Auditing di Eventi

Daniele Di Lucente

Un caso che potrebbe essere reale

- Un intruso è riuscito a penetrare nella rete informatica della società XYZ.
- Chi è l'intruso? Come ha fatto ad entrare?
- Quali informazioni avrà carpito? Sarà ancora in grado di fare danni?

Il Problema

- Perché una strategia di sicurezza sia efficace è necessario tener traccia di determinati eventi
- Spesso si apprende ciò nel modo peggiore – dopo un incidente di sicurezza
- Come è possibile investigare sulle cause e sugli effetti di un'intrusione?

La Soluzione

- Una politica di **Auditing (*controllo)*** permette di:
  - Creare una linea base per le normali attività di network e computer
  - Segnalare tentativi di intrusione nella rete o nel computer
  - Accertare quali sistemi e quali dati sono stati compromessi durante o dopo un incidente di sicurezza
  - Limitare i danni conseguenti ad un intrusione
  - Rispondere ad eventuali requisiti di legge

Determinare gli eventi da controllare

- Il primo passo per creare una politica di auditing è scegliere *quali* eventi monitorare
- La risposta più facile sarebbe *tutti*, ma non è una soluzione proponibile:
  - Comporterebbe un'enorme richiesta di risorse di sistema
  - Con il crescere del numero diventa più difficile individuare gli eventi *critici* tra quelli registrati
- Un metodo efficace per stabilire una politica è decidere e poi tradurre in specifiche politiche:
  - Le azioni o le operazioni di cui si vuole tener traccia
  - I sistemi su cui si vuole registrare la traccia di questi eventi

Success e Failure Events

- Gli eventi di auditing possono essere divisi in due categorie:
  - **Success Events**, che indicano operazioni completate con successo dal sistema operativo
  - **Failure Events**, che indicano tentativi di operazioni non riusciti

Success e Failure Events

- I Failure Events sono molto utili per tenere traccia di tentati attacchi
- I Success Events sono più difficili da interpretare
  - La gran parte di questo tipo di eventi sono una semplice indicazione di normale attività
  - Ma anche un intruso che riesce ad entrare in un sistema genererà un Success Event!

Success e Failure Events

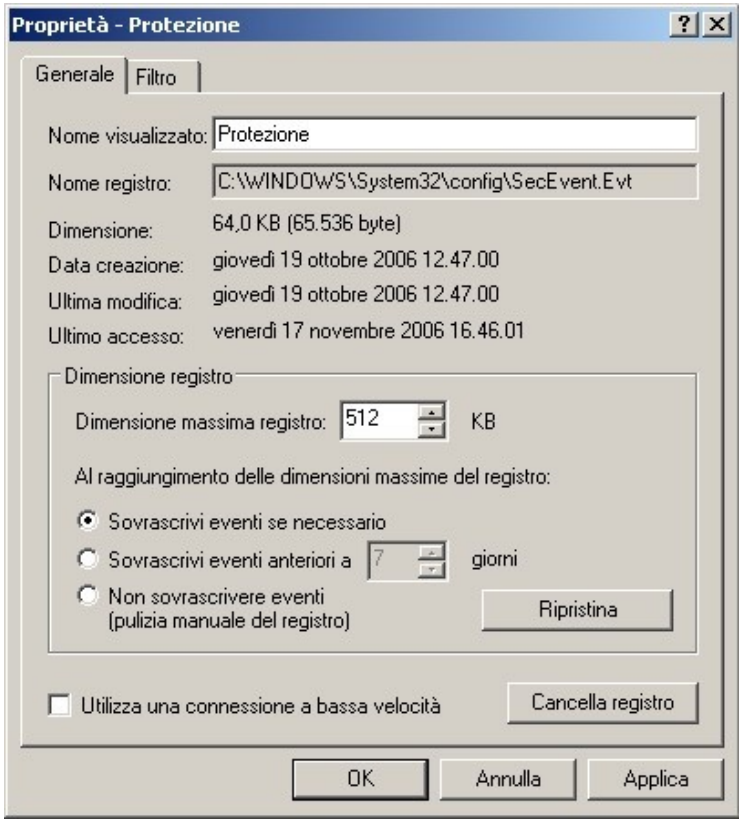
- Oltre agli eventi in se, può essere importante lo **schema** degli eventi
  - Una serie di Failure Events seguita da un successo potrebbe indicare un attacco andato a buon fine
  - Anche la deviazione da uno schema abituale può indicare attività sospetta
  - Ad esempio, Login occasionali di utenti in orari non abituali potrebbero indicare attacchi e vanno quindi investigati

