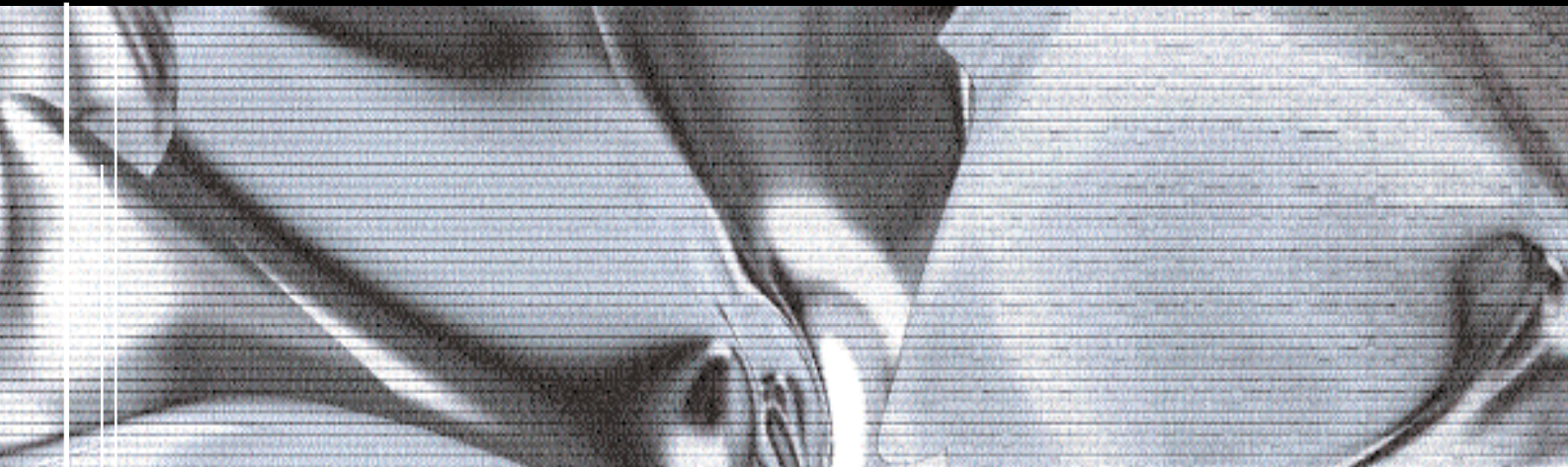


@ÆNIGMA D.I

UN SISTEMA DISTRIB PER LA RILEVAZIONE DELLE INTRUSIONI



■ 1. Introduzione

DIDS è l'acronimo di **Distributed Intrusion Detection System**. I sistemi di Intrusion Detection sono un elemento fondamentale per qualsiasi architettura di *network security*: essi forniscono infatti un layer di sicurezza aggiuntivo, monitorizzando il traffico sul perimetro della rete protetta ed evidenziando la presenza di pattern d'attacco predefiniti (**signature-based** Intrusion Detection) o in generale di traffico anomalo (**anomaly-based** Intrusion Detection). Al verificarsi di specifici events, gli IDS inviano degli *alerts* agli amministratori di rete o fanno scattare delle contromisure specifiche predefinite, volte ad arginare il pericolo rappresentato dai tentativi d'attacco individuati (reset della connessione sospetta, aggiornamento dinamico delle regole di firewalling, SNMP traps). Esistono molti tipi di IDS: l'attuale sviluppo nel settore fa pensare che il futuro sia rappresentato dai siste-

mi distribuiti (DIDS), in grado di fornire la *centralizzazione assoluta* della configurazione e la gestione avanzata degli allarmi, esigenze richieste in primo luogo da responsabili di NOC e SOC (Network Operation Centers, Security Operation Centers). In questo primo articolo analizzeremo @Ænigma, il primo DIDS basato sull'engine di Snort ed interamente sviluppato in Italia.

■ 2. Architettura del sistema

Come abbiamo già detto, @Ænigma è un sistema di Intrusion Detection distribuito. Esso implementa la **catalogazione centralizzata degli Alerts** generati e la **gestione centralizzata dei sensori**, attraverso un **database controllato da un'intuitiva interfaccia web**. @Ænigma fornisce inoltre un sottosistema per la **gestione degli allarmi in tempo reale** (via E-mail o SMS), configurabile attraverso la **GUI di gestione** in am-

biente Microsoft Windows.

