Ejercicios Modulo 3 Unidad 2
Hardening - Configuraciones y servicios (Parte 01)
Alumno: Rodrigo Vila

Ejercicio Número 1 Unidad 2

¿Qué es el Hardening?

- ✓ Configuración segura y robusta del sistema operativo

• Una manera de endurecer un dispositivo

• Hardware seguro solamente

• Es una técnica que usan los atacantes para ver nuestras debilidades

De acuerdo a su elección, justificar el porqué de la misma.:

El Hardening es el proceso de asegurar un sistema operativo, reduciendo su superficie de ataque y minimizando las vulnerabilidades. Esto incluye deshabilitar servicios innecesarios, configurar adecuadamente las políticas de seguridad, instalar actualizaciones de seguridad y aplicar parches. No se trata solo de hardware seguro, ni es una técnica utilizada por los atacantes, sino una práctica defensiva que fortalece la seguridad del sistema operativo.

El ítem de la lista “Una manera de endurecer un dispositivo” también podría ser, pero le faltaría mas desarrollo a las posibles respuestas para satisfacer la complejidad del concepto.

En resumen, según mis palabras, se trata de eliminar al mínimo posible el rango de vulnerabilidades e incrementar al máximo la seguridad manteniendo la eficiencia. Ya sea en sistemas operativos, como firmwares, configuraciones, etc. de cada dispositivo individual beneficiando a la red completa.

“…en principio un sistema con una única función es más seguro que uno con muchos propósitos.”

¿Qué queremos conseguir?

– Prevenir la pérdida de información y caídas del sistema

– Proteger el sistema contra ataques y accesos no autorizados

– Limitar el impacto de vulnerabilidades

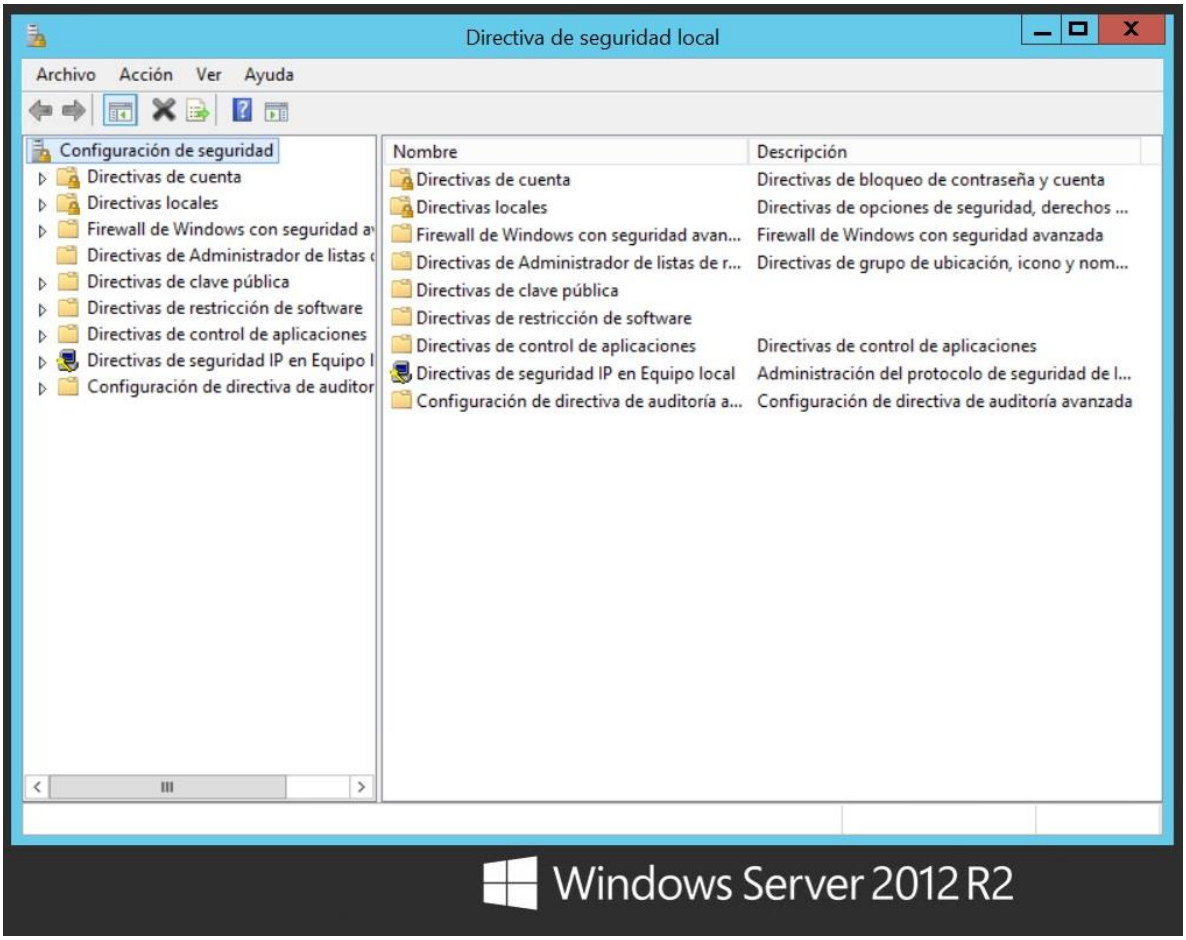
– Prevenir el uso no autorizado del sistema a los usuarios

– Evitar vectores y técnicas de ataques conocidos

En una máquina virtual, que disponga de un SO basado en Windows 10, hacer uso de lo expuesto relacionado a seguridad y mejora del mismo.

