

Comment détecter les hackers sur votre serveur web

Attrapez les hackers la main dans le sac avec une surveillance en temps réel des journaux d'évènements de sécurité

Ce document parle des différentes méthodes utilisées par les hackers pour attaquer des serveurs web IIS, et comment vous pouvez utiliser la surveillance de journaux sur votre serveur web et être alerté des attaques immédiatement.

Introduction

Cet article explique de quelle façon les administrateurs peuvent paramétrer leurs serveurs web avec succès et en toute sécurité. En décrivant les outils utilisés par les pirates informatiques pour s'introduire au sein de vos serveurs web IIS, ce livre blanc présente en détails les étapes nécessaires pour détecter les intrusions effectuées au sein de votre réseau. Il explique également comment empêcher de telles attaques de votre serveur web.

Introduction.....	2
Le piratage d'un serveur web est un jeu d'enfant	2
Outils des hackers.....	3
Détection d'intrusions en surveillant les fichiers systèmes clés.....	5
Comment détecter les hackers sur votre serveur	6
A propos de GFI LANguard Security Event Log Monitor (S.E.L.M.).....	12
A propos de GFI Software.....	13

Le piratage d'un serveur web est un jeu d'enfant

Les serveurs web Internet Information Services (IIS) sont très populaires dans les entreprises. Il y a plus de 6 millions d'installations dans le monde. Malheureusement, cela signifie aussi qu'ils constituent les cibles préférées des hackers. De ce fait, de nouveaux exploits émergents régulièrement qui mettent en danger l'intégrité et la stabilité de votre serveur web IIS.

Pour beaucoup d'administrateurs il est difficile de toujours avoir les derniers patches de sécurisation pour IIS et ainsi être protégé contre les nouveaux exploits qui facilitent l'accès aux vulnérabilités du serveur web pour les utilisateurs malicieux. Prendre avantage d'un exploit n'est pas difficile pour quiconque possède les bons outils – même un adolescent peut facilement attaquer ou contrôler votre serveur web, voir pénétrer votre réseau interne.

En d'autres termes, il n'est pas difficile d'avoir accès aux informations prioritaires d'une entreprise. Pire encore, les hackers ne sont pas nécessairement des adolescents à la recherche de grands frissons, comme on le pense : des employés mécontents et la compétition, par exemple, ont leurs propres raisons de vouloir pénétrer dans les zones confidentielles de votre réseau.

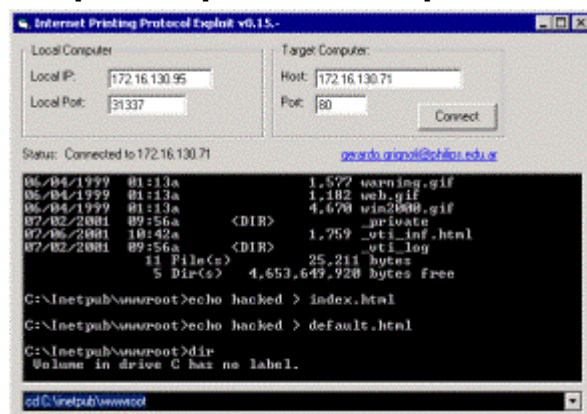
Quelques attaques sont reconnaissables sur le champ, et un petit nombre d'entre elles sont considérées assez importantes pour en faire part aux journaux. La plupart ne sont pas faciles à découvrir car beaucoup d'intrus préfèrent rester dans l'anonymat pour pouvoir utiliser le serveur web IIS qu'ils ont piraté comme une base pour d'autres attaques sur des serveurs bien plus grands ou plus populaires. A part le fait de mettre en danger l'intégrité de votre site, l'usage illicite de votre serveur peut vous rendre responsable des attaques lancées sur d'autres

compagnies.

