Distribution EOLE - Tâche #33540

Scénario # 33478 (Terminé (Sprint)): Rendre fonctionnel le paquet era-actions en 2.8

Tester

17/12/2021 16:07 - Matthieu Lamalle

Statut:	Fermé	**Début:**	02/12/2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	Prestation Cadoles MEN 2021 50-02	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 17/12/2021 16:07 - Matthieu Lamalle

installer era-action sur un etb1.amon
reconfigure
sur l'ead3, tester que les actions par-feu sont fonctionnelles

#2 - 20/12/2021 15:08 - Ludwig Seys

- Statut changé de Nouveau à En cours

#3 - 20/12/2021 15:39 - Ludwig Seys

- Assigné à mis à Ludwig Seys

- % réalisé changé de 0 à 40

installation du paquet era-actions
reconfigure
+ déconnexion & reconnexion sur l'EAD3 si déjà connecté avant l'installation ou le reconfigure.
- ajout de règle dans : règles de pare-feu volatiles, et validation du portage dans iptables
- dans Gérer les règles optionnelles activation/désactivation et validation des changements de :
- Interdiction des forums
- Interdire les connexions FTP
- Interdire l'utilisation des dialogues en direct
- Interdiction des protocoles de messagerie
- Internet restreint

#4 - 20/12/2021 15:45 - Ludwig Seys

- Fichier EAD3-regle-volatile.png ajouté

- % réalisé changé de 40 à 70

ajout de la règle (cf image), retrouvé dans iptables-save :
root@amon:~# iptables-save | grep 1200
-A FORWARD -s 192.168.200.0/32 -d 0.0.0.0/32 -p tcp -m state --state NEW -m tcp --dport 1200 --tcp-flags SYN,RST,ACK SYN -m comment --comment "iptablesvolatiles:1640011333.435942" -j ACCEPT

La suppression depuis EAD 3 entraîne bien la suppression dans iptables-save

#5 - 20/12/2021 16:00 - Ludwig Seys

- Statut changé de En cours à Résolu

- % réalisé changé de 70 à 100

ajout de l'interdiction des forums, s'applique bien sur le serveur. (même principe de test, activation depuis l'interface et validation avec les règles iptables)

un à un (activation/désactivation) :
interdiction des forums => OK
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 119 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de news, forums ..." -j DROP

Interdire les connexions FTP => OK
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 20:21 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: Interdire les connexions FTP" -j DROP

Interdire l'utilisation des dialogues en direct => OK

-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 517:518 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 1863 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 666 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 994 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 194 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 6665:6669 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de discussion en ligne (irc ...)" -j DROP

Interdiction des protocoles de messagerie => OK

-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 143 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 993 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 389 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 636 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 110 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 995 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 25 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP
-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --dport 465 --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : interdire les protocoles de messagerie (pop, imap ...)" -j DROP

Internet restreint => OK

-A ped-ext -i ens6 -o ens4 -p tcp -m state --state NEW -m tcp --tcp-flags SYN,RST,ACK SYN -m comment --comment "era: pedago -> exterieur : tout interdire (sauf le web via le proxy)" -j DROP
-A ped-ext -i ens6 -o ens4 -p udp -m state --state NEW -m udp -m comment --comment "era: pedago -> exterieur : tout interdire (sauf le web via le proxy)" -j DROP

Tous en même temps (activation/désactivation) => OK

temps d'application ~ 13 secondes

#6 - 06/01/2022 18:44 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

Vu

Fichiers

EAD3-regle-volatile.png	26,2 ko	20/12/2021	Ludwig Seys