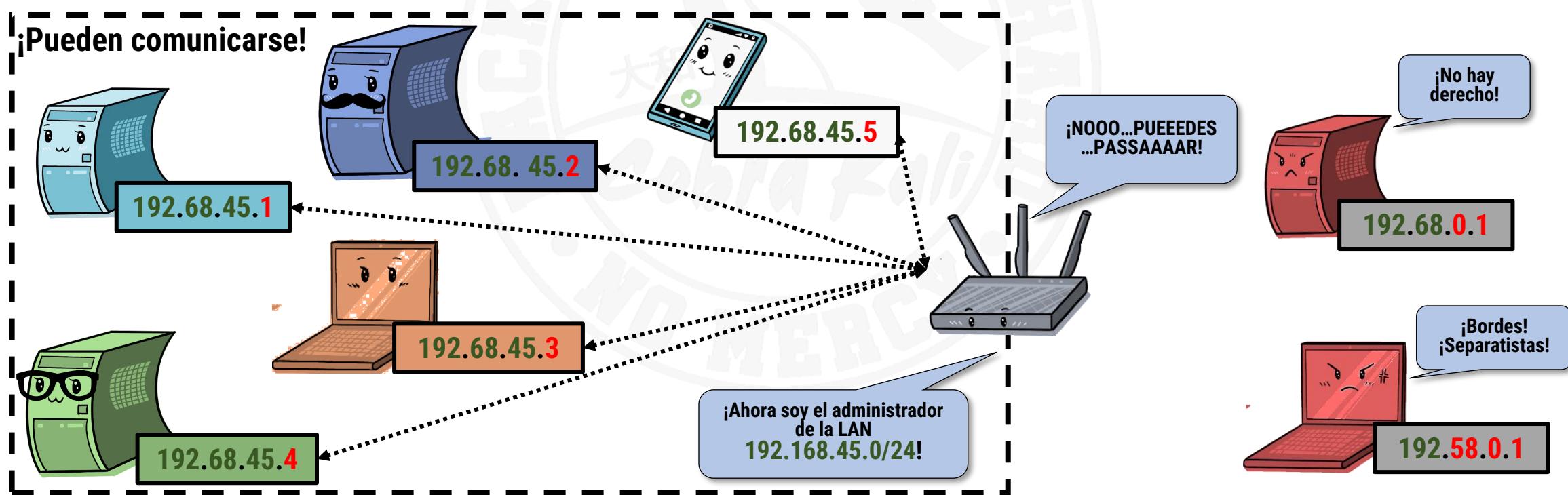
- *¿Crees que estas a punto de pillarlo?... Pues te pongo otro ejemplo*

- 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! ($8+8+8 = 24$)



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! ;)





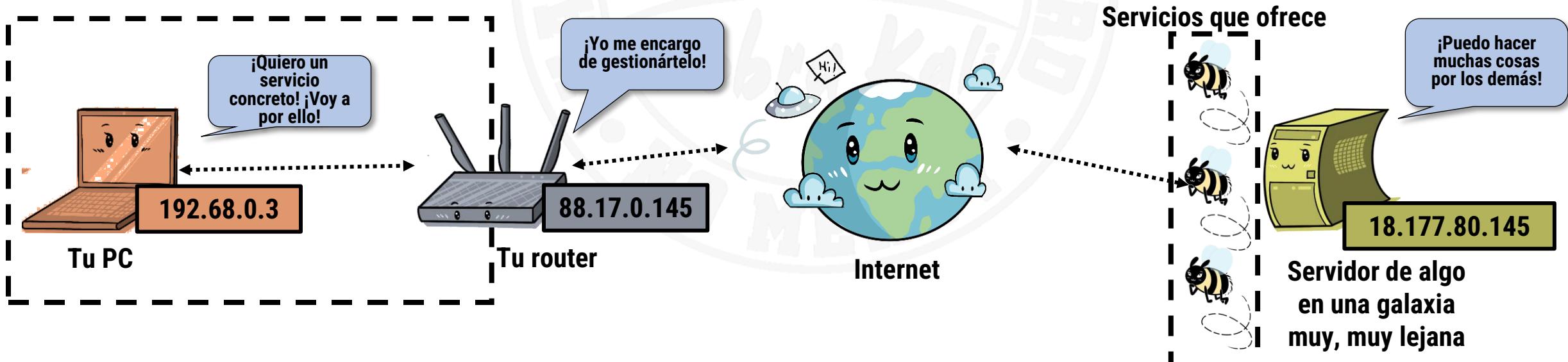
Puertos y servicios

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...**)



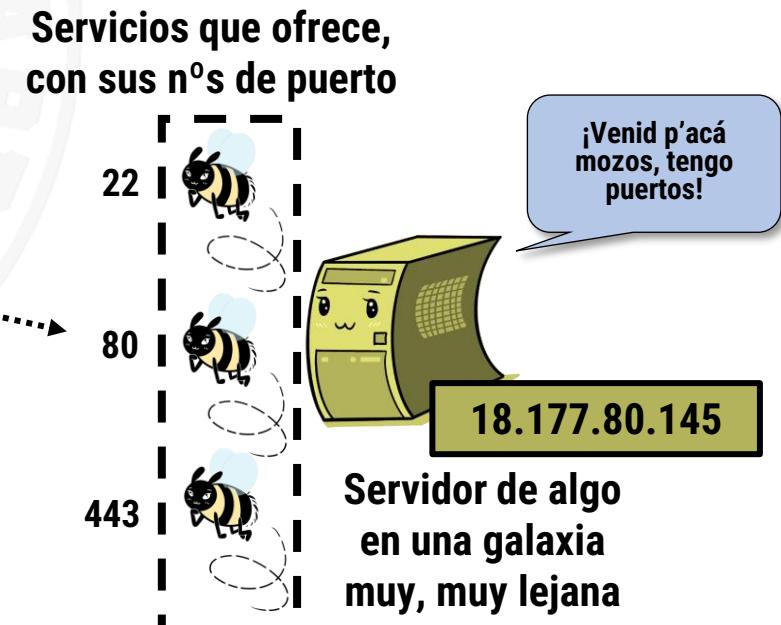
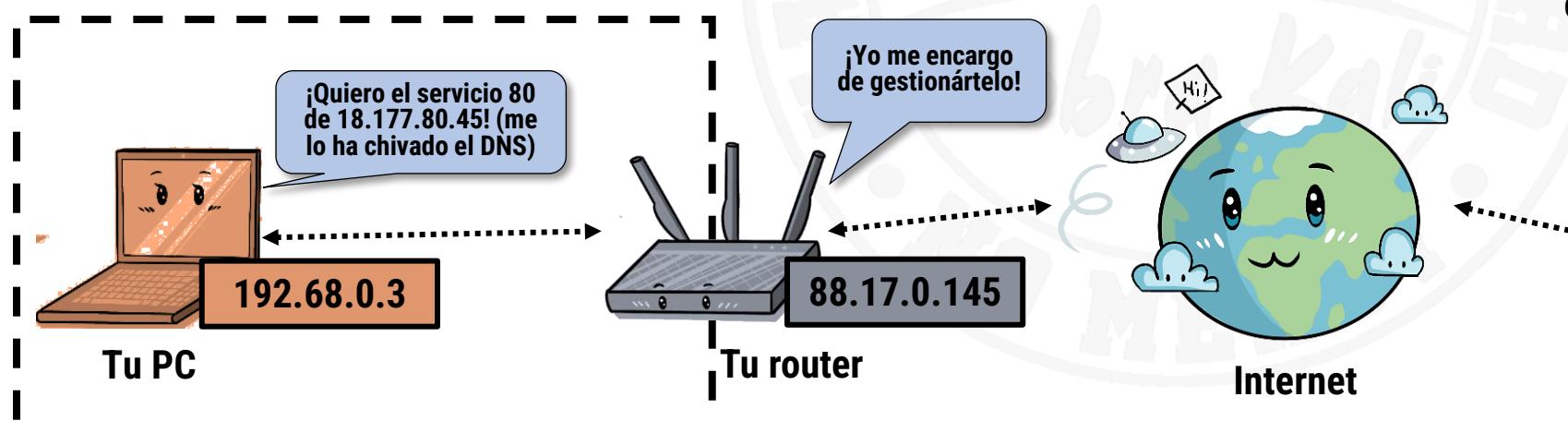
LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

● ¡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)



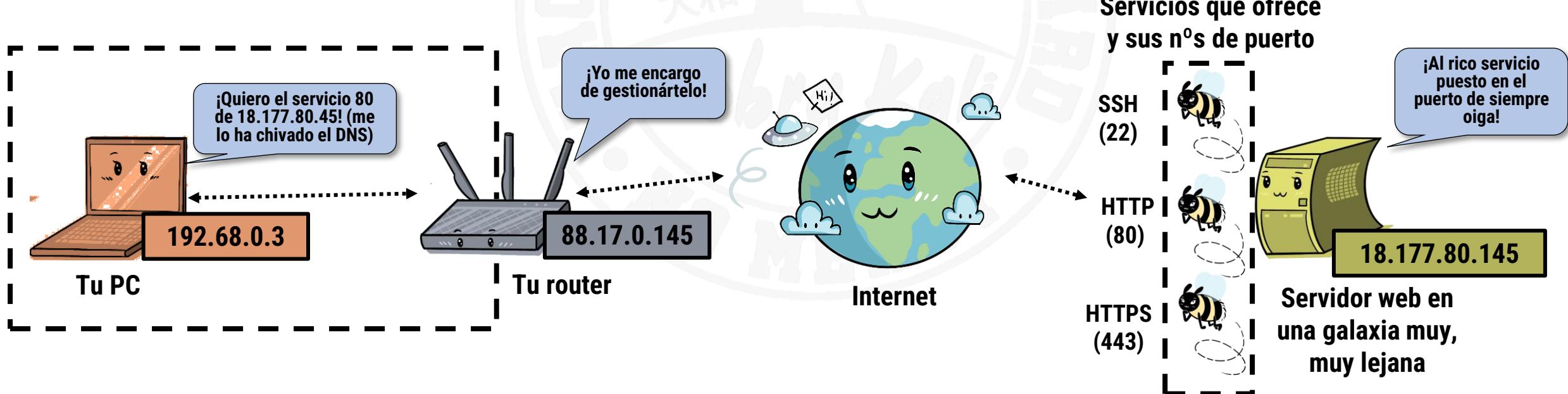
LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

