10/3/21, 3:49 PM OneNote

## Finding Password

মঙ্গলবার, 6 জুলাই, 2021 4:38 PM

## bandit4@bandit:~/inhere\$ Is

-file00 -file02 -file04 -file06 -file08

-file01 -file03 -file05 -file07 -file09

bandit4@bandit:~/inhere\$ cat < -file02

## e�)�#��5��

? bandit4@bandit:~/inhere\$ cat < -file05

r = 1\$\$?h\$9('\$\$\phi\$!y\$e\$#\$x\$0\$\$\phi\$=\$\phi\$\phi\$andit:\(\circ\)inhere\$ cat < -file06

 $ly \diamondsuit \diamondsuit \diamondsuit \sim \diamondsuit \land \triangle f \diamondsuit \diamondsuit \diamondsuit \diamondsuit - E \diamondsuit \{ \diamondsuit \diamondsuit \diamondsuit m \diamondsuit \diamondsuit \diamondsuit \diamondsuit \diamondsuit m \diamondsuit \diamondsuit \diamondsuit \diamondsuit m Mbandit4@bandit:^/inhere$ cat < -file07$ 

ko ReBOKuIDDepwhWk7jZC0RTdopnAYKh

bandit4@bandit:~/inhere\$ cat < -file07

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

10/3/21, 3:49 PM OneNote

## Connecting to bandit5

মঙ্গলবার, 6 জুলাই, 2021 4:50 PM

r—(manarat⊕kali)-[~]

└\$ ssh bandit5@bandit.labs.overthewire.org -p 2220

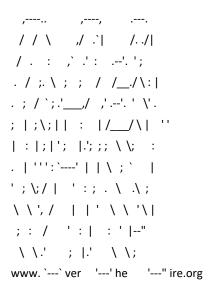
This is a OverTheWire game server. More information on <a href="http://www.overthewire.org/wargames">http://www.overthewire.org/wargames</a>

bandit5@bandit.labs.overthewire.org's password:

Permission denied, please try again.

bandit5@bandit.labs.overthewire.org's password:

Linux bandit.otw.local 5.4.8 x86\_64 GNU/Linux



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 10/3/21, 3:49 PM OneNote

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 (<a href="https://github.com/hugsy/gef">https://github.com/hugsy/gef</a>) in /usr/local/gef/
- \* pwndbg (<a href="https://github.com/pwndbg/pwndbg">https://github.com/pwndbg/pwndbg</a>) in /usr/local/pwndbg/
- \* peda (<a href="https://github.com/longld/peda.git">https://github.com/longld/peda.git</a>) in /usr/local/peda/
- \* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
- \* pwntools (<a href="https://github.com/Gallopsled/pwntools">https://github.com/Gallopsled/pwntools</a>)
- \* 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 <a href="http://www.overthewire.org/wargames/">http://www.overthewire.org/wargames/</a>

For support, questions or comments, contact us through IRC on irc.overthewire.org #wargames.

Enjoy your stay!