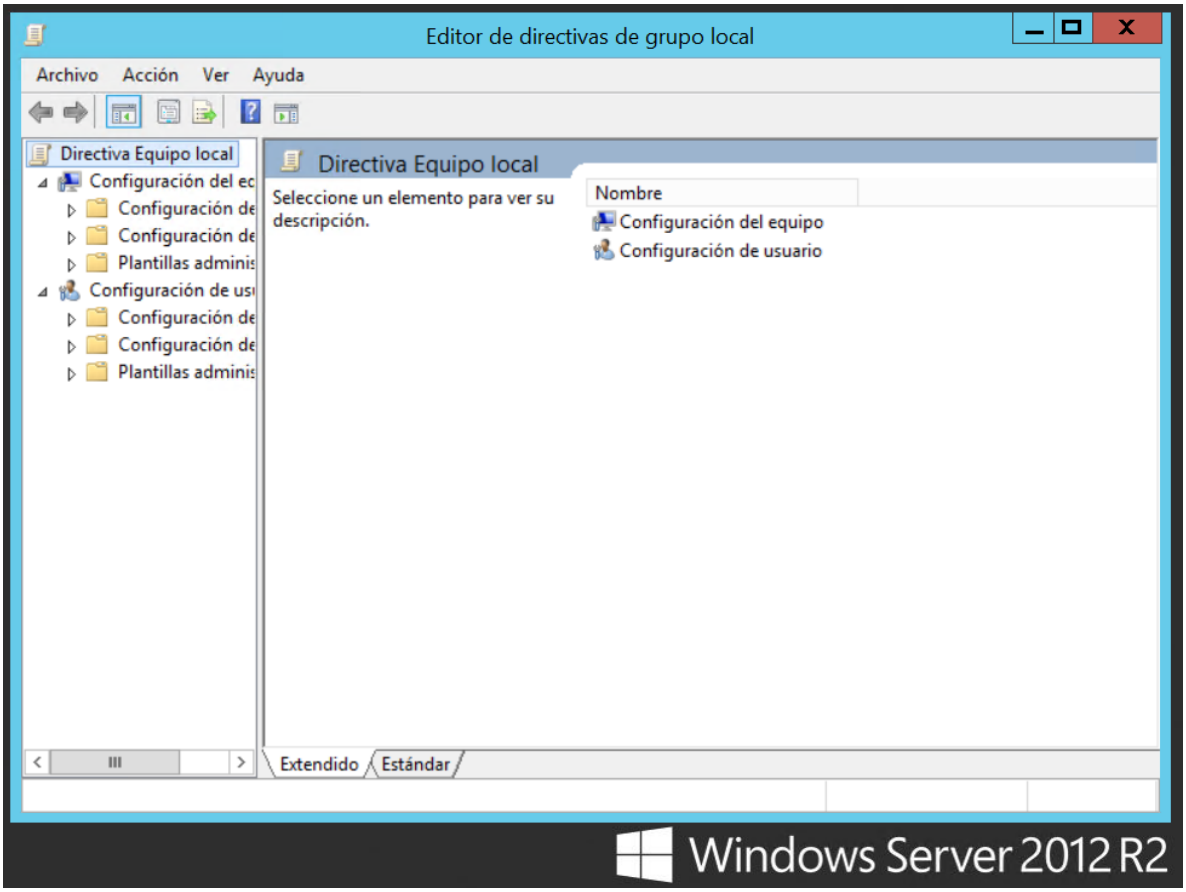
A) Uso de SECPOL.MSC y de GPEDIT.MSC (desde botón inicio, ejecutar)

secpol.msc:



Permite configurar la política de seguridad local. A través de esta herramienta, se pueden establecer políticas de auditoría, políticas de cuenta, políticas de clave pública, entre otras, que ayudan a reforzar la seguridad del sistema.

gpedit.msc:

