靶机渗透_hackthebox__Writeup -6

原创

河里一只虾 于 2019-11-11 21:47:56 发布 857 收藏
分类专栏： 靶机渗透_hackthebox

本文链接：https://blog.csdn.net/qq_34717555/article/details/103017468

host:10.10.10.138

nmap 扫描一下 这次也尝试了一下自己的选项和A 选项发现A 比自己设置的要好很多不过这样被发现的几率也大了一些

自己配置的可以有很多降低被发现的选项

```
# Nmap 7.70 scan initiated Tue Aug  6 20:47:35 2019 as: nmap -A -o nmap.scan 10.
10.10.138
Nmap scan report for 10.10.10.138
Host is up (0.34s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 dd:53:10:70:0b:d0:47:0a:e2:7e:4a:b6:42:98:23:c7 (RSA)
|   256 37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (ECDSA)
|_  256 93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/writeup/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Nothing here yet.
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 at Tue Aug  6 20:48:22 2019 -- 1 IP address (1 host up) scanned in 4
7.41 seconds
```

只有80，22端口

扫描信息里有 writeup目录robots.txt

但是根据index 页面是一个维护中的web没什么信息
在扫描过程中有一个robots.txt 中一个disallow 页面 所以去看了一下

在目录爆破时发现 网站开启了防止DOS 暂时没办法所以只能手动验证

不过在爆破的时候发现一个admin然后发现了防止dos的存在

手动检查 挨个看看源码，源码中有网站的CMS 信息 CMS Made Simple - Copyright (C) 2004-2019. All ri ghts reserved.

搜不过没有获得版本信息，但是获得了最新版本是2.2.10

而且有一个CVE 2019 9053 <=2.2.9一下的sql注入漏洞 不出意外应该是可以使用

找到EXP 修改一下运行----拿到 凭证密码加密（很常见）md5网站走一波

jkr用户不过没有进入admin突然想到还有一个22端口

```
ssh ${user}@${ip}
```

上传LinEnum.sh脚本枚举一下没有什么方向，随后逛了一下论坛

都有提到在用户登陆的时候会有特殊的进程出现 所以pspy 观察一下并且另外ssh连接

```
2019/08/08 09:11:25 CMD: UID=0    PID=2565   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/u
sysinit /etc/update-motd.d > /run/motd.dynamic.new
2019/08/08 09:11:09 CMD: UID=0    PID=2555   | /bin/sh /etc/update-motd.d/10-uname
2019/08/08 09:30:11 CMD: UID=0    PID=3058   | /usr/bin/python3 /usr/bin/fail2ban-server -s /var/run/fail2b
an.pid -b
2019/08/08 09:30:11 CMD: UID=0    PID=3066   | iptables -w -I f2b-apache-404 1 -s 10.10.15.64 -j REJECT --r
2019/08/08 09:30:11 CMD: UID=0    PID=3059   | /bin/sh -c iptables -w -n -L INPUT | grep -q 'f2b-apache-404
```

观察到第一个进程 UID为0 root

sh -c 执行一个命令 ENV 环境变量的设置 -i 以空的环境变量开始
并且之后又设置了一个环境变量 PATH=/usr/local/sbin/.....等
执行命令 run-parts --ls.... /etc/update-motd.d >.....
查看了一下 /usr/local/sbin 目录的权限

查看一下 /usr/local/sbin 可以写但是不可以读staff 用户

编辑一个run-parts 文件给相应权限，放入一个反弹shell的脚本

拿到root flag