WHITE PAPER

Eindringlingserkennung auf Web-Servern

Sofortige Abwehr von Hacker-Angriffen mit Hilfe der Echtzeit-Überwachung von Ereignisprotokollen

Dieses White Paper informiert über verschiedene Methoden, die Hacker für Angriffe auf IIS Web-Server einsetzen. Es wird erläutert, wie die Echtzeit-Überwachung der Ereignisprotokolle eines Web-Servers eine sofortige Alarmierung nach einem erfolgreichen Angriff ermöglicht.

Einführung

Dieses White Paper zeigt, wie Administratoren ihre Web-Server zuverlässig vor unerlaubten Zugriffen absichern können. Informationen zu verschiedenen Backdoor-Tools zeigen, welche Methoden Hacker anwenden, um Zugang zu einem IIS Web-Server zu erlangen. Zudem wird erklärt, welche Möglichkeiten es gibt, unberechtigte Zugriffe auf ein Netzwerk zu erkennen und wie man sich vor solchen Angriffen schützen kann.

Das Hacken von Web-Servern – ein leichtes Spiel

IIS-Web-Server (Internet Information Services), die Web-Seiten hosten und Anwendern zur Verfügung stellen, sind bei Unternehmen sehr beliebt – weltweit gibt es über sechs Millionen dieser Server. Diese Tatsache macht sie aber leider auch zu einem sehr beliebten Ziel von Hackern. Immer öfter treten neue Exploits in Erscheinung, die die Funktionsfähigkeit und Stabilität von IIS-Web-Servern gefährden.

Einigen Administratoren fällt es daher schwer, bei den vielen verschiedenen Sicherheits-Patches für IIS auf dem Laufenden zu bleiben und somit für jedes neue Exploit gerüstet zu sein. Das macht es böswilligen Anwendern wiederum recht einfach, anfällige Web-Server im Internet zu finden. Hacker-Werkzeuge sind im Internet leicht zu finden. Mit ihnen können auch jugendliche Angreifer einen Web-Server leicht angreifen, sogar kontrollieren und vielleicht sogar in das interne Netzwerk eindringen.

Mit anderen Worten: Es ist für Außenstehende nicht allzu schwer, Zugang zu vertraulichen Unternehmensinformationen zu erlangen. Noch schlimmer ist jedoch die Tatsache, dass es sich bei den Hackern nicht unbedingt, wie oft angenommen, um Teenager handeln muss, die sich beweisen wollen: Verärgerte Mitarbeiter und Konkurrenten verfolgen ebenfalls ganz eigene Interessen, wenn sie in nicht öffentliche Bereiche von Unternehmensnetzwerken eindringen.

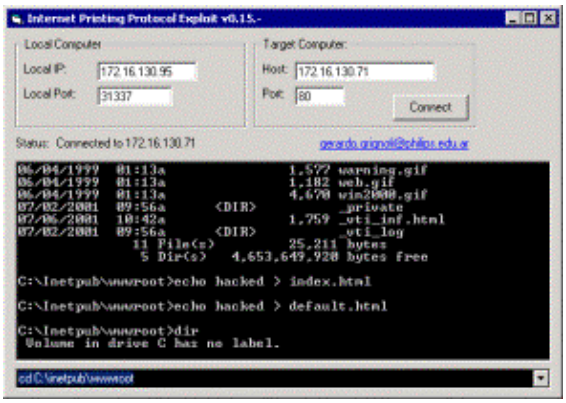
Nur wenige Hacker-Angriffe werden sofort auch als solche erkannt, und noch weniger von ihnen geraten in die Schlagzeilen der Medien. Die meisten Angriffe sind nur schwer erkennbar, weil viele Eindringlinge es vorziehen unbemerkt zu bleiben, um so den von ihnen gehackten IIS-Web-Server als Ausgangsbasis für Angriffe auf weitaus wichtigere und beliebtere Web-

Server zu benutzen. Außer der Gefährdung der Integrität Ihrer eigenen Web-Seite könne auch Sie selbst für einen solchen Missbrach Ihres Servers zur Verantwortung gezogen werden, sollte er z. B. für einen Angriff auf ein anderes Unternehmen dienen.