- *¿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?*

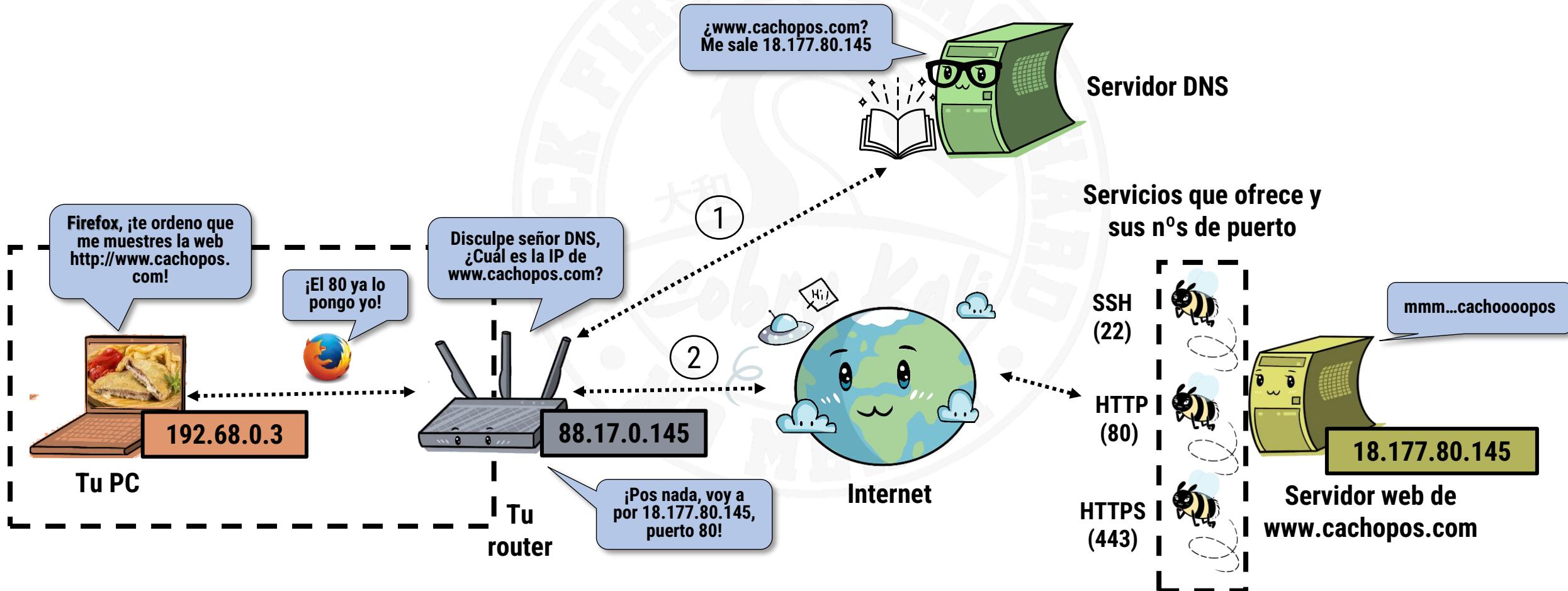
- ¡Sí! Siempre es el 80 (**http**)
- O el 443 (**https**, si la web va con candado, es decir, la transmisión no se puede “cotillear”)



LA “MAGIA” DE INTERNET: PUERTOS Y SERVICIOS

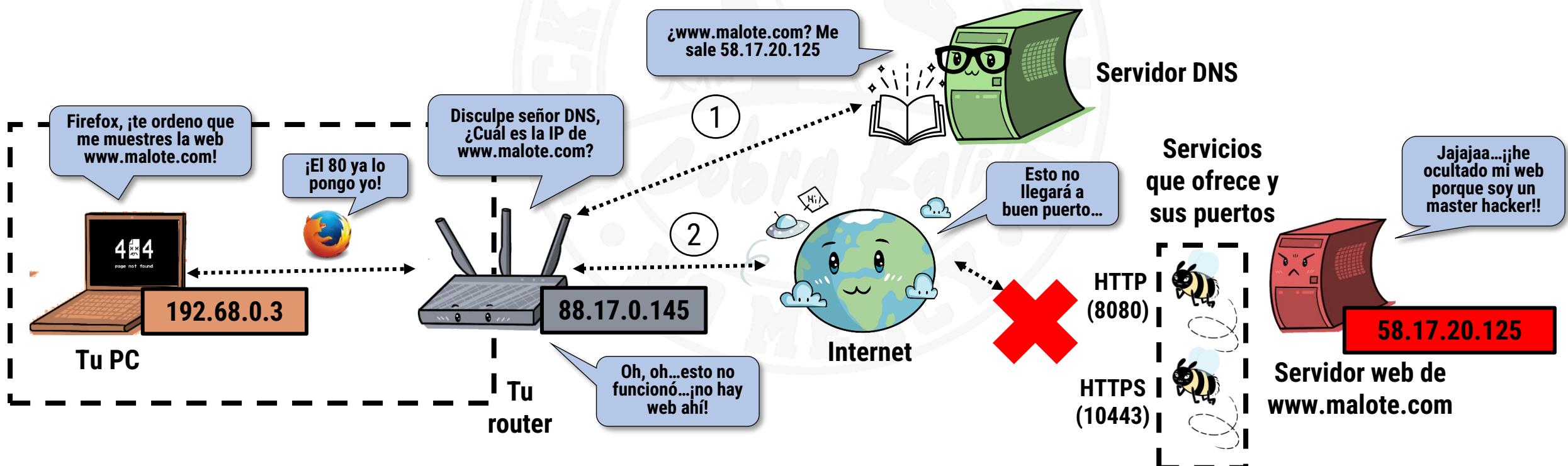
- ¡Pero yo nunca pongo puertos de nada en el navegador!

- ¡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

TCP/UDP Port Numbers					
7 Echo	554 RTSP	2745 Bagle.H	6891-6901 Windows Live	José Manuel López	
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime	Hernando López	
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf		
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649 CU-SeeMe		
23 Telnet	587 SMTP	3124 HTTP Proxy	8000 Internet Radio		
25 SMTP	591 FileMaker	3127 MyDoom	8080 HTTP Proxy		
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087 Kaspersky AV		
43 WHOIS	631 Internet Printing	3222 GLBP	8118 Privoxy		
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200 VMware Server		
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion		
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak		
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B		
70 Gopher	860 iSCSI	3690 Subversion	9100 HP JetDirect		
79 Finger	873 rsync	3724 World of Warcraft	9101-9103 Bacula		
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119 MXit		
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800 WebDAV		
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898 Dabber		
110 POP3	995 POP3 over SSL	4664 Google Desktop	9999 Urchin		
113 Ident	1025 Microsoft RPC	4672 eMule	10000 Webmin		
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000 BackupExec		
123 NTP	1080 SOCKS Proxy	5000 UPnP	10113-10116 NetIQ		
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	11371 OpenPGP		
137-139 NetBIOS	1194 OpenVPN	5001 iperf	12035-12036 Second Life		
143 IMAP4	1214 Kazaa	5004-5005 RTP	12345 NetBus		
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	13720-13721 NetBackup		
177 XDMCP	1311 Dell OpenManage	5060 SIP	14567 Battlefield		
179 BGP	1337 WASTE	5190 AIM/ICQ	15118 Dipnet/Oddbob		
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	19226 AdminSecure		
264 BGMP	1512 WINS	5432 PostgreSQL	19638 Ensim		
318 TSP	1589 Cisco VQP	5500 VNC Server	20000 Usermin		
381-383 HP Openview	1701 L2TP	5554 Sasser	24800 Synergy		
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	25999 Xfire		
411-412 Direct Connect	1725 Steam	5800 VNC over HTTP	27015 Half-Life		
443 HTTP over SSL	1741 CiscoWorks 2000	5900+ VNC Server	27374 Sub7		
445 Microsoft DS	1755 MS Media Server	6000-6001 X11	28960 Call of Duty		
464 Kerberos	1812-1813 RADIUS	6112 Battle.net	31337 Back Orifice		
465 SMTP over SSL	1863 MSN	6129 DameWare	33434+ traceroute		
497 Retrospect	1985 Cisco HSRP	6257 WinMX	Legend		
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella	Chat		
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade	Encrypted		
513 rlogin	2049 NFS	6566 SANE	Gaming		
514 syslog	2082-2083 cPanel	6588 AnalogX	Malicious		
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC	Peer to Peer		
520 RIP	2222 DirectAdmin	6679/6697 IRC over SSL	Streaming		
521 RIPng (IPv6)	2302 Halo	6699 Napster			
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent			

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



NAT y DHCP

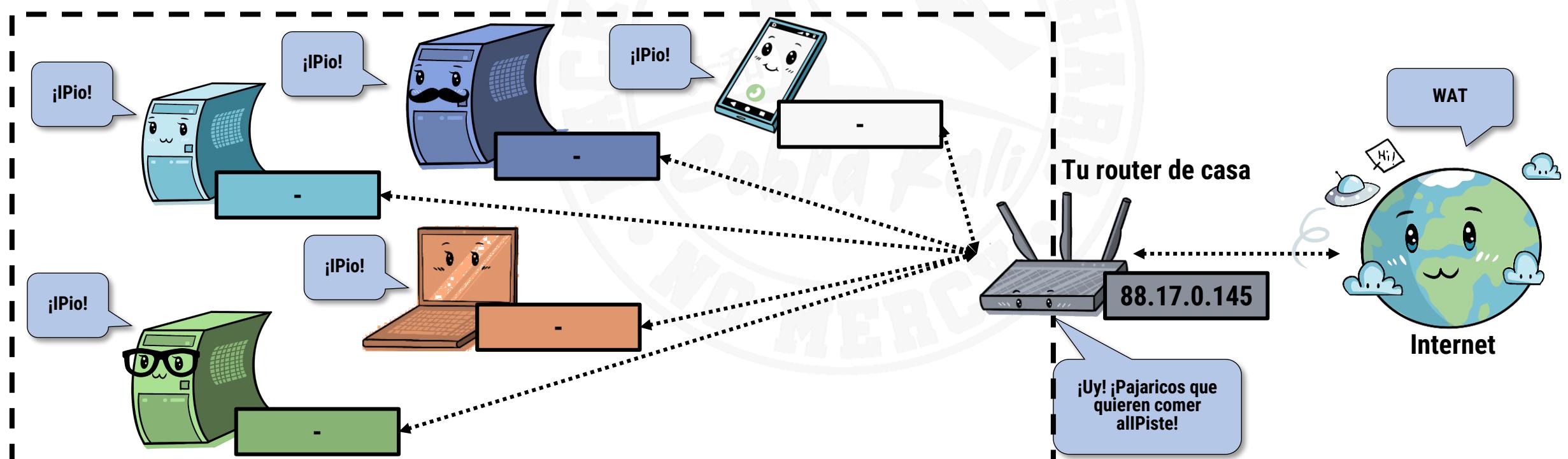
¡Los últimos elementos para entender todo!