Gestire il Visualizzatore di Eventi

- Tutti gli eventi di sicurezza del sistema operativo sono registrati nel **Registro di Sicurezza del Visualizzatore di Eventi** (*Event Viewer Security log)*
- Eventi addizionali relativi alla sicurezza possono essere registrati nel **Registro Applicazioni** e nel **Registro Sistema**
- Prima di abilitare politiche di auditing, si deve valutare se le configurazioni di default del registro sono impostate secondo le esigenze

Impostazioni dei Registri di Eventi

- Per ogni Registro di Eventi, si devono determinare:
  - **Locazione di Memorizzazione**
  - **Dimensione Massima del file del Registro**
  - **Politica di sovrascrittura**



Determinare la Locazione di Memorizzazione

- Il Registro di Eventi di Sicurezza è memorizzato di default nella cartella **%systemroot%\system32\config** in un file chiamato **SecEvent.evt**
- La posizione di ogni file di registro può essere modificata editando il valore di registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security
- Solo l'account di Sistema e il gruppo Amministratori hanno accesso al registro eventi di sicurezza

Determinare la Dimensione Massima dei File di Registro

- La dimensione predefinita che un file può raggiungere prima che si inserisca una politica di sovrascrittura è
  - **16 MB** in Windows Server2003
  - **512 KB o superiori** in Windows XP e 2000
- Data la maggior disponibilità di spazio attuale, è preferibile impostare la dimensione massima ad almeno **50 MB**

Determinare la Dimensione Massima dei File di Registro

- La dimensione complessiva di tutti i file di registro non dovrebbe superare i **300 MB**
- Ogni evento di sicurezza pesa tra i **350** e **500** bytes
  - Perciò un registro eventi di **10 MB** conterrà da **20,000** a **25,000** eventi di sicurezza

Determinare la Dimensione Massima dei File di Registro

- La dimensione massima di un File di Registro può essere modificata:
  - Su computer individuali
    - Impostandola nella pagina delle proprietà del file di registro
    - Editando la voce di registro HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\Security \Maxsize
  - Su più computers usando un template di politica di gruppo

Configurare la politica di Sovrascrittura

- Quando il File di Registro raggiunge la dimensione massima sono disponibili tre politiche:
  - **Sovrascrivi eventi se necessario**
  - **Sovrascrivi eventi anteriori a *[x]* giorni**
  - **Non sovrascrivere eventi**
    (pulizia manuale del registro)

Spegnimento Automatico del sistema

- Se non è possibile scrivere eventi nel file di registro di sicurezza, si può impostare lo spegnimento automatico del sistema operativo
- Il computer mostrerà un *blue screen of death* con il seguente messaggio di errore:
  - STOP: C0000244 {Audit Failed}
    An attempt to generate a security audit failed

Pro e Contro dello Spegnimento Automatico

- **PRO**
  - Il computer non opererà normalmente fino all'intervento di un Amministratore
  - Assicura che tutti gli eventi siano registrati
- **CONTRO**
  - Un grande numero di eventi generati da un attacco o da un problema del network genererebbero disservizi
  - In molti casi, non è **contrattualmente** consigliabile o possibile spegnere il server (SLAs). Si dovrà implementare un metodo di pulizia automatica degli eventi di auditing

Impostare lo Spegnimento Automatico *(CrashOnAuditFail)*

- Si deve impostare il valore di registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail ad **1**
- Quando il computer si spegnerà, il valore passerà a **2**
  - Un Amministratore Locale deve entrare nel sistema e riportare il valore ad **1**
- Il valore impostato a **0** disattiva questa funzione

Configurare criteri di Auditing (Auditing Policies)

