☰   🔍 (https://profile.intra.42.fr/searches)   **milyass**

(https://profile.intra.42.fr)

SCALE FOR PROJECT BOOT2ROOT (/PROJECTS/42CURSUS-BOOT2ROOT)

You should evaluate 4 students in this team

★

Git repository

`git@vogsphere-v2.1337.ma:vogsphere/intra-uuid-9bee0d83-fb6b-4` 📋

Introduction

For the smooth running of this evaluation, please respect the following rules:

- Remain polite, kind, respectful and constructive whatever happens during
this conversation. It's a matter of confidence between you and the
42 community.

- Highlight the potential problems you've had with the work you're presented
to the person or the group you're grading, and take the time to talk about
and discuss those issues.

- Accept the fact that the exam subject or required functions might lead
to different interpretations. Listen to your discussion partner's
perspective with an open mind (are they right or wrong ?) and grade them as
fairly as possible.
42's teaching methods can make sense only if peer-evaluation is
taken seriously.

Guidelines

- You must only evaluate what you will find in the student's or group's
GiT repository.

- Take the time to check that the GiT repository matches the student or
group and the project.

- Double check that no malicious alias was used to mislead you and make you
grade something different from the official repository content.

- If a script supposed to help evaluate the exam is supplied by either side, the
other side will have to strictly check it to avoid nasty surprises.

- If the evaluating student has not yet taken this project, they will have to
read the exam subject in its entirety before starting the evaluation.

- Use the flags available on this grading system to signal an empty or non-
functional project, a norm flaw, cheating, etc. In that case, evaluation stops
and final grade is 0 (or -42 if it's a cheating problem). However, if it's
not a cheating problem, you are invited to keep talking about the work that
has been done (or not done, as a matter of fact) in order to identify the
issues that lead to this stalemate and avoid it next time.

- Assessment must be made with a virtual machine running Linux with a core >
3.14 with root rights.

- In order to verify that the user is the real root, verify the user_id is
indeed 0 as is the whoami command response. Beware: it takes a real shell to
prove the user is indeed the system's root and not just a service such as a
database.

Attachments

📝 subject.pdf (https://cdn.intra.42.fr/pdf/pdf/75162/en.subject.pdf)

🔗 Born2root.iso (https://cdn.intra.42.fr/isos/BornToSecHackMe-v1.1.iso)

boot2root

Check git

Preliminaries

Before starting the evaluation, please check the following:

- The project includes 2 writeup
- The project includes the folders required in the subject,
- No binary should be included in the repository.
- The writeup must indicate ways to become root on the server WITHOUT exploiting the given ISO file.

We would like to remind you that if an explanation involves modifying/extracting the iso file and/or an action when
loading it into the virtual machine, you must use the CHEAT flag.

Each explanation must show a way to get a shell with the server's root user. If, at the end of an explanation,
the end user is not the server's root user, the solution will not be valid.

If either point is invalid, assessment stops.

⊘ Yes   ✕ No

Mandatory part

Required explanation for each step of these writeup.

First writeup

Two group members must be able to explain each step in order to exploit
the server.

The evaluator will select the two members.

Other group members will not be able to help.

Each step will require explanations.

By following the explanations of the different steps used, the evaluator should be able
to understand what is being done in a clear manner In case of any doubt, the evaluator can
ask any questions he wants.

If an explanation does not seem VERY clear it is recommended to end the evaluation at this point.
You must use the appropriate flag.

The explanation must show a way to get a shell with the server's root user.
If, at the end of an explanation, the end user is not the server's root user, the solution will not be valid.

We would like to remind you that if an explanation involves modifying/extracting the iso file and/or an action when
loading it into the virtual machine, you must use the CHEAT flag.

Rate it from 0 (failed) through 5 (excellent)

(5)

Second writeup

Two group members must be able to explain each step in order to exploit
the server.

The evaluator will select the two members.

Other group members will not be able to help.

Each step will require explanations.

By following the explanations of the different steps used, the evaluator should be able
to understand what is being done in a clear manner In case of any doubt, the evaluator can
ask any questions he wants.

If an explanation does not seem VERY clear it is recommended to end the evaluation at this point.
You must use the appropriate flag.

The explanation must show a way to get a shell with the server's root user.
If, at the end of an explanation, the end user is not the server's root user, the solution will not be valid.

We would like to remind you that if an explanation involves modifying/extracting the iso file and/or an action when loading it into the virtual machine, you must use the CHEAT flag.

Rate it from 0 (failed) through 5 (excellent)

○

Bonus

Bonus

If a bonus is included, evaluate it the same way you evaluated the rest of the project.

There should be one writeup per solution, and each should describe each step used to gain root access on the server.

You can give 2 points for a bonus if it is really inventive and uses many different skills/tools.

Otherwise, it's one point per bonus.

Each explanation must show a way to get a shell with the server's root user. If, at the end of an explanation, the end user is not the server's root user, the solution will not be valid.

We would like to remind you that if an explanation involves modifying/extracting the iso file and/or an action when loading it into the virtual machine, you must use the CHEAT flag.

Rate it from 0 (failed) through 5 (excellent)

○

Ratings

Don't forget to check the flag corresponding to the defense

✔ Ok   ★ Outstanding project

▌ Empty work   ▌ Incomplete work   ☠ Invalid compilation   ▛ Cheat   ♟ Crash

👤 Incomplete group   ⚠ Concerning situation

Conclusion

Leave a comment on this evaluation

Finish evaluation

Terms of use for video surveillance (https://profile.intra.42.fr/legal/terms/1)
Rules of procedure (https://profile.intra.42.fr/legal/terms/4)
Declaration on the use of cookies (https://profile.intra.42.fr/legal/terms/2)
General term of use of the site (https://profile.intra.42.fr/legal/terms/6)
Legal notices (https://profile.intra.42.fr/legal/terms/3)
Privacy policy (https://profile.intra.42.fr/legal/terms/5)