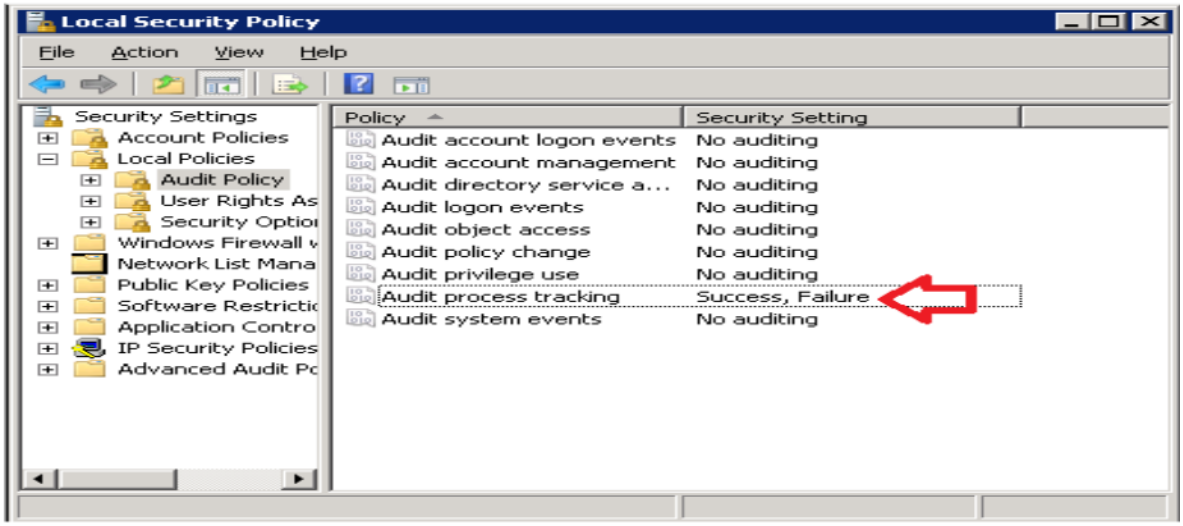


Permite modificar las políticas de grupo en una máquina con Windows. Con esta herramienta, puedes configurar políticas de seguridad, administrar plantillas administrativas, y controlar configuraciones de usuario y equipo en un entorno Windows.

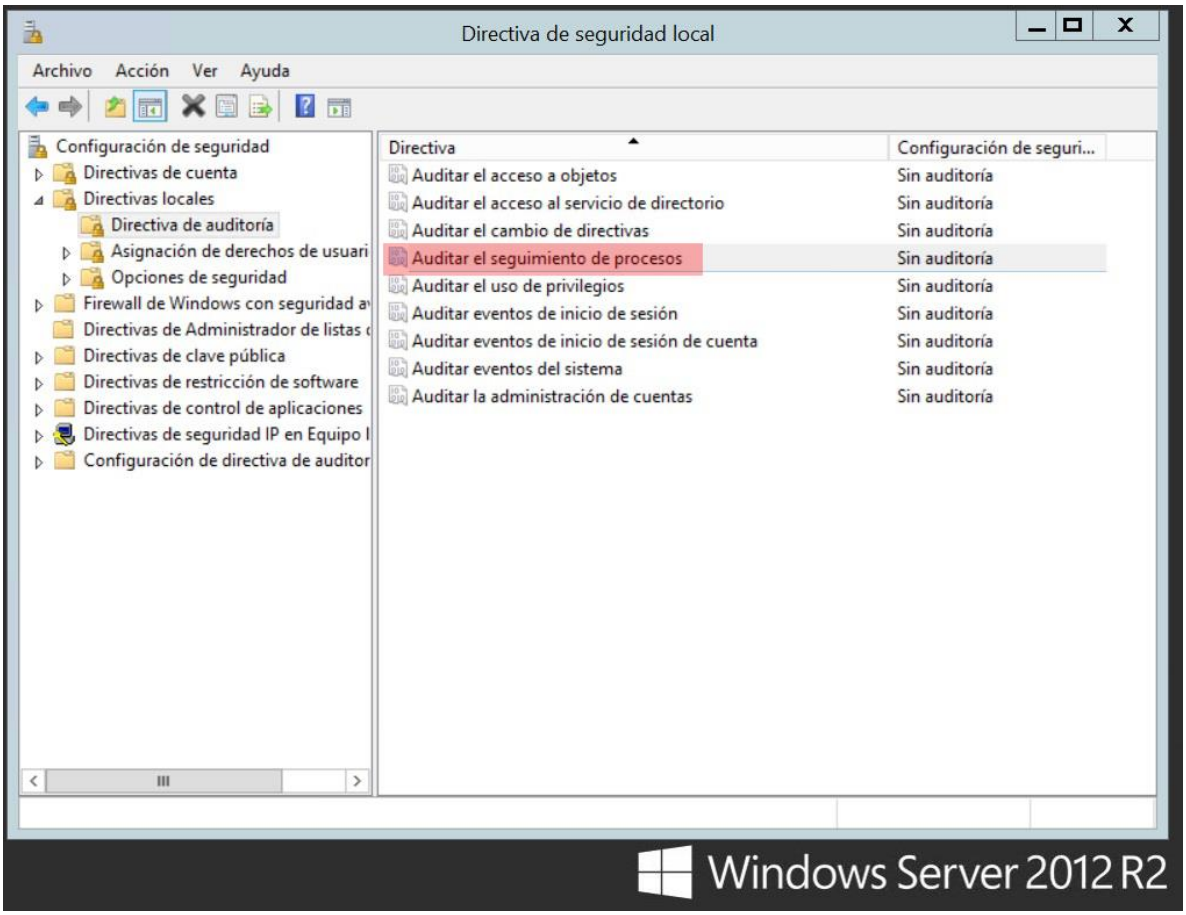
Ejercicio Número 2 Unidad 2

Probar las siguientes opciones e informar qué procesos se están llevando a cabo:

La imagen que muestra el módulo:



Equivalente en mi Windows Server 2012 r2:



La directiva “Access process tracking” o “Auditar el seguimiento de procesos” es una configuración de seguridad que determina si el sistema operativo

audita eventos relacionados con procesos como la creación de un proceso, la finalización de un proceso, identificadores duplicados y acceso indirecto a objetos.