Typische Hacker-Tools

Es gibt viele Werkzeuge, die Hacker dazu befähigen, eine Web-Site zu verunstalten. Solche Werkzeuge sind so einfach zu bedienen, dass selbst ein unerfahrener Hacker sehr schnell und einfach einen Web-Server unbrauchbar machen kann.

Der IPP-Exploit (Internet Printing Protocol)



Einsatz des IPP-Exploit

Ein Programm, das den IPP-Exploit verwendet, ist Internet Printing Protocol Exploit v.0.15 (siehe Abbildung oben). Er basiert auf dem berüchtigten ursprünglichen Exploit-Code eines C-Programms mit dem Namen "jill.c", der von einem Hacker mit dem Pseudonym "Dark Spyrit" veröffentlicht wurde.

Diese Anwendung nutzt eine Anfälligkeit beim IPP-Buffer-Overflow von IIS-Web-Servern aus. Ein Hacker muss nur den Namen des anzugreifenden Web-Servers (oder eines Computers, auf dem IIS installiert ist) eingeben und auf "Connect" klicken.

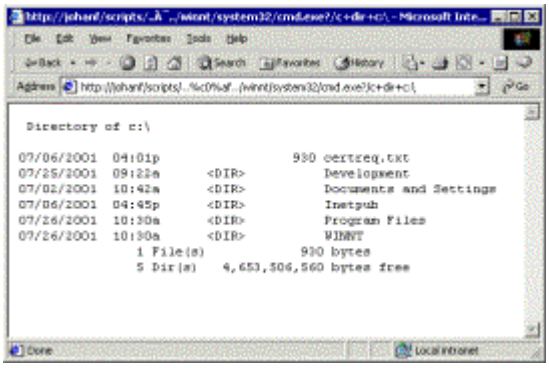
Wenn die Verbindung aufgebaut ist, sendet das Programm die Zeichenkette, die den Overflow im Stack verursacht, was zur Ausführung des speziellen Programm-Codes führt (der als Shell-Code bekannt ist) und die Datei "cmd.exe" mit dem vorgegebenen Port auf der Angreiferseite verbindet (der Standard-Port ist 31337).

So lassen sich typische Firewall-Einstellungen und ähnliche Sicherheitsmaßnahmen umgehen.

Danach stehen dem Hacker Befehlszeile und SYSTEM-Zugang zur Verfügung, über die ihm einige Aktivitäten möglich sind, die ein Administrator auf keinen Fall einschränken würde, z. B. der Zugriff auf Datenbanken, die Kreditkarteninformationen oder sonstige vertrauliche Daten

enthalten.

Die UNICODE- und CGI-Decode-Exploits



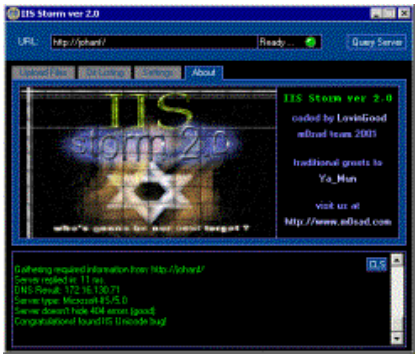
UNICODE-Exploit unter Internet Explorer

Zwei andere bei Hackern für die Web-Site-Manipulation sehr beliebte Exploits sind die UNICODE- und CGI-Decode-Exploits. Hier kann nur mit Hilfe des Browsers auf dem Zielrechner, auf dem eine ungepatchte Version der IIS läuft, jede mögliche Aktion durchgeführt werden. Alles, was benötigt wird, ist der Internet Explorer und ein "Magic String", um unter dem anonymen Konto des IIS Schäden aller Art zu verursachen. Der obige Screenshot zeigt einen Directory-Dump von Laufwerk c:\ des IIS-Servers direkt im Web-Browser! Dies ist nur ein einfaches Beispiel, um zu zeigen, dass ein Hacker Zugriff auf die Festplatte eines Web-Servers nehmen kann.