¿DHCP? ¿MÁS ACRÓNIMOS?

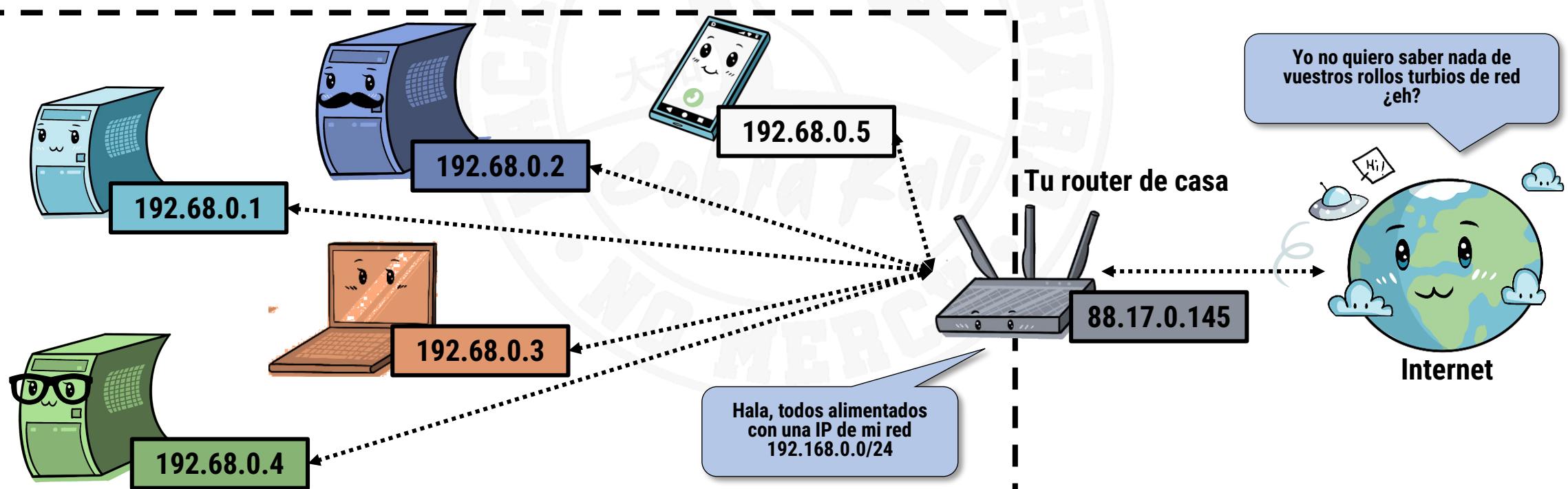
- Antes mencionamos de pasada dos acrónimos, NAT y DHCP, que son parte de la “magia” que hace funcionar todo esto

- 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 ☺



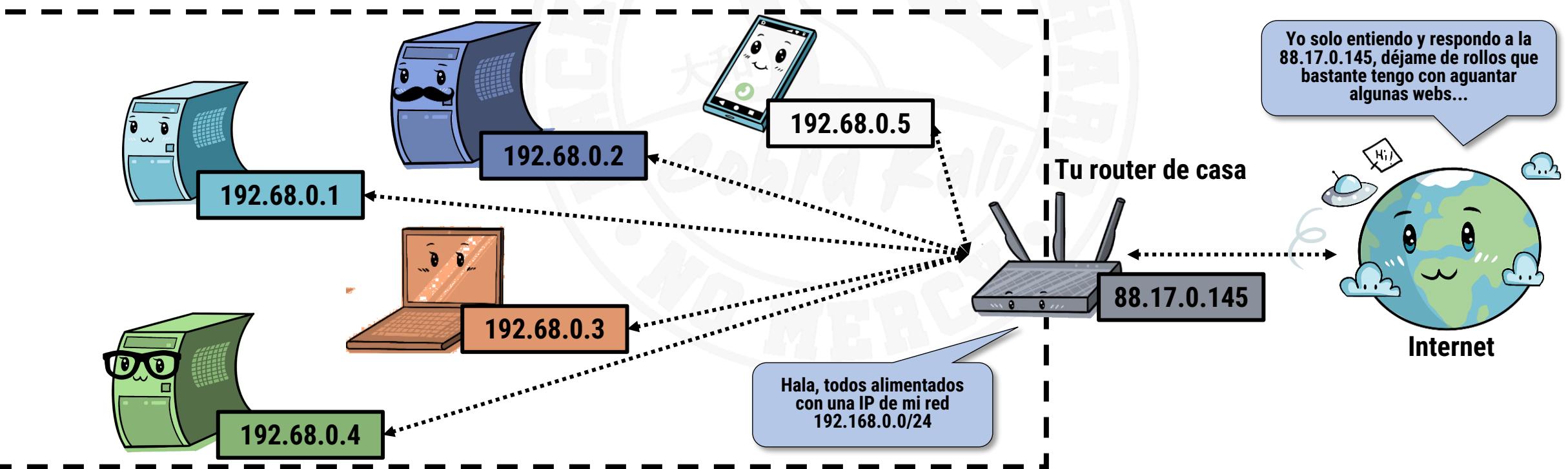
DHCP

- 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, 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

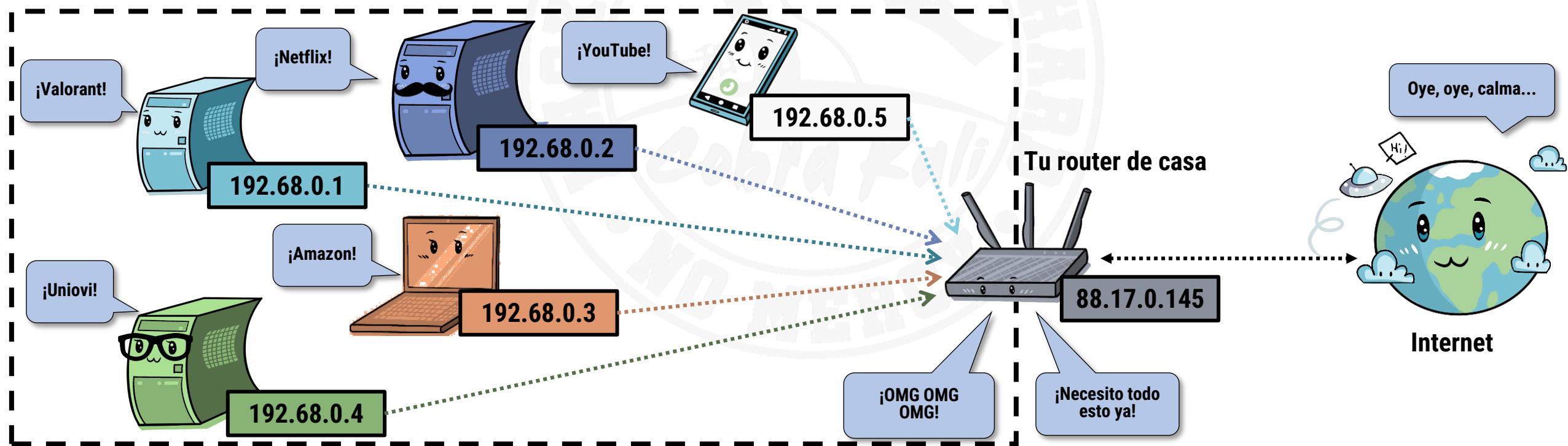
NAT

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

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

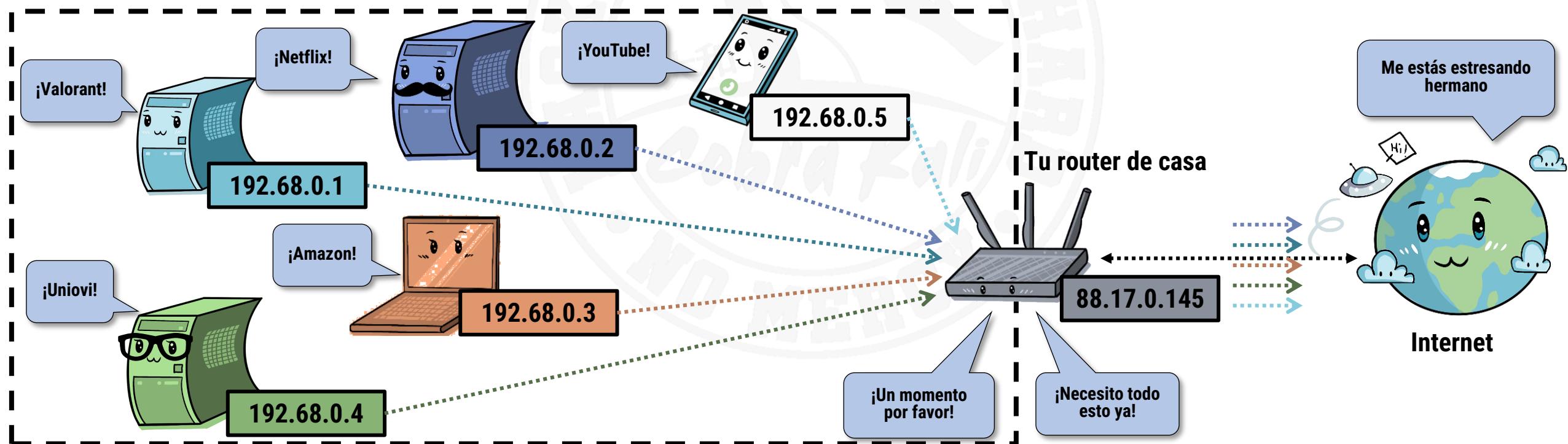
- **Grosso modo, tu router es un repartidor de pedidos MUY ocupado**