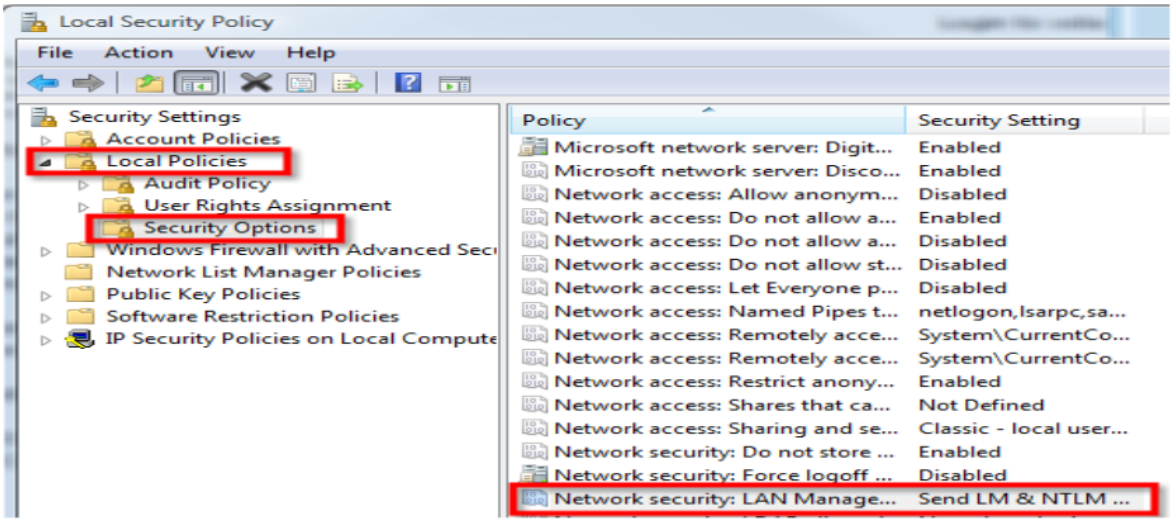
Si se define esta configuración de directiva, el administrador puede especificar si auditar solo los eventos correctos, los incorrectos, ambos o ninguno de estos eventos (es decir, ni correctos ni incorrectos).

Si se habilita la auditoría de eventos correctos, se genera una entrada de auditoría cada vez que el sistema operativo realiza alguna de estas actividades relacionadas con procesos.

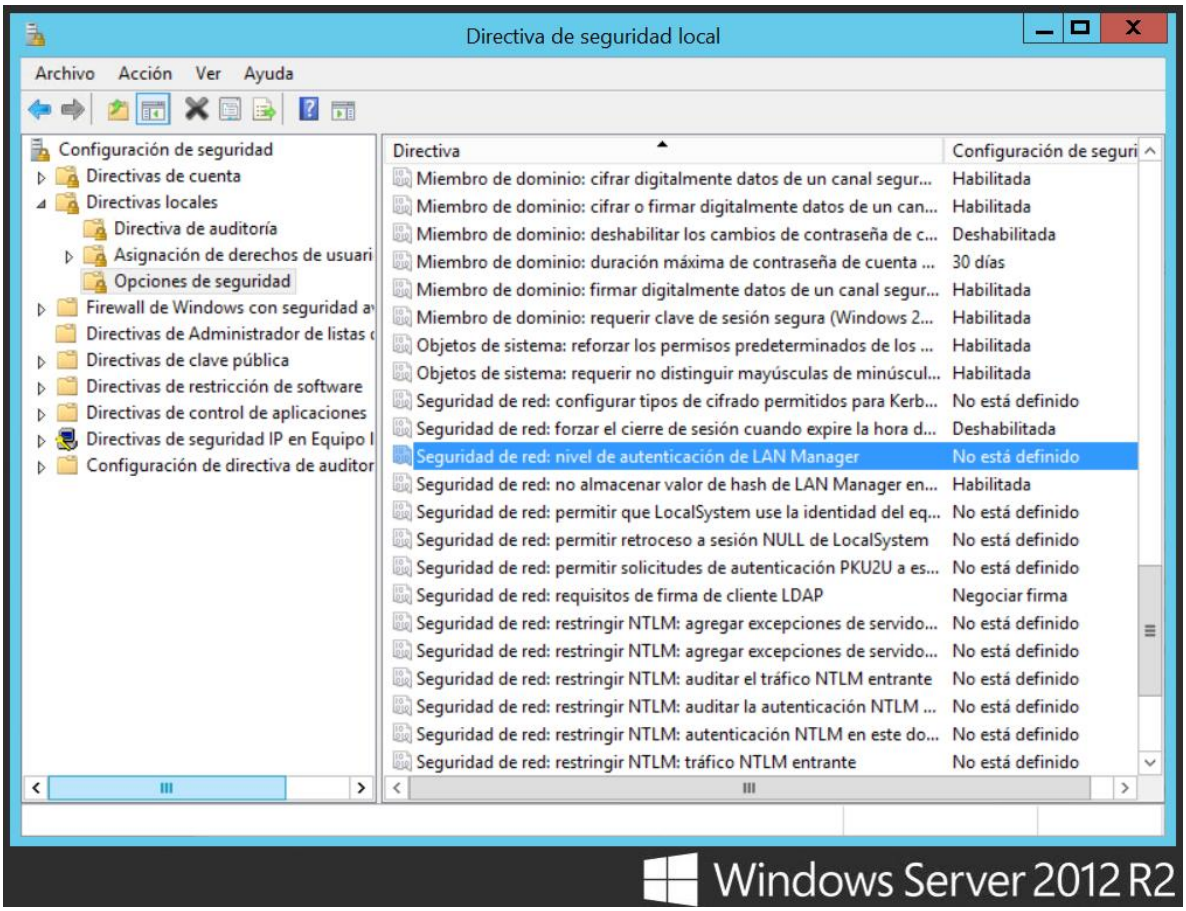
Si se habilita la auditoría de eventos incorrectos, se genera una entrada de auditoría cada vez que el sistema operativo no consigue realizar alguna de estas actividades.

