
Come scoprire gli hacker sul server web

Cogliere gli hacker con le mani nel sacco grazie al controllo, in tempo reale, dei log degli eventi della sicurezza

Discussione sui metodi utilizzati dagli hacker per attaccare i server web IIS e su come sia possibile utilizzare il controllo dei log degli eventi sul server web per essere immediatamente avvertiti in caso di attacchi riusciti.

Introduzione

Questa white paper si sofferma sul modo in cui gli amministratori possono configurare i propri server web in maniera efficace e sicura. Descrivendo gli strumenti utilizzati dagli hacker per avere accesso ai server web IIS tramite backdoor, questo documento illustra in maniera dettagliata i passi necessari per individuare con successo eventuali intrusioni nella rete, oltre a spiegare come prevenire tali attacchi al server web.

Introduzione.....	2
Manipolare un server web non è difficile.....	2
Strumenti di “lavoro” degli hacker.....	3
Scoperta d'intrusione mediante il monitoraggio dei file di sistema principali.....	5
Come scoprire attacchi al server.....	6
Informazioni su GFI LANguard Security Event Log Monitor (S.E.L.M.).....	12
Informazioni su GFI.....	13

Manipolare un server web non è difficile

I server web Internet Information Services (IIS) sono molto popolari tra le aziende commerciali, con oltre 6 milioni di installazioni in tutto il mondo. Sfortunatamente, ciò li rende un obiettivo altrettanto popolare tra gli hacker. Di conseguenza, ogni tanto, emergono nuovi exploit che mettono in pericolo l'integrità e la stabilità del proprio server web IIS.

Per molti amministratori diventa difficile mantenersi al passo con le varie patch di sicurezza rilasciate per IIS a fronte di ogni nuovo exploit, facilitando le possibilità, per utenti pericolosi, di trovare su Internet un server web vulnerabile. Trarre vantaggio da un exploit non è difficile, con gli opportuni strumenti di cui dispongono gli hacker. Questi consentono all'hacker teenager medio di attaccare facilmente e, persino controllare, il server web, con la possibilità di penetrare nella rete interna.

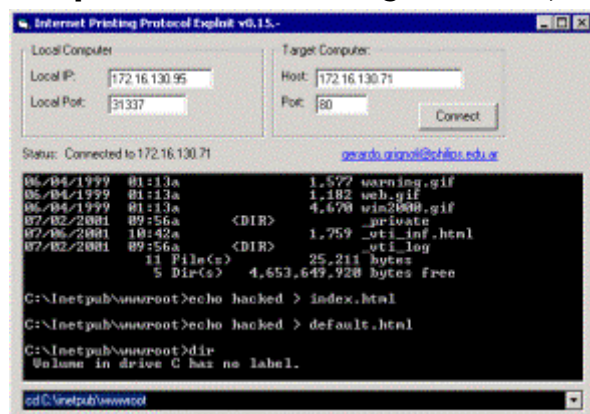
In altri termini, non è molto difficile per soggetti esterni accedere ad informazioni aziendali riservate. Peggio, non necessariamente gli hacker sono teenager alla ricerca del brivido, come si pensa comunemente: per esempio, dipendenti scontenti o concorrenti dell'azienda possono avere le loro buone ragioni per penetrare in zone confidenziali della rete.

Pochi attacchi di hacker sono immediatamente e davvero riconoscibili come tali e ancora meno sono quelli che diventano “affari di alto profilo” riportati dai mezzi di comunicazione. La maggior parte degli attacchi non è facile da scoprire, poiché molti intrusi preferiscono rimanere nascosti in modo da poter utilizzare il server web manipolato come base di lancio di attacchi nei confronti di server web molto più importanti o popolari. Oltre a danneggiare l'integrità del proprio sito web, un tale utilizzo del server può rendere responsabile l'azienda in caso di

attacchi nei confronti di altre aziende.

