Pourquoi les noms d'ordinateurs ou les noms d'utilisateurs NULL sont-ils connectés aux journaux d'accès ?

Contenu

Question

- Pourquoi les noms d'ordinateurs ou les noms d'utilisateurs NULL sont-ils connectés aux journaux d'accès ?
- Comment identifiez-vous les demandes à l'aide d'informations d'identification NULL ou de station de travail pour une exemption d'authentification ultérieure ?

Environnement

- Cisco Web Security Appliance (WSA) - toutes les versions
- Schéma d'authentification NTLMSSP avec substitution IP
- Windows Vista et les nouveaux systèmes d'exploitation Microsoft pour PC de bureau et mobile

Symptômes

Le WSA bloque les requêtes de certains utilisateurs ou se comporte de manière inattendue. Les journaux d'accès affichent les noms des ordinateurs ou les noms d'utilisateur et de domaine NULL au lieu des ID utilisateur.

Le problème se résout après :

- Délai d'expiration des substitutions (la valeur par défaut du délai d'expiration des substitutions est de 60 minutes)
- Redémarrage du processus proxy (commande CLI > *diagnostic* > *proxy* > *kick*)
- Vidage du cache d'authentification (commande CLI > *authcache* > *flushall*)

Informations générales

Dans les versions récentes de Microsoft Operating System, il n'est plus nécessaire qu'un utilisateur réel soit connecté pour que les applications puissent envoyer des requêtes vers Internet. Lorsque ces requêtes sont reçues par l'appareil de sécurité Web et qu'elles sont requises pour s'authentifier, aucune information d'identification utilisateur n'est disponible pour l'authentification par la station de travail cliente qui peut prendre le nom de l'ordinateur pour remplacer le nom de l'ordinateur.

Le WSA prend le nom de l'ordinateur fourni et le transmet à Active Directory (AD) qui le valide.

Avec une authentification valide, le WSA crée une substitution IP liant le nom de la station de travail de l'ordinateur à l'adresse IP de la station de travail. D'autres requêtes provenant de la même adresse IP utiliseront le nom de la station de travail de substitution et, par conséquent, le nom de la station de travail.

Comme le nom de la station de travail n'est membre d'aucun groupe AD, les requêtes ne peuvent pas déclencher la stratégie d'accès attendue et donc être bloquées. Le problème persiste jusqu'à ce que la substitution expire et que l'authentification doive être renouvelée. Cette fois, avec un utilisateur réel connecté et des informations d'identification valides disponibles, une nouvelle substitution IP sera créée avec ces informations et d'autres demandes correspondront à la stratégie d'accès attendue.

Un autre scénario apparaît lorsque les applications envoient des informations d'identification non valides (nom d'utilisateur NULL et domaine NULL) et des informations d'identification d'ordinateur NON valides. Ceci est considéré comme un échec d'authentification et sera bloqué ou si les stratégies d'invité sont activées, l'authentification échouée est considérée comme un « invité ».

Le nom de la station de travail se termine par un **$** suivi de **@DOMAIN** qui facilite le suivi des noms de stations de travail en utilisant la commande CLI **grep** sur les journaux d'accès pour **$@**. Voir l'exemple ci-dessous pour plus de précisions.

```
> 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 ligne ci-dessus montre un exemple de substitution IP déjà créé pour l'adresse IP 10.20.30.40 et le nom de la machine **gb0000d01$.**

Pour trouver la demande qui a envoyé le nom de la machine, la première occurrence du nom de la station de travail pour l'adresse IP spécifique doit être identifiée. La commande CLI suivante permet de réaliser ceci :

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

Recherchez le résultat de la première occurrence du nom de la station de travail. Les trois premières demandes sont généralement reconnues comme une connexion NTLM à connexion unique (NTLMSSP/NTLMSSP), comme décrit ici et illustré dans l'exemple ci-dessous :

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

Lors du dépannage, assurez-vous que ces requêtes portent sur la même URL et sont enregistrées dans un intervalle de temps très court indiquant qu'il s'agit d'une connexion NTLMSSP automatisée.

Dans l'exemple ci-dessus, les requêtes précédentes sont enregistrées avec le code de réponse HTTP 407 (Authentification proxy requise) pour les requêtes explicites, tandis que les requêtes transparentes sont enregistrées avec le code de réponse HTTP 401 (Non authentifié).

Il existe une nouvelle fonctionnalité disponible sur AsyncOS 7.5.0 et versions ultérieures où vous pouvez définir un délai d'expiration de substitution différent pour les informations d'identification de l'ordinateur. Il peut être configuré à l'aide de la commande suivante :

```
> 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]>.
```

Vous pouvez utiliser les mêmes étapes pour détecter les demandes qui reçoivent les informations d'identification NULL envoyées et découvrir l'URL ou l'agent utilisateur qui envoient les informations d'identification non valides et les exempter de l'authentification.

Exonération de l'URL de l'authentification

Afin d'éviter que cette requête ne provoque la création de la fausse substitution, l'URL doit être exemptée de l'authentification.Ou, au lieu d'exempter l'URL de l'authentification, vous pouvez décider d'exempter l'application qui envoie la requête elle-même de l'authentification, en veillant à obtenir toutes les demandes pour que l'application soit exemptée de l'authentification. Cela est possible en ajoutant l'Agent utilisateur à connecter aux journaux d'accès en ajoutant le paramètre supplémentaire **%u** dans les **champs personnalisés** facultatifs dans l'abonnement au journal d'accès WSA. Après avoir identifié l'agent utilisateur, il doit être exempté de l'authentification.