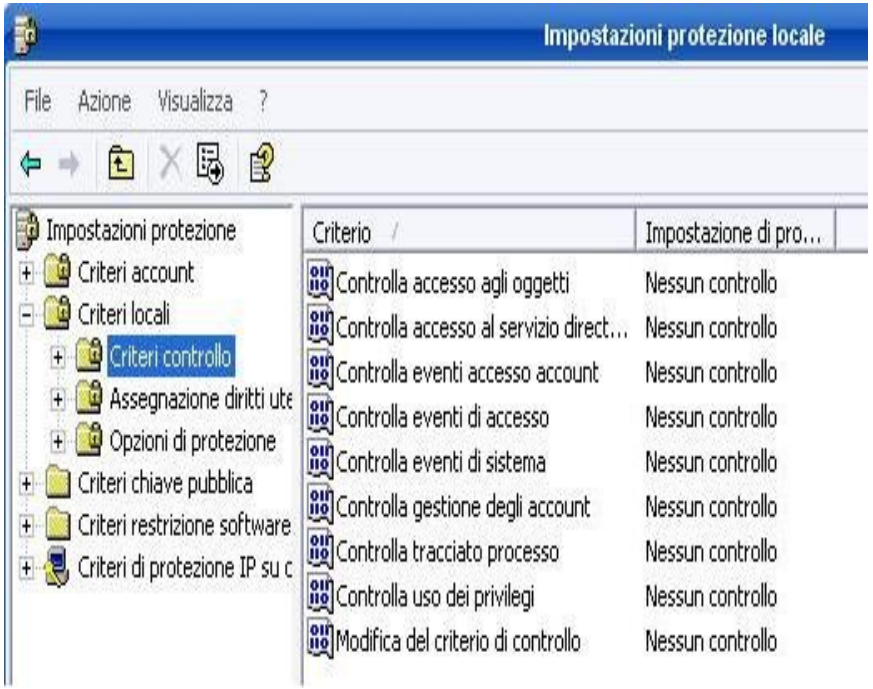
- Windows Server 2003, Windows 2000 ed XP forniscono diverse categorie di Auditing di eventi
- In un criterio di Auditing è possibile includere Failure e Success events per ciascuna categoria

Categorie di eventi

Account Logon Events	Logon o logoff ad un computer remoto
Account Management	Gestione di Account (Creazione etc.)
Directory Access	Accesso ad oggetti di Active Directory
Logon Events	Logon o Logoff / connessione di rete al computer locale
Object Access	Accesso di utente ad oggetti di sistema
Policy Change	Modifica dei criteri
Privilege Use	Utilizzo di privilegi da parte di un utente
Process Tracking	Attivazione, chiusura etc. dei processi
System Events	Chiusura o riavvio del sistema

Configurare criteri di Auditing

- Si può controllare in ogni momento lo stato dell'auditing per ogni area guardando nella **Console di gestione dei criteri di protezione locale**, negli strumenti di amministrazione



Eventi di Accesso ad Account

- L'auditing di eventi di accesso ad Account registra tentativi di Logon sul controller di dominio che valida l'utente
- Gli eventi di accesso ad account vengono generati quando un pacchetto di autenticazione valida (con successo o no) le credenziali di un utente o di un computer
  - Se vengono utilizzate credenziali di dominio, gli eventi vengono generati solo nel registro eventi dei controller di dominio
  - Se vengono utilizzate credenziali locali, gli eventi sono generati nel registro degli eventi di sicurezza del server o della workstation

Eventi di Accesso ad Account

- L'Auditing di Success Events di questa categoria fornirà un archivio degli avvenuti Logon di utenti e computer su domini e computer locali
- L'auditing dei Failure Events può essere importante nel riconoscere attacchi
  - Ad esempio, centinaia o migliaia di falliti Logon con intervalli di pochi secondi potrebbero indicare un attacco di forza bruta sulla password di un account utente

Eventi di Accesso ad Account

- Oltre ad identificare l'account oggetto del Logon (riuscito o no) , si possono identificare le seguenti informazioni:
  - Nome del computer sul quale ha avuto origine il tentativo di Logon – spesso mascherato dagli intrusi utilizzando caratteri non stampabili
  - Nome del Dominio o del computer per l'account usato da un computer di un workgroup per tentare l'attacco

Eventi di Accesso ad Account

- Tipo di tentativo di Logon

Logon Type	Name	Description
2	Interactive	Includes both logons from Terminal Services users in Windows 2000 and users who are physically at the computer
3	Network	Generally for file and print access
4	Batch	Initiated by a process with batch logon rights
5	Service	Initiated by services using the Logon As A Service right
6	Proxy	Has never been implemented by any version of the Windows operating system
7	Unlock Workstation Logon	Recorded when the console of a computer is unlocked
8	NetworkCleartext	Reserved for cleartext logons over the network
9	NewCredentials	Initiated by using the RunAs command with the /netonly switch
10	RemoteInteractive	Recorded for Terminal Services logons in Windows Server 2003 and Windows XP
11	CachedInteractive	Recorded when cached credentials are used to log on locally to a computer
13	CachedUnlock	Recorded when the computer was unlocked and the user's credentials were verified against previously cached credentials

Eventi di Accesso ad Account

- Il processo che ha originato il Logon
- Il pacchetto di autenticazione usato per il tentativo di Logon
- L'indirizzo IP e il source port in Windows Server 2003

Eventi di Accesso ad Account

- E' fondamentale controllare Failure e Success Events di questa categoria:
  - I Success Events sono indispensabili per individuare una linea base del comportamento degli utenti e possono costituire informazioni importanti per investigazioni
  - I failure events possono segnalare tentativi di intrusione e monitorandoli attivamente si possono evitare danni

Event ID	Description
672	An Authentication Service ticket was successfully issued and validated.
673	A Ticket Granting Service ticket was granted.
674	A security principal renewed an Authentication Service ticket or Ticket Granting Service ticket.
675	Kerberos preauthentication failed.
676	Authentication ticket request failed. This event is not implemented in Windows XP or Windows Server 2003.
677	A Ticket Granting Service ticket was not granted. This event is not implemented in Windows XP or Windows Server 2003.
678	An account was successfully mapped to a domain account.
679	An account failed to map to a domain account.
680	The account used for the successful logon attempt was identified. This event also indicates the authentication package used to authenticate the account.
681	A failed domain account logon was attempted. This event is not implemented in Windows XP or Windows Server 2003. Instead, event 672 is logged.
682	A user has reconnected to a disconnected Terminal Services session.
683	A user disconnected from a Terminal Services session without logging off. Terminal Services sessions can be left in a connected state that allows processes to continue running after the session ends. Event ID 683 indicates when a user does not log off from the Terminal Services session, and event ID 682 indicates when a connection to a previously disconnected session has occurred.

Eventi di Gestione Account

- Chiunque con accesso ad account amministrativi ha l'autorità di conferire ad altri account maggiori privilegi e permessi e di creare nuovi account
- Risulta chiaro che l'Auditing di Eventi di Gestione Account è fondamentale per qualsiasi strategia di sicurezza network
- Salvo sofisticati sistemi di biometrica, è molto difficile stabilire se la persona che sta usando un account amministrativo è l'utente per il quale l'account è stato creato
- Inoltre il controllo di questi eventi è uno dei modi in cui le organizzazioni possono ritenere responsabili gli amministratori per le loro azioni

Eventi di Gestione Account

- Attivando l'auditing di eventi di questa categoria, si potranno registrare eventi come questo:
  - Un account utente è creato, modificato, cancellato
  - Un account utente è rinominato, disattivato, attivato
  - Una password è impostata o cambiata
  - Un criterio di sicurezza di un computer è modificato

Eventi di Gestione Account

- Cambiare i privilegi di un utente può sembrare a prima vista un evento di Gestione Account
- In realtà è un evento di **Modifica di criteri (*Policy change)***
- Se entrambi le categorie di evento sono disattivate, un amministratore “disonesto” può sovvertire la sicurezza di un network senza lasciare traccia

Eventi di Gestione Account

- Anche i cambiamenti di criteri di sicurezza del computer sono registrati in questa categoria
  - Modifiche inaspettate potrebbero essere preludio di un attacco
  - Ad esempio un intruso potrebbe disattivare determinati criteri di sicurezza di un computer per portare a termine un attacco che richiede risorse normalmente disabilitate

Eventi di Gestione Account

- E’ buona norma attivare ambedue i Failure e i Success events di questa categoria
  - Failure events indicano spesso che un amministratore di livello più basso sta cercando di aumentare i suoi privilegi
  - Success events, anche se di norma inoffensivi, costituiscono un inestimabile archivio di attività quando un network è stato compromesso
    - Ad esempio è possibile vedere quali account sono stati creati o modificati

Eventi di Gestione Account

Event ID	Description
624	A user account was created.
627	A password change was attempted; this event records both successful and failed attempts.
632	A global group member was added.
633	A global group member was removed.
634	A global group was deleted.
635	A local group (distribution) was created.
636	A security local group member was added.
637	A local group member was removed.
638	A local group was deleted.
639	A local group was changed.
641	A global group was changed.
642	A user account was changed.
643	A domain policy was changed.
644	A user account was locked out; when an account is locked out, two events will be logged at the primary domain controller (PDC) emulator operations master. A 644 event will occur, indicating that the account name was locked out. Then a 642 event will be recorded, indicating that the user account is now locked out. This event is logged only at the PDC emulator.
645	A computer account was created.
646	A computer account was changed.
647	A computer account was deleted.
648	A local security group (distribution) was created.
649	A local security group (distribution) was changed.
650	A member was added to a local security group (distribution).
651	A member was removed from a local security group (distribution).
652	A local group was deleted (distribution).
653	A global group was created (distribution).
654	A global group was changed (distribution).

Event ID	Description
655	A member was added to a global group (distribution).
656	A member was removed from a global group (distribution).
657	A distribution global group was deleted.
658	A security universal group was created.
659	A security universal group was changed.
660	A member was added to a security universal group.
661	A member was removed from a security universal group.
662	A security universal group was deleted.
663	A distribution universal group was created.
664	A distribution universal group was changed.
665	A member was added to a distribution universal group.
666	A member was removed from a distribution universal group.
667	A distribution universal group was deleted.
668	A group type was changed.
684	The security descriptor of members of administrative groups was set. Every 60 minutes on domain controllers, a background thread searches all members of administrative groups, including domain, enterprise, and schema administrators, and reapplies the security descriptor on them. This event is logged each time the ACL is reset.
685	A name of an account was changed.

Accesso ad Oggetti di Active Directory

- Attivare gli eventi di questa categoria permette di registrare altre modifiche oltre a quelle contenute nella Gestione Account:
  - Modifica di Componenti infrastruttura di Active Directory
  - Modifica di Schemi di Active Directory
  - Modifica di oggetti dell' Enterprise Certification Authority
- Per controllare correttamente questi eventi bisogna configurare la lista di controllo di accesso al sistema (SACL) per ogni oggetto che si vuole monitorare

Accesso ad Oggetti di Active Directory

- Anche eventi di Active Directory come la replicazione vengono registrati
- Di conseguenza, attivare l'auditing dei Success Events di questa categoria comporta un notevole aumento di eventi registrati nel registro di sicurezza
- Oltre al problema delle dimensioni del file di registro, diventa più difficile individuare eventi significativi senza l'ausilio di sofisticati strumenti di analisi

Accesso ad Oggetti di Active Directory

- Tutti gli eventi di Accesso ad Oggetti di Active Directory vengono registrati con l'ID 565 o 566 nel registro di sicurezza
- Solo esaminando i dettagli di ogni evento 565 o 566 si può stabilire se sia stato completato con successo o no

Eventi di Accesso (*Logon)*

- Attivando l'auditing di questi eventi, si può controllare ogni accesso e disconnessione di un utente su una macchina
- L'evento sarà creato nel registro della macchina in cui si tenta l'accesso (o disconnessione)
- Similmente, questi eventi vengono generati quando una macchina si connette in remoto ad un'altra. Gli eventi saranno registrati nel registro della macchina remota con due voci:
  - Computer Account
  - User Account del computer che tenta l'accesso
- Se la macchina che tenta l'accesso ha come sistema operativo Windows 95 o 98 sarà registrato solo l'User Account

Eventi di Accesso

- Gli Eventi di Accesso sono utili per tenere traccia di accessi interattivi ad un server o investigare su attacchi lanciati da un particolare computer
- C'è una sottile differenza tra questi eventi e gli eventi di Accesso ad Account:
  - Gli eventi di Accesso ad Account sono registrati sulla macchina che autentica l'Account
  - Gli eventi di Accesso sono generati nella macchina in cui viene utilizzato l'Account

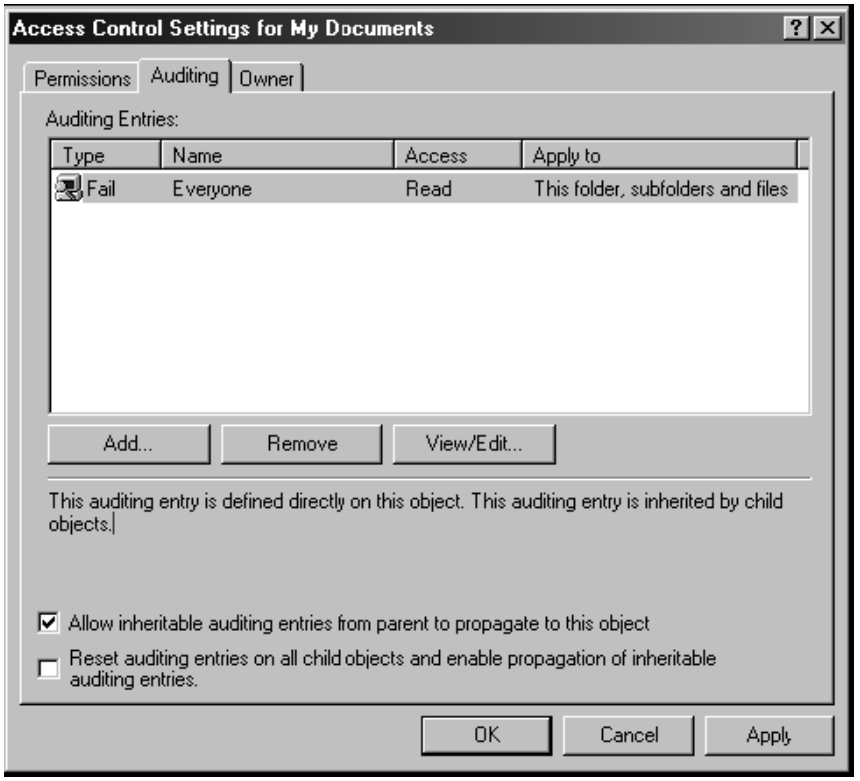
Eventi di Accesso

- Entrambi i Failure e i Success Events di questa categoria dovrebbero sempre essere attivati
  - I Success Events costituiscono una linea base di comportamento degli utenti utile per individuare comportamenti sospetti
  - Controllando i Failure Events, si possono evitare attacchi o limitare i danni di un'intrusione

Event ID	Description
528	A user successfully logged on to a computer.
529	The logon attempt was made with an unknown user name or a known user name with a bad password.
530	The user account tried to log on outside the allowed time.
531	A logon attempt was made by using a disabled account.
532	A logon attempt was made by using an expired account.
533	The user is not allowed to log on at this computer.
534	The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive.
535	The password for the specified account has expired.
536	The Netlogon service is not active.
537	The logon attempt failed for other reasons.
538	A user logged off.
539	The account was locked out at the time the logon attempt was made. This event is logged when a user or computer attempts to authenticate with an account that has been previously locked out.
540	Network logon succeeded.
682	A user has reconnected to a disconnected Terminal Services session.
683	A user disconnected a Terminal Services session without logging off.

Accesso ad Oggetti

- Abilitando l'auditing per l'accesso ad oggetti, si può tener traccia dei tentativi di accesso a risorse di file, stampa e registro
- Ogni azione genera un gran numero di eventi, quindi bisogna decidere con cura quali accessi controllare
- Come per gli oggetti di Active Directory, è necessario configurare la SACL per ogni risorsa da controllare



Configurare la SACL

- Una lista di controllo di accesso al sistema consiste di voci di controllo di accesso (ACEs) ciascuna delle quali contiene tre informazioni:
  - Security Principal da controllare (utente, computer, gruppo)
  - Lo specifico tipo di accesso da controllare (access mask)
  - Una flag che indica quali eventi controllare (Success, failure o entrambi)
- Nel configurare la SACL bisogna definire solo le azioni che effettivamente si vogliono controllare

Accesso ad Oggetti

Event ID	Description
560	Access was granted to an already-existing object.
561	A handle to an object was allocated.
562	A handle to an object was closed.
563	An attempt was made to open an object with the intent to delete it.
564	A protected object was deleted.
565	Access was granted to an already-existing object type.
567	A permission associated with a handle was used. Note: A handle is created with certain granted permissions (Read, Write, and so on). When the handle is used, up to one audit event is generated for each of the permissions that were used.
568	An attempt was made to create a hard link to a file that is being audited.
569	The resource manager in Authorization Manager attempted to create a client context.
570	A client attempted to access an object. Note: An audit event is generated for every attempted operation on the object.
571	The client context was deleted by the Authorization Manager application.
572	The Administrator Manager initialized the application.
772	The Certificate Manager denied a pending certificate request.
773	Certificate Services received a resubmitted certificate request.
774	Certificate Services revoked a certificate.
775	Certificate Services received a request to publish the certificate revocation list (CRL).
776	Certificate Services published the CRL.
777	A certificate request extension was made.
778	One or more certificate request attributes changed.
779	Certificate Services received a request to shut down.
780	Certificate Services backup was started.
781	Certificate Services backup was completed.
782	Certificate Services restore was started.
783	Certificate Services restore was completed.
784	Certificate Services was started.
785	Certificate Services was stopped.
786	The security permissions for Certificate Services changed.
787	Certificate Services retrieved an archived key.
788	Certificate Services imported a certificate into its database.
789	The audit filter for Certificate Services changed.
790	Certificate Services received a certificate request.
791	Certificate Services approved a certificate request and issued a certificate.
792	Certificate Services denied a certificate request.
793	Certificate Services set the status of a certificate request to pending.
794	The Certificate Manager settings for Certificate Services changed.
795	A configuration entry changed in Certificate Services.
796	A property of Certificate Services changed.
797	Certificate Services archived a key.
798	Certificate Services imported and archived a key.
799	Certificate Services published the Certification Authority (CA) certificate to Active Directory.
800	One or more rows have been deleted from the certificate database.
801	Role separation was enabled.

Events 772 through 801 are generated only by computers that are running Windows Server 2003 and Certificate Services.

Modifica dei criteri (*policies*)

- Con l'auditing del cambio di criteri si può tener traccia delle seguenti modifiche:
  - Assegnazione di privilegi utente
  - Criteri di Auditing
  - Relazioni di fiducia di dominio
- Entrambi i Failure e i Success events di questa categoria dovrebbero essere abilitati

Event ID	Description
608	A user right was assigned.
609	A user right was removed.
610	A trust relationship with another domain was created.
611	A trust relationship with another domain was removed.
612	An audit policy was changed.
613	An Internet Protocol Security (IPSec) policy agent was started.
614	An IPSec policy agent was disabled.
615	An IPSec policy agent was changed.
616	An IPSec policy agent encountered a potentially serious failure.
617	A Kerberos version 5 policy was changed.
618	Encrypted Data Recovery policy was changed.
620	A trust relationship with another domain was modified.
621	System access was granted to an account.
622	System access was removed from an account.
623	Auditing policy was set on a per-user basis.
625	Auditing policy was refreshed on a per-user basis.
671	Security policy was changed or refreshed. ("--" in the Changes Made field means that no changes were made during the refresh.)
768	A collision was detected between a namespace element in one forest and a namespace element in another forest.
769	Trusted forest information was added.
770	Trusted forest information was deleted.
771	Trusted forest information was modified.
805	The Event Log service read the Security log configuration for a session.

Utilizzo di Privilegi

- Tramite questa categoria è possibile monitorare l'utilizzo di privilegi da parte di account, con alcune eccezioni
- L'auditing di questa categoria permette di rilevare eventi spesso associati ad un attacco (Spegnimento di sistemi, operazioni sui driver dei dispositivi etc.)

Utilizzo di Privilegi

- I Failure Events di questa categoria dovrebbero essere attivati
  - Sono sintomi di un malfunzionamento della rete
  - Possono indicare tentativi di aprire una breccia nella sicurezza
- I Success Events dovrebbero essere abilitati solo per necessità specifiche

Event ID	Description
576	Specified privileges were added to a user's access token. (This event is generated when the user logs on.)
577	A user attempted to perform a privileged system service operation.
578	Privileges were used on an already-open handle to a protected object.

Controllo dei Processi

- Questa categoria fornisce un dettagliato registro dell'esecuzione di ogni processo
- Il controllo dei processi è eccellente per le applicazioni di Troubleshooting, ma genera un enorme numero di eventi (almeno due per processo)
- Questi eventi dovrebbero essere abilitati solo per reali necessità insieme ad un metodo automatico di analisi

Event ID	Description
592	A new process was created.
593	A process exited.
594	A handle to an object was duplicated.
595	Indirect access to an object was obtained.

Eventi di Sistema

- Abilitando questa categoria, si può tener traccia di modifiche nell'ambiente del computer come:
  - Cancellazione dei registri di sicurezza
  - Spegnimento del computer locale
  - Modifica dei pacchetti di autenticazione etc.
- Di norma si dovrebbero abilitare i Success Events che registrano il riavvio del sistema
- Tentativi riusciti di pulizia del registro di sicurezza sono registrati a prescindere da quali eventi di sistema siano sotto controllo

Event ID	Description
512	The Windows operating system is starting up.
513	The Windows operating system is shutting down.
514	An authentication package was loaded by the Local Security Authority (LSA).
515	A trusted logon process has registered with the LSA.
516	Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.
517	The Security log was cleared.
518	A notification package was loaded by the Security Accounts Manager (SAM).
520	The system time was changed.

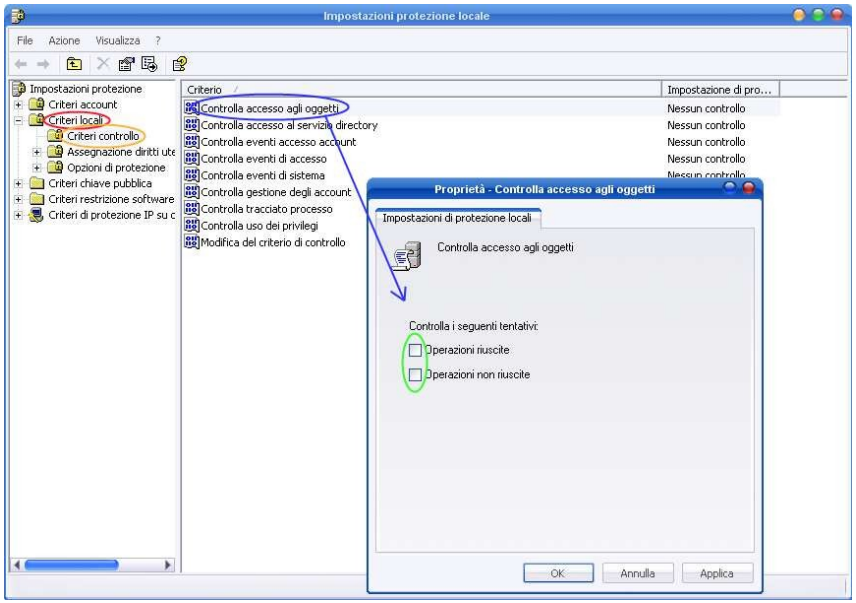
Abilitare Criteri di Auditing

- I Criteri di Auditing possono essere attivati
  - Localmente nella Console di gestione dei criteri di protezione locale o tramite template di sicurezza
  - In remoto tramite le Group Policy

Audit Policy	Events to Audit
Audit Account Logon Events	Success, Failure
Audit Account Management	Success, Failure
Audit Directory Service Access	Success, Failure
Audit Logon Events	Success, Failure
Audit Object Access	Success, Failure
Audit Policy Change	Success
Audit Privilege Use	Failure
Audit Process Tracking	None
Audit System Events	Success

Abilitare Criteri di Auditing

1. Aprire la Console negli Strumenti di Amministrazione
2. Doppio click su Criteri locali, doppio click su Criteri di controllo
3. Nel pannello destro, doppio click sui criteri che si vogliono abilitare
4. Spuntare le voci Operazioni riuscite \ non riuscite secondo le esigenze
5. Chiudere la Console



Monitorare Eventi di Auditing

- Esistono diversi metodi per monitorare gli eventi scritti nel registro eventi
- A seconda delle necessità e delle circostanze si può scegliere tra 4 metodi principali:
  - Visualizzatore di eventi
  - Script personalizzati
  - Event Comb
  - Strumenti completamente automatizzati (es. Microsoft Operations Manager)

Visualizzatore di Eventi

- E’ lo strumento più semplice per monitorare gli eventi e permette di:
  - Vedere i dettagli degli eventi
  - Ordinare eventi per tipo, criterio di auditing, data
  - Cercare eventi per aree comuni
  - Filtrare eventi per aree comuni
  - Esportare registri di eventi in formato .evt, .csv, .txt
  - Connettersi a computer remoti e gestire il Registro Eventi

Visualizzatore di Eventi

- Il Visualizzatore di Eventi non permette l'unione di eventi
  - Ciò può creare problemi per eventi registrati su più server, come gli eventi di Accesso ad Account
- Il Visualizzatore non permette la ricerca di dettagli di eventi
- Esportando gli eventi in un file, si possono importare in un database o eseguire script personalizzati da molti computer

Script Personalizzati

- Esiste una varietà di Script per gestire eventi:
  - Dumpel.exe
    - Riversa e filtra registri eventi in un file di testo separato
  - Eventlog.pl
    - Script in Perl per Windows 2000 che ripulisce e copia file di registro, mostra e modifica le relative impostazioni
  - Eventquery.vbs
    - Script in visual basic che mostra gli eventi di file di registro di Windows Server 2003 ed XP
  - LogParser 2.2
    - Un versatile strumento che analizza file basati su testo come i registri di auditing e crea rapporti in linguaggio SQL-like

Event Comb

- L'Event Comb analizza registri eventi da più server, generando percorsi distinti di esecuzione per ciascun server incluso nei criteri di ricerca
- L'Event Comb permette di
  - Mettere insieme eventi da più computer
  - Cercare occorrenze di eventi per qualsiasi area negli eventi riuniti
  - Cercare tra i registri archiviati
  - Eseguire ricerche molto specifiche grazie ai parametri offerti

Concludendo: Migliori Pratiche

- Determinare quali eventi dovrebbero essere registrati
- Sincronizzare il tempo su tutti i computer e i dispositivi di rete
- Creare una linea base di eventi
- Controllare i file di registro in cerca di comportamenti sospetti