Outils des hackers

Il existe plusieurs outils qui facilitent le travail des hackers désireux de modifier un site web. De tels outils sont faciles à utiliser et même une personne inexpérimentée en matière de piratage peut perturber un serveur web en un rien de temps

L'exploit du protocole d'impression Internet (IPP)



Exploit IPP facilité

Un programme qui utilise cet exploit est Internet Printing Protocol Exploit v.0.15 (voir l'image ci-dessus). Il se base sur le fameux code d'exploit dans un fichier programme dans le pilote C appelé « jill.c », qui a été rendu public par un hacker utilisant l'ancien « dark spyrit ».

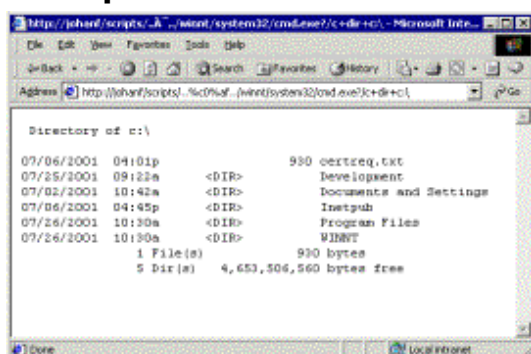
Cette application utilise une vulnérabilité du dépassement de mémoire tampon sur un serveur web ISS. Tout ce que les hackers ont besoin de faire est de taper le nom du serveur web cible (ou le nom d'un ordinateur avec ISS installé sur le serveur) et de cliquer sur « Connecter ».

Lors de la connexion, l'application envoie la chaîne actuelle qui dépasse le tampon, menant à l'exécution des codes personnalisés (qui est aussi connu sous le nom de shell code) et connectant le fichier cmd.exe au port spécifié du côté du hacker (le défaut étant 31337).

Cela permet de contourner les configurations traditionnelles des pare-feux et autres mesures sécuritaires du même genre.

Ensuite, le hacker reçoit une ligne de commandes et un accès au SYSTEME, à partir duquel il/elle peut mener un certain nombre d'activités qu'un administrateur n'aurait jamais autorisées, telles qu'avoir accès aux bases de données qui contiennent les détails de cartes de crédit et autres données confidentielles.

Les exploits UNICODE et CGI-Decode



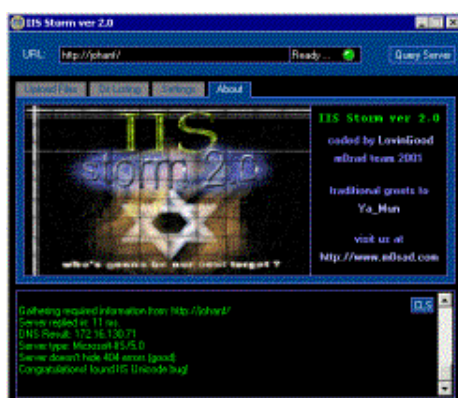
Exploit Unicode se servant d'Internet Explorer

Deux autres exploits préférés des hackers de sites web incluent les exploits UNICODE et CGI-Decode. Ici, le hacker peut simplement utiliser le navigateur même pour faire ce dont il a envie sur la machine cible qui exécute des versions IIS sans patch. On a juste besoin d'Internet Explorer et d'une « chaîne magique » pour faire ce que l'on veut sous un compte anonyme d'IIS. La capture d'écran ci-dessus montre un registre liste du disque C:\ du serveur IIS dans le navigateur web même. Cela est un exemple simple qui montre que le hacker peut avoir accès au disque dur de votre serveur web.

A la base, cet accès est limité aux droits d'utilisateur du compte anonyme du ISS (IUSR_nomordinateur). Une fois que le hacker obtient un accès anonyme, il peut facilement charger un fichier ASP, qui lui permet d'avoir un plus grand accès aux privilèges de SYSTEM. Une telle action lui donne un accès complet à l'ordinateur « envahi », ce qui signifie qu'il peut faire ce qu'il veut.

Applications sur mesure

Certains groupes d'intrusions de sites Internet préfèrent créer leurs propres applications pour automatiser le procédé de modification d'un site.



