
Het detecteren van hackers op uw webserver

Met realtime security event log monitoring kunt u hackers op heterdaad betrappen

Een discussie van de methoden die hackers gebruiken om IIS webserver aan te vallen, en hoe u event log monitoring op uw webserver kunt gebruiken om meteen op de hoogte te worden gebracht van succesvolle aanvallen

Inleiding

Dit white paper helpt netwerkbeheerders hun webserver te beveiligen. Er zal worden ingegaan op de methodes die hackers gebruiken om via de achterdeur uw IIS webserver binnen te komen, hoe u succesvolle inbraken op uw netwerk kunt detecteren en hoe u dergelijke aanvallen op uw webserver kunt voorkomen.

Inleiding	2
Het kraken van een webserver is niet moeilijk	2
De gereedschappen van de hacker	3
Inbraakdetectie door het monitoren van belangrijke systeembestanden	5
Het detecteren van hackers op uw webserver	6
Over de GFI LANguard Security Event Log Monitor (S.E.L.M.)	12
Over GFI	13

Het kraken van een webserver is niet moeilijk

Internet Information Services (IIS) webserver zijn zeer populair onder bedrijven. Wereldwijd zijn er meer dan zes miljoen geïnstalleerd. Hierdoor zijn ze helaas een populair doelwit voor hackers. Eens in de zoveel tijd duiken er nieuwe exploits op die een gevaar betekenen voor de integriteit en de stabiliteit van uw IIS webserver.

Veel netwerkbeheerders kunnen de stroom uitgaven van patches voor exploits moeilijk bijbenen. Hierdoor is het voor kwaadaardige gebruikers gemakkelijk om op internet een kwetsbare webserver te vinden. Als je over de juiste middelen beschikt is het niet moeilijk om je voordeel te halen uit een exploit. De gemiddelde zestienjarige hacker kan dus gemakkelijk uw webserver aanvallen en zelfs de controle ervan overnemen om vervolgens uw interne netwerk binnen te dringen.

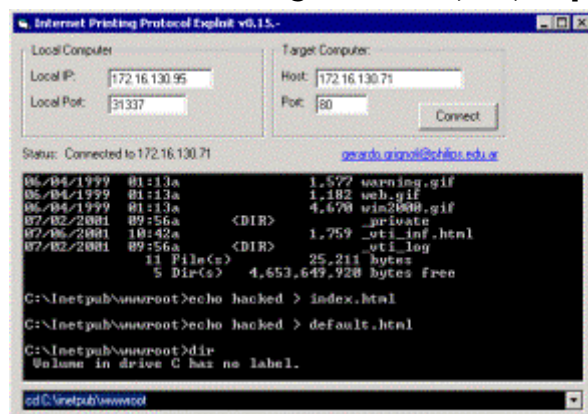
Het is dus niet al te moeilijk voor buitenstaanders om zich toegang te verschaffen tot vertrouwelijke informatie. Wat het nog erger maakt is dat hackers niet altijd verveelde tieners zijn, zoals de meeste mensen denken. Zo kunnen concurrenten en ontevreden werknemers hun eigen redenen hebben om in te breken op vertrouwelijke onderdelen van uw netwerk.

Slechts weinig aanvallen van hackers zijn meteen als zodanig herkenbaar, en het aantal waarvan uitgebreid in de media verslag wordt gedaan is maar het topje van de ijsberg. De meeste aanvallen zijn niet eenvoudig te ontdekken aangezien de meeste indringers er de voorkeur aangeven onzichtbaar te blijven zodat ze vanaf de IIS webserver die ze net hebben gekraakt nog veel belangrijkere of populairdere webserver kunnen aanvallen. Dit brengt niet alleen de integriteit van uw eigen website in gevaar maar u kunt ook juridisch aansprakelijk worden gesteld als uw server is gebruikt om een andere organisatie aan te vallen.

De gereedschappen van de hacker

Hackers die op een website willen inbreken hebben vele middelen tot hun beschikking. Sommige daarvan zijn zelfs zo eenvoudig in het gebruik dat zelfs een beginner in geen tijd een zootje kan maken van een webserver.

