23 July, 24

BYTEWISE FELLOWSHIP CYBERSECURITY

Bandit Level 31-34

BY: SEERAT E MARRYUM

Bandit Level 30 → Level 31

Level Goal

There is a git repository at ssh://bandit30-git@localhost/home/bandit30-git/repo via the port 2220. The password for the user bandit30-git is the same as for the user bandit30.

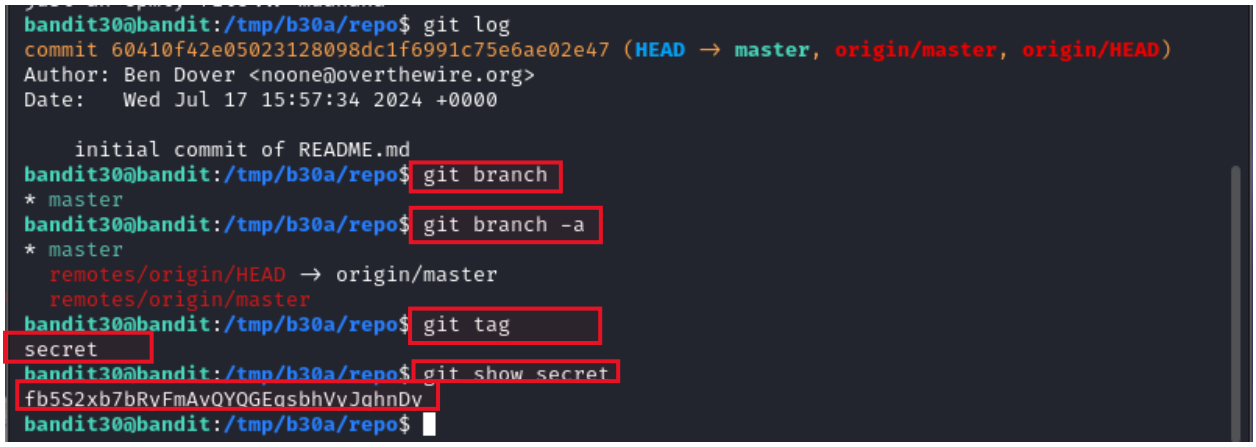
Clone the repository and find the password for the next level.

Commands you may need to solve this level

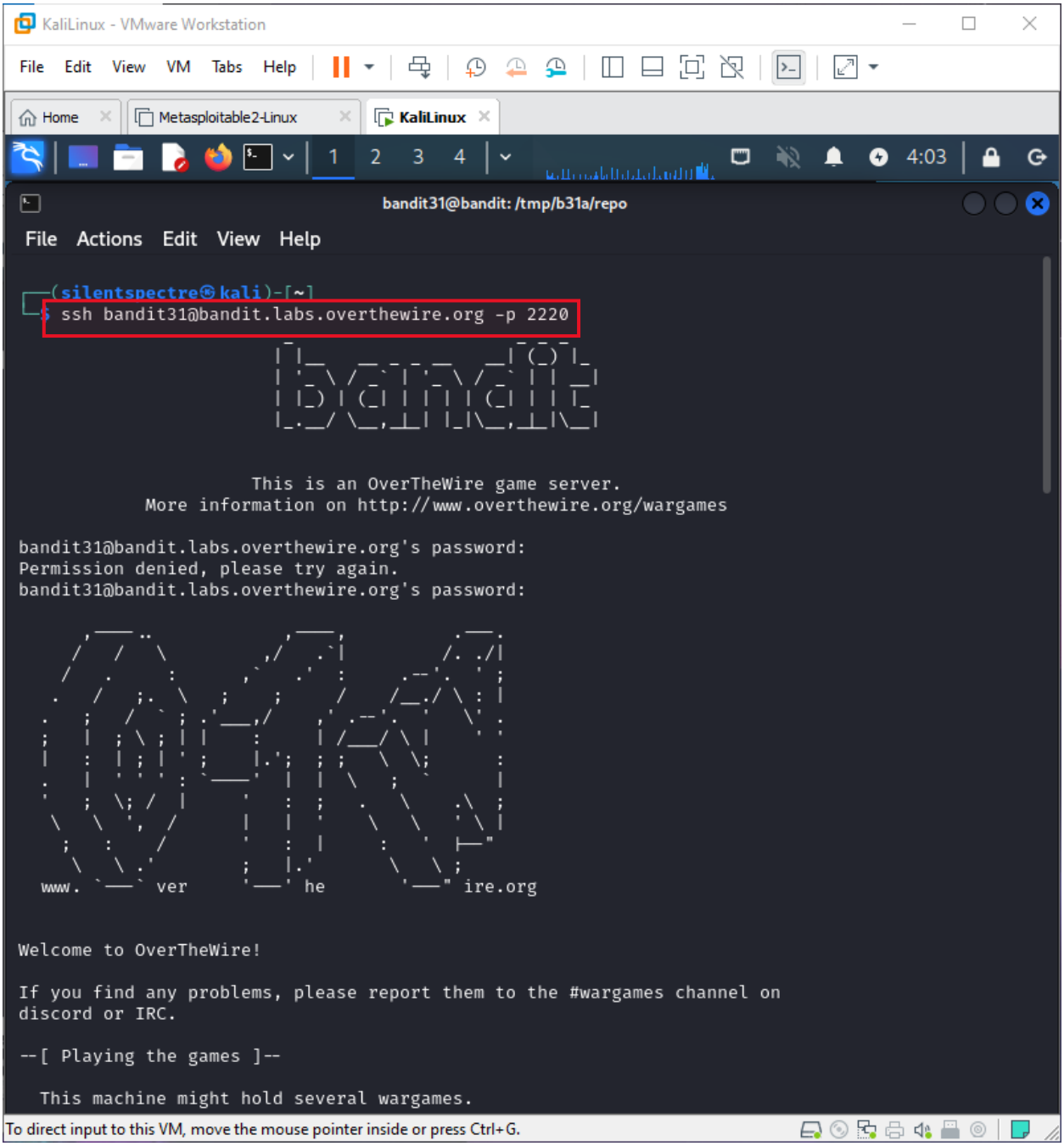
git

```
bandit30@bandit:~$ mkdir b30a
mkdir: cannot create directory ‘b30a’: Permission denied
bandit30@bandit:~$ mkdir /tmp/b30a
bandit30@bandit:~$ cd /tmp/b30a
bandit30@bandit:/tmp/b30a$ GIT_SSH_COMMAND='ssh -p 2220 -o UserKnownHostsFile=/dev/null -o Stric
tHostKeyChecking=no' git clone ssh://bandit30-git@localhost:2220/home/bandit30-git/repo
Cloning into 'repo'...
Warning: Permanently added '[localhost]:2220' (ED25519) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit30@bandit:/tmp/b30a$ ls
repo
bandit30@bandit:/tmp/b30a$ cd repo
bandit30@bandit:/tmp/b30a/repo$ ls
README.md
bandit30@bandit:/tmp/b30a/repo$ cat README.md
just an epmty file... muahaha
bandit30@bandit:/tmp/b30a/repo$ git log
commit 60410f42e05023128098dc1f6991c75e6ae02e47 (HEAD -> master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Wed Jul 17 15:57:34 2024 +0000

    initial commit of README.md
```

