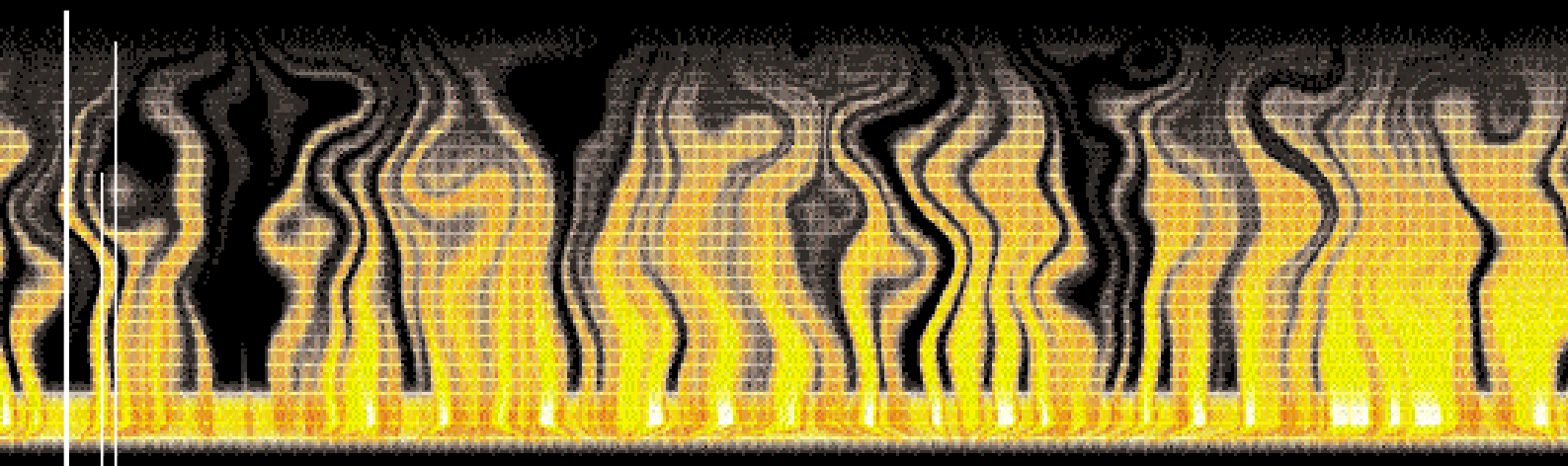


@ÆNIGMA D.I. IMPIEGO IN UNO SCENARIO REALE



Come abbiamo visto nel precedente articolo, @ÆNIGMA DIDS è un Intrusion Detection System distribuito in grado di monitorizzare il traffico su differenti segmenti di rete e di evidenziare la presenza di traffico anomalo, basandosi su una serie di pattern d'attacco predefiniti (signatures) configurabili dal Security Manager attraverso un'interfaccia web centralizzata.

L'architettura del sistema è basata su 3 sottosistemi principali che comunicano tra di loro attraverso specifici canali protetti da cifratura:

- **Central Management Station (CMS):** è il "cuore" del Distributed Intrusion Detection System, si occupa della catalogazione ragionata degli allarmi (Alerts) ricevuti dai NIDS e della gestione centralizzata dei sensori (Remote Sensor Management). La CMS @ÆNIGMA fornisce una soluzione di sicurezza fault-tolerant e di semplice configurazione, compatibile con i più diffusi dialetti Unix (Linux, *BSD,

Solaris).

- **Network Intrusion Detection Sensor (NIDS):** si tratta dei sensori che hanno l'incarico di monitorizzare continuamente il traffico di rete alla ricerca di anomalie e possibili minacce. L'engine dei NIDS @ÆNIGMA è basata su Snort (e di conseguenza il ruleset è compatibile al 100% con quello del prodotto open-source), a cui sono state aggiunte funzionalità di log centralizzato sul database proprietario della CMS e di Real-time alerting.

È proprio il sottosistema di gestione degli allarmi in tempo reale a costituire la vera innovazione introdotta da @ÆNIGMA DIDS. Anche i NIDS @ÆNIGMA sono compatibili con i principali dialetti Unix (Linux, *BSD e Solaris).

