Protección de Identidades

Transcribed on August 8, 2025 at 11:25 AM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la protección de identidades.

Vamos a hablar de diferentes tecnologías que nos ayudan a proteger las identidades, especialmente dentro del entorno del directorio activo.

Hablaremos de las directivas de autenticación de los polis y hilos, hablaremos de cómo configurar estos elementos y luego hablaremos de otras tecnologías que nos ayudan en la protección de credenciales como Credenti Algar.

Vamos a hablar de los requerimientos y la configuración de Credenti Algar.

Hablaremos también de Windows Defender Application Control y luego también ter remmoe Credenti G.

Vamos a ver cómo configurar estas tecnologías y qué implicaciones tiene el habilitar este tipo de características.

Las credenciales por defecto de las diez últimas contraseñas se cachean en los equipos de forma local.

Esta característica representa un riesgo de seguridad que puede facilitar un ataque sobre las credenciales de una organización.

Microsoft proporciona diferentes tecnologías que pueden ayudar a minimizar el riesgo sobre este tipo de ataques.

Por ejemplo, como hemos visto, el grupo de usuarios protegidos que previene el proceso de cacheo de credenciales en los perfiles de los equipos, que requiere autenticación de querberos, limita los tickets TGT a un periodo de cuatro horas y que no permite el inicio de sesión offline.

Tenemos también las directivas de autenticación que van a permitir configurar políticas de autenticación dentro del directorio activo para después aplicar a cuentas de servicio, cuentas de usuario o cuentas dequipi.

Ofrece la posibilidad también de personalizar los tickets TGT y puede interactuar con una tecnología que se llama DINMICA Test Control ##EMOS de Dinamica Control, que es una tecnología muy interesante para la personalización de condiciones.

Y luego tenemos los polis y hilos, que realmente es una agrupación donde nosotros vamos a configurar o vamos a agrupar de forma conjunta directivas de autenticación para cuentas de usuario, para cuentas de servicio y para cuentas dequipo.

Las directivas de autenticación son un nuevo objeto dentro de las clases del sistema operativo Windows que nos va a permitir trabajar con directivas de autenticación de tal forma que vamos a poder hacer configuraciones más restrictivas para querberos y especificar esas configuraciones para cuentas de usuario, para cuentas de servicio o para cuentas dequipit.

Además vamos a poder interactuar con los clims de DINMICASST Control, que son unos tokens, unas pequeñas piezas de información que nosotros podemos definir y que nos van a ayudar a generar condiciones específicas.

Por ejemplo, yo puedo generar una pieza de información que sea confidencial y luego esa pieza de información que sea confidencial puedo añadirla a un documento o puedo añadirla a un determinado objeto de Activo Directory, cualquier cosa es un objeto, un usuario es un objeto, un servicio, una aplicación, una carpeta, un documento.

Entonces yo con estos pequeños claims que genero con dnmic Accs Control puedo generar una serie de piezas de información que después puedo añadir a esos objetos, puedo enlazar con esos objetos y de esta manera voy a poder hacer condiciones mucho más específicas.

Yo por ejemplo puedo hacer que una carpeta, cuando se accede a la documentación de esa carpeta de forma local se pueda leer y escribir, pero cuando se accede a esa carpeta de forma remota sólo se pueda leer, pero puedo generar un clim que sea Jefe de Departamento y ese clim, por ejemplo a ese usuario que va a ser Jefe de Departamento le voy a permitir modificar esa carpeta aunque sea de forma remota.

Entonces Dinámica GST Control es una tecnología muy interesante que nos va a enriquecer el sistema de condiciones que nosotros podemos utilizar para los permisos en un ámbito muy amplio.

Podemos en este caso agregar piezas de información de Dinámicas Control a directivas de autenticación, pero trabaja también por ejemplo Confederation Service con los servicios federados del Directorio Activo, podemos utilizar los clen generados por Dinmic TES Control, incluirlos dentro de las condiciones de Federation Service.

Los requerimientos para las directivas de autenticación es Windows Server 2012 R o versiones superiores para los Controladores de dominio, Nivel funcional de dominio 2012-R y después los controladores de dominio tienen que soportar dinámica C control, es decir que tenemos que configurar una directiva para que todos los controladores de dominio puedan utilizar Dark.

Cuando nosotros configuramos las directivas de autenticación vamos a poder configurar una serie de parámetros, vamos a poder configurar el nombre, la descripción, si esa directiva dónde va a ser aplicada o qué condiciones de restricciones vamos a aplicar o podemos ponerla también en modo de auditoría, es decir que podemos hacer que se apliquen esas restricciones pero que no eviten que sólo auditen y se generan unos registros, pues antes de poner esa directiva activada, la vamos a poner en modo auditoría, vamos a observar cómo funciona y después podemos ponerla en modo restrictivo.

