

NETSTAT

PROJECT BY:

JON BENETT AUSTRIA

JAMES DYLON JOSE

CHE COS'È?

- E' un comando utilizzato su Windows e Linux, per visualizzare lo stato delle connessioni instaurate sul computer locale.



QUAL È IL SUO SCOPO?

Restituire le informazioni
complete sulle connessioni
del nostro sistema come:

- Statistiche dell'interfacce;
 - Tabella di routing;
 - Maschera di connessione;
 - Elenco delle connessioni in ascolto o attive.
-

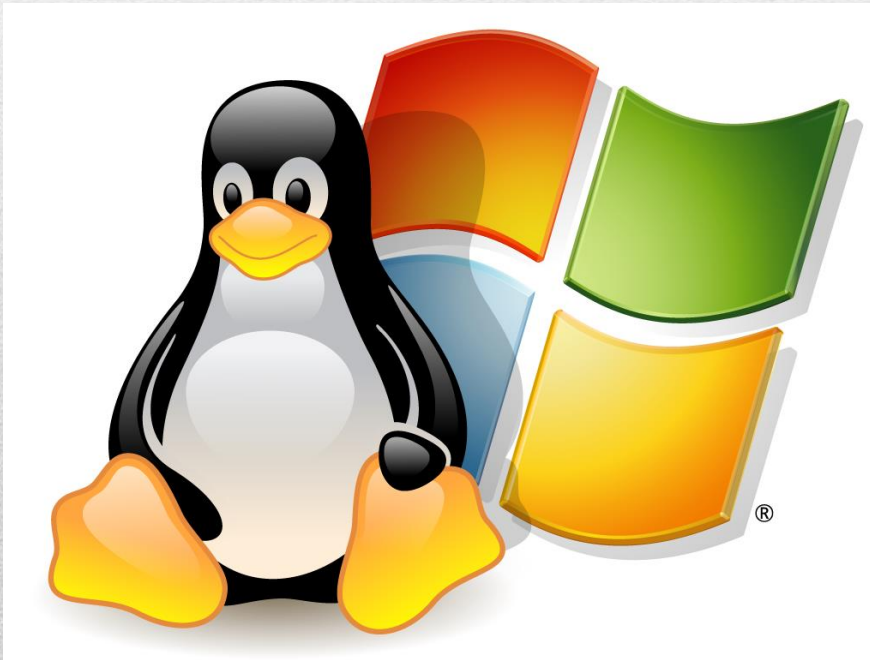
PROGRAMMI PER ESEGUIRE NETSTAT

LINUX

- Terminale

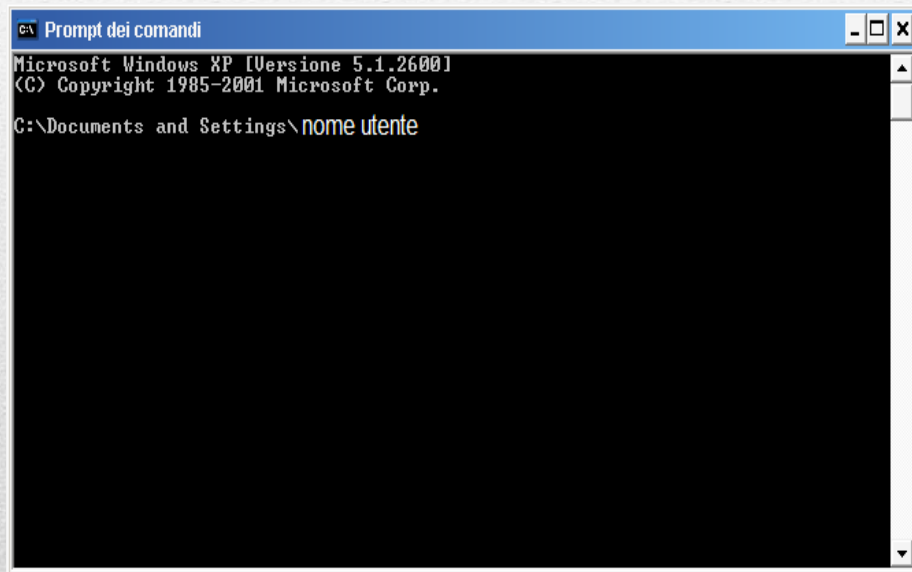
WINDOWS

- Prompt dei comandi
- Powershell



WINDOWS

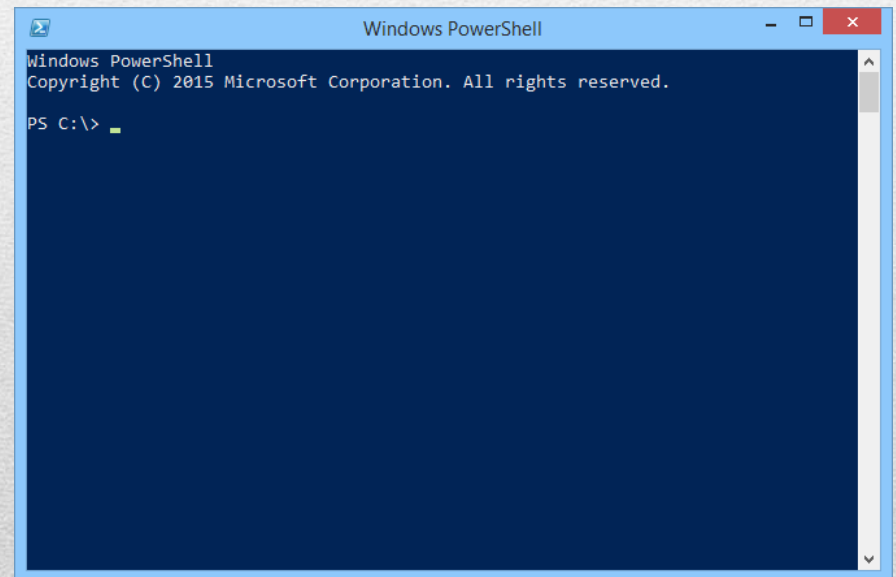
PROMPT DEI COMANDI



A screenshot of the Windows Command Prompt window. The title bar is blue and reads "Prompt dei comandi". The window has a black background with white text. The text displayed is: "Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\nome utente". The cursor is at the end of the last line.

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\nome utente
```

POWERSHELL



A screenshot of the Windows PowerShell window. The title bar is blue and reads "Windows PowerShell". The window has a dark blue background with white text. The text displayed is: "Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS C:\>". The cursor is at the end of the last line.

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
PS C:\>
```

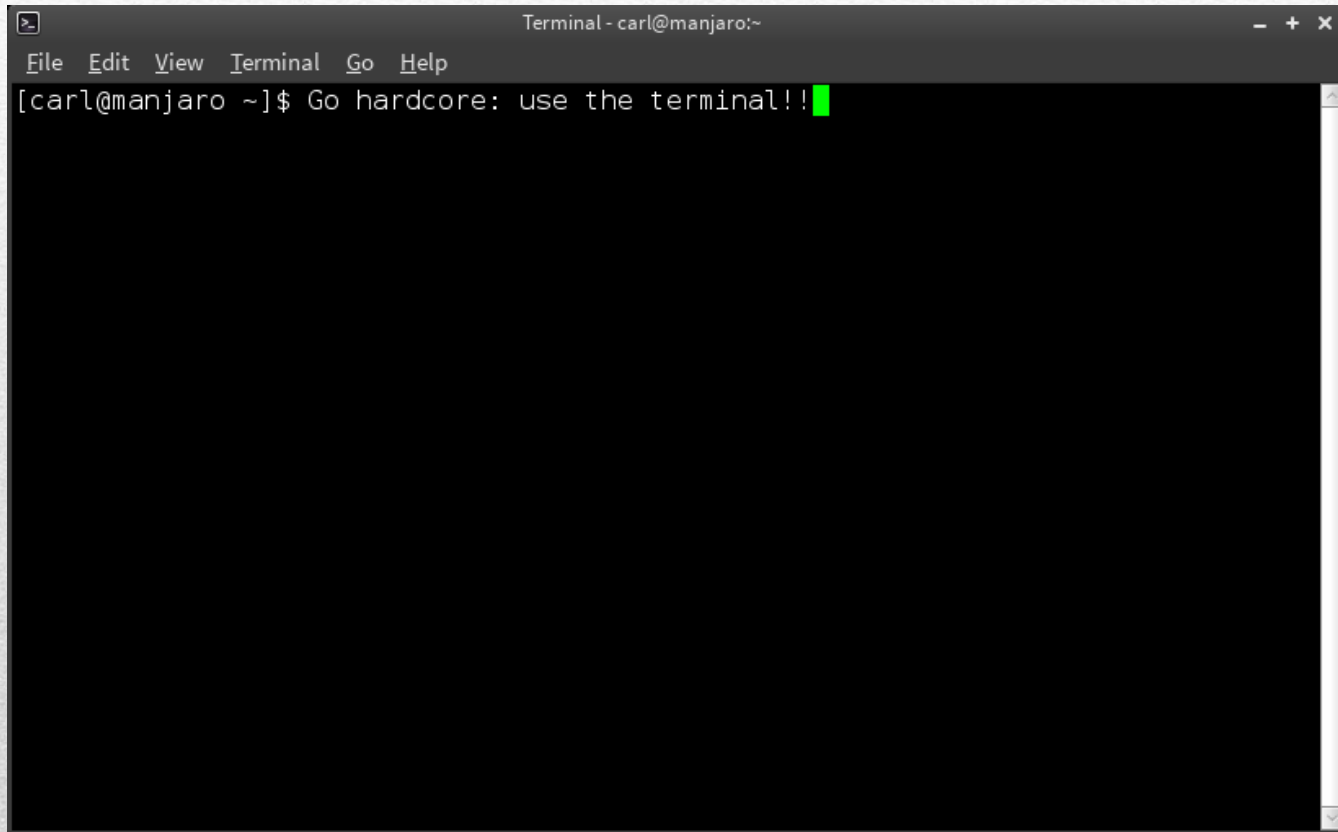

PROMPT DEI COMANDI

- Digitare il comando *cmd/prompt dei comandi* nel menù *Start/Esegui* e confermando con *Invio*, comparirà la schermata nera del DOS.
-

POWERSHELL

- Digitare *powershell* nel menù *Start/Esegui* e confermare con *Invio*.
-

LINUX



```
Terminal - carl@manjaro:~  
File Edit View Terminal Go Help  
[carl@manjaro ~]$ Go hardcore: use the terminal!!
```

A screenshot of a Linux terminal window. The window title is "Terminal - carl@manjaro:~". The menu bar includes "File", "Edit", "View", "Terminal", "Go", and "Help". The terminal content shows a prompt "[carl@manjaro ~]" followed by the command "Go hardcore: use the terminal!!" and a green cursor. The terminal background is black.

TERMINALE

- Scegliere *Applicazioni* → *Accessori* → *Terminale*;
 - Premere *Alt+F2* e digitare *gnome-terminal*.
-

COMANDI

- Digitando su *Prompt dei comandi/PowerShell/Terminale*

NETSTAT -(OPZIONE)

compariranno maggiori e precise informazioni.

COMANDI PIÙ UTILIZZATI

- `/?` Mostra i dettagli sulle varie opzioni del comando.

```
Visualizza statistiche relative ai protocolli e alle
connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a          Visualizza tutte le connessioni e le porte di ascolto.
-b          Visualizza il file eseguibile utilizzato per la creazione
           di ogni connessione o porta di ascolto. Alcuni file
           eseguibili conosciuti includono più componenti indipendenti.
           In tali casi viene visualizzata la sequenza dei componenti
           utilizzati per la creazione della connessione o porta di
           ascolto e il nome del file eseguibile viene visualizzato
           in fondo, tra parentesi quadre ([]). Nella parte superiore
           è indicato il componente chiamato e così via, fino al
           raggiungimento di TCP/IP. Se si utilizza questa opzione,
           l'esecuzione del comando può richiedere molto tempo e
           riuscirà solo se si dispone di autorizzazioni sufficienti.
-e          Visualizza le statistiche Ethernet. Può essere utilizzata
           insieme all'opzione -s.
-f          Visualizza i nomi di dominio completi (FQDN, Fully Qualified
           Domain Name) per gli indirizzi esterni.
-n          Visualizza indirizzi e numeri di porta in forma numerica.
-o          Visualizza l'ID del processo proprietario associato a ogni
           connessione.
-p proto    Visualizza le connessioni relative al protocollo specificato
           da "proto", che può essere TCP, UDP, TCPv6 o UDPv6.
           Se utilizzato insieme all'opzione -s per le statistiche per
           protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP,
           TCPv6, UDP o UDPv6.
-q          Visualizza tutte le connessioni, le porte di ascolto e le porte
           TCP non di ascolto associate. Le porte non di ascolto associate
           possono essere associate o meno a una connessione attiva.
-r          Visualizza la tabella di routing.
-s          Visualizza le statistiche per protocollo. Per impostazione
           predefinita, vengono visualizzate le statistiche per IP,
           IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare
           un sottoinsieme dei valori predefiniti, è possibile
           utilizzare l'opzione -p.
-t          Visualizza lo stato di offload della connessione corrente.
-x          Visualizza le connessioni, i listener e gli endpoint
           condivisi.
-y          Visualizza il modello di connessione TCP per tutte le
           connessioni. Non può essere utilizzata in combinazione con le
           altre opzioni.
interval    Ripete la visualizzazione delle statistiche selezionate,
           con una pausa di un numero di secondi pari a "interval"
           dopo ogni visualizzazione. Per interrompere la ripetizione
           della visualizzazione delle statistiche, premere CTRL+C.
           Se questa opzione viene omissa, le informazioni di
           configurazione correnti verranno visualizzate una volta sola.
```


- **-a** La lista di tutte le porte upd e tcp attive e in ascolto sul sistema;

Netstat -opzione(+flag)

- **-at** Solo la lista delle porte TCP;
 - **-an** Tutte le connessioni in formato numerico.
-

- Aggiungendo al comando precedente l'opzione *-p* è possibile specificare il protocollo(TCP,UDP..)

netstat -a -p tcp

netstat -a -p udp

- *-l* Solo la lista delle connessioni in ascolto (listening);
 - *-s* Completa descrizione delle statistiche;
 - *-o* PID(Identificatore di processo) che controlla ciascuna connessione.
-

- *-r* Tabella di routing IP;
 - *-e* Statistiche Ethernet;
 - *-n* Gli indirizzi e le porte in forma di indirizzo IP.
-

- *-p* Le connessioni o le statistiche solo per un particolare protocollo(max 1);
Può essere eseguito senza definire un protocollo.

Esempi di Protocolli:

- TCP;
 - UDP;
 - TCPv6 o IDPv6.
-

PROTOCOLLI INTERNET

- *-t* Stato dei socket TCP(Transfer Control Protocol);
- *-u* Stato dei socket UDP(User Datagram Protocol).

UDP è un protocollo di trasporto di Internet non orientato alla connessione e non confermato.(Non affidabile);

TCP è un protocollo di trasporto e si occupa di rendere affidabile la comunicazione dati in rete tra mittente e destinatario(Affidabile).

COME INTERPRETARE LE CONNESSIONI DI RETE

- CLOSE;
- ESTABLISHED;
- FIN_WAIT_1;
- LISTENING;
- SYN_SEND;
- TIME_WAIT.

```
C:\Program Files>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:4105	0.0.0.0:0	LISTENING
TCP	0.0.0.0:4728	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7163	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54674	0.0.0.0:0	LISTENING
TCP	0.0.0.0:57634	0.0.0.0:0	LISTENING
TCP	127.0.0.1:4105	127.0.0.1:54475	ESTABLISHED
TCP	127.0.0.1:4105	127.0.0.1:54525	ESTABLISHED
TCP	127.0.0.1:4105	127.0.0.1:54672	ESTABLISHED
TCP	127.0.0.1:4105	127.0.0.1:54673	ESTABLISHED
TCP	127.0.0.1:4105	127.0.0.1:54675	ESTABLISHED
TCP	127.0.0.1:4105	127.0.0.1:54676	ESTABLISHED

COME SCORPIRE SE IL COMPUTER HA UN VIRUS O SPIATO

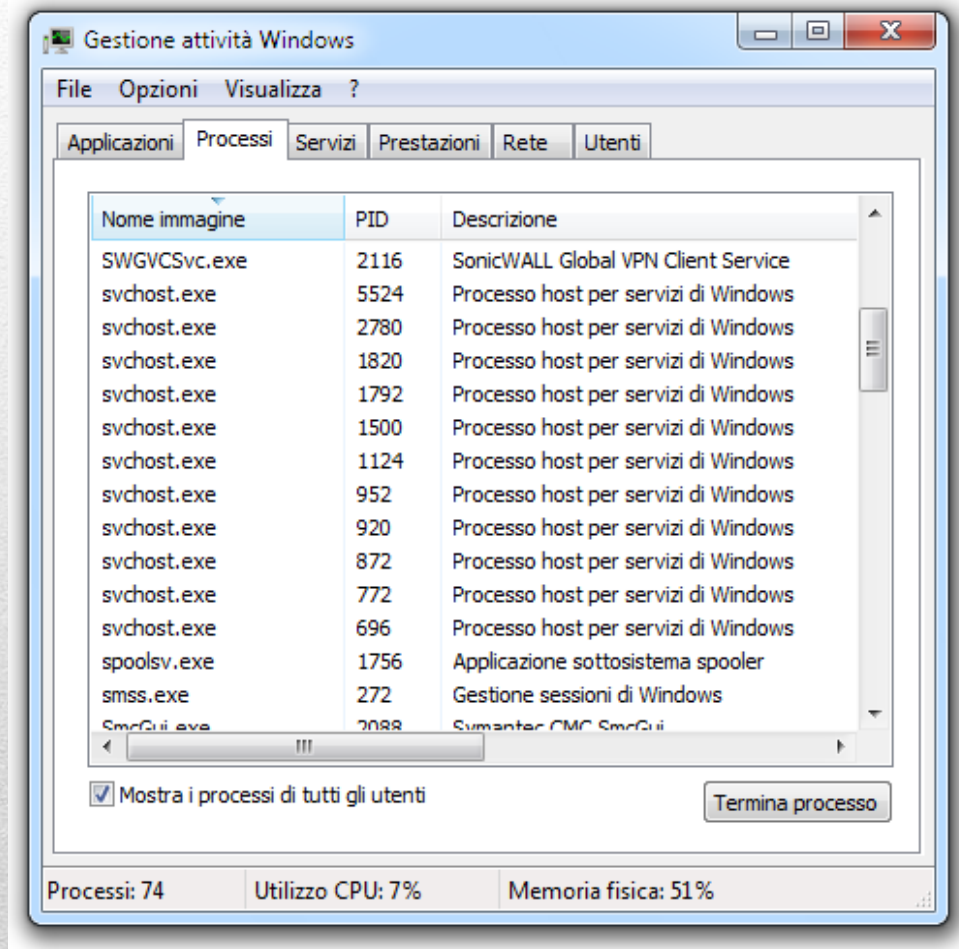
- <https://www.youtube.com/watch?v=tvLz09a1hlo>

```
C:\>netstat -ano
Active Connections

```

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	912
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:990	0.0.0.0:0	LISTENING	744
TCP	0.0.0.0:1039	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	1256
TCP	0.0.0.0:1503	0.0.0.0:0	LISTENING	3332
TCP	0.0.0.0:1720	0.0.0.0:0	LISTENING	3332
TCP	0.0.0.0:2492	0.0.0.0:0	LISTENING	3784
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	4412
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	864
TCP	0.0.0.0:5022	0.0.0.0:0	LISTENING	1256
TCP	0.0.0.0:8083	0.0.0.0:0	LISTENING	1384
TCP	0.0.0.0:8093	0.0.0.0:0	LISTENING	1288
TCP	127.0.0.1:1074	0.0.0.0:0	LISTENING	3024
TCP	127.0.0.1:1180	127.0.0.1:1181	ESTABLISHED	2652
TCP	127.0.0.1:1181	127.0.0.1:1180	ESTABLISHED	2652
TCP	127.0.0.1:1198	127.0.0.1:1199	ESTABLISHED	2652
TCP	127.0.0.1:1199	127.0.0.1:1198	ESTABLISHED	2652
TCP	127.0.0.1:1434	0.0.0.0:0	LISTENING	1256
TCP	127.0.0.1:3253	127.0.0.1:8093	TIME_WAIT	0
TCP	127.0.0.1:3315	127.0.0.1:8093	ESTABLISHED	1384
TCP	127.0.0.1:5679	0.0.0.0:0	LISTENING	3248
TCP	127.0.0.1:7438	0.0.0.0:0	LISTENING	3248
TCP	127.0.0.1:8093	127.0.0.1:3315	ESTABLISHED	1288
TCP	127.0.0.1:9080	0.0.0.0:0	LISTENING	3784

GESTIONE ATTIVITA



JON BENETT

AUSTRIA



JAMES DYLAN

JOSE

