User, Poweruser, Administrator e SYSTEM

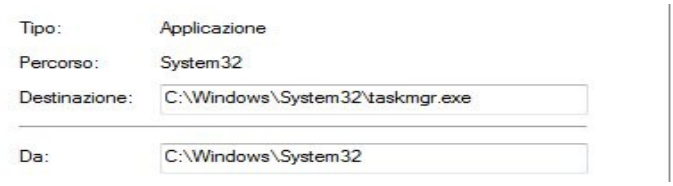
(Root per GNU/Linux, SYSTEM per Windows)

Augusto Scatolini (webmaster@comunecampagnano.it) (a.scatolini@linux4campagnano.net)
Miniguida n. 157
Ver. 1.0 Gennaio 2012

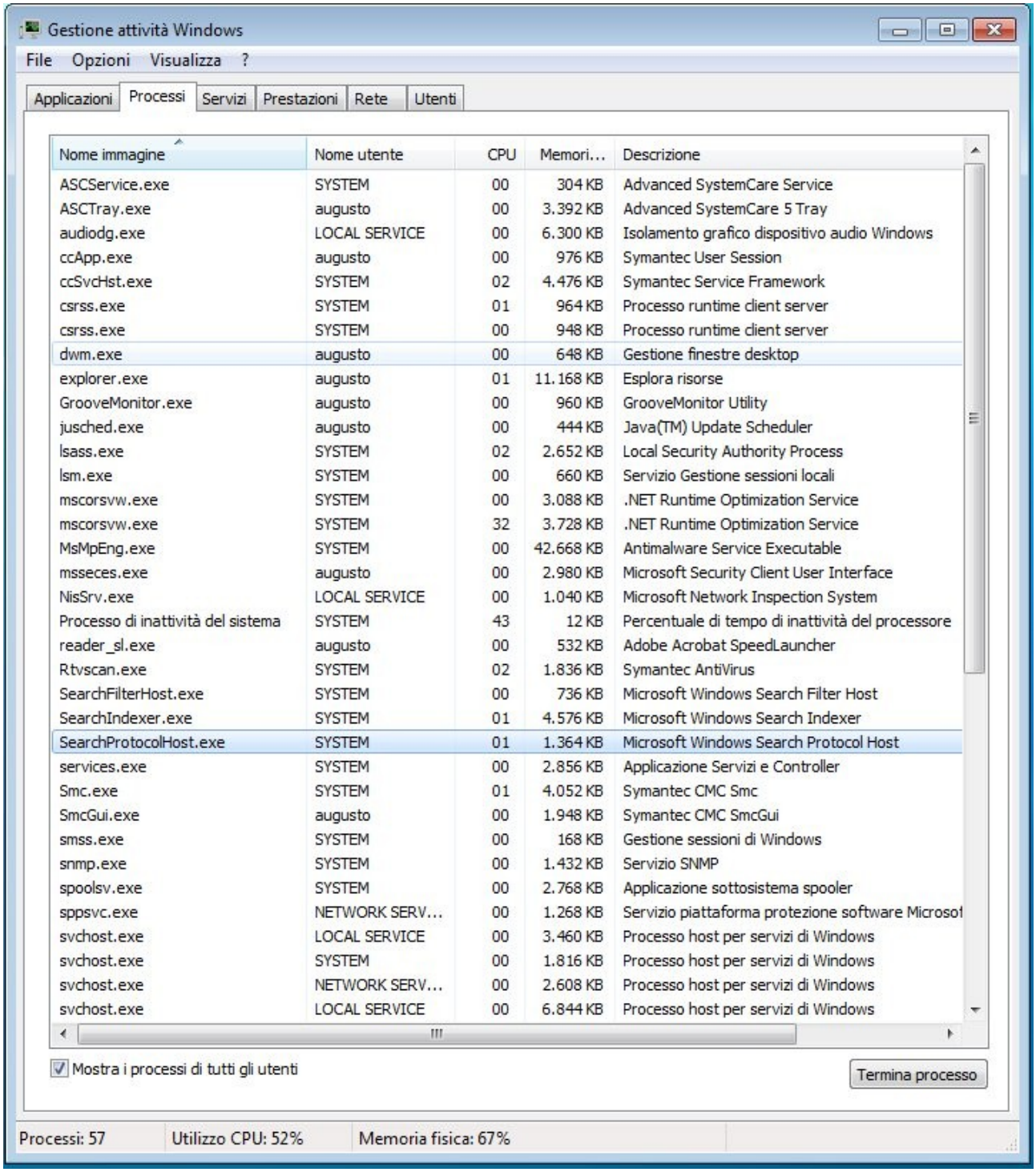
Supponiamo di avere un account su Windows7 di nome augusto che fa parte del gruppo degli amministratori.