Las cuentas de equipo de servicio de usuario pueden definirse de forma separada y también nos va a permitir modificar o personalizar los tickets TGT.

Después para una configuración centralizada y que sea más cómoda, podemos utilizar los polisis hilos, los polis y hil los van a permitir a los administradores configurar las cuentas de equipo de servicio y de usuario y administrarlas de forma conjunta.

Nos van a poder restringir el acceso a las estructuras de archivos y vamos a poder también habilitarlas en modo de auoría o poder habilizarlas en modo de restricción.

Tenemos otras tecnologías que nos ayudan en la protección de credenciales como son credencial al bar, cuando nosotros iniciamos sesión en un equipo Windows, todos los tokens de credenciales que nosotros tenemos habilitados, que nosotros vamos a utilizar, es decir, pues las credenciales ENTLM, los ticks, TGTB, carberos, creces, SP, pues todos los elementos que nosotros vamos a utilizar se van a almacenar en un proceso de la memoria que es Local Security Authority.

Entonces muchos ataques conocidos como por ejemplo con herramientas como VCE o mimicad, lo que hacen es extraer los credenciales de memoria y después utilizan el token de esas creciales MTLM o el ticket TGT para después hacer suplantación de identidad y utilizar por ejemplo ese ticket de carperos para poder acceder a todos los servicios o todos los privilegios que podría acceder el usuario legítimo.

¿Cómo funciona Credenti Algar?

Pues lo que hace es generar un nuevo proceso separado del resto del sistema por tecnología de elcoalizmiento y después mantiene todos los secretos y las credenciales almacenados en ese nuevo proceso que se llama el SA aislado.

Entonces si nosotros tratamos de acceder a ese proceso, no vamos a poder acceder porque el sistema está protegido del sistema mediante tecnología de virtualización y si nosotros hacemos un volcado de memoria de LSA a estar vacío, no va a tener secretos ni va a tener las credencialestlm de carguos, etcéa, etcétera.

Y si hacemos un volcado de el SA aislado pues va a estar cifrado.

Entonces todos los ataques que se basan en corden, ticken, pastejah, todo este tipo de ataques que extraen las credenciales de memoria para luego poder utilizarlas pues van a fracasar y van a dejar de funcionar.

De hecho miicap tiene una estrategia en la que reinicia el dispositivo para deshabilitar Credencia Algar y después poder extraer las credenciales de memoria.

Es una estrategia que además de ser bastante escandalosa, bastante ruidosa, porque si reiniciamos un equipo de producción normalmente eso se va a detectar.

Aparte de eso nosotros podemos habilitar Credencial Algar para que tenga protección en el sistema de arranque de wifi, de tal forma que cuando nosotros tenemos un reinicio del sistema el propio Windows va a proteger el arranque para que no se puedan deshabilitar o modificar características, con lo cual Mimica en este caso tampoco funciona.

Entonces si nosotros hacemos una correcta configuración de Credenti Algar pues va a ser muy difícil que se extragan las credenciales y va a dificultar mucho los ataques de escalada horizontal o escalado vertical en los que yo me hago con credenciales para lugo iniciar sesión en otros dispositivos o para tener privilegios para hacer ciertas operaciones en el dispositivo en el liancño.

¿Cuál es el inconveniente dec credenti algar?

Bueno, credenti algar necesita todos los requerimientos que veis en la diapositiva de tal forma que en máquinas físicas sea realmente fácil de implementar.

Las máquinas moverass casi todas van a ser compatibles con la tecnología paraed al gas, pero máquinas virtuales es un poquito más complejo.

De hecho cuando nosotros trabajamos con Credenti Algar generalmente se puede desplegar Credenti Algar pero no se va a activar porque la máquina virtual no va a tener las tecnologías de virtualización, los requisitos de virtualización correspondientes para que Credenti Algar funcione.

Para esto nosotros tendríamos que configurar la máquina virtual dentro de una tecnología de virtualización anidada.

Si por ejemplo trabajamos con iperv, iperv tiene una característica que se llama virtualización anidada en el que una máquina virtual pueda a su vez ser un servidor de máquinas virtuales, porque cuando nosotros utilizamos tecnología de virtualización por el visor delalbose, vware o i per v, cualquiera de los tres, la máquina virtual deja de ver el hardware de la máquina física y va ar aquella parte del hardware que el hipervisor le permite.

Cuando nosotros habilitamos la virtualización anidada la máquina virtual puede ver todo el hardware con lo cual también tiene capacidad de virtualización y Credente Algar, al ser una tecnología que se basa en virtualización, necesita esa tecnología.

Entonces en máquinas virtuales es más complejo habilitar Credente al G.

Si nosotros utilizamos virtualización anidada vamos a poder habilitar la característica.

De hecho cuando tenemos máquinas en Azure, en Azure tenemos máquinas virtuales y podemos habilitar Credencial Algar.

Aparte, Credenti Algar va a restringir una serie de tecnologías para evitar que esas credenciales que están aisladas mediante virtualización pues se puedan atacar con protocolos inseguros.

Entonces no permite delegación de carberos, no permite cifrado con DES y no soporta NTM vers 1, MSCHAP vers 2 o Cretesp.

Si nosotros utilizamos una tecnología de VPN, acceso a un servicio, una aplicación que utilice cualquiera de estas tecnologías, no podríamos habilitar credittialgar porque esa tecnología no funcionaría.

Tenemos otra característica, la proteción de dispositivos, que sería ir un pasito más allá, que es Windows Defender Application Control.

Lo que va a hacer realmente esta tecnología es que nosotros vamos a crear una lista de aquellos elementos que se pueden ejecutar dentro del sistema.

Es una tecnología quizás de las más potentes o de las más restrictivas dentro de Microsoft, pero también de las más eficientes porque nos va a permitir la ejecución de malware, incluso de ataques Zeo Days.

Nosotros vamos a generar una lista blanca de lo que se puede ejecutar en el dispositivo y después no va a permitir que se ejecute nada que no esté en esa lista.

Evidentemente un malware 1 day o con un malicioso no va a estar en esa lista, por lo tanto no va a permitir que se ejecute y tampoco va a permitir las llamadas dinámicas o las inyecciones o cargas de código desde los procesos que tenemos en la máquina.

Es una de las maneras más eficientes de defender un dispositivo.

Todas estas tecnologías que le dente al GAP o Application Control, etc.

Etcétera, normalmente son tecnologías para desplegar en una parte de la organización.

Son tecnologías para desplegar en toda la organización porque no sería viable y muchas de las aplicaciones o servicios que utilizamos habitualmente dejarían de funcionar.

Pero para aquellas máquinas críticas para ciertos servicios, para ciertas partes de la organización, son unas tecnologías muy eficientes y nos da un grado de seguridad muy alto.

Otra tecnología que va en esta misma línea es Remote credentialgar Remote Credenti.

Lo que nos va a permitir es no entregar las credenciales.

Cuando nosotros hacemos una conexión de escritorio remoto, conectamos con un determinado servicio, cuando nosotros habilitamos la característica de Remo Credentialgar, cuando hacemos una petición a OB Servidor o hacemos una petición de escritorio remoto, lo que estamos haciendo es que esa petición se redirige hacia el controlador de dominio, de tal forma que el controlador de dominio autoriza esa operación y entregaas credenciales o deja las credenciales en el equipo de origen, con lo que nunca se entregan credenciales en el dispositivo de destino.

Vamos a poder configurar Rembo Credenti al dar mediante la habilitación del registro como veis en la diapositiva.

También podemos hacerlo por línea de comandos con el comando por ejemplo recdd en la ruta que tenéis en la diapositiva con la sintaxis que podéis ver y también podemos hacerlo a través de directivas de grupo.

Muchas de estas tecnologías que nosotros estamos hablando, una de las formas más eficientes y más seguras de configurarlas es mediante el GPO, mediante objeto de directiva de no sólo la vamos a configurar de una forma segura sin tocar el registro a pelo, sino que además vamos a poder hacer la configuración, aplicarla a una unidad organizativa y que se aplique un amplio número de equipos o un amplio número de usuarios y de esta forma vamos a tener la tecnología de una forma mucho más segura y mucho más controlada.

Por eso es importante entender correctamente cómo funcionan los objetos de directivo de grupo porque después nos van a servir para aplicar de forma eficiente diferentes tecnologías de seguridad.

Remote Credenti Algar también podemos pasarlo como parámetro cuando nosotros iniciamos una conexión de escritorio remoto con los comandos que tenéis en el final de la diapositiva.

Vamos a ver un poco toda esta tecnología.

Bueno, estamos en Windows Server y dentro de Windows Server vamos a ir a la parte de Tools, nos vamos a ir a Usuarios equipos de Active Directory y dentro de Usuarios Equipos de Active Directory tenemos aquí una unidad organizativa que hemos creado que se llama Protecteded Server, tenemos un equipo que es el servidor y si nos vamos a la parte de administración de directivas de grupo, dentro de la unidad organizativa de Protectage Service tenemos una GPU que se llama credentialgar, que si nos vamos a ver la

Dentro de la parte de plantillas administrativas nos vamos a la parte de System y vamos a tener aquí davidgarard.

Dentro de davidgar vemos que tenemos habilitada la protección basada en virtualización.

Si nosotros vamos a ver las características tendríamos aquí la explicación de cómo funcionaría esta tecnología y vamos a tener aquí diferentes elementos que nos van a permitir trabajar o configurar esta característica.

Podemos habilitar la parte de arranque seguro o arranque seguro con protección de MIA.

Tenemos aquí la protección de integridad de código que podríamos habilitarla con bloqueo de wifi y tenemos aquí la posibilidad de configurar Credenti Algar.

Y dentro de la posibilidad podemos también habilitarlo con bloqueo de wifi, es decir, que vamos a bloquear el sistema de arranque seguro y mediante WEL wifi para que no se pueda modificar en el sistema de arranque.

Si además a esto nosotros añadimos que ciframos el volumen de sistema con bitlocker, bitlocker también va a ayudarnos a proteger todos los archivos del sistema de arranque como hemos visto en vídeos anteriores, con lo cual vamos a dificultar mucho el poder modificar esa configuración de Credente Algar.

Otra tecnología que tenemos en la misma categoría es la de control de aplicaciones.

Si nosotros habilitamos esta tecnología nosotros tendríamos aquí la posibilidad de habilitarla y después aquí pondríamos la ruta de ese archivo con esa lista que vamos a permitir de lo que se va a permitir que se ejecute en el dispositivo.

Es una configuración que es muy estricta pero también es una de las configuraciones más seguras que hay.

Si nosotros queremos configurar Remote Credenti al dar tenemos en la parte de delegación de credenciales una serie de configuraciones mediante objetos de directiva de grupo que son muy interesantes.

Tendríamos aquí la configuración de Remot Credentida, daríamos aquí habilitado y aquí podemos requerir Remón Credenti Algar, Administración restringida o la delegación de credenciales.

Pero aparte de esta tecnología de REM Credenti Algar, nosotros vamos a tener aquí toda una serie de configuraciones de diferentes GPOs que sirven para la parte de delegación de credenciales.

Yo os recomiendo que dediquéis unos minutos a revisar cada una de estas opciones porque la delegación de credenciales es uno de los elementos más importantes en la configuración cuando nosotros estamos haciendo un proceso de fortificación de un sistema operativo o de una infraestructura.

Bueno, todas estas tecnologías, todas estas tecnologías con las que nosotros estamos trabajando que se basa en virtualización nos van a ayudar en la protección de credenciales.

Si ahora nosotros nos vamos al equipo server 7, estamos en el equipo servidor 7 y en el equipo servidor siente, una manera muy fácil de verificar la tecnología de virtualización y cómo está funcionando es con MS Info.

Bueno si nosotros nos vamos a la parte de abajo en la consola de MS Info, vamos a ver la tecnología de virtualización y las protecciones que tenemos.

Vemos que tenemos aquí la protección de DMA del kernel que está apagada, vemos que tenemos aquí la virtualización que está habilitada, la seguridad basada en virtualización que está habilitada pero que no se está ejecutando y después vemos que tenemos aquí SecureB y vemos que tenemos aquí credente al PA.

Es decir que nosotros tenemos todas estas tecnologías que se están utilizando que están configuradas.

Lo que pasa aqu el inconveniente es que algunas de estas tecnologías en la máquina virtual no se ejecutan porque la máquina virtual desde VirtualBox no ve toda la capacidad de virtualización y todos los componentes, todos los requisitos que necesita el dispositivo en la parte de hardware.

Eso no quiere decir que el dispositivo real no tenga los requisitos o no cumplan los requisitos para que funcionen estos elementos, pero al estar un hipervisor en el medio entre la máquina virtual y el hardware no le permite utilizar todas estas tecnologías.

Si nosotros utilizáramos iypperv y dentro de hypperv utilizemos virtualización anidaa, sí que podríamos habilitar todas estas tecnologías porque en la mayor parte de los casos los componentes de hardware de los dispositivos actuales son compatibles con Remoote, Credenti Algar, con Credenti Algar, con DA Car y con todo este tipo de tecnologías.

Como hemos visto tenemos una serie de elementos, tanto las directivas de autenticación como los polis y silos, como otras tecnologías como Credenti Algar, Credenti Algar, etcéter que nos van a permitir aseurizar y hacer un proceso de fortificación de la administración y manejo de credenciales dentro de una infraestructura basada en tecnología de Microsoft.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.