IIS Storm par M0sad

Un de ces groupes est M0sad, une unité de hackers Israéliens qui ont développé et lancé un utilitaire de piratage sous le nom de IIS Storm v.2. Voici un morceau extrait du manuel de IIS Storm : « IIS Storm est un utilitaire créé pour la Modification à Distance de Site Web (*Remote Web Site Defacement*) qui s'exécute sur IIS (*Internet Information Server [NT platform]*) et qui est aussi vulnérable à l'Exploit Unicode. »

De tels utilitaires donnent aux hackers débutants et confirmés de grandes possibilités de piratage. IIS Storm permet aussi aux utilisateurs de cacher leur adresse IP grâce à des proxies anonymes, et de facilement remplacer les fichiers du site web cible avec leurs propres pages HTML.

PoizonB0x, un autre groupe bien connu qui s'est autoproclamé « cyber-terroristes » et « guerriers du Net », a créé iisautoexp.pl, un utilitaire automatisé qui s'occupe de toutes les tâches nécessaires pour obtenir l'accès et performer des opérations de modifications.

De façon à modifier le site web, tout ce que les utilisateurs malicieux doivent faire est de donner le nom du site au script et de le lancer. Si le site est sensible aux attaques (c'est-à-dire, s'il ne possède pas les patches appropriés), la page de garde (index.htm, default.asp ou variations) devient « PoizonB0x Ownz YA ». De cette façon, les hackers créent un lot de fichiers avec les noms de leur sites web ciblés, produisant des modifications en masse des serveurs web IIS. Ce script peut être adapté et exécuté sur des machines Windows et UNIX.

Savoir que votre serveur web a été attaqué est simple si votre page web est modifiée. Cependant, plusieurs hackers préfèrent les attaques furtives et installent un cheval de Troie qui siphonnera les données ou qui s'adonnera à d'autres activités malicieuses. Ils font attention de ne pas laisser de traces de leurs intrusions.

Détection d'intrusions en surveillant les fichiers systèmes clés

Comment peut-on se protéger contre ce flot éventuel d'attaques ? Presque tous les outils d'exploits de serveurs IIS utilisent un ou plusieurs fichiers système. En contrôlant l'activité de ces fichiers en temps réel, un administrateur peut attraper un hacker la main dans le sac. Les fichiers système ci-dessous sont souvent utilisés par les outils des hackers :

1. cmd.exe: la ligne de commande d'émulation de programme dans Windows ; de là, les utilisateurs peuvent administrer le serveur.
2. ftp.exe: la ligne de commande client FTP disponible sur toutes les plateformes Windows ; les hackers l'utilisent pour obtenir les fichiers dont ils ont besoin sur la machine serveur à partir d'un serveur FTP distant.
3. net.exe: ce programme vous permet d'administrer la machine ; sous le compte système, les hackers peuvent utiliser cet outil pour créer des groupes et des utilisateurs backdoor, lancer et arrêter des services, accéder à d'autres machines sur le réseau, et bien plus.

4. ping.exe: ce programme envoie simplement un paquet écho ICMP aux hôtes distants ; les hackers peuvent utiliser votre serveur ainsi que d'autres serveurs vulnérable pour lancer ping contre un hôte cible, d'où la création d'un DDoS (Distributed Denial of Service attack) sur la cible.
5. tftp.exe: un client TFTP qui est aussi disponible sur toutes les machines Microsoft Windows ; certains hackers préfèrent utiliser ce tftp.exe pour récupérer les fichiers dont ils ont besoin pour s'introduire sur le serveur IIS.

Lorsqu'un pirate lance cmd.exe en utilisant l'exploit UNICODE, il est en fait lancé par le compte invité Internet (*Internet Guest Account*) (IUSR_nomdelamachine). Puisque cet utilisateur n'a aucune exécution dans ce fichier, une surveillance de journaux d'évènements de réseau telle que GFI LANguard S.E.L.M. peut journaliser tous les évènements pour lesquels ce compte lance cmd.exe. De cette façon, GFI LANguard S.E.L.M. informe immédiatement l'administrateur de l'intrusion.