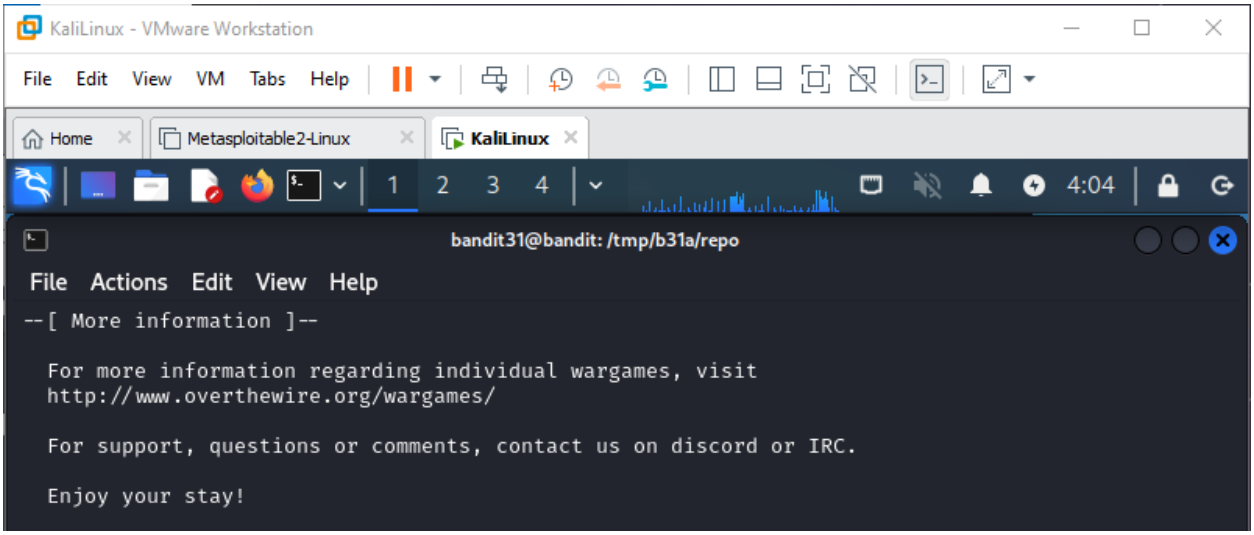
23 July, 24


bandit30@bandit:/tmp/b30a/repo$ git log
commit 60410f42e05023128098dc1f6991c75e6ae02e47 (HEAD → master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date: Wed Jul 17 15:57:34 2024 +0000
initial commit of README.md
bandit30@bandit:/tmp/b30a/repo$ git branch
* master
bandit30@bandit:/tmp/b30a/repo$ git branch -a
* master
remotes/origin/HEAD → origin/master
remotes/origin/master
bandit30@bandit:/tmp/b30a/repo$ git tag
secret
bandit30@bandit:/tmp/b30a/repo$ git show secret
fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy
bandit30@bandit:/tmp/b30a/repo$

23 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
4:03
bandit31@bandit: /tmp/b31a/repo
File Actions Edit View Help
(silentspectre㉿kali)-[~]
$ ssh bandit31@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit31@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit31@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
--[Playing the games]--
This machine might hold several wargames.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 24



Bandit Level 31 → Level 32

Level Goal

There is a git repository at ssh://bandit31-git@localhost/home/bandit31-git/repo via the port 2220. The password for the user bandit31-git is the same as for the user bandit31.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

