

Práctica: 34. DNS y Nslookup (Por HxC Mods-Adm)

Ya hemos comentado la importancia de las transferencias de zona en servidores DNS que lo permitan, para ello podemos usar la utilidad nslookup del propio sistema operativo:

La salida es “algo cruda” pero efectiva, nslookup dispone de muchas opciones y parámetros, para extraer la zona de un servidor DNS usaremos server seguido del nombre del dominio DNS y luego ejecutaremos la instrucción ls -d

```
c:\>nslookup

Servidor predeterminado:  dns.terra.es
Address:  195.235.113.3

server dream-es.com

> Servidor predeterminado:  dream-es.com
Address:  217.126.149.131

ls -d dream-es.com

> [dream-es.com]
dream-es.com.      SOA      srv.dream-es.com
admin.
dream-es.com.     A        192.168.0.1
dream-es.com.     A        192.168.0.11
dream-es.com.     NS       srv.dream-es.com
gc._msdcs         A        192.168.0.11
gc._msdcs         A        192.168.0.1
dream-es          MX       10      dream-es.com
```

Las líneas sombreadas son las que debes teclear desde la ventana de comandos, los resultados “se han recortado” para que se lean mejor, observa que nos proporciona las direcciones IP internas del dominio, los nombres netbios y algún dato más como un registro MX que indica la presencia de un servidor de correo, y el nombre del equipo junto con la IP del catálogo global (gc.msdcs)

Advertencia: Este dominio es real y su administrador ya ha sido avisado en repetidas ocasiones de los fallos de configuración y conexiones anónimas, no hace caso a nuestros avisos, aun así es posible que en el futuro configure sus servidores “*como Dios manda*” y no consigas estos resultados.

Existen utilidades y herramientas de terceros que logran esto mismo con una salida más “vistosa”, ya hemos usado alguna de ellas, NetScanTools, Sam Spade, etc. Si deseas una herramienta especializada en Servidores DNS prueba con DNS Expert

No sólo sirve para transferencias de zona, sino que puede verificar la configuración de vuestro propio servidor DNS y advertiros de los fallos de seguridad que tengáis.