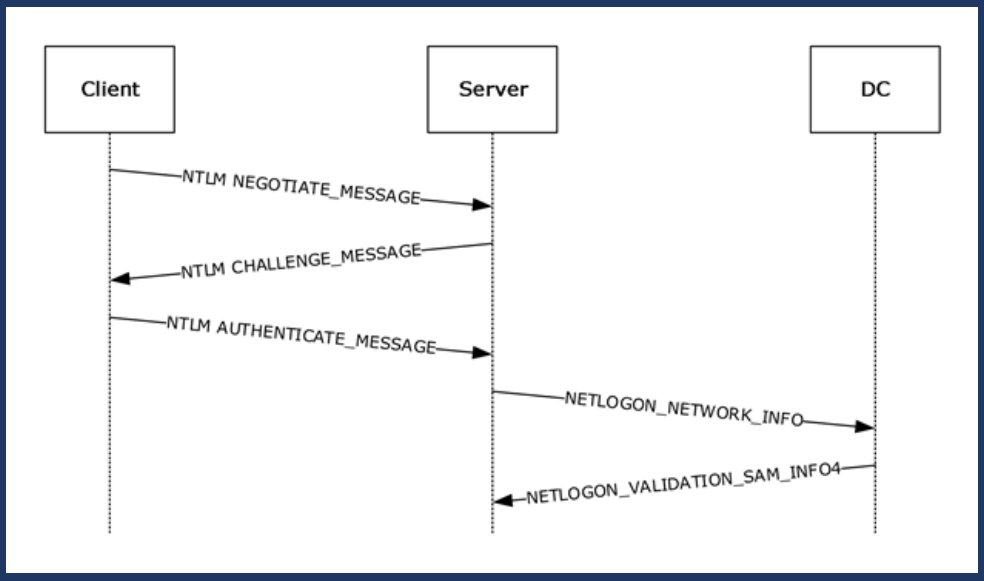
Presentación

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

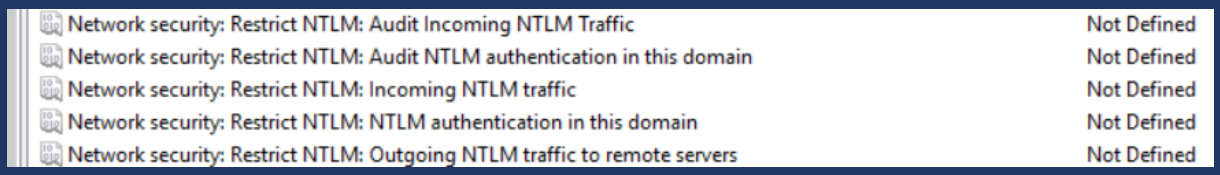


- Muchos administradores de sistemas de Windows (tal vez incluso usted) han permitido que el NT anticuado, Protocolo de autenticación de LAN Manager (NTLM).
- Desde Windows Server 2003, Kerberos se ha sugerido en lugar de NTLM, ya que es un protocolo de autenticación más fuerte que utiliza la autenticación mutua en lugar del método de desafío/respuesta NTLM. NTLM tiene una serie de vulnerabilidades conocidas, incluyendo que utiliza criptografía más débil y no tiene autenticación de servidor. Es posible fuerza bruta una contraseña de longitud 8 usando NTLM en sólo unas horas, y NTLM también es vulnerable al paso del ataque hash.

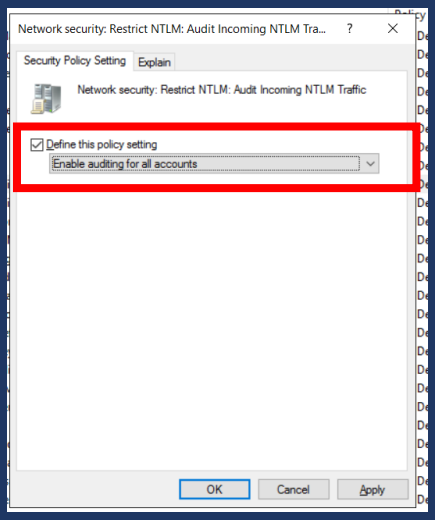
- Las opciones de directiva de grupo para NTLM se encuentran en Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad.

- Donde las políticas que habilitaremos serán las siguientes:

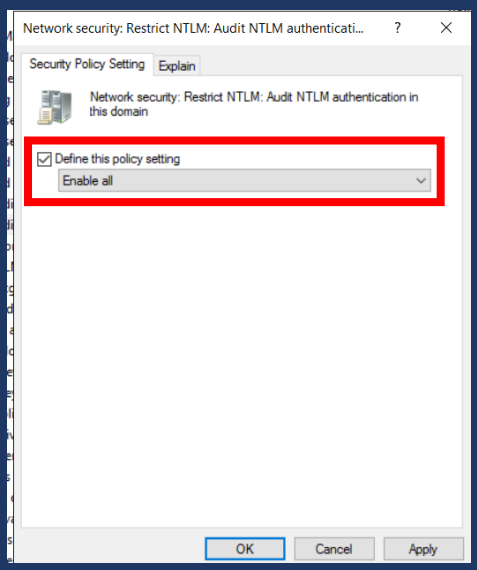
    - Network Security: Restrict NTLM: NTLM Authentication In This Domain.
    - Network Security: Restrict NTLM: Incoming NTLM Traffic.
    - Network Security: Restrict NTLM: Outgoing NTLM Traffic To Remote Servers.
    - Network Security: Restrict NTLM: Audit NTLM Authentication In This Domain.
    - Network Security: Restrict NTLM: Audit Incoming NTLM Traffic.
- Justamente las que se ven en la imagen.



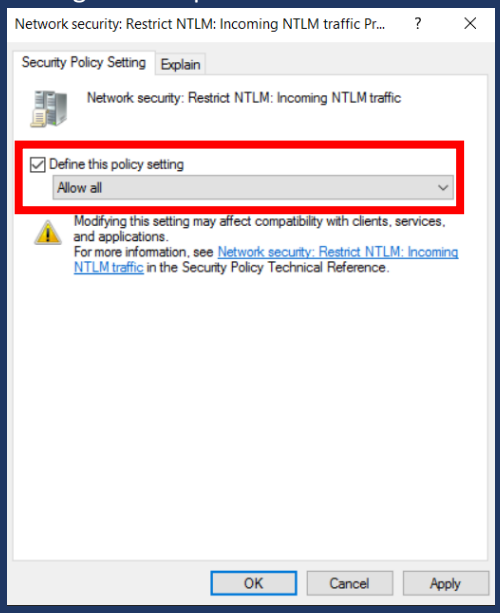
- Comenzaremos editando por el mismo orden de la imagen, la primera seria **Audit incoming NTLM trafic**, donde con esta GPO se busca que el servidor audite o supervise los traficos NTLM entrantes en el servidor, si damos click en la política, marcamos la casilla, y como el objetivo es desplegarlo a todo el mundo seleccionamos la opción **Enable auditing for all accounts, aplicamos y aceptamos.**



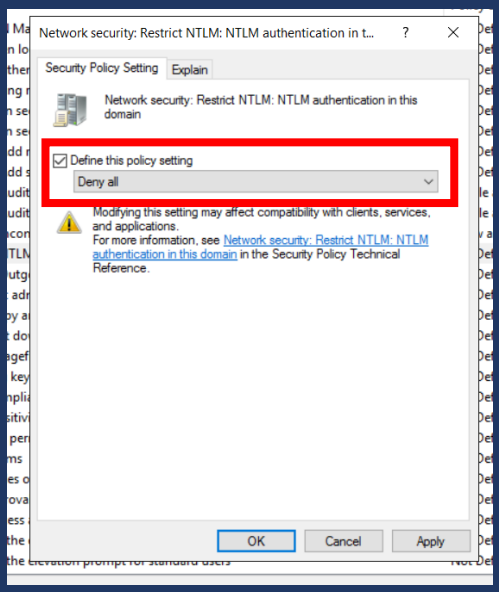
- La siguiente política seria Audit NTLM authentication in this domain, donde su nombre bien lo dice donde va a supervisar y auditar los login NTLM en el dominio. Estas primeras políticas se basan en reconocimiento las posteriores a estas se refieren al bloqueo. A esta política marcamos la casilla para poder elegir aquien va a aplicar la política en este caso la habilitamos para todos.



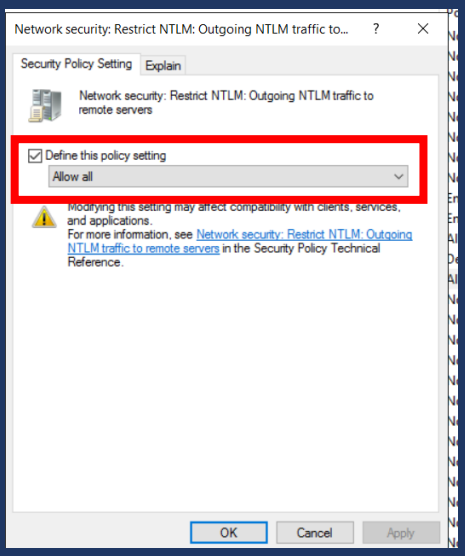
- La tercera política es **incoming NTLM TRAFFIC**, donde con esta política estamos restringiendo el tráfico NTLM entrante en el servidor y como mencionamos anteriormente como la política aplica para todos elegimos la opción de **allow all**.



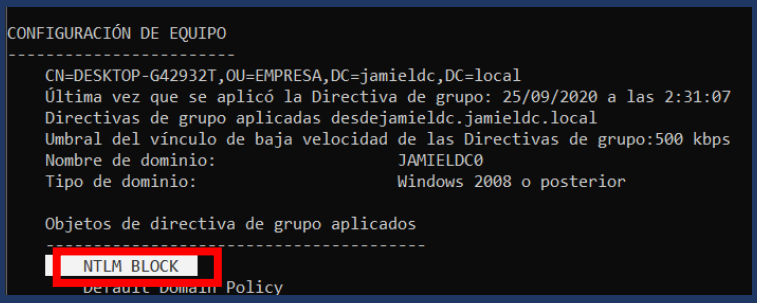
- Ahora pasamos a configurar la política más importante en este laboratorio es la de restringir la autentificación NTLM en el dominio, le negamos la autentificación a todo el user que se encuentre dentro del dominio.



- La última política para configurar será la que va a restringir el tráfico saliente NTLM a servidores remotos, esto es muy importante ya que siempre el AD y el servidor DNS se encuentran separados y se comunican entre si para lograr la autentificación esto la bloqueara obligatoriamente.



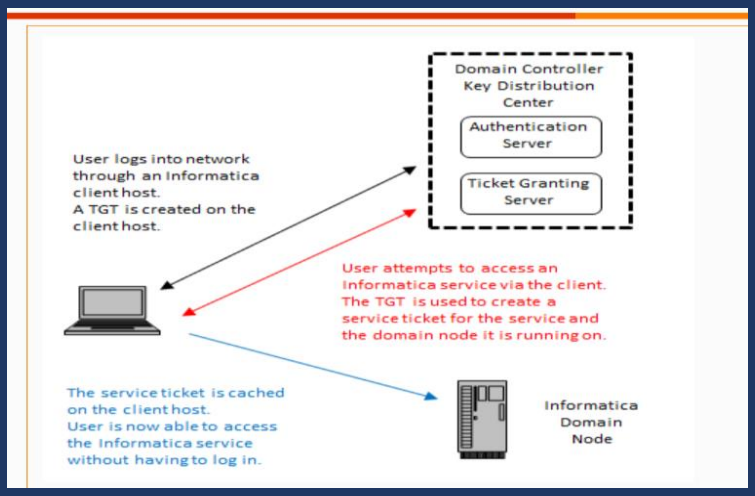
- Teniendo las políticas configuradas ya podemos desplegar la GPO a nuestra máquina cliente, nos dirigimos a la máquina cliente ejecutamos **gpupdate /force**, para actualizar las directivas, posteriormente ejecutamos un **gpresult /r** para mostrar los resultados de la directiva y vemos como efectivamente la directiva está corriendo.



- **Abundar sobre el funcionamiento de NTLM vs Kerberos.**
  - **NTLM** es un protocolo de autenticación. Era el protocolo predeterminado utilizado en las versiones antiguas de Windows, pero todavía se utiliza hoy en día. Si por alguna razón Kerberos falla, NTLM se utilizará en su lugar. NTLM tiene un mecanismo de desafío/respuesta.
  - **Kerberos** es un protocolo de autenticación. Es el protocolo de autenticación predeterminado en las versiones de Windows anteriores a W2k, reemplazando el protocolo de autenticación NTLM.
- **NTLM funciona de la siguiente manera:**

  - El cliente envía un nombre de usuario al host.
  - El host responde con un número aleatorio, el desafío.
  - El cliente crea un valor hash a partir de ese número y la contraseña del usuario y lo devuelve como respuesta.
  - Del mismo modo, el host, que también conoce la contraseña, crea el valor hash y, a continuación, lo compara con la respuesta del cliente.
  - Si ambos valores coinciden, se confirma la autenticidad del cliente y se permite el acceso. Si no hay coincidencia, se bloquea al cliente.

- **Funcionamiento de Kerbeos:**
  1. Un usuario de cliente de Informatica inicia sesión en un equipo de la red que aloja un cliente de Informatica.
  2. La solicitud de inicio de sesión se dirige al Servidor de autenticación, un componente del Centro de distribución de claves (KDC) de Kerberos. El KDC es un servicio de red con acceso a la información de la cuenta del usuario que se ejecuta en cada controlador de dominio del dominio de Active Directory.
  3. El Servidor de autenticación comprueba que el usuario existe en la base de datos de la entidad de seguridad y después crea un token de Kerberos llamado vale de concesión de vales (TGT) en el equipo del usuario.
  4. El usuario intenta acceder a un proceso o servicio del dominio de Informatica mediante un cliente de Informatica.
  5. Informatica y las bibliotecas de Kerberos usan el TGT para solicitar un vale de servicio y una clave de sesión para el servicio solicitado del servidor que concede vales, que también se ejecuta en el KDC.
  6. Kerberos usa el vale de servicio para autenticar el cliente con el servicio solicitado.
  7. El vale de servicio se almacena en la memoria caché en el equipo que aloja el cliente de Informatica, permitiendo que el cliente use el vale mientras siga siendo válido. Si el usuario cierra y después reinicia el cliente de Informatica, el cliente vuelve a usar el mismo vale para acceder a los procesos y servicios del dominio de Informatica.



- **Ventajas de Kerbeos frente a NTLM:**
  - **Los hashes NTLMv1** podrían romperse en segundos con la informática actual, ya que siempre tienen la misma longitud.

  - **NTLMv2** es un poco mejor, ya que es de longitud variable y cifrado mediante un hash, pero no mucho mejor. A pesar de que el hash está cifrado antes de que se envíe, se guarda sin cifrar en la memoria de una máquina. Y por supuesto, cuando hablamos de NTLM, hablamos de un mecanismo de desafío/respuesta, que expone su contraseña al agrietamiento fuera de línea al responder al desafío.

  - **Kerberos** proporciona varias ventajas sobre NTLM: - Más seguro: No se almacena ninguna contraseña localmente o se envía a través de la red. Mejor rendimiento: rendimiento mejorado sobre autenticación NTLM. - Soporte de delegación: los servidores pueden suplantar a los clientes y utilizar el contexto de seguridad del cliente para acceder a un recurso. Gestión de confianza más sencilla: evita la necesidad de tener relaciones de confianza p2p en el entorno de varios dominios.

  - - Soporta MFA (Multi Factor Authentication)