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

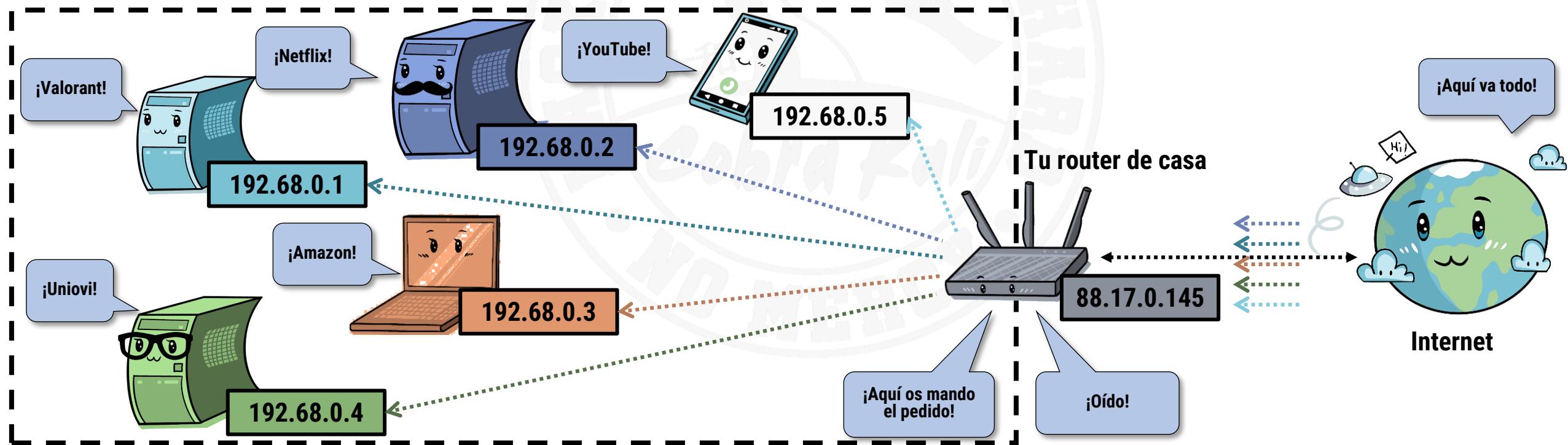


NAT

- Y es que, al final, tu router “da la cara” en Internet por todas las máquinas 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 lo que ha pedido, 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 ☺

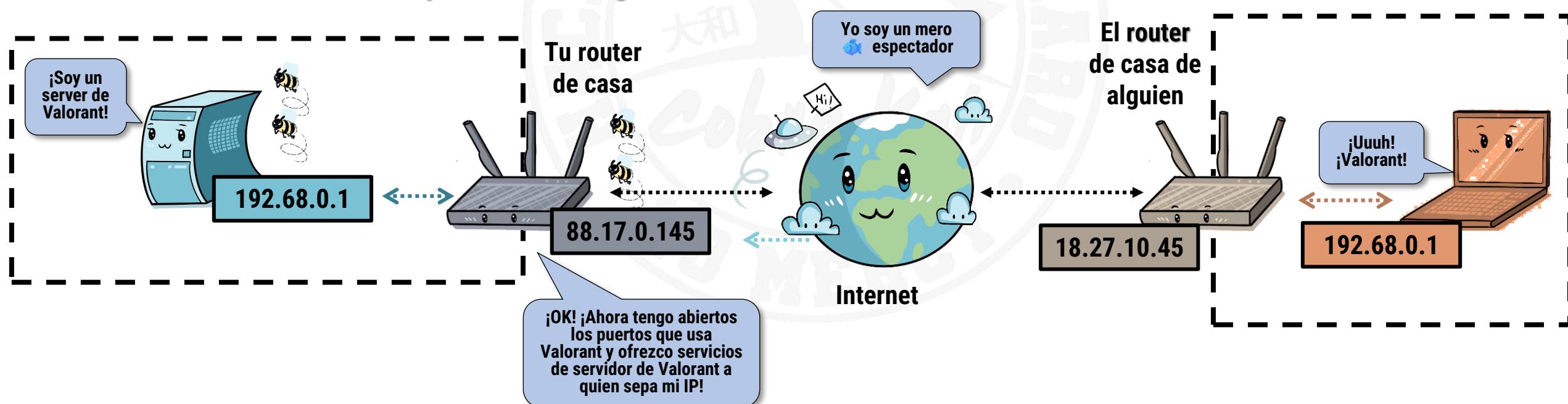
OYE, OYE, ¿Y SI ALGUNA DE MIS MÁQUINAS QUIERE OFRECER ALGO EN INTERNET?

- 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 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!!!



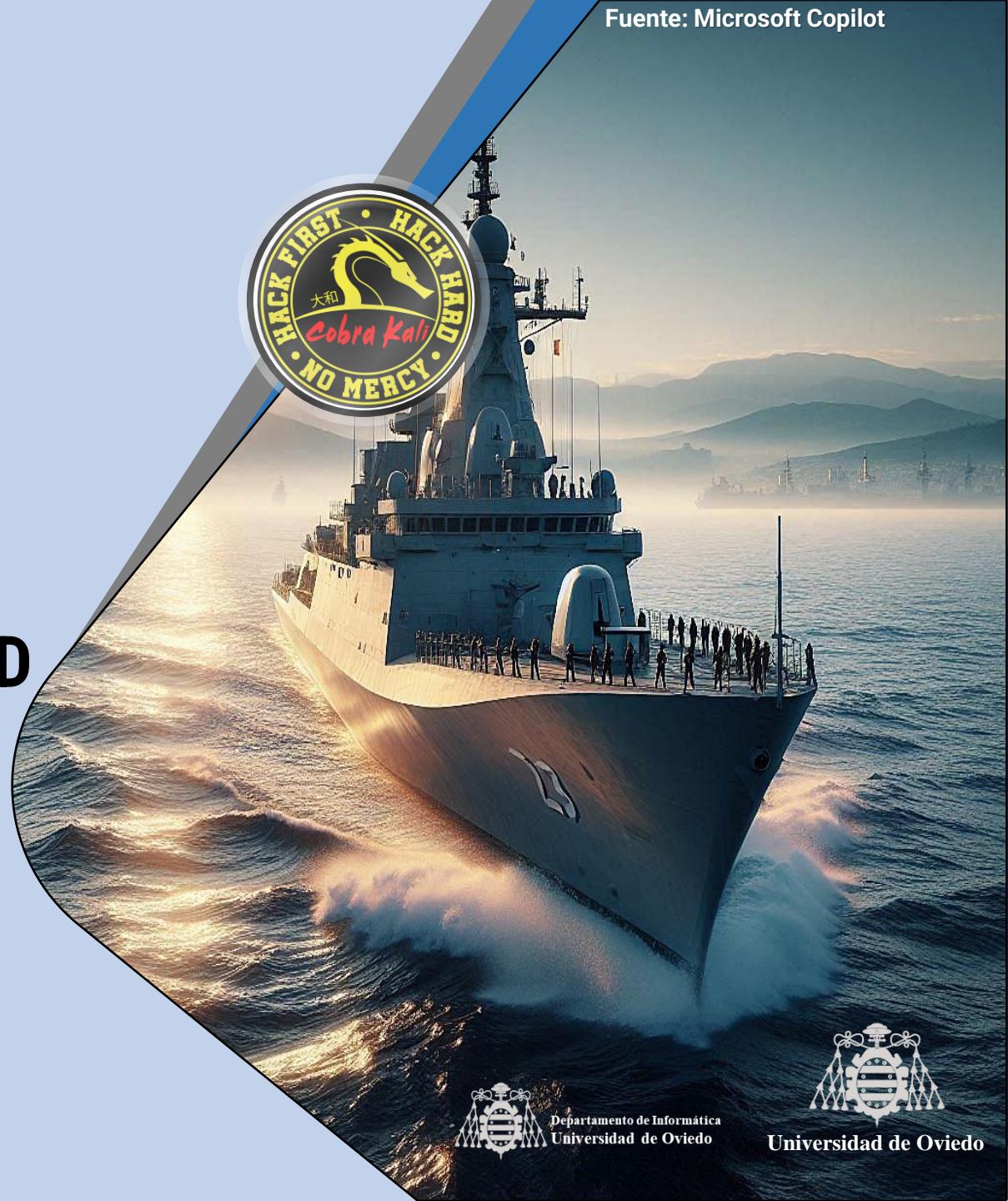
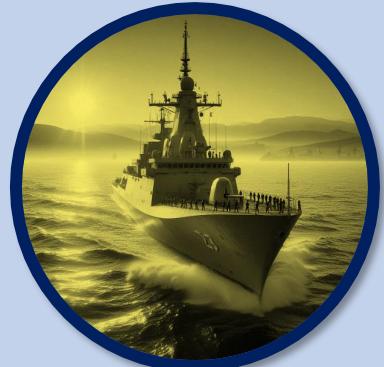
Nmap

< Ir al Índice



NMAP, EL DETECTIVE DE LA RED

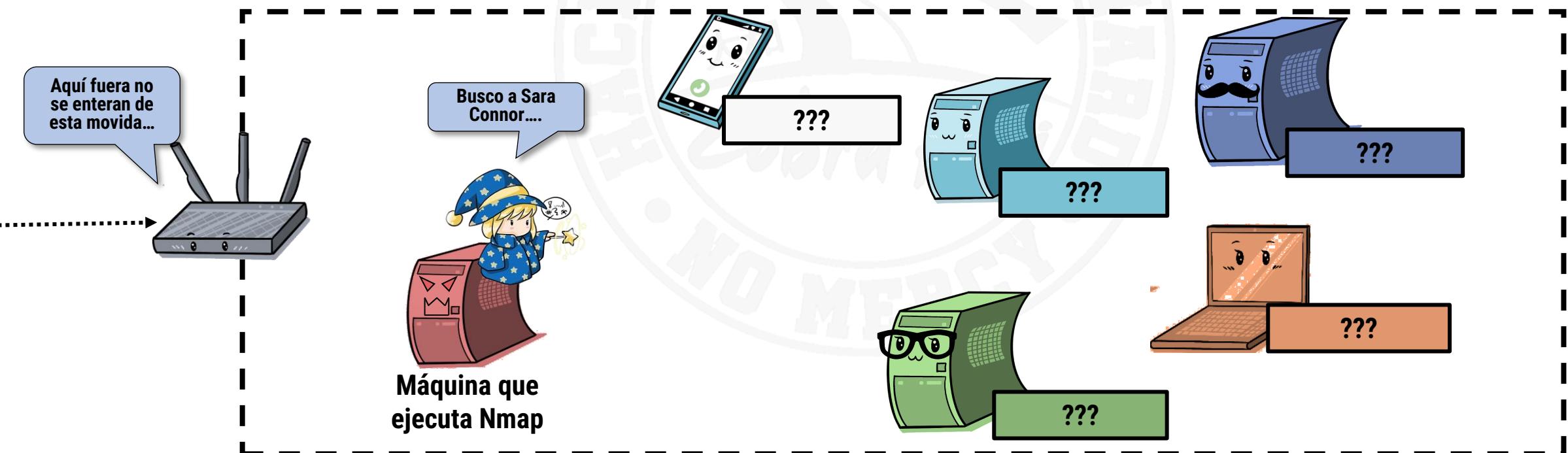
¡El Sherlock Holmes de las ondas!



