Universitat Oberta de Catalunya

uoc.edu

Seguridad en Redes Empresariales: Protegiendo el Acceso Privilegiado

Daniel López Jiménez

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Trabajo de Fin de Máster. Sistemas de Autenticación y Autorización

Director del TFM: Amadeu Albós Raya

Nombre Profesor/a responsable de la asignatura: Víctor García Font

Fecha: 08/06/2020

A mi familia, a todos mis Crummie5, a David Muñoz, a JC y a mi compañero Wint3r, espero que te encuentres bien allá donde estés.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Seguridad en redes empresariales: protegiendo el acceso privilegiado*
Nombre del autor:	*Daniel López Jiménez*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Víctor García Front*
Fecha de entrega (mm/aaaa):	06 / 2020
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*Sistemas de Autenticación y Autorización*
Idioma del trabajo:	*Español*
Palabras clave	*Seguridad de entornos empresariales, protección del acceso privilegiado, infraestructuras internas*

Resumen del Trabajo

Este trabajo busca explicar y visibilizar los beneficios de utilizar un diseño seguro de infraestructura interna en las empresas de la actualidad.

En los primeros capítulos se presentan las problemáticas principales por las cuales un cibercriminal suele comprometer con relativa facilidad este tipo de entornos y el origen de las mismas.

Una vez entendido el origen de las problemáticas, se presenta la necesidad de utilizar un diseño de infraestructura seguro, ordenado y fácil de administrar y monitorizar. En este aspecto, se estudian diferentes buenas prácticas que ayudan a la implementación de este tipo de diseños.

A continuación, se realiza la implementación práctica de un diseño seguro concreto – Active Directory Red Forest – aplicando todas las buenas prácticas vistas anteriormente y comprobando su eficacia para solventar o minimizar las problemáticas expuestas inicialmente.

Por último, este trabajo finaliza con la realización de unas conclusiones sobre todo lo que se ha visto a lo largo del documento.

Abstract

This project aims to explain and visualize the benefits of using a safe well-organized internal infrastructure in today's enterprises.

In the first chapters, common reasons for which cybercriminals tend to compromise these environments are presented along with their root causes. After their analysis and understanding, the need of a secure and easy manageable infrastructure design is presented. Different good practices are then studied to help the implementation of this type of designs.

Subsequently, a practical implementation of a specific security design – Active Directory Red Forest – is carried out. Within this design, all the good practices previously seen are adopted and tested to ensure their effectiveness in solving or minimizing the problems exposed in the first chapters.

Finally, this document finishes with some conclusions about all the contents studied.

Índice

Lista de figuras

1. INTRODUCCIÓN

1.1. Contexto y Justificación del Trabajo

Existe un problema generalizado con respecto a la seguridad de las infraestructuras internas organizacionales. Desafortunadamente, la seguridad de estos entornos – como ocurre en muchos otros ámbitos – ha empezado a visibilizarse años después de múltiples casos y brechas de seguridad.

A pesar de que Internet en general ofrezca numerosa información útil sobre la seguridad de estos entornos, la realidad es que todavía, a día de hoy, es muy común encontrar organizaciones que no dan a la seguiridad la prioridad que merece. Cuando una organización parte de una buena infraestructura interna, en la que se ha tenido la seguridad en cuenta, le será notablemente más fácil gestionarla y asegurarla en contraposición a organizaciones que simplemente se hayan enfocado en ofrecer funcionalidad y usabilidad.

Dentro de este aspecto, este trabajo busca visibilizar los problemas que pueden surgir por estructurar una red organizativa sin tener en cuenta la seguridad desde un principio, destacando Active Directory como base de trabajo, pero revisando otras opciones alternativas o complementarias como Samba o FreeIPA. Así mismo, busca demostrar de forma práctica los retos que surgen al intentar aplicar estos modelos de seguridad tan recomendados a través de la red. Para ello se utilizará como base el diseño “Active Directory Red Forest Design” propuesto por Microsoft para entornos Active Directory, pero nuevamente intentando contemplar otras opciones fuera de esta tecnología.

A menudo se encuentra demasiada teoría y poca práctica en la documentación que cubre esta temática. La justificación final de este trabajo es ofrecer un vistazo, lo más realista posible, sobre la viabilidad de este tipo de diseños en organizaciones reales, teniendo en cuenta sus ventajas, desventajas y retos de implementación.

1.2. Objetivos del Trabajo

Los principales objetivos de la investigación son los siguientes:

1. Estudio e investigación de las infraestructuras y tecnologías actuales utilizadas en entornos corporativos.
2. Estudio de la situación actual respecto a la seguridad de este tipo de entornos e investigación de las problemáticas comunes a las que se enfrentan.
3. Revisión de los diseños tradicionales que se llevan a cabo mediante tecnologías como Active Directory, FreeIPA o Samba.
4. Estudio del diseño de seguridad Red Forest, planteado principalmente para Active Directory, realizando una comparativa con los diseños investigados en el punto anterior.

5. Implementación de un laboratorio simulando una empresa ficticia con la tecnología Active Directory, siguiendo el diseño Red Forest y sus recomendaciones.
6. Investigación de los retos que supone la implementación anterior, tanto para un laboratorio de pruebas, como para una potencial empresa de mayor tamaño.
7. Realización de pruebas de seguridad al laboratorio para demostrar la eficacia de la implementación y sus lagunas.
8. Proposición de un diseño completo de seguridad para empresas.
9. Conclusiones del trabajo, desarrollo de la memoria final y realización del video.

1.3. Metodología

La metodología aplicada a este proyecto tendrá como fin el cumplimento de los objetivos marcados en el punto anterior. De esta manera, se basará en lo siguiente:

- Estudiar y entender la necesidad, por parte de las organizaciones, de disponer de una infraestructura interna para poder llevar a cabo sus objetivos, ahorrando costes y mejorando la productividad.
- Investigar las tecnologías comunes que utilizan las empresas para crear sus infraestructuras internas, contemplando el panorama desde el punto de vista de los dos sistemas operativos predominantes: Windows y Linux/Unix.
- Comprobar qué tipo de implementación suelen realizar las organizaciones de las tecnologías vistas en el punto anterior, con el fin de identificar malas prácticas en lo que respecta a la seguridad, pero también entender el origen de las mismas.
- Analizar las recomendaciones y buenas prácticas comunes aplicadas a estructuras internas desde fuentes fiables como organizaciones dedicadas a la seguridad IT o Microsoft.
- Aplicar y comprobar la teoría estudiada con ejemplos prácticos, de manera que se puedan evidenciar posibles situaciones o escenarios no contemplados en la teoría, a la vez que se estudia su validez.
- Por último, sustraer una serie de conclusiones en base a los resultados obtenidos de las investigaciones y las prácticas.

1.4. Listado de Tareas

A continuación se muestra un listado de las tareas a llevar a cabo con la descripción de sus contenidos.

1- Estudio de Soluciones Identity Management

El objetivo de esta tarea es estudiar y entender los componentes clave de algunas de las soluciones de Identity Management más utilizadas en el mercado como Active Directory o FreeIPA.

2- Seguridad de Entornos Corporativos

En esta tarea se estudiarán los problemas principales a los que se enfrentan las organizaciones para con respecto a la seguridad. Se estudiará el problema de la exposición de credenciales, la división pobre de privilegios, la falta de segmentación interna y, por último, la falta de control dentro de la red organizativa.

3- Infraestructuras Enfocadas en la Seguridad

Tras entender los problemas principales a los que se expone una organización, esta tarea pretende estudiar algunas de las soluciones propuestas en Internet. En este aspecto, se hará especial hincapié en Active Directory y la idea del diseño Red Forest propuesta por Microsoft.

4- Implementación Práctica del Diseño Red Forest

Creación de una organización ficticia siguiendo el diseño Red Forest mediante máquinas virtuales con VMWare. El planteamiento inicial será a través de dos bosques – uno de Producción y otro de Administración – siguiendo las pautas y recomendaciones de Microsoft en la medida de lo posible, teniendo en cuenta el tiempo y recursos disponibles.

5- Pentesting Red Forest

Realización de diferentes pruebas de seguridad a la empresa ficticia para comprobar la efectividad del diseño empleado y las soluciones instaladas. En este punto se busca demostrar con evidencias las ventajas de estructurar Active Directory correctamente, pero también las lagunas que no cubre en cuanto a cuestiones de seguridad. Además, se tendrá en cuenta esta información para introducir un modelo de seguridad potencialmente completo, intentando cubrir el mayor espectro posible de superficie de ataque en estos entornos.

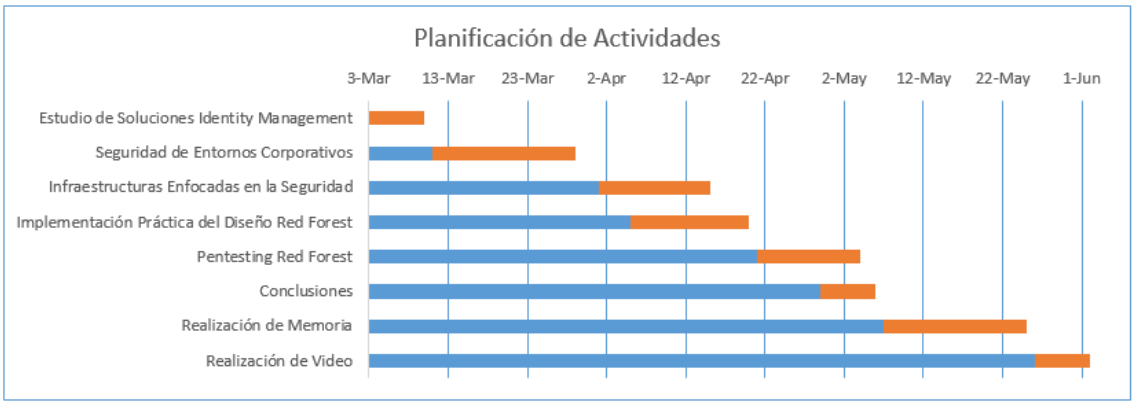
6- Conclusiones

Este punto tratará de recoger todos los resultados de las investigaciones y pruebas realizadas a lo largo del documento para desembocar en unas conclusiones sobre la temática.

1.5. Planificación del Trabajo

A continuación se muestra la planificación de trabajo temporal para este documento:

Actividad	Duración	Inicio	Fin
Estudio de Soluciones Identity Management	7	3-Mar	10-Mar
Seguridad de Entornos Corporativos	18	11-Mar	30-Mar
PEC2	27	4-Mar	31-Mar
Infraestructuras Enfocadas en la Seguridad	14	1-Apr	15-Apr
Implementación Práctica del Diseño Red Forest	15	5-Apr	20-Apr
Pentesting Red Forest	13	21-Apr	28-Apr
PEC3	27	1-Apr	28-Apr
Conclusiones	7	29-Apr	6-May
Realización de Memoria	18	7-May	25-May
Realización de Video	7	26-May	2-Jun
PEC4	34	29-Apr	2-Jun



1.6. Estado del Arte

Durante los años 80 y 90, se comenzó a ver un uso proliferado de ordenadores personales por parte de las organizaciones, con el fin de automatizar y llevar a cabo tareas que antaño se habían realizado de forma manual o dependían de aspectos externos. Un ejemplo clásico de las ventajas que trajo este cambio es la comunicación que ofrece Internet a través de los correos electrónicos, que a día de hoy es un eje clave en el buen funcionamiento de cualquier empresa.

Con esta transformación de los entornos de trabajo, las organizaciones pronto se dieron cuenta de que era necesaria una forma de gestionar todos estos puestos "tecnológicos", y fue en 1999 cuando Microsoft respondió a dicha necesidad lanzando Active Directory al mercado. Active Directory puso sobre la mesa una forma de gestionar usuarios, sistemas, políticas y servicios de forma centralizada, facilitando a los administradores conectar y ofrecer activos a lo largo de una organización.

Junto a Active Directory, han aparecido numerosas alternativas. No obstante, actualmente, Active Directory es la opción de gestión de identidad más utilizada por las empresas a nivel mundial.

No es atrevido afirmar que este tipo de tecnologías han pasado a ser el corazón de muchas organizaciones y que, en caso de ser comprometidas, todos – o la mayor parte de – sus activos pasarían a estar en riesgo. Es por este motivo por el cual los adversarios o ciberdelincuentes

han estado poniendo su foco en aprender y atacar este tipo de entornos durante años, y prueba de ello son las múltiples brechas de seguridad y compromisos que han rellenado publicaciones de prensa, así como las que ni si quiera se habrán detectado o salido al público.

Desafortunadamente, la seguridad de estos entornos – como ocurre en muchos otros ámbitos – ha empezado a visibilizarse años más tarde. Con el nacimiento de blogs como "adsecurity.org" (2012), y gracias a personas como Sean Metcalf, a día de hoy se puede encontrar gran cantidad de información sobre cómo atacar y defender infraestructuras organizacionales que emplean tecnologías como Active Directory, facilitando herramientas y soluciones a las empresas para proteger el "corazón" de sus activos.

Por su parte, las empresas responsables de estas tecnologías – como por ejemplo, Microsoft – han ido mejorando incrementalmente muchos aspectos de su seguridad, ofreciendo pautas y buenas prácticas para su configuración e implementación.

A día de hoy, con la información disponible en Internet, un administrador dispone de muchas herramientas para mejorar y fortalecer sus entornos. Día a día aparecen nuevas utilidades, ataques y mecanismos de protección que permiten visibilizar y mantenerse actualizado del estado de seguridad - e inseguridad - actual en las empresas. Grandes ejemplos de esto son las soluciones Endpoint Detection and Response (EDR), que permiten combinar funciones como el análisis de comportamiento, control de aplicaciones, monitorización de la red y respuesta a incidentes; otro ejemplo son las pruebas de concepto y herramientas ofensivas como PowerSploit, que permiten a un equipo de seguridad entender el origen y la forma de ataques comunes llevados a cabo en entornos empresariales.

Hace unos años existía mucha oscuridad y falta de información sobre estos temas. En la actualidad, a pesar de ser una tarea muy compleja, es posible conseguir un estado de seguridad aceptable partiendo de una buena infraestructura, siguiendo las recomendaciones comunes y manteniéndose al día sobre los ataques y técnicas que cogen importancia en la red.

2. INTRODUCCIÓN A LOS ENTORNOS CORPORATIVOS

Con la proliferación del uso de ordenadores personales, se hizo necesario un cambio en los puestos de trabajo y la administración de los mismos dentro de las empresas. Hoy en día, casi todas las empresas disponen de una red interna donde se encuentran conectados muchos de los sistemas y recursos pertenecientes a las mismas. Estos recursos pueden ser desde documentos hasta servidores de correo o páginas web.

A causa de este cambio en la forma de trabajar, **las empresas requirieron formas de poder administrar y controlar** toda esa cantidad de empleados, ordenadores, servidores y recursos. A esta necesidad es a la que responden las tecnologías de gestión de identidades o "**Identity Management**".

Las soluciones Identity Management buscan ofrecer a los administradores herramientas y capacidades para poder gestionar una red interna empresarial. Parten de la idea del **principal**, objeto que encapsula cuestiones como **usuarios, servicios, ordenador o incluso aplicaciones**.

Un **principal** se define como un objeto que requiere **autenticación, autorización y privilegios**. Por lo tanto, en estas tecnologías, todos los usuarios, servicios, ordenadores y aplicaciones van a requerir dichas cuestiones.

- Autenticación: es lo que permite identificar a un principal. Las autenticaciones no se limitan en estos casos a la tradicional combinación de usuario y contraseña, sino que pueden existir otros aproximamientos como las autenticaciones de segundo factor (2FA), tarjetas inteligentes, tokens, certificados… etcétera.
- Autorización**:** es lo que permite controlar quién tiene acceso a qué dentro de la red, y puede venir implementada de diferentes formas. Las más comunes suelen ser por medio de Access Control Lists (ACL), Role-Based Access Controls (RBAC) o Host-based Access Controls (HBAC).
- Privilegios**:** engloban cuestiones como permisos, roles, grupos, herencias o delegaciones, y permiten administrar cuestiones de autorización concretas.

Además, la forma en que trabajan estas tecnologías busca en todo momento aumentar la seguridad y productividad dentro de las redes empresariales, mientras se eliminan costes y trabajo innecesario por medio de la automatización de tareas.

En este documento se va a hacer hincapié principalmente en dos soluciones de Identity Management: Active Directory y FreeIPA. A continuación, se explicará brevemente cómo funciona cada uno en lo que respecta a las temáticas de autenticación, autorización y privilegios. Se puede encontrar más información sobre estas tecnologías en los Anexos 10.1, 10.2 y 10.3.

2.1. Identidad

Como se ha indicado anteriormente, las soluciones de Identity Management parten de la idea del “principal” como objeto que requiere autenticación, autorización y privilegios.

Tanto Active Directory como FreeIPA consisten en servicios de directorio con una estructura jerárquica que almacena información sobre todos los principals u objetos de un dominio/ámbito. Para ello, utilizan una base de datos en la cual se almacena toda esa información que, a su vez, puede ser replicada con el objetivo de crear una red distribuida, manteniendo la funcionalidad e integridad de los datos. Para interactuar con los datos, utilizan el protocolo LDAP.

Cuando se habla de objetos, realmente se está hablando de la representación que realizan estas tecnologías de cuestiones como, por ejemplo, un usuario. Esto es, disponen de una serie de clases con atributos definidos para representar todas aquellas cuestiones que requieran ser administradas en una red empresarial. Algunas de las clases de objeto más comunes son las siguientes:

- Usuarios
- Grupos
- Ordenadores
- Políticas
- Contenedores de objetos

Para cada una de ellas vienen definidos una serie de atributos y características. Por ejemplo, en Active Directory, los objetos de tipo usuario disponen de atributos que informan sobre cuestiones como cuándo fue la última vez que se conectó una cuenta, o si ha cambiado su contraseña recientemente. Más información de este caso concreto se puede comprobar en la página de documentación de Microsoft.

Todos estos objetos se van a encontrar agrupados en lo que comúnmente se denominan dominios/domains (Active Directory) o ámbitos/realms (FreeIPA). En este aspecto, Active Directory extiende el concepto mediante los bosques, que corresponden a una agrupación de dominios que confían entre sí.

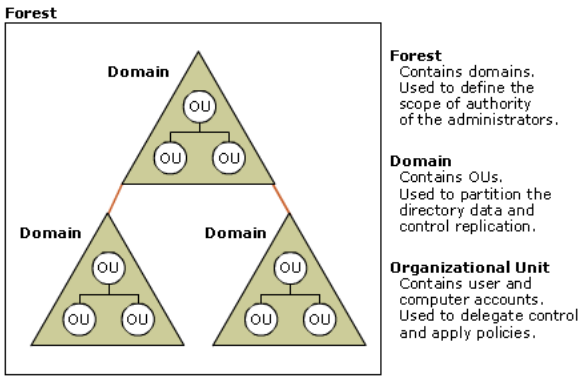


Ilustración 1 - Bosques, dominos y unidades organizacionales. Fuente: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756901(v=ws.10)?redirectedfrom=MSDN

En estas tecnologías existe el concepto de relaciones de confianza. Este concepto permite que diferentes dominios, bosques o ámbitos puedan identificarse y configurarse el acceso a recursos entre sí si es necesario. Active Directory permite las relaciones de confianza entre dominios y bosques de la misma tecnología. FreeIPA, por su parte, soporta relaciones de confianza con dominios Active Directory a través del uso de Samba pero, según su web oficial, todavía no las soporta entre diferentes dominios de la propia tecnología.

Por último, otro componente principal del que dependen estas tecnologías es el sistema de nombres de dominio (DNS). Mediante este sistema, los clientes pueden localizar servidores y servicios dentro de un dominio, destacando sobre todo la posibilidad de localizar a los sistemas clave que almacenan la información del directorio o que llevan a cabo las autenticaciones: los domain controllers o KDC servers. Además, es importante saber que tecnologías como Kerberos dependen del sistema de nombres de dominio para funcionar, puesto que sus servicios vienen en dicho formato y no soportan, por defecto, el uso de direcciones IP.

2.2. Autenticación

La autenticación es el proceso que permite identificar a un principal dentro de, en este caso, una red interna empresarial. En lo que respecta a autenticación, Active Directory y FreeIPA se sirven del protocolo **Kerberos**, aunque cada uno a su manera.

Por un lado, Windows partió de la idea original del protocolo Kerberos, presentada por el instituto tecnológico de Massachusetts (MIT), y la **extendió con diferentes capacidades y modificaciones**. En redes Active Directory, los sistemas Windows utilizan este protocolo por defecto para sistemas del dominio actual o dominios de confianza. No obstante, para situaciones en las que Kerberos no está soportado, o para sistemas que no son de confianza, Windows mantiene el soporte del protocolo NTLM para llevar a cabo dichas autenticaciones. Más información de Kerberos y NTLM en la documentación de Microsoft.

En el caso de FreeIPA, esta tecnología implementa **Kerberos a través del software facilitado por** MIT y se utiliza para ofrecer autenticación a través de los dominios FreeIPA, para todos sus principals. En el caso de FreeIPA, por defecto no existe un "fallback" a otros protocolos para autenticaciones no soportadas por Kerberos, tal y como hacía Active Directory con NTLM.

Tanto Active Directory como FreeIPA ofrecen Kerberos a través de un servidor denominado **KDC** (Key Distribution Center), junto a los componentes **Authentication Server** (AS) y **Ticket-Granting Server** (TGS). Mediante lo mismos, un principal puede utilizar sus credenciales para autenticarse en un dominio y así poder recibir los denominados tickets y claves de Kerberos.

Más información sobre el funcionamiento de Kerberos en los siguientes enlaces: Active Directory y FreeIPA.

Ilustración 2 - Single Sign-On. Fuente: https://www.iniciarsesioncorreo.club/que-es-el-single-sign-on-o-sso/

Gracias a estos nuevos objetos de credenciales (los tickets), un principal puede solicitar acceso a diferentes recursos de la red **sin necesidad de especificar sus credenciales originales una y otra vez**. Este concepto se denomina Single Sign-On (SSO) y es lo que permite trabajar cómodamente en este tipo de redes, pues autenticarse en cada recurso especificando credenciales consume mucho tiempo y va en contra de la esencia de lo que este tipo de tecnologías buscan ofrecer: conectar y confiar en la red interna.

Se debe tener en cuenta que el Single Sign-On no se limita exclusivamente a Kerberos en el caso de Active Directory. Windows dispone de diferentes paquetes de autenticación disponibles por defecto, como NTLM, que habilitan también el mencionado SSO. Windows consigue esto **almacenando credenciales en la memoria del sistema**, tal y como se indica en el siguiente artículo de Microsoft.

1. El usuario se autentica por primera vez y envía sus credenciales al sistema objetivo.
2. Windows adapta las credenciales enviadas para cada paquete de autenticación que tiene disponible en el sistema. Por ejemplo, para Kerberos y NTLM almacena el hash derivado de la contraseña del usuario.
3. El sistema delega la autenticación a un domain controller puesto que el usuario es de dominio, no local.
4. Una vez el usuario se ha autenticado en el dominio, en el momento en el que quiera utilizar un servicio, Windows utilizará las credenciales almacenadas. Si el usuario se autentica a través de NTLM, Windows utilizará el hash nuevamente, que será comprobado una vez más en el domain controller; si lo hace con Kerberos, el usuario ya dispondrá de un ticket TGT que le permitirá solicitar tickets de servicio, con los que finalmente podrá utilizar el servicio.

Todos los componentes que permiten funcionar la autenticación dentro de estas tecnologías suelen encontrarse en un mismo sistema, que por razones lógicas es considerado **crítico**. Para dominios Active Directory, este sistema se llama Domain Controller; mientras que en FreeIPA suele ser denominado simplemente KDC server.

2.3. Autorización y Privilegios

La autorización y los privilegios permiten el **control de los accesos a recursos** dentro de una red empresarial. Tanto Active Directory como FreeIPA implementan una mezcla entre controles basados en Access Control Lists (ACL) y uso de grupos/roles (RBAC).

Por una parte, todos los objetos que requieren autorización implementan una **lista de reglas donde se indica quién tiene acceso y de qué forma** a cada uno. En el ejemplo de la imagen siguiente se puede ver que el usuario "Tony Soprano" tiene privilegios de tipo "Full control" sobre el grupo Domain Admins para el dominio CAP de Active Directory.

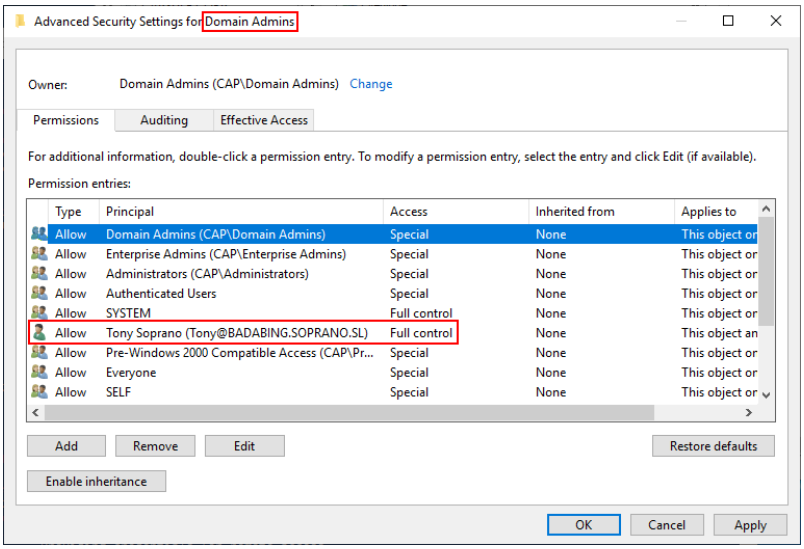


Ilustración 3 - Descriptor de seguridad del objeto Domain Admins

Por otra parte, existe el concepto de **grupos o roles**, que permiten juntar una serie de privilegios que quedan heredados a cada usuario miembro. Ejemplos de grupos son Domain Admins para Active Directory y Admins para FreeIPA, que en general ofrecen permisos para administrar el dominio al que pertenecen.

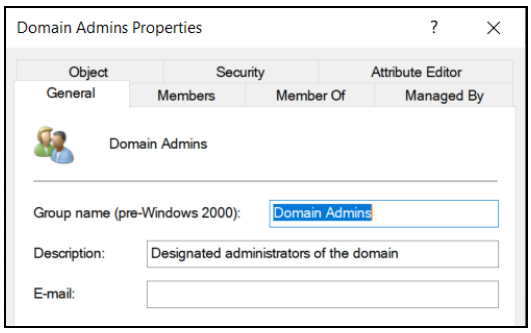


Ilustración 4 - Domain Admins

El concepto de privilegios o permisos hace referencia a cuestiones como **la lectura, la escritura o la ejecución** aplicada a recursos. Existen también diferentes privilegios predefinidos que no son más que una agrupación de permisos de una forma similar a cómo funcionan los grupos para los usuarios.

Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	Administrators,Backup Operators,Account Operators,Server Operators,Print Operators,ENTERPRISE DOMAIN CONTROLLERS
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operators,Server Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Authenticated Users,Pre-Windows 2000 Compatible Access
Change the system time	LOCAL SERVICE,Administrators,Server Operators

Ilustración 5 - Ejemplos de permisos asignables

Además de todo lo anterior, estas tecnologías permiten cuestiones como la delegación o herencia de privilegios, de tal forma que se pueda ofrecer acceso a recursos sin la necesidad de que el usuario concreto pertenezca a grupos altamente privilegiados.

Más información sobre cómo funcionan los controles de acceso en Active Directory y FreeIPA.

3. SEGURIDAD DE ENTORNOS CORPORATIVOS

Aprender una nueva tecnología requiere **tiempo y esfuerzo**. Requiere que la persona en cuestión se familiarice con la tecnología mediante actividades como la lectura de su documentación, la visualización de la tecnología en funcionamiento, o practicando con ella. De esta forma, una vez familiarizado con ella, la persona puede ponerla a funcionar.

Un ejemplo simple podría ser un servidor Tomcat, ampliamente utilizado en las empresas para ofrecer recursos escritos en Java. Una persona que quiera crear un servidor Tomcat en su empresa deberá entender cómo funciona esta tecnología y qué requisitos o dependencias tiene asociados. Una vez hecho esto, desplegará el servidor en la red interna de su empresa y podrá ser utilizado para ofrecer recursos.

La cuestión es ¿Se suele tener en cuenta la seguridad a la hora de aprender o desplegar una tecnología?

Lamentablemente, la experiencia y los hechos demuestran que no. A menudo se suele aprender una tecnología **exclusivamente para hacerla funcionar**, y no se tienen en cuenta las implicaciones de seguridad que tienen asociadas algunas de las decisiones que se toman. Siguiendo el ejemplo de Tomcat, esta tecnología lleva siendo explotada años y años debido a que sigue siendo extremadamente común encontrar instancias que utilizan cuentas por defecto con contraseñas como “admin”, “tomcat” o “secret”.

Evidentemente, la raíz del problema se encuentra en la falta de conciencia; y normalmente esa conciencia se suele adquirir cuando se es víctima de algún problema de seguridad. ¿Por qué? porque aprender una nueva tecnología requiere tiempo y esfuerzo, pero aprenderla **teniendo en cuenta la seguridad**, lo requiere aún más.

Las medidas de seguridad suelen llevar implícito un aumento en los costes de las empresas (auditorías de seguridad cada cierto tiempo, instalación y configuración de software, aprendizaje y concienciación de los empleados…). Además, algunas de estas medidas pueden ser tediosas, lo que puede acabar resultando en que el remedio es peor que la enfermedad. Un ejemplo común es la imposición a los empleados de cambiar sus contraseñas cada mes, lo que termina en que utilicen combinaciones como “Enero2020”, “Febrero2020”, “Marzo2020” … y así sucesivamente.

Al final, todo lo anterior dificulta que se adopten buenas prácticas de seguridad en muchos aspectos. Si en lugar de hablar de un servidor Tomcat concreto, se estuviera hablando de toda una red empresarial con múltiples servidores, estaciones de trabajo y usuarios… uno puede darse cuenta de que el problema que se presenta **no es para nada sencillo** de resolver.

No obstante, la solución a muchos de los problemas que se presentan en estos entornos parte de algo tan simple, y a la vez tan complicado, como el **organizar, aislar, controlar y proteger los recursos sensibles**. El objetivo de este apartado consiste en analizar las problemáticas habituales que suelen surgir a raíz de utilizar tecnologías Identity Management sin tener en cuenta la seguridad.

El capítulo se dividirá en los siguientes problemas o temáticas:

- Exposición de credenciales: esta temática responde a la facilidad que tiene un atacante de comprometer credenciales (en muchos casos privilegiadas) en redes internas empresariales.
- División pobre de los privilegios: en este apartado se hablará de la falta de aislamiento de los recursos sensibles y el mal uso - o abuso - de privilegios para llevar a cabo tareas en redes empresariales.
- Falta de segmentación interna: este problema hace referencia a la falta de separación entre recursos a nivel de red.
- Falta de control en la red: esta temática responde a la falta de control que existe en las redes empresariales a la hora de detectar anomalías dentro de las mismas.

A partir de este momento se hará especial hincapié en Windows Active Directory, ya que corresponde a la tecnología predominante en estos entornos. No obstante, gran parte de los ejemplos son perfectamente extrapolables a entornos FreeIPA o similar, ya que la raíz de los problemas que se van a presentar a menudo se abstrae de la tecnología utilizada.

3.1. Exposición de Credenciales

Si se hace un análisis de las técnicas que se suelen utilizar para comprometer redes empresariales, el denominador común de todas ellas es uno: **comprometer credenciales**. Sean Metcalf (creador de adsecurity.org) lo explica perfectamente en la siguiente presentación sobre Active Directory.

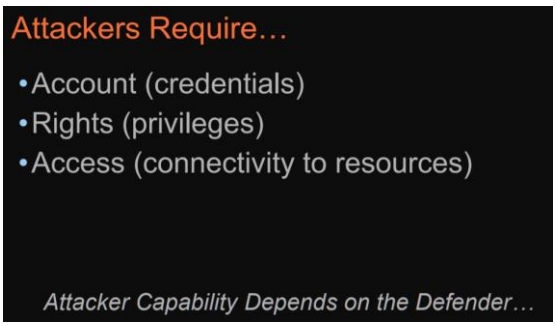


Ilustración 6 - Sean Metcalf - The Current State of Active Directory (& Azure AD) Security: The Good and the Bad

Realmente, cuando se habla de credenciales se está haciendo referencia a la **posibilidad de suplantar la identidad de un usuario y actuar en su nombre**. No obstante, hay que ser consciente de que las credenciales en sí mismas no se limitan a la vieja combinación de nombre de usuario y contraseña; cualquier objeto o situación que permita obtener el contexto de seguridad de un usuario se puede encapsular como objeto de credenciales. Por ejemplo, si un atacante consigue acceso a un ticket TGT de Kerberos de otro usuario, podrá utilizarlo para actuar en su nombre y obtener sus privilegios, y esto será válido tanto en entornos FreeIPA como Active Directory. Más información sobre Pass-the-Ticket en entornos Active Directory en MITRE o el siguiente artículo sobre Pass-the-Cache (Linux) en Stealthbits.

Cuando un atacante accede a una red débil en términos de seguridad, dispone de **infinitas maneras** para comprometer credenciales. Estas técnicas pueden ir desde el abuso de protocolos inseguros (LLMNR, NBT-NS), hasta el uso de phishing (documentos con macros,

ficheros HTA), explotación de servicios (Tomcat, SMB) o simplemente la búsqueda de información sensible en lugares accesibles.

Los pasos que suele realizar un atacante para comprometer un entorno de este estilo son los siguientes:

1. En primer lugar, el atacante debe obtener acceso a la red interna de la manera que sea. Las formas más comunes son el uso de phishing, la explotación de algún servicio vulnerable expuesto en Internet o el abuso de servicios como Office 365 o VPNs con el fin de realizar ataques de fuerza bruta.

2. Una vez el atacante accede a la red interna, comenzará una fase de enumeración. Comprobará la visibilidad que tiene dentro de la red, investigando servicios, tráfico de red y sistemas.

3. En algún momento, tras la fase de enumeración sin autenticación, el atacante obtendrá acceso a algún sistema o credenciales de usuario por medio de técnicas como las explicadas anteriormente (abuso de protocolos, phishing, explotación de servicios vulnerables… etcétera). En este aspecto, hay que entender que las soluciones Identity Management están creadas para automatizar y conectar todos los recursos de una red, lo que permite a usuarios malintencionados la obtención de una gran cantidad de información valiosa una vez autenticados. Con toda esa información, el atacante puede realizar un mapa de la red: sus usuarios, sistemas, políticas y, sobre todo, darse cuenta de posibles fallos de configuración.

4. Habiéndose familiarizado con la red interna a comprometer, el atacante elabora diferentes rutas de ataque. A través de los privilegios del usuario o sistema que haya comprometido inicialmente, se moverá hacia otros sistemas con el objetivo de continuar adquiriendo nuevas credenciales y suplantando a nuevos usuarios.

5. Finalmente, el atacante accederá o comprometerá el objetivo por el que había accedido a dicha red.

El proceso descrito anteriormente puede variar para entornos Active Directory y FreeIPA en algunos aspectos. No obstante, los componentes clave de ambas tecnologías, y la forma de cortar de raíz muchos de los ataques que utilizan el patrón descrito en los puntos anteriores, parten de la misma idea: **proteger la exposición de credenciales**.

Es necesario entender qué significa exactamente esto, ya que a esta idea se le puede llamar de muchas formas y ver desde muchos enfoques diferentes. Además, las posibles soluciones a este problema no recaen sobre una sola cuestión, sino que se enriquecen de **asegurar diferentes componentes y llevar a cabo buenas prácticas** que se irán viendo a lo largo de estos capítulos.

Para mostrar el impacto de la exposición de credenciales se comenzará con un ejemplo utilizando la conocida herramienta Mimikatz. Esta herramienta, creada por Benjamin Delpy y Vincent Le Toux, destaca por muchas cosas; pero sobre todo por sus capacidades para extraer credenciales de sistemas Windows. La idea que se quiere mostrar con este ejemplo es que una vez un atacante tiene privilegios en un sistema, **tiene control sobre prácticamente todo lo que ocurre en él**, sea el sistema operativo o tecnología que sea.

A continuación, se muestran dos de los ejemplos más comunes en lo que a extracción de credenciales se refiere (se debe tener en cuenta que existen más formas).

1. Volcado de credenciales residentes en la base de datos SAM, o NTDS para controladores de dominio: cada sistema Windows dispone de una base de datos local con toda la información de seguridad referente a sus usuarios locales y secretos del sistema; en el caso de controladores de dominio, esta información equivale a los usuarios, sistemas y secretos del dominio. En las siguientes imágenes se puede ver una extracción de credenciales para una base de datos SAM de un sistema arbitrario, y una base de datos NTDS correspondiente a un controlador de dominio.

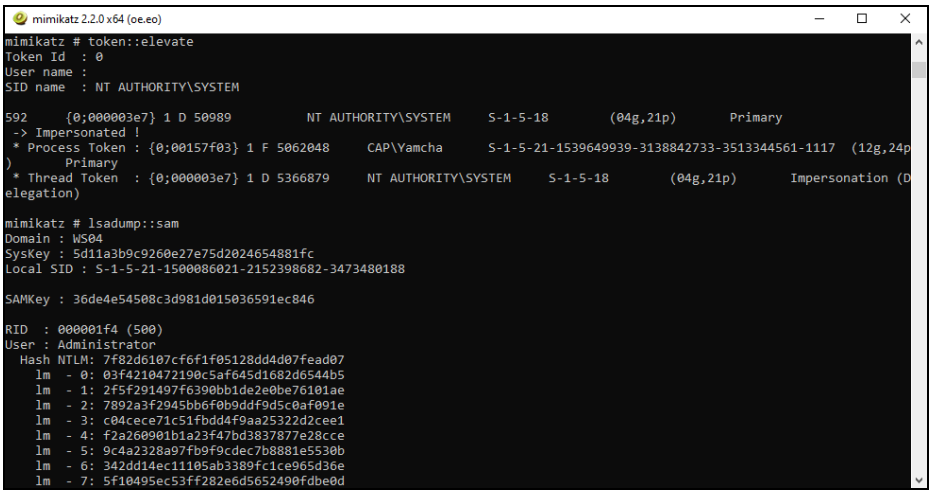


Ilustración 7 - Volcado de credenciales de SAM

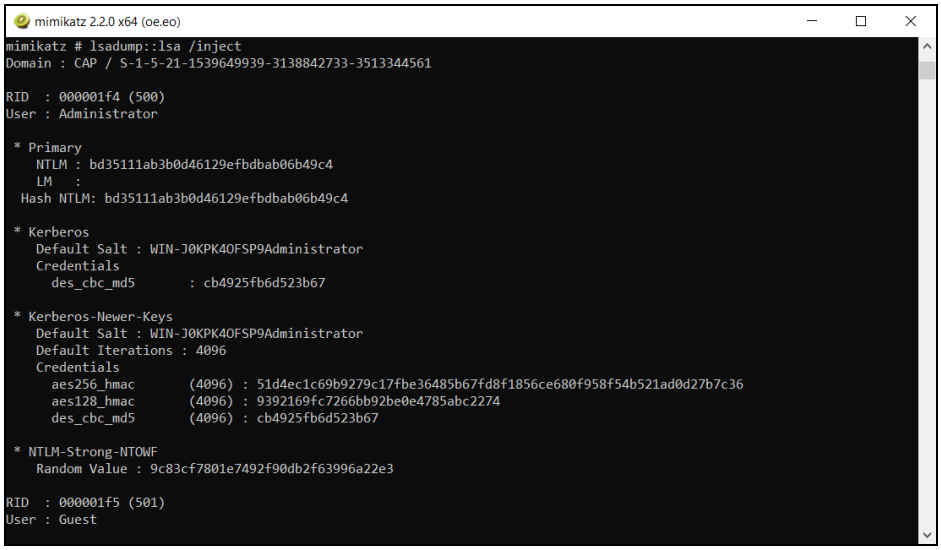


Ilustración 8 - Volcado de credenciales de NTDS

2. Volcado de credenciales residentes en la memoria del proceso lsass.exe, que corresponde al componente Local Security Authority (LSA): estas credenciales están ligadas a las denominadas logon sessions de cada usuario. Dentro cada logon session se establecen credenciales para cada paquete de autenticación soportado en el sistema. En la siguiente imagen se pueden ver las credenciales del usuario Yamcha, del dominio Capsule.corp (CAP), para el paquete de autenticación Msv0_1 (paquete que corresponde a NTLM).

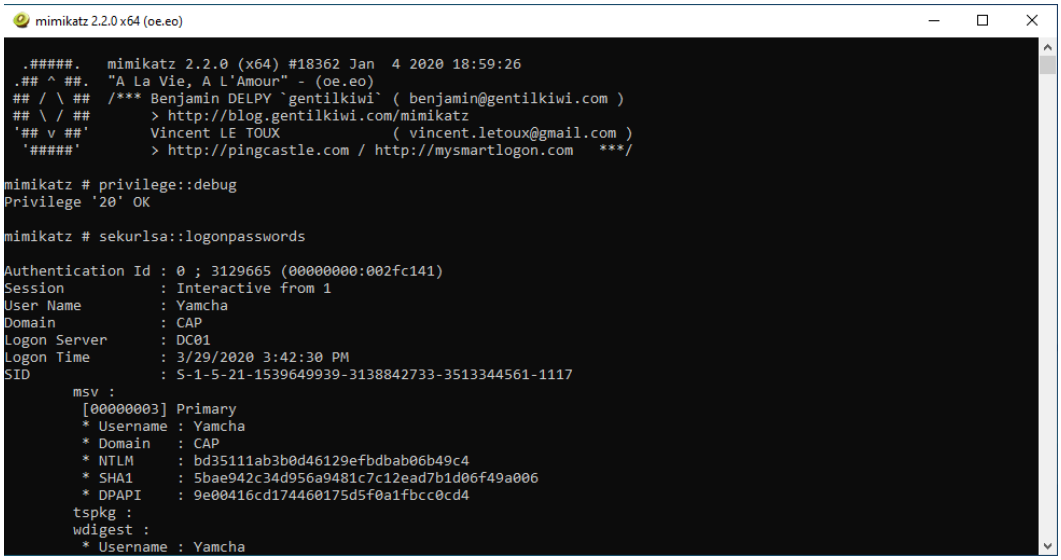


Ilustración 9 - Volcado de credenciales en memoria con Mimikatz

Más información sobre cómo funciona la autenticación en Windows en el siguiente enlace.

De los ejemplos anteriores se pueden obtener las siguientes conclusiones:

1. Si un usuario compromete un sistema Windows va a tener acceso completo a la base de datos local SAM y a toda su información. Destacan principalmente las credenciales de los usuarios locales y los secretos del sistema.

2. Si un usuario compromete un sistema Windows, puede extraer las credenciales residentes en la memoria del proceso lsass.exe. Estas credenciales se almacenan en dicho proceso cuando un usuario se autentica interactivamente en un sistema y permiten la experiencia Single Sign-on (SSO).

3. Si un usuario compromete un controlador de dominio, tendrá acceso a la base de datos NTDS, y con ello a toda la información de dicho dominio (entre ella, las credenciales de todos los usuarios).

En resumen, **con los privilegios suficientes, un atacante puede actuar con libertad dentro de una red o sistema**. Pero, ¿cómo se puede tratar este problema?

Para los ejemplos mostrados, uno podría pensar que una forma de tratar el problema que supone Mimikatz recae en el uso de soluciones antivirus para detectarlo; o bien se podría pensar que es necesario añadir más capas de seguridad a componentes como SAM, NTDS o el proceso lsass.exe. Aunque es cierto que dichas medidas **podrían y pueden ayudar** (Credential Guard, por ejemplo), no dejan de ser protecciones que un atacante con el suficiente tiempo podría evadir.

Para entender por qué este problema afecta a tantas organizaciones, es necesario **identificar y aislar las causas que lo provocan**; como se dice comúnmente, “mejor prevenir que curar”.

En este punto se ha visto que, si un atacante compromete un sistema, podrá extraer gran cantidad de información sensible que le permitirá comprometer otros sistemas. Por ejemplo, si el usuario Yamcha es administrador en diez sistemas diferentes, y sus credenciales son comprometidas por un atacante, este a priori podrá acceder a los veinte sistemas con privilegios. De este ejemplo nace la siguiente pregunta… **¿Es necesario que Yamcha sea administrador en veinte sistemas diferentes?**

3.2. División Pobre de los Privilegios

El apartado anterior hacía referencia a la exposición de credenciales como uno de los motivos más importantes con el que se pueden comprometer redes empresariales. Y es así, pero es importante entender que el problema de la exposición de credenciales no recae solamente en el hecho de que un atacante tenga la posibilidad de extraerlas de un sistema. También es muy importante **entender si esas credenciales deberían estar, en primer lugar, donde están**.

En este documento se va a hablar de división pobre de los privilegios a dos situaciones diferentes – pero relacionadas – que se pueden presentar en una organización, independientemente de la tecnología utilizada:

1. La situación en la que se configuran **permisos innecesarios** (a menudo exagerados) a una gran cantidad de objetos dentro de una red empresarial.
2. La situación en la que objetos críticos o privilegiados "conviven" con objetos que tienen mayor superficie de ataque y facilidad para ser comprometidos. Es decir, una **falta de separación en base a la importancia de los objetos**.

Rescatando el ejemplo propuesto en el apartado anterior - Yamcha es administrador en veinte sistemas diferentes - el punto número uno vendría a cuestionar por qué Yamcha **"necesita" ser administrador en veinte sistemas diferentes**; mientras que el punto número dos cuestionaría el **cómo podría llegar a ser comprometido** Yamcha, o **las posibilidades que tendría Yamcha para comprometer a otros usuarios**.

Permisos Innecesarios

Para entender este problema no hay ejemplo más simple que el del grupo Domain Admins en dominios Active Directory o el grupo Admins para dominios FreeIPA. Estos grupos vienen por defecto en la instalación de estas tecnologías y tienen un objetivo claro: **administrar la red interna**.

Un miembro de cualquiera de estos grupos va a tener facilidad para moverse por la red, acceder a los sistemas, configurar políticas, crear o modificar usuarios… etcétera. Las empresas tienden a abusar de estos grupos para realizar tareas dentro de sus redes, ya que son una vía **rápida y cómoda** en lo que a privilegios se refiere. Algunos ejemplos comunes:

- La empresa necesita un usuario para administrar una serie de sistemas: en lugar de configurar los permisos enfocándose en los sistemas concretos, se añade al usuario a un grupo privilegiado como Domain Admins.
- La empresa ofrece un nuevo servicio que corre bajo una cuenta de servicio que requiere ciertos privilegios para trabajar con otros sistemas: en lugar de analizar las necesidades del servicio y configurar una política de privilegio mínimo necesario, se añade la cuenta de servicio a Domain Admins.
- La empresa necesita a un usuario que cree políticas: en lugar de añadirlo a un grupo específico que permita la creación de las mismas, se añade a un grupo general como Domain Admins, lo que ofrece a dicho usuario privilegios innecesarios.

Esto desemboca en organizaciones con **innumerables usuarios que disponen de vías para comprometer todo un dominio**. Es importante tener en cuenta que Domain Admins y Admins son solo un ejemplo de un problema mayor. Por ejemplo, Active Directory por defecto trae numerosos grupos privilegiados que no se recomienda utilizar de forma descuidada.

Algunos ejemplos:

- Enterprise Admins: sus miembros disponen de todos los privilegios en todos los dominios pertenecientes al bosque al que pertenezcan.
- Schema Admins: disponen de privilegios para modificar el esquema de un bosque.
- Backup Operators: disponen de privilegios para autenticarse de Domain Controllers y realizar tareas de copias de seguridad en todo el dominio.
- Group Policy Creator Owners: sus miembros pueden crear, modificar y eliminar políticas de grupo en un dominio.

Esto se traduce en que un usuario malicioso dispone de una superficie de ataque enorme, ya que cuantos más usuarios privilegiados hay en un dominio, más posibilidades hay de que uno de ellos pueda ser comprometido.

Groups

Group Name	Nb Admins	Nb Enabled	Nb Disabled	Nb Inactive	Nb PWd never expire	Nb Smart Card required	Nb Service accounts	Nb can be delegated	Nb external users
Account Operators	160	103	57	18	26	0	2	103	0
Administrators	209	143	66	18	29	0	3	142	0
Backup Operators	1	1	0	0	1	0	1	0	0
Cert Publishers	0	0	0	0	0	0	0	0	0
Crypto Operators	0	0	0	0	0	0	0	0	0
Domain Admins	25	21	4	3	16	0	2	21	0
Enterprise Admins	1	1	0	0	1	0	1	0	0
Incoming Forest Trust Builders	0	0	0	0	0	0	0	0	0
Network Operators	0	0	0	0	0	0	0	0	0
Print Operators	149	92	57	15	17	0	2	92	0
Schema Admins	20	20	0	1	13	0	2	17	0
Server Operators	76	68	8	7	34	0	2	67	0

Ilustración 10 - Grupos administrativos AD mediante PingCastle

La imagen anterior muestra un escenario que podría presentarse en una empresa con respecto a los grupos administrativos de Active Directory (tabla creada a partir de la herramienta PingCastle). Como puede verse, aunque el grupo Domain Admins solo disponga de 25

miembros, la cantidad de miembros que tienen otros grupos con privilegios parecidos o similares es mayor (Administrators dispone de 209 miembros, Account Operators 160 miembros, Print Operators 149 miembros… etcétera).

Falta de Separación en Base a la Importancia de los Objetos

El segundo punto comentado anteriormente es el de la **convivencia de recursos críticos con recursos regulares**. Un ejemplo clave para entender el impacto de esta situación podría ser un escenario en el que un administrador de red trabaja en el mismo ordenador que varios empleados regulares de la empresa.

Evidentemente esto es un riesgo ya que se sabe que **un usuario con privilegios en un sistema controla todo lo que pasa en él**. En el momento en el que cualquiera de estos empleados regulares sea comprometido, el atacante tendrá vía directa para comprometer al administrador de la red – por el medio que sea – pues trabajan todos en el mismo sistema.

En este aspecto es clave entender cómo funcionan las tecnologías Single Sign-On para cada sistema operativo. La explicación se centrará para Windows y Active Directory, aunque muchas de las implicaciones que se verán se puede aplicar perfectamente a FreeIPA u otras tecnologías.

En primer lugar, se sabe que **Single Sign-On** o "inicio de sesión único" hace referencia a la tecnología que habilita a un usuario a **acceder a diferentes recursos a partir de una única autenticación**. Esto se puede comprobar fácilmente en Active Directory autenticándose en un sistema y accediendo a una carpeta compartida a través de la red. Si el usuario utilizado tiene permisos para acceder a la carpeta, se comprobará que **no es necesario volver a especificar las credenciales** en dicho acceso.

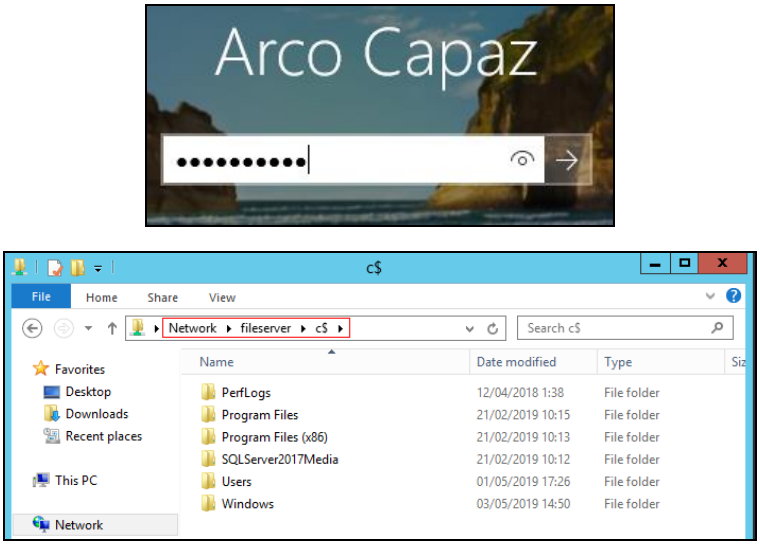


Ilustración 11 - Single Sign-On accediendo a carpeta de red

Este SSO se consigue a través del **almacenamiento de credenciales en la memoria del sistema**, tras la primera autenticación de un usuario. En el ejemplo anterior, una vez que un usuario autenticado quiere acceder a un recurso de la red (por ejemplo, una carpeta compartida), Windows utiliza las credenciales almacenadas para autenticar al usuario de forma transparente y habilitarle el acceso.

Recordando lo explicado en el apartado 3.1 de exposición de credenciales, Mimikatz permite la extracción de las mismas a través del comando sekurlsa::logonpasswords.

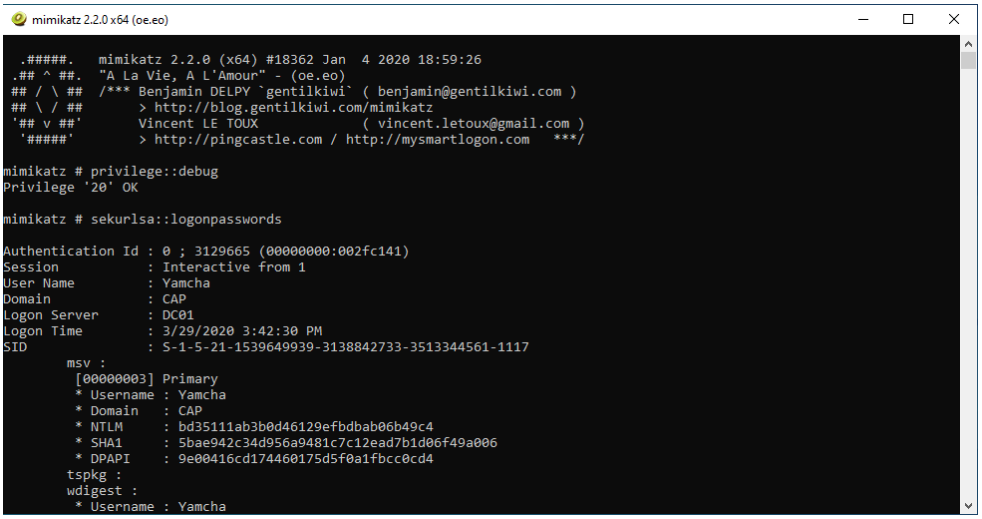


Ilustración 12 - Sekurlsa::logonpasswords

Con este comando, Mimikatz se encarga de extraer las credenciales que Windows utiliza para llevar a cabo el SSO con los diferentes paquetes de autenticación soportados por el sistema (normalmente, Kerberos y NTLM en entornos de Active Directory actuales).

No obstante, es importante diferenciar **qué situaciones acaban con credenciales en memoria y cuáles no**.

Microsoft diferencia dos tipos de autenticaciones: las interactivas y las no interactivas.

- Autenticaciones interactivas: corresponden normalmente a aquellas que se realizan cuando un empleado inserta sus credenciales para utilizar el ordenador estando frente a él. Como ya se ha indicado anteriormente, estas autenticaciones **resultan en credenciales almacenadas en la memoria del sistema**. Otros ejemplos son el uso de escritorio remoto o la creación de procesos especificando credenciales con runas.exe.

- Autenticaciones no interactivas: corresponden normalmente a los accesos de red. En el ejemplo explicado anteriormente, cuando el usuario accede a una carpeta de red, se está realizando una autenticación no interactiva en el sistema que está compartiendo dicha carpeta. Estas autenticaciones tienen la peculiaridad de que el usuario simplemente **demuestra que dispone de las credenciales correctas, pero estas no son almacenadas en el sistema remoto** (existen algunas excepciones como el caso de escritorio remoto).

Por lo tanto, uno de los motivos más importantes por el que un atacante puede moverse y acabar comprometiendo una red empresarial es la presencia de estas credenciales en la memoria de los sistemas, a causa de las autenticaciones interactivas.

De este apartado "División Pobre de los Privilegios" se pueden sacar dos conclusiones claras.

1. Una empresa que no se asegure de cumplir una política de mínimo privilegio a la hora de llevar a cabo sus tareas, tendrá una **gran cantidad de usuarios privilegiados**. Esto afectará directamente a la cantidad de credenciales privilegiadas presentes en diferentes sistemas (sistemas donde se hayan autenticado interactivamente esos

usuarios) y **aumentará las posibilidades y superficie de ataque** a usuarios malintencionados que se encuentren dentro de la red.

2. Una empresa que no se asegure de **dividir los objetos en base a la importancia** o privilegios que tienen, resultará en un entorno en el cual los objetos privilegiados se encuentren igual de expuestos que cualquier otro objeto regular. Esto facilitará enormemente la labor a un atacante para tener acceso a elementos privilegiados de la red.

Si se suma el impacto de los dos puntos anteriores, y se tiene en cuenta lo que ya se explicó en el apartado de exposición de credenciales, poco a poco se va haciendo evidente el problema de organización que suele presentarse en las empresas.

3.3. Falta de Segmentación Interna

De los apartados anteriores se ha concluido que, en empresas mal estructuradas, un atacante dispone de multitud de oportunidades para comprometer credenciales que, en muchos casos, acaban siendo de usuarios con altos privilegios.

Uno de los motivos explicados en el apartado anterior hacía referencia a la **falta de separación en base a la importancia de los objetos**. Es decir, los objetos críticos (por ejemplos, miembros de Domain Admins), en muchas empresas conviven junto a objetos regulares (usuarios comunes).

En el apartado anterior convivir hacía referencia a utilizar el mismo sistema. En este apartado se va a extender la idea propuesta en el apartado anterior, pero en lugar de hablar a nivel de un sistema, se hablará **a nivel de red**.

Un ejemplo para entender esta situación podría ser el siguiente:

- Un **administrador** de red utiliza un ordenador con un **Windows vulnerable**.
- Un **usuario regular** utiliza una estación de trabajo que tiene **visibilidad a todos los servicios y sistemas de la red**.

Es importante entender que cuando se habla de visibilidad, no se está hablando necesariamente de permisos para acceder. En el ejemplo anterior, un atacante que lograra comprometer la estación de trabajo regular, a priori no tendría permisos para acceder al sistema del administrador. No obstante, tendría vía directa para analizar y explotar vulnerabilidades en él, lo que en este ejemplo resultaría en un riesgo similar a disponer de privilegios.

Por supuesto, que un administrador utilice un Windows vulnerable es un riesgo inaceptable; pero la idea que hay que sacar de este ejemplo es que **una estación de trabajo regular tampoco debería disponer de visibilidad hacia un sistema de administración**. En una empresa normal, no debería existir situación ni justificación que respalde esa visibilidad.

La siguiente imagen muestra un escenario como el mencionado, donde todos los sistemas se encuentran en la misma red sin restricciones de acceso.

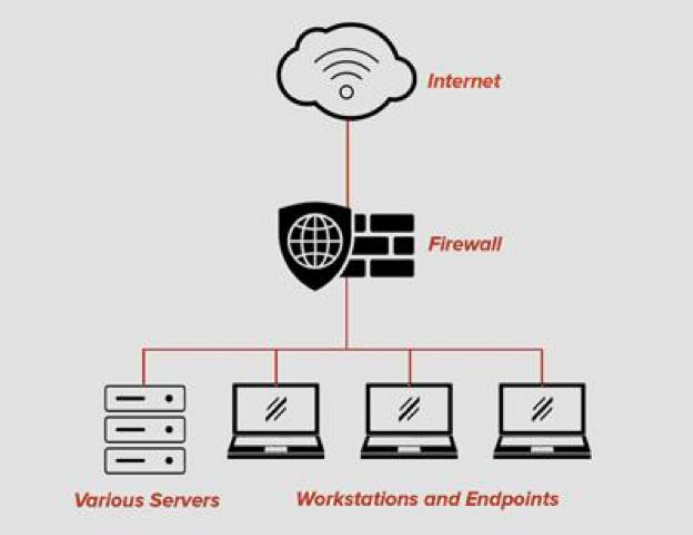


Ilustración 13 - Ejemplo de red sin segmentar. Fuente: https://www.rgtech-elp.com/segmented-networks/

Por este motivo se recomienda realizar una segmentación de los recursos a nivel de red, para evitar la exposición innecesaria de información y acceso.

3.4. Falta de Control en la Red

Por último, pero desde luego no menos importante, se encuentra la falta de control en las redes internas. Se va a hablar de control en el sentido de que exista un **equipo de seguridad** monitorizando los movimientos y eventos que surgen en la red interna y sus sistemas: el comúnmente denominado **Blue Team**. A pesar de que en este documento no se entrará en detalles sobre cómo funciona uno de estos equipos, es conveniente entender su papel.

En los últimos años, las empresas han dedicado muchos de sus recursos a proteger sus **redes perimetrales**. Es un movimiento lógico, ya que los sistemas que se encuentran en estas redes están expuestos al público (Internet) y pueden ser una ventana de acceso crítica hacia las redes internas. No obstante, esta importancia que se le ha dado a las redes perimetrales, se le ha restado en muchos casos a las redes internas, resultando en organizaciones que apenas tienen visibilidad sobre lo que sucede en ellas.

Los equipos de seguridad deberían encargarse de **detectar comportamientos anómalos en las redes y sistemas de la organización**. Esta tarea suele ser extremadamente compleja por dos motivos principales:

1. **Cuando una red está ordenada y es predecible, es fácil de administrar y monitorizar**. Pero si la empresa falla en los puntos que se han venido explicando en apartados anteriores, la red va a ser un caos. Esto afecta directamente a las capacidades de un Blue Team, ya que una red de estas características es impredecible, lo que hace extremadamente complejo diferenciar comportamientos normales frente a comportamientos anómalos.

2. Los atacantes con más experiencia van a buscar **mezclarse con los comportamientos legítimos de una red**. Incluso para organizaciones bien estructuradas, puede llegar a ser muy complejo detectar el rastro de un atacante precavido con experiencia.

Un ejemplo para entender los dos puntos anteriores podría ser el siguiente. Supongamos una estación de trabajo (Workstation01), donde trabaja el usuario Yamcha, y un servicio sensible llamado Service01 al que Yamcha tiene acceso por un incorrecto establecimiento de permisos.

Si la empresa está bien organizada, sabrá que al servicio Service01 **solo deben acceder** ciertos usuarios o grupos predefinidos. En el momento en el que se detecte que un usuario fuera de ese ámbito (Yamcha) ha accedido al servicio, se detectará como un **evento anómalo**. El equipo de seguridad recibirá una alerta e investigará si esto ha sido a raíz de un ataque o una simple coincidencia o fallo humano; de cualquier manera, permitiría descubrir que Yamcha disponía de permisos mal configurados y se podrían corregir.

En cambio, si la empresa está mal organizada, en ningún caso va a tener constancia de los usuarios o grupos que utilizan el servicio Service01 (probablemente porque además de Yamcha, lo podrán utilizar muchos más). Esto resulta en que, aunque el equipo de seguridad pueda por casualidad ver que Yamcha ha accedido al servicio, no tendrá la capacidad – o llevará mucho más trabajo conseguirla – de relacionar dicho evento con algo anómalo.

Como conclusión, **una empresa bien estructurada será más fácil de administrar y proteger**. Por ello es tan importante tener en cuenta la seguridad en las etapas tempranas de cualquier proceso.

4. INFRAESTRUCTURAS ENFOCADAS EN LA SEGURIDAD

La seguridad de una red interna organizacional **depende en gran medida de la integridad de las cuentas privilegiadas** que se utilizan para administrar, gestionar y desarrollar dentro de la misma. Los usuarios maliciosos a menudo buscarán comprometer estas cuentas con el fin de acceder a recursos sensibles gracias a los privilegios obtenidos. Por este motivo se plantea la necesidad de un diseño seguro, estructurado e íntegro.

Las infraestructuras enfocadas en la seguridad deben tener muy en cuenta lo anterior, y su objetivo principal deberá ser el de **proteger y aislar** dichas cuentas privilegiadas para minimizar las posibilidades de que sean comprometidas por un atacante.

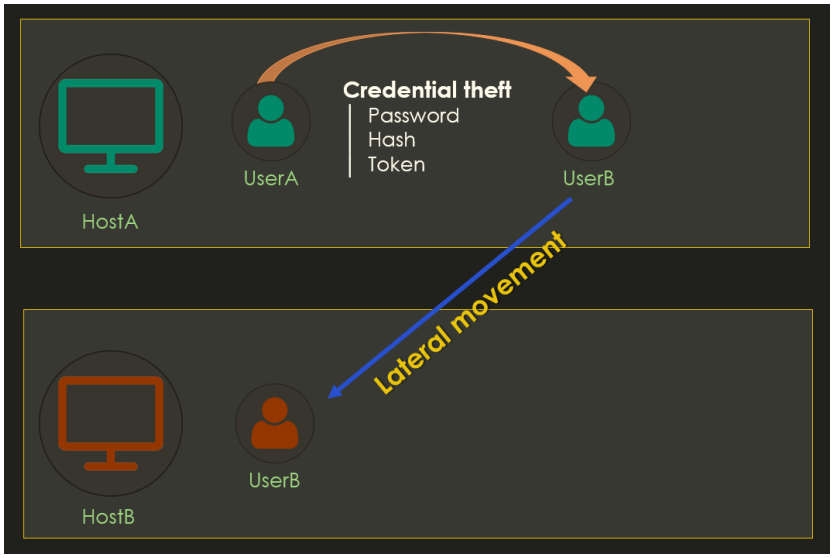


Ilustración 14 - Compromiso de una cuenta y suplantación

Recordando los puntos explicados en el capítulo anterior, una cuenta privilegiada es comprometida cuando se tiene acceso a algún tipo de credencial que permite definirla: contraseña en claro, hash, token... etcétera. Es decir, una cuenta privilegiada **siempre debe actuar de tal forma que no se expongan sus credenciales** en lugares accesibles por cuentas regulares o de menor valor para la empresa.

A parte de lo anterior, es importante ser consciente de la cantidad de cuentas privilegiadas que dispone una organización ya que, como se vio en los ejemplos del capítulo anterior, es común encontrar cuentas con **permisos exagerados e innecesarios**, lo que aumenta la exposición y probabilidades de sean comprometidas.

La **segmentación de la red interna** también jugaba un papel importante a la hora de proteger frente a posibles ataques en la red interna. En este aspecto, segmentar una red permite, sobre todo, **facilitar su administración y monitorización**; no obstante, también puede dificultar los movimientos de un atacante dentro de la red, lo que podría desembocar en una detección más eficaz del mismo.

Para conseguir proteger sus cuentas privilegiadas, una organización debe **separar** efectivamente las tareas administrativas, de gestión y desarrollo frente al resto de tareas comunes que se realizan dentro de la red interna. Las cuentas de administración, gestión o

desarrollo deben usarse solo para tal fin; y dicho fin debe realizarse desde un entorno seguro y aislado, libre del máximo de superficie de ataque posible.

Se debe tener en cuenta, no obstante, que no existe un método infalible frente al compromiso o a los ataques. Este apartado pretende mostrar buenas prácticas que ayudarán a disminuir, sobre todo, **las probabilidades de compromiso de cuentas privilegiadas**. Pueden existir, y existen, otros enfoques y buenas prácticas que podrían aplicarse alternativa o complementariamente a las explicadas en este apartado.

En relación a lo anterior, es recomendable que una empresa asuma lo que comúnmente se denomina como "**assume breach mindset"** (asumir el compromiso). Esto es, no buscar una solución infalible que probablemente no exista, sino ser consciente de que en cualquier momento puede haber un incidente y se deben disponer diferentes capas de seguridad para poder **detectar**, **responder**, y **tomar medidas lo más rápido posible**. Este enfoque es el que siguen grandes empresas como, por ejemplo, Microsoft.

Tal y como dijo el ya retirado director de la CIA y NSA en 2012, Michael Hyden:

> *"Fundamentally, if somebody wants to get in, they're getting in… accept that. What we tell clients is: number one, you're in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated."*

En este apartado se verán los siguientes puntos o medidas que tienen como objetivo final **aislar y proteger las cuentas privilegiadas** de una red empresarial, lo que disminuirá la superficie de ataque y facilitará la administración y monitorización de la red.

- Separación de cuentas privilegiadas
- Uso de sistemas protegidos
- Segmentación de la estructura organizacional y red interna

4.1. Separación de Cuentas Privilegiadas

Como ya se ha explicado anteriormente, una cuenta privilegiada hace referencia a una cuenta que tiene **acceso a todos o gran parte de los recursos** de una organización.

Un ejemplo de cuenta privilegiada es la que pertenece a grupos como Doman Admins (Active Directory) o Admins (FreeIPA), pero también podrían ser las cuentas utilizadas para Helpdesk (soporte de las estaciones de trabajo) o para administración de servicios (Sharepoint, Exchange, Cloud, etcétera). En resumen, una cuenta privilegiada es aquella cuyo compromiso podría significar un **impacto considerable en el negocio de una organización**.

Para todas las tareas consideradas como privilegiadas se recomienda crear cuentas dedicadas exclusivamente para la realización de las mismas. De esta forma se pueden separar los riesgos a los que se enfrentan las cuentas regulares – como ataques de phishing – y evitar su exposición innecesaria.

Es decir, una cuenta privilegiada **no debería utilizarse** para navegar por Internet, comprobar el correo o realizar tareas comunes del día a día; una cuenta privilegiada **debe utilizarse única y exclusivamente** para la tarea para la que fue creada, tal y como se indica en este documento.

Por ejemplo, supongamos que Bulma realiza tareas de administración en el dominio CAPSULE.CORP. En este escenario, Bulma debería disponer de dos cuentas diferentes:

- Una para sus tareas de día a día como navegar por Internet o acceder al correo electrónico: **bulma@capsule.corp**.
- Otra con permisos de Domain Admin para realizar únicamente tareas de administración en el dominio: **bulma_da@capsule.corp**.

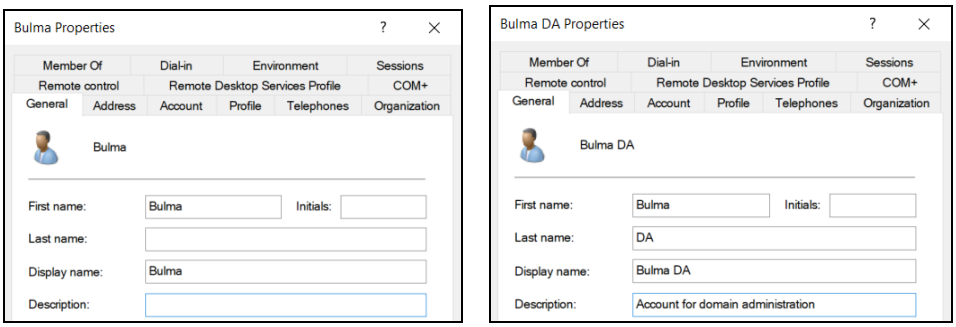


Ilustración 15 - Separación de cuentas

Si Bulma fuera víctima de un ataque originado desde Internet, la cuenta que debería estar utilizando es la de un usuario regular. De esta manera, el atacante que ha obtenido acceso a la red interna lo hará desde un **punto de vista no privilegiado**, lo que permitirá a la organización un cierto margen para actuar e intentar detectarlo antes de que se genere un impacto sobre su negocio.

Mediante esta práctica se puede hacer frente a los problemas de **división pobre de los privilegios** y **exposición de credenciales** explicados en el capítulo 3 de este documento. No obstante, como se verá a continuación, el crear diferentes cuentas no es una medida eficaz en sí misma, sino que, como se verá en el siguiente apartado, debe utilizarse junto a otras medidas para que así lo sea.

4.2. Uso de Sistemas Protegidos

El ejemplo del apartado anterior demuestra la gran ventaja que tiene separar cuentas privilegiadas para evitar su exposición directa a riesgos como Internet. No obstante, la separación de cuentas en sí misma no evita exposiciones indirectas que puedan suceder una vez un atacante tiene acceso a la red organizacional.

Recogiendo nuevamente el ejemplo de Bulma, supongamos que ha sido víctima de un ataque de phishing y el atacante logra acceso a su sistema.

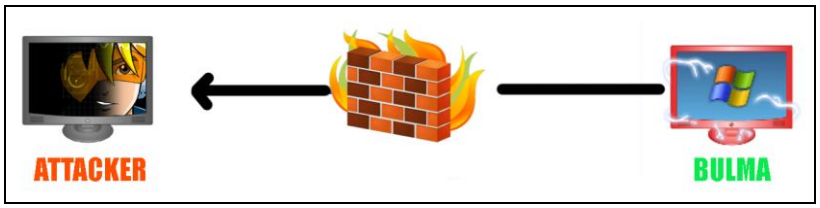


Ilustración 16 - Compromiso de Bulma

Es cierto que inicialmente, gracias a la separación de cuentas, el atacante solo dispondrá de los permisos otorgados por la cuenta regular de Bulma. Sin embargo, si Bulma utiliza su cuenta privilegiada en el mismo sistema en el que usa su cuenta regular, la separación no servirá para nada: el atacante probablemente termine accediendo a ella.

Este problema se vio en el capítulo 3 de este documento y responde a una exposición de credenciales y falta de separación en base a la importancia de los objetos.

Ilustración 17 - Compromiso de privilegios. Fuente: https://docs.microsoft.com/es-es/windows-server/identity/securing-privileged-access/privileged-access-workstations

De nuevo, se enfatiza en que esta problemática no afecta a una tecnología en particular; si un atacante consigue privilegios en un sistema, tiene un potencial control sobre lo que sucede en el mismo.

Por ejemplo, supongamos que el escenario es en un dominio FreeIPA y Bulma utiliza un sistema Linux. Como en estos entornos se utiliza Kerberos para llevar a cabo las autenticaciones, Bulma dispondría de diferentes tickets en su sistema. Un atacante con permisos en dicho sistema podría acceder fácilmente a esa información, por lo que, si Bulma utilizara su cuenta privilegiada, el atacante tendría acceso a ella.

Un ejemplo de esta situación es descrito en este artículo de la empresa de seguridad SpecterOps, donde un usuario con permisos de root en un sistema unido a un dominio FreeIPA puede volcar todos los tickets del sistema mediante la utilidad tickey.

```
[root@bastion GNU-Linux-x86]# kinit admin
Password for admin@WESTEROS.LOCAL:
[root@bastion GNU-Linux-x86]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@WESTEROS.LOCAL

Valid starting       Expires              Service principal
11/12/2019 23:53:56  11/13/2019 23:53:54  krbtgt/WESTEROS.LOCAL@WESTEROS.LOCAL
[root@bastion GNU-Linux-x86]# ./tickey
Tickey - Copyright 2019 Tarlogic
[*] krb5 ccache_name = KEYRING:persistent:%{uid}
[+] root detected, so... DUMP ALL THE TICKETS!!
[*] [uid:0] 4 tickets found
[+] [uid:0] Tickets written into /tmp/__krb_0.ccache
[root@bastion GNU-Linux-x86]# export KRB5CCNAME=/tmp/__krb_0.ccache
[root@bastion GNU-Linux-x86]# klist
```

Ilustración 18 - Volcado de tickets de Kerberos con Tickey

Por estos motivos se recomienda realizar una separación no solo de cuentas, sino también de sistemas. Utilizar sistemas protegidos y aislados, para realizar aquellas tareas consideradas como privilegiadas.

Microsoft llama a estos sistemas **Privileged Access Workstations** o **PAW**, pero, en esencia, no dejan de ser simples ordenadores o máquinas virtuales **aislados y con más restricciones** que uno común.

Una estación PAW consiste en un sistema dedicado exclusivamente a realizar tareas privilegiadas, lo que permite evitar los riesgos que conllevan actividades comunes como el acceso a Internet. De forma simplificada, son estaciones de trabajo restringidas y diseñadas para disponer del máximo grado de seguridad posible. Para conseguir esto, deben disponer siempre de software actualizado e implementar diferentes mecanismos de seguridad para prevenir y/o registrar posibles riesgos.

Ilustración 19 - Privileged Access Workstations. Fuente: https://docs.microsoft.com/es-es/windows-server/identity/securing-privileged-access/privileged-access-workstations

Este tipo de sistemas suelen enfocarse en mitigar los riesgos de mayor impacto y mayor probabilidad de compromiso, incluyendo además posibles riesgos que puedan disminuir la efectividad de las PAW.

A modo de esquema, una PAW suele disponer de las siguientes características:

- La mayor parte de ataques a organizaciones son originados directa o indirectamente desde Internet. Por ello, este tipo de sistemas son aislados y no disponen de acceso a Internet.
- Al tratarse de sistemas restringidos con numerosas medidas de seguridad, esto puede afectar a la usabilidad de los mismos. Si una PAW es extremadamente compleja para realizar tareas, los usuarios tratarán de evitarla (lo que puede suponer un riesgo). Por este motivo, hay que asegurarse de realizar un balance entre seguridad y usabilidad cuando se hace uso de este tipo de sistemas.
- Una PAW debe encontrarse aislada dentro de la propia red interna organizacional. Aunque no estén expuestas directamente a potenciales ataques de Internet, muchos otros sistemas de la red sí que lo van a estar. Por este motivo es importante proteger las estaciones PAW de posibles ataques originados dentro de la propia red interna (se hablará de esto en el apartado “Segmentación de la estructura organizacional y red interna”).
- Estas estaciones deben estar protegidas también frente a posibles ataques físicos, y asegurar la integridad de todo el software y hardware que interactúa con ellas.

En resumen, y recogiendo el ejemplo inicial expuesto en el capítulo, el uso de PAWs evitaría que un atacante con permisos administrativos en el sistema de Bulma consiguiese acceso a su cuenta administrativa. Esto es debido a que Bulma únicamente utilizaría dicha cuenta en un sistema aislado y protegido – la PAW – lo que obligaría al atacante a buscar otros métodos para moverse y comprometer la red.

Por lo tanto, mediante la separación de cuentas privilegiadas y el uso de PAWs se haría frente, de una manera eficaz, a los problemas de exposición de credenciales y división pobre de los privilegios explicados en el punto 3 de este documento.

4.3. Segmentación de la Estructura Organizacional y Red Interna

Finalmente, como ya se mencionó en los apartados del capítulo 3 sobre segmentación interna y falta de control en la red, disponer de una correcta organización de la estructura interna empresarial es clave para administrarla y controlarla frente a posibles anomalías.

No todos los sistemas, servidores o cuentas tienen el mismo valor para la empresa. Por lo tanto, el valor de un recurso puede ser una buena variable para categorizarlo dentro de las estructuras organizacionales y/o subredes de la empresa. Este apartado se dividirá en dos campos:

- La organización de los recursos en capas administrativas dentro del directorio de la tecnología Identity Management utilizada.
- La división de los sistemas de la empresa en diferentes subredes.

Modelo de Capas Administrativas

El modelo de capas administrativas consiste en dividir la estructura organizacional de sistemas en base a diferentes capas o zonas dentro del directorio de la empresa. El propósito de este modelo es el de **separar las capas de alto riesgo** – y con mayor probabilidad de compromiso – de aquellas que contienen sistemas considerados como sensibles o de alto valor (que será, a su vez, donde se encuentren las cuentas privilegiadas trabajando).

Este modelo se puede aplicar de muchas formas dependiendo la organización o entorno, no obstante, para este apartado se va a tomar como referencia las recomendaciones de Microsoft.

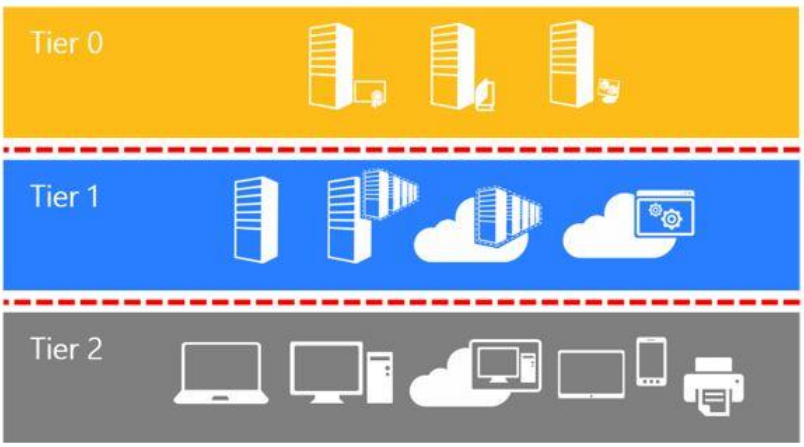


Ilustración 20 - Capas administrativas. Fuente: https://docs.microsoft.com/es-es/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Microsoft divide este modelo en tres niveles o capas que reflejan exclusivamente la organización de cuentas y sistemas administrativos.

- Tier 0: Esta capa hace referencia a todas las cuentas que tienen control sobre el dominio empresarial. En ella se incluirían cuentas, grupos y recursos que, directa o indirectamente, dispongan de privilegios en el dominio/bosque Active Directory o

FreeIPA (por ejemplo). Todos los recursos de esta capa deberían disponer del mismo nivel de protección, ya que su compromiso supone el compromiso del resto de recursos que haya en el dominio.

- Tier 1: Esta capa hace referencia a las cuentas que tienen control sobre servidores o aplicaciones dentro del dominio empresarial. En ella se incluirían todos los servidores de aplicaciones del dominio (bases de datos, cloud, aplicaciones empresariales…). A pesar de que no deberían permitir comprometer un dominio completo, las cuentas dentro de esta capa tienen acceso a una gran cantidad de información de gran valor para la empresa.

- Tier 2: Esta capa hace referencia a las cuentas que tienen control sobre las estaciones de trabajo de los usuarios y sus dispositivos. Nuevamente, a pesar de que no podrán acceder a información de las capas superiores, las cuentas administrativas de esta capa tendrán acceso a toda la información que esté alojada en estaciones de trabajo y dispositivos de los usuarios.

La idea de utilizar este modelo es con el fin de ordenar la estructura organizacional para prevenir posibles situaciones de "escalado de privilegios". Esto se consigue limitando lo que pueden controlar los administradores y a dónde pueden acceder.

Por un lado, el modelo de capas debe evitar que una cuenta de una capa inferior pueda acceder a recursos de una capa superior; por otro lado, debe restringir también que una cuenta de una capa superior exponga sus credenciales en una capa inferior. La siguiente imagen muestra esta idea:

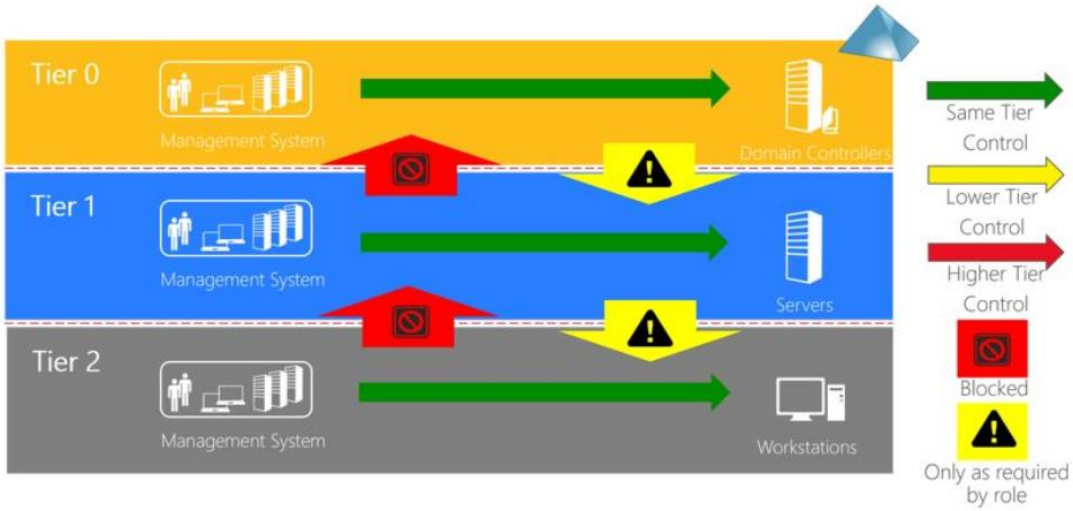


Ilustración 21 - Restricciones de acceso. Fuente: https://docs.microsoft.com/es-es/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Por ejemplo, las cuentas de la capa 2 no deberían tener en ningún caso privilegios para administrar recursos de la capa 1.

Lo que sí se puede dar es el caso en el que, por cuestiones de negocio de la empresa, cuentas de la capa 1 tengan privilegios para administrar recursos de la capa 2. En estas situaciones se debe prestar especial atención a que dicha administración se realice de forma segura sin exponer las credenciales de las cuentas privilegiadas. Para entender esto hay que recordar cómo funcionan las tecnologías de Single Sign-on (SSO) como Kerberos o NTLM.

Más información de estos procesos se puede encontrar en el siguiente enlace de Microsoft.

Supongamos que el administrador Paco de la capa 1 trabaja en un sistema llamado PacoPC.

Si Paco necesita administrar un servidor de su red, solicitará y utilizará el material de credenciales pertinente para llevar a cabo la autenticación en dicho servidor. Por ejemplo, en dominios Active Directory o FreeIPA, Paco tendría que solicitar un ticket TGT a través de Kerberos con su contraseña y, posteriormente, solicitar un ticket de servicio para acceder al servidor que quiere administrar.

Lo importante que hay que entender del anterior proceso es que, **en el servidor objetivo, no se almacenará por defecto ningún material de credenciales perteneciente a Paco**. Esto es debido a que **se trata de una autenticación de red, donde solo se demuestra que se tienen las credenciales, pero no se envían al servidor objetivo**, lo que evita que potenciales atacantes con permisos en dicho servidor puedan suplantar la identidad de Paco y utilizar sus privilegios para moverse por la red.

Por defecto **una autenticación de red no debería almacenar credenciales** de ningún tipo en el sistema accedido. No obstante, la realidad es que **existen excepciones** en las que sí que se almacenan credenciales en el sistema accedido. Por ejemplo, utilizar escritorio remoto para acceder a sistemas Windows por defecto almacena credenciales en el sistema accedido; otro ejemplo es el uso de la delegación de Kerberos, característica que si es configurada en un sistema puede desembocar en el almacenamiento de credenciales cuando se accede al mismo.

Por las excepciones anteriores existen **características como "Account is sensitive and cannot be delegated" o el grupo Protected Users** dentro de tecnologías como Active Directory. Estos dos recursos se **aseguran de que una cuenta nunca envíe sus credenciales para ser almacenadas** en un servidor por medio del Single Sing-On. No obstante, se debe tener en cuenta que estas características no protegen de que un administrador utilice sus credenciales explícitamente en el servidor accedido lo cual, evidentemente, las expondría dentro de ese sistema.

En resumen, el modelo de capas debe asegurar que los administradores trabajan dentro de sus límites marcados, y que llevan a cabo la administración de una forma segura. De esta manera, se combate la exposición de credenciales y la división pobre de los privilegios vistas en el punto 3 de este documento, además de mejorar la separación interna y el control de los recursos.

División en Subredes

Una vez se han organizado correctamente los recursos de una empresa a nivel de directorio, es recomendable también realizar la **división lógica** de los mismos **a través de subredes aisladas**.

La segmentación de red consiste en dividir una red plana en pequeñas subredes, **controlando cómo fluye el tráfico** entre las mismas. Este control se basa en definir reglas mediante diferentes variables para permitir, bloquear o limitar el tráfico entre las subredes de una empresa. La división de subredes suele realizarse por medio de tecnologías como firewalls, listas de controles de acceso (ACL) y/o redes virtuales (VLAN). De esta forma se crea una separación lógica entre recursos que no deberían relacionarse, o deberían hacerlo de una manera acotada.

Supongamos que en una red empresarial existe un servidor de base de datos que los usuarios utilizan para guardar registros indirectamente por medio de una página web. La segmentación en este caso permitiría **aislar la base de datos de la red donde trabajan los usuarios regulares**, evitando su exposición innecesaria. Al utilizarse a través de la página web, **no es necesario** que el servidor de base de datos esté expuesto directamente a los usuarios regulares, por lo que se disminuye drásticamente su superficie de ataque y facilita la labor de gestión y monitorización (pues solo debería llegar tráfico originado de la página web o de sistemas de administración).

En resumen, la división en subredes permite, como las medidas anteriores, aislar los recursos privilegiados, facilitar su administración y, sobre todo, mejorar la monitorización de anomalías para los mismos.

4.4. Conclusiones

Como conclusión y resumen de las medidas vistas en este capítulo:

- La separación de cuentas es llevada a cabo con el fin de **separar tareas**. Esta separación de tareas está motivada por evitar los problemas de seguridad que llevan asociadas cuestiones como navegar por internet o acceder al correo electrónico. **Las cuentas privilegiadas solo deben llevar a cabo las tareas privilegiadas por las que fueron creadas**, y en ningún caso otras que puedan llevar implícitos riesgos innecesarios.
- **El uso de sistemas protegidos complementa la separación de cuentas** dando cobijo a las cuentas privilegiadas. Estos sistemas buscan estar **más protegidos y restringidos que un sistema regular**, lo que permite minimizar la exposición de quienes los utiliza.
- Finalmente, **la segmentación permite aislar y controlar dónde se establecen los recursos y quién tiene acceso a los mismos**. Los sistemas regulares deben estar todos en un mismo ámbito, mientras que los sistemas sensibles y servidores deben establecerse en capas de mayor seguridad.

Como ya se indicó al inicio de este capítulo 4, la seguridad de una red interna organizacional depende en gran medida de la integridad de las cuentas privilegiadas que se utilizan para administrar, gestionar y desarrollar dentro de la misma.

Con las anteriores medidas se consigue aislar y proteger eficazmente no solo las cuentas privilegiadas de un dominio empresarial, sino también los sistemas y servidores donde trabajan. Como ya se ha recalcado más de una vez, **este aislamiento de recursos no solo los protege de riesgos, sino que también facilita su monitorización y detección frente a anomalías, lo que ayuda a establecer una posición de "assume breach"**. Por ello es tan importante llevar a cabo un diseño ordenado y enfocado en la seguridad.

5. IMPLEMENTACIÓN PRÁCTICA DEL DISEÑO RED FOREST

En el capítulo anterior se planteaba la necesidad de un diseño de infraestructura seguro y estructurado, y se explicaban algunas de las características que debía cumplir para proteger los recursos privilegiados de una empresa. En este capítulo se pretende implementar de forma práctica, y con la tecnología Active Directory, un ejemplo de diseño seguro concreto: el diseño Red Forest o Enhanced Security Administrative Environment (ESAE) de Microsoft.

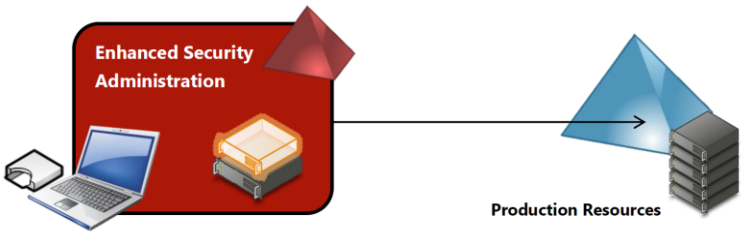


Ilustración 22 - Red Forest. Fuente: https://social.technet.microsoft.com/wiki/contents/articles/37509.active-directory-red-forest-design-aka-enhanced-security-administrative-environment-esae.aspx

El objetivo del diseño Red Forest es el de utilizar diferentes tecnologías y buenas prácticas – como las que se han visto en este documento – con el fin último de limitar la exposición de credenciales privilegiadas en entornos Active Directory. Algunas de las características que busca implementar este diseño son:

- Proveer de un entorno de seguridad para la administración separado completamente del entorno de producción.
- Implementar herramientas de seguridad para mitigar y disminuir la superficie de ataque sobre los recursos de la red.
- Separación entre cuentas regulares y administrativas.
- Separación en capas administrativas.
- Restringir el acceso privilegiado a sistemas de confianza aislados y securizados (PAWs).
- Restringir el acceso a Internet y otras tareas del día a día peligrosas para cuentas privilegiadas.
- Monitorización de los recursos sensibles para detectar anomalías
- Facilidad de uso para los administradores.

En los siguientes apartados se verá cómo se ha implementado de forma práctica este diseño en una serie de máquinas virtuales. Los apartados se centrarán en mostrar lo visto a lo largo de este trabajo. Debido a que algunas características son especiales o específicas de Red Forest o Active Directory, estas se trasladarán a anexos.

5.1. Estructura del Laboratorio

El laboratorio simulará a la empresa Capsule Corporation cuya red empresarial constará de dos bosques Active Directory: **capsule.corp** y **soprano.sl**. Como se puede ver en la siguiente imagen, existirá una relación de confianza unidireccional donde capsule.corp confiará en soprano.sl, pero no al revés. Esta forma de confianza es necesaria para aislar el bosque administrativo Red Forest – en este caso, soprano.sl – y que ningún objeto de capsule.corp tenga acceso a él, pero sí viceversa.

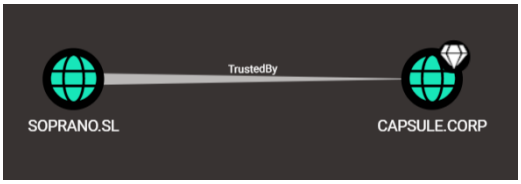


Ilustración 23 - Relación de confianza

Capsule.corp simulará el bosque de producción de la empresa, el cual dispondrá de un total de cuatro máquinas virtuales en la red 10.11.0.0/16:

- Controladores de dominio: dc01.capsule.corp [10.11.3.5]
- Estaciones de trabajo: ws01.capsule.corp [10.11.1.10]
- PAW: paw01.capsule.corp [10.11.2.10]
- Servidores: sql01.capsule.corp [10.11.3.10]

Soprano.sl simulará el bosque administrativo o Red Forest de Capsule Corporation, desde el cual se administrarán muchos de los recursos del bosque de producción. Dispondrá de una máquina virtual en la red 10.12.1.0/24:

- Controladores de dominio: red-dc01.soprano.sl [10.12.1.5]

Por último, se utilizarán dos máquinas virtuales como router/firewall con la tecnología **pfSense**:

- Fw01.capsule.corp: actuará de puerta de enlace hacia Internet, y firewall para las redes del dominio capsule.corp
- Fw02.soprano.sl: actuará de firewall entre el dominio capsule.corp y soprano.sl

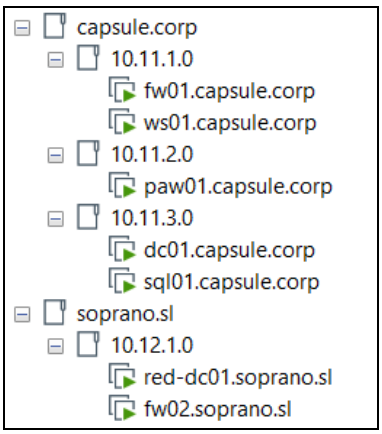


Ilustración 24 - Laboratorio Red Forest

Se muestra un diagrama de la red resultante:

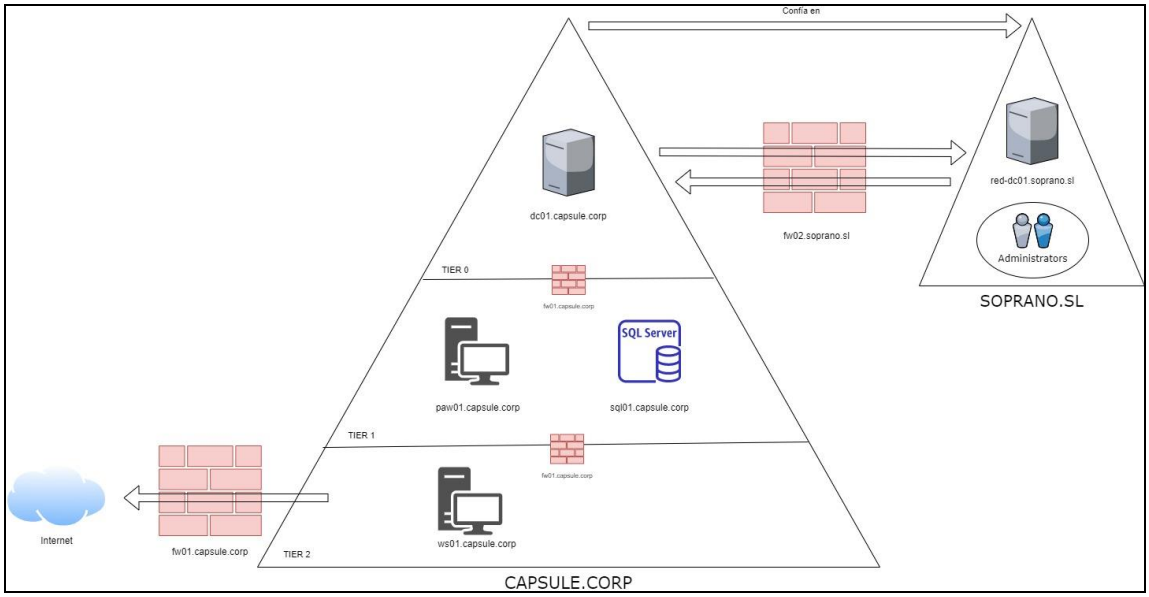


Ilustración 25 - Diagrama de red de la empresa Capsule Corporation

NOTA: La idea del diseño Red Forest es evitar el uso de grupos administrativos como Domain Admins dentro del dominio de Producción (capsule.corp) y realizar toda la administración desde un bosque externo (soprano.sl) a través de los denominados Shadow Principals. Ya que esta funcionalidad es específica de Active Directory, en este apartado se ha buscado realizar una explicación general válida para otros tipos de tecnología. Por este motivo, se ha trasladado el apartado "Administración desde un Bosque Externo Administrativo" al anexo 10.5.

5.2. Segmentación de la Estructura Organizacional y Red Interna

Este laboratorio se ha creado desde su inicio pensando en la organización de los recursos y su seguridad. Para ello, en este apartado se ha buscado seguir las recomendaciones explicadas en el punto 4.3 de este documento: utilizar un modelo de capas administrativas y dividir el laboratorio en subredes.

División a nivel de red

En primer lugar, como se ha indicado en la estructura del laboratorio, la red empresarial se divide en dos principales:

- **10.11.0.0/16** (red del bosque capsule.corp) con las siguientes subredes:
  - 10.11.1.0/24 (subred de clientes): en esta red se encuentran las estaciones de trabajo de los empleados regulares.
  - 10.11.2.0/24 (subred de administración): en esta red se encuentran las PAWs para administrar las estaciones de trabajo y servidores.

- 10.11.3.0/24 (subred de servidores): en esta red se encuentran los servidores.

- **10.12.1.0/24** (red del bosque soprano.sl): en esta red se encuentran las PAWs para administrar todo el ámbito empresarial de capsule.corp desde un bosque externo.

Las redes están controladas por firewalls que permiten filtrar el tráfico de las mismas. Más información sobre las reglas establecidas en el laboratorio en el anexo 10.4.

El esquema final de visibilidad entre sistemas sería algo parecido a lo siguiente:

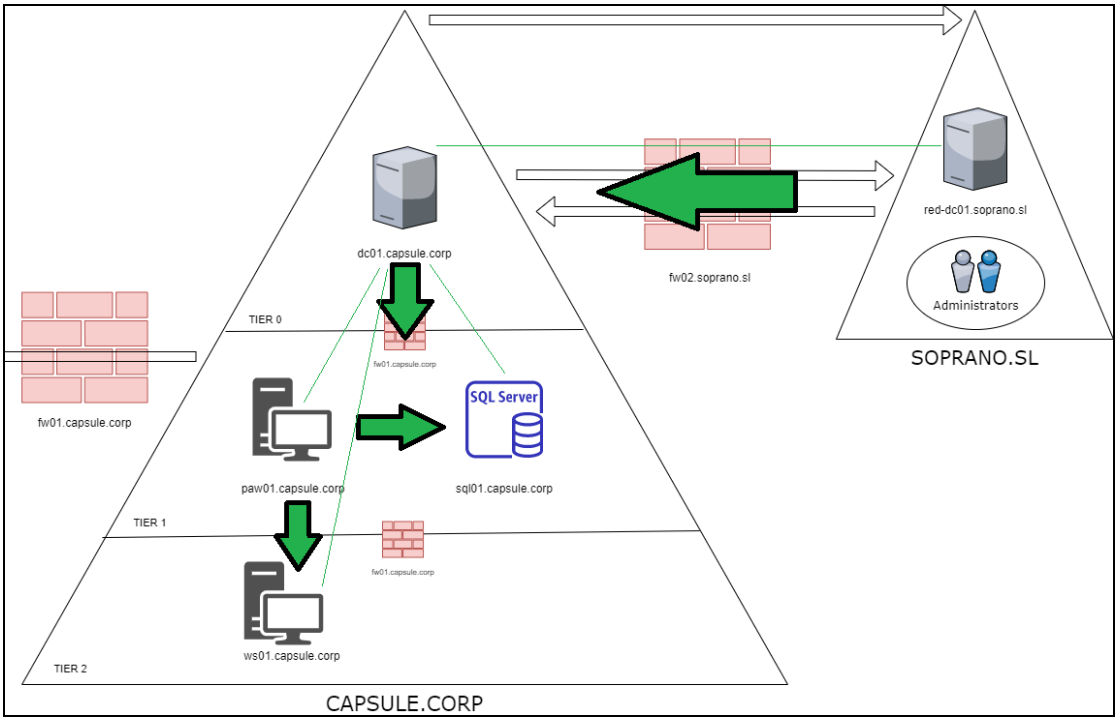


Ilustración 26 - Esquema de visibilidad

Las líneas verdes pretenden hacer referencia a la visibilidad que requiere Active Directory para que ciertos protocolos y capacidades funcionen correctamente (por ejemplo, todos los sistemas de un dominio deben poder interactuar con ciertos servicios de un Domain Controller como Kerberos o LDAP por motivos de autenticación, identidad y acceso). Por otro lado, las flechas verdes hacen referencia a la visibilidad administrativa que disponen ciertos sistemas para realizar labores privilegiadas:

- Dc01.capsule.corp: dispone de visibilidad total a los servicios de todos los sistemas del bosque capsule.corp.

- Paw01.capsule.corp**:** dispone de visibilidad total dentro de la subred de servidores (donde se encuentra sql01.capsule.corp), así como dentro de la red de clientes (donde se encuentra ws01.capsule.corp).

- Red-dc01.soprano.sl dispone de visibilidad total al bosque capsule.corp

División a nivel de directorio

Para poder administrar correctamente todo lo anterior a nivel de directorio, es necesario llevar un orden a la hora de organizar los recursos. En este laboratorio se ha hecho uso de los scripts provistos por Microsoft "Privileged Access Workstation (PAW) Content" para generar las unidades organizacionales y grupos oportunos para un modelo de administración por capas:

- https://gallery.technet.microsoft.com/Privileged-Access-3d072563

El resultado de utilizar dichos scripts en el dominio capsule.corp desemboca en la siguiente estructura:

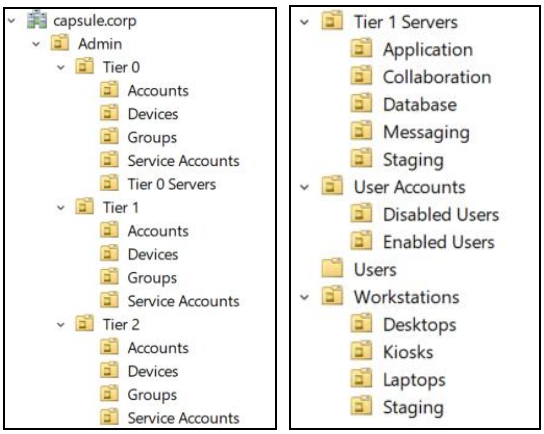


Ilustración 27 - Estructura organizacional de capsule.corp

Gracias a esta estructura es posible reunir y administrar a todos los objetos privilegiados en un mismo lugar - unidad organizacional Admin - ya sean cuentas de usuarios, dispositivos, grupos, cuentas de servicio… etcétera. Además, los scripts también generan una estructura para ordenar y administrar servidores y estaciones de trabajo – Tier 1 Servers y Workstations.

Los sistemas del laboratorio se han establecido en las siguientes localizaciones:

- Dc01.capsule.corp:
  - CN=DC01, OU=Domain Controllers, DC=capsule, DC=corp
- Ws01.capsule.corp:
  - CN=WS01, OU=Desktops, OU=Workstations, DC=capsule, DC=corp
- Paw01.capsule.corp:
  - CN=PAW01, OU=Devices, OU=Tier 1, OU=Admin, DC=capsule, DC=corp
- Sql01.capsule.corp:
  - CN=SQL01, OU=Database, OU=Tier 1 Servers, DC=capsule, DC=corp

En el caso de este laboratorio, el sistema paw01 se utiliza para administrar tanto la red de servidores (Tier1) como la red de clientes/estaciones de trabajo (Tier2). Como puede verse en los puntos anteriores, este sistema se ha establecido en la capa Tier1 ya que es la de mayor privilegio (aunque paw01.capsule.corp cubra las dos en este caso).

Gracias a esta estructura de directorio es posible establecer permisos y aplicar políticas de una forma cómoda y fluida. Veamos un ejemplo con las políticas de grupo "ServerAdmins" y "WorkstationAdmins".

- ServerAdmins**:** consiste en una política que establece al grupo **CAP\tier1admins** permisos de administración en cualquier servidor Tier 1 (sql01.capsule.corp). Cualquier usuario que sea miembro de dicho grupo podrá administrar un servidor de la capa 1. Es importante tener en cuenta que para dominios de gran tamaño, con diferentes tipos de servicios, sería conveniente separar tareas de administración y no cubrir todo con un mismo grupo. Podría haber un grupo para administrar aplicaciones, otro para bases de datos… etcétera.

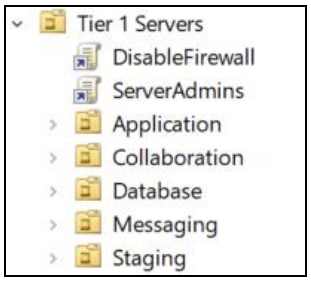


Ilustración 28 - GPO ServerAdmins

- WorkstationAdmins**:** consiste en una política que establece al grupo **CAP\tier2admins** permisos de administración en cualquier estación de trabajo de la red de clientes (ws01.capsule.corp). Nuevamente, cualquier usuario que sea miembro de este grupo podrá administrar todas las estaciones de trabajo de capsule.corp. Para dominios de gran tamaño se recomienda lo indicado en la política anterior.

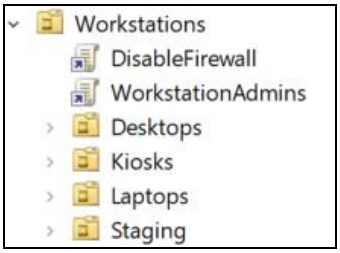


Ilustración 29- GPO WorkstationAdmins

En conclusión, con todas las configuraciones anteriores se consigue segmentar y estructurar capsule.corp de una forma apropiada, tanto a nivel de directorio como a nivel de red.

- Por un lado, a través de las **subredes y firewalls** se ha conseguido aislar los sistemas en base a su función.
    - Ws01.capsule.corp: solo dispone visibilidad dentro de su red (podría a priori ver a otras estaciones de trabajo que estuvieran en dicha red).
    - Sql01.capsule.corp: solo dispone de visibilidad dentro de su red (podría a priori ver otros servidores que estuvieran en dicha red).
    - Paw01.capsule.corp: dispone de visibilidad tanto a la red donde se encuentra ws01.capsule.corp como a la red de sql01.capsule.corp para poder administrarlas.

- Dc01.capsule.corp: dispone de visibilidad completa a todas las redes de su bosque para poder administrarlas.
- Red-dc01.soprano.sl: dispone de visibilidad completa a su red y a la red capsule.corp para poder administrarla.

- Por otro lado, a través de las unidades organizacionales y grupos se ha conseguido establecer los permisos de administración necesarios.
  - CAP\tier1admins: dispone de privilegios en todos los servidores Tier1 a través de la política ServerAdmins aplicada a la unidad organizacional "Tier 1 Servers" donde se encuentra sql01.capsule.corp.
  - CAP\tier2admins: dispone de privilegios en todas las estaciones de trabajo Tier2 a través de la política WorkstationAdmins aplicada a la unidad organizacional "Workstations" donde se encuentra ws01.capsule.corp.

5.2. Separación de Cuentas Privilegiadas

En el capítulo 4.1 se hablaba de la separación de cuentas privilegiadas para aislarlas de los riesgos asociados a las tareas regulares como navegar por Internet. Para llevar a cabo las pruebas se han creado los siguientes usuarios, respetando la separación de cuentas privilegiadas:

- **Tier 0**
  - Bulma_da (Domain Admin): cuenta administrativa de Bulma con permisos de Domain Admin. Esta cuenta se debe utilizar única y exclusivamente para realizar tareas de administración que tengan que ver con el dominio Active Directory (creación de políticas, gestión de permisos a nivel de directorio, estructuración de la organización…).
- **Tier 1**
  - Vegeta_sa (Server Admin): cuenta administrativa de Vegeta con permisos de administración en servidores gracias a ser miembro del grupo **CAP\tier1admins**. Esta cuenta se debe utilizar única y exclusivamente para administrar los servidores de capsule.corp como sql01.capsule.corp. Gestionar sus permisos, bases de datos, registros… etcétera.
- **Tier 2**
  - Mutenroshi_wa (Workstation Admin): cuenta administrativa de Mutenroshi con permisos de administración en estaciones de trabajo gracias a ser miembro del grupo **CAP\tier2admins**. Esta cuenta se debe utilizar para realizar tareas de mantenimiento en los equipos de los trabajadores como ws01.capsule.corp, forzar políticas de seguridad, proveer de software… etcétera.

Por otro lado, en el laboratorio se han creado numerosas cuentas de usuarios regulares sin privilegios, entre las que destacan las cuentas regulares de Bulma, Vegeta y Mutenroshi que

podrán utilizar para tareas como navegar por internet o revisar el correo (siempre y cuando se encuentren en un sistema habilitado para ello).

5.3. Uso de Sistemas Protegidos

Tal y como se especifica al final del apartado anterior, Bulma, Vegeta y Mutenroshi solo pueden utilizar sus cuentas regulares sin privilegios en sistemas habilitados para ello. En el caso de este laboratorio, esa sería la función de sistemas como ws01.capsule.corp. En cambio, sus cuentas privilegiadas – Bulma_da, Vegeta_sa, Mutenroshi_wa – deben ser utilizadas desde PAWs protegidas y aisladas como paw01.capsule.corp.

Por falta de recursos se ha creado exclusivamente una PAW en capsule.corp. Se debe tener en cuenta que lo recomendable habría sido crear, al menos, una PAW para cada capa administrativa:

- Tier0**:** debería disponer de PAWs para administrar servidores críticos y ser utilizadas por usuarios como Bulma_da.
- Tier1: debería disponer de PAWs para administrar servidores como sql01.capsule.corp y ser utilizadas por usuarios como Vegeta_sa.
- Tier2: debería disponer de PAWs para administrar las estaciones de trabajo como ws01.capsule.corp y ser utilizadas por usuarios como Mutenroshi_wa.

No obstante, con el fin de simplificar el laboratorio, se va a suponer que paw01.capsule.corp cubre las capas 1 y 2, y es utilizada tanto por Vegeta_sa y Mutenroshi_wa. Para la capa 0 se supondrá que existe una segunda PAW utilizada por Bulma_da.

Como ya se explicó en el capítulo 4.3.1, por defecto, **una autenticación de red no debería almacenar credenciales** de ningún tipo en el sistema accedido. Gracias a este hecho, los usuarios privilegiados podrán acceder desde sus PAWs a los sistemas que desean administrar sin exponer sus credenciales en el proceso.

Por ejemplo, en la siguiente imagen se puede ver cómo Mutenroshi_wa accede desde el sistema paw01.capsule.corp al sistema ws01.capsule.corp por medio de las herramientas de PS Remoting (protocolo WSMAN).

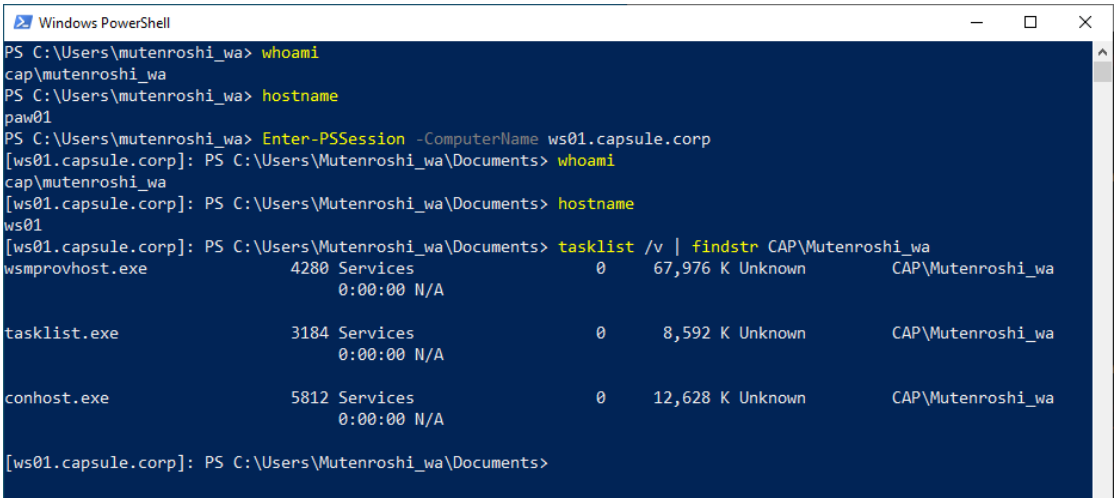


Ilustración 30 - Administración de ws01.capsule.corp

Si un atacante se encontrase en dicho momento dentro de ws01.capsule.corp e intentara extraer las credenciales de Mutenroshi_wa, se encontraría con que **no existe ninguna en dicho sistema**. A pesar de haber procesos de Mutenroshi_wa, ni su hash NTLM ni su ticket TGT estarán en dicho sistema tras la autenticación de red realizada con PS Remoting (Enter-PSSession).

No obstante, se debe tener cuidado. Si Mutenroshi_wa hubiera accedido a ws01.capsule.corp a través de escritorio remoto, por defecto, sus credenciales **sí que habrían quedado expuestas**.

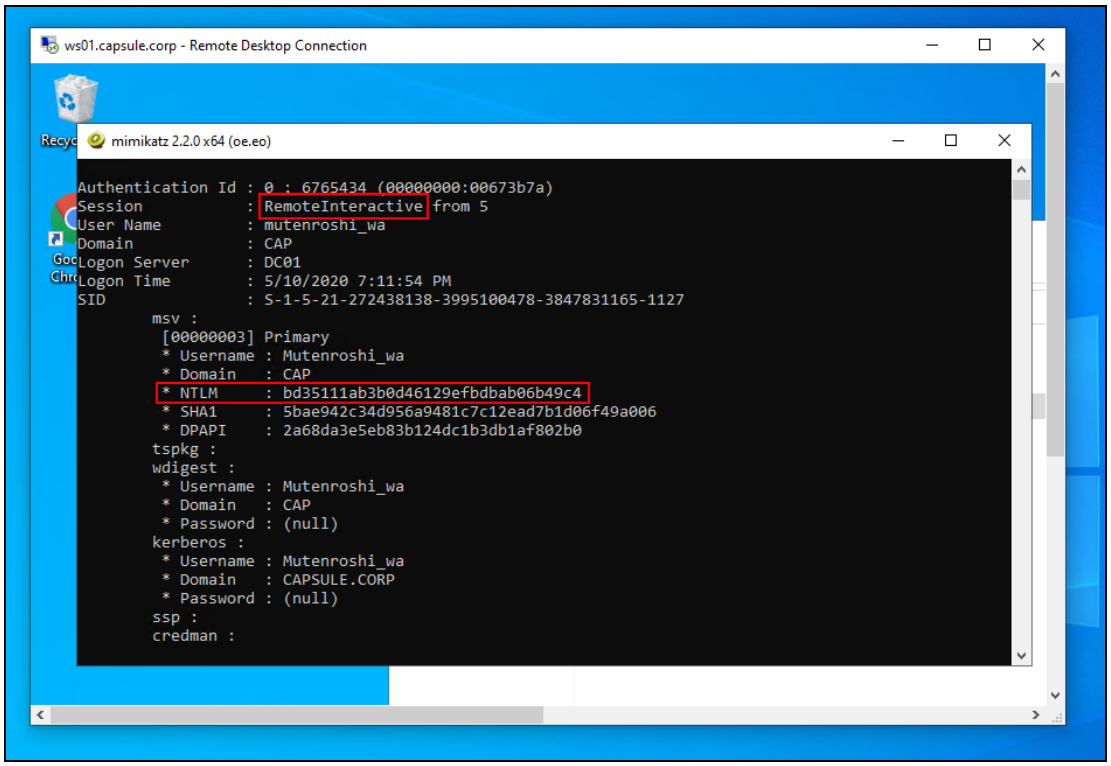


Ilustración 31 - Credenciales expuestas a través de RDP

Como también se explicó en el capítulo 4.3.1, existen características en Active Directory para evitar este comportamiento en RDP – y otros casos excepcionales como la delegación de

Kerberos – con el fin de que las credenciales de un usuario privilegiado nunca queden expuestas en el sistema accedido.

Así pues, para evitar posibles problemas como el de RDP anterior, se configuran las cuentas Bulma_da, Vegeta_sa y Mutenroshi_wa como miembros del grupo Protected Users.

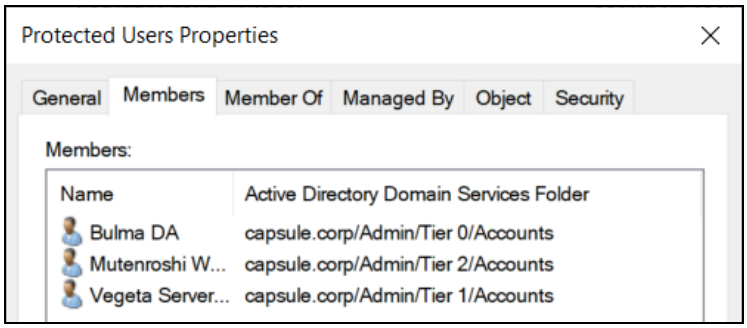


Ilustración 32 - Protected users

En conclusión, gracias al uso de PAWs y la separación de cuentas privilegiadas, se ha creado un ambiente seguro para la administración dentro de capsule.corp. Bulma, Vegeta y Mutentoshi tienen la posibilidad de utilizar sus cuentas regulares para llevar a cabo tareas del día a día en sus estaciones de trabajo regulares (como ws01.capsule.corp); mientras que también pueden realizar tareas administrativas de forma segura por medio de sus cuentas privilegiadas desde una PAW.

5.4. Pentesting Red Forest

Un atacante que lograra acceso a la red interna de la empresa Capsule Corporation se vería limitado en sus acciones por las medidas aplicadas en los apartados vistos en este capítulo. Aunque de forma simplificada, el laboratorio permite ver los beneficios de un diseño de infraestructura seguro.

Lo más probable es que, en caso de compromiso, un atacante lograra acceso a la estación de trabajo **WS01**, ya que dispone de acceso a Internet. Supongamos que Vegeta (usuario que dispone de una cuenta administrativa y una regular) ha sido víctima de un ataque de phishing y el atacante consigue acceso a dicho sistema.

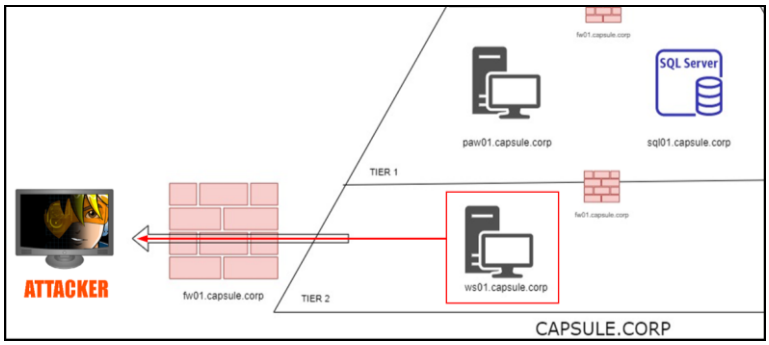


Ilustración 33 - Compromiso de WS01

Llegados a este punto, el atacante no debería tener acceso más que al sistema WS01, y ni si quiera como administrador local, ya que gracias a la **separación de cuentas privilegiadas**, la cuenta comprometida de Vegeta debería ser su cuenta regular sin privilegios. Si el atacante

quisiera revisar la totalidad del sistema sin restricciones, debería primero elevar privilegios localmente.

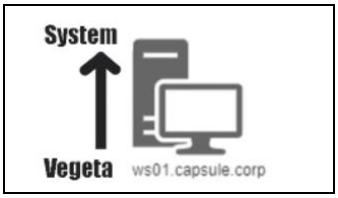


Ilustración 34 - Escalado de privilegios

Si se diera el caso de que el atacante lograra elevar privilegios dentro de dicho sistema, a priori no existirá ninguna credencial o recurso presente que le permita moverse a otro sistema dentro de la red, puesto que, nuevamente, Vegeta solo debería utilizar su cuenta administrativa desde una **PAW**, de tal forma que no se expongan sus credenciales en los sistemas administrados. No obstante, se podría dar el caso de que Vegeta expusiera sin querer sus credenciales.

Si Vegeta se descuidara y utilizara su cuenta administrativa de una forma insegura en WS01, el atacante podría extraer sus credenciales y tener un acceso potencial a aquellos recursos accesibles gracias a los privilegios de dicha cuenta. No obstante, se debe tener en cuenta que desde la red de estaciones de trabajo donde se encuentra WS01 **no existe visibilidad** a aquellos sistemas donde Vegeta es administrador, gracias a la **segmentación en subredes y uso de firewalls**.

Recordemos el diagrama de accesos visto en el apartado 5.2:

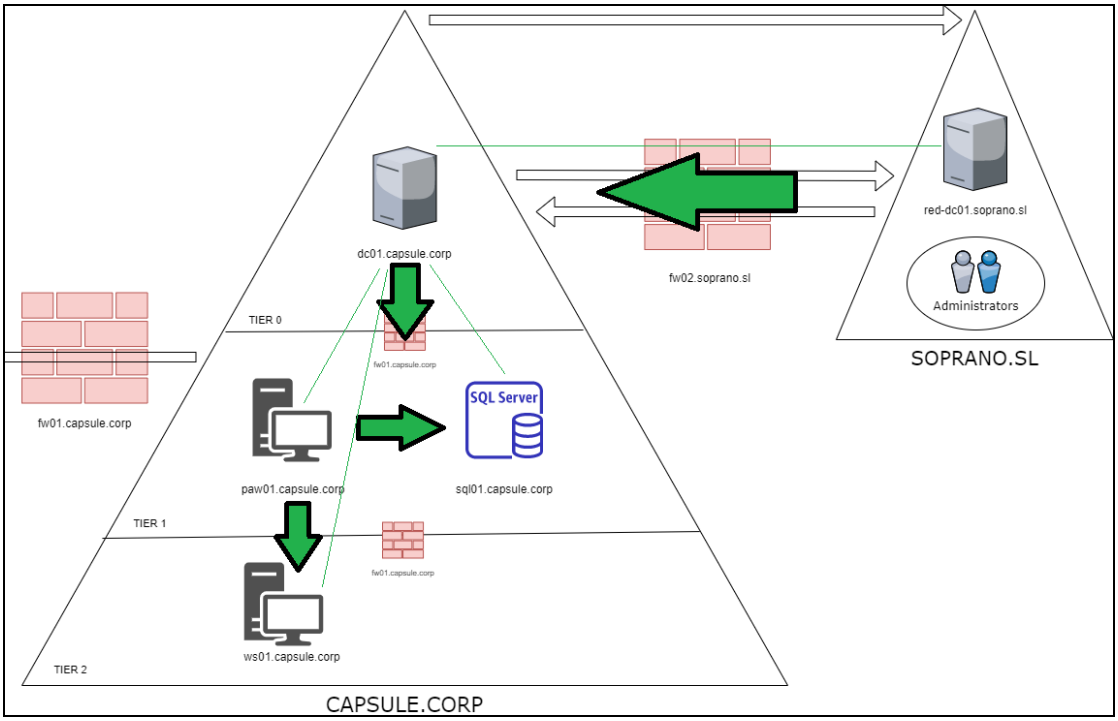


Ilustración 35 - Diagrama de accesos

Desde WS01, el atacante solo tendrá visibilidad a servicios dentro de su subred - que en el caso de este laboratorio no hay - por lo que no podrá acceder ni analizar sistemas como PAW01 (subred de administración) o SQL01 (subred de servidores) en busca de información a pesar de disponer de las credenciales administrativas de Vegeta.

En resumen, la empresa Capsule Corporation dispone de diferentes capas de seguridad fruto de la buena organización de sus recursos. Si a este laboratorio además se le añadieran servicios de monitorización como un SIEM, con la posibilidad de configurar alertas, se comprobarían las virtudes de disponer de diferentes subredes con recursos bien ordenados para poder diferenciar comportamientos normales de los anómalos.

6. CONCLUSIONES FINALES

Una de las grandes razones por las que una organización puede ser comprometida es por no disponer de una **infraestructura madura en términos de seguridad**. Una infraestructura ordenada, actualizada y fácil de administrar y monitorizar.

Cuando un atacante accede a la red interna de una organización, a menudo no necesita de grandes herramientas o exploits sino que se sirve de las herramientas y fallos de configuración presentes para moverse y alcanzar sus metas. Dentro de este punto destaca la **exposición de credenciales** presente en muchas de las empresas actuales, que habilitan a un atacante a suplantar y conseguir privilegios dentro de la red sin depender, como ya se ha indicado, de cuestiones laboriosas como encontrar nuevas vulnerabilidades y/o explotarlas.

Es decir, aprovechar funcionamientos legítimos de una tecnología es **fácil, barato y silencioso**.

En este documento se ha expuesto el problema de la falta de protección que existe con respecto al acceso privilegiado con cuestiones como la **exposición de credenciales**, **la división pobre de los privilegios** o la **falta de segmentación o control de la red interna**. Todas ellas demuestran por qué un atacante puede, con relativa facilidad, acceder y comprometer gran parte de los recursos de una organización sin que esta pueda responder o actuar en un tiempo razonable.

Todos los problemas vistos en este documento se resumen en la misma idea: **aislar para proteger**.

Cuando se han presentado las infraestructuras enfocadas en la seguridad, la idea de aislar recursos se ha puesto en acción. Se ha visto la **separación de cuentas privilegiadas** para evitar los riesgos que llevan asociadas acciones como navegar por Internet, el uso de **sistemas protegidos o PAWs** como entornos seguros para el uso de cuentas privilegiadas, así como la **segmentación de los recursos,** tanto a nivel de directorio con las unidades organizacionales y grupos, como a nivel de red con el uso de subredes y firewalls.

El ejemplo práctico que se ha utilizado ha sido el diseño **Red Forest** de Microsoft, para entornos Active Directory. Con dicho laboratorio se ha podido comprobar, de primera mano, las ventajas de seguir un diseño de infraestructura ordenado y seguro. Gracias a las buenas prácticas llevadas a cabo, la superficie de ataque y posibilidades de compromiso de la empresa ficticia Capsule Corporation se redujeron enormemente frente a si se hubiera utilizado un diseño común sin tener en cuenta la seguridad.

¿Se han cumplido los objetivos principales de este trabajo?

Personalmente pienso que sí.

Se ha estudiado uno de los problemas más graves a los que se enfrentan las organizaciones y se han presentado diferentes acercamientos para disminuir su impacto. No obstante, cabe recordar que un diseño de infraestructura seguro no es la solución a todos los problemas de seguridad a los que puede enfrentarse una empresa.

Recogiendo el final de ejemplo presentado en el punto 5.4 (Pentesting Red Forest), el atacante no podía utilizar unas credenciales robadas (al usuario Vegeta) porque no disponía de

visibilidad a otras subredes desde el ordenador comprometido. En la realidad, las redes empresariales son mucho más vastas y complejas; además, al igual que un atacante puede romper las barreras perimetrales de una empresa a través de técnicas como el phishing, estas se podrían utilizar para acceder a aquellas subredes a priori innacesibles (tier1 y tier0).

Es decir, un diseño de infraestructura seguro no solo se centra en prevenir ataques, sino que su objetivo principal es el de servir de base para el correcto funcionamiento de los equipos de seguridad y administración. En este aspecto también es importante saber que no todas las empresas van a poder "empezar de cero" con su infraestructura interna. Muchas van a disponer de una infraestructura montada que tocará revisar y estructurar, poco a poco, para conseguir los resultados que se buscan en este documento (lo cual puede ser complejo y costoso).

De cualquier manera, el objetivo de disponer de una infraestructura segura y ordenada debería ser uno de los **más importantes** a llevar a cabo por una organización.

¿Cuáles serían las líneas de trabajo futuro?

En este documento solo se ha visto la superficie de lo que representa una red interna organizacional segura. Como se ha indicado anteriormente, las medidas vistas ayudan a organizar y aislar, pero no son la solución a todos los problemas de seguridad de una empresa.

Para conseguir una madurez en términos de seguridad, es importante destacar la labor de **los equipos de seguridad o Blue Team**.

Recordemos que un atacante con experiencia siempre buscará pasar lo más desapercibido posible, aprovechando funcionalidades y flujos legítimos dentro de una organización. Por este motivo, es muy importante entender que cuestiones como los Antivirus o los Firewalls nunca van a frenar completamente a este tipo de adversarios.

Para estas situaciones, es necesario disponer de equipos de seguridad que monitoricen la red frente a anomalías y comportamientos fuera de lo común; equipos que conozcan su red y puedan responder eficazmente a las diferentes etapas que podría llevar a cabo un adversario, como son las infecciones iniciales, los posteriores movimientos laterales dentro de la red o el establecimiento de persistencias en los equipos.

Para llevar a cabo esta monitorización y respuesta, un equipo de seguridad debe tener acceso a la información de una manera sencilla y rápida. En este punto es donde entran cuestiones como los **SIEM** (Security Information and Event Management) o el uso de tecnologías **EDR** (Endpoint Detection and Response).

Además de tener en cuenta todo lo relativo al Blue Team, existen muchas tecnologías y buenas prácticas que no se han visto en este documento, que podrían mejorar y ayudar a la protección de una organización. Una de las más importantes y conocidas es el uso autenticación de múltiples factores o ***Multi-factor Authentication*** **(MFA)**, para llevar a cabo las autenticaciones dentro de los servicios de una organización. Dentro de este tipo de "tecnologías de seguridad", y poniendo de ejemplo a Active Directory, se pueden encontrar diversidad de ellas: LAPS, JEA, JIT… etcétera.

Espero que este documento sirva para otros tanto como ha servido para mí: para entender el positivo impacto de una red interna estructurada, a la vez que demostrar la gran importancia que tienen los equipos de seguridad dentro de una empresa.

7. BIBLIOGRAFÍA

[1] Securing Privileged Access. Microsoft Docs. [Consulta: 10 de Marzo de 2020] <https://docs.microsoft.com/es-es/windows-server/identity/securing-privileged-access/securing-privileged-access>

[2] Active Directory Red Forest Design AKA Enhanced Security Administrative Environment (ESAE). Microsoft TechNet. [Consulta: 15 de Marzo de 2020] <https://social.technet.microsoft.com/wiki/contents/articles/37509.active-directory-red-forest-design-aka-enhanced-security-administrative-environment-esae.aspx>

[3] FreeIPA Documentation. FreeIPA. [Consulta: 3 de Marzo de 2020] <https://www.freeipa.org/page/Documentation>

[4] Samba Documentation. Samba. [Consulta: 3 de Marzo de 2020] <https://www.samba.org/samba/docs/>

[5] PfSense Documentation. Netgate. [Consulta: 10 de Abril de 2020] <https://docs.netgate.com/pfsense/en/latest/index.html>

[6] Active Directory Security. ADSecurity. [Consulta: 4 de Marzo de 2020] <https://adsecurity.org/>

[7] Future Forests: Realistic Strategies for AD Security & "Red Forest" Architecture. Knowles, Katie. [Consulta: 5 de Abril de 2020] <https://www.youtube.com/watch?v=i6BI-9myiHY>

[8] Tiered Administrative Model - ESAE - Active Directory Red Forest Architecture. Smith, Russell. [Consulta: 27 de Marzo de 2020] <https://www.youtube.com/watch?v=t4I2saNpoFE>

[9] Active Directory Security: The Journey. Metcalf, Sean. [Consulta: 15 de Marzo de 2020] **<**https://adsecurity.org/wp-content/uploads/2017/11/BlueHat-2017-Metcalf-ActiveDirectorySecurityTheJourney-Final.pdf>

[10] Mimikatz. GitHub. Delpy, Benjamin. [Consulta: 18 de Marzo de 2020] <https://github.com/gentilkiwi/mimikatz>

[11] LSA Logon Sessions. Microsoft Docs. [Consulta: 18 de Marzo de 2020] <https://docs.microsoft.com/en-us/windows/win32/secauthn/lsa-logon-sessions>

[12] PLANTING THE RED FOREST: IMPROVING AD ON THE ROAD TO ESAE. F-Secure. [Consulta: 5 de Abril de 2020] <https://www.f-secure.com/en/consulting/our-thinking/planting-the-red-forest-improving-ad-on-the-road-to-esae>

[13] Understanding "Red Forest" - The 3-Tier ESAE and Alternative Ways to Protect Privileged Credentials. Quest. [Consulta: 5 de Abril de 2020] <https://es.slideshare.net/QuestSoftware/understanding-red-forest-the-3tier-esae-and-alternative-ways-to-protect-privileged-credentials>

[14] Attack and Defend Microsoft Enhanced Security Administrative Environment. Wang, Hao. Rodanant, Yohin. [Consulta: 15 de Abril de 2020]
<https://download.ernw-insight.de/troopers/tr18/slides/TR18_AD_Attack-and-Defend-Microsoft-Enhanced-Security.pdf>

[15] Windows Server 2016: Set Up Privileged Access Management. Smith, Russel. [Consulta: 18 de Abril de 2020]
<https://www.petri.com/windows-server-2016-set-privileged-access-management>

[16] How NOT to use the PAM trust - Leveraging Shadow Principals for Cross Forest Attacks. Mittal, Nikhil. [Consulta: 18 de Abril de 2020]
<https://www.labofapenetrationtester.com/2019/04/abusing-PAM.html>

8. ANEXOS

8.1. Active Directory

Como su nombre indica, Active Directory (o más concretamente, Active Directory Domain Services) se trata de un servicio de directorio con una estructura jerárquica que almacena información sobre objetos. Para ello, utiliza una base de datos (NTDS) en la cual se almacena toda la información. A su vez, esta base de datos puede ser replicada con el objetivo de crear una red distribuida manteniendo la funcionalidad e integridad de los datos.

Cuando se habla de objetos, realmente se está hablando de la representación que realiza Active Directory de cuestiones como, por ejemplo, un usuario. Esto es, Active Directory dispone de una serie de clases con atributos definidos para representar todas aquellas cosas que requieran ser administradas en una red empresarial. Algunas de las clases de objeto más comunes son las siguientes:

- Usuarios
- Grupos
- Ordenadores
- Políticas de grupo (GPO)
- Dominios
- Bosques
- Contenedores (por ejemplo, unidades organizacionales)

Para cada una de estas clases vienen definidos una serie de atributos y características. Por ejemplo, los objetos de tipo usuario disponen de atributos que informan sobre cuestiones como cuándo fue la última vez que se conectó un usuario o si ha cambiado su contraseña recientemente. Así mismo, Active Directory dispone de características para este tipo de objetos con el fin de que, por ejemplo, se pueda elegir que un usuario no tenga que cambiar su contraseña cada cierto tiempo porque no expira.

El servicio de Active Directory Domain Services se puede instalar en cualquier Windows Server y conlleva una serie de implicaciones en el sistema donde se ha instalado. Si es la primera vez que se instala este servicio de directorio, será necesario crear un nuevo bosque, que vendrá representado con el nombre de dominio elegido por el administrador.

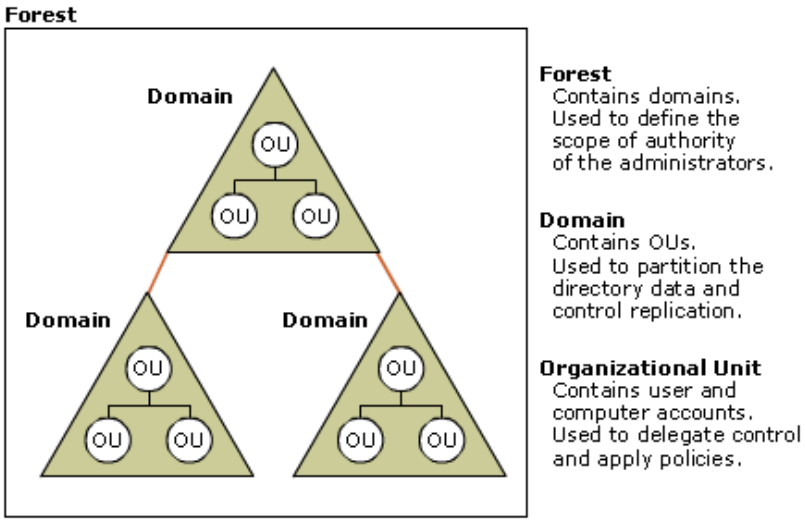


Ilustración 36 - Bosques, dominos y unidades organizacionales. Fuente: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756901(v=ws.10)?redirectedfrom=MSDN

Un bosque en el ámbito de Active Directory hace referencia a una agrupación de dominios. As su vez, un dominio en el ámbito de Active Directory hace referencia a una agrupación de objetos (usuarios, sistemas, políticas…). Normalmente, una organización dispondrá de uno o varios bosques con una serie de dominios en cada uno. Además, los bosques y dominios pueden establecer relaciones de confianza de diferentes maneras, lo que permite controlar interacciones entre los recursos de unos y otros, habilitando cuestiones como las posibles relaciones externas de una empresa con otras (por ejemplo, cuando una compra a otra).

Como ejemplo, la empresa Capsule Corp podría tener un bosque que representara a toda la empresa (caspule.corp) y, dentro del mismo, diferentes dominios para cada país en el que opera (es.capsule.corp, uk.capsule.corp, fr.capsule.corp…).

Tal y como se puede comprobar en la nomenclatura de los dominios y bosques, uno puede intuir el uso de nombres del sistema de nombres de dominio (DNS) por parte de Active Directory. De esta forma, los clientes pueden localizar sistemas y servicios y, sobre todo, pueden localizar a los sistemas clave que almacenan la información del directorio: los domain controllers (o controladores de dominio).

Cuando se instala Active Directory Domain Services en un sistema Windows Server, este pasa a convertirse en un domain controller para el dominio creado. En una organización común existirá más de un domain controller por cada dominio, y cada uno de ellos dispondrá de una copia de la base de datos NTDS, que replicaran entre sí para mantener la integridad de la información a lo largo de la empresa.

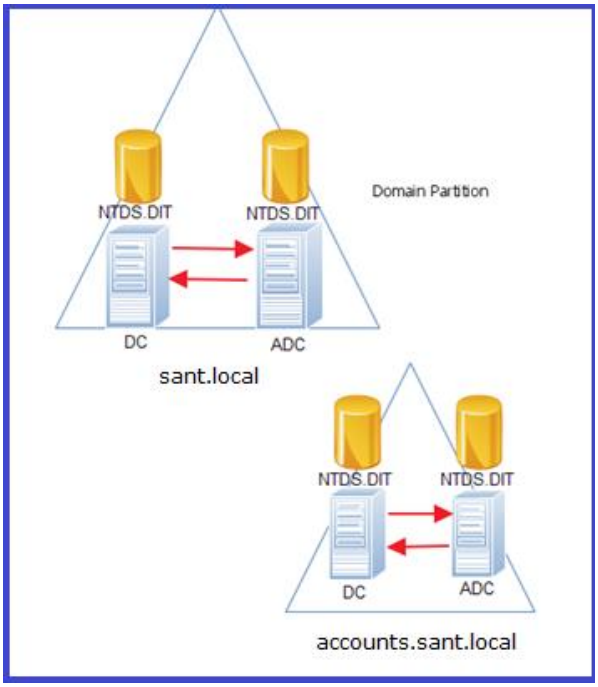


Ilustración 37 - Domain Controllers y replicación de NTDS. Fuente: https://santhoshksblog.wordpress.com/2016/07/26/active-directory-partition/

Los domain controllers no solo se encargan de almacenar la información de un dominio, sino que tambien se encargan de llevar a cabo la autenticación de los principals (usuarios, sistemas, cuentas de servicio…) dentro del mismo. Active Directory lleva a cabo dichas autenticaciones principalmente a través dos protocolos de autenticación: Kerberos y NTLM.

Ambos protocolos dependen de ciertos objetos de credenciales que, a su vez, son creados a partir de las contraseñas (o medios de autenticación) de cada uno de los usuarios y sistemas pertenecientes al dominio. Por ejemplo, en el caso de NTLM, a la contraseña de los usuarios se les aplica una función hash, y el resultado de dicha función es el que se utiliza para autenticar al usuario frente a recursos de la red. A su vez, Kerberos utiliza la contraseña de un usuario para facilitarle un objeto denominado Ticket Granting Ticket (TGT), con el cual un usuario puede solicitar acceso a los recursos de la red e identificarse dentro del dominio Active Directory.

Mediante estos protocolos, Active Directory consigue una experiencia Single Sign-On (SSO). Es decir, los usuarios no tienen que insertar repetidamente sus credenciales durante la jornada laboral, sino que Windows las almacena la primera vez que el usuario se autentica, y las utiliza posteriormente de forma transparente al usuario, ofreciendo fluidez a la hora de acceder recursos dentro de un dominio.

En resumen, un domain controller se encarga de almacenar toda la información de un dominio y de llevar a cabo la autenticación de todos los principals pertenecientes al mismo. Por este motivo, estos sistemas son considerados críticos en una organización, puesto que su compromiso equivale al compromiso de todo el dominio y todo el bosque al que pertenece.

Por último, en lo que respecta a controles de acceso, Active Directory implementa una mezcla entre Access Control Lists (ACL) y Role-Based Access Controls (RBAC). Por una parte, todos los objetos que requieren autorización en Windows (no solo Active Directory) son comúnmente llamados “securable objects”. Este nombre es debido a que todos ellos disponen de una

característica llamada descriptor de seguridad, dentro de la cual los objetos establecen una lista de reglas para controlar quién tiene acceso (o no) a sus propiedades.

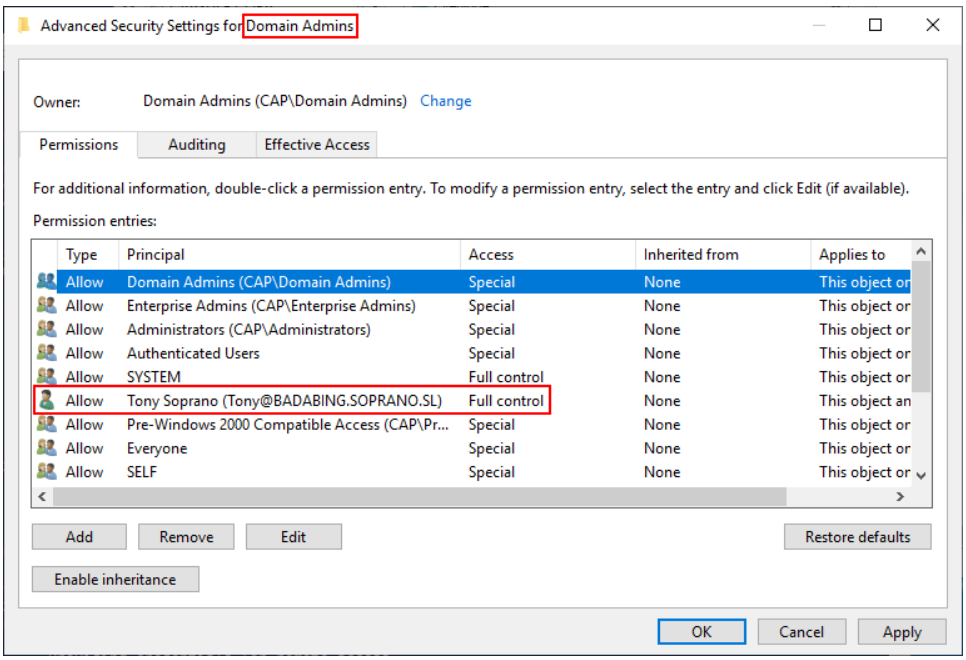


Ilustración 38 - Descriptor de seguridad del objeto Domain Admins

Por ejemplo, al revisar el descriptor de seguridad del grupo Domain Admins en la imagen anterior, se puede comprobar que el propietario de dicho objeto es el propio grupo Domain Admins. Así mismo en la pestaña "Permissions" se pueden comprobar las reglas de acceso al objeto. En el caso de la imagen anterior, se puede ver cómo el usuario Tony Soprano dispone de control total sobre Domain Admins, lo que le permitiría, en otras cosas, controlar (añadiendo o quitando) quién es miembro de dicho grupo.

Además de las listas de controles de acceso, Windows en general hace uso de grupos para implementar un funcionamiento similar al control de acceso basado en roles (RBAC). Por ejemplo, los miembros del grupo Administrators tienen la posibilidad de actuar en integridad alta dentro de un sistema y llevar a cabo acciones administrativas en él. Esto es debido a que el grupo Administrators facilita el acceso a una serie de privilegios como, por ejemplo, el SeDebugPrivilege. Mediante este privilegio, un usuario puede consultar y modificar la memoria de cualquier proceso en un sistema.

Por lo tanto, Windows y Active Directory implementan sus controles de acceso mezclando el uso de ACL, grupos/roles y privilegios específicos.

8.2. FreeIPA

FreeIPA es una solución que implementa capacidades de Identity Management enfocadas a entornos donde predominan los sistemas Linux. IPA hace referencia a Identity, Policy y Audit, ya que el objetivo de esta tecnología es similar al explicado en el punto anterior con Active Directory. Esta tecnología busca ofrecer una interfaz para gestionar principals de una manera segura y centralizada a través de diferentes métodos como acceso a través de clientes, una interfaz web o acceso mediante procedimientos remotos o remote procedure calls (RPC).

Esta tecnología implementa también el denominado Single Sign-On (SSO) para todos sus sistemas, servicios y aplicaciones, consiguiendo esa experiencia de autenticación única donde los usuarios tan solo tienen que insertar sus credenciales una vez para trabajar dentro de la red interna.

Respecto a las políticas, FreeIPA permite crearlas para configurar características respecto a las autenticaciones o los controles de acceso que afectan a las identidades dentro del entorno. Así mismo, se pueden controlar servicios como los de DNS, SUDO, Selinux o autofs.

Además, esta solución permite implementar relaciones de confianza con entornos como Active Directory, lo que facilita enormemente los escenarios de uso de la misma.

FreeIPA diferencia y simplifica sus componentes clave en los siguientes:

- Un servidor de autenticación KDC (Key Distribution Center) para autenticar a los principals pertenecientes al entorno.
- Una base de datos central con la información del entorno que funciona a través de LDAP.
- Un servicio PKI para firmar y crear certificados para los sistemas, recursos y aplicaciones del entorno.
- Un servicio de nombres del sistema de nombres de dominio (DNS) para localizar todos los recursos y sistemas del entorno.

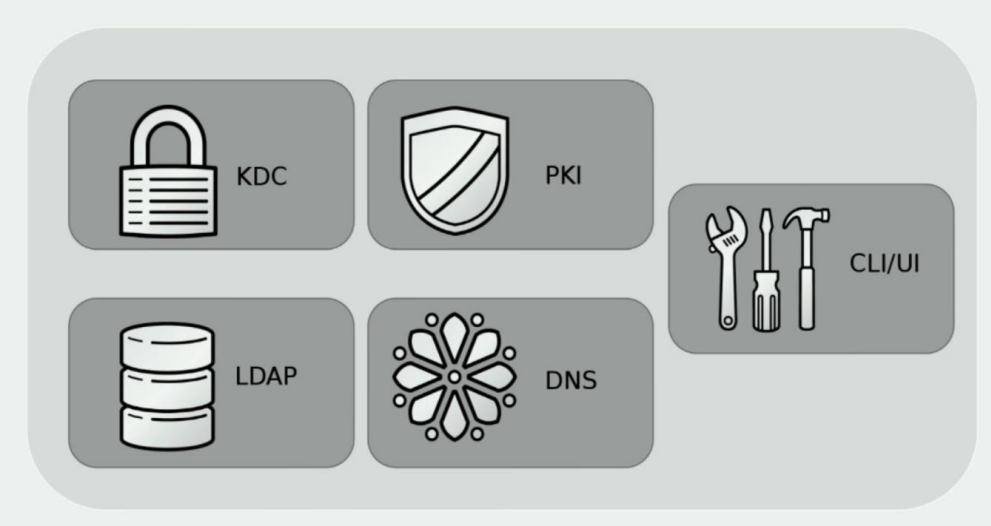


Ilustración 39 - Componentes de FreeIPA. Fuente: Christian Heimes - Identity management, single sign-on and certificates with FreeIPA

El servidor de directorio trabaja sobre un servidor LDAP que funciona como método de almacenamiento para toda la información del directorio o dominio. Este mismo sistema, además, actúa como servidor de autenticación, de autorización y otras políticas. Haciendo una similitud con Active Directory, estos sistemas serían los domain controllers de FreeIPA.

Como se ha indicado en el anterior párrafo, el servicio de autenticación dentro del directorio viene implementado por Kerberos. El servidor de autenticaciones dentro de esta tecnología se denomina Key Distribution Center, y entre sus componentes se encuentra el Authentication Server (AS). Este servicio se encarga de recibir peticiones de autenticación y responder con tickets de acceso a aquellas autenticaciones que resulten válidas. Como ya se mencionó en el apartado de Active Directory, estos tickets son llamados Ticket-Granting Ticket (TGT).

Una vez un usuario dispone de su TGT, el KDC dispone de otro componente denominado Ticket-Granting Server (TGS). Este servicio ofrece a los usuarios la posibilidad de presentar sus tickets TGT con el objetivo de obtener tickets de servicio para servicios específicos dentro del entorno FreeIPA.

Por ejemplo, un usuario que quisiera acceder a una página web interna de forma autenticada, podría solicitar un ticket de servicio para la misma utilizando su TGT en el servidor TGS. El servidor TGS le devolvería dicho ticket, que el usuario podría presentar en la página web como objeto de credenciales.

El servicio de Public Key Infrastructure (PKI) integrado en FreeIPA viene de la mano del proyecto Dogtag (http://pki.fedoraproject.org/). Este servicio permite el firmado y la publicación de certificados para los servicios y aplicaciones ofrecidos dentro de un directorio FreeIPA. Su gestión puede realizarse a través de una serie de servicios web integrados con la autenticación Kerberos para solicitar, mostrar o buscar certificados.

Por último, el servicio DNS que ofrece FreeIPA permite a los administradores crear y servir registros DNS en el dominio mediante las mismas herramientas (cliente o cliente web) con las que se puede gestionar el resto de componentes. Para que Kerberos funcione correctamente, es necesario que la implementación de DNS a lo largo de todo el dominio sea correcta, por ese motivo FreeIPA ofrece herramientas y automatización a la hora de gestionar este servicio.

8.3. Samba

A pesar de que Samba no sea una solución enfocada al Identity Management, se ha incluido por su importancia en el mundo actual de las redes internas empresariales.

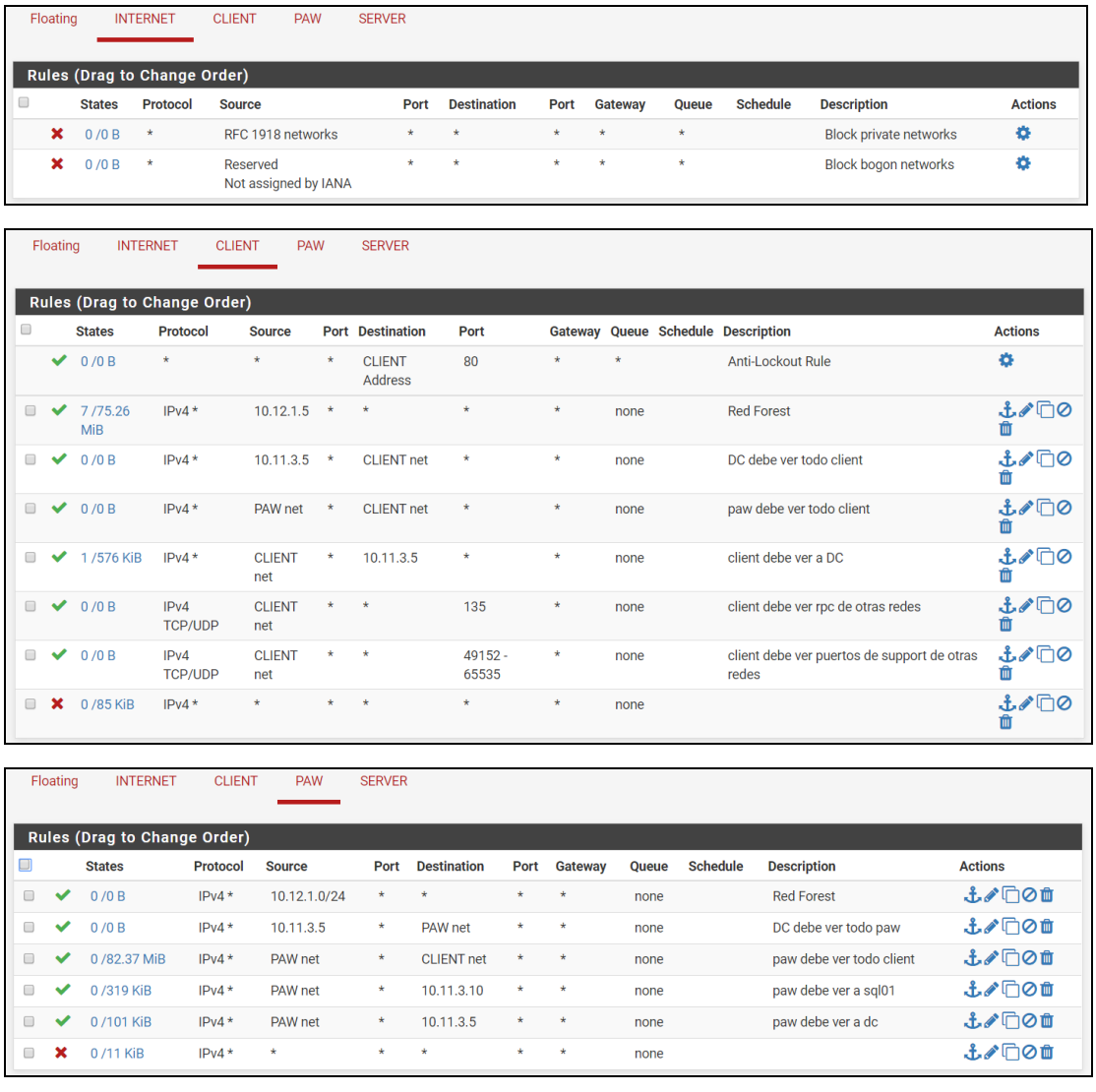
Tal y como se explica en su propia página web (https://www.samba.org/), con la llegada de Internet a los hogares, las personas daban por hecho que los sistemas Windows y Unix comenzarían a trabajar para integrarse en ciertos aspectos. Esto no fue así, y por esta razón nació Samba.

Samba se compone de una suite de herramientas que funcionan en plataformas Unix. Su objetivo es permitir la comunicación con clientes Windows de una forma similar a la nativa, implementando el protocolo CIFS. Este protocolo, creado por Microsoft, se basa en el famoso Server Message Block (SMB) con ciertas mejoras, y es ampliamente utilizado para compartir ficheros e impresoras dentro de redes Windows.

Hoy en día, gracias a Samba, es posible integrar sistemas y servidores Linux/Unix dentro de entornos Active Directory, tanto como miembros de un dominio, como funcionando incluso de domain controllers. Por ello Samba es, y lleva siendo años, un recurso clave para las empresas.

8.4. Reglas de Firewall

En este laboratorio se utiliza el firewall **fw01.capsule.corp** para controlar el tráfico dentro de la red de producción (10.11.0.0/16). En la siguiente imagen se pueden ver las reglas creadas para esta red junto a la descripción de cada una (nótese que se trata de reglas muy básicas creadas específicamente para este laboratorio como prueba de concepto, por lo que no se recomiendan para ningún caso).



Floating | INTERNET | CLIENT | PAW | SERVER

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

Floating | INTERNET | CLIENT | PAW | SERVER

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	*	*	*	CLIENT Address	80	*	*		Anti-Lockout Rule	
7 /75.26 MiB	IPv4 *	10.12.1.5	*	*	*	*	none		Red Forest	
0 /0 B	IPv4 *	10.11.3.5	*	CLIENT net	*	*	none		DC debe ver todo client	
0 /0 B	IPv4 *	PAW net	*	CLIENT net	*	*	none		paw debe ver todo client	
1 /576 KiB	IPv4 *	CLIENT net	*	10.11.3.5	*	*	none		client debe ver a DC	
0 /0 B	IPv4 TCP/UDP	CLIENT net	*	*	135	*	none		client debe ver rpc de otras redes	
0 /0 B	IPv4 TCP/UDP	CLIENT net	*	*	49152 - 65535	*	none		client debe ver puertos de support de otras redes	
0 /85 KiB	IPv4 *	*	*	*	*	*	none			

Floating | INTERNET | CLIENT | PAW | SERVER

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /0 B	IPv4 *	10.12.1.0/24	*	*	*	*	none		Red Forest	
0 /0 B	IPv4 *	10.11.3.5	*	PAW net	*	*	none		DC debe ver todo paw	
0 /82.37 MiB	IPv4 *	PAW net	*	CLIENT net	*	*	none		paw debe ver todo client	
0 /319 KiB	IPv4 *	PAW net	*	10.11.3.10	*	*	none		paw debe ver a sql01	
0 /101 KiB	IPv4 *	PAW net	*	10.11.3.5	*	*	none		paw debe ver a dc	
0 /11 KiB	IPv4 *	*	*	*	*	*	none			

Floating | INTERNET | CLIENT | PAW | SERVER

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	4 /2.71 MiB	IPv4 TCP	10.11.3.5	*	This Firewall	80 (HTTP)	*	none		DC debe ver dashboard del firewall	
✓	0 /0 B	IPv4 *	10.12.1.0/24	*	*	*	*	none		Red Forest	
✓	0 /0 B	IPv4 *	PAW net	*	SERVER net	*	*	none		paw debe ver todo server	
✓	0 /0 B	IPv4 *	*	*	10.11.3.5	*	*	none		Todos deben ver al DC	
✓	0 /996 KiB	IPv4 TCP/UDP	10.11.3.5	*	*	5985 - 5986	*	none		dc debe ver wsman de otras redes	
✓	0 /0 B	IPv4 TCP/UDP	SERVER net	*	*	49152 - 65535	*	none		server debe ver puertos de support de otras redes	
✓	0 /0 B	IPv4 TCP/UDP	SERVER net	*	*	135	*	none		server debe ver rpc de otras redes	
DC debe ver servicios del Red Forest											
✓	0 /124 KiB	IPv4 TCP/UDP	10.11.3.5	*	10.12.1.5	53 (DNS)	*	none			
✓	0 /9 KiB	IPv4 TCP/UDP	10.11.3.5	*	10.12.1.5	135	*	none			
✓	0 /0 B	IPv4 TCP/UDP	10.11.3.5	*	10.12.1.5	389 (LDAP)	*	none			
✓	0 /56 KiB	IPv4 TCP/UDP	10.11.3.5	*	10.12.1.5	49152 - 65535	*	none			
✗	0 /97 KiB	IPv4 *	*	*	*	*	*	none			

Por otro lado, **fw02.soprano.sl** se utiliza como barrera entre el bosque de producción y el bosque administrativo. A continuación, se muestran las reglas de dicho firewall.

Floating | PROD | RED

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 /0 B	IPv4 TCP	10.11.3.5	*	10.12.1.5	3389 (MS RDP)	*	none		Block RDP	
✗	0 /2 KiB	IPv4 TCP	10.11.3.5	*	10.12.1.5	139 (NetBIOS-SSN)	*	none		Block NB	
✗	0 /0 B	IPv4 TCP	10.11.3.5	*	10.12.1.5	445 (MS DS)	*	none		Block CIFS	
✗	0 /156 B	IPv4 TCP	10.11.3.5	*	10.12.1.5	5985 - 5986	*	none		Block WSMAN	
✓	0 /13 KiB	IPv4 *	10.11.3.5	*	*	*	*	none			
✗	0 /104 KiB	IPv4 *	*	*	*	*	*	none			

Floating | PROD | RED

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 /913 KiB	*	*	*	RED Address	80	*	*		Anti-Lockout Rule	
✓	0 /73.03 MiB	IPv4 *	*	*	*	*	*	none			

8.5. Administración desde un Bosque Externo Administrativo

Una de las características del diseño Red Forest es la utilización de un **bosque administrativo**, aislado del bosque de producción, para realizar todas las tareas administrativas de forma remota y segura. Esta forma de administración sigue el mismo planteamiento visto a lo largo de este documento, por ejemplo, con el uso de PAWs: **aislar y proteger la exposición de credenciales**.

El objetivo de tener un bosque externo administrativo es el de evitar la utilización de cuentas privilegiadas como las de **Domain Admins** o **Enterprise Admins** en el bosque de producción. Si nadie utiliza estas cuentas, *debería ser improbable* que un atacante lograse acceso a ellas.

El laboratorio práctico establece este escenario con los bosques **capsule.corp** (producción) y **soprano.sl** (Red Forest). Como se puede ver en la siguiente imagen, se ha establecido una relación de confianza **unidireccional** donde capsule.corp confía en soprano.sl pero no viceversa.

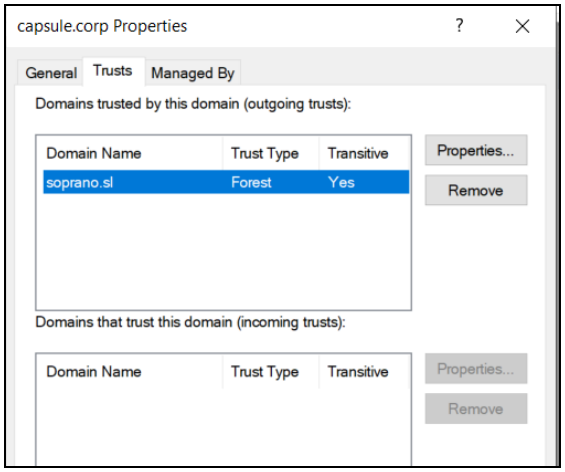


Ilustración 40 - Relación de confianza unidireccional

Con esto se consigue que capsule.corp **conozca y pueda configurar accesos** a cuentas de soprano.sl pero, por otro lado, ninguna cuenta o recurso de capsule.corp va a poder interactuar con soprano.sl. De esta forma se consigue aislar dicho bosque administrativo de posibles errores humanos que se puedan cometer en el bosque de producción.

Para poder administrar el bosque de producción desde el bosque administrativo, es necesario configurar privilegios de alguna forma a las cuentas de soprano.sl. Microsoft añadió el concepto de **Shadow Principals** en Windows 2016, y es lo que recomienda utilizar para este modelo de administración con bosques externos.

Para poder administrar mediante Shadow Principals, es necesario desactivar una protección que viene por defecto en las relaciones de confianza entre bosques llamada **SID Filtering**. Esta protección se encarga de **filtrar/ignorar** un atributo denominado **SID History**, que se encuentra en los tickets de Kerberos.

SID Filtering está activado por defecto porque, en caso contrario, un atacante que ha comprometido un bosque podría **crear tickets de Kerberos válidos** para comprometer cualquier otro bosque externo con el que tuviera confianza. Esto sería posible porque el atacante podría **especificar que es miembro de grupos privilegiados externos** – como Enterprise Admins – en el atributo SID History de sus tickets. De esta manera, al presentar el

ticket, el bosque externo confiaría en la información y le otorgaría los privilegios. Más información sobre cómo abusar esta funcionalidad en el siguiente enlace.

De la misma manera que un atacante puede **abusar** del atributo SID History para comprometer dominios o bosques "vulnerables", un administrador puede **aprovecharlo** para crear un entorno de administración aislado y conveniente.

En el laboratorio existe una relación de confianza unidireccional donde capsule.corp confía en soprano.sl. Nosotros sabemos que soprano.sl es un entorno aislado y protegido de riesgos como Internet o software desactualizado, por lo que desactivar la protección SID Filtering en este escenario es perfectamente viable. En la siguiente imagen se comprueba dicha configuración:

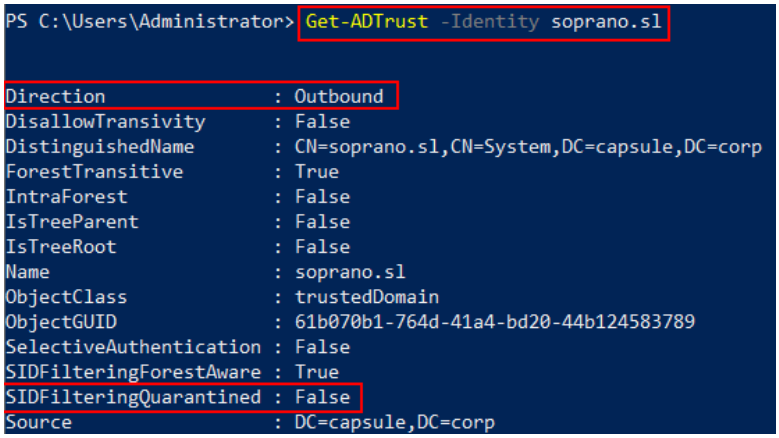


Ilustración 41 - SID Filtering desactivado

Una vez se ha permitido el uso del atributo SID History, tan solo es necesario crear los Shadow Principals oportunos para la administración. Para ello es necesario instalar las características de **PAM** (Privileged Access Management) en soprano.sl con un comando de PowerShell como el siguiente:

- Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope ForestorconfigurationSet -Target soprano.sl

Una vez instaladas, vamos a configurar la cuenta **redadmin** de soprano.sl para que disponga de privilegios de Enterprise Admins en el bosque de producción capsule.corp.

Para ello, se crea un objeto de tipo **msDS-ShadowPrincipal** con el identificador de seguridad (SID) de **Enterprise Admins del bosque capsule.corp**. Una vez creado el Shadow Principal, se añade a la cuenta redadmin como miembro del mismo.

Los comandos de PowerShell utilizados son los siguientes:

- # Se obtiene el SID del grupo Enterprise Admins del bosque capsule.corp
  $ShadowPrincipalSid = (Get-ADGroup -Identity 'Enterprise Admins' -Properties ObjectSID -Server capsule.corp).ObjectSID
- # Se guarda la dirección del contenedor de Shadow Principals en soprano.sl
  $Container = 'CN=Shadow Principal Configuration,CN=Services,CN=Configuration,DC=soprano,DC=sl'
- # Se crea el Shadow Principal con el SID obtenido anteriormente
  New-ADObject -Type msDS-ShadowPrincipal -Name "capsule-

ShadowEnterpriseAdmin" -Path $Container -OtherAttributes @{'msDS-ShadowPrincipalSid'= $ShadowPrincipalSid}

- # Se añade la cuenta redadmin a dicho Shadow Principal para que disponga de los privilegios
  Set-ADObject -Identity "CN=capsule-ShadowEnterpriseAdmin,CN=Shadow Principal Configuration,CN=Services,CN=Configuration,DC=soprano,DC=sl" -Add @{'member'="CN=redadmin,CN=Users,DC=soprano,DC=sl"} -Verbose

Tras realizar esta configuración, se puede confirmar que redadmin pertenece al Shadow Principal creado a través de la interfaz gráfica (nótese que también se ha añadido la cuenta a otro Shadow Principal para otorgar permisos de Domain Admins).

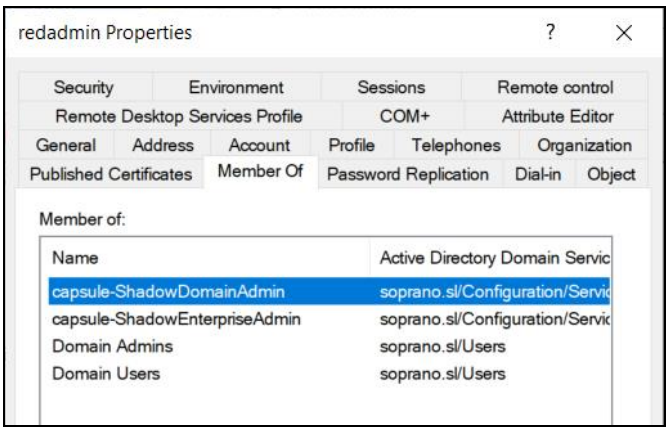


Figure 1 - Shadow Principal

Gracias a esto, redadmin puede acceder a recursos de capsule.corp sin necesidad de indicar ningún tipo de credencial y de una forma segura (ni su contraseña, ni su hash, ni sus tickets quedan almacenados en los sistemas accedidos).

En la siguiente imagen se puede ver cómo se accede al Domain Controller de capsule.corp a través de PS Remoting:

```
PS C:\> whoami
soprano\redadmin
PS C:\> hostname
red-dc01
PS C:\> Enter-PSSession -ComputerName dc01.capsule.corp -Authentication NegotiateWithImplicitCredential
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents>
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents>
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents> whoami
soprano\redadmin
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents> hostname
dc01
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==========
Everyone                                   Well-known group S-1-1-0                                        Mandatory
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory
BUILTIN\Administrators                     Alias            S-1-5-32-544                                   Mandatory
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory
SOPRANO\Domain Admins                      Group            S-1-5-21-2597617849-483382974-3078061232-512 Mandatory
CAP\Domain Admins                          Group            S-1-5-21-272438138-3995100478-3847831165-512   Mandatory
CAP\Enterprise Admins                      Group            S-1-5-21-272438138-3995100478-3847831165-519   Mandatory
CAP\Denied RODC Password Replication Group Alias            S-1-5-21-272438138-3995100478-3847831165-572   Mandatory
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
[dc01.capsule.corp]: PS C:\Users\redadmin.SOPRANO\Documents>
```

Ilustración 42 - Administración desde soprano.sl

Si se comprueban los grupos de Domain Admins y Enterprise Admins en el bosque capsule.corp, se verá que redadmin no es miembro de ninguno de ellos. Gracias al atributo SID History, redadmin puede obtener dichos privilegios sin necesidad de ser miembro.

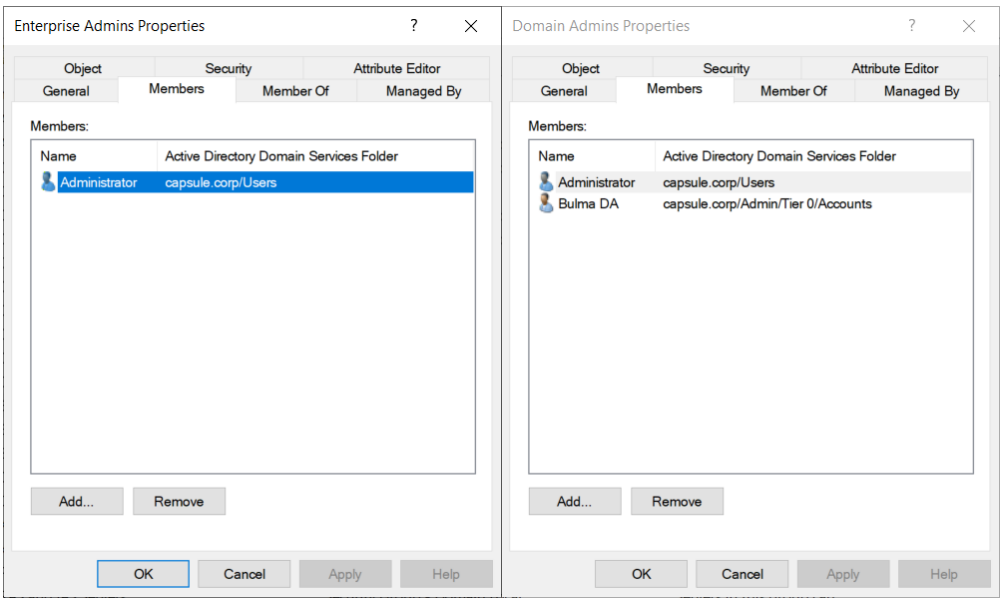


Ilustración 43 - Redadmin no es miembro