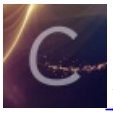
Hack The Box - Access Writeup

原创

ShinJoe 于 2019-01-23 09:54:02 发布 1080 收藏 1
分类专栏： hackthebox 文章标签： CTF

本文链接：https://blog.csdn.net/qq_23026851/article/details/86604311



第一次尝试Hack The Box，在难度较低的Access上，前后花了有两天的时间，汗。收获还是很大，在此记录一下，以便后阅。

- 首先是获取user，通过nmap扫描，可以发现目标主机开了三个端口21（FTP），23（telnet），80（HTTP)。80端口是迷惑信息，先尝试利用FTP。
- 但是因为不知道登陆FTP的账号密码，这里也卡了很久TAT。后来才发现有anonymous登陆这种操作。上去看到两个文件，一个.mdb，一个zip。zip需要密码，所以得先从.mdb入手。
- 接下来又是一个大坑。mdb文件是Microsoft Access的数据库文件，我因为没有装Access，所以尝试了excel，在线工具等，结果都不行。后来用了linux上的mdbtools，结果提示文件已损坏。我猜是文件传输的时候出了问题，于是下了个FileZilla，果然这次下载的文件可以被mdbtools打开。Linux自带的FTP不靠谱啊。
- mdb文件里有一个密码，用这个密码解压zip文件，得到一个.pst文件。这是一个Outlook的文件夹文件，然后我主机里也没有Outlook。。。于是曲线救国，下了个pstviewer，成功读取并得到了username和password。
- Telnet登陆目标机，浏览一番，在对应的Desktop文件夹里找到了user的hash。
- 然后就是获取root了，或者说，读到root的桌面上的root.txt就可以了，但是我的当前用户没有进入root文件夹的权限。毫无头绪一开始，后来上HTB的论坛逛了逛，发现了一些hint都让用runas命令，于是去学习了runas的用法。RUNAS [[/noprofile | /profile] [/env] [/savecred | /netonly]] /**user**:*UserName program*。
- 这个box把runas的命令行输出全部隐藏掉了=。=，好吧，先在自己主机测试。参数上使用了/env，/savecred因为我不知道Administrator的密码（废话），/user要包括主机名称（ACCESS\Administrator）。
- 至于运行哪个program还是有点tricky的，我一开始用了Notepad，嗯，显然没用，因为我只有一个command shell。而copy/type这些是internal的程序，不能直接作为program跟在后面。于是经过研究之后，发现了这样的命令是行得通的：runas /env /savecred /user:ACCESS\Administrator "cmd /K copy a.txt b.txt"。
- 最后，我的目标是读取root.txt。我先尝试了把root/Desktop/root.txt复制出来，然后发现复制的文件保留了原来的权限，因此还是无法读取。直接type到命令行上？好吧，输出被隐藏掉了。那我把root.txt打印出来，然后存在另一个文件里呢？runas /env /savecred /user:ACCESS\Administrator "cmd /K type Administrator\Desktop\root.txt > mytest.txt"，然后读取mytest.txt，成功！！！