Por que são os nomes de máquina do computador ou os nomes de usuário NULOS accesslogs entrados?

Índice

Pergunta

- Por que são os nomes de máquina do computador ou os nomes de usuário NULOS accesslogs entrados?
- Como você identifica os pedidos usando a estação de trabalho ou credenciais NULAS para uma isenção mais atrasada da autenticação?

Ambiente

- Ferramenta de segurança da Web de Cisco (WSA) - todas as versões
- Método de autenticação NTLMSSP com substitutos IP
- Windows Vista e sistemas mais novos da operação de Microsoft do desktop e do móbil

Sintomas

O WSA obstrui pedidos de alguns usuários ou comporta-se inesperadamente.
Os accesslogs mostram nomes de máquina do computador ou username e domínio NULOS em vez dos userIDs.

A edição resolve-se em seguida:

- Os substitutos cronometram para fora (o valor padrão para o intervalo substituto é 60 minutos)
- Reiniciando o processo do proxy (comando CLI > *diagnóstico* > *proxy* > *retrocesso*)
- Esconderijo de nivelamento da autenticação (comando CLI > *authcache* > *flushall*)

Informações de Apoio

Nas versões recentes do sistema operacional Microsoft, não se exige que um usuário real está

entrado anymore para que os aplicativos enviem pedidos ao Internet anymore. Quando aqueles pedidos são recebidos pelo WSA e pedidos autenticar, nenhuma credenciais do usuário está disponível para usar-se para a autenticação pela estação de trabalho cliente que pelo contrário pode tomar o nome de máquina do computador para um substituto.

O WSA tomará o nome de máquina fornecido e enviá-lo-á ao diretório ativo (AD) que o valida.

Com uma autenticação válida, o WSA cria um substituto IP que liga o nome da estação de trabalho da máquina ao endereço IP de Um ou Mais Servidores Cisco ICM NT da estação de trabalho. Uns pedidos mais adicionais que vêm do mesmo IP usarão o nome do substituto e assim da estação de trabalho.

Com o nome da estação de trabalho que não é membro de qualquer grupo AD, os pedidos não podem provocar a política de acesso prevista e assim ser obstruídos. O problema persiste até que o substituto cronometre para fora e a autenticação tiver que ser renovada. Esta vez, com um usuário real entrado e as credenciais do usuário válido disponíveis, um substituto novo IP será criado com esta informação e mais os pedidos combinarão a política de acesso prevista.

Uma outra encenação considerada é quando os aplicativos enviam credenciais inválidas (username NULO e domínio NULO) e credenciais inválidas da máquina. Isto é considerado uma falha de autenticação e será obstruído ou se as políticas do convidado são permitidas, o AUTH falhado é considerado como um “convidado”.

O nome da estação de trabalho termina com **$** seguido por **@DOMAIN** que faz nomes da estação de trabalho fáceis seguir usando o **grep do** comando CLI nos accesslogs para **$@**. Veja o exemplo abaixo para o esclarecimento.

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

A linha acima mostra um exemplo de um substituto IP já que está sendo criado para o endereço IP 10.20.30.40 e o nome de máquina **gb0000d01 $.**

A fim encontrar o pedido que enviou o nome de máquina, a primeira ocorrência do nome da estação de trabalho para o endereço IP de Um ou Mais Servidores Cisco ICM NT específico tem que ser identificada. O seguinte comando CLI realiza este:

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

Procure o resultado pela primeira ocorrência do nome da estação de trabalho. Os três primeiros pedidos são reconhecidos geralmente como um NTLM Único-Pecado-no aperto de mão (NTLMSSP/NTLMSSP) como descritos aqui e mostrados no exemplo abaixo:

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

Ao pesquisar defeitos, assegure-se de que estes pedidos do thee sejam para a mesma URL e estejam entrados muito um intervalo de curto período de tempo que indicatiting que é um aperto de mão automatizado NTLMSSP.

No exemplo acima, os pedidos de precedência são registrados com o código 407 da resposta HTTP (autenticação de proxy exigida) para pedidos explícitos, quando os pedidos transparentes seriam registrados com o código 401 da resposta HTTP (não-autenticado).

Há uns novos recursos disponíveis em AsyncOS 7.5.0 e mais alto onde você pode definir um intervalo substituto diferente para credenciais da máquina. Pode ser configurado usando o comando seguinte:

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

Você pode usar as mesmas etapas para detectar que pedidos obtêm as credenciais NULAS enviadas e descobre que URL ou agente de usuário está enviando as credenciais inválidas e isenta-as da autenticação.

Isentando a URL da autenticação

A fim impedir este pedido que faz com que o substituto falso seja criado, a URL tem que ser isentada da autenticação. Ou, em vez de isentar a URL da autenticação, você pôde decidir isentar o aplicativo que envia o pedido próprio da autenticação, certificando-se obter todos os pedidos para que o aplicativo seja isentado da autenticação. Isto é possível adicionando o agente de usuário a ser entrado os accesslogs adicionando o **%u** adicional do parâmetro nos **campos feitos sob encomenda** opcionais na assinatura do accesslog do WSA. Após ter identificado o agente de usuário, tem que ser isentado da autenticação.