Finding Password

মঙ্গলবার, 6 জুলাই, 2021   5:27 PM

bandit6@bandit:~$ ls -la

total 20

drwxr-xr-x 2 root root 4096 May 7 2020 .

drwxr-xr-x 41 root root 4096 May 7 2020 ..

-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout

-rw-r--r-- 1 root root 3526 May 15 2017 .bashrc

-rw-r--r-- 1 root root 675 May 15 2017 .profile

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

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/17849/task/17849/fdinfo/6': No such file or directory

find: '/proc/17849/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-bandit7': Permission denied

find: '/run/screen/S-bandit0': Permission denied

find: '/run/screen/S-bandit1': Permission denied

find: '/run/screen/S-bandit12': Permission denied

find: '/run/screen/S-bandit11': Permission denied

find: '/run/screen/S-bandit10': Permission denied

```
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit27': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit20': 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
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Connecting bandit7

বুধবার, 7 জুলাই, 2021   12:26 AM

┌──(manarat㊉kali)-[~]

└─$ ssh bandit7@bandit.labs.overthewire.org -p 2220

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

bandit7@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!