Ahora vamos con la segunda imagen:

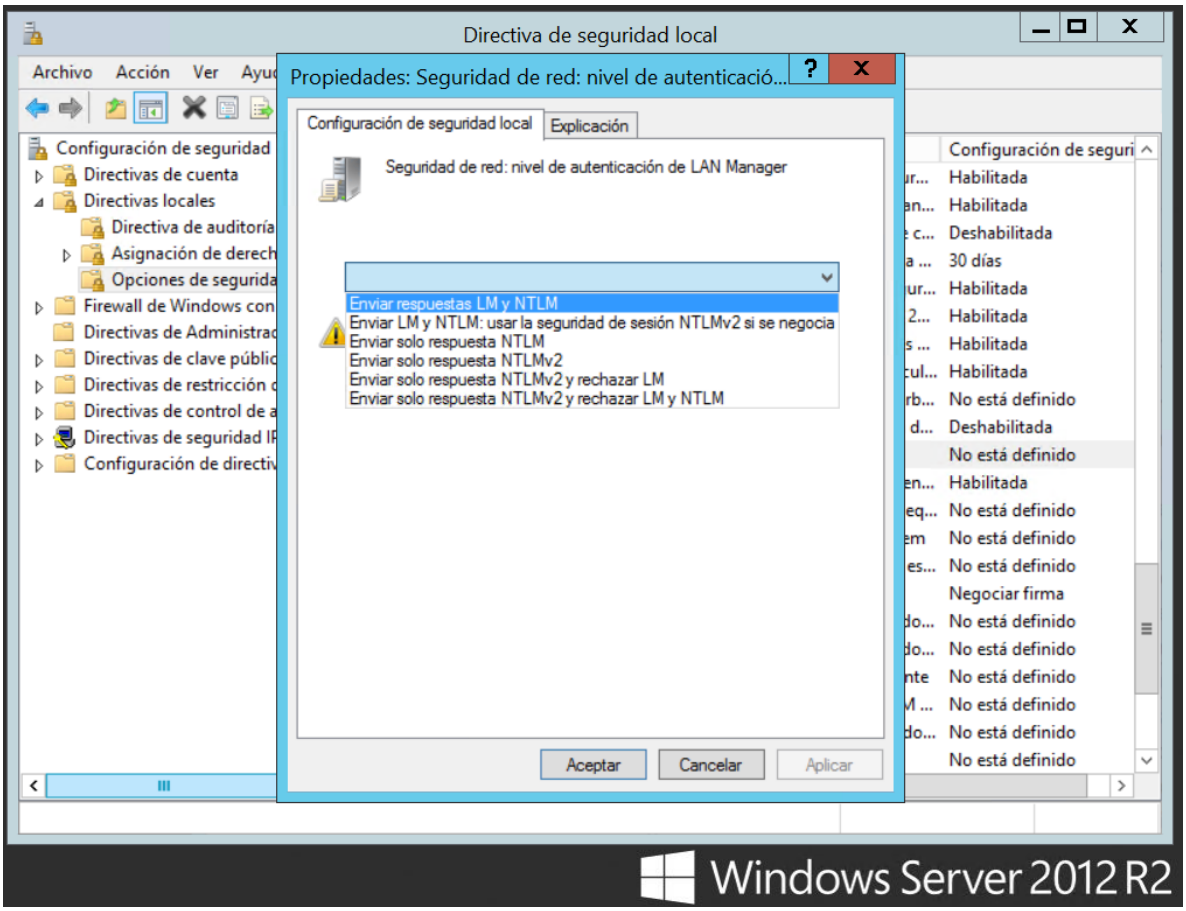
Imagen que muestra el módulo:



El nombre no se ve completo, pero voy a suponer que se trata de la directiva "Network Security: LAN Manager authentication level". El equivalente en Windows Server 2012 r2 en español sería “Seguridad de red: nivel de autenticación de LAN Manager”.:



Dentro de las propiedades de ésta directiva nos encontramos con las siguientes configuraciones a elegir:



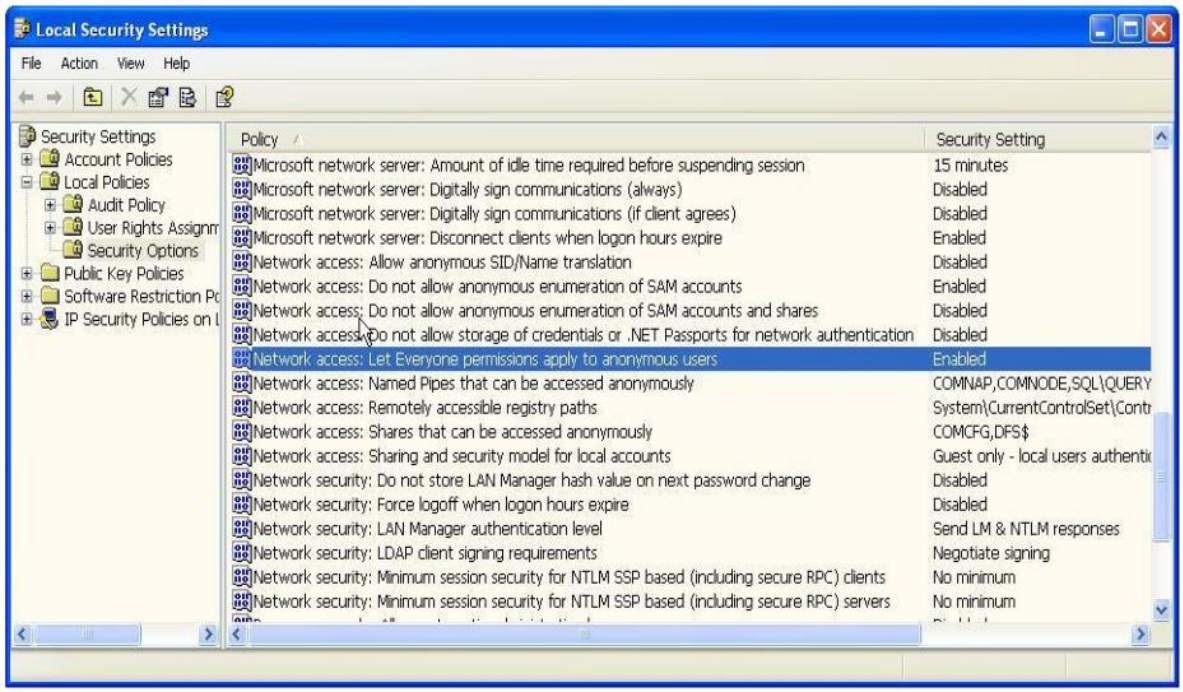
Esta configuración de seguridad determina el protocolo de autenticación desafío/respuesta que se usa para inicios de sesión de red. Esta opción afecta al nivel de protocolo de autenticación usado por los clientes, el nivel de seguridad de sesión negociado y el nivel de autenticación aceptado por los servidores de la siguiente manera:

- Enviar respuestas LM y NTLM: los clientes usan la autenticación LM y NTLM, y no usan nunca la seguridad de sesión NTLMv2; los controladores de dominio aceptan la autenticación LM, NTLM y NTLMv2.
- Enviar LM y NTLM: usar la seguridad de sesión NTLMv2 si se negocia: los clientes usan la autenticación LM y NTLM, así como la seguridad de sesión NTLMv2 si el servidor la admite; los controladores de dominio aceptan la autenticación LM, NTLM y NTLMv2.
- Enviar solo respuesta NTLM: los clientes solo usan la autenticación NTLM, así como la seguridad de sesión NTLMv2 si el servidor la admite;

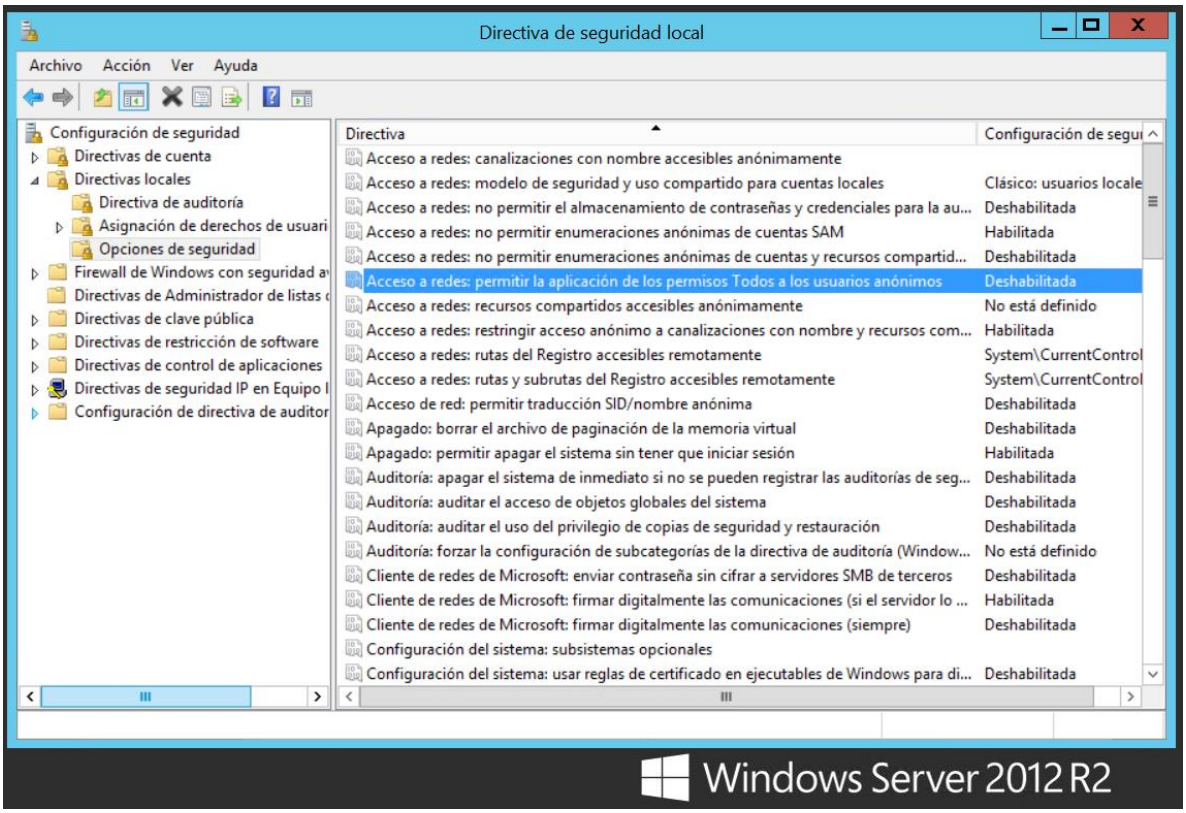
los controladores de dominio aceptan la autenticación LM, NTLM y NTLMv2.

