



Anno 2 - N. 36
23 Ottobre - 6 Novembre 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it

Contributors: bismark.it, Michele "SoNiK©" Bruseghin, Nicola D'Agostino, DaMe', fantoibed, Imperator, pctips, >>—Robin—>>, Vincenzo Selvaggio, Angelo Zarrillo, Il Coccia

DTP: Cesare Salgaro

Graphic designer: Dopl Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa, elaborazione di Warcraft 3

Publishing company

4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing

Roto 2000

Distributore

Parrini & C. S.P.A.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti

Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190. Direttore responsabile - Editore Luca Sprea

Gli articoli contenuti in Hacker Journal hanno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilita' circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione gratuita su qualsiasi pubblicazione anche non della 4ever S.r.l.

Copyright 4ever S.r.l.

Testi, fotografie e disegni, pubblicazione anche parziale vietata.

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack'er (hāk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

UN FANTASTICO FORUM

Il forum del sito di Hacker Journal è pieno zeppo di argomenti, discussioni e posizioni interessanti, utili e anche divertenti. E' una cosa viva, e questo grazie soprattutto a voi.

Tanto bello che, a gran voce, gli utenti del forum richiedono una maggiore interazione con la rivista "di carta", e non hanno tutti i torti. Qualcuno ha anche proposto di pubblicare sulla rivista i messaggi più interessanti del forum. L'idea non sarebbe male, se avessimo a disposizione molte pagine da utilizzare. Invece HJ è piuttosto piccola. Credo quindi che replicare sulla rivista i contenuti del forum non sia una buona idea.

E poi, molto spesso, il bello di un thread ben "riuscito" è che nel confrontarsi con gli altri, le posizioni cambiano, si smussano. Oppure si radicalizzano. Dipende. In ogni caso, il thread si arricchisce di nuove idee. Questo è possibile proprio perché il forum (come newsgroup e mailing list) gode di quella fantastica caratteristica di Internet che è l'interazione bidirezionale in tempo reale. Una caratteristica che sulla carta verrebbe irrimediabilmente sacrificata (io scrivo, tu leggi).

Prossimamente, quindi, cominceremo a pubblicare nella pagina 3, qui accanto, alcune segnalazioni sugli argomenti più dibattuti, sui singoli messaggi più interessanti, e anche resoconti su cosa succede nella nostra piccola, grande comunità. Per fare esercizio, metto un esempio di ciò che si potrà trovare dal prossimo numero:

La tua ultima visita è stata: 14 Ott 2003 03:25 pm
La data di oggi è: 14 Ott 2003 03:44 pm
Indice del forum

Guarda i messaggi dall'ultima visita
Guarda i tuoi messaggi
Guarda i messaggi senza risposta

Forum	Argomenti	Messaggi	Ultimo Messaggio
Generale			
Annunci Annunci dalle Staff. Moderatore Carmageddon	13	10	14 Set 2003 10:23 am bismark
Forum Generale Di la tua sulla rivista... commenti, critiche per migliorare hj Moderatore Carmageddon	388	3252	14 Ott 2003 03:18 pm hubevaluation
Try2hack-Reloaded Nuovo gioco di hj.it e glesius.it... Moderatore Glesius	180	971	14 Ott 2003 03:17 pm F2Rw
Uplink Il forum sul gioco... consigli e tanta altro Moderatore Carmageddon	38	169	06 Ott 2003 08:12 am arneth
Filosofia Hacker Il significato di "hacker", commenti, pensieri... Moderatori Mio_Cutty, Lord_Dex	76	1387	14 Ott 2003 11:57 am Mio_Cutty
In Edicola Tutti i numeri commentati da voi...	28	256	13 Ott 2003 09:29 pm fuocafelice
Sicurezza			

"Nel Forum Generale si sta discutendo di come far interagire meglio il sito e la comunità di HJ con la rivista. L'idea è nata da un post di JF[k], subito raccolta da molti altri membri (INTERNaTo, ~brc~ e Neurromante tra i primi). Stiamo valutando come individuare il miglior materiale del forum per segnalarlo sulla rivista, e si sta costituendo un gruppo di volontari. Se vuoi partecipare, corri subito a leggerti il thread".

grand@hackerjournal.it

FREE HACKNET

Saremo di nuovo in edicola Giovedì 6 novembre !



La prima rivista hacking italiana

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI
E ARTICOLI

LE PASSWORD PER IL SITO DI HJ

Ogni tanto, qualcuno ha dei problemi con le password per accedere ai servizi protetti del nostro sito. Qualche volta, si tratta di un errore vero, ma molto più spesso la risposta è una delle seguenti:

1) Per tutti i servizi che richiedono una password, è necessario che i cookie siano abilitati nel browser, e che non ci siano programmi di terze parti che bloccano la ricezione dei cookie.

2) Nell'inserire le password della Secret Zone, fai attenzione a lettere e numeri. Tutti i codici usati sono una combinazione di lettere e numeri che può essere letta come una parola di senso compiuto. Per esempio, 2llo (duello, e non 2110), 9lla (novella, e non 911a) e così via

3) Le password valide sono sempre quelle pubblicate sulla rivista attualmente in edicola, e scadono quando esce il numero nuovo.

4) Lo username da usare per la casella di posta è l'indirizzo completo, e non solo il nome utente scelto. Per esempio, devi usare "tuonome@hackerjournal.it" e non solamente "tuonome".

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici.

Non fermatevi al primo tentativo!

user: **nett1**
pass: **abb8nato**

FREE HACKNET



freeHACKnet è il servizio gratuito di collegamento a Internet targato Hacker Journal: indirizzo email @hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Niente abbonamento, nessuno sbattimento, paghi solo la tariffa telefonica urbana. Corri subito a iscriverti su www.hackerjournal.it/freeinternet

I vostri siti...

Mandate le vostre segnalazioni a redazione@hackerjournal.it, ma evitate di linkare siti con crackz, numeri di serie, virus, trojan eccetera...



www.animatrixzone.tk



mailto:

redazione@hackerjournal.it

LINUX E MODEM: NON SEMPRE È GRAVE...

Ho da poco comprato un MODEM BLASTER V.92 SERIAL della CREATIVE... il mio linux (mandrake 9.0) lo ha riconosciuto come un qualsiasi altro modem... ma quando vado a connettermi mi da un errore ... cioè mi dice che non trova il segnale ... anche se in realtà il classico TURTLE io lo sento benissimo !!!!! Ho cercato driver per aggiornare il mio linux... ma non ho trovato nulla

Linux ha un po' di difficoltà a usare i modem progettati per lavorare solo con Windows (i famosi WinModem) ma in questo caso, molto probabilmente, non si tratta di una incompatibilità, quanto di una sbagliata configurazione.

Molti modem sono impostati per rilevare il segnale di "linea libera" in uso negli USA (e altri paesi). Questo segnale è diverso in Italia, quindi il modem crede di non essere collegato ad alcuna linea telefonica. Ti basta impostare il software di connessione per ignorare il segnale di linea, oppure aggiungere X3 alla stringa di configurazione del Modem (dovresti trovarla sempre nel tool di connessione).

IRC VIA CELLULARE

Son dovuto andare fuori città per studiare e mi son portato il portatile e l'ho collegato al mio cellulare gprs. Ho attivato la promozione gprs omnitel flat e mi connesso a internet tranquillamente. Il problema sorge quando devo connettermi a server irc per chattare (vorrei infatti mantenere i contatti con persone della mia città). Infatti nn riesco a entrare in nessun server se non su azzurra.net (oppure org). Direte voi, non vanno bene questi server? No visto che non c'è il canale di mio interesse (trapani). La stringa di errore che da è Too many host connection oppure bad password. Informandomi di qua e di là sembrerebbe che il problema sia che omnitel assegna molti ip uguali e irc ne accetta al massimo 2 a volta! Infatti è successo solo una volta che sono riuscito a connettermi a irc.tin.it! Sembra dunque che il problema sia una restrizione omnitel o roba simile. Vorrei però da voi maggiori delucidazioni e soprattutto (una soluzione). Voglio mantenere dei contatti di chat. Non entra neanche dai siti web irc. Vi prego di essere più elementari possibili visto la mia scarsa conoscenza di informatica applicata alle reti ecc ecc! Grazie mille!

Alessandro

Il problema non è di Vodafone, ma dei server Irc. Per evitare affollamenti e uso di cloni, molti server Irc limitano il numero di connessioni effettuate da uno stesso indirizzo IP. Nei casi normali, non ci sono problemi. Se invece si usa un provider che fa uscire tutti i suoi abbonati con uno stesso numero IP (il proxy del provider), come quelli Gprs o gli abbonamenti Fastweb, è possibile vedersi rifiutare l'accesso da parte del server Irc, perché qualcun altro è già collegato col nostro stesso indirizzo IP.

Dovresti quindi chiedere a chi amministra i server Irc di risolvere il problema. Per Fastweb, ad esempio, Azzurra ha predisposto un server particolare, al quale si possono collegare gli utenti di questo provider.



Tech Humor



FIREWALL E IDS

Approfitto per farvi una domanda che mi perseguita: esiste un firewall per linux che assomigli a Tiny personal firewall (ora Kerio) per Windows, ovvero che mi chieda dinamicamente se tale programma debba connettersi a tale indirizzo, un personal firewall per internet da casa, insomma, dato che trovo le regole di iptables troppo fisse e non applicabili solo ad un dato programma (che io sappia) e soprattutto non interattive; non mi va di chiudere tale porta o indirizzo a *tutti i programmi*. Ho provato vari programmi, ma si sono rivelati come non altro che frontend per iptables; ho provato poi firewallbuilder, ma è fatto per chi ha una VPN o cose simili...Spero in una risposta, anche in privato.

Algol

In realtà, sebbene software come Kerio o ZoneAlarm si definiscano Firewall, le funzionalità di cui parli non rientrano strettamente in questa categoria. Il firewall infatti si limita a consentire oppure no connessioni da e verso il PC in base a regole che riguardano solo il protocollo o la porta impiegata, o gli indirizzi degli host remoti che richiedono la connessione. Quello di consentire o meno a un certo programma di collegarsi a Internet, o di agire come server, è il compito di programmi per il controllo dell'accesso a Internet, o al limite degli IDS (Intrusion Detection Systems). Il problema però su Linux è



Tech Humor



Apple iMac



Rowenta Surfline Iron



Separati alla nascita?



meno sentito: su Windows è infatti facile che un programma si installi a insaputa dell'utente, e che mascheri le sue connessioni a Internet. Su Linux, invece, per installare un programma è necessaria la password di amministrazione, ed è molto più difficile che un software faccia connessioni all'insaputa dell'utente del PC.

MAME ED EMULATORI SUL NOKIA N-GAGE?

Siccome sta per uscire il tanto discusso Nokia N-Gage;



volevo sapere se esistono versioni del Mame e del Genecyst (emulatore Sega Mega Drive) compatibili con il questo cell. e anche dove poterlo scaricare.

Daniele Commodore Boy

Credo sia ancora troppo presto, ma sicuramente è un settore da tenere sott'occhio. Indagheremo...

GRAFICA 3D E CAD SU LINUX

Sono un Vostro lettore sin dal primo numero, ma ancora per certe cose sono un newbie. Ho iniziato adesso ad usare solo

Hardware: The parts of a computer system that can be kicked.



linux, ma volevo sapere una cosa che non sono riuscito a trovare in giro sulla rete: Esiste una versione sotto licenza GNU di Maya ed AutoCAD???

Siete mitici...

THE_SHARK

Il sito sourceforge.net, praticamente la biblioteca di Alessandria del software libero, elenca 370 progetti di modellazione 3D, e 661 per il rendering. Al momento, nessuno sembra

avere la popolarità e le caratteristiche di Maya o Autocad, ma senz'altro vale la pena di spulciare i vari progetti alla ricerca di qualcosa di interessante. Qcad, per esempio, è un CAD per Linux che gestisce nativamente il formato Dxf di Autocad (www.ribbonsoft.com/qcad.html). E' rilasciato sotto licenza GPL, mentre altri CAD per Linux sono invece commerciali.

Per quanto riguarda la grafica 3D, invece, si sta facendo spazio Blender, un software originariamente proprietario e per piattaforma Windows ma ora - dopo che ne sono stati rilasciati i sorgenti sotto licenza GPL - è stato portato su altre piattaforme, tra cui Linux e Mac OS X.

HACKING E MAC

Ho notato che da qualche numero avete smesso quasi completamente di parlare di Macintosh. OK, alcuni programmi citati o tecniche descritte si possono usare paro paro anche su Mac OS X, ma ogni tanto un articolo sui computer della mela ci può anche stare, no?

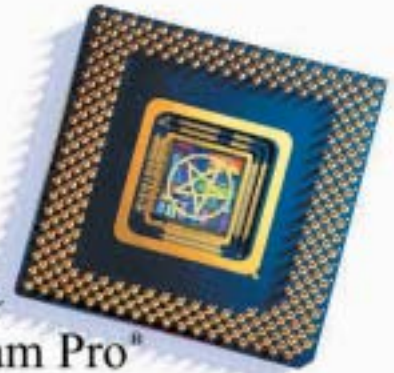
Macniaco

Purtroppo, con il ridotto numero di pagine a disposizione, ogni tanto dobbiamo operare delle scelte, e sacrificare qualcosa. I dati di accesso al nostro sito mostrano che i lettori che navigano col Mac non sono poi così tanti da giustificare una rubrica fissa. Dobbiamo, per forza di cose, cercare di accontentare il maggior numero

inhell.

666 mhz
"A devilishly fast CPU!"

Pentagram Pro[®]
Processor



possibile dei nostri lettori. Parlando di sito, queste limitazioni ovviamente non valgono per il forum, dove gli articoli di ogni tipo, anche su Mac OS X, sono i benvenuti. Hacker della mela, fattevi avanti.

PRECISAZIONI SU IP TABLES

Cara redazione vorrei segnalare un imprecisione nell'articolo del n°35 "Gli errori di Verisign", in cui si dice di creare la regola di iptables con

```
iptables -A blocked_sites -p TCP -d 64.94.110.11 -j REJECT --reject-with icmp-host-unreachable
```

Questo comando "appende" una regola, che se non esiste deve essere precedentemente creata con

```
iptables -N blocked_sites
```

altrimenti il programma segnala un errore (Unknown arg '-j'), dopodiché si può digitare il precedente comando; poiché l'articolo ha due teschi credo sia stato dato per scontato, ma potrebbe disorientare un principiante come me.

NEWS



HOT!

LIBRI DI SCUOLA GRATIS

Provate a immaginare un libro di scuola che non si paghi. Un libro vero, stampato, con tutto quello che serve per studiare: ma gratuito. Provate a immaginare un libro di scuola che cresca ogni anno, che si arricchisca di nuove proposte, idee, contributi. Provate a immaginare un libro che, prima di finire sui banchi della vostra scuola, nasca da altri banchi, si nutra del pensiero e del lavoro di altre scuole. Provate a immaginare di diventare voi autori di questo libro". Così parlano i curatori del progetto Scuola OnLine (<http://edu.supereva.it/scuolaonline/>), ...e noi non avremmo saputo dirlo meglio.

POVERI PROGRAMMATORI

Qualche anno fa si permettevano di rifiutare lavori da 100 milioni l'anno, e oggi sono tra le figure meno retribuite nel mondo informatico. Stiamo parlando dei programmatori, e l'osservazione prende spunto da un rapporto pubblicato da Assinform, l'associazione delle aziende che operano nel mondo della cosiddetta Information Technology (www.assinform.it).

SEGRETI IN UFFICIO

Di solito, incontra i suoi clienti di notte o nei weekend, quando non c'è nessuno in giro. Alcuni di essi, esigono che lei chiami solo sui loro telefoni cellulari, per paura dei pettegolezzi delle segretarie". Così inizia un articolo pubblicato su MSNBC che parla della curiosa professione di Jennifer Shaheen. Ma cosa avete capito? Jennifer insegna in segreto i rudimenti dell'uso di un PC a potenti manager che - si suppone - dovrebbero essere bene avvezzi nell'uso di un computer, ma che spesso hanno bisogno di aiuto per spedire un'email o aprire un foglio di calcolo.

VERISIGN (PER ORA) BLOCCA SITEFINDER

Sui numeri scorsi avevamo parlato del discusso "servizio" Site Finder di Verisign, l'azienda che gestisce i domini .com e .net. Grazie a modifiche apportate nei DNS centrali di Internet, Verisign

aveva fatto in modo che tutte le volte che un utente digitava un indirizzo sbagliato, con suffisso .com o .net, venisse ridirezionato su un motore di ricerca a pagamento di proprietà di Verisign, appunto.

