# Objective: Recover the Elfen Ring—Answers Only

## Clone with a Difference

### Answer

You start with this from the terminal:  
git clone [git@haugfactory.com:asnowball/aws\_scripts.git](mailto:git@haugfactory.com:asnowball/aws_scripts.git)

It doesn’t work because you do not have the SSH keys, git config, and maybe .ssh/config that it needs. Instead, you need HTTPS because it is easy to use on public repos without authentication. There are two steps: replace the SSH-style git@ with https:// and change the ‘:’ with a ‘/’ to keep the web server happy.  
git clone <https://haugfactory.com/asnowball/aws_scripts.git>

Text

Description automatically generated

Put the word, maintainers, into the objective, Clone with a Difference, on your badge.

## Prison Escape

### Answer 1

The developers should not have made the host file system visible to you and should not have given you root access via sudo. They do not have to worry about permission problems when developing their application, but it is a serious security flaw. Mount the host file system just as you would [mount a CDROM](https://linuxhint.com/mount-cd-rom-centos-8/).

Text

Description automatically generated

### Answer 2

Text

Description automatically generated  
<snip>  
A picture containing text

Description automatically generated

## Jolly CI/CD

### Answer 1

First, clone the public repo with  
git clone <http://gitlab.flag.net.internal/rings-of-powder/wordpress.flag.net.internal.git>

A computer screen capture

Description automatically generated with medium confidence

Then run  
git log

  
<snip>  
A screenshot of a computer

Description automatically generated with medium confidence

Now investigate the commit called whoops with  
git show abdea0ebb21b156c01f7533cea3b895c26198c98

  
<snip>  
Text

Description automatically generated

Well, well. The file .ssh/.deploy is his private key, and deploy.pub is his public key. Note that the diff command that git is using puts a “+” at the beginning of every line to show that it is added material. Remove the “+”s to get a valid key.

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW

QyNTUxOQAAACD+wLHSOxzr5OKYjnMC2Xw6LT6gY9rQ6vTQXU1JG2Qa4gAAAJiQFTn3kBU5

9wAAAAtzc2gtZWQyNTUxOQAAACD+wLHSOxzr5OKYjnMC2Xw6LT6gY9rQ6vTQXU1JG2Qa4g

AAAEBL0qH+iiHi9Khw6QtD6+DHwFwYc50cwR0HjNsfOVXOcv7AsdI7HOvk4piOcwLZfDot

PqBj2tDq9NBdTUkbZBriAAAAFHNwb3J4QGtyaW5nbGVjb24uY29tAQ==

-----END OPENSSH PRIVATE KEY-----

Public key is one line:

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP7AsdI7HOvk4piOcwLZfDotPqBj2tDq9NBdTUkbZBri [sporx@kringlecon.com](mailto:sporx@kringlecon.com)

### Answer 2

1. There are ways to update your repo rather than deleting the local copy and starting over, but I found it easiest just to delete the old one.  
   
2. The git log gave us the username and email address.  
   A screenshot of a computer

   Description automatically generated  
   You can [add those to your Git configuration](https://support.atlassian.com/bitbucket-cloud/docs/configure-your-dvcs-username-for-commits/).  
   
3. Use a text editor in the terminal (vim or nano) to enter your stolen keys into ~/.ssh/id\_rsa and id\_rsa.pub.  
     
   Then paste  
   Text

   Description automatically generated  
   and do the same for id\_rsa.pub. Also, protect your private key.  
   Text

   Description automatically generated  
     
   If you insist on naming your keys id\_ed25519, you will need to do this:  
     
   Graphical user interface, application

   Description automatically generated
4. Test your keys. If you didn’t remove the extra characters from the git log, this will fail.  
   Text

   Description automatically generated
5. Test to see if the site will accept the keys. Remember that gitlab always uses the user ‘git’ for SSH connections.  
   Text

   Description automatically generated
6. Clone the repo using SSH and the keys you stole. To force git to use SSH you must use the correct format. git@repoHost:pathToRepo. The main github site uses the format [git@github.com:username/repoPath](mailto:git@github.com:username/repoPath), because the username is actually the first directory in its path (example: [git@github.com:john-r2/HolidayHackLessonized.git](mailto:git@github.com:john-r2/HolidayHackLessonized.git)). Our site does not put the username at the top of the path. Note: [this format is derived from scp](https://www.hostinger.com/tutorials/using-scp-command-to-transfer-files/).  
   A screenshot of a computer

   Description automatically generated with medium confidence  
   git clone [git@gitlab.flag.net.internal:rings-of-powder/wordpress.flag.net.internal.git](mailto:git@gitlab.flag.net.internal:rings-of-powder/wordpress.flag.net.internal.git)

Now that you have cloned the repo with knee-oh’s credentials, you will be able to use git push to upload changes. You can use git remote -v while inside the repository to see that it will remember you and push to the proper place using the stolen credentials.  
Text

Description automatically generated

### Answer 3

I chose to use a [simple PHP webshell](https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/php/simple-backdoor.php) to gain access to wordpress.flag.net.internal. I just used a text editor on the terminal to put the code into a file I called backdoor.php.

  
Text

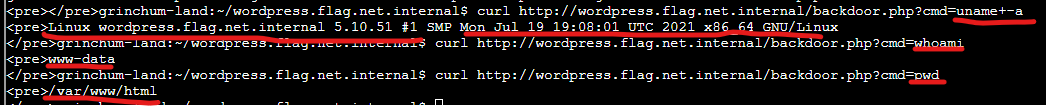
Description automatically generated

### Answer 4

A few commands, and you pwn the webserver.  
Text

Description automatically generated

### Answer 5

Pillaging is the fun part. You can use simple commands to explore a little. 

Note that if your command includes a /, you need to enclose your command in single quotes.Text

Description automatically generated

A picture containing graphical user interface

Description automatically generated

Now that you have pwn’d the WordPress server, feel free to play and see what else you can do.

At last!  
A picture containing text, device, meter, gauge

Description automatically generated