NMAP POWER: LA ESPÍA QUE ME MAPEO

- Nmap es una herramienta que se usa fundamentalmente para preguntar

- Aunque tiene otros muchos 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



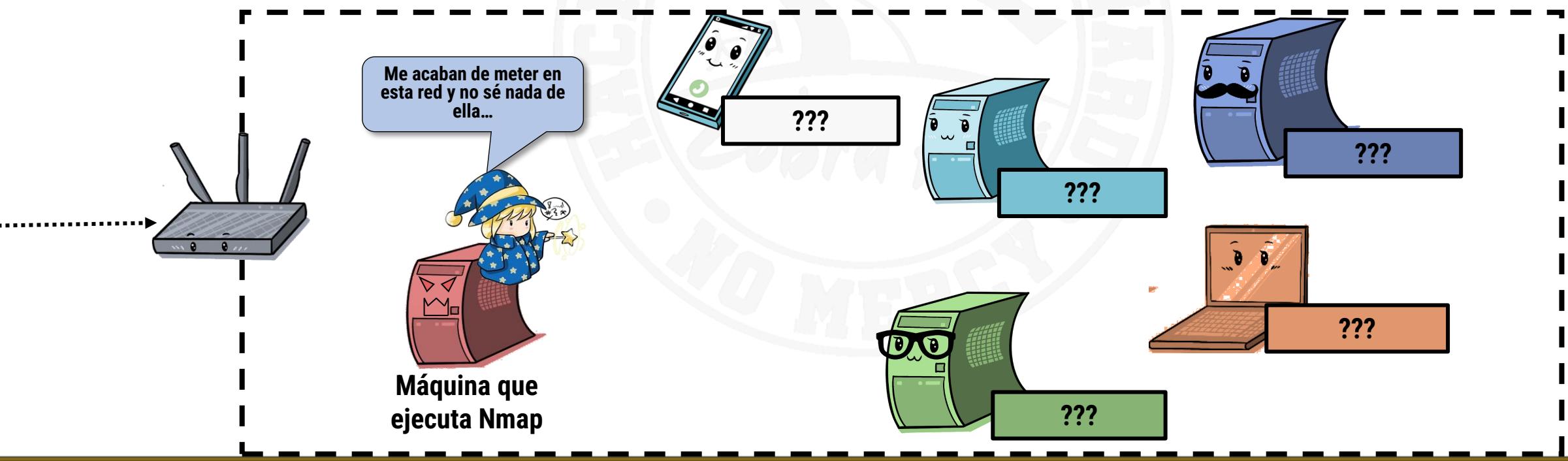
NMAP POWER: LA ESPÍA QUE ME MAPEO

• *¿Pero eso no lo sé de antemano?*

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

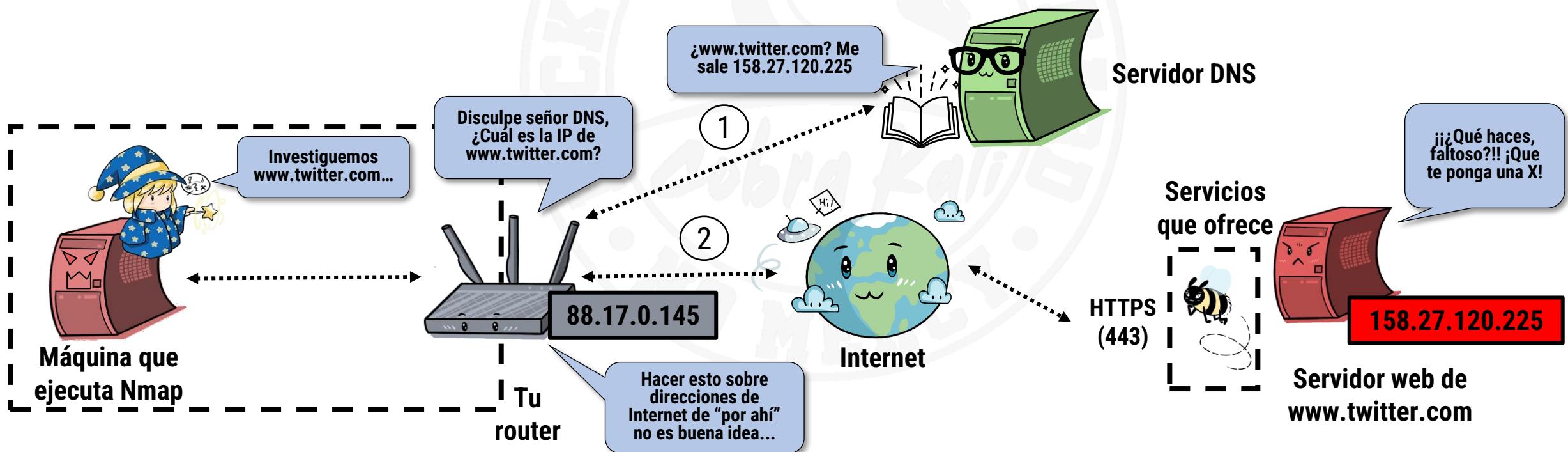
• **Voy a enseñarte varios usos de nmap que llevan parámetros**

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



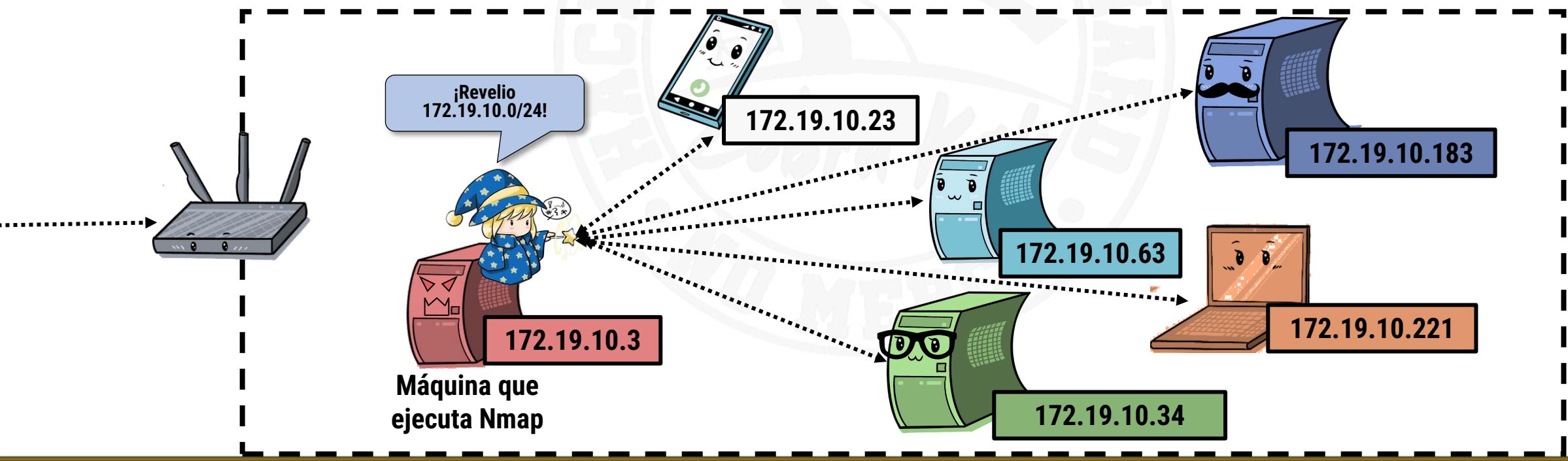
NMAP POWER: LA ESPÍA QUE ME MAPEO

- 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!
 - No se debe hacer sin autorización de la otra parte
- Para probar puedes intentarlo sobre scanme.nmap.org



