

eoale-wpad - Tâche #13382

Scénario # 13736 (Terminé (Sprint)): Gestion des sites déclarés en exception d'authentification avec cNTLM

Problème d'accès à la DMZ à travers cNTLM depuis un réseau des postes clients

06/10/2015 11:43 - Fabrice Barconnière

Statut:	Fermé	Début:	05/01/2016
Priorité:	Normal	Echéance:	
Assigné à:	Emmanuel GARETTE	% réalisé:	100%
Version cible:	sprint 2016 01-03 - Equipe MENESR	Temps estimé:	3.00 heures
		Temps passé:	3.50 heures

Description

En utilisant cNTLM il n'est pas possible d'accéder aux services HTTP de la DMZ depuis un poste admin ou péda.

Test avec 4 machines :

- Un poste **etb1.pcprofs-7** intégré au domaine utilisant le proxy **10.1.2.1:3128**
- Un poste **etb1.pcprofs-xubuntu** non intégré au domaine utilisant la détection de proxy automatique (cNTLM sur **10.1.2.1:3127**)
- Un poste **etb1.pcadmin-7** intégré au domaine utilisant le proxy **10.1.1.1:3128**
- Un poste **etb1.pcadmin-xubuntu** non intégré au domaine utilisant la détection de proxy automatique (cNTLM sur **10.1.1.1:3127**)

Tableau récapitulatif des tests :

	etb1.pcprofs-7	etb1.pcprofs-xubuntu	etb1.pcadmin-7	etb1.pcadmin-xubuntu
https://etb1.ac-test.fr:4203	☐	☐	☐	☐
https://192.168.0.31:4203	☐	☐	☐	☐
https://scribe.etb1.lan:4200	☐		☐	
https://10.1.3.5:4200	☐		☐	

Révisions associées

Révision 36239f09 - 07/01/2016 15:34 - Emmanuel GARETTE

ne pas passer par cNTLM pour les réseaux locaux (ref #13382 @2h)

Révision 547c52bb - 07/01/2016 15:56 - Emmanuel GARETTE

ne pas passer par cNTLM si l'authentification n'est pas activée sur l'interface (ref #13382 @1h)

Révision 30040b23 - 07/01/2016 15:58 - Emmanuel GARETTE

cache les variables activer_cntlm_eth si squid_auth_eth n'est pas activé sur l'interface (ref #13382)

Historique

#1 - 07/10/2015 11:03 - Scrum Master

- Tâche parente changé de #13367 à #13401

#2 - 08/10/2015 10:32 - Daniel Dehennin

Le problème ne se présente qu'avec le proxy cNTLM.

Voilà les seuls logs disponibles en essayant de se connecter à l'interface de sympa.

```
==> cntlm.debug.log <==
```

```
2015-10-08T10:19:29.199769+02:00 amon.etb1.lan cntlm[27049]: message repeated 2 times: [ 10.1.2.51 GET http://scribe.etb1.lan:8888/wws2]
```

```
==> e2guardian0.err.log <==  
2015-10-08T10:19:29.527353+02:00 amon.etb1.lan e2guardian0[1369]: NTLM - step 2 was not part of an auth handshake! (HTTP/1.1 200 OK#015)  
2015-10-08T10:19:29.528535+02:00 amon.etb1.lan e2guardian0[1369]: Auth plugin returned error code: -1
```

#3 - 08/10/2015 10:40 - Daniel Dehennin

- *Sujet changé de Correction SCRIBE-T03-007 2.5.1b2 à Impossible de se connecter à sympa à travers le proxy cNTLM (SCRIBE-T03-007 2.5.1b2)*

#4 - 08/10/2015 16:35 - Daniel Dehennin

- *Tâche parente #13401 supprimé*

#5 - 08/10/2015 16:46 - Daniel Dehennin

- *Tracker changé de Tâche à Scénario*

- *Sujet changé de Impossible de se connecter à sympa à travers le proxy cNTLM (SCRIBE-T03-007 2.5.1b2) à Problème d'accès à la DMZ à travers cNTLM depuis un réseau des postes clients*

- *Description mis à jour*

- *Version cible Sprint 2015 39-41 - Équipe MENESR supprimé*

- *Début 05/10/2015 supprimé*

Il apparaît que le réseau DMZ sur l'interface eth3 est exclu de l'authentification squid (eole-proxy:source:tmpl/common-squid1.conf@fdd03d2#L736)

```
root@amon:~# rgrep -F 'dst 10.1.3.0' /etc/squid3/  
/etc/squid3/common-squid1.conf:acl reseaueth3 dst 10.1.3.0/24  
root@amon:~# rgrep -F 'reseaueth3' /etc/squid3/  
/etc/squid3/common-squid1.conf:acl reseaueth3 dst 10.1.3.0/24  
/etc/squid3/common-squid1.conf:http_access allow reseaueth3
```

Comme tous les autres réseaux gérés par l'amon.

#6 - 08/10/2015 16:47 - Daniel Dehennin

- *Temps estimé 1.00 h supprimé*

#7 - 23/10/2015 16:53 - Emmanuel GARETTE

- *Tracker changé de Scénario à Tâche*

- *Temps estimé mis à 3.00 h*

- *Tâche parente mis à #13736*

#8 - 05/01/2016 17:41 - Emmanuel GARETTE

- Statut changé de Nouveau à En cours
- Assigné à mis à Emmanuel GARETTE
- Début mis à 05/01/2016

#9 - 07/01/2016 12:27 - Emmanuel GARETTE

De plus, l'authentification peut être géré que pour une interface (et pas la 2eme).

#10 - 07/01/2016 16:19 - Emmanuel GARETTE

- % réalisé changé de 0 à 100
- Restant à faire (heures) changé de 1.0 à 0.25

#11 - 08/01/2016 09:54 - Scrum Master

- Statut changé de En cours à Résolu

#12 - 21/01/2016 09:08 - Fabrice Barconnière

- Restant à faire (heures) changé de 0.25 à 0.0

Test sur poste admin hors domaine :

- Avec wpad : OK
- En forçant le proxy cNTLM : NOK (on le sait)
- Avec wpad en désactivant l'authentification Squid sur eth1 : OK, on passe bien par 3128 et la variable est cachée dans gen_config

#13 - 21/01/2016 09:54 - Scrum Master

- Statut changé de Résolu à Fermé