- **@ÆNIGMA Application Server (AAS):** è il componente chiave dell'architettura di @ÆNIGMA DIDS. Esso si occupa della gestione decentralizzata degli allarmi in tempo reale (con possibilità di spedizione

di Alerts via E-mail e SMS), sfruttando un protocollo proprietario basato sul Multicast addressing. I principali vantaggi di questo approccio sono il guadagno in termini di performance e l'assoluta scalabilità della soluzione di sicurezza. @ÆNIGMA AAS supporta Microsoft Windows 95/98/NT/2000/XP.

Di seguito analizzeremo il funzionamento coordinato di tutti i sottosistemi di @ÆNIGMA DIDS inseriti in uno scenario di rete reale.

■ Lo scenario di esempio

Descriviamo brevemente lo scenario di esempio in cui andremo a configurare il nostro sistema distribuito di rilevazione delle intrusioni. Tralasciando gli altri aspetti (flussi di lavoro, policy aziendali), concentriamoci sulla struttura e sui componenti della rete che abbiamo scelto di prendere in esame.

Supponiamo di avere 2 Zone A e B

Nella situazione descritta in figura è presente un'unica CMS all'interno del NOC centrale: qualora se ne presenti la necessità, è inoltre possibile impiegare delle sotto-CMS di backup per ogni singola Zona, come ulteriore garanzia di protezione da fault.

Ogni Zona, infine, ha i suoi AAS configurati ad hoc. Anche il NOC dovrà avere uno o più AAS allo scopo di monitorare ogni singola Zona secondo le specifiche esigenze. Come vedremo più dettagliatamente in seguito, ad ogni Zona sarà assegnato uno specifico gruppo Multicast (assimilabile ad una sorta di "canale" su cui i sensori trasmettono e gli Application Servers che si sintonizzano ricevono), che verrà utilizzato dagli AAS come discriminante principale per distinguere la provenienza di ogni singolo allarme, insieme agli altri dati contenuti nel pacchetto (nome del sensore che ha generato l'Alert, identificativo univoco dell'evento all'interno del database, indirizzo IP di provenienza dell'attacco, ecc.).

Vediamo ora separatamente la configurazione di ogni singola componente di @ÆNIGMA DIDS.

■ Configurazione della CMS

Per costruire un'infrastruttura distribuita di Intrusion Detection basata su @ÆNIGMA DIDS, è in primo luogo necessario installare la Central Management Station (CMS), che avrà il compito di custodire le configurazioni di tutti i sensori (offrendo un'interfaccia web per la loro gestione centralizzata), conservare tutti gli Alerts all'interno di un database relazionale e fornire gli strumenti di

query interattiva e generazione della reportistica.

I prerequisiti per l'installazione della CMS sono i seguenti:

- Presenza di un sistema operativo supportato, selezionabile a scelta tra Linux, OpenBSD, FreeBSD, NetBSD e Solaris. Esso dovrà essere installato seguendo le linee guida fornite da @ Mediaservice.net Srl, volte a garantire un livello di hardening soddisfacente.
- Presenza del database relazionale MySQL. Esso è stato scelto come piattaforma preferenziale per via delle performances, della stabilità e della licenza GPL. È in programma per le prossime releases il supporto per Oracle e per altri sistemi database commerciali.
- Presenza del server web Apache con supporto SSL e PHP4. L'interfaccia web di gestione è interamente scritta in PHP, mentre SSL è necessario per garantire la riservatezza delle comunicazioni effettuate via web.

Non analizziamo nel dettaglio la procedura di installazione, che viene gestita da un semplice script di shell per Unix. L'installazione della CMS è in realtà molto rapida, al termine avremo sul sistema le seguenti componenti:

- Programmi e API di gestione per l'interrogazione del database, la configurazione delle signatures e il Remote Sensor Management.
- Database principale per la conservazione degli Alerts e database secondari contenenti la configurazione dei singoli sensori (che saranno popolati dalle signatures selezionate al momento dell'installazione dei NIDS). Potranno eventualmente essere creati database contenenti ruleset relativi alle diverse Policy di Intrusion De-

tection per le differenti tipologie di rete da monitorare.