- Enviar solo respuesta NTLMv2: los clientes usan solo la autenticación NTLMv2, así como la seguridad de sesión NTLMv2 si el servidor la admite; los controladores de dominio aceptan la autenticación LM, NTLM y NTLMv2.
- Enviar solo respuesta NTLMv2 y rechazar LM: los clientes solo usan la autenticación NTLMv2, así como la seguridad de sesión NTLMv2 si el servidor la admite; los controladores de dominio rechazan LM (solo aceptan la autenticación NTLM y NTLMv2).
- Enviar solo respuesta NTLMv2 y rechazar LM y NTLM: los clientes solo usan la autenticación NTLMv2, así como la seguridad de sesión NTLMv2 si el servidor la admite; los controladores de dominio rechazan LM y NTLM (solo aceptan la autenticación NTLMv2).

Tercera imagen del módulo:



Equivalente en mi S.O expuesto:

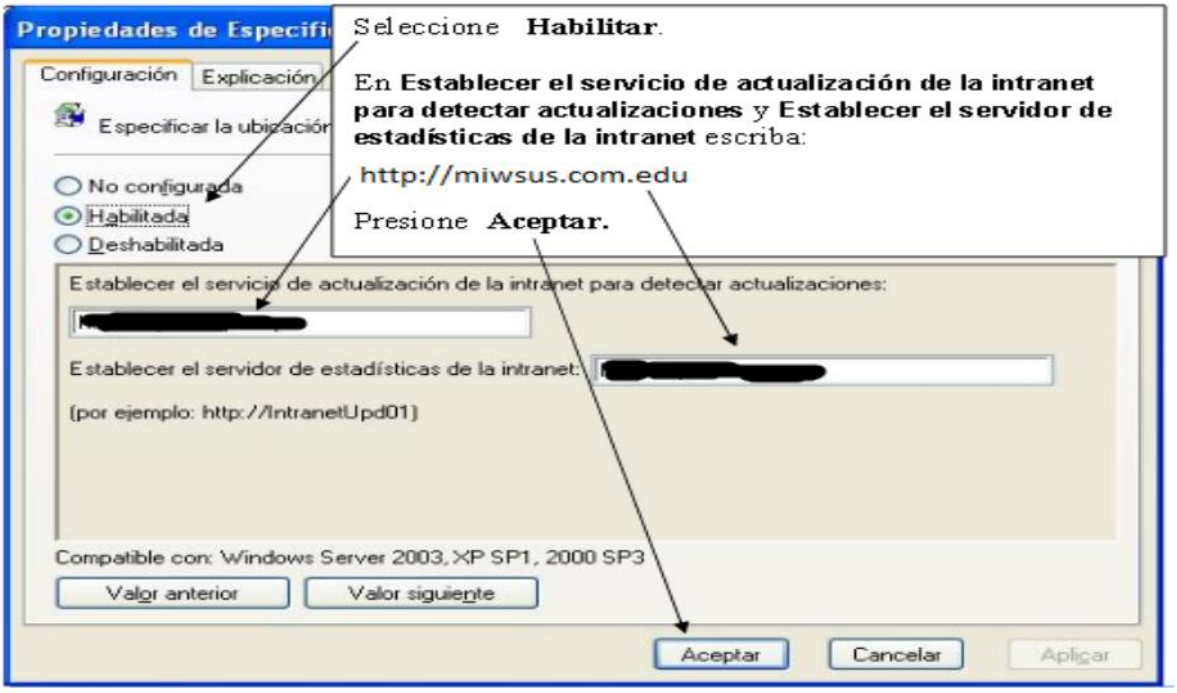


Esta configuración de seguridad determina los permisos adicionales que se conceden para conexiones anónimas al equipo.

Windows permite a los usuarios anónimos realizar ciertas actividades, como enumerar los nombres de cuentas de dominio y recursos compartidos de red. Esto es conveniente, por ejemplo, cuando un administrador desee conceder acceso a usuarios en un dominio de confianza que no mantiene una confianza recíproca. De manera predeterminada, se quita el identificador de seguridad (SID) de “Todos” del token creado para conexiones anónimas. Por tanto, los permisos concedidos al grupo “Todos” no se aplican a los usuarios anónimos. Si se establece esta opción, los usuarios anónimos solo tienen acceso a los recursos para los que se les haya concedido permiso explícitamente.

