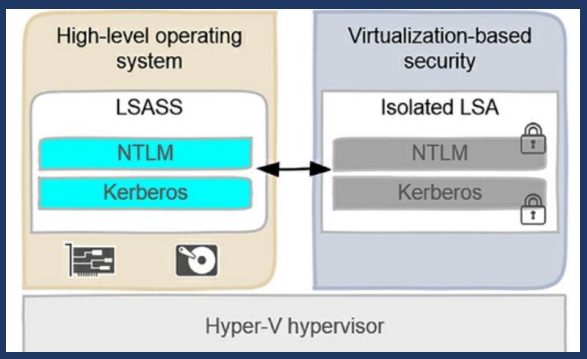
Presentación

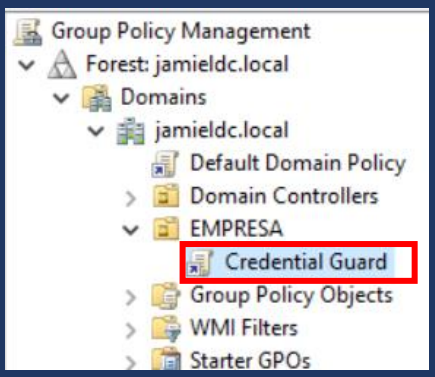
- **Nombre del estudiante:** Jamiel Santana.
- **Matricula:** 2019-8095
- Nombre del profesor: Geancarlos Sosa
- **Mat:** Seguridad de SO.
- **Tema:** Credential Guard.
- **Centro Educativo:** Instituto tecnológico de las Américas.

- Puede que sepa que ha habido un control de cuentas de usuario (UAC) y un archivo / carpeta de virtualización desde Windows Server 2008. Este tipo de virtualización protege áreas clave del sistema de archivos y el registro de Windows contra el acceso no autorizado.
- Credential Guard utiliza lo que Microsoft llama "seguridad basada en la virtualización" para almacenar Secretos de NTLM y Kerberos en un proceso de autoridad de seguridad local (LSA) aislado.
- vemos una computadora con Windows en la que Credential Guard no está configurado esto hace que los secretos de NTLM y Kerberos se van almacenen en la memoria del modo de usuario dentro del proceso LSASS. Esto hace que las credenciales sean accesibles para los atacantes que buscan elevar su privilegio con herramientas de piratería como Mimikatz.
- A la derecha vemos el mismo sistema Windows, esta vez con Credential Guard habilitado.
- Gracias al hipervisor Hyper-V subyacente, se almacenan los secretos NTLM y Kerberos.

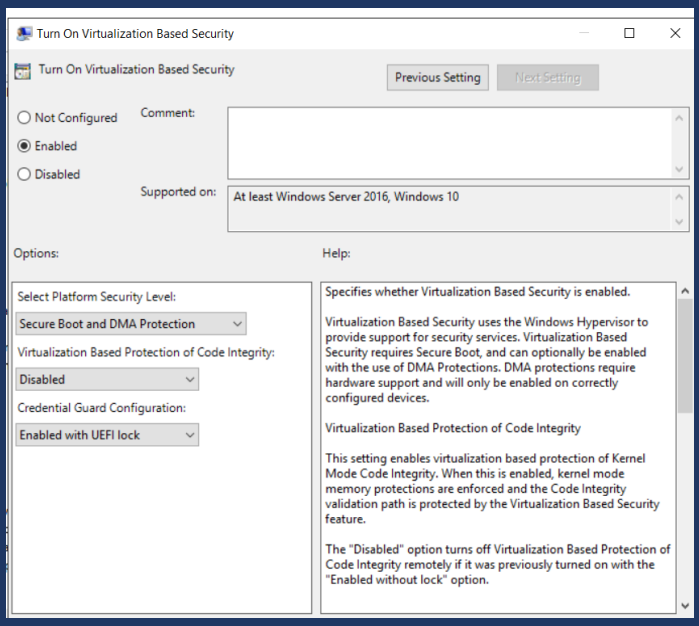


- Es interesante porque los requisitos del sistema para Credential Guard en realidad se remontan a algunas de las características que discutimos anteriormente:
    - Sistema operativo de 64 bits Esto no es un problema para Windows Server, pero podría ser un problema para dispositivos Windows Client.
    - El firmware UEFI, v2.3.1 o superior, es necesario UEFI cuando se confía en el arranque seguro para Credential Guard.
    - Extensiones de virtualización de CPU Para procesadores Intel, esto es VT-x. Para AMD procesadores, es AMD-V. De cualquier manera, las extensiones deben ser compatibles con Second Level.
    - Traducción de direcciones (SLAT) también.
    - TPM v1.2 o 2.0 El TPM es necesario para almacenar las claves de cifrado de Credential Guard También, necesita ejecutar Windows 10 Enterprise Edition si planea habilitar Credential Guard en los sistemas cliente de Windows.

- **Crear una GPO habilitando Credential Guard y desplegarla a los equipos del dominio:**
  - Lo primero que haremos es crear una GPO llamada Credentian Guard haciendo referencia al nombre del proyecto la cual se la asignaremos a nuestra OU, para esto nos vamos al **GROUP POLICY MANAGEMENT, para crear la GPO.**



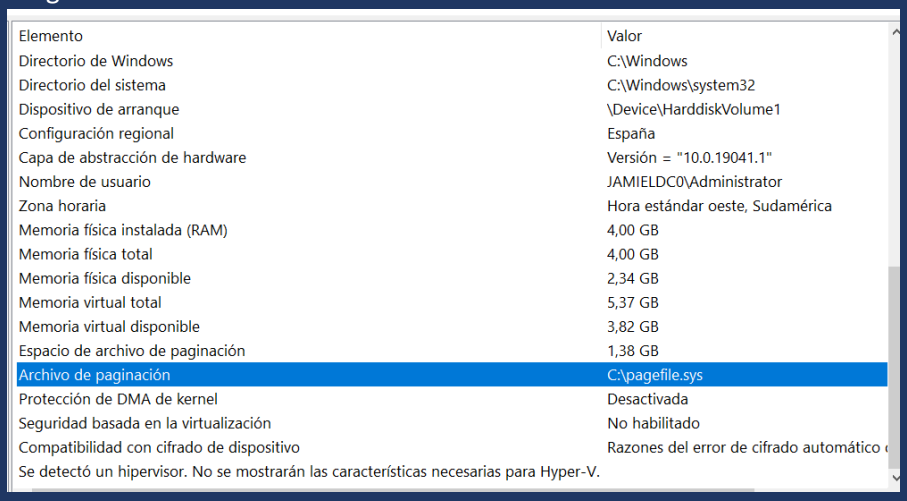
- Una vez creada la GPO procedemos a editarla para habilitar el credential guard, para poder habilitar dicha política nos dirigimos a la siguiente ruta dentro del GROUP POLICY MANAGEMENT EDITOR, pólice > Administrative template > system > device guard, ya dentro de device guard encontraremos dos políticas donde solo habilitaremos la segunda, llamada **turn on virtualization based security**. Donde el nivel de seguridad de la plataforma seleccionamos SECURE BOOT AND DMA PROTECTION, donde el DMA protection protege el acceso directo a la memoria y el booteo seguro se define solo, la segunda opción la dejamos deshabilitada y el crendential guard configuration que es el más importante escogemos la opción de Enable whith UEFI, asea activado con el UEFI bloqueado brindando mayor seguridad, realizado esto podemos guardar y aplicar cambios.



- Ahora nos dirigimos del lado cliente para realizar un gpupdate /forcé para que se actualicen las directivas de grupo, realizado esto si no tenemos un TPM habilitado con dará un error de la clave de cifrado, pero como esto es con motivos prácticos lo obviaremos**, recalcando que para el correcto funcionamiento de este se necesita utilizar hyperv y habilitar el TMP**, ya actualizada las directivas si damos un ctrl + r y escribimos msinfo32 par poder ver infomaciones más profundas sobre el sistema.

- Y nos dirigimos a la parte baja de dicha ventana nos encontraremos con las siguientes informaciones.

- Si vamos atrás y vemos como se encontraba msinfo32 antes de estas configuraciones se encontraba de la siguiente manera.



- Vemos como ninguna de las opciones aparecen.

- **Abundar sobre los ataques “pass the hash”:**
  - En el mundo de la seguridad informática esto es una técnica de hacking muy utilizada en entrornos de directorio activo, pero en concreto esto es una técnica que permite al atacante acceder a un servidor remoto mediante el uso del hash NTLM.
  - Existen varias formas de obtener el hash NTLM de la red la forma que utilizo es mediante un responder que envenena la red para obtener dichos hashes, para posteriormente poder autenticarme fácilmente con herramientas como pth-winexe.

- **Añadir ejemplos de uso:**
  1. Un usuario accede a un equipo cliente y proporciona un nombre de dominio, un nombre de usuario y una contraseña. El cliente calcula un hash criptográfico de la contraseña y descarta la contraseña real. El cliente envía el nombre de usuario al servidor (en texto sin formato).

  2. El servidor genera un número aleatorio de 16 bytes, llamado desafío, y lo envía de vuelta al cliente.

  3. El cliente cifra este desafío con el hash de la contraseña del usuario y devuelve el resultado al servidor. Esto se denomina respuesta.

  4. El servidor envía los tres elementos siguientes al controlador de dominio: - Nombre de usuario - Desafío enviado al cliente - Respuesta recibida del cliente.

  5. El controlador de dominio utiliza el nombre de usuario para recuperar el hash de la contraseña del usuario. Compara el desafío cifrado con la respuesta del cliente (en el paso 4). Si son idénticos, la autenticación se realiza correctamente y el controlador de dominio notifica al servidor.

  6. A continuación, el servidor envía la respuesta apropiada al cliente.