Eseguiamo il login come augusto,

apriamo il task manager e andiamo a verificare quali utenti sono attivi:

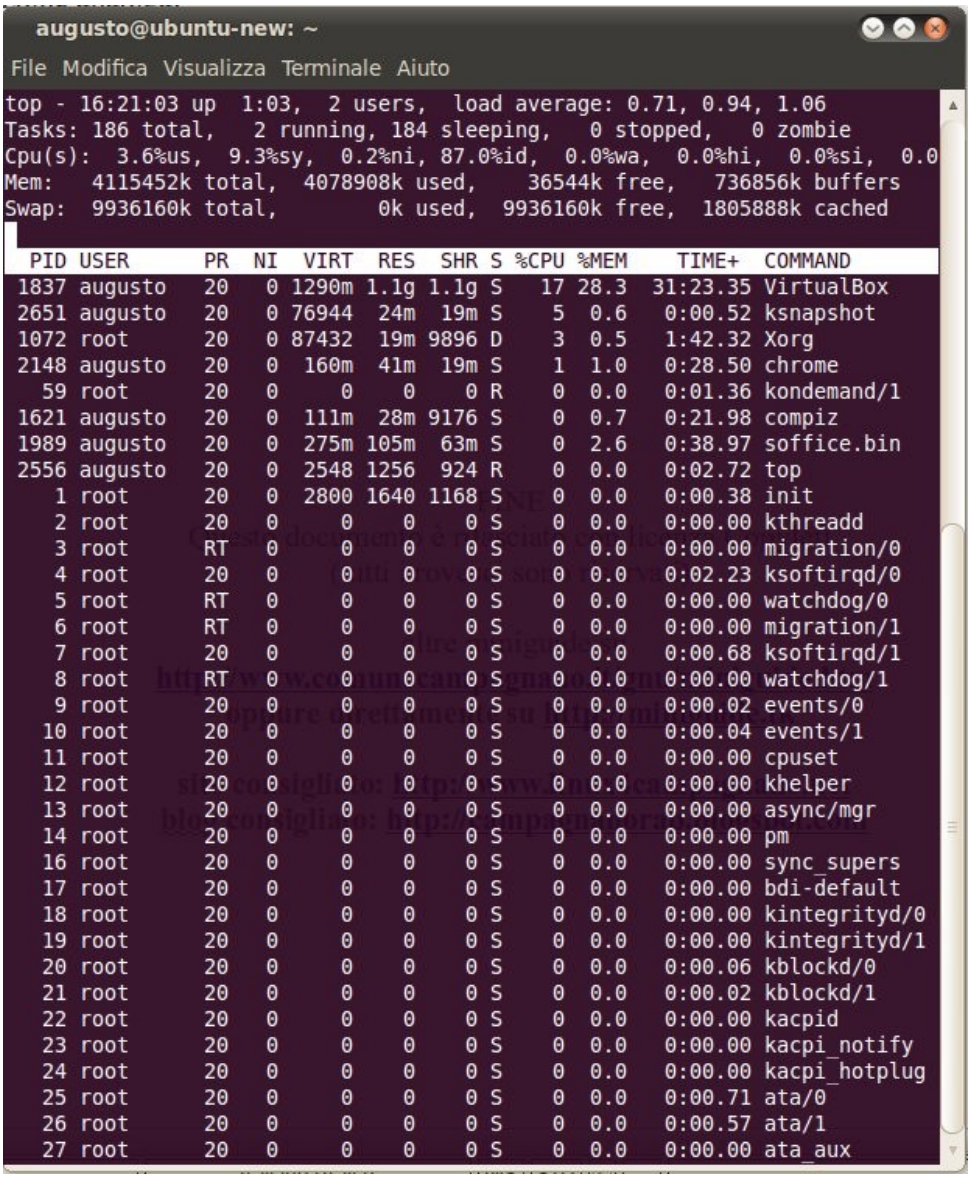


possiamo notare che oltre ai vari LOCAL SERVICE e NETWORK SERVICE e all'utente “augusto” (quello che ha eseguito il login) c'è un altro utente “SYSTEM” che ha avviato molti processi importanti sui quali l'utente “augusto” benché amministratore della macchina non ha possibilità di intervenire.



Ma allora c'è un utente più potente dell'amministratore? E chi è questo utente SYSTEM? E come si diventa SYSTEM?

Su una macchina GNU/Linux se l'utente "augusto" facente parte del gruppo degli amministratori esegue il login e poi avvia su un terminale il programma "top" (equivalente a taskmgr.exe) si noterà una situazione analoga:



oltre all'utente "augusto" (quello che ha eseguito il login) c'è un altro utente "root" che ha avviato molti processi importanti sui quali l'utente "augusto" benché amministratore della macchina non ha possibilità di intervenire direttamente.

Ma allora c'è un utente più potente dell'amministratore "augusto"? E chi è questo utente "root"? E come si diventa root?

Nei sistemi Unix-like (GNU/Linux è uno di questi) è molto semplice diventare root, anzi ci sono due modalità, una temporanea tramite il comando sudo che si premette al comando da impartire e una permanente tramite i comandi "sudo -s" o "sudo su"

La logica di questa complicazione (su GNU/Linux) è che l'utente root è tanto potente quanto pericoloso, il suo utilizzo, infatti, deve essere ridotto al minimo e solo in determinate e necessarie circostanze.

Il mondo Windows, come è ben risaputo, è molto meno democratico dei sistemi Unix-like nel senso che all'utente "augusto" (benché facente parte del gruppo degli amministratori della macchina) non solo viene impedito di accedere al sistema come "Administrator" perché questo utente è addirittura disabilitato (in Windows 7) ma gli viene nascosta l'esistenza di un utente equivalente a "root" cioè di "SYSTEM".

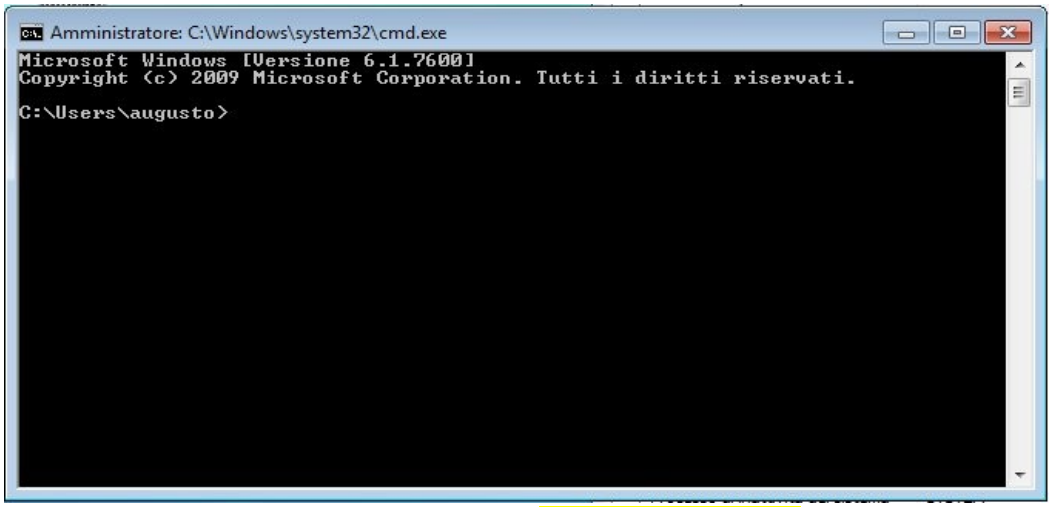
Nei sistemi Windows XP è anche peggio in quanto l'utente Administrator è attivo ma con password blank. Il massimo della sicurezza!