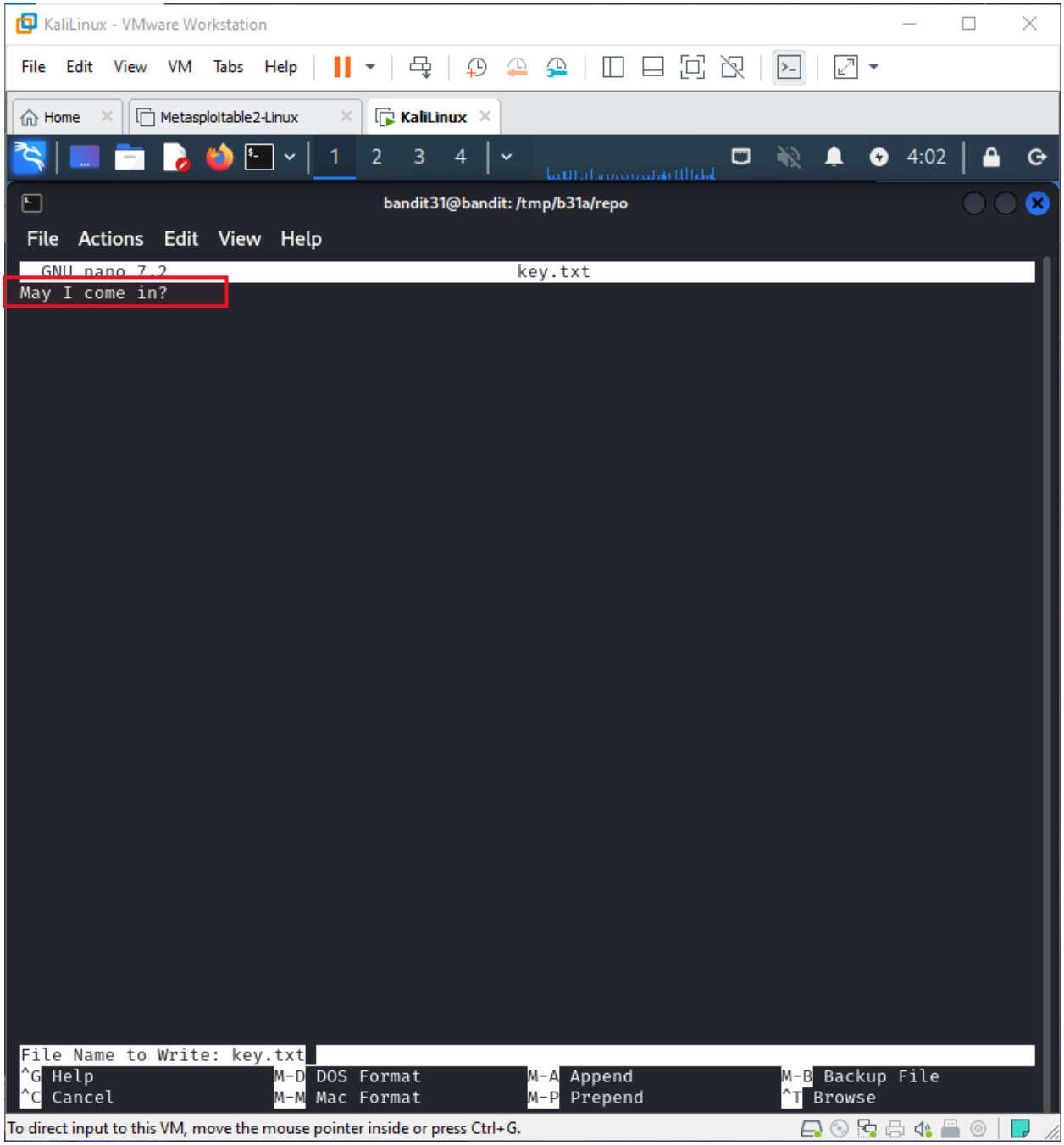
git

23 July, 24

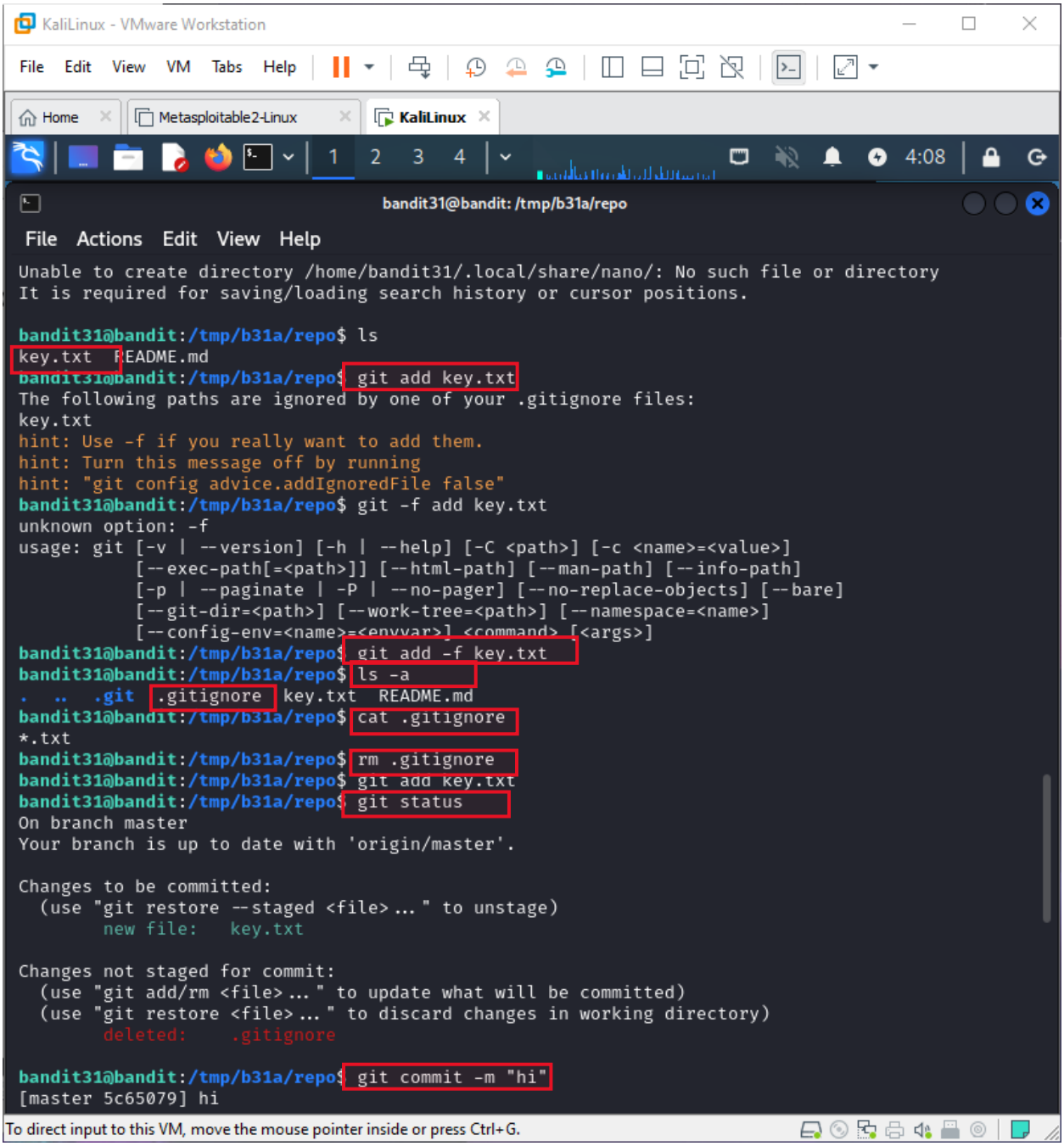
```
bandit31@bandit:~$ mkdir /tmp/b31a
bandit31@bandit:~$ cd /tmp/b31a
bandit31@bandit:/tmp/b31a$ GIT_SSH_COMMAND='ssh -p 2220 -o UserKnownHostsFile=/dev/null -o Stric
tHostKeyChecking=no' git clone ssh://bandit31-git@localhost:2220/home/bandit31-git/repo
Cloning into 'repo'...
Warning: Permanently added '[localhost]:2220' (ED25519) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit31-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/b31a$ ls
repo
bandit31@bandit:/tmp/b31a$ cd /repo
-bash: cd: /repo: No such file or directory
bandit31@bandit:/tmp/b31a$ cd repo
bandit31@bandit:/tmp/b31a/repo$ ls
README.md
bandit31@bandit:/tmp/b31a/repo$ cat README.md
This time your task is to push a file to the remote repository.
```

```
bandit31@bandit:/tmp/b31a/repo$ cat README.md
This time your task is to push a file to the remote repository.

Details:
    File name: key.txt
    Content: 'May I come in?'
    Branch: master

bandit31@bandit:/tmp/b31a/repo$ nano key.txt
```

