

User, Poweruser, Administrator e SYSTEM (Root per GNU/Linux, SYSTEM per Windows)

Augusto Scatolini (webmaster@comunecampagnano.it) (a.scatolini@linux4campagnano.net)
Miniguia 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 agosto,



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.

Tipo: Applicazione
Percorso: System32
Destinazione: C:\Windows\System32\taskmgr.exe
Da: C:\Windows\System32

Nome immagine	Nome utente	CPU	Memori...	Descrizione
ASCSvc.exe	SYSTEM	00	304 KB	Advanced SystemCare Service
ASCTray.exe	augusto	00	3.392 KB	Advanced SystemCare 5 Tray
audiodg.exe	LOCAL SERVICE	00	6.300 KB	Isolamento grafico dispositivo audio Windows
ccApp.exe	augusto	00	976 KB	Symantec User Session
ccSvcHst.exe	SYSTEM	02	4.476 KB	Symantec Service Framework
csrss.exe	SYSTEM	01	964 KB	Processo runtime client server
csrss.exe	SYSTEM	00	948 KB	Processo runtime client server
dwm.exe	augusto	00	648 KB	Gestione finestre desktop
explorer.exe	augusto	01	11.168 KB	Esplora risorse
GrooveMonitor.exe	augusto	00	960 KB	GrooveMonitor Utility
jusched.exe	augusto	00	444 KB	Java(TM) Update Scheduler
lsass.exe	SYSTEM	02	2.652 KB	Local Security Authority Process
lsm.exe	SYSTEM	00	660 KB	Servizio Gestione sessioni locali
mscorsvw.exe	SYSTEM	00	3.088 KB	.NET Runtime Optimization Service
mscorsvw.exe	SYSTEM	32	3.728 KB	.NET Runtime Optimization Service
MpEng.exe	SYSTEM	00	42.668 KB	Antimalware Service Executable
mssecexe.exe	augusto	00	2.980 KB	Microsoft Security Client User Interface
NisSrv.exe	LOCAL SERVICE	00	1.040 KB	Microsoft Network Inspection System
Processo di inattività del sistema	SYSTEM	43	12 KB	Percentuale di tempo di inattività del processore
reader_sl.exe	augusto	00	532 KB	Adobe Acrobat SpeedLauncher
Rtvscan.exe	SYSTEM	02	1.836 KB	Symantec AntiVirus
SearchFilterHost.exe	SYSTEM	00	736 KB	Microsoft Windows Search Filter Host
SearchIndexer.exe	SYSTEM	01	4.576 KB	Microsoft Windows Search Indexer
SearchProtocolHost.exe	SYSTEM	01	1.364 KB	Microsoft Windows Search Protocol Host
services.exe	SYSTEM	00	2.856 KB	Applicazione Servizi e Controller
Smc.exe	SYSTEM	01	4.052 KB	Symantec CMC Smc
SmcGui.exe	augusto	00	1.948 KB	Symantec CMC SmcGui
smss.exe	SYSTEM	00	168 KB	Gestione sessioni di Windows
snmp.exe	SYSTEM	00	1.432 KB	Servizio SNMP
spoolsv.exe	SYSTEM	00	2.768 KB	Applicazione sottosistema spooler
spssvc.exe	NETWORK SERV...	00	1.268 KB	Servizio piattaforma protezione software Microsof
svchost.exe	LOCAL SERVICE	00	3.460 KB	Processo host per servizi di Windows
svchost.exe	SYSTEM	00	1.816 KB	Processo host per servizi di Windows
svchost.exe	NETWORK SERV...	00	2.608 KB	Processo host per servizi di Windows
svchost.exe	LOCAL SERVICE	00	6.844 KB	Processo host per servizi di Windows