De Internet Printing Protocol (IPP) exploit



Gemakkelijke uitbuiting van IPP exploits

Een programma dat van deze exploit gebruik maakt is de Internet Printing Protocol Exploit v.0.15 (zie figuur hierboven) Deze is gebaseerd op de beruchte originele exploitcode in een C-programmabestand genaamd "jill c". Deze code werd openbaar gemaakt door een hacker die de alias "dark spyrit" gebruikte.

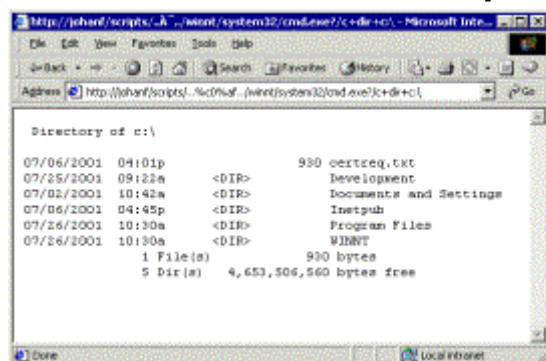
Deze applicatie maakt gebruik van een zwakke plek in de IPP bufferoverloop op een IIS-web server. Het enige wat de hacker hoeft te doen is de naam van een webserver (of een computer met IIS erop geïnstalleerd) intypen en op "Verbinden" klikken.

Als er eenmaal verbinding is stuurt de applicatie de tekenreeks die het stapelgeheugen doet overstromen, waarna een shellcode wordt gerund en het bestand cmd.exe aan de gespecificeerde poort aan de kant van de aanvaller wordt verbonden (default 31337).

Hierdoor kunnen de meeste firewallconfiguraties en vergelijkbare veiligheidsmaatregelen gepasseerd worden.

Vervolgens krijgt de hacker een opdrachtregel en SYSTEM-toegang en kan hij een aantal activiteiten uitvoeren die de beheerder nooit zou hebben goedgekeurd, zoals het openen van databases met creditcardgegevens en andere vertrouwelijke informatie.

De UNICODE en CGI-Decode exploits



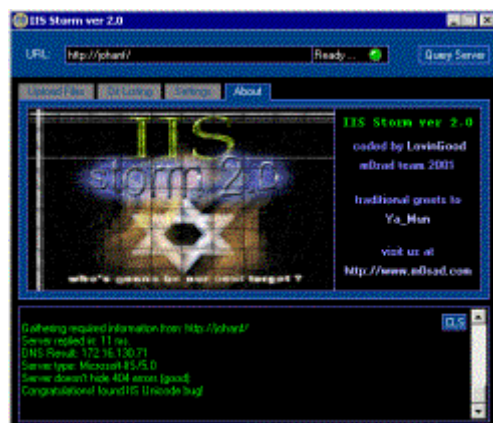
Unicode-exploit met Internet Explorer

Twee andere exploits die populair zijn onder hackers zijn de UNICODE en CGI-Decode exploits. In dit geval kan de hacker de browser zelf gebruiken om in te breken op een machine waarop een ongepatchte versie van IIS draait. Het enige wat hiervoor nodig is is Internet Explorer en een “magische tekenreeks” en men kan runnen wat men wil onder de anonieme account van de IIS. In het bovenstaande screenshot ziet u een directory dump van C:\ van de IIS server in de browser zelf! Dit is een eenvoudig voorbeeld om te laten zien dat hackers toegang kunnen verkrijgen tot de harde schijf van uw webserver.

Aanvankelijk is deze toegang beperkt tot de gebruikersrechten van de anonieme gebruikersaccount van de IIS (IUSR_computernaam). Daarna kan hij gemakkelijk een ASP-bestand uploaden, waarmee hij toegang kan verkrijgen tot SYSTEM-privileges. Zo kan hij volledige toegang krijgen tot de gehackte computer en kan hij dus doen wat hij wil.

Op maat gemaakte applicaties

Sommige crackergroepen maken hun eigen applicaties om het proces van het schenden van websites te automatiseren.