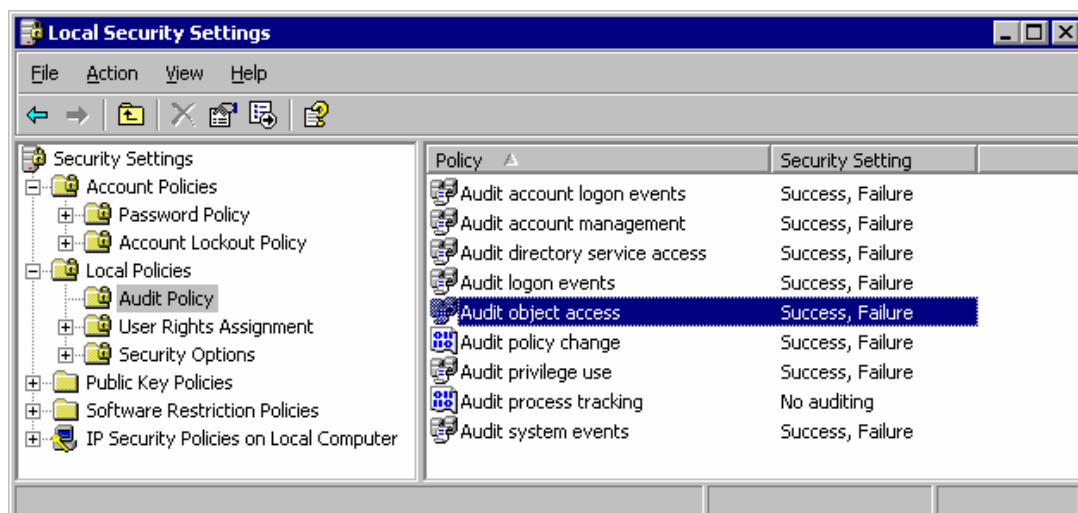
Les attaques du dépassement de mémoire tampon obtiennent le compte système à la place. Cela signifie qu'à partir de là l'utilisateur malicieux qui a déjà pénétré la machine peut prendre l'identité de n'importe quel autre utilisateur et faire tout ce dont le système d'exploitation est capable. Cependant, si GFI LANguard S.E.L.M. est paramétré pour surveiller cmd.exe et répertorier chaque accès du compte système à ce fichier, l'administrateur de réseau sera en mesure de détecter de telles activités – car pour prendre l'identité d'un autre utilisateur, les utilisateurs doivent utiliser la ligne de commande même.

Comment détecter les hackers sur votre serveur

Après examen des activités des intrus, les administrateurs peuvent configurer leurs serveurs et GFI LANguard S.E.L.M. de façon à ce qu'ils interceptent les hackers la main dans le sac.

Etape 1 : Configuration de votre serveur web à l'audit d'objets

Pour surveiller les fichiers souvent utilisés, l'audit d'objet doit être activé dans les serveurs web Windows.



