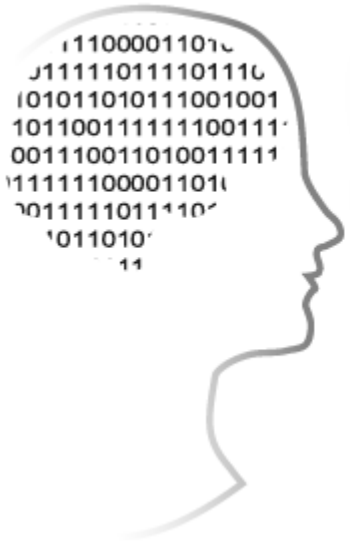
Lección 13: Seguridad en DNS



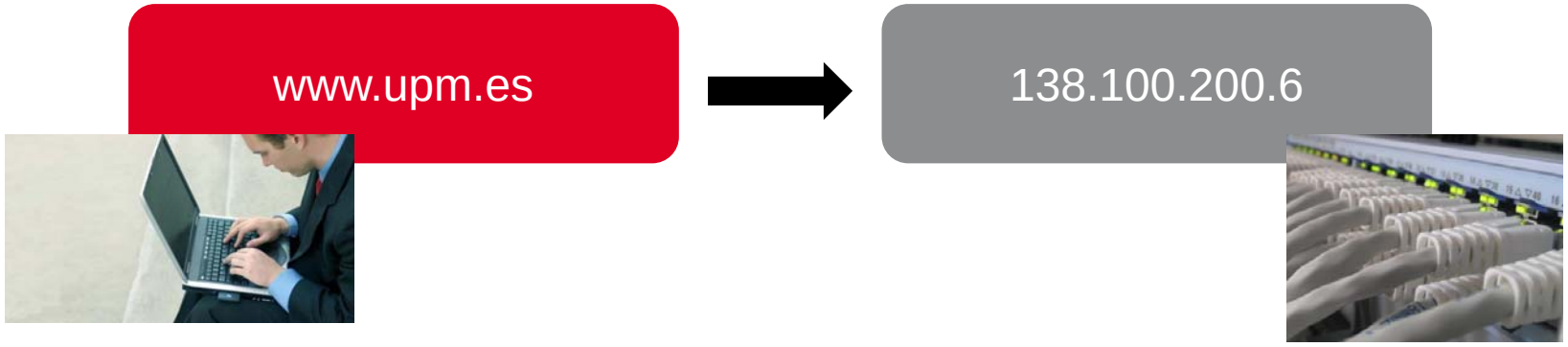
intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Javier Osuna
josuna@gmv.com
GMV – Jefe de División de Consultoría de Seguridad

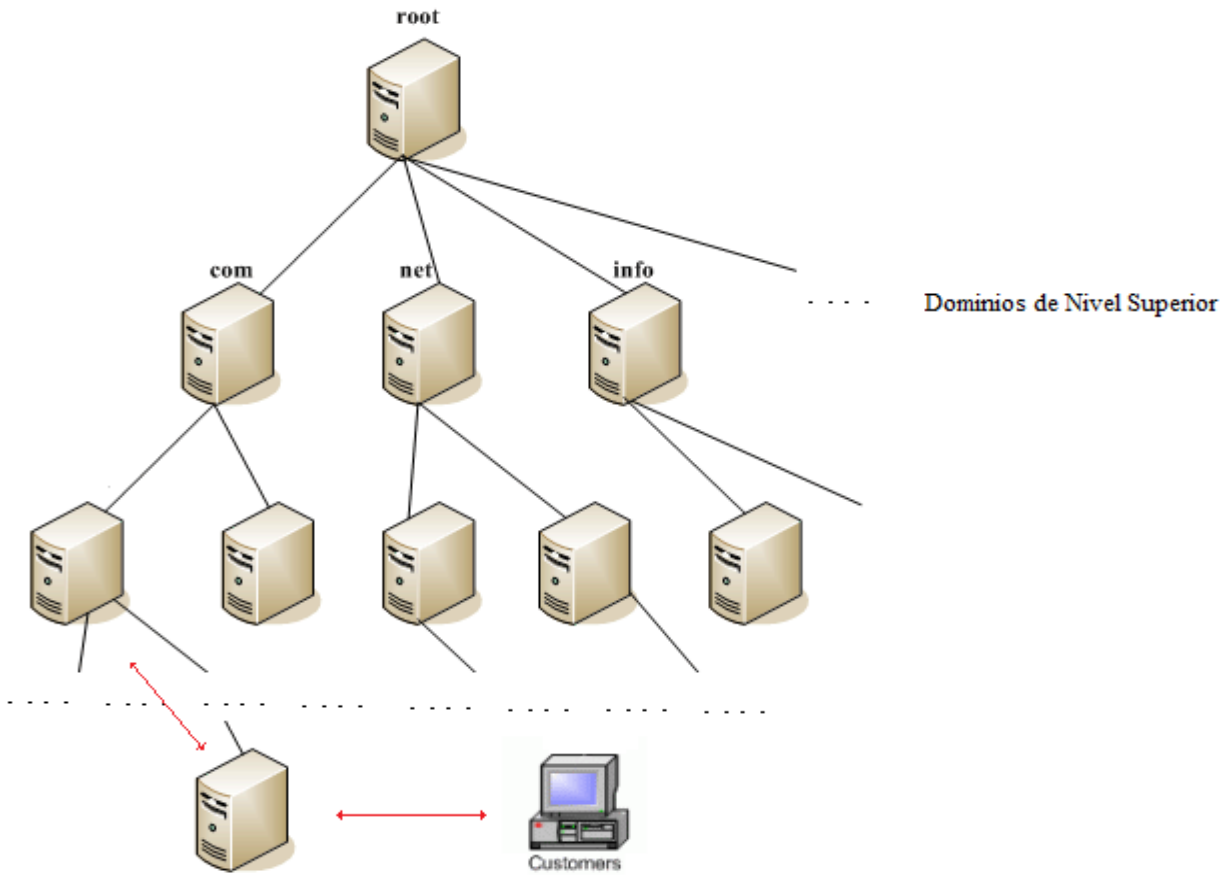
Introducción a los DNSs

Los DNSs facilitan a las personas utilizar y navegar a través de Internet, ya que permiten traducir direcciones fáciles de recordar en las direcciones que entienden los ordenadores.



Domain Name System
Sistemas de Nombres de Dominio

Arquitectura DNS
Estructura Jerárquica



Arquitectura DNS
Estructura Jerárquica

- Servidores raiz (root): repartidos mundialmente. Su seguridad es crítica.
- Dominios de Nivel Superior
  - Generales (.com, .edu, .org, .net …)
  - Nacionales (.es, .fr, .us, …)
- Resolución de dominios
  - Consulta iterativa o recursiva
- Registros DNS

Arquitectura DNS
Registros DNS

- La base de datos existente en cada servidor DNS organiza la información por medio de registros.
  - registro A, AAAA, CNAME, HINFO, MX, NS, PTR, SOA, SPF…

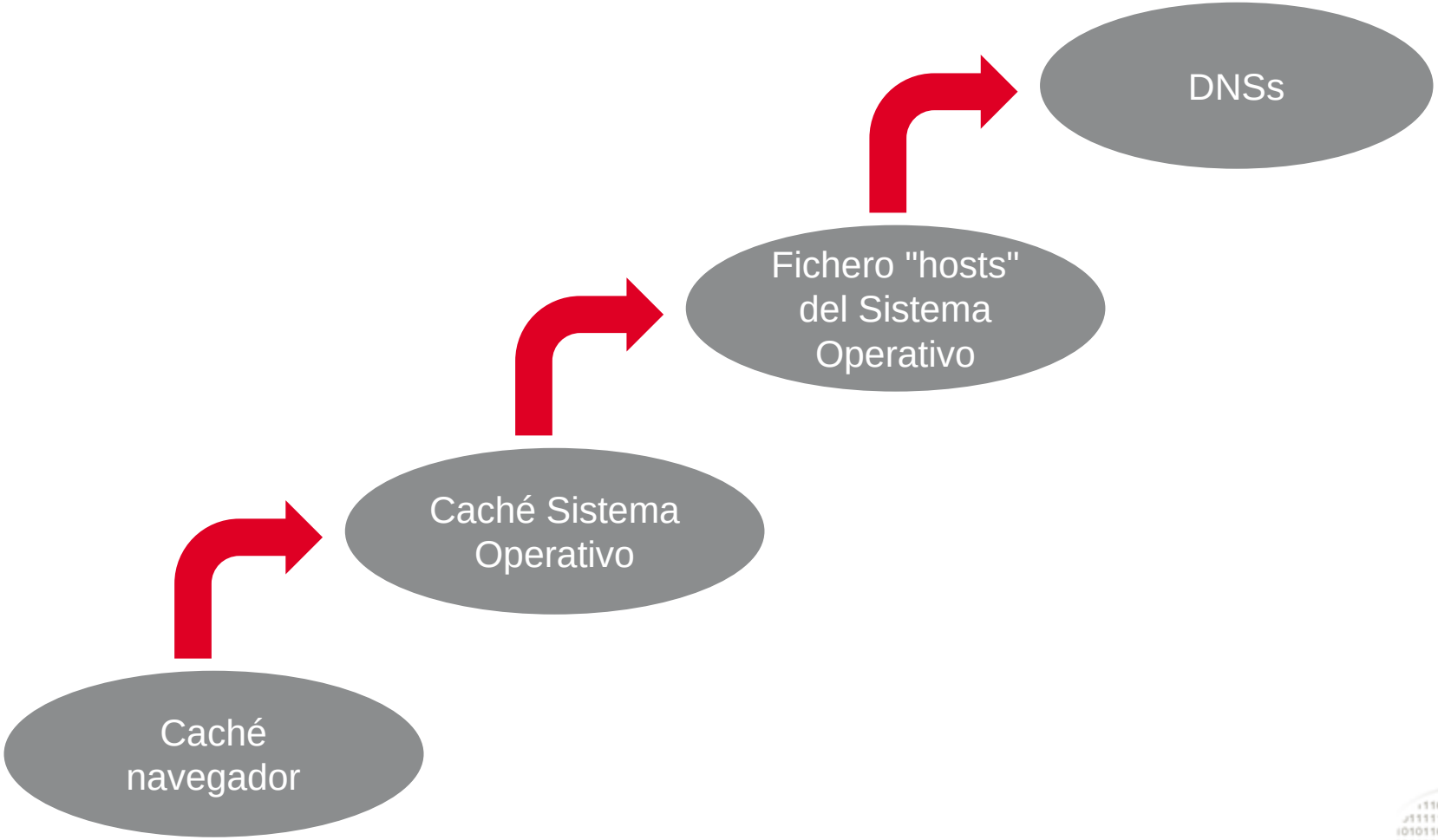
A = Address – (Dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

CNAME = Canonical Name – (Nombre Canónico) Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio.

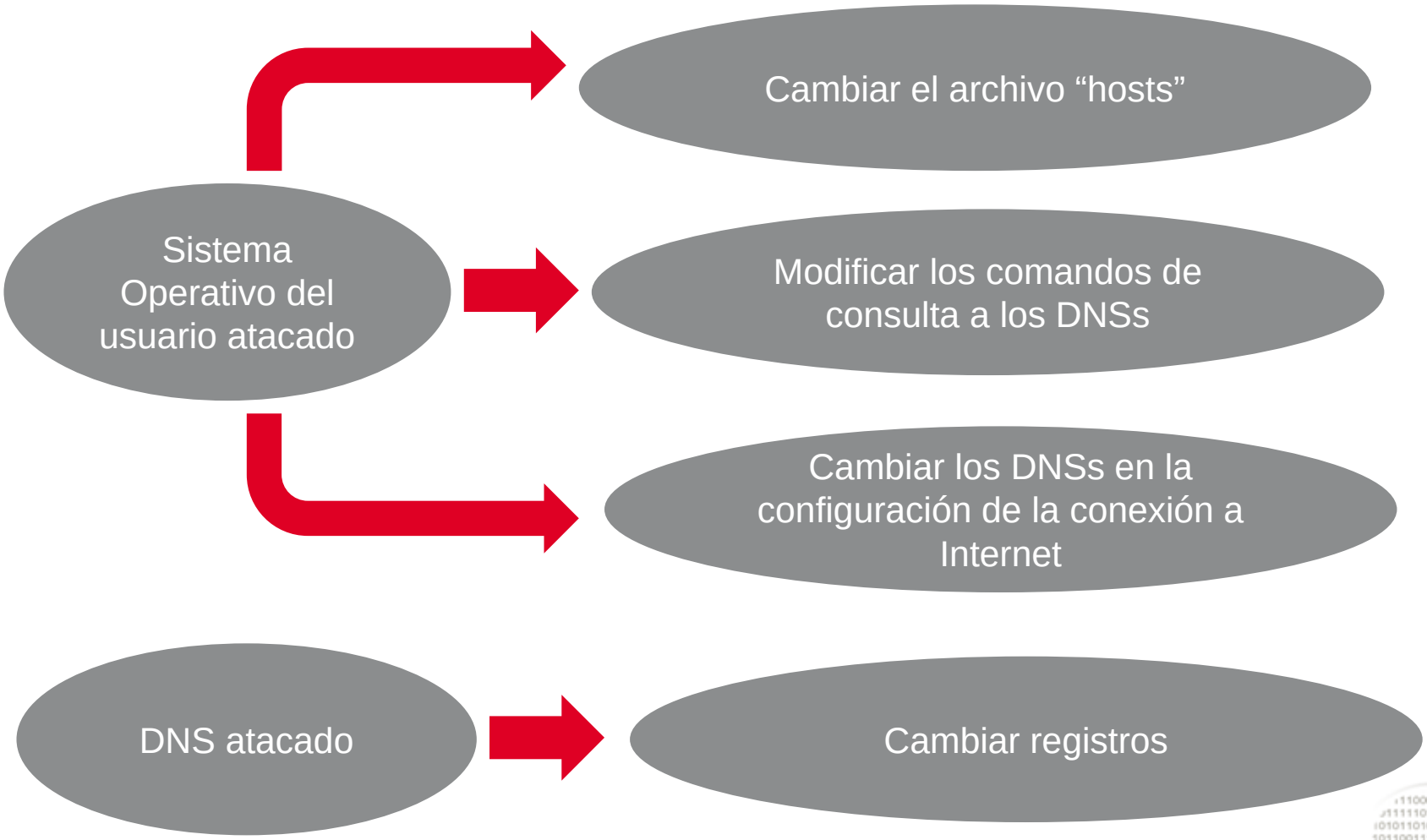
MX (registro) = Mail Exchange – (Registro de Intercambio de Correo) Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

PTR = Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

Flujo de Consulta de un dominio (Ej. Navegador Web)



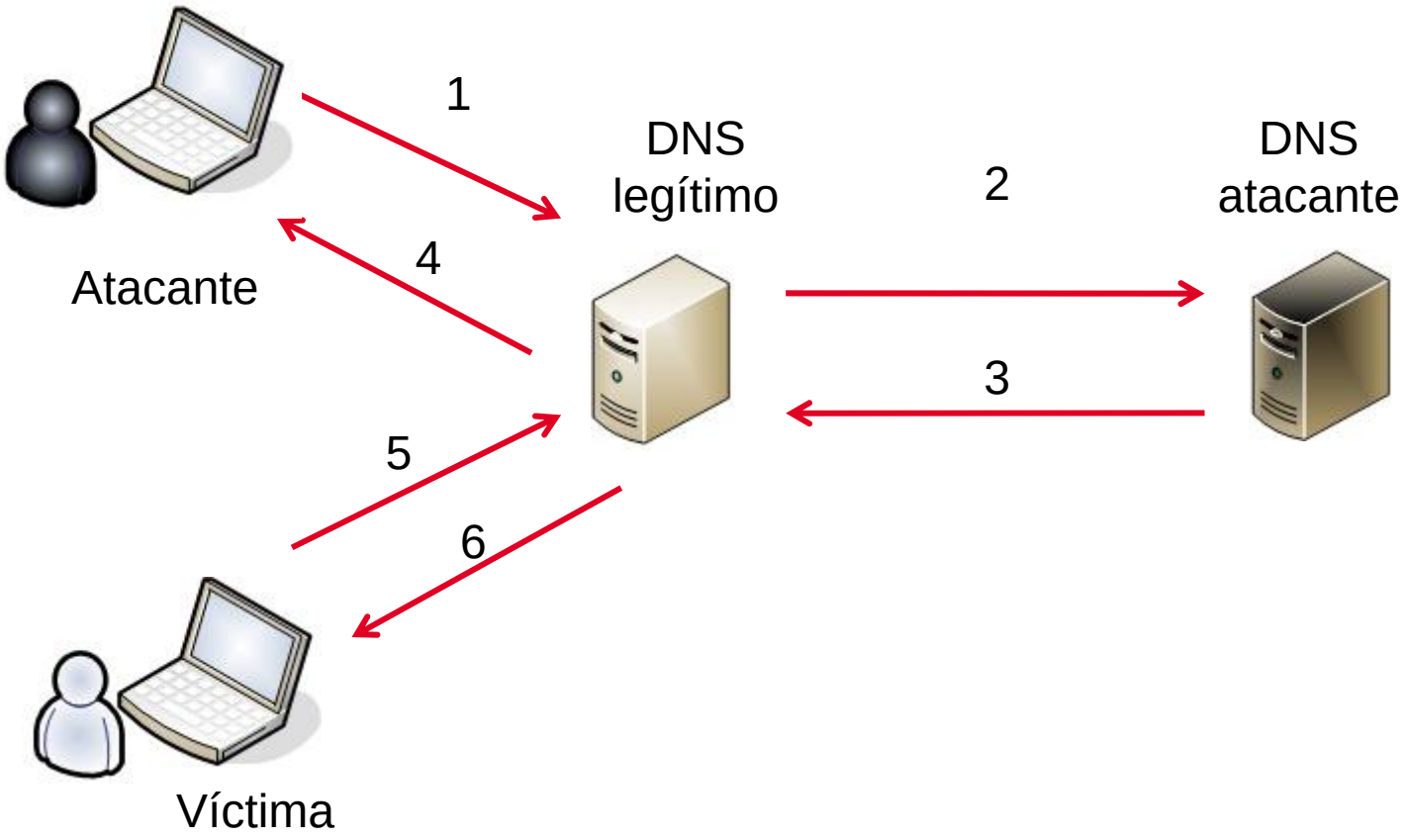
Los Ataques Básicos



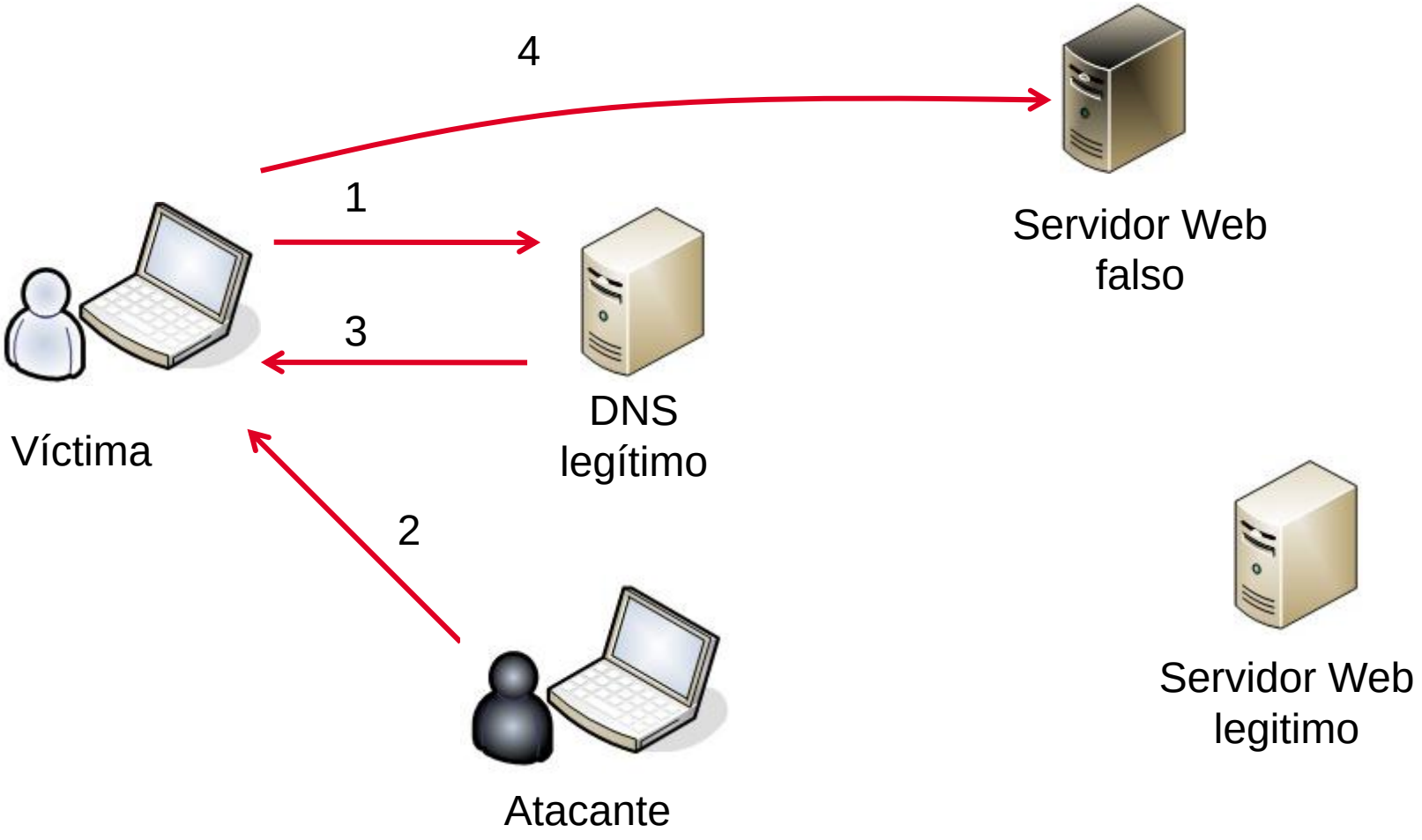
Pharming y sus Objetivos

- Los ataques relacionados con la resolución de dominios se denominan **Pharming**.
- Redirecciona el tráfico dirigido a un servidor legítimo a otro falso para, por ejemplo:
  - robar usuarios y claves de acceso a páginas Web que necesitan de un registro previo: bancos, redes sociales, juegos online, etc.
  - interceptar comunicaciones

Ataque - DNS Caché Poisoning

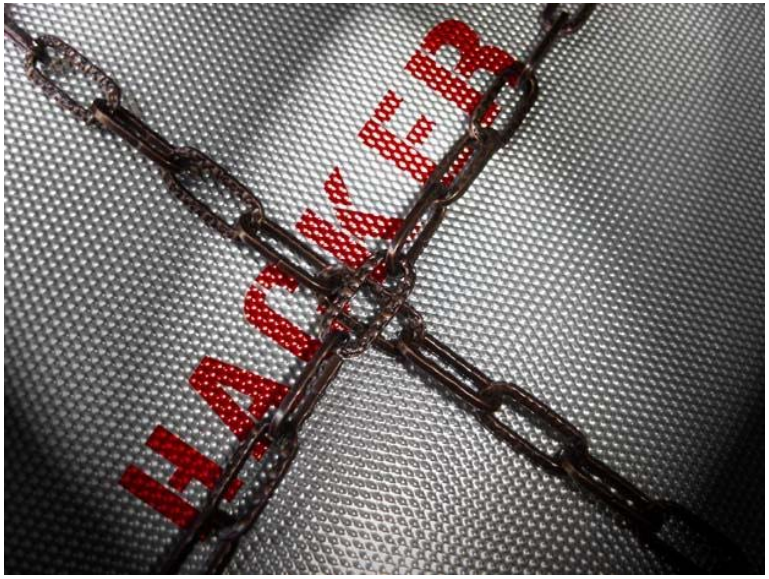


Ataque - DNS ID Spoofing with Sniffing



Ataque - DNS Caché Snooping

- El atacante hará consultas a un DNS con la intención de saber que dominios tiene cacheados.
- Permite conocer los dominios que otros han visitado: bancos, partidos políticos, información médica, etc.
- Facilita otros ataques: phising, ingeniería social o explotación de vulnerabilidades.



Ataque - Man-in-the-Middle

Utilización segura de resolución de dominios (usuarios finales)

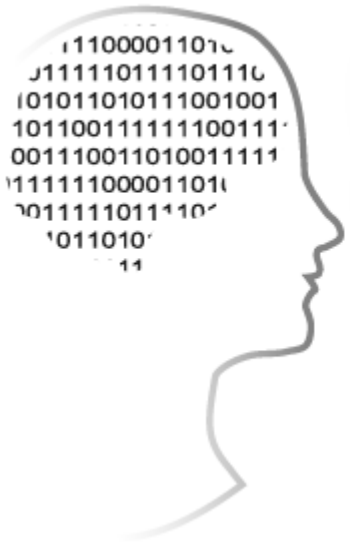
- Control del acceso en local al Sistema Operativo.
- Actualización del Sistema Operativo y aplicaciones.
- Instalación y configuración de un antivirus y un cortafuegos.
- Evitar la instalación de software que no sea de confianza.
- Estar atentos a las alertas de seguridad que los navegadores nos muestren en los certificados de servidor que se utilizan en las conexiones HTTPS.

Securización de DNSs (1 de 2)

- Control de accesos seguro
- Concienciación de usuarios sobre la existencia y métodos de ingeniería social.
- Trazabilidad de quién, qué y cuándo se modifica la información que contienen los DNSs.
- Sistema de monitorización eficaz.

Securización de DNSs (2 de 2)

- Utilización de últimas versiones del software asociado al DNS y actualización continua.
- Configuración apropiada de los DNSs.
- Limitación de las redes desde las que se puede acceder a la cache del DNS, si es posible.



intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com