Contenido

Pregunta

- ¿Por qué son los nombres de la máquina del ordenador o los nombres de usuario NULOS accesslogs abiertos una sesión?
- ¿Cómo usted identifica las peticiones usando el puesto de trabajo o las credenciales NULAS para la exención posterior de la autenticación?

Entorno

- Dispositivo de seguridad de la red de Cisco (WSA) - todas las versiones
- Esquema de autenticación NTLMSSP con los sustitutos IP
- Windows Vista y más nuevos sistemas de la operación de Microsoft del escritorio y del móvil

Síntomas

El WSA bloquea las peticiones de algunos usuarios o se comporta inesperado.
Los accesslogs muestran los nombres de la máquina del ordenador o nombre de usuario y dominio NULOS en vez de las identificaciones del usuario.

El problema se resuelve después:

- Los sustitutos miden el tiempo hacia fuera (el valor predeterminado para el descanso sustituto es 60 minutos)
- Recomenzando el proceso del proxy (comando CLI > *diagnóstico* > *proxy* > *retroceso*)
- Caché de la autenticación que vacia (comando CLI > *authcache* > *flushall*)

Antecedentes

En las versiones recientes del sistema operativo Microsoft, no se requiere que abren una sesión a un usuario real más para que las aplicaciones envíen las peticiones a Internet más. Cuando esas peticiones son recibidas por el WSA y pedidas autenticar, no hay credenciales de usuario disponibles utilizar para la autenticación por la estación de trabajo del cliente que en lugar de otro puede tomar el nombre de la máquina del ordenador para un substituto.

El WSA tomará el nombre de la máquina proporcionado y le transmitirá el Active Directory (AD) que lo valida.

Con una Autenticación válida, el WSA crea a un sustituto IP que ata el nombre del puesto de trabajo de la máquina a la dirección IP del puesto de trabajo. Otras peticiones que vienen del mismo IP utilizarán el nombre del sustituto y así del puesto de trabajo.

Con el nombre del puesto de trabajo no siendo miembro de cualquier grupo AD, las peticiones no pueden accionar la política de acceso prevista y ser bloqueadas así. El problema persiste hasta que el sustituto haya medido el tiempo hacia fuera y la autenticación tiene que ser renovada. Esta vez, con un usuario real abierto una sesión y las credenciales del usuario válido disponibles, crearán a un nuevo sustituto IP con esta información y las peticiones harán juego más lejos la política de acceso prevista.

Otro escenario considerado es cuando las aplicaciones envían las credenciales inválidas (nombre de usuario NULO y dominio NULO) y las credenciales inválidas de la máquina. Esto se considera una falla de autenticación y será bloqueada o si se habilitan las directivas del invitado, el auth fallado se considera como “invitado”.

El nombre del puesto de trabajo termina con un **$** seguido por **@DOMAIN** que haga los nombres del puesto de trabajo fáciles localizar usando el **grep del** comando CLI en los accesslogs para **$@**. Vea el ejemplo abajo para la clarificación.

```
> 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 antedicha muestra un ejemplo de un sustituto IP que es creado ya para la dirección IP 10.20.30.40 y el nombre de la máquina **gb0000d01 $.**

Para encontrar la petición que envió el nombre de la máquina, el primer acontecimiento del nombre del puesto de trabajo para la dirección IP específica tiene que ser identificado. El comando CLI siguiente logra esto:

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

Busque el resultado para el primer acontecimiento del nombre del puesto de trabajo. Las tres primeras peticiones se reconocen comúnmente como NTLM Solo-Pecado-en el apretón de manos (NTLMSSP/NTLMSSP) según lo descritas aquí y mostradas en el ejemplo abajo:

```
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 peticiones del thee están para el mismo URL y están abiertas una sesión mismo un intervalo de breve periodo de tiempo indicatiting que es NTLMSSP automatizado un apretón de manos.

En el ejemplo anterior, las peticiones anteriores se registran con el código 407 (autenticación de representación del HTTP de respuesta requerida) para las peticiones explícitas, mientras que las peticiones transparentes serían registradas con el código 401 (unauthenticated) del HTTP de respuesta.

Hay una nueva función disponible en AsyncOS 7.5.0 y más alto donde usted puede definir un diverso descanso sustituto para las credenciales de la máquina. Puede ser configurado usando el siguiente comando:

```
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,-,"-","-"> -
```

Usted puede utilizar los mismos pasos para detectar qué peticiones consiguen las credenciales NULAS enviadas y descubre qué URL o agente de usuario está enviando las credenciales inválidas y las exime de la autenticación.

Exención del URL de la autenticación

Para prevenir esta petición que hace al sustituto falso ser creado, el URL tiene que ser eximido de la autenticación. O, en vez de eximir el URL de la autenticación, usted puede ser que decida eximir la aplicación que enviaba la petición sí mismo de la autenticación, aseegurandose conseguir cualquier pedido la aplicación de ser eximido de la autenticación. Esto es posible agregando el agente de usuario que se abrirá una sesión los accesslogs agregando el **%u** adicional del parámetro en los **campos de encargo** opcionales en la suscripción del accesslog WSA. Después de identificar el agente de usuario, tiene que ser eximida de la autenticación.