Pourquoi les noms d'ordinateur d'ordinateur ou les noms d'utilisateur NULS des accesslogs sont-ils ouverts une session ?

Contenu

Question

- Pourquoi les noms d'ordinateur d'ordinateur ou les noms d'utilisateur NULS des accesslogs sont-ils ouverts une session ?
- Comment identifiez-vous les demandes utilisant le poste de travail ou les qualifications de NULL pour l'exemption postérieure d'authentification ?

Environnement

- Appliance de sécurité Web de Cisco (WSA) - toutes les versions
- Modèle d'authentification NTLMSSP avec des substituts IP
- Windows Vista et plus nouveaux systèmes d'exploitation de Microsoft d'appareil de bureau et de mobile

Symptômes

Le WSA bloque des demandes de quelques utilisateurs ou se comporte inopinément.
Les accesslogs affiche des noms d'ordinateur d'ordinateur ou nom d'utilisateur et domaine NULS au lieu des IDs utilisateurs.

La question se résout ensuite :

- Les substituts chronomètrent (la valeur par défaut pour le délai d'attente de remplacement est de 60 minutes)
- Redémarrant le processus de proxy (*diagnostic* > *proxy* > *coup-de-pied de* command> CLI)
- Cache vidant d'authentification (*authcache* > *flushall de* command> CLI)

Informations générales

Dans des versions récentes de système d'exploitation de Microsoft, on ne l'exige pas qu'un utilisateur réel est ouvert une session désormais pour que des applications envoient des demandes à l'Internet plus. Quand ces demandes sont reçues par le WSA et sont demandées d'authentifier, aucun identifiant utilisateur n'est disponible pour l'utiliser pour l'authentification par le poste de travail de client qui à la place peut prendre le nom d'ordinateur de l'ordinateur pour une substitution.

Le WSA prendra le nom d'ordinateur fourni et lui fera suivre le Répertoire actif (AD) qui le valide.

Avec une authentification valide, le WSA crée un substitut IP liant le nom du poste de travail de l'ordinateur à l'adresse IP du poste de travail. D'autres demandes provenant le même IP utiliseront le nom de substitut et ainsi de poste de travail.

Avec le nom de poste de travail n'étant pas membre de tout groupe d'AD, des demandes ne peuvent déclencher la stratégie prévue d'Access et être bloquées ainsi. Le problème persiste jusqu'à ce que le substitut ait chronométré et l'authentification doit être renouvelée. Cette fois, avec un utilisateur réel ouvert une session et les identifiants utilisateurs valides disponibles, un nouveau substitut IP sera créé avec ces informations et plus loin les demandes apparieront la stratégie prévue d'Access.

Un autre scénario vu est quand les applications envoient les qualifications non valides (nom d'utilisateur et domaine NULS de NULL) et les qualifications non valides d'ordinateur. Ceci est considéré un échec d'authentification et sera bloqué ou si des stratégies d'invité sont activées, l'authentique défectueux est considéré en tant que « invité ».

Le nom de poste de travail finit avec un **$** suivi de **@DOMAIN** qui rend des noms de poste de travail faciles à tracer à l'aide du **grep de** commande CLI sur les accesslogs pour **$@**. Voyez l'exemple ci-dessous pour la clarification.

```
> 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 affiche un exemple d'un substitut IP ayant été déjà créé pour l'adresse IP 10.20.30.40 et le nom d'ordinateur **gb0000d01 $.**

Afin de trouver la demande qui a envoyé le nom d'ordinateur, la première occurrence du nom de poste de travail pour l'adresse IP spécifique doivent être identifiées. La commande suivante CLI accomplit ceci :

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

Recherchez le résultat pour la première occurrence du nom de poste de travail. Les trois premières demandes sont généralement identifiées comme NTLM Simple-Péché-sur la prise de contact (NTLMSSP/NTLMSSP) comme décrit ici et affichées 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,-,"-","-"> -
```

Le pour le dépannage, s'assurent que ces demandes de thee sont pour le même URL et sont ouvertes une session très un intervalle de courte durée indicatiting que c'est une prise de contact automatisée NTLMSSP.

Dans l'exemple ci-dessus, les demandes précédentes sont enregistré avec le code 407 (authentification de proxy de réponse de HTTP requise) pour des demandes explicites, alors que les demandes transparentes sont enregistré avec le code 401 de réponse de HTTP (Unauthenticated).

Il y a une nouvelle caractéristique disponible sur AsyncOS 7.5.0 et plus élevé où vous pouvez définir un délai d'attente de remplacement différent pour des qualifications d'ordinateur. Il peut être configuré utilisant la commande suivante :

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

Vous pouvez employer les mêmes étapes pour détecter que les demandes obtiennent les qualifications NULLES envoyées et les découvrez que l'agent URL ou d'utilisateur envoient aux qualifications non valides et exemptez de l'authentification.

Exemption de l'URL de l'authentification

Afin d'empêcher cette demande causant le substitut faux d'être créé, l'URL doit être exempté de l'authentification. Ou, au lieu d'exempter l'URL de l'authentification, vous pourriez décider d'exempter l'application envoyant la demande elle-même de l'authentification, veillant à obtenir toutes les demandes de l'application d'être exempté de l'authentification. C'est possible en ajoutant l'agent d'utilisateur à ouvrir une session les accesslogs en ajoutant le paramètre supplémentaire **%u** dans les **domaines faits sur commande** facultatifs dans l'abonnement de l'accesslog du WSA. Après avoir identifié l'agent d'utilisateur, il doit être exempté de l'authentification.