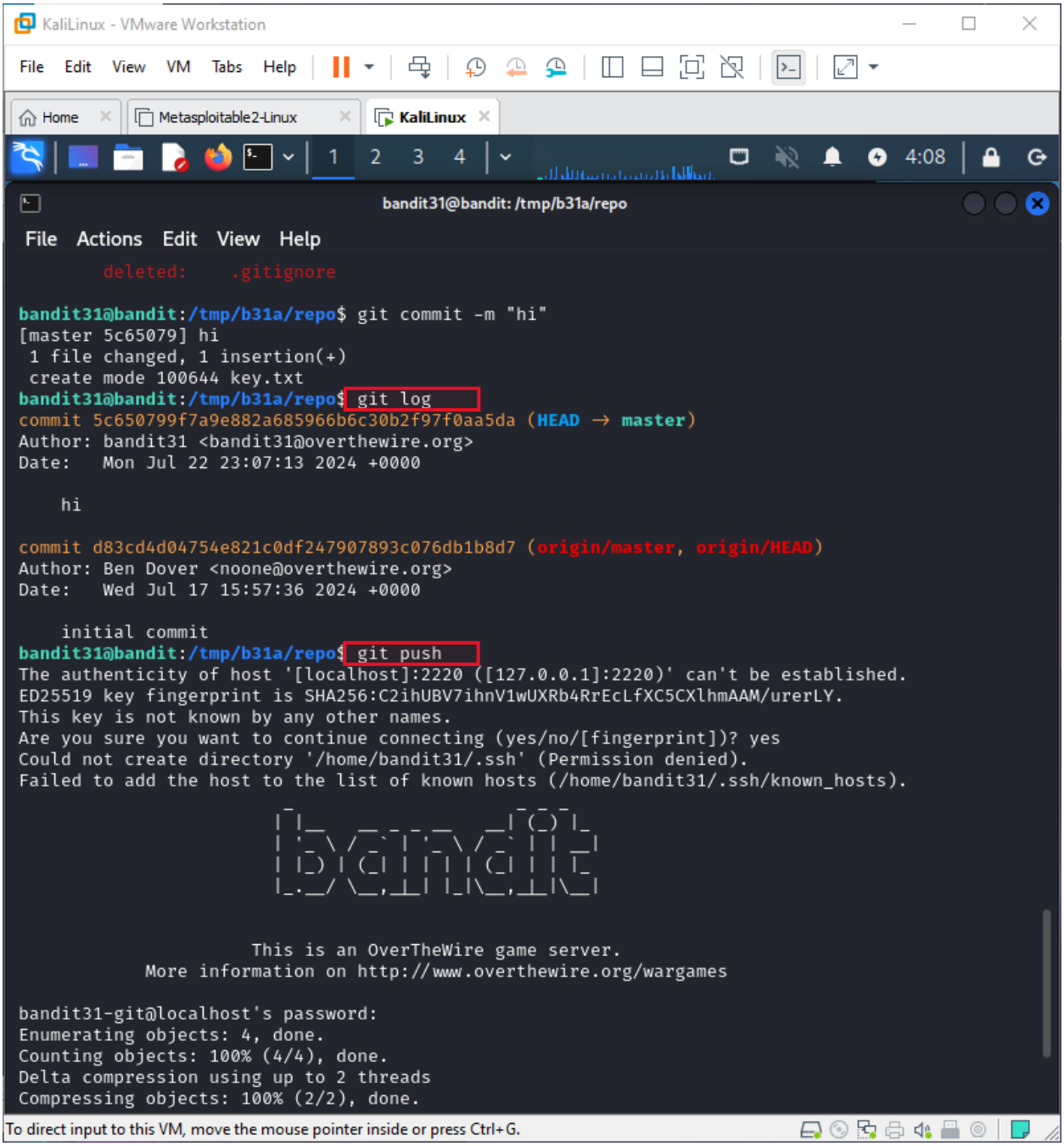
23 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
4:02
bandit31@bandit: /tmp/b31a/repo
File Actions Edit View Help
GNU nano 7.2 key.txt
May I come in?
File Name to Write: key.txt
^G Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T Browse
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

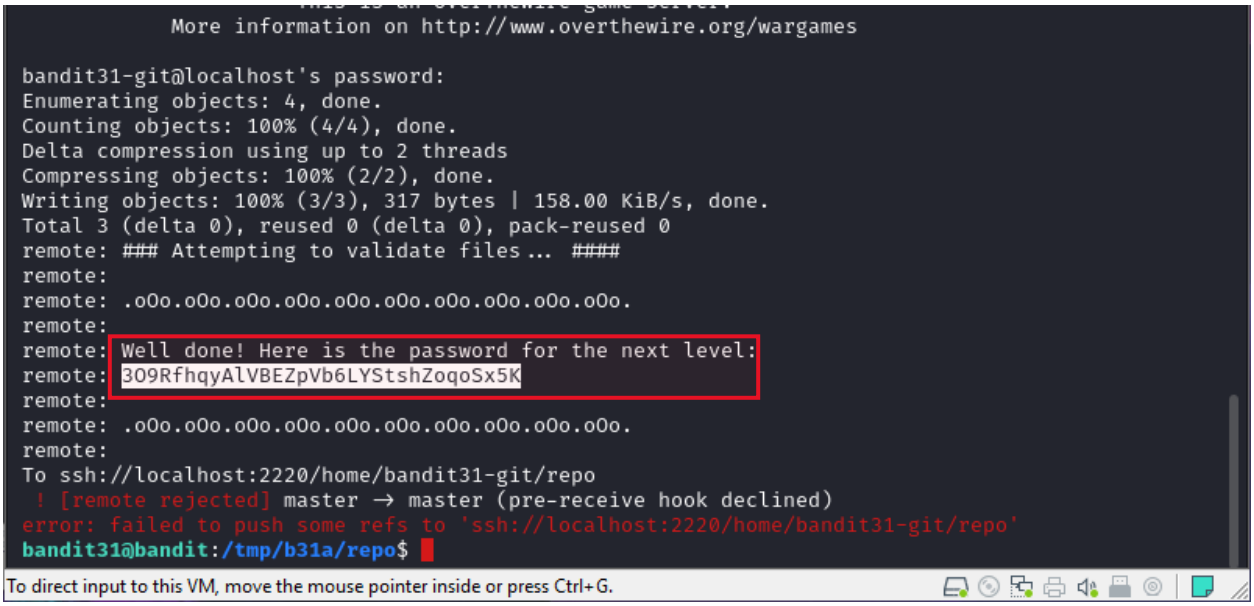
23 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
4:08
bandit31@bandit: /tmp/b31a/repo
File Actions Edit View Help
Unable to create directory /home/bandit31/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
bandit31@bandit:/tmp/b31a/repo$ ls
key.txt README.md
bandit31@bandit:/tmp/b31a/repo$ git add key.txt
The following paths are ignored by one of your .gitignore files:
key.txt
hint: Use -f if you really want to add them.
hint: Turn this message off by running
hint: "git config advice.addIgnoredFile false"
bandit31@bandit:/tmp/b31a/repo$ git -f add key.txt
unknown option: -f
usage: git [-v | --version] [-h | --help] [-C <path>] [-c <name>=<value>]
[--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
[-p | --paginate | -P | --no-pager] [--no-replace-objects] [--bare]
[--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
[--config-env=<name>=<envvar>] <command> [<args>]
bandit31@bandit:/tmp/b31a/repo$ git add -f key.txt
bandit31@bandit:/tmp/b31a/repo$ ls -a
. .. .git .gitignore key.txt README.md
bandit31@bandit:/tmp/b31a/repo$ cat .gitignore
*.txt
bandit31@bandit:/tmp/b31a/repo$ rm .gitignore
bandit31@bandit:/tmp/b31a/repo$ git add key.txt
bandit31@bandit:/tmp/b31a/repo$ git status
On branch master
Your branch is up to date with 'origin/master'.
Changes to be committed:
(use "git restore --staged <file>..." to unstage)
new file: key.txt
Changes not staged for commit:
(use "git add/rm <file>..." to update what will be committed)
(use "git restore <file>..." to discard changes in working directory)
deleted: .gitignore
bandit31@bandit:/tmp/b31a/repo$ git commit -m "hi"
[master 5c65079] hi
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