Zunächst ist der Zugriff auf die Rechte des anonymen IIS-Anwenderkontos beschränkt (IUSR_computername). Hat ein Hacker aber erst einmal anonymen Zugriff auf die IIS, kann er mit Leichtigkeit eine ASP-Datei hochladen, die seine Zugriffsrechte auf SYSTEM-Rechte erweitern kann. Solch eine Aktion würde dem Angreifer also uneingeschränkten Zugriff auf den gehackten Computer geben.

Selbst entwickelte Anwendungen

Einige Gruppen, die sich mit dem Hacken von Web-Sites beschäftigen, bevorzugen es, eigene Anwendungen für die automatisierte Verunstaltung der Sites zu erstellen.



***IIS Storm* von m0sad**

Eine dieser Gruppen ist M0sad, eine israelische Hacker-Gruppe, die das Hacking-Tool IIS Storm v.2 entwickelt und veröffentlicht. Hier ein Auszug aus dem Handbuch zu *IIS Storm*: “IIS Storm is a tool made for Remote Web Site Defacement that is running IIS (Internet Information Server [NT platform]) and that also vulnerable to the Unicode Exploit.”

Sowohl geübte als auch unerfahrene Hacker werden von Tools wie diesem bei ihren illegalen Aktivitäten umfassend unterstützt. IIS Storm ermöglicht es Anwendern außerdem, über anonyme Proxies ihre echte IP-Adresse zu verheimlichen und auf einfache Weise Dateien auf der angegriffenen Web-Site mit eigenen HTML-Seiten zu ersetzen.

PoizonB0x, eine weitere berüchtigte Gruppe selbsternannter "Cyber-Terroristen" und “Net-Warriors", ist das Programm iisautoexp.pl zu verdanken, ein automatisiertes Tool, das dem Hacker die mit dem illegalen Zugriff und der Verunstaltung von Web-Seiten verbundene Arbeit praktisch abnimmt.

Um eine Web-Site zu verunstalten, muss ein böswilliger Benutzer nur den Namen der Site eingeben und das Skript starten. Wenn die Web-Seite gegen einen Angriff nicht geschützt ist (d. h., wenn nicht die entsprechenden Patches installiert sind), wird die Startseite (index.htm, default.htm, default.asp o. ä.) verändert und der Schriftzug "PoizonB0x Ownz YA" angezeigt. Auf diese Weise können Hacker eine Batch-Datei mit den Namen der anzugreifenden Seiten erstellen und eine große Anzahl von IIS-Web-Servern kompromittieren. Dieses Skript kann modifiziert werden und sowohl auf Windows- als auch auf UNIX-Rechnern laufen.

Die Verunstaltung einer Web-Seite lässt leicht erkennen, dass der Web-Server angegriffen wurde. Viele Hacker wollen jedoch unerkannt bleiben und installieren stattdessen einen Trojaner, der Daten sammelt oder andere böswillige Aktivitäten durchführen soll. In diesem Fall sind sie sehr darauf bedacht, dass ihr Eindringen unbemerkt bleibt und es auch keine Hinweise auf die Kompromittierung des Systems gibt.

Eindringlingserkennung durch Überwachung wichtiger Systemdateien

Welche Schutzmaßnahmen sollten nun gegen potenzielle Angriffe getroffen werden? Fast alle Exploit-Tools für IIS-Server greifen auf eine oder mehrere Systemdateien des Servers zu. Daher können durch eine Überwachung dieser Dateien in Echtzeit die meisten böswilligen Aktivitäten sofort festgestellt werden. Folgende Systemdateien werden häufig von Hacker-Tools verwendet und modifiziert:

1. cmd.exe: Dies ist das Emulationsprogramm für Befehlszeilen unter Windows, mit dem Anwender den Server verwalten können.
2. ftp.exe: Dies ist der Command-Line FTP-Client, der auf allen Microsoft Windows-

Plattformen enthalten ist. Hacker verwenden ihn, um die auf dem Server benötigten Dateien von einem Remote-FTP-Server abzurufen.