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

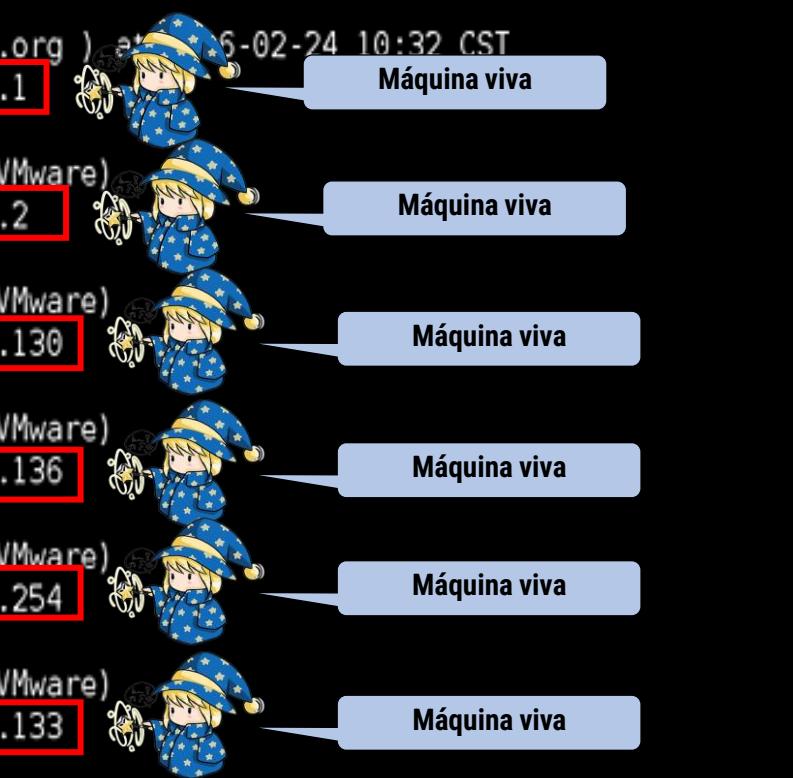
- **¿El qué exactamente?**

- ¡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
```



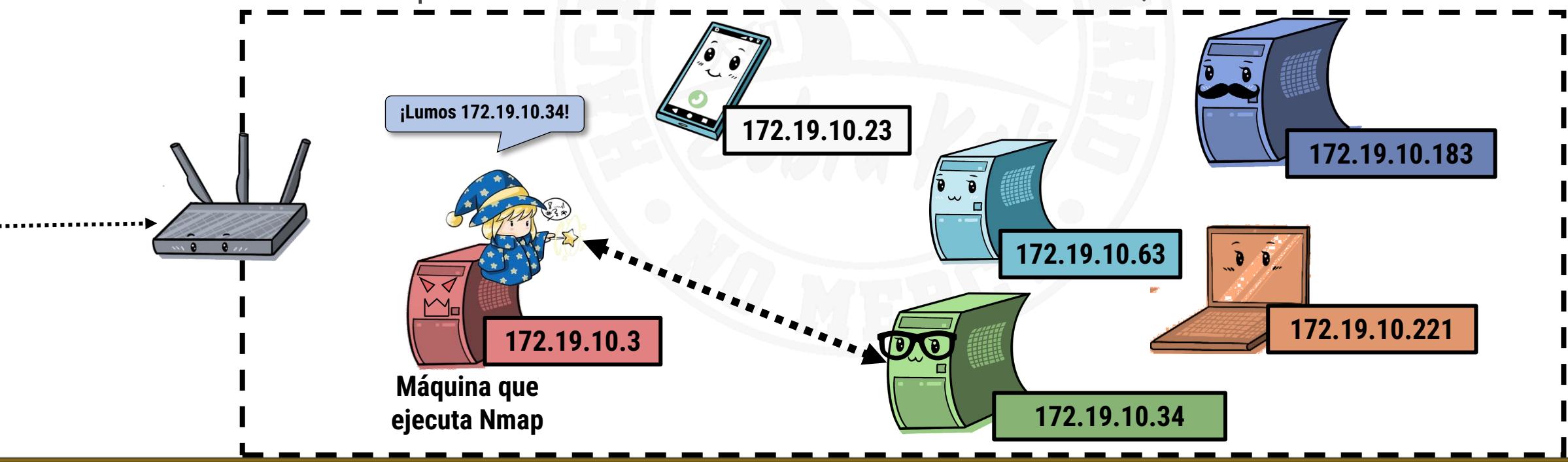
NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿TÚ QUÉ “VENDES”?

- 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

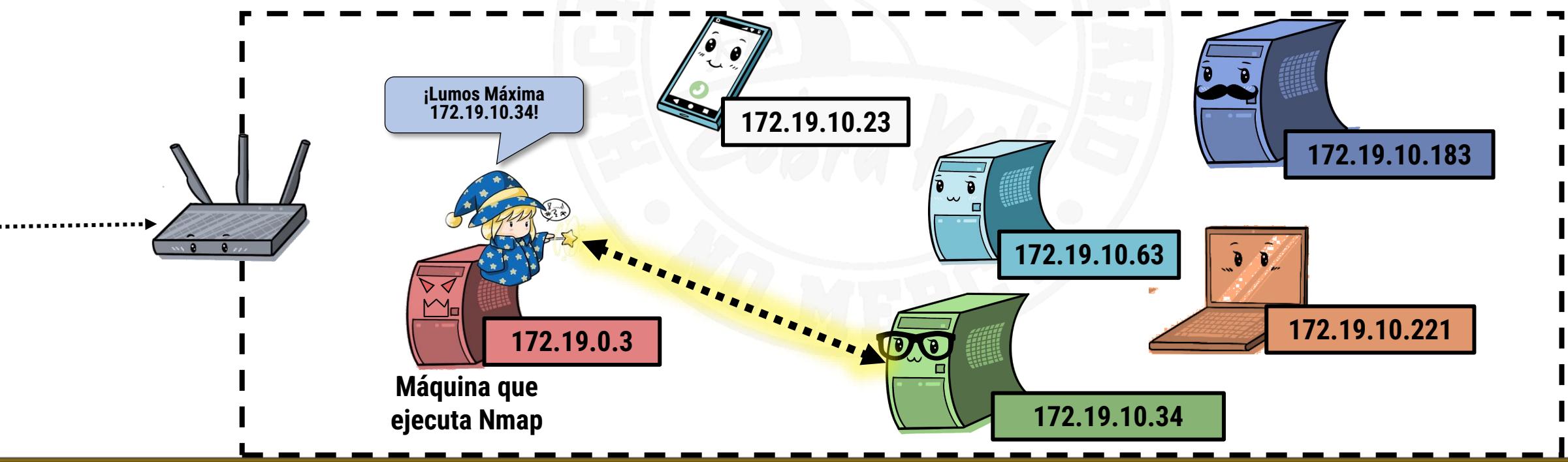
NMAP POWER: LA ESPÍA QUE ME MAPEO. ¿TU QUÉ “VENDES”?

- ¡¡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)  OS: Linux
| 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 los servicios FTP y SSH.

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

Servicio SAMBA (protocolo SMB para compartir archivos de Microsoft, pero su implementación de Linux)

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

El servidor admite el método HTTP TRACE, que puede ser peligroso para algunos navegadores:
<https://www.beyondsecurity.com/scan-pentest-network-vulnerabilities-http-trace-method-xss-vulnerability.html>

Microsoft Remote Procedure Calls (servicio típico de Windows) y soporte de HTTPS

Servicio WinRM (Windows Remote Management): <https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-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) 2019-09-10T19:45:44Z
| 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 50 : Vendors Vendor Cvss Scores Products Product Cvss Scores Versions Other : Microsoft Bulletins Bugtraq 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

OpenBSD >> **OpenSSH** Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending Total number of vulnerabilities : 96 Page : 1 (This Page) 2 Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.	
1	CVE-2000-0525			Exec Code	2000-06-08	2017-10-10	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
2	CVE-2000-0999			+Priv	2000-12-11	2008-09-05	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
3	CVE-2001-0144			Exec Code Overflow	2001-03-12	2018-05-03	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
4	CVE-2002-0083	189		+Priv	2002-03-15	2016-10-18	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
5	CVE-2002-0639			Exec Code Overflow	2002-07-03	2016-10-18	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
6	CVE-2002-0640			Exec Code Overflow	2002-07-03	2016-10-18	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
7	CVE-2003-0693			Exec Code	2003-09-22	2018-05-03	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
8	CVE-2003-0786			+Priv	2003-11-17	2008-09-10	10.0		None	Remote	Low	Not required	Complete	Complete	Complete
9	CVE-2006-5051														
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															
41															
42															
43															
44															
45															
46															
47															
48															
49															
50															

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

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

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 Ubuntu
l 2.0.0~
| 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	Version Details Vulnerabilities
8.5	*	-	*	1	Version Details Vulnerabilities
8.4	*	-	*	1	Version Details Vulnerabilities
8.3	*	-	*	1	Version Details Vulnerabilities
8.3	*	P1	*	1	Version Details Vulnerabilities
8.2	*	*	*		
7.9					
7.7		P1			
7.7					
7.6		P1			
7.5					

¡Revelo! 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	Broadcom	Fabric Operating System	-	*	*	*	Version Details	Vulnerabilities
2	Application	Netapp	Active Iq Unified Manager	*	*	*	*	Version Details	Vulnerabilities
3	Hardware	Netapp	Hci Compute Node	-	*	*	*	Version Details	Vulnerabilities
4	Application	Netapp	Hci Management Node	-	*	*	*	Version Details	Vulnerabilities
5	Hardware	Netapp	Hci Storage Node	-	*	*	*	Version Details	Vulnerabilities
6	Application	Netapp	Solidfire	-	*	*	*	Version Details	Vulnerabilities

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 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





José Manuel
Redondo López

EXPLOIT-DB

- <<Próximamente>>





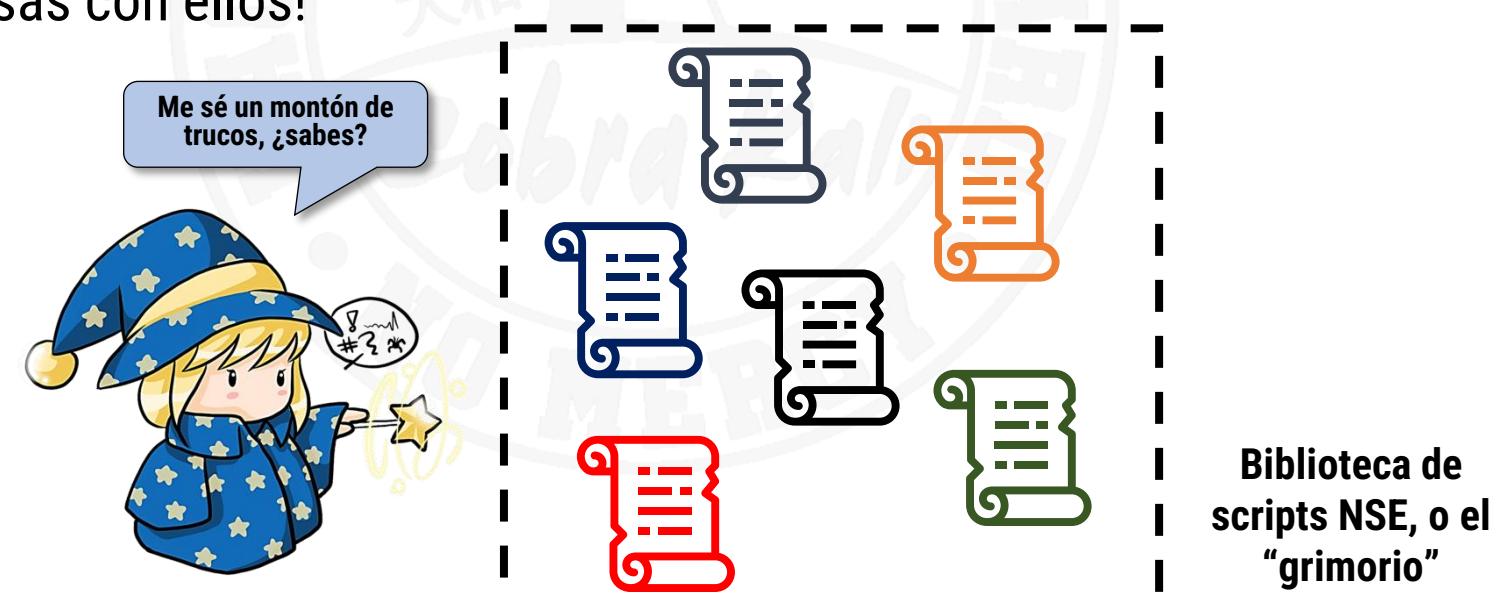
  “Serious” Nmap 😊

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!



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

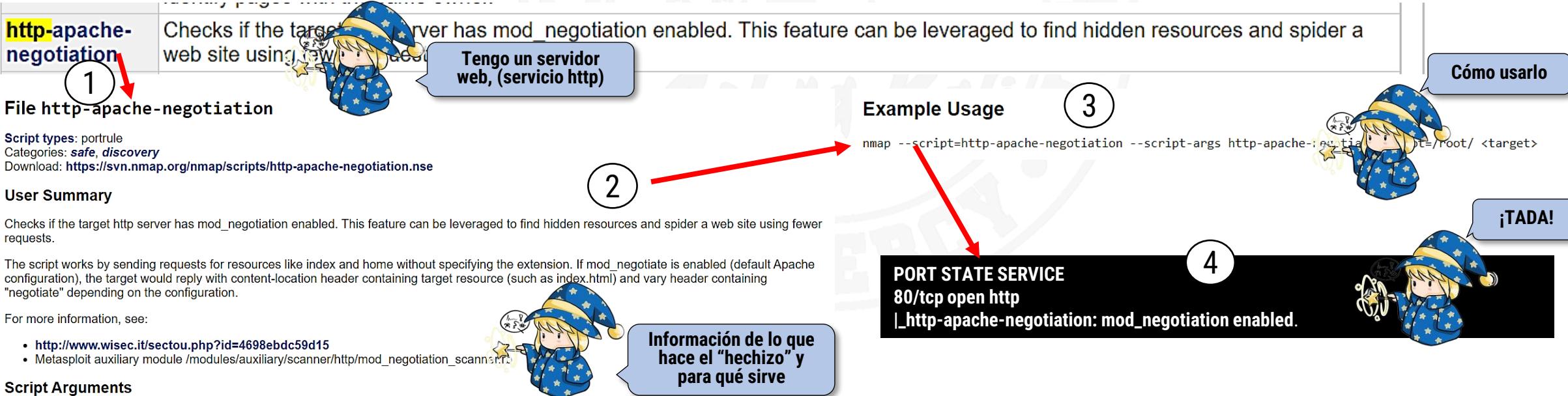
See the documentation for the unpwdb library.

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?
 - 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 ☺



The screenshot shows the Nmap Script Database interface. At the top, there's a search bar and a navigation menu. Below it, a list of scripts is displayed.

File http-apache-negotiation (1)

Tengo un servidor web, (servicio http)

Cómo usarlo

Example Usage (3)

```
nmap --script=http-apache-negotiation --script-args http-apache-negotiation=mod_negotiation <target>
```

PORT STATE SERVICE (4)

80/tcp open http
|_http-apache-negotiation: mod_negotiation enabled.

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

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.

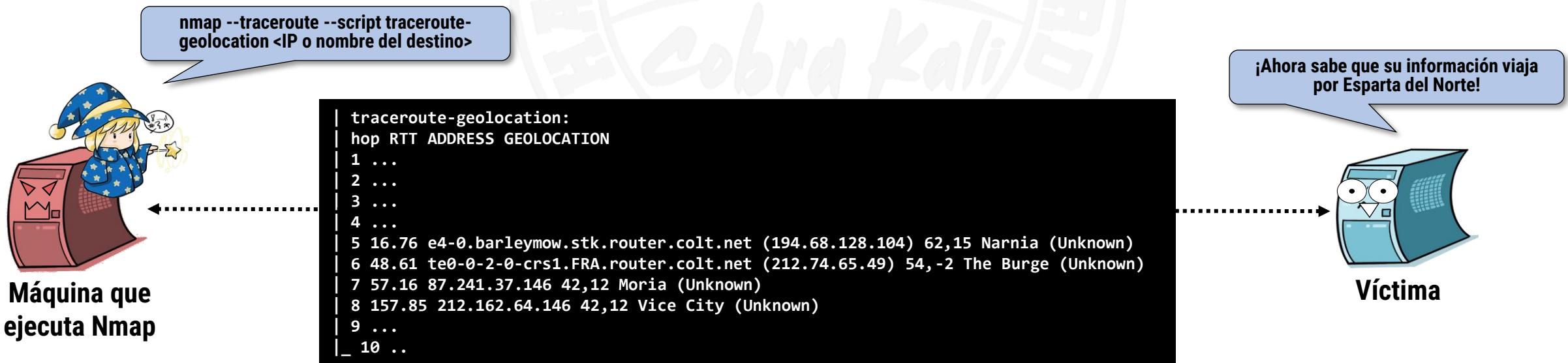
For more information, see:

- <http://www.wisec.it/sectou.php?id=4698ebdc59d15>
- Metasploit auxiliary module /modules/auxiliary/scanner/http/mod_negotiation_scanner

Script Arguments

NMAPSTER CHEF: COCINANDO CON SCRIPTS

- 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...



- <<Próximamente>>



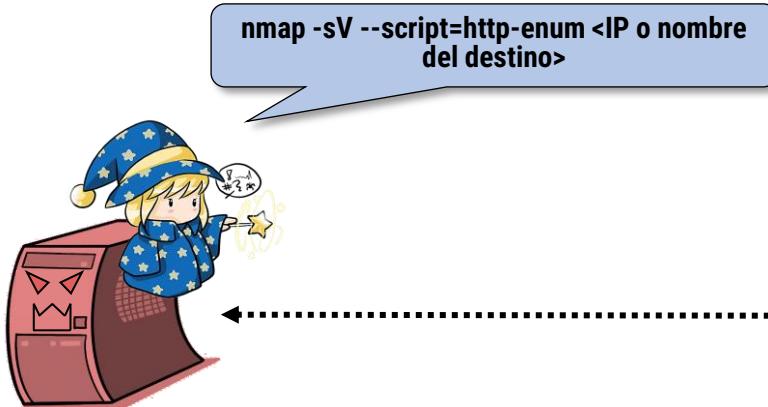
NMAPSTER CHEF: COCINANDO CON SCRIPTS

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



NMAPSTER CHEF: COCINANDO CON SCRIPTS

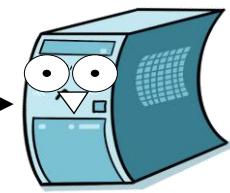
- El script **http-enum** tiene una lista de rutas comunes que suele haber en cualquier web (/admin, /login...) y las prueba todas
- Meca, ¿Y eso para qué?
 - Porque si alguna de ellas es una dirección “oculta” (no hay un enlace que va hacia ella) ¡la descubrirá!



nmap -sV --script=http-enum <IP o nombre del destino>

```
...
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/:
...
...
```

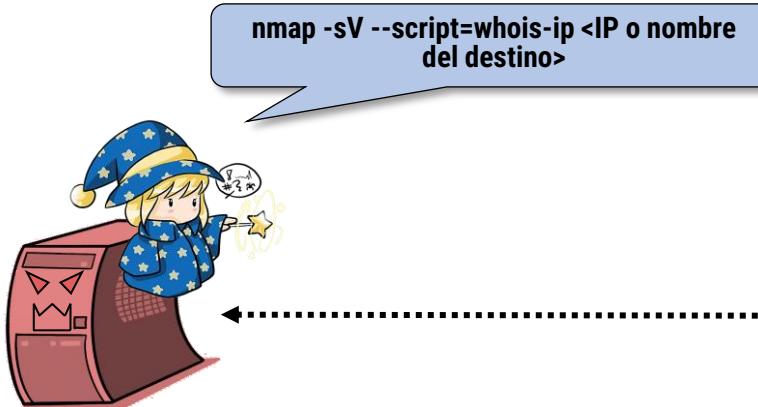
¡Tenía una web /tarjetas_black y me la han descubierto!



Víctima

NMAPSTER CHEF: COCINANDO CON SCRIPTS

- 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**
 - O bien tu proveedor de hosting **dará la suya por ti**



Máquina que ejecuta Nmap

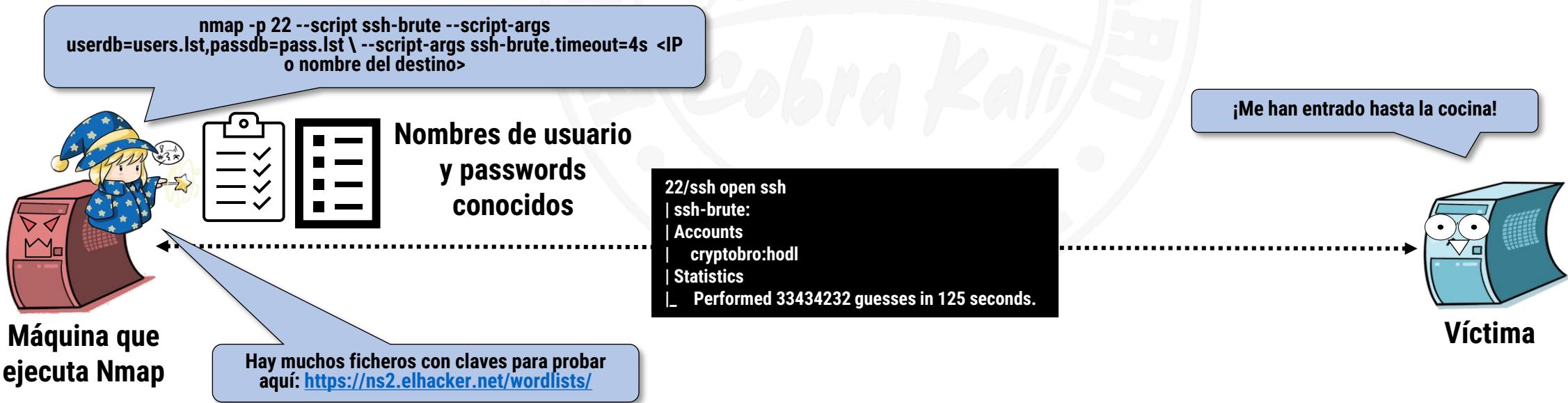
Host script results:
| whois-ip: Record found at whois.arin.net
| netrange: 64.13.134.0 - 64.13.134.63
| netname: NET-64-13-143-0-26
| orgname: Rude Gotenks Networks
| orgid: WREX
| _country: US stateprov: CA



Víctima

NMAPSTER CHEF: COCINANDO CON SCRIPTS

- 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: COCINANDO CON SCRIPTS

- ¿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>)
 - Y hay que instalarlo aparte, como dice en su web...



vulnersCom / nmap-vulners (Public)

Code Issues 13 Pull requests 1 Actions Projects Wiki Security Insights

master 1 branch 7 tags Go to file Add file Code

File	Description	Last Commit
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: COCINANDO CON SCRIPTS

```
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.lab08_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-OPENSHELL-CVE-2020-14145/ 4.3      https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSHELL-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!



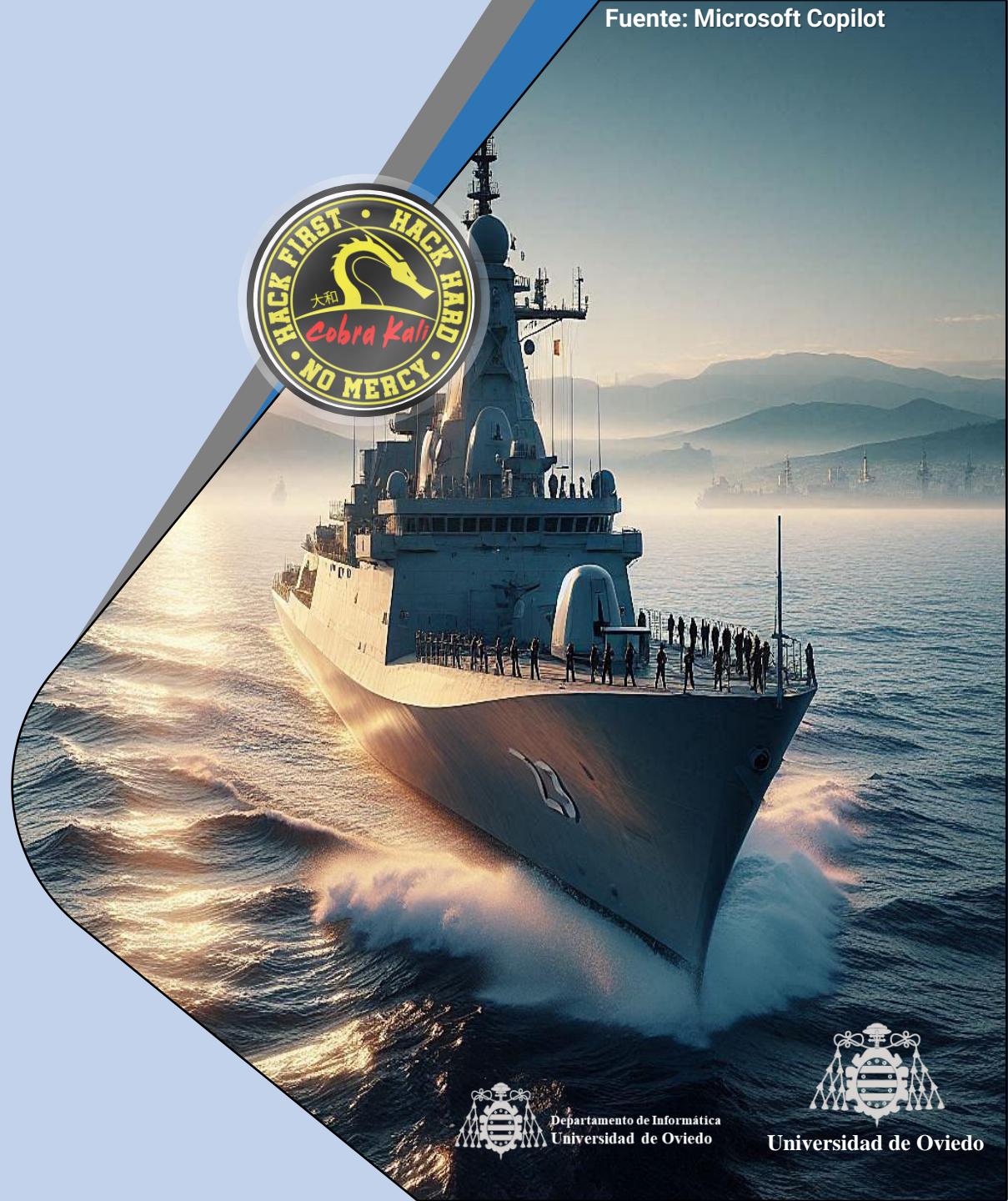
¡Sectumsempra!



< Ir al Índice

SHODAN GO ON!

El buscador de máquinas de todo tipo por Internet



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo



José Manuel
Redondo López

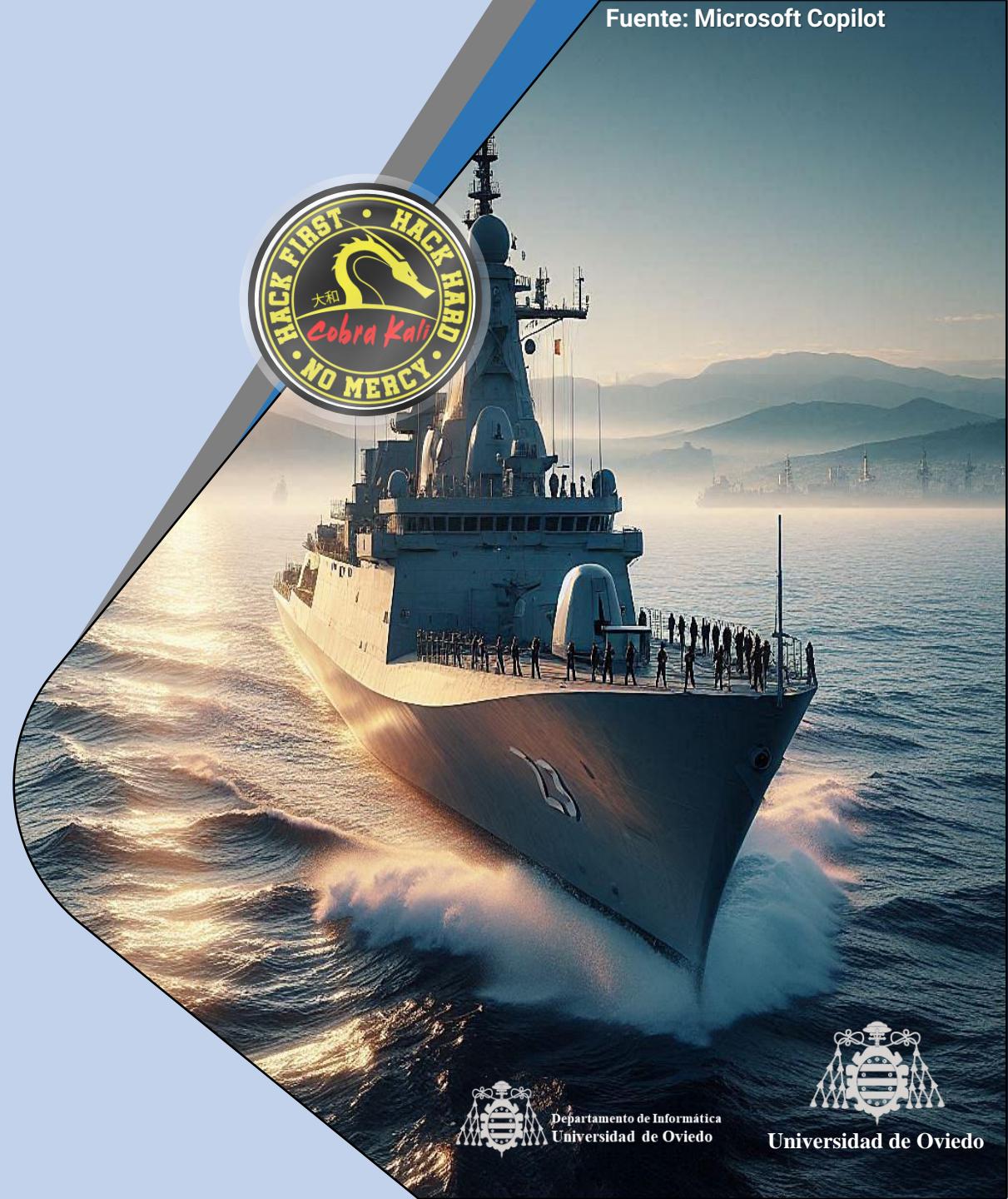
- <<Próximamente>>



< Ir al Índice

ESCANEADORES DE VULNERABILIDADES

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



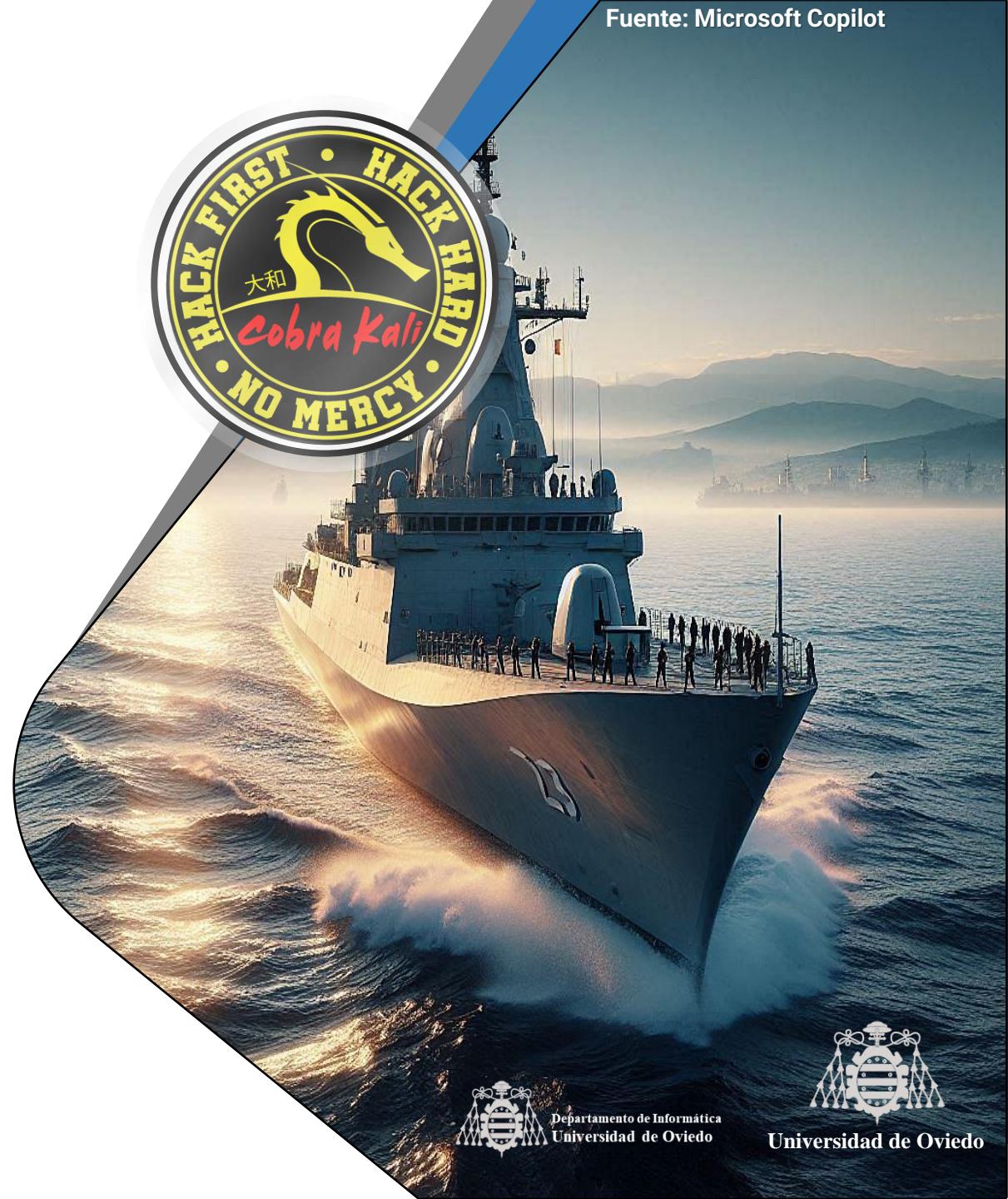


José Manuel
Redondo López

- <<Próximamente>>



VIGILANDO LAS REDES: ATAQUE



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo