.....:::::::Crossing Platforms::::::.....

di 5am ...no warranty!

Un piccolo how to di base per poter utilizzare le proprie risorse su qualsiasi piattaforma.

Introduzione.

Spesso ci troviamo davanti a dei problemi che possiamo risolvere facilmente da sole, uniformando l'utilizzo della mail, scambiando file in formati leggibili da tutti, standard, verificando la presenza di virus e processi molesti, e -soprattutto- mantenendo l'anonimato, indipendentemente dal sistema operativo che stiamo utilizzando. Questo perche' possiamo trovarci difronte ad pc con Windows, o ad un MacOSX o ad un pc con linux, a casa di un amic@, sul posto di lavoro, ad un internet caffe' o a scuola/all'universita'.

1. I file.

Un file (termine inglese per "archivio") in informatica e' un insieme di informazioni codificate organizzate come una sequenza di byte, dove per byte (contrazione di binary term) si intende una sequenza di bit, il cui numero dipende dall'implementazione fisica del computer che abbiamo, immagazzinate come un singolo blocco su di una memoria di massa (qualsiasi supporto che sia capace di archiviare informazioni, hard disk, floppy, cdrom, dvd, penna usb, smartcard) all'interno del File System esistente.

I file si differenziano tra loro per permessi (ovvero chi puo' fare cosa e come) ed eseguibilita' (interazione con il computer).

Il bello di linux e' che tutto e' un file; il problema nasce quando cerchiamo di fare qualcosa con altri sistemi operativi... quindi importante e' capire come scambiare file, o meglio quali estensioni utilizzare! Per estensione s'intende la capacita' di far associare programma/file e renderlo visibile all'utente.

file.txt lo leggono tutti > testo non formattato
file.pdf lo leggono tutti > testo formattato impaginato
file.htm o .html lo leggono tutti > browser di rete
file.zip lo leggono tutti > pacchetto compresso
file.jpeg o file.jpg lo leggono tutti> immagine
file.gif lo leggono tutti > immagine
file.png lo leggono tutti >immagine
file.mp3 lo leggono tutti >audio
file.ogg lo leggono tutti >audio
file.avi lo loggono tutti >video
file.mp4 lo leggono tutti > video
file.mpg lo leggono tutti > video

Importante quindi utilizzare estensioni â??standardâ?? e non specifiche di un programma, in modo che, indipendentemente dal sistema operativo in uso, il file sia utilizzabile.

2. La posta

La posta elettronica e' uno strumento indispensabile oggi ma, bisogna essere coscienti del suo utilizzo.
Evitare invio di dati personali. Farlo solo se si e'sicuri del destinatario e della transazione!
Cercare, finche' possibile, un utilizzo anonimo; se possibile, utilizzare posta cripata. Se si invia un messaggio a molte persone che tra loro non si conoscono e' importante non far visualizzare i diversi indirizzi dei destinatari; si deve utilizzare la funzione BCC, (Blind Carbon Copy:, in italiano CCN, ovvero Copia Carbone Nascosta:): indirizzi e-mail dei destinatari in copia conoscenza nascosta; e' bene inviare come primo destinario se' stessi e tutti gli altri in BCC.
E' possibile inserire dei file come allegati al corpo di una mail.
Molti server impongono limiti massimi alla dimensione del messaggio da trasmettere, che devono essere rispettati; altrimenti il messaggio non viene inviato. Verificare sempre da chi si ricevono allegati; spesso potrebbero rivelarsi virus (per microsoft) Via allegato e' possibile inviare qualsiasi tipo di file, in genere i client di posta possono permettere di impostare filtri per non far "scaricare" quel tipo un tipo di file o la posta da un determinato indirizzo, verificare se si potra' utilizzare il file ricevuto, meglio sempre utilizzare estensioni standard e non proprietarie (nda vedi 1).
Non inviare lo stesso attachment a liste di persone almeno che non ne siano a conoscenza.

2.1 Client di posta

Il client di posta e' il programma che ci permette la consegna dell'e-mail; le e-mail possono essere consegnate direttamente dal "postino" (smtp -simple mail transfer protocol-) "a casa" (pop pop3) o consegnate "all'ufficio postale" (imap -internet message access protocol- o webmail). Il postino in questo caso e' un protocollo che a seconda della “divisa” ci permette una connessione. Smtp trasmette la mail, pop pop3 imap sono i protocolli di consegna come webmail.
Si possono utilizzare diversi client (uffici postali), ma nella logica di semplificarsi la vita consiglio Thunderbird, che si puo'installare su qualsiasi sistema operativo molto facilmente, sempre se si ha un pc che permette la gestione dell'interfaccia grafica ;) ed abbia permessi per farti installare cose!
Utilizzare SSL (Secure Socket Layer)* sia per la posta, configurare il client, verificare sempre la sorgente da cui si scaricano programmi, dati immagini etc.; verificare sempre chi la invia e cosa.

3. Browser

Il browser e' un programma che permette agli utenti di visualizzare (interpretare) file multipli (ipertesto) con estensione html o xhtml o htm.
I browser possono interpretare piu' o meno liberamente il codice html (HyperText Markup Language). Spesso alcuni editor di html mettono dei tag proprietari che non tutti possono interpretare, a.e.

"FrontPage", che ottimizza le pagine html per explorer, ma su altri browser crea problemi di interpretazione! Utilizzare quando e dove e' possibile SSL, che permette invio/ricezione pagine web crittate.

4. Virus & processi

I virus sono programmi che si autoriproducono e, una volta insediati nel computer, agiscono, danneggiando in alcuni casi direttamente solo il software della macchina che lo ospita, e in altri anche l'hardware, causando lo spegnimento della ventola o l'overclocking (ovvero aumentare la frequenza di progettazione) del processore. Tutto cio' si riferisce al "mondo" windows. In riferimento a linux non possiamo parlare di virus, ma di “buchi di sicurezza” e “vulnerabilita' dei processi”.

4.1 Windows

Windows, il sistema operativo "a finestre" di casa Microsoft e' composto, nel suo kernel (nucleo) da stringhe* e chiavi* che compongonoi registri*. Le chiavi di registro corrispondono alle variabili (valore che si assegna ad una casella di memoria) in ambiente linux. Un file .exe dipende sempre da un file .dll o .inf. Un virus e' composto da un gruppetto di file sparsi nel System32 o System, insinuandosi anche nei registri, in modo che la sua eseguibilita' sia assicurata all'avvio del sistema.
Esistono molti programmi che puliscono chiavi di registro, ma a loro volta ne creano altre.

Per visualizzare il registro di windows:

finestra start---> run ---> regedit ---> enter

Si aprira' una finestra con una serie di directory 'madri' e sottodirectory le classi di registri sono costituite cosi':

HKEY_CLASSES_ROOT >> apertura programmi associa file/programma
HKEY_CURRENT_USER >> configurazione utente e castomizzazioni
HKEY_CURRENT_CONFIG >> configurazione hardware
HKEY_USERS >> configurazione di tutti gli utenti
HKEY_LOCAL_MACHINE >> configurazioni di tutti gli utenti corrisponde al systemroot\system32\config hw, software e sistema operativo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run >>qui abitano gli .exe che partono allo start del sistema
HKEY_USERS\username\Software\Microsoft\Windows\CurrentVersion\Run >>qui abitano gli .exe che partono allo start del sistema, riferiti all'utente.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page >> qui si modifica la pagina di start di explorer

Per aprire una console (riga di comando) con windows xp

start ---> run ---> cmd (command line) enter

A questo punto si aprira' una finestra DOS in cui si possono digitare comandi per verificare lo stato del computer; per vedere lo stato della nostra connessione di rete esistono due comandi fondamentale da digitare "netstat -an" avremmo indirizzo porta stato della connessione, le porte (numeri che servono per identificare una specifica connessione) e gli indirizzi IP (e' il nome e cognome della tua scheda di rete); altro comando ipconfig /all per vedere la configurazione dei diversi supporti di rete.

Tips:
Disabilitare Outlook
Disabilitare system restore
Disabilitare Macros* e connessioni ai server dei diversi programmi (Adobe, Winplayer...) utilizzare programmi alternativi che hanno licenza gnu/gpl:

OpenOffice valido per tutte le piattaforme...e non soffro piu'!
Aggiornare sempre programmi e sistema con le patch che vengono rilasciate di volta in volta.
Disabilitare le funzioni di Macro in Office e di Outlook. Questa operazione si effettua in fase di installazione dei programmi (suite Office per Windows).

4.2 Linux

Se stiamo lavorando con un pc con linux o roba simile, sicuramente avremmo meno problemi di virus e codice malizioso, una buona policy e' quella di abilitare e disabilitare i servizi secondo le necessita' e i propri scopi. Per verificare quali processi sono attivi digitare dalla riga di comando:

```
[my_machine@me me]$ ps  -aux
```

Comando che permette di visualizzare tutti i processi di sistema con il nome utente, il numero di attivazione del processo (id) e la path* (percorso) del processo, il consumo risorse, e la console sul quale sta girando il processo. Da qui si vede subito se qualcosa non va.
Per verificare lo stato della connessione e le comunicazioni che abbiamo stabilito con altri computer digitare:

```
[my_machine@me me]$ netstat -aepln
```

e

```
[my_machine@me me]$ more /var/log/messages
```

Visualizzando questo file sappiamo quello che sta facendo il nostro computer; errori di sistema, report di vario genere, negoziazioni tra diversi host, autenticazioni.
Ci sono alcuni servizi (cose che posso fare) che sono "pericolosi": telnet*, che permette di comunicare con altri computer nella stessa rete, di fatto e' un protocollo di comunicazione, parla su di una porta specifica (23), cosi' come l' ftp, altro protocollo utilizzato per trasferire file da un pc all'altro; anche l'ftp "parla" su di una porta specifica (21)... cosi' come ssh* (22) o http* (80) il file che gestisce queste informazione e' /etc/services.

"A closed port is a totally safe port!!!" (una porta chiusa e' una porta sicura!!!)

I servizi risiedono (come processi) in /etc/rc.d/... o /etc/init.d/ dipende dalla distribuzione linux che utilizzate). Importante in un sistema operativo e' capire cosa ci serve e cosa no, in modo da poter utilizzare al meglio le risorse ed avere maggiore sicurezza. Uno strumento utile e' chkrootkit, il kit di root! Chkrootkit e' un insieme di strumenti di diagnostica per i processi in ambiente Unix e svolge un ottimo lavoro di scansione di tutte le parti del sistema.
ssh/scp/sftp SSH (secure shell) e' un metodo per poter loggarsi su di un altro host e scambiare/copiare file da un host all'altro. Aggiornare sempre la versione; in genere bisogna barcamenarsi con .tar.gz da compilare a mano. Scp e' un protocollo criptato che permette di scambiare file tra 2 host, cosi' come sftp, la versione criptata di ftp (File Transfer Protocol); reperibile per qualsiasi piattaforma.

Tips:
Multiutenza come autodifesa (root, users e su); mai loggarsi come root, utilizzare l'utente e se necessito di privilegi di amministratori utlizzo su o sudo, (su e' piu' facile)!

5. Password
Mantieni la password segreta.
Non dare la tua password a nessuno.
Non utilizzare la stessa password per piu' cose.
Non utilizzare la password di root per nient'altro che la password di root!
Non scrivela mai o registrarla on line.
La password dovrebbe essere una combinazione ragionevolmente lunga di lettere maiuscole/minuscole, numeri e punteggiatura .
Non utilizzare parole riconducibili al dizionario.
Non utilizzare informazioni personali come eta', hostname, data di nascita...
Memorizzare le password!

6."Live Distro"

Puo' accadere di non poter "entrare" in un computer e cosi' una distribuzione live CD puo' salvare facilmente la nostra esistenza, far partire il pc dal cdrom, inserire il cd e far partire in questa maniera avremmo accesso a tutte le risorse senza dover "manomettere" nulla, se il pc non parte da cd dovrete entrare nel bios ed impostare Boot device CDROM. Le distibuzione live sono tantissime scegliete la vostra preferita; ovvio si puo' utilizzare anche un cd d'installazione "insediare" nulla sull'hard disk. Lavorare in questa maniere richiede una di conoscenze base, sia hardware che software.

Link di supporto ed indormazioni:

http://www.cert.org
http://www.symantec.com
http://www.openssh.org
http://www.openssl.org
http://www.chkrootkit.org
http://en.wikipedia.org
http://www.linuxiso.co.uk