3. net.exe: Dieses Programm ermöglicht die Administration eines Rechners. Unter dem Systemkonto können Hacker Backdoor-Anwender und -Gruppen erstellen, Dienste starten und stoppen, auf andere Rechner im Netzwerk zugreifen und vieles mehr.
4. ping.exe: Dieses Programm sendet einfach ein ICMP-Echo-Packet an Remote-Hosts. Hacker können einen kompromittierten Server zusammen mit anderen ungeschützten Servern benutzen, um mit Hilfe von Ping einen DDoS-Angriff (Distributed Denial of Service) auf einen Ziel-Host zu starten.
5. tftp.exe: Dies ist ein TFTP-Client, der ebenfalls auf allen Microsoft Windows-Rechnern verfügbar ist. Einige Hacker bevorzugen ihn gegenüber ftp.exe, um Dateien abzurufen, die sie benötigen, um noch weiter in die Strukturen des IIS-Server einzudringen.

Wenn ein Cracker das Programm cmd.exe unter Verwendung des UNICODE-Exploits startet, läuft es eigentlich unter dem Internet-Gästekonto (IUSR_machinename). Da dieser Benutzer diese Datei aber eigentlich nicht ausführen dürfte, kann ein netzwerkweit eingesetzter Ereignisprotokoll-Monitor wie GFI LANguard S.E.L.M. Ereignisse protokollieren, wo unter diesem Konto das Programm cmd.exe ausgeführt wird. Auf diese Weise kann GFI LANguard S.E.L.M. Administratoren sofort über ein unautorisiertes Eindringen informieren.

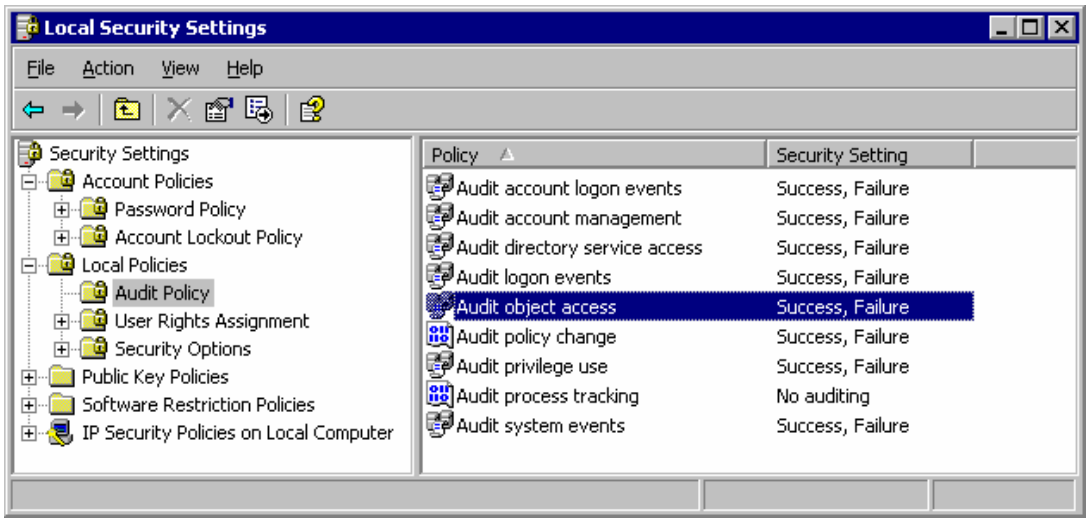
Buffer-Overflow-Angriffe basieren stattdessen auf dem SYSTEM-Konto. Dies bedeutet, dass Angreifer, die ohnehin schon in den Rechner eingedrungen sind, von hier aus zu einem anderen Anwenderkonto wechseln und ihnen im Grunde alle Möglichkeiten des Betriebssystems
offen stehen. Ist jedoch GFI LANguard S.E.L.M. so konfiguriert, dass die Datei cmd.exe überwacht und ein Protokolleintrag erstellt wird, sobald das SYSTEM-Konto auf diese Datei zugreift, kann der Netzwerk-Administrator nun diese Aktivität erkennen, da die Tools für einen Kontowechsel das Befehlszeilenprogramm verwenden.

Identifizierung von Angriffen auf Web-Server

Nachdem erläutert wurde, wie Eindringlinge bei der Kompromittierung eines Systems vorgehen können, lassen sich Server mit Hilfe von GFI LANguard S.E.L.M. so konfigurieren, dass Hacker auf frischer Tat ertappt werden.

Schritt 1: Konfigurierung des Web-Servers für die Überwachung von Objekten

Um häufig verwendete Dateien zu überwachen, muss die Objektüberwachung unter Windows aktiviert sein.



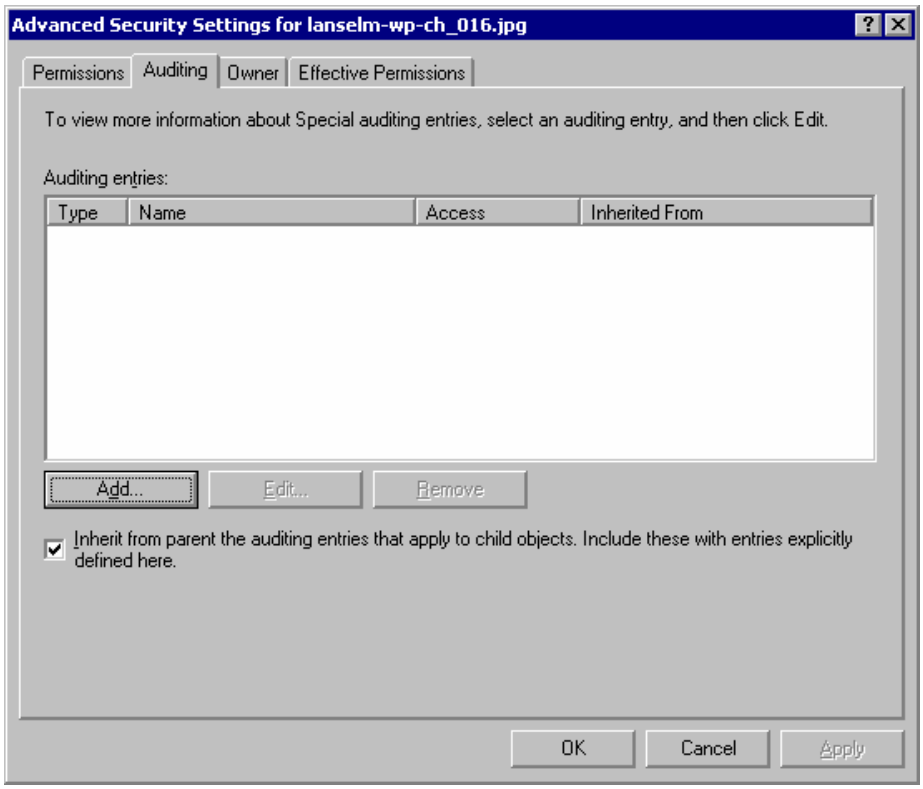
Überwachungsrichtlinie – Objektzugriffsversuche

Um die Objektüberwachung auf einem eigenständigen Server zu aktivieren, sind folgende Schritte zu befolgen:

1. Die Lokale Sicherheitsrichtlinie muss über “Start” > “Einstellungen” > “Systemsteuerung“ > “Verwaltung” > “Lokale Sicherheitsrichtlinie” aufgerufen werden.
2. Dort ist unter den lokalen Richtlinien die Überwachungsrichtlinie zu wählen.
3. Nach einem Doppelklick auf “Objektzugriffe überwachen” ist “Erfolgreich” und “Fehlgeschlagen” zu aktivieren.

Ist der Web-Server Teil der Domäne, muss die Objektüberwachung als Domänenrichtlinie aktiviert werden (und nicht etwa nur als lokale Richtlinie). Dies erfolgt ebenfalls über Verwaltung und die Domänen-Sicherheitsrichtlinie.

Im Anschluss daran müssen die zu überwachenden Dateien festgelegt werden. In diesem Fall sollen überwacht werden: cmd.exe, ftp.exe, net.exe, ping.exe und tftp.exe.