Uno dei punti di forza di @Ænigma è l'assoluta unicità della soluzione proposta: non esistono infatti altri esempi di Intrusion Detection System basati su Snort che siano paragonabili per funzionalità e possibilità concrete di impiego. La compatibilità assoluta con diversi dialetti Unix (Linux, *BSD, SUN Solaris), la semplicità di installazione e la possibilità di integrazione con altre soluzioni di sicurezza (firewall, antivirus, application proxy, CA) lo rendono un prodotto particolarmente interessante.

@Ænigma è costituito da 3 elementi principali.

- **Central Management Station (CMS)**: si occupa della catalogazione degli Alerts e della gestione centralizzata dei sensori (Remote Sensor Management), fornendo una soluzione di sicurezza fault-tolerant e di semplice configurazione.
- **Network Intrusion Detection Sensor (NIDS)**: sensori basati sull'engine di Snort, con ruleset compa-

.D.S. UITO

di Marco Ivaldi e Raoul Chiesa

I sistemi di Intrusion Detection sono un elemento fondamentale dell'architettura di sicurezza di una rete: essi consentono infatti di individuare i tentativi di attacco su un numero di scenari virtualmente illimitato. In questo articolo gli autori forniscono una panoramica sul primo Distributed Intrusion Detection System (DIDS), basato sull'engine di Snort, interamente sviluppato in Italia: @Ænigma DIDS, risultato finale di due anni investiti in R&D dalla Divisione Sicurezza Dati della @ Mediaservice.net Srl.



tibile in maniera assoluta con il prodotto open-source e performances sopra la media per quanto riguarda la gestione del traffico IP frammentato e la monitoraggio di reti FastEthernet (100 Mbit/s).

- **@Ænigma Application Server (AAS):** utilizzati per la spedizione de-centralizzata degli allarmi in tempo reale (via E-mail e SMS su rete GSM) e la gestione avanzata della criticità degli Alerts generati dai Sensori.

Analizziamo ora separatamente ogni sottosistema, fornendo una descrizione dettagliata del suo funzionamento.

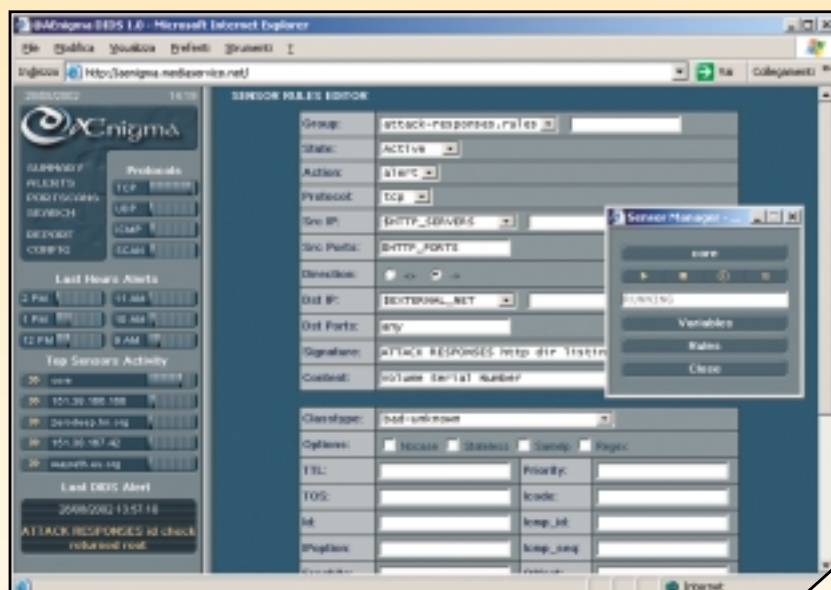
3. Network Intrusion Detection Sensor (NIDS)

I sensori @Ænigma sono equipaggiati con un plugin proprietario per Snort assolutamente innovativo,

che consente la gestione del database centralizzato degli Alerts e del sistema di allarme in tempo reale (real-time alerting).

Le performances e la stabilità sono assicurate dall'engine di Snort, il NIDS open-source più diffuso e premiato al mondo: test comparativi

(funzionali e prestazionali), fatti eseguire presso appositi laboratori esterni, hanno evidenziato la netta superiorità di @Ænigma rispetto agli altri prodotti presenti sul mercato. Per ulteriori informazioni su Snort è possibile fare riferimento al sito ufficiale del progetto, all'url



<http://www.snort.org>.

Il ruleset di @Ænigma è assolutamente compatibile con quello di Snort e lo pone al primo posto per velocità di aggiornamento delle signatures e semplicità di configurazione rispetto agli altri NIDS.

Grazie anche alle caratteristiche delle signatures di Snort, @Ænigma possiede un'elevata capacità di adattamento ad ambienti molto diversificati. Il tuning su reti anche complesse è pertanto semplice e veloce da effettuare.

I sistemi operativi attualmente supportati dal NIDS @Ænigma sono Linux, OpenBSD, FreeBSD, NetBSD e Solaris (piattaforme hardware Intel e Sparc).

■ 4. Central Management Station (CMS)

La Central Management Station im-

plementa la gestione centralizzata delle signatures e la conservazione dei logs degli attacchi. Il database della CMS, infatti, contiene tutte le informazioni relative alla configurazione dei sensori sotto il suo controllo, oltre al log repository globale. La gestione centralizzata delle configurazioni dei sensori rende @Ænigma una soluzione assolutamente fault-tolerant, in grado di garantire il rapido recupero delle attività a seguito di eventuali faults (hardware e software) dei sensori installati.

@Ænigma è infine dotato di un sottosistema avanzato di gestione delle attività dei sensori chiamato **Remote Sensor Manager (RSM)**, che permette il controllo e la monitoraggio degli stessi. L'interfaccia di gestione è interamente sviluppata su web, approccio che offre compatibilità assoluta con tutti i sistemi operativi in grado di lavorare su TCP/IP.

I sistemi operativi attualmente sup-

portati dalla CMS @Ænigma sono Linux, OpenBSD, FreeBSD, NetBSD e Solaris (Intel e Sparc edition).

■ 5. Real-Time Application Server (AAS)

Il vero punto di forza dell'architettura modulare di @Ænigma è l'**Application Server (AAS)**, che rappresenta la vera innovazione verso l'Intrusion Detection distribuita. Contrapposta alla centralizzazione assoluta della gestione dei sensori, infatti, la de-centralizzazione del sottosistema di allarme in tempo reale consente un'elevata scalabilità della soluzione, oltre ad un'estrema elasticità nella configurazione globale del DIDS.

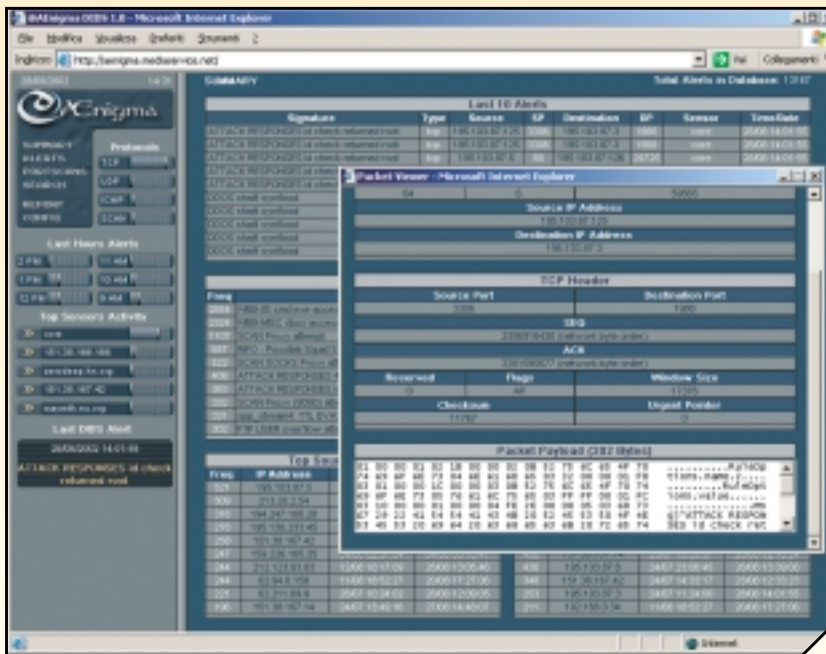
Il Real-Time Application Server @Ænigma, implementato tramite tecnologia multicast cifrata attraverso Secure Socket Layer (SSL), offre una gestione avanzata della criticità degli allarmi generati dai sensori attraverso una comoda Graphical User Interface (GUI).