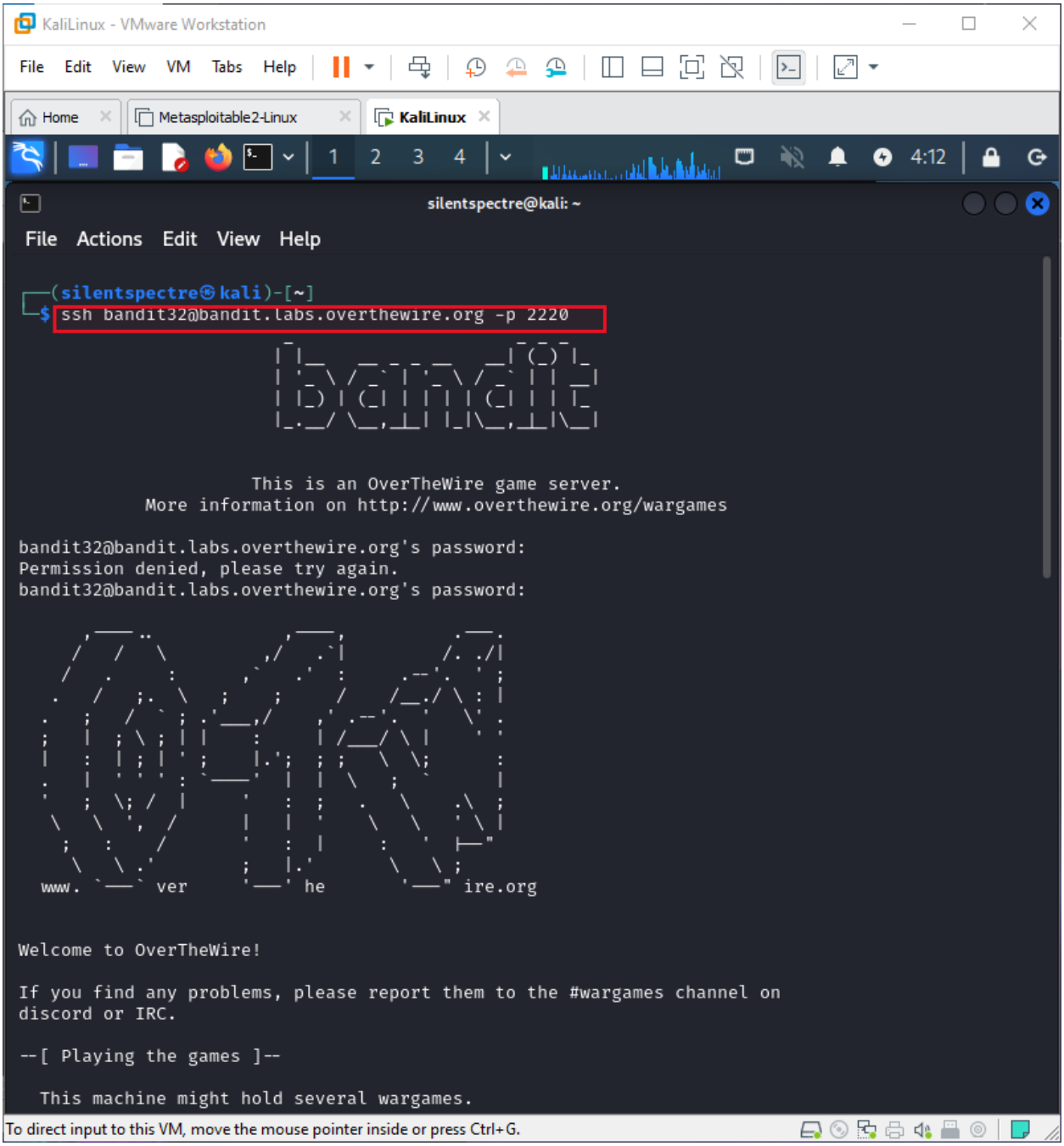
23 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
4:08
bandit31@bandit: /tmp/b31a/repo
File Actions Edit View Help
deleted: .gitignore
bandit31@bandit:/tmp/b31a/repo$ git commit -m "hi"
[master 5c65079] hi
1 file changed, 1 insertion(+)
create mode 100644 key.txt
bandit31@bandit:/tmp/b31a/repo$ git log
commit 5c650799f7a9e882a685966b6c30b2f97f0aa5da (HEAD → master)
Author: bandit31 <bandit31@overthewire.org>
Date: Mon Jul 22 23:07:13 2024 +0000
hi
commit d83cd4d04754e821c0df247907893c076db1b8d7 (origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date: Wed Jul 17 15:57:36 2024 +0000
initial commit
bandit31@bandit:/tmp/b31a/repo$ git push
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 24


