



Sniffer, gli spio

Hanno un nome strano. Gli esperti di sicurezza ne parlano spesso. A volte vengono usati dagli hacker... di cosa stiamo parlando? Degli sniffer, ovviamente

In effetti il nome "sniffer" suona un po' strano per una categoria di programmi così importante, anche perché ricorda, per la sua onomatopea, un qualcosa che serve ad annusare. Cosa non molto lontana dalla verità, perché lo sniffer ha, in un certo senso, proprio il compito di "annusare" come un segugio i byte che circolano su una rete.

Occhio al segugio

Si tratta di un software molto particolare, nato in passato solo per i sistemi Linux, che negli ultimi anni

ha trovato la sua evoluzione naturale anche su Windows, a causa della continua crescita dei computer connessi alla Rete.

Lo sniffer può, di fatto, considerarsi una via di mezzo tra un firewall e un debugger, poiché si inserisce tra il sistema operativo e una connessione di rete (proprio come fa un firewall) e cattura tutti i pacchetti scambiati, byte dopo byte, da e verso il mondo esterno, consentendo poi ad un utente di analizzarli e decodificarli (cosa che ricorda molto i debugger) per cercare errori di trasmissione o informazioni

di vario genere.

Che software! Raro come un tartufo

C'è da dire che su Internet è raro trovare sniffer buoni per Windows, ancor meno in versione trial o dimostrativa, tuttavia noi siamo riusciti nell'intento e dopo svariate ricerche, abbiamo scelto Sniff'em, uno sniffer (chiamato anche network analyzer) per sistemi Windows 9x/Me a dir poco grandioso, che abbiamo anche testato in queste pagine (le versioni per XP e 2000 sono pianificate e

Info

IL SITO UFFICIALE:
www.sniff-em.com

DOVE LO TROVO:
Sniff'em è prelevabile direttamente alla pagina www.sniff-em.com/download.shtml in versione trial con alcune limitazioni. E' possibile richiedere al produttore anche una versione "full enabled", limitata solo nel tempo d'uso, mandando una e-mail all'indirizzo demo@sniff-em.com.

A CHI RIVOLGERSI:
YASC (www.yasc.net)
Thierry Zoller
thierry@sniff-em.com

NOTE SULLA VERSIONE:
Le versioni in prova di Sniff'em sono tre in tutto: le prime due sono trial limitate in half-duplex (cioè capaci di catturare solo i pacchetti in uscita) per sistemi Win9x/Me e Win2K/XP; la terza, da richiedere esplicitamente, è invece una versione completa full-duplex (cattura pacchetti in entrata e in uscita) utilizzabile per 30 giorni, periodo dopo il quale cessa di funzionare.