C'è un modo per diventare SYSTEM?

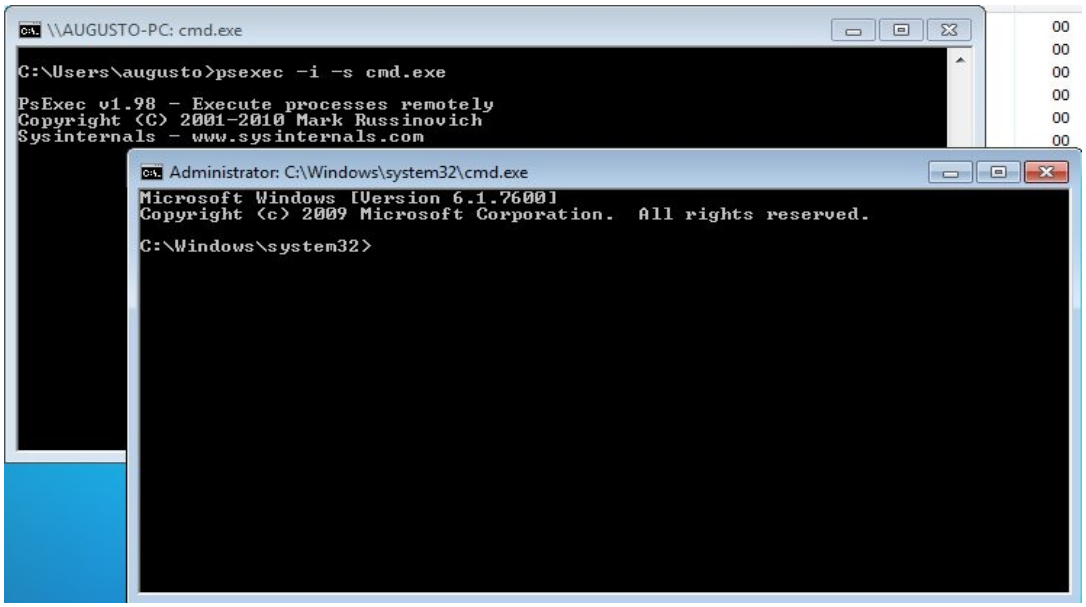
Su Windows 7 è abbastanza semplice, è sufficiente scaricare il programma psexec.exe che fa parte del pacchetto pstools.zip che fa parte della suite sysinternal che è stata acquistata proprio da Microsoft.

Si copia il programma dentro C:\windows\system32\ per poterlo eseguire da qualunque posizione.

Si lancia il comando cmd



e poi sulla finestra DOS appena aperta si digita il comando psexec -i -s cmd.exe

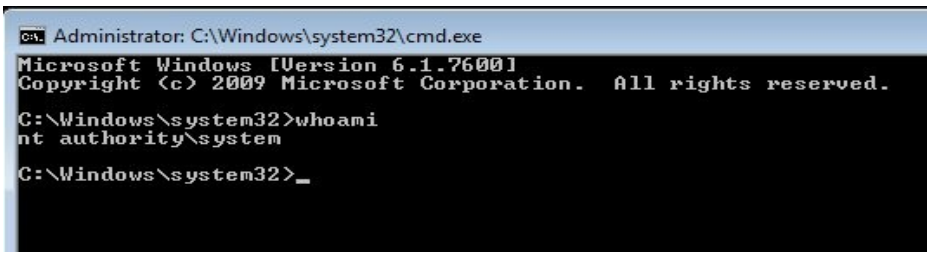


si apre immediatamente una seconda finestra DOS

ma a differenza dalla prima, sulla cornice della finestra appare "Administrator" e ci troviamo dentro la cartella C:\windows\system32

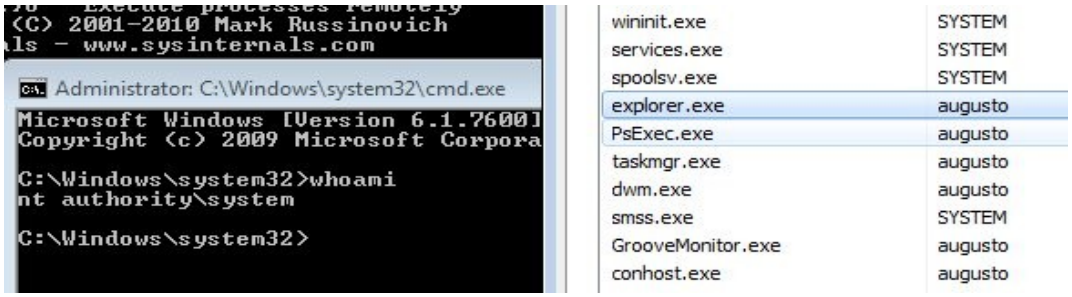
se proviamo il comando "whoami" (chi sono?) la risposta è

"nt authority\system"

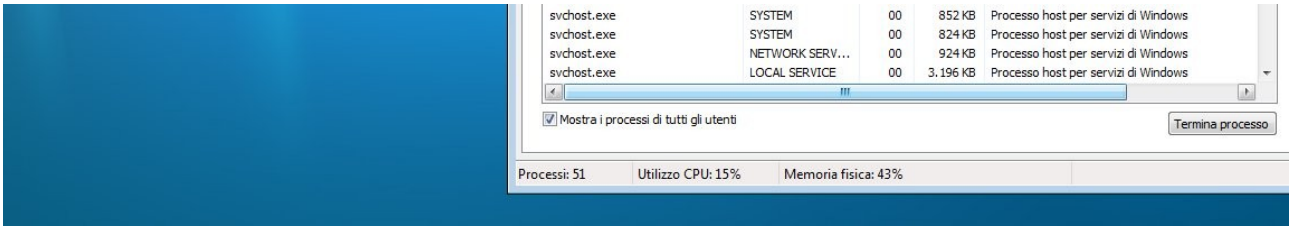


siamo diventati SYSTEM

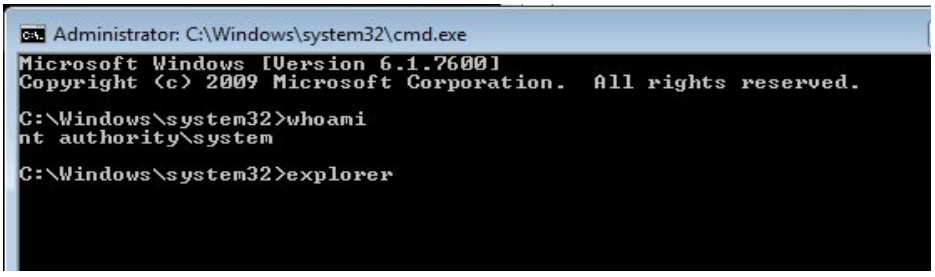
a questo punto se terminiamo il processo “explorer” che appartiene all'utente “augusto”

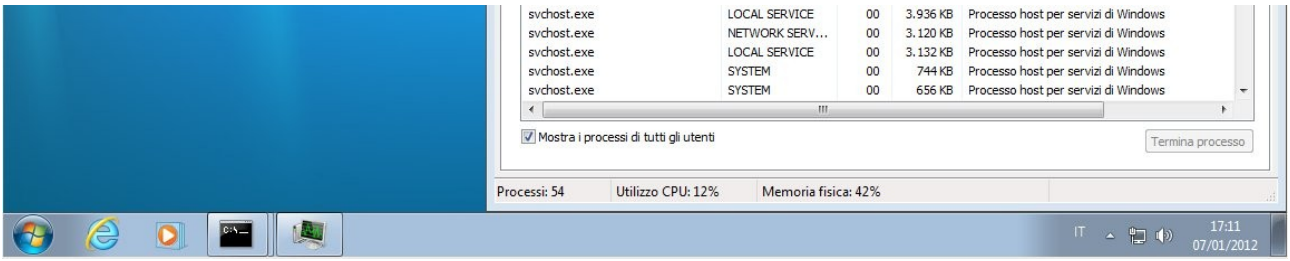


scompare completamente il desktop dell'utente “augusto”

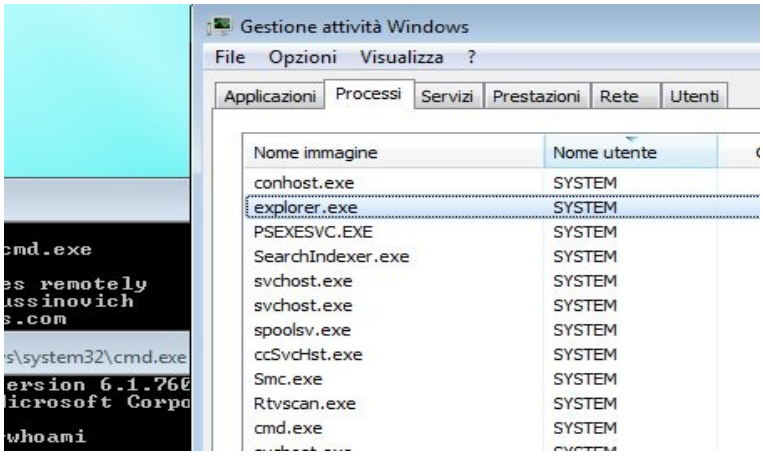


se nella nuova finestra DOS digitiamo “explorer” si aprirà il nuovo desktop dell'utente SYSTEM

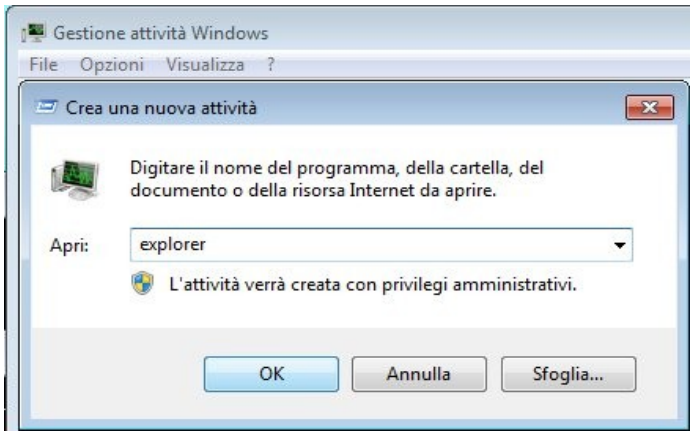


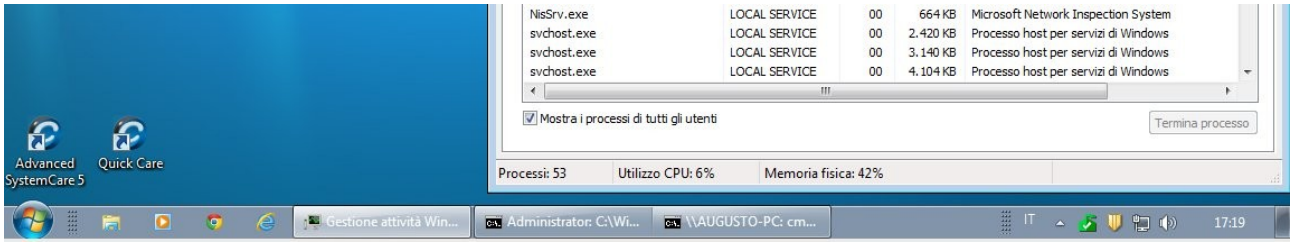


infatti il processo “explorer” ora risulta avviato dall'utente “SYSTEM”



per tornare indietro all'utente “augusto” si deve killare il processo explorer (avviato da SYSTEM) e successivamente creare una nuova attività di nome explorer





Siamo tornati al punto di partenza.

~~~~~~

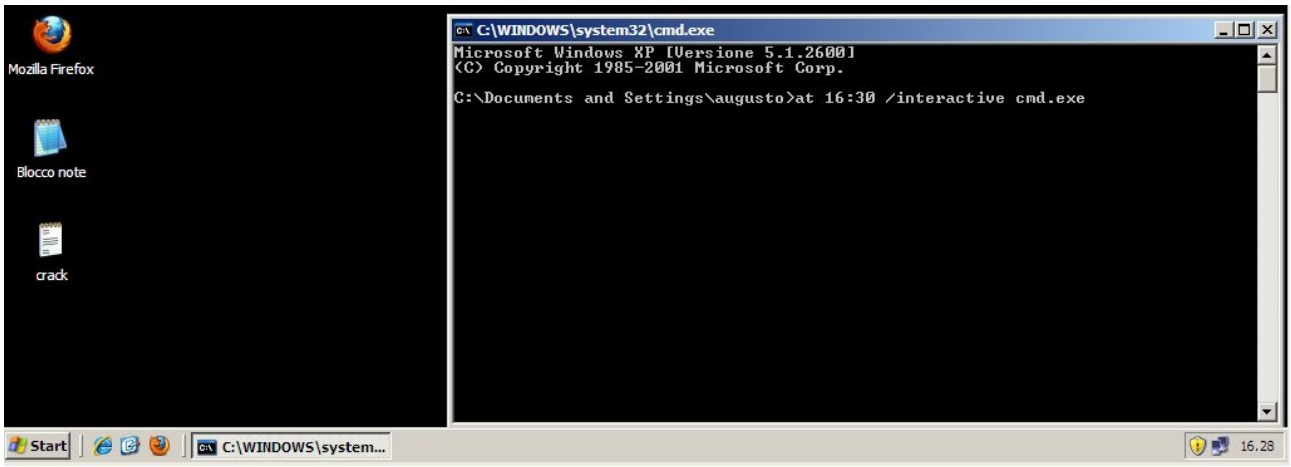
~~~~~~

E su Windows XP come si può fare?

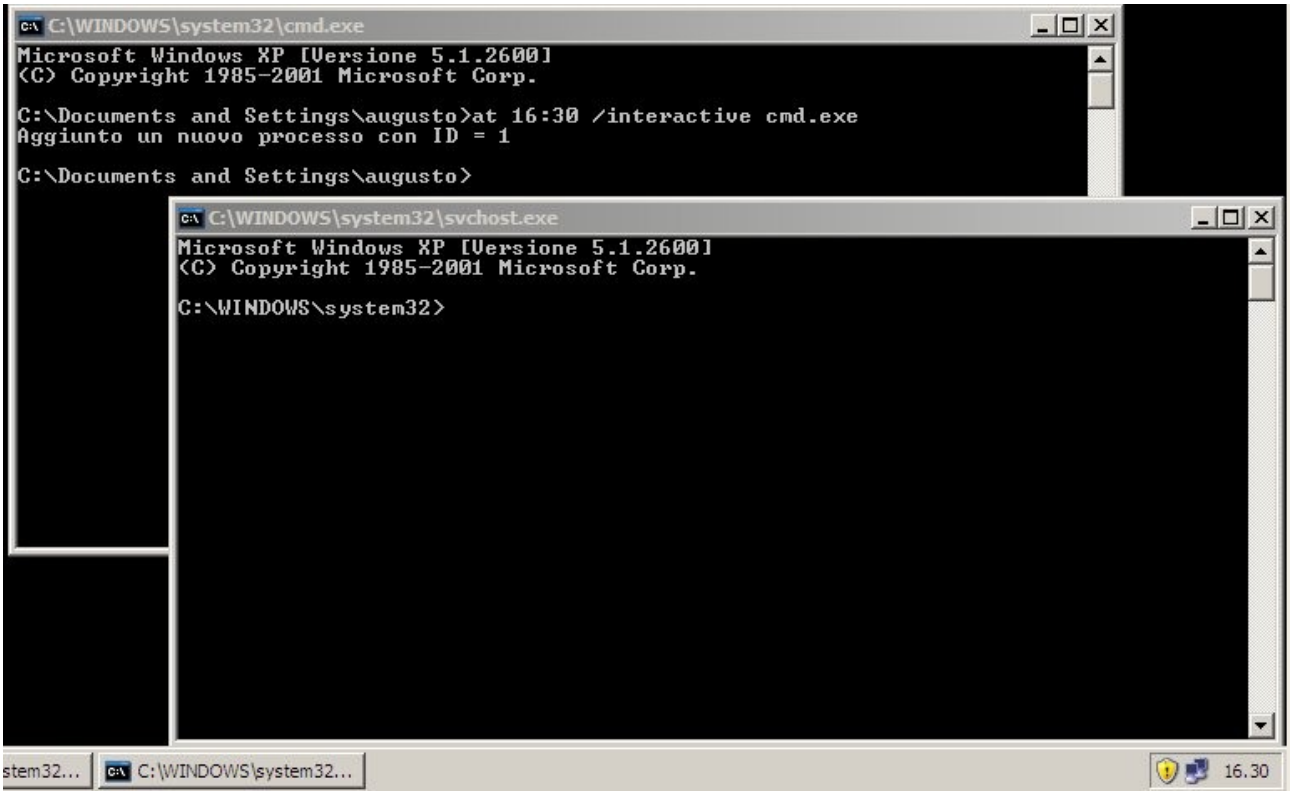
Supponiamo di avere un account su Windows XP PRO sp3 di nome augusto che fa parte del gruppo degli amministratori.

Eseguiamo il login come augusto,

controlliamo l'orologio del sistema, (in questo caso 16:28) apriamo una finestra DOS e digitiamo "at 16:30 /interactive cmd.exe" avendo cura di inserire un orario di 1 o 2 minuti posteriore all'ora del sistema



alle 16:30 (orario in formato militare) si aprirà una seconda finestra DOS



ma a differenza dalla prima, sulla cornice della finestra appare "svchost" e ci troviamo dentro la cartella C:\windows\system32

siamo diventati SYSTEM (il comando whoami su XP non funziona).

Il resto è analogo a quanto mostrato per Windows 7.

a chiusura

Gli utenti comuni di Windows 7 forse non lo sanno, ma esiste un account chiamato Super-Amministratore, o Super-Admin, che ha maggiori privilegi del normale gruppo di amministratori e di default è non solo disattivato, ma anche accuratamente tenuto nascosto. Questo account, a differenza degli altri, ha pieni diritti sul computer ma sempre meno dell'utente SYSTEM.

Nelle precedenti versioni a Windows 7 e Vista, l'account Amministratore non era nascosto e molti utenti lo usavano come account principale. Questo tipo di utente ha i pieni diritti sul computer. In Windows 7 e Vista invece non è così, perché l'account di Amministratore è soggetto all'UAC (User Account Control), un sistema introdotto con questo nuovo OS e pensato per proteggere gli utenti meno esperti. Il Super-Amministratore può effettuare qualsiasi tipo di modifica al sistema e non è soggetto all'UAC.

Per abilitare l'utente Administrator su Windows 7 cliccare sul menù start e digitare secpol.msc nella barra di ricerca. Premete invio, si aprirà il Local Security Policy;

- *Navigate in Local Policies-> Security Options. Cercate la voce Accounts: Administrator account;*
- Fate doppio click *sulla* voce per attivare o disattivare l'account amministratore.
- *Riavviare la macchina.*

L'utente SYTEM è l'account virtuale sotto cui girano tutti i processi di sistema, ha i privilegi più alti all'interno del sistema, più dell'Administrator, in quanto è responsabile dei processi fondamentali di sistema e dei servizi. Se volete fare disperatamente qualcosa e vi viene dato Accesso negato state sicuri che lui può farlo…

L'utente System su windows è colui che tutto può, un vero SuperUtente. Come root.

FINE

altre miniguide su
http://www.comunecampagnano.it/gnu/miniguide.htm
oppure direttamente su http://miniguide.tk

sito consigliato: http://www.linux4campagnano.net
blog consigliato: http://campagnanorap.blogspot.com