

SISTEMI DI ELABORAZIONE SU RETI:
SICUREZZA SU RETI

GESTIONE DEI LOG DEGLI EVENTI

CUDA MONICA
56/100138

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANGuard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

PERCHE' GESTIRE I LOG PROBLEMATICHE DI SICUREZZA

- Molti sono i siti web vulnerabili che utenti pericolosi trovano su Internet.
- Pochi attacchi di hacker sono immediatamente riconoscibili come tali.
- Molti intrusi utilizzano il server web manipolato come base di lancio di attacchi nei confronti di server web molto più importanti o popolari.

PERCHE' GESTIRE I LOG IL DETECTIVE DEI LOG

- Nel caso di trasmissione di malicious code o virus, o nel caso di tentato accesso fraudolento, le aziende devono poter bloccare il traffico non autorizzato.
- Se analizzati correttamente, i log dei firewall possono evidenziare attacchi di Denial of Service o altre attività sospette.
- La firewall log analysis è un'operazione molto complessa che richiede il controllo simultaneo di migliaia di eventi.

PERCHE' GESTIRE I LOG FIREWALL MANAGEMENT

- Molti MSSP (Managed Security Service Provider) semplicemente informano il cliente dell'irregolarità nel file di log e suggeriscono l'azione preventiva da intraprendere.
- Spesso le aziende non sono in grado di effettuare le opportune modifiche dei firewall.
- La gestione remota delle firewall policy è una componente critica dei servizi di sicurezza gestiti.

PERCHE' GESTIRE I LOG GESTIONE DEI LOG SULLA RETE

- Le tecnologie multiplatforma differiscono per:
 - Meccanismi di log ,
 - Sintassi,
 - Strumenti di GUI e di amministrazione,
 - Comandi di reportistica
 - Completamente indipendenti l'uno con l'altro.
- E' necessario avere un sistema che conosce tutti i formati dei log, li analizza e crea un database degli eventi per memorizzarli uniformati in sintassi.

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANguard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

SCOPRIRE GLI HACKER

STRUMENTI DI LAVORO DEGLI HACKER

- Esistono molti strumenti a disposizione degli hacker che vogliono "imbrattare" un sito web.
- L'exploit Internet Printing Protocol (IPP)
- Gli exploit di UNICODE e CGI-Decode
- Applicazioni personalizzate

SCOPRIRE GLI HACKER

MONITORAGGIO DI FILE DI SISTEMA

- I file di sistema che gli hacker utilizzano di frequente sono:
 - cmd.exe
 - ftp.exe
 - net.exe
 - ping.exe
 - tftp.exe

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANguard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

I LOG DI UNIX

SYSLOG E LOG DEI SISTEMI UNIX

- I log del sistema vengono generalmente scritti in directory come **/var/log** e **/var/adm** o dove definito nei file di configurazione dei singoli programmi.
- In quasi tutti i sistemi Unix il demone **syslogd** si occupa della gestione dei log tramite il file di configurazione **/etc/syslog.conf**.
- Le recenti distribuzioni Linux utilizzano **syslogd**, una versione evoluta di **syslogd** che gestisce anche il logging del kernel (tramite il demone **klogd**).

I LOG DI UNIX

INTRODUZIONE A LOGWATCH

- Logwatch e' uno strumento che permette l'analisi e il monitoraggio dei log.
 - semplice,
 - versatile
 - flessibile
- I file e le directory principali di logwatch sono generalmente:
 - /etc/log.d/conf/logwatch.conf
 - /etc/log.d/conf/services/
 - /etc/log.d/conf/logfiles/
 - /etc/log.d/scripts/shared/
 - /etc/log.d/scripts/logfiles/
 - /etc/log.d/scripts/services/

I LOG DI UNIX

LOGROTATION E ARCHIVIAZIONE DEI LOG

- Le dimensioni dei log possono crescere a dismisura in pochissimo tempo, fino a saturare il filesystem.
- **Logrotate** semplifica l'amministrazione dei log, permette di comprimere, rimuovere ed inviare il log via mail, esegue una rotazione di file.
- Il file di configurazione è **/etc/logrotate.conf**