IIS Storm van m0sad

Een voorbeeld van een dergelijke groep is MOsad, een Israëlische hackersgroep die IIS Storm v.2 heeft ontwikkeld en uitgebracht. Hier is een fragment uit de handleiding van IIS Storm: "IIS Storm is een tool voor Remote Web Site Defacement die ISS (Internet Information Server [NT platform]) runt en ook de Unicode-exploit uitbuit".

Met dergelijke tools hebben zowel ervaren als onervaren hackers alle mogelijkheden. Met IIS Storm kunnen gebruikers tevens hun originele IP-adressen verbergen door middel van anonieme proxies en bestanden op uw website vervangen door zelfgemaakte HTML-pagina's.

PoizonB0x, een andere beruchte groep zelfuitgeroepen "cyberterroristen" en "netstrijders", is de maker van iisautoexp.pl, een geautomatiseerde tool waarmee men gemakkelijk toegang kan krijgen tot en schade kan aanbrengen aan websites.

Het enige wat de hacker hoeft te doen is het script de naam van de website geven en het uitvoeren. Als een website gemakkelijk aan te vallen is (i.e. als de benodigde patches ontbreken), wordt de voorpagina (index.htm, default.htm, default.asp of varianten daarop) veranderd in "PoizonB0x Ownz YA". Op deze manier kunnen hackers een batchbestand maken met de namen van de websites die ze willen aanvallen en zo schade toebrengen aan een groot aantal IIS web servers. Het script kan worden aangepast en kan dus op zowel Windows- als UNIX-machines draaien.

Als er schade is toegebracht aan uw website weet u meteen dat uw webserver is aangevallen. Veel hackers handelen echter liever in het geheim en installeren een trojan om gegevens te stelen of andere kwaadaardige trucs uit te voeren. Zij zorgen ervoor dat hun inbraak geen sporen achterlaat.

Inbraakdetectie door het monitoren van belangrijke systeembestanden

Hoe kan men zich dan beschermen tegen dit soort aanvallen? Bijna alle exploit tools voor IIS servers maken gebruik van een of meer systeembestanden. Door de activiteit op deze bestanden in realtime te monitoren kan de netwerkbeheerder hackers op heterdaad betrappen. De volgende systeembestanden worden vaak door hacker tools gebruikt:

1. cmd.exe: dit is het programma in Windows dat de opdrachtregel emuleert. Hiervandaan kunnen gebruikers de controle over de server overnemen.
2. ftp.exe: de command line FTP client die geleverd wordt met alle Microsoft Windows platforms; hackers maken hiervan gebruik om vanaf een FTP server op afstand toegang te krijgen tot bestanden op de server.
3. net.exe: met behulp van dit programma kan de machine worden beheerd; hackers kunnen onder de system account backdoor users en groups aanmaken, diensten starten en stoppen, toegang verkrijgen tot andere computers op het netwerk, enzovoort.
4. ping.exe: dit programma stuurt eenvoudigweg een ICMP-echopakket naar hosts op

afstand. Hackers kunnen uw server samen met andere kwetsbare servers gebruiken om ping te runnen tegen een host die wordt aangevallen. Zo voeren ze een DDoS (Distributed Denial of Service)-aanval uit op hun doelwit.

5. `ftpd.exe` dit is een TFTP client die ook geleverd wordt met alle Microsoft Windows machines; sommige hackers gebruiken dit liever dan `ftp.exe` en zullen het gebruiken om aan bestanden te komen waarmee ze de IIS-server nog verder kunnen binnendringen.

Als een cracker `cmd.exe` draait met de UNICODE-exploit wordt het eigenlijk gerund door de Internet Guest Account (IUSR_machinename). Aangezien deze gebruiker dit bestand helemaal niet hoort te draaien kan een netwerkwide event log monitor zoals GFI LANguard S.E.L.M. alle events loggen waarin deze account `cmd.exe` draait. Op deze manier kan GFI LANguard S.E.L.M. de netwerkbeheerder onmiddellijk op de hoogte stellen van de inbraak.