Strumenti di “lavoro” degli hacker Esistono molti strumenti a disposizione degli hacker che vogliono “imbrattare” un sito web. Questi strumenti sono talmente semplici da utilizzare che persino qualcuno con nessuna esperienza precedente come hacker può imbrattare un server web in pochissimo tempo.

L’exploit Internet Printing Protocol (IPP)



L’exploit IPP è stato semplificato

Un programma che utilizza questo exploit è l’Internet Printing Protocol Exploit v.0.15 (si veda la figura sopra riportata). Si basa sul noto codice di exploit originale di un file di programma in C denominato “jill.c”, reso pubblico da un hacker il cui soprannome era “dark spyrit”.

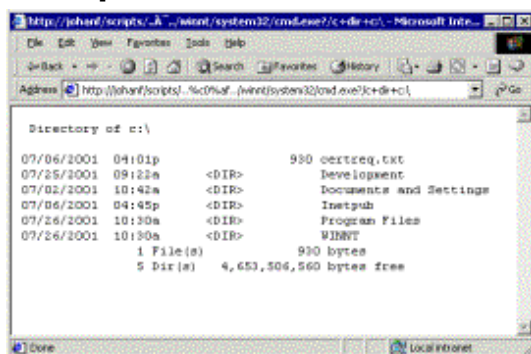
Quest’applicazione utilizza una vulnerabilità da buffer overflow dell’IPP su un server web IIS. Tutto ciò che l’hacker deve fare è digitare il nome del server web preso di mira (oppure un computer su cui sia installato IIS) e fare clic su “Connetti”.

Con la connessione, l’applicazione invierà la stringa vera che causa l’overflow dello stack, comportando l’esecuzione di un programma personalizzato (noto come shell code – programma shell) e la connessione del file cmd.exe alla porta specifica dell’aggressore (quella predefinita è la n. 31337).

Questa è in grado di aggirare configurazioni di firewall tipiche ed altre misure di sicurezza simili.

Una volta fatto questo, l’hacker ottiene una riga di comando e un accesso al SISTEMA, da cui potrebbe portare avanti una serie di attività che un amministratore non avrebbe certamente autorizzato, come l’accesso a database che potrebbero contenere dati relativi a carte di credito ed altre informazioni confidenziali.

Gli exploit di UNICODE e CGI-Decode



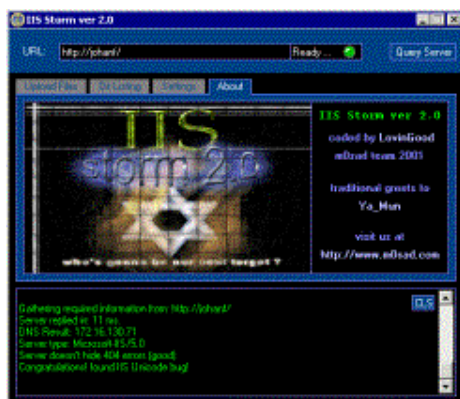
L'exploit di Unicode attraverso Internet Explorer

Altri due exploit preferiti dai *defacer* (“*imbrattatori*”) sono costituiti dagli exploit di UNICODE e CGI-Decode. In questo caso, l’hacker può semplicemente utilizzare il browser stesso per fare qualsiasi cosa sulla macchina target che su cui sia installata una versione priva di patch di IIS. Tutto quello che serve è Internet Explorer ed una “stringa magica” per eseguire qualsiasi cosa sotto l’account anonimo dell’IIS. La schermata precedente illustra il “riversamento” della directory di C:\ del server IIS nel browser web stesso! Non si tratta che di un piccolo esempio che dimostra come l’hacker può ottenere accesso al disco rigido del proprio server web.

L’accesso è limitato inizialmente alle autorizzazioni utente dell’account utente anonimo IIS (IUSR_nomedelcomputer). Quando l’hacker ha accesso all’account anonimo IIS, è in grado di scaricare facilmente un file ASP, con quale può a sua volta accedere a privilegi di SISTEMA. Un’azione del genere gli darebbe accesso totale al computer manipolato, vale a dire, l’hacker potrebbe fare tutto ciò che vuole.