More information on http://www.overthewire.org/wargames
bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 317 bytes | 158.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ####
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
! [remote rejected] master → master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
bandit31@bandit:/tmp/b31a/repo$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 24



Bandit Level 32 → Level 33

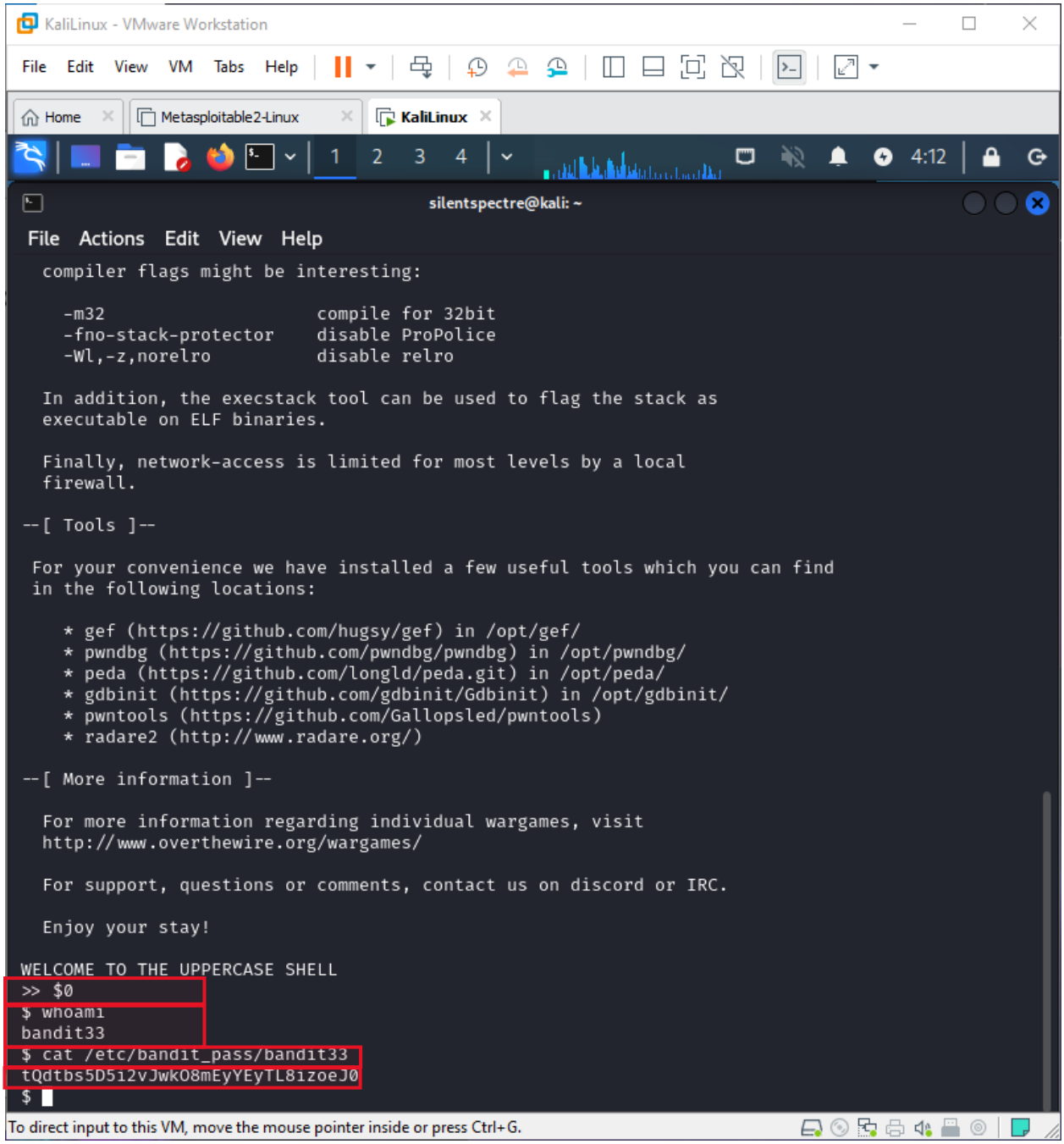
Level Goal

After all this git stuff, it’s time for another escape. Good luck!

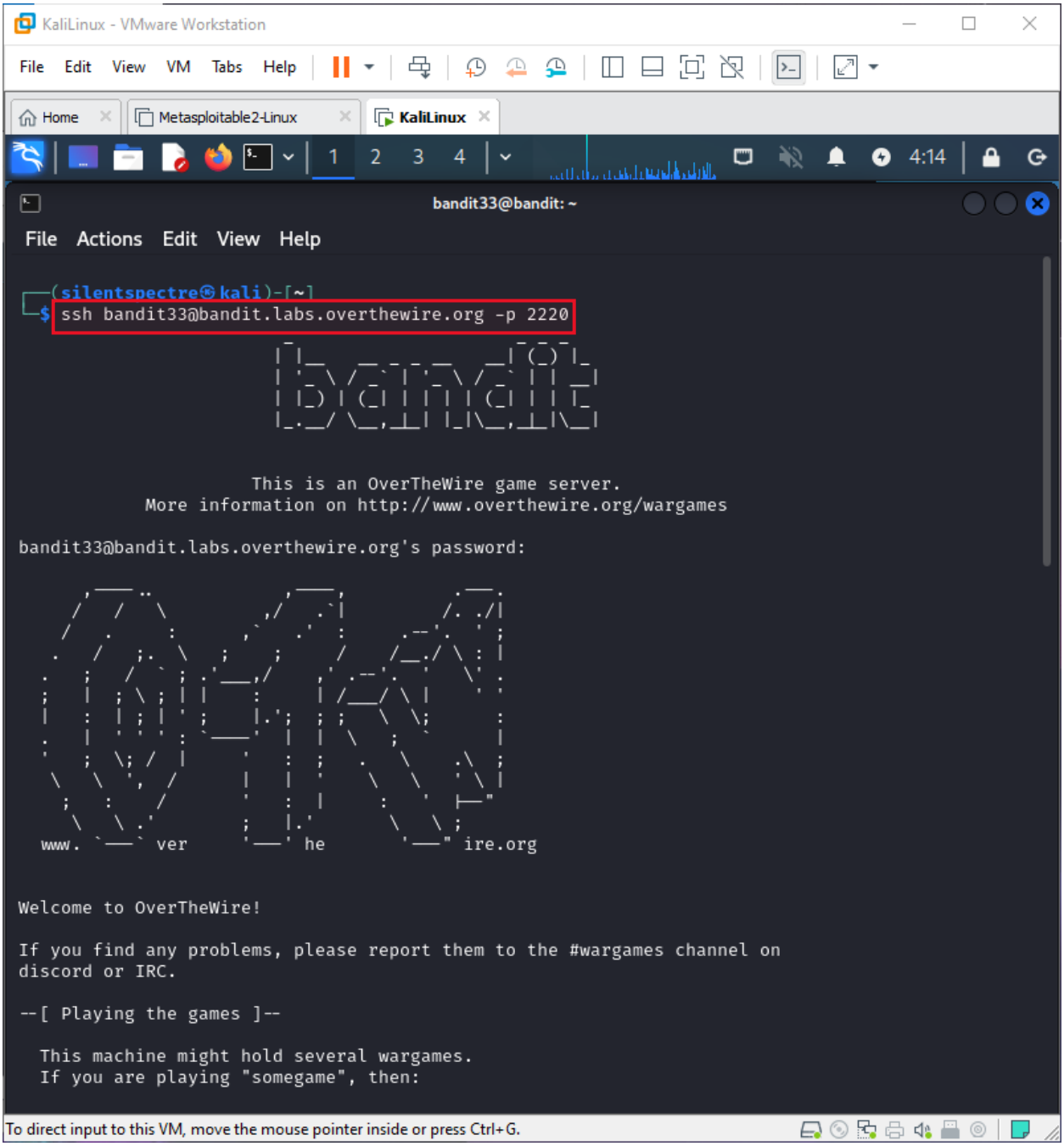
Commands you may need to solve this level