Mostra i processi di tutti gli utenti Termina processo

Processi: 57 Utilizzo CPU: 52% Memoria fisica: 67%

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.

```
augusto@ubuntu-new: ~
File Modifica Visualizza Terminale Aiuto
top - 16:21:03 up 1:03, 2 users, load average: 0.71, 0.94, 1.06
Tasks: 186 total, 2 running, 184 sleeping, 0 stopped, 0 zombie
Cpu(s): 3.6%us, 9.3%sy, 0.2%ni, 87.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 4115452k total, 4078908k used, 36544k free, 736856k buffers
Swap: 9936160k total, 0k used, 9936160k free, 1805888k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 1837 agosto    20   0 1290m 1.1g 1.1g  S   17  28.3   31:23.35 VirtualBox
 2651 agosto    20   0 76944 24m  19m  S    5   0.6   0:00.52 ksnapshot
 1072 root       20   0 87432 19m 9896  D    3   0.5   1:42.32 Xorg
 2148 agosto    20   0  160m 41m  19m  S    1   1.0   0:28.50 chrome
   59 root       20   0    0    0    0   R    0   0.0   0:01.36 kondemand/1
 1621 agosto    20   0  111m 28m 9176  S    0   0.7   0:21.98 compiz
 1989 agosto    20   0 275m 105m 63m  S    0   2.6   0:38.97 soffice.bin
 2556 agosto    20   0  2548 1256 924   R    0   0.0   0:02.72 top
   1 root       20   0  2800 1640 1168  S    0   0.0   0:00.38 init
   2 root       20   0    0    0    0   S    0   0.0   0:00.00 kthreadd
   3 root       20   0    0    0    0   S    0   0.0   0:00.00 migration/0
   4 root       20   0    0    0    0   S    0   0.0   0:02.23 ksoftirqd/0
   5 root       20   0    0    0    0   S    0   0.0   0:00.00 watchdog/0
   6 root       20   0    0    0    0   S    0   0.0   0:00.00 migration/1
   7 root       20   0    0    0    0   S    0   0.0   0:00.68 ksoftirqd/1
   8 root       20   0    0    0    0   S    0   0.0   0:00.00 watchdog/1
   9 root       20   0    0    0    0   S    0   0.0   0:00.02 events/0
  10 root       20   0    0    0    0   S    0   0.0   0:00.04 events/1
  11 root       20   0    0    0    0   S    0   0.0   0:00.00 cpuset
  12 root       20   0    0    0    0   S    0   0.0   0:00.00 khelper
  13 root       20   0    0    0    0   S    0   0.0   0:00.00 async/mgr
  14 root       20   0    0    0    0   S    0   0.0   0:00.00 pm
  16 root       20   0    0    0    0   S    0   0.0   0:00.00 sync_supers
  17 root       20   0    0    0    0   S    0   0.0   0:00.00 bdi-default
  18 root       20   0    0    0    0   S    0   0.0   0:00.00 kintegrityd/0
  19 root       20   0    0    0    0   S    0   0.0   0:00.00 kintegrityd/1
  20 root       20   0    0    0    0   S    0   0.0   0:00.06 kblockd/0
  21 root       20   0    0    0    0   S    0   0.0   0:00.02 kblockd/1
  22 root       20   0    0    0    0   S    0   0.0   0:00.00 kacpid
  23 root       20   0    0    0    0   S    0   0.0   0:00.00 kacpi_notify
  24 root       20   0    0    0    0   S    0   0.0   0:00.00 kacpi_hotplug
  25 root       20   0    0    0    0   S    0   0.0   0:00.71 ata/0
  26 root       20   0    0    0    0   S    0   0.0   0:00.57 ata/1
  27 root       20   0    0    0    0   S    0   0.0   0:00.00 ata_aux
```

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.

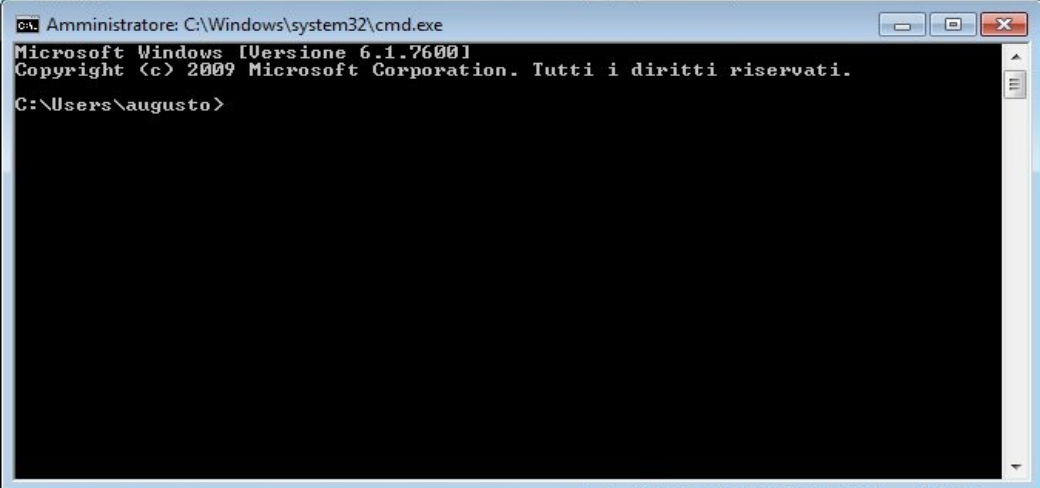
Il mondo Windows, come è ben risaputo, è molto meno democratico dei sistemi Unix-like nel senso che all'utente "augusto" (benché facente parte del gruppo degli amministratori della macchina) non solo viene impedito di accedere al sistema come "Administrator" perché questo utente è addirittura disabilitato (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 `sysinternals` che è stata acquistata proprio da **Microsoft**.