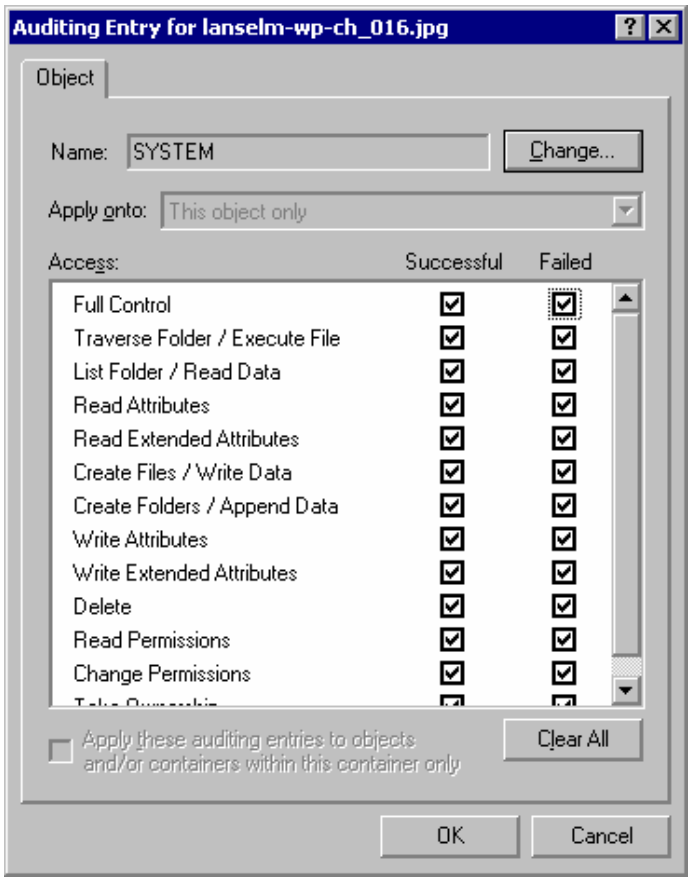


Registerkarte “Überwachung“

Damit mit Hilfe der Objektzugriffsüberwachung bei jedem Versuch des SYSTEM-Kontos und des Internet-Gästekontos, auf die Datei cmd.exe zuzugreifen, ein Protokolleintrag vorgenommen wird, sind folgende Einstellungen notwendig:

1. Nach einem rechten Mausklick auf cmd.exe ist "Eigenschaften“ auszuwählen.
2. In der Registerkarte “Sicherheitseinstellungen“ muss auf “Erweitert...“ geklickt werden.
3. In der Registerkarte “Überwachung“ ist “Hinzufügen...“ zu wählen.
4. Nun kann festgelegt werden, welche Benutzer zu protokollieren sind, wenn sie versuchen, auf das Objekt (cmd.exe) zuzugreifen: Hierfür ist das SYSTEM-Konto anzugeben.
5. Um eine umfassende Überwachung von cmd.exe / des SYSTEM-Kontos zu ermöglichen, müssen die Optionen “Erfolgreich“ und “Fehlgeschlagen“ aktiviert werden.
6. Nach der Bestätigung durch einen Mausklick auf “OK“ und “Hinzufügen...“ sind dieselben Einstellungen für das IUSR-Konto vorzunehmen.
7. Diese Prozedur ist jeweils für die Dateien ftp.exe, net.exe, ping.exe und tftp.exe zu wiederholen.

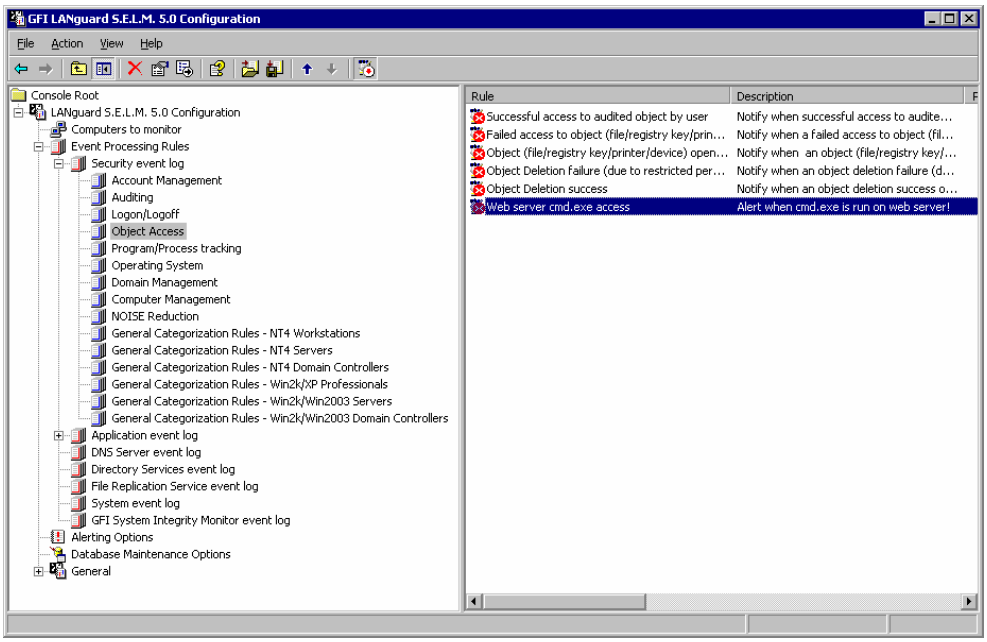
Danach wird jeder Zugriff auf diese Dateien über das SYSTEM- oder IUSR-Konto im Sicherheitsprotokoll verzeichnet.



Konfigurierung der zu überwachenden Zugriffsereignisse

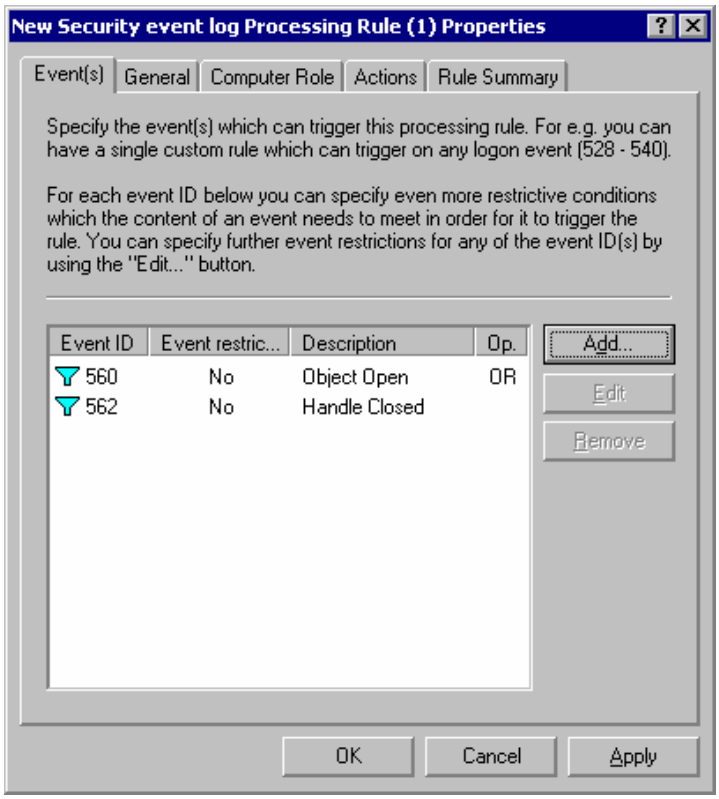
Schritt 2: Konfigurierung von GFI LANguard S.E.L.M. zur Überwachung dieser Ereignisse und Administrator-Benachrichtigung

Nachdem die Überwachung der Dateizugriffe eingerichtet wurde, muss GFI LANguard S.E.L.M. für die Erkennung dieser Sicherheitsereignisse konfiguriert werden.



