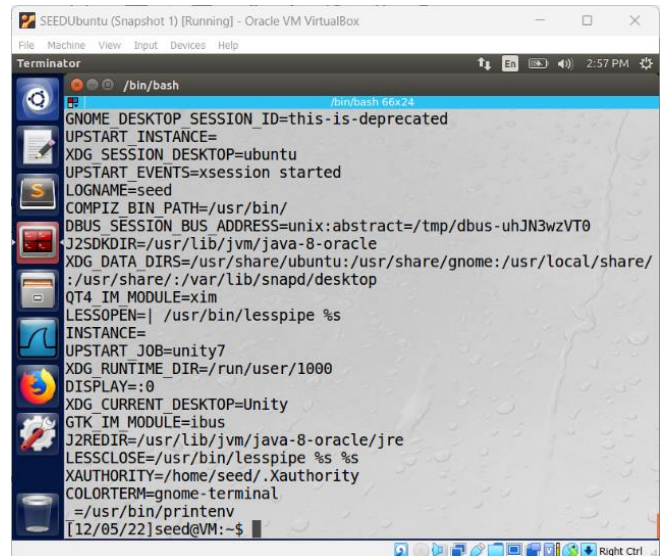


Laborator 7 – SI

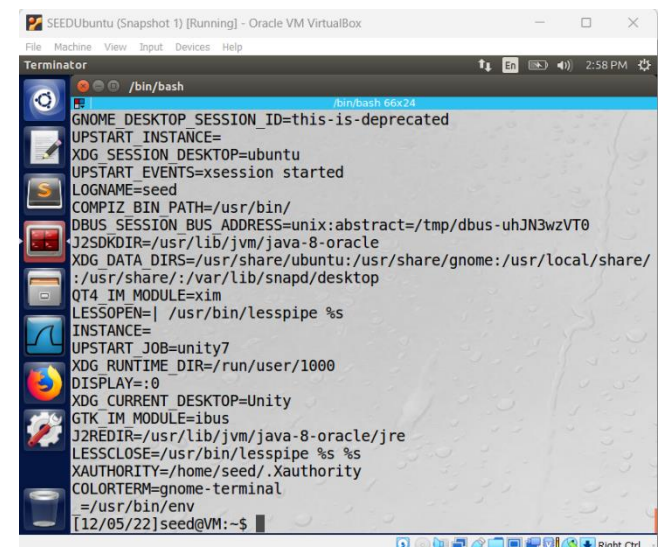
Task 1: Manipulating Environment Variables

printenv – afișează variabilele de mediu ale sistemului



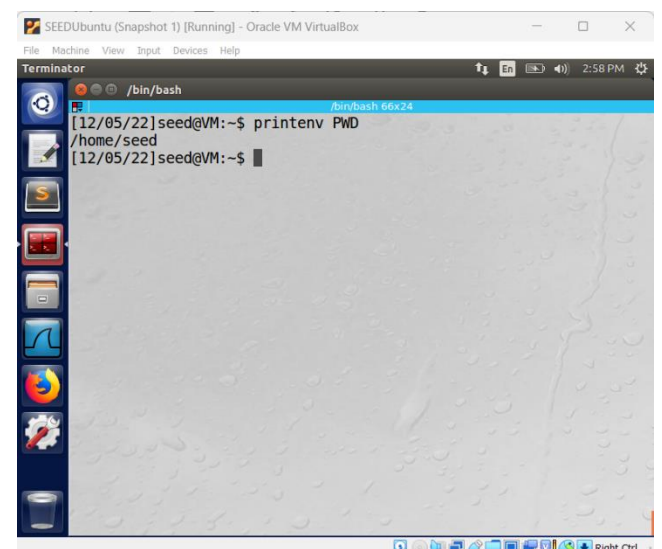
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-uhJN3wzVT0
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/flatpak/desktop
QT4_IM_MODULE=xim
LESSOPEN=| /usr/bin/lesspipe %s
INSTANCE=
UPSTART_JOB=unity7
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
XDG_CURRENT_DESKTOP=Unity
GTK_IM_MODULE=ibus
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
LESSCLOSE=/usr/bin/lesspipe %s %s
XAUTHORITY=/home/seed/.Xauthority
COLORTERM=gnome-terminal
=/usr/bin/printenv
[12/05/22]seed@VM:~$
```

env – afișează variabilele de mediu ale sistemului, rezultatul fiind la fel ca și comanda **printenv**



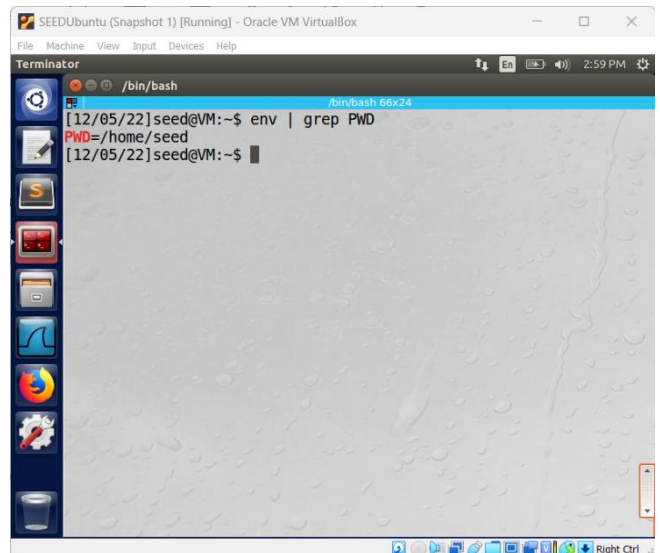
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-uhJN3wzVT0
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/flatpak/desktop
QT4_IM_MODULE=xim
LESSOPEN=| /usr/bin/lesspipe %s
INSTANCE=
UPSTART_JOB=unity7
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
XDG_CURRENT_DESKTOP=Unity
GTK_IM_MODULE=ibus
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
LESSCLOSE=/usr/bin/lesspipe %s %s
XAUTHORITY=/home/seed/.Xauthority
COLORTERM=gnome-terminal
=/usr/bin/env
[12/05/22]seed@VM:~$
```

printenv PWD – afișează valoarea variabilei de mediu PWD



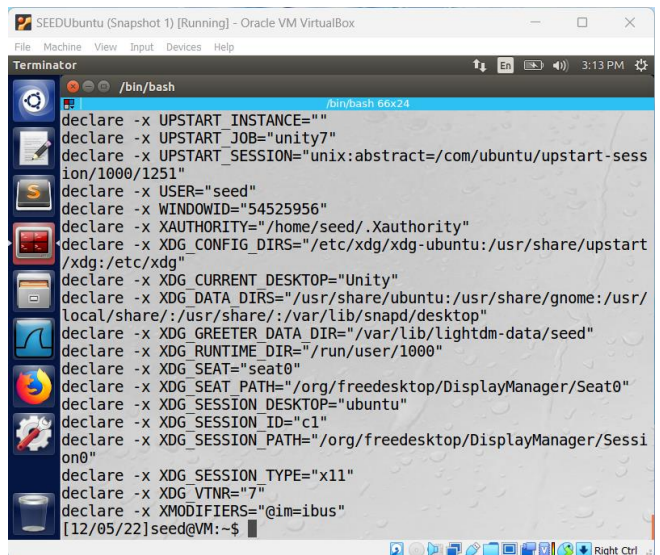
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~$ printenv PWD
/home/seed
[12/05/22]seed@VM:~$
```

env | grep PWD – afișează numele variabilei de mediu și valoarea sa



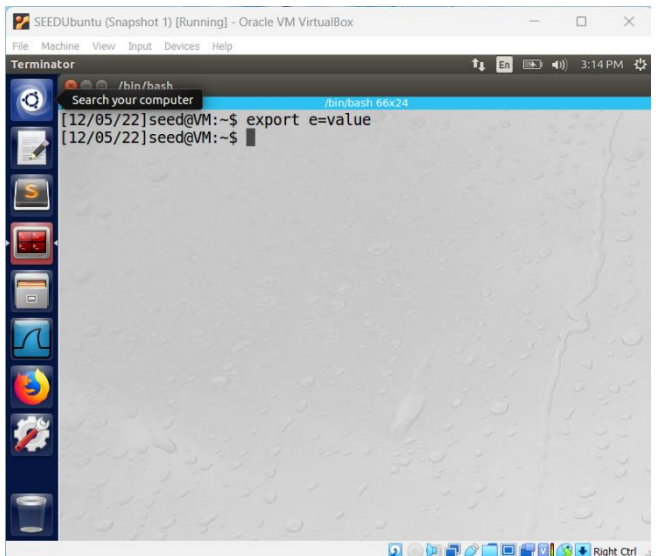
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[12/05/22] seed@VM:~$ env | grep PWD
PWD=/home/seed
[12/05/22] seed@VM:~$
```

export – afișează toate variabilele de mediu exportate



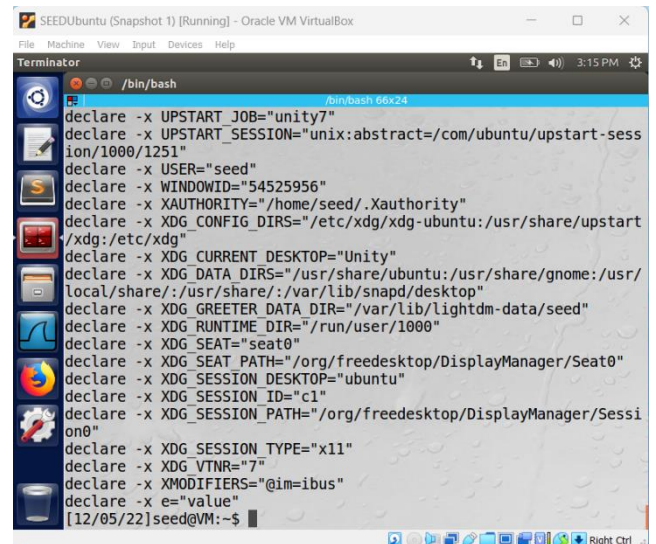
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
declare -x UPSTART_INSTANCE=""
declare -x UPSTART_JOB="unity7"
declare -x UPSTART_SESSION="unix:abstract=/com/ubuntu/upstart-session/1000/1251"
declare -x USER="seed"
declare -x WINDOWID="54525956"
declare -x XAUTHORITY="/home/seed/.Xauthority"
declare -x XDG_CONFIG_DIRS="/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
declare -x XDG_CURRENT_DESKTOP="Unity"
declare -x XDG_DATA_DIRS="/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/flatpak/desktop"
declare -x XDG_GREETER_DATA_DIR="/var/lib/lightdm-data/seed"
declare -x XDG_RUNTIME_DIR="/run/user/1000"
declare -x XDG_SEAT="seat0"
declare -x XDG_SEAT_PATH="/org/freedesktop/DisplayManager/Seat0"
declare -x XDG_SESSION_DESKTOP="ubuntu"
declare -x XDG_SESSION_ID="c1"
declare -x XDG_SESSION_PATH="/org/freedesktop/DisplayManager/Session0"
declare -x XDG_SESSION_TYPE="x11"
declare -x XDG_VTNR="7"
declare -x XMODIFIERS="@im=ibus"
[12/05/22] seed@VM:~$
```

export e=value – creează variabila de mediu **e** cu valoarea **value**



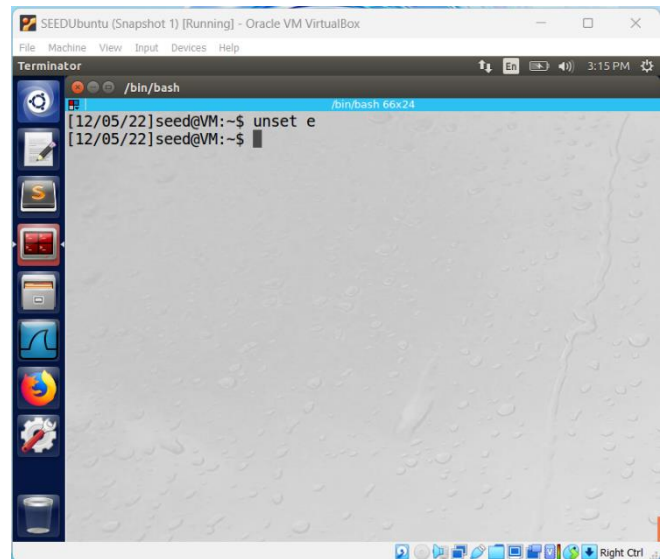
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[12/05/22] seed@VM:~$ export e=value
[12/05/22] seed@VM:~$
```

Afișarea variabilelor de mediu exportate după setarea unei variabile de mediu.



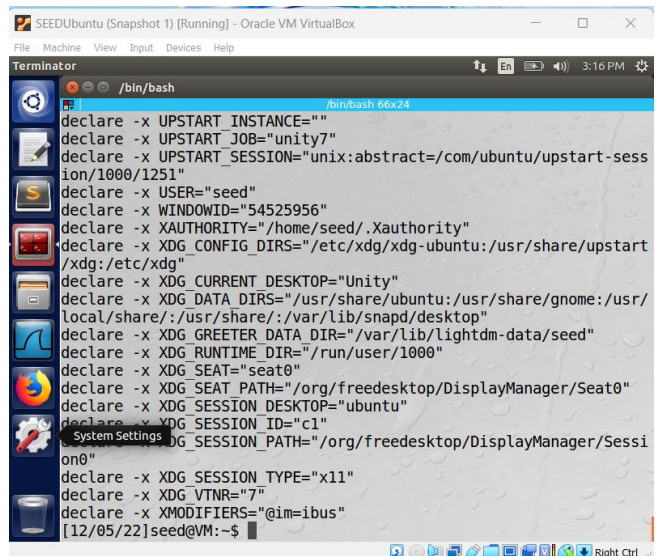
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
declare -x UPSTART_JOB="unity7"
declare -x UPSTART_SESSION="unix:abstract=/com/ubuntu/upstart-session/1000/1251"
declare -x USER="seed"
declare -x WINDOWID="54525956"
declare -x XAUTHORITY="/home/seed/.Xauthority"
declare -x XDG_CONFIG_DIRS="/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
declare -x XDG_CURRENT_DESKTOP="Unity"
declare -x XDG_DATA_DIRS="/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/snapd/desktop"
declare -x XDG_GREETER_DATA_DIR="/var/lib/lightdm-data/seed"
declare -x XDG_RUNTIME_DIR="/run/user/1000"
declare -x XDG_SEAT="seat0"
declare -x XDG_SEAT_PATH="/org/freedesktop/DisplayManager/Seat0"
declare -x XDG_SESSION_DESKTOP="ubuntu"
declare -x XDG_SESSION_ID="c1"
declare -x XDG_SESSION_PATH="/org/freedesktop/DisplayManager/Session0"
declare -x XDG_SESSION_TYPE="x11"
declare -x XDG_VTNR="7"
declare -x XMODIFIERS="@im=ibus"
declare -x e="value"
[12/05/22]seed@VM:~$
```

unset e – anulează variabila de mediu **e** creata



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~$ unset e
[12/05/22]seed@VM:~$
```

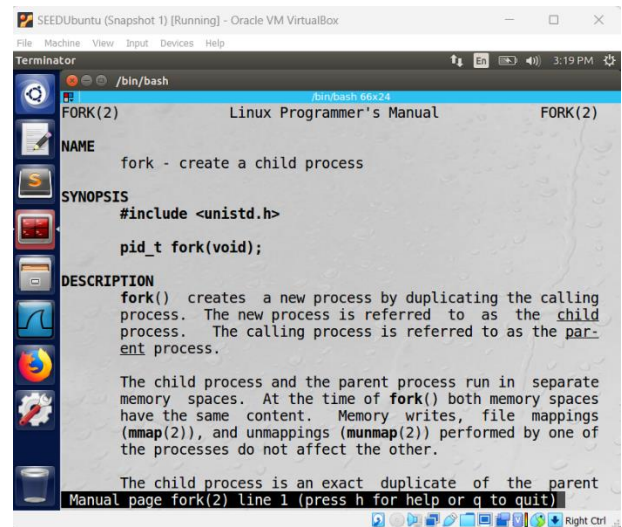
Afișarea variabilelor de mediu exportate după anularea unei variabile de mediu.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
declare -x UPSTART_INSTANCE=""
declare -x UPSTART_JOB="unity7"
declare -x UPSTART_SESSION="unix:abstract=/com/ubuntu/upstart-session/1000/1251"
declare -x USER="seed"
declare -x WINDOWID="54525956"
declare -x XAUTHORITY="/home/seed/.Xauthority"
declare -x XDG_CONFIG_DIRS="/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
declare -x XDG_CURRENT_DESKTOP="Unity"
declare -x XDG_DATA_DIRS="/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/snapd/desktop"
declare -x XDG_GREETER_DATA_DIR="/var/lib/lightdm-data/seed"
declare -x XDG_RUNTIME_DIR="/run/user/1000"
declare -x XDG_SEAT="seat0"
declare -x XDG_SEAT_PATH="/org/freedesktop/DisplayManager/Seat0"
declare -x XDG_SESSION_DESKTOP="ubuntu"
declare -x XDG_SESSION_ID="c1"
declare -x XDG_SESSION_PATH="/org/freedesktop/DisplayManager/Session0"
declare -x XDG_SESSION_TYPE="x11"
declare -x XDG_VTNR="7"
declare -x XMODIFIERS="@im=ibus"
[12/05/22]seed@VM:~$
```


Task 2: Passing Environment Variables from Parent Process to Child Process

man fork – afișează manualul funcției fork()

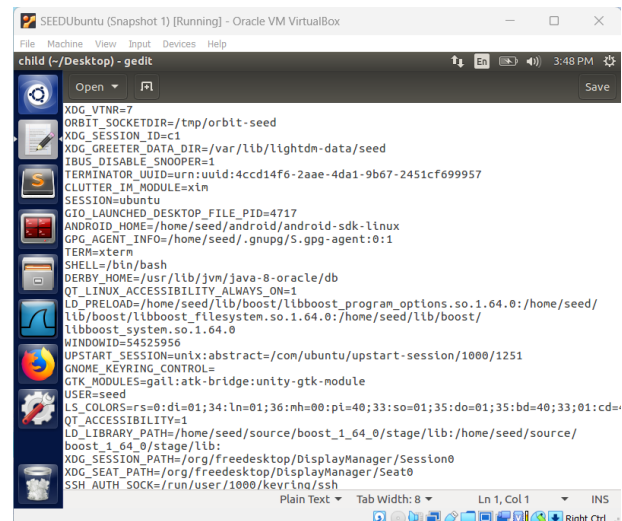


```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
fork(2) Linux Programmer's Manual FORK(2)
NAME
fork - create a child process
SYNOPSIS
#include <unistd.h>
pid_t fork(void);
DESCRIPTION
fork() creates a new process by duplicating the calling
process. The new process is referred to as the child
process. The calling process is referred to as the par-
ent process.
The child process and the parent process run in separate
memory spaces. At the time of fork() both memory spaces
have the same content. Memory writes, file mappings
(mmap(2)), and unmappings (munmap(2)) performed by one of
the processes do not affect the other.
The child process is an exact duplicate of the parent
Manual page fork(2) line 1 (press h for help or q to quit)

```

La compilarea și rularea exemplului, în fișierul **child** s-au afișat toate variabilele de mediu ale sistemului.

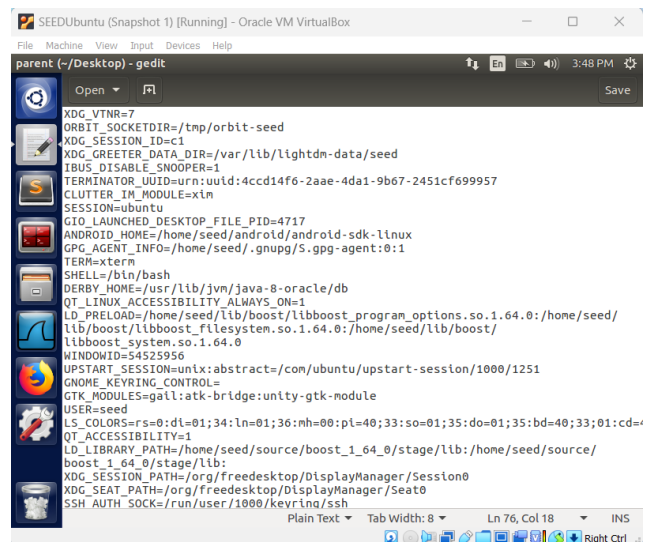


```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
child (~/Desktop) - gedit
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:4ccd14f6-2aae-4da1-9b67-2451cf699957
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=4717
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=54525956
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1251
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:nh=00:pi=40;33:so=01;35:bd=40;33:01:cd=
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/kevrino/ssh

```

La modificarea programului, compilarea și rularea exemplului, în fișierul **parent** s-au afișat toate variabilele de mediu ale sistemului, nesesizând nicio diferență.

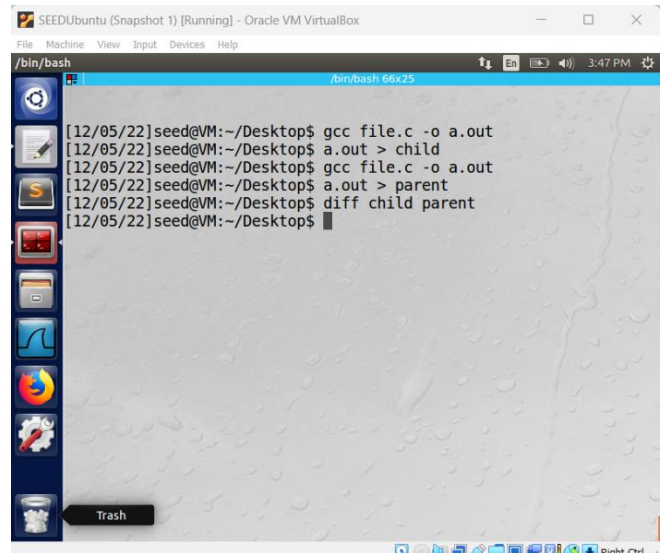


```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
parent (~/Desktop) - gedit
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:4ccd14f6-2aae-4da1-9b67-2451cf699957
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=4717
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=54525956
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1251
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:nh=00:pi=40;33:so=01;35:bd=40;33:01:cd=
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/kevrino/ssh

```

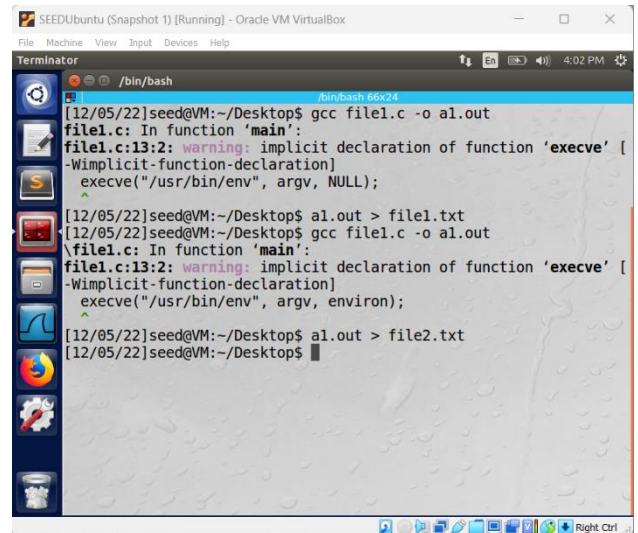
diff child parent – nu s-a afișat nicio diferență dintre cele 2 fișiere, ceea ce duce la concluzia că procesul părinte, cât și procesul copil au acces la aceleași variabile de mediu.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[12/05/22]seed@VM:~/Desktop$ gcc file.c -o a.out
[12/05/22]seed@VM:~/Desktop$ a.out > child
[12/05/22]seed@VM:~/Desktop$ gcc file.c -o a.out
[12/05/22]seed@VM:~/Desktop$ a.out > parent
[12/05/22]seed@VM:~/Desktop$ diff child parent
[12/05/22]seed@VM:~/Desktop$
```

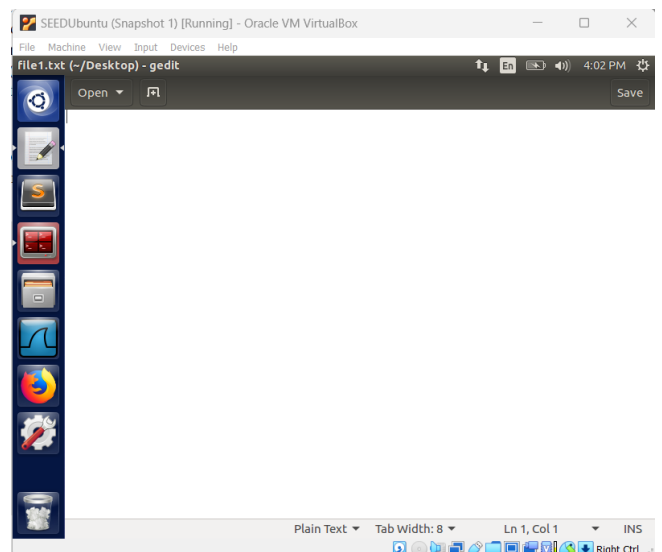
Task 3: Environment Variables and execve()

La compilarea programului a apărut o avertizare.



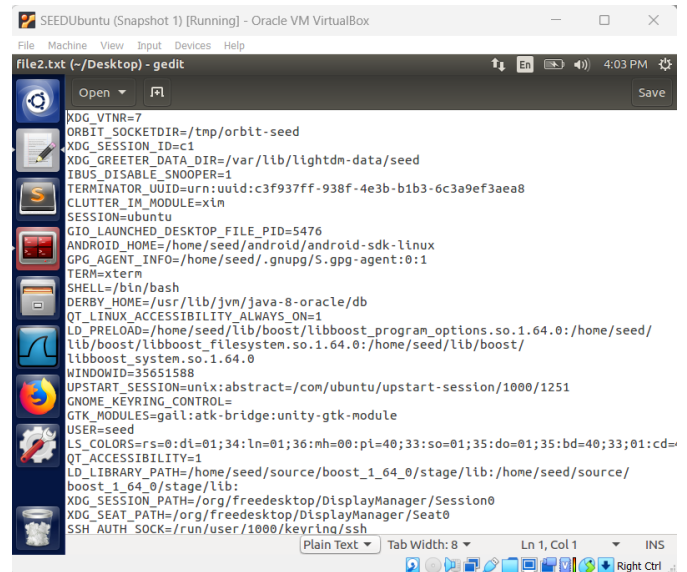
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[12/05/22]seed@VM:~/Desktop$ gcc file1.c -o a1.out
file1.c: In function 'main':
file1.c:13:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, NULL);
  ^
[12/05/22]seed@VM:~/Desktop$ a1.out > file1.txt
[12/05/22]seed@VM:~/Desktop$ gcc file1.c -o a1.out
file1.c: In function 'main':
file1.c:13:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, environ);
  ^
[12/05/22]seed@VM:~/Desktop$ a1.out > file2.txt
[12/05/22]seed@VM:~/Desktop$
```

La rularea programului nu s-a afișat nimic în fișier.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
file1.txt (~/.Desktop) - gedit
Open Save
Ln 1, Col 1 INS
```

La modificarea programului, s-a afișat în fișier toate variabilele de mediu, concluzionând faptul că la apelul de sistem când se rulează noul program, nu se moștenesc automat variabilele de mediu.

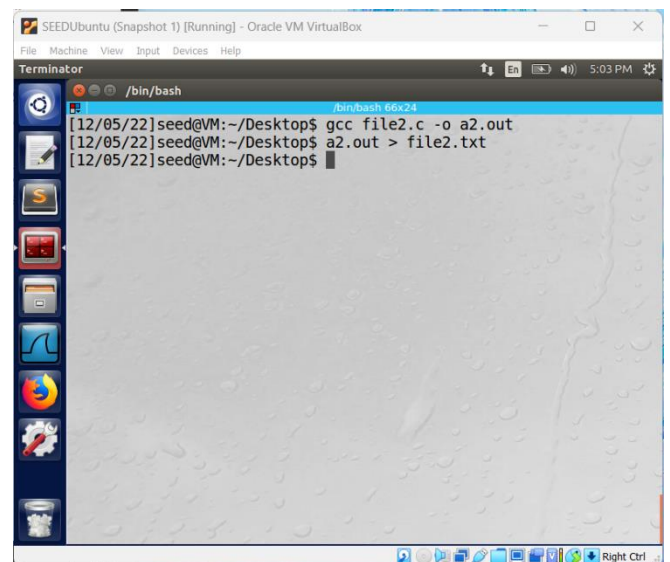


```

XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:c3f937ff-938f-4e3b-b1b3-6c3a9ef3aea8
CLUTTER_IM_MODULE=xln
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=5476
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=35651588
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1251
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:nh=00:pl=40;33:so=01;35:do=01;35:bd=40;33;01:cd=
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
  
```

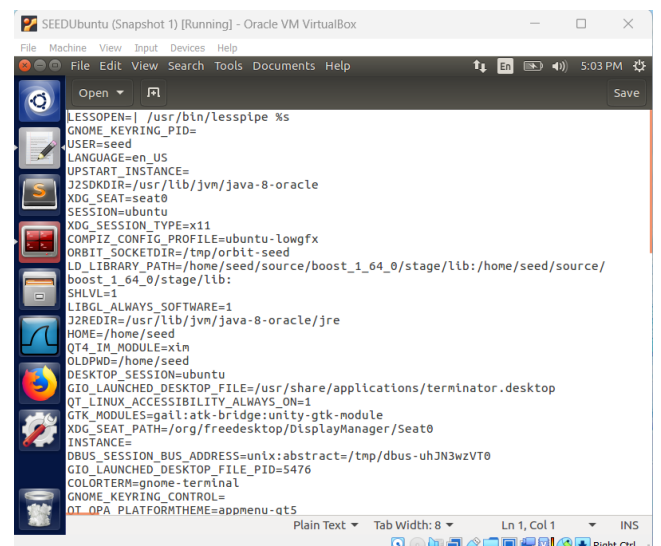
Task 4: Environment Variables and system()

La compilarea și rularea programului, se observă în fișierul de tip text pe prima linie că variabilele de mediu ale procesului de apelare sunt transmise noului program `/bin/sh`.



```

[12/05/22]seed@VM:~/Desktop$ gcc file2.c -o a2.out
[12/05/22]seed@VM:~/Desktop$ a2.out > file2.txt
[12/05/22]seed@VM:~/Desktop$
  
```



```

LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J25DKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
ORBIT_SOCKETDIR=/tmp/orbit-seed
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
SHLVL=1
LIBGL_ALWAYS_SOFTWARE=1
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
HOME=/home/seed
QT4_IM_MODULE=xln
OLDPWD=/home/seed
DESKTOP_SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GTK_MODULES=gail:atk-bridge:unity-gtk-module
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
INSTANCE=
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-uhJN3wzVT0
GIO_LAUNCHED_DESKTOP_FILE_PID=5476
COLORTERM=gnome-terminal
GNOME_KEYRING_CONTROL=
QT_OPA_PLATFORMTHEME=appmenu-qt5
  
```

Task 5: Environment Variable and Set-UID Programs

Variabila de mediu **PATH** s-a afișat modificată, concluzionând că se transmite procesului copil **Set-UID**

```

WINDOWID=65011716
OLDPWD=/home/seed
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1230
GNOME_KEYRING_CONTROL=
GTK_MODULES=gall:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=
QT_ACCESSIBILITY=1
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
PATH=/bin
QT_IM_MODULE=ibus
QT_OPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/Desktop
JOB=unity-settings-daemon
XMODIFIERS=@ln=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
GDMSESSION=ubuntu

```

Variabila de mediu **LD_LIBRARY_PATH** nu s-a transmis, concluzionând că această variabila de mediu nu se transmite procesului copil **Set-UID**

```

WINDOWID=65011716
OLDPWD=/home/seed
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1230
GNOME_KEYRING_CONTROL=
GTK_MODULES=gall:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=
QT_ACCESSIBILITY=1
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
PATH=/bin
QT_IM_MODULE=ibus
QT_OPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/Desktop
JOB=unity-settings-daemon
XMODIFIERS=@ln=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LD_LIBRARY_PATH=

```

Variabila de mediu **laborator** creată personal la fel s-a transmis procesului copil **Set-UID**, se observă că variabila **PATH** fiind modificată a dus la coruperea sistemului, astfel fiind o vulnerabilitate în sistem.

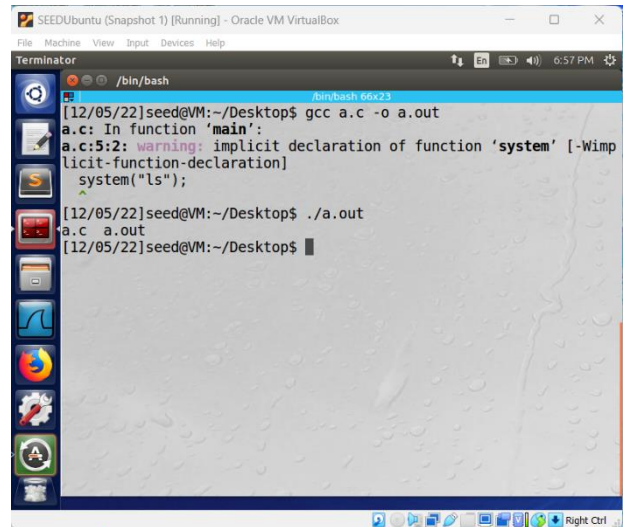
```

WINDOWID=65011716
OLDPWD=/home/seed
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1230
GNOME_KEYRING_CONTROL=
GTK_MODULES=gall:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=
QT_ACCESSIBILITY=1
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
PATH=/bin
QT_IM_MODULE=ibus
QT_OPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/Desktop
JOB=unity-settings-daemon
XMODIFIERS=@ln=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LABORATOR=1
LANGUAGE=en_US
LIBGL_ALWAYS_SOFTWARE=1
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=session started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Z4qgYtuTu
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/snapd/desktop
QT4_IM_MODULE=xim
LESSOPEN=| /usr/bin/lesspipe %s
INSTANCE=
UPSTART_JOB=unity7
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
XDG_CURRENT_DESKTOP=Unity
GTK_IM_MODULE=ibus
J2REDIR=/usr/lib/jvm/java-8-oracle/jre

```


Task 6: The PATH Environment Variable and Set-UID Programs

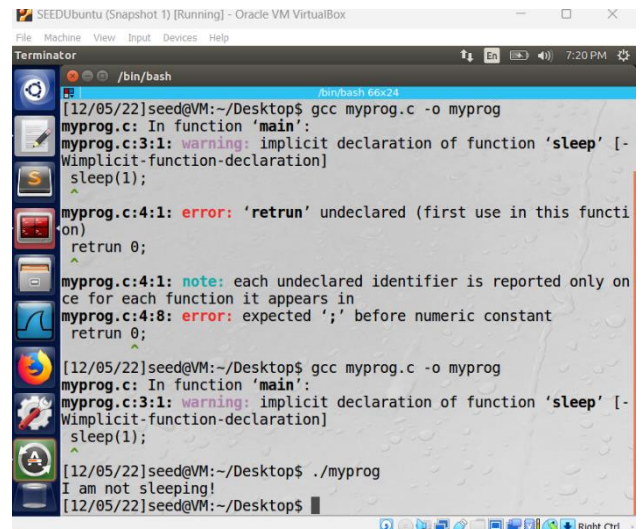
Programul rulează și afișează pe ecran rezultatul comenzii **ls**, însă fiind un program **Set-UID** nu rulează cu privilegii ale utilizatorului **root**, deoarece imediat ce este rulat, își schimbă privilegiile ale utilizatorului curent.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~/Desktop$ gcc a.c -o a.out
a.c: In function 'main':
a.c:5:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
  system("ls");
  ^
[12/05/22]seed@VM:~/Desktop$ ./a.out
a.c a.out
[12/05/22]seed@VM:~/Desktop$
```

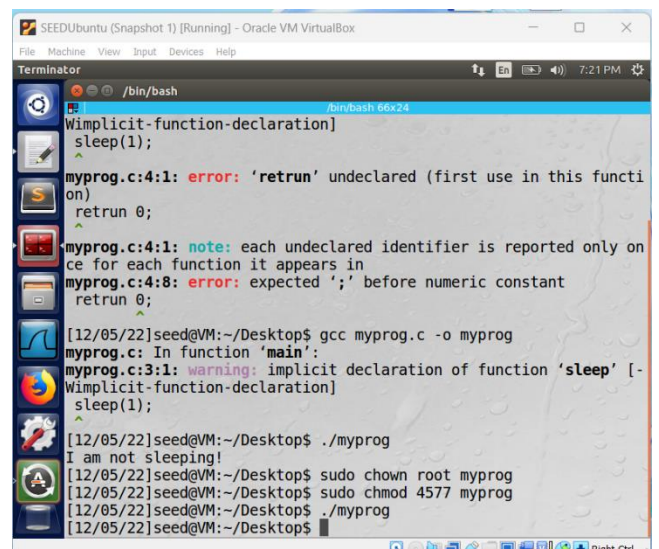
Task 7: The LD_PRELOAD Environment Variable and Set-UID Programs

Programul **myprog** rulează funcția **sleep** schimbată, concluzionând că variabila de mediu **LD_PRELOAD** s-a schimbat la userul normal.



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
myprog.c:4:1: error: 'retrun' undeclared (first use in this function)
  retrun 0;
  ^
myprog.c:4:1: note: each undeclared identifier is reported only once for each function it appears in
myprog.c:4:8: error: expected ';' before numeric constant
  retrun 0;
  ^
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[12/05/22]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[12/05/22]seed@VM:~/Desktop$
```

Programul **myprog** rulează funcția **sleep** neschimbată, concluzionând că **Set_UID** fiind într-un proces copil nu s-a moștenit variabila de mediu



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
Wimplicit-function-declaration]
  sleep(1);
  ^
myprog.c:4:1: error: 'retrun' undeclared (first use in this function)
  retrun 0;
  ^
myprog.c:4:1: note: each undeclared identifier is reported only once for each function it appears in
myprog.c:4:8: error: expected ';' before numeric constant
  retrun 0;
  ^
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[12/05/22]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[12/05/22]seed@VM:~/Desktop$ sudo chown root myprog
[12/05/22]seed@VM:~/Desktop$ sudo chmod 4577 myprog
[12/05/22]seed@VM:~/Desktop$ ./myprog
[12/05/22]seed@VM:~/Desktop$
```


Programul **myprog** rulează funcția **sleep** neschimbată, concluzionând că **Set_UID** fiind într-un proces copil nu s-a moștenit variabila de mediu, nici în cazul când s-a mai schimbat o dată variabila de mediu

```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
myprog.c:4:1: error: 'retrun' undeclared (first use in this function)
  retrun 0;
^
myprog.c:4:1: note: each undeclared identifier is reported only once for each function it appears in
myprog.c:4:8: error: expected ',' before numeric constant
  retrun 0;
      ^
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[12/05/22]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[12/05/22]seed@VM:~/Desktop$ sudo chown root myprog
[12/05/22]seed@VM:~/Desktop$ ./myprog
[12/05/22]seed@VM:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
[12/05/22]seed@VM:~/Desktop$ ./myprog
[12/05/22]seed@VM:~/Desktop$ ./myprog

```

Programul **myprog** rulează funcția **sleep** schimbată, concluzionând că variabila de mediu **LD_PRELOAD** s-a schimbat și la userul 1 normal

```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[12/05/22]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[12/05/22]seed@VM:~/Desktop$ sudo chown root myprog
[12/05/22]seed@VM:~/Desktop$ ./myprog
[12/05/22]seed@VM:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
[12/05/22]seed@VM:~/Desktop$ ./myprog
[12/05/22]seed@VM:~/Desktop$ gcc myprog.c -o myprog1
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[12/05/22]seed@VM:~/Desktop$ ./myprog1
I am not sleeping!
[12/05/22]seed@VM:~/Desktop$

```

Task 8: Invoking External Programs Using system() versus execve()

La rulare programul a funcționat corect, afișându-se conținutul fișierului.

```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[12/05/22]seed@VM:~$ gcc a.c -o a
gcc: error: a.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[12/05/22]seed@VM:~$ cd Desktop
[12/05/22]seed@VM:~/Desktop$ gcc a.c -o a.out
[12/05/22]seed@VM:~/Desktop$ sudo chown root a.out
[12/05/22]seed@VM:~/Desktop$ sudo chmod 4755 a.out
[12/05/22]seed@VM:~/Desktop$ ./a.out file
file file file
[12/05/22]seed@VM:~/Desktop$

```

Funcția **system** fiind vulnerabila, s-a putut modifica conținutul fișierului, fiind apelată și funcția **cat**, fiindcă variabila de mediu **PATH** afectează comportamentul funcției **system**, deoarece variabila afectează modul în care funcționează **shell-ul**.

```

[12/05/22]seed@VM:~/Desktop$ cd Desktop
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ file
Usage: file [-bcEhikLlNnprsvzZ] [--apple] [--extension] [--mime-encoding] [--mime-type] [-e testname] [-F separator] [-f namefile] [-m magicfiles]
file ...
file -C [-m magicfiles]
file [--help]
[12/05/22]seed@VM:~/Desktop$ cat file
[12/05/22]seed@VM:~/Desktop$ ./a.out file
[12/05/22]seed@VM:~/Desktop$ ./a.out file
file file file
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$

```

Funcția **execve** nu este vulnerabila, fiind ca nu s-a putut modifica conținutul fișierului, deoarece funcția **execve** nu invocă **shell-ul**.

```

file -C [-m magicfiles]
file [--help]
[12/05/22]seed@VM:~/Desktop$ cat file
[12/05/22]seed@VM:~/Desktop$ ./a.out file
[12/05/22]seed@VM:~/Desktop$ ./a.out file
file file file
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ ./a.out cat>file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ gcc a.c -o a1.out
a.c: In function 'main':
a.c:21:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
   execve(v[0], v, NULL);
   ^~~~~
[12/05/22]seed@VM:~/Desktop$ sudo chown root a1.out
[12/05/22]seed@VM:~/Desktop$ sudo chmod 4755 a1.out
[12/05/22]seed@VM:~/Desktop$ ./a1.out file
file file file
[12/05/22]seed@VM:~/Desktop$ ./a1.out cat >file
/bin/cat: cat: No such file or directory
[12/05/22]seed@VM:~/Desktop$ ./a1.out cat >file
bash: file: Permission denied

```

Task 9: Capability Leaking

În acest program fișierul **/etc/zzz** a fost modificat chiar dacă avea privilegiile de **root**, deoarece programul fiind unul de tip **Set-UID** la început, mai apoi s-au anulat aceste privilegii, însă având loc unele scăpări, aceste privilegii au rămas, făcând acest lucru posibil.

```

a.c:14:9: warning: implicit declaration of function 'getuid' [-Wimplicit-function-declaration]
   setuid(getuid());
   ^~~~~
a.c:15:9: warning: implicit declaration of function 'fork' [-Wimplicit-function-declaration]
   if(fork()) {
   ^~~~~
a.c:16:2: warning: implicit declaration of function 'close' [-Wimplicit-function-declaration]
   close(fd);
   ^~~~~
a.c:19:2: warning: implicit declaration of function 'write' [-Wimplicit-function-declaration]
   write(fd, "malicious data\n", 15);
   ^~~~~
[12/05/22]seed@VM:~/Desktop$ sudo chmod 4755 a.out
[12/05/22]seed@VM:~/Desktop$ sudo chown root a.out
[12/05/22]seed@VM:~/Desktop$ ./a.out
malicious data
[12/05/22]seed@VM:~/Desktop$ cat /etc/zzz
malicious data
[12/05/22]seed@VM:~/Desktop$

```