Nini Ola
Cyber security practice
4/7/2024

Mitnick Attack

1. Task 1: manipulating environment variables

a. Before export

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ printenv
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=niniola142002
PWD=/home/niniola142002/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
_=/usr/bin/printenv
OLDPWD=/home/niniola142002
seed@instance-20240226-171941:/home/niniola142002/Labsetup$
```

b. After export

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ export LAB6SETUP="/home/niniola142002/Labsetup/lab6
"
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ env
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=niniola142002
PWD=/home/niniola142002/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LAB6SETUP=/home/niniola142002/Labsetup/lab6
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
OLDPWD=/home/niniola142002
_=/usr/bin/env
```

- After unset: the set variable has been unset

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ unset LAB6SETUD
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ env
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=niniola142002
PWD=/home/niniola142002/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
OLDPWD=/home/niniola142002
_=/usr/bin/env
```

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

a. Running step 1

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc myprintenv.
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls
a.out       catall.c            image_ubuntu_mitnick  mtnk2.2.py  myprintenv.c
cap_leak.c  docker-compose.yml  mitm_sample.py        myenv.c     volumes
```

b. Output for step 1: print the environment variables

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls -l output
-rw-r--r-- 1 root root 0 Apr 18 21:59 output
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo touch output
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chmod u+w output
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./a.out > output
bash: output: Permission denied
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./a.out | sudo tee output
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
MAIL=/var/mail/root
LOGNAME=root
USER=root
HOME=/root
SHELL=/bin/bash
SUDO_COMMAND=./a.out
SUDO_USER=seed
SUDO_UID=1002
SUDO_GID=1003
```

c. Running step 2: print out environment variables

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./a.out | sudo tee output2
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
MAIL=/var/mail/root
LOGNAME=root
USER=root
HOME=/root
SHELL=/bin/bash
SUDO_COMMAND=./a.out
SUDO_USER=seed
SUDO_UID=1002
SUDO_GID=1003
```

d. Step 3: using diff command

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ diff output output2
1c1
< LANGC.UTF-8
---
> LANG=C.UTF-8
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ cat output 2
LANGC.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
MAIL=/var/mail/root
LOGNAME=root
USER=root
HOME=/root
SHELL=/bin/bash
SUDO_COMMAND=./a.out
SUDO_USER=seed
SUDO_UID=1002
SUDO_GID=1003
```

- **Draw conclusions:** the output here are the same, the environment variables of the parent process are the same and the child process will inherit the environment variables of the parent process

It appears that the only difference between the output and output2 files is in the first line regarding the LANG environment variable:

- In output, the value of LANG is LANGC.UTF-8.
- In output2, the value of LANG is LANG=C.UTF-8.

Based on this observation, it seems that the child process inherits the LANG environment variable from the parent process. The change in the value of LANG between the two outputs suggests that the child process received this environment variable from its parent. This aligns with the typical behavior of the fork() function in Unix, which creates a new process that inherits most of its environment variables from the parent process

3. Task 3: Task 3: Environment Variables and execve()

a. Step1 and 2 output

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc myenv.c -o myenv
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./myenv | sudo tee output3
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc myenv.c -o myenv
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ cat output3
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vum myenv.c
sudo: vum: command not found
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vim myenv.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc myenv.c -o myenv
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./myenv | sudo tee output3
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
MAIL=/var/mail/root
LOGNAME=root
USER=root
HOME=/root
SHELL=/bin/bash
SUDO_COMMAND=./myenv
SUDO_USER=seed
SUDO_UID=1002
SUDO_GID=1003
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ cat output3
LANG=C.UTF-8
```

b. Step 1 prints nothing while step 2 prints something the same as the env instructions

c. Draw conclusions = When you added execve("/usr/bin/env", argv, environ); to the code, you instructed the program to execute /usr/bin/env with the current environment variables (environ) instead of passing a NULL pointer as the third argument. This change likely caused /usr/bin/env to print out the environment variables inherited by the program, resulting in the output you observed.

Here's why this happened:

1. initially used execve("/usr/bin/env", argv, NULL);, the program executed /usr/bin/env with a NULL environment, which means it did not pass any environment variables to /usr/bin/env. Therefore, /usr/bin/env did not print any environment variables.
2. After modifying the code to use execve("/usr/bin/env", argv, environ);, the program passed the current environment variables (environ) to /usr/bin/env. This allowed /usr/bin/env to print out the environment variables inherited by the program.

Conclusion:

- The new program (myenv) gets its environment variables from the parent process (the shell) just like any other program launched from the shell.
- When myenv executes /usr/bin/env using execve, it can either pass a NULL pointer (resulting in /usr/bin/env not inheriting any environment variables) or pass the current environment variables (environ) to /usr/bin/env (resulting in /usr/bin/env inheriting the environment variables of myenv).
- By using execve("/usr/bin/env", argv, environ);, you instructed /usr/bin/env to inherit the environment variables of myenv, leading to the observed output.
- The man execve query learned that the execve function receives three variables, the first is to open the executable file, the second is the complete command, and the third is the environment variable that executes the command. The environment variable was not imported in Step1, so the env execution file was not found, and the execution failed. Set the global environment variable environ in Step2. After receiving the execve, find env in the environment variable and execute it. Supplement: Why use environ instead of the envp that comes with the main function? Environ is a global variable. If the environment variable changes during the execution of the program, the above execve will adopt the latest environment variable. Envp is imported when the main function is run. If the environment variable is modified during the execution of the main function, the envp will not be modified, then the execve function uses the old version of the environment variable and needs to be re-obtained by putenv(), setenv()

4. Task 4 Environment Variables and `system()`

a. Running result = env instructions result

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vim task4.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc task4.c -o task4
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./task4 | sudo tee output3
SUDO_GID=1003
MAIL=/var/mail/root
USER=root
HOME=/root
SUDO_UID=1002
LOGNAME=root
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SUDO_COMMAND=./task4
SHELL=/bin/bash
SUDO_USER=seed
PWD=/home/niniola142002/Labsetup
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./task4 | sudo tee output4
SUDO_GID=1003
MAIL=/var/mail/root
USER=root
HOME=/root
SUDO_UID=1002
```


```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo ./task4 | sudo tee output4
SUDO_GID=1003
MAIL=/var/mail/root
USER=root
HOME=/root
SUDO_UID=1002
LOGNAME=root
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
LANG=C.UTF-8
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=40;33;01:or=40;31;01:mi=00:su=
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.t
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip
=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*
.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear
=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;
31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01
;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;3
5:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35
:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*
.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=
01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:
*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SUDO_COMMAND=./task4
SHELL=/bin/bash
SUDO_USER=seed
PWD=/home/niniola142002/Labsetup
seed@instance-20240226-171941:/home/niniola142002/Labsetup$
```


b. Here system() actually executes the "/bin /sh -c command. Rewrites the original command to a new string command and requires the shell to execute

the command unlike the direct execution command of execve()

5. **Task 5:Environment Variable and `Set-UID` Programs**

PATHS

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ export PATH=$PATH:file:///home/niniola142002/Labset
up/task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:file:///hom
e/niniola142002/Labsetup/task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ export LAB5NINI=file:///home/niniola142002/Labsetup
/task5.c
```

STEP 5 OUTPUT

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc -o task5 task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chown root task5
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chmod 4755 task5
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task5 |grep PATH
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:file://
/home/niniola142002/Labsetup/task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc -o task5 task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chown root ./task5
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chmod 4755 ./task5
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task5 |grep PATH
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:file://
/home/niniola142002/Labsetup/task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task5 |grep LD_LIBRARY_PATH
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task5 |grep LAB5NINI
LAB5NINI=file:///home/niniola142002/Labsetup/task5.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$
```

Explanation: the program can't find the LD_LIBRARY_PATH path, but the other two paths are found and printed.

- This is because the program is a setuid program which can be authorized as a root user, so when executing the env program, Ubuntu executes the protection program anf filters out the critical path which is LD_LIBRARY_PATH

6. **TASK 8: Invoking External Programs Using `system()` Versus `execve()`**

   a. FILE PRESENT

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls -l
total 168
-rwxr-xr-x 1 root root 16752 Apr 18 22:33 a.out
-rw-rw-r-- 1 root root   761 Dec 27  2020 cap_leak.c
-rw-rw-r-- 1 root root   471 Feb 19  2021 catall.c
-rw-r--r-- 1 root root  1102 Dec  5  2020 docker-compose.yml
drwxr-xr-x 2 root root  4096 Dec  5  2020 image_ubuntu_mitnick
-rwxrwxr-x 1 root root   540 Jan  9  2021 mitm_sample.py
-rw-r--r-- 1 root root     0 Apr  8 00:43 mtnk2.2.py
-rwxr-xr-x 1 root root 16824 Apr 18 22:41 myenv
-rw-rw-r-- 1 root root   182 Apr 18 22:40 myenv.c
-rw-rw-r-- 1 root root   417 Apr 18 22:14 myprintenv.c
-rw-r--r-- 1 root root  1749 Apr 18 22:19 output
-r--r--r-- 1 root root     0 Apr 18 21:59 output.txt
-rw-r--r-- 1 root root  1749 Apr 18 22:15 output2
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output3
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output4
-rw-r--r-- 1 root root   417 Apr 23 04:49 tash8
-r--r--r-- 1 root root   417 Apr 23 04:53 tash8.c
-rwxr-xr-x 1 root root 16696 Apr 18 22:55 task4
-rw-r--r-- 1 root root    89 Apr 18 22:54 task4.c
-rwsr-xr-x 1 root root 16768 Apr 19 19:35 task5
-rwsr-xr-x 1 root root   159 Apr 19 19:16 task5.c
-rwxr-xr-x 1 root root 16928 Apr 23 05:12 task8
-rw-r--r-- 1 root root   545 Apr 23 05:12 task8.c
drwxrwxr-x 2 root root  4096 Apr  8 17:37 volumes
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vim task8.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task8 "./tash8.c;sudo rm -f ./tash8.c
```

- OUTPUT: FILE DELETED : TASK4.C

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vim tash8.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo chmod 444 task4.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task8 "./task4.c;sudo rm -f ./task4.c"
#include <stdio.h>
#include <stdlib.h>
int main()
{
system("/usr/bin/env");
return 0 ;
}
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls-l
ls-l: command not found
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls -l
total 164
-rwxr-xr-x 1 root root 16752 Apr 18 22:33 a.out
-rw-rw-r-- 1 root root   761 Dec 27  2020 cap_leak.c
-rw-rw-r-- 1 root root   471 Feb 19  2021 catall.c
-rw-r--r-- 1 root root  1102 Dec  5  2020 docker-compose.yml
drwxr-xr-x 2 root root  4096 Dec  5  2020 image_ubuntu_mitnick
-rwxrwxr-x 1 root root   540 Jan  9  2021 mitm_sample.py
-rw-r--r-- 1 root root     0 Apr  8 00:43 mtnk2.2.py
-rwxr-xr-x 1 root root 16824 Apr 18 22:41 myenv
-rw-rw-r-- 1 root root   182 Apr 18 22:40 myenv.c
-rw-rw-r-- 1 root root   417 Apr 18 22:14 myprintenv.c
-rw-r--r-- 1 root root  1749 Apr 18 22:19 output
-r--r--r-- 1 root root     0 Apr 18 21:59 output.txt
-rw-r--r-- 1 root root  1749 Apr 18 22:15 output2
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output3
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output4
-rw-r--r-- 1 root root   417 Apr 23 04:49 tash8
-r--r--r-- 1 root root   417 Apr 23 04:53 tash8.c
-rwxr-xr-x 1 root root 16696 Apr 18 22:55 task4
-rwsr-xr-x 1 root root 16768 Apr 19 19:35 task5
-rwsr-xr-x 1 root root   159 Apr 19 19:16 task5.c
-rwxr-xr-x 1 root root 16928 Apr 23 05:12 task8
-rw-r--r-- 1 root root   545 Apr 23 05:22 task8.c
drwxrwxr-x 2 root root  4096 Apr  8 17:37 volumes
```

Step 2: THE FILE STILL EXIST THEREFORE THE ATTACK METHOD USED IN STEP 1 WONT WORK HERE DUE USING AN ALTERNATIVE TO SYSTEM()

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls -l
total 168
-rwxr-xr-x 1 root root 16752 Apr 18 22:33 a.out
-rw-rw-r-- 1 root root   761 Dec 27  2020 cap_leak.c
-rw-rw-r-- 1 root root   471 Feb 19  2021 catall.c
-rw-r--r-- 1 root root  1102 Dec  5  2020 docker-compose.yml
drwxr-xr-x 2 root root  4096 Dec  5  2020 image_ubuntu_mitnick
-rwxrwxr-x 1 root root   540 Jan  9  2021 mitm_sample.py
-rw-r--r-- 1 root root     0 Apr  8 00:43 mtnk2.2.py
-rwxr-xr-x 1 root root 16824 Apr 18 22:41 myenv
-rw-rw-r-- 1 root root   182 Apr 18 22:40 myenv.c
-rw-rw-r-- 1 root root   417 Apr 18 22:14 myprintenv.c
-rw-r--r-- 1 root root  1749 Apr 18 22:19 output
-r--r--r-- 1 root root     0 Apr 18 21:59 output.txt
-rw-r--r-- 1 root root  1749 Apr 18 22:15 output2
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output3
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output4
-rw-r--r-- 1 root root   417 Apr 23 04:49 tash8
-r--r--r-- 1 root root   417 Apr 23 04:53 tash8.c
-rwxr-xr-x 1 root root 16696 Apr 18 22:55 task4
-rwsr-xr-x 1 root root 16768 Apr 19 19:35 task5
-rwsr-xr-x 1 root root   159 Apr 19 19:16 task5.c
-rwxr-xr-x 1 root root 16928 Apr 23 05:36 task8
-r--r--r-- 1 root root   225 Apr 23 05:34 task8.2.c
-rw-r--r-- 1 root root   593 Apr 23 05:36 task8.c
drwxrwxr-x 2 root root  4096 Apr  8 17:37 volumes
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task8 "./task8.2.c;sudo rm -f ./task8.2.c"
/bin/cat: './task8.2.c;sudo rm -f ./task8.2.c': No such file or directory
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ls -l
total 168
-rwxr-xr-x 1 root root 16752 Apr 18 22:33 a.out
-rw-rw-r-- 1 root root   761 Dec 27  2020 cap_leak.c
-rw-rw-r-- 1 root root   471 Feb 19  2021 catall.c
-rw-r--r-- 1 root root  1102 Dec  5  2020 docker-compose.yml
drwxr-xr-x 2 root root  4096 Dec  5  2020 image_ubuntu_mitnick
-rwxrwxr-x 1 root root   540 Jan  9  2021 mitm_sample.py
-rw-r--r-- 1 root root     0 Apr  8 00:43 mtnk2.2.py
-rwxr-xr-x 1 root root 16824 Apr 18 22:41 myenv
-rw-rw-r-- 1 root root   182 Apr 18 22:40 myenv.c
-rw-rw-r-- 1 root root   417 Apr 18 22:14 myprintenv.c
-rw-r--r-- 1 root root  1749 Apr 18 22:19 output
-r--r--r-- 1 root root     0 Apr 18 21:59 output.txt
-rw-r--r-- 1 root root  1749 Apr 18 22:15 output2
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output3
-rw-r--r-- 1 root root  1782 Apr 18 22:55 output4
-rw-r--r-- 1 root root   417 Apr 23 04:49 tash8
-r--r--r-- 1 root root   417 Apr 23 04:53 tash8.c
-rwxr-xr-x 1 root root 16696 Apr 18 22:55 task4
-rwsr-xr-x 1 root root 16768 Apr 19 19:35 task5
-rwsr-xr-x 1 root root   159 Apr 19 19:16 task5.c
-rwxr-xr-x 1 root root 16928 Apr 23 05:36 task8
-r--r--r-- 1 root root   225 Apr 23 05:34 task8.2.c
-rw-r--r-- 1 root root   593 Apr 23 05:36 task8.c
drwxrwxr-x 2 root root  4096 Apr  8 17:37 volumes
seed@instance-20240226-171941:/home/niniola142002/Labsetup$
```

EXPLANATION: The implementation principle of the system() function is shown in task4. Step1 is equivalent to execution: /bin/cat ./ttt.c;rm ./ttt.c. The semicron divides the command into two sentences, but because they are all executed by sub-processes created by system() and have root permissions, the ttt.c file is successfully deleted. The implementation principle of the execve() function is shown in task3. In Step2, because it is an array of obtained strings, "./ttt.c;rm ./ttt.c" is regarded as a string element, and the cat program execution cannot find the file, so the attack failed.

7. Task 9 : CAPABILITY LEAKING

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo cat /etc/zzz
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc -o task9 task9.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo vim task9.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo gcc -o task9 task9.c
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo cat /etc/zzz
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task9
```

```
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ ./task9
fd is 3
$ maliciois data
/bin/sh: 1: maliciois: not found
$ sudo echo "malicious data" >> /etc/zzz
$ exit
seed@instance-20240226-171941:/home/niniola142002/Labsetup$ sudo cat /etc/zzz
malicious data
seed@instance-20240226-171941:/home/niniola142002/Labsetup$
```

EXPLANATION: The program has been reduced to an ordinary user after executing the 19th line, but the fd handle can still open /etc/zzz because it is set when it has root permission, that is, it has root permission, causing a memory leak.

Files opened under root permissions should be closed immediately after completing the work that requires root permissions and reducing the rights, otherwise it will cause memory leakage.