Introduction to the DNS Protocol

Santiago Hernández Ramos
@santiagohramos

WHAT IS DNS?

- DNS is the acronym for Domain Name System.
- It maps domain names to IP addresses.
- It is one of the most important protocols on the Internet.

WHY ARE WE INTERESTED IN DNS?

- Obtain public information about a domain or an organization
- Discover relationships between domains and hosts
- Specific exploitation techniques to gain access (e.g., DNS Spoofing)

¿HOW DNS WORKS?

- DNS Zone: Grouping of DNS records (data)
- DNS Zones contain different types of records:

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	Dirección IP de un host	32 bits
MX	Mail Exchange	Domain for email
NS	Name Server	Name of a server for this domain
Cname	Canonical Name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host Description	CPU and OS in ASCII
TXT	Texto	Text information

¿HOW DNS WORKS?

User

Local DNS Resolver

DNS root name server

Top-Level DNS Servers

Authoritative DNS Servers

Web Server