Выполнил

ст. гр. 11405120

Лоза М.Г.

Лабораторная работа 6

**Прохождение уровней bandit**

**Уровень 0**

Необходимо подключиться к хосту на bandit.labs.overthewire.org, порт 2220 и зайти за пользователя bandit0 с паролем bandit0. Сказано — сделано. Используем стандартный синтаксис команды ssh с флагом -p, отвечающим за указание порта для подключения:

:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220

This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password: <b>bandit0</b>

...

bandit0@bandit:~$

**Уровень 1**

Пароль для перехода на следующий уровень находится в файле **readme** в домашней директории. Для его прочтения нам понадобится команда cat, выводящая в окне терминала содержимое файла:

bandit0@bandit:~$ cat readme

boJ9jbbUNNfktd78OOpsqOltutMc3MY1  
В конце каждого уровня подключаемся с помощью ssh к следующему пользователю на localhost:

bandit0@bandit:~$ ssh bandit1@localhost

Could not create directory '/home/bandit0/.ssh'.

The authenticity of host 'localhost (127.0.0.1)' can't be established.

ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.

Are you sure you want to continue connecting (yes/no)? yes

Failed to add the host to the list of known hosts (/home/bandit0/.ssh/known\_hosts).

This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit1@localhost's password: <b>Пароль</b>

bandit1@bandit:~$

**Уровень 2**

Пароль к следующему уровню хранится в файле с названием - и это единственное, чем он отличается от предыдущего. Используем ту же команду cat с небольшим изменением:

bandit1@bandit:~$ cat ./-

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

bandit1@bandit:~$ ssh bandit2@localhost  
Пропускаем предупреждение, подключаемся к bandit2 и переходим на следующий уровень.

**Уровень 3**

На этом уровне файл **spaces in this filename**, содержащий пароль, имеет в названии пробелы. С этим тоже легко справиться, заключив название файла в кавычки:

bandit2@bandit:~$ cat "spaces in this filename"

UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

bandit2@bandit:~$ ssh bandit3@localhost

Уровень 4

Пароль к следующему уровню находится в скрытом файле в директории **inhere**, чтобы его показать в консоли используем команду ls, выводящую в терминал содержимое директории, с флагом -a, включающим в список содержимое, название которого начинается с точки. Перейдем в директорию командой cd, через пробел указав ее название:

bandit3@bandit:~$ cd inhere

bandit3@bandit:~/inhere$ ls

bandit3@bandit:~/inhere$ ls -a

. .. .hidden

bandit3@bandit:~/inhere$ cat .hidden

pIwrPrtPN36QITSp3EQaw936yaFoFgAB

bandit3@bandit:~/inhere$ ssh bandit4@localhost

**Уровень 5**

Пароль находится в единственном файле, который вы сможете прочитать (буквально), в директории **inhere**. Чтобы получить информацию о типе файле будем использовать команду file. Для начала перейдем в директорию и посмотрим, что внутри:

bandit4@bandit:~$ cd inhere

bandit4@bandit:~/inhere$ ls

-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09  
Все файлы начинаются с -, поэтому используем синтаксис из второго уровня и дополним \* (символ wildcard, обозначающий сколько угодно любых знаков до или, в нашем случае, после), чтобы получить информацию о всех файлах сразу:

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

./-file00: data

./-file01: data

./-file02: data

./-file03: data

./-file04: data

./-file05: data

./-file06: data

./-file07: ASCII text

./-file08: data

./-file09: data  
Как мы видим, единственный файл, который мы можем прочитать это -file07. Чем и займемся, используя знакомую нам команду cat.

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

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

bandit4@bandit:~/inhere$ ssh bandit5@localhost

**Уровень 6**

Теперь, помимо читаемости файла, нужно учесть размер в 1033 байта и факт, что файл не исполняемый. Для этого воспользуемся командой find с параметром -size 1033c . Сначала сменим директорию и посмотрим, что внутри.

bandit5@bandit:~$ cd inhere

bandit5@bandit:~/inhere$ ls

maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18

maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19

maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17

bandit5@bandit:~/inhere$ find -size 1033c

./maybehere07/.file2

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

DXjZPULLxYr17uwoI01bNLQbtFemEgo7

bandit5@bandit:~/inhere$ ssh bandit6@localhost

**Уровень 7**

Продолжаем изучать возможные тесты команды find и ищем файл **на сервере**, который принадлежит пользователю **bandit7**, группе **bandit6** и весит **33 байта**. Перейдем в корень и начнем поиски, используя для уточнения поиска флаги -user для пользователя и -group для группы пользователей, а также знакомый -size:

bandit6@bandit:~$ cd /

bandit6@bandit:/$ find -user bandit7 -group bandit6 -size 33c

find: ‘./root’: Permission denied

find: ‘./home/bandit28-git’: Permission denied

find: ‘./home/bandit30-git’: Permission denied

find: ‘./home/bandit5/inhere’: Permission denied

find: ‘./home/bandit27-git’: Permission denied

find: ‘./home/bandit29-git’: Permission denied

find: ‘./home/bandit31-git’: Permission denied

find: ‘./lost+found’: Permission denied

find: ‘./etc/ssl/private’: Permission denied

find: ‘./etc/polkit-1/localauthority’: Permission denied

find: ‘./etc/lvm/archive’: Permission denied

find: ‘./etc/lvm/backup’: Permission denied

find: ‘./sys/fs/pstore’: Permission denied

find: ‘./proc/tty/driver’: Permission denied

find: ‘./proc/26731/task/26731/fd/6’: No such file or directory

find: ‘./proc/26731/task/26731/fdinfo/6’: No such file or directory

find: ‘./proc/26731/fd/5’: No such file or directory

find: ‘./proc/26731/fdinfo/5’: No such file or directory

find: ‘./cgroup2/csessions’: Permission denied

find: ‘./boot/lost+found’: Permission denied

find: ‘./tmp’: Permission denied

find: ‘./run/lvm’: Permission denied

find: ‘./run/screen/S-bandit26’: Permission denied

find: ‘./run/screen/S-bandit18’: Permission denied

find: ‘./run/screen/S-bandit13’: Permission denied

find: ‘./run/screen/S-bandit16’: Permission denied

find: ‘./run/screen/S-bandit31’: Permission denied

find: ‘./run/screen/S-bandit8’: Permission denied

find: ‘./run/screen/S-bandit14’: Permission denied

find: ‘./run/screen/S-bandit19’: Permission denied

find: ‘./run/screen/S-bandit21’: Permission denied

find: ‘./run/screen/S-bandit12’: Permission denied

find: ‘./run/screen/S-bandit5’: Permission denied

find: ‘./run/screen/S-bandit22’: Permission denied

find: ‘./run/screen/S-bandit24’: Permission denied

find: ‘./run/screen/S-bandit25’: Permission denied

find: ‘./run/screen/S-bandit0’: Permission denied

find: ‘./run/screen/S-bandit20’: Permission denied

find: ‘./run/screen/S-bandit23’: Permission denied

find: ‘./run/shm’: Permission denied

find: ‘./run/lock/lvm’: Permission denied

find: ‘./var/spool/bandit24’: Permission denied

find: ‘./var/spool/cron/crontabs’: Permission denied

find: ‘./var/spool/rsyslog’: Permission denied

find: ‘./var/tmp’: Permission denied

find: ‘./var/lib/apt/lists/partial’: Permission denied

find: ‘./var/lib/polkit-1’: Permission denied

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

find: ‘./var/log’: Permission denied

find: ‘./var/cache/apt/archives/partial’: Permission denied

find: ‘./var/cache/ldconfig’: Permission denied

Мы видим единственный файл, к которому имеем доступ.

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

HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

bandit6@bandit:/$ ssh bandit7@localhost

**Уровень 8**

Необходимо осуществить поиск по файлу **data.txt** и найти пароль напротив слова **millionth**. Воспользуемся командой grep, выводящую в терминал содержимое файла, соответствующее паттерну (маске), на интуитивно понятном уровне:

bandit7@bandit:~$ grep millionth data.txt

millionth cvX2JJa4CFALtqS87jk27qwqGhBM9plV

bandit7@bandit:~$ ssh bandit8@localhost

**Уровень 9**

Нужно найти в файле **data.txt** уникальную строку. Воспользуемся командами sort, сортирующей файл по определенным требованиям, и uniq, выводящей в терминал все уникальные строки из файла, с опцией -u, указывающей команде вывести только строки, встречающиеся один раз. Если повторяющиеся строки не идут друг за другом, отсюда обращение к sort, на выходе дающей отсортированный по алфавиту файл (т. е. повторяющиеся строки будут как раз друг за другом, это должно быть понятно). Вертикальная палочка между двумя командами называется pipe и позволяет передать на вход команде за палочкой результат выполнения команды перед палочкой:

bandit8@bandit:~$ sort data.txt | uniq -u

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

bandit8@bandit:~$ ssh bandit9@localhost

**Уровень 10**

Нужной найти пароль среди огромного количества случайных символов в файле **data.txt**. Воспользуемся волшебной командой strings, выводящей из файла последовательности читаемых символов длиной не меньше четырех и сразу поставим побольше непрерывных символов в строке, например, 10.

bandit9@bandit:~$ strings -10 data.txt

========== the\*2i"4

========== password

Z)========== is

&========= truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

8Zpc $FOxF[