This day will be gaining elevated privileges on an unsecure server, it is running the Jenkins service.



The dashboard looks like below.

A screenshot of a chat

Description automatically generated

**Question 1) What is the default Port for Jenkins?**

**Answer**: 8080

**Question 2) What is the password of the user Tracy?**

First I need to get inside the machine.

A close-up of a message

Description automatically generatedUnder the manage Jenkins tab, I scrolled down until I found ‘Script Console’.

A screen shot of a computer

Description automatically generatedThen I can enter a reverse shell for access.

Now I am in.

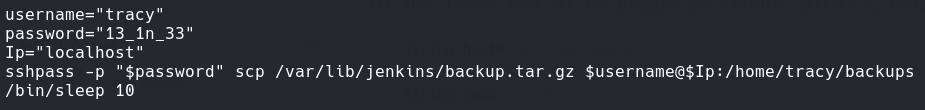
A close up of a black background

Description automatically generated

Upgrade the shell.



After snooping around for a bit, I found the backup file.



**Credentials** – tracy:13\_1n\_33

**Answer**: 13\_1n\_33

**Question 3) What is the root flag?**



After typing in the password, I now have access to the user tracy.

A screen shot of a computer screen

Description automatically generated

The security issue here is that I now have full sudo permissions to run any command as root.

Now I can switch to root.





The flag is in the root directory.

**Answer**: ezRo0tW1thoutDiD

**Question 4) What is the error message when you login as tracy again and try ‘sudo -l’ after its removal from the sudoers group?**

A black background with white text

Description automatically generatedTo remedy this security issue, the recommended practice is to do the following.

This command will the vulnerable user ‘Tracy’ from the sudoers file, meaning the privilege escalation will no longer work.

**Answer**: Sorry, user tracy may not run sudo on Jenkins.

**Question 5) What is the SSH flag?**

I will use nano to edit the /etc/ssh/sshd\_config

A close-up of white text

Description automatically generated

I will comment out the include line and then change password-authentication to no.

Then I will restart the service.



**Why do this?**

Remember that as attackers, we were able to use SSH in this server to move laterally from a lower-level user. In light of this, we can disable password-based SSH logins so we can thwart the possibility of an SSH login via compromised plaintext credentials that are just lying around.

**Answer**: Ne3d2SecureTh1sSecureSh31l

**Question 6) What is the Jenkins flag?**

Then key directory for this question is /var/lib/Jenkins.



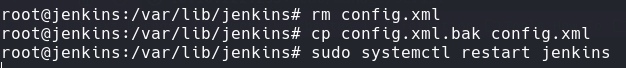
Thinking back, how did I get in? Using the web service Jenkins implementation. This is because the system administrator used a full trust policy, while you want to be using a zero-trust implementation. Instead of allowing the dashboard to be accessible to everyone it’s best to only allow specific users.

A screen shot of a computer

Description automatically generatedSince there is two config.xml files, I will use the backup one.

A screen shot of a computer

Description automatically generatedThe orange part of the text I will configure. Everything will be uncommented.

Now I can replace the file and restart the service.

**Answer**: FullTrust\_has\_n0\_Place1nS3cur1ty