Finding Password

মঙ্গলবার, 6 জুলাই, 2021 4:53 PM

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls
-file1  -file2  -file3  spaces file1  spaces file2  spaces file3
bandit5@bandit:~/inhere/maybehere07$ ls -la
total 56
drwxr-x---  2 root bandit5 4096 May  7  2020 .
drwxr-x--- 22 root bandit5 4096 May  7  2020 ..
-rwxr-x---  1 root bandit5 3663 May  7  2020 -file1
-rwxr-x---  1 root bandit5 3065 May  7  2020 .file1
-rw-r-----  1 root bandit5 2488 May  7  2020 -file2
-rw-r-----  1 root bandit5 1033 May  7  2020 .file2
-rwxr-x---  1 root bandit5 3362 May  7  2020 -file3
-rwxr-x---  1 root bandit5 1997 May  7  2020 .file3
-rwxr-x---  1 root bandit5 4130 May  7  2020 spaces file1
-rw-r-----  1 root bandit5 9064 May  7  2020 spaces file2
-rwxr-x---  1 root bandit5 1022 May  7  2020 spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Note:

1. b - for 512-byte blocks (this is the default if no suffix is used)
2. c - for bytes.
3. w - for two-byte words.
4. k - for Kilobytes (units of 1024 bytes)
5. M - for Megabytes (units of 1048576 bytes)
6. G - for Gigabytes (units of 1073741824 bytes)

Connecting to bandit6

মঙ্গলবার, 6 জুলাই, 2021   4:53 PM

```
┌──(manarat㉿kali)-[~]
└─$ ssh bandit6@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit6@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux


     ,----..           ,----,          .---.
    /  /  \        ,/  .`|        /. ./|
   /  .    :     ,`  .' :    .--'. ';
  .  /  ;. \  ;   ;    /   /__./ \ : |
 .  ;  / `; .'___,/   ,' .--'. '  \' .
 ;  | ;\ ; | |   :    | /___/ \ |   ''
 |  : | ; | ';   |.'; ; ;  \ \;     :
 .  | ''' : `----' |  | \  ; `      |
 '  ; \; / |    '  : ;  .  \   .\ ;
  \  \ ', /     |  | '  \  \  '\ |
   ;  :  /      '  : |    :  '  |--"
    \  \.'      ;  |.'     \  \;
 www. `---` ver    '---' he       '---" ire.org


Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

  This machine might hold several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
```

```
  easily guessable or short names will be periodically deleted!

  Please play nice:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
    * don't annoy other players
    * don't post passwords or spoilers
    * again, DONT POST SPOILERS!
      This includes writeups of your solution on your blog or website!

--[ Tips ]--

  This machine has a 64bit processor and many security-features enabled
  by default, although ASLR has been switched off.  The following
  compiler flags might be interesting:

    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

For your convenience we have installed a few usefull tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
```

irc.overthewire.org #wargames.

Enjoy your stay!