¿Por qué hay nombres de equipos informáticos o nombres de usuario NULOS registrados en los registros de accesorios?

Contenido

Pregunta

- ¿Por qué hay nombres de equipos informáticos o nombres de usuario NULOS registrados en los registros de accesorios?
- ¿Cómo se identifican las solicitudes utilizando credenciales de estación de trabajo o NULL para una exención de autenticación posterior?

Entorno

- Dispositivo de seguridad Cisco Web Security Appliance (WSA): todas las versiones
- Esquema de autenticación NTLMSSP con sustitutos IP
- Windows Vista y los sistemas operativos de Microsoft móviles y de escritorio más recientes

Síntomas

WSA bloquea las solicitudes de algunos usuarios o se comporta de forma inesperada.
Los registros de acceso muestran nombres de equipos informáticos o nombre de usuario y dominio NULL en lugar de IDs de usuario.

El problema se resuelve después de:

- Tiempo de espera de los sustitutos (el valor predeterminado para el tiempo de espera sustituto es de 60 minutos)
- Reinicio del proceso de proxy (comando CLI > *diagnóstico* > *proxy* >)
- Eliminación de la caché de autenticación (comando CLI > *authcache* > *vaciar*)

Antecedentes

En las versiones recientes de Microsoft Operating System, ya no es necesario que un usuario real

esté conectado para que las aplicaciones envíen solicitudes a Internet. Cuando WSA recibe esas solicitudes y se les solicita que se autentiquen, no hay credenciales de usuario disponibles para que las utilice la estación de trabajo cliente, que en su lugar puede tomar el nombre de la máquina del equipo como sustituto.

El WSA tomará el nombre de máquina proporcionado y lo reenviará al Active Directory (AD) que lo validará.

Con una autenticación válida, WSA crea un sustituto IP que enlaza el nombre de la estación de trabajo de la máquina a la dirección IP de la estación de trabajo. Las solicitudes adicionales que vengan de la misma IP utilizarán el sustituto y, por lo tanto, el nombre de la estación de trabajo.

Dado que el nombre de la estación de trabajo no es miembro de ningún grupo AD, las solicitudes no pueden activar la política de acceso esperada y, por lo tanto, se pueden bloquear. El problema persiste hasta que el sustituto ha agotado el tiempo de espera y la autenticación debe renovarse. Esta vez, con un usuario real conectado y credenciales de usuario válidas disponibles, se creará un nuevo suplente IP con esta información y las solicitudes adicionales coincidirán con la política de acceso esperada.

Otra situación que se observa es cuando las aplicaciones envían credenciales no válidas (nombre de usuario NULL y dominio NULL) y credenciales de máquina NO válidas. Esto se considera una falla de autenticación y se bloqueará o si se habilitan las políticas de invitado, la autenticación fallida se considera un "invitado".

El nombre de la estación de trabajo termina con un **$** seguido por **@DOMAIN** que hace que los nombres de la estación de trabajo sean fáciles de rastrear usando el comando CLI **grep** en los registros de acceso para **$@**. Consulte el ejemplo siguiente para obtener más información.

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

La línea anterior muestra un ejemplo de un sustituto IP que ya se ha creado para la dirección IP 10.20.30.40 y el nombre de máquina **gb0000d01$.**

Para encontrar la solicitud que envió el nombre de la máquina, se debe identificar la primera aparición del nombre de la estación de trabajo para la dirección IP específica. El siguiente comando CLI lo logra:

```
> grep 10.20.30.40 -p accesslogs
```

Busque el resultado de la primera aparición del nombre de la estación de trabajo. Las tres primeras solicitudes se reconocen comúnmente como un intercambio de señales NTLM Single-Sin-On (NTLMSSP/NTLMSSP), como se describe aquí y se muestra en el ejemplo siguiente:

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
```

```
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

Al resolver problemas, asegúrese de que estas solicitudes se corresponden con la misma URL y se registran en un intervalo de tiempo muy corto que indica que se trata de un intercambio de señales NTLMSSP automatizado.

En el ejemplo anterior, las solicitudes anteriores se registran con el código de respuesta HTTP 407 (autenticación de proxy requerida) para las solicitudes explícitas, mientras que las solicitudes transparentes se registran con el código de respuesta HTTP 401 (no autenticado).

Hay una nueva función disponible en AsyncOS 7.5.0 y superiores donde puede definir un tiempo de espera sustituto diferente para las credenciales de la máquina. Se puede configurar mediante el siguiente comando:

```
> advancedproxyconfigChoose a parameter group:- AUTHENTICATION - Authentication
related parameters- CACHING - Proxy Caching related parameters- DNS - DNS related
parameters- EUN - EUN related parameters- NATIVEFTP - Native FTP related parameters-
FTPOVERHTTP - FTP Over HTTP related parameters- HTTPS - HTTPS related parameters-
SCANNING - Scanning related parameters- WCCP - WCCPv2 related parameters-
MISCELLANEOUS - Miscellaneous proxy relatedparameters[]> AUTHENTICATION...Enter the
surrogate timeout.[3600]>Enter the surrogate timeout for machine credentials.[10]>.
```

Puede utilizar los mismos pasos para detectar qué solicitudes reciben las credenciales NULAS enviadas y descubrir qué URL o agente de usuario están enviando las credenciales no válidas y eximirlas de autenticación.

Exención de la Autenticación de URL

Para evitar que esta solicitud provoque la creación del sustituto falso, la URL debe estar exenta de autenticación. O bien, en lugar de eximir la URL de la autenticación, puede decidir eximir a la aplicación que envía la solicitud de autenticación, asegurándose de obtener cualquier solicitud para que la aplicación esté exenta de autenticación. Esto es posible agregando el agente de usuario para que se registre en los registros de acceso agregando el parámetro adicional **%u** en los **campos personalizados** opcionales en la suscripción de registro de acceso de WSA. Después de identificar el agente de usuario, debe estar exento de autenticación.