

Guide d'utilisateur
Prewikka version Libre

Écrit par Sébastien Tricaud <s.tricaud@inl.fr>

Présentation

Prewikka est l'interface graphique du système de détection et prévention d'intrusions hybride Prelude IDS.

Cette interface permet de visualiser les alertes, que un ou plusieurs concentrateurs Prelude ("prelude-manager") ont stocké en base de données, de façon conviviale.

Lorsque vous vous connectez sur l'interface, vous pouvez voir quelque chose de similaire à ceci :

The screenshot shows the Prewikka Prelude console interface. At the top, it displays 'Prewikka company Ltd.' and 'Prelude console'. Below this, there are tabs for 'Alertes', 'Alertes de Corrélation', and 'Alertes d'outils'. The main area is a table of alerts with columns for 'Classification', 'Source', 'Destination', 'Sonde', and 'Temps'. The alerts are color-coded: red for high severity, orange for medium, green for low, and blue for information. A red circle '1' is placed in the center of the table area. On the left side, there is a sidebar with a menu containing 'Evénements', 'Agents', 'Paramètres', and 'A propos'. A red circle '2' is placed next to 'Evénements'. At the bottom left, there is a filter section with a 'Limite' field set to '50' and a 'Rafraichir' button. A red circle '3' is placed next to the '50' value. At the bottom, there are navigation buttons for 'préc', 'actual', and 'suiv', and a status bar showing '1 ... 8 (total:8)'.

Les règles de vos différents IDS sont visibles par couleur correspondant à la gravité de l'attaque :

- En rouge, les alertes correspondant aux attaques de niveau élevé
- En orange, les alertes correspondant aux attaques de niveau moyen
- En vert, les alertes correspondant aux attaques de niveau faible
- En bleu, les alertes correspondant à des informations

L'écran est aussi divisé en plusieurs parties : **(1)** Fenêtre de visualisation, **(2)** Menu et **(3)** Fenêtre de filtres.

Guide express : prise en main en 10mn top chrono

Objectif : Nous voulons afficher seulements 100 alertes provenant des sondes Snort, ayant une gravité élevée sur les 6 dernières heures.

Tout d'abord, rendez-vous dans le menu "Paramètres", vous tomberez sur une page ressemblant à :

The screenshot shows a web interface for managing filters. On the left is a sidebar with menu items: Evénements, Agents, Paramètres, and A propos. The main area has three tabs: Filtres (selected), Mon compte, and Utilisateurs. Under the 'Filtres' tab, there is a section titled 'Filtres disponibles' containing a search input field, a 'Charger' button, and an 'Effacer' button. Below this is an 'Edition' section. It contains two rows of filter definitions. Row A: 'alert.analyzer.model' followed by an equals sign, a dropdown arrow, and the value 'Snort'. Row B: 'alert.assessment.impact.severity' followed by an equals sign, a dropdown arrow, and the value 'high'. To the right of each row are minus and plus signs. Below the filter rows are three input fields: 'Formule : A AND B', 'Nom : Filtrage express', and 'Commentaire :'. An 'Enregistrer' button is located at the bottom right of the 'Edition' section.

Pour créer votre nouveau filtre, vous pouvez charger un filtre ancien, puis vous effectuez les modifications voulues et enregistrer votre filtre sous un autre nom.

Ou bien vous pouvez en créer un nouveau, depuis la fenêtre "Edition".

Dans notre cas, nous cherchons les sondes de type Snort. En langage IDMEF, qui est la langue utilisée par les analystes en détection d'intrusions, une sonde qui effectue l'opération de collecte + analyse s'appelle un **analyseur**.

Ainsi, bien que tout analyseur peut avoir un nom unique, le modèle reste identique.

Pour filtrer tous les modèles "Snort", il faut :

- définir le chemin IDMEF "alert.analyzer.model" pour qu'il corresponde strictement ("=") à la valeur "Snort".
- ajouter l'expression du filtre en cliquant sur "+" à droite de la valeur.

Ensuite, on rajoute l'indice de gravité "high" sur le chemin IDMEF "alert.assessment.impact.severity".

Il ne nous reste plus qu'à définir les relations entre les différentes expressions. Vous remarquez qu'à gauche de chaque expression, une lettre est associée. Nous

avons deux expressions, alors nous pouvons voir "A" pour la première puis "B" pour la deuxième.

Nous filtrons ainsi ces deux expressions en tapant "A AND B", le AND correspondant au ET liant la condition nécessitant les deux en même temps.

Pour enregistrer votre filtre, cliquez sur "Enregistrer".

Ensuite, revenez sur la page principale via le menu "Évènements" sur la fenêtre de filtres.

Dans le menu déroulant **Filtre**, choisir "Filtrage express" correspondant au nom du filtre que l'on a défini auparavant.

Ensuite, sur **Période** choisir 6 Heures.

Enfin, choisir une **Limite** de 100.

Vous pouvez maintenant soit **Appliquer** le filtre sur la vue actuelle, soit **Enregistrer** ce filtre afin de l'avoir comme vue par défaut.