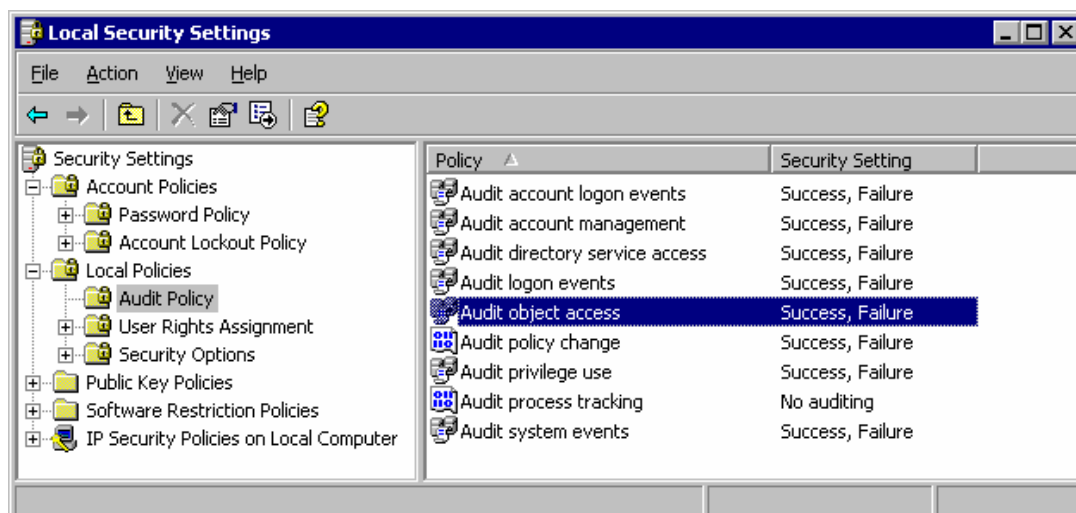
Bufferoverloopaanvallen daarentegen nemen de controle over de SYSTEMaccount over. Dit betekent dat de kwaadaardige gebruiker die al op de machine heeft ingebroken zich vervolgens kan voordoen als iedere andere gebruiker en alles kan doen wat het besturingssysteem zelf kan. Als GFI LANguard S.E.L.M. echter is ingesteld om `cmd.exe` te monitoren en te loggen wanneer de SYSTEMaccount dit file opent, dan kan de netwerkbeheerder dergelijke activiteit detecteren – om van gebruikersnaam te kunnen wisselen moet immers de opdrachtregel worden gebruikt.

Het detecteren van hackers op uw webserver

Nu u weet hoe indringers te werk gaan, kunt u uw server en GFI LANguard S.E.L.M. zo configureren dat u hackers op heterdaad kunt betrappen.

Stap 1: Configureer uw webserver voor de auditing van objecten

Om veel gebruikte bestanden te kunnen monitoren moet object auditing aanstaan in de Windows webserver.



