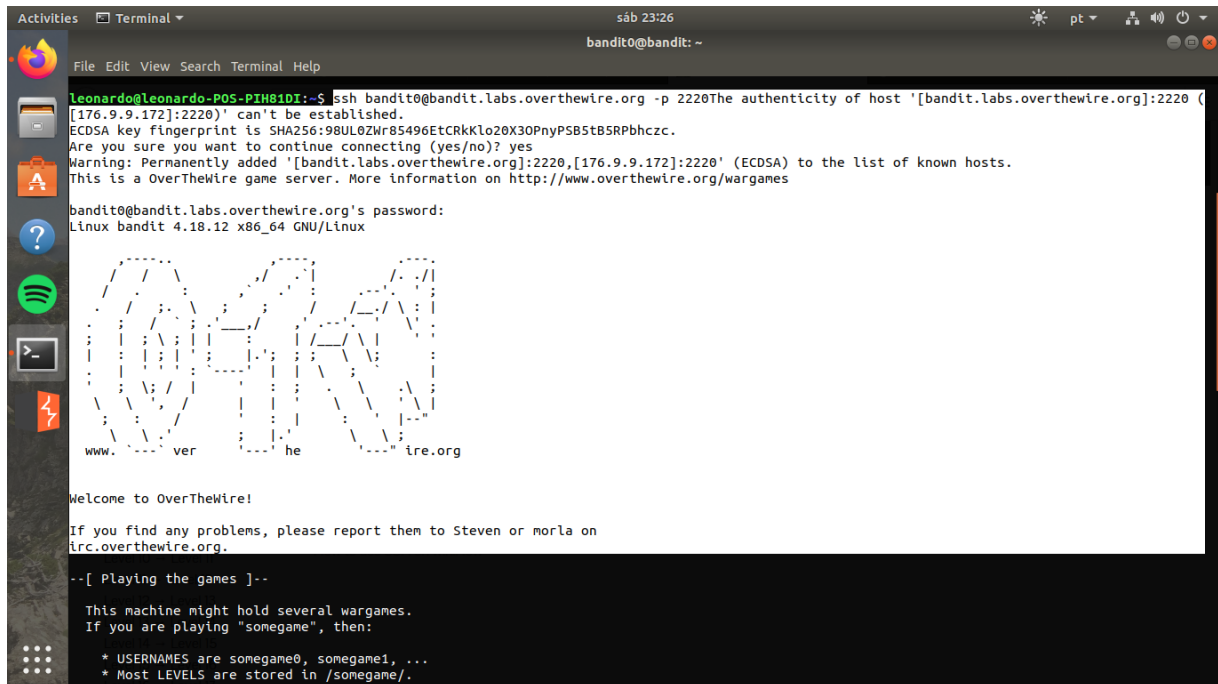


PROCESSO SELETIVO: GRIS – 2020

NOME: Leonardo Andrade

TAG OTW – BANDIT

Level 0: Logar usando SSH



```
Leonardo@Leonardo-P05-PIH8101:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5SRPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit 4.18.12 x86_64 GNU/Linux

      Oo4Ww
     www... ver... he... ire.org

Welcome to OverTheWire!

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

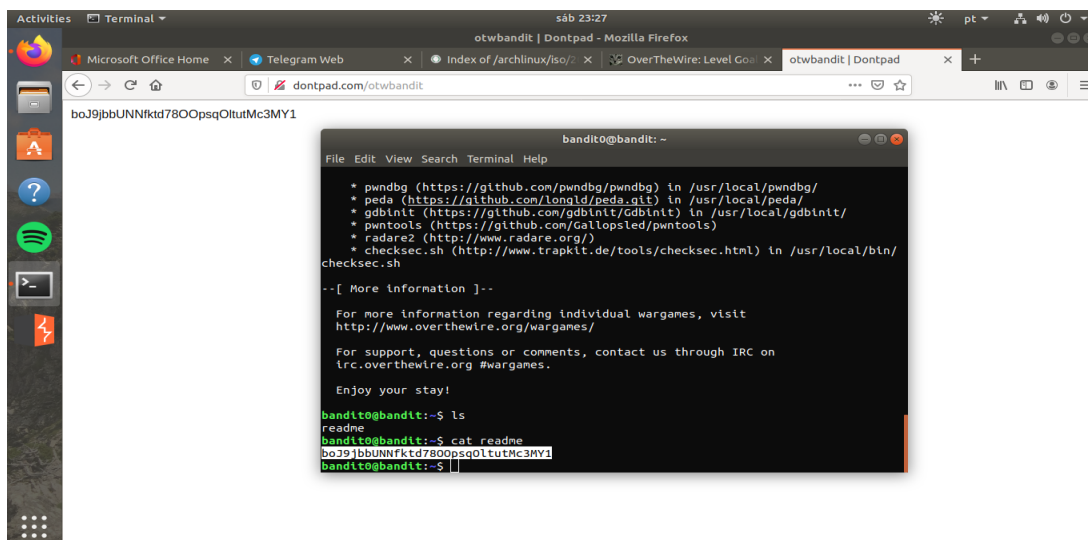
--[ Playing the games ]--

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

* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
```

Nesse desafio bastava logar e digitar a senha SSH

Level 0 – Level 1



```
bandit0@bandit: ~
File Edit View Search Terminal Help

* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* 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/

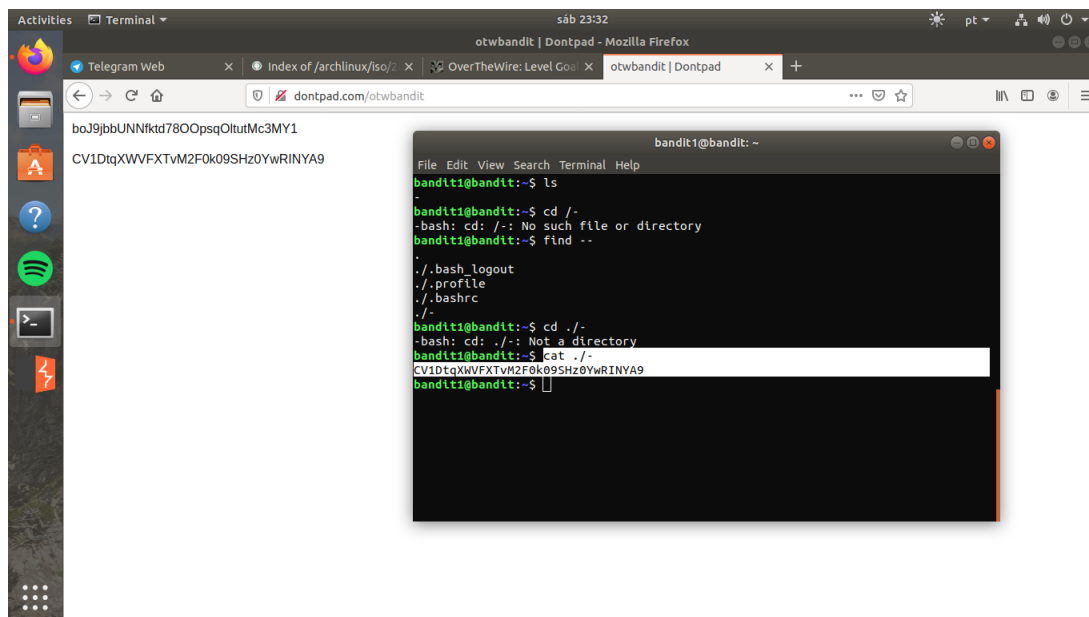
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd780Opsq0ltutMc3MY1
bandit0@bandit:~$
```

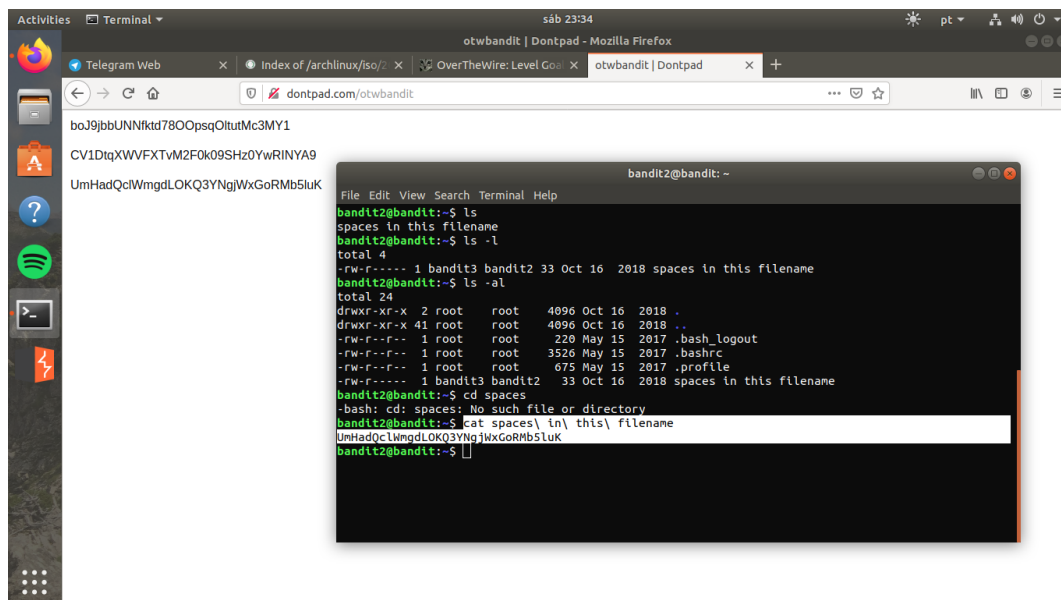
Apenas usar um cat para ler o arquivo. Abri um dontpad para ir guardando as senhas de cada desafio concluído.

Level 1 – Level 2



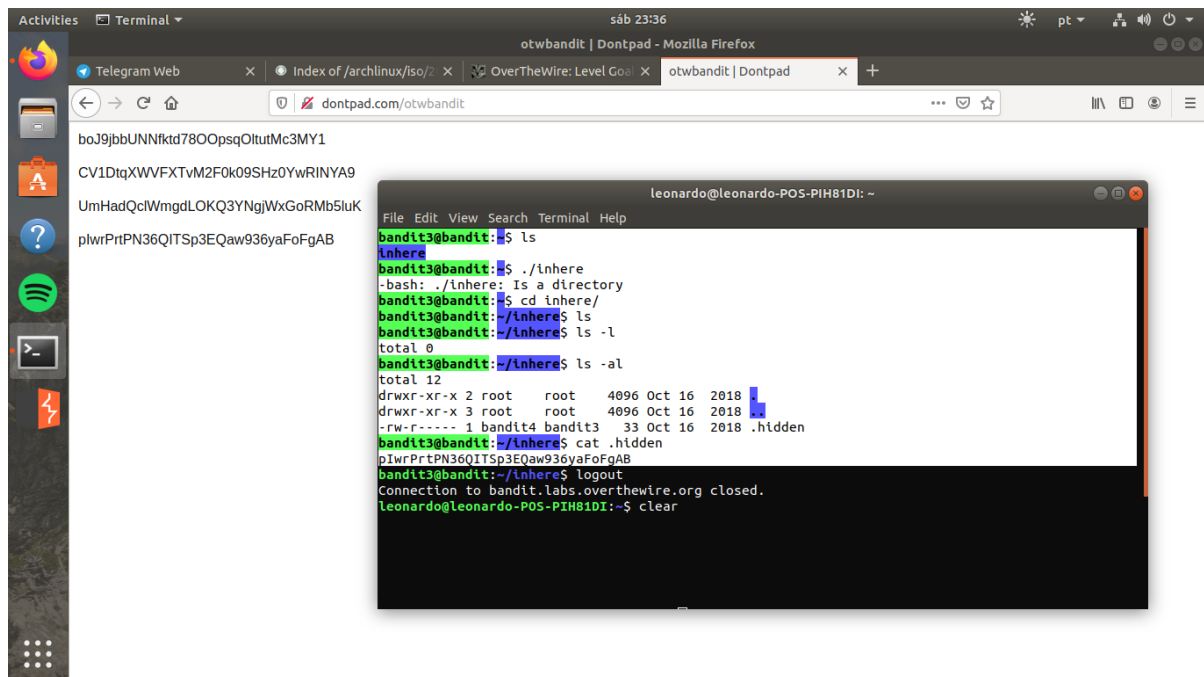
Nesse aqui tinha uma malandragem, tentei usar o cat de primeira mas não consegui. Precisava usar o “.” antes para que fosse reconhecível para o comando.

Level 2 - Level 3



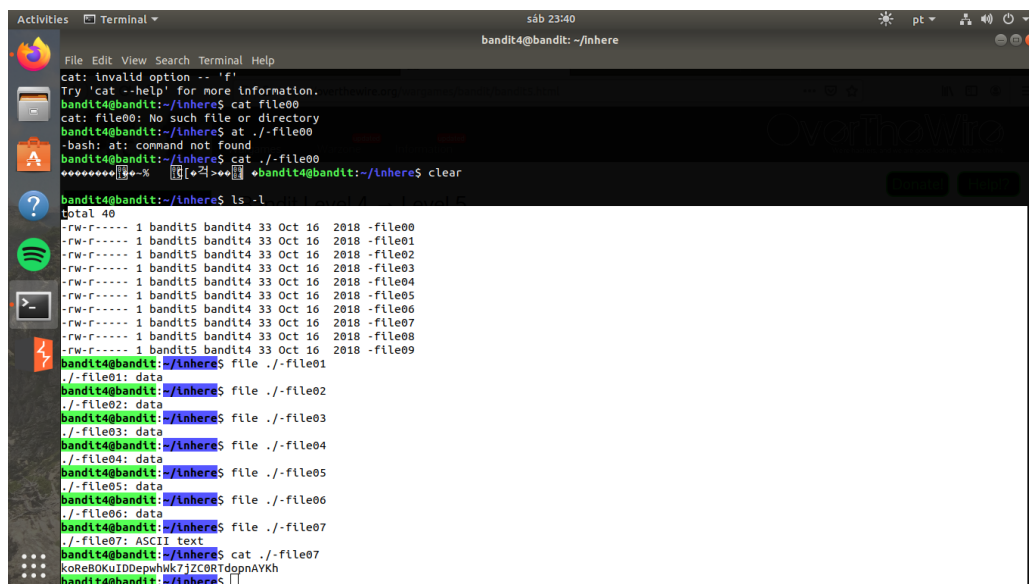
Usar “cat” novamente. Os espaços entre as palavras podem complicar um pouco, mas bastava escrever “spaces” e dar um “tab”.

Level 3 - Level 4



Usei cat de novo, porém para encontrar o nome do arquivo usei o comando ls seguido de um -al que lista todos os arquivos e diretórios.

Level 4 – Level 5



Nesse aqui eu precisei entrar no diretório e verificar quem era legível ou não, usando o "file" para isso. Quem era "data" não era legível, mas temos um que é "ASCII text", dando um cat vemos que é a nossa senha.