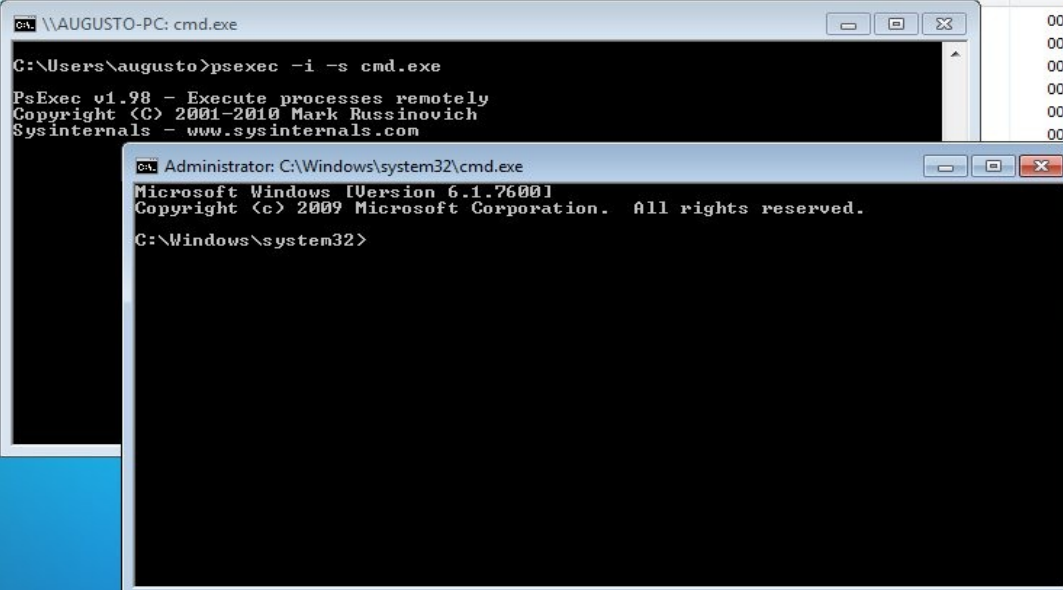
Si copia il programma dentro `C:\windows\system32\` per poterlo eseguire da qualunque posizione.



```
Amministratore: C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\augusto>
```

Si lancia il comando `cmd`

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



```
\\AUGUSTO-PC: cmd.exe
C:\Users\augusto>psexec -i -s cmd.exe
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Amministratore: C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

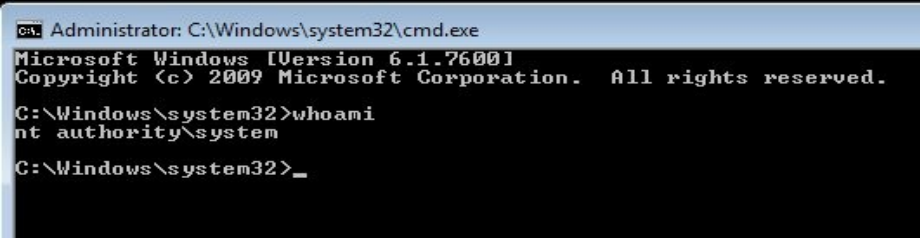
si apre immediatamente una seconda finestra DOS

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

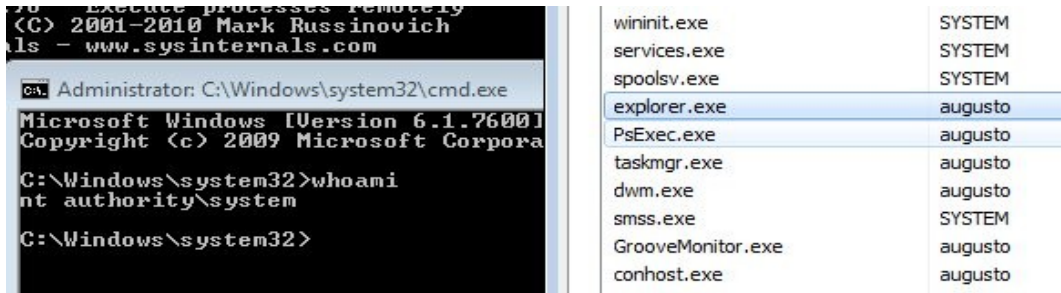
“`nt authority\system`”

siamo diventati SYSTEM

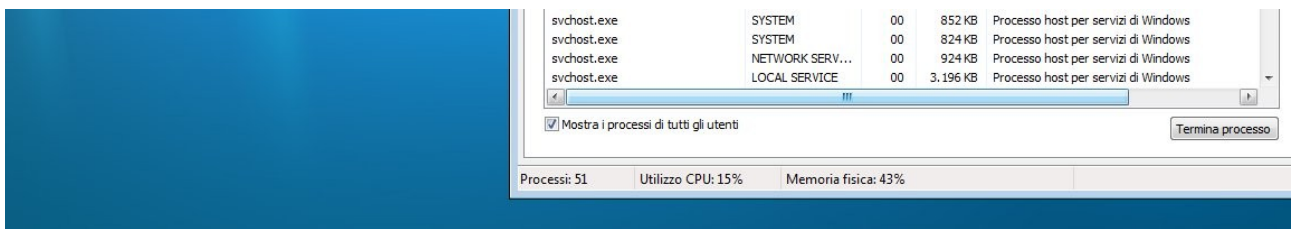


```
Amministratore: C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>_
```

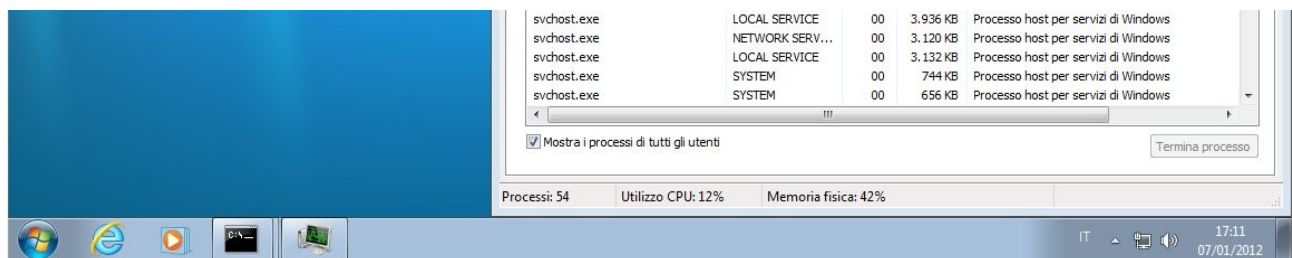
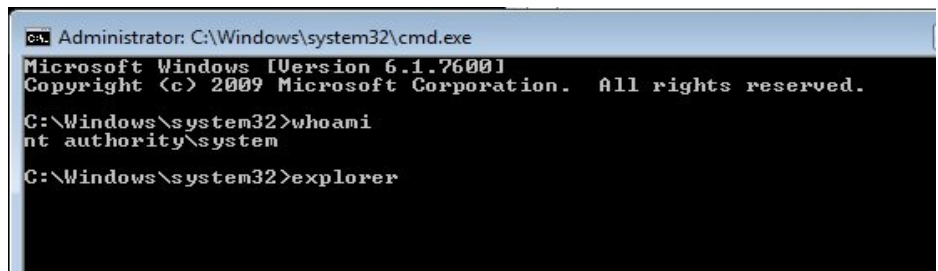
a questo punto se terminiamo il processo “explorer” che appartiene all'utente “augusto”



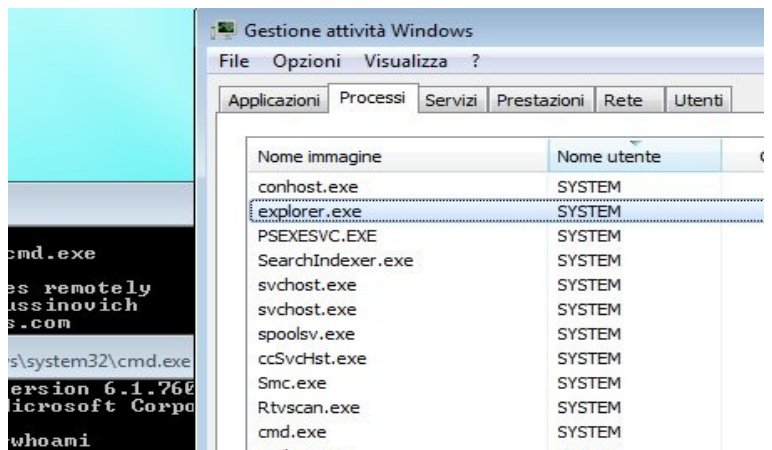
scompare completamente il desktop dell'utente “augusto”



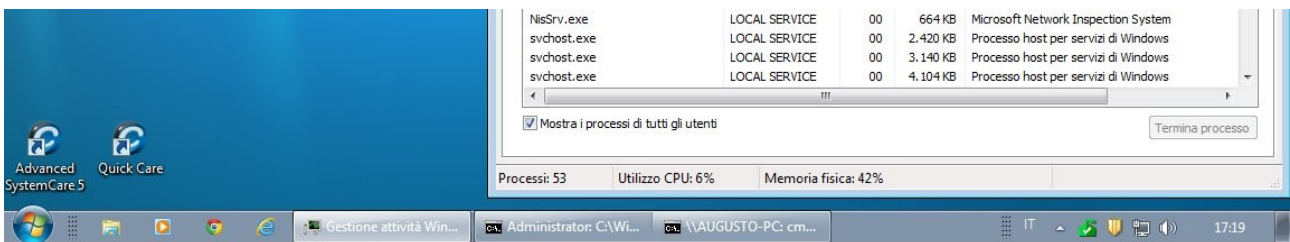
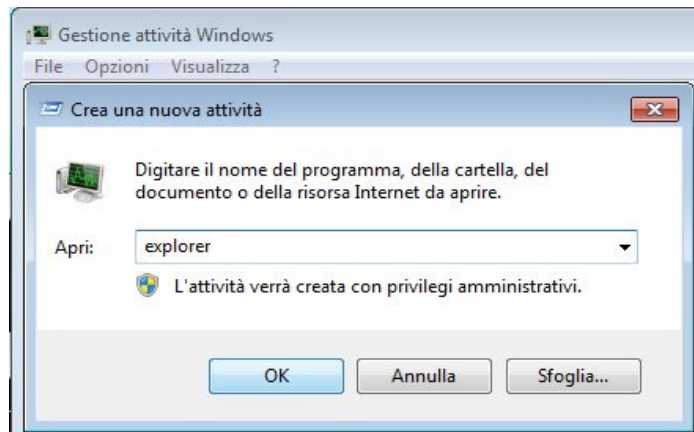
se nella nuova finestra DOS digitiamo “explorer” si aprirà il nuovo desktop dell'utente SYSTEM



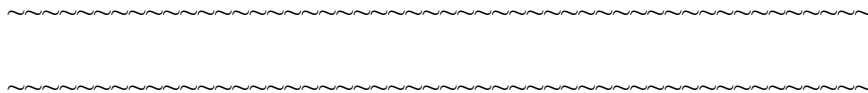
infatti il processo “explorer” ora risulta avviato dall'utente “SYSTEM”



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.



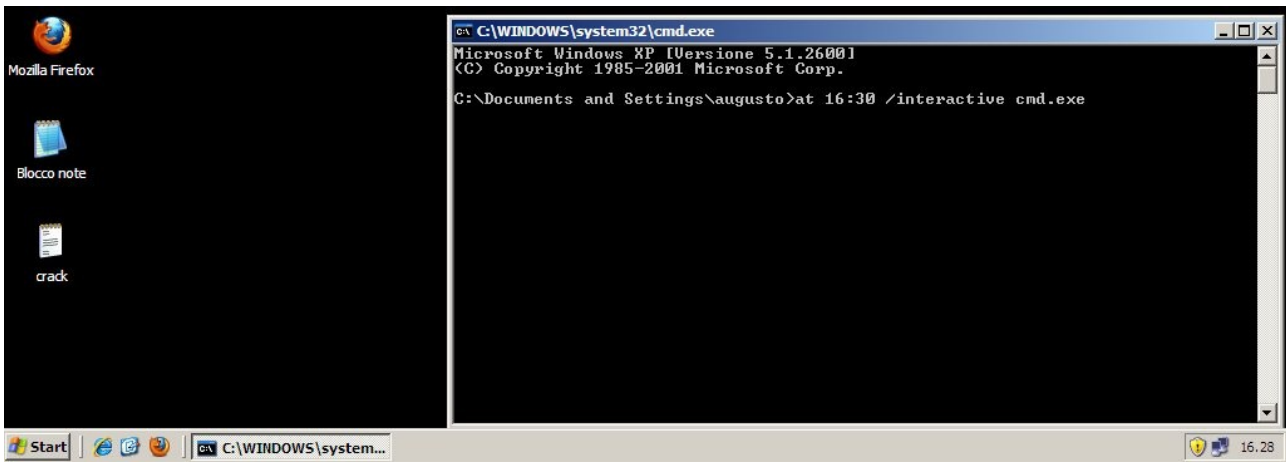
E su Windows XP come si può fare?

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

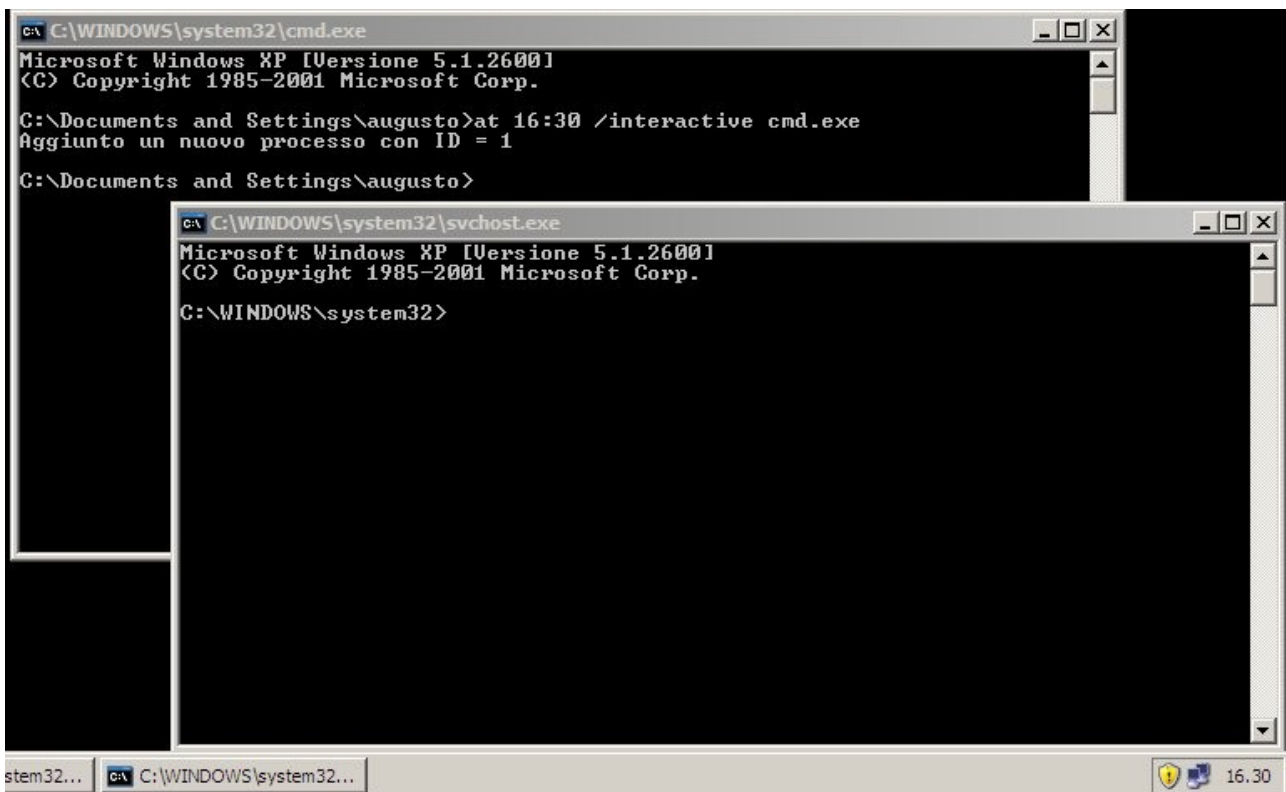
Eseguiamo il login come agosto,



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-Administratore, 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

Questo documento è rilasciato con licenza Copyleft
(tutti i rovesci sono riservati)

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>