

Introducción al protocolo DNS

Santiago Hernández Ramos
@santiagohramos

¿QUÉ ES DNS?

- DNS es el acrónimo de **Domain Name System**
- Realiza un mapeo entre nombres de dominio y direcciones IP
- Se corresponde con uno de los protocolos más importantes de Internet

¿POR QUÉ NOS INTERESA EL DNS?

- Obtener información pública sobre un dominio o una organización
- Descubrir relaciones entre dominios y hosts
- Técnicas de explotación específicas para ganar acceso (Ej. *DNS Spoofing*)

¿CÓMO FUNCIONA DNS?

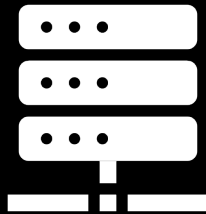
- **DNS Zone:** Agrupación de registros (datos) DNS
- Las DNS Zones contienen diferentes tipos de registros:

Tipo	Significado	Valor
SOA	Start of Authority	Parámetros para esta zona
A	Dirección IP de un host	32 bits
MX	Mail Exchange	Dominio para correo
NS	Name Server	Nombre de un servidor para este dominio
Cname	Canonical Name	Nombre del dominio
PTR	Pointer	Alias para una dirección IP
HINFO	Host Description	CPU y SO en ASCII
TXT	Texto	Información de Texto

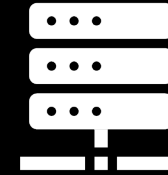
FUNCIONAMIENTO DNS



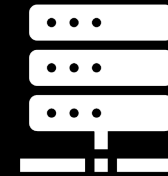
Usuario



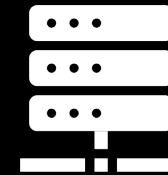
Local DNS Resolver



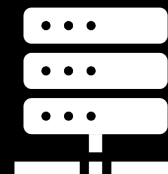
DNS root name server



Top-Level DNS Servers



Authoritative DNS Servers



Web server