Si se habilita esta directiva, se agrega el SID de “Todos” al token creado para conexiones anónimas. En este caso, los usuarios anónimos tienen acceso a todos los recursos para los que se haya concedido permiso al grupo “Todos”.

Servicio WSUS (Windows Server Update Services)



A pesar de que podemos configurar las actualizaciones apuntando a donde queremos que las encuentre, quien se anima a explicar lo bueno y lo malo de esta opción de uso de WSUS.:

Si se configura el WSUS (Windows Server Update Services) para apuntar a una dirección maliciosa, el atacante puede controlar las actualizaciones que se distribuyen a los sistemas. Esto puede permitir la instalación de actualizaciones falsas o maliciosas, comprometiendo la seguridad de todos los sistemas que dependen de ese WSUS. El atacante podría instalar malware, obtener acceso no autorizado a los sistemas, y potencialmente controlar toda la red que depende de ese servidor de actualizaciones.

Formas de mitigar este ataque

Establecer usuarios con permisos limitados: Solo los administradores deben tener permisos para cambiar la configuración del WSUS. Los usuarios normales no deberían tener la capacidad de modificar estos ajustes críticos.

Servidor de actualizaciones centralizado: Utilizar un servidor de actualizaciones centralizado que descargue actualizaciones únicamente de los

servicios de Windows asegura que las actualizaciones son legítimas y no han sido alteradas.

Actualizaciones firmadas por Microsoft: Configurar el sistema para que solo acepte actualizaciones firmadas digitalmente por Microsoft previene la instalación de software no autorizado.

Bloquear servicios no esenciales: Configurar el firewall para permitir que el servicio de actualización se comunique solo con los servidores oficiales de Microsoft o el servidor centralizado de actualizaciones.

Lo bueno y lo malo de ésta opción de uso de WSUS:

<u>Lo bueno:</u>

- Control Centralizado:

Permite centralizar la administración de actualizaciones, lo que facilita el control y la supervisión de los parches y actualizaciones aplicadas a todos los dispositivos de la red. Esto asegura que todos los sistemas estén actualizados de manera uniforme. También mejora la seguridad al asegurar que las actualizaciones críticas se apliquen de manera oportuna y consistente en toda la infraestructura.

- Optimización del Ancho de Banda:

Reduce el uso del ancho de banda de internet, ya que las actualizaciones se descargan una vez en el servidor WSUS y luego se distribuyen localmente a todos los clientes. A su vez aumenta la eficiencia de la red y mejora el rendimiento general, especialmente en entornos con múltiples sistemas.

- Aprobación de Actualizaciones:

Permite a los administradores aprobar o rechazar actualizaciones antes de que se apliquen a los clientes. Esto proporciona un control adicional sobre qué actualizaciones que se implementan. Así se reduce el riesgo de problemas causados por actualizaciones defectuosas o incompatibles.

Lo malo:

- Riesgo de Configuración Incorrecta:

Una configuración incorrecta puede llevar a que los sistemas no reciban actualizaciones críticas, lo que puede dejar a la red vulnerable a ataques y exploits. Esto puede comprometer la seguridad y la estabilidad del sistema si las actualizaciones no se gestionan correctamente.

- Dependencia del Servidor WSUS:

Si el servidor WSUS falla o está fuera de línea, los clientes pueden quedar sin la capacidad de recibir actualizaciones, lo que podría llevar a una exposición prolongada a vulnerabilidades conocidas. Esto aumenta el riesgo de fallos de seguridad y la necesidad de contar con un plan de contingencia robusto.

- Carga Administrativa:

Requiere una administración continua y diligente para asegurarse de que las actualizaciones se prueben y aprueben antes de ser implementadas en los sistemas de producción. Esto incrementa la carga de trabajo para los administradores de IT, que deben estar atentos a las nuevas actualizaciones y a los posibles problemas que puedan surgir.

- Configuraciones Maliciosas:

Si un atacante compromete el servidor WSUS o redirige las actualizaciones a un servidor malicioso, podría distribuir software malicioso bajo la apariencia de actualizaciones legítimas. Podría llevar a la instalación de malware en toda la red, comprometiendo la integridad y la seguridad de todos los sistemas.

Ejercicio Número 3 Unidad 2

Si en vez de poner esa dirección, hubiésemos puesto otra dirección, pero de forma maliciosa ¿quése puede lograr u obtener?

Detallar en lo posible, lo que un atacante quiere disponer o realizar.:

Creo que ésta pregunta se responde sola con algunos de los ejemplos expuestos en la consigna anterior, pero para dar una mirada personal, se me

ocurre que un atacante podría poner la dirección a un repositorio de malware, con herramientas autoejecutables que modifiquen el comportamiento del sistema, como deshabilitar protecciones, y para resumirlo un poco, instalar backdoors para tener acceso al sistema e incluso a la red mas garantizado aunque modifiquen nuevamente la dirección de los updates.

Scanning with Lynis:

Starting…

Finishing…

Rodrigo Vila.-