Verisign ha per fortuna deciso di bloccare l'odioso servizio, dopo le reazioni negative di milioni di utenti Internet, centinaia di aziende e soprattutto dopo che l'icann, l'ente deputato a gestire i domini .com e .net, aveva minacciato di revocare a Verisign la concessione per la gestione dei domini in questione.



Verisign però ha detto che si tratta di un blocco temporaneo, e che in un modo o nell'altro tornerà alla carica, perché ha bisogno dei soldi che potrebbero provenire

dalle inserzioni a pagamento su SiteFinder per gestire in tutta sicurezza l'infrastruttura dei domini su Internet. Nel tentativo di raccogliere consensi, Russell Lewis (Vice Presidente di Verisign) ha fatto quello che ogni buon presidente USA farebbe al suo posto: ha sventolato lo spauracchio dei nemici cattivi, e ha dichiarato che "senza le risorse di SiteFinder, Verisign potrebbe non riuscire a fronteggiare un attacco ai DNS centrali come quello sferrato da alcuni cracker nell'ottobre 2002. Rabbriviamo.

LE SETTE VITE DI NAPSTER

Se il simbolo di Napster è da sempre un gatto, un motivo ci sarà. Secoli fa, quando con Internet uno studentello poteva guadagnare miliardi inventando un sistema per scambiarsi musica su Internet, Napster è stata la prima società a raggiungere le alte vette della finanza con un piano affaristico sfacciatamente in odore di illegalità, e altrettanto velocemente precipitare al suolo e chiudere i battenti in seguito all'azione giudiziaria degli industriali della musica.



Il marchio però era forte (probabilmente il software che vanta nel nome il maggior numero di imitazioni: Grokster, PhAster, Macster, Aimster e via clonando), e quindi varie aziende si sono battute per acquistare il diritto di usarlo. A differenza delle altre aziende proprietarie, l'ultimo detentore del marchio, Roxio, ha deciso di mettere a frutto l'investimento, questa volta però all'insegna della legalità. Roxio ha infatti stretto accordi con le majors per vendere musica online, con modalità e prezzi simili al servizio iTunes di Apple o Listen.com: comprare un brano su Napster costerà 99 centesimi di dollaro, mentre serviranno 9,95 dollari per acquistare un intero CD. Al momento, il servizio è attivo solo per gli Stati Uniti.



➔ LINUX COMPIE 2.6 VERSIONI



La versione finale del Kernel 2.6 di Linux dovrebbe vedere la luce entro fine novembre. Lo ha dichiarato Linus Torvalds in persona, che ha anche congelato tutte le attività di sviluppo che non siano tese a risolvere problemi già esistenti. Difficilmente le novità più importanti avranno però risalto per l'utilizzo domestico o personale del Pinguino;

le nuove funzionalità e i miglioramenti principali sono mirati a un più efficace utilizzo in ambito aziendale (pare che per i WinModem bisognerà dannarsi l'anima ancora un po'...), e non a caso tra le prime distribuzioni a permettere l'installazione di un kernel 2.6 di prova troviamo SuSE Linux 9.0 (la casa tedesca è tra le favorite per quanto riguarda l'utilizzo professionale di Linux).

➔ UNA PROTEZIONE MINUSCOLA PER I CD



BMG ha introdotto su alcuni suoi titoli di CD musicali una nuova tecnologia anticopia, chiamata MediaMax CD3 e sviluppata da SunnComm

basta tenere premuto il tasto shift mentre si inserisce il CD nel lettore del computer. Tutto il meccanismo si basa infatti sulle funzionalità di autorun di Windows e Mac OS X; disabilitando l'autorun, infatti, la protezione è inefficace.

Gli oppositori dell'industria della musica impegnati a sbeffeggiare SunnComm e BMG, però, probabilmente non hanno riflettuto su alcune dichiarazioni fatte da queste aziende. Le due, infatti, hanno dichiarato di essere perfettamente consapevoli di quanto facilmente la protezione potesse essere aggirata, ma di aver voluto creare un sistema non troppo restrittivo, in modo da scoraggiare le copie occasionali senza penalizzare troppo chi il CD lo ha acquistato e ha tutto il diritto di duplicare il CD o copiare i brani su un lettore portatile. Un segnale interessante o un disperato tentativo di salvare la faccia?

Technologies. La notizia è rimbalzata sui siti di notizie di tutto il mondo non tanto per la novità tecnologica, ma piuttosto perché per disabilitare questo sistema di protezione, e fare quante copie si vuole del disco acquistato,

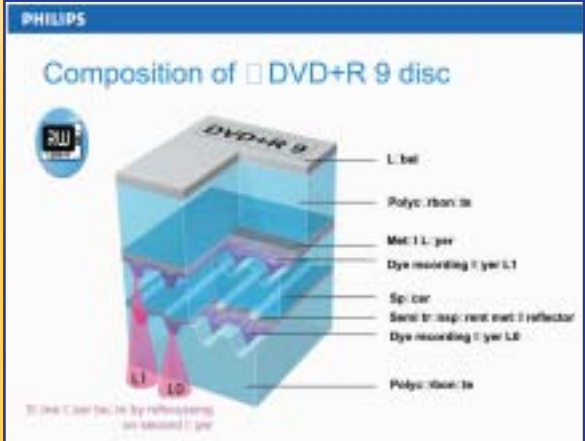
➔ I BLOG STANNO UCCIDENDO GOOGLE?

Questa è la tesi di alcuni specialisti della ricerca su Internet, secondo i quali la facilità con cui si può usare la funzionalità di TrackBack per collegare tra loro i messaggi pubblicati su blog diversi, può portare ad alterare sensibilmente le graduatorie con cui Google restituisce i risultati. Google infatti

classifica più in alto tra i risultati proprio quei siti e quelle pagine che vengono citate su altri siti, e quindi presumibilmente attendibili. Ora, coi blog, questo avviene sistematicamente, anche quando il contenuto in questione non è poi così importante da meritare un piazzamento così elevato.



➔ DVD-R A DOPPIA FARCITURA



Uno dei limiti degli attuali DVD registrabili è che, su una singola faccia, possono registrare solo la metà dei dati che è possibile infilare in un DVD vero e proprio (4,7 GB contro 9). Ebbene, Philips è riuscita a creare dei supporti (e un masterizzatore) in grado di scrivere i dati su doppio strato, come accade coi DVD commerciali, arrivando fino a 8,5 GByte. Il nuovo sistema, chiamato DVD+R 9, vedrà la luce entro il 2004.

➔ OPEN OFFICE: PUNTO UNO E A CAPO



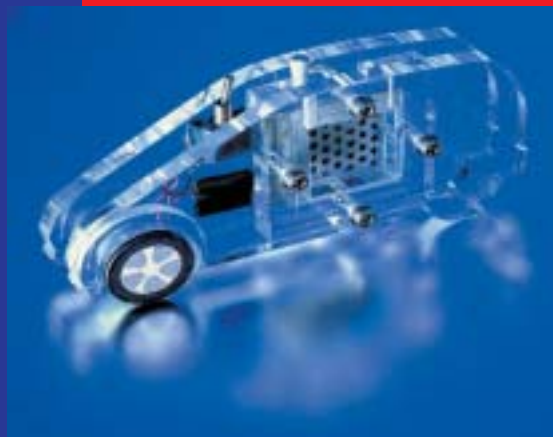
interfaccia migliorata, supporto di nuovi formati di file tra cui PDF, Flash, XML e XHTML, migliore compatibilità con l'Office di casa Microsoft e prestazioni migliorate: queste le credenziali con cui si presenta la versione 1.1 di OpenOffice, suite open source che mira a risolvere tutte le esigenze di produttività di un ufficio (word processor, foglio di calcolo, presentazioni, grafica...). Il pacchetto è scaricabile gratuitamente da www.openoffice.org per Windows e Linux; non ancora pronto invece l'aggiornamento per la versione Mac OS X, che segue un filone di sviluppo parallelo e non sincronizzato.

NEWS



NOTI

IL PIENO AL NOTEBOOK



Toshiba ha presentato la sua prima di cella a combustibile portatile, che utilizza metanolo per produrre energia elettrica; il modello in questione è pensato come batteria "di emergenza" per cellulari o altri dispositivi, ma sono in molti a ritenere che questo tipo di batterie diventerà lo standard per tutti i dispositivi elettronici portatili ad alto consumo, come cellulari o computer portatili. Con un "pieno" di metanolo si può produrre continuamente un watt di potenza per 20 ore: mica male...

IL PIÙ BEL LAVORO AL MONDO

Macché fluffer... il parco di divertimenti Legoland California sta selezionando persone che possano assumere il ruolo di "Master Lego Model Builder" all'interno del complesso. In pratica, si tratta di creare e mantenere le svariate (ed enormi) costruzioni di mattoncini di plastica colorata presenti nel luna park.



MICROSOFT E TRIBUNALI

In molti ci hanno pensato almeno una volta, ma la californiana Marcy Hamilton ha fatto seguire le parole ai fatti. Ha intentato una causa contro Microsoft, ritenendola corresponsabile della diffusione di virus e worm, e della facilità con cui si può entrare in un sistema Windows remoto, evento



questo che è alla base di un "furto di identità" che la donna ha subito nei mesi scorsi. È difficile che la Hamilton la spunti in tribunale, ma l'episodio fa riflettere su certe clausole delle licenze del software che sollevano il produttore

da qualsiasi responsabilità, anche in casi di negligenza o ingenuità palesi.

Nel frattempo, in Israele, il ministro del commercio ha sospeso ogni contratto governativo con Microsoft (upgrade compresi), per via del verdetto dell'autorità antitrust

israeliana, che ha stabilito che Microsoft è un monopolio. Alla base della vicenda ci sono le proteste di associazioni di consumatori che lamentavano il mancato supporto delle lingue ebraiche e arabe nella versione Mac di Office.

RADAR BASATI SUI CELLULARI

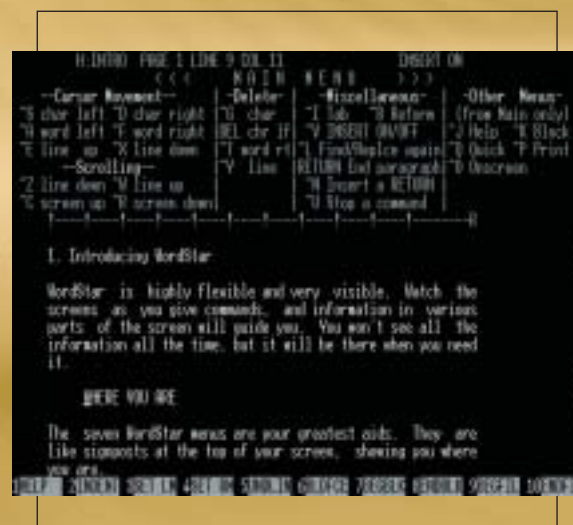
Se già siete preoccupati del fatto che, grazie al vostro cellulare, è possibile sapere in quale zona vi trovate, e ricreare una mappa dei vostri spostamenti, state a sentire questa: una nuova tecnologia, denominata Celldar, promette di riuscire a individuare in modo preciso veicoli in movimento in una zona coperta dalle reti cellulari. Il principio è semplice: un radar emette un segnale radio e calcola la posizione degli oggetti in base al segnale che rimbalza e torna indietro. Celldar non ha bisogno di emettere alcun segnale: sfrutta le onde radio dei ripetitori dei cellulari, radio e TV. L'apparecchiatura necessaria è talmente economica (una postazione costa

circa 3000 dollari) che il rischio che Celldar venga adottato come sistema di controllo di una nazione intera è molto elevato.



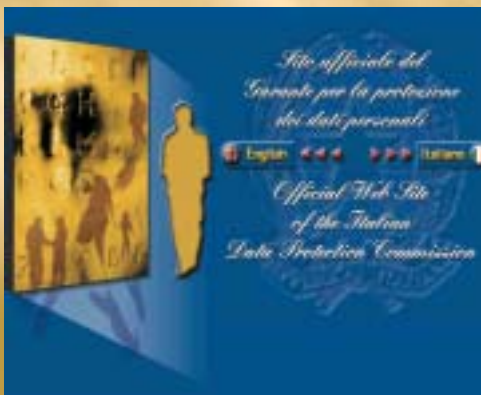
ARCHEOLOGIA DEL SOFTWARE

Brewster Kahle di Archive.org (che ospita tra l'altro le vecchie versioni di siti Web), vorrebbe tramandare ai posteri anche i vecchi software, originariamente memorizzati su floppy disk e per questo destinati a scomparire, visto che il rapido invecchiamento di questi supporti li renderà illeggibili in breve tempo. Purtroppo, il più grosso ostacolo che Brewster sta incontrando non è di tipo tecnologico, ma burocratico: duplicare quei programmi comporterebbe una violazione delle leggi americane sul copyright (il temibile DMCA). Lotus 1-2-3, WordStar e altre perle del passato rischiano quindi di scomparire per sempre.



➔ WOW. IL GARANTE SERVE A QUALCOSA

Tra i varie autorità di garanzia italiane, quella per la privacy è probabilmente tra le più attive, pur nei limiti imposti dal tipo di istituzione, che emette pareri più che prendere provvedimenti. Questa volta invece il Garante Rodotà ci è andato giù con la mano pesante contro sette aziende accusate di spamming: congelamento dei database, in attesa di un giudizio definitivo, che potrebbe addirittura prevedere il carcere. Così si fa! Parlando dell'authority, è online una nuova versione del sito, www.garanteprivacy.it, molto più snella e navigabile della precedente.



➔ HALF LIFE 2 COLPITO AL CUORE

Molti giocatori stavano aspettando il rilascio di Half Life 2, sequel di uno dei giochi più



innovativi degli ultimi anni. Qualcuno dovrà attendere un po' più a lungo, mentre qualcun altro potrà vederne qualche anticipazione fuori programma. Il codice sorgente del gioco è infatti stato rubato, e questo creerà non pochi problemi ai produttori. Il gioco è stato prelevato dai server della società attraverso Internet, e diffuso poi in Rete. Sebbene il solo motore di gioco non basti a creare un gioco completo, pare che il ladro sia riuscito ad aggiungere le componenti aggiuntive (grafica e musica) per produrre una versione funzionante, anche se non completa.

➔ DOMENICA IN: "BASTA" CREDERE ALLE FAVOLE



quando alla domanda "a cosa gli italiani dicono basta?" il primo posto è stato conquistato dalla risposta "Basta a Berlusconi e ai politici che dicono e non fanno".

Il direttore della comunicazione Rai, Guido Paglia, dice che fino a due giorni prima, nel sondaggio non c'era traccia di nomi di politici; come si spiega una così rapida scalata della classifica da parte di Berlusconi, se non con un intervento da parte di un pirata informatico? "Se gli hacker sono entrati al Pentagono...", è stato il laconico commento. Il consigliere di amministrazione Marcello Veneziani invece pensa a un sabotatore informatico interno alla Rai.

Cosa raccontano i dirigenti Rai ai loro figli prima che si addormentino? Ma la favola dell'hacker cattivo, ovvio. E il bello è che a questa favola sembrano crederci davvero (i dirigenti, non i figli). Questo è quanto emerge leggendo i commenti imbarazzati sull'episodio del sondaggio di Domenica In di metà ottobre,

L'hacker cattivo, al solito, diventa il capro espiatorio buono a giustificare qualsiasi inadempienza, imprevisto o nefandezza (anche col black out ci hanno provato...). Scommettiamo che anche l'effetto serra è opera di qualche smanettone cattivo che ha overclocato troppo il suo Pentium IV?

hacker

➔ IL VOIP (PER ORA) NON SI PAGA

Le autorità americane, dietro pressioni della Lobby delle telecomunicazioni, stanno prendendo provvedimenti per richiedere una licenza di operatore telefonico a qualsiasi azienda venda servizi per la telefonia "Voice Over IP". Per ora, la Corte Suprema sta cassando i provvedimenti presi da alcuni stati in questo senso, e quindi gli americani possono ben sperare che le telefonate via Internet rimangano gratuite. Noi, possiamo solo sperare che Telecom non lo venga a sapere...

➔ SMAU: QUANTI ANNI ANCORA?

smau

Cercando "Smau" su Google News compaiono titoli come "Smau 2003: soddisfazione tra gli espositori", "uno Smau compatto non è necessariamente ridotto", "meno pubblico ma di qualità" e "verso il rilancio di un'economia stagnante". Curioso, perché con quasi tutti i giornalisti che abbiamo incontrato in Smau ci siamo chiesti: "quanti anni durerà ancora Smau? Due? Tre?". Poche aziende espositrici, molti meno visitatori (e, al solito, per la maggior parte costituiti da quindicenni che hanno bigliato a scuola), e un meccanismo di spettacolarizzazione che costringe persino la serissima IBM a esibire finti predicatori americani che decantano deliranti il mantra aziendale (il Business On Demand...). Il settore, è risaputo, non attraversa un bel periodo, ma noi a Smau c'eravamo e vi assicuro che era una tristezza girare per quei padiglioni semivuoti...

Un DoS locale: Fork Bombing

Il termine Denial of Service spesso si associa ad attacchi alla rete ma esistono anche tipi di DoS locali.

Un attacco **Denial of Service**, in generale, ha come obiettivo principale quello di **rendere impraticabile un servizio** messo a disposizione da un certo sistema, occupando tutte le sue risorse. Quando leggiamo la sigla DoS, pensiamo subito ad attacchi alla rete, per esempio mirati a saturare la banda di un sito per renderlo inaccessibile ad altri utenti; in realtà esistono **anche DoS locali** (spesso definiti **Bombe Logiche**) il cui scopo è quello di imballare un sistema operativo che, in ultima analisi, è anch'esso un fornitore di servizi.

>> DoS locale

Effettuare un DoS necessita una profonda conoscenza della gestione delle risorse del sistema da attaccare. Se vogliamo rendere inutilizzabile un sistema Unix bisogna per prima cosa **conoscere come questo gestisca la memoria**, la risorsa che vogliamo intasare per renderlo inagibile.

Quando un processo deve essere eseguito, cioè deve passare dallo stato

Ready a quello **Running** (sul n.34 è stato pubblicato un articolo dettagliato sulla gestione dei processi), le sue pagine vengono caricate dal disco alla RAM (gestione detta **"a memoria virtuale"**). Le **pagine** non sono altro che dei blocchi di memoria a lunghezza fissa in cui sono contenuti dati e istruzioni. Non tutte le pagine relative ad un processo vengono caricate in RAM, ma solo un sottoinsieme che contiene almeno i dati e le istruzioni che occorrono al processore per eseguire il processo stesso (vedi **Figura 1**). Se durante la sua esecuzione il processo necessita di una pagina che risiede ancora su disco si genera un TRAP (meccanismo di interruzione) detta **"Page Fault"**. Quest'ultima interrompe il processo in esecuzione, carica la pagina opportuna in RAM (**SWAP IN**) e ripristina il processo interrotto che, quindi, può continuare la sua evoluzione. Evidentemente lo SWAP IN necessita di un precedente **SWAP OUT**. UNIX prevede una gestione a **"pagine libere"**: quando viene fatta una richiesta di SWAP IN già ci sono pagine libere da utilizzare. Altri sistemi operano a **"pagine piene"**, il che vuol dire che una pagina viene passata da

RAM a disco solo quando è necessaria l'operazione opposta. Quale sarà la pagina vittima dello SWAP OUT? In Unix viene utilizzato il cosiddetto algoritmo della **"Seconda Chance"**. Per una descrizione più dettagliata vediamo il **Riquadro** corrispondente.

>> Il punto debole

Se fossero caricati in memoria troppi processi, ad ognuno verrebbe attribuito un numero esiguo di pagine e quindi verrebbero generati troppi Page Fault. Addirittura si potrebbe causare il fenomeno del **TRASHING**: un processo ri-

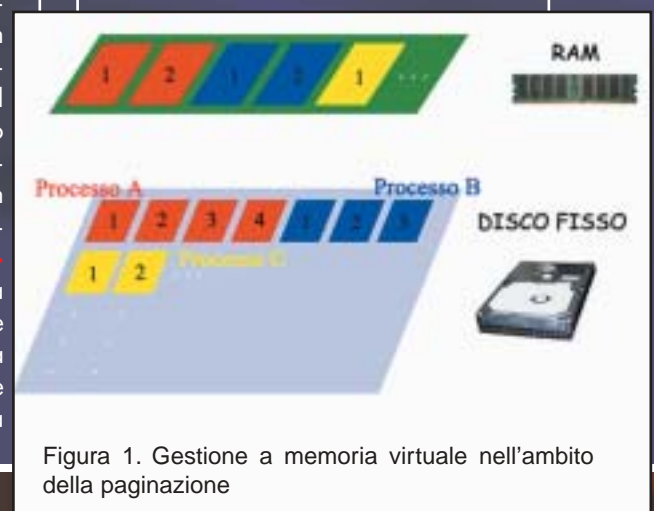


Figura 1. Gestione a memoria virtuale nell'ambito della paginazione

Programma forkbomb.c

```
//file forkbomb.c
#include <sys/types.h>

int main(){

    pid_t processo; //tipo identificatore di processo

    int i;//indice

    //generazione figli
    for ( i=0; i<100; i++)
        processo=fork();
    //Ogni figlio del processo padre esegue il ramo if
    if (processo==0){
        printf("Sono il figlio e genero miei figli\n");
        //generazione figli dei figli
        for ( i=0; i<100; i++)
            processo=fork();
    }
    else{
        // padre
        printf("Sono il padre\n");
    }
} //fine del main
```

chiederebbe più risorse per effettuare i Page Fault che per eseguire i propri compiti. Per evitare tutto questo, Unix prevede che il numero di processi in esecuzione sia limitato. Di qui, riuscendo ad eseguire un certo numero di processi, impediamo l'utilizzo del sistema: noi non possiamo avviare alcun altro programma, altri utenti non potranno nemmeno effettuare il **LOGIN**, perché per farlo Unix deve fornire loro una **SHELL**, l'interprete dei comandi, che è esso stesso un processo.

>> Fork Bombing

In Unix a partire da un processo (padre) possiamo generarne un altro attraverso la semplice primitiva **Fork()**. Questa non fa altro che generare un processo (**figlio**) con la stessa area dati e istruzioni di quello che lo ha generato, ma che prende un flusso diverso. Per discriminare il flusso del padre da quello del figlio la primitiva restituisce il valore zero al figlio e l'identificatore (**PID**) del figlio al padre. Ecco un semplice esempio:

```
pid_t processo; //identificatore di processo
processo=fork();//generazione del figlio
if (processo==0){
    // figlio
}
else{
    // padre
}
```

In pratica, dopo la **Fork()**, esisteranno in memoria due processi con lo stesso codice: il padre che esegue il ramo **else** e il figlio che esegue quello **if**. Da quello che abbiamo potuto capire dai paragrafi precedenti, il nostro scopo è quello di generare il massimo numero di processi che il sistema può contenere in memoria; nulla di più semplice: generare un ciclo con all'interno la funzione **Fork()**.

Come si può vedere dal programma **forkbomb.c**, il padre cercherà di generare 100 processi figlio e i figli, a loro volta, cercheranno di generare altri processi (figli dei figli) provocando una sorta di reazione a catena (**Figura 2**). Il sistema operativo logicamente non genererà tutti questi processi, ma solo una parte, per le questioni di cui abbiamo prima parlato. Il programma è innocuo e rallenterà il sistema solo per pochi secondi, questo perché i processi avranno il solo compito di stampare a video delle stringhe. Per rendere la fork bombing più efficace, basterà inserire funzioni ricorsive all'interno del blocco dei figli, mentre, se vogliamo



Algoritmo della Seconda Chance

Unix, come abbiamo già accennato, lavora a pagine libere le quali possiamo interpretare come un serbatoio che ha un livello minimo e uno massimo. Ad intervalli di tempo (ogni 250 millisecondi) viene attivato un DAEMON il cui compito è quello di controllare il serbatoio: solo se questo è sotto il livello minimo allora si attiva una procedura per riportarlo al massimo. Per implementare questa procedura, ad ogni pagina è associato un bit di riferimento, inizializzato a zero e settato ad uno ogni volta che si fa accesso alla pagina. Lo stato del DAEMON è proprio un puntatore ad uno dei bit di riferimento, i quali sono disposti in coda circolare: se il bit è uno, significa che quella pagina è stata utilizzata nell'ultimo intervallo di tempo, quindi viene posto a zero per dare una seconda possibilità (seconda chance). Dopo quest'ultima operazione il puntatore punterà al successivo bit e così via, fin quando non verrà trovato uno zero: in questo caso, dall'ultimo passaggio del DAEMON, la pagina non è stata più utilizzata, di conseguenza viene eliminata. Un'ultima considerazione da fare è che la procedura del DAEMON, una volta attivata, non si fermerà fino a che il serbatoio non è riportato al massimo livello.

tenere occupati pure i dischi rigidi, basterà inserire funzioni di apertura, lettura e chiusura dei file.

>> Conclusioni

I **Kernel** più aggiornati evitano questo tipo di attacco limitando il numero dei processi che ogni utente può generare simultaneamente. Di conseguenza, un attacco **Fork Bombing** non possiamo più sferzarlo in modalità utente ma solo ottenendo accesso privilegiato (**root**). Qui però entra in gioco l'abilità dell'attaccante con il **Buffer Overflow**. A buon intenditore poche parole! 🚩

Vincenzo Selvaggio
selvin@cplusplus.it



Figura 2. Fork Bombing con reazione a catena



Vi sono alcune analogie tra quegli hacker esperti di reti e computer e i geek. Descrivere però l'hacker come un geek o utilizzare il termine geek come sinonimo di hacker è sbagliato.

A

attus Norvegicus, in un suo scritto dal titolo **"del crank e del geek"** su Rekombinant, descrive il geek come **"il tipico impallinato di scienza e tecnologia, che legge fantascienza e che spesso si comporta in modo strambo e scarsamente socievole"**.

Ed è sempre stato così. In principio, infatti, geek (si pronuncia ghik e non va assolutamente tradotto come "geco") è riferito, in senso dispregiativo, a coloro che, durante il carnevale o altre feste, staccano a morsi teste di polli o serpenti e che assumono comportamenti così "stravaganti", da essere considerati alla stregua di selvaggi. In seguito viene esteso a chiunque abbia un stile di vita e di compor-

tamento "eccentrico", che vive ai margini della società, una **"persona intellettualmente capace, ma spesso oggetto di disapprovazione sociale"** (Merriam-Webster Dictionary), **"socialmente indesiderabile"** (High-Tech Dictionary).

Con l'avvento dell'informatica diviene anche **"un individuo la cui passione per i computer sopravanza le normali passioni umane"**

(Webopedia), una **"persona socialmente inetta ma, al contempo, esperta nell'uso dei computer"** (High-Tech Dictionary), **"qualcuno che mangia le 'cimici' dei computer per guadagnarsi da vivere"** (New Hacker's Dictionary di Eric S. Raymond). Questa sua natura lo distingue da un qualunque appassionato di computer e tele-

matica, lo rende però simile, ma non identico, all'hacker da giovane.

>> Ritratto dell'hacker da giovane

Geek, spiega Raymond, è soprattutto **"qualcuno che soddisfa tutti gli stereotipi negativi sugli hacker"**, **"un individuo privo di ogni pregio"**. Può però anche essere **"un pro-to-hacker allo stato larvale"**, anche definito 'turbo nerd' o 'turbo geek' (New Hacker's Dictionary). Quelli che oggi sono considerati dei **wizard** (maghi) o **guru** (santoni), cioè hacker specializzati in uno specifico campo, veri esperti in un settore, hanno spesso attraversato un periodo - è questa la "fase larvale" di cui parla Raymond - di concentrazione maniacale sul computer e di ossessivo apprendimento delle tecniche. Insomma una sorta di rituale di passaggio o di transizione. **"Sintomi comuni includono il perpetrarsi di più di un hacking run (sessione di hacking) di 36 ore alla settimana e il dimenticarsi di ogni altra attività"** (Federica Guerrini). Anche gli hacker del M.I.T, così come sono descritti da Steven Levy, erano dei geek, nel senso di "impallinati" di tecnologia, "primi della classe" che persero la testa per l'infor-



Non è un geek

matica, al punto che si potrebbe quasi parlare di una fase larvale della storia hacker. **"Tutto iniziò nel 1958 al Mit**, con gli amanti dei trenini del Tech model railroad club, le loro furtive utilizzazioni dei computer militari e la creazione dei primi programmi per suonare". Essere un hacker però significava e significa tuttora condividere un sistema di valori, sintetizzare l'etica (Federica Guerrini). **"Qui nacque l'etica hacker, una sorta di manifesto programmatico, che non poteva non far presa sull'humus libertario degli anni Sessanta.** Tecniche di scassinamento delle porte dei laboratori, telefonate gratuite e radio pirata, il mercato, la lotta per l'accesso all'informazione..." (Hackers, ed. Shake)

>> L'ascesa dei Geek

Il termine geek ha sempre avuto connotazioni negative ed è sempre stato attribuito a persone considerate prive di fascino e di utilità sociale. **Quando internet però comincia a diffondersi** al di là della ristretta cerchia degli hacker, **essere definiti geek non è più un insulto, ma un complimento.** Se gli hacker lo usano con orgoglio, ma nel suo significato di "disadattato", per dichiarare la propria indipendenza dalle normali aspettative sociali, tra quei ragazzi che cominciano

ad avvicinarsi alle nuove tecnologie informatiche, geek è una **"persona eccezionalmente appassionata di computer e amante della telematica"**. Molti di essi passano gran parte del loro tempo nelle cosiddette "case dei geek", ma contrariamente a quanto affermato dai media, le frequentano non certo per isolarsi, ma per avere più facile accesso alle tecnologie informatiche. Queste "teco-comunità" - spiega John Katz - "trovavano la loro ragion d'essere nel fatto che le connessioni alla Rete erano rare e costose, che la condivisione di hardware, software e accesso a Internet (spesso fraudolento) era una necessità". Le case dei geek scompaiono, ma il termine continua a diffondersi riferito a tutti coloro che si dedicano ossessivamente allo sviluppo di Internet e del World Wide Web, ma anche a tutti quelli che partecipano con entusiasmo alla nuova

rivoluzione tecnologica. John Katz nel 1999 parla dei geek come di una **"nuova élite culturale caratterizzata da individui socialmente scontenti, amanti della cultura pop e delle nuove tecnologie"**. Quando internet diventa una moda e i computer strumenti importanti per la vita di tutti, e il mondo del lavoro richiede sempre più figure specializzate in campo informatico, i geek sono i più esperti e quindi gli unici capaci di operare con i sofisticati sistemi informatici e della rete. Cominciano così ad occupare posizioni di rilievo nella società, e per il loro status ad essere oggetto d'invidia.

>> Potere geek

In una società tecnologicamente evoluta, il geek, che ha competenze e abilità, non può che divenire indispensabile e persino potente. Mantiene e allarga continuamente i confini di Internet e del World Wide Web, gestisce i sistemi che controllano il mondo, è artefice





della nuova economia globale. **Si pensi a Bill Gates!!!** Come ci racconta **John Katz in Geeks**, un libro che parla appunto del consolidamento sociale della nuova classe dei geek, la domanda di lavoro è così forte che molti frequentano e abbandonano l'università. Hanno conoscenze e sanno fare cose che la maggior parte delle persone ignorano e non sono in grado di fare e questo li rende arroganti. Per il loro potere contrattuale si permettono il lusso di non dover crescere, diventare responsabili e adulti. Non hanno l'obbligo, una volta entrati nel mondo del lavoro, di "normalizzarsi", di conformarsi come devono fare gli "altri", i cosiddetti normali, i perdenti, quelli che si divertono a incasinare i sistemi che loro hanno creato. I geek, oramai, non sono più giovani asociali e disadattati. Sono per lo più descritti come **"i talenti della new-economy, internet maniaci che vivono per il lavoro"**. Dal loro senso un po' esclusivo di appartenenza è nata una comunità virtuale, formata da giovani, appassionati di tecnologia e computer, che comunicano tra di loro, via mail, IRC, chat o giochi multiplayer, hanno dei propri usi e costumi, una mitologia e persino un codice linguistico con il quale si identificano: il **Geek Code**. Ormai tutti vogliono essere chiamati geek, tutti parlano dei geek. **Geek appare nelle pubblicità, sulle t-shirt, sui cappelli e persino nei programmi televisivi.**

>> Non sono hacker

L'hacker **non sempre è un esperto di computer**. E' soprattutto un entusiasta, un dilettante appassionato, un

crank, "una persona eccentrica dai tratti un po' maniacali". Gli uomini di scienza e gli appassionati di tecnologia sono sempre stati un po' crank. Con questo termine, ad esempio, già alla fine dell'800, Federico Di Trocchio, indicava tra gli scienziati statunitensi: "ogni personaggio strano e incoerente che si mostri incline a seguire idee eccentriche e progetti impraticabili o che appaia entusiasticamente



posseduto da una particolare mania o hobby (Rattus Norvegicus). Anche il geek è crank e forse ciò che ha in comune con l'hacker è proprio questa eccessiva, quasi maniacale, passione per le cose che fa. Il geek però non è un hacker. **Al livello più elevato della "gerarchia" hacker, come si è visto, vi è infatti il wizard, il vero mago.** Non tutti gli hacker, inoltre, vivono una fase geek (Raymond). I geek non sono hacker soprattutto perchè non hanno atteggiamenti e ideologia da hacker. I geek sono più interessati alle applicazioni e al futuro delle tecnologie che non alla parte puramente meccanica o ideologica. Gli hacker considerano la rete e i computer strumenti con cui realizzare un diritto: **il libero accesso all'informazione**. Come gli hacker, i geek diffidano delle istituzioni, ma solo perchè queste ultime non sono dalla loro parte. Si interessano anche al free

BIBLIOGRAFIA E SITOGRAFIA

- Rattus Norvegicus: "Del crank e del geek"
<http://www.mail-archive.com/laser@inventati.org/msg00324.html>
- Eric S. Raymond: How To Become A Hacker
<http://www.catb.org/~esr/faqs/hacker-howto.html>
- Eric S. Raymond: Come Diventare Un Hacker
<http://www.saprionline.com/gratis/informatica/hacker-howto-it.html>
- Federica Guerrini: Gli hackers come contro cultura tra identità e rappresentazione
<http://space.tin.it/spettacolo/fguerrin/frmain02.htm>
- Levy Steven: Hackers. Gli eroi della rivoluzione informatica, Shake
<http://www.shake.it/hackers.html>
http://www.unilibro.it/find_buy/result_editori.asp?editore=Shake&idaff=0
<http://www.csmtbo.mi.cnr.it/decoder/shake/catalogo/cybpnk/4levy.htm>
- Steven Levy Home Page
<http://mosaic.echonyc.com/~steven/index.html>
- Jon Katz: Geeks, Fazi
 Primo capitolo on line:
<http://www.fazieditore.it/pdf/88-8112-184-0.pdf>
- Di Robert A. Hayden: Il Codice dei Geeks v3.12
http://fc.retecivica.milano.it/~roberto.waha/geek_ita.html
- Riccardo Staglianò: Il mondo di gloria degli intraducibili "geek"
 La Repubblica
http://www.repubblica.it/online/tecnologie_internet/geek/geek/geek.html
- La rivincita dei Geek
 Mediamente
<http://www.mediamente.rai.it/rasstampa/010725.asp>
- Anna Masera: Umano, tecno umano
 Viaggio nella "cultura geek": cosa leggono, quali film vedono, che musica ascoltano. I protagonisti della rivoluzione digitale
 La Stampa
http://www.lastampa.it/redazione/news_high_tech/archivio/0307/nggeek.asp
- Vanessa Banfi: Codice Geek: apocalittici e integrati
 MyTech
<http://www.mytech.it/mytech/internet/art006010041637.jsp>
- Pekka Himanen - Etica Hacker e lo spirito dell'età dell'informazione, Feltrinelli
<http://www.hackerethic.org/>
http://www.feltrinelli.it/IntervistaInterna?id_int=53

software, ma per gli hacker è un "dovere etico condividere le loro competenze scrivendo free software e facilitare l'accesso alle informazioni e alle risorse di calcolo ogniqualvolta sia possibile". I geek mangiano le cimici dei computer per guadagnarsi da vivere. "L'hacker, invece, è una persona che è andata al di là dell'uso del computer per sopravvivere ("Mi porto a casa la pagnotta programmando")...", motiva la propria attività con gli obiettivi del valore sociale e dell'apertura (Pekka Himanem, Etica Hacker). ☑

DaMe`
www.dvara.net/HK

PER APPROFONDIMENTI

Nella sezione Contenuti Extra della Secret Zone del nostro sito troverete decine di link su questo argomento. Le immagini sono tratte da siti che vendono gadget o pubblicano fumetti per geek, come:

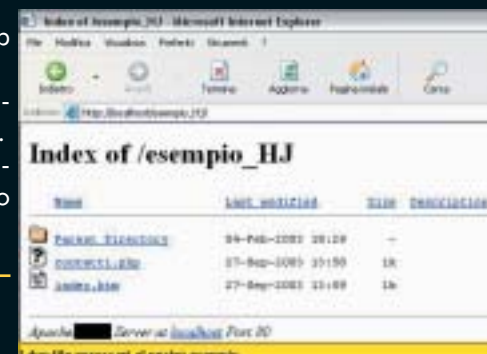
www.thinkgeek.com
www.cashncarrion.co.uk
<http://ars.userfriendly.org>
www.clarence.com/city/tobestrip/



NIENTE SPAM SUL WEB

Ovvero, come camuffare gli indirizzi mailto su una pagina Web senza usare JavaScript, ma con un pizzico di scripting sul lato server.

Come abbiamo visto sul numero 34 di HJ, gli indirizzi e-mail presenti sulle pagine Web **possono essere facile preda per gli spammer senza scrupoli**. Non è difficile creare script in grado di setacciare la rete e "catturare" tutti gli indirizzi e-mail nei tag del tipo: ``. Senza dover ricorrere a script in Javascript che rallenterebbero la velocità di navigazione, per non dire il loro supporto richiesto da parte del client interessato, questo metodo sfrutterà la tecnologia server-side (ormai ampiamente presente anche su spazi gratuiti).



>> Il lato server

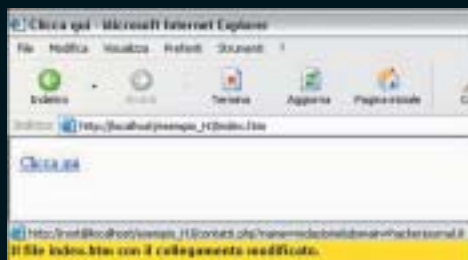
Gli esempi trattati funzioneranno indipendentemente se si usi come server **IIS o Apache**, in quanto verranno trattati come linguaggi rispettivamente l'ASP e il PHP.

Prendete in considerazione questo tag html:

```
<a href="contatti.asp?name=redazione&domain=hackerjournal.it"></a> (ASP)
<a href="contatti.php?name=redazione&domain=hackerjournal.it"></a> (PHP)
```

Hanno poco in comune con quello precedente, ma con il codice giusto nel posto giusto, otterremo lo stesso risultato. Prendiamo in esame la pagina contatti.asp (contatti.php): ha dei valori che potremo modificare a piacimento. Si può benissimo notare l'assenza della chiocciola (@), perché verrà implementata successivamente. **Otterremo così un indirizzo e-mail più "camuffato"**.

Ecco il codice da inserire in contatti.asp:



```
<%
    nome = request("name")
    dominio = request("domain")
If nome <> "" And dominio <> "" Then
Response.redirect("mailto:" & nome & "@" & dominio & ".")
End if
%>
```

Il codice presentato non fa altro che prendere il testo presente nel collegamento e metterlo nel posto giusto. Questo provcherà sul client l'apertura del programma di posta elettronica predefinito, pronto per inviare l'email a **redazione@hackerjournal.it**, senza necessariamente mostrare sul Web l'indirizzo e-mail nel formato tradizionale. Ecco anche il codice in versione PHP:

```
<?
    echo("<a href =mailto:.".$name."@".$domain.">Clicca per inviare un-email a
<b>".$name."</b></a>");
?>
```

Funziona in modo differente: direziona l'utente nella pagina contatti.php e da qui gli permette di selezionare l'e-mail, ottenendo comunque lo stesso risultato dell'altro script.

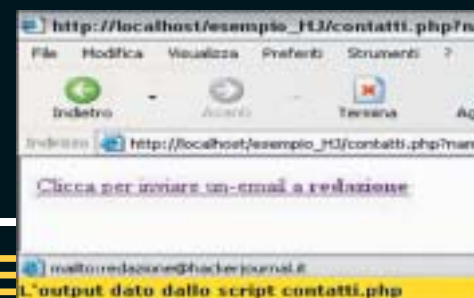
>> Possibili miglioramenti

Vedrete che sarà facile da implementare in un sito web che metterà al sicuro le vostre e-mail. Per rendere il tutto più dinamico potreste creare una connessione a una base dati e aprire il programma di posta in base all'utente, con un collegamento del tipo:

```
<a href="contatti.asp?utente=redazione"></a>
```

Ma questo lo lascio a voi, per fare esperienza e pratica. ☒

Bruseghin "SoNiK@" Michele - sonik.sniper@libero.it - www.snipernorth.too.it



Ultime notizie dal Pianeta AMIGA

Le uniche alternative a Win sono Linux e Mac? Date un po' un occhio a questo sistema operativo "non solo per nostalgici".

D

el numero 27 di HJ è stata narrata la storia di un computer glorioso e innovativo, l'Amiga, e delle peripezie e tribolazioni del sistema e dei suoi utenti dal fallimento della casa produttrice, la Commodore, sino ai nostri giorni.

Gli ultimi mesi hanno portato però qualche certezza in più nel presente degli Amighisti veraci. Anzitutto c'è la **disponibilità concreta e reale di soluzioni hardware ufficiali** (e non), e a questa si aggiungono segnali promettenti sul versante del sistema operativo dove però impera ancora pa-



recchia disomogeneità e incertezza.

Una buona occasione per tastare con mano il rinnovato clima di ottimismo è stata offerta dalla manifestazione italiana **Pianeta Amiga 2003** (www.pianetaamiga.it), svoltasi ad Empoli (Fi) e che è giunta ormai alla settima edizione. Rispetto all'anno scorso erano ora esposte ed acquistabili entrambe le offerte hardware disponibili: **Pegasos** della francese **Genesi** e **AmigaOne** della **Eyeteck**. Seppure si differenziano su molti aspetti, tra cui il supporto software ed i prezzi, le due ditte concorrenti offrono entrambe macchine nuove e tecnologicamente valide, accomunate dall'usare **processori RISC PowerPC G3 e G4 mono e multiprocessore**, scelta che per gli utenti ha il non indifferente valore aggiuntivo della coerenza con il passato di Amiga.

>> Pegasos

Il primato, perlomeno a livello cronologico, spetta alla piattaforma Pegasos della francese Genesi (<http://www.pegasosppc.com/>). Dietro al progetto ci sono **personaggi da sempre impegnati attivamente** nello sviluppo per Amiga: tre anni fa, dopo aver iniziato la realizzazione di un sistema operativo clone di AmigaOS, il **MorphOS** (www.morphos.net) la Genesi, in un momento ancora incerto per il settore Amiga, optò per la creazione di un 'Amiga del futuro'.

Il Pegasos è disponibile sotto forma di una **scheda madre di tipo MicroATX** (236 mm x 172 mm) che l'utente può montare in un case, aggiungendo alimentatore e componenti PC standard. Le caratteristiche sono: processore PowerPC G3 750 CXe a 600 MHz, (sostituibile con fino a un massimo di due processori G4), due slot di ram PC133 (fino ad un massimo di 2 Gb), uno slot AGP e tre PCI, USB 1.1, Firewire 400, scheda ethernet RealTek, scheda audio AC97 con connettori digi-



tali SPDIF, due canali ATA-100, attacchi per mouse e tastiera PS/2, infrarosso e numerose porte tra cui seriale e parallela. La prima comparsa del Pegasos in Italia è del settembre del 2002: attualmente il prezzo da listino (www.virtualworks.it) è di **649 Euro** ma per la fine del 2003 si prevede la disponibilità di macchine della seconda generazione. A livello di sistema operativo, il Pegasos **non è compatibile con l'AmigaOS**, ma la scheda è venduta dalla Genesi con due sistemi operativi: Linux e il già citato **MorphOS**, che fornisce vari livelli di compatibilità ed emulazione con i programmi Amiga. In generale uno dei punti di forza del Pegasos è proprio quello di puntare sul supporto di una vasta scelta di sistemi operativi: oltre a quelli nominati si parla dei GNU/Linux di SuSE, Gentoo e Yellow Dog oltre a FreeBSD, OpenBSD, AROS, FreeBSD, NewOS, e addirittura OpenBeOS.

>> AmigaOne

Assolutamente compatibile con l'AmigaOS e anzi, **macchina di riferimento per la nuova versione del sistema operativo** è invece la proposta della inglese Eyeteck, che si chiama AmigaOne (<http://www.eyeteck.co.uk/amigaone/>). Anche qui si tratta non di un intero computer ma di una motherboard. L'AmigaOne è disponibile in **quattro configurazioni**, due con il processore G3 a 600 e 800 MHz e due con il G4 a 800 e 933 MHz. Le altre caratteristiche parlano di formato ATX per la scheda, fino a 2 Gb di memoria SDRAM PC133MHz, uno slot AGP e 4 slot PCI, controller UDMA100 (2 canali, 4 dispositivi), USB (2 connettori su scheda madre, 2 tramite header), controller ethernet 10/100 3Com, scheda sonora, infrarosso e ovviamente connettori assortiti per seriale, parallela, floppy disk,



mouse e tastiera in formato PS/2. I prezzi presso la Soft3 (www.soft3.net) di Bologna vanno da 684 a 890 EUR. Tutte le versioni tranne quella base con il G3 a 600 MHz (detta AmigaOne G3 SE) hanno la CPU su slot ed è possibile eseguire l'upgrade a modelli G3 oppure G4 superiori quando questi saranno disponibili.

Come sistema operativo **l'AmigaOne supporterà AmigaOS 4**. Usiamo il futuro perché la nuova versione dell'OS **non è ancora pronta** (vedi sotto): nel frattempo le schede sono fornite con lo GNU/Linux Debian 3.0 per PowerPC, fornito dell'emulatore AUE (Amiga Unix Emulator) e AmigaOS 3.9 oppure, a richiesta, con la distribuzione Yellow Dog PPC 2.3.

>> "ready when it's done"

Una delle transizioni più traumatiche e lunghe verso il futuro di Amiga è quella che vede il sistema operativo fare il salto verso le macchine non più dotate di processori 68X00 ma PPC. Questo vuol dire i nuovi sistemi AmigaOne con G3 e G4 ma anche le numerose macchine che montano schede acceleratrici con PPC60X, che **verranno purtroppo**



supportate solo parzialmente.

Lo sviluppo della versione 4.0 dell'OS è affidato alla **Hyperion Entertainment** (www.hyperion-entertainment.com) ditta belgo-tedesca, che si avvale della collaborazione di vari sviluppatori in

tutto il mondo (anche in Italia). Il lavoro sulla nuova versione, inizialmente solo un passaggio dalla 3.9 alla 4.0 e poi diventata una riscrittura con aggiunta di molte novità, **è tuttora in corso**. L'attesa per AmigaOS 4, come l'impazienza degli utenti, è molta, tant'è che la risposta standard alle domande su date di rilascio è "it will be ready when it's done" (**sarà pronto quando è finito**).

In realtà la data si avvicina e dovrebbe coincidere con il 2004, come confermano i notevoli progressi fatti di recente. Oltre al funzionamento su macchine con schede acceleratrici, proprio a Pianeta Amiga di quest'anno è stato mostrato in anteprima mondiale il funzionamento sulla piattaforma AmigaOne, con un notevole eco in rete e non. Meno ottimisticamente, i detentori del marchio sono alle prese con **problemi finanziari e beghe legali con la Genesi**, che rivendica accordi fatti in passato.

C'è inoltre chi critica il prezzo alto delle proposte hardware, evidenziando come i nuovi Amiga siano macchine dallo spirito e dal pubblico molto diverso da quelli che animarono e infiammarono la seconda metà degli anni '80. Altri ancora, con tono melodrammatico, dicono che **Amiga è morta anni fa**, di una fine peggiore dei vari NeXT o BeOS e che si dovrebbe passare oltre. C'è probabilmente un fondo di verità in alcune di queste critiche, ma è innegabile anche che, dopo anni di buio, sono disponibili sul mercato nuove e concrete evoluzioni hardware Amiga (e prossimamente anche software) di ampio respiro e non più palliativi o prodotti di ripiego. Questo non solo premia la lunga e difficile "resistenza" degli Amighisti ma offre **interessanti sviluppi verso altri sistemi operativi** o, grazie ai processori G3 e G4, esperimenti come l'emulazione a velocità fattibili dei "cugini" Apple. ☑

Nicola D'Agostino
dagostino@nezmar.com

Si ringrazia per la collaborazione Massimiliano Tretene della Soft3, Jares Cappelli, Claudio Marro Filosa e Joachim Thomas.

SMONTARE UN PROGRAMMA

Passiamo dalla teoria alla pratica e proviamo a

F

are e non dire di fare! Questa è l'esortazione che usa il mio Maestro di Judo quando noi allievi battiamo un po' la fiacca. Ora io la rigiro a me stesso e a voi lettori. Dopo la generica ma utilissima chiacchierata sul reversing del numero 32, è arrivato il momento di rimboccarci le maniche e di vedere, in pratica, **come ci si debba comportare davanti ad un eseguibile da analizzare e modificare.**

>> Il programma da studiare

Visto che per molti di voi è il primo esempio in assoluto, ho voluto creare

un programma molto semplice da capire e da modificare. Se date un'occhiata ai sorgenti, vedrete che viene eseguito un confronto sulla variabile "risolto": se vale 'S' viene visualizzata una finestrella di congratulazioni, altrimenti appare un'altra finestrella che ci dice che dobbiamo modificare l'eseguibile per risolvere il giochino.

Per chi capisce almeno un filino il linguaggio C, è evidente che non c'è modo di ottenere le congratulazioni, dal momento che il valore iniziale della variabile "risolto" è 'N' e non viene mai modificato durante l'esecuzione. Siccome i compilatori C possono inserire codice in più di quello strettamente necessario all'esecuzione del programma, ho **riscritto il tutto direttamente in assembly** e l'ho ottimizzato post compilazione per ottenere la maggiore chiarezza e semplicità possibile. Trovate il programmino già pronto per il reversing nella "Secret Zone" del sito. È ovvio che in genere non abbiamo a disposizione il codice sorgente di ciò che dobbiamo reversare, né l'eseguibile viene ottimizzato per facilitare il lavoro agli smanettoni, ma noi siamo qui per imparare!!!

>> Debugging con SoftICE

Il programma più potente e più divertente da usare per fare reversing è sicuramente **SoftICE** e quindi inizieremo proprio da lui. Vogliamo intercettare la

```

00401000 EB7-0063FF70 ESP=0063FF3C EIP=00401034 o 4 1 5 z + 7 c
05-0167 35-016F 35-016F ES=0167 FS=2F7F GS=0000
PROT32
0167:00481000 90 NOP
0167:00481001 833D0030400053 CMP DWORD PTR [00480000],53
0167:00481008 7516 JNZ 00481028
0167:0048100A 6A48 PUSH 48
0167:0048100C 6804304000 PUSH 00483004
0167:00481011 6810304000 PUSH 00483018
0167:00481016 6A00 PUSH 00
0167:00481018 FF1588204000 CALL [USEK32!MessageBoxA]
0167:0048101E EB14 JMP 00481034
0167:00481020 6A30 PUSH 30
0167:00481022 6833304000 PUSH 00483033
0167:00481027 6840304000 PUSH 00483048
0167:0048102C 6A00 PUSH 00
0167:0048102E FF1588204000 CALL [USEK32!MessageBoxA]
0167:00481034 6A00 PUSH 00
0167:00481036 FF1500204000 CALL [KERNEL32!ExitProcess]
GIOCHINO1.txt
4 483008 L 1
0030:00483008 4E 00 00 00 43 6F 6E 67-72 61 74 75 6C 61 78 69 M...Congratulazi
4 483004 L 8
0030:00483004 43 6F 6E 67 72 61 74 75-6C 61 78 69 6F 6E 69 21 Congratulazioni!
4 483018 L 16
0030:00483018 48 61 69 20 72 69 73 6F-6C 74 6F 28 69 6C 20 67 Hai risolto il g
0030:00483028 69 6F 63 68 69 6E 6F 21-00 00 00 47 69 6F 63 68 iachiso!...Gioch
4 483033 L 8
0030:00483033 47 69 6F 63 68 69 6E 6F-2E 2E 89 88 88 48 6F 64 Giochino....Mod
4 483048 L 32
0030:00483048 4D 6F 64 69 66 69 63 61-20 6C 27 65 73 65 67 75 Modifica l'esegu
0030:00483058 69 62 69 6C 65 28 78 65-72 63 68 EB 28 69 6F 73 ibile perch. mos
0030:00483068 74 72 69 28 69 6C 28 6D-65 73 73 61 67 67 69 6F tri il messaggio
0030:00483070 20 6E 61 73 63 6F 73 74-6F 21 00 00 00 00 00 00 nascoste!.....
\scrindump c:\passa\h\j2\aso.raw
Invalid command Giochin

```

chiamata alla funzione **MessageBoxA** e, per farlo, settiamo un **breakpoint** a tale funzione. Stò parlando arabo? Spero di no, comunque passando dalle parole ai fatti molti dubbi si risolvono da soli. Chiamiamo **SoftICE**



MMMA: ESEMPIO PRATICO

“reversare” e “crackare” un semplice programmino.

premendo **CTRL+D**. Appare una schermata nera in stile DOS con un po' di codice assembly nella parte centrale, e una specie di prompt nella parte inferiore. Digittiamo **“bpx messageboxa”** e premiamo **invio**. A questo punto, il breakpoint è settato. Cosa significa ciò? In pratica, quando un programma qualsiasi richiamerà la funzione MessageBoxA, entrerà in funzione il SoftICE **prendendo il controllo della situazione**. Chiudiamo la finestra del nostro debugger preferito premendo nuovamente CTRL+D e facciamo partire il nostro programma **“giochino_1.exe”**. Appare il SoftICE, che ci mostra il codice della funzione su cui abbiamo settato il breakpoint. A noi però **interessa il disassemblato del nostro programmino**, non quello di qualche strana funzione presente nelle librerie del nostro sistema operativo. Premiamo allora il tasto funzione **F12**, che manda avanti l'esecuzione fino al termine della funzione in cui ci troviamo. Appare la solita finestrella **“Giochino...”**. Clicchiamo su **OK** e finalmente ci troviamo nella parte di codice che a noi interessa. Il nostro programma inizia alla riga **401000**. Alla prima riga c'è un **“NOP”**, che significa **“no operation”** e in pratica non serve a nulla, l'ho aggiunta io con degli scopi ben precisi che vedremo meglio nel prosieguo dell'articolo. Alla riga successiva c'è il confronto tra la variabile contenuta all'indirizzo **403000** (quella che nel programmino in C si chiama **“risolto”**) ed il valore **53** (in esadecimale). Se avete una tabella ASCII a disposizione, noterete che a **53h** corrisponde il carattere **‘S’**. L'istruzione **CMP** corrisponde pressappoco

alla nostra **“if”** in C. Se i due caratteri confrontati sono uguali viene settata la flag **“Z”** della cpu, altrimenti no. Alla riga successiva (**401008**) c'è un salto condizionato. Se la flag **“Z”** non è settata, e cioè se **“risolto”** è diverso da **‘S’**, allora l'esecuzione passa alla riga **401020**, altrimenti continua alla riga successiva.

Di seguito c'è la parte di codice necessaria a chiamare le due messagebox. È da notare che i parametri vengono passati in ordine inverso (mi riferisco alle istruzioni **PUSH**). Quindi il primo dei quattro push che precedono ognuna delle due **CALL** è lo **“stile”** della finestra, il secondo è l'indirizzo di memoria in cui è contenuta la stringa che verrà visualizzata come titolo, il terzo è l'indirizzo della stringa che verrà mostrata all'interno della finestrella ed il quarto è uno zero, il **“NULL”** del listato in C. Usando il comando **‘d’** (come dump) di SoftICE possiamo visualizzare il contenuto di queste stringhe, come mostrato in figura. Alla fine viene chiamata la funzione ExitProcess dopo averle passato come parametro uno zero. Serve ad uscire correttamente dal programma. Prima di chiudere il SoftICE con **CTRL+D**, ricordiamoci di cancellare tutti i breakpoint con il comando **“bc *”**.

>> Editing con Hiew

Hiew è un potente editor esadecimale, che è molto utile nel caso si voglia modificare un programma per windows. Diamogli in pasto il programmino **giochino_1.exe**, premiamo un paio di volte **invio** per visualizzare il sorgente assembly e andiamo in giù fino alla riga **“00401000”** che corrisponde all'inizio del programma. Per prima cosa notiamo che il listato in assembly è leggermente diverso nella notazione rispetto a quello mostrato da **SoftICE**, anche se le istruzioni, ovviamente, sono le stesse. Per far sì che appaia la finestrella di congratulazioni al posto dell'altra possiamo agire in vari modi. Possiamo, ad esempio, cancellare l'istruzione di salto condizionato (lunga due bytes) con due istruzioni inutili **“NOP”** (lunghe un byte ognuna). Per far ciò posizioniamoci sulla riga da modificare e premiamo **F3** per passare in modalità di editing e **F2** per l'editing in assembly. Cancelliamo l'istruzione che ci viene mostrata e scriviamo **“nop”** al suo posto. Premiamo **invio** e ci verrà mostrata l'istruzione successiva, cancelliamo anche questa e scriviamo **“nop”** seguito da **invio**. Fatto ciò usciamo dalla moda-

```

00004000  EC          INT3
00004001  83380030400053  CMP     EAX,EBX
00004008  7516        JNE     000000420
0000400A  6A40        PUSH   040
0000400C  6804304000  PUSH   000403004 ; "04"
00004011  6818304000  PUSH   000403018 ; "01"
00004016  6A00        PUSH   000
00004018  FF1508204000  CALL   000402000
0000401E  EB14        JMP    000000434
00004034  6A00        PUSH   000
00004036  FF1508204000  CALL   000402000

```

Pentium(R) Pro Assembler
jne 000000420

```

00004034  6A00        PUSH   000
00004036  FF1508204000  CALL   000402000

```



lità di editing premendo **ESC** e salviamo le modifiche sul file premendo **F9**. Usciamo da Hiew con **F10** e mandiamo in esecuzione il nostro programma. Se non abbiamo commesso errori, dovrebbe apparire la finestrella "Hai risolto il giochino!".

Possiamo agire in modo diverso? Certamente! Possiamo, ad esempio, editare la riga del confronto anziché quella del salto condizionato e sostituire il **53** (cioè 'S') con **4E** (cioè 'N') che è il valore della variabile "risolto". Possiamo fare anche il viceversa, ossia spostarci nell'area dati del programma e sostituire il carattere 'N' con 'S'. Sappiamo infatti che tale valore è memorizzato all'indirizzo **403000**, quindi basterà premere qualche volta il tasto **Page-Down** e lo troveremo subito. Ovviamente in questo caso non servirà passare alla modalità di editing in assembly ma sarà sufficiente la modalità esadecimale. Non ripeto il procedimento passo passo per questi ultimi due casi visto che cambia pochissimo, ma vi esorto a farlo per esercizio, sempre che aspiriate a diventare dei reverser...

>> Il trucco dell'interrupt 3

Commentando il codice assembly mostrato da SoftICE avevo lasciato in sospeso il motivo per cui avevo inserito un'istruzione "NOP" all'inizio del programma. Come abbiamo potuto constatare in precedenza, mettendo un **breakpoint** sulla funzione **MessageBoxA** siamo in grado di accedere al disassemblato del nostro programma solo dopo che tale funzione è già stata chiamata. A volte però, può essere utile, se non indispensabile, entrare in un punto ben preciso del programma. In questo caso supponiamo che si voglia accedere all'inizio del programma per seguirne l'esecuzione passo passo. Uno dei metodi più sbrigativi per fare ciò è quello di sostituire un'istruzione del programma (in questo caso il "NOP" iniziale) con una chiamata all'interrupt 3, di facile intercettazione all'interno di **SoftICE**. Siccome abbiamo appena vi-

```

EAX=00401000  EBX=00530000  ECX=01910020  EDI=01910000  ESI=01910000
EDI=00000000  EBP=0063FF7B  ESP=0063FE3C  EIP=00401008  a d 1 5 2 a p c
CS=0167  DS=016F  SS=016F  ES=016F  FS=0FD7  GS=0000

GIOCHINO1: test
0030:00401000 50 03 3D 00 30 40 00 53-75 16 6A 40 60 04 30 40  ..-09.5a.jp5.DPA
0030:00401010 90 60 18 30 40 00 6A 00-FF 15 00 20 40 00 EB 14  h.00.j....p...
0030:00401020 6A 30 60 33 30 40 00 60-40 30 40 00 6A 00 FF 15  10h300.h000.j...
0030:00401030 08 20 40 00 6A 00 FF 15-00 20 40 00 00 00 00 00  ..j....0....

0167:00400FFE FFFF                INVALID
0167:00401000 50                NOP
0167:00401001 033D0030400053    CMP     DWORD PTR [00403000],53
0167:00401002 7516              JNZ     00401020 (NO_JUMP)
0167:00401003 6A40              PUSH   40
0167:00401004 6A043004          PUSH   00403004
0167:00401005 6A183018          PUSH   00403018
0167:00401006 6A00              PUSH   00
0167:00401007 FF1500204000     CALL   USER32!MessageBoxA
0167:00401008 EB14              JMP     00401034
-> 00401020 6A30              PUSH   30
0167:00401022 6A33304000       PUSH   00403033
0167:00401023 6A403040          PUSH   00403040
0167:00401024 6A00              PUSH   00
0167:00401025 FF1500204000     CALL   USER32!MessageBoxA
0167:00401026 6A00              PUSH   00

GIOCHINO1+0FFE
FINICE: Load32  0hJ-0002  Add-016F:BFE0C000 Len=00001000 Mod=ADVAPI32
FINICE: Load32  0hJ-0003  Add-016F:BFE0D000 Len=00001000 Mod=ADVAPI32
FINICE: Load32  0hJ-0004  Add-016F:BFE0E000 Len=00001000 Mod=ADVAPI32
FINICE: Load32  0hJ-0005  Add-016F:BFE0F000 Len=00001000 Mod=ADVAPI32
Break due to BPINT 03 (ET=1.68 seconds)
eb 401000 90
/screendump c:\spasmsh\N2ndue.raw

```

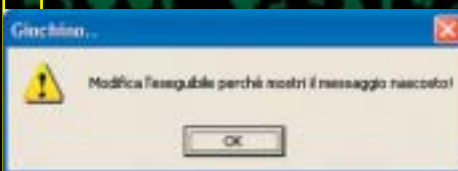
sto insieme il metodo con cui si può modificare un programma utilizzando l'editor Hiew, non ci dovrebbero essere problemi ad effettuare questa modifica. Riprendiamo, quindi, il "giochino_1.exe" originale e sostituiamogli il "nop" con un "int 3". Se proviamo a far partire il programma dopo la modifica, otteniamo una segnalazione di errore da parte di Windows, che ci chiede di terminare il programma. Niente paura! Richiamiamo il SoftICE con **CTRL+D** e scriviamo "pbint 3", premiamo invio, chiudiamo la finestra con **CTRL+D** e facciamo ripartire il programma. Questa volta entreremo in SoftICE all'inizio del nostro "giochi-

D'ora in poi possiamo "steppare" un'istruzione alla volta con il tasto **F8**, e modificare il programma in fase di esecuzione. Premiamo **F8** fino a posizionarci sulla riga **401008**. Ci apparirà nella parte destra l'indicazione "JUMP" con una freccia verso il basso, ma per veder apparire il messaggio di congratulazioni sappiamo che non dobbiamo saltare. Posizioniamo allora il cursore in alto a destra sopra la "z" in minuscolo della finestra dei registri e premiamo "Ins". La "z" minuscola diventerà maiuscola e azzurra. Abbiamo cambiato una flag interna alla cpu. Clickiamo ora da qualche parte nella finestra centrale e vedremo che la scritta "JUMP" si è trasformata in "NO JUMP". Togliamo allora tutti i breakpoints con "bc *", premiamo invio e chiudiamo SoftICE con il consueto **CTRL+D**. Apparirà la finestrella di congratulazioni!

>> Conclusioni

Mi rendo conto che chi è nuovo a questo mondo possa aver trovato un po' di difficoltà, ma se invece di leggere questo articolo seduti sul divano, lo fate a fianco del computer acceso, vi divertirete un sacco a risolvere questo giochino (in un certo senso, a craccare un programma) in molti modi diversi. Per qualsiasi commento, la mia email è quella qui sotto! Ciao! ☺

fantoibed
fantoibed@libero.it



no_1". La prima cosa da fare è rimettere a posto il "NOP" precedente, quindi digitiamo "eb 401000 90" e premiamo invio. Il significato di questo comando è "edita e sostituisci il byte all'indirizzo 401000 con un 90" dove, per la cronaca, "90" in esadecimale è l'opcode dell'istruzione "NOP".

Come ti apro il file...

1 Il registro è **un enorme database** che contiene tutte le informazioni relative alla postazione di lavoro su cui vi trovate. Il registro di configurazione non dovrebbe essere utilizzato nel lavoro quotidiano perché **multi parametri possono essere modificati tramite le opzioni del pannello di controllo** o di files di sistema oppure attraverso componenti software di terze parti, ma agire direttamente sul registro è **più divertente**. Bene cominciamo!

>> Il programma necessario

Per aprire l'editor di registro si utilizza un programma apposito, chiamato **Regedit.exe**, un'applicazione che permette di visualizzare in forma gerarchica tutte le informazioni del sistema disposte in sezioni.

Premiamo il pulsante Start (o Avvio per chi possiede Win95/98), scegliamo **Esegui**, e nella casella scriviamo "**Regedit**" (senza virgolette) senza preoccuparci delle maiuscole/minuscole. Apparirà una finestra come quella riportata in figura 1.

Come potete notare, **assomiglia molto all'explorer di Windows** (il cosiddetto Gestione Risorse), organizzato in cartelle (**chiavi**, keys), **sotto chiavi** (subkeys) e **valori** (sul pannello di destra).

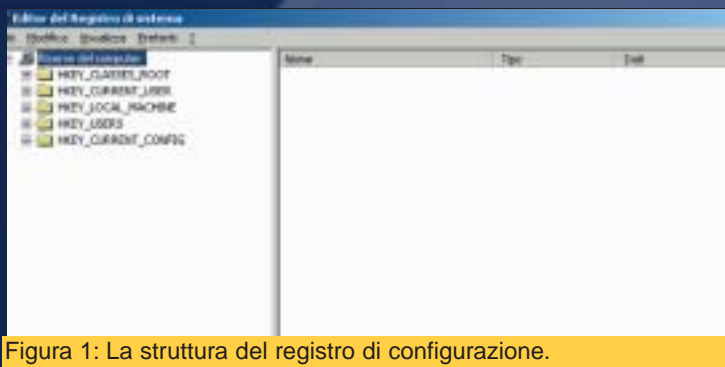


Figura 1: La struttura del registro di configurazione.

Se Windows è NT...

Esiste anche l'editor Regedt32.exe per le versioni NT di Microsoft (NT/2000/XP/2003), ma è sostanzialmente indifferente operare sull'uno o sull'altro usando tali piattaforme.

>> Le chiavi

Tutte le informazioni sono raccolte e organizzate nelle cosiddette "chiavi". Queste sono molto numerose e ognuna di esse contiene informazioni specifiche:

HKEY_CLASSES_ROOT: contiene informazioni sui tipi di files e sulle associazioni di queste.

HKEY_CURRENT_USER: contiene tutte le informazioni relative all'utente che sta utilizzando Windows (combinazione di suoni utilizzata, sfondo, impostazioni internazionali).

HKEY_LOCAL_MACHINE: contiene tutte le informazioni relative all'intera macchina, cioè le impostazioni valide per tutti gli utenti che accedono alla postazione.

HKEY_USERS: contiene informazioni relative a tutti gli utenti. E' una raccolta dei dati della chiave CURRENT_USER per tutti gli utenti.

HKEY_CURRENT_CONFIG e HKEY_DYN_DATA: contengono informazioni sulla configurazione del sistema e sui dati dinamici, informazioni su VXD's realtime per le applicazioni Win32.

I valori contenuti nelle chiavi possono essere di tre tipi:



String (Stringa): una serie di caratteri alfanumerici.



Binary (Binario): un valore binario.



DWord (Dword): un valore long (double word).

Esistono anche stringhe multivalore e stringhe espansibili, ma restano in ogni caso semplici stringhe.

>> Modifiche al registro

Passiamo ora a qualcosa di pratico. Cercheremo di assegnare ad un tipo di file l'apertura con un programma. Per esempio **faremo aprire i file *.log con il Blocco Note** di Windows.

ATTENZIONE: prima di effettuare una qualsiasi modifica è conveniente salvare il contenuto del registro. Per farlo è sufficiente selezionare dal menu file la voce **Esporta** e salvare tutto il contenuto e non la selezione.

Apriamo il registro (**Start-Esegui-Regedit**), facciamo doppio clic su **Hkey_Classes_Root**, rintracciamo la chiave ***.log** e, una volta selezionata, leggiamo nel valore (**predefinito**) che le sue informazioni sono contenute nella chiave **Log.File** (come mostrato in figura 2).



Figura 2. Le informazioni dei files con estensione log sono contenute nella chiave Log.File.

Ora scorriamo la barra laterale fino a trovare la suddetta chiave. Clicchiamoci su col pulsante destro e selezioniamo **Nuovo-Chiave** (vedi figura 3), dandole il nome di **"Shell"** (se non esiste). Ancora una volta, clic col destro su **Shell** e selezioniamo **Nuovo-Chiave**, e stavolta diamole il nome **"&Blocco Note"** (la **&** serve per creare uno shortcut da tastiera).

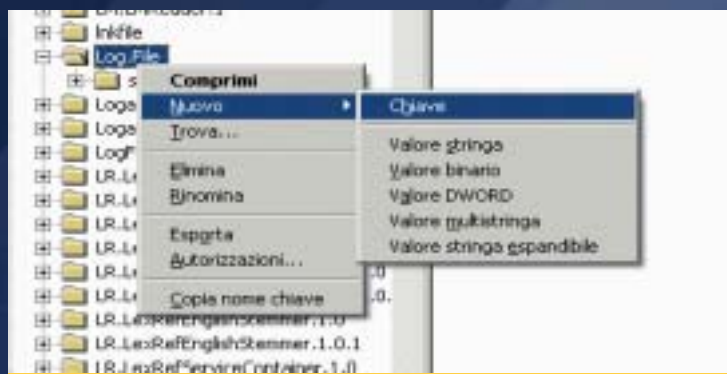


Figura 3. Con un tasto destro del mouse creiamo una nuova chiave.

Selezioniamo tale chiave e ancora col pulsante destro **Nuovo-Chiave**, questa volta col nome **Command**. Selezioniamo **Command** e facciamo doppio clic sul valore (**predefinito**) e scriviamo nella casella **"C:\WINDOWS\notepad.exe %1"** (figura 4), dove **C:** è il volume su cui è installato Windows e **Windows** è la cartella dei file di installazione, **Notepad.exe** è il file programma del Blocco Note (nell'esempio riportato il volume è **"E:"** e la cartella dei files è **WinNT**).

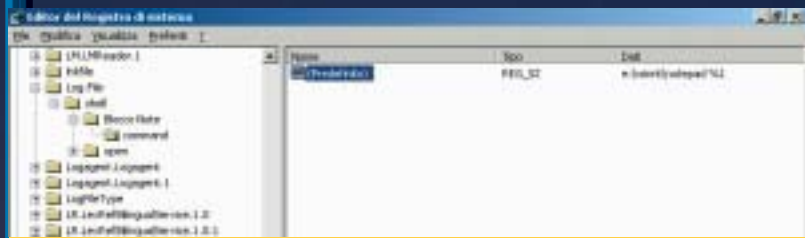


Figura 4. Nel valore (predefinito) inseriamo il comando che farà aprire il file col blocco note.

Ecco fatto! Cliccando ora col pulsante destro del mouse su un file con estensione **log** ci sarà una nuova voce **Blocco Note** (attivabile anche da tastiera con la lettera **b**, per effetto della **&**) che consentirà di aprire il file con il notepad di Windows (vedi figura 5). La procedura descritta può sembrare lunga e complicata: in realtà si tratta di una semplice tecnica che non toglierà a chiunque di voi, dai neofiti ai più esperti non più di due minuti.

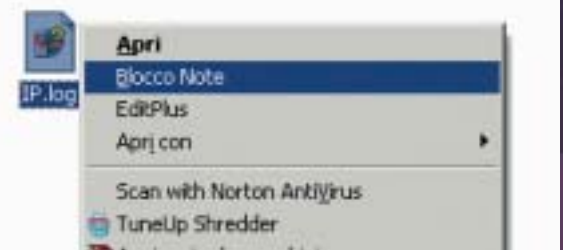


Figura 5. Il menu a tendina che compare cliccando col tasto destro su un file *.log.

>> Automatizzare la procedura

Figura 6. Un esempio di file di registro.

Per chi è alle prime armi, o per chi preferisce **non modificare il registro** direttamente, è possibile automatizzare il processo attraverso l'uso di **file di registro** che non sono altro che semplici files di testo che indicano quali modifiche effettuare. I files di registro hanno estensione ***.reg** e cominciano tutti con una frase specifica per indicare il loro tipo. Tali files per sistemi Win95/98 cominciano con la parola **Regedit4**, mentre quelli basati su WinXP iniziano con la frase **Windows Registry Editor Version 5.00**.

Vogliamo ora vedere come rendere il tutto automatico, cioè come creare un file **CreaMenu.reg** che esegua le operazioni descritte in precedenza. Creiamo innanzi tutto un **nuovo documento di testo**, facendo clic col pulsante destro del mouse sul desktop, scegliendo **Nuovo-Documento di testo** e assegniamogli il nome **CreaMenu.reg**. Ci verrà chiesto se vogliamo cambiare estensione al file, clicchiamo **Sì** e prepariamoci a scrivere il **codice** necessario.

Selezioniamo il file appena creato col pulsante destro del mouse e selezioniamo la voce **Modifica**. Si aprirà una finestra del Blocco Note in cui inseriamo il seguente testo (ricordiamo di effettuare un INVIO al termine della scrittura):

```
1 Windows Registry Editor Version 5.00
2 [HKEY_CLASSES_ROOT\Log.File\shell]
3 [HKEY_CLASSES_ROOT\Log.File\shell\Blocco Note]
4 [HKEY_CLASSES_ROOT\Log.File\shell\Blocco Note\command]
5 @="c:\\windows\\notepad.exe %1"
```



La seconda, la terza e la quarta riga non fanno altro che **creare la struttura ad albero necessaria**; la più importante è la **quinta riga** che inserisce la riga di comando da eseguire quando selezioniamo la voce **Blocco Note** dal menu di scelta rapida. Particolare è il modo di scrivere un path (un percorso di file); infatti, per suddividere le directory si utilizza un **doppio backslash** (\). Il **simbolo di percentuale** seguito dal numero uno indica che deve essere eseguito il comando per il primo file che verrà passato come parametro (nel nostro caso il file su cui abbiamo fatto clic sulla voce Blocco Note). Inoltre, come potete notare, i percorsi sono racchiusi tra **parentesi quadre** mentre i valori vengono scritti al di sotto dei rispettivi percorsi. La @ ("at") rappresenta il **valore predefinito**.

Coloro che non hanno tempo da perdere e vogliono mettersi subito all'opera, troveranno il file già pronto (**Menu.zip**) nella sezione **Contenuti Extra** su hackerjournal.it. All'interno troverete anche un file **RimuoviMenu.reg** che consente di eliminare le modifiche effettuate. Ecco il codice:

```
Windows Registry Editor Version 5.00
[-HKEY_CLASSES_ROOT\Log.File\shell\Blocco Note]
```

Il metodo per eliminare una chiave è semplicemente quello di **anteporre un segno meno prima del percorso**. Viceversa, per eliminare un valore basta postporre al segno di uguale il segno meno.

Una volta aperto l'archivio, è possibile estrarre i files su una cartella qualsiasi del disco e con un doppio clic sul file **CreaMenu.reg** potremo aggiornare il registro di sistema. Apparirà una finestra (vedi figura 7) che chiederà conferma della aggiunta delle nuove informazioni; basta cliccare su **Si**.

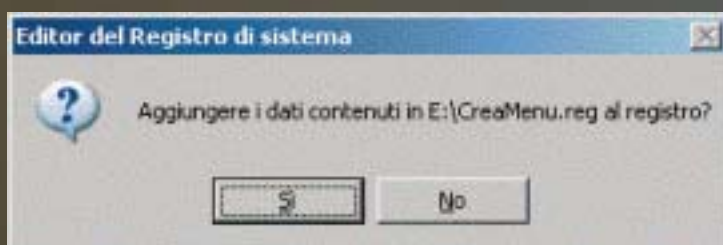


Figura 7. Con un doppio clic su un file di registro ci viene chiesto se aggiungere i nuovi dati.

Questo inserirà tutto il necessario sul registro e vi consentirà di aprire i files con estensione ***.log** con il blocco note di Windows. In maniera analoga è possibile associare ad ogni tipo di file un programma diverso cambiando semplicemente l'estensione da modificare.

È possibile, in questo modo, **modificare qualsiasi valore all'interno del registro purchè si sappia bene cosa fare**: ricordiamo sempre che il registro non è un file qualunque e se utilizzato in maniera scorretta può provocare anche **l'impossibilità di avvio del sistema**.

>> Conclusioni

In questo articolo ci siamo occupati di fornire una descrizione generale della struttura a chiavi del registro di configurazione dei sistemi Windows. Abbiamo imparato a muoverci nel registro e ad apportare modifiche quali creazioni di chiavi, sottochiavi e valori. Inoltre abbiamo appreso come modificare l'assegnazione dei programmi alle estensioni di files, come creare la struttura ad albero necessaria e come automatizzare il processo attraverso l'uso dei files di registro. ☑

Angelo Zarrillo
giozarrillo@inwind.it
www.cplusplus.it

Trucchi sparsi...

Aprire MS-DOS da ogni cartella

Funziona con: Windows 95, 98, Me, NT

Per aprire il prompt di MS-DOS con il prompt già posizionato in una cartella, lanciate Regedit, fate clic su HKEY_CLASSES_ROOT, poi su Directory e quindi su shell. Create una nuova chiave chiamata "command" e inserite come valore predefinito "Apri finestra DOS".

Poi create un'altra chiave all'interno di command e chiamatela ancora command. Impostate il valore predefinito su

```
cmd /k title Prompt dei comandi && cd %L
```

Velocizzare il menu Avvio

Funziona con: Windows 95, 98, Me, NT, 2000, XP

Andate alla chiave HKEY_CURRENT_USER/Control Panel/Desktop. Modificate il valore dell'attributo MenuShowDelay da 400 a 200 o 100 (il numero indica i millisecondi di ritardo).

Scaricare più di 4 file con Explorer

Aprirete Regedit e andate su HKEY_CURRENT_USER/Software/Microsoft Windows/CurrentVersion/Internet Settings, e aggiungete due nuovi valori DWORD a quelli già presenti, facendo clic con il tasto destro, e selezionando Nuovo/Valore DWORD dal menu a comparsa.

I nomi dei due nuovi attributi devono essere:

```
MaxConnectionsPerServer  
MaxConnectionsPer1_0Server
```

Con un doppio clic potete modificare il valore di questi parametri, inserendo il numero massimo di download contemporanei per Explorer.

INTERNET. ■ ■

QUATTRO MILIONI di amici AL BAR...

Come cominciare a frequentare i newsgroup, la piazza globale più popolata al mondo, senza complicazioni.

1 newsgroup sono un sistema pubblico di comunicazione virtuale nati nel lontano 1979 negli Stati Uniti, da lì in pochi anni si sono diffusi a macchia d'olio in tutto il mondo, così **molti paesi hanno creato dei sottogruppi di discussione nella propria lingua**, come l'Italia che conta addirittura tre gerarchie:

- **La free.it.*** che è basata sulla libertà d'espressione senza censure e sulla facilità nella creazione dei newsgroup;

- **La it.*** con la possibilità di creare un gruppo moderato;

- **La italia.*** basata sulle reti civiche.

Queste gerarchie hanno diffusione mondiale, ma ve ne sono altre locali, ovvero presenti solo sul newserver madre (è il caso di tin.*, libero.*, eccetera) e vengono chiamate **gerarchie proprietarie**.

>> Una piazza enorme

Ma quanti newsgroup esistono? Questa è una domanda che viene spesso posta e che è la cosiddetta domanda da un milione di dollari. Usenet, infatti, si è talmente espansa in poco tempo e in

tutto il mondo che **non è più possibile fare questi calcoli**, si parla di **100.000 newsgroup**, ma io azzarderei dicendo che ne esistono **140-150.000**, pensando anche ai **50 Gb** che girano giornalmente su usenet, non è un errore di battitura, sono proprio cinquanta gigabyte!!!

Se vogliamo semplificare la cosa, possiamo paragonarli alle bacheche scolastiche degli anni '60 dove ognuno attaccava un pezzetto di carta con su scritto "Vendo libro di latino", "Si cerca chitarrista", un messaggio politico, un messaggio d'amore, la caricatura di un professore eccetera.

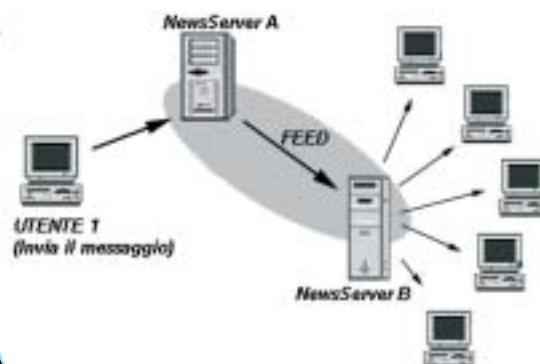
Può sembrare un paragone stupido, ma in fondo è così, si invia il post (che nel gergo di usenet sarebbe il messaggio) con la richiesta, l'appunto, l'opinione, il consiglio o quello che volete al newsgroup e **rimane lì dove tutti possono visionarlo**, leggerlo e rispondergli, facendo nascere così delle vere e proprie discussioni. Nonostante usenet sia "nato" prima di internet, viene tutt'oggi considerato un'applicazione di internet come le e-mail, le cha... ma **Usenet non è internet** e questa è una cosa fondamentale da capire, anche perché usenet ha delle peculiari-

tà in più rispetto a un forum o una mailing list. I newsgroup infatti sono adatti **sia a un grande che a un piccolo numero** di utenti, si possono **scaricare solo i messaggi di proprio interesse** leggendoli e **rispondendo offline** e si possono seguire facilmente le discussioni grazie alla disposizione ad albero dei thread.

>> Il funzionamento interno

Ora diamo qualche nozione tecnica per poi passare alla pratica.

Il protocollo alla base di questa rete logica è **l'NNTP** (per approfondimenti vi rimando alla **RCF 977**) che si basa sul-



Galateo informatico

Anche nei newsgroup, come nella vita reale esistono delle regole necessarie per vivere in armonia nella società, queste norme in rete vengono chiamate netiquette e sono fondamentali per restare in armonia con i partecipanti del newsgroup. Le più elementari sono quelle di leggere per una settimana il newsgroup prima di postarci e di controllare nei vecchi messaggi che un argomento non sia stato già trattato, evitando così di riproporlo, leggere il manifesto del gruppo dove sono contenute le regole e le indicazioni più importanti, discutere in modo civile e soprattutto usare il buon senso, che è la regola più importante.

lo scambio di informazioni che vengono inviate e ricevute dagli utenti.

Dallo schema riportato qui sopra possiamo capire un po' il suo funzionamento, in pratica l'utente 1 si collega al newsserver A (che non è altro che un computer dove gira il demone **NNTP** che è incaricato di gestire il traffico dei newsgroup) e **invia il suo messaggio**; il newsserver lo inserisce nel newsgroup e lo **"spedisce" agli altri newsserver** (questo scambio di messaggi si chiama feed) che non fanno la medesima cosa. Gli utenti del newsserver B si collegano ad esso dove possono leggere e rispondere al messaggio inviato dall'utente A.

Ora sorge spontanea una domanda: "on questo meccanismo un newsserver non potrebbe ricevere più copie dello stesso messaggio, oppure un messaggio potrebbe girare all'infinito"?

La risposta è semplicemente **NO**, infatti il protocollo NNTP ha previsto anche questo e **assegna a ogni messaggio inviato una specie di codice, il message-id**, che non è altro che una stringa alfanumerica tipo **biftdf\$fl5S2@lacerta.tiscalinet.it** che identifica il messaggio.

Nell'atto del feed i due newsserver si inviano i message-id dei messaggi, il newsserver verifica quali messaggi mancano nel suo database e li accetta, rifiutando invece quelli di cui è già in possesso, che **non gli verranno mai più riproposti**.

Al giorno d'oggi alcuni newsserver aggiungono anche dei **filtri nell'accettazione dei messaggi**, così da preservare i propri utenti dallo spam, in effetti vedere un messaggio di questo tipo nei newsgroup è sempre più raro, e anche se riuscisse ad eludere questi, i newsmaster o delle persone che hanno

questo compito, "mandano" i cosiddetti cancel che sono dei comandi in remoto che servono per cancellare questi messaggi.

>> Difendiamo la privacy

La cosa più importante è sicuramente **evitare di pubblicare dati personali** perché non dobbiamo dimenticare che tutti possono leggere i nostri messaggi.

Ma il flagello maggiore che infesta i newsgroup è la ricerca di indirizzi email, infatti **gli autori di spam usano dei subdoli programmi che sono in grado di scandagliare i gruppi di discussione e ricavarne indirizzi email**. Ma non temiamo, c'è una soluzione. Infatti basta aggiungere alcune lettere all'indirizzo email, ovvero usare un indirizzo del tipo **userNOSPAM@provider.com** oppure **user@provider.com.invalid**, questo truccetto semplice ma molto efficace ci preserverà da gran parte della posta spazzatura.

>> Leggiamo i newsgroup

Dopo un po' di teoria possiamo entrare nel mondo dei newsgroup. Nella sezione Contenuti Extra troverete un tutorial per configurare Outlook Express, che però non è affatto l'unico programma per la lettura dei newsgroup. Infatti, per gli utenti più smaliziati o che non sono al loro primo impatto con i newsgroup, esistono anche **FreeAgent** (www.fortinc.com), **XNews** (<http://xnews.newsguy.com>), e **Netscape Mail & Newsgroup** (www.netscape.com), tutti quanti freeware. Per chi invece non ha voglia di stare a configurare un client può leggere i newsgroup (e postare previa iscrizione gratuita) da <http://groups.google.com> dove si trova inoltre l'archivio storico che contiene i post da circa 8 anni a questa parte del mondo usenet; oppure www.mynewsgate.net dove sono presenti tutti i newsgroup italiani.



NEWBIE



>> Per concludere...

Dopo una fase iniziale macchinosa e con qualche difficoltà la "cybervita" nel mondo dei newsgroup **diventerà semplice e divertente**; scoprirete che è un luogo dove chiedere qualsiasi cosa, ricevere una risposta a una qualunque vostra domanda, trovare gente con la quale fare discorsi costruttivi e scambiare qualche opinione, eccetera. Per qualsiasi problema di configurazione, per avere informazione o per chiedere qualcosa attinente all'argomento, non esitate a contattarmi, sarò lieto di aiutarvi. ☒

Imperator
imp3r4tor@libero.it

LA METAFORA DEL BAR

Da anni in Rete circola questo divertente ma illuminante testo sulle dinamiche di un newsgroup.

"Il vecchio paragone del bar funziona sempre. Se provi a guardare questo NG come un bar capisci quasi tutto: il bar è un locale aperto al pubblico, in cui c'è gente che passa una volta soltanto per un caffè o per fare una telefonata urgente; ma ci sono anche dei frequentatori abituali, gente del quartiere, compagnie fisse, e qualcuno che addirittura vive quasi lì, seduto al suo tavolino di sempre davanti a una birretta piccola.

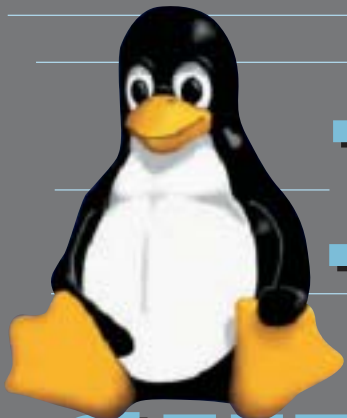
La gente nuova è guardata con interesse e curiosità, gli abituee commentano e pettegolano, e se qualcuno appena entrato si mette a sbraitare perché nessuno lo serve all'istante, e magari picchia un pugno sul tavolo e sputa per terra, be'... quelli di sempre borbottano.

E qualche testa calda, con tre grappe di troppo nello stomaco e su per la testa, magari lo prende a parolacce, lo afferra per la collottola e gli pianta un bel calcio in culo.

Ma c'è anche tanta gente che entra, si siede tranquillo, guarda lo sbronzio di turno che pontifica, ascolta le chiacchiere, abbozza un commentino sorridente, offre un giro di bianchi ai presenti.

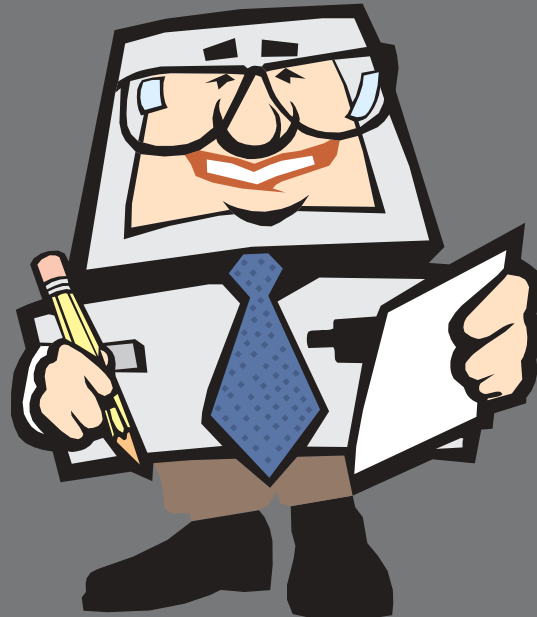
E diventa quasi subito uno di quelli di sempre."

Programmare



1a

SHELL



Come modificare l'ambiente a linea di comando per fargli fare ciò che volete.

La shell di un sistema operativo è un'astrazione che **permette all'utente di interagire con la macchina**. Generalmente essa è di tipo testuale, ma esistono delle anche implementazioni grafiche (le cosiddette GUI, Graphical User Interface) o addirittura vocali. La **bash** (Bourne Again SHell) è la shell più diffusa per GNU/Linux ed offre diversi costrutti che consentono ai programmatori di realizzare degli **script** anche piuttosto complessi.

Lo scopo di questa serie di articoli è guidare il lettore passo dopo passo nella realizzazione di programmi per GNU/Linux sfruttando le caratteristiche della bash.

>> Script elementari

La struttura base di uno script di shell è molto semplice. Ecco un esempio :

```
#!/bin/bash
echo "Hello World"
```

La prima riga definisce l'**interprete** (stiamo lavorando con un linguaggio che non genera file binari eseguibili) che dovrà elaborare ed eseguire il contenuto dello script. È possibile utilizzare indifferentemente **/bin/bash** o **/bin/sh** (in quest'ultimo caso 'sh' deve essere un collegamento a 'bash').

La seconda riga invece stampa la scritta 'Hello World' sullo

schermo. Le **virgolette** sono utili per evitare alla shell di espandere la stringa digitata e quindi di eseguire comandi indesiderati. Per eseguire questo script è necessario che abbia il permesso di esecuzione (**chmod +x script.sh**) oppure che venga dato come file di input all'interprete bash (es. **bash script.sh**). L'estensione del file è a piacere.

>> Variabili e commenti

Ora analizziamo un programma leggermente più complesso :

```
#!/bin/bash
# Questo è un commento
VARIABILE="Hello World"
echo $VARIABILE
```

In questo **sorgente** abbiamo introdotto l'utilizzo dei **commenti** e delle **variabili**.

Un commento è una riga di testo iniziante con il simbolo '#': essi vengono adoperati per fare delle annotazioni.

Una variabile invece è un costrutto che permette di associare ad un'**etichetta** una determinata **stringa**. Essa si crea definendone il **nome**, seguito dal simbolo '=' (uguale) e dalla stringa (preferibilmente racchiusa tra **virgolette**). Una variabile può essere richiamata da un comando facendone precedere il nome dal simbolo '\$'.



Ricordo che questo linguaggio è **case sensitive**, quindi 'VARIABLE' sarà diverso da 'variabile' o 'Variabile'.

>> In and out

In un programma può essere necessario chiedere all'utente un dato attraverso lo **standard input**. Vediamo come :

```
#!/bin/bash
echo -n "Digita una parola: "
read PAROLA
echo "La parola digitata è: $PAROLA"
```

L'opzione **-n** di **echo** comunica al programma di non andare a capo dopo l'ultima parola: in questo caso l'input dell'utente verrà visualizzato subito dopo la fine della stringa.

Il comando **read** legge dallo standard input ed assegna alla prima variabile specificata la prima parola digitata, alla seconda variabile la seconda parola digitata e così via.

L'ultima riga infine visualizza il contenuto della variabile **PAROLA**.

>> Ridirezione dell'I/O

La shell bash offre degli **operatori di ridirezione** che permettono appunto di ridirigere l'output o l'input di un programma. Essi sono molto utili poiché consentono di **gestire in maniera migliore l'I/O**.

L'operatore **'>'** permette di salvare l'output di un programma su un file. Esso prende i dati direttamente dallo standard output e non mostra alcun messaggio sullo schermo appartenente a questo standard. Ecco un esempio :

```
#!/bin/bash
# Salvo il contenuto della directory corrente nel file
output.txt
ls -al > output.txt
```

Lo scopo di questo programma è **memorizzare l'output** del comando ls all'interno del file **output.txt**.

L'operatore **'<'** permette invece di ridirigere il contenuto di un file nello standard input di un programma. Analizziamo insieme questo sorgente :

```
#!/bin/bash
# Mostro il contenuto del file output.txt
less < output.txt
```

Questo programma reimpagina il contenuto del file **output.txt** con l'ausilio del comando **less**.

In molte situazioni questo operatore può essere omesso, ma con comandi come **patch** è obbligatorio.

In alcuni casi può essere necessario **ridirigere l'output di un**

programma nello standard input di un altro.

Esiste un operatore chiamato **pipe**, caratterizzato dal simbolo **'|'**, che svolge questo compito. Ecco un esempio di utilizzo della pipe :

```
#!/bin/bash
# Reimpagino il contenuto della directory corrente
ls -al | less
```

Questo programma reimpagina l'output del comando ls attraverso less.

L'ultimo operatore che analizzeremo è **'>'**: esso svolge una funzione analoga all'operatore **'>'** ma si preoccupa di **appendere** l'output generato dal programma al contenuto del file su cui si effettuerà la ridirezione, **preservandone il contenuto**. L'operatore **'>'** invece comporta la **cancellazione del contenuto del file di destinazione**. Ecco un esempio :

```
#!/bin/bash
# Genero due elenchi differenti per la directory corrente
ls > output.txt
ls -al > output.txt
```

Lo scopo di questo script è molto semplice: realizzare due elenchi differenti (uno classico e l'altro con file nascosti ed altre informazioni) per la directory corrente. In particolare viene creato prima l'elenco classico e quindi memorizzato sul file **output.txt** (è possibile usare indifferentemente **'>'** e **'>'**); successivamente l'elenco più dettagliato viene appeso ai dati già esistenti.

>> Istruzioni decisionali

Le **istruzioni decisionali** sono quelle che permettono al computer di effettuare una scelta, secondo la logica booleana, in base ad una condizione prestabilita. L'istruzione decisionale per eccellenza è **if**. Analizziamo insieme questo esempio in cui compare tale istruzione:

```
#!/bin/bash
# Ottengo una parola dall'utente e vedo se corrisponde a "cane"
echo -n "Digita una parola: "
read PAROLA
if [ $PAROLA = "cane" ]
then
echo "Hai digitato la parola \"cane\""
else
echo "Non hai digitato la parola \"cane\""
fi
```





Il costrutto **if** ha una sintassi molto semplice: si esprime la **condizione** tra parentesi quadre e se essa risulta vera la shell esegue le istruzioni subito dopo **then**. In caso contrario è possibile specificare delle istruzioni opzionali alternative subito dopo **else**. Ogni costrutto **if** termina con **fi**. Per esprimere una condizione si può fare un raffronto tra due variabili oppure tra una variabile ed una stringa: il simbolo '=' indica uguaglianza, mentre '!=' disuguaglianza.

Nell'esempio abbiamo incontrato anche il simbolo \ (o comunemente **backslash**). Esso serve a evitare l'espansione di una parola chiave, di una stringa, di un simbolo e così via. Nel caso in cui non l'avessimo utilizzato nelle istruzioni con **echo** prima delle virgolette che precedono la parola 'cane', quest'ultime verrebbero automaticamente ignorate dalla bash.

Un'altra istruzione decisionale molto utilizzata ed apprezzata è **case**. Essa può essere utilizzata al posto di **if** nel caso in cui l'adozione di quest'ultima possa risultare dispendiosa e macchinosa. Ecco un esempio :

```
#!/bin/bash
# Ottengo una parola dall'utente e la confronto con altre
echo -n "Digita una parola: "
read PAROLA
case $PAROLA in
    cane) echo "Hai digitato la parola \"cane\"" ;;
    festa) echo "Hai digitato la parola \"festa\"" ;;
    *) echo "Hai digitato una parola sconosciuta !" ;;
esac
```

Ogni istruzione **case** richiede almeno un **pattern** (in questo caso la variabile **PAROLA**; pattern multipli possono essere specificati separandoli con una **pipe** ma non sono molto usati); successivamente vanno specificati i singoli valori seguiti dal simbolo **)**, dalle relative istruzioni e infine da una **coppia di punti e virgole**. Il simbolo ***** esprime tutti i valori non specificati ed è opzionale. Ogni costrutto **case** termina con **esac**.

>> Le funzioni

Una **funzione** è un particolare costrutto che permette di associare ad un'etichetta una serie di istruzioni. Esse sono molto utili poiché permettono di risparmiare tantissimo tempo nella realizzazione di programmi che ripetono ciclicamente le stesse istruzioni. Analizziamo insieme questo esempio con le funzioni:

```
#!/bin/bash
# Stampo la scritta "Hello World !" sullo schermo
# servendomi delle funzioni

function funzione_prova {
echo "Hello World"
}
funzione_prova
```



```
NAME
  bash - GNU Bourne-Again Shell

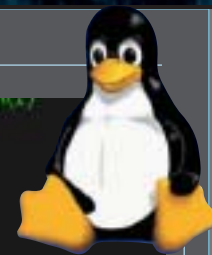
SYNOPSIS
  bash [options] [file]

COPYRIGHT
  Bash is Copyright (C) 1989-2001 by the Free Software Foundation, Inc.

DESCRIPTION
  Bash is an sh-compatible command language interpreter that executes commands read from the standard input or from a file. Bash also incorporates useful features from the Korn and C shells (ksh and csh).

  Bash is intended to be a conformant implementation of the IEEE POSIX Shell and Tools specification (IEEE Working Group 1003.2).

OPTIONS
  !
```



Volete saperne di più sulla shell?

Digitate `man bash` sul terminale e troverete il manuale di istruzioni.

Ogni funzione è strutturata in maniera molto semplice: dopo **function** si specifica l'**etichetta** da assegnare alla funzione e tra **parentesi graffe** si scrivono le istruzioni da eseguire. Ogni funzione si richiama digitandone il nome, proprio come se fosse un altro script o programma. È possibile passare dei parametri ad una funzione, ma studieremo questa possibilità nelle prossime puntate. Esiste anche un altro metodo per definire una funzione, molto noto ai programmatori in C:

```
etichetta() {
  istruzioni
}
```

>> Conclusione

Nella prima puntata di questo mini-corso abbiamo studiato i fondamenti della programmazione di shell, che sono comuni a un po' tutti i linguaggi di programmazione. Nella sezione **Contenuti Extra** del sito di Hacker Journal potete trovare gli script citati in queste pagine, per fare un po' di pratica. Nei prossimi numeri ci addenteremo nei meandri della shell bash utilizzando le **istruzioni iterative**, gli **operatori di controllo**, le **variabili di shell** e molto altro ancora.

pctips

Copyright (c) 2003 pctips <pctips@hardwaretips.com>

E' garantito il permesso di copiare, distribuire o modificare il testo di questo documento in base ai termini della GNU Free Documentation License, Versione 1.2 o successive pubblicate dalla Free Software Foundation; senza Invariant Sections, Front-Cover Texts, né Back-Cover Texts.



IL PROGRAMMA

TI ASCOLTA

Come un programma può interagire con l'utente, accettando parametri in ingresso e restituendo dei risultati in uscita.

Siamo entrati in confidenza con le strutture fondamentali che costituiscono la logica della programmazione, e che sono alla base della struttura dei nostri futuri programmi; abbiamo gettato le fondamenta e abbiamo i mattoni per costruire, mancano le rifiniture per completare l'opera.

In questo articolo prenderemo in esame gli **input tramite tastiera** e gli **output su schermo**.

Insomma, il passo in avanti che dobbiamo fare è quello di fornire al nostro programma una certa interazione con l'utente, in modo che quest'ultimo possa **essere guidato nella corretta esecuzione del programma stesso**.

Per chiarire l'importanza dell'interazione fra utente e programma facciamo un esempio. Si vuole creare un programma per **calcolare l'area di un quadrato**; quello che dovrà immettere l'utente, ovviamente sarà la **lunghezza del lato** del quadrato.

Come pensate che si possa sentire un utente che dopo aver lanciato il programma vede comparire sullo schermo un punto di domanda o peggio il solo cursore lampeggiante?

Alquanto smarrito, non sa che fare; una situazione simile al protagonista della leggenda internetiana (non metropolitana) del "press any key"!

Quindi per prima cosa è buona norma stampare a video qualche riga di presentazione del programma del tipo:

```
*****
* Calcola area quadrato *
*****
```

ed eventualmente stampare anche il nome dell'autore del

programma, la data di realizzazione il numero di versione ed anche un indirizzo e-mail per poter essere contattati (è sempre meglio avere un feed-back con l'utente finale che attraverso le sue critiche, potrà portare ad una migliore realizzazione del programma e ci aiuterà nello scovare i possibili, per non dire certi!, errori e nel trovare il giusto rimedio).

Dopo di che ogni volta che è richiesta la partecipazione dell'utente, è sempre meglio **mandare un messaggio a schermo**, del tipo:

Immetti lato quadrato:

Il nostro programma sta così guidando passo passo, l'utente nell'immissione dei dati di input necessari all'esecuzione del programma.

A questo punto, il programma **sviluppa le operazioni necessarie** (una banale moltiplicazione in questo esempio) e **stampa a video il risultato** numerico ottenuto.

Anche in questo caso è sempre meglio evidenziare che cosa si è ottenuto, ad esempio tramite:

L'area del quadrato è:

>> Si fa presto a dire output...

Abbiamo visto che **ogni linguaggio di programmazione ammette una diversa sintassi**, e non fanno eccezione a questo le varie tipologie di formato, per una ordinata visualizzazione dei dati di output.

Il problema di visualizzare i dati in formato opportuno è parti-

PROGRAMMAZIONE. ■ ■

colarmente sentito in ambiente scientifico-numerico, dove spessissimo si ha la necessità di incolonnare i dati risultanti dai calcoli.

Vedremo adesso degli esempi nei vari linguaggi che abbiamo preso come punto di riferimento (il linguaggio **C**, il **Pascal** e il **Visual Basic**).

Linguaggio C

Prima di tutto è necessario includere la libreria che gestisce le funzioni standard di input e output:

```
#include <stdio.h>
```

Dopo di che la stampa su schermo è ottenuta attraverso la funzione **printf**; ad esempio:

```
printf("Lato= %i metri\n\a",lato);
```

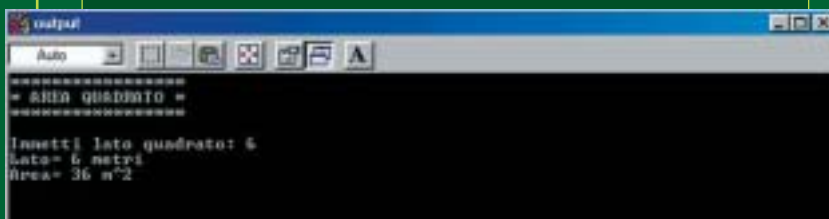
"%i" indica il formato di stampa su video della variabile di nome lato (vedi box sui marcatori di conversione).

\n il cursore viene posizionato su una nuova linea (a capo).

\a emette un beep.

\t introduce una tabulazione.

\? visualizza un punto interrogativo.



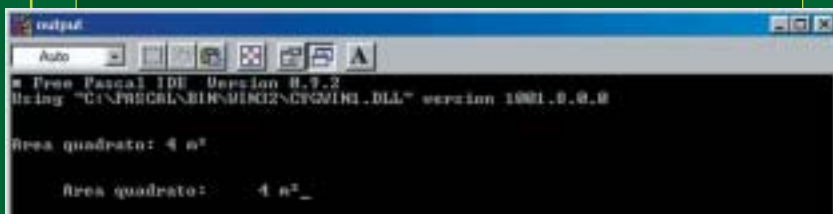
Pascal

Per stampare a video un messaggio si ricorre al comando **write** o al comando **writeln**; la differenza fra i due è che quest'ultimo una volta stampato quello specificato, pone automaticamente il cursore su una nuova riga (line; da qui write + ln).

```
write('Area quadrato: ',area,' m2');
```

Un uso un po' più sofisticato permette di specificare il numero di caratteri necessari alla visualizzazione di ogni singola espressione:

```
write('Area quadrato: ':20,area:5,' m2');
```



In questo modo abbiamo riservato **20 caratteri** per la scrittura della stringa "Area quadrato" e **5 caratteri** per contene-

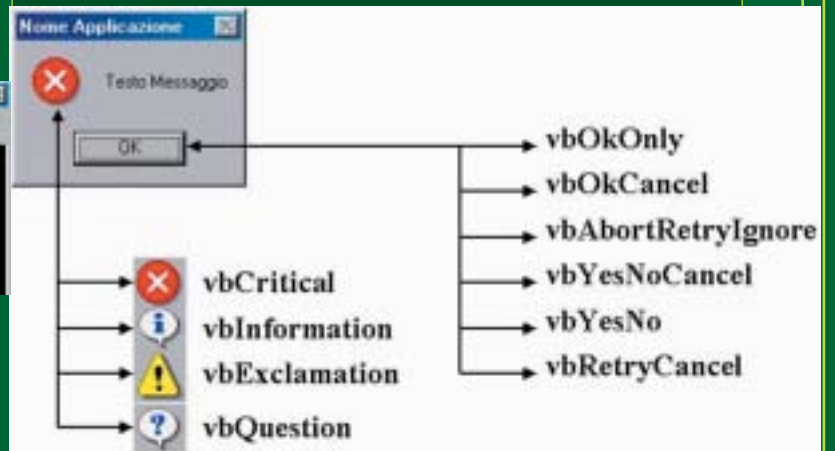
re il valore relativo all'area del quadrato. Nel caso il numero da rappresentare sia un numero reale possiamo anche specificare il numero di decimali che si vogliono visualizzare.

```
write(area:10:2);
```

Riserva al numero contenuto nella variabile **"area"** 10 caratteri di cui 1 per la virgola e 2 per i decimali.

Visual Basic

Un discorso a parte merita il Visual Basic; infatti in tale linguaggio l'interazione utente-programma **viene un po' stravalta da quelli che sono i normali canoni**. Il codice va in esecuzione in base a quelli che sono gli eventi attivati dall'utente, ad esempio: fare clic su di un pulsante, fare clic su di una immagine, inserire del testo in una casella di testo e così via. Di conseguenza sia l'input (da parte dell'utente) che l'output (da parte del calcolatore) **può avvenire nelle forme più disparate**. Per esempio il risultato di una operazione può essere inserito in una casella di testo, oppure in una tabella. Ma forse la forma che più si avvicina alla "classica" forma di output è il così detto **MsgBox()**.



La sintassi del comando è la seguente:

```
intMessaggio = MsgBox("Testo Messaggio",  
vbCritical + vbOkOnly, "Nome Applicazione")
```

Come possiamo vedere (sia dalla sintassi che dalla figura) il corpo del messaggio è molto articolato; distinguiamo il corpo del messaggio vero e proprio **"Testo Messaggio"**, un titolo del messaggio **"Nome Applicazione"**, la presenza di una eventuale icona (**vbCritical**) e della tipologia dei pulsanti visualizzati (**vbOkOnly**). Si noti inoltre che l'intero corpo del messaggio **MsgBox(...)** è stato posto uguale a una variabile **intMessaggio** di tipo intero (prefisso **int**), questo perché in tale variabile è memorizzato un numero intero che corrisponde al tipo di tasto schiacciato dall'utente:

intMessaggio = 1 se l'utente ha fatto click su Ok

intMessaggio = 2 se l'utente ha fatto click su Annulla

intMessaggio = 3 se l'utente ha fatto click su Termina



intMessaggio = 4 se l'utente ha fatto click su Riprova
intMessaggio = 5 se l'utente ha fatto click su Ignora
intMessaggio = 6 se l'utente ha fatto click su Sì
intMessaggio = 7 se l'utente ha fatto click su No
 Nell'esempio di figura **intMessaggio** potrà assumere solo il valore 1.

>> ...e gli input?

Dopo aver visto come i vari linguaggi implementano la funzione di stampa a schermo, vediamo come affrontano l'argomento opposto, cioè l'immissione di valori.

Linguaggio C

Dopo aver incluso la libreria per la gestione degli input e degli output (stdio.h), l'acquisizione di una grandezza avviene attraverso la funzione **scanf**; ad esempio:

```
scanf("%i",&lato);
```

"%i" indica come prima il formato di acquisizione della variabile (vedi box sui marcatori di conversione) di nome lato. Si noti come il nome della variabile sia preceduto dal carattere "&" (ampersand).

Pascal

Per immettere un dato da tastiera si può ricorrere a **read** o al comando **readln**; per esempio:

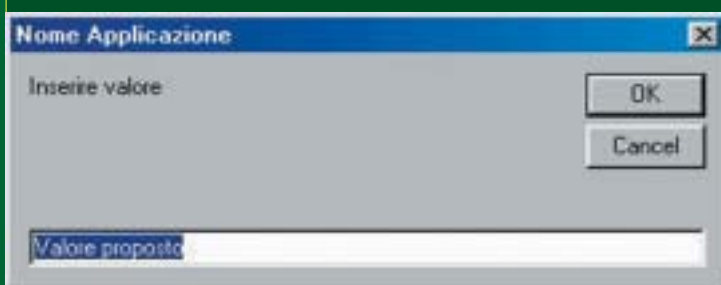
```
read(a,b);
```

Richiede l'input sulla stessa riga (visto che non si è usato readln) di 2 valori da tastiera che siano separati da uno spazio.

Visual Basic

Anche in questo caso per il Visual Basic possiamo parlare di una "classica" forma di Input attraverso la funzione **InputBox()**.

La sintassi del comando è la seguente:



```
strInput = InputBox("Inserire valore",  
"Nome Applicazione", "Valore proposto", 300,  
500)
```

Come per l'analogica funzione di output (**MsgBox**), anche la funzione di Input (**InputBox**) è molto articolata: vi è una inte-

stazione per la finestra di input "**Nome Applicazione**", un messaggio descrittivo "**Inserire valore**" e un eventuale (può anche non esserci) suggerimento "**Valore proposto**"; **300** e **500** indicano rispettivamente la coordinata x ed y dello spigolo in alto a sinistra della finestra di input (in una unità di misura particolare il twip = 1/567 cm = 1/1440 pollice); qualora siano omesse tali coordinate, la visualizzazione della finestra di input avviene **al centro dello schermo**. Si noti come anche in questo caso il tutto è posto uguale a una variabile stringa di nome **strInput** che conterrà il valore immesso dall'utente attraverso la finestra di **InputBox**.

>> In conclusione

Abbiamo visto come gli input e gli output permettano un efficace e gradevole colloquio fra utente e calcolatore, come siano semplici da usare ma un pochino complessi (soprattutto per quanto riguarda i formati) qualora se ne voglia fare un utilizzo avanzato, ma che sicuramente può qualificare ulteriormente la nostra applicazione. Inoltre si è visto come ogni linguaggio abbia una struttura particolare nella gestione degli input e degli output, anche se l'obiettivo da raggiungere è il medesimo.

>> Nel prossimo articolo...

Nel prossimo articolo prenderemo in esame un'altra forma di input e di output: i file. ☞

>>--Robin-->

RobinHood.Sherwood@libero.it

Parametri per l'output

Numero	Stringa visualizzata (b= spazio vuoto)	Marcatore per printf()
1000	1000	%i
1000	bbb100	%7i
1000	b1000	%5d
123.4567	123.456700	%f
123.4567	bbbb123.46	%10.2f
123.4567	b123.45670	%10.5f
123.4567	1.234567e+002	%e
123.4567	1.2346E+002	%.4E

Parametri per l'input

Tipo variabile	Marcatore per scanf()
int	%i, %d
long int	%li, %ld
float	%f, %e, %E, %g, %G
double	%lf, %le, %lE, %lg, %lG
long double	%Lf, %Le, %LE, %Lg, %LG

Per una trattazione più completa dei marcatori si rimanda ad un qualsiasi manuale per il linguaggio C