# Objective: Recover the Elfen Ring

More adventures await in the Elfen Ring, which takes us into the world of the cloud and the [Git](https://www.w3schools.com/git/git_intro.asp?remote=github) version control system. Git maintains your software repository and logs all changes you make. It can quickly revert to earlier versions if needed. [Git hosted runners](https://docs.github.com/en/actions/using-github-hosted-runners/about-github-hosted-runners) can automatically deploy changes to servers as soon as they are pushed to the Git repository. You will get a brief peek into the world of [CI/CD](https://about.gitlab.com/topics/ci-cd/).

You can manage a Git repository through a web interface or through a command line interface (CLI) which [can be installed](https://git-scm.com/book/en/v2/Getting-Started-Installing-Git) on most any operating system. Don’t worry though, it is already installed in the terminals that need it.

Graphical user interface

Description automatically generated

## Clone with a Difference

The point of this objective is to practice cloning a Git repository. There are several ways to do this, but the predominant ones are HTTPS and SSH. The HTTPS method is often used for public repositories and can be used without authentication. The SSH method usually requires public/private keys and may allow you to push changes; it always uses git as the SSH username, as in [git@github.com](mailto:git@github.com)....

Graphical user interface, application

Description automatically generated

Table

Description automatically generated with medium confidence

<https://github.com/git-guides/git-clone>

### Question

What is the command to clone the repository using HTTPS?

### Answer

You start with this command in SSH format 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

Much of your work in the cloud will be with [containers](https://cloud.google.com/learn/what-are-containers) that separate your applications from others in the cloud. Examples of containers are [Docker](https://aws.amazon.com/docker/#:~:text=Docker%20is%20a%20software%20platform,tools%2C%20code%2C%20and%20runtime.) and [Kubernetes](https://cloud.google.com/learn/what-is-kubernetes). In this challenge you will be working in a Docker container. A primary advantage of containers is that they isolate applications from the host running Docker, and from each other. As a penetration tester, your goal is to execute code or examine files in the host operating system. This is called container escape and can be quite complicated. Fortunately, it is simple in this challenge.

Text

Description automatically generated

A picture containing text

Description automatically generated

Text

Description automatically generated

You also received some great hints from Bow Ninecandle as a reward for completing his Clone with a Difference challenge.

Text

Description automatically generated

Graphical user interface, text

Description automatically generatedGraphical user interface, text

Description automatically generated

The hint, Mount Up, is key. Have you ever [mounted a CDROM in Linux](https://linuxhint.com/mount-cd-rom-centos-8/)? Remember that you will need to run your [commands with root privileges](https://xkcd.com/149/).

### Question 1

The objective asks for the contents of a file on the host file system. Gain access to the host file system.

### 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

### Question 2

Now that you have access, find the flag, and enter it in the objective. Remember that .ssh is a hidden directory.

### Answer 2

Text

Description automatically generated  
<snip>  
A picture containing text

Description automatically generated

## Jolly CI/CD

Here you will have your own environment with multiple servers. Once you have cloned their public repository (Tinsel Upatree has the link), pillage the repo for information leaks.

Graphical user interface

Description automatically generated

A picture containing text

Description automatically generated

Text

Description automatically generated

Tinsel has goodies once you solve the Prison Escape.Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

The link to the repo from Tinsel, which only works inside the terminal, is  
<http://gitlab.flag.net.internal/rings-of-powder/wordpress.flag.net.internal.git>

Depending on the load on the terminal, it may take 5 minutes or more to spin up all the servers. You can tell if they are up by  
ping gitlab.flag.net  
If you get an error message, the servers aren’t up yet.

### Question 1

Clone the public repo with HTTP. Then examine it using the git log command to find secrets. The command git show <hash value> may also be helpful.

What secrets did you find?

### 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)

### Question 2

The next step is to delete the repo you just cloned and clone it again with the credentials you stole so that you can push changes to the repo. There are several steps you need to complete before you can clone the repo with SSH. This was the most troublesome part for the people I helped with this challenge and is the reason the instructions are more detailed than usual.

1. Delete the old repo. Unless you specify a new path when you clone the repo again, it will generate an error if the old repo still exists.
2. Git needs to be [configured](https://git-scm.com/book/en/v2/Getting-Started-First-Time-Git-Setup) with a username and email address.
3. If you want to clone without modifying any configuration files for SSH, you need to name your keys as the default, ~/.ssh/id\_rsa and ~/.ssh/id\_rsa.pub. If it bothers you that the keys are ED\_25519 and you are calling them RSA, you can name the keys as you like and create a ~/.ssh/config file to tell SSH what your keys are. [See this article](https://build-me-the-docs-please.readthedocs.io/en/latest/Using_Git/SetUpSSHForGit.html), step 3. Remember to protect your private key with chmod 600 id\_rsa, or SSH will fail.
4. Check your keys for validity with [this procedure](https://support.cpanel.net/hc/en-us/articles/360056952833-How-to-verify-if-a-public-and-private-RSA-SSH-key-match-).
5. Test your keys against the SSH server with [this procedure](https://docs.github.com/en/authentication/connecting-to-github-with-ssh/testing-your-ssh-connection).
6. Finally, [clone the repo](https://ralphjsmit.com/git-custom-ssh-key) using the SSH format. I had to [prefix my URL](https://git-scm.com/book/en/v2/Git-on-the-Server-The-Protocols) in git clone with ssh:// to get it to work. Remember that the username in the SSH git clone is always git.

Clone the repo with your stolen credentials.

### 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.  
   A computer screen capture

   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

### Question 3

You can now add or change anything in the repo that you want to. Also, this site uses CI/CD, so anything that is pushed to the repository is automatically deployed to the wordpress.flag.internal webserver. You may remember this from when the terminal first came up:  
Text

Description automatically generated  
You should be cackling and rubbing your hands together at this point. You can put anything on the PHP webserver that you want to. I recommend keeping it simple.

What will you push to the wordpress.flag.net.internal server?

### 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

### Question 4

Now push your evil payload to the server. There are [instructions in this link](https://www.datacamp.com/tutorial/git-push-pull); you can start at step 5 because the repository is already established. Also, when you get to the step to push, all you need to do is use git push. Everything else is stored in your configuration (see git remote -v, above.)

Note: It is also possible to pwn the gitlab server using the gitlab yml file in the repository. The flag is not available on the gitlab server, alas.

### Answer 4

A few commands, and you pwn the webserver.  
Text

Description automatically generated

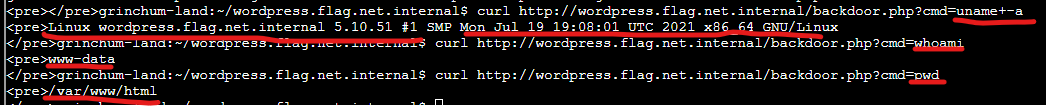
### Question 5

Now, use your access to pillage the file system and find the flag. Most Linux commands work through the simple backdoor, although you may have to enclose them in single quotes. Note that any space character should be replaced with ‘+’. Remember the usage instructions,  
  
You don’t have access to a web browser, so use curl. Note that the command above will not work through curl unless you enclose it in single quotes, 'cmd=cat+/etc/passwd'.

Be careful with the change directory (cd) command. It locked up my terminal and I had to start over.

Find the flag! Good luck!

### 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