I LOG DI UNIX

COLORIZE: VISUALIZZAZIONE COLORATA DEI LOG

- Colorize è un piccolo script, di **Karaszi Istvan** e rilasciato sotto **GPL**, scritto in linguaggio **Perl**.
- Permette di visualizzare i **log**, con una sintassi **colorata** in modo da renderli più facilmente leggibili.
- E' possibile eseguire il download dal sito dell'autore:
http://colorize.raszi.hu/downloads/colorize_0.3.4.tar.gz
- Una volta scaricato lo script è sufficiente scompattarlo:
tar xvzf colorize_0.3.4.tar.gz

I LOG DI UNIX

STAMPA DEI LOG

- È consigliato salvare on-the-fly i log su un dispositivo fisico esterno alla memoria del pc, che potrebbe essere manomessa.
- Ecco un esempio per tener d'occhio i log del kernel in real time:
tail -f /var/log/messages | grep -v "Inbound" > /dev/lp0

I LOG DI UNIX

LOGROTATE

- Logrotate permette di comprimere, rimuovere ed inviare via mail i file di log in base a:
 - **criteri temporali**
 - **dimensioni.**
- Logrotate utilizza **/var/lib/logrotate/status** per tenere traccia dei log elaborati e **/etc/logrotate.conf** per quanto riguarda la configurazione.

I LOG DI UNIX

/etc/syslog.conf

- E' il file di configurazione principale del demone syslog.
- Il file si puo' suddividere in due campi, suddivisi da uno o piu' spazi bianchi o TAB:
 - **ACTION**:Identifica il "logfile" dove vengono scritti i log corrispondenti.
 - **SELECTOR**:
 - **facility** (identifica chi o cosa ha prodotto il messaggio)
 - **priority**(identifica il livello di priorit  del messaggio)

I LOG DI UNIX

/etc/logrotate.conf

- E' il file principale riguardante la configurazione di logrotate.
-   possibile definire il comportamento dell'applicazione in due contesti:
 - **livello globale**
 - **livello locale**
- Tra le direttive pi  utili:
 - Criteri di rotazione
 - Compressione
 - Gestione file
 - Configurazione
 - Operazioni pre-log e post-log

Indice

- Perché gestire i log
 - Scoprire gli hacker su server web
 - I log di Unix
 - I log di Apache
 - GFI LANguard S.E.L.M.
 - Security Report NEXA
 - ACP Profiler
 - Link
-

I LOG DI APACHE

LOG DI ERRORE E LOG DI ACCESSO

- Apache tiene traccia di tutte le richieste http eseguite al server web.
 - Generalmente su un server web si prevedono 2 diversi tipi di log:
 - Error_log: Contiene traccia di tutti gli errori incontrati da Apache.
 - Transfer_log: Vengono registrate tutte le richieste HTTP fatte al server dai client in rete.
-

I LOG DI APACHE

ANALISI DEL TRAFFICO WEB: STRUMENTI E FUNZIONI

- Il tipo di informazioni loggate da un server web sono, per ogni file servito:
 - data e ora della richiesta,
 - IP del client remoto,
 - client utilizzato,
 - URL della pagina che ha il link al file richiesto,
 - nome del file.
 - Esistono in circolazione una moltitudine di log analyzers, gratuiti o a pagamento.
-

I LOG DI APACHE

CUSTOMIZZARE IL FORMATO DEI LOG

- Apache permette di scrivere nei propri log di accesso una serie di informazioni relative ad ogni richiesta fatta via HTTP.
 - Con la direttiva **LogFormat** si assegna un nickname al log e si decide il formato dei dati che deve contenere.
 - LogFormat formato
 - LogFormat formato nickname
-

I LOG DI APACHE

LOGROTATION E ARCHIVIAZIONE DEI LOG

- **Cronolog** rende particolarmente semplice la segmentazione di log in file diversi generati secondo unità di tempo configurabili.
 - Il vantaggio è di sollevare l'amministratore dalla pratica di gestione e archiviazione dei log, che se non automatizzata può portare a file system riempiti al 100%, file di log enormi, perdita di dati e simili contrattempi.
-

