

# Networking & business

Di Simone Zanardi



*La struttura informatica degli uffici e delle piccole aziende dipende dell'efficienza del network. Un buon software di scansione può ottimizzarla.*

## Conoscere meglio la rete per farla rendere al massimo

Un buon amministratore di rete sa che affinché il network renda sempre al meglio è essenziale che esso sia sottoposto a un monitoraggio continuo. Non si tratta solo di una problematica di sicurezza, ma anche di un approccio che consente di capire come i vari dispositivi informatici interagiscono con la struttura, di come cambiano con il passare del tempo i requisiti e le esigenze delle postazioni di lavoro, oltre che di individuare e interpretare eventuali colli di bottiglia o inefficienze che possono compromettere la produttività dell'intero ambiente di lavoro.

Sul mercato esistono numerosi software in grado di assistere il personale IT nella gestione del network aziendale: si va dagli analizzatori di pacchetto, che intercettano il traffico in transito per esaminarne il contenuto e quindi la funzione, ai port scanner, che interrogano i vari terminali presenti in rete per comprendere quali siano i canali aperti e le applicazioni in attesa di comunicazioni provenienti dal network.

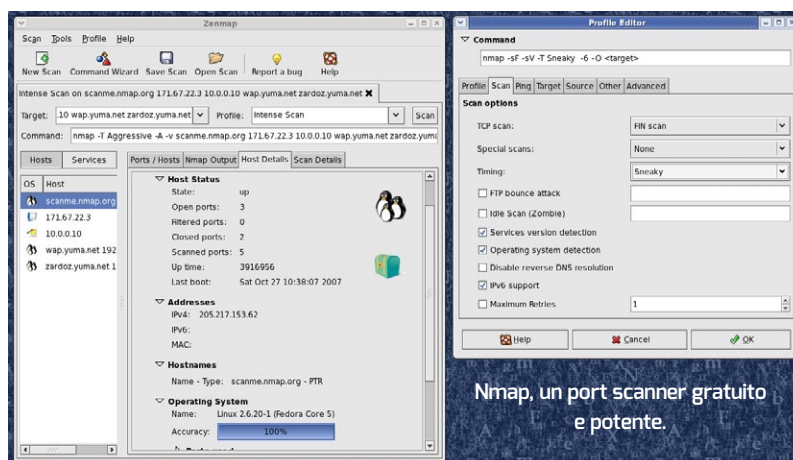
Entrambe le tipologie di software sono efficaci per l'individuazione di vulnerabilità, malfunzionamenti o inefficienze della struttura.

**Nmap** (gratuito per Windows, OS X e Linux, <http://nmap.org/>) è un software di scansione delle porte molto famoso nell'ambiente degli addetti ai lavori e non solo (è stato "utilizzato" come espediente di scena in numerosi film come *Matrix Reloaded*).

Sfrutta pacchetti IP grezzi per interrogare le macchine sulla rete e riportare numerose informazioni sul terminale tra cui il sistema operativo installato e la relativa versione, la presenza di firewall e Nat, le porte di comunicazioni aperte ed eventuali servizi in ascolto. È in grado di scansare reti con

centinaia di terminali operativi, ma si adatta senza problemi anche alle realtà di dimensioni più limitate; attraverso il sistema di monitoring integrato, l'amministratore di rete può sfruttare le informazioni captate per inventoriare il parco macchine, stabilire il programma di aggiornamenti del software o essere notificato in caso di problematiche di connessione degli host. Nmap è in grado di portare a termine la scansione sui principali sistemi operativi, tra cui Windows, Linux, OS X, ma anche Solaris, FreeBSD e Sun OS, e può essere eseguito sia in modalità linea di comando (utile per l'integrazione all'interno di file batch) sia attraverso una intuitiva interfaccia utente. La natura open source del progetto permette inoltre di modificare il codice sorgente per migliorare il pacchetto ed adattarlo alle proprie esigenze. Esistono anche diversi porting non ufficiali per Android, che permettono di analizzare la rete direttamente da smartphone e tablet.

**Wireshark** (gratuito per Windows, OS X, Linux, [www.wireshark.org](http://www.wireshark.org/)) è uno dei



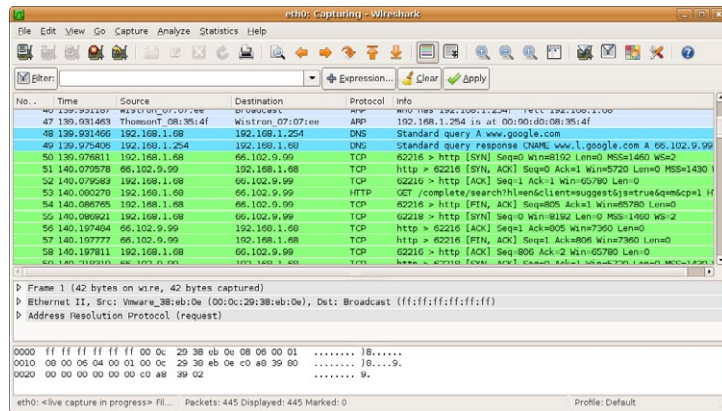
Nmap, un port scanner gratuito e potente.

più noti analizzatori di pacchetto presenti sul mercato. Precedentemente noto come Ethereal, richiede una discreta conoscenza di networking e presenta una curva di apprendimento impegnativa, ma offre una serie di funzionalità che difficilmente si possono trovare anche all'interno di pacchetti commerciali dal costo non indifferente.

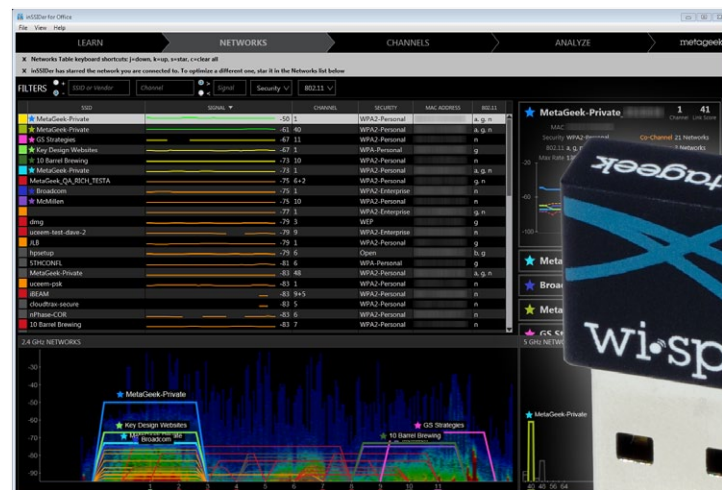
Wireshark cattura i pacchetti in transito sulla rete e li analizza alla ricerca di anomalie. In base ai problemi rilevati, i pacchetti sono evidenziati attraverso una gamma di colori che identifica il relativo livello di allerta, dalla semplice ripetizione di un errore di comunicazione alla presenza di pacchetti dal contenuto non ben formato, ovvero non conforme ai protocolli utilizzati.

Le anomalie possono indicare malfunzionamenti del tutto "innocenti", come un server che non risponde più per un semplice guasto, o traffico maligno che potrebbe essere sfruttato per mettere in crisi la rete, come nel caso degli attacchi Dos e Ping of Death. I pacchetti possono essere filtrati secondo regole specifiche in modo da semplificare l'analisi ed eliminare dalla visualizzazione il traffico lecito e non problematico. Oltre ai classici pacchetti IP, Wireshark può analizzare il traffico Wi-Fi, Bluetooth e Usb, anche in questo caso rilevando comportamenti anomali che possono compromettere l'efficienza o la sicurezza della struttura informatica.

**InSSIDer** (19,99 \$, per Windows e Mac OS X, [www.inssider.com](http://www.inssider.com)) si focalizza sulle trasmissioni wireless, con una serie di soluzioni adatte sia alle grandi aziende sia ai piccoli uffici. La versione base del programma consente innanzitutto di rilevare le reti Wi-Fi presenti nel raggio di azione, raggruppandole in base all'identificativo di rete o al canale di trasmissione. Inoltre, visualizza



Wireshark, uno dei più diffusi analizzatori di rete.



InSSIDer, uno strumento specifico per l'analisi di reti wireless.

lizza le reti in conflitto, permettendo di eliminare le interferenze distruttive all'interno della propria struttura o di massimizzare la resa in caso di coabitazione con reti wireless di terze parti operanti sui medesimi canali. Il monitoraggio in tempo reale dei segnali permette poi di verificare l'andamento della potenza di emissione del singolo access point con il passare del tempo. InSSIDer supporta l'analisi delle bande 2,4 e 5 GHz, anche in contemporanea, e supporta tutti i protocolli 802.11, tra

cui l'ultima versione "ac". Il solo software rileva unicamente le trasmissioni radio delle reti Wi-Fi. La versione inSSIDer Office (199 dollari) amplia le funzionalità, anche grazie all'adattatore Usb Wi-Spy Mini incluso. In questo caso l'hardware consente di rivelare le trasmissioni radio operanti sulle medesime frequenze del Wi-Fi ma provenienti da altri sistemi di comunicazione come tele-allarmi, baby-monitor senza fili, telefoni cordless e altro ancora.



“Gli analizzatori di pacchetto intercettano il traffico in transito alla ricerca di anomalie, i port scanner interrogano i vari terminali presenti in rete per individuare tra l'altro quali siano i canali di comunicazione aperti.”