Análisis de Tráfico DNS

Conocimiento general del DNS

Herramientas: Wireshark • dig • Python (Scapy)

Dominios analizados: 7
Paquetes capturados: 713 DNS

Equipo 2
Alberto Boughton Reyes A01178500
Valeria Garcia Hernandez A01742811
Facundo Bautista Barbera A01066843
Emiliano Ruiz López A01659693
Daniel Garnelo Martinez A00573086

¿Qué es DNS?

Domain Name System (DNS) traduce nombres de dominio a direcciones IP

Importancia del Análisis DNS:

a. Verificar configuraciones de servidores
b. Analizar redundancia y disponibilidad
c. Identificar adopción de IPv6
d. Comprender la jerarquía de nombres
e. Detectar problemas de resolución

Metodología

Captura: Wireshark en interfaz en0, filtrando puerto 53 (DNS)

Consultas: Comando dig para registros SOA, NS, A, AAAA

Análisis: Script Python con Scapy para procesar registros

Dominios analizados:

a. cinvestav.mx
b. gob.mx
c. ipn.mx
d. tec.mx
e. uanl.mx
f. udg.mx
g. unam.mx

Análisis: unam.mx

Registro SOA

- Servidor primario: ns1.unam.mx
- Serial: 2025118101 | Refresh: 1h | Retry: 20min

Servidores NS (5)

- ns1.unam.mx (TTL: 525s)
- ns2.unam.mx (TTL: 525s)
- ns3.unam.mx (TTL: 525s)

Registros A - IPv4 (4)

- 132.248.166.19 (TTL: 3899s)
- 132.248.166.20 (TTL: 3899s)

Soporte IPv6: Sí (4 registros)

Análisis: tec.mx

Registro SOA

- Servidor primario: ns1.itesm.mx
- Serial: 706970049 | Refresh: 1h | Retry: 10min

Servidores NS (2)

- ns1e.itesm.mx (TTL: 85785s)
- ns2e.itesm.mx (TTL: 85785s)

Registros A - IPv4 (2)

- 45.60.86.212 (TTL: 3594s)
- 45.60.115.212 (TTL: 3594s)

Soporte IPv6: No (0 registros)

Análisis: gob.mx

Registro SOA

- Servidor primario: m.mx-ns.mx
- Serial: 1763596684 | Refresh: 0h | Retry: 15min

Servidores NS (6)

- c.mx-ns.mx (TTL: 53592s)
- e.mx-ns.mx (TTL: 53592s)
- i.mx-ns.mx (TTL: 53592s)

Registros A - IPv4 (1)

- 207.249.118.158 (TTL: 3279s)

Soporte IPv6: No (0 registros)

Tabla Comparativa

Dominio	NS	IPv4	IPv6	Soporte IPv6
cinvestav.mx	3	1	1	Sí
gob.mx	6	1	0	No
ipn.mx	3	1	0	No
tec.mx	2	2	0	No
uanl.mx	2	1	0	No
udg.mx	3	1	1	Sí
unam.mx	5	4	4	Sí

Árbol DNS de Dependencias

cinvestav.mx
- NS: dns3.tamps.cinvestav.mx
- NS: soun.red.cinvestav.mx
- NS: mvax1.red.cinvestav.mx

gob.mx
- NS: c.mx-ns.mx
- NS: e.mx-ns.mx
- NS: i.mx-ns.mx
- NS: m.mx-ns.mx
- NS: o.mx-ns.mx
- NS: x.mx-ns.mx

ipn.mx
- NS: dns1.ipn.mx
- NS: dns2.ipn.mx
- NS: dns3.ipn.mx

tec.mx
- NS: ns1e.itesm.mx
- NS: ns2e.itesm.mx

Hallazgos Interesantes

Fortalezas:

- Alta redundancia: gob.mx con 6 servidores NS
- UNAM lidera con 4 registros IPv4 + 4 IPv6
- Balance de carga en múltiples instituciones
- TTL optimizados según necesidades

Áreas de Mejora:

- Solo 43% (3/7) soportan IPv6
- Algunos dominios con redundancia mínima (2 NS)
- Inconsistencia en estándares de configuración

Conclusiones

Resumen:

- Se analizaron 7 dominios .mx con 713 paquetes DNS
- Todos tienen configuración SOA correcta
- Promedio de 3.4 servidores NS por dominio
- UNAM destaca por infraestructura robusta
- gob.mx muestra máxima redundancia (6 NS)

Recomendaciones:

- Acelerar adopción de IPv6
- Mínimo 3 servidores NS para redundancia
- Evaluar estrategia de TTL según necesidades
- Implementar monitoreo periódico