- Sistema di autenticazione per l'inserimento degli Alerts da parte dei sensori e per le modifiche di configurazione di @ÆNIGMA DIDS (lo script di installazione richiede l'inserimento delle password di gestione del sistema).

■ Configurazione dei NIDS

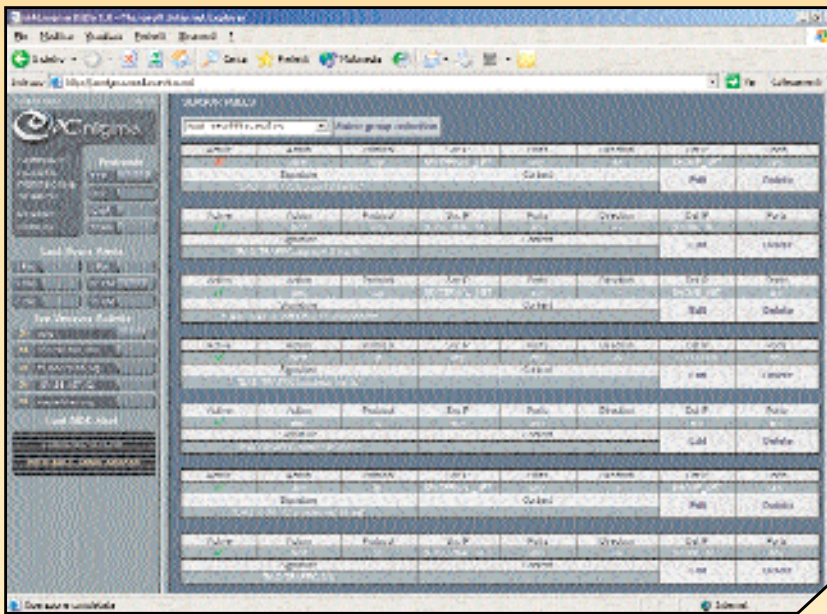
Una volta che la CMS è stata correttamente installata e configurata, è possibile occuparsi dei NIDS ad essa relativi, che come è già stato accennato dovranno essere uno per ogni **segmento di rete fisico**.

La distribuzione di @ÆNIGMA DIDS contiene pacchetti differenti, ognuno precompilato su un sistema operativo diverso e ottimizzato per una serie di architetture hardware (i386 base, i586, i686, Sparc, ecc.). Questo approccio permette di massimizzare le performance del sensore a seconda della piattaforma hardware e software selezionata.

A parte la base costituita dal sistema operativo (installato secondo le linee guida fornite da @ Mediaservice.net), i NIDS @ÆNIGMA non necessitano di particolari prerequisiti. Lo script di installazione formula alcune semplici domande riguardanti l'ambiente in cui sarà impiegato ogni singolo sensore.

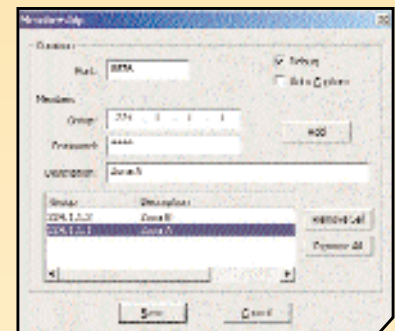
Tra i dati richiesti vi sono:

- Directory di installazione sul sistema locale.
- Nome univoco del sensore (hostname o indirizzo IP).
- Interfaccia di rete il cui traffico deve essere monitorato.
- Opzioni relative al supporto Multicast, tra cui il gruppo di trasmis-



ta UDP da utilizzare (il default per @ENIGMA DIDS è 8876), il gruppo su cui sintonizzarsi e la relativa password per la decodifica del traffico cifrato.