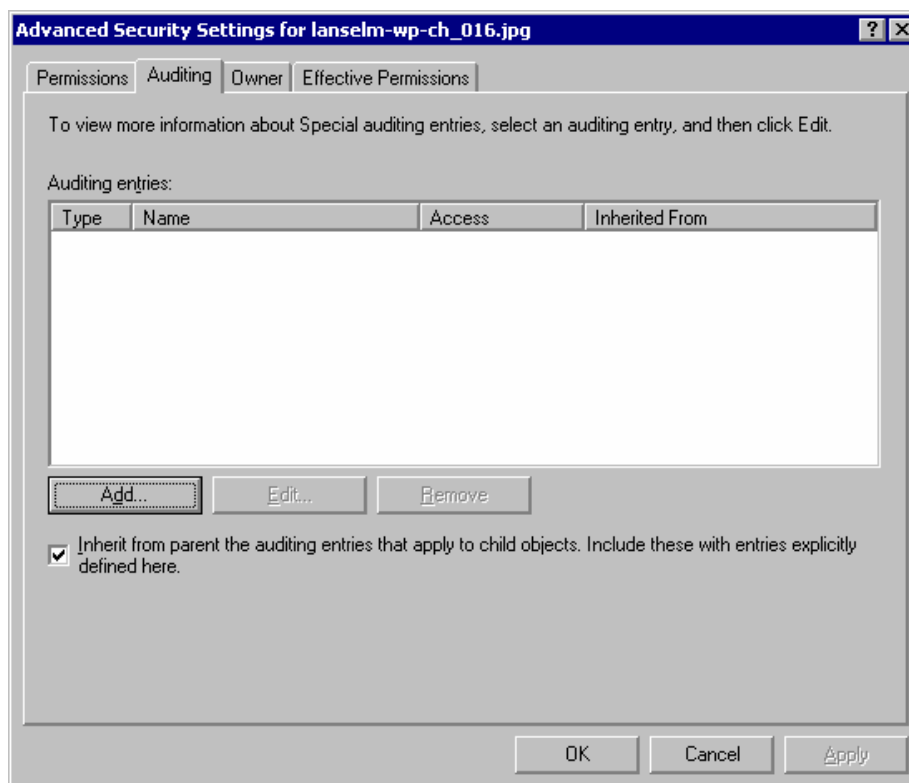
Audit Policy – accès à objet

Si le serveur web est autonome, pour activer l'audit d'objets vous devez : aller sur Outils d'administration – Stratégie de sécurité locale ;

2. sélectionner Stratégies Locales et Stratégies d'audit ;
3. cliquer double sur Auditer l'accès aux objets et Opération réussie et Echec.

Si le serveur web fait partie du domaine, vous devez activer l'audit d'objets comme une Stratégie de Domaine (à la place de Stratégies Locales). Cela se fait de la même façon, sous Outils d'administration – Stratégie de Sécurité de Domaine.

Ensuite, précisez les fichiers que vous voulez auditer. Dans le cas présent nous voulons auditer : cmd.exe, ftp.exe, net.exe, ping.exe et tftp.exe.

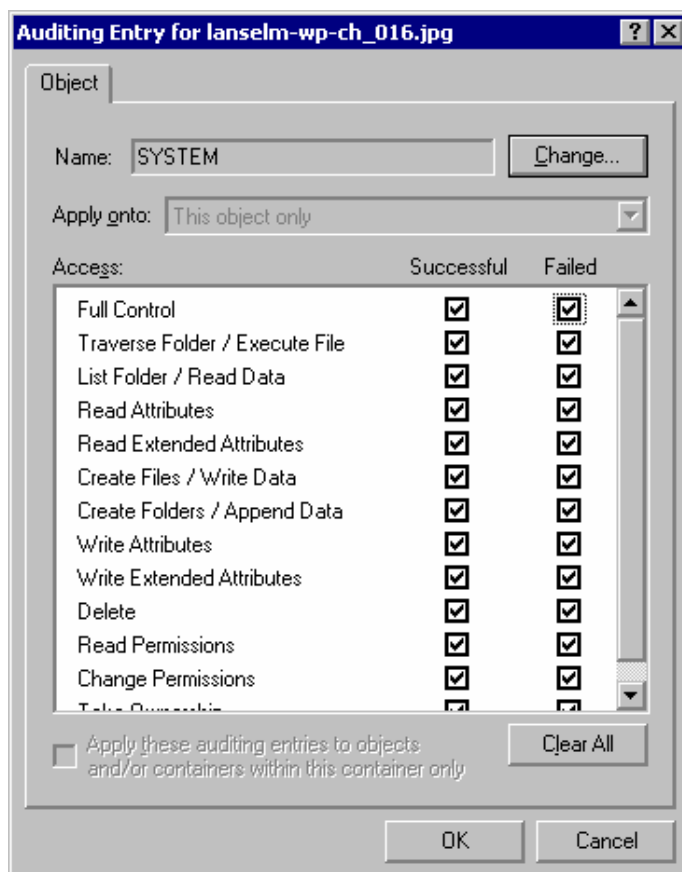


Onglet d'audit

Pour permettre à l'option « Auditer l'accès aux objets » d'enregistrer toutes les fois que le compte SYSTEME et le compte invité Internet lancent cmd.exe :

1. Cliquez droit sur cmd.exe et sélectionnez 'Propriétés'.
2. Sélectionnez l'onglet de sécurité et cliquez sur Avancé.
3. Sélectionnez l'onglet Auditer et cliquez sur Ajouter.
4. Vous pouvez maintenant saisir les utilisateurs à surveiller lorsqu'ils tentent d'accéder à l'Objet (cmd.exe) : sélectionnez le compte SYSTEME.
5. Pour un audit complet de cmd.exe / compte SYSTEME, choisissez toutes les options Réussite et Echec.
6. Cliquez sur OK, Ajouter et faites la même chose pour le compte IUSR.
7. Ce procédé doit être suivi aussi pour ftp.exe, net.exe, ping.exe, et tftp.exe.

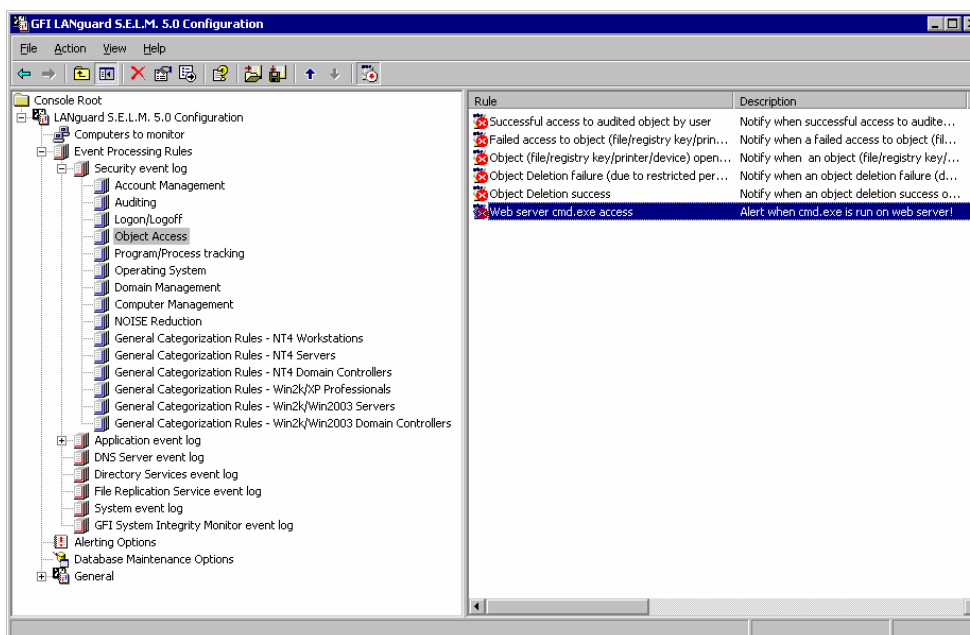
L'accès à ces fichiers par le compte Système ou IUSR sera désormais répertorié dans le journal d'évènements de sécurité.