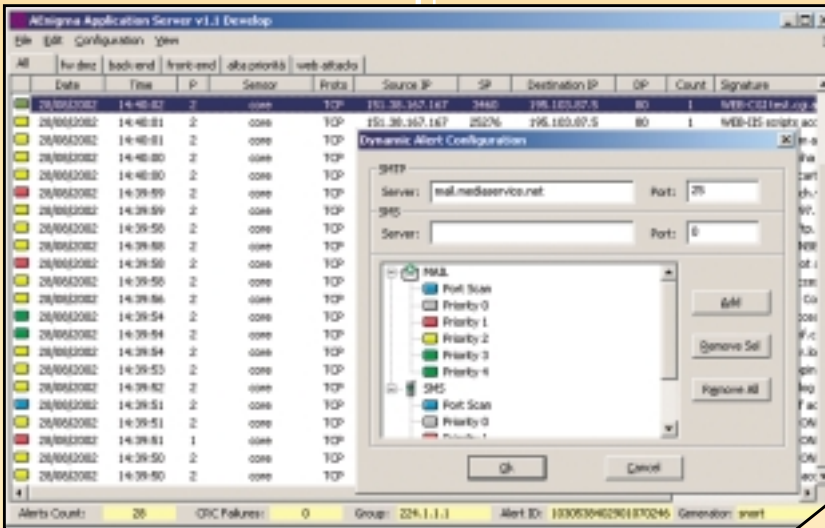
L'AAS supporta Microsoft Windows 95/98/NT/2000/XP.

■ 6. Funzionamento di @Ænigma DIDS

Facciamo una rapida panoramica del funzionamento del sistema di Intrusion Detection distribuito: nel prossimo numero avremo modo di approfondire ulteriormente il flusso di lavoro di @Ænigma introducendo un esempio concreto tratto da un caso reale.

Quando un sensore attestato su di un segmento di rete protetto identifica la presenza di un pattern di at-





tacco, diciamo che si verifica un event. Questo event genera una risposta da parte del sensore, che tipicamente consiste in un Alert salvato nel database centralizzato della CMS ed inviato in tempo reale agli amministratori di rete.

La generazione dell'Alert può essere concettualmente separata in 2 fasi che vengono eseguite in parallelo: 1) Viene inviata una comunicazione Unicast alla CMS, contenente tutti i dati relativi al pacchetto (o ai pacchetti) contenente l'anomalia che ha fatto scattare l'allarme. La CMS provvede al salvataggio nel database centralizzato per la successiva consultazione tramite interfaccia web.

Tra i dati salvati vi sono la data e l'ora di generazione dell'Alert, la signature a cui esso fa riferimento, la tipologia di traffico interessata (TCP, UDP, ICMP o altro), gli indirizzi IP coinvolti e le porte sorgente e destinazione, oltre all'identificativo del sensore che ha individuato l'anomalia. Sono inoltre conservati tutti i pacchetti sospetti, decodificati a layer-3 (IP), layer-4 (TCP, UCP o ICMP) e layer-7 (payload del pacchetto, in forma binaria e in ASCII)

del modello di riferimento ISO/OSI. 2) Viene inviato un pacchetto Multicast contenente le informazioni salienti sul pacchetto anomalo.

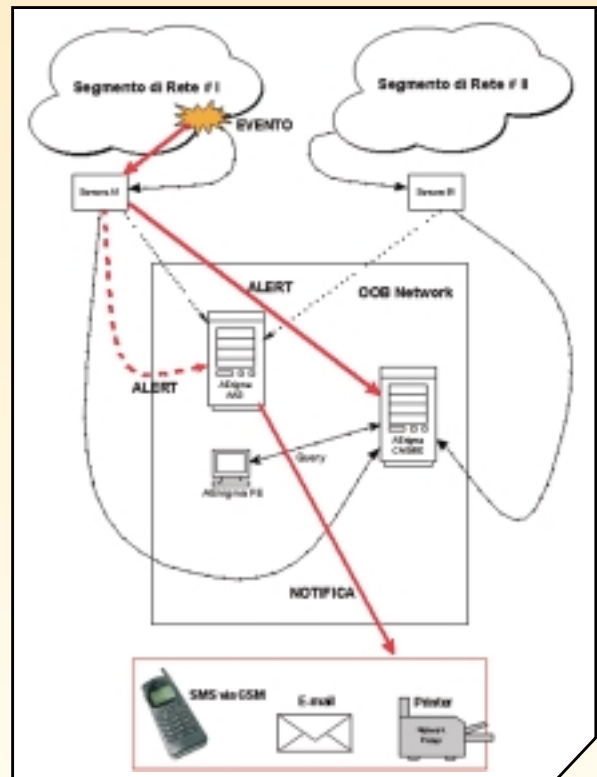
Tutti gli AAS che sono "sintonizzati" sullo stesso gruppo Multicast del sensore (e quindi hanno competenza per il singolo sensore che ha generato l'Alert) ricevono il pacchetto e lo processano separatamente, secondo la propria configurazione. Ad esempio, se l'Alert ha una particolare priorità è possibile inviarlo via E-mail o SMS (attraverso modem GSM) all'amministratore competente reperibile in quel momento (ad esempio attraverso l'interfacciamento diretto con un **database di reperibilità centralizzato**).

La netta separazione tra sottosistema

di conservazione dei logs e sottosistema di allarme in tempo reale fa sì che @Enigma DIDS possieda un'elevata affidabilità e scalabilità, oltre ad un'estrema comodità di gestione. L'approccio modulare alla progettazione costituisce pertanto uno dei maggiori punti di forza del Distributed Intrusion Detection System @Enigma, che si configura come una soluzione ideale in particolare per MSSP (Managed Security Service Provider) e altre grandi realtà aziendali.

7. Il futuro di @Enigma

@Enigma è ovviamente un progetto in continuo sviluppo da parte del team R&D della Divisione Sicurezza Dati (DSD) di @ Mediaservice.net



GLOSSARIO DEI TERMINI TECNICI

- **Event:** particolare occorrenza relativa ad un segmento di rete o ad un host considerata rilevante dal punto di vista della sicurezza.
- **Incident:** insieme di events che costituisce un attacco strutturato o in generale una minaccia per la sicurezza di una rete.
- **Signature:** firma univoca che può essere utilizzata per identificare un particolare attacco o una particolare famiglia di attacchi.
- **Ruleset:** raccolta di signatures, che può essere organizzata in policy di sicurezza specifiche per ogni segmento di rete.
- **Tuning:** attività di configurazione del ruleset su una rete specifica.
- **HIDS:** Host Intrusion Detection System, implementato attraverso agents specializzati residenti su ogni singolo host allo scopo di monitorizzare i log di sistema, l'integrità dei files ed eventualmente implementare una protezione a kernel-level.
- **NIDS:** Network Intrusion Detection System, implementato attraverso sensori collegati alla rete in modalità promiscua. In pratica si tratta di sniffer altamente performanti con funzionalità di pattern-matching.
- **DIDS:** Distributed Intrusion Detection System. Esso introduce la centralizzazione della configurazione dei sensori (network o host-based) e la gestione avanzata degli events.

Srl. Tra le funzionalità previste nelle prossime release vi sono:

- Integrazione di funzionalità di Intrusion Detection host-based.
- Supporto per reti WLAN 802.11b (Wireless Intrusion Detection).
- Automated Remote Upgrade di signatures ed engines.
- Integrazione di meccanismi avanzati di disaster recovery.
- Integrazione di modelli avanzati di analisi statistica degli incidents.

■ 8. Nel prossimo numero...

Come abbiamo già anticipato, nel prossimo numero vedremo un esempio di impiego di @Enigma DIDS in uno scenario reale: analizzeremo in maniera dettagliata la configurazione delle varie componenti del sistema distribuito e gli effetti che queste avranno sulla gene-

razione e sulla gestione degli Alerts e seguiremo passo-passo il percorso compiuto da un Alert (Unicast e Multicast). ■

Copyright © 2002 <Raoul Chiesa e Marco Ivaldi> (GNU/FDL License)

Copyright © 2002 <@ Mediaservice.net Srl – Torino, ITALY> (GNU/FDL License)

This article is under the GNU Free Documentation License, <http://www.gnu.org/copyleft/fdl.html> Verbatim copying and distribution of this entire article is permitted in any medium, provided this notice is preserved.

SCHEDA DEL PRODOTTO

Nome: @Enigma DIDS

Categoria: Intrusion Detection System

Produttore: @ Mediaservice.net Srl, Torino

Sito Internet:

<http://@Mediaservice.net>

Contatti: dsd@mediaservice.net

Assistenza on-site: Fornita direttamente dal produttore

Personalizzazioni: Realizzabili su progetto

■ Gli autori

Marco Ivaldi aka Raptor

Ricercatore e consulente nel campo della sicurezza informatica, si interessa di networking, telefonia, protocolli di comunicazione e crittografia: fa parte della D.S.D. di @ Mediaservice.net Srl.

È socio fondatore di Antifork Research

(<http://www.antifork.org>)

e ITBH (<http://www.blackhats.it>).

È a capo del team di sviluppo di @Enigma DIDS.

raptor@mediaservice.net

Raoul Chiesa aka Nobody

Chief Technical Officer presso la Divisione Sicurezza Dati di @ Mediaservice.net Srl.

Socio Fondatore e Membro del Comitato Direttivo di CLU-SIT – Associazione Italiana Sicurezza Informatica

ITBH (Italian Black Hats Association) Founder Member

rchiesa@clusit.it