Il dialogo per la configurazione della Web Interface consente invece l'integrazione tra le varie componenti di



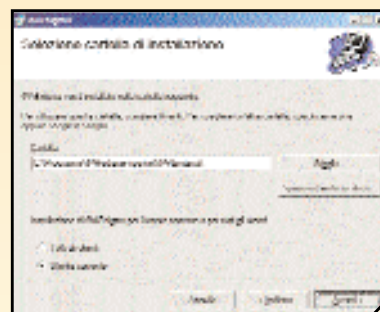
scaricare le nuove regole, attraverso l'apposito controllo messo a disposizione dall'interfaccia web.

di installazione è molto veloce ed utilizza la classica finestra di dialogo messa a disposizione dall'Install Shield di Microsoft Windows.

■ Configurazione dell'AAS

Restano da configurare gli @ENIGMA Application Servers. Esaminiamo ad esempio la configurazione di un AAS con il compito di monitorare l'attività dei NIDS attestati nella Zona A della nostra WAN, supponendo che tali sensori siano configurati per trasmettere sul gruppo Multicast 224.1.1.1, mentre invece quelli della Zona B lavorino sul gruppo 224.1.1.2 (ovviamente è possibile utilizzare qualsiasi indirizzo Multicast valido per distinguere un'area dall'altra; gli indirizzi Multicast validi sono compresi tra 224.0.0.0 e 239.255.255.255).

Per prima cosa sarà necessario installare l'AAS sulla macchina Windows scelta per svolgere la funzione di Application Server. La procedura



Forniamo ora un semplice esempio di configurazione dei seguenti sottosistemi dell'AAS:

- Multicast Membership
- Web Interface
- Real-time Alerts
- E-mail/SMS Alerts

L'interfaccia di configurazione della Membership permette di assegnare all'Application Server uno o più gruppi Multicast su cui rimanere in ascolto.

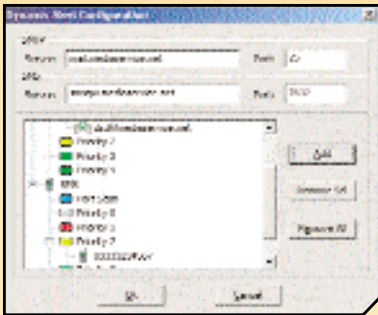
Essa consente di selezionare la por-

@ENIGMA DIDS: in particolare, una volta inserita l'URL su cui risponde l'interfaccia web montata sulla CMS, sarà possibile accedere direttamente ai dati memorizzati sul database centralizzato, con un semplice click del mouse, in ambiente AAS.

Oltre alla rappresentazione degli allarmi con gestione della priorità, AAS @ENIGMA consente l'invio di Alerts in tempo reale via E-mail ed SMS.

L'interfaccia di configurazione di questa funzionalità è semplice ed intuitiva: è sufficiente inserire gli indirizzi del Mail Server e dell'SMS Server (se presente), specificando poi a quali caselle di posta elettronica (o cellulari GSM) inviare gli Alerts con una determinata e specifica priorità. Sono ovviamente presenti dei meccanismi di sicurezza per la prevenzione di eventuali *flood*, studiati per evitare situazioni di Denial of Service (DoS) e, soprattutto, senza perdere allarmi importanti.

Infine, AAS mette a disposizione del Security Manager una serie di filtri preimpostati per differenziare la rap-



presentazione degli Alerts generati dai sensori. È possibile associare uno o più filtri (che possono inoltre essere ridefiniti a piacimento) ad una data finestra, per effettuare controlli incrociati in tempo reale e per mantenere sempre sott'occhio le situazioni di importanza critica (particolari porzioni di rete, allarmi con priorità elevata, servizi vitali o critici).

Terminata questa breve carrellata sulle funzionalità di @ÆNIGMA Application Server, siamo pronti per esporre il comportamento di @ÆNIGMA DIDS al momento dell'intercettazione di traffico anomalo su uno dei segmenti di rete monitorati.

■ @ÆNIGMA DIDS in azione

Per mostrare @ÆNIGMA DIDS in azione, forgiamo ora un pacchetto anomalo in uno dei segmenti di rete della Zona A, allo scopo di far scattare un allarme sul NIDS che monitorizza tale segmento. Supponendo che vi sia un web server attivo simuliamo, ad esempio, l'accesso al programma CGI vulnerabile ad un attacco di tipo PHF, tramite un qualsiasi

web browser:

lynx <IP_del_web_server>/phf

A questo punto, il sensore che ha l'incarico di monitorare il traffico relativo al web server vittima del tentativo di attacco confronta i pacchetti inviati dal browser con le signature contenute all'interno del suo rule-set e, essendo presente una signature di default che identifica l'accesso al CGI phf come traffico potenzialmente pericoloso, genera un Alert.

Come abbiamo visto nell'articolo precedente, quando un sensore attestato su di un segmento di rete protetto identifica la presenza di un pattern di attacco, diciamo che si verifica un event. Questo event genera una risposta da parte del sensore, che in pratica consiste nell'esecuzione parallela delle 2 azioni seguenti:

- 1) Viene inviata una comunicazione Unicast alla CMS, contenente tutti i dati relativi al pacchetto (o ai pacchetti) anomalo che ha fatto scattare l'allarme. La CMS prov-

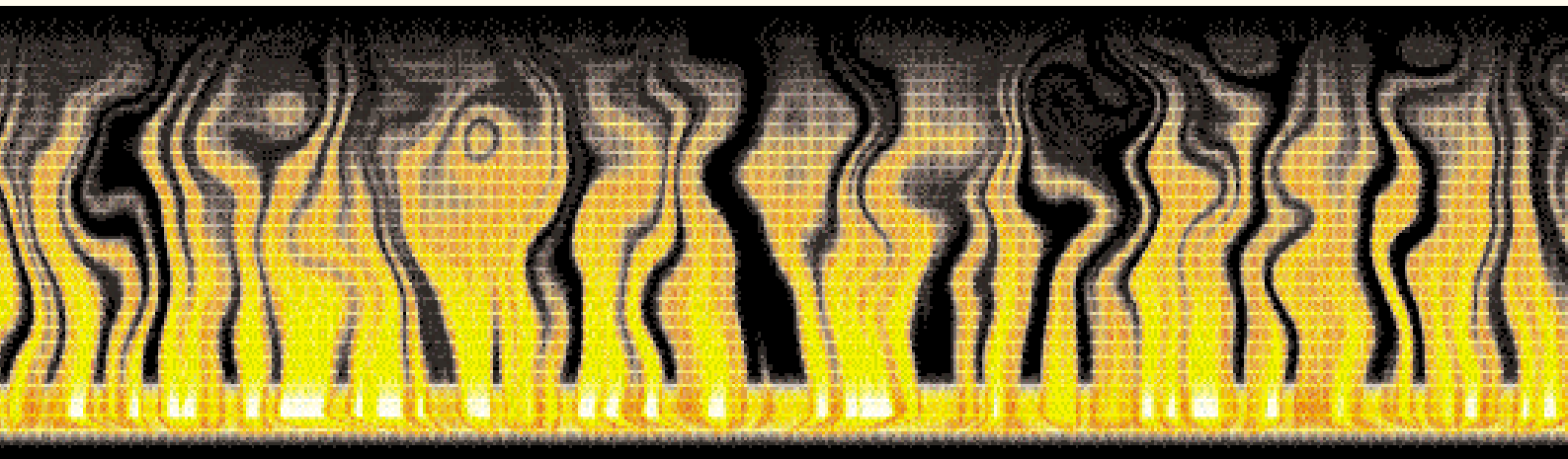
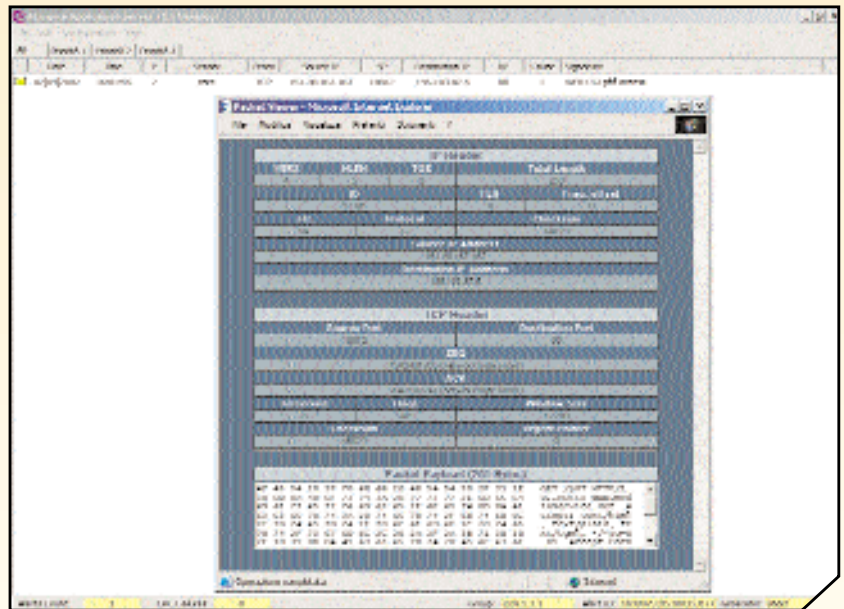
vede di conseguenza al salvataggio nel database centralizzato per la successiva consultazione tramite interfaccia web.

- 2) Viene inviata una comunicazione Multicast al gruppo configurato sul dato sensore, contenente le informazioni salienti sul pacchetto contenente l'anomalia (nel nostro caso 224.1.1.1). L'AAS "sintonizzato" sul gruppo Multicast relativo, riceve il pacchetto e lo processa, secondo la propria configurazione. Nel nostro esempio abbiamo impostato l'AAS per inviare un allarme via SMS al verificarsi di Alerts con priorità 2. Pertanto l'Application Server si preoccuperà di recapitare il messaggio, appoggiandosi al server da noi precedentemente definito.

Ed ecco il nostro Alert, come si presenta sulla GUI dell'AAS e sull'interfaccia web della CMS.

■ Conclusioni

Con questo secondo articolo ab-



GLOSSARIO DEI TERMINI TECNICI

- **NOC:** Network Operating Center. È il nucleo centrale di una WAN privata, che collega tutte le sottoreti (topologia a stella) e ne monitorizza le attività.
- **SOC:** Security Operating Center. Il concetto è il medesimo di quello di NOC, ma si applica generalmente agli MSSP, che gestiscono centralmente la sicurezza di un grande numero di clienti, tutti connessi al centro stella (generalmente tramite VPN cifrate passanti per Internet).
- **MSSP:** Managed Security Service Provider. Fornitore e gestore della sicurezza dei propri clienti: tipicamente si avvale di sistemi avanzati per l'Intrusion Detection e offre supporto 24x7.
- **Unicast:** Tipologia di traffico diretta ad un ben preciso host (pensiamo ad esempio ad una connessione TCP).
- **Multicast:** Tipologia di traffico simile al broadcast, in grado però di inviare pacchetti solo agli hosts che vogliono riceverli, utilizzando l'indirizzamento IP su classe D.
- **NIC:** Network Interface Card. Scheda di rete (tipicamente ethernet).
- **SPAN port:** Detta anche Mirror port, è una porta di uno switch configurata per replicare tutto il traffico delle altre porte. Utile per i NIDS perché permette lo sniffing su rete switchata.
- **TAP:** Dispositivo hardware in grado di replicare il traffico di rete, garantendo l'assoluta non-intrusività nei confronti della rete monitorata.
- **Rete OOB:** Rete Out Of Band. Denominazione utilizzata per denotare una rete che non ha contatti con l'esterno (come ad esempio la Management Network di @ÆNIGMA DIDS).

biamo concluso una panoramica sull'architettura e sulla configurazione di @ÆNIGMA DIDS, il sistema di Intrusion Detection distribuito basato sull'engine di Snort svi-

luppato dal team R&D di @ Mediaservice.net Srl. Per maggiori informazioni su @ÆNIGMA DIDS e sugli altri prodotti e servizi della Divisione Sicurezza Dati fate riferimento

all'indirizzo e-mail <dsd@mediaservice.net>. ■

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, 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: @Ænigma 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 @Ænigma 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 CLUSIT – Associazione Italiana Sicurezza Informatica

ITBH (Italian Black Hats Association) Founder Member

rchiesa@clusit.it