sh, man

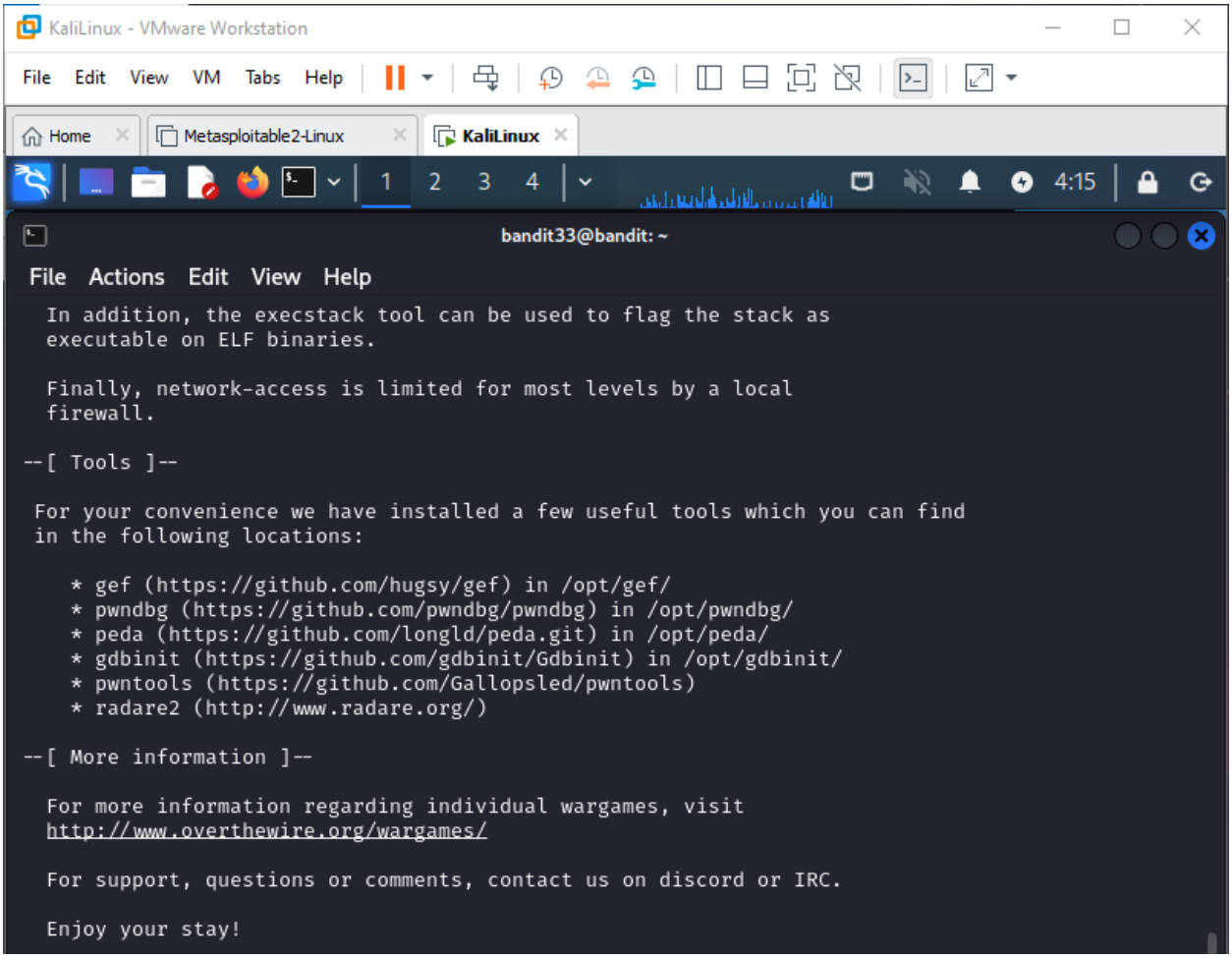
23 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
4:12
silentspectre@kali: ~
File Actions Edit View Help
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 useful tools which you can find in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
WELCOME TO THE UPPERCASE SHELL
>> $0
$ whoami
bandit33
$ cat /etc/bandit_pass/bandit33
tQdtbs5D5i2vJwkO8mEyYEyTL8izoeJ0
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 24

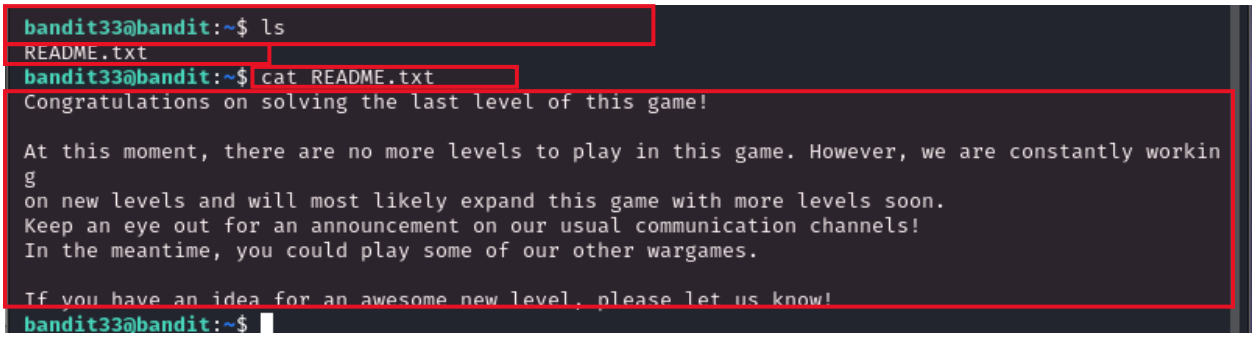

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
4:14
bandit33@bandit: ~
File Actions Edit View Help
(silentspectre㉿kali)-[~]
$ ssh bandit33@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit33@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
--[Playing the games]--
This machine might hold several wargames.
If you are playing "somegame", then:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 24



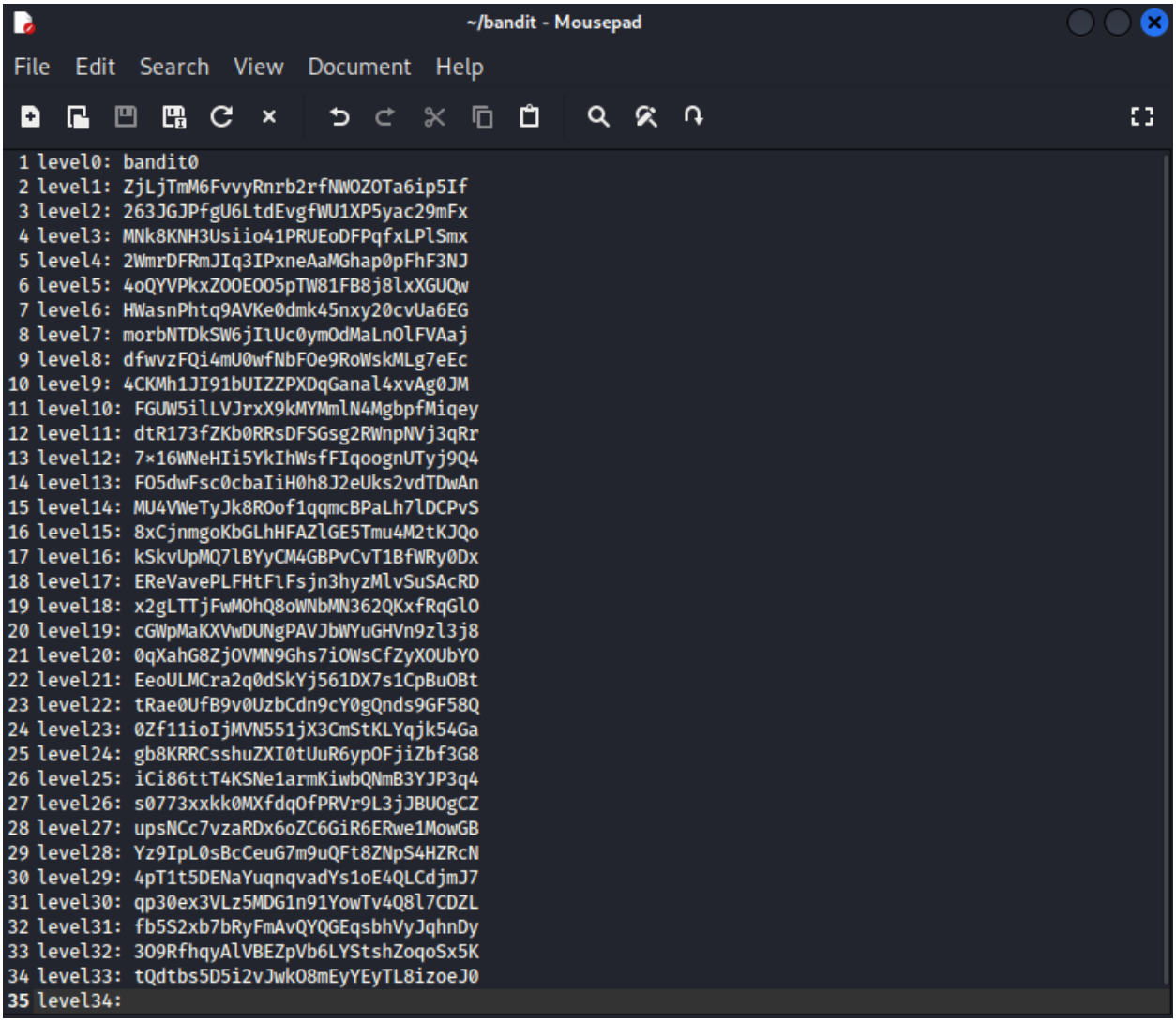
Bandit Level 33 → Level 34

At this moment, level 34 does not exist yet.



All levels passwords:

23 July, 24


~/bandit - Mousepad
File Edit Search View Document Help
1 level0: bandit0
2 level1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
3 level2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
4 level3: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
5 level4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
6 level5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
7 level6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
8 level7: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
9 level8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
10 level9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
11 level10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
12 level11: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
13 level12: 7×16WNeHIi5YkIhWsfFIqoognUTyj9Q4
14 level13: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
15 level14: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
16 level15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
17 level16: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
18 level17: EReVavePLFHtFlFsjn3hyzMlvSuSAcRD
19 level18: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
20 level19: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
21 level20: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
22 level21: EeoULMCra2q0dSkYj561DX7s1CpBuOBt
23 level22: tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
24 level23: 0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
25 level24: gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8
26 level25: iCi86ttT4KSNe1armKiwbQNmB3YJP3q4
27 level26: s0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ
28 level27: upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB
29 level28: Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN
30 level29: 4pT1t5DENaYuqnqvadYs1oE4QLCdjmJ7
31 level30: qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL
32 level31: fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy
33 level32: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K
34 level33: tQdtbs5D5i2vJwkO8mEyYEyTL8izoeJ0
35 level34: