TEMA 1
INTRODUCCIÓN

"Este mundo no necesita héroes, necesita profesionales"

JOSÉ MANUEL REDONDO LÓPEZ PROYECTO *"S-81 ISAAC PERAL"* V4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo
Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

ÍNDICE

< Ir al Índice

CÓDIGO ÉTICO

Los hackers NO son criminales, así que tienes que tener un código ético

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Código ético

- **Vamos a describir varias técnicas y herramientas reales de pentesting**
  - Usarlos contra objetivos sin autorización previa **ES UN DELITO**
  - El mal uso de algunas de ellas puede hacer mucho daño o deshabilitar un objetivo
- **DEBES cumplir con este código ético**
  - Convertirse en un criminal tarde o temprano arruinará tu vida y la de los demás
    - Siempre habrá alguien que sepa más que tú que te podría "cazar"
    - Puedes dejar a familias enteras sin ningún tipo de ingreso (**NO es gracioso**)
    - Incluso puedes matar indirectamente a las personas (**es un delito grave**)
      - ¿No me crees? Busca "ransomware en hospitales" o sitios similares...
  - Proteger a otros contra ciberdelincuentes es una forma de obtener un trabajo bien remunerado
    - **Pero para eso, necesitas saber cómo trabajan**
    - Esa es la razón por la que enseñamos ciertas cosas
  - **Tu elección, tu responsabilidad, tu vida**

CÓDIGO ÉTICO

- **CUALQUIER uso no autorizado de cualquiera de estas herramientas y técnicas significa que estás cometiendo un delito**
  - Y que las probabilidades de ser "cazado" son muy altas
- Usa SIEMPRE estas técnicas contra objetivos autorizados
  - **Porque has sido contratado** para evaluar la seguridad de algunos sistemas (es su trabajo)
  - Porque estás en una plataforma legal de **entrenamiento en ciberseguridad** (es tu “campo de pruebas")
  - Porque es un sistema que **creaste tú** para entrenar (es tu “campo de pruebas" privado)
    - Típicamente llamados "laboratorios de pentesting" (también puedes encontrarlos preconstruidos)
- SIEMPRE aplica estas técnicas siguiendo las reglas / límites establecidos
  - Por el **contrato** que firmaste (es tu trabajo)
  - Según las reglas de la **plataforma** que estás utilizando (sin DoS ...) (es tu "patio de recreo" legal)
  - Por la **capacidad** (recursos) de tu infraestructura (es tu "patio de recreo" privado legal)

Código ético

- **Algunas de estas técnicas son puramente para hacer intrusiones**
  - Web shells, escalado de privilegios, características de Metasploit...
- **Se pueden usar para evaluar la gravedad de una vulnerabilidad**
  - Pero también, **en concursos de hacking y CTF** o webs de “entrenamiento legal en hacking"
    - Hack the Box, Try to Hack me…
    - **¡Esa es la razón por la que explicamos estas técnicas!**
    - Se gana obteniendo información o datos ("banderas“ o “flags”) explotando vulnerabilidades
    - Y también son un **recurso de aprendizaje muy útil**
  - Al prepararte para ser capaz de enfrentar los desafíos típicos de CTF...
    - Estamos creando una “base” por si sigues aprendiendo ciberseguridad (si le gusta este mundo)
    - Pero incluso si no te gusta, **podrás ser mucho mejor ingeniero de software**
    - Tus aplicaciones tienen menos probabilidades de ser "asaltadas" ☺

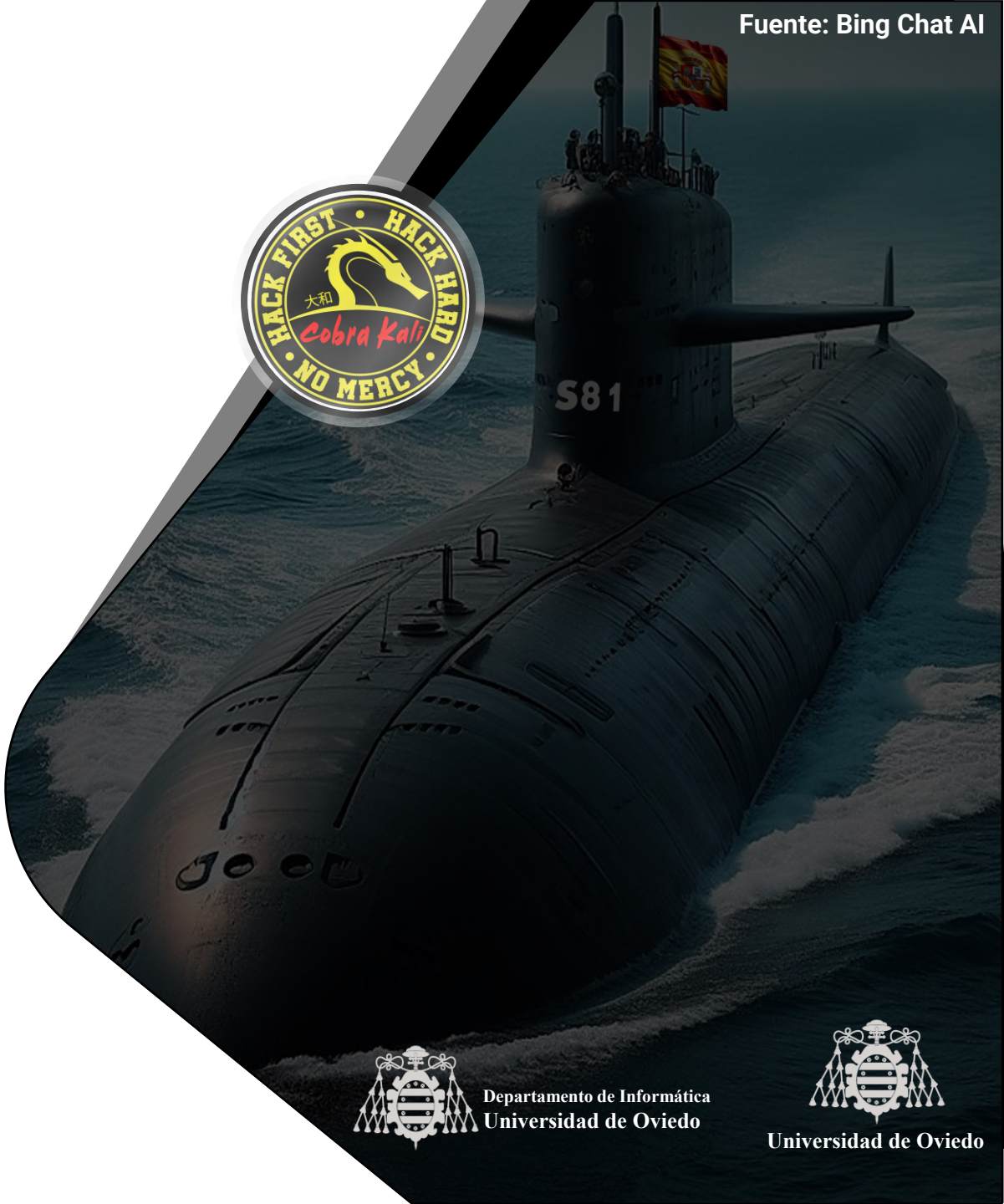
< Ir al Índice

INTRODUCCIÓN

¡Viento en popa, a toda vela! ☺

*Iconos por Bing Chat AI

Fuente: Bing Chat AI



Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Introducción: Objetivos de aprendizaje

- **Lo que pretendemos es que puedas hacer lo siguiente sobre los sistemas informáticos que manejes**
  1. Conocer diferentes conceptos relacionados con su seguridad
  2. Identificar los **riesgos** que pueden comprometer su seguridad
  3. Conocer las **vulnerabilidades**, **amenazas**, **técnicas de ataque** y otras cosas involucradas en la seguridad de los mismos
  4. Identificar diferentes tipos de **daño** que se les pueda causar

SEGURIDAD DE SISTEMAS INFORMÁTICOS

- Un sistema informático es **seguro** cuando responde según lo previsto
  - Permite a cada usuario legítimo realizar todas las operaciones para las que está autorizado
  - Evita que los usuarios realicen operaciones para las que no tienen autorización
- Además, también **garantiza a los usuarios legítimos tres cosas**
  - **Confidencialidad**: Los datos privados solo son **visibles** para sus legítimos propietarios
  - **Integridad**: Los datos solo pueden ser **modificados** por sus legítimos propietarios
  - **Disponibilidad**: Los datos son siempre **accesibles** para sus legítimos propietarios
- Por lo tanto, los **objetivos de la seguridad de los sistemas informáticos** son
  - **Identificar vulnerabilidades** que pueda tener un sistema informático
  - Crear y hacer funcionar **contramedidas** contra ellos
  - **Evitar amenazas existentes** que **aprovechan** (**exploit**) estas vulnerabilidades

SEGURIDAD DE SISTEMAS INFORMÁTICOS

- **Esto implica**
  - Estudiar posibles **amenazas**, **riesgos**...
  - Mejorar la seguridad de los sistemas informáticos (**hardening**)
  - Diseñar **políticas de gestión de seguridad** para sistemas de información (SGSI)
  - **Hacking ético**, **pentesting** y **análisis forense** informático
- **Debido a ello, esta asignatura está relacionada con otras muchas**
  - Omite varios temas de administración de sistemas y se centra sólo en los de seguridad
    - Nuestra "asignatura hermana", Administración de Sistemas y Redes (ASR) trata de eso
  - Se saltará la ciencia forense
    - La asignatura optativa Informática Forense y Auditoría (IFA) trata de eso
  - Solo mencionará la gestión de riesgos
    - La asignatura de Gestión de Proyectos (4º año) (DPPI) trata de eso
  - Solo mencionará temas relacionados con la ley
    - La asignatura Aspectos Sociales, Legales, Éticos y Profesionales de la Ing. (ASLEPI) (4º año) tratarán eso
  - No se centrará en la seguridad web, solo en sus fundamentos
    - Las asignaturas de la iniciativa "Cobra Kali" del Máster en Ingeniería Web (MIW) tratarán eso

ATAQUES CONTRA LA CONFIDENCIALIDAD

- **Acceso no autorizado al sistema (suplantación)**
  - Acceso a datos restringidos (archivos, información privada...)
  - Acceso a software restringido (productos con licencia, software personalizado...)
- **Acceso a la comunicación no autorizado (sniffing)**
  - Acceso a los datos que el objetivo envía y/o recibe
  - Mensajes, archivos, información privada...
- **Acceso físico a un ordenador (instalación de malware, robo de datos...)**
  - O un dispositivo de almacenamiento (robar datos o el propio dispositivo)
- **Acceso lógico o físico a copias de seguridad de datos/software**
- **Acceso a datos / software restringido o privado**
  - Mediante técnicas de **ingeniería social**
  - A través de **malware** o **escalada de privilegios**

ATAQUES CONTRA LA INTEGRIDAD

- **Los mismos ataques que contra la confidencialidad**
  - Pero **no se limitan a solo acceder a la información / software**
- **Una vez que se logra el acceso no autorizado, los atacantes pueden**
  - Introducir datos / software **falsos o maliciosos**
  - **Dañar o corromper** los datos / software (versiones troyanizadas)
  - **Modificar** los datos / software para lograr otros efectos no deseados
    - Denegación de servicio, aumento del consumo de recursos, propagación de información falsa, alteración de las operaciones de la empresa...
- **Comprometer la integridad en los canales de comunicación generalmente se hace mediante ataques Attacker-in-the-Middle (AitM)**
  - Anteriormente llamados "Man-in-the-Middle" (MitM)

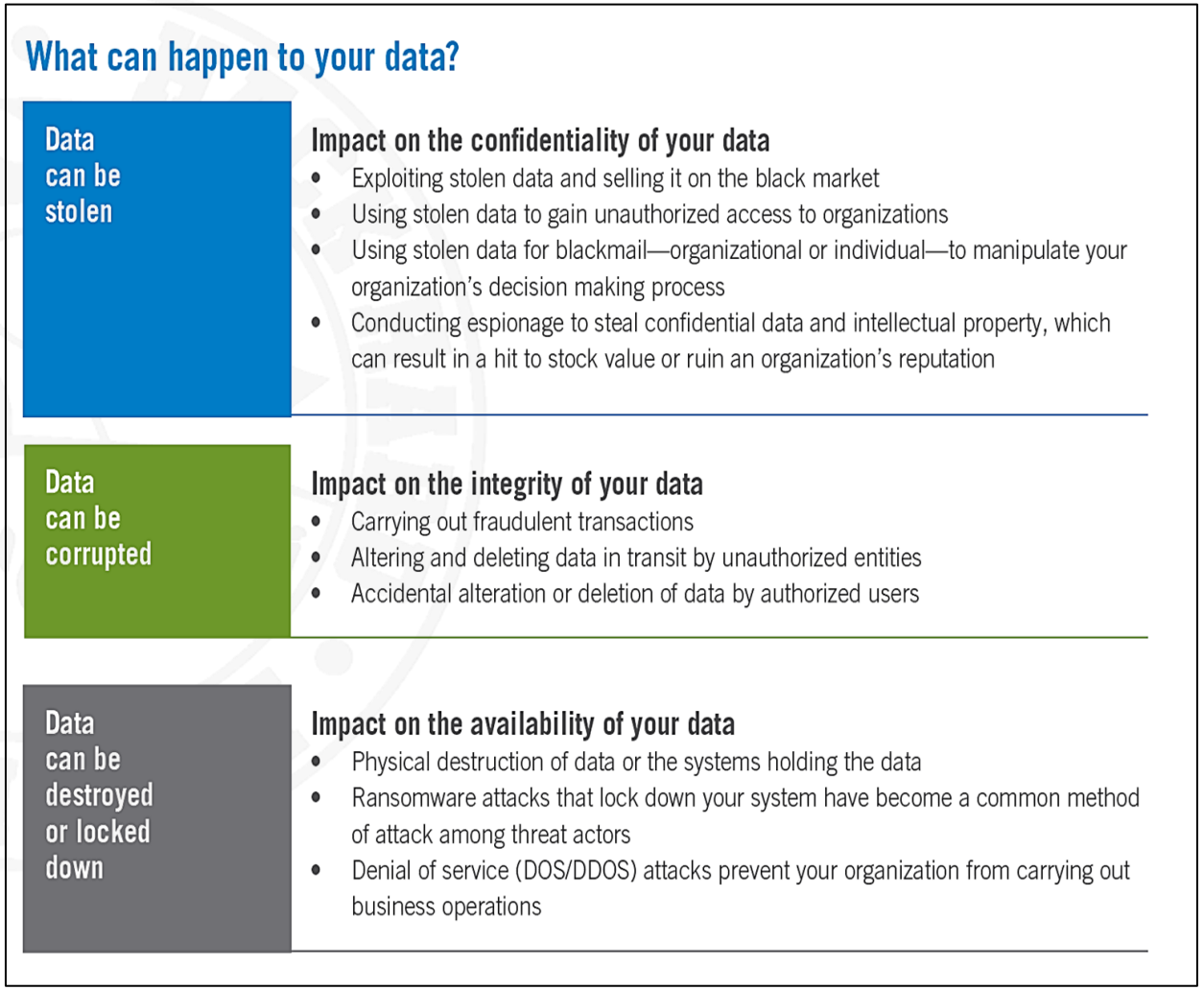
ATAQUES CONTRA LA DISPONIBILIDAD

- Toda forma de ataque que tienen como objetivo **negar o reducir la capacidad** de un sistema informático para dar un determinado servicio o conjunto de servicios
  - **Saturación** usando ciertos tipos de malware (reduciendo sustancialmente el rendimiento)
  - **Dejar al sistema sin recursos** con variantes de ataques DoS (denegación de servicio) o DDoS (DoS distribuido)
  - **Eliminar o dañar deliberadamente el hardware existente**, incluido el hardware de comunicación
  - **Apagar el sistema** o alguno de sus periféricos importantes

¡LOS DATOS SON OBJETIVO!

- Como puedes ver, hay muchas cosas que pueden pasarle a los datos
- Además de con medidas de seguridad, la forma de evitar perder datos críticos son las **copias de seguridad**
  - **Copia a menudo** y en dispositivos externos
  - Lo ideal es tener **más de uno** (rotar copias de seguridad)
  - Más ideal aún es que **al menos uno debe estar en un lugar diferente**
    - Dropbox, OneDrive... pueden ayudar
  - **¡Comprueba que puedes restaurar las copias cuando las hagas!**
- Detalles y políticas de backup (Windows / Linux) se ven en ASR

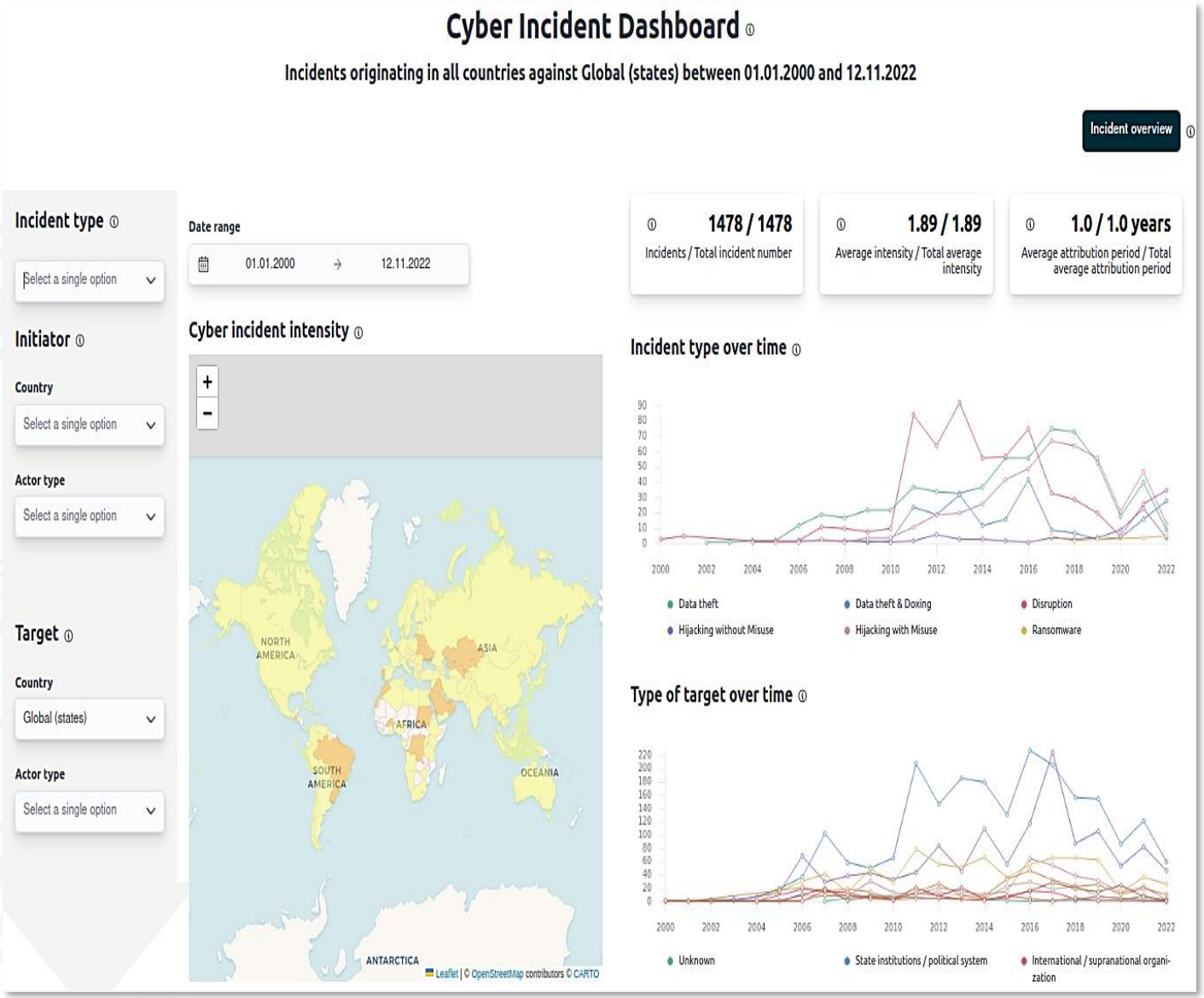
Fuente: https://www.cybervista.net/what-every-executive-really-needs-to-know-about-cyber-part-1/



LA SEGURIDAD, HOY

Seguridad de Sistemas Informáticos

- **Los perfiles relacionados con la ciberseguridad tienen una gran demanda**
  - https://cso.computerworld.es/ciberseguridad/cuales-son-los-perfiles-mas-buscados-en-los-departamentos-de-seguridad
- **Porque los ataques son constantes en todo el mundo**
  - https://cybermap.kaspersky.com/
  - Ejemplos hay en las noticias a diario...
- **Evolucionan con la actualidad**
  - Por ejemplo, la pandemia ha aumentado considerablemente los ataques de escritorio remoto (RDP)
  - Y ransomware...

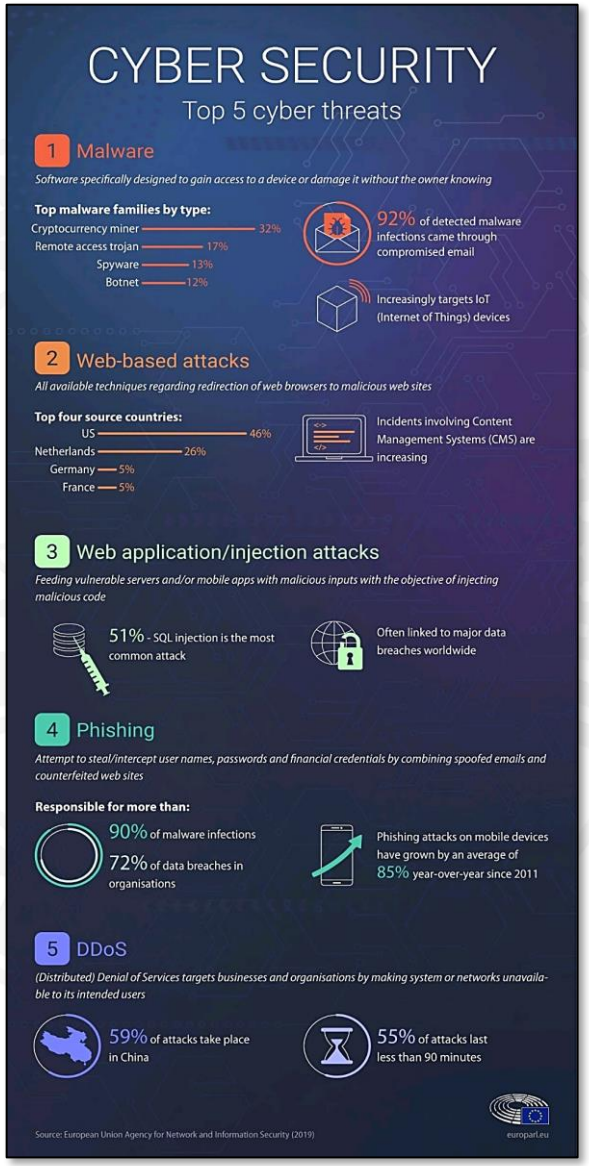


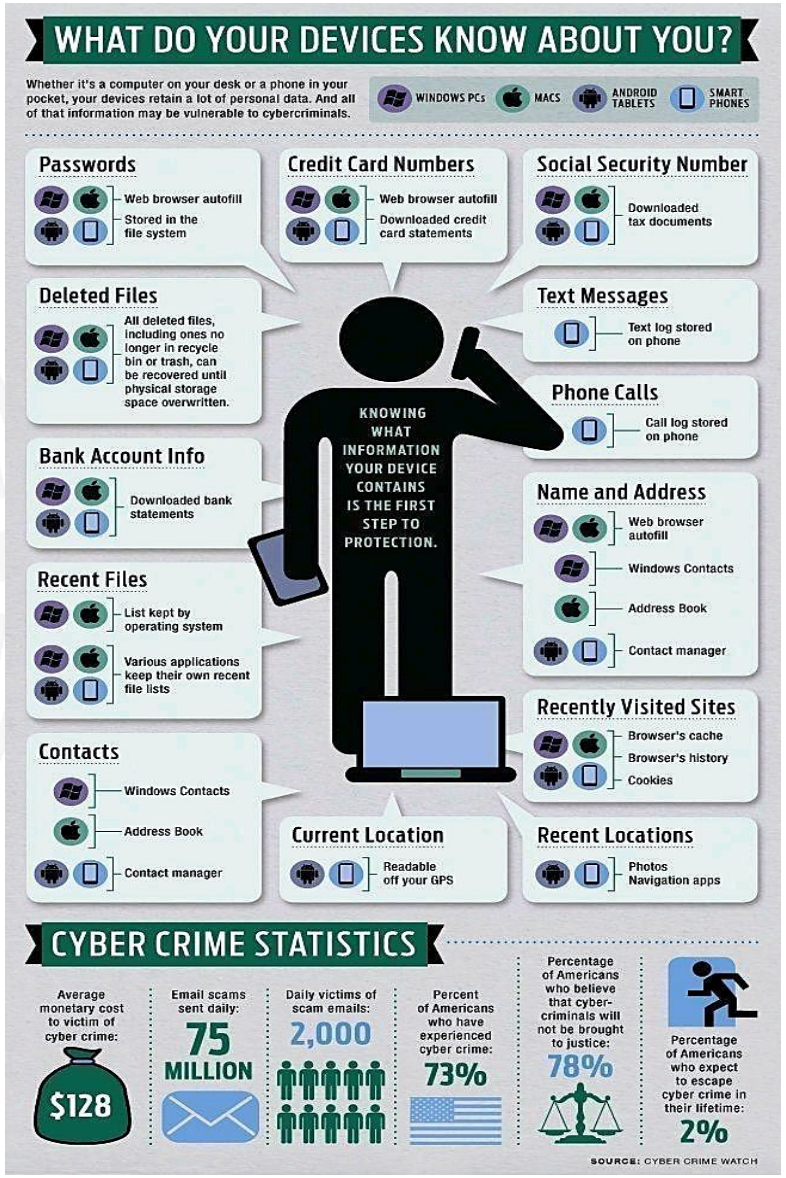
Fuente: https://eurepoc.eu/dashboard

La seguridad, hoy

Fuente: https://m.facebook.com/comptechcyber/posts/ **Fuente:** https://www.cybercrimeswatch.com/

- Algunos tipos de ataques son más frecuentes que otros
- El acceso a dispositivos individuales es ahora mucho más rentable para los delincuentes que hace años
- Por lo tanto, el **malware** y el **phishing** están ganando importancia a la hora de robar información privada de usuarios
  - Normalmente asociados con técnicas **OSINT** (Open-Source INTelligence) contra usuarios





El mundo de la seguridad desde una perspectiva de "novato"

- Sabemos que la mayoría de vosotros no tenéis experiencia en seguridad
- También sabemos que mucha gente cree que este mundo es algo difícil e inalcanzable

¡NO ES VERDAD!

- Vamos a abordarlo desde una aproximación de "conocimiento cero"
  - Primero os explicaremos las bases que necesitamos
  - Y más adelante, exploraremos temas cada vez más avanzados
  - Al final, podrás **defender tus sistemas** y **comprobar su seguridad** de forma solvente
- Comencemos con **algunos conceptos básicos**

< Ir al Índice

Tipos de Malware >

Fuente: Bing Chat AI

TERMINOLOGÍA BÁSICA

Entendiendo conceptos básicos y “palabros” ☺

*Iconos por Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Qué es un **CVE** y lo que representa
- Que es el **CVSS**
- Los conceptos de **riesgo**, **ataque** y **daño**
- Qué es un **control de seguridad**
- Qué tipo de **atacantes** hay
- Qué tipo de **equipos de seguridad** hay
- Distintos **tipos de malware** y lo que hacen

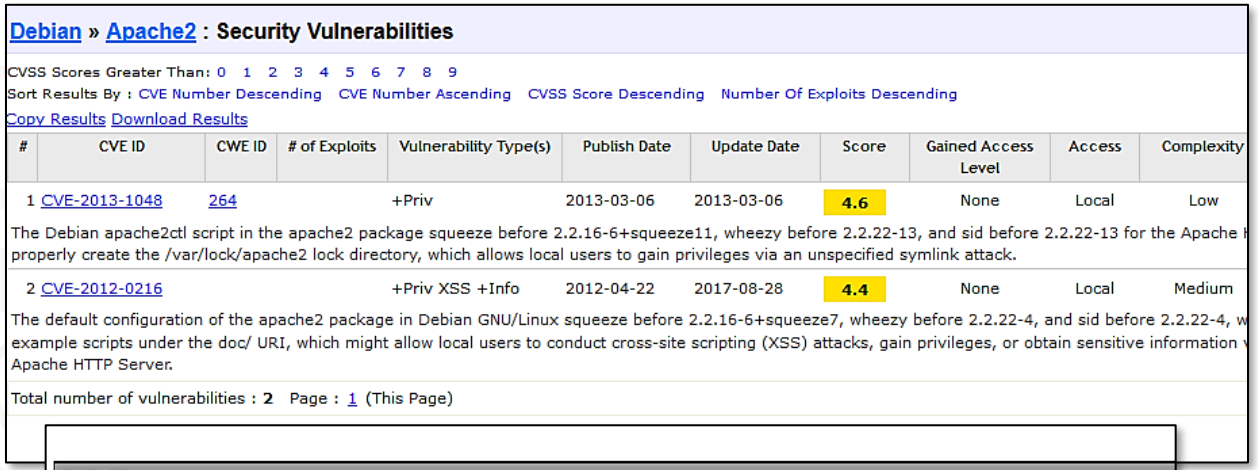
TERMINOLOGÍA BÁSICA

- **Amenaza**: elementos que suponen cualquier clase de peligro para los sistemas
  - **Personas** (usuario legítimo o no legítimo)
  - **Software** (malware)
  - Una **catástrofe natural** (inundación, incendio...) (seguridad física, **Seminario 2**)
  - Posibles factores que aprovechan las vulnerabilidades
- **Vulnerabilidad**: partes del sistema (o aplicaciones) que pueden ser atacadas
  - Son los **puntos más débiles de un sistema**, muy probablemente elegidos para iniciar ataques
  - El **payload** es el código que realiza la acción maliciosa de un ataque
- **Exploit**: Técnicas o código que permiten aprovechar una vulnerabilidad
  - Para lanzar ataques de diferentes tipos
  - Estos ataques pueden detener parte de los servicios del sistema, comprometer su funcionalidad, alterar el comportamiento de alguna parte del sistema, corromper/robar datos...

Common Vulnerabilities and Exposures (CVE)

- Información de vulnerabilidades de seguridad conocidas públicamente de cualquier **software**
- La BD completa de CVE conocidos de la mayoría de los productos es **accesible de forma gratuita**
  - https://cve.mitre.org/
  - https://www.cvedetails.com/
  - …
- Permite buscar y obtener detalles de cualquier vulnerabilidad de software conocida, clasificada por su versión
  - La mantiene MITRE Corporation
  - Con financiación de la División Nacional de Seguridad Cibernética de EE.UU

Fuente: https://www.cvedetails.com/vulnerability-list/vendor_id-23/product_id-22264/Debian-Apache2.html



Debian » Apache2 : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

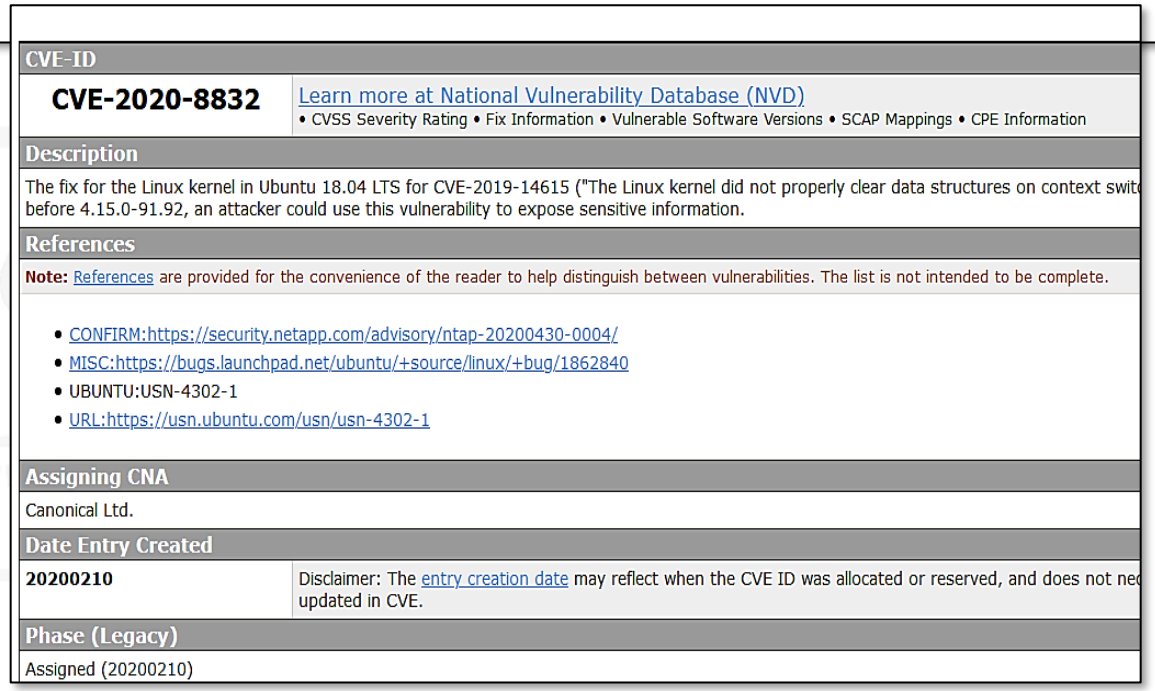
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2013-1048	264		+Priv	2013-03-06	2013-03-06	4.6	None	Local	Low

The Debian apache2ctl script in the apache2 package squeeze before 2.2.16-6+squeeze11, wheezy before 2.2.22-13, and sid before 2.2.22-13 for the Apache H properly create the /var/lock/apache2 lock directory, which allows local users to gain privileges via an unspecified symlink attack.

2	CVE-2012-0216			+Priv XSS +Info	2012-04-22	2017-08-28	4.4	None	Local	Medium

The default configuration of the apache2 package in Debian GNU/Linux squeeze before 2.2.16-6+squeeze7, wheezy before 2.2.22-4, and sid before 2.2.22-4, w example scripts under the doc/ URI, which might allow local users to conduct cross-site scripting (XSS) attacks, gain privileges, or obtain sensitive information v Apache HTTP Server.

Total number of vulnerabilities : 2 Page : 1 (This Page)



CVE-ID

CVE-2020-8832 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 ("The Linux kernel did not properly clear data structures on context swit before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://security.netapp.com/advisory/ntap-20200430-0004/
- MISC:https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1862840
- UBUNTU:USN-4302-1
- URL:https://usn.ubuntu.com/usn/usn-4302-1

Assigning CNA

Canonical Ltd.

Date Entry Created

20200210 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not ne updated in CVE.

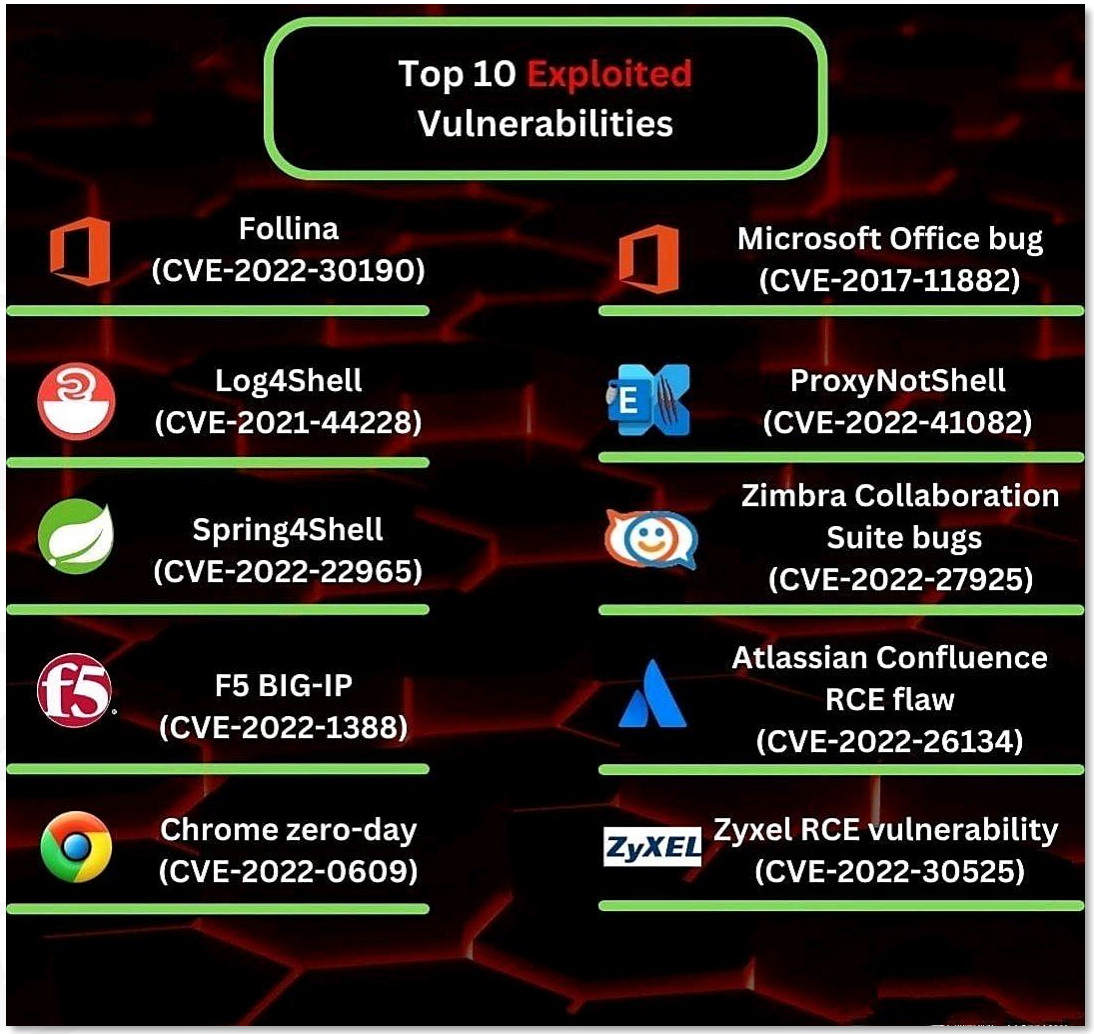
Phase (Legacy)

Assigned (20200210)

Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8832

Common Vulnerabilities and Exposures (CVE)

- Los CVE permiten hablar “un lenguaje común” entre muchas herramientas y sitios que tratan con vulnerabilidades
- “Esta aplicación es vulnerable al CVE-<año de descubrimiento>-<ID único>”
  - Dicen **MUCHO** en una simple frase
  - Sabemos dónde ir para encontrar todos los datos conocidos de la vulnerabilidad
- Si una vulnerabilidad se explota de forma masiva permite reaccionar e informar de ello de forma más eficiente
  - ¡Y esto ocurre en la vida real! (ver imagen)
  - Necesitas saber producto y versión...y a veces eso lo puedes sacar **con un simple navegador** ☹



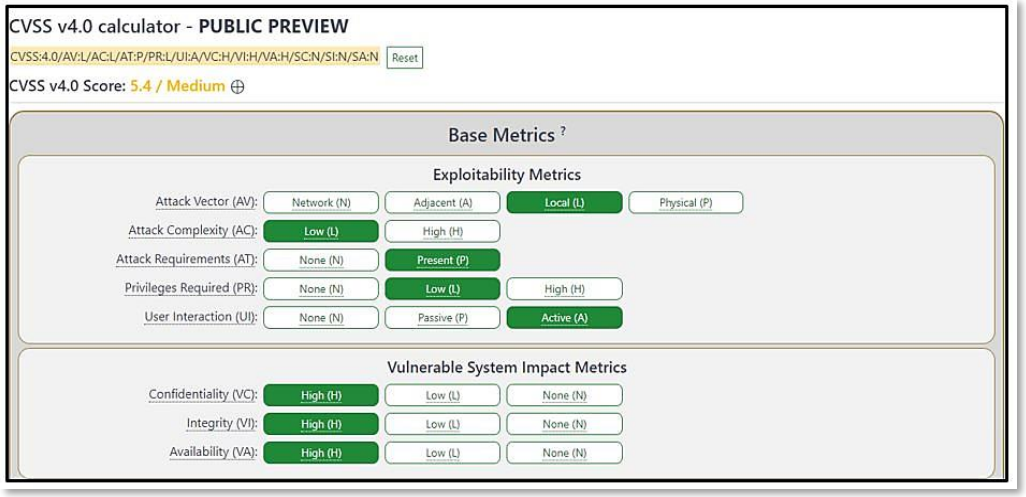
Fuente: https://es.linkedin.com/in/jsalasrodriguez

➢ Ejercicio **L1B3_CVEHTTP**

CVSS (Common Vulnerability Scoring System) 4.0

- **Por tanto, el CVE es como un glosario que clasifica las vulnerabilidades conocidas**
  - Y lo que se sabe de ellas
- **La gravedad de esas vulnerabilidades se puntúa con CVSS**
- **Muy recientemente ampliado a la versión 4.0**
  - Para dejar claro que un CVSS **no es solo una puntuación**
  - **Incluye más métricas** que modelan mejor el **tipo** de vulnerabilidad, su **impacto**, lo que hace falta para que **se explote** (privilegios, interacción del usuario...), etc.
  - También **cómo impacta la vulnerabilidad sobre la CIA** vista anteriormente

El grupo de métricas CVSS para caracterizar la gravedad de un CVE. Fuente: https://www.incibe.es/incibe-cert/blog/cvss-v40-avanzando-en-la-evaluacion-de-vulnerabilidades



Terminología básica

- **Riesgo**: Se obtiene multiplicando la magnitud del daño provocado por un ataque y la probabilidad de que ocurra
  - *Riesgo = Amenaza x Vulnerabilidad x Valor del objetivo*
- **Ataque**: Acción consciente e intencional realizada para causar daño a un sistema informático, compuesta por tres elementos centrales
  - **Motivo**
  - **Método** (el exploit utilizado para desplegarlo)
  - **Oportunidad**
- **Daños**: producidos por un fallo del sistema, ya sea accidental o provocado (ataque)
  - Económico, técnico, moral, de imagen empresarial / de marca...

TERMINOLOGÍA BÁSICA

- **Control (de seguridad)** o **contramedida**: mecanismo de protección que mitiga o elimina un riesgo y puede centrarse en
  - **Prevención** de ataques
  - **Mitigación** de ataques
    - Ralentizar, disminuir la superficie de ataque o aumentar la dificultad del mismo
  - **Redirección** de ataques a otros objetivos con seguridad mejorada no vulnerables al ataque
    - O que pueden implementar contramedidas o respuestas proactivas a la misma
    - Listas de bloqueo que se puedan aplicar en toda la infraestructura, alertas, informes...
  - **Detección** de ataques
  - **Recuperación** de ataques
  - Por lo general, se llaman **controles de seguridad (security controls)** en la mayoría de las metodologías / estándares / marcos / protocolos relacionados con la ciberseguridad
  - Hay muchas herramientas que nos recomiendan controles de seguridad (Ej.: Lynis) o nos descubren algunos que nos faltan de acuerdo a esos **estándares o políticas** (**Tema 4**)

➢ Ejercicio **L1B2_LYNIS**, **L1B3_LYNISREPORT**

Terminología básica: Tipos de atacantes (o "adversarios")

- **Script kiddies** o **n00bs** (aka **skiddies**)
  - **Personas con pocos conocimientos**, pero con acceso a herramientas de ataque avanzadas
  - Por lo general, a ciegas o con poco conocimiento sobre lo que está pasando "por debajo"
- **Pentesters** (hackers de sombrero blanco o white hat)
  - **Profesionales contratados legalmente para probar el estado de la seguridad de un sistema**
  - Usar las mismas técnicas que los atacantes malintencionados
  - Pero en entornos controlados y con limitaciones preestablecidas (**acuerdos contractuales**)
- **Crackers** (hackers de sombrero negro o black hat)
  - **Personas que dañan los sistemas con razones espurias**
  - Intelectual, económico, política, terrorismo, ciberguerra...
  - *... (incluso "por los LOLes", con un sentido del humor un tanto "peculiar")*

UN HACKER NO ES UN CIBERDELINCUENTE (A PESAR DE LO QUE DIGA LA PRENSA)

Terminología básica: Equipos de seguridad

- **Equipo rojo** (red team): grupo independiente que desafía a una organización a mejorar la efectividad de su seguridad asumiendo un "rol de adversario"

  - Contratado para **actuar como atacantes reales**, colocando payloads, exploits, actuando igual...
  - Después de un período infiltrado, informan de sus hallazgos, por lo que se puede mejorar la seguridad
  - Evalúan la seguridad general probando varios medios de protección (técnica, física, humana)

- **Equipo azul** (blue team): analiza la seguridad de los sistemas de información

  - Identifica fallos, verifica la efectividad de las medidas de seguridad, responde a incidentes, busca amenazas, realiza análisis forenses y operaciones de control de daños
  - Asegurar que todas las medidas de seguridad sean efectivas después de su implementación
  - "Lucha" contra atacantes/equipos rojos para mejorar la seguridad de los sistemas, respondiendo a sus ataques y protegiendo una organización y su información con una estrategia defensiva

- **Equipo morado** (purple team): maximiza la efectividad de ambos equipos

  - Integra tácticas defensivas (azul) con amenazas y vulnerabilidades (rojo) y comparte información
  - **Más información**: https://danielmiessler.com/study/red-blue-purple-teams/

Fuente: *PowerPoint* icons

Clasificación del malware

Clases de programas creados para dañar(te)

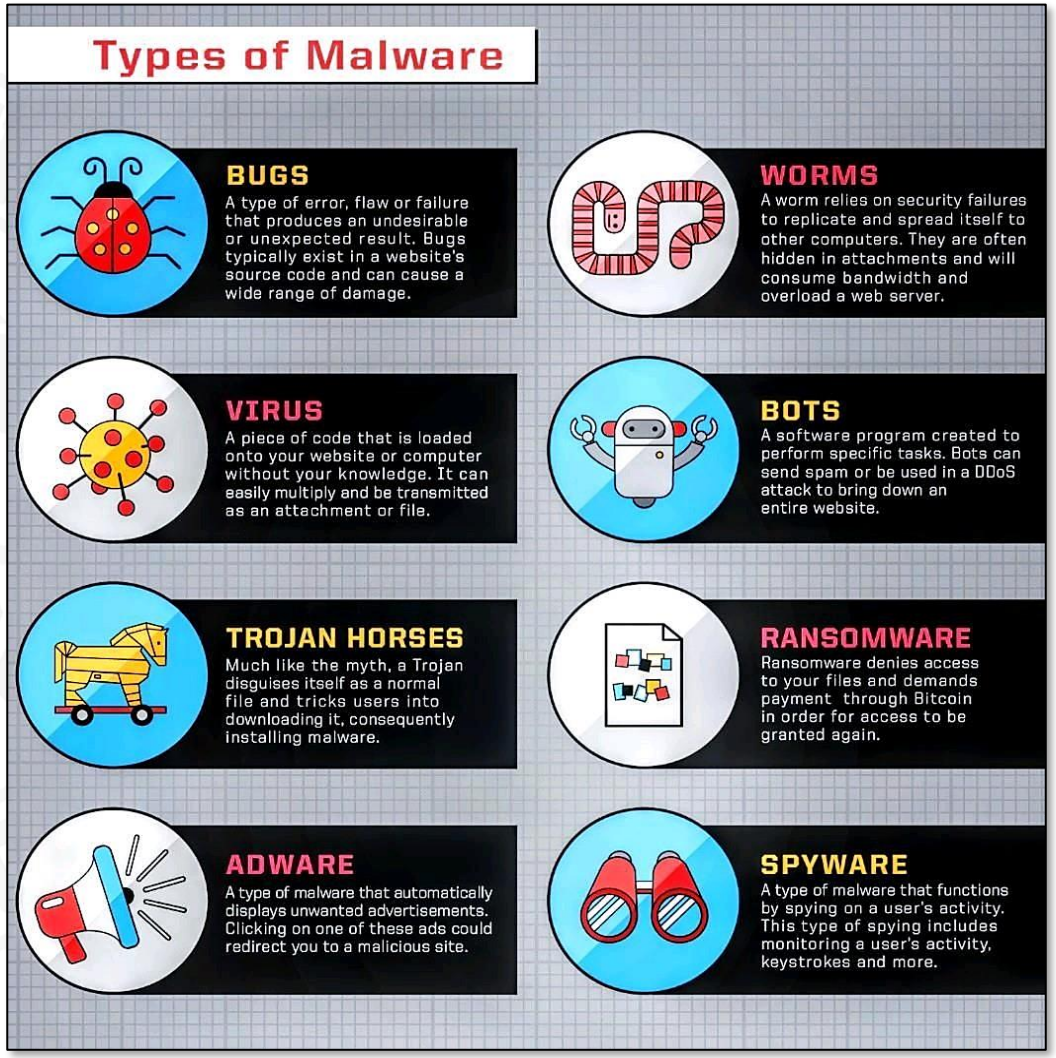
*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Malware (Malicious software)

- **Software para obtener accesos no autorizados**
  - O causar cualquier tipo de daño en sistemas informáticos
  - También llamado **código malicioso**
  - El software que lo **detecta y elimina** se conoce genéricamente como antimalware
- **Algunos efectos comunes son**
  - **Causar fallos**: Virus, gusanos, troyanos...
  - **Robar información personal / privada**: Spyware, Keyloggers, Stealers...
  - **Ataques distribuidos/coordinados**: Botnets...
  - **Insertar anuncios** (maliciosos): Adware, Hijackers...
  - **Extorsión / daño financiero**: Ransomware...
  - **Otros**: Rogue software, rootkits...

Fuente: https://m.facebook.com/viehgroup/photos/types-of-malwarebugs-worms-virus-bots-trojanhorse-ransomware-adware-spyware/2432740090357492/



➢ Ejercicios **L1B3_MALSCAN, L1B3_VIRUST**

Malware según sus efectos: Causar fallos en el sistema. Propagadores

Virus

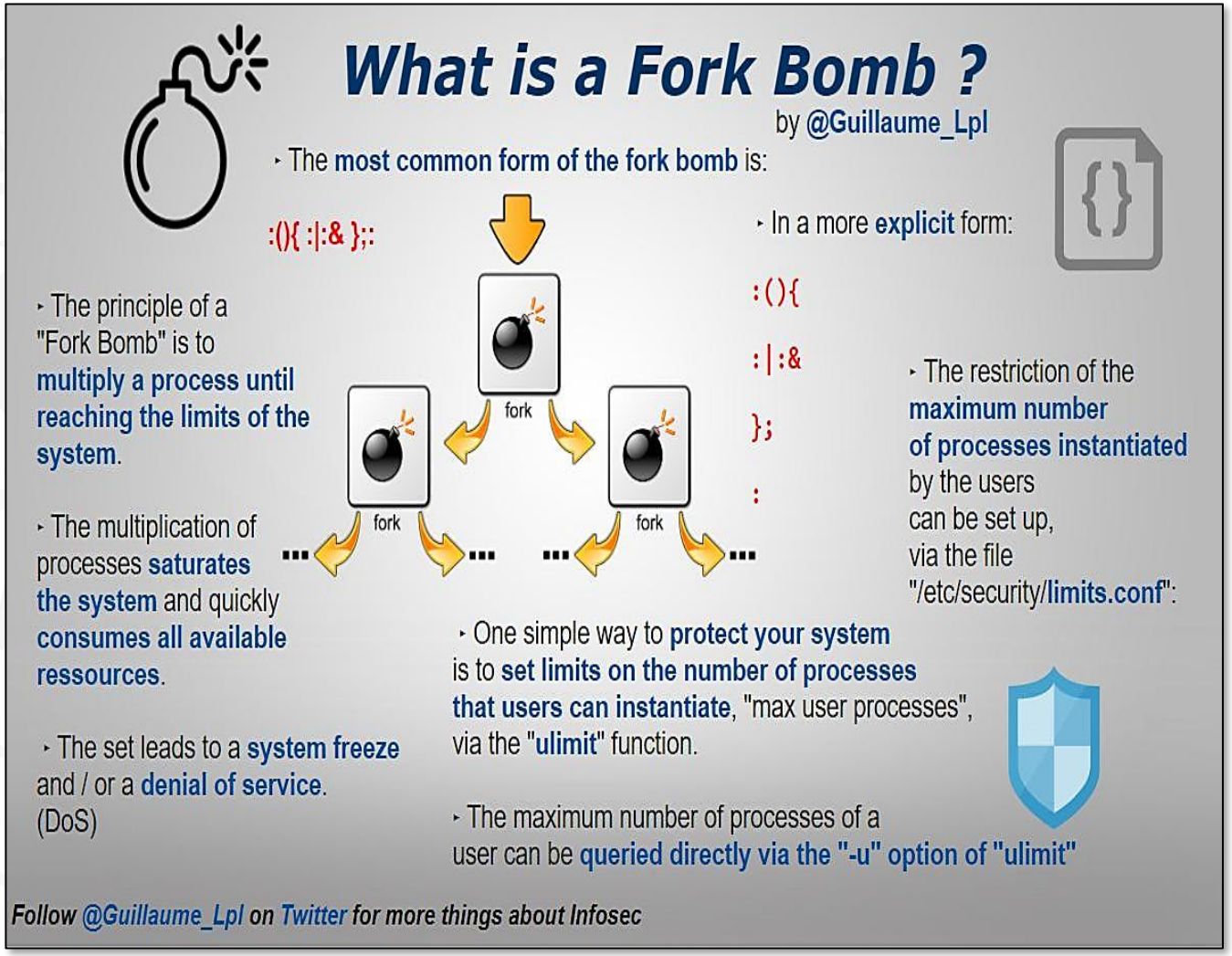
- **Malware creado con un doble propósito: dañar y propagarse**
- Causar cualquier tipo de **daño** cuando se ejecuta: destruir información, impedir el uso normal ...
- Se **propaga** a otros sistemas a través de diferentes medios
  - Dispositivos extraíbles, carpetas compartidas (Ej.: protocolo SMB), servicios en Internet...
- Por lo general, tienen un "**programa host**" que, una vez ejecutado, lanza el virus y sus efectos
  - Generalmente es software residente (servicios del sistema) o versiones modificadas / falsas de aplicaciones populares

Gusanos (Worms)

- **Malware con una capacidad de replicación agresiva**
- Se replica en un equipo o en una red informática para **aumentar el uso de recursos**, de modo que
  - Los ordenadores o redes cesan su actividad
  - El rendimiento se ve comprometido, por lo que el funcionamiento normal es imposible
- La propagación a menudo explota una vulnerabilidad existente en un servicio
  - Ej.: EternalBlue, https://en.wikipedia.org/wiki/EternalBlue
- A diferencia de los virus, no necesitan (y no infectan) otro software

Malware según sus efectos: Causar fallos en el sistema. Wabbits

- Malware de **denegación de servicio**
- Procesos que se replican continuamente para agotar los recursos
  - Ralentizan o bloquean un sistema por esta falta de recursos
- Gusanos sin capacidad de propagación
- Las **bombas fork** son el ejemplo más conocido
  - Implementarlos es simple: https://en.wikipedia.org/wiki/Fork_bomb



Malware según sus efectos: Causar fallos en el sistema. Troyano

- **Malware** "disfrazado" de software legítimo (controladores, herramientas...)
- Por lo general, implementan una funcionalidad legítima
  - Pero también vienen con efectos nocivos ocultos (puertas traseras, spyware, mostrar anuncios...)
- Se encuentran en sitios de descarga no oficiales (Ej.: Softonic)
  - Y en markets de aplicaciones no oficiales... ¡O incluso los oficiales!
  - Programas legítimos con "mejoras" o "añadidos" que resultan maliciosos o molestos
  - Los markets para móvil están plagados de este tipo de malware (¡**cuidado**!)
    - Especialmente Google Play Store de Android
- Hoy día, los casos de ataques a la cadena de suministro (**supply chain attacks**) están aumentando y usan troyanos
  - Versiones oficiales de software legítimo, pero troyanizadas en sus servidores / mirrors oficiales
  - Dispositivos IoT u otros aparatos electrónicos (cargadores, ...) con troyanos preinstalados
- El malware que implementa técnicas de dropper suele ser un troyano
  - El código malicioso real se descarga (en una o más partes) cuando se ejecuta un programa

Malware según sus efectos: Robo de información

- **Spyware**
  - **Obtiene información sobre individuos**, ordenadores u organizaciones sin su consentimiento
  - Incluso cumpliendo una serie de requisitos legales, o descargados de sitios oficiales (anti-cheat...)
  - Recopilan datos en segundo plano
    - Archivos, contactos, correos electrónicos, cuentas, contraseñas, URLs visitadas, hábitos de navegación, horarios, lugares visitados...
    - Esta información luego se **vende**, se envía a **compañías publicitarias** u **organizaciones criminales**
  - Si se ha añadido a un software legítimo troyanizado, se les suelen llamar **stealers**
- **Keyloggers**
  - **Roba información** monitorizando pulsaciones de teclado, movimientos del ratón, capturas de pantalla...
  - Esta información del comportamiento de los usuarios se envía posteriormente a un tercero
    - Que puede usarlo para obtener algún beneficio (acceso a cuentas bancarias, extorsión...) o venderlo
  - Se utiliza también para robar cuentas y contraseñas, revelar conversaciones privadas...
  - ...o también para **estudios de usabilidad y hábitos** (delito si no hay consentimiento)

Malware según sus efectos: Anuncios molestos / maliciosos

Adware

- **Software que muestra anuncios intrusivos en navegadores / aplicaciones**
- Usando ventanas emergentes, anuncios a pantalla completa, tácticas de engaño, advertencias falsas...
  - Imitar la interfaz de usuario de Windows / Linux, botones falsos, mensajes preocupantes ("¡has sido infectado!") ...
- Intentan engañar a los usuarios para que hagan clic en el anuncio, y así puedan ejecutar su payload
  - Se han encontrado anuncios maliciosos en productos legítimos
  - Insertados por servicios publicitarios que no aplican (o no pueden imponer) limitaciones correctas a lo que publican
- A veces los anuncios son utilizados por los programas para obtener beneficios económicos
  - Las licencias de uso del programa rara vez se leen / entienden
  - **Los anuncios pueden recopilar una cantidad sustancial de datos** o realizar operaciones no deseadas o no reguladas

Secuestradores de navegador (Browser hijackers)

- **Bloquean o dificultan el uso del browser** para obtener beneficios financieros o posicionamiento en búsquedas
- Reemplazando su web inicial por una con anuncios (aumentar las visitas publicitarias y el dinero ganado)
- Redireccionando a páginas no deseadas (porno, tiendas, páginas de descarga...) para aumentar visitas
- Alterando resultados de búsqueda para redirigir a ciertas páginas, o forzando a usar ciertos motores
- En general, se centran en **ganar dinero haciendo clic / visitando anuncios**, no robando dinero de los usuarios

Malware según sus efectos: Daño financiero / extorsión. Ransomware

- **Bloquean el uso del ordenador y / o sus datos**
  - Tomando el control total de sus funciones / archivos y **pidiendo un rescate** para recuperarlo
- **Los archivos importantes del usuario se cifran y son irrecuperables sin una clave de descifrado, que debe comprarse pagando un rescate**
- **Las instrucciones de pago se muestran cuando se completa la infección**
  - No cuando infecta el dispositivo por primera vez
  - Pueden permanecer inactivos una cierta cantidad de tiempo hasta que se activan (máximo daño)
  - Utilizan métodos de pago no rastreables (Ej.:: criptomonedas)
- **Es posible que los datos no se recuperen incluso pagando**
  - Clave no enviada o defectuosa, datos dañados, múltiples extorsiones...
  - Usar copias de seguridad no infectadas es la solución más recomendable
  - ¡Por tanto, una estrategia de backups sólida es algo obligatorio!
- **Más información:** https://www.osi.es/es/actualidad/avisos/ransomware

Fuente: TrendMicro

RANSOMWARE

Seguridad de Sistemas Informáticos

The Ransomware Kill Chain

RECONNAISSANCE

During the Reconnaissance phase, the attacker collects as much information as possible: mailing lists, social media presence, potential vulnerabilities...

During the Weaponization phase, attackers prepare their malicious software. There is a plethora of techniques to disguise the payload in a benign-looking file, (pdf, word, excel...), or in a compromised or malicious website.

WEAPONIZATION

DELIVERY

During the Delivery phase, the malicious payload (the dropper) is delivered to the intended target through an infected link to a file or site, an infected attachment, visiting infected websites (watering-hole, exploit kit or drive-by-download attacks) or malvertising.

During the Exploitation phase, existing vulnerabilities will be leveraged to deliver malicious code onto the system to get a better foothold.

EXPLOITATION

INSTALLATION

Once the dropper is on the victim's computer, the Installation process starts. Typically it connects to the Command & Control (C2) server to download key data (a malicious executable file, in some cases the encrytion key...).

There are variants of ransomware that operate on a self-propagation basis and will attempt to infect system files and spread to other hosts. Then, the ransomware starts to encrypt files on the infected computer, and possibly on the network and cloud storage, too.

COMMAND & CONTROL

ACTIONS ON OBJECTIVES

Now, following a succesful installation, C2 establishment and encryption across the existing infrastructure (local hosts, network and cloud resources), we reach the Actions on Objectives phase. The ransomware displays a ransom message to the victim. Typically, the desktop wallpaper is used for this purpose.

Finally, the criminals expect the ransom to be paid in cryptocurrency in a wallet they own. If the victim does not pay, the data is either lost (encryption keys deleted) or breached.

Cyber Startup Observatory©

cyberstartupobservatory.com

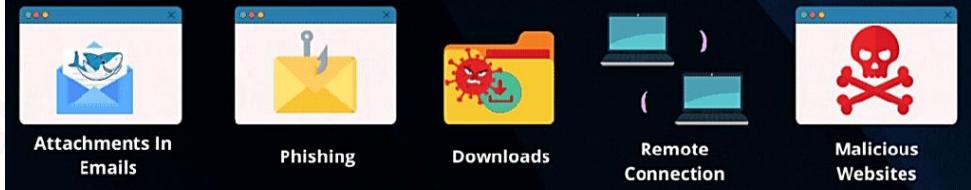
Malware and Ransomware

Cyber Writes
cyberwrites.com

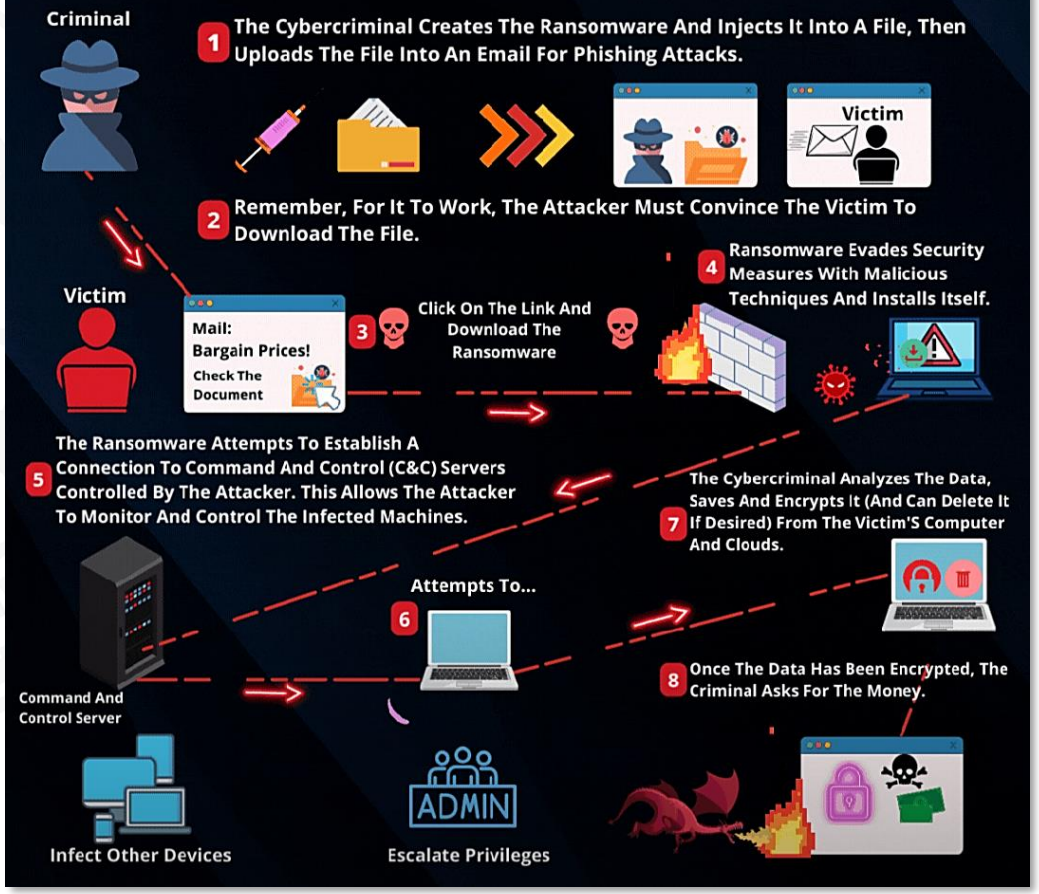
It Is A Type Of Malicious Software That Encrypts Files, Usually The User'S Office Files, And Extorts Money From The Affected Party In Exchange For A "Ransom" For The Affected Information.

How Does It Work?

It All Starts With The Infection Of The Computer By Means Of These Possible Attack Vectors:



Here Is An Example Of A Ransomware Attack:



Malware según sus efectos: Rootkit

- **Software** no solicitado y no autorizado que **se instala con privilegios de superusuario**
- Su objetivo suele ser **robar información** o **crear una puerta trasera** (backdoor)
  - Y permanecer en el sistema sin ser detectado por el usuario
  - Pueden estar compuestos por archivos de sistema falsos / ocultos / críticos que imitan a legítimos
  - Por lo general, implementan técnicas de ocultación de procesos
    - Que no los muestran en listas de procesos típicas o software de gestión e información de procesos
- **Pueden habilitar puertas traseras para introducir malware adicional**
- **Esta técnica también fue utilizada por software de prevención de copia o anticheat**
  - ¡Por empresas legales!
  - Esto causó un gran escándalo cuando se descubrió
  - https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

Malware según sus efectos: Rogue software

- **Programas falsos** que afirman implementar funcionalidades que no implementan
- Las variantes incluyen
  - **Antivirus falsos**: incluso afirmando (falsamente) que los ordenadores están infectados como reclamo para su descarga
  - **Herramientas de "limpieza" de malware**: de nuevo, alegando infecciones falsas
    - Incluso pueden convertirse en malware adicional, como spyware
  - **"Optimizadores" de SSOO**: Que realmente no realizan ningún tipo de optimización
    - Y también puede ocultar malware
- Típico de tiendas de aplicaciones de dispositivos móviles, especialmente Android
  - ¡E incluso en la tienda oficial!
- Una vez instalados, pueden ejecutar un payload con otro tipo de malware

CRIMEWARE

- **Cualquier software especialmente creado para cometer delitos**
  - Financiero, robo de datos...
- **No son** programas legítimos infectados
  - Pero sí software creado con el propósito de cometer ciertos delitos
  - Robo de identidad, robo de contraseñas, captura de datos confidenciales...
- **Pueden replicarse a sí mismos, como los worms**
- **Se pueden crear para ser vendidos a otros delincuentes sin la capacidad de crear su propio malware**
  - Paquetes de exploits, herramientas de exploiting...
  - El **Ransomware-as-a-Service** (RaaS) es uno de los ejemplos actuales más peligrosos
    - *¿Quieres implementar una campaña de ransomware contra alguien, pero no sabes cómo?*
    - ¡No hay problema! Te **alquilan** todas las herramientas necesarias y manuales de instrucciones
      - O piden un porcentaje de las "ganancias"

BACKDOORS

- **Métodos alternativos / no oficiales para acceder** a un ordenador o software
- Permite a los atacantes acceder / controlar los sistemas sin utilizar mecanismos de autenticación normales
  - Una vez dentro del sistema, pueden obtener permisos y realizar operaciones privilegiadas
  - **Son un grave riesgo para la seguridad**
- ¿Por qué existen?
  - **Creadas intencionadamente** por los desarrolladores de un software o cualquier biblioteca de terceros que utilice ese software
    - Tal vez sin intenciones maliciosas... cuentas “de prueba" no documentadas, "paneles de control" para desarrollo que no se desactivaron al pasar a producción...
  - Una **consecuencia de una vulnerabilidad no intencionada**
    - Ej.: versiones antiguas de páginas web / servicios dejados accidentalmente en línea
  - Creadas por algún **crimeware**

¿Y AHORA QUÉ?

- **Para explorar los diferentes aspectos del mundo de la ciberseguridad, necesitamos objetivos legales de estudio**
- **Los objetivos pueden ser**
  - **Máquinas** y **redes** de máquinas
  - **Personas** (sí, ¡también son objetivos!)
- **Esto implica**
  - **Crearlos**
    - Nuestros propios objetivos personalizados (nunca reales, ya que es ilegal a menos que exista un contrato)
    - Uso de Inteligencia de código abierto (OSINT): información disponible públicamente en Internet
  - **Poder llegar a ellos**
    - Y esto requiere más conocimientos técnicos básicos, **especialmente cuando se localizan máquinas y redes**
    - **¡Vamos a por ellos!**

¿Crees que lo has entendido todo? ¡Autoevalúate!

Eres capaz de hacer lo siguiente

- *Sabes a grandes rasgos qué contiene un CVE y por qué es importante en seguridad*
- *Sabes qué es el sistema de puntuación CVSS, que tipo de elementos contiene y como interpretar una puntuación de este tipo*
- *Entiendes lo que es un riesgo de seguridad, y como se calcula*
- *Distingues entre ataque y daño*
- *Entiendes lo que es un control de seguridad y sus contenidos relativos a la prevención y respuesta a ataques*
- *Sabes distinguir entre un **script kiddie**, un **pentester** y un **cracker***
  - *Y, sobre todo, qué NO es un **hacker***
- *Sabes distinguir entre un equipo rojo, un equipo azul y un equipo morado*
- *Puedes distinguir los distintos tipos de malware que existen y lo que hacen: Virus, **worms**, **wabbits**, troyano, **spyware**, **keylogger**, **adware**, **hijackers**, **ransomware**, **rootkit**, **rogue software**, **crimeware** y **backdoor***
- *Entiendes la "**kill chain**" del **ransomware**, como actúa y cómo compromete una infraestructura*

< Ir al Índice

Fuente: Bing Chat AI

Redes de máquinas >

DNS >

Conceptos básicos de redes

¡No puedes hackear lo que no puedes ver!

*Iconos por Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- **En la primera parte de este bloque aprenderás**
  - Cómo se hace la **comunicación entre máquinas**
  - Cómo interpretar una **dirección IPv4** y una **máscara CIDR de una red**
- **En la segunda, aprenderás**
  - Que máquinas en redes distintas **también se pueden comunicar entre ellas** si hay elementos que permitan "saltar" entre las redes
  - Qué es una **IP privada** y una pública
  - Qué es **NAT** y para qué sirve
  - Como tienes (probablemente) **montada tu conexión a Internet en casa**
- **En la tercera, aprenderás**
  - **Por qué existe el DNS** y la función que cumple dentro de las conexiones a máquinas que hacemos a diario
  - **Cómo se organiza** el sistema de nombres DNS
  - **Cómo funciona a nivel general** una petición DNS típica

¿CÓMO SE COMUNICAN LAS MÁQUINAS ENTRE ELLAS?

- **Cuando queremos comunicarnos con otros usuarios en redes sociales...**
  - Los localizamos y les enviamos un mensaje
  - Luego, estos usuarios interactúan con nosotros de acuerdo con los protocolos de redes sociales
    - "Me gusta", retweets, gifs, emojis, memes...
- **Curiosamente, ¡este es el mismo principio que usan las máquinas para comunicarse entre ellas!**
  - Y créeme, ¡hoy en día **hay MUCHOS tipos de máquinas** distintos que se comunican entre ellos!

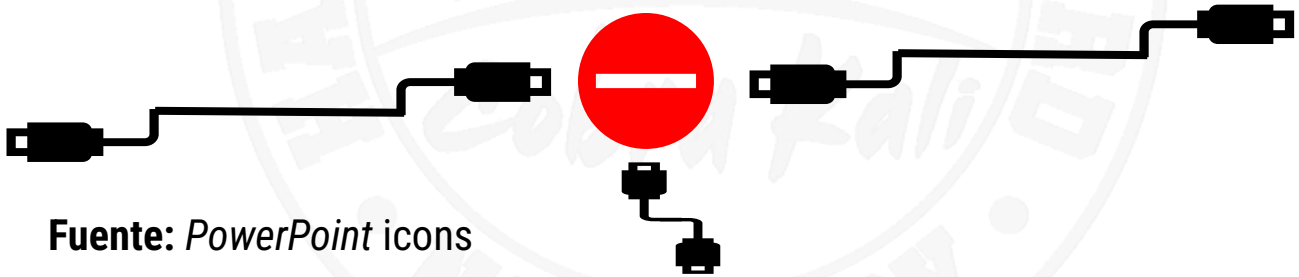
Fuente: https://formatalent.com/cursos-de-m2m-machine-to-machine

¿CÓMO SE COMUNICAN LAS MÁQUINAS ENTRE ELLAS?

- **En cada red social tenemos un identificador único que nos distingue de los demás**
  - En Twitter, si quiero comunicarme con César Granda (exalumno y hacker profesional) debo escribir a `@CacharroHacks`
- **¡Pero las máquinas no tienen identificaciones! Ya, pero tienen IPs ☺**
  - **La IP de una máquina es lo que la distingue de otras máquinas** en una red
  - Máquinas capaces de comunicarse **DIRECTAMENTE** entre ellas **NO PUEDEN tener la misma IP**
    - De la misma manera que dos usuarios de la misma red social no pueden tener el mismo ID
    - ¡Suplantación de usuarios / máquinas! (conocida como “colisión de IPs”)
- **Las personas tenemos redes sociales, pero las máquinas tienen redes IP**
  - ¡El enfoque es el mismo!
  - Recordemos conceptos de FCR ☺

REDES IP

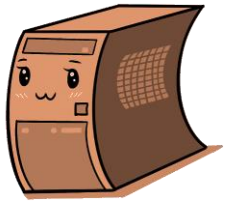
- **LAN**: una red que interconecta maquinas dentro de un área limitada
  - Residencia, escuela, laboratorio, campus, oficina...
- **Sin la ayuda de otros dispositivos, las máquinas en diferentes LAN no pueden verse entre sí**
  - Esto también significa que dos máquinas en diferentes LAN pueden tener la misma IP
  - ¡El problema aparece con máquinas en la misma LAN!



Fuente: *PowerPoint* icons

Mi red de casa (LAN) 192.168.10.X

IP 192.168.10.10



IP 192.168.10.130

IP 192.168.10.210

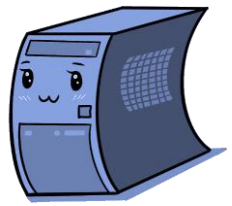
La red de mi vecino (LAN) 192.168.10.X

IP 192.168.10.10

IP 192.168.10.130

Mi red del trabajo (LAN) 192.168.30.X

IP 192.168.30.10



IP 192.168.30.30

IP 192.168.30.120

Direcciones IP v4

- **El protocolo de Internet pertenece a la capa de red**
  - ¿Recuerdas las capas de red y los protocolos de FCR?
- **Las direcciones del protocolo de Internet (direcciones IP) son la base de las comunicaciones actuales**
  - Cada dispositivo conectado (ordenador, teléfono, tablet, Raspberry, bombilla IoT...) tiene una dirección IP
  - Es lo que nos permite comunicarnos y conectarnos con ella
  - Es decir, es su **dirección de contacto**
- **Históricamente, se ha venido usando IP versión 4 (IPv4)**
  - Sus direcciones constan de cuatro grupos de 8 bits, por ejemplo `192.168.1.100` (32 bits)
  - Cada uno de los números entre los puntos (.) es un byte, es decir, un dato de 8 bits
  - Por lo tanto, cada número estará en el rango de 0-255
  - **Se han agotado**: las redes mundiales están (lentamente) haciendo transición a IPv6 (128 bits)

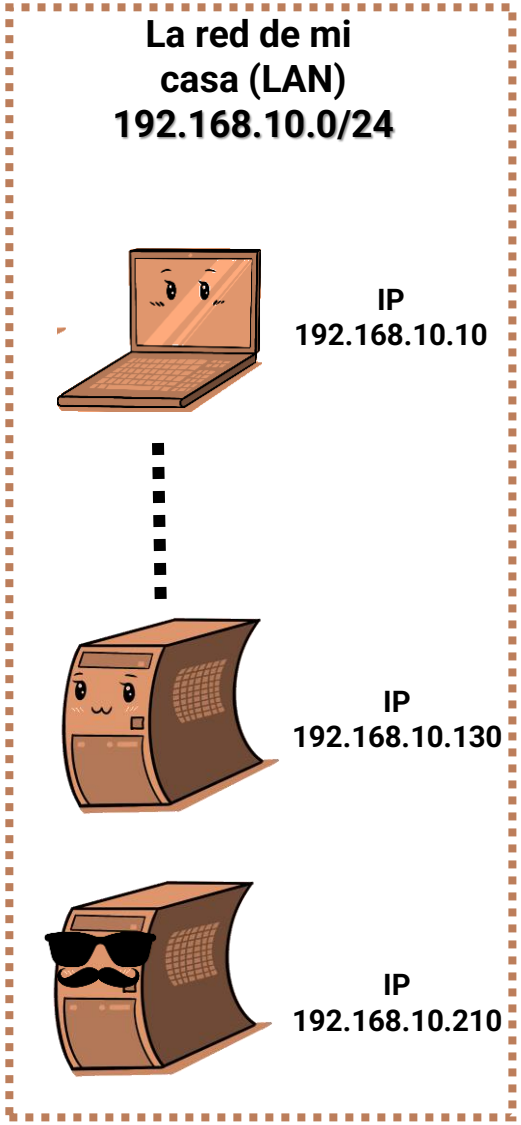
Classless Inter-Domain Routing (CIDR)

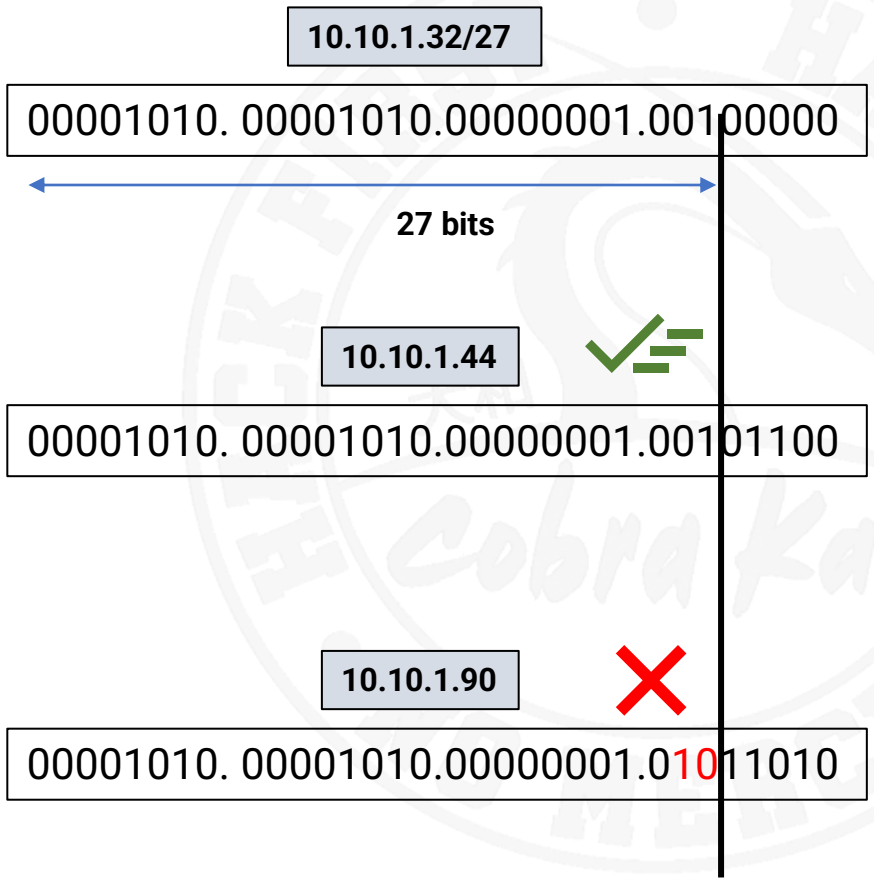
- **CIDR es un estándar basado en bits que utiliza prefijos para mostrar direcciones IP con sus propiedades de enrutamiento**
  - Facilita el enrutamiento, agrupando bloques de IPs en una única entrada de una tabla de rutas
  - En otras palabras, es una forma de representar grupos de IPs con un mismo identificador
- **Estos grupos se denominan bloques CIDR**
  - Las IP en el mismo bloque CIDR comparten una secuencia de bits inicial (de cierta longitud) en su forma binaria
  - Esta secuencia se llama **prefijo**
- **Los bloques CIDR IPv4 usan una sintaxis similar a las direcciones IP:** `A.B.C.D/N`
  - Una dirección IPv4 decimal con puntos, seguida de una barra diagonal
  - Luego un número (N) de 0 a 32
  - Este número es la longitud del prefijo
    - El número de bits iniciales **compartidos por todas las máquinas de la red representada**
    - Contando desde el bit más significativo

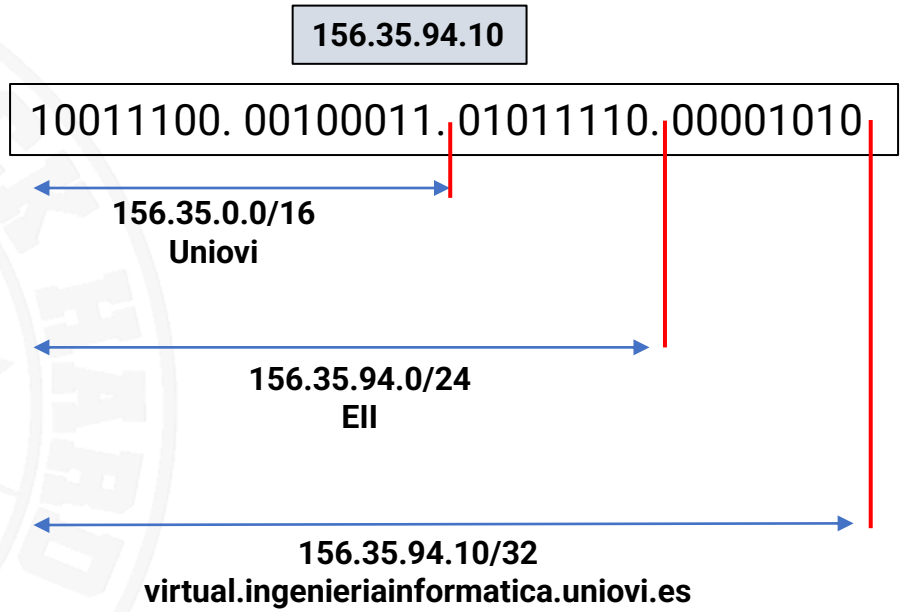
Classless Inter-Domain Routing (CIDR)

- **Al especificar sólo el tamaño de red, se omite la dirección de la notación**
  - Por lo tanto, un bloque `/20` es un bloque CIDR con un prefijo de 20 bits no especificado
- **Una dirección IP es parte de un bloque CIDR (coincide con el prefijo CIDR) si los N bits iniciales de la dirección y los indicados por el prefijo CIDR son los mismos**
  - Una dirección IPv4 es de 32 bits, por lo que un prefijo CIDR de N-bits deja 32-N bits “libres”
  - Lo que significa que $2^{(32-N)}$ las direcciones IPv4 pueden encajar con un prefijo CIDR de N bits dado
  - **Prefijos CIDR más cortos encajan con más direcciones, y los más largos encajan con menos**
    - Prefijos más cortos implican menos redes con más máquinas potenciales (algunas redes grandes)
    - Más grandes implican más redes con menos máquinas potenciales (muchas redes pequeñas)
    - Una misma dirección puede coincidir con varios prefijos CIDR de diferentes longitudes
  - A veces esto se representa con una máscara de bits (`255.255.255.0` vs `/24`)
- **CIDR también se utiliza para direcciones IPv6 y la semántica es idéntica**
  - La longitud del prefijo puede variar de 0 a 128, debido al mayor número de bits

Classless Inter-Domain Routing (CIDR)







¿Quieres practicar esto?
https://www.ipaddressguide.com/cidr

Fuente: *PowerPoint* icons

Classless Inter-Domain Routing (CIDR)

Seguridad de Sistemas Informáticos

- Las LAN pequeñas y grandes (N de `/28` a `/24`) son las más usadas actualmente
- Para laboratorios y pruebas, es muy común utilizar `/24`
  - Hasta 256 máquinas en la red
- Los `/31` se utilizan para crear enlaces punto a punto entre dispositivos
  - Dos dispositivos unidos directamente
- Los ISP (ej.: Telecable) generalmente tienen `/21` o inferior

IPv4 Subnetting

packetlife.net

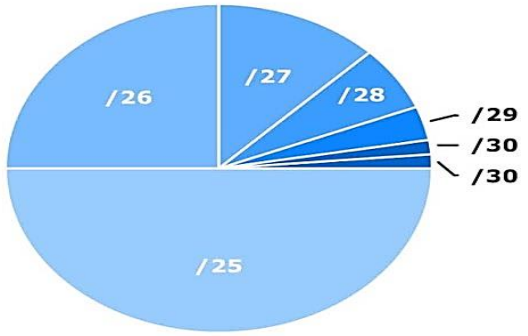
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

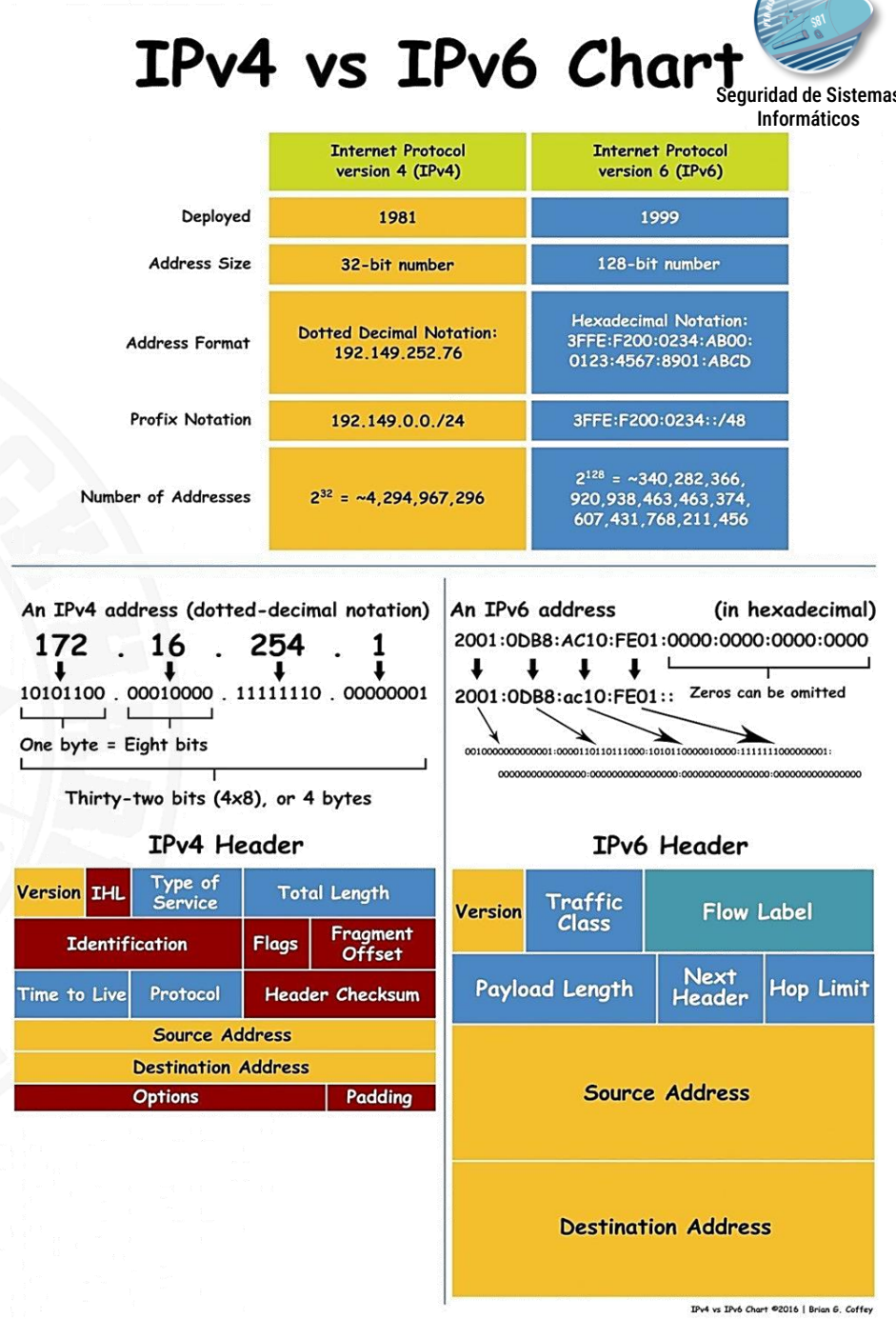
by Jeremy Stretch v2.0

Classless Inter-Domain Routing (CIDR): Direcciones reservadas

- Las LAN pequeñas y grandes son los tipos de red más implementados
- Normalmente, la primera dirección de una subred (todos los bits de host a 0) se reserva **para referirse a la propia red**
  - Ejemplo: `192.168.35.0`
- La última dirección (todos los bits de host a 1) se utiliza como dirección de **broadcast** para **todas las máquinas de la red**
  - Ejemplo: `192.168.35.255`
  - Dirección para enviar un mensaje a todos los hosts de la red al mismo tiempo
- Esto reduce el número de direcciones disponibles para máquinas en 2

DIRECCIONES IP v6

- **El crecimiento de Internet agotó el conjunto de direcciones IPv4 disponibles**
  - Se estandarizó una nueva versión de IP (IPv6), de 128 bits
  - Implica un espacio de direccionamiento mucho mayor (2^{128})
- **Como IPv4, las direcciones IPv6 identifican una interfaz de red de un dispositivo**
  - Pero conectado a una red informática IPv6
- **Una dirección IPv6 se representa como 8 grupos de cuatro dígitos hexadecimales**
  - Cada grupo representa 16 bits
  - Los grupos están separados por dos puntos (`:`)
  - **Ejemplo**: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
- **Más información**
  - https://www.ipv6.com/general/ipv6-addressing/



¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Entiendes que dentro de una misma red las IPs identifican a las distintas máquinas y que, por tanto, no puede haber dos máquinas con la misma IP*
  - *Comprendes el concepto de LAN*
  - *Sabes cómo es una IPv4 y su estructura*
    - *Y por qué solo pueden estar compuestas por nºs de 0 a 255*
  - *Comprendes el concepto de máscara CIDR y para qué sirve*
    - *Así como la técnica que se usa para saber si una IP pertenece o no a una máscara CIDR dada*
  - *Sabes para qué sirven las dos direcciones IP reservadas típicamente dentro de una red*
  - *Entiendes para qué se han creado las IPv6 y su estructura general*

Redes de máquinas

Ellas no bailan solas ☺

*Iconos por Bing Chat AI

Entendiendo las redes de máquinas

- **En una red social normalmente puedes comunicarte con todos los usuarios de esa red**
  - A menos que el usuario se aísle de los demás (cuentas privadas, grupos cerrados...)
- **En una red de máquinas, puedes comunicarte con todos los dispositivos que tengan una IP compatible con la tuya**
  - Dispositivos **cuya IP encaja en el mismo CIDR**
  - Las máquinas en la misma red normalmente pueden comunicarse entre ellas
  - A menos que también restrinjan esto a máquinas específicas
    - Por ejemplo, mediante firewalls
  - ¡También tienen sus grupos cerrados / cuentas privadas, como en las redes sociales!

Entendiendo las redes de máquinas

- **Pero *¿qué pasa si emisores y receptores están en redes diferentes?***
- **En las redes sociales, la comunicación entre diferentes redes no es posible o está muy restringida**
  - No puedes enviar un tweet a un usuario de Facebook
  - Sin embargo, puede enviar una historia o foto de Instagram a una cuenta de Facebook conectada
- **Pero PUEDES comunicar máquinas en diferentes redes**
  - Gracias a dispositivos especiales que actúan como "puentes" (bridges) o "pasarelas" (gateways) entre ambas redes
  - ¡Y eso es lo que vamos a explicar ahora!
  - Pero primero, necesitamos revisar dos conceptos respecto a las IPs

IPs PÚBLICAS Y PRIVADAS. NAT

- Como dijimos, IPv4 ya no tiene direcciones para todos los dispositivos de Internet
- Se desarrolló un sistema para usar un grupo de IP solo en LAN: **IPs privadas**
  - `192.168.0.0 - 192.168.255.255`
  - `10.0.0.0 - 10.255.255.255`
  - `172.16.0.0 - 172.16.255.255`
- Diferentes LAN en el mundo pueden usar direcciones en estos rangos
  - Pero **no se pueden usar en Internet**
- Normalmente, un **router** asigna una IP privada a cada dispositivo conectado a él
  - Formando su LAN privada
- Y envía todas las conexiones fuera de su LAN privada a través de una IP única
  - Válida en la red que está "al otro lado" del router
  - "Traducir" IPs privadas a IPs que se pueden usar en la red del "otro lado"
  - En algún momento de esta cadena de conexiones, la IP traducida es **pública y válida en Internet**
  - Este mecanismo de traducción se llama **NAT** (Network Address Translation)

¿NAT?

- El concepto NAT desde una perspectiva de red social es como grupos “al revés"
- Publicar en un grupo de usuarios significa que todos los usuarios del grupo lo reciben
- ¡Pero esto es lo contrario!
  - Un mensaje creado por un miembro del grupo (máquina)
    - Se publica al exterior con el id de grupo / nombre / hashtag (una IP válida en la red de la máquina receptora)
    - El usuario (máquina) que emitió el mensaje no es visible
  - Si alguien responde al mensaje
    - Solo el remitente original recibe esta respuesta
  - Es decir
    - Las peticiones se traducen a IPs de la red de destino
    - Las respuestas se traducen a IPs de la red de origen
      - Y enrutadas solo a la máquina que originó la solicitud
    - Esto lo hace software como iptables (ver ASR)

Fuente: https://www.profesionalreview.com/2020/08/22/modo-nat-que-es/

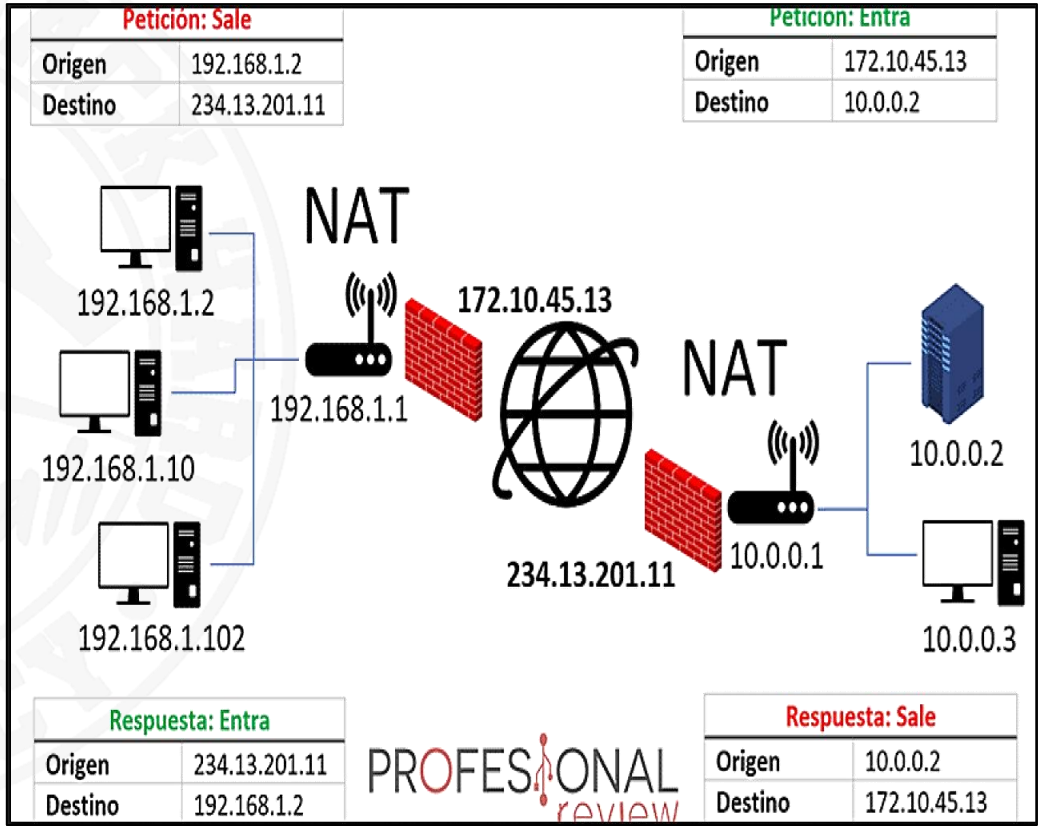
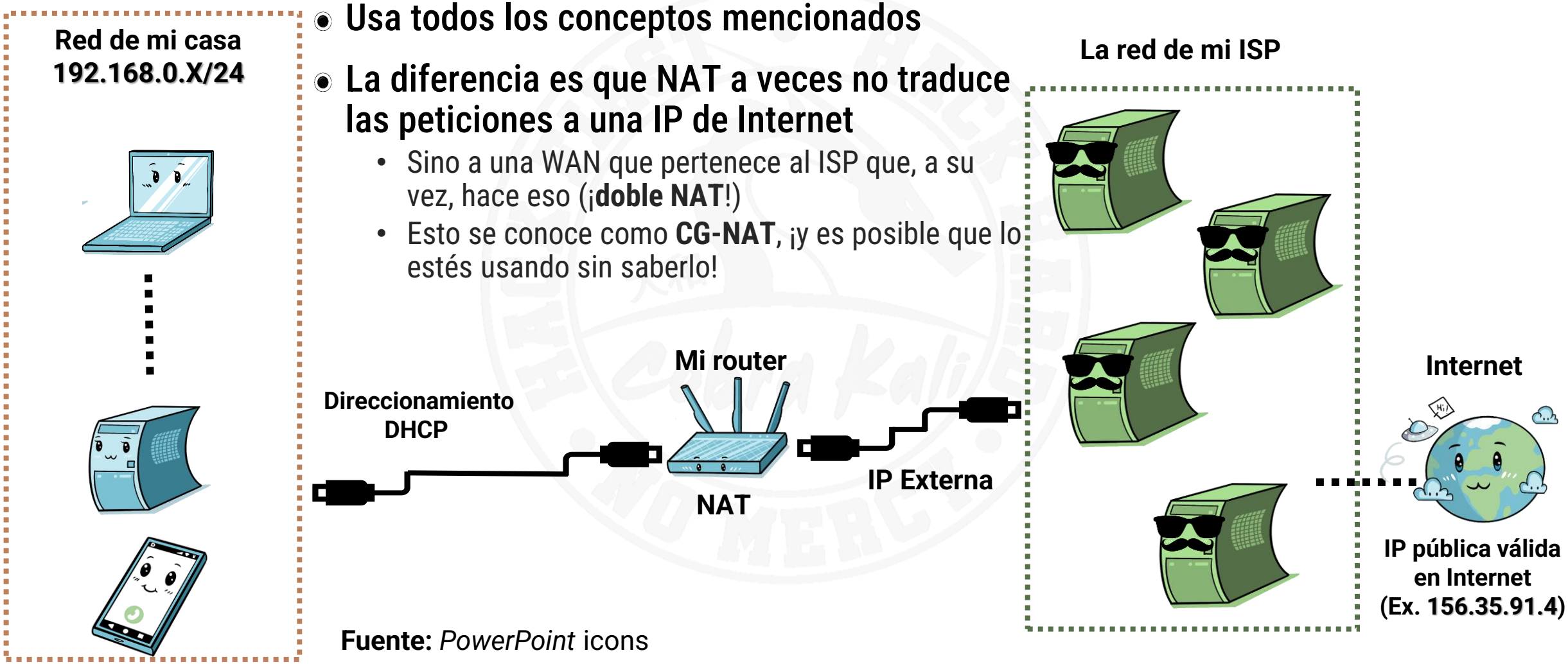


Diagrama: Típico montaje de NAT ISP + router DCHP en un hogar

- Este es el diseño típico de una red doméstica
- Usa todos los conceptos mencionados
- La diferencia es que NAT a veces no traduce las peticiones a una IP de Internet
  - Sino a una WAN que pertenece al ISP que, a su vez, hace eso (¡**doble NAT**!)
  - Esto se conoce como **CG-NAT**, ¡y es posible que lo estés usando sin saberlo!



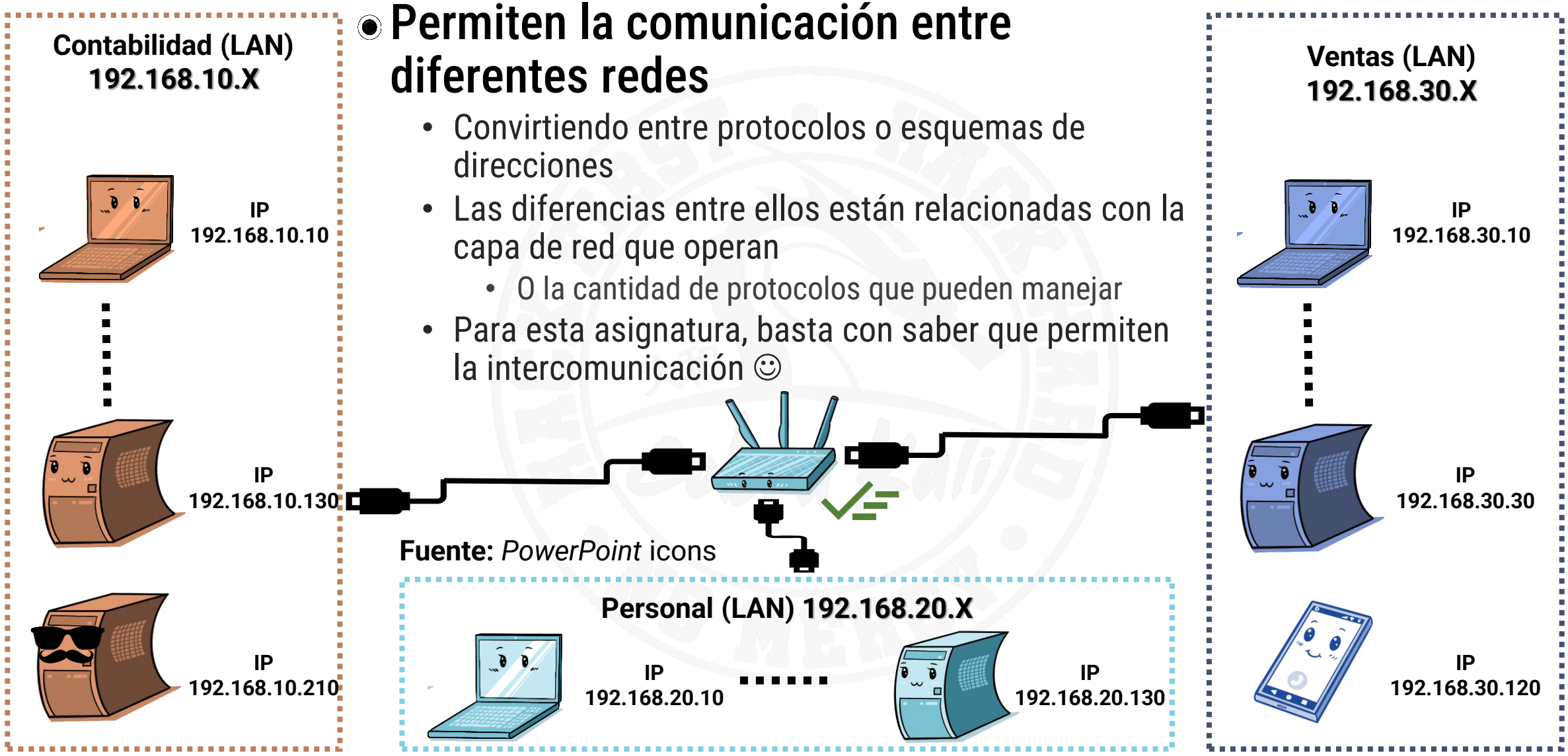
Fuente: *PowerPoint* icons

DHCP (Dynamic Host Configuration Protocol)

- **Los routers asignan IPs a sus dispositivos de red de forma manual o automática**
- **DHCP es el protocolo que asigna direcciones IP de forma automática y dinámica**
  - Esto significa que un dispositivo no tiene que tener la misma dirección IP todo el tiempo, pero tampoco se preocupa por cómo obtenerla ☺
  - Verás más detalles sobre DHCP en ASR
- **Es muy típico de las redes locales**
  - Cuando un dispositivo se conecta a una LAN, pide una dirección IP a un servidor DHCP (Ej.: el router)
  - Luego, el servidor DHCP asigna una dirección IP a ese sistema durante un período de tiempo fijo conocido como **lease**
  - Cada vez que te conectes a la LAN, es probable que recibas una dirección IP (**dinámica**) diferente
    - Pero generalmente en el mismo rango
    - Por ejemplo, `192.168.0.0` - `192.168.255.255` (IP privadas)
- **Esto, combinado con la NAT del router, hace que cualquier hogar / oficina / … pueda conectar dispositivos a Internet con un mínimo esfuerzo (y con solo una IP)**

Gateways / Bridges / Routers / Switches

- **Permiten la comunicación entre diferentes redes**
  - Convirtiendo entre protocolos o esquemas de direcciones
  - Las diferencias entre ellos están relacionadas con la capa de red que operan
    - O la cantidad de protocolos que pueden manejar
  - Para esta asignatura, basta con saber que permiten la intercomunicación ☺



Fuente: *PowerPoint* icons

En resumen...

- **Es un poco más complicado que las redes sociales**
- **La IP de tu máquina (identificador) determina las máquinas con las que puedes "hablar" directamente**
  - Hay IPs "compatibles" (encajan con el CIDR de su red)
  - E "incompatibles" (no encajan)
- **Para "hablar" con máquinas en diferentes redes necesitas un "traductor"**
  - Los gateways, los bridges, los routers o los switches son diferentes tipos de traductores
  - Que se utilizan en función de los protocolos y la topología de red
- **De esta manera, cualquier máquina puede potencialmente hablar con cualquier otra en el mundo...**
  - Pero normalmente, hay elementos que prohíben las comunicaciones por razones de seguridad (como los firewalls)
  - ¡Hablaremos de ellos más adelante en la asignatura!

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entiendes que dentro de una misma red las máquinas se pueden comunicar entre ellas*
    - *Salvo que exista algo que lo impida, como un **firewall***
  - *Comprendes que hay elementos que permiten la comunicación entre máquinas que se encuentran en distintas redes independientes, como **gateways**, **routers**...*
  - *Comprendes que, gracias a ello, hoy en día tenemos una enorme cantidad de redes diferentes interconectadas*
    - *Y que, como usuarios, hacen un trabajo que solo vemos cuando fallan*
  - *Entiendes qué es una IP privada y por qué tu PC de casa tiene una*
  - *Sabes qué es el concepto de NAT y cómo te permite tener muchos dispositivos conectados a Internet con un solo **router** y una sola IP pública*
  - *Comprendes la gran cantidad de trabajo de administración de redes que nos quita de encima el protocolo DHCP*

DNS

Domain Name Service

*Iconos por Bing Chat AI

¡LAS IP SON DIFÍCILES DE RECORDAR!

- **En las redes sociales utilizamos hashtags únicos para recordar a los usuarios**
  - Son mucho más fáciles de recordar (y buscar) que una serie de números (IPv4) o caracteres hexadecimales (IPv6)
  - `@hibarikky` es mucho más fácil de recordar que "`TwitterUser13224343245`"
    - Si Twitter sigue existiendo cuando leas esto ☺
- **Los usuarios normalmente tienen un nombre común vinculado a su hashtag**
  - "Tomás Balaguer" es mucho más fácil de recordar (y buscar) que `@eftomas`
- **Aparte, (casi) nunca navegamos usando IPs (¡es cosa de hackers! ☺)**
- **Cada máquina en una red tiene una IP asignada, pero no la usamos, usamos su "nombre" único (Ej.: `www.facebook.com`)**
  - ¿Cómo es posible?
  - Porque hay un servicio de "**traducción**" que convierte IPs en nombres y viceversa
  - ¡Es el servicio **DNS** (Domain Name System)!

Domain Name System (DNS)

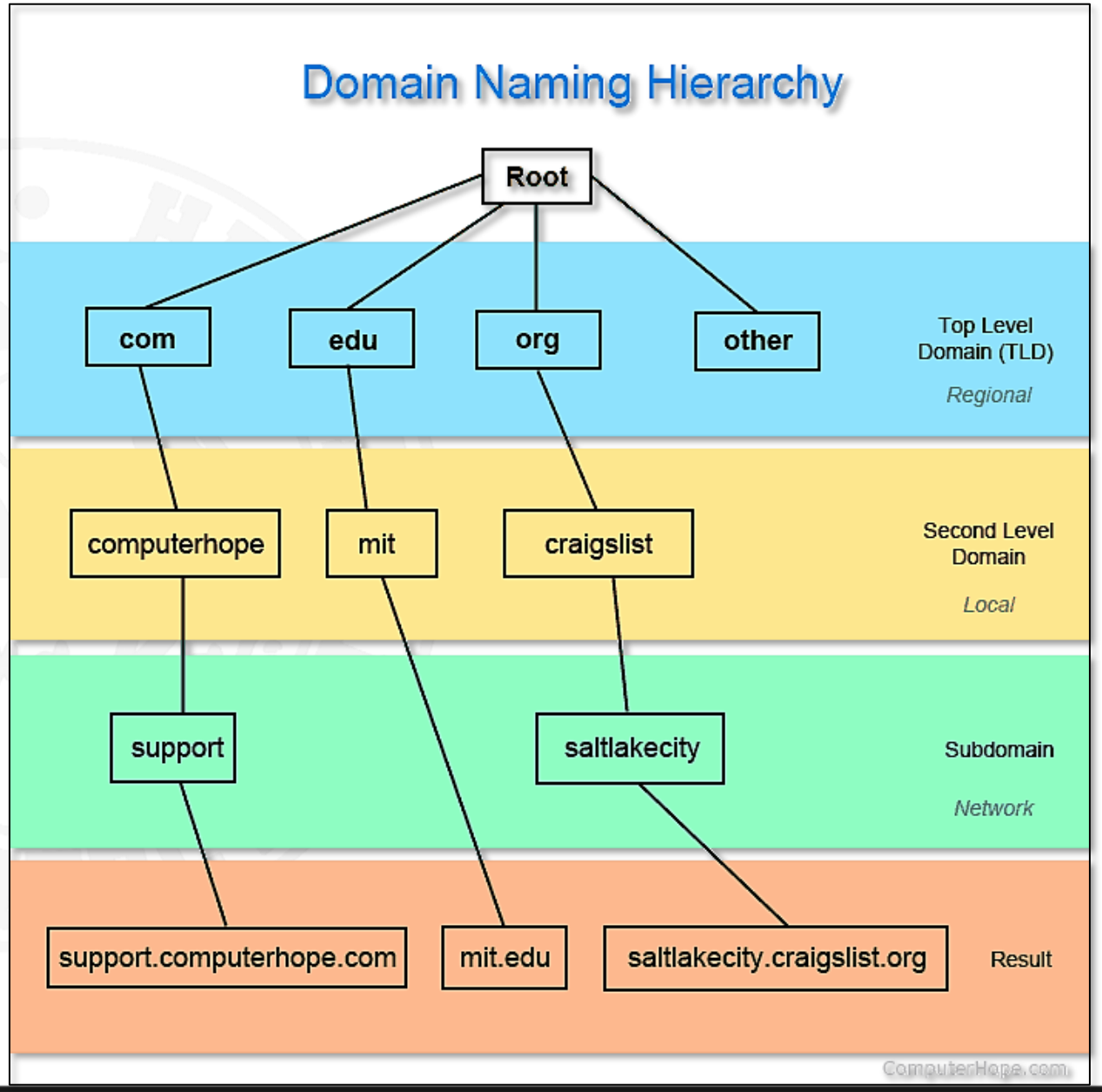
- **Sistema de nombres** jerárquico y descentralizado para dispositivos, servicios u otros recursos conectados a cualquier red
  - Asocia direcciones IP con nombres de dominio (**human-friendly** ☺) asignados a esas entidades
    - Ej.: `156.35.94.1` es www.ingenieriainformatica.uniovi.es
  - **Es distribuido**: puede delegar la responsabilidad de asignar nombres de dominio y asignar esos nombres a recursos de Internet a otras entidades
    - Designando **servidores de nombres DNS autoritativos** para cada dominio
      - El que responde a las peticiones de una zona (zone) concreta del espacio de nombres DNS (¡el boss de esa zona! ☺)
    - Los administradores de red pueden **delegar la autoridad** sobre subdominios a otros servidores de nombres
    - Por tanto, es un servicio distribuido y tolerante a fallos para evitar usar una única BD central grande
- **Un servidor de nombres DNS almacena los registros DNS de un dominio**
  - Responden consultas a su base de datos de nombres
  - Verás muchos más detalles sobre los DNS en ASR
    - Aquí solo necesitamos entender los conceptos básicos sobre cómo funciona para continuar
    - Acuérdate de la herramienta `nslookup` de ASR

Domain Name System (DNS): Cosas a recordar

- **El sistema de nombres de dominio o DNS permite acceder a máquinas remotas mediante un nombre fácil de recordar**
  - En lugar de su IP única
  - El nombre de un sistema remoto se denomina **nombre de dominio**
  - Por tanto, DNS fue diseñado para traducir un nombre de dominio en una dirección IP
  - El proceso de traducción inversa (IP a nombre de dominio) **también se puede implementar**
  - Funciona con IPv4 e IPv6
- **El proceso de traducción es automático y transparente**
  - Eso es lo que hace posible Internet hoy en día
  - Como controla todos los sitios a los que navegas, **puede ser un elemento de seguridad**
    - Evitando que navegues a sitios que **se sabe que son maliciosos** de antemano. Ej.: NextDNS
- **Para ser escalable, no depende de un solo archivo o servidor**
  - Sino de muchos en todo el mundo
  - Los servidores DNS tienen una organización jerárquica
  - Y de ahí la forma separada por puntos de los nombres que resuelven

Nombres de dominio

- **Los nombres de dominio deben estar registrados en ICANN**
  - Internet Corporation for Assigned Names and Numbers
- **Normalmente a través de una empresa que funciona como intermediario**
  - Por ejemplo, a la que le contratamos el hosting para una web
- **Los dominios de nivel superior se denominan TLD**
  - Son los `.com`, `.edu`, `.org`..., y muchos otros que solemos ver al final del **Fully Qualified Domain Name** (FQDN)



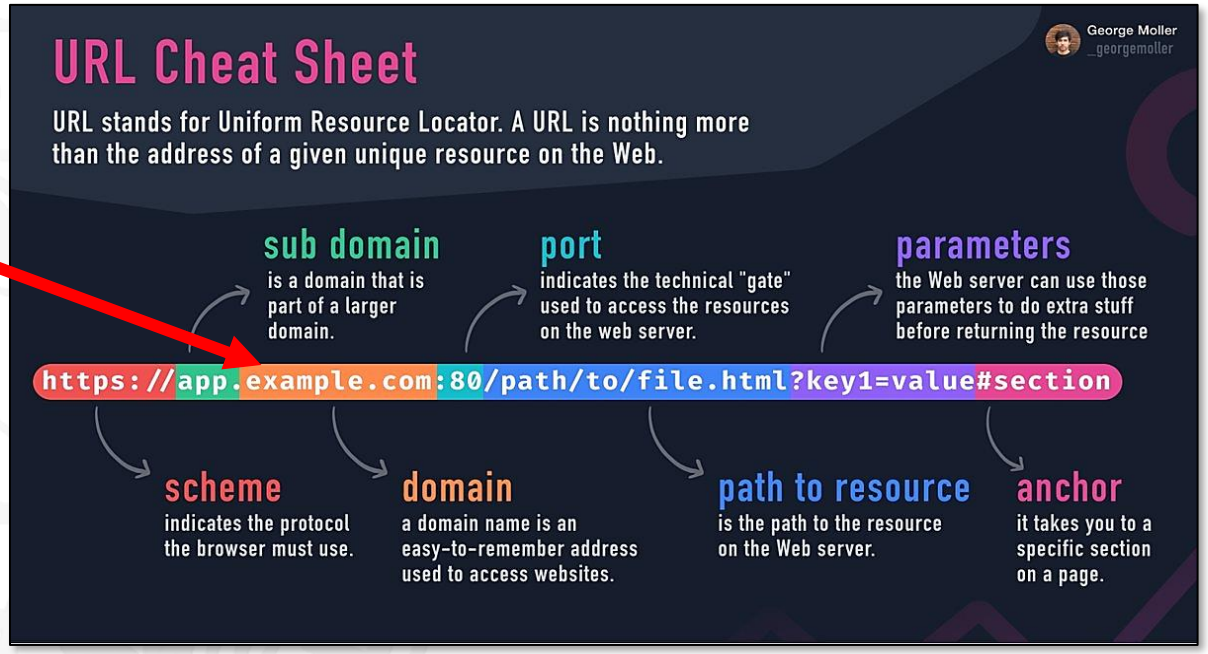
Fuente: https://www.computerhope.com/jargon/d/dns.htm

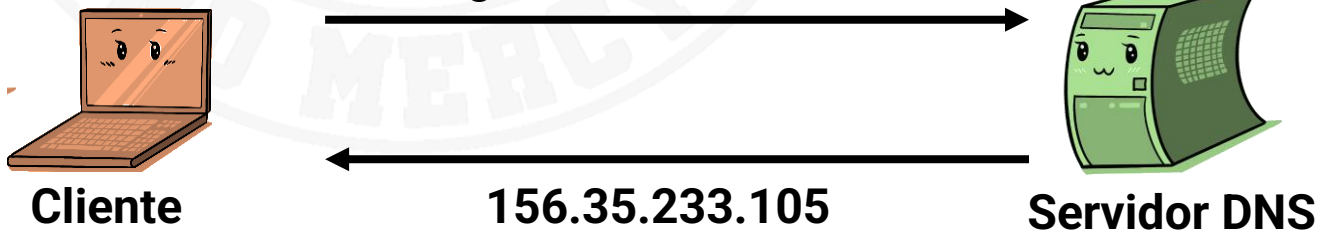
Nombres de dominio

- **Como hemos dicho, DNS funciona de forma jerárquicamente**
  - Los dominios de nivel superior o TLD pueden tener varios subdominios debajo de ellos
  - En el diagrama anterior, `.mit` y `.craiglist` forman parte de los dominios `.edu` y `.org` de nivel superior, respectivamente
  - Estos se denominan **subdominios** (SLD, Second-Level Domain)
    - Dominios que forman parte de un dominio más grande
    - En el ejemplo, `mit` y `craiglist` son dominios de segundo nivel bajo su propio TLD
  - Y, por supuesto, debajo de estos SLD puede haber **muchos otros subdominios**
    - En el ejemplo, debajo de `.com`, tenemos `computerhope.com` y `support.computerhope.com`
  - Esto subdivide el dominio en partes
    - La parte más a la izquierda es siempre **la más específica**
    - Mientras que la parte más a la derecha **es la más general**
    - **Léelos de derecha a izquierda, separando las secciones por '.'**
      - Ej.: `support.computerhope.com`: Comercio (`com`) llamado "Computer Hope" (`computerhope`), sección de soporte (`support`)
- **El servicio WHOIS te da información de un dominio y de su titular**

Cómo funciona un DNS

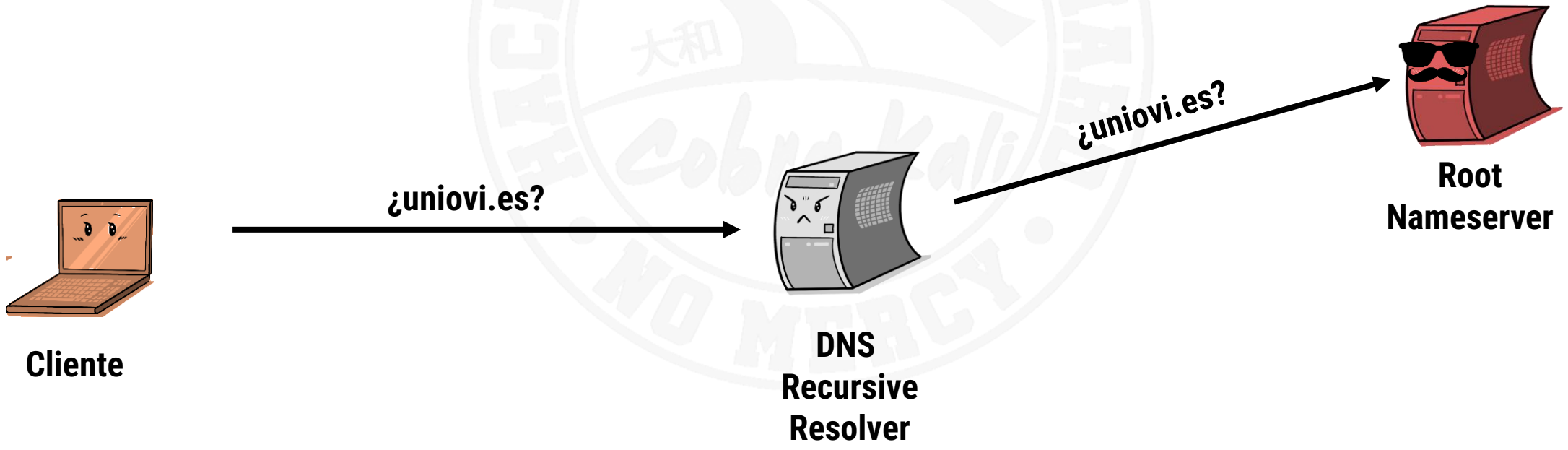
- **¿Qué pasa cuando escribes una URL y das Intro?**
  - Desde el punto de vista del cliente, no mucho
    - Pide la IP del **nombre de dominio** a su DNS
  - Si ese servidor DNS conoce la IP asociada a ese nombre, simplemente la devuelve
  - La parte complicada comienza cuando el servidor DNS **no** conoce esta IP
    - Tiene una cantidad limitada de espacio para almacenar estas asociaciones...





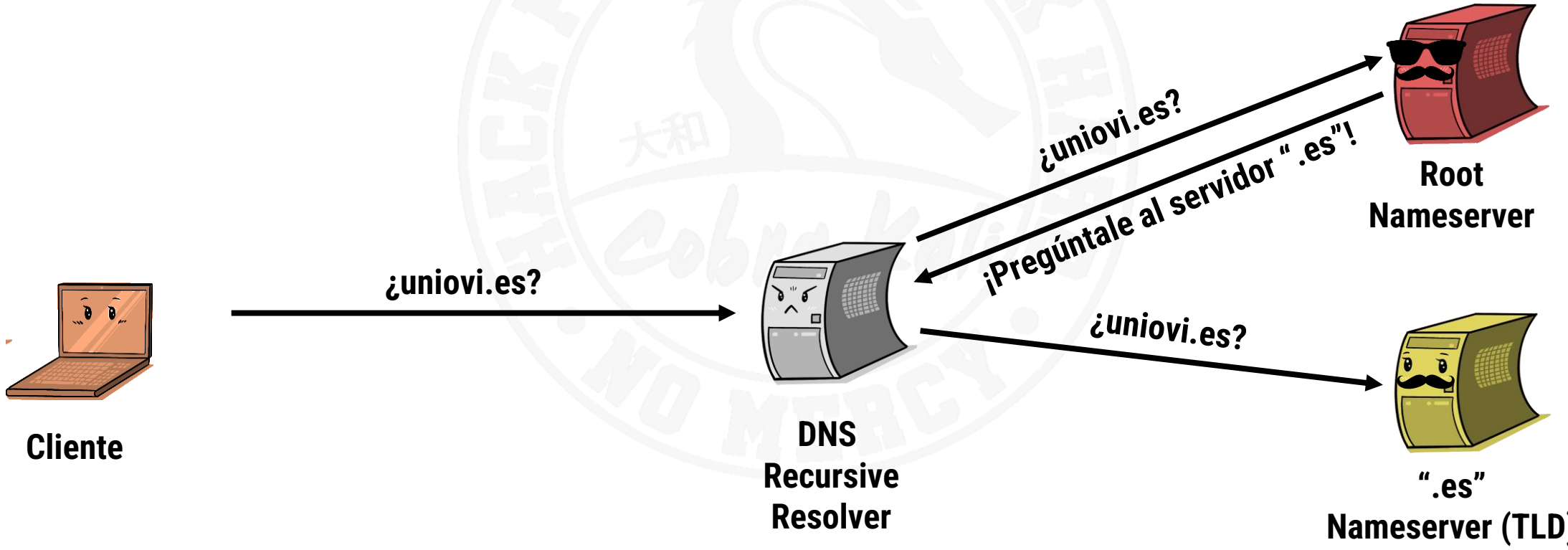
Cómo funciona un DNS

- **Si el servidor DNS no conoce la IP del nombre de dominio, utiliza un proceso de resolución recursiva (DNS Recursive Resolver) para buscarla**
  - Primero el DNS Recursive Resolver envía una consulta DNS a un **Root Nameserver**
  - Sabe la dirección IP de los **Root Nameserver**



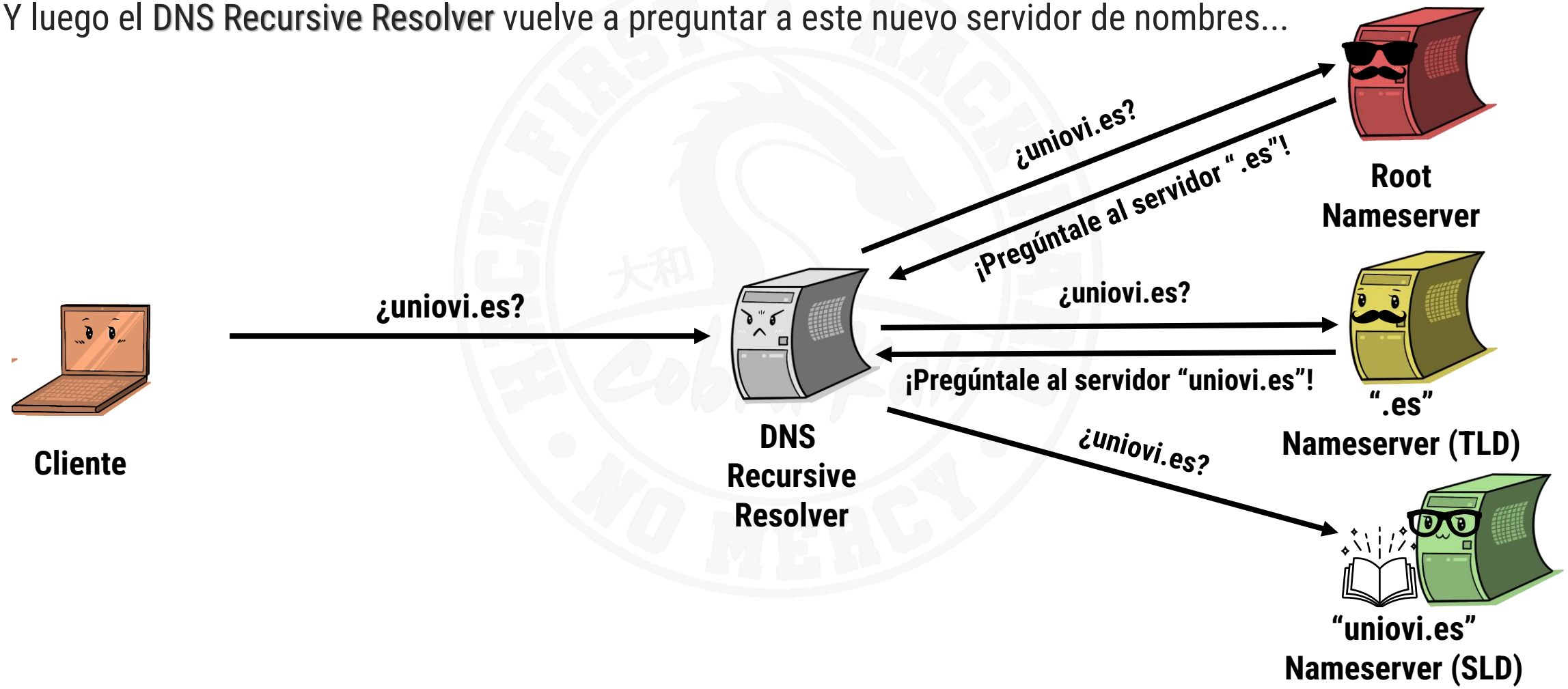
Cómo funciona un DNS

- **A continuación, el Root Nameserver responde con la dirección IP del servidor de nombres TLD correspondiente**
  - El servidor de nombres "`.es`" en nuestro caso
  - Y el DNS Recursive Resolver luego le pide a este nuevo servidor de nombres el nombre de dominio



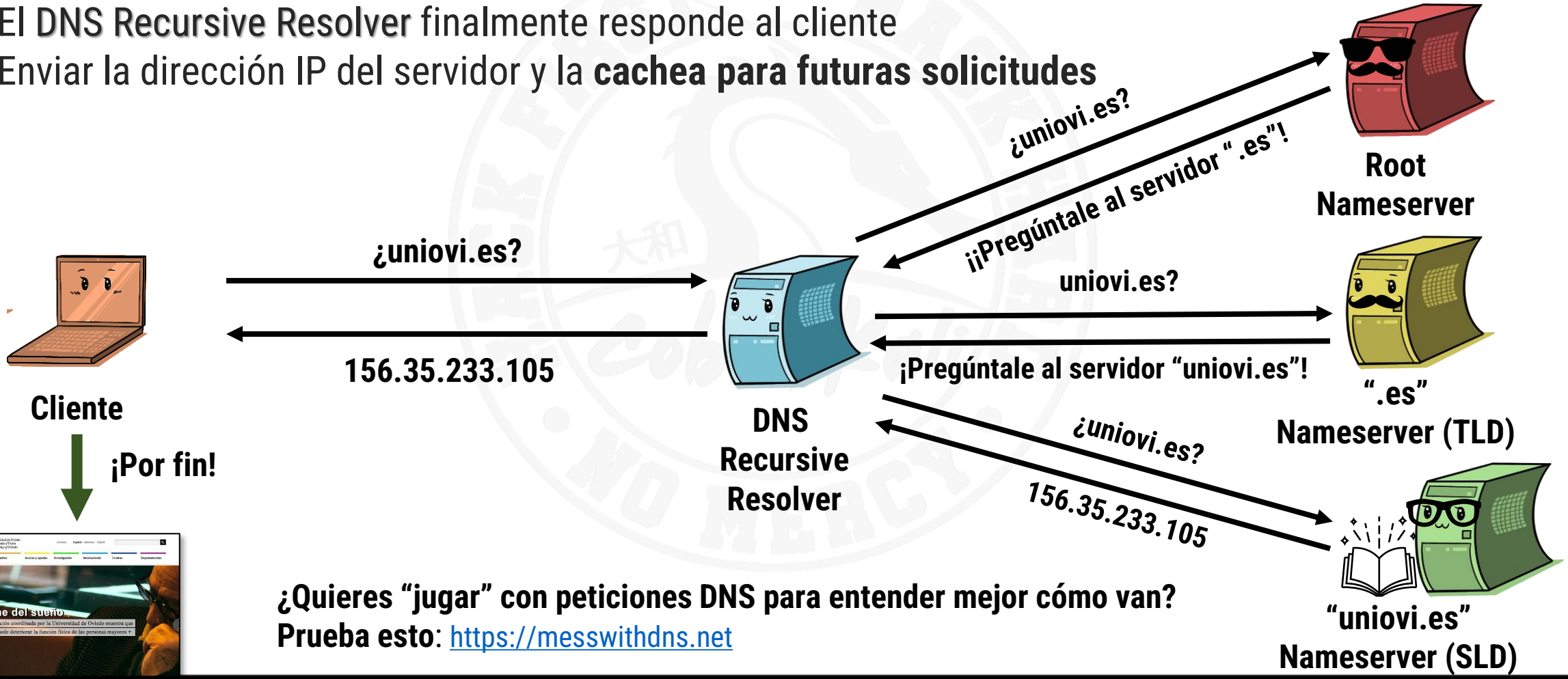
Cómo funciona un DNS

- El servidor de nombres TLD responde con la dirección IP de un servidor de nombres de dominio SLD adecuado (el servidor de nombres "`uniovi.es`")
  - Y luego el DNS Recursive Resolver vuelve a preguntar a este nuevo servidor de nombres...



Cómo funciona un DNS

- Este servidor de nombres de dominio SLD está marcado como **autoritativo** para `uniovi.es`
  - ¡Por lo que responde con la dirección IP del servidor por fin!
  - El DNS Recursive Resolver finalmente responde al cliente
  - Enviar la dirección IP del servidor y la **cachea para futuras solicitudes**



¿Quieres "jugar" con peticiones DNS para entender mejor cómo van?
Prueba esto: https://messwithdns.net

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Comprendes que, sin un DNS, tendríamos que recordar cada IP de cada máquina, y que eso no es humanamente posible*
  - *Entiendes que si un DNS es jerárquico y descentralizado es precisamente para ser resistente a fallos de partes de su infraestructura*
  - *Sabes que es un servidor de nombres DNS autoritativo*
  - *Entiendes que, si un servidor DNS no sabe la IP de una máquina, delega en otras siguiendo un algoritmo conocido*
  - *Sabes que es el concepto de TLD y de SLD*
  - *Comprendes qué parte de una URL realmente se usa en una búsqueda DNS*
  - *A consecuencia de todo lo anterior, entiendes que, si alguien consiguiese intervenir en el sistema de DNS mundial para controlar las respuestas, Internet caería*

< Ir al Índice

MÁQUINAS COMO OBJETIVO

Máquinas vistas desde distintas perspectivas

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿Qué te vas a encontrar en este bloque?

En este bloque aprenderás

- Qué es y qué significa un **puerto** de una máquina
- Qué es y qué significa un **servicio** en una máquina
- Qué es y qué significa un **protocolo**
- Cómo se puede usar la **herramienta nmap** para ver todo lo anterior
- Cuál es el problema básico de seguridad de una red **Wifi pública**

¿Qué es una máquina vista desde fuera?

- Una vez contactamos con la máquina objetivo, tenemos una visión **externa** de lo que ofrece a los usuarios
- Está compuesta por
  - **Puertos**, que tienen **servicios** que se comunican con los potenciales clientes
  - Usando ciertos **protocolos de comunicación**
    - Los protocolos son como las acciones que podemos hacer en una red social
    - Podemos enviar mensajes en diferentes formatos: textos, imágenes, memes, gifs animados, likes, retweets...
    - Para comunicarse con otros, las redes sociales tienen un protocolo de formatos de mensajes permitidos
    - Este concepto es el mismo que lo que pasa con máquinas
- Repasemos estos conceptos

Puertos de red

- **Un puerto completa el acceso a un servicio ofrecido por una máquina**
  - ¡La misma máquina puede ofrecer muchos servicios! (**uno por puerto**)
  - La IP es la dirección de la máquina a la que nos conectamos
  - El puerto decide **qué servicio** (de todos los que ofrece la máquina) de esa dirección IP se va a usar
    - "Se llegar al aeropuerto, pero al final, tendré que elegir un vuelo concreto" ☺
    - Por ejemplo, si el sitio web de nuestra escuela está en la IP `156.35.94.1`
      - Para navegar por el necesitamos un cliente adecuado que se conecte al puerto `80` o al `443` (servicios HTTP(S))
    - Y para conectarse de forma segura como usuario, usar el puerto 22 (**servicio SSH**)
- **Hay 65.536 puertos diferentes posibles en una máquina**
  - Los primeros 1.024 se conocen como "**puertos comunes**", **reservados para servicios típicos**
    - El resto se puede utilizar para crear programas que "escuchen" conexiones y den diversos servicios
  - Los números de puerto más utilizados aparecen en la siguiente diapositiva
  - "**Abrir un puerto**" significa ofrecer un servicio a máquinas de fuera desde la tuya
    - Por ejemplo: servidor web, servidor Minecraft ...
  - **¡No se pueden abrir puertos bajo CG-NAT! (¡cuidado!)**

Acerca de los puertos...

Seguridad de Sistemas Informáticos

- **Los puertos > 1024 "normalmente" tienen los servicios de la imagen**
  - Pero a diferencia de los reservados, no es obligatorio
  - Usa esta lista como una aproximación
- **Los puertos se pueden inspeccionar con `nmap`**
  - https://nmap.org/
  - También nos permite saber
    - Qué servicio está "detrás" de cada puerto
    - Si está activo (envía/recibe solicitudes)

Common Ports

packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
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	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

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

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

by Jeremy Stretch v1.1

SERVICIOS

- **Programas** que se ejecutan asociados a un puerto de red
  - Ellos "escuchan" en ese puerto (¿el qué? Peticiones de clientes en otras máquinas, claro ☺)
  - Son procesos, como los que viste en SO
- Estos programas se ejecutan en el equipo de destino y esperan las conexiones entrantes de clientes
  - Cuando un cliente se conecta a ellos y utiliza el protocolo de comunicación adecuado, el servicio procesa la solicitud del cliente y envía una respuesta
  - O un error si la solicitud no es válida
    - O contiene cualquier tipo de datos / comandos inesperados ...
- De esta manera, cualquier máquina puede proporcionar un servicio a otras máquinas
- ¡Y esta es la base de las comunicaciones entre máquinas hoy en día! ☺

PROTOCOLO DE COMUNICACIONES

- **Sistema de reglas que permiten a dos o más entidades de un sistema de comunicaciones transmitir información (Ej.: protocolos TCP, UDP)**
  - Define las reglas, la sintaxis, la semántica y la sincronización de la comunicación
  - Y las posibles formas de recuperarse de errores (¿recuerdas FCR?)
- **Los sistemas de comunicación usan formatos bien definidos para intercambiar mensajes**
  - Cada mensaje tiene un significado exacto, destinado a obtener una respuesta de una gama de posibles respuestas predeterminadas para cada situación
  - El comportamiento especificado en el protocolo suele ser independiente de su implementación
    - Los protocolos suelen ser estándares aprobados
- **Para describir diferentes aspectos de una sola comunicación, generalmente son necesarios varios protocolos**
  - Un grupo de protocolos diseñados para trabajar juntos se conoce como **protocol suite**
  - Cuando se implementan en software, son una **protocol stack**

NMAP PARA HACER RECONOCIMIENTO DE RED

- Normalmente el 1er paso de una operación de pentesting / CTF es el **Reconocimiento**
- Determina cuántas máquinas están "vivas"
  - Capaces de recibir tráfico
  - Este paso aún no identifica necesariamente los puertos / servicios
- Una vez hecho esto, cada máquina interesante se investiga más a fondo.
  - Este es el segundo paso, **Enumeración** (**Tema 5**)

Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 1: Reconnaissance (Basic)

https://nmap.org/

GENERAL USAGE

nmap [Scan Type(s)] [Options] {target specification}

NOTES

Target specifications can be host names, IP addresses, ranges, networks, etc. (scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254)

Use these options to locate "alive machines" (sometimes only returns that, sometimes they also return some port / service information)

TARGET SPECIFICATION

- **-iL <inputfilename>**: Input from from file a list of hosts/networks
- **-iR <num hosts>**: Choose random targets
- **--exclude <host1[,host2][,host3],...>**: Exclude hosts/networks
- **--excludefile <exclude_file>**: Exclude list from file

RECONOISSANCE EXAMPLES

- *nmap -sn scanme.nmap.org*
- *sudo nmap -PS22,80 scanme.nmap.org*
- *sudo nmap --traceroute scanme.nmap.org*

```
operario@kali:~$ nmap -sn 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:38 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00085s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

```
operario@kali:~$ sudo nmap -PS22,80 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:42 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

HOST DISCOVERY OPTIONS (WAYS TO CHECK "ALIVE" MACHINES)

- **--dns-servers <serv1[,serv2],...>**: Specify custom DNS servers
- **-n/-R**: Never do DNS resolution/Always resolve [default: sometimes]
- **-PE/PP/PM**: ICMP echo, timestamp, and netmask request discovery probes
- **-Pn**: Treat all provided hosts as online -- skip host discovery
- **-PO[protocol list]**: IP Protocol Ping
- **-PS/PA/PU/PY[portlist]**: TCP SYN/ACK, UDP or SCTP discovery to given ports
- **-sL**: List Scan - simply list targets to scan
- **-sn**: Ping Scan - disable port scan
- **--system-dns**: Use OS's DNS resolver
- **--traceroute**: Trace hop path to each host

PONIÉNDOLO TODO JUNTO…

- **Los puertos son extremos de comunicación**
  - Las conexiones físicas e inalámbricas terminan en puertos de un dispositivo
  - Identifican un **proceso** o un **servicio** de red
  - Multiplexando los servicios de una sola dirección IP
  - Un puerto siempre está asociado a una IP y al protocolo de la comunicación
  - Los protocolos más comunes son **TCP** (Transmission Control Protocol) y **UDP** (User Datagram Protocol)
  - Los tres forman la **dirección de red de destino o de origen** de un mensaje
    - Por ejemplo: `156.35.94.1:80/tcp` (servidor web típico)
  - Motores de búsqueda como Shodan o Censys hacen lo mismo que `nmap` **con máquinas expuestas en Internet**

```
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 972 filtered ports
PORT      STATE  SERVICE         VERSION
22/tcp    open   ssh             OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Lin
ux; protocol 2.0)
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open   http            Apache httpd 2.4.7 ((Ubuntu))
110/tcp   closed pop3
111/tcp   closed rpcbind
113/tcp   closed ident
135/tcp   closed msrpc
143/tcp   closed imap
199/tcp   closed smux
256/tcp   closed fw1-secureremote
554/tcp   closed rtsp
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
1025/tcp  closed NFS-or-IIS
1720/tcp  closed h323q931
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
4446/tcp  closed n1-fwp
5900/tcp  closed vnc
8080/tcp  closed http-proxy
8090/tcp  closed opsmessaging
8888/tcp  closed sun-answerbook
9929/tcp  open   nping-echo       Nping echo
10617/tcp closed unknown
31337/tcp open   tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

¡¡Mamma Mia!! ¡Esto no puede llegar a buen puerto!

- **Nintendo® recomendó esto para permitir el juego en red en Splatoon® y otros juegos**
  - Esto significa abrir el acceso en tu router a cualquier persona a todos los servicios posibles
    - A la dirección IP de la consola Switch®
    - Y solo para conexiones que utilizan el protocolo UDP
  - ¡Todos los servicios expuestos por la Switch® son visibles desde el exterior!
- **¿Qué sucede si esta IP se asigna a través de DHCP? (caso típico, por cierto...)**
  - Mañana otro dispositivo distinto puede usarla, y alguien puede tener acceso a todos sus servicios...
  - **¡Es un consejo de seguridad MUY MALO!**

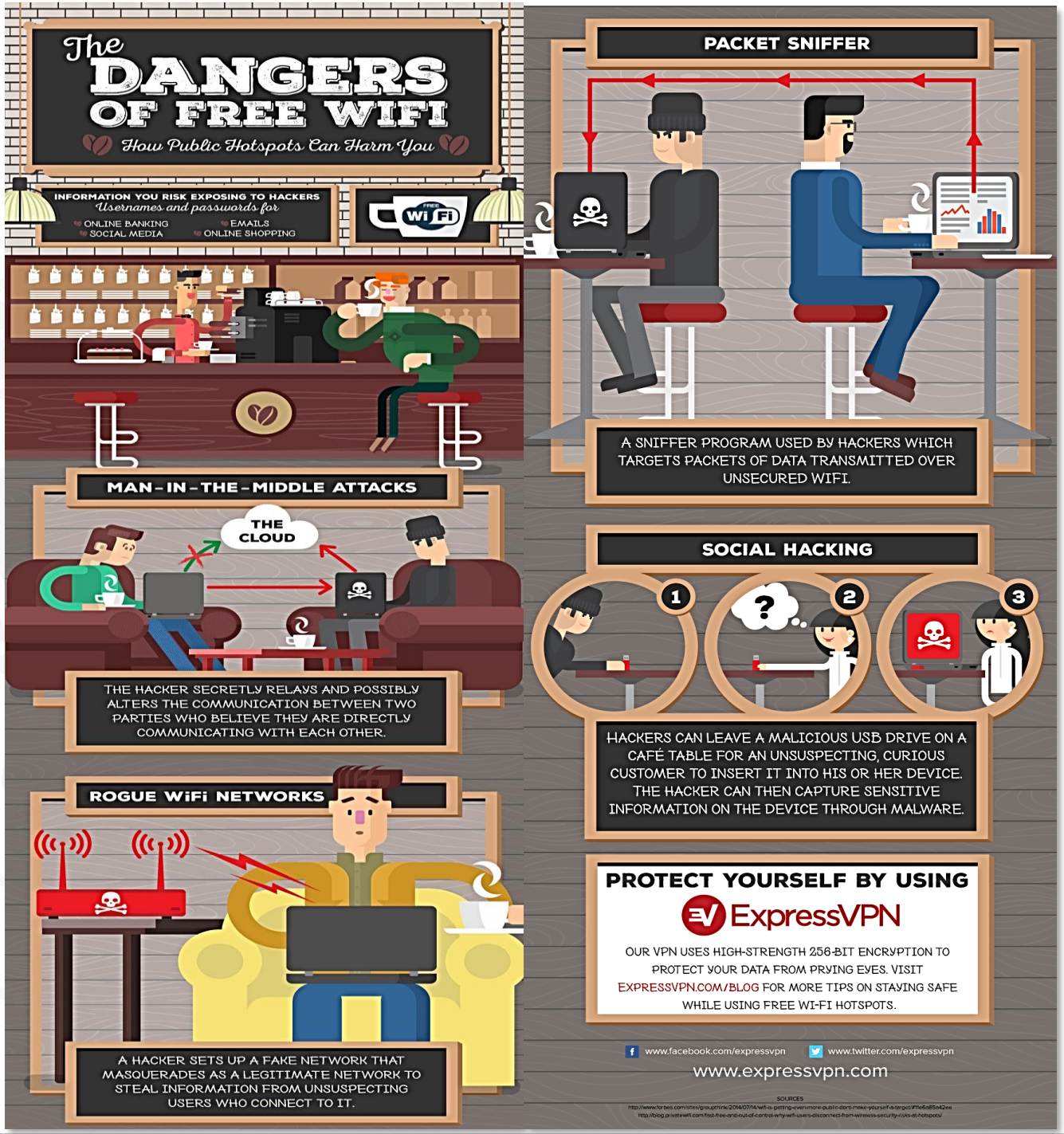
On a PC or smart device

1. Access your router's settings.
2. Locate the Port Forwarding settings. While the location will vary from router to router, it will typically be located in an area titled firewall, virtual server, security, or applications and gaming.
3. When asked for an application name, you can enter any word (Nintendo Switch, etc.)
4. Within the port range, enter the starting port and the ending port to forward. For the Nintendo Switch console, this is port **1 through 65535**.
5. Set the protocol as UDP.
6. Enter the IP address you assigned to the console.
7. Check Enable or Apply to turn on this rule.
8. Save the changes to the router.

¿Qué pasa con las redes Wi-Fi?

Seguridad de Sistemas Informáticos

- **No son diferentes de las redes cableadas en estructura**
  - IPs, puertos, servicios...
- **¡Pero están expuestas a más amenazas!**
  - Tus datos viajan "libres" en todas las direcciones en un espacio abierto
  - Podrían ser leídos por cualquier persona en tu misma red Wi-Fi
    - Con un rastreador de paquetes (sniffer)
    - Para analizar y descifrar tu tráfico o alterarlo
  - ¡Especialmente en redes Wi-Fi gratuitas!
    - **EVITA el Wi-Fi gratuito a toda costa**
    - Utiliza siempre tráfico cifrado (SSH, HTTPS) o VPNs (**Tema 5**)



¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Sabes lo que significa un puerto, el límite de puertos que una máquina puede tener y que significa abrir uno*
  - *Sabes distinguir entre puertos reservados y no reservados*
  - *Entiendes el concepto de servicio "escuchando" en una máquina*
  - *Entiendes el concepto de protocolo como reglas estrictas que se establecen para la comunicación entre determinados servicios*
  - *Entiendes como nmap te permite ver puertos y servicios en funcionamiento en una máquina, así como los protocolos que usan*
  - *Comprendes porque una red Wifi pública es peligrosa para tus datos*

< Ir al Índice

Cuando los usuarios son el objetivo

Ataques cuyo objetivo es humano

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

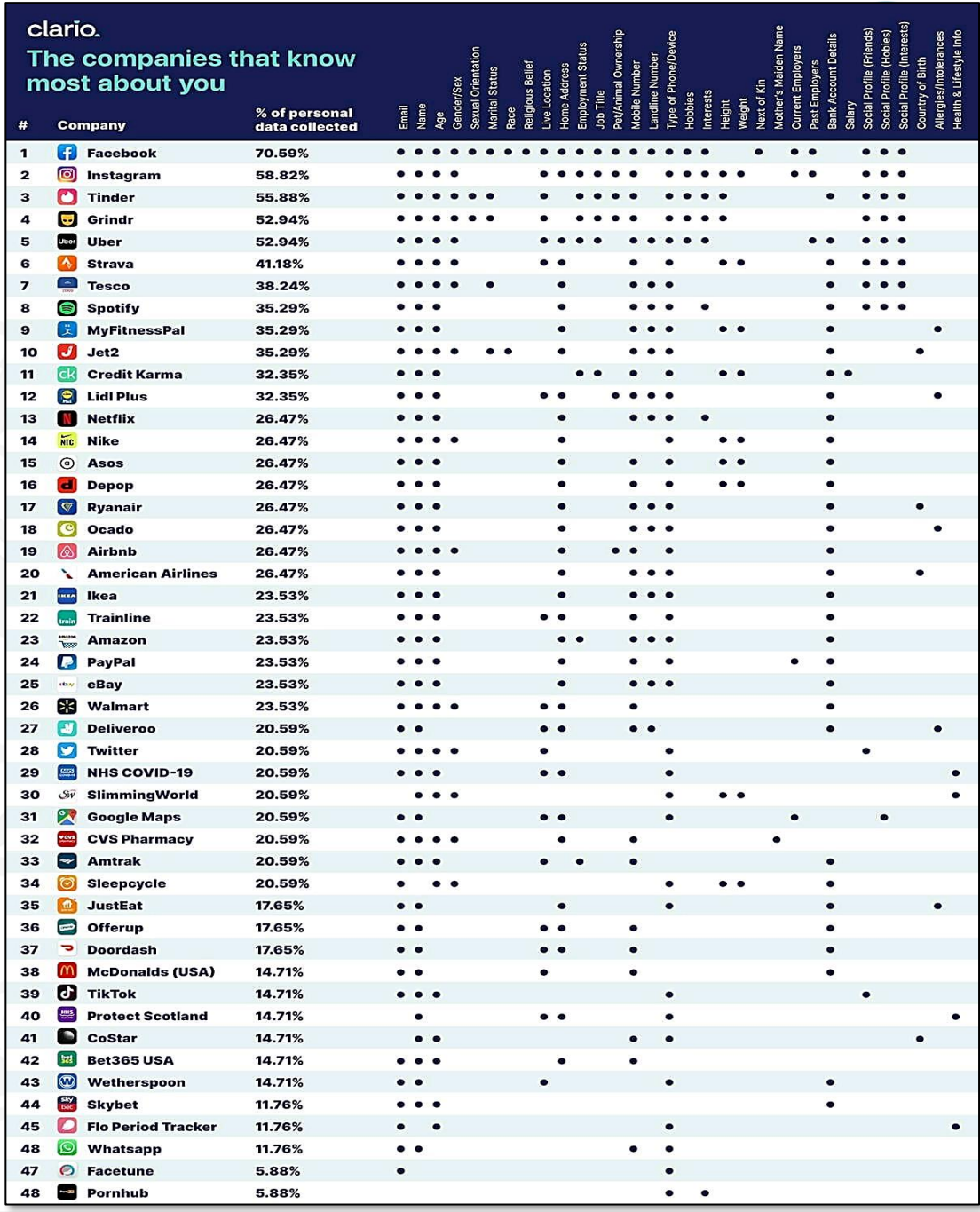
¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Por qué lo que haces mientras navegas, tus gustos, tus preferencias, etc. (en definitiva, tu privacidad) **son moneda**
- Qué navegadores respetan más la **privacidad**
- Que son los conceptos de spam, phishing, hoax, watering hole, drive-by download y APT
- Qué es el **OSINT** como concepto

PRIVACIDAD

- El historial de navegación de los usuarios, su comportamiento, sus características físicas y sociales, ... son muy interesantes para las empresas publicitarias
  - Y otras empresas que procesan estos datos con fines de lucro
  - **Si un servicio es "gratuito", ¡tus datos son el pago!**
- La tabla muestra los datos de usuario recopilados por servicios conocidos
  - La única forma de evitarlo es configurar el navegador con extensiones que limiten a las técnicas de adquisición de datos
  - Algunas herramientas (Ej.: Blacklight) dan una idea clara de **cómo de extendida está esta práctica**



➢ Ejercicio **L2B4_PRIVACIDAD**

NAVEGADORES Y PRIVACIDAD

Seguridad de Sistemas Informáticos

- Los navegadores también recopilan datos de usuario y navegación mientras los usan
- Esta tabla muestra diferentes pruebas de privacidad
  - Para ayudarte a elegir el más adecuado si te preocupan estos temas
- No necesitas entender las pruebas en sí, solo la cantidad que cada navegador pasa

PrivacyTests.org News About

No. 3 — *Open-source tests of web browser privacy.* — *Updated 2021-11-02*

✓ = Passed privacy test ✗ = Failed privacy test – = No such feature

Desktop Browsers (click anywhere for more info)	Brave 1.31	Brave 1.31 Private	Brave 1.31 Tor	Chrome 95.0	Chrome 95.0 Private	Edge 95.0	Edge 95.0 Private	Firefox 93.0	Firefox 93.0 Private	Opera 80.0	Opera 80.0 Private	Safari 15.1	Safari 15.1 Private	Tor 10.5	Vivaldi 4.3	Vivaldi 4.3 Private
State Partitioning tests																
AltSvc	✗	✗	–	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
blob	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
BroadcastChannel	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	–	–	✓	✗	✗
CacheStorage	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
cookie	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
CSS cache	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗
favicon cache	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗
H1 connection	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗
H2 connection	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗
H3 connection	✗	✗	–	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
HSTS cache	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗
indexedDB	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
localStorage	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
locks	✓	✓	✓	✗	✓	✗	✗	–	–	✗	✓	–	–	–	✗	✓
prefetch cache	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	–	–	✓	✓	✗
ServiceWorker	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
SharedWorker	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	–	–	✓	✗	✓
TLS Session ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web SQL Database	✓	✓	✓	✗	✓	✗	✗	–	–	✗	✓	–	–	–	✗	✓
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Navigation tests																
document.referrer	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
sessionStorage	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓
window.name	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗
HTTPS tests																
Insecure website	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Upgradable address	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Upgradable hyperlink	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Upgradable image	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓
Upgradable script	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

SPAM

- **E-mails fraudulentos / no deseados enviados masivamente con varios fines**
  - **Sitios publicitarios** de productos que normalmente no se encuentran en tiendas web típicas, o relacionados con actividades ilegales / legales
  - **Estafas** (estafas nigerianas, crowdfundings fraudulentos, mulas, timos de pago por adelantado...)
  - Propagar **malware**
  - Difundir campañas de **phishing**
  - ... *(muchas, muchas formas nuevas de fraude aparecen constantemente ☹)*
- **Además de los efectos potenciales del payload del email, también podrían**
  - Saturar (y por lo tanto realizar un DoS) redes / servidores de correo electrónico
    - Ej.: bombas zip, https://es.wikipedia.org/wiki/Bomba_zip
  - Iniciar cualquier clase de estafa (scam) o fraude (phishing)
- **Muchas veces se usan cuentas robadas por filtraciones de datos de empresas para propagar campañas de spam de manera más creíble**
  - El servicio Have I been pwnd? (https://haveibeenpwned.com/) permite **descubrir estas filtraciones**

PHISHING / SPEAR PHISHING

- **Mensajes (e-mail, WhatsApp, Telegram...) cuya fuente parece ser legítima (banco, empresa...) pero se crean con un efecto malicioso para engañar a los usuarios**
  - Robar información privada del usuario (inicios de sesión, contraseñas, tarjetas de crédito, cuentas de correo electrónico...), ejecutar malware...
  - Esta información es clave para cometer otros tipos de fraude más adelante
  - Los intentos de phishing son comunes durante la navegación normal (anuncios/scripts maliciosos...)
    - Un "**browser fortificado**" evita muchos (bloqueador de ads/scripts, Google Safe Browsing, DNS seguro...)
- **Spear phishing: intentos de phishing dirigidos a individuos o empresas específicas**
  - Los atacantes suelen recopilar y usar información personal sobre su objetivo para aumentar el éxito
  - Ej.: El Threat Group-4127 (Fancy Bear APT group, Rusia) usó tácticas de esta clase para atacar cuentas de correo electrónico vinculadas a la campaña presidencial de Hillary Clinton en 2016
- **El phishing es un tipo de fraude**
  - Hay una enorme cantidad de tipos de fraude, imposibles de cubrir en este curso
  - La Universidad de Oviedo ofrece **un curso gratis contra el ciberfraude** que complementa a esta asignatura: https://uniovix.uniovi.es/course/view.php?id=62

HOAXES

- **Mensajes o publicaciones no deseados con información falsa / sesgada de varios tipos**
  - Enviada a través de correos electrónicos, redes sociales (Twitter, Facebook...), aplicaciones de mensajería instantánea (WhatsApp, Telegram...), SMS...
  - También presente en algunos periódicos (desinformación intencionada o noticias falsas)
- **Principalmente tienen el objetivo de "cosechar" cuentas de correo electrónico activas (que se lean, vamos)**
  - Que son objetivos posteriores de ataques de phishing / spam
  - También pueden saturar el sistema de correo electrónico de una empresa
- **A menudo se utilizan también para dañar la reputación o la imagen pública de organizaciones / grupos / individuos**
- **Páginas como MalditoBulo (https://maldita.es/malditobulo/) pueden ayudarnos a descubrir algunos**

WATERING HOLE

- **Estrategia de ataque en la que la víctima pertenece a un grupo de usuarios concreto (organización, industria, región...)**
  - El atacante adivina u observa **qué sitios web utilizan a menudo miembros de este grupo**
  - Luego se dirige a ellos **para infectarlos (a uno o más) con malware**
  - Eventualmente, algún miembro del grupo objetivo se infecta
  - Y con ello **se puede lanzar un ataque totalmente personalizado**
    - Ej.: hacks que buscan información específica y que solo atacan a usuarios provenientes de direcciones IP concretas
    - Los ataques se crean a partir de toda la información que se ha obtenido sobre los miembros del grupo
- **Esto hace que estos ataques sean más difíciles de detectar e investigar**
- **Más información:** https://en.wikipedia.org/wiki/Watering_hole_attack

Drive-by download (aka Descargas automáticas)

- Sitios web que **descargan e instalan spyware / malware** sin el **consentimiento o conocimiento** de su usuario
  - O bien con el consentimiento, pero sin entender las consecuencias
- **Este tipo de descargas también puede ocurrir al mostrar un adjunto de un mensaje o hacer clic en una ventana emergente**
  - La ventana emergente puede mostrar un error falso, advertencia u otra información engañosa
  - Una vez se hace clic, la descarga se inicia y el ataque se puede desplegar
- **Estos ataques pueden ser automáticos, utilizando vulnerabilidades web existentes**
  - Insertando un script que puede solicitar scripts maliciosos adicionales (con los exploits reales) a un servidor controlado por el atacante
  - Si el exploit tiene éxito, el malware puede ser ejecutado
- **Más información:** https://es.wikipedia.org/wiki/Drive-by-Download

Advanced Persistent Threat (APT)

- **Actores de amenazas ocultos** de redes informáticas que obtienen acceso no autorizado a una red y **permanecen sin ser detectados durante mucho tiempo**
  - El objetivo es colocar código malicioso personalizado en varios equipos para tareas específicas
  - Cuanto más tiempo se queden, más daño / información robada
- **Suele ser un estado, nación o un grupo patrocinado por el estado (espionaje)**
  - También puede referirse a otros grupos que realizan intrusiones dirigidas a gran escala
- **Las motivaciones son típicamente políticas o económicas**
  - Todos los principales sectores empresariales (gobierno, defensa, servicios financieros, servicios legales, industriales, telecomunicaciones ...) han registrado casos de ataques por parte de APTs
  - Con objetivos específicos, buscando robar, espiar o interrumpir
- **Algunos utilizan vectores "tradicionales"**
  - Ingeniería social (OSINT), inteligencia humana (HUMINT)... para acceder a ubicaciones físicas que habiliten ataques de red

OSINT

- **Open-Source INTelligence** (OSINT) es un conjunto de datos recopilados de fuentes públicas para ser utilizados en el estudio de un objetivo
- Según el Departamento de Defensa de EE.UU

  "Información disponible públicamente que se recopila, explota y distribuye de manera predeterminada a una audiencia apropiada, con la intención de cumplir con un requisito específico de investigación "
- Por lo tanto, es un conjunto de información pública **legalmente accesible**
  - Que se puede utilizar para averiguar ciertos datos, rutinas, estructuras, etc. de un colectivo / persona / empresa determinado
- Existen herramientas OSINT especializadas para cada fuente de datos
  - https://ciberpatrulla.com/links/
- Tendrás tu inmersión en el mundo del OSINT gracias a
  - El **Seminario 1**
  - Los **Trabajos en Grupo** de esta asignatura

OSINT

- **Se usa para seguridad nacional, policía, negocios / investigación de mercado**
- **Las fuentes de información se pueden dividir en seis categorías**
  1. **Medios de comunicación**: periódicos impresos, revistas, radio y televisión de uno o más países
  2. **Internet**: Publicaciones, **documentos** (y sus **metadatos**), blogs, foros y medios electrónicos asociados con ciudadanos específicos, como teléfonos o contenido creado por el usuario
     - También incluye YouTube, **redes sociales** y todo el material **publicado en el pasado** (Wayback Machine)
     - Es la principal fuente: Se usan motores de búsqueda para encontrar datos privados (Google Hacking)
  3. **Datos públicos gubernamentales**: informes, facturas, directorios telefónicos, revistas de prensa, charlas...
  4. **Publicaciones profesionales y académicas**: revistas, congresos, simposios, artículos académicos, tesis, proyectos...
  5. **Datos comerciales**: estudios financieros y/o industriales, bases de datos, imágenes...
  6. **Otros trabajos**: informes técnicos, preprints, patentes, artículos en proceso, documentos comerciales, artículos inéditos, boletines informativos

➢ Ejercicios **L2B1_ROBOTS**, **L2B1_METADATOS**, **L2B2_GHACK**, **L2B2_WAYBACK**

¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que, si un servicio es gratuito, tus datos son el pago*
    - *Y que esos datos se usan para mostrarte anuncios que son más relevantes para tus gustos (supuestamente)*
    - *Y que, por supuesto, es una vía de financiación muy lucrativa para las empresas*
  - *Comprender que incluso si tu servicio no es gratuito, podrían estar también obteniendo tus datos con fines lucrativos*
  - *Comprendes que es, a nivel general, el **spam***
  - *Sabes distinguir el **phishing** del **spear phishing***
  - *Sabes qué es un **hoax** y para qué se puede usar*
  - *Sabes qué es un **watering hole** y por qué se considera un ataque dirigido a un colectivo*
  - *Sabes qué es un **drive-by download** y por qué son peligrosos*
  - *Sabes qué es un APT y normalmente a qué tipo de intereses obedecen*
  - *Entiendes qué es el OSINT y cómo gracias a él todo lo que cualquier persona publique en la red puede ser usado en su contra de alguna forma*

< Ir al Índice

¿Qué es lo siguiente?

Organización de la asignatura

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

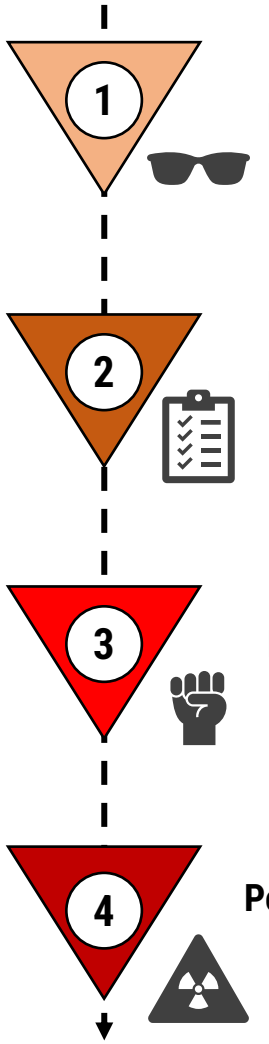
Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

DEFENSA CONTRA LAS ARTES OSCURAS...

Seguridad de Sistemas Informáticos

La "Cyber Kill Chain"



	Ataque	Defensa
Reconocimiento: La etapa de observación: los atacantes suelen evaluar la situación desde el exterior, con el fin de identificar tanto los objetivos como las tácticas para el ataque	Tema 1	Tema 5
Enumeración / Intrusión: Basado en lo que los atacantes descubrieron en la fase de reconocimiento, son capaces de entrar en sus sistemas: a menudo aprovechando el malware o vulnerabilidades de seguridad	Tema 5	Tema 3 Tema 4 Tema 5
Explotación: El acto de explotar vulnerabilidades, e introducir código malicioso en el sistema, para obtener un mejor punto de apoyo	Tema 7	Tema 2 Tema 3 Tema 4 Tema 6
Post-Explotación: Escalada de privilegios, Movimiento Lateral, Ofuscación / Anti-forenses, Denegación de servicio, Exfiltración, Escaneo de puertos, Pivotaje, Persistencia. Acciones maliciosas realizadas en el sistema explotado para aumentar los efectos de ataque o hacer el máximo daño	Tema 7	Tema 3 Tema 4

OSI LAYER	ACTIVITY	ATTACK VECTOR
7 APPLICATION LAYER	▪ User Interface and Software Application ▪ Web Browsing, Email Communication, File Transfer ▪ Protocols Like HTTP, SMTP, FTP	1 Malware Injection 2 Phishing Attacks 3 Application-Level DDoS attacks
6 PRESENTATION LAYER	▪ Data Encryption & Decryption ▪ Data Compression & Expansion ▪ Viewing Compressed Files	1 Data Encoding/Decoding Vulnerabilities 2 Malicious Code Injection 3 Format String attacks
5 SESSION LAYER	▪ Establishes, Manages and Terminates Connections ▪ Manages Session State ▪ Video Conferencing	1 Session Hijacking 2 Brute Force attacks 3 Session fixation attacks
4 TRANSPORT LAYER	▪ Ensures end-to-end data delivery ▪ TCP and UDP Protocols ▪ Error Correction	1 Man-in-the-middle attacks 2 SYN/ACK Flooding 3 TCP/IP Vulnerabilities
3 NETWORK LAYER	▪ Routing and Addressing ▪ IPV4, IPV6 and Routing Protocols [Example: OSPF] ▪ Subnet Configuration	1 IP Spoofing 2 Routing Table Manipulation 3 DDoS Attack
2 DATA LINK LAYER	▪ Frames and error detection/correction ▪ Ethernet, WI-FI and bridging	1 MAC address spoofing 2 ARP Spoofing 3 VLAN Hopping
1 PHYSICAL LAYER	▪ Physical medium and electrical/Optical Signaling ▪ Ethernet Cables, Fiber optics, etc., ▪ Radio waves in wireless links	1 Physical Tampering 2 Wiretapping 3 Electromagnetic Interference

Ethical Hackers Academy.

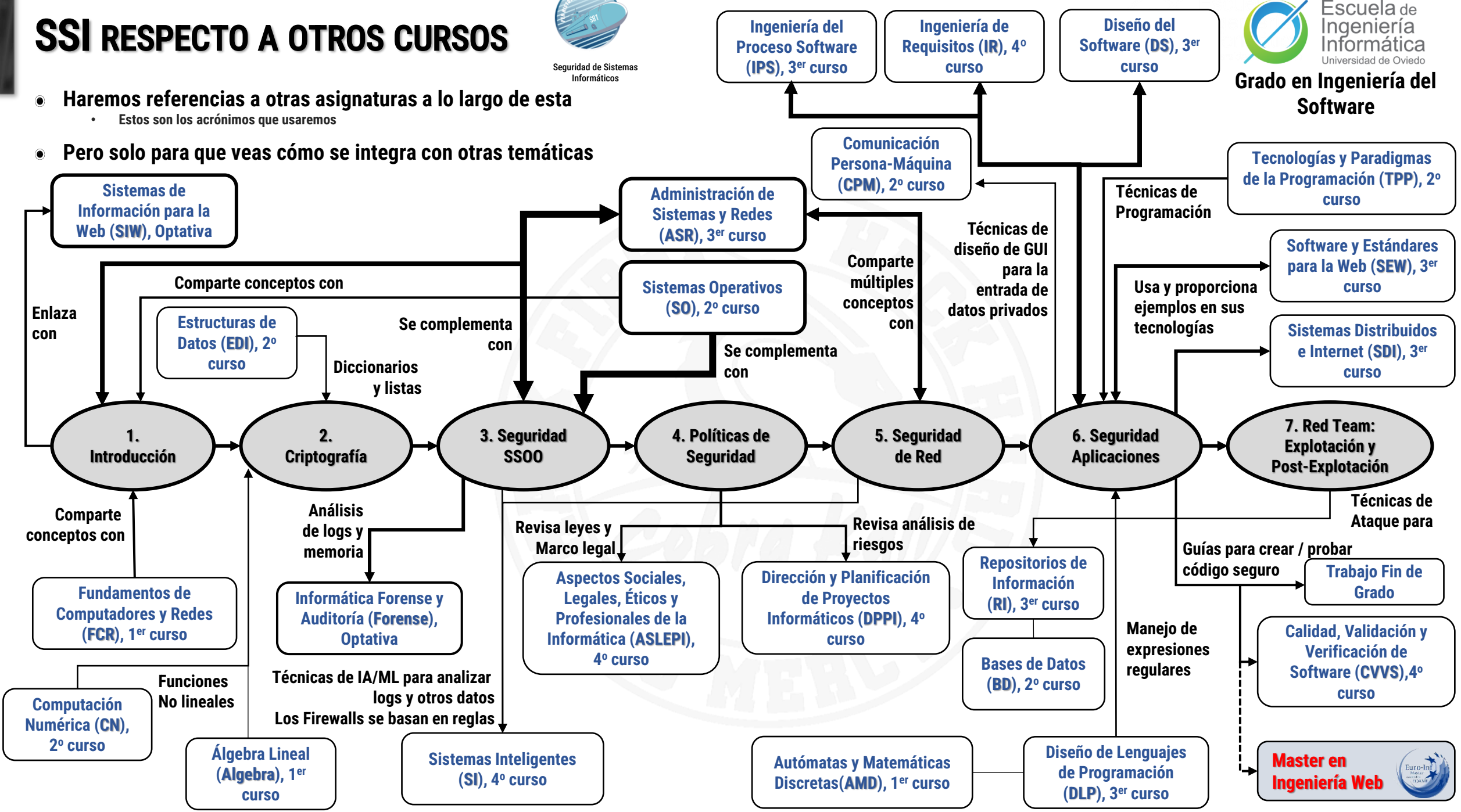
SSI RESPECTO A OTROS CURSOS

Seguridad de Sistemas Informáticos

Escuela de Ingeniería Informática
Universidad de Oviedo

Grado en Ingeniería del Software

- Haremos referencias a otras asignaturas a lo largo de esta
  - Estos son los acrónimos que usaremos
- Pero solo para que veas cómo se integra con otras temáticas



TEMA 1
INTRODUCCIÓN

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo