

**Direttamente dalla
sorgente**
“Network IDS Oggi & nel Futuro”

Graham Welch
Director EMEA , Sourcefire Inc.

SOURCEfire
network SECURITY

Agenda

- ▶ Background sull'Intrusion Detection
 - ▼ Un giorno nella vita di ...
- ▶ Intrusion Prevention vs. Intrusion Detection
- ▶ Il futuro degli IDS
- ▶ Q & A

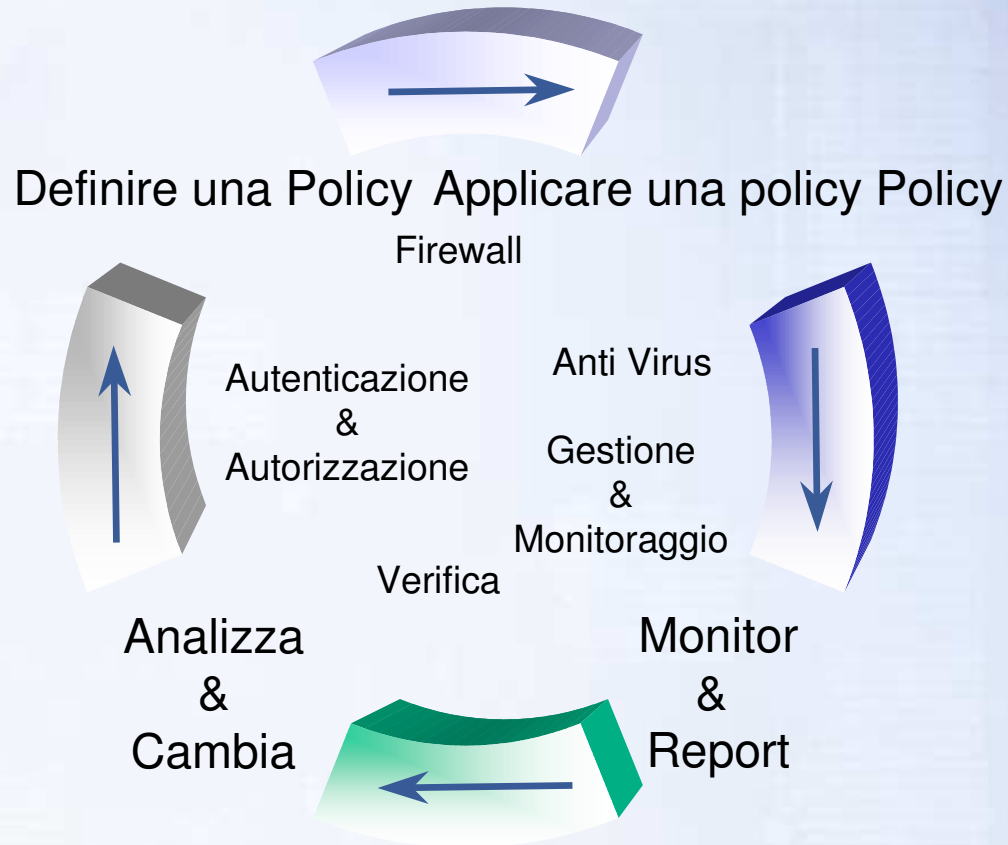
Background sull' Intrusion Detection

SOURCEfire
network SECURITY

Una buona Network Security

- ▶ Definire le Policy
- ▶ Applicare le Policy
- ▶ Monitor & Report
- ▶ Analizzare e Modificare
 - ▼ Firewall
 - ▼ Anti-virus
 - ▼ Monitoring

Good Network Security



Cos'è un NIDS?

Un Network Intrusion Detection System (NIDS) monitora il traffico in tempo reale e invia alert quando vengono rilevate delle attività sospette



Perché i NIDS sono importanti?

Il controllo degli accessi (firewalling) rappresenta solo una parte delle soluzioni di security, per una completa sicurezza aziendale si ha bisogno di una tecnologia di network monitoring (Defense in Depth)

Misure di sicurezza complementari

- ▶ Network IDS completa ed accresce le funzionalità dei firewall
 - ▼ Fornisce una “assicurazione” in caso che il firewall venga bypassato o sia configurato male
 - ▼ Protegge dalle minacce interne
 - ▼ Permette un’analisi forense su ambienti mutevoli e vettori di minacce



La prospettiva a livello SYSTEM

- ▶ I *sistemi* di intrusion detection NON sono *sensori* di intrusion detection
- ▶ Gli Intrusion Detection System consistono di una serie di componenti che devono tutti essere gestiti e la cui importanza è critica per il successo generale dell'implementazione
 - ▼ Componente sensore
 - ▼ Componente gestione dei dati
 - ▼ Componente interfaccia di amministrazione/console
- ▶ Ogni parte del sistema è critica!

**Un giorno nella
vita di...**

SOURCEfire
network SECURITY

Amministratore

- ▶ Responsabile dell'amministrazione quotidiana del network e delle misure di sicurezza
- ▶ Spesso operato di lavoro e a corto di personale
- ▶ Tipicamente manca di esperienza con i sistemi operativi sottostanti
- ▶ Si sforza di rimanere aggiornato sulle ultime vulnerabilità, minacce, patch, etc.

Amministratore

Requisiti specifici per IDS

- ▶ Facilità di deployment e utilizzo
 - ▼ Nessuna componente di terze parti
 - ▼ Nessun sistema operativo da installare o aggiornare
- ▶ Riduzione/eliminazione di falsi positivi
- ▶ Risposta automatica alle nuove vulnerabilità

Analista

- ▶ Responsabile del mantenimento della sicurezza del network aziendale e dell'applicazione delle policy di security
- ▶ Deve prendere quasi in tempo reale decisioni basate su informazioni provenienti da diverse fonti
- ▶ Deve essere in grado di decidere rapidamente quale danno è avvenuto

Analista

Requisiti specifici per IDS

- ▶ Capacità di aggregare e correlare informazioni su eventi quasi in tempo reale
- ▶ Facile accesso a informazioni forensi dettagliate
- ▶ Capacità di modificare le regole per applicare le policy di sicurezza

Dirigente

- ▶ Responsabile per le decisioni di acquisto
- ▶ Sovrintende l'intero team addetto alla sicurezza
- ▶ Esposizione limitata al sistema

Dirigente

Requisiti specifici per IDS

- ▶ Total Cost of Ownership (TCO) basso
 - ▼ Soluzione end-to-end
 - ▼ Non vi sono costi nascosti
- ▶ Supporto e manutenzione completi
- ▶ Meccanismo avanzato di reporting per individuare facilmente il ROI

Intrusion Prevention vs. Intrusion Detection

Il trend del futuro?

SOURCEfire
network SECURITY

Intrusion Prevention - Il mito

- ▶ E' la fine dell'IDS come siamo abituati a conoscerlo, ma non mi preoccupa

“La tecnologia IDS è stata costruita sul presupposto che il numero delle vulnerabilità di sicurezza - e quello degli hacker intelligenti in grado di individuarle e sfruttarle - fosse troppo elevato per tentare al strada della prevenzione; perciò, le imprese devono monitorare gli eventi, piuttosto che cercare di bloccare gli attacchi. Gartner crede, comunque, che le soluzioni di protezione disponibili ed emergenti, come l'intrusion prevention, siano destinate a relegare questa teoria nello stesso cestino che contiene client/server, banner pubblicitari e pet rocks.”

- R. Stiennon, M. Easley, Gartner Group

Intrusion Prevention - La verità

- ▶ IDS e IPS sono due cose **DISTINTE!**
 - ▼ L'intrusion prevention è una tecnologia di controllo degli accessi
 - ▼ L'intrusion detection è una tecnologia di monitoraggio delle reti
- ▶ Si ha bisogno di entrambe per assicurare al proprio network una difesa appropriata

Defense-in-depth non è assicurata dal solo IPS!

Intrusion Prevention - Tipi

▶ Due tipi di intrusion prevention system (IPS)

▼ Host-based

- Risiede su un singolo host individuale e difende solo quel'host dagli attacchi monitorando il traffico/comportamento e interrompendo le attività ostili/fuori dalla specifiche
- In sostanza, un air-bag per il vostro PC (funziona solo nel momento in cui siete già stati colpiti)

▼ Network-based

- Analisi/intrusion detection del traffico in-line
- “Smart Firewall” - l'evoluzione logica del “proxying” firewalls?
- Chiude sessioni/scarta pacchetti giudicati ostili

Intrusion Prevention - Esame realistico

- ▶ Intrusion Prevention System (IPS) sono tecnologie nuove - immature
- ▶ Falsi positivi portano a Denial of Service
- ▶ Open / close non riusciti portano a Denial of Service o alla perdita di capacità di protezione senza avviso
- ▶ Alcune delle maggiori installazioni di IPS si basano su Snort, ma non sono ancora largamente adottati
 - ▼ Hogwash
 - ▼ Snort-inline

Intrusion Prevention - Considerazioni serie

- ▶ Come potete sapere se il vostro sistema di intrusion prevention si lascia sfuggire un attacco?
 - ▼ Fareste meglio ad avere un buon IDS!!
- ▶ Network IPS è una tecnologia in-line
 - ▼ Analizza solamente il traffico che passa attraverso il device
 - ▼ Il traffico che non passa attraverso il device NON viene analizzato!
 - ▼ Fareste meglio ad avere un buon IDS!!

Il futuro dell'IDS

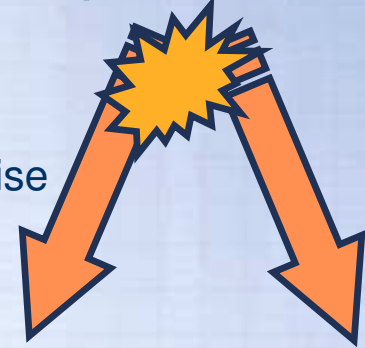
Cosa c'è dopo?



SOURCEfire
network SECURITY

Oltre l'Intrusion Detection

- ▶ IDS si evolve per supportare due funzioni specifiche ...
- ▶ Funzione 1: Difesa Perimetrale
 - ▼ Evoluzione della funzione firewall
 - ▼ Richiede metodologie di rilevazione estremamente precise
 - ▼ Deve avere meccanismi flessibili di blocco
- ▶ Funzione 2: Security Monitoring
 - ▼ Monitoraggio della difesa perimetrale
 - ▼ Intrusion detection
 - ▼ Applicazione delle policy
 - ▼ Analisi dell'utilizzo dei sistemi
 - ▼ Profiling dei sistemi
 - ▼ Ottimizzazione delle infrastrutture di sicurezza
- ▶ I network devono averle entrambe!!!



Sicurezza unificata del network

- ▶ Monitoraggio allo “stato dell’arte” (IDS)
- ▶ Difesa perimetrale saldamente integrata (IPS)
- ▶ Real-time Network Awareness (RNA™)
- ▶ Gestione integrata dei dati, analisi & ottimizzazione del sistema (MC)

Security Monitoring (IDS)

- ▶ Metodologie di ispezione del traffico accurate
 - ▼ Algoritmi intelligenti di stateful analysis
 - ▼ Decoder avanzati di protocolli
 - ▼ Motore di rilevazione rule-driven
- ▶ Flessibilità estrema
 - ▼ Attacchi conosciuti e sconosciuti
 - ▼ Minacce esterne ed interne
 - ▼ Rileva tutti i tipi di minacce
 - Exploit
 - Contenuti di tipo malicious
 - Violazione delle policy
- ▶ Assolutamente robusto
 - ▼ Dynamic load balancing
 - ▼ Internal self-preservation
 - ▼ Supporto per la continuità delle operazioni

Difesa perimetrale (IPS)

- ▶ Filtraggio in-line del traffico malicious
- ▶ Packet scrubbing
- ▶ Interazione automatica con altri dispositivi di rete
 - ▼ Firewall
 - ▼ Switch
 - ▼ Router
- ▶ Terminazione delle sessione
 - ▼ UDP
 - ▼ TCP
- ▶ Bloccaggio porte

Real-time Network AwarenessTM

- ▶ **Analisi passiva del network**
 - ▼ Continua identificazione dei dispositivi di rete
 - ▼ Continua identificazione dei profili di comportamento
 - ▼ Continua identificazione delle vulnerabilità
- ▶ **Fornisce un ampio contesto per una correlazione avanzata**
- ▶ **Permette ottimizzazione IDS/IPS automatica**
 - ▼ Set di regole
 - ▼ Parametri di anomalia
 - ▼ Algoritmi di elaborazione del traffico
 - ▼ Risposte automatiche

System Management

- ▶ Unifica tutte le funzioni critiche della network security
 - ▼ Monitoraggio eventi
 - ▼ Correlazione eventi & analisi forense
 - ▼ Conoscenza del sistema & ottimizzazione della security
 - ▼ Gestione sensori
 - ▼ Distribuzione & applicazione delle policy
- ▶ Data management integrato ad alte prestazioni
 - ▼ Costruita per questo scopo, pre-installata, pre-configurata, e self-maintaining
 - ▼ Facilita la risposta alle minacce in tempo reale e l'analisi forense
 - ▼ Scalabile fino a 100 milioni di ingressi senza impattare sulle performance
- ▶ Riduce i TCO
 - ▼ Interfacce workflow-oriented
 - ▼ Sistema di gestione semplificato
 - ▼ Niente costi nascosti

Cosa evitare

- ▶ Evitare le limitazioni di un vulnerability scanning attivo
 - ▼ Interruzione del servizio di dispositivi chiave
 - ▼ Consumo di banda
 - ▼ Descrizione intermittente della rete
- ▶ Evitare le limitazioni di approcci host-based
 - ▼ Rileva gli host o i servizi sconosciuti
 - ▼ Nessuna manutenzione sull'host

Grazie...

Domande?

SOURCE*fire*
network SECURITY