I LOG DI APACHE

UTILIZZO DEI PIPED LOG

- Una funzionalità del sistema di logging di Apache è la possibilità di inviare i dati di un log ad un programma, tramite una normale pipe, invece che scriverli direttamente su un file.
 - Il programma che riceve il log in standard input potrà processarli e scriverli in standard output secondo criteri assolutamente gestibili.
 - Va notato che il programma a cui si passano i log viene eseguito con i permessi di root.
-

I LOG DI APACHE

NON LOGGARE LE IMMAGINI SU APACHE

- Il trasferimento loggin di Apache scrive una riga di log per ogni oggetto richiesto dai client.
- In alcuni siti può essere utile evitare di scrivere innumerevoli righe di log per tutte le immagini richieste e limitare il logging alle pagine html o simili.
- Per farlo si possono usare alcune caratteristiche evolute della direttiva che può eseguire controlli e decisioni sulla base delle variabili d'ambiente.

I LOG DI APACHE

GESTIRE LA ROTAZIONE DEI LOG SU APACHE

- Il processo di ruotare i log su Apache, se fatto manualmente, richiede una certa attenzione, ma può essere automatizzato con script e tool specifici.
- La procedura manuale, richiede un riavvio del server web.
- Può essere automatizzata direttamente in configurazione con filtri come **Cronolog** o il comando **rotatelog**.
- Alternativamente si possono usare programmi come **LogRotate** che gestiscono la rotazione di ogni tipo di log.

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANGuard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

GFI LANGUARD S.E.L.M.

INFORMAZIONI SU GFI

- GFI è un produttore di software per la sicurezza della rete, del contenuto e per la messaggistica.
- Uno dei prodotti di GFI è GFI LANGuard S.E.L.M. il quale è munito di un motore per l'analisi degli eventi della sicurezza che tiene conto:
 - del tipo di evento di sicurezza,
 - del livello di protezione di ciascun computer,
 - di quando l'evento è accaduto,
 - del ruolo del computer
 - del suo sistema operativo.

GFI LANGUARD S.E.L.M.

SCOPRIRE GLI HACKER SUL SERVER WEB

- Configurare i server e GFI LANGuard S.E.L.M.:
 - Fase 1: configurazione del server web ai fini del controllo di oggetti
 - 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
 - Fase 3: verifica dei nuovi ID

GFI LANGUARD S.E.L.M.

FUNZIONAMENTO DI GFI LANGUARD S.E.L.M.

- **Panoramica sull'architettura**
 - GFI LANGuard S.E.L.M. utilizza la normale tecnologia Windows
 - L'amministratore installa GFI LANGuard S.E.L.M. su un solo computer host e, poi, si limita a registrare tutti gli altri sistemi da controllare.
 - L'agente di raccolta
 - utilizza le API di Win32 native per raccogliere eventi della sicurezza dai computer controllati
 - archivia gli eventi in un database Microsoft Access oppure su un server Microsoft SQL

GFI LANGUARD S.E.L.M.

FUNZIONAMENTO DI GFI LANGUARD S.E.L.M.

■ **Panoramica sull'architettura**

- L'Alerter Agent di GFI LANGuard
 - confronta gli eventi raccolti con una tabella di Regole di Categorizzazione
 - classifica gli eventi a bassa sicurezza, media sicurezza, sicurezza elevata o critici.

- L'Alerter Agent invia notifiche SMTP relative ad eventi critici ad un indirizzo email configurato dall'amministratore

GFI LANGUARD S.E.L.M.

FUNZIONAMENTO DI GFI LANGUARD S.E.L.M.

■ **Controllo in tempo reale e categorizzazione degli eventi di sicurezza**

- Il cuore della capacità di informativa di GFI LANGuard S.E.L.M. è costituito dal nodo delle Regole di elaborazione degli eventi.

- Le regole di categorizzazione della sicurezza predefinite sono progettate per riconoscere eventi importanti.

- Gli amministratori possono adeguare le regole di elaborazione alle esigenze e caratteristiche specifiche della rete.

GFI LANGUARD S.E.L.M.

FUNZIONAMENTO DI GFI LANGUARD S.E.L.M.

■ **Controllo delle stazioni di lavoro e dei server su tutta la rete**

- Ogni evento include una descrizione che spiega cosa l'evento potrebbe indicare e suggerisce le azioni da intraprendere.

- Occorre considerare
 - il livello di sicurezza relativa del computer,
 - il potenziale carico di prestazioni
 - le necessarie tempistiche dei messaggi di allerta
 - gli scenari di rischio specifici dell' ambiente.

GFI LANGUARD S.E.L.M.

SELEZIONARE I LIVELLI DI SICUREZZA

- GFI LANGuard S.E.L.M. si affida all'amministratore per selezionare il livello di sicurezza idoneo di ogni computer controllato.

- Le stazioni di lavoro di utenti che hanno accesso a risorse importanti dovrebbero essere configurate come a rischio di sicurezza elevato.

- Le stazioni di lavoro di utenti che hanno scarso accesso ad informazioni o procedure critiche dovrebbero essere configurate come a basso rischio di sicurezza.

- La classificazione nel medio rischio di sicurezza può essere utilizzata per le stazioni di lavoro di utenti che rientrano fra questi due estremi.

GFI LANGUARD S.E.L.M.

EQUILIBRARE IL CONSUMO DI RISORSE

- La frequenza di raccolta degli eventi si ripercuote sull'utilizzo della CPU dei computer e sulla complessiva larghezza di banda della rete.

- Maggiore è il livello di sicurezza di un computer, maggiore sarà la frequenza di interrogazione del computer stesso.

GFI LANGUARD S.E.L.M.

GESTIRE MANUTENZIONE E INTEGRITA' DEI LOG

- Windows registra fedelmente uno specifico evento ogniqualvolta il log viene cancellato.

- GFI LANGuard S.E.L.M. cancella automaticamente il log della sicurezza, perciò la cancellazione manuale del log non è mai necessaria.

- Gli amministratori devono configurare la dimensione massima del log della sicurezza di ciascun sistema.

- Windows può essere configurato in modo da bloccarsi quando il log della sicurezza si riempie.

GFI LANGUARD S.E.L.M.

CONTROLLO DI ACCESSO AI FILE PER LA SICUREZZA

- Il controllo dei file di Windows consente agli amministratori di abilitare il controllo su file selezionati per determinati tipi di accesso.
- GFI LANGuard S.E.L.M. offre la capacità di promuovere eventi di accesso all'oggetto connessi a file o directory importanti
- Maggiore è il numero di oggetti controllati, maggiore sarà il consumo di tempo della CPU, larghezza di banda della rete e spazio sul disco.

GFI LANGUARD S.E.L.M.

RILEVARE L'INTRUSIONE

- Un server web configurato secondo la migliore prassi conterrà cartelle di file HTML, ASP e d'immagini chiaramente definite.
- Per essere informato di modifiche al sito web, l'amministratore deve:
 - Configurare Windows perché controlli modifiche riuscite a tali directory
 - Configurare GFI LANGuard S.E.L.M. affinché promuova gli eventi di accesso collegati ai nomi dei file presenti in dette directory.

GFI LANGUARD S.E.L.M.

CONCLUSIONI

- Windows contiene una funzionalità di "cattura" degli eventi della sicurezza completa, ma offre poco in materia di analisi, archiviazione e capacità di controllo in tempo reale.
- GFI LANGuard S.E.L.M. si aggiunge ai controlli di base di Windows per offrire un modo semplice da impiegare, per soddisfare tali esigenze.

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANGuard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

SECURITY REPORT NEXA

SECURITY REPORT

- SecurityReport è il servizio per la raccolta e l'analisi delle Statistiche, dei Report e degli Attacchi relativi alla Sicurezza aziendale.
- L'obiettivo principale è rendere molto più semplice l'identificazione e la relativa soluzione di vulnerabilità disperse su installazioni di apparati multipli.
- Il servizio SecurityReport, erogato dalla sede Nexa, è consultabile tramite una interfaccia grafica intuitiva, completa di grafici statistici e report chiari e concisi.

SECURITY REPORT NEXA

CARATTERISTICHE DEI REPORT

- Sono disponibili ben 11 categorie di Report con più di 140 report, la cui generazione è flessibile e completamente configurabile.
- I parametri dei Report definibili sono:
 - il periodo
 - le query
 - i filtri
 - periodo di schedulazione delle elaborazioni
 - i formati dei dati in uscita
- Le notifiche delle analisi dei Report possono essere configurate:
 - per singolo dispositivo
 - per tutti i dispositivi (qualora fossero presenti più apparati o più sedi dotate di firewall)

SECURITY REPORT NEXA

GESTIONE DEI LOG

- Il sistema permette una Gestione dei Log completa di:
 - Esportazione ed importazione dei Log per una corretta storicizzazione e visualizzazione degli stessi
 - Analisi degli eventi divisi per tipologie
 - Notifica tramite E-mail per gli Eventi reimpostati, tipicamente per gli attacchi critici.
 - Integrazione con le regole di privacy HIPAA e con altre regole definite dai Clienti

SECURITY REPORT NEXA

CORRELAZIONE ATTACCHI ED EVENTI

- Il sistema fornisce un veloce reperimento, grazie ad una grafica user-friendly, delle seguenti informazioni relative agli attacchi:
 - localizzazione degli attacchi provenienti dalla stessa fonte/sorgente
 - localizzazione di tutti i target (obiettivi) dello stesso attacco
- Il risultato concreto è l'efficacia di gestione della rete grazie alla possibilità di isolare gli attacchi ed identificare rapidamente le modalità di risoluzione dei problemi.

Indice

- Perché gestire i log
- Scoprire gli hacker su server web
- I log di Unix
- I log di Apache
- GFI LANguard S.E.L.M.
- Security Report NEXA
- ACP Profiler
- Link

ACP PROFILER

OVERVIEW

- Monitorare il funzionamento delle applicazioni è un'attività tanto più critica quanto più l'applicazione gestisce processi "core" per l'azienda.
- Ancora più importante è analizzare il comportamento degli utilizzatori dell'applicazione soprattutto se si tratta di applicazioni web che sono a disposizione dei clienti.
- La fase di elaborazione dei dati dei log riveste un ruolo fondamentale. Il risultato delle elaborazioni deve essere memorizzato in strutture dati accessibili in modo assolutamente trasparente.

ACP PROFILER

DESCRIZIONE TECNICA

- ACP Profiler è una libreria configurabile mediante file XML, facilmente estendibile ed integrabile in ogni applicazione realizzata in linguaggio Java.
- In ACP Profiler gli eventi sono organizzati in canali/ambienti diversi.
- Ad ogni canale/ambiente può corrispondere:
 - una comunità,
 - un servizio,
 - un contenuto,
 - una comunicazione,
 - o qualsiasi altro elemento logico dell'applicazione.
- ACP Profiler si affida ad un indice destrutturato per memorizzare gli eventi, i metadati e le informazioni.

ACP PROFILER

CARATTERISTICHE

- Realizzata completamente con tecnologia Java ed XML (SDK java 1.4.1)
- Interfaccia di programmazione del server basata su API Java.
- Rappresentazione dei log con template XML personalizzati.
- Gestione di canali/ambienti gerarchici.
- Gestione di tracciati log personalizzati
- Generazione di indicatori statistici
- Rilevazione di eventi secondo criteri definiti dall'utente.
- Generazione di output tabellari.

Indice

- Perché gestire i log
 - Scoprire gli hacker su server web
 - I log di Unix
 - I log di Apache
 - GFI LANguard S.E.L.M.
 - Security Report NEXA
 - ACP Profiler
 - Link
-

LINK UTILI

- News ed articoli sul problema della sicurezza
<http://www.dolmen.it/retiesistemi.asp>
 - Articolo: "MSS: gestione e sicurezza vanno a braccetto" di Lorenzo Grillo da web magazine online
<http://www.nwi.it/showPage.php?template=rubriche&id=4651>
 - corsi e servizi LINUX
<http://openskills.info/topic.php?ID=28>
 - Guide e manuali per webmaster:
Guida ad apache
http://www.risorse.net/apache/analisi_log.asp
 - Le informazioni riguardanti i tre applicativi sono state reperite dai siti delle rispettive aziende:
 - GFI LANguard S.E.L.M.
<http://www.gfi-italia.com>
 - Security report NEXA
<http://www.nexa.it>
 - ACP Profiler
<http://www.acpnet.it>
-