Applicazioni personalizzate

Alcuni gruppi di cracker di siti web preferiscono produrre le proprie applicazioni per automatizzare il processo di “imbrattamento” di un sito web.



IIS Stom di m0sad

Uno di questi gruppi è M0sad, un'unità hacker israeliana che ha sviluppato e rilasciato uno strumento di hacking denominato IIS Storm v.2. Un estratto tratto dal manuale di IIS Storm dice: "IIS Storm costituisce uno strumento per Remote Web Site Defacement che utilizza IIS (Internet Information Server [piattaforma NT]) ed è vulnerabile all'Exploit di Unicode".

Strumenti del genere conferiscono capacità da hacker complete sia ad hacker esperti sia ad hacker inesperti. IIS Storm permette inoltre agli utenti di nascondere il loro IP originale mediante proxy anonimi e di sostituire facilmente con proprie pagine HTML personalizzate file del sito web preso di mira.

PoizonB0x, un altro noto gruppo di auto-proclamati "cyber-terroristi" e "guerrieri della rete", ha realizzato *iisautoexp.pl*, uno strumento automatico che gestisce tutto il lavoro "pesante" necessario per ottenere l'accesso ed eseguire operazioni di *defacing* (imbrattamento).

Per imbrattare un sito web, tutto quello che gli utenti malintenzionati devono fare è dare il nome del sito web allo script ed eseguirlo. Se il sito web è vulnerabile ad attacchi (se, cioè, non è munito delle opportune patch), la pagina iniziale (index.htm, default.htm, default.asp o sue varianti) viene cambiata in "PoizonB0x Ownz YA". In questo modo, gli hacker possono creare file di batch con i nomi dei siti web presi di mira, realizzando un imbrattamento di massa di server web IIS. Questo script può essere adattato ed eseguito sia su macchine Window sia su macchine UNIX.

Sapere che il server web è stato attaccato è facile se la propria pagina web è imbrattata. Tuttavia, molti hacker installano furtivamente un Trojan per sottrarre dati in modo illegale o eseguire altre attività pericolose. Faranno in modo da non lasciare alcuna traccia del loro passaggio.

Scoperta d'intrusione mediante il monitoraggio dei file di sistema principali

Allora, come ci si può proteggere da una tale possibile offensiva di attacchi? Ebbene, quasi tutti gli strumenti di exploit per server IIS fanno uso di uno o più file di sistema. Controllando l'attività di questi file in tempo reale, un amministratore può cogliere l'hacker con le mani nel sacco. Gli hacker utilizzano spesso i seguenti file di sistema:

1. *cmd.exe*: si tratta del programma di emulazione della riga di comando di Windows; da qui gli utenti sono in grado di amministrare il server
2. *ftp.exe*: riga di comando client FTP disponibile con tutte le piattaforme Microsoft Windows; gli hacker la usano per ottenere i file della macchina server di cui hanno bisogno tramite il server FTP remoto
3. *net.exe*: questo programma consente l'amministrazione della macchina, sotto l'account di sistema; gli hacker possono utilizzare questo strumento per creare utenti e gruppi backdoor, avviare e arrestare servizi, accedere alle altre macchine della rete ed altro.

4. ping.exe: questo programma invia semplicemente un pacchetto eco (per misurare la distanza) agli host remoti; gli hacker possono usare il server dell'azienda presa di mira insieme ad altri server vulnerabili per eseguire ping contro un host mirato, creando così un attacco di tipo DDoS (Distributed Denial of Service) sul target.
5. tftp.exe: si tratta di un client TFTP anch'esso disponibile con tutte le macchine Microsoft Windows; alcuni hacker lo preferiscono a ftp.exe e lo utilizzano per ottenere i file di cui necessitano per penetrare ulteriormente nel server IIS.

Quando un cracker esegue cmd.exe utilizzando l'exploit di UNICODE, esso è in realtà eseguito dall'Internet Guest Account (Account Internet Ospite) (IUSR_nomemacchina). Poiché tale utente non ha attività che eseguono questo file, un monitor dei log degli eventi di tutta la rete qual'è GFI LANguard S.E.L.M. è in grado di registrare tutti gli eventi in cui questo account esegue cmd.exe. In questo modo, GFI LANguard S.E.L.M. può immediatamente informare l'amministratore dell'intrusione.

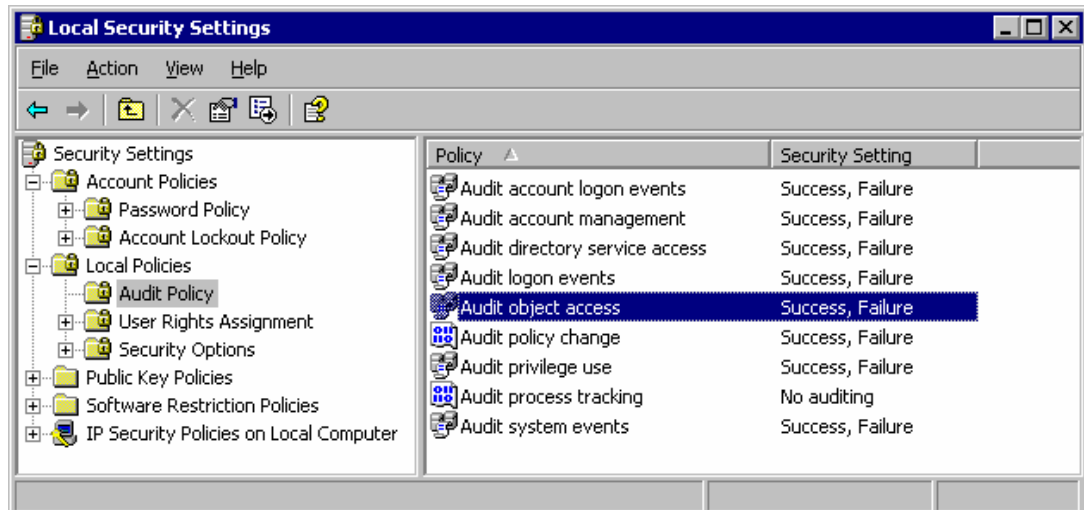
Gli attacchi di buffer overflow, invece, ottengono l'account di SISTEMA. Ciò significa che da qui, l'utente malintenzionato, che si è già introdotto nella macchina, è in grado di cambiarsi in qualsiasi altro utente e, sostanzialmente, fare tutto quello che lo stesso sistema operativo è in grado di fare. Tuttavia, se GFI LANguard S.E.L.M. viene abilitato al controllo di cmd.exe e a registrare ogni volta che l'account di SISTEMA ha accesso a questo file, l'amministratore di rete sarà in grado di rilevare detta attività, perché, per cambiarsi in un altro utente, gli strumenti fanno uso della riga di comando stessa.

Come scoprire attacchi al server

Dopo aver esaminato le modalità d'intrusione degli hacker, gli amministratori possono quindi configurare i loro server e GFI LANguard S.E.L.M. in modo da coglierli con le mani nel sacco.

Fase 1: configurazione del server web ai fini del controllo di oggetti

Per monitorare file usati comunemente, sui server web di Windows va abilitato il controllo degli oggetti.



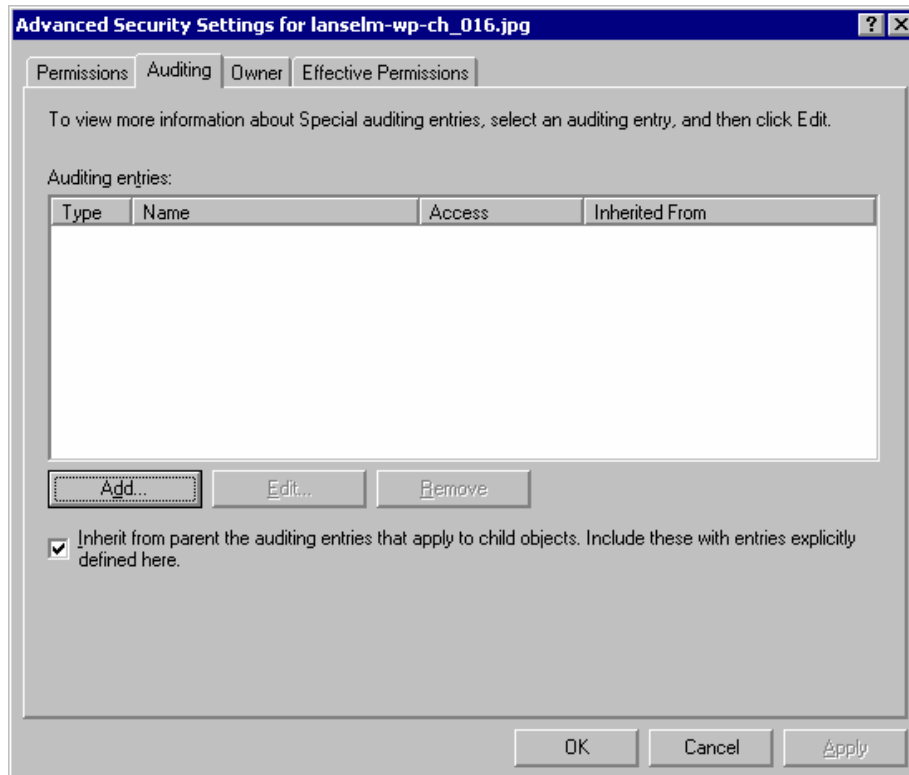
Politica di controllo – accesso all’oggetto

Se il server web è un server indipendente, per abilitare il controllo degli oggetti bisogna:

1. Aprire Administrative Tools – Local Security Policy (“Strumenti di amministrazione” – Politica di sicurezza locale)
2. Selezionare Local Policies (“Politiche locali”) e quindi Audit Policy (“Politica di controllo”)
3. Fare doppio clic su Audit Object Access (“Controlla accesso all’oggetto”) e selezionare Success and Failure (“Riuscito” e “Non riuscito”).

Se il server web fa parte del dominio, bisogna abilitare il controllo dell’oggetto come Domain Policy (“Politica del dominio”), invece che come semplice Local Policy (“Politica locale”). Tale operazione si esegue con le stesse modalità, tramite Administrative Tools – Domain Security Policy (“Strumenti di amministrazione” – Politica di sicurezza del dominio”).

Una volta compiuta tale operazione, bisogna specificare i file che si desidera controllare. In questo esempio si vogliono controllare: cmd.exe, ftp.exe, net.exe, ping.exe e tftp.exe.

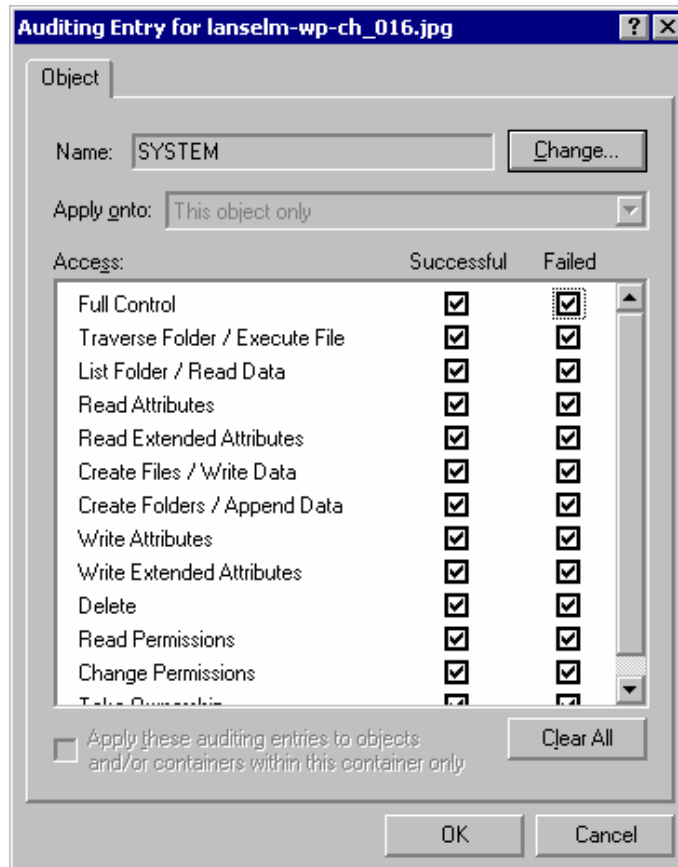


La scheda Auditing (“Controllo”)

Per abilitare il controllo di accesso all’oggetto, affinché registri ogni tentativo di eseguire cmd.exe da parte dell’account di SISTEMA e dell’account ospite di Internet, procedere come segue:

1. Fare clic con il tasto destro del mouse su cmd.exe e selezionare Properties (“Proprietà”)
2. Quindi selezionare la scheda Security (“Sicurezza”) e fare clic su Advanced (“Avanzate”)
3. Selezionare la scheda Auditing (“Controllo”) e fare clic su Add (“Aggiungi”)
4. È ora possibile inserire gli utenti che devono essere registrati quando tentano di accedere all’Oggetto (cmd.exe): selezionare l’account di SISTEMA
5. Per abilitare il controllo completo su cmd.exe dell’account di SISTEMA, selezionare tutte le opzioni Successful (“Riuscito”) e Failed (“Non riuscito”)
6. Premere OK, selezionare Add (“Aggiungi”) e ripetere l’operazione per l’account IUSR.
7. Questa procedura va eseguita per ftp.exe, net.exe, ping.exe e tftp.exe.

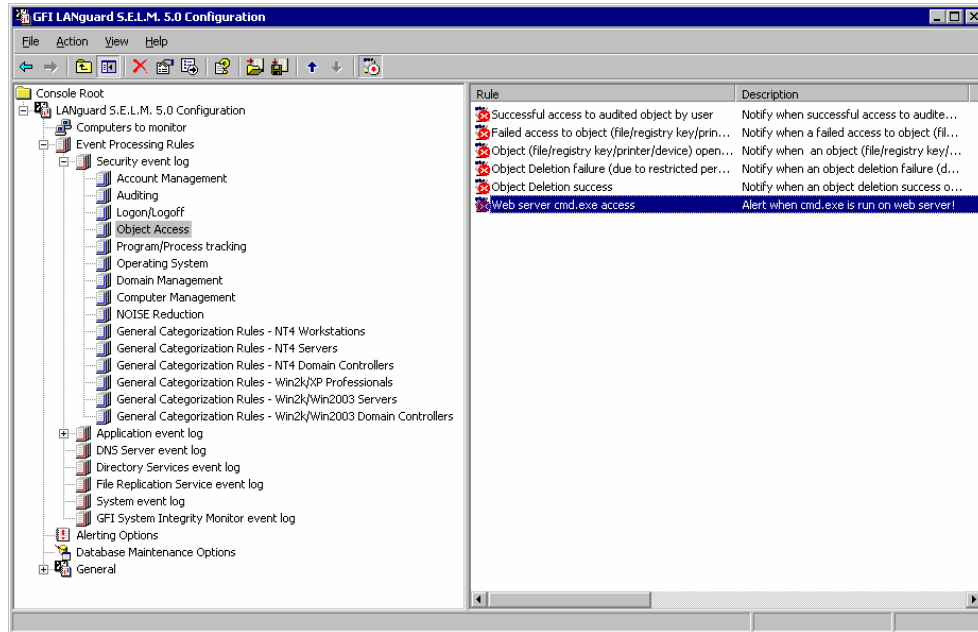
D’ora in poi l’accesso ai suddetti file da parte degli account di Sistema o IURS verrà registrato nel log degli eventi della sicurezza.



Configurazione del controllo

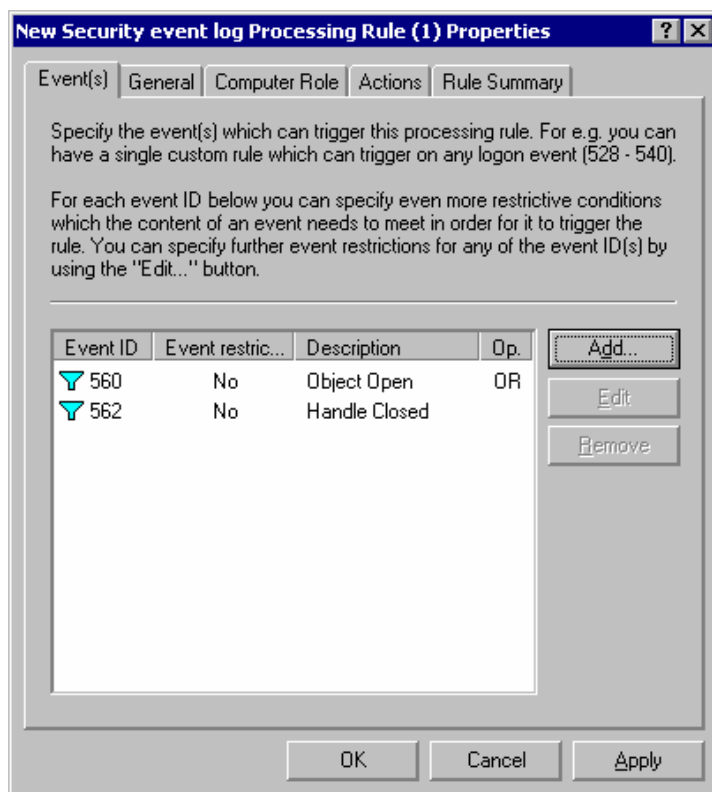
Fase 2: configurazione di GFI LANguard S.E.L.M. ai fini del monitoraggio di questi eventi e dell'invio di messaggi di allerta all'amministratore

Dopo aver configurato il controllo di accesso ai file, bisogna configurare GFI LANguard S.E.L.M. perché rilevi questi eventi della sicurezza:



Console di configurazione di GFI LANguard S.E.L.M.

1. Nel pannello di Configurazione di GFI LANguard S.E.L.M., assicurarsi che il server web risulti elencato nel nodo dei computer da controllare.
2. Passare ora al nodo Event Processing Rules > Security Event Log > Object Access (“Regole di elaborazione degli eventi > Log degli eventi di sicurezza > Accesso all’oggetto”). Selezionare il nodo, fare clic su di esso con il tasto destro del mouse e selezionare New > Processing rule (“Nuova > Regola di elaborazione”)
3. Fare clic su “aggiungi” e aggiungere gli eventi nn. 560 e 562. Questi eventi identificheranno un’intrusione. Evento 560: Object Open (“Oggetto aperto”) – significa che si è verificato un accesso all’oggetto (per esempio, è stato eseguitocmd.exe) ed Evento 562: Handle Closed (“Oggetto chiuso”) – significa che l’oggetto non è più in uso (ad esempio, Cmd.exe è stato chiuso)
4. Per impostazione predefinita, tale regola verrà applicata su tutti i computer monitorati da GFI LANguard SELM. Per specificare il solo server web, aprire la scheda general (“Generale”) e specificare il nome del computer server web. Specificare inoltre una descrizione dettagliata.
5. Fare clic su OK per aggiungere la regola.



Creazione di una nuova regola di accesso all'oggetto

GFI LANguard S.E.L.M. monitorerà ora i server web alla ricerca di tali eventi e qualora fosse eseguito il file CMD.exe, si verrà avvertiti immediatamente!

Fase 3: verifica dei nuovi ID

Una volta configurato quanto descritto in precedenza, è possibile testarlo. Si può effettuare tale test creando un nuovo script ASP. Se le politiche di controllo sono state impostate in maniera opportuna e si è abilitato l'accesso all'oggetto sui file indicati, tale script creerà ed attiverà una regola di controllo dell'oggetto. GFI LANguard S.E.L.M acquisirà quindi dal log degli eventi della sicurezza l'evento generato e, in virtù dell'esistenza di una regola corrispondente, invierà un messaggio email di allerta all'amministratore per informarlo che si è verificato un accesso al file cmd.exe.

Lo script riportato di seguito si limiterà semplicemente ad eseguire cmd.exe e a creare un elenco di directory di C:\ in background. Si può collocare questo file sul proprio server IIS e provare ad accedervi tramite il browser web.

```
<%@ Language=VBScript %>
<%' -----
' SELM_test.asp : utilizzato per provare Languard S.E.L.M
```

```
' a cura di : 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>  
You should now receive an alert from GFI LANguard S.E.L.M  
</BODY>  
<HTML>
```

Questo script ASP può essere scaricato dal sito: <ftp:gfi.com/testselm.zip>

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

GFI LANguard Security Event Log Monitor (S.E.L.M.) esegue la scoperta d'intrusione basata sui log degli eventi e la gestione dei log degli eventi di tutta la rete. GFI LANguard S.E.L.M. archivia ed analizza i log degli eventi di tutte le macchine della rete e avverte in tempo reale di eventuali problemi di sicurezza, attacchi ed altri eventi critici. L'analisi intelligente di GFI LANguard S.E.L.M. implica che non è necessario essere dei 'guru degli eventi' per poter: controllare gli utenti che tentano di accedere alle condivisioni protette e ai file confidenziali; controllare i server critici e creare messaggi di allerta per eventi e condizioni specifici che si verificano sulla rete; copiare ed eliminare in modo automatico i log degli eventi su macchine remoti; scoprire gli attacchi che utilizzano account di utenti locali e molto altro!

Per ulteriori informazioni su GFI LANguard S.E.L.M. e per scaricare una versione di prova gratuita, visitare <http://www.gfi-italia.com/italia/lanselm/>.

Informazioni su GFI

GFI è una società leader nello sviluppo di software, che offre agli amministratori di rete un'unica fonte in grado di soddisfare le loro esigenze di protezione della rete, sicurezza del contenuto e messaggistica. Grazie alla tecnologia vincitrice di numerosi riconoscimenti, ad una politica tariffaria aggressiva e alla particolare attenzione rivolta alle piccole e medie aziende, GFI riesce a soddisfare le esigenze di continuità e produttività aziendali delle organizzazioni in generale. Costituita nel 1992, GFI ha uffici a Malta, Londra, Raleigh, Hong Kong, Adelaide, e Amburgo, a supporto di oltre 200.000 installazioni in tutto il mondo. GFI è orientata alla collaborazione con partner e si avvale infatti di oltre 10.000 partner in tutto il mondo. GFI è inoltre Microsoft Gold Certified Partner. Maggiori informazioni su GFI sono reperibili sul sito <http://www.gfi-italia.com>.

© 2007 GFI Software. Tutti i diritti riservati. Le informazioni contenute nel presente documento rappresentano l'attuale conoscenza della GFI, in merito agli argomenti trattati, alla data di pubblicazione. A causa di cambiamenti nelle condizioni di mercato, non deve essere considerato in alcun modo un impegno da parte di GFI, e GFI non può garantire l'esattezza delle informazioni fornite dopo la data di pubblicazione. Questa white paper deve essere considerata a puri fini informativi. GFI NON OFFRE GARANZIE, ESPLICITE O IMPLICITE, NEL PRESENTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor e i rispettivi loghi sono marchi registrati o marchi di GFI Software negli Stati Uniti e/o in altri paesi. Tutti i prodotti e le aziende nominate nel presente documento sono marchi registrati dei rispettivi proprietari.