GFI LANguard S.E.L.M Konfigurationskonsole

1. In der Konfigurationskonsole von GFI LANguard S.E.L.M. muss der Web-Server im Knoten der zu überwachenden Rechner aufgeführt sein.
2. Danach sind die Unterknoten “Event Processing Rules“ > “Security Event Log“ > “Object Access” aufzurufen. Nach einem rechten Mausklick auf “Object Access” ist “New“ > “Processing rule“ auszuwählen.
3. Nach einem Klick auf “Add” sind die Ereignisse mit den IDs 560 und 562 hinzuzufügen. Diese informieren Administratoren über einen Eindringversuch. Ereignis 560: Objekt Offen – Dies bedeutet, dass auf das Objekt zugegriffen wurde (z. B.cmd.exe wurde ausgeführt), und Ereignis 562: Handle Geschlossen – Dies bedeutet, dass auf das Objekt nicht mehr zugegriffen wird (z. B. cmd.exe wurde geschlossen).
4. Diese Regel wird standardmäßig auf alle mit GFI LANguard S.E.L.M. überwachten Rechner angewandt. Um sie auf den Web-Server zu begrenzen, muss der Rechnername des Web-Servers über die Registerkarte “General“ angegeben werden. Zudem ist eine eindeutige Beschreibung erforderlich.
5. Mit einem Mausklick auf "OK" wird die Regel hinzugefügt.



Erstellen einer neuen Regel für den Objektzugriff

GFI LANguard S.E.L.M. überwacht nun den Web-Server auf alle festgelegten Ereignisse. Wird cmd.exe gestartet, erhalten Administratoren sofort eine Warnmitteilung.

Schritt 3: Test des neuen IDS

Nachdem die erforderlichen Konfigurationsschritte vorgenommen wurden, sollten die neuen Sicherheitsfunktionen getestet werden. Hierfür eignet sich am besten die Erstellung eines neuen ASP-Skripts. Wenn die Überwachungsrichtlinien richtig konfiguriert sind und die Objektzugriffsüberwachung für die erwähnten Dateien aktiviert ist, wird dieses Skript einen Ereignisprotokoll-Eintrag erstellen und die entsprechende Objektüberwachungsregel auslösen. GFI LANguard S.E.L.M. wird dann den generierten Ereigniseintrag aus der Sicherheitsprotokoll-Datei abrufen und, da eine entsprechende Regel existiert, eine E-Mail-Warnung an den Administrator senden und ihn somit benachrichtigen, dass auf die Datei cmd.exe zugegriffen wurde.

Folgendes Skript wird lediglich cmd.exe ausführen und im Hintergrund das Verzeichnis von Laufwerk C:\ aufrufen. Diese Datei kann auf den IIS-Server kopiert und mit dem Web-Browser aufgerufen werden.

```
<%@ 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>
Nun sollte eine Warnmitteilung von GFI LANguard S.E.L.M. beim Administrator eintreffen.
</BODY>
</HTML>
```

Dieses ASP-Skript steht zum Download bereit unter: ftp.gfi.com/testselm.zip

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

GFI LANguard Security Event Log Monitor (S.E.L.M.) bietet Eindringlingserkennung mit Hilfe der Ereignisprotokolle, die netzwerkweit verwaltet werden können. GFI LANguard S.E.L.M. archiviert und analysiert die Event-Logs aller Netzwerk-Rechner. Bei Sicherheitsproblemen, Angriffen und anderen kritischen Ereignissen erfolgt die Alarmierung in Echtzeit. Dank der intelligenten Analysetechnik von GFI LANguard S.E.L.M. sind keine Expertenkenntnisse notwendig, um Benutzer zu überwachen, die versuchen, auf geschützte Freigaben und vertrauliche Dateien zuzugreifen. Sicherheitskritische Server lassen sich effizient kontrollieren, und auch das Erstellen von Warnhinweisen für einzelne Netzwerk-Ereignisse und Bedingungen ist problemlos möglich. Zudem können Ereignisprotokolle auf Remote-Rechnern automatisch gelöscht
oder gesichert werden. Angriffe über lokale Benutzerkonten lassen sich ebenfalls schnell erkennen und bekämpfen.

Weitere Informationen zu GFI LANguard S.E.L.M. und eine kostenfreie Testversion finden Sie unter http://www.gfisoftware.de/de/lanselm/.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Fax-Connector GFI FAXmaker für Exchange- und SMTP-Mail-Server, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, die E-Mail-Archivierungslösung GFI MailArchiver, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen, GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien sowie GFI WebMonitor zur Überwachung von HTTP/FTP-Verbindungen mit Virenschutz für ISA Server. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter http://www.gfisoftware.de.