Allora iniziamo col dire cosa è Telnet. Telnet è un'applicazione standard dell'Internet ed è disponibile nella maggior parte delle implementazioni del TCP/IP (Transfer Control Protocol/Internet Protocol...spero sappiate cosa siano), indipendentemente dal sistema operativo host.

In pratica consente di realizzare un collegamento remoto con un altro calcolatore connesso attraverso Internet al vostro. Il vostro terminale (o il vostro personal che "finge" di esserlo con un programma di emulazione) diventerà per tutto il tempo del collegamento un terminale del calcolatore remoto, per ritrasformarsi alla fine nel vostro computer di tutti i giorni.

Potrete quindi collegarvi a qualsiasi demone (programma che "vigila" sulle porte; se non sai cosa sono le porte è un problema). Praticamente le porte, quando sei connesso, evitano che i programmi mischino i loro dati mentre li trasmettono (Per evitare il CONFLITTO) e si disturbino a vicenda. Ognuna di essa svolge un servizio che non può essere svolto da un'altra porta. Spero di essere stato chiaro.

Ma torniamo a telnet.

La struttura di una connessione Telnet e' basata anch'essa su un'architettura client-server: la macchina che vuole stabilire la connessione deve avere montato un client Telnet mentre sulla macchina che riceve la richiesta di connessione deve essere approntato un server Telnet; quando il client vuole stabilire una connessione, invia la richiesta al server dopodiche' viene stabilita la connessione, e saremo collegati alla macchina remota. Telnet rilancia i caratteri battuti sulla tastiera dell'utente direttamente al calcolatore remoto come se essi fossero battuti su una tastiera direttamente connessa ad esso. Inoltre Telnet ritorna l'output della macchina remota indietro fino allo schermo dell'utente.

Per collegarsi normalmente tramite Telnet bisogna sapere il nome del "sito" o l'indirizzo IP, oltre che il numero della porta. La porta standard di Telnet è la 23. Ma se per esempio volgiamo spedire e-mail bisogna collegarsi all porta SMTP cioè la 25. Come ho detto ogni porta ha la sua funzione.

Per collegarsi basta fare:

Windows:
1)Start / Esegui / scrivete "Telnet" e cliccate Ok. Selezionate Connetti.
2)facendo click sul file "telnet.exe" presente nella cartella "windows".
3)digitando "telnet" nel prompt ms-dos.

In ogni caso appare:

Nome host: indirizzo dell'host a cui collegarsi
Porta: numero della porta a cui collegarsi
tipo di terminale: Per ora è meglio che non toccate!

Linux [da console]:
telnet nomehost porta

Niente d'impossibile.
Adesso vi faccio un esempio di connessione con telnet così capite meglio. Facciamo finta che vogliamo prendere una shell:

Nome host: nether.net
Porta: Telnet (o 23...è uguale)
Tipo Terminale vt100

Clikki su ok e sei connesso! In questo caso dovrebbe apparire:

Kernel SunOS 5.6 Generic_105181-17 on a sun4d
Welcome to nether.net
(o qualcosa del genere)

Login: (chiede il login...per esempio newuser)
Password: scrivi una pass (di solito nn viene visualizzata).

E così via...non sto a scrivere tutti i comandi perchè cambiano da demone a demone. Potrete trovare una lista delle porte utili in c:windowsservices

Vabbè spero di aver soddisfatto la vostra curiosità...uhm c'è tempo per trattare un altro argomento utile:

Elenco di tecniche utili per hackerare un sito con telnet
1) Default Login
2) Backdoors
3) Password List o Password Guessing

1)Questo consiste nell'inserire una lista di account seguiti da password comuni, ovvero di quelle password che i sysop (system operator: operatori di sistema cioè coloro che controllano tutto il sistema) più ingenui mettono

per controllare i propri accessi. Solitamente il login è di 1-8 lettere mentre la password di 6-8. Prima di incominciare ad inserire le password e gli account, dovete scoprire tutte le informazioni possibili sul bersaglio.

Probabilmente avrete sentito parlare di social engineering e il default login è una possibile applicazione di questa tecnica.

2) Backdoors:

Le backdoors sono quelle password che il programmatore del sistema mette per avere accesso in futuro a quel dato computer e che solamente lui conosce. Per cercare di individuare la password bisogna fare lunghe ricerca sulla persona che ha impostato tutto il sistema.

Anche qui tanto e tanto social engineering.

Sicuramente questo è il sistema più difficile ma credo che dopo una lunga ricerca sia anche il più sicuro poichè poche persone (cioe' quelle furbe) inseriscono come password qualcosa che non gli è familiare.

3) Password List o Password Guessing:

Un altro metodo per inserirsi in un sistema è quello di "rubare" la password di un altro utente. Per prendere un valido account a cui dare una password bisogna "fingerare" (attacco tramite finger) l'utente e leggere (anche se criptato) il passwd file; è meglio se il finger viene fatto durante il giorno.

Una volta trovato l'account (tramite il finger oppure nel passwd file), bisogna inserire una alla volta le password della lista consigliata per ogni sistema per cercare di individuarne una giusta e per poter così accedere al sistema.