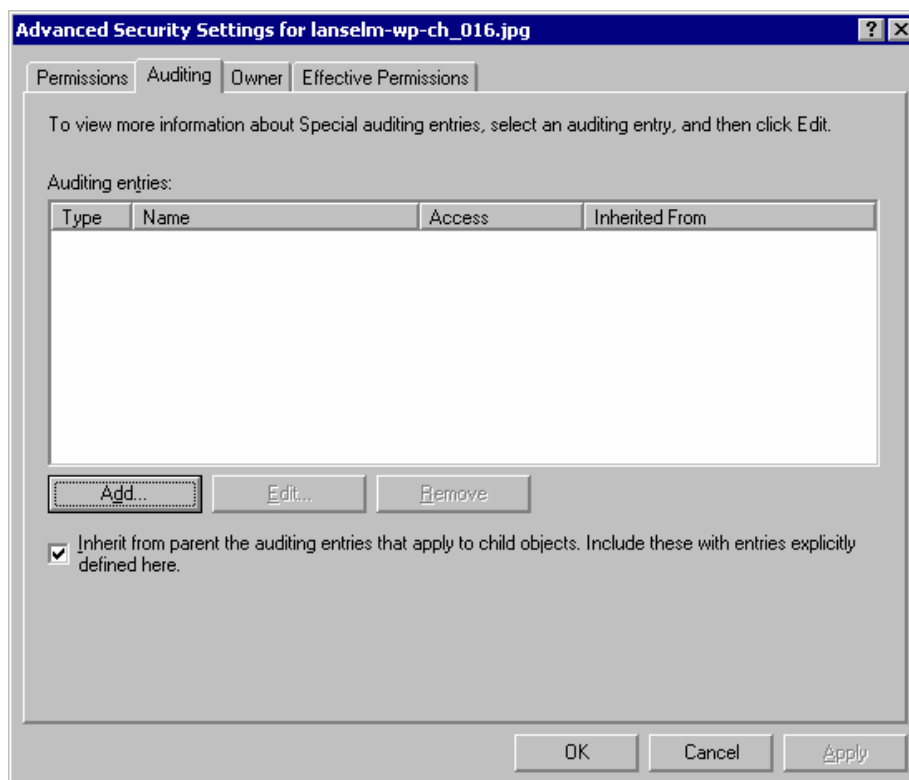
Auditbeleid – toegang tot objecten

Als de webserver een standalone server is moet u het volgende doen om object auditing in te stellen:

1. Ga naar de Administrative Tools – Local Security Policy
2. Selecteer Local Policies en vervolgens Audit Policy
3. Dubbelklik op Audit Object Access en selecteer Success and Failure.

Als de webserver onderdeel is van het domein moet u object auditing instellen als Domain Policy in plaats van alleen Local Policy. Dit gebeurt op dezelfde manier, dus via Administrative Tools en Domain Security Policy.

Vervolgens moet u de bestanden die u wilt auditen specificeren. In dit geval zijn dat de volgende bestanden: cmd.exe, ftp.exe, net.exe, ping.exe en tftp.exe.

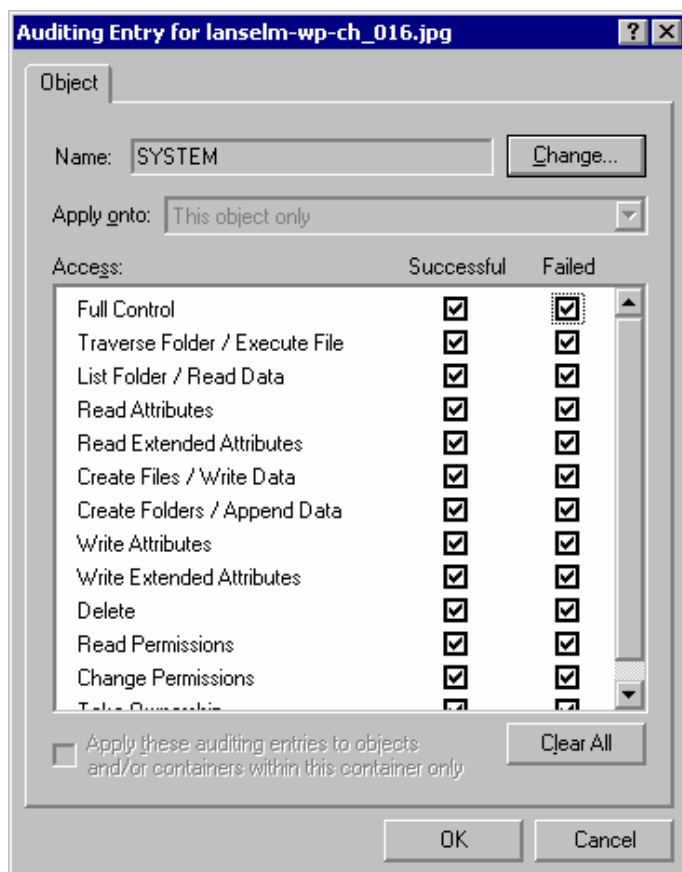


Het tabblad Auditing

Om object access auditing een log te laten maken iedere keer als de SYSTEMaccount en de Internet guest account cmd.exe proberen te draaien, moet u het volgende doen:

1. Klik met de rechtermuisknop op cmd.exe en selecteer Properties
2. Selecteer vervolgens de Security tab en klik op Advanced
3. Selecteer de Auditing tab en klik op Add
4. Nu kunt u aangeven welke gebruikers gelogd moeten worden wanneer ze proberen om het object (cmd.exe) te openen: Selecteer de SYSTEMaccount
5. Voor volledige auditing op cmd.exe/ SYSTEMaccount selecteert u alle Successful and Failed opties.
6. Klik op OK, selecteer Add en doe hetzelfde voor de IUSR-account.
7. Deze procedure volgt u voor ftp.exe, net.exe, ping.exe, en tftp.exe.

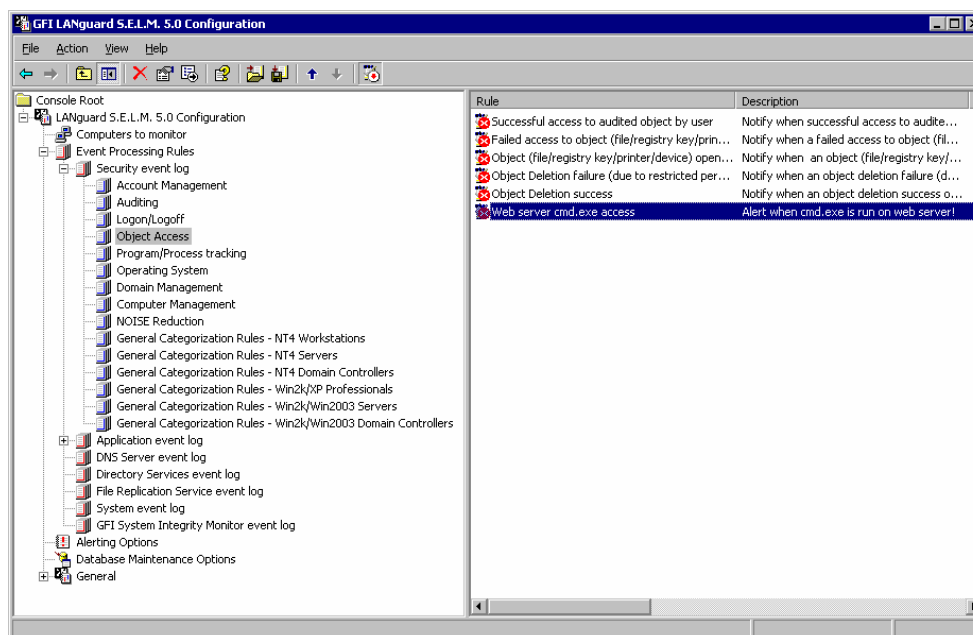
Voortaan wordt er een log aangelegd wanneer de Systemaccount of de IUSR-account een van deze bestanden probeert te openen.



Het configureren van auditing

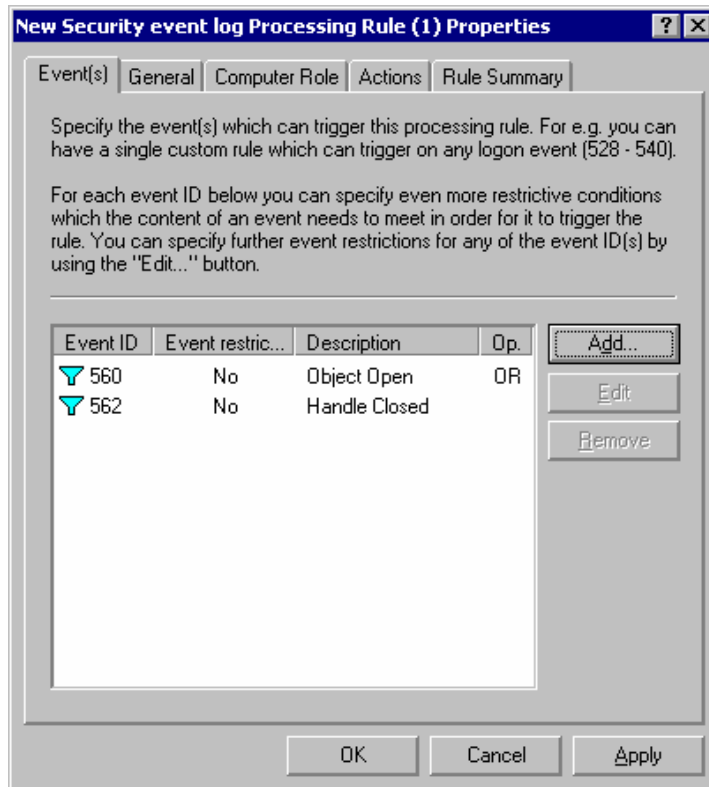
Stap 2: Het configureren van GFI LANguard S.E.L.M. om deze events te monitoren en de beheerder op de hoogte te brengen.

Nu u file access auditing heeft geconfigureerd moet u GFI LANguard S.E.L.M configureren voor het detecteren van deze security events:



GFI LANguard S.E.L.M. configuratie-console

1. Zorg ervoor dat de webserver in de lijst van computers die gemonitord worden staat.
2. Ga naar Event Processing Rules > Security Event Log > Object Access node. Selecteer de node, klik erop met de rechtermuisknop en selecteer New > Processing rule
3. Klik op add en voeg de events met de nummers 560 en 562 toe. Deze events identificeren inbraken. Event 560: Object Open – betekent dat het object (bijv. cmd.exe heeft gedraaid) is geopend, en Event 562: Handle Closed – betekent dat het object niet langer in gebruik is (bijv. cmd.exe is afgesloten).
4. De regel wordt standaard toegepast op alle computers die door GFI LANguard S.E.L.M. worden gemonitord. Als u alleen de webserver wilt specificeren gaat u naar de algemene tab en specificeert u de naam van de webserver. Specificeer ook een duidelijke omschrijving.
5. Klik op OK om de regel toe te voegen.



Het aanmaken van een nieuwe object access rule

GFI LANguard S.E.L.M. monitort uw webserver nu op deze events en brengt u onmiddellijk op de hoogte als cmd.exe wordt gerund!

Stap 3: Het testen van uw nieuwe IDS

Zodra u het bovenstaande heeft geconfigureerd kunt u het testen. U kunt dit doen door een nieuw ASP-script te creëren. Als u uw auditing policies goed heeft ingesteld en object access op de aangegeven bestanden heeft ingesteld wordt door dit script een object audit rule gecreëerd en geactiveerd. GFI LANguard S.E.L.M haalt dan het gegenereerde event uit het security event log. Aangezien er een bijpassende regel bestaat, stuurt het vervolgens een e-mail alert naar de beheerder om te laten weten dat cmd.exe is geopend.

Het onderstaande script runt cmd.exe en maakt een directory listing van de C:\ op de achtergrond. U kunt dit bestand op uw ISS-server plaatsen en het openen via de webbrowser.

```
<%@ Language=VBScript %>
<%' -----
' SELM_test.asp : used to test Languard S.E.L.M.
' By : Sandro Gauci <Sandro@gfi.com>
' Co : GFI
```

```
'-----  
Dim oScript  
On Error Resume Next  
Set oScript = Server.CreateObject("WSCRIPT.SHELL")  
Call oScript.Run ("cmd.exe /c dir C:\", 0, True)  
%>  
<HTML>  
<BODY>  
Als het goed is krijgt u nu een alert van GFI LANguard S.E.L.M.  
</BODY>  
</HTML>
```

U kunt dit ASP-script downloaden op <ftp.gfi.com/testselm.zip>.

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

GFI LANguard Security Event Log Monitor v5 detecteert indringers in uw systeem met behulp van een event log. GFI LANguard archiveert en analyseert de event logs van alle machines op het netwerk en brengt u in realtime op de hoogte van beveiligingsproblemen, aanvallen en andere kritieke events. Dankzij de intelligente analyse van GFI LANguard S.E.L.M. hoeft u geen 'Event Goeroe' te zijn voor het monitoren van gebruikers die toegang proberen te krijgen tot beveiligde shares en vertrouwelijke bestanden; monitoren van kritieke servers en creëren van alerts voor specifieke events en omstandigheden op uw netwerk; automatisch backuppen en wissen van event logs vanaf machines op afstand; detecteren van aanvallen vanaf lokale gebruikersaccounts; en nog veel meer!

Ga naar <http://www.gfi.nl/nl/lanselm/> voor meer informatie over dit product en een gratis trialversie.

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

