OverTheWire Bandit Writeup （1-10）

原创

合天网安实验室 于 2018-08-07 20:00:00 发布 187 收藏

点击上方蓝字关注我们


OverTheWire是一个wargame网站。其中Bandit是一个适合学习Linux指令的游戏，主要是考察一些基本的Linux命令行操作。规则是每一关利用提供的主机加端口和上一关得到的密码通过ssh进入指定的环境，按照要求拿到指定的key，而得到的key又作为下一关的密码。

网站：http://overthewire.org/wargames/bandit/

Level0-1

描述：需要你使用ssh登陆bandit.labs.overthewire.org端口是2220.用户名和密码都是bandit0，然后使用ls,cd,cat,file,du,find等命令，查看一个叫readme的文件，里面存储了到下一关的密码。

sshbandit0@bandit.labs.overthewire.org-p2220

登录之后，就看到欢迎界面，和一些列说明，包括一些规则说明，提示等等

查看文件，找到有用的信息

bandit0@bandit:~$ls

readme

bandit0@bandit:~$catreadme

boJ9jbbUNNfktd78OOpsqOltutMc3MY1

bandit0@bandit:~$

Level1→2

通过上一关得到的密码登录bandit1

bandit0@bandit:~$sshbandit1@localhost

描述：下一关的密码存储在家目录下的“-”文件中。

这里考察是我们对linux目录操作的理解，因为linux中“-”代表的是“进入此目录之前所在的目录”，所以不能直接使用”cat-“来查看。加上文件的路径就可以了

bandit1@bandit:~$ls-al//查看当前目录下所有文件

bandit1@bandit:~$cat./-

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level2→3

使用前一关的密码登录bandit2

bandit0@bandit:~$sshbandit2@localhost

描述：下一关的密码存储在家目录下一个含有空格的文件中。这里考察我们对linuxshell转义符的理解，我们只需要把空格进行转义即可,或者用”“包裹也可以。

```
bandit2@bandit:~$ls-al
-rw-r-----1bandit3bandit233Dec282017spacesinthisfilename
bandit2@bandit:~$cat"spacesin this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$catspaces\in\this\filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level3→4

使用前一关的密码登录bandit3//后续就不再重复写了，每一关都是这样

描述：下一关的密码存储在inhere目录下的一个隐藏文件中。这里考察的是ls命令的用法，默认情况不显示隐藏文件，只要加上-a就好了，隐藏文件是以”.“开头的，然后cat查看。

bandit3@bandit:~$lsinhere/

bandit3@bandit:~$

bandit3@bandit:~$ls-ainhere/

....hidden

bandit3@bandit:~$catinhere/.hidden

pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Level4→5

描述：下一关的密码存储在inhere目录中，是一个人类可以阅读的文件（严格来说是ASCII字符）。

先来看下有哪些文件吧？

bandit4@bandit:~$ls./inhere/-l

total40

-rw-r-----1bandit5bandit433Dec282017-file00

-rw-r-----1bandit5bandit433Dec282017-file01

-rw-r-----1bandit5bandit433Dec282017-file02

-rw-r-----1bandit5bandit433Dec282017-file03

-rw-r-----1bandit5bandit433Dec282017-file04

-rw-r-----1bandit5bandit433Dec282017-file05

-rw-r-----1bandit5bandit433Dec282017-file06

-rw-r-----1bandit5bandit433Dec282017-file07

-rw-r-----1bandit5bandit433Dec282017-file08

-rw-r-----1bandit5bandit433Dec282017-file09

有十个文件，要怎么才能知道哪一个文件是我们人可以看得懂的呢？难道一个个去看？这就太低效率了吧。这时候我们可以用file这个命令。file命令就是用来查看文件类型的,也可用来辨别一些文件的编码格式。它是通过查看文件的头部信息来获取文件类型。

bandit4@bandit:~$file./inhere/*

./inhere/-file00:data

./inhere/-file01:data

./inhere/-file02:data

./inhere/-file03:data

./inhere/-file04:data

./inhere/-file05:data

./inhere/-file06:data

./inhere/-file07:ASCII text

./inhere/-file08:data

./inhere/-file09:data

可以看到除了"-file07"之外，其他都是二进制格式的文件，我们知道二进制格式只有机器看得懂。人类肯定看不懂。

bandit4@bandit:~$cat./inhere/-file07

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level5→6

描述：下一关的密码存储在inhere目录中一个文件中，但是这个文件必须满足三个条件，分别是：人类可阅读；大小是1033bytes；不是可执行文件。

```
bandit5@bandit:~$cd./inhere
bandit5@bandit:~/inhere$ls-al
total88
drwxr-x---22rootbandit54096Dec282017.
drwxr-xr-x3rootroot4096Dec282017..
drwxr-x---2rootbandit54096Dec282017maybehere00
drwxr-x---2rootbandit54096Dec282017maybehere01
drwxr-x---2rootbandit54096Dec282017maybehere02
drwxr-x---2rootbandit54096Dec282017maybehere03
drwxr-x---2rootbandit54096Dec282017maybehere04
drwxr-x---2rootbandit54096Dec282017maybehere05
drwxr-x---2rootbandit54096Dec282017maybehere06
drwxr-x---2rootbandit54096Dec282017maybehere07
drwxr-x---2rootbandit54096Dec282017maybehere08
drwxr-x---2rootbandit54096Dec282017maybehere09
```

```
drwxr-x---2rootbandit54096Dec282017maybehere10
drwxr-x---2rootbandit54096Dec282017maybehere11
drwxr-x---2rootbandit54096Dec282017maybehere12
drwxr-x---2rootbandit54096Dec282017maybehere13
drwxr-x---2rootbandit54096Dec282017maybehere14
drwxr-x---2rootbandit54096Dec282017maybehere15
drwxr-x---2rootbandit54096Dec282017maybehere16
drwxr-x---2rootbandit54096Dec282017maybehere17
drwxr-x---2rootbandit54096Dec282017maybehere18
drwxr-x---2rootbandit54096Dec282017maybehere19
```

这么多目录，难道一个个去找，当然不是这样的。

这里考察的就是find命令的用法，我们通过find命令指定查找文件的大小就能快速找到

bandit5@bandit:~/inhere$find.-size1033c

./maybehere07/.file2

bandit5@bandit:~/inhere$cat./maybehere07/.file2

DXjZPULLxYr17uwol01bNLQbtFemEgo7

Level6→7

描述：下一关密码文件存储在服务器的某个位置，但是有三个特征，1、文件拥有者是bandit7；2、文件所属组是bandit6；3、文件大小是33bytes。

这里考察的是find的更高级的用法，指定文件所属的用户，用户组

bandit6@bandit:~$find/-userbandit7-groupbandit6-size33c2>/dev/null

/var/lib/dpkg/info/bandit7.password

bandit6@bandit:~$cat/var/lib/dpkg/info/bandit7.password

HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

Tips:这里因为输出太多，所以把多余的输出重定向到了/dev/null

Level7→8

描述：下一关的密码存储在data.txt文件中millionth单词旁边，可能用到的命令：
grep,sort,uniq,strings,base64,tr,tar,gzip,bzip2,xxd

从这一关开始考察我们对linux文件内容的操作了

bandit7@bandit:~$ls-al

total4108

drwxr-xr-x2rootroot4096Dec282017.

drwxr-xr-x42rootroot4096Jul2218:42..

-rw-r--r--1rootroot220Sep12015.bash_logout

-rw-r--r--1rootroot3771Sep12015.bashrc

-rw-r--r--1rootroot655Jun242016.profile

-rw-r-----1bandit8bandit74184396Dec282017data.txt

bandit7@bandit:~$grep"millionth"./data.txt//使用grep命令过滤关键字找到密码

millionthcvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level8→9

描述：下一关密码存储在data.txt文件中，内容是文件中只出现过一次的行。并且提示给出了需要用到管道和重定向这里我们可以使用uniq查找文件中唯一的行，通常和sort命令一起使用，首先使用sort进行排序，然后用uniq找出唯一不重复的行。

bandit8@bandit:~$sortdata.txt|uniq-u//-u：仅显示出一次的行列

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level9→10

描述：下一关的密码存储在data.txt文件中，里面只有极少的人类可以阅读的字符，并且是以几个”=“开头。

这里我们可以用strings命令，strings命令在对象文件或二进制文件中查找可打印的字符串，也就是人类可阅读的字符（（ASCII字符中的可见字符，也叫可打印字符）。然后用grep过滤关键字

bandit9@bandit:~$stringsdata.txt|grep"=="

==========theP`

==========password

L==========isA

==========truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

未完待续.....

公元2018年8月6日23时59分，夜已深，我们下次见

别忘了投稿哦

大家有好的技术原创文章

欢迎投稿至邮箱：edu@heetian.com 或 qq:3200599554

合天会根据文章的时效、新颖、文笔、实用等多方面评判给予100元-500元不等的稿费哦

有才能的你快来投稿吧！

了解投稿详情点击重金悬赏 | 合天原创投稿等你来！

长按二维码　识别加关注