

Distribution EOLE - T che #36027

Sc nario # 35882 (Termin  (Sprint)): EOLE 2.10 : Erreur nf_conntrack_helper   l'instance du module Amon

 tude

24/06/2024 16:27 - Laurent Gourvenec

Statut:	Ferm�	D�but:	01/10/2022
Priorit�:	Normal	Ech�ance:	
Assign� �:	Laurent Gourvenec	% r�alis�:	100%
Version cible:	Livraison Cadol�s - MEN 30/06/2024 (60+18)	Temps estim�:	0.00 heure
		Temps pass�:	0.00 heure
Description			

R visions associ es

R vision 59e9c4b0 - 26/06/2024 11:47 - Laurent Gourvenec

Ajout de commentaires li s au suivi de connexions par netfilter

Ref #36027

Historique

#1 - 24/06/2024 16:35 - Laurent Gourvenec

Les tests Squash AM-T02-005a et AM-T02-005b devront  tre modifi s.

Le param tre nf_conntrack_helper a disparu depuis la version du noyau 6.0

netfilter: remove nf_conntrack_helper sysctl and modparam toggles

__nf_ct_try_assign_helper() remains in place but it now requires a template to configure the helper.

A toggle to disable automatic helper assignment was added by:

a9006892643a ("netfilter: nf_ct_helper: allow to disable automatic helper assignment")

in 2012 to address the issues described in "Secure use of iptables and connection tracking helpers". Automatic conntrack helper assignment was disabled by:

3bb398d925ec ("netfilter: nf_ct_helper: disable automatic helper assignment")

back in 2016.

This patch removes the sysctl and modparam toggles, users now have to rely on explicit conntrack helper configuration via ruleset.

- > Avant le noyau de 2012, la feature "conntrack helper" permettait de suivre les connexions pour certains protocoles afin de les rattacher (https://en.wikipedia.org/wiki/Netfilter#Connection_tracking_helpers)
- > En 2012, suite au document <https://home.regit.org/netfilter-en/secure-use-of-helpers/> une option a  t  ajout e pour d sactiver
- > En 2016, l'option a chang  de valeur par d faut pour d sactiver par d faut le helper.
- > En 2018, le pr c dent changement arrive dans EOLE -> demande pour inverser la valeur <https://dev-eole.ac-dijon.fr/issues/25554>
- > En 2022, l'option dispara t du noyau Linux
- > En 2024, le pr c dent changement arrive dans EOLE -> demande actuelle pour corriger un message d'erreur, mais en r alit  il y a la fonctionnalit    r parer (ou non ?).

Questions :

1. Est-ce qu'on veut mettre du connection tracking et si oui, pour quels protocoles ?

2. Comment tester ?

Réponses :

1. A priori, on veut mettre du connection tracking pour ftp et tftp là où era est déployé puisque ce sont les 2 modules insérés aujourd'hui sur Amon (nf_conntrack_tftp et nf_conntrack_ftp). Avec eole-proftpd, seulement ftp.
2. A confirmer, mais une connexion d'un client en ftp devrait afficher des paquets en "RELATED" que l'on doit pouvoir logger avec une règle iptables

De plus, je propose d'ajouter dans les règles statiques d'ERA

```
iptables -A PREROUTING -t raw -m rpfilter --invert -j DROP
```

pour un peu d'anti-spoofing.

De plus, je propose de renommer ip_conntrack_* par nf_conntrack_* (/lib/modules/5.4.0-189-generic/modules.alias)

#2 - 26/06/2024 14:14 - Laurent Gourvenec

- Statut changé de Nouveau à À valider
- % réalisé changé de 0 à 100

#3 - 04/07/2024 10:07 - Benjamin Bohard

- Statut changé de À valider à Résolu

#4 - 04/07/2024 15:28 - Joël Cuissinat

- Statut changé de Résolu à Fermé
- Restant à faire (heures) mis à 0.0