Bloquer les principaux ports avec Kerio - créer une règle de filtrage

Date de dernière mise à jour : 27/06/2007 à 19:36

Source : http://www.vulgarisation-informatique.com/bloquer-ports.php.
Distribution interdite sans accord écrit d'Anthony ROSSETTO (http://www.vulgarisation-informatique.com/contact.php)

Nous allons créer une règle de filtrage avec **kerio** (vous pouvez apprendre à **configurer kerio** d'une manière générale ici : **configurer kerio**) pour bloquer les principaux ports pouvant servir à des attaques de pirates. Nous ne bloquerons dans notre exemple que le trafic entrant (requête d'une machine distante vers votre machine), mais vous pouvez très bien bloquer dans les deux sens (pas pour tous les ports cependant, ça dépend de l'utilisation de votre PC et des logiciels s'y trouvant).

Commencez par démarrer kerio, puis cliquez à gauche sur Sécurité du réseau.

-	Co	Configure		Internet		
cuité du réseau servorpison	Entrante	Sotanie	Enikarke	Sonanke	voun	
LSA Shell (Export Version)	× iefuser	🗶 refuser	X refuter	💡 dema		
cuité du mistèrie 📓 Application d'ouverture de session Windo	wsNT 🖌 autoni	🗙 refuser	× reiuser	🤋 dema		
Application d'ouverture de session Userini	i 🗸 autori	× refuter	X ieluter	? dema		
Generic Host Process for Win32 Services	🖌 🖌 Autori.	auton_	🖌 autori	🖌 aukon		
Microsoft File and Printer Sharing	🗙 refuser	× refuser	× refuser	🗙 refuser		
📴 Keiio Virtual Private Network	× refuser	? dema_	X refuter	X refuter		
🔐 Opera Internet Browsei	🦻 dema	🤗 dema	🦻 dema	🚽 autori		
Exetox	× refuser	🖌 auton	X refuser	🖌 aukon		
Mozilla Thundeibird	? dema.	🖌 sukos	? dema	🖌 aukon		
Internet Explorer	? dema.	🖌 aukoi	? dema	🖌 aukon	141	
Windows® installer	7 dema.	🖌 🖌 aukon	7 dema.	? dema.		
Kerio Personal Firewall 4 - GUI	🦻 dema.	🦻 dema	X refuser	🕴 dema		
EasyPHP Manager	💡 dema	🗸 auton	? dema	? dema_		
Kala apache	× refuser	🖌 autos_	X refuser	? dema		
Kok 😥 Lecteur Windows Media	🖌 autori.	× refuser	? dema	× refuser		
eMide	🖌 aukori.	🖌 autori	🖌 aukori	🖌 aukori		
K FTP Expert	🖌 aukom	🖌 🖌 auton	🖌 autori	🖌 aukon		
	sty 🤶 dema.	🖌 auton	? dema	💡 dema		
Java(TM) 2 Platform Standard Edition bina						

Cliquez ensuite sur le bouton intitulé Filtrage. Une nouvelle fenêtre s'ouvre :

Sécurité du réseau	- Filtrage de	paquets avan	cé				2	jla
	Règles	Groupes IP	1					
Nom du groupe	Description		Direction	Action	Jo.	AI_	Local	
Toutes les règles		ll n'y a aucu	n élément à af	licher dans cet	të vue.			4
Tetracosument								
Mooher								
Ajouter								
Inserer								
Suppone	<		1				×	
				Vulga	risatio	ntinfo	Baltai	he LCOI
			Aide	QK		Annuk	ar Ag	plique

Pour l'instant on constate qu'aucune règle de filtrage n'a été créée. Cliquez sur le bouton Ajouter.

Parcouni Ajouter Modifier
Ajouter
Ajouter Modifier
Ajouter Modifier
Modifier
Modifier
Supprime
Ajouter
Modilier
Supprime
Ajouter
Modifier
Supprime

Commencez par nommer votre règle. Ici je l'ai nommée **Blocage des principaux ports**. Nous allons bloquer des ports pour toutes les applications les utilisant, donc choisissez **any** dans la liste **Application**. Vous pouvez enregistrer les actions sur les futurs ports bloqués dans un fichier log en cochant la case **Journaliser**.

Nous allons maintenant bloquer les actions entrantes sur les ports suivants :

-Port 21 (correspondant au FTP)
-Port 23 (Telnet)
-Port 80 (HTTP)
-Port 135 (Pouvant être utilisé par des pirates)
-Port 139 (NetBios, utilisé pour le partage de fichiers entre réseaux)
-Port 443 (HTTPS)
-Port 445 (Pouvant lui aussi être utilisé par des pirates)

Dans la zone Direction, choisissez Entrant, et dans la zone Action choisissez Refuser. Cliquez ensuite dans la zone Local, cliquez sur le bouton Ajouter, puis sur Ajouter un port.

Nom:		-		
Numéro:	135	-		
Description	Port 135			
		Vulgarisati	on-infor	matique.co

Dans la zone **Numéro**, ajoutez le numéro du port et cliquez sur **Ok**. Répétez l'opération pour tous les ports de la liste (ainsi que d'autres ports si vous le souhaitez).

Cliquez ensuite deux fois sur Ok. Vos ports sont désormais bloqués contre toute tentative d'intrusion.

Source : http://www.vulgarisation-informatique.com/bloquer-ports.php. Distribution interdite sans accord écrit d'Anthony ROSSETTO (http://www.vulgarisation-informatique.com/contact.php)