Configuration de l'audit

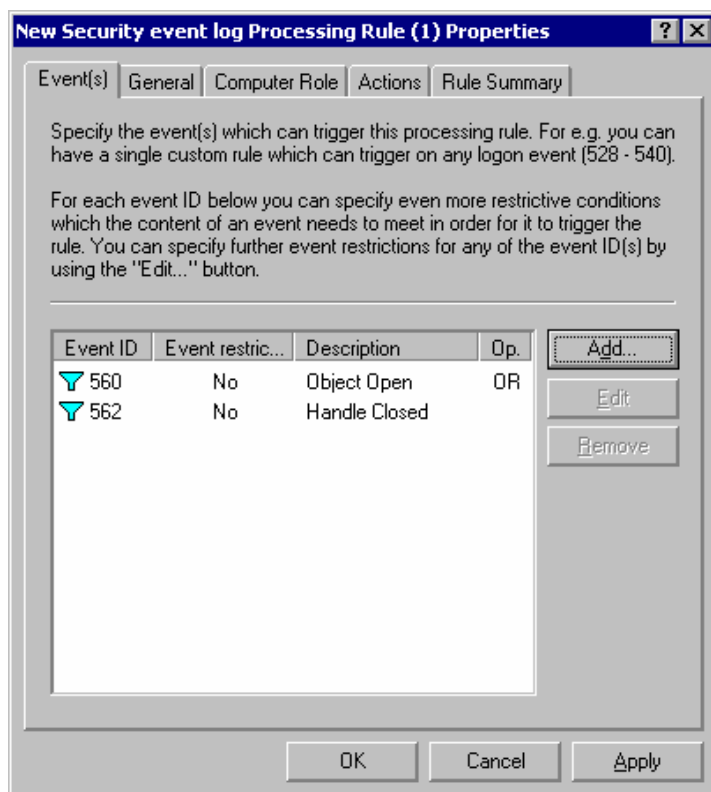
Etape 2 : Configuration de GFI LANguard S.E.L.M. pour la surveillance de ces évènements et alerter les administrateurs

Maintenant que vous avez configuré l'audit d'accès fichiers, vous devez configurer GFI LANguard S.E.L.M. pour qu'il détecte les évènements de sécurité suivants :



Console de configuration de GFI LANguard S.E.L.M.

1. Dans le panneau de configuration de GFI LANguard S.E.L.M., assurez-vous que le serveur web soit listé dans le nœud des ordinateurs à surveiller.
2. Allez sur le nœud Règles de traitement d'évènements > Journal d'évènement de Sécurité > Accéder Objet. Sélectionnez le nœud, cliquez droit et choisissez Nouveau > Règle de traitement.
3. Cliquez sur Ajouter, et ajoutez les évènements 560 et 562. Ils identifieront les intrusions. Evènement 560 : *Object Open* – signifie que l'objet a été atteint (par ex. cms.exe fut lancé), et Evènement 562 : *Handle Closed* – signifie que l'objet n'est plus en service (par ex. cmd.exe a été interrompu)
4. Par défaut, la règle sera appliquée à tous les ordinateurs surveillés par GFI LANguard SELM. Pour spécifier uniquement le nom du serveur web, allez sur l'onglet général et saisissez le nom de l'ordinateur serveur. Ajouter aussi une description claire.
5. Cliquez sur **OK** pour créer une règle.



Création d'une nouvelle règle d'accès objet

GFI LANguard S.E.L.M. surveillera ces événements sur votre serveur web, et si cmd.exe est lancé, il vous en avertira immédiatement.

Etape 3 : Evaluation de vos nouvelles ID

Une fois les configurations ci-dessus effectuées, vous pouvez les tester. Pour cela il faut créer un nouveau script ASP. Si vous avez correctement paramétré vos stratégies d'audit et activé l'accès objet sur les fichiers indiqués, ce script créera et déclenchera une règle d'audit d'objet. GFI LANguard S.E.L.M. récupèrera ensuite l'évènement généré à partir du journal d'évènements, et – puisqu'une règle identique existe – il enverra une alerte par email à l'administrateur pour l'avertir que cmd.exe a été activé.

Le script ci-dessous lance cmd.exe et crée une liste registre du C:\ en arrière plan. Vous pouvez placer ce fichier sur votre serveur IIS et essayer d'y avoir accès via le navigateur web.

```
<%@ Language=VBScript %>
<%' -----
' SELM_test.asp : Utilisé pour l'évaluation de Languard S.E.L.M.
Par : Sandro Gauci <Sandro@gfi.com>
' Co : GFI Software
```

```
'-----  
Dim oScript  
On Error Resume Next  
Set oScript = Server.CreateObject("WSCRIPT.SHELL")  
Appelez oScript.Run ("cmd.exe /c dir C:\", 0, True)  
%>  
<HTML>  
<BODY>  
GFI LANguard S.E.L.M. doit vous avoir envoyé une alerte  
</BODY>  
</HTML>
```

Ce script peut être téléchargé depuis : <ftp.gfi.com/testselm.zip>.

A propos de GFI LANguard Security Event Log Monitor (S.E.L.M.)

GFI LANguard Security Event Log Monitor (S.E.L.M) effectue une détection d'intrusion basée sur les journaux d'événements et le management de l'ensemble du réseau des journaux d'événements. GFI LANguard S.E.L.M. archive et analyse les journaux d'événements de toutes les machines réseau et vous alerte en temps réel des problèmes de sécurité, attaques et autres événements cruciaux. L'analyse intelligente de GFI LANguard S.E.L.M. signifie que l'on a pas besoin d'être un expert des événements pour être capable de : surveiller les utilisateurs tentant d'accéder aux fichiers et partages confidentiels et sécurisés, surveiller les serveurs cruciaux et créer des alertes pour des événements spécifiques et certaines conditions survenant sur votre réseau, créer un back-up et éliminer les journaux d'événements automatiquement sur des machines à distance, détecter des attaques grâce à des comptes d'utilisateurs locaux, et bien plus ! Pour de plus amples informations sur GFI LANguard S.E.L.M. et pour télécharger votre essai gratuit, veuillez visiter <http://www.gfsfrance.com/fr/lanselm/>.

A propos de GFI Software

GFI Software est l'un des leaders dans le domaine de la sécurité de réseau, de la sécurité du contenu et des logiciels de messagerie. Ses produits-clés comprennent le connecteur fax GFI FAXmaker for Exchange et serveur fax sur réseau ; GFI MailSecurity, vérification du contenu / d'exploits et antivirus ; GFI MailEssentials, progiciel anti-spam basé sur le serveur ; GFI LANguard Network Security Scanner (N.S.S.) qui vérifie la sécurité du réseau et permet aux administrateurs d'installer à distance les patchs et services packs ; GFI Network Server Monitor, qui envoie automatiquement des alertes et corrige les problèmes du réseau et des serveurs ; et GFI LANguard Security Event Log Monitor (S.E.L.M.) qui effectue une détection d'intrusion et une gestion de journaux d'événement sur l'ensemble du réseau ; et GFI LANguard Portable Storage Control qui permet de surveiller les média amovibles sur l'ensemble du réseau. Les clients de GFI Software comprennent Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, US IRS et USAF. GFI Software est installé aux Etats-Unis, au Royaume-Uni, en Allemagne, à Chypre, en Roumanie, en Australie et à Malte et opère par le biais d'un réseau mondial de distribution. GFI Software est un partenaire certifié Microsoft Gold et a remporté le titre de progiciel de l'année « Microsoft Fusion (GEM) Packaged Application Partner of the Year ». Pour plus d'information à propos de GFI, visitez <http://www.gfsfrance.com>.

© 2005 GFI Software Ltd. Tous droits réservés. L'information contenue dans ce document représente la position actuelle de GFI Software concernant les questions citées à la date de publication. GFI Software doit répondre à des conditions de marché variables, le présent document ne doit donc pas être interprété comme un engagement de la part de GFI Software, et GFI Software ne peut garantir la véracité des informations présentées après la date de publication. Ce document blanc est offert uniquement à titre d'information. GFI SOFTWARE NE PROCEDE A AUCUNE GARANTIE EXPRESSE OU IMPLICITE DANS LE PRESENT DOCUMENT. GFI Software, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity et le logo sont soit des marques commerciales ou des marques déposées de GFI Software Ltd. aux Etats-Unis et/ou ailleurs. Tous les noms de produits ou de sociétés cités dans la présente peuvent être les marques déposées de leurs propriétaires respectifs.

