DISCOVERING SU SISTEMA OPERATIVO LINUX

Informazioni di Sistema:

- Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64 GNU/Linux

File System:

- Filesystem Inodes IUsed IFree IUse% Mounted on
- udev 241099 393 240706 1% /dev
- tmpfs 251508 635 250873 1% /run
- /dev/sda1 5251072 464351 4786721 9% /
- tmpfs 251508 1 251507 1% /dev/shm
- tmpfs 251508 2 251506 1% /run/lock
- tmpfs 50301 116 50185 1% /run/user/1000

Risorse di rete:

- eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
- inet 192.168.1.67 netmask 255.255.255.0 broadcast 192.168.1.255
- inet6 fe80::a00:27ff:fecb:7ef5 prefixlen 64 scopeid 0x20<link>
- ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
- RX packets 78667 bytes 4784140 (4.5 MiB)
- RX errors 0 dropped 0 overruns 0 frame 0
- TX packets 63 bytes 7910 (7.7 KiB)
- TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
-
- lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
- inet 127.0.0.1 netmask 255.0.0.0
- inet6 ::1 prefixlen 128 scopeid 0x10<host>
- loop txqueuelen 1000 (Local Loopback)
- RX packets 31 bytes 4160 (4.0 KiB)
- RX errors 0 dropped 0 overruns 0 frame 0
- TX packets 31 bytes 4160 (4.0 KiB)
- TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Utenti e Autorizzazioni:

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:107:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
lightdm:x:110:116:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:111:118::/var/lib/saned:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false
stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:119:127::/var/lib/snmp:/bin/false
sslh:x:120:128::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin
redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin
iodine:x:125:65534::/run/iodine:/usr/sbin/nologin
miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
```

Visualizzare processi in esecuzione:

```
┌──(kali㉿kali)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  21160 12628 ?        Ss   Dec18   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    Dec18   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Dec18   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Dec18   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Dec18   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Dec18   0:00 [netns]
root          11  0.0  0.0      0     0 ?        I<   Dec18   0:00 [mm_percpu_wq]
root          12  0.0  0.0      0     0 ?        I    Dec18   0:00 [rcu_tasks_kthread]
root          13  0.0  0.0      0     0 ?        I    Dec18   0:00 [rcu_tasks_rude_kthread]
root          14  0.0  0.0      0     0 ?        I    Dec18   0:00 [rcu_tasks_trace_kthread]
root          15  0.0  0.0      0     0 ?        S    Dec18   0:03 [ksoftirqd/0]
root          16  0.0  0.0      0     0 ?        I    Dec18   0:16 [rcu_preempt]
root          17  0.0  0.0      0     0 ?        S    Dec18   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    Dec18   0:00 [idle_inject/0]
root          19  0.0  0.0      0     0 ?        S    Dec18   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    Dec18   0:00 [cpuhp/1]
root          21  0.0  0.0      0     0 ?        S    Dec18   0:00 [idle_inject/1]
root          22  0.0  0.0      0     0 ?        S    Dec18   0:01 [migration/1]
root          23  0.0  0.0      0     0 ?        S    Dec18   0:04 [ksoftirqd/1]
root          28  0.0  0.0      0     0 ?        S    Dec18   0:00 [kdevtmpfs]
root          29  0.0  0.0      0     0 ?        I<   Dec18   0:00 [inet_frag_wq]
root          30  0.0  0.0      0     0 ?        S    Dec18   0:00 [kauditd]
root          31  0.0  0.0      0     0 ?        S    Dec18   0:00 [khungtaskd]
root          32  0.0  0.0      0     0 ?        S    Dec18   0:00 [oom_reaper]
root          34  0.0  0.0      0     0 ?        I<   Dec18   0:00 [writeback]
root          35  0.0  0.0      0     0 ?        S    Dec18   0:01 [kcompactd0]
root          36  0.0  0.0      0     0 ?        SN   Dec18   0:00 [ksmd]
root          37  0.0  0.0      0     0 ?        SN   Dec18   0:02 [khugepaged]
root          38  0.0  0.0      0     0 ?        I<   Dec18   0:00 [kintegrityd]
root          39  0.0  0.0      0     0 ?        I<   Dec18   0:00 [kblockd]
root          40  0.0  0.0      0     0 ?        I<   Dec18   0:00 [blkcg_punt_bio]
root          41  0.0  0.0      0     0 ?        I<   Dec18   0:00 [tpm_dev_wq]
root          42  0.0  0.0      0     0 ?        I<   Dec18   0:00 [edac-poller]
root          43  0.0  0.0      0     0 ?        I<   Dec18   0:00 [devfreq_wq]
root          45  0.0  0.0      0     0 ?        S    Dec18   0:00 [kswapd0]
root          52  0.0  0.0      0     0 ?        I<   Dec18   0:00 [kthrotld]
root          54  0.0  0.0      0     0 ?        I<   Dec18   0:00 [acpi_thermal_pm]
```

```
root          65  0.0  0.0      0     0 ?        I<   Dec18   0:00 [kworker/u5:0]
root         130  0.0  0.0      0     0 ?        I<   Dec18   0:00 [cryptd]
root         132  0.0  0.0      0     0 ?        I<   Dec18   0:00 [ata_sff]
root         134  0.0  0.0      0     0 ?        S    Dec18   0:00 [scsi_eh_0]
root         135  0.0  0.0      0     0 ?        S    Dec18   0:00 [irq/18-vmwgfx]
root         136  0.0  0.0      0     0 ?        S    Dec18   0:00 [scsi_eh_1]
root         137  0.0  0.0      0     0 ?        I<   Dec18   0:00 [scsi_tmf_1]
root         138  0.0  0.0      0     0 ?        I<   Dec18   0:00 [scsi_tmf_0]
root         140  0.0  0.0      0     0 ?        S    Dec18   0:00 [scsi_eh_2]
root         141  0.0  0.0      0     0 ?        I<   Dec18   0:00 [ttm]
root         142  0.0  0.0      0     0 ?        I<   Dec18   0:00 [scsi_tmf_2]
root         230  0.0  0.0      0     0 ?        S    Dec18   0:00 [jbd2/sda1-8]
root         231  0.0  0.0      0     0 ?        I<   Dec18   0:00 [ext4-rsv-conver]
root         385  0.0  0.2   8264  5088 ?        Ss   Dec18   0:01 /usr/sbin/haveged --Foreground --verbose=1
root         414  0.0  0.4 310880  9564 ?        Ssl  Dec18   0:00 /usr/libexec/accounts-daemon
message+     415  0.0  0.2  10780  5888 ?        Ss   Dec18   0:04 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
polkitd      420  0.0  0.5 384424 10348 ?        Ssl  Dec18   0:01 /usr/lib/polkit-1/polkitd --no-debug
root         452  0.0  1.0 333024 21468 ?        Ssl  Dec18   0:00 /usr/sbin/NetworkManager --no-daemon
root         473  0.0  0.7 392132 14360 ?        Ssl  Dec18   0:00 /usr/sbin/ModemManager
root         477  0.0  0.0      0     0 ?        I<   Dec18   0:00 [rpciod]
root         478  0.0  0.0      0     0 ?        I<   Dec18   0:00 [xprtiod]
root         482  0.0  0.1   6636  2560 ?        Ss   Dec18   0:00 /usr/sbin/cron -f
root         520  0.0  0.1 358540  3332 ?        Sl   Dec18   0:07 /usr/sbin/VBoxService
root         576  0.0  0.1   5880  3328 ?        Ss   Dec18   0:00 dhclient -4 -v -i -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
root         664  0.0  0.4 382308  9028 ?        SLsl Dec18   0:00 /usr/sbin/lightdm
root         675  0.1 10.0 474024 201644 tty7    Ssl+ Dec18   2:39 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
root         677  0.0  0.0   5896  1920 tty1     Ss+  Dec18   0:00 /sbin/agetty -o -p -- \u --noclear - linux
root         693  0.0  0.0      0     0 ?        S    Dec18   0:00 [psimon]
rtkit        721  0.0  0.1  88336  3200 ?        SNsl Dec18   0:01 /usr/libexec/rtkit-daemon
root         952  0.0  0.5 236228 10240 ?        Sl   Dec18   0:00 lightdm --session-child 13 24
kali         959  0.0  0.5  19816 11392 ?        Ss   Dec18   0:00 /lib/systemd/systemd --user
kali         960  0.0  0.2  22148  5288 ?        S    Dec18   0:00 (sd-pam)
kali         976  0.0  0.7 118748 14720 ?        Ssl  Dec18   0:00 /usr/bin/pipewire
kali         977  0.0  0.2  95212  5888 ?        Ssl  Dec18   0:00 /usr/bin/pipewire -c filter-chain.conf
kali         978  0.0  1.8 575604 36596 ?        Ssl  Dec18   0:00 /usr/bin/wireplumber
kali         979  0.0  0.4 101108  9344 ?        Ssl  Dec18   0:00 /usr/bin/pipewire-pulse
kali         981  0.0  0.2   9736  5244 ?        Ss   Dec18   0:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
kali         982  0.0  0.5 314268 11852 ?        SLsl Dec18   0:00 /usr/bin/gnome-keyring-daemon --foreground --components=pkcs11,secrets --control-directory=/run/user/1000/keyring
kali         999  0.0  1.3 341140 26632 ?        Ssl  Dec18   0:00 xfce4-session
kali        1052  0.0  0.0  19172  1536 ?        S    Dec18   0:00 /usr/bin/VBoxClient --clipboard
kali        1053  0.0  0.1 217360  3968 ?        Sl   Dec18   0:00 /usr/bin/VBoxClient --clipboard
kali        1067  0.0  0.0  19172  1536 ?        S    Dec18   0:00 /usr/bin/VBoxClient --seamless
kali        1069  0.0  0.1 217460  3200 ?        Sl   Dec18   0:22 /usr/bin/VBoxClient --seamless
kali        1075  0.0  0.0  19172  1664 ?        S    Dec18   0:00 /usr/bin/VBoxClient --draganddrop
kali        1076  0.0  0.1 217976  2944 ?        Sl   Dec18   2:00 /usr/bin/VBoxClient --draganddrop
kali        1088  0.0  0.0   7952  1908 ?        Ss   Dec18   0:00 /usr/bin/ssh-agent x-session-manager
kali        1098  0.0  0.5 385112 10064 ?        Ssl  Dec18   0:00 /usr/libexec/at-spi-bus-launcher
kali        1105  0.0  0.2   9384  4864 ?        S    Dec18   0:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 11 --address=unix:path=/run/user/1000/at-spi/bus_0
kali        1117  0.0  0.4 238376  9940 ?        Sl   Dec18   0:01 /usr/libexec/at-spi2-registryd --use-gnome-session
kali        1129  0.0  0.2  81264  5324 ?        SLs  Dec18   0:00 /usr/bin/gpg-agent --supervised
kali        1131  0.0  5.1 1026896 103944 ?      Sl   Dec18   1:18 xfwm4
kali        1135  0.0  0.4 311836  9716 ?        Ssl  Dec18   0:00 /usr/libexec/gvfsd
kali        1141  0.0  0.4 457272  9032 ?        Sl   Dec18   0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f
kali        1160  0.0  0.0  19172  1664 ?        S    Dec18   0:00 /usr/bin/VBoxClient --vmsvga
```