Authentique échoue par WSA quand le client utilise NEGOEXTS

Contenu

Introduction

Ce document décrit comment à l'overocme la question si authentique échoue par l'appliance de sécurité Web de Cisco (WSA) quand le client utilise NEGOEXTS.

Informations générales

L'appliance de sécurité Web de Cisco (WSA) peut authentifier des utilisateurs pour appliquer des stratégies basées sur l'utilisateur ou le groupe. Une des méthodes qui est disponible est Kerberos. En utilisant le Kerberos comme méthode d'authentification dans une identité, le WSA répond à la demande de HTTP d'un client avec des 401 (transparents) ou la réponse de HTTP 407 (explicite) qui contient l'en-tête WWW-**authentifient : Négociez**. En ce moment, le client envoie une nouvelle demande de HTTP avec l'**autorisation : Négociez l'**en-tête, qui contient l'interface de programmation générique de service de sécurité (GSS-API) et des protocoles protégés simples de la négociation (SPNEGO). Sous SPNEGO, l'utilisateur présente les **mechTypes** qu'il prend en charge. Ce sont les mechTypes que WSA prend en charge :

- KRB5- la méthode authentique de Kerberos qui est utilisée si le Kerberos est pris en charge et configuré correctement sur le client et si un ticket Kerberos valide est présente pour le service étant accédé à
- NTLMSSP- le fournisseur de support de Sécurité de Microsoft NTLM que la méthode qui est utilisé si aucun ticket Kerberos valide n'est disponible mais négocie la méthode authentique est pris en charge

Problème : Authentique échoue par WSA quand le client utilise NEGOEXTS

Dans des versions plus récentes de Microsoft Windows, une nouvelle méthode authentique est prise en charge a appelé NegoExts, qui est une extension au protocole d'authentification de négociation. Ce mechType est considéré plus sécurisés que NTLMSSP, et est préféré par le client quand les seules méthodes prises en charge sont NEGOEXTS et NTLMSSP. Plus d'informations peuvent être trouvées dans ce lien :

Introduire des extensions au module d'authentification de négociation

Ce scénario se produit typiquement quand la méthode authentique de négociation est sélectionnée et il n'y a aucun mechType KRB5 (très probablement dû à manquer un ticket Kerberos valide pour le service WSA). Si le client sélectionne NEGOEXTS (peut être vu comme NEGOEX dans le wireshark), alors le WSA unabled pour traiter la transaction authentique et authentique échoue pour le client. Quand ceci se produit, ces logs sont vus dans les logs authentiques :

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP
packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

Si authentique échoue, ceci se produit :

Si des privilèges d'invité sont activés - le client est classifié en tant qu'**Unauthenticated** et réorienté au site Web

Si des privilèges d'invité sont désactivés - le client est présenté avec des 401 ou des 407 différents (selon la méthode de proxy) avec les méthodes authentiques restantes présentées dans l'en-tête de réponse (Negotiate n'est pas présentée de nouveau). Une demande authentique est susceptible d'être produite si NTLMSSP et/ou authentique de base est configuré. S'il n'y a de pas autres méthodes authentiques (l'identité est configurée seulement pour le Kerberos), alors authentique échoue simplement.

Solution

La solution à cette question est à ou retirent le Kerberos authentique de l'identité - ou réparent le client de sorte qu'elle obtienne un ticket Kerberos valide pour le service WSA.