Maintenant, il ne vous reste plus qu'à admirer le résultat :

Prewikka company Ltd.		Prelude console				
		Alertes		Alertes d'outils		admin le jeudi 06 décembre 2007 déconnexion
Évènements		Classification	Source	Destination	Sonde	Temps
Agents	3 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	14:46:32 - 14:46:22
Paramètres	3 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	14:46:32 - 14:46:22
A propos	3 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	14:46:31 - 14:46:23
	(INL rulesets) Violation de politique de securite				snort (Serveur IPS)	14:43:14
	(INL rulesets) Violation de politique de securite				snort (Serveur IPS)	14:22:48
	12 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:54 - 12:16:44
	18 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:54 - 12:16:44
	15 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:54 - 12:15:56
	21 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:53 - 12:16:41
	2 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:52
	15 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:51 - 12:15:49
	16 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:51 - 12:16:50
	12 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:51 - 12:15:49
	11 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:51 - 12:16:49
	17 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:50 - 12:15:30
	14 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:48 - 12:16:46
	8 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:48
	12 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:48
	21 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:48 - 12:16:38
	15 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:47 - 12:15:48
	8 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:46
	11 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:42 - 12:16:40
	28 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:41 - 12:16:29
	20 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:34 - 12:16:23
	14 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:30 - 12:16:29
	15 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:29 - 12:16:26
	17 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:29 - 12:15:31
	7 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:28 - 12:15:31
	7 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:27 - 12:15:57
	11 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:27 - 12:16:25
	8 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:27 - 12:16:26
	15 x (INL rulesets) Violation de politique de securite				snort (Serveur IPS)	12:16:27 - 12:15:36

La vue “Évènements”

Lorsque vous vous connectez à Prewikka, la vue “Évènements” est celle présentée par défaut.

Elle se présente sous forme d'un tableau de cinq colonnes avec à droite de chaque ligne une case à cocher, servant à supprimer l'alerte visualisée.

Chaque colonne exprime une donnée de l'alerte :

Classification

La classification présente le titre de l'alerte, avec une couleur définissant sa gravité.

Chaque classification est unique par rapport à un type d'alerte donné.

Chemin IDMEF du texte : *alert.classification.text*

Source

La source correspond à l'origine de l'attaque extrait de l'alerte, avec le port source ainsi que le protocole lorsque cela est indiqué.

Chemin IDMEF de l'adresse source : *alert.source.node.address.address*

Chemin IDMEF du port source : *alert.source.service.port*

Chemin IDMEF du protocole : *alert.source.service.protocol*

Destination

La destination correspond à la machine, l'utilisateur ou encore le processus ciblés par l'attaque.

Chemin IDMEF de l'adresse de destination : *alert.target.node.address.address*

Chemin IDMEF de l'utilisateur de destination : *alert.target.user.user_id.name*

Chemin IDMEF du processus de destination : *alert.target.process.name*

Sonde

La sonde correspond à l'origine de l'attaque qui est ensuite traité par l'analyseur. Cela correspond par exemple à sshd, si l'attaque vise un serveur ssh, lorsqu'elle est analysée par l'analyseur de log “Prelude LML”.

Chemin IDMEF de la classe de la sonde : *alert.analyzer.class*

Chemin IDMEF du modèle de la sonde : *alert.analyzer.model*

Temps

Le temps correspond à l'heure d'origine de l'alerte.

Chemin IDMEF de la détection de l'attaque : alert.detect_time

Chemin IDMEF de la création de l'alerte : alert.create_time

La vue "Agents"

Ce vue vous permet de visualiser le bon fonctionnement de vos sondes, trié par localisation géographique.

Effacer	Nom	Modèle	Version	Classe	Dernière pulsation	Status
<input type="checkbox"/>	prelude-lml	Prelude LML	0.9.10.1	Log Analyzer	2007-12-06 17:02:57 +01:00	Connecté
<input type="checkbox"/>	prelude-manager	Prelude Manager	0.9.10	Concentrator	2007-12-06 17:05:37 +01:00	Connecté
<input type="checkbox"/>	snort	Snort	2.6.1.5	NIDS	2007-12-06 17:03:52 +01:00	Connecté

L'interface permet aussi d'effacer une ou plusieurs sondes.

La vue "Paramètres"

C'est à l'aide de la vue paramètres que vous allez pouvoir définir vos filtres, ainsi que gérer votre compte et ceux de vos utilisateurs.

Nous avons déjà eu l'occasion de voir le fonctionnement des filtres lors que la prise en main expresse de Prewikka.

Identifiant : admin

Langue : Français

Permissions :

- IDMEF_VIEW
- IDMEF_ALTER
- USER_MANAGEMENT
- COMMAND
- INTRUSIVE_COMMAND

Cocher tout

Modifier le mot de passe

Mot de passe actuel :

Nouveau mot de passe :

Confirmation du mot de passe :

Soumettre les modifications

La vue de votre compte courant permet de définir la langue, votre mot de passe, ainsi que les possibilités de gestion des alertes dans Prewikka.

Cette gestion est définie en 5 critères :

- IDMEF_VIEW : pour la visualisation d'alertes
- IDMEF_ALTER : pour modifier des valeurs
- USER_MANAGEMENT : pour ajouter/modifier/enlever des comptes
- COMMAND et INTRUSIVE_COMMAND sont des options de la version professionnelle de Prewikka.

Filtres	Mon compte	Utilisateurs				
Identifiant	IDMEF VIEW	IDMEF ALTER	USER MANAGEMENT	COMMAND	INTRUSIVE COMMAND	
admin	x	x	x	x	x	<input type="checkbox"/>
Créer un utilisateur			Effacer l'utilisateur			

La vue des utilisateurs, permet de facilement ajouter/modifier ou supprimer des comptes.