# Mi primera revisión de Directorio Activo desde un punto de vista ofensivo

## Dominio Churrasco

* ¿En qué rango está la IP?
* ¿Cómo se llama la máquina en la que estás?
* ¿Tu usuario es local o de dominio?
* ¿Cómo se llama tu usuario de dominio?
* ¿Existe algún usuario local que no sea por defecto de Windows?
* ¿Está activado el usuario Administrador local?
* ¿A qué grupos pertenece tu usuario de dominio?
* ¿A qué grupos pertenece el usuario local que has identificado antes?
* ¿Qué tipo de acceso remoto tienen tus usuarios (RDP, WinRM, SSH…)?
* ¿Cuál es el nombre de DNS del dominio?
* ¿Y su nombre de NETBIOS?
* ¿Cuántos usuarios tiene el dominio?
* ¿Y grupos?
* ¿Qué usuarios pertenecen al grupo RRHH?
* ¿Cuántos equipos hay en el dominio?
* ¿Cómo se llama cada equipo del dominio?
* ¿Qué funcionalidad tiene el dominio?
* ¿Cuántas GPOs de dominio hay desplegadas?
* Introduce los nombres separados por comas sin espacio (gpo1,gpo2,...)
* ¿Existe alguna GPO local en algún equipo?
* ¿Existe más de un DC?
* ¿Qué tipo de confianza hay entre cada DC? (Forest, external, realm, enlace)
* ¿Es bidireccional?
* Introduce el nombre del usuario con información sensible en sus atributos
* ¿Existe algún servidor (HTTP, SMB) en el dominio?
* ¿Qué hay escuchando en dicho puerto HTTP?
* ¿Existen carpetas compartidas en el dominio?
* Introduce el nombre de la carpeta
* ¿Qué grupo de AD tiene acceso a dicho fichero (solo puede verse siendo Administrador de dicha máquina)?
* ¿Cuántos usuarios han iniciado sesión en el equipo FILESERVER?
* ¿Cuánto hace que no se cambia la contraseña del KRBTGT? (Días)

## Dominio Paletilla

* ¿Cómo se llama el usuario con el que has podido acceder a este dominio?
* ¿A qué grupos pertenece tu usuario?
* ¿Cuál es el nombre de DNS del dominio?
* ¿Y su nombre de NETBIOS?
* ¿Cuántos usuarios tiene el dominio?
* ¿Y grupos (no por defecto)?
* ¿Qué usuarios pertenecen al grupo Administración?
* ¿Cuántos equipos hay en el dominio?
* ¿Puedes tener una sesión local como César en cualquier equipo del dominio churrasco.region?
* En caso positivo, explica por qué
* ¿Y acceso por RDP?