DNS enumeration

Domain Name System (DNS) enumeration is the process of identifying the DNS servers and records associated with a target:

Address (A) records containing the IP addresses for domains

Mail Exchange (MX) records containing mail addresses

Canonical Name (CNAME) records used for aliasing domains and identifying subdomains within DNS records

Name Server (NS) records show the authoritative (or main) name server for the domain

State of Authority (SOA) records have important information about the domain such as the primary name server, timestamp showing last update and the party responsible for the domain

Pointer Records (PTR) map an IPv4 address to the CNAME on the host, aka ‘reverse record’ because it connects a record with an IP address to a hostname instead